Citrix ADC SDX 13.1

Machine translated content

Disclaimer

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

Contents

Introduction

June 13, 2022

L'appliance Citrix ADC SDX est une plateforme mutualisée sur laquelle vous pouvez provisionner et gérer plusieurs machines virtuelles Citrix ADC (instances). L'appliance SDX répond aux exigences de cloud computing et de mutualisation en permettant à un seul administrateur de configurer et de gérer l'appliance et de déléguer l'administration de chaque instance hébergée aux locataires. L'appliance SDX permet à l'administrateur de l'appliance de fournir à chaque locataire les avantages suivants :

- Une instance complète. Chaque instance dispose des privilèges suivants :
  - Ressources dédiées pour CPU et mémoire
  - Un espace séparé pour les entités
  - L'indépendance nécessaire pour gérer la version et la construction de leur choix
  - Indépendance du cycle de vie
- Un réseau complètement isolé. Le trafic destiné à une instance particulière est envoyé uniquement à cette instance.

L'appliance SDX fournit un service de gestion préconfiguré sur l'appliance. Le service de gestion fournit une interface utilisateur (modes HTTP et HTTPS) et une API pour configurer, gérer et surveiller l'appliance, le service de gestion et les instances. Un certificat auto-signé Citrix est préemballé pour la prise en charge HTTPS. Citrix vous recommande d'utiliser le mode HTTPS pour accéder à l'interface utilisateur du service de gestion.

Notes de publication

January 27, 2022

Les notes de publication décrivent les améliorations, les modifications, les corrections de bogues et les problèmes connus pour une version ou un build particulier du logiciel Citrix ADC. Les notes de mise à jour de Citrix ADC SDX sont abordées dans le cadre des notes de mise à jour de Citrix ADC.

Pour obtenir des informations détaillées sur les améliorations de SDX 13.1, les problèmes connus et les corrections de bogues, consultez lesnotes de publication de Citrix ADC.

Premiers pas avec l'interface utilisateur du service de gestion

January 27, 2022

Pour commencer à configurer, gérer et surveiller l'appliance, le service de gestion et les instances virtuelles, connectez-vous à l'interface utilisateur du service de gestion à l'aide d'un navigateur. Provisionnez ensuite les instances virtuelles sur l'appliance.

Vous pouvez vous connecter à l'interface utilisateur du service de gestion en utilisant l'un des navigateurs pris en charge suivants :

- Internet Explorer
- Google Chrome
- Apple Safari
- Mozilla Firefox

Ouvrez une session sur l'interface utilisateur du service de gestion

1. Dans le champ d'adresse de votre navigateur Web, saisissez l'un des éléments suivants :

   `http://Management Service IP Address`

   ou

   `https://Management Service IP Address`

2. Sur la page Connexion, dans Nom d'utilisateur et mot de passe, tapez le nom d'utilisateur et le mot de passe du service de gestion. Le nom d'utilisateur par défaut est `nsroot`. Si le mot de passe par défaut précédent ne fonctionne pas, essayez de saisir le numéro de série de l'appliance. Le code à barres du numéro de série est disponible à l'arrière de l'appliance. Citrix vous recommande de modifier le mot de passe par défaut après la configuration initiale. Pour plus d'informations sur la modification du mot de passe administrateur, consultez Modification du mot de passe du compte d'utilisateur par défaut.

3. Cliquez sur Afficher les options, puis procédez comme suit :

   a) Dans la liste **Commencer dans**, sélectionnez la page qui doit être affichée immédiatement après que vous vous êtes connecté à l'interface utilisateur. Les options disponibles sont Accueil, Surveillance, Configuration, Documentation et Téléchargements. Par exemple, si vous souhaitez que le service de gestion affiche la page Configuration lorsque vous ouvrez une session, sélectionnez **Configuration** dans la liste **Démarrer dans** .

   b) Dans **Délai**d'expiration, tapez la durée (en minutes, heures ou jours) après laquelle vous souhaitez que la session expire. La valeur minimale du délai d'expiration est de 15 minutes.

   Les paramètres **Début** et **Délai d'expiration sont** conservés d'une session à l'autre. Leurs valeurs par défaut ne sont restaurées qu'après avoir effacé le cache.

4. Cliquez sur **Connexion** pour vous connecter à l'interface utilisateur du service de gestion.

Assistant de configuration initiale

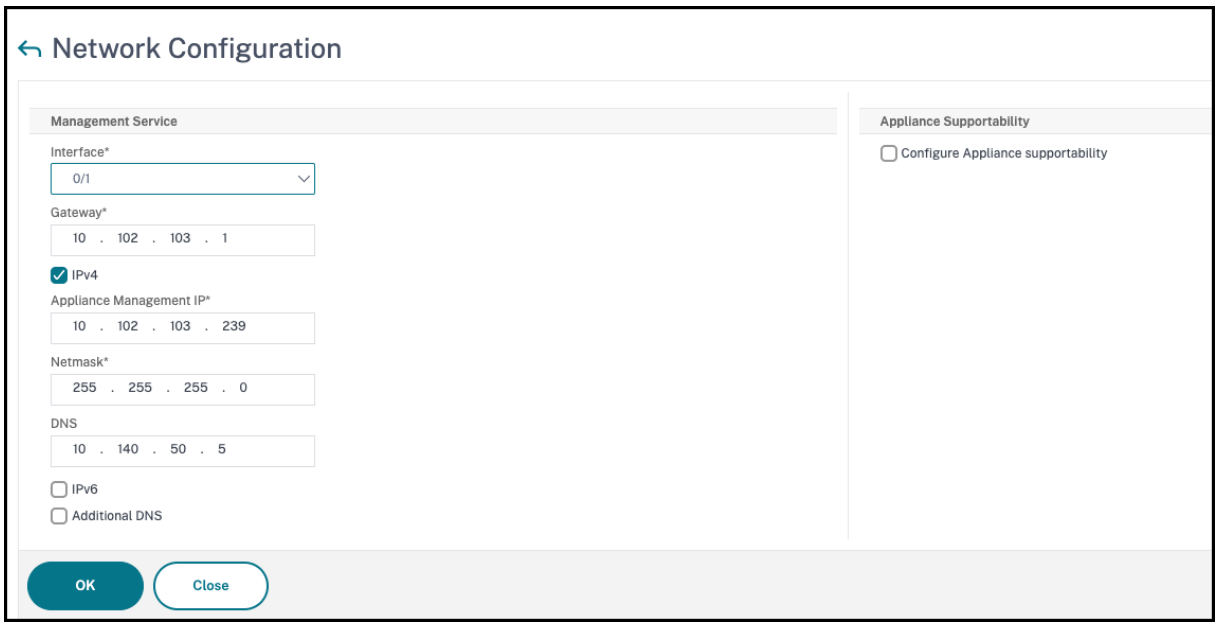
Vous pouvez utiliser l'assistant d'installation pour effectuer toutes les premières configurations en un seul flux.

Vous pouvez utiliser l'Assistant pour configurer les détails de configuration réseau et les paramètres système, modifier le mot de passe administratif par défaut et gérer et mettre à jour les licences.

Vous pouvez également utiliser cet Assistant pour modifier les détails de configuration réseau que vous avez spécifiés pour l'appliance SDX lors de la configuration initiale.

Pour accéder à l'Assistant, accédez à **Configuration > Système** et, sous **Configurer le matériel**, cliquez sur **Assistant d'installation**. Entrez des valeurs pour les paramètres suivants.

- **Interface : interface** de gestion qui connecte l'appliance à un poste de travail ou à un réseau de gestion. Valeurs possibles : 0/1, 0/2. Valeur par défaut : 0/1.
- **Passerelle :** adresse IP du routeur qui transfère le trafic hors du sous-réseau de l'appliance.
- Activez la case à cocher IPv4 si vous souhaitez utiliser l'adresse IPv4 pour le service de gestion et entrez les détails des paramètres suivants :
  - **IP de gestion du matériel :** adresse IPv4 utilisée pour accéder au service de gestion à l'aide d'un navigateur Web.
  - **Masque réseau : masque** de sous-réseau dans lequel se trouve l'appliance SDX.
- **DNS :** adresse IPv4 du serveur DNS principal. Les adresses IPv6 ne sont pas prises en charge pour le serveur DNS principal.
- Activez la case à cocher IPv6 si vous souhaitez utiliser l'adresse IPv6 pour le service de gestion et entrez les détails des paramètres suivants :
  - **Adresse IP du service de gestion :** adresse IPv6 utilisée pour accéder au service de gestion à l'aide d'un navigateur Web.
  - **Adresse IPv6 de la passerelle :** adresse IPv4 du routeur qui transfère le trafic hors du sous-réseau de l'appliance.
- Sélectionnez **DNS supplémentaire** pour ajouter des adresses IP de serveur DNS en tant que serveur DNS supplémentaire en dehors du serveur DNS principal. Les adresses IP peuvent être IPv4 ou IPv6.



> **Important**
>
> Citrix vous recommande de garder la prise en charge des appareils désactivée pour améliorer la sécurité. Pour désactiver la prise en charge du matériel, accédez à **Système > Configuration réseau** et décochez la case **Configurer la prise en charge du matériel** .

Sous **Paramètres système**, vous pouvez spécifier que le service de gestion et une instance Citrix ADC doivent communiquer entre eux uniquement via un canal sécurisé. Vous pouvez également restreindre l'accès à l'interface utilisateur du service de gestion. Les clients peuvent ouvrir une session sur l'interface utilisateur du service de gestion uniquement en utilisant https.

Vous pouvez modifier le fuseau horaire du service de gestion et de Citrix Hypervisor. Le fuseau horaire par défaut est UTC. Vous pouvez modifier le mot de passe administratif en cochant la case **Modifier le mot de passe** et en saisissant le nouveau mot de passe.

Sous Gérer les licences, vous pouvez gérer et allouer des licences. Vous pouvez utiliser votre numéro de série matériel (HSN) ou votre code d'accès de licence pour attribuer vos licences. Si une licence est déjà présente sur votre ordinateur local, vous pouvez également la télécharger sur l'appliance.

Sélectionnez les licences sur l'appliance et cliquez sur **Terminé** pour terminer la configuration initiale.

Provisionner des instances sur une appliance SDX

Vous pouvez mettre en service une ou plusieurs instances Citrix ADC ou tierces sur l'appliance SDX à l'aide du service de gestion. Le nombre d'instances que vous pouvez installer dépend de la licence que vous avez achetée. Si le nombre d'instances ajoutées est égal au nombre spécifié dans la licence, le service de gestion n'autorise pas le provisionnement d'autres instances.

Pour plus d'informations sur le provisionnement d'instances tierces, consultez la section Machines virtuelles tierces.

Accès à la console

Vous pouvez accéder à la console des instances Citrix ADC, au service de gestion, à Citrix Hypervisor et aux machines virtuelles tierces à partir de l'interface du service de gestion. Cet accès est utile pour le débogage et le dépannage des instances hébergées sur l'appliance SDX.

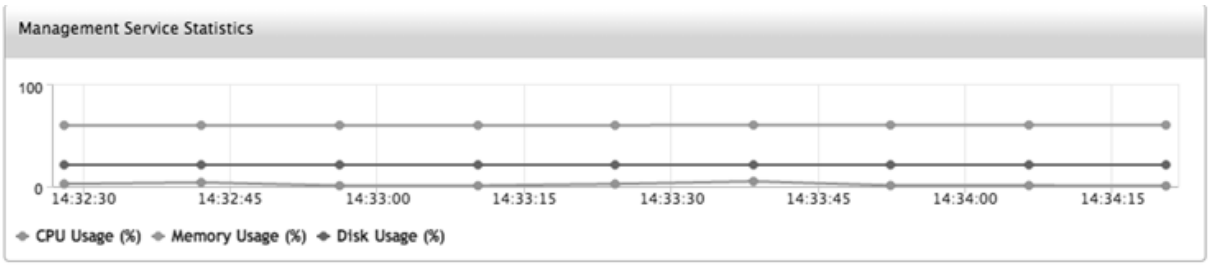
Pour accéder à la console des machines virtuelles, accédez à la liste des instances, sélectionnez la machine virtuelle dans la liste, puis dans la liste **Action**, cliquez sur **Accès à la console**.

Pour accéder à la console de Management Service ou Citrix Hypervisor, accédez à **Configuration > Système**, puis sous **Accès à la console**, cliquez sur le lien **Service de gestion** ou **Citrix Hypervisor** .

Remarque : le navigateur Internet Explorer ne prend pas en charge l'accès à la console. Citrix recommande d'utiliser la fonctionnalité d'accès à la console uniquement via les sessions HTTPS du service de gestion.

Statistiques du service de gestion

Le tableau de bord inclut désormais les statistiques du service de gestion pour surveiller l'utilisation de la mémoire, du processeur et des ressources de disque par le service de gestion sur l'appliance SDX.



Authentification unique au service de gestion et aux instances Citrix ADC

Après vous être connecté au service de gestion à l'aide de vos informations d'identification utilisateur, vous n'avez pas à fournir à nouveau les informations d'identification de l'utilisateur pour vous connecter à une instance. Par défaut, la valeur **Timeout** est définie sur 30 minutes et l'onglet de configuration s'ouvre dans une nouvelle fenêtre de navigateur.

Gérer la page d'accueil

La page d'accueil du service de gestion fournit une vue d'ensemble des performances de l'appliance SDX et des instances provisionnées sur votre appliance. Les informations relatives à l'appliance et à

l'instance SDX sont affichées dans des gadgets que vous pouvez ajouter et supprimer en fonction de vos besoins.

Les gadgets suivants sont disponibles par défaut sur la page d'accueil.

- **Ressources système :** affiche le nombre total de cœurs de processeur, le nombre total de puces SSL, le nombre de puces SSL libres, la mémoire totale et la mémoire libre sur l'appliance.
- **CPU du système | Utilisation de la mémoire (%) :** affiche le pourcentage d'utilisation du processeur et de la mémoire de l'appliance au format graphique.
- **Débit WAN/LAN du système (Mbits/s) :** affiche le débit total de l'appliance SDX pour le trafic entrant et sortant dans un graphique tracé en temps réel et mis à jour à intervalles réguliers.
- **Instances Citrix ADC :** affiche les propriétés des instances Citrix ADC. Les propriétés affichées sont Nom, État de la machine virtuelle, État de l'instance, Adresse IP, Rx (Mbit/s), Tx (Mbits/s), Req/s HTTP et Utilisation du processeur (%) et Utilisation de la mémoire (%).
  Remarque : Lors de la première connexion, la page d'accueil n'affiche aucune donnée relative aux instances Citrix ADC car vous n'avez provisionné aucune instance sur votre appliance.
- **Événements de surveillance de l'état :** affiche les 25 derniers événements, avec leur gravité, leur message, ainsi que la date et l'heure auxquelles l'événement s'est produit.

Vous pouvez effectuer les opérations suivantes sur la page d'accueil :

- Afficher et masquer les détails de l'instance Citrix ADC

  Vous pouvez afficher et masquer les détails d'une instance Citrix ADC particulière en cliquant sur le nom de l'instance dans la colonne Nom.
  Vous pouvez également cliquer sur Développer tout pour développer tous les nœuds d'instance et sur Réduire tout pour réduire tous les nœuds d'instance.

- Ajouter et supprimer des gadgets

  Vous pouvez également ajouter des gadgets pour afficher d'autres informations système.

  Pour ajouter ces gadgets, cliquez sur la flèche («) dans le coin supérieur droit de la page d'accueil, saisissez des mots clés dans la zone de recherche, puis cliquez sur OK. Les caractères autorisés sont : a-z, A-Z, 0—9, ^, $, * et _. Cliquez sur OK sans saisir de caractère dans la zone de recherche pour afficher tous les gadgets disponibles. Une fois le gadget affiché, cliquez sur Ajouter au tableau de bord.

  Actuellement, vous pouvez ajouter les gadgets suivants à la page d'accueil :

  - **Détails de l'hyperviseur :** le gadget Détails de l'hyperviseur affiche des informations sur la disponibilité, l'édition, la version, le nom qualifié iSCSI (IQN) de Citrix Hypervisor, le code produit, le numéro de série, la date de build et le numéro de build.
  - **Licences :** le gadget Licences affiche les informations suivantes : la plate-forme matérielle SDX, le nombre maximum d'instances prises en charge sur la plate-forme, le débit maximum pris en charge en Mbit/s et le débit disponible en Mbit/s.

Si vous supprimez un gadget qui est disponible sur la page d'accueil par défaut, vous pouvez le réajouter à la page d'accueil en recherchant le gadget.

Ports

Les ports suivants doivent être ouverts sur l'appliance SDX pour qu'elle fonctionne correctement.

Type	Port	Détails
TCP	80	Utilisé pour les requêtes HTTP entrantes (GUI et NITRO). L'une des principales interfaces permettant d'accéder à l'interface du service de gestion SDX.
TCP	443	Utilisé pour les requêtes HTTP sécurisées entrantes (GUI et NITRO). L'une des principales interfaces permettant d'accéder à l'interface du service de gestion SDX.
TCP	22	Utilisé pour l'accès SSH et SCP à l'interface du service de gestion SDX.
UDP	162	L'interface du service de gestion SDX écoute les interruptions SNMP provenant des instances Citrix ADC hébergées sur l'appliance SDX.
UDP	161	L'interface du service de gestion SDX écoute les demandes pas/get SNMP.

Gouvernance des données

January 27, 2022

Qu'est-ce qu'un service Citrix ADM Connect ?

Citrix Application Delivery Management (ADM) Service Connect est une fonctionnalité qui permet une intégration transparente des appliances Citrix ADC SDX au service Citrix ADM. Cette fonctionnalité permet à l'appliance Citrix ADC SDX de se connecter automatiquement et en toute sécurité au service Citrix ADM et de lui envoyer des données système, d'utilisation et de télémétrie. Sur la base de ces données, vous obtenez des informations et des recommandations pour votre infrastructure Citrix ADC sur le service Citrix ADM.

En utilisant la fonctionnalité de connexion au service Citrix ADM et en intégrant vos appliances Citrix ADC SDX au service Citrix ADM, vous pouvez gérer tous vos actifs Citrix ADC et Citrix Gateway, que ce soit sur site ou dans le cloud. En outre, vous bénéficiez d'un accès à un ensemble complet de fonctionnalités de visibilité qui permettent d'identifier rapidement les problèmes de performances, l'utilisation élevée des ressources, les erreurs critiques, etc. Le service Citrix ADM offre un large éventail de fonctionnalités pour vos instances et applications Citrix ADC. Pour plus d'informations sur le service Citrix ADM, consultez la section Citrix Application Delivery Management Service.

> **Important**
>
> - Ce document concerne les appliances Citrix ADC SDX. Pour plus d'informations sur l'appliance Citrix ADC, consultez Présentation de Citrix ADM Service Connect pour les appliances Citrix ADC.
> - Citrix Gateway prend également en charge la fonctionnalité de connexion au service Citrix ADM. Pour plus de facilité, l'appliance Citrix Gateway n'est pas appelée explicitement dans les sections consécutives.

Remarque :
la fonctionnalité de connexion au service Citrix ADM a été publiée pour les instances Citrix ADC et les instances Citrix Gateway. Toutefois, la fonctionnalité correspondante sur le service Citrix ADM est disponible dans la prochaine version. La valeur de cette fonctionnalité sera bientôt dévoilée avec la version de service Citrix ADM. Citrix mettra à jour cette note dès que cela se produira.
Les avantages de cette nouvelle fonctionnalité peuvent être utilisés une fois publiés sur le service Citrix ADM.

Qu'est-ce que le service Citrix ADM ?

Le service Citrix ADM est une solution basée sur le cloud qui vous aide à gérer, surveiller, orchestrer, automatiser et dépanner vos instances Citrix ADC SDX en vous fournissant des informations analytiques et des recommandations organisées basées sur l'apprentissage automatique sur les instances Citrix ADC SDX et sur l'état des applications, les performances et sécurité. Pour plus d'informations, consultez la section Vue d'ensemble du service Citrix ADM.

Comment la connexion du service Citrix ADM est-elle activée ?

Citrix ADM Service Connect est activé par défaut, après avoir installé ou mis à niveau Citrix ADC SDX vers la version 13.1.

Quelles sont les données capturées à l'aide de Citrix ADM Service Connect ?

Les informations suivantes sont capturées à l'aide de Citrix ADM Service Connect :

- **Informations sur Citrix ADC SDX**
  - Adresse IP de gestion
  - Description de la plateforme
  - Type de plateforme
  - Nom d'hôte
  - ID système
  - Numéro de série codé
  - Version
  - ID de série
  - ID d'hôte
  - Type
  - Type de construction
- **Indicateurs d'utilisation clés**
  - Pourcentage de CPU de gestion
  - Pourcentage d'utilisation de la mémoire
  - Pourcentage d'utilisation de l'UC
  - Temps de disponibilité du système
  - Date et heure du système

Comment les données sont-elles utilisées ?

En collectant les données, Citrix peut fournir en temps opportun des informations détaillées sur vos installations Citrix ADC SDX, notamment :

- **Principales mesures**. Détails des mesures clés relatives au processeur, à la mémoire, au débit, au débit SSL et mise en évidence du comportement anormal sur les instances Citrix ADC SDX.
- **Erreurs critiques**. Toute erreur critique susceptible de se produire sur vos instances Citrix ADC.
- **Avis de déploiement**. Identifiez les instances Citrix ADC déployées en mode autonome, mais qui présentent un débit élevé et sont vulnérables à un point de défaillance unique.

Combien de temps les données collectées sont-elles conservées ?

Toutes les données collectées sont conservées pendant 13 mois au maximum.

Si vous décidez de mettre fin à l'utilisation du service en désactivant la fonctionnalité de connexion du service Citrix ADM depuis Citrix ADC, toutes les données collectées précédemment sont supprimées après une période de 30 jours.

Où les données sont stockées et dans quelle mesure sont-elles sécurisées ?

Toutes les données collectées par le service Citrix ADM connect sont stockées dans l'une des trois régions, soit les États-Unis, l'Union européenne et l'Australie et la Nouvelle-Zélande (ANZ). Pour plus d'informations, voir Considérations géographiques.

Les données sont stockées en toute sécurité avec une isolation stricte des locataires au niveau de la couche de base de données.

Comment désactiver Citrix ADM service connect ?

Si vous souhaitez désactiver la collecte de données via Citrix ADM Service Connect, consultez Comment activer et désactiver Citrix ADM Service Connect.

Présentation du service Citrix ADM connect pour les appliances Citrix ADC SDX

January 27, 2022

Le service Citrix ADM est une solution basée sur le cloud qui vous aide à gérer, surveiller, orchestrer, automatiser et dépanner vos appliances Citrix ADC SDX. Il fournit également des informations analytiques et des recommandations basées sur l'apprentissage automatique pour la santé, les performances et la sécurité de vos applications. Pour de plus amples informations, consultez la section Service Citrix ADM.

La connexion au service Citrix Application Delivery Management (ADM) permet une intégration transparente des appliances Citrix ADC SDX au service Citrix ADM. Cette fonctionnalité permet aux appliances Citrix ADC SDX et au service Citrix ADM de fonctionner comme une solution holistique, offrant aux clients de multiples avantages.

La fonctionnalité de connexion au service Citrix ADM permet à l'instance Citrix ADC SDX de se connecter automatiquement au service Citrix ADM et de lui envoyer des données de système, d'utilisation et de télémétrie. À l'aide de ces données, le service Citrix ADM vous fournit des informations et des recommandations sur votre infrastructure Citrix ADC SDX, telles que l'identification rapide des problèmes de performances et l'utilisation élevée des ressources.

Pour exploiter la puissance du service Citrix ADM, vous pouvez choisir d'intégrer vos appliances Citrix ADC SDX au service Citrix ADM. Le processus d'intégration utilise ADM Service Connect et rend l'expérience fluide et rapide pour vous.

> **Points à noter**
>
> - Citrix ADM Service Connect est désormais disponible sur les instances Citrix ADC MPX, SDX et VPX, ainsi que sur les appliances Citrix Gateway.
> - La connexion au service Citrix ADM n'est pas encore disponible sur le service Citrix ADM.

Pour plus d'informations, voir Gouvernance des données.

Comment le service Citrix ADM se connecte-t-il au service Citrix ADM ?

Voici un flux de travail de haut niveau sur la façon dont la fonctionnalité de connexion du service Citrix ADM sur Citrix ADC interagit avec le service Citrix ADM.

1. La fonctionnalité de connexion au service Citrix ADM sur l'appliance Citrix ADC SDX se connecte automatiquement au service Citrix ADM à l'aide d'une demande de sonde périodique.
2. Cette demande contient des données système, d'utilisation et de télémétrie, à l'aide desquelles le service Citrix ADM vous fournit des informations et des recommandations sur votre infrastructure Citrix ADC, telles que l'identification rapide des problèmes de performances et l'utilisation élevée des ressources.
3. Vous pouvez consulter les informations et les recommandations et décider d'intégrer vos appliances Citrix ADC SDX au service Citrix ADM pour commencer à gérer vos appliances Citrix ADC SDX.
4. Lorsque vous décidez d'intégrer, la fonctionnalité de connexion au service Citrix ADM permet de terminer l'intégration en toute transparence.

Sur quelles versions de Citrix ADC Citrix ADM Service Connect est-il pris en charge ?

Citrix ADM Service Connect est pris en charge sur toutes les plates-formes Citrix ADC et tous les modèles d'appliance (MPX, VPX et SDX). À partir de Citrix ADC version 13.0 build 64.xx, Citrix ADM Service Connect est activé par défaut pour les appliances Citrix ADC SDX.

Comment activer la connexion au service Citrix ADM ?

Si vous êtes un client Citrix ADC existant et que vous effectuez une mise à niveau vers Citrix ADC version 13.0 build 64.xx, Citrix ADM Service Connect est activé par défaut dans le cadre du processus de mise à niveau.

Si vous êtes un nouveau client Citrix ADC et que vous installez Citrix ADC version 13.0 build 64.xx, Citrix ADM Service Connect est activé par défaut dans le cadre du processus d'installation.

> **Remarque**
>
> Contrairement aux nouvelles appliances Citrix ADC, les appliances Citrix ADC SDX existantes trouvent l'itinéraire via Citrix Insight Service (CIS) ou Call Home.

Comment activer et désactiver la connexion au service Citrix ADM ?

Vous pouvez activer et désactiver la connexion au service Citrix ADM à partir des méthodes CLI, GUI ou NITRO API.

Utilisation de la CLI

Pour activer le service Citrix ADM, connectez-vous à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set autoreg_setting autoreg=true
```

Pour désactiver le service Citrix ADM se connecter à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set autoreg_setting autoreg=false
```

Pour afficher les paramètres Citrix ADM Service Connect à l'aide de l'interface de ligne de commande

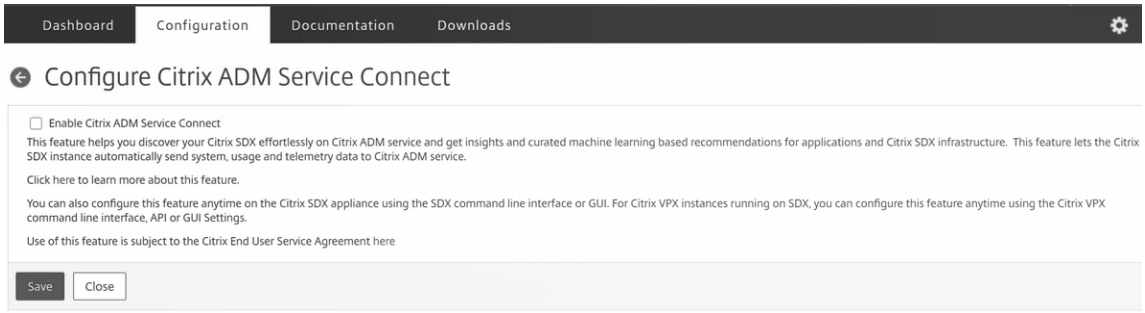
```
show autreg_setting

                autoreg: true

     is_banner_displayed: true

Done
```

Utilisation de l'interface graphique

Pour désactiver le service Citrix ADM, connectez-vous à l'aide de l'interface graphique Citrix ADC.

1. Accédez à **Système**. Sur la page **Système**, cliquez sur **Configurer la connexion au service Citrix ADM** dans la section **Paramètres système** .

2. Sur la page **Configurer les paramètres ADM**, **désactivez Activer la connexion au service Citrix ADM**, puis cliquez sur **OK**.



Utilisation de l'API NITRO

Vous pouvez désactiver Citrix ADM Service Connect à l'aide de la commande NITRO .

```
curl -X PUT -H "Content-Type:application/json"http://192.0.2.10/nitro/v1/config/sdx_autoreg -d '{ "sdx_autoreg":{ "autoreg":"false" } } ' -u nsroot:Test@1
```

Comportement de l'agent intégré Citrix ADM

À partir de Citrix ADC version 13.0 build 61.xx et supérieures, les instances Citrix ADC SDX disposent d'un agent intégré avec la fonctionnalité de connexion au service ADM. L'agent intégré Citrix ADM disponible sur les instances Citrix ADC SDX démarre comme un démon actif et communique avec le service ADM. Une fois la communication établie avec le service ADM, l'agent intégré se met automatiquement à niveau vers la dernière version logicielle régulièrement.

Références

Pour plus d'informations sur Citrix ADM service connect, consultez les rubriques suivantes :

- Gouvernance des données : gouvernance des données.
- Service Citrix ADM : Citrix Application Delivery Management Service.

Mise à niveau unique

November 9, 2022

Remarque : La connexion au service Citrix ADM est activée par défaut, après avoir installé ou mis à niveau l'appliance Citrix ADC SDX vers la version 13.1. Pour plus de détails, consultez la section Gouvernance des données et connexion au service Citrix ADM.

La mise à niveau d'un bundle unique, disponible à partir des versions 11.0 et ultérieures, combine tous les composants, à l'exception de l'image d'instance ADC VPX et du microprogramme LOM, dans un seul fichier image. Ce fichier s'appelle l'image SDX.

> **Remarque**
>
> À partir de la version 12.0 build 57.19, le microprogramme de gestion de l'éclairage (LOM) est ajouté au SBI et les clients Citrix n'ont pas à mettre à niveau le LOM séparément. Le microprogramme LOM n'est pas écrit par Citrix.

À l'aide de cette image, vous pouvez mettre à niveau tous les composants en une seule étape, éliminant ainsi les risques d'incompatibilité entre les différents composants. La mise à niveau d'un bundle unique garantit également que votre appliance exécute toujours une version que Citrix a testée et prise en charge. Étant donné que tous les composants SDX sont combinés dans un seul fichier, le fichier image SDX est plus volumineux que le fichier image du service de gestion.

Le nom de fichier de l'image est au format `build-sdx-13.1-<build_number>.tgz`. Une fois le service de gestion mis à niveau vers SDX 13.1, la nouvelle interface graphique n'affiche pas les options permettant de télécharger le fichier image Citrix Hypervisor, les packs supplémentaires ou les correctifs logiciels. Les options sont manquantes car SDX 13.1 ne prend pas en charge la mise à niveau de composants individuels.

Points à noter

- La mise à niveau d'une offre groupée est un processus en plusieurs étapes qui peut prendre jusqu'à 90 minutes.
- Tout d'abord, le service de gestion est mis à niveau vers la version la plus récente fournie. Au cours de la mise à niveau, la connectivité au service de gestion peut être perdue. Reconnectez-vous au service de gestion pour surveiller l'état de la mise à niveau.
- Ensuite, le nouveau service de gestion met à niveau Citrix Hypervisor et termine le reste de la mise à niveau de l'appliance. Le service de gestion des versions 11.0 et ultérieures peut effectuer la mise à niveau complète de Citrix Hypervisor.
- Ne redémarrez pas l'appliance pendant la mise à niveau de Citrix Hypervisor.
- Citrix vous recommande d'utiliser une console série Citrix Hypervisor (ou une console LOM) pour surveiller la mise à niveau de Citrix Hypervisor.

Mettez à niveau l'ensemble de l'appliance vers 13.1

Remarque : Le processus de mise à niveau redémarre l'ensemble de l'appliance SDX, y compris toutes les instances VPX, plusieurs fois. Avant d'effectuer cette procédure, si les instances VPX se trouvent dans une configuration HA, basculez tous les nœuds HA principaux vers le nœud secondaire. Si vous ne disposez pas d'un déploiement haute disponibilité, planifiez le temps d'arrêt en conséquence.

Pour mettre à niveau l'appliance :

1. Téléchargez le fichier image d'ensemble unique, accédez à **Configuration > Service de gestion > Images logicielles**, puis cliquez sur **Télécharger**.
2. Accédez à **Configuration > Système > Administration du système**.
3. Dans le groupe Administration système, cliquez sur **Mettre à niveau le matériel**.
   Le processus de mise à niveau prend quelques minutes.

Avant la mise à niveau, le service de gestion affiche les informations suivantes :

- Nom du fichier image d'ensemble unique.
- La version actuelle de SDX exécutée sur votre appliance.
- La version sélectionnée vers laquelle l'appliance doit être mise à niveau.
- Durée approximative de mise à niveau de l'appliance.
- Informations diverses.

Avant de cliquer sur **Mettre à niveau le matériel**, assurez-vous d'avoir pris connaissance de toutes les informations affichées à l'écran. Vous ne pouvez pas abandonner le processus de mise à niveau une fois qu'il a commencé

Chemins de mise à niveau non

Version source	Version cible
10.5	13.0, 13.1
11.0	13.0—64.x et versions supérieures, 13.1
11.1	13.0, 13.1
11.1–65.x	12.0
11.1–65.x	12.1–55.x ou inférieur
11.1–65.x	13.0–47.x ou inférieur

> **Remarque**
>
> Vous pouvez effectuer une mise à niveau directement vers n'importe quelle version de Citrix ADC versions 13.0 et 13.1 à partir de la version 12.1 d'ADC uniquement.

Informations connexes

Matrice de compatibilité matérielle et logicielle Citrix ADC SDX

Démystifier le processus de mise à niveau de l'appliance NetScaler SDX

Mise à niveau d'une instance Citrix ADC

January 6, 2023

> **Remarques**
>
> - La connexion au service Citrix ADM est activée par défaut, après avoir installé ou mis à niveau l'appliance Citrix ADC SDX vers la version 13.1. Pour plus de détails, consultez Gouvernance des données et connexion au service Citrix ADM.
> - Le processus de mise à niveau de l'appliance Citrix ADC SDX nécessite un seul redémarrage au lieu de deux redémarrages à partir de la version 13.1 build 37.x.

Le processus de mise à niveau des instances Citrix ADC implique le téléchargement du fichier de génération, puis la mise à niveau de l'instance Citrix ADC.

> **Important**
>
> La rétrogradation d'une instance ADC à l'aide du service de gestion n'est pas prise en charge Utilisez l'instance CLI pour rétrograder.

Téléchargez les images logicielles Citrix ADC sur l'appliance Citrix ADC SDX avant de mettre à niveau les instances Citrix ADC. Pour installer une nouvelle instance, vous avez besoin du fichier XVA Citrix ADC.

Dans le volet **Images logicielles**, vous pouvez afficher les détails suivants.

- **Nom :** nom du fichier image du logiciel de l'instance Citrix ADC. Le nom du fichier contient le numéro de version et le numéro de version. Par exemple, le nom de fichier build-10-53.5_nc.tgz fait référence à la version 10 build 53.5.
- **Dernière modification :** date à laquelle le fichier a été modifié pour la dernière fois.
- **Taille :** taille, en Mo, du fichier.

Pour télécharger une image logicielle

1. Dans le volet de navigation, développez Citrix ADC, puis cliquez sur **Images logicielles**.
2. Dans le volet **Images logicielles**, cliquez sur **Télécharger**.
3. Dans la boîte de dialogue **Charger l'image logicielle Citrix ADC**, cliquez sur **Parcourir** et sélectionnez le fichier image Citrix ADC que vous souhaitez télécharger.
4. Cliquez sur **Charger**. Le fichier image s'affiche dans le volet Images logicielles Citrix ADC.

Pour créer une sauvegarde en téléchargeant un fichier de génération

1. Dans le volet Images logicielles, sélectionnez le fichier que vous souhaitez télécharger, puis cliquez sur **Télécharger**.

2. Dans la boîte de message, dans la liste **Enregistrer**, sélectionnez **Enregistrer sous**.
3. Dans la boîte de message Enregistrer sous, accédez à l'emplacement dans lequel vous souhaitez enregistrer le fichier, puis cliquez sur **Enregistrer**.

Pour télécharger un fichier XVA

1. Dans le volet de navigation, développez Citrix ADC, puis cliquez sur **Images logicielles**.
2. Dans le volet Images logicielles, sous l'onglet **Fichiers XVA**, cliquez sur **Télécharger**.
3. Dans la boîte de dialogue **Upload Citrix ADC XVA File**, cliquez sur **Browse** (Parcourir) et sélectionnez le fichier Citrix ADC XVA que vous souhaitez télécharger.
4. Cliquez sur **Charger**. Le fichier XVA apparaît dans le volet **Fichiers XVA** .

Pour créer une sauvegarde en téléchargeant un fichier XVA

1. Dans le volet Fichiers XVA, sélectionnez le fichier que vous souhaitez télécharger, puis cliquez sur **Télécharger**.
2. Dans la zone de message, dans la liste Enregistrer, sélectionnez **Enregistrer sous**.
3. Dans la zone de message **Enregistrer sous**, accédez à l'emplacement où vous souhaitez enregistrer le fichier, puis cliquez sur **Enregistrer**.

Mettre à niveau les instances Citrix ADC VPX

Vous pouvez utiliser le service de gestion pour mettre à niveau une ou plusieurs des instances VPX exécutées sur l'appliance. Avant de mettre à niveau une instance, assurez-vous d'avoir téléchargé la bonne version sur l'appliance SDX.

Avant de commencer à mettre à niveau une instance, assurez-vous de bien comprendre le cadre de licence et les types de licences. Une mise à niveau de l'édition logicielle (par exemple, d'une édition standard vers l'édition entreprise ou d'une édition entreprise vers l'édition Platinum) peut nécessiter de nouvelles licences. Notez également les points suivants :

- Pour éviter toute perte de configuration, enregistrez la configuration sur chaque instance avant de mettre à niveau les instances.
- Vous pouvez également mettre à niveau une instance individuelle à partir du nœud Instances. Pour ce faire, sélectionnez l'instance dans le nœud Instances. Dans le volet d'informations, sélectionnez l'instance, puis dans le menu déroulant Actions, cliquez sur Mettre à niveau.

> **Important**
>
> Utilisez le service de gestion SDX uniquement et non l'interface graphique VPX pour mettre à niveau les instances VPX, de sorte que pendant les sauvegardes, les images de mise à niveau fassent partie du fichier de sauvegarde. Ces fichiers de sauvegarde vous aident à restaurer

> l'instance en douceur.

Pour mettre à niveau des instances VPX

1. Dans l'onglet **Configuration**, dans le volet de navigation, cliquez sur **Citrix ADC**.
2. Dans le volet d'informations, sous **Configuration Citrix ADC**, cliquez sur **Mettre à niveau**.
3. Dans la boîte de dialogue **Mettre à niveau Citrix ADC**, dans **Image logicielle**, sélectionnez le fichier de génération de mise à niveau Citrix ADC de la version vers laquelle vous souhaitez effectuer la mise à niveau.
4. Dans la liste déroulante **Adresse IP de l'instance**, sélectionnez les adresses IP des instances que vous souhaitez mettre à niveau.
5. Cliquez sur **OK**, puis sur Fermer.

Informations connexes

Matrice de compatibilité matérielle et logicielle Citrix ADC SDX

Démystifier le processus de mise à niveau de l'appliance NetScaler SDX

Gérer et surveiller l'appliance SDX

February 1, 2022

Une fois que votre appliance Citrix ADC SDX est opérationnelle, vous pouvez effectuer diverses tâches pour gérer et surveiller l'appliance à partir de l'interface utilisateur du service de gestion.

Pour modifier la configuration réseau de l'appliance SDX, cliquez sur **Système**. Dans le volet **Système**, sous le groupe Setup Appliance, cliquez sur **Configuration réseau** et entrez les détails dans l'Assistant.

Modifier la configuration réseau de l'appliance SDX

Vous pouvez modifier les détails de configuration réseau que vous avez fournis pour l'appliance SDX lors de la configuration initiale.

Pour modifier la configuration réseau de l'appliance SDX, cliquez sur **Système**. Dans le volet **Système**, sous le groupe **Setup Appliance**, cliquez sur **Configuration réseau** et entrez les détails dans l'Assistant.

Modifier le mot de passe du compte utilisateur par défaut

Le compte d'utilisateur par défaut fournit un accès complet à toutes les fonctionnalités de l'appliance Citrix SDX. Pour préserver la sécurité, utilisez le compte administrateur par défaut uniquement lorsque cela est nécessaire. Seules les personnes dont les fonctions nécessitent un accès complet doivent connaître le mot de passe du compte administrateur par défaut. Citrix recommande de modifier fréquemment le mot de passe administrateur par défaut. Si vous perdez le mot de passe, vous pouvez réinitialiser le mot de passe par défaut en rétablissant les paramètres d'usine de l'appliance, puis modifier le mot de passe.

Pour modifier le mot de passe du compte d'utilisateur par défaut, cliquez sur **Système** > **Administration des utilisateurs> Utilisateurs**. Sélectionnez un utilisateur et cliquez sur**Modifier** pour modifier le mot de passe.

Modifier le fuseau horaire de l'appareil

Vous pouvez modifier le fuseau horaire du service de gestion et de Citrix Hypervisor. Le fuseau horaire par défaut est UTC.

Pour modifier le fuseau horaire, cliquez sur **Système** et dans le groupe **Paramètres système**, cliquez sur **Modifier le fuseau horaire**.

Modifier le nom d'hôte de l'appliance

Vous pouvez modifier le nom d'hôte du service de gestion.

Filtrage VLAN

Le filtrage VLAN permet de séparer les données entre les instances VPX qui partagent un port physique. Par exemple, si vous avez configuré deux instances VPX sur deux VLAN différents et que vous activez le filtrage des VLAN, une instance ne peut pas afficher le trafic de l'autre instance. Si le filtrage VLAN est désactivé, toutes les instances peuvent voir les paquets de diffusion balisés ou non balisés, mais les paquets sont abandonnés au niveau logiciel. Si le filtrage VLAN est activé, chaque paquet de diffusion balisé atteint uniquement l'instance qui appartient au VLAN balisé correspondant. Si aucune des instances n'appartient au VLAN balisé correspondant, le paquet est abandonné au niveau matériel (NIC).

Si le filtrage VLAN est activé sur une interface, un nombre limité de VLAN balisés peut être utilisé sur cette interface. 63 VLAN balisés sur une interface 10G et 32 VLAN balisés sur une interface 1G. Une instance VPX reçoit uniquement les paquets qui ont les ID de VLAN configurés. Redémarrez les instances VPX associées à une interface si vous modifiez l'état du filtre VLAN de DÉSACTIVÉ à ACTIVÉ sur cette interface.

Le filtrage VLAN est activé par défaut sur l'appliance SDX. Si vous désactivez le filtrage VLAN sur une interface, vous pouvez configurer jusqu'à 4 096 VLAN sur cette interface.

Remarque : Le filtrage VLAN ne peut être désactivé que sur une appliance SDX exécutant Citrix Hypervisor version 6.0.

Pour activer le filtrage VLAN sur une interface, cliquez sur **Système** > **Interfaces**. Sélectionnez une interface, cliquez sur **Filtre VLAN** et entrez les détails pour activer le filtrage VLAN.

Configurer la synchronisation d'horloge

Lorsque vous activez la synchronisation NTP (Network Time Protocol), le service de gestion est redémarré. Vous pouvez configurer votre dispositif SDX pour synchroniser son horloge locale avec un serveur NTP. Par conséquent, l'horloge de l'appliance SDX possède les mêmes paramètres de date et d'heure que les autres serveurs de votre réseau. La configuration de la synchronisation de l'horloge ne change pas si l'appliance est redémarrée, mise à niveau ou rétrogradée. Toutefois, la configuration n'est pas propagée à l'instance secondaire de Citrix ADC dans une configuration haute disponibilité.

L'horloge est synchronisée immédiatement si vous ajoutez un serveur NTP ou modifiez l'un des paramètres d'authentification. Vous pouvez également activer et désactiver explicitement la synchronisation NTP.

Remarque : Si vous n'avez pas de serveur NTP local, vous pouvez trouver une liste des serveurs NTP publics en libre accès sur le site officiel NTP, http://www.ntp.org. Avant de configurer votre Citrix ADC pour utiliser un serveur NTP public, assurez-vous de lire la page Règles d'engagement (lien inclus dans toutes les pages des serveurs de temps publics).

Pour configurer un serveur NTP, cliquez sur **Système > Serveurs NTP**.

Pour activer la synchronisation NTP

1. Dans le volet de navigation, développez **Système**, puis cliquez sur **Serveurs NTP**.
2. Dans le volet d'informations, cliquez sur **Synchronisation NTP**.
3. Dans la boîte de dialogue **Synchronisation NTP**, sélectionnez **Activer la synchronisation NTP**.
4. Cliquez sur **OK**, puis sur **Fermer**.

Pour modifier les options d'authentification

1. Dans le volet de navigation, développez **Système**, puis cliquez sur **Serveurs NTP**.
2. Dans le volet d'informations, cliquez sur **Paramètres d'authentification**.
3. Dans la boîte de dialogue **Modifier les options d'authentification**, définissez les paramètres suivants :

- **Authentification** : activez l'authentification NTP. Valeurs possibles : OUI, NON. Par défaut : OUI.
- **ID de clé de confiance :** ID de clé de confiance. Lors de l'ajout d'un serveur NTP, vous sélectionnez un identificateur de clé dans cette liste. Valeur minimale : 1. Valeur maximale : 65534.
- **Revoke Interval**(Intervalle de révocation) : intervalle entre la ré-randomisation de certaines valeurs cryptographiques utilisées par le schéma Autokey, sous la forme d'une puissance de 2, en secondes. Valeur par défaut : 17 (2 ^ 17 = 36 heures).
- **Intervalle Automax** : intervalle entre la régénération de la liste de clés de session utilisée avec le protocole Autokey, avec une puissance de 2, en secondes. Valeur par défaut : 12 (2 ^ 12 = 1,1 heure).

4. Cliquez sur **OK**, puis sur **Fermer**.

Afficher les propriétés de l'appliance SDX

Affichez les propriétés du système telles que le nombre de cœurs de processeur et de puces SSL, la mémoire totale disponible et la mémoire disponible, ainsi que divers détails sur le produit dans l'onglet **Configuration** .

Pour afficher les propriétés de l'appliance SDX, cliquez sur l'onglet **Configuration** .

Vous pouvez afficher les informations suivantes concernant les ressources système, l'hyperviseur, la licence et le système :

Ressources système :

- **Nombre total de cœurs de processeur ;** nombre de cœurs de processeur sur l'appliance SDX.
- **Nombre total de puces SSL :** nombre total de puces SSL sur l'appliance SDX.
- **Puces SSL gratuites :** nombre total de puces SSL qui n'ont pas été attribuées à une instance.
- **Mémoire totale (Go) :** mémoire totale du matériel en Go.
- **Mémoire disponible (Go) :** mémoire libre du matériel en Go.

Informations sur l'hyperviseur :

- **Uptime :** temps écoulé depuis le dernier redémarrage de l'appliance, en nombre de jours, d'heures et de minutes.
- **Edition :** édition de Citrix Hypervisor installée sur l'appliance SDX.
- **Version :** version de Citrix Hypervisor installée sur l'appliance SDX.
- **IQN iSCSI :** nom qualifié iSCSI.
- **Code produit :** code produit de Citrix Hypervisor.

- **Numéro de série :** numéro de série de Citrix Hypervisor.
- **Date de construction :** date de création de Citrix Hypervisor.
- **Numéro de version :** numéro de build de Citrix Hypervisor.
- **Pack supplémentaire :** version du pack supplémentaire installé sur l'appliance SDX.

Informations sur la licence :

- **Plate-forme :** numéro de modèle de la plate-forme matérielle, basé sur la licence installée.
- **Instances maximales :** nombre maximum d'instances que vous pouvez configurer sur l'appliance SDX, en fonction de la licence installée.
- **Instances disponibles (partagées) :** nombre d'instances pouvant être configurées en fonction du nombre de cœurs de processeur encore disponibles.
- **Débit maximal (Mbit/s) :** débit maximal pouvant être atteint sur l'appliance, en fonction de la licence installée.
- **Débit disponible (Mbit/s) :** Débit disponible basé sur la licence installée.

Informations sur le système :

- **Plate-forme :** numéro de modèle de la plate-forme matérielle.
- **Produit :** Type de produit NetScaler.
- **Build :** version et build de NetScaler exécutés sur l'appliance SDX.
- **Adresse IP :** adresse IP du service de gestion.
- **ID d'hôte : ID** d'hôte Citrix Hypervisor.
- **Identifiant du système : ID** système Citrix Hypervisor.
- **Numéro de série : numéro de série**Citrix Hypervisor.
- **Heure système : Heure** système affichée au format Jour Mois Date Heures:Min:Sec Fuseau horaire Année.
- **Uptime :** temps écoulé depuis le dernier redémarrage du service de gestion, en nombre de jours, d'heures et de minutes.
- **Version du BIOS :** version du BIOS.

Afficher le débit des appareils en temps réel

Le débit total de l'appliance SDX pour le trafic entrant et sortant est tracé en temps réel dans un graphique mis à jour à intervalles réguliers. Par défaut, les débits du trafic entrant et sortant sont tracés ensemble sur le graphique.

Pour afficher le débit de l'appliance SDX, sur l'interface graphique, cliquez sur Tableau de **bord** et cochez**Débit système (Mbits/s)**.

Affichage de l'utilisation du processeur et de la mémoire

Vous pouvez afficher un graphique de l'utilisation du processeur et de la mémoire de l'appliance. Le graphique est tracé en temps réel et mis à jour à intervalles réguliers.

Pour afficher l'utilisation du processeur et de la mémoire de l'appliance SDX, sur l'interface graphique, cliquez sur Tableau de **bord** et cochez **Statistiques du service de gestion**.

Afficher l'utilisation du processeur pour tous les cœurs

Vous pouvez afficher l'utilisation de chaque cœur de processeur sur l'appliance SDX.

Le volet **Utilisation du cœur du processeur** affiche les informations suivantes :

- **Numéro de cœur : numéro** de cœur du processeur sur l'appliance.
- **Processeur physique :** numéro de processeur physique de ce cœur.
- **Hyper Threads :** Threads hyper associés à ce cœur de processeur.
- **Instances :** les instances qui utilisent ce cœur de processeur.
- **Utilisation moyenne du cœur :** Utilisation moyenne du cœur, exprimée en pourcentage.

Pour afficher l'utilisation du processeur pour tous les cœurs de l'appliance SDX, sur l'interface graphique, cliquez sur **Tableau de bord** et cochez**Utilisation du processeur système (%)**.

Installez un certificat SSL sur l'appliance SDX

L'appliance SDX est livrée avec un certificat SSL par défaut. Pour des raisons de sécurité, vous pouvez remplacer ce certificat par votre propre certificat SSL. Pour ce faire, vous devez d'abord télécharger votre certificat SSL sur le service de gestion, puis installer le certificat. L'installation d'un certificat SSL met fin à toutes les sessions client en cours avec le service de gestion. Ouvrez une session sur le service de gestion pour toutes les tâches de configuration supplémentaires.

Pour installer un certificat SSL, cliquez sur **Système**. Dans le groupe **Configurer le matériel**, cliquez sur **Installer le certificat SSL** et entrez les détails dans l'assistant.

Afficher le certificat SSL sur le service de gestion

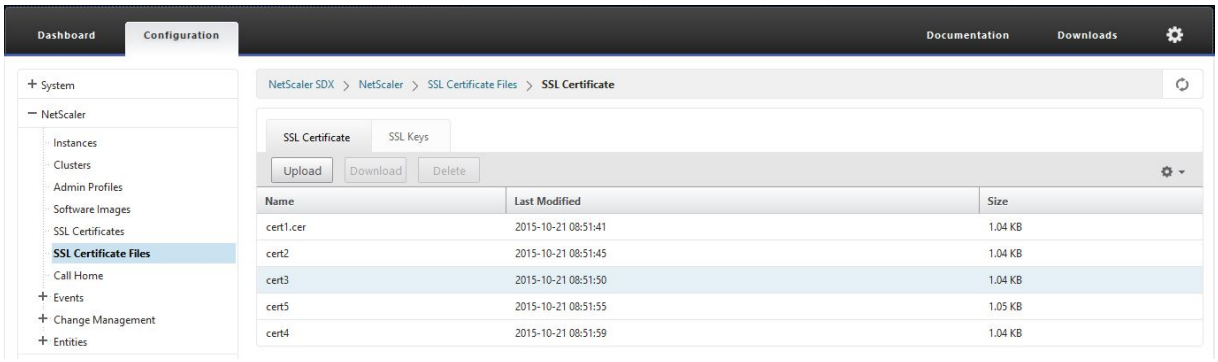
Le service de gestion utilise un certificat SSL pour sécuriser les connexions client. Affichez les détails de ce certificat, tels que le statut de validité, l'émetteur, l'objet, les jours avant expiration, les dates de début et de fin de validité, la version et le numéro de série.

Pour afficher le certificat SSL, cliquez sur **Système** et dans le groupe **Configurer le dispositif**, cliquez sur **Afficher le certificat SSL**.

Certificats et clés SSL pour les instances Citrix ADC

Des vues distinctes des certificats SSL et des clés pour les instances Citrix ADC offrent une facilité d'utilisation améliorée. Utilisez un nouveau nœud de service de gestion, Fichiers de certificats SSL, pour télécharger et gérer les certificats SSL et les paires de clés publiques et privées correspondantes qui peuvent être installées sur les instances Citrix ADC.

Pour accéder aux certificats et clés SSL pour les instances Citrix ADC, accédez à **Configuration > Citrix ADC > Fichiers de certificats SSL.**



Modifier les paramètres du système

Pour des raisons de sécurité, vous pouvez spécifier que le service de gestion et une instance VPX doivent communiquer entre eux uniquement sur un canal sécurisé. Vous pouvez également restreindre l'accès à l'interface utilisateur du service de gestion. Les clients peuvent ouvrir une session sur l'interface utilisateur du service de gestion uniquement en utilisant https.

Pour modifier les paramètres du système, cliquez sur **Configuration > Système** et dans le groupe Paramètres système, cliquez sur **Modifier les paramètres système**.

Redémarrez l'appareil

Le service de gestion fournit une option pour redémarrer l'appliance SDX. Lors du redémarrage, l'appliance arrête toutes les instances hébergées, puis redémarre Citrix Hypervisor. Lorsque Citrix Hypervisor redémarre, il démarre toutes les instances hébergées avec le service de gestion.

Pour redémarrer l'appliance, cliquez sur **Configuration > Système** et dans le groupe Administration système, cliquez sur **Redémarrer le matériel.**

Arrêtez l'appareil

Vous pouvez arrêter l'appliance SDX à partir du service de gestion.

Pour arrêter l'appliance, cliquez sur **Configuration > Système**, puis dans le groupe Administration système, cliquez sur **Arrêter l'appliance**.

Domaines d'administration SDX

January 27, 2022

La fonctionnalité des domaines d'administration SDX vous aide à créer plusieurs domaines administratifs. Vous pouvez utiliser les domaines administratifs pour séparer les ressources des différents services. Les domaines administratifs peuvent donc améliorer le contrôle des ressources, et les ressources peuvent être réparties entre différents domaines pour une utilisation optimale.

Une appliance SDX est livrée avec des ressources fixes, telles que les cœurs de processeur, le débit de données, la mémoire, l'espace disque, les puces SSL et un nombre spécifique d'instances pouvant être provisionnées. Le nombre d'instances que vous pouvez créer dépend de la licence.

Une appliance SDX prend en charge jusqu'à trois niveaux de domaines administratifs. Lorsque l'appliance est expédiée, toutes les ressources sont allouées au propriétaire.

Tous les domaines administratifs que vous créez sont des sous-domaines du domaine propriétaire. Dans chaque cas, les ressources du sous-domaine sont allouées à partir du pool de ressources du domaine parent. Les utilisateurs d'un domaine administratif ont accès aux ressources de ce domaine. Ils n'ont pas accès aux ressources des autres domaines au même niveau hiérarchique, ni aux ressources du domaine parent qui n'ont pas été allouées à leur domaine. Toutefois, les utilisateurs d'un domaine parent peuvent accéder aux ressources des sous-domaines de ce domaine.

Exemples d'allocation de ressources à des sous-domaines

Le Tableau 1 répertorie les ressources du domaine racine par défaut. L'administrateur SDX peut allouer ces ressources à des sous-domaines. Dans ce cas, l'administrateur peut allouer au maximum, par exemple, 10 cœurs de processeur et 840 Go d'espace disque.

Tableau 1. Ressources pour les propriétaires

Cœur du processeur	10
Débit (Mbits/s)	18500

Mémoire (Mo)	87300
Espace disque (Go)	840
Puces SSL	36
Instances	36

Le tableau 2 répertorie les ressources allouées à un sous-domaine nommé *Test*. Ce sous-domaine s'est vu attribuer 5 des 10 cœurs de processeur de son domaine parent, ce qui laisse 5 cœurs pouvant être alloués à d'autres sous-domaines du propriétaire.

Tableau 2. Ressources de Test Domain

Cœur du processeur	5
Débit (Mbits/s)	1024
Mémoire (Mo)	2048
Espace disque (Go)	40
Puces SSL	8
Instances	4

Lors de la création de sous-domaines, l'administrateur du domaine de *test* ne peut allouer que les ressources répertoriées dans le tableau 2. Le domaine de *test* ne peut comporter qu'un seul niveau de sous-domaines, car seuls trois niveaux de domaines peuvent être créés.

La figure suivante montre un autre exemple d'allocation de ressources entre sous-domaines, en utilisant des valeurs différentes de celles répertoriées dans les tableaux 1 et 2.

Pour créer un domaine administratif, accédez à **Configuration > Système > Domaine administratif** et sélectionnez les options souhaitées. Suivez les instructions qui s'affichent à l'écran. Une fois qu'un nouveau domaine est créé, connectez-vous à ce domaine en utilisant la page de connexion du service de gestion et fournissez le nom de domaine et le nom d'utilisateur. Par exemple, si vous avez créé un domaine nommé NewDomain avec un utilisateur NewUser, connectez-vous en tant que NewDomain \ NewUser.

Attribuer des utilisateurs à des domaines

Lorsqu'un sous-domaine est créé, deux groupes d'utilisateurs sont automatiquement créés : un groupe d'administrateurs et un groupe en lecture seule. Par défaut, chaque utilisateur fait partie du groupe d'administrateurs. Un utilisateur peut être ajouté à plusieurs groupes.

Gestion de l'allocation de disque RAID sur la plate-forme SDX 22000

July 12, 2022

Les appliances Citrix ADC SDX 22040/22060/22080/22100/22120 incluent désormais un contrôleur RAID (Redundant Array of Independent Disks), qui peut prendre en charge jusqu'à huit disques physiques. Les disques multiples offrent non seulement des gains de performances, mais également une fiabilité accrue. La fiabilité est particulièrement importante pour une appliance SDX, car elle héberge de nombreuses machines virtuelles et une défaillance de disque affecte plusieurs machines virtuelles. Le contrôleur RAID du service de gestion prend en charge la configuration RAID 1, qui met en œuvre la mise en miroir des disques. En d'autres termes, deux disques conservent les mêmes données. En cas de défaillance d'un disque de la matrice RAID 1, son miroir fournit immédiatement toutes les données nécessaires.

La mise en miroir de disques RAID 1 combine deux disques physiques en un seul disque logique. La capacité utile d'un disque logique est équivalente à la capacité de l'un de ses disques physiques. La combinaison de deux lecteurs de 1 téraoctet, par exemple, crée un seul disque logique d'une capacité utile totale de 1 téraoctet. Cette combinaison de lecteurs apparaît comme un seul lecteur logique aux yeux de l'appliance.

L'appliance SDX est livrée avec une configuration qui inclut le lecteur logique 0 et le lecteur logique 1. Le lecteur logique 0 est alloué au service de gestion et Citrix Hypervisor et le lecteur logique 1 est alloué aux instances Citrix ADC que vous provisionnez. Pour utiliser davantage de lecteurs physiques, vous devez créer de nouveaux lecteurs logiques.

Afficher les propriétés et les opérations du disque

Une appliance SDX prend en charge un maximum de huit emplacements de disque physique, c'est-à-dire une paire de quatre emplacements de chaque côté de l'appliance. Vous pouvez insérer des disques physiques dans les emplacements. Avant de pouvoir utiliser un disque physique, vous devez l'intégrer à un lecteur logique.

Dans le service de gestion, l'écran **Configuration > Système > RAID** inclut des onglets pour les lecteurs logiques, les disques physiques et les référentiels de stockage.

Disques logiques

Dans l'onglet **Configuration > Système > RAID > Disques logiques**, vous pouvez afficher le nom, l'état, la taille de chaque disque logique et des informations sur les lecteurs physiques de ses composants. Le tableau suivant décrit les états du lecteur virtuel.

State	Description
Optimal	L'état de fonctionnement du lecteur virtuel est bon. Tous les lecteurs configurés sont en ligne.
Dégradé	L'état de fonctionnement du lecteur virtuel n'est pas optimal. L'un des lecteurs configurés est en panne ou est hors ligne.
Échec	Le lecteur virtuel est en panne.
Hors-ligne	Le lecteur virtuel n'est pas disponible pour le contrôleur RAID.

Vous pouvez également afficher les détails des lecteurs physiques associés au lecteur logique en sélectionnant le lecteur logique et en cliquant sur **Afficher le lecteur physique**.

Pour créer un nouveau lecteur logique

1. Accédez à **Configuration** > **Système** > **RAID**, puis sélectionnez l'onglet **Disques logiques** .
2. Cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer un disque logique**, sélectionnez deux emplacements contenant des lecteurs physiques opérationnels, puis cliquez sur **Créer**.

Disques physiques

Une appliance SDX prend en charge un maximum de huit emplacements physiques, c'est-à-dire une paire de quatre emplacements de chaque côté de l'appliance. Dans l'onglet
Configuration > Système > RAID > Disques physiques, vous pouvez afficher les informations suivantes :

- **Emplacement :**—Emplacement physique associé au lecteur physique.
- **Size :**—Taille du disque physique.
- **État du microprogramme :**—État du microprogramme. Valeurs possibles :
  - **En ligne, spun up :**—Le disque physique est actif et est contrôlé par RAID.
  - **Non configuré (bon) :**—Le lecteur physique est en bon état et peut être ajouté en tant que partie de la paire de lecteurs logiques.

  - **Non configuré (mauvais) :**—Le lecteur physique n'est pas en bon état et ne peut pas être ajouté en tant que partie d'un lecteur logique.
- **État étranger :**— Indique si le disque est vide.
- **Disque logique :**— Lecteur logique associé.

Dans le volet **Lecteurs physiques**, vous pouvez effectuer les actions suivantes sur les lecteurs physiques :

- **Initialize :**—Initialise le disque. Vous pouvez initialiser le lecteur physique s'il n'est pas en bon état et doit être ajouté en tant que partie de la paire de lecteurs logiques.
- **Rebuild :**—Lance une reconstruction du lecteur. Lorsqu'un lecteur d'un groupe de lecteurs tombe en panne, vous pouvez le reconstruire en recréant les données qui étaient stockées sur le lecteur avant sa défaillance. Le contrôleur RAID recrée les données stockées sur les autres disques du groupe de lecteurs.
- **Localiser :**localisez le lecteur sur l'appliance, en faisant clignoter le voyant d'activité du lecteur associé au lecteur.
- **Stop Locate :**arrête de localiser le lecteur sur l'appliance.
- **Prepare to Remove :**désactive le lecteur physique sélectionné afin qu'il puisse être retiré.

Référentiel de stockage

Dans l'onglet **Configuration > Système > RAID > Référentiel de stockage**, vous pouvez afficher l'état des référentiels de stockage sur l'appliance SDX. Vous pouvez également afficher des informations sur un lecteur de référentiel de stockage qui n'est pas connecté, et vous pouvez supprimer un tel lecteur en le sélectionnant puis en cliquant sur **Supprimer**. L'onglet **Référentiel de stockage** affiche les informations suivantes concernant chaque référentiel de stockage :

- **Name :**—Nom du lecteur du référentiel de stockage.
- **Is Drive Attached :**indique si le référentiel de stockage est connecté ou non. Si le lecteur n'est pas connecté, vous pouvez cliquer sur **Supprimer** pour le supprimer.
- **Size :**—Taille du référentiel de stockage.
- **Utilisé :**—Quantité d'espace de stockage utilisé dans le référentiel.

Ajoutez un lecteur logique à l'appliance SDX 22000

Pour ajouter un lecteur logique supplémentaire à la plate-forme SDX 22000 :

1. Ouvrez une session sur le service de gestion.
2. Accédez à **Configuration > Système > RAID**.
3. À l'arrière de l'appliance SDX 22000, insérez les deux SSD vides dans les emplacements 4 et 5. Vous pouvez ajouter les SSD dans un système en cours d'exécution.
   Remarque : Assurez-vous que les SSD sont certifiés Citrix.

4. Dans le service de gestion, accédez à**Configuration > Système > RAID** et l'onglet **Disques physiques**. Vous pouvez voir les SSD que vous avez ajoutés.
5. Accédez à l'onglet **Logical Drive** et cliquez sur **Add**.
6. Sur la page **Créer un disque logique** :
   a) Dans la liste déroulante **Premier emplacement**, sélectionnez 4.
   b) Dans la liste déroulante **Deuxième emplacement**, sélectionnez 5.
   c) Cliquez sur **Créer**.
      Remarque : Dans Management Service, le numéro d'emplacement commence par zéro. La numérotation des emplacements dans le service de gestion diffère donc de la numérotation des emplacements sur l'appliance physique.

Le lecteur logique est créé et est répertorié sous l'
onglet Disque logique. Cliquez sur l'icône d'actualisation pour mettre à jour l'ordre des lecteurs logiques.

Ajoutez un deuxième lecteur logique sur l'appliance SDX 22000

Pour ajouter un autre lecteur logique, insérez les SSD dans les emplacements 6 et 7. Sur la page **Créer un disque logique**, sélectionnez 6 dans la liste **Premier emplacement**, puis 7 dans la liste **Deuxième emplacement** .

Remplacez un disque SSD défectueux par un disque SSD vierge

Pour remplacer un disque SSD défectueux par un disque SSD vierge :

1. Accédez à **Configuration > Système > RAID**.
2. Dans l'onglet **Disques physiques**, sélectionnez le lecteur défectueux que vous souhaitez remplacer.
3. Cliquez sur **Préparer le retrait** pour retirer le lecteur.
4. Cliquez sur l'icône d'actualisation pour actualiser la liste des lecteurs physiques.
5. Retirez physiquement le lecteur défectueux de l'emplacement.
6. Insérez le nouveau SSD vérifié Citrix dans l'emplacement d'où vous avez retiré le SSD défectueux.
7. Dans le service de gestion, accédez à **Configuration > Système > RAID**. Le nouveau SSD est répertorié dans la section**Disques physiques** . Le processus de reconstruction du disque démarre automatiquement.

Cliquez sur l'icône d'actualisation pour vérifier l'état du processus de reconstruction. Lorsque le processus de reconstruction est terminé, vous pouvez voir l'état En ligne, Spun Up dans la colonne **État du microprogramme** .

Présentation des licences SDX

October 4, 2022

Dans le service de gestion Citrix ADC SDX, vous pouvez utiliser votre numéro de série matériel (HSN) ou votre code d'accès de licence pour allouer vos licences. Le logiciel Management Service récupère en interne le numéro de série de votre appliance et Citrix envoie le code d'accès à la licence par e-mail lorsque vous achetez une licence.

Si une licence est déjà présente sur votre ordinateur local, vous pouvez également la télécharger sur l'appliance.

Pour toutes les autres fonctionnalités, telles que le retour ou la réallocation de votre licence, vous devez utiliser le portail de licences. Le cas échéant, vous pouvez toujours utiliser le portail de licences pour l'allocation de licences. Pour plus d'informations, consultez Gérer les licences sur citrix.com.

Pour plus d'informations sur les options de licence SDX, consultez :

- Choisir la bonne plateforme et les bonnes options d'édition.
- Modèles de licences

Remarque : L'installation d'une licence perpétuelle ou groupée ne nécessite pas de redémarrage de l'appliance SDX.

Conditions préalables

Pour utiliser le numéro de série du matériel ou le code d'accès de licence pour allouer vos licences :

1. Vous devez être en mesure d'accéder aux domaines publics via l'appliance. Par exemple, l'appliance doit pouvoir accéder au site www.citrix.com. Le logiciel d'allocation de licence accède en interne au portail de licences Citrix pour votre licence. Pour accéder à un domaine public, vous devez configurer l'adresse IP du service de gestion et configurer un serveur DNS.
2. Votre licence doit être liée à votre matériel ou vous devez disposer d'un code d'accès à la licence valide.

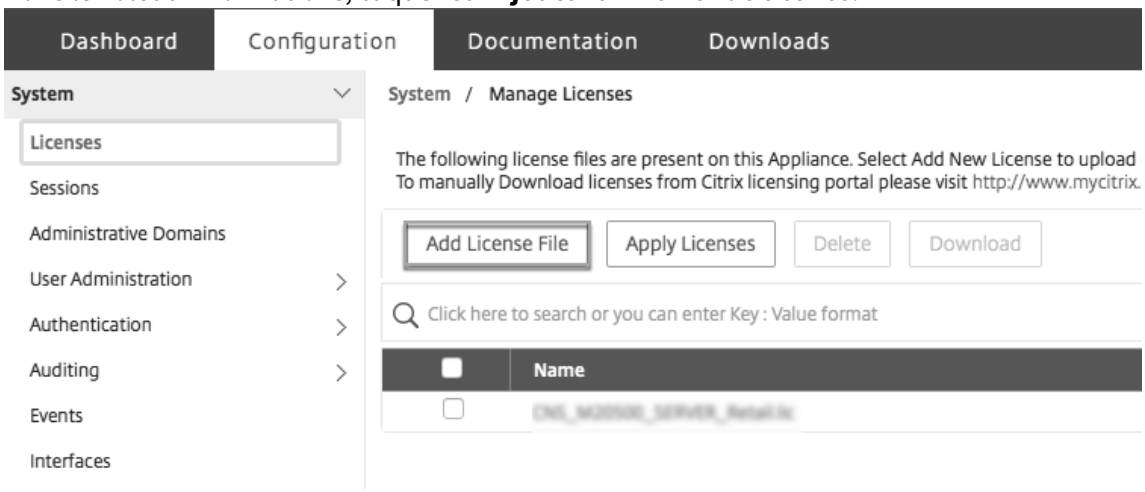
Allocation de votre licence à l'aide du service de gestion

Si votre licence est déjà liée à votre matériel, le processus d'attribution des licences peut utiliser le numéro de série du matériel. Sinon, vous devez entrer le code d'accès à la licence.

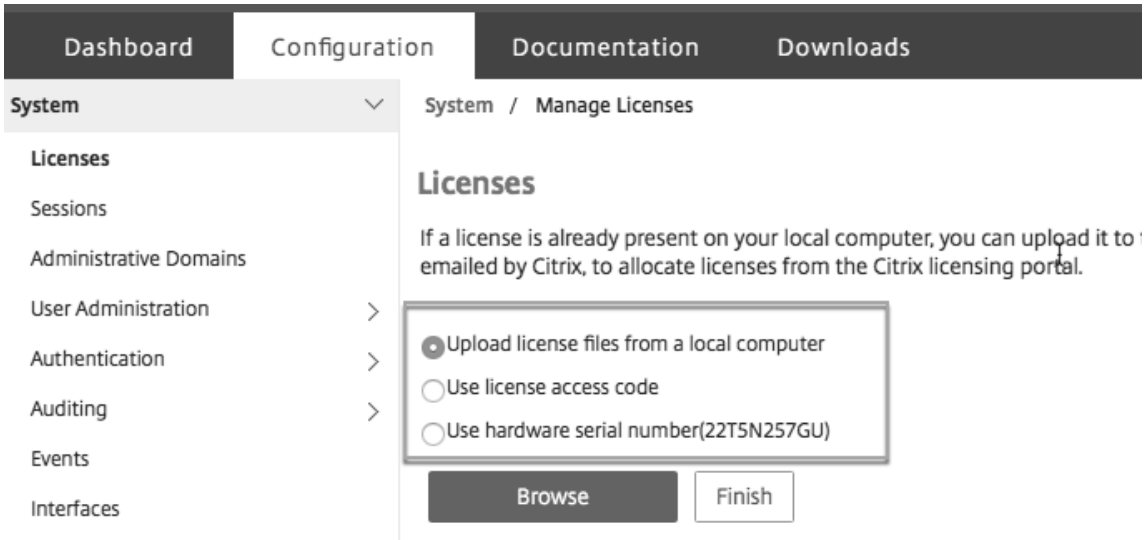
Vous pouvez allouer partiellement des licences selon les besoins de votre déploiement. Par exemple, si votre fichier de licences contient 10 licences, mais que vos besoins actuels ne concernent que six licences, vous pouvez allouer six licences maintenant et en attribuer d'autres ultérieurement. Vous ne pouvez pas allouer plus de licences que le nombre total de licences présentes dans votre fichier de licences.

Pour attribuer votre licence

1. Dans un navigateur Web, saisissez l'adresse IP du service de gestion de l'appliance SDX (par exemple, http://10.102.126.251).
2. Dans **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification de l'administrateur.
3. Sous l'onglet **Configuration**, accédez à **Système > Licences**.
4. Dans le volet d'informations, cliquez sur **Ajouter un fichier de licence**.



5. Sélectionnez ensuite l'une des options suivantes :
   - Télécharger des fichiers de licence à partir d'un ordinateur local (cette option est sélectionnée par défaut)
   - Utiliser le code d'accès aux licences
   - Utiliser le numéro de série du matériel



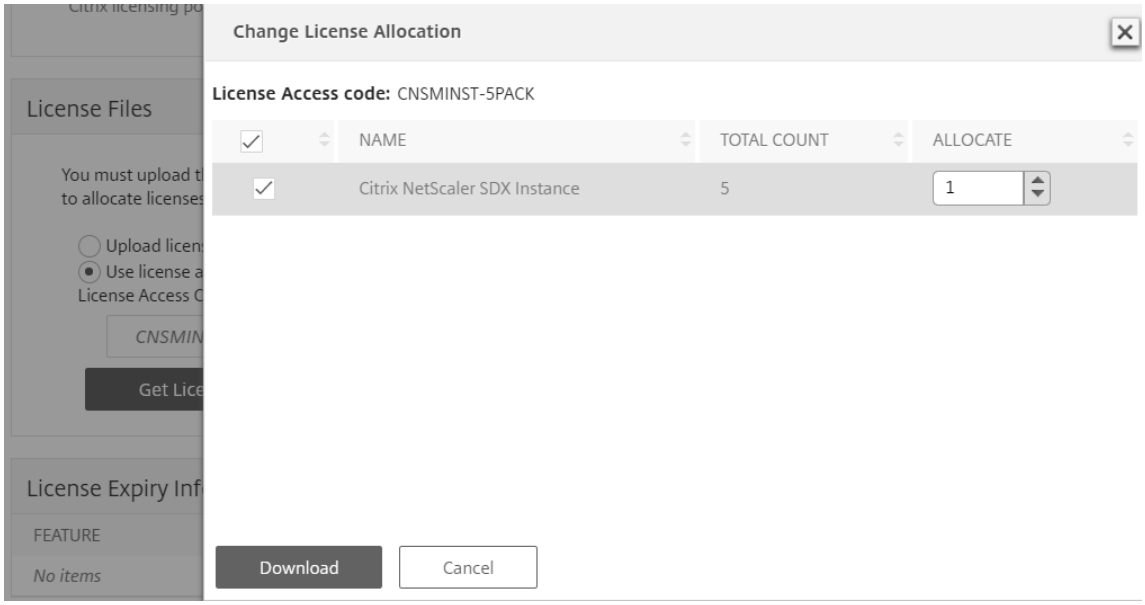
- **Charger des fichiers de licence depuis un ordinateur local** : Si vous choisissez cette option,

cliquez sur **Parcourir** pour sélectionner la licence à capacité nulle sur votre machine locale. Puis, cliquez sur **Terminer**.

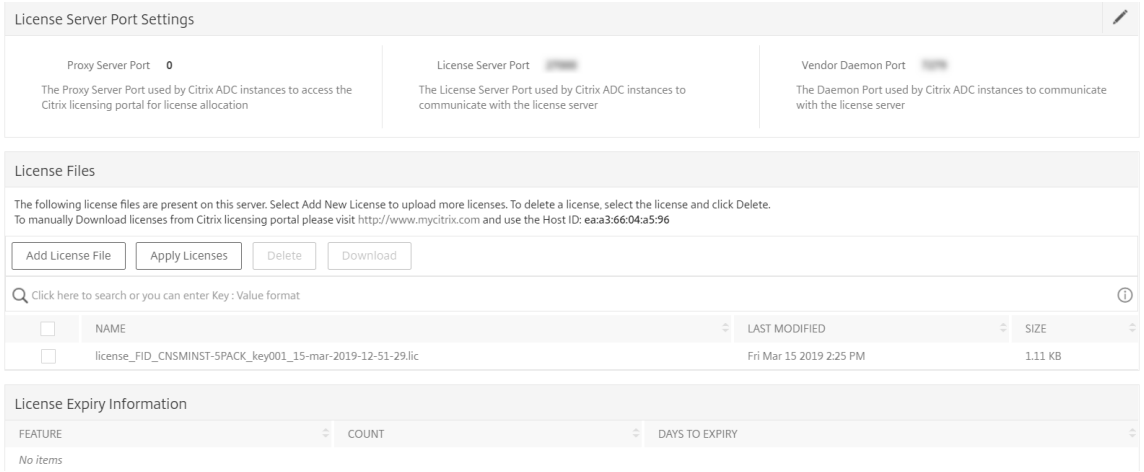
1. Une fois que la licence à capacité nulle est appliquée avec succès, la section **Mode de licence** apparaît sur la page **Licences** .
2. Vous pouvez choisir entre des licences **groupées ou des licences** de **pool autogérées**.
3. Dans le champ **Nom du serveur de licences ou Adresse IP**, entrez les détails du serveur de licences.
4. Dans le champ **Numéro de port**, entrez le port du serveur de licences. Valeur par défaut : 27000.
5. Cliquez sur **Obtenir licences**.
6. Dans la fenêtre **Allouer les licences**, spécifiez les instances et la bande passante requises, puis cliquez sur **Allouer**.
7. Sur la page **Gérer les licences**, vous pouvez afficher les détails du serveur de licences, de l'édition de licences, des instances et de la bande passante allouées à partir du pool.

> **Remarque :**
>
> À partir de la version 13.1 build 30.x de Citrix ADC, l'appliance Citrix ADC SDX prend en charge la licence Self Managed Pool. Cette licence vous permet de simplifier et d'automatiser le téléchargement de fichiers de licence sur le serveur de licences. Vous pouvez utiliser Citrix ADM pour créer une structure de licences comprenant une bande passante ou un processeur virtuel et un pool d'instances communs.

- **Utiliser le code d'accès à la licence** : si vous sélectionnez cette option, indiquez le **LAC** dans le champ **Code d'accès de licence** ou cochez la case pour vous connecter via un serveur proxy. Cliquez ensuite sur **Obtenir des licences**.
  - Sélectionnez le fichier de licences que vous souhaitez utiliser pour allouer vos licences.
  - Dans la colonne **Allocate**, saisissez le nombre de licences à allouer. Cliquez ensuite sur **Télécharger**.



Si la licence est téléchargée, elle apparaît sous **Fichiers de licence**. Sélectionnez le fichier de licence et cliquez sur**Appliquer les licences**.



- **Utiliser le numéro de série du matériel** : si vous choisissez cette option, le logiciel récupère en interne le numéro de série de votre appliance et utilise ce numéro pour afficher vos licences.
  - Cliquez sur **Obtenir des licences**ou activez la case à cocher **Connexion via un serveur proxy**, puis cliquez sur **Obtenir des licences**.

  Après avoir téléchargé le fichier de licence, sélectionnez-le et cliquez sur **Appliquer les licences**.

Pour plus d'informations sur les licences groupées, consultez Mettre à niveau une licence perpétuelle dans un Citrix ADC SDX vers une capacité groupée Citrix ADC.

Visualiseur de ressources SDX

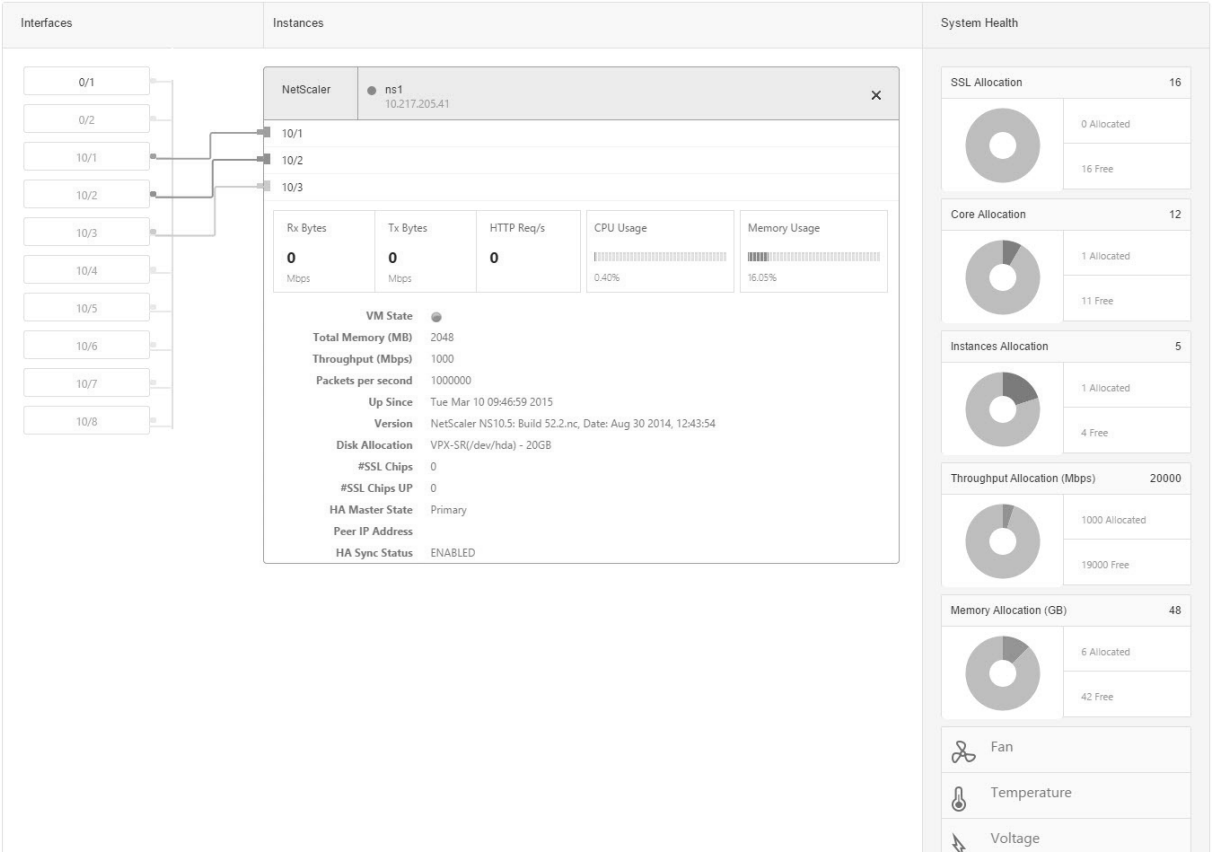
January 27, 2022

Lorsqu'une instance Citrix ADC est provisionnée sur une appliance Citrix ADC SDX, diverses ressources telles que le processeur, le débit et la mémoire doivent être allouées à une instance. Avec SDX actuel, les informations relatives aux différentes ressources disponibles ne sont pas affichées.

À l'aide du visualiseur de ressources, toutes les ressources disponibles qui peuvent être utilisées pour provisionner une instance sont affichées dans un seul tableau de bord. Toutes les ressources disponibles et utilisées sont affichées sous forme graphique. Le visualiseur de ressources affiche également d'autres paramètres tels que l'état de l'alimentation et la température, en plus des ressources qui peuvent être allouées.

Le visualiseur de ressources affiche également les différentes ressources utilisées par une instance. Pour voir les différentes ressources associées à une instance, cliquez sur le nom de l'instance dans le visualiseur. Le côté droit du visualiseur affiche toutes les ressources disponibles et utilisées dans un format graphique.

L'illustration suivante montre les détails capturés dans le visualiseur de ressources :



Gérer les interfaces

January 27, 2022

Dans le volet **Interfaces**, vous pouvez afficher le mappage des interfaces virtuelles sur les instances VPX vers l'appliance SDX et attribuer des adresses MAC aux interfaces.

Remarque : La négociation automatique n'est pas prise en charge sur une interface à laquelle un câble à connexion directe (DAC) est connecté.

Dans la liste des interfaces du volet **Interfaces**, dans la colonne **État**, UP indique que l'interface reçoit du trafic normalement. DOWN indique un problème réseau en raison duquel l'interface est incapable d'envoyer ou de recevoir du trafic.

Important : le contrôle du débit n'est pas recommandé pour les connexions supérieures à 1 Go.

Pour configurer une interface

1. Dans l'onglet **Configuration**, dans le volet de navigation, développez **Système**, puis cliquez sur **Interfaces**.
2. Dans le volet **Interfaces**, cliquez sur l'interface que vous souhaitez configurer, puis cliquez sur **Modifier**.
3. Dans la fenêtre **Configurer l'interface**, spécifiez des valeurs pour les paramètres suivants :
    - **Négociation automatique** : activez la négociation automatique. Valeurs possibles : ON, OFF. Par défaut : ON.
    - **Vitesse** : vitesse Ethernet de l'interface, en Mo/s. Valeurs possibles : 10, 100, 1000 et 10 000.
    - **Duplex :** type d'opération recto-verso de l'interface. Valeurs possibles : Full, Half, NONE. Par défaut : AUCUN.
    - **Négociation automatique du contrôle**de flux : négocie automatiquement les paramètres de contrôle Valeurs possibles : ON, OFF. Par défaut : ON
    - **Contrôle du débit Rx**— Activez le contrôle du débit Rx. Valeurs possibles : ON, OFF. Par défaut : ON
    - **Contrôle du débit Tx**— Active le contrôle du débit Tx. Valeurs possibles : ON, OFF. Par défaut : ON
4. Cliquez sur **OK**, puis sur **Fermer**.

Pour réinitialiser les paramètres d'une interface à leurs valeurs par défaut

1. Dans l'onglet **Configuration**, dans le volet de navigation, développez **Système**, puis cliquez sur **Interfaces**.

2. Dans le volet **Interfaces**, cliquez sur l'interface que vous souhaitez réinitialiser, puis cliquez sur **Réinitialiser**.

Afficher le mappage des interfaces virtuelles sur l'instance VPX vers les interfaces physiques

Dans l'instance Citrix ADC VPX, l'interface graphique et l'interface de ligne de commande affichent le mappage des interfaces virtuelles sur l'instance vers les interfaces physiques de l'appliance.

Après vous être connecté à l'instance VPX, dans l'utilitaire de configuration, accédez à **Réseau**, puis cliquez sur **Interfaces.** Le numéro d'interface virtuelle sur l'instance et le numéro d'interface physique correspondant sur l'appliance apparaissent dans le champ **Description**, comme illustré dans la figure suivante :

Dans l'interface de ligne de commande, tapez la commande `show interface`. Par exemple :

```
> show interface
1) Interface 10/3 (10G VF Interface, PF 10/4) #2
flags=0xe460 <ENABLED, UP, UP, HAMON, 802.1q>
MTU=1500, native vlan=1, MAC=6e:b6:f5:21:5d:db, uptime 43h03m35s
Actual: media FIBER, speed 10000, duplex FULL, fctl NONE, throughput
    10000
RX: Pkts(2547925) Bytes(287996153) Errs(0) Drops(527183) Stalls(0)
TX: Pkts(196) Bytes(8532) Errs(0) Drops(0) Stalls(0)
NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
Bandwidth thresholds are not set.
...
<!--NeedCopy-->
```

Affectation d'une adresse MAC à une interface

Lorsque vous provisionnez une instance ADC sur une appliance SDX, Citrix Hypervisor attribue en interne une adresse MAC à une interface virtuelle associée à cette instance. La même adresse MAC peut être attribuée à une interface virtuelle associée à une autre instance sur le même matériel ou sur un autre matériel. Pour empêcher l'attribution d'adresses MAC en double, vous pouvez appliquer des adresses MAC uniques.

Il existe deux manières d'attribuer une adresse MAC à une interface :

1. Attribuer une adresse MAC de base et une plage à une interface : le service de gestion attribue une adresse MAC unique à l'aide de l'adresse et de la plage de base.
2. Attribuer une adresse MAC de base globale : une adresse MAC de base globale s'applique à toutes les interfaces. Le service de gestion génère ensuite les adresses MAC pour toutes les interfaces. Si vous définissez l'adresse MAC de base globale, la plage d'une interface 1G est définie

sur 8. La plage pour une interface 10G est définie sur 64. Consultez le tableau suivant pour obtenir des exemples d'adresses MAC de base si l'adresse MAC de base globale est définie sur 00:00:00:00:00:00.

Interface physique	Adresse MAC de base
0/1	00:00:00:00:00:00
0/2	00:00:00:00:00:08
1/1	00:00:00:00:00:10
12	00:00:00:00:00:18
1/3	00:00:00:00:00:20
1/4	00:00:00:00:00:28
1/5	00:00:00:00:00:30
1/6	00:00:00:00:00:38
1/7	00:00:00:00:00:40
1/8	00:00:00:00:00:48
10/1	00:00:00:00:00:50
10/2	00:00:00:00:00:90

Tableau 1. Exemple d'adresses MAC de base générées à partir d'une adresse MAC de base globale

L'adresse MAC de base des ports de gestion est fournie à titre de référence uniquement. Le service de gestion génère des adresses MAC, en fonction de l'adresse MAC de base, pour les ports 1/x et 10/x uniquement.

Remarque : Vous ne pouvez pas attribuer d'adresse MAC de base à un canal.

Pour effectuer les différentes opérations avec l'adresse MAC, cliquez sur **Système > Interfaces**. Sélectionnez une interface, puis cliquez sur **Modifier**. Effectuez l'opération d'adresse MAC dans la fenêtre **Configurer l'interface** .

Désactiver ou activer les interfaces physiques sur l'appliance SDX

Si vous n'utilisez aucune des interfaces physiques sur l'appliance SDX, vous pouvez désactiver l'interface physique à l'aide du service de gestion. Cette action est utile pour des raisons de sécurité.

Remarque : Par défaut, toutes les interfaces physiques de l'appliance SDX sont activées. De même, si une interface est utilisée par un VPX ou un canal, vous ne pouvez pas désactiver l'interface.

Pour désactiver l'interface physique :

1. Dans l'onglet **Configuration**, dans le volet de navigation, développez **Système**, puis cliquez sur **Interfaces**.
2. Dans le volet **Interfaces**, sélectionnez l'interface que vous souhaitez désactiver.
3. Dans la liste déroulante **Action**, cliquez sur **Désactiver**.

Si vous souhaitez utiliser l'interface physique désactivée, vous pouvez l'activer à l'aide du service de gestion.

Pour activer l'interface physique désactivée :

1. Dans l'onglet **Configuration**, dans le volet de navigation, développez **Système**, puis cliquez sur **Interfaces**.
2. Dans le volet **Interfaces**, sélectionnez l'interface de désactivation que vous souhaitez activer.
3. Dans la liste déroulante **Action**, cliquez sur **Activer**.

Trames Jumbo sur les appareils SDX

January 27, 2022

Les appliances Citrix ADC SDX prennent en charge la réception et la transmission de trames Jumbo contenant jusqu'à 9 216 octets de données IP. Les trames Jumbo peuvent transférer des fichiers volumineux plus efficacement qu'il n'est possible avec la taille MTU IP standard de 1 500 octets.

Une appliance Citrix ADC SDX peut utiliser des trames Jumbo dans les scénarios de déploiement suivants :

- **Jumbo to Jumbo** : L'appliance reçoit les données sous forme de trames Jumbo et les envoie sous forme de trames Jumbo.
- **Non Jumbo to Jumbo** : L'appliance reçoit les données sous forme de trames non jumbo et les envoie sous forme de trames Jumbo.
- **Jumbo to Non-Jumbo** : L'appliance reçoit les données sous forme de trames étendues et les envoie en tant que trames non jumbo.

Les instances Citrix ADC provisionnées sur l'appliance SDX prennent en charge les trames Jumbo dans une configuration d'équilibrage de charge pour les protocoles suivants :

- TCP
- Tout autre protocole sur TCP
- SIP

Pour plus d'informations sur les trames Jumbo, consultez les cas d'utilisation.

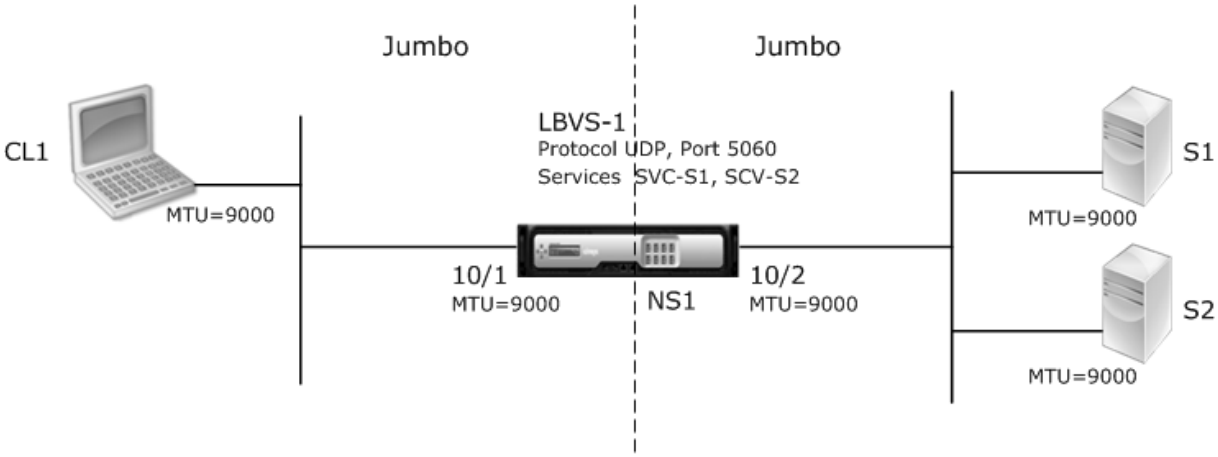
Cas d'utilisation : configuration Jumbo to Jumbo

Prenons un exemple de configuration Jumbo à Jumbo dans laquelle le serveur virtuel d'équilibrage de charge SIP LBVS-1, configuré sur l'instance Citrix ADC NS1, est utilisé pour équilibrer la charge du trafic SIP entre les serveurs S1 et S2. La connexion entre le client CL1 et NS1 et la connexion entre NS1 et les serveurs prennent en charge les trames étendues.

L'interface 10/1 de NS1 reçoit ou envoie du trafic depuis ou vers le client CL1. L'interface 10/2 de NS1 reçoit ou envoie du trafic depuis ou vers le serveur S1 ou S2. Les interfaces 10/1 et 10/2 de NS1 font partie du VLAN 10 et du VLAN 20, respectivement.

Pour la prise en charge des trames Jumbo, le MTU est réglé sur 9216 pour les interfaces 10/1, 10/2 et les VLAN VLAN 10, VLAN 20.

Tous les autres périphériques réseau, y compris CL1, S1, S2, dans cet exemple de configuration, sont également configurés pour prendre en charge les trames Jumbo.



Le tableau suivant répertorie les paramètres utilisés dans l'exemple.

Entité	Nom	Détails
Adresse IP du client CL1	CL1	192.0.2.10
Adresse IP des serveurs	S1	198.51.100.19
	S2	198.51.100.20
MTU spécifiées pour les interfaces (à l'aide de l'interface du service de gestion) et les VLAN sur NS1 (à l'aide de l'interface CLI).	10/1	9000
	10/2	9000
	VLAN 10	9000

Entité	Nom	Détails
	VLAN 20	9000
Services sur NS1 représentant des serveurs	SVC-S1	Adresse IP : 198.51.100.19 ; Protocole : SIP ; Port : 5060
Services sur NS1 représentant des serveurs	SVC-S2	Adresse IP : 198.51.100.20 ; Protocole : SIP ; Port : 5060
Serveur virtuel d'équilibrage de charge sur le VLAN 10	LBVS-1	Adresse IP : 203.0.113.15 ; Protocole : SIP ; Port : 5060 ; SVC-S1, SVC-S2

Voici le flux de trafic de la demande de CL1 à NS1 :

1. CL1 crée une demande SIP de 20 000 octets pour LBVS1.
2. CL1 envoie les données de demande sous forme de fragments IP à LBVS1 de NS1. La taille de chaque fragment IP est égale ou inférieure à la MTU (9000) définie sur l'interface à partir de laquelle CL1 envoie ces fragments à NS1.
    - Taille du premier fragment [IP = en-tête IP+en-tête UDP + segment de données SIP] = [20 + 8 + 8972] = 9000
    - Taille du deuxième fragment [IP = en-tête IP+segment de données SIP] = [20 + 8980] = 9000
    - Taille du dernier fragment IP[IP = en-tête IP+segment de données SIP] = [20 + 2048] = 2068
3. NS1 reçoit les fragments IP de la requête à l'interface 10/1. NS1 accepte ces fragments, car la taille de chacun de ces fragments est inférieure ou égale à la MTU (9000) de l'interface 10/1.
4. NS1 réassemble ces fragments IP pour former la demande SIP de 27 000 octets. NS1 traite cette demande.
5. L'algorithme d'équilibrage de charge de LBVS-1 sélectionne le serveur S1.
6. NS1 envoie les données de demande sous forme de fragments IP à S1. La taille de chaque fragment IP est égale ou inférieure à la MTU (9000) de l'interface 10/2, à partir de laquelle NS1 envoie ces fragments à S1. Les paquets IP proviennent d'une adresse SNIP NS1.
    - Taille du premier fragment IP [IP = en-tête IP+en-tête UDP + segment de données SIP] = [20 + 8 + 8972] = 9000
    - Taille du deuxième fragment IP [IP = en-tête IP+segment de données SIP] = [20 + 8980] = 9000
    - Taille du dernier fragment IP =[IP = en-tête IP+segment de données SIP][20 + 2048] = 2068

Voici le flux de trafic de la réponse de S1 à CL1 dans cet exemple :

1. Le serveur S1 crée une réponse SIP de 30 000 octets à envoyer à l'adresse SNIP de NS1.
2. S1 envoie les données de réponse sous forme de fragments IP à NS1. La taille de chaque fragment IP est égale ou inférieure au MTU (9000) défini sur l'interface à partir de laquelle S1 envoie

ces fragments à NS1.

- Taille du premier fragment IP [IP = en-tête IP+en-tête UDP + segment de données SIP] = [20 + 8 + 8972] = 9000
- Taille du deuxième et du troisième fragment IP = [IP = en-tête IP+segment de données SIP] = [20 + 8980] = 9000
- Taille du dernier fragment IP[IP = en-tête IP+segment de données SIP] = [20 + 3068] = 3088

3. NS1 reçoit les fragments IP de réponse à l'interface 10/2. NS1 accepte ces fragments, car la taille de chaque fragment est inférieure ou égale à la MTU (9000) de l'interface 10/2.
4. NS1 réassemble ces fragments IP pour former la réponse SIP de 27 000 octets. NS1 traite cette réponse.
5. NS1 envoie les données de réponse sous forme de fragments IP à CL1. La taille de chaque fragment IP est égale ou inférieure à la MTU (9000) de l'interface 10/1, à partir de laquelle NS1 envoie ces fragments à CL1. Les fragments IP proviennent de l'adresse IP de LBVS-1. Ces paquets IP proviennent de l'adresse IP de LBVS-1 et sont destinés à l'adresse IP de CL1.
   - Taille du premier fragment IP [IP = en-tête IP+en-tête UDP + segment de données SIP] = [20 + 8 + 8972] = 9000
   - Taille du deuxième et du troisième fragment IP = [IP = en-tête IP+segment de données SIP] = [20 + 8980] = 9000

Taille du dernier fragment IP =[IP = en-tête IP+segment de données SIP][20 + 3068] = 3088

Les**tâches de configuration** :

Sur le service de gestion SDX, accédez à **la page Configuration > Système > Interfaces** . Sélectionnez l'interface requise et cliquez sur **Modifier**. Définissez la valeur MTU et cliquez sur **OK**.

Exemple :

Définissez la valeur MTU pour l'interface 10/1 sur 9000 et pour l'interface 10/2 sur 9000.

Ouvrez une session sur l'instance Citrix ADC et utilisez l'interface de ligne de commande ADC pour terminer les étapes de configuration restantes.

Le tableau suivant répertorie les tâches, les commandes et les exemples permettant de créer la configuration requise sur les instances Citrix ADC.

Tâches	Syntaxe de la commande ADC	Exemples
Créez des VLAN et définissez le MTU des VLAN souhaités pour la prise en charge des trames Jumbo.	`add vlan <id> -mtu < positive_integer>;show vlan <id>`	`add vlan 10 -mtu 9000; add vlan 20 -mtu 9000`

Tâches	Syntaxe de la commande ADC	Exemples
Liez les interfaces aux VLAN.	`bind vlan <id> -ifnum <interface_name>;` `show vlan <id>`	`bind vlan 10 -ifnum 10/1;` `bind vlan 20 -ifnum 10/2`
Ajoutez une adresse SNIP.	`add ns ip <IPAddress> <netmask> -type SNIP;` `show ns ip`	`add ns ip 198.51.100.18 255.255.255.0 -type SNIP`
Créez des services représentant des serveurs SIP.	`add service <serviceName> <ip> SIP_UDP <port>;` `show service <name>`	add service SVC-S1 198.51.100.19 SIP_UDP 5060; dd service SVC-S2 198.51.100.20 SIP_UDP 5060

Créer des serveurs virtuels d'équilibrage de charge SIP et y lier les services	`add lb vserver <name> SIP_UDP <ip> <port>`
	`bind lb vserver <vserverName> <serviceName>;`
	`show lb vserver <name>`
		`add lb vserver LBVS-1 SIP_UDP 203.0.113.15 5060bind lb vserver LBVS-1 SVC-S1;bind lb vserver LBVS-1 SVC-S2`

`bind lb vserver LBVS-1 SVC-S2`	`save ns config;` `show ns config`	

Cas d'utilisation : configuration non Jumbo à Jumbo

Prenons un exemple de configuration non jumbo à jumbo dans laquelle le serveur virtuel d'équilibrage de charge LBVS1, configuré sur une instance Citrix ADC NS1, est utilisé pour équilibrer la charge du trafic entre les serveurs S1 et S2. La connexion entre le client CL1 et NS1 prend en charge les trames non jumbo, et la connexion entre NS1 et les serveurs prend en charge les trames Jumbo.

L'interface 10/1 de NS1 reçoit ou envoie du trafic depuis ou vers le client CL1. L'interface 10/2 de NS1 reçoit ou envoie du trafic depuis ou vers le serveur S1 ou S2.

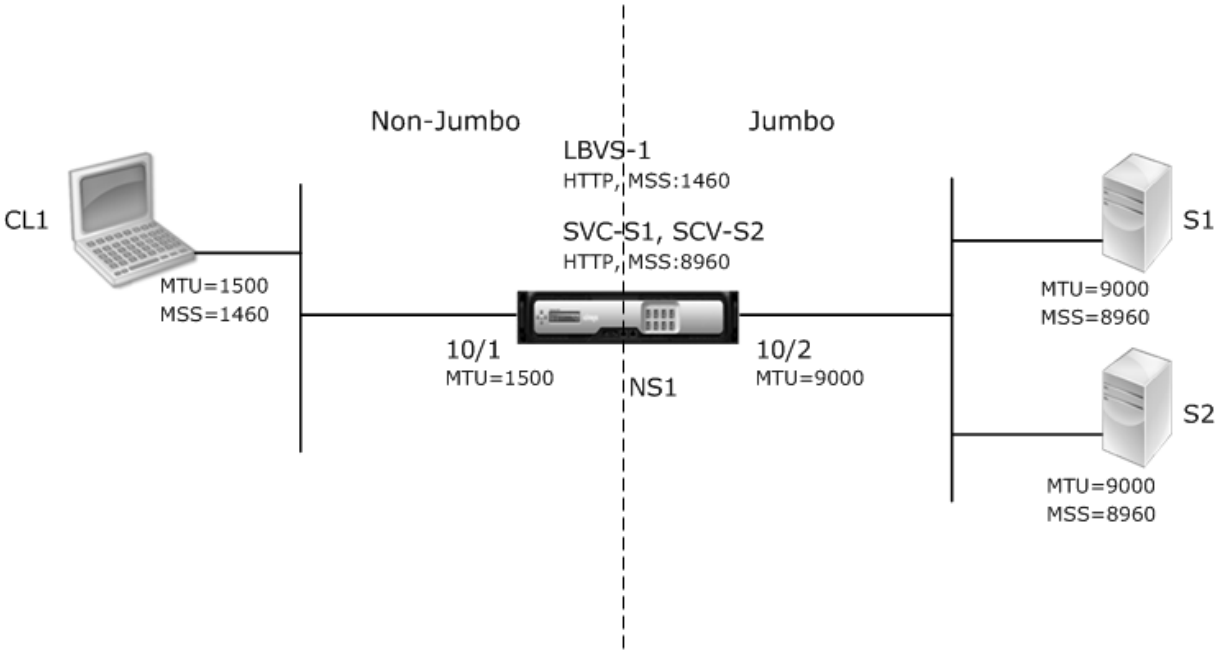
Les interfaces 10/1 et 10/2 de NS1 font partie du VLAN 10 et du VLAN 20, respectivement. Pour prendre en charge uniquement les trames non jumbo entre CL1 et NS1, le MTU est défini sur la valeur par défaut de 1500 pour l'interface 10/1 et le VLAN 10.

Pour la prise en charge des trames Jumbo entre NS1 et les serveurs, le MTU est défini sur 9000 pour l'interface 10/2 et le VLAN 20.

Les serveurs et tous les autres périphériques réseau entre NS1 et les serveurs sont également config-

urés pour prendre en charge les trames Jumbo. Le trafic HTTP étant basé sur TCP, les MSS sont définis en conséquence à chaque point d'extrémité pour la prise en charge des trames Jumbo :

- Pour la connexion entre CL1 et le serveur virtuel LBVS1 de NS1, le MSS sur NS1 est défini dans un profil TCP, qui est ensuite lié à LBVS1.
- Pour la connexion entre une adresse SNIP NS1 et S1, le MSS sur NS1 est défini dans un profil TCP, qui est ensuite lié au service (SVC-S1) représentant S1 sur NS1.



Le tableau suivant répertorie les paramètres utilisés dans cet exemple :

Entité	Nom	Détails
Adresse IP du client CL1	CL1	192.0.2.10
Adresse IP des serveurs	S1	198.51.100.19
	S2	198.51.100.20
MTU pour l'interface 10/1 (à l'aide de l'interface du service de gestion).		1500
MTU défini pour l'interface 10/2 (à l'aide de l'interface du service de gestion).		9000
MTU pour VLAN 10 sur NS1 (à l'aide de l'interface de ligne de commande ADC).		1500

Entité	Nom	Détails
MTU défini pour le VLAN 20 sur NS1 (à l'aide de l'interface de ligne de commande ADC).		9000
Services sur NS1 représentant des serveurs	SVC-S1	Adresse IP : 198.51.100.19 ; Protocole : HTTP ; Port : 80 ; MSS : 8960
	SVC-S2	Adresse IP : 198.51.100.20 ; Protocole : HTTP ; Port : 80 ; MSS : 8960
Serveur virtuel d'équilibrage de charge sur le VLAN 10	LBVS-1	Adresse IP : 203.0.113.15 ; Protocole : HTTP ; Port : 80. Services liés : SVC-S1, SVC-S2 ; MSS : 1460

Voici le flux de trafic de la demande de CL1 à S1 dans cet exemple :

1. Le client CL1 crée une demande HTTP de 200 octets à envoyer au serveur virtuel LBVS-1 de NS1.
2. CL1 ouvre une connexion à LBVS-1 de NS1. CL1 et NS1 échangent leurs valeurs MSS TCP respectives lors de l'établissement de la connexion.
3. Étant donné que le MSS de NS1 est plus grand que la demande HTTP, CL1 envoie les données de la demande dans un seul paquet IP à NS1.
   1.

```
<div id="concept_57AEA1C9D3DA47948B6D834341388D29__d978e142">

Size of the request packet = [IP Header + TCP Header + TCP Request
    ] = [20 + 20 + 200] = 240

</div>
```

4. NS1 reçoit le paquet de requête à l'interface 10/1, puis traite les données de requête HTTP dans le paquet.
5. L'algorithme d'équilibrage de charge de LBVS-1 sélectionne le serveur S1 et NS1 ouvre une connexion entre l'une de ses adresses SNIP et S1. NS1 et CL1 échangent leurs valeurs MSS TCP respectives lors de l'établissement de la connexion.
6. Étant donné que le MSS de S1 est plus grand que la requête HTTP, NS1 envoie les données de la demande dans un seul paquet IP à S1.

a) Taille du paquet de demande = [En-tête IP+En-tête TCP + [Demande TCP] = [20 + 20 + 200] = 240

Voici le flux de trafic de la réponse de S1 à CL1 dans cet exemple :

1. Le serveur S1 crée une réponse HTTP de 18 000 octets à envoyer à l'adresse SNIP de NS1.
2. S1 segmente les données de réponse en multiples du MSS de NS1 et envoie ces segments dans des paquets IP à NS1. Ces paquets IP proviennent de l'adresse IP de S1 et sont destinés à l'adresse SNIP de NS1.
   - Taille des deux premiers paquets = [en-tête IP+en-tête TCP + (segment TCP = taille MSS de NS1)] = [20 + 20 + 8960] = 9000
   - Taille du dernier paquet = [en-tête IP+en-tête TCP + (segment TCP restant)] = [20+2080] = 2120
3. NS1 reçoit les paquets de réponse à l'interface 10/2.
4. À partir de ces paquets IP, NS1 assemble tous les segments TCP pour former les données de réponse HTTP de 18 000 octets. NS1 traite cette réponse.
5. NS1 segmente les données de réponse en multiples du MSS de CL1 et envoie ces segments en paquets IP, de l'interface 10/1 à CL1. Ces paquets IP proviennent de l'adresse IP de LBVS-1 et sont destinés à l'adresse IP de CL1.
   - Taille de tous les paquets sauf le dernier = [en-tête IP+en-tête TCP + (charge utile TCP = taille MSS de CL1)] = [20 + 20+1460] = 1500
   - Taille du dernier paquet [en-tête IP+en-tête TCP + (segment TCP restant)] = [20 + 20 + 480] = 520

Les**tâches de configuration** :

Sur le service de gestion SDX, accédez à **la page Configuration > Système > Interfaces** . Sélectionnez l'interface requise et cliquez sur **Modifier**. Définissez la valeur MTU et cliquez sur **OK**.

Exemple :

Définissez les valeurs MTU suivantes :

- Pour interface 10/1 comme 1500
- Pour interface 10/2 comme 9000

Ouvrez une session sur l'instance Citrix ADC et utilisez l'interface de ligne de commande ADC pour terminer les étapes de configuration restantes.

Le tableau suivant répertorie les tâches, les commandes et les exemples permettant de créer la configuration requise sur les instances Citrix ADC.

Tâches	Syntaxe de ligne de commande ADC	Exemple
Créez des VLAN et définissez le MTU des VLAN souhaités pour la prise en charge des trames Jumbo.	`add vlan <id> -mtu <positive_integer>; show vlan <id>`	`add vlan 10 -mtu`

1500; add vlan 20 -mtu 9000|
|Liez les interfaces aux VLAN.|bind vlan <id> -ifnum <interface_name>; show vlan <id>
|bind vlan 10 -ifnum 10/1; bind vlan 20 -ifnum 10/2|
|Ajoutez une adresse SNIP.|add ns ip <IPAddress> <netmask> -type SNIP; show ns ip
|add ns ip 198.51.100.18 255.255.255.0 -type SNIP|
|Créer des services représentant des serveurs HTTP|add service <serviceName> <ip>
HTTP <port>; show service <name>|add service SVC-S1 198.51.100.19 http 80;
add service SVC-S2 198.51.100.20 http 80|
|Créer des serveurs virtuels d'équilibrage de charge HTTP et y lier les services|add lb vserver
<name> HTTP <ip> <port>bind lb vserver <vserverName> <serviceName>; show lb
vserver <name>|add lb vserver LBVS-1 http 203.0.113.15 80; bind lb vserver
LBVS-1 SVC-S1|
|Créez un profil TCP personnalisé et définissez son MSS pour la prise en charge des trames
Jumbo.|add tcpProfile <name> -mss <positive_integer>; show tcpProfile <name>
|add tcpprofile NS1-SERVERS-JUMBO -mss 8960|
|Liez le profil TCP personnalisé aux services souhaités.|set service <Name> -tcpProfileName
<string>; show service <name>|set service SVC-S1 -tcpProfileName NS1-SERVERS
-JUMBO; set service SVC-S2 -tcpProfileName NS1-SERVERS-JUMBO|
|Enregistrer la configuration|save ns config ; show ns config|

Cas d'utilisation : coexistence de flux Jumbo et non Jumbo sur le même ensemble d'interfaces

Prenons un exemple dans lequel les serveurs virtuels d'équilibrage de charge LBVS1 et LBVS2 sont configurés sur l'instance NS1 de Citrix ADC. LBVS1 est utilisé pour équilibrer la charge du trafic HTTP entre les serveurs S1 et S2, et global est utilisé pour équilibrer la charge du trafic entre les serveurs S3 et S4.

CL1 se trouve sur le VLAN 10, S1 et S2 sont sur VLAN20, CL2 est sur le VLAN 30, et S3 et S4 sont sur le VLAN 40. Le VLAN 10 et le VLAN 20 prennent en charge les trames Jumbo, tandis que les VLAN 30 et VLAN 40 prennent uniquement en charge les trames non jumbo.

En d'autres termes, la connexion entre CL1 et NS1 et la connexion entre NS1 et le serveur S1 ou S2 prennent en charge les trames Jumbo. La connexion entre CL2 et NS1 et la connexion entre NS1 et le serveur S3 ou S4 prennent uniquement en charge les trames non jumbo.

L'interface 10/1 de NS1 reçoit ou envoie du trafic depuis ou vers des clients. L'interface 10/2 de NS1 reçoit ou envoie du trafic depuis ou vers les serveurs.

L'interface 10/1 est liée au VLAN 10 et au VLAN 20 en tant qu'interface balisée. L'interface 10/2 est liée au VLAN 30 et au VLAN 40 en tant qu'interface balisée.

Pour la prise en charge des trames Jumbo, le MTU est réglé sur 9216 pour les interfaces 10/1 et 10/2.

Sur NS1, le MTU est défini sur 9000 pour le VLAN 10 et le VLAN 30 pour la prise en charge des trames Jumbo. Le MTU est défini sur la valeur par défaut de 1500 pour le VLAN 20 et le VLAN 40 pour la prise en charge uniquement des trames non jumbo.

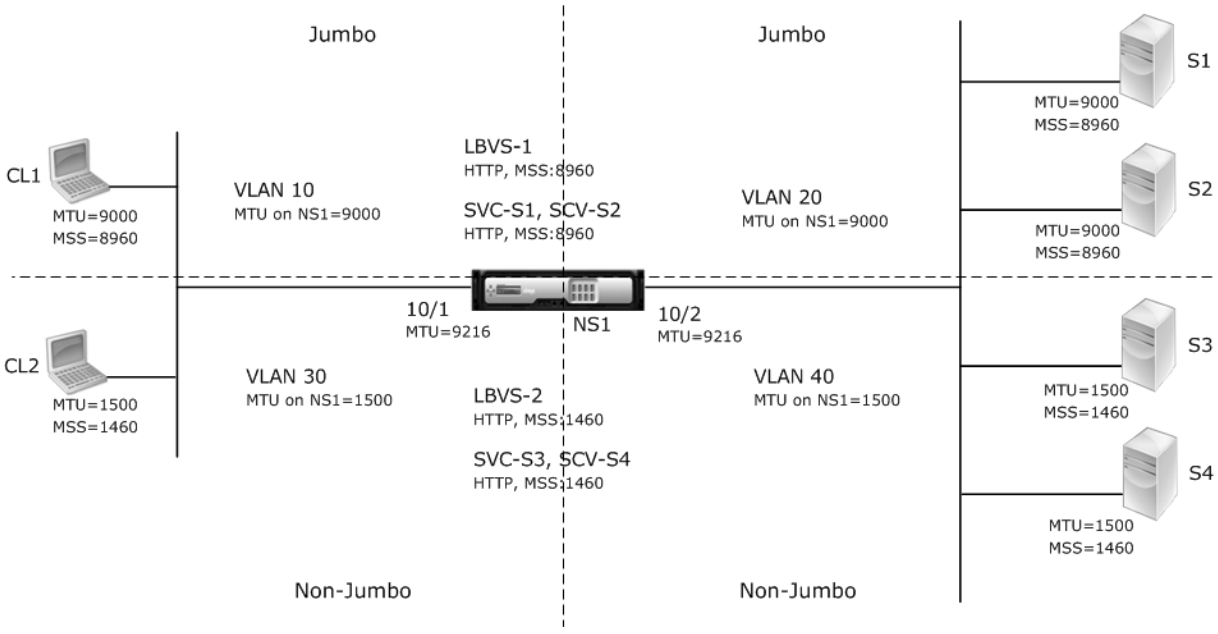
Le MTU effectif sur une interface ADC pour les paquets marqués VLAN est le MTU de l'interface ou le MTU du VLAN, la valeur la plus faible étant retenue. Par exemple :

- Le MTU de l'interface 10/1 est 9216. Le MTU du VLAN 10 est 9000. Sur l'interface 10/1, le MTU des paquets balisés VLAN 10 est 9000.
- Le MTU de l'interface 10/2 est 9216. Le MTU du VLAN 20 est 9000. Sur l'interface 10/2, le MTU des paquets balisés VLAN 20 est 9000.
- Le MTU de l'interface 10/1 est 9216. Le MTU du VLAN 30 est de 1500. Sur l'interface 10/1, le MTU des paquets balisés VLAN 30 est de 1500.
- Le MTU de l'interface 10/2 est 9216. Le MTU du VLAN 40 est de 1500. Sur l'interface 10/2, le MTU des paquets balisés VLAN 40 est de 9000.

CL1, S1, S2 et tous les périphériques réseau entre CL1 et S1 ou S2 sont configurés pour des trames Jumbo.

Le trafic HTTP étant basé sur TCP, les MSS sont définis en conséquence à chaque point d'extrémité pour la prise en charge des trames Jumbo.

- Pour la connexion entre CL1 et le serveur virtuel LBVS-1 de NS1, le MSS sur NS1 est défini dans un profil TCP, qui est ensuite lié à LBVS1.
- Pour la connexion entre une adresse SNIP NS1 et S1, le MSS sur NS1 est défini dans un profil TCP, qui est ensuite lié au service (SVC-S1) représentant S1 sur NS1.



Le tableau suivant répertorie les paramètres utilisés dans cet exemple.

|Entité|Nom|Détails|
|—|—|—|
|Adresse IP des clients|CL1|192.0.2.10
||CL2|192.0.2.20
|Adresse IP des serveurs|S1|198.51.100.19
||S2|198.51.100.20
||S3|198.51.101.19
||S4|198.51.101.20
|Adresses SNIP sur NS1||198.51.100.18 ; 198.51.101.18
|MTU spécifiée pour les interfaces et les VLAN sur NS1|10/1|9216
||10/2|9216
|VLAN 10|9000
|VLAN 20|9000
|VLAN 30|9000
|VLAN 40|1500
|Profil TCP par défaut|NSTCP_DEFAULT_PROFIL|MSS : 1460
|Profil TCP personnalisé|Tout-Jumbo|MSS : 8960
|Services sur NS1 représentant des serveurs|SVC-S1|Adresse IP : 198.51.100.19 ; Protocole : HTTP ; Port : 80 ; Profil TCP : ALL-JUMBO (MSS : 8960)
||SVC-S2 Adresse IP : 198.51.100.20 ; Protocole : HTTP ; Port : 80 ; Profil TCP : ALL-JUMBO (MSS : 8960)
||SVC-S3 | Adresse IP : 198.51.101.19 ; Protocole : HTTP ; Port : 80 ; Profil TCP : nstcp_default_profile (MSS : 1460)
||SVC-S4|adresse IP : 198.51.101.20 ; Protocole : HTTP ; Port : 80 ; Profil TCP : nstcp_default_profile (MSS : 1460)
|Serveurs virtuels d'équilibrage de charge sur NS1|LBVS-1|adresse IP = 203.0.113.15 ; Protocole : HTTP ; Port : 80. Services liés : SVC-S1, SVC-S2 ; Profil TCP : ALL-JUMBO (MSS : 8960)
||LBVS-2|adresse IP = 203.0.114.15 ; Protocole : HTTP ; Port : 80. Services liés : SVC-S3, SVC-S4 ; profil TCP : nstcp_default_profile (MSS : 1460)

Voici le flux de trafic de la demande de CL1 à S1 :

1. Le client CL1 crée une demande HTTP de 20 000 octets à envoyer au serveur virtuel LBVS-1 de NS1.
2. CL1 ouvre une connexion à LBVS-1 de NS1. CL1 et NS1 échangent leurs valeurs MSS TCP lors de l'établissement de la connexion.
3. Étant donné que la valeur MSS de NS1 est inférieure à la requête HTTP, CL1 segmente les données de la demande en multiples de MSS de NS1 et envoie ces segments dans des paquets IP marqués VLAN 10 à NS1.
    - Taille des deux premiers paquets = [En-tête IP+En-tête TCP + (segment TCP = NS1 MSS)] = [20 + 20 + 8960] = 9000
    - Taille du dernier paquet = [en-tête IP+en-tête TCP + (segment TCP restant)] = [20+2080] =

2120

4. NS1 reçoit ces paquets à l'interface 10/1. NS1 accepte ces paquets car la taille de ces paquets est égale ou inférieure au MTU effectif (9000) de l'interface 10/1 pour les paquets balisés VLAN 10.
5. À partir des paquets IP, NS1 assemble tous les segments TCP pour former la demande HTTP de 20 000 octets. NS1 traite cette demande.
6. L'algorithme d'équilibrage de charge de LBVS-1 sélectionne le serveur S1 et NS1 ouvre une connexion entre l'une de ses adresses SNIP et S1. NS1 et CL1 échangent leurs valeurs MSS TCP respectives lors de l'établissement de la connexion.
7. NS1 segmente les données de demande en multiples de MSS de S1 et envoie ces segments dans des paquets IP marqués VLAN 20 vers S1.
    - Taille des deux premiers paquets = [en-tête IP +en-tête TCP + (charge utile TCP = S1 MSS)][20 + 20 + 8960] = 9000
    - Taille du dernier paquet = [en-tête IP+en-tête TCP + (segment TCP restant)] = [20+2080] = 2120

Voici le flux de trafic de la réponse de S1 à CL1 :

1. Le serveur S1 crée une réponse HTTP de 30 000 octets à envoyer à l'adresse SNIP de NS1.
2. S1 segmente les données de réponse en multiples du MSS de NS1 et envoie ces segments dans des paquets IP marqués VLAN 20 vers NS1. Ces paquets IP proviennent de l'adresse IP de S1 et sont destinés à l'adresse SNIP de NS1.
    - Taille des trois premiers paquets [en-tête IP+en-tête TCP + (segment TCP = taille MSS de NS1)] = [20 + 20 + 8960] = 9000
    - Taille du dernier paquet [en-tête IP+en-tête TCP + (segment TCP restant)] = [20 + 20 + 3120] = 3160
3. NS1 reçoit les paquets de réponse à l'interface 10/2. NS1 accepte ces paquets, car leur taille est inférieure ou égale à la valeur MTU effective (9000) de l'interface 10/2 pour les paquets balisés VLAN 20.
4. À partir de ces paquets IP, NS1 assemble tous les segments TCP pour former la réponse HTTP de 30 000 octets. NS1 traite cette réponse.
5. NS1 segmente les données de réponse en multiples du MSS de CL1 et envoie ces segments dans des paquets IP étiquetés VLAN 10, de l'interface 10/1 à CL1. Ces paquets IP proviennent de l'adresse IP de LBVS et sont destinés à l'adresse IP de CL1.
    - Taille des trois premiers paquets = [en-tête IP+en-tête TCP + [(charge utile TCP = taille MSS de Cl1)][20 + 20 + 8960] = 9000
    - Taille du dernier paquet = = [en-tête IP+en-tête TCP + (segment TCP restant)][20 + 20 + 3120] = 3160

Les**tâches de configuration** :

Sur le service de gestion SDX, accédez à **la page Configuration > Système > Interfaces** . Sélectionnez

l'interface requise et cliquez sur **Modifier**. Définissez la valeur MTU et cliquez sur **OK**.

Exemple :

Définissez les valeurs MTU suivantes :

- Pour interface 10/1 comme 9216
- Pour interface 10/2 comme 9216

Ouvrez une session sur l'instance Citrix ADC et utilisez l'interface de ligne de commande ADC pour terminer les étapes de configuration restantes.

Le tableau suivant répertorie les tâches, les commandes et les exemples permettant de créer la configuration requise sur les instances Citrix ADC.

Tâche	Syntaxe	Exemple
—	—	—
Créez des VLAN et définissez le MTU des VLAN souhaités pour la prise en charge des trames Jumbo.	add vlan <id> -mtu <positive_integer>; show vlan <id>	add vlan 10 -mtu 9000add vlan 20 -mtu 9000;add vlan 30 -mtu 1500;add vlan 40 -mtu 1500
Liez les interfaces aux VLAN.	bind vlan <id> -ifnum <interface_name>;show vlan <id>	bind vlan 10 -ifnum 10/1 -taggedbind vlan 20 -ifnum 10/2 -tagged;bind vlan 30 -ifnum 10/1 -tagged;bind vlan 40 -ifnum 10/2 -tagged
Ajoutez une adresse SNIP.	add ns ip <IPAddress> <netmask> -type SNIP;show ns ip	add ns ip 198.51.100.18 255.255.255.0 -type SNIP;add ns ip 198.51.101.18 255.255.255.0 -type SNIP
Créez des services représentant des serveurs HTTP.	add service <serviceName> <ip> HTTP <port>;show service <name>	add service SVC-S1 198.51.100.19 http 80add service SVC-S2 198.51.100.20 http 80;add service SVC-S3 198.51.101.19 http 80;add service SVC-S4 198.51.101.20 http 80
Créer des serveurs virtuels d'équilibrage de charge HTTP et y lier les services	add lb vserver <name> HTTP <ip> <port>bind lb vserver <vserverName> <serviceName>;show lb vserver <name>	add lb vserver LBVS-1 http 203.0.113.15 80bind lb vserver LBVS-1 SVC-S1;bind lb vserver LBVS-1 SVC-S2
		add lb vserver LBVS-2 http 203.0.114.15 80bind lb vserver LBVS-2 SVC-S3;bind lb vserver LBVS-2 SVC-S4
Créez un profil TCP personnalisé et définissez son MSS pour la prise en charge des trames Jumbo.	add tcpProfile <name> -mss <positive_integer>;show tcpProfile <name>	add tcpprofile ALL-JUMBO -mss 8960
Liez le profil TCP personnalisé au serveur virtuel et aux services d'équilibrage de charge souhaités.	set service <Name> -tcpProfileName <string>;show service <name>	set lb vserver LBVS-1 - tcpProfileName ALL-JUMBOset service SVC-S1 - tcpProfileName ALL-JUMBO;set service SVC-S2 - tcpProfileName ALL-JUMBO
Save the configuration	save ns config; show ns config

Configuration du SNMP sur les appliances SDX

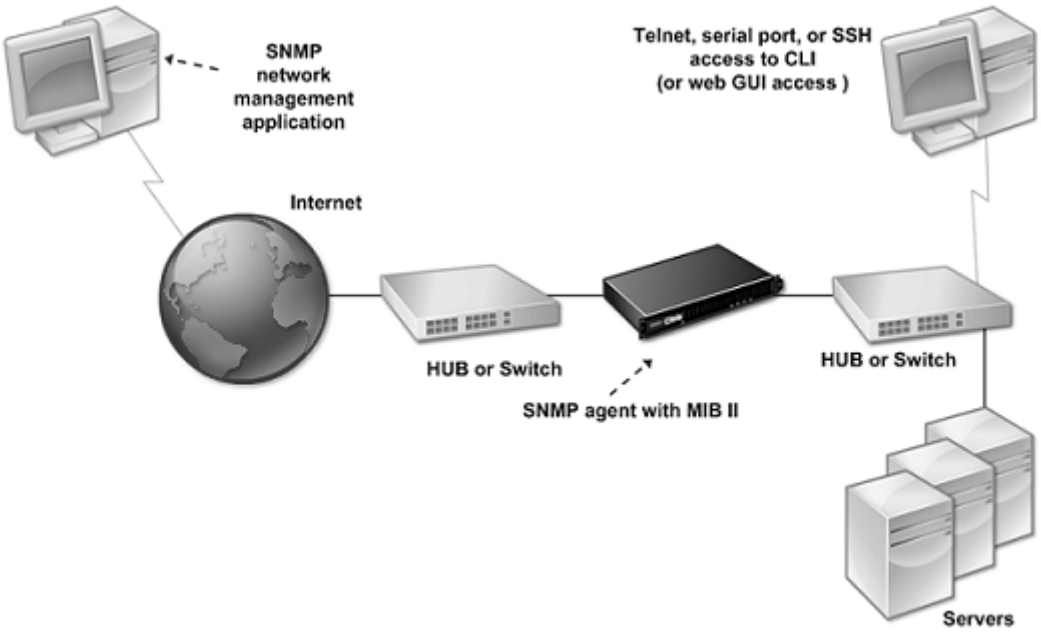
January 27, 2022

Vous pouvez configurer un agent SNMP sur l'appliance Citrix ADC SDX pour générer des événements asynchrones, appelés interruptions. Les interruptions sont générées chaque fois que des conditions anormales se produisent sur l'appliance SDX. Les interruptions sont ensuite envoyées à un périphérique distant appelé *écouteur d'interruption*, qui signale l'état anormal de l'appliance SDX.

Outre la configuration d'une destination d'interruption SNMP, le téléchargement de fichiers MIB et la configuration d'un ou plusieurs gestionnaires SNMP, vous pouvez configurer l'appliance Citrix ADC SDX pour les requêtes SNMPv3.

La figure suivante illustre un réseau doté d'une appliance SDX sur laquelle le protocole SNMP est activé et configuré. Sur la figure, chaque application de gestion de réseau SNMP utilise SNMP pour communiquer avec l'agent SNMP sur l'appliance SDX.

Figure 1. *Appliance SDX prenant en charge SNMP*



L'agent SNMP sur l'appliance SDX génère des interruptions conformes à SNMPv2 uniquement. Les interruptions prises en charge peuvent être affichées dans le fichier MIB SDX. Vous pouvez télécharger ce fichier à partir de la page Téléchargements de l'interface utilisateur SDX.

Pour ajouter une destination d'interruption SNMP

1. Sous l'onglet Configuration, dans le volet de navigation, développez **Système > SNMP**, puis cliquez sur Destinations des interruptions SNMP.

2. Dans le volet Destinations des interruptions SNMP, cliquez sur Ajouter.
3. Sur la page Configurer la destination d'interruption SNMP, spécifiez des valeurs pour les paramètres suivants :
   - Serveur de destination : adresse IPv4 de l'écouteur d'interruption auquel envoyer les messages d'interruption SNMP.
   - Port : port UDP sur lequel l'écouteur d'interruption écoute les messages d'interruption. Doit correspondre au paramètre de l'écouteur d'interruption, sinon l'écouteur supprime les messages. Valeur minimale : 1. Par défaut : 162.
   - Communauté : mot de passe (chaîne) envoyé avec les messages d'interruption, afin que l'écouteur d'interruption puisse les authentifier. Peut inclure des lettres, des chiffres et un trait d'union (-), un point (.), un hachage (#), un espace (), un caractère at (@), égal à (=), deux-points (:) et un trait de soulignement (_).
     Remarque : Spécifiez la même chaîne de communauté sur le périphérique d'écoute d'interruption, sinon l'écouteur supprime les messages. Par défaut : public.
4. Cliquez sur Ajouter, puis sur Fermer. La destination d'interruption SNMP que vous avez ajoutée s'affiche dans le volet Interruptions SNMP.

   Pour modifier les valeurs des paramètres d'une destination d'interruption SNMP, dans le volet Destinations des interruptions SNMP, sélectionnez la destination d'interruption à modifier, puis cliquez sur Modifier. Dans la boîte de dialogue Modifier la destination d'interruption SNMP, modifiez les paramètres.

   Pour supprimer un déroutement SNMP, dans le volet Destinations des interruptions SNMP, sélectionnez la destination d'interruption à supprimer, puis cliquez sur Supprimer. Dans la zone de message Confirmer, cliquez pour supprimer la destination d'interruption SNMP.

Téléchargement de fichiers MIB

Vous devez télécharger le fichier suivant avant de commencer à surveiller une appliance SDX.

SDX-MIB-smiv2.mib. Ce fichier est utilisé par les gestionnaires SNMPv2 et les récepteurs d'interruption SNMPv2.

Le fichier inclut une MIB d'entreprise Citrix ADC qui fournit des événements spécifiques à SDX.

Pour télécharger des fichiers MIB

1. Ouvrez une session sur la page Téléchargements de l'interface utilisateur de l'appliance SDX.
2. Sous Fichiers SNMP, cliquez sur SNMP v2 - Définitions d'objets MIB. Vous pouvez ouvrir le fichier à l'aide d'un navigateur MIB.

Ajout d'une communauté de gestionnaires SNMP

Configurez les gestionnaires SNMP sur l'appliance SDX pour interroger et surveiller l'appliance et les appareils gérés hébergés sur l'appliance. Vous devez également fournir au gestionnaire SNMP les informations spécifiques à l'appliance requises. Pour un gestionnaire SNMP IPv4, vous pouvez spécifier un nom d'hôte au lieu de l'adresse IP du gestionnaire. Dans ce cas, vous devez ajouter un serveur de noms DNS qui résout le nom d'hôte du gestionnaire SNMP en son adresse IP.

Configurez au moins un gestionnaire SNMP. Si vous ne configurez pas de gestionnaire SNMP, l'appliance n'accepte ni ne répond aux requêtes SNMP provenant d'aucune adresse IP du réseau. Si vous configurez un ou plusieurs gestionnaires SNMP, l'appliance accepte et répond uniquement aux requêtes SNMP provenant de ces adresses IP spécifiques.

Pour configurer un gestionnaire SNMP

1. Sous l'onglet Configuration, dans le volet de navigation, développez Système, puis SNMP.
2. Cliquez sur Managers.
3. Dans le volet d'informations, cliquez sur Ajouter.
4. Dans la page Créer une communauté de gestionnaire SNMP, définissez les paramètres suivants :
    - Gestionnaire SNMP : adresse IPv4 du gestionnaire SNMP. Au lieu d'une adresse IPv4, vous pouvez également spécifier un nom d'hôte qui a été attribué à un gestionnaire SNMP. Dans ce cas, vous devez ajouter un serveur de noms DNS qui résout le nom d'hôte du gestionnaire SNMP en son adresse IP.
    - Community : chaîne de communauté SNMP. Peut contenir de 1 à 31 caractères, dont des lettres majuscules et minuscules, des chiffres et le trait d'union (-), point (.) livre (#), at (@), égal (=), deux-points (:) et trait de soulignement (_).
    - Cochez la case **Activer le réseau de gestion** pour spécifier les gestionnaires SNMP à l'aide du masque de réseau.
    - Dans le champ **Masque réseau**, saisissez le masque de réseau de la communauté SNMP.
5. Cliquez sur Ajouter, puis sur Fermer.

Configuration de l'appliance SDX pour les requêtes SNMPv3

SNMPv3 est basé sur la structure et l'architecture de base de SNMPv1 et SNMPv2. Cependant, SNMPv3 améliore l'architecture de base pour intégrer des fonctionnalités d'administration et de sécurité, telles que l'authentification, le contrôle d'accès, la vérification de l'intégrité des données, la vérification de l'origine des données, la vérification de l'actualité des messages et la confidentialité des données.

L'appliance Citrix SDX prend en charge les entités suivantes qui vous permettent de mettre en œuvre les fonctionnalités de sécurité de SNMPv3 :

- Vues SNMP

- Utilisateurs SNMP

Ces entités fonctionnent ensemble pour implémenter les fonctionnalités de sécurité SNMPv3. Les vues sont créées pour permettre l'accès aux sous-arborescences de la MIB.

Ajout d'un gestionnaire SNMP

Configurez l'appliance SDX pour permettre aux gestionnaires SNMP appropriés de l'interroger. Fournissez également au gestionnaire SNMP les informations spécifiques à l'appliance requises. Pour un gestionnaire SNMP IPv4, vous pouvez spécifier un nom d'hôte au lieu de l'adresse IP du gestionnaire. Dans ce cas, vous devez ajouter un serveur de noms DNS qui résout le nom d'hôte du gestionnaire SNMP en son adresse IP.

Configurez au moins un gestionnaire SNMP. Si vous ne configurez pas de gestionnaire SNMP, l'appliance n'accepte ni ne répond aux requêtes SNMP provenant d'aucune adresse IP du réseau. Si vous configurez un ou plusieurs gestionnaires SNMP, l'appliance accepte et répond uniquement aux requêtes SNMP provenant de ces adresses IP spécifiques.

Pour configurer un gestionnaire SNMP :

1. Accédez à la page **Système > Configuration** .
2. Sous l'onglet Configuration, dans le volet de navigation, développez Système, puis SNMP.
3. Cliquez sur Managers.
4. Dans le volet d'informations, cliquez sur Ajouter.
5. Dans la boîte de dialogue Ajouter une communauté du gestionnaire SNMP, définissez les paramètres suivants :
   - **Gestionnaire SNMP** : adresse IPv4 du gestionnaire SNMP. Au lieu d'une adresse IPv4, vous pouvez également spécifier un nom d'hôte qui a été attribué à un gestionnaire SNMP. Dans ce cas, vous devez ajouter un serveur de noms DNS qui résout le nom d'hôte du gestionnaire SNMP en son adresse IP.
   - **Community** : chaîne de communauté SNMP. Peut contenir de 1 à 31 caractères, dont des lettres majuscules et minuscules, des chiffres et le trait d'union (-), point (.) livre (#), at (@), égal (=), deux-points (:) et trait de soulignement (_).
6. Cliquez sur Ajouter, puis sur Fermer.

Configuration d'une vue SNMP

Les vues SNMP limitent l'accès des utilisateurs à des parties spécifiques de la MIB. Les vues SNMP sont utilisées pour implémenter le contrôle d'accès.

Pour configurer une vue

1. Sous l'onglet Configuration, dans le volet de navigation, développez Système, puis SNMP.

2. Cliquez sur Affichages.
3. Dans le volet d'informations, cliquez sur Ajouter.
4. Dans la boîte de dialogue Ajouter une vue SNMP, définissez les paramètres suivants :
    - Nom : nom de la vue SNMPv3. Peut contenir de 1 à 31 caractères, dont des lettres majuscules et minuscules, des chiffres et le trait d'union (-), point (.) livre (#), at (@), égal (=), deux-points (:) et trait de soulignement (_). Choisissez un nom qui permet d'identifier la vue SNMPv3.
    - Sous-arbre : branche particulière (sous-arbre) de l'arborescence MIB, que vous souhaitez associer à cette vue SNMPv3. Spécifiez le sous-arbre en tant qu'OID SNMP.
    - Type (Type) : inclut ou exclut la sous-arborescence, spécifiée par le paramètre de sous-arborescence, dans ou à partir de cette vue. Ce paramètre peut être utile lorsque vous avez inclus un sous-arbre, tel que A, dans une vue SNMPv3 et que vous souhaitez exclure un sous-arbre spécifique de A, tel que B, de la vue SNMPv3.

Configuration d'un utilisateur SNMP

Après avoir créé une vue SNMP, ajoutez des utilisateurs SNMP. Les utilisateurs SNMP ont accès aux MIB nécessaires pour interroger les gestionnaires SNMP.

Pour configurer un utilisateur

1. Sous l'onglet Configuration, dans le volet de navigation, développez Système, puis SNMP.
2. Cliquez sur Utilisateurs.
3. Dans le volet d'informations, cliquez sur Ajouter.
4. Dans la page Créer un utilisateur SNMP, définissez les paramètres suivants :
    - Nom : nom de l'utilisateur SNMPv3. Peut contenir de 1 à 31 caractères, dont des lettres majuscules et minuscules, des chiffres et le trait d'union (-), point (.) livre (#), at (@), égal (=), deux-points (:) et trait de soulignement (_).
    - Niveau de sécurité : niveau de sécurité requis pour la communication entre l'appliance et les utilisateurs SNMPv3. Sélectionnez l'une des options suivantes :
        - noAuthNoPriv : ne nécessitent ni authentification ni chiffrement.
        - authNoPriv : nécessite une authentification mais aucun cryptage.
        - authPriv : nécessite une authentification et un cryptage.
    - Protocole d'authentification : algorithme d'authentification utilisé par l'appliance et l'utilisateur SNMPv3 pour authentifier la communication entre eux. Spécifiez le même algorithme d'authentification lorsque vous configurez l'utilisateur SNMPv3 dans le gestionnaire SNMP.
    - Mot de passe d'authentification : phrase secrète à utiliser par l'algorithme d'authentification. Peut contenir de 1 à 31 caractères, dont des lettres majuscules et minuscules, des chiffres

et le trait d'union (-), point (.) livre (#), espace (), at (@), égal (=), deux-points (:) et trait de soulignement (_).

- Protocole de confidentialité : algorithme de chiffrement utilisé par l'appliance et l'utilisateur SNMPv3 pour chiffrer la communication entre eux. Spécifiez le même algorithme de chiffrement lorsque vous configurez l'utilisateur SNMPv3 dans le gestionnaire SNMP.
- Nom de la vue : nom de la vue SNMPv3 configurée que vous souhaitez lier à cet utilisateur SNMPv3. Un utilisateur SNMPv3 peut accéder aux sous-arborescences liées à cette vue SNMPv3 en tant que type INCLUDED, mais ne peut pas accéder à celles de type EXCLUDED.

Configuration d'une alarme SNMP

L'appliance fournit un ensemble prédéfini d'entités de condition appelées alarmes SNMP. Lorsque la condition définie pour une alarme SNMP est remplie, l'appliance génère des messages d'interruption SNMP qui sont envoyés aux écouteurs d'interruption configurés. Par exemple, lorsque l'alarme DeviceAdded est activée, un message d'interruption est généré et envoyé à l'écouteur d'interruption chaque fois qu'un périphérique (instance) est provisionné sur l'appliance. Vous pouvez attribuer un niveau de gravité à une alarme SNMP. Ce niveau de gravité est alors affecté aux messages d'interruption correspondants.

Voici les niveaux de gravité définis sur l'appliance, par ordre de gravité décroissant :

- Critical
  - Major
- Mineur
- Avertissement
- Informationnel (par défaut)

Par exemple, si vous définissez un niveau de gravité d'avertissement pour l'alarme SNMP nommée DeviceAdded, les messages d'interruption générés lors de l'ajout d'un périphérique sont affectés au niveau de gravité Avertissement.

Vous pouvez également configurer une alarme SNMP pour consigner les messages d'interruption correspondants générés chaque fois que la condition de cette alarme est remplie.

Pour modifier une alarme SNMP prédéfinie, cliquez sur **Système > SNMP > Alarmes**.

Configurer les notifications Syslog

January 27, 2022

SYSLOG est un protocole de journalisation standard. Il comprend deux composants : le module d'audit SYSLOG, qui s'exécute sur l'appliance Citrix ADC SDX, et le serveur SYSLOG, qui peut s'exécuter sur un système distant. SYSLOG utilise UDP pour le transfert de données.

Lorsque vous exécutez un serveur SYSLOG, il se connecte à l'appliance SDX. L'appliance commence alors à envoyer toutes les informations de journal au serveur SYSLOG, et le serveur peut filtrer les entrées de journal avant de les stocker dans un fichier journal. Un serveur SYSLOG peut recevoir des informations de journal de plusieurs dispositifs SDX, et un boîtier SDX peut envoyer des informations de journal à plusieurs serveurs SYSLOG.

Les informations de journal qu'un serveur SYSLOG collecte auprès d'une appliance
SDX sont stockées dans un fichier journal sous forme de messages. Ces messages contiennent généralement les informations suivantes :

- L'adresse IP de l'appliance SDX qui a généré le message de journal
- Un horodatage
- Le type de message
- Le niveau de journalisation (critique, erreur, avis, avertissement, information, débogage, alerte ou urgence)
- Les informations de message

Vous pouvez utiliser ces informations pour analyser la source de l'alerte et prendre des mesures correctives si nécessaire. Configurez d'abord un serveur Syslog auquel l'appliance envoie des informations de journal, puis spécifiez les données et le format d'heure pour l'enregistrement des messages de journal.

Configurer un serveur Syslog

1. Accédez à **Système > Notifications > Serveurs Syslog**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la page **Créer un serveur Syslog**, spécifiez des valeurs pour les paramètres du serveur Syslog. Pour obtenir la description d'un paramètre, placez le curseur de la souris sur le champ correspondant.
4. Cliquez sur **Ajouter**, puis sur **Fermer**.

Configurez les paramètres de Syslog

1. Accédez à **Système > Notifications > Serveurs Syslog**.
2. Dans le volet d'informations, cliquez sur **Paramètres Syslog**.
3. Dans la page **Configurer les paramètres Syslog**, spécifiez le format de date et d'heure.
4. Cliquez sur **OK**, puis sur **Fermer**.

Configuration des notifications par e-mail

January 27, 2022

Configurez un serveur SMTP pour recevoir un message électronique chaque fois qu'une alerte est déclenchée. Configurez d'abord un serveur SMTP, puis configurez un profil de messagerie. Dans le profil de messagerie, utilisez des virgules pour séparer les adresses des destinataires.

Pour configurer un serveur SMTP

1. Accédez à **Système > Notifications > E-mail**.
2. Dans le volet d'informations, cliquez sur l'onglet **Serveur de messagerie**, puis sur **Ajouter**.
3. Sur la page **Créer un serveur de messagerie**, spécifiez des valeurs pour les paramètres du serveur. Pour obtenir la description d'un paramètre, placez le curseur de la souris sur le champ correspondant.
4. Cliquez sur **Créer**.

Pour configurer un profil de messagerie

1. Accédez à **Système > Notifications > E-mail**.
2. Dans le volet d'informations, cliquez sur l'onglet **E-mail**, puis sur **Ajouter**.
3. Sur la page **Créer une liste de distribution d'e-mails**, spécifiez des valeurs pour les paramètres. Pour obtenir la description d'un paramètre, placez le curseur de la souris sur le champ correspondant.
4. Cliquez sur **Créer**.

Configurer les notifications par SMS

January 27, 2022

Configurez un serveur de service de messages courts (SMS) pour recevoir un message SMS chaque fois qu'une alerte est déclenchée. Configurez d'abord un serveur SMS, puis configurez un profil SMS. Dans le profil SMS, utilisez des virgules pour séparer les adresses des destinataires.

Configurer un serveur SMS

1. Accédez à **Système > Notifications > SMS**.
2. Dans le volet d'informations, cliquez sur **Serveur SMS**, puis sur **Ajouter**.

3. Sur la page **Créer un serveur SMS**, spécifiez les valeurs des paramètres du serveur SMS. Les valeurs de ces paramètres sont fournies par le fournisseur.
4. Cliquez sur **Créer**, puis sur **Fermer**.

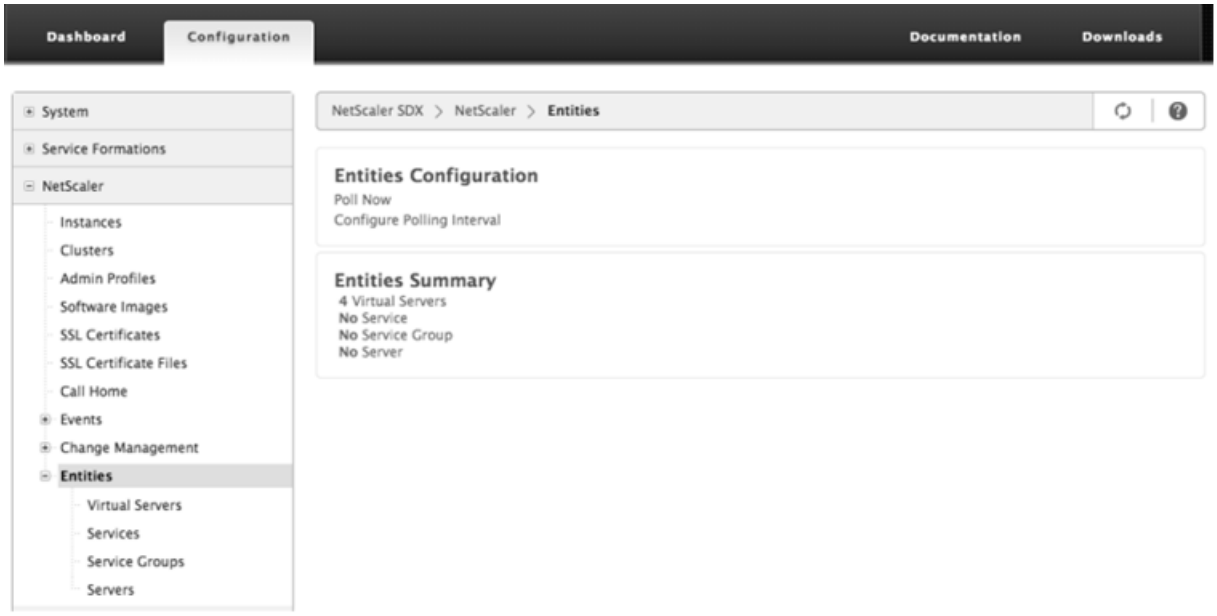
Configurer un profil SMS

1. Accédez à **Système > Notifications > SMS**.
2. Dans le volet d'informations, cliquez sur **Liste de distribution des SMS**, puis sur **Ajouter**.
3. Sur la page **Créer une liste de distribution SMS**, spécifiez les valeurs des paramètres de profil de messagerie. Pour obtenir la description d'un paramètre, placez le curseur de la souris sur le champ correspondant.
4. Cliquez sur **Créer**, puis sur **Fermer**.

Surveillez et gérez l'état en temps réel des entités configurées sur une appliance SDX

January 27, 2022

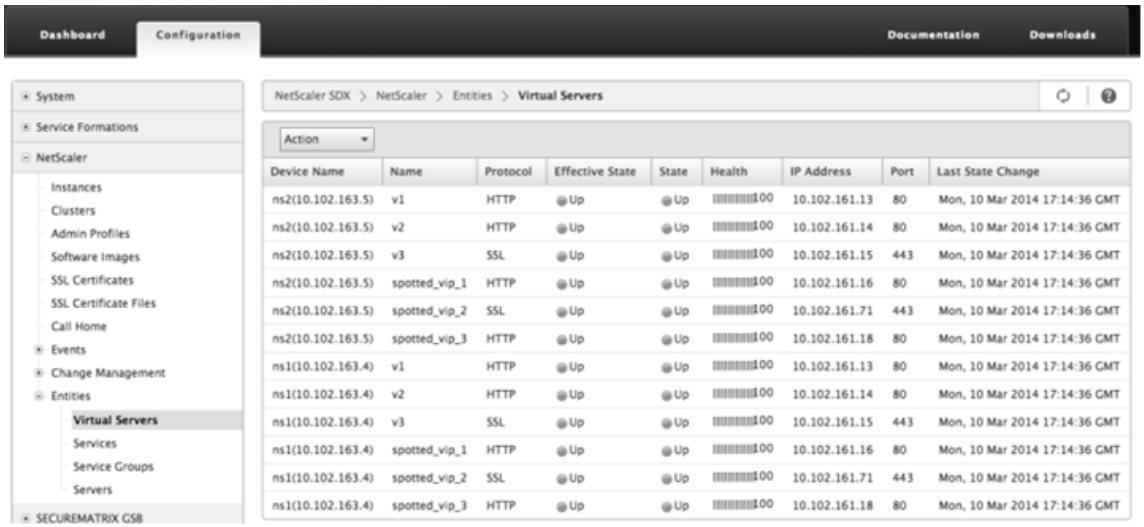
L'appliance Citrix ADC SDX peut surveiller et gérer les états des serveurs virtuels, des services, des groupes de services et des serveurs sur les dispositifs virtuels hébergés sur l'appliance SDX. Vous pouvez surveiller des valeurs, telles que l'état d'un serveur virtuel et le temps écoulé depuis le dernier changement d'état d'un service ou d'un groupe de services. Cette surveillance vous donne une visibilité sur l'état en temps réel des entités et facilite la gestion de ces entités lorsque de nombreuses entités sont configurées sur vos instances Citrix ADC.



Afficher l'état des serveurs virtuels

Vous pouvez surveiller les valeurs en temps réel de l'état et de la santé d'un serveur virtuel. Vous pouvez également afficher les attributs d'un serveur virtuel, tels que le nom, l'adresse IP et le type de serveur virtuel.

- Pour afficher l'état d'un serveur virtuel
  1. Dans l'onglet Configuration, dans le volet de navigation, cliquez sur **Citrix ADC > Entités > Serveurs virtuels**.
  2. Dans le volet droit, sous Serveurs virtuels, affichez les statistiques suivantes :
     - Nom du périphérique : nom du VPX sur lequel le serveur virtuel est configuré.
     - Nom : nom du serveur virtuel.
     - Protocole : type de service du serveur virtuel. Par exemple, HTTP, TCP et SSL.
     - État effectif : état effectif du serveur virtuel, en fonction de l'état des serveurs virtuels de sauvegarde. Par exemple, UP, DOWN ou OUT OF SERVICE.
     - État : état actuel du serveur virtuel. Par exemple, UP, DOWN ou OUT OF SERVICE.
     - Santé : pourcentage de services dont l'état est actif et qui sont liés au serveur virtuel. La formule suivante est utilisée pour calculer le pourcentage de santé : (Nombre de services UP liés * 100)/Total des services liés
     - Adresse IP : adresse IP du serveur virtuel. Les clients envoient des demandes de connexion à cette adresse IP.
     - Port : port sur lequel le serveur virtuel écoute les connexions client.
     - Dernière modification d'état : temps écoulé (en jours, heures, minutes et secondes) depuis le dernier changement d'état du serveur virtuel. C'est-à-dire la durée pendant laquelle le serveur virtuel a été dans l'état actuel. Ces informations ne sont disponibles que pour les serveurs virtuels configurés sur NetScaler 9.0 et versions ultérieures.

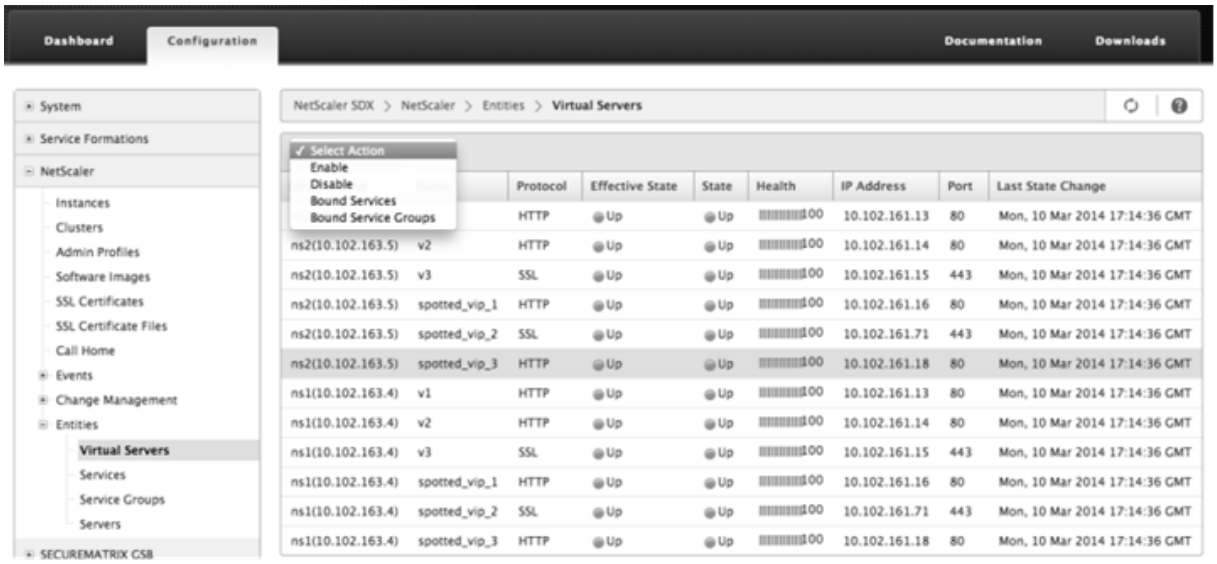


- Affichage des services et des groupes de services liés à un serveur virtuel

Vous pouvez surveiller l'état en temps réel des services et des groupes de services liés à un serveur virtuel. Cette surveillance vous permet de vérifier l'état des services susceptibles d'entraîner une baisse du pourcentage de santé d'un serveur virtuel, afin que vous puissiez prendre les mesures appropriées.

Pour afficher les services et les groupes de services liés à un serveur virtuel

1. Dans l'onglet Configuration, dans le volet gauche, cliquez sur **Citrix ADC > Entités > Serveurs virtuels**.
2. Dans le volet d'informations, sous Serveurs virtuels, cliquez sur le nom du serveur virtuel pour lequel vous souhaitez afficher les services liés et les groupes de services, puis sous Actions, cliquez sur Services liés ou Groupes de services liés. Vous pouvez également cliquer avec le bouton droit sur le nom du serveur virtuel, puis cliquer sur Services liés ou Groupes de services liés.



Afficher l'état des services

Vous pouvez surveiller les valeurs en temps réel de l'état d'un service et la durée pendant laquelle le service a été dans l'état actuel.

Pour afficher l'état des serveurs virtuels

1. Dans l'onglet Configuration, dans le volet de navigation, cliquez sur **Citrix ADC > Entités > Service**.
2. Dans le volet d'informations, sous Services, affichez les statistiques suivantes :
   - Nom de l'appareil : nom de l'appareil sur lequel le service est configuré.
   - Nom : nom du service.
   - Protocole : type de service, qui détermine le comportement du service. Par exemple, HTTP, TCP, UDP ou SSL.

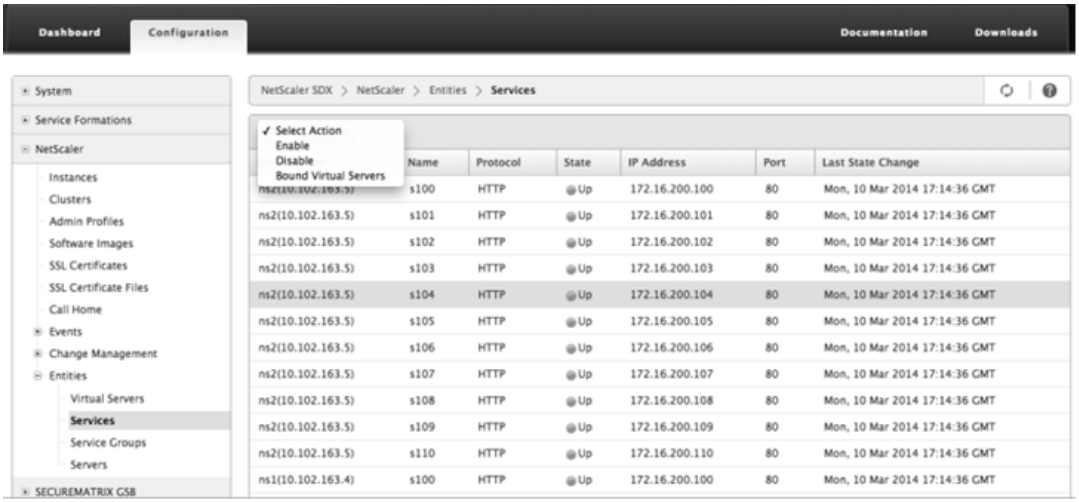
- État : état actuel du service. Par exemple, UP, DOWN ou OUT OF SERVICE.
- Adresse IP : adresse IP du service.
- Port : port sur lequel le service écoute.
- Dernière modification d'état : temps écoulé (en jours, heures, minutes et secondes) depuis la dernière modification de l'état du service. C'est-à-dire la durée pendant laquelle le service a été dans l'état actuel.

- Affichage des serveurs virtuels auxquels un service est lié

  Vous pouvez afficher les serveurs virtuels auxquels un service est lié et surveiller l'état en temps réel des serveurs virtuels.

  Pour afficher les serveurs virtuels auxquels un service est lié

  1. Dans l'onglet Configuration, dans le volet de navigation, cliquez sur **Citrix ADC > Entités > Service**.
  2. Dans le volet d'informations, sous Services, cliquez sur le nom du service dont vous souhaitez afficher les serveurs virtuels liés. Ensuite, dans le menu Action, sélectionnez Serveurs virtuels liés. Vous pouvez également cliquer avec le bouton droit sur le service, puis cliquer sur Serveurs virtuels liés.



Afficher l'état des groupes de services

Vous pouvez surveiller l'état en temps réel d'un membre du groupe de services à partir de l'interface SDX.

Pour afficher l'état des groupes de services

1. Dans l'onglet Configuration, dans le volet de navigation, cliquez sur **Citrix ADC > Entités > Groupes de services**.
2. Dans le volet d'informations, sous Groupes de services, affichez les statistiques suivantes :

- Nom du périphérique : nom de l'appareil sur lequel le groupe de services est configuré.
- Nom : nom du groupe de services.
- Adresse IP : adresse IP de chaque service membre du groupe de services.
- Port : ports sur lesquels les membres du groupe de services écoutent.
- Protocole : type de service, qui détermine le comportement du groupe de services. Par exemple, HTTP, TCP, UDP ou SSL.
- État effectif : état effectif du groupe de serveurs virtuels, en fonction de l'état des serveurs virtuels de sauvegarde. Par exemple, UP, DOWN ou OUT OF SERVICE
- État : état effectif du groupe de services, qui est basé sur l'état du membre du groupe de services. Par exemple, UP, DOWN ou OUT OF SERVICE.
- Dernière modification d'état : temps écoulé (en jours, heures, minutes et secondes) depuis la dernière modification de l'état du membre du groupe de services. C'est-à-dire la durée pendant laquelle le membre du groupe de services a été dans l'état actuel. Ces informations ne sont disponibles que pour les membres du groupe de services configurés sur NetScaler 9.0 et versions ultérieures.

- Affichage des serveurs virtuels auxquels un service est lié

  Vous pouvez afficher les serveurs virtuels auxquels un service est lié et surveiller l'état en temps réel des serveurs virtuels.

  Pour afficher les serveurs virtuels auxquels le service est lié

  1. Dans l'onglet Configuration, dans le volet gauche, cliquez sur **Citrix ADC > Entités > Serveurs**.
  2. Dans le volet droit, sous Serveurs, sélectionnez le serveur dans la liste, puis dans le menu Actions, cliquez sur Services virtuels liés. Vous pouvez également cliquer avec le bouton droit sur le service et sélectionner Serveurs virtuels liés

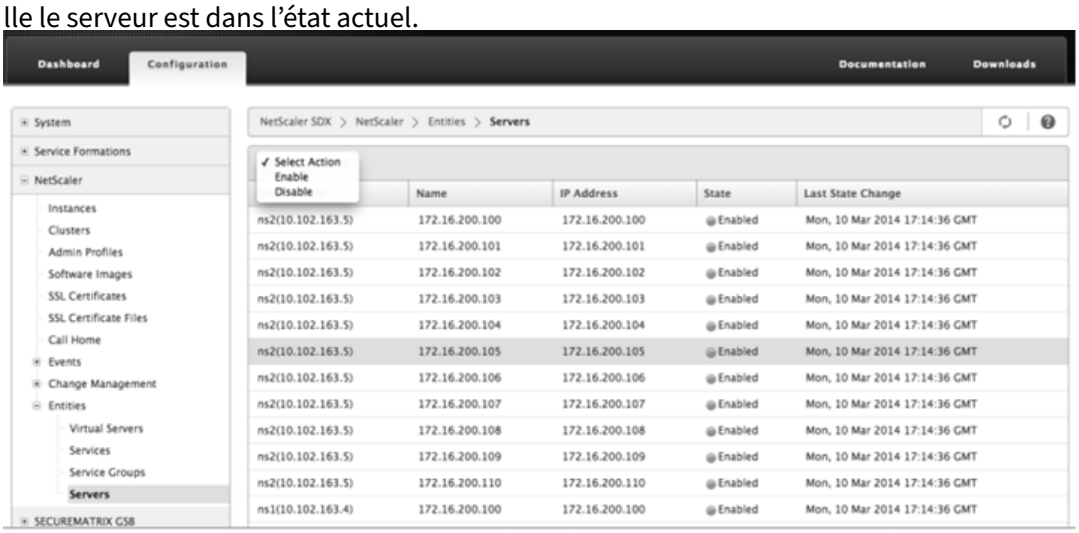
Afficher l'état des serveurs

Vous pouvez surveiller et gérer les états des serveurs sur les instances Citrix ADC. Cette surveillance vous donne une visibilité sur l'état en temps réel des serveurs et facilite la gestion de ces serveurs lorsque vous avez de nombreux serveurs.

Pour afficher l'état des serveurs

1. Dans l'onglet Configuration, dans le volet de navigation, cliquez sur **Citrix ADC > Entités > Serveurs**.
2. Dans le volet d'informations, sous Serveurs, affichez les statistiques suivantes :
   - Nom de l'appareil : spécifie le nom de l'appareil sur lequel le serveur est configuré.
   - Nom : spécifie le nom du serveur.
   - Adresse IP : spécifie l'adresse IP du serveur. Les clients envoient des demandes de connexion à cette adresse IP.

- État : spécifie l'état actuel du serveur. Par exemple, UP, DOWN et OUT OF SERVICE.
- Dernière modification d'état : spécifie le temps écoulé (en jours, heures, minutes et secondes) depuis le dernier changement d'état du serveur. C'est-à-dire la durée pendant laquelle le serveur est dans l'état actuel.



Configurer l'intervalle d'interrogation

Vous pouvez définir l'intervalle de temps pendant lequel vous souhaitez que l'appliance SDX interroge les valeurs en temps réel des serveurs virtuels, des services, des groupes de services et des serveurs. Par défaut, l'appliance interroge les valeurs toutes les 30 minutes.

- Pour configurer l'intervalle d'interrogation pour les serveurs virtuels, les services, les groupes de services et les serveurs.

  1. Dans l'onglet Configuration, cliquez sur **Citrix ADC > Entités**, puis dans le volet droit, cliquez sur Configurer l'intervalle d'interrogation.
  2. Dans la boîte de dialogue Configurer l'intervalle d'interrogation, tapez le nombre de minutes que vous souhaitez définir comme intervalle de temps pour lequel SDX doit interroger la valeur de l'entité. La valeur minimale de l'intervalle d'interrogation est de 30 minutes. Cliquez sur OK.

Surveillance et gestion des événements générés sur les instances Citrix ADC

January 27, 2022

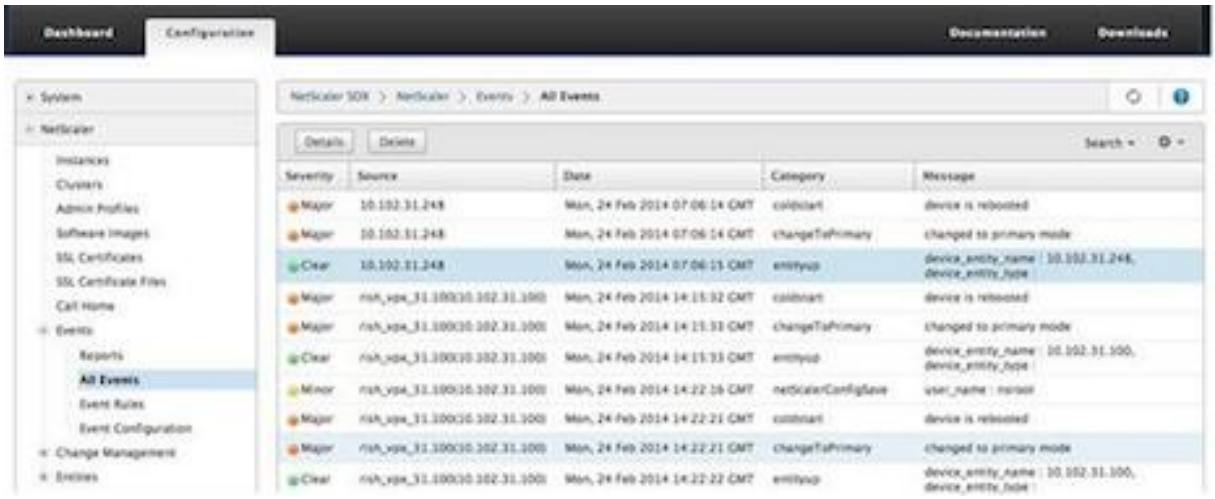
Utilisez la fonctionnalité Événements pour surveiller et gérer les événements générés sur les instances Citrix ADC. Le service de gestion identifie les événements en temps réel, vous aide à résoudre les prob-

lèmes immédiatement et assure le bon fonctionnement des instances Citrix ADC. Vous pouvez également configurer des règles d'événement pour filtrer les événements générés et recevoir une notification pour prendre des mesures sur la liste d'événements filtrée.

Afficher tous les événements

Vous pouvez afficher tous les événements générés sur les instances Citrix ADC provisionnées sur l'appliance Citrix ADC SDX. Vous pouvez afficher les détails tels que la gravité, la catégorie, la date, la source et le message de chacun des événements.

Pour afficher les événements, accédez à **Configuration > Citrix ADC > Événements > Tous les événements**.



Vous pouvez afficher l'historique de l'événement et les détails de l'entité en sélectionnant l'événement et en cliquant sur le bouton **Détails** . Vous pouvez également rechercher un événement particulier ou le supprimer de cette page.

Remarque : Une fois les événements supprimés, vous ne serez pas en mesure de les récupérer.

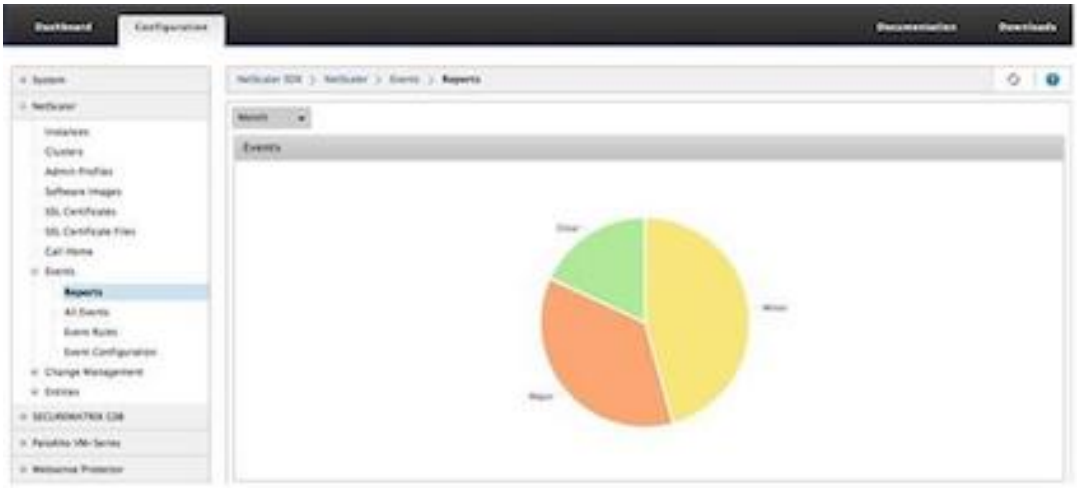
- Affichage de rapports

  La page Rapports affiche le résumé des événements dans un format graphique. Votre vue des rapports peut être basée sur différentes échelles de temps. Par défaut, l'échelle de temps est Jour.

  Pour afficher les rapports, accédez à **Configuration > Citrix ADC > Événements > Rapports**. Voici les rapports graphiques pris en charge par le service de gestion

  - **Événements**

    Le rapport Événements est une représentation graphique à secteurs du nombre d'événements, segmentés et codés par couleur en fonction de leur gravité.

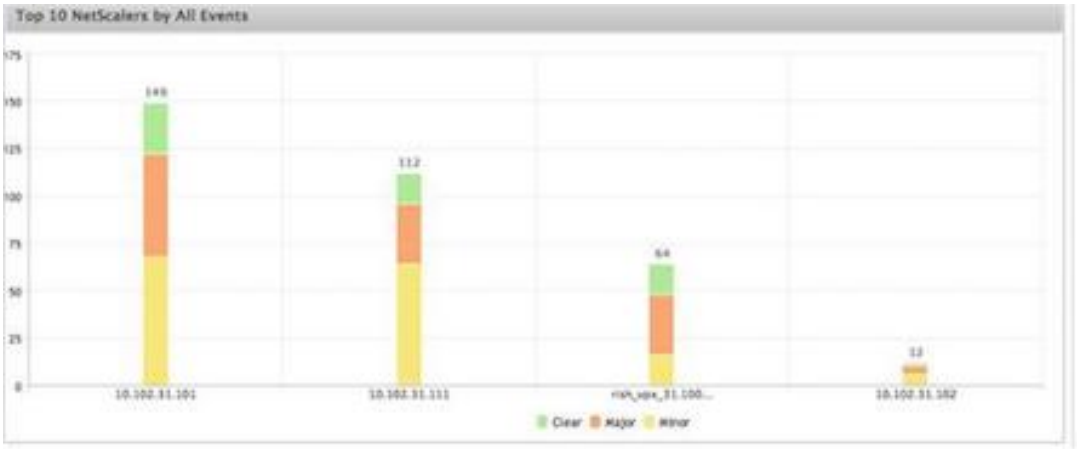


Pour afficher les détails des événements d'une gravité particulière, cliquez sur ce segment du graphique à secteurs, vous pouvez afficher les détails suivants :

* Source : nom du système, nom d'hôte ou adresse IP sur laquelle l'événement a été généré.
* Date : Date et heure auxquelles l'alarme a été générée.
* Catégorie : catégorie d'événement (par exemple, `entityup`).
* Message : Description de l'événement.

– **Top 10 des instances Citrix ADC selon tous les événements**

Ce rapport est un graphique à barres qui affiche les 10 meilleures instances Citrix ADC en fonction du nombre d'événements pour l'échelle de temps sélectionnée.



– **10 principales instances Citrix ADC par événements de modification de l'état de l'entité**

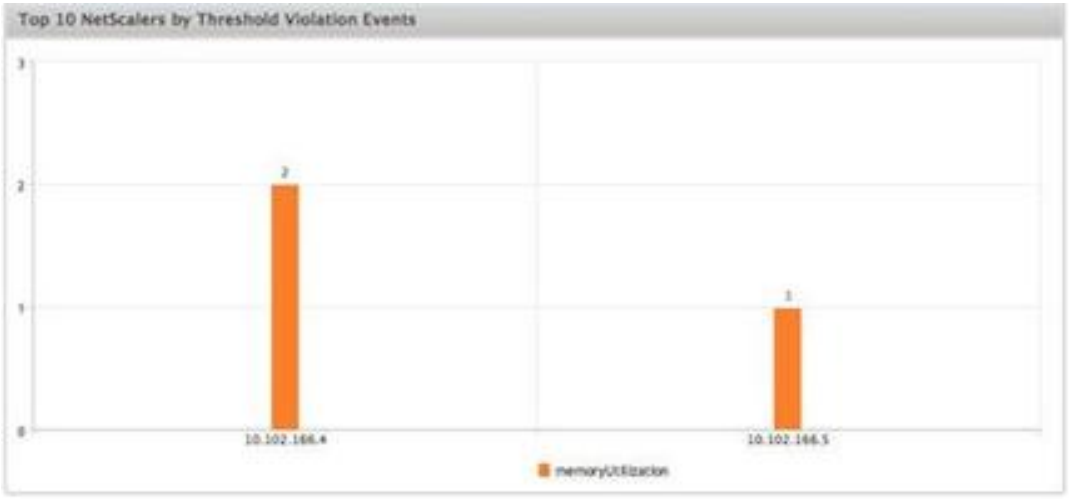
Ce rapport est un graphique à barres qui affiche les 10 premières instances Citrix ADC en fonction du nombre de changements d'état de l'entité pour l'échelle de temps sélectionnée. Les changements d'état de l'entité reflètent les événements d'entité en hausse, en

baisse ou hors service.

– **10 instances Citrix ADC les plus fréquentes par événements de violation de seuil**

Ce rapport est un graphique à barres qui affiche les 10 principales instances Citrix ADC en fonction du nombre d'événements de violation de seuil pour l'échelle de temps sélectionnée. Les événements de violation de seuil reflètent les événements suivants :

* cpuUtilization
* memoryUtilization
* diskUsageHigh
* temperatureHigh
* voltageLow
* voltageHigh
* fanSpeedLow
* temperatureCpuHigh
* interfaceThroughputLow
* interfaceBWUseHigh
* aggregateBWUseHigh



- **10 principales instances Citrix ADC par événements de défaillance matérielle**
  Ce rapport est un graphique à barres qui affiche les 10 premières instances Citrix ADC en fonction du nombre d'événements de défaillance matérielle pour l'échelle de temps sélectionnée. Les événements de défaillance matérielle reflètent les événements suivants :
  * hardDiskDriveErrors
  * compactFlashErrors
  * powerSupplyFailed
  * "sslCardFailed"
- **10 principales instances de Citrix ADC par événements de modification de configuration**

  Ce rapport est un graphique à barres qui reflète les 10 principales instances Citrix ADC en fonction du nombre d'événements de modification de configuration pour l'échelle de temps sélectionnée. Vous pouvez cliquer sur le graphique pour effectuer une hiérarchisation vers le bas et afficher les modifications de configuration basées sur l'utilisateur pour une instance. Vous pouvez également consulter les détails de l'autorisation et de l'état d'exécution en cliquant sur ce graphique.

- <**Top 10 des instances Citrix ADC par événements d'échec d'authentification**

Ce rapport est un graphique à barres qui affiche les 10 principales instances Citrix ADC en fonction du nombre d'événements d'échec d'authentification pour l'échelle de temps sélectionnée. Vous pouvez cliquer sur le graphique pour effectuer une hiérarchisation vers le bas et afficher les échecs d'authentification basés sur les utilisateurs pour une instance.

- Configuration des règles d'événement

  Vous pouvez filtrer un ensemble d'événements en configurant des règles avec des conditions spécifiques et en affectant des actions aux règles. Lorsque les événements générés répondent aux critères de filtre de la règle, l'action associée à la règle est exécutée. Les conditions pour lesquelles vous pouvez créer des filtres sont les suivantes : gravité, appareils, objets de défaillance et catégorie.

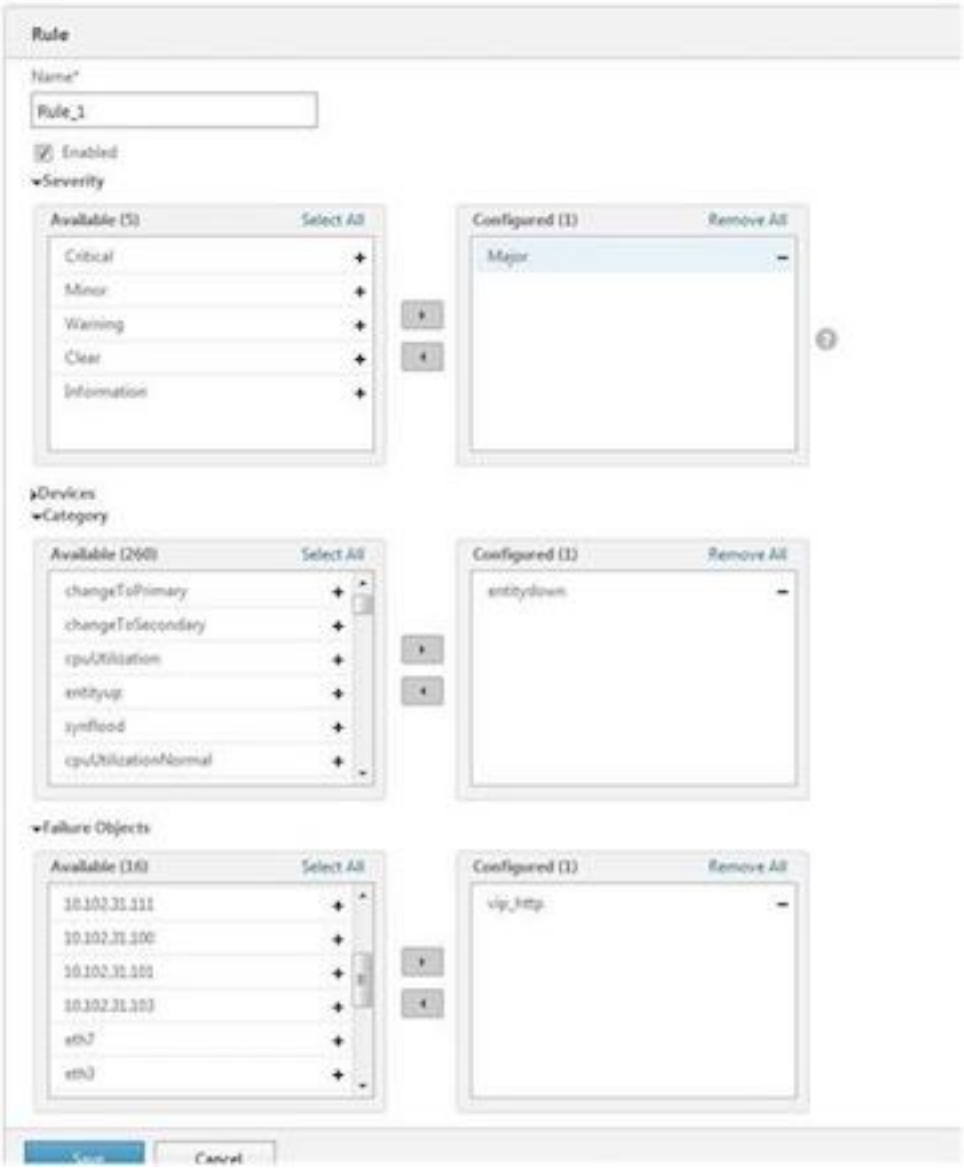
  Vous pouvez affecter les actions suivantes aux événements :

  - **Action Envoyer un e-mail** Envoie un e-mail pour les événements qui correspondent aux critères de filtre.
  - **Action Envoyer un SMS** Envoie un service de messages courts (SMS) pour les événements qui correspondent aux critères de filtre.

  Pour ajouter des règles d'événement

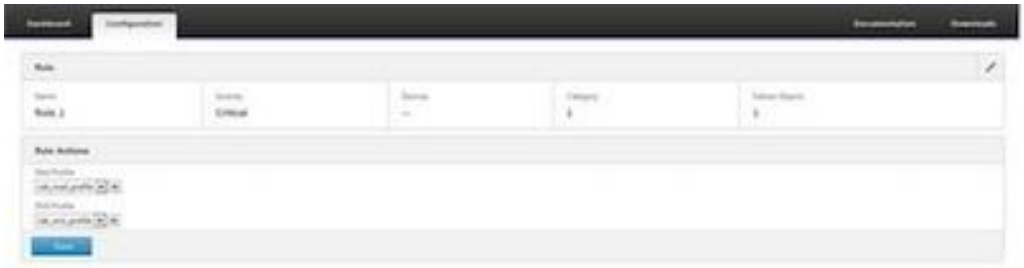
  1. Accédez à **Configuration > Citrix ADC > Événements > Règles d'événement**, puis cliquez sur Ajouter.

2. Sur la page Règle, définissez les paramètres suivants :
   - Nom : nom de la règle d'événement.
   - Activé : permet d'activer la règle d'événement.
   - Gravité : gravité des événements pour lesquels vous souhaitez ajouter la règle d'événement.
   - Appareils : adresses IP des instances Citrix ADC pour lesquelles vous souhaitez définir une règle d'événement.
   - Catégorie : catégorie ou catégories des événements générés par les instances Citrix ADC.
   - Objets d'échec : instances ou compteurs d'entité pour lesquels un événement a été généré.



Remarque : Cette liste peut contenir des noms de compteurs pour tous les événements liés aux seuils, des noms d'entités pour tous les événements liés à l'entité et des noms de certificats pour les événements liés aux certificats.

3. Cliquez sur Enregistrer.
4. Sous Actions de règle, vous pouvez affecter les actions de notification pour l'événement.
   a) Profil de messagerie : détails du serveur de messagerie et du profil de messagerie. Un e-mail est déclenché lorsque les événements répondent aux critères de filtre définis.
   b) Profil SMS : détails du serveur SMS et du profil SMS. Un SMS est déclenché lorsque les événements répondent aux critères de filtre définis.

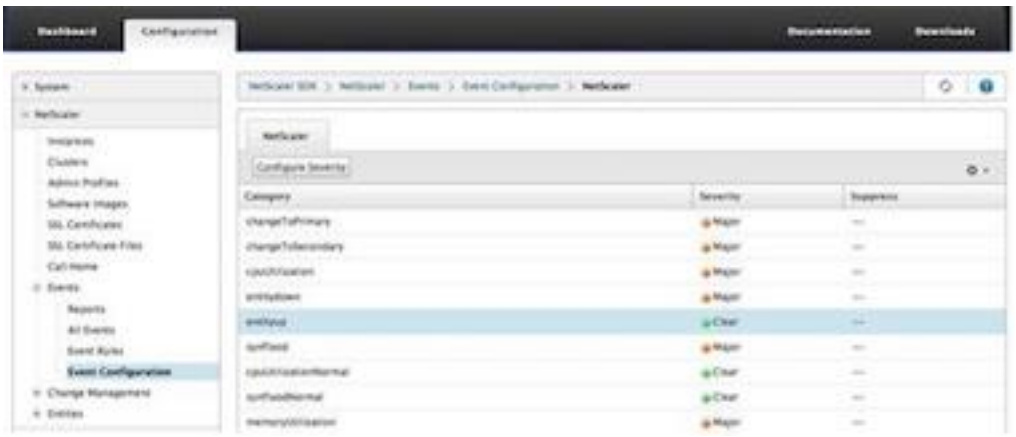


5. Cliquez sur Terminé.

- Configuration des événements

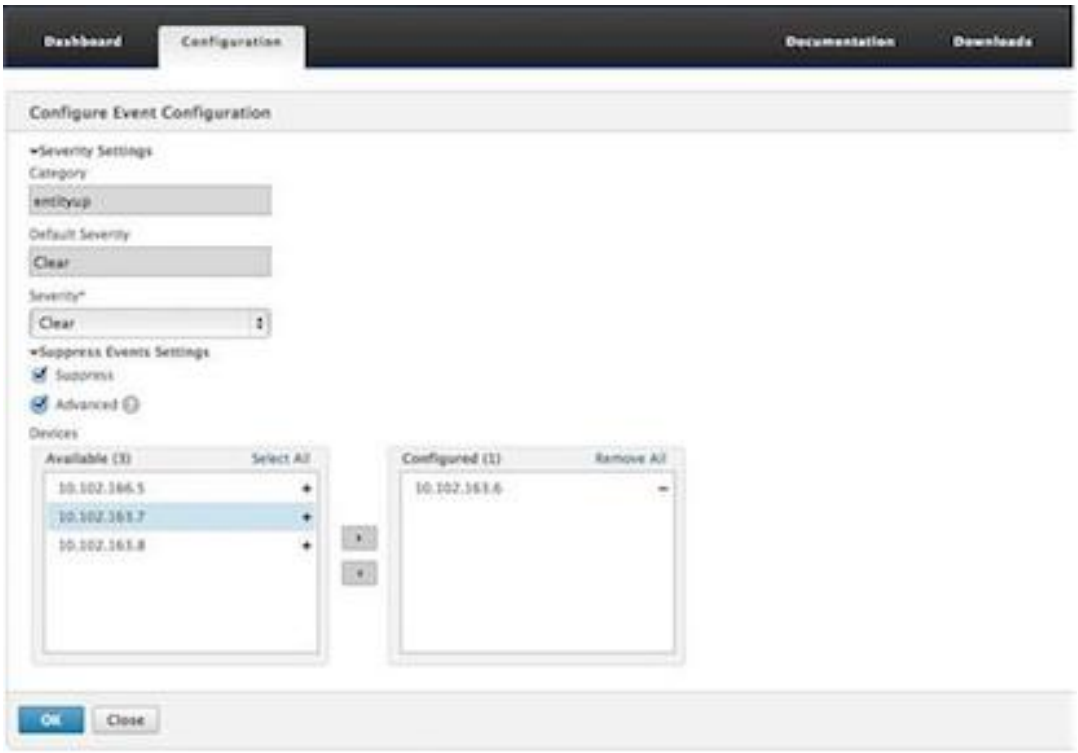
Vous pouvez attribuer des niveaux de gravité aux événements qui sont générés pour les instances Citrix ADC sur l'appliance SDX. Vous pouvez définir les types de niveaux de gravité suivants : Critique, Majeur, Mineur, Avertissement, Clair et Informations. Vous pouvez également supprimer les événements pendant un certain temps.
Pour configurer la gravité :

1. Accédez à **Configuration > Citrix ADC > Événements > Configuration de l'événement**, sélectionnez l'événement dans la liste, puis cliquez sur Configurer la gravité.



2. Sur la page Configurer la configuration des événements, sélectionnez le niveau de gravité requis dans la liste déroulante.

3. Vous pouvez également supprimer les événements en cochant la case Supprimer. Vous pouvez également spécifier les instances Citrix ADC pour lesquelles vous souhaitez supprimer cet événement à l'aide de l'option Avancé.



4. Cliquez sur OK.

Assistance Call Home pour les instances Citrix ADC sur une appliance SDX

January 27, 2022

La fonctionnalité Call Home surveille vos instances Citrix ADC pour détecter les conditions d'erreur courantes. Vous pouvez désormais configurer, activer ou désactiver la fonctionnalité Call Home sur les instances Citrix ADC à partir de l'interface utilisateur du service de gestion.

Remarque : L'instance Citrix ADC doit être enregistrée auprès du serveur de support technique Citrix avant que Call Home puisse télécharger les données système sur le serveur lorsque des conditions d'erreur prédéfinies se produisent sur l'appliance. L'activation de la fonctionnalité Call Home sur l'instance Citrix ADC lance le processus d'enregistrement.

- Activation et désactivation de Call Home sur une instance Citrix ADC

  Vous pouvez activer la fonctionnalité Call Home sur une instance Citrix ADC à partir du service

de gestion. Lorsque vous activez la fonctionnalité Call Home, le processus Call Home enregistre l'instance Citrix ADC auprès du serveur de support technique Citrix. L'enregistrement prend un certain temps. Pendant ce temps, le service de gestion affiche la progression de l'enregistrement.

Pour activer la fonctionnalité Call Home, accédez à **Configuration > Citrix ADC > Call Home**, sélectionnez l'instance Citrix ADC et cliquez sur le bouton Activer. Sur la page de confirmation, cliquez sur Oui.

Pour désactiver la fonctionnalité Call Home, accédez à **Configuration > Citrix ADC > Call Home**, sélectionnez l'instance Citrix ADC et cliquez sur le bouton Désactiver. Sur la page de confirmation, cliquez sur Oui.

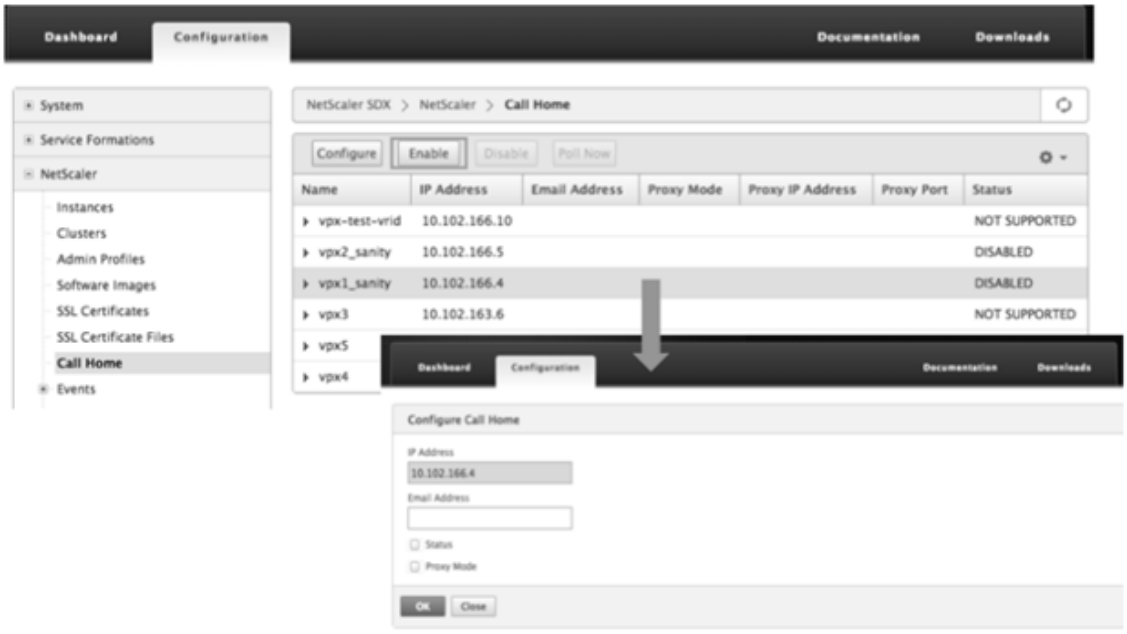
Si vous activez Call Home, vous pouvez configurer les options suivantes :

1. (Facultatif) Spécifiez l'adresse e-mail de l'administrateur. Le processus Call Home envoie l'adresse e-mail au serveur de support, où elle est stockée pour toute correspondance future concernant Call Home.
2. (Facultatif) Activez le mode proxy Call Home. Call Home peut télécharger les données de votre instance Citrix ADC sur le serveur Citrix TaaS via un serveur proxy. Pour utiliser cette fonctionnalité, activez-la sur votre instance Citrix ADC et spécifiez l'adresse IP et le numéro de port d'un serveur proxy HTTP. Tout le trafic du serveur proxy vers les serveurs TaaS (sur Internet) passe par SSL et est crypté, de sorte que la sécurité et la confidentialité des données ne sont pas compromises.

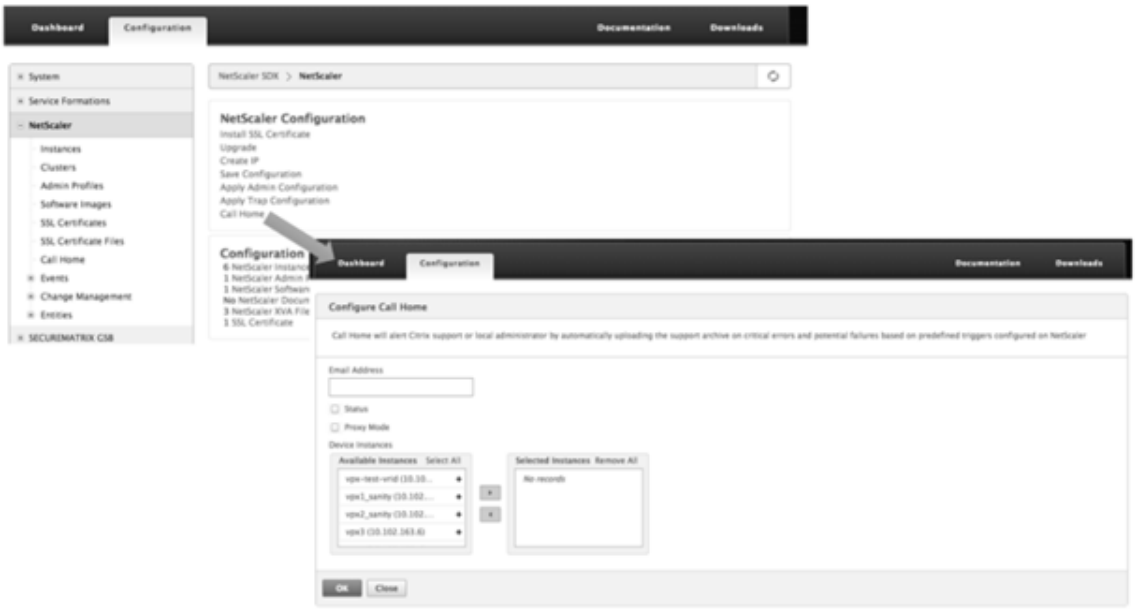
- Pour configurer Call Home sur l'instance Citrix ADC à partir du service de gestion

  Vous pouvez configurer la fonction Call Home sur une seule instance ou sur plusieurs instances en même temps.

  Pour configurer la fonctionnalité Call Home sur une seule instance Citrix ADC, accédez à **Configuration > Citrix ADC > Call Home**, sélectionnez l'instance Citrix ADC, puis cliquez sur le bouton Configurer. Dans la page Configurer l'Call Home, cliquez sur OK.



Pour configurer la fonctionnalité Call Home sur plusieurs instances Citrix ADC, accédez à **Configuration > Citrix ADC**. Dans le volet droit, cliquez sur Call Home. Sur la page Configurer l'Call Home, sélectionnez les instances Citrix ADC dans la section Instances disponibles, spécifiez d'autres détails, puis cliquez sur OK.



– Interrogation des instances Citrix ADC

  Pour interroger la fonctionnalité Call Home à partir de toutes les instances Citrix ADC et afficher l'état actuel, accédez à **Configuration > Citrix ADC > Call Home**, puis cliquez sur **Poll Now**. Sur la page de confirmation, cliquez sur **Oui**.

Surveillance de l'état du

January 27, 2022

La surveillance de l'état du système détecte les erreurs dans les composants surveillés, afin que vous puissiez prendre des mesures correctives pour éviter une défaillance. Les composants suivants sont surveillés sur une appliance Citrix ADC SDX :

- Ressources matérielles et logicielles
- Disques physiques et virtuels
- <Les capteurs matériels, tels que les capteurs de ventilateur, de température, de tension et d'alimentation
- Interfaces

Dans l'onglet **Surveillance**, cliquez sur **Santé du système**. Un résumé de tous les composants s'affiche. Pour afficher les détails des composants surveillés, développez **Santé du système**, puis cliquez sur le composant que vous souhaitez surveiller.

- Surveillance des ressources sur l'appliance SDX

  Vous pouvez surveiller les composants matériels et logiciels de l'appliance SDX et prendre des mesures correctives si nécessaire. Pour afficher les composants surveillés, dans l'onglet Surveillance, développez Santé du système, puis cliquez sur Ressources. Les informations relatives aux ressources matérielles et logicielles s'affichent. Pour tous les composants matériels, les valeurs actuelles et attendues sont affichées. Pour les composants logiciels, à l'exception de la version du microprogramme du contrôleur BMC, les valeurs actuelles et attendues sont affichées comme non applicables (NA).

- **Nom :** nom du composant, tel que le processeur, la mémoire ou la version du microprogramme du contrôleur BMC.

- **État :** État (état) du composant. Pour le
  matériel et pour la version du microprogramme BMC, ERROR indique un écart par rapport à la valeur attendue. Pour les appels à Citrix Hypervisor, ERROR indique que le service de gestion n'est pas en mesure de communiquer avec Citrix Hypervisor à l'aide d'un appel API, HTTP, PING ou SSH. Pour
  le plug-in Health Monitor, ERROR indique que le plug-in n'est pas installé sur Citrix Hypervisor.

- **Valeur actuelle :** valeur actuelle du composant. Dans des conditions normales, la valeur actuelle est la même que la valeur attendue.

- **Valeur attendue :** valeur attendue pour le composant. Ne s'applique pas aux appels logiciels vers Citrix Hypervisor.

Surveillez les ressources de stockage sur l'appliance SDX

Vous pouvez surveiller les disques de l'appliance SDX et prendre des mesures correctives si nécessaire. Pour afficher les composants surveillés, dans l'onglet **Surveillance**, développez **Santé du système**, puis cliquez sur **Stockage**. Les détails s'affichent pour les disques physiques et pour les disques virtuels ou les partitions créés à partir de disques physiques.

Pour les disques (Disk), les détails suivants sont affichés :

- **Nom** Le nom du disque physique.
- **Taille :** taille du disque, en Go.
- **Utilisée :** quantité de données sur le disque, en Go.
- **Transactions/s :** Nombre de blocs en cours de lecture ou d'écriture par seconde. Ce numéro est lu à partir de la `iostat` sortie.
- **Blocks Read/s :** Nombre de blocs lus par seconde. Vous pouvez utiliser cette valeur pour mesurer le taux de sortie du disque.
- **Blocks Written/s :** Nombre de blocs en cours d'écriture par seconde. Vous pouvez utiliser cette valeur pour mesurer le taux d'entrée sur le disque.
- **Nombre total de blocs lus :** nombre de blocs lus depuis le dernier démarrage de l'appliance.
- **Nombre total de blocs écrits :** nombre de blocs écrits depuis le dernier démarrage de l'appliance.

Pour les disques virtuels ou les partitions (référentiel de stockage), les détails suivants sont affichés :

- **Baie de lecteur :** numéro du lecteur dans la baie de lecteur. Vous pouvez trier les données de ce paramètre.
- **État :** État (état) du lecteur dans la baie de lecteur. Valeurs possibles :
  - GOOD : le lecteur est en bon état et est prêt à être utilisé.
  - FAIL : Le lecteur est en panne et doit être remplacé.
  - MISSING : aucun lecteur n'est détecté dans la baie de lecteur.
  - UNKNOWN : un nouveau lecteur non formaté existe dans la baie de lecteur.
- **Nom : Nom** défini par le système du dépôt de stockage.
- **Taille :** taille du référentiel de stockage, en Go.
- **Utilisée :** quantité de données dans le référentiel de stockage, en Go.

Surveillez les capteurs matériels de l'appliance SDX

Vous pouvez surveiller les composants matériels de l'appliance SDX et prendre des mesures correctives si nécessaire. Dans l'onglet **Surveillance**, développez **Santé du système**, puis cliquez sur **Capteurs matériels**. La fonction de surveillance affiche des détails sur la vitesse des différents ventilateurs, la température et la tension des différents composants et l'état de l'alimentation électrique.

Pour la vitesse du ventilateur, les informations suivantes sont affichées :

- **Nom :** Nom du ventilateur.
- **État :** État (état) du ventilateur. ERROR indique un écart par rapport à la valeur attendue. NA indique que le ventilateur n'est pas présent.
- **Valeur actuelle (tr/min) :** Rotations actuelles par minute.

Les informations de température incluent les informations suivantes :

- **Nom :** Nom du composant, tel que CPU ou module de mémoire (par exemple, P1-DIMM1A).
- **État :** État (état) du composant. ERROR indique que la valeur actuelle est hors limites.
- **Valeur actuelle (degré C) :** Température actuelle, en degrés, du composant.

Les informations de tension incluent les informations suivantes :

- **Nom :** Nom du composant, tel que le cœur du processeur.
- **État :** État (état) du composant. ERROR indique que la valeur actuelle est hors limites.
- **Valeur actuelle (volts) :** tensions actuelles présentes sur le composant.

Les informations relatives au bloc d'alimentation incluent les informations suivantes :

- **Nom :** nom du composant.
- **État :** État (état) du composant. Valeurs possibles :
  - **Erreur** : un seul bloc d'alimentation est connecté ou fonctionne.
  - **OK** : les deux blocs d'alimentation sont connectés et fonctionnent comme prévu.

Surveillez les interfaces sur l'appliance SDX

Vous pouvez surveiller les interfaces de l'appliance SDX et prendre des mesures correctives si nécessaire. Dans l'onglet **Surveillance**, développez **Santé du système**, puis cliquez sur **Interfaces**. La fonction de surveillance détaille les informations suivantes concernant chaque interface :

- **Interface :** numéro d'interface sur l'appliance SDX.
- **État :** État de l'interface. Valeurs possibles : UP, DOWN.
- **VfS affectés/total :** nombre de fonctions virtuelles affectées à l'interface et nombre de fonctions virtuelles disponibles sur cette interface. Vous pouvez attribuer jusqu'à sept fonctions virtuelles sur une interface 1G et jusqu'à 40 fonctions virtuelles sur une interface 10G.
- **Paquets Tx :** nombre de paquets transmis depuis le dernier démarrage de l'appliance.
- **Paquet Rx :** nombre de paquets reçus depuis le dernier démarrage de l'appliance.
- **Tx Bytes :** nombre d'octets transmis depuis le dernier démarrage de l'appliance.
- **Octets Rx :** nombre d'octets reçus depuis le dernier démarrage de l'appliance.
- **Erreurs de transmission :**nombre d'erreurs lors de la transmission des données depuis le dernier démarrage de l'appliance.
- **Erreurs Rx :** nombre d'erreurs lors de la réception des données depuis le dernier démarrage de l'appliance.

Configuration des paramètres de notification du système

February 1, 2022

Vous pouvez envoyer des notifications pour communiquer avec certains groupes d'utilisateurs pour un certain nombre de fonctions liées au système. Vous pouvez configurer un serveur de notification dans SDX Management Service pour configurer des serveurs de passerelle de messagerie et de messages courts (SMS) pour envoyer des notifications par e-mail et texte (SMS) aux utilisateurs.

> **Remarque**
>
> Après la mise à niveau vers SDX Management Service version 11.1, la notification système est activée pour toutes les catégories d'événements et les notifications sont envoyées au profil e-mail ou SMS existant.

Pour configurer les paramètres de notification du système

1. Accédez à **Système > Notifications > Paramètres,** puis cliquez sur **Modifier les paramètres de notification.**
2. Sur la page **Configurer les paramètres de notification du système**, entrez les informations suivantes :
   - **Catégorie** — Catégorie ou catégories des événements générés par le service de gestion SDX.
     - Email : sélectionnez une liste de distribution d'e-mails dans le menu déroulant. Vous pouvez également créer une nouvelle liste de distribution d'e-mails en cliquant sur l'icône **+** et en saisissant les détails du nouveau serveur de messagerie dans les champs appropriés.
     - SMS : sélectionnez une liste de distribution de SMS dans le menu déroulant. Vous pouvez également créer une
     nouvelle liste de distribution de SMS en cliquant sur l'icône **+** et en saisissant les nouveaux détails du serveur SMS dans les champs appropriés.
3. Cliquez sur **OK.**

Activer et désactiver les fonctionnalités du service de gestion

January 27, 2022

> **Remarque** :
>
> Cette fonctionnalité est disponible dans la version 13.1 build 12.x et ultérieures.

Sur une appliance Citrix ADC SDX, le service de gestion interroge les instances Citrix ADC en arrière-plan pour des opérations, telles que les certificats SSL, les fonctions réseau et l'audit de configuration. Une option est disponible pour activer ou désactiver ce sondage en fonction de vos besoins. La désactivation de ce sondage améliore les performances du service de gestion et des instances ADC.

Pour activer ou désactiver des fonctionnalités à l'aide de l'interface graphique

1. Accédez à **Système > Paramètres système**.
2. Cliquez sur **Configurer les fonctionnalités**.
3. Sélectionnez une fonctionnalité et cliquez sur **Activer** ou **Désactiver**.

Configurer le service de gestion

January 27, 2022

Le service de gestion vous permet de gérer les sessions des clients et d'effectuer des tâches de configuration, telles que la création et la gestion de comptes d'utilisateurs et l'ajustement des politiques de sauvegarde et d'nettoyage en fonction de vos besoins. Vous pouvez également redémarrer le service de gestion et mettre à niveau la version du service de gestion. Vous pouvez également créer des fichiers tar du service de gestion et de Citrix Hypervisor et les envoyer au support technique.

Gérer les sessions client

Une session client est créée lorsqu'un utilisateur ouvre une session sur le service de gestion. Vous pouvez afficher toutes les sessions client sur l'appliance dans le volet **Sessions** .

Dans le volet **Sessions**, vous pouvez afficher les informations suivantes :

- **Nom d'utilisateur :** compte d'utilisateur utilisé pour la session.
- **Adresse IP :** adresse IP du client à partir duquel la session a été créée.
- **Port :** port utilisé pour la session.
- **Heure de connexion :** heure à laquelle la session en cours a été créée sur l'appliance SDX.
- Heure de la**dernière activité : heure** à laquelle l'activité de l'utilisateur a été détectée pour la dernière fois dans la session.
- La**session expire dans :** temps restant pour l'expiration de la session.

Pour afficher les sessions client, sous l'onglet **Configuration**, accédez à **Système > Sessions**.

Pour mettre fin à une session client, dans le volet **Sessions**, cliquez sur la session que vous souhaitez supprimer, puis sur Mettre **fin à la session**.

Vous ne pouvez pas mettre fin à une session à partir du client qui a initié cette session.

Configurer les stratégies

Pour maintenir la taille des données enregistrées dans des limites gérables, l'appliance SDX exécute automatiquement des stratégies de sauvegarde et de nettoyage des données à un moment donné.

La stratégie de nettoyage s'exécute tous les jours à 00 h 00 et spécifie le nombre de jours de conservation des données sur l'appliance. Par défaut, l'appliance élague les données de plus de 3 jours, mais vous pouvez spécifier le nombre de jours de données que vous souhaitez conserver. Seuls les journaux d'événements, les journaux d'audit et les journaux des tâches sont supprimés.

La stratégie de sauvegarde s'exécute tous les jours à 00 h 30 et crée une sauvegarde des journaux et des fichiers de configuration. Par défaut, la stratégie conserve trois sauvegardes, mais vous pouvez spécifier le nombre de sauvegardes que vous souhaitez conserver. En outre, à l'aide de la stratégie de sauvegarde, vous pouvez :

- Cryptez les fichiers de sauvegarde.
- Configurez l'appliance SDX pour transférer les fichiers de sauvegarde vers un serveur de sauvegarde externe via FTP, SFTP et SCP.

Pour spécifier le nombre de jours pendant lesquels les données enregistrées sont élaguées :

1. Dans l'onglet **Configuration**, dans le volet de navigation, cliquez sur **Système**.
2. Dans le volet **Système**, sous **Administration des politiques**, cliquez sur **Stratégie de nettoyage**.
3. Dans la boîte de dialogue **Modifier la stratégie de nettoyage**, dans **Données à conserver (jours)**, spécifiez le nombre de jours de données que l'appliance doit conserver à un moment donné.
4. Cliquez sur **OK**.

Pour configurer la stratégie de sauvegarde :

1. Dans l'onglet **Configuration**, dans le volet de navigation, cliquez sur **Système**.
2. Dans le volet **Système**, sous **Administration des politiques**, cliquez sur **Stratégie de sauvegarde**.
3. Dans la boîte de dialogue **Modifier la stratégie de sauvegarde**, dans **Sauvegardes précédentes** à conserver, spécifiez le nombre de sauvegardes que l'appliance doit conserver à tout moment.
4. Sélectionnez **Crypter le fichier de sauvegarde** pour chiffrer le fichier de sauvegarde.
5. Sélectionnez **Transfert externe** et procédez comme suit pour transférer le fichier de sauvegarde vers un serveur de sauvegarde externe :
    a) Dans le champ **Serveur**, saisissez le nom d'hôte ou l'adresse IP du serveur de sauvegarde externe.
    b) Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez le nom d'utilisateur et le mot de passe pour accéder au serveur de sauvegarde externe.
    c) Dans le champ **Port**, saisissez le numéro de port.

d) Dans le champ **Protocole de transfert**, sélectionnez le protocole que vous souhaitez utiliser pour transférer le fichier de sauvegarde vers le serveur de sauvegarde externe.
e) Dans le champ **Chemin du répertoire**, saisissez le chemin du répertoire du serveur de sauvegarde externe où vous souhaitez stocker les fichiers de sauvegarde.

6. **Supprimer le fichier du service de gestion après le transfert :** sélectionnez cette option si vous souhaitez supprimer le fichier de sauvegarde de l'appliance SDX après avoir transféré le fichier de sauvegarde vers le serveur de sauvegarde externe.
7. Cliquez sur **OK**.

Redémarrez le service de gestion

Vous pouvez redémarrer le service de gestion à partir du volet **Système** . Le redémarrage du service de gestion n'affecte pas le fonctionnement des instances. Les instances continuent de fonctionner pendant le processus de redémarrage du service de gestion.

Pour redémarrer le service de gestion :

1. Dans l'onglet **Configuration**, dans le volet de navigation, cliquez sur **Système**.
2. Dans le volet **Système**, sous **Administration du système**, cliquez sur **Service de gestion du redémarrage**.

Supprimer les fichiers du service de gestion

Vous pouvez supprimer tous les fichiers de build et de documentation du service de gestion inutiles de l'appliance SDX.

Pour supprimer un fichier de service de gestion :

1. Sous l'onglet **Configuration**, dans le volet de navigation, développez **Service de gestion**, puis cliquez sur le fichier à supprimer.
2. Dans le volet d' **informations**, sélectionnez le nom du fichier, puis cliquez sur **Supprimer**.

Génération d'une archive tar pour le support technique

Vous pouvez utiliser l'option Support technique pour générer une archive tar de données et de statistiques à soumettre au support technique Citrix. Ce tar peut être généré pour le service de gestion ou Citrix Hypervisor, ou pour les deux en même temps. Vous pouvez ensuite télécharger le fichier sur votre système local et l'envoyer au support technique Citrix.

Dans le volet **Support technique**, vous pouvez afficher les détails suivants.

- **Nom :** nom du fichier d'archive tar. Le nom du fichier indique si le tar est destiné au service de gestion ou au serveur Citrix Hypervisor.
- **Dernière modification :** date à laquelle ce fichier a été modifié pour la dernière fois.

- **Taille :** taille du fichier tar.

Pour générer l'archive tar pour le support technique :

1. Dans l'onglet **Configuration**, accédez à **Diagnostics > Support technique**.
2. Dans le volet d' **informations**, dans la liste **Action**, sélectionnez **Générer un fichier de support technique**.
3. Dans la boîte de dialogue **Générer un fichier de support technique**, dans la liste **Mode**, sélectionnez l'option appropriée.
4. Cliquez sur **OK**.

Pour télécharger l'archive tar pour le support technique :

1. Dans le volet **Support technique**, sélectionnez le fichier de support technique que vous souhaitez télécharger.
2. Dans la liste **Action**, sélectionnez **Télécharger**. Le fichier est enregistré sur votre ordinateur local.

Support CLI pour le service de gestion

Vous pouvez désormais utiliser l'interface de ligne de commande pour effectuer des opérations sur le service de gestion. Les opérations suivantes sont prises en charge :

- Ajouter, définir, supprimer : pour configurer les ressources.
- Do : pour effectuer des opérations au niveau du système. Par exemple, mise à niveau ou arrêt du service de gestion, ou redémarrage.
- Enregistrer : pour ajouter des interfaces, qui sont utilisées pour le provisionnement.

Pour accéder à l'interface de ligne de commande, démarrez le client Secure Shell (SSH) à partir de n'importe quel poste de travail connecté à l'adresse IP du service de gestion. Ouvrez une session en utilisant les informations d'identification de l'administrateur.

Vous pouvez accéder à des informations détaillées sur l'utilisation et la syntaxe des commandes à partir des pages de manuel.

Remarque : L'interface de ligne de commande n'est pas prise en charge sur la console d'accès

Configurer les paramètres d'authentification et d'autorisation

January 27, 2022

L'authentification avec le service de gestion Citrix ADC SDX peut être locale ou externe. Avec l'authentification externe, le service de gestion accorde l'accès à l'utilisateur en fonction de la

réponse d'un serveur externe. Le service de gestion prend en charge les protocoles d'authentification externes suivants :

- Service utilisateur de numérotation d'authentification à distance (RADIUS)
- Système de contrôle d'accès au contrôleur d'accès terminal (TACACS)
- LDAP (Lightweight Directory Access Protocol)

Le service de gestion prend également en charge les demandes d'authentification provenant de SSH. L'authentification SSH prend uniquement en charge les demandes d'authentification interactives au clavier. L'autorisation des utilisateurs SSH est limitée aux privilèges d'administrateur uniquement. Les utilisateurs disposant de privilèges en lecture seule ne peuvent pas se connecter via SSH.

Pour configurer l'authentification, spécifiez le type d'authentification et configurez un serveur d'authentification.

L'autorisation via le service de gestion est locale. Le service de gestion prend en charge deux niveaux d'autorisation. Les utilisateurs disposant de privilèges d'administrateur sont autorisés à effectuer n'importe quelle action sur le service de gestion. Les utilisateurs disposant de privilèges en lecture seule sont autorisés à effectuer uniquement des opérations de lecture. L'autorisation des utilisateurs SSH est limitée aux privilèges d'administrateur uniquement. Les utilisateurs disposant de privilèges en lecture seule ne peuvent pas se connecter via SSH.

L'autorisation pour RADIUS et LDAP est prise en charge par l'extraction de groupe. Vous pouvez définir les attributs d'extraction de groupe lors de la configuration des serveurs RADIUS ou LDAP sur le service de gestion. Le nom de groupe extrait est mis en correspondance avec les noms de groupe sur le service de gestion afin de déterminer les privilèges accordés à l'utilisateur. Un utilisateur peut appartenir à plusieurs groupes. Dans ce cas, si un groupe auquel l'utilisateur appartient possède des privilèges d'administrateur, l'utilisateur dispose de privilèges d'administrateur. Un attribut de groupe d'authentification par défaut peut être défini lors de la configuration. Ce groupe est pris en compte avec les groupes extraits pour autorisation.

Dans l'autorisation TACACS, l'administrateur du serveur TACACS doit autoriser une commande spéciale, admin pour un utilisateur ayant des privilèges d'administrateur et refuser cette commande pour les utilisateurs disposant de privilèges en lecture seule. Lorsqu'un utilisateur ouvre une session sur un dispositif SDX, le service de gestion vérifie si l'utilisateur est autorisé à exécuter cette commande. Si l'utilisateur dispose d'une autorisation, l'utilisateur se voit attribuer les privilèges d'administrateur, sinon l'utilisateur se voit attribuer des privilèges en lecture seule.

Ajouter un groupe d'utilisateurs

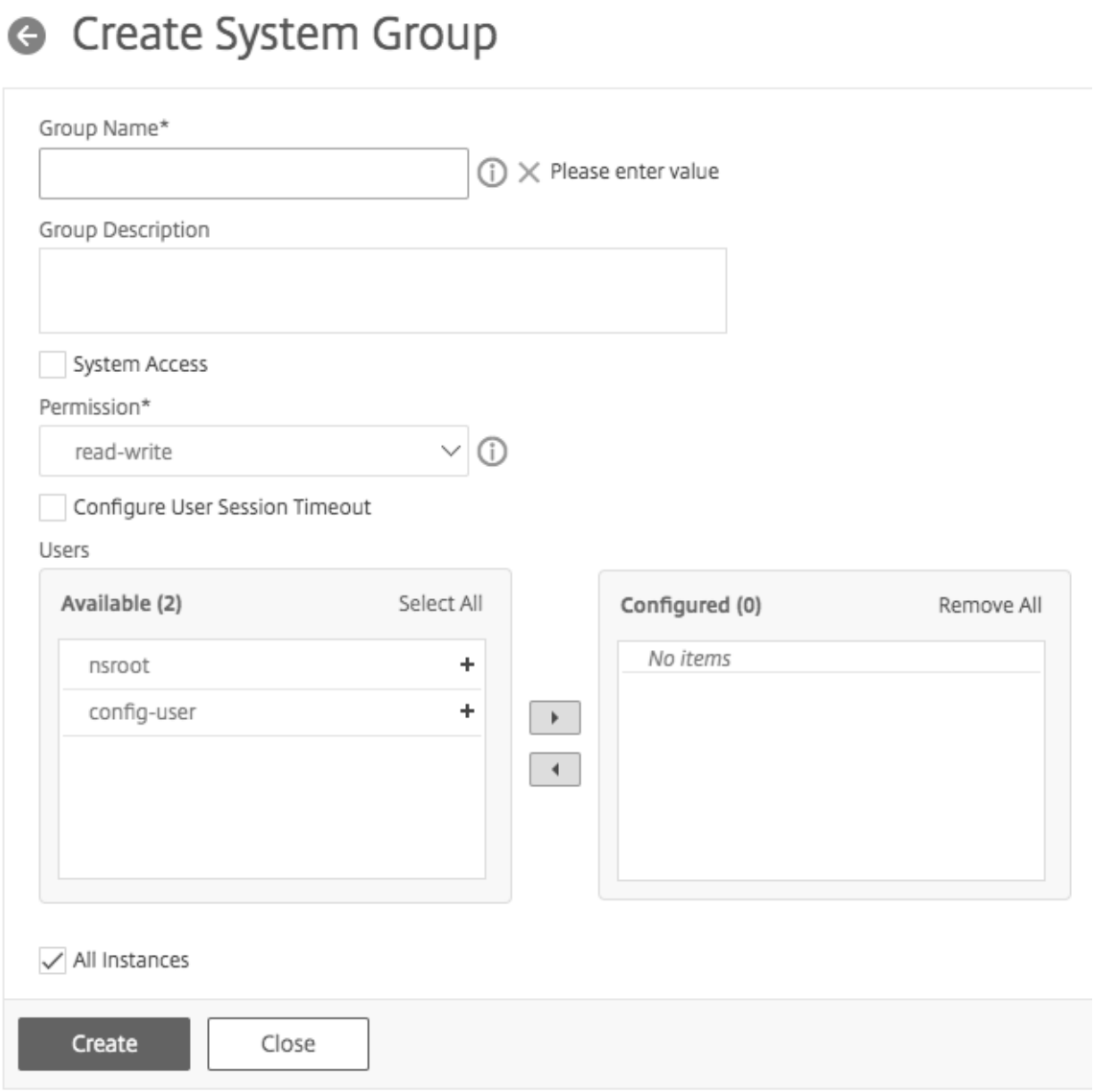
Les groupes sont des ensembles logiques d'utilisateurs qui ont besoin d'accéder à des informations communes ou d'effectuer des tâches similaires. Vous pouvez organiser les utilisateurs en groupes définis par un ensemble d'opérations courantes. En accordant des autorisations spécifiques à des

groupes plutôt qu'à des utilisateurs individuels, vous pouvez gagner du temps lors de la création d'utilisateurs.

Si vous utilisez des serveurs d'authentification externes pour l'authentification, les groupes dans SDX peuvent être configurés pour correspondre aux groupes configurés sur les serveurs d'authentification. Lorsqu'un utilisateur appartenant à un groupe dont le nom correspond à un groupe sur un serveur d'authentification, ouvre une session et est authentifié, l'utilisateur hérite des paramètres du groupe.

Pour ajouter un groupe d'utilisateurs

1. Dans l'onglet **Configuration**, sous **Système**, développez **Administration des utilisateurs**, puis cliquez sur **Groupes**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.



3. Sur la page **Créer un groupe de systèmes**, définissez les paramètres suivants :
    - Nom du groupe
    - Description du groupe
    - Accès au système : Cochez cette case pour donner accès à l'ensemble de l'appliance SDX et aux instances qui s'y exécutent. Vous pouvez également spécifier les instances sous Instances pour l'accès au niveau de l' **instance**.
    - Autorisation
    - Configurer le délai d'expiration de session utilisateur
    - Utilisateurs : utilisateurs de la base de données appartenant au groupe. Sélectionnez les utilisateurs que vous souhaitez ajouter au groupe.
4. Cliquez sur **Créer** et **Fermer**.

Remarque : Pour créer un groupe avec un rôle d'administrateur sur une appliance SDX mise à niveau de la version 10.5 vers la version 11.1, activez l'autorisation « lecture-écriture » et la case à cocher « Accès au système ». Dans SDX 10.5, cette case à cocher n'est pas disponible et les valeurs de l'autorisation sont « admin » et « lecture seule ».

Configurer les comptes utilisateur

Un utilisateur ouvre une session sur l'appliance SDX pour effectuer des tâches de gestion de l'appliance. Pour autoriser un utilisateur à accéder à l'appliance, vous devez créer un compte utilisateur sur l'appliance SDX pour cet utilisateur. Les utilisateurs sont authentifiés localement, sur l'appliance.

Important : Le mot de passe s'applique à l'appliance
SDX, au service de gestion et à Citrix Hypervisor. Ne modifiez pas le mot de passe directement sur Citrix Hypervisor.

Pour configurer un compte utilisateur

1. Dans l'onglet **Configuration**, sous **Système**, développez **Administration**, puis cliquez sur **Utilisateurs**. Le volet Utilisateurs affiche une liste des comptes d'utilisateurs existants, avec leurs autorisations.
2. Dans le volet **Utilisateurs**, effectuez l'une des opérations suivantes :
    - Pour créer un compte utilisateur, cliquez sur **Ajouter**.
    - Pour modifier un compte d'utilisateur, sélectionnez-le, puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Créer un utilisateur systèmeou Modifier un utilisateur système**, définissez les paramètres suivants :

- Nom* : nom d'utilisateur du compte. Les caractères suivants sont autorisés dans le nom : les lettres de a à z et de A à Z, les chiffres de 0 à 9, le point (.), l'espace et le trait de soulignement (_). Longueur maximale : 128. Vous ne pouvez pas modifier le nom.
- Mot de passe* : mot de passe pour la connexion à l'appliance. Longueur maximale : 128
- Confirmer le mot de passe* : le mot
- Permission* : les privilèges de l'utilisateur sur l'appliance. Valeurs possibles :
  - ADMIN : l'utilisateur peut effectuer toutes les tâches d'administration liées au service de gestion.
  - Lecture seule : l'utilisateur peut uniquement surveiller le système et modifier le mot de passe du compte.
    Par défaut : admin.
- Activer l'authentification externe : active l'authentification externe pour cet utilisateur. Le service de gestion tente une authentification externe avant l'authentification des utilisateurs de la base Si ce paramètre est désactivé, l'utilisateur n'est pas authentifié auprès du serveur d'authentification externe.
  Remarque : Si le serveur d'authentification distant n'est pas accessible, l'utilisateur risque de perdre l'accès à l'appliance. Dans ce cas, l'authentification revient à l'utilisateur admin par défaut (`nsroot`).
- Configurer le délai d'expiration de session : vous permet de configurer la période pendant laquelle un utilisateur peut rester actif. Spécifiez les détails suivants :
  - Délai d'expiration de session : la période pendant laquelle une session utilisateur peut rester active.
  - Session Timeout Unit : unité de délai d'expiration, en minutes ou en heures.
- Groupes : affectez les groupes à l'utilisateur.

*Paramètre obligatoire

4. Cliquez sur Créer ou sur OK, puis cliquez sur Fermer. L'utilisateur que vous avez créé est répertorié dans le volet Utilisateurs.

Pour supprimer un compte utilisateur

1. Sous l'onglet **Configuration**, dans le volet de navigation, développez **Système**, développez **Administration**, puis cliquez sur **Utilisateurs**.
2. Dans le volet **Utilisateurs**, sélectionnez le compte d'utilisateur, puis cliquez sur **Supprimer**.
3. Dans la zone de message Confirmer, cliquez sur **OK**.

Définition du type d'authentification

Dans l'interface du service de gestion, vous pouvez spécifier une authentification locale ou externe. L'authentification externe est désactivée par défaut pour les utilisateurs locaux. Il peut être activé en

cochant l'option
Activer l'authentification externe lors de l'ajout de l'utilisateur local ou de la modification des paramètres de l'utilisateur.

Important : L'authentification externe n'est prise en charge qu'après avoir configuré un serveur d'authentification RADIUS, LDAP ou TACACS.

Pour définir le type d'authentification

1. Dans l'onglet Configuration, sous Système, cliquez sur Authentification.
2. Dans le volet d'informations, cliquez sur Configuration de l'authentification.
3. Définissez les paramètres suivants :
   - Type de serveur : type de serveur d'authentification configuré pour l'authentification des utilisateurs. Valeurs possibles : LDAP, RADIUS, TACACS et Local.
   - Nom du serveur : nom du serveur d'authentification configuré dans le service de gestion. Le menu répertorie tous les serveurs configurés pour le type d'authentification sélectionné.
   - Activer l'authentification locale de secours : vous pouvez également choisir d'authentifier un utilisateur avec l'authentification locale en cas d'échec de l'authentification externe. Cette option est activée par défaut.
4. Cliquez sur OK.

Activer ou désactiver l'authentification de base

Vous pouvez vous authentifier auprès de l'interface NITRO du service de gestion en utilisant l'authentification de base. Par défaut, l'authentification de base est activée dans l'appliance SDX. Pour désactiver l'authentification de base à l'aide de l'interface du service de gestion, procédez comme suit

Pour désactiver l'authentification de base

1. Dans l'onglet **Configuration**, cliquez sur **Système**.
2. Dans le groupe **Paramètres système**, cliquez sur **Modifier les paramètres système**.
3. Dans la boîte de dialogue Configurer les paramètres du système, désactivez la case à cocher **Autoriser l'authentification de base** .
4. Cliquez sur **OK**.

Configuration du serveur d'authentification externe

April 8, 2022

Le service de gestion Citrix ADC SDX peut authentifier les utilisateurs avec des comptes d'utilisateurs locaux ou à l'aide d'un serveur d'authentification externe. L'appliance prend en charge les types d'authentification suivants :

- Local : s'authentifie auprès du service de gestion à l'aide d'un mot de passe, sans référence à un serveur d'authentification externe. Les données utilisateur sont stockées localement sur le service de gestion.
- RADIUS : authentifie auprès d'un serveur d'authentification RADIUS externe.
- LDAP : authentifie auprès d'un serveur d'authentification LDAP externe.
- TACACS : authentifie auprès d'un serveur d'authentification externe du système de contrôle d'accès du contrôleur d'accès au terminal (TACACS).

Pour configurer une authentification externe, spécifiez le type d'authentification et configurez un serveur d'authentification.

Ajout d'un serveur RADIUS

Pour configurer l'authentification RADIUS, spécifiez le type d'authentification RADIUS et configurez le serveur d'authentification RADIUS.

Le service de gestion prend en charge l'authentification par réponse de défi RADIUS conformément aux spécifications RADIUS Les utilisateurs RADIUS peuvent être configurés avec un mot de passe à usage unique sur le serveur RADIUS. Lorsque l'utilisateur ouvre une session sur un dispositif SDX, l'utilisateur est invité à spécifier ce mot de passe à usage unique.

Pour ajouter un serveur RADIUS

1. Dans l'onglet **Configuration**, sous **Système**, développez **Authentification**, puis cliquez sur **Radius**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer un serveur Radius**, tapez ou sélectionnez les valeurs des paramètres :
    - Nom* : nom du serveur.
    - Nom du serveur/adresse IP* : nom de domaine complet (FQDN) ou adresse IP du serveur. **Remarque** : Le DNS doit être en mesure de résoudre le nom de domaine complet spécifié en une adresse IP, et seul le DNS principal est utilisé pour résoudre le nom de domaine complet. Pour définir manuellement le DNS principal, reportez-vous à la section « Ajout d'un DNS principal pour la résolution de nom de domaine complet ».

- **Port*** : port sur lequel le serveur RADIUS est en cours d'exécution. Valeur par défaut : 1812.
- Timeout* : nombre de secondes pendant lesquelles le système attend une réponse du serveur RADIUS. Valeur par défaut : 3.
- Clé secrète* : clé partagée entre le client et le serveur. Ces informations sont requises pour la communication entre le système et le serveur RADIUS.
- Activer l'extraction d'adresse IP du NAS : si cette option est activée, l'adresse IP du service de gestion est envoyée `nasip` au serveur conformément au protocole RADIUS.
- NASID : si elle est configurée, cette chaîne est envoyée au serveur RADIUS `nasid` conformément au protocole RADIUS.
- Préfixe de groupe : chaîne de préfixe qui précède les noms de groupe au sein d'un attribut RADIUS pour l'extraction de groupes RADIUS.
- ID de fournisseur de groupe : ID de fournisseur pour utiliser l'extraction de groupe RADIUS.
- Type d'attribut de groupe : type d'attribut pour l'extraction de groupe RADIUS.
- Séparateur de groupe : chaîne de séparateur de groupe qui délimite les noms de groupe dans un attribut RADIUS pour l'extraction de groupes RADIUS.
- Identificateur de fournisseur d'adresse IP : ID fournisseur de l'attribut dans le RADIUS qui indique l'adresse IP intranet. La valeur 0 indique que l'attribut n'est pas codé par le fournisseur.
- Type d'attribut d'adresse IP : type d'attribut de l'attribut d'adresse IP distante dans une réponse RADIUS.
- Identificateur de fournisseur de mot de passe : ID fournisseur du mot de passe dans la réponse RADIUS. Permet d'extraire le mot de passe utilisateur.
- Type d'attribut de mot de passe : type d'attribut de l'attribut mot de passe dans une réponse RADIUS.
- Encodage du mot de passe : comment les mots de passe doivent être codés dans les paquets RADIUS transmis du système au serveur RADIUS. Valeurs possibles : pap, chap, mschapv1 et mschapv2.
- Groupe d'authentification par défaut : groupe par défaut choisi lorsque l'authentification réussit, en plus des groupes extraits.
- Comptabilité : permet au service de gestion de consigner les informations d'audit avec le serveur RADIUS.

4. Cliquez sur Créer, puis sur Fermer.

Ajout d'un serveur d'authentification LDAP

Pour configurer l'authentification LDAP, spécifiez le type d'authentification LDAP et configurez le serveur d'authentification LDAP.

Pour ajouter un serveur LDAP

1. Dans l'onglet **Configuration**, sous **Système**, développez **Authentification**, puis cliquez sur **LDAP**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Créer un serveur LDAP, tapez ou sélectionnez les valeurs des paramètres :
   - Nom* : nom du serveur.
   - Nom du serveur/adresse IP* : nom de domaine complet ou adresse IP du serveur.
     Remarque : Le DNS doit être en mesure de résoudre le nom de domaine complet spécifié en une adresse IP, et seul le DNS principal est utilisé pour résoudre le nom de domaine complet.Pour définir manuellement le DNS principal, reportez-vous à la section « Ajout d'un DNS principal pour la résolution de nom de domaine complet ».
   - **Port*** : port sur lequel le serveur LDAP est en cours d'exécution. Valeur par défaut : 389.
   - Timeout* : nombre de secondes pendant lesquelles le système attend une réponse du serveur LDAP.
   - DN de base : base ou nœud sur lequel la recherche LDAP doit commencer.
   - Type : type de serveur LDAP. Valeurs possibles : Active Directory (AD) et Novell Directory Service (NDS).
   - DN de liaison administrative : nom unique complet utilisé pour la liaison au serveur LDAP.
   - Mot de passe administratif : mot de passe utilisé pour la liaison au serveur LDAP.
   - Valider le certificat LDAP : cochez cette option pour valider le certificat reçu du serveur LDAP.
   - Nom d'hôte LDAP : nom d'hôte du serveur LDAP. Si le paramètre ValidateServerCert est activé, ce paramètre spécifie le nom d'hôte sur le certificat du serveur LDAP. Une incompatibilité de nom d'hôte entraîne un échec de connexion.
   - Attribut de nom d'ouverture de session du serveur—Attribut de nom utilisé par le système pour interroger le serveur LDAP externe ou un Active Directory.
   - Filtre de recherche : chaîne à combiner avec la chaîne de recherche utilisateur LDAP par défaut pour former la valeur. Par exemple, vpnallowed=true avec ldaploginame `samaccount` et le nom d'utilisateur fourni par l'utilisateur bob donnerait une chaîne de recherche LDAP de : (& (vpnallowed=true) (samaccount=bob).
   - Attribut de groupe : nom d'attribut pour l'extraction de groupe à partir du serveur LDAP.
   - Nom du sous-attribut : nom du sous-attribut pour l'extraction de groupe à partir du serveur LDAP.
   - Type de sécurité : type de cryptage pour la communication entre l'appliance et le serveur d'authentification. Valeurs possibles :
     PLAINTEXT : aucun cryptage n'est requis.
     TLS : communiquez à l'aide du protocole TLS.
     SSL : communiquer à l'aide du protocole SSL

- Groupe d'authentification par défaut : groupe par défaut choisi lorsque l'authentification réussit, en plus des groupes extraits.
- Références : permet de suivre les références LDAP reçues du serveur LDAP.
- Nombre maximum de références LDAP : nombre maximum de références LDAP à suivre.
- Activer le changement de mot de passe : autorise l'utilisateur à modifier le mot de passe si le mot de passe expire. Vous pouvez modifier le mot de passe uniquement lorsque le type de sécurité configuré est TLS ou SSL.
- Activer l'extraction de groupes imbriqués : permet d'activer la fonction d'extraction de groupes imbriqués.
- Niveau d'imbrication maximal : nombre de niveaux auxquels l'extraction de groupe est autorisée.
- Identificateur de nom de groupe : nom qui identifie de manière unique un groupe sur le serveur LDAP.
- Attribut de recherche de groupe : attribut de recherche de groupe LDAP. Permet de déterminer les groupes auxquels appartient un groupe.
- Sous-attribut de recherche de groupe : sous-attribut de recherche de groupe LDAP. Permet de déterminer les groupes auxquels appartient un groupe.
- Filtre de recherche de groupe : chaîne à combiner avec la chaîne de recherche de groupe LDAP par défaut pour former la valeur de recherche.

4. Cliquez sur Créer, puis sur Fermer.

Support de l'authentification par clé publique SSH pour les utilisateurs LDAP

L'appliance SDX peut désormais authentifier les utilisateurs LDAP via l'authentification par clé publique SSH pour l'ouverture de session. La liste des clés publiques est stockée sur l'objet utilisateur du serveur LDAP. Lors de l'authentification, SSH extrait les clés publiques SSH du serveur LDAP. L'ouverture de session réussit si l'une des clés publiques récupérées prend en charge SSH.

Le même nom d'attribut de la clé publique extraite doit être présent à la fois sur le serveur LDAP et dans l'appliance Citrix ADC SDX.

> **Important**
>
> Pour l'authentification basée sur les clés, vous devez spécifier un emplacement des clés publiques en définissant la valeur de `Authorizedkeysfile` dans le `/etc/sshd_config` fichier dans l'aspect suivant :
>
> `AuthorizedKeysFile .ssh/authorized_keys`

Utilisateur du système. Vous pouvez spécifier l'emplacement des clés publiques pour n'importe quel utilisateur du système en définissant la valeur de `Authorizedkeysfile` dans le `/etc/sshd_config`fichier* '.

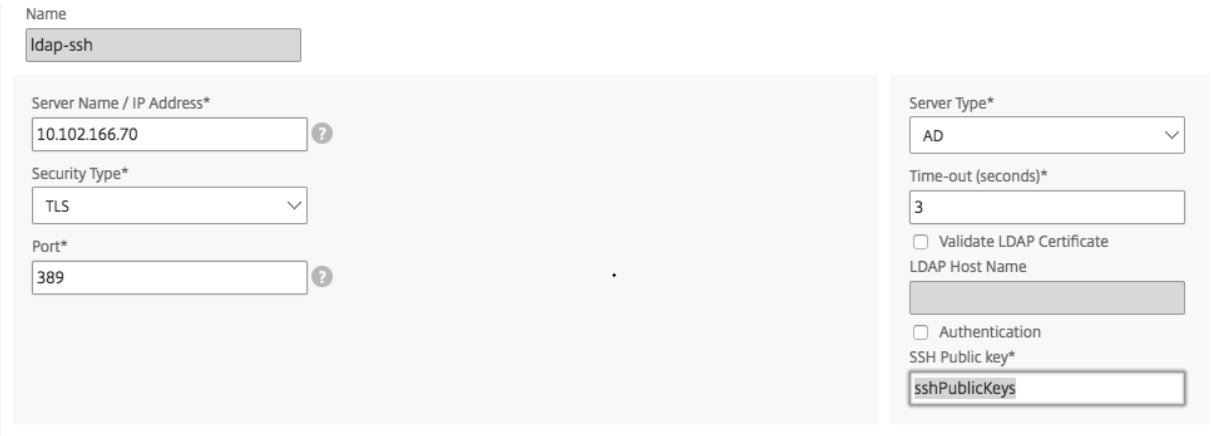
Utilisateurs LDAP. La clé publique récupérée est stockée dans le `/var/pubkey/<user_name>/tmp_authorized_keys-<pid>` répertoire. Le `pid` est le numéro unique ajouté pour différencier les demandes SSH simultanées du même utilisateur. Cet emplacement est un emplacement temporaire où se trouve la clé publique pendant le processus d'authentification. La clé publique est supprimée du système une fois l'authentification terminée.

Pour vous connecter avec l'utilisateur, exécutez la commande suivante à partir de l'invite du shell :

```
$ ssh -i <private key> <username>@<IPAddress>
```

Pour configurer le serveur LDAP à l'aide de l'interface graphique :

1. Accédez à **Système > Authentification > LDAP**.
2. Sur la page LDAP, cliquez sur l'onglet ****Serveurs**** .
3. Cliquez sur l'un des serveurs LDAP disponibles.
4. Sur la page **Configurer le serveur LDAP d'** authentification, sélectionnez **Authentification**.



> **Remarque :**
>
> Désactivez la case à cocher Authentification pour utiliser « sshPublicKeys » pour l'authentification des utilisateurs LDAP.

Ajout d'un DNS principal pour la résolution de nom de domaine complet

Si vous définissez un serveur RADIUS ou LDAP à l'aide du nom de domaine complet du serveur au lieu de son adresse IP, définissez manuellement le DNS principal pour résoudre le nom du serveur. Vous pouvez utiliser l'interface graphique ou l'interface de ligne de commande.

Pour définir le DNS principal à l'aide de l'interface graphique, accédez à **Système > Configuration réseau > DNS**.

Pour définir le DNS principal à l'aide de l'interface de ligne de commande, procédez comme suit.

1. Ouvrez une console Secure Shell (SSH).

2. Ouvrez une session sur l'appliance Citrix ADC SDX à l'aide des informations d'identification de l'administrateur.
3. Exécutez la commande `networkconfig`.
4. Sélectionnez le menu approprié et mettez à jour l'adresse IPv4 DNS, puis enregistrez les modifications.

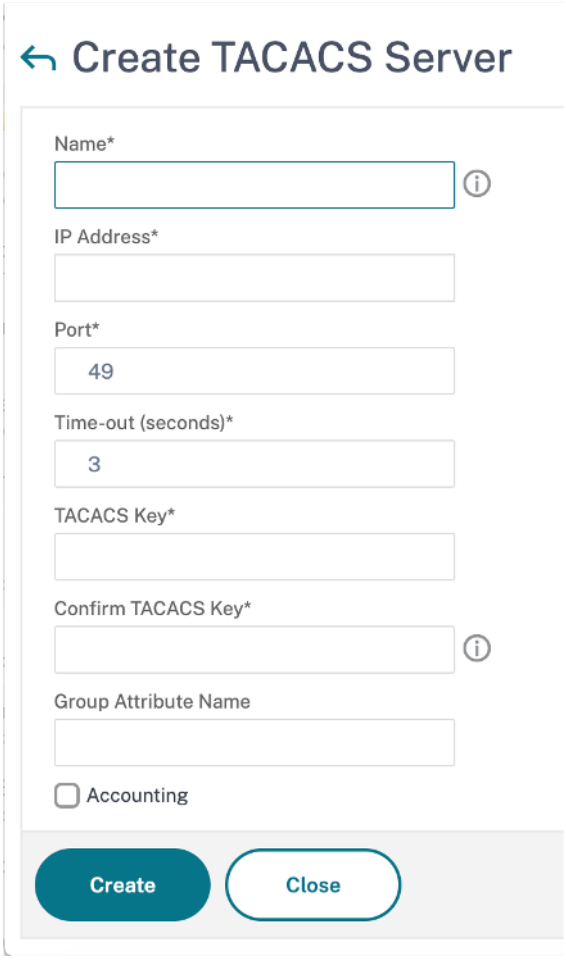
Si vous exécutez à nouveau la commande `networkconfig`, l'adresse DNS mise à jour s'affiche.

Ajouter un serveur TACACS

Pour configurer l'authentification TACACS, spécifiez le type d'authentification TACACS, puis configurez le serveur d'authentification TACACS.

Pour ajouter un serveur TACACS

1. Dans l'onglet **Configuration**, sous **Système**, développez **Authentification**, puis cliquez sur **TACACS**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Créer un serveur TACACS, tapez ou sélectionnez les valeurs des paramètres :
   - Nom : nom du serveur TACAS
   - Adresse IP : adresse IP du serveur TACACS
   - Port : port sur lequel le serveur TACACS est en cours d'exécution. Valeur par défaut : 49
   - Time-out : nombre maximal de secondes pendant lequel le système attend une réponse du serveur TACACS
   - Clé TACACS : clé partagée entre le client et le serveur. Ces informations sont nécessaires pour que le système puisse communiquer avec le serveur TACACS.
   - Comptabilité : permet au service de gestion de consigner les informations d'audit avec le serveur TACACAS
   - Nom de l'attribut de groupe : nom de l'attribut de groupe configuré sur le serveur TACACS+



4. Cliquez sur **Créer**, puis sur **Fermer**.

Configurer l'agrégation de liens depuis le service de gestion

January 27, 2022

L'agrégation de liens combine plusieurs liaisons Ethernet en une seule liaison haut débit. La configuration de l'agrégation de liens augmente la capacité et la disponibilité du canal de communication entre l'appliance Citrix ADC SDX et les autres appareils connectés. Un lien agrégé est également appelé « canal ».

Lorsqu'une interface réseau est liée à un canal, les paramètres de canal ont priorité sur les paramètres d'interface réseau. (En d'autres termes, les paramètres de l'interface réseau sont ignorés.) Une interface réseau ne peut être liée qu'à un seul canal.

Lorsqu'une interface réseau est liée à un canal, elle abandonne sa configuration VLAN. L'interface est supprimée du VLAN auquel elle appartenait à l'origine et ajoutée au VLAN par défaut. Toutefois, vous

pouvez lier le canal à l'ancien VLAN ou à un nouveau. Par exemple, si vous liez les interfaces réseau 1/2 et 1/3 à un VLAN avec l'ID 2 (VLAN 2), puis que vous les liez au canal LA/1, les interfaces réseau sont déplacées vers le VLAN par défaut, mais vous pouvez lier le canal au VLAN 2.

Remarque :

- Une interface doit faire partie d'un seul canal.
- Au moins deux interfaces sont nécessaires pour configurer un canal.
- Les interfaces qui font partie d'un canal ne sont pas répertoriées dans la vue Paramètres réseau lorsque vous ajoutez ou modifiez une instance Citrix ADC. Au lieu des interfaces, les canaux sont répertoriés.

Si vous configurez un canal à l'aide de trois interfaces attribuées à une instance et qu'une deuxième instance utilise certaines de ces interfaces, le service de gestion arrête la deuxième instance, modifie les paramètres réseau et redémarre l'instance. Par exemple, supposons deux instances, Instance1 et Instance2. Lorsque ces instances sont provisionnées, les interfaces 10/1, 10/2 et 10/3 sont attribuées à Instance1, et les interfaces 10/1 et 10/2 sont affectées à Instance2. Si un canal LA est créé avec les interfaces 10/1, 10/2 et 10/3, l'instance1 n'est pas redémarrée. Toutefois, le service de gestion arrête Instance2, attribue l'interface 10/3 à Instance2, puis redémarre Instance2.

Si vous supprimez une interface d'un canal LA, les modifications sont stockées dans la base de données et l'interface apparaît dans la vue Paramètres réseau lorsque vous ajoutez ou modifiez une instance. Avant de supprimer l'interface, seul le canal dont elle fait partie est répertorié.

Configuration d'un canal à partir du service de gestion

January 27, 2022

Vous pouvez configurer un canal manuellement ou utiliser le protocole LACP (Link Aggregation Control Protocol). Vous ne pouvez pas appliquer LACP à un canal configuré manuellement, ni configurer manuellement un canal créé par LACP. Configurez un canal à partir du service de gestion. Sélectionnez ensuite le canal au moment du provisionnement ou de la modification d'une instance Citrix ADC.

Un canal LA est une entité logique permettant la redondance des liaisons et l'agrégation de la bande passante. Les interfaces qui font partie d'un canal ne peuvent pas se voir attribuer d'adresses IP distinctes.

Remarque : Une appliance Citrix ADC SDX prend en charge l'agrégation de liens mais ne prend pas en charge la redondance des liens.

Pour configurer un canal à partir du service de gestion

1. Accédez à **Système > Canaux**.

2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter un canal**, définissez les paramètres suivants :
    - Channel ID : ID du canal LA à créer. Spécifiez un canal LA en notation LA/x, où x peut aller de 1 à un nombre égal à la moitié du nombre d'interfaces. Ne peut pas être modifié après la création du canal LA.
    - Type : type de canal. Valeurs possibles :
        - Statique : configuré uniquement sur les interfaces de données.
        - Actif-actif : configuré uniquement sur les interfaces de gestion 0/x.
        - Actif-passif : configuré uniquement sur les interfaces de gestion 0/x.
        - LACP : configuré sur les interfaces de données et les interfaces de gestion 0/x.
    - Débit (s'applique uniquement à un canal statique et LACP) : valeur seuil faible pour le débit du canal LA, en Mbit/s. Dans une configuration HA, le basculement est déclenché si le canal LA a HA MON activé et que le débit est inférieur au seuil spécifié.
    - Bande passante élevée (s'applique uniquement à un canal statique et à un LACP) : valeur de seuil élevée pour l'utilisation de la bande passante du canal LA, en Mbit/s. L'appliance génère un message d'interruption SNMP lorsque l'utilisation de la bande passante du canal LA est égale ou supérieure à la valeur seuil élevée spécifiée.
    - Bande passante normale (s'applique uniquement à un canal statique et LACP) : valeur de seuil normale pour l'utilisation de la bande passante du canal LA, en Mbit/s. Lorsque l'utilisation de la bande passante du canal LA devient égale ou inférieure au seuil normal spécifié après avoir dépassé le seuil élevé, l'appliance Citrix ADC SDX génère un message d'interruption SNMP pour indiquer que l'utilisation de la bande passante est revenue à la normale.
4. Dans l'onglet **Interfaces**, ajoutez les interfaces que vous souhaitez inclure dans ce canal.
5. Dans l'onglet **Paramètres**, définissez les paramètres suivants :
    - État du canal (s'applique uniquement à un canal statique) : active ou désactive le canal LA.
    - Heure LACP (s'applique uniquement au LACP) : temps après lequel un lien n'est pas agrégé s'il ne reçoit pas de LACPDU. La valeur doit correspondre sur tous les ports participant à l'agrégation de liens sur l'appliance SDX et le nœud partenaire.
    - Surveillance HA : dans une configuration haute disponibilité (HA), surveillez le canal pour détecter les événements de défaillance. La défaillance d'un canal LA sur lequel HA MON est activé déclenche le basculement HA.
    - Tout étiqueter : ajoutez une balise 802.1q de quatre octets à chaque paquet envoyé sur ce canal. Le paramètre ON applique des balises pour tous les VLAN liés à ce canal. OFF applique la balise à tous les VLAN autres que le VLAN natif.
    - Nom d'alias : nom d'alias pour le canal LA. Utilisé uniquement pour améliorer la lisibilité. Pour effectuer toutes les opérations, vous devez spécifier l'ID du canal LA.
6. Cliquez sur **Créer**, puis sur **Fermer**.

> **Remarques**
>
> - Vous ne pouvez pas créer de LA de gestion si les interfaces 0/1 et 0/2 font partie d'une instance VPX et que cette instance fait partie d'un cluster.
> - Vous ne pouvez pas supprimer un LA de gestion s'il fait partie d'une instance VPX et si cette instance fait partie d'un cluster.

Listes de contrôle d'accès

April 8, 2022

Une liste de contrôle d'accès (ACL) est un ensemble de conditions que vous pouvez appliquer à une appliance réseau pour filtrer le trafic IP et protéger votre appliance contre les accès non autorisés.

Vous pouvez configurer une liste de contrôle d'accès sur l'interface graphique de votre service de gestion Citrix ADC SDX pour limiter et contrôler l'accès à l'appliance.

> **Remarque :**
>
> Les listes de contrôle d'accès sur les appliances SDX sont prises en charge à partir de la version 12.0 57.19.

Cette rubrique comprend les sections suivantes :

- Directives d'utilisation
- Comment configurer les ACL
- Autres actions pour les règles ACL
- Résolution des problèmes

Directives d'utilisation

Gardez à l'esprit les points suivants lorsque vous créez des listes de contrôle d'accès sur votre appliance :

- Lorsque vous mettez à niveau l'appliance SDX vers la version 11.0 57.19, la fonctionnalité ACL est désactivée par défaut.
- Les administrateurs SDX peuvent contrôler uniquement les paquets entrants via l'ACL sur l'appliance SDX.
- Si vous utilisez Citrix Application Delivery Management pour gérer votre appliance SDX, vous devez créer des règles ACL appropriées pour autoriser la communication entre MAS et le service de gestion SDX.
- Toutes les autres configurations sur l'appliance SDX, telles que le provisionnement ou la suppression de VPX, l'ajout/la suppression de serveurs externes, la gestion SNMP, ne nécessitent

aucune modification de la configuration ACL existante. La communication avec ces entités est prise en charge par le service de gestion.

Comment configurer une liste de contrôle d'accès

La configuration d'une ACL implique les étapes suivantes :

- Activer la fonctionnalité ACL
- Création d'une règle ACL
- Activer la règle ACL

> **Remarque :**
>
> Vous pouvez créer des règles ACL sans activer la fonctionnalité ACL. Toutefois, si la fonctionnalité n'est pas activée, vous ne pouvez pas activer une règle ACL après l'avoir créée.

Activer la fonctionnalité ACL

1. Pour activer la fonctionnalité ACL, connectez-vous à l'interface graphique du service de gestion SDX et accédez à **Configuration > Système > ACL**.
2. En utilisant le bouton bascule, activez la fonction ACL.

Création d'une règle ACL

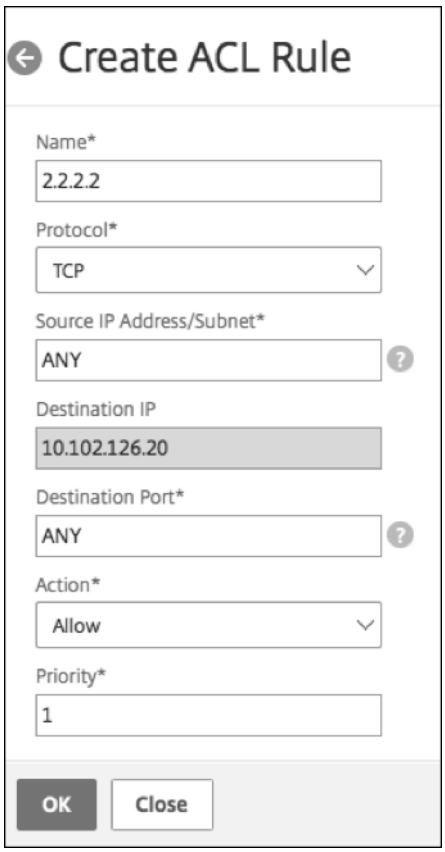
1. Sur la page ACL, cliquez sur **Créer une règle**.
2. La fenêtre **Créer une règle** s'ouvre. Ajoutez les détails répertoriés dans le tableau suivant.

Propriété	Description
Nom	Ajoutez un nom.
Protocole	Sélectionnez un protocole dans le menu. Par défaut, TCP est sélectionné. Vous pouvez sélectionner **N'IMPORTE QUEL** pour autoriser tous les protocoles.

Propriété	Description
Adresse IP source/sous-réseau	Spécifiez l'adresse IP ou le sous-réseau source auquel la règle s'applique. Sélectionnez **ANY** si la règle doit être appliquée à tout le trafic entrant.
IP destination	L'adresse IP du service de gestion SDX est renseignée automatiquement en tant qu'adresse IP de destination. Ce champ ne peut pas être édité.
Port de destination	Spécifiez le port de destination auquel la règle s'applique. Sélectionnez **N'IMPORTE QUEL** si la règle s'applique à tous les ports de destination.
Action	Sélectionnez l'action de la règle, qui est Autoriser ou Refuser.
Priority	Attribuez une priorité pour spécifier l'ordre dans lequel la règle doit être évaluée. Les numéros de priorité déterminent l'ordre dans lequel les règles ACL sont mises en correspondance avec un paquet entrant. Un numéro de priorité inférieure a une priorité plus élevée. Par exemple, la priorité numéro 1 a une priorité supérieure à la priorité numéro 1. Si aucune des règles ne correspond au paquet entrant, le paquet est bloqué.

3. Cliquez sur **OK** pour créer la règle.

   Figure : Exemple de règle ACL



Une fois la règle créée, elle est à l'état désactivé. Pour que la règle soit effective, vous devez l'activer.

> **Remarque :**
>
> Pour activer une règle, la fonctionnalité ACL doit être activée. Si la fonctionnalité est désactivée et que vous tentez d'activer une règle ACL, un message « L'ACL n'est pas en cours d'exécution » s'affiche.

Activer une règle ACL

1. Passez votre souris sur la règle que vous souhaitez activer, puis cliquez sur le cercle à trois points.
2. Dans le menu, sélectionnez **Activer**.
3. Vous pouvez également sélectionner le bouton radio correspondant à cette règle et cliquer sur l'onglet **Activer** .
4. À l'invite, cliquez sur **Oui** pour confirmer.

Autres actions pour les règles ACL

Vous pouvez appliquer les actions suivantes aux règles ACL :

1. Désactiver une règle ACL
2. Modification d'une règle ACL
3. Supprimer une règle ACL
4. Renuméroter la priorité des règles ACL

Désactiver une règle ACL

1. Passez la souris sur la règle que vous souhaitez désactiver et sélectionnez le cercle à trois points.
2. Cliquez sur **Désactiver** dans la liste.
3. Vous pouvez également sélectionner le bouton radio correspondant à cette règle et cliquer sur l'onglet **Désactiver** .
4. Cliquez sur **Oui** pour confirmer.

> **Remarque :**
>
> Lorsque vous désactivez une règle, elle ne s'applique plus au trafic entrant. Toutefois, la configuration de la règle reste sous les paramètres ACL.

Modification d'une règle ACL

1. Passez le curseur de la souris sur la règle que vous souhaitez modifier et sélectionnez le cercle à trois points.
2. Cliquez sur **Modifier la règle** dans la liste. La fenêtre **Modifier la règle** s'ouvre.
3. Vous pouvez également sélectionner le bouton radio correspondant à cette règle et cliquer sur l'onglet **Modifier la règle** . La fenêtre **Modifier la règle** s'ouvre.
4. Apportez les modifications et cliquez sur **OK**.

> **Remarque :**
>
> Vous pouvez modifier une règle à la fois dans l'état activé et désactivé. Si vous modifiez une règle déjà activée, les modifications sont appliquées immédiatement. Pour une règle dont l'état est désactivé, les mises à jour sont appliquées lorsque vous activez la règle.

Supprimer une règle ACL

1. Assurez-vous que la règle est dans l'état désactivé.

2. Passez le curseur de la souris sur la règle à supprimer et sélectionnez le cercle à trois points. Cliquez sur **Supprimer la règle** dans la liste.
3. Vous pouvez également sélectionner le bouton radio correspondant à cette règle et cliquer sur l'onglet **Supprimer la règle** .
4. Cliquez sur **Oui** pour confirmer.

> **Remarque :**
>
> Vous ne pouvez pas supprimer une règle dont l'état est activé.

Renuméroter les priorités des règles ACL

1. Passez le curseur de la souris sur la règle dont vous souhaitez renuméroter les priorités et sélectionnez le cercle à trois points. Cliquez sur **Renuméroter les priorités** dans la liste.
2. Vous pouvez également sélectionner le bouton radio correspondant à cette règle et cliquer sur l'onglet **Sélectionner une action** .
3. Sélectionnez **Renuméroter les priorités**.
4. Le service de gestion SDX attribue automatiquement de nouveaux numéros de priorité, qui sont des multiples de 10, à toutes les règles existantes.
5. Modifiez les règles pour attribuer des numéros de priorité en fonction de vos besoins. Consultez la section « Pour modifier une règle ACL » pour plus d'informations sur la façon de modifier une règle.

Figurine. Exemple de numéros de priorité existants

	Priority ↑	Name	Source IP Address/Subnet
☐	1	2.2.2.2	ANY
☐	2	test1	1.1.1.1
☐	3	test2	ANY

Figurine. Exemple de numéros de priorité par multiples de 10, après la renumérotation des priorités

	Priority ↑	Name	Source IP Address/Subnet
☐	10	2.2.2.2	ANY
☐	20	test1	1.1.1.1
☐	30	test2	ANY

Résolution des problèmes

Si les règles ACL ne sont pas correctement configurées, l'accès peut être refusé à tous les comptes d'utilisateurs. Si vous perdez par inadvertance tout accès réseau au service de gestion SDX en raison d'une configuration incorrecte de la liste de contrôle d'accès, procédez comme suit pour y accéder.

1. Connectez-vous à l'adresse IP de gestion Citrix Hypervisor à l'aide de SSH et de votre compte « racine ».
2. Ouvrez une session sur la console de la machine virtuelle du service de gestion en utilisant les privilèges d'administrateur.
3. Exécutez la commande `pfctl -d`.
4. Ouvrez une session sur le service de gestion via l'interface graphique et reconfigurez l'ACL en conséquence.

Configurer un cluster d'instances Citrix ADC

January 27, 2022

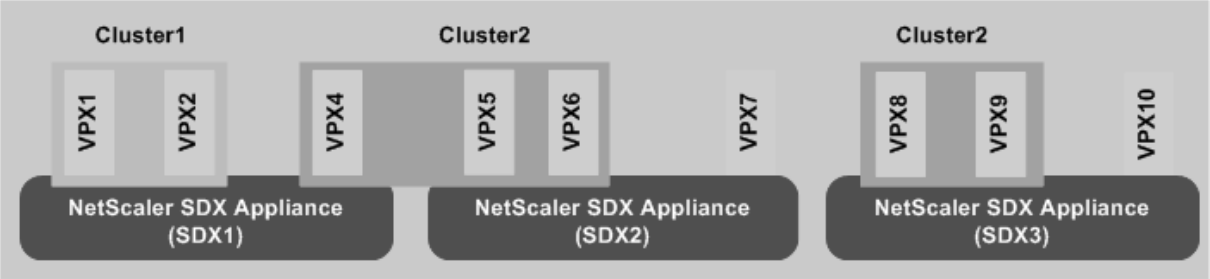
Après avoir provisionné des instances Citrix ADC sur une ou plusieurs appliances SDX, vous pouvez créer un cluster d'instances Citrix ADC.

Citrix vous recommande d'effectuer la configuration du cluster à partir du service de gestion. Lorsque vous effectuez la configuration du cluster à partir d'une instance VPX, le service de gestion prend connaissance de la configuration lors de la découverte automatique toutes les 30 minutes. Dans le pire des cas, les informations de clustering ne sont pas découvertes pendant 30 minutes. Bien que le cluster puisse fonctionner correctement, certains contrôles de validation essentiels pour les dépendances de cluster ne sont pas effectués. Le service de gestion effectue ces vérifications avant de configurer le cluster sur des instances ADC. Par conséquent, vous devez effectuer toute configuration de cluster à partir du service de gestion.

Remarque :

- Pour configurer un cluster, vous devez comprendre le clustering Citrix ADC. Pour plus d'informations, consultez la section Clustering.
- Pour les clusters qui ont des instances Citrix ADC sur des appliances SDX, Citrix vous recommande d'utiliser des instances Citrix ADC provenant de trois appliances SDX. Ce processus garantit que les critères de cluster d'un minimum de (n/2 +1) nœuds sont toujours satisfaits.

Figure 1. Cluster d'instances SDX Citrix ADC



La figure précédente montre trois appliances SDX, SDX1, SDX2 et SDX3, sur le même sous-réseau. Les instances Citrix ADC sur ces appliances sont utilisées pour former deux clusters : Cluster1 et Cluster2.

- Cluster1 inclut deux instances sur SDX1.
- Cluster2 inclut une instance sur SDX1, deux instances sur SDX2 et deux autres instances sur SDX3.

Points à retenir

- La formation CLAG avec les interfaces Mellanox (50G et 100G) n'est pas prise en charge sur une plate-forme SDX.
- Tous les nœuds d'un cluster doivent être du même type. Vous ne pouvez pas former un cluster avec les combinaisons suivantes :
  - Appliances matérielles et virtuelles.
  - les instances Citrix ADC VPX et les instances Citrix ADC SDX.
  - Instances ADC sur différentes plates-formes matérielles SDX.
- Les instances Citrix ADC doivent être de la même version, qui doit être la version 10.1 ou ultérieure.
- Les instances Citrix ADC doivent toutes disposer de la même licence de fonctionnalité.
- Aucune configuration ne peut être mise à jour sur des instances Citrix ADC individuelles après leur ajout au cluster. Toutes les modifications doivent être effectuées via l'adresse IP du cluster.
- Les instances Citrix ADC doivent toutes disposer des mêmes ressources (mémoire, processeur, interfaces, etc.).
- Le MTU du fond de panier doit être supérieur de 78 octets à celui de l'interface de données.
- Assurez-vous que la valeur MTU de l'interface de données est inférieure à 9138 octets.
- À partir de la version 13.0 build 82.x, vous êtes invité à ajouter une adresse SNIP lors de l'ajout d'un nœud à un cluster. Vous pouvez également créer des adresses SNIP dynamiquement lors de l'ajout d'un nœud. Cette fonctionnalité permet de résoudre les problèmes de sécurité liés à la vérification stricte de l'adresse IP source.
- **Important** Utilisez l'option **Supprimer le cluster** avec précaution. Lorsque vous cliquez sur **Supprimer le cluster**, le cluster est supprimé sans aucun avertissement.

Pour configurer un cluster sur une appliance SDX

1. Ouvrez une session sur l'appliance SDX.
2. Dans l'onglet **Configuration**, accédez à **Citrix ADC > Clusters > Instances de cluster**.
3. Créez le cluster :
   a) Cliquez sur **Créer un cluster**.
   b) Dans la boîte de dialogue **Créer un cluster**, définissez les paramètres requis pour le cluster. Pour obtenir la description d'un paramètre, placez le curseur de la souris sur le champ correspondant.
   c) Cliquez sur **Suivant** pour afficher le résumé de la configuration.
   d) Cliquez sur **Terminer** pour créer le cluster.
   Remarque : lorsqu'une instance Citrix ADC avec un VLAN L2 configuré est ajoutée au cluster, la commande
   add VLAN est enregistrée avec le paramètre
   `sdxvlan` défini sur Oui. Ce paramètre est un argument interne et est utilisé pour éviter la perte de connectivité lors de la formation d'un cluster SDX.
4. Ajoutez des nœuds au cluster :
   a) Cliquez sur **Ajouter un nœud**.
   b) Dans la boîte de dialogue **Ajouter un nœud**, configurez les paramètres nécessaires à l'ajout d'un nœud de cluster. Pour obtenir la description d'un paramètre, placez le curseur de la souris sur le champ correspondant.
   c) Cliquez sur **Suivant** pour afficher le résumé de la configuration.
   d) Cliquez sur **Terminer** pour ajouter le nœud au cluster.
   e) Répétez les étapes a à d pour ajouter un autre nœud au cluster.

   Après avoir créé le cluster, vous devez le configurer en y accédant via l'adresse IP du cluster.

> **Remarque :**
>
> Pour obtenir une liste mise à jour des clusters Citrix ADC, dont chacun possède au moins une instance Citrix ADC de l'appliance SDX, utilisez l'option **Redécouvrir** .

Pour ajouter une instance Citrix ADC qui existe sur une appliance SDX à un cluster configuré sur une autre appliance SDX

1. Ouvrez une session sur l'appliance SDX à partir de laquelle vous souhaitez ajouter l'instance Citrix ADC.
2. Dans l'onglet **Configuration**, accédez à **Citrix ADC**, puis cliquez sur **Clusters**.
3. Cliquez sur **Ajouter un nœud**.

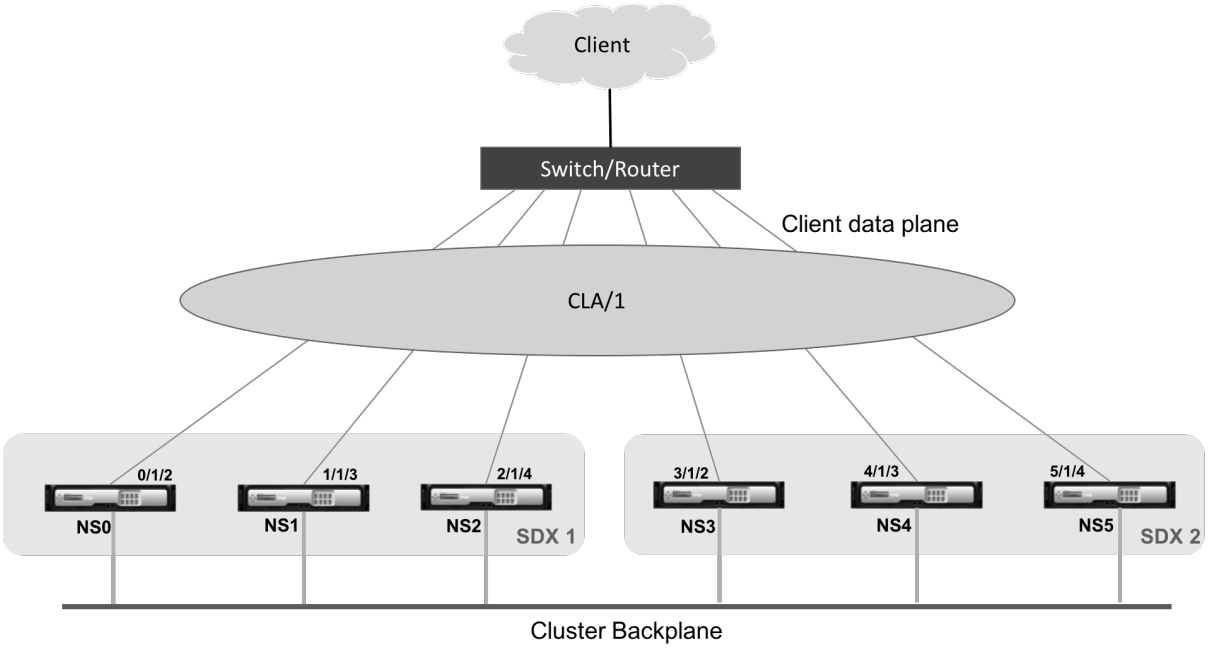
4. Dans la boîte de dialogue **Ajouter un nœud**, configurez les paramètres nécessaires à l'ajout d'un nœud de cluster. Pour obtenir la description d'un paramètre, placez le curseur de la souris sur le champ correspondant.
   Remarque : Assurez-vous que les valeurs des paramètres Adresse IP du
   cluster et Mot de passe IP du cluster correspondent au cluster auquel vous souhaitez ajouter le nœud.
5. Cliquez sur **Suivant** pour afficher le résumé de la configuration.
6. Cliquez sur **Terminer** pour ajouter le nœud au cluster.

Configuration du regroupement de liens de cluster

June 13, 2022

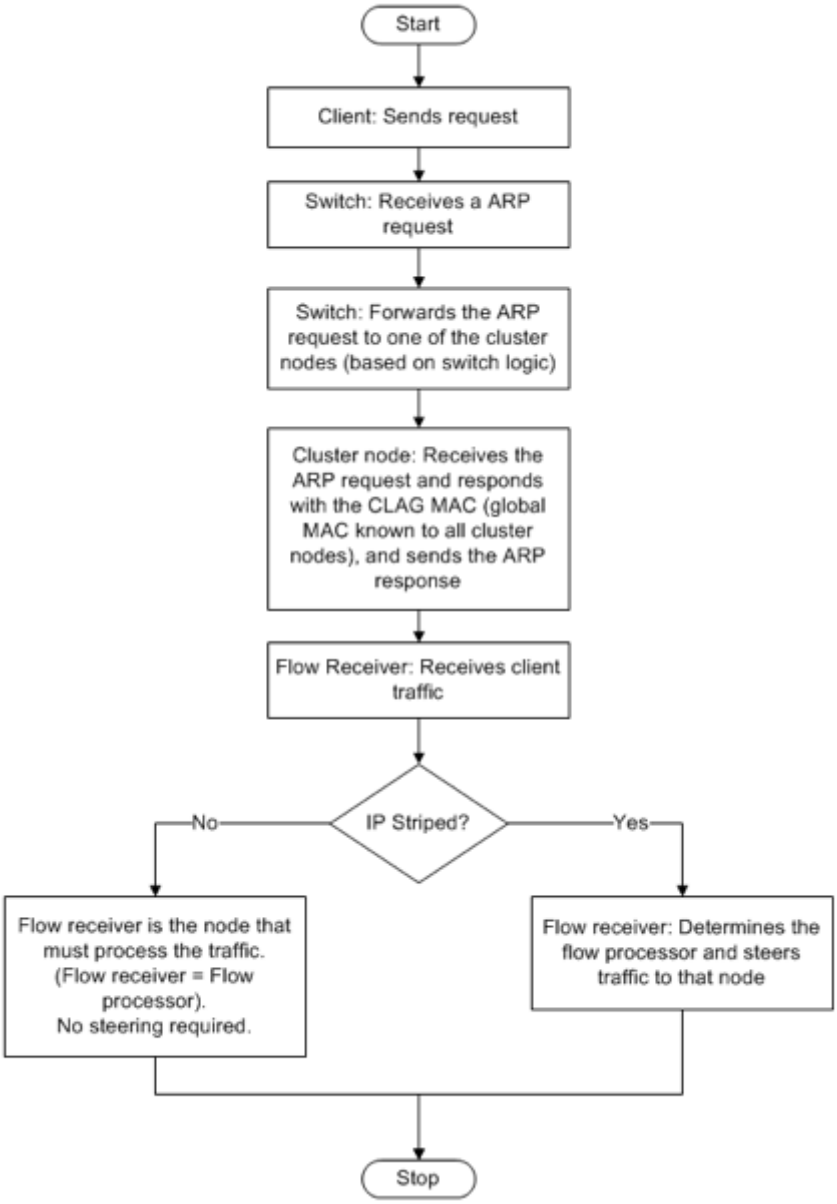
L'agrégation de liens de cluster, comme son nom l'indique, combine un groupe d'interfaces cluster-nœud dans un canal. Il s'agit d'une extension de l'agrégation de liens Citrix ADC (LA). La seule différence est que, bien que l'agrégation de liens nécessite que les interfaces se trouvent sur le même périphérique, dans l'agrégation de liens de cluster, les interfaces se trouvent sur des nœuds différents du cluster. Pour plus d'informations sur l'agrégation de liens, voir Configuration de l'agrégation de liens.

Prenons l'exemple d'un cluster à six nœuds, sur deux appliances SDX, dans lequel les six nœuds sont connectés à un commutateur en amont. Un canal LA de cluster (CLA/1) est formé par des interfaces de liaison 0/1/2, 1/1/3, 2/1/4, 3/1/2, 4/1/3 et 5/1/4.



Un canal LA de cluster possède les attributs suivants :

- Chaque canal possède une adresse MAC unique convenue par les nœuds du cluster.
- Le canal peut lier les interfaces des nœuds SDX locaux et distants.
- Un maximum de quatre canaux LA de cluster sont pris en charge dans un cluster.
- Un maximum de 16 interfaces peuvent être liées à chaque canal LA du cluster.
- Les interfaces de fond de panier ne peuvent pas faire partie d'un canal LA de cluster.
- Lorsqu'une interface est liée à un canal LA de cluster, les paramètres de canal ont priorité sur les paramètres d'interface réseau.
- Une interface réseau ne peut être liée qu'à un seul canal.
- Ne configurez pas l'accès de gestion à un nœud de cluster sur un canal LA du cluster (par exemple, CLA/1) ou ses interfaces membres. Lorsque le nœud est INACTIF, l'interface LA du cluster correspondante est marquée comme POWER OFF, ce qui entraîne la perte de l'accès à la gestion.



Implémentez des configurations similaires sur l'adresse IP du cluster et sur le périphérique de connexion externe. Si possible, configurez le commutateur en amont pour distribuer le trafic en fonction de l'adresse IP ou du port au lieu de l'adresse MAC.

Points à retenir :

- Activez LACP (en spécifiant le mode LACP comme ACTIVE ou PASSIVE).
  Remarque : Assurez-vous que le mode LACP n'est pas défini sur PASSIF à la fois sur le cluster Citrix ADC et sur le périphérique de connexion externe.
- Pour créer un canal LA de cluster, la clé LACP peut avoir une valeur comprise entre 5 et 8. Ces clés LACP sont mappées à CLA/1, CLA/2, CLA/3 et CLA/4.
- Sur l'appliance SDX, les interfaces membres du groupe d'agrégation de liens de cluster (CLAG)

ne peuvent pas être partagées avec d'autres machines virtuelles.

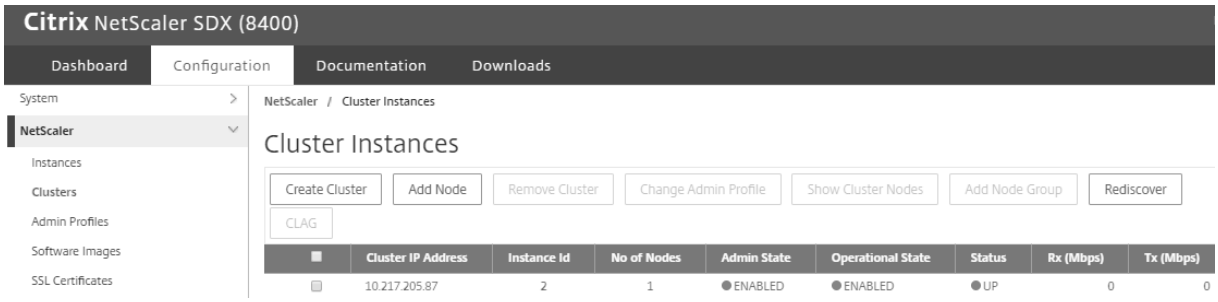
- Sur le commutateur en amont, définissez le délai d'expiration LACP sur « court » pour éviter les trous noirs de trafic de longue durée sur les nœuds du cluster. Ce paramètre est utile lorsque le commutateur en amont n'est pas averti de la mise hors tension du CLAG et de ses interfaces membres avant l'expiration du délai LACP.

Prérequis :

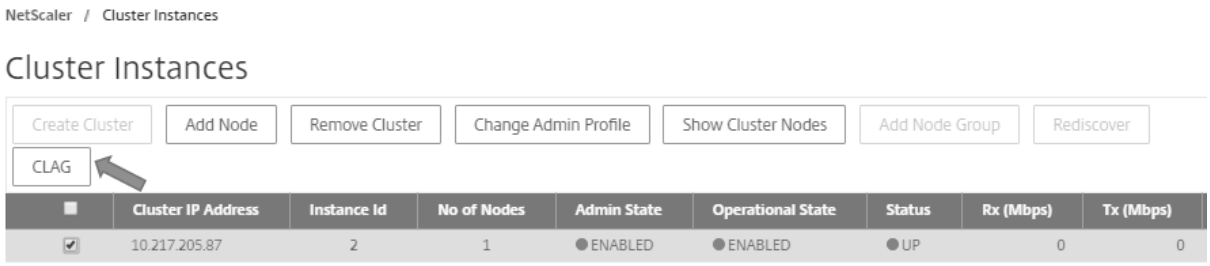
Créez un cluster d'instances Citrix ADC. Les nœuds du cluster peuvent être des instances Citrix ADC sur la même appliance SDX ou sur d'autres appliances SDX disponibles sur le même sous-réseau.

Pour configurer un canal LA de cluster à l'aide du service de gestion :

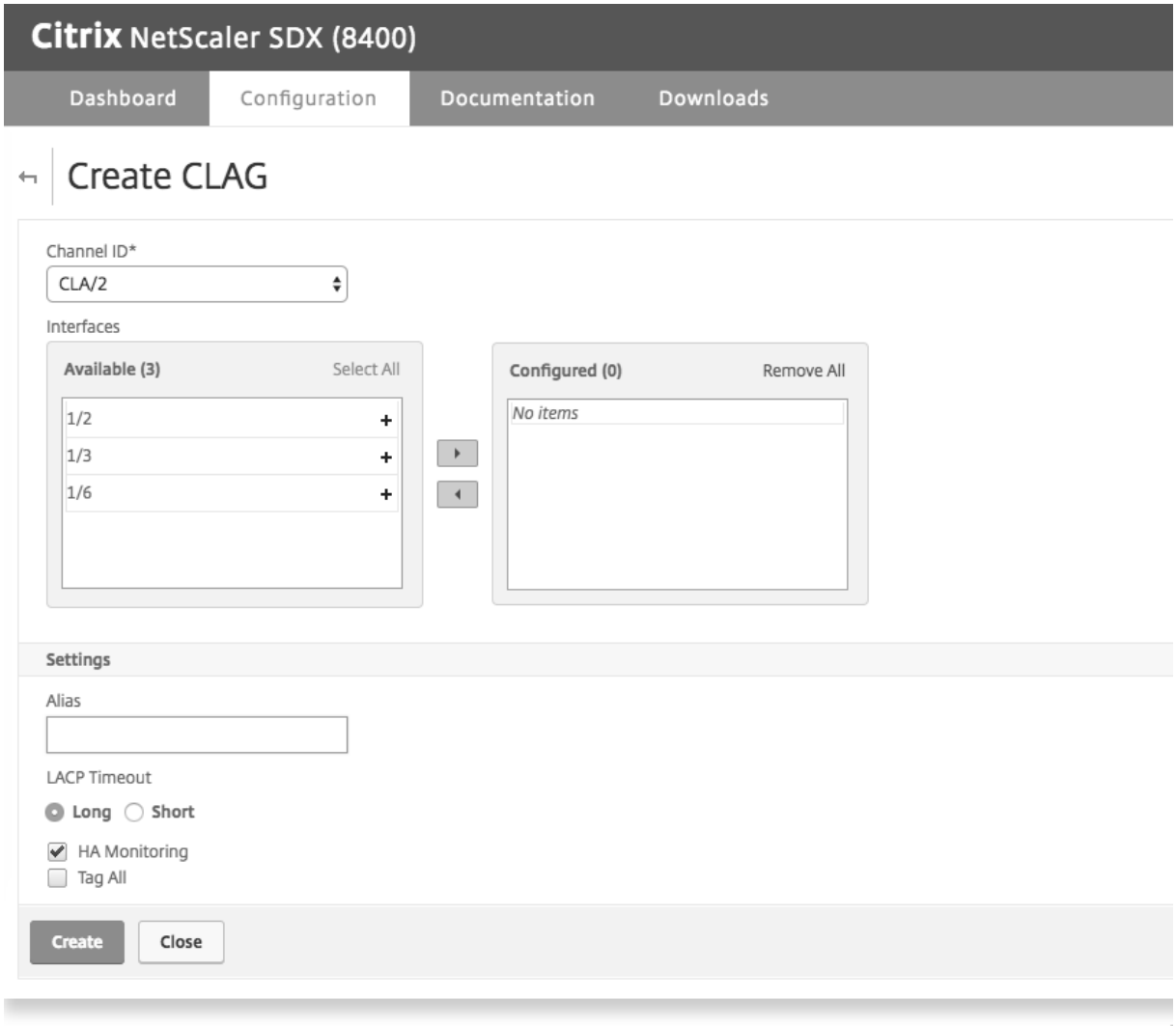
1. Ouvrez une session sur l'appliance SDX.
2. Dans l'onglet **Configuration**, accédez à **Citrix ADC**, puis cliquez sur **Clusters**.



3. Sur la page **Instances de cluster**, sélectionnez le cluster et cliquez sur **CLAG**.

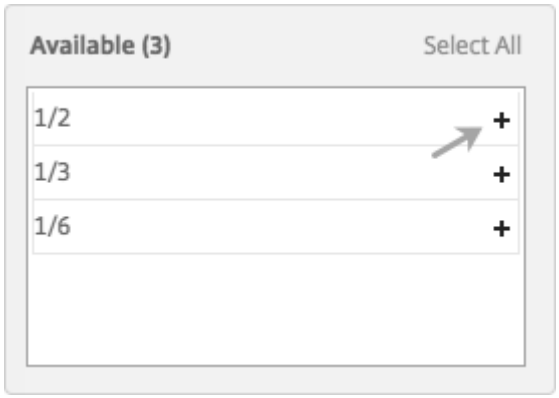


4. Dans la boîte de dialogue **Créer un CLAG**, procédez comme suit :



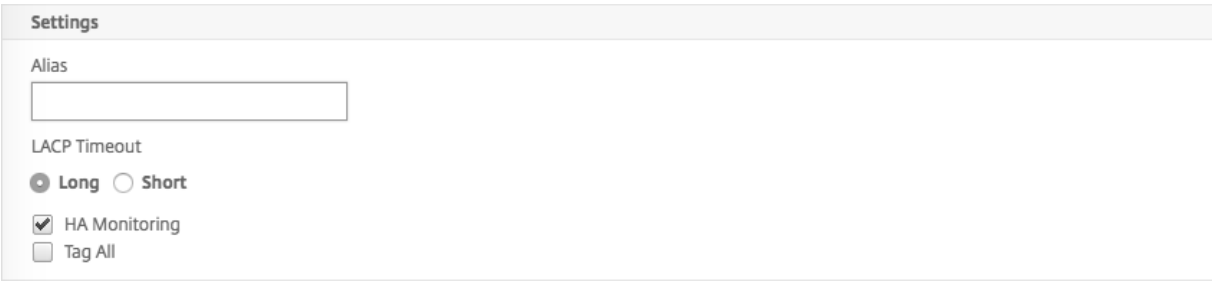
a. Dans la liste déroulante **Channel ID**, sélectionnez l'ID de canal LA du cluster.

b. Dans la section **Interfaces**, dans la zone de sélection **Disponible**, sélectionnez les interfaces et cliquez sur **+**.



Les interfaces sélectionnées s'affichent sous la zone de sélection **Configuré** .

c. Dans la section **Paramètre**, procédez comme suit :



i. Dans le champ **Alias**, saisissez un autre nom pour le canal LA du cluster.

ii. Dans le champ **Délai d'expiration LACP**, sélectionnez l'une des valeurs suivantes pour définir l'intervalle après lequel un lien n'est pas agrégé, si le lien ne reçoit pas de LACPDU.

La valeur doit correspondre sur tous les ports participant à l'agrégation de liens sur l'appliance SDX et le nœud partenaire :

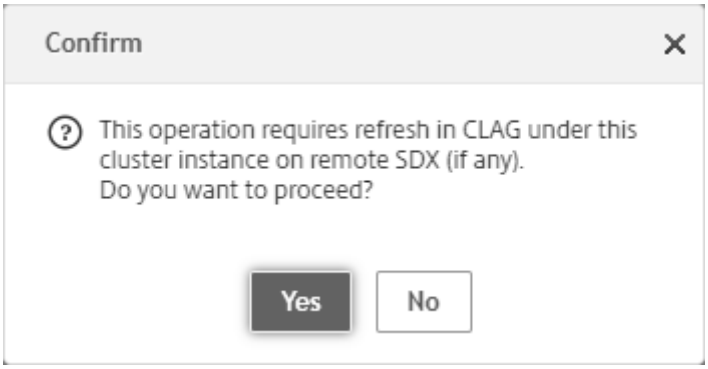
- **Longue durée** : 30 secondes
- **Court** — 1 seconde

iii. Pour la configuration haute disponibilité (HA), cochez la case **Surveillance HA** pour surveiller le canal à la recherche d'événements de défaillance. La défaillance d'un canal LA sur lequel HA MON est activé déclenche le basculement HA.

iv. Sélectionnez **Tag All** pour ajouter une balise 802.1q de quatre octets à chaque paquet envoyé sur ce canal. Le paramètre **ON** applique des balises à tous les VLAN liés à ce canal. OFF applique la balise à tous les VLAN autres que le VLAN natif.

d. Cliquez sur **Créer** pour configurer un CLAG pour l'un des dispositifs SDX.

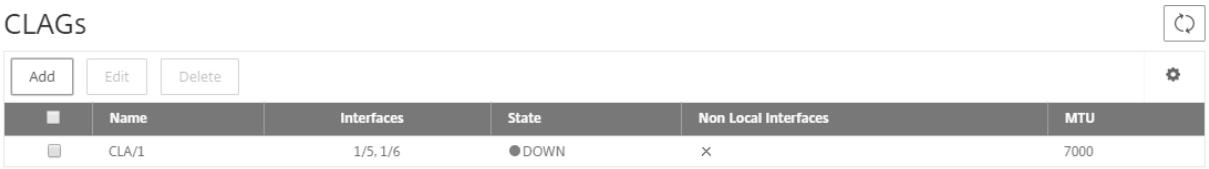
5. Dans la boîte de dialogue **Confirmer**, cliquez sur **Oui** pour actualiser les paramètres CLAG des autres appliances SDX.



Remarque : Si vous sélectionnez**Non**, le CLAG n'est pas configuré.

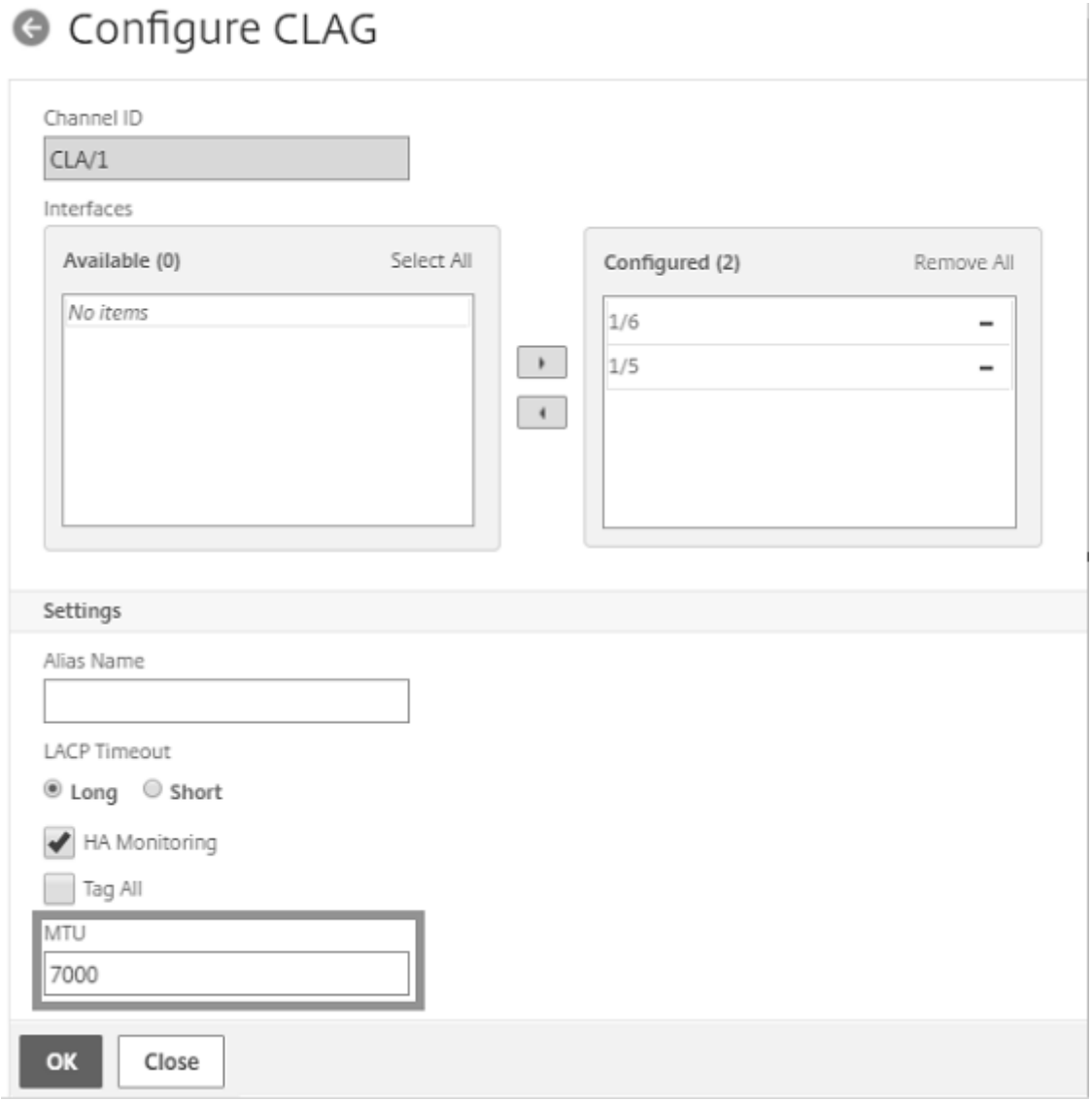
> **Important :**
>
> - Actualisez manuellement les paramètres CLAG dans les autres appliances SDX.
> - Les paramètres MTU doivent être identiques sur les deux appliances SDX. Les paramètres MTU doivent être modifiés manuellement sur l'un ou l'autre des dispositifs SDX.

6. Pour modifier les paramètres MTU dans la boîte de dialogue **CLags**, procédez comme suit :

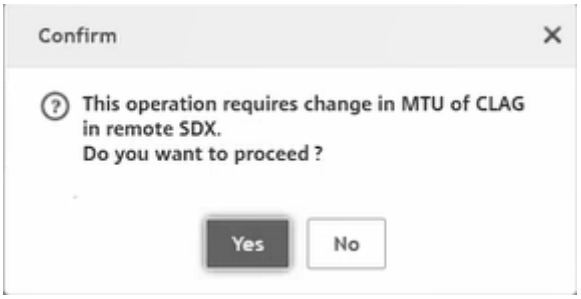


i. Sélectionnez **CLA/1** et cliquez sur **Modifier**.

ii. Dans la boîte de dialogue **Configurer CLAG**, définissez le MTU manuellement dans le champ **MTU** et cliquez sur **OK.**



7. Dans la boîte de dialogue **Confirmer**, cliquez sur **Oui**.



Configurez les chiffrements SSL pour accéder en toute sécurité au service de gestion

October 4, 2022

Vous pouvez sélectionner des suites de chiffrement SSL dans une liste de chiffrements SSL pris en charge par les appliances Citrix ADC SDX. Liez n'importe quelle combinaison de chiffrements SSL pour accéder au service de gestion SDX en toute sécurité via HTTPS. Une appliance SDX fournit 37 groupes de chiffrement prédéfinis, qui sont des combinaisons de chiffrements similaires, et vous pouvez créer des groupes de chiffrement personnalisés à partir de la liste des chiffrements SSL pris en charge.

Limitations

- Les chiffrements de liaison avec échange de clés = « DH » ou « ECC-DHE » ne sont pas pris en charge.
- La liaison des chiffrements avec Authentication = « DSS » n'est pas prise en charge.
- Les chiffrements de liaison qui ne font pas partie de la liste des chiffrements SSL pris en charge, ou l'inclusion de ces chiffrements dans un groupe de chiffrement personnalisé, ne sont pas pris en charge.

Chiffrements SSL pris en charge

Le tableau suivant répertorie les chiffrements SSL pris en charge. La valeur de la colonne **Protocole** est le protocole le plus bas pris en charge. Par exemple, si SSLv3 est répertorié, SSLv3/TLSv1/TLSv1.1/TLSv1.2 sont tous pris en charge.

Nom du chiffrement Citrix	Nom de chiffrement OpenSSL	Code Hex	Protocole	algorithme d'échange de clés	algorithme d'authentification	Algorithme de code d'authentification de message (MAC)
TLS1-AES-256-CBC-SHA	AES256-SHA	0x0035	SSLv3	RSA	RSA	AES (256)
TLS1-AES-128-CBC-SHA	AES128-SHA	0x002F	SSLv3	RSA	RSA	AES (128)

Nom du chiffrement Citrix	Nom de chiffrement OpenSSL	Code Hex	Protocole	algorithme d'échange de clés	algorithme d'authentification	Algorithme de code d'authentification de message (MAC)
TLS1.2-AES-256-SHA256	AES256-SHA256	0x003D	TLSv1.2	RSA	RSA	AES (256)
TLS1.2-AES-128-SHA256	AES128-SHA256	0x003C	TLSv1.2	RSA	RSA	AES (128)
TLS1.2-AES256-GCM-SHA384	AES256-GCM-SHA384	0x009D	TLSv1.2	RSA	RSA	AES-GCM(256)
TLS1.2-AES128-GCM-SHA256	AES128-GCM-SHA256	0x009C	TLSv1.2	RSA	RSA	AES-GCM(128)
TLS1-ECDHE-RSA-AES256-SHA	ECDHE-RSA-AES256-SHA	0xC014	SSLv3	ECC-DHE	RSA	AES (256)
TLS1-ECDHE-RSA-AES128-SHA	ECDHE-RSA-AES128-SHA	0xC013	SSLv3	ECC-DHE	RSA	AES (128)
TLS1.2-ECDHE-RSA-AES-256-SHA384	ECDHE-RSA-AES256-SHA384	0xC028	TLSv1.2	ECC-DHE	RSA	AES (256)

Nom du chiffrement Citrix	Nom de chiffrement OpenSSL	Code Hex	Protocole	algorithme d'échange de clés	algorithme d'authentification	Algorithme de code d'authentification de message (MAC)
TLS1.2-ECDHE-RSA-AES-128-SHA256	ECDHE-RSA-AES128-SHA256	0xC027	TLSv1.2	ECC-DHE	RSA	AES (128)
TLS1.2-ECDHE-RSA-AES256-GCM-SHA384	ECDHE-RSA-AES256-GCM-SHA384	0xC030	TLSv1.2	ECC-DHE	RSA	AES-GCM(256)
TLS1.2-ECDHE-RSA-AES128-GCM-SHA256	ECDHE-RSA-AES128-GCM-SHA256	0xC02F	TLSv1.2	ECC-DHE	RSA	AES-GCM(128)
TLS1.2-DHE-RSA-AES-256-SHA256	DHE-RSA-AES256-SHA256	0x006B	TLSv1.2	DH	RSA	AES (256)
TLS1.2-DHE-RSA-AES-128-SHA256	DHE-RSA-AES128-SHA256	0x0067	TLSv1.2	DH	RSA	AES (128)
TLS1.2-DHE-RSA-AES256-GCM-SHA384	DHE-RSA-AES256-GCM-SHA384	0x009F	TLSv1.2	DH	RSA	AES-GCM(256)

Nom du chiffrement Citrix	Nom de chiffrement OpenSSL	Code Hex	Protocole	algorithme d'échange de clés	algorithme d'authentification	Algorithme de code d'authentification de message (MAC)
TLS1.2-DHE-RSA-AES128-GCM-SHA256	DHE-RSA-AES128-GCM-SHA256	0x009E	TLSv1.2	DH	RSA	AES-GCM(128)
TLS1-DHE-RSA-AES-256-CBC-SHA	DHE-RSA-AES256-SHA	0x0039	SSLv3	DH	RSA	AES (256)
TLS1-DHE-RSA-AES-128-CBC-SHA	DHE-RSA-AES128-SHA	0x0033	SSLv3	DH	RSA	AES (128)
TLS1-DHE-DSS-AES-256-CBC-SHA	DHE-DSS-AES256-SHA	0x0038	SSLv3	DH	DSS	AES (256)
TLS1-DHE-DSS-AES-128-CBC-SHA	DHE-DSS-AES128-SHA	0x0032	SSLv3	DH	DSS	AES (128)
TLS1-ECDHE-RSA-DES-CBC3-SHA	ECDHE-RSA-DES-CBC3-SHA	0xC012	SSLv3	ECC-DHE	RSA	3DES(168)
SSL3-EDH-RSA-DES-CBC3-SHA	EDH-RSA-DES-CBC3-SHA	0x0016	SSLv3	DH	RSA	3DES(168)
SSL3-EDH-DSS-DES-CBC3-SHA	EDH-DSS-DES-CBC3-SHA	0x0013	SSLv3	DH	DSS	3DES(168)

Nom du chiffrement Citrix	Nom de chiffrement OpenSSL	Code Hex	Protocole	algorithme d'échange de clés	algorithme d'authentification	Algorithme de code d'authentification de message (MAC)
TLS1-ECDHE-RSA-RC4-SHA	ECDHE-RSA-RC4-SHA	0xC011	SSLv3	ECC-DHE	RSA	RC4(128)
SSL3-DES-CBC3-SHA	DES-CBC3-SHA	0x000A	SSLv3	RSA	RSA	3DES(168)
SSL3-RC4-SHA	RC4-SHA	0x0005	SSLv3	RSA	RSA	RC4(128)
SSL3-RC4-MD5	RC4-MD5	0x0004	SSLv3	RSA	RSA	RC4(128)
SSL3-DES-CBC-SHA	DES-CBC-SHA	0x0009	SSLv3	RSA	RSA	DES (56)
SSL3-EXP-RC4-MD5	EXP-RC4-MD5	0x0003	SSLv3	RSA (512)	RSA	RC4(40)
SSL3-EXP-DES-CBC-SHA	EXP-DES-CBC-SHA	0x0008	SSLv3	RSA (512)	RSA	DES (40)
SSL3-EXP-RC2-CBC-MD5	EXP-RC2-CBC-MD5	0x0006	SSLv3	RSA (512)	RSA	RC2(40)
SSL2-DES-CBC-MD5	DHE-DSS-AES128-SHA256	0x0040	SSLv2	RSA	RSA	DES (56)
SSL3-EDH-DSS-DES-CBC-SHA	EDH-DSS-DES-CBC-SHA	0x0012	SSLv3	DH	DSS	DES (56)
SSL3-EXP-EDH-DSS-DES-CBC-SHA	EXP-EDH-DSS-DES-CBC-SHA	0x0011	SSLv3	DH (512)	DSS	DES (40)

Nom du chiffrement Citrix	Nom de chiffrement OpenSSL	Code Hex	Protocole	algorithme d'échange de clés	algorithme d'authentification	Algorithme de code d'authentification de message (MAC)
SSL3-EDH-RSA-DES-CBC-SHA	EDH-RSA-DES-CBC-SHA	0x0015	SSLv3	DH	RSA	DES (56)
SSL3-EXP-EDH-RSA-DES-CBC-SHA	EXP-EDH-RSA-DES-CBC-SHA	0x0014	SSLv3	DH (512)	RSA	DES (40)
SSL3-ADH-RC4-MD5	ADH-RC4-MD5	0x0018	SSLv3	DH	Aucun	RC4(128)
SSL3-ADH-DES-CBC3-SHA	ADH-DES-CBC3-SHA	0x001B	SSLv3	DH	Aucun	3DES(168)
SSL3-ADH-DES-CBC-SHA	ADH DES CBC-SHA	0x001A	SSLv3	DH	Aucun	DES (56)
TLS1-ADH-AES-128-CBC-SHA	ADH-AES128-SHA	0x0034	SSLv3	DH	Aucun	AES (128)
TLS1-ADH-AES-256-CBC-SHA	ADH-AES256-SHA	0x003A	SSLv3	DH	Aucun	AES (256)
SSL3-EXP-ADH-RC4-MD5	EXP-ADH-RC4-MD5	0x0017	SSLv3	DH (512)	Aucun	RC4(40)
SSL3-EXP-ADH-DES-CBC-SHA	EXP-ADH-DES-CBC-SHA	0x0019	SSLv3	DH (512)	Aucun	DES (40)
SSL3-NULL-MD5	NULL-MD5	0x0001	SSLv3	RSA	RSA	Aucun
SSL3-NULL-SHA	NULL-SHA	0x0002	SSLv3	RSA	RSA	Aucun

Groupes de chiffrement prédéfinis

Le tableau suivant répertorie les groupes de chiffrement prédéfinis fournis par l'appliance SDX.

Nom du groupe de chiffrement	Description
ALL	Tous les chiffrements pris en charge par l'appliance SDX, à l'exception des chiffrements NULL
DEFAULT	Liste de chiffrement par défaut avec une force de chiffrement >= 128 bits
kRSA	Chiffrements avec l'algo Key-Ex en tant que RSA
kEDH	Chiffrements avec l'algo Key-Ex comme éphémère-DH
DH	Chiffrements avec l'algo Key-Ex en tant que DH
EDH	Chiffrements avec l'algo Key-EX/Auth en tant que DH
aRSA	Chiffrements avec l'algorithme d'authentification en tant que RSA
aDSS	Chiffrements avec l'algorithme Auth en tant que DSS
aNULL	Chiffrements avec l'algo Auth comme NULL
DSS	Chiffrements avec l'algorithme Auth en tant que DSS
DES	Chiffrements avec l'algorithme Enc en tant que DES
3DES	Chiffrements avec l'algorithme Enc en tant que 3DES
RC4	Chiffrements avec l'algorithme Enc en tant que RC4
RC2	Chiffrements avec l'algorithme Enc en tant que RC2
NULL	Chiffrements avec l'algo Enc comme NULL
MD5	Chiffrements avec l'algo MAC en tant que MD5
SHA1	Chiffrements avec l'algo MAC en tant que SHA-1

Nom du groupe de chiffrement	Description
SHA	Chiffrements avec l'algo MAC en tant que SHA
NULL	Chiffrements avec l'algo Enc comme NULL
RSA	Chiffrements avec algo Key-EX/Auth en tant que RSA
ADH	Chiffrements avec l'algo Key-Ex comme DH et l'algo Auth comme NULL
SSLv2	Chiffrement du protocole SSLv2
SSLv3	Chiffrement du protocole SSLv3
TLSv1	Chiffrement du protocole SSLV3/TLSv1
TLSv1_ONLY	Chiffrement du protocole TLSv1
EXP	Chiffrements d'exportation
EXPORT	Chiffrements d'exportation
EXPORT40	Chiffrement d'exportation avec cryptage 40 bits
EXPORT56	Chiffrement d'exportation avec cryptage 56 bits
LOW	Chiffrements à faible puissance (cryptage 56 bits)
MEDIUM	Chiffrements de force moyenne (cryptage 128 bits)
HIGH	Chiffrements haute résistance (cryptage 168 bits)
AES	Chiffrements AES
FIPS	Chiffrements approuvés FIPS
ECDHE	Chiffres éphémères DH à courbe elliptique
AES-GCM	Chiffrements avec l'algorithme Enc comme AES-GCM
SHA2	Chiffrements avec l'algo MAC en tant que SHA-2

Afficher les groupes de chiffrement prédéfinis

Pour afficher les groupes de chiffrement prédéfinis, sous l'onglet **Configuration**, dans le volet de navigation, développez **Service de gestion**, puis cliquez sur **Groupes de chiffrement**.

Créer des groupes de chiffrement personnalisés

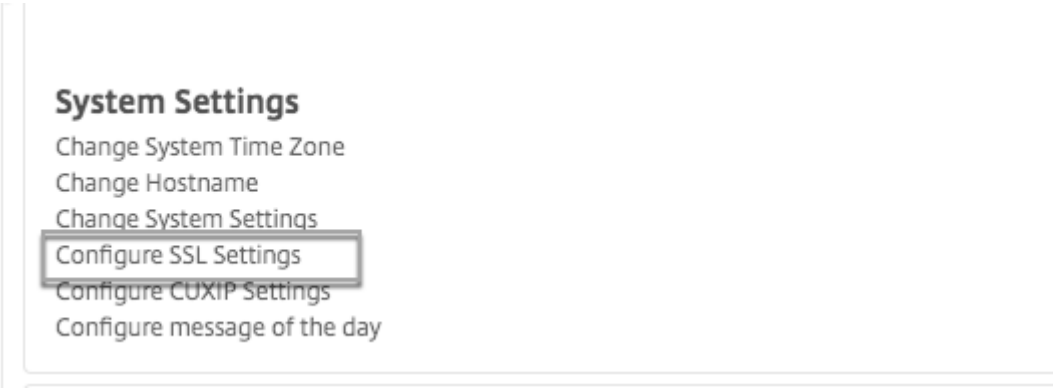
Vous pouvez créer des groupes de chiffrement personnalisés à partir de la liste des chiffrements SSL pris en charge.

Pour créer des groupes de chiffrement personnalisés :

1. Dans l'onglet **Configuration**, dans le volet de navigation, développez **Service de gestion**, puis cliquez sur **Groupes de chiffrement**.
2. Dans le volet **Groupes de chiffrement**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer un groupe de chiffrement**, effectuez les opérations suivantes :
   a) Dans le champ **Nom du groupe**, saisissez un nom pour le groupe de chiffrement personnalisé.
   b) Dans le champ **Description du groupe de chiffrement**, saisissez une brève description du groupe de chiffrement personnalisé.
   c) Dans la section **Suites de chiffrement**, cliquez sur **Ajouter** et sélectionnez les chiffrements à inclure dans la liste des chiffrements SSL pris en charge.
   d) Cliquez sur **Créer**.

Afficher les liaisons de chiffrement SSL existantes

Pour afficher les liaisons de chiffrement existantes, sous l'onglet **Configuration**, dans le volet de navigation, développez **Système**, puis cliquez sur **Configurer les paramètres SSL** sous **Paramètres système**.



Remarque : Après la mise à niveau vers la dernière version du service de gestion, la liste des suites de chiffrement existantes indique les noms OpenSSL. Une fois que vous avez lié les chiffre-

> ments à partir du service de gestion mis à niveau, l'affichage utilise la convention d'appellation Citrix.

Lier les chiffrements au service HTTPS

1. Dans l'onglet **Configuration**, dans le volet de navigation, cliquez sur **Système**.
2. Dans le volet **Système**, sous Paramètres système, cliquez sur **Configurer les paramètres SSL**.
3. Dans le volet **Modifier les paramètres**, cliquez sur **Suites de chiffrement**.
4. Dans le volet **Suites de chiffrement**, effectuez l'une des opérations suivantes :
    - Pour choisir un groupe de chiffrement parmi les groupes de chiffrement prédéfinis, sélectionnez **Groupes de chiffrement**, sélectionnez un groupe de **chiffrement dans la liste Groupes de chiffrement**, puis cliquez sur **OK**.
    - Pour faire votre choix dans la liste des chiffrements pris en charge, activez la case à cocher **Suites de chiffrement**, cliquez sur **Ajouter** pour sélectionner les chiffrements, puis cliquez sur **OK**.

Sauvegardez et restaurez les données de configuration de l'appliance SDX

April 8, 2022

Le processus de sauvegarde de l'appliance Citrix ADC SDX est un processus en une étape qui crée un fichier de sauvegarde contenant les éléments suivants :

- Image d'un seul lot :
    - Image de Citrix Hypervisor
    - Correctifs logiciels et packs supplémentaires de Citrix Hypervisor
    - Image du service de gestion
- Image XVA
- Image mise à niveau
- Configuration SDX
- Configuration

Sauvegarder la configuration actuelle

1. Dans l'onglet **Configuration**, dans le volet de navigation, développez **Service de gestion**, puis cliquez sur **Fichiers de sauvegarde**.
2. Dans le volet **Fichiers de sauvegarde**, cliquez sur **Sauvegarder**.

3. dans la boîte de dialogue **Nouveau fichier de sauvegarde**, cochez la case **Protéger le fichier par mot de passe** pour chiffrer le fichier de sauvegarde.
4. Dans les champs **Mot de passe** et **Confirmer le mot** de passe, saisissez et confirmez le mot de passe du fichier de sauvegarde.
5. Cliquez sur **Continuer**.

Le processus de sauvegarde crée un fichier de sauvegarde. Le nom de fichier du fichier de sauvegarde inclut l'adresse IP actuelle du service de gestion et l'horodatage de la sauvegarde. Pour vérifier la présence éventuelle de divergences dans le fichier de sauvegarde, à partir de l'interface graphique SDX, accédez à **Configuration > Système > Événements/Alarmes**.

Sauvegarde planifiée

Par défaut, SDX crée une sauvegarde toutes les 24 heures à l'aide d'une stratégie de sauvegarde. À l'aide de la stratégie de sauvegarde, vous pouvez définir le nombre de fichiers de sauvegarde que vous souhaitez conserver dans l'appliance SDX. Vous pouvez également chiffrer les fichiers de sauvegarde planifiés à l'aide d'un mot de passe pour garantir la sécurité du fichier de sauvegarde.

Modifier la stratégie de sauvegarde

1. Dans l'onglet **Configuration**, cliquez sur **Système**.
2. Dans le volet **Administration des politiques**, cliquez sur **Stratégie de sauvegarde**.
3. Dans le volet**de stratégie Configurer la sauvegarde**, effectuez les opérations suivantes :
    a) Dans le champ**Sauvegardes précédentes à conserver**, saisissez le nombre de fichiers de sauvegarde que vous souhaitez conserver.
    b) Pour chiffrer les fichiers de sauvegarde, cochez la case**Chiffrer le fichier de sauvegarde** .
    c) Dans les champs **Mot de passe** et **Confirmer le mot** de passe, saisissez et confirmez le mot de passe pour chiffrer le fichier de sauvegarde.

Transférer manuellement le fichier de sauvegarde vers un serveur de sauvegarde externe

Vérifiez que vous disposez des informations relatives au serveur de sauvegarde externe avant de transférer manuellement le fichier de sauvegarde.

Transférez le fichier de sauvegarde vers un serveur de sauvegarde externe

1. Dans l'onglet **Configuration**, dans le volet de navigation, développez **Service de gestion**, puis cliquez sur **Fichiers de sauvegarde**.
2. Dans le volet **Fichiers de sauvegarde**, sélectionnez le fichier de sauvegarde, puis cliquez sur **Transférer**.

3. Dans le champ **Serveur**, saisissez le nom d'hôte ou l'adresse IP du serveur de sauvegarde externe.
4. Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez le nom d'utilisateur et le mot de passe pour accéder au serveur de sauvegarde externe.
5. Dans le champ **Port**, saisissez le numéro de port.
6. Dans le champ **Protocole de transfert**, sélectionnez le protocole que vous souhaitez utiliser pour transférer le fichier de sauvegarde vers le serveur de sauvegarde externe.
7. Dans le champ **Chemin du répertoire**, saisissez le chemin du répertoire sur le serveur de sauvegarde externe sur lequel vous souhaitez stocker les fichiers de sauvegarde.
8. Sélectionnez **Supprimer le fichier du service de gestion** pour supprimer le fichier de sauvegarde de l'appliance SDX après avoir transféré le fichier de sauvegarde vers le serveur de sauvegarde externe.
9. Cliquez sur **OK**.

Restaurer l'appareil

Vous pouvez restaurer l'appliance SDX selon la configuration disponible dans le fichier de sauvegarde. Lors de la restauration de l'appliance, toute la configuration actuelle est supprimée.

Points à noter :

- Avant de restaurer l'appliance SDX à l'aide du fichier de sauvegarde d'une autre appliance SDX, ajoutez les paramètres réseau du service de gestion en fonction des paramètres disponibles dans le fichier de sauvegarde.
- Assurez-vous que la variante de plate-forme sur laquelle la sauvegarde a été effectuée est la même que celle sur laquelle vous essayez de restaurer. La restauration du fichier de sauvegarde entre deux variantes de plate-forme différentes n'est pas prise en charge.
- Citrix recommande de restaurer la sauvegarde SDX uniquement après la définition de la configuration réseau. Vous pouvez spécifier les paramètres réseau suivants pour SVM :
  - Adresse IP de SVM
  - Adresse IP de l'hyperviseur
  - Masque de sous-réseau
  - Gateway
  - Serveur DNS

Restaurer l'appliance à partir du fichier de sauvegarde

1. Dans l'onglet **Configuration**, dans le volet de navigation, développez **Service de gestion**, puis cliquez sur **Fichiers de sauvegarde**.
2. Dans le volet **Fichiers de sauvegarde**, cliquez sur le fichier de sauvegarde, puis sur **OK**.

3. Dans la boîte de dialogue**Restaurer**, sélectionnez**Restauration du matériel**, puis cliquez sur **Continuer**.

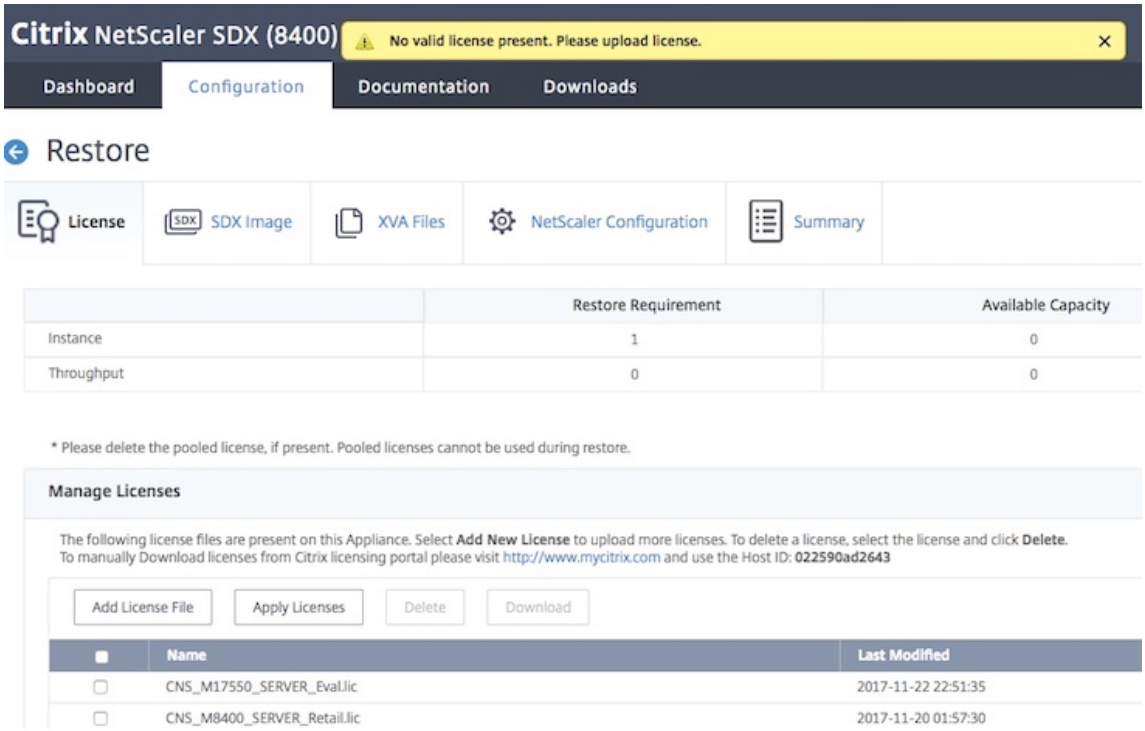
   Les différents composants de la restauration de l'application sont affichés :

   - Licence
   - Image SDX
   - Fichiers XVA
   - Configuration de Citrix ADC
   - Résumé

   Si l'un des composants requis est manquant dans le fichier de sauvegarde, vous êtes invité à télécharger l'élément manquant avant de poursuivre.

   Pour savoir si un fichier de sauvegarde peut être restauré sur la version d'image SDX Single Bundle actuelle, reportez-vous au tableau suivant. En règle générale pour l'image d'ensemble unique, aucune sauvegarde de version inférieure ne peut pas être restaurée sur une version ultérieure.

Version actuelle de l'image SDX Single Bundle	Version du fichier de sauvegarde
11.1	11.1, 12.0, 12.1, 13.0 pris en charge ; 11.0 non pris en charge
12.0	12.0, 12.1, 13.0 pris en charge ; 11.0 et 11.1 non pris en charge
12.1	12.1, 13.0 pris en charge, 11.0, 11.1, 12.0 non pris en charge
13.0	13.0 pris en charge ; 11.0, 11.1, 12.0, 12.1 non pris en charge
13.1	13.1 pris en charge ; 11.0, 11.1, 12.0, 12.1, 13.0 non pris en charge



4. Sur la page **Licence**, vérifiez qu'une licence valide est présente et cliquez sur **Suivant**.
5. La page **Image SDX** s'affiche. Si aucune image SDX n'est requise pour effectuer la restauration, cliquez sur **Suivant**. Sinon, lorsque vous y êtes invité, téléchargez une image SDX valide et cliquez sur **Suivant**.
6. La page **Fichier XVA** s'ouvre. Cliquez sur **Suivant** si des images XVA pour toutes les instances sont présentes. Si le fichier XVA d'une instance est absent du fichier de sauvegarde, vous pouvez le télécharger ou ignorer la restauration de cette instance. Cliquez sur **Suivant** pour passer à la page suivante.
7. La page Configuration de Citrix ADC s'ouvre. Les fichiers de configuration Citrix ADC ne sont pas obligatoires. Vous pouvez mettre en service l'instance sans restaurer sa configuration. Si le fichier de configuration Citrix ADC est manquant dans le fichier de sauvegarde, vous pouvez procéder uniquement au provisionnement d'instance ou ignorer la restauration de l'instance. Cliquez sur **Suivant** pour passer à la page suivante.
8. La page récapitulative s'affiche avec les détails suivants concernant toutes les instances présentes dans le fichier de sauvegarde :
    - Adresse IP
    - Nom d'hôte
    - Version SDX
    - Version XVA
    - Embout de version

- Restaurer : si l'appliance ou l'instance est prête pour la restauration, une coche apparaît. Si ce n'est pas le cas, une croix apparaît.
- Messages d'erreur : si l'appliance ou l'instance n'est pas prête pour la restauration, un message d'erreur s'affiche pour expliquer la raison.

9. Cliquez sur **Restaurer** pour terminer le processus de restauration de l'application.

Restaurer l'instance Citrix ADC

Vous pouvez restaurer l'instance Citrix ADC dans l'appliance SDX sur les instances Citrix ADC disponibles dans le fichier de sauvegarde.

Remarque : une instance VPX ne parvient pas à être restaurée si :

- Aucune carte réseau de gestion n'est affectée à l'instance, et
- L'instance est gérée à partir du service de gestion SDX uniquement via LACP.
  La restauration échoue car le service de gestion SDX ne peut pas restaurer les configurations de canal automatiquement. Pour éviter ce problème, restaurez manuellement la configuration du canal pour terminer la restauration de l'instance VPX.

Pour restaurer l'instance Citrix ADC dans le fichier de sauvegarde :

1. Dans l'onglet **Configuration**, dans le volet de navigation, développez **Service de gestion**, puis cliquez sur **Fichiers de sauvegarde**.
2. Dans le volet **Fichiers de sauvegarde**, sélectionnez le fichier de sauvegarde, puis cliquez sur **Restaurer**.
3. Dans la boîte de dialogue **Restaurer**, sélectionnez**Restauration d'instance**.
4. Sélectionnez les instances Citrix ADC que vous souhaitez restaurer, puis cliquez sur **Poursuivre**.
5. (Facultatif) Si le fichier de sauvegarde est chiffré, tapez le mot de passe lorsque vous y êtes invité, puis cliquez sur**OK**.

> **Remarque**
>
> Assurez-vous qu'une configuration XVA, une image de construction et une configuration de canal appropriées sont présentes sur l'appliance SDX qui exécute l'instance en cours de restauration.

Effectuer une réinitialisation de l'appareil

January 27, 2022

L'appliance Citrix ADC SDX vous permet de :

- Réinitialisez la configuration de l'appliance.

> **Remarque :**
>
> Lorsque vous réinitialisez la configuration, vous devez vous connecter en utilisant le numéro de série du matériel comme mot de passe.

- Réinitialisez l'appliance à la version d'usine.
- Réinitialisez l'appliance sur une version d'image d'ensemble unique particulière.

Avant d'effectuer une réinitialisation de l'appliance, sauvegardez toutes les données stockées sur l'appliance, y compris les paramètres de toutes les instances Citrix ADC provisionnées sur l'appliance.

Citrix recommande de stocker les fichiers en dehors de l'appliance. L'exécution d'une réinitialisation du matériel met fin à toutes les sessions client en cours avec le service de gestion. Reconnectez-vous au service de gestion pour toutes les tâches de configuration supplémentaires. Lorsque vous êtes prêt à restaurer les données, importez les fichiers de sauvegarde à l'aide du service de gestion.

Le service de gestion propose les options suivantes pour réinitialiser l'appliance :

- Réinitialisation de configuration
- Réinitialisation d'usine
- Installation propre

Réinitialiser la configuration de l'appliance

Le service de gestion fournit l'option de réinitialisation de la configuration pour réinitialiser la configuration de l'appliance. L'option Config Reset effectue les opérations suivantes :

- Supprime les instances VPX.
- Supprime les fichiers clés et les certificats SSL.
- Supprime les fichiers d'archives techniques et de licence.
- Supprime la configuration NTP sur l'appliance.
- Rétablit le fuseau horaire sur UTC.
- Restaure les paramètres par défaut des stratégies de nettoyage et de sauvegarde.
- Supprime l'image du service de gestion.
- Supprime l'image Citrix ADC SDX.
- Supprime toutes les images XVA à l'exception du dernier fichier image auquel vous avez accédé sur l'appliance.
- Restaure les paramètres d'interface par défaut.
- Restaure la configuration par défaut de l'appliance, y compris les profils, les utilisateurs et les paramètres système par défaut.
- Restaure les mots de passe par défaut pour Citrix Hypervisor et le service de gestion.
- Redémarre le service de gestion.

Réinitialiser la configuration de l'appliance

1. Accédez au **groupe Configuration > Système > Administration du**système.
2. Cliquez sur**Réinitialisation du matériel**.
3. Dans la boîte de dialogue**Réinitialisation du matériel**, sélectionnez**Réinitialisation de la configuration**dans la liste**Type de réinitialisation** .
4. Cliquez sur **OK**.

Réinitialiser la version d'usine de l'appliance

Le service de gestion fournit l'option de réinitialisation aux paramètres d'usine pour réinitialiser l'appliance à la version d'usine. L'option Réinitialisation aux paramètres d'usine réinitialise les adresses IP actuelles du service de gestion et de Citrix Hypervisor sur les adresses IP par défaut du service de gestion et de Citrix Hypervisor.

Assurez-vous de sauvegarder toutes les données stockées sur l'appliance, y compris les paramètres de toutes les instances Citrix ADC provisionnées sur l'appliance. Citrix recommande de stocker les fichiers en dehors de l'appliance. L'exécution d'une réinitialisation d'usine met fin à toutes les sessions client en cours avec le service de gestion. Reconnectez-vous au service de gestion pour toutes les tâches de configuration supplémentaires. Lorsque vous êtes prêt à restaurer les données, importez les fichiers de sauvegarde à l'aide du service de gestion.

> **Important**
>
> Assurez-vous de connecter un câble de console série à l'appliance avant d'effectuer une réinitialisation aux paramètres d'usine.

Réinitialisez l'appliance à la version d'usine

1. Accédez à **Configuration > Système > Administration du système**.
2. Cliquez sur**Réinitialisation du matériel**.
3. Dans la boîte de dialogue **Réinitialisation du matériel**, sélectionnez **Réinitialisation aux paramètres d'usine** dans la liste **Type de réinitialisation** .
4. Cliquez sur **OK**.

Réinitialiser l'appliance à une seule version d'image groupée

Le service de gestion fournit l'option Installation propre qui vous permet d'installer une version arbitraire d'une seule image de bundle sur l'appliance. Il vous permet d'effectuer une nouvelle installation de l'image d'ensemble unique en tant que nouvelle image de démarrage par défaut. L'installation propre supprime la configuration existante, à l'exception des paramètres réseau, dans l'appliance SDX.

> **Remarque :**
>
> Si votre dispositif SDX a été livré avec la version logicielle 11.0 ou antérieure, l'installation propre vers la version 13.1 ou ultérieure échoue.

L'option d'installation propre est prise en charge sur les éléments suivants :

Version d'image d'un seul ensemble	Plateformes SDX
11.0.xx	SDX 14xxx, SDX 25xxx. **Remarque** : L'option d'installation propre est prise en charge sur les autres plates-formes SDX si elles disposent d'une partition d'usine 10G.
11.1.xx	SDX 14xxx, SDX 25xxx. **Remarque** : L'option d'installation propre est prise en charge sur les autres plates-formes SDX si elles ont une partition d'usine 10G
11.1.51.x	Toutes les plateformes SDX.
12.1.xx	Toutes les plateformes SDX.
13.0.xx	Toutes les plateformes SDX.
13.1.xx	Toutes les plateformes SDX.

Conditions préalables

Assurez-vous que :

- Vous basculez tous les nœuds haute disponibilité principaux vers un autre dispositif SDX. Si vous ne disposez pas de fonctionnalités de haute disponibilité, assurez-vous de planifier le temps d'arrêt en conséquence.
- Téléchargez l'image de l'ensemble unique sur votre machine locale.

> **Important :**
>
> Assurez-vous de ne pas redémarrer ou mettre hors tension l'appliance lorsque vous utilisez l'option Nettoyer l'installation.
> L'appliance est redémarrée plusieurs fois.

Réinitialiser l'appliance à une seule version d'image groupée

1. Accédez au groupe **Configuration > Système > Administration** du système.
2. Cliquez sur**Réinitialisation du matériel**.

3. Dans la boîte de dialogue **Réinitialisation du matériel**, sélectionnez **Installation propre** dans la liste **Type de réinitialisation** .
4. Cliquez sur **OK**.

Serveurs d'authentification externes en cascade

April 8, 2022

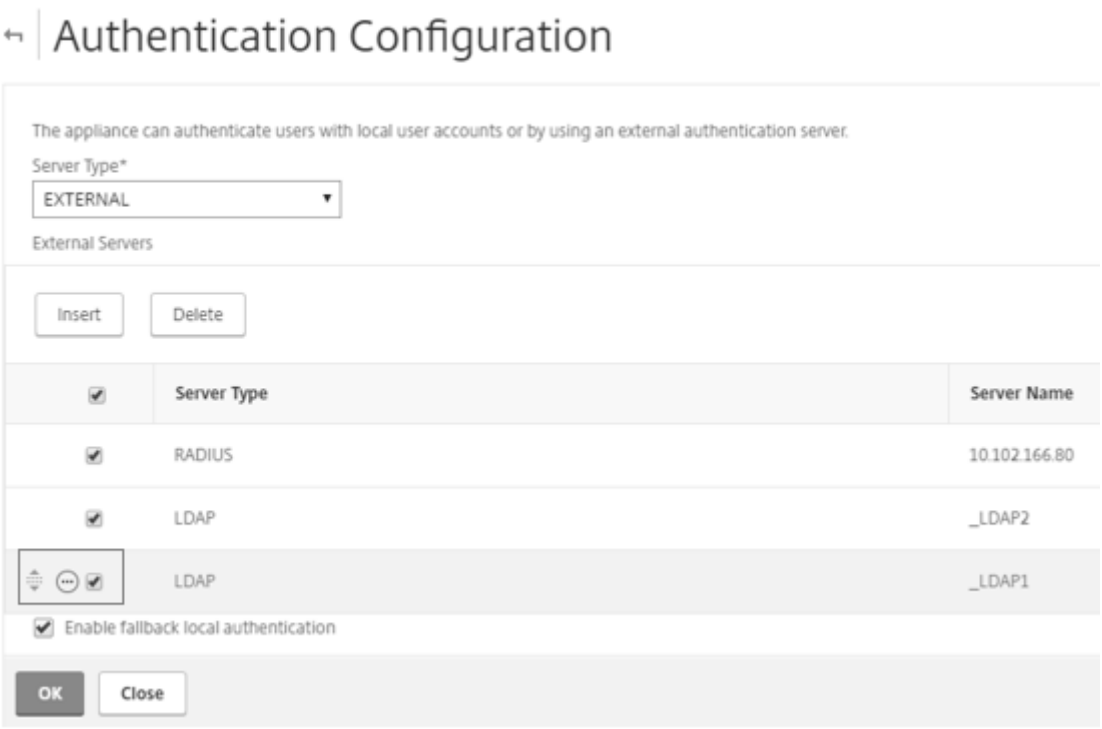
La mise en cascade de plusieurs serveurs d'authentification externes fournit un processus continu et fiable d'authentification et d'autorisation des utilisateurs externes. Si l'authentification échoue sur le premier serveur d'authentification, le service de gestion tente d'authentifier l'utilisateur à l'aide du deuxième serveur d'authentification externe.

Pour activer l'authentification en cascade, ajoutez les serveurs d'authentification externes au service de gestion. Pour plus d'informations, consultez Configuration de l'authentification externe. Vous pouvez ajouter n'importe quel type de serveurs d'authentification externes pris en charge (RADIUS, LDAP et TACACS). Par exemple, pour ajouter quatre serveurs d'authentification externes pour l'authentification en cascade, vous pouvez ajouter n'importe quelle combinaison de serveurs RADIUS, LDAP et TACACS. Vous pouvez également ajouter les quatre serveurs du même type. Vous pouvez configurer jusqu'à 32 serveurs d'authentification externes dans Citrix Application Delivery Management.

Serveurs d'authentification externes Cascade

1. Dans l'onglet **Configuration**, sous **Système**, développez **Authentification**.
2. Sur la page **Authentification**, cliquez sur **Configuration de l'authentification**.
3. Sur la page **Configuration de l'authentification**, sélectionnez **EXTERNE** dans la liste déroulante **Type de serveur** (vous ne pouvez monter en cascade que des serveurs externes).
4. Cliquez sur **Insérer**, puis sur la page **Serveurs externes** qui s'ouvre, sélectionnez un ou plusieurs serveurs d'authentification que vous souhaitez mettre en cascade.
5. Cliquez sur **OK**.

Les serveurs sélectionnés sont affichés sur la page **Serveurs d'authentification**, comme illustré dans la figure suivante. Pour modifier l'ordre d'authentification, utilisez l'icône en regard du nom d'un serveur pour déplacer le serveur vers le haut ou vers le bas de la liste.



Déverrouiller un utilisateur

January 27, 2022

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

Déverrouiller un utilisateur en utilisant l'interface graphique

1. Accédez à **Configuration > Système > Administration des utilisateurs > Utilisateurs**.
2. Sélectionnez l'utilisateur à déverrouiller.
3. Cliquez sur **Déverrouiller**.

Déverrouiller un utilisateur à l'aide du CLI

À l'invite de commandes, tapez :

```
set systemuser id=<ID> unlock=true
```


Provisionner des instances Citrix ADC

January 6, 2023

> **Remarque**
>
> La connexion au service Citrix ADM est activée par défaut, après avoir installé ou mis à niveau l'appliance Citrix ADC SDX vers la version 13.1. Pour plus de détails, consultez la section Gouvernance des données et connexion au service Citrix ADM.

Vous pouvez mettre en service une ou plusieurs instances Citrix ADC sur l'appliance SDX à l'aide du service de gestion. Le nombre d'instances que vous pouvez installer dépend de la licence que vous avez achetée. Si le nombre d'instances ajoutées est égal au nombre spécifié dans la licence, le service de gestion n'autorise pas le provisionnement d'autres instances Citrix ADC.

> **Remarque :**
>
> Vous pouvez configurer jusqu'à 20 instances VPX sur une interface réseau indépendante de la plate-forme matérielle sous-jacente.

Le provisionnement d'une instance Citrix ADC VPX sur l'appliance SDX comprend les étapes suivantes.

1. Définissez un profil d'administrateur à attacher à l'instance Citrix ADC. Ce profil spécifie les informations d'identification de l'utilisateur qui sont utilisées par le service de gestion pour provisionner l'instance ADC et les versions ultérieures, pour communiquer avec l'instance afin de récupérer les données de configuration. Vous pouvez également utiliser le profil d'administrateur par défaut.
2. Téléchargez le fichier image .xva vers le service de gestion.
3. Ajoutez une instance Citrix ADC à l'aide de l'assistant Provisionner Citrix ADC dans le service de gestion. Le service de gestion déploie implicitement l'instance Citrix ADC sur l'appliance SDX, puis télécharge les détails de configuration de l'instance.

> **Avertissement**
>
> Assurez-vous de modifier les interfaces réseau provisionnées ou les VLAN d'une instance à l'aide du service de gestion au lieu d'effectuer les modifications directement sur l'instance.

Créer un profil d'administrateur

Les profils d'administrateur spécifient les informations d'identification de l'utilisateur qui sont utilisées par le service de gestion lors du provisionnement des instances Citrix ADC. Ces informations d'identification sont utilisées ultérieurement lors de la communication avec les instances pour récupérer les données de configuration. Les informations d'identification utilisateur spécifiées dans un profil d'administrateur sont également utilisées par le client lors de la connexion aux instances Citrix ADC via l'interface de ligne de commande ou l'interface graphique.

Les profils d'administrateur vous permettent également de spécifier que le service de gestion et une instance VPX communiquent entre eux uniquement via un canal sécurisé ou via HTTP.

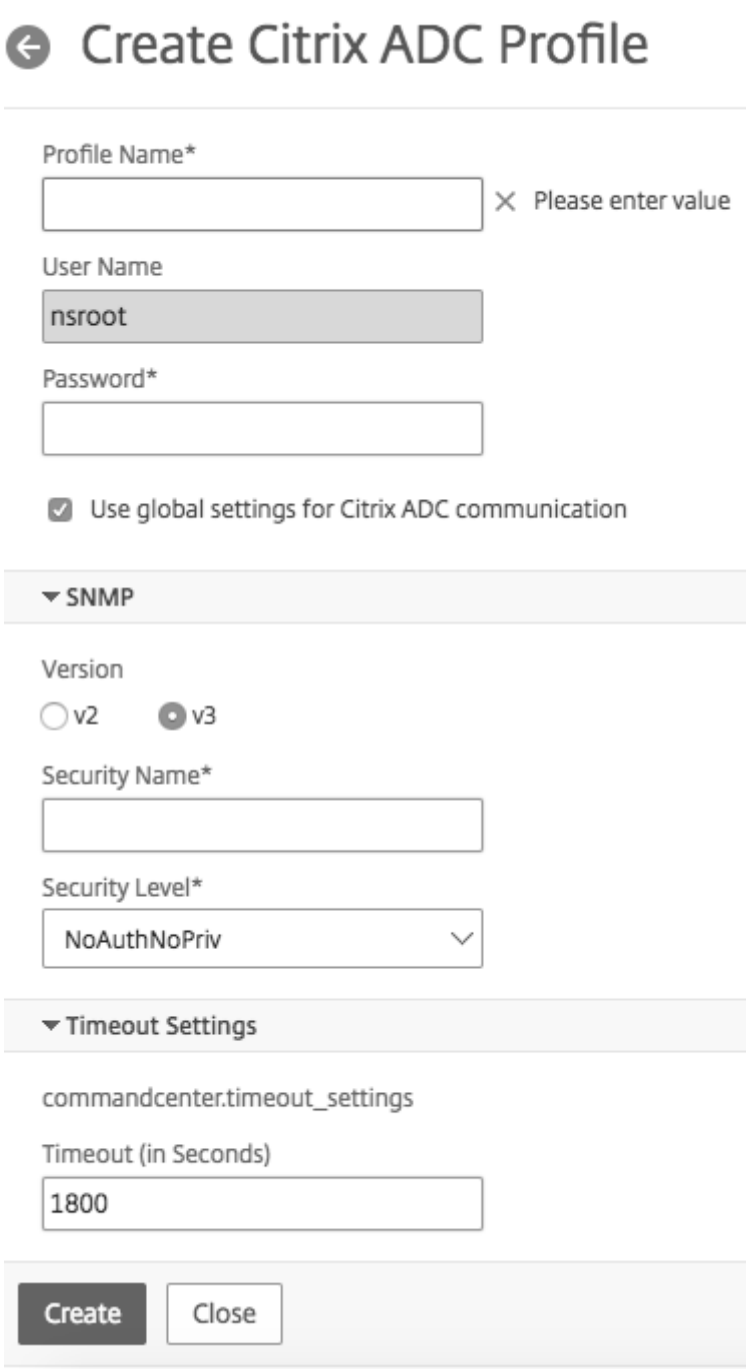
Le profil d'administrateur par défaut d'une instance spécifie le nom d'utilisateur administrateur par défaut. Ce profil ne peut être ni modifié ni supprimé. Toutefois, vous devez remplacer le profil par défaut en créant un profil d'administrateur défini par l'utilisateur et en l'attachant à l'instance lorsque vous provisionnez l'instance. L'administrateur du service de gestion peut supprimer un profil d'administrateur défini par l'utilisateur s'il n'est associé à aucune instance Citrix ADC.

> **Important**
>
> Ne modifiez pas le mot de passe directement sur l'instance VPX. Dans ce cas, l'instance devient inaccessible à partir du service de gestion. Pour modifier un mot de passe, créez d'abord un profil d'administrateur, puis modifiez l'instance Citrix ADC, en sélectionnant ce profil dans la liste Profil d'administrateur.

Pour modifier le mot de passe des instances Citrix ADC dans une configuration haute disponibilité, modifiez d'abord le mot de passe sur l'instance désignée comme nœud secondaire. Modifiez ensuite le mot de passe sur l'instance désignée comme nœud principal. N'oubliez pas de modifier les mots de passe uniquement à l'aide du service de gestion.

Créer un profil d'administrateur

1. Dans l'onglet **Configuration**, dans le volet de navigation, développez **Configuration Citrix ADC**, puis cliquez sur **Profils d'administration**.
2. Dans le volet **Profils d'administration**, cliquez sur **Ajouter**.
3. La boîte **de dialogue Créer un profil d'administrateur** s'affiche.



Définissez les paramètres suivants :

- Nom du profil : nom du profil administrateur. Le nom du profil par défaut est `nsroot`. Vous pouvez créer des noms de profil définis par l'utilisateur.
- Mot de passe : mot de passe utilisé pour se connecter à l'instance Citrix ADC. Longueur maximale : 31 caractères.
- Port SSH : définissez le port SSH. Le port par défaut est 22.

- **Utiliser les paramètres globaux pour la communication Citrix ADC :** sélectionnez cette option si vous souhaitez que le paramètre soit défini dans les paramètres système pour la communication entre le service de gestion et l'instance Citrix ADC. Vous pouvez désactiver cette case et modifier le protocole en HTTP ou HTTPS.
  - Sélectionnez l'option **http** pour utiliser le protocole HTTP pour la communication entre le service de gestion et l'instance Citrix ADC.
  - Sélectionnez l'option **https** pour utiliser le canal sécurisé pour la communication entre le service de gestion et l'instance Citrix ADC.

4. Sous **SNMP**, sélectionnez la version. Si vous sélectionnez v2, passez à l'étape 5. Si vous sélectionnez v3, passez à l'étape 6.

5. Sous SNMP v2, ajoutez le nom de la **communauté** SNMP.

6. Sous SNMP v3, ajoutez le **nom de sécurité** et le **niveau de sécurité**.

7. Sous **Paramètres du délai**d'expiration, spécifiez la valeur.

8. Cliquez sur **Créer**, puis sur **Fermer**. Le profil d'administrateur que vous avez créé s'affiche dans le volet **Profils d'administration** .

Si la valeur de la colonne **Par défaut** est true, le profil par défaut est le profil administrateur. Si la valeur est false, un profil défini par l'utilisateur est le profil administrateur.

Si vous ne souhaitez pas utiliser un profil d'administrateur défini par l'utilisateur, vous pouvez le supprimer du service de gestion. Pour supprimer un profil administrateur défini par l'utilisateur, dans le volet **Profils d'administration**, sélectionnez le profil que vous souhaitez supprimer, puis cliquez sur **Supprimer**.

Charger une image .xva Citrix ADC

Un fichier .xva est requis pour ajouter une instance Citrix ADC VPX.

Téléchargez les fichiers .xva Citrix ADC SDX sur l'appliance SDX avant de provisionner les instances VPX. Vous pouvez également télécharger un fichier image .xva sur un ordinateur local en tant que sauvegarde. Le format de fichier image .xva est : `NSVPX-XEN-ReleaseNumber-BuildNumber_nc` .xva.

Dans le volet **Citrix ADC XVA Files**, vous pouvez afficher les détails suivants.

- **Nom :** nom du fichier image .xva. Le nom du fichier contient la version et le numéro de version. Par exemple, le nom de fichier `NSVPX-XEN-12.1-56.22.xva.gz` fait référence à la version 12.1 build 56.22.
- **Dernière modification :** date à laquelle le fichier image .xva a été modifié pour la dernière fois.
- **Taille :** taille, en Mo, du fichier image .xva.

Pour télécharger un fichier .xva Citrix ADC

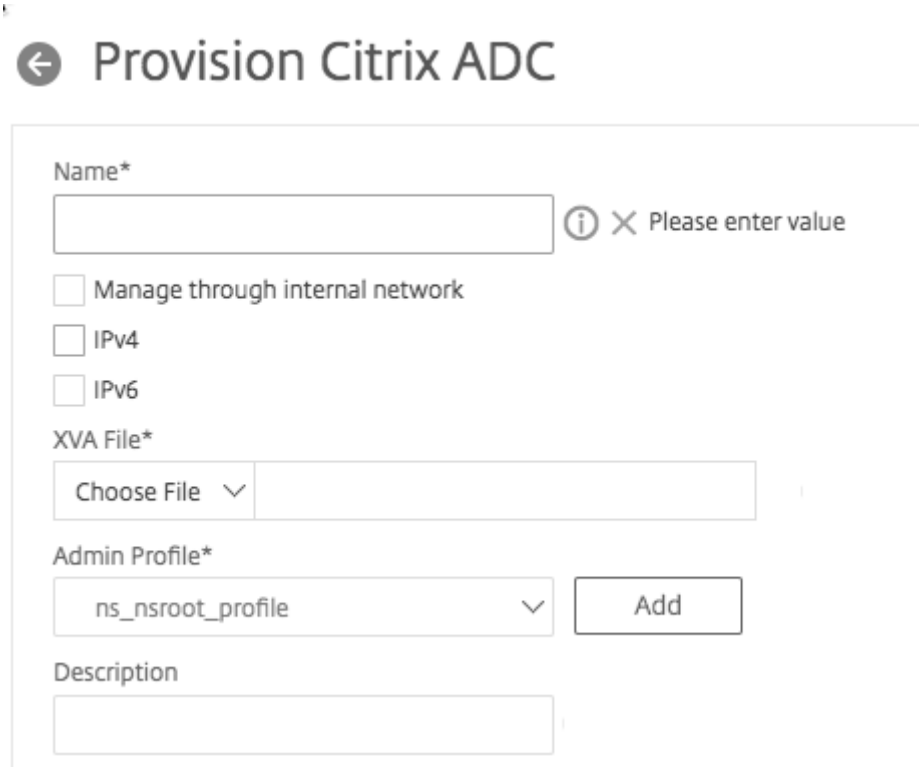
1. Dans l'onglet **Configuration**, dans le volet de navigation, développez **Configuration Citrix ADC**, puis cliquez sur **Fichiers XVA**.
2. Dans le volet **Citrix ADC XVA Files**, cliquez sur **Upload**.
3. Dans la boîte de dialogue **Upload Citrix ADC instance XVA**, cliquez sur **Parcourir** et sélectionnez le fichier image XVA que vous souhaitez télécharger.
4. Cliquez sur **Charger**. Le fichier image XVA s'affiche dans le volet **Fichiers XVA Citrix ADC** après son chargement.

Pour créer une sauvegarde en téléchargeant un fichier Citrix ADC .xva

1. Dans le volet **Fichiers de génération Citrix ADC**, sélectionnez le fichier que vous souhaitez télécharger, puis cliquez sur **Télécharger**.
2. Dans la zone de message **Téléchargement de fichier**, cliquez sur **Enregistrer**.
3. Dans la zone de message **Enregistrer sous**, accédez à l'emplacement où vous souhaitez enregistrer le fichier, puis cliquez sur **Enregistrer**.

Ajouter une instance Citrix ADC

Lorsque vous ajoutez des instances Citrix ADC à partir du service de gestion, vous devez fournir des valeurs pour certains paramètres. Le service de gestion configure implicitement ces paramètres sur les instances Citrix ADC.



- **Nom** : attribuez un nom à l'instance Citrix ADC.
- Sélectionnez **Gérer via le réseau interne** pour activer une connectivité interne indépendante permanente entre le service de gestion SDX et l'instance VPX. Cette fonctionnalité est prise en charge dans les versions 13.0-36.27 et supérieures des instances VPX exécutées sur l'appliance SDX.
- Sélectionnez une adresse IPv4 ou IPv6 ou des adresses IPv4 et IPv6 pour accéder à l'instance Citrix VPX à des fins de gestion. Une instance Citrix ADC ne peut avoir qu'une seule adresse IP de gestion (NSIP). Vous ne pouvez pas supprimer une adresse NSIP.
- Attribuez un masque de réseau, une passerelle par défaut et l'étape suivante au service de gestion pour l'adresse IP.
- Les champs **Gateway** et **Nexthop to Management Service** sont facultatifs dans l'une des conditions suivantes, lorsque VPX est provisionné avec la version 13.0-88.9 ou 13.1-37.8, et leurs versions supérieures :
  - Lorsque la **gestion via le réseau interne** est activée.
  - Lorsque l'adresse IPv4 configurée se trouve dans le même sous-réseau que l'adresse IP du service de gestion.

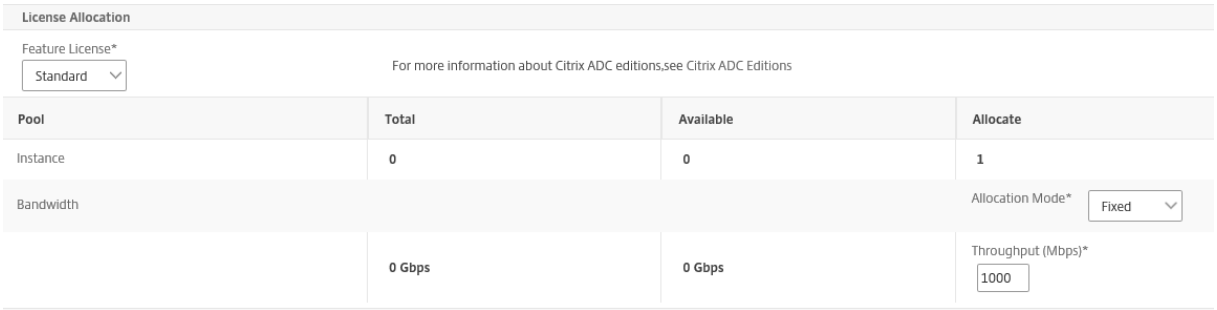
Ajoutez ensuite le fichier XVA, le profil d'administration et une description de l'instance.

Remarque : Pour une configuration haute disponibilité (actif-actif ou actif-veille), Citrix vous recommande de configurer les deux instances Citrix ADC VPX sur des appliances SDX différentes. Assurez-vous que les instances de l'installation disposent de ressources identiques, telles que le processeur, la mémoire, les interfaces, les paquets par seconde (PPS) et le débit.

Allocation de licences

Dans cette section, spécifiez la licence que vous avez obtenue pour Citrix ADC. La licence peut être Standard, Enterprise et Platinum.

Remarque : Un astérisque indique les champs obligatoires.



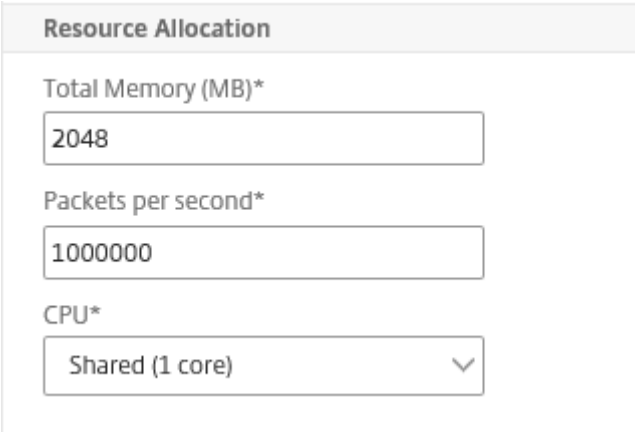
Si vous avez besoin d'une capacité d'éclatement de la bande passante, sélectionnez **Burstable** sous **Mode d'allocation**. Pour plus d'informations, consultez la section Mesure de la bande passante dans SDX.

Allocation cryptographique

À partir de la version 12.1 48.13, l'interface de gestion de la capacité de chiffrement a changé. Pour plus d'informations, consultez Gérer la capacité de chiffrement.

Allocation des ressources

Sous Allocation de ressources, affectez la mémoire totale, les paquets par seconde et le processeur.



CPU

Attribuez un ou plusieurs cœurs dédiés à l'instance, ou l'instance partage un cœur avec d'autres instances. Si vous sélectionnez Partagé, un cœur est affecté à l'instance, mais le cœur peut être partagé avec d'autres instances en cas de manque de ressources. Redémarrez les instances affectées si les cœurs de processeur sont réaffectés. Redémarrez les instances sur lesquelles les cœurs de processeur sont réaffectés pour éviter toute dégradation des performances.

À partir de la version SDX 11.1.x.x (MR4), si vous utilisez la plate-forme SDX 25000xx, vous pouvez attribuer un maximum de 16 cœurs à une instance. De plus, si vous utilisez la plate-forme SDX 2500xxx, vous pouvez affecter un maximum de 11 cœurs à une instance.

Remarque : Pour une instance, le débit maximal que vous configurez est de 180 Gbit/s.

Le tableau suivant répertorie le VPX pris en charge, la version d'image d'ensemble unique et le nombre de cœurs que vous pouvez attribuer à une instance :

Nom de la plateforme	Nombre total de noyaux	Nombre total de cœurs disponibles pour le provisionnement VPX	Nombre maximal de cœurs pouvant être affectés à une seule instance
SDX 8015, SDX 8400 et SDX 8600	4	3	3
SDX 8900	8	7	7
SDX 11500, SDX 13500, SDX 14500, SDX 16500, SDX 18500 et SDX 20500	12	10	5

Nom de la plateforme	Nombre total de noyaux	Nombre total de cœurs disponibles pour le provisionnement VPX	Nombre maximal de cœurs pouvant être affectés à une seule instance
SDX 11515, SDX 11520, SDX 11530, SDX 11540 et SDX 11542	12	10	5
SDX 17500, SDX 19500 et SDX 21500	12	10	5
SDX 17550, SDX 19550, SDX 20550 et SDX 21550	12	10	5
SDX 14020, SDX 14030, SDX 14040, SDX 14060, SDX 14080 et SDX 14100	12	10	5
SDX 22040, SDX 22060, SDX 22080, SDX 22100 et SDX 22120	16	14	7
SDX 24100 et SDX 24150	16	14	7
SDX 14020 40 G, SDX 14030 40 G, SDX 14040 40 G, SDX 14060 40 G, SDX 14080 40 G et SDX 14100 40 G	12	10	10
FIPS SDX 14020, FIPS SDX 14030, FIPS SDX 14040, FIPS SDX 14060, FIPS SDX 14080 et FIPS SDX 14100	12	10	5

Nom de la plateforme	Nombre total de noyaux	Nombre total de cœurs disponibles pour le provisionnement VPX	Nombre maximal de cœurs pouvant être affectés à une seule instance
SDX 14040 40S, SDX 14060 40S, SDX 14080 40S et SDX 14100 40S	12	10	10
SDX 25100A, 25160A, 25200A	20	18	9
SDX 25100-40G, 25160-40G, 25200-40G	20	18	16 (si la version est 11.1-51.x ou supérieure) ; 9 (si la version est 11.1-50.x ou inférieure ; toutes les versions de 11.0 et 10.5)
SDX 26100, 26160, 26200, 26250	28	26	16
SDX 26100-50S, 26160-50S, 26200-50S, 26250-50S	28	26	16
SDX 26100-100 G, 26160-100 G, 26200-100 G, 26250-100 G	28	26	25
SDX 15000	16	14	14
SDX 15000-50G	16	14	14
SDX 9100	10	9	9
SDX 16000	32	30	16

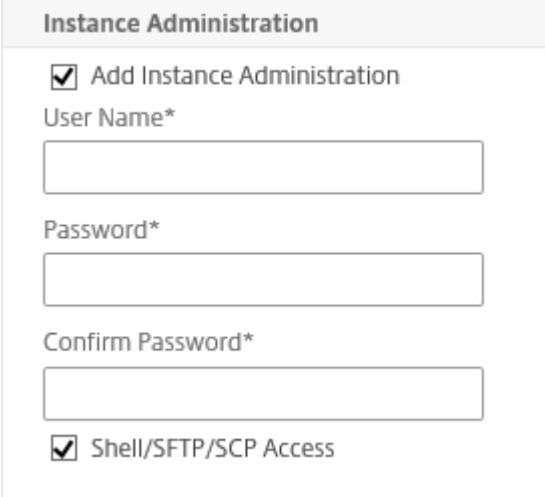
Remarque :

Pour les versions de Citrix ADC antérieures à 13.1-24.x, un maximum de 26 cœurs de processeur peuvent être attribués à une instance VPX sur la plate-forme SDX 26000. À partir de la version 13.1-24.x, un maximum de 25 cœurs de processeur peuvent être attribués à une instance VPX sur la plate-forme SDX 26000. Toutefois, si des unités de chiffrement sont affectées à l'instance,

> le nombre maximum de cœurs dépend du nombre d'unités cryptographiques et d'interfaces de données. Par exemple, si vous affectez 24000 unités de chiffrement à une instance, vous pouvez affecter 24 cœurs de CPU et deux interfaces de données maximum à l'instance. L'appliance SDX considère les interfaces de données et les unités de chiffrement comme des périphériques PCI. Avec 26 000 unités de chiffrement, une instance VPX ne peut pas être provisionnée car il n'y a pas de place pour les interfaces de données.

Administration des instances

Vous pouvez créer un utilisateur administrateur pour l'instance VPX en sélectionnant **Add Instance Administration sous Administration** de **l'instance**.



Ajoutez les informations suivantes :

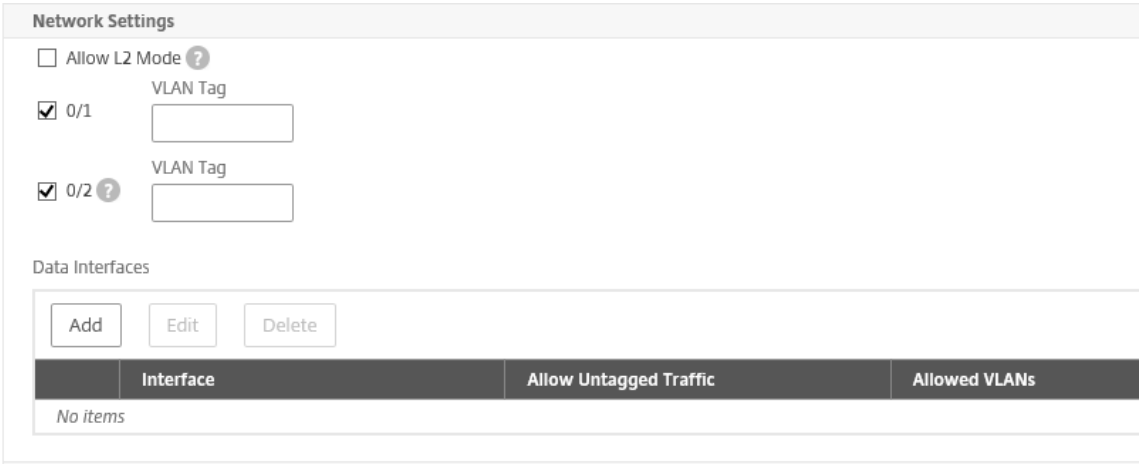
Nom d'utilisateur : nom d'utilisateur de l'administrateur de l'instance Citrix ADC. Cet utilisateur dispose d'un accès superutilisateur mais n'a pas accès aux commandes réseau pour configurer les VLAN et les interfaces.

Mot de passe : mot de passe associé au nom d'utilisateur.

Accès**Shell/Sftp/Scp :** accès autorisé à l'administrateur de l'instance Citrix ADC. Cette option est sélectionnée par défaut.

Paramètres réseau

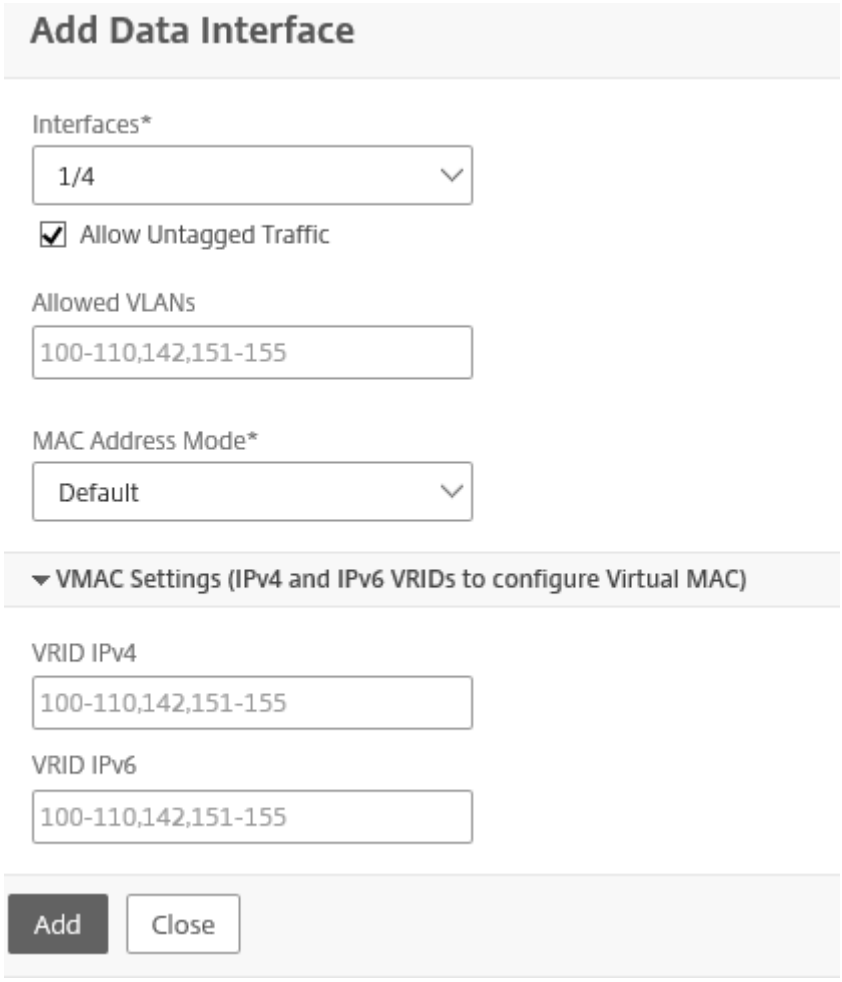
- **Autoriser le mode L2 :** vous pouvez autoriser le mode L2 sur l'instance Citrix ADC. Sélectionnez **Autoriser le mode L2** sous **Paramètres réseau**. Avant de vous connecter à l'instance et d'activer le mode L2. Pour plus d'informations, consultez Autorisation du mode L2 sur une instance Citrix ADC.



> **Remarque :**
>
> – Si vous désactivez le mode L2 pour une instance à partir du service de gestion, vous devez vous connecter à l'instance et désactiver le mode L2 à partir de cette instance. Si vous ne le faites pas, tous les autres modes Citrix ADC risquent d'être désactivés après le redémarrage de l'instance.
> – Une fois qu'une instance ADC est provisionnée sur SDX, vous ne pouvez pas supprimer une interface ou un canal de l'instance ADC. Vous pouvez toutefois ajouter une nouvelle interface ou un nouveau canal à l'instance ADC.

- **Interface 0/1 et 0/2 :** Par défaut, les interfaces 0/1 et 0/2 sont sélectionnées pour la gestion LA.
- **Balise VLAN :** Spécifiez un ID VLAN pour l'interface de gestion. Ajoutez ensuite des interfaces de données.

> **Remarque** :
>
> Les ID d'interface des interfaces que vous ajoutez à une instance ne correspondent pas nécessairement à la numérotation de l'interface physique sur l'appliance SDX. Si la première interface que vous associez à l'instance 1 est l'interface 1/4, elle apparaît comme interface 1/1 lorsque vous affichez les paramètres d'interface sur l'instance. La numérotation change car il s'agit de la première interface que vous avez associée à l'instance 1.



- **Autoriser le trafic non marqué :** cochez la case **Autoriser le trafic non marqué** pour permettre à l'instance Citrix ADC de traiter le trafic non marqué.

  > **Remarque :**
  >
  > Lorsque la version de l'appliance SDX est 13.1-24.x ou ultérieure et que la version de l'instance Citrix ADC est antérieure à 13.1-24.x, l'instance ADC traite le trafic non marqué sur les interfaces Mellanox même si la case à cocher **Autoriser le trafic non marqué** est désactivée.

- **VLAN autorisés :**spécifiez une liste d'ID de VLAN pouvant être associés à une instance Citrix ADC.
- **Mode adresse MAC :** attribuez une adresse MAC. Sélectionnez l'une des options suivantes :
  - **Par défaut :** Citrix Hypervisor attribue une adresse MAC.
  - **Personnalisé :** choisissez ce mode pour spécifier une adresse MAC qui remplace l'adresse MAC générée.
  - **Généré :** générez une adresse MAC à l'aide de l'adresse MAC de base définie précédemment. Pour plus d'informations sur la définition d'une adresse MAC de base, reportez-vous

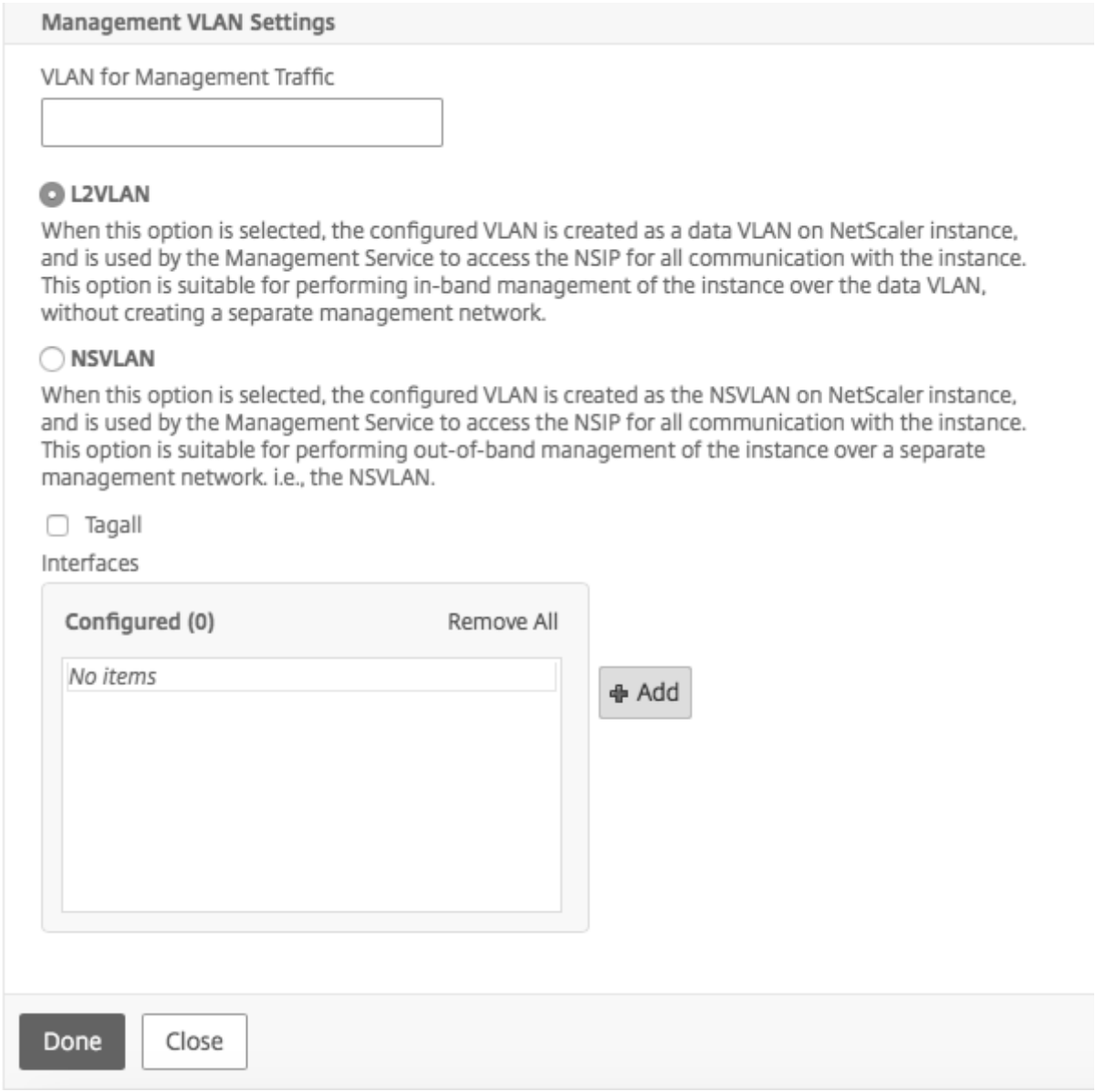
à la section Attribution d'une adresse MAC à une interface.

- Paramètres VMAC (VRID IPv4 et IPv6 pour configurer Virtual MAC)
  - **VRID IPV4 :** VRID IPv4 qui identifie le VMAC. Valeurs possibles : 1—255. Pour plus d'informations, consultez Configuration de vMac sur une interface.
  - **VRID IPV6 :** VRID IPv6 qui identifie le VMAC. Valeurs possibles : 1—255. Pour plus d'informations, consultez Configuration de vMac sur une interface.

Paramètres du VLAN de gestion

En règle générale, le service de gestion et l'adresse de gestion (NSIP) de l'instance VPX se trouvent dans le même sous-réseau, et la communication s'effectue via une interface de gestion. Toutefois, si le service de gestion et l'instance se trouvent dans des sous-réseaux différents, vous devez spécifier un ID de VLAN au moment du provisionnement d'une instance VPX. Cet ID est requis pour que l'instance soit joignable sur le réseau lorsqu'elle démarre. Si votre déploiement nécessite que le NSIP soit accessible uniquement par l'interface sélectionnée au moment du provisionnement de l'instance VPX, sélectionnez l'option NSVLAN.

Si l'option **NSVLAN** est sélectionnée, vous ne pouvez pas modifier ce paramètre après avoir provisionné l'instance Citrix ADC.



Remarque :

- Les battements de cœur HA sont envoyés uniquement sur les interfaces qui font partie du NSVLAN.
- Vous pouvez configurer un NSVLAN uniquement à partir de VPX XVA build 9.3 53.4 et versions ultérieures.

Important : Si NSVLAN n'est pas sélectionné, l'exécution de la commande « clear config full » sur l'instance VPX supprime la configuration du VLAN.

Cliquez sur **Terminé** pour provisionner l'appliance Citrix ADC VPX.

Modifier une instance Citrix ADC

Pour modifier les valeurs des paramètres d'une instance ADC provisionnée, dans le volet **Instances Citrix ADC**, sélectionnez l'instance que vous souhaitez modifier, puis cliquez sur **Modifier**. Dans l'Assistant Modification du CAN, modifiez les paramètres.

Points à noter :

- Si vous modifiez les paramètres suivants : nombre de puces SSL, interfaces, mémoire et licence des fonctionnalités, l'instance Citrix ADC s'arrête et redémarre implicitement pour que ces paramètres prennent effet.
- Vous ne pouvez pas modifier les paramètres Image et Nom d'utilisateur.
- Les interfaces ou les canaux ne peuvent pas être supprimés de l'instance ADC. Toutefois, de nouvelles interfaces ou de nouveaux canaux peuvent être ajoutés à l'instance ADC.
- Pour supprimer une instance ADC provisionnée sur l'appliance SDX, dans le volet **Instances Citrix ADC**, sélectionnez l'instance que vous souhaitez supprimer, puis cliquez sur **Supprimer**. Dans la zone de message **Confirmer**, cliquez sur **Oui** pour supprimer l'instance Citrix ADC.

Restreindre les VLAN à des interfaces virtuelles spécifiques

L'administrateur de l'appliance SDX peut appliquer des VLAN 802.1Q spécifiques sur les interfaces virtuelles associées aux instances Citrix ADC. Cette fonctionnalité est particulièrement utile pour restreindre l'utilisation des VLAN 802.1Q par les administrateurs d'instance. Si deux instances appartenant à deux sociétés différentes sont hébergées sur une appliance SDX, vous pouvez empêcher les deux sociétés d'utiliser le même ID de VLAN. Ce faisant, une entreprise ne voit pas le trafic de l'autre. Si un administrateur d'instance essaie d'attribuer une interface à un VLAN 802.1Q, une validation est effectuée pour vérifier que l'ID de VLAN spécifié fait partie de la liste autorisée.

Par défaut, n'importe quel ID de VLAN peut être utilisé sur une interface. Pour restreindre les VLAN balisés sur une interface, spécifiez les ID de VLAN dans les paramètres réseau au moment du provisionnement d'une instance Citrix ADC. Vous pouvez également le spécifier ultérieurement en modifiant l'instance. Pour spécifier une plage, séparez les ID par un trait d'union (par exemple 10 à 12). Si vous spécifiez initialement certains ID de VLAN, puis que vous les supprimez tous de la liste autorisée, vous pouvez utiliser n'importe quel ID de VLAN sur cette interface. En fait, vous avez rétabli le réglage par défaut.

Après avoir créé une liste de VLAN autorisés, l'administrateur SDX n'a pas besoin de se connecter à une instance pour créer les VLAN. L'administrateur peut ajouter et supprimer des VLAN pour des instances spécifiques à partir du service de gestion.

Important : Si le mode L2 est activé, l'administrateur doit veiller à ce que les ID de VLAN sur différentes instances Citrix ADC ne se chevauchent pas.

Pour spécifier les ID de VLAN autorisés

1. Dans l'Assistant Provisionnement ADC ou l'Assistant Modification du CAN, sur la page Paramètres réseau, dans **VLAN autorisés**, spécifiez un ou plusieurs ID de VLAN autorisés sur cette interface. Utilisez un trait d'union pour spécifier une plage. Par exemple, 2—4094.
2. Suivez les instructions de l'assistant.
3. Cliquez sur **Terminer**, puis sur **Fermer**.

Pour configurer des VLAN pour une instance à partir du service de gestion

1. Dans l'onglet **Configuration**, accédez à Citrix ADC > Instances.
2. Sélectionnez une instance, puis cliquez sur **VLAN**.
3. Dans le volet d'informations, cliquez sur **Ajouter**.
4. Dans la boîte de dialogue **Créer un VLAN Citrix ADC**, spécifiez les paramètres suivants :
    - ID VLAN : nombre entier qui identifie de manière unique le VLAN auquel appartient une trame particulière. Le Citrix ADC prend en charge un maximum de 4094 VLAN. L'ID 1 est réservé au VLAN par défaut.
    - Routage dynamique IPV6 : activez tous les protocoles de routage dynamique IPv6 sur ce VLAN. Remarque : Pour que le paramètre **ENABLED** fonctionne, vous devez vous connecter à l'instance et configurer les protocoles de routage dynamique IPv6 à partir de la ligne de commande VTYSH.
5. Sélectionnez les interfaces qui doivent faire partie du VLAN.
6. Cliquez sur **Créer**, puis sur **Fermer**.

Gérer la capacité crypto

July 12, 2022

À partir de la version 12.1 48.13, l'interface de gestion de la capacité de chiffrement a changé. Le service de gestion fournit des unités cryptographiques asymétriques (ACU), des unités cryptographiques symétriques (SCU) et des interfaces virtuelles de chiffrement pour indiquer la capacité SSL sur l'appliance Citrix ADC SDX. Auparavant, la capacité de chiffrement était attribuée en unités de puces SSL, de cœurs SSL et de fonctions virtuelles SSL. Consultez le tableau de conversion des puces SSL héritées en unités ACU et SCU pour plus d'informations sur la façon dont les puces SSL héritées se traduisent en unités ACU et SCU.

À l'aide de l'interface graphique du service de gestion, vous pouvez allouer la capacité de chiffrement à l'instance Citrix ADC VPX en unités d'ACU et de SCU.

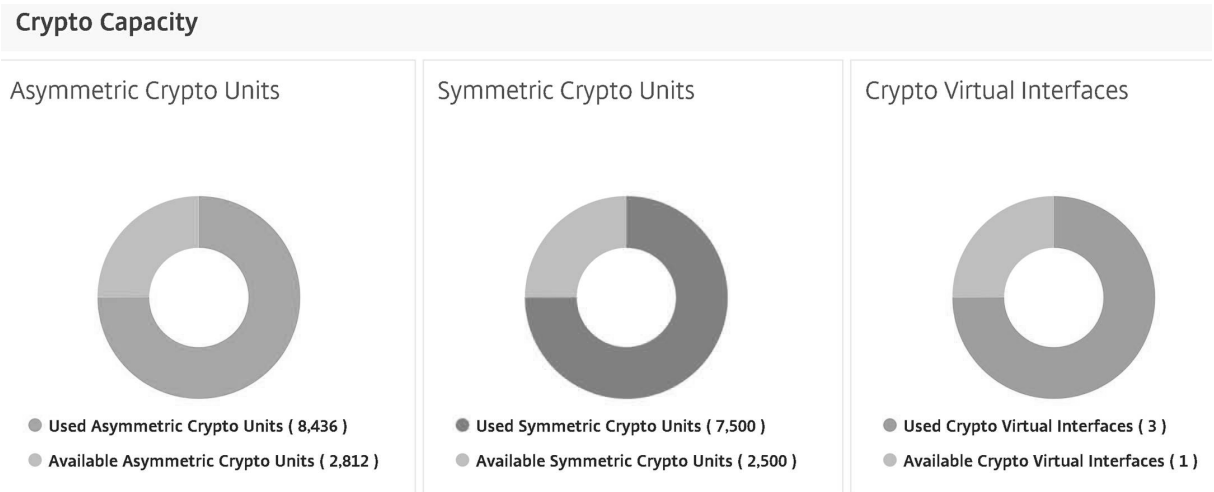
Le tableau suivant fournit de brèves descriptions des ACU, des SCU et des instances virtuelles de chiffrement.

Tableau. Unités cryptographiques unitaires

Nouvelles unités cryptographiques	Description
Unité cryptographique asymétrique (ACU)	1 ACU = 1 opération par seconde (ops) de déchiffrement (RSA) 2 K (taille de clé 2048 bits). Pour plus de détails, voir Tableau de conversion des ressources ACU en PKE.
Unité cryptographique symétrique (SCU)	1 SCU = 1 Mbits/s d'AES-128-CBC + SHA256-HMAC à 1 024 B. Cette définition s'applique à toutes les plateformes SDX.
Interfaces virtuelles Crypto	Également appelées fonctions virtuelles, les interfaces virtuelles cryptographiques représentent l'unité de base du matériel SSL. Une fois ces interfaces épuisées, le matériel SSL ne peut plus être affecté à une instance VPX. Les interfaces virtuelles de chiffrement sont des entités en lecture seule, et l'appliance SDX alloue automatiquement ces entités.

Afficher la capacité de chiffrement de l'appliance SDX

Vous pouvez afficher la capacité de chiffrement de l'appliance SDX dans le tableau de bord de l'interface graphique SDX. Le tableau de bord affiche les ACU, les unités de traitement et les interfaces virtuelles utilisées et disponibles sur l'appliance SDX. Pour afficher la capacité de chiffrement, accédez à **Tableau de bord > Capacité de chiffrement**.



Allouer la capacité de chiffrement lors du provisionnement de l'instance VPX

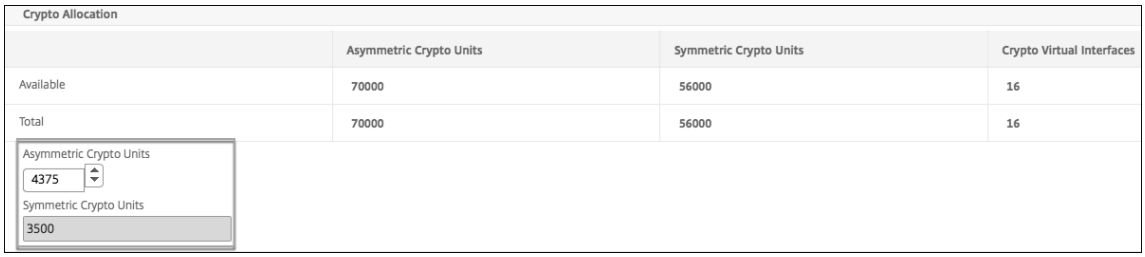
Lors du provisionnement d'une instance VPX sur l'appliance SDX, sous **Allocation de chiffrement**, vous pouvez allouer le nombre d'ACU et de SCU pour l'instance VPX. Pour obtenir des instructions sur la mise en service d'une instance VPX, consultez Provisioning d'instances Citrix ADC.

Pour allouer la capacité de chiffrement lors du provisionnement d'une instance VPX, procédez comme suit.

1. Ouvrez une session sur le service de gestion.
2. Accédez à **Configuration > Citrix ADC > Instances**, puis cliquez sur **Ajouter**.
3. Sous **Allocation cryptographique**, vous pouvez afficher les interfaces virtuelles ACU, SCU et cryptographiques disponibles. La façon d'allouer les ACU et les SCU diffère selon l'appliance SDX :

   a. Pour les appliances répertoriées dans la valeur minimale d'un compteur ACU disponible pour différents appliances SDX, vous pouvez attribuer des ACU en multiples d'un nombre spécifié. Les SCU sont automatiquement allouées et le champ d'allocation des SCU n'est pas modifiable. Vous pouvez augmenter l'allocation d'ACU dans les multiples de l'ACU minimum disponible pour ce modèle. Par exemple, si l'ACU minimum est 4375, l'incrément d'ACU est 8750, 13125, etc.

   Exemple. Allocation cryptographique où les SCU sont automatiquement attribuées et les ACU sont attribuées en multiples d'un nombre spécifié.



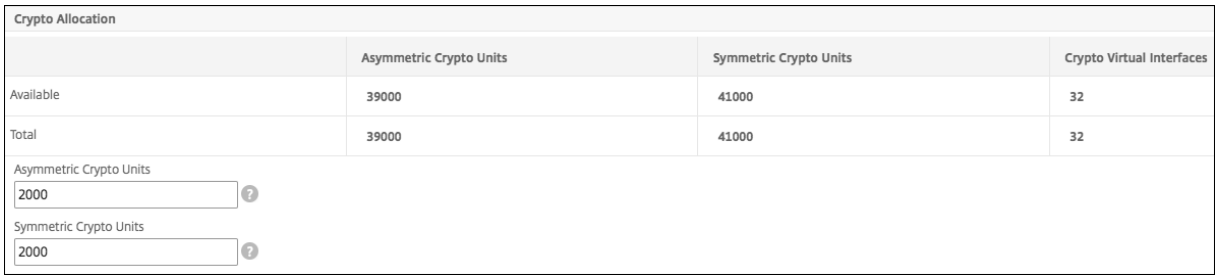
Valeur minimale d'un compteur ACU disponible pour différents appareils SDX

Plateforme SDX	Valeur minimale du compteur ACU
22040, 22060, 22080, 22100, 22120, 24100, 24150 (36 ports)	2187
8400, 8600, 8010, 8015	2812
17500, 19500, 21500	2812
17550, 19550, 20550, 21550	2812

Plateforme SDX	Valeur minimale du compteur ACU
11500, 13500, 14500, 16500, 18500, 20500	2812
11515, 11520, 11530, 11540, 11542	4375
14xxx	4375
14xxx 40S	4375
14xxx 40G	4375
14xxx FIPS	4375
25xxx	4375
25xxx A	4575

b. Pour les autres plates-formes SDX, qui ne sont pas répertoriées dans le tableau précédent, vous pouvez attribuer librement des ACU et des SCU. L'appliance SDX alloue automatiquement les interfaces virtuelles de chiffrement.

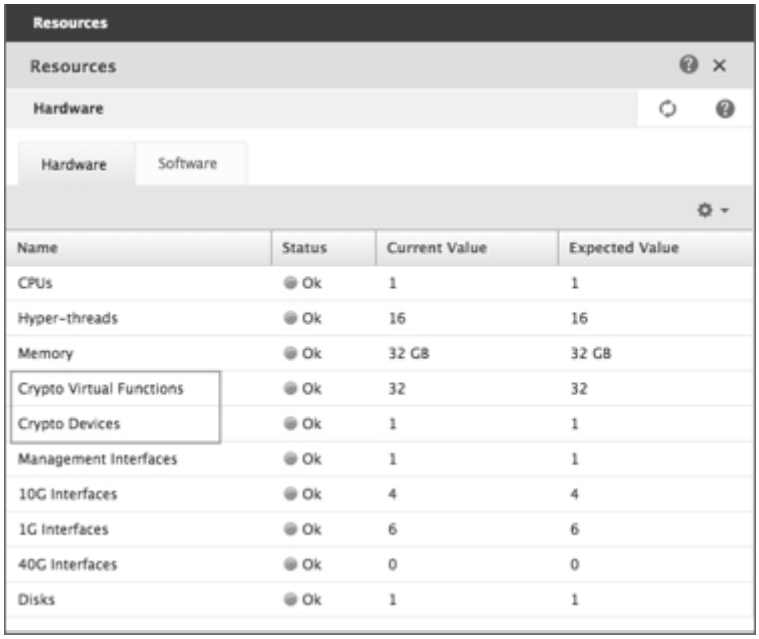
Exemple. Allocation cryptographique où l'ACU et les SCU sont assignés librement



4./ Effectuez toutes les étapes de provisionnement de l'instance VPX, puis cliquez sur **Terminé**. Pour de plus amples informations, consultez Provisioning des instances Citrix ADC.

Afficher la santé du matériel cryptographique

Dans le service de gestion, vous pouvez afficher l'état du matériel de chiffrement fourni avec l'appliance SDX. La santé du matériel cryptographique est représentée par les périphériques cryptographiques et les fonctions virtuelles cryptographiques. Pour afficher l'état du matériel de chiffrement, accédez à **Tableau de bord > Ressources**.



Points à noter

Gardez à l'esprit les points suivants lorsque vous mettez à niveau l'appliance SDX vers la dernière version.

- Seule l'interface utilisateur SDX est mise à niveau, mais la capacité matérielle de l'appliance reste la même.
- Le mécanisme d'allocation de chiffrement reste le même et seule la représentation sur l'interface graphique SDX change.
- L'interface Crypto est rétrocompatible et n'affecte aucun mécanisme d'automatisation existant qui utilise l'interface NITRO pour gérer l'appliance SDX.
- Lors de la mise à niveau de l'appliance SDX, le chiffrement attribué aux instances VPX existantes ne change pas ; seule sa représentation sur le service de gestion change.

Tableau de conversion des ressources ACU en PKE

Plateforme SDX	ACU	RSA-RSA1K	RSA-RSA2K	RSA-RSA4K	ECDHE-RSA	ECDHE-ECDSA
22040, 22060, 22080, 22100, 22120, 24100, 24150 (36 ports)	2187	12497	2187	312	256	190
8400, 8600, 8010, 8015	2812	17000	2812	424	330	S.O.
11515, 11520, 11530, 11540, 11542	4375	25000	4375	625	512	381
22040, 22060, 22080, 22100, 22120 (24 ports)	4375	25000	4375	625	512	381
17500, 19500, 21500	2812	17000	2812	424	330	S.O.
17550, 19550, 20550, 21550	2812	17000	2812	424	330	S.O.
11500, 13500, 14500, 16500, 18500, 20500	2812	17000	2812	424	330	S.O.

Plateforme SDX	ACU	RSA-RSA1K	RSA-RSA2K	RSA-RSA4K	ECDHE-RSA	ECDHE-ECDSA
14000, 14000-40G, 25000, 25000A	4375	25000	4375	625	512	381
14000 FIPS	4375	25000	4375	625	512	381
14000-40S	4375	25000	4375	625	512	381
*8900 (8910, 8920, 8930)	1000	4615	1000	136	397	494
*9100 (9110, 9120, 9130)	1000	4615	1000	136	397	494
*26000-100G (26100, 26160, 26200 et 26250)	1000	4615	1000	136	397	494
*15000	1000	4615	1000	136	397	494
*15000-50G	1000	4615	1000	136	397	494
*26000-50S	1000	4615	1000	136	397	494

*Sur ces plateformes, les nombres PKE sont les valeurs minimales garanties.

Comment lire le tableau de conversion des ressources ACU en PKE

Le tableau de conversion des ressources ACU en PKE est basé sur les points suivants :

- Le service de gestion permet d'allouer des ressources cryptographiques à chaque VPX individuel. Le service de gestion ne peut pas allouer ou promettre des
- Les performances réelles varient en fonction de la taille du paquet, du chiffrement/keyex/hmac (ou de leurs variations) utilisés, etc.

L'exemple suivant vous permet de comprendre comment lire et appliquer l'ACU à la table de conversion des ressources PKE.

Exemple. Conversion de ressources ACU en PKE pour la plate-forme SDX 22040

L'allocation de 2187 ACU à une instance VPX sur une plate-forme SDX 22040 alloue des ressources cryptographiques équivalentes à 256 opérations ECDHE-RSA ou 2187 opérations RSA-2K, etc.

Tableau de conversion des puces SSL héritées en ACU et SCU

Pour plus d'informations sur la façon dont les puces SSL héritées sont converties en ACU et SCU, consultez le tableau suivant.

Tableau de conversion ACU et SCU

Provisionner des machines virtuelles tiers

January 6, 2023

> **Avertissement :**
>
> La prise en charge **des instances tierces** est obsolète dans l'interface graphique Citrix ADC SDX à partir de la version 13.1 build 37.x. Si vous souhaitez toujours utiliser les instances tierces, Citrix vous recommande d'effectuer les opérations suivantes :
>
> - Connectez-vous au shell du service de gestion.
> - Créez un fichier `.thirdPartyVM` dans le répertoire `/mpsconfig`.
> - Redémarrez le service de gestion en exécutant la `svmd restart` commande.

L'appliance SDX prend en charge le provisionnement des machines virtuelles tierces suivantes (instances) :

- SECUREMATRIX GSB
- InterScan Web Security
- Protecteur Websense
- Serveur BlueCat DNS/DHCP
- Passerelle CA Access
- Série Palo Alto VM

SECUREMATRIX GSB fournit un système de mot de passe hautement sécurisé qui élimine le besoin de transporter des jetons. Websense Protector fournit des fonctionnalités de surveillance et de blocage, empêchant la perte de données et les fuites d'informations sensibles. Le serveur BlueCat DNS/DHCP fournit des services DNS et DHCP pour votre réseau. La série PaloAlto VM sur Citrix SDX permet de consolider les fonctionnalités avancées de sécurité et d'ADC sur une plate-forme unique, pour un accès sécurisé et fiable aux applications par les entreprises et les clients fournisseurs de services. La

combinaison de la série VM sur Citrix SDX fournit également une solution ADC complète, validée et sécurisée pour les déploiements Citrix Virtual Apps and Desktops.

Vous pouvez mettre en service, surveiller, gérer et dépanner une instance à partir du service de gestion. Toutes les instances tierces précédentes utilisent le `SDXTools` démon pour communiquer avec le service de gestion. Le démon est préinstallé sur l'instance provisionnée. Vous pouvez mettre à niveau le démon lorsque de nouvelles versions sont disponibles.

Lorsque vous configurez des machines virtuelles tierces, les interfaces SR-IOV (1/x et 10/x) qui font partie d'un canal n'apparaissent pas dans la liste des interfaces. Les interfaces sont manquantes car les canaux ne sont pas pris en charge sur les machines virtuelles tierces.

> **Remarque :**
>
> Le nombre total d'instances que vous pouvez mettre en service sur une appliance SDX dépend de la licence installée sur l'appliance.

Important : Vous devez mettre à niveau votre version Citrix Hypervisor vers la version 6.1.0 avant d'installer une instance tierce.

SECUREMATRIX GSB

January 27, 2022

SECUREMATRIX est une solution d'authentification par mot de passe à usage unique (OTP) hautement sécurisée, sans jeton, facile à utiliser et rentable. Il utilise une combinaison d'emplacement, de séquence et de modèle d'image provenant d'une table matricielle pour générer un mot de passe à usage unique. Le serveur GSB SECUREMATRIX avec le serveur d'authentification SECUREMATRIX améliore considérablement la sécurité des points de terminaison VPN/SSL-VPN, des applications et des ressources basées sur le cloud, de la connexion au bureau/bureau virtuel et des applications Web (proxy inverse avec OTP). Il fournit une solution compatible avec les PC, les bureaux virtuels, les tablettes et les téléphones intelligents.

En utilisant l'architecture de plate-forme mutualisée Citrix ADC SDX dans un réseau défini par logiciel, la fonction d'authentification forte de SECUREMATRIX peut être intégrée à d'autres locataires ou à des services cloud fournis via Citrix ADC, tels que l'interface Web, Citrix Virtual Apps and Desktops et de nombreuses autres applications les services qui nécessitent une authentification.

Pour plus d'informations, consultez SECUREMATRIX.

Provisionner une instance GSB SECUREMATRIX

SECUREMATRIX GSB nécessite un serveur d'authentification SECUREMATRIX qui doit être configuré en dehors de l'appliance SDX. Sélectionnez exactement une interface et spécifiez les paramètres réseau

pour cette interface uniquement.

Remarque : Les interfaces SR-IOV (1/x et 10/x) qui font partie d'un canal n'apparaissent pas dans la liste des interfaces. Les canaux ne sont pas pris en charge sur une instance GSB SECUREMATRIX.

Téléchargez une image XVA à partir du site Web SECUREMATRIX et téléchargez-la sur l'appliance SDX avant de commencer à provisionner l'instance. Pour plus d'informations sur le téléchargement d'une image XVA, consultez le site Web SECUREMATRIX. Assurez-vous que vous utilisez la version 118.7 ou ultérieure du service de gestion sur l'appliance SDX.

Dans l'onglet **Configuration**, accédez à **SECUREMATRIX GSB > Images logicielles**.

Pour télécharger une image XVA sur l'appliance SDX :

1. Dans le volet d'informations, sous **Fichiers XVA > Action**, cliquez sur **Charger**.
2. Dans la boîte de dialogue qui s'affiche, cliquez sur **Parcourir**, puis sélectionnez le fichier XVA que vous souhaitez télécharger.
3. Cliquez sur **Charger**. Le fichier XVA s'affiche dans le volet Fichiers XVA.

Pour provisionner une instance SECUREMATRIX

1. Dans l'onglet **Configuration**, accédez à **SECUREMATRIX GSB > Instances**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans l'assistant **Provisionn SECUREMATRIX GSB**, suivez les instructions qui s'affichent à l'écran.
4. Cliquez sur **Terminer**, puis sur **Fermer**.

Après avoir provisionné l'instance, connectez-vous à l'instance et effectuez une configuration détaillée. Pour plus d'informations, consultez le site Web SECUREMATRIX .

Pour modifier les paramètres d'une instance SECUREMATRIX provisionnée, dans le volet **Instances SECUREMATRIX**, sélectionnez l'instance que vous souhaitez modifier, puis cliquez sur **Modifier**. Dans l'assistant Modify SECUREMATRIX GSB, modifiez les paramètres.

Remarque : Si vous modifiez l'un des paramètres de l'interface ou le nom de l'instance, l'instance s'arrête et redémarre pour appliquer les modifications.

Générez une archive tar à soumettre au support technique. Pour plus d'informations sur la génération d'un fichier de support technique, voir Génération d'une archive Tar pour le support technique.

Sauvegardez la configuration d'une instance GSB SECUREMATRIX et utilisez ultérieurement les données de sauvegarde pour restaurer la configuration de l'instance sur l'appliance SDX. Pour plus d'informations sur la sauvegarde et la restauration d'une instance, consultez Sauvegarde et restauration des données de configuration de l'appliance SDX.

Surveiller une instance GSB SECUREMATRIX

L'appliance SDX collecte des statistiques, telles que la version de SDXTools, les états des démons SSH et CRON, et l'état du serveur Web, d'une instance GSB SECUREMATRIX.

Pour afficher les statistiques relatives à une instance GSB SECUREMATRIX :

1. Accédez à **SECUREMATRIX GSB > Instances**.
2. Dans le volet d'informations, cliquez sur la flèche en regard du nom de l'instance.

Gérer une instance GSB SECUREMATRIX

Vous pouvez démarrer, arrêter, redémarrer, forcer l'arrêt ou forcer le redémarrage d'une instance GSB SECUREMATRIX à partir du service de gestion.

Dans l'onglet **Configuration**, développez **SECUREMATRIX GSB**.

Pour démarrer, arrêter, redémarrer, forcer l'arrêt ou forcer le redémarrage d'une instance :

1. Cliquez sur **Instances**.
2. Dans le volet d'informations, sélectionnez l'instance sur laquelle vous souhaitez effectuer l'opération, puis sélectionnez l'une des options suivantes :
   - Démarrer
   - Arrêter
   - Redémarrez
   - Forcer l'arrêt
   - Forcer le redémarrage
3. Dans la zone de message Confirmer, cliquez sur **Oui**.

Mettez à niveau le fichier d'outils SDX pour une instance GSB SECUREMATRIX

SDXTools, un démon exécuté sur l'instance GSB SECUREMATRIX, est utilisé pour la communication entre le service de gestion et l'instance.

SDXTools La mise à niveau implique le téléchargement du fichier sur l'appliance SDX, puis la mise à niveau SDXTools après avoir sélectionné une instance. Vous pouvez télécharger un SDXTools fichier depuis un ordinateur client vers l'appliance SDX.

Pour télécharger un fichier SDXTools :

1. Dans le volet de navigation, développez **Service de gestion**, puis cliquez sur **Fichiers SDXTools**.
2. Dans le volet d'informations, dans la liste **Action**, sélectionnez **Télécharger**.
3. Dans la boîte de dialogue **Charger les fichiers SDXTools**, cliquez sur **Parcourir**, accédez au dossier qui contient le fichier, puis double-cliquez sur le fichier.
4. Cliquez sur **Charger**.

Pour mettre à niveau SDXTools :

Dans l'onglet **Configuration**, développez **SECUREMATRIX GSB**.

1. Cliquez sur **Instances**.
2. Dans le volet d'informations, sélectionnez une instance.
3. Dans la liste **Action**, sélectionnez **Mettre à niveau SDXTools**.
4. Dans la boîte de dialogue **Mettre à niveau SDXTools**, sélectionnez un fichier, cliquez sur **OK**, puis sur **Fermer**.

Mettre à niveau et rétrograder une instance GSB SECUREMATRIX

Le processus de mise à niveau de l'instance GSB SECUREMATRIX implique le téléchargement de l'image logicielle de la version cible sur l'appliance SDX, puis la mise à niveau de l'instance. La rétrogradation charge une version antérieure de l'instance.

Dans l'onglet **Configuration**, développez **SECUREMATRIX GSB**.

Pour télécharger l'image logicielle :

1. Cliquez sur **Images logicielles**.
2. Dans le volet d'informations, dans la liste **Action**, sélectionnez **Télécharger**.
3. Dans la boîte de dialogue, cliquez sur **Parcourir**, accédez au dossier qui contient le fichier de génération, puis double-cliquez sur le fichier de construction.
4. Cliquez sur **Charger**.

Pour mettre à niveau l'instance :

1. Cliquez sur **Instances**.
2. Dans le volet d'informations, sélectionnez une instance.
3. Dans la liste **Action**, sélectionnez **Mettre à niveau**.
4. Dans la boîte de dialogue qui s'affiche, sélectionnez un fichier, cliquez sur **OK**, puis sur **Fermer**.

Pour rétrograder une instance :

1. Cliquez sur **Instances**.
2. Dans le volet d'informations, sélectionnez une instance.
3. Dans la liste **Action**, sélectionnez **Rétrograder**.
4. Dans la zone de message Confirmer, cliquez sur **Oui**.

Dépannage d'une instance GSB SECUREMATRIX

Envoyez un ping à une instance GSB SECUREMATRIX à partir du service de gestion pour vérifier si le périphérique est accessible. Vous pouvez suivre l'itinéraire d'un paquet entre le service de gestion et une instance afin de déterminer le nombre de sauts nécessaires pour atteindre l'instance.

Redécouvrez une instance pour afficher l'état et la configuration les plus récents d'une instance. Lors de la redécouverte, le service de gestion récupère la configuration et la version du GSB SECUREMATRIX exécuté sur l'appliance SDX. Par défaut, le service de gestion planifie la redécouverte des instances toutes les 30 minutes.

Dans l'onglet **Configuration**, développez **SECUREMATRIX GSB**.

Pour envoyer un ping à une instance :

1. Cliquez sur **Instances**.
2. Dans le volet d'informations, sélectionnez l'instance à laquelle vous souhaitez envoyer un ping, puis dans la liste **Action**, cliquez sur **Ping**. La boîte de message Ping indique si le ping a réussi.

Pour tracer la route d'une instance :

1. Cliquez sur **Instances**.
2. Dans le volet d'informations, sélectionnez l'instance pour laquelle vous souhaitez suivre l'itinéraire, puis dans la liste **Action**, cliquez sur **TraceRoute**. La boîte de message Traceroute affiche l'itinéraire vers l'instance.

Pour redécouvrir une instance :

1. Cliquez sur **Instances**.
2. Dans le volet d'informations, sélectionnez l'instance que vous souhaitez redécouvrir, puis dans la liste **Action**, cliquez sur **Redécouvrir**.
3. Dans la zone de message Confirmer, cliquez sur **Oui**.

Sécurité Web Trend Micro InterScan

January 27, 2022

Trend Micro InterScan Web Security est une appliance virtuelle logicielle qui protège de manière dynamique contre les menaces Web traditionnelles et émergentes au niveau de la passerelle Internet. Il intègre le contrôle des applications, l'analyse anti-malware, la réputation Web en temps réel, le filtrage flexible des URL et une protection avancée contre les menaces. En conséquence, il offre une protection supérieure ainsi qu'une visibilité et un contrôle accrus sur l'utilisation croissante des applications basées sur le cloud sur le réseau. Les rapports en temps réel et la gestion centralisée offrent à vos administrateurs un outil de prise de décision proactif, permettant une gestion des risques sur place.

InterScan Web Security :

- Permet une meilleure visibilité sur l'activité Internet des utilisateurs finaux
- Centralise la gestion pour un contrôle maximal

- Surveille l'utilisation du Web en temps réel
- Permet la remédiation sur place
- Réduit la prolifération des appareils et les coûts énergétiques
- Fournit une protection contre la perte de données en option et une analyse d'exécution

Avant de pouvoir mettre en service une instance d'InterScan Web Security, vous devez télécharger une image XVA à partir du site Web de Trend Micro. Après avoir téléchargé l'image XVA, téléchargez-la sur l'appliance Citrix ADC SDX.

Remarque : Les interfaces SR-IOV (1/x et 10/x) qui font partie d'un canal n'apparaissent pas dans la liste des interfaces. Les canaux ne sont pas pris en charge sur une instance d'InterScan Web Security.

Pour télécharger une image XVA sur l'appliance SDX :

1. Dans l'onglet **Configuration**, accédez à **TrendMicro IWSVA > Images logicielles**.
2. Dans le volet d'informations, sous l'onglet **Fichiers XVA**, cliquez sur **Charger**.
3. Dans la boîte de dialogue qui s'affiche, cliquez sur **Parcourir**, puis sélectionnez le fichier XVA que vous souhaitez télécharger.
4. Cliquez sur **Charger**. Le fichier XVA s'affiche dans le volet Fichiers XVA.

Pour provisionner une instance IWSVA TrendMicro :

1. Dans l'onglet **Configuration**, accédez à **TrendMicro IWSVA > Instances**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans l'assistant **Provisionnement TrendMicro IWSVA**, suivez les instructions qui s'affichent à l'écran.
4. Cliquez sur **OK**, puis sur **Fermer**.

Après avoir provisionné l'instance, connectez-vous à l'instance et effectuez la configuration détaillée.

Pour modifier les valeurs des paramètres d'une instance provisionnée, dans le volet d'informations, sélectionnez l'instance que vous souhaitez modifier, puis cliquez sur **Modifier**. Dans l'assistant **Modify TrendMicro IWSVA**, définissez les paramètres sur des valeurs adaptées à votre environnement.

Protecteur Websense

January 27, 2022

Le protecteur de sécurité des données Websense (maintenant connu sous le nom de Forcepoint) est une machine virtuelle qui intercepte le trafic HTTP sortant (publications). Il analyse ensuite le trafic pour éviter la perte de données et les fuites de données sensibles sur le Web. Le protecteur communique avec un serveur Windows dédié pour obtenir des informations de stratégie DLP et peut surveiller ou bloquer la publication de données lorsqu'une correspondance est détectée. L'analyse

du contenu est effectuée sur la boîte, de sorte qu'aucune donnée sensible ne quitte le protecteur pendant ce processus.

Pour utiliser les fonctionnalités de prévention contre la perte de données (DLP) du protecteur, procédez comme suit :

- Acheter et installer Websense Data Security
- Configurer les stratégies Web DLP dans le gestionnaire de sécurité des données
- Effectuez la configuration initiale via le service de gestion.

Pour plus d'informations, consultez le site Web Websense Protector .

Provisionner une instance de Websense Protector

Le protecteur Websense© nécessite un serveur de gestion de la sécurité des données qui doit être configuré en dehors de l'appliance SDX. Sélectionnez exactement une interface de gestion et deux interfaces de données. Pour les interfaces de données, vous devez sélectionner Autoriser le mode L2. Assurez-vous que le serveur de gestion de la sécurité des données est accessible via le réseau de gestion du protecteur Websense. Pour le serveur de noms, saisissez l'adresse IP du serveur de noms de domaine (DNS) qui sert ce protecteur.

Remarque : Les interfaces SR-IOV (1/x et 10/x) qui font partie d'un canal n'apparaissent pas dans la liste des interfaces. Les chaînes ne sont pas prises en charge sur une instance de protection Websense.

Téléchargez une image de protection à partir du site Web Websense et téléchargez-la sur l'appliance SDX avant de commencer à provisionner l'instance. Pour plus d'informations sur le téléchargement d'une image de protection, consultez le site Web [Websense]. Assurez-vous que vous utilisez la version 118.7 ou ultérieure du service de gestion sur l'appliance SDX.

Dans l'onglet **Configuration**, accédez à **Websense Protector > Images logicielles**.

Pour télécharger une image XVA sur l'appliance SDX

1. Dans le volet d'informations, sous **Fichiers XVA > Action**, cliquez sur **Charger**.
2. Dans la boîte de dialogue qui s'affiche, cliquez sur Parcourir, puis sélectionnez le fichier XVA que vous souhaitez télécharger.
3. Cliquez sur **Charger**. Le fichier XVA s'affiche dans le volet Fichiers XVA.

Pour mettre en service une instance de protection Websense

1. Dans l'onglet **Configuration**, accédez à **Websense Protector > Instances**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans l'assistant **Provisionner Websense Protector**, suivez les instructions à l'écran.
4. Cliquez sur **Terminer**, puis sur **Fermer**.

Après avoir provisionné l'instance, connectez-vous à l'instance et effectuez la configuration détaillée.

Pour modifier les paramètres d'une instance de protection Websense provisionnée, dans le volet Instances Websense Protector, sélectionnez l'instance que vous souhaitez modifier, puis cliquez sur **Modifier**. Dans l'assistant Modifier Websense Protector, définissez les paramètres. Ne modifiez pas les interfaces qui ont été sélectionnées au moment du provisionnement d'une instance Websense. Le fichier XVA ne peut être modifié qu'après avoir supprimé l'instance et configuré une nouvelle instance.

Vous pouvez générer une archive tar à soumettre au support technique. Pour plus d'informations sur la génération d'un fichier de support technique, voir Génération d'une archive Tar pour le support technique.

Surveiller une instance de Websense Protector

L'appliance SDX collecte des statistiques, telles que la version de `SDXTools`, l'état du moteur de stratégie de sécurité des données Websense© et l'état du proxy de sécurité des données.

Pour afficher les statistiques relatives à une instance de protection Websense :

1. Accédez à **Websense Protector > Instances**.
2. Dans le volet d'informations, cliquez sur la flèche en regard du nom de l'instance.

Gérer une instance de Websense Protector

Vous pouvez démarrer, arrêter, redémarrer, forcer l'arrêt ou forcer le redémarrage d'une instance de protection Websense© à partir du service de gestion.

Dans l'onglet **Configuration**, développez **Websense Protector**.

Pour démarrer, arrêter, redémarrer, forcer l'arrêt ou forcer le redémarrage d'une instance de protection Websense

1. Cliquez sur **Instances**.
2. Dans le volet d'informations, sélectionnez l'instance sur laquelle vous souhaitez effectuer l'opération, puis sélectionnez l'une des options suivantes :
   - Démarrer
   - Arrêter
   - Redémarrez
   - Forcer l'arrêt
   - Forcer le redémarrage
3. Dans la zone de message Confirmer, cliquez sur **Oui**.

Mettre à niveau le fichier d'outils SDX pour une instance de Websense Protector

`SDXTools`, un démon s'exécutant sur l'instance tierce, est utilisé pour la communication entre le service de gestion et l'instance tierce.

`SDXTools` La mise à niveau implique le téléchargement du fichier sur l'appliance SDX, puis la mise à niveau `SDXTools` après avoir sélectionné une instance. Vous pouvez télécharger un `SDXTools` fichier depuis un ordinateur client vers l'appliance SDX.

Pour télécharger un fichier d'outils SDX

1. Dans le volet de navigation, développez **Service de gestion**, puis cliquez sur **Fichiers SDXTools**.
2. Dans le volet d'informations, dans la liste **Action**, sélectionnez **Télécharger**.
3. Dans la boîte de dialogue **Charger les fichiers SDXTools**, cliquez sur **Parcourir**, accédez au dossier qui contient le fichier, puis double-cliquez sur le fichier.
4. Cliquez sur **Charger**.

Pour mettre à niveau les outils SDX

Dans l'onglet **Configuration**, développez
Websense Protector.

1. Cliquez sur **Instances**.
2. Dans le volet d'informations, sélectionnez une instance.
3. Dans la liste **Action**, sélectionnez **Mettre à niveau SDXTools**.
4. Dans la boîte de dialogue **Mettre à niveau SDXTools**, sélectionnez un fichier, cliquez sur **OK**, puis sur **Fermer**.

Mettez à niveau l'instance de Websense Protector vers une version ultérieure

Le processus de mise à niveau de l'instance de protection Websense© implique le téléchargement de l'image logicielle de la version cible sur l'appliance SDX, puis la mise à niveau de l'instance.

Dans l'onglet **Configuration**, développez **Websense Protector**.

Pour télécharger l'image logicielle

1. Cliquez sur **Images logicielles**.
2. Dans le volet d'informations, dans la liste **Action**, sélectionnez **Télécharger**.
3. Dans la boîte de dialogue, cliquez sur **Parcourir**, accédez au dossier qui contient le fichier de génération, puis double-cliquez sur le fichier de construction.
4. Cliquez sur **Charger**.

Pour mettre à niveau l'instance

1. Cliquez sur **Instances**.
2. Dans le volet d'informations, sélectionnez une instance.
3. Dans la liste **Action**, sélectionnez **Mettre à niveau**.
4. Dans la boîte de dialogue qui s'affiche, sélectionnez un fichier, cliquez sur **OK**, puis sur **Fermer**.

Dépannage d'une instance de Websense Protector

Envoyez un ping à une instance de Websense Protector à partir du service de gestion pour vérifier si l'appareil est accessible. Vous pouvez suivre l'itinéraire d'un paquet entre le service de gestion et une instance afin de déterminer le nombre de sauts nécessaires pour atteindre l'instance.

Redécouvrez une instance pour afficher l'état et la configuration les plus récents d'une instance. Lors de la redécouverte, le service de gestion récupère la configuration et la version du protecteur Websense en cours d'exécution sur l'appliance SDX. Par défaut, le service de gestion planifie la redécouverte des instances toutes les 30 minutes.

Dans l'onglet **Configuration**, développez **Websense Protector**.

Pour envoyer un ping à une instance

1. Cliquez sur **Instances**.
2. Dans le volet d'informations, sélectionnez l'instance à laquelle vous souhaitez envoyer un ping, puis dans la liste **Action**, cliquez sur **Ping**. La boîte de message Ping indique si le ping a réussi.

Pour suivre l'itinéraire d'une instance

1. Cliquez sur **Instances**.
2. Dans le volet d'informations, sélectionnez l'instance pour laquelle vous souhaitez suivre l'itinéraire, puis dans la liste **Action**, cliquez sur **TraceRoute**. La boîte de message Traceroute affiche l'itinéraire vers l'instance.

Pour redécouvrir une instance

1. Cliquez sur **Instances**.
2. Dans le volet d'informations, sélectionnez l'instance que vous souhaitez redécouvrir, puis dans la liste **Action**, cliquez sur **Redécouvrir**.
3. Dans la zone de message Confirmer, cliquez sur **Oui**.

BlueCat DNS/DHCP

January 27, 2022

BlueCat DNS/DHCP Server™ est une solution logicielle prise en charge par l'appliance Citrix ADC SDX. Il est hébergé sur la plate-forme Citrix SDX pour fournir des services de réseau principal DNS et DHCP fiables, évolutifs et sécurisés sans frais de gestion supplémentaires ni d'espace de centre de données. Les services DNS critiques peuvent être équilibrés de charge sur plusieurs nœuds DNS au sein d'un seul système ou sur plusieurs appliances SDX sans avoir besoin de matériel supplémentaire.

Les instances virtuelles de BlueCat DNS/DHCP Server™ peuvent être hébergées sur SDX pour fournir un moyen plus intelligent de connecter des appareils mobiles, des applications, des environnements virtuels et des nuages.

Pour en savoir plus sur BlueCat et Citrix, visitez le site Web BlueCat à l'adresse https://citrixready.citrix.com/bluecat-networks.html.

Si vous êtes déjà client BlueCat, vous pouvez télécharger le logiciel et la documentation via le portail d'assistance BlueCat à l'adresse https://care.bluecatnetworks.com/.

Provisionnement d'une instance DNS/DHCP BlueCat

Téléchargez une image XVA auprès du service clientèle BlueCat, à l'adresse https://care.bluecatnetworks.com. Après avoir téléchargé l'image XVA, téléchargez-la sur l'appliance SDX avant de commencer à provisionner l'instance. Assurez-vous que vous utilisez la version 118.7 ou ultérieure du service de gestion sur l'appliance SDX.

Les canaux de gestion sur les interfaces 0/1 et 0/2 sont pris en charge sur les machines virtuelles BlueCat DNS/DHCP. Pour plus d'informations, consultez Configuration du canal à partir du service de gestion.

Remarque : Les interfaces SR-IOV (1/x et 10/x) qui font partie d'un canal n'apparaissent pas dans la liste des interfaces car les canaux ne sont pas pris en charge sur une instance DNS/DHCP BlueCat.

Dans l'onglet **Configuration**, accédez à **BlueCat DNS/DHCP > Images logicielles**.

Pour télécharger une image XVA sur l'appliance SDX :

1. Dans le volet d'informations, sous **Fichiers XVA > Action**, cliquez sur **Charger**.
2. Dans la boîte de dialogue qui s'affiche, cliquez sur **Parcourir**, puis sélectionnez le fichier XVA que vous souhaitez télécharger.
3. Cliquez sur **Charger**. Le fichier XVA s'affiche dans le volet Fichiers XVA.

Pour mettre en service une instance DNS/DHCP BlueCat :

1. Dans l'onglet Configuration, accédez à BlueCat DNS/DHCP > Instances.

2. Dans le volet d'informations, cliquez sur Ajouter. La page Provisionner le serveur DNS/DHCP BlueCat s'ouvre.
3. Dans l'assistant Provisionner BlueCat DNS/DHCP, suivez les instructions à l'écran.
    - Sous Création d'instance, dans le champ Nom, saisissez un nom pour l'instance et sélectionnez l'image téléchargée dans le menu déroulant Fichier XVA, puis cliquez sur Suivant. Le cas échéant, dans le champ Nom de domaine, saisissez un nom de domaine pour l'instance.

      Remarque : Le nom ne doit pas contenir d'espaces.
    - Sous Paramètres réseau, dans le menu déroulant Interface de gestion, sélectionnez l'interface par laquelle gérer l'instance, définissez l'adresse IP et la passerelle pour cette interface. Vous pouvez attribuer des interfaces explicitement pour la haute disponibilité et le service. Sélectionnez les paramètres, puis cliquez sur **Suivant**.

      Remarque : Lorsque vous affectez des interfaces pour la gestion, la haute disponibilité et le service, assurez-vous d'attribuer les interfaces en fonction de la combinaison d'interfaces prise en charge :

Vous pouvez sélectionner la même interface pour les trois.
Vous pouvez sélectionner une interface différente pour les trois.
Vous pouvez sélectionner la même interface pour la gestion et le service, mais sélectionner une interface différente pour la haute disponibilité.
Cliquez sur **Terminer**, puis sur **Fermer**. L'instance est créée, démarrée et configurée avec l'adresse IP sélectionnée.

Après avoir provisionné l'instance, connectez-vous à l'instance via SSH pour terminer la configuration. Pour plus de détails sur la configuration du serveur BlueCat DNS/DHCP ou le placer sous le contrôle du gestionnaire d'adresses BlueCat, consultez la documentation BlueCat, disponible à l'adresse https://care.bluecatnetworks.com.

Pour modifier les paramètres d'une instance de serveur BlueCat DNS/DHCP, **dans le volet Instances DNS/DHCP BlueCat**, sélectionnez l'instance que vous souhaitez modifier, puis cliquez sur **Modifier**. Dans l'assistant Modifier BlueCat DNS/DHCP, modifiez les paramètres.

Remarque : Si vous modifiez l'un des paramètres de l'interface ou le nom de l'instance, l'instance s'arrête et redémarre pour appliquer les modifications.

Surveiller une instance DNS/DHCP BlueCat

L'appliance SDX collecte des statistiques, telles que la version d' `SDXTools` exécution sur l'instance, d'une instance DNS/DHCP BlueCat.

Pour afficher les statistiques relatives à une instance DNS/DHCP BlueCat :

1. Accédez à BlueCat DNS/DHCP > Instances.
2. Dans le volet d'informations, cliquez sur la flèche en regard du nom de l'instance.

Gérer une instance DNS/DHCP BlueCat

Vous pouvez démarrer, arrêter, redémarrer, forcer l'arrêt ou forcer le redémarrage d'une instance BlueCat DNS/DHCP à partir du service de gestion.

Dans l'onglet **Configuration**, développez **BlueCat DNS/DHCP**.

Pour démarrer, arrêter, redémarrer, forcer l'arrêt ou forcer le redémarrage d'une instance DNS/DHCP BlueCat :

1. Cliquez sur Instances.
2. Dans le volet d'informations, sélectionnez l'instance sur laquelle vous souhaitez effectuer l'opération, puis sélectionnez l'une des options suivantes :
   - Démarrer
   - Arrêter
   - Redémarrez
   - Forcer l'arrêt
   - Forcer le redémarrage
3. Dans la zone de message Confirmer, cliquez sur Oui.

Mettez à niveau le `SDXTools` fichier pour une instance DNS/DHCP BlueCat

`SDXTools`, un démon s'exécutant sur l'instance tierce, est utilisé pour la communication entre le service de gestion et l'instance tierce.

`SDXTools` La mise à niveau implique le téléchargement du fichier sur l'appliance SDX, puis la mise à niveau `SDXTools` après avoir sélectionné une instance. Vous pouvez télécharger un `SDXTools` fichier depuis un ordinateur client vers l'appliance SDX.

Pour télécharger un fichier SDXTools :

1. Dans le volet de navigation, développez **Service de gestion**, puis cliquez sur **Fichiers SDXTools**.
2. Dans le volet d'informations, dans la liste **Action**, sélectionnez **Télécharger**.
3. Dans la boîte de dialogue **Charger les fichiers SDXTools**, cliquez sur **Parcourir**, accédez au dossier qui contient le fichier, puis double-cliquez sur le fichier.
4. Cliquez sur **Charger**.

Pour mettre à niveau SDXTools :

Dans l'onglet **Configuration**, développez **BlueCat DNS/DHCP**.

1. Cliquez sur **Instances**.
2. Dans le volet d'informations, sélectionnez une instance.
3. Dans la liste Action, sélectionnez **Mettre à niveau SDXTools**.

4. Dans la boîte de dialogue **Mettre à niveau SDXTools**, sélectionnez un fichier, cliquez sur **OK**, puis sur **Fermer**.

Redécouvrez une instance DNS/DHCP BlueCat

Vous pouvez redécouvrir une instance pour afficher l'état et la configuration les plus récents d'une instance. Lors de la redécouverte, le service de gestion récupère la configuration. Par défaut, le service de gestion planifie les instances pour la redécouverte de toutes les instances toutes les 30 minutes.

Dans l'onglet **Configuration**, développez **BlueCat DNS/DHCP**.

1. Cliquez sur **Instances**.
2. Dans le volet d'informations, sélectionnez l'instance que vous souhaitez redécouvrir, puis dans la liste **Action**, cliquez sur **Redécouvrir**.
3. Dans la zone de message **Confirmer**, cliquez sur **Oui**.

Passerelle CA Access

January 27, 2022

CA Access Gateway est un serveur autonome évolutif, gérable et extensible qui fournit une solution basée sur un proxy pour le contrôle d'accès. CA Access Gateway utilise un moteur proxy qui fournit une passerelle réseau pour l'entreprise et prend en charge plusieurs schémas de session qui ne reposent pas sur la technologie traditionnelle basée sur les cookies.

L'agent Web intégré permet l'authentification unique (SSO) dans toute l'entreprise. CA Access Gateway fournit un contrôle d'accès pour les requêtes HTTP et HTTPS et l'authentification unique sans cookie. En outre, le produit stocke les informations de session dans le magasin de sessions en mémoire. Les règles de proxy définissent la façon dont CA Access Gateway transfère ou redirige les demandes vers des ressources situées sur des serveurs de destination au sein de l'entreprise.

En fournissant une passerelle unique pour les ressources réseau, CA Access Gateway sépare le réseau d'entreprise et centralise le contrôle d'accès.

Remarque : Les interfaces SR-IOV (1/x et 10/x) qui font partie d'un canal n'apparaissent pas dans la liste des interfaces car les canaux ne sont pas pris en charge sur une instance de CA Access Gateway. Pour plus d'informations sur les fonctionnalités de CA Access Gateway, consultez la documentation de ce produit.

Provisionner une instance de CA Access Gateway

Avant de pouvoir mettre en service une instance de CA Access Gateway, vous devez télécharger une image XVA. Après avoir téléchargé l'image XVA, téléchargez-la sur l'appliance SDX. Assurez-vous que vous utilisez Management Service version 10.5 build 52.3.e ou ultérieure sur l'appliance SDX. Pour mettre en service une passerelle CA Access Gateway, vous devez d'abord télécharger l'image XVA sur l'appliance SDX, puis provisionner une instance.

Pour télécharger une image XVA sur l'appliance SDX :

1. Dans l'onglet **Configuration**, accédez à **CA Access Gateway** > **Images logicielles**.
2. Dans le volet d'informations, sous **Fichiers XVA**, dans la liste déroulante **Action**, cliquez sur **Charger**.
3. Dans la boîte de dialogue qui s'affiche, cliquez sur **Parcourir**, puis sélectionnez le fichier XVA que vous souhaitez télécharger.
4. Cliquez sur **Charger**. Le fichier XVA s'affiche dans le volet Fichiers **XVA** .

Pour provisionner une instance de CA Access Gateway :

1. Dans l'onglet **Configuration**, accédez à **CA Access Gateway**> **Instances**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans l'assistant Provisionner CA Access Gateway, suivez les instructions qui s'affichent à l'écran.
4. Cliquez sur **Terminer**, puis sur **Fermer**.

Après avoir provisionné l'instance, connectez-vous à l'instance et effectuez la configuration détaillée.

Pour modifier les valeurs des paramètres d'une instance provisionnée, dans le volet d'informations, sélectionnez l'instance à modifier, puis cliquez sur **Modifier**. Dans l'assistant Modifier CA Access Gateway, définissez les paramètres sur des valeurs adaptées à votre environnement.

Remarque :

Si vous modifiez l'un des paramètres de l'interface ou le nom de l'instance, l'instance s'arrête et redémarre pour appliquer la modification.

Surveiller une instance de CA Access Gateway

L'appliance SDX collecte des statistiques, telles que la version d' `SDXTools` exécution sur l'instance, d'une instance de CA Access Gateway.

Pour afficher les statistiques relatives à une instance de CA Access Gateway :

1. Accédez à **CA Access Gateway > Instances**.
2. Dans le volet d'informations, cliquez sur la flèche en regard du nom de l'instance.

Gérer une instance de CA Access Gateway

Vous pouvez démarrer, arrêter, redémarrer, forcer l'arrêt ou forcer le redémarrage d'une instance de CA Access Gateway à partir du service de gestion. Pour effectuer ces tâches, procédez comme suit :

1. Dans l'onglet **Configuration**, développez **CA Access Gateway**.
2. Accédez à **CA Access Gateway > Instances**.
3. Dans le volet d'informations, sélectionnez l'instance sur laquelle vous souhaitez effectuer l'opération, puis sélectionnez l'une des options suivantes :
   - Démarrer
   - Arrêter
   - Redémarrez
   - Forcer l'arrêt
   - Forcer le redémarrage
4. Dans la zone de message Confirmer, cliquez sur **Oui**.

Gamme VM de Palo Alto Networks

January 27, 2022

Les pare-feu virtuels de la série VM de Palo Alto Networks utilisent le même ensemble de fonctionnalités PAN-OS disponible dans les dispositifs de sécurité physique de l'entreprise, fournissant toutes les fonctions de sécurité réseau clés. La série VM sur Citrix SDX permet de consolider les fonctionnalités avancées de sécurité et d'ADC sur une plate-forme unique, pour un accès sécurisé et fiable aux applications par les entreprises, les unités commerciales et les clients fournisseurs de services. La combinaison de la série VM sur Citrix SDX fournit également une solution complète et validée de sécurité et ADC pour les déploiements Citrix Virtual Apps and Desktops.

Vous pouvez mettre en service, surveiller, gérer et dépanner une instance à partir du service de gestion.

Points à noter :

- Le nombre total d'instances que vous pouvez mettre en service sur une appliance SDX dépend des ressources matérielles SDX disponibles.
- Les interfaces SR-IOV (1/x et 10/x) qui font partie d'un canal n'apparaissent pas dans la liste des interfaces car les canaux ne sont pas pris en charge sur une instance de la série VM de Palo Alto. Pour plus d'informations sur la série VM réseau Palo Alto, consultez la documentation réseau Palo Alto.

Provisionner une instance de la série VM Palo Alto

Avant de pouvoir mettre en service une instance de la série VM de Palo Alto, vous devez télécharger une image XVA à partir du site Web de Palo Alto Networks. Après avoir téléchargé l'image XVA, téléchargez-la sur l'appliance SDX.

Pour télécharger une image XVA sur l'appliance SDX :

1. Dans l'onglet **Configuration**, accédez à **Paloalto VM Series > Images logicielles**.
2. Dans le volet d'informations, sous **Fichiers XVA**, dans la liste déroulante **Action**, cliquez sur **Charger**.
3. Dans la boîte de dialogue qui s'affiche, cliquez sur **Parcourir**, puis sélectionnez le fichier XVA que vous souhaitez télécharger.
4. Cliquez sur **Charger**. Le fichier XVA s'affiche dans le volet Fichiers **XVA** .

Pour provisionner une instance de la série VM de Palo Alto :

1. Dans l'onglet **Configuration**, accédez à **Paloalto VM Series > Instances**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans l'assistant Provisionnement Paloalto VM Series, suivez les instructions qui s'affichent à l'écran.
4. Cliquez sur **Terminer**, puis sur **Fermer**.

Après avoir provisionné l'instance, connectez-vous à l'instance et effectuez la configuration détaillée.

Pour modifier les valeurs des paramètres d'une instance provisionnée, dans le volet d'informations, sélectionnez l'instance à modifier, puis cliquez sur **Modifier**. Dans l'assistant Modifier la série PaloAlto VM, définissez les paramètres sur des valeurs adaptées à votre environnement.

Remarque : Si vous modifiez l'un des paramètres de l'interface ou le nom de l'instance, l'instance s'arrête et redémarre pour appliquer la modification.

Surveiller une instance de la série VM de Palo Alto

L'appliance SDX collecte des statistiques, telles que la version d' `SDXTools` exécution sur l'instance, d'une instance de la série VM Palo Alto.

Pour afficher les statistiques relatives à une instance de la série VM de Palo Alto, procédez comme suit :

1. Accédez à **Paloalto VM Series > Instances**.
2. Dans le volet d'informations, cliquez sur la flèche en regard du nom de l'instance.

Gérer une instance PaloAlto VM Series

Vous pouvez démarrer, arrêter, redémarrer, forcer l'arrêt ou forcer le redémarrage d'une instance Paloalto VM à partir du service de gestion.

Dans l'onglet **Configuration**, développez **Paloalto VM Series**.

1. Accédez à **Paloalto VM Series > Instances**.
2. Dans le volet d'informations, sélectionnez l'instance sur laquelle vous souhaitez effectuer l'opération, puis sélectionnez l'une des options suivantes :
   - Démarrer
   - Arrêter
   - Redémarrez
   - Forcer l'arrêt
   - Forcer le redémarrage
3. Dans la zone de message Confirmer, cliquez sur **Oui**.

Dépannage d'une instance PaloAlto VM Series

Effectuez une commande ping sur une instance PaloAlto de la série VM à partir du service de gestion pour vérifier si le périphérique est accessible. Vous pouvez suivre l'itinéraire d'un paquet entre le service de gestion et une instance afin de déterminer le nombre de sauts nécessaires pour atteindre l'instance.

Redécouvrez une instance pour afficher l'état et la configuration les plus récents d'une instance. Lors de la redécouverte, le service de gestion récupère la configuration et la version de la série PaloAlto VM exécutée sur l'appliance SDX. Par défaut, le service de gestion planifie la redécouverte des instances toutes les 30 minutes.

Dans l'onglet **Configuration**, développez **Paloalto VM Series**.

Pour envoyer un ping à une instance :

1. Cliquez sur **Instances**.
2. Dans le volet d'informations, sélectionnez l'instance à laquelle vous souhaitez envoyer un ping, puis dans la liste **Action**, cliquez sur **Ping**. La boîte de message **Ping** indique si le ping a réussi.

Pour suivre l'itinéraire d'une instance :

1. Cliquez sur **Instances**.
2. Dans le volet d'informations, sélectionnez l'instance à laquelle vous souhaitez envoyer un ping, puis dans la liste **Action**, cliquez sur **TraceRoute**. La boîte de message **Traceroute** affiche l'itinéraire vers l'instance.

Pour redécouvrir une instance :

1. Cliquez sur **Instances**.
2. Dans le volet d'informations, sélectionnez l'instance que vous souhaitez redécouvrir, puis dans la liste **Action**, cliquez sur **Redécouvrir**.
3. Dans la zone de message Confirmer, cliquez sur **Oui**.

Déployer une instance Citrix SD-WAN VPX sur une appliance Citrix ADC SDX

June 13, 2022

La technologie Citrix SD-WAN applique les concepts de réseau défini par logiciel (SDN) aux connexions WAN. La technologie soustrait la gestion et la surveillance du trafic du matériel réseau et les applique à des applications individuelles. Le résultat est une amélioration des performances, une expérience utilisateur de haute qualité sur des sites géographiquement dispersés et un déploiement simplifié des réseaux étendus et d'accès au cloud. Pour de plus amples informations, consultez Citrix SD-WAN.

> **Remarque :** Seule l'édition standard SD-WAN VPX est prise en charge. Pour plus d'informations, consultez Éditions SD-WAN VPX.

Le déploiement d'une instance Citrix SD-WAN VPX sur une appliance SDX inclut les tâches suivantes :

- Installation du matériel : assurez-vous que le matériel SDX est correctement installé. Pour plus d'informations, reportez-vous à la section Installation du matériel.
- Configuration et configuration du service de gestion SDX. Pour plus d'informations, consultezDémarrage avec l'interface utilisateur du service de gestion et Configuration du service de gestion.
- Provisionnement de l'instance VPX SD-WAN sur l'appliance SDX. Pour plus d'informations, consultez Provisionner l'instance Citrix SD-WAN VPX sur un Citrix ADC SDX.
- Configuration de l'instance VPX SD-WAN. Pour plus d'informations, consultez les documentations de configuration et Configuration du service de chemin d'accès virtuel entre le MCN et les sites clients.

Conditions préalables

Vérifiez que vous disposez des licences suivantes :

- Licence Citrix SD-WAN VPX
- Licence pour la plateforme Citrix ADC SDX

Configuration requise pour Citrix SD-WAN VPX

Le Citrix SD-WAN VPX sur la plate-forme SDX peut agir à la fois en tant que site et MCN. Le MCN peut gérer un débit bidirectionnel de 1 Gbit/s et 64 sites.

Débit pris en charge pour le MCN et le site

- Débit bidirectionnel de 250 Mo/s à 1 Gbit/s

- Le MCN prend en charge 64 sites

Configuration matérielle requise pour le débit pris en charge

Site

- 4 processeurs à 16 processeurs
- 4 Go à 16 Go de RAM
- Stockage sur disque de 60 Go à 250 Go
- 4 cartes réseau minimum : une pour la gestion et 3 autres pour le chemin de données

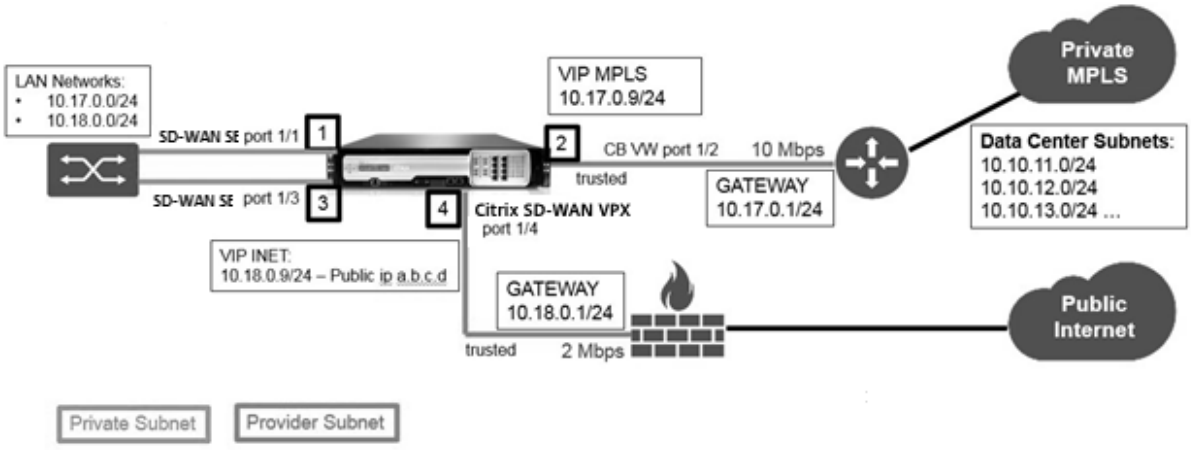
Nœud de contrôle principal (MCN)

- 4, 8 et 16 processeurs
- 16 GO DE RAM
- Stockage sur disque de 250 Go
- 4 cartes réseau minimum : une pour la gestion et les 3 autres pour le chemin de données, avec des cartes réseau dédiées pour le chemin de données

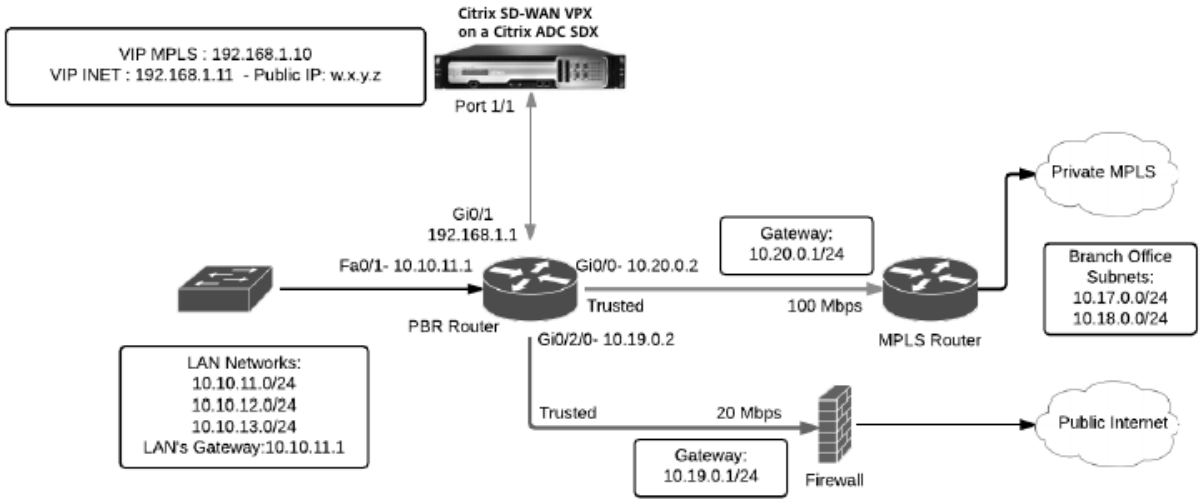
Topologie du centre de données

Vous pouvez déployer une appliance Citrix SD-WAN VPX sur un Citrix ADC SDX en mode route basée sur des stratégies (PBR) ou en mode en ligne. Reportez-vous aux scénarios 1 et 2 pour la topologie du centre de données pour ces deux modes pris en charge. Pour plus d'informations, consultez Déploiement du SD-WAN en mode virtuel en ligne).

Scénario 1 : mode Inline



Scénario 2 : mode PBR ou mode virtuel en ligne

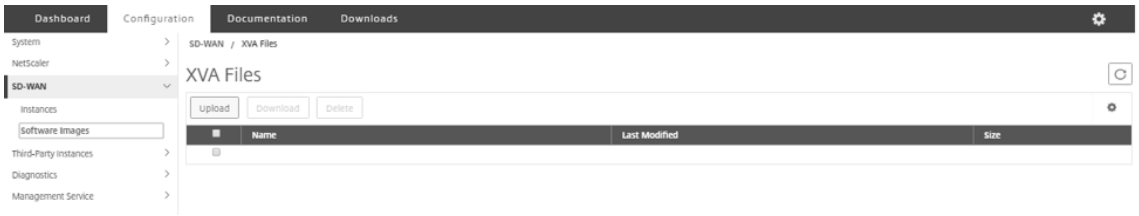


Provisionner l'instance de Citrix SD-WAN VPX sur un Citrix ADC SDX

Avant de mettre en service l'appliance Citrix SD-WAN VPX, téléchargez l'image SD-WAN VPX à partir du site de téléchargement du produit Citrix : https://www.citrix.com/downloads/netscaler-sd-wan/.

Suivez ces étapes pour provisionner l'appliance Citrix SD-WAN VPX.

1. Ouvrez une session sur l'appliance Citrix ADC SDX.
2. Accédez à **Configuration > SD-WAN > Instances**.
3. Sélectionnez **Images logicielles > Charger** et télécharger le fichier XVA SD-WAN.



4. Sélectionnez **Instances > Ajouter**. La page **Provisionner une instance SD-WAN** s'affiche.
5. Sur la page **Provisionner une instance SD-WAN**, entrez les informations suivantes :

   a. Nom

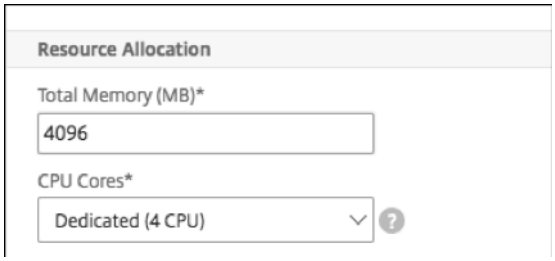
   b. adresse IP

   c. Masque réseau

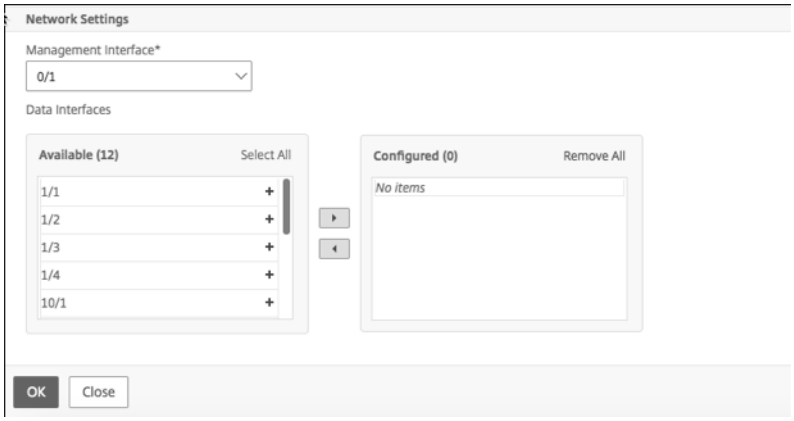
   d. Adresse de la passerelle

   e. Téléchargez le fichier XVA

   f. Sous **Allocation des ressources**, allouez des ressources.



g. Sous **Paramètres réseau**, provisionnez les interfaces de gestion et sélectionnez **OK** pour créer afin de provisionner l'instance VPX SD-WAN sur l'appliance SDX.



> **Remarque :** Le service de gestion SDX lie les interfaces à l'instance VPX dans la séquence croissante de noms d'interface. Par exemple, si vous ajoutez 1/4 et 1/1, le service de gestion les organise comme 1/1, 1/4.
> Lorsque vous ajoutez de nouvelles interfaces, la séquence existante est conservée et une nouvelle séquence est créée. Par exemple, vous ajoutez des interfaces 1/2, 10/1, 1/3. La nouvelle séquence serait 1/1, 1/4 ; 1/2, 1/3, 10/1.

6. L'instance VPX SD-WAN apparaît sous la **page Instance**. Voici un exemple.

```
1 ![Image](/en-us/sdx/media/sd-wan-vpx-example.png)
```

Pour modifier l'instance, accédez à **Configuration > SD-WAN > Instances**. Sélectionnez et cliquez sur l'instance. Une fois les modifications terminées, cliquez sur **OK** pour enregistrer les modifications.

Configuration de l'instance Citrix SD-WAN VPX

Après avoir créé une instance SD-WAN sur l'appliance SDX, configurez l'instance SD-WAN en effectuant ces deux tâches :

1. Appliquez la configuration à la fois pour les dispositifs MCN et de site.
2. Configurez le chemin virtuel et transmettez le trafic.

Pour plus d'informations, consultez les rubriques suivantes :

- Configuration
- Configuration du service de chemin virtuel entre le MCN et les sites clients

Informations connexes

Pour plus d'informations sur la mise en route d'une appliance Citrix SD-WAN, consultez Citrix SD-WAN.

Pour plus d'informations sur l'appliance Citrix ADC SDX, consultez Citrix ADC SDX.

Mesure de la bande passante dans SDX

January 27, 2022

La mesure de la bande passante Citrix ADC SDX vous fournit un schéma de mesure précis, fiable et facile à utiliser qui vous permet d'allouer efficacement la capacité de traitement et de monétiser l'utilisation de la bande passante. Un schéma de comptage est nécessaire pour allouer de manière optimale la bande passante entre les différentes ressources, en gardant à l'esprit que tous les utilisateurs obtiennent à tout moment la bande passante allouée.

L'allocation de bande passante peut être effectuée selon les deux modes suivants :

- Bande passante dédiée avec un débit fixe
- Bande passante dédiée avec un débit minimum garanti et une capacité d'éclatement de bande passante

Bande passante dédiée avec un débit fixe

Dans la méthode d'allocation de bande passante, chaque instance VPX se voit attribuer une bande passante dédiée. L'instance est autorisée à utiliser la bande passante jusqu'à la limite définie. En mode dédié, la bande passante minimale et maximale allouée est la même. Si, au cours d'une période donnée, l'instance VPX nécessite plus de bande passante que celle allouée, alors en mode dédié, l'instance ne peut pas augmenter son débit. Ce problème peut être un inconvénient si une instance VPX traite des demandes critiques.

En outre, si une appliance SDX possède quelques instances VPX et que certaines d'entre elles n'utilisent pas leur bande passante allouée, vous ne pouvez pas partager leur bande passante inutilisée en mode dédié. Pour surmonter tous ces défis, une bande passante dédiée avec un débit minimum garanti avec la capacité d'augmenter dynamiquement la bande passante est utile.

Bande passante dédiée avec un débit minimum garanti et une capacité d'éclatement de bande passante

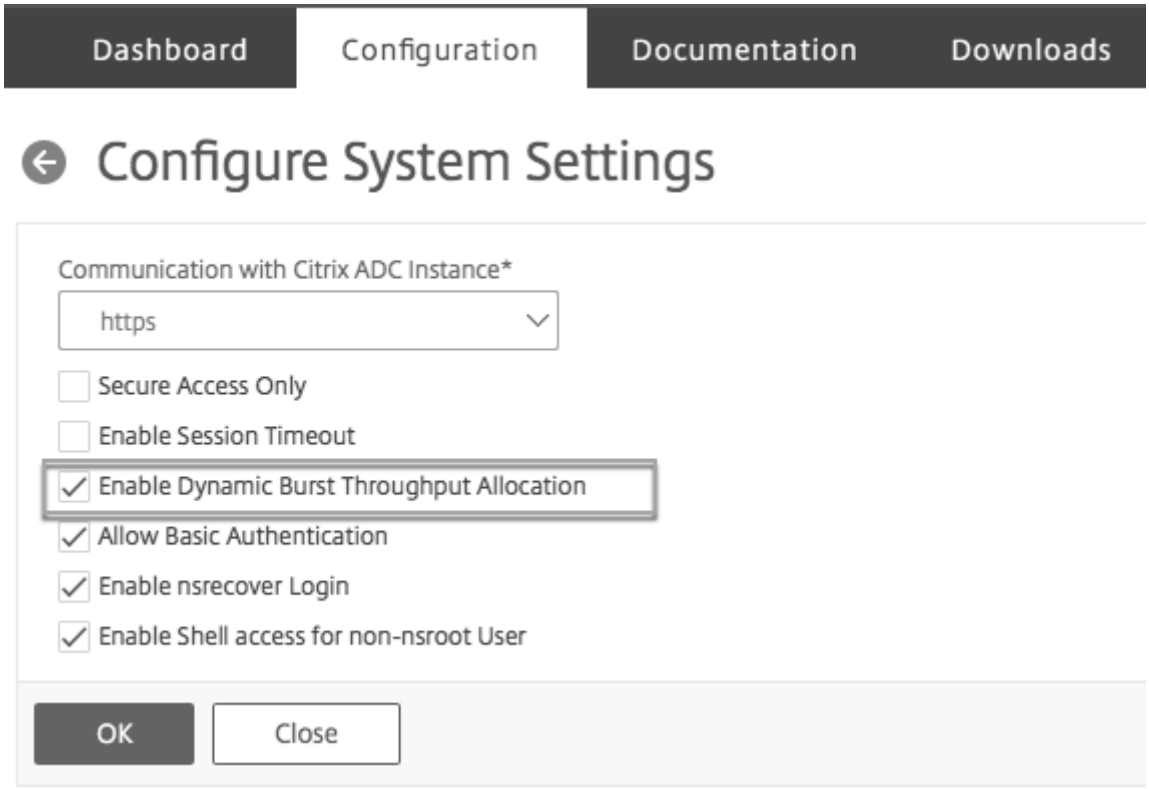
Dans cette méthode d'allocation de bande passante, un VPX se voit attribuer une bande passante minimale garantie avec la flexibilité d'augmenter sa bande passante jusqu'à une limite prédéfinie. La bande passante supplémentaire qu'un VPX peut utiliser est appelée capacité de rafale.

L'avantage de la capacité de rafale est visible lorsque certaines instances ont une capacité supplémentaire et certains VPX avec une capacité inutilisée. La capacité supplémentaire de ces instances VPX peut être allouée à d'autres instances VPX qui ont pleinement utilisé leur bande passante allouée et qui en ont besoin depuis un certain temps. Différents fournisseurs de services souhaitent également fournir divers services complémentaires à leurs clients qui ont besoin d'une capacité dédiée. En même temps, ils ne veulent pas surcharger la bande passante. La bande passante extensible est utile dans les scénarios où les clients sont assurés d'avoir une bande passante spécifique avec la possibilité d'augmenter la bande passante pendant les périodes de forte demande.

Sélection du mode d'allocation de bande passante

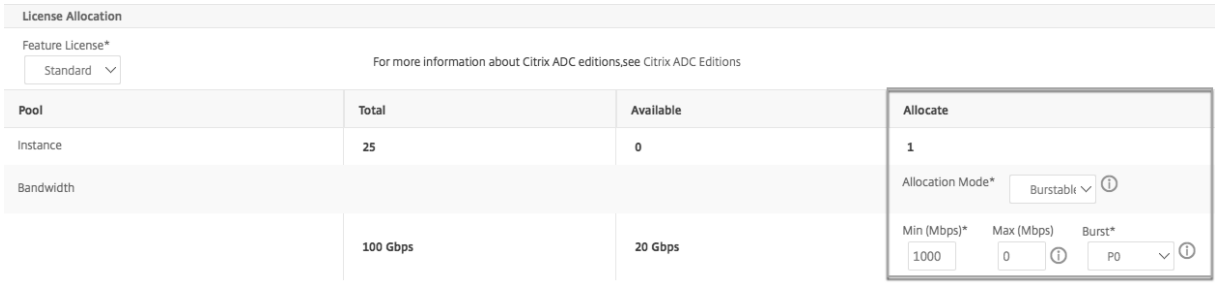
Avant de choisir le débit en rafale, vous devez activer l'allocation dynamique du débit en rafale. Pour activer cette option, procédez comme suit.

1. Dans la console de gestion SDX, accédez à **Configuration > Système**.
2. Dans le groupe **Paramètres système**, sélectionnez **Modifier les paramètres système**.
3. Cochez la case **Activer l'allocation de débit de rafale dynamique** pour activer le débit dynamique.



Lorsque vous mettez en service un VPX, vous pouvez choisir entre une rafale de bande passante ou un débit dynamique.

1. Dans le **service de gestion SDX**, cliquez sur **Configuration > Citrix ADC > Instances > Ajouter**.
2. La page **Provisionner Citrix ADC** s'ouvre. Sous **License Allocation**, choisissez **Burstable** à partir du **mode d'allocation**.



Pour plus d'informations sur la façon de provisionner une instance Citrix ADC, consultez Provisioning d'instances Citrix ADC.

Si vous souhaitez utiliser un débit fixe, sélectionnez **Fixe**. Par défaut, le mode fixe est défini pour l'allocation de bande passante. Il n'est pas nécessaire que toutes les instances VPX fonctionnent dans le même mode. Chaque instance VPX peut être configurée dans un mode différent.

Remarque : Si vous migrez SDX depuis la version 10.5.e et les versions antérieures, toutes les instances VPX sont par défaut en mode d'allocation fixe.

Détermination de la bande passante maximale en rafale pour une instance VPX

La mesure dans laquelle chaque VPX est autorisé à éclater est calculée au moyen d'un algorithme. Lorsque vous mettez en service un VPX avec une bande passante extensible, chacun de ces VPX doit avoir une priorité. L'allocation de bande passante extensible dépend de cette priorité de rafale. La priorité varie de P0 à P4, P0 étant la priorité la plus élevée et P4 la plus faible.

Prenons un cas où il y a 2 VPX, à savoir VPX1 et VPX2. La bande passante minimale allouée à VPX1 et VPX2 est respectivement de 4 Gbit/s et 2 Gbit/s avec une bande passante extensible de 2 Gbit/s et 1 Gbit/s chacune. Le tableau suivant présente les paramètres :

|Nom VPX|Paramètre|Valeur|
|–|–|–|
|VPX1|Bande passante minimale garantie|4 Gbits/s
|-|-|Bande passante extensible maximale|2 Gbits/s
|-|-|Priorité|P0
|VPX2|Bande passante minimale garantie|2 Gbit/s
|-|-|Bande passante extensible maximale|1 Gbit/s
|-|-|Priorité|P1

Dans ce cas, supposons que la bande passante totale sous licence soit de 8 Gbit/s. Si les deux instances VPX atteignent leurs limites maximales d'éclatement, c'est :

1. VPX1 utilise sa bande passante maximale extensible, c'est-à-dire 2 Gbps, alors il utilise un total de 4 + 2 = 6 Gbit/s
2. VPX2 utilise sa bande passante maximale extensible, c'est-à-dire 1 Gbit/s, alors il utilise un total de 2 + 1 = 3 Gbit/s

Dans ce cas, la bande passante maximale utilisée est supérieure à la capacité autorisée de 8 Gbit/s. Ainsi, pour réduire l'utilisation à une bande passante dans les limites de la capacité autorisée, l'un des VPX devrait renoncer à sa bande passante extensible. Dans ce cas, puisque VPX2 a une priorité inférieure à VPX1, il abandonne donc sa bande passante burstable de 1 Gbit/s. VPX1 continuerait à exploser car il a une priorité plus élevée que VPX2. Dans tous ces scénarios, on s'assure que la bande passante minimale garantie est toujours respectée.

Vérification des statistiques de débit et de consommation de données

Pour chaque VPX, vous pouvez consulter les statistiques de débit et de consommation de données dans les graphiques. Pour accéder aux graphiques, procédez comme suit :

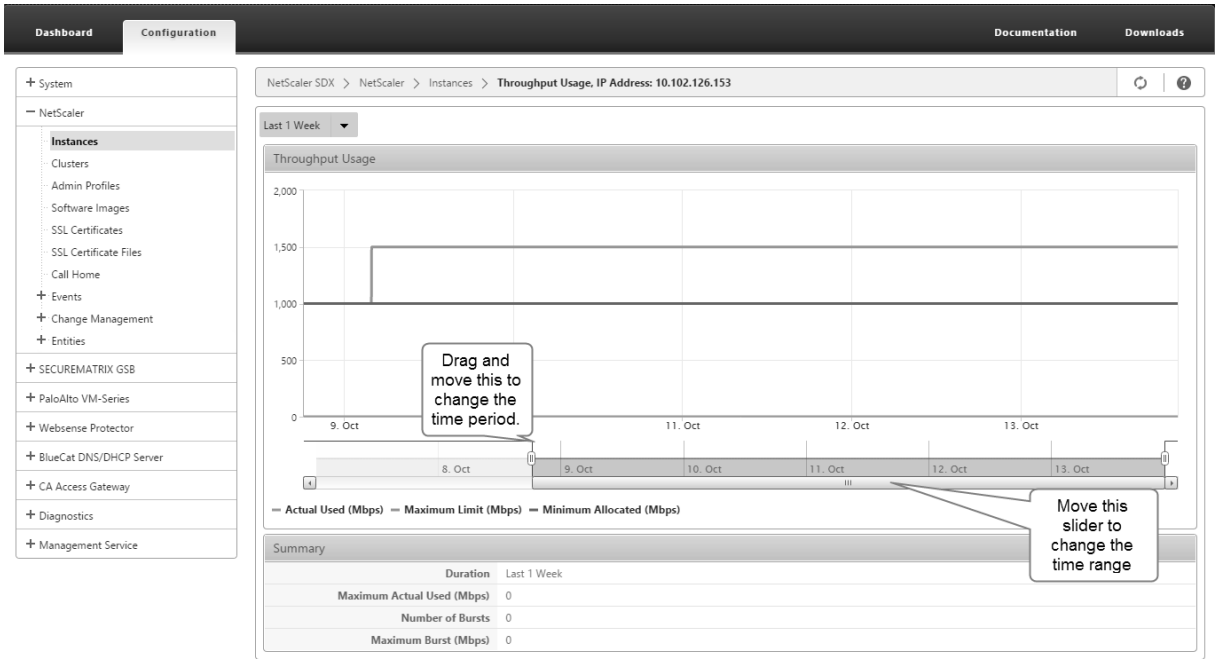
1. Dans le service de gestion SDX, accédez à **la page Configuration > Citrix ADC > Instances** .
2. Sélectionnez une instance VPX, puis cliquez sur la liste **déroulante Action** .
3. Dans la liste, sélectionnez Statistiques de **débit ou Statistiquesd'utilisation des données**.

Les graphiques vous permettent de vérifier les statistiques de consommation et de débit de données pour différentes périodes, telles que :

- Dernière heure
- 1 dernier jour
- La dernière semaine
- Le dernier mois, et
- Le mois précédent

Vous pouvez également sélectionner une période spécifique dans le graphique en ajustant le curseur en bas du graphique. Déplacez votre souris sur les lignes du graphique pour vérifier les données de consommation ou de débit de données pour un moment précis.

L'illustration suivante montre un exemple de graphique des données de débit pendant 1 semaine :



Configurer et gérer les instances Citrix ADC

January 27, 2022

Une fois que vous avez provisionné des instances Citrix ADC sur votre appliance, vous êtes prêt à configurer et à gérer les instances. Commencez par créer une adresse IP de sous-réseau (SNIP), puis enregistrez la configuration. Vous pouvez ensuite effectuer des tâches de gestion de base sur les instances. Vérifiez si vous devez appliquer la configuration d'administration.

Avertissement : Assurez-vous de modifier les interfaces réseau provisionnées ou les VLAN d'une instance à l'aide du service de gestion au lieu d'effectuer les modifications directement sur l'instance.

Créer une adresse SNIP sur une instance Citrix ADC

Vous pouvez attribuer une adresse SNIP aux instances Citrix ADC après son provisionnement sur l'appliance SDX.

Un SNIP est utilisé dans la gestion des connexions et la surveillance des serveurs. Il n'est pas obligatoire de spécifier un SNIP lorsque vous configurez initialement l'appliance Citrix ADC SDX. Vous pouvez attribuer SNIP à l'instance Citrix ADC à partir du service de gestion.

Pour ajouter une adresse SNIP sur une instance Citrix ADC

1. Dans l'onglet **Configuration**, dans le volet de navigation, cliquez sur **Citrix ADC**.
2. Dans le volet d'informations, sous **Configuration Citrix ADC**, cliquez sur **Créer une adresse IP**.
3. Dans la boîte de dialogue **Créer une adresse IP Citrix ADC**, spécifiez des valeurs pour les paramètres suivants.
   - **Adresse IP :** spécifiez l'adresse IP attribuée en tant qu'adresse SNIP.
   - **Masque réseau :** spécifiez le masque de sous-réseau associé à l'adresse SNIP.
   - **Type :** Par défaut, la valeur est SNIP.
   - **Enregistrer la configuration :** sélectionnez cette option pour enregistrer la configuration sur Citrix ADC. La valeur par défaut est false.
   - **Adresse IP de l'instance :** spécifiez l'adresse IP de l'instance Citrix ADC.
4. Cliquez sur **Créer**, puis sur **Fermer**.

Enregistrez la configuration

Vous pouvez enregistrer la configuration en cours d'exécution d'
une instance Citrix ADC à partir du service de gestion.

Pour enregistrer la configuration sur une instance Citrix ADC

1. Dans l'onglet **Configuration**, dans le volet de navigation, cliquez sur **Citrix ADC**.
2. Dans le volet d'informations, sous **Configuration Citrix ADC**, cliquez sur **Enregistrer la configuration**.
3. Dans la boîte de dialogue **Enregistrer la configuration**, dans **Adresse IP de l'instance**, sélectionnez les adresses IP des instances Citrix ADC dont vous souhaitez enregistrer la configuration.
4. Cliquez sur **OK**, puis sur **Fermer**.

Gérer une instance Citrix ADC

Le service de gestion vous permet d'effectuer les opérations suivantes sur les instances Citrix ADC. Vous pouvez effectuer ces opérations à partir du volet **Instances Citrix ADC** de l'onglet **Configuration**

ou du gadget d'instances Citrix ADC sur la page d'accueil.

Démarrez une instance Citrix ADC : démarrez n'importe quelle instance Citrix ADC à partir de l'interface utilisateur du service de gestion. Lorsque l'interface utilisateur du service de gestion transmet cette demande au service de gestion, elle démarre l'instance Citrix ADC.

Arrêtez une instance Citrix ADC : arrêtez toute instance Citrix ADC à partir de l'interface utilisateur du service de gestion. Lorsque l'interface utilisateur du service de gestion transmet cette demande au service de gestion, elle arrête l'instance Citrix ADC.

Redémarrez une instance Citrix ADC : redémarrez l'instance Citrix ADC.

Supprimer une instance Citrix ADC : si vous ne souhaitez pas utiliser d'instance Citrix ADC, vous pouvez supprimer cette instance à l'aide du service de gestion. La suppression d'une instance supprime définitivement l'instance et ses détails associés de la base de données de l'appliance
SDX.

Pour démarrer, arrêter, supprimer ou redémarrer une instance Citrix ADC

1. Dans l'onglet **Configuration**, dans le volet de navigation, cliquez sur **Instances Citrix ADC**.
2. Sélectionnez l'instance Citrix ADC sur laquelle vous souhaitez effectuer l'opération, puis cliquez sur **Démarrer** ou **Arrêter** ou **Supprimer** ou **Redémarrer**.
3. Dans la zone de message Confirmer, cliquez sur **Oui**.

Supprimer les fichiers d'instance Citrix ADC

Vous pouvez supprimer tous les fichiers d'instance Citrix ADC, tels que les XVA, les builds, la documentation, les clés SSL ou les certificats SSL, de l'appliance.

Pour supprimer des fichiers d'instance Citrix ADC

1. Dans l'onglet **Configuration**, dans le volet de navigation, développez **Configuration Citrix ADC**, puis cliquez sur le fichier que vous souhaitez supprimer.
2. Dans le volet d'informations, sélectionnez le nom du fichier, puis cliquez sur **Supprimer**.

Appliquer la configuration d'administration

Au moment du provisionnement d'une instance VPX, le service de gestion crée certaines stratégies, un profil d'administration d'instance (administrateur) et d'autres configurations sur l'instance VPX. Si le service de gestion ne parvient pas à appliquer la configuration d'administration, vous pouvez explicitement pousser la configuration du service de gestion vers l'instance VPX. L'une des raisons de cet échec est peut-être que le service de gestion et l'instance VPX se trouvent sur des sous-réseaux

différents et que le routeur est hors service. Une autre raison peut être que les deux se trouvent sur le même sous-réseau, mais que le trafic doit passer par un commutateur externe et que l'un des liens est en panne.

Pour appliquer la configuration d'administration sur une instance Citrix ADC

1. Dans l'onglet **Configuration**, dans le volet de navigation, cliquez sur **Citrix ADC**.
2. Dans le volet d'informations, sous **Configuration Citrix ADC**, cliquez sur **Appliquer la configuration d'administration**.
3. Dans la boîte de dialogue **Appliquer la configuration d'administration**, dans **Adresse IP de l'instance**, sélectionnez l'adresse IP de l'instance VPX sur laquelle vous souhaitez appliquer la configuration d'administration.
4. Cliquez sur **OK**.

Installation et gestion des certificats SSL

January 27, 2022

Le processus d'installation des certificats SSL implique d'abord le téléchargement du certificat et des fichiers clés sur l'appliance Citrix ADC SDX. Installez ensuite le certificat SSL sur les instances Citrix ADC.

Téléchargez le fichier de certificat sur l'appliance SDX

Pour toute transaction SSL, le serveur a besoin d'un certificat valide et de la paire de clés privées et publiques correspondante. Le fichier de certificat doit être présent sur l'appliance SDX lorsque vous installez le certificat SSL sur les instances Citrix ADC. Vous pouvez également télécharger les fichiers du certificat SSL sur un ordinateur local en tant que sauvegarde.

Dans le volet **Certificats SSL**, vous pouvez afficher les détails suivants.

- **Nom**

Le nom du fichier de certificat.

- **Dernière modification**

Date à laquelle le fichier de certificat a été modifié pour la dernière fois.

- **Taille**

Taille du fichier de certificat en octets.

Pour télécharger des fichiers de certificat SSL sur l'appliance SDX

1. Dans le volet de navigation, développez Service de gestion, puis cliquez sur Fichiers de certificat SSL.
2. Dans le volet Certificats SSL, cliquez sur Upload.
3. Dans la boîte de dialogue Upload SSL Certificate, cliquez sur Browse (Parcourir) et sélectionnez le fichier de certificat que vous souhaitez télécharger.
4. Cliquez sur Charger. Le fichier de certificat s'affiche dans le volet Certificats SSL.

Pour créer une sauvegarde en téléchargeant un fichier de certificat SSL

1. Dans le volet Certificats SSL, sélectionnez le fichier que vous souhaitez télécharger, puis cliquez sur Télécharger.
2. Dans la zone de message, dans la liste Enregistrer, sélectionnez Enregistrer sous.
3. Dans la zone de message Enregistrer sous, accédez à l'emplacement où vous souhaitez enregistrer le fichier, puis cliquez sur Enregistrer.

Téléchargement de fichiers clés SSL sur l'appliance SDX

Pour toute transaction SSL, le serveur a besoin d'un certificat valide et de la paire de clés privées et publiques correspondante. Le fichier clé doit être présent sur l'appliance SDX lorsque vous installez le certificat SSL sur les instances Citrix ADC. Vous pouvez également télécharger les fichiers de clé SSL sur un ordinateur local en tant que sauvegarde.

Dans le volet Clés SSL, vous pouvez afficher les détails suivants.

- **Nom**

Le nom du fichier clé.

- **Dernière modification**

Date à laquelle le fichier clé a été modifié pour la dernière fois.

- **Taille**

Taille du fichier clé en octets.

Pour télécharger des fichiers de clé SSL sur l'appliance SDX

1. Dans le volet de navigation, développez Service de gestion, puis cliquez sur Fichiers de certificat SSL.
2. Dans le volet Certificat SSL, sous l'onglet Clés SSL, cliquez sur Upload.
3. Dans la boîte de dialogue Upload SSL Key File, cliquez sur Browse (Parcourir) et sélectionnez le fichier clé que vous souhaitez télécharger.

4. Cliquez sur Upload pour télécharger le fichier de clé sur l'appliance SDX. Le fichier de clé s'affiche dans le volet Clés SSL.

Pour créer une sauvegarde en téléchargeant un fichier de clé SSL

1. Dans le volet Certificat SSL, sous l'onglet Clés SSL, sélectionnez le fichier que vous souhaitez télécharger, puis cliquez sur Télécharger.
2. Dans la zone de message, dans la liste Enregistrer, sélectionnez Enregistrer sous.
3. Dans la zone de message Enregistrer sous, accédez à l'emplacement où vous souhaitez enregistrer le fichier, puis cliquez sur Enregistrer.

Installation d'un certificat SSL sur une instance Citrix ADC

Le service de gestion vous permet d'installer des certificats SSL sur une ou plusieurs instances Citrix ADC. Avant de commencer à installer le certificat SSL, assurez-vous que vous avez téléchargé le certificat SSL et les fichiers clés sur l'appliance SDX.

Pour installer des certificats SSL sur une instance Citrix ADC

1. Dans le volet de navigation, cliquez sur Citrix ADC.
2. Dans le volet d'informations, sous Configuration Citrix ADC, cliquez sur Installer les certificats SSL.
3. Dans la boîte de dialogue Installer les certificats SSL, spécifiez des valeurs pour les paramètres suivants. (*) indique les champs obligatoires.
    - Fichier de certificat : spécifiez le nom de fichier du certificat valide. Le fichier de certificat doit être présent sur l'appliance SDX.
    - Fichier de clé : spécifiez le nom de fichier de la clé privée utilisée pour créer le certificat. Le fichier clé doit être présent sur l'appliance SDX.
    - Nom du certificat : spécifiez le nom de la paire de clés de certificat à ajouter à Citrix ADC. Longueur maximale : 31
    - Format du certificat : spécifiez le format du certificat SSL pris en charge par Citrix ADC. Une appliance Citrix ADC SDX prend en charge les formats PEM et DER pour les certificats SSL.
    - Mot de passe : spécifiez la phrase secrète qui a été utilisée pour chiffrer la clé privée. Cette option peut être utilisée pour charger des clés privées chiffrées. Longueur maximale : 32. **Remarque : La**clé privée protégée par mot de passe est prise en charge uniquement pour le format PEM.
    - Enregistrer la configuration : spécifiez si la configuration doit être enregistrée sur Citrix ADC. La valeur par défaut est false.
    - Adresse IP de l'instance : spécifiez les adresses IP des instances Citrix ADC sur lesquelles vous souhaitez installer le certificat SSL.

4. Cliquez sur OK, puis sur Fermer.

Mise à jour d'un certificat SSL sur une instance Citrix ADC

Vous pouvez mettre à jour certains paramètres, tels que le fichier de certificat, le fichier de clé et le format de certificat d'un certificat SSL installé sur une instance Citrix ADC. Vous ne pouvez pas modifier l'adresse IP et le nom du certificat.

Pour mettre à jour le certificat SSL sur une instance Citrix ADC

1. Dans le volet de navigation, développez Citrix ADC, puis cliquez sur Certificats SSL.
2. Dans le volet Certificats SSL, cliquez sur Mettre à jour.
3. Dans la boîte de dialogue Modifier le certificat SSL, définissez les paramètres suivants :
    - Fichier de certificat : le nom de fichier du certificat valide. Le fichier de certificat doit être présent sur l'appliance SDX.
    - Fichier de clé : le nom de fichier de la clé privée utilisée pour créer le certificat. Le fichier clé doit être présent sur l'appliance SDX.
    - Format du certificat : format du certificat SSL pris en charge par l'appliance Citrix ADC SDX. L'appliance prend en charge les formats PEM et DER pour les certificats SSL.
    - Mot de passe : le mot de passe qui a été utilisé pour chiffrer la clé privée. Cette option peut être utilisée pour charger des clés privées chiffrées. Longueur maximale : 32 caractères.

      Remarque : Laclé privée protégée par mot de passe est prise en charge uniquement pour le format PEM.
    - Enregistrer la configuration : indiquez si la configuration doit être enregistrée sur l'appliance SDX. La valeur par défaut est false.
    - Aucune vérification de domaine : ne vérifiez pas le nom de domaine lors de la mise à jour du certificat.
4. Cliquez sur OK, puis sur Fermer.

Interrogation des certificats SSL sur les instances Citrix ADC

Si vous ajoutez un certificat SSL directement sur une instance Citrix ADC après vous être connecté à cette instance, le service de gestion n'a pas connaissance de ce nouveau certificat. Pour éviter ce scénario, spécifiez un intervalle d'interrogation après lequel le service de gestion interroge toutes les instances Citrix ADC pour vérifier la présence de nouveaux certificats SSL. Vous pouvez également effectuer un sondage à tout moment à partir du service de gestion. Par exemple, si vous souhaitez obtenir immédiatement une liste des certificats SSL de toutes les instances Citrix ADC.

Pour configurer un intervalle d'interrogation

1. Dans le volet de navigation, développez Citrix ADC, puis cliquez sur Certificats SSL.
2. Dans le volet Certificats SSL, cliquez sur Configurer l'intervalle d'interrogation.
3. Dans la boîte de dialogue Configurer l'intervalle d'interrogation, définissez les paramètres suivants :
   - Intervalle d'interrogation : délai après lequel le service de gestion interroge les instances Citrix ADC.
   - Unité d'intervalle : unité de temps. Valeurs possibles : heures, minutes. Par défaut : heures.
4. Cliquez sur OK, puis sur Fermer.

Pour effectuer un sondage immédiat

1. Dans le volet de navigation, développez Citrix ADC, puis cliquez sur Certificats SSL.
2. Dans le volet Certificats SSL, cliquez sur Sonder maintenant.
3. Dans la boîte de dialogue Confirmer, cliquez sur Oui. Le volet Certificats SSL est actualisé et les nouveaux certificats, le cas échéant, apparaissent dans la liste.

Autoriser le mode L2 sur une instance Citrix ADC

January 27, 2022

En mode de couche 2 (L2), une instance Citrix ADC agit en tant que pont d'apprentissage et transmet tous les paquets dont elle n'est pas la destination. Certaines fonctionnalités, telles que Citrix CloudBridge, nécessitent que le mode L2 soit activé sur l'instance Citrix ADC. Lorsque le mode L2 est activé, l'instance peut recevoir et transférer des paquets pour des adresses MAC autres que sa propre adresse MAC. Toutefois, pour activer le mode L2 sur une instance Citrix ADC exécutée sur une appliance Citrix ADC SDX, l'administrateur doit d'abord autoriser le mode L2 sur cette instance. Si vous autorisez le mode L2, vous devez prendre des précautions pour éviter les boucles de pontage.

Précautions :

1. Sur une interface 1/x donnée, les paquets non balisés doivent être autorisés sur une seule instance. Pour toutes les autres instances activées sur la même interface, vous devez sélectionner Marqué.

   Remarque :

   Citrix vous recommande de sélectionner Marqué pour toutes les interfaces attribuées aux instances en mode L2. Si vous sélectionnez balisé, vous ne pouvez pas recevoir de paquets non marqués sur cette interface.

Si vous avez sélectionné Marqué pour une interface affectée à une instance, connectez-vous à cette instance et configurez un VLAN 802.1q pour recevoir des paquets sur cette interface.

2. Pour les interfaces 1/x et 10/x partagées par les instances Citrix ADC sur lesquelles le mode L2 est autorisé, assurez-vous que les conditions suivantes sont remplies :
   - Le filtrage VLAN est activé sur toutes les interfaces.
   - Chaque interface se trouve sur un VLAN 802.1q différent.
   - Une seule instance peut recevoir des paquets non balisés sur l'interface. Si cette interface est affectée à d'autres instances, vous devez sélectionner Marqué sur cette interface pour ces instances.
3. Si vous autorisez des paquets non balisés sur une interface 1/x pour une instance sur laquelle le mode L2 est autorisé, aucune autre instance ne peut recevoir de paquets non marqués sur cette interface. Cette condition s'applique indépendamment du fait que le mode L2 soit autorisé ou non autorisé sur l'autre instance.
4. Si vous autorisez des paquets non balisés sur une interface 1/x pour une instance dont le mode L2 est désactivé, une instance avec le mode L2 autorisé ne peut pas recevoir de paquets non marqués sur cette interface.
5. Si une interface 0/x est affectée à l'instance1 provisionnée en mode L2, et que cette interface est également affectée à l'instance2, sélectionnez Marqué pour toutes les autres interfaces affectées à l'instance2.

Remarque : Si les deux interfaces de gestion sont affectées à une instance en mode L2, seule l'une de ces interfaces peut être affectée à une autre instance ADC avec le mode L2 activé. En d'autres termes, vous ne pouvez pas associer les deux interfaces de gestion à plusieurs instances Citrix ADC sur lesquelles le mode L2 est activé.

Pour autoriser le mode L2 sur une instance

1. Dans l'Assistant Provisionnement ADC ou l'Assistant Modification du CAN, sur la page **Paramètres réseau**, sélectionnez **Autoriser le mode L2**.
   Remarque : Vous pouvez activer le paramètre Autoriser le mode L2 sur une instance lorsque vous provisionnez l'instance ou lorsque l'instance est en cours d'exécution.
2. Suivez les instructions de l'assistant.
3. Cliquez sur **Terminer**, puis sur **Fermer**.

Configuration d'un MAC virtuel sur une interface

January 6, 2023

Une instance Citrix ADC utilise un MAC virtuel (VMAC) pour les configurations haute disponibilité (actif-actif ou actif-veille). Une adresse MAC virtuelle (VMAC) est une entité flottante partagée par les nœuds principal et secondaire dans une configuration haute disponibilité.

Dans une configuration haute disponibilité, le nœud principal possède toutes les adresses IP flottantes, telles que les adresses MIP, SNIP et VIP. Le nœud principal répond aux demandes ARP (Address Resolution Protocol) pour ces adresses IP avec sa propre adresse MAC. En conséquence, la table ARP d'un périphérique externe (par exemple, un routeur en amont) est mise à jour avec l'adresse IP flottante et l'adresse MAC du nœud principal.

Lorsqu'un basculement se produit, le nœud secondaire prend le relais en tant que nouveau nœud principal. Il utilise ensuite l'ARP gratuit (GARP) pour annoncer les adresses IP flottantes qu'il a acquises auprès du principal. Cependant, l'adresse MAC annoncée par le nouveau serveur principal est l'adresse MAC de sa propre interface.

Certains appareils (notamment quelques routeurs) n'acceptent pas les messages GARP générés par l'appliance Citrix ADC SDX. De tels dispositifs conservent l'ancien mappage IP vers MAC annoncé par l'ancien nœud principal, et un site peut tomber en panne en conséquence.

Vous pouvez résoudre ce problème en configurant un VMAC sur les deux nœuds d'une paire HA. Les deux nœuds possèdent alors des adresses MAC identiques. Par conséquent, en cas de basculement, l'adresse MAC du nœud secondaire reste inchangée et les tables ARP des périphériques externes n'ont pas besoin d'être mises à jour.

La configuration d'un VMAC est un processus en deux étapes :

1. Configurez le VMAC sur le service de gestion SDX. Vous ajoutez un VRID pour une interface ou un canal LA. Configurez le VMAC sur le service de gestion SDX.
2. Configurez le VMAC sur l'instance Citrix. Pour plus d'informations, consultez l'article de support du groupe Configurer un VMAC sur un canal .

Configurez le VMAC sur le service de gestion SDX

Pour configurer VMAC, ajoutez un VRID IPv4 ou IPv6 à une interface ou à un canal LA à partir du service de gestion. Le service de gestion génère en interne un VMAC. Spécifiez le même VRID lorsque vous configurez le mode actif-actif sur l'instance Citrix ADC. Cette configuration active-active n'est pas prise en charge sur les interfaces Mellanox.

Gardez à l'esprit les points suivants :

1. Ajoutez un VRID à partir du service de gestion et spécifiez le même VRID dans l'instance Citrix ADC. Si vous ajoutez un VRID directement dans l'instance Citrix ADC, l'instance ne peut pas recevoir de paquet dont l'adresse MAC de destination est une adresse VMAC.
2. Vous ne pouvez pas utiliser le même VRID sur différentes instances exécutées dans le même dispositif SDX.

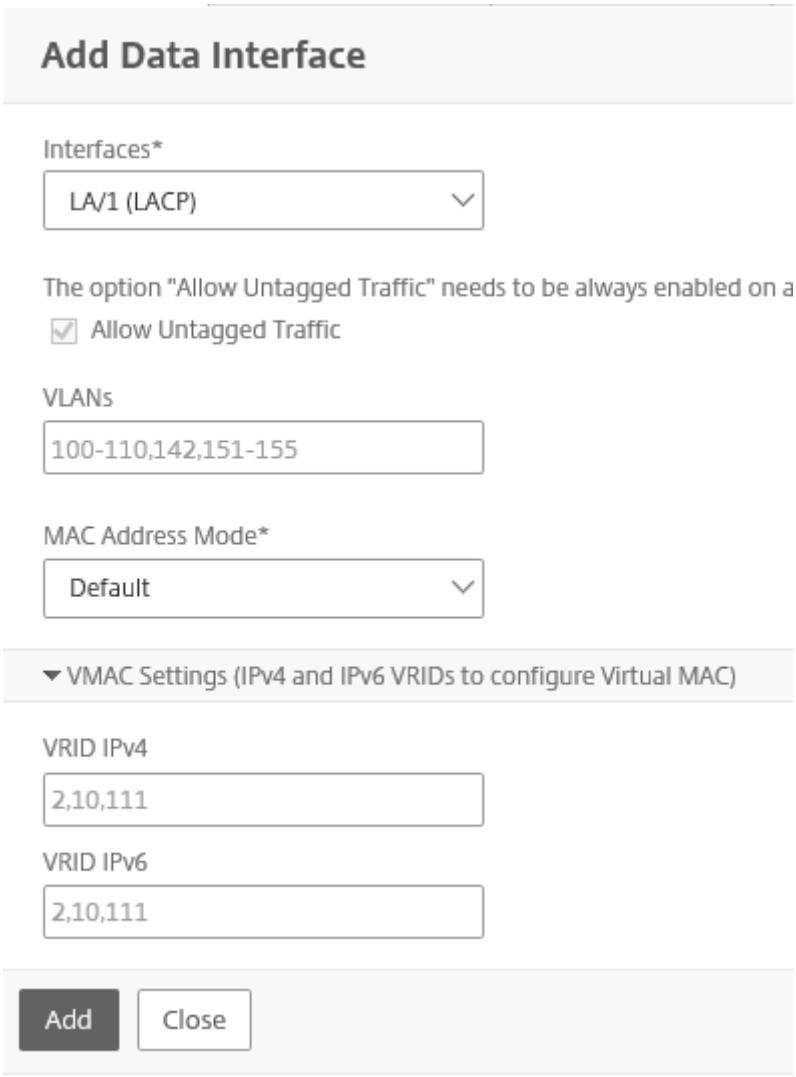
3. Vous pouvez ajouter ou supprimer les VRID d'une interface affectée à une instance pendant que l'instance est en cours d'exécution.
4. Dans une configuration actif-actif, vous pouvez spécifier plusieurs VRID pour une interface affectée à une instance. Le déploiement actif-actif n'est pas pris en charge sur les interfaces Mellanox.
5. Un maximum de 86 VMAC sont autorisés sur une interface 10G et un maximum de 16 VMAC sur une interface 1G. Si aucun autre filtre VMAC n'est disponible, réduisez le nombre de VRID sur une autre instance.

Vous pouvez ajouter un VRID au moment de l'ajout d'une instance Citrix ADC VPX, ou vous pouvez modifier une instance Citrix ADC existante pour ajouter un VRID.

Pour ajouter un VRID IPv4 ou IPv6 à une interface ou à un canal LA

1. Lors de l'ajout d'une instance VPX sur SDX, sous **Paramètres réseau**, sélectionnez **Interfaces de données**. Pour plus d'informations sur la façon d'ajouter une instance VPX sur SDX, consultez Ajouter une instance Citrix ADC.
2. Dans le menu déroulant **Interfaces**, sélectionnez l'interface ou le canal LA.
3. Sous Paramètres VMAC, puis définissez l'une des valeurs suivantes ou les deux :
   - VRID IPv4 : VRID IPv4 qui identifie le VMAC. Valeurs possibles : 1—255.
   - VRID IPv6 : VRID IPv6 qui identifie le VMAC. Valeurs possibles : 1—255.

     Remarque : Utilisez une virgule pour séparer plusieurs VRID. Par exemple, 12,24.
4. Cliquez sur **Ajouter** pour ajouter les paramètres **VMAC** à l'interface.
5. Cliquez sur **Terminer**, puis sur **Fermer**.



Si l'instance est déjà provisionnée, pour ajouter un VRID IPv4 ou IPv6, procédez comme suit.

1. Dans le service de gestion SDX, accédez à **Configuration > Citrix ADC > Instances**.
2. Sélectionnez l'instance et cliquez sur **Modifier**.
3. Sous **Interfaces de données**, sélectionnez l'interface et cliquez sur Modifier.
4. Sous Paramètres VMAC, définissez les valeurs VRID. Cliquez sur **Ajouter**, puis sur **Terminé**.

Générez des adresses MAC de partition pour configurer une partition d'administration sur une instance Citrix ADC dans l'appliance SDX

January 27, 2022

Une instance Citrix ADC sur une appliance Citrix ADC SDX peut être partitionnée en entités logiques appelées partitions d'administration. Chaque partition peut être configurée et utilisée en tant

qu'instance Citrix ADC distincte. Pour plus d'informations sur les partitions d'administration, consultez Partitionnement d'administration.

Pour utiliser des partitions d'administration avec une configuration VLAN partagée, vous avez besoin d'une adresse MAC virtuelle pour chaque partition. Une telle adresse MAC virtuelle est appelée adresse MAC de partition (PMAC), et elle est utilisée pour classer le trafic reçu sur un VLAN partagé. Cette adresse PMAC est utilisée sur tous les VLAN partagés liés à cette partition.

Générez et configurez l'adresse PMAC à l'aide de l'interface utilisateur du service de gestion, avant d'utiliser la partition d'administration. Le service de gestion vous permet de générer des adresses MAC de partition en :

- Utilisation d'une adresse MAC de base
- Spécification d'adresses MAC personnalisées
- Adresses MAC générées aléatoirement

Remarque
Après avoir généré les adresses MAC de partition, vous devez redémarrer l'instance Citrix ADC avant de configurer les partitions d'administration.

Pour générer les adresses MAC de la partition à l'aide d'une adresse MAC de base :

1. Dans l'onglet **Configuration**, dans le volet gauche, développez **Citrix ADC**, puis cliquez sur **Instances**.
2. Dans le volet **Instances**, sélectionnez l'instance Citrix ADC pour laquelle vous souhaitez générer les adresses MAC de partition.
3. Dans la liste déroulante **Action**, cliquez sur **Partitionner des MAC**.
4. Dans le volet **Partition MAC**, cliquez sur **Générer**.
5. Dans la boîte de dialogue **Générer des MAC de partition**, dans la section **Méthode de génération**, sélectionnez **Utilisation de l'adresse de base**.
6. Dans le champ **Adresse MAC de base**, saisissez l'adresse MAC de base.
7. Dans le champ **Incrément par**, saisissez la valeur selon laquelle l'adresse MAC de base doit être incrémentée pour chaque adresse MAC suivante.
   Par exemple, si vous avez spécifié l'adresse MAC de base comme 00:A1:C 9:11:C 8:11 et la valeur d'incrément comme 2, l'adresse MAC suivante est générée sous la forme 00:A1:C 9:11:C 8:13.
8. Dans le champ **Nombre**, saisissez le nombre d'adresses MAC de partition que vous souhaitez générer.
9. Cliquez sur **Générer**.

Pour générer les adresses MAC de partition en spécifiant des adresses MAC personnalisées :

1. Dans l'onglet **Configuration**, dans le volet gauche, développez **Citrix ADC**, puis cliquez sur **Instances**.
2. Dans le volet **Instances**, sélectionnez l'instance Citrix ADC pour laquelle vous souhaitez générer les adresses MAC de partition.

3. Dans la liste déroulante **Action**, cliquez sur **Partitionner des MAC**.
4. Dans le volet **Partition MAC**, cliquez sur **Générer**.
5. Dans la boîte de dialogue **Générer des MAC de partition**, dans la section **Méthode de génération**, sélectionnez Spécifié par **l'utilisateur**.
6. Dans le champ **Adresses MAC**, saisissez une adresse MAC.
7. Cliquez sur l'icône **+**, puis saisissez l'adresse MAC suivante. Répétez l'opération pour spécifier d'autres adresses MAC personnalisées.
8. Cliquez sur **Générer**.

Pour générer aléatoirement les adresses MAC de la partition :

1. Dans l'onglet **Configuration**, dans le volet gauche, développez **Citrix ADC**, puis cliquez sur **Instances**.
2. Dans le volet **Instances**, sélectionnez l'instance Citrix ADC pour laquelle vous souhaitez générer les adresses MAC de partition.
3. Dans la liste déroulante **Action**, cliquez sur **Partitionner des MAC**.
4. Dans le volet **Partition MAC**, cliquez sur **Générer**.
5. Dans la boîte de dialogue **Générer des MAC de partition**, dans la section **Méthode de génération**, sélectionnez **Aléatoire**.
6. Dans le champ **Nombre**, saisissez le nombre d'adresses MAC de partition que vous souhaitez générer.
7. Cliquez sur **Générer**.

Après avoir généré des adresses MAC de partition dans une appliance SDX, utilisez les adresses MAC de partition générées pour configurer les partitions d'administration sur l'instance Citrix ADC.

Gestion des modifications pour les instances VPX

January 27, 2022

Vous pouvez suivre toutes les modifications apportées à la configuration sur une instance Citrix ADC VPX à partir du service de gestion. Le volet d'informations répertorie le nom de l'appareil avec l'adresse IP, la date et l'heure de sa dernière mise à jour. Il indique également s'il existe une différence entre la configuration enregistrée et la configuration en cours. Sélectionnez un périphérique pour afficher sa configuration en cours, sa configuration enregistrée, l'historique des modifications de configuration et toute différence entre les configurations avant et après une mise à niveau. Vous pouvez télécharger la configuration d'une instance VPX sur votre ordinateur local. Par défaut, le service de gestion interroge toutes les instances toutes les 24 heures, mais vous pouvez modifier cet intervalle. Vous pouvez créer un modèle d'audit en copiant les commandes à partir d'un fichier de configuration existant. Vous pouvez ensuite utiliser ce modèle pour rechercher tout changement dans la configuration d'une instance et prendre des mesures correctives si nécessaire.

Pour afficher la gestion des modifications pour les instances VPX

1. Dans l'onglet **Configuration**, accédez à **Citrix ADC > Gestion des modifications**.
2. Dans le volet **Gestion des modifications**, sélectionnez une instance VPX, puis dans la liste **Action**, sélectionnez l'une des options suivantes :
   - Configuration en cours d'exécution : affiche la configuration en cours de l'instance VPX sélectionnée dans une nouvelle fenêtre.
   - Configuration enregistrée : affiche la configuration enregistrée de l'instance VPX sélectionnée dans une nouvelle fenêtre.
   - Vs enregistrés. Running Diff : affiche la configuration enregistrée, la configuration en cours et la commande corrective (la différence).
   - Diff de l'historique des révisions : affiche la différence entre le fichier de configuration de base et le deuxième fichier de configuration.
   - Pré c. Post Upgrade Diff : affiche la différence de configuration avant et après une mise à niveau, ainsi que la commande corrective (la différence).
   - Différence de modèle (Template Diff) : affiche la différence entre la configuration enregistrée ou en cours et le modèle. Vous pouvez enregistrer cette différence en tant que fichier de commandes. Pour appliquer la configuration du modèle à l'instance, appliquez ce fichier de commandes à l'instance.
   - Télécharger : télécharge la configuration de l'instance VPX sélectionnée et l'enregistre sur un appareil local.

Pour rechercher des mises à jour de la configuration de l'une des instances Citrix ADC

1. Dans l'onglet **Configuration**, accédez à **Citrix ADC > Gestion des modifications**.
2. Dans le volet **Gestion des modifications**, dans la liste **Action**, sélectionnez l'une des options suivantes :
   - Poll Now : le service de gestion effectue une interrogation immédiate pour les mises à jour de la configuration (ns.conf) de l'une des instances VPX installées sur l'appliance.
   - Configurer l'intervalle d'interrogation : délai après lequel le service de gestion interroge les mises à jour de la configuration (ns.conf) de l'une des instances VPX installées sur l'appliance. L'intervalle d'interrogation par défaut est de 24 heures.

Pour configurer un modèle d'audit pour une instance Citrix ADC

1. Ouvrez un fichier de configuration existant et copiez sa liste de commandes.
2. Dans l'onglet **Configuration**, accédez à **Citrix ADC > Gestion des modifications > Modèles d'audit**.
3. Dans le volet d'informations, cliquez sur **Ajouter**.

4. Dans la boîte **de dialogue Ajouter un modèle**, ajoutez un nom et une description pour le modèle.
5. Dans la zone de texte **Commande**, collez la liste des commandes que vous avez copiées à partir du fichier de configuration.
6. Cliquez sur **Créer**, puis sur **Fermer**.

Surveiller les instances Citrix ADC

January 27, 2022

Une vue de haut niveau des performances de l'appliance et des instances VPX provisionnées sur l'appliance s'affiche sur la page Surveillance de l'interface utilisateur du service de gestion. Après avoir provisionné et configuré l'instance Citrix ADC, vous pouvez effectuer diverses tâches pour surveiller l'instance Citrix ADC.

Afficher les propriétés des instances VPX

L'interface utilisateur du service de gestion affiche la liste et la description de toutes les instances VPX provisionnées sur l'appliance SDX. Utilisez le volet des **instances Citrix ADC** pour afficher des détails, tels que le nom et l'adresse IP de l'instance, l'utilisation du processeur et de la mémoire, le débit et la mémoire totale affectée à l'instance.

Cliquez sur l'adresse IP de l'instance VPX pour ouvrir l'utilitaire de configuration (GUI) de cette instance dans un nouvel onglet ou un nouveau navigateur.

Pour afficher les propriétés des instances VPX

1. Dans l'onglet Configuration, dans le volet gauche, développez Configuration Citrix ADC, puis cliquez sur Instances.
   Remarque : Vous pouvez également afficher les propriétés d'une instance VPX à partir de l'onglet
   Accueil.
2. Dans le volet d'instance Citrix ADC, vous pouvez afficher les détails suivants pour l'instance Citrix ADC :
   - **Nom : nom** d'hôte attribué à l'instance Citrix ADC lors du provisionnement.
   - **État de la machine virtuelle :** état de la machine virtuelle.
   - **État Citrix ADC :** état de l'instance Citrix ADC.
   - **Adresse IP :** adresse IP de l'instance Citrix ADC. Cliquez sur l'adresse IP pour ouvrir l'interface graphique de cette instance dans un nouvel onglet ou un nouveau navigateur.

- **Rx (Mbit/s) :** paquets reçus sur l'instance Citrix ADC.
- **Tx (Mbps) :** paquets transmis par l'instance Citrix ADC.
- **Req/s HTTP :** nombre total de demandes HTTP reçues sur l'instance Citrix ADC toutes les secondes.
- **Utilisation du processeur (%) :** pourcentage d'utilisation du processeur sur Citrix ADC.
- **Utilisation de la mémoire (%) :** pourcentage d'utilisation de la mémoire sur Citrix ADC.

3. Cliquez sur la flèche en regard du nom d'une instance Citrix ADC pour afficher les propriétés de cette instance. Vous pouvez également cliquer sur **Tout développer** pour afficher les propriétés de toutes les instances Citrix ADC. Vous pouvez afficher les propriétés suivantes :

   - **Masque réseau :** adresse IP du masque de réseau de l'instance Citrix ADC.
   - **Passerelle :** adresse IP de la passerelle par défaut, le routeur qui transfère le trafic en dehors du sous-réseau dans lequel l'instance est installée.
   - **Paquets par seconde :** nombre total de paquets passant par seconde.
   - **Cartes réseau :** noms des cartes réseau utilisées par l'instance Citrix ADC, ainsi que la fonction virtuelle attribuée à chaque interface.
   - **Version : version** de génération, date de génération et heure du logiciel Citrix ADC en cours d'exécution sur l'instance.
   - **Nom d'hôte :** nom d'hôte de l'instance Citrix ADC.
   - **Mémoire totale (Go) :** mémoire totale affectée à l'instance Citrix ADC.
   - **Débit (Mbit/s) :** débit total de l'instance Citrix ADC.
   - **Up Since :** date et heure écoulées depuis le moment où l'instance est restée en permanence dans l'état UP.
   - **Chips SSL :** nombre total de puces SSL attribuées à l'instance.
   - **Adresse IP homologue : adresse** IP de l'homologue de cette instance Citrix ADC si elle se trouve dans une configuration HA.
   - **État :** état des opérations effectuées sur une instance Citrix ADC, tel que l'état indiquant si l'inventaire de l'instance est terminé.
   - **État principal HA :** état de l'appareil. L'état indique si l'instance est configurée dans une installation autonome ou principale ou fait partie d'une configuration haute disponibilité. Dans une configuration haute disponibilité, l'état indique également s'il est en mode principal ou secondaire.
   - **État de synchronisation HA :** mode de l'état de synchronisation HA, par exemple activé ou désactivé.
   - **Description :** La description saisie lors du provisionnement de l'instance Citrix ADC.

> **Remarques :**
>
> Lorsqu'une instance ADC est hors service en raison d'un échec d'authentification, la couleur de l'état de l'instance passe au gris si les conditions suivantes sont remplies :

- Le mot de passe d'instance ADC est modifié directement à l'aide de l'instance CLI.
- Le mot de passe ne correspond pas au mot de passe du profil d'administrateur d'instance stocké dans le service de gestion.
- La session précédente est perdue après le premier redémarrage de l'instance.

En règle générale, lorsqu'une instance est hors service, la couleur de l'état de l'instance est jaune.

Pour récupérer l'instance, effectuez l'une des opérations suivantes :

- Dans l'interface de ligne de commande de l'instance, modifiez le mot de passe de l'instance pour qu'il corresponde au mot de passe du profil administrateur de l'instance. Redécouvrez ensuite l'instance à partir du service de gestion.
- Créez un profil d'administrateur avec le même mot de passe que le mot de passe actuel de l'instance ADC. Ensuite, mettez à jour l'instance ADC avec le nouveau profil d'administrateur.

Afficher la configuration en cours et enregistrée d'une instance Citrix ADC

En utilisant le service de gestion, vous pouvez afficher la configuration en cours d'exécution d'une instance Citrix ADC. Vous pouvez également afficher la configuration enregistrée d'une instance Citrix ADC et l'heure à laquelle la configuration a été enregistrée.

Pour afficher la configuration en cours et enregistrée d'une instance Citrix ADC

1. Dans l'onglet Configuration, dans le volet gauche, développez Configuration Citrix ADC, puis cliquez sur Instances.
2. Dans le volet Instances Citrix ADC, cliquez sur l'instance Citrix ADC dont vous souhaitez afficher la configuration en cours ou enregistrée.
3. Pour afficher la configuration en cours, cliquez sur Configuration en cours d'exécution, et pour afficher la configuration enregistrée, cliquez sur Configuration enregistrée.
4. Dans la fenêtre Citrix ADC Running Config ou Citrix ADC Saved Config, vous pouvez afficher la configuration en cours ou enregistrée de l'instance Citrix ADC.

Ping sur une instance Citrix ADC

Vous pouvez envoyer un ping à une instance Citrix ADC à partir du service de gestion pour vérifier si l'appareil est accessible.

Pour envoyer un ping à une instance Citrix ADC

1. Dans l'onglet Configuration, dans le volet gauche, développez Configuration Citrix ADC, puis cliquez sur Instances.

2. Dans le volet Instances Citrix ADC, cliquez sur l'instance Citrix ADC à laquelle vous souhaitez envoyer un ping, puis cliquez sur Ping. Dans la zone de message Ping, vous pouvez voir si le ping a réussi.

Suivre l'itinéraire d'une instance Citrix ADC

Vous pouvez suivre l'itinéraire d'un paquet du service de gestion vers une instance Citrix ADC en déterminant le nombre de sauts utilisés pour atteindre l'instance.

Pour suivre l'itinéraire d'une instance Citrix ADC

1. Dans l'onglet Configuration, dans le volet gauche, développez Configuration Citrix ADC, puis cliquez sur Instances.
2. Dans le volet Instances Citrix ADC, cliquez sur l'instance Citrix ADC que vous souhaitez suivre, puis cliquez sur TraceRoute. Dans la boîte de message Traceroute, vous pouvez afficher l'itinéraire vers Citrix ADC.

Redécouvrez une instance Citrix ADC

Vous pouvez redécouvrir une instance Citrix ADC lorsque vous devez afficher l'état et la configuration les plus récents d'une instance Citrix ADC.

Lors de la redécouverte, le service de gestion récupère la configuration. Par défaut, le service de gestion planifie la redécouverte des appareils toutes les 30 minutes.

Pour redécouvrir une instance Citrix ADC

1. Dans l'onglet **Configuration**, dans le volet gauche, développez **Configuration Citrix ADC**, puis cliquez sur **Instances**.
2. Dans le volet **Instances Citrix ADC**, cliquez sur l'instance Citrix ADC que vous souhaitez redécouvrir, puis cliquez sur **Redécouvrir**.
3. Dans la zone de message Confirmer, cliquez sur **Oui**.

Utilisez des journaux pour surveiller les opérations et les événements

January 27, 2022

Utilisez les journaux d'audit et de tâches pour surveiller les opérations effectuées sur le service de gestion et sur les instances Citrix ADC SDX. Vous pouvez également utiliser le journal des événements

pour suivre tous les événements relatifs aux tâches effectuées sur le service de gestion et Citrix Hypervisor.

Afficher les journaux d'audit

Toutes les opérations effectuées à l'aide du service de gestion sont consignées dans la base de données de l'appliance. Utilisez les journaux d'audit pour afficher les opérations effectuées par un utilisateur du service de gestion, la date et l'heure, ainsi que l'état de réussite ou d'échec de chaque opération. Vous pouvez également trier les détails par utilisateur, opération, durée de l'audit, état, etc. en cliquant sur l'en-tête de colonne approprié.

La pagination est prise en charge dans le volet Journal d'audit. Sélectionnez le nombre d'enregistrements à afficher sur une page. Par défaut, 25 enregistrements sont affichés sur une page.

Pour afficher les journaux d'audit, procédez comme suit :

1. Dans le volet de navigation, développez Système, puis cliquez sur Audit.
2. Dans le volet Journal d'audit, vous pouvez afficher les informations suivantes.
    - **Nom d'utilisateur :** utilisateur du service de gestion qui a effectué l'opération.
    - **Adresse IP :** adresse IP du système sur lequel l'opération a été effectuée.
    - **Port :** port sur lequel le système était en cours d'exécution lorsque l'opération a été effectuée.
    - **Type de ressource :** le type de ressource utilisé pour effectuer l'opération, tel que xen_vpx_image et connexion.
    - **Nom de la ressource :** le nom de la ressource utilisée pour effectuer l'opération, tel que vpx_image_name et le nom d'utilisateur utilisé pour se connecter.
    - **Audit Time :** heure à laquelle le journal d'audit a été généré.
    - **Opération :** tâche qui a été effectuée, telle que l'ajout, la suppression et la déconnexion.
    - **État :** état de l'audit, par exemple Réussite ou Échec.
    - **Message :** message décrivant la cause de l'échec si l'opération a échoué et l'état de la tâche, tel que Terminé, si l'opération a réussi.
3. Pour trier les journaux en fonction d'un champ particulier, cliquez sur l'en-tête de la colonne.

Afficher les journaux des tâches

Utilisez les journaux des tâches pour afficher et suivre les tâches, telles que la mise à niveau des instances et l'installation de certificats SSL, qui sont exécutées par le service de gestion sur les instances Citrix ADC. Le journal des tâches vous permet de voir si une tâche est en cours, a échoué ou a réussi.

La pagination est prise en charge dans le **volet Journal** des tâches. Sélectionnez le nombre d'enregistrements à afficher sur une page. Par défaut, 25 enregistrements sont affichés sur une page.

Pour afficher le journal des tâches, procédez comme suit :

1. Dans le volet de navigation, développez Diagnostics, puis cliquez sur Journal des tâches.
2. Dans le volet Journal des tâches, vous pouvez afficher les détails suivants.
    - **Nom :** le nom de la tâche en cours d'exécution ou qui a déjà été exécutée.
    - **État :** état de la tâche, par exemple En cours, Terminée ou Échec.
    - **Exécuté par :** utilisateur du service de gestion qui a effectué l'opération.
    - **Heure de début :** l'heure à laquelle la tâche a commencé.
    - **Heure de fin :** l'heure à laquelle la tâche s'est terminée.

Afficher les journaux des périphériques de tâches

Utilisez les journaux des périphériques de tâches pour afficher et suivre les tâches effectuées sur chaque instance SDX. Le journal de la machine de tâches vous permet de voir si une tâche est en cours, a échoué ou a réussi. Il affiche également l'adresse IP de l'instance sur laquelle la tâche est effectuée.

Pour afficher le journal de la machine de tâches, procédez comme suit :

1. Dans le volet de navigation, développez **Diagnostics**, puis cliquez sur **Journal des tâches**.
2. Dans le volet **Journal des tâches**, double-cliquez sur la tâche pour afficher les détails du périphérique de tâches.
3. Dans le volet **Journal de la machine de tâches**, pour trier les journaux en fonction d'un champ particulier, cliquez sur l'en-tête de la colonne.

Afficher les journaux des commandes de tâches

Utilisez les journaux des commandes de tâches pour afficher l'état de chaque commande d'une tâche exécutée sur une instance Citrix ADC. Le journal des commandes de tâches vous permet de voir si une commande a été exécutée avec succès ou si elle a échoué. Il affiche également la commande exécutée et la raison pour laquelle une commande a échoué.

Pour afficher le journal des commandes de tâches, procédez comme suit :

1. Dans le volet de navigation, développez **Diagnostics**, puis cliquez sur **Journal des tâches**.
2. Dans le volet **Journal des tâches**, double-cliquez sur la tâche pour afficher les détails du périphérique de tâches.
3. Dans le volet **Journal de la machine de tâches**, double-cliquez sur la tâche pour afficher les détails de la commande de tâche.
4. Dans le volet **Journal des commandes de tâches**, pour trier les journaux en fonction d'un champ particulier, cliquez sur l'en-tête de la colonne.

Voir les événements

Utilisez le volet **Événements** de l'interface utilisateur du service de gestion pour surveiller les événements générés par le service de gestion pour les tâches effectuées sur le service de gestion.

Pour afficher les événements, procédez comme suit :

1. Accédez à **Système > Événements**.
2. Dans le volet **Événements**, vous pouvez afficher les détails suivants.
    - **Gravité :** gravité d'un événement, qui peut être critique, majeur, mineur, clair et informatif.
    - **Source :** adresse IP sur laquelle l'événement est généré.
    - **Date :** date à laquelle l'événement est généré.
    - **Catégorie : catégorie** d'événement, telle que PolicyFailed et DeviceConfigChange.
    - **Message :** le message décrivant l'événement.
3. Pour trier les événements en fonction d'un champ particulier, cliquez sur l'en-tête de la colonne.

Cas d'utilisation pour les appliances Citrix ADC SDX

January 27, 2022

Pour les composants réseau (tels que les pare-feu et les contrôleurs de mise à disposition d'applications), la prise en charge de l'architecture mutualisée a toujours impliqué la possibilité de découper un seul périphérique en plusieurs partitions logiques. Cette approche permet de mettre en œuvre différents ensembles de politiques pour chaque locataire sans avoir besoin de nombreux appareils distincts. Traditionnellement, il est toutefois sévèrement limité en termes de degré d'isolement atteint.

De par sa conception, l'appliance SDX n'est pas soumise aux mêmes limitations. Dans l'architecture SDX, chaque instance s'exécute en tant que machine virtuelle (VM) distincte avec son propre noyau Citrix ADC dédié, des ressources CPU, des ressources de mémoire, un espace d'adressage et une allocation de bande passante. Les E/S réseau sur l'appliance SDX maintiennent non seulement les performances globales du système, mais permettent également une séparation complète du trafic du plan de données et du plan de gestion de chaque locataire. Le plan de gestion inclut les interfaces 0/x. Le plan de données inclut les interfaces 1/x et 10/x. Un plan de données peut également être utilisé comme plan de gestion.

Les principaux cas d'utilisation d'une appliance SDX sont liés à la consolidation, qui réduit le nombre de réseaux nécessaires tout en maintenant l'isolation de la gestion. Voici les scénarios de consolidation de base :

- Consolidation lorsque le service de gestion et les instances Citrix ADC se trouvent sur le même réseau.

- Consolidation lorsque les instances du service de gestion et de Citrix ADC se trouvent sur des réseaux différents mais que toutes les instances se trouvent sur le même réseau.
- Consolidation de la sécurité.
- Consolidation avec des interfaces dédiées pour chaque instance.
- Consolidation avec partage d'un port physique par plusieurs instances.

Consolidation lorsque le service de gestion et les instances Citrix ADC se trouvent sur le même réseau

June 13, 2022

Un type simple de cas de consolidation sur l'appliance SDX est la configuration du service de gestion et des instances Citrix ADC dans le cadre du même réseau. Ce cas d'utilisation est applicable si :

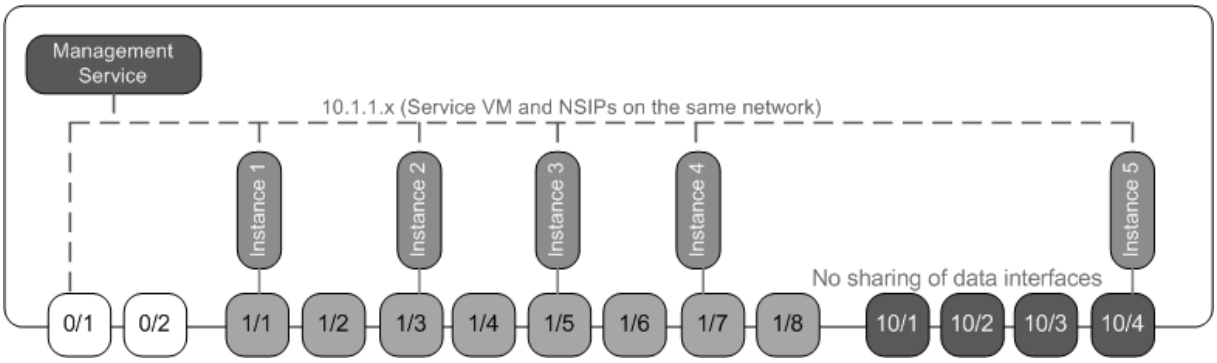
- L'administrateur de l'appliance est également l'administrateur d'instance.
- Les exigences de conformité de votre organisation ne spécifient pas que des réseaux de gestion distincts sont requis pour le service de gestion et les adresses NSIP des différentes instances.

Les instances peuvent être provisionnées sur le même réseau (pour le trafic de gestion). Les adresses VIP peuvent être configurées dans différents réseaux (pour le trafic de données), et donc dans différentes zones de sécurité.

Dans l'exemple suivant, les instances du service de gestion et de Citrix ADC font partie du réseau 10.1.1.x. Les interfaces 0/1 et 0/2 sont les interfaces de gestion, 1/1 à 1/8 sont des interfaces de données 1G et 10/1 à 10/4 sont des interfaces de données 10G. Chaque instance possède sa propre interface physique dédiée. Par conséquent, le nombre d'instances est limité au nombre d'interfaces physiques disponibles sur l'appliance. Par défaut, le filtrage VLAN est activé sur chaque interface de l'appliance SDX. Le nombre de VLAN est limité à 32 sur une interface 1G et à 63 sur une interface 10G. Le filtrage VLAN peut être activé et désactivé pour chaque interface. Désactivez le filtrage VLAN pour configurer jusqu'à 4 096 VLAN par interface sur chaque instance. Dans cet exemple, le filtrage VLAN n'est pas nécessaire car chaque instance possède sa propre interface dédiée. Pour plus d'informations sur le filtrage VLAN, consultez la section **Filtrage VLAN** dans Gérer et surveiller l'appliance SDX.

La figure suivante illustre le cas d'utilisation précédent.

Figure 1. Topologie réseau d'une appliance SDX avec service de gestion et NSIP pour les instances du même réseau



Le tableau suivant répertorie les noms et les valeurs des paramètres utilisés pour le provisionnement de l'instance 1 de Citrix ADC dans l'exemple précédent.

Nom du paramètre	Valeurs pour l'instance 1
Nom	vpx8
IP Address	10.1.1.2
Masque réseau	255.255.255.0
Gateway	10.1.1.1
Fichier XVA	NS-VPX-XEN-10.0-51.308.a_nc.xva
Licence de fonctionnalité	Platine
Profil de l'administrateur	ns_ns_root_profile
User Name	vpx8
Mot de passe	Sdx1
Confirm Password	Sdx1
Accès Shell/Sftp/Scp	Vrai
Mémoire totale (Mo)	2048
Jetons #SSL	1
Débit (Mbits/s)	1 000
Paquets par seconde	1000000
CPU	Partagé
Interface	0/1 et 1/1

Provisionner l'instance 1 de Citrix ADC comme indiqué dans cet exemple

1. Dans l'onglet Configuration, dans le volet de navigation, développez Configuration Citrix ADC, puis cliquez sur Instances.
2. Dans le volet Instances Citrix ADC, cliquez sur Ajouter.
3. Dans l'assistant Provisionner Citrix, suivez les instructions de l'assistant pour spécifier les valeurs de paramètre indiquées dans le tableau précédent.
4. Cliquez sur Créer, puis sur Fermer. L'instance Citrix ADC que vous avez provisionnée s'affiche dans le volet des instances Citrix ADC.

Consolidation lorsque le service de gestion et les instances Citrix ADC se trouvent sur des réseaux différents

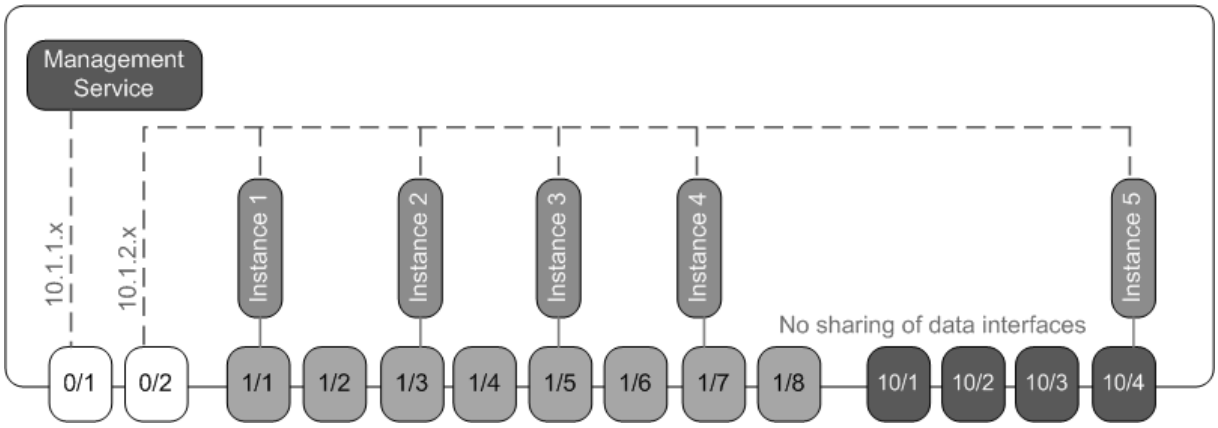
January 27, 2022

Dans certains cas, l'administrateur de l'appliance peut autoriser d'autres administrateurs à effectuer des tâches d'administration sur des instances individuelles. Cela peut être fait en toute sécurité en accordant à un administrateur d'instance individuel des droits de connexion sur cette instance uniquement. Toutefois, pour des raisons de sécurité, l'administrateur du dispositif peut ne pas vouloir autoriser l'instance à se trouver sur le même réseau que le service de gestion. Il s'agit d'un scénario courant dans les environnements de fournisseurs de services, et il est de plus en plus courant dans les entreprises qui adoptent des architectures de virtualisation et de cloud.

Dans l'exemple suivant, le service de gestion se trouve sur le réseau 10.1.1.x et les instances Citrix ADC se trouvent sur le réseau 10.1.2.x. Les interfaces 0/1 et 0/2 sont les interfaces de gestion, 1/1 à 1/8 sont des interfaces de données 1G et 10/1 à 10/4 sont des interfaces de données 10G. Chaque instance possède son propre administrateur dédié et sa propre interface physique dédiée. Par conséquent, le nombre d'instances est limité au nombre d'interfaces physiques disponibles sur l'appliance. Le filtrage VLAN n'est pas nécessaire, car chaque instance possède sa propre interface dédiée. Vous pouvez également désactiver le filtrage VLAN pour configurer jusqu'à 4 096 VLAN par instance et par interface. Dans cet exemple, vous n'avez pas besoin de configurer un NSVLAN, car les instances ne partagent pas d'interface physique et il n'existe aucun VLAN balisé. Pour plus d'informations sur les NSVLAN, consultez la section Ajout d'une instance Citrix ADC

La figure suivante illustre le cas d'utilisation précédent.

Figure 1. Topologie réseau d'une appliance SDX avec service de gestion et NSIP pour les instances de différents réseaux



En tant qu'administrateur de l'appliance, vous pouvez conserver le trafic entre le service de gestion et les adresses NSIP sur l'appliance SDX. Vous pouvez également forcer le trafic à quitter l'appareil si, par exemple, vous souhaitez que le trafic passe par un pare-feu externe ou un autre intermédiaire de sécurité, puis retourne à l'appliance.

Le tableau suivant répertorie les noms et les valeurs des paramètres utilisés pour le provisionnement de l'instance 1 de Citrix ADC dans cet exemple.

Nom du paramètre	Valeurs pour l'instance 1
Nom	vpx1
IP Address	10.1.2.2
Masque réseau	255.255.255.0
Gateway	10.1.2.1
Fichier XVA	NS-VPX-XEN-10.0-51.308.a_nc.xva
Licence de fonctionnalité	Platine
Profil de l'administrateur	ns_ns_root_profile
Nom d'utilisateur	vpx1
Mot de passe	Sdx1
Confirm Password	Sdx1
Accès Shell/Sftp/Scp	Vrai
Mémoire totale (Mo)	2048
Jetons #SSL	1
Débit (Mbits/s)	1 000
Paquets par seconde	1000000
CPU	Partagé

Nom du paramètre	Valeurs pour l'instance 1
Interface	0/2 et 1/1

Pour provisionner l'instance 1 de Citrix ADC comme indiqué dans cet exemple

1. Dans l'onglet **Configuration**, dans le volet de navigation, développez **Configuration Citrix ADC**, puis cliquez sur **Instances**.
2. Dans le volet Instances Citrix ADC, cliquez sur **Ajouter**.
3. Dans l' **assistant Provisionner Citrix ADC**, suivez les instructions de l'assistant pour définir les paramètres sur les valeurs indiquées dans le tableau précédent.
4. Cliquez sur **Créer**, puis sur **Fermer**. L'instance Citrix ADC que vous avez provisionnée s'affiche dans le volet des instances Citrix ADC.

Consolidation entre zones de sécurité

January 27, 2022

Une appliance SDX est souvent utilisée pour la consolidation entre les zones de sécurité. La zone démilitarisée ajoute une couche de sécurité supplémentaire au réseau interne d'une organisation, car un attaquant n'a accès qu'à la zone démilitarisée. Il n'a pas accès au réseau interne de l'organisation. Dans les environnements à haute conformité, une seule instance Citrix ADC avec des adresses VIP à la fois dans la zone démilitarisée et dans un réseau interne n'est pas acceptable. Avec SDX, vous pouvez mettre en service des instances hébergeant des adresses VIP dans la zone démilitarisée et d'autres instances hébergeant des adresses VIP dans un réseau interne.

Vous pouvez parfois avoir besoin de réseaux de gestion distincts pour chaque zone de sécurité. Les adresses NSIP des instances de la zone démilitarisée peuvent se trouver dans un réseau. Les adresses NSIP des instances ayant des adresses VIP dans le réseau interne peuvent se trouver dans un réseau de gestion différent. En outre, il arrive souvent que la communication entre le service de gestion et les instances doive être acheminée via un périphérique externe, tel qu'un routeur. Vous pouvez configurer des stratégies de pare-feu pour contrôler le trafic envoyé au pare-feu et pour enregistrer le trafic.

L'appliance SDX possède deux interfaces de gestion (0/1 et 0/2) et, selon le modèle, jusqu'à huit ports de données 1G et huit ports de données 10G. Vous pouvez également utiliser les ports de données comme ports de gestion (par exemple, lorsque vous devez configurer des VLAN balisés, car le balisage n'est pas autorisé sur les interfaces de gestion). Dans ce cas, le trafic provenant du service de gestion doit quitter l'appliance, puis revenir à l'appliance. Vous pouvez acheminer ce trafic ou, éventuellement, spécifier un NSVLAN sur une interface affectée à l'instance. Si une interface de gestion est com-

mune entre une instance et le service de gestion, le trafic entre les deux n'a pas besoin d'être routé. Toutefois, si votre configuration l'exige explicitement, le trafic peut être acheminé.

Remarque Le balisage est pris en charge dans Citrix Hypervisor version 6.0.

Consolidation avec des interfaces dédiées pour chaque instance

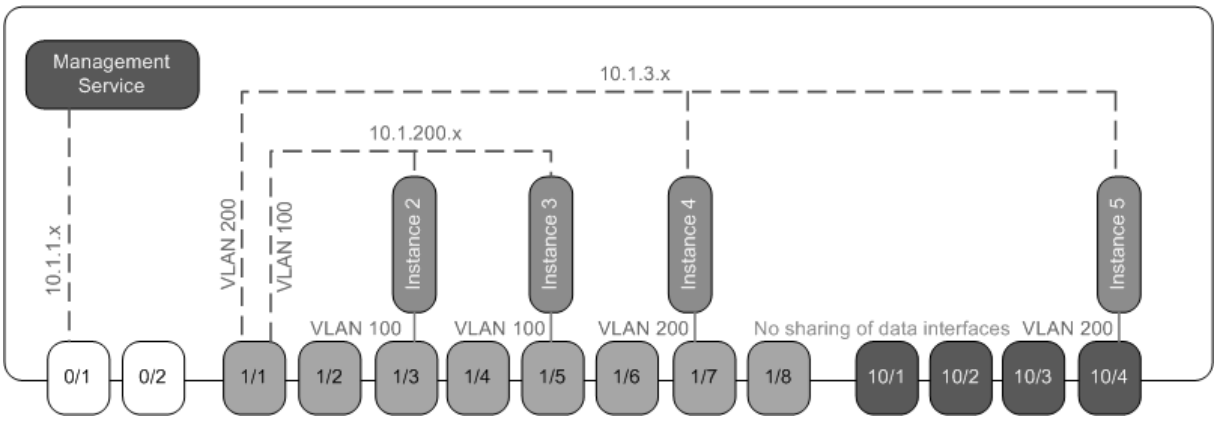
January 27, 2022

Dans l'exemple suivant, les instances font partie de plusieurs réseaux. L'interface 0/1 est affectée au service de gestion, qui fait partie du réseau interne 10.1.1.x. Les instances 2 et 3 de Citrix ADC font partie du réseau 10.1.200.x (VLAN 100). Les instances 4 et 5 de Citrix ADC font partie du réseau 10.1.3.x (VLAN 200).

Vous pouvez également configurer un NSVLAN sur toutes les instances.

La figure suivante illustre le cas d'utilisation précédent.

Figure 1. Topologie réseau d'une appliance SDX avec des instances Citrix ADC sur plusieurs réseaux



L'appliance SDX est connectée à un commutateur. Assurez-vous que les ID VLAN 100 et 200 sont configurés sur le port du commutateur auquel le port 1/1 de l'appliance est connecté.

Le tableau suivant répertorie les noms et les valeurs des paramètres utilisés pour le provisionnement des instances Citrix ADC 5 et 3 dans cet exemple.

Nom du paramètre	Valeurs pour l'exemple 5	Valeurs pour l'instance 3
Nom	vpx5	vpx3
IP Address	10.1.3.2	10.1.200.2
Masque réseau	255.255.255.0	255.255.255.240
Gateway	10.1.3.1	10.1.200.1

Nom du paramètre	Valeurs pour l'exemple 5	Valeurs pour l'instance 3
Fichier XVA	NS-VPX-XEN-10.0-51.308.a_nc.xva	NS-VPX-XEN-10.0-51.308.a_nc.xva
Licence de fonctionnalité	Platine	Platine
Profil de l'administrateur	ns_ns_root_profile	ns_ns_root_profile
Nom d'utilisateur	vpx5	vpx3
Mot de passe	Sdx1	racine
Confirm Password	Sdx1	racine
Accès Shell/Sftp/Scp	Vrai	Vrai
Mémoire totale (Mo)	2048	2048
Jetons #SSL	1	1
Débit (Mbits/s)	1 000	1 000
Paquets par seconde	1000000	1000000
CPU	Partagé	Partagé
Interface	1/1 et 10/4	1/1 et 1/5
NSVLAN	200	100
Ajouter (interface)	1/1	1/1
Interface balisée	Sélectionner le **tag**	Sélectionner le **tag**

Pour provisionner les instances Citrix ADC 5 et 3 comme indiqué dans cet exemple

1. Dans l'onglet **Configuration**, dans le volet de navigation, développez **Configuration Citrix ADC**, puis cliquez sur **Instances**.
2. Dans le volet Instances Citrix ADC, cliquez sur **Ajouter**.
3. Dans l' **assistant Provisionner Citrix ADC**, suivez les instructions de l'assistant pour définir les paramètres sur les valeurs indiquées dans le tableau précédent.
4. Cliquez sur **Créer**, puis sur **Fermer**. L'instance Citrix ADC que vous avez provisionnée s'affiche dans le volet des instances Citrix ADC.

Consolidation avec partage d'un port physique par plusieurs instances

June 13, 2022

Vous pouvez activer et désactiver le filtrage VLAN sur une interface selon vos besoins. Par exemple, pour configurer plus de 100 VLAN sur une instance, attribuez une interface physique dédiée à cette instance et désactivez le filtrage VLAN sur cette interface. Activez le filtrage VLAN sur les instances qui partagent une interface physique, afin qu'une instance ne puisse pas voir le trafic d'une autre instance.

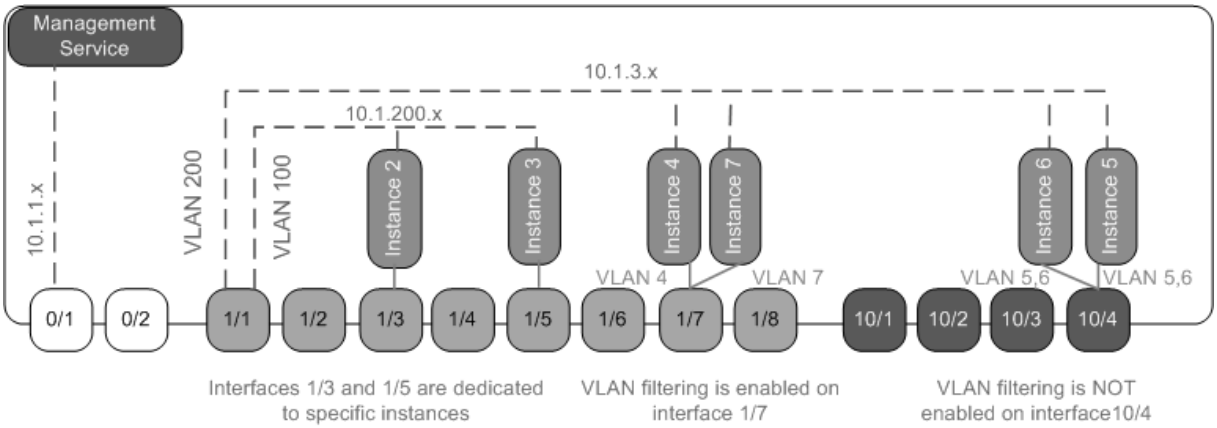
Remarque : Le filtrage VLAN n'est pas un paramètre global sur l'appliance. Vous activez ou désactivez le filtrage VLAN sur une interface, et le paramètre s'applique à toutes les instances associées à cette interface. Si le filtrage VLAN est désactivé, vous pouvez configurer jusqu'à 4 096 VLAN. Si le filtrage VLAN est activé, vous pouvez configurer jusqu'à 63 VLAN balisés sur une interface 10G et jusqu'à 32 VLAN balisés sur une interface 1G.

Dans l'exemple suivant, les instances font partie de plusieurs réseaux.

- L'interface 1/1 est affectée en tant qu'interface de gestion à toutes les instances. L'interface 0/1 est affectée au service de gestion, qui fait partie du réseau interne 10.1.1.x.
- Les instances 2 et 3 de Citrix ADC se trouvent sur le réseau 10.1.200.x, et les instances 4, 5, 6 et 7 se trouvent sur le réseau 10.1.3.x. Les instances 2 et 3 disposent chacune d'une interface physique dédiée. Les instances 4 et 7 partagent l'interface physique 1/7, et les instances 5 et 6 partagent l'interface physique 10/4.
- Le filtrage VLAN est activé sur l'interface 1/7. Le trafic pour l'instance 4 est balisé pour le VLAN 4, et le trafic pour l'instance 7 est balisé pour le VLAN 7. Par conséquent, le trafic pour l'instance 4 n'est pas visible pour l'instance 7. Inversement, le trafic pour l'instance 7 n'est pas visible pour l'instance 4. Un maximum de 32 VLAN peuvent être configurés sur l'interface 1/7.
- Le filtrage VLAN est désactivé sur l'interface 10/4, de sorte que vous pouvez configurer jusqu'à 4 096 VLAN sur cette interface. Configurez les VLAN 500 à 599 sur l'instance 5 et les VLAN 600 à 699 sur l'instance 6. L'instance 5 peut voir le trafic de diffusion et de multidiffusion provenant du VLAN 600—699, mais les paquets sont abandonnés au niveau logiciel. De même, l'instance 6 peut voir le trafic de diffusion et de multidiffusion du VLAN 500—599, mais les paquets sont abandonnés au niveau logiciel.

La figure suivante illustre le cas d'utilisation précédent.

Figure 1. Topologie réseau d'une appliance SDX avec des instances Management Service et Citrix ADC distribuées sur les réseaux



Le tableau suivant répertorie les noms et les valeurs des paramètres utilisés pour le provisionnement des instances Citrix ADC 7 et 4 dans cet exemple.

Nom du paramètre	Valeurs pour l'instance 7	Valeurs pour l'exemple 4
Nom	vpx7	vpx4
IP Address	10.1.3.7	10.1.3.4
Masque réseau	255.255.255.0	255.255.255.240
Gateway	10.1.3.1	10.1.3.1
Fichier XVA	NS-VPX-XEN-10.0-51.308.a_nc.xva	NS-VPX-XEN-10.0-51.308.a_nc.xva
Licence de fonctionnalité	Platine	Platine
Profil de l'administrateur	ns_ns_root_profile	ns_ns_root_profile
User Name	vpx4	vpx4
Mot de passe	Sdx1	Sdx1
Confirm Password	Sdx1	Sdx1
Accès Shell/Sftp/Scp	Vrai	Vrai
Mémoire totale (Mo)	2048	2048
Jetons #SSL	1	1
Débit (Mbits/s)	1 000	1 000
Paquets par seconde	1000000	1000000
CPU	Partagé	Partagé
Interface	1/1 et 1/7	1/1 et 1/7
NSVLAN	200	200

Pour provisionner les instances Citrix ADC 7 et 4 dans cet exemple

1. Dans l'onglet **Configuration**, dans le volet de navigation, développez Configuration Citrix ADC, puis cliquez sur **Instances**.
2. Dans le volet Instances Citrix ADC, cliquez sur **Ajouter**.
3. Dans l'assistant Provisionner Citrix ADC, suivez les instructions de l'assistant pour définir les paramètres sur les valeurs indiquées dans le tableau précédent.
4. Cliquez sur **Créer**, puis sur **Fermer**. L'instance Citrix ADC que vous avez provisionnée s'affiche dans le volet des instances Citrix ADC.

API NITRO

January 27, 2022

Le protocole Citrix SDX NITRO vous permet de configurer et de surveiller l'appliance SDX par programmation.

NITRO expose ses fonctionnalités via des interfaces REST (Representational State Transfer). Par conséquent, les applications NITRO peuvent être développées dans n'importe quel langage de programmation. En outre, pour les applications qui doivent être développées en Java, .NET ou Python, le protocole NITRO est exposé en tant que bibliothèques pertinentes qui sont empaquetées sous forme de kits de développement logiciel distincts.

Remarque : Vous devez avoir une connaissance de base de l'appliance SDX avant d'utiliser NITRO.

Pour utiliser le protocole NITRO, l'application cliente a besoin des éléments suivants :

- Accès à un appareil SDX.
- Pour utiliser les interfaces REST, vous devez disposer d'un système capable de générer des demandes HTTP ou HTTPS (charge utile au format JSON) à l'appliance SDX. Vous pouvez utiliser n'importe quel langage ou outil de programmation.
- Pour les clients Java, vous devez disposer d'un système sur lequel la version 1.5 ou supérieure du Java Development Kit (JDK) est disponible. Le JDK peut être téléchargé à partir de http://www.oracle.com/technetwork/java/javase/downloads/index.html.
- Pour les clients .NET, vous devez disposer d'un système sur lequel .NET Framework 3.5 ou une version supérieure est disponible. Le framework .NET peut être téléchargé à partir de http://www.microsoft.com/downloads/en/default.aspx.
- Pour les clients Python, vous devez disposer d'un système sur lequel la version Python 2.7 ou supérieure et la bibliothèque Requests (disponible dans <NITRO_SDK_HOME>/lib) sont installées.

Obtention du pack NITRO

January 27, 2022

Le package NITRO est disponible sous forme de fichier tar sur la page Téléchargements de l'utilitaire de configuration de l'appliance SDX. Vous devez télécharger et décompresser le fichier dans un dossier de votre système local. Ce dossier est appelé <NITRO_SDK_HOME> dans cette documentation.

Le dossier contient les bibliothèques NITRO du sous-dossier
lib. Les bibliothèques doivent être ajoutées au chemin de classe de l'application cliente pour accéder à la fonctionnalité NITRO. Le dossier
<NITRO_SDK_HOME> contient également des exemples et de la documentation qui peuvent vous aider à comprendre le SDK NITRO.

Remarque :

- Le package REST contient uniquement la documentation relative à l'utilisation des interfaces REST.
- Pour le SDK Python, la bibliothèque doit être installée sur le chemin du client. Pour obtenir des instructions d'installation, consultez le fichier \/README.txt.

SDK .NET

January 27, 2022

Les API SDX NITRO sont classées en fonction de leur portée et de leur objectif en API système et en API de configuration. Vous pouvez également résoudre les problèmes liés aux opérations NITRO.

API système

La première étape pour utiliser NITRO consiste à établir une session avec l'appliance SDX, puis à authentifier la session à l'aide des informations d'identification de l'administrateur.

Créez un objet de la classe nitro_service en spécifiant l'adresse IP de l'appliance et le protocole pour se connecter à l'appliance (HTTP ou HTTPS). Vous pouvez ensuite utiliser cet objet et vous connecter à l'appliance en spécifiant le nom d'utilisateur et le mot de passe de l'administrateur.

Remarque : Vous devez disposer d'un compte d'utilisateur sur cette appliance. Les opérations de configuration que vous pouvez effectuer sont limitées par le rôle administratif attribué à votre compte.

L'exemple de code suivant se connecte à un dispositif SDX dont l'adresse IP est 10.102.31.16 à l'aide du protocole HTTPS :


```
1 //Specify the IP address of the appliance and service type
2 nitro_service nitroservice = new nitro_service ("10.102.31.16", "https"
      );
3
4 //Specify the login credentials
5 nitroservice.login("nsroot", "verysecret");
6 <!--NeedCopy-->
```

Remarque : Utilisez l'objet
nitro_service dans toutes les autres opérations NITRO sur l'appliance.

Pour vous déconnecter de l'appliance, appelez la méthode logout () comme suit :

```
1 nitroservice.logout();
2 <!--NeedCopy-->
```

API de configuration

Le protocole NITRO peut être utilisé pour configurer les ressources de l'appliance SDX.

Les API permettant de configurer une ressource sont regroupées en packages ou espaces de noms au format com.citrix.sdx.nitro.resource.config.. Chacun de ces packages ou espaces de noms contient une classe nommée qui fournit les API pour configurer la ressource.

Par exemple, la ressource NetScaler possède le package ou l'espace de noms com.citrix.sdx.nitro.resource.config.ns

Une classe de ressources fournit des API pour effectuer d'autres opérations. Ces opérations peuvent être la création d'une ressource, l'extraction de ressources et de propriétés de ressource, la mise à jour d'une ressource, la suppression de ressources et l'exécution d'opérations en bloc sur les ressources.

Créer une ressource

Pour créer une ressource (par exemple, une instance Citrix ADC) sur l'appliance SDX :

1. Définissez la valeur des propriétés requises de la ressource en utilisant le nom de propriété correspondant. Le résultat est un objet de ressource qui contient les détails requis pour la ressource.
   Remarque : Ces valeurs sont définies localement sur le client. Les valeurs ne sont pas reflétées sur l'appliance tant que l'objet n'est pas chargé.
2. Téléchargez l'objet de ressource sur l'appliance, à l'aide de la méthode statique add ().

L'exemple de code suivant crée une instance Citrix ADC nommée « ns_instance » sur l'appliance SDX :

```
1 ns newns = new ns();
```



```
2
3  //Set the properties of the NetScaler locally
4  newns.name = "ns_instance";
5  newns.ip_address = "10.70.136.5";
6  newns.netmask = "255.255.255.0";
7  newns.gateway = "10.70.136.1";
8  newns.image_name = "nsvpx-9.3.45_nc.xva";
9  newns.profile_name = "ns_nsroot_profile";
10 newns.vm_memory_total = 2048;
11 newns.throughput = 1000;
12 newns.pps = 1000000;
13 newns.license = "Standard";
14 newns.username = "admin";
15 newns.password = "admin";
16
17 int number_of_interfaces = 2;
18 network_interface[] interface_array = new network_interface[
      number_of_interfaces];
19
20 //Adding 10/1
21 interface_array[0] = new network_interface();
22 interface_array[0].port_name = "10/1";
23
24 //Adding 10/2
25 interface_array[1] = new network_interface();
26 interface_array[1].port_name = "10/2";
27
28 newns.network_interfaces = interface_array;
29
30 //Upload the Citrix ADC instance
31 ns result = ns.add(nitroservice, newns);
32 <!--NeedCopy-->
```

Récupération des détails

Pour récupérer les propriétés d'une ressource sur l'appliance SDX, procédez comme suit :

1. Récupérez les configurations de l'appliance à l'aide de la méthode get (). Le résultat est un objet de ressource.
2. Extrayez la propriété requise de l'objet en utilisant le nom de propriété correspondant.

L'exemple de code suivant récupère les détails de toutes les ressources NetScaler :

```
1 //Retrieve the resource object from the SDX appliance
2 ns[] returned_ns = ns.get(nitroservice);
```



```
3
4 //Extract the properties of the resource from the object
5 Console.WriteLine(returned_ns[i].ip_address);
6 Console.WriteLine(returned_ns[i].netmask);
7 <!--NeedCopy-->
```

Récupération des statistiques

Une appliance SDX collecte des statistiques sur l'utilisation de ses fonctionnalités. Vous pouvez récupérer ces statistiques à l'aide de NITRO.

L'exemple de code suivant récupère les statistiques d'une instance Citrix ADC portant l'ID 123456a :

```
1 ns obj = new ns();
2 obj.id = "123456a";
3 ns stats = ns.get(nitroservice, obj);
4 Console.WriteLine("CPU Usage:" + stats.ns_cpu_usage);
5 Console.WriteLine("Memory Usage:" + stats.ns_memory_usage);
6 Console.WriteLine("Request rate/sec:" +stats.http_req);
7 <!--NeedCopy-->
```

Mettre à jour une ressource

Pour mettre à jour les propriétés d'une ressource existante sur l'appliance, procédez comme suit :

1. Définissez la propriété id sur l'ID de la ressource à mettre à jour.
2. Définissez la valeur des propriétés requises de la ressource en utilisant le nom de propriété correspondant. Le résultat est un objet de ressource.
   Remarque : Ces valeurs sont définies localement sur le client. Les valeurs ne sont pas reflétées sur l'appliance tant que l'objet n'est pas chargé.
3. Téléchargez l'objet de ressource sur l'appliance, à l'aide de la méthode update ().

L'exemple de code suivant met à jour le nom de l'instance Citrix ADC portant l'ID 123456a en « ns_instance_new » :

```
1 ns update_obj = new ns();
2
3 //Set the ID of the NetScaler to be updated
4 update_obj.id = "123456a";
5
6 //Get existing NetScaler details
7 update_obj = ns.get(nitroservice, update_obj);
8
9 //Update the name of the NetScaler to "ns_instance_new" locally
```



```
update_obj.name = "ns_instance_new";

//Upload the updated NetScaler details
ns result = ns.update(nitroservice, update_obj);
<!--NeedCopy-->
```

Supprimer une ressource

Pour supprimer une ressource existante, appelez la méthode statique delete () sur la classe de ressources, en passant l'ID de la ressource à supprimer, en tant qu'argument.

L'exemple de code suivant supprime une instance Citrix ADC portant l'ID 1 :

```
ns obj = new ns();
obj.id = "123456a";
ns.delete(nitroservice, obj);
<!--NeedCopy-->
```

Opérations en vrac

Vous pouvez interroger ou modifier plusieurs ressources simultanément et ainsi réduire le trafic réseau. Par exemple, vous pouvez ajouter plusieurs appliances Citrix ADC SDX au cours de la même opération.

Chaque classe de ressources possède des méthodes qui prennent un tableau de ressources pour ajouter, mettre à jour et supprimer des ressources. Pour effectuer une opération en bloc, spécifiez les détails de chaque opération localement, puis envoyez les détails en une seule fois au serveur.

Pour tenir compte de l'échec de certaines opérations au sein de l'opération en bloc, NITRO vous permet de configurer l'un des comportements suivants :

- **sortie.** Lorsque la première erreur est rencontrée, l'exécution s'arrête. Les commandes qui ont été exécutées avant l'erreur sont validées.
- **Continuer.** Toutes les commandes de la liste sont exécutées même si certaines commandes échouent.

Remarque : Configurez le comportement requis lors de l'établissement d'une connexion avec l'appliance, en définissant
`onerror` le paramètre dans la méthode
nitro_service ().

L'exemple de code suivant ajoute deux dispositifs ADC en une seule opération :

```
ns[] newns = new ns[2];
```



```
2
3  //Specify details of first NetScaler
4  newns[0] = new ns();
5  newns[0].name = "ns_instance1";
6  newns[0].ip_address = "10.70.136.5";
7  newns[0].netmask = "255.255.255.0";
8  newns[0].gateway = "10.70.136.1";
9  ...
10 ...
11
12 //Specify details of second NetScaler
13 newns[1] = new ns();
14 newns[1].name = "ns_instance2";
15 newns[1].ip_address = "10.70.136.8";
16 newns[1].netmask = "255.255.255.0";
17 newns[1].gateway = "10.70.136.1";
18 ...
19 ...
20
21 //upload the details of the ADC appliances to the NITRO server
22 ns[] result = ns.add(nitroservice, newns);
23 <!--NeedCopy-->
```

Gestion des exceptions

Le champ Code d'erreur indique l'état de l'opération.

- Un code d'erreur de 0 indique que l'opération a réussi.
- Un code d'erreur différent de zéro indique une erreur dans le traitement de la demande NITRO.

Le champ du message d'erreur fournit une brève explication et la nature de l'échec.

La classe com.citrix.sdx.nitro.exception.nitro_exception intercepte toutes les exceptions dans l'exécution des API NITRO. Pour obtenir des informations sur l'exception, vous pouvez utiliser la `getErrorCode()` méthode.

Pour une description plus détaillée des codes d'erreur, consultez la référence de l'API disponible dans le `<NITRO_SDK_HOME>/doc` dossier.

Services Web REST

January 27, 2022

REST (Representational State Transfer) est un style architectural basé sur de simples requêtes et réponses HTTP entre le client et le serveur. REST est utilisé pour interroger ou modifier l'état des objets côté serveur. Dans REST, le côté serveur est modélisé comme un ensemble d'entités où chaque entité est identifiée par une URL unique.

Chaque ressource possède également un état dans lequel les opérations suivantes peuvent être effectuées :

- **Créer.** Les clients peuvent créer de nouvelles ressources côté serveur sur une ressource « conteneur ». Les ressources de conteneur peuvent être considérées comme des dossiers et les ressources enfants comme des fichiers ou des sous-dossiers. Le client appelant fournit l'état de la ressource à créer. L'état peut être spécifié dans la demande en utilisant le format XML ou JSON. Le client peut également spécifier l'URL unique qui identifie le nouvel objet. Le serveur peut également choisir et renvoyer une URL unique identifiant l'objet créé. La méthode HTTP utilisée pour les demandes de création est POST.
- **Lisez.** Les clients peuvent récupérer l'état d'une ressource en spécifiant son URL à l'aide de la méthode HTTP GET. Le message de réponse contient l'état de la ressource, exprimé au format JSON.
- **Mise à jour.** Vous pouvez mettre à jour l'état d'une ressource existante en spécifiant l'URL qui identifie cet objet et son nouvel état au format JSON ou XML, à l'aide de la méthode HTTP PUT.
- **Supprimer.** Vous pouvez détruire une ressource qui existe côté serveur à l'aide de la méthode HTTP DELETE et de l'URL identifiant la ressource à supprimer.

Outre ces quatre opérations CRUD (créer, lire, mettre à jour et supprimer), les ressources peuvent prendre en charge d'autres opérations ou actions. Ces opérations utilisent la méthode HTTP POST, le corps de la requête en JSON spécifiant l'opération à effectuer et les paramètres de cette opération.

Les API SDX NITRO sont classées en fonction de leur portée et de leur objectif en API système et en API de configuration.

API système

La première étape pour utiliser NITRO consiste à établir une session avec l'appliance SDX, puis à authentifier la session à l'aide des informations d'identification de l'administrateur.

Spécifiez le nom d'utilisateur et le mot de passe dans l'objet de connexion. L'ID de session créé doit être spécifié dans l'en-tête de demande de toutes les autres opérations de la session.

Remarque : Vous devez disposer d'un compte d'utilisateur sur cette appliance. Les configurations que vous pouvez effectuer sont limitées par le rôle administratif attribué à votre compte.

Pour vous connecter à un dispositif SDX dont l'adresse IP est 10.102.31.16 à l'aide du protocole HTTPS :

- **URL** `https://10.102.31.16/nitro/v2/config/login/`
- **Méthode HTTP** POST

- **Demander**
  - **En-tête**

```
Content-Type:application/vnd.com.citrix.sdx.login+json
<!--NeedCopy-->
```

Remarque : Les types de contenu tels que « application/x-www-form-urlencoded » qui étaient pris en charge dans les versions antérieures de NITRO peuvent également être utilisés. Assurez-vous que la charge utile est la même que celle utilisée dans les versions précédentes. Les charges utiles fournies dans cette documentation ne s'appliquent que si le type de contenu est de la forme « application/vnd.com.citrix.sdx.login+json ».

  - **Charge utile**

```
{

    "login":
    {

        "username":"nsroot",
        "password":"verysecret"
     }

 }

<!--NeedCopy-->
```

- **Charge utile de réponse**
  - **En-tête**

```
HTTP/1.0 201 Created
Set-Cookie:
NITRO_AUTH_TOKEN=##87305E9C51B06C848F0942; path=/nitro/v2
<!--NeedCopy-->
```

Remarque : Utilisez l'ID de session dans toutes les autres opérations NITRO sur l'appliance.

Remarque : Par défaut, la connexion à l'appliance expire après 30 minutes d'inactivité. Vous pouvez modifier le délai d'expiration en spécifiant un nouveau délai d'expiration (en secondes) dans l'objet de
connexion. Par exemple, pour modifier le délai d'expiration à 60 minutes, la charge utile de la demande est la suivante :

```
{

    "login":
```



```
4      {
5
6          "username":"nsroot",
7          "password":"verysecret",
8          "timeout":3600
9       }
10
11   }
12
13  <!--NeedCopy-->
```

Vous pouvez également vous connecter à l'appliance pour effectuer une seule opération, en spécifiant le nom d'utilisateur et le mot de passe dans l'en-tête de demande de l'opération. Par exemple, pour vous connecter à un dispositif lors de la création d'une instance Citrix ADC :

- **URL**
- **Méthode HTTP**
- **Demander**
  - **En-tête**

    ```
    1  X-NITRO-USER:nsroot
    2  X-NITRO-PASS:verysecret
    3  Content-Type:application/vnd.com.citrix.sdx.ns+json
    4  <!--NeedCopy-->
    ```

  - **Charge utile**

    ```
    1  {
    2
    3      "ns":
    4      {
    5
    6          ...
    7       }
    8
    9    }
    10
    11  <!--NeedCopy-->
    ```

- **Réponse.**
  - **En-tête**

    ```
    1  HTTP/1.0 201 Created
    2  <!--NeedCopy-->
    ```

Pour vous déconnecter de l'appliance, utilisez la méthode DELETE :

- **URL**
- **Méthode HTTP** DELETE
- **Demander**
  - **En-tête**

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
Content-Type:application/vnd.com.citrix.sdx.login+json
<!--NeedCopy-->
```

API de configuration

Le protocole NITRO peut être utilisé pour configurer les ressources de l'appliance SDX.

Chaque ressource SDX est associée à une URL unique, selon le type d'opération à effectuer. Les URL pour les opérations de configuration ont le format suivant : `http://<IP>/nitro/v2/config/<resource_type>`

Créer une ressource

Pour créer une ressource (par exemple, une instance Citrix ADC) sur l'appliance SDX, spécifiez le nom de la ressource et d'autres arguments associés dans l'objet de ressource spécifique. Par exemple, pour créer une instance Citrix ADC nommée vpx1 :

- **URL**
- **Méthode HTTP**
- **Demander**
  - **En-tête**

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
Content-Type:application/vnd.com.citrix.sdx.ns+json
<!--NeedCopy-->
```

  - **Charge utile**

```
{

    "ns":
    {

        "name":"vpx1",
        "ip_address":"192.168.100.2",
        "netmask":"255.255.255.0",
        "gateway":"192.168.100.1",
        "image_name":"nsvpx-9.3-45_nc.xva",
```



```
11          "vm_memory_total":2048,
12          "throughput":1000,
13          "pps":1000000,
14          "license":"Standard",
15          "profile_name":"ns_nsroot_profile",
16          "username":"admin",
17          "password":"admin",
18          "network_interfaces":
19          [
20              {
21
22                  "port_name":"10/1"
23               }
24  ,
25              {
26
27                  "port_name":"10/2"
28               }
29
30          ]
31      }
32
33   }
34
35  <!--NeedCopy-->
```

Récupération des détails et des statistiques

Les détails des ressources SDX peuvent être récupérés comme suit :

- Pour récupérer les détails d'une ressource spécifique sur l'appliance SDX, spécifiez l'ID de la ressource dans l'URL.
- Pour récupérer les propriétés des ressources en fonction de certains filtres, spécifiez les conditions du filtre dans l'URL.

  L'URL se présente sous la forme suivante : `http://<IP>/nitro/v2/config/<resource_type>?filter=<property1>:<value>,<property2>:<value>`
- Si votre demande est susceptible d'entraîner le renvoi de nombreuses ressources par l'appliance, vous pouvez récupérer ces résultats par segments en les divisant en « pages » et en les récupérant page par page.

  Par exemple, supposons que vous souhaitez récupérer toutes les instances Citrix ADC sur un SDX qui en possède 53. Au lieu de récupérer les 53 dans une réponse volumineuse, configurez

les résultats pour qu'ils soient divisés en pages de 10 instances Citrix ADC chacune (6 pages au total). Ensuite, récupérez-les page par page sur le serveur.

Vous spécifiez le nombre de pages avec le paramètre de chaîne de requête taille de page et utilisez le paramètre de chaîne de requête de numéro de page pour spécifier le numéro de page que vous souhaitez récupérer.
L'URL se présente sous la forme suivante : `http://<IP>/nitro/v2/config/<resource_type>?pageno=<value>&pagesize=<value>`

Il n'est pas nécessaire de récupérer toutes les pages, ni de récupérer les pages dans l'ordre. Chaque demande est indépendante et vous pouvez même modifier le paramètre de taille de page entre les demandes.

Remarque : Pour avoir une idée du nombre de ressources susceptibles d'être renvoyées par une demande, vous pouvez utiliser le paramètre de chaîne de requête count pour demander le nombre de ressources à renvoyer, plutôt que les ressources elles-mêmes. Pour obtenir le nombre d'instances Citrix ADC disponibles, l'URL serait
`http://<IP>/nitro/v2/config/<resource_type>?count=yes`

Pour récupérer les informations de configuration de l'instance Citrix ADC portant l'ID 123456a :

- **URL**
- **Méthode HTTP** GET

Mettre à jour une ressource

Pour mettre à jour une ressource SDX existante, utilisez la méthode HTTP PUT. Dans la charge utile de la requête HTTP, spécifiez le nom et les autres arguments qui doivent être modifiés. Par exemple, pour modifier le nom de l'instance Citrix ADC portant l'ID 123456a en vpx2 :

- **URL**
- **Méthode HTTP**
- **Charge utile de la demande**
  - **En-tête**

```
1 Cookie:NITRO_AUTH_TOKEN=tokenvalue
2 Content-Type:application/vnd.com.citrix.sdx.ns+json
3 <!--NeedCopy-->
```

  - **Charge utile**

```
1 {
2
3     "ns":
4     {
5
```



```
6           "name":"vpx2",
7           "id":"123456a"
8       }
9
10   }
11
12  <!--NeedCopy-->
```

Supprimer une ressource

Pour supprimer une ressource existante, spécifiez le nom de la ressource à supprimer dans l'URL. Par exemple, pour supprimer une instance Citrix ADC portant l'ID 123456a :

- **URL**
- **Méthode HTTP**
- **Demander**
  - **En-tête**

```
1  Cookie:NITRO_AUTH_TOKEN=tokenvalue
2  Content-Type:application/vnd.com.citrix.sdx.ns+json
3  <!--NeedCopy-->
```

Opérations en vrac

Vous pouvez interroger ou modifier plusieurs ressources simultanément et ainsi réduire le trafic réseau. Par exemple, vous pouvez ajouter plusieurs appliances Citrix ADC SDX au cours de la même opération. Vous pouvez également ajouter des ressources de différents types en une seule demande.

Pour tenir compte de l'échec de certaines opérations au sein de l'opération en bloc, NITRO vous permet de configurer l'un des comportements suivants :

- **sortie.** Lorsque la première erreur est rencontrée, l'exécution s'arrête. Les commandes qui ont été exécutées avant l'erreur sont validées.
- **Continuer.** Toutes les commandes de la liste sont exécutées même si certaines commandes échouent.

Remarque : Configurez le comportement requis dans l'en-tête de la demande à l'aide du `X-NITRO-ONERROR` paramètre.

Pour ajouter 2 ressources Citrix ADC en une seule opération et continuer en cas d'échec d'une commande :

- **URL.**
- **Méthode HTTP.**

- **Charge utile de la demande.**
  - **En-tête**

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
Content-Type:application/vnd.com.citrix.sdx.ns+json
X-NITRO-ONERROR:continue
<!--NeedCopy-->
```

  - **Charge utile**

```
{

    "ns":
    [
        {

            "name":"ns_instance1",
            "ip_address":"10.70.136.5",
            "netmask":"255.255.255.0",
            "gateway":"10.70.136.1"
         }
,
        {

            "name":"ns_instance2",
            "ip_address":"10.70.136.8",
            "netmask":"255.255.255.0",
            "gateway":"10.70.136.1"
         }

    ]
 }

<!--NeedCopy-->
```

Pour ajouter plusieurs ressources (Citrix ADC et deux utilisateurs MPS) en une seule opération et continuer en cas d'échec d'une commande :

- **URL.**
- **Méthode HTTP.** POST
- **Charge utile de la demande.**
  - **En-tête**

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
Content-Type:application/vnd.com.citrix.sdx.ns+json
X-NITRO-ONERROR:continue
```



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

- **Charge utile**

```
{

    "ns":
    [
        {

            "name":"ns_instance1",
            "ip_address":"10.70.136.5",
            "netmask":"255.255.255.0",
            "gateway":"10.70.136.1"
         }
,
        {

            "name":"ns_instance2",
            "ip_address":"10.70.136.8",
            "netmask":"255.255.255.0",
            "gateway":"10.70.136.1"
         }

    ],
     "mpsuser":
    [
        {

            "name":"admin",
            "password":"admin",
            "permission":"superuser"
         }
,
        {

            "name":"admin",
            "password":"admin",
            "permission":"superuser"
         }

    ]
 }

<!--NeedCopy-->
```


Gestion des exceptions

Le champ Code d'erreur indique l'état de l'opération.

- Un code d'erreur de 0 indique que l'opération a réussi.
- Un code d'erreur différent de zéro indique une erreur dans le traitement de la demande NITRO.

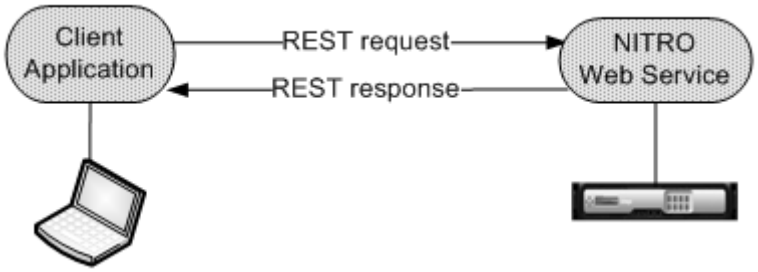
Le champ du message d'erreur fournit une brève explication et la nature de l'échec.

Comment fonctionne NITRO

January 27, 2022

L'infrastructure NITRO se compose d'une application cliente et du service Web NITRO s'exécutant sur une appliance Citrix ADC SDX. La communication entre l'application cliente et le service Web NITRO est basée sur une architecture REST utilisant HTTP ou HTTPS.

Figure 1. Workflow NITRO



Étapes détaillant le flux de travail :

1. L'application cliente envoie un message de demande REST au service Web NITRO. Lors de l'utilisation des kits SDK, un appel d'API est traduit en message de demande REST approprié.
2. Le service Web traite le message de demande REST.
3. Le service Web NITRO renvoie le message de réponse REST correspondant à l'application cliente. Lors de l'utilisation des kits SDK, le message de réponse REST est traduit en réponse appropriée pour l'appel d'API.

Pour réduire le trafic sur le réseau, récupérez l'état complet d'une ressource à partir du serveur. Apportez des modifications locales à l'état de la ressource. Téléchargez-le ensuite sur le serveur en une seule transaction réseau.

Remarque : Les opérations locales sur une ressource (modification de ses propriétés) n'affectent pas son état sur le serveur tant que l'état de l'objet n'est pas explicitement chargé.

Les API NITRO sont synchrones par nature. En d'autres termes, l'application cliente attend une réponse du service Web NITRO avant d'exécuter une autre API NITRO.

SDK Java

January 27, 2022

Les API SDX NITRO sont classées en fonction de leur portée et de leur objectif en API système et en API de configuration. Vous pouvez également résoudre les problèmes liés aux opérations NITRO.

API système

La première étape pour utiliser NITRO consiste à établir une session avec l'appliance SDX, puis à authentifier la session à l'aide des informations d'identification de l'administrateur.

Créez un objet de la classe nitro_service en spécifiant l'adresse IP de l'appliance et le protocole pour se connecter à l'appliance (HTTP ou HTTPS). Vous pouvez ensuite utiliser cet objet et vous connecter à l'appliance en spécifiant le nom d'utilisateur et le mot de passe de l'administrateur.

Remarque : Vous devez disposer d'un compte d'utilisateur sur cette appliance. Les opérations de configuration que vous pouvez effectuer sont limitées par le rôle administratif attribué à votre compte.

L'exemple de code suivant se connecte à un dispositif SDX dont l'adresse IP est 10.102.31.16 à l'aide du protocole HTTPS :

```
1 //Specify the IP address of the appliance and service type
2 nitro_service nitroservice = new nitro_service ("10.102.31.16", "https"
      );
3
4 //Specify the login credentials
5 nitroservice.login("nsroot", "verysecret");
6 <!--NeedCopy-->
```

Remarque : Utilisez l'objet
nitro_service dans toutes les autres opérations NITRO sur l'appliance.

Pour vous déconnecter de l'appliance, appelez la `logout()` méthode comme suit :

```
1 nitroservice.logout();
2 <!--NeedCopy-->
```

API de configuration

Le protocole NITRO peut être utilisé pour configurer les ressources de l'appliance SDX.

Les API permettant de configurer une ressource sont regroupées en packages ou espaces de noms au format com.citrix.sdx.nitro.resource.config.. Chacun de ces packages ou espaces de noms contient une classe nommée qui fournit les API pour configurer la ressource.

Par exemple, la ressource NetScaler possède le package ou l'espace de noms com.citrix.sdx.nitro.resource.config.ns

Une classe de ressources fournit des API pour effectuer de nombreuses autres opérations. Ces opérations peuvent être la création d'une ressource, la récupération de détails et de statistiques sur les ressources, la mise à jour d'une ressource, la suppression de ressources et l'exécution d'opérations en bloc sur les ressources.

Création d'une ressource

Pour créer une ressource (par exemple, une instance Citrix ADC) sur l'appliance SDX, procédez comme suit :

1. Définissez la valeur des propriétés requises de la ressource en utilisant le nom de propriété correspondant. Le résultat est un objet de ressource qui contient les détails requis pour la ressource.
   Remarque : Ces valeurs sont définies localement sur le client. Les valeurs ne sont pas reflétées sur l'appliance tant que l'objet n'est pas chargé.
2. Téléchargez l'objet de ressource sur l'appliance, à l'aide de la méthode statique add ().

L'exemple de code suivant crée une instance Citrix ADC nommée « ns_instance » sur l'appliance SDX :

```
ns newns = new ns();

//Set the properties of the NetScaler locally
newns.set_name("ns_instance");
newns.set_ip_address("10.70.136.5");
newns.set_netmask("255.255.255.0");
newns.set_gateway("10.70.136.1");
newns.set_image_name("nsvpx-9.3.45_nc.xva");
newns.set_profile_name("ns_nsroot_profile");
newns.set_vm_memory_total(new Double(2048));
newns.set_throughput(new Double(1000));
newns.set_pps(new Double(1000000));
newns.set_license("Standard");
newns.set_username("admin");
newns.set_password("admin");

int number_of_interfaces = 2;
network_interface[] interface_array = new network_interface[
    number_of_interfaces];

//Adding 10/1
interface_array[0] = new network_interface();
interface_array[0].set_port_name("10/1");

```



```
//Adding 10/2
interface_array[1] = new network_interface();
interface_array[1].set_port_name("10/2");

newns.set_network_interfaces(interface_array);

//Upload the Citrix ADC instance
ns result = ns.add(nitroservice, newns);
<!--NeedCopy-->
```

Extraction des détails sur les ressources

Pour récupérer les propriétés d'une ressource sur l'appliance SDX, procédez comme suit :

1. Récupérez les configurations de l'appliance à l'aide de la méthode get (). Le résultat est un objet de ressource.
2. Extrayez la propriété requise de l'objet en utilisant le nom de propriété correspondant.

L'exemple de code suivant récupère les détails de toutes les ressources NetScaler :

```
//Retrieve the resource object from the SDX appliance
ns[] returned_ns = ns.get(nitroservice);

//Extract the properties of the resource from the object
System.out.println(returned_ns[i].get_ip_address());
System.out.println(returned_ns[i].get_netmask());
<!--NeedCopy-->
```

Extraction des statistiques sur les ressources

Une appliance SDX collecte des statistiques sur l'utilisation de ses fonctionnalités. Vous pouvez récupérer ces statistiques à l'aide de NITRO.

L'exemple de code suivant récupère les statistiques d'une instance Citrix ADC portant l'ID 123456a :

```
ns obj = new ns();
obj.set_id("123456a");
ns stats = ns.get(nitroservice, obj);
System.out.println("CPU Usage:" + stats.get_ns_cpu_usage());
System.out.println("Memory Usage:" + stats.get_ns_memory_usage());
System.out.println("Request rate/sec:" +stats.get_http_req());
<!--NeedCopy-->
```


Mettre à jour une ressource

Pour mettre à jour les propriétés d'une ressource existante sur l'appliance, procédez comme suit :

1. Définissez la propriété id sur l'ID de la ressource à mettre à jour.
2. Définissez la valeur des propriétés requises de la ressource en utilisant le nom de propriété correspondant. Le résultat est un objet de ressource.
   Remarque : Ces valeurs sont définies localement sur le client. Les valeurs ne sont pas reflétées sur l'appliance tant que l'objet n'est pas chargé.
3. Téléchargez l'objet de ressource sur l'appliance, à l'aide de la méthode update ().

L'exemple de code suivant met à jour le nom de l'instance Citrix ADC portant l'ID 123456a en « ns_instance_new » :

```
ns update_obj = new ns();

//Set the ID of the NetScaler to be updated
update_obj.set_id("123456a");

//Get existing NetScaler details
update_obj = ns.get(nitroservice, update_obj);

//Update the name of the NetScaler to "ns_instance_new" locally
update_obj.set_name("ns_instance_new");

//Upload the updated NetScaler details
ns result = ns.update(nitroservice, update_obj);
<!--NeedCopy-->
```

Supprimer une ressource

Pour supprimer une ressource existante, appelez la méthode statique delete () sur la classe de ressources, en passant l'ID de la ressource à supprimer, en tant qu'argument.

L'exemple de code suivant supprime une instance Citrix ADC portant l'ID 1 :

```
ns obj = new ns();
obj.set_id("123456a");
ns.delete(nitroservice, obj);
<!--NeedCopy-->
```


Opérations en vrac

Vous pouvez interroger ou modifier plusieurs ressources simultanément et ainsi réduire le trafic réseau. Par exemple, vous pouvez ajouter plusieurs appliances Citrix ADC SDX au cours de la même opération.

Chaque classe de ressources possède des méthodes qui prennent un tableau de ressources pour ajouter, mettre à jour et supprimer des ressources. Pour effectuer une opération en bloc, spécifiez les détails de chaque opération localement, puis envoyez les détails en une seule fois au serveur.

Pour tenir compte de l'échec de certaines opérations au sein de l'opération en bloc, NITRO vous permet de configurer l'un des comportements suivants :

- **sortie.** Lorsque la première erreur est rencontrée, l'exécution s'arrête. Les commandes qui ont été exécutées avant l'erreur sont validées.
- **Continuer.** Toutes les commandes de la liste sont exécutées même si certaines commandes échouent.

Remarque : Configurez le comportement requis lors de l'établissement d'une connexion avec l'appliance, en définissant
`onerror` le paramètre dans la méthode
nitro_service ().

L'exemple de code suivant ajoute deux dispositifs ADC en une seule opération :

```
ns[] newns = new ns[2];

//Specify details of first NetScaler
newns[0] = new ns();
newns[0].set_name("ns_instance1");
newns[0].set_ip_address("10.70.136.5");
newns[0].set_netmask("255.255.255.0");
newns[0].set_gateway("10.70.136.1");
...
...
...

//Specify details of second NetScaler
newns[1] = new ns();
newns[1].set_name("ns_instance2");
newns[1].set_ip_address("10.70.136.8");
newns[1].set_netmask("255.255.255.0");
newns[1].set_gateway("10.70.136.1");
...
...

```



```
//upload the details of the NetScalers to the NITRO server
ns[] result = ns.add(nitroservice, newns);
<!--NeedCopy-->
```

Gestion des exceptions

Le champ Code d'erreur indique l'état de l'opération.

- Un code d'erreur de 0 indique que l'opération a réussi.
- Un code d'erreur différent de zéro indique une erreur dans le traitement de la demande NITRO.

Le champ du message d'erreur fournit une brève explication et la nature de l'échec.

La classe com.citrix.sdx.nitro.exception.nitro_exception intercepte toutes les exceptions dans l'exécution des API NITRO. Pour obtenir des informations sur l'exception, vous pouvez utiliser la `getErrorCode()` méthode.

Pour une description plus détaillée des codes d'erreur, consultez la référence de l'API disponible dans le <NITRO_SDK_HOME>/doc dossier.

