NetScaler Application Delivery Management 13.0

Machine translated content

Disclaimer

Contents

Notes de publication

February 1, 2024

Les notes de publication de Citrix Application Delivery Management (ADM) 13.0 décrivent les nouvelles fonctionnalités, les améliorations apportées aux fonctionnalités existantes et les problèmes connus d'une version. Le document de notes de publication de la version 13.0 comprend les sections suivantes :

- **Nouveautés** : Les nouvelles fonctionnalités et améliorations apportées aux fonctionnalités existantes publiées dans une version.
- **Problèmes connus** : Les problèmes qui existent dans une version et leurs solutions de contournement, le cas échéant.
- **Problèmes résolus** : problèmes résolus dans une version.

Pour consulter le document complet des notes de publication, cliquez sur le lien suivant :

Notes de publication	Date de publication	Version
Notes de mise à jour pour la version 92.18 de la version 13.0 de Citrix ADM	Publié le : 6 septembre 2023	Version de la note de publication : 1.0
Notes de mise à jour pour la version 91.12 de Citrix ADM 13.0	Date de publication : 18 mai 2023	Version de la note de publication : 1.0
Notes de publication pour la version 90.7 de la version 13.0 de Citrix ADM	Date de publication : 1 février 2023	Version de la note de publication : 1.0
Notes de publication pour la version 89.7 de la version 13.0 de Citrix ADM	Publié le 19 décembre 2022	Version de la note de publication : 1.0
Notes de mise à jour pour la build 88.12 de la version 13.0 de Citrix ADM	Publié le 20 octobre 2022	Version de la note de publication : 1.0
Notes de mise à jour pour la version 87.9 de Citrix ADM 13.0	Publié le 6 février 2023	Version de note de version : 2.0
Notes de mise à jour pour la version 86.17 de Citrix ADM 13.0	Publié le : 20 juin 2022	Version de la note de publication : 1.0

Notes de publication	Date de publication	Version
Notes de publication pour la build 85.19 de la version 13.0 de Citrix ADM	Publié le : 14 juin 2022	Version de la note de publication : 1.0
Notes de publication pour la version 84.10 de Citrix ADM 13.0	Publié le : 14 décembre 2021	Version de la note de publication : 1.0
Notes de publication pour la version 83.27 de Citrix ADM 13.0	Publié le : 28 septembre 2021	Version de la note de publication : 1.0
Notes de publication pour la version 82.41 de Citrix ADM 13.0	Publié le : 9 juin 2021	Version de la note de publication : 1.0
Notes de publication pour la version 79.64 de Citrix ADM 13.0	Publication : 06 avril 2021	Version de la note de publication : 1.0
Notes de publication pour la version 76.29 de Citrix ADM 13.0	Publication : 19 février 2021	Version de la note de publication : 1.0
Notes de publication pour la version 71.40 de Citrix ADM 13.0	Publication : 20 janvier 2021	Version de note de version : 2.0
Notes de publication pour la version 67.42 de Citrix ADM 13.0	Publication : 28 octobre 2020	Version de la note de version : 1.0. **Remarque** : Build 67.42 remplace la version 67.39
Notes de publication pour la version 67.39 de Citrix ADM 13.0	Publication : 16 octobre 2020	Version de note de version : 2.0
Notes de publication pour la version 64.35 de Citrix ADM 13.0	Publication : 16 octobre 2020	Version de note de version : 2.0
Notes de publication pour la version 61.48 de Citrix ADM 13.0	Publication : 18 septembre 2020	Version de note de version : 2.0
Notes de publication pour la version 58.30 de Citrix ADM 13.0	Publié le : 10 juin 2020	Version de la note de mise à jour : 1.0
Notes de publication pour la version 52.24 de Citrix ADM 13.0	Publié le : 26 mars 2020	Version de la note de mise à jour : 1.0
Notes de publication pour la version 47.22 de Citrix ADM 13.0	Publié le : 10 décembre 2019	Version de la note de mise à jour : 1.0
Notes de publication pour la version 41.28 de Citrix ADM 13.0	Publié le : 27 septembre 2019 (la version 41.28 remplace la version 41.22)	Version de la note de mise à jour : 1.0

> **Remarque**
>
> Ces notes de publication ne documentent pas les correctifs liés à la sécurité. Pour obtenir la liste des correctifs et des conseils liés à la sécurité, consultez le bulletin de sécurité Citrix.

Migrer Citrix ADM sur site vers Citrix Cloud

February 1, 2024

Vous pouvez migrer localement **Citrix ADM 13.0 64.35 ou une version ultérieure** vers Citrix Cloud. Si votre ADM possède la version 12.1 ou une version antérieure, vous devez d'abord effectuer une mise à niveau vers la version **13.0 64.35 ou une version ultérieure**, puis migrer vers Citrix Cloud. Pour plus d'informations, consultez la section Mise à niveau .

Le service ADM via Citrix Cloud vous permet d'obtenir :

- Des versions plus rapides, environ toutes les deux semaines avec les dernières mises à jour des fonctionnalités.
- Analyse basée sur l'apprentissage automatique pour la sécurité des applications, les robots, les performances et l'utilisation.
- Diverses autres fonctionnalités actuellement prises en charge uniquement dans le service ADM, telles que l'analyse des périodes de pointe et creuses durée, l'analyse basée sur l'apprentissage automatique pour la sécurité des applications et des robots, l'analyse du processeur des applications, et bien d'autres encore.

Pour une migration réussie, vous devez :

- Assurez-vous d'avoir une connexion Internet dans ADM local pour l'accessibilité Citrix Cloud
- Configurer l'agent de service ADM
- Obtenir le client et le fichier CSV secret à partir de Citrix Cloud
- Valider les licences du service ADM
- Migrer à l'aide d'un script

Après avoir migré d'ADM local vers le service ADM, si vous souhaitez à nouveau continuer avec ADM local, vous pouvez utiliser le script d'annulation. Pour plus d'informations, consultez la section Roll back to OnPremise ADM.

Configurer l'agent de service ADM

Pour activer les communications entre les instances Citrix ADC et Citrix ADM, vous devez configurer un agent. Les agents Citrix ADM sont, par défaut, automatiquement mis à niveau vers la dernière version. Vous pouvez également sélectionner une heure spécifique pour la mise à niveau de l'agent. Pour plus d'informations, consultez Configuration des paramètres de mise à niveau de l'agent

- Si votre ADM local existant (paire autonome ou HA) n'a pas d'agents locaux configurés, vous devez configurer au moins un agent pour le service ADM.
- Si votre ADM local existant (paire autonome ou HA) a configuré avec des agents locaux pour les déploiements multisites, vous devez configurer le même nombre d'agents pour le service ADM.

Pour plus d'informations sur la configuration d'un agent, consultez la section Mise en route.

Obtenir le client et le fichier CSV secret à partir de Citrix Cloud

Après avoir configuré l'agent, récupère le client et le fichier CSV secret à partir de la page Citrix Cloud :

1. Connectez-vous à citrix.cloud.com
2. Cliquez sur l'icône **Accueil** et sélectionnez **Gestion des identités et des accès**.
3. Dans l'onglet **Accès aux API**, entrez un nom de client sécurisé et cliquez sur **Créer un client**.
4. ID et Secret sont générés. Cliquez sur **Télécharger** et enregistrez le fichier CSV dans l'ADM local.

   Par exemple, enregistrez le fichier CSV dans le répertoire /var.

Valider les licences du service ADM

Vous devez obtenir des licences pour le service ADM.

- Les licences VIP dans le service ADM doivent être supérieures ou égales aux licences VIP locales.

  > **Remarque**
  >
  > Si les licences VIP sont inférieures, les serveurs virtuels sont sélectionnés au hasard et la configuration de niveau VIP pour le service ADM échoue.

- Si vous utilisez le déploiement local ADM en tant que serveur de licences, réaffectez vos licences au service ADM avant la migration. Pour plus d'informations, consultez Configurer un serveur ADM uniquement en tant que serveur de licences groupé et Comment réallouer un fichier de licences.

- Si vous utilisez les licences regroupées dans ADM local, vous devez obtenir les licences regroupées pour le service ADM, puis allouer des licences aux instances ADC. Pour plus d'informations, consultez Configurer les licences groupées. Les versions ADC prises en charge suivantes vous permettent de modifier l'allocation de licence d'ADM :
  - Citrix ADC SDX : 13.0 74.11 ou versions ultérieures.
  - Citrix ADC VPX et MPX : 13.0 47.24 ou versions ultérieures, 12.1 58.14 ou versions ultérieures, et 11.1 65.10 ou versions ultérieures.

Migrer à l'aide d'un script

- À l'aide de la version ADM 82.x, vous pouvez sélectionner la fonctionnalité, puis procéder à la migration.
- Pour les versions ADM 76.x ou ultérieures, les scripts de migration (`servicemigrationtool.py` et `config_collect_onprem.py`) sont disponibles dans le cadre de la build, disponibles à l'adresse `cd /mps/scripts`.
- Pour les versions ADM antérieures à 76.x, vous devez télécharger les scripts de migration et copier les scripts dans ADM local.

> Remarque
>
> Assurez-vous que l'ADM local dispose d'une connectivité Internet pendant la migration.

1. À l'aide d'un client SSH, connectez-vous à l'ADM local.

> Remarque
>
> Pour une paire ADM HA, ouvrez une session sur le nœud principal.

2. Tapez **shell** et appuyez sur **Entrée** pour passer en mode bash.
3. Copiez l'ID client et le fichier CSV secret. Par exemple, copiez le fichier dans le répertoire /var.

   Après avoir copié le fichier CSV, vous pouvez valider si le fichier CSV est présent.

```
bash-3.2# cd /var
bash-3.2# pwd
/var
bash-3.2# ls -ltr secureclient.csv
-rw-r--r--  1 root  nobody  102 Dec 11 19:09 secureclient.csv
bash-3.2#
```

> Remarque
>
> Pour une paire ADM HA, copiez le fichier CSV dans le nœud principal.

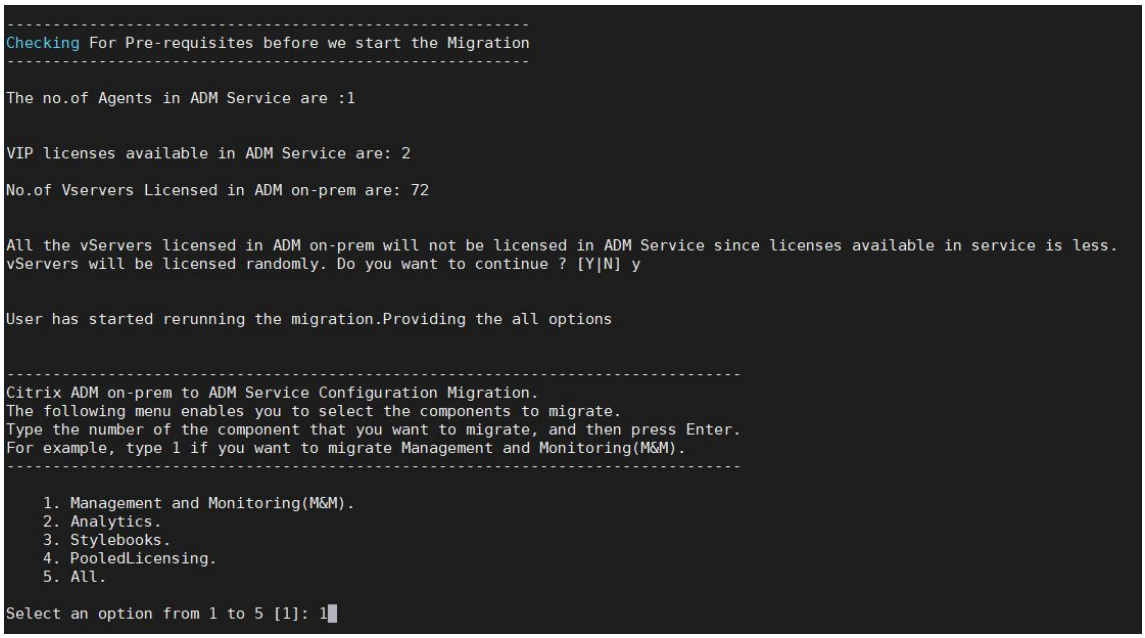
4. Pour la **version ADM 13.0 82.xx**, exécutez les commandes suivantes pour terminer la migration :

   a) `cd /mps/scripts`

   b) `python servicemigrationtool.py <path of ClientID/Secret File in on-premises Citrix ADM VM>`

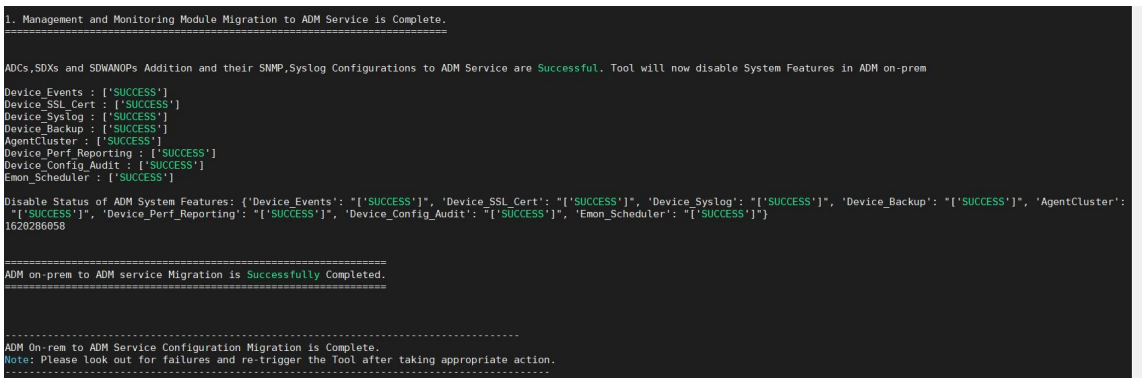
   Par exemple, `python servicemigrationtool.py /var/secureclient.csv`

   Après avoir exécuté le script de migration, l'outil affiche les options suivantes :



   Selon le choix que vous offrez, seule cette fonctionnalité est migrée vers le service ADM.

   Dans cet exemple, l'option 1 est sélectionnée. L'outil termine la migration de la gestion et de la surveillance (M&M) et affiche le message suivant :



   La fonction **de gestion et de surveillance (M&M)** comprend :

   - Instances ADC, balises, groupes d'instances, profils, applications personnalisées, tâches de configuration, SNMP, configurations Syslog.

- Sites, blocs d'adresses IP, rapports réseau, seuils d'analyse, paramètres de notification, paramètres d'nettoyage des données.
- Configure les modèles d'audit, les intervalles d'interrogation, les règles d'événement et les paramètres.
- Groupes, rôles et stratégies RBAC

La fonctionnalité **Analytics** inclut :

- Configuration Appflow par serveur virtuel à partir d'instances ADC.
- Configuration Appflow par périphérique SDWAN.

> Remarque :
>
> - La fonctionnalité Gestion et surveillance (M&M) est automatiquement migrée, même si vous sélectionnez une autre fonctionnalité (2, 3 ou 4).
> - Vous ne pouvez spécifier qu'une seule fonction à la fois.
> - Une fois la migration d'une fonctionnalité terminée, si vous souhaitez migrer une autre fonctionnalité ultérieurement, la fonctionnalité déjà migrée n'apparaît pas dans la liste. Par exemple, si vous terminez d'abord la migration de la fonctionnalité **Analytics**, la prochaine fois que vous exécuterez le script de migration, vous ne pourrez voir que les options **StyleBooks**, **Licences groupées**et **Toutes** .

5. Pour la **version ADM 13.0 76.xx**, exécutez les commandes suivantes pour terminer la migration :

   a) `cd /mps/scripts`

   b) `python servicemigrationtool.py <path of ClientID/Secret File in on-premises Citrix ADM VM>`

   Par exemple, `python servicemigrationtool.py /var/secureclient.csv`

6. Pour ADM antérieure à la version 13.0 76.xx :

   a) Téléchargez le script de migration à partir de l'emplacement suivant : `https://download.citrixnetworkapi.net/root/download/v1/public/software?product=admonprem&build=migrationtool&model=servicemigration.tgz`

   The downloaded file comprises two bundle scripts, `servicemigrationtool_27.py` and `config_collect_onprem_27.py`.

   b) Enregistrez les deux scripts dans ADM local. Par exemple, enregistrez dans le répertoire /var

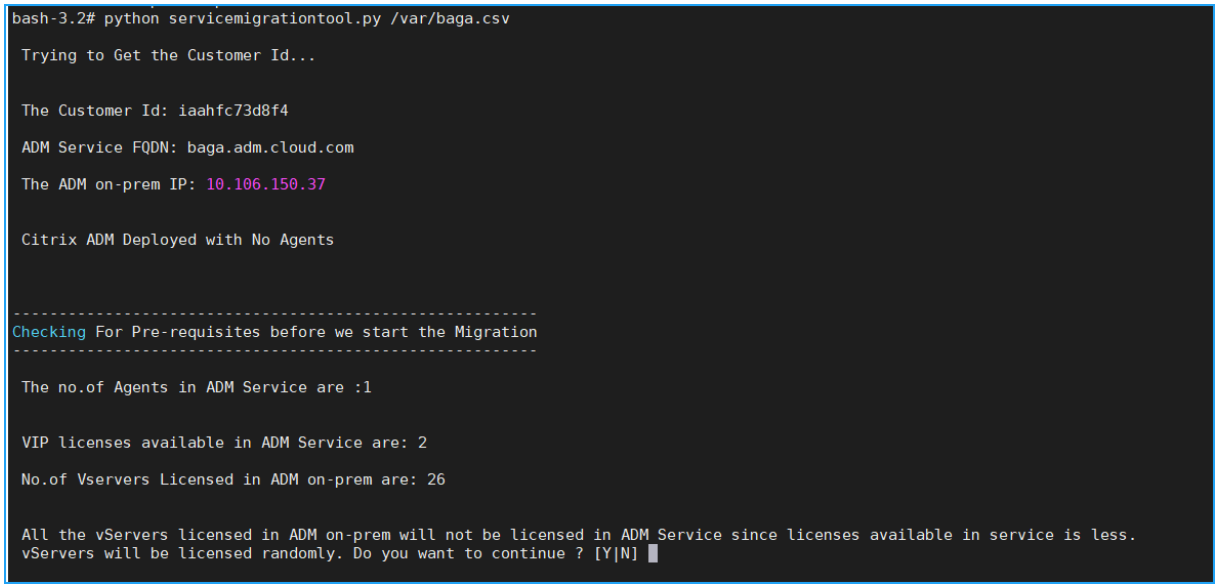
c) Exécutez les commandes suivantes pour migrer :

i. `cd /var`

ii. `servicemigrationtool_27.py <path of ClientID/Secret File in on-premises ADM VM>`

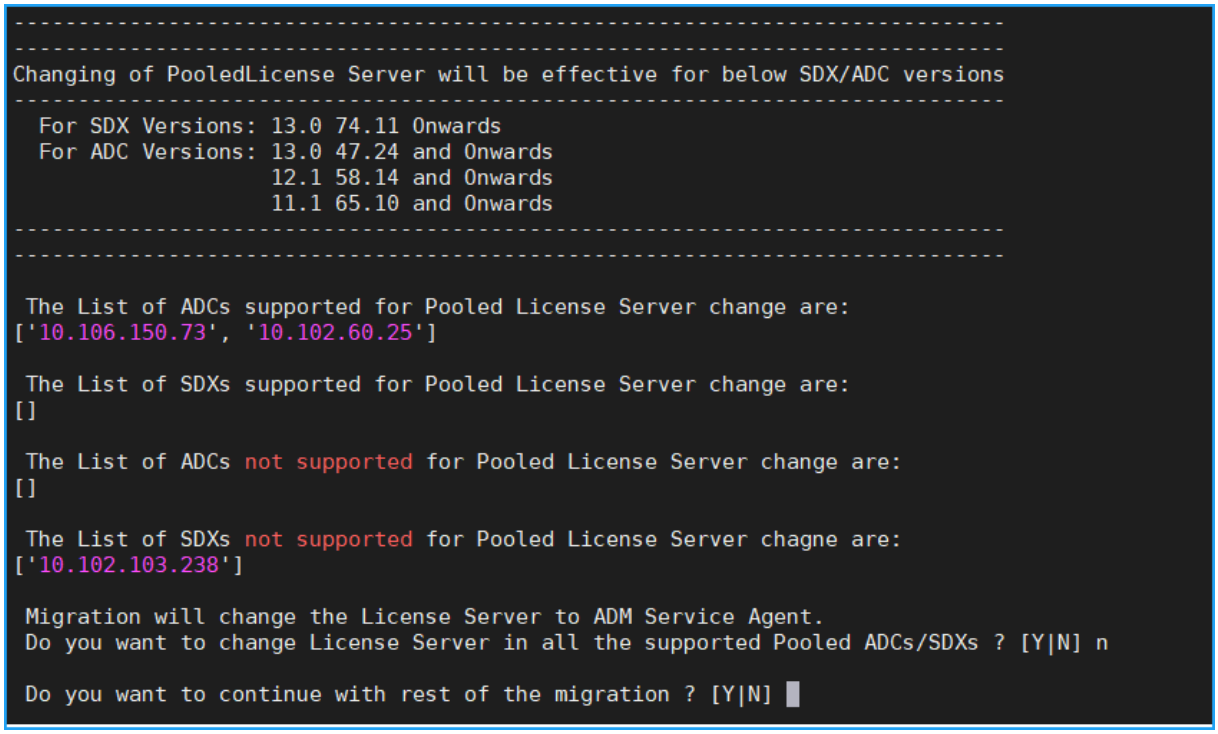
Par exemple, `python servicemigrationtool_27.py /var/secureclient.csv`

Après avoir exécuté le script, il vérifie les conditions préalables, puis procède à la migration. Le script vérifie d'abord la disponibilité de la licence. Le message suivant s'affiche uniquement si vous disposez d'une licence de service ADM inférieure à la licence locale.



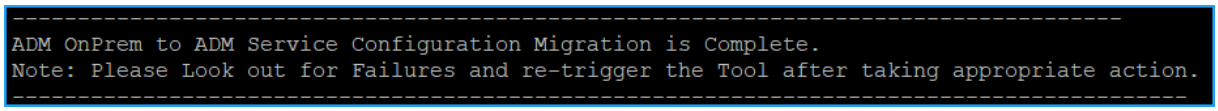
Si vous sélectionnez **Y**, la migration se poursuit en accordant une licence au VIP de manière aléatoire. Si vous sélectionnez **N**, le script arrête la migration.

Si vous disposez de la version d'instance ADC non prise en charge pour le serveur de licences groupé, le message suivant s'affiche :



Si vous sélectionnez **Y**, le processus de migration continue en modifiant le serveur de licences. Si vous sélectionnez **N**, le script vous invite si vous souhaitez poursuivre le reste de la migration. Le script arrête la migration si vous sélectionnez **N**.

Selon la configuration locale, la durée approximative de la migration se termine entre quelques minutes et quelques heures. Une fois la migration terminée, le message suivant s'affiche :



La migration réussit une fois que toutes les instances WANOP ADC et SD-WAN et leurs configurations respectives ont été transférées vers le service ADM. Après la migration réussie, Citrix ADM local arrête de traiter les événements d'instance suivants :

- Certificats SSL
- Messages Syslog
- Sauvegarde
- Cluster d'agents
- Rapports sur le rendement
- Audit de configuration
- Emon planificateur

Revenir à ADM sur site

Si vous souhaitez revenir à ADM local, assurez-vous que les conditions préalables sont remplies.

Conditions préalables

Si votre ADM local (avant la migration vers le service ADM) est :

- Utilisé en tant que serveur de licences groupé, assurez-vous que vous disposez des licences groupées requises dans l'ADM local.
- Configuré avec des agents ADM locaux, assurez-vous que les agents sont disponibles dans l'état « UP ».

Utilisez le script de restauration

> Remarque
>
> Après la restauration, les mêmes configurations (avant la migration) dans Analytics, SNMP et les licences groupées sont à nouveau disponibles dans ADM local. Si vous avez apporté des modifications à ces configurations après la migration, ces modifications ne sont pas reflétées dans ADM local.

- Pour les versions **ADM 82.xx ou ultérieures**, le script d'annulation est disponible dans le cadre de la génération et accessible à l'adresse `/mps/scripts`.
- Pour les versions d'**ADM antérieures à 79.xx**, vous pouvez soit mettre à niveau vers la version 82.x et utiliser le script d'annulation, soit télécharger le script d'annulation et copier le script dans ADM local.

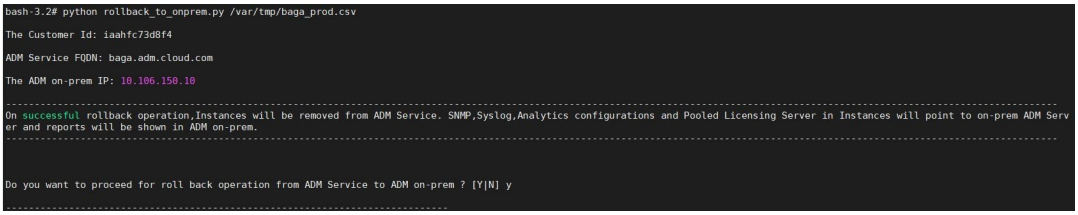
1. À l'aide d'un client SSH, connectez-vous à l'ADM local.
2. Tapez shell et appuyez sur Entrée pour passer en mode bash.
3. Pour la version **82.xx d'ADM 13.0**, exécutez les commandes suivantes pour terminer l'annulation :

   a) cd /mps/scripts

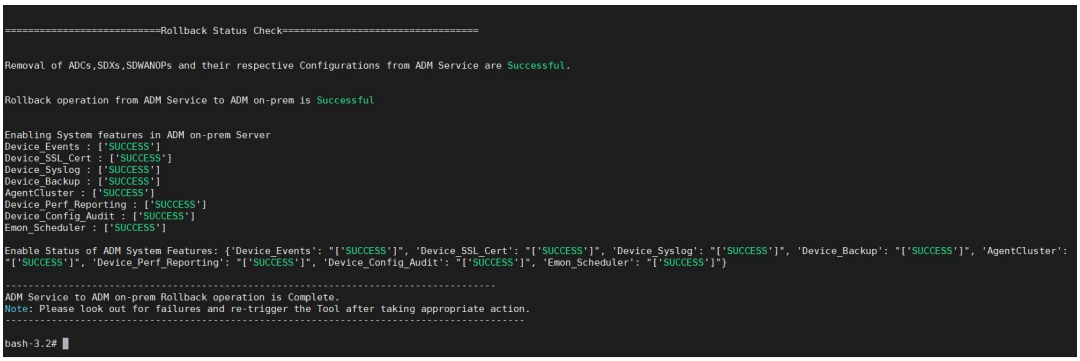
   b) rollback_to_onprem.py de python <`path of ClientID/Secret File in ADM on-prem VM`>

   Par exemple, `python rollback_to_onprem.py /var/ secureclient.csv.csv`

   L'outil lance l'opération d'annulation et un message vous demande si vous souhaitez continuer. Tapez **Y** pour continuer.



Le message suivant s'affiche une fois l'annulation terminée.



4. Pour ADM antérieur à 82.xx build :

   a) Téléchargez le script de restauration à partir de l'emplacement suivant :

      `https://download.citrixnetworkapi.net/root/download/v1/public/software?product=admonprem&build=migrationtool&model=servicemigration.tgz`

   b) Pour les versions ADM 79.xx et 76.xx, enregistrez le script dans `/mps/scripts` et exécutez les commandes suivantes pour revenir en arrière :

      i. `cd /mps/scripts`

      ii. `python rollback_to_onprem.py < path of client/secret csv file in ADM on-prem>`

      Par exemple, `python rollback_to_onprem.py /var/ secureclient.csv`

   c) Pour les versions d'ADM antérieures à 76.xx, enregistrez le script dans ADM local. Par exemple, enregistrez-le à l'emplacement `/var` et exécutez les commandes suivantes pour revenir en arrière :

      i. `cd /var`

      ii. `python rollback_to_onprem_27.py < path of client/secret csv file in ADM on-prem>`

      Par exemple, `python rollback_to_onprem_27.py /var/secureclient.csv`

L'outil lance l'opération d'annulation et un message vous demande si vous souhaitez continuer. Tapez **Y** pour continuer.

FAQ

February 1, 2024

Service ADM

L'agent de service ADM est-il facultatif similaire à l'agent Citrix ADM local ?

Non. L'agent de service ADM est obligatoire pour le service ADM et toutes les communications entre les instances et le service ADM sont transmises par l'intermédiaire de l'agent de service ADM. L'agent ADM local est facultatif ; toutefois, vous pouvez configurer l'agent local uniquement pour économiser la consommation de bande passante.

Pourquoi le service ADM ?

Le service ADM via Citrix Cloud offre les avantages suivants, sans nécessiter de nouvelles versions périodiques :

- Offre SaaS basée sur le cloud avec intégration plus facile et coût de possession moindre que le Citrix ADM local.
- Des versions plus rapides, environ toutes les deux semaines avec les dernières mises à jour des fonctionnalités.
- Analyse basée sur l'apprentissage automatique pour la sécurité, les performances et l'utilisation des applications.
- Diverses autres fonctionnalités actuellement prises en charge uniquement dans le service ADM, telles que l'analyse des périodes de pointe et creuses, l'analyse de la sécurité des applications basée sur l'apprentissage automatique pour WAF et bot, l'analyse du processeur applicatif et bien d'autres encore.

Vous pouvez également participer au webinaire mensuel du service Citrix ADM pour comprendre les dernières fonctionnalités et solutions du produit. Inscrivez-vous au webinaire en utilisant le lien suivant :

`https://attendee.gotowebinar.com/register/4248811314610265355`

Ou

https://attendee.gotowebinar.com/register/1601431406507289611

Que se passe-t-il après la migration si Citrix ADM local est une paire HA ?

Toutes les configurations sont déplacées vers Citrix Cloud. La configuration d'un nœud de reprise après sinistre n'est pas requise.

Que se passe-t-il si l'agent tombe pour une raison quelconque ?

Vous pouvez vous attendre à une perte de données potentielle jusqu'à ce que l'agent soit opérationnel. Toutefois, vous pouvez également configurer des agents ADM pour les déploiements multisites afin d'assurer la continuité en cas de basculement d'agent. Pour plus d'informations, consultez la section Configurer les agents ADM pour le déploiement multisite.

La sauvegarde d'instance est-elle également migrée ?

La sauvegarde n'est pas incluse dans la migration.

Les données historiques sont-elles également migrées ?

Les données historiques ne sont pas migrées. Vous pouvez exporter les données à partir de l'ADM local.

Les licences locales sont-elles également migrées ?

Non. Le fichier de licence local ne peut pas être utilisé pour le service ADM. Vous devez obtenir des licences pour le service ADM. Pour plus d'informations, consultez l'article Licences. Si vous utilisez des licences groupées dans ADM local, vous devez obtenir des licences groupées pour le service ADM, puis allouer des licences aux instances.

Qu'est-ce qui n'est pas migré à partir de Citrix ADM local ?

Les fonctionnalités suivantes ne peuvent pas être migrées vers le service ADM :

- **RBAC** —Dans le service ADM, l'accès utilisateur est basé sur l'invitation de l'administrateur. Les utilisateurs du service ADM doivent disposer d'un compte dans Citrix Cloud. Par conséquent, les utilisateurs ADM locaux ne sont pas migrés.

- **Programmes d'exportation : les** programmes d'exportation incluent des détails tels que l'exploration vers le bas et les calendriers provenant de différentes pages. Tous ces calendriers d'exportation détaillés ne sont pas migrés.
- **Certificats SSL/clés/CSRS** —Le service ADM ne peut afficher que les certificats SSL ADC, les clés/CSR. Par conséquent, les certes/clés SSL chargés sur Citrix ADM local ne seront pas migrés vers le service ADM.

Citrix ADM sur site est intégré à Citrix Director. Qu'advient-il de l'intégration ?

L'intégration de Director avec ADM est actuellement prise en charge uniquement dans ADM local.

Après la migration, est-il de nouveau nécessaire de concéder une licence sur l'instance ou d'activer l'analyse ?

Vous devez vous assurer que les licences du service ADM sont supérieures ou égales aux licences VIP locales. Si les licences sont déjà supérieures à Citrix ADM VIP local, les serveurs virtuels sont automatiquement sous licence. Si ce n'est pas le cas, les licences sont attribuées de manière aléatoire.

Outil de migration

Après l'exécution du script de migration, des messages d'erreur s'affichent. Quel peut être le problème ?

Un fichier journal avec des raisons d'échec s'affiche. Vous pouvez prendre les mesures correctives appropriées et exécuter à nouveau le script de migration. En général, avant d'exécuter le script de migration, assurez-vous de :

- Configurer l'agent de service ADM
- Obtenir les licences du service ADM
- Copiez le chemin correct où vous avez stocké le client et le fichier CSV sécurisé

Les instances ADC ont des versions inférieures à la limite mentionnée pour les licences groupées. Que se passe-t-il si l'option 'Y'est sélectionnée pour changer le serveur de licences ?

Le changement de serveur de licences se produit uniquement pour les versions Citrix ADC MPX, VPX et SDX prises en charge.

Que se passe-t-il si le script de migration a échoué la configuration concernant les instances WANOP ADC/SD-WAN ?

Les instances WANOP ADC et SD-WAN continuent à fonctionner sur la configuration d'ADM locale. Vous pouvez prendre les mesures nécessaires à partir de la raison d'échec suggérée et exécuter à nouveau le script de migration.

Que se passe-t-il si certaines instances WANOP ADC ou SD-WAN ne parviennent pas à passer au service ADM. La réexécution du script de migration sera-t-elle utile ?

Oui. Après avoir réexécuté le script, seules les instances ayant échoué sont migrées. Supposons que deux instances sur cinq n'ont pas réussi à bouger. Après avoir pris des mesures correctives et réexécuter le script de migration, trois instances qui ont été déplacées avec succès plus tôt affichent le message « Périphérique existe déjà ». Et les deux autres instances qui ont échoué précédemment sont migrées avec succès.

Existe-t-il un fichier journal pour vérifier l'état de la migration ?

Oui, un fichier journal est généré dans le répertoire `/var/mps/log/`. ADM avec python3.7 a le fichier journal comme `servicemigrationtool.py.log` et ADM avec python 2.7 a le fichier journal comme `servicemigrationtool_27.py.log`.

Que se passe-t-il si la session est terminée lors de l'exécution du script de migration ?

Vous pouvez réexécuter le script de migration. Dans la nouvelle session, les instances déjà ajoutées de la dernière session s'affichent comme « Le périphérique existe déjà », et la migration continue.

Que se passe-t-il si le service ADM dispose de licences inférieures à celles du Citrix ADM local et que le script de migration est lancé ?

Une fois le script de migration exécuté, une suggestion apparaît, mentionnant les licences est moindre et invite à continuer ou à arrêter. Si vous souhaitez continuer avec des licences moins réduites, les serveurs virtuels sont sous licence aléatoirement à partir des licences disponibles.

Que se passe-t-il lorsque Citrix ADM local est migré vers le compte Express du service ADM ?

Le compte Express du service ADM ne possède que deux licences de serveur virtuel, deux packs de configuration StyleBook et deux tâches de configuration. Si votre ADM local possède plus de configurations que ces configurations et que vous lancez la migration avec Express Account, le script peut

migrer uniquement les configurations mentionnées applicables à Express Account (deux licences de serveur virtuel, deux packs de configuration StyleBook et deux tâches de configuration)

Que se passe-t-il si un utilisateur invité Citrix Cloud (autre que l'utilisateur Admin qui a créé un compte Citrix Cloud) tente de migrer la configuration ADM locale ?

Il est recommandé à l'administrateur d'exécuter le script de migration. Un utilisateur invité ne dispose pas de privilèges d'administrateur (AdminExceptSystem_Group). Par conséquent, la migration des groupes, des rôles et des stratégies échoue et le message « L'utilisateur n'a pas d'autorisation » s'affiche.

En tant que solution, l'administrateur (qui a créé le compte Citrix Cloud) peut modifier le groupe associé à l'utilisateur invité en tant que « admin_group ».

Script d'annulation

Que se passe-t-il si un script d'annulation est utilisé dans une paire ADM HA locale ?

La paire HA ADM locale est restaurée avec toutes les configurations qui étaient disponibles avant la migration.

Qu'advient-il du nœud de reprise après sinistre après avoir utilisé le script de restauration ?

Le nœud de reprise après sinistre est également restauré avec toutes les configurations avant la migration.

Dépannage

February 1, 2024

Lorsque vous exécutez le script de migration pour la première fois, il vérifie les conditions préalables et procède à la migration. Si toutes les conditions préalables sont remplies, la migration se termine sans erreur. Si une condition préalable échoue, le script affiche des messages d'erreur avec les raisons. Après avoir corrigé les erreurs, vous devez réexécuter le script.

> Remarque
>
> Si vous voyez un message d'erreur qui affiche « déjà existe », cela signifie que :
>
> - Vous avez peut-être exécuté le script de migration plusieurs fois et certaines configurations

> sont déjà migrées vers le service ADM.
>
> - Vous avez peut-être créé manuellement la même configuration dans le service ADM, avant d'exécuter le script de migration.

Reportez-vous à certains des messages d'erreur suivants :

Profil manuel ajouté au service ADM

```
==================Profiles Addition to ADM Service====================


60.26 : FAILURE : Profile 60.26 already exists


 The list of ADC profiles added to ADM Service are :

{'60.26': "['FAILURE']"}
```

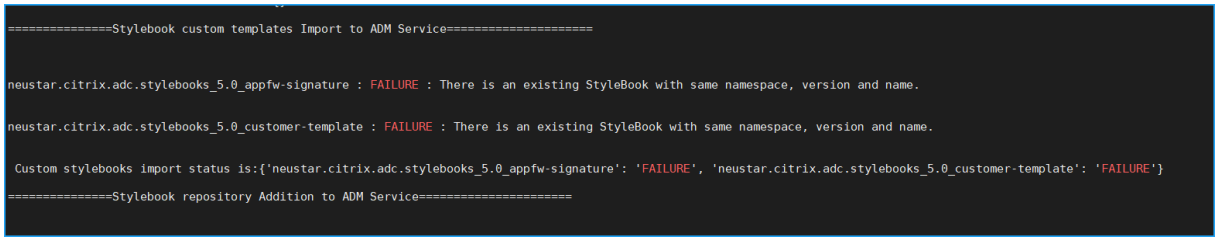
Solution : si vous avez créé des profils d'administrateur dans le service Citrix ADM avant d'exécuter le script de migration, assurez-vous de supprimer ces profils et de réexécuter le script de migration.

Périphérique Citrix ADC ajouté au service ADM

```
==============ADC Device Addition================

10.106.150.53 : FAILURE : Error in contacting Citrix ADC, invalid credentials.
10.102.60.26 : FAILURE :Device with this IP address already exists.


The list of ADCs added to ADM Service are:


['10.102.60.26']
```

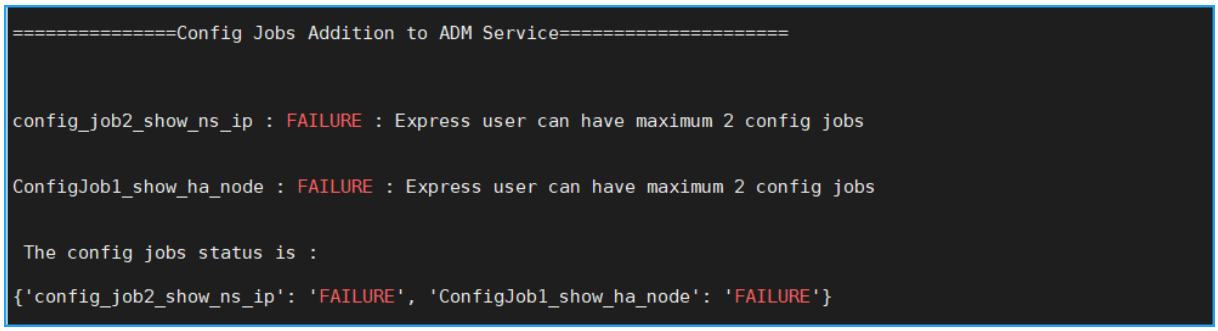
Solution : Dans ADM local, vérifiez l'état de l'instance et vérifiez si vous pouvez accéder à l'instance sans problème. Si un problème persiste, corrigez le problème et réexécutez le script de migration.

Importation de modèles personnalisés StyleBook vers le service ADM



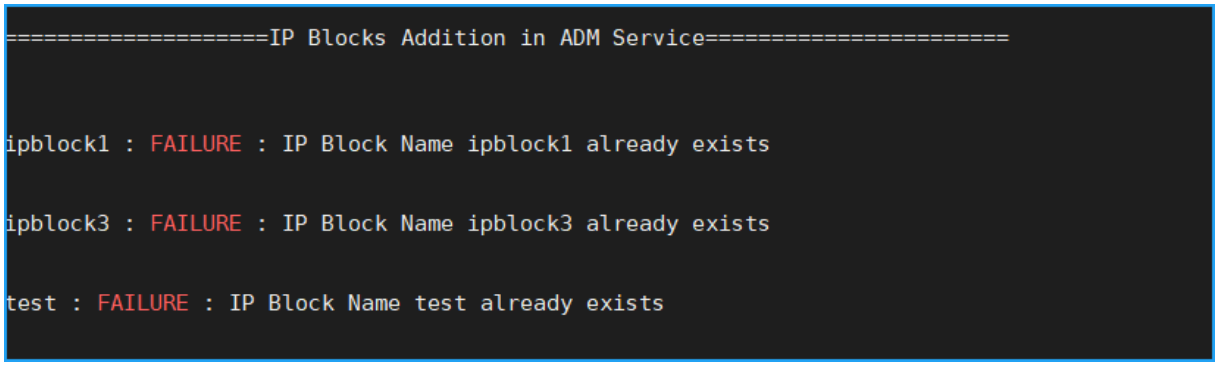
Solution : ce message d'erreur est un exemple pour le StyleBook déjà migré. Vous pouvez également voir cette erreur si vous avez créé manuellement un StyleBook portant le même nom, la version et l'espace de noms, dans le service Citrix ADM avant d'exécuter le script de migration.

Jobs de configuration ajoutés au service ADM



Solution : cette erreur se produit si vous êtes abonné à Express Account et avez plus de deux tâches de configuration. Vous devez obtenir un abonnement valide pour que toutes vos tâches de configuration soient migrées.

Blocs IP ajoutés au service ADM



Solution : supprimez le bloc IP créé manuellement dans le service ADM et réexécutez le script de migration.

État d'ajout du rapport de tableau de bord

```
================Network Dashboard Reports Addition to ADM Service================


new456 : FAILURE : Dashboard new456 already exists

new123 : FAILURE : Dashboard new123 already exists

 The network dashoard reports addition status is:
{'new456': "['FAILURE']", 'new123': "['FAILURE']"}
```

Solution : supprimez le tableau de bord créé manuellement dans le service ADM et réexécutez le script de migration.

Liste des articles pratiques

February 1, 2024

Les « articles pratiques » de Citrix Application Delivery Management (Citrix ADM) sont des articles simples, pertinents et faciles à mettre en œuvre sur les fonctionnalités de Citrix ADM. Ces articles contiennent des informations sur certaines des fonctionnalités populaires de Citrix ADM, telles que la gestion des instances, la gestion des applications, les StyleBooks, la gestion des certificats et les analyses.

Cliquez sur le nom d'une fonctionnalité dans le tableau ci-dessous pour afficher la liste des articles pratiques relatifs à cette fonctionnalité.

		Sujets		
Gestion des instances	Gestion d'événements	StyleBooks	Gestion des certificats	Système Citr
Gestion des applications	Gestion de la configuration	Authentification	Analytics	Fonctions ré

Gestion des instances

Comment surveiller les sites distribués à l'échelle mondiale

Comment gérer les partitions d'administration des instances Citrix ADC

Comment ajouter des instances à Citrix ADM

Comment créer des groupes d'instances sur Citrix ADM

Comment faire pour configurer des sites pour Geomaps dans Citrix ADM

Comment forcer un basculement vers l'instance secondaire de Citrix ADC à l'aide de Citrix ADM

Comment forcer une instance secondaire de Citrix ADC à rester secondaire à l'aide de Citrix ADM

Comment sauvegarder et restaurer une instance à l'aide de Citrix ADM

Comment utiliser le tableau de bord Citrix ADM pour surveiller une instance HAProxy

Comment afficher les détails des frontends configurés sur les instances HAProxy

Comment afficher les détails des backends configurés sur les instances HAProxy

Comment afficher les détails des serveurs configurés sur les instances HAProxy

Comment redémarrer une instance HAProxy à partir de Citrix ADM

Comment sauvegarder et restaurer une instance HAProxy à l'aide de Citrix ADM

Comment modifier le fichier de configuration HAProxy à l'aide de Citrix ADM

Comment redécouvrir plusieurs instances Citrix ADC VPX

Comment interroger les instances et entités Citrix ADC dans Citrix ADM

Comment annuler la gestion d'une instance sur Citrix ADM

Comment tracer l'itinéraire vers une instance à partir de Citrix ADM

Gestion de la configuration

Comment créer une tâche de configuration sur Citrix ADM

Comment utiliser la commande SCP (put) dans les tâches de configuration

Comment faire pour mettre à niveau des instances Citrix ADC SDX à l'aide de Citrix ADM

Comment planifier des tâches créées à l'aide de modèles intégrés dans Citrix ADM

Comment replanifier des travaux configurés à l'aide de modèles intégrés dans Citrix ADM

Comment réutiliser les tâches de configuration exécutées

Comment faire pour mettre à niveau des instances Citrix ADC à l'aide de Citrix ADM

Comment utiliser des variables dans des tâches de configuration sur Citrix ADM

Comment utiliser des modèles de configuration pour créer des modèles d'audit sur Citrix ADM

Comment créer des tâches de configuration à partir de commandes correctives sur Citrix ADM

Comment répliquer les commandes de configuration en cours d'exécution et enregistrées d'une instance Citrix ADC vers une autre sur Citrix ADM

Comment faire pour créer des tâches de configuration pour les instances WO Citrix SD-WAN dans Citrix ADM

Comment utiliser Record-and-Play pour créer des tâches de configuration

Comment faire pour utiliser les tâches de configuration pour répliquer la configuration d'une instance vers plusieurs instances

Comment faire pour utiliser le modèle de configuration maître sur Citrix ADM

Comment interroger l'audit de configuration des instances Citrix ADC

Comment réutiliser les modèles d'audit de configuration dans les tâches de configuration

Comment importer et exporter des modèles de configuration

Comment générer un diff d'audit de configuration pour les pièges SNMP ConfigChange

Gestion des certificats

Comment configurer une stratégie d'entreprise sur Citrix ADM

Comment installer des certificats SSL sur une instance Citrix ADC à partir de Citrix ADM

Comment mettre à jour un certificat installé depuis Citrix ADM

Comment lier et dissocier des certificats SSL à l'aide de Citrix ADM

Comment créer une demande de signature de certificat (CSR) à l'aide de Citrix ADM

Comment configurer les notifications pour l'expiration du certificat SSL à partir de Citrix ADM

Comment faire pour utiliser le tableau de bord SSL sur Citrix ADM

Comment interroger les certificats SSL à partir d'instances Citrix ADC

Gestion des applications

Comment créer une définition d'application dans Citrix ADM

StyleBooks

Comment afficher différents groupes de StyleBooks

Comment créer vos propres StyleBooks

Comment utiliser des StyleBooks définis par l'utilisateur dans Citrix ADM

Comment utiliser l'API pour créer des configurations à partir de StyleBooks

Comment activer les analyses et configurer les alarmes sur un serveur virtuel défini dans un StyleBook

Comment créer un StyleBook pour télécharger des fichiers vers Citrix ADM

Comment utiliser l'API pour créer des configurations permettant de télécharger n'importe quel type de fichier

Comment faire pour créer un StyleBook pour charger des fichiers de certificat SSL et de clé de certificat vers Citrix ADM

Comment utiliser l'API pour créer des configurations afin de télécharger des fichiers de certificats et de clés

Comment faire pour utiliser Microsoft Skype for Business StyleBook dans les entreprises

Comment utiliser Microsoft Exchange StyleBook dans les entreprises

Comment faire pour utiliser Microsoft SharePoint StyleBook dans les entreprises

Analytics

Comment activer les analyses sur les instances

Comment configurer des seuils adaptatifs

Comment configurer la gestion des SLA

Comment configurer la synthèse des bases de données à des fins d'analyse

Comment créer des seuils et des alertes à l'aide de Citrix ADM

Comment désactiver la collecte de données URL à des fins d'analyse à partir de Citrix ADM

Comment afficher le type de vidéos diffusées en continu et le volume de données consommé à partir de votre réseau

Comment afficher le débit de données de pointe pour une période donnée

Comment afficher l'efficacité du réseau

Gestion d'événements

Comment définir l'âge des événements sur Citrix ADM

Comment planifier un filtre d'événements à l'aide de Citrix ADM

Comment configurer des notifications par e-mail répétées pour les événements provenant de Citrix ADM

Comment supprimer des événements à l'aide de Citrix ADM

Comment utiliser le tableau de bord des événements pour surveiller les événements

Comment créer des règles d'événement sur Citrix ADM

Comment faire pour modifier la gravité signalée des événements qui se produisent sur les instances de Citrix ADC

Comment afficher le résumé des événements dans Citrix ADM

Comment afficher la sévérité des événements et les asymétries des pièges SNMP sur Citrix ADM

Comment exporter des messages syslog à l'aide de Citrix ADM

Comment supprimer les messages Syslog dans Citrix ADM

Comment configurer les paramètres de paramétrage pour les événements d'instance

Authentification

Comment activer les serveurs d'authentification externes de secours et en cascade

Comment ajouter des serveurs d'authentification RADIUS

Comment ajouter des serveurs d'authentification LDAP

Comment ajouter des serveurs d'authentification TACACS

Comment extraire un groupe de serveurs d'authentification dans Citrix ADM

Comment activer l'authentification locale de secours

Système Citrix ADM

Comment mettre à niveau Citrix ADM

Comment réinitialiser le mot de passe pour Citrix ADM

Comment générer un fichier de support technique pour Citrix ADM

Comment sauvegarder et restaurer votre serveur Citrix ADM dans le cadre d'un déploiement de serveur unique

Comment sauvegarder et restaurer une configuration Citrix ADM dans une paire HA

Comment activer l'accès au shell pour les utilisateurs autres que ceux par défaut dans Citrix ADM

Comment configurer le serveur NTP sur Citrix ADM

Comment configurer les paramètres SSL pour Citrix ADM

Comment configurer l'intervalle de purge Syslog pour Citrix ADM

Comment afficher les informations d'audit de Citrix ADM

Comment configurer les paramètres de notification système de Citrix ADM

Comment surveiller l'utilisation du processeur, de la mémoire et du disque de Citrix ADM

Comment configurer un groupe de chiffrement pour Citrix ADM

Comment créer des pièges, des gestionnaires et des utilisateurs SNMP sur Citrix ADM

Comment attribuer un nom d'hôte à un serveur Citrix ADM

Comment configurer les paramètres d'nettoyer du système pour Citrix ADM

Comment configurer les paramètres de sauvegarde du système à l'aide de Citrix ADM

Comment configurer et afficher les alarmes système sur Citrix ADM

Fonctions réseau

Comment générer des rapports pour les entités d'équilibrage de charge

Comment exporter ou planifier l'exportation de rapports sur les fonctions réseau

Vue d'ensemble

February 1, 2024

Citrix Application Delivery Management (ADM) est une solution de gestion centralisée qui simplifie les opérations en fournissant aux administrateurs une visibilité à l'échelle de l'entreprise et en automatisant les tâches de gestion qui doivent être exécutées sur plusieurs instances. Vous pouvez gérer et surveiller les produits de mise en réseau des applications Citrix, notamment Citrix ADC MPX, Citrix ADC VPX, Citrix ADC SDX, Citrix ADC CPX, Citrix Gateway et Citrix SD-WAN. Vous pouvez utiliser ADM pour gérer, surveiller et dépanner l'ensemble de l'infrastructure globale de mise à disposition d'applications à partir d'une console unifiée unique.

ADM est une appliance virtuelle qui s'exécute sur Citrix Hypervisor, VMware ESXi et Linux KVM. ADM relève le défi de la visibilité des applications en collectant les informations détaillées suivantes sur le trafic des applications Web et des postes de travail virtuels :

- informations au niveau de la session utilisateur
- Données de performance des pages Web
- qui circulent dans les instances ADC de votre site et fournissent des rapports exploitables.

ADM permet aux administrateurs informatiques de dépanner et de surveiller de manière proactive les problèmes des clients en quelques minutes.

Caractéristiques et solutions

February 1, 2024

Citrix Application Delivery Management (ADM) fournit les fonctionnalités suivantes :

Analyse et gestion des applications

Analyse des performances des applications

App Score est le produit d'un système de notation qui définit les performances d'une application. Il montre si l'application fonctionne bien en termes de réactivité, n'est pas vulnérable aux menaces et si tous les systèmes sont opérationnels.

Analyses de sécurité des applications

Le tableau de bord de la sécurité des applications fournit une vue globale de l'état de sécurité de vos applications. Par exemple, il affiche des mesures de sécurité clés telles que les violations de sécurité, les violations de signature, les indices de menaces. Le tableau de bord App Security affiche également des informations relatives aux attaques telles que les attaques SYN, les attaques de petites fenêtres et les attaques par saturation DNS pour les instances ADC découvertes.

Réseaux

Instances

Permet de gérer les instances Citrix ADC, Citrix Gateway, Citrix SD-WAN et HAProxy.

Groupes d'instances

Vous permet de regrouper vos instances comme suit :

- Groupe statique : vous permet de définir un groupe de périphériques que vous pouvez utiliser dans différentes tâches telles que les tâches de configuration, etc.
- Blocage IP privé : vous permet de regrouper vos instances en fonction de leur localisation géographique.

Gestion d'événements

Lorsque l'adresse IP d'une instance ADC est ajoutée à ADM, un appel NITRO est envoyé par ADM et s'ajoute implicitement comme destination d'interruption pour que l'instance reçoive ses interruptions ou événements.

Les événements représentent des occurrences d'événements ou d'erreurs sur une instance ADC gérée.

Gestion des certificats

Citrix ADM simplifie désormais tous les aspects de la gestion des certificats pour vous. Grâce à une console unique, vous pouvez établir des stratégies automatisées pour garantir l'émetteur, la force de clé et les algorithmes corrects, tout en gardant un œil étroit sur les certificats inutilisés ou bientôt expirés. Pour commencer à utiliser le tableau de bord SSL d'ADM et ses fonctionnalités, vous devez comprendre ce qu'est un certificat SSL et comment utiliser ADM pour suivre vos certificats SSL.

Gestion de la configuration

Citrix ADM vous permet de créer des tâches de configuration qui vous aident à effectuer des tâches de configuration, telles que la création d'entités, la configuration de fonctionnalités, la réplication des modifications de configuration, les mises à niveau du système et d'autres activités de maintenance en toute simplicité sur plusieurs instances. Les tâches et les modèles de configuration simplifient les tâches administratives les plus répétitives en une seule tâche sur ADM.

Audit de configuration

Permet de surveiller et d'identifier les anomalies dans les configurations de vos instances.

- Conseil de configuration : permet d'identifier les anomalies de configuration.
- Modèle d'audit : permet de surveiller les modifications dans une configuration spécifique.

Rapports sur le réseau

Vous pouvez optimiser l'utilisation des ressources en surveillant les rapports de votre réseau sur ADM.

Analytics

Web Insight

Fournit une visibilité sur les applications Web d'entreprise et permet aux administrateurs informatiques de surveiller toutes les applications Web desservies par Citrix ADC en fournissant une surveillance intégrée et en temps réel des applications. Web Insight fournit des informations critiques telles que le temps de réponse des utilisateurs et des serveurs, ce qui permet aux entreprises informatiques de surveiller et d'améliorer les performances des applications.

HDX Insight

Fournit une visibilité de bout en bout sur le trafic ICA transitant par Citrix ADC. HDX Insight permet aux administrateurs d'afficher en temps réel les mesures de latence des clients et du réseau, les rapports historiques, les données de performance de bout en bout et de résoudre les problèmes de performances.

Gateway Insight

Fournit une visibilité sur les échecs rencontrés par les utilisateurs lors de la connexion, quel que soit le mode d'accès. Vous pouvez afficher la liste des utilisateurs connectés à un moment donné, ainsi que le nombre d'utilisateurs actifs, le nombre de sessions actives, ainsi que les octets et licences utilisés par tous les utilisateurs à un moment donné.

Security Insight

Fournit une solution à volet unique pour vous aider à évaluer l'état de sécurité de vos applications et à prendre des mesures correctives pour sécuriser vos applications.

SSL Insight

SSL Insight fournit une visibilité sur les transactions Web sécurisées (HTTPS) et permet aux administrateurs informatiques de surveiller toutes les applications Web sécurisées desservies par l'Citrix ADC en fournissant une surveillance intégrée et en temps réel et historique des transactions Web sécurisées.

TCP Insight

TCP Insight fournit une solution simple et évolutive pour surveiller les métriques des techniques d'optimisation et des stratégies (ou algorithmes) de contrôle de congestion utilisées dans les instances ADC afin d'éviter la congestion du réseau lors de la transmission de données.

Video Insight

La fonctionnalité Video Insight fournit une solution simple et évolutive pour surveiller les mesures des techniques d'optimisation vidéo utilisées par les instances Citrix ADC afin d'améliorer l'expérience client et l'efficacité opérationnelle.

WAN Insight

L'analyse WAN Insight permet aux administrateurs de surveiller facilement le trafic WAN accéléré et non accéléré qui circule entre les appliances d'optimisation WAN du centre de données et des succursales. WAN Insight offre également une visibilité sur les clients, les applications et les succursales du réseau afin de résoudre efficacement les problèmes réseau.

Orchestration

Orchestration dans le cloud

Permet l'intégration des produits Citrix ADC à l'orchestration cloud d'OpenStack. Citrix ADM et OpenStack implémentent leurs API respectives, ce qui permet d'intégrer la fonctionnalité d'équilibrage de charge (LBaaS) de l'instance Citrix ADC à l'orchestration cloud d'OpenStack.

Orchestration

Citrix ADM prend en charge le SDN dans le réseau d'entreprise en s'intégrant aux contrôleurs SDN de différents fournisseurs. ADM prend en charge VMware NSX Manager et Cisco Application Policy Infrastructure Controller (APIC).

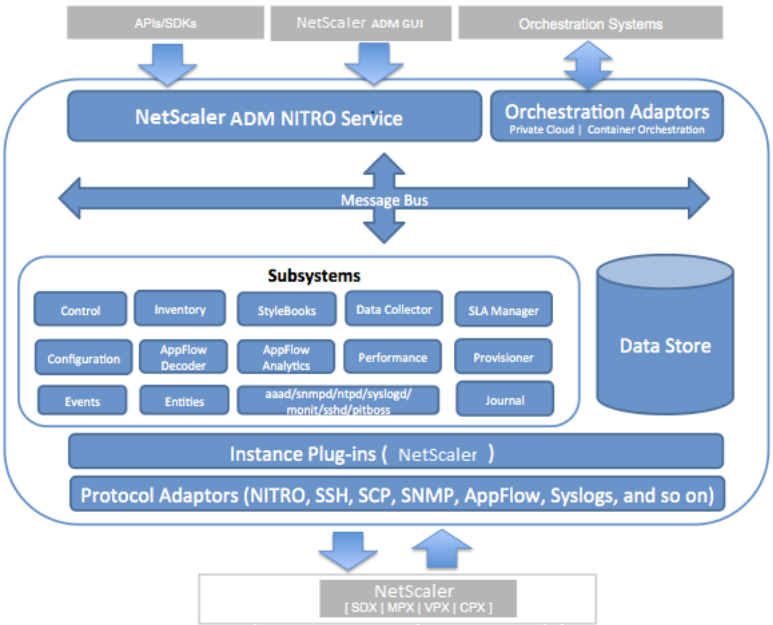
Architecture

February 1, 2024

La base de données Citrix Application Delivery Management (ADM) est intégrée au serveur et le serveur gère tous les processus clés, tels que la collecte de données et les appels NITRO. Dans son magasin de données, le serveur stocke un inventaire des détails d'instance, tels que le nom d'hôte, la version du logiciel, la configuration en cours d'exécution et enregistrée, les détails du certificat, les entités configurées sur l'instance. Un déploiement sur un seul serveur convient si vous souhaitez traiter de petites quantités de trafic ou stocker des données pendant une durée limitée.

Actuellement, ADM prend en charge deux types de déploiements logiciels : un serveur unique et une haute disponibilité.

L'image suivante montre les différents sous-systèmes d'ADM et comment la communication se produit entre le serveur ADM et les instances gérées.



Le sous-système Service d'ADM agit comme un serveur Web qui gère les requêtes HTTP et les réponses envoyées aux sous-systèmes d'ADM à partir de l'interface graphique ou de l'API, à l'aide des ports 80 et 443. Ces demandes sont envoyées aux sous-systèmes via le bus de messages (système de traitement des messages) à l'aide du mécanisme IPC (communication inter-processus). Une demande est

envoyée au sous-système Contrôle, qui traite les informations ou les envoie au sous-système approprié. Chacun des autres sous-systèmes (inventaire, livres de style, collecteur de données, configuration, décodeur AppFlow, Analytics AppFlow, Performances, Events, Entités, Gestionnaire de SLA, Provisioner et Journal) a un rôle spécifique.

Les plug-ins d'instance sont des bibliothèques partagées qui sont uniques à chaque type d'instance pris en charge par ADM. Les informations sont transférées entre ADM et les instances gérées à l'aide d'appels NITRO ou via le protocole SNMP, Secure Shell (SSH) ou Secure Copy (SCP). Ces informations sont ensuite traitées et stockées dans la base de données interne (banque de données).

Comment Citrix ADM découvre des instances

February 1, 2024

Les instances sont des appliances Citrix ou des appliances virtuelles que vous souhaitez découvrir, gérer et surveiller à partir de Citrix Application Delivery Management (ADM). Pour gérer et surveiller ces instances, vous devez les ajouter au serveur Citrix ADM. Vous pouvez ajouter les appliances Citrix et les appliances virtuelles suivantes à ADM :

- Instances Citrix ADC
  - Citrix MPX
  - Citrix VPX
  - Citrix SDX
  - Citrix CPX
  - Citrix BLX
- Instances Citrix Gateway
- Instances Citrix SD-WAN

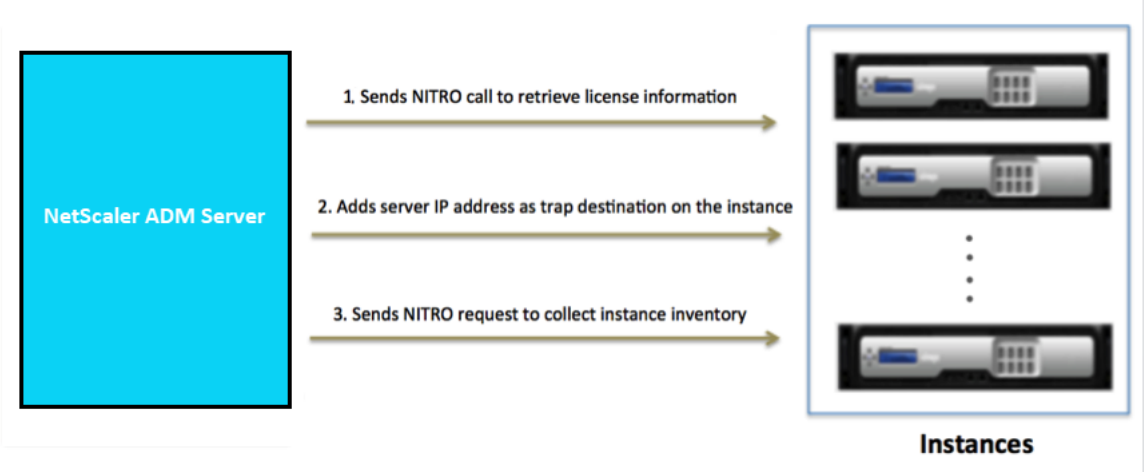
Vous pouvez ajouter des instances lors de la configuration du serveur Citrix ADM pour la première fois ou plus tard.

> **Remarque**
>
> Citrix ADM utilise l'adresse IP Citrix ADC (NSIP) des instances ADC pour la communication. ADM peut également détecter les instances ADC avec une adresse IP de sous-réseau (SNIP) sur laquelle l'accès de gestion est activé. Pour plus d'informations sur les ports qui doivent être ouverts entre les instances ADC et ADM, consultez Ports.
>
> Si vous souhaitez ajouter une paire ADC HA à l'aide de SNIP, veillez à activer le mode INC (In-

> dependent Network Configuration) sur la paire ADC HA. Pour plus d'informations sur l'ajout d'instances, consultez la section Ajouter des instances.
>
> Pour Citrix SD-WAN WO, ADM utilise l'adresse IP de gestion des instances pour la communication.
>
> Vous ne pouvez pas ajouter d'instances Citrix SD-WAN SE/PE dans ADM. Vous pouvez configurer ADM en tant que collecteur AppFlow sur les appliances Citrix SD-WAN SE/PE.

Lorsque vous ajoutez une instance au serveur ADM, le serveur s'ajoute implicitement comme destination d'interruption pour l'instance et recueille l'inventaire de l'instance.

Le diagramme suivant décrit comment ADM découvre et ajoute implicitement des instances.



Comme indiqué dans le diagramme, les étapes suivantes sont exécutées implicitement par Citrix ADM.

1. Citrix ADM utilise les détails du profil d'instance pour ouvrir une session sur l'instance. À l'aide d'un appel ADC NITRO, ADM récupère les informations de licence de l'instance. Sur la base des informations de licence, il détermine si l'instance est une instance ADC et le type de plate-forme ADC (par exemple, Citrix ADC MPX, ADC VPX, ADC SDX, ADC BLX ou Citrix Gateway). Lors de la détection réussie de l'instance, elle est ajoutée à la base de données d'ADM.

   Pour les instances WO Citrix SD-WAN, ADM ne détecte pas l'instance à l'aide des informations de licence. Il envoie une requête NITRO à l'instance pour vérifier le type et la version de l'instance.

   Cette étape peut échouer si le profil d'instance n'inclut pas les informations d'identification correctes. Pour les instances ADC MPX, ADC VPX, ADC SDX, ADC BLX et Citrix Gateway, cette étape peut également échouer si les licences ne sont pas appliquées à l'instance.

   > **Remarque**
   >
   > À l'aide du protocole HTTP, vous pouvez ajouter toutes les instances à ADM même si les licences ne sont pas configurées sur les instances.

2. ADM ajoute son adresse IP à la liste des destinations d'interruptions de l'instance. Cela permet à ADM de recevoir des interruptions générées sur l'instance ADC.

   Cette étape peut échouer si le nombre de destinations d'interruptions sur l'instance dépasse la limite maximale de destinations d'interruptions. La limite maximale d'instances est de 20.

   Pour les instances WO Citrix SD-WAN, ADM ajoute son adresse IP en tant que gestionnaire SNMP sur l'instance.

3. ADM collecte l'inventaire de l'instance en envoyant une demande NITRO. Il recueille des détails d'instance tels que le nom d'hôte, la version du logiciel, la configuration en cours d'exécution et enregistrée, les détails du certificat, les entités configurées sur l'instance.

   Cette étape peut échouer en raison de problèmes de réseau ou de pare-feu.

   Pour savoir comment ajouter des instances à ADM, consultez la section Ajouter des instances.

Vue d'ensemble de l'interrogation

February 1, 2024

L'interrogation est un processus dans le cadre duquel Citrix Application Delivery Management (ADM) collecte certaines informations à partir d'instances de Citrix ADC. Vous avez peut-être configuré plusieurs instances Citrix ADC pour votre organisation, dans le monde entier. Pour surveiller vos instances via Citrix ADM, Citrix ADM doit collecter certaines informations telles que l'utilisation du processeur, l'utilisation de la mémoire, les certificats SSL, les fonctionnalités sous licence, les types de licence, etc. à partir de toutes les instances ADC gérées. Voici les différents types d'interrogation qui se produisent entre ADM et les instances gérées :

- Sondage d'instance
- Interprétation d'inventaire
- Collecte de données de performance
- Sondage de sauvegarde d'instance
- Sondage d'audit de configuration
- Interrogation de certificats SSL
- Sondage des entités

Citrix ADM utilise des protocoles tels que NITRO call, Secure Shell (SSH) et Secure Copy (SCP) pour interroger les informations des instances Citrix ADC.

Procédure d'interrogation par Citrix ADM des instances et des entités gérées

Citrix ADM interroge automatiquement à intervalles réguliers par défaut. Citrix ADM vous permet également de configurer les intervalles d'interrogation pour certains types de sondages et vous permet de sonder manuellement si nécessaire.

Le tableau suivant décrit les détails des types d'interrogation, de l'intervalle d'interrogation, du protocole utilisé, etc. :

Type de sondage	Intervalle d'interrogation	Informations sondées	Protocole utilisé	Configuration des intervalles d'interrogation
Sondage d'instance	Toutes les 5 minutes (par défaut)	Informations statistiques telles que l'état, les requêtes HTTP par seconde, l'utilisation du processeur, l'utilisation de la mémoire et le débit.	Appel NITRO.	Non
Interprétation d'inventaire	Toutes les 60 minutes (par défaut)	Détails de l'inventaire tels que la version de construction, les informations système, les fonctionnalités sous licence et les modes.	Appels NITRO et SSH	Non
Collecte de données de performance	Toutes les 5 minutes (par défaut)	Informations de reporting du réseau	Appel NITRO	Non

Type de sondage	Intervalle d'interrogation	Informations sondées	Protocole utilisé	Configuration des intervalles d'interrogation
Sondage de sauvegarde d'instance	Toutes les 12 heures (par défaut)	Fichier de sauvegarde de l'état actuel des instances ADC gérées	Appels NITRO, SSH et SCP.	Oui. Accédez à **Réseaux** > **Instances** > **Citrix ADC**. Sélectionnez l'instance et dans la liste **Sélectionner une action**, cliquez sur **Sauvegarde/Restaurer** .
Sondage d'audit de configuration	Toutes les 10 heures (par défaut)	Changements de configuration qui se produisent sur les instances ADC (par exemple, configuration en cours d'exécution ou configuration enregistrée)	Appel SSH, SCP et NITRO	Oui. Accédez à **Réseaux** > **Audit de configuration**. Dans la page Audit de configuration, cliquez sur **Paramètres** et configurez l'intervalle d'interrogation pour l'interrogation d'audit de configuration.

Type de sondage	Intervalle d'interrogation	Informations sondées	Protocole utilisé	Configuration des intervalles d'interrogation
				Vous pouvez interroger manuellement les audits de configuration et ajouter immédiatement tous les audits de configuration des instances à Citrix ADM. Pour ce faire, accédez à **Réseaux** > **Audit de configuration** et cliquez sur **Interroger maintenant**. La page **Interroger maintenant** vous permet d'interroger toutes les instances ou certaines du réseau.
interrogation de certificats SSL	Toutes les 24 heures (par défaut)	Certificats SSL installés sur les instances Citrix ADC.	Appels NITRO et SCP	Oui. Accédez à **Réseaux** > **Tableau de bord SSL**. Sur la page Tableau de bord SSL, cliquez sur **Paramètres** pour configurer l'intervalle d'interrogation

Type de sondage	Intervalle d'interrogation	Informations sondées	Protocole utilisé	Configuration des intervalles d'interrogation
				Vous pouvez interroger manuellement les certificats SSL et ajouter immédiatement tous les certificats des instances à Citrix ADM. Pour ce faire, accédez à **Réseaux** > Tableau de **bord SSL** et cliquez sur **Interroger maintenant**. La page **Interroger maintenant** vous permet d'interroger toutes les instances ou certaines du réseau.

Type de sondage	Intervalle d'interrogation	Informations sondées	Protocole utilisé	Configuration des intervalles d'interrogation
Sondage des entités	Toutes les 60 minutes (par défaut)	Toutes les entités configurées sur les instances. Une entité est une stratégie, un serveur virtuel, un service ou une action attachée à une instance ADC. Pour activer l'interrogation des entités, reportez-vous à la section Activer ou désactiver les fonctionnalités ADM.	NITRO appelle.	Oui, mais ne peut pas être réglé sur moins de 10 minutes. Pour configurer, accédez à **Réseaux** > **Fonctions réseau**. Dans la page Fonction réseaux, cliquez sur **Paramètres** pour configurer l'intervalle d'interrogation.

Type de sondage	Intervalle d'interrogation	Informations sondées	Protocole utilisé	Configuration des intervalles d'interrogation
				Vous pouvez interroger les entités manuellement et ajouter immédiatement toutes les entités des instances à Citrix ADM. Pour ce faire, accédez à **Réseaux** > **Fonctions réseau**, puis cliquez sur **Interroger maintenant**. La page **Sondage maintenant** vous permet d'interroger toutes les instances ou les instances sélectionnées du réseau

Remarque

En plus de l'interrogation, les événements générés par les instances ADC gérées sont reçus par Citrix ADM via des interruptions SNMP envoyées aux instances. Par exemple, un événement est généré en cas de défaillance du système ou de modification de la configuration.

Lors de la sauvegarde de l'instance, les fichiers SSL, les fichiers de certificat CA, les modèles ADC, les informations de base de données, etc. sont téléchargés sur Citrix ADM. Lors d'un audit de configuration, les fichiers ns.conf sont téléchargés et stockés dans le système de fichiers. Toutes les informations collectées à partir des instances Citrix ADC gérées sont stockées en interne dans la base de données.

Différentes manières de sonder les instances

Voici les différentes méthodes d'interrogation que Citrix ADM effectue sur les instances gérées :

- Sondage mondial des instances
- interrogation manuelle des instances
- Interrogation manuelle des entités

Sondage mondial des instances

Citrix ADM interroge automatiquement toutes les instances gérées du réseau en fonction de l'intervalle que vous avez configuré. Bien que l'intervalle d'interrogation par défaut soit de 30 minutes, vous pouvez le définir en fonction de vos besoins en accédant à **Réseaux** > **Fonctions réseau** > **Paramètres**.

Interrogation manuelle des instances

Lorsque Citrix ADM gère de nombreuses entités, le cycle d'interrogation prend plus de temps pour générer le rapport, ce qui peut entraîner l'affichage d'un écran vide ou le système peut toujours afficher des données antérieures.

Dans Citrix ADM, il existe une période d'intervalle d'interrogation minimale lorsque l'interrogation automatique ne se produit pas. Si vous ajoutez une nouvelle instance Citrix ADC ou si une entité est mise à jour, Citrix ADM ne reconnaît pas la nouvelle instance ou les mises à jour apportées à une entité avant la prochaine interrogation. De plus, il n'est pas possible d'obtenir immédiatement une liste d'adresses IP virtuelles pour des opérations ultérieures. Vous devez attendre que la période minimale d'interrogation s'écoule. Bien que vous puissiez effectuer un sondage manuel pour découvrir les instances récemment ajoutées, cela entraîne l'interrogation de l'ensemble du réseau Citrix ADC, ce qui crée une charge importante sur le réseau. Au lieu d'interroger l'ensemble du réseau, Citrix ADM vous permet désormais d'interroger uniquement les instances et entités sélectionnées à un moment donné.

Citrix ADM interroge automatiquement les instances gérées pour collecter des informations à des heures définies dans la journée. L'interrogation sélectionnée réduit le temps d'actualisation dont Citrix ADM a besoin pour afficher l'état le plus récent des entités liées à ces instances sélectionnées.

Pour interroger des instances spécifiques dans Citrix ADM :

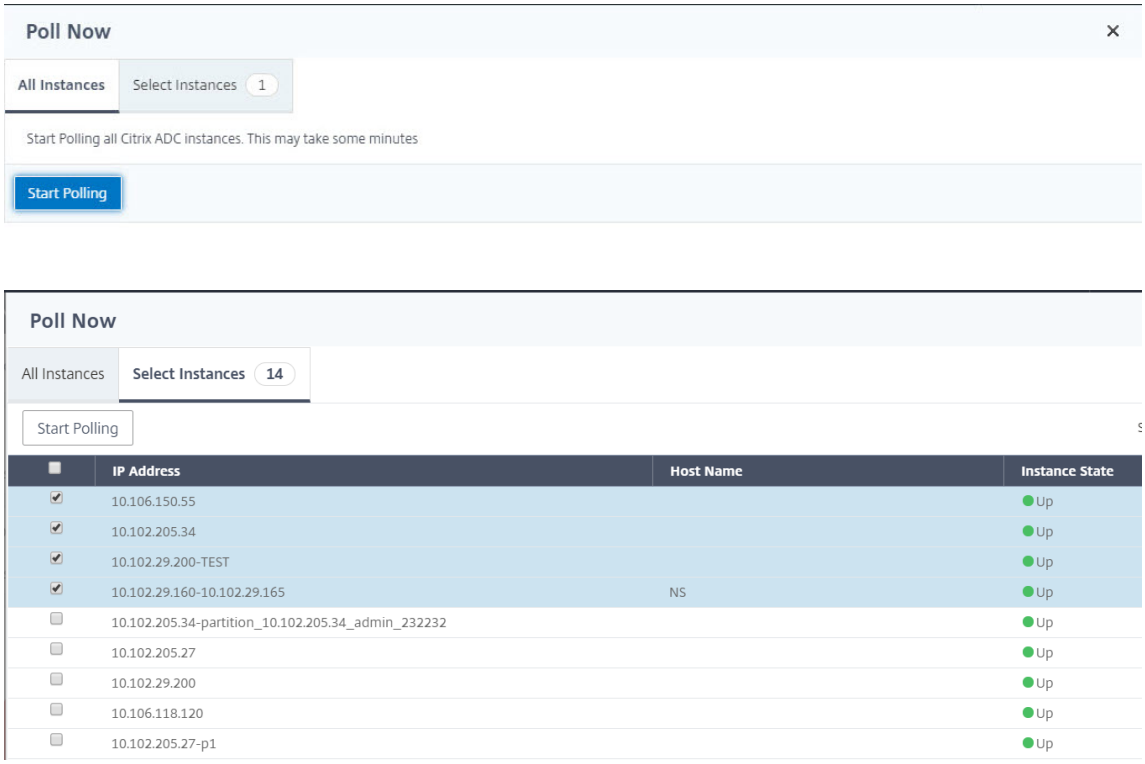
1. Dans Citrix ADM, accédez à **Réseaux** > **Fonctions réseau**.
2. Sur la page **Fonctions réseau**, en haut à droite, cliquez sur **Sondage maintenant** .

3. La page contextuelle **Interroger maintenant** vous offre une option pour interroger toutes les instances Citrix ADC du réseau ou interroger les instances sélectionnées.

   a) Onglet**Toutes les instances** : cliquez sur **Commencer le sondage** pour interroger toutes les instances.

   b) Onglet**Sélectionner les instances** - sélectionnez les instances dans la liste

4. Cliquez sur **Démarrer l'interrogation**.



Citrix ADM lance l'interrogation manuelle et ajoute toutes les entités.

Interrogation manuelle des entités

Citrix ADM vous permet également d'interroger uniquement quelques entités sélectionnées liées à une instance particulière. Par exemple, vous pouvez utiliser cette option pour connaître le dernier statut d'une entité particulière dans une instance. Dans un tel cas, vous n'avez pas besoin d'interroger l'instance dans son ensemble pour connaître l'état d'une entité mise à jour. Lorsque vous sélectionnez et interroger une entité, Citrix ADM interroge uniquement cette entité et met à jour l'état dans l'interface graphique Citrix ADM.

Prenons l'exemple d'un serveur virtuel en panne . L'état de ce serveur virtuel est peut-être passé à UP avant le prochain sondage automatique. Pour afficher l'état modifié du serveur virtuel, vous pouvez

demander uniquement à ce serveur virtuel afin que l'état correct soit immédiatement affiché sur l'interface graphique.

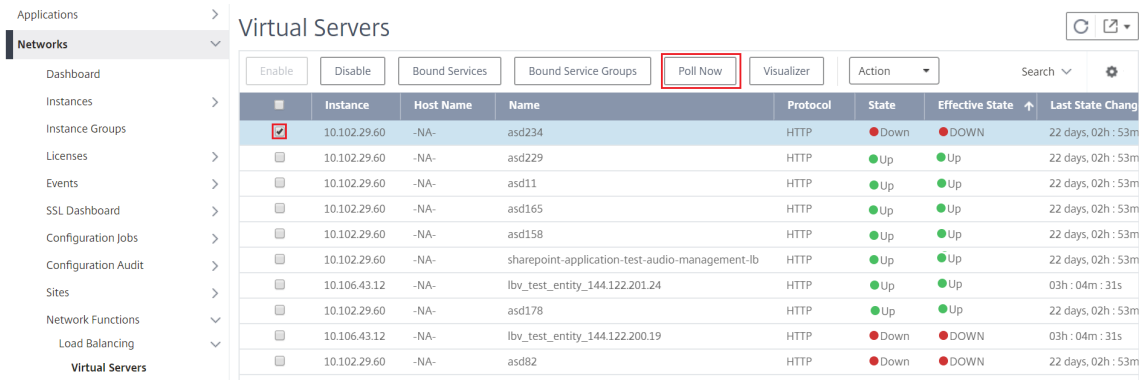
Vous pouvez désormais interroger les entités suivantes pour connaître toute mise à jour de leur statut : services, groupes de services, serveurs virtuels d'équilibrage de charge, serveurs virtuels de réduction de cache, serveurs virtuels de commutation de contenu, serveurs virtuels d'authentification, serveurs virtuels VPN, serveurs virtuels GSLB et serveurs d'applications.

> **Remarque**
>
> Si vous interrogez un serveur virtuel, seul ce serveur virtuel est interrogé. Les entités associées telles que les services, les groupes de services et les serveurs ne sont pas interrogées. Si vous devez interroger toutes les entités associées, vous devez interroger les entités manuellement ou vous devez interroger l'instance.

Pour interroger des entités spécifiques dans Citrix ADM :

Par exemple, cette tâche vous aide à interroger les serveurs virtuels d'équilibrage de charge. De même, vous pouvez interroger d'autres entités de fonction réseau aussi.

1. Dans Citrix ADM, accédez à**Réseaux**>**Fonctions réseau** > **Équilibrage de charge > Serveursvirtuels**.
2. Sélectionnez le serveur virtuel qui affiche l'état DOWN, puis cliquez sur **Interroger maintenant**. L'état du serveur virtuel passe désormais à UP .



Gouvernance des données

February 1, 2024

Citrix collecte des statistiques sur vos déploiements Citrix Application Delivery Management (ADM) afin de comprendre l'utilisation et l'échelle du déploiement. Les statistiques incluent l'état, l'état et le modèle d'utilisation du déploiement d'ADM dans vos locaux. Les statistiques aident Citrix à résoudre de manière proactive les problèmes liés à votre déploiement ADM.

- **Créez une identité client sur Citrix Cloud** : pour envoyer des statistiques importantes sur l'état et l'état d'ADM, ainsi que d'autres indicateurs du déploiement local d'ADM vers un compte Citrix Cloud.

  Après avoir créé une identité client, le « Cloud Connect » établit la connexion entre ADM sur site et le service ADM en créant un compte Citrix Cloud. Consultez la section Configurer l'identité du client.

- **Configurer les scripts de maintenance** - Pour optimiser la base de données. L'optimisation de la base de données peut créer des tables, modifier des colonnes, etc. La même fonctionnalité « Cloud Connect » est utilisée pour configurer les scripts de maintenance. Consultez la section Optimisation de la base dedonnées à

- **Programme d'amélioration de l'expérience utilisateur client (CUXIP)** - Ce programme est activé par défaut. Il collecte les données d'utilisation auprès de Citrix ADM. Ces données permettent d'optimiser l'expérience d'ADM grâce à des workflows guidés, des articles de recherche, des notifications sur les produits, des commentaires, des sondages, etc. Reportez-vous à la section Programme d'amélioration de l'expérience utilisateur.

Configurer l'identité du client

Citrix Application Delivery Management (ADM) nécessite que vous vous authentifiiez sur l'interface graphique d'ADM avant de commencer à accéder aux informations. Vous devez vous inscrire sur les services Citrix Cloud avant de vous authentifier sur ADM. Fournissez les informations d'identification de l'utilisateur Citrix Cloud sur l'interface graphique ADM. Pour de plus amples informations, consultez la section S'inscrire à Citrix Cloud.

Il existe différentes façons de vous authentifier sur Citrix ADM. Les sections suivantes décrivent les workflows si vous êtes un nouvel utilisateur ou un utilisateur existant sur ADM.

Workflow 1 - Si vous êtes un nouvel utilisateur

1. Terminez l'installation de Citrix ADM sur l'Hypervisor sélectionné.
2. Configurez les différentes adresses IP requises.
3. Dans un navigateur Web, tapez l'adresse IP de Citrix ADM.
4. Dans les champs **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.

   La page **Configurer l'identité du client** s'ouvre dans laquelle vous devez vous identifier à l'aide de vos informations d'identification Citrix Cloud.

   Si vous n'avez pas créé de compte sur Citrix Cloud, cliquez sur Citrix Cloud pour vous inscrire.

5. Cliquez sur **Authentifier** et indiquez votre adresse e-mail que vous avez utilisée pour vous inscrire sur Citrix Cloud.
6. **Cochez la case à côté de**J'accepte de partager des données**pour la télémétrie et cliquez sur Soumettre.**

Workflow 2 : si vous êtes un utilisateur existant qui effectue une mise à niveau vers la dernière version d'ADM

1. Après avoir mis à niveau le Citrix ADM vers la dernière version, dans un navigateur Web, tapez l'adresse IP du Citrix ADM.
2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.
3. La page **Configurer l'identité du client** s'ouvre dans laquelle vous devez vous identifier à l'aide de vos informations d'identification Citrix Cloud.

   Si vous n'avez pas créé de compte sur Citrix Cloud, cliquez sur Citrix Cloud pour vous inscrire.
4. Cliquez sur **Authentifier** et indiquez votre adresse e-mail que vous avez utilisée pour vous inscrire sur Citrix Cloud.
5. Activez la case à cocher à côté de « J'accepte de partager des données pour la télémétrie » et cliquez sur Soumettre.

En tant qu'utilisateur existant, vous pouvez également configurer votre identité sur ADM ultérieurement de l'une des deux manières suivantes :

- Accédez à **Système > Administration du système**, puis cliquez sur **Authentification**.
- Cliquez sur le symbole du cloud en haut à droite de l'interface graphique ADM.
  Une fois l'authentification réussie, la coche X se transforme en une coche de couleur verte.

> **Remarque**
>
> Assurez-vous que les domaines suivants sont en liste blanche :
>
> - `*.citrixnetworkapi.net`
> - `*.blob.core.windows.net`

En téléchargeant vos données sur Citrix ADM et en utilisant les fonctionnalités Citrix ADM, vous acceptez et consentez à ce que Citrix puisse collecter, stocker, transmettre, maintenir, traiter et utiliser des informations techniques, utilisateur ou connexes sur vos produits et services Citrix.

Les informations reçues par Citrix sont toujours traitées conformément à la stratégie de confidentialité de Citrix.com.

Diagnostic et collecte de données

Citrix ADM collecte les données télémétriques suivantes à l'aide de l'identité du client :

- **Actions effectuées dans ADM** :
  - Actions effectuées à l'aide de l'interface UI/API Citrix ADM.
  - Actions effectuées à l'aide de l'interface du SDK Citrix ADM.
  - Nombre d'opérations en une seule journée. Ce décompte inclut toutes les requêtes non GET provenant de l'API ou de l'interface utilisateur.
  - Nombre de mises à niveau de ADC effectuées par ADM.
- **Informations sur la licence Citrix ADM** : nombre de serveurs virtuels autorisés.
- **Statistiques clés** :
  - Nombre total de règles de l'événement.
  - Nombre total de livres de style définis par l'utilisateur et définis par l'utilisateur.
  - Nombre d'applications gérées et personnalisées.
  - Nombre d'agents enregistrés.
  - Débit global sur le Citrix ADC (Rx+Tx).
  - Nombre d'instances gérées. Ce nombre inclut également les partitions d'administration.
  - Nombre d'administrateurs utilisant Citrix ADM SaaS.
- **Géolocalisation de Citrix ADM**
- **Informations de déploiement** : ces informations incluent les types de déploiement tels que la haute disponibilité, la reprise après sinistre et les agents ADM.

Pourquoi les données sont-elles collectées ?

Les données de télémétrie collectées permettent de :

- Recommandez un dimensionnement et un déploiement corrects de Citrix ADM.
- Résoudre de manière proactive les problèmes liés aux déploiements sur site ADM.

Qui peut utiliser ces données ?

Citrix est l'unique propriétaire des informations collectées. Citrix a accès/collecte les informations que vous nous fournissez volontairement. Nous ne vendons ni ne louons ces informations à personne. Nous ne partageons pas vos informations avec des tiers extérieurs à notre organisation, sauf si cela est nécessaire pour répondre à votre demande. Exemple : pour expédier une commande ou pour résoudre des problèmes de manière proactive.

Combien de temps conservons-nous vos données ?

En règle générale, nous conservons les données personnelles/d'utilisation jusqu'à ce que l'utilisateur utilise nos services. Ou bien, nous avons un autre objectif à atteindre. Par la suite, les données ne sont pas conservées plus longtemps que ce qui est requis ou autorisé par la loi ou nécessaire à des fins de reporting interne et de rapprochement.

Toutes les données de télémétrie sont stockées pendant une période n'excédant pas 13 mois ou 396 jours.

Optimisation des bases de données à l'aide de scripts

Les scripts de maintenance sont utilisés pour résoudre les problèmes liés à la base de données lors des déploiements ADM locaux. Le logiciel ADM télécharge automatiquement les scripts de maintenance de base de données à partir du service ADM, ce qui permet de résoudre plus rapidement les problèmes liés à la base de données. Auparavant, ces problèmes ont été résolus en exécutant manuellement les scripts.

Avec cette fonctionnalité, le déploiement sur site d'ADM télécharge périodiquement les scripts de maintenance de base de données à partir du service ADM. Pour ce faire, veillez à configurer l'identité du client.

Les scripts de maintenance s'exécutent quotidiennement et chaque semaine. En outre, les scripts peuvent créer des tables ou ajouter ou supprimer des colonnes pour améliorer les performances de la base de données.

Programme d'amélioration de l'expérience utilisateur client

Chez Citrix Systems, notre objectif est de fournir à nos utilisateurs une expérience produit attrayante. Le**programme d'amélioration de l'expérience utilisateur (CUXIP)** utilise Pendo pour guider les utilisateurs dans certaines tâches courantes mais détaillées en leur fournissant des articles de recherche, des guides intégrés à l'application, etc. Nous aidons également nos utilisateurs à rester au courant de toutes les annonces récentes.

Quelles données d'utilisation sont collectées via CUXIP ?

Les données d'utilisation concernent uniquement les actions des utilisateurs. Également appelées données au niveau des événements, les données d'utilisation incluent tout, des pages que les utilisateurs consultent sur un site Web au nombre de clics sur une fonctionnalité donnée. Les données d'utilisation sont des informations précieuses sur la façon dont les utilisateurs se déplacent dans nos applications. Ces données permettent d'optimiser l'expérience de nos utilisateurs.

Voici quelques-unes des données d'utilisation que nous collectons :

- Détails des pages vues, du temps passé sur chaque page.
- L'identifiant visiteur est un identifiant anonyme unique qui permet d'identifier le nombre de visiteurs uniques sur une page.
- Statistiques de l'enquête : score, vues, nombre de soumissions, etc.

Comment CUXIP vous aide ?

Nous utilisons les données d'utilisation pour améliorer votre expérience avec ADM. Voici quelques-unes des manières dont nous avons l'intention d'améliorer l'expérience utilisateur des clients :

- Flux de travail guidés intégrés à l'application et possibilité de rechercher des articles pertinents.
- Participez à une enquête depuis l'application pour améliorer le produit.
- Restez au courant des dernières annonces et autres notifications.
- Postez une question ou un commentaire à l'équipe produit.

Comment fonctionne CUXIP ?

L'appliance Citrix ADM peut se trouver dans le réseau interne. Le navigateur doit avoir une connectivité Internet pour bénéficier des avantages de l'assistance guidée sur CUXIP.

Comment puis-je désactiver CUXIP sur mon ADM ?

Pour désactiver CUXIP, procédez comme suit dans l'interface graphique d'ADM :

1. Accédez à **Système > Administration du système** .
2. Dans **Paramètres CUXIP**, puis désactivez CUXIP.

Modifications apportées à notre Stratégie de confidentialité

Nous pouvons mettre à jour notre Stratégie de confidentialité de temps à autre. Nous vous informerons des modifications en publiant la nouvelle Stratégie de confidentialité sur cette page. Nous vous en informerons par e-mail et/ou par un avis bien visible sur notre Service, avant que la modification n'entre en vigueur et mettrons à jour la « date d'entrée en vigueur » en haut de cette Stratégie de confidentialité.

Nous vous conseillons de consulter périodiquement la présente Stratégie de confidentialité pour tout changement. Les modifications apportées à cette stratégie de confidentialité entrent en vigueur lorsqu'elles sont publiées sur la page de stratégie de confidentialité Citrix .

Références

Stratégie de confidentialité Citrix : https://www.citrix.com/about/legal/privacy/

Licences

February 1, 2024

Citrix Application Delivery Management (ADM) nécessite une licence Citrix ADC vérifiée pour gérer et surveiller les instances Citrix ADC, lorsque les instances sont découvertes via le protocole `https`.

Vous pouvez gérer et surveiller n'importe quel nombre d'instances et d'entités sans licence. Toutefois, vous ne pouvez gérer que 30 applications découvertes sur l'App Dashboard et afficher les données d'analyse de 30 serveurs virtuels sans demander de licence. Au-delà de 30 applications découvertes ou de 30 serveurs virtuels, vous devez acheter et appliquer une licence.

	Fonctionnalités de Citrix ADM	[**GRATUIT**] La licence Citrix ADM n'est pas requise quel que soit le nombre de serveurs virtuels	La licence Citrix ADM est requise pour plus de 30 serveurs virtuels	Exigence de licence Citrix ADC
Analytics	Web Insight	Non	Oui	Sans objet
	HDX Insight*	Non	Oui	Avancé (reporting < 1 heure) Premium (reporting = illimité)
	Security Insight	Non	Oui	Licence Premium (ou) Advanced avec App Firewall
	SSL Insight	Non	Oui	Sans objet
	Gateway Insight	Non	Oui	Avancé (reporting < 1 heure) Premium (reporting = illimité)
	TCP Insight	Non	Oui	Sans objet

	Fonctionnalités de Citrix ADM	[**GRATUIT**] La licence Citrix ADM n'est pas requise quel que soit le nombre de serveurs virtuels	La licence Citrix ADM est requise pour plus de 30 serveurs virtuels	Exigence de licence Citrix ADC
	Video Insight	Non	Oui	Premium (série Citrix-T 1000, VPX-T)
	WAN Insight	Non	Sans objet	Utiliser l'édition d'optimisation des instances Citrix SD-WAN (WANOP)
Applications				
	Statistiques des applications (Tableau de bord de l'application, Tableau de bord de la sécurité de l'application)	Non	Oui	Les informations relatives au Web App Firewall Citrix ADC sur le tableau de bord de l'application et le tableau de bord de sécurité de l'application nécessitent une licence Premium (ou) Advanced with App Firewall.
	StyleBooks	Oui	Non	Sans objet
Réseaux				
	Serveur de licences	Oui	Non	Sans objet

	Fonctionnalités de Citrix ADM	[**GRATUIT**] La licence Citrix ADM n'est pas requise quel que soit le nombre de serveurs virtuels	La licence Citrix ADM est requise pour plus de 30 serveurs virtuels	Exigence de licence Citrix ADC
	Gestion de l'inventaire : tableau de bord de l'infrastructure, groupes d'instances, tableau de bord des instances et sites	Oui	Non	Sans objet
	Gestion des événements et Syslog	Oui	Non	Sans objet
	Tâches de configuration, audit de configuration et conseils de configuration	Oui	Non	Sans objet
	Rapports réseau (au niveau de l'instance)	Oui	Non	Sans objet
	Rapports réseau (au niveau du serveur virtuel)	Oui	Non	Sans objet
	Fonctions réseau (visibilité et gestion des serveurs virtuels, des services, des groupes de services, des serveurs)	Oui	Non	Sans objet

	Fonctionnalités de Citrix ADM	[**GRATUIT**] La licence Citrix ADM n'est pas requise quel que soit le nombre de serveurs virtuels	La licence Citrix ADM est requise pour plus de 30 serveurs virtuels	Exigence de licence Citrix ADC
	Gestion, surveillance et tableau de bord des certificats SSL (au niveau de l'instance)	Oui	Non	Sans objet
	Tableau de bord des certificats SSL (au niveau du serveur virtuel)	Oui	Non	Sans objet
System				
	Authentification RBAC et externe (niveau d' instance)	Oui	Non	Sans objet
	RBAC et authentification externe	Oui	Non	Sans objet
Orchestration				
	Intégration à OpenStack	Oui	Non	Sans objet
	Intégration à VMware NSX	Oui	Non	Sans objet
	Intégration Cisco APIC	Oui	Non	Sans objet
	Intégration de conteneurs	Oui	Non	Sans objet
Équilibreurs de charge tiers				

	Fonctionnalités de Citrix ADM	[**GRATUIT**] La licence Citrix ADM n'est pas requise quel que soit le nombre de serveurs virtuels	La licence Citrix ADM est requise pour plus de 30 serveurs virtuels	Exigence de licence Citrix ADC
	HAProxy : visibilité sur l'hôte/l'instance/le backend/les serveurs/le front end, configuration du téléchargement ou du chargement et redémarrage de l'appliance.	Oui	Non	Sans objet
	Tableau de bord des applications	Non	Oui (nécessite une licence distincte)	Sans objet

*Pour l'intégration de Citrix Director avec la prise en charge Citrix ADM, Citrix Director doit disposer d'une licence Premium.

Les licences pour plus de serveurs virtuels sont disponibles dans des packs de serveurs virtuels de 10. Vous pouvez obtenir une licence valide et ajouter les licences sur les serveurs Citrix ADM via l'interface graphique Citrix ADM.

Haute disponibilité

Le serveur Citrix ADM peut contenir des licences VIP, CICO et de capacité groupée. Lorsque les licences sont émises à un serveur ADM, les licences sont liées à l'ID hôte du serveur. De plus, l'attribution de licences à un autre serveur ADM est restreinte.

Si vous configurez une paire ADM haute disponibilité en tant que serveur de licences, les serveurs principal et secondaire doivent avoir les mêmes fichiers de licence. Par conséquent, dans le déploiement ADM haute disponibilité, Citrix ADM prend en charge vous attribuer les mêmes fichiers de licence aux deux serveurs.

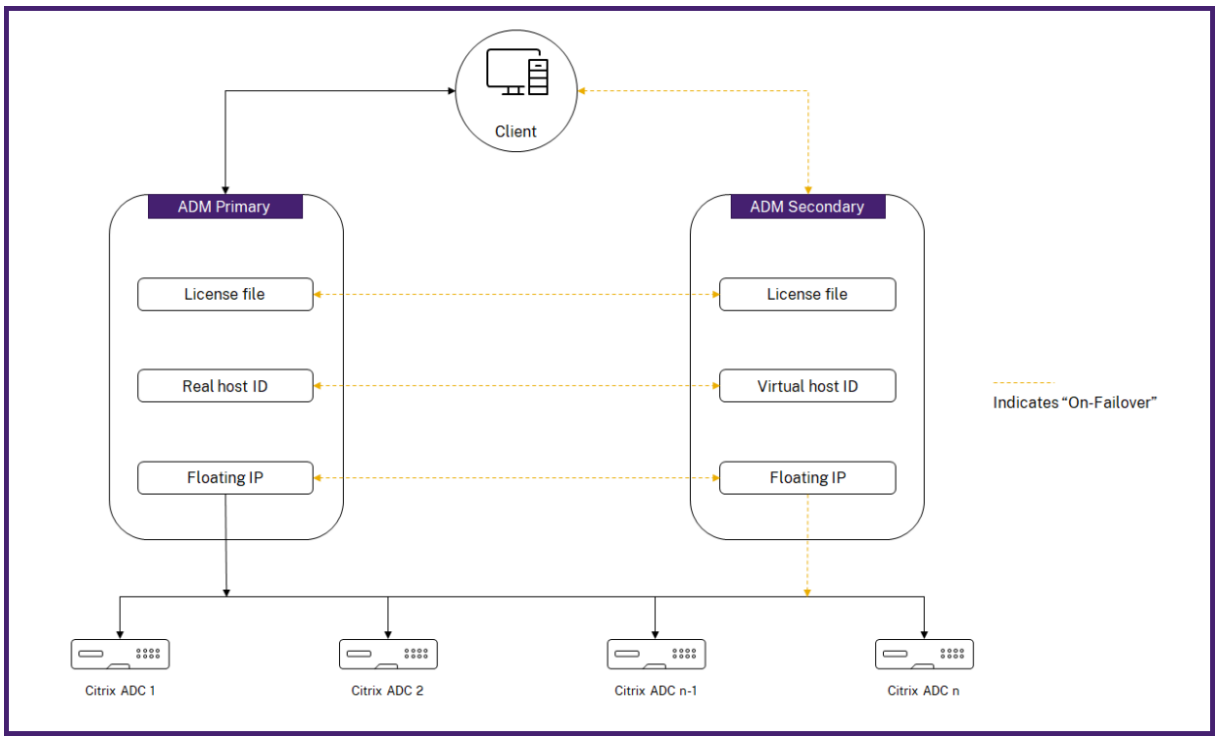
Remarque

- Si vous avez installé Citrix ADM 12.1.49.x ou des versions antérieures, vous bénéficiez d'un délai de grâce de 30 jours pour conserver les licences sur le nœud secondaire. Après le délai de grâce, vous devez contacter Citrix pour réhéberger la licence d'origine.
- Pour les versions 12.1.50.x ou ultérieures, la licence Citrix ADM est automatiquement synchronisée avec le nœud secondaire.
- Les licences regroupées sont automatiquement synchronisées avec le nœud secondaire à partir de la version 12.1.50.x ou ultérieure.

Comment les licences sont-elles synchronisées entre les nœuds haute disponibilité ADM ?

Chaque fois qu'un basculement se produit, le serveur secondaire assume le rôle du serveur principal. L'ID d'hôte réel du serveur principal est configuré comme ID d'hôte virtuel du nouveau serveur principal. Les fichiers de licence reconnaissent le nouveau serveur principal à l'aide de l'ID d'hôte virtuel.

- **ID d'hôte réel** - Cet ID est généré à partir d'une adresse MAC du serveur ADM. Chaque déploiement autonome ADM possède un ID d'hôte unique.
- **ID d'hôte virtuel** - Cet ID est généré automatiquement pendant le déploiement HA. L'ID d'hôte réel d'un serveur principal ADM est utilisé comme ID d'hôte virtuel d'un serveur secondaire. Cet ID est stocké dans la base de données ADM sous un format crypté et les modifications apportées à cet ID sont restreintes. L'ID d'hôte virtuel est préféré au véritable ID d'hôte.



Supposons que Node-1 est le serveur principal et Node-2 est le serveur secondaire. L'ID d'hôte virtuel de Node-1 est synchronisé avec Node-2.

1. Les fichiers de licence disponibles dans Node-1 sont synchronisés avec Node-2.
2. Tous les nouveaux fichiers de licence sur Node-1 sont synchronisés périodiquement sur Node-2.
3. ADM s'assure que le serveur de licences s'exécute uniquement sur Node-1 afin d'éviter le doublement de la capacité de licence.
4. Les instances Citrix ADC extraient les licences de Node-1 à l'aide de l'adresse IP flottante.

Les licences sont verrouillées sur les instances ADC. Pour extraire des licences d'un Citrix ADM HA, les instances nécessitent l'adresse IP de l'appliance spécifique. Lorsque vous appliquez des licences sur un serveur principal, ce dernier sera chargé des licences et applique toutes les licences futures sur cette instance. Vous pouvez supprimer des licences uniquement du serveur sur lequel vous avez installé les licences.

Orchestration

Le module d'orchestration est indépendant des licences et est toujours disponible.

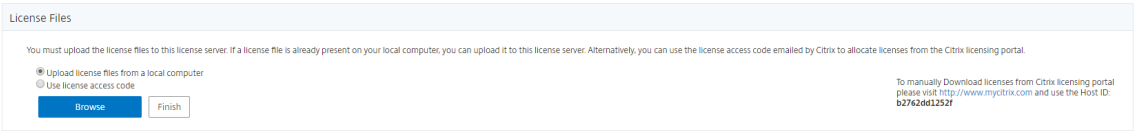
Mettre à niveau les licences de serveur virtuel

Vous pouvez mettre à niveau les licences sur Citrix ADM pour surveiller et gérer davantage de serveurs virtuels hébergés sur les appliances Citrix ADC.

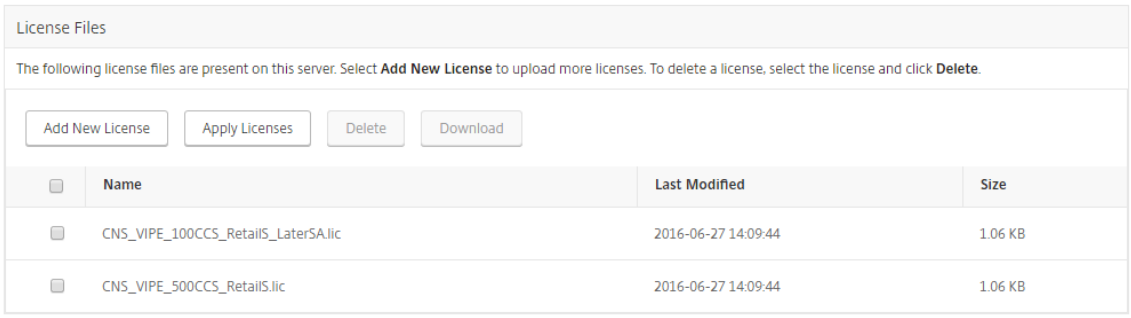
Pour mettre à niveau les licences de votre appliance :

1. Ouvrez une session sur Citrix ADM à l'aide des informations d'identification de l'administrateur.
2. Accédez à **Réseaux** > **Licences** > **Paramètres**.
3. Dans le volet de détails, accédez à License Files, puis sélectionnez l'une des options suivantes :
   - **Téléchargez des fichiers de licence à partir d'un ordinateur local**. Si une licence est déjà présente sur votre ordinateur local, cliquez sur**Parcourir** et sélectionnez le fichier de licence (.lic) que vous souhaitez utiliser pour allouer vos licences. Cliquez sur**Terminer**.
   - **Utilisez le code d'activation de licence**. Citrix envoie par e-mail le code d'accès à la licence que vous avez achetée. Entrez le code d'accès à la licence dans la zone de texte, puis cliquez sur **Obtenir des licences**.

   > **Remarque**
   >
   > Si vous sélectionnez cette option, Citrix ADM doit être connecté à Internet ou un serveur proxy doit être disponible.

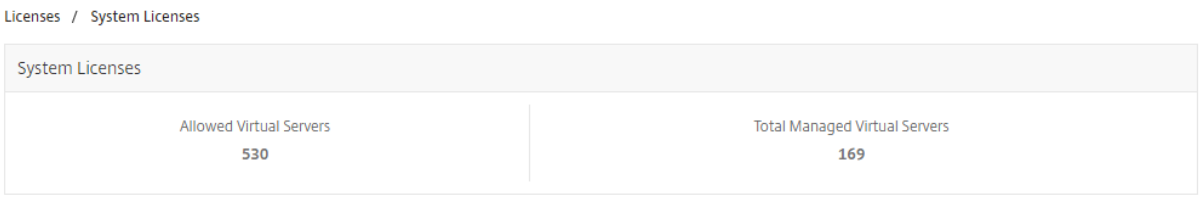


4. Vous pouvez ajouter d'autres licences à partir de la page Paramètres de licence à tout moment.



Vérification

Vous pouvez vérifier les licences installées sur votre Citrix ADM en accédant à**Système > Licensing**& Analytics.



Gérer les serveurs virtuels

Vous pouvez sélectionner les serveurs virtuels ou les serveurs virtuels tiers que vous souhaitez gérer et surveiller via Citrix ADM.

> **Points à noter**
>
> - Par défaut, Citrix ADM octroie automatiquement des licences aux serveurs virtuels de manière aléatoire après chaque cycle d'interrogation du serveur virtuel.
> - Si le nombre total de serveurs virtuels découverts dans votre Citrix ADM est inférieur au nombre de licences de serveur virtuel installées, Citrix ADM, par défaut, octroie des licences à tous les serveurs virtuels.

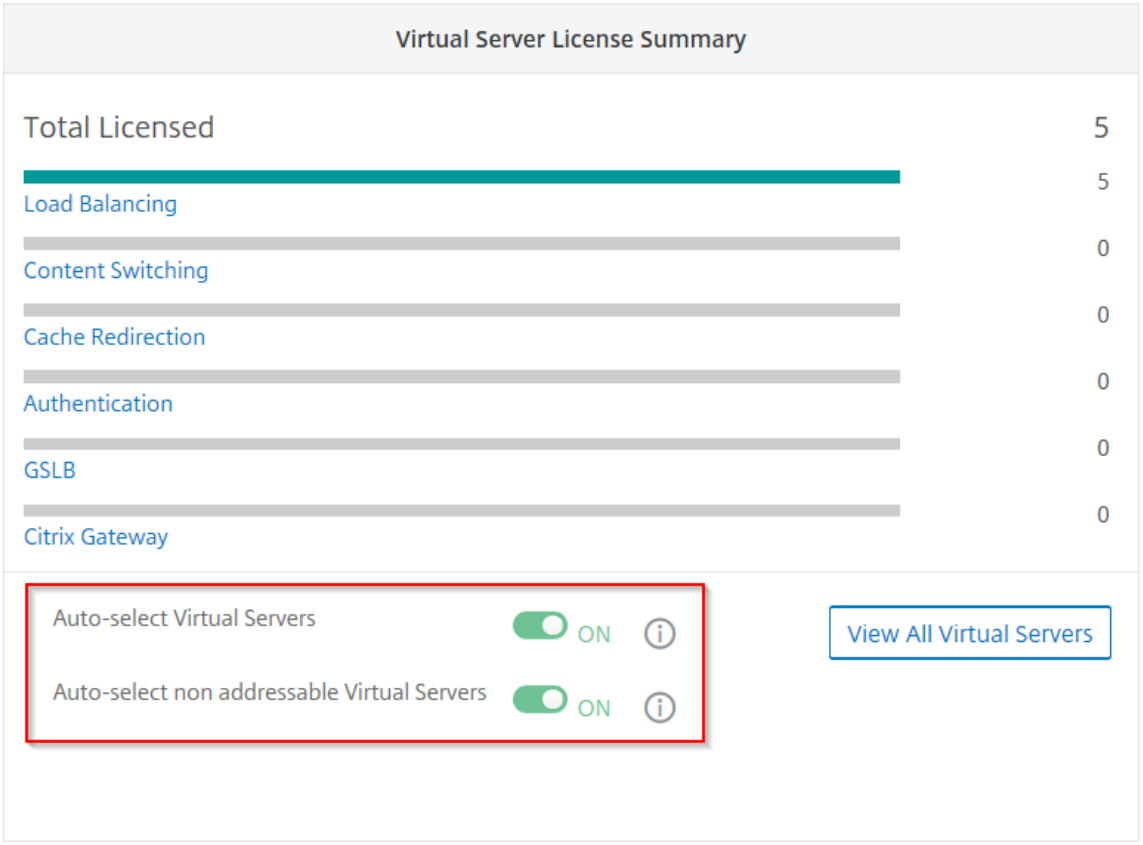
Pour sélectionner manuellement les serveurs virtuels ou pour limiter les licences aux serveurs virtuels limités, vous devez d'abord désactiver la licence automatique des serveurs virtuels, puis sélectionner les serveurs virtuels que vous souhaitez gérer.

Désactiver les serveurs virtuels sous licence automatique

1. Accédez à **Système > Licences et analyses**.

   Le tableau de bord affiche les licences de serveur virtuel disponibles, les serveurs virtuels gérés ainsi que le type de serveur virtuel et les informations d'expiration de licence.

2. Dans **Allocation de licence de serveur virtuel**, désactivez les **serveurs virtuels sous licence automatique** et **sélectionnez automatiquement les serveurs virtuels non adressables**.

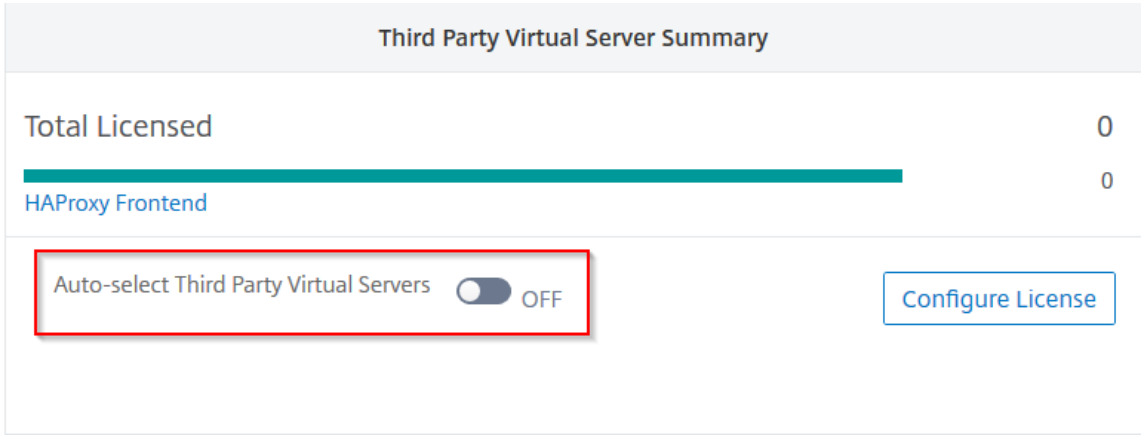


Sélectionner des serveurs virtuels tiers pour l'octroi de licences

1. Accédez à **Système > Licences et analyses**.

   Le tableau de bord affiche les licences de serveur virtuel disponibles, les serveurs virtuels gérés ainsi que le type de serveur virtuel et les informations d'expiration de licence.

2. Dans **Récapitulatif des serveurs virtuels tiers**, désactivez **la sélection automatique des serveurs virtuels tiers**.



Appliquer manuellement des licences de serveur virtuel

Vous pouvez appliquer manuellement des licences à un serveur virtuel individuel.

1. Dans **Allocation de licences de serveur virtuel**, sélectionnez **Configurer les licences**.

   La page **Tous les serveurs** virtuels s'affiche.
2. Filtrer les serveurs virtuels sans licence à l'aide de la propriété : `Licensed: No`.
3. Sélectionnez le serveur virtuel pour lequel vous souhaitez obtenir une licence.
4. Cliquez sur **Licence**.

Configuration des licences de serveur virtuel basées sur des stratégies

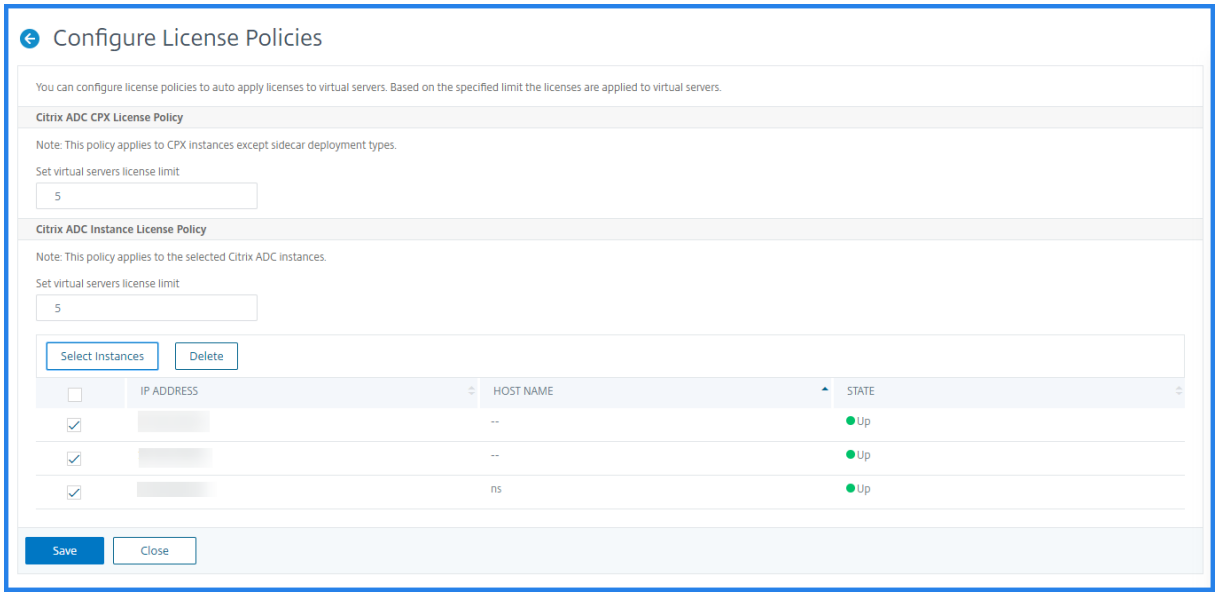
Vous pouvez configurer une stratégie pour appliquer une licence aux serveurs virtuels. Cette stratégie contrôle le nombre de serveurs virtuels pour lesquels vous souhaitez obtenir une licence automatique. Il applique également les licences aux serveurs virtuels des instances sélectionnées uniquement.

Cliquez sur **Modifier les stratégies** et vous pouvez spécifier les éléments suivants :

- Définissez la limite des serveurs virtuels sur les instances CPX séparément pour appliquer des licences. L'ADM applique une licence aux serveurs virtuels sur des instances CPX jusqu'à concurrence d'une limite spécifiée.

  > **Important**
  >
  > Cette limite s'applique aux instances CPX, à l'exception des types de déploiement sidecar.
  >
  > Pour afficher les instances CPX des types de déploiement sidecar, filtrez les serveurs virtuels à l'aide de la propriété : `License Type: Freely Managed`.

- Définissez la limite des serveurs virtuels sur certaines instances ADC (MPX/VPX/BLX) pour appliquer des licences. L'ADM applique des licences aux serveurs virtuels sur les instances ADC jusqu'à une limite spécifiée.
- Sélectionnez les instances ADC prioritaires pour appliquer les licences de serveur virtuel. Par conséquent, l'ADM peut appliquer une licence aux serveurs virtuels des instances sélectionnées uniquement.



Afficher les serveurs virtuels sous licence

Une fois les licences appliquées aux serveurs virtuels, vous pouvez consulter les serveurs virtuels sous licence ou les serveurs virtuels tiers sur la page **Licensing & Analytics** . Pour afficher les serveurs virtuels sous licence, effectuez les opérations suivantes :

1. Accédez à **Système > Licences et analyses**.
2. Cliquez sur le type de serveur virtuel dans la section **Licence totale** du **Récapitulatif des licences de serveurs virtuels**.

Configurer la prise en charge automatique des licences pour les serveurs virtuels non adressables

Par défaut, Citrix ADM n'applique pas automatiquement les licences aux serveurs virtuels non adressables. Pour obtenir des licences de serveurs virtuels non adressables, vous devez désactiver l'option de licence automatique et sélectionner manuellement les serveurs virtuels non adressables. Cela augmente vos efforts pour sélectionner manuellement les serveurs non adressables initialement lorsque vous appliquez les licences. Vous devez également sélectionner manuellement les nouveaux serveurs virtuels non adressables chaque fois qu'ils sont ajoutés à votre réseau.

Citrix ADM fournit une option dans Citrix ADM sous **Virtual Server License Allocation**. Si vous activez l'option **Sélection automatique des serveurs virtuels non adressables**, appliquez automatiquement les licences des serveurs virtuels non adressables.

Remarque

- Par défaut, Citrix ADM ne sélectionne toujours pas automatiquement les serveurs virtuels non adressables pour les licences.
- L'analyse des applications (App Dashboard) est la seule analyse prise en charge actuellement sur les serveurs virtuels non adressables sous licence.

Contrôles d'expiration pour les licences de serveurs virtuels

Vous pouvez désormais afficher l'état et définir des alertes pour l'expiration de la licence de serveur virtuel dans Citrix ADM.

Pour afficher l'état des licences :

1. Accédez à **Réseaux**> **Licences** > **Licences système.**
2. Dans la section **Informations sur l'expiration de la licence**, vous trouverez les détails des licences qui vont expirer :
    - **Fonctionnalité :** Type de licence qui va expirer.
    - **Nombre :** nombre de serveurs virtuels ou d'instances concernés.
    - **Jours d'expiration :** nombre de jours restants avant l'expiration.

Pour configurer les paramètres de notification des licences :

1. Accédez à **Réseaux** > **Licences** > **Paramètres**.
2. Dans la section **Paramètres de notification**, cliquez sur l'icône en forme de crayon et modifiez les paramètres.
    - **Profil d'e-mail :** profil d'e-mail ou liste de distribution pour l'envoi de notifications lorsque les licences atteignent le seuil ou expirent.
    - **SMS (SMS) :** profil SMS ou liste de distribution permettant d'envoyer des notifications lorsque les licences atteignent le seuil ou arrivent à expiration.
    - **Slack** - Spécifiez les détails du profil Slack.
    - **Alertes PagerDuty** - Spécifiez un profil PagerDuty. En fonction des paramètres de notification configurés dans votre portail PagerDuty, une notification est envoyée lorsque vos certificats sont sur le point d'expirer.
    - **M'avertir :** définissez le pourcentage de licences regroupées pour informer les administrateurs par e-mail ou SMS.

- **Seuil d'expiration de licence :** Nombre de jours avant l'expiration du nombre de licences déterminé par le seuil d'alerte.
- **Expiration des licences :** nombre de jours restants avant l'expiration.

Configuration système requise

February 1, 2024

Avant d'installer Citrix Application Delivery Management (ADM), vous devez comprendre la configuration logicielle requise, la configuration requise pour le navigateur, les informations de port, les informations de licence et les limitations.

Configuration requise pour Citrix ADM

Composant	Exigences
RAM	32 GB
CPU virtuel	8 processeurs **Remarque :** Citrix recommande d'utiliser la technologie SSD (Solid State Drive) pour les déploiements Citrix ADM.
Espace de stockage	L'espace de stockage par défaut requis est de 120 Go. Les besoins réels de stockage dépendent de l'estimation de la taille de Citrix ADM. Utilisez le calculateur de taille mentionné dans la section **Limites maximales** (numéro de page 7) du Guide de déploiement Citrix ADM HA. Ce guide est disponible sur notre site de téléchargement, sous **NetScaler MAS Release 12.1 > Versions antérieures**. **Remarque** : vous avez besoin d'un compte Citrix pour accéder au guide de déploiement et à la calculatrice de dimensionnement.

Composant	Exigences
	Si votre besoin de stockage Citrix ADM dépasse 120 Go, vous devez connecter un disque supplémentaire. Vous ne pouvez ajouter qu'un seul disque supplémentaire. Citrix vous recommande d'estimer le stockage et d'attacher un disque supplémentaire au moment du déploiement initial. Pour plus d'informations, consultez Comment attacher un disque supplémentaire à Citrix ADM.
Interfaces réseau virtuelles	1
Débit	1 Gbit/s ou 100 Mbit/s

> Remarque
>
> Citrix ADM n'est pas pris en charge par les chipsets AMD.

Configuration requise pour l'agent sur site Citrix ADM

Composant	Exigences
RAM	32 GB
CPU virtuel	8 processeurs
Espace de stockage	30 GB
Interfaces réseau virtuelles	1
Débit	1 Gbit/s

> Remarque
>
> L'agent Citrix ADM n'est pas pris en charge par le chipset AMD.

Version minimale de Citrix ADC requise pour les fonctionnalités Citrix ADM

> **Important**
>
> La version et la version de Citrix ADM doivent être **égales ou supérieures à** celles de votre version et build de Citrix ADC. Par exemple, si vous avez installé Citrix ADM 12.1 Build 50.39, assurez-vous

> d'avoir installé Citrix ADC 12.1 Build 50.28/50.31 ou une version antérieure.

Fonctionnalités de Citrix ADM	Version du logiciel Citrix ADC
StyleBooks	10.5 et versions ultérieures
Prise en charge d'OpenStack/CloudStack	11.0 et versions ultérieures, si une partition est requise 11.1 et versions ultérieures, si une partition sur un réseau local virtuel partagé est requise
Prise en charge de NSX	11.1 Build 47.14 et versions ultérieures (VPX)
Assistance Mesos/Marathon	10.5 et versions ultérieures
Sauvegarde/restauration	Pour Citrix ADC, 10.1 et versions ultérieures Pour Citrix SDX, 11.0 et versions ultérieures
Surveillance, création de rapports et configuration à l'aide des tâches	10.1 et versions ultérieures
Fonctionnalités d'analyse	
Web Insight	10.5 et versions ultérieures
HDX Insight	10.1 et versions ultérieures
Security Insight	11.0.65.31 et versions ultérieures
Gateway Insight	11.0.65.31 et versions ultérieures
Insight du cache	10.5 et versions ultérieures*
SSL Insight	12.0 et versions ultérieures

* Les métriques de cache intégrées ne sont pas prises en charge dans Citrix ADM avec les instances Citrix ADC exécutant la version 11.0 build 66.x.

Configuration requise pour la gestion des instances Citrix SD-WAN

Matrice d'interopérabilité des éditions/versions de la plate-forme Citrix SD-WAN et des fonctionnalités Citrix ADM

Édition Plateforme	Citrix SD-WAN WANOP	Citrix SD-WAN SE	Citrix SD-WAN PE
Détection	Oui	Oui	Oui
Configuration	Oui	Non	Non
Surveillance	Oui	Non	Non
Rapports (rapports réseau)	Oui	Non	Non
Gestion des événements	Oui	Non	Non
HDX Insight	Oui	Non	Non
WAN Insight	Oui	Non	Non
HDX Insight (déploiement à sauts multiples)	Oui	Oui	Non

Clients légers pris en charge pour les instances Citrix SD-WAN

Citrix ADM prend en charge les clients légers suivants pour surveiller les déploiements Citrix SD-WAN :

- Client léger Dell Wyse WTOS modèle R10L Rx0L
- NComputing N400
- Dell Wyse WTOS modèle CX0 C00X Xenith
- Dell Wyse WTOS modèle TXO T00X Xenith2
- Modèle CX0 C10LE WTOS de Dell Wyse
- Client léger HDX Dell Wyse WTOS modèle R00LX Rx0L
- Dell Wyse Enhanced SUSE Linux Enterprise, modèle Dx0D, D50D
- Client léger Dell Wyse ZX0 Z90D7 (WES7)

Configuration requise pour les analyses Citrix ADM

Versions minimales de Citrix Virtual Apps and Desktops requises pour les fonctionnalités de Citrix ADM

Fonctionnalités de Citrix ADM	Version Citrix Virtual Apps and Desktops
HDX Insight	Citrix Virtual Apps and Desktops 7.0 et versions ultérieures

> **Remarque**
>
> La fonctionnalité Citrix Gateway (appelée Access Gateway Enterprise pour les versions 9.3 et 10.x) doit être disponible sur l'instance Citrix ADC. Citrix ADM ne prend pas en charge les appliances Access Gateway Standard autonomes.

Citrix ADM peut générer des rapports pour les applications publiées sur Citrix Virtual Apps ou Citrix Virtual Desktops et accessibles via Citrix Receiver. Toutefois, cette fonctionnalité dépend du système d'exploitation sur lequel Receiver est installé. Actuellement, un Citrix ADC n'analyse pas le trafic ICA pour les applications ou les postes de travail accessibles via Citrix Receiver s'exécutant sur les systèmes d'exploitation iOS ou Android.

Clients légers pris en charge pour des informations HDX

- Clients légers Dell Wyse Windows
- Clients légers basés sur Dell Wyse Linux
- Clients légers basés sur Dell Wyse ThinOS
- Clients légers basés sur Ubuntu 10ZiG
- IGEL UD3 W7+ (M340)
- IGEL UD3 W7 (M340C)

Licence d'instance Citrix ADC requise pour HDX Insight

Les données collectées par Citrix ADM pour HDX Insight dépendent de la version et des licences des instances Citrix ADC surveillées. Les rapports HDX Insight sont affichés uniquement pour les appliances Citrix ADC Premium et Advanced exécutant les versions 10.5 et ultérieures.

Licence/Durée Citrix ADC	5 minutes	1 heure	1 jour	1 semaine	1 mois
Standard	Non	Non	Non	Non	Non

Advanced	Oui	Oui	Non	Non	Non
Premium	Oui	Oui	Oui	Oui	Oui

Hyperviseurs pris en charge

Le tableau suivant répertorie les hyperviseurs pris en charge par Citrix ADM.

Hyperviseur	Versions
Citrix Hypervisor	7.1 et 7.4
VMware ESX	6,0, 6,5, 6,7 et 7,0
Microsoft Hyper-V	2012 R2 et 2016
KVM générique	RHEL 7.4 et Ubuntu 16.04

Systèmes d'exploitation et versions de Receiver prises en charge

Le tableau suivant répertorie les systèmes d'exploitation pris en charge par Citrix ADM et les versions de Citrix Receiver actuellement prises en charge par chaque système :

Système d'exploitation	Version de Receiver
Windows	Édition standard 4.0
Linux	13.0.265571 et versions ultérieures
Mac	11.8, build 238301 et versions ultérieures
HTML5	1.5*
Appli Chrome	1.5*

* Applicable avec Citrix CloudBridge (Citrix SD-WAN WANOP) version 7.4 et ultérieure.

Navigateurs pris en charge

Le tableau suivant répertorie les navigateurs Web pris en charge par Citrix ADM :

Navigateur Web	Version
Microsoft Edge	79 et versions ultérieures
Google Chrome	51 et versions ultérieures
Safari	10 et versions ultérieures
Mozilla Firefox	52 et versions ultérieures

Ports supportés

Citrix ADM utilise l'adresse IP Citrix ADC (connue sous le nom NSIP) pour communiquer avec Citrix ADC. Vous pouvez utiliser l'agent ADM comme intermédiaire entre l'instance ADC et ADM ou l'instance SD-WAN et ADM. Pour établir une communication avec ces serveurs, ouvrez les ports requis.

> **Remarque**
>
> Si vous avez configuré Citrix ADC en mode Haute disponibilité, Citrix ADM utilise l'adresse IP du sous-réseau Citrix ADC (Management SNIP) pour communiquer avec Citrix ADC. Pour la communication à l'aide de SNIP avec Citrix ADM, les ports requis restent les mêmes.

Schéma des ports réseau pour un déploiement sans agent :

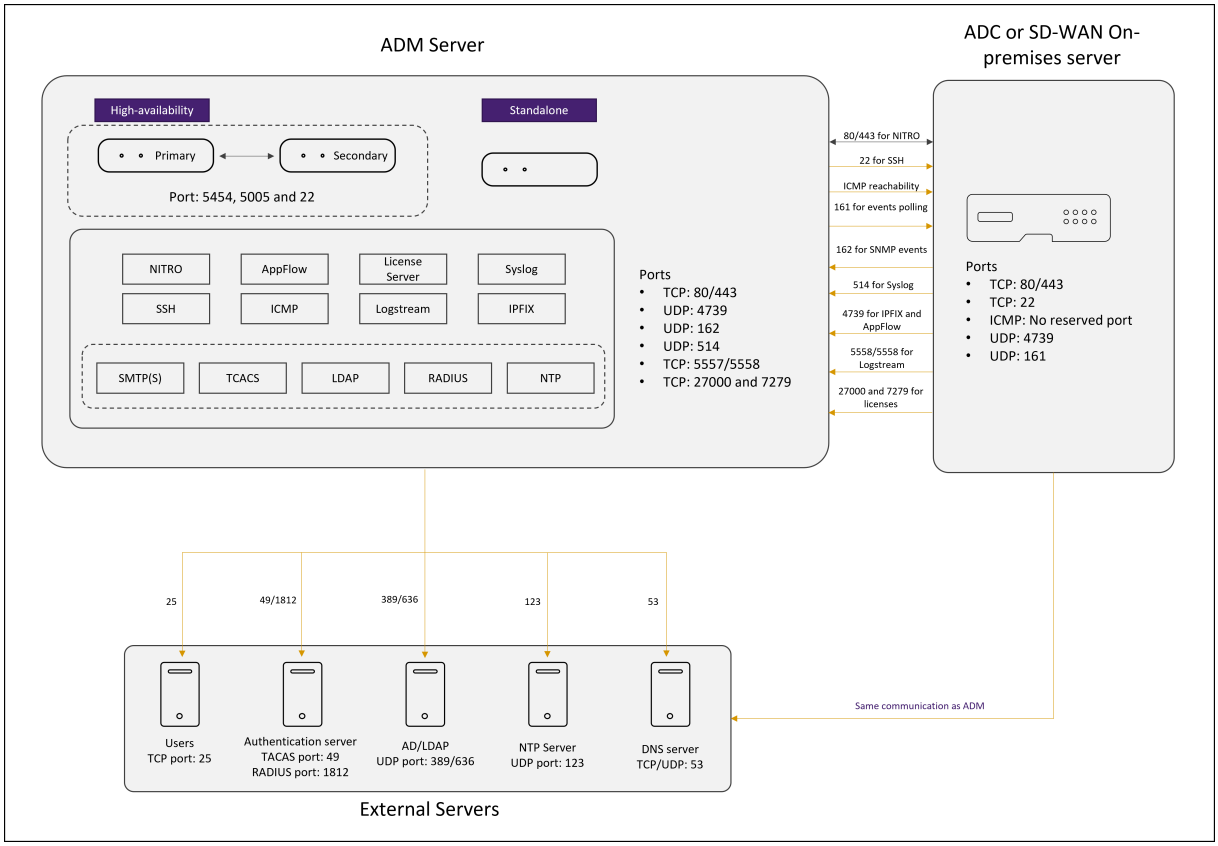
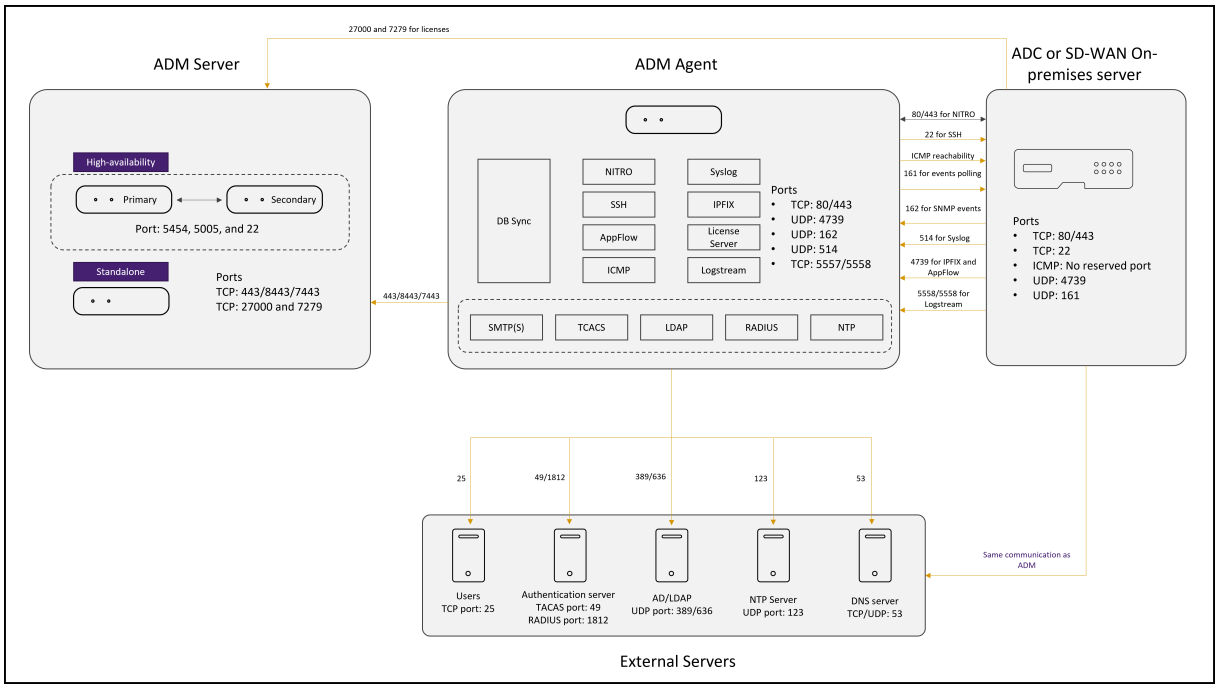


Diagramme des ports réseau pour le déploiement qui inclut l'agent ADM :



Les sections suivantes expliquent les ports requis et leur but :

- Serveur ADM

- Agent ADM
- Instance ADC ou SD-WAN
- Serveurs externes

Ports pour le serveur ADM

Ce tableau explique les ports requis qui doivent être ouverts sur le serveur ADM.

Port	Type	Détails	Direction de la communication
5454 et 22	TCP	Port par défaut pour la communication et la synchronisation de base de données entre les nœuds Citrix ADM en mode haute disponibilité.	Nœud principal Citrix ADM vers le nœud secondaire Citrix ADM
443/8443/7443	TCP	Port pour la communication entre l'agent Citrix ADM et Citrix ADM.	L'agent Citrix ADM initie la communication avec Citrix ADM. Citrix ADM et l'agent interagissent ensuite l'un avec l'autre.

Si les instances ADM et ADC n'utilisent pas d'agent de communication, assurez-vous d'ouvrir les ports suivants sur le serveur ADM :

Port	Type	Détails	Direction de la communication
80/443	TCP	Pour les communications NITRO entre Citrix ADM et Citrix ADC ou une instance Citrix SD-WAN.	Agent Citrix ADM vers Citrix ADC et Citrix ADC vers Citrix ADM

Port	Type	Détails	Direction de la communication
4739	UDP	Pour la communication AppFlow à partir d'une instance Citrix ADC ou Citrix SD-WAN vers Citrix ADM.	Citrix ADC ou Citrix SD-WAN vers Citrix ADM agent
162	UDP	Pour recevoir des événements SNMP de l'instance Citrix ADC vers Citrix ADM.	Agent Citrix ADC vers Citrix ADM
514	UDP	Pour recevoir des messages syslog à partir d'une instance Citrix ADC ou Citrix SD-WAN vers Citrix ADM.	Citrix ADC ou Citrix SD-WAN vers Citrix ADM agent
5557/5558	TCP	Pour la communication logstream (pour Security Insight, Web Insight et HDX Insight) de Citrix ADC à Citrix ADM.	Citrix ADC vers Citrix ADM
5005	TCP	Port pour échanger les pulsations entre les nœuds HA.	Nœud principal à nœud secondaire Citrix ADM. Nœud secondaire à nœud principal Citrix ADM.

Ports pour l'agent ADM

Ce tableau explique les ports requis qui doivent être ouverts sur l'agent ADM.

Port	Type	Détails	Direction de la communication
80/443	TCP	Pour les communications NITRO entre Citrix ADM et Citrix ADC ou une instance Citrix SD-WAN.	Agent Citrix ADM vers Citrix ADC et Citrix ADC vers Citrix ADM
4739	UDP	Pour la communication AppFlow à partir d'une instance Citrix ADC ou Citrix SD-WAN vers Citrix ADM.	Citrix ADC ou Citrix SD-WAN vers Citrix ADM agent
162	UDP	Pour recevoir des événements SNMP de l'instance Citrix ADC vers Citrix ADM.	Agent Citrix ADC vers Citrix ADM
514	UDP	Pour recevoir des messages syslog à partir d'une instance Citrix ADC ou Citrix SD-WAN vers Citrix ADM.	Citrix ADC ou Citrix SD-WAN vers Citrix ADM agent
5557/5558	TCP	Pour la communication logstream (pour Security Insight, Web Insight et HDX Insight) de Citrix ADC à Citrix ADM.	Citrix ADC vers Citrix ADM

Ports pour instances ADC et SD-WAN

Ce tableau explique les ports requis qui doivent être ouverts sur les instances Citrix ADC et SD-WAN.

Port	Type	Détails	Direction de la communication
80/443	TCP	Pour la communication NITRO depuis Citrix ADM vers Citrix ADC ou Citrix SD-WAN instance.443. Pour la communication NITRO entre les serveurs Citrix ADM en mode haute disponibilité.	Citrix ADM vers Citrix ADC et Citrix ADC vers Citrix ADM
22	TCP	Pour la communication SSH depuis Citrix ADM vers Citrix ADC ou Citrix SD-WAN instance. Pour la synchronisation entre les serveurs Citrix ADM déployés en mode haute disponibilité. Et, ce port est requis pour la communication SSH entre l'agent ADM et Citrix ADC.	Citrix ADM à Citrix ADC. Ou, agent Citrix ADM à Citrix ADC.
Aucun port réservé	ICMP	Pour détecter l' accessibilité réseau entre les instances Citrix ADM et Citrix ADC, les instances SD WAN ou le serveur Citrix ADM secondaire déployé en mode haute disponibilité.	Citrix ADM vers Citrix ADC
161	UDP	Pour interroger les événements à partir d' instances ADC.	Citrix ADM vers Citrix ADC

> **Remarque :**
>
> Dans le cadre du déploiement haute disponibilité d'ADM, toutes les communications d'ADM utilisent l'adresse IP du nœud principal.

Ports pour serveurs externes

Ce tableau explique les ports requis qui doivent être ouverts sur des serveurs externes :

Port	Type	Détails	Direction de la communication
25	TCP	Pour envoyer des notifications SMTP depuis Citrix ADM aux utilisateurs.	Citrix ADM aux utilisateurs.
389/636	TCP	Port par défaut pour le protocole d'authentification. Pour la communication entre Citrix ADM et le serveur d'authentification externe LDAP.	Serveur d'authentification externe Citrix ADM vers LDAP
123	UDP	Port du serveur NTP par défaut pour, synchronisation avec plusieurs sources temporelles.	Citrix ADM vers serveur NTP
1812	RADIUS	Port par défaut pour le protocole d'authentification. Pour la communication entre Citrix ADM et le serveur d'authentification externe RADIUS.	Serveur d'authentification externe Citrix ADM vers RADIUS

Port	Type	Détails	Direction de la communication
49	TACACS	Port par défaut pour le protocole d'authentification. Pour la communication entre Citrix ADM et le serveur d'authentification externe TACACS.	Serveur d'authentification externe Citrix ADM vers TACACS

Limitations

À partir de Citrix ADM 12.1 ou version ultérieure, les fonctionnalités suivantes prennent en charge le format IPv6 des adresses IP :

1. Accès à la gestion pour l'interface graphique Citrix ADM
2. Accès à la gestion pour Citrix ADC
3. Enregistrement et inventaire
4. Tableau de bord réseau
5. Tableau de bord SSL
6. Tâches Config
7. Audit de configuration
8. Fonctions réseau
9. Rapports sur le réseau
10. Sauvegarde et restauration des instances ADC
11. Événements SNMP des Citrix ADC

Les fonctionnalités suivantes ne prennent pas en charge IPv6 :

1. IP flottante haute disponibilité
2. Syslog reçus des ADC qui prennent en charge IPv6
3. StyleBooks sur ADC prenant en charge IPv6
4. Analytics
5. Licences groupées

Mise en route

February 1, 2024

Ce document vous explique comment commencer à déployer et configurer Citrix Application Delivery Management (ADM) pour la première fois. Ce document est destiné aux administrateurs réseau et d'applications qui gèrent des périphériques réseau Citrix (Citrix SD-WAN WO, Citrix Gateway, etc.) ainsi que des appareils tiers tels que HAProxy. Suivez les étapes décrites dans ce document quel que soit le type de périphérique que vous envisagez de gérer à l'aide de Citrix ADM.

Si vous êtes un utilisateur existant de Citrix ADM, il est recommandé de consulter les notes de publication, la configuration système requiseet les détails de licence avant de mettre à niveau votre serveur vers la dernière version de Citrix ADM.

Étape 1 - Examiner les exigences du système

Avant de commencer à déployer Citrix ADM dans votre centre de données, passez en revue la configuration logicielle requise, la configuration requise en matière de navigateur, les informations de port, les informations de licence et les limitations.

- **Informations sur la licence**. Vous pouvez gérer et surveiller n'importe quel nombre d'instances et d'entités sans licence. Toutefois, vous ne pouvez gérer que 30 applications découvertes et consulter les informations d'analyse de deux serveurs virtuels uniquement sans appliquer de licence. Pour gérer plus de 30 applications ou afficher des analyses pour plus de deux serveurs virtuels, vous devez acheter des licences appropriées. En savoir plus.
- **Exigences relatives au système d'exploitation et au récepteur**. Vérifiez ces informations pour vous assurer que vous disposez de la version du récepteur correcte pour les systèmes d'exploitation pris en charge. En savoir plus.
- **Exigences du navigateur**. Pour accéder à l'interface graphique Citrix ADM, vous devez vous assurer que vous disposez du navigateur requis et de la version correcte. En savoir plus.
- **Ports**. Assurez-vous que les ports requis sont ouverts pour que Citrix ADM puisse communiquer avec les instances Citrix ADC ou SD-WAN ou les instances Citrix ADC et SD-WAN. En savoir plus.
- **Configuration requise pour l'instance de Citrix ADC**. Différentes fonctionnalités de Citrix ADM sont prises en charge sur différentes versions du logiciel Citrix ADC. Vérifiez ces informations pour vous assurer que vous avez mis à niveau vos instances Citrix ADC vers la version correcte. En savoir plus.
- **Configuration requise pour l'instance Citrix SD-WAN**.Vérifiez ces informations pour vous assurer que vous avez mis à niveau vos instances Citrix SD-WAN vers la version correcte et que vous disposez des éditions de plate-forme correctes. En savoir plus.

Étape 2 - Déployer Citrix ADM

Pour gérer et surveiller les applications et l'infrastructure réseau, vous devez d'abord installer Citrix ADM sur l'un des hyperviseurs. Vous pouvez déployer Citrix ADM en tant que serveur unique ou en mode haute disponibilité. Si vous utilisez Citrix ADC Insight Center, vous pouvez migrer vers Citrix ADM et bénéficier des fonctionnalités de gestion, de surveillance, d'orchestration et de gestion des applications en plus des fonctionnalités d'analyse.

- **Déploiement d'un serveur unique**.Dans un déploiement de serveur unique Citrix ADM, la base de données est intégrée au serveur et un seul serveur traite tout le trafic. Vous pouvez déployer Citrix ADM avec Citrix Hypervisor, VMware ESXi, Microsoft Hyper-V et Linux KVM. Voir :
  - Citrix ADM avec Citrix Hypervisor
  - Citrix ADM avec Microsoft Hyper-V
  - Citrix ADM avec VMware ESXi
  - Citrix ADM avec serveur KVM Linux
- **Déploiement haute disponibilité.** Un déploiement haute disponibilité (HA) de deux serveurs Citrix ADM fournit des opérations ininterrompues. Dans une configuration haute disponibilité, les deux nœuds Citrix ADM doivent être déployés en mode actif-passif, sur le même sous-réseau en utilisant la même version et le même build de logiciel, et doivent avoir les mêmes configurations. Avec le déploiement HA, la possibilité de configurer l'adresse IP flottante sur le nœud principal Citrix ADM élimine le besoin d'un équilibreur de charge Citrix ADC distinct. Pour en savoir plus, consultez la section Configurer dans un déploiement haute disponibilité.

Étape 3 - Ajouter des instances à Citrix ADM

Les instances sont des appliances Citrix, des appliances virtuelles ou des appareils tiers que vous souhaitez découvrir, gérer et surveiller à partir de Citrix ADM. Vous devez ajouter des instances au serveur Citrix ADM si vous souhaitez gérer et surveiller ces instances. Vous pouvez ajouter les instances suivantes à Citrix ADM :

- Citrix ADC
  - Citrix ADC MPX
  - Citrix ADC VPX
  - Citrix ADC SDX
  - Citrix ADC CPX

  - Citrix Gateway
  - Citrix SD-WAN
- HaProxy

Lorsque vous ajoutez une instance au serveur Citrix ADM, le serveur communique implicitement avec les instances et collecte un inventaire de ces instances.

En savoir plus

Étape 4 - Activer les analyses sur les serveurs virtuels

Pour afficher les données d'analyse du flux de trafic de votre application, vous devez activer la fonctionnalité Analytics sur les serveurs virtuels qui reçoivent du trafic pour les applications spécifiques.

En savoir plus

Étape 5 - Configurer le serveur NTP sur Citrix ADM

Vous devez configurer un serveur NTP (Network Time Protocol) dans Citrix ADM pour synchroniser son horloge avec le serveur NTP. La configuration d'un serveur NTP garantit que l'horloge Citrix ADM possède les mêmes paramètres de date et d'heure que les autres serveurs du réseau.

En savoir plus

Étape 6 - Configurer les paramètres système pour des performances optimales de Citrix ADM

Avant de commencer à utiliser Citrix ADM pour gérer et surveiller vos instances et applications, il est recommandé de configurer quelques paramètres système qui garantissent des performances optimales de votre serveur Citrix ADM.

- **Configurez les alarmes système**. Configurez les alarmes système pour vous assurer que vous êtes au courant de tout problème système critique ou majeur. Par exemple, vous pouvez être averti si l'utilisation de l'UC est élevée ou s'il y a plusieurs échecs de connexion au serveur.
- **Configurez les notifications système**. Vous pouvez envoyer des notifications à certains groupes d'utilisateurs pour diverses fonctions liées au système. Vous pouvez configurer un serveur de notifications dans Citrix ADM et configurer des serveurs de Gateway de messagerie et SMS (Short Message Service) pour envoyer des notifications par courrier électronique et texte aux utilisateurs. Cela garantit que vous êtes informé de toutes les activités au niveau du système, telles que la connexion utilisateur ou le redémarrage du système.

- **Configurez les paramètres de nettoyage du système**. Pour limiter la quantité de données de rapport stockées dans la base de données de votre serveur Citrix ADM, vous pouvez spécifier l'intervalle pendant lequel vous souhaitez que Citrix ADM conserve les données de rapport réseau, les événements, les journaux d'audit et les journaux des tâches. Par défaut, ces données sont nettoyées toutes les 24 heures (à 00.00 heures).
- **Configurez les paramètres de sauvegarde du système**. Citrix ADM sauvegarde automatiquement le système tous les jours à 00 h 30. Par défaut, il enregistre trois fichiers de sauvegarde. Vous souhaiterez peut-être conserver un plus grand nombre de sauvegardes du système.
- **Configurez les paramètres de sauvegarde d'instance**. Si vous sauvegardez l'état actuel d'une instance Citrix ADC, vous pouvez utiliser les fichiers de sauvegarde pour restaurer la stabilité au cas où l'instance deviendrait instable. Cela est particulièrement important avant d'effectuer une mise à niveau. Par défaut, une sauvegarde est effectuée toutes les 12 heures et trois fichiers de sauvegarde sont conservés dans le système.
- **Configurez les paramètres de nettoyage d'événement d'instance**. Pour limiter la quantité de données de messages d'événement stockées dans la base de données de votre serveur Citrix ADM, vous pouvez spécifier l'intervalle pendant lequel vous souhaitez que Citrix ADM conserve les données de rapport réseau, les événements, les journaux d'audit et les journaux des tâches. Par défaut, ces données sont effacées toutes les 24 heures (à 00:00 heures).
- **Configurez les paramètres de purge Syslog de l'instance**.Pour limiter la quantité de données syslog stockées dans la base de données, vous pouvez spécifier l'intervalle auquel vous souhaitez purger les données syslog. Vous pouvez spécifier le nombre de jours après lequel les données syslog suivantes seront supprimées de Citrix ADM :
  - Données Syslog génériques
  - Données AppFirewall
  - Données Citrix Gateway.

    En savoir plus

Prochaine étape

Après avoir déployé et configuré Citrix ADM, vous pouvez commencer à gérer et à surveiller vos instances et applications.

Gestion des instances et des applications Citrix ADC. Toutes les fonctionnalités de Citrix ADM sont prises en charge sur les instances Citrix ADC. Vous pouvez commencer à utiliser n'importe laquelle des fonctionnalités.

Gestion des instances SD-WAN Citrix ADC. Toutes les fonctionnalités de Citrix ADM ne sont pas prises en charge sur les instances WO SD-WAN. Par exemple, la gestion des certificats ou l'audit de configura-

tion ne sont pas pris en charge. Pour savoir quelles fonctionnalités sont prises en charge et comment les utiliser, consultez la section Gestion de Citrix SD-WAN WO à l'aide de Citrix ADM.

Gestion des instances et des applications HaProxy. Vous pouvez surveiller les frontaux, les backends et les serveurs configurés dans un déploiement HAProxy. Vous pouvez également utiliser la fonctionnalité de gestion des applications pour surveiller les statistiques en temps réel des frontaux surveillés par Citrix ADM. Pour savoir quelles fonctionnalités sont prises en charge pour HAProxy et comment les utiliser, consultez Gestion et surveillance des instances HAProxy à l'aide de Citrix ADM.

Déployer

February 1, 2024

Avant d'utiliser Citrix ADM pour gérer et surveiller vos applications et votre infrastructure réseau, vous devez d'abord l'installer sur l'un des hyperviseurs ou sur un cluster Kubernetes. Si vous déployez Citrix ADM sur un hyperviseur, vous pouvez le déployer en tant que serveur unique ou en mode haute disponibilité. Le mode haute disponibilité n'est pas applicable sur un cluster Kubernetes. Si vous utilisez NetScaler Insight Center, vous pouvez migrer vers Citrix ADM et bénéficier des fonctionnalités de gestion, de surveillance, d'orchestration et de gestion des applications en plus des fonctionnalités d'analyse.

- **Déploiement sur un serveur unique** : pour un ADM autonome déployé sur un hyperviseur, la base de données est intégrée au serveur et un seul serveur traite l'ensemble du trafic. Vous pouvez déployer Citrix ADM avec Citrix Hypervisor, VMware ESXi, Microsoft Hyper-V et Linux KVM. Voir :
  - Citrix ADM sur Citrix Hypervisor
  - Citrix ADM sur Microsoft Hyper-V
  - Citrix ADM sur VMware ESXi
  - Citrix ADM sur le serveur KVM Linux
  - Citrix ADM sur un cluster Kubernetes
- **Déploiement à haute disponibilité (HA)** : un déploiement HA de deux serveurs Citrix ADM assure des opérations ininterrompues. Dans une configuration HA, les deux nœuds Citrix ADM doivent être déployés en mode actif-passif, sur le même sous-réseau en utilisant la même version logicielle et le même build, et doivent avoir les mêmes configurations. Avec le déploiement HA, la possibilité de configurer l'adresse IP flottante sur le nœud principal Citrix ADM élimine le besoin d'un équilibreur de charge Citrix ADC distinct. Voir :Configurer dans un déploiement haute disponibilité.

> Remarque La
>
> haute disponibilité n'est pas applicable pour ADM déployé sur un cluster Kubernetes.

- **Migrer de NetScaler Insight Center vers Citrix ADM** : vous pouvez migrer votre déploiement de NetScaler Insight Center vers Citrix ADM sans perdre la configuration, les paramètres ou les données existants. Avec Citrix ADM, vous pouvez non seulement afficher les différentes analyses générées par les instances Citrix ADC et Citrix SD-WAN, mais également gérer, surveiller et dépanner l'ensemble de l'infrastructure globale de distribution d'applications à partir d'une console unifiée unique. Voir :Migration de NetScaler Insight Center vers Citrix ADM
- **Intégrer Citrix ADM à Director** : Director s'intègre à Citrix ADM pour l'analyse du réseau et la gestion des performances. Voir : Intégrer Citrix ADM à Director

Conditions préalables à l'installation de Citrix ADM

February 1, 2024

Vous pouvez télécharger et installer Citrix Application Delivery Management (ADM) pour les plates-formes Microsoft HyperV,
VMware ESXi, Linux KVM et Citrix Hypervisor en tant qu'appliance virtuelle. Avant d'installer NetScaler ADM, vous devez comprendre la configuration logicielle requise, la configuration requise du navigateur, les
informations de port, les informations de licence et les limitations de toutes ces plates-formes.

Pour connaître les exigences spécifiques de la plate-forme et les étapes détaillées d'installation de Citrix ADM, consultez les rubriques suivantes :

- Citrix ADM avec Citrix Hypervisor
- Citrix ADM avec Microsoft HyperV
- Citrix ADM avec VMware ESXi
- Citrix ADM avec serveur KVM Linux

Configuration requise pour Citrix ADM

Composant	Exigences
RAM	32 GB

Composant	Exigences
CPU virtuel	8 processeurs
Espace de stockage	Citrix recommande d'utiliser la technologie SSD (Solid State Drive) pour les déploiements Citrix ADM. L'espace de stockage par défaut requis est de 120 Go. Les besoins réels de stockage dépendent de l'estimation de la taille de Citrix ADM. Utilisez le calculateur de taille mentionné dans la section **Limites maximales** (numéro de page 7) du Guide de déploiement Citrix ADM HA. Ce guide est disponible sur notre site de téléchargement, sous **NetScaler MAS Release 12.1 > Versions antérieures**. **Remarque** : vous avez besoin d'un compte Citrix pour accéder au guide de déploiement et à la calculatrice de dimensionnement Si votre besoin de stockage Citrix ADM dépasse 120 Go, vous devez attacher un disque supplémentaire. Citrix vous recommande d'estimer le stockage et d'attacher un disque supplémentaire au moment du déploiement initial. Vous ne pouvez ajouter qu'un seul disque supplémentaire. Pour plus d'informations, consultez Comment attacher un disque supplémentaire à Citrix ADM.
Interfaces réseau virtuelles	1
Débit	1 Gbit/s

> Remarque :
>
> Citrix vous recommande d'héberger le disque dur virtuel Citrix ADM sur un stockage local. Lorsqu'il est hébergé sur des périphériques de stockage dans un SAN, Citrix ADM peut ne pas fonctionner comme prévu. Le déploiement d'ADM sur le SAN n'est donc pas pris en charge.

Citrix ADM sur Citrix Hypervisor

February 1, 2024

Pour installer Citrix ADM sur Citrix Hypervisor (anciennement XenServer), vous devez d'abord télécharger le fichier image .xva Citrix ADM sur votre ordinateur local. Vous devez utiliser Citrix XenCenter pour effectuer l'installation de Citrix ADM.

> **Remarque :**
>
> Citrix ADM ne prend pas en charge XenMotion.

Conditions préalables

Avant d'installer Citrix ADM, vérifiez que les exigences suivantes sont respectées :

- Citrix Hypervisor version 7.1 ou ultérieure est installé sur le matériel qui répond à la configuration minimale requise.
- XenCenter est installé sur un poste de travail de gestion qui répond aux exigences minimales. Vous devez utiliser XenCenter pour installer Citrix ADM sur Citrix Hypervisor.
- Vous avez téléchargé le fichier image .XVA de Citrix ADM.

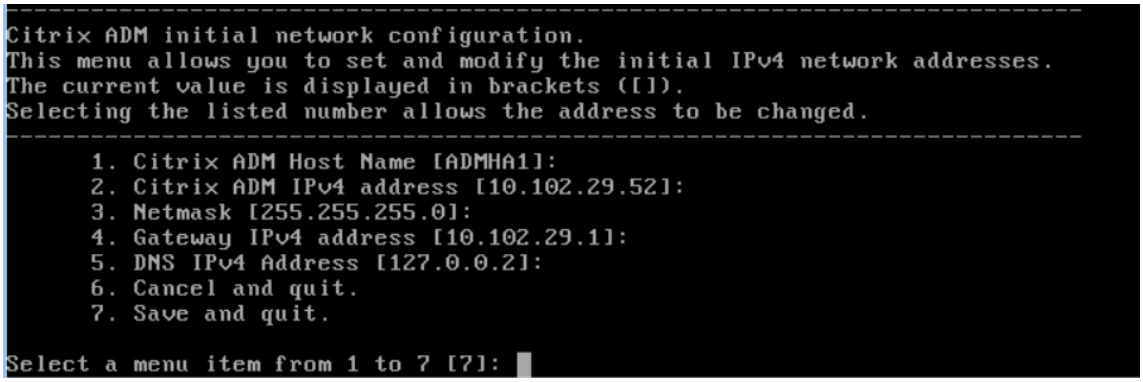
Configuration système requise pour XenCenter

XenCenter est une application cliente Windows. Il ne peut pas s'exécuter sur la même machine que l'hôte Citrix Hypervisor. Le tableau suivant décrit la configuration minimale requise.

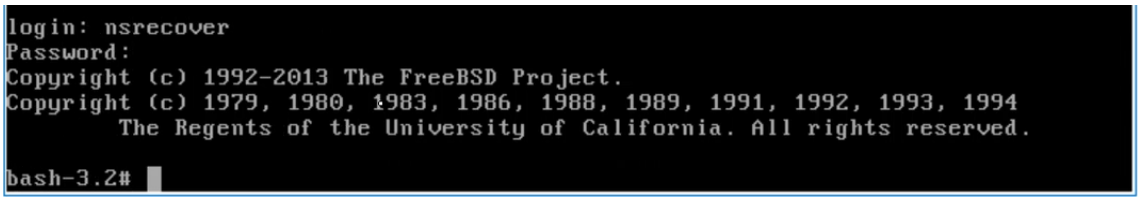
Composant	Exigences
Système d'exploitation	Windows 7, Windows Server 2003 ou Windows 10
.NET framework	Version 2.0 ou ultérieure
UC	750 MHz (MHz), recommandé : 1 gigahertz (GHz) ou plus rapide
RAM	1 Go, Recommandé : 2 Go
Carte d'interface réseau	Carte réseau 100 mégabits par seconde (Mbps) ou plus rapide

Installation de Citrix Application Delivery Management

1. Importez le fichier image XVA dans votre Citrix Hypervisor et, à partir de l'onglet **Console**, configurez les options de configuration réseau initiales.

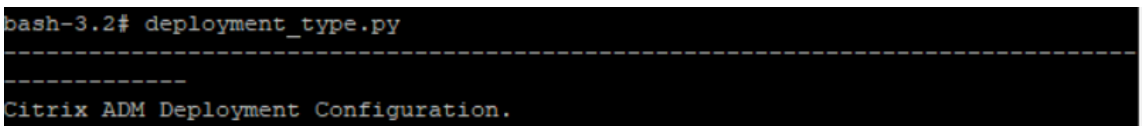


2. Après avoir spécifié les adresses IP requises, enregistrez les paramètres de configuration.
3. Lorsque vous y êtes invité, ouvrez une session à l'aide des informations d'identification nsrecover/nsroot.

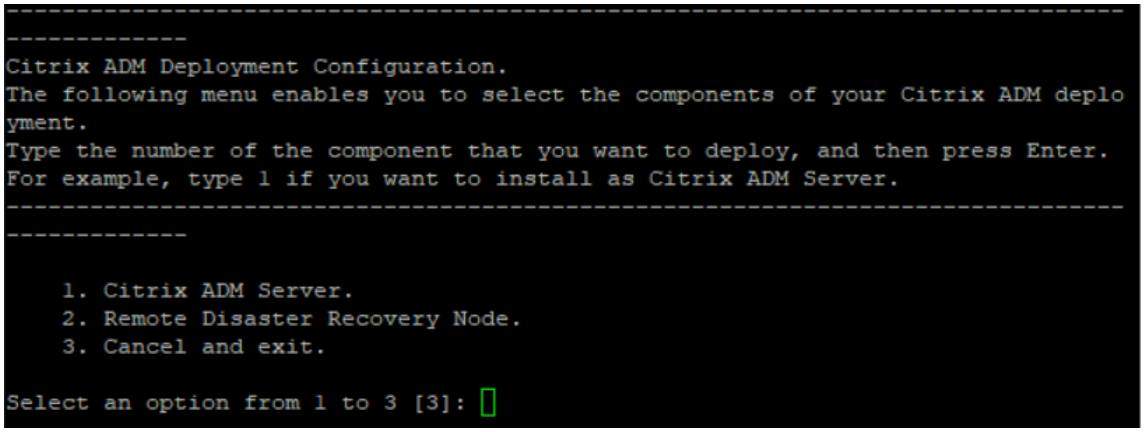


> **Remarque**
>
> Une fois que vous ouvrez une session, si vous souhaitez mettre à jour la configuration réseau initiale, tapez `networkconfig`, mettez à jour la configuration et enregistrez la configuration.

4. Exécutez le script de déploiement en saisissant la commande à l'invite du shell : `/mps/deployment_type.py`



5. Sélectionnez le type de déploiement **Citrix ADM Server**. Si vous ne sélectionnez aucune option, par défaut, elle est déployée en tant que serveur.



6. Tapez**Oui**pour déployer Citrix ADM en tant que déploiement autonome.
7. Tapez **Oui** pour redémarrer le serveur Citrix ADM.

> **Remarque**
>
> Après avoir installé Citrix ADM, vous pouvez mettre à jour les paramètres de configuration initiaux ultérieurement.

Vérification

Une fois le serveur installé, vous pouvez accéder à l'interface graphique en tapant l'adresse IP du serveur Citrix ADM dans le navigateur Web. Les informations d'identification d'administrateur par défaut pour se connecter au serveur sont nsroot/nsroot.

Le navigateur affiche l'utilitaire de configuration Citrix ADM.

Citrix ADM sur Microsoft Hyper-V

February 1, 2024

Pour installer Citrix ADM sur Microsoft Hyper-V, vous devez d'abord télécharger le fichier image Citrix ADM sur votre ordinateur local. Assurez-vous également que votre système dispose des extensions de virtualisation matérielle et vérifiez que les extensions de virtualisation du processeur sont disponibles.

Conditions préalables

Avant d'installer l'appliance virtuelle Citrix ADM, vérifiez que les conditions suivantes ont été remplies :

- Microsoft Hyper-V version 6.2 ou ultérieure est installé sur le matériel qui répond à la configuration minimale requise.
- Installez Microsoft Hyper-V Manager sur un poste de travail de gestion qui répond à la configuration système minimale requise.
- Vous avez téléchargé le fichier image Citrix ADM.

Configuration système requise pour Microsoft Hyper-V

Microsoft Hyper-V est une application cliente Windows. Le tableau suivant décrit la configuration minimale requise.

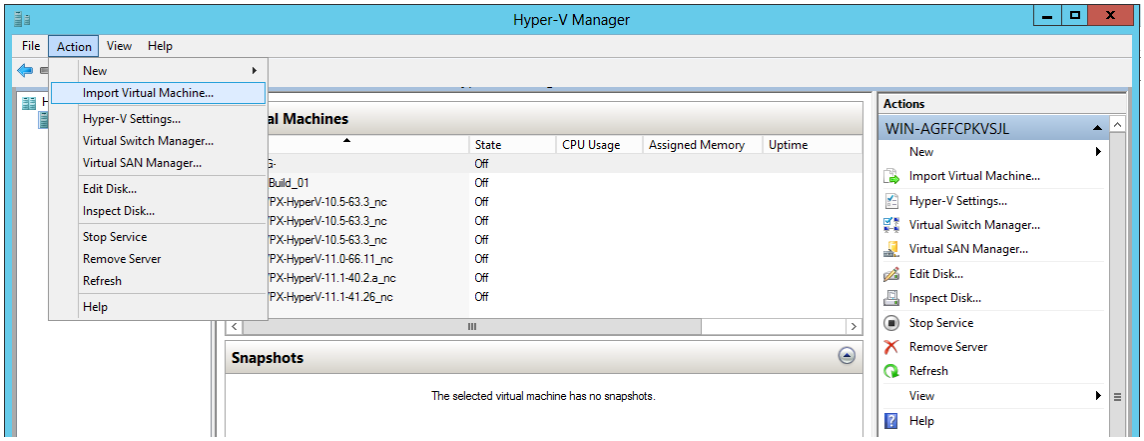
Composant	Exigences
Système d'exploitation	Windows Server 2012 R2
.NET framework	Version 2.0 ou ultérieure
UC	750 MHz (MHz), recommandé : 1 gigahertz (GHz) ou plus rapide
RAM	1 Go, Recommandé : 2 Go
Carte d'interface réseau	Carte réseau 100 mégabits par seconde (Mbps) ou plus rapide

Installation de Citrix Application Delivery Management

Le nombre de serveurs Citrix ADM que vous pouvez installer dépend de la mémoire disponible sur le serveur Hyper-V.

Pour installer Citrix ADM :

1. Démarrez le client Hyper-V Manager sur votre station de travail.
2. Dans le menu **Action**, cliquez sur **Importer une machine virtuelle**.



3. Importez l'image Hyper-V et procédez comme suit :

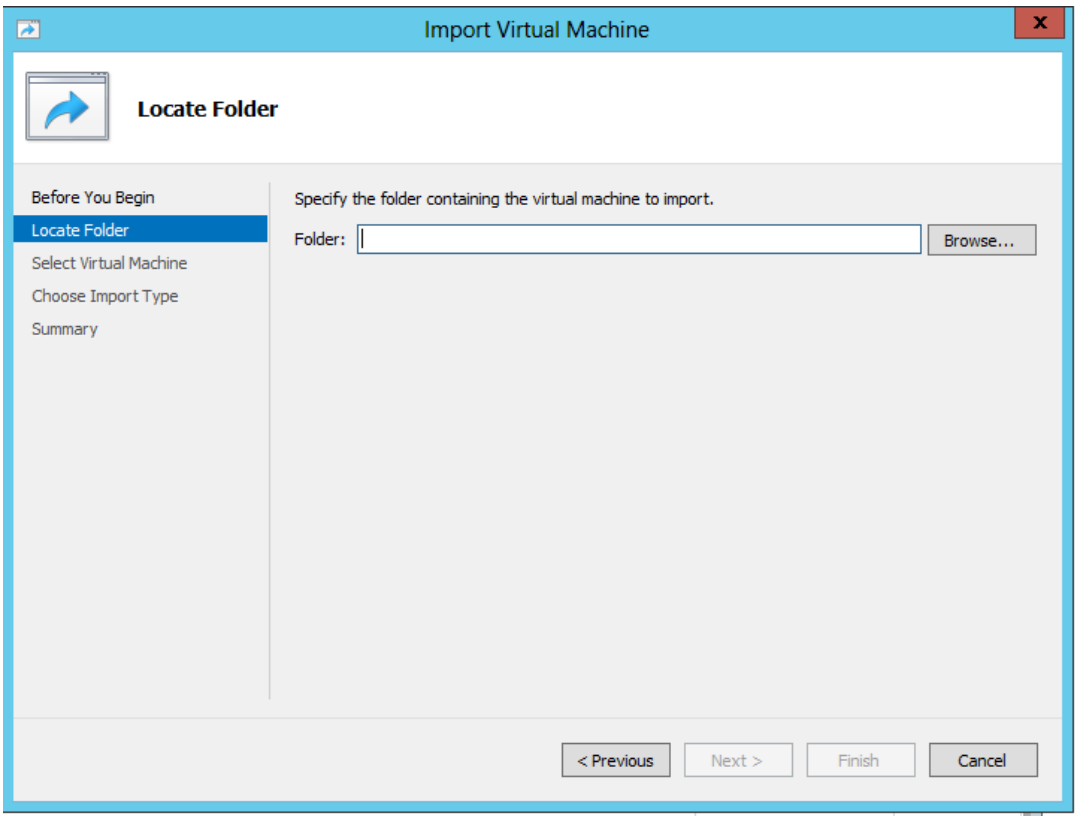
   a) Dans la boîte de dialogue Importer une machine virtuelle, dans la section **Localiser** un dossier, accédez au dossier dans lequel vous avez enregistré l'image Citrix ADM Hyper-V, sélectionnez le dossier et cliquez sur **Suivant**.

   b) Dans la section Sélectionner une machine virtuelle, sélectionnez le nom de la machine virtuelle appropriée.

   c) Dans la section **Choisir le type d'importation**, sélectionnez l'option Copier la machine virtuelle (créer un nouvel identifiant unique) et cliquez sur Suivant.

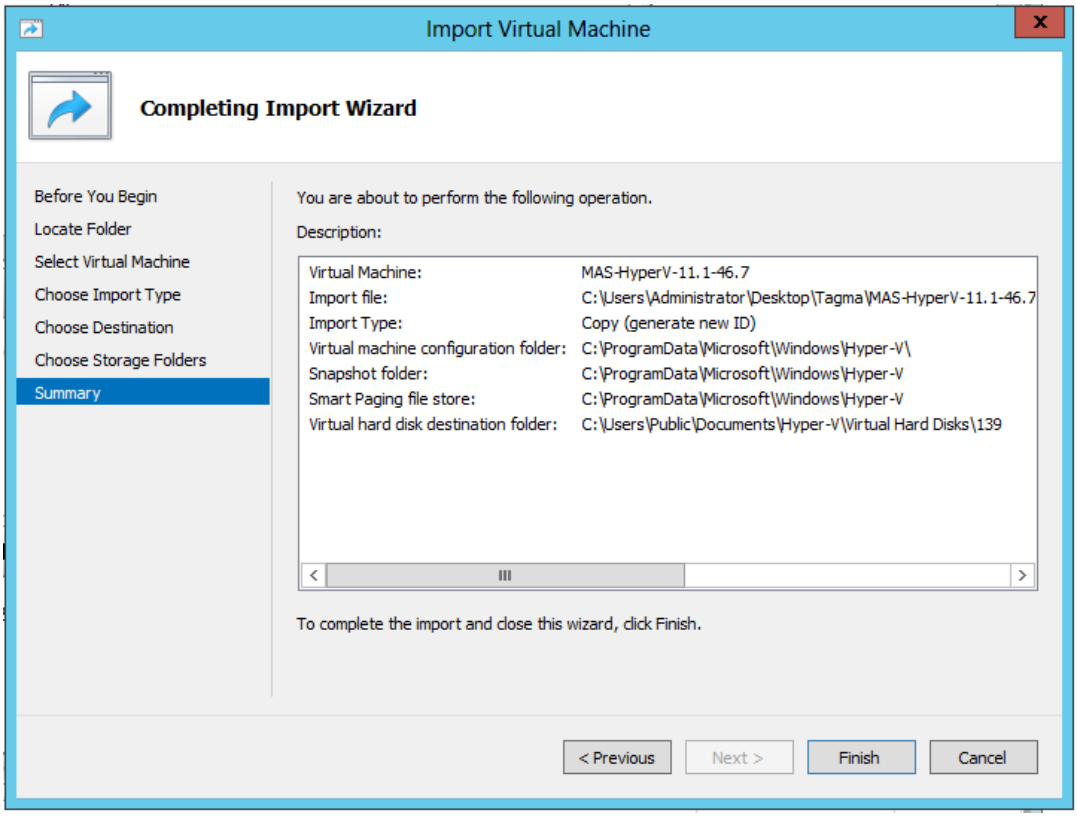
   d) Dans la section **Choisir une destination**, vous pouvez spécifier les dossiers dans lesquels stocker les fichiers de la machine virtuelle.

   > **Remarque**
   >
   > Par défaut, l'assistant importe les fichiers de la machine virtuelle dans les dossiers Hyper-V par défaut de votre hôte local.



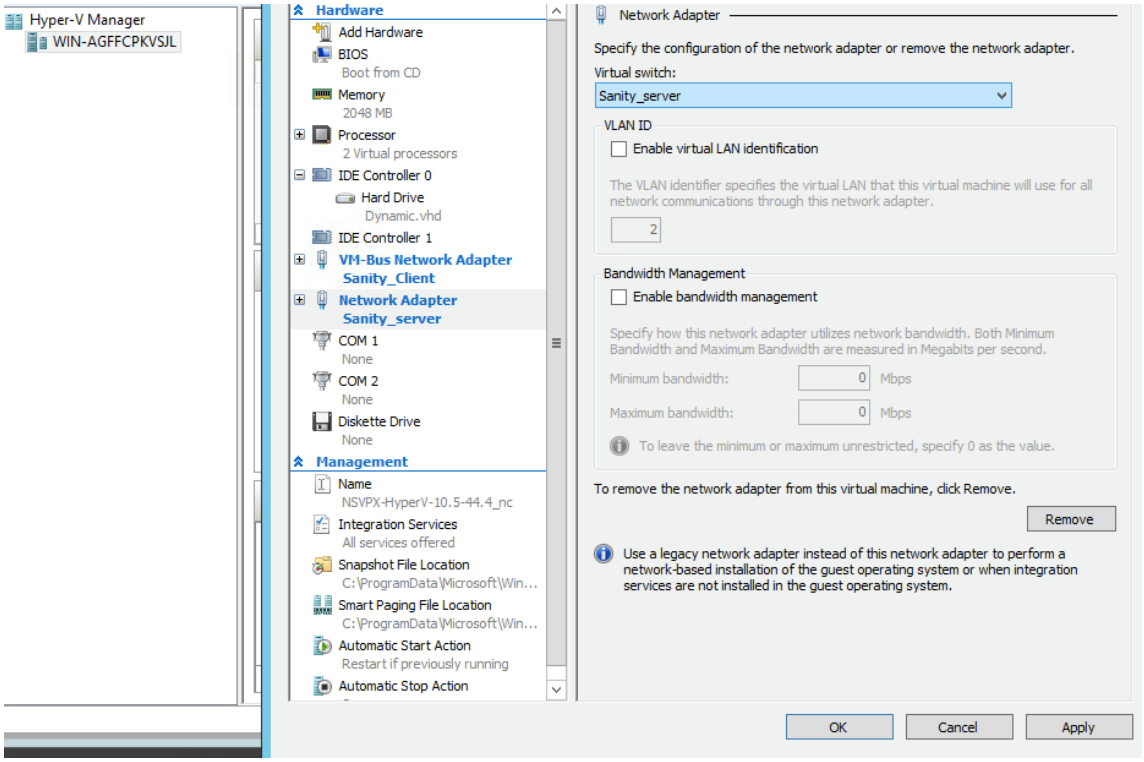
e) Dans la section **Choisir les dossiers de stockage**, vous pouvez sélectionner l'emplacement dans lequel vous souhaitez stocker les disques durs virtuels, puis cliquer sur **Suivant**.

f) Vous pouvez vérifier les détails de la machine virtuelle dans le volet récapitulatif, cliquez sur **Terminer**.

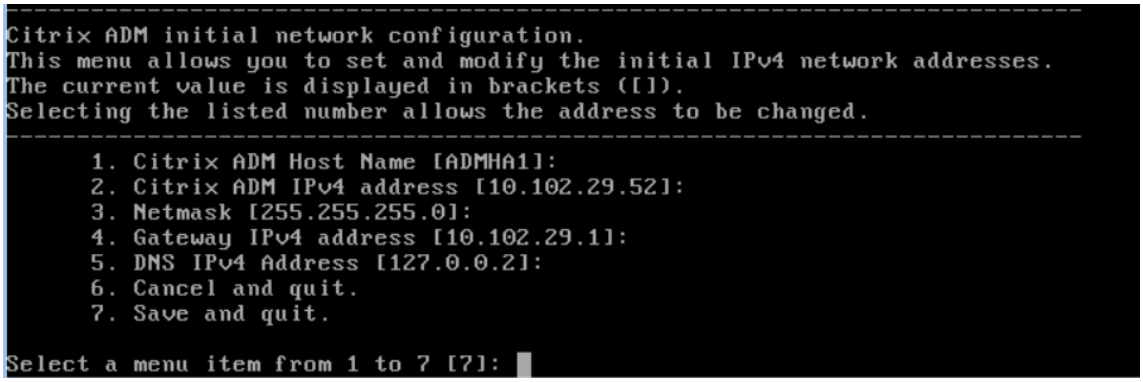


L'image Citrix ADM Hyper-V s'affiche dans le volet droit.

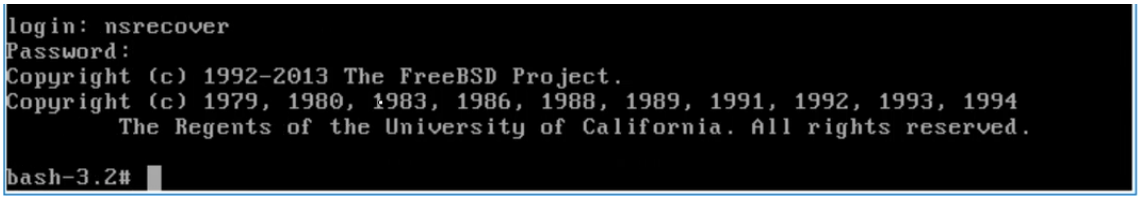
4. Cliquez avec le bouton droit sur l'image Citrix ADM Hyper-V, puis cliquez sur **Paramètres**.
5. Dans le volet gauche de la boîte de dialogue qui s'affiche, accédez à **Matériel** > **VM_Bus Network Adaptor**et, dans le volet droit, sélectionnez le réseau approprié dans la liste Réseau.



6. Cliquez sur **Appliquer**, puis sur **OK**.
7. Cliquez avec le bouton droit sur l'image Citrix ADM Hyper-V, puis cliquez sur **Connecter**.
8. Dans la fenêtre de la console, cliquez sur le bouton **Démarrer**.
9. Configurez les options de configuration réseau initiales.



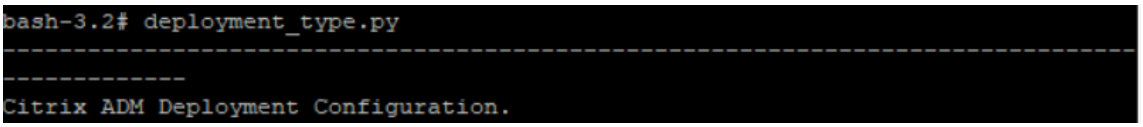
10. Après avoir spécifié les adresses IP requises, enregistrez les paramètres de configuration.
11. Lorsque vous y êtes invité, ouvrez une session à l'aide des informations d'identification nsrecover/nsroot.



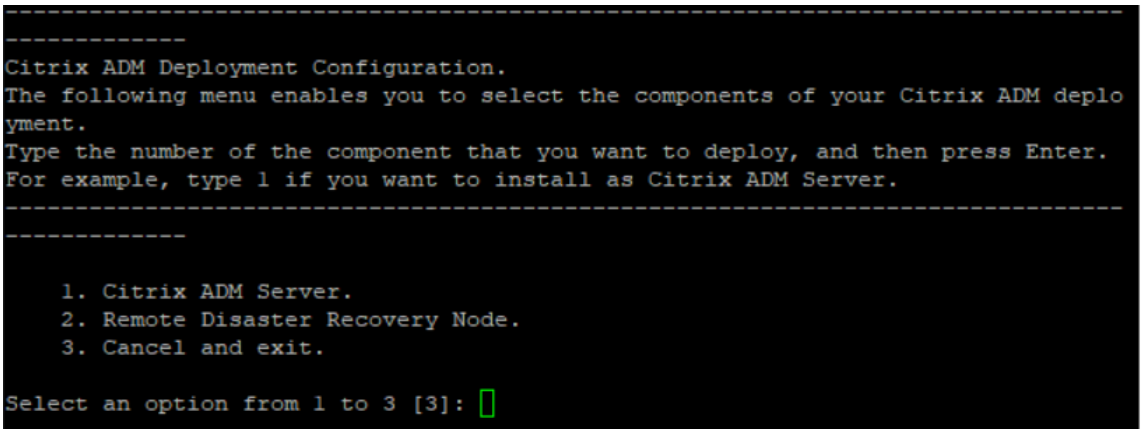
> **Remarque**
>
> Une fois que vous ouvrez une session, si vous souhaitez mettre à jour la configuration réseau initiale, tapez `networkconfig`, mettez à jour la configuration et enregistrez la configuration.

12. Exécutez le script de déploiement en saisissant la commande à l'invite du shell :

```
deployment_type.py
<!--NeedCopy-->
```



13. Sélectionnez le type de déploiement **Citrix ADM Server**. Si vous ne sélectionnez aucune option, par défaut, elle est déployée en tant que serveur.



14. Tapez **Oui** pour déployer Citrix ADM en tant que déploiement autonome.
15. Tapez **Oui** pour redémarrer le serveur Citrix ADM.

> **Remarque**
>
> Après avoir installé Citrix ADM, vous pouvez mettre à jour les paramètres de configuration initiaux ultérieurement.

Vérification

Une fois le serveur installé, vous pouvez accéder à l'interface graphique en tapant l'adresse IP du serveur Citrix ADM dans la barre d'adresse de votre navigateur. Les informations d'identification d'administrateur par défaut pour se connecter au serveur sont nsroot/nsroot.

Le navigateur affiche l'utilitaire de configuration Citrix ADM.

Citrix ADM sur VMware ESXi

February 1, 2024

Pour installer des appliances virtuelles Citrix ADM sur VMware ESXi, utilisez le client VMware vSphere.

Conditions préalables

Avant de commencer l'installation d'un dispositif virtuel, vérifiez que les exigences suivantes sont les suivantes :

- Installez une version prise en charge de VMware ESXi (6.0, 6.5, 6.7 et 7.0).
- Installez VMware Client sur une station de travail de gestion qui répond à la configuration système minimale requise.
- Téléchargez les fichiers d'installation de Citrix ADM.

> Remarque
>
> VMotion est pris en charge uniquement à partir de **Citrix ADM 13.0 Build 47.22 ou version ultérieure**. Vous pouvez planifier et automatiser la migration du serveur ADM déployé sur un hyperviseur ESXi, y compris les configurations haute disponibilité vSphere et vSphere DRS.

Pour installer Citrix ADM

> **Remarque**
>
> Les étapes et les captures d'écran sont basées sur VMware ESXi version 6.0. L'interface graphique peut différer dans les autres versions d'ESXi. Le numéro de build 17325551 de VMware ESXi version 7.0.1c avec adaptateur VMXNET3 est pris en charge dans **Citrix ADM 13.0 71.40 ou version ultérieure**. Reportez-vous à la documentation VMware pour connaître les étapes spécifiques à la version.

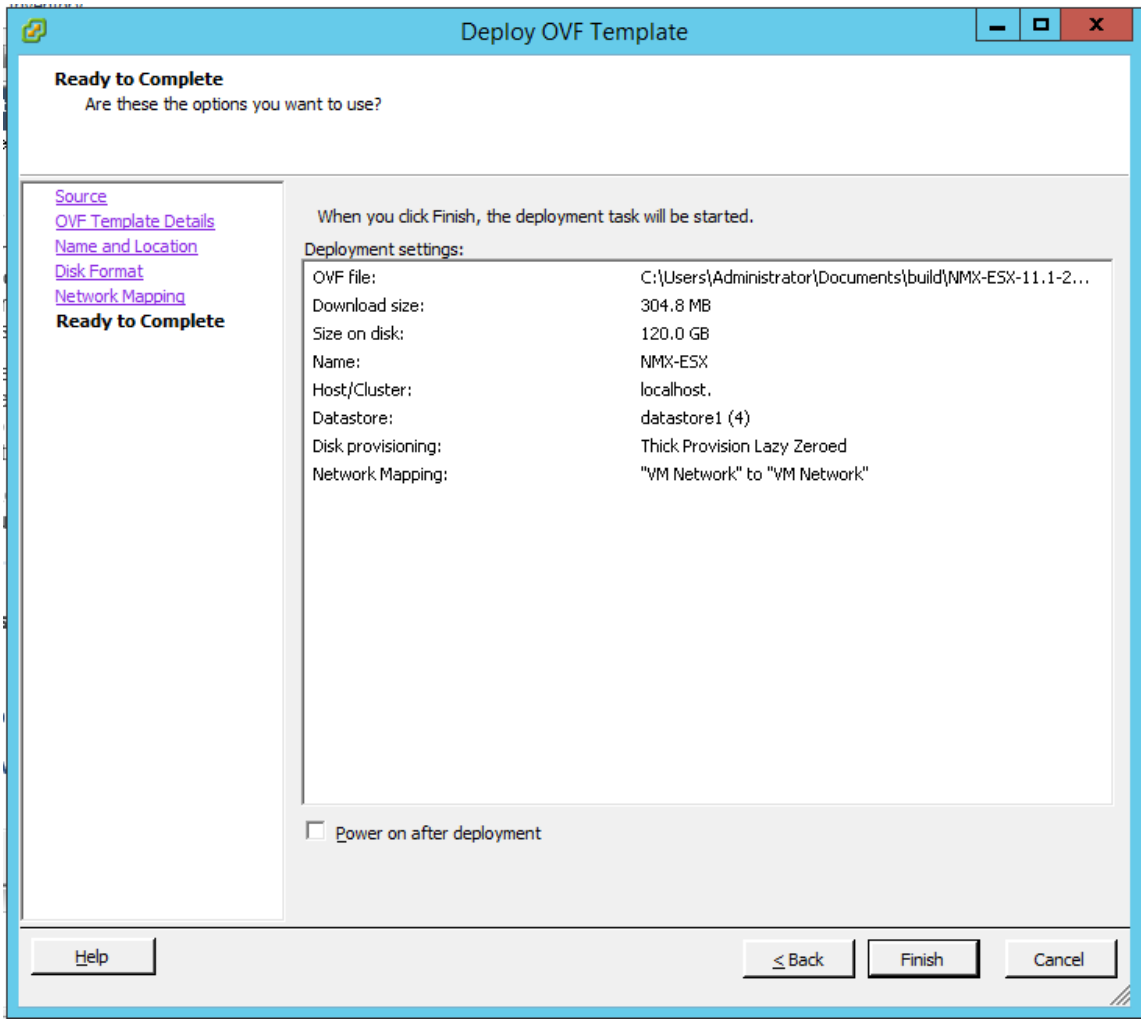
1. Démarrez le client VMware vSphere sur votre station de travail.
2. Dans la zone de texte **Adresse IP/Nom**, tapez l'adresse IP du serveur VMware ESXi auquel vous souhaitez vous connecter.
3. Dans les zones de texte **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification de l'administrateur, puis cliquez sur **Connexion**.
4. Dans le menu **Fichier**, cliquez sur **Déployer le modèle OVF**.
5. Dans la boîte de dialogue **Déployer le modèle OVF**, dans **Déployer à partir d'un fichier ou d'une URL**, sélectionnez le fichier .ovf, puis cliquez sur **Suivant**.

   > **Remarque**
   >
   > Si un message d'avertissement s'affiche avec le texte suivant : L'identificateur du système d'exploitation n'est pas pris en charge sur l'hôte sélectionné, vérifiez si le serveur VMware prend en charge le système d'exploitation FreeBSD. Cliquez sur **Oui**.

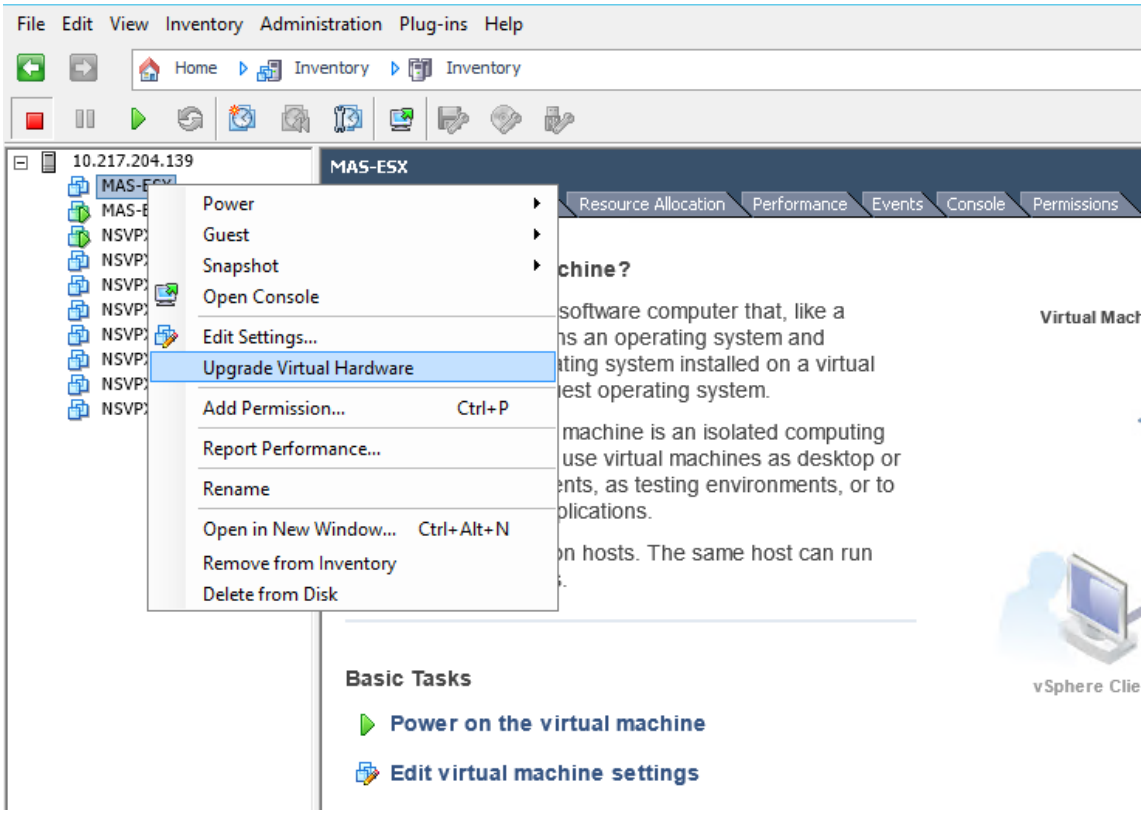
6. Sur la page **Détails du modèle OVF**, cliquez sur **Suivant**.
7. Tapez un nom pour l'appliance virtuelle Citrix ADM, puis cliquez sur **Suivant**.
8. Spécifiez le format de disque en sélectionnant le format provisionné fin ou le format provisionné épais.

   > **Remarque**
   >
   > Citrix vous recommande de sélectionner le **format provisionné Thick**.

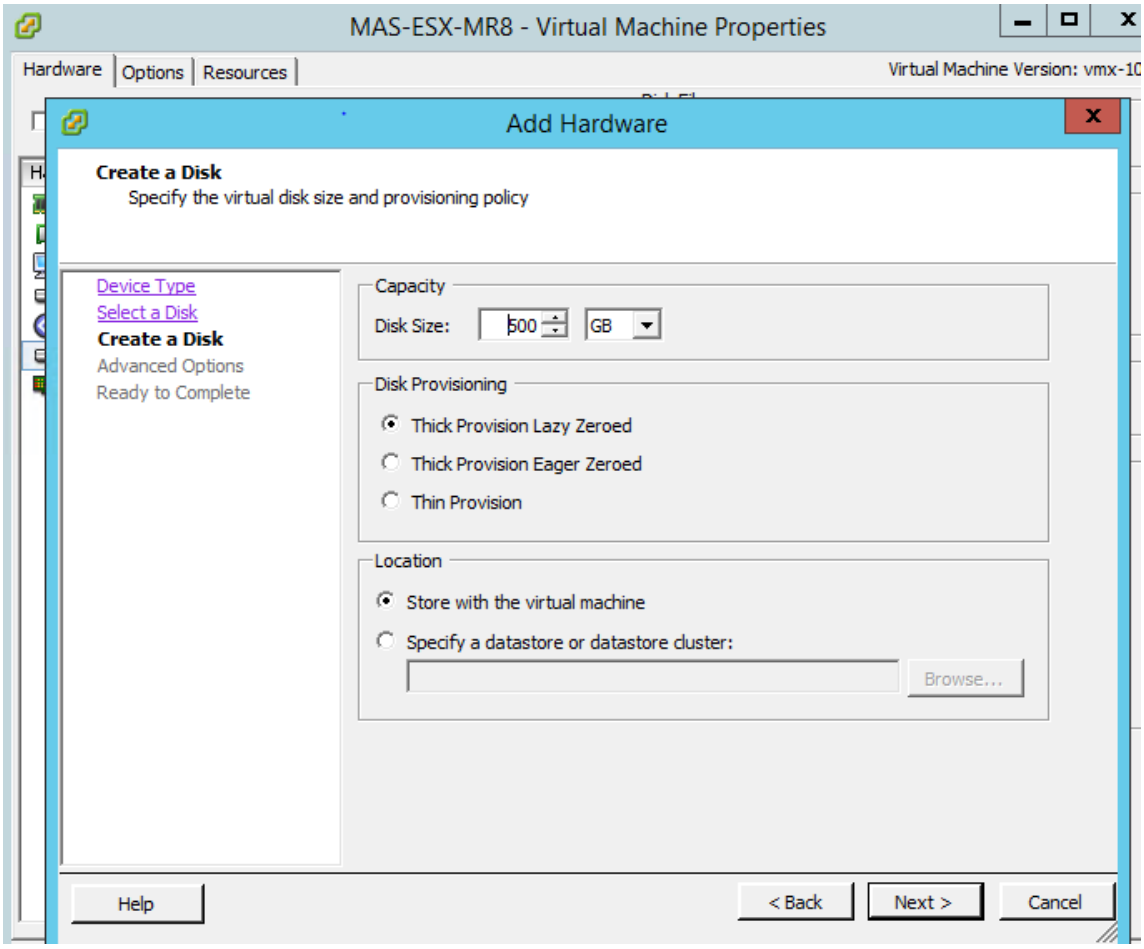
9. Cliquez sur **Terminer** pour démarrer le processus d'installation.



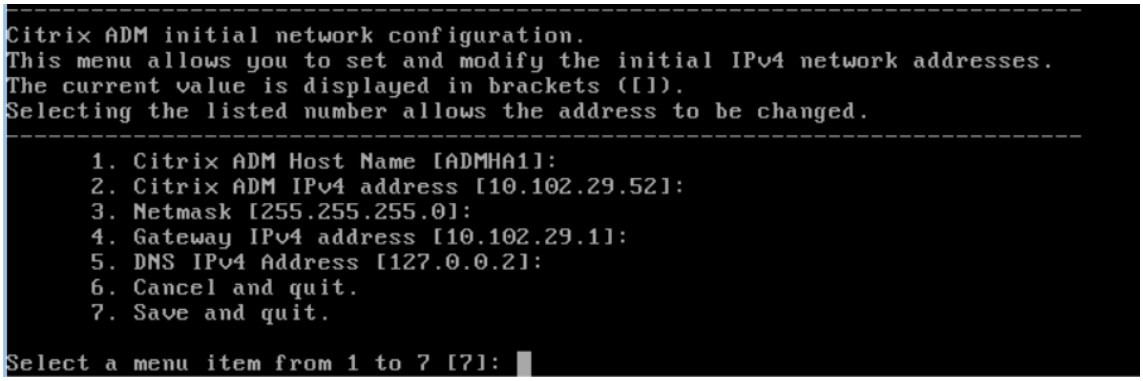
10. Vous êtes maintenant prêt à démarrer l'appliance virtuelle Citrix ADM.
11. Dans le volet de navigation, sélectionnez l'appliance virtuelle que vous avez installée. Dans le menu **Inventaire**, cliquez avec le bouton droit sur la **machine virtuelle**, puis cliquez sur **Mettre à niveau le matériel virtuel**. Dans la boîte de dialogue **Confirmer la machine virtuelle**, cliquez sur **Oui**.



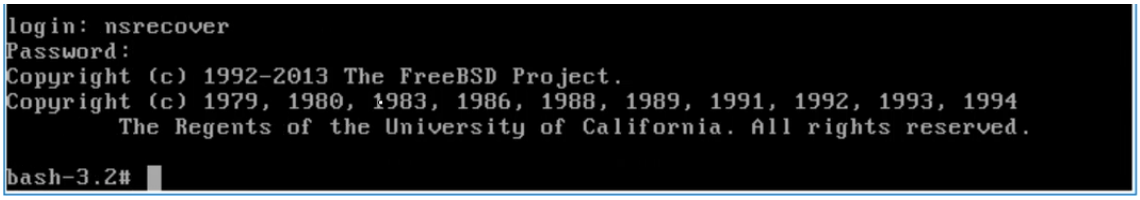
12. Dans le menu **Inventaire**, cliquez sur **Machine virtuelle**, puis sur **Modifier les paramètres**.
13. Dans la boîte de dialogue **Propriétés de la machine virtuelle**, sous l'onglet **Matériel**, cliquez sur **Mémoire**, puis dans le volet droit, spécifiez la **taille de la mémoire** sur 32 Go.
14. Cliquez sur **CPU**, puis dans le volet droit, spécifiez les processeurs sur 8. Cliquez sur **OK**.
15. Ajoutez un disque supplémentaire selon vos besoins.



16. Dans le volet de navigation, sélectionnez l'appliance virtuelle que vous avez installée. Dans le menu **Inventaire**, cliquez sur **Machine virtuelle**, sur **Power**, puis **sur Power On**.
17. Cliquez sur l'onglet **Console** pour afficher les options de configuration réseau initiale de Citrix ADM.



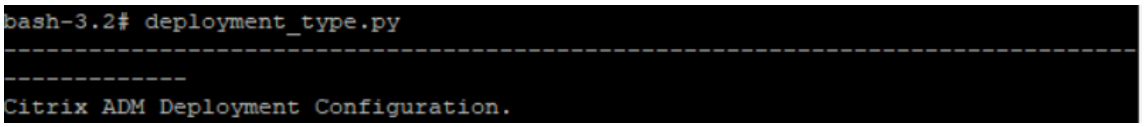
18. Après avoir spécifié les adresses IP requises, enregistrez les paramètres de configuration.
19. Lorsque vous y êtes invité, ouvrez une session à l'aide des informations d'identification nsrecover/nsroot.



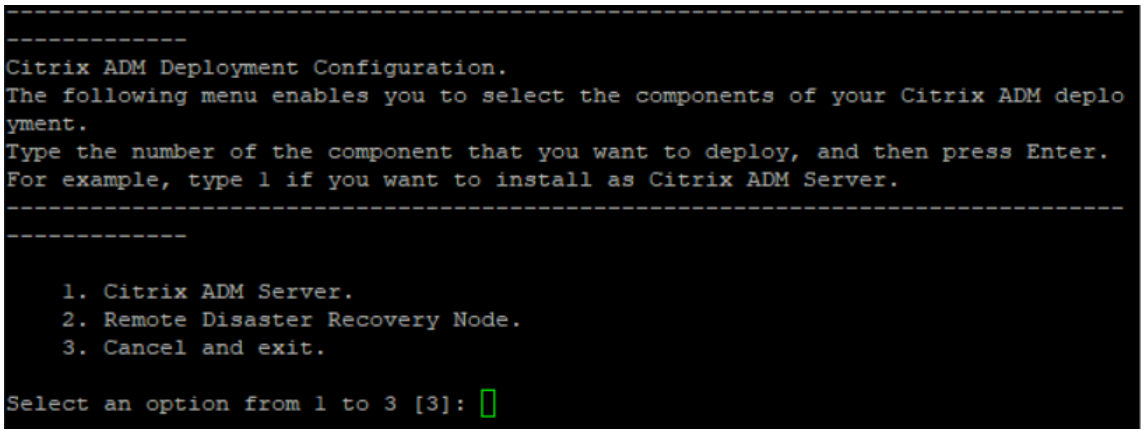
> **Remarque**
>
> Une fois que vous ouvrez une session, si vous souhaitez mettre à jour la configuration réseau initiale, tapez `networkconfig`, mettez à jour la configuration et enregistrez la configuration.

20. Exécutez le script de déploiement en saisissant la commande à l'invite du shell :

```
deployment_type.py
<!--NeedCopy-->
```



21. Sélectionnez le type de déploiement **Citrix ADM Server**. Si vous ne sélectionnez aucune option, par défaut, elle est déployée en tant que serveur.



22. Tapez**Oui**pour déployer Citrix ADM en tant que déploiement autonome.
23. Tapez **Oui** pour redémarrer le serveur Citrix ADM.

> **Remarque**
>
> Après avoir installé Citrix ADM, vous pouvez mettre à jour les paramètres de configuration initiaux ultérieurement.

Vérification

Une fois le serveur installé, vous pouvez accéder à l'interface utilisateur graphique en saisissant l'adresse IP du serveur Citrix ADM dans le navigateur. Les informations d'identification d'administrateur par défaut pour se connecter au serveur sont nsroot/nsroot.

Le navigateur affiche l'utilitaire de configuration Citrix ADM.

> **Remarque**
>
> Le temps d'installation d'ADM est généralement d'environ 10 minutes sur VMware ESXi, mais cela peut prendre plus de temps sur certains systèmes.

Citrix ADM sur le cluster Kubernetes

February 1, 2024

Avant d'installer les dispositifs virtuels Citrix ADM sur un cluster Kubernetes, lisez la section sur les conditions préalables.

Conditions préalables

Assurez-vous que les conditions préalables suivantes sont remplies avant d'installer ADM.

Cluster Kubernetes

- Le cluster Kubernetes doit être de la version suivante ou supérieure :
  - Version du serveur v1.13
  - Version client v1.13

  Tapez la commande `kubectl version` pour vérifier la version.
- L'application Helm installée sur le cluster doit être de la version suivante ou supérieure.
  - Version du serveur v2.12.1
  - Version client v2.12.0

  Utilisez la commande `helm version` pour vérifier la version.
- Kubernetes cluster CNI (Container Network Interface) doit être Calico version v3.1.3 ou supérieure.

- Tous les nœuds subordonnés du cluster doivent avoir un client NFS installé sur eux. En effet, l'application ADM persiste les données et la configuration sur les volumes montés sur un serveur de fichiers réseau. Pour installer un client NFS sur un subordonné Ubuntu, tapez les commandes suivantes :

```
apt-get update
apt install nfs-common
```

- L'application ADM a besoin de 32 Go de mémoire et de 8 vCPU sur le cluster et de 120 Go d'espace sur NFS.

Partage NFS

L'application ADM a besoin de volumes persistants pour stocker des données telles que la configuration, les certificats, les images et autres. Pour ce faire, ADM nécessite des montages NFS. L'application nécessite deux dossiers à partir des supports réseau partagés :

- Un pour stocker des fichiers tels que des certificats, des images et autres
- L'autre pour la base de données

> Remarque
>
> Il est recommandé d'avoir un NFS avec un SSD.

Ces deux dossiers peuvent être différents ou identiques. Les deux dossiers doivent disposer d'autorisations 777. Le premier dossier doit avoir un espace minimum de 10 Go. La taille du second dossier dépend de la quantité de données qui doit être persistante dans la base de données. La taille minimale est de 100 Go.
Pour l'environnement de production, nous recommandons d'avoir une solution NFS de qualité production.

Appliance Citrix ADC

L'appliance Citrix ADC est requise en tant que périphérique d'entrée. ADC met à disposition les services applicatifs requis en dehors du
cluster Kubernetes. L'appliance Citrix ADC doit être en dehors du cluster Kubernetes et les nœuds de travail doivent être accessibles depuis l'ADC. Procédez comme suit :

- Configurez un SNIP sur l'ADC. ADC utilise ce SNIP pour atteindre les nœuds de travail du cluster Kubernetes.
- Identifiez une adresse IP libre à utiliser comme adresse IP du serveur virtuel pour rendre les services applicatifs requis disponibles en dehors du cluster Kubernetes.

Installer ADM sur le cluster Kubernetes

Procédez comme suit pour installer une appliance ADM sur un cluster Kubernetes :

1. Accédez au site de téléchargement Citrix et téléchargez le fichier pour le graphique Helm Chart Citrix ADM pour Kubernetes.
2. Extrayez l'archive Helm Chart téléchargée dans le répertoire /var du nœud principal du cluster Kubernetes.
3. Ouvrez le `values.yaml` fichier sous le `/var/citrixadm` répertoire.
4. Entrez un mot de passe pour la base de données dans le champ `dbpasswd` du fichier.
5. Modifiez les valeurs suivantes. L'application ADM utilise ces valeurs pour configurer l'appliance Citrix ADC afin que les services soient exposés au monde externe :

   - `ingressIP` : une adresse IP virtuelle configurée dans Citrix ADC pour accéder à l'application.
   - `applicationID` : ID unique permettant de distinguer la configuration d'entrée du reste de la configuration sur l'appliance Citrix ADC.
   - `ingressADCIP` : adresse IP (NSIP) Citrix ADC, qui est utilisée comme entrée pour l'application ADM.
   - `ingressADCUsername`: nom d'utilisateur permettant d'accéder à l'appliance Citrix ADC. Cet utilisateur doit disposer de privilèges d'écriture.
   - `ingressADCPassword` : Mot de passe pour le nom d'utilisateur.

   ```
   # ingressIP is the Virtual IP configured in the Citrix ADC for accessing the application
   ingressIP: "xx.xx.xx.xx"

   # coreDumpFilePath is the directory on slave nodes of the cluster which will be used to store core dumps files in case
   application runs into faulty state
   # this setting is optional
   # Admin needs to create this directory on each of the slave nodes and then run the command: "echo <coreDumpFilePath_value>/
   core.%h.%e.%p > /proc/sys/kernel/core_pattern"
   coreDumpFilePath: "/var/mps/cores"

   # applicationID is the identifier for ingress configuration
   applicationID: "citrixadm"

   # ingressADCIP is the NSIP of the northbound ADC used to expose the ADM application to the outside world
   ingressADCIP: "xx.xx.xx.xx"

   # ingressADCUsername is the username of the northbound ADC
   ingressADCUsername: "nsroot"

   # ingressADCUsername is the password for above username
   ingressADCPassword: "nsroot"
   ```

6. Modifiez les valeurs suivantes dans la section **Stockage** . Ces valeurs spécifient la persistance requise pour stocker les fichiers requis par l'application ADM.

   - `nfsServer`: nom d'hôte ou adresse IP du serveur NFS
   - `path`: montez le chemin d'accès au dossier pour stocker les fichiers d'application.
   - `size`: au moins 10 Go.

> Remarque
>
> L'unité pour cette valeur est Gi. Par exemple, 10Gi, 20Gi.

7. Accédez à la section **Stockage** sous `pg-datastore` et modifiez les valeurs suivantes. Ces valeurs spécifient la persistance utilisée pour créer une base de données.
   - `nsfServer`: nom d'hôte ou adresse IP du serveur NFS.
   - `size` : montez un chemin d'accès pour le dossier utilisé pour la banque de données.
   - `path`: au moins 100 Go.

   > Remarque
   >
   > L'unité pour cette valeur est Gi. Par exemple, 100Gi, 200Gi.

8. Accédez au répertoire /var/citrix du nœud principal et exécutez la commande suivante pour installer une application ADM :
   `helm install -n citrixadm --namespace <name> ./citrixadm`

   > Remarque
   >
   > Cette commande de barre n'est pas prise en charge dans la version 3.x de barre.

   Cette commande installe également les espaces requis dans votre cluster. L'argument espace de noms est facultatif. Si aucun espace de noms n'est fourni, Helm installe ADM dans l'espace de noms par défaut. Pour faciliter la gestion, installez ADM dans un espace de noms distinct.

9. Ouvrez votre navigateur, saisissez `http://< virtual server IP address >` et connectez-vous à ADM en utilisant `nsroot`/`nsroot` comme informations d'identification. Pour un type d'accès sécurisé `https://< virtual server IP address >`.

> Remarque
>
> Au cours du déploiement, l'application ADM crée des tables dans la banque de données, ce qui peut prendre un certain temps. Selon les ressources allouées par Kubernetes aux différents espaces de l'application ADM, la mise en place du service peut prendre entre 5 et 15 minutes.

Citrix ADM sur le serveur KVM Linux

February 1, 2024

Les plates-formes de virtualisation sur lesquelles Citrix Application Delivery Management (ADM) peut être provisionné incluent Linux-KVM.

Avant d'installer Citrix ADM sur Linux-KVM, assurez-vous que votre système dispose des extensions de virtualisation matérielle et vérifiez que les extensions de virtualisation du processeur sont disponibles. Vérifiez que `virsh` (un outil de ligne de commande pour gérer les machines virtuelles) est disponible sur l'hyperviseur.

Utilisez vos informations d'identification d'administrateur pour vous connecter au site Web Citrix.com, accéder aux derniers fichiers d'installation de Citrix ADM et les télécharger sur votre ordinateur. Ensuite, installez Citrix ADM sur votre plate-forme Linux-KVM et configurez-le pour votre réseau.

Conditions préalables

Avant d'installer l'appliance virtuelle Citrix ADM, vérifiez que Linux-KVM version 3.6.11-4 et ultérieure est installée sur du matériel répondant à la configuration minimale requise.

Configuration matérielle requise

Composant	Exigences
UC	Processeur x86 64 bits doté des fonctionnalités de virtualisation matérielle incluses dans le processeur Intel VT-X. Fournissez au moins 2 cœurs de CPU pour héberger Linux-KVM. **Remarque** Pour vérifier si votre CPU prend en charge l'hôte Linux, entrez la commande suivante à l'invite du shell Linux hôte : `*. egrep'^flags.\* ( vmx | svm )' /proc/cpuinfo*` Si les paramètres du BIOS de l'extension sont désactivés, vous devez les activer dans le BIOS. Il n'y a pas de recommandation spécifique pour la vitesse du processeur, mais plus la vitesse est élevée, plus les performances du Citrix ADM sont meilleures.
Mémoire (RAM)	Minimum 4 Go pour le noyau Linux hôte. Ajoutez de la mémoire supplémentaire selon les besoins des machines virtuelles.

Composant	Exigences
Disque dur	Calculez l'espace requis pour le noyau Host Linux et les machines virtuelles. Une seule machine virtuelle Citrix ADM nécessite 120 Go d'espace disque.

> **Remarque**
>
> Les besoins en mémoire et en disque dur spécifiés sont pour le déploiement de Citrix ADM sur la plate-forme OpenStack, étant donné qu'aucune autre machine virtuelle ne s'exécute sur l'hôte. La configuration matérielle requise pour OpenStack dépend du nombre de machines virtuelles qui s'y exécutent.

Configuration logicielle requise

Citrix recommande des noyaux plus récents, tels que la version 64 bits du noyau 3.6.11-4 ou une version ultérieure.

Configuration réseau requise Citrix ADM prend en charge une seule interface réseau paravirtualisée VirtiO. Assurez-vous de connecter cette interface au réseau de gestion de l'hôte Linux-KVM, afin que Citrix ADM et Linux-KVM puissent communiquer.

Télécharger les fichiers d'installation de Citrix ADM

Pour télécharger les fichiers d'installation de Citrix ADM à partir de www.citrix.com :

1. Ouvrez un navigateur Web et saisissez www.citrix.com dans la barre d'adresse.
2. Passez la souris sur **l'option Connexion** et cliquez sur **My Account**, entrez vos informations d'identification Citrix, puis cliquez à nouveau sur **Connexion**.
3. Accédez à la section **Téléchargements**.
4. Dans la liste **Téléchargements**, sélectionnez **Citrix Application Delivery Management**.
5. Sur la page **Citrix Application Delivery Management**, sélectionnez la version. Par exemple, sélectionnez **Version 13.0**.
6. Cliquez sur **Logiciel produit** pour le développer, puis cliquez sur la dernière version. Par exemple, sélectionnez **NetScaler MAS Release (Feature Phase) 13.0**Build 36.27.

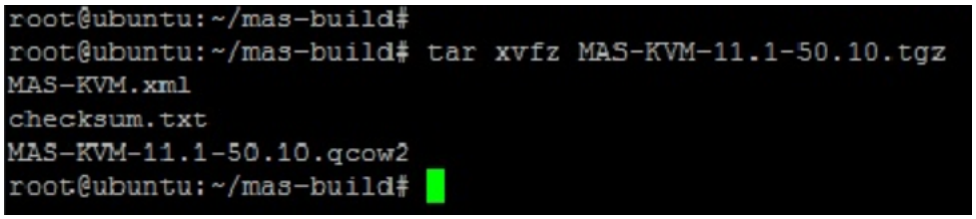
   La page de construction sélectionnée s'affiche.

7. Dans la liste **Saut au téléchargement**, sélectionnez **NetScaler MAS image pour KVM, 13.0 Build xx.xx**
8. Cliquez sur **Télécharger le fichier**, acceptez le CLUF et téléchargez le fichier image compressée dans n'importe quel dossier de votre ordinateur local.

Installer Citrix Application Delivery Management sur Linux-KVM

1. À l'aide de SSH, connectez-vous à l'hôte KVM.
2. À l'invite de l'interface de ligne de commande, à l'aide de l'un des programmes de transfert de fichiers, copiez l'image dans un dossier sur le serveur.
3. Accédez au répertoire dans lequel vous avez enregistré l'image téléchargée.
4. Exécutez les opérations suivantes sur la ligne de commande :
   a) Répertorier les fichiers dans le répertoire vérifier la présence du fichier image.
   b) Utilisez la commande tar pour dégouter le fichier image Citrix Application Delivery Management. Le paquet décompressé contient les composants suivants :
      i. Fichier XML de domaine spécifiant les attributs Citrix ADM
      ii. Fichier texte qui spécifie la somme de contrôle de l'image disque de domaine
      iii. Une image disque de domaine

```
tar -xvfz MAS-KVM.tgz
MAS-KVM.xml
MAS-KVM.qcow2
checksum.txt
<!--NeedCopy-->
```



      iv. Créez une copie de mas-kvm.xml en tant que mas1-kvm.xml, en tant qu'option de sauvegarde. Ouvrez le fichier MAS1-KVM.xml à l'aide de l'éditeur vi.
      v. Modifiez Mas1-kvm.xml pour les attributs réseau suivants :
         A. `name` - Indiquez le nom.
         B. `mac` - Spécifiez l'adresse MAC.
         C. `source file` - Spécifiez le chemin d'accès absolu de la source de l'image disque. Le chemin du fichier doit être absolu.

> **Remarque**
>
> Le nom de domaine et l'adresse MAC doivent être uniques.

D. `mode` - Spécifie le mode.

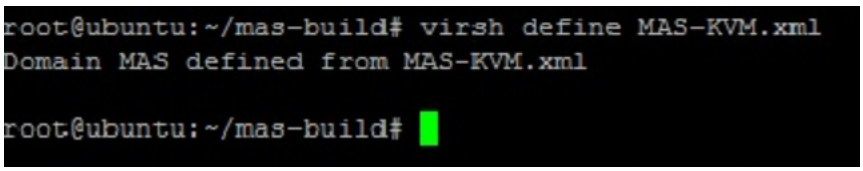
E. `model type` - Réglez sur virtIO.

F. `source dev` - Spécifiez l'interface.

```
<name> MAS1-KVM</name>
<mac address='52:54:00:29:74:b3'/>
<source file='/var/ MAS-KVM.qcow2'/>
<source dev='eth0' mode='bridge'/>
<model type='virtio'/>
<!--NeedCopy-->
```

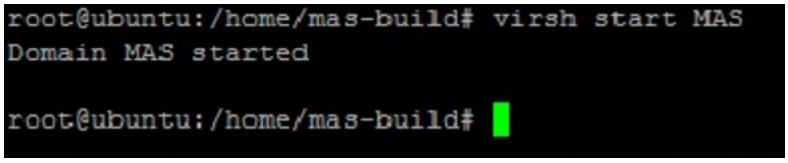
vi. Définissez les attributs de machine virtuelle dans le fichier MAS1-KVM.xml à l'aide de la commande suivante : `virsh define \<FileName\>.xml`

```
virsh define MAS-KVM.xml
Domain MAS defined from MAS-KVM.xml
<!--NeedCopy-->
```



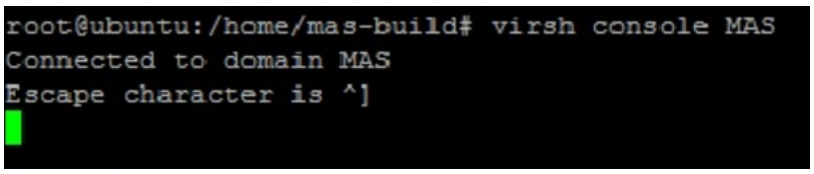
vii. Démarrez Citrix ADM en entrant la commande suivante : `virsh start \[\<DomainName\> | \<DomainUUID\>\]`

```
virsh start MAS
Domain MAS started
<!--NeedCopy-->
```



viii. Vous pouvez vous connecter à la machine virtuelle Citrix ADM à l'aide de la commande suivante : `virsh console \<DomainName\>`

```
virsh console MAS
Connected to domain MAS
Escape character is ^]
<!--NeedCopy-->
```

Configurer Citrix Application Delivery Management

> **Remarque**
>
> Sur certains hôtes KVM Linux, les invités FreeBSD ne parviennent pas à redémarrer correctement s'ils ont plusieurs CPU. Lorsque le dispositif virtuel Citrix ADM est redémarré, l'interface de ligne de commande et l'interface graphique Citrix ADM ne répondent plus. Pour plus de détails, voir https://bugs.launchpad.net/qemu/+bug/1329956
>
> Pour éviter que l'interface de ligne de commande et l'interface graphique Citrix ADM ne répondent plus lorsque le dispositif virtuel Citrix ADM est redémarré, arrêtez toutes les machines virtuelles sur l'hôte KVM et effectuez les opérations suivantes sur l'hôte KVM :
>
> 1. Supprimez le module kvm_intel à l'aide de la commande suivante :
>   `rmmod kvm\\_intel`
> 2. Désactivez **APICV** et rechargez le module kvm_intel à l'aide de la commande suivante :
>   `modprobe kvm\\_intel enable\\_apicv=N`
> 3. Démarrez les machines virtuelles sur l'hôte KVM.

Après avoir installé Citrix ADM, allouez environ 10 minutes pour que les services deviennent disponibles, puis ouvrez une session sur Citrix ADM.

1. Sur la ligne de commande, utilisez les informations d'identification par défaut de l'administrateur système pour ouvrir une session sur le système :
   - Nom d'utilisateur : `nsroot`
   - Mot de passe : `nsroot`

   > **Remarque**
   >
   > Après avoir ouvert une session pour la première fois, modifiez le mot de passe administratif. Ensuite, configurez le MAS pour qu'il fonctionne dans votre réseau. Vous pouvez modifier le mot de passe à partir de l'interface utilisateur Citrix ADM. Dans la page d'accueil de Citrix ADM, accédez à **Système** > **Administration** des **utilisateurs > Utilisateurs**. Sélectionnez l'utilisateur et cliquez sur **Modifier**, puis mettez à jour le mot de passe dans le champ Mot de passe.

2. À l'invite, tapez : *shell*

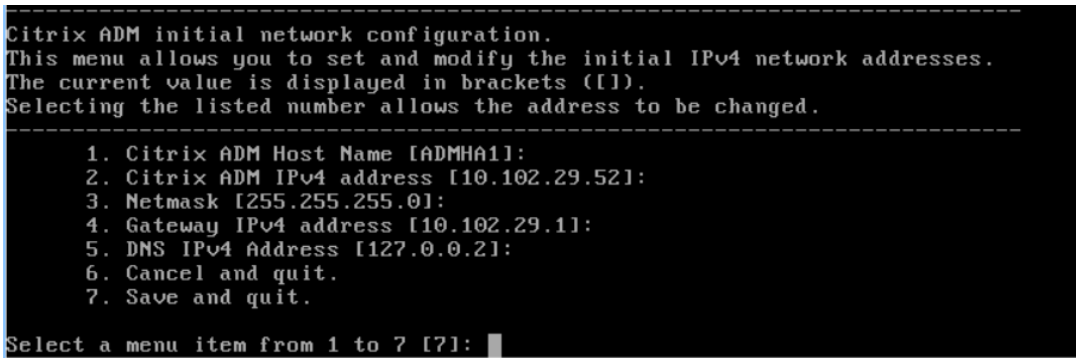
3. Tapez **networkconfig** pour entrer dans le menu de configuration réseau initiale Citrix ADM. Configurez l'adresse IP de gestion.
4. Pour terminer la configuration réseau initiale de Citrix ADM, suivez les instructions. La console affiche les options de configuration réseau initiale Citrix ADM permettant de définir les paramètres suivants pour Citrix ADM. Le nom d'hôte est renseigné par défaut.

    a) Entrez **2** pour mettre à jour Citrix ADM IPv4 adresse - adresse IP de gestion à laquelle vous accédez à un Citrix ADM

    b) Entrez **3** pour mettre à jour le masque de sous-réseau associé à l'adresse IP de gestion

    c) Entrez **4** pour mettre à jour l'adresse IPv4 de Gateway - adresse IP de passerelle par défaut pour le sous-réseau de l'adresse IP de gestion de l'Citrix ADM

    d) Entrez **7** pour enregistrer et quitter - enregistre vos modifications de configuration et quitte le système.

5. Exécutez le script de déploiement en saisissant la commande à l'invite du shell : `deployment_type.py`
6. Dans l'écran de déploiement qui s'affiche, sélectionnez le type de déploiement en tant que **serveur Citrix ADM**.

7. Tapez **Oui** pour déployer Citrix ADM en tant que déploiement autonome.

8. Tapez **Oui** pour redémarrer le serveur Citrix ADM.
9. Après le redémarrage du serveur ADM Citrix, ouvrez une session sur Citrix ADM en utilisant les informations d'identification par défaut de l'administrateur comme nsroot/nsroot via la ligne de commande ou l'interface graphique.

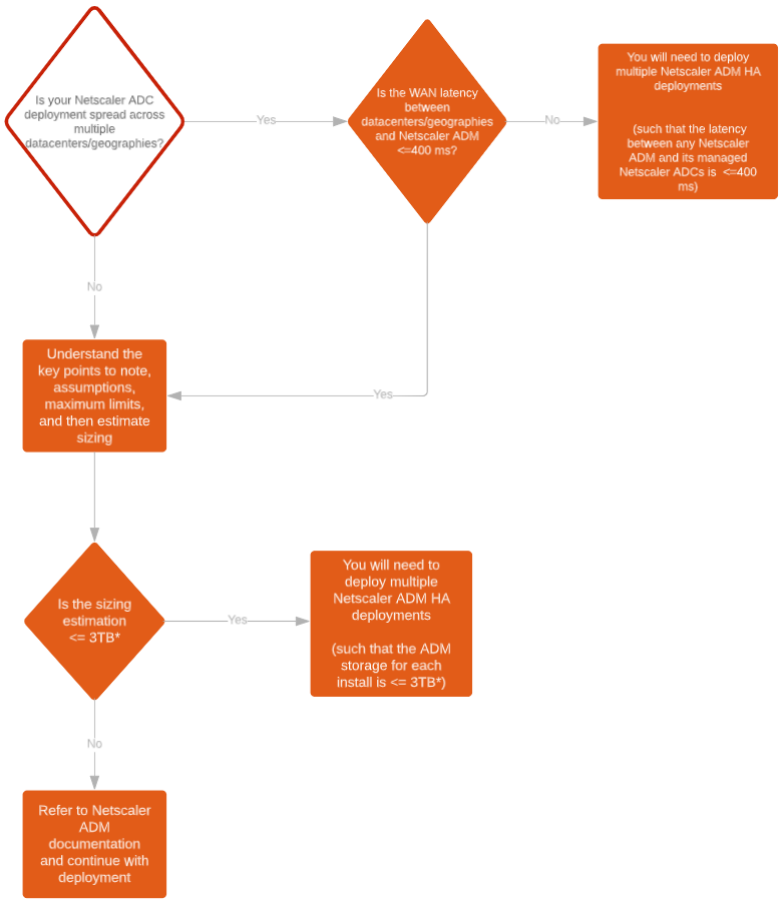
   Vous pouvez accéder ultérieurement à Citrix ADM en tapant l'adresse IP du serveur Citrix ADM dans la barre d'adresse de votre navigateur. Les informations d'identification d'administrateur par défaut pour se connecter au serveur sont *nsroot/nsroot* .

Configurer le déploiement haute disponibilité

February 1, 2024

La haute disponibilité (HA) fait référence à un système qui est toujours disponible pour un utilisateur sans aucune interruption des services. La configuration de haute disponibilité est cruciale lors des interruptions du système, des défaillances du réseau ou des applications, et constitue une exigence essentielle pour toute entreprise. Un déploiement haute disponibilité de deux nœuds Citrix ADM en mode actif-passif avec les mêmes configurations garantit des opérations ininterrompues.

Scénario de déploiement



> **Remarque**
>
> La limite de stockage maximale validée pour un seul déploiement Citrix ADM HA est de 3 To. Pour plus d'informations, consultez le guide de déploiement.
>
> **Important**
>
> **Pour accéder à Citrix ADM 12.1 build 48.18 ou à des versions ultérieures à l'aide du protocole HTTPS :**
>
> Si vous avez configuré une instance Citrix ADC pour équilibrer la charge de Citrix ADM en mode haute disponibilité, supprimez d'abord l'instance Citrix ADC. Configurez ensuite une adresse IP flottante pour accéder à Citrix ADM en mode haute disponibilité.

Les avantages du déploiement de la haute disponibilité dans Citrix ADM sont les suivants :

- Un mécanisme amélioré pour surveiller les battements cardiaques entre le noeud principal et le noeud secondaire.
- Fournit une réplication en continu physique de la base de données au lieu d'une réplication

bidirectionnelle logique.

- Possibilité de configurer l'adresse IP flottante sur le nœud principal pour éliminer le besoin d'un équilibreur de charge Citrix ADC distinct.
- Permet d'accéder facilement à l'interface utilisateur de Citrix ADM à l'aide de l'adresse IP flottante.
- L'interface utilisateur Citrix ADM est fournie uniquement sur le nœud principal. En utilisant le nœud principal, vous pouvez éliminer le risque d'accéder au nœud secondaire et d'y apporter des modifications.
- La configuration de l'adresse IP flottante gère la situation de basculement et la reconfiguration des instances n'est pas nécessaire.
- Fournit la capacité intégrée de détecter et de gérer les situations de division cérébrale.

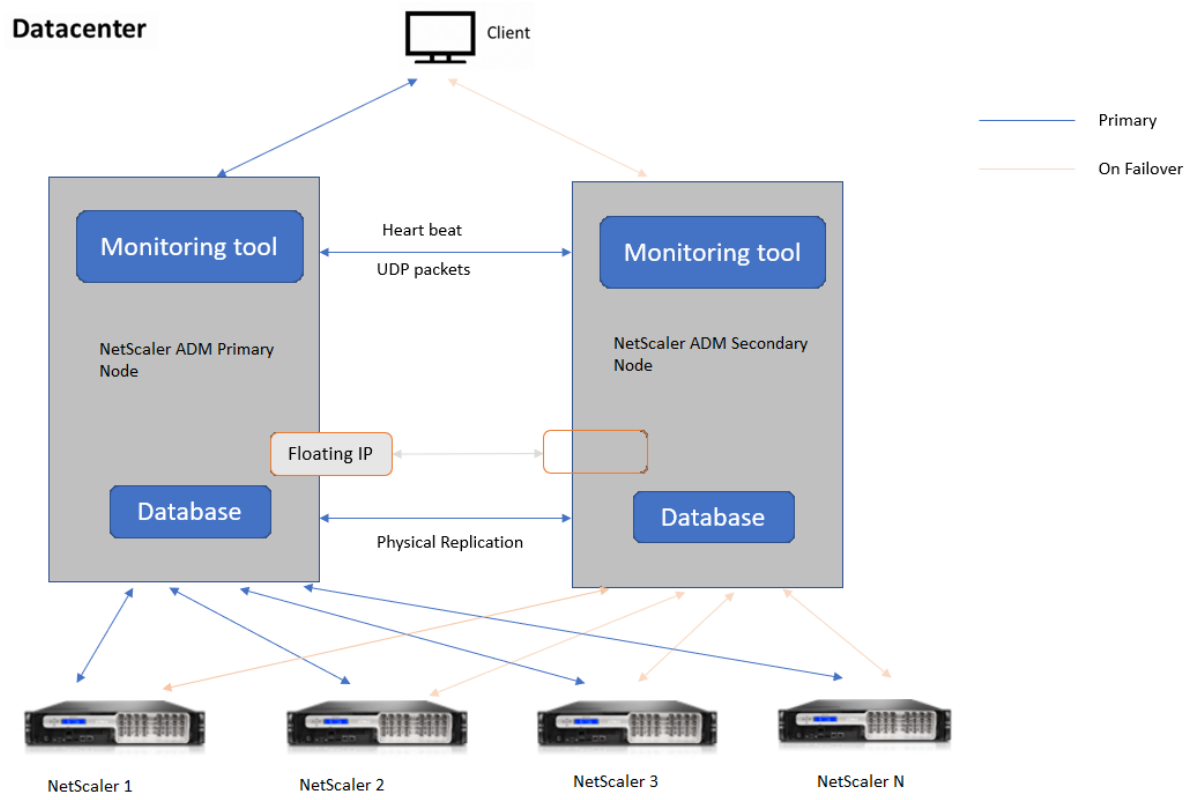
Le tableau suivant décrit les termes utilisés dans le cadre du déploiement à haute disponibilité.

Termes	Description
Nœud principal	Premier nœud enregistré dans le déploiement de haute disponibilité.
Nœud secondaire	Deuxième nœud enregistré dans le déploiement de haute disponibilité.
Battement de cœur	Mécanisme utilisé pour échanger des messages entre le nœud principal et le nœud secondaire dans la configuration de haute disponibilité. Les messages déterminent l'état et l'état de santé de l'application sur chaque nœud individuel.
Adresse IP flottante	Une adresse IP flottante est une adresse IP qui peut être déplacée instantanément d'un nœud à un autre dans le même sous-réseau. En interne, il est configuré en tant qu'alias sur l'interface réseau du nœud principal. En cas de basculement, l'adresse IP flottante est déplacée de manière fluide de l'ancien serveur principal vers le nouveau. Il est utile dans la configuration de haute disponibilité car il permet aux clients de communiquer avec les nœuds de haute disponibilité à l'aide d'une seule adresse IP.

> **Remarque**
>
> Pour plus d'informations sur les ports et les protocoles, reportez-vous à la section Ports.

Composants de l'architecture haute disponibilité

La figure suivante illustre l'architecture de deux nœuds Citrix ADM déployés en mode haute disponibilité.



Dans le déploiement à haute disponibilité, un nœud Citrix ADM est configuré en tant que nœud principal (MAS 1) et l'autre en tant que nœud secondaire (MAS 2). Si le nœud principal tombe en panne pour une raison quelconque, le nœud secondaire prend la relève en tant que nouveau nœud principal.

Outil de surveillance

L'outil de surveillance est un processus interne utilisé pour surveiller, alerter et gérer les situations de basculement. L'outil est actif et s'exécute sur chaque nœud en haute disponibilité. Il est chargé de démarrer les sous-systèmes, de lancer la base de données sur les deux nœuds, de choisir le nœud principal ou secondaire en cas de basculement, etc.

Nœud principal

Le nœud principal accepte les connexions et gère les instances. Tous les processus tels que AppFlow, SNMP, LogStream, syslog, etc. sont gérés par le nœud principal. L'accès à l'interface utilisateur Citrix ADM est disponible sur le nœud principal. L'adresse IP flottante est configurée sur le nœud principal.

Nœud secondaire

Le nœud secondaire écoute les messages de pulsation envoyés par le nœud principal. La base de données sur le nœud secondaire est en mode lecture réplica uniquement. Aucun des processus n'est actif sur le nœud secondaire et l'interface utilisateur Citrix ADM n'est pas accessible sur le nœud secondaire.

Réplication physique en continu

Les nœuds principal et secondaire se synchronisent par le biais d'un mécanisme de battement de cœur. Lors de la réplication physique en streaming de la base de données, le nœud secondaire démarre en mode lecture-réplique. Le nœud secondaire écoute les messages de pulsation reçus du nœud principal. Si le nœud secondaire ne reçoit aucun battement de cœur pendant une période de 180 secondes, le nœud principal est considéré comme étant en panne. Ensuite, le nœud secondaire prend le relais en tant que nœud principal.

Messages sur les battements cardiaques

Les messages de pulsation sont des paquets UDP (User Datagram Packets) qui sont envoyés et reçus entre le nœud principal et le nœud secondaire. Il surveille tous les sous-systèmes de Citrix ADM et de la base de données pour échanger des informations sur l'état, l'état du nœud, les processus, etc. Les informations sont partagées chaque seconde entre les nœuds haute disponibilité. Les notifications sont envoyées sous forme d'alertes à l'administrateur en cas de basculement ou de rupture des états de haute disponibilité.

Adresse IP flottante

L'adresse IP flottante est associée au nœud principal dans la configuration de haute disponibilité. Il s'agit d'un alias attribué à l'adresse IP du nœud principal, que le client peut utiliser pour se connecter à Citrix ADM sur le nœud principal. Étant donné que l'adresse IP flottante est configurée sur le nœud principal, la reconfiguration de l'instance n'est pas requise en cas de basculement. Les instances se reconnectent à la même adresse IP pour atteindre le nouveau serveur principal.

Points clés à noter

- Dans une configuration haute disponibilité, les deux nœuds Citrix ADM sont déployés en mode actif-passif. Ils doivent être sur les mêmes sous-réseaux utilisant la même version du logiciel et la même génération, et avoir les mêmes configurations.
- Adresse IP flottante :
  - L'adresse IP flottante est configurée sur le nœud principal.
  - Les instances n'ont pas besoin d'être reconfigurées en cas de basculement.
  - Vous pouvez accéder à un nœud haute disponibilité depuis l'interface utilisateur, soit en utilisant l'adresse IP du nœud principal, soit en utilisant l'adresse IP flottante.

    > **Remarque**
    >
    > Citrix vous recommande d'utiliser l'adresse IP flottante pour accéder à l'interface utilisateur.

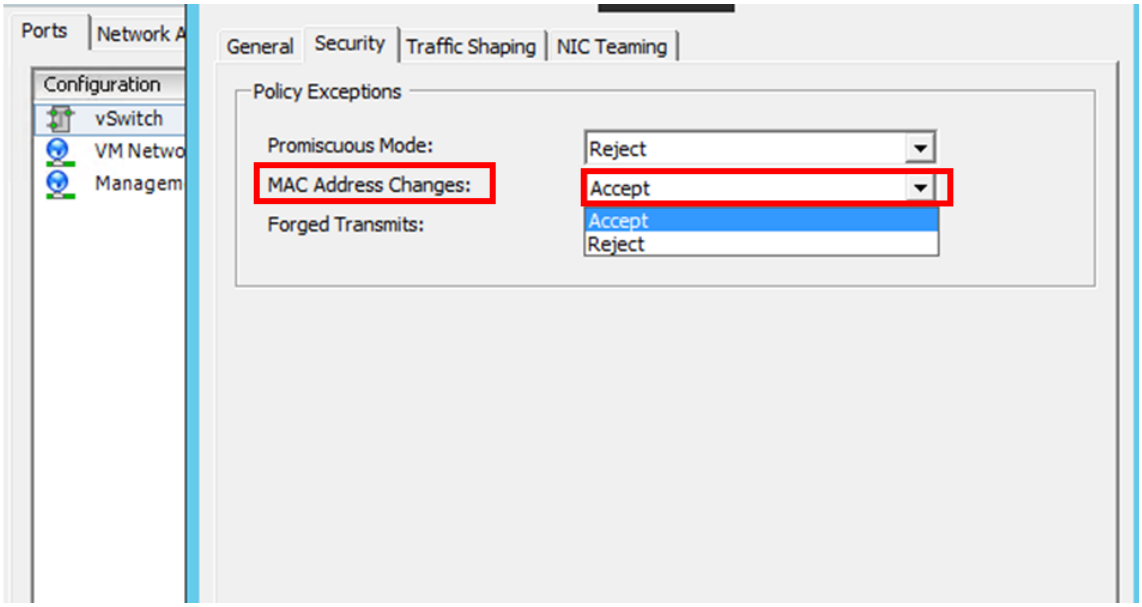
- Base de données :
  - Dans une configuration haute disponibilité, tous les fichiers de configuration sont synchronisés automatiquement du nœud principal vers le nœud secondaire à un intervalle d'une minute.
  - La synchronisation de la base de données s'effectue instantanément par réplication physique de la base de données.
  - La base de données sur le nœud secondaire est en mode lecture-réplica.
- Mise à niveau de Citrix ADM :
  - Les processus internes mettent implicitement à niveau Citrix ADM par rapport aux versions précédentes.

    > **Remarque**
    >
    > Une fois la mise à niveau réussie, vous devez configurer l'adresse IP flottante.

- Le port UDP par défaut 5005 est disponible sur les deux nœuds pour l'envoi de pulsations et pour la réception de messages.
- Adresse MAC
  Le paramètre de l'option « Changements d'adresse MAC » dans un hyperviseur affecte le trafic reçu par une machine virtuelle. Autoriser l'activation des modifications d'adresse MAC sur le commutateur virtuel afin que l'adresse IP flottante se déplace en toute transparence vers le nouveau nœud principal après le basculement.

Par exemple, lorsque vous déployez Citrix ADM en haute disponibilité sur VMware ESXi, assurez-vous d'accepter les modifications d'adresse MAC. ESXi autorise désormais les requêtes à modifier l'adresse MAC active en autre que l'adresse MAC initiale.

> **Remarque**
>
> Pour Citrix ADM déployé sur ESXI version 6.7, vous pouvez également définir l'option **Modifications d'adresse MAC** sur **Refuser**. Après le basculement sur incident, le trafic est acheminé vers le nouveau nœud principal de manière transparente, quel que soit le paramètre des **modifications d'adresse MAC**. Par conséquent, accepter les modifications apportées à l'adresse MAC n'est pas obligatoire.
>
> Si Citrix ADM est déployé sur la version ESXI inférieure à 6.7, assurez-vous que l'option **Modifications d'adresse MAC** est définie sur **Accepter** uniquement.



Conditions préalables

Avant de configurer la haute disponibilité pour les nœuds Citrix ADM, tenez compte des prérequis suivants :

- Le déploiement de la haute disponibilité de Citrix ADM est pris en charge à partir de Citrix ADM version 12.0 build 51.24.
- Téléchargez le fichier image Citrix Application Delivery Management (.xva) depuis le site de téléchargement de Citrix : https://www.citrix.com/downloads/

Citrix vous recommande de définir la priorité CPU (dans les propriétés de la machine virtuelle) au niveau le plus élevé pour améliorer le comportement de planification et la latence réseau.

Le tableau suivant répertorie les exigences minimales pour les ressources informatiques virtuelles :

Composant	Exigences
RAM	**32 GB**
CPU virtuel	**8 processeurs**
Espace de stockage	Citrix recommande d'utiliser la technologie SSD (Solid-State Drive) pour les déploiements Citrix ADM. La valeur par défaut est 120 Go. Les besoins réels de stockage dépendent de l'estimation de la taille de Citrix ADM. Si vos besoins de stockage Citrix ADM dépassent 120 Go, vous devez connecter un disque supplémentaire. **Remarque** Vous ne pouvez ajouter qu'un seul disque supplémentaire. Citrix vous recommande d'estimer le stockage et d'attacher un disque supplémentaire au moment du déploiement initial. Pour plus d'informations, consultez Comment attacher un disque supplémentaire à Citrix ADM.
Interfaces réseau virtuelles	1
Débit	1 Gbit/s ou 100 Mbit/s
Hyperviseur	**Versions**
Citrix Hypervisor	6.2 et 6.5
VMware ESXi	5.5 et 6.0
Microsoft Hyper-V	2012 R2
Linux KVM	Ubuntu et Fedora

Pour configurer Citrix ADM en mode haute disponibilité

1. Enregistrez et déployez le premier serveur (nœud principal).
2. Enregistrez et déployez le deuxième serveur (nœud secondaire).
3. Déployez le nœud principal et le nœud secondaire pour une configuration à haute disponibilité.

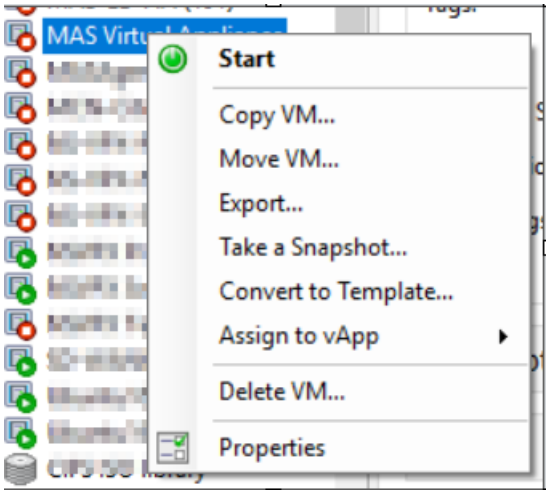
Enregistrer et déployer le premier serveur (nœud principal)

Pour enregistrer le premier nœud :

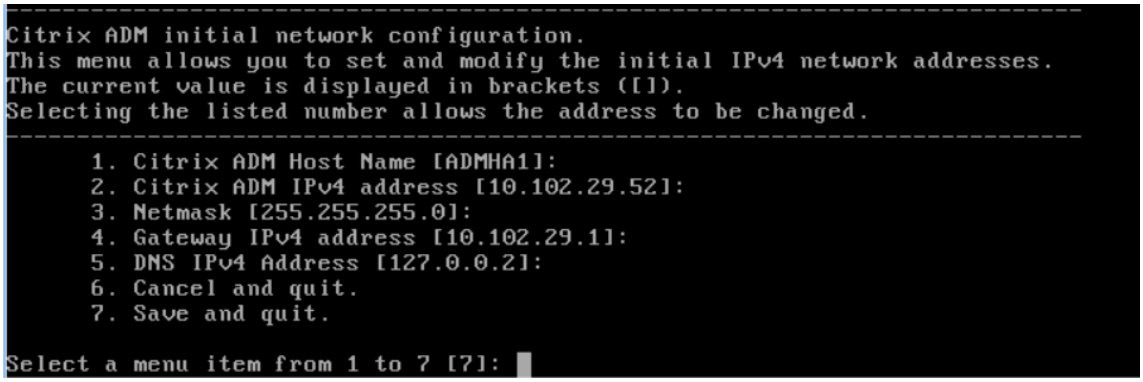
1. Utilisez le fichier image .xva téléchargé depuis le site de téléchargement de Citrix et importez-le dans votre hyperviseur.

   > **Remarque**
   >
   > L'importation et le démarrage du fichier image .xva peuvent prendre quelques minutes. Vous pouvez voir l'état en bas de l'écran.
   >
   >
   >

2. Une fois l'importation réussie, cliquez avec le bouton droit de la souris et cliquez sur **Démarrer**.

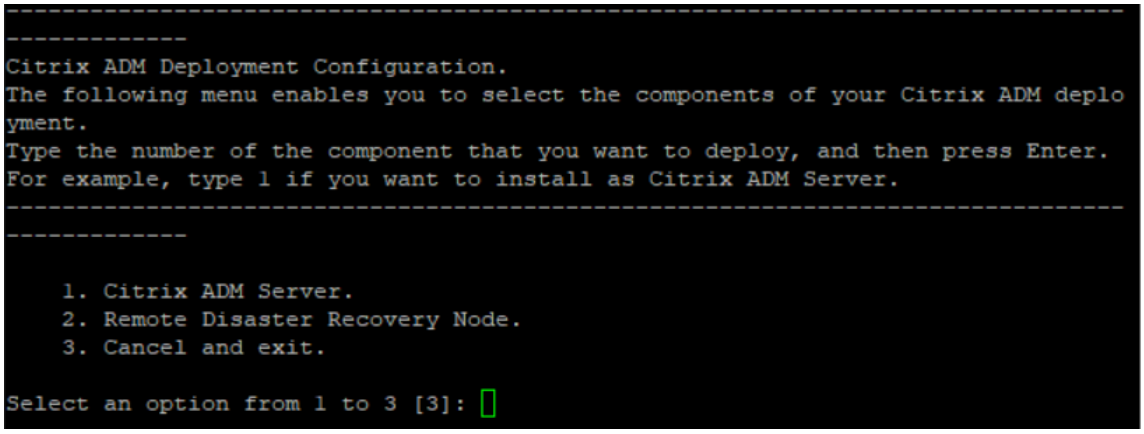
3. Dans l'onglet **Console**, configurez Citrix ADM avec les configurations réseau initiales.

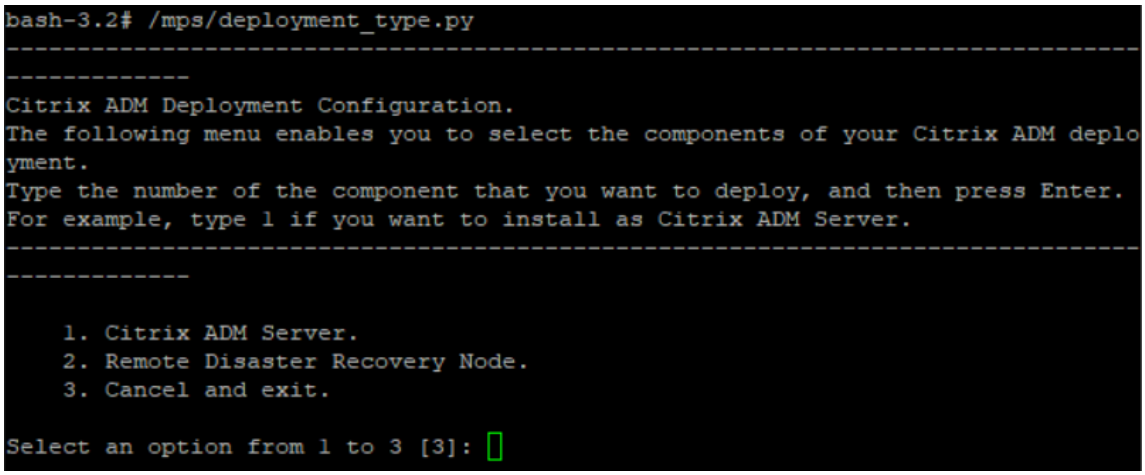
4. Une fois la configuration réseau initiale terminée, le système demande une connexion. Ouvrez une session à l'aide des informations d'identification suivantes : *nsrecover/nsroot*.

> **Remarque**
>
> Une fois que vous ouvrez une session, si vous souhaitez mettre à jour la configuration réseau initiale, tapez `networkconfig`, mettez à jour la configuration et enregistrez la configuration.

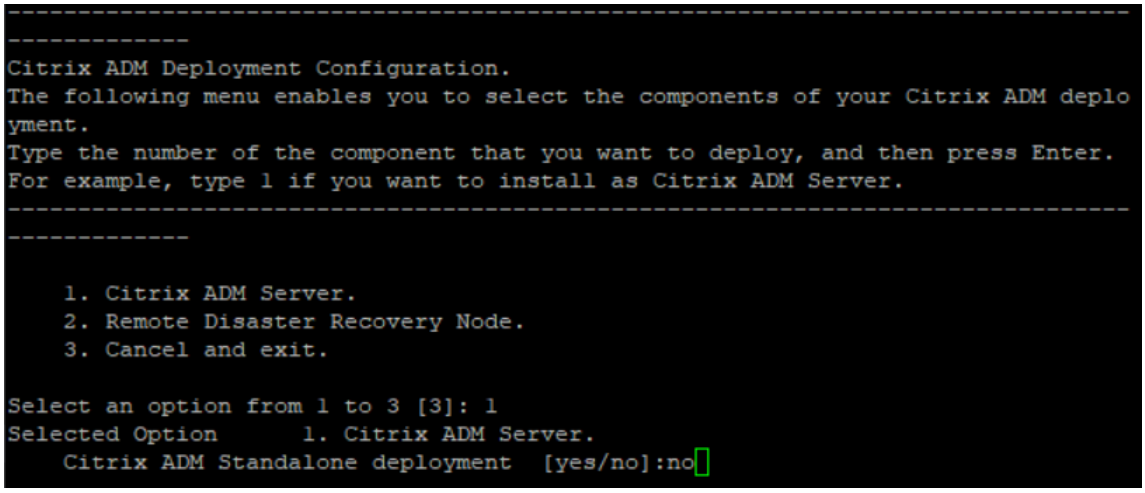
5. Pour déployer le nœud principal, saisissez **/mps/deployment_type.py**. Le menu de configuration du déploiement Citrix ADM s'affiche.



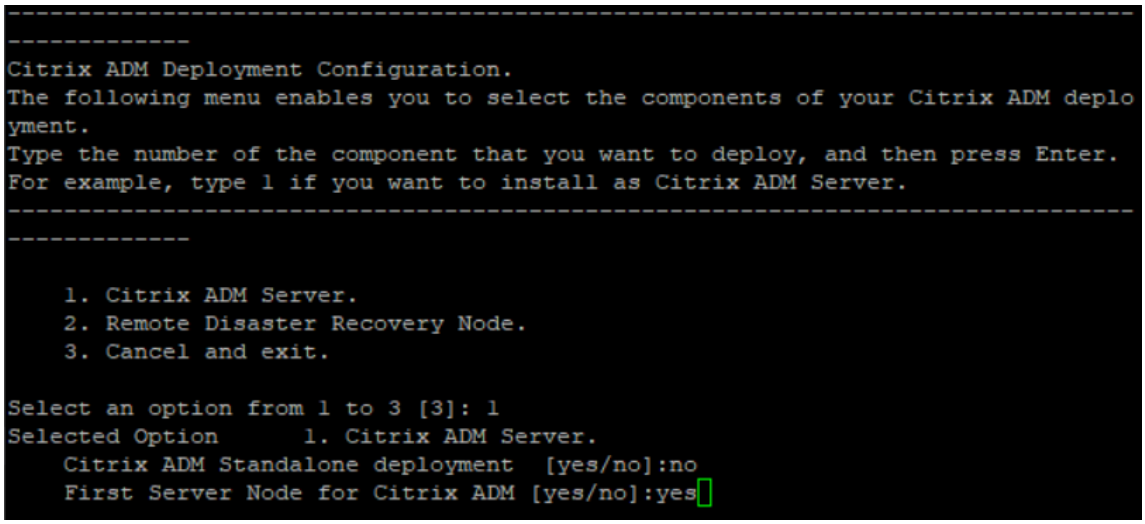
6. Sélectionnez **1** pour enregistrer le serveur Citrix ADM en tant que nœud principal.



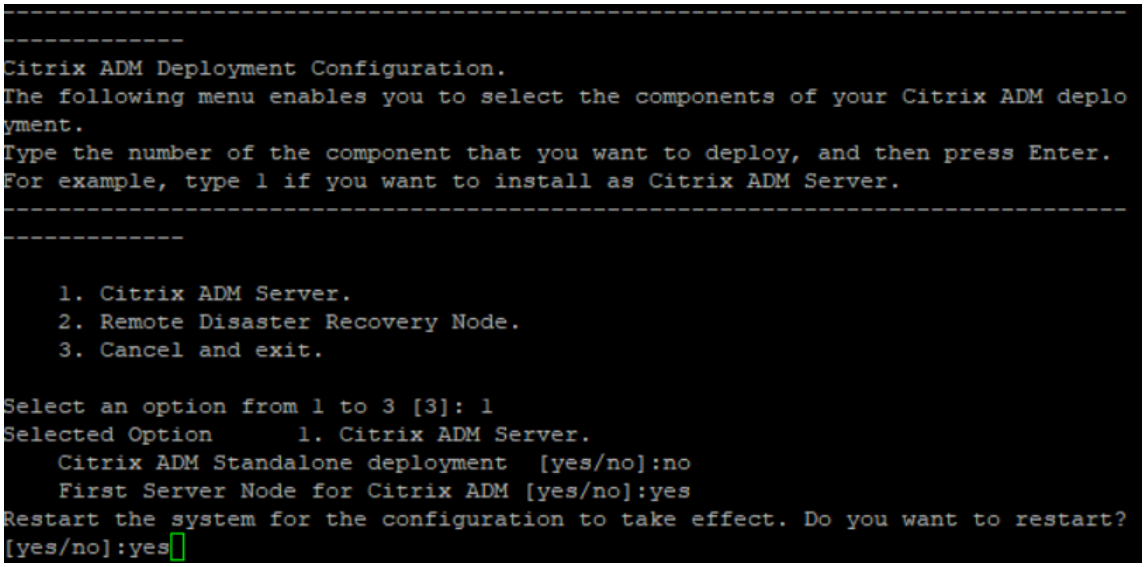
7. La console vous invite à sélectionner le déploiement autonome Citrix ADM. Saisissez **Non** pour confirmer le déploiement comme haute disponibilité.



8. La console vous invite à sélectionner le premier nœud de serveur. Entrez**Oui** pour confirmer que le nœud est le premier nœud.



9. La console vous invite à redémarrer le système. Entrez **Oui** pour redémarrer.



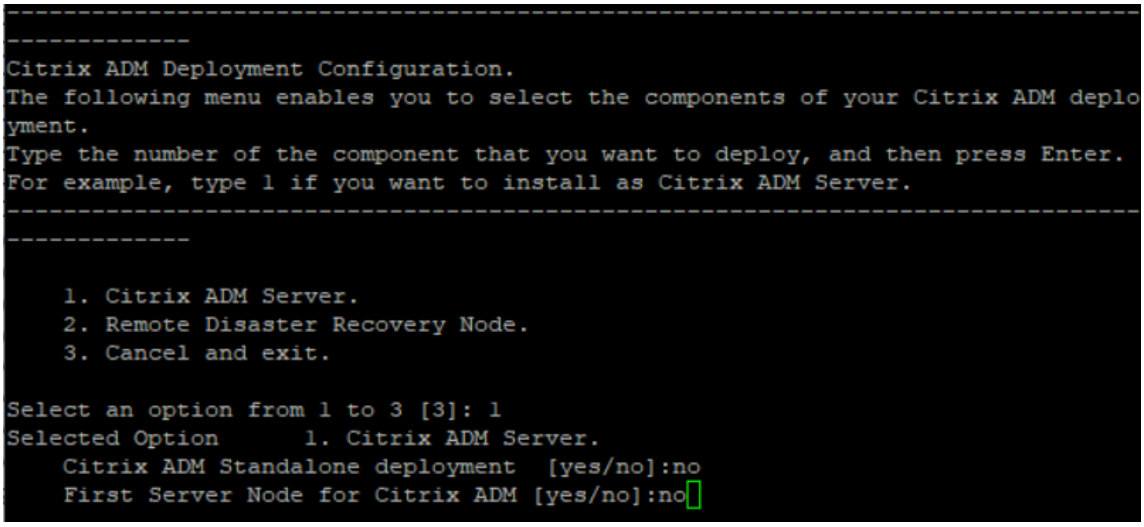
Le système redémarre et s'affiche en tant que nœud principal dans l'interface utilisateur Citrix ADM.

Inscrire et déployer le deuxième serveur (nœud secondaire)

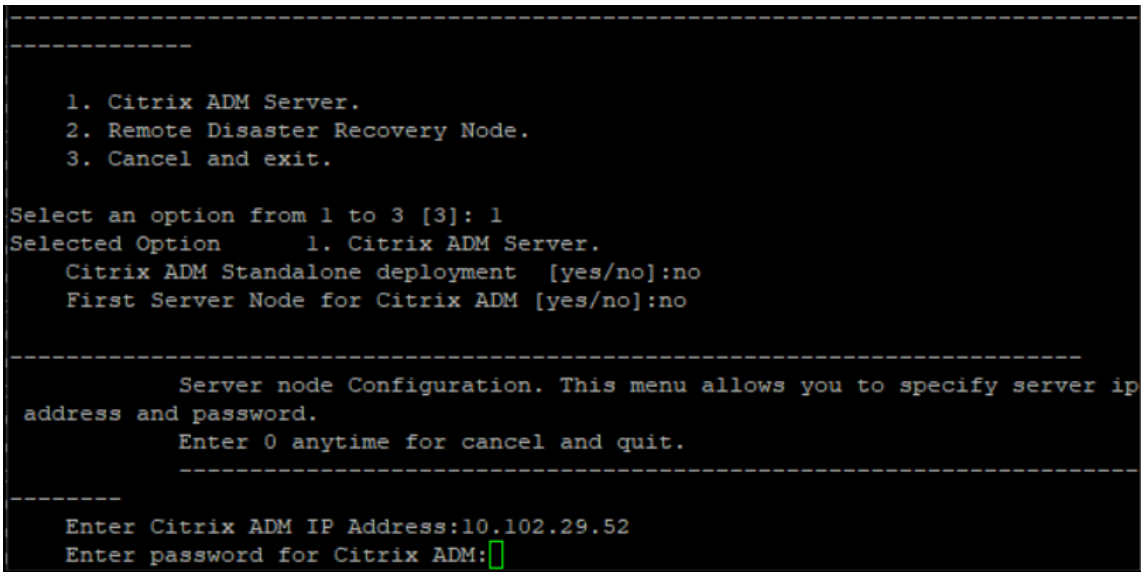
1. Utilisez le fichier image **.xva** téléchargé depuis le site de téléchargement de Citrix et importez-le dans votre hyperviseur.
2. Dans l'onglet **Console**, configurez Citrix ADM avec les configurations réseau initiales, comme indiqué dans l'image suivante.
3. Une fois la configuration réseau initiale terminée, le système demande une connexion. Ouvrez une session à l'aide des informations d'identification suivantes : *nsrecover/nsroot*.

   > **Remarque**
   >
   > Une fois que vous ouvrez une session, si vous souhaitez mettre à jour la configuration réseau initiale, tapez `networkconfig`, mettez à jour la configuration et enregistrez la configuration.

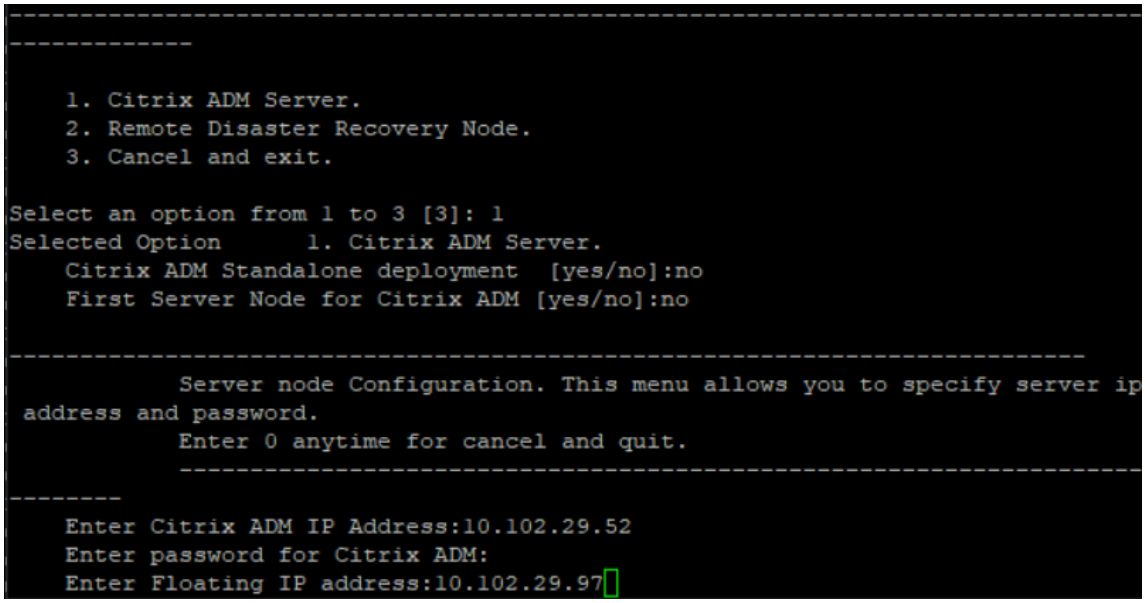
4. Pour déployer le nœud secondaire, saisissez **/mps/deployment_type.py**. Le menu de configuration du déploiement Citrix ADM s'affiche.
5. Sélectionnez **1** pour enregistrer le serveur Citrix ADM en tant que nœud secondaire.
6. La console vous invite à sélectionner Citrix ADM en tant que déploiement autonome. Saisissez **Non** pour confirmer le déploiement comme haute disponibilité.
7. La console vous invite à sélectionner le premier nœud de serveur. Entrez**Non** pour confirmer que le nœud est le deuxième serveur.



8. La console vous invite à entrer l'adresse IP et le mot de passe du nœud principal.



9. La console vous invite à entrer l'adresse IP flottante.



10. La console vous invite à redémarrer le système. Entrez **Oui** pour redémarrer.

> **Remarque**
>
> - L'adresse IP flottante est obligatoire pour le déploiement de nœuds à haute disponibilité.
> - Le système affichera des messages d'erreur en cas de problème de configuration.
> - Le système redémarre et les configurations ne prennent effet que quelques minutes.

Déployer le nœud principal et secondaire en tant que paire haute disponibilité

Après l'enregistrement, les nœuds principal et secondaire sont affichés sur l'interface utilisateur de Citrix ADM. Déployez ces nœuds dans une paire de haute disponibilité.

> **Remarque**
>
> - Avant de déployer les nœuds dans une paire de haute disponibilité, assurez-vous que le nœud secondaire est terminé par un redémarrage, après la configuration réseau initiale.
> - Une fois le déploiement de la haute disponibilité terminé, utilisez l'adresse IP flottante pour accéder à l'interface utilisateur Citrix ADM.

Pour déployer des nœuds en tant que paire haute disponibilité :

1. Ouvrez un navigateur Web et entrez l'adresse IP du premier nœud du serveur Citrix ADM.
2. Dans les champs **Nom d'utilisateur** et **mot de passe**, entrez les informations d'identification de l'administrateur.

3. Cliquez sur **Commencer** sur la page d'accueil.
4. Sélectionnez le type de déploiement en tant que**Deux serveurs déployés en mode haute disponibilité**, puis cliquez sur**Suivant**.
5. Sur la page Déploiement, cliquez sur**Déployer**.
6. Un message de confirmation s'affiche. Cliquez sur **Oui**.

   Citrix ADM redémarre et prend environ 10 minutes pour que la configuration prenne effet.

   > **Remarque**
   >
   > Vous pouvez maintenant commencer à utiliser l'adresse IP flottante.

7. Connectez-vous à Citrix ADM à l'aide des informations d'identification de l'administrateur, cliquez sur **Get Started** sur la page d'accueil et, si vous le souhaitez, effectuez les opérations suivantes :

   a) Ajouter des instances de Citrix ADC

   b) Configurer l'identité du client

   > **Remarque**
   >
   > Vous pouvez également cliquer sur **Ignorer** pour le terminer ultérieurement et cliquer sur **Terminer**.

8. Accédez à **Système** > **Déploiement** pour valider le déploiement.

   Pour plus d'informations, consultez la Foire aux questions.

Désactiver la haute disponibilité

Vous pouvez désactiver la haute disponibilité sur une paire de haute disponibilité Citrix ADM et convertir les nœuds en serveurs Citrix ADM autonomes.

> **Remarque**
>
> Désactivez la haute disponibilité depuis le nœud principal.

Pour désactiver la haute disponibilité :

1. Dans un navigateur Web, entrez l'adresse IP du nœud principal du serveur Citrix ADM.
2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Sous l'onglet**Système**, accédez à**Déploiement** et cliquez sur**Break HA**.

   Une boîte de dialogue s'affiche. Cliquez sur **Oui** pour interrompre le déploiement de la haute disponibilité.

Redéployez la haute disponibilité

Après avoir désactivé la haute disponibilité dans un déploiement autonome, vous pouvez le redéployer en mode haute disponibilité. Le redéploiement de la haute disponibilité est similaire au premier déploiement de la haute disponibilité. Pour plus de détails, consultez Déployer le nœud principal et le nœud secondaire en tant que paire haute disponibilité.

Scénarios de basculement à haute disponibilité

Un basculement se produit si l'une des conditions suivantes est remplie :

- **Échec du nœud** : le nœud principal s'éteint, aucun rythme cardiaque n'est détecté à partir du nœud principal pendant 180 secondes.
- **Échec de l'intégrité des applications** : le nœud principal est en cours d'exécution, mais l'un des processus Citrix ADM est en panne.

Scénario de cerveau divisé

Lorsqu'il n'y a aucune communication entre les deux nœuds en raison d'une interruption de la liaison réseau, alors :

- Le nœud principal continue de fonctionner en tant que nœud principal
- Le nœud secondaire prend le relais en tant que nœud principal en raison de l'impossibilité de recevoir les battements cardiaques
- Les deux nœuds exécuteraient leurs instances de base de données individuelles

Par exemple, dans une entreprise, deux nœuds Citrix ADM ont été déployés en tant que nœuds principal et secondaire. En raison d'une éventuelle interruption de la liaison réseau, la communication entre les deux nœuds Citrix ADM est complètement interrompue. Comme il n'y a pas d'échange de battements de cœur pendant plus de 180 secondes, les deux nœuds se considèrent comme le nœud principal. Les deux nœuds agissent comme des nœuds actifs et exécutent leurs propres instances de base de données.

À partir de Citrix ADM 12.1 ou version ultérieure, cette situation de double cerveau est gérée avec élégance une fois la liaison réseau et le rythme cardiaque rétablis. La synchronisation haute disponibilité est restaurée automatiquement. Le temps de restauration dépend des données et de la vitesse de la liaison entre les nœuds.

> **Remarque**
>
> En cas de division du cerveau, les modifications survenues sur l'ancien nœud principal sont réini-

> tialisées avec le nouveau nœud principal lorsqu'il est rejoint en haute disponibilité. Les changements survenus sur le nouveau nœud primaire lors de la division du cerveau restent intacts.

Configurer la reprise après sinistre pour une haute disponibilité

February 1, 2024

La catastrophe est une perturbation soudaine des fonctions commerciales causée par des catastrophes naturelles ou des événements d'origine humaine. Les catastrophes affectent les opérations des centres de données, après quoi les ressources et les données perdues sur le site du sinistre doivent être entièrement reconstruites et restaurées. La perte de données ou les temps d'arrêt dans le datacenter sont critiques et réduit la continuité de l'activité.

La fonctionnalité de reprise après sinistre (DR) Citrix ADM fournit des fonctionnalités complètes de sauvegarde et de restauration du système pour Citrix ADM déployées en mode haute disponibilité. Au moment de la récupération, des certificats, des fichiers de configuration et une sauvegarde complète de la base de données sont disponibles sur le site de récupération.

Le tableau suivant décrit les termes utilisés lors de la configuration de la reprise après sinistre dans Citrix ADM.

Termes	Description
Site principal (datacenter A)	Le site principal comporte des nœuds Citrix ADM déployés en mode haute disponibilité.
Site de récupération (centre de données B)	Le site de récupération dispose d'un nœud de reprise après sinistre déployé en mode autonome. Ce nœud est en mode lecture seule et n'est pas opérationnel tant que le site principal n'est pas en panne.
Nœud de reprise après sinistre	Le nœud de récupération est un nœud autonome déployé sur le site de récupération. Ce nœud est rendu opérationnel (vers le nouveau principal) en cas de sinistre sur le site principal et qu'il n'est pas fonctionnel.

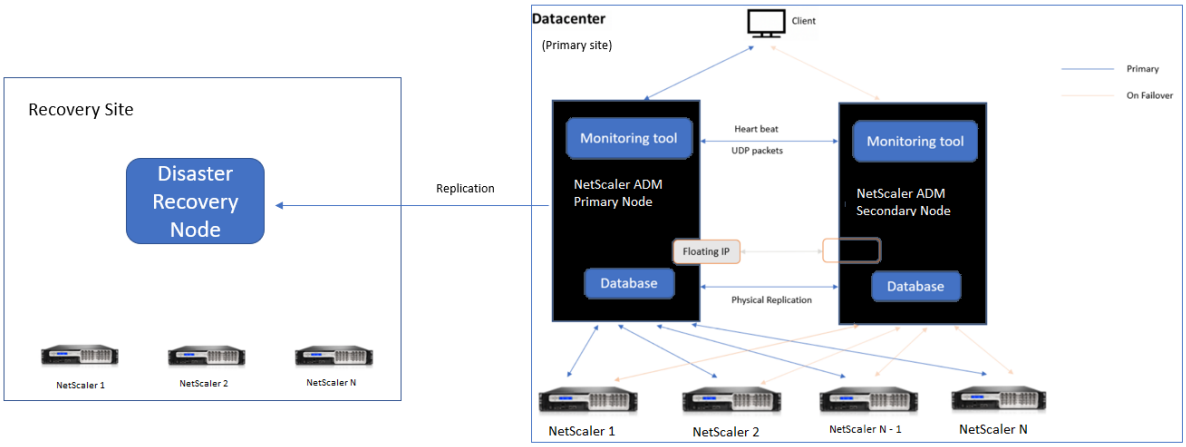
> Remarque : Le site principal et le site de reprise après sinistre communiquent entre eux via les

> ports 5454 et 22, et ces ports sont activés par défaut.
> Pour plus d'informations sur les ports et les protocoles, reportez-vous à la section Ports.

Workflow de reprise après sinistre

L'image suivante montre le flux de travail de reprise après sinistre, la configuration initiale avant le sinistre et le flux de travail après le sinistre.

Configuration initiale avant sinistre



L'image montre la configuration de la reprise après sinistre avant sinistre.

Les nœuds Citrix ADM du site principal sont déployés en mode haute disponibilité. Pour en savoir plus, consultez Déploiement haute disponibilité

Le site de récupération dispose d'un nœud de reprise après sinistre Citrix ADM autonome déployé à distance. Le nœud de reprise après sinistre est en mode lecture seule et reçoit des données du nœud principal pour créer une sauvegarde de données. Les instances Citrix ADC présentes sur le site de récupération sont également découvertes, mais aucun trafic ne les traverse. Au cours du processus de sauvegarde, toutes les données, fichiers et configurations sont répliqués sur le nœud de reprise après sinistre à partir du nœud principal.

Conditions préalables

Avant de configurer le nœud de reprise après sinistre, notez les conditions préalables suivantes :

- Pour activer les paramètres de reprise après sinistre, les nœuds Citrix ADM du site principal doivent être configurés en mode haute disponibilité.

- Le déploiement autonome de Citrix ADM sur le site principal ne prend pas en charge la fonctionnalité de reprise après sinistre.
- La paire Citrix ADM HA (sur le site principal) et le nœud autonome (sur le site DR) doivent avoir la même version logicielle, la même version et les mêmes configurations.

Citrix vous recommande de définir la priorité CPU (dans les propriétés de la machine virtuelle) au niveau le plus élevé pour améliorer le comportement de planification et la latence réseau.

Le tableau suivant répertorie la configuration minimale requise pour configurer le nœud Disaster Recovery :

Composant	Exigences
RAM	32 GB
CPU virtuel	8 processeurs
Espace de stockage	Citrix recommande d'utiliser la technologie SSD (Solid State Drive) pour les déploiements Citrix ADM. La valeur par défaut est 120 Go. Les besoins réels de stockage dépendent de l'estimation de la taille de Citrix ADM. Si vos besoins de stockage Citrix ADM dépassent 120 Go, vous devez connecter un disque supplémentaire. **Remarque** Vous ne pouvez ajouter qu'un seul disque supplémentaire. Citrix vous recommande d'estimer le stockage et d'attacher plus de disque au moment du déploiement initial. Pour plus d'informations, consultez Comment attacher un disque supplémentaire à Citrix ADM.
Interfaces réseau virtuelles	1
Débit	1 Gbit/s ou 100 Mbit/s
Hyperviseur	**Versions**
Citrix Hypervisor	6.2 et 6.5
VMware ESXi	5.5 et 6.0
Microsoft Hyper-V	2012 R2
Linux KVM	Ubuntu et Fedora

Première configuration de la reprise après sinistre

- Déployer Citrix ADM en mode haute disponibilité
- Déployer et enregistrer le nœud de reprise après sinistre Citrix ADM
- Activer et désactiver les paramètres de reprise après sinistre à partir de l'interface utilisateur

Déployer Citrix ADM en mode haute disponibilité

Pour configurer les paramètres de reprise après sinistre, assurez-vous que Citrix ADM est déployé en mode haute disponibilité. Pour plus d'informations sur le déploiement de Citrix ADM en haute disponibilité, consultez Déploiement haute disponibilité

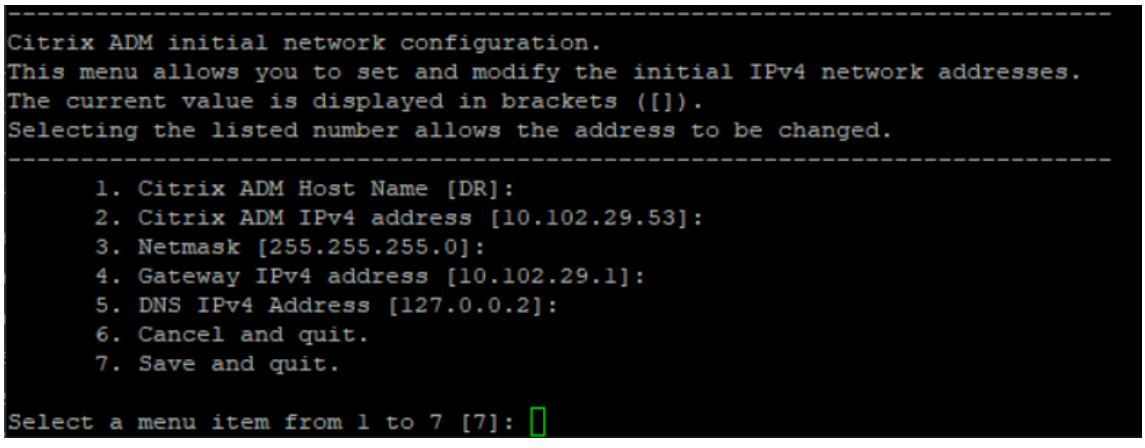
> **Remarque**
>
> - Citrix ADM déployé en mode haute disponibilité doit être mis à niveau vers la version 13.0 de Citrix ADM.
> - **L'adresse IP flottante est obligatoire** pour enregistrer le nœud de reprise après sinistre auprès du nœud principal.

Déployez et enregistrez le nœud de reprise après sinistre Citrix ADM à l'aide de la console DR

Pour enregistrer le nœud de reprise après sinistre Citrix ADM :

1. Téléchargez le fichier image `.xva` depuis le site de téléchargement de Citrix et importez-le dans votre hyperviseur.
2. Dans l'onglet **Console**, configurez Citrix ADM avec les configurations réseau initiales.

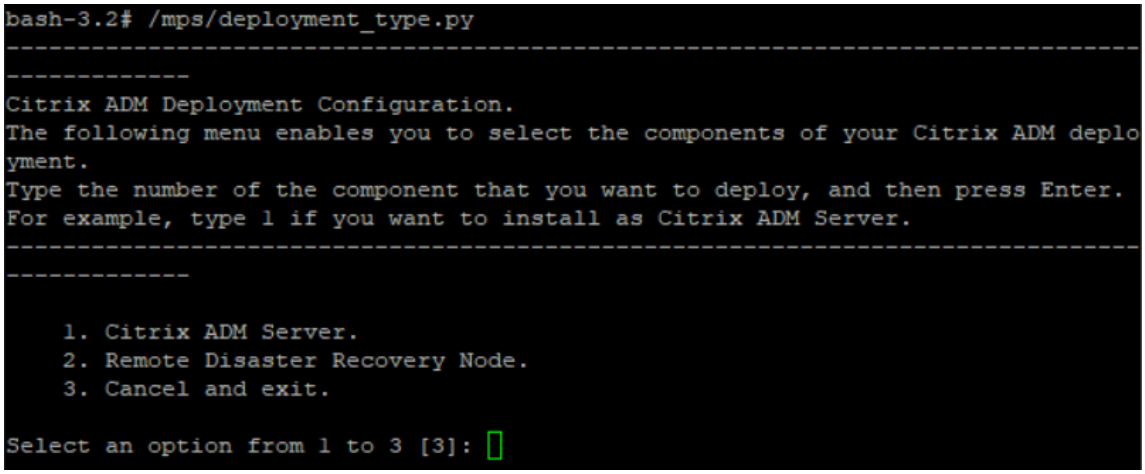
   > **Remarque**
   >
   > Le nœud de reprise après sinistre peut se trouver sur un sous-réseau différent.



3. Une fois la configuration réseau initiale terminée, le système demande une connexion. Connectez-vous à l'aide des informations d'identification suivantes —`nsrecover`/`nsroot`.

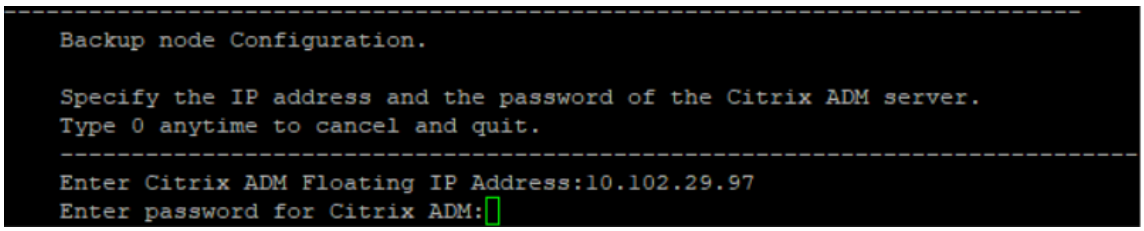
   > **Important**
   >
   > Ne modifiez pas les informations d'identification du nœud DR (`nsrecover`/`nsroot`) lors de l'enregistrement. Vous pouvez modifier les informations d'identification du nœud DR une fois que vous avez correctement enregistré le nœud DR.

4. Pour déployer le nœud de reprise après sinistre, tapez **/mps/deployment_type.py** et appuyez sur Entrée. Le menu de configuration du déploiement Citrix ADM s'affiche.

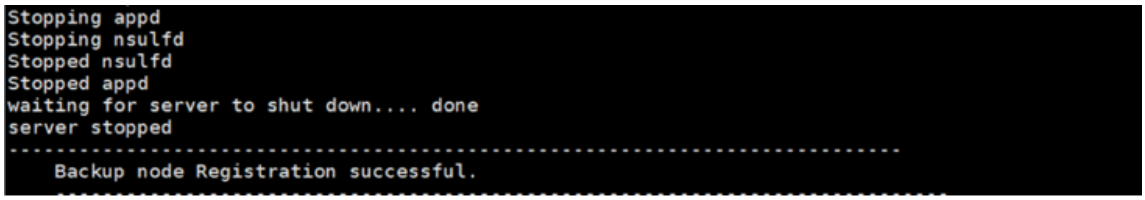


5. Sélectionnez **2** pour enregistrer le nœud de reprise après sinistre.

6. La console demande l'adresse IP flottante du nœud haute disponibilité et du mot de passe.
7. Entrez l'adresse IP flottante et le mot de passe pour enregistrer le nœud de reprise après sinistre sur le nœud principal.



Le nœud de reprise après sinistre est maintenant enregistré avec succès.



> **Remarque**
>
> Le nœud de reprise après sinistre n'a pas d'interface graphique.

8. Si vous souhaitez modifier le mot de passe du nœud DR, exécutez le script suivant :

```
/mps/change_freebsd_password.sh <username> <password>
<!--NeedCopy-->
```

Déployer le nœud de reprise après sinistre à l'aide de l'interface graphique Citrix ADM

Une fois le nœud de reprise après sinistre enregistré avec succès à l'aide de la console DR, déployez le nœud DR à partir de l'interface graphique Citrix ADM. Cette étape active les paramètres de reprise après sinistre à partir du site principal de Citrix ADM.

1. Accédez à **Système > Administration système > Paramètres de reprise après sinistre.**
2. Sur la page de **reprise après sinistre**, sélectionnez **Déployer le nœud de reprise après sinistre**.
3. Une boîte de dialogue de confirmation s'affiche. Cliquez sur **Oui** pour continuer.

> **Remarque**
>
> Le temps nécessaire à la sauvegarde du système dépend de la taille des données et de la vitesse de liaison WAN.

Une fois que vous avez correctement déployé le nœud DR dans l'interface graphique Citrix ADM, vous pouvez surveiller l'état de la base de données, la mémoire, le processeur et l'utilisation du disque du nœud DR.

Pour désactiver les paramètres de reprise après sinistre, sélectionnez **Supprimer le nœud de reprise après sinistre**. Une boîte de dialogue de confirmation s'affiche. Cliquez sur **Oui** pour continuer.

Pour réactiver le nœud de reprise après sinistre, reconfigurez le nœud de reprise après sinistre pour votre paire de haute disponibilité :

1. Connectez-vous au nœud DR à l'aide d'un Hypervisor ou d'une console SSH.
2. Configurez le nœud de reprise après sinistre en suivant la procédure disponible dans Déployer et enregistrez le nœud de reprise après sinistre Citrix ADM à l'aide de la console DR.
3. Déployez le nœud de reprise après sinistre à l'aide de l'interface graphique Citrix ADM

Pour plus d'informations, consultez la FAQ.

> **Important**
>
> - Il incombe à l'administrateur de détecter qu'un sinistre s'est produit sur le site principal.
> - Le workflow de reprise après sinistre est lancé manuellement par l'administrateur une fois le site principal arrêté.
> - Un administrateur doit lancer manuellement le processus en exécutant un script de récupération sur le nœud de reprise après sinistre sur le site de récupération.
> - Si vous mettez à niveau la paire HA dans le site principal, vous devez également mettre à niveau manuellement le nœud autonome dans le site DR.

Flux de travail après le désastre

Lorsque le site principal tombe en panne après un sinistre, le flux de travail de reprise après sinistre doit être lancé comme suit :

1. L'administrateur constate qu'un sinistre a frappé le site principal et que celui-ci n'est pas opérationnel.
2. L'administrateur lance le processus de récupération.
3. L'administrateur doit exécuter manuellement l'un des scripts de récupération suivants sur le nœud de reprise après sinistre en fonction de vos besoins (sur le site de récupération) :

   - Configurez SNMP, Syslog et Analytics sur le nœud DR :

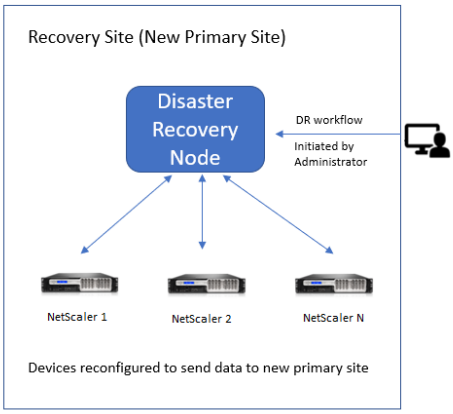
   ```
   /mps/scripts/pgsql/pgsql_restore_remote_backup.sh

   <!--NeedCopy-->
   ```

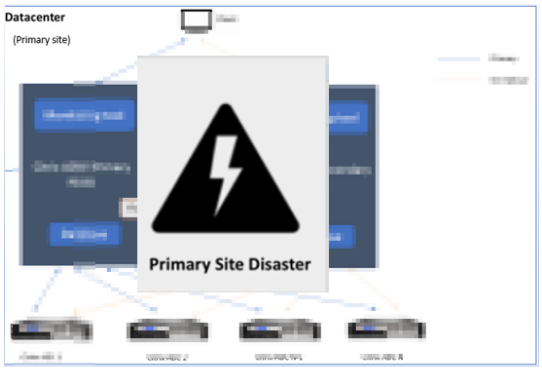
   - Configurez également le nœud DR en tant que serveur de licences :

   ```
   /mps/scripts/pgsql/pgsql_restore_remote_backup.sh -reconfig-
      ls <IP-address-of-the-primary-site>

   <!--NeedCopy-->
   ```


4. En interne, les instances Citrix ADC sont automatiquement reconfigurées pour envoyer les données au nœud de reprise après sinistre qui est maintenant devenu le nouveau site principal.

   L'image suivante montre que le flux de travail de reprise après sinistre après le site principal est frappé par un sinistre.





> Remarque :
>
> Une fois que vous avez lancé le script sur le site DR, le site DR devient désormais le nouveau site principal. Vous pouvez également accéder à l'interface utilisateur DR.

Reprise après sinistre

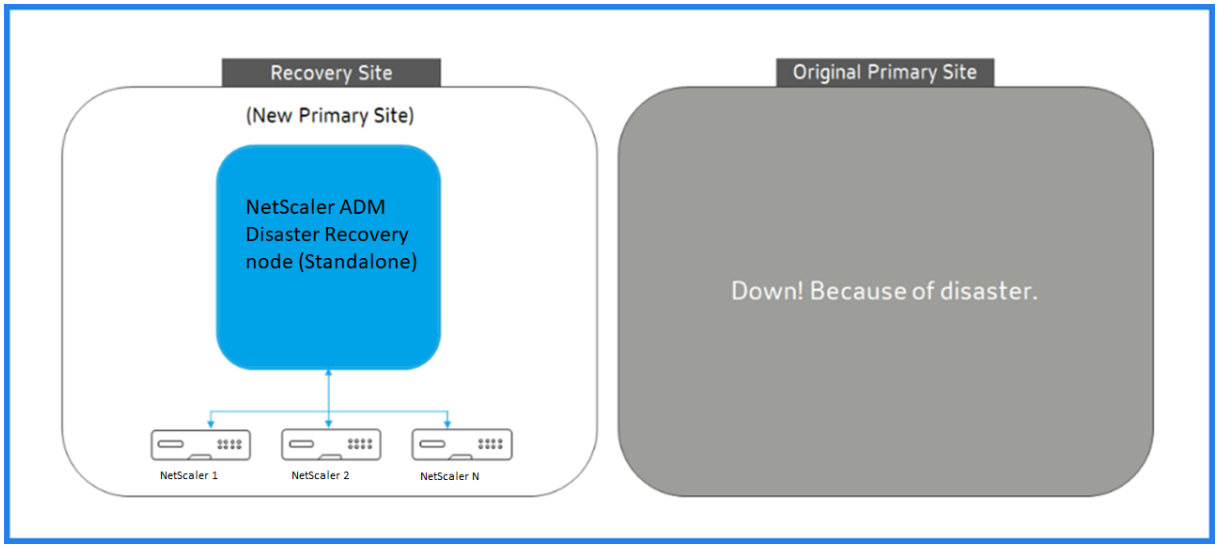
Une fois le sinistre survenu et que l'administrateur initie le script de récupération, le site de reprise après sinistre devient désormais le nouveau site principal.

Si vous souhaitez rétablir les configurations sur le site d'origine ultérieurement, reportez-vous à la section Rétablir les configurations sur le site principal d'origine.

> **Important**
>
> - Si vous avez installé Citrix ADM 12.1.49.x ou des versions antérieures, vous disposez d'un délai de grâce de 30 jours pour contacter Citrix afin de réhéberger la licence d'origine sur Citrix ADM (sur le site DR).
> - Pour les versions 12.1.50.x ou ultérieures, la licence Citrix ADM est automatiquement synchronisée avec le site DR (il n'est pas obligatoire de contacter Citrix pour obtenir la licence).
> - La licence groupée pour le site de reprise après sinistre est prise en charge à partir de 12.1.50.x ou versions ultérieures. Si vous avez appliqué des licences groupées pour les instances, reconfigurez manuellement les instances sur le site de reprise après sinistre.

Rétablir les configurations sur le site principal d'origine

Après le sinistre, le nœud de reprise après sinistre (DR) configuré devient le nouveau site principal et le trafic client passe par ce nœud.



Pour plus d'informations, consultez Workflow après le sinistre.

Lorsque votre site principal d'origine est exempt de sinistre et que vous décidez de déplacer toutes les opérations vers le site principal, reconfigurez le site principal d'origine pour qu'il corresponde aux configurations du nœud de reprise après sinistre.

Avant de commencer, assurez-vous que le site principal et le site DR sont actifs.

Pour annuler les modifications apportées au site principal d'origine à partir du site DR, effectuez les opérations suivantes :

1. Connectez-vous au site principal d'origine et exécutez la commande suivante :

```
nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-
    password> -L <primary-node-password> &
<!--NeedCopy-->
```

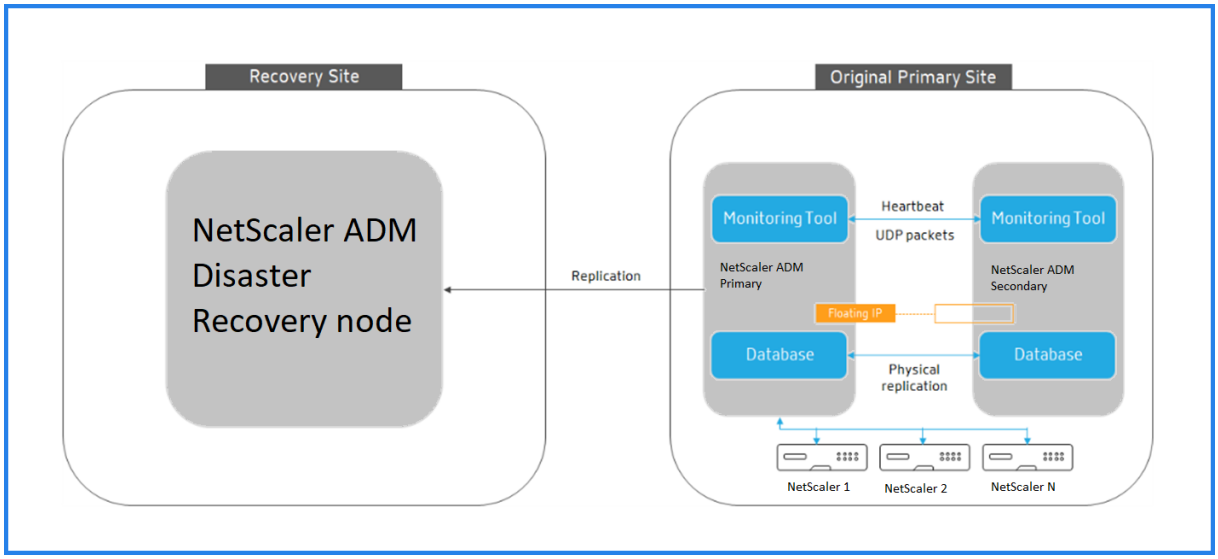
   Cette commande configure uniquement Syslog, SNMP et Analytics sur le site principal.

   Si vous souhaitez configurer le site principal en tant que serveur de licences groupé pour les instances ADC, exécutez la commande suivante :

```
nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-
    password> -L <primary-node-password>  -O yes &
<!--NeedCopy-->
```

   La commande `-O` récupère l'adresse IP du site de reprise après sinistre et reconfigure le site principal en tant que serveur de licences groupé.

2. Reconfigurez le site de reprise après sinistre. Voir Déployer la configuration de la reprise après sinistre.



Une fois que vous avez rétabli les configurations du site de reprise après sinistre au site principal d'origine, le trafic client passe par le nœud principal Citrix ADM.

Configurer les agents sur site pour un déploiement multisite

February 1, 2024

Dans les versions antérieures de Citrix ADM, les instances Citrix ADC déployées dans des centres de données distants peuvent être gérées et surveillées à partir de Citrix ADM s'exécutant dans un centre de données principal. Les instances Citrix ADC ont envoyé des données directement à Citrix ADM principal, ce qui a entraîné la consommation de bande passante WAN. En outre, le traitement des données d'analyse utilise les ressources CPU et mémoire du principal Citrix ADM.

Vous pouvez avoir des centres de données situés dans le monde entier. Les agents jouent un rôle essentiel dans les scénarios suivants :

- Pour installer des agents dans des centres de données distants afin de réduire la consommation de bande passante WAN.
- Limiter le nombre d'instances qui envoient directement du trafic vers Citrix ADM principal pour le traitement des données.

> **Remarque**
>
> - Il est recommandé d'installer des agents pour les instances dans un datacenter distant,

> mais pas obligatoire. Si nécessaire, les utilisateurs peuvent directement ajouter des instances Citrix ADC à Citrix ADM principal.
>
> - Si vous avez installé des agents pour un ou plusieurs centres de données distants, la communication entre les agents et le site principal se fait par l'intermédiaire d'une adresse IP flottante. Pour plus d'informations, reportez-vous à la section port.
> - Vous pouvez installer des agents et appliquer des licences regroupées aux instances d'un ou plusieurs centres de données distants. Dans ce scénario, la communication entre le site principal et un ou plusieurs centres de données distants se fait via l'adresse IP flottante.

À partir de Citrix ADM 12.1 ou version ultérieure, les instances peuvent être configurées avec des agents pour communiquer avec le Citrix ADM principal situé dans un autre centre de données.

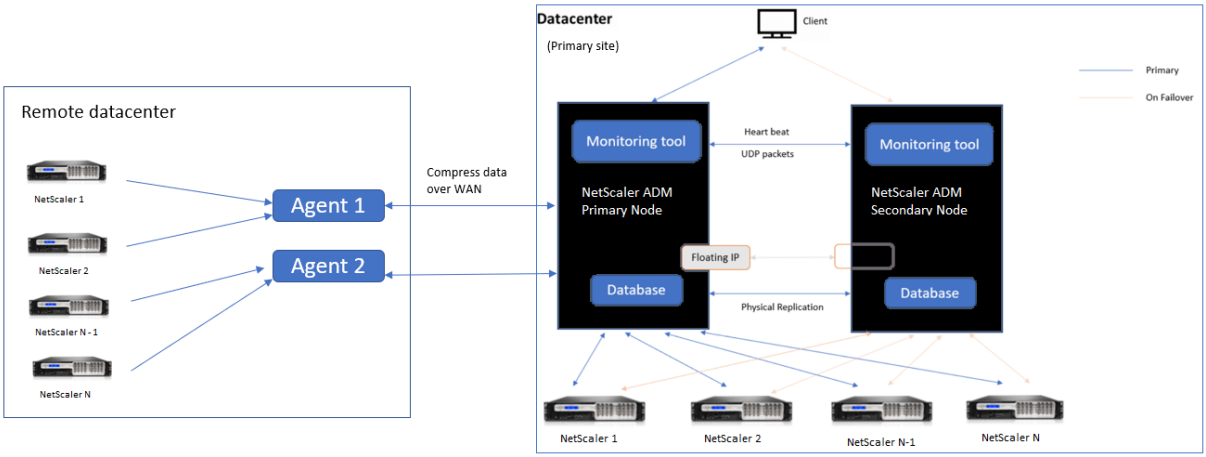
Les agents agissent en tant qu'intermédiaire entre le Citrix ADM principal et les instances découvertes dans différents centres de données. Les avantages de l'installation d'agents sont les suivants :

- Les instances sont configurées pour les agents de sorte que les données non traitées soient envoyées directement aux agents au lieu de Citrix ADM principal. Les agents effectuent le premier niveau de traitement des données et envoient les données traitées au format compressé au Citrix ADM principal pour le stockage.
- Les agents et les instances sont co-implantés dans le même centre de données afin que le traitement des données soit plus rapide.
- La mise en cluster des agents permet la redistribution des instances Citrix ADC lors du basculement de l'agent. Lorsqu'un agent d'un site échoue, le trafic provenant des instances Citrix ADC est transféré vers un autre agent disponible sur le même site.

  > **Remarque**
  >
  > Le nombre d'agents à installer par site dépend du trafic traité.

Architecture

La figure suivante illustre les instances Citrix ADC dans deux centres de données et le déploiement haute disponibilité Citrix ADM à l'aide d'une architecture basée sur un agent multisite.



Les nœuds Citrix ADM du site principal sont déployés dans une configuration haute disponibilité. Les instances de Citrix ADC sur le site principal sont directement enregistrées auprès de Citrix ADM.

Sur le site secondaire, les agents sont déployés et enregistrés auprès du serveur Citrix ADM sur le site principal. Ces agents travaillent dans un cluster pour gérer un flux de trafic continu en cas de basculement d'agent. Les instances de Citrix ADC sur le site secondaire sont enregistrées auprès du serveur Citrix ADM principal par le biais d'agents situés sur ce site. Les instances envoient des données directement aux agents au lieu de Citrix ADM principal. Les agents traitent les données reçues des instances et les envoient au Citrix ADM principal dans un format compressé. Les agents communiquent avec le serveur Citrix ADM via un canal sécurisé et les données envoyées via ce canal sont compressées pour une meilleure efficacité de la bande passante.

Mise en route

- Installation de l'agent dans un centre de données
  - Enregistrer l'agent
  - Associer l'agent à un site
- Ajouter des instances de Citrix ADC
  - Ajouter une nouvelle instance
  - Mettre à jour une instance existante

Installation de l'agent dans un centre de données

Vous pouvez installer et configurer l'agent pour activer la communication entre l'Netscaler ADM principal et les instances Citrix ADC gérées dans un autre centre de données.

Vous pouvez installer un agent sur les hyperviseurs suivants dans votre centre de données d'entreprise :

- Citrix Hypervisor
- VMware ESXi
- Microsoft Hyper-V
- Serveur KVM Linux

> **Remarque**
>
> Les agents sur site pour le déploiement multisite sont pris en charge uniquement avec le déploiement haute disponibilité Citrix ADM.

Avant de commencer l'installation de l'agent, assurez-vous que vous disposez des ressources informatiques virtuelles requises que l'Hypervisor doit fournir pour chaque agent.

Composant	Exigences
RAM	32 GB
CPU virtuel	8 processeurs
Espace de stockage	30 GB
Interfaces réseau virtuelles	1
Débit	1 Gbit/s

Ports

À des fins de communication, les ports suivants doivent être ouverts entre l'agent et le serveur sur site Citrix ADM.

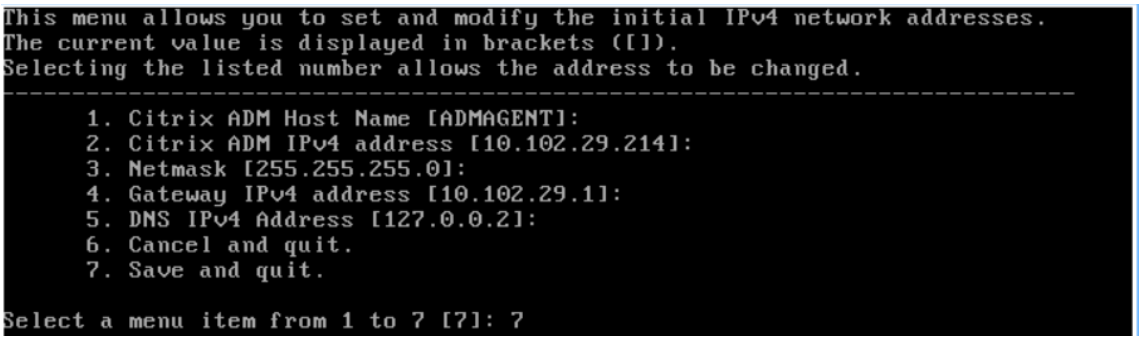
Type	Port	Détails	Direction de la communication
TCP	8443, 7443, 443	Pour les communications sortantes et entrantes entre l'agent et le serveur sur site Citrix ADM.	Agent Citrix ADM vers Citrix ADM

Les ports suivants doivent être ouverts entre l'agent et les instances Citrix ADC.

Type	Port	Détails	Direction de la communication
—-	—	——-	—-
TCP	80	Pour la communication NITRO entre l'agent et l'instance Citrix ADC ou Citrix SD-WAN.	Citrix ADM vers Citrix ADC et Citrix ADC vers Citrix ADM
TCP	22	Pour la communication SSH entre l'agent et l'instance Citrix ADC ou Citrix SD-WAN. Pour la synchronisation entre les serveurs Citrix ADM déployés en mode haute disponibilité.	Citrix ADM vers Citrix ADC et agent Citrix ADM vers Citrix ADC
UDP	4739	Pour la communication AppFlow entre l'agent et l'instance Citrix ADC ou Citrix SD-WAN.	Citrix ADC ou Citrix SD-WAN vers Citrix ADM
ICMP	Aucun port réservé	Pour détecter l'accessibilité du réseau entre les instances Citrix ADM et Citrix ADC, les instances WAN SD ou le serveur Citrix ADM secondaire déployé en mode haute disponibilité.
UDP	161, 162	Pour recevoir des événements SNMP de l'instance Citrix ADC vers l'agent. |Port 161 - Citrix ADM vers Citrix ADC|
		Port 162 - Citrix ADC vers Citrix ADM
UDP	514	Pour recevoir des messages syslog de l'instance Citrix ADC ou Citrix SD-WAN vers l'agent.	Citrix ADC ou Citrix SD-WAN vers Citrix ADM
TCP	5557	Pour les communications Logstream entre l'agent et les instances Citrix ADC.	Citrix ADC vers Citrix ADM

Enregistrer l'agent

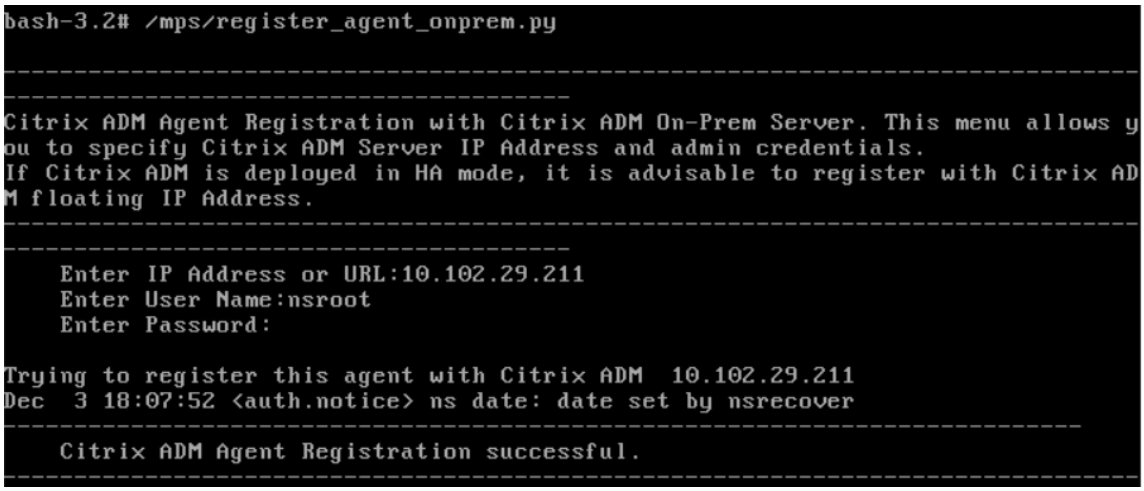
1. Utilisez le fichier image de l'agent téléchargé à partir du site de téléchargement Citrix et importez-le dans votre Hypervisor. Le modèle de dénomination du fichier image de l'agent est le suivant, **MASAGENT-<HYPERVISOR>-<Version.no>.** Par exemple : **Masagent-XEN-13.0-XY.XVA**
2. Dans l'onglet **Console**, configurez Citrix ADM avec les configurations réseau initiales.
3. Entrez le nom d'hôte Citrix ADM, l'adresse IPv4 et l'adresse IPv4 de la passerelle. Sélectionnez l'option 7 pour enregistrer et quitter la configuration.



4. Une fois l'enregistrement réussi, la console vous invite à ouvrir une session. Utilisez *nsrecov-*

er/nsroot comme informations d'identification.

5. Pour enregistrer l'agent, entrez**/mps/register_agent_onprem.py**. Les informations d'identification d'enregistrement de l'agent Citrix ADM sont affichées comme indiqué dans l'image suivante.
6. Entrez l'adresse IP flottante Citrix ADM et les informations d'identification de l'utilisateur.



Une fois l'enregistrement réussi, l'agent redémarre pour terminer le processus d'installation.

Après le redémarrage de l'agent, accédez à l'interface graphique Citrix ADM, à partir du menu principal, accédez à la page **Réseaux > Agents** pour vérifier l'état de l'agent.L'agent nouvellement ajouté est affiché à l'état **Up**.

> **Remarque**
>
> Citrix ADM affiche la version de l'agent et vérifie également si l'agent est sur la dernière version. L'icône de téléchargement indique que l'agent n'utilise pas la dernière version et qu'il doit être mis à niveau. Citrix vous recommande de mettre à niveau la version de l'agent vers la version de Citrix ADM.

Attacher un agent à un site

1. Sélectionnez l'agent et cliquez sur **Joindre le site.**
2. Dans la page**Joindre un site**, sélectionnez un site dans la liste ou créez un site à l'aide du bouton plus (+).
3. Cliquez sur **Enregistrer.**

> **Remarque**
>
> - Par défaut, tous les nouveaux agents enregistrés sont ajoutés au centre de données par défaut.

> - Il est important d'associer l'agent au bon site. En cas de défaillance d'un agent, les instances Citrix ADC qui lui sont affectées sont automatiquement commutées vers d'autres agents fonctionnels sur le même site.

Actions d'agent

Vous pouvez appliquer diverses actions à un agent sous **Réseaux > Agents > Sélectionner des actions**.

Sous **Sélectionner une action**, vous pouvez utiliser les fonctionnalités suivantes :

Installer un nouveau certificat : si vous avez besoin d'un certificat d'agent différent pour répondre à vos exigences de sécurité, vous pouvez en ajouter un.

Modifiez le mot de passe par défaut : pour assurer la sécurité de votre infrastructure, modifiez le mot de passe par défaut d'un agent.

Générer un fichier de support technique : générez un fichier de support technique pour un agent Citrix ADM sélectionné. Vous pouvez télécharger ce fichier et l'envoyer au support technique Citrix pour enquête et dépannage.

Ajouter des instances de Citrix ADC

Les instances sont des appliances Citrix ou des appliances virtuelles que vous souhaitez découvrir, gérer et surveiller depuis Citrix ADM via des agents. Vous pouvez ajouter les appliances Citrix et les appliances virtuelles suivantes à Citrix ADM ou aux agents :

- Citrix ADC MPX
- Citrix ADC VPX
- Citrix ADC SDX
- Citrix ADC CPX
- Citrix Gateway
- Proxy de transfert SSL Citrix
- Citrix SD-WAN WO

Pour de plus amples informations, consultez la section Ajouter des instances à Citrix ADM.

Joindre une instance existante à l'agent

Si une instance est déjà ajoutée au Citrix ADM principal, vous pouvez l'attacher à un agent en modifiant un agent.

1. Accédez à **Réseaux > Instances** et sélectionnez le type d'instance. Par exemple, Citrix ADC.
2. Cliquez sur **Modifier** pour modifier une instance existante.
3. Cliquez sur pour sélectionner l'agent.
4. Dans la page **Agent**, sélectionnez l'agent auquel vous souhaitez associer l'instance, puis cliquez sur**OK**.

   > **Remarque**
   >
   > Assurez-vous de sélectionner le **site** auquel vous souhaitez associer l'instance.

Accéder à l'interface graphique d'une instance pour valider les événements

Une fois les instances ajoutées et l'agent configuré, accédez à l'interface graphique d'une instance pour vérifier si la destination d'interruption est configurée.

Dans Citrix ADM, accédez à**Réseaux > Instances**. Sous **Instances**, sélectionnez le type d'instance auquel vous souhaitez accéder (par exemple, Citrix ADC VPX), puis cliquez sur l'adresse IP d'une instance spécifique.

L'interface graphique de l'instance sélectionnée s'affiche dans une fenêtre contextuelle.

Par défaut, l'agent est configuré en tant que destination de trap sur l'instance. Pour confirmer, connectez-vous à l'interface graphique de l'instance et vérifiez les destinations des interruptions.

> **Important**
>
> L'ajout d'un agent pour les instances Citrix ADC dans les centres de données distants est recommandé mais pas obligatoire.
>
> Si vous souhaitez ajouter l'instance directement au MAS principal, ne sélectionnez pas**d'agent** lors de l'ajout d'instances.

Basculement sur incident de l'agent Citrix ADM

Le basculement de l'agent peut se produire sur un site qui a deux agents enregistrés ou plus. Lorsqu'un agent devient inactif (état DOWN) sur le site, Citrix ADM redistribue les instances ADC de l'agent inactif avec d'autres agents actifs.

> **Important**
>
> - Assurez-vous que la fonctionnalité de **basculement de l'agent** est activée sur votre compte. Pour activer cette fonctionnalité, reportez-vous à la section Activer ou désactiver les fonctionnalités ADM.

> - Si un agent exécute un script, assurez-vous qu'il est présent sur tous les agents du site. Par conséquent, l'agent modifié peut exécuter le script après le basculement de l'agent.

Pour attacher un site à un agent dans l'interface graphique d'ADM, reportez-vous à la section Attacher un agent à un site.

Pour effectuer un basculement de l'agent, sélectionnez les agents Citrix ADM un par un et attachez-les au même site.

Par exemple, deux agents 10.106.1xx.2x et 10.106.1xx.3x sont rattachés et opérationnels sur le site de Bangalore. Si un agent devient inactif, Citrix ADM le détecte et affiche l'état comme arrêté.

Lorsqu'un agent Citrix ADM devient inactif (état Down) sur un site, Citrix ADM attend pendant cinq minutes que l'agent devienne actif (état Up). Si l'agent reste inactif, Citrix ADM redistribue automatiquement les instances entre les agents disponibles sur le même site.

Citrix ADM déclenche une redistribution d'instance toutes les 30 minutes pour équilibrer la charge entre les agents actifs du site.

Installer un agent ADM en tant que microservice sur un cluster Kubernetes

February 1, 2024

Le déploiement d'un agent Citrix ADM en tant que microservice est utile pour gérer votre Citrix ADC CPX. Les procédures disponibles dans ce document ne s'appliquent que si le cluster Citrix ADM et Kubernetes sont configurés sur un réseau différent. Dans ce scénario, vous pouvez configurer un agent ADM en tant que microservice, où le cluster Kubernetes est hébergé.

> Remarque
>
> Vous pouvez également configurer un agent sur site et enregistrer l'agent sur le réseau, où le cluster Kubernetes est hébergé.

Mise en route

1. Dans Citrix ADM, accédez à **Réseaux > Agents**.
2. **Dans la liste Sélectionner une action**, sélectionnez l'option **Microservice de l'agent de téléchargement**.
3. Dans la page **Microservice de l'agent de téléchargement**, spécifiez les paramètres suivants :

a) **ID d'application** —ID de chaîne permettant de définir le service de l'agent dans le cluster Kubernetes et de distinguer cet agent des autres agents du même cluster.

b) **Mot de passe** —Indiquez un mot de passe pour que CPX utilise ce mot de passe pour embarquer CPX à ADM via l'agent.

c) **Confirmer le mot de passe** —Spécifiez le même mot de passe pour confirmation.

> Remarque
>
> Vous ne devez pas utiliser le mot de passe par défaut (`nsroot`).

d) Cliquez sur **Télécharger le fichier Yaml**.

Installer l'agent Citrix ADM dans le cluster Kubernetes

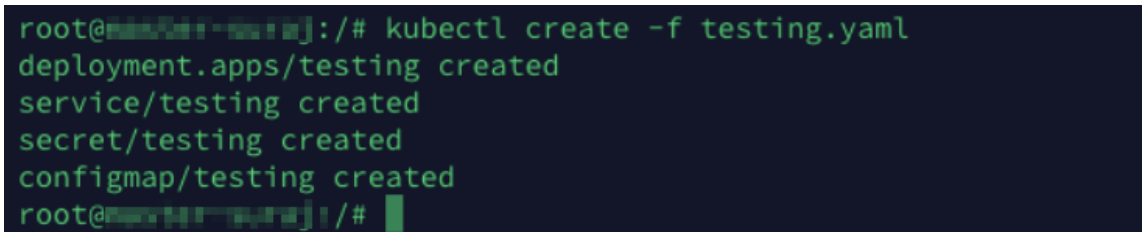
Dans le nœud principal de Kubernetes :

1. Enregistrer le fichier YAML téléchargé
2. Exécutez la commande suivante :

   `kubectl create -f <yaml file>`

   Par exemple, `kubectl create -f testing.yaml`

   L'agent est créé avec succès.



Dans Citrix ADM, accédez à **Réseaux** > **Agents** pour afficher l'état de l'agent.

Pour plus d'informations sur la mise en route du graphe de service, reportez-vous à la section Configuration du graphique de service.

Migrer le déploiement d'un serveur unique Citrix ADM vers un déploiement haute disponibilité

February 1, 2024

Vous pouvez mettre à niveau votre serveur unique Citrix ADM vers un déploiement haute disponibilité de deux serveurs Citrix ADM. Une paire de serveurs Citrix ADM à haute disponibilité est en mode actif-passif, et les deux serveurs ont la même configuration. Dans ce type de déploiement actif-passif, un serveur Citrix ADM est configuré en tant que nœud principal et l'autre en tant que nœud secondaire. Si, pour une raison quelconque, le nœud principal tombe en panne, le nœud secondaire prend le relais.

Pour migrer un serveur unique Citrix ADM vers une paire haute disponibilité, vous devez provisionner un nouveau nœud de serveur Citrix ADM, le configurer en tant que deuxième serveur unique Citrix ADM et déployer les deux serveurs Citrix ADM en tant que paire haute disponibilité.

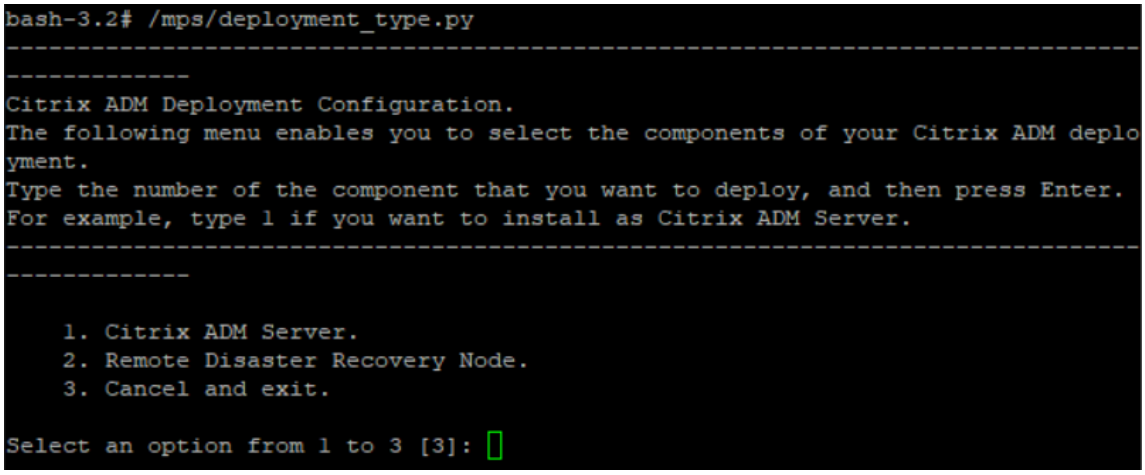
La migration d'un serveur unique Citrix ADM vers un mode haute disponibilité implique les étapes suivantes :

1. Modification du nœud de serveur existant
2. Provisioning du deuxième nœud de serveur
3. Déploiement des deux nœuds en mode HA
4. Configuration de la paire haute disponibilité

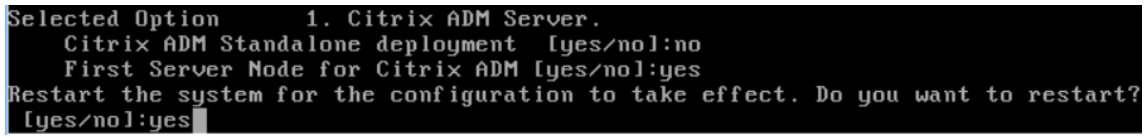
Modifier le nœud de serveur Citrix ADM existant

Pour faire passer le Citrix ADM du mode serveur unique au mode haute disponibilité, vous devez modifier le type de déploiement initial du nœud de serveur en mode haute disponibilité.

1. Sur une station de travail ou un ordinateur portable, ouvrez la console du nœud de serveur Citrix ADM existant. Par exemple, considérez que vous avez déployé un Citrix ADM dont l'adresse IP est 10.106.171.17 en tant que serveur autonome.
2. Connectez-vous à Citrix ADM. Les informations d'identification par défaut sont `nsroot` et `nsroot`.
3. Dans l'invite du shell `/mps/deployment_type.py`, tapez et appuyez sur **Entrée**.
4. Sélectionnez le type de déploiement en tant que serveur Citrix ADM. Si vous ne sélectionnez aucune option, par défaut, elle est déployée en tant que serveur.



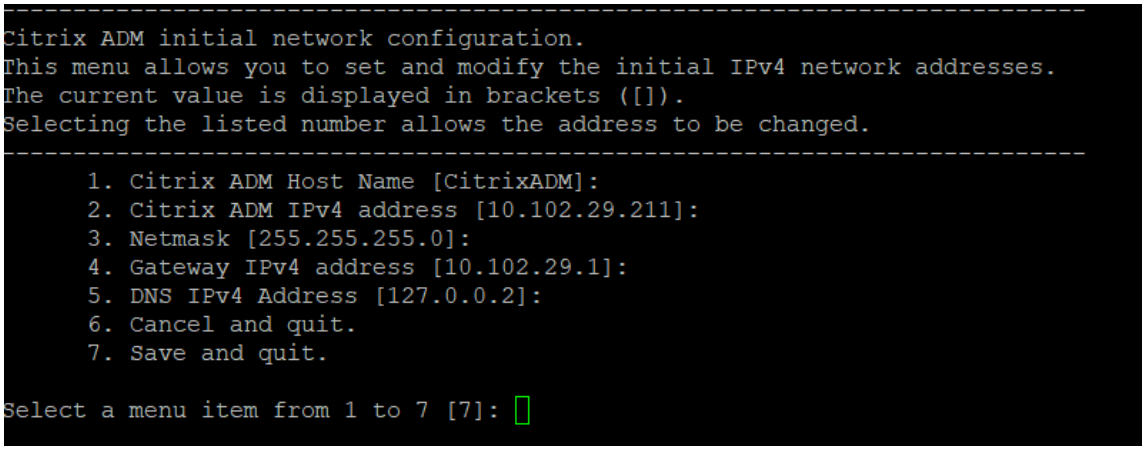
5. La console de déploiement vous invite à sélectionner le déploiement du serveur (en tant que serveur autonome). Tapez **Non** pour confirmer le déploiement comme paire haute disponibilité.
6. La console vous invite à sélectionner le (premier nœud de serveur). Entrez **Oui** pour confirmer que le nœud est le premier nœud de serveur.
7. La console vous invite à redémarrer le serveur.
8. Tapez **Oui** pour redémarrer.



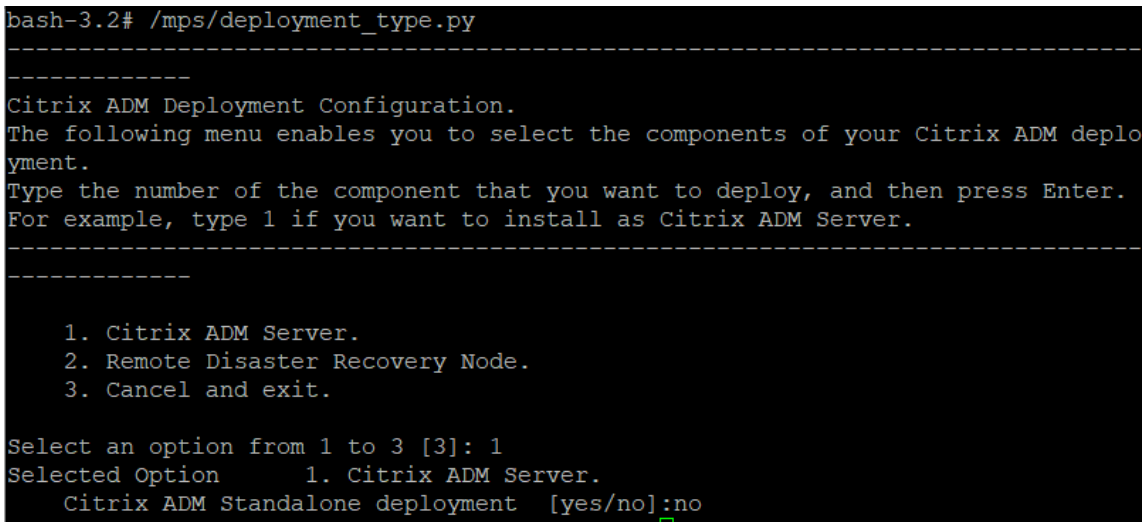
Provisionner le deuxième nœud de serveur

Vous devez provisionner le second serveur sur votre Hypervisor. Utilisez le même fichier image que celui que vous avez utilisé pour installer le premier serveur ou procurez-vous un fichier image de la même version sur le site de téléchargement de Citrix.

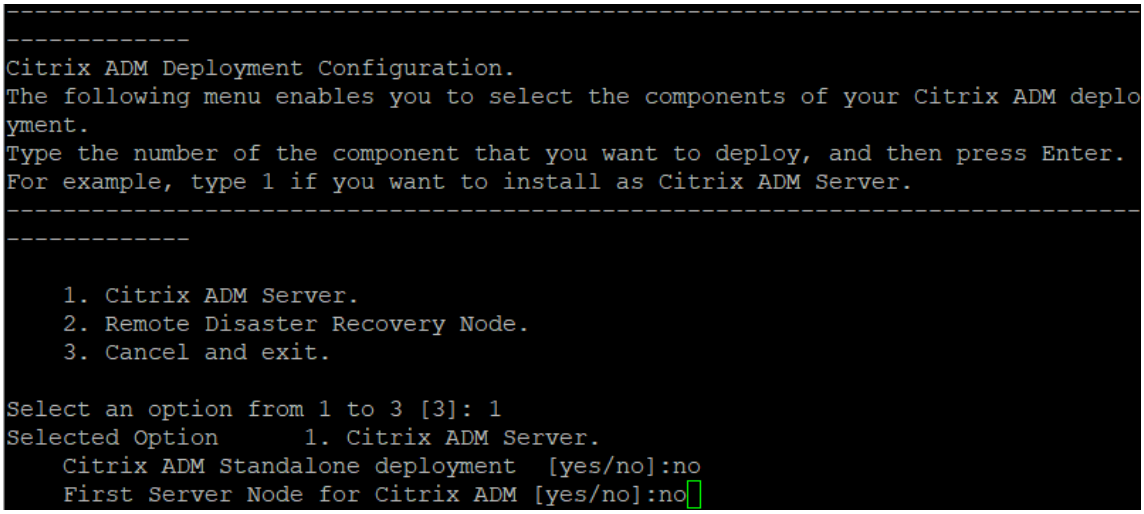
1. Importez le fichier image dans votre Hypervisor, puis, à partir de l'onglet Console, configurez les options de configuration réseau initiales comme expliqué sur l'écran suivant :



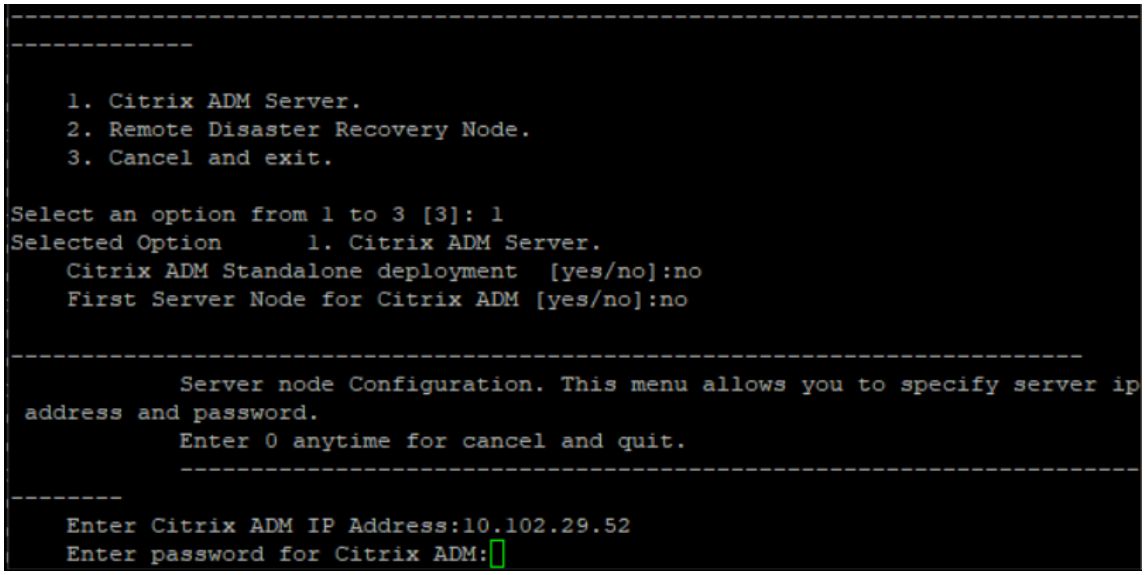
2. Après avoir spécifié les adresses IP requises, dans l'invite du shell, tapez /mps/deployment_type.py et appuyez sur Entrée.
3. Sélectionnez le type de déploiement en tant que **serveur Citrix ADM.**
4. La console de déploiement vous invite à sélectionner le déploiement du serveur (en tant que serveur autonome). Tapez **Non** pour confirmer le déploiement comme paire haute disponibilité.



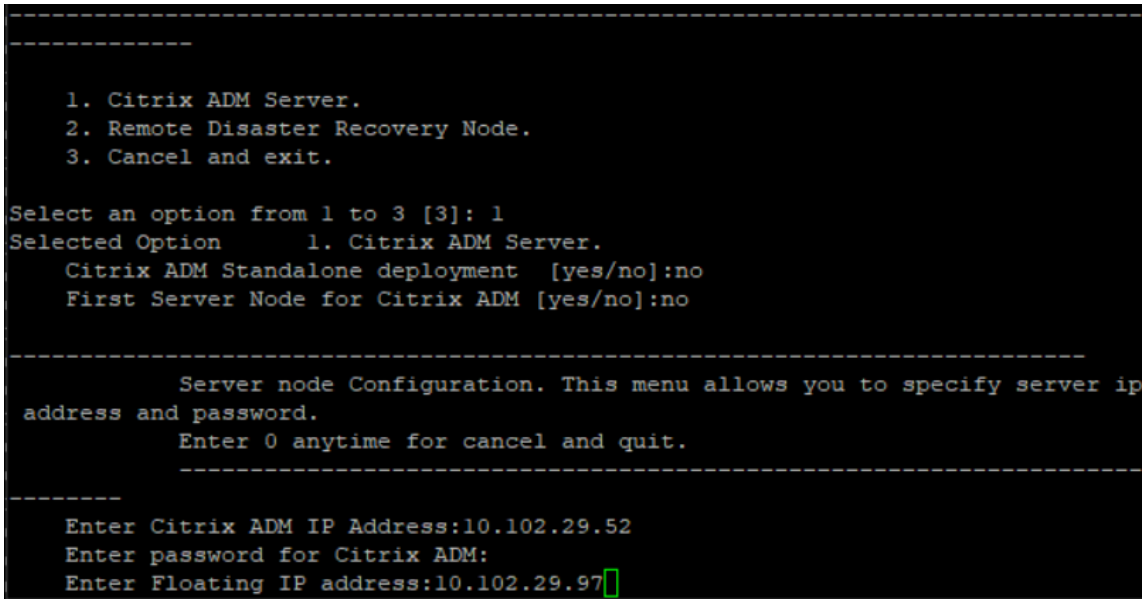
5. La console vous invite ensuite à sélectionner le (premier nœud de serveur). Tapez **Non** pour confirmer que le nœud est le deuxième nœud du serveur.



6. Entrez l'adresse IP et le mot de passe du premier serveur.



7. Entrez l'adresse IP flottante du premier nœud.



8. La console vous invite à redémarrer le système. Entrez **Oui** pour redémarrer.

Déployer les deux serveurs en mode haute disponibilité

Pour terminer le processus d'installation des deux nœuds de serveur en tant que paire haute disponibilité, vous devez déployer ces nœuds à partir de l'interface graphique du nœud de serveur Citrix ADM existant précédemment. La communication interne entre les deux serveurs démarre lorsque vous déployez les deux nœuds de serveur.

> **Important**
>
> Avant de déployer des nœuds haute disponibilité, veillez à modifier le mot de passe par défaut.

1. Dans un navigateur Web, tapez l'adresse IP du nœud serveur Citrix ADM existant précédemment.
2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Sous l'onglet **Système**, accédez à **Déploiement** et cliquez sur **Déployer**.
4. Un message de confirmation s'affiche. Cliquez sur **Oui**.

   > **Remarque**
   >
   > Après avoir déployé Citrix ADM en haute disponibilité, vous pouvez accéder au nœud principal ou à l'adresse IP flottante. Vous ne pouvez pas accéder au nœud secondaire à partir de la version 12.1.

5. Bien que vous ayez saisi l'adresse IP flottante lors de la configuration du deuxième nœud de serveur, vous avez la possibilité de mettre à jour le FIP sur la page **Systèmes** . Cliquez sur

Paramètres HA > **Configurer l'adresse IP flottante pour le mode haute disponibilité**. Vous pouvez afficher l'adresse IP flottante que vous avez configurée précédemment. Vous pouvez entrer une nouvelle adresse IP et cliquer sur **OK**.

Migrer de NetScaler Insight Center vers Citrix ADM

February 1, 2024

Vous pouvez désormais migrer votre déploiement NetScaler Insight Center vers Citrix ADM sans perdre la configuration, les paramètres ou les données existants. Avec Citrix ADM, vous pouvez non seulement afficher les différentes analyses générées par les instances Citrix ADC associées à une application, mais également gérer, surveiller et dépanner l'ensemble de l'infrastructure de distribution d'applications globale à partir d'une console unifiée unique.

> **Remarque**
>
> La migration n'est actuellement prise en charge que sur les instances NetScaler Insight Center Standalone.

Conditions préalables

Avant de migrer l'appliance virtuelle NetScaler Insight Center vers Citrix ADM, vérifiez que les conditions suivantes ont été remplies :

- NetScaler Insight Center 11.1 Build 47.14 ou version ultérieure est installé.
- Vous avez téléchargé le fichier image Citrix ADM 12.0 build 57.24 .tgz.

  > **Remarque**
  >
  > Vous devez installer Citrix ADM 12.0 build 57.24, puis mettre à niveau vers la dernière version de Citrix ADM 13.0. Pour plus d'informations, consultez la section Mettre à niveau.

- Vous avez téléchargé le dernier fichier d'image .tgz de génération Citrix ADM 13.0.

Exigences matérielles

Composant	Exigences
RAM	32 GB

Composant	Exigences
CPU virtuel	8 processeurs
Espace de stockage	120 GB **Remarque** Citrix vous recommande d'utiliser**500 Go**pour de meilleures performances. Citrix recommande également d'utiliser la technologie SSD (Solid State Drive) pour les déploiements Citrix ADM.
Interfaces réseau virtuelles	1
Débit	1 Gbit/s ou 100 Mbit/s
Exigences relatives à l'hyperviseur	
Citrix Hypervisor	6.2, 6.5
VMware ESX	5.5, 6.0
Microsoft Hyper-V	2012 R2
Linux - KVM	Ubuntu, Fedora

Procédure d'installation

Pour migrer NetScaler Insight Center vers Citrix ADM :

1. Connectez-vous à l'invite shell de NetScaler Insight Center.
2. Téléchargez la version 57.24 de Citrix ADM 12.0 dans le dossier */var/mps/mps_images*.
3. Décompressez le fichier TGZ à l'aide de la commande **tar -zxvf build-mas-12.0-57.24.tgz**.

```
bash-3.2# tar -zxvf build-mas-12.0.57.24.tgz
```

4. Installez Citrix ADM à l'aide de **. /installmas**.

```
bash-3.2# ./installmas
```

5. Après l'installation de Citrix ADM 12.0 build 57.24, vous devez effectuer la mise à niveau vers la dernière version de Citrix ADM 13.0 en effectuant les étapes ci-dessus.

Après la migration, toutes les instances Citrix ADC qui ont été découvertes dans l'inventaire NetScaler Insight Center apparaissent dans la section **Réseaux > Instances** de Citrix ADM. Toutefois, pour la première fois, vous devez interroger manuellement les serveurs virtuels hébergés dans les appliances découvertes.

> **Remarque**
>
> Dans Citrix ADM, par défaut, il n'y a aucun coût de licence pour gérer et surveiller deux serveurs virtuels créés dans les instances Citrix ADC découvertes. Pour surveiller et gérer plus de deux serveurs virtuels, installez les licences Citrix ADM requises. Pour plus de détails, consultez la section Système de licences Citrix ADM.

Intégrer Citrix ADM avec Citrix Director

February 1, 2024

Director s'intègre à Citrix ADM pour l'analyse du réseau et la gestion des performances.

- L'analyse du réseau permet d'obtenir des rapports HDX Insight auprès de Citrix ADM et fournit une vue d'application et de bureau du réseau. Grâce à cette fonctionnalité, Director fournit une vue analytique avancée du trafic ICA dans votre déploiement.
- La gestion des performances fournit un archivage des données d'historique ainsi que des rapports de tendance. Avec la conservation de l'historique des données par rapport à l'évaluation en temps réel, vous pouvez créer des rapports de tendance, y compris des tendances de capacité et d'intégrité.

Une fois que vous avez intégré Citrix ADM à Director, les rapports HDX Insight vous fournissent les informations suivantes dans Director :

- L'onglet Réseau de la page Tendances indique les effets de latence et de bande passante pour les applications, les postes de travail et les utilisateurs tout au long de votre déploiement.
- La page Détails de l'utilisateur affiche des informations spécifiques à la latence et à la bande passante pour une session utilisateur particulière.

Conditions préalables

Configuration matérielle requise pour la migration de HDX Insight vers Citrix ADM

Composant	Exigences
RAM	32 GB
CPU virtuel	8
Espace de stockage	500 GB. Citrix recommande d'utiliser la technologie SSD (Solid State Drive) pour les déploiements Citrix ADM.
Interfaces réseau virtuelles	1
Débit	1 Gbit/s ou 100 Mbit/s

Configuration logicielle requise

Avant de migrer vers l'appliance virtuelle Citrix ADM, vérifiez que les conditions suivantes ont été remplies :

- La version 1811 de Director est installée
- NetScaler HDX Insight version 10.1 ou ultérieure est installé
- HDX Insight et Citrix ADM prennent en charge Citrix VDA version 7.0 et versions ultérieures
- Citrix Workspace est pris en charge sur Citrix Virtual Apps and Desktops version 7.0 et ultérieure
- Assurez-vous que MAC, Citrix Receiver pour Mac version 11.8 et versions ultérieures, et Windows Citrix Receiver pour Windows 14.0 et versions ultérieures sont disponibles pour afficher des métriques ICA RTT précises.
- Citrix ADM version 11.0 et ultérieure est installé. Pour plus d'informations sur la façon d'installer Citrix ADM, consultez Déployer Citrix ADM.

Limitations

- La disponibilité de cette fonctionnalité dépend de la licence de votre organisation et vos permissions d'administrateur.
- La session Round Trip Time (RTT) de l'ICA affiche correctement les données pour Citrix Receiver pour Windows 3.4 ou version ultérieure et pour Citrix Receiver pour Mac 11.8 ou version ultérieure. Pour les versions antérieures de ces Receiver, les données ne s'affichent pas correctement.
- Dans la vue Tendances, les données d'ouverture de session de connexion HDX ne sont pas collectées pour les VDA antérieurs à la version 7. Pour les VDA antérieurs, les données du graphique sont affichées en tant que 0.

- Pour les déploiements qui possèdent déjà un disque dur externe dont l'espace de stockage est inférieur à 500 Go, vous ne pouvez pas ajouter un autre disque dur.

> **Remarque**
>
> - Pour plus d'informations sur Director et pour les étapes à suivre pour intégrer Citrix ADM à Director, reportez-vous à la section https://docs.citrix.com/en-us/xenapp-and-xendesktop/7-15-ltsr/director/hdx-insight.html.
> - Pour plus d'informations sur HDX Insight, reportez-vous à la sectionhttp://docs.citrix.com/en-us/xenapp-and-xendesktop/7-11/director/hdx-insight.html.

Attacher un disque supplémentaire à Citrix ADM

February 1, 2024

Les besoins en stockage de Citrix Application Delivery Management (ADM) sont déterminés en fonction de votre estimation de dimensionnement Citrix ADM. Par défaut, Citrix ADM vous fournit une capacité de stockage de 120 Go. Si vous avez besoin de plus de 120 Go pour stocker vos données, vous pouvez attacher un disque supplémentaire.

> **Remarque**
>
> - Estimez les besoins en stockage et connectez un disque supplémentaire au serveur au moment du déploiement initial de Citrix ADM.
> - Pour un déploiement Citrix ADM mono-serveur, vous ne pouvez attacher qu'un seul disque au serveur en plus du disque par défaut.
> - Pour un déploiement haute disponibilité Citrix ADM, vous devez attacher un disque supplémentaire à chaque nœud. La taille des deux disques doit être identique.
> - Si vous avez déjà rattaché un disque externe de capacité inférieure, vous devez le retirer avant de joindre un nouveau disque.
> - Vous pouvez attacher un disque supplémentaire d'une capacité supérieure à 2 téraoctets. Si nécessaire, la taille du disque peut également être inférieure à 2 téraoctets.
> - Citrix recommande d'utiliser la technologie SSD (Solid State Drive) pour les déploiements Citrix ADM.

Ce document explique les scénarios suivants concernant l'attachement d'un nouveau disque supplémentaire, la création de partitions et le redimensionnement des disques supplémentaires :

1. Attacher un nouveau disque supplémentaire
2. Lancez l'outil de partitionnement de disque
3. Créer des partitions dans le nouveau disque supplémentaire
4. Redimensionner le disque supplémentaire existant
5. Supprimer les partitions sur le disque supplémentaire

Attacher un disque supplémentaire dans un Citrix ADM autonome

Pour attacher un disque à la machine virtuelle, procédez comme suit :

1. Arrêtez la machine virtuelle Citrix ADM.
2. Dans l'Hypervisor, attachez un disque supplémentaire de la taille de disque requise à la machine virtuelle Citrix ADM.

   Le disque nouvellement connecté stocke les données de base de données et les fichiers journaux Citrix ADM. Le disque par défaut existant de 120 gigaoctets est désormais utilisé pour stocker les fichiers principaux, les fichiers journaux du système d'exploitation, etc.
3. Démarrez la machine virtuelle Citrix ADM.

Outil de partition de disque Citrix ADM

Citrix ADM fournit désormais l'**outil de partition de disque Citrix ADM**, un nouvel outil de ligne de commande. Les fonctionnalités de cet outil sont décrites en détail comme suit :

1. À l'aide de l'outil, vous pouvez créer des partitions dans le disque supplémentaire nouvellement ajouté.
2. Vous pouvez également redimensionner un disque supplémentaire existant à l'aide de cet outil. Mais le disque externe existant ne doit pas dépasser 2 téraoctets.

   > **Remarque**
   >
   > - Il n'est pas possible de redimensionner des disques existants au-delà de 2 téraoctets sans perdre de données. Cela est dû à une limitation connue de la plateforme.
   > - Pour créer une capacité de stockage supérieure à 2 téraoctets, vous devez supprimer les partitions existantes et créer des partitions à l'aide de ce nouvel outil.

3. À l'aide de ce nouvel outil, vous pouvez effectuer n'importe quelle action de partition sur le disque de manière explicite. L'outil vous offre une visibilité et un contrôle clairs sur le disque et les données associées.

> **Remarque**
>
> Vous ne pouvez utiliser cet outil que sur le disque supplémentaire que vous avez connecté au serveur Citrix ADM. Vous ne pouvez pas créer de partitions sur le disque principal (par défaut) de 120 gigaoctets à l'aide de cet outil.

Lancez l'outil de partition de disque

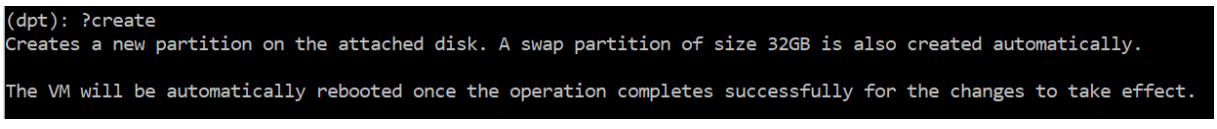
1. Ouvrez une connexion SSH à Citrix ADM à l'aide d'un client SSH, tel que PuTTY.
2. Ouvrez une session sur Citrix ADM à l'aide des informations d'identification de l'administrateur.
3. Passez à l'invite shell et tapez :

```
/mps/DiskPartitionTool.py
<!--NeedCopy-->
```

> **Remarque**
>
> Pour Citrix ADM dans le cadre d'un déploiement haute disponibilité, vous devez lancer l'outil sur les deux nœuds et créer ou redimensionner des partitions après avoir attaché des disques aux machines virtuelles respectives.

Créez des partitions sur le nouveau disque supplémentaire

La commande **create** est utilisée pour créer des partitions chaque fois qu'un nouveau disque secondaire est ajouté. Vous pouvez également utiliser cette commande pour créer des partitions sur un disque secondaire existant après la suppression des partitions existantes à l'aide de la commande « remove ».

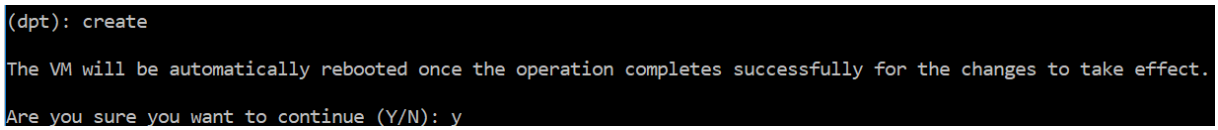


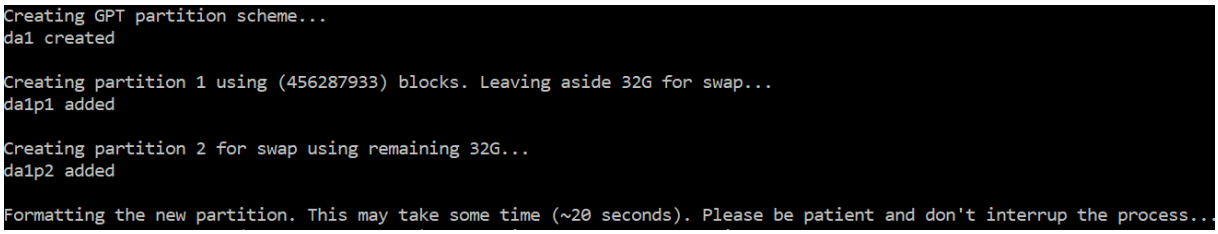
> **Remarque**
>
> Il n'y a pas de limitation de taille de 2 téraoctets lors de la création de partitions avec l'outil de

> partition de disque. L'outil peut créer des partitions de plus de 2 téraoctets. Lorsque vous partitionnez le disque, une partition d'échange d'une taille de 32 Go est automatiquement ajoutée. La partition principale utilise alors tout l'espace restant sur le disque.

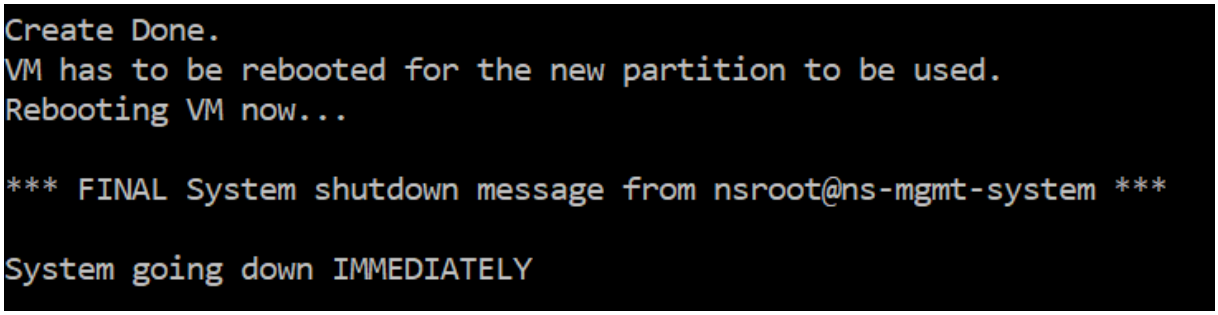
Une fois la commande exécutée, un schéma de partition de table de partition GUID (GPT) est créé. Une partition de swap de 32 Go et une partition de données sont également créées pour utiliser le reste de l'espace. Un nouveau système de fichiers est ensuite créé sur la partition principale.

> **Remarque**
>
> Ce processus peut prendre quelques secondes et vous ne devez pas interrompre le processus.

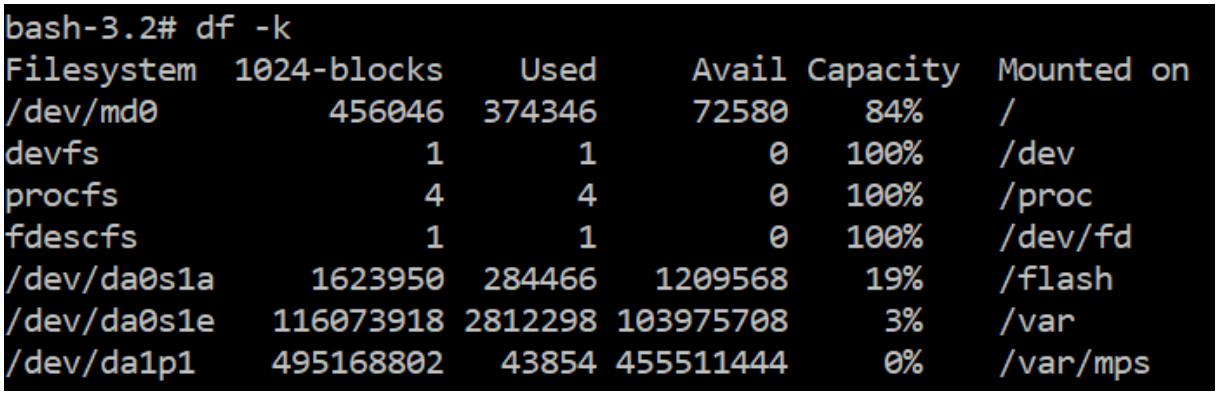




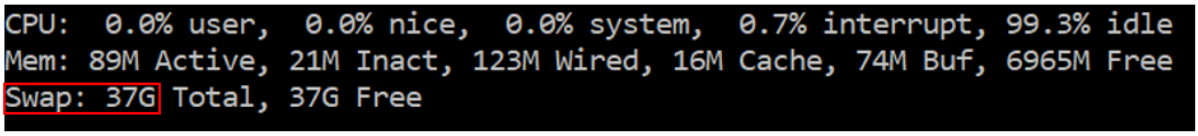
Une fois la commande create terminée, la machine virtuelle est automatiquement redémarrée pour que la nouvelle partition soit montée.



Après le redémarrage, la nouvelle partition est montée sur /var/mps.



La partition swap ajoutée apparaît sous forme d'espace swap dans la sortie de la commande « create ».

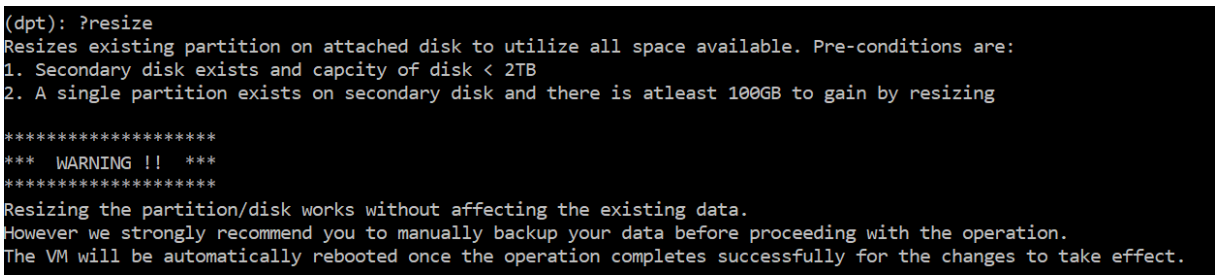


> **Remarque**
>
> L'outil redémarre la machine virtuelle une fois que vous avez créé la partition.

Redimensionner les partitions du disque supplémentaire existant

Vous pouvez utiliser la commande **resize** pour redimensionner le disque attaché (secondaire). Vous pouvez redimensionner un disque doté d'un schéma `master boot record` (MBR) ou GPT. La taille du disque doit être inférieure à 2 téraoctets pour un maximum de 2 téraoctets.

> **Remarque**
>
> - La commande « redimensionner » est conçue pour fonctionner sans perdre de données existantes. Citrix recommande toutefois de sauvegarder les données critiques de ce disque sur un stockage externe avant de tenter le redimensionnement. La sauvegarde des données est utile dans les cas où les données du disque peuvent être corrompues pendant l'opération de redimensionnement.
> - Assurez-vous d'augmenter l'espace disque par incréments de 100 Go d'espace lors du redimensionnement des partitions. Une telle augmentation incrémentielle garantit que vous n'auriez pas à redimensionner plus fréquemment.



La commande « redimensionner » vérifie toutes les conditions préalables et procède si toutes les conditions préalables sont remplies et après avoir donné votre consentement au redimensionnement. Il arrête les processus accédant au disque, notamment les sous-systèmes Citrix ADM, les processus de base de données PostgreSQL et le processus de surveillance Citrix ADM. Une fois les processus arrêtés, le disque est démonté pour le préparer au redimensionnement. Le redimensionnement se fait en étendant la partition pour occuper tout l'espace disponible, puis en développant le système de fichiers. Si une partition d'échange existe sur le disque, elle est supprimée et recréée à la fin du disque après

le redimensionnement. La partition d'échange est abordée dans la section **Créer** une commande du document.

> **Remarque**
>
> Le processus de « croissance du système de fichiers » peut prendre un certain temps et veiller à ne pas interrompre le processus pendant qu'il est en cours. L'outil redémarre la machine virtuelle après avoir redimensionné la partition.

```
(dpt): resize

********************
***  WARNING !!  ***
********************
Resizing the partition/disk works without affecting the existing data.
However we strongly recommend you to manually backup your data before proceeding with the operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to resize (Y/N): y
```

```
Unmounting partition: /dev/da1p1 from: /var/mps
OK to resize existing partition.
Disabling swap on partition: /dev/da1p2
Deleting swap partition: da1p2
Resizing partition da1p1...
da1p1 resized

Adding a swap partition da1p2...
da1p2 added

Formatting the newly added portions of the partition. This may take some time (~10 seconds). Please be patient and don't
 interrup the process...
```

Toutes les étapes intermédiaires du processus de redimensionnement (arrêt des applications, redimensionnement du disque, croissance du système de fichiers) sont affichées sur la console. Une fois le processus terminé, le message suivant s'affiche.

```
Resize Done.
VM has to be rebooted for the resized partition to be used.
Rebooting VM now...

*** FINAL System shutdown message from nsroot@ns-mgmt-system ***

System going down IMMEDIATELY
```

Après le redémarrage, l'augmentation de taille peut être observée à l'aide de la commande « df ». Voici les détails avant et après avoir augmenté la taille :

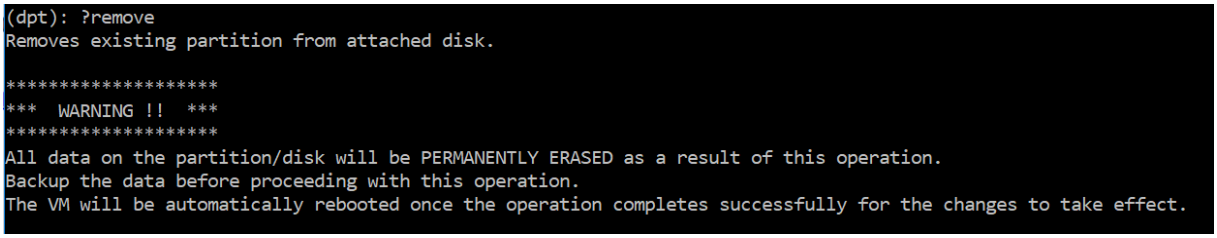
```
bash-3.2# df -k
Filesystem  1024-blocks    Used     Avail Capacity  Mounted on
/dev/md0         456046  374864     72062    84%    /
devfs                 1       1         0   100%    /dev
procfs                4       4         0   100%    /proc
fdescfs               1       1         0   100%    /dev/fd
/dev/da0s1a     1623950  284468   1209566    19%    /flash
/dev/da0s1e   116073918 1662048 105125958     2%    /var
/dev/da1s1a   152329216 3082226 137060654     2%    /var/mps
```

```
bash-3.2# df -k
Filesystem  1024-blocks    Used     Avail Capacity  Mounted on
/dev/md0         456046  374838     72088    84%    /
devfs                 1       1         0   100%    /dev
procfs                4       4         0   100%    /proc
fdescfs               1       1         0   100%    /dev/fd
/dev/da0s1a     1623950  284468   1209566    19%    /flash
/dev/da0s1e   116073918 1666800 105121206     2%    /var
/dev/da1s1a   304651668 3137954 277141582     1%    /var/mps
```

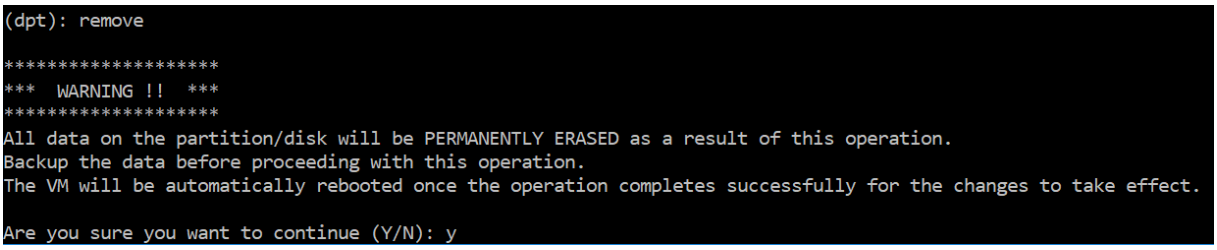

Supprimez les partitions du disque supplémentaire

Une partition existante sur le disque secondaire peut être redimensionnée jusqu'à 2 téraoctets. Ceci est dû à une limitation connue de la partition. Si vous voulez un disque de plus de 2 téraoctets, connectez un nouveau disque et partitionnez-le à l'aide de l'outil de partition de disque. Vous pouvez également supprimer la partition existante à l'aide de la commande **remove**, puis créer une partition.

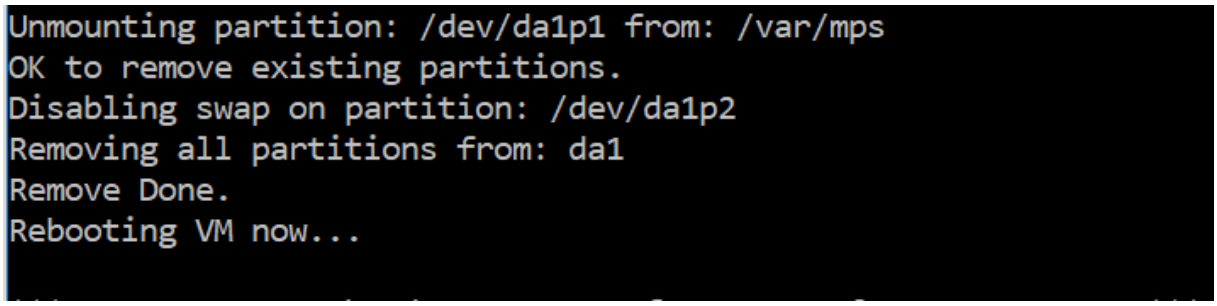
> **Remarque**
>
> La suppression de la partition existante supprime toutes les données existantes. Par conséquent, toutes les données critiques doivent être sauvegardées sur un stockage externe avant d'utiliser cette commande.



L'exécution de la commande « remove » vous demande une confirmation et une fois confirmée, elle arrête tous les processus (tels que les sous-systèmes ADM, les processus PostgreSQL et le moniteur ADM) à l'aide du disque secondaire. Si une partition de swap existe et que le swap est activé sur la partition, le swap est désactivé.



Lorsque vous tapez « y », la commande démonte le disque et supprime toutes les partitions du disque.



> **Remarque**
>
> L'outil redémarre la machine virtuelle une fois que vous avez supprimé la partition.

Redémarrez la machine virtuelle

Lorsqu'une partition est créée ou redimensionnée, ou lorsqu'un fichier d'échange est créé, redémarrez la machine virtuelle. Les modifications ne prennent effet qu'après le redémarrage. A cet effet, une commande de **redémarrage** est fournie dans l'outil.

```
(dpt): ?reboot
Reboot the VM. Note: VM has to be rebooted after new partition is created, existing one is resized or swap file is creat
ed.
The VM is rebooted automatically after these operations. If the automatic reboot does not happen, then this command can
be used to reboot the VM.
```

Vous êtes invité à confirmer et une fois confirmé, il arrête tous les processus (tels que les sous-systèmes ADM, les processus PostgreSQL et le moniteur ADM). La machine virtuelle est ensuite redémarrée.

```
(dpt): reboot
Are you sure you want to reboot the VM (Y/N): y
```

```
Rebooting VM now...

*** FINAL System shutdown message from nsroot@ns-mgmt-system ***

System going down IMMEDIATELY
```

Créer un fichier de sauvegarde des données du disque

Voici les étapes à suivre pour sauvegarder les données Citrix ADM avant de redimensionner ou de supprimer les partitions.

> **Remarque**
>
> La création d'un fichier de sauvegarde nécessite de l'espace disque. Citrix vous recommande de vous assurer qu'il y a suffisamment d'espace disque disponible (50 % ou plus) avant l'exécution des commandes de sauvegarde.

1. Arrêtez ADM.

```
1 /mps/masd stop
2 <!--NeedCopy-->
```

2. Arrêtez PostgreSQL.


```
su -l mpspostgres /mps/scripts/pgsql/stoppgsql_smart.sh
<!--NeedCopy-->
```

3. Arrêter le moniteur ADM.

```
/mps/scripts/stop_mas_monit.sh
<!--NeedCopy-->
```

4. Créez un tarball.

```
cd /var
tar cvfz /var/mps/mps_backup.tgz mps
<!--NeedCopy-->
```

> **Remarque**
>
> L'opération prend du temps en fonction de la taille des données à sauvegarder.

5. Générer une somme de contrôle.

```
md5 /var/mps/mps_backup.tgz > /var/mps/mps_backup_checksum
<!--NeedCopy-->
```

6. Copiez les fichiers tarball et de somme de contrôle sur un serveur distant.
7. Valider l'exactitude de l'archive copiée. Générez une somme de contrôle du fichier transféré et comparez-la à la somme de contrôle source.
8. Supprimez l'archive tar de la machine virtuelle ADM.

```
cd /var/mps/
rm mps_backup.tgz  mps_backup_checksum
<!--NeedCopy-->
```

Commandes supplémentaires

Outre les commandes répertoriées précédemment, vous pouvez également utiliser les commandes suivantes dans l'outil :

Commande d'aide :

Pour répertorier les commandes prises en charge, tapez **help** ou **?** et appuyez sur Entrée. Pour obtenir de l'aide supplémentaire sur chacune des commandes appuyez sur l'**aide** ou **?** suivi du nom de la commande et appuyez sur la touche **Entrée**.


```
(dpt): help

DPT Commands
------------
create  create_swapfile  exit  help  info  reboot  remove  resize

(dpt):
```

Commande Info :

La commande **info** fournit des informations sur le disque secondaire connecté s'il existe. La commande fournit le nom du périphérique, le schéma de partition, la taille sous forme lisible par l'homme et le nombre de blocs de disque. Le schéma peut être MBR ou GPT. Un schéma MBR signifie que le disque a été partitionné à l'aide d'une version antérieure de la version Citrix ADM. La partition basée sur MBR/GPT peut être redimensionnée mais pas au-delà de 2 téraoctets. Le schéma de partition GPT signifie que le disque a été partitionné à l'aide de Citrix ADM 12.1 ou version ultérieure.

> **Remarque**
>
> Une partition GPT peut être supérieure à 2 téraoctets, mais lors de sa création. Toutefois, vous ne pouvez pas redimensionner le disque à une taille supérieure à 2 téraoctets après avoir créé un disque de taille inférieure. Il s'agit d'une limitation connue de la plate-forme.

```
(dpt): ?info
Provides information about attached disk (if found).
(dpt): info
--------------
Disk: da1
Scheme: MBR
Size: (150G)
Blocks: 314572737
--------------
(dpt):
```

Commande Create_SWAPFile :

La partition d'échange par défaut sur le disque principal de Citrix ADM est de 4 Go et, par conséquent, l'espace d'échange par défaut est de 4 Go. Pour la configuration de mémoire par défaut de Citrix ADM, qui est de 2 Go, cet espace d'échange est suffisant. Toutefois, lorsque vous exécutez Citrix ADM avec une configuration de mémoire plus élevée, vous devez disposer de plus d'espace d'échange alloué sur le disque.

> **Remarque**
>
> La partition de swap est généralement une partition dédiée qui est créée sur un disque dur (HDD) lors de l'installation du système d'exploitation. Une telle partition est également appelée espace de permutation. La partition d'échange est utilisée pour la mémoire virtuelle qui simule la mémoire principale supplémentaire.

Les disques secondaires ajoutés dans les versions antérieures de Citrix ADM n'ont pas de partition d'échange créée par défaut. La commande « create_swapfile » est destinée aux disques secondaires créés à l'aide d'anciennes versions de Citrix ADM qui n'ont pas de partition d'échange. La commande vérifie les éléments suivants :

- Présence d'un disque secondaire
- Disque en cours de montage
- Taille du disque (au moins 500 Go)
- L'existence du fichier d'échange

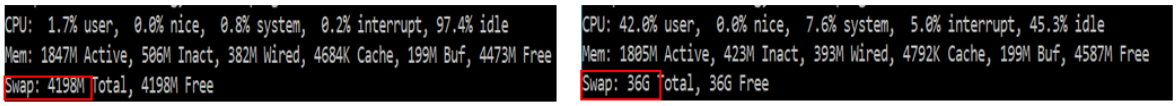
La commande « create_swapfile » n'est utile que lorsque la mémoire est supérieure ou égale à 16 Go et non lorsque la mémoire est faible. Par conséquent, cette commande vérifie également la mémoire avant de procéder à la création du fichier d'échange.

```
(dpt): ?create_swapfile
Creates a 32GB swap file on the secondary disk. Pre-conditions are:
1. Secondary disk exists
2. Secondary disk is partitioned and mounted
3. Capacity of disk >= 500GB
4. Swap file is not already found
5. RAM size >= 16GB

Creating swapfile is a time consuming operation and can take ~5 minutes to complete. Once started the operation should n
ot be interrupted.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

Si toutes les conditions sont remplies et que l'utilisateur consent à continuer, un fichier d'échange de 32 Go est créé sur le disque secondaire. Le processus de création du fichier d'échange prend quelques minutes et veillez à ne pas interrompre le processus en cours. Une fois terminé, un redémarrage est effectué pour que le fichier d'échange prenne effet.

```
Creating swapfile. This may take some time (~5 mins). Please be patient and don't interrupt the process...
32768+0 records in
32768+0 records out
34359738368 bytes transferred in 724.061475 secs (47454173 bytes/sec)

Changing permissions for created swapfile...

Create (swapfile) Done.
VM has to be rebooted for the newly created swapfile to take effect.
```

Après le redémarrage, l'augmentation du swap peut être observée à l'aide de la commande supérieure.



Commande de sortie :

Pour quitter l'outil, tapez exit et appuyez sur la touche **Entrée**.

Attacher des disques supplémentaires à Citrix ADM déployés en haute disponibilité

Considérons un scénario dans lequel vous avez configuré une paire de serveurs Citrix ADM dans une configuration haute disponibilité sans disque secondaire. Considérons également que vous avez ajouté 2 instances Citrix ADC ou plus, vérifié et vérifié que tous les processus sont en cours d'exécution. Dans cette configuration, vous pouvez ajouter des disques secondaires aux machines virtuelles. Dans une configuration haute disponibilité, vous devez ajouter des disques supplémentaires aux deux nœuds, comme indiqué dans cette tâche :

1. Supposons que les noms de nœud Citrix ADM soient « ADM_Primary » et « ADM_Secondary ».
2. Commencez par exécuter l'outil de partition sur ADM_Secondary, puis ajoutez un disque secondaire. La machine virtuelle redémarre après l'ajout du disque.
3. Arrêtez ADM_Secondary après son redémarrage.
4. Exécutez maintenant l'outil de partition sur ADM_Primary et ajoutez un disque secondaire. La machine virtuelle redémarre après l'ajout du disque.

   Assurez-vous d'ajouter des disques de capacité similaire aux deux nœuds. Par exemple, si vous ajoutez un disque d'une capacité de 500 Go au nœud principal, ajoutez également un disque d'une capacité de 500 Go au nœud secondaire.
5. Après le redémarrage d'ADM_Primary, vérifiez qu'il s'agit bien du nœud principal.
6. Démarrez maintenant le nœud ADM_Secondary. Assurez-vous qu'il est apparu en tant que nœud secondaire et que les bases de données ont été synchronisées.
7. Confirmez que toutes les données existent toujours.

Pour augmenter la capacité de la mémoire vive sur les deux nœuds :

1. Arrêtez ADM_Secondary et augmentez la taille de la RAM si nécessaire. Ne redémarrez pas le nœud.

2. Arrêtez ADM_Primary et augmentez la taille de la RAM si nécessaire.

   Assurez-vous d'augmenter la taille de la RAM de manière égale sur les deux nœuds. Par exemple, si vous augmentez la taille de la RAM sur le nœud principal à 16 Go, procédez de même sur le nœud secondaire.

3. Redémarrez ADM_Primary.
4. Après le redémarrage d'ADM_Primary, vérifiez qu'il s'agit bien du nœud principal.
5. Démarrez maintenant le nœud ADM_Secondary. Après le redémarrage, assurez-vous qu'il est devenu secondaire et que la synchronisation de la base de données fonctionne.
6. Confirmez maintenant que toutes les données existent toujours.

> **Remarque**
>
> Une fois que vous avez ajouté le disque secondaire, le nœud principal met un certain temps à apparaître. En outre, l'ensemble du processus d'ajout de disques secondaires aux deux nœuds et d'augmentation de la capacité de la RAM nécessite que les deux nœuds soient inactifs pendant un certain temps. Prenez en compte ce temps d'arrêt lorsque vous planifiez cette activité de maintenance.

Configurer

February 1, 2024

Vous ne pouvez accéder à un serveur Citrix ADM qu'à l'aide de l'interface graphique. Vous devez accéder à l'interface graphique pour ajouter des instances, gérer et surveiller vos instances et applications, afficher les analyses et configurer le serveur Citrix ADM.

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

Les navigateurs suivants sont pris en charge.

Navigateur Web	Version
Internet Explorer	11.0 et versions ultérieures
Google Chrome	Chrome 19 et versions ultérieures
Safari	Safari 5.1.1 et versions ultérieures
Mozilla Firefox	Firefox 3.6.25 et versions ultérieures

Pour accéder à l'interface graphique Citrix ADM :

Ouvrez une session sur Citrix ADM à l'aide des informations d'identification de l'administrateur.

Après avoir ouvert une session sur Citrix ADM, vous devez effectuer les opérations suivantes pour démarrer :

- Ajoutez des instances à Citrix ADM.Vous devez ajouter des instances au serveur Citrix ADM si vous souhaitez gérer et surveiller ces instances.
- Activez les analyses sur les serveurs virtuels.Pour afficher les données d'analyse pour le flux de trafic de votre application, vous devez activer la fonctionnalité Analytics sur les serveurs virtuels qui reçoivent le trafic pour les applications spécifiques.
- Configurez le serveur NTP sur Citrix ADM.Vous devez configurer un serveur NTP (Network Time Protocol) dans Citrix ADM pour synchroniser son horloge avec le serveur NTP.
- Configurez les paramètres système pour optimiser les performances Citrix ADM.Avant de commencer à utiliser Citrix ADM pour gérer et surveiller vos instances et applications, il est recommandé de configurer quelques paramètres système qui garantissent des performances optimales de votre serveur ADM Citrix.

Ajouter des instances à Citrix ADM

February 1, 2024

Les instances sont des appliances Citrix ou des appliances virtuelles que vous souhaitez découvrir, gérer et surveiller à partir de Citrix ADM. Vous devez ajouter des instances au serveur Citrix ADM si vous souhaitez gérer et surveiller ces instances. Vous pouvez ajouter les appliances Citrix et les appliances virtuelles suivantes à Citrix ADM :

- Citrix ADC MPX
- Citrix ADC VPX
- Citrix ADC SDX
- Citrix ADC CPX
- Citrix ADC BLX
- Citrix Gateway
- Citrix SD-WAN

Vous pouvez ajouter des instances lors de la configuration du serveur Citrix ADM pour la première fois ou plus tard. Vous devez ensuite spécifier un profil d'instance que Citrix ADM peut utiliser pour accéder à l'instance.

> **Remarque**
>
> - Citrix ADM utilise l'adresse IP NetScaler (NSIP) des instances Citrix ADC pour la communication. Pour plus d'informations sur les ports qui doivent être ouverts entre les instances Citrix ADC et Citrix ADM, consultez Ports.
> - Pour les instances Citrix SD-WAN WO et Citrix SD-WAN EE, Citrix ADM utilise l'adresse IP de gestion des instances pour la communication.
> - Pour savoir comment Citrix ADM découvre des instances, consultez la section Découvrir des instances.

Comment créer un profil Citrix ADC

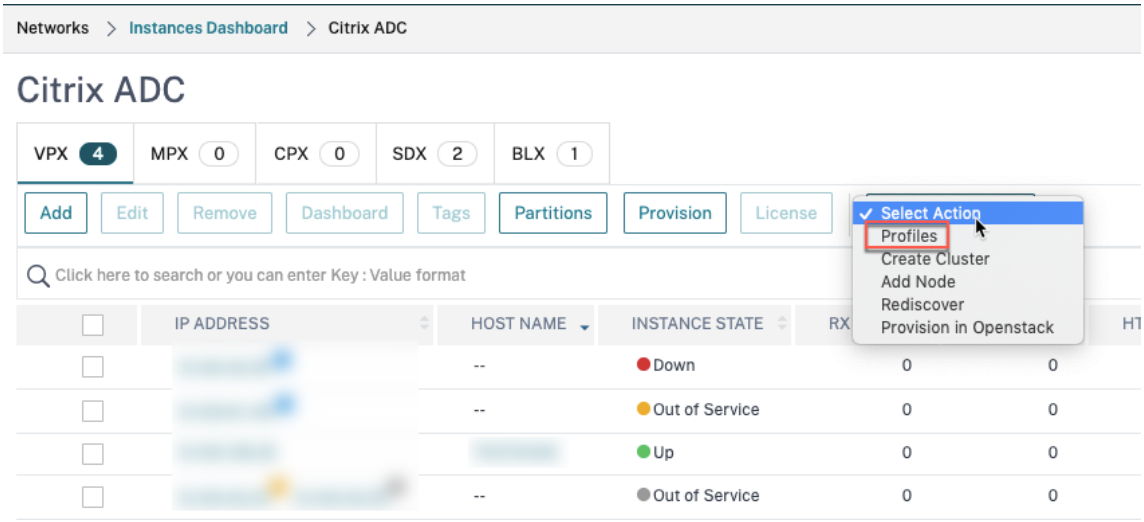
Le profil Citrix ADC contient le nom d'utilisateur, le mot de passe, les ports de communication et les types d'authentification des instances que vous souhaitez ajouter à Citrix ADM. Pour chaque type d'instance, un profil par défaut est disponible. Par exemple, le `nsroot` est le profil par défaut pour les instances Citrix ADC. Le profil par défaut est défini à l'aide des informations d'identification d'administrateur Citrix ADC par défaut. Si vous avez modifié les informations d'identification d'administrateur par défaut de vos instances, vous pouvez définir des profils d'instance personnalisés pour ces instances. Si vous modifiez les informations d'identification d'une instance après sa découverte, vous devez modifier le profil d'instance ou créer un profil, puis redécouvrir l'instance.

Vous pouvez créer un profil Citrix ADC à partir de la page **Instance** ou lors de l'ajout ou de la modification d'une instance.

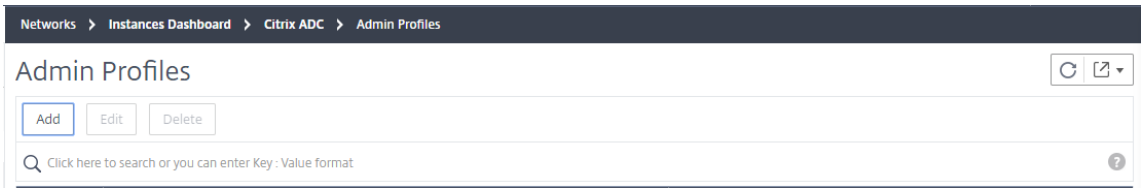
> **Remarque**
>
> Assurez-vous d'utiliser le compte de super administrateur pour créer un profil d'instance.

Pour créer un profil Citrix ADC à partir de la page Instance :

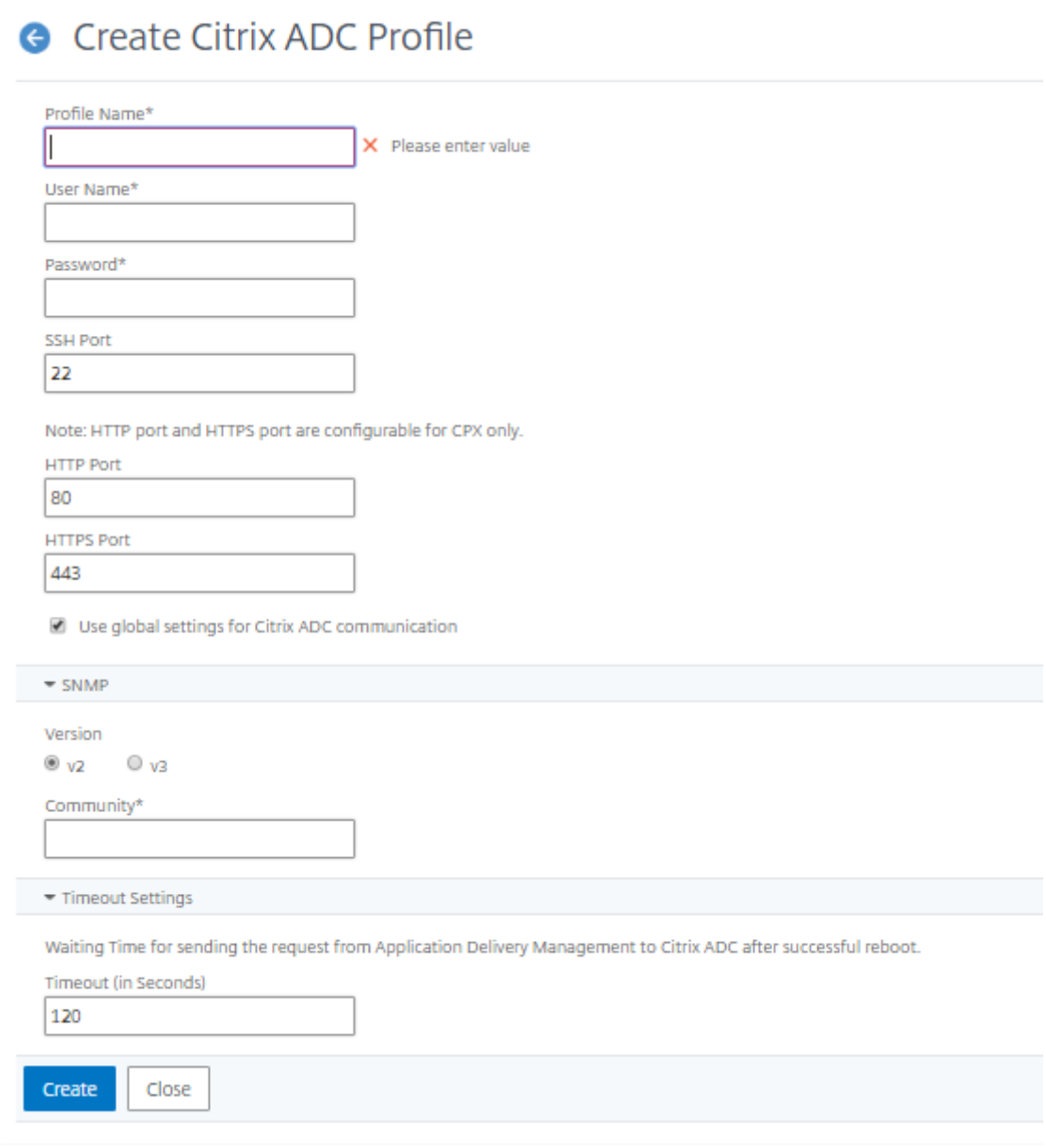
1. Accédez à **Réseaux > Instances**.
2. Sélectionnez une instance. Par exemple, Citrix ADC.
3. Sur la page Citrix ADC, sous **Sélectionner une action**, sélectionnez **Profils**.



4. Sur la page **Profils d'administration**, sélectionnez **Ajouter**.



5. Sur la page **Créer un profil Citrix ADC**, procédez comme suit :



a) **Nom du profil** : spécifiez un nom de profil pour l'instance Citrix ADC.

b) **Nom d'utilisateur** : spécifiez un nom d'utilisateur pour vous connecter à l'instance Citrix ADC.

c) **Mot de passe** : spécifiez un mot de passe pour vous connecter à l'instance Citrix ADC.

d) **Port SSH** : Spécifiez le port de communication SSH entre Citrix ADM et l'instance Citrix ADC.

e) **Port HTTP** : Spécifiez le port de communication HTTP entre Citrix ADM et l'instance Citrix ADC.

> **Remarque**
>
> Le port HTTP par défaut est 80. Vous pouvez également spécifier le port HTTP personnalisé ou autre que celui par défaut que vous avez peut-être configuré dans votre instance CPX Citrix ADC. Le port HTTP personnalisé peut être utilisé pour la communication uniquement entre Citrix ADM et Citrix ADC CPX.

f) **Port HTTPS** : Spécifiez le port pour la communication HTTPS entre Citrix ADM et l'instance Citrix ADC.

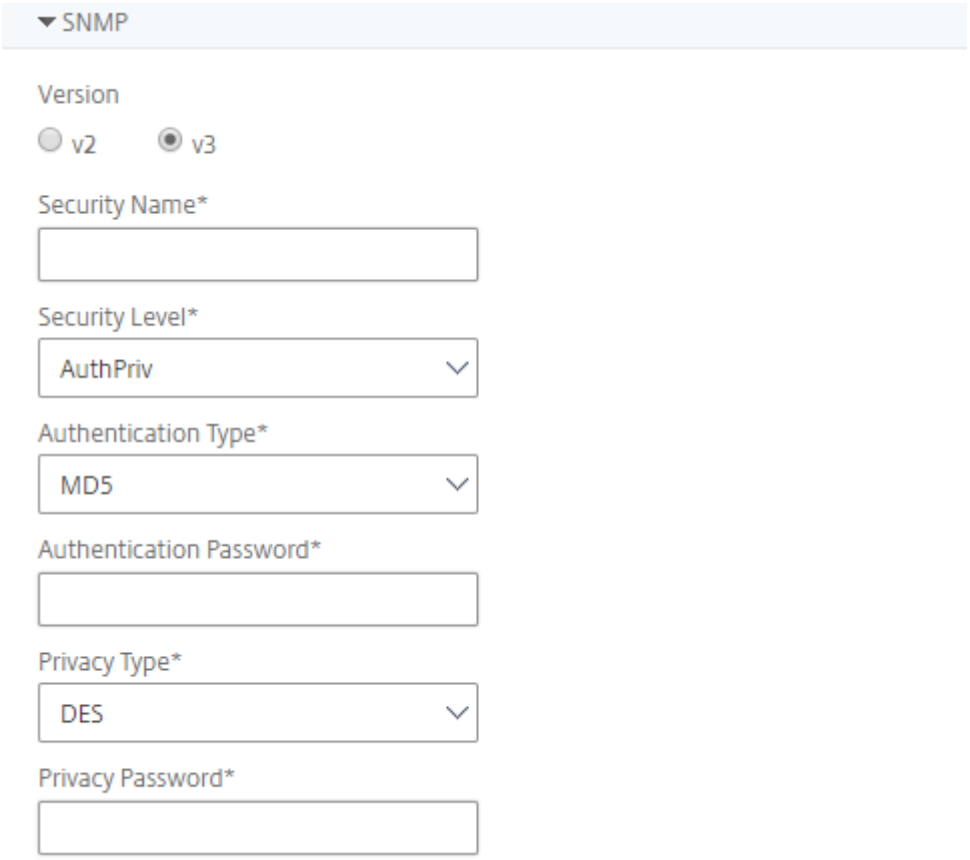
> **Remarque**
>
> Le port HTTPS par défaut est 443. Vous pouvez également spécifier le port HTTPS personnalisé ou autre que celui par défaut que vous avez peut-être configuré dans votre instance CPX Citrix ADC. Le port HTTPS personnalisé peut être utilisé pour la communication uniquement entre Citrix ADM et Citrix ADC CPX.

g) **Utiliser les paramètres globaux pour la communication Citrix ADC** : sélectionnez cette option si vous souhaitez utiliser les paramètres système pour la communication entre Citrix ADM et l'instance Citrix ADC, sinon sélectionnez HTTP ou https.

h) **Version SNMP** : sélectionnez **SNMPv2** ou **SNMPv3** et procédez comme suit :

   i. Si vous sélectionnez SNMPv2, spécifiez le nom de la **communauté** pour l'authentification.

   ii. **Si vous sélectionnez SNMPv3, spécifiez le**nom de sécurité et le niveau de sécurité**.** En fonction du niveau de sécurité, sélectionnez le **type d'authentification** et le **type de confidentialité**.



> **Remarque**
>
> Pour Citrix ADC SDX, seul le protocole **SNMPv2** est pris en charge.

i) **Paramètres de délai d'attente** : Spécifiez le temps pendant lequel Citrix ADM doit attendre avant d'envoyer une demande de connexion à l'instance Citrix ADC après un redémarrage.

j) Sélectionnez **Créer**.

Ajouter des instances ADC à Citrix ADM

Vous pouvez ajouter des instances lors de la configuration du serveur Citrix ADM pour la première fois ou plus tard.

Pour ajouter des instances, vous devez spécifier le nom d'hôte ou l'adresse IP de chaque instance Citrix ADC, ou une plage d'adresses IP.

Pour les instances SD-WAN, spécifiez l'adresse IP de chaque instance ou une plage d'adresses IP. Notez que Citrix ADM prend uniquement en charge les éditions Citrix SD-WAN WO et Citrix SD-WAN PE.

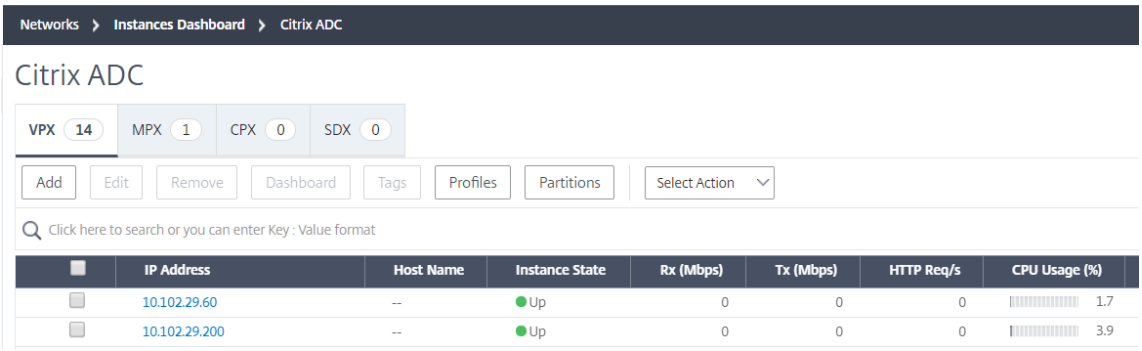
> **Remarque**
>
> - Pour ajouter des instances Citrix ADC configurées dans un cluster, vous devez spécifier l'adresse IP du cluster ou l'un des nœuds individuels de la configuration du cluster. Toutefois, sur Citrix ADM, le cluster est représenté uniquement par son adresse IP.
> - Pour les instances Citrix ADC configurées en tant que paire HA, lorsque vous ajoutez une instance, l'autre instance de la paire est automatiquement ajoutée.

Si deux serveurs Citrix ADM sont configurés en mode haute disponibilité, lorsqu'une instance est ajoutée, la source de trafic passe par l'adresse IP flottante ADM.

Lorsque vous ajoutez une instance à partir d'une donnée distante configurée avec un agent sur site, la source de trafic passe par l'agent ADM.

Pour ajouter une instance à Citrix ADM :

1. Ouvrez une session sur Citrix ADM avec les informations d'identification de l'administrateur.
2. Accédez à**Réseaux**>**Instances** > **Citrix ADC**. Sélectionnez le type d'instance à ajouter (par exemple, Citrix ADC VPX) et cliquez sur**Ajouter**.



3. Sélectionnez l'une des options suivantes :

   - **Entrez l'adresse IP du périphérique**- Pour les instances Citrix ADC, spécifiez le nom d'hôte ou l'adresse IP de chaque instance, ou une plage d'adresses IP.

     Si vous souhaitez découvrir une paire ADC HA à l'aide de SNIP, assurez-vous que le mode INC (Independent Network Configuration) est activé. Et spécifiez les adresses SNIP au format suivant :

     ```
     <SNIP of primary instance>#<SNIP of secondary instance>
     <!--NeedCopy-->
     ```

     Par exemple, `10.10.10.11#10.10.10.12`

     Pour les instances SD-WAN, spécifiez l'adresse IP de chaque instance ou une plage d'adresses IP.

- **Importer à partir d'un fichier**- À partir de votre système local, téléchargez un fichier texte contenant les adresses IP de toutes les instances que vous souhaitez ajouter.

4. Dans **Nom du profil**, sélectionnez le profil d'instance approprié ou créez un nouveau profil en cliquant sur l'icône +.
5. Dans **Site**, sélectionnez l'emplacement auquel vous souhaitez ajouter l'instance, ou créez un nouvel emplacement en cliquant sur l'icône **+** .
6. Cliquez sur**OK** pour lancer le processus d'ajout d'instances à Citrix ADM.

> **Remarque**
>
> Si vous souhaitez redécouvrir une instance, accédez à **Réseaux** > **Instances** > **Citrix ADC**. Sélectionnez le type d'instance (par exemple, VPX) et sélectionnez l'instance à redécouvrir, puis dans la liste **Sélectionner une action**, cliquez sur **Redécouvrir**.

Ajouter des instances CPX ADC à Citrix ADM

Citrix ADM a été amélioré pour prendre en charge les améliorations apportées aux fonctionnalités CPX. L'instance CPX Citrix ADC est désormais ajoutée à Citrix ADM en fournissant une adresse IP pour le CPX ainsi qu'un profil de périphérique. Le processus d'ajout d'une instance CPX est maintenant similaire à la façon dont d'autres types d'ADC tels que VPX ou MPX sont ajoutés dans ADM. De plus, l'enregistrement de CPX dans ADM a été amélioré. Lorsqu'un CPX démarre, Citrix ADM détecte et enregistre automatiquement l'instance CPX. Une instance CPX n'est plus découverte via l'hôte Docker.

1. Accédez à **Réseaux** > **Instances** > **Citrix ADC**, puis cliquez sur l'onglet **CPX**.
2. Cliquez sur **Ajouter** pour ajouter de nouvelles instances CPX dans Citrix ADM.
3. La page **Ajouter Citrix ADC CPX** s'ouvre. Entrez les valeurs pour les paramètres suivants :

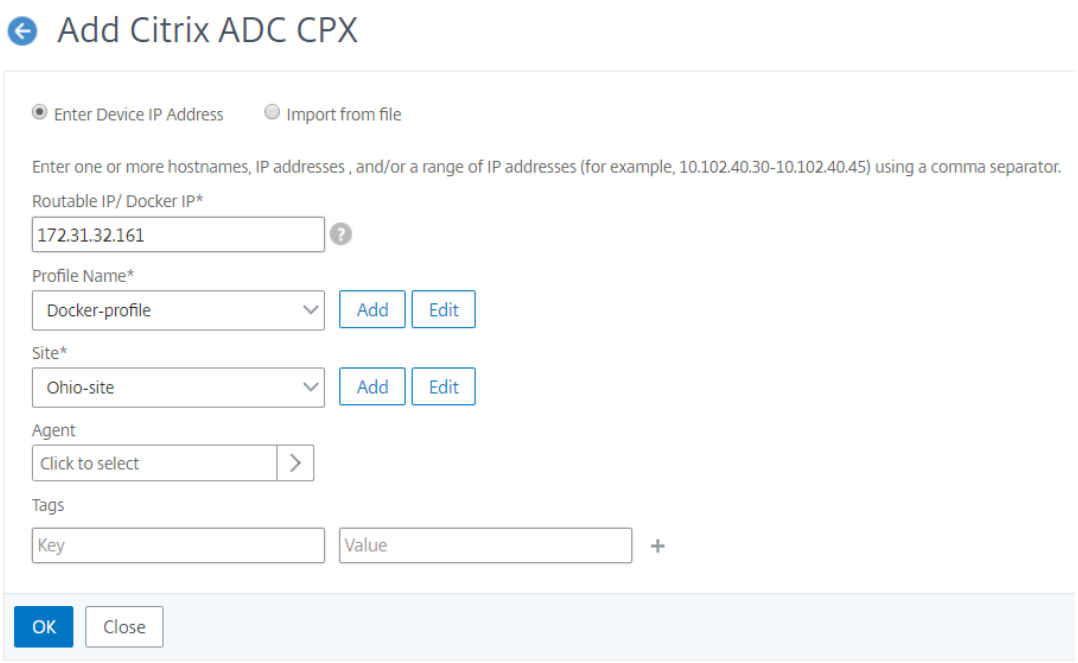
   a) Vous pouvez ajouter des instances CPX en fournissant l'adresse IP accessible de l'instance CPX ou l'adresse IP du conteneur Docker où l'instance CPX est hébergée.

   b) Sélectionnez le profil de l'instance CPX.

   c) Sélectionnez le site sur lequel les instances doivent être déployées.

   d) Sélectionnez l'agent.

   e) En option, vous pouvez entrer la paire clé-valeur de l'instance. L'ajout d'une paire clé-valeur vous permet de rechercher plus tard l'instance.



> **Remarque**
>
> Pour les instances CPX Citrix ADC, vous devez spécifier les détails des ports **HTTP, HTTPS, SSH**et **SNMP** de l'hôte lors de la création du profil d'instance CPX. Vous pouvez également spécifier la plage de ports publiés par l'hôte dans les champs **Port de départ** et **nombre de ports** .

4. Cliquez sur **OK**.

Ajouter une instance Citrix ADC BLX autonome dans Citrix ADM

Une instance autonome Citrix ADC BLX est une instance unique qui s'exécute sur le serveur Linux hôte dédié.

1. Accédez à **Réseaux** > **Instances** > **Citrix ADC**.
2. Dans l'onglet **BLX**, cliquez sur **Ajouter**.
3. Sélectionnez l'option **Autonome** dans la liste **Type d'instance**.
4. Dans le champ **Adresse IP**, spécifiez l'adresse IP de l'instance BLX.
5. Dans le champ **Adresse IP de l'hôte**, spécifiez l'adresse IP du serveur Linux sur lequel l'instance BLX est hébergée.
6. Dans la liste **Nom du profil**, sélectionnez le profil approprié pour une instance BLX ou créez un profil.

   Pour créer un profil, cliquez sur **Ajouter**.

> **Important**
>
> Assurez-vous d'avoir spécifié le nom d'utilisateur hôte et le mot de passe corrects du serveur Linux dans le profil.

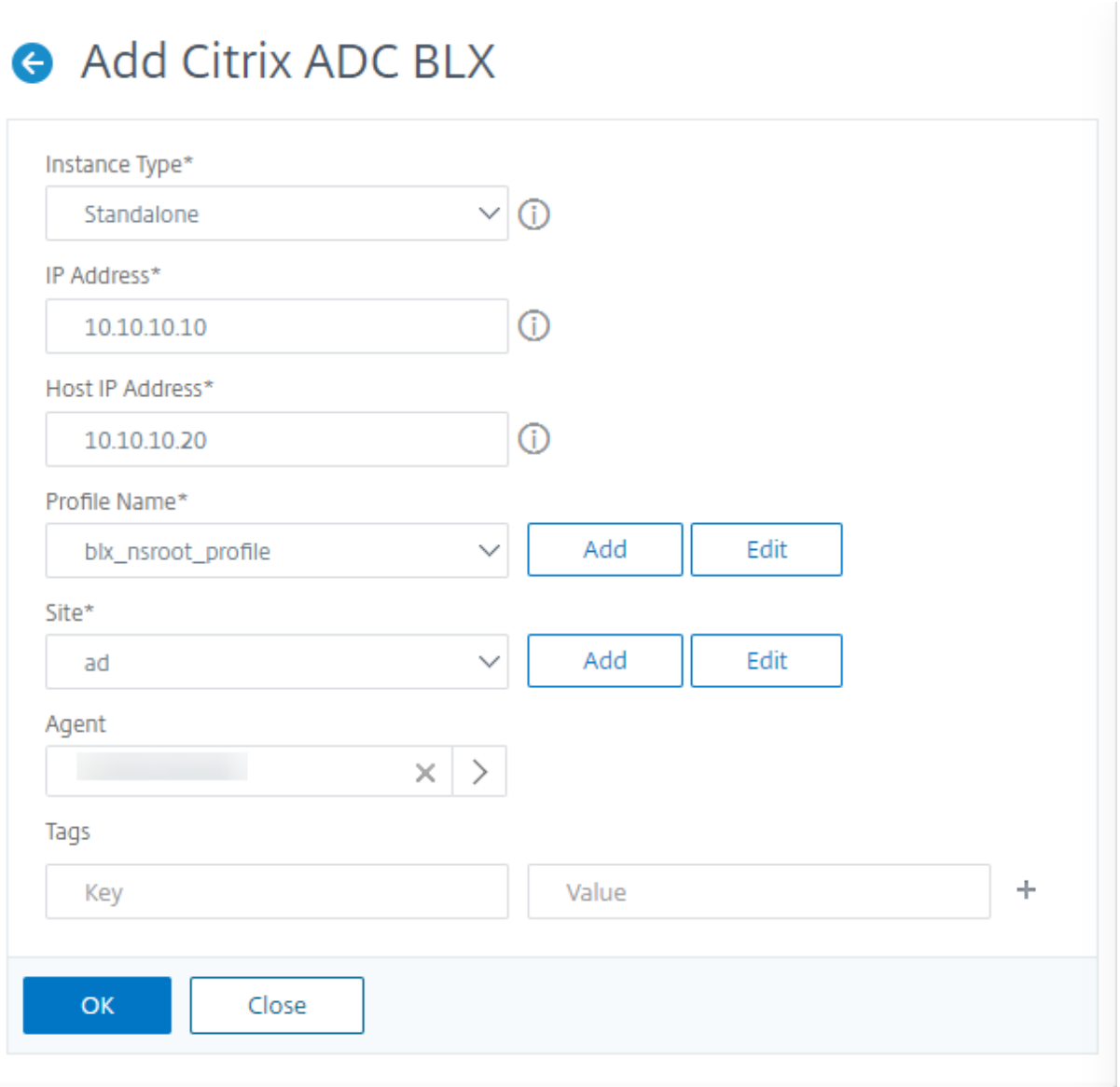
7. Dans la liste des **sites**, sélectionnez le site auquel vous souhaitez ajouter une instance.

   Si vous souhaitez ajouter un site, cliquez sur **Ajouter**.

8. Dans la liste des **agents**, sélectionnez l'agent Citrix ADM auquel vous souhaitez associer l'instance.

   S'il n'y a qu'un seul agent configuré sur votre Citrix ADM, cet agent est sélectionné par défaut.

9. Cliquez sur **OK**.



Ajouter des instances Citrix ADC BLX à haute disponibilité dans Citrix ADM

Les instances BLX Citrix ADC haute disponibilité qui s'exécutent sur différents serveurs Linux hôtes. Un serveur Linux ne peut pas héberger plus d'une instance BLX.

1. Dans l'onglet **BLX**, cliquez sur **Ajouter**.
2. Sélectionnez l'option **Haute disponibilité** dans la liste **Type d'instance**.
3. Dans le champ **Adresse IP**, spécifiez l'adresse IP de l'instance BLX.
4. Dans le champ **Adresse IP de l'hôte**, spécifiez l'adresse IP du serveur Linux sur lequel l'instance BLX est hébergée.
5. Dans le champ **Adresse IP homologue**, spécifiez l'adresse IP de l'instance BLX homologue.
6. Dans le champ **Adresse IP de l'hôte homologue**, spécifiez l'adresse IP du serveur Linux sur lequel l'instance BLX homologue est hébergée.
7. Dans la liste **Nom du profil**, sélectionnez le profil approprié pour une instance BLX ou créez un profil.

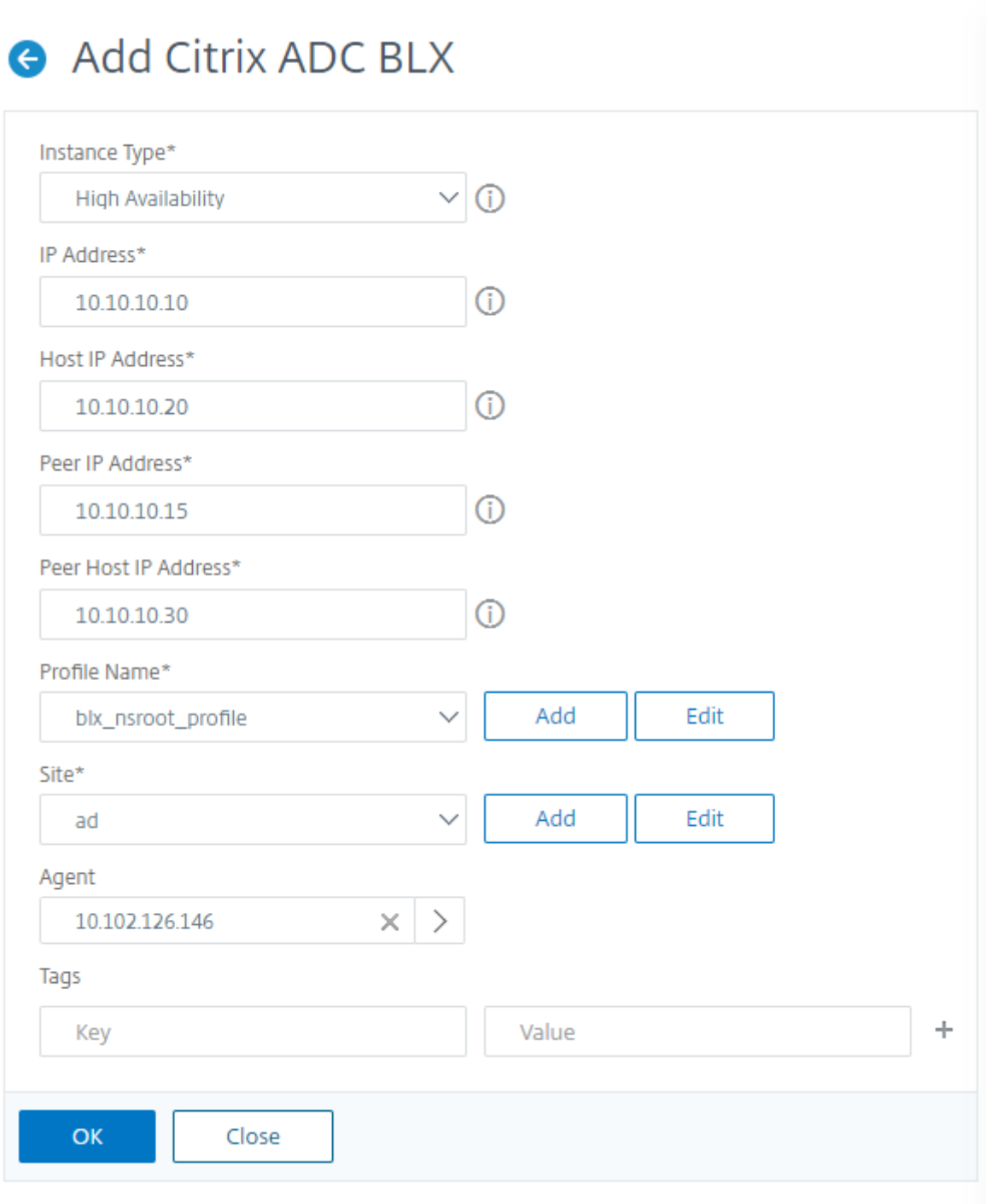
   Pour créer un profil, cliquez sur **Ajouter**.

   > **Important**
   >
   > Assurez-vous d'avoir spécifié le nom d'utilisateur hôte et le mot de passe corrects du serveur Linux dans le profil.

8. Dans la liste des **sites**, sélectionnez le site auquel vous souhaitez ajouter une instance.

   Si vous souhaitez ajouter un site, cliquez sur **Ajouter**.
9. Dans la liste des **agents**, sélectionnez l'agent Citrix ADM auquel vous souhaitez associer l'instance.

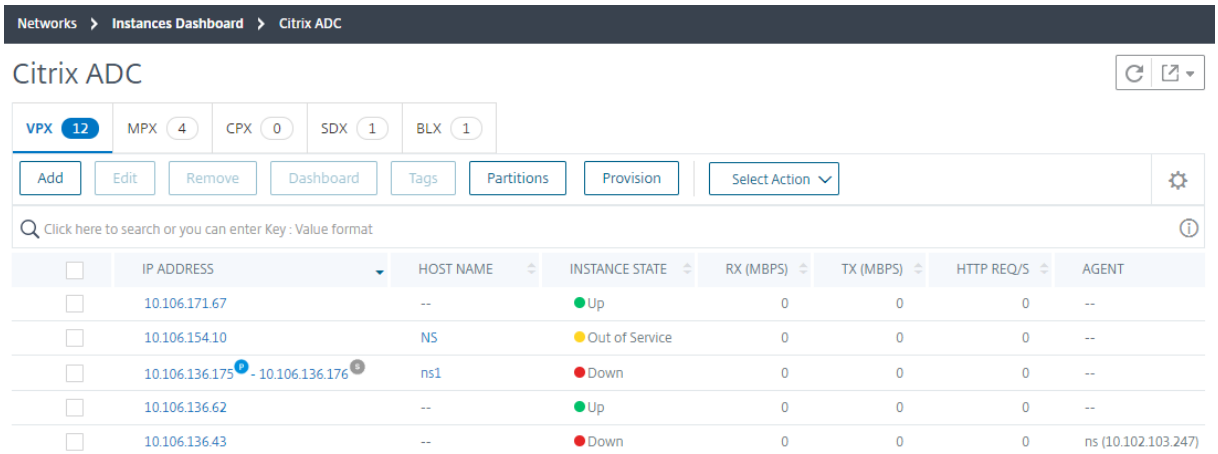
   S'il n'y a qu'un seul agent configuré sur votre Citrix ADM, cet agent est sélectionné par défaut.
10. Cliquez sur **OK**.



Accéder à une interface graphique d'instance à partir de Citrix ADM

1. Accédez à **Réseaux > Instances** > **Citrix ADC** .
2. Sélectionnez le type d'instance auquel vous souhaitez accéder (par exemple, VPX, MPX, CPX, SDX ou BLX).

3. Cliquez sur l'adresse IP Citrix ADC ou le nom d'hôte requis.



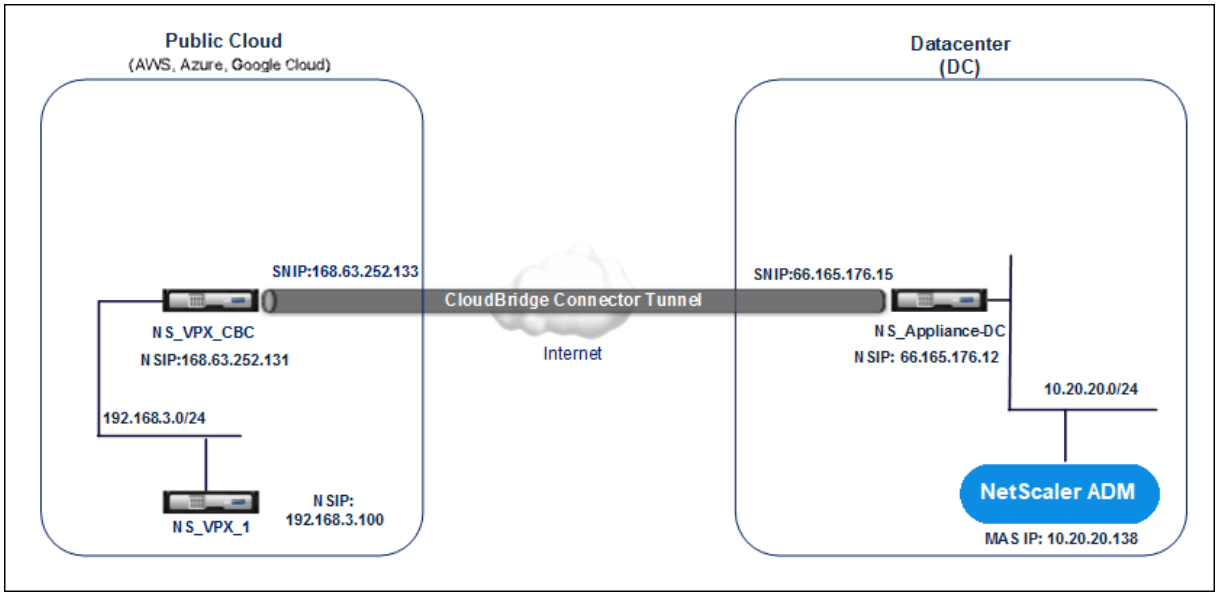
L'interface graphique de l'instance sélectionnée apparaît dans une fenêtre contextuelle.

Ajouter des instances Citrix ADC VPX déployées dans le cloud à Citrix ADM

February 1, 2024

Vous pouvez utiliser Citrix ADM pour gérer et surveiller les instances Citrix ADC VPX déployées sur un cloud public tel qu'Amazon Web Services (AWS) ou Microsoft Azure. Vous devez établir une connectivité de couche 3 entre Citrix ADM et les instances Citrix ADC VPX déployées sur le cloud public. Pour établir la connectivité de couche 3, vous pouvez utiliser des solutions telles que Citrix CloudBridge Connector, Citrix SD-WAN, Direct Connect to AWS, VPN dans Azure ou des connecteurs tiers tels qu'Equinix, etc.

L'exemple de topologie suivant utilise Citrix CloudBridge Connector pour la connectivité de couche 3 entre Citrix ADM et les instances Citrix ADC VPX déployées dans le cloud.



Un tunnel Citrix CloudBridge Connector est configuré entre l'appliance Citrix ADC NS_Appliance-DC, dans le contrôleur de domaine de données et l'appliance virtuelle Citrix ADC (VPX) NS_VPX_CBC dans le cloud public. NS_Appliance-DC et NS_VPX_CBC permettent la communication entre Citrix ADM et l'instance Citrix ADC VPX, NS_VPX_1, déployée dans le cloud public. Une fois la communication établie, vous pouvez découvrir NS_VPX_1 dans Citrix ADM.

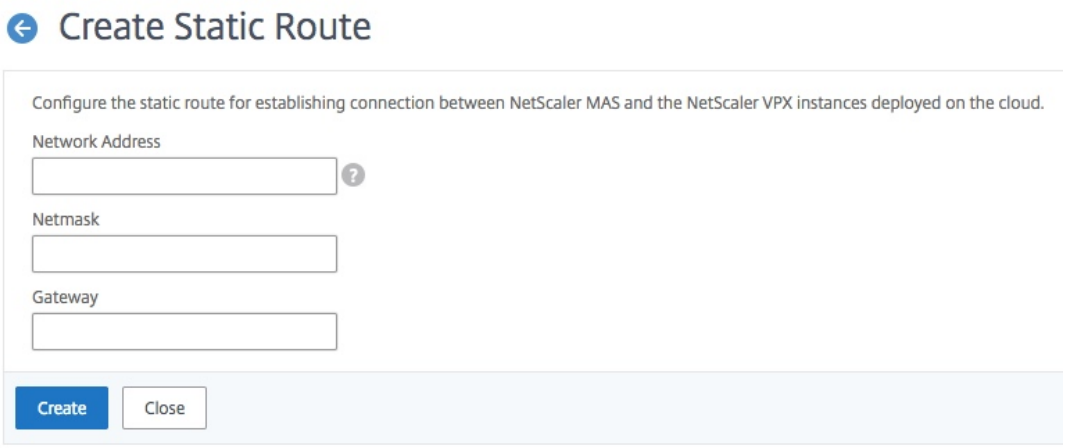
Pour configurer cette topologie :

1. Installez, configurez et démarrez une instance Citrix ADC VPX dans le cloud public.
   - Pour obtenir des instructions, consultez Installation de Citrix ADC VPX sur AWS.
   - Pour obtenir des instructions, reportez-vous à la section Installation de Citrix ADC VPX sur Microsoft Azure.
2. Déployez et configurez une appliance physique Citrix ADC, ou provisionnez et configurez un dispositif virtuel Citrix ADC (VPX) sur une plate-forme de virtualisation dans le centre de données.
   - Pour obtenir des instructions, consultez la section Installer une instance Citrix ADC VPX sur Citrix Hypervisor.
   - Pour obtenir des instructions, reportez-vous à la section Installer des dispositifs virtuels Citrix sur VMware ESXi.
   - Pour obtenir des instructions, reportez-vous à la section Installer des dispositifs virtuels Citrix ADC sur Microsoft Hyper-V.
3. Configurez Citrix CloudBridge Connector entre le centre de données et le cloud public. Pour obtenir des instructions, reportez-vous à la section Configuration du connecteur Citrix CloudBridge.

4. Configurez la route statique pour établir la connexion entre Citrix ADM et les instances Citrix ADC VPX déployées sur le cloud, comme suit :

   a) Connectez-vous à Citrix ADM.

   b) Accédez à **Système > Routes statiques**, puis cliquez sur **Ajouter**.



   c) Dans le champ **Adresse réseau**, entrez l'adresse du réseau que vous souhaitez établir un itinéraire statique à partir de Citrix ADM via le connecteur.

   d) Dans le champ **Masque réseau**, entrez le masque réseau du réseau.

   e) Dans le champ **Passerelle**, entrez l'adresse de la Gateway.

5. Ajoutez les instances de cloud Citrix ADC VPX à Citrix ADM en spécifiant la plage d'adresses IP des instances Citrix ADC VPX dans le cloud public. Pour obtenir des instructions détaillées, cliquez sur Ajouter des instances à Citrix ADM.

Gérer les licences et activer les analyses sur les serveurs virtuels

February 1, 2024

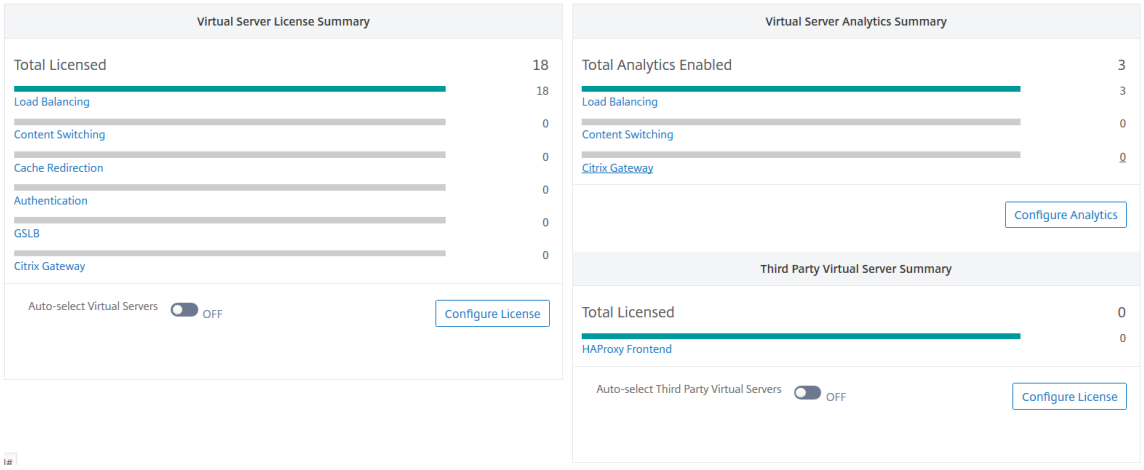
> **Remarque**
>
> - Les informations et la procédure suivantes pour activer l'analyse ne s'appliquent que si votre version Citrix ADM est **13.0 build 41.x** ou ultérieure. Si votre version de Citrix ADM est antérieure à **13.0 build 36.27**, consultez Activer l'analyse.
> - Par défaut, l'option **Serveurs virtuels sous licence automatique** est activée. Vous devez vous assurer de disposer de licences suffisantes pour obtenir des licences pour les serveurs virtuels. Si vous avez des licences limitées et que vous souhaitez attribuer uniquement

> des licences aux serveurs virtuels sélectifs en fonction de vos besoins, désactivez l'option **Serveurs virtuels sous licence automatique** . Accédez à **Systèmes > Licences et analyses** et désactivez l'option **Serveurs virtuels sous licence automatique** sous **Allocation de licence de serveur virtuel**.

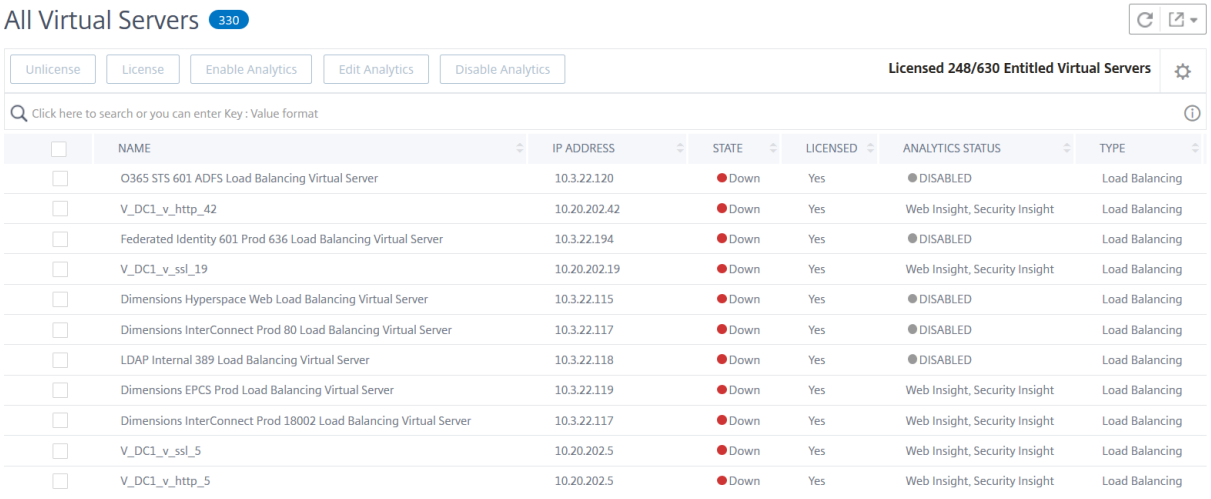
Le processus d'activation de l'analyse est simplifié. Vous pouvez désormais octroyer une licence au serveur virtuel et activer les analyses dans un seul workflow.

Accédez à **Système** > **Licences et analyses** pour :

- Afficher le **résumé des licences de serveur virtuel**
- Afficher le **résumé des analyses de serveur virtuel**



Lorsque vous cliquez sur **Configurer la licence** ou sur **Configurer Analytics**, la page **Tous les serveurs virtuels** s'affiche.



Sur la page **Tous les serveurs virtuels**, vous pouvez :

- Appliquer une licence pour les serveurs virtuels sans licence

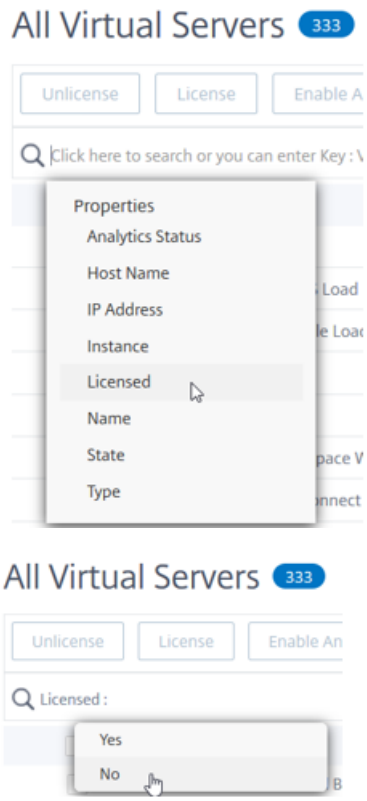
- Supprimer la licence pour les serveurs virtuels sous licence
- Activez les analyses sur des serveurs virtuels sous licence
- Modifier les analyses
- Désactiver l'analyse

> **Remarque**
>
> Les serveurs virtuels pris en charge pour permettre l'analyse sont l'équilibrage de charge, la commutation de contenu et Citrix Gateway.

Gestion des licences sur les serveurs virtuels

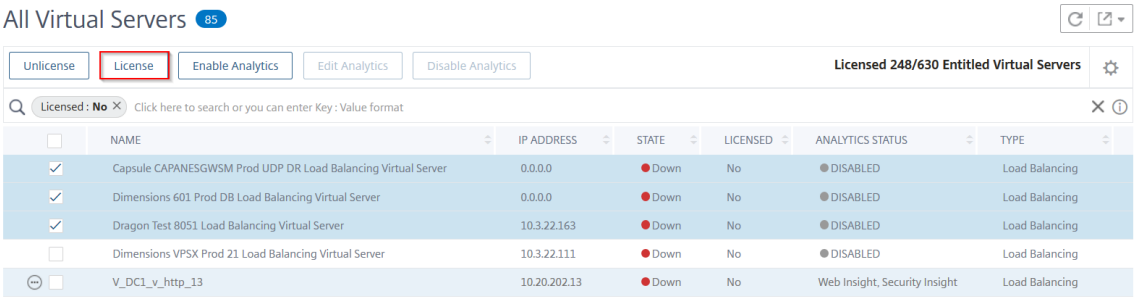
Pour obtenir une licence pour les serveurs virtuels, depuis la page **Tous les serveurs virtuels** :

1. Cliquez sur la barre de recherche, sélectionnez **Sous licence**, puis sélectionnez **Non**.



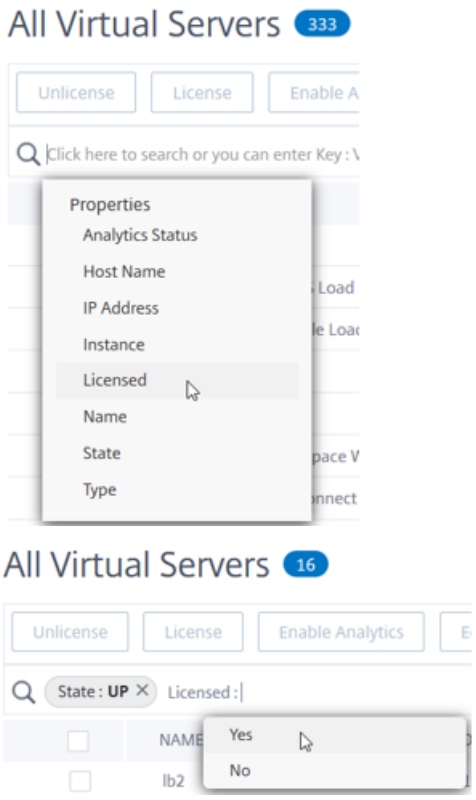
   Le filtre est maintenant appliqué et seuls les serveurs virtuels sans licence sont affichés.

2. Sélectionnez les serveurs virtuels, puis cliquez sur **Licence**.

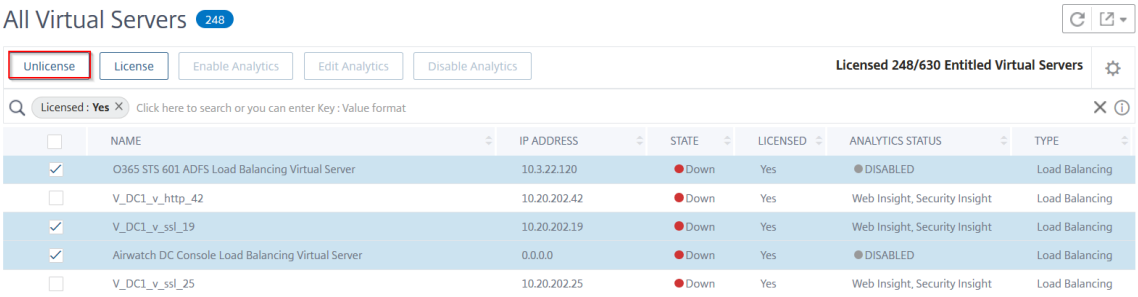


Pour annuler la licence des serveurs virtuels, depuis la page **Tous les serveurs virtuels** :

1. Cliquez sur la barre de recherche, sélectionnez **Licence**, puis **Oui**.



2. Sélectionnez les serveurs virtuels et cliquez sur **Annuler la licence**.



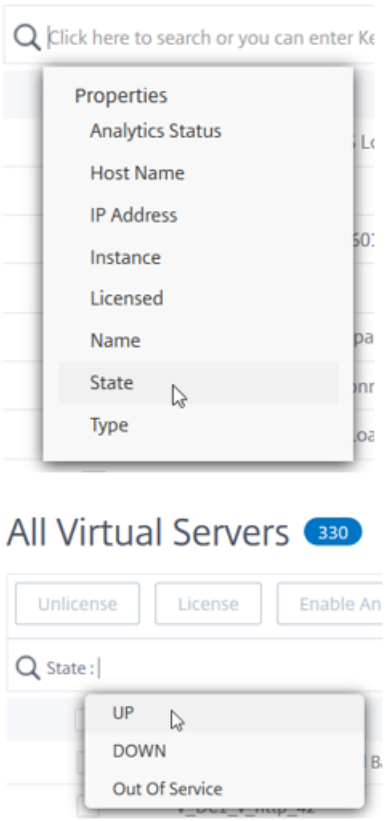
Activer l'analyse

Les conditions préalables à l'activation de l'analyse pour les serveurs virtuels sont les suivantes :

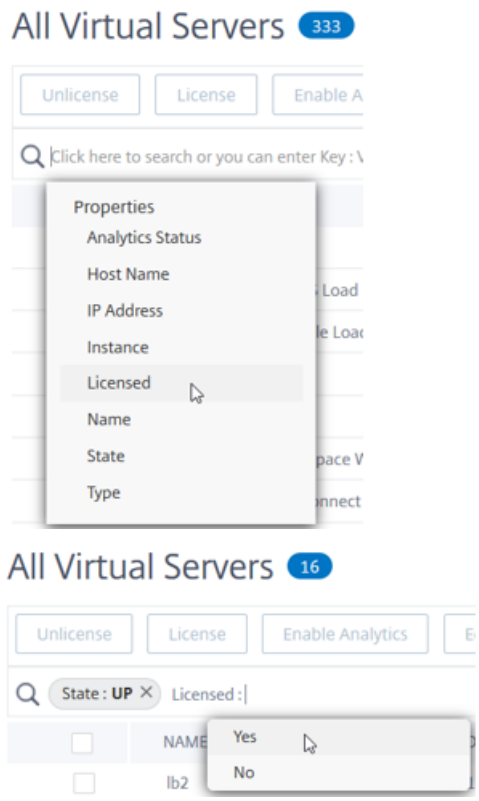
- Assurez-vous que les serveurs virtuels sont **sous licence**
- Assurez-vous que l'état des analyses est **désactivé**
- Assurez-vous que les serveurs virtuels sont en état **UP**

Vous pouvez filtrer les résultats pour identifier les serveurs virtuels mentionnés dans les prérequis.

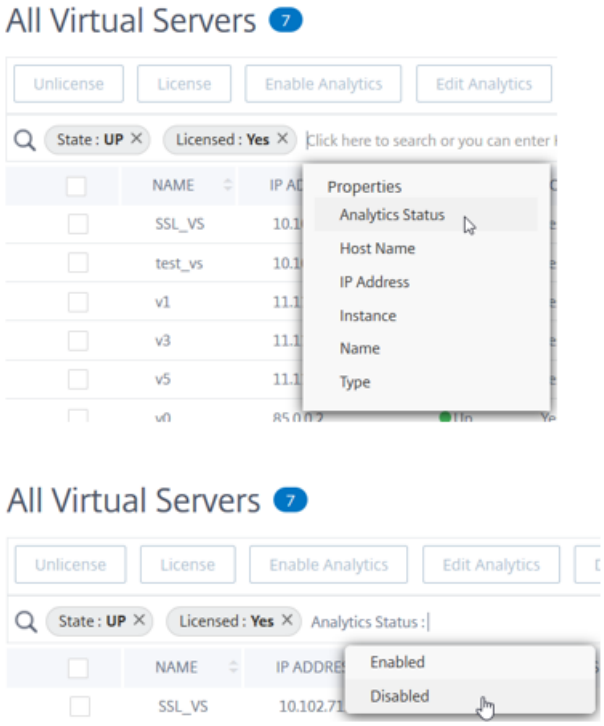
1. Cliquez sur la barre de recherche et sélectionnez **État**, puis sélectionnez **UP**.



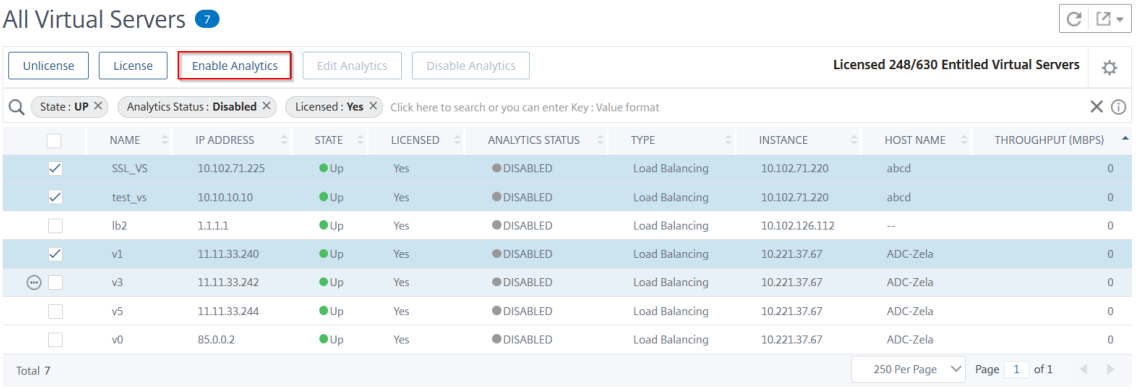
2. Cliquez sur la barre de recherche et sélectionnez **Licence**, puis sélectionnez **Oui**.



3. Cliquez sur la barre de recherche et sélectionnez **État Analytics**, puis sélectionnez **Désactivé**.



4. Après avoir appliqué les filtres, sélectionnez les serveurs virtuels, puis cliquez sur **Activer Analytics**.



> **Remarque**
>
> Vous pouvez également activer les analyses pour une instance particulière :
>
> ```
> 1. Accédez à **Réseaux** > **Instances** > **Citrix ADC**, puis sélectionnez le type d'instance. Par exemple, VPX.
>
> 1. Sélectionnez l'instance et, dans la liste **Sélectionner une action**, sélectionnez **Configurer Analytics**
>
> 1. Sur la page Configurer Analytics sur des serveurs virtuels, sélectionnez le serveur virtuel et cliquez sur **Activer Analytics**.
> ```

5. Dans la fenêtre **Activer Analytics** :

   a) Sélectionnez les types d'informations (Web Insight ou Security Insight)

   b) Sélectionnez **Logstream** comme mode de transport

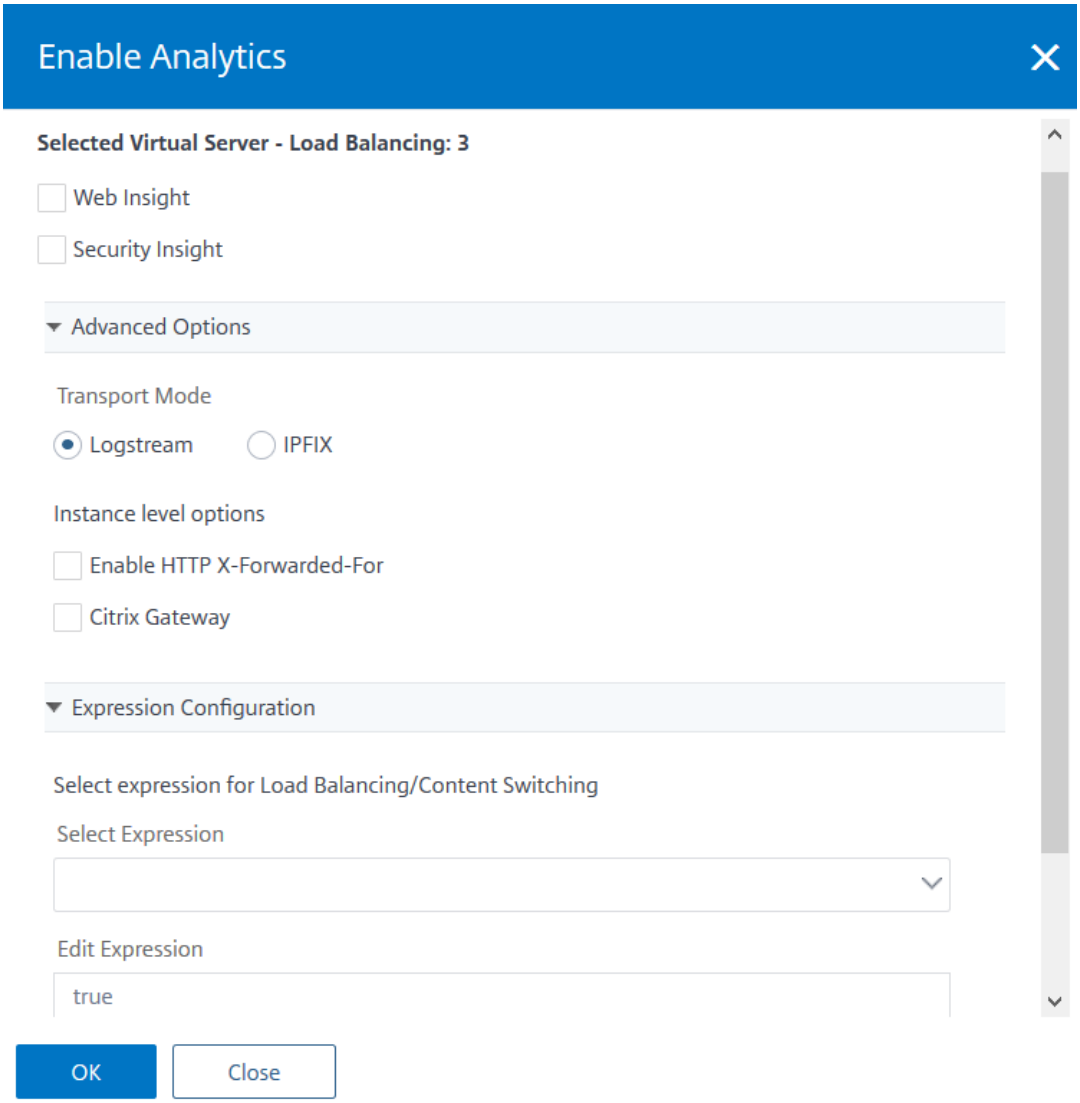
   > **Remarque**
   >
   > Pour Citrix ADC 12.0 ou version antérieure, **IPFIX** est l'option par défaut pour le mode de transport. Pour Citrix ADC 12.0 ou version ultérieure, vous pouvez sélectionner **Logstream** ou **IPFIX** comme mode de transport.
   >
   > Pour plus d'informations sur IPFIX et Logstream, consultez la section Présentation de Logstream .

   c) Sous **Options au niveau de l'instance** :

   - **Activer HTTP X-Forwarded-For** : sélectionnez cette option pour identifier l'adresse IP de la connexion entre le client et l'application, via un proxy HTTP ou un équilibreur de charge.
   - **Citrix Gateway** : sélectionnez cette option pour afficher les analyses de Citrix Gateway.

d) L'expression est true par défaut

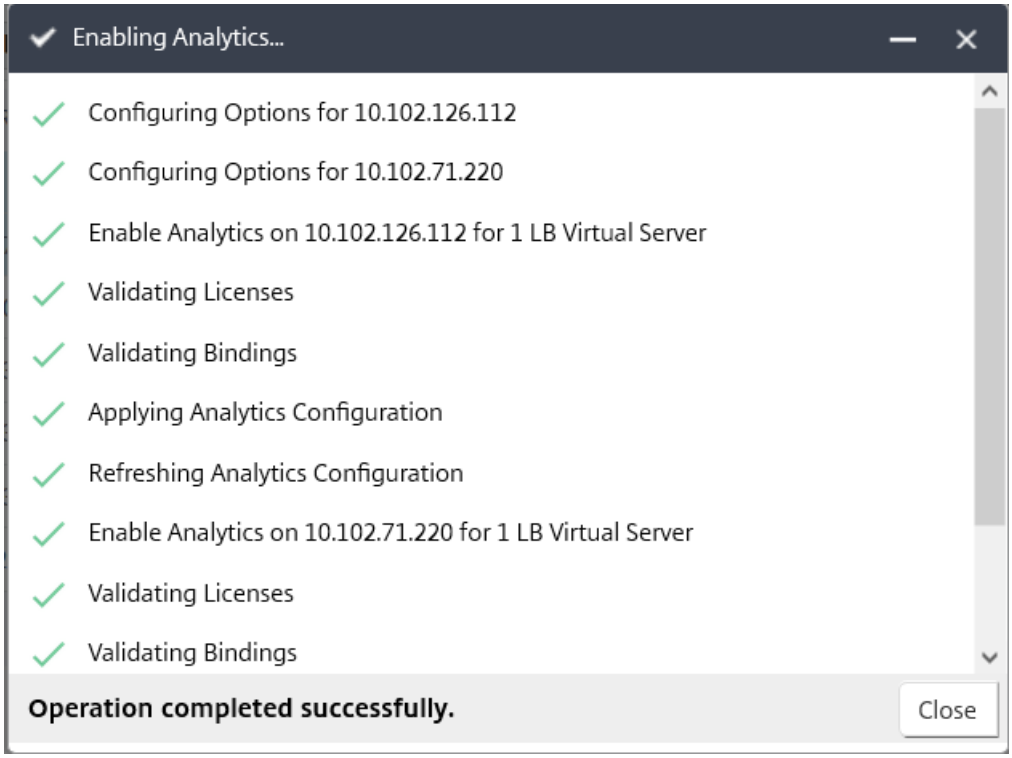
e) Cliquez sur **OK**.



Remarque

- Si vous sélectionnez des serveurs virtuels qui ne sont pas sous licence, Citrix ADM octroie d'abord des licences à ces serveurs virtuels, puis active les analyses
- Pour les partitions d'administration, seul **Web Insight** est pris en charge
- Pour les serveurs virtuels tels que la redirection du cache , l'authentification et le GSLB , vous ne pouvez pas activer les analyses. Un message d'erreur s'affiche.

Après avoir cliqué sur **OK**, Citrix ADM traite pour activer les analyses sur les serveurs virtuels sélectionnés.



Remarque

Citrix ADM utilise Citrix ADC SNIP pour Logstream et NSIP pour IPFIX. Si un pare-feu est activé entre l'agent Citrix ADM et l'instance Citrix ADC, assurez-vous d'ouvrir le port suivant pour permettre à Citrix ADM de collecter le trafic AppFlow :

Mode de transport	IP source	Type	Port
IPFIX	NSIP	UDP	4739
Logstream	SNIP	TCP	5557

Modifier les analyses

Pour modifier les analyses sur les serveurs virtuels :

1. Sélectionner les serveurs virtuels

   Remarque

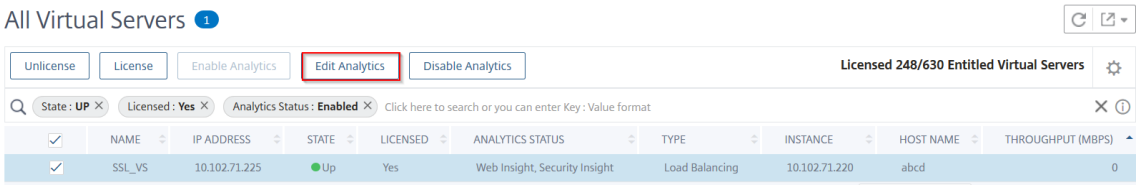
   Vous pouvez également modifier les analyses pour une instance particulière :

   ```
   1.  Accédez à **Réseaux** > **Instances** > **Citrix ADC**,
       puis sélectionnez le type d'instance. Par exemple, VPX.
   2
   ```



```
3  1.  Sélectionnez l'instance et cliquez sur **Modifier les
       analyses**.
```

2. Cliquez sur **Modifier les analyses**

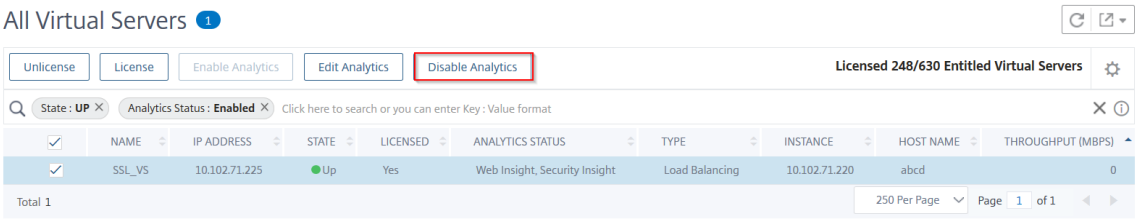


3. Modifiez les paramètres que vous souhaitez appliquer dans la fenêtre **Modifier la configuration d'Analytics**
4. Cliquez sur **OK**.

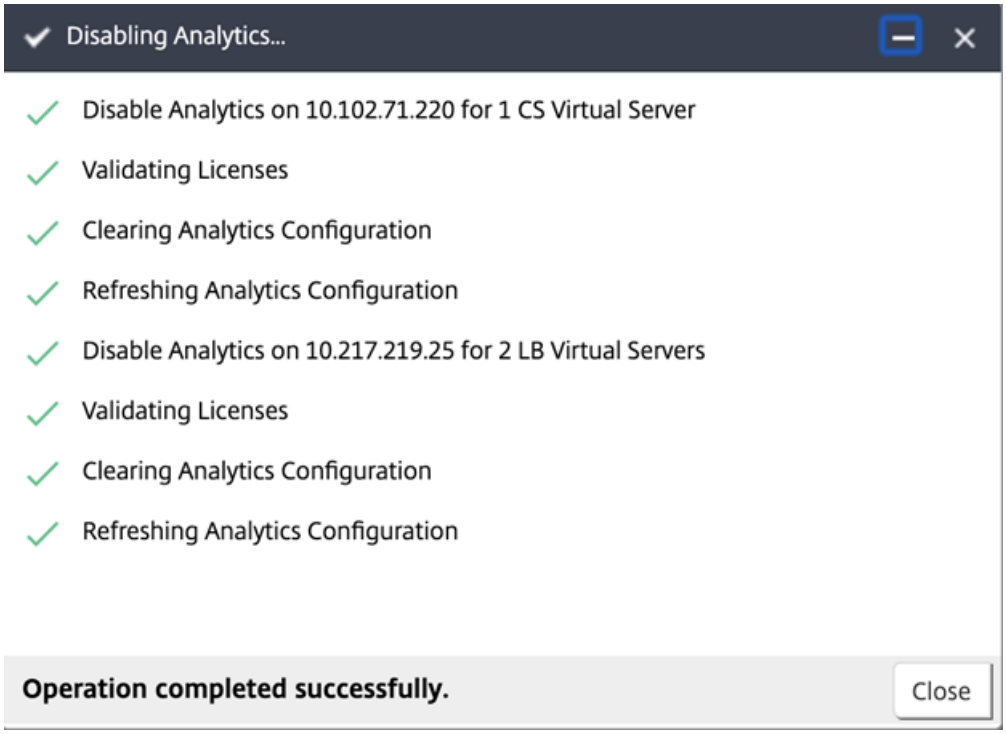
Désactiver l'analyse

Pour désactiver les analyses sur les serveurs virtuels sélectionnés, procédez comme suit :

1. Sélectionner les serveurs virtuels
2. Cliquez sur **Désactiver Analytics**



Citrix ADM désactive l'analyse sur les serveurs virtuels sélectionnés



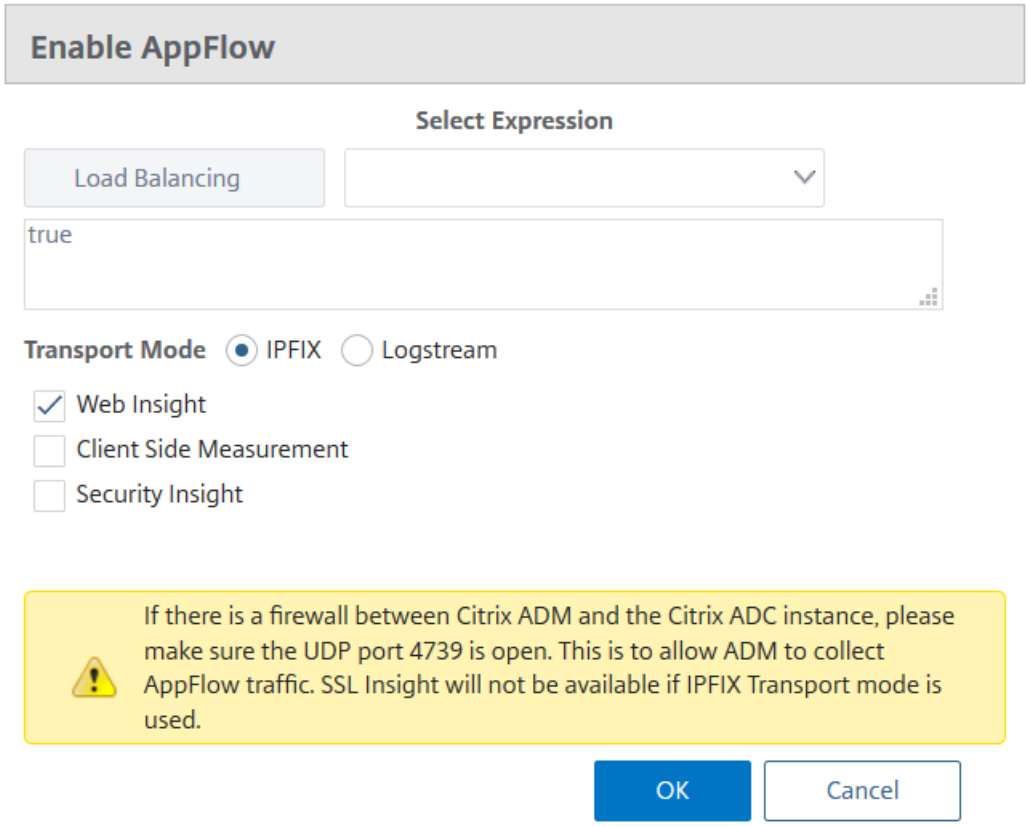
Le tableau suivant décrit les fonctionnalités de Citrix ADM qui prennent en charge IPFIX et Logstream en tant que mode de transport :

Fonctionnalité	IPFIX	Logstream
Web Insight	•	•
Security Insight	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	Non pris en charge	•
CR Insight	•	•
Réputation IP	•	•
AppFirewall	•	•
Mesure côté client	•	•
Syslog/Auditlog	•	•

Activez l'analyse sur les serveurs virtuels pour les versions antérieures

Pour activer l'analyse sur les serveurs virtuels pour **Citrix ADM 13.0**build 36.27 :

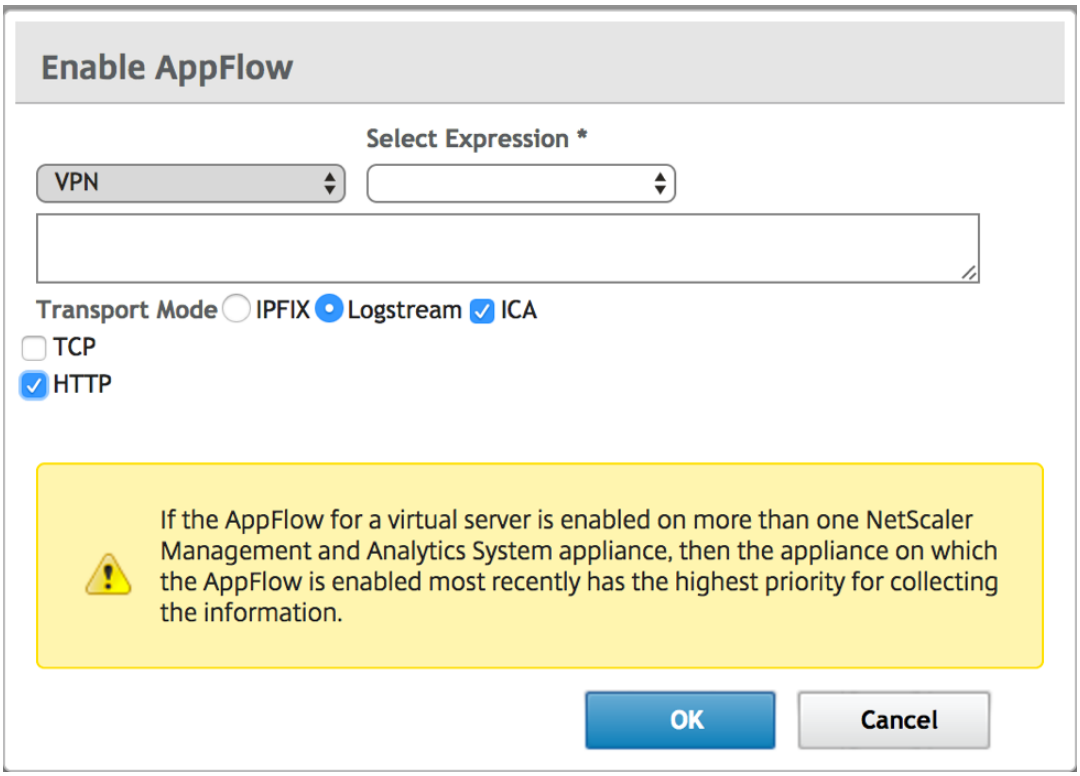
1. Accédez à **Réseaux** > **Instances** > **Citrix ADC**, puis sélectionnez l'instance Citrix ADC pour laquelle vous souhaitez activer les analyses.
2. Dans la liste des instances, sélectionnez une instance.
3. **Dans la liste Sélectionner une action**, sélectionnez **Configurer les analyses**.
4. Dans la liste des applications, sélectionnez les serveurs virtuels et cliquez sur **Activer AppFlow**.
5. Dans le champ **Enable AppFlow**, tapez true et, en fonction des analyses que vous souhaitez activer, sélectionnez Security Insight ou Web Insight, ou les deux.



> **Remarque**
>
> Citrix ADM utilise Citrix ADC SNIP pour Logstream et NSIP pour IPFIX. Si un pare-feu est activé entre Citrix ADM et Citrix ADC instance, assurez-vous d'ouvrir le port suivant pour permettre à Citrix ADM de collecter le trafic AppFlow :

Mode de transport	IP source	Type	Port
IPFIX	NSIP	UDP	4739
Logstream	SNIP	TCP	5557

- Pour HDX Insight et Gateway Insight, lorsque vous cliquez sur Activer AppFlow, vous devez sélectionner le serveur virtuel VPN configuré sur votre instance Citrix ADC et cocher les cases ICA ou HTTP du protocole en conséquence.



- Pour TCP Insight, accédez à **Système** > **Paramètres Analytics** > **Configurer les fonctionnalités**, puis sélectionnez **Activer TCP Insight**.
- Pour Video Insight, vous devez apporter les modifications de configuration sur l'appliance Citrix ADC. Pour plus d'informations sur la façon d'activer les analyses pour Video Insight, consultez Video Insight.
- Pour WAN Insight :
  - Accédez à **Infrastructure > Instances > Citrix SD-WAN WO et sélectionnez l'appliance d'optimisation WAN**du centre de données.
  - Dans la liste **Action**, sélectionnez **Enable Insight**.
  - Sélectionnez les paramètres suivants selon les besoins :
    - Collecte de données géographiques pour HDX Insight : partage l'adresse IP du client avec l'API Google Geo.
    - AppFlow : commence à collecter des données à partir des instances d'optimisation WAN.
      - TCP et WanOpt : fournit des rapports TCP et WanOpt Insight .

- HDX : fournit des rapports HDX Insight.
- TCP uniquement pour HDX : fournit TCP uniquement pour les rapports HDX Insight.

Vous pouvez sélectionner le mode de transport AppFlow sur **IPFIX** ou **Logstream** tout en activant AppFlow sur les instances Citrix ADC découvertes dans Citrix ADM. Pour plus d'informations sur IPFIX et Logstream, consultez la section Présentation de Logstream .

Le tableau suivant décrit les fonctionnalités de Citrix ADM qui prennent en charge IPFIX et Logstream en tant que mode de transport :

Fonctionnalité	IPFIX	Logstream
Web Insight	•	•
Security Insight	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	Non pris en charge	•
CR Insight	•	•
Réputation IP	•	•
AppFirewall	•	•
Mesure côté client	•	•
Syslog/Auditlog	•	•

Vous pouvez également activer ou désactiver le traitement du trafic Web Insight à l'aide de l'option Enable Web Insight de Citrix ADM. Si vous ne souhaitez pas surveiller le trafic Web Insight, vous pouvez désactiver cette option. Citrix ADM ne traite pas le trafic Web Insight à partir des serveurs virtuels sur vos instances gérées.

Configurer le serveur NTP

February 1, 2024

Vous pouvez configurer un serveur NTP (Network Time Protocol) dans Citrix ADM pour synchroniser son horloge avec le serveur NTP. La configuration d'un serveur NTP garantit que l'horloge Citrix ADM possède les mêmes paramètres de date et d'heure que les autres serveurs du réseau.

Pour configurer un serveur NTP sur Citrix ADM:

1. À partir de l'interface graphique d'ADM, accédez à **Système > Administration**. Dans la page **Administration système**, sous **Configurations réseau**, cliquez sur **Serveurs NTP**. Cliquez ensuite sur **Ajouter**.
2. Dans la page **Créer un serveur NTP**, entrez les détails suivants :
    - **Nom du serveur/adresse IP** —Entrez le nom de domaine ou l'adresse IP du serveur NTP. Le nom ou l'adresse IP ne peuvent pas être modifiés après avoir ajouté le serveur NTP.
    - Intervalle**minimum d'interrogation** : spécifiez la valeur minimale de l'intervalle entre les messages NTP transmis, en secondes sous la forme d'une puissance de 2. Par exemple, si vous souhaitez que l'intervalle minimal entre les interrogations soit de 64 secondes, ce qui peut être exprimé sous la forme 2^6, entrez 6
    - Intervalle**maximum d'interrogation**: spécifiez la valeur maximale de l'intervalle entre les messages NTP transmis, en secondes sous la forme d'une puissance de 2. Par exemple, si vous souhaitez que l'intervalle d'interrogation maximal soit de 256 secondes, ce qui peut être exprimé sous la forme 2^8, entrez 8.
    - **Identifiant de clé** : entrez l'identifiant de clé qui peut être utilisé pour l'authentification par clé symétrique auprès du serveur NTP. N'ajoutez pas d'identifiant de clé si vous choisissez de sélectionner Autokey.
    - **Autokey** : sélectionnez **Autokey** si vous souhaitez utiliser l'authentification par clé publique avec le serveur NTP. Ne sélectionnez pas si vous souhaitez ajouter un identifiant clé.
    - **Préféré** —Sélectionnez cette option si vous souhaitez spécifier ce serveur NTP comme serveur préféré pour la synchronisation des horloges. Cela ne s'applique que si plusieurs serveurs sont configurés.
3. Cliquez sur **Créer**.

Pour activer la synchronisation NTP sur Citrix ADM :

1. Accédez à **Système** > **Serveurs NTP**.
2. Cliquez sur **Synchronisation NTP** et **activez la case à cocher Activer la synchronisation NTP**.
3. Cliquez sur **OK**.

Configurer les paramètres système

February 1, 2024

Avant de commencer à utiliser Citrix ADM pour gérer et surveiller vos instances et applications, il est recommandé de configurer quelques paramètres système pour garantir des performances optimales de votre serveur ADM Citrix.

Configurer les alarmes système

Configurez les alarmes système pour vous assurer que vous êtes au courant de tout problème système critique ou majeur. Par exemple, vous pouvez être averti si l'utilisation de l'UC est élevée ou s'il y a plusieurs échecs de connexion au serveur. Pour certaines catégories d'alarmes, telles que CPUUsageHigh ou MemoryUsageHigh, vous pouvez définir des seuils et définir la gravité (critique ou majeure, par exemple) pour chacune d'entre elles. Pour certaines catégories, telles que InventoryFailed ou LoginFailure, vous ne pouvez définir que la gravité. Lorsque le seuil est dépassé pour une catégorie d'alarme (par exemple, MemoryUsageHigh) ou lorsqu'un événement se produit correspondant à la catégorie d'alarme (par exemple, LoginFailure), un message est enregistré dans le système et vous pouvez afficher le message en tant que message Syslog.

Pour configurer les alarmes système :

1. Accédez à **Système > SNMP**, puis cliquez sur l'onglet **Alarmes** dans le coin supérieur droit.
2. Sélectionnez l'alarme à configurer, puis cliquez sur **Modifier**.
3. Sur la page **Configurer l'alarme**, sélectionnez la gravité de l'alarme et définissez le seuil.
4. Pour afficher les alarmes qui ont enfreint le seuil ou pour lesquelles un événement s'est produit, accédez à **Système > Audit** et cliquez sur **Messages Syslog**.

Configurer les notifications système

Vous pouvez envoyer des notifications à certains groupes d'utilisateurs pour diverses fonctions liées au système. Vous pouvez configurer un serveur de notifications dans Citrix ADM et configurer des serveurs de Gateway de messagerie et SMS (Short Message Service) pour envoyer des notifications par courrier électronique et texte aux utilisateurs. La configuration de la notification garantit que vous êtes informé de toutes les activités au niveau du système, telles que la connexion utilisateur ou le redémarrage du système.

Pour configurer les notifications système :

1. Accédez à **Système > Administration**. Dans la page **Administration système**, sous **Notifications d'événements**, cliquez sur **Configurer la notification et le résumé des événements > Notification d'événements**.
2. Dans la page **Configurer les paramètres de notification système**, sélectionnez la catégorie ou la catégorie d'événements générés par Citrix ADM.

3. Ensuite, configurez le serveur de messagerie ou le serveur SMS pour recevoir une notification par e-mail ou SMS, ou les deux.

Configurer les paramètres de nettoyage du système

Pour limiter la quantité de données de rapport stockées dans la base de données de votre serveur Citrix ADM, vous pouvez spécifier l'intervalle pendant lequel vous souhaitez que Citrix ADM conserve les données de rapport réseau, les événements, les journaux d'audit et les journaux des tâches. Par défaut, ces données sont nettoyées toutes les 24 heures (à 00.00 heures).

Pour configurer le paramètre de nettoyage du système :

1. Accédez à **Système > Administration du système** . Sous **Nettoyage des données**, cliquez sur **Nettoyage des données du système et de l'instance**.
2. Sur la page **Système**, spécifiez le nombre de jours pendant lesquels les données doivent être conservées, puis cliquez sur **Enregistrer**.

Configurer les paramètres de l'instance Syslog pour nettoyer

Pour limiter la quantité de données syslog stockées dans la base de données, vous pouvez spécifier l'intervalle suivant lequel vous souhaitez purger les données syslog. Vous pouvez spécifier le nombre de jours après lesquels les données de Syslog génériques sont supprimées de Citrix ADM.

Pour configurer les paramètres de purge de syslog d'instance :

1. Accédez à **Système > Administration > Nettoyage des données**.
2. Cliquez sur **Nettoyage des données système et instance > Instance Syslog**.
3. Sur la **page Configurer les paramètres Syslog Prune de l'instance**, spécifiez le nombre de jours compris entre 1 et 180 dans le champ **Retain Syslog** Generic Data.
4. Cliquez sur **Enregistrer**.

Configurer les paramètres de nettoyage d'événement d'instance

Pour limiter la quantité de données de messages d'événement stockées dans la base de données de votre serveur Citrix ADM, vous pouvez spécifier l'intervalle pendant lequel vous souhaitez que Citrix ADM conserve les données de rapport réseau, les événements, les journaux d'audit et les journaux des tâches. Par défaut, ces données sont effacées toutes les 24 heures (à 00:00 heures).

Pour configurer les paramètres de nettoyage d'événement d'instance :

1. Accédez à **Système > Administration**.

2. Dans la page **Administration du système**, sous **Nettoyage des données**, cliquez sur **Nettoyage des données système et instance**.
3. Dans la page **Nettoyage des données**, cliquez sur **Événements d'instance**.
4. Dans le champ **Données à conserver (jours)**, entrez l'intervalle de temps, en jours, pour lequel vous souhaitez conserver les données sur le serveur Citrix ADM, puis cliquez sur **Enregistrer**.

Configurer les paramètres de sauvegarde du système

Citrix ADM sauvegarde automatiquement le système tous les jours à 00 h 30. Par défaut, il enregistre trois fichiers de sauvegarde. Vous souhaiterez peut-être conserver un plus grand nombre de sauvegardes du système. Vous pouvez également chiffrer le fichier de sauvegarde. Vous pouvez également choisir d'enregistrer la sauvegarde sur un serveur externe.

Pour configurer les paramètres de sauvegarde du système :

1. Accédez à **Système > Administration**.
2. Sous **Sauvegarde**, cliquez sur **Configurer la sauvegarde du système et de l'instance**.
3. Cliquez sur **Système** et, sur la page **Configurer les paramètres de sauvegarde du système**, spécifiez les valeurs requises.

Configurer les paramètres de sauvegarde d'instance

Si vous sauvegardez l'état actuel d'une instance Citrix ADC, vous pouvez utiliser les fichiers de sauvegarde pour restaurer la stabilité si l'instance devient instable. Cela est particulièrement important avant d'effectuer une mise à niveau. Par défaut, une sauvegarde est effectuée toutes les 12 heures et trois fichiers de sauvegarde sont conservés dans le système.

Pour configurer les paramètres de sauvegarde d'instance :

1. Accédez à **Système > Administration**.
2. Sous **Sauvegarde**, cliquez sur **Configurer la sauvegarde du système et de l'instance**.
3. Cliquez sur **Instance**, sous **Configurer les paramètres de sauvegarde de l'instance**, et spécifiez les valeurs requises.

Activer ou désactiver les fonctionnalités ADM

En tant qu'administrateur, vous pouvez activer ou désactiver les fonctionnalités suivantes dans la page **Système > Administration > Fonctionnalités configurables** :

- **Basculement** de l'agent : le basculement de l'agent peut se produire sur un site qui a deux agents actifs ou plus. Lorsqu'un agent devient inactif (état DOWN) sur le site, le service Citrix ADM redistribue les instances ADC de l'agent inactif avec d'autres agents actifs. Pour plus d'informations, consultez Configurer des agents sur site pour un déploiement multisite.
- **Fonction de réseau d'interrogation** d'entité - Une entité est une stratégie, un serveur virtuel, un service ou une action attachée à une instance ADC. Par défaut, Citrix ADM interroge automatiquement les entités de fonction réseau configurées toutes les 60 minutes. Pour plus d'informations, consultez la section Vue d'ensemble du sondage.
- **Sauvegarde d'instance - Sauvegardez** l'état actuel d'une instance Citrix ADC et utilisez ultérieurement les fichiers sauvegardés pour restaurer l'instance ADC dans le même état. Pour de plus amples informations, consultez Sauvegarde et restauration des instances Citrix ADC.
- **Audit de configuration d'instance** : surveillez les modifications de configuration sur les instances Citrix ADC gérées, résolvez les erreurs de configuration et récupérez les configurations non enregistrées. Pour plus d'informations, consultez la section Création de modèles d'audit.
- **Événements d'instance** - Les événements représentent des occurrences d'événements ou d'erreurs sur une instance Citrix ADC gérée. Les événements reçus dans Citrix ADM sont affichés sur la page **Résumé des événements** (**Réseaux > Événements**), et tous les événements actifs sont affichés sur la page Messages d'événements (**Réseaux > Événements > Messages** d'événements). Pour plus d'informations, consultez la section Événements.
- **Rapports réseau d'instance** : vous pouvez générer des rapports pour les instances à un niveau global. Aussi, pour les entités telles que les serveurs virtuels et les interfaces réseau. Pour plus d'informations, consultez la section Rapports réseau.
- **Certificats SSL d'instance** - Citrix ADM fournit une vue centralisée des certificats SSL installés sur toutes les instances Citrix ADC gérées. Pour plus d'informations, consultez Tableau de bord SSL.
- **Instance Syslog** - Vous pouvez surveiller les événements syslog générés sur vos instances Citrix ADC si vous avez configuré votre appareil pour rediriger tous les messages syslog vers Citrix ADM.

Pour activer une fonctionnalité, effectuez les opérations suivantes :

1. Sélectionnez la fonctionnalité que vous souhaitez activer dans la liste.
2. Cliquez sur **Activer**.

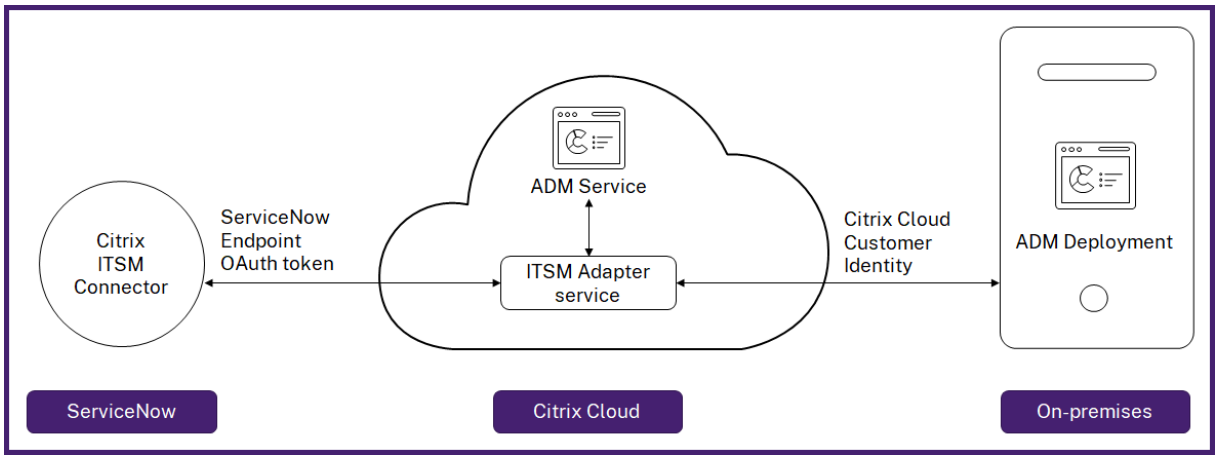
> **Important**
>
> Si une fonction est désactivée, l'utilisateur ne peut pas effectuer les opérations associées à cette fonctionnalité.

Intégrer Citrix ADM à l'instance ServiceNow

February 1, 2024

Lorsque vous souhaitez activer les notifications ServiceNow pour les événements Citrix ADC et ADM, intégrez Citrix ADM à l'instance ServiceNow. Cette intégration utilise le connecteur Citrix ITSM pour communiquer entre Citrix ADM et l'instance ServiceNow.

L'intégration de ServiceNow à ADM utilise le service d'adaptateur ITSM pour l'authentification par jeton. Pour ce faire, il crée une instance de point de terminaison dans ServiceNow. Pour plus d'informations, consultez la section Fonctionnement de l'adaptateur ITSM.



Pour connecter votre déploiement ADM sur site à un adaptateur ITSM, assurez-vous de configurer l'identité du client. Pour plus d'informations, consultez Configurer l'identité du client.

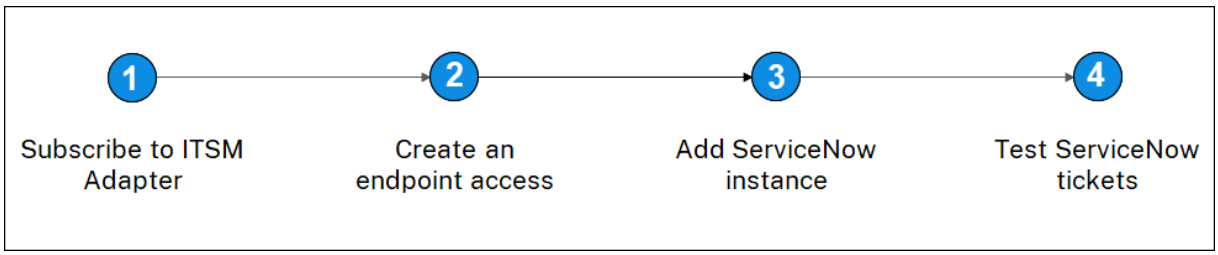
Conditions préalables

Avant d'intégrer ADM à ServiceNow, assurez-vous des points suivants :

1. Inscrivez-vous à Citrix Cloud. Assurez-vous d'avoir accès pour pouvoir gérer les administrateurs Citrix Cloud. Pour plus d'informations, consultez Gérer les administrateurs Citrix Cloud.

Comment intégrer ADM à ServiceNow ?

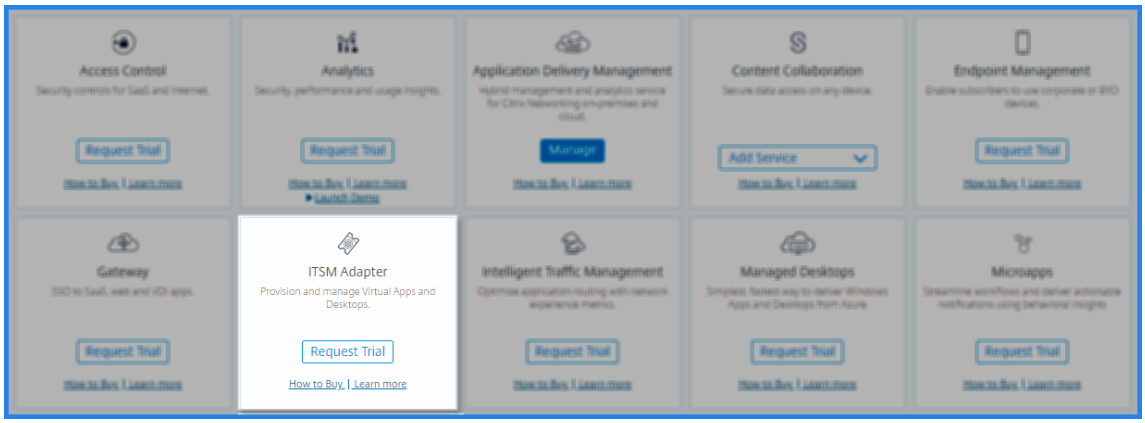
Effectuez les étapes suivantes pour intégrer Citrix ADM à ServiceNow à l'aide du connecteur ITSM :



1. Abonnez-vous au service d'adaptateur ITSM dans Citrix Cloud.
2. Créez un accès au point de terminaison dans l'instance ServiceNow.
3. Ajoutez une instance ServiceNow.
4. Testez la génération automatique de tickets ServiceNow dans ADM.

Étape 1 - S'abonner au service d'adaptateur ITSM dans Citrix Cloud

1. Sur la vignette **Adaptateur ITSM**, cliquez sur **Demander une évaluation** .

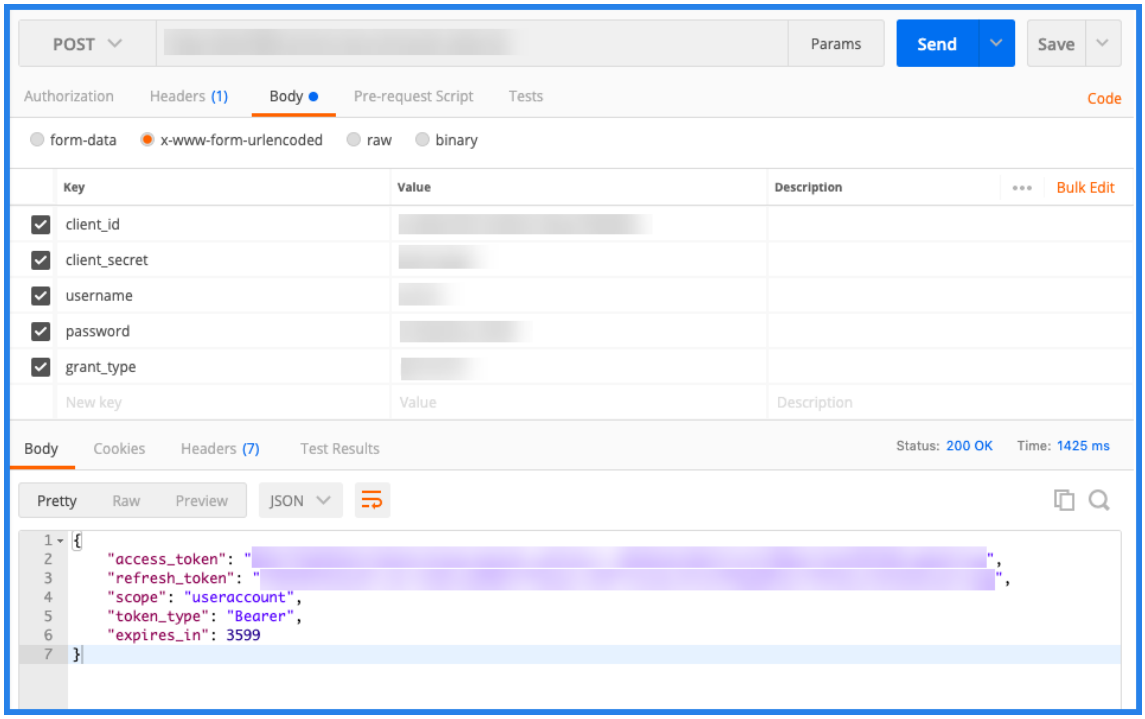


2. Accédez à **Identity Access and Management** > **API Access** et notez les informations **Client ID** et **Client Secret** .

Étape 2 - Créer un accès au point de terminaison dans l'instance ServiceNow

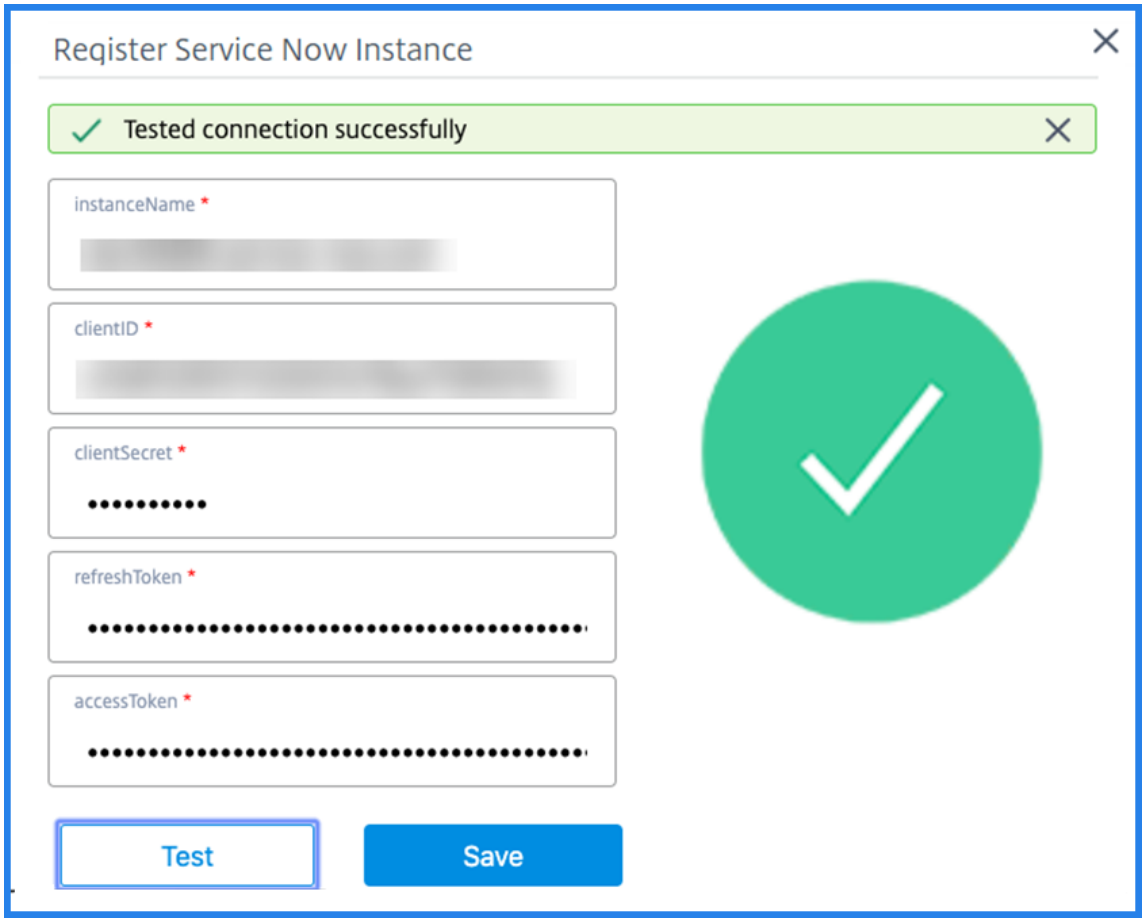
1. Connectez-vous à votre instance ServiceNow avec des informations d'identification d'administrateur.
2. Accédez au magasin ServiceNow. Téléchargez et installez le **connecteur Citrix ITSM**.
3. Dans le volet **Citrix ITSM Connector**, sélectionnez **Accueil**, puis cliquez sur **Authentifier**. Entrez l'ID client et le code secret que vous avez notés dans Citrix Cloud.
4. Testez la connexion.
5. Enregistrez la configuration. Un accusé de réception de ServiceNow apparaît indiquant que la connexion est active.

6. Créez un point de terminaison pour accéder à une instance ServiceNow. Consultez la section Créer un point de terminaison permettant aux clients d'accéder à l'instance.
7. Obtenez les jetons d'accès et d'actualisation à l'aide de l'ID client et du secret client. Consultez la section Jetons OAuth.



Étape 3 - Ajouter une instance ServiceNow

1. Dans l'onglet **Gérer**, sélectionnez Ajouter une instance ServiceNow.
2. Spécifiez le **nom de l'instance**, l'**ID du client**, le **secret du client**, le **jeton d'actualisation**et le **jeton d'accès**.
3. Cliquez sur **Test**.



L'instance ServiceNow est désormais connectée au service ITSM Adapter.

4. Après avoir testé la connexion avec succès, cliquez sur **Enregistrer** pour ajouter une instance ServiceNow.

Étape 4 - Test de génération automatique de tickets ServiceNow dans ADM

1. Connectez-vous à Citrix ADM.
2. Accédez à **Compte > Notifications** et sélectionnez **ServiceNow** .
3. Sélectionnez le profil ServiceNow dans la liste.
4. Cliquez sur **Tester** pour générer automatiquement un ticket ServiceNow et vérifier la configuration.

   Si vous souhaitez afficher les tickets ServiceNow dans l'interface graphique Citrix ADM, sélectionnez **ServiceNow Tickets**.

Configurer les notifications ServiceNow dans ADM

Une fois l'instance ServiceNow enregistrée sur l'adaptateur ITSM, vous pouvez configurer des notifications ServiceNow pour les événements suivants dans l'interface graphique Citrix ADM :

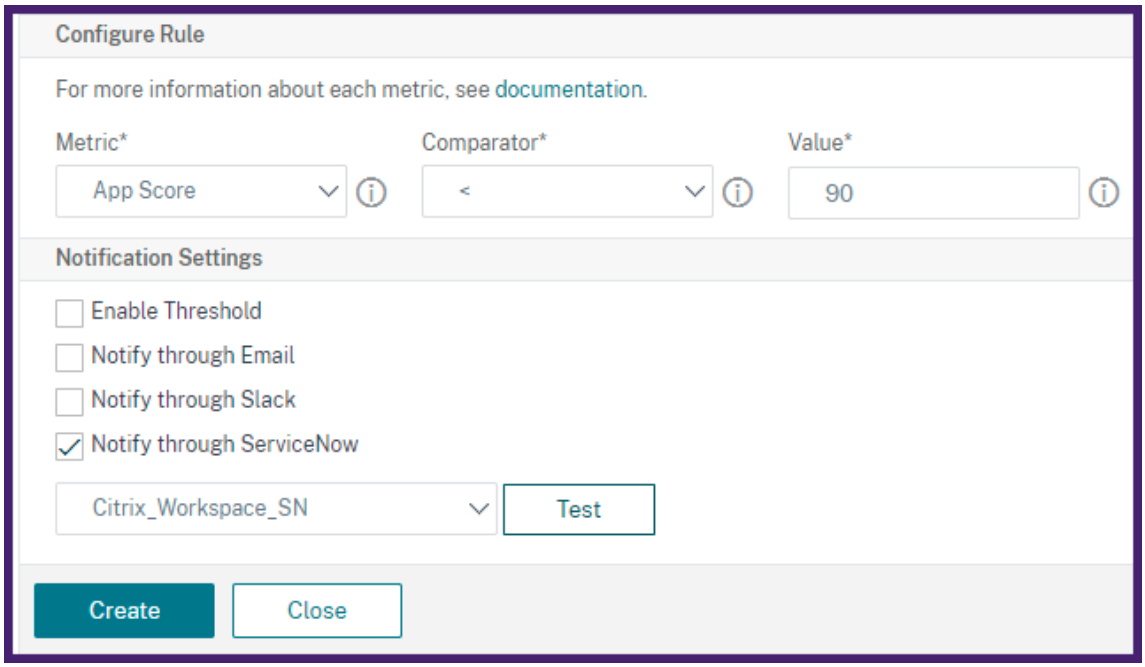
> **Important**
>
> Cette fonctionnalité est prise en charge sur ServiceNow Cloud.

- **Événements Citrix ADC** : Citrix ADM peut générer les incidents ServiceNow pour l'ensemble sélectionné d'événements Citrix ADC à partir d'instances Citrix ADC gérées sélectionnées.

  Pour envoyer des notifications ServiceNow pour les événements Citrix ADC à partir des instances gérées, vous devez configurer une règle d'événement et affecter l'action de règle comme **Envoyer des notifications ServiceNow**.

  Créez une règle d'événement sur l'ADM en accédant à **Réseaux** > **Événements** > **Règles**. Pour plus d'informations, consultez la section Envoyer des notifications ServiceNow.

- **Analyse des applications** : Citrix ADM peut générer des incidents ServiceNow pour les applications qui dépassent le seuil spécifié.



  Dans cet exemple, un incident ServiceNow est généré lorsque le score des applications tombe en dessous de 90.

- **Événements de certificat SSL et de licence ADM** : Citrix ADM peut générer les incidents ServiceNow pour l'expiration du certificat SSL et les événements d'expiration de licence ADM.

  Pour envoyer des notifications ServiceNow concernant l'expiration d'un certificat SSL, reportez-vous à la section L'expiration du certificat SSL.

Pour envoyer des notifications ServiceNow concernant l'expiration d'une licence ADM, reportez-vous à la section Expiration de la licence Citrix ADM.

Exporter ou planifier des rapports d'exportation

February 1, 2024

Dans Citrix ADM, vous pouvez exporter un rapport complet pour la fonctionnalité Citrix ADM sélectionnée. Ce rapport fournit une vue d'ensemble du mappage entre les instances, les partitions et les détails correspondants.

Citrix ADM affiche des rapports d'exportation planifiée spécifiques aux entités sous des entités ADM individuelles, que vous pouvez afficher, modifier ou supprimer. Par exemple, pour afficher les rapports d'exportation des instances Citrix ADC, accédez à **Réseau > Instances > Citrix ADC** et cliquez sur l'icône d'exportation. Vous pouvez exporter ces rapports au format PDF, JPEG, PNG et CSV.

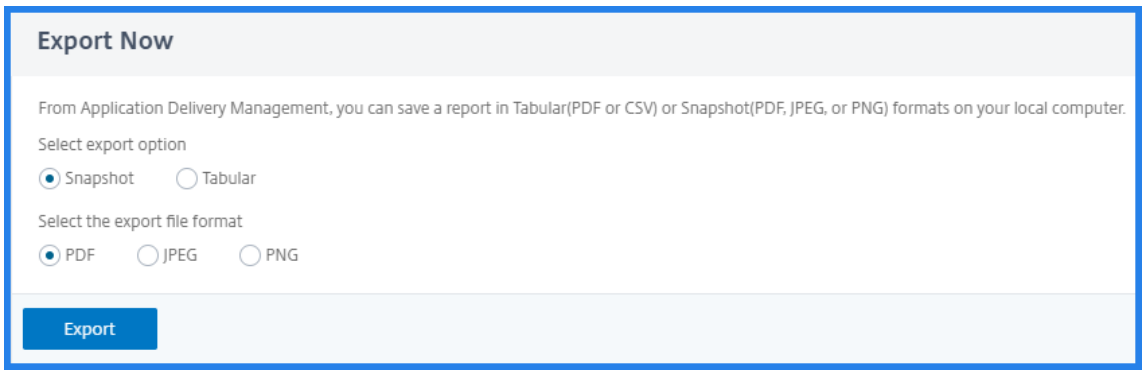
Dans **Exporter des rapports**, vous pouvez effectuer les actions suivantes :

- Exporter un rapport vers un ordinateur local
- Planification des rapports d'exportation
- Afficher, modifier ou supprimer les rapports d'exportation planifiés

Exporter un rapport

Pour exporter un rapport de l'ADM vers l'ordinateur local, effectuez les opérations suivantes :

1. Cliquez sur l'icône d'exportation dans le coin supérieur droit de la page.
2. Sélectionnez **Exporter maintenant**.
3. Sélectionnez l'une des options d'exportation suivantes :
    - **Snapshot** - Cette option exporte les rapports ADM sous la forme d'un instantané.
    - **Tabulaire** - Cette option exporte les rapports ADM dans un format tabulaire. Vous pouvez également choisir le nombre d'enregistrements de données à exporter dans un format tabulaire

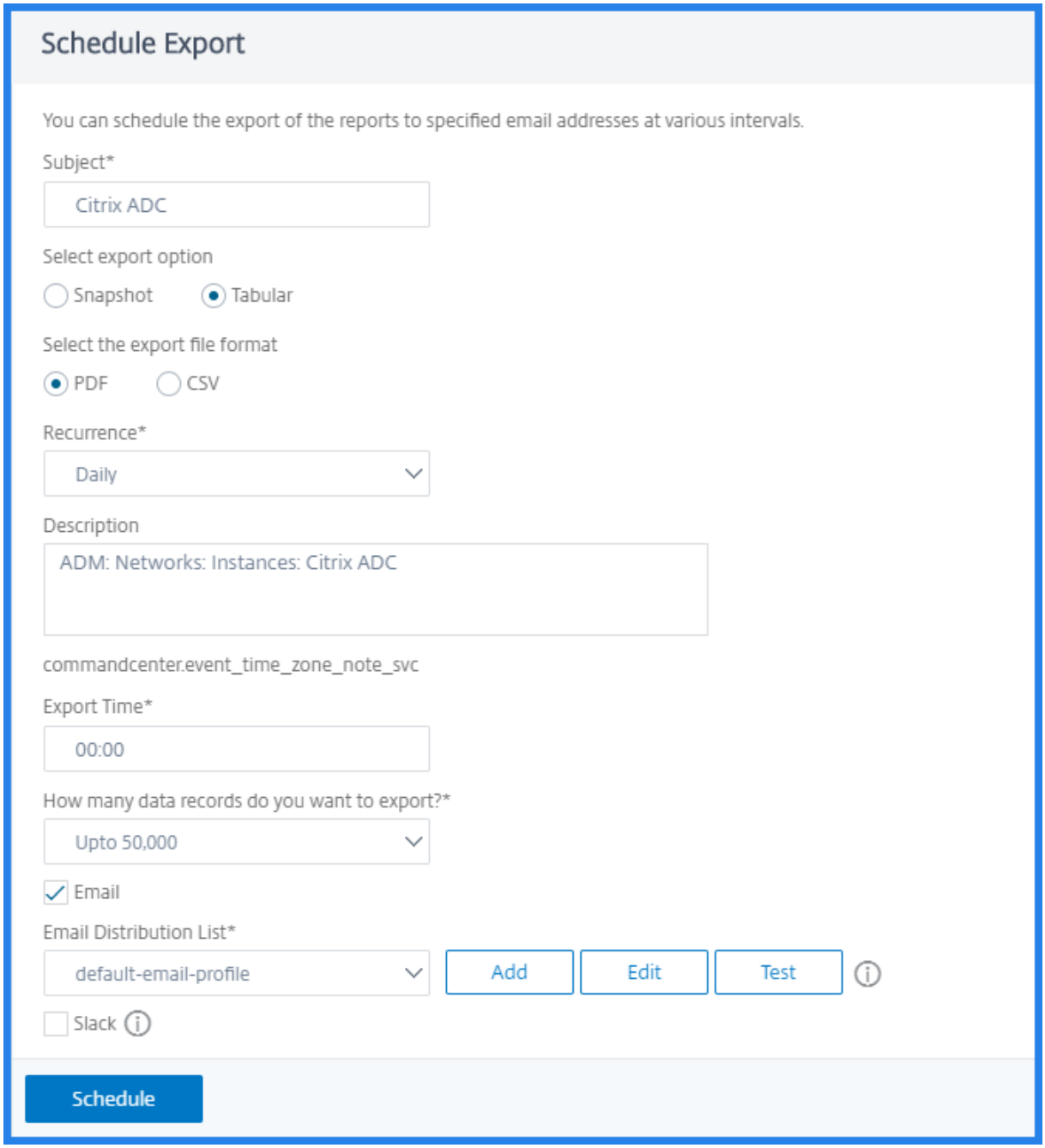


4. Sélectionnez le format de fichier que vous souhaitez enregistrer le rapport sur votre ordinateur local.
5. Cliquez sur **Exporter**.

Planifier le rapport d'exportation

Pour planifier le rapport d'exportation à intervalles réguliers, spécifiez l'intervalle de récurrence. Citrix ADM envoie le rapport exporté à l'adresse e-mail configurée ou au profil Slack.

1. Cliquez sur l'icône d'exportation dans le coin supérieur droit de la page.
2. Sélectionnez **Planifier l'exportation** et spécifiez les éléments suivants :
   - **Objet** : par défaut, ce champ renseigne automatiquement le nom de la fonction sélectionnée. Cependant, vous pouvez le réécrire avec un titre significatif.
   - **Option d'** exportation - Exporter les rapports ADM dans un instantané ou un format tabulaire. Vous pouvez également choisir le nombre d'enregistrements de données à exporter dans un format tabulaire
   - **Format** : sélectionnez le format de fichier que vous souhaitez recevoir le rapport sur le profil de courrier électronique ou de slack configuré.
   - **Récurrence** : sélectionnez **Quotidien**, **Hebdomadaire**ou **Mensuel** dans la liste.
   - **Description :** spécifiez la description significative d'un rapport.
   - **Heure d'exportation** : spécifiez l'heure à laquelle vous souhaitez exporter le rapport.
   - **E-mail** : cochez la case et sélectionnez le profil dans la zone de liste. Si vous souhaitez ajouter un profil, cliquez sur **Ajouter**.
   - **Slack** : cochez la case et sélectionnez le profil dans la zone de liste. Si vous souhaitez ajouter un profil, cliquez sur **Ajouter**.
3. Cliquez sur **Planifier**.



Afficher et modifier les rapports d'exportation planifiée

Pour consulter les rapports d'exportation, procédez comme suit :

1. Cliquez sur l'icône d'exportation dans le coin supérieur droit de la page.

   La page **Exporter le rapport** affiche tous les rapports d'exportation spécifiques aux fonctionnalités.

2. Sélectionnez le rapport à modifier, puis cliquez sur **Modifier**.

Mettre à niveau

February 1, 2024

Chaque version de Citrix ADM offre des fonctionnalités nouvelles et mises à jour avec des fonctionnalités améliorées. Citrix vous recommande de mettre à niveau Citrix ADM vers la dernière version pour bénéficier des nouvelles fonctionnalités et des corrections de bogues. Une liste complète des améliorations, des problèmes connus et des corrections de bogues est incluse dans les notes de mise à jour accompagnant chaque annonce de publication. Il est également important de comprendre le cadre de licence et les types de licences qui peuvent être utilisés avant de commencer la mise à niveau. Pour plus d'informations sur les licences Citrix ADM, reportez-vous à la section Gestion

Les informations relatives au chemin de mise à niveau sont également disponibles dans le Guide de mise à niveau Citrix

Avant de procéder à la mise à niveau

Téléchargez le package de mise à niveau à partir de la page Téléchargements Citrix ADM et suivez les instructions de cet article pour mettre à niveau votre système vers la dernière version 13.0. Après le début du processus de mise à niveau, ADM redémarre et les connexions existantes sont arrêtées et reconnectées à la fin de la mise à niveau. La configuration existante est conservée, mais Citrix ADM ne traite aucune donnée tant que la mise à niveau n'est pas terminée.

> **Important**
>
> La version et la version de Citrix ADM doivent être **égales ou supérieures à** celles de votre version et build de Citrix ADC. Par exemple, si vous avez installé Citrix ADM 12.1 Build 50.39, assurez-vous d'avoir installé Citrix ADC 12.1 Build 50.28/50.31 ou une version antérieure.

Points à noter avant la mise à niveau vers la version 13.0 :

- Si vous effectuez une mise à niveau à partir de la version 11.1 ou 12.0 56.x et des versions précédentes, effectuez les opérations suivantes :
    1. Mettre à niveau à partir de la version existante vers 12.0 build 57.24.
    2. Mettez à niveau vers la dernière version de la version 12.1.
    3. Mise à niveau vers la version 13.0.

- Si vous effectuez une mise à niveau à partir de 12.0 build 57.24 et versions ultérieures, commencez par mettre à niveau vers 12.1, puis vers 13.0.
- Si vous effectuez une mise à niveau à partir de 12.1, vous pouvez directement mettre à niveau vers 13.0.
- Si vous effectuez une mise à niveau vers 13.0 67.xx et versions ultérieures, effectuez d'abord la mise à niveau vers 13.0 64.xx puis vers 13.0 67.xx et versions ultérieures, pour une meilleure expérience utilisateur.

Points importants à noter avant la mise à niveau vers 13.0 67.xx et versions ultérieures

Lorsque vous mettez à niveau le logiciel ADM vers la version 13.0 67.xx et ultérieure, votre base de données ADM est également migrée. Cette migration de données se produit car ADM utilise désormais PostgreSQL version 10.11.

> **Remarque**
>
> La rétrogradation du logiciel ADM n'est pas prise en charge. Ne tentez pas de rétrograder.

Précautions recommandées :

- Prenez un instantané du serveur Citrix ADM si vous effectuez une mise à niveau vers 13.0 67.xx et versions ultérieures.
- Sauvegardez le serveur Citrix ADM avant de procéder à la mise à niveau.
- Après la mise à niveau, vous devrez peut-être rétablir les connexions entre le serveur Citrix ADM et les instances gérées. Une invite de confirmation vous avertit que les connexions peuvent échouer si vous continuez.
- Pour les serveurs Citrix ADM dans une configuration haute disponibilité, lors de la mise à niveau, n'apportez aucune modification de configuration sur aucun des nœuds.

  > **Avertissement**
  >
  > N'actualisez pas le navigateur tant que le processus de mise à niveau n'est pas terminé. Vérifiez l'interface graphique pour connaître la durée approximative de la mise à niveau.

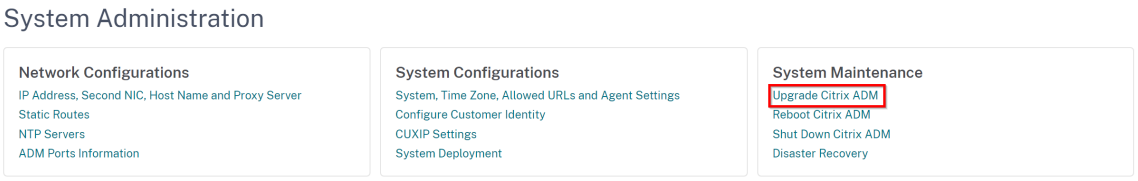
- Après la mise à niveau, le nœud actif peut changer dans une paire de haute disponibilité.

Mettre à niveau un seul serveur Citrix ADM

Pour mettre à niveau un serveur Citrix ADM unique :

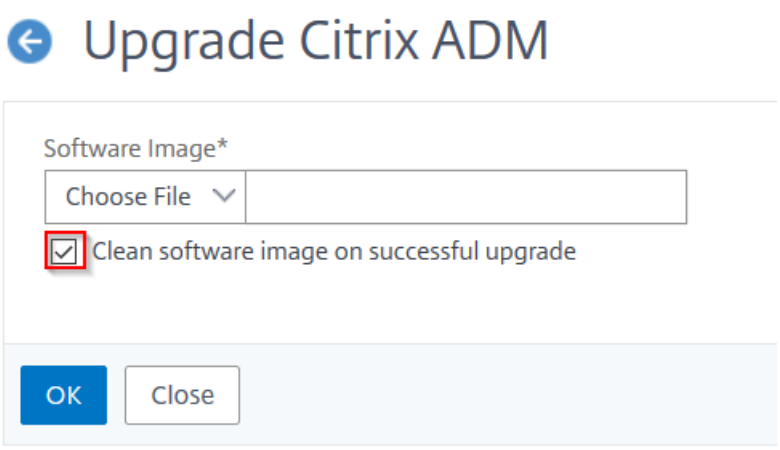
1. Ouvrez une session sur Citrix ADM avec les informations d'identification de l'administrateur.

2. Accédez à **Système** > **Administration système**. Sous le sous-titre**Administration du système**, cliquez sur **Mettre à niveau Citrix ADM**.

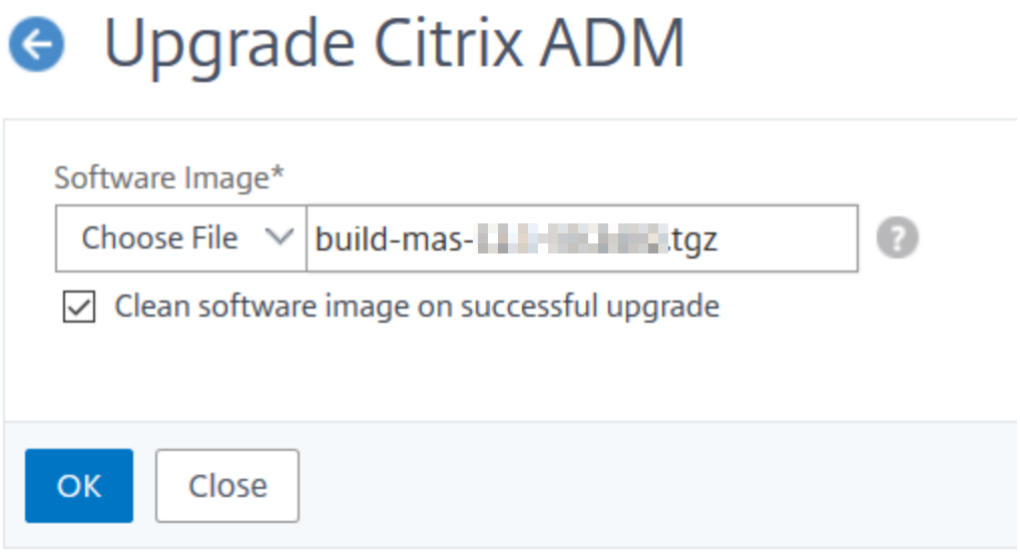


3. Sur la page**Mettre à niveau Citrix ADM**, activez la case à cocher**Nettoyer l'image logicielle lors de la mise à niveau réussie** pour supprimer les fichiers image après la mise à niveau. La sélection de cette option supprime automatiquement les fichiers image Citrix ADM lors de la mise à niveau.

> **Remarque**
>
> Cette option est sélectionnée par défaut. Si vous ne cochez pas cette case avant de commencer le processus de mise à niveau, vous devez supprimer manuellement les images.



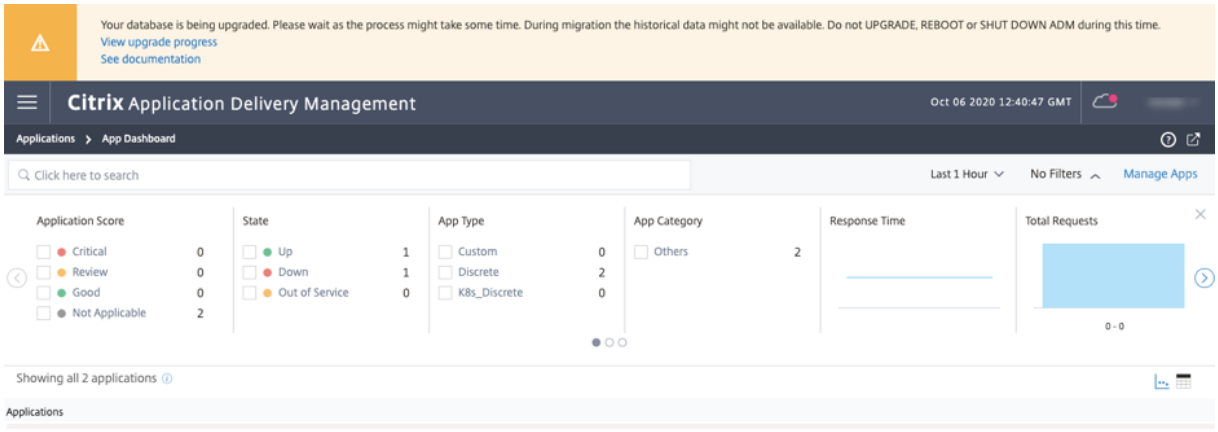
4. Vous pouvez ensuite télécharger un nouveau fichier image en sélectionnant**Local** (votre machine locale) ou**Appliance**. Le fichier de construction doit être présent sur l'appliance virtuelle Citrix ADM.



5. Cliquez sur **OK**.
   La boîte de dialogue Confirmer s'affiche. Cliquez sur **Oui**.

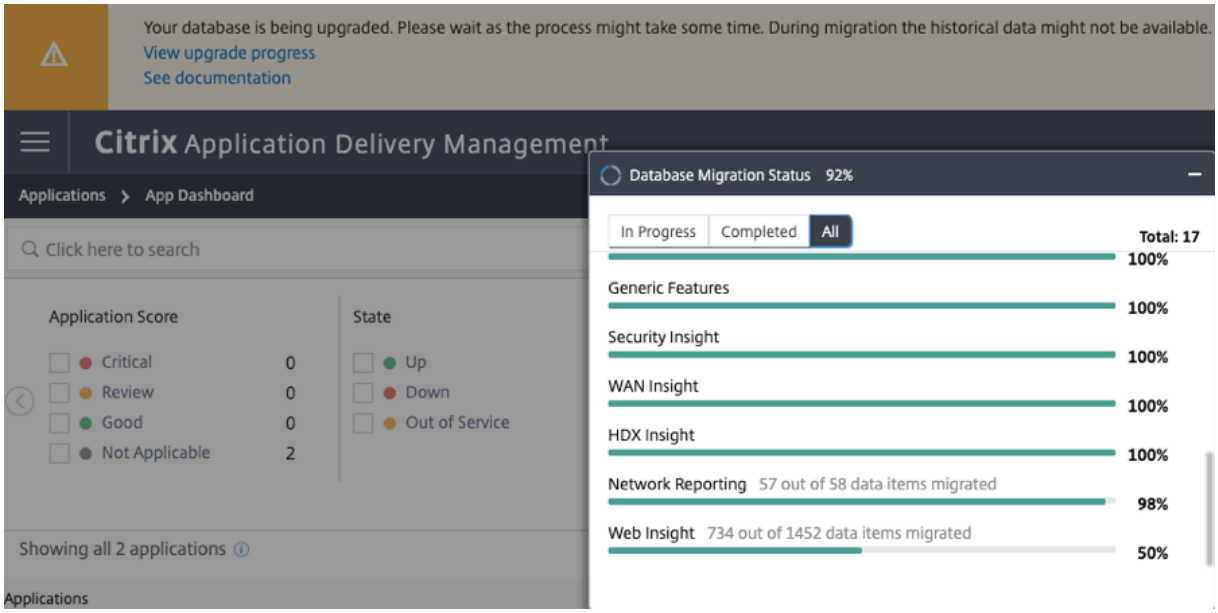
   Le processus de mise à niveau démarre.

Une fois votre configuration migrée, vous pouvez vous connecter à l'interface graphique ADM. Lors de l'ouverture de session, les données historiques commencent à migrer en arrière-plan pendant que vous pouvez continuer à travailler sur ADM.



Lors de la migration des données historiques, certaines des anciennes données peuvent ne pas être disponibles. Le temps nécessaire à la migration de votre base de données dépend de la taille des données et du nombre de tables.

Vous pouvez surveiller la migration de la base de données à l'aide de l'interface graphique ADM. Cliquez sur **Afficher la progression de la mise à niveau** pour afficher l'**état de migration de la base**



Résolution des problèmes de migration de base de données

Pendant le processus de mise à niveau vers 13.0 67.xx et versions ultérieures, la migration des données historiques Web Insight peut parfois sembler bloquée. Dans de tels cas, pour vérifier les détails de la migration des données, procédez comme suit.

Connectez-vous à l'invite ADM shell et exécutez la commande suivante pour afficher les détails granulaires de la progression.

```
1     cat /var/mps/log/db_upgrade/web_insight_mapping_migration_status
2
3 <!--NeedCopy-->
```

Voici un exemple de sortie

```
1     bash-3.2# cat /var/mps/log/db_upgrade/
         web_insight_mapping_migration_status
2     Tue Oct  6 07:41:55 GMT 2020
3     157 out of 127346 done in 54 seconds
4     File
5      /var/mps/db_upgrade/hist_table_mig_data/Web_Insight/
          af_app_client_server_resp_second_l3p_d7_dump
6     bash-3.2#
7
8  <!--NeedCopy-->
```

Dans cet exemple, `af_app_client_server_resp_second_l3p_d7` est l'entrée en cours de mise à niveau. Et 157 entrées sur 127 346 sont migrées en 54 secondes.

Mettre à niveau une paire haute disponibilité de la version 12.1 vers la version 13.0

Pour les serveurs Citrix ADM en mode haute disponibilité, vous pouvez effectuer une mise à niveau en accédant au nœud actif ou à l'adresse IP flottante. Les deux serveurs Citrix ADM sont automatiquement mis à niveau vers la dernière version une fois que vous lancez le processus de mise à niveau dans l'un ou l'autre des serveurs.

> **Remarque**
>
> Si vous mettez à niveau une paire haute disponibilité à partir de versions 12.0 ou antérieures, consultez la section Mise à niveau de Citrix ADM 12.1

Mettre à niveau le déploiement de reprise après sinistre Citrix ADM

La mise à niveau du déploiement de reprise après sinistre Citrix ADM se fait en deux étapes :

- Mettez à niveau les nœuds Citrix ADM configurés en mode haute disponibilité sur le site principal. Plus tard, vous devez mettre à niveau le nœud de reprise après sinistre.
- Assurez-vous d'avoir mis à niveau les serveurs Citrix ADM déployés en haute disponibilité avant de mettre à niveau le nœud de reprise après sinistre.

Mettre à niveau le nœud de reprise après sinistre Citrix ADM

1. Télécharger le fichier image de mise à niveau Citrix ADM à partir du site de téléchargement Citrix.
2. Téléchargez ce fichier vers le nœud de reprise après sinistre à l'aide des informations d'identification `nsrecover`.
3. Connectez-vous au nœud de reprise après sinistre à l'aide des informations d'identification `nsrecover`.
4. Accédez au dossier dans lequel vous avez placé le fichier image et décompressez le fichier.

```
login as: nsrecover
Using keyboard-interactive authentication.
Password:
Last login: Wed May 15 05:27:10 2019 from 10.252.241.103
bash-3.2# cd /var/mps/mps_images
bash-3.2# tar xvfz build-mas-13.0-36.25.tgz
```

5. Exécutez le script suivant :

   . /installmas

```
bash-3.2# ./installmas
```


Mettre à niveau les agents sur site pour un déploiement multisite

La mise à niveau du déploiement de l'agent Citrix ADM s'effectue en trois étapes.
Assurez-vous d'avoir effectué les tâches suivantes avant de mettre à niveau les agents sur site :

1. Mettez à niveau les serveurs Citrix ADM déployés en haute disponibilité.
2. Mettez à niveau le nœud de reprise après sinistre Citrix ADM.

   Pour plus d'informations, consultez Mettre à niveau le déploiement de récupération d'urgence Citrix ADM.

Mettre à niveau l'agent sur site

1. Télécharger le fichier image de mise à niveau de l'agent Citrix ADM à partir du site de téléchargement Citrix.
2. Téléchargez ce fichier sur le nœud de l'agent à l'aide des `nsrecover` informations d'identification.
3. Assurez-vous que vous téléchargez l'image de mise à niveau de l'agent correcte. Voici un exemple de format de nom de fichier image :

   build-masagent-13.0-48.18.tgz
4. Connectez-vous à l'agent sur site à l'aide des `nsrecover` informations d'identification.
5. Accédez au dossier dans lequel vous avez placé le fichier image et décompressez le fichier.

```
login as: nsrecover
Using keyboard-interactive authentication.
Password:
Last login: Thu Aug 30 08:50:48 2018 from 10.252.241.37
bash-3.2# cd /var/mps/mps_images/
bash-3.2# tar zxvf build-masagent-12.1-502.109.tgz
```

6. Exécutez le script suivant :

   `./installmasagent`

```
bash-3.2# ./installmasagent
```

Ajouter un disque supplémentaire au serveur Citrix ADM

Si votre besoin de stockage Citrix ADM dépasse l'espace disque par défaut (120 Go), vous pouvez attacher un disque supplémentaire. Vous pouvez attacher plus de disque dans les déploiements mono-serveur et haute disponibilité.

Lorsque vous mettez à niveau Citrix ADM à partir de la version 12.1—13.0, les partitions que vous aviez créées sur le disque supplémentaire dans la version précédente restent les mêmes. Les partitions ne sont pas supprimées et ne sont pas redimensionnées.

La procédure pour connecter un disque supplémentaire reste la même dans la version mise à niveau. Vous pouvez maintenant utiliser le nouvel outil de partitionnement de disque dans Citrix ADM pour créer des partitions dans le disque nouvellement ajouté. Vous pouvez également utiliser l'outil pour redimensionner les partitions dans le disque supplémentaire existant. Pour plus d'informations sur la façon d'attacher davantage de disques et d'utiliser le nouvel outil de partitionnement de disque, consultez Comment attacher un disque supplémentaire à Citrix ADM.

Provisionner des instances Citrix ADC dans OpenStack à l'aide de StyleBooks

A partir de Citrix ADM 12.1 build 49.23, l'architecture d'un workflow d'orchestration OpenStack a été mise à jour. Le workflow utilise désormais Citrix ADM StyleBooks pour configurer les instances Citrix ADC. Si vous effectuez une mise à niveau vers Citrix ADM 13.0 à partir de la version 12.0 ou 12.1 build 48.18, vous devez exécuter le script de migration suivant :

```
/mps/scripts/migration_scripts/migrate_configurations.py
<!--NeedCopy-->
```

Pour plus d'informations sur le `os-cs-lb-mon` StyleBook et le script de migration, consultez Provisioning of Citrix ADC VPX instance on OpenStack using StyleBook

Authentification

February 1, 2024

Les utilisateurs peuvent être authentifiés soit en interne par Citrix ADM, soit en externe par un serveur d'authentification, soit les deux. Si l'authentification locale est utilisée, l'utilisateur doit se trouver dans la base de données de sécurité Citrix ADM. Si l'utilisateur est authentifié en externe, le « nom externe » de l'utilisateur doit correspondre à l'identité de l'utilisateur externe enregistrée auprès du serveur d'authentification, en fonction du protocole d'authentification sélectionné.

Citrix ADM prend en charge l'authentification externe par les serveurs RADIUS, LDAP et TACACS. Cette prise en charge unifiée fournit une interface commune permettant d'authentifier et d'autoriser tous les utilisateurs des serveurs d'authentification, d'autorisation et de comptabilité locaux et externes qui accèdent au système. Citrix ADM peut authentifier les utilisateurs quels que soient les protocoles qu'ils utilisent pour communiquer avec le système. Lorsqu'un utilisateur tente d'accéder à une implémentation Citrix ADM configurée pour l'authentification externe, le serveur d'applications demandé

envoie le nom d'utilisateur et le mot de passe au serveur RADIUS, LDAP ou TACACS pour authentification. Si l'authentification est réussie, l'utilisateur est autorisé à accéder à Citrix ADM.

Serveurs d'authentification externes

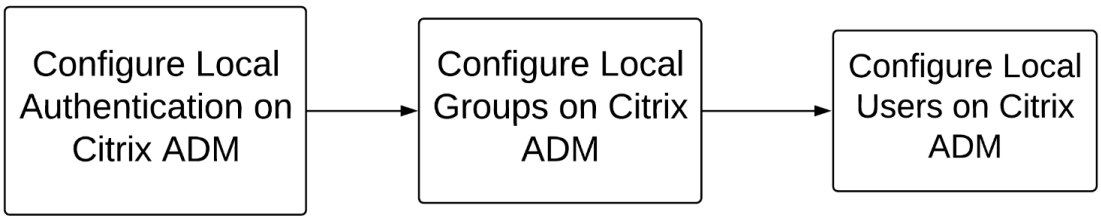
Citrix ADM envoie toutes les demandes de service d'authentification, d'autorisation et d'audit au serveur RADIUS, LDAP ou TACACS distant. Le serveur d'authentification, d'autorisation et d'audit à distance reçoit la demande, valide la demande et envoie une réponse à Citrix ADM. Lorsqu'il est configuré pour utiliser un serveur RADIUS, TACAS ou LDAP distant pour l'authentification, Citrix ADM devient un client RADIUS, TACACS ou LDAP. Dans l'une de ces configurations, les enregistrements d'authentification sont stockés dans la base de données du serveur hôte distant. Le nom du compte, les autorisations attribuées et les enregistrements de comptabilisation temporelle sont également stockés sur le serveur d'authentification, d'autorisation et d'audit pour chaque utilisateur.

En outre, vous pouvez utiliser la base de données interne de Citrix ADM pour authentifier les utilisateurs localement. Vous créez des entrées dans la base de données pour les utilisateurs, leurs mots de passe et leurs rôles par défaut. Vous pouvez également sélectionner l'ordre d'authentification pour des types d'authentification spécifiques. La liste des serveurs d'un groupe de serveurs est une liste ordonnée. Le premier serveur de la liste est toujours utilisé à moins qu'il ne soit indisponible, auquel cas le serveur suivant de la liste est utilisé. Vous pouvez configurer les serveurs de manière à inclure la base de données interne en tant que sauvegarde d'authentification de secours à la liste configurée des serveurs d'authentification, d'autorisation et d'audit.

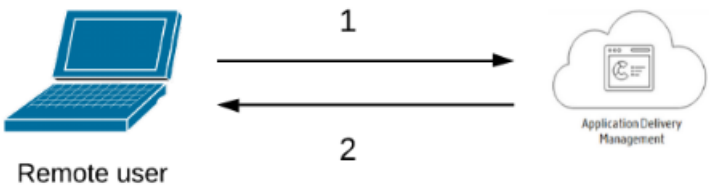
Authentifier les utilisateurs dans Citrix ADM

Vous pouvez authentifier vos utilisateurs dans Citrix ADM de deux manières :

- Utilisateurs locaux configurés dans Citrix ADM



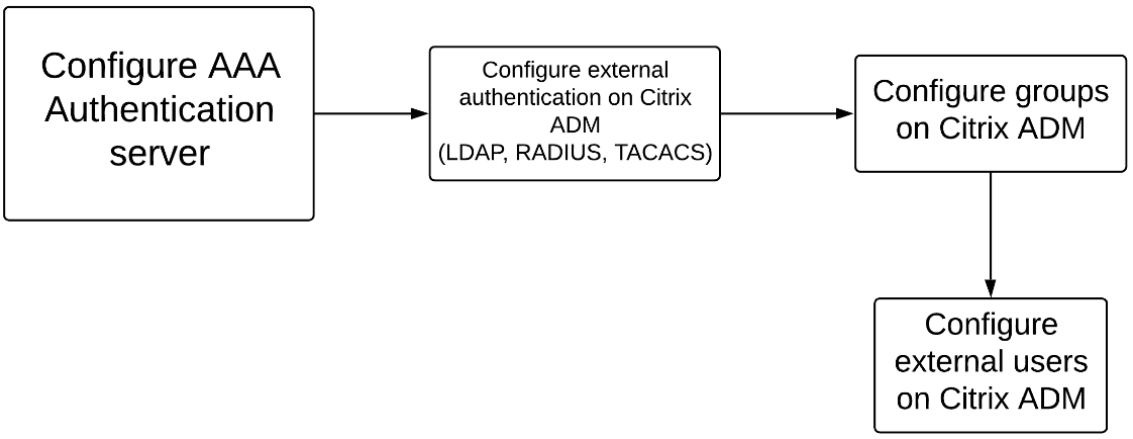
Après la configuration, ce qui suit est le flux de travail pour l'authentification de l'utilisateur sur le serveur local.



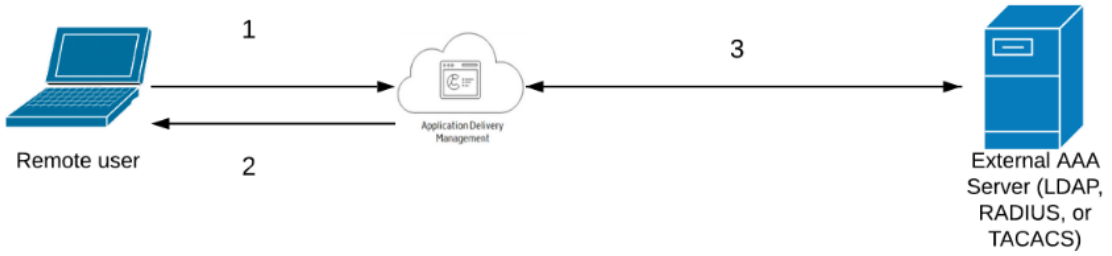
1 —L'utilisateur se connecte à Citrix ADM

2 —Citrix ADM invite les utilisateurs à saisir les informations d'identification pour l'authentification et vérifie si les informations d'identification correspondent dans la base de données ADM.

- Utilisation de serveurs d'authentification externes



Après la configuration, ce qui suit est le flux de travail d'authentification utilisateur sur le serveur d'authentification externe, d'autorisation et d'audit :



1 —L'utilisateur se connecte à Citrix ADM

2 —Citrix ADM invite l'utilisateur à fournir des informations d'identification

3 —Citrix ADM valide les informations d'identification de l'utilisateur avec le serveur externe d'authentification, d'autorisation et d'audit. Si la validation est réussie, l'utilisateur peut continuer à ouvrir une session

Configurer des serveurs d'authentification externes dans Citrix ADM

February 1, 2024

Après avoir configuré le serveur LDAP, RADIUS ou TACACS, vous pouvez ajouter ces serveurs dans Citrix ADM.

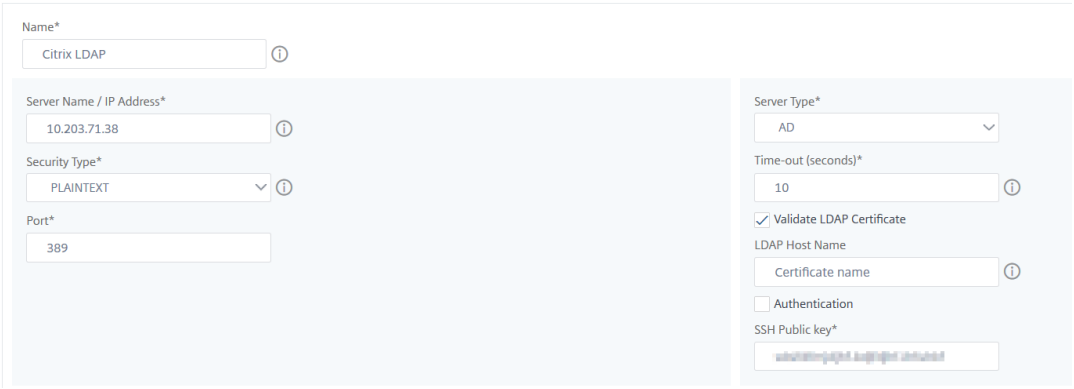
Ajouter un serveur d'authentification LDAP

February 1, 2024

Lorsque vous intégrez le protocole LDAP aux serveurs d'authentification RADIUS et TACACS, vous pouvez utiliser ADM pour rechercher et authentifier les informations d'identification des utilisateurs à partir de répertoires distribués.

1. Accédez à **Système** > **Authentification**.
2. Sélectionnez l'onglet **LDAP**, puis cliquez sur **Ajouter**.
3. Sur la page **Créer un serveur LDAP**, spécifiez les paramètres suivants :
    a) **Nom** : spécifiez le nom du serveur LDAP
    b) **Nom du serveur/adresse IP** —**Spécifiez l'adresse IP** LDAP ou le nom du serveur
    c) **Type de sécurité** : type de communication requis entre le système et le serveur LDAP. Sélectionnez dans la liste. Si la communication en texte brut est inadéquate, vous pouvez choisir une communication cryptée en sélectionnant Transport Layer Security (TLS) ou SSL
    d) **Port** —Par défaut, le port 389 est utilisé pour PLAINTEXT. Vous pouvez également spécifier le port 636 pour SSL/TLS
    e) **Type de serveur** : sélectionnez Active Directory (AD) ou Novell Directory Service (NDS) comme type de serveur LDAP
    f) **Délai d'attente (secondes)** : durée en secondes pendant laquelle le système Citrix ADM attend une réponse du serveur LDAP
    g) **Nom d'hôte LDAP** —Activez la case à cocher Valider le certificat LDAP et spécifiez le nom d'hôte à saisir sur le certificat

    Désactivez l'option **Authentification** et spécifiez la clé publique SSH. Avec l'authentification par clé, vous pouvez désormais récupérer la liste des clés publiques stockées sur l'objet utilisateur sur le serveur LDAP via SSH.



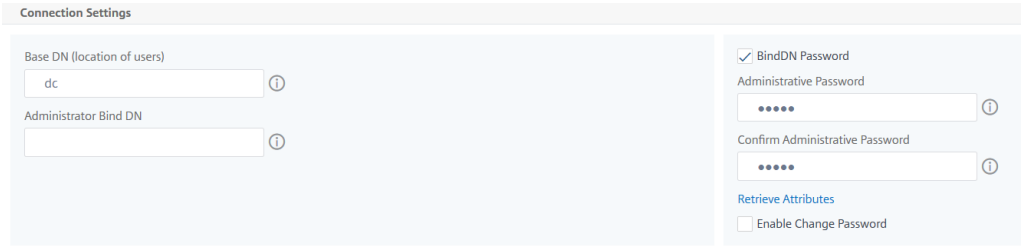
Sous Paramètres de connexion, spécifiez les paramètres suivants :

i. **Base DN** : nœud de base permettant au serveur LDAP de démarrer la recherche

ii. **Administrator Bind DN** : nom d'utilisateur associé à la liaison au serveur LDAP. Par exemple, admin@aaa.local.

iii. **Bind DN password** : sélectionnez cette option pour fournir un mot de passe pour l'authentification

iv. **Activer le changement de mot de passe** —Sélectionnez cette option pour activer le changement de mot de passe



Sous **Autres paramètres**, spécifiez les paramètres suivants

i. Attribut de**nom de connexion au serveur : attribut** de nom utilisé par le système pour interroger le serveur LDAP externe ou un Active Directory. Sélectionnez **SAMAccountName** dans la liste.

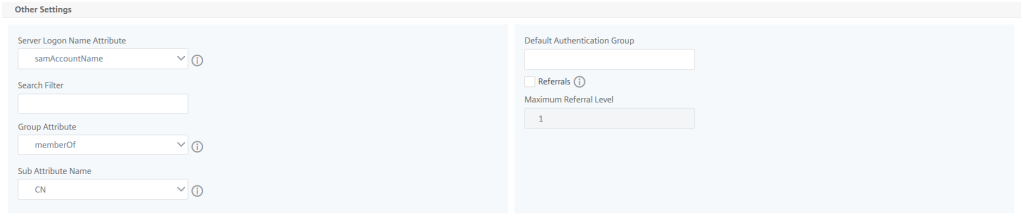
ii. **Filtre de recherche** : configurez les utilisateurs externes pour l'authentification à deux facteurs en fonction du filtre de recherche configuré dans le serveur LDAP. Par exemple, vpnallowed=true avec ldaploginame `samaccount` et le nom d'utilisateur bob fourni par l'utilisateur donnerait une chaîne de recherche LDAP de : &(`vpnallowed`=**`true`**)(`samaccount`=`bob`).

> Remarque
>
> Par défaut, les valeurs du filtre de recherche sont placées entre parenthèses.

iii. **Attribut de groupe** : sélectionnez MemberOf dans la liste.

iv. **Nom du sous-attribut** : nom du sous-attribut pour l'extraction de groupes depuis le serveur LDAP.

v. **Groupe d'authentification** par défaut : groupe par défaut à choisir lorsque l'authentification aboutit, en plus des groupes extraits.



4. Cliquez sur **Créer**.

   Le serveur LDAP est maintenant configuré.

   > Remarque
   >
   > Si les utilisateurs sont des membres du groupe Active Directory, le groupe et les noms des utilisateurs sur Citrix ADM doivent avoir les mêmes noms que les membres du groupe Active Directory.

Ajouter un serveur d'authentification RADIUS

February 1, 2024

1. Accédez à **Système** > **Authentification**.
2. Sélectionnez l'onglet **RADIUS**, puis cliquez sur **Ajouter**.

   Sur la page **Créer un serveur RADIUS**, spécifiez les paramètres suivants :

   a) **Nom** —Spécifiez un nom de serveur RADIUS

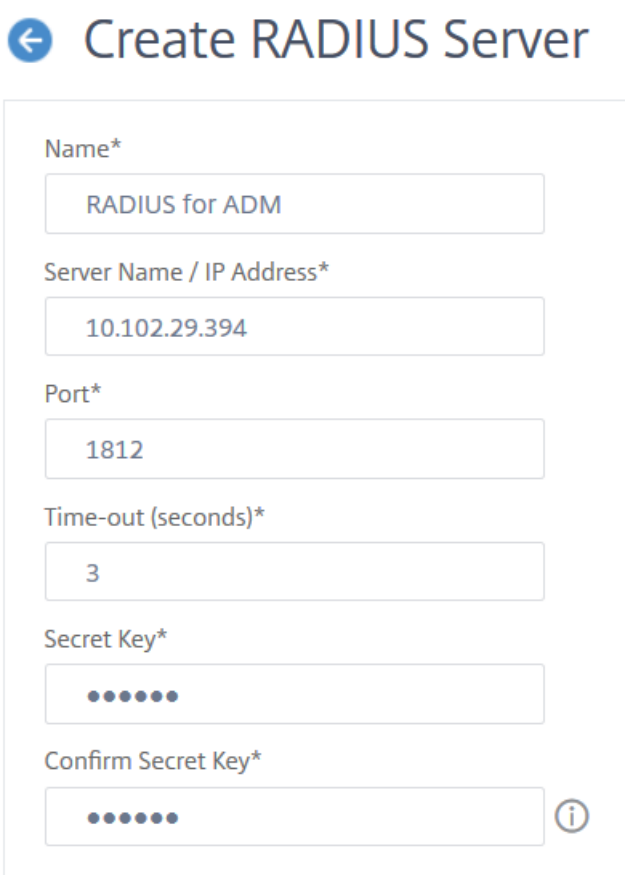
   b) **Nom du serveur/adresse IP** —Spécifiez l'adresse IP du serveur RADIUS

   c) **Port** —Spécifiez le numéro de port sur lequel le serveur RADIUS est hébergé. Le port par défaut est 1812

   d) **Délai d'attente (secondes)** : durée en secondes pendant laquelle le système Citrix ADM attend une réponse du serveur RADIUS

   e) **Clé secrète** —Spécifie la clé secrète RADIUS pour l'authentification

   f) **Confirmer la clé secrète** —Spécifiez à nouveau la clé pour confirmation



Sous **Détails**, spécifiez les paramètres suivants :

i. **ID NAS** —Spécifiez l'ID pour envoyer l'identifiant au serveur RADIUS

ii. **Identifiant du fournisseur du groupe : spécifiez l'identifiant** du fournisseur pour l'utilisation de l'extraction de groupe RADIUS

iii. **Préfixe de groupe** : chaîne qui précède les noms de groupes dans un attribut RADIUS pour l'extraction de groupes RADIUS

iv. **Type d'attribut de groupe** —Spécifiez le type d'attribut pour l'extraction de groupes RADIUS

v. **Séparateur de groupes** : chaîne qui délimite les noms de groupes au sein d'un attribut RADIUS pour l'extraction de groupes RADIUS

vi. **Identifiant du fournisseur de l'adresse IP** —**L'identifiant** du fournisseur dans RADIUS indique l'adresse IP de l'intranet. La valeur 0 indique que l'attribut n'est pas codé par le fournisseur.

vii. **Identifiant du fournisseur du mot de passe : mot de passe de l'identifiant** du fournisseur dans la réponse RADIUS pour extraire le mot de passe utilisateur

viii. **Type d'attribut d'adresse IP** : attribut d'adresse IP distante auquel le RADIUS doit répondre

ix. **Type d'attribut de mot** de passe —L'attribut de mot de passe permettant au RADIUS de répondre

x. **Codage du mot** de passe : sélectionnez pap, chap, mschapv1 ou mschapv2 dans la liste. Cela indique comment les mots de passe doivent être codés dans les paquets RADIUS circulant du système vers le serveur RADIUS.

xi. **Groupe d'authentification** par défaut : groupe par défaut à choisir lorsque l'authentification réussit, en plus des groupes extraits

Sélectionnez Comptabilité si vous souhaitez que l'appliance enregistre les informations d'audit avec le serveur RADIUS.

3. Cliquez sur **Créer**.

Le serveur RADIUS est maintenant configuré.

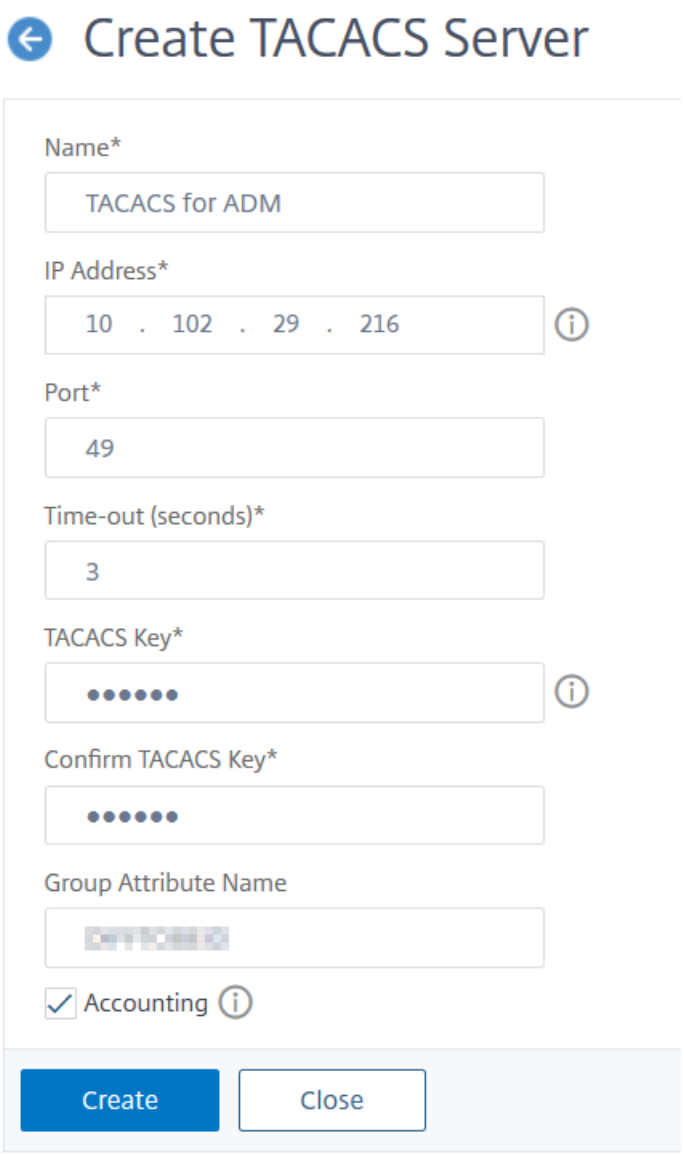
Ajouter un serveur d'authentification TACACS

February 1, 2024

1. Accédez à **Système** > **Authentification**.
2. Sélectionnez l'onglet **TACACS**, puis cliquez sur **Ajouter**.
3. Sur la page **Create TACACS**, spécifiez les paramètres suivants :
   a) **Nom** —Spécifiez un nom de serveur TACACS
   b) **Adresse IP** —Spécifiez l'adresse IP TACACS
   c) **Port** —Spécifiez le numéro de port sur lequel le serveur TACACS est hébergé. Le port par défaut est 49
   d) **Délai d'attente (secondes)** : durée en secondes pendant laquelle le système Citrix ADM attend une réponse du serveur LDAP
   e) Clé**TACACS** —Spécifiez la clé TACACS pour l'authentification
   f) **Confirmer la clé TACACS** —Spécifiez à nouveau la clé TACACS pour confirmation
   g) **Nom de l'attribut du groupe** —Spécifiez le nom du groupe

   Sélectionnez **Comptabilité** si vous souhaitez que l'appliance enregistre les informations d'audit avec le serveur TACACS.

4. Cliquez sur **Créer**.



Utilisateurs dans Citrix ADM

February 1, 2024

Vous pouvez créer des comptes d'utilisateurs localement sur Citrix ADM pour compléter les utilisateurs sur les serveurs d'authentification. Par exemple, vous pouvez créer des comptes d'utilisateurs locaux pour des utilisateurs temporaires, tels que des consultants ou des visiteurs, sans créer d'entrée pour ces utilisateurs sur le serveur d'authentification.

Pour plus d'informations sur la configuration des utilisateurs, consultez Configurer des utilisateurs.

> Remarque
>
> Si les utilisateurs sont sur Active Directory, assurez-vous que le nom de groupe dans Citrix ADM est identique à celui du groupe Active Directory sur le serveur externe.

Groupes d'utilisateurs dans Citrix ADM

Citrix ADM vous permet d'authentifier et d'autoriser vos utilisateurs en créant des groupes et en ajoutant les utilisateurs aux groupes. Un groupe peut disposer d'autorisations « admin » ou « lecture seule » et tous les utilisateurs de ce groupe recevront des autorisations égales.

Dans Citrix ADM :

- Un groupe est défini comme un ensemble d'utilisateurs ayant des autorisations similaires
- Un groupe peut avoir un ou plusieurs rôles
- Un utilisateur est défini comme une entité qui peut avoir accès en fonction des autorisations attribuées
- Un utilisateur peut appartenir à un ou plusieurs groupes

Vous pouvez créer des groupes locaux dans Citrix ADM et utiliser l'authentification locale pour les utilisateurs des groupes. Si vous utilisez des serveurs externes pour l'authentification, configurez les groupes sur Citrix ADM pour qu'ils correspondent aux groupes configurés sur les serveurs d'authentification du réseau interne. Lorsqu'un utilisateur ouvre une session et est authentifié, si un nom de groupe correspond à un groupe sur un serveur d'authentification, l'utilisateur hérite des paramètres du groupe sur Citrix ADM.
Si vous utilisez l'authentification locale, créez des utilisateurs et ajoutez-les à des groupes configurés sur Citrix ADM. Les utilisateurs héritent ensuite des paramètres de ces groupes.

Pour plus d'informations sur la configuration des groupes et l'attribution d'autorisations de groupe, consultez Configurer des groupes.

Extraire un groupe de serveurs d'authentification

February 1, 2024

> **Remarque**
>
> L'extraction du serveur TACACS est prise en charge à partir de **Citrix ADM 13.0**.

Citrix ADM vous permet de :

- Extrayez la liste des groupes auxquels un utilisateur appartient sur le serveur d'authentification externe.
- Affectez-les aux paramètres de groupe correspondant aux groupes configurés sur le serveur externe.

Avantages:

- Vous n'avez pas besoin de créer des utilisateurs dans Citrix ADM, car ils sont gérés sur le serveur externe.
- Citrix ADM effectue l'autorisation des utilisateurs en attribuant des autorisations de groupe pour accéder à des serveurs virtuels d'équilibrage de charge spécifiques et à des applications spécifiques sur le système.

Activer les serveurs d'authentification externes de secours et en cascade

February 1, 2024

L'option de secours permet à l'authentification locale de prendre le relais en cas d'échec de l'authentification du serveur externe. Un utilisateur configuré à la fois sur Citrix ADM et sur un serveur d'authentification externe peut se connecter à Citrix ADM, même si les serveurs d'authentification externes configurés sont en panne ou inaccessibles. Pour garantir le fonctionnement de l'authentification de secours :

- Les utilisateurs non-NSroot doivent pouvoir accéder à Citrix ADM si le serveur externe est en panne ou inaccessible
- Vous devez ajouter au moins un serveur externe

Citrix ADM prend également en charge un système unifié de protocoles d'authentification, d'autorisation et de comptabilité (AAA) (LDAP, RADIUS et TACACS), ainsi que l'authentification locale. Ce support unifié fournit une interface commune pour authentifier et autoriser tous les utilisateurs et clients AAA externes accédant au système.

Citrix ADM peut authentifier les utilisateurs quels que soient les protocoles qu'ils communiquent avec le système.
La mise en cascade des serveurs d'authentification externes fournit un processus continu sans échec pour l'authentification et l'autorisation des utilisateurs externes. Si l'authentification échoue sur le premier serveur d'authentification, Citrix ADM tente d'authentifier l'utilisateur à l'aide du second serveur d'authentification externe, etc. Pour activer l'authentification en cascade, vous devez ajouter

les serveurs d'authentification externes dans Citrix ADM. Vous pouvez ajouter n'importe quel type de serveurs d'authentification externes pris en charge (RADIUS, LDAP et TACACS).

Par exemple, considérez que vous souhaitez ajouter quatre serveurs d'authentification externes et configurer deux serveurs RADIUS, un serveur LDAP et un serveur TACACS. Citrix ADM tente de s'authentifier auprès des serveurs externes, en fonction des configurations. Dans cet exemple de scénario, Citrix ADM tente de :

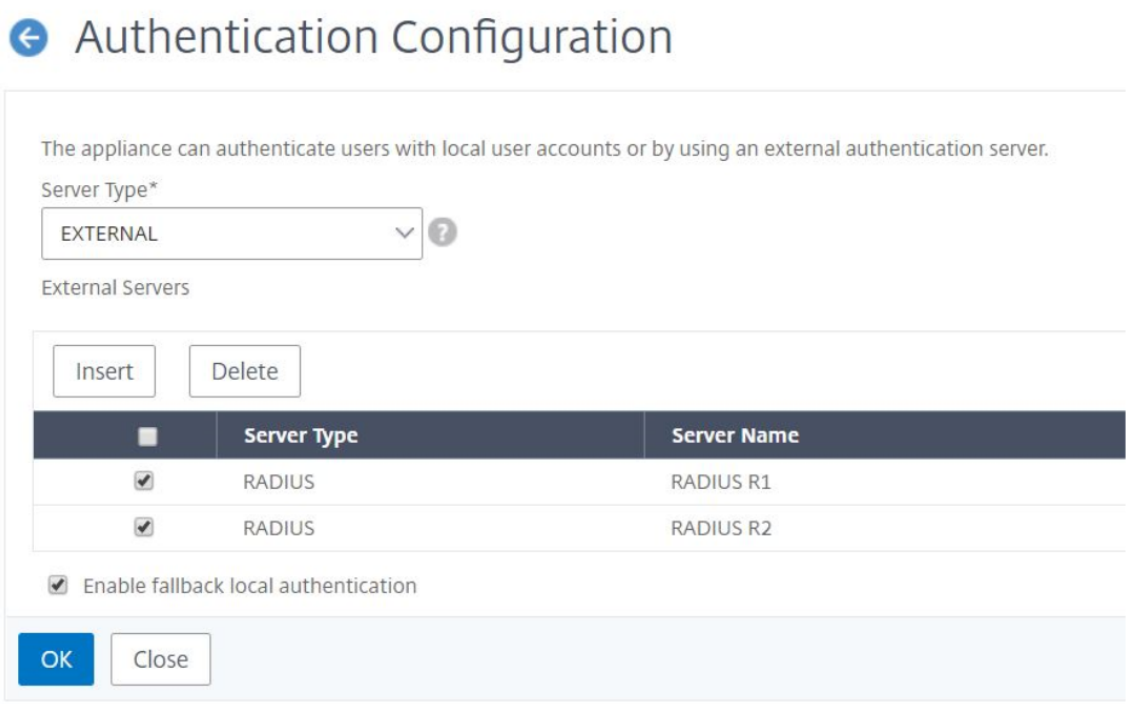
- Connectez-vous au premier serveur RADIUS
- Connectez-vous au deuxième serveur RADIUS, si l'authentification a échoué avec le premier serveur RADIUS
- Connectez-vous au serveur LDAP, si l'authentification a échoué avec les deux serveurs RADIUS
- Connectez-vous au serveur TACACS, si l'authentification a échoué à la fois avec les serveurs RADIUS et le serveur LDAP.

> Remarque
>
> Vous pouvez configurer jusqu'à 32 serveurs d'authentification externes dans Citrix ADM.

Configurer des serveurs externes de secours et en cascade

1. Accédez à **Système** > **Authentification**.
2. Sur la page **Authentification**, cliquez sur **Paramètres**
3. Sur la page **Configuration de l'authentification**, sélectionnez **EXTERNE** dans la liste des **types de serveurs** (seuls les serveurs externes peuvent être mis en cascade).
4. Cliquez sur **Insérer**et, sur la page **Serveurs externes**, sélectionnez un ou plusieurs serveurs d'authentification à mettre en cascade.
5. Cochez la case **Activer l'authentification locale de secours** si vous souhaitez que l'authentification locale prenne le relais en cas d'échec de l'authentification externe.
6. Cochez la case **Enregistrer les informations du groupe externe** si vous souhaitez capturer les informations du groupe d'utilisateurs externes dans le journal d'audit du système.
7. Cliquez sur **OK** pour fermer la page.

   Les serveurs sélectionnés sont affichés sous Serveurs externes :



Vous pouvez également spécifier l'ordre d'authentification à l'aide de l'icône située en regard des noms de serveur pour déplacer les serveurs vers le haut ou vers le bas de la liste.

Contrôle d'accès

February 1, 2024

L'authentification est un processus par lequel vous vérifiez que quelqu'un est ce qu'il prétend être. Pour effectuer l'authentification, un utilisateur doit déjà avoir un compte créé dans un système qui peut être interrogé par le mécanisme d'authentification, ou un compte doit être créé dans le cadre du processus de la première authentification. Citrix Application Delivery Management (ADM) fournit une méthode d'authentification à la fois des utilisateurs locaux et des utilisateurs externes. Tandis que les utilisateurs locaux sont authentifiés en interne, Citrix ADM prend en charge l'authentification externe avec les protocoles RADIUS, LDAP et TACACS. Lorsqu'un utilisateur tente d'accéder à Citrix ADM configuré pour l'authentification externe, le serveur d'applications demandé envoie le nom d'utilisateur et le mot de passe au serveur RADIUS, LDAP ou TACACS pour l'authentification. Une fois authentifié, le protocole requis est utilisé pour identifier l'utilisateur sur Citrix ADM.

Le contrôle d'accès est le processus d'application de la sécurité requise pour une ressource particulière. Il s'agit d'une technique de sécurité qui peut être utilisée pour réglementer qui peut consulter ou utiliser des ressources dans un environnement informatique. Le but du contrôle d'accès est de limiter les actions ou les opérations qu'un utilisateur légitime d'un système informatique peut effectuer.

Le contrôle d'accès limite ce qu'un utilisateur peut faire directement et quels programmes exécutés pour le compte des utilisateurs sont autorisés à faire. De cette façon, le contrôle d'accès vise à prévenir toute activité susceptible d'entraîner une violation de la sécurité. Le contrôle d'accès suppose que l'authentification de l'utilisateur a été vérifiée avec succès avant l'application du contrôle d'accès via un moniteur de référence. Citrix ADM permet un contrôle d'accès basé sur les rôles (RBAC), qui permet aux administrateurs de fournir des autorisations d'accès aux utilisateurs en fonction des rôles des utilisateurs individuels au sein d'une entreprise. Le RBAC dans Citrix ADM est réalisé en créant des stratégies d'accès, des rôles, des groupes et des utilisateurs.

Contrôle d'accès sur rôle

February 1, 2024

Citrix ADM fournit un contrôle d'accès basé sur les rôles (RBAC), avec lequel vous pouvez accorder des autorisations d'accès en fonction des rôles des utilisateurs individuels au sein de votre entreprise. Dans ce contexte, l'accès est la possibilité d'effectuer une tâche spécifique, telle que l'affichage, la création, la modification ou la suppression d'un fichier. Les rôles sont définis en fonction de l'autorité et de la responsabilité des utilisateurs au sein de l'entreprise. Par exemple, un utilisateur peut être autorisé à effectuer toutes les opérations réseau, tandis qu'un autre utilisateur peut observer le flux de trafic dans les applications et aider à créer des modèles de configuration.

Les rôles sont déterminés par dans les stratégies. Après avoir créé des stratégies, vous créez des rôles, vous liez chaque rôle à une ou plusieurs stratégies et vous attribuez des rôles aux utilisateurs. Vous pouvez également affecter des rôles à des groupes d'utilisateurs.

Un groupe est un ensemble d'utilisateurs qui ont des autorisations communes. Par exemple, les utilisateurs qui gèrent un centre de données particulier peuvent être affectés à un groupe. Un rôle est une identité accordée à des utilisateurs ou à des groupes en fonction de conditions spécifiques. Dans Citrix ADM, la création de rôles et de stratégies est spécifique à la fonctionnalité RBAC dans Citrix ADC. Les rôles et les stratégies peuvent être facilement créés, modifiés ou supprimés au fur et à mesure que les besoins de l'entreprise évoluent, sans avoir à mettre à jour individuellement les privilèges de chaque utilisateur.

Les rôles peuvent être basés sur des fonctionnalités ou des ressources. Par exemple, pensez à un administrateur SSL/sécurité et à un administrateur d'application. Un administrateur SSL/Security doit avoir un accès complet aux fonctionnalités de gestion et de surveillance des certificats SSL, mais doit avoir un accès en lecture seule pour les opérations d'administration système. Un administrateur d'application doit pouvoir accéder uniquement aux ressources de la portée.

Exemple :

Chris, le chef de groupe ADC, est le super administrateur de Citrix ADM dans son organisation. Chris crée trois rôles d'administrateur : administrateur de sécurité, administrateur d'application et administrateur réseau.

David, l'administrateur de la sécurité, doit disposer d'un accès complet pour la gestion et la surveillance des certificats SSL, mais aussi avoir un accès en lecture seule pour les opérations d'administration système.

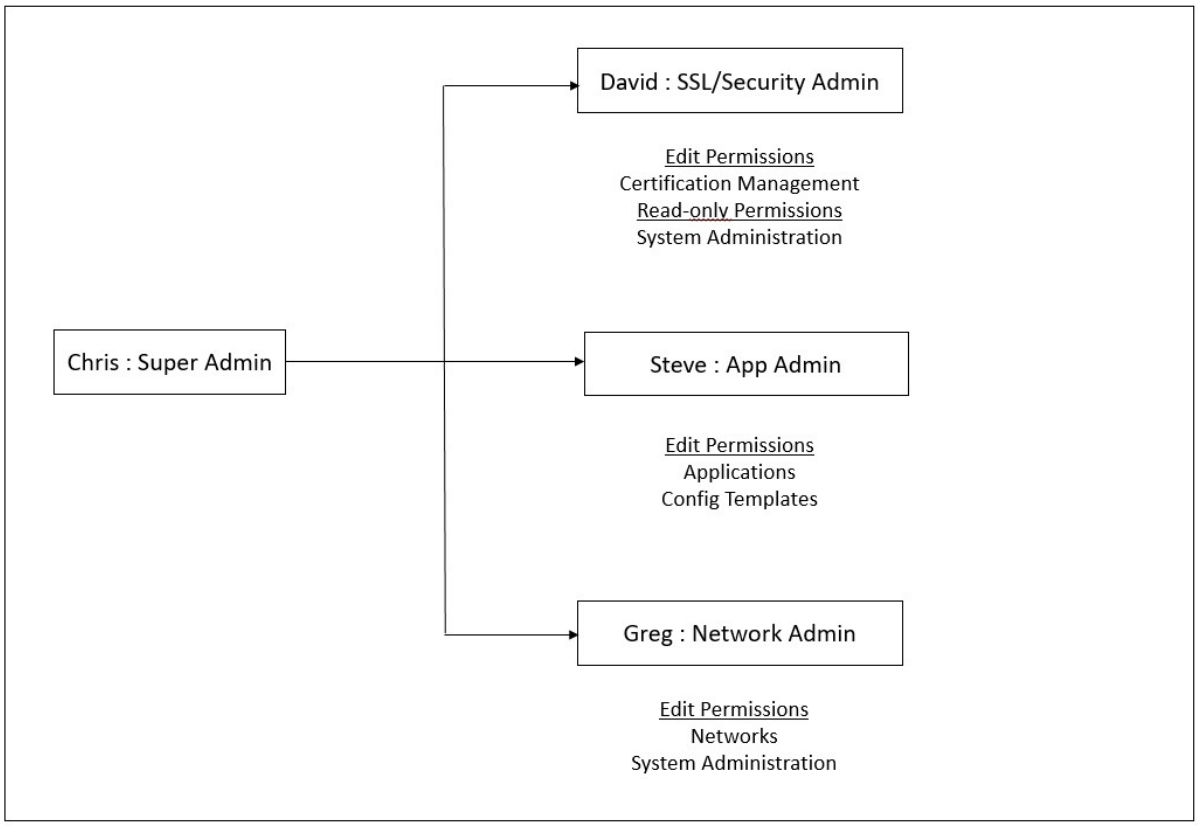
Steve, administrateur d'applications, a besoin d'accéder uniquement à des applications spécifiques et uniquement à des modèles de configuration spécifiques.

Greg, administrateur réseau, a besoin d'un accès à l'administration du système et du réseau.

Chris doit également fournir RBAC à tous les utilisateurs, indépendamment du fait qu'ils soient locaux ou externes.

Les utilisateurs Citrix ADM peuvent être authentifiés localement ou authentifiés via un serveur externe (RADIUS/LDAP/TACACS). Les paramètres RBAC doivent être applicables à tous les utilisateurs, quelle que soit la méthode d'authentification adoptée.

L'image suivante montre les autorisations dont disposent les administrateurs et les autres utilisateurs et leurs rôles dans l'organisation.



Limitations

RBAC n'est pas entièrement pris en charge pour les fonctionnalités Citrix ADM suivantes :

- **Analytics** - RBAC n'est pas entièrement pris en charge dans les modules d'analyse. La prise en charge du RBAC est limitée au niveau de l'instance et ne s'applique pas au niveau de l'application dans les modules d'analyse Web Insight, SSL Insight, Gateway Insight, HDX Insight et Security Insight. Par exemple :

Exemple 1 : RBAC basé sur une instance (pris en charge)

Un administrateur auquel quelques instances ont été attribuées ne peut voir que ces instances sous **Web Insight** > **Instances**, et uniquement les serveurs virtuels correspondants sous **Web Insight** > **Applications**, car le RBAC est pris en charge au niveau de l'instance.

Exemple 2 : RBAC basé sur l'application (non pris en charge)

Un administrateur auquel quelques applications ont été attribuées peut voir tous les serveurs virtuels sous **Web Insight** > **Applications**, mais ne peut pas y accéder, car le RBAC n'est pas pris en charge au niveau des applications.

- **StyleBooks** : le RBAC n'est pas entièrement pris en charge pour StyleBooks.
  - Dans Citrix ADM, les StyleBooks et les packs de configuration sont considérés comme des ressources distinctes. Les autorisations d'accès (affichage, modification ou les deux) peuvent être fournies séparément ou simultanément pour StyleBook et les packs de configuration. Une autorisation d'affichage ou de modification sur les packs de configuration permet implicitement à l'utilisateur d'afficher les StyleBooks, ce qui est essentiel pour obtenir les détails du pack de configuration et créer des packs de configuration.
  - L'autorisation d'accès pour StyleBook ou packs de configuration spécifiques n'est pas prise en charge
    Exemple : S'il existe déjà un pack de configuration sur l'instance, les utilisateurs peuvent modifier la configuration sur une instance Citrix ADC cible même s'ils n'ont pas accès à cette instance.
- **Orchestration** - RBAC n'est pas pris en charge pour Orchestration.

Configurer les stratégies d'accès

February 1, 2024

Les stratégies d'accès définissent les autorisations. Une stratégie peut être appliquée à un seul utilisateur ou groupe, ou à plusieurs utilisateurs et plusieurs groupes. Citrix Application Delivery Management (ADM) fournit quatre stratégies d'accès prédéfinies :

1. **adminpolicy**. Autorise l'accès à toutes les fonctionnalités de Citrix ADM. L'utilisateur dispose d'autorisations d'affichage et de modification, peut afficher tout le contenu Citrix ADM et peut effectuer toutes les opérations de modification. Autrement dit, l'utilisateur peut effectuer des opérations d'ajout, de modification et de suppression sur les ressources.
2. **readonlypolicy**. Octroie des autorisations en lecture seule. L'utilisateur peut afficher tout le contenu sur Citrix ADM, mais n'est autorisé à effectuer aucune opération.
3. **appAdminPolicy**. Octroie des autorisations d'administration pour accéder aux fonctionnalités de l'application dans Citrix ADM. Un utilisateur lié à cette stratégie peut ajouter, modifier et supprimer des applications personnalisées et activer ou désactiver les services, les groupes de services et les différents serveurs virtuels, tels que la commutation de contenu, la redirection de cache et les serveurs virtuels HAProxy.
4. **appReadOnlyPolicy**. Octroie une autorisation en lecture seule pour les fonctionnalités de l'application. Un utilisateur lié à cette stratégie peut afficher les applications, mais ne peut pas effectuer d'opérations d'ajout, de modification, de suppression, d'activation ou de désactivation.

> **Remarque** Les stratégies prédéfinies ne peuvent pas être modifiées.

Vous pouvez également créer vos propres stratégies (définies par l'utilisateur).

Pour créer des stratégies d'accès définies par l'utilisateur :

1. Dans Citrix ADM, accédez à **Système** > **Administration des utilisateurs** > **Stratégies d'accès**.
2. Cliquez sur **Ajouter**.
3. Dans le champ **Nom de la stratégie**, entrez le nom de la stratégie et entrez la description dans le champ **Description de la stratégie** .

   La section **Autorisations** répertorie toutes les fonctionnalités Citrix ADM, avec des options permettant de spécifier l'accès en lecture seule, l'activation/désactivation ou la modification.
4. Cliquez sur l'icône (+) pour développer chaque groupe d'entités en plusieurs entités.

   a) Cochez la case d'autorisation à côté du nom de la fonctionnalité pour accorder des autorisations aux utilisateurs.

   - **Afficher :** Cette option permet à l'utilisateur de visualiser la fonctionnalité dans Citrix ADM.

- **Activer/Désactiver :** cette option est disponible uniquement pour les fonctionnalités **Network Functions** qui permettent d'activer ou de désactiver des actions sur Citrix ADM. L'utilisateur peut activer ou désactiver la fonctionnalité. Et l'utilisateur peut également effectuer l'action **Poll Now** .

  Lorsque vous accordez l'autorisation **Activer-Désactiver** à un utilisateur, l'autorisation **Afficher** est également accordée. Vous ne pouvez pas désélectionner cette option.

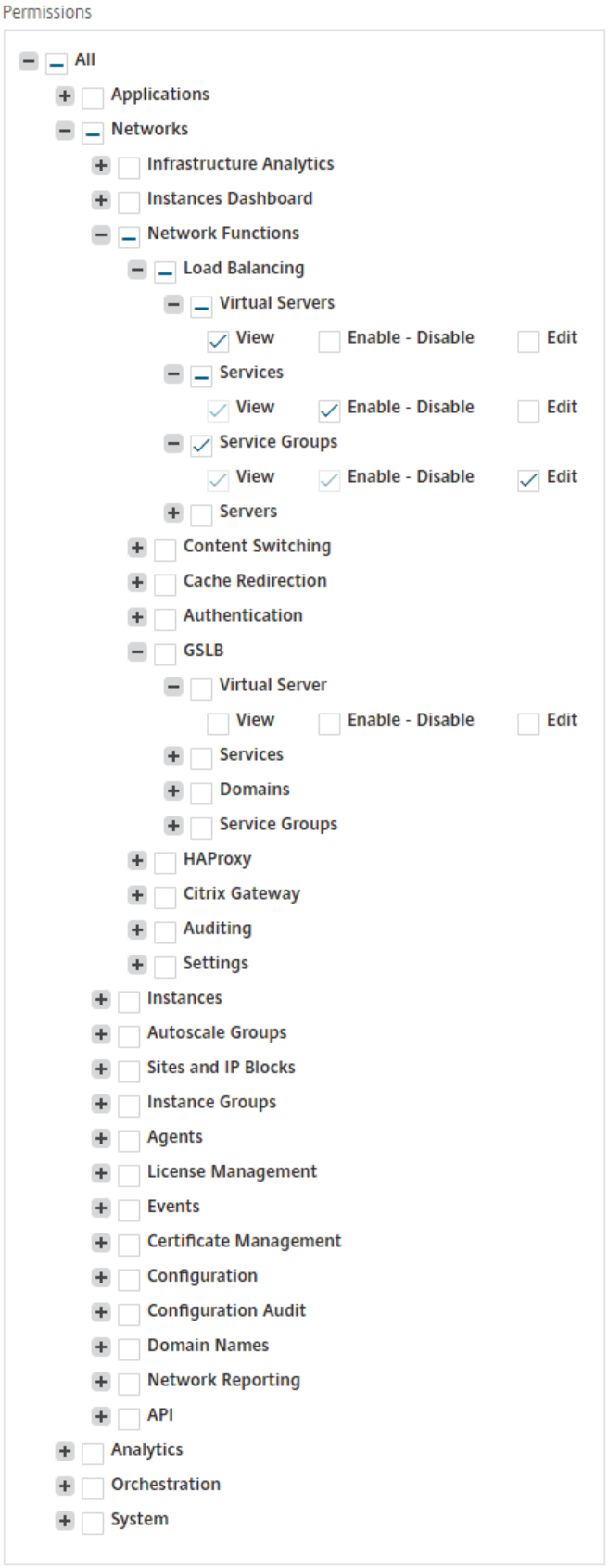
- **Modifier :** Cette option accorde l'accès complet à l'utilisateur. L'utilisateur peut modifier la fonction et ses fonctions.

  Si vous accordez l'autorisation de **modification**, les autorisations **Afficher** et **Activer/Désactiver** sont accordées. Vous ne pouvez pas désélectionner les options sélectionnées automatiquement.

Si vous cochez la case de la fonctionnalité, toutes les autorisations associées à la fonctionnalité sont sélectionnées.

> **Remarque**
>
> Développez Load Balancing et GSLB pour afficher d'autres options de configuration.

Dans l'image suivante, les options de configuration de la fonction d'équilibrage de charge ont des autorisations différentes :



L'autorisation **Afficher** est accordée à un utilisateur pour la fonctionnalité **Serveurs virtuels**. L'utilisateur peut afficher les serveurs virtuels d'équilibrage de charge dans Citrix ADM. Pour afficher les serveurs virtuels, accédez à **Réseaux** > **Fonctions réseau** > **Équilibrage de charge** et sélectionnez l'onglet **Serveurs virtuels** .

L'autorisation **Enable-Disable** est accordée à un utilisateur pour la fonctionnalité **Services** . Cette autorisation accorde également l'autorisation d'**affichage** . L'utilisateur peut activer ou désactiver les services liés à un serveur virtuel d'équilibrage de charge. En outre, l'utilisateur peut effectuer l'action **Poll Now** sur les services. Pour activer ou désactiver des services, accédez à **Réseaux** > **Fonctions réseau** > **Équilibrage de charge** et sélectionnez l'onglet **Services**.

> **Remarque**
>
> Si un utilisateur dispose de l'autorisation **Enable-Disable**, l'action d'activation ou de désactivation sur un service est restreinte dans la page suivante :
>
> a) Accédez à **Réseaux** > **Fonctions du réseau**.
>
> b) Sélectionnez un serveur virtuel et cliquez sur **Configurer**.
>
> c) Sélectionnez la page **Load Balancing Virtual Server Service Binding** .
> Cette page affiche un message d'erreur si vous sélectionnez **Activer** ou **Désactiver**.

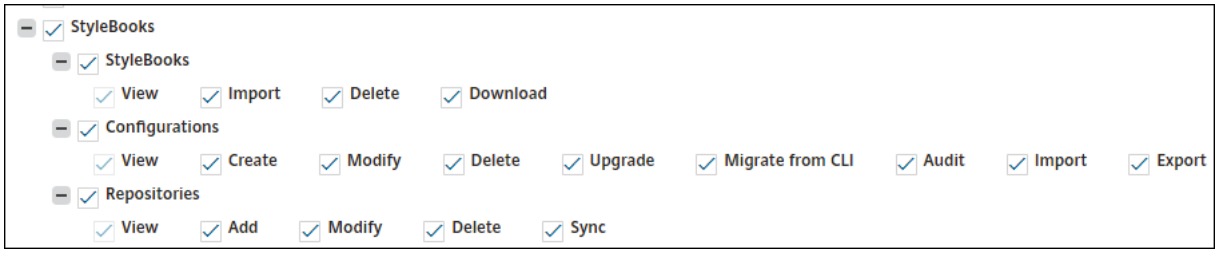
L'autorisation de **modification** est accordée à un utilisateur pour la fonctionnalité **Groupes de services** . Cette autorisation accorde l'accès complet lorsque les autorisations **Afficher** et **Activer/Désactiver** sont accordées. L'utilisateur peut modifier les groupes de services liés à un serveur virtuel d'équilibrage de charge. Pour modifier des groupes de services, accédez à **Réseaux** > **Fonctions réseau** > **Équilibrage de charge** et sélectionnez l'onglet **Groupes de services** .

5. Cliquez sur **Créer**.

Accorder des autorisations StyleBook aux utilisateurs

Vous pouvez créer une stratégie d'accès pour accorder des autorisations StyleBook telles que l'importation, la suppression, le téléchargement, etc.

> **Remarque**
>
> L'autorisation Afficher est automatiquement activée lorsque vous accordez d'autres autorisations StyleBook.



Configurer les groupes

February 1, 2024

Dans Citrix ADM, un groupe peut avoir un accès au niveau des fonctionnalités et des ressources. Par exemple, un groupe d'utilisateurs peut avoir accès uniquement à certaines instances Citrix ADC ; un autre groupe ne disposant que de quelques applications sélectionnées, etc.

Lorsque vous créez un groupe, vous pouvez attribuer des rôles au groupe, fournir un accès au groupe au niveau de l'application et affecter des utilisateurs au groupe. Tous les utilisateurs de ce groupe se voient attribuer les mêmes droits d'accès dans Citrix ADM.

Vous pouvez gérer l'accès d'un utilisateur dans Citrix ADM au niveau individuel des entités de fonction réseau. Vous pouvez attribuer dynamiquement des autorisations spécifiques à l'utilisateur ou au groupe au niveau de l'entité.

Citrix ADM traite les serveurs virtuels, les services, les groupes de services et les serveurs en tant qu'entités de fonction réseau.

- **Serveur virtuel (applications)** : équilibrage de charge (lb), GSLB, commutation de contexte (CS), redirection de cache (CR), authentification (`Auth`) et Citrix Gateway (VPN)
- **Services** - Équilibrage de charge et services GSLB
- **Groupe de services** : équilibrage de charge et groupes de services GSLB
- **Serveurs - Serveurs** d'équilibrage de charge

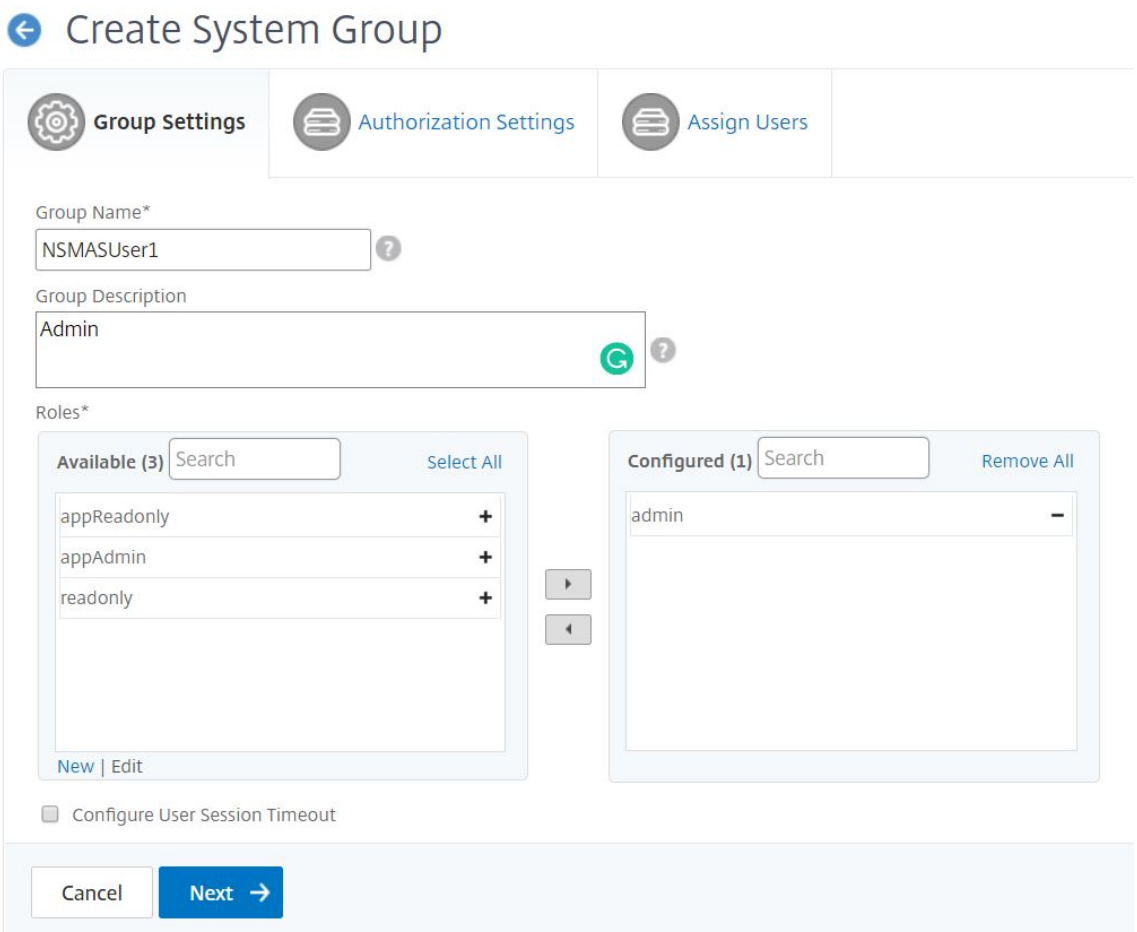
Créer un groupe d'utilisateurs

1. Dans Citrix ADM, accédez à **Système** > **Administration des utilisateurs** > **Groupes**.
2. Cliquez sur **Ajouter**.

   La page **Créer un groupe de systèmes** s'affiche.
3. Dans le champ **Nom du groupe**, entrez le nom du groupe.

4. Dans le champ **Description du groupe**, saisissez une description de votre groupe. Fournir une bonne description du groupe vous aide à mieux comprendre le rôle et la fonction du groupe ultérieurement.
5. Dans la section **Rôles**, ajoutez ou déplacez un ou plusieurs rôles dans la liste **Configuré**.

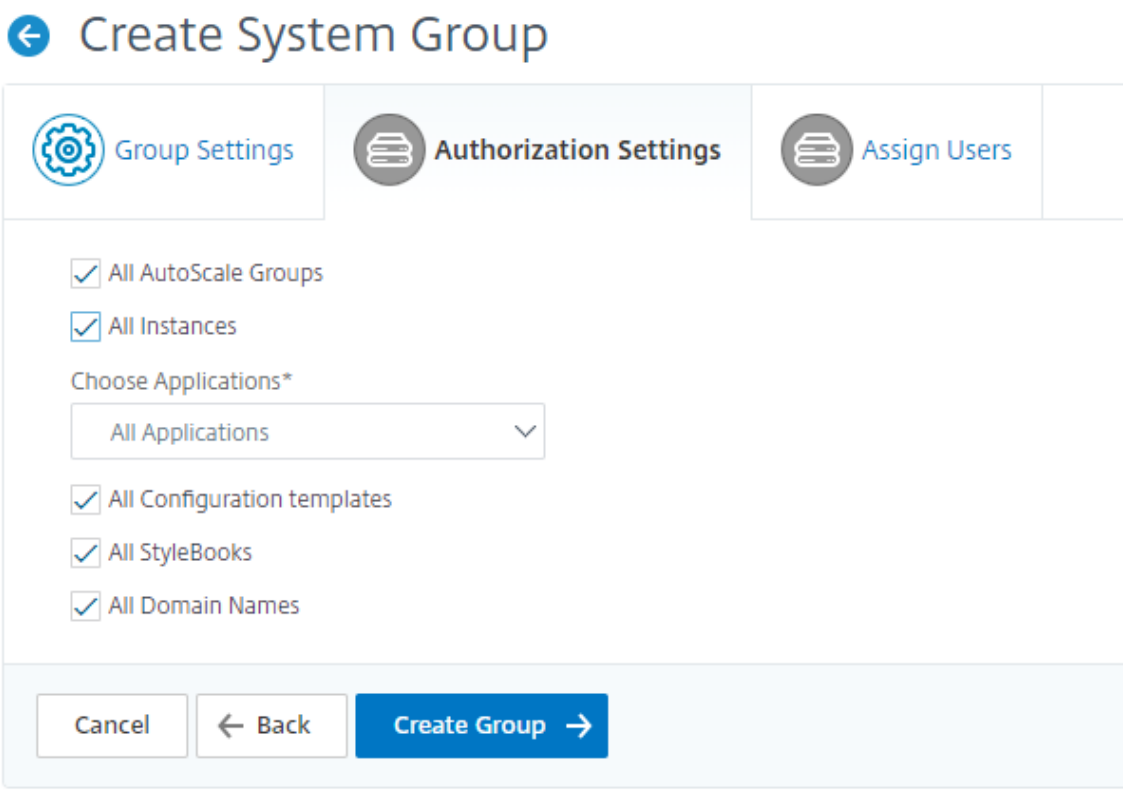
> **Remarque**
> Dans la liste **Disponible**, vous pouvez cliquer sur **Nouveau** ou **Modifier** et créer ou modifier des rôles. Vous pouvez également accéder à **Système** > **Administration** des **utilisateurs** > **Utilisateurs** et créer ou modifier des utilisateurs.



6. Cliquez sur **Suivant**. Dans l'onglet **Paramètres d'autorisation**, vous pouvez définir les paramètres d'autorisation pour les ressources suivantes :

   - Groupes de mise à l'échelle automatique
   - Instances
   - Applications
   - Modèles de configuration
   - StyleBooks

- Configpacks
- Noms de domaine



Vous pouvez sélectionner des ressources spécifiques parmi les catégories auxquelles les utilisateurs peuvent accéder.

Groupes de mise à l'échelle automatique :

Si vous souhaitez sélectionner les groupes Autoscale spécifiques qu'un utilisateur peut afficher ou gérer, effectuez les étapes suivantes :

a) Désactivez la case à cocher **Tous les groupes d'échelle automatique** et cliquez sur **Ajouter des groupes d'échelle automatique**.

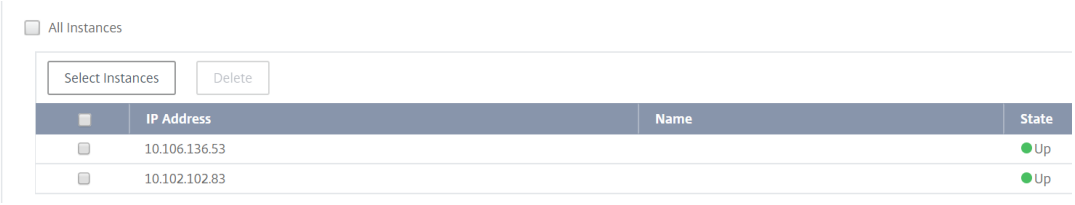
b) Sélectionnez les groupes Autoscale requis dans la liste et cliquez sur **OK**.

Instances :

Si vous souhaitez sélectionner les instances spécifiques qu'un utilisateur peut consulter ou gérer, effectuez les étapes suivantes :

a) Décochez la case **Toutes les instances** et cliquez sur **Sélectionner les instances**.

b) Sélectionnez les instances requises dans la liste et cliquez sur **OK**.



Applications :

La liste **Choisir les applications** vous permet d'accorder l'accès à un utilisateur pour les applications requises.

Vous pouvez accorder l'accès aux applications sans sélectionner leurs instances. Parce que les applications sont indépendantes de leurs instances pour accorder l'accès aux utilisateurs.

Lorsque vous accordez à un utilisateur l'accès à une application, l'utilisateur est autorisé à accéder uniquement à cette application, quelle que soit la sélection de l'instance.

Cette liste propose les options suivantes :

- **Toutes les applications :** cette option est sélectionnée par défaut. Il ajoute toutes les applications présentes dans Citrix ADM.
- **Toutes les applications des instances sélectionnées :** cette option s'affiche uniquement si vous sélectionnez des instances dans la catégorie **Toutes les instances** . Il ajoute toutes les applications présentes sur l'instance sélectionnée.
- **Applications spécifiques :** Cette option vous permet d'ajouter les applications requises auxquelles vous souhaitez que les utilisateurs puissent accéder. Cliquez sur **Ajouter des applications** et sélectionnez les applications requises dans la liste.
- **Sélectionner un type d'entité individuel :** Cette option vous permet de sélectionner un type spécifique d'entité fonctionnelle réseau et les entités correspondantes.

  Vous pouvez ajouter des entités individuelles ou sélectionner toutes les entités sous le type d'entité requis pour accorder l'accès à un utilisateur.

  L'option **Appliquer aux entités liées autorise également** les entités liées au type d'entité sélectionné. Par exemple, si vous sélectionnez une application et que vous sélectionnez **également Appliquer aux entités liées**, Citrix ADM autorise toutes les entités liées à l'application sélectionnée.

  > **Remarque**
  >
  > Assurez-vous d'avoir sélectionné un seul type d'entité si vous souhaitez autoriser les entités liées.

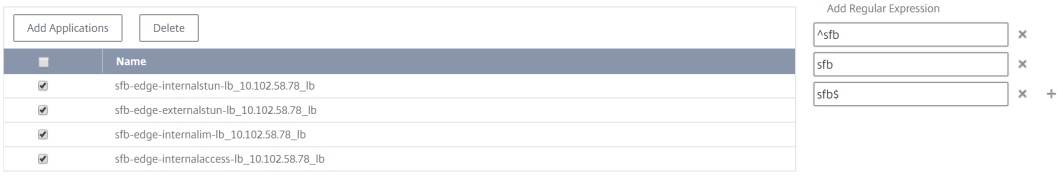
Vous pouvez utiliser des expressions régulières pour rechercher et ajouter les entités de fonction réseau qui répondent aux critères d'expression régulière des groupes. L'expression regex

spécifiée est conservée dans Citrix ADM. Pour ajouter une expression régulière, effectuez les opérations suivantes :

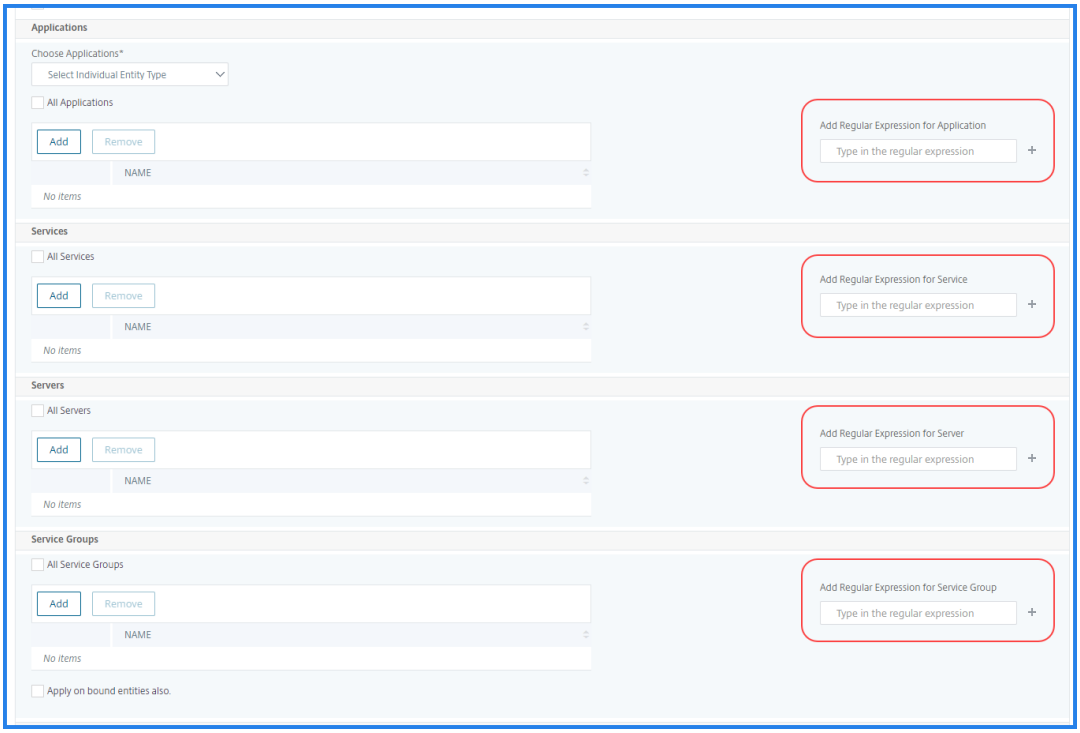
a) Cliquez sur **Ajouter une expression régulière**.

b) Spécifiez l'expression régulière dans la zone de texte.

L'image suivante explique comment utiliser l'expression régulière pour ajouter une application lorsque vous sélectionnez l'option **Applications spécifiques** :



L'image suivante explique comment utiliser l'expression régulière pour ajouter des entités de fonction réseau lorsque vous choisissez l'option **Sélectionner le type d'entité individuelle** :



Si vous souhaitez ajouter d'autres expressions régulières, cliquez sur l'icône **+** .

> **Remarque :**
>
> L'expression régulière correspond uniquement au nom du serveur pour le type d'entité **Servers** et non à l'adresse IP du serveur.

Si vous sélectionnez l'option **Appliquer également aux entités liées** pour une entité découverte, un utilisateur peut accéder automatiquement aux entités liées à l'entité découverte.

L'expression régulière est stockée dans le système pour mettre à jour la portée de l'autorisation. Lorsque les nouvelles entités correspondent à l'expression régulière de leur type d'entité, Citrix ADM met à jour l'étendue d'autorisation pour les nouvelles entités.

Modèles de configuration :

Si vous souhaitez sélectionner le modèle de configuration spécifique qu'un utilisateur peut consulter ou gérer, effectuez les étapes suivantes :

a) Décochez la case **Tous les modèles de configuration** et cliquez sur **Ajouter un modèle de configuration**.

b) Sélectionnez le modèle requis dans la liste et cliquez sur **OK**.

StyleBooks:

Si vous souhaitez sélectionner le StyleBook spécifique qu'un utilisateur peut consulter ou gérer, effectuez les opérations suivantes :

a) Désactivez la case à cocher **Tous les StyleBooks** et cliquez sur **Ajouter un StyleBook au groupe**. Vous pouvez sélectionner des StyleBooks individuels ou spécifier une requête de filtre pour autoriser les StyleBooks.

Si vous souhaitez sélectionner les StyleBooks individuels, sélectionnez les StyleBooks dans le volet **StyleBooks individuels** et cliquez sur **Enregistrer la sélection**.

Si vous souhaitez utiliser une requête pour rechercher dans StyleBooks, sélectionnez le volet **Filtres personnalisés** . Une requête est une chaîne de paires clé-valeur où les clés sont `name`, `namespace` et `version`.

Vous pouvez également utiliser des expressions régulières comme valeurs pour rechercher et ajouter des StyleBooks répondant aux critères de regex pour les groupes. Une requête de filtre personnalisée pour rechercher StyleBooks prend en charge les opérateurs `And` et `Or`.

Exemple :

```
1 name=lb-mon|lb AND namespace=com.citrix.adc.stylebooks AND
     version=1.0
2 <!--NeedCopy-->
```

Cette requête répertorie les StyleBooks qui remplissent les conditions suivantes :

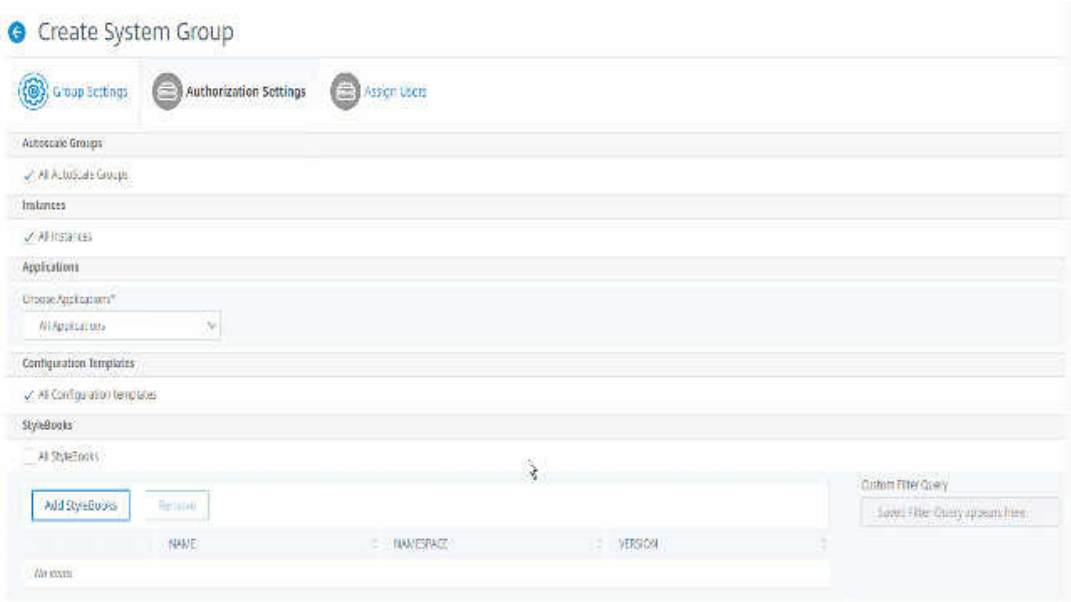
- Le nom de StyleBook est `lb-mon` ou `lb`.
- L'espace de noms StyleBook est `com.citrix.adc.stylebooks`.
- La version StyleBook est `1.0`.

Utilisez un opérateur `Or` entre des expressions de valeur définie à l'expression clé.

Exemple :

- La requête `name=lb-mon | lb` est valide. Il renvoie les StyleBooks ayant un nom `lb-mon` ou `lb`.
- La requête `name=lb-mon | version=1.0` n'est pas valide.

Appuyez sur `Enter` pour afficher les résultats de la recherche et cliquez sur **Enregistrer la requête**.



La requête enregistrée apparaît dans la **requête Filtres personnalisés**. En fonction de la requête enregistrée, l'ADM fournit aux utilisateurs l'accès à ces livres StyleBooks.

b) Sélectionnez les StyleBooks requis dans la liste et cliquez sur **OK**.

Vous pouvez sélectionner les StyleBooks requis lorsque vous créez des groupes et ajoutez des utilisateurs à ce groupe. Lorsque votre utilisateur sélectionne le StyleBook autorisé, tous les StyleBooks dépendants sont également sélectionnés.

Configpacks :

Dans **Configpacks**, sélectionnez l'une des options suivantes :

- **Toutes les configurations** : Cette option est sélectionnée par défaut. Il ajoute tous les packs de configuration qui sont dans ADM.
- **Toutes les configurations des StyleBooks sélectionnés** : Cette option ajoute tous les packs de configuration du StyleBook sélectionné.
- **Configurations spécifiques** : Cette option vous permet d'ajouter les packs de configuration requis.

  Vous pouvez sélectionner les packs de configuration requis lorsque vous créez des groupes et ajoutez des utilisateurs à ce groupe.

Noms de domaine :

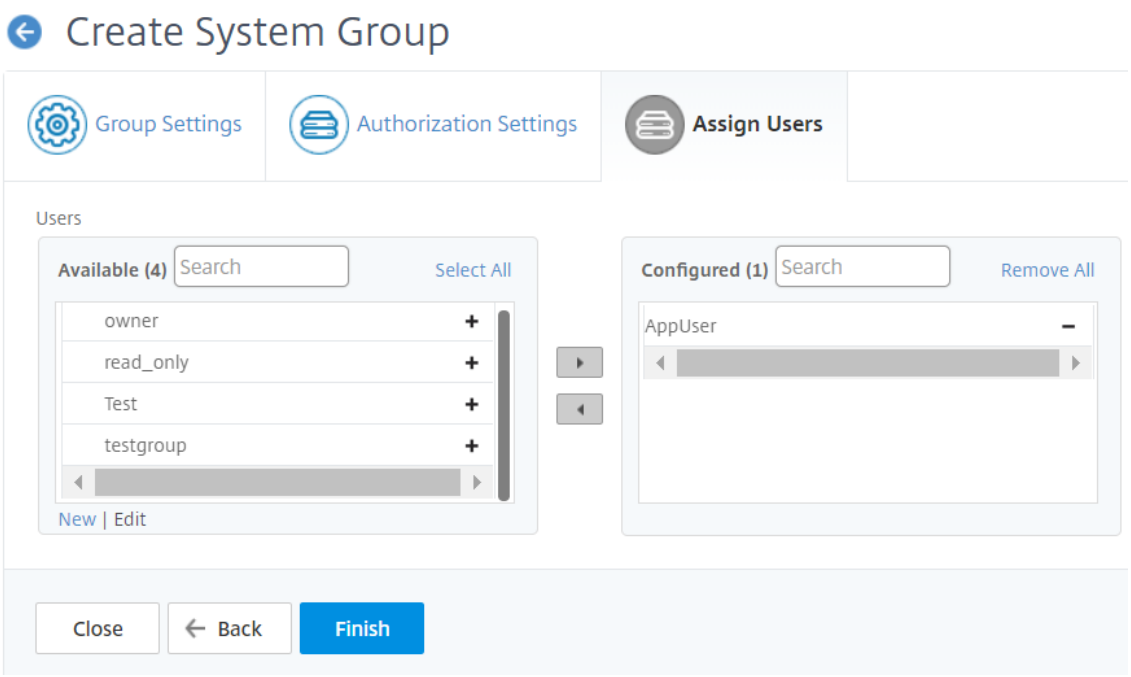
Si vous souhaitez sélectionner le nom de domaine spécifique qu'un utilisateur peut consulter ou gérer, procédez comme suit :

a) Décochez la case **Tous les noms de domaine** et cliquez sur **Ajouter un nom de domaine**.

b) Sélectionnez les noms de domaine requis dans la liste et cliquez sur **OK**.

7. Cliquez sur **Créer un groupe**.
8. Dans la section **Affecter des utilisateurs**, sélectionnez l'utilisateur dans la liste **Disponible** et ajoutez-le à la liste des utilisateurs **configurés** .

> **Remarque**
>
> Vous pouvez également ajouter des utilisateurs en cliquant sur **Nouveau**.



9. Cliquez sur **Terminer**.

Gérer l'accès utilisateur sur plusieurs entités de fonction réseau

En tant qu'administrateur, vous pouvez gérer l'accès des utilisateurs au niveau individuel des entités de fonction réseau dans Citrix ADM. De plus, vous pouvez attribuer dynamiquement des autorisations spécifiques à l'utilisateur ou à un groupe au niveau de l'entité à l'aide du filtre d'expression régulière.

Ce document explique comment définir l'autorisation utilisateur au niveau de l'entité.

Avant de commencer, créez un groupe. Consultez Configurer des groupes sur Citrix ADM pour plus d'informations.

Scénario d'utilisation :

Imaginons un scénario dans lequel une ou plusieurs applications (serveurs virtuels) sont hébergées sur le même serveur. Un super administrateur (George) souhaite accorder à Steve (un administrateur d'applications) l'accès uniquement à App1 et non au serveur d'hébergement.

Le tableau suivant illustre cet environnement, dans lequel Server-A héberge les applications App-1 et App-2.

Serveur hôte	Application (serveur virtuel)	Service	Groupe de services
Serveur A	App1	App-service-1	App-service-group-1
Serveur A	App2	App-service-2	App-service-group-2

> **Remarque**
>
> Citrix ADM traite le serveur virtuel, les services, les groupes de services et les serveurs comme des entités de fonction réseau. Le serveur virtuel de type d'entité est appelé une application.

Pour attribuer des autorisations utilisateur à des entités fonctionnelles du réseau, George définit les autorisations utilisateur comme suit :

1. Accédez à **Compte > Administration des utilisateurs > Groupes** et ajoutez un groupe.
2. Dans l'onglet **Paramètres d'autorisation**, sélectionnez Choisir les applications.
3. Choisissez **Sélectionner un type d'entité individuel**.
4. Sélectionnez le type **d'entité Toutes les applications** et ajoutez l'entité App-1 dans la liste disponible.
5. Cliquez sur **Créer un groupe**.
6. Dans **Attribuer des utilisateurs**, sélectionnez les utilisateurs qui ont besoin de l'autorisation. Pour ce scénario, George sélectionne le profil utilisateur de Steve.
7. Cliquez sur **Terminer**.

Avec ce paramètre d'autorisation, Steve ne peut gérer que l'App-1 et aucune autre entité fonctionnelle réseau.

> **Remarque**
>
> Assurez-vous que l'option **Appliquer aux entités liées est également** désactivée. Sinon, Citrix ADM accorde l'accès à toutes les entités de fonction réseau liées à App-1. En conséquence, accorde également l'accès au serveur d'hébergement.

Un super administrateur peut spécifier les expressions régulières (regex) pour chaque type d'entité. L'expression régulière est stockée dans le système pour mettre à jour l'étendue d'autorisation utilisateur. Lorsque les nouvelles entités correspondent à l'expression régulière de leur type d'entité, Citrix ADM peut autoriser dynamiquement les utilisateurs à accéder à des entités de fonction réseau spécifiques.

Pour accorder des autorisations utilisateur de manière dynamique, le super administrateur peut ajouter des expressions régulières dans l'onglet **Paramètres d'autorisation**.

Dans ce scénario, George ajoute App* en tant qu'expression régulière pour le type d'entité Applications et les applications qui correspondent aux critères d'expression régulière apparaissent dans la liste. Avec ce paramètre d'autorisation, Steve peut accéder à toutes les applications qui correspondent à l'expression régulière App*. Toutefois, son accès est limité uniquement aux applications et non au serveur hébergé.

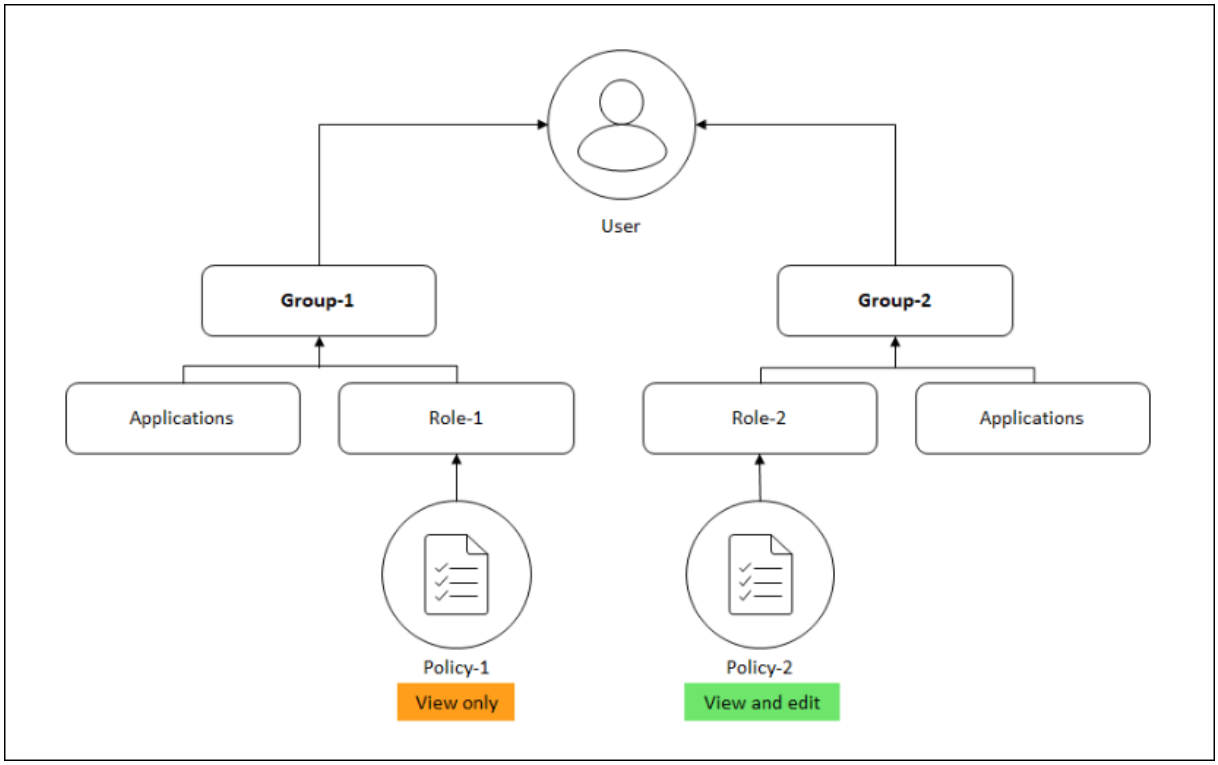
Comment l'accès utilisateur change en fonction de la portée d'autorisation

Lorsqu'un administrateur ajoute un utilisateur à un groupe qui a des paramètres de stratégie d'accès différents, l'utilisateur est mappé à plusieurs étendues d'autorisation et stratégies d'accès.

Dans ce cas, l'ADM accorde à l'utilisateur l'accès aux applications en fonction de l'étendue d'autorisation spécifique.

Considérez un utilisateur qui est affecté à un groupe doté de deux stratégies Stratégie-1 et Stratégie-2.

- **Policy-1** —Affiche uniquement les autorisations pour les applications.
- **Policy-2** —Afficher et modifier l'autorisation des applications.



L'utilisateur peut consulter les applications spécifiées dans Policy-1. En outre, cet utilisateur peut afficher et modifier les applications spécifiées dans la stratégie 2. L'accès à la modification des applications du groupe 1 est restreint car il n'est pas sous la portée de l'autorisation du groupe 1.

Mappage de RBAC lors de la mise à niveau de Citrix ADM de la version 12.0 vers les versions ultérieures

Lorsque vous mettez à niveau Citrix ADM de la version 12.0 à la version 13.0, les options permettant de fournir des autorisations de « lecture-écriture » ou de « lecture » lors de la création de groupes ne s'affichent pas. Ces autorisations ont été remplacées par « rôles et stratégies d'accès », ce qui vous donne plus de flexibilité pour fournir des autorisations basées sur les rôles aux utilisateurs. Le tableau suivant montre comment les autorisations de la version 12.0 sont mappées à celles de la version 13.0 :

12.0	Autoriser les applications uniquement	13.0
admin read-write	False	`admin`
admin read-write	True	`appAdmin`
admin read-only	False	`readonly`
admin read-only	True	`appReadonly`

Configurer les rôles

February 1, 2024

Dans Citrix Application Delivery Management (ADM), chaque rôle est lié à une ou plusieurs stratégies d'accès. Vous pouvez définir des relations un-à-un, un-à-plusieurs et plusieurs vers plusieurs entre les stratégies et les rôles. Vous pouvez lier un rôle à plusieurs stratégies, et vous pouvez lier plusieurs rôles à une seule stratégie.

Par exemple, un rôle peut être lié à deux stratégies, l'une définissant les autorisations d'accès pour une entité et l'autre définissant les autorisations d'accès pour une autre entité. Une stratégie peut autoriser l'ajout d'instances Citrix ADC dans Citrix ADM, tandis que l'autre stratégie peut autoriser la création et le déploiement de StyleBooks et la configuration d'instances Citrix ADC.

Lorsque plusieurs stratégies définissent des autorisations de mise à jour et de lecture seule pour une seule entité, les autorisations de mise à jour ont la priorité.

Citrix ADM fournit quatre rôles prédéfinis :

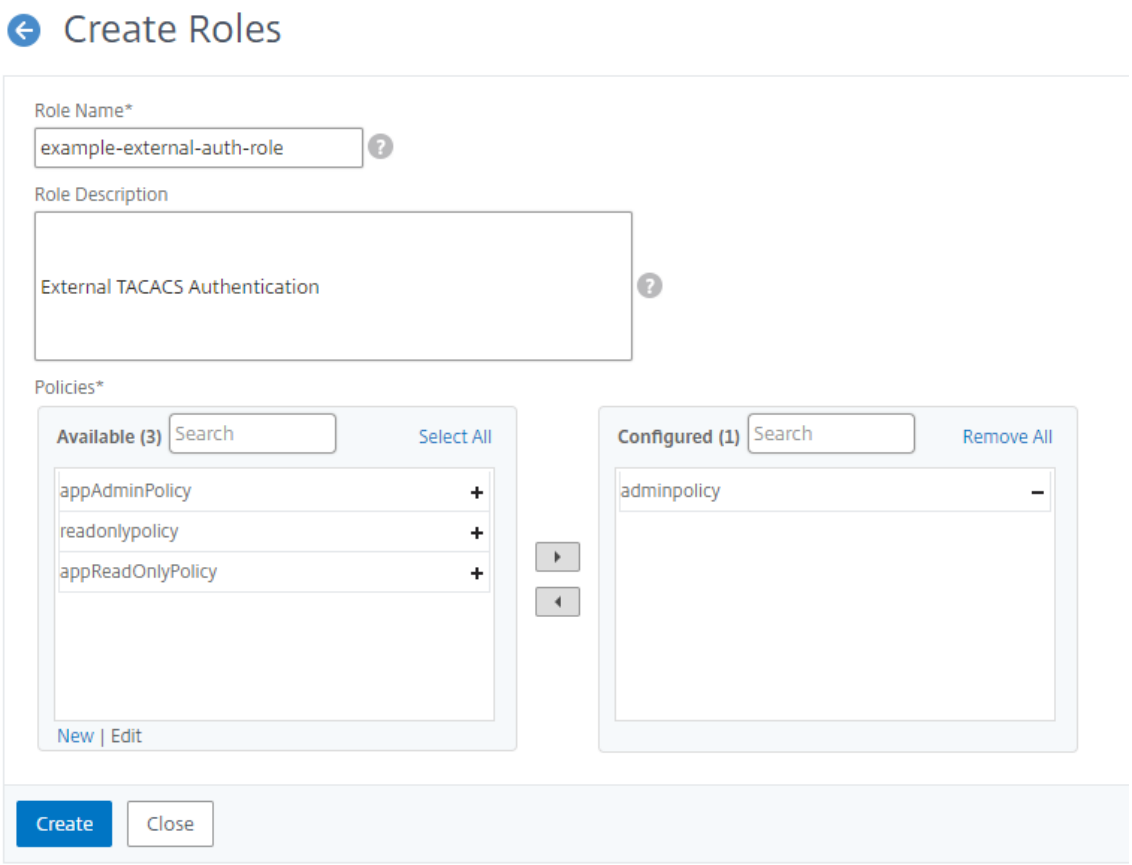
- **admin**. A accès à toutes les fonctionnalités Citrix ADM. (Ce rôle est lié à adminpolicy.)
- **readonly**. Accès en lecture seule. (Ce rôle est lié à la stratégie de lecture uniquement.)
- **appAdmin**. Accès administratif uniquement aux fonctionnalités de l'application dans Citrix ADM. (Ce rôle est lié à appAdminPolicy).
- **appReadonly**. Dispose d'un accès en lecture seule aux fonctionnalités de l'application. (Ce rôle est lié à appReadOnlyPolicy.)

> **Remarque** Les rôles prédéfinis ne peuvent pas être modifiés.

Vous pouvez également créer vos propres rôles (définis par l'utilisateur).

Pour créer des rôles et leur attribuer des stratégies :

1. **Dans Citrix ADM, accédez à**Système**>**Administration des utilisateurs > Rôles**.**
2. Cliquez sur **Ajouter**.
3. Dans le champ **Nom du rôle**, entrez le nom du rôle et fournissez la description dans le champ **Description du rôle** (facultatif).
4. Dans la section **Stratégies**, ajoutez ou déplacez une ou plusieurs stratégies vers la liste **configurée** .



5. Cliquez sur **Créer**.

Configurer les utilisateurs

February 1, 2024

Par défaut, Citrix Application Delivery Management (ADM) possède un utilisateur :

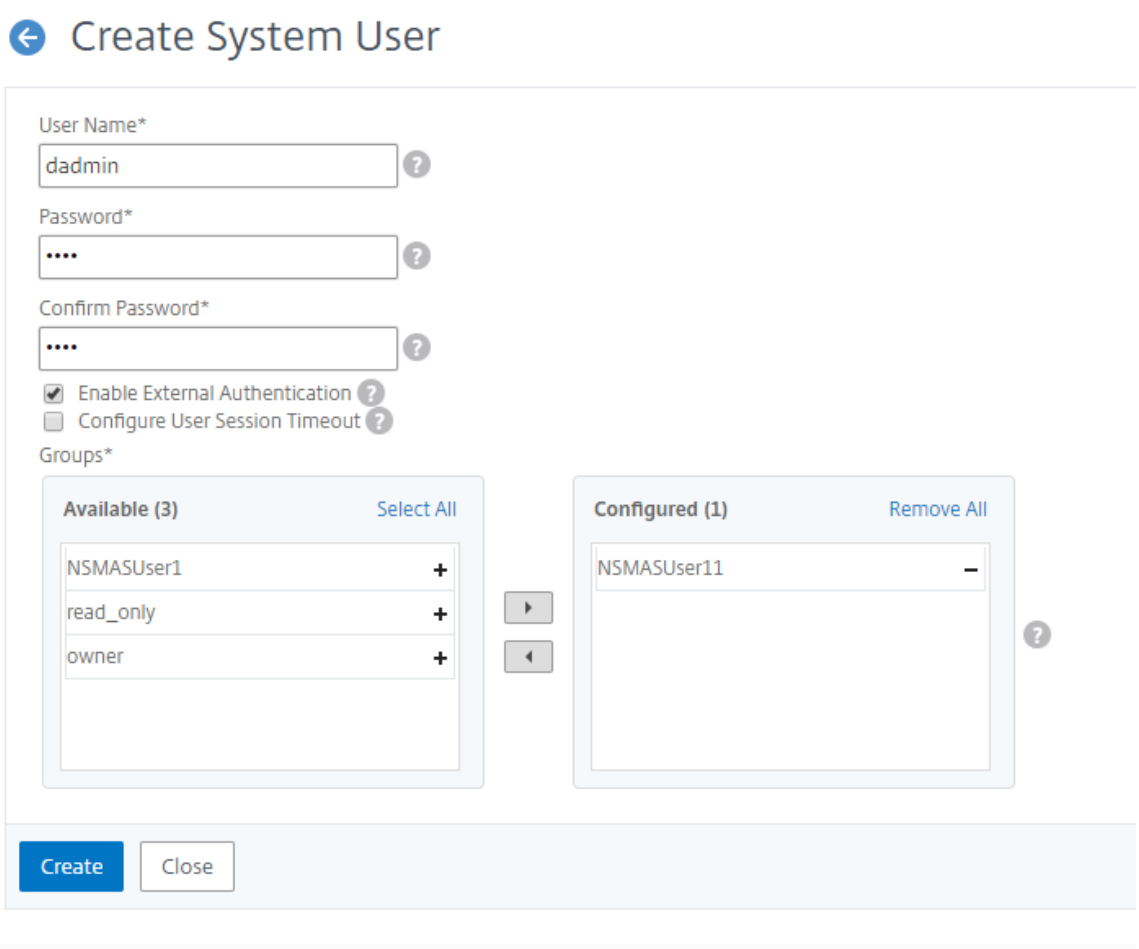
nsroot : l'utilisateur root (nsroot) dispose de privilèges d'administration complets sur l'appliance. L'utilisateur nsroot est le super administrateur de Citrix ADM.

Vous pouvez créer des utilisateurs supplémentaires en configurant des comptes pour eux. Lorsque vous ajoutez de nouveaux utilisateurs à Citrix ADM, vous pouvez définir leurs autorisations en attribuant les groupes, les rôles et les stratégies appropriés.

Vous pouvez affecter un utilisateur à un groupe et lier le groupe à des rôles. Vous pouvez définir des relations un-à-un, un-à-plusieurs ou plusieurs à plusieurs entre les utilisateurs, les groupes, les rôles et les stratégies d'accès. Un utilisateur peut être affecté à plusieurs groupes. Un groupe peut avoir plusieurs rôles et plusieurs groupes peuvent avoir des rôles identiques.

Pour configurer des utilisateurs dans Citrix ADM :

1. Dans Citrix ADM, accédez à **Système** > **Administration des utilisateurs** > **Utilisateurs**.
2. Cliquez sur **Ajouter**.
3. Entrez les informations suivantes :
   a) **Nom d'utilisateur**. Nom de l'utilisateur
   b) **Mot de passe**. Mot de passe avec lequel l'utilisateur se connecte à Citrix ADM
4. Vous pouvez également sélectionner **Activer l'authentification externe**afin que l'utilisateur puisse être authentifié via un serveur d'authentification externe.
5. Si vous avez créé des groupes et souhaitez affecter l'utilisateur à un groupe, dans la section **Groupes**, déplacez un ou plusieurs groupes de la liste **Disponible** vers la liste **configurée** .



6. Cliquez sur **Créer**.

Applications

February 1, 2024

La fonctionnalité d'analyse et de gestion des applications de Citrix ADM vous permet de surveiller les applications grâce à une approche centrée sur les applications. Cette approche vous permet de :

- Vérifiez le score et analysez les performances globales des applications
- Vérifiez si des problèmes persistent avec le serveur ou le client
- Détectez les anomalies dans les flux de trafic des applications et prenez des mesures correctives

> **Remarque**
>
> Les applications font référence à un ou plusieurs serveurs virtuels configurés sur les instances (Citrix ADC).

Vous pouvez surveiller les applications pendant une durée telle que 1 heure, 1 jour, 1 semaine et 1 mois.

Conditions préalables

- Assurez-vous d'avoir ajouté des instances Citrix ADC dans Citrix ADM
- Assurez-vous que vous disposez d'une licence valide pour vos instances Citrix ADC. Pour plus d'informations, voir Licences
- Vérifiez que vous avez appliqué la licence pour les serveurs virtuels. Pour plus d'informations, consultez Gérer les licences sur les serveurs virtuels

Présentation de l'application

Les applications peuvent être :

- Applications discrètes
- Applications personnalisées
- Applications de microservices (k8s_discrete)

Applications discrètes

Tous les serveurs virtuels sous licence sont appelés applications discrètes.

Applications personnalisées

Les serveurs virtuels d'une catégorie sont appelés applications personnalisées. En tant qu'administrateur, vous devez ajouter des applications personnalisées en fonction d'une catégorie. Vous pouvez ensuite gérer et surveiller les applications via le tableau de bord. Vous pouvez facilement surveiller des applications spécifiques regroupées dans une seule catégorie.

Par exemple, vous pouvez créer une catégorie pour votre centre de données1 et ajouter ses instances ADC. Une fois que vous avez défini une catégorie et ajouté l'instance pour votre centre de données1, le tableau de bord de l'application s'affiche avec une catégorie distincte, comprenant toutes les applications liées à votre centre de données1.

Points à noter

- Les applications discrètes qui sont ajoutées aux applications personnalisées sont supprimées des applications discrètes.
- Toutes les applications qui ne sont pas ajoutées à aucune catégorie sont disponibles en tant que **« autres »**.
- Par défaut, Citrix ADM vous permet d'ajouter des licences pour un maximum de deux applications. Selon votre licence, vous pouvez sélectionner et appliquer des licences pour les applications que vous souhaitez surveiller.

Applications de microservices

Dans un cluster Kubernetes, Citrix fournit un contrôleur d'entrée pour Citrix ADC MPX (matériel), Citrix ADC VPX (virtualisé) et Citrix ADC CPX (conteneurisé). Pour de plus amples informations, consultez Citrix Ingress Controller.

Les applications discrètes qui sont configurées à l'aide des instances Citrix ADC CPX sont appelées applications de microservices.

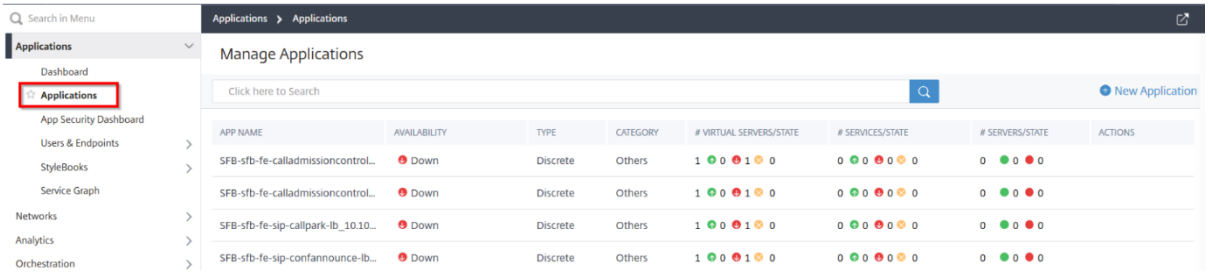
Gestion des applications et tableau de bord des applications

February 1, 2024

Citrix ADM vous permet de gérer les applications à partir de la page **Applications** et d'afficher les détails de l'application à partir de la page **Tableau de bord**.

Mes Applications

La page **Applications** vous permet d'afficher toutes les applications personnalisées et discrètes.



À partir de la page **Applications**, en tant qu'administrateur, vous pouvez :

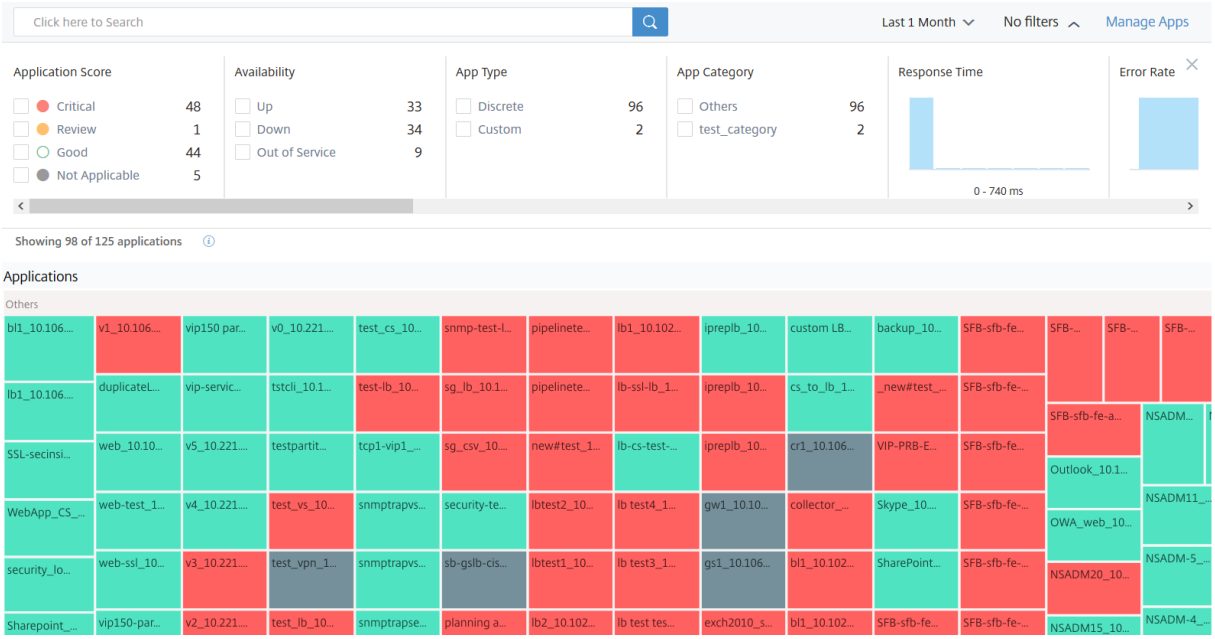
- Ajouter des applications
- Consultez les détails de l'application tels que le nom de l'application, le type d'application, la catégorie d'application, les serveurs virtuels associés, les services associés, etc.
- Modifier ou supprimer des applications personnalisées

Après avoir ajouté, modifié ou supprimé des applications, les détails sont immédiatement reflétés dans la page Applications.

Pour plus d'informations, consultez la section Gérer les applications.

Tableau de bord de l'application

Accédez à **Applications** > **Tableau de bord** pour afficher la liste des applications sous forme de tableau ou de graphique.



Toutes les applications s'affichent dans le tableau de bord uniquement lorsque les applications commencent à renseigner les données. Dans le tableau de bord, cliquez sur une application pour afficher des informations détaillées sur les performances de l'application. Pour plus d'informations, consultez la section Détails de l'application.

Si les analyses de l'application ne s'affichent pas même après une durée approximative de 10 à 15 minutes, effectuez les étapes de dépannage décrites dans Dépannage du tableau de bord de l'application.

Mises à jour dans le nouveau comportement du tableau de bord par rapport au tableau de bord précédent

- Après avoir ajouté ou modifié une application personnalisée, l'affichage de l'application dans le tableau de bord peut prendre quelques minutes.
- Si vous supprimez une application personnalisée, le tableau de bord affiche toujours l'application supprimée jusqu'à ce qu'ADM dispose de ses données d'analyse (durée maximale d'un mois).

  Imaginons que vous ayez créé une application le 2 janvier 2020 et que vous l'ayez supprimée le 4 janvier 2020. Dans ce scénario :

  - Le tableau de bord peut toujours afficher l'application supprimée le 4 janvier 2020, lorsque vous sélectionnez la durée des derniers 1 jour, 1 semaine et 1 mois.
  - Le tableau de bord peut toujours afficher l'application supprimée le 5 janvier 2020, lorsque vous sélectionnez la durée de la dernière semaine et du dernier mois.
  - Lorsque la durée dépasse la date de suppression de l'application, l'application n'est pas affichée dans le tableau de bord. En d'autres termes, le tableau de bord ne s'affiche pas avec l'application supprimée le 6 janvier 2020 (pour le dernier jour), le 12 janvier 2020 (pour la dernière semaine) et après le 5 février 2020 (pour le dernier mois).

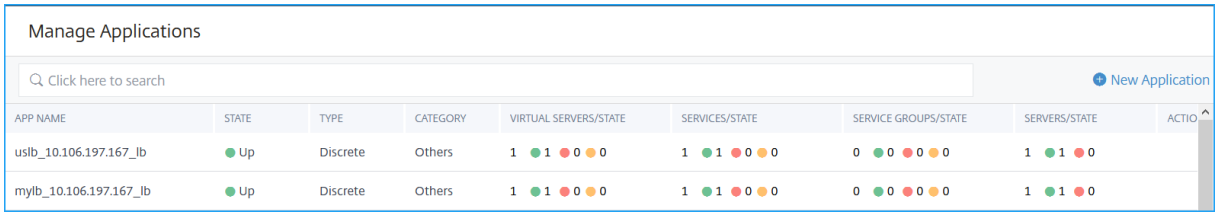
    > **Remarque**
    >
    > Après avoir ajouté une application, si l'instance Citrix ADC associée est en panne, hors service ou inaccessible en raison d'un problème réseau temporaire :
    >
    > -Les applications associées à l'instance ADC ne sont visibles que sur la page **Applications**, mais pas dans le tableau de bord.
    >
    > -Les applications sont affichées dans le tableau de bord après l'exécution de l'instance ADC.

Mes Applications

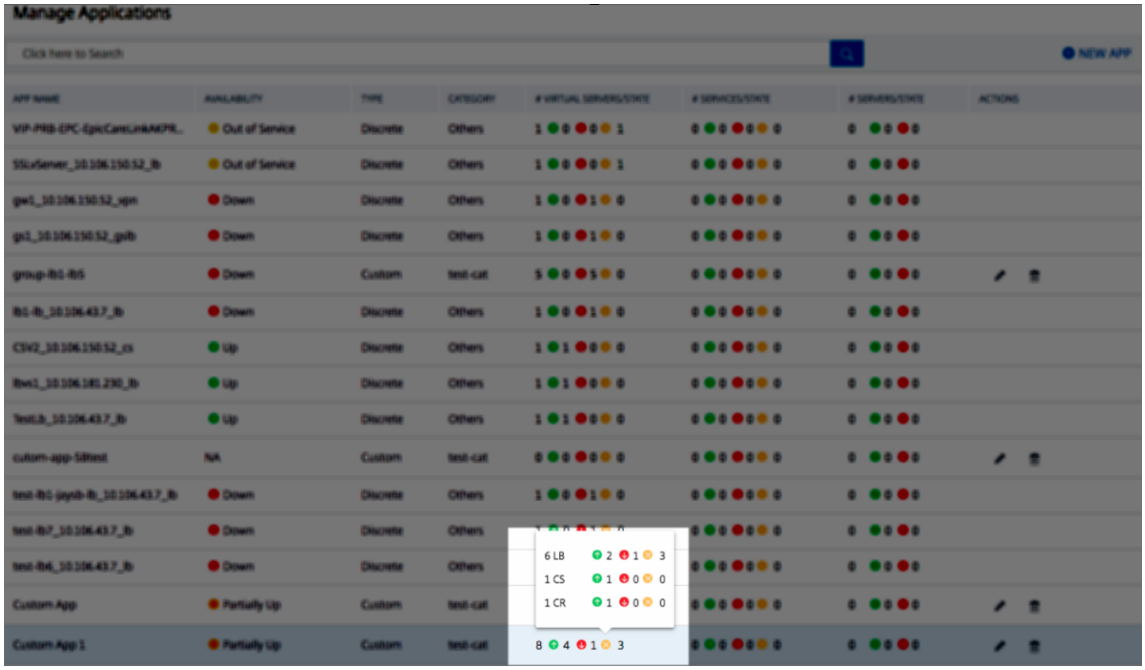
February 1, 2024

Dans le tableau de bord, cliquez sur **Gérer les applications** pour afficher les détails de l'application et ajouter, modifier ou supprimer des applications personnalisées.

Afficher les détails de l'application



- **Nom de l'application** —Indique le nom de l'application
- **Disponibilité **: indique la disponibilité actuelle de l'application, par exemple en cours d'exécution, **en **panne**, partiellement**opérationnelle, hors service**et NA**
  - **Up** : tous les serveurs virtuels associés à l'application sont Up.
  - **Arrêté** : tous les serveurs virtuels associés à l'application sont hors service
  - **Partiellement actif** : l'un des éléments virtuels associés à l'application est en panne ou hors service
  - **Hors service** : tous les serveurs virtuels associés aux applications sont hors service
  - **NA** —Aucun serveur virtuel n'est configuré pour l'application
- **Type** : indique si l'application appartient à la catégorie Custom ou Discrete
- **Catégorie** —Indique la catégorie d'application qui est groupée
- **Serveur/état virtuel** : indique le nombre total de serveurs virtuels configurés et l'état actuel de tous les serveurs virtuels. Passez le pointeur de la souris pour afficher les détails tels que le nombre total de serveurs virtuels, le type de serveur virtuel et l'état du serveur virtuel

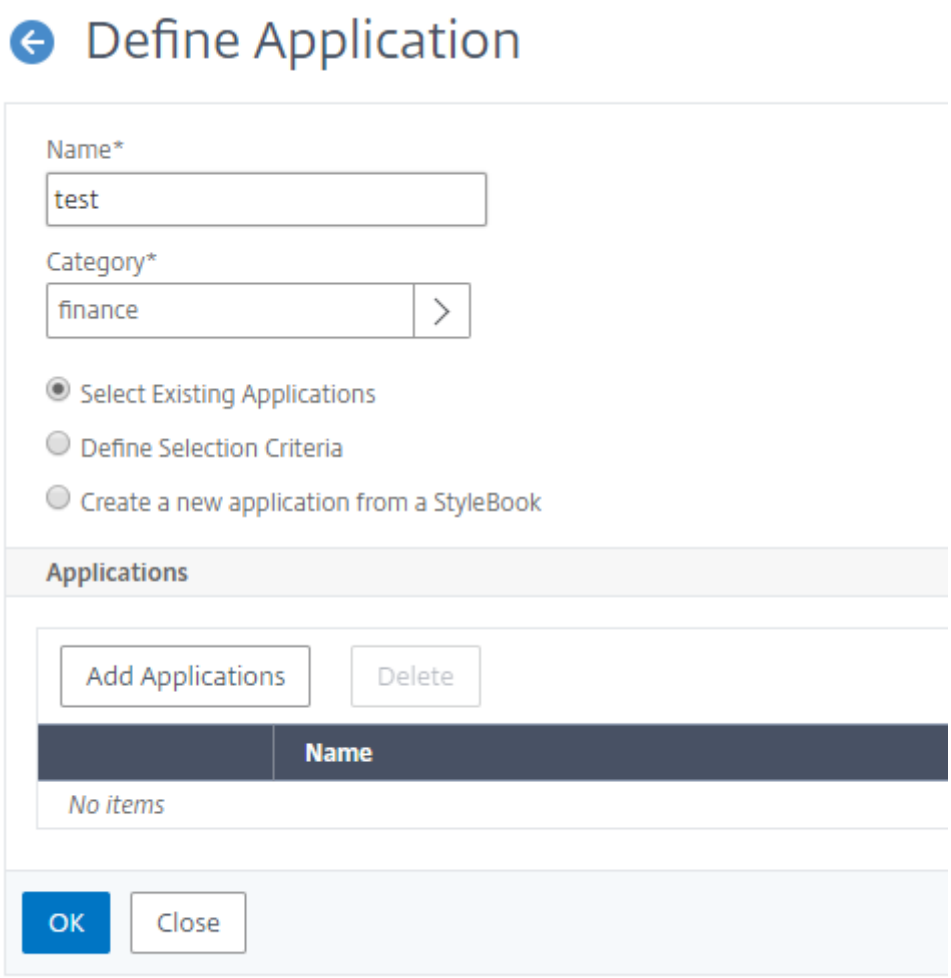


- **Services/état** —Indique le total des services configurés et l'état actuel de tous les services
- **Groupes de services/état** —Indique le nombre total de groupes de services configurés et l'état de tous les groupes de services
- **Serveurs/état** —Indique le nombre total de serveurs configurés pour l'application et l'état actuel de tous les serveurs
- **Actions** –permet de modifier ou de supprimer les applications personnalisées

Ajouter une application

1. Cliquez sur **Nouvelle application** pour créer une nouvelle application

   La page **Définir l'application** s'affiche



> **Remarque :**
>
> Vous pouvez également cliquer sur **Applications**, puis sélectionner **Nouvelle application** pour ajouter une nouvelle application.

2. Définissez les paramètres suivants :

Champ	Description
Nom	Nom de l'application personnalisée. Par exemple, LB_TEST.

Champ	Description
Catégorie	Catégorie dans laquelle vous pouvez regrouper les applications. Cliquez pour accéder à la page des catégories d'applications. Sélectionnez la catégorie et cliquez sur **Sélectionner**. Pour ajouter une catégorie a) Cliquez sur **Ajouter**. a) Entrez le nom de votre choix. a) Cliquez sur **Créer**.
Sélectionner des applications existantes	Vous permet de sélectionner les applications existantes ajoutées aux instances Citrix ADC.
Ajouter une application	Affiche tous les serveurs virtuels configurés sur les instances. Sélectionnez les applications dans la liste et cliquez sur **OK**.
Définir les critères de sélection	Option permettant de définir l'application par plage de serveurs virtuels ou par plage d'adresses IP de serveur/service d'origine. • **Serveur.** Spécifiez l'adresse IP du serveur ou du service, le nom du serveur ou le port du serveur principal sur lequel les applications s'exécutent. Vous pouvez entrer une adresse IP, une plage d'adresses IP ou une combinaison des deux séparées par des virgules. Par exemple, vous pouvez entrer 10.102.29.20, 10.102.43.10-60, 10.216.43.45. • **Serveurs virtuels.** Vous pouvez spécifier l'une des options suivantes : l'adresse IP du serveur virtuel, le nom du serveur virtuel ou le port du serveur principal sur lequel les applications s'exécutent. Vous pouvez entrer une adresse IP ou une plage d'adresses IP ou une combinaison des deux séparées par des virgules. Par exemple, vous pouvez entrer 10.102.29.20, 10.102.43.10-60, 10.216.43.45.

Champ	Description
Créer une nouvelle application à partir d'un StyleBook	Permet de créer une application à l'aide du StyleBook. Pour plus d'informations, voir Création d'une application à l'aide du StyleBook.

3. Cliquez sur **OK**.

   > **Remarque :**
   >
   > Actuellement, Application Dashboard prend uniquement en charge l'équilibrage de charge et le changement de contenu des serveurs virtuels.

   Le tableau de bord de l'application est maintenant affiché avec la catégorie et toutes les applications sont regroupées en dessous.

   Si vous sélectionnez **Créer une nouvelle application à partir d'une option StyleBook** pour l'application personnalisée, vous devez autoriser Citrix ADM à sélectionner automatiquement les serveurs virtuels pour l'octroi de licences. Pour activer la sélection automatique des serveurs virtuels :

   a) Accédez à **Système> Licences et analyses** .

   b) Sous **Virtual Server License Summary**, cliquez sur **Auto-select Serveurs virtuels**et **Auto-select Serveurs virtuels non adressables**à activer.

Créer une application à l'aide du StyleBook

Pour créer une application à l'aide du StyleBook :

1. Dans Citrix ADM, accédez à **Applications** > **Tableau de bord** et cliquez sur **Définir une application personnalisée** pour créer une application personnalisée.
2. Dans la page **Définir une application**, tapez le nom de l'application dans le champ **Nom** .
3. Sélectionnez la catégorie d'application dans la section Catégorie. Citrix ADM vous permet de définir des catégories pour regrouper les applications définies par l'utilisateur. Vous pouvez également ajouter d'autres catégories si nécessaire.
4. Cliquez pour sélectionner **Créer une nouvelle application à partir d'un StyleBook**, puis cliquez sur **OK.**

   La page Choose StyleBook s'affiche. Cette page contient tous les StyleBooks par défaut disponibles dans Citrix ADM.

5. Sélectionnez le StyleBook.
   La page **Détails de configuration** s'affiche.
6. Entrez les valeurs de tous les paramètres dans le StyleBook. Vous pouvez également cliquer sur View Definition pour afficher la construction du StyleBook avant de l'utiliser.

   Pour plus d'informations, consultez la section Utiliser les StyleBooks par défaut.
7. Cliquez sur **Créer**.

   Vous pouvez également cliquer sur **Exécuter à sec** pour vérifier les configurations que Citrix ADM tente de créer sur l'instance Citrix ADC sélectionnée. Cette option est uniquement destinée à votre test pour voir la vérification finale des configurations. Même si l'option Dry Run est réussie, la configuration réelle sur le Citrix ADC sélectionné peut toujours échouer pour diverses raisons (conflit IP, instance inaccessible, etc.)

Modifier ou supprimer une application

Sur la page **Applications**, vous pouvez modifier ou supprimer les applications personnalisées. Cliquez sur le bouton Modifier pour modifier une application et sur le bouton Supprimer pour supprimer l'application.

Exporter les rapports du tableau de bord de l'application et du tableau de bord de

Citrix ADM vous permet de prendre un instantané du tableau de bord actuel de l'application et de les exporter sous forme de rapports. À intervalles réguliers, les administrateurs de l'application peuvent avoir besoin d'utiliser ces rapports pour mettre à jour l'utilisation de l'application et les pénalités de performance.

Grâce à cette fonctionnalité, les administrateurs peuvent extraire ces données sous forme de rapports .png, .jpeg ou .pdf.

> **Remarque :**
>
> Contrairement aux autres options d'exportation de rapports dans Citrix ADM, vous pouvez exporter les rapports App Dashboard et Security Dashboard uniquement sous forme de fichiers .pdf ou .png. Le format .csv n'est pas pris en charge actuellement.

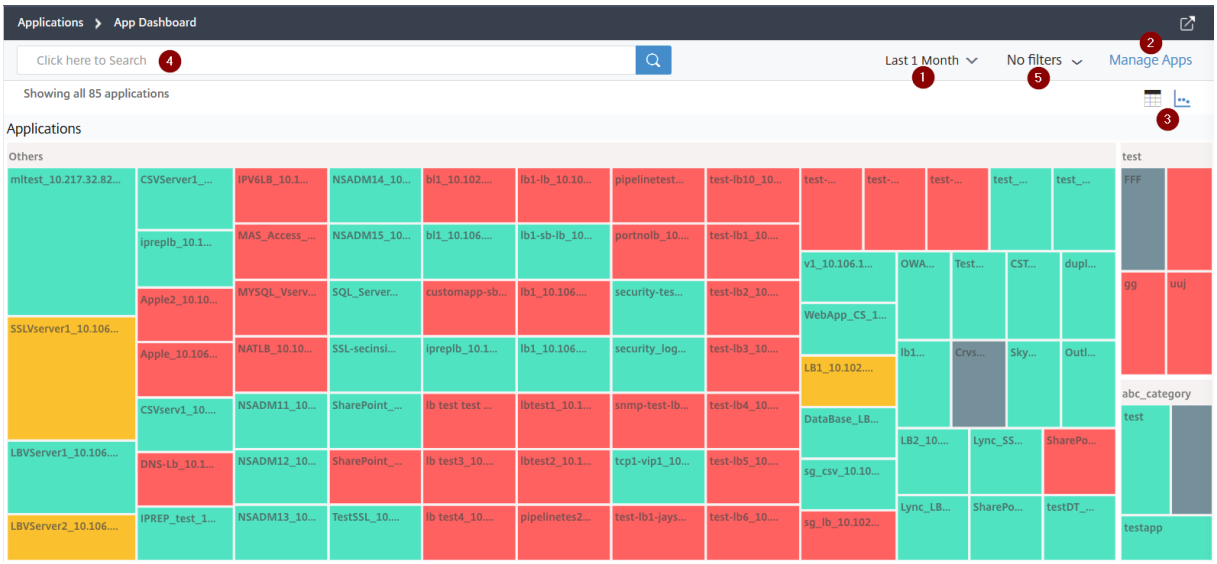
Le rapport se télécharge sur votre système. À partir des pages App Dashboard et App Security Dashboard, vous pouvez également accéder à des pages de deuxième niveau et les exporter sous forme de rapports. Actuellement, vous pouvez télécharger des rapports d'une seule application à la fois.

Vue d'ensemble du tableau de bord des applications

February 1, 2024

Le tableau de bord de l'application affiche les applications discrètes sous **Autres** et les applications personnalisées regroupées sous leurs catégories respectives.

Accédez à **Application** > **Tableau de bord** pour afficher le tableau de bord de l'application.



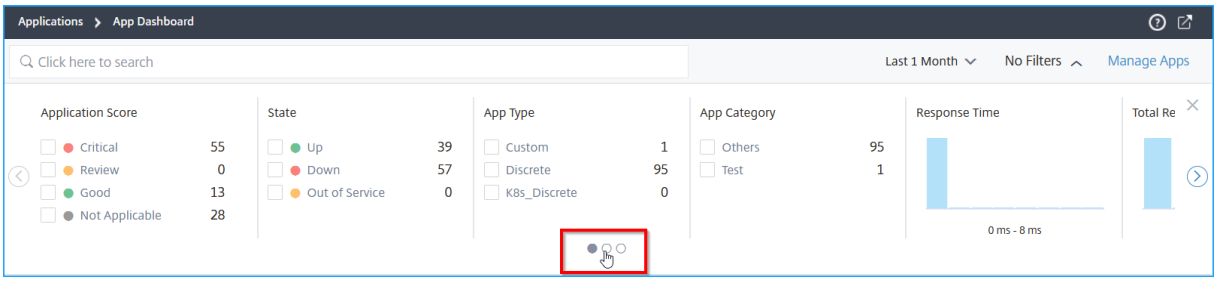
1 —Affiche les détails de l'application pour la durée sélectionnée, par exemple 1 heure, 1 jour, 1 semaine et 1 mois.

2 —Vous permet de gérer les applications et d'ajouter de nouvelles applications

3 —Vous permet de visualiser les applications sous forme de tableau ou de graphique

4 —Vous permet de rechercher une application à l'aide de la barre de recherche

5 —Vous permet d'appliquer des filtres pour afficher les applications. Cliquez pour voir plus de détails.

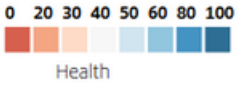


Vous pouvez sélectionner le curseur de carrousel qui vous permet d'accéder facilement à toutes les options.

Vous pouvez :

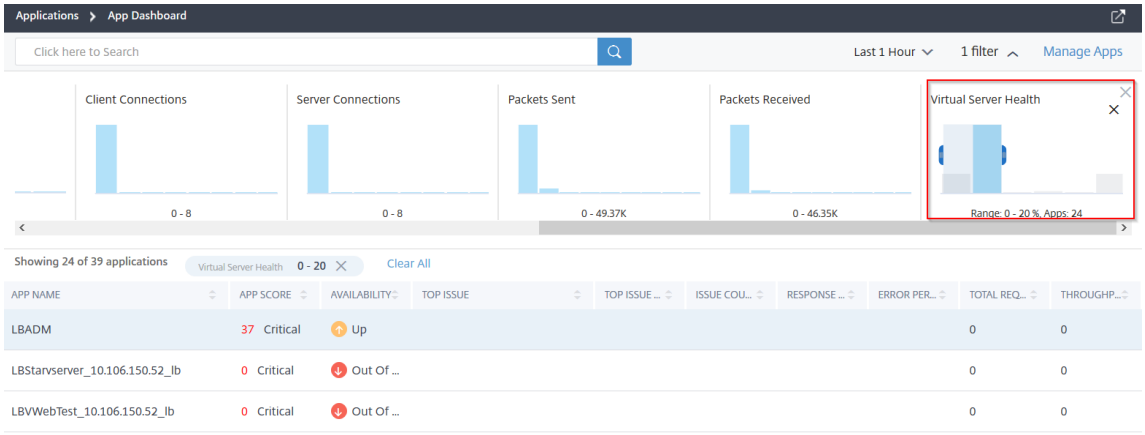
- Sélectionnez cette option pour afficher les applications en fonction des scores.
  - **Critique** : le score de l'application est compris entre 0 et < 40
  - **Passable** —Le score de l'application se situe entre 40 et < 75
  - **Bon** —Le score de l'application est supérieur à 75
  - **Non applicable** : aucun serveur virtuel n'est configuré pour l'application

    Le tableau suivant décrit les différences entre le score antérieur de l'application et le score actuel de l'application.

Note attribuée à l'application (critique, évaluation, bonne, sans objet)	Score de l'application (vue précédente avec légendes en couleur)
Le score est calculé comme **100 moins le score de pénalité pour tous les problèmes actuels de l'application**. Les applications sont affichées dans des couleurs telles que le **rouge (critique)**, l'**orange (critique)**, le **vert (bon)**et le **gris (sans objet)**	Le score est calculé comme **100 —(ressource serveur d'applications + ressource système Citrix ADC)** Les applications sont affichées dans des légendes de couleurs. 

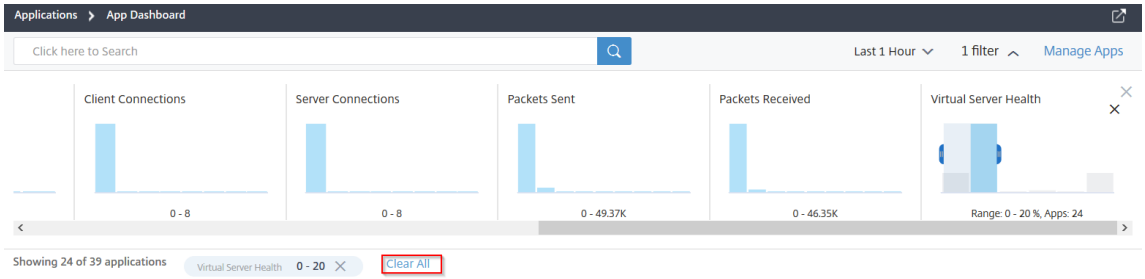
- Sélectionnez cette option pour afficher les applications en fonction de l'état de l'application, comme le haut, le bas et le hors service.
- Sélectionnez cette option pour afficher les applications en fonction du type d'application, par exemple Discrète ou Personnalisée
- Sélectionnez cette option pour afficher les applications en fonction des catégories regroupées ci-dessous
- Faites glisser l'histogramme pour appliquer des filtres et afficher les applications.

  Par exemple, si vous souhaitez afficher des applications dont l'état de santé du serveur virtuel est compris entre 0 et 20, faites glisser l'histogramme de santé du serveur virtuel pour filtrer les résultats.



> **Remarque**
>
> Vous pouvez également cliquer sur l'histogramme pour afficher les applications pertinentes.

Cliquez sur **Tout effacer** pour effacer le filtre appliqué.



Voici le résumé de l'application pour lequel vous pouvez appliquer des filtres :

- **Temps de réponse** : histogramme qui affiche le temps de réponse moyen reçu par les applications
- **Taux d'erreur** : histogramme qui affiche le pourcentage d'erreur moyen des erreurs 5xx pour les applications.
- **Nombre total de demandes** : histogramme qui affiche le nombre total de demandes reçues par les applications
- **Débit** : histogramme qui affiche le débit réseau total traité par les applications
- **Volume de données** : histogramme qui affiche le total des données traitées par les applications. Le volume de données est calculé par le nombre total d'octets de requête et d'octets de réponse pour les applications.
- **Connexions client** : histogramme qui affiche le nombre moyen de connexions client établies par les applications.
- **Connexions au serveur** : histogramme qui affiche le nombre moyen de connexions au serveur établies par les applications

- **Paquets envoyés** : histogramme qui affiche le nombre total de paquets envoyés par les applications.
- **Paquets reçus** : histogramme qui affiche le nombre total de paquets reçus par les applications
- **Santé du serveur virtuel** : histogramme qui affiche le total des applications entre la plage de score de 0 à 100 %. L'état d'un serveur virtuel est (%) des services actifs associés à l'application. Par exemple, si un serveur virtuel est configuré avec 2 services et si l'un d'eux est en panne, le score est de 50 %.

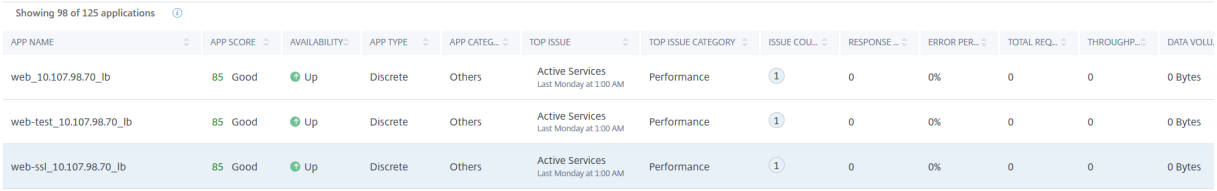
Recherche et filtrage des résultats à l'aide de la barre de recherche

Vous pouvez placer le pointeur de la souris sur la barre de recherche et sélectionner la catégorie pour affiner la recherche.

Afficher les applications

February 1, 2024

Par défaut, le tableau de bord de l'application affiche toutes les applications. En fonction de vos besoins, vous pouvez utiliser l'option de filtre pour afficher les applications.



Le tableau de bord affiche les détails suivants de l'application :

- **Nom de l'application** —Indique le nom de l'application
- **Score de l'application** : indique le score de l'application et son statut, tel que **Critique**, **Bon**, **Passable**et **Non applicable**
- **Disponibilité **: indique la disponibilité actuelle de l'application, par exemple en cours d'exécution, **en **panne**, partiellement**opérationnelle, hors service**et NA**
  - **Up** : tous les serveurs virtuels associés à l'application sont Up.
  - **Arrêté** : tous les serveurs virtuels associés à l'application sont hors service.
  - **Partiellement actif** : l'un des éléments virtuels associés à l'application est en panne ou hors service.

  - **Hors service** : tous les serveurs virtuels associés aux applications sont hors service.
  - **NA** : aucun serveur virtuel n'est configuré pour l'application.

- **Problème principal** : indique le problème pour lequel l'application compte le plus grand nombre d'erreurs
- **Catégorie du numéro** le plus publié —Indique la catégorie du numéro
- **Nombre de problèmes** —Indique le nombre total de problèmes pour l'application
- **Temps de réponse** —Indique le temps de réponse moyen pour répondre à partir de l'application
- **Pourcentage d'erreur** —Indique le pourcentage d'erreur total de 5xx erreurs pour l'application

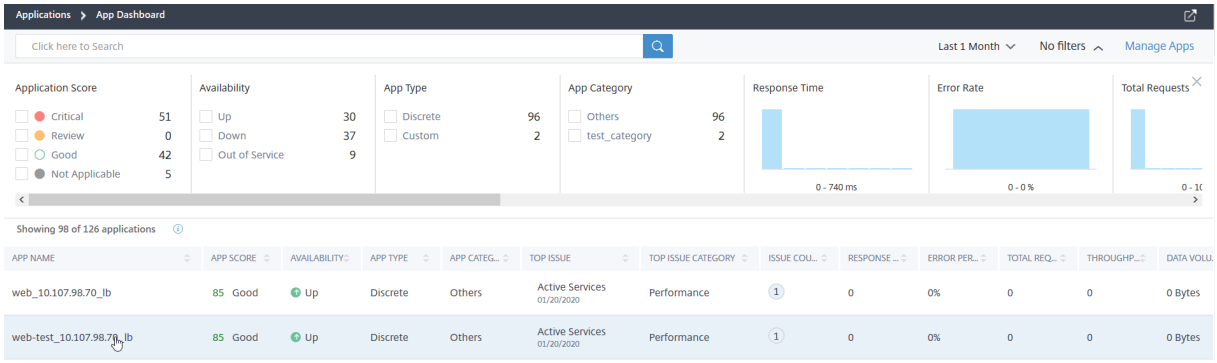
  > **Remarque**
  >
  > La mesure de pourcentage d'erreur 5xx s'affiche uniquement pour **Citrix ADC 13.0 ou version ultérieure**. Pour les versions antérieures, la valeur est affichée sous la forme **0**.

- **Nombre total de demandes** —Indique le nombre total de demandes reçues par l'application
- **Débit** : indique le débit réseau total de l'application. Le débit est calculé par la valeur Req Octets/Sec + Res Octets/Sec pour les serveurs virtuels
- **Volume de données** —Indique le total des données traitées par l'application
- **Connexions client** : indique le nombre moyen de connexions client établies par l'application
- **Connexions au serveur** —Indique la moyenne des connexions au serveur établie par l'application

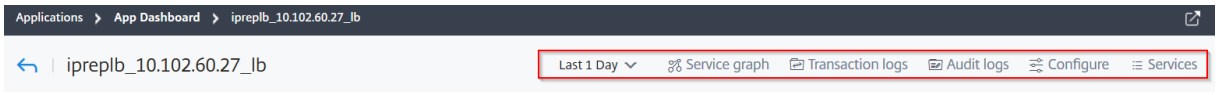
Détails de l'application

February 1, 2024

Cliquez sur une application depuis le tableau de bord pour accéder à des informations plus détaillées.



La page de l'application sélectionnée s'affiche.

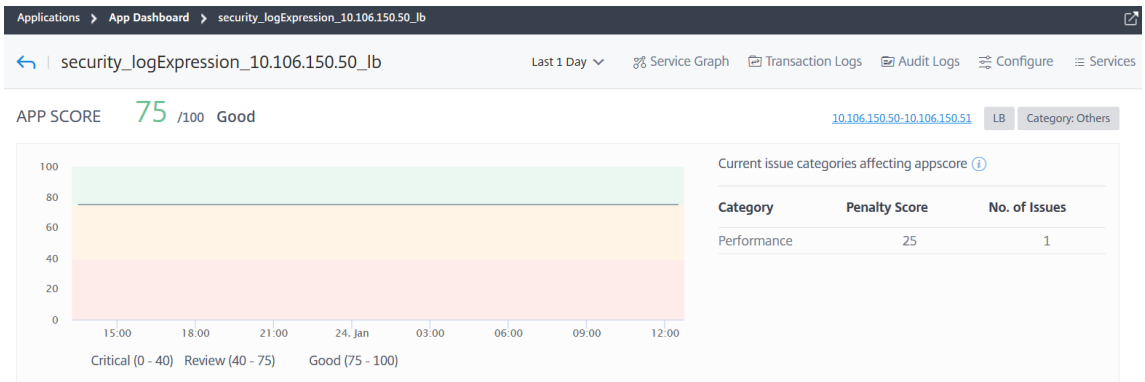


À partir de la page des détails de l'application :

- Sélectionnez la durée dans la liste pour afficher les détails de la durée spécifique
- Cliquez sur **Graphique de service** pour afficher le graphique de service de l'application sélectionnée. Pour plus d'informations, voir Graphique de service pour les applications
- Cliquez sur **Journaux des transactions** pour afficher les transactions détaillées pour les erreurs 5xx
- Cliquez sur **Journaux d'audit** pour afficher les informations détaillées du journal d'audit
- Cliquez sur **Configurer** pour afficher ou modifier la configuration du service et du groupe de services de l'application
- Cliquez sur **Service** pour afficher les services liés à l'application

Après avoir sélectionné la durée, les détails de l'application suivants s'affichent :

- **Score** de l'application —Score de l'application pour la durée sélectionnée. Le score final est calculé comme **100 moins la pénalité totale**.

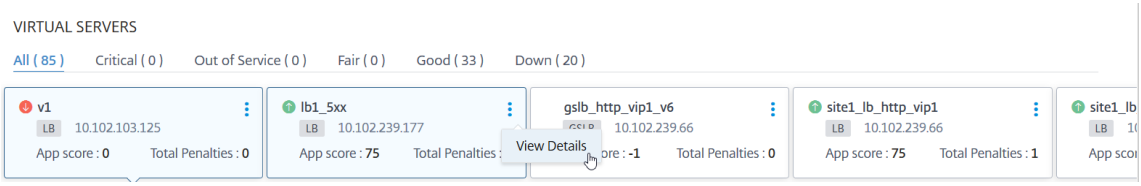


Ce tableau de bord vous permet également d'afficher les problèmes actuels qui affectent le score de l'application. Vous pouvez afficher les détails des problèmes sous Problèmes.

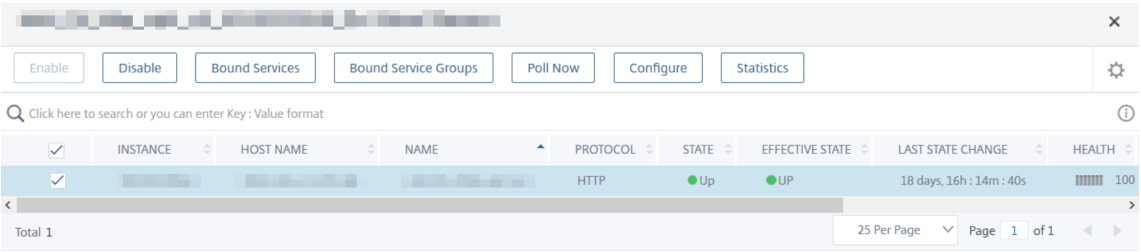
- **Serveurs virtuels** —

> **Remarque**
>
> La section **Serveurs virtuels** s'affiche uniquement pour les applications personnalisées. Pour les applications discrètes, cliquez sur l'**adresse IP** pour afficher les détails du serveur virtuel.

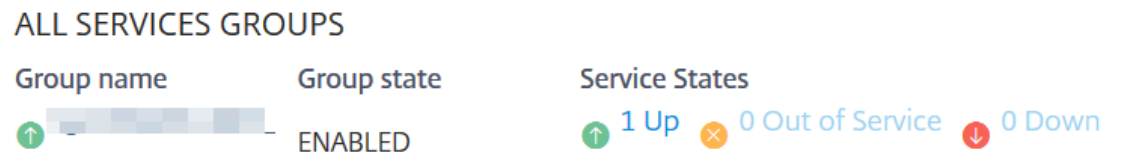
Affiche tous les serveurs virtuels associés à l'application personnalisée



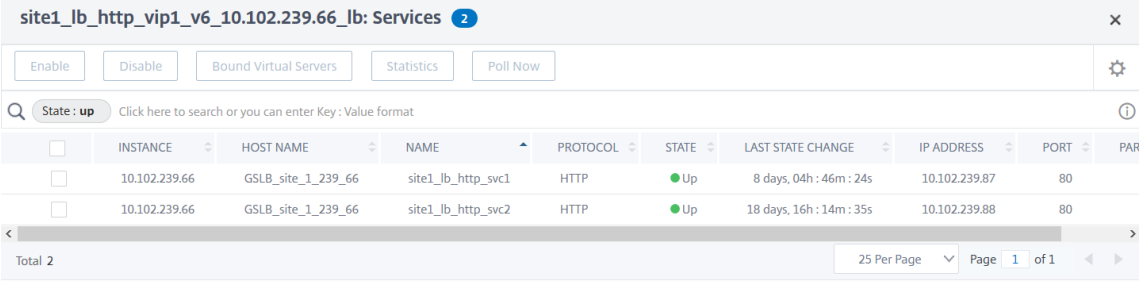
Cliquez sur **Afficher les détails** pour afficher et gérer les paramètres du serveur virtuel.



- **Tous les services** : les services liés à l'application



Cliquez pour afficher les détails du service et pour gérer les paramètres du service



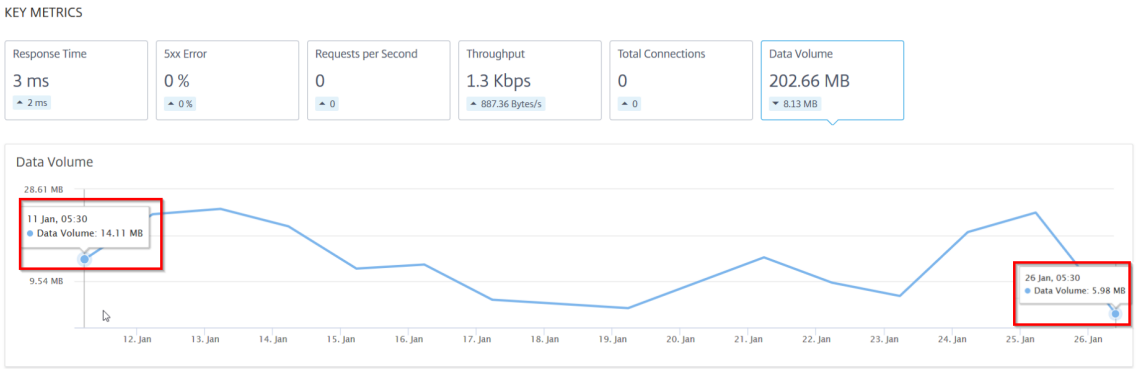
- **Mesures clés** —Détails des mesures de l'application, tels que **Temps de réponse de l'application**, **Pourcentage d'erreur**, **Demandes par seconde**, **Débit**, **Nombre total de connexions**et **Volume de données**. Pour les applications liées à SSL, d'autres informations sur les mesures telles que les **coups de session**, le **taux d'octets chiffrés**, le **taux d'octets déchiffrés**et la **nouvelle session SSL créée** s'affichent.

  > **Remarque**
  >
  > La mesure de pourcentage d'erreur 5xx s'affiche uniquement pour **Citrix ADC 13.0 ou version ultérieure**. Pour les versions antérieures, la valeur est affichée sous la forme **0**.

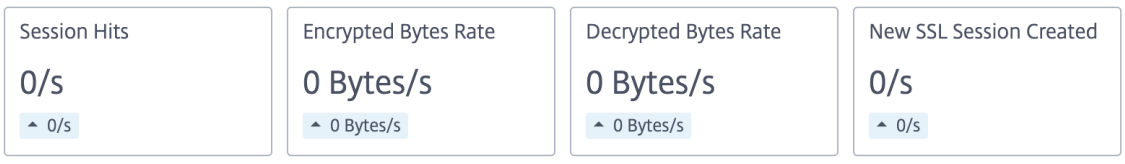
  Dans chaque mesure, vous pouvez afficher la valeur moyenne et la valeur de différence pour la durée sélectionnée. La valeur de différence est calculée comme la **première valeur moins la dernière valeur** de la durée sélectionnée.

  Vous pouvez afficher les mesures d'instance suivantes dans un format graphique pour la durée sélectionnée :

  L'image suivante est un exemple de volume de données et la durée sélectionnée est de 1 mois. La valeur 202,66 Mo est le volume de données total pour la durée d'un mois et la valeur 8,13 Mo est la valeur de différence. Dans le graphique, la première valeur est 14,11 et la dernière valeur est 5,98. La valeur de la différence est de 14,11 à 5,98 = 8,13 Mo.



  Pour les applications liées à SSL, vous pouvez afficher les autres mesures suivantes :



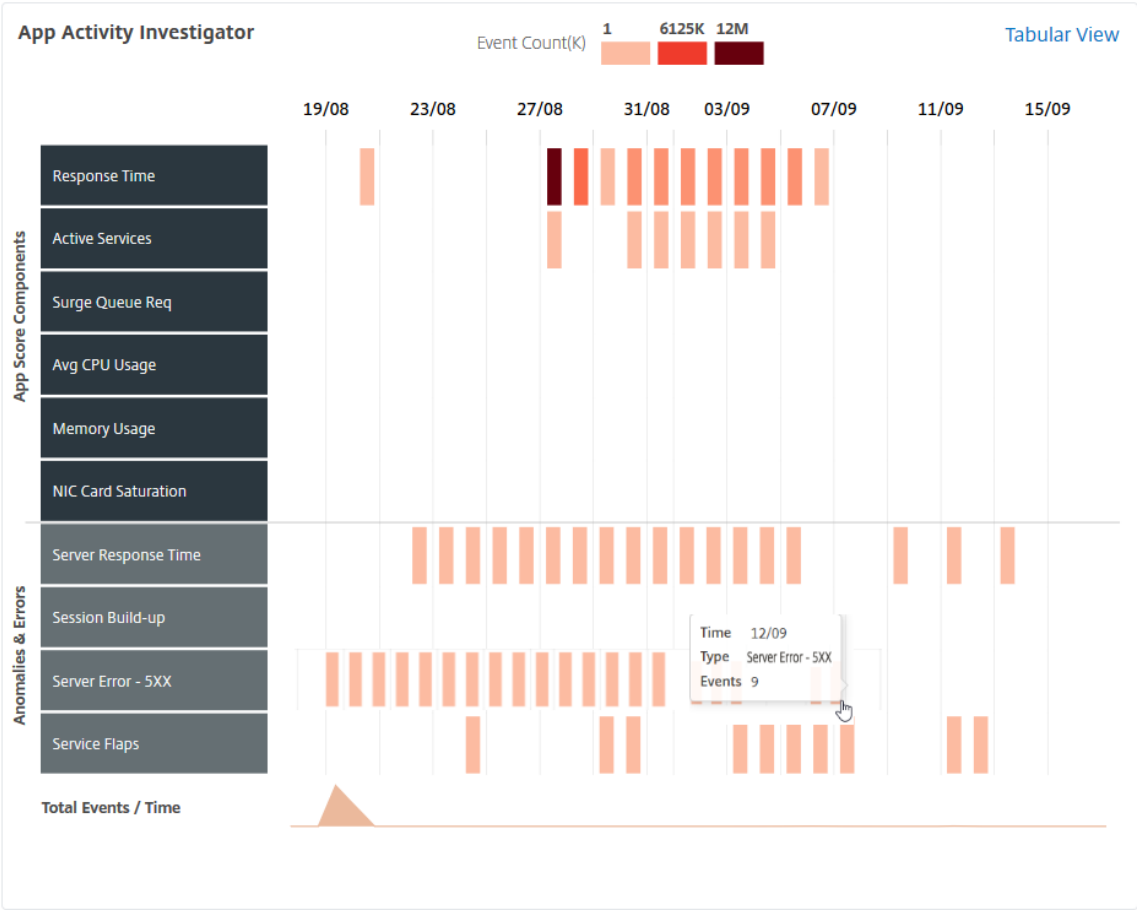
- **Problèmes** —Problèmes applicables à la demande sélectionnée. Vous pouvez afficher les problèmes suivants avec sa catégorie :

Performances	Santé de l'instance	Config	Ressources système
Temps de réponse	Utilisation moyenne du processeur	Serveur instable	Type de persistance incorrect
Services actifs	Utilisation de la mémoire	Paquets HTTP exceptionnellement volumineux	Saturation de la carte NIC
Réutilisation de session faible		TCP reassemble queue limit hits	
Accumulation dans la file d'attente de surtension			
Trafic SSL en temps réel			
Création de sessions			
Volets de service			

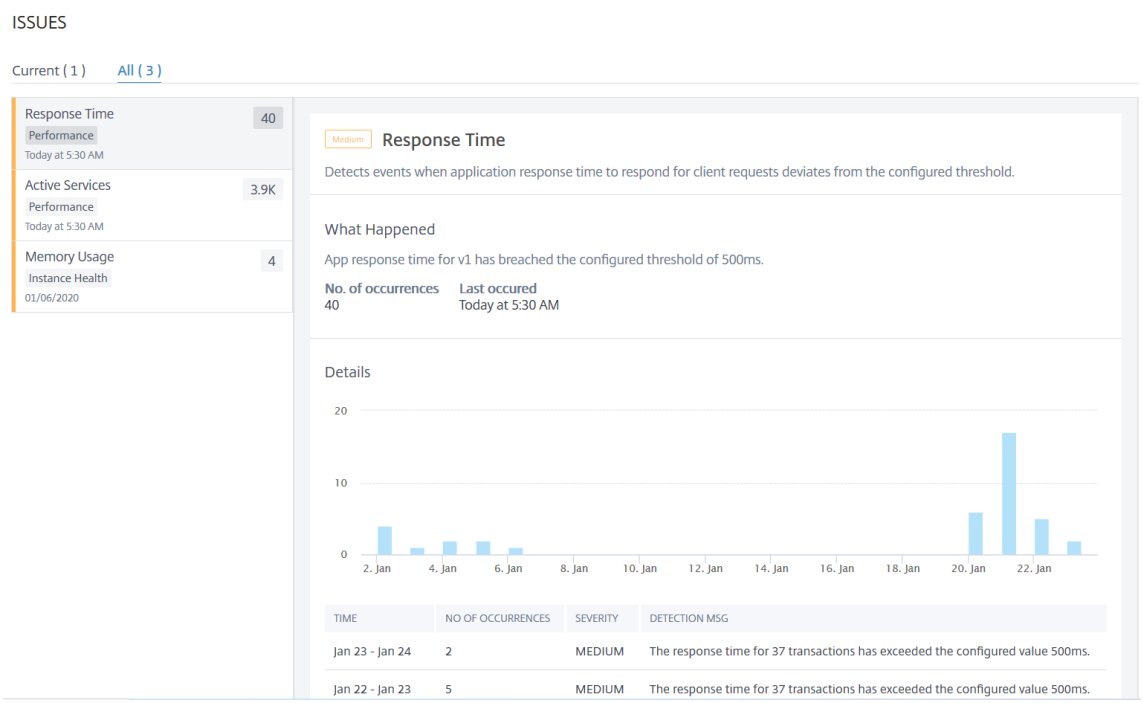
Cliquez sur chaque problème pour vérifier les détails tels que le message de détection, la date à laquelle le problème s'est produit, les actions recommandées et les détails.

Pour plus d'informations, voir Indicateurs de performance pour l'analyse des applications.

L'image suivante est la vue antérieure de la page App Activity Investigator :



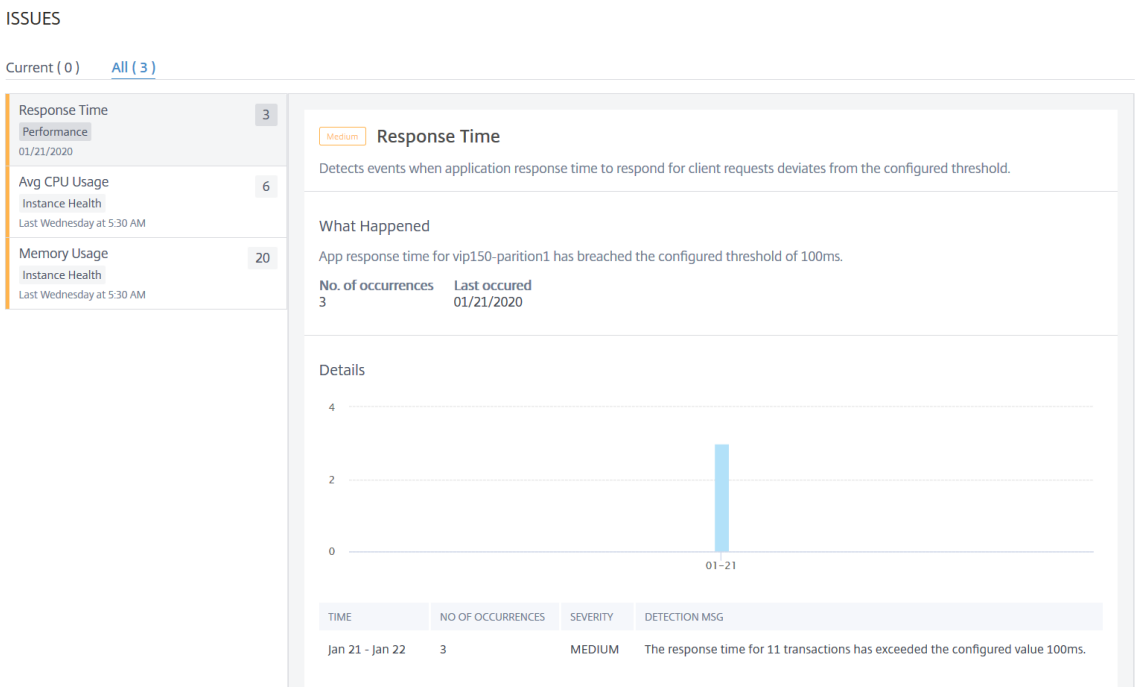
Vous pouvez désormais consulter tous les problèmes dans la section **Problèmes**, ainsi que la catégorie que vous pouvez consulter sur la page **App Activity Investigator** .



- Les problèmes qui s'affichent dans l'onglet En **cours** font référence aux problèmes de l'application pour la durée sélectionnée.
- Les problèmes qui s'affichent dans l'onglet **Tous** font référence à l'ensemble des problèmes d'application.

L'exemple suivant présente les problèmes d'application pour une durée d'un jour. L'onglet **Actuel** indique qu'aucun problème actuel n'a d'impact sur le score de l'application.

L'onglet **Tous** affiche le nombre total de problèmes détectés pendant une journée.



Sélectionnez les composants App Score et définissez des seuils

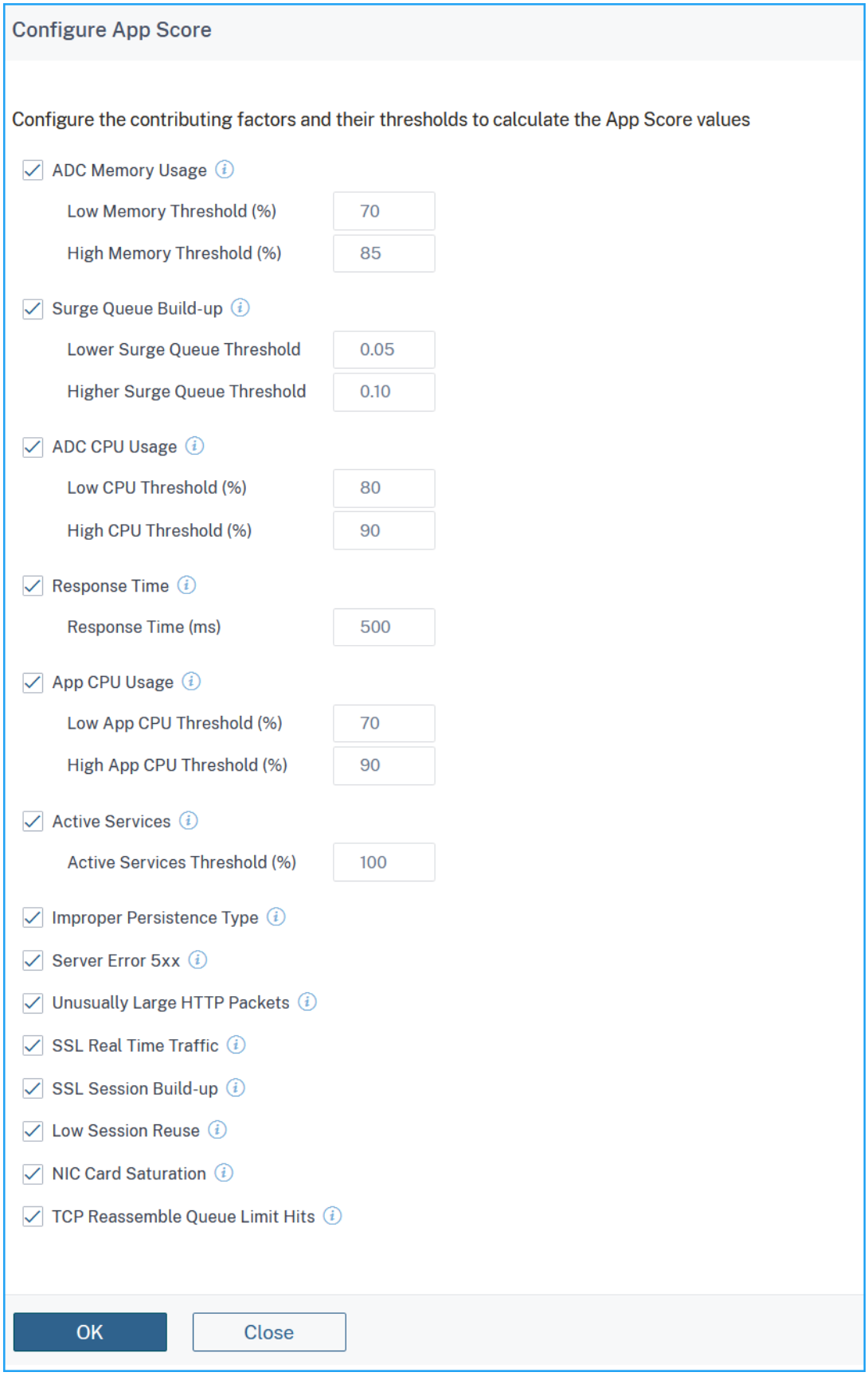
February 1, 2024

Dans le **Tableau de bord des applications**, en tant qu'administrateur, vous pouvez décider de sélectionner les composants et de configurer des seuils pour le calcul du score de l'application. App Score est le système de notation qui définit :

- Comment une application fonctionne bien
- Si l'application fonctionne bien en termes de réactivité

Accédez à **Applications > Tableau de bord**, puis sélectionnez l'icône Paramètres.

Dans la page **Configurer le score de l'application**, vous pouvez sélectionner les composants et configurer des seuils pour déterminer le score final de l'application.



Le calcul du score de l'application est basé sur les éléments suivants :

Composants App Score	Seuils configurés par l'utilisateur	Description
Utilisation de la mémoire ADC	Oui	Valeur de seuil faible et élevée pour l'utilisation totale de la mémoire dans l'instance Citrix ADC
Build de file d'attente de surtension	Oui	Valeur de seuil faible et élevée pour le nombre total de demandes de surtension qui sont en file d'attente et qui nécessitent une réponse.
Utilisation du processeur ADC	Oui	Valeur de seuil faible et élevé pour l'utilisation totale de l'UC dans l'instance Citrix ADC.
Temps de réponse	Oui	Intervalle de temps entre l'envoi d'un paquet de requête et la réception du premier paquet de réponse à partir du service configuré sur le serveur virtuel.
Utilisation du processeur de l'application	Oui	Valeur seuil faible et élevée pour l'utilisation totale de l'UC par l'application.
Services actifs	Oui	Valeur de seuil du pourcentage de services qui doivent être actifs et qui sont liés au serveur virtuel.
Type de persistance incorrect	Non	Indique si l'utilisation de persistance sur un serveur virtuel est faible.
Erreur serveur (5xx)	Non	Indique si le serveur Web répond avec des erreurs 5xx.
Paquets HTTP exceptionnellement volumineux	Non	Indique les occurrences, si les messages HTTP avec la taille d'en-tête HTTP dépassent les valeurs configurées dans l'instance Citrix ADC.

Composants App Score	Seuils configurés par l'utilisateur	Description
Trafic en temps réel SSL	Non	Analyse le trafic SSL pour identifier le trafic en temps réel et suggère des paramètres de configuration optimaux pour améliorer la latence.
Construction de session SSL	Non	Indique l'accumulation de session sur une période de temps, ce qui peut entraîner une grande quantité de mémoire est retenue par ces sessions dans l'instance Citrix ADC.
Réutilisation basse session	Non	Indique si le nombre réel de sessions réutilisées par l'instance Citrix ADC est inférieur.
Saturation de carte réseau	Non	Indique le nombre total de paquets rejetés par les interfaces.
TCP reassemble queue limit hits	Non	Indique si les paquets hors service sur une connexion TCP dépassent la taille de la file d'attente de paquets hors commande configurée.

Par défaut, tous les composants sont activés. Si vous désactivez un composant, Citrix ADM effectue le calcul final du score de l'application uniquement en fonction des composants sélectionnés.

> Remarque
>
> Vous pouvez également continuer à configurer les seuils en accédant à **Analytics > Paramètres** et en cliquant sur **Configurer le score de l'application**.

Détails de la demande pour les applications de microservices

February 1, 2024

Cliquez sur une application de microservices dans le tableau de bord pour accéder à des informations plus détaillées.

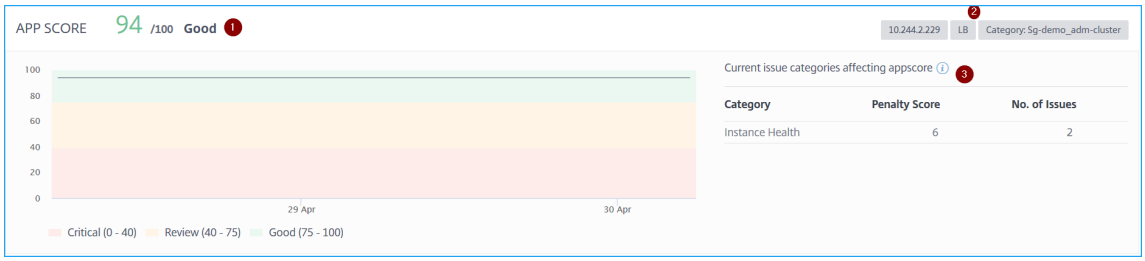
La page de l'application sélectionnée s'affiche.

À partir de la page des détails de l'application :

- Sélectionnez la durée dans la liste pour afficher les détails de la durée spécifique
- Cliquez sur **Graphique de service** pour afficher le graphique de service de l'application sélectionnée. Pour plus d'informations, voir Graphique de service pour les applications
- Cliquez sur **Journaux des transactions** pour afficher les transactions détaillées pour l'application sélectionnée.
- Cliquez sur **Journaux d'audit** pour afficher les informations détaillées du journal d'audit

Après avoir sélectionné la durée, les détails de l'application suivants s'affichent :

- **Score** de l'application —Score de l'application pour la durée sélectionnée. Vous pouvez également afficher les problèmes d'application actuels, qui est connu sous le nom de score de pénalité applicable en fonction de la catégorie de problème. Le score final est calculé comme **100 moins la pénalité totale**.



1 —Indique le score actuel de l'application

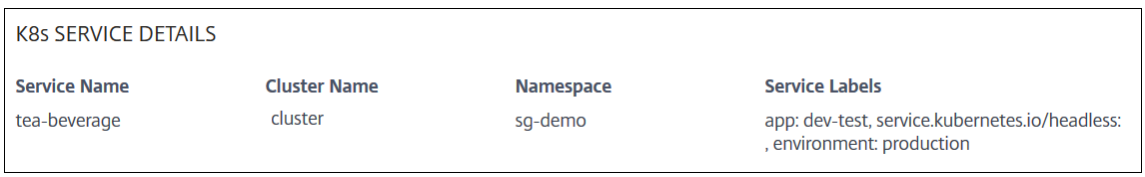
2 —Indique l'adresse IP CPX, le type d'application tel que l'équilibrage de charge ou la commutation de contenu, et l'espace de noms du service et le nom de cluster où le service est hébergé

3 —Indique les problèmes affectant le score de la demande actuelle

Ce tableau de bord vous permet également d'afficher les problèmes actuels qui affectent le score de l'application. Vous pouvez afficher les détails des problèmes sous Problèmes.

- **Détails du service K8s**

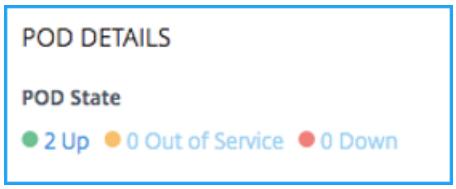
  Vous pouvez consulter les détails suivants :



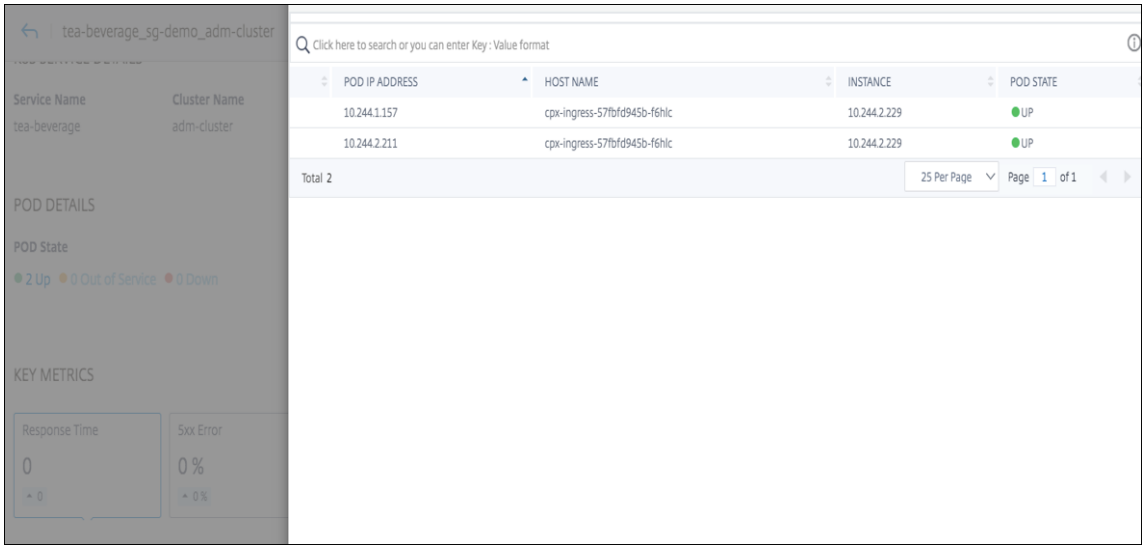
- **Nom du service** : nom du service
- **Nom du cluster** —Nom du cluster où le service est hébergé
- **Espace de noms** : espace de noms attribué au service
- **Étiquettes de service** —Les étiquettes de service attribuées au service

- **Détails du Pod**

  Un conteneur est un groupe de conteneurs hébergés dans le cluster Kubernetes. Dans un conteneur, vous pouvez déployer plusieurs applications conteneurisées. Chaque module est associé à une adresse IP.



  Cliquez sur l'état du conteneur pour afficher les détails

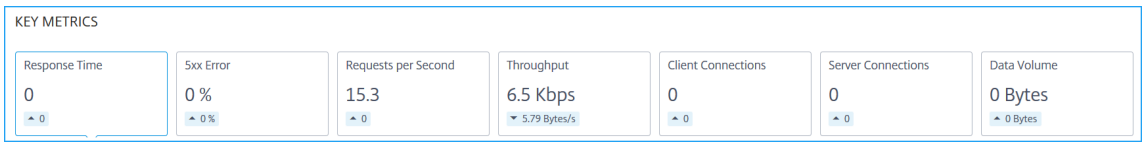


  - **Adresse IP du Pod** —Indique l'adresse IP du Pod
  - **Nom d'hôte** —Indique le nom d'hôte affecté au conteneur
  - **Instance** —Indique l'adresse IP CPX Citrix ADC
  - **état POD** —Indique l'état actuel du conteneur

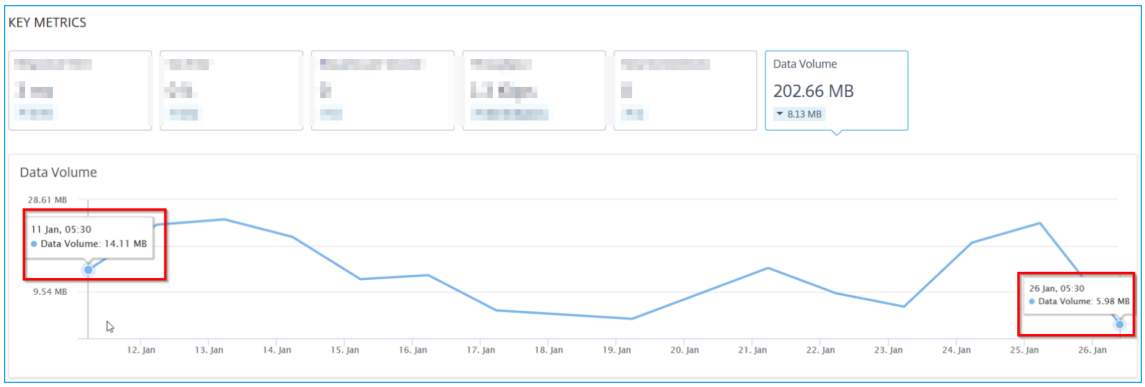
- **Mesures clés** —Les détails des mesures clés, tels que le **temps de réponse**, les **erreurs 5xx**, les **demandes par seconde**, le **débit**, les **connexions client, les connexionsserveur**et le**volume de données**, s'affichent.

Dans chaque mesure, vous pouvez afficher la valeur moyenne et la valeur de différence pour la durée sélectionnée. La valeur de différence est calculée comme la **première valeur moins la dernière valeur** de la durée sélectionnée.

Vous pouvez afficher les mesures d'instance suivantes dans un format graphique pour la durée sélectionnée :



L'image suivante est un exemple de **volume de données** et la durée sélectionnée est de 1 mois. La valeur 202,66 Mo est le volume de données total pour la durée d'un mois et la valeur 8,13 Mo est la valeur de différence. Dans le graphique, la première valeur est 14,11 et la dernière valeur est 5,98. La valeur de la différence est de 14,11 à 5,98 = 8,13 Mo.

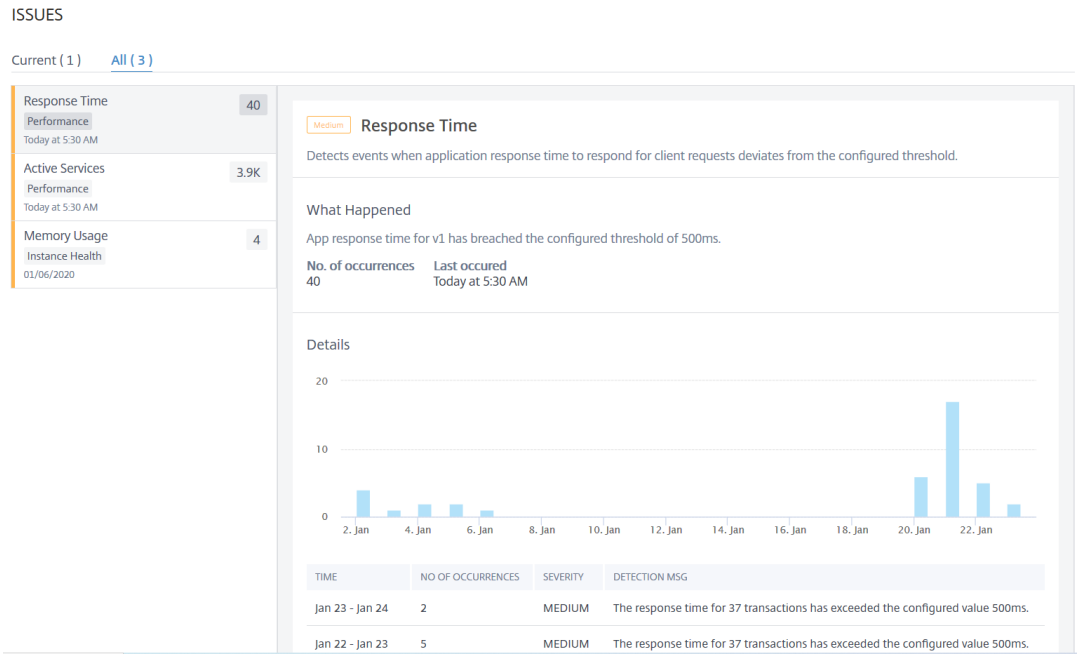


- **Problèmes** —Problèmes applicables à la demande sélectionnée. Vous pouvez afficher les problèmes suivants avec sa catégorie :

Performances	Santé de l'instance	Config	Ressources système
Temps de réponse	Utilisation moyenne du processeur	Réponse élevée 5xx	Type de persistance incorrect
Réutilisation de session faible	Utilisation de la mémoire	Paquets HTTP exceptionnellement volumineux	Saturation de la carte NIC
Accumulation dans la file d'attente de surtension		TCP reassemble queue limit hits	
Trafic SSL en temps réel			

Cliquez sur chaque problème pour afficher les informations suivantes :

- Total des occurrences
- Actions recommandées pour résoudre le problème
- Les détails du problème tels que l'heure, le nom du service, le nombre total d'occurrences, la gravité et le message de détection



  * Les problèmes qui s'affichent dans l'onglet En **cours** font référence aux problèmes de l'application pour la durée sélectionnée.
  * Les problèmes qui s'affichent dans l'onglet **Tous** font référence à l'ensemble des problèmes d'application.

L'exemple suivant présente les problèmes d'application pour une durée d'un jour. L'onglet **Actuel** indique qu'aucun problème actuel n'a d'impact sur le score de l'application.

L'onglet **Tous** affiche le nombre total de problèmes détectés pendant une journée.

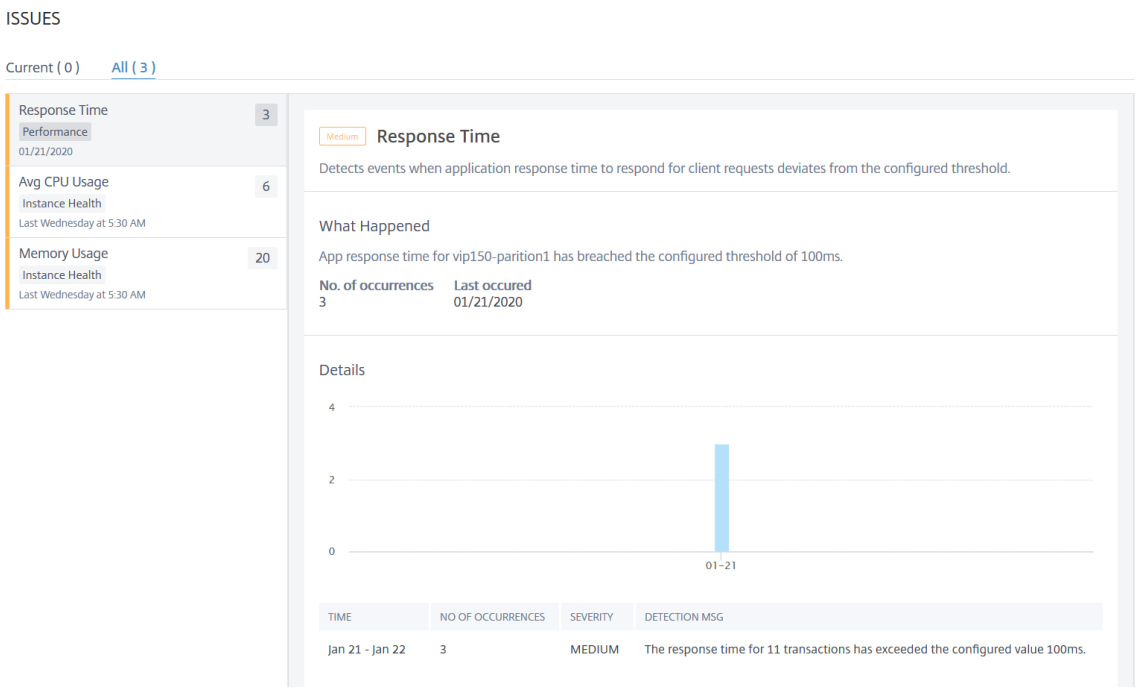


Tableau de bord Web Insight

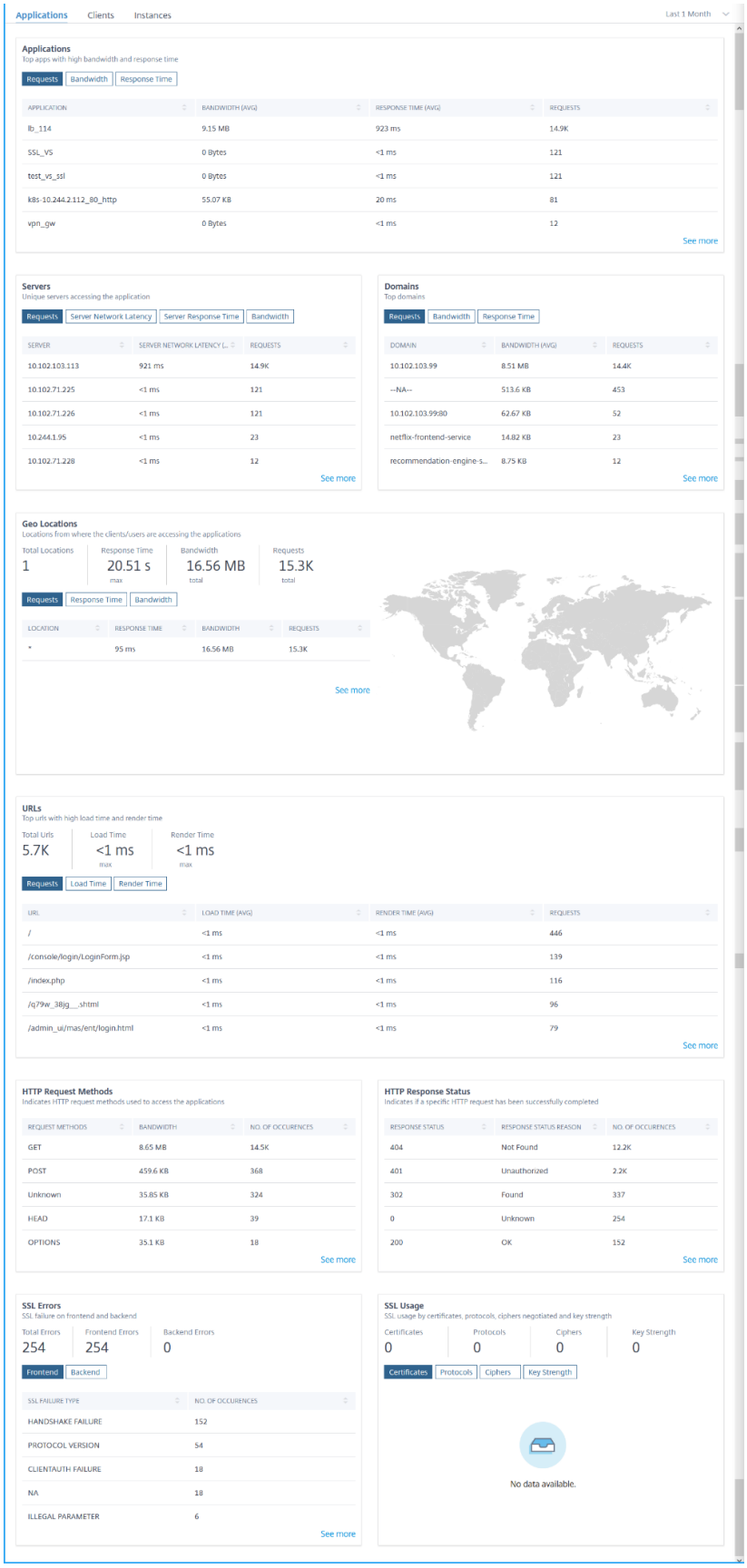
February 1, 2024

La fonctionnalité améliorée de Web Insight est augmentée et fournit une visibilité sur les mesures détaillées pour les applications Web, les clients et les instances Citrix ADC. Cette amélioration Web Insight vous permet d'évaluer et de visualiser l'application complète du point de vue des performances et de l'utilisation ensemble. En tant qu'administrateur, vous pouvez afficher Web Insight pour :

- Une application. Accédez à **Applications > Tableau de bord**, cliquez sur une application, puis sélectionnez l'onglet **Web Insight** pour afficher les mesures détaillées. Pour plus d'informations, consultez Analyse de l'utilisation des applications.
- Toutes les applications. Accédez à **Applications > Web Insight** et cliquez sur chaque onglet (Applications, Clients, Instances) pour afficher les mesures suivantes :

Applications	Clientèle	Instances
Applications	Clientèle	Mesures d'instance
Serveurs	Emplacements géographiques	Applications
Domaines	Méthodes de requête HTTP	Domaines

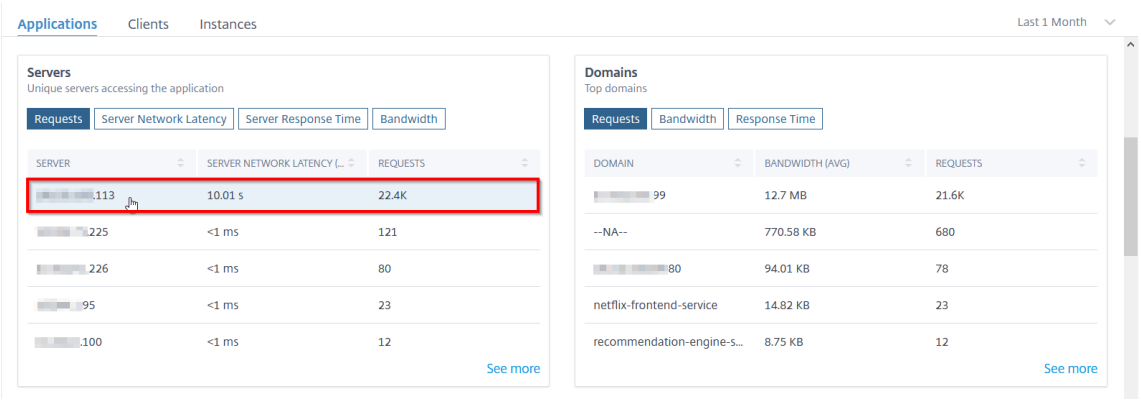
Applications	Clientèle	Instances
Emplacements géographiques	État de la réponse HTTP	URL
URL	URL	Méthodes de requête HTTP
Méthodes de requête HTTP	Système d'exploitation	État de la réponse HTTP
État de la réponse HTTP	Navigateurs	Clientèle
Erreurs SSL	Erreurs SSL	Serveurs
Utilisation de SSL	Utilisation de SSL	Système d'exploitation
		Navigateurs



Dans chaque mesure, vous pouvez voir les 5 meilleurs résultats. Vous pouvez cliquer pour approfondir l'exploration vers le bas pour analyser le problème et prendre des mesures de dépannage plus rapidement.

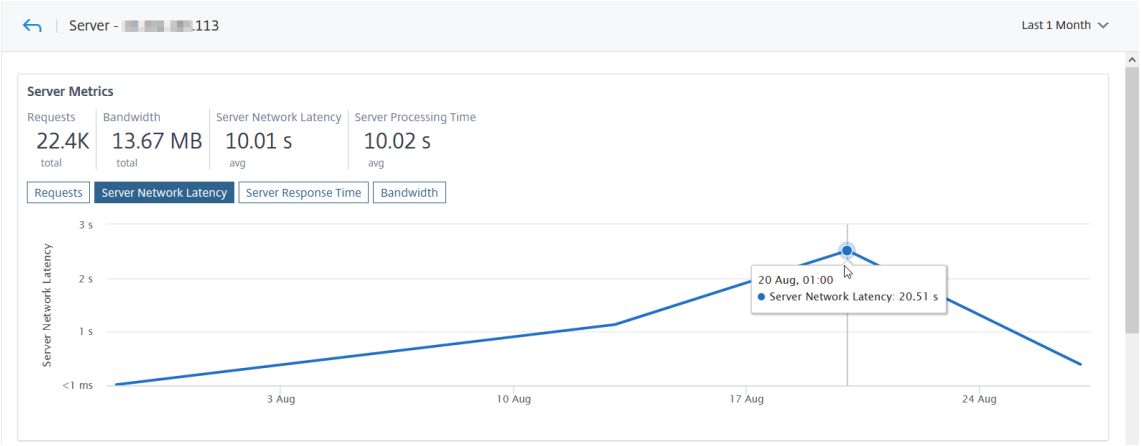
Par exemple, considérez que vous souhaitez analyser la latence du réseau du serveur pour une durée d'un mois et prendre la décision d'augmenter ou de réduire l'environnement de production. Pour analyser ceci :

1. Sélectionnez 1 dernier mois dans la liste et dans l'onglet **Applications**, faites défiler jusqu'à **Serveurs**, puis cliquez sur un serveur.



   Les détails des mesures pour le serveur sélectionné s'affichent.

2. Sélectionnez l'onglet **Latence réseau du serveur** pour analyser la latence.



   La latence moyenne indique 10,01 s et à partir du graphique, vous pouvez analyser que la latence réseau serveur pour le dernier mois semble être élevée. En tant qu'administrateur, vous pouvez prendre la décision d'étendre l'environnement de production.

   Pour plus d'informations sur le cas d'utilisation de Web Insight, consultez Web Insight.

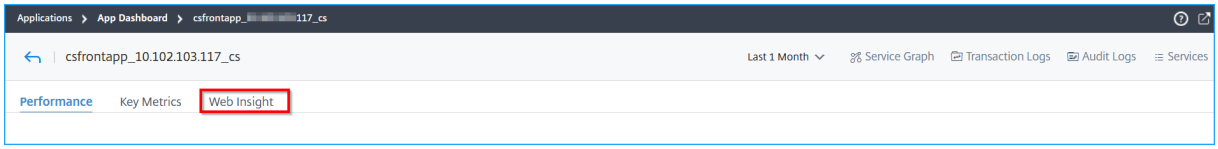
Analyse de l'utilisation des applications

February 1, 2024

Les propriétaires d'applications doivent avoir la capacité d'évaluer et de visualiser l'application complète du point de vue de la performance et de l'utilisation.

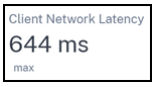
Le tableau de **bord des applications** improvisé vous permet de visualiser toutes les performances de l'application et les mesures d'utilisation ensemble. Lorsque vous cliquez sur une application, parallèlement aux mesures de performances de l'application existantes, l'onglet **Web Insight** affiche les détails des mesures qui vous aident à :

- Comprenez l'utilisation de votre application.
- Corréler les écarts de performances avec les mesures d'utilisation.



Remarque

Pour chaque mesure, vous pouvez afficher les options qui indiquent la valeur maximale et la valeur totale. Par exemple :

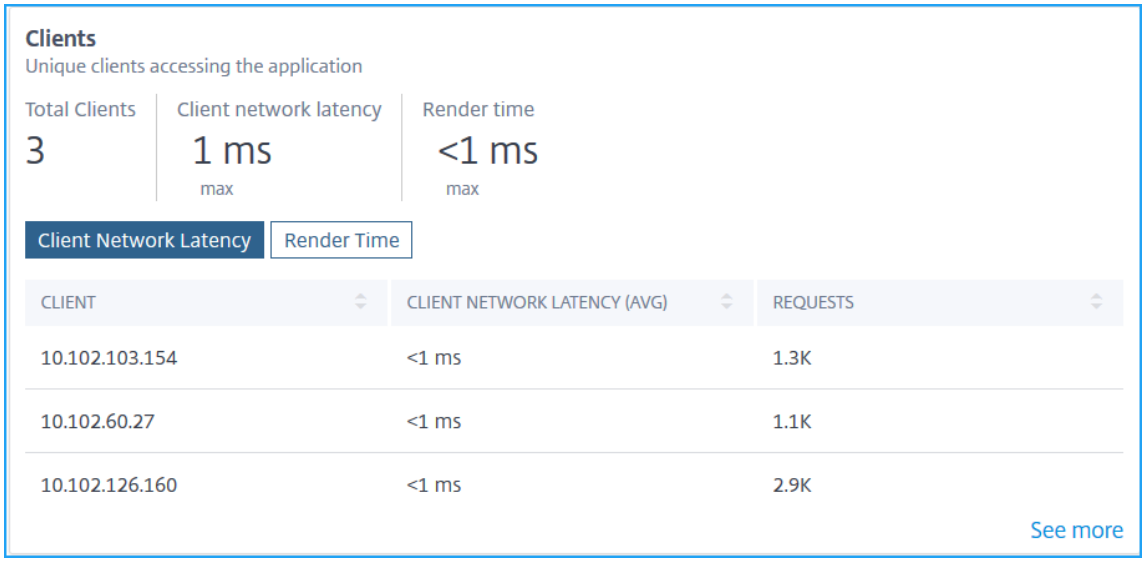
- 

: latence maximale du réseau client pour la durée sélectionnée. Considérez que vous avez la latence réseau pour le client 1 = 30 ms, le client 2 = 15 ms et le client 3 = 3 ms. Dans ce scénario, la **latence réseau client** affiche 30 ms.
- 

- La bande passante totale consommée par tous les clients/serveurs disponibles pendant la durée sélectionnée. Considérez que vous avez la consommation de bande passante pour le client 1 = 30 Mo, Client 2 = 45 Mo, Client 3 = 40 Mo.
Dans ce scénario, la bande passante affiche (30 Mo + 45 Mo + 40 Mo) = 115 Mo.

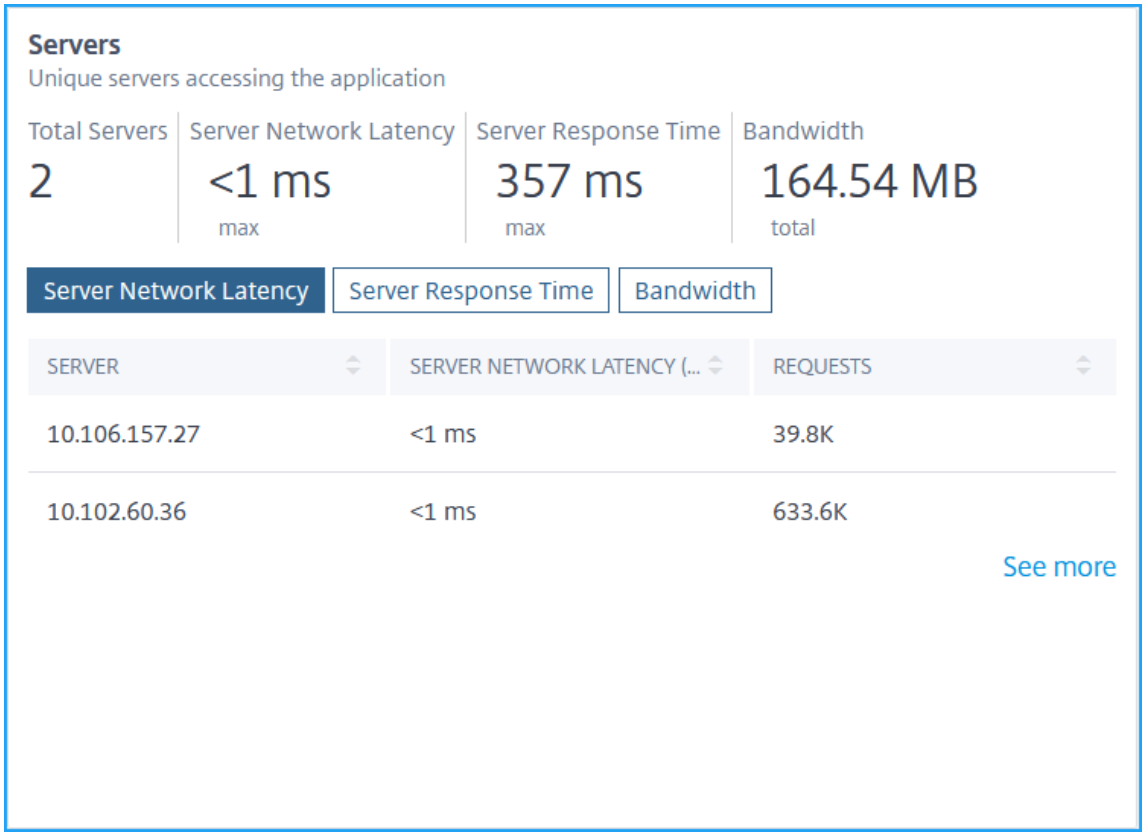
Voici les mesures Web Insight que vous pouvez afficher à partir de l'onglet **Utilisation** :

- **Clients** —Affiche les informations pour les clients accédant à l'application :



- **Total clients** : affiche le nombre total de clients accédant à l'application.
- **Latence réseau client** : affiche la latence réseau du client vers Citrix ADC. Cliquez sur l'onglet **Latence réseau client** pour afficher :
  - **Client** —Adresse IP du client.
  - **Latence réseau client (avg)** : latence réseau moyenne à partir du client.
  - **Demandes** : nombre total de demandes du client.
- **Temps de rendu** : affiche le temps nécessaire pour rendre la réponse du serveur. Cliquez sur l'onglet **Temps de rendu** pour afficher :
  - **Client** —Adresse IP du client.
  - **Temps de rendu (moyenne)** : temps de rendu moyen à partir du client.
  - **Demandes** : nombre total de demandes du client.

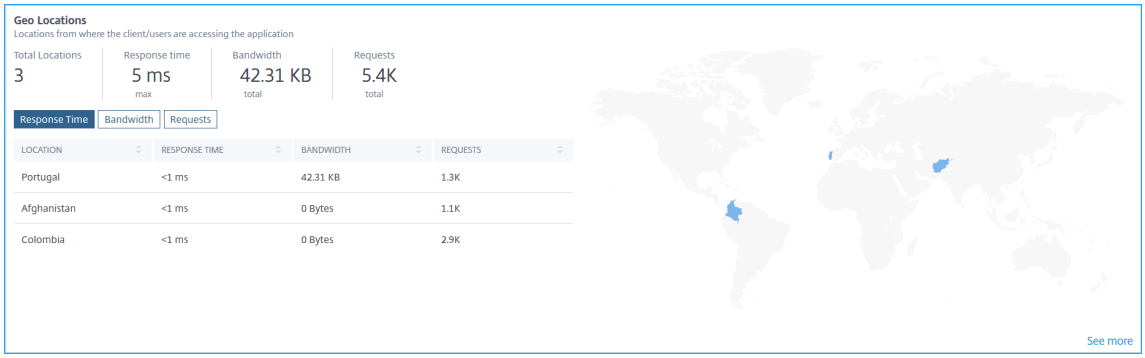
- **Serveurs** : affiche les informations relatives aux serveurs accédant à l'application :



- **Total Serveurs** : affiche le nombre total de serveurs accédant à l'application.
- **Latence réseau du serveur** : affiche la latence réseau du serveur vers Citrix ADC. Cliquez sur l'onglet **Latence réseau du serveur** pour afficher :
  - **Serveur** —Adresse IP du serveur.
  - **Latence réseau du serveur (moy)** : latence réseau moyenne à partir du serveur.
  - **Requêtes** : nombre total de demandes provenant du serveur.
- **Temps de réponse du serveur** : affiche le temps nécessaire au serveur pour répondre aux demandes. Cliquez sur l'onglet **Temps de réponse du serveur** pour afficher :
  - **Serveur** —Adresse IP du serveur.
  - **Temps de réponse (moyenne)** : temps de réponse moyen du serveur.
  - **Requêtes** : nombre total de demandes provenant du serveur.
- **Bande passante** : affiche la bande passante totale consommée par les serveurs. Cliquez sur l'onglet **Bande passante** pour afficher :
  - **Serveur** —Adresse IP du serveur.
  - **Bande passante** : bande passante totale consommée à partir du serveur.

    - **Requêtes** : nombre total de demandes provenant du serveur.

- **Emplacements géographiques** : affiche les informations pour les clients accédant à l'application depuis un emplacement particulier :

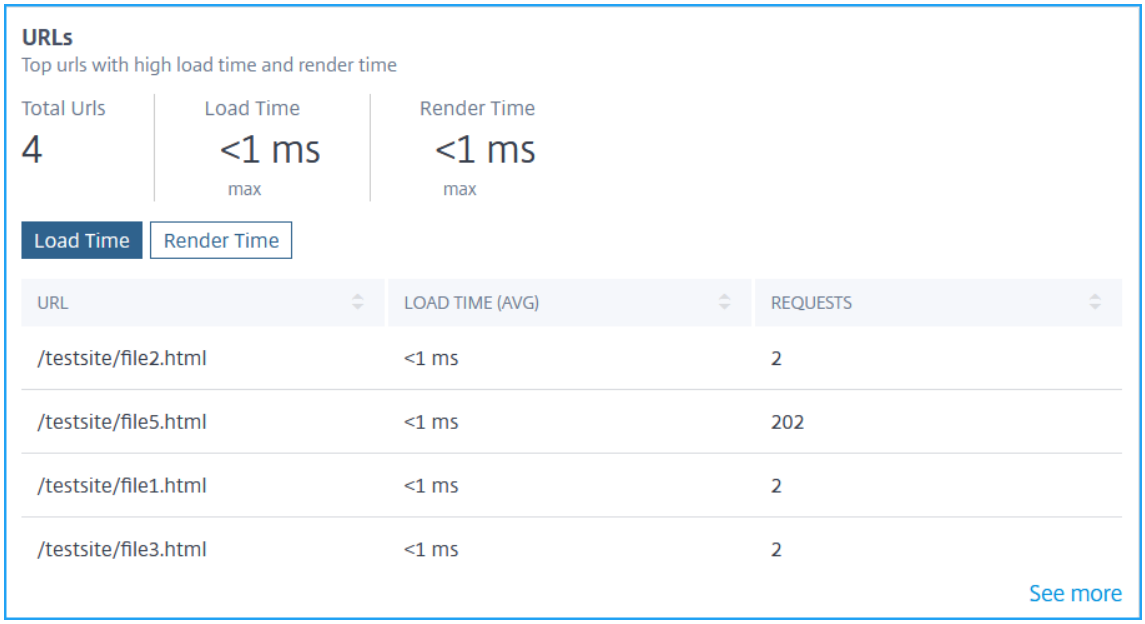


    - **Nombre total d'emplacements** : affiche le nombre total d'emplacements clients accédant à l'application.
    - **Temps de réponse** : affiche le temps de réponse à partir de l'emplacement du client.
    - **Bande passante** : affiche la bande passante totale consommée par les clients dans tous les emplacements.
    - **Demandes** : affiche le nombre total de demandes provenant de tous les emplacements clients.

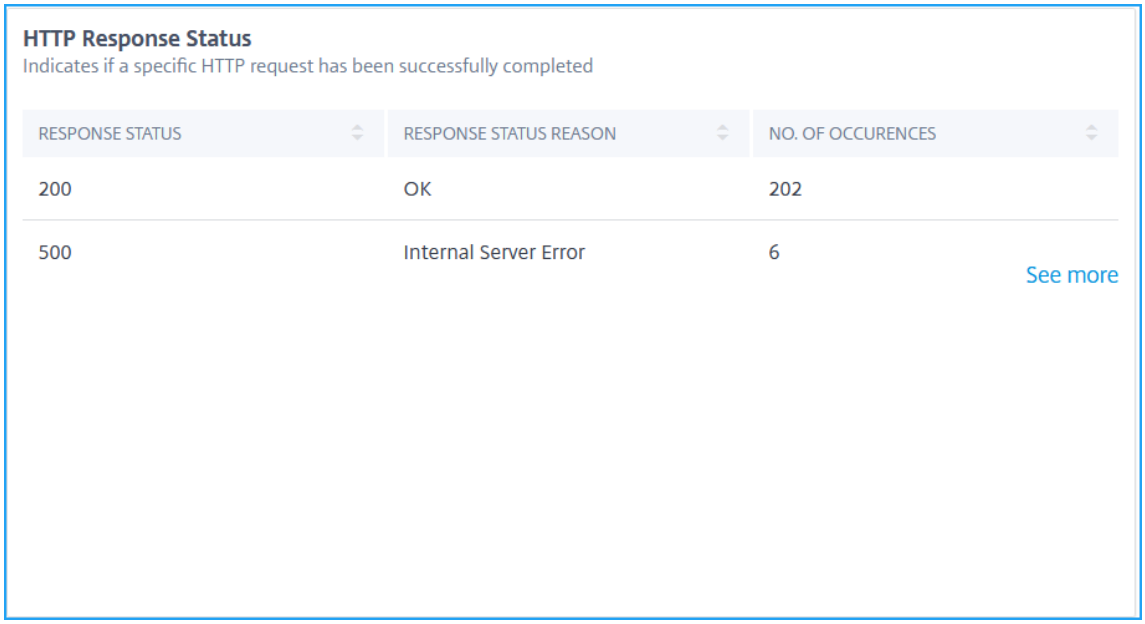
      Cliquez sur chaque onglet pour afficher :

        - **Emplacement** —Nom de l'emplacement.
        - Temps de**réponse : temps** de réponse moyen à partir de l'emplacement du client.
        - **Bande passante** : bande passante consommée à partir de l'emplacement client.
        - **Demandes** : nombre total de demandes provenant de l'emplacement client.

- **URL** : affiche les informations relatives aux URL avec un temps de chargement et de rendu élevés :

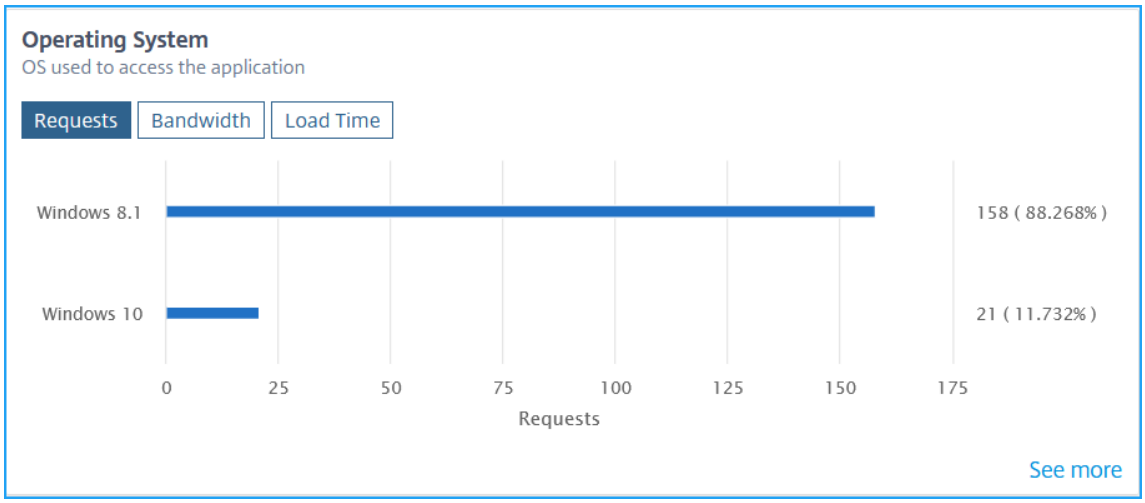


  - **Total des URL** : affiche le total des URL.
  - Temps de chargement : affiche le temps nécessaire au chargement de l'URL. Cliquez sur l'onglet **Temps de chargement** pour afficher :
    - **URL** —Nom de l'URL.
    - **Heure de chargement (moyenne)** : temps moyen de chargement de l'URL.
    - **Requêtes** —Nombre total de demandes provenant de l'URL.
  - **Temps de rendu** : affiche le temps nécessaire pour le rendu et l'affichage de l'URL. Cliquez sur l'onglet **Temps de rendu** pour afficher :
    - **URL** —Nom de l'URL.
    - **Temps de rendu (avg)** : temps moyen de rendu de l'URL.
    - **Requêtes** —Nombre total de demandes provenant de l'URL.
- **Statut de la réponse HTTP** : affiche les informations relatives à une requête HTTP terminée spécifique.



  - **État** de la réponse : affiche le code de réponse tel que 2xx, 4xx, 5xx, etc.
  - **Raison du statut** de la réponse —Affiche le motif de réponse, tel que l'erreur interne du serveur, Introuvable, etc.
  - **Nombre d'occurrences** : affiche le nombre total d'occurrences.

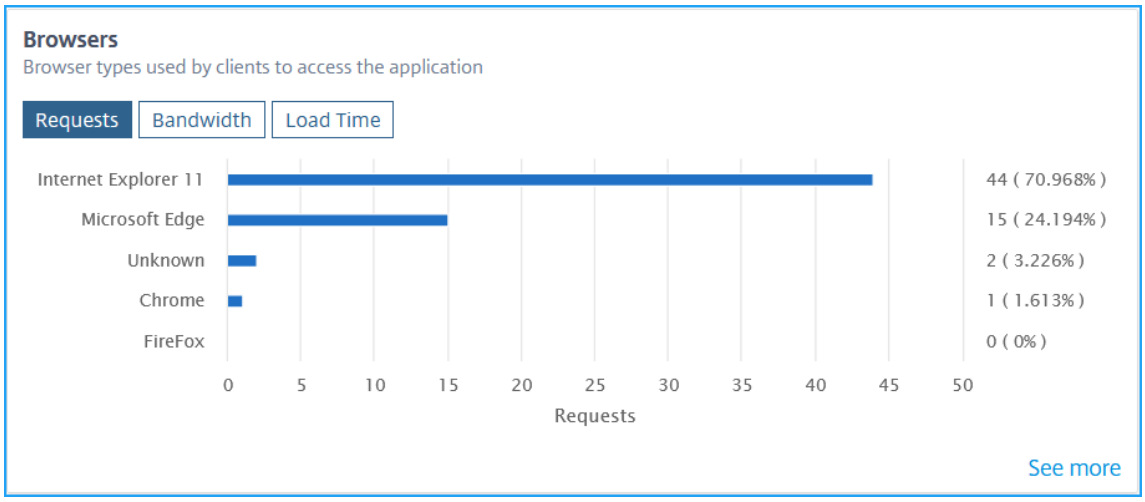
- **Système d'exploitation** : affiche les informations relatives au système d'exploitation qui accède à l'application.



  - **Demandes** : affiche le nombre total de demandes provenant de chaque système d'exploitation.
  - **Bande passante** : affiche la bande passante totale consommée par chaque système d'exploitation.

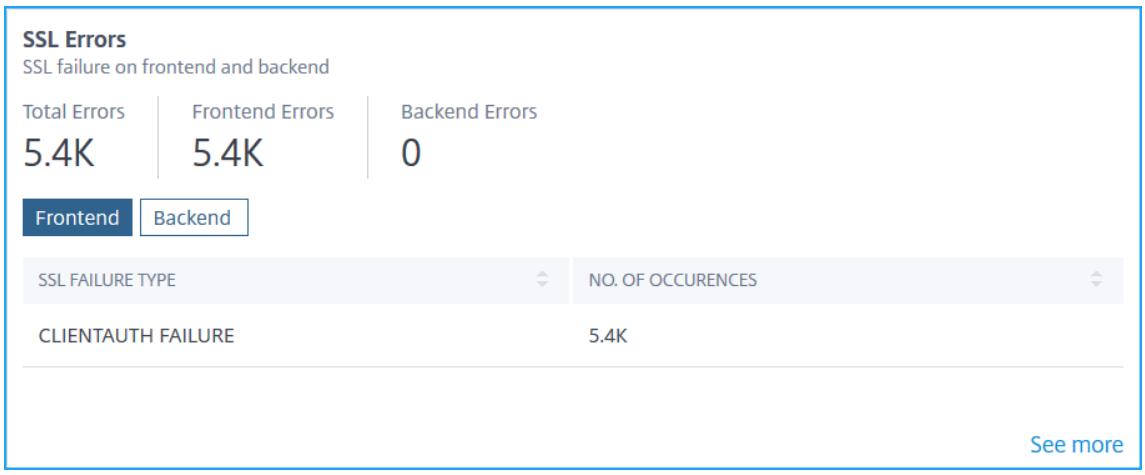
- **Heure de chargement** : affiche le temps total nécessaire à chaque système d'exploitation pour charger à partir du serveur.

- **Navigateurs** : affiche les informations relatives aux types de navigateur utilisés par les clients pour accéder à l'application.



  - **Demandes** : affiche le nombre total de demandes provenant de chaque navigateur.
  - **Bande passante** : affiche la bande passante totale consommée par chaque navigateur.
  - **Temps de chargement** : affiche le temps total nécessaire au chargement d'un navigateur à partir du serveur.

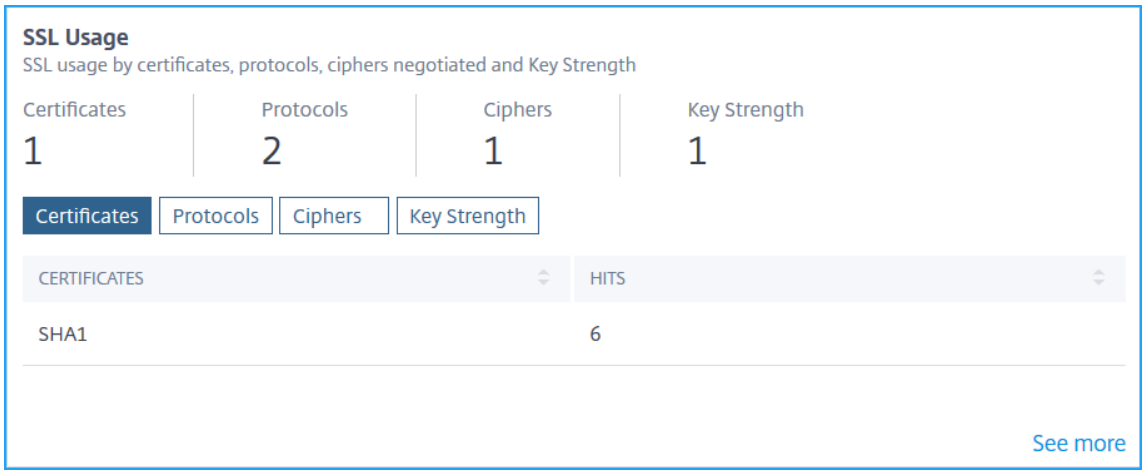
- **Erreurs SSL** —Affiche les informations relatives aux erreurs SSL provenant du serveur frontal et du serveur back-end.



  - **Nombre total d'erreurs** : affiche le total des occurrences d'erreur SSL.
  - **Frontend** —Affiche le total des erreurs SSL du serveur frontal. Cliquez sur l'onglet **Frontend** pour afficher le type d'erreur SSL et le nombre total d'occurrences.

  - **Backend** —Affiche le total des erreurs SSL du serveur principal. Cliquez sur l'onglet **Backend** pour afficher le type d'erreur SSL et le nombre total d'occurrences.

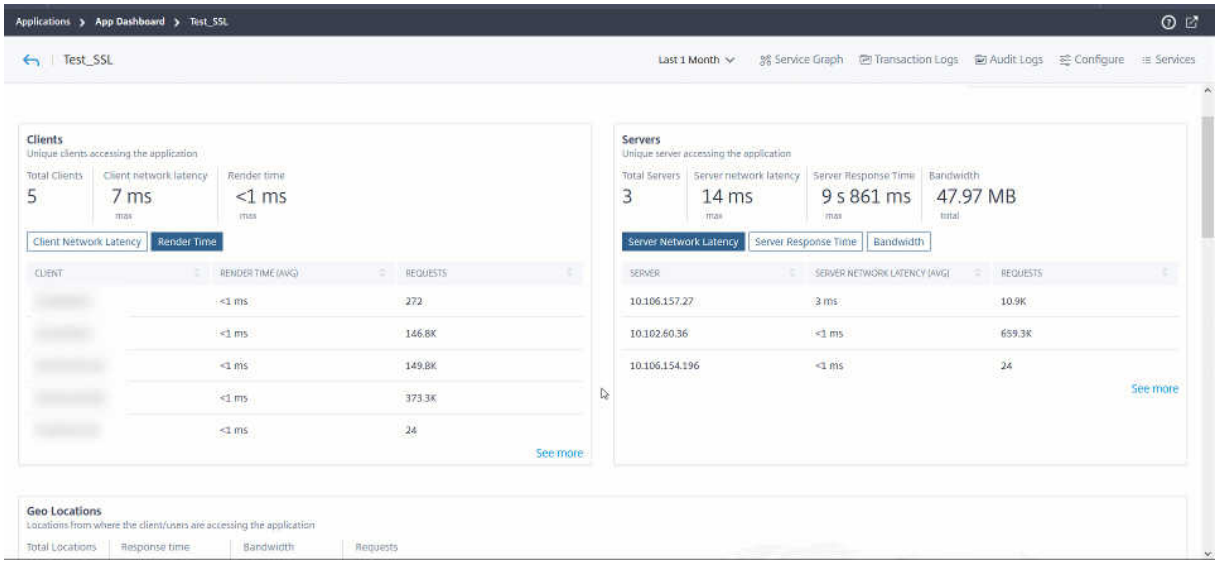
- **Utilisation de SSL** : affiche les informations relatives à l'utilisation du protocole SSL, telles que les certificats SSL, les protocoles, les chiffrements et la force de clé.



  - **Certificats** : affiche le nombre total de certificats SSL. Cliquez sur l'onglet **Certificats** pour afficher le nom du certificat et le nombre total de succès.
  - **Protocoles** : affiche le total des protocoles SSL. Cliquez sur l'onglet **Protocoles** pour afficher les détails avec le protocole SSL/TSL et le nombre total de succès.
  - **Ciphers** : affiche le nombre total de chiffrements. Cliquez sur l'onglet **Ciphers** pour afficher les détails de chaque nom de suite de chiffrement et le nombre total de succès.
  - **Force clé** : affiche la force de clé totale utilisée dans les certificats SSL. Cliquez sur l'onglet **Force clé** pour afficher les détails de chaque force clé et nombre total de coups.

Afficher les détails des mesures au format graphique

Pour chaque mesure, vous pouvez afficher plus de détails dans un format graphique en cliquant sur l'option **Voir plus**. Cliquez sur ** pour afficher les détails dans un format graphique.



Voici les détails que vous pouvez afficher pour chaque mesure après avoir cliqué sur l'option **Voir plus** :

Nom Insight	Métriques	Description
—-	—-	—-
Clients	Clientèle	Indique la liste des clients
	Temps de rendu (AVG)	Indique le temps moyen nécessaire au client pour rendre la réponse du serveur
	Latence réseau client (AVG)	Indique la latence réseau moyenne du client vers l'instance Citrix ADC
	Demandes	Indique le nombre total de demandes du client
Serveurs	Serveur	Indique la liste des serveurs
	Temps de traitement du serveur (AVG)	Indique le temps moyen nécessaire au serveur pour traiter les requêtes
	Latence réseau serveur (AVG)	Indique la latence réseau moyenne entre le serveur et l'instance Citrix ADC
	Accès	Indique le nombre total d'accès reçus par le serveur
Emplacements géographiques	Lieux	Indique les emplacements du client
	Temps de réponse	Indique le temps de réponse total à partir de l'emplacement du client
	Bande passante	Indique la bande passante totale consommée à partir de l'emplacement
	Demandes	Indique le nombre total de demandes provenant de l'emplacement
Adresse URL	Temps de rendu (AVG)	Indique le temps moyen de chargement de la page à partir du serveur
	Temps de chargement (AVG)	Indique le temps moyen nécessaire pour le rendu et l'affichage de l'URL
	Accès	Indique le nombre total d'accès de l'URL
État de la réponse HTTP	Nom	Indique le nom d'état de la réponse tel que OK, Introuvable, Erreur interne du serveur, etc.

	État de la réponse	Indique le code d'état de réponse reçu du serveur tel que 200, 400, 500, etc.
	Accès	Indique le nombre total d'accès du code de réponse
	Bande passante	Indique la bande passante totale consommée
Système d'exploitation	Système d'exploitation	Indique le nom du système d'exploitation tel que Windows, MAC
	Temps de chargement	Indique le temps total nécessaire au chargement du système d'exploitation à partir du serveur
	Bande passante	Indique la bande passante totale consommée par le système d'exploitation
	Demandes	Indique le nombre total de demandes provenant du système d'exploitation
Navigateurs	Navigateurs	Indique le nom du navigateur tel que Mozilla Firefox, Chrome, etc.
	Temps de chargement	Indique le temps total nécessaire au chargement d'un navigateur à partir du serveur
	Bande passante	Indique la bande passante totale consommée par le navigateur
	Demandes	Indique le nombre total de demandes du navigateur
Erreurs SSL	Type de défaillance SSL	Indique le nom de l'erreur, tel que CLIENTAUTH FAILURE
	Occurrences	Indique le nombre total d'occurrences pour l'erreur SSL
Utilisation SSL	Indique le nom du protocole et les versions telles que TLS, SSL
	Hits	Désigne le nombre total d'accès du protocole

Pour plus d'informations sur les cas d'utilisation de Web Insight, consultez Web Insight.

Résoudre les problèmes liés au tableau de bord

February 1, 2024

Après avoir ajouté une application dans le Tableau de bord des applications, le tableau de bord affiche immédiatement les détails de configuration de base de l'application. Les détails de l'analyse des applications tels que le score de l'application, les mesures clés et les problèmes commencent à être remplis en quelques minutes (environ 10 à 15 minutes). Pour plus d'informations, consultez la section Applications.

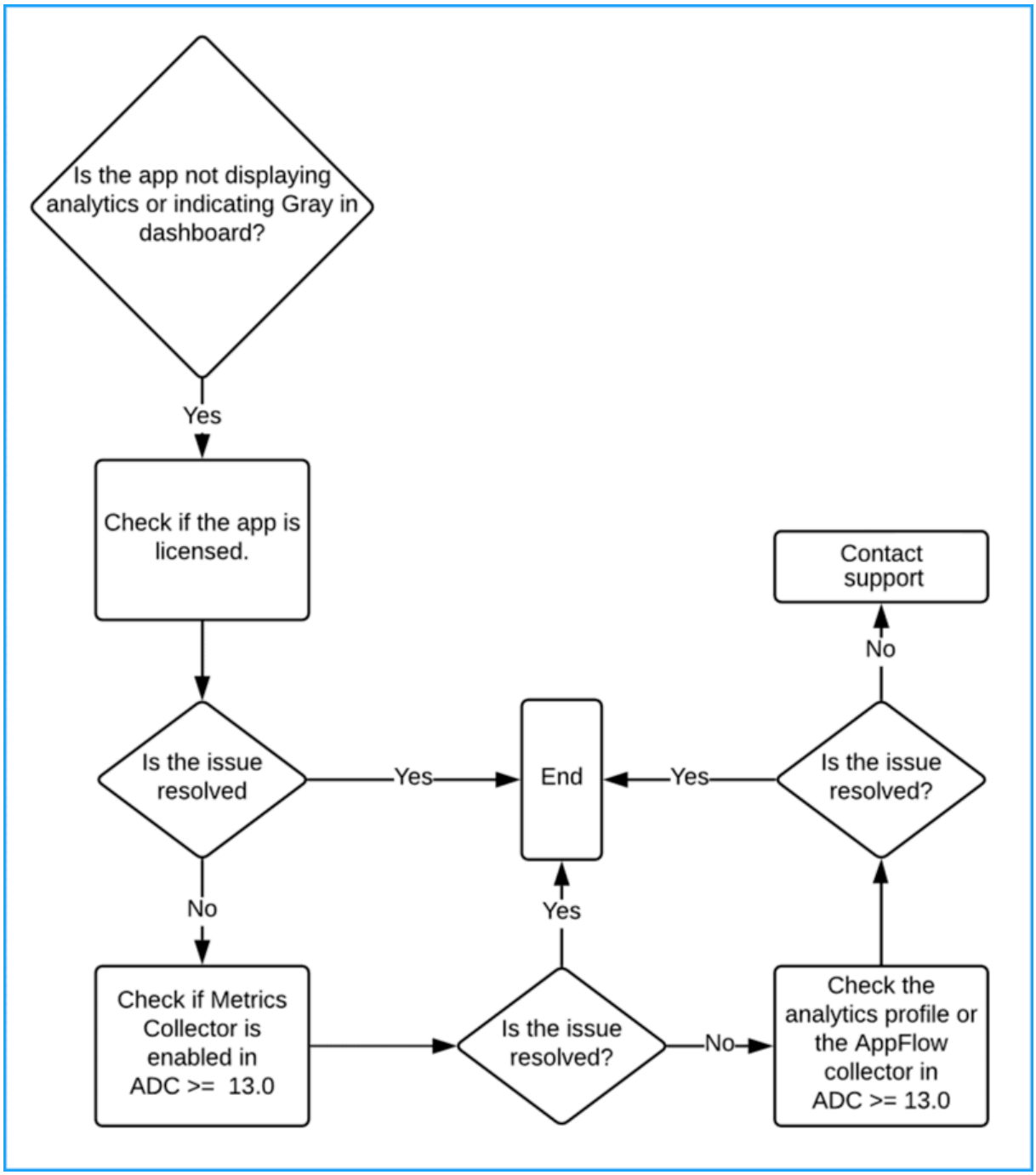
Vous devez vous assurer qu'il n'y a aucun problème avec le flux de données des métriques (collecteur AppFlow ou profil Analytics) à partir de l'instance Citrix ADC. Vous pouvez obtenir plus d'informations sur le collecteur AppFlow et le profil analytique dans ce document.

Ce document décrit les étapes de dépannage que vous devez effectuer lorsque :

- Si vous cliquez sur une application, les analyses de l'application sélectionnée n'affichent pas les données requises même après la durée mentionnée (10 à 15 minutes).
- L'application CS ou LB indique toujours la couleur grise (statut**Non applicable**) dans le Tableau de bord de l'application.

> **Remarque**
>
> Les procédures de dépannage mentionnées dans ce document ne s'appliquent qu'aux serveurs virtuels de **commutation de contenu** et d'**équilibrage de charge**.

Scénario de dépannage



L'application est sous licence

Vous devez vous assurer que l'application est autorisée.

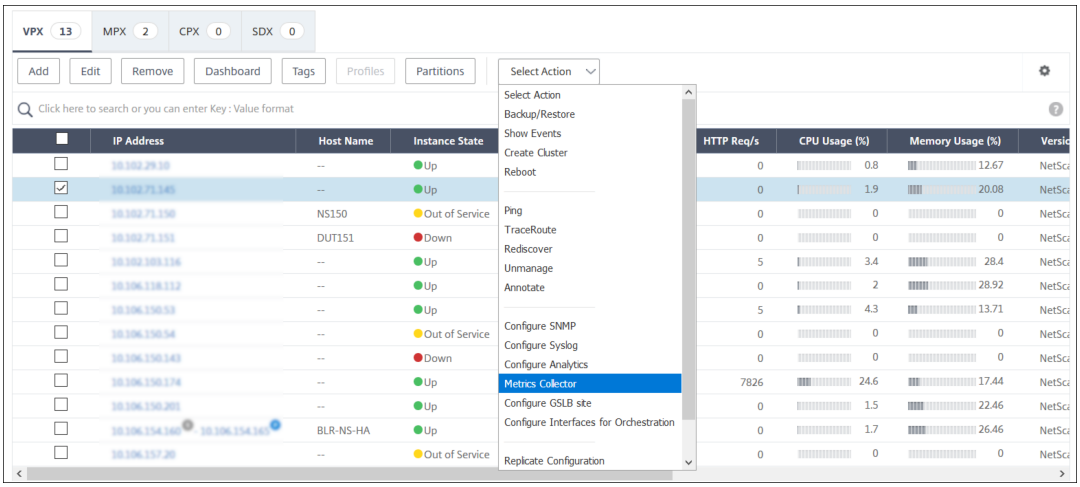
- **Service ADM** - Accédez à **Compte > Abonnements** et vérifiez si l'application est sous licence **Virtual Server License Summary**. Si l'application n'est pas concédée sous licence, consultez Gérer les licences et activer l'analyse sur les serveurs virtuels pour octroyer une licence au serveur virtuel.
- **ADM sur site** — Accédez à **Système > Licensing & Analytics** et vérifiez si l'application est sous licence **Virtual Server License Summary**. Si l'application n'est pas concédée sous licence, consultez Gérer les licences et activer l'analyse sur les serveurs virtuels pour octroyer une licence au serveur virtuel.

Le collecteur de mesures est activé

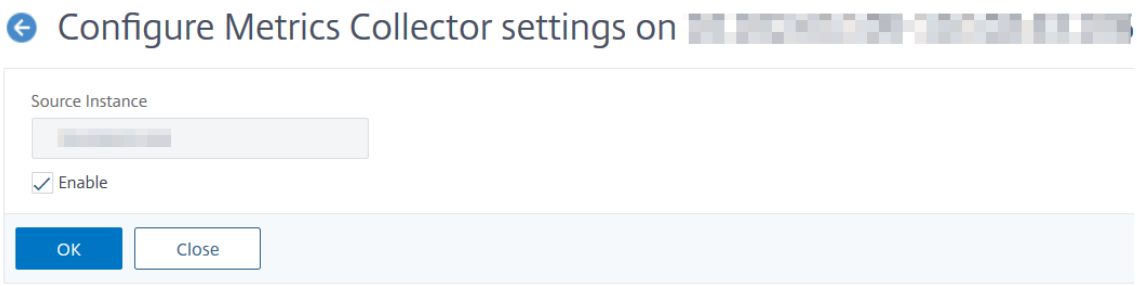
Vous devez vous assurer que **Metrics Collector** est activé dans l'instance Citrix ADC.

Pour Citrix ADC version 13.0 ou ultérieure, Metrics Collector est activé par défaut, une fois l'instance ADC ajoutée avec succès dans ADM. Pour vous assurer que le collecteur de mesures est activé :

1. Accédez à **Réseaux > Instances**. Sous Instances, sélectionnez le type d'instance (par exemple, Citrix ADC VPX).
2. Sélectionnez l'instance de Citrix ADC.
   a) **Dans la liste Sélectionner une action**, sélectionnez **Metrics Collector**.



3. Dans la page **Configurer les paramètres du collecteur** de mesures, vérifiez si l'option **Activer** est sélectionnée. Si ce n'est pas le cas, sélectionnez l'option **Activer** et cliquez sur **OK**.



Après avoir activé le collecteur de mesures et si vous n'êtes toujours pas en mesure d'afficher les données, validez :

- Le collecteur AppFlow de l'instance Citrix ADC version 13.0 **antérieure à la version 47.x** .
- Le profil d'analyse dans l'instance Citrix ADC build **47.x ou version ultérieure**.

Conversion antérieure de l'instance Citrix ADC

Dans Citrix ADC :

1. Exécutez la commande suivante pour vous assurer que le collecteur est **UP** et s'exécute sur le port 5563 :

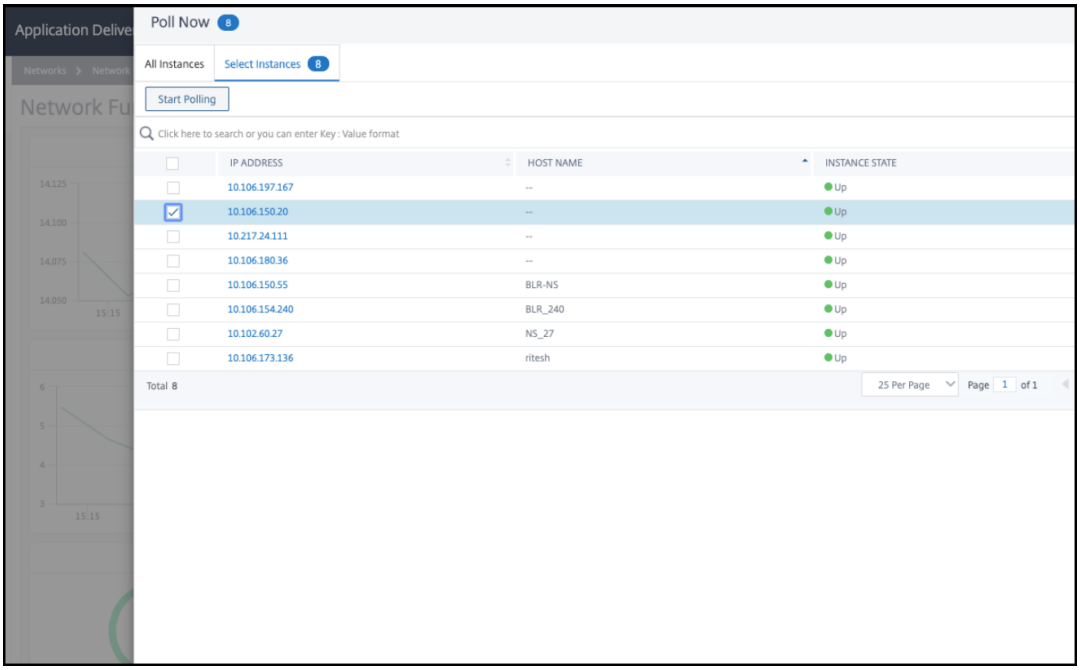
   ```
   sh appflow collector af_collector_rest_<adm_receiver_ip>
   ```

   ```
   > sh appflow collector af_collector_rest_10.102.103.114
   1) Name: af_collector_rest_10.102.103.114
   IPv4 address: 10.102.103.114
   Port: 5563
   Netprofile:
   Transport: rest
   State: UP
   Done
   ```

2. Si aucun collecteur n'est disponible, effectuez une interrogation manuelle d'instance dans Citrix ADM.

   a) Accédez à **Réseaux > Fonction réseau > Sondage maintenant**

   b) Sélectionnez l'instance et cliquez sur **Démarrer l'interrogation**.



Si l'interrogation échoue, supprimez l'instance ADC d'ADM, puis ajoutez à nouveau l'instance ADC. Lorsque vous ajoutez l'instance ADC, le collecteur est ajouté sur ADC.

Si le collecteur indique l'état **Down** :

1. Vérifiez si SNIP est configuré.

```
> sh ip | grep SNIP
2)  10.106.150.34    0              SNIP           Active   Enabled  Enabled  NA      Enabled
```

   Si SNIP n'est pas configuré, vous devez configurer SNIP. Pour plus d'informations, consultez Configuration du SNIP.

2. Assurez-vous que si l'instance ADC est accessible à ADM.

   Vous pouvez valider en effectuant un test ping. Exécutez `ping -S <SNIP> <adm_receiver_ip>`.

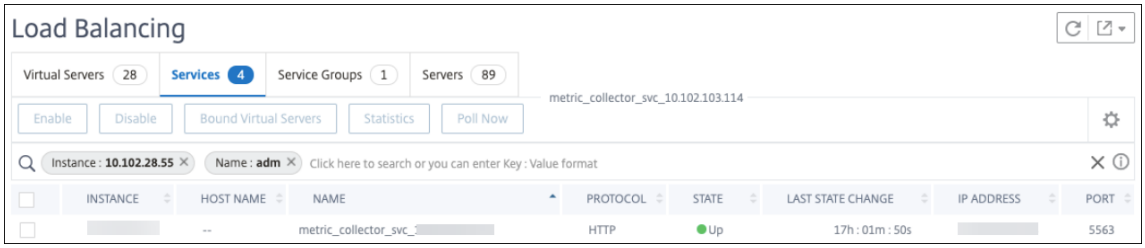
```
> ping -S 10.106.150.34 10.102.103.114
PING 10.102.103.114 (10.102.103.114) from 10.106.150.34: 56 data bytes
64 bytes from 10.102.103.114: icmp_seq=0 ttl=62 time=0.770 ms
64 bytes from 10.102.103.114: icmp_seq=1 ttl=62 time=0.446 ms
64 bytes from 10.102.103.114: icmp_seq=2 ttl=62 time=0.402 ms
```

Instance Citrix ADC versions ultérieures

Dans Citrix ADM, assurez-vous que le service collecteur de mesures est disponible :

1. Accédez à **Réseaux > Fonction réseau > Équilibrage de charge > Services**.
2. Dans la barre de recherche, filtrez par **instance : (adresse IP)** et **Nom : ADM**.
3. Vérifiez si `adm_metric_collector_svc_<adm_receiver ip>` est disponible. L'adresse IP peut être l'adresse IP de gestion ADM ou l'adresse IP de l'agent.

   Assurez-vous que ce service est en état **UP** et s'exécute sur le port 5563.



Si vous ne pouvez toujours pas afficher les données, assurez-vous que le service collecteur est lié au profil d'analyse de séries chronologiques dans Citrix ADC.

1. Connectez-vous à Citrix ADC
2. Exécutez la commande suivante :

   ```
   sh analytics profile ns_analytics_time_series_profile
   ```

```
> sh analytics profile ns_analytics_time_series_profile
1)  Name: ns_analytics_time_series_profile
    Collector: adm_metric_collector_svc_10.102.103.114
    Profile-type: timeseries
        Output Mode: avro
        Metrics: ENABLED
        Events: ENABLED
        Auditlog: DISABLED
    Reference Count: 0
 Done
```

Si le collecteur indique l'état **Down** :

1. Vérifiez si SNIP est configuré.

```
> sh ip | grep SNIP
2)  10.106.150.34    0              SNIP           Active   Enabled  Enabled  NA       Enabled
```

   Si SNIP n'est pas configuré, vous devez configurer SNIP. Pour plus d'informations, consultez Configuration du SNIP.

2. Assurez-vous que si l'instance ADC est accessible à ADM.

Vous pouvez valider en effectuant un test ping. Exécutez `ping -S <SNIP> <adm_receiver_ip>`.

```
> ping -S 10.106.150.34 10.102.103.114
PING 10.102.103.114 (10.102.103.114) from 10.106.150.34: 56 data bytes
64 bytes from 10.102.103.114: icmp_seq=0 ttl=62 time=0.770 ms
64 bytes from 10.102.103.114: icmp_seq=1 ttl=62 time=0.446 ms
64 bytes from 10.102.103.114: icmp_seq=2 ttl=62 time=0.402 ms
```

3. Assurez-vous que la connectivité du trafic via telnet est capable de connecter le service.

```
root@ns# telnet 10.102.103.114 5563
Trying 10.102.103.114...
Connected to 10.102.103.114.
Escape character is '^]'.
^]
telnet> q
Connection closed.
```

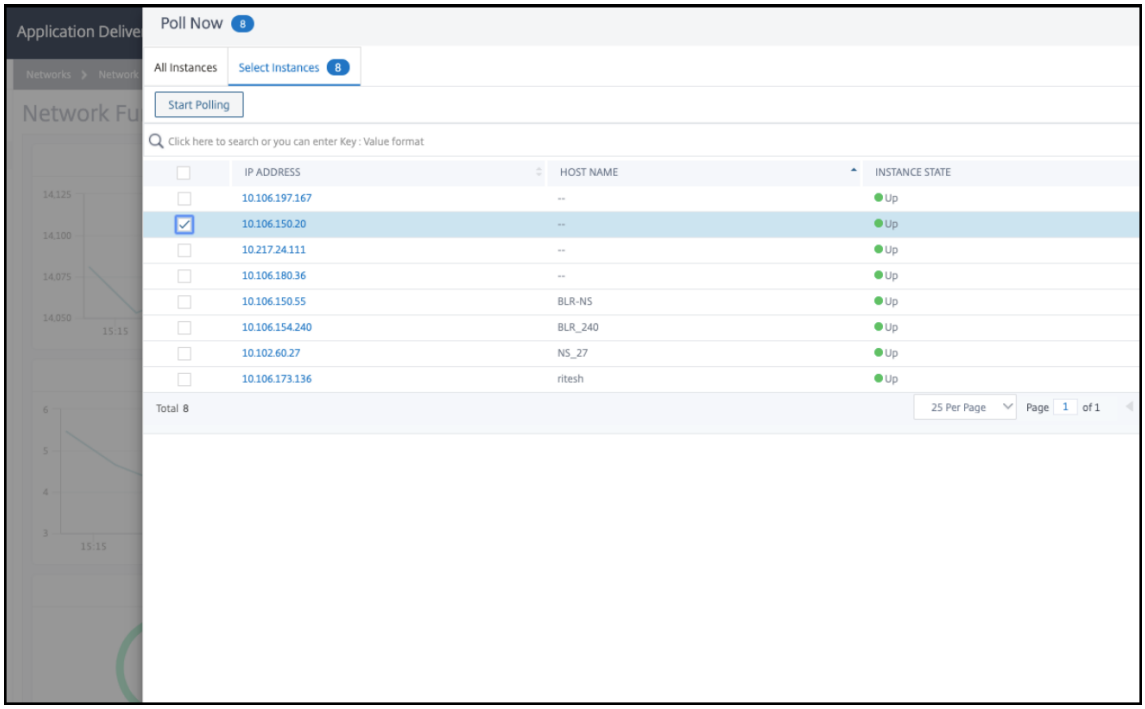
Si telnet est capable de connecter le service, un pare-feu existe et bloque le flux de données de mesure. Vous devez résoudre le problème de blocage du pare-feu.

Si aucun service de collecteur n'est lié au profil analytique de séries chronologiques dans Citrix ADC, le collecteur s'affiche comme vide.

```
> sh analytics profile ns_analytics_time_series_profile
1)  Name: ns_analytics_time_series_profile
    Collector:
    Profile-type: timeseries
        Output Mode: avro
        Metrics: ENABLED
        Events: ENABLED
        Auditlog: DISABLED
    Reference Count: 0
 Done
```

Vous devez effectuer une interrogation manuelle d'instance dans Citrix ADM.

1. Accédez à **Réseaux > Fonction réseau > Sondage maintenant**
2. Sélectionnez l'instance et cliquez sur **Démarrer l'interrogation**.



Si l'interrogation échoue, ajoutez le service collector directement à l'instance Citrix ADC à l'aide des commandes suivantes :

```
add service adm_metric_collector_svc_<adm_receiver_ip> <adm_receiver_ip
> HTTP 5563
```

```
unset analyticsprofile ns_analytics_time_series_profile -collectors
```

```
set analytics profile ns_analytics_time_series_profile -collectors
 adm_metric_collector_svc_<adm_receiver_ip> -metrics enabled -
events enabled
```

Le profil des séries chronologiques analytiques est mis à jour.

```
> add service adm_metric_collector_svc_10.102.103.114 10.102.103.114 HTTP 5563
 Done
> unset analyticsprofile ns_analytics_time_series_profile  -collectors
 Done
> set analytics profile ns_analytics_time_series_profile -collectors adm_metric_collector_svc_10.102.103.114 -metrics enab
 Done
> sh analytics profile ns_analytics_time_series_profile
1)  Name: ns_analytics_time_series_profile
    Collector: adm_metric_collector_svc_10.102.103.114
    Profile-type: timeseries
        Output Mode: avro
        Metrics: ENABLED
        Events: ENABLED
        Auditlog: DISABLED
    Reference Count: 0
 Done
```

Si le problème persiste même après avoir effectué toutes les étapes de dépannage mentionnées, con-

tactez le **support Citrix**.

Créer un seuil et une alerte pour l'analyse des applications

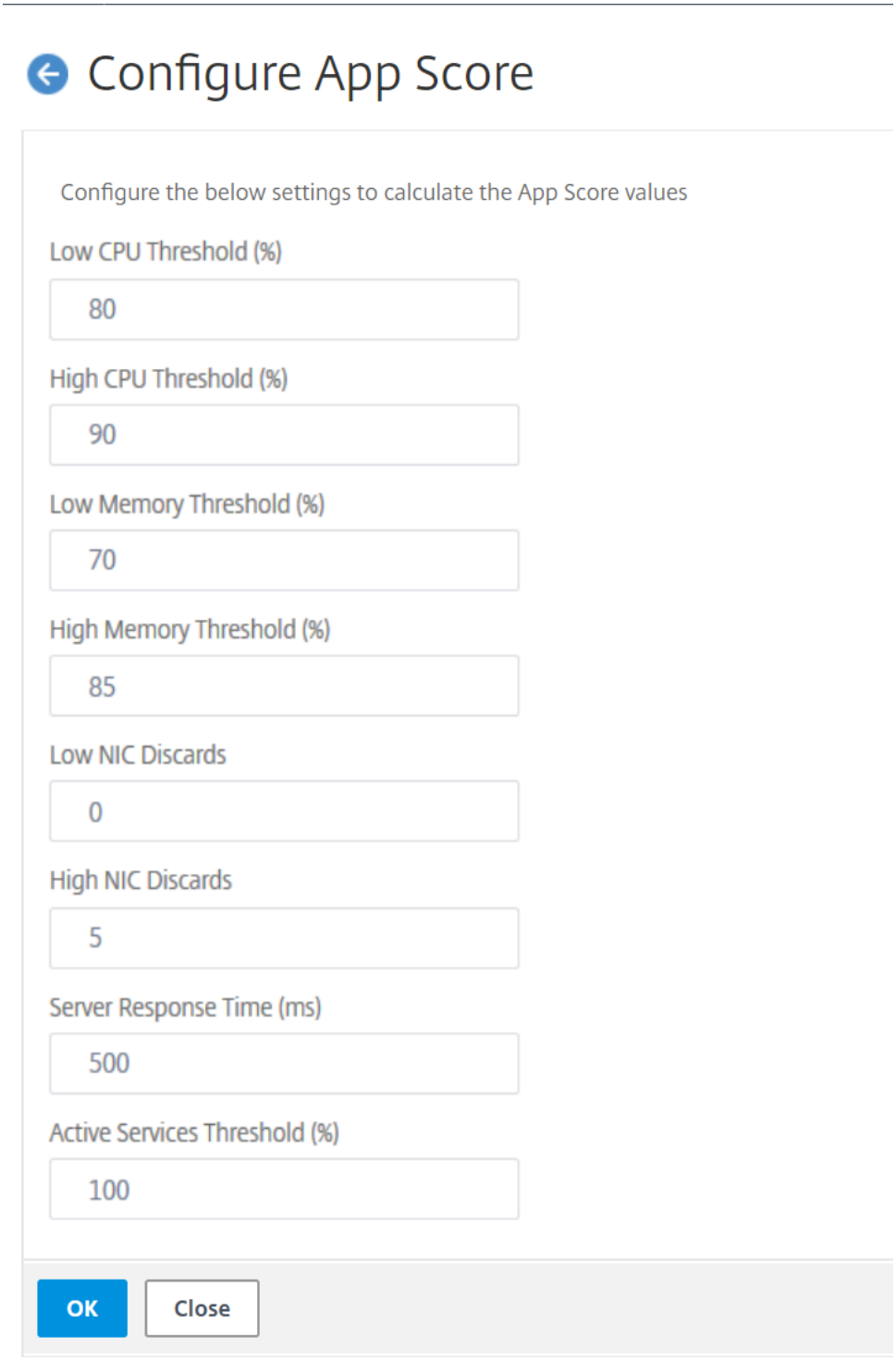
February 1, 2024

L'analyse des applications sur Citrix ADM vous permet de surveiller les différents types de trafic passant par les instances Citrix ADC. Citrix ADM vous permet de définir des seuils sur les compteurs suivants pour surveiller le trafic et le score d'application.

Vous pouvez configurer des seuils et surveiller le score de l'application pour le processeur, la mémoire, les défausses de carte réseau et le temps de réponse.

Pour configurer le score d'application dans Citrix ADM :

1. Dans Citrix ADM, accédez à **Analytics** > **Paramètres** .
2. Dans la page **Paramètres**, cliquez sur **Configurer le score de l'application**.
3. Sur la page **Configurer le score d'application**, entrez les valeurs des paramètres suivants :
    a) **Seuil de CPU faible**. Valeur de seuil inférieure de l'utilisation totale de l'UC dans l'instance de Citrix ADC.
    b) **Seuil CPU élevé**. Valeur de seuil plus élevée de l'utilisation totale de l'UC dans l'instance de Citrix ADC.
    c) **Seuil de mémoire faible**. Valeur de seuil inférieure de l'utilisation totale de la mémoire dans l'instance de Citrix ADC.
    d) **Seuil de mémoire élevé**. Valeur de seuil plus élevée de l'utilisation totale de la mémoire dans l'instance de Citrix ADC.
    e) **SLA de rejets de carte réseau faible**. La valeur seuil inférieure des paquets rejetés par les interfaces.
    f) **SLA de rejst de carte réseau élevé**. La valeur seuil la plus élevée des paquets rejetés par les interfaces.
    g) **Temps de réponse**. Intervalle de temps entre l'envoi d'un paquet de requête et la réception du premier paquet de réponse à partir du service configuré sur le serveur virtuel. La valeur par défaut configurée dans Citrix ADM est 500 ms.
    h) **Seuil des services actifs**. Valeur de seuil du pourcentage de services qui doivent être actifs et qui sont liés au serveur virtuel.



4. Cliquez sur **OK**.

Analyses intelligentes des applications

February 1, 2024

Intelligent App Analytics vous permet d'identifier les problèmes de performances des applications à l'aide d'algorithmes basés sur des règles et d'apprentissage automatique. La fonctionnalité Intelligent App Analytics de Citrix ADM :

- Fournit une solution simple et évolutive pour la surveillance et le dépannage des applications fournies via des instances Citrix ADC.
- Surveille tous les niveaux des applications afin de réduire les délais de résolution des problèmes et d'améliorer la disponibilité globale des applications.

Dans un déploiement classique, des milliers de serveurs répondent aux besoins en données des utilisateurs. Le trafic envoyé à ces serveurs est équilibré en charge et surveillé par des serveurs virtuels configurés sur les appliances Citrix ADC. Chaque serveur virtuel est lié à plusieurs services représentant les serveurs principaux. Dans de tels déploiements, la fonctionnalité Intelligent App Analytics vous aide à :

- Surveillez, gérez et prenez des décisions lors de pannes et d'autres événements
- Surveillez les serveurs virtuels et les services configurés pour une application
- Affichez des informations critiques sur les serveurs et services virtuels, afin que vous puissiez modifier les configurations selon vos besoins afin d'obtenir des performances optimales des applications.

Lorsque vous agrandissez le parc de serveurs de votre organisation, il devient difficile de suivre les problèmes liés à l'énorme volume de trafic reçu sur les serveurs et de se limiter à la résolution des problèmes nécessaires.

Lorsqu'une application est en cours d'exécution et reçoit un trafic important, vous pouvez rencontrer divers problèmes. Vous pouvez afficher les indicateurs de performances pour l'analyse des applications en accédant à **Applications** > **Tableau de bord**, en sélectionnant une application et en faisant défiler vers le bas pour afficher les problèmes dans la section **Problèmes**.

Configurer l'analyse intelligente des applications

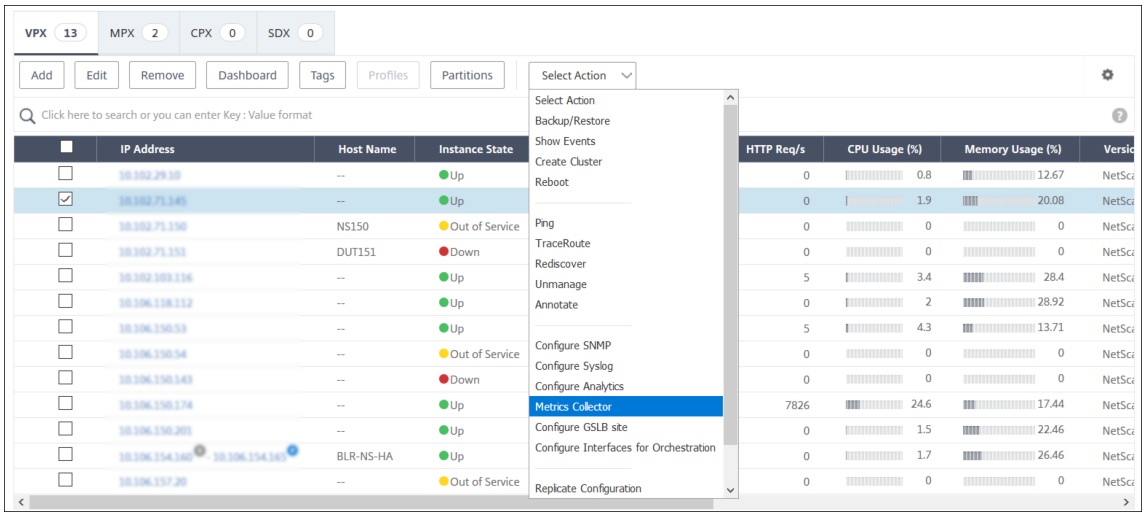
February 1, 2024

La fonctionnalité Intelligent App Analytics est prise en charge uniquement dans **Citrix ADC 12.1.50.x ou version ultérieure**. **Metrics Collector** transmet les données du compteur Citrix ADC à Citrix ADM,

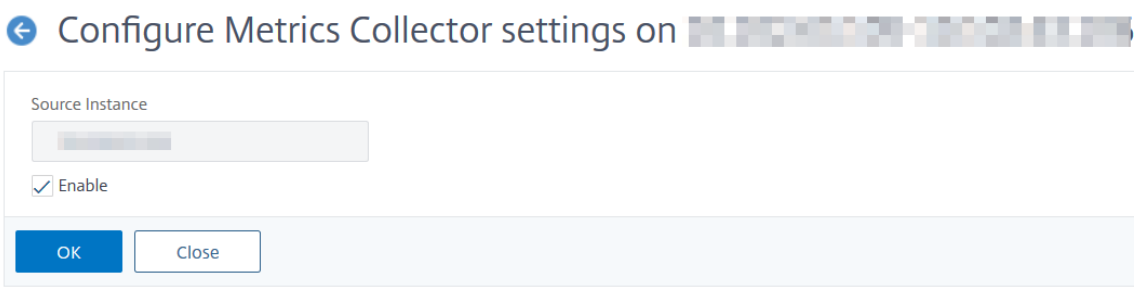
qui est utilisé pour détecter les problèmes d'application. Pour utiliser la fonctionnalité Intelligent App Analytics, **Metrics Collector** doit être configuré sur chaque instance Citrix ADC. Par défaut, **Metrics Collector** est activé sur Citrix ADC, tandis que vous ajoutez l'instance à Citrix ADM.

Pour vérifier si **Metrics Collector** est activé :

1. Accédez à **Réseaux** > **Instances** > **Citrix ADC** et sélectionnez le type d'instance à surveiller (par exemple, Citrix ADC VPX).
2. Sélectionnez l'instance de Citrix ADC.
3. **Dans la liste Sélectionner une action**, sélectionnez **Metrics Collector**.



4. Sur la page des **paramètres de Configurer Metrics Collector**, l'option **Activer** est sélectionnée par défaut. Si cette option n'est pas sélectionnée, veillez à sélectionner l'option **Activer**, puis cliquez sur **OK**.



> **Remarque**
>
> Pour afficher les anomalies relatives aux **erreurs de serveur** et à sa **transaction Web détaillée**, vous devez activer l'analyse sur les serveurs virtuels.

Indicateurs de performance pour l'analyse des applications

February 1, 2024

Vous pouvez afficher les indicateurs de performances, ainsi que les catégories qui se produisent dans les applications Web Citrix ADC. Pour afficher ces indicateurs, vous devez vous assurer d'activer le collecteur d'analyses et de mesures sur l'instance ADC :

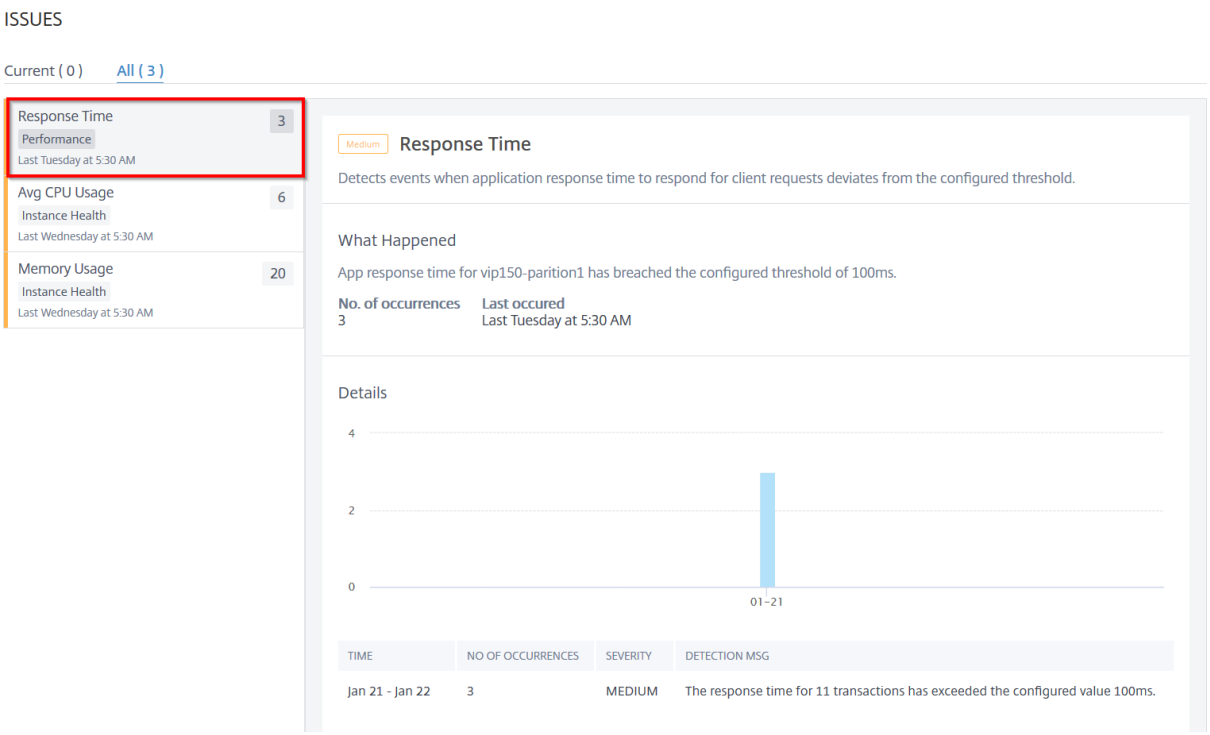
Après avoir activé le collecteur d'analyses et de mesures, vous pouvez afficher les indicateurs suivants en accédant à **Applications** > **Tableau de bord**, en sélectionnant une application et en faisant défiler jusqu'à la section **Problèmes** :

- Temps de réponse
- Services actifs
- Utilisation moyenne du processeur
- Utilisation de la mémoire
- Saturation de la carte NIC
- Bagotement du service
- Réutilisation de session faible
- Type de persistance incorrect
- Serveur instable (5xx)
- Trafic SSL en temps réel
- Paquets HTTP exceptionnellement volumineux
- Limites de file d'attente de réassemblage TCP
- Accumulation dans la file d'attente de surtension

Temps de réponse

February 1, 2024

Ce problème détecte lorsque le temps de réponse de l'application aux demandes des clients s'écarte de la valeur seuil configurée. Cliquez sur l'onglet **Temps de réponse** pour afficher les détails du problème.



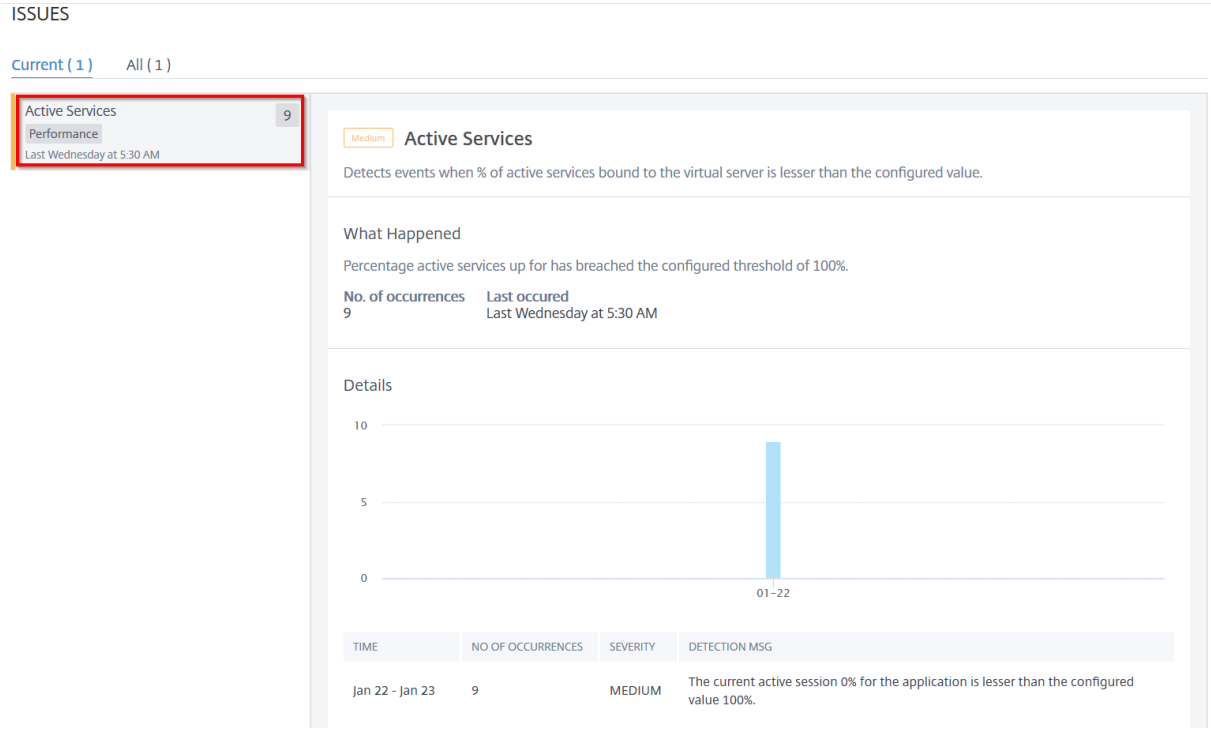
Sous **Détails**, vous pouvez afficher :

- Le graphique indiquant le nombre total d'événements pour la période sélectionnée. Cliquez pour appliquer le filtre et afficher les détails
- Lorsque le problème est survenu
- Le nombre total d'occurrences pour la période sélectionnée
- La gravité du problème, par exemple faible, moyen et élevé
- Message de détection indiquant le temps de réponse total de la transaction dépassant la valeur de seuil configurée

Services actifs

February 1, 2024

Ce problème est détecté lorsque le % de services actifs liés au serveur virtuel est inférieur à la valeur seuil configurée. Cliquez sur l'onglet **Services actifs** pour afficher les détails du problème.



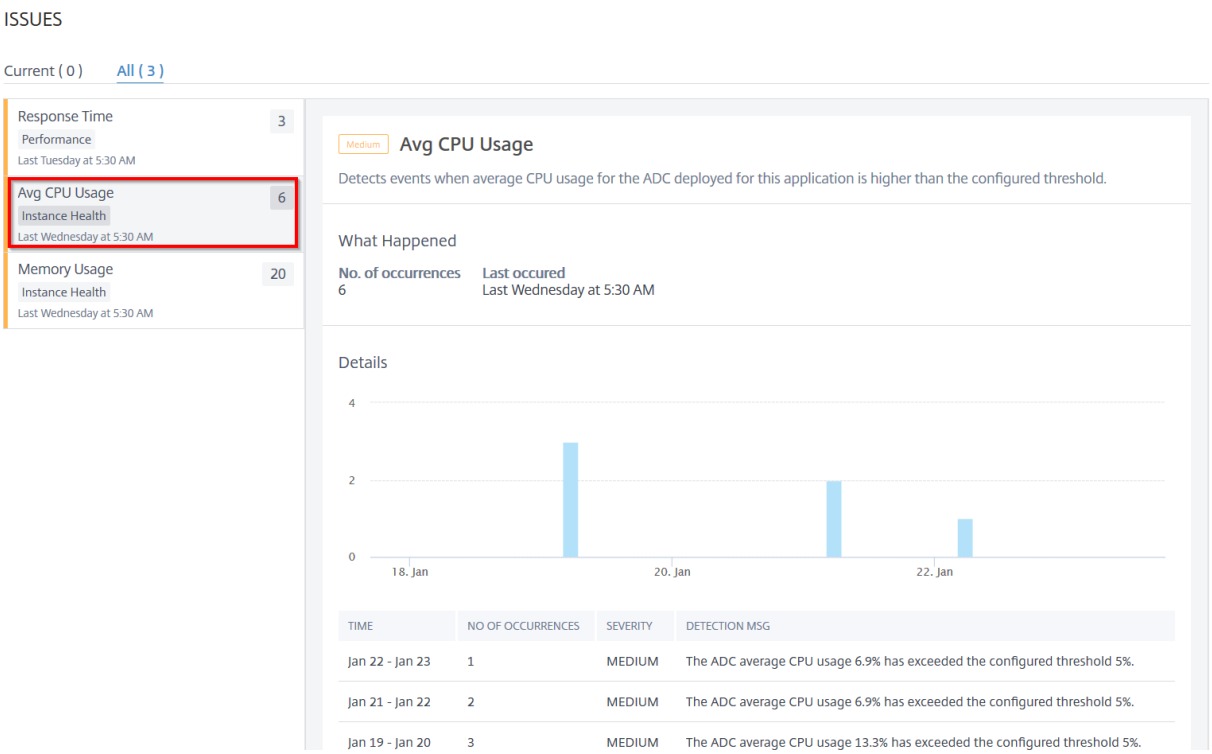
Sous **Détails**, vous pouvez afficher :

- Le graphique indiquant le nombre total d'événements pour la durée sélectionnée. Cliquez pour appliquer le filtre et afficher les détails
- Lorsque le problème est survenu
- Le nombre total d'occurrences pour la durée sélectionnée
- La gravité du problème, par exemple faible, moyen et élevé
- Le message de détection indiquant le pourcentage de sessions de service actives et la valeur de seuil configurée

Utilisation moyenne du processeur

February 1, 2024

Ce problème est détecté lorsque l'utilisation du processeur ADC pour cette application dépasse la valeur seuil configurée. Cliquez sur l'onglet **Utilisation moyenne du processeur** pour afficher les détails du problème.



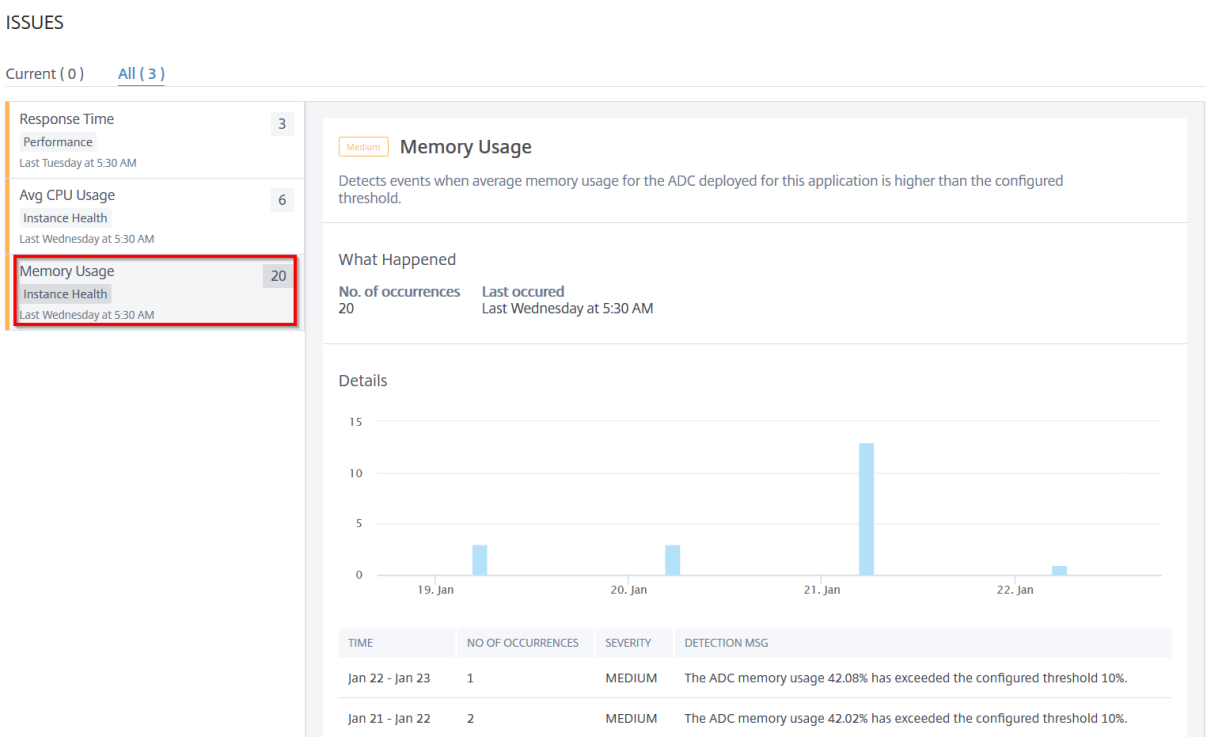
Sous **Détails**, vous pouvez afficher :

- Le graphique indiquant le nombre total d'événements pour la durée sélectionnée. Cliquez pour appliquer le filtre et afficher les détails
- Lorsque le problème est survenu
- Le nombre total d'occurrences pour la durée sélectionnée
- La gravité du problème, par exemple faible, moyen et élevé
- Le message de détection indiquant le % d'utilisation moyenne du processeur ADC et la valeur de seuil configurée

Utilisation de la mémoire

February 1, 2024

Ce problème est détecté lorsque l'utilisation de la mémoire ADC pour cette application dépasse la valeur seuil configurée. Cliquez sur l'onglet **Utilisation de la mémoire** pour afficher les détails du problème.



Sous **Détails**, vous pouvez afficher :

- Le graphique indiquant le nombre total d'événements pour la durée sélectionnée. Cliquez pour appliquer le filtre et afficher les détails
- Lorsque le problème est survenu
- Le nombre total d'occurrences pour la durée sélectionnée
- La gravité du problème, par exemple faible, moyen et élevé
- Le message de détection indiquant le pourcentage moyen d'utilisation de la mémoire de l'ADC et la valeur de seuil configurée

Bagotement du service

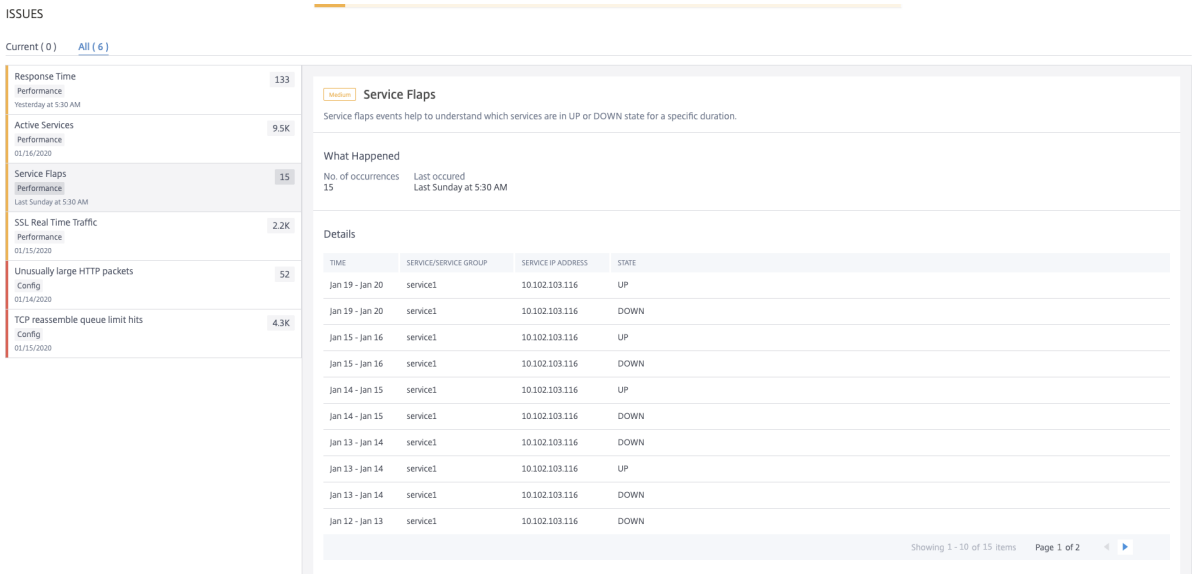
February 1, 2024

En tant qu'administrateur réseau, vous devez vous assurer de la disponibilité optimale de l'application. En cas de problèmes de réseau ou de configuration, l'état et la disponibilité d'un serveur d'applications peuvent avoir un impact sur les performances globales.

À l'aide des événements de bagotement du service, vous pouvez identifier l'application qui présente des problèmes. Les événements de bagotement du service vous aident également à :

- Déterminer quel service est en panne pendant une durée spécifique
- Découvrez combien de services sont en mode UP ou DOWN pendant une durée spécifique

Cliquez sur l'onglet **Service Flaps** pour afficher les détails de bagotement du service.



Vous pouvez consulter des détails tels que le nombre d'occurrences et l'heure de la dernière occurrence.

Sous **Détails**, vous pouvez afficher :

- L'heure à laquelle s'est produite l'anomalie du volet de service
- Le nom du service/groupe de services
- Adresse IP du service
- L'état actuel du service

Serveur instable

February 1, 2024

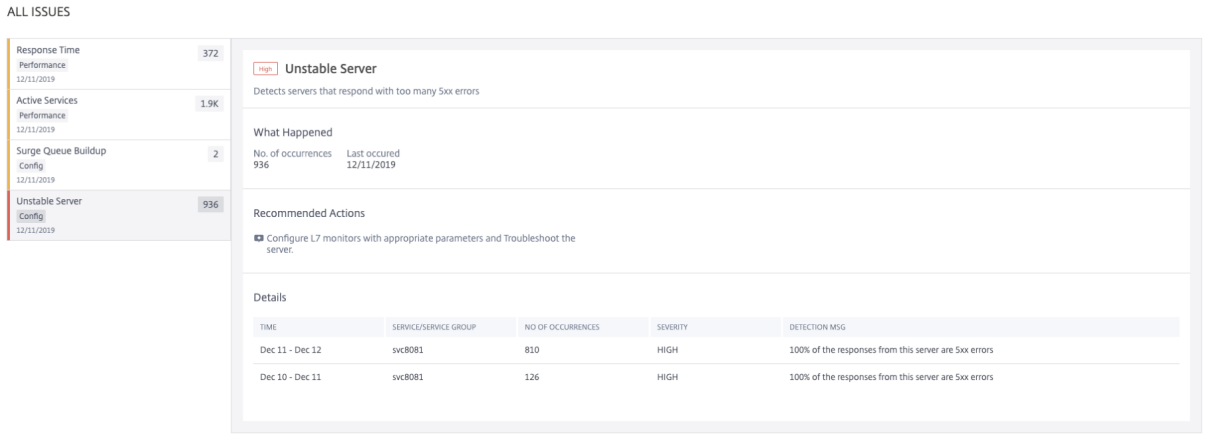
Dans certains scénarios, le serveur Web répond par des codes d'état lorsqu'il n'est pas en mesure de traiter les demandes pour des raisons telles que des demandes non valides, une surcharge temporaire ou une maintenance du serveur. Ces erreurs sont affichées avec des codes d'erreur, qui définissent différents scénarios d'erreurs. Par exemple, les opérations suivantes peuvent être effectuées :

- **502 Passerelle incorrecte**
  Le serveur agit en tant que passerelle ou proxy et a reçu une réponse non valide du serveur en amont.
- **503 Service indisponible**
  Le serveur est actuellement indisponible. Les serveurs sont peut-être surchargés ou indisponibles pour des raisons de maintenance.
- **504 Délai d'expiration de la passerelle**
  Le serveur agit en tant que passerelle ou proxy et n'a pas reçu de réponse en temps voulu du serveur en amont.

Ces conditions peuvent être temporaires, mais vous devez parfois mettre en œuvre une mesure corrective sur les serveurs Web pour rendre les pages Web disponibles.

À l'aide de l'indicateur de **serveur instable**, vous pouvez visualiser ces défaillances et prendre des décisions concernant les mesures correctives à prendre pour résoudre les problèmes et garantir que les demandes des clients sont satisfaites et que les pages Web sont toujours disponibles.

Sélectionnez l'onglet **Serveur instable** pour afficher les détails du problème.



Les **actions recommandées** pour résoudre le problème sont les suivantes :

- Configurez les moniteurs L7 avec les paramètres appropriés pour le serveur qui répond par des erreurs 5xx. Un moniteur est une entité qui suit l'état du service. L'appliance sonde régulièrement les serveurs à l'aide du moniteur lié à chaque service. Si un serveur ne répond pas dans un délai de réponse spécifié et que les sondes spécifiées échouent, le service est marqué comme INACTIF. L'appliance effectue ensuite l'équilibrage de la charge entre les services restants. Pour plus d'informations sur la configuration d'un moniteur, voir Moniteurs personnalisés
- Dépannage du serveur

Sous **Détails**, vous pouvez afficher :

- Heure à laquelle s'est produite l'anomalie du serveur instable

- Le nom du service/groupe de services
- Total des occurrences
- La gravité de l'anomalie, telle que élevée, faible et moyenne
- Message de détection indiquant le pourcentage des réponses de ce service signalant des erreurs 5xx

Pour plus d'informations sur la transaction Web d'erreur de serveur, voir Analyse des transactions Web pour les erreurs de serveur

Construction de session

February 1, 2024

Pour toutes les transactions sécurisées, Citrix ADC exécute le processus de déchargement SSL pour la première transaction, puis stocke la session SSL en fonction de la configuration de **réutilisation de session**.

En fonction du taux de trafic, l'accumulation de session peut se produire sur une certaine période, ce qui peut conduire à une grande quantité de mémoire maintenue par ces sessions dans Citrix ADC.

Les événements d'accumulation de session alertent les administrateurs et fournissent des actions recommandées pour résoudre cet événement. Cliquez sur l'onglet **Session Buildup** pour afficher les détails du problème

Sous **Détails**, vous pouvez afficher :

- Heure à laquelle s'est produite l'anomalie de création de session
- Le nom du serveur virtuel
- La gravité de l'anomalie, telle que élevée, faible et moyenne
- Message indiquant qu'un nombre **X** de sessions SSL sont disponibles sur le serveur virtuel et qu'il existe actuellement **Y** de connexions SSL par seconde pendant la session de temporisation configurée.

L'**action recommandée** pour corriger cette anomalie consiste à réduire le délai d'expiration de la session ou à désactiver la réutilisation de la session. Pour plus d'informations, consultez la section Délai d'expiration de session.

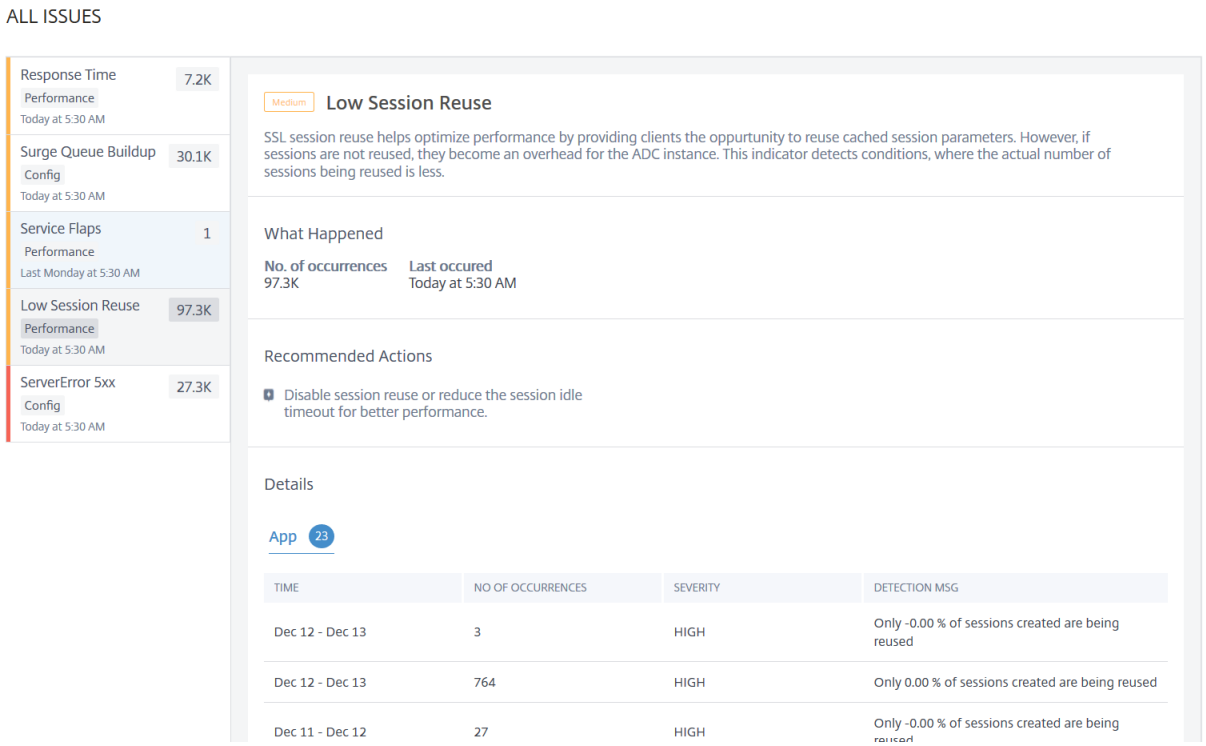
Réutilisation de session faible

February 1, 2024

Les instances Citrix ADC traitent les transactions SSL en déchargeant le processus de connexion SSL du serveur. À la réception de la réponse du serveur, l'instance Citrix ADC termine la transaction sécurisée avec le client. À l'aide des paramètres de session mis en cache, l'instance Citrix ADC termine le processus de connexion SSL pour les demandes consécutives.

Si ces sessions ne sont pas réutilisées, elles deviennent une surcharge pour les instances de Citrix ADC. À l'aide de l'indicateur de **faible réutilisation des sessions**, vous pouvez déterminer si le nombre réel de sessions réutilisées est inférieur.

Cliquez sur l'onglet **Low Session Reuse** pour afficher les détails du problème.



L'**action recommandée** pour résoudre le problème consiste à désactiver la réutilisation de la session ou à réduire le délai d'expiration de la session. Pour plus d'informations, consultez la section Réutilisation de session.

Sous **Détails**, vous pouvez afficher :

- Nombre total d'applications ayant une faible réutilisation des sessions
- L'heure à laquelle s'est produite l'anomalie de réutilisation de session faible
- Total des occurrences

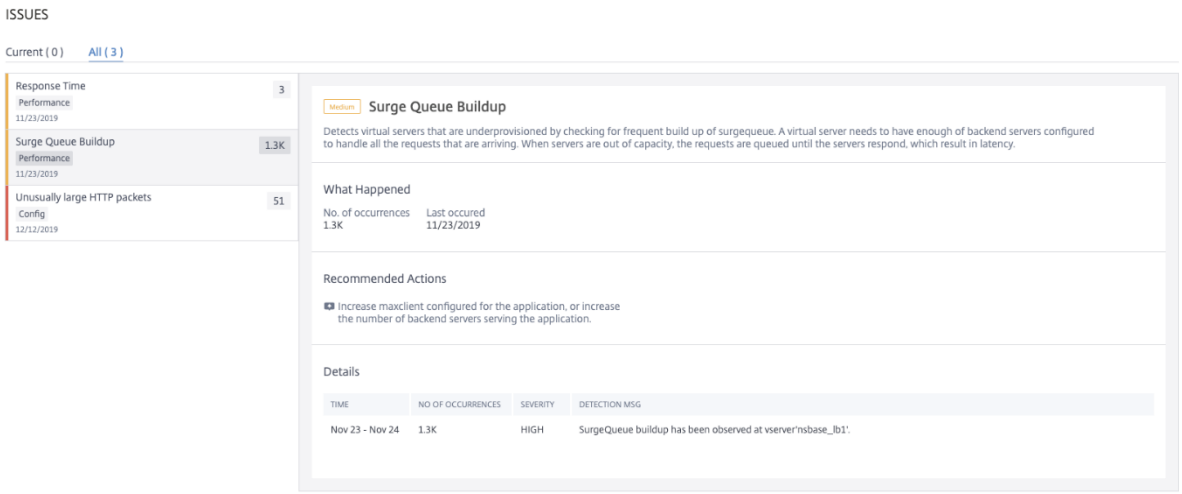
- La gravité de l'anomalie, telle que élevée, faible et moyenne
- Le message de détection indiquant que seuls % des sessions configurées sont réutilisées

Accumulation dans la file d'attente de surtension

February 1, 2024

Lorsqu'un serveur reçoit une vague de demandes, il met du temps à répondre aux clients. Souvent, la surcharge provoque également les clients à recevoir des pages d'erreur. Un serveur virtuel doit avoir suffisamment de serveurs back-end configurés pour gérer les demandes entrantes.

À l'aide de l'indicateur **d'accumulation de files d'attente de surtension**, vous pouvez afficher les serveurs virtuels qui ont accumulé de la file d'attente de surtension. Cliquez sur l'onglet **Surge Queue Buildup** pour afficher les détails du problème.



Les **actions recommandées** pour résoudre le problème sont les suivantes :

- Augmentez la limite du nombre de connexions client. Pour plus d'informations, consultez Définir une limite sur le nombre de connexions client
- Augmenter les serveurs back-end pour répondre aux demandes d'application

Sous **Détails**, vous pouvez afficher :

- Heure à laquelle s'est produite l'anomalie d'accumulation de files d'attente de surtension
- Total des occurrences
- La gravité de l'anomalie, telle que élevée, faible et moyenne
- Le message de détection indiquant l'accumulation de files d'attente de surtension sur le serveur virtuel

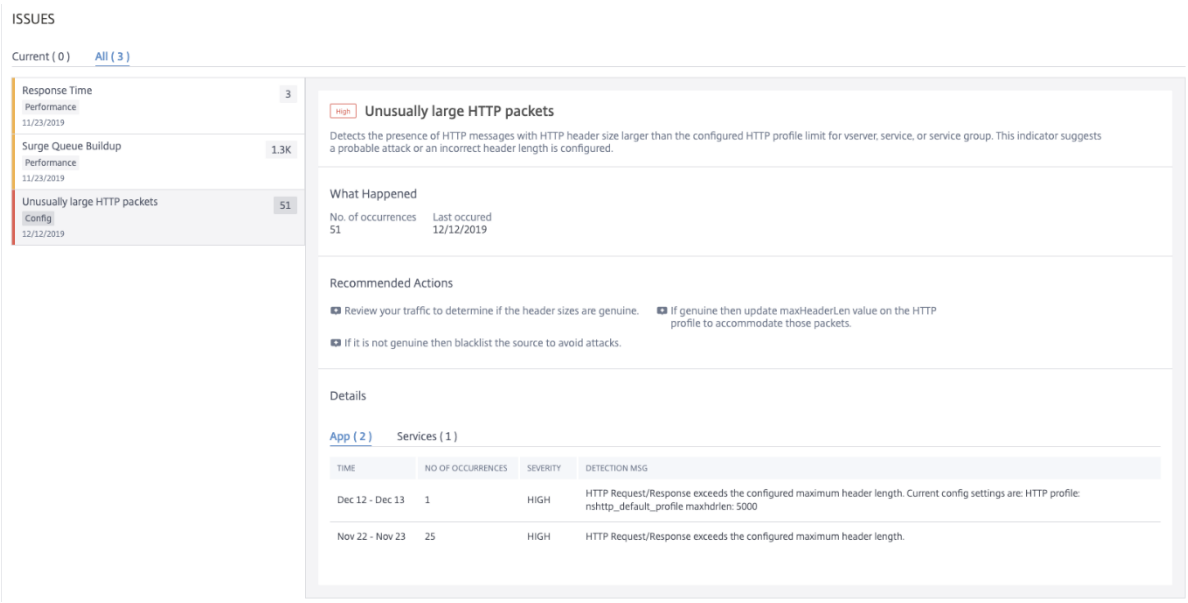
Paquets HTTP exceptionnellement volumineux

February 1, 2024

Une transaction HTTP utilise des messages de requête-réponse entre le client et le serveur. Dans les messages de requête et de réponse, les en-têtes HTTP sont les valeurs affichées dans le protocole HTTP. Vous pouvez configurer la longueur de l'en-tête HTTP dans un serveur virtuel, un service ou un groupe de services pour éviter les erreurs 4xx

Lorsqu'une requête/réponse HTTP dépasse la longueur maximale d'en-tête, il peut s'agir d'une attaque possible. À l'aide de l'indicateur de **paquets HTTP anormalement volumineux**, vous pouvez voir les occurrences où les messages HTTP dont la taille d'en-tête HTTP dépasse les valeurs configurées.

Cliquez sur l'onglet **Paquets HTTP anormalement volumineux** pour afficher les détails du problème.



Les **actions recommandées** pour résoudre le problème sont les suivantes :

- Passez en revue le trafic pour déterminer si la taille de l'en-tête est authentique. Si la taille de l'en-tête est authentique, mettez à jour la valeur de l'en-tête sur le profil HTTP. Pour plus d'informations, consultez la section Vérification du débordement de tampon
- Si la taille de l'en-tête n'est pas authentique, bloquez la liste de la source pour éviter les attaques.

Sous **Détails**, vous pouvez afficher :

- L'heure qui s'est produite l'anomalie

- Total des occurrences
- La gravité de l'anomalie, telle que élevée, faible et moyenne
- Le message de détection indiquant la longueur d'en-tête HTTP actuelle configurée sur le serveur virtuel, le serveur ou le groupe de services

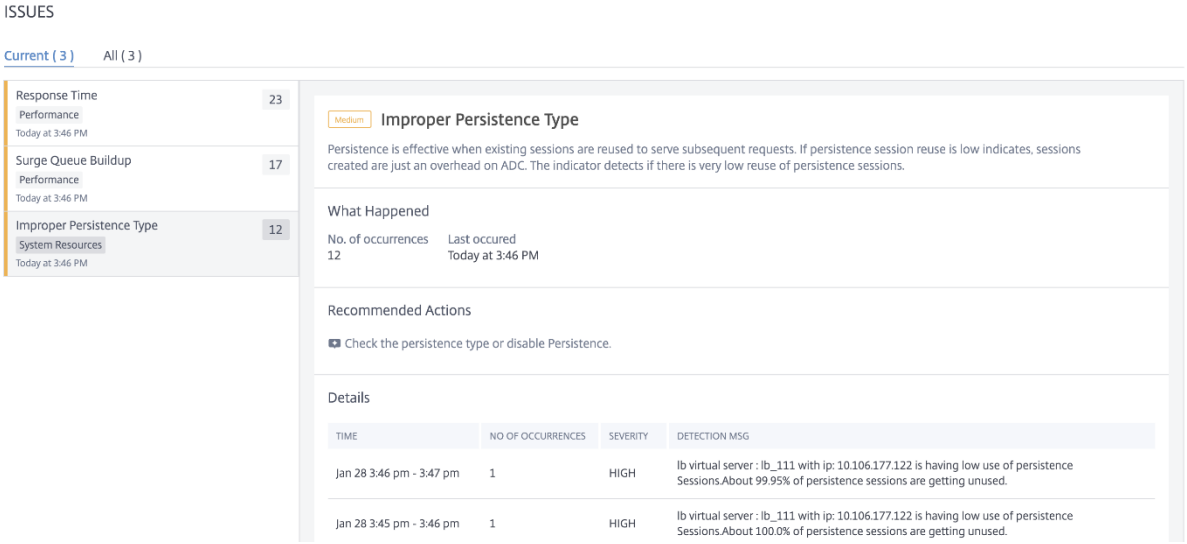
Type de persistance incorrect

February 1, 2024

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

La persistance est efficace lorsque les sessions existantes sont réutilisées pour répondre aux demandes ultérieures. Si la réutilisation des sessions de persistance est faible, les sessions créées sur ADC ne sont qu'une surcharge.

À l'aide de l'indicateur **de type de persistance incorrect**, vous pouvez déterminer si l'utilisation de la persistance sur un serveur virtuel est faible. Cliquez sur l'onglet **Type de persistance incorrecte** pour afficher les détails du problème.



L'**action recommandée** pour résoudre le problème consiste à vérifier le type de persistance ou à désactiver la persistance. Pour plus d'informations, consultez la section Paramètres de persistance.

Sous **Détails**, vous pouvez afficher :

- L'heure qui s'est produite l'anomalie
- Total des occurrences
- La gravité de l'anomalie, telle que élevée, faible et moyenne
- Le message de détection indiquant le % de sessions non utilisées

TCP reassemble queue limit hits

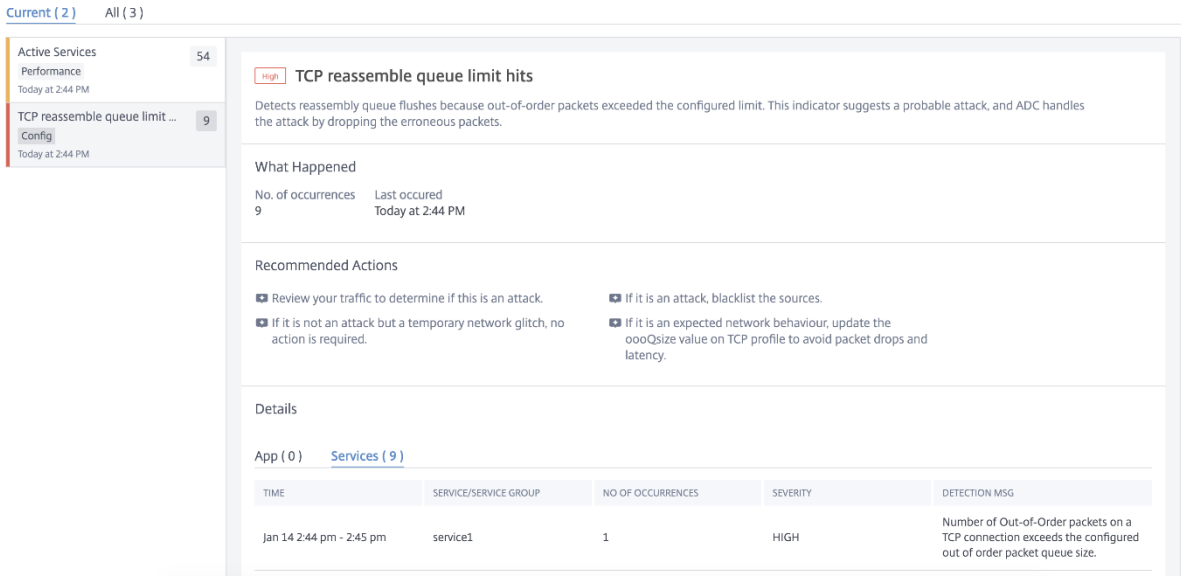
February 1, 2024

TCP maintient une file d'attente hors ordre pour conserver les paquets OOO dans la communication TCP. Ce paramètre affecte la mémoire Citrix ADC si la taille de la file d'attente est longue que les paquets doivent être conservés dans la mémoire d'exécution.

Cette taille de file d'attente doit être optimisée en fonction des caractéristiques du réseau et de l'application.

À l'aide de l'indicateur d'accès de **TCP reassemble queue limit hits**, vous pouvez voir si les paquets hors commande d'une connexion TCP dépassent la taille de file d'attente de paquets hors commande configurée.

Cliquez sur l'onglet **TCP reassemble queue limit hits** d'attente pour afficher les détails du problème.



Les **actions recommandées** pour résoudre le problème sont les suivantes :

- Examinez le trafic et bloquez la liste de la source s'il s'agit d'une attaque

- Si ce comportement est un comportement réseau attendu, mettez à jour la valeur de taille des paquets hors commande sur le profil TCP. Pour plus d'informations, consultez Optimisation TCP
- S'il s'agit simplement d'un problème de réseau temporaire, aucune autre action n'est requise

Sous **Détails**, vous pouvez afficher :

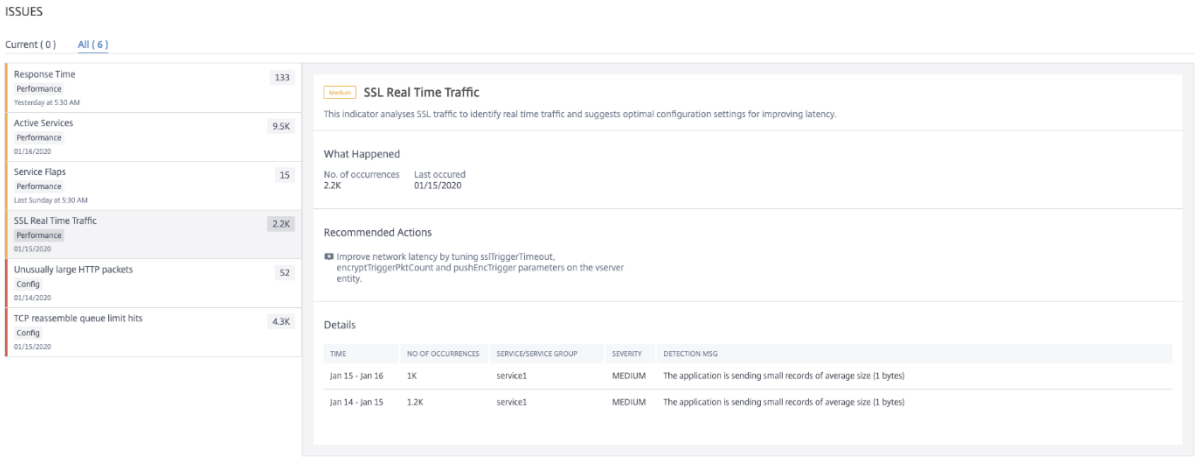
- L'heure qui s'est produite l'anomalie
- Total des occurrences
- La gravité de l'anomalie, telle que faible, moyenne et élevée
- Le message de détection indiquant le profil TCP actuel et les paramètres OOOQSize

Trafic SSL en temps réel

February 1, 2024

Dans l'instance Citrix ADC, vous pouvez utiliser un profil SSL pour traiter le trafic SSL. Le profil SSL comprend certains paramètres SSL pour les serveurs virtuels, les services et les groupes de services. L'indicateur de **trafic en temps réel SSL** analyse le trafic SSL pour identifier le trafic en temps réel et suggère des paramètres de configuration optimaux pour améliorer la latence.

Cliquez sur l'onglet **SSL Real Time Traffic** pour afficher les détails du problème.



L'**action recommandée** pour résoudre le problème consiste à améliorer la latence réseau en mettant à jour les paramètres SSL. Pour plus d'informations, consultez Paramètres SSL globaux.

Sous **Détails**, vous pouvez afficher :

- L'heure qui s'est produite l'anomalie
- Le nom du service/groupe de services

- La gravité de l'anomalie, telle que faible, moyenne et élevée
- Le message de détection avec le réglage actuel de l'application

Tableau de bord de la sécurité des applications

February 1, 2024

Le tableau **de bord Sécurité des applications** fournit une vue d'ensemble des mesures de sécurité pour les applications détectées/sous licence. Ce tableau de bord affiche les informations sur les attaques de sécurité pour les applications détectées/sous licence, telles que les attaques de synchronisation, les attaques de petites fenêtres, les attaques par saturation DNS, etc.

Pour afficher les mesures de sécurité sur le tableau de bord de sécurité de l'application :

1. Accédez à **Applications> Tableau de bord de sécurité** des applications.
2. Sélectionnez l'adresse IP de l'instance dans la liste Instance.

   Les rapports contiennent les renseignements suivants pour chaque application :

   - **Indice des menaces**. Système de classement à un chiffre indiquant la criticité des attaques sur l'application. Plus les attaques sur une application sont critiques, plus l'indice de menace pour cette application est élevé. Les valeurs varient de 1 à 7.

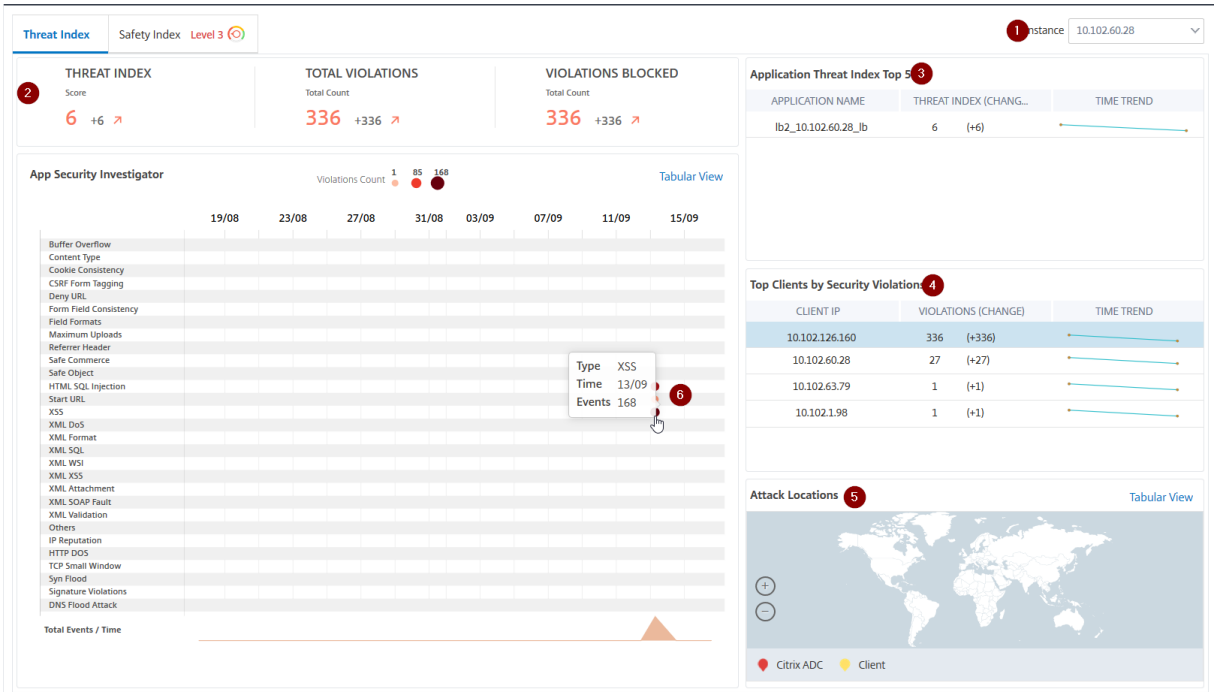
     L'indice des menaces est basé sur les informations d'attaque. Les informations relatives à l'attaque, telles que le type de violation, la catégorie d'attaque, l'emplacement et les détails du client, donnent un aperçu des attaques visant l'application. Les informations de violation sont envoyées à Citrix ADM uniquement lorsqu'une violation ou une attaque se produit. Un grand nombre de violations et de vulnérabilités conduisent à une valeur d'indice de menace élevée.

   - **Indice de sécurité**. Système de notation à un chiffre indiquant la manière dont vous avez configuré en toute sécurité les instances Citrix ADC pour protéger les applications contre les menaces et les vulnérabilités externes. Plus les risques pour la sécurité d'une application sont faibles, plus l'indice de sécurité est élevé. Les valeurs varient de 1 à 7.

     L'index de sécurité tient compte à la fois de la configuration du pare-feu de l'application et de la configuration de sécurité du système Citrix ADC. Pour un indice de sécurité élevé, les deux configurations doivent être solides. Par exemple, si des vérifications rigoureuses du pare-feu des applications sont en place, mais que les mesures de sécurité du système Citrix ADC, telles qu'un mot de passe fort pour l'utilisateur `nsroot`, n'est pas fournie, les applications se voient attribuer une valeur d'indice de sécurité faible.

Vous pouvez afficher les écarts signalés sur **App Security Investigator**.

Détails de l'index des menaces



1 - Affiche l'adresse IP de l'instance Citrix ADC pour laquelle vous pouvez afficher les détails.

2 - Affiche des détails tels que le score de l'indice de menace, le total des violations survenues et le nombre total de violations bloquées

3 - Affiche le serveur virtuel de l'instance sélectionnée.

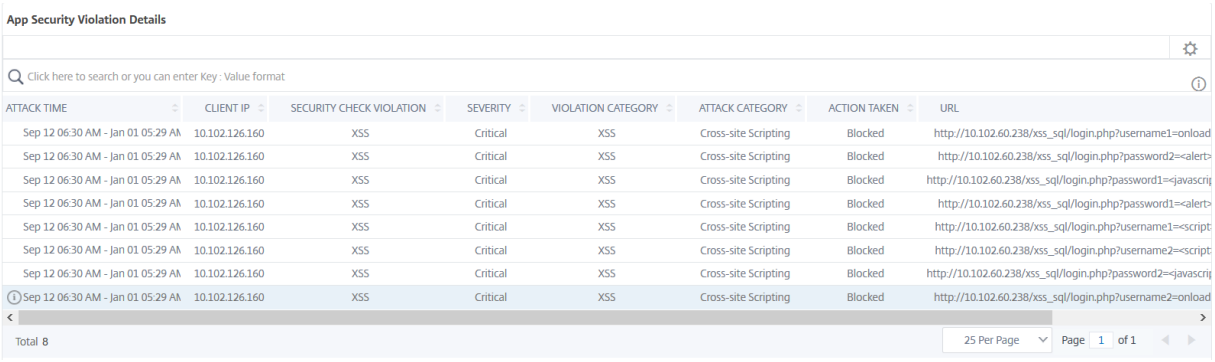
4 - Affiche les violations de sécurité en fonction des clients. Le graphique App Security Investigator s'affiche pour chaque client. Vous pouvez cliquer sur chaque adresse IP client pour afficher les résultats.

5 - Affiche les violations en mode carte et tabulaire.

6 - Affiche les détails de la violation. Lorsque vous placez le pointeur de la souris sur le graphique, les détails tels que le type de violation, l'heure de l'attaque et le total des événements sont affichés.

Lorsque vous cliquez sur un graphique à bulles, les détails s'affichent dans la page **Détails des violations de sécurité des applications**. Par exemple, si vous souhaitez afficher plus de détails sur la violation de script intersite (script inter-site), cliquez sur le graphique rempli pour **XSS** dans **App Security Investigator**.

Les **détails des violations de sécurité de l'application** sont affichés avec des détails de violation tels que le temps d'attaque, la catégorie d'attaque, la gravité, l'URL, etc.



Vous pouvez également cliquer sur l'option **Paramètres** pour sélectionner les options que vous souhaitez afficher.

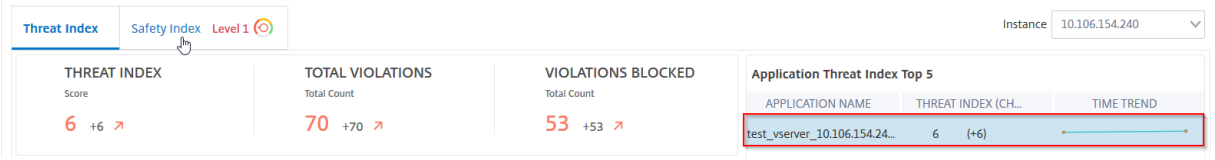
Détails de l'indice de sécurité

Après avoir examiné l'exposition aux menaces d'une application, vous souhaitez déterminer quelles configurations de sécurité des applications sont en place et quelles configurations sont manquantes pour cette application. Vous pouvez obtenir ces informations en consultant le résumé de l'indice de sécurité de l'application.

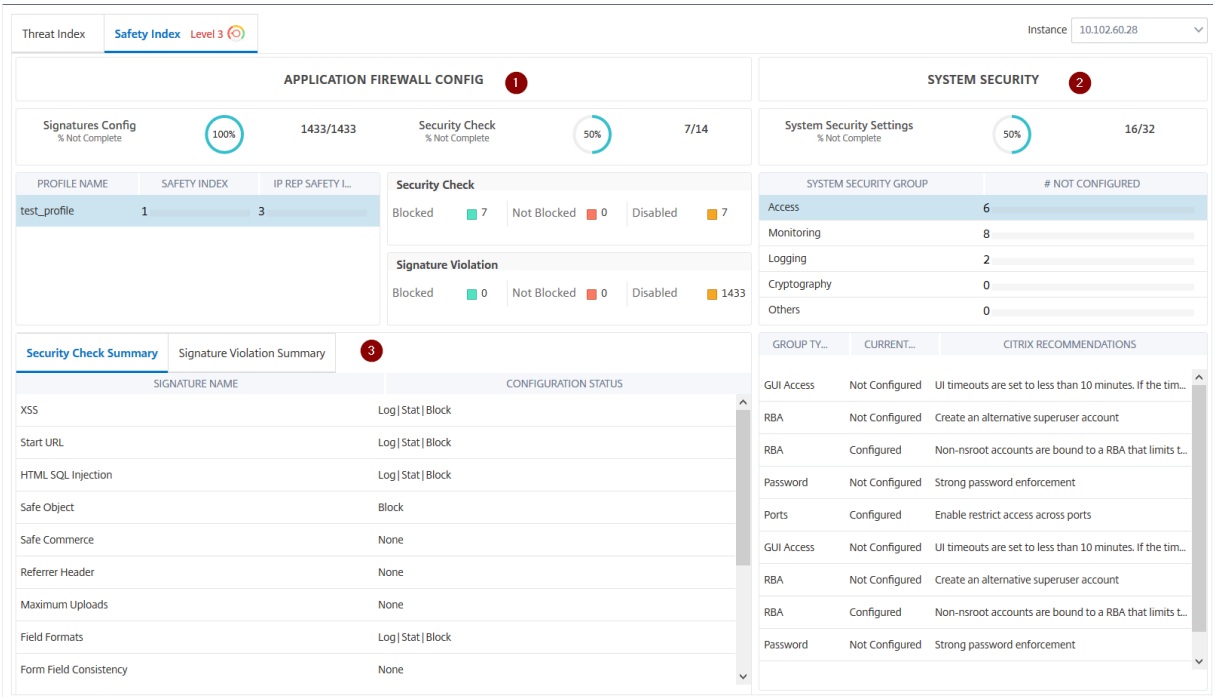
Le résumé de l'indice de sécurité fournit des informations sur l'efficacité des configurations de sécurité suivantes :

- **Configuration du pare-feu d'application**. Indique le nombre d'entités de signature et de sécurité qui ne sont pas configurées.
- **Citrix ADM System Security**. Indique combien de paramètres de sécurité système ne sont pas configurés.

Pour afficher les détails de l'**index de sécurité**, sélectionnez un serveur/application virtuel et cliquez sur l'onglet **Indice de sécurité** .



Les détails sont affichés.



1 - Affiche les informations détaillées pour les configurations du pare-feu d'application.

2 - Affiche les informations détaillées pour la sécurité du système. Cliquez sur chaque groupe de sécurité pour obtenir des informations détaillées sur l'état actuel et les recommandations de Citrix.

3 - Affiche le résumé de la vérification de sécurité et de la violation de signature.

Vous pouvez également afficher le résumé de l'environnement des menaces en activant les informations de sécurité pour les serveurs virtuels, puis en accédant à **Analytics** > **Security Insight**. Pour plus d'informations sur le cas d'utilisation de l'indice de sécurité, voir Security Insight

Graphique de service

February 1, 2024

La fonctionnalité de graphique de service dans Citrix ADM vous permet de surveiller tous les services dans une représentation graphique. Cette fonctionnalité vous permet également d'afficher une analyse détaillée et des mesures exploitables des services. Vous pouvez afficher le graphique de service pour :

- Applications configurées sur toutes les instances Citrix ADC
- Applications Kubernetes
- Applications Web à 3 niveaux

Graphique des services pour les applications sur toutes les instances Citrix ADC

La fonction de graphique de service global vous permet d'obtenir une visualisation holistique de la `clients to infrastructure to application` vue. À partir de cette vue graphique de service à volet unique, en tant qu'administrateur, vous pouvez :

- Comprendre la région à partir de laquelle les utilisateurs accèdent aux applications spécifiques (applications Web à 3 niveaux et applications microservices)
- Visualiser la vue de l'infrastructure (instance Citrix ADC) que la demande du client est traitée
- Comprendre si les problèmes surviennent à partir du client, de l'infrastructure ou de l'application
- Exercer davantage vers le bas pour résoudre le problème

Accédez à **Applications > Service Graph** et cliquez sur l'onglet **Global** pour afficher :

- Détails de bout en bout de toutes les applications connectées du client aux serveurs back-end
- Toutes les instances Citrix ADC connectées à ses centres de données respectifs

  > **Remarque**
  >
  > Vous pouvez afficher les centres de données uniquement si vous disposez d'applications GSLB.

- Informations sur les mesures du client
- Informations sur les mesures Citrix ADC
- Toutes les instances Citrix ADC qui ont des applications discrètes, des applications personnalisées et des applications de microservice distinctes
- Les 4 applications les plus faibles qui appartiennent à des applications personnalisées, des applications discrètes et des applications de microservices
- Informations sur les mesures pour les 4 serveurs virtuels les plus bas cotés
- Les applications (applications discrètes, applications personnalisées et applications de microservices) sont des statuts tels que **Critique**, **Review**, **Bon**et **Non applicable**.

Pour plus d'informations, reportez-vous à la section Graphique de la vue holistique des applications en service.

Graphique de service pour les applications Kubernetes

Accédez à **Applications > Service Graph** et cliquez sur l'onglet **Microservices** pour afficher :

- Garantir les performances globales des applications de bout en bout

- Identifiez les blocages créés par l'interdépendance des différents composants de vos applications
- Recueillez des informations sur les dépendances des différents composants de vos applications
- Surveiller les services au sein du cluster Kubernetes
- Surveiller quel service rencontre des problèmes
- Vérifiez les facteurs qui contribuent aux problèmes de performance
- Afficher la visibilité détaillée des transactions HTTP de service
- Analyser les mesures HTTP, TCP et SSL

En visualisant ces mesures dans Citrix ADM, vous pouvez analyser la cause première des problèmes et prendre les mesures de dépannage nécessaires plus rapidement. Le graphique de service affiche vos applications dans divers services de composants. Ces services s'exécutant à l'intérieur du cluster Kubernetes peuvent communiquer avec divers composants à l'intérieur et à l'extérieur de l'application. Pour commencer, reportez-vous à la section Configuration du graphique de service.

Graphique de service pour les applications Web à 3 niveaux

Accédez à **Applications > Service Graph** et cliquez sur l'onglet **Web Apps** pour afficher :

- Détails sur la configuration de l'application (avec un serveur virtuel de commutation de contenu et un serveur virtuel d'équilibrage de charge)

  Pour les applications GSLB, vous pouvez afficher les serveurs virtuels de centre de données, d'instance ADC, de CS et de LB.
- Transactions de bout en bout du client au service
- Emplacement à partir duquel le client accède à l'application
- Le nom du centre de données où les demandes client sont traitées et les mesures Citrix ADC du centre de données associées (uniquement pour les applications GSLB)
- Détails des mesures pour les serveurs clients, les services et les serveurs virtuels
- Si les erreurs proviennent du client ou du service
- L'état du service, tel que **Critique, Révision**et**Bon**. Citrix ADM affiche l'état du service en fonction du temps de réponse du service et du nombre d'erreurs.
  - **Critique (rouge)** - Indique si le temps de réponse moyen du service est supérieur à 200 ms ET le nombre d'erreurs > 0
  - **Avis (orange)** - Indique si le temps de réponse moyen du service est supérieur à 200 ms OU le nombre d'erreurs > 0

  - **Bon (vert)** - Indique l'absence d'erreur et le temps de réponse moyen du service est inférieur à 200 ms

- L'état du client, tel que **Critique, Révision**et**Bon**. Citrix ADM affiche l'état du client en fonction de la latence du réseau client et du nombre d'erreurs.
  - **Critique (rouge)**- Indique si la latence moyenne du réseau client est > 200 ms ET le nombre d'erreurs > 0
  - **Avis (orange)** - Indique lorsque la latence moyenne du réseau client est > 200 ms OU le nombre d'erreurs > 0
  - **Bon (vert)** - Indique l'absence d'erreur et la latence moyenne du réseau client est inférieure à 200 ms
- L'état du serveur virtuel, tel que **Critique, Révision**et**Bon**. Citrix ADM affiche l'état du serveur virtuel en fonction du score de l'application.
  - **Critique (rouge)** - Indique lorsque le score de l'application est inférieur à 40
  - **Avis (orange)** - Indique quand le score de l'application se situe entre 40 et 75
  - **Bon (vert)** - Indique lorsque le score de l'application est > 75

Points à noter :

- Seuls les serveurs virtuels d'équilibrage de charge, de commutation de contenu et de GSLB sont affichés dans le graphique de service.
- Si aucun serveur virtuel n'est lié à une application personnalisée, les détails ne sont pas visibles dans le graphique de service de l'application.
- Vous pouvez afficher les mesures pour les clients et les services dans le graphique de service uniquement si des transactions actives se produisent entre les serveurs virtuels et l'application Web.
- Si aucune transaction active n'est disponible entre les serveurs virtuels et l'application Web, vous pouvez uniquement afficher les détails dans le graphique de service en fonction des données de configuration telles que l'équilibrage de charge, la commutation de contenu, les serveurs virtuels GSLB et les services.
- Si des modifications ont été apportées à la configuration de l'application, cela peut prendre 10 minutes pour refléter dans le graphique de service.

Pour plus d'informations, consultez la section Graphique de service pour les applications.

Configuration d'un graphique de service

February 1, 2024

Configuration logicielle requise

Distribution Kubernetes	Version Kubernetes	Interfaces réseau de conteneurs (CNI)	Version CPX	Version CIC	Version Citrix ADM	Version de l'agent Citrix ADM
Open Source	v1.16.3	Flanelle, Calico ou Canal	13.0—41.28 ou version ultérieure	1.5.25 ou version ultérieure	13.0—47.22 ou version ultérieure	13.0—47.22 ou version ultérieure

Vous pouvez configurer le cluster Kubernetes avec différentes topologies de déploiement et le tableau suivant fournit les topologies prises en charge dans le graphique de service :

Topologie	Graphique de service pris en charge
Une entrée unifiée ou unifiée	Oui
Double niveau	Oui
Cloud	Oui, mais l'équilibreur de charge dans le cloud n'est pas affiché dans le graphique
Service mesh lite	Oui
Service mesh	Oui
Services de type LoadBalancer	Non
Services de type NodePort	Non

Pour terminer la configuration du graphique de service dans Citrix ADM, cliquez sur le type de topologie que vous avez configuré pour votre cluster Kubernetes et effectuez les procédures mentionnées :

- Topologie d'entrée unifiée ou unifiée
- Topologie à deux niveaux ou Service Mesh Lite
- Topologie de maillage de service

> **Remarque**
>
> La procédure de configuration du graphique de service pour les topologies à double niveau et service mesh lite reste la même.

Avant de commencer

Vous pouvez afficher le graphique de service à l'aide des scénarios suivants :

- Citrix ADM et Kubernetes cluster sur le même réseau (par exemple, Citrix ADM et Kubernetes cluster hébergé sur le même Citrix Hypervisor).
- Cluster Citrix ADM et Kubernetes sur un réseau différent. Dans ce scénario, vous devez configurer un agent sur site et enregistrer l'agent sur le réseau, où le cluster Kubernetes est hébergé.

Topologie d'entrée unifiée ou à niveau unique

Assurez-vous que vous avez :

- Cluster Kubernetes configuré avec topologie d'entrée unique ou unifiée.
- Ajout d'une instance VPX, MPX, SDX, BLX dans Citrix ADM et **Web Insight**activé.
- Ajout d'un cluster Kubernetes dans Citrix ADM.

Topologie à deux niveaux ou Service Mesh Lite

Assurez-vous que vous avez :

- Cluster Kubernetes configuré avec l'une des topologies prises en charge.
- Itinéraires statiques configurés sur Citrix ADM pour permettre la communication entre Citrix ADM et Citrix ADC CPX.

  > **Remarque**
  >
  > Vous pouvez ignorer cette procédure si vous avez déployé Citrix ADM en tant que microservice dans le même cluster.

- J'ai téléchargé les exemples de fichiers de déploiement depuis le référentiel GitHub.
- Les paramètres requis ont été ajoutés dans le fichier CPX YAML pour garantir un enregistrement CPX réussi auprès de Citrix ADM.
- Ajout d'une instance VPX, MPX, SDX ou BLX dans Citrix ADM.
- Ajout du cluster Kubernetes dans Citrix ADM.

- Déploiement d'un exemple d'application de microservice.
- Citrix ADC CPX déployé et CPX enregistré auprès d'ADM (applicable uniquement pour l'architecture à deux niveaux)
- Activation de la sélection automatique des serveurs virtuels pour attribuer une licence aux serveurs virtuels.
- Activation des paramètres de transaction Web et de transaction TCP sur **Tous** pour que l'agent Citrix ADM obtienne les transactions HTTP et TCP.
- Trafic envoyé aux microservices.

Topologie de maillage de service

Assurez-vous que vous avez :

- Version de cluster Kubernetes configurée `1.14.0` avec l'une des topologies de maillage de service suivantes :
  - Citrix ADC CPX en tant que proxy sidecar pour Istio
  - Citrix ADC en tant que passerelle d'entrée pour Istio

  Pour plus d'informations, consultez Architecture de déploiement de l'adaptateur Citrix ADC Istio
- API `admissionregistration.k8s.io/v1beta1` activée. Vous pouvez vérifier l'API en utilisant :

  ```
  kubectl api-versions | grep admissionregistration.k8s.io/v1beta1
  ```

  La sortie suivante indique que l'API est activée :

  ```
  admissionregistration.k8s.io/v1beta1
  ```
- Istio installé `istio v.1.3.0`.
- Installation de Helm version 3.x.
- Itinéraires statiques configurés sur Citrix ADM pour permettre la communication entre Citrix ADM et Citrix ADC CPX.

  > **Remarque**
  >
  > Vous pouvez ignorer cette procédure si vous avez déployé l'agent Citrix ADM en tant que microservice dans le même cluster.

- Configuré les paramètres requis pour renseigner les données de topologie du maillage de service.

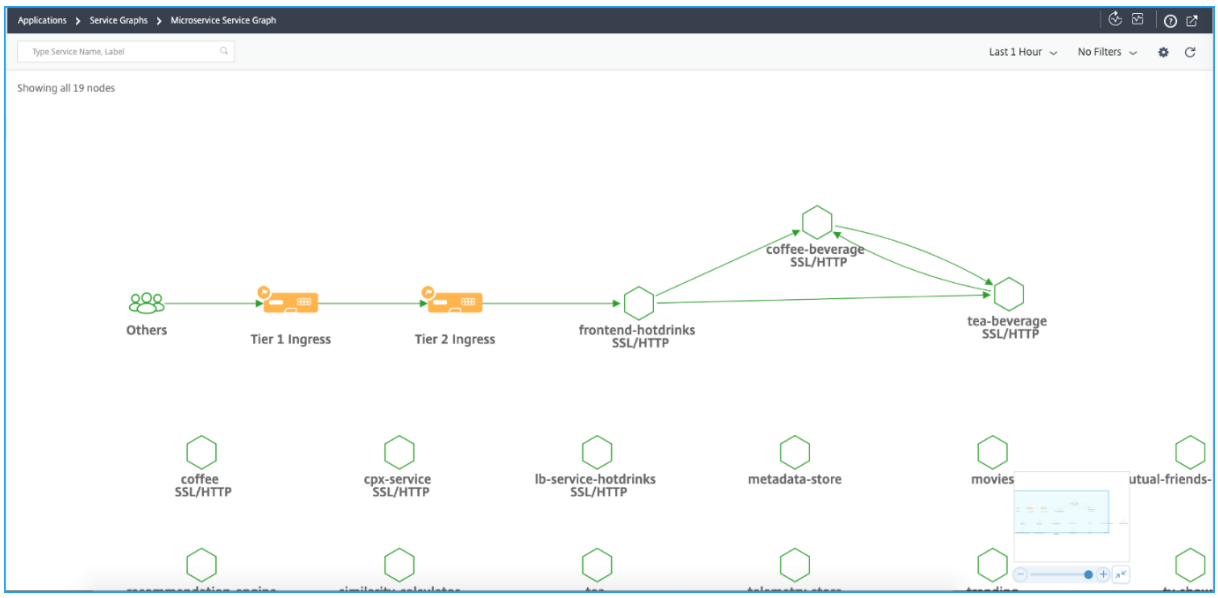
- Déploiement d'un exemple d'application.
- Ajout du cluster Kubernetes dans Citrix ADM.
- Activation de la sélection automatique des serveurs virtuels pour attribuer une licence aux serveurs virtuels.
- Activation des paramètres de transaction Web et de transaction TCP sur **Tous** pour que l'agent Citrix ADM obtienne les transactions HTTP et TCP.
- Trafic envoyé aux microservices.

Afficher les détails dans le graphique de service

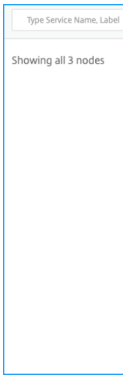
February 1, 2024

Dans Citrix ADM, accédez à **Application > Graphiques de service > Kubernetes Service Graph** et sélectionnez la durée dans la liste pour afficher les détails du graphique de service.

Topologie à deux niveaux de service Mesh Lite



Topologie



- **Tier 1** : Citrix Ingress Controller dans le cluster Kubernetes configure une instance Citrix ADC (VPX/MPX/SDX/BLX) en dehors du cluster Kubernetes.
- **Tier 2** : Citrix Ingress Controller s'exécute en tant que sidecar avec l'instance Citrix ADC CPX dans le cluster Kubernetes.
- **Ingress** : affiche pour toutes les autres topologies de déploiement.

Tableau de bord graphique de service

1 - Carte du réseau de bout en bout de votre application qui montre comment les services de vos composants communiquent

2 —Graphique indiquant les résultats et les erreurs pour une durée spécifique

3 —Barre de recherche pour rechercher des services

4 —Liste des heures pour sélectionner la durée

5 - Appliquer des filtres aux services d'affichage

6 —Icône de réglage

7 —Zoom avant et zoom arrière vue

8 —Vue graphique ou vue tabulaire

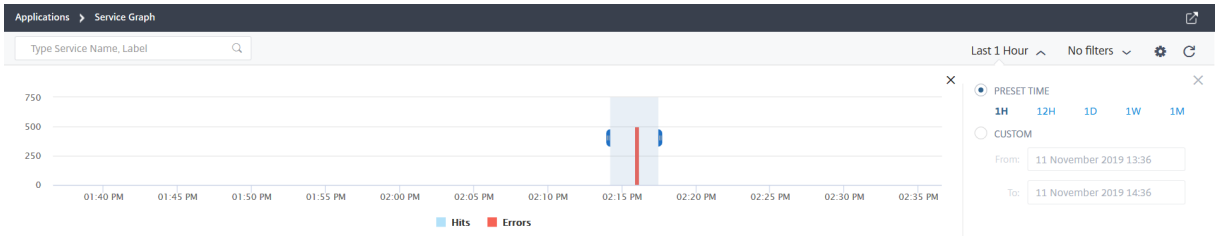
En fonction de la durée sélectionnée, vous pouvez afficher le graphique de service.

Icône Service	Description
	La largeur de l'arête indique le nombre de coups. Plus la largeur d'arête est grande ou supérieure, indique que le nombre de coups est plus élevé.

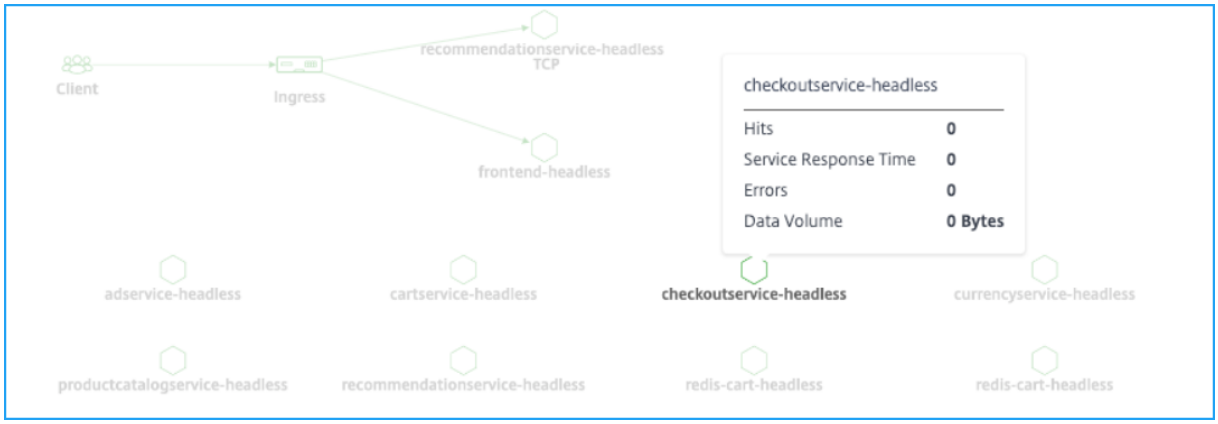
Icône Service	Description
	Le service avec une icône d'avertissement indique que le service a des erreurs.
	Le service avec une icône de chronomètre indique que le service présente des problèmes de latence ou de temps de réponse.
	Le service avec des icônes de chronomètre et d'avertissement indique que le service présente à la fois des erreurs et des problèmes de latence/temps de réponse.

> **Remarque**
>
> Si un service n'a pas d'icône d'avertissement ou de chronomètre, il indique que le service présente des anomalies ou une rupture de seuil pour les Hits.

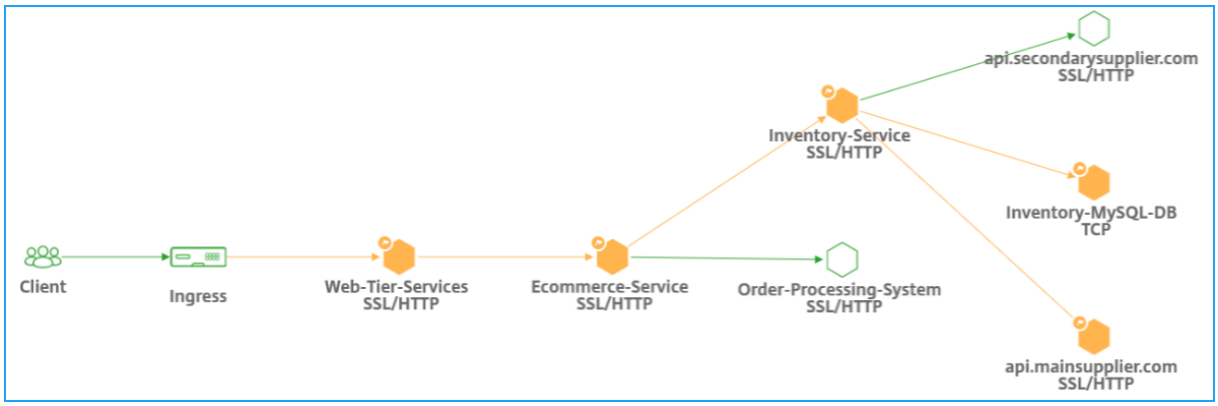
En fonction de la durée sélectionnée, vous pouvez afficher le graphique de service. Sélectionnez dans le graphique la période qui indique les résultats à explorer plus bas pour plus d'informations.



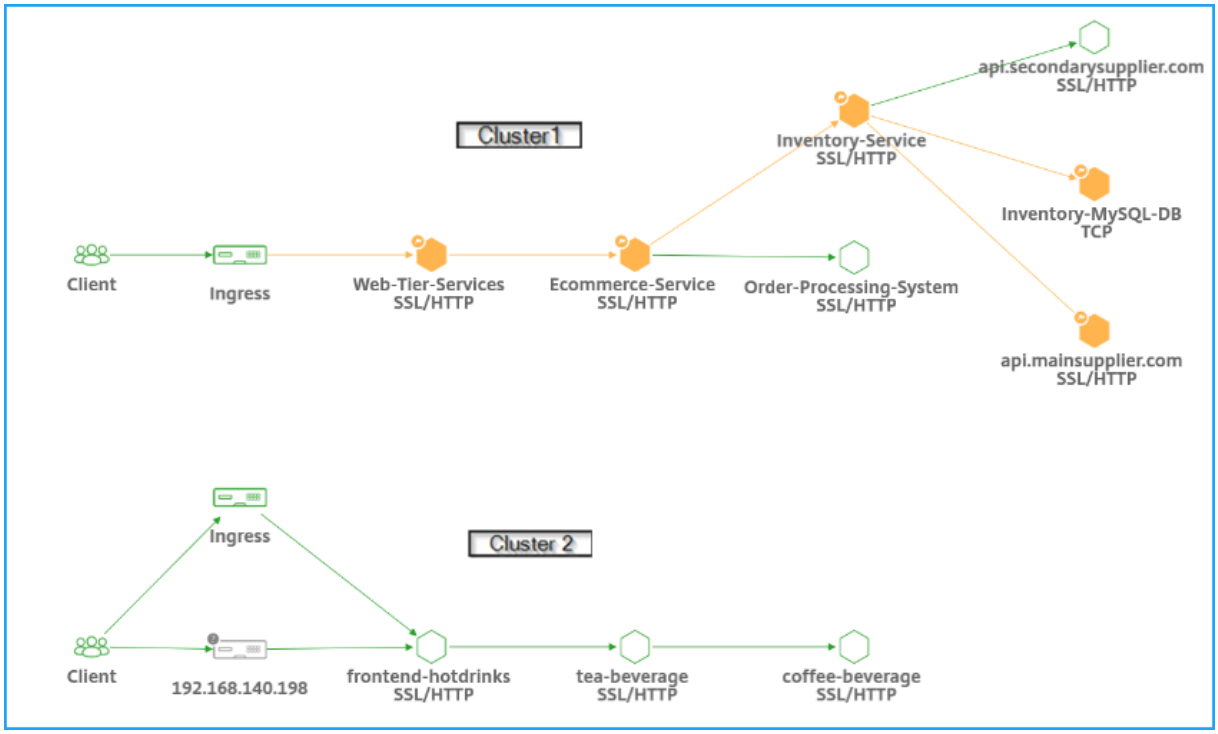
> **Remarque**
>
> Si aucune transaction active n'a été reçue par Citrix ADM, vous pouvez afficher uniquement les services qui sont équilibrés par l'instance Citrix ADC. Lorsque vous placez le pointeur de la souris sur un service, toutes les mesures sont affichées sous la forme 0.



Le graphique de service s'affiche avec le protocole utilisé par les services. Considérez que vous avez les services suivants en cours d'exécution dans votre cluster Kubernetes, comme illustré dans l'image :



> Remarque
>
> Si vous avez ajouté plusieurs clusters dans **Orchestration** > **Kubernetes** > **Clusters**, vous pouvez afficher les services associés à chaque cluster.



Vous pouvez afficher l'état suivant pour vos services :

- **Critique (rouge)** - Indique si le temps de réponse moyen du service est supérieur à 200 ms ET le nombre d'erreurs > 0
- **Avis (orange)** - Indique si le temps de réponse moyen du service est supérieur à 200 ms OU le nombre d'erreurs > 0
- **Bon (vert)** - Indique l'absence d'erreur et le temps de réponse moyen du service est inférieur à 200 ms

Les protocoles suivants vous permettent d'identifier le protocole utilisé par un service :

- **TCP** —Indique que le service utilise le protocole TCP.
- **SSL, HTTP** —Indique que le service utilise le protocole SSL sur HTTP.
- **SSL, TCP** —Indique que le service utilise le protocole SSL sur TCP.

> **Remarque**
>
> Le service sans protocole indique que le service utilise le protocole HTTP.

Afficher les tendances des mesures clés à l'aide de la vue tabulaire

En utilisant la vue tabulaire, vous pouvez voir :

- Mesures clés pour le service

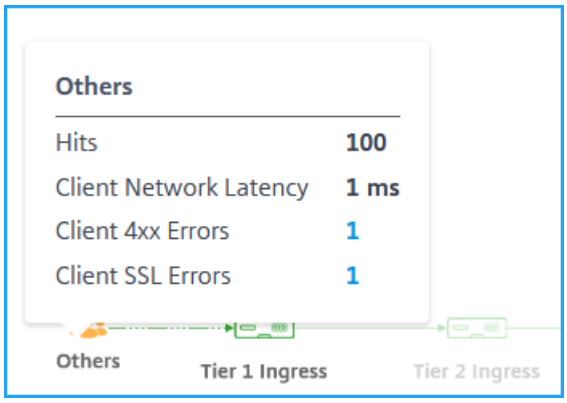
- Mesures clés entre un service source et un service de destination

En tant qu'administrateur, à l'aide de ces mesures clés, vous pouvez analyser les tendances des signaux dorés pour la durée sélectionnée.

Afficher les mesures client

Vous pouvez afficher à partir de quel emplacement le client accède au service. En tant qu'administrateur, vous pouvez visualiser les mesures client et analyser les problèmes qui se produisent à partir du client.

Placez le pointeur de la souris sur une région cliente pour afficher les mesures.



- **Hits** - Indique le nombre total d'accès reçus par le client.
- **Latence réseau client** - Indique la latence moyenne du réseau client.
- **Erreurs client 4xx** - Indique le total des erreurs 4xx client.
- **Erreurs SSL client** - Indique le nombre total d'erreurs SSL client.

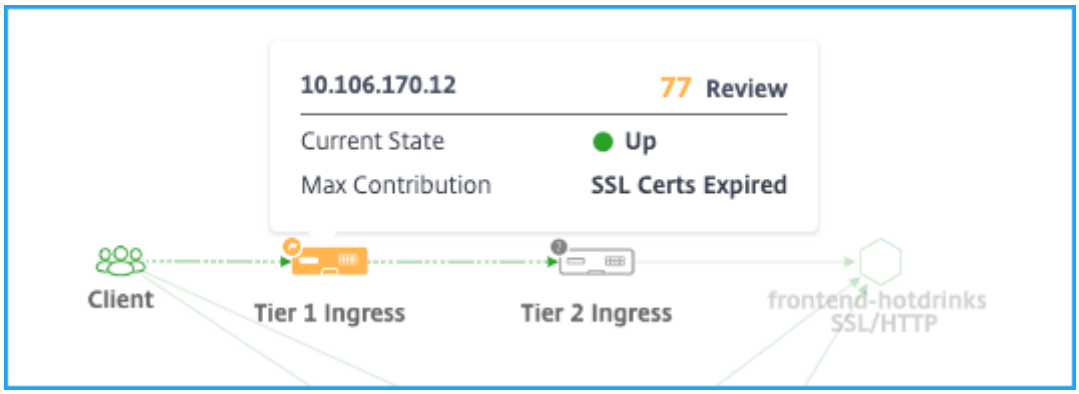
Blocs IP dans Citrix ADM - Citrix ADM peut reconnaître l'emplacement du client si le client utilise une adresse IP publique. Citrix ADM possède son fichier CSV d'emplacement intégré qui correspond à l'emplacement basé sur la plage d'adresses IP du client.

Citrix ADM peut reconnaître l'emplacement du client avec une adresse IP privée uniquement lorsque l'adresse IP est ajoutée au serveur Citrix ADM. Par exemple, si l'adresse IP du client appartient à une plage d'adresses IP privée associée à la ville A, Citrix ADM reconnaît que le trafic provient de la ville A pour ce client.

Pour plus d'informations, consultez Créer un bloc d'adresse IP privé.

Afficher les mesures d'entrée

Vous pouvez afficher le type d'entrée utilisé dans le cluster Kubernetes.



- Adresse IP Citrix ADC et son score
- **État actuel** —Indique si l'instance Citrix ADC est Hors, Down ou Hors état
- **Contribution maximale** : indique le problème qui affecte le score d'instance

Pour la topologie à un seul niveau, vous ne pouvez afficher qu'une **entrée**unique.

Cliquez sur l'**entrée** pour approfondir l'exploration vers le bas pour plus de détails. Pour plus d'informations, consultez Afficher les détails d'entrée pour la résolution des problèmes.

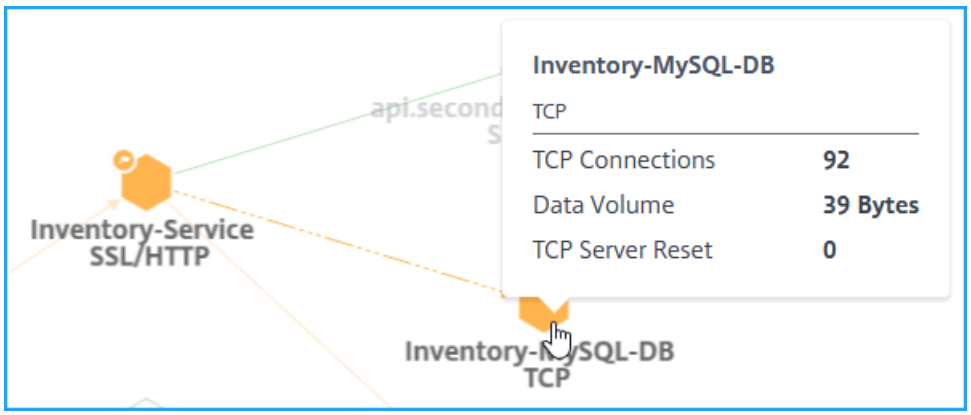
Afficher les mesures TCP et SSL

À l'aide des mesures TCP et SSL, vous pouvez :

- Afficher les détails de la connexion TCP entre les services
- Déterminez si les problèmes liés au protocole TCP proviennent du service source ou de destination
- Afficher si l'erreur SSL provient du service source ou de destination
- Afficher la version du protocole SSL utilisée par les services SSL

Métriques TCP

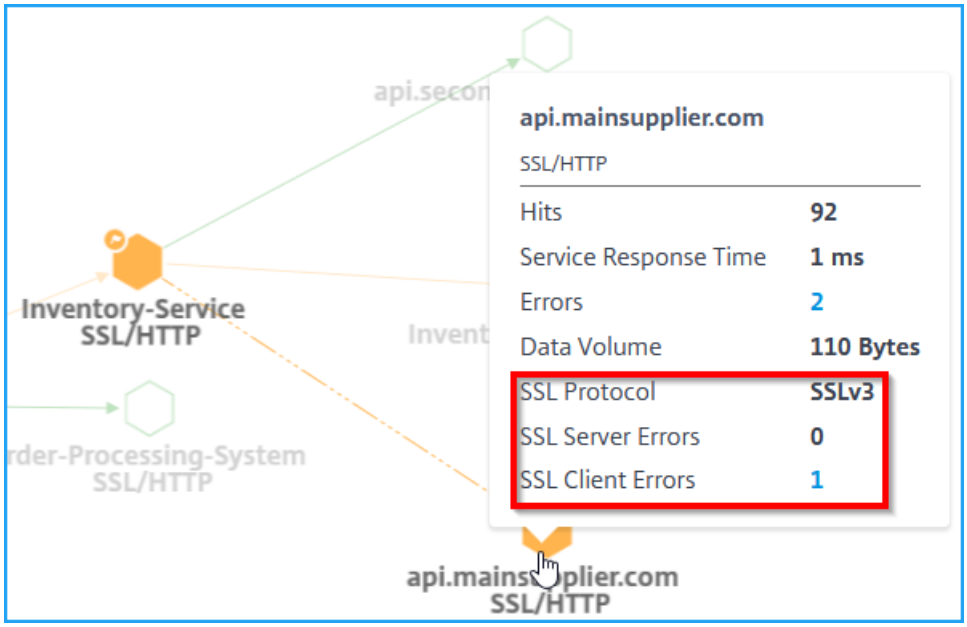
Passez le pointeur de la souris sur un service TCP ou son service entrant associé pour afficher les métriques TCP.



- **Connexions TCP** : nombre total de connexions établies entre les services
- **Volume de données** —Total des données traitées par le service
- **Réinitialisation du serveur TCP** —**Nombre total de réinitialisations** TCP initiées depuis le serveur

Mesures SSL

Passez le pointeur de la souris sur un service qui utilise le protocole SSL pour afficher les métriques SSL.



- **Erreurs du serveur SSL** —Indique le nombre total d'erreurs SSL provenant du serveur. (Par exemple, certificat SSL inconnu)
- **Protocole SSL** —Indique la version du protocole SSL utilisée par le service

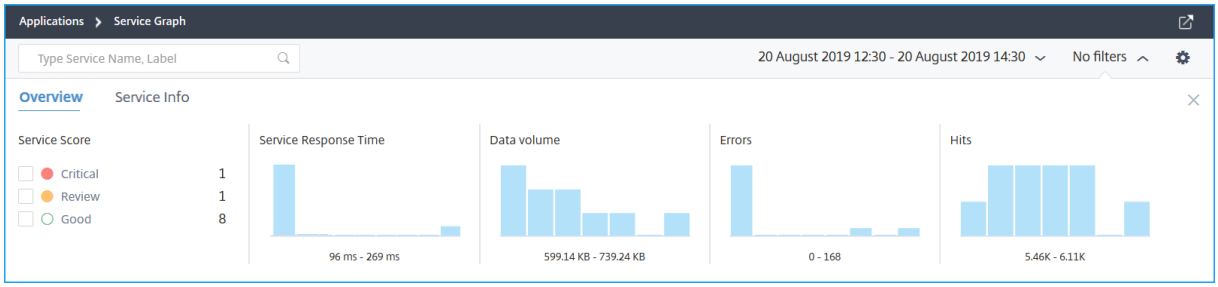
- **Erreurs du client SSL** : indiquez le nombre total d'erreurs SSL provenant du client. (Par exemple, erreur d'authentification du client SSL)

Afficher les détails du service

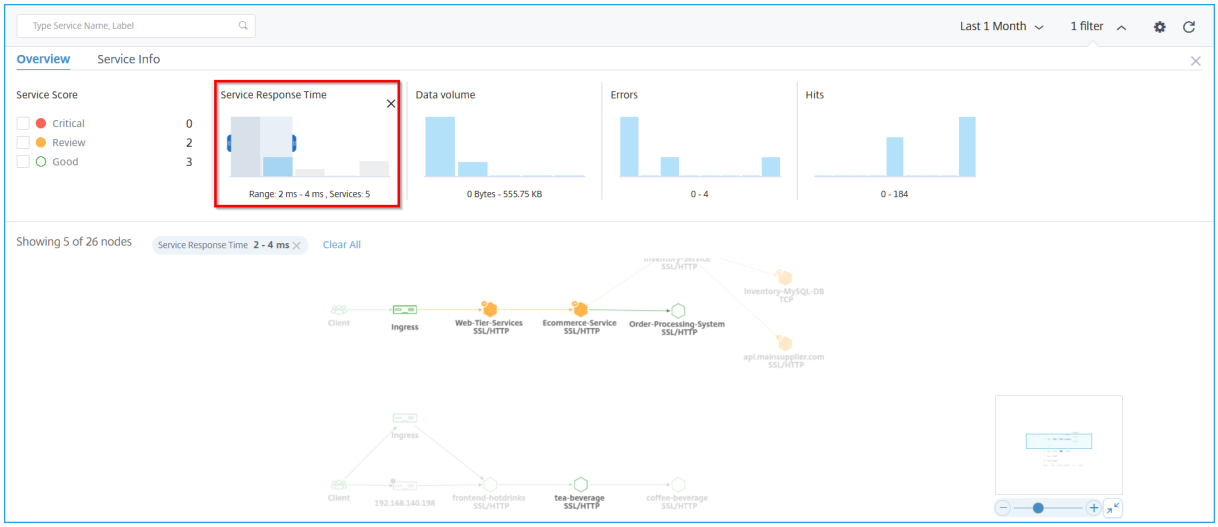
Cliquez sur un service et sélectionnez **Afficher les détails** pour afficher les détails du service. Pour plus d'informations, consultez Afficher les détails du service.

Appliquer les filtres

Vous pouvez appliquer des filtres pour afficher des informations de service spécifiques. Cliquez sur **Aucune liste de filtres** pour obtenir les options de filtre.

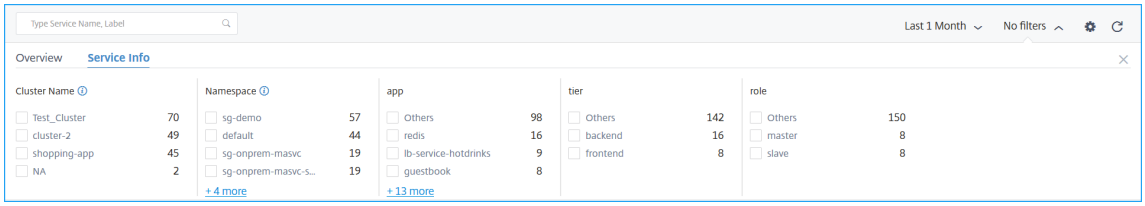


Par exemple, si vous souhaitez afficher les services dont la latence est inférieure à 150 ms, cliquez sur le graphique à barres situé sous **Temps de réponse du service** pour afficher les résultats.



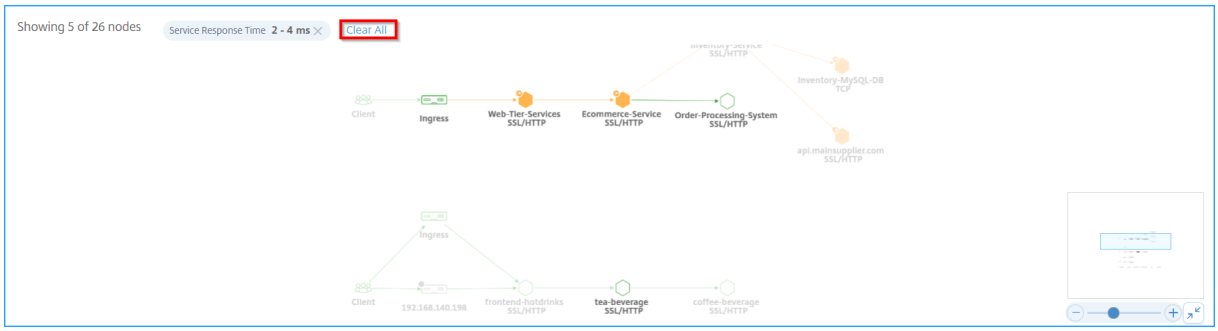
Cliquez sur **Infos sur le service** pour sélectionner et appliquer des filtres pour :

- **Cluster** : affiche tous les services applicables au ou aux clusters sélectionnés.
- **Espace de noms** : affiche tous les services applicables à l'espace de noms sélectionné.

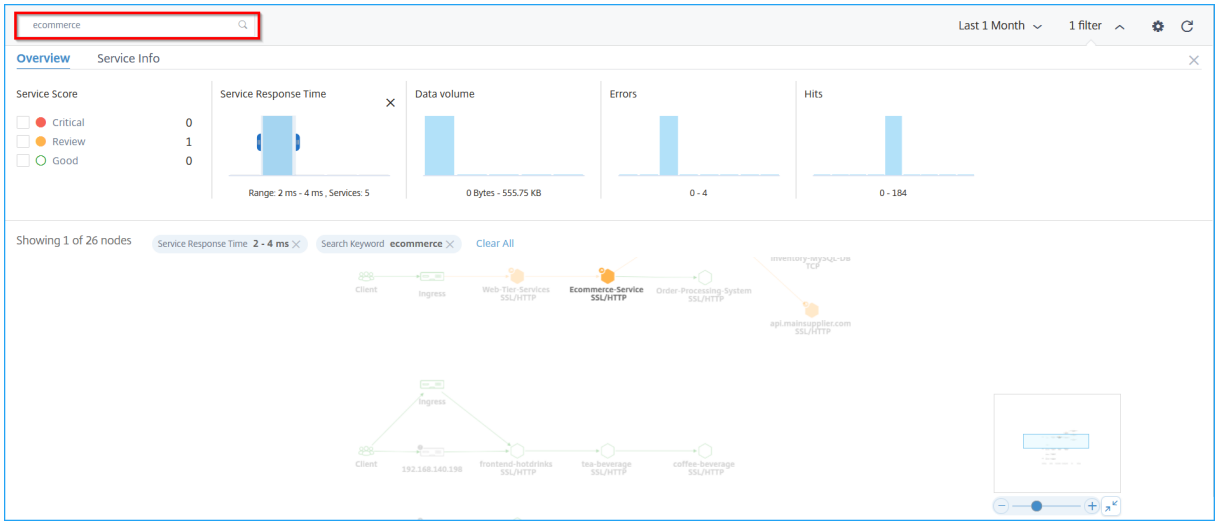


> **Remarque**
>
> Selon les étiquettes configurées pour le service dans la définition du service YAML de définition de service Kubernetes, vous pouvez également afficher d'autres options de filtre.

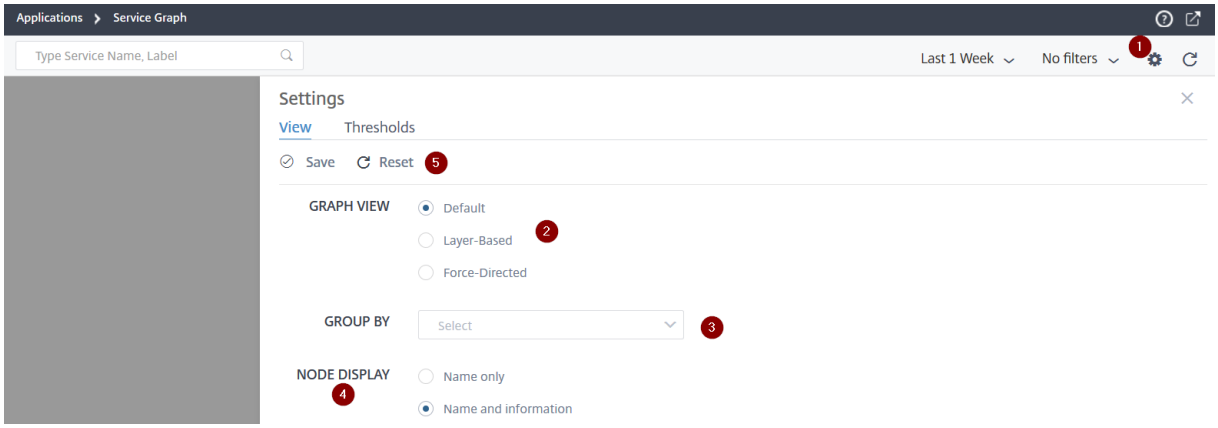
Cliquez sur **Effacer tout** pour effacer tous les filtres.



Vous pouvez également utiliser la zone de texte de recherche et saisir un nom de service pour afficher les résultats sur le graphe des services.



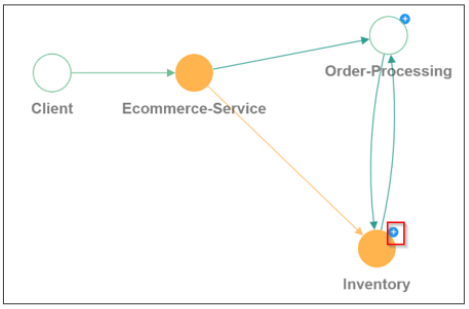
Utilisation de l'option Paramètres



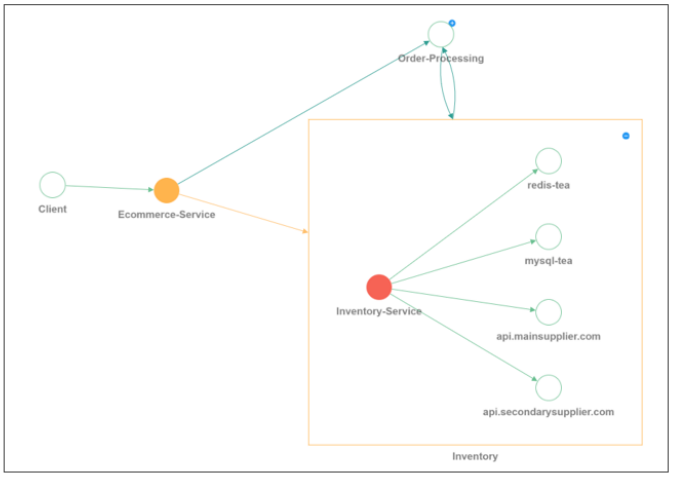
1 —Icône des paramètres

2 —Options pour afficher le graphe de service sous forme de vues par défaut, basées sur des couches ou dirigées par la force

3 —Sélectionnez les options dans la liste pour afficher les services en fonction des catégories. Après avoir sélectionné une catégorie dans la liste, cliquez sur **+** sur le graphique pour afficher tous les services



Collapsed view



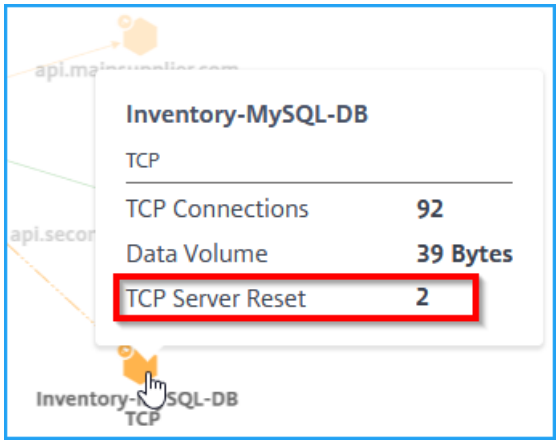
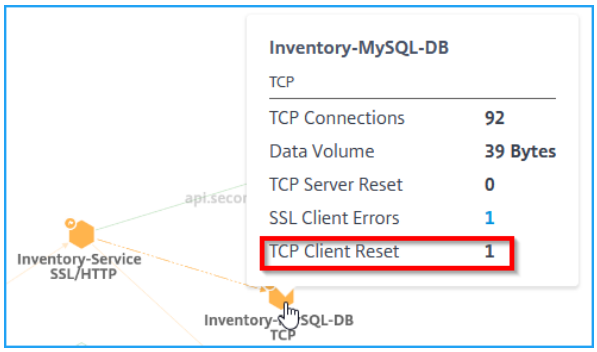
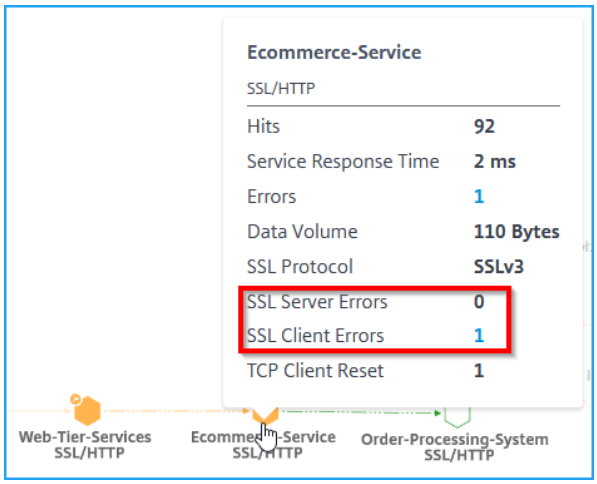
Expanded view

4 —Permet de sélectionner l'option sur la façon dont vous souhaitez afficher les services.

5 - Options pour enregistrer les paramètres ou pour réinitialiser la valeur par défaut.

Analyser les erreurs

Passez le pointeur de la souris sur un service qui indique des erreurs.

Erreur	Description
	La **réinitialisation du serveur TCP** indique le nombre total de réinitialisations TCP initiées depuis le serveur.
	La **réinitialisation du client TCP** indique le total des réinitialisations TCP initiées par le client.
	Les erreurs du client SSL indiquent le nombre total d'erreurs SSL provenant du client. (Par exemple, erreur d'authentification du client SSL).

Erreur	Description
	Les erreurs du serveur SSL Indiquez le nombre total d'erreurs SSL provenant du serveur. (Par exemple, certificat SSL inconnu)

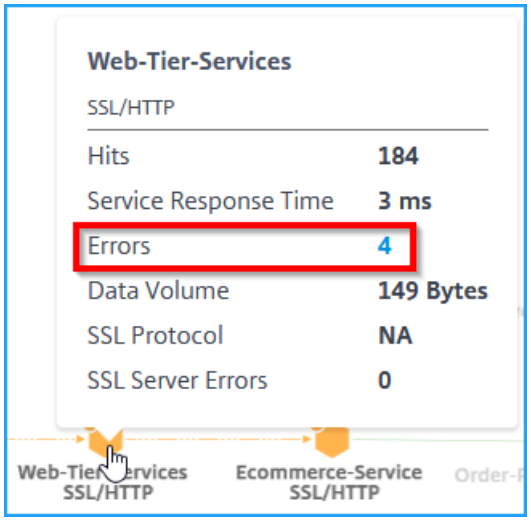
Remarque

- Le nombre d'erreurs client (quel que soit le type de protocole) s'affiche dans n'importe quel service si le nombre d'erreurs client est égal **ou supérieur à 1**.
- Le nombre d'erreurs du client affiché pour n'importe quel service indique que les erreurs proviennent du côté client.

Afficher les détails des transactions HTTP

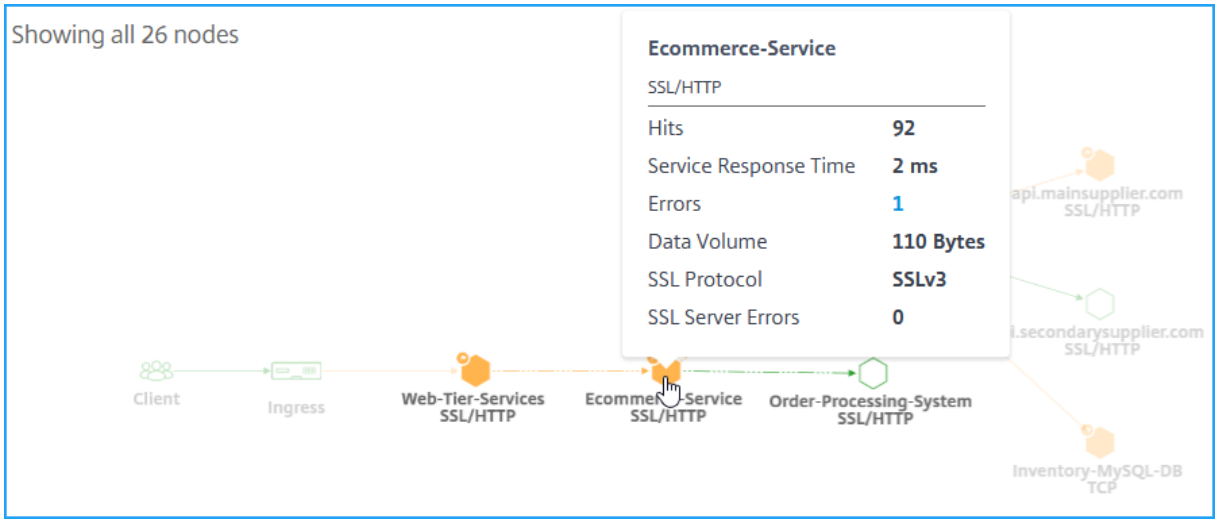
Remarque

Vous pouvez afficher les erreurs en plaçant le pointeur de la souris sur un service erroné et en cliquant sur le nombre de problèmes.

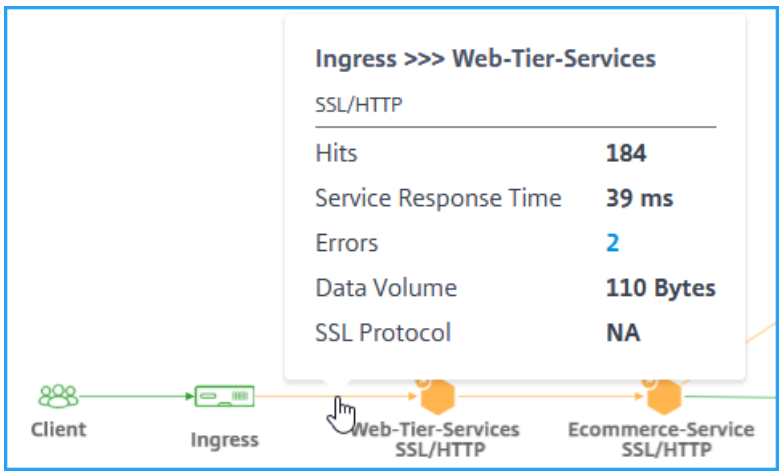


Selon l'exemple illustré dans l'image, vous pouvez afficher une carte réseau de bout en bout de votre application qui montre comment vos services de composants communiquent.

Lorsque vous placez le pointeur de la souris sur le **service de commerce**électronique, vous pouvez afficher les détails des métriques du **service de commerce**électronique.



Citrix ADM vous permet également de consulter les détails des transactions entre Ingress et les services. Passez le pointeur de la souris pour afficher des détails tels que le nombre total d'erreurs, le temps de réponse moyen du service, etc. entre l'entrée et le service.



Affichages —Indique le nombre total de requêtes reçues par le service.

Temps de réponse du service —Indique le temps de réponse moyen pris par le service pour répondre au délai jusqu'au premier octet (TTFB).

Erreurs —Indique le nombre total d'erreurs telles que 4xx, 5xx, etc.

Volume de données : indique le volume total de données traitées par le service.

Protocole SSL —Indique la version du protocole SSL.

Cliquez sur la flèche située entre l'**entrée** et le **service** pour afficher les transactions détaillées.

Pour plus d'informations, consultez Afficher les analyses pour les transactions Web.

Configurer les seuils dans le graphique de service

February 1, 2024

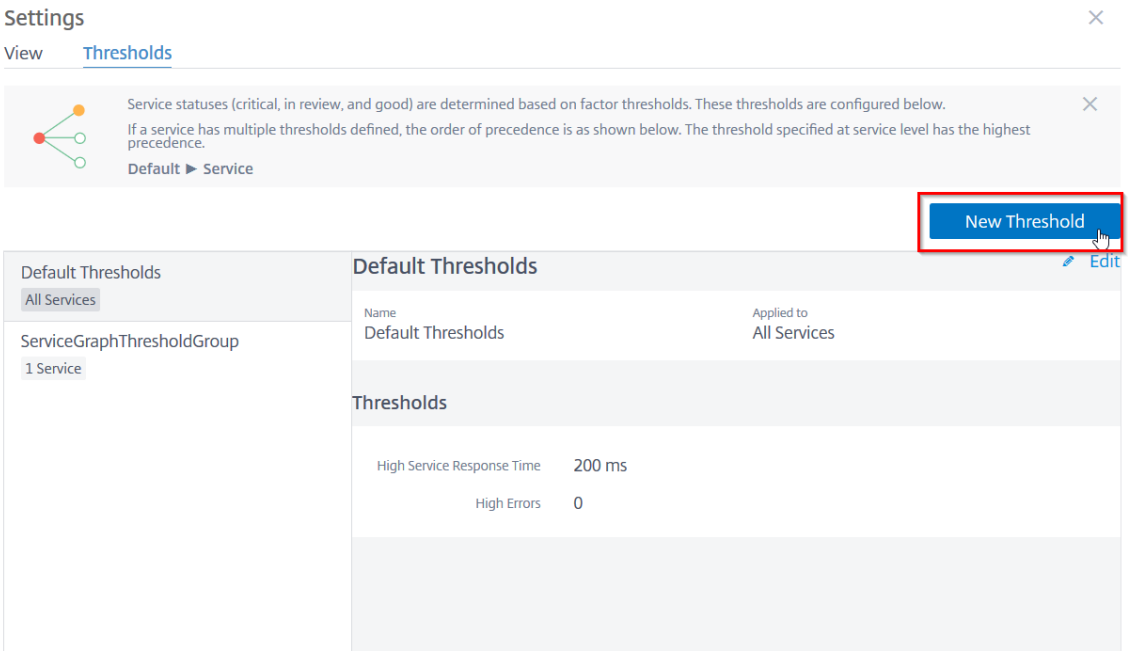
En tant qu'administrateur, vous pouvez configurer des seuils pour les services Kubernetes. Citrix ADM affiche l'état du service (Critique, Révision et Bon) en fonction du temps de réponse du service et du nombre d'erreurs. Par défaut, vous pouvez afficher le **seuil par défaut** (temps de réponse du service = 200 ms et nombre d'erreurs = 0) appliqué à tous les services.

> **Remarque**
>
> Vous ne pouvez pas supprimer le seuil par défaut.

Pour configurer un nouveau seuil :

Graphique en service :

1. Cliquez sur l'icône des paramètres et sélectionnez l'onglet **Seuils**.
2. Cliquez sur **Nouveau seuil** pour configurer un nouveau seuil.



   La page **Nouveau seuil** s'affiche.

3. Configurez les paramètres suivants :

   a) **Nom** : spécifiez un nom pour le seuil.

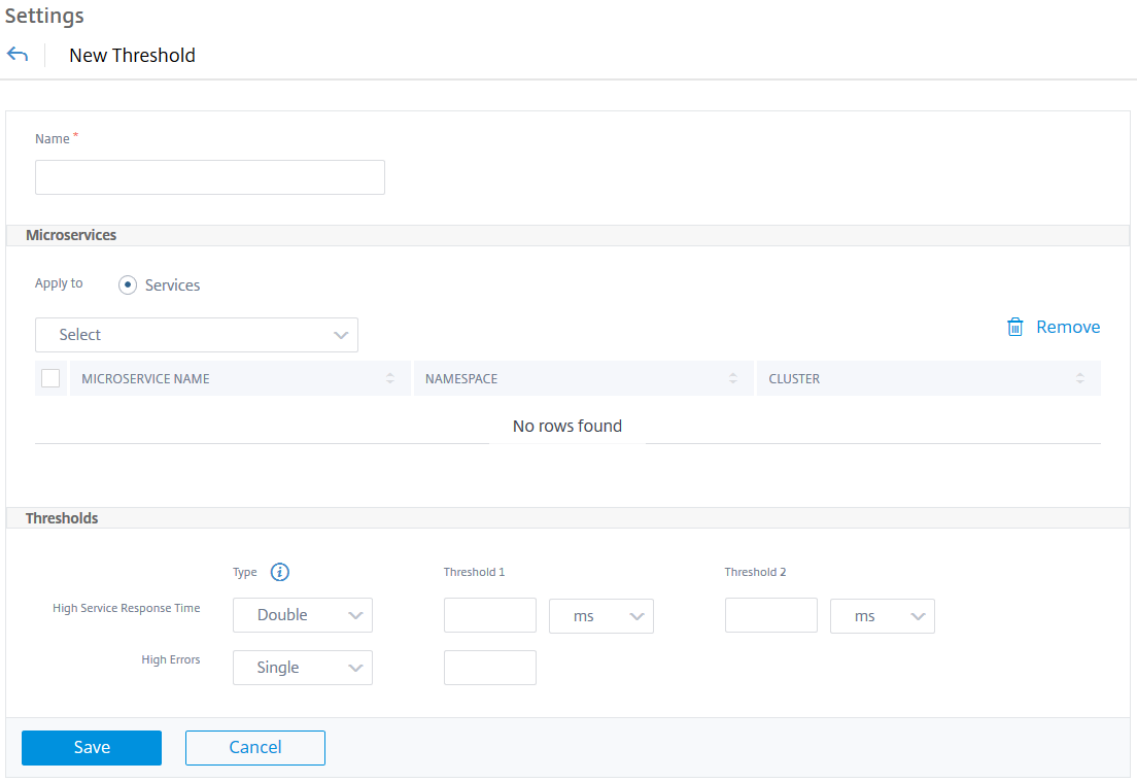
   b) Sous **Microservices**, sélectionnez les services auxquels vous souhaitez appliquer le seuil

c) Sous **Seuils**, sélectionnez **Simple** ou **Double** pour un temps de réponse élevé et des erreurs élevées

d) Spécifiez les valeurs de seuil.

> **Remarque**
>
> Si vous sélectionnez le double seuil, assurez-vous que :
>
> - La valeur du seuil 1 est inférieure à la valeur du seuil 2. Par exemple, si vous configurez le seuil 1 comme 250 ms, le seuil 2 doit être de 251 ms ou plus.
> - La valeur du seuil 1 ne doit pas être la même que la valeur Seuil 2.

4. Cliquez sur **Enregistrer**.



Le seuil a été créé avec succès. Vous pouvez afficher les détails des **seuils** dans la page Seuils.

Seuil unique

Lorsque vous configurez un seuil unique, Citrix ADM :

- Compare les valeurs actuelles avec les valeurs de seuil configurées
- Calcule la pénalité totale en fonction des seuils dépassés
- Affiche le score de service et l'état du service en fonction du calcul de la pénalité

Double seuil

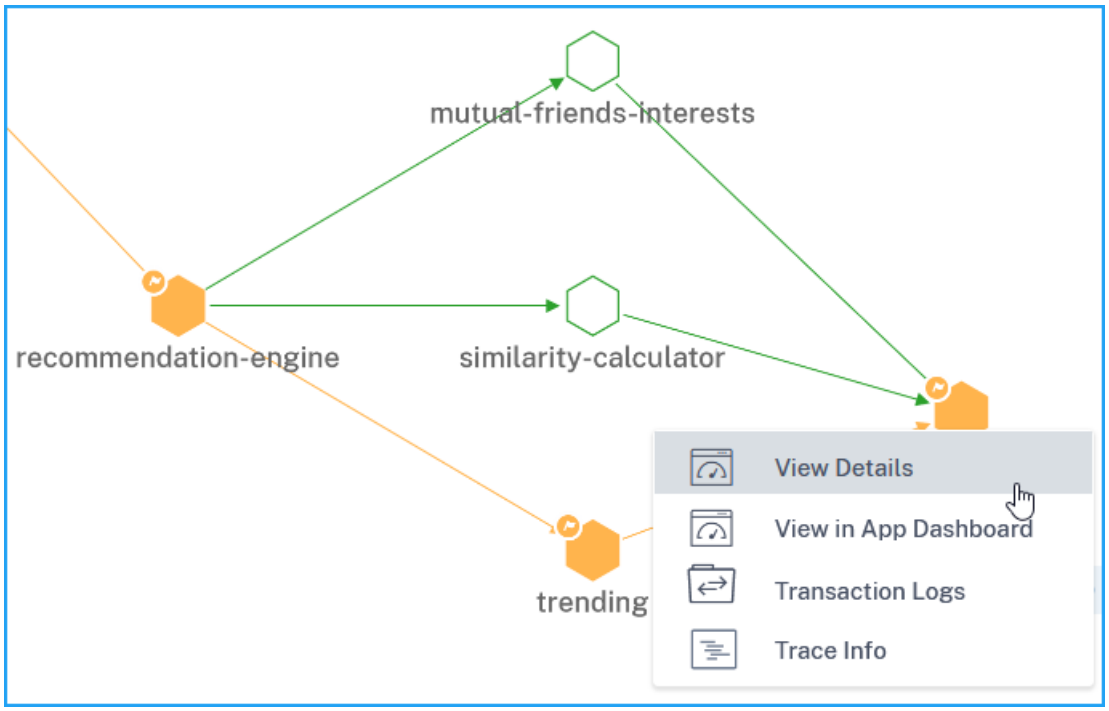
Lorsque vous configurez le double seuil, Citrix ADM :

- Compare les valeurs actuelles avec les valeurs de seuil configurées
- Vérifie si les valeurs actuelles sont :
  - Moins que le seuil 1
  - Entre le seuil 1 et le seuil 2
  - Supérieur au seuil 2
- Calcule la pénalité totale en fonction des seuils dépassés
- Affiche le score de service et l'état du service en fonction du calcul de la pénalité

Afficher les détails du service

February 1, 2024

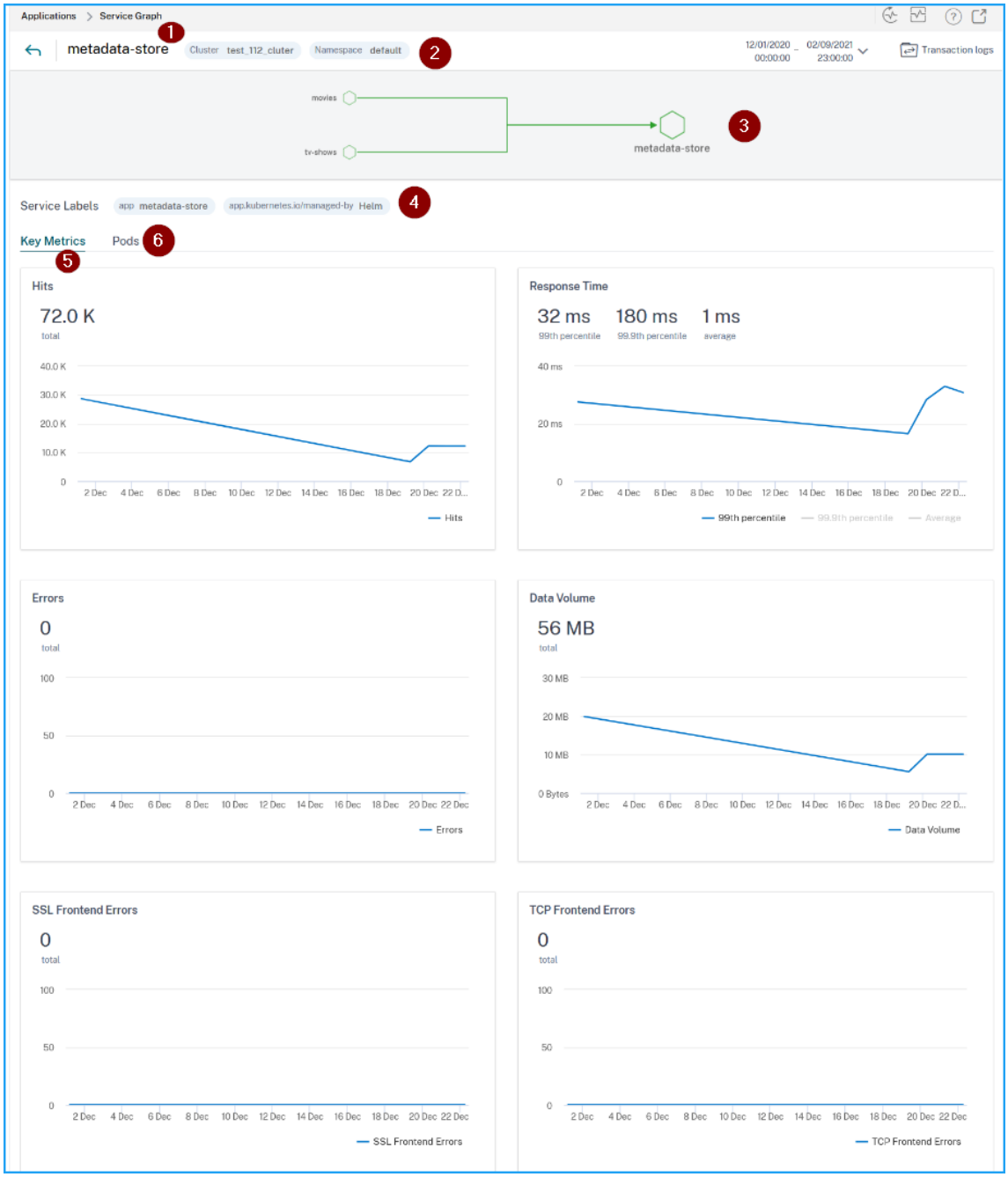
Cliquez sur un service et sélectionnez **Afficher les détails**.



La page des détails du service vous permet d'afficher :

- Nom du cluster dans lequel le service est hébergé (1)

- L'espace de noms et les étiquettes de service du service (2) (4)
- Tous les services entrants et sortants associés connectés au service sélectionné (3)
- Mesures de clé de service dans un format graphique telles que les accès, le temps de réponse, les erreurs, le volume de données, les erreurs frontales SSL et les erreurs frontales TCP (5).
- Les pods backend associés au service (6).



À l'aide de ces tendances de mesures clés, vous pouvez analyser les performances du service pour une durée spécifique.

La mesure **Temps de réponse** vous permet d'afficher :

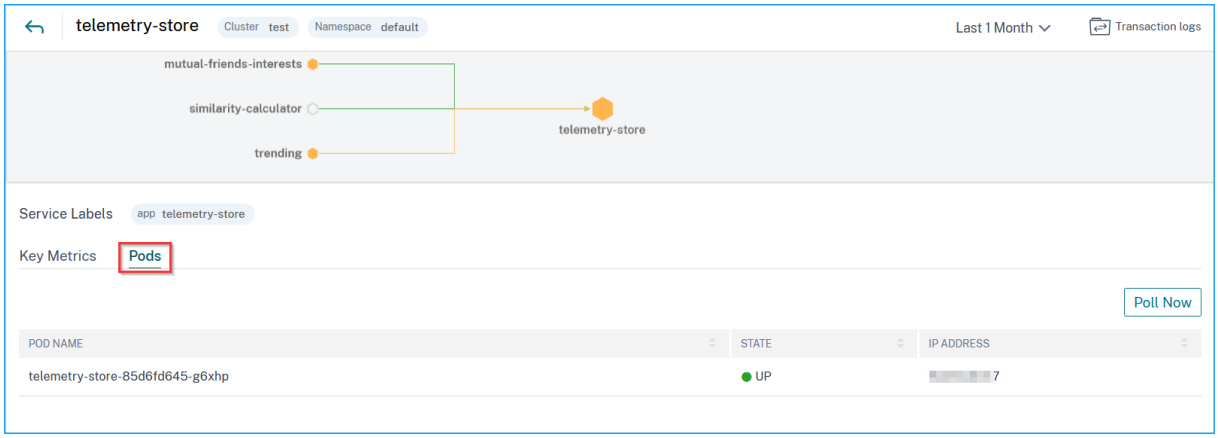
- **99e centile** —Indique que 99 % des demandes pour la durée sélectionnée sont inférieures à 32 ms (selon l'exemple d'image).
- **Moyenne** —Indique le temps de réponse moyen du service
- **99,9e centile** —Indique le temps de réponse le plus élevé du service

Détails des mesures

Métriques	Description
Accès	Nombre total de demandes reçues par le service
Erreurs	Nombre total d'erreurs HTTP du service
Temps de réponse du service	Temps de réponse moyen pris par le service pour répondre à la période de temps au premier octet (TTFB).
Volume de données	Volume total de données traité par le service
Erreurs front-end SSL	Nombre total d'erreurs front-end SSL provenant du service. Par exemple : SSL CLIENTAUTH FAILURE
Erreurs back-end SSL	Nombre total d'erreurs SSL back-end du service. Par exemple : Erreurs du client SSL
Erreurs back-end TCP	Nombre total d'erreurs de back-end TCP provenant du service. Par exemple : Réinitialisation du serveur TCP
Erreurs front-end TCP	Nombre total d'erreurs front-end TCP provenant du service. Par exemple : Réinitialisation du client TCP

Afficher les détails du module backend

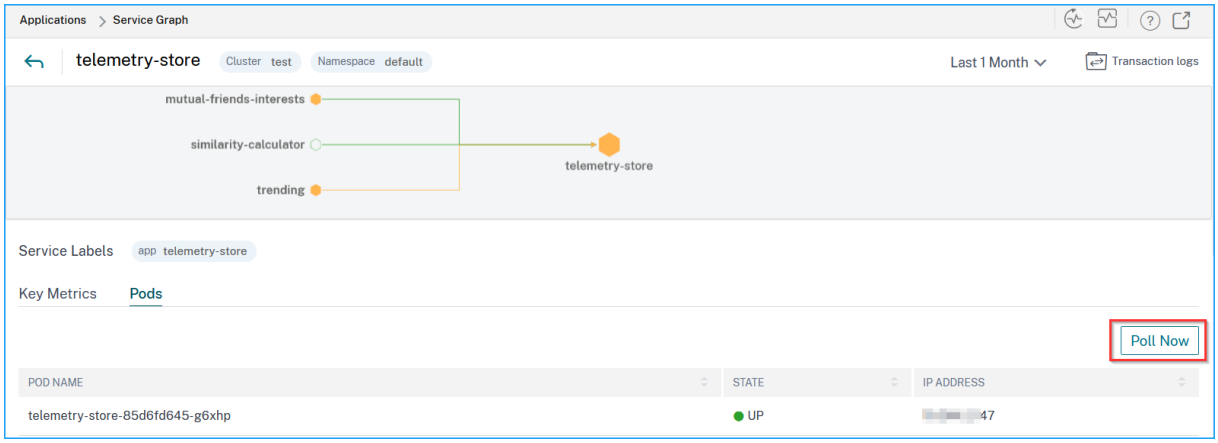
Cliquez sur l'onglet **Pods** pour afficher les pods backend associés au service.



- **Nom du module** —Indique le nom du module
- **Statut** : indique si le conteneur est en cours d'exécution (UP) ou non (DOWN).
- **Adresse IP** —Indique l'adresse IP du conteneur

Utilisez l'option Sondage maintenant pour obtenir l'état du conteneur

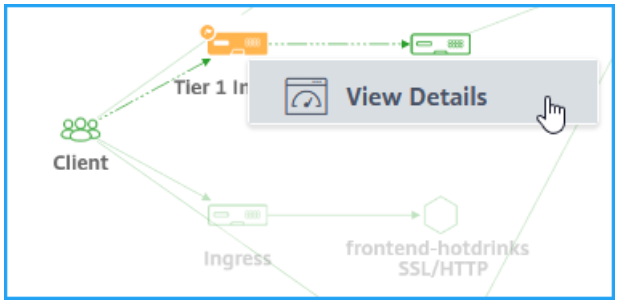
L'option **Sondage maintenant** récupère le dernier état du conteneur à partir du cluster.



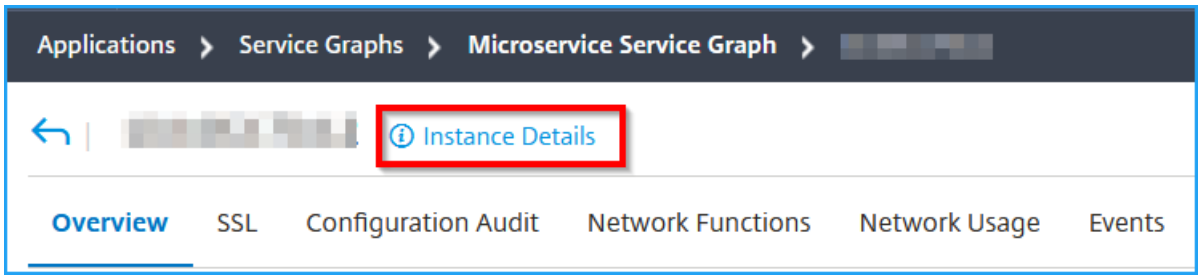
Afficher les détails d'entrée pour résoudre les problèmes

February 1, 2024

Dans le graphique de service, cliquez sur l'entrée et sélectionnez **Afficher les détails** pour visualiser les détails de l'instance Citrix ADC configurée pour le cluster Kubernetes.

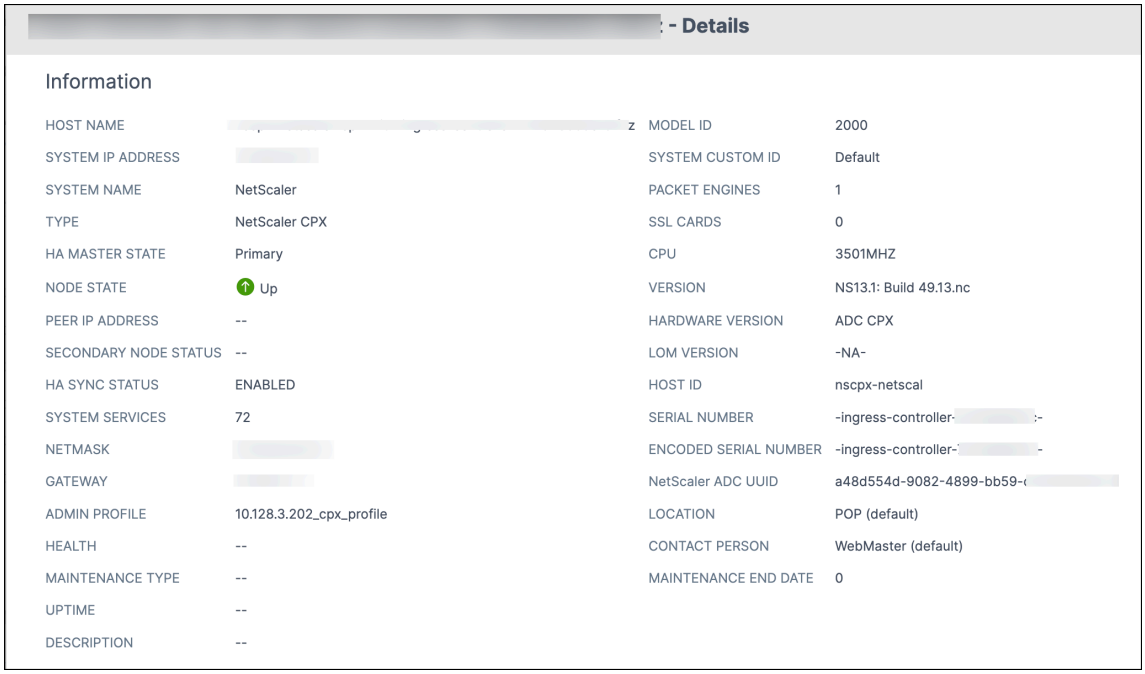


Cliquez sur **Détails de l'instance** pour afficher les détails.

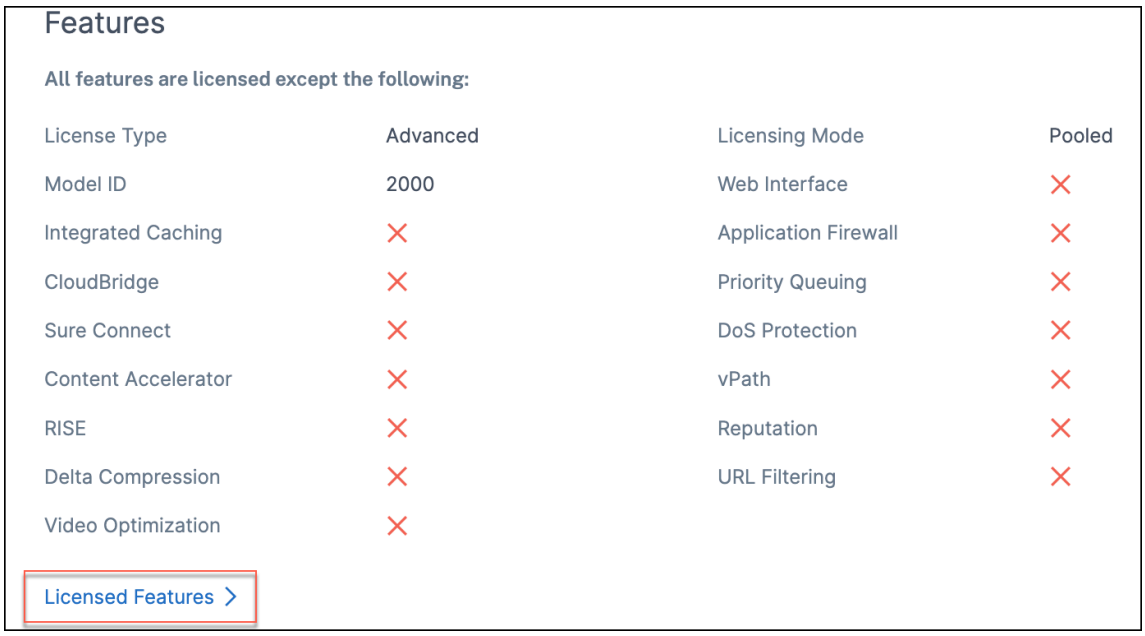


Les détails suivants s'affichent :

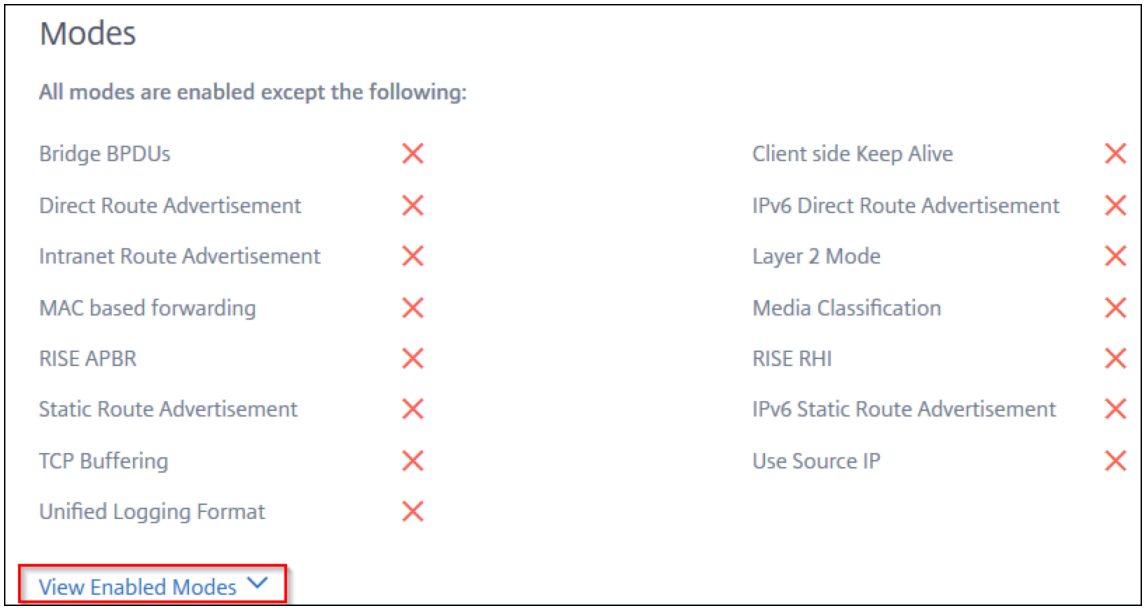
- **Informations** : détails d'instance tels que le type d'instance, le type de déploiement, la version, le modèle, etc.



- **Fonctionnalités** : par défaut, les fonctionnalités qui ne sont pas sous licence sont affichées. Cliquez sur **Fonctionnalités sous licence** pour afficher les fonctionnalités sous licence.

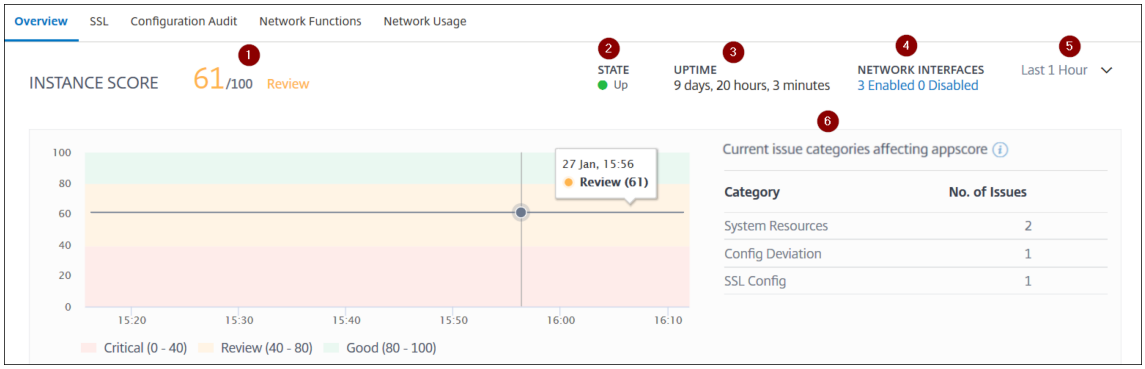


- **Modes** : par défaut, tous les modes désactivés sur l'instance sont affichés. Cliquez sur **Afficher les modes activés** pour afficher les modes activés sur l'instance.



Le tableau de bord de l'instance présente un aperçu de l'instance dans lequel vous pouvez consulter les informations suivantes :

- **Score d'instance**



1 —Indique le score actuel de l'instance Citrix ADC pour la durée sélectionnée. Le score final est calculé comme **100 moins le total des pénalités**. Le graphique affiche les plages de score pour la durée sélectionnée.

2 —Indique l'état actuel de l'instance Citrix ADC, par exemple En **haut**, **en bas**et **hors service**.

3 —Indique la durée pendant laquelle l'instance de Citrix ADC est en cours d'exécution.

4 —Indique le nombre total d'interfaces réseau activées et désactivées pour l'instance. Cliquez pour afficher les détails tels que le nom de l'interface réseau et son état (activé ou désactivé).

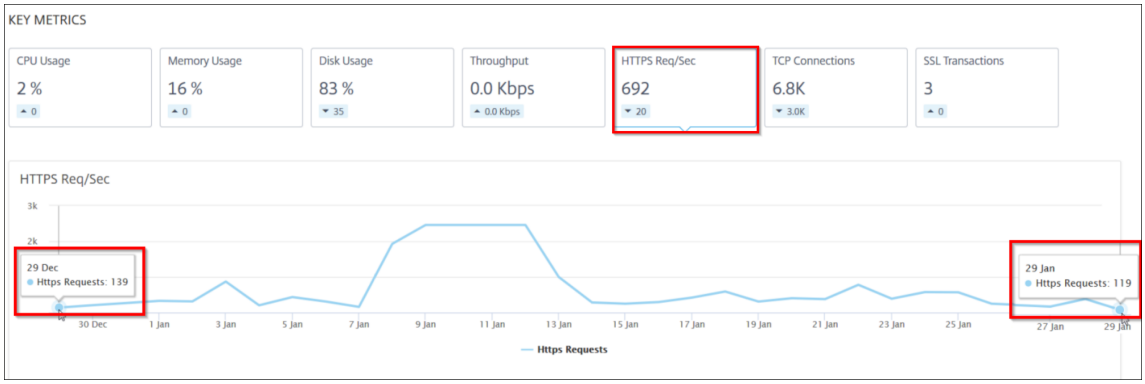
5 —Sélectionnez la durée dans la liste pour afficher les détails de l'instance.

6 —Affiche le nombre total de problèmes et la catégorie de problèmes de l'instance ADC.

- **Indicateurs clés**

  Cliquez sur chaque onglet pour afficher les détails. Dans chaque mesure, vous pouvez afficher la valeur moyenne et la valeur de différence pour l'heure sélectionnée.

  L'image suivante est un exemple pour HTTPS Req/Sec et la durée sélectionnée est pour 1 dernier mois. La valeur **692** est la moyenne HTTPS Req/Sec pour la durée du dernier mois et la valeur **20** est la valeur de différence. Dans le graphique, la première valeur est **139** et la dernière valeur est **119**. La valeur de la différence est de **139** —**119 = 20**.



  Vous pouvez afficher les mesures d'instance suivantes dans un format graphique pour la durée sélectionnée :

- **Utilisation du processeur** : % de CPU moyen de l'instance pendant la durée sélectionnée (s'affiche à la fois pour le processeur par paquets et pour le processeur de gestion).
- **Utilisation de la mémoire** : % d'utilisation moyenne de la mémoire de l'instance pendant la durée sélectionnée.
- **Utilisation du disque** : pourcentage d'espace disque moyen de l'instance pendant la durée sélectionnée.
- **Débit** : débit réseau moyen traité par l'instance pendant la durée sélectionnée.
- **Demande HTTPS/sec** : nombre moyen de requêtes HTTPS reçues par l'instance pendant la durée sélectionnée.
- Connexions**TCP** —**Les connexions** TCP moyennes établies par le client et le serveur pendant la durée sélectionnée.
- **Transactions SSL** : transactions SSL moyennes traitées par l'instance pendant la durée sélectionnée.

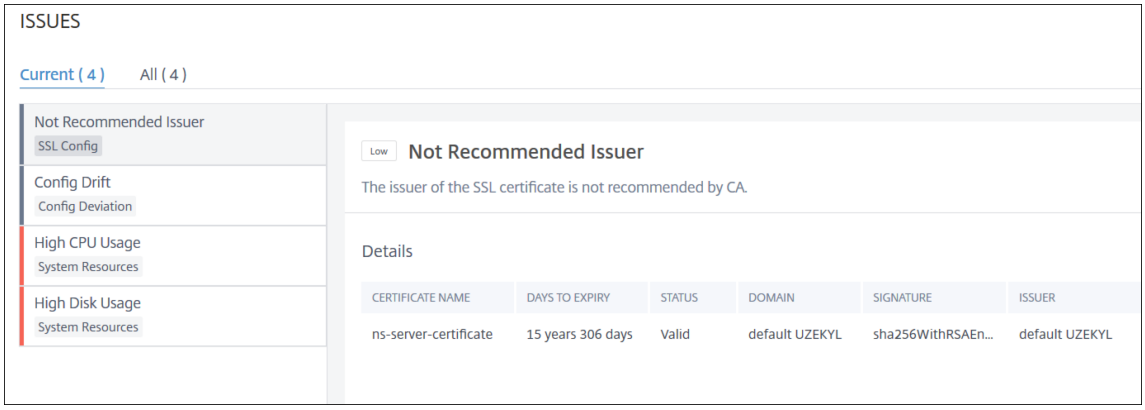
- **Problèmes**

  Vous pouvez consulter les problèmes suivants qui se produisent dans l'instance Citrix ADC :

Catégorie de problème	Description	Problèmes
Ressources système	Affiche tous les problèmes liés à la ressource système Citrix ADC tels que le processeur, la mémoire, l'utilisation du disque, etc.	– Utilisation élevée du processeur – Utilisation élevée de la mémoire – Utilisation élevée du disque – Défaillances de cartes SSL – Panne de courant – Erreur de disque – Erreur Flash – Rejets de cartes réseau
Configuration SSL	Affiche tous les problèmes liés à la configuration SSL sur l' instance Citrix ADC.	– Les certificats SSL ont expiré

Catégorie de problème	Description	Problèmes
		– Émetteur non recommandé – Algorithme non recommandé – Intensité clé non recommandée
Déviation de configuration	Affiche tous les problèmes liés aux tâches de configuration appliquées dans l'instance Citrix ADC.	– Dérive de configuration – Running vs Template
Problèmes de capacité	Affiche les problèmes de capacité ADC. L'ADM interroge ces événements toutes les cinq minutes à partir de l'instance ADC et affiche les baisses de paquets ou les incréments de compteur de limite de vitesse s'il existe. Les problèmes sont classés en fonction des paramètres de capacité suivants.	– Limite de débit atteinte
Réseau	Affiche les problèmes opérationnels qui se produisent dans les instances.	Pour plus d'informations, consultez Analyse d'infrastructure améliorée avec de nouveaux indicateurs.

Cliquez sur chaque onglet pour analyser et résoudre le problème. Par exemple, considérez qu'une instance présente les erreurs suivantes pour la durée sélectionnée :



- L'onglet **Actuel** affiche les problèmes opérationnels ADC actuels qui affectent le score de l'instance.
- L'onglet **Tout** affiche tous les problèmes infra détectés pour la durée sélectionnée.

Suivi distribué

February 1, 2024

Dans le graphique des services, vous pouvez utiliser la vue de suivi distribuée pour :

- Analysez les performances globales du service.
- Visualisez le flux de communication entre le service sélectionné et ses services interdépendants.
- Identifier le service qui indique des erreurs et dépanner le service erroné
- Afficher les détails de transaction entre le service sélectionné et chaque service interdépendant.

Conditions préalables

Pour afficher les informations de suivi du service, vous devez :

- Assurez-vous qu'une application conserve les en-têtes de trace suivants, tout en envoyant tout trafic est-ouest :

- x-request-id
- x-b3-traceid
- x-b3-spanid
- x-b3-parentspanid
- x-b3-sampled
- x-b3-flags
- x-ot-span-context

- Pour les **versions CIC antérieures à la version 1.7.23**, mettez à jour le fichier YAML CPX avec la valeur `NS_DISTRIBUTED_TRACING` et `yes`

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: cpx-ingress
spec:
  selector:
    matchLabels:
      app: cpx-ingress
  replicas: 1
  template:
    metadata:
      name: cpx-ingress
      labels:
        app: cpx-ingress
      annotations:
    spec:
      serviceAccountName: cpx-ingress-k8s-role
      containers:
        - name: cpx-ingress
          image: "quay.io/citrix/citrix-k8s-cpx-ingress:13.0-47.103"
          securityContext:
            privileged: true
          env:
          - name: "EULA"
            value: "yes"
          - name: "KUBERNETES_TASK_ID"
            value: ""
          - name: "NS_MGMT_SERVER"
            value: "192.168.0.1"
          - name: "NS_MGMT_FINGER_PRINT"
            value: "12:12:AB:CD:EA:72:E3:10:47:CD:AF:AG:C3:B7:82:6O:97:3D:E2:5D"
          - name: "NS_HTTP_PORT"
            value: "9080"
          - name: "NS_HTTPS_PORT"
            value: 9443"
          - name: "LOGSTREAM_COLLECTOR_IP"
            value: "192.168.0.1"
          imagePullPolicy: Always
```

- Pour les **versions CIC postérieures à 1.7.23**, vous devez utiliser un ConfigMap.

  ConfigMaps vous permet de séparer vos configurations de vos pods et de rendre vos charges de travail portables. Grâce à ConfigMaps, vous pouvez facilement modifier et gérer vos configurations de charge de travail et réduire le besoin de coder en dur les données de configuration en fonction des spécifications du module.

  Avec la prise en charge de ConfigMap, vous pouvez mettre à jour la configuration automatiquement tout en conservant le conteneur de Citrix ingress controller en cours d'exécution. Vous n'avez pas besoin de redémarrer le module après la mise à jour. Pour plus d'informations, voir Prise en charge de ConfigMap pour le contrôleur d'entrée.

À l'aide de ConfigMap, vous pouvez activer ou désactiver le suivi distribué, les événements, les journaux d'audit, etc. Pour utiliser le ConfigMap :

1. Créez un fichier YAML en utilisant les paramètres requis.

   Le suivi distribué est activé dans le fichier YAML suivant et d'autres variables telles que les journaux d'audit, les événements et les transactions sont désactivés :

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: cic-configmap
  namespace: default
data:
  LOGLEVEL: 'debug'
  NS_PROTOCOL: 'http'
  NS_PORT: '80'
  NS_HTTP2_SERVER_SIDE: 'ON'
  NS_ANALYTICS_CONFIG:
    distributed_tracing:
      enable: 'true'
      samplingrate: 100
    endpoint:
      server: <ADM-AgentIP> / <ADM-AppserverIP>
    timeseries:
      port: 5563
      metrics:
        enable: 'true'
        mode: 'avro'
      auditlogs:
        enable: 'false'
      events:
        enable: 'false'
    transactions:
      enable: 'false'
      port: 5557
<!--NeedCopy-->
```

   > Remarque
   >
   > Vous pouvez fournir les valeurs pour `Samplingrate` comprises entre 0 et 100. Citrix ADM affiche le nombre de transactions de suivi mentionné.

2. Déployez ConfigMap à l'aide de :

   `kubectl create -f <configmap-yaml>.yaml`

3. Modifiez le fichier CPX YAML et utilisez `envFrom` ou `args` pour spécifier les arguments suivants :

```
envFrom:
 - configMapRef:
```



```
      name: cic-configmap
<!--NeedCopy-->
```

OU

```
args:
   - --configmap
     default/cic-configmap
```

4. Si vous souhaitez modifier la valeur d'une variable, modifiez les valeurs dans ConfigMap. Dans cet exemple, toutes les autres variables sont changées de **false** à **true**.

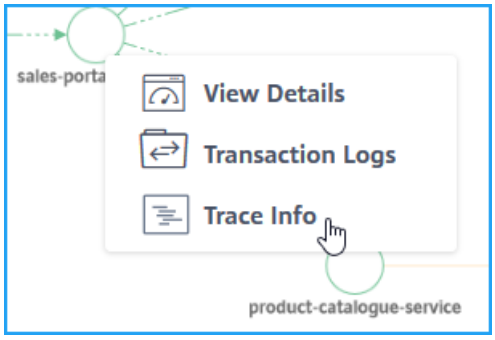
```
apiVersion: v1
kind: ConfigMap
metadata:
  name: cic-configmap
  namespace: default
data:
  LOGLEVEL: 'debug'
  NS_PROTOCOL: 'http'
  NS_PORT: '80'
  NS_HTTP2_SERVER_SIDE: 'ON'
  NS_ANALYTICS_CONFIG:
    distributed_tracing:
      enable: 'true'
      samplingrate: 100
    endpoint:
      server: <ADM-AgentIP> / <ADM-AppserverIP>
    timeseries:
      port: 5563
      metrics:
        enable: 'true'
        mode: 'avro'
      auditlogs:
        enable: 'true'
      events:
        enable: 'true'
    transactions:
      enable: 'true'
      port: 5557
  <!--NeedCopy-->
```

5. Appliquez à nouveau ConfigMap à l'aide de la commande suivante :

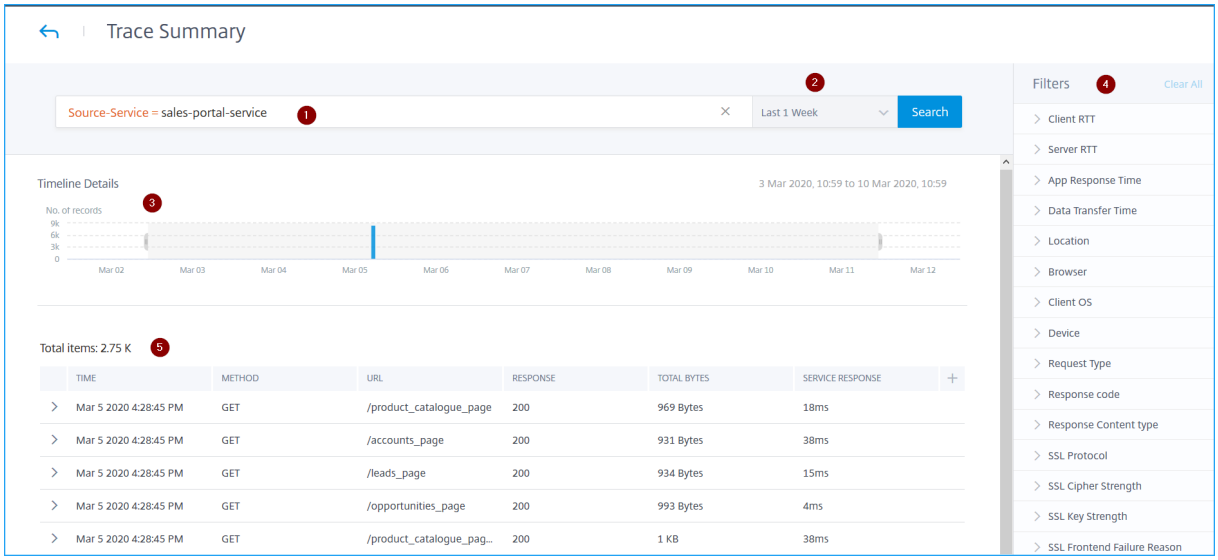
```
kubectl apply -f <yaml-file>.yaml
```

Afficher les détails du suivi du service

Dans le graphique des services, cliquez sur un service, puis sélectionnez **Trace Info**.



La page Résumé du suivi s'affiche pour le service sélectionné.



Le **résumé du suivi** affiche :

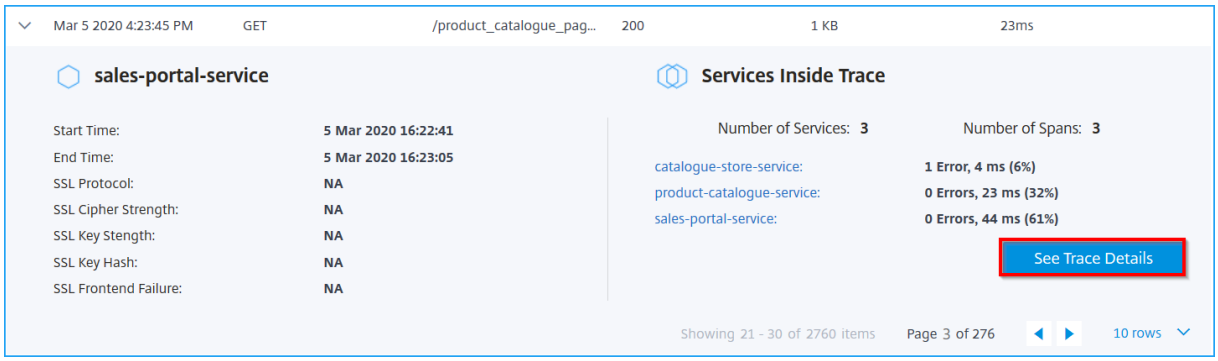
- Une recherche avancée qui vous permet de rechercher des transactions avec des suggestions et des opérateurs (1). Pour plus d'informations, consultez la section Recherche avancée.
- Liste de durée de temps qui vous permet de sélectionner la durée de temps telle que 1 heure, 12 heures, 1 jour, 1 semaine, 1 mois et heure personnalisée (2).
- Le graphique des détails de la chronologie qui vous permet de faire glisser et sélectionner pour afficher les résultats pendant une durée spécifique (3).
- Le panneau Filtres qui vous permet de sélectionner des options pour chaque métrique (4).
- Les détails de la transaction pour le service sélectionné (5).

Afficher les détails de la transaction

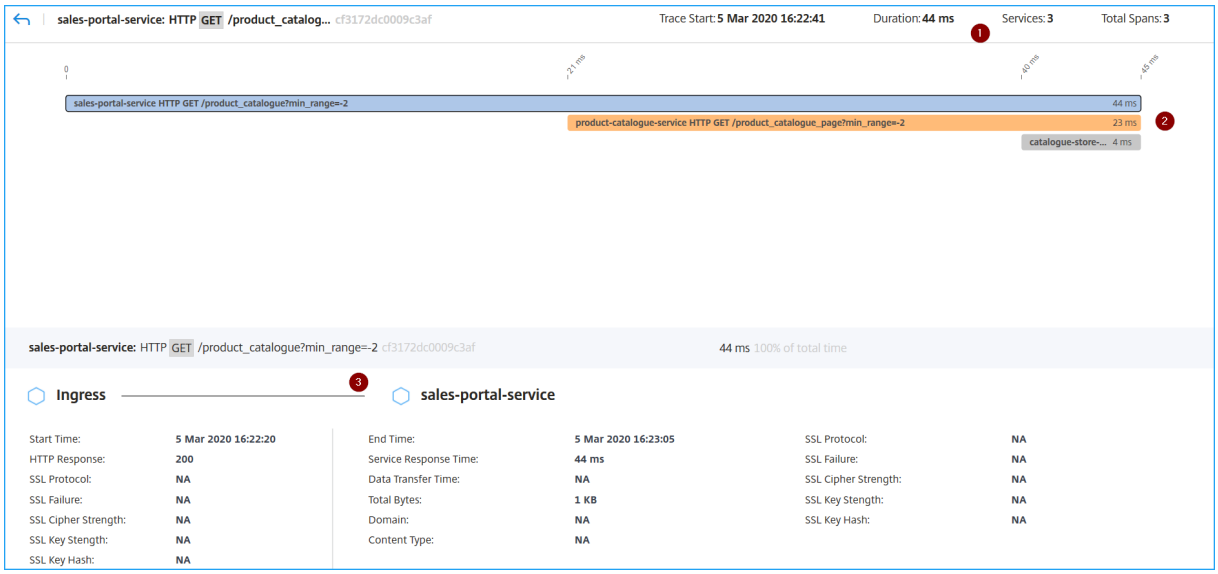
Cliquez sur une transaction pour accéder à des informations détaillées. Vous pouvez consulter les détails des transactions pour le service sélectionné, tels que :

- Heure de début
- Heure de fin
- Mesures SSL
- Communication avec des services interdépendants (ainsi que les erreurs et le temps de réponse pour chaque service).

L'exemple suivant indique une erreur provenant de `catalogue-store-service`. Cliquez sur **Voir les détails du suivi** pour plus de détails.



La page Détails du suivi s'affiche.

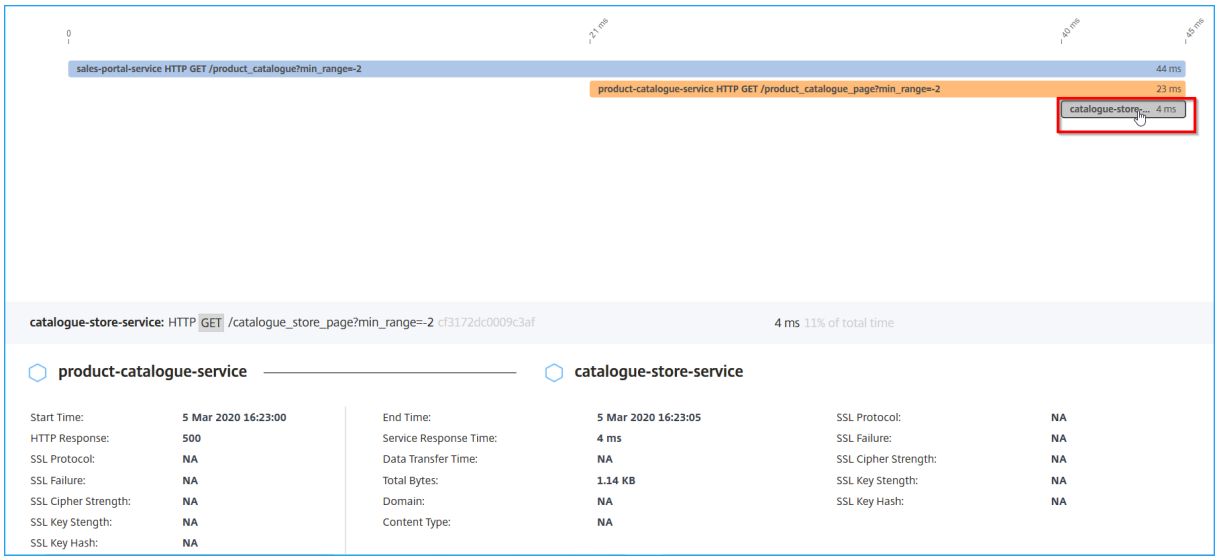


1 —Affiche l'heure de début, le temps de réponse, le total des services et la durée totale de la transaction.

2 —Affiche les détails du service sélectionné qui a communiqué avec ses services d'interdépendance. Vous pouvez cliquer sur chaque transaction pour en afficher les détails.

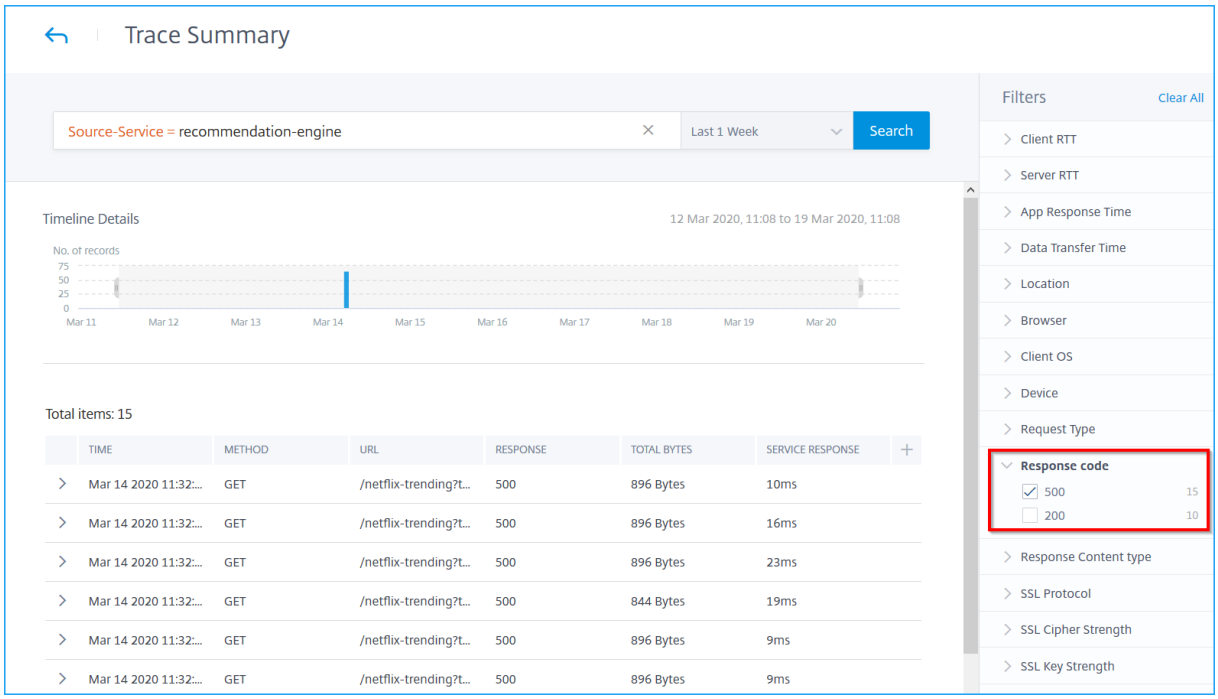
3 —Affiche les détails de la transaction pour chaque service.

Selon l'image d'exemple, `catalogue-store-service` indique une erreur. Cliquez sur la transaction disponible pour `catalogue-store-service`.



Les détails de la transaction entre `product-catalogue-service` et `catalogue-store-service` indiquent que la réponse HTTP est 500. Grâce à ces informations, en tant qu'administrateur, vous pouvez analyser le service erroné et le résoudre `product-catalogue-service` afin de le résoudre.

Vous pouvez également filtrer les résultats en sélectionnant les options de chaque métrique dans le panneau **Filtres** . Par exemple, si vous souhaitez voir toutes les transactions 5xx, cliquez sur **Code de réponse** et sélectionnez **500**.



- **Client RTT** : durée pendant laquelle un paquet doit être acheminé depuis le client.
- **Serveur RTT** : durée pendant laquelle un paquet doit être acheminé depuis le serveur.
- Temps de**réponse de l'application : temps**de réponse moyen de l'application
- **Temps de transfert des**données : taille du transfert de données et vitesse à laquelle la transmission peut se faire depuis/vers un service.
- **Lieu** : L'adresse du client
- **Navigateur** : types de navigateurs utilisés par les clients. Par exemple : Chrome, Firefox.
- Système d'**exploitation client** : système d'exploitation client basé sur les détails de l'agent utilisateur du navigateur.
- **Appareil** : les appareils basés sur les détails de l'agent utilisateur du navigateur. Par exemple : Tablet, Mobile.
- **Type de demande : type**de demande de transaction. Par exemple : GET.
- **Code de réponse** : code de réponse reçu du serveur. Par exemple : 501, 404, 200.
- **Type de contenu de réponse** : le type de contenu de la transaction. Si la demande du client porte sur du texte/html, la réponse du serveur doit être text/html.
- **Protocole SSL** : version du protocole SSL utilisée par les clients. Par exemple : SSLv3.
- **Force de chiffrement SSL : puissance**de chiffrement basée sur la taille de la clé du certificat SSL, telle que élevée, moyenne et faible.
- Force de**clé SSL : La force**de chiffrement SSL est calculée à partir de la taille de la clé du certificat SSL. La longueur de la clé définit la sécurité de l'algorithme SSL. Par exemple : 2048
- **Raison d'échec SSL frontal** : le message d'erreur de connexion SSL frontal. Par exemple : SSL CLIENTAUTH FAILURE

Afficher les détails de diagnostic pour des données partielles ou incomplètes dans le graphique de service

February 1, 2024

Une fois que vous avez terminé la configuration requise du graphe de service et que vous avez ajouté le cluster Kubernetes dans Citrix ADM, le graphique de service commence à remplir les données. Dans certains scénarios, vous pouvez observer que le graphique de service affiche des données partielles ou aucune donnée. Voici quelques-unes des raisons possibles pour les données partielles ou l'absence de données dans le graphique de service :

- L'itinéraire statique n'est pas configuré
- L'état du cluster Kubernetes est en panne
- Échec de l'enregistrement CPX
- Les serveurs virtuels CPX ne sont pas sous licence
- La configuration d'analyse requise n'est pas définie qui empêche le graphique de service de charger toutes les données

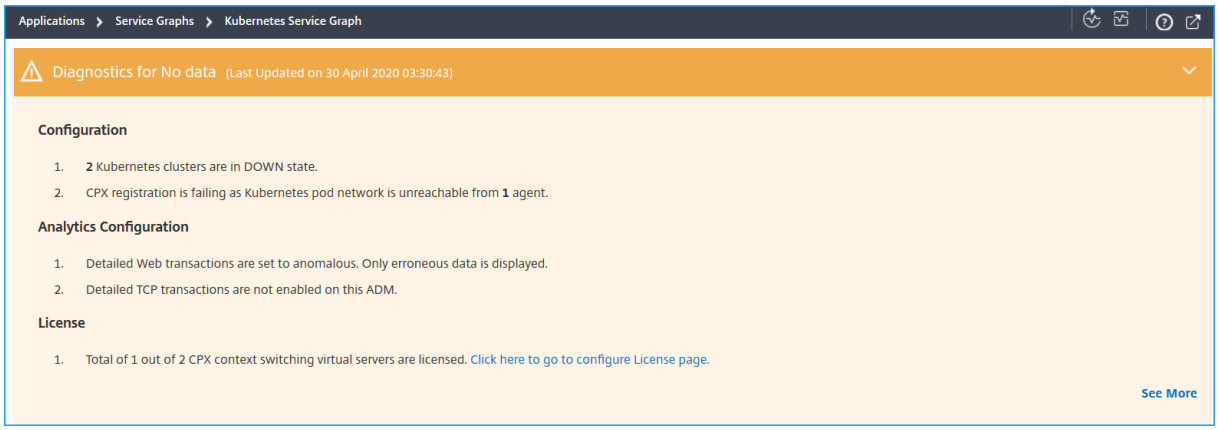
En tant qu'administrateur, vous pourriez avoir du mal à analyser les raisons lorsque vous voyez un graphique de service affichant des données partielles ou aucune donnée. La page Informations de diagnostic dans le graphique de service vous permet de voir les raisons possibles et les actions requises pour résoudre les problèmes de données partielles ou aucun problème de données.

Dans Citrix ADM, accédez à **Applications** > **Service Graph** et cliquez sur l'onglet **Microservices**.

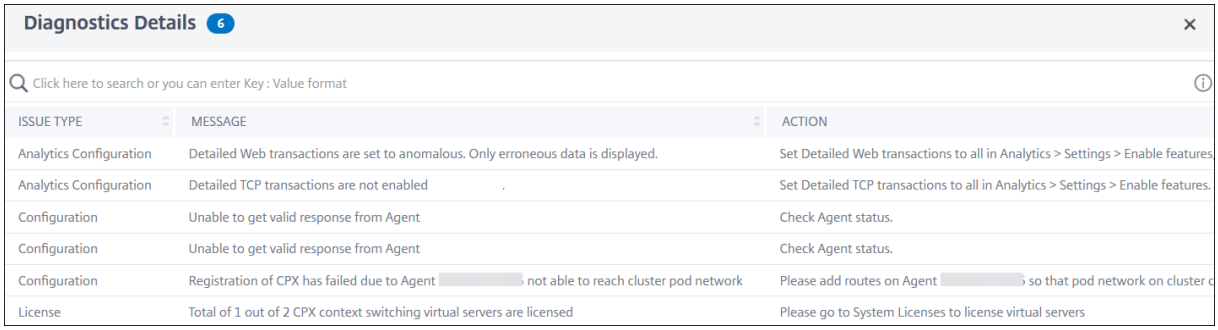
Diagnostics pour aucune donnée

Si le graphique de service n'affiche aucune donnée, le message de diagnostic suivant s'affiche.

Cliquez sur ** pour afficher les détails. Vous pouvez afficher les raisons possibles pour le graphique de service n'affichant aucune donnée. L'image suivante est un exemple pour aucune donnée dans le graphique de service.



Cliquez sur **Voir plus** pour afficher les détails des problèmes.

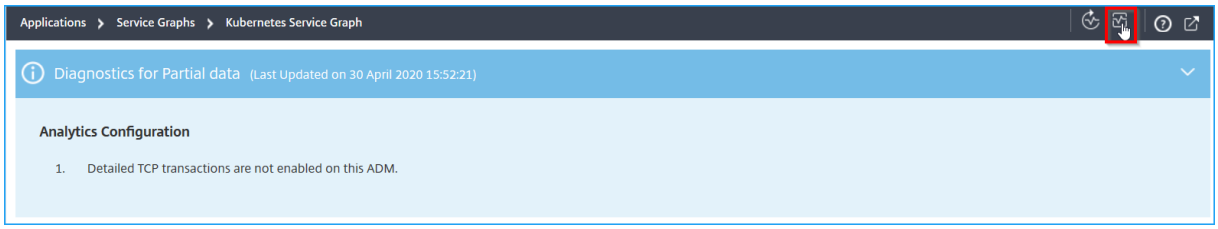


- **Type de problème** : indique si les problèmes se produisent à partir de la configuration, de la configuration d'analyse ou de la licence.
- **Message** —Indique ce qui a causé le problème.
- **Action** : indique quelle action doit être effectuée pour résoudre le problème.

Diagnostics des données partielles

Si le graphique de service est affiché uniquement avec des données partielles, cliquez sur le bouton **Afficher les diagnostics** pour afficher les informations de diagnostic.

L'exemple suivant indique que les transactions TCP sont désactivées.

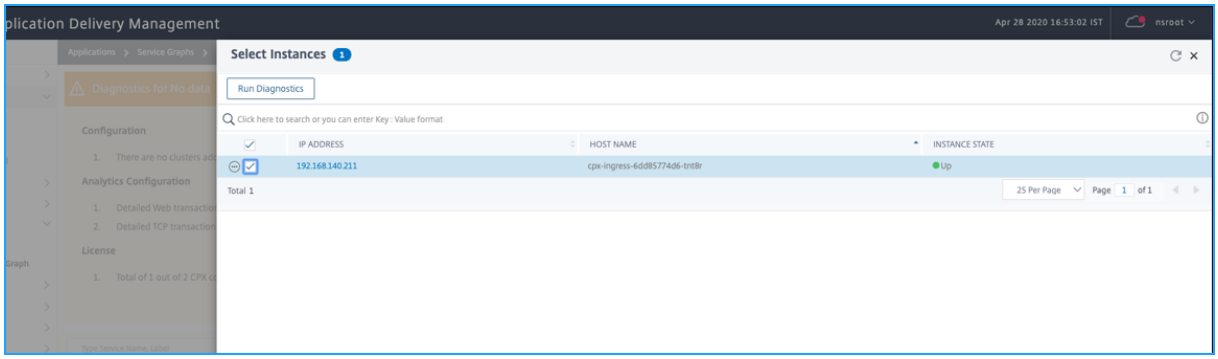


Pour cet exemple, vous devez activer les **paramètres de transaction TCP** sur **Tous** en accédant à **Analytics** > **Paramètres**.

Dépannage

En tant qu'administrateur, à l'aide de ces messages de diagnostic, vous pouvez valider ces problèmes et essayer de les résoudre. Après le dépannage, Citrix ADM exécute automatiquement une vérification de diagnostic périodique à un intervalle régulier. Une fois la vérification des diagnostics terminée, le problème de données partielles ou aucune donnée dans le graphique de service sera résolu.

Vous pouvez également cliquer sur **Exécuter les tests de diagnostic**, sélectionner les **instances CPX**, puis cliquer sur **Exécuter les tests de diagnostic**.



Pour plus de scénarios de dépannage, consultez la FAQ.

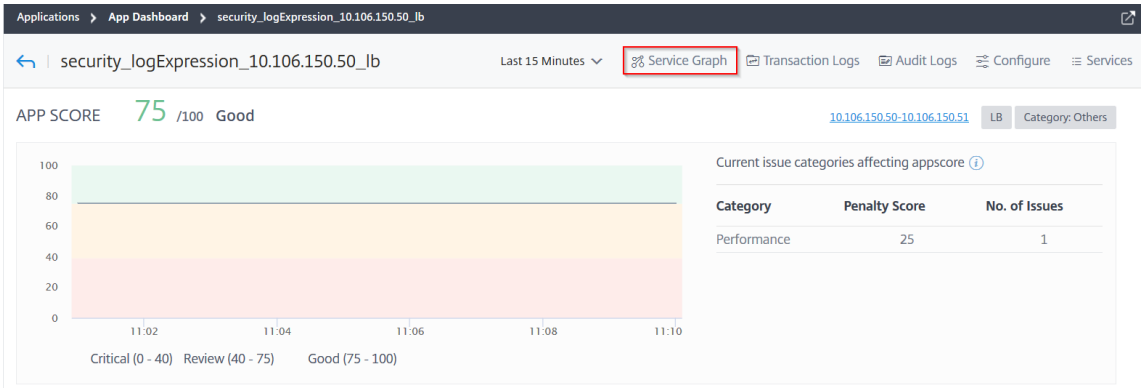
Graphique de service pour les applications

February 1, 2024

Pour afficher le graphique de service d'une application :

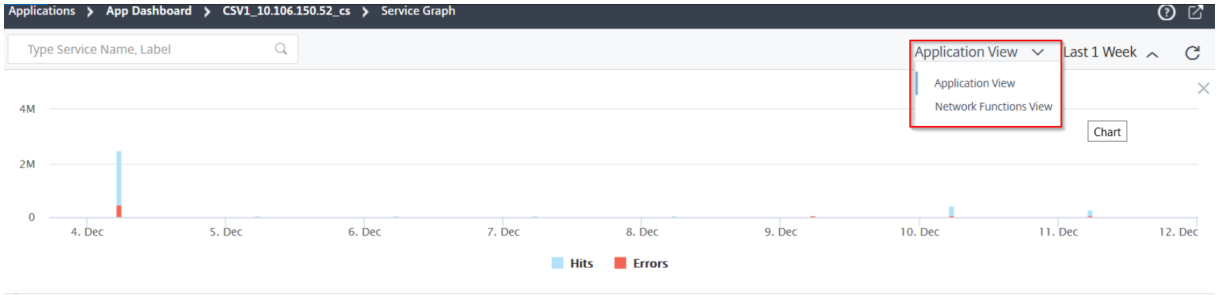
1. Accédez à **Applications** > **Tableau de bord**.
2. Sélectionnez une application.

   La page de détails de l'application s'affiche.
3. Sélectionnez la durée et cliquez sur **Service Graph**.

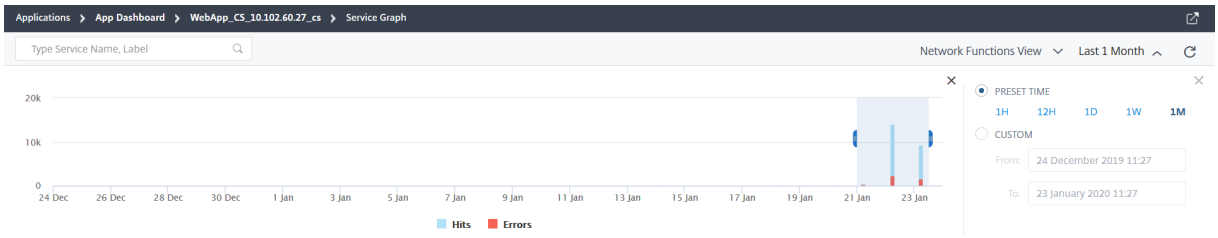


   La page graphique des services s'affiche pour l'application sélectionnée.

Vous pouvez afficher le graphique des services dans la **vue des applications** ou dans la **vue des fonctions réseau**.

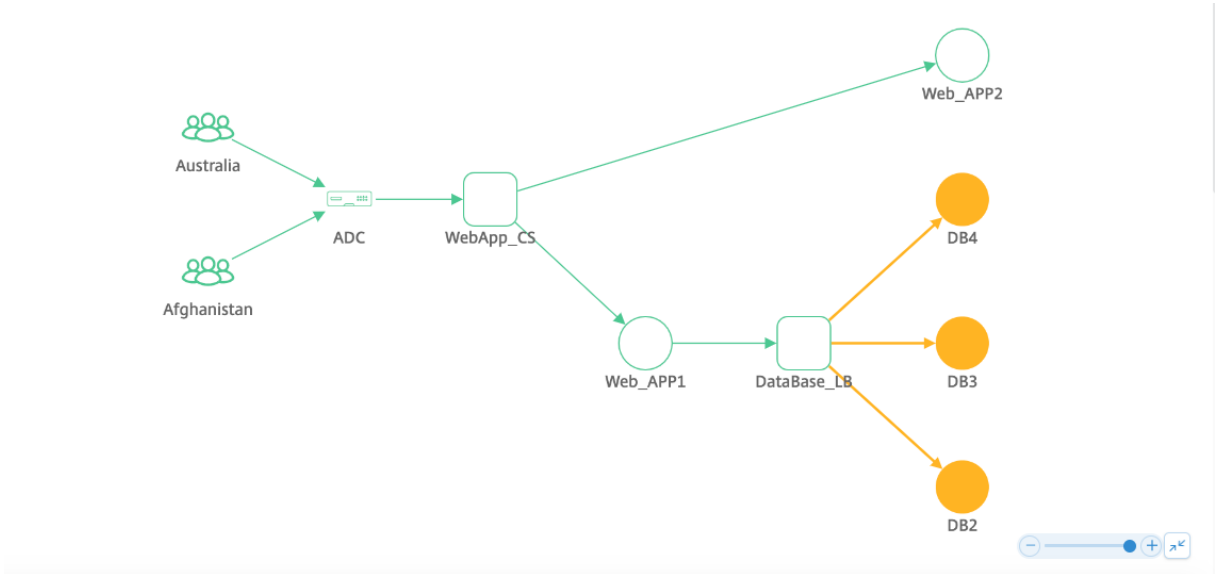


Vous pouvez également faire glisser et sélectionner les résultats et les erreurs pour modifier les résultats.



Vue de l'application

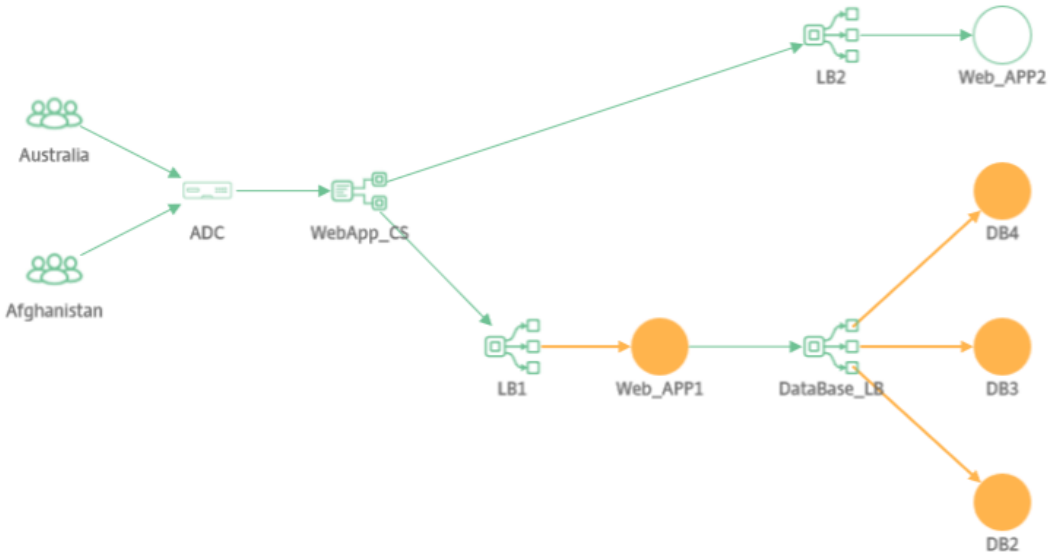
Affiche la vue d'ensemble de la configuration de l'application. Dans cette vue, vous pouvez visualiser la communication entre le client, l'ADC et les applications Web.



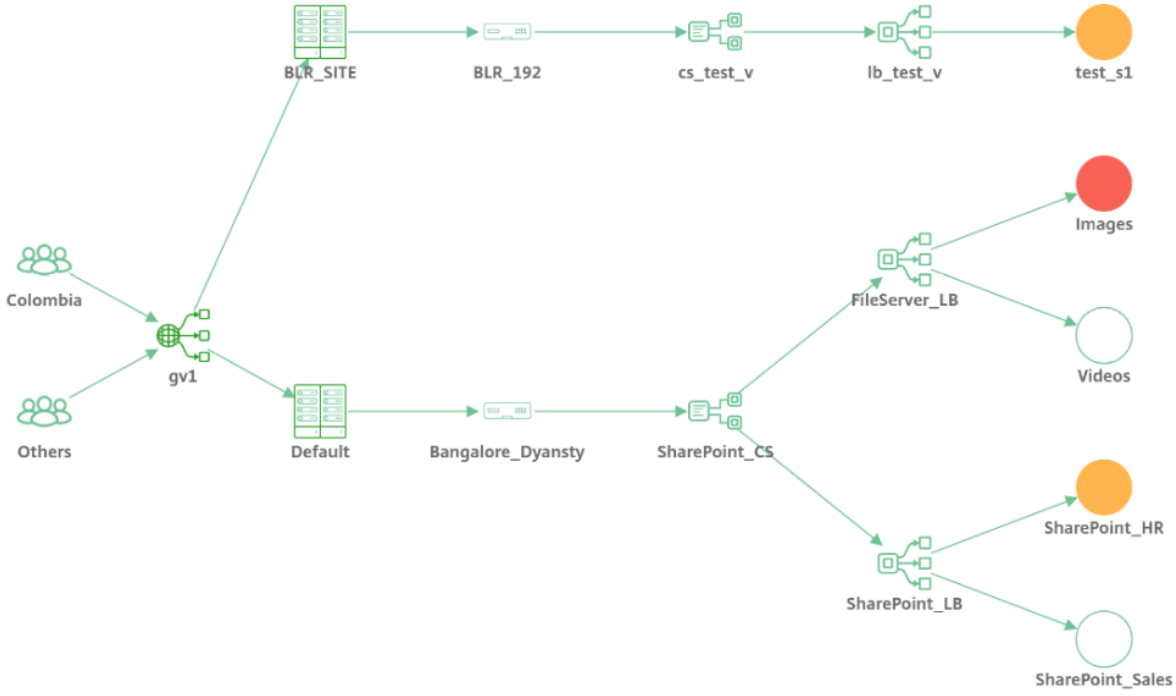
Vue des fonctions du réseau

Affiche les serveurs virtuels associés à l'application. Dans cette vue, vous pouvez voir si l'ADC communique avec :

- Serveur virtuel de commutation de contenu pour accéder à l'application
- Serveur virtuel d'équilibrage de charge pour accéder à l'application
- Serveurs virtuels de commutation de contenu et d'équilibrage de charge pour accéder à l'application



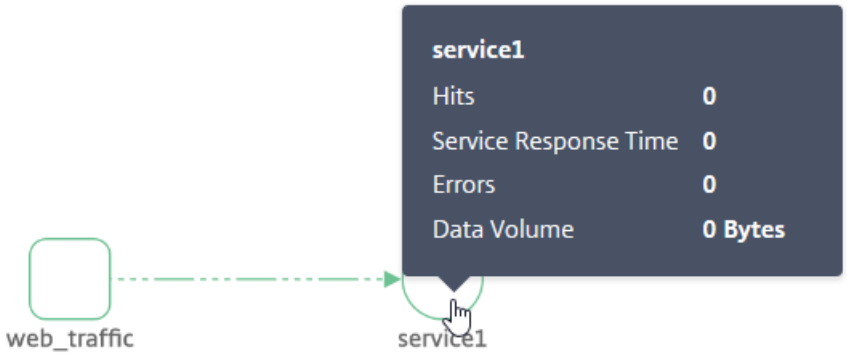
Pour l'application GSLB, les détails sont affichés avec le centre de données et Citrix ADC.



Affichage graphique de service pour aucune transaction active

Si aucune transaction active n'a lieu entre ADC et l'application Web, Service Graph affiche uniquement la configuration de base de l'application (sans client ni ADC).

Lorsque vous placez le pointeur de la souris sur un service ou un serveur virtuel, les détails s'affichent sous la forme 0 pour toutes les mesures, car aucune transaction n'est effectuée.

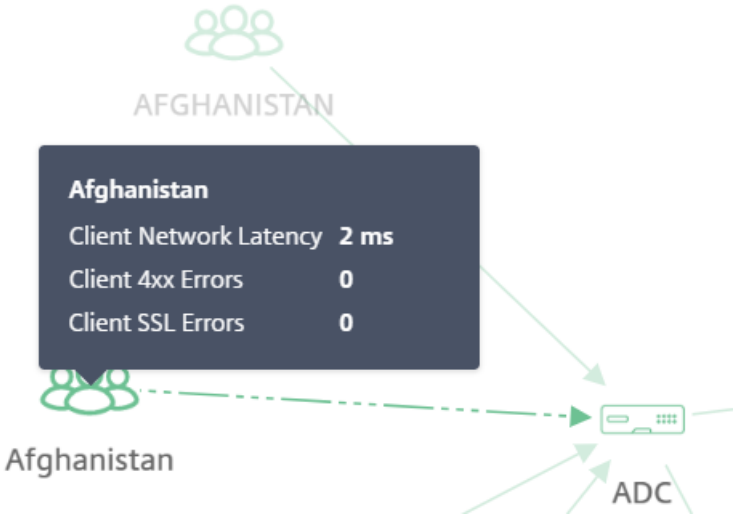


Analyser les indicateurs

Placez le pointeur de la souris sur chaque service pour afficher les détails des mesures en mode Application ou en mode Fonction réseau.

Mesures client

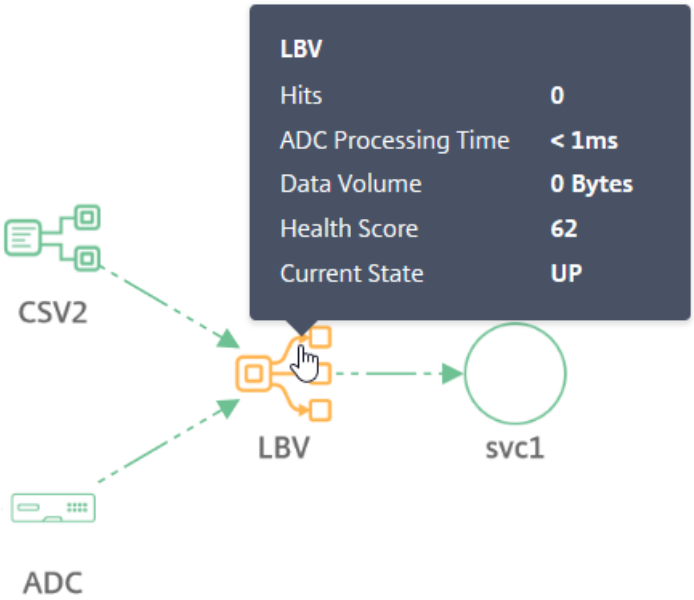
Passez le pointeur de la souris sur le client pour afficher les statistiques du client.



- **Latence du réseau client** —Indique la latence du réseau depuis le client.
- **Erreurs du client 4xx** : indique le nombre total d'erreurs 4xx survenues chez le client.
- **Erreurs SSL du client** : indique le nombre total d'erreurs SSL provenant du client.

Mesures de fonction réseau

Passez le pointeur de la souris sur un service d'équilibrage de charge ou de commutation de contenu pour afficher les détails des métriques.

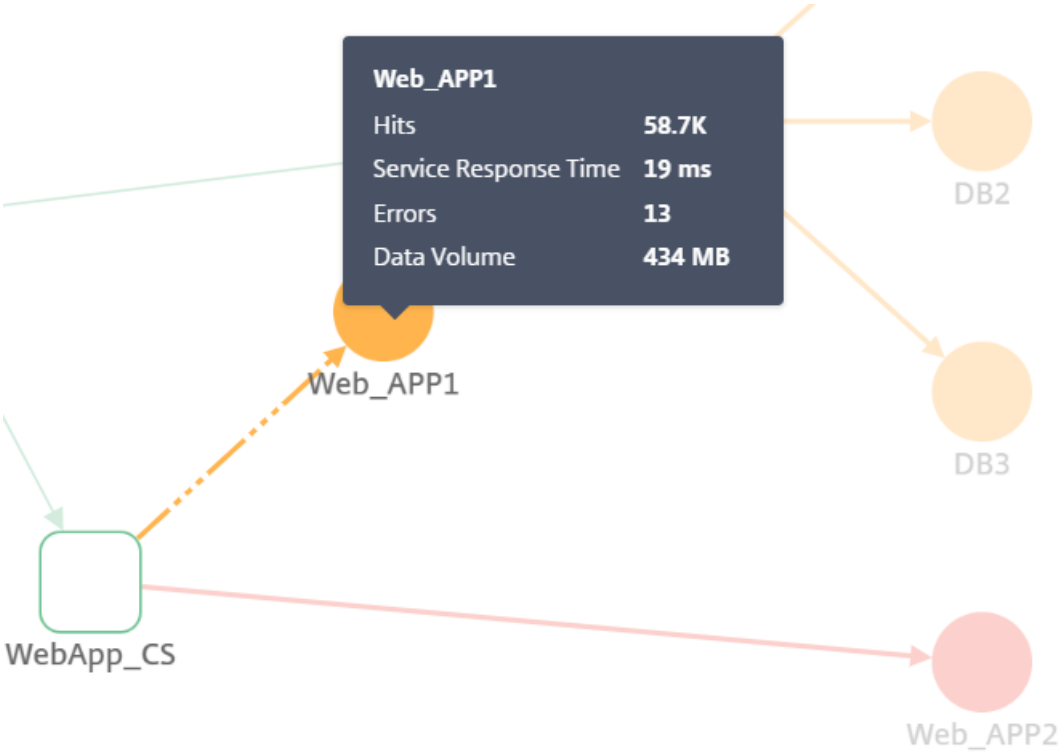


- **Hits** —Indique le nombre total d'accès reçus par le serveur virtuel
- **Temps de traitement ADC** —Indique le temps de traitement moyen par l'instance ADC

- **Volume de données** : indique le volume total de données traité par le serveur virtuel
- **Score de santé** —Indique le score de l'application
- **État actuel** —Indique l'état actuel du serveur virtuel

Mesures de service

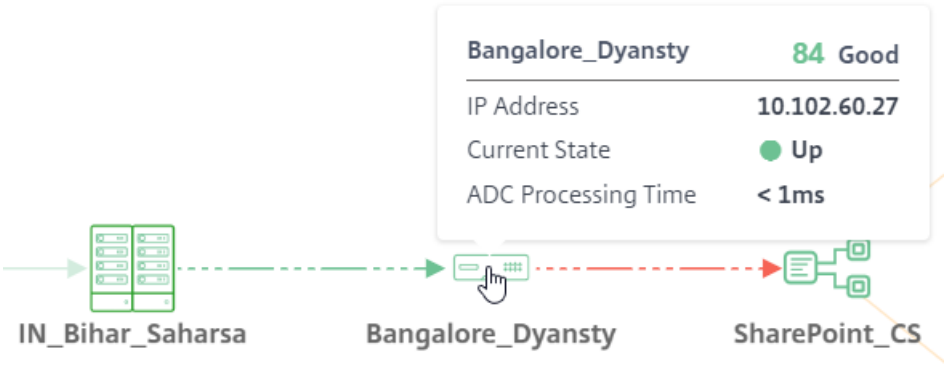
Passez le pointeur de la souris sur un service (application Web) pour afficher les mesures



- **Affichages** —Indique le nombre total de visites reçues par le service
- **Temps de réponse du service** —Indique le temps de réponse moyen du service
- **Erreurs** —Indique le nombre total d'erreurs survenues à partir du service
- **Volume de données** —Indique le total des données traitées par le service

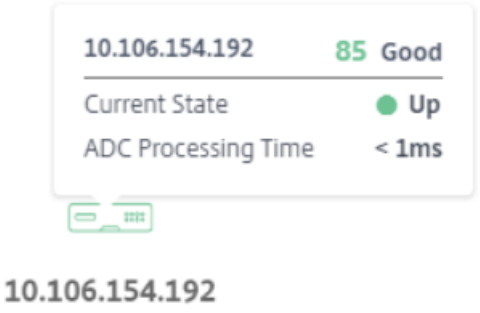
Metrics Citrix ADC (uniquement pour les applications GSLB)

Passez le pointeur de la souris sur l'ADC pour afficher les métriques.



- Affiche le nom de l'hôte et le score ADC actuel. Le score est calculé en fonction des différents problèmes potentiels de Citrix ADC. Pour plus d'informations, consultez Score d'instance.
- **Adresse IP** —Indique l'adresse IP Citrix ADC
- **État actuel** : indique l'état de Citrix ADC, tel que Up, Down ou Out of service
- **Temps de traitement ADC** : indique le temps de traitement moyen par l'instance ADC

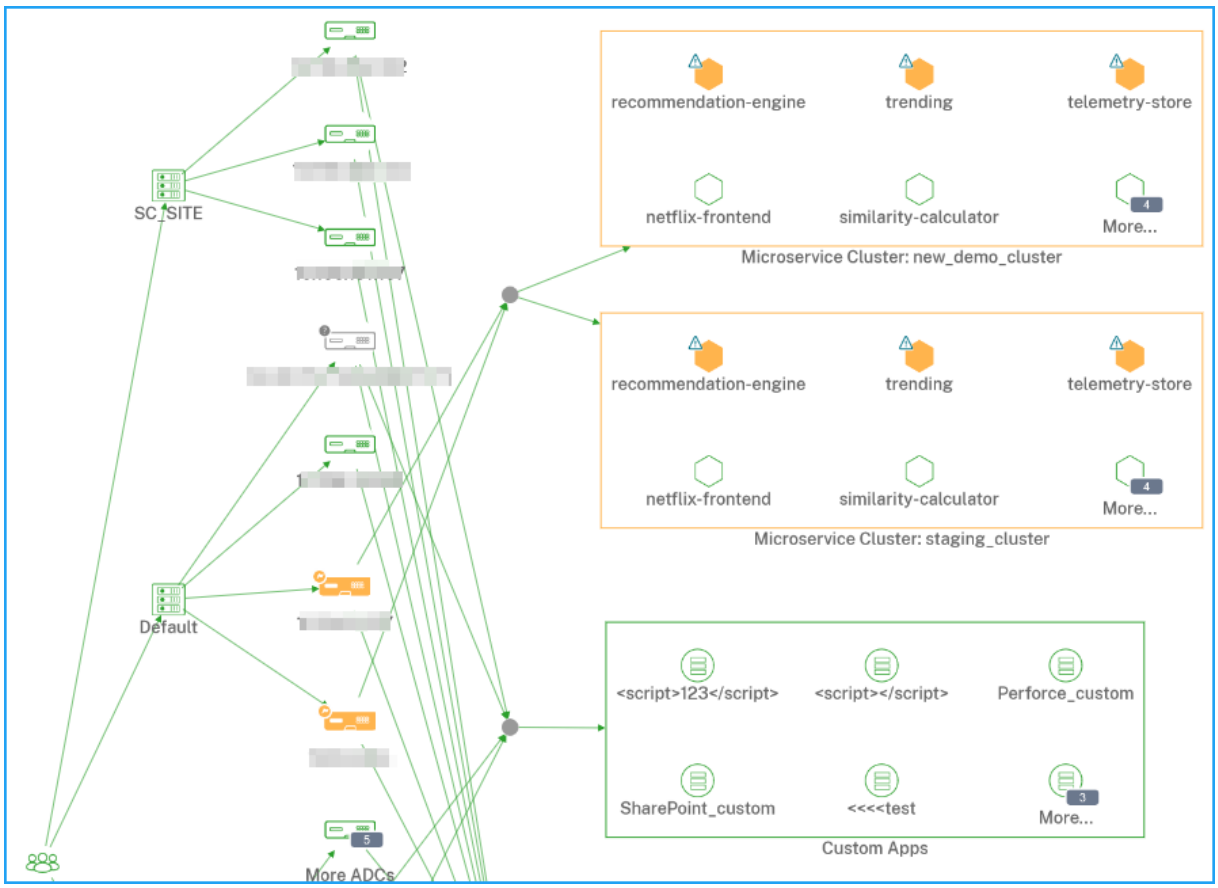
> **Remarque**
>
> Si aucun nom d'hôte n'est attribué à Citrix ADC :
>
> -L'adresse IP Citrix ADC s'affiche à la place du nom d'hôte.
>
> -Dans les mesures, les informations d'adresse IP Citrix ADC ne sont pas affichées.



Vue holistique de toutes les applications dans le graphique de service

February 1, 2024

Accédez à **Applications** > **Graphique de service**, puis cliquez sur **Global**.



Le graphique de service affiche les éléments suivants pour la durée sélectionnée :

- Région à partir de laquelle les utilisateurs accèdent à l'application spécifique

Centres de données où les instances Citrix ADC sont hébergées

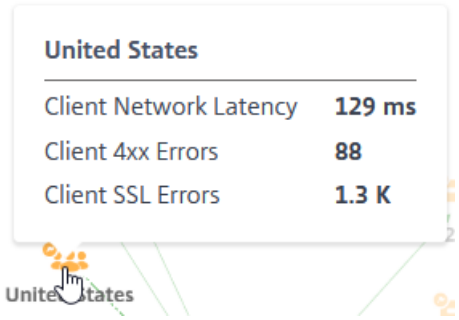
- Nombre total d'applications discrètes de toutes les instances Citrix ADC

> **Remarque**
>
> Si une instance Citrix ADC ne possède pas d'applications discrètes, la flèche vers le serveur virtuel discret à partir de l'instance Citrix ADC n'est pas visible

- Nombre total d'applications personnalisées de toutes les instances Citrix ADC
- Nombre total d'applications de microservice à partir de l'instance Citrix ADC CPX

Afficher les mesures client

Placez le pointeur de la souris sur une région cliente pour afficher les mesures.

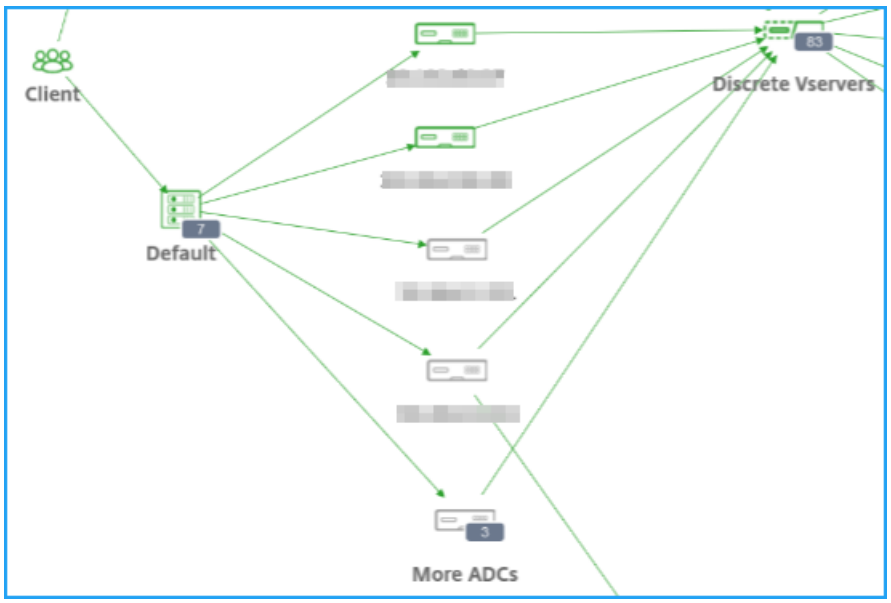


- **Latence réseau client** - Indique la latence moyenne du réseau client.
- **Erreurs client 4xx** - Indique le total des erreurs 4xx client.
- **Erreurs SSL client** - Indique le nombre total d'erreurs SSL client.

Afficher les détails de Citrix ADC

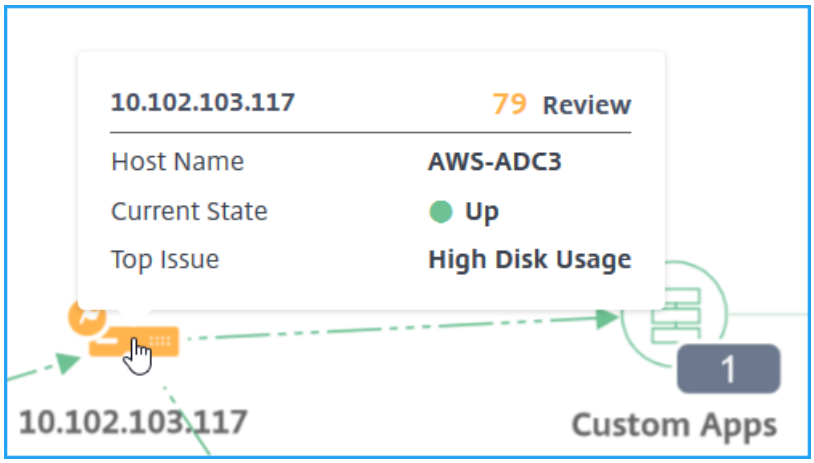
Le graphique de service vous permet d'afficher :

- Le centre de données regroupé avec son nombre total d'instances Citrix ADC
- Seules les 4 premières instances Citrix ADC à faible score de chaque centre de données



Cliquez sur **Autres ADC** pour afficher toutes les instances Citrix ADC en sélectionnant les onglets d'état respectifs (Critique, Révision, Bon et Non applicable).

Placez le pointeur de la souris sur une instance Citrix ADC pour afficher les mesures.



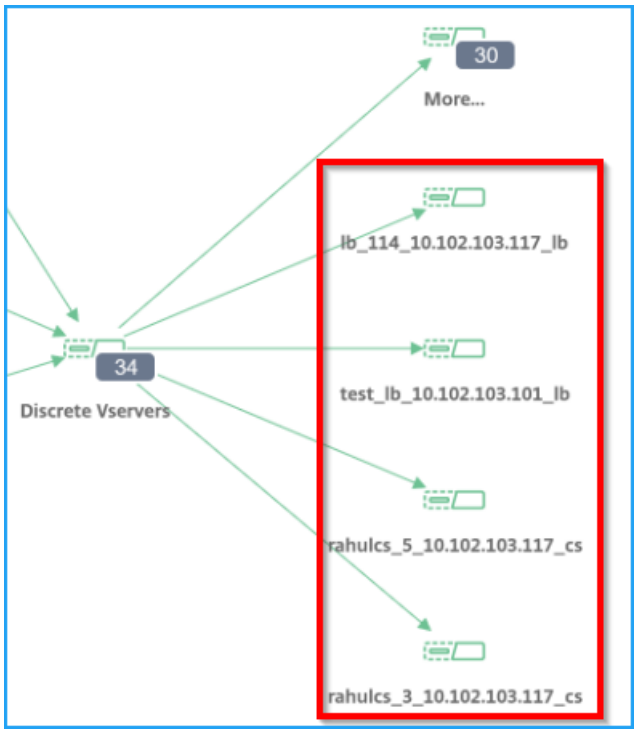
Vous pouvez consulter les éléments suivants :

- Adresse IP et score de l'instance Citrix ADC
- **Nom d'hôte** —Indique le nom d'hôte affecté à l'instance Citrix ADC
- **État actuel** —Indique l'état actuel de l'instance Citrix ADC, par exemple, en haut, en panne, en panne.
- **Problème le plus** élevé —Indique le problème le plus élevé qui affecte le score Citrix ADC actuel

Cliquez sur l'**instance Citrix ADC** pour afficher les détails de l'instance, tels que le score de l'instance, les mesures clés et les problèmes associés à l'instance ADC. Pour plus d'informations, consultez Afficher les détails de l'instance dans Infrastructure Analytics.

Afficher les applications discrètes

Le graphique de service affiche les 4 applications discrètes notées les plus faibles.



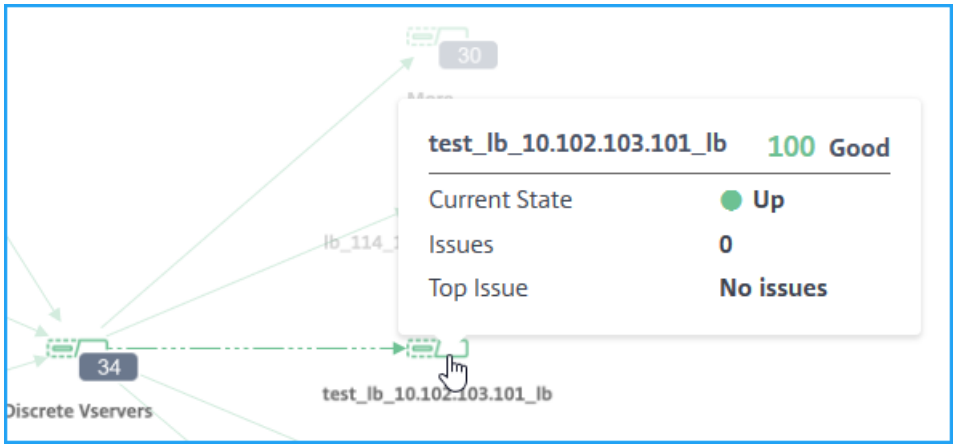
Considérez que vous avez les applications discrètes suivantes :

Nom de l'application	Citrix ADC	Score de l'application	État de l'application
App1	10.102.29.50	35 (Critique)	Actif
App2	10.102.29.90	100 (Bon)	Inactif
Appli 3	10.102.32.40	49 (Revue)	Actif
App 4	10.102.113.208	92 (Bon)	Inactif
App 5	10.102.25.25	86 (Bon)	Actif
App 6	10.102.29.41	77 (Bon)	Actif
App 7	10.102.29.102	41 (Revue)	Actif

Dans ce scénario, vous pouvez afficher App1, App3, App6 et App 7 comme les 4 applications les plus faibles dans le graphique de service.

De même, vous pouvez également afficher les 4 applications les plus faibles pour les applications **personnalisées** et **Microservices**.

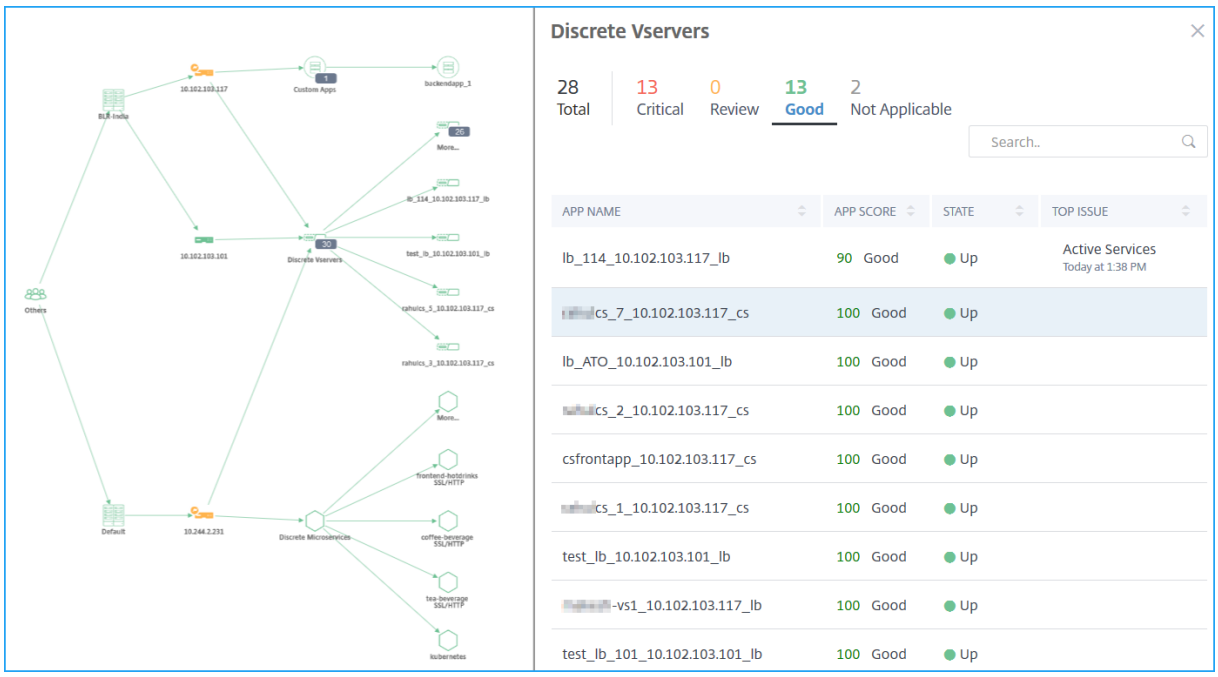
Placez le pointeur de la souris sur un service pour afficher les informations sur les mesures.



Vous pouvez consulter les éléments suivants :

- Le nom et le score de l'application
- **État actuel** —Indique l'état actuel de l'application, par exemple, haut ou bas
- **Questions** —Indique le nombre total de questions applicables à la demande
- **Problème le plus** élevé —Indique le problème le plus élevé qui a une incidence sur le score global des demandes

Cliquez sur **Plus** pour afficher toutes les applications discrètes. La page Serveur virtuel discret s'affiche comme illustré dans l'image suivante :

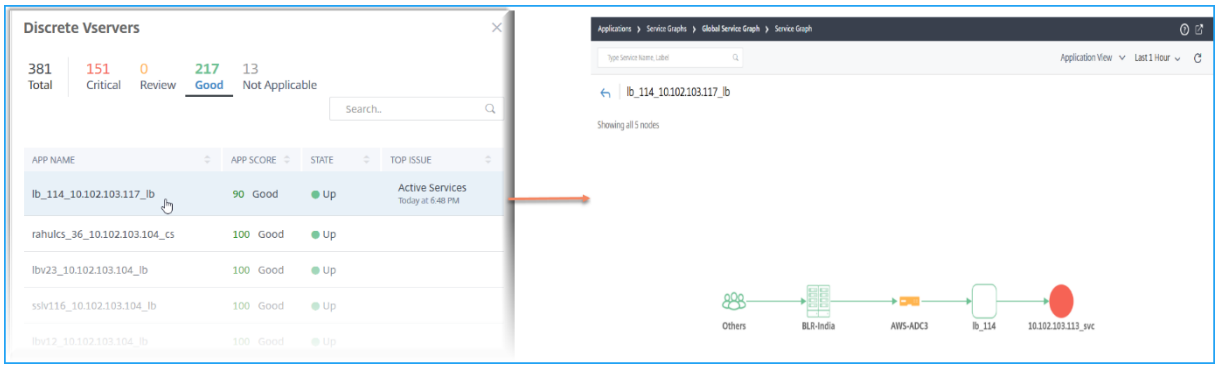


Les serveurs virtuels sont affichés en fonction de l'état.

- **Total** —Total des applications discrètes

- **Critique** —Le score de l'application est compris entre 0 et < 40
- **Évaluations** —Le score de l'application est compris entre 40 et < 75
- **Bon** —Le score de l'application est > 75
- **Non applicable** —L'application n'est liée à aucun serveur virtuel

Vous pouvez cliquer sur chaque onglet pour afficher les serveurs virtuels. Lorsque vous cliquez sur une application, le graphique de service de l'application sélectionnée s'affiche.



Pour plus d'informations, consultez Graphique de service pour les applications.

Afficher les applications de microservices

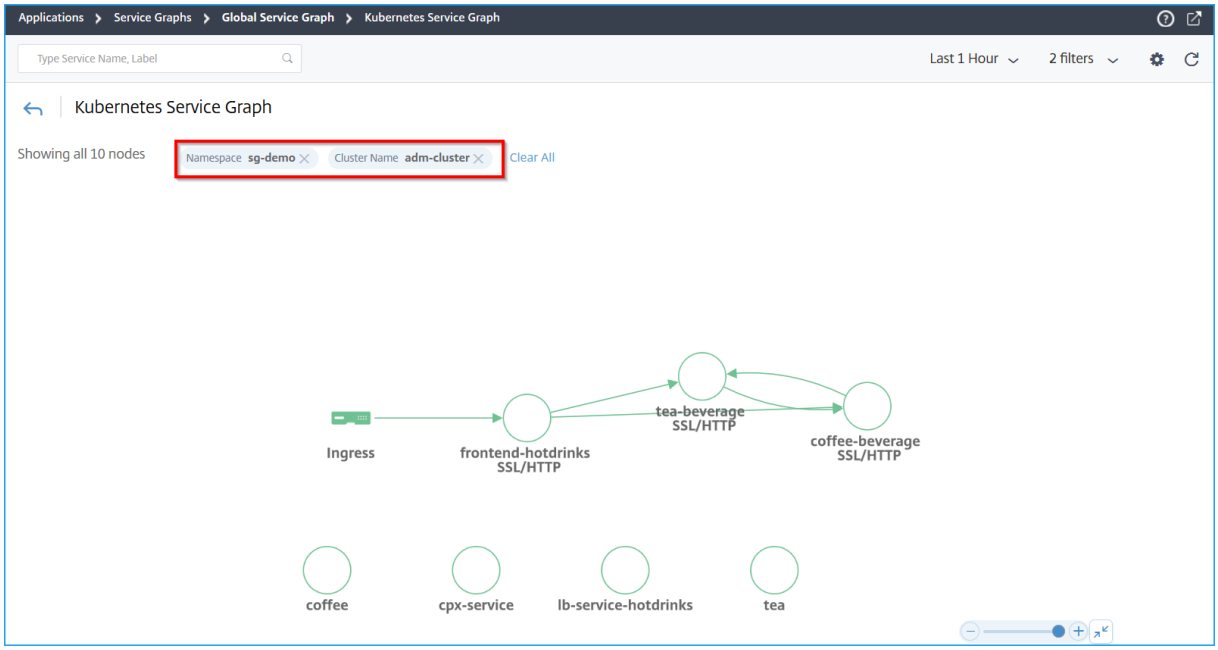
Le graphique de service affiche également toutes les applications de microservice appartenant aux clusters Kubernetes. Placez le pointeur de la souris sur un service pour afficher les détails des mesures.

Vous pouvez consulter les éléments suivants :

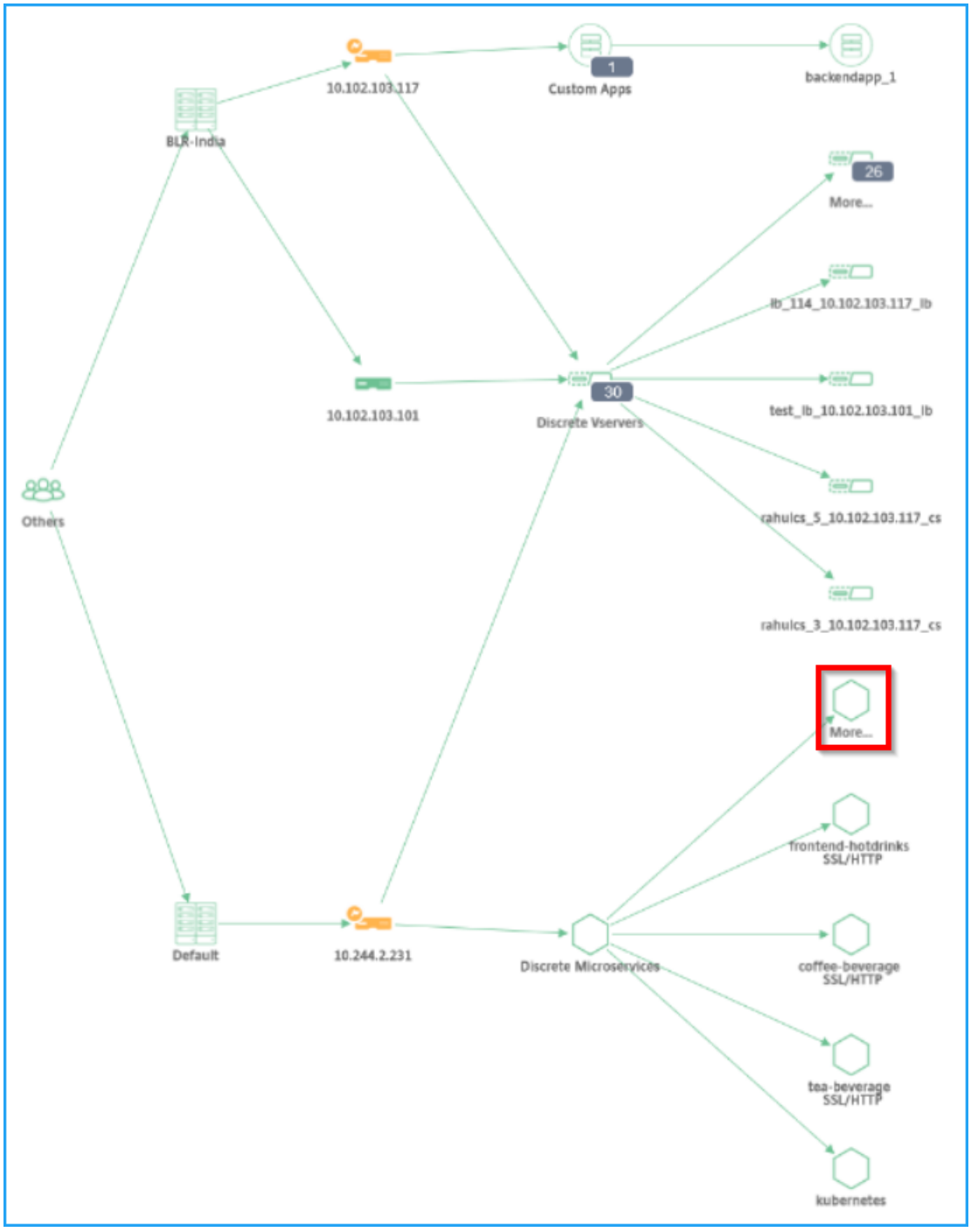
- Le nom du service
- Le protocole utilisé par le service tel que SSL, HTTP, TCP, SSL sur HTTP
- **Hits** —Nombre total d'accès reçus par le service
- **Temps de réponse du service** —Temps de réponse moyen pris par le service.

  (Temps de réponse = RTT client + demande le dernier octet —demande le premier octet)
- **Erreurs** —Les erreurs totales telles que 4xx, 5xx, et ainsi de suite
- **Volume de données** —Volume total de données traitées par le service
- **Espace de noms** —Espace de noms du service
- **Nom du cluster** —Nom du cluster où le service est hébergé
- **Erreurs SSL Server** : nombre total d'erreurs SSL provenant du service

Lorsque vous cliquez sur un service, le graphique de service Kubernetes pour le service sélectionné s'affiche, ainsi que l'espace de noms de service et les filtres de noms de cluster appliqués.



Cliquez sur **Plus** pour afficher le graphique des services Kubernetes qui contient tous les services. Pour plus d'informations sur le graphique de service Kubernetes, consultez Graphique de service pour les applications natives du cloud.

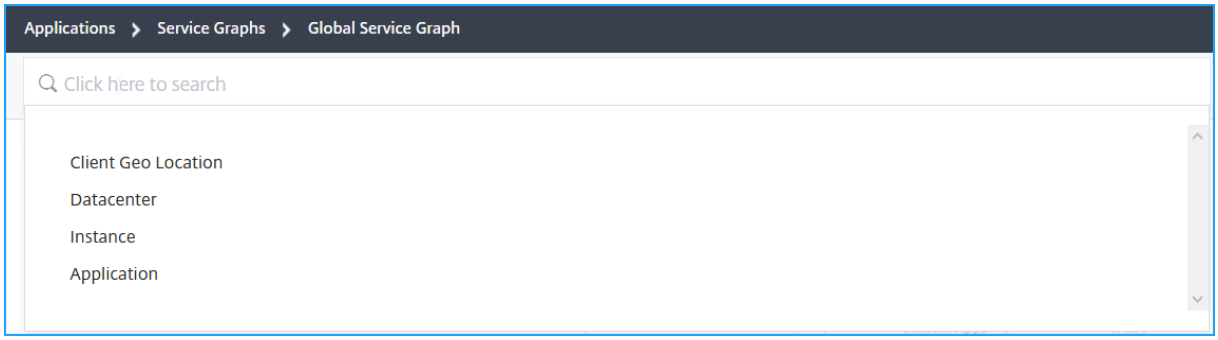


barre de recherche pour filtrer les résultats

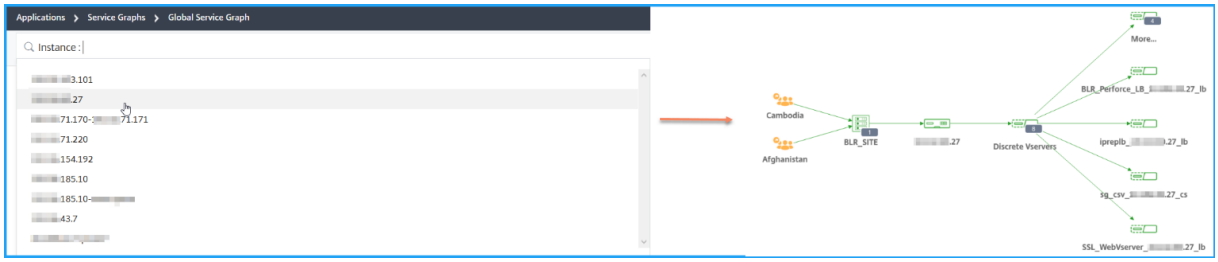
Vous pouvez utiliser la barre de recherche pour filtrer les résultats. En tant qu'administrateur, cette barre de recherche vous permet de réduire rapidement une instance/client/application/centre de données particulier, lorsque vous avez :

- Une grande entreprise avec de nombreux centres de données
- Configuration de nombreuses instances Citrix ADC pour chaque centre de données
- Configuration de nombreuses applications déployées ou accessibles via chaque instance Citrix ADC
- Clients accédant à l'application depuis différents emplacements

Placez le pointeur de la souris sur la barre de recherche et sélectionnez la catégorie que vous souhaitez créer le filtre.



Par exemple, si vous souhaitez afficher une instance ADC particulière, sélectionnez Instance dans la barre de recherche et sélectionnez l'adresse IP de l'instance. Le graphique de service global affiche l'instance sélectionnée et ses applications, centres de données et emplacements clients associés.



StyleBooks

February 1, 2024

StyleBooks simplifie la gestion des configurations Citrix ADC complexes pour vos applications. Un StyleBook est un modèle que vous pouvez utiliser pour créer et gérer des configurations Citrix ADC. Vous pouvez créer un StyleBook pour configurer une fonctionnalité spécifique de Citrix ADC, ou vous pouvez concevoir un StyleBook pour créer des configurations pour le déploiement d'une application d'entreprise telle que Microsoft Exchange ou Lync.

Les StyleBooks s'intègrent parfaitement aux principes de l'infrastructure en tant que code appliqués par les équipes DevOps, où les configurations sont déclaratives et contrôlées par version. Les configurations sont également répétées et déployées dans leur ensemble. Les StyleBooks offrent les avantages suivants :

- **Déclaratif** : StyleBooks sont écrits dans une syntaxe déclarative plutôt que impérative. Les stylebooks vous permettent de vous concentrer sur la description du résultat ou de l'« état souhaité » de la configuration plutôt que sur les instructions étape par étape sur la façon de l'atteindre sur une instance Citrix ADC particulière. Citrix Application Delivery Management (ADM) calcule la différence entre l'état existant sur un Citrix ADC et l'état souhaité que vous avez spécifié, et apporte les modifications nécessaires à l'infrastructure. Étant donné que StyleBooks utilise une syntaxe déclarative, écrite en YAML, les composants d'un StyleBook peuvent être spécifiés dans n'importe quel ordre, et Citrix ADM détermine l'ordre correct en fonction de leurs dépendances calculées.
- **Atomic** : lorsque vous utilisez StyleBooks pour déployer des configurations, la configuration complète est déployée ou aucune d'entre elles n'est déployée, ce qui garantit que l'infrastructure reste toujours dans un état cohérent.
- **Versionné** : un StyleBook possède un nom, un espace de noms et un numéro de version qui le distinguent de manière unique de tous les autres StyleBook du système. Toute modification apportée à un StyleBook nécessite la mise à jour de son numéro de version (ou de son nom ou de son espace de noms) afin de conserver ce caractère unique. La mise à jour de version vous permet également de conserver plusieurs versions du même StyleBook.
- **Composable** : une fois qu'un StyleBook est défini, le StyleBook peut être utilisé comme une unité pour créer d'autres StyleBooks. Vous pouvez éviter de répéter les modèles de configuration courants. Cela vous permet également d'établir des éléments de base standard au sein de votre organisation. Comme les StyleBooks sont versionnés, les modifications apportées aux StyleBooks existants génèrent de nouveaux StyleBooks, garantissant ainsi que les StyleBooks dépendants ne sont jamais cassés involontairement.
- **Centré sur les applications** : les StyleBooks peuvent être utilisés pour définir la configuration Citrix ADC d'une application complète. La configuration de l'application peut être abstraite à l'aide de paramètres. Par conséquent, les utilisateurs qui créent des configurations à partir d'un StyleBook peuvent interagir avec une interface simple consistant à remplir quelques paramètres pour créer ce qui peut être une configuration Citrix ADC complexe. Les configurations créées à partir de StyleBooks ne sont pas liées à l'infrastructure. Une configuration unique peut donc être déployée sur un ou plusieurs Citrix ADC et peut également être déplacée d'une instance à l'autre.
- **UI générée automatiquement** : Citrix ADM génère automatiquement des formulaires d'interface utilisateur utilisés pour remplir les paramètres du StyleBook lorsque la configuration est ef-

fectuée à l'aide de l'interface graphique Citrix ADM. Les auteurs de StyleBook n'ont pas besoin d'apprendre un nouveau langage d'interface utilisateur ni de créer des pages et des formulaires d'interface utilisateur séparément

- **Piloté par API** : toutes les opérations de configuration sont prises en charge à l'aide de l'interface graphique Citrix ADM ou via des API REST. Les API peuvent être utilisées en mode synchrone ou asynchrone. Outre les tâches de configuration, les API StyleBooks vous permettent également de découvrir le schéma (description des paramètres) de n'importe quel StyleBook lors de l'exécution.

Vous pouvez utiliser un StyleBook pour créer plusieurs configurations. Chaque configuration est enregistrée en tant que pack de configuration. Par exemple, considérez que vous disposez d'un StyleBook qui définit une configuration d'application d'équilibrage de charge HTTP typique. Vous pouvez créer une configuration avec des valeurs pour les entités d'équilibrage de charge et l'exécuter sur une instance de Citrix ADC. Cette configuration est enregistrée en tant que pack de configuration. Vous pouvez utiliser le même StyleBook pour créer une autre configuration avec des valeurs différentes et l'exécuter sur la même instance Citrix ADC ou une autre. Un nouveau pack de configuration est créé pour cette configuration. Un pack de configuration est enregistré à la fois sur Citrix ADM et sur l'instance Citrix ADC sur laquelle la configuration est exécutée.

Vous pouvez utiliser les StyleBooks par défaut, livrés avec Citrix ADM, pour créer des configurations pour votre déploiement, ou concevoir vos propres StyleBooks et les importer dans Citrix ADM. Vous pouvez utiliser les StyleBooks pour créer des configurations à l'aide de l'interface graphique Citrix ADM ou à l'aide d'API.

Ce document contient les informations suivantes :

- Comment consulter des StyleBooks
- StyleBooks par défaut
- Stylebooks développés pour les applications professionnelles
- StyleBooks personnalisés
- API dans StyleBooks
- Grammaire de StyleBooks

Catégories de StyleBook

February 1, 2024

Il existe deux catégories de StyleBook dans Citrix Application Delivery Management (ADM). Il s'agit des StyleBooks par défaut et des StyleBooks personnalisés. Qu'il s'agisse d'un livre par défaut ou personnalisé, un StyleBook est un StyleBook public ou privé. Dans Citrix ADM, vous pouvez afficher

tous les StyleBooks présents dans le système, quel que soit leur type ou leur état de visibilité. Vous pouvez également afficher un affichage graphique de la manière dont StyleBooks sont connectés les uns aux autres.

Ce document explique les différents types de StyleBooks. En outre, il explique les actions suivantes que vous pouvez effectuer sur les StyleBooks à partir de Citrix ADM :

- Téléchargez un StyleBook personnalisé et apportez des modifications, ou créez un StyleBook basé sur un livre existant.
- Masquer les StyleBooks par défaut d'ADM.
- Supprimez un StyleBook personnalisé de Citrix ADM.
- Ajoutez des balises aux StyleBooks.

StyleBooks personnalisés et par défaut

- Les **StyleBooks par défaut** sont les StyleBooks fournis avec Citrix ADM et ils vous permettent de créer des configurations que vous pouvez déployer sur vos instances Citrix ADC. Vous ne pouvez pas supprimer les livres StyleBooks par défaut, mais vous pouvez les masquer dans l'interface graphique ADM.
- Les**livres StyleBooks personnalisés** sont vos propres StyleBooks que vous avez importés dans Citrix ADM.

Les StyleBooks par défaut et personnalisés peuvent être publics ou privés.

StyleBooks publics et privés

Les StyleBooks à partir desquels vous pouvez créer des packs de configuration peuvent être classés comme StyleBooks **publics**. C'est-à-dire qu'ils sont tous disponibles pour votre utilisation directe afin de créer des configurations à partir de l'interface graphique et des API Citrix ADM.

Mais certains StyleBooks sont utilisés comme blocs de construction pour d'autres StyleBooks. De tels StyleBooks sont marqués comme **privés**. Les StyleBooks privés ne peuvent pas être directement utilisés pour créer des packs de configuration à partir de l'interface graphique Citrix ADM. Mais, vous pouvez toujours afficher et afficher ces StyleBooks sur Citrix ADM. Pour marquer l'un de vos StyleBooks personnalisés comme **privé**, définissez l'attribut private dans le StyleBook sur **true**. Vous pouvez toujours utiliser des StyleBooks privés pour créer des packs de configuration à l'aide des API Citrix ADM.

Exemple d'un StyleBook marqué comme privé

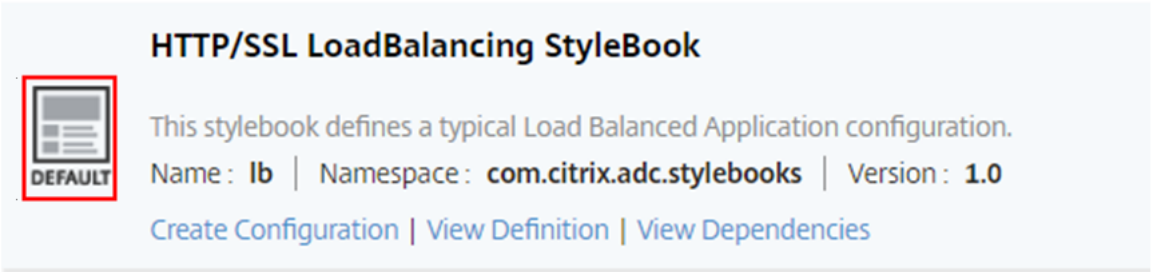

```
name: basic-lb-config
namespace: com.example.stylebooks
version: "0.1"
display-name: Load Balancing Configuration
description: |
    This StyleBook defines a simple load balancing configuration and is
        a building block to build other load balancing configurations.
schema-version: "1.0"
private: true
<!--NeedCopy-->
```

Voir StyleBooks

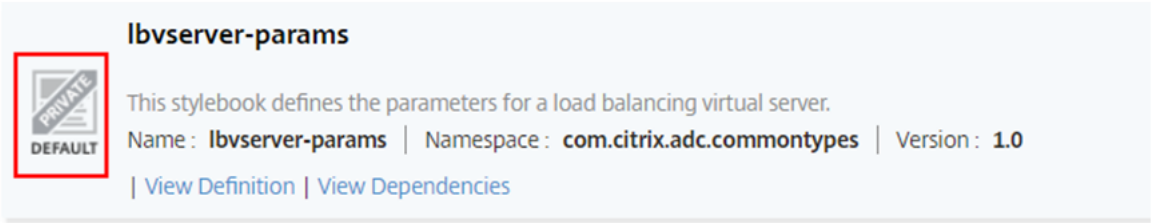
Le nombre de StyleBooks - à la fois par défaut et privé augmente dans Citrix ADM. Vous pouvez rechercher le StyleBook particulier auquel vous souhaitez accéder. Vous pouvez également afficher les deux types de StyleBooks séparément.

Dans Citrix ADM, lorsque vous accédez à **Applications** > **StyleBooks**, vous pouvez consulter la liste des StyleBooks présents dans le système.

Un StyleBook public par défaut comporte l'icône suivante dans son panneau :

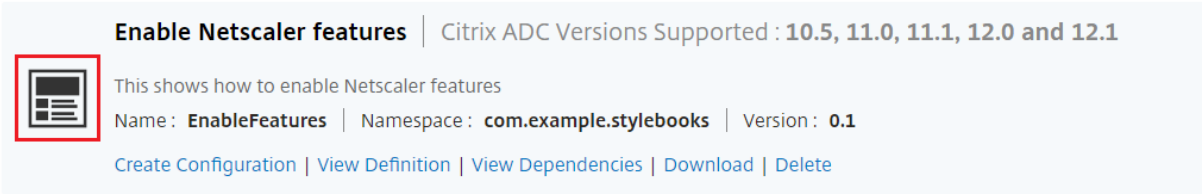


Attendu qu'un StyleBook privé par défaut possède une icône qui le déclare en tant que StyleBook privé :

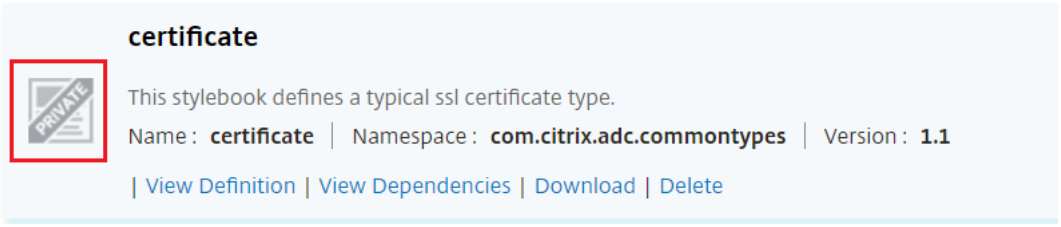


Bien que vous puissiez afficher la définition et les dépendances d'un StyleBook privé, vous ne pouvez pas créer de packs de configuration à partir d'un StyleBook privé à l'aide de l'interface graphique. Le but principal d'un StyleBook privé est de l'utiliser comme bloc de construction pour un autre StyleBook. L'utilisation de Building-blocks-Stylebooks encourage la réutilisation des modèles de configuration courants.

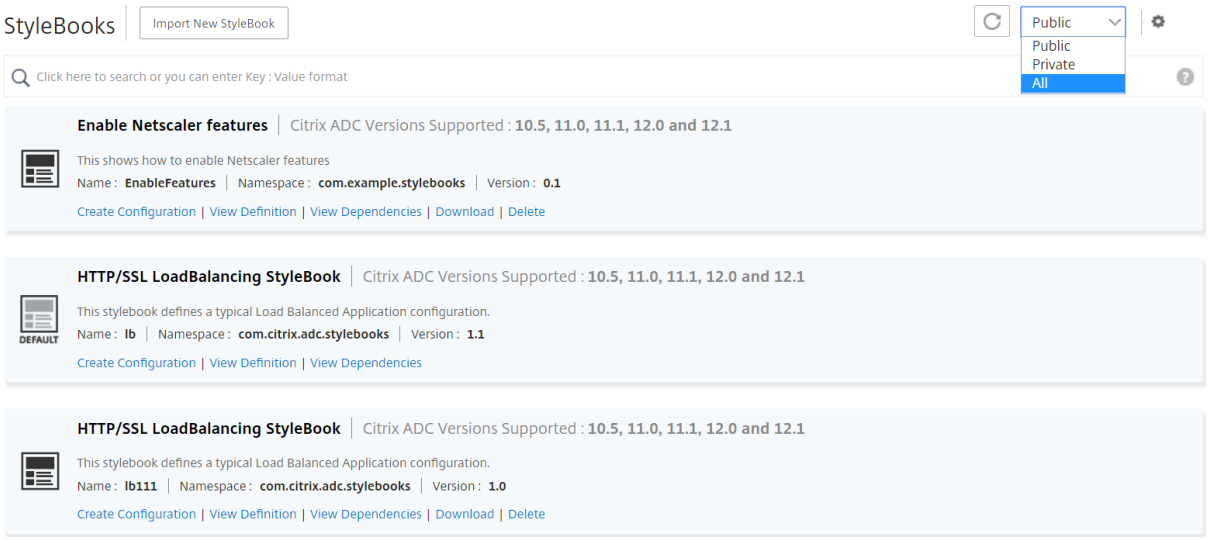
Un StyleBook public personnalisé a une icône différente, comme indiqué dans l'image suivante :



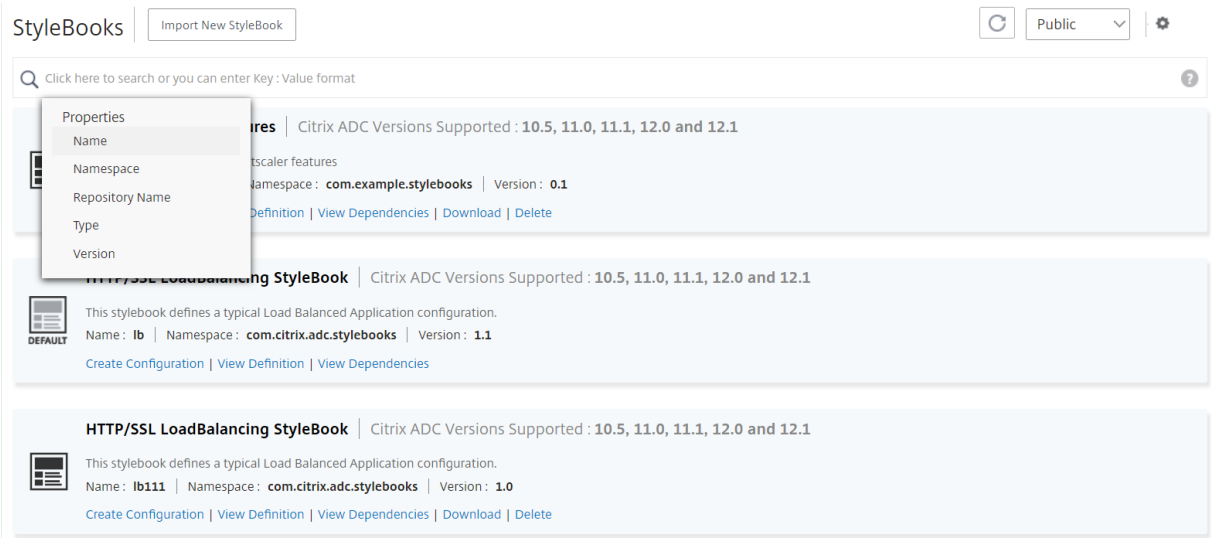
Alors qu'un StyleBook privé personnalisé apparaît avec cette icône :



En haut à droite de la page, vous pouvez voir une option permettant de sélectionner le type de StyleBooks à afficher. Il y a trois options - toutes, publiques ou privées StyleBooks. Cliquez sur l'une des options.



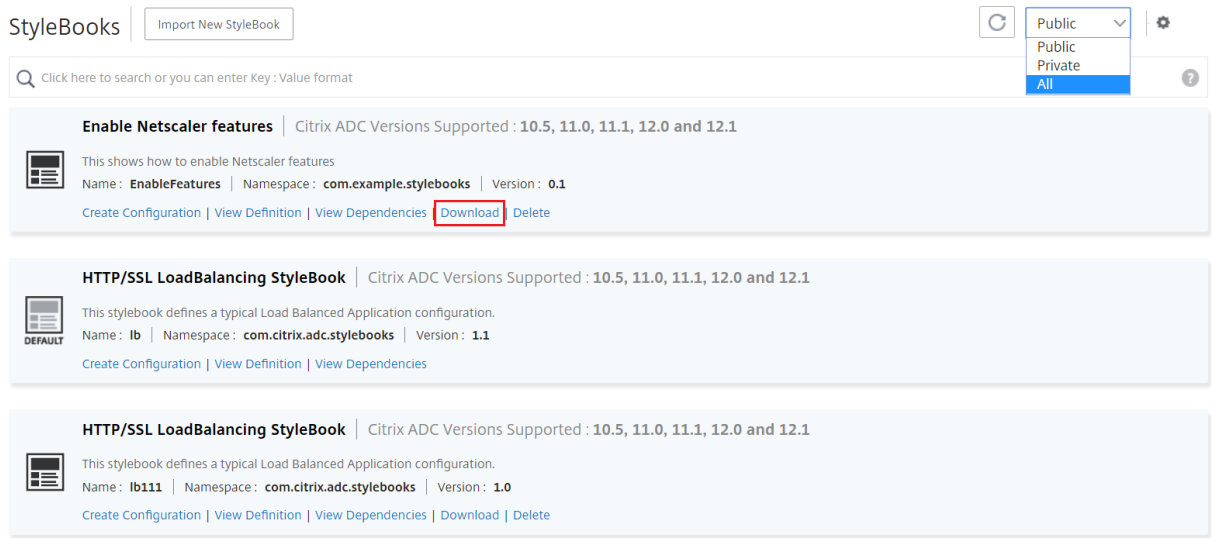
Vous pouvez également rechercher un StyleBook particulier en cliquant sur l'icône de recherche. Vous pouvez effectuer une recherche par nom, espace de noms et attributs de version ou une combinaison de ces options. L'opération de recherche n'est pas sensible à la casse.



Télécharger des StyleBooks personnalisés

Pour télécharger les StyleBooks personnalisés à partir de Citrix ADM, accédez à **Applications** > **StyleBooks** > **Configurations**. Dans la liste des StyleBooks affichés dans le panneau de droite, cochez l'option permettant de télécharger les StyleBooks personnalisés. Cliquez sur **Download (Télécharger)**. Si le StyleBook a des StyleBooks personnalisés dépendants, vous pouvez inclure les StyleBooks dépendants dans le bundle téléchargé.

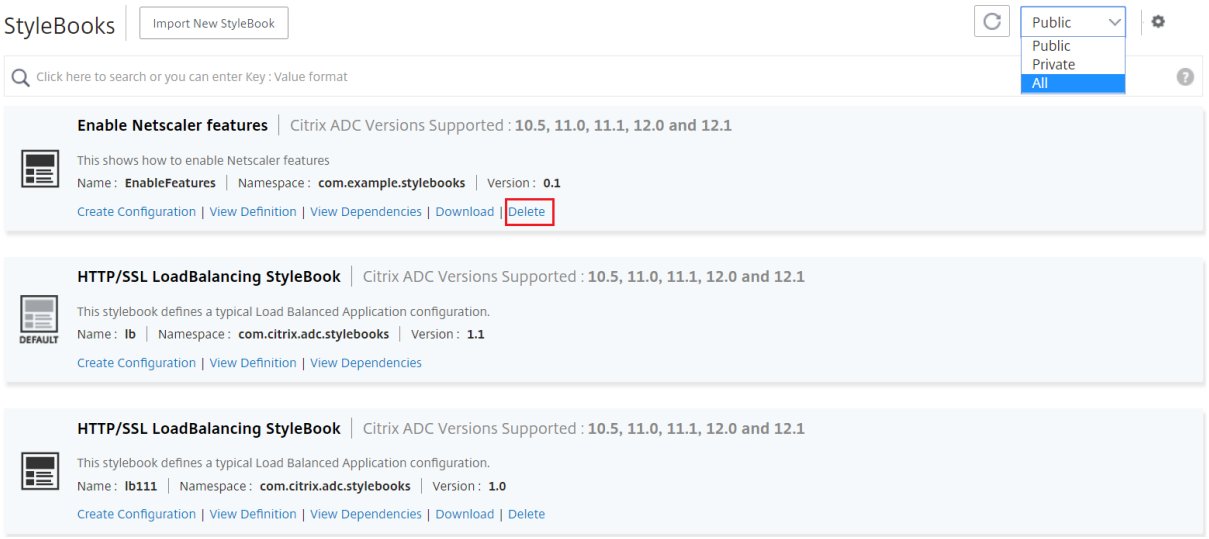
> **Remarque :**
>
> vous pouvez télécharger des StyleBooks personnalisés marqués comme publics ou privés.



> **Remarque :**
>
> Vous ne pouvez pas télécharger les StyleBooks par défaut de Citrix ADM. Vous pouvez afficher leurs définitions et dépendances. Pour ce faire, cliquez sur **les liens**Afficher la définition**et Afficher les dépendances** dans le panneau StyleBook.

Supprimer des StyleBooks personnalisés

Vous pouvez également supprimer un StyleBook personnalisé en cliquant sur le bouton **Supprimer**. Une fenêtre contextuelle vous invite à confirmer si vous souhaitez supprimer le StyleBook de Citrix ADM. Si le StyleBook utilise d'autres StyleBooks personnalisés, vous pouvez choisir de supprimer ces StyleBooks en cochant la case.



> **Remarque :**
>
> Ne supprimez pas un StyleBook personnalisé s'il a des StyleBooks dépendants dans Citrix ADM. Sinon, il casserait les StyleBooks existants.

Afficher les dépendances StyleBook

Une caractéristique importante et puissante de StyleBooks est qu'ils peuvent être utilisés comme blocs de construction pour d'autres StyleBooks. Vous pouvez importer un StyleBook dans un autre StyleBook. Un StyleBook importé est déclaré en tant que type et est utilisé par les composants ou les paramètres du second StyleBook. Vous pouvez étudier les StyleBooks par défaut existants dans Citrix ADM pour savoir comment créer un StyleBook sur un autre StyleBook.

Citrix ADM vous permet d'afficher un affichage graphique de la manière dont StyleBooks sont connectés les uns aux autres. Cette représentation est particulièrement utile pour les StyleBooks complexes

qui sont construits en utilisant d'autres StyleBooks comme blocs de construction. En regardant le graphique des dépendances, il est possible de voir les relations et les dépendances entre plusieurs StyleBooks.

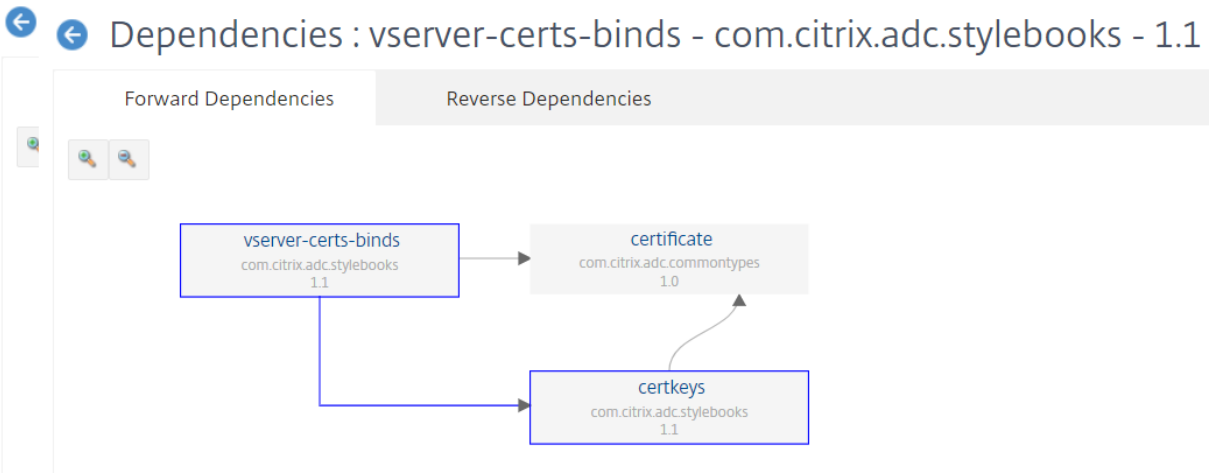
Un StyleBook utilisé par d'autres StyleBooks ne peut pas être supprimé du système car il briserait les StyleBooks existants. À l'aide de l'affichage du graphique des dépendances, vous pouvez identifier les StyleBooks qui empêchent la suppression d'un StyleBook.

Pour afficher les dépendances de StyleBook

Dans Citrix ADM, accédez à Applications**> StyleBooks.** La page StyleBooks affiche tous les StyleBooks disponibles pour votre utilisation dans Citrix ADM. Faites défiler vers le bas et trouvez votre StyleBook. La vignette **StyleBook** affiche des liens permettant de créer une configuration, d'afficher la définition de StyleBook et d'afficher les dépendances StyleBook. Cliquez sur **Afficher les dépendances**.

Dépendances de transfert

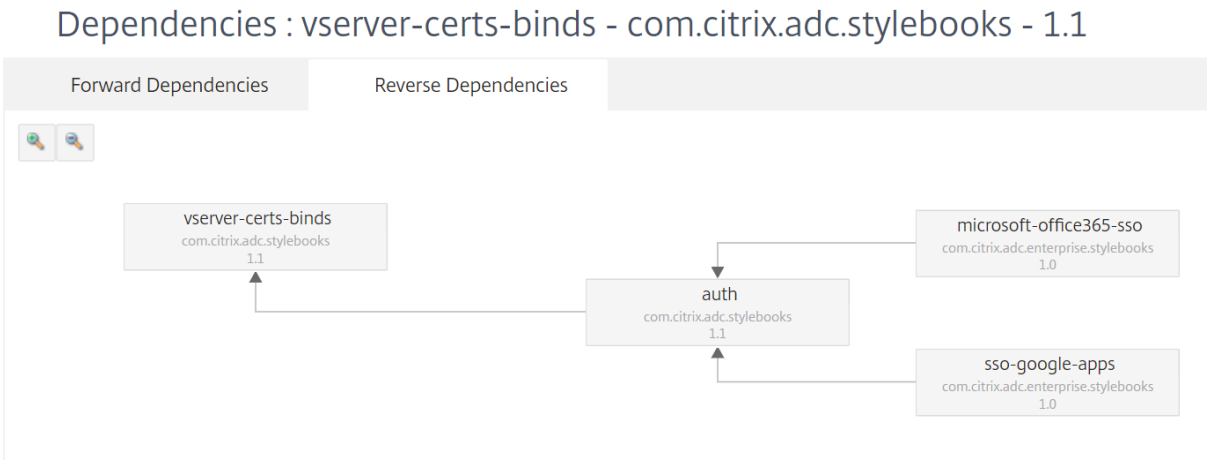
L'onglet **Forward Dependencies** vous permet de visualiser les différents StyleBooks par défaut que votre StyleBook utilise. Suivez les flèches pour trouver le StyleBook utilisé par un StyleBook. Lorsque vous pointez votre souris sur l'une des flèches, la flèche et les StyleBooks connectés les uns aux autres sont surlignés. Vous pouvez également cliquer sur les noms du StyleBook pour afficher la définition de ce StyleBook.



Inverser les dépendances

L'onglet **Dépendances inversées** vous permet d'afficher graphiquement les StyleBooks qui utilisent votre StyleBook. Si vous suivez les flèches, vous pouvez voir que tous les StyleBooks dans l'affichage

pointent vers votre StyleBook. Certains StyleBooks utilisent directement le StyleBook et certains StyleBook peuvent l'utiliser via un autre StyleBook.



Auditer la configuration ADC par rapport au pack de configuration

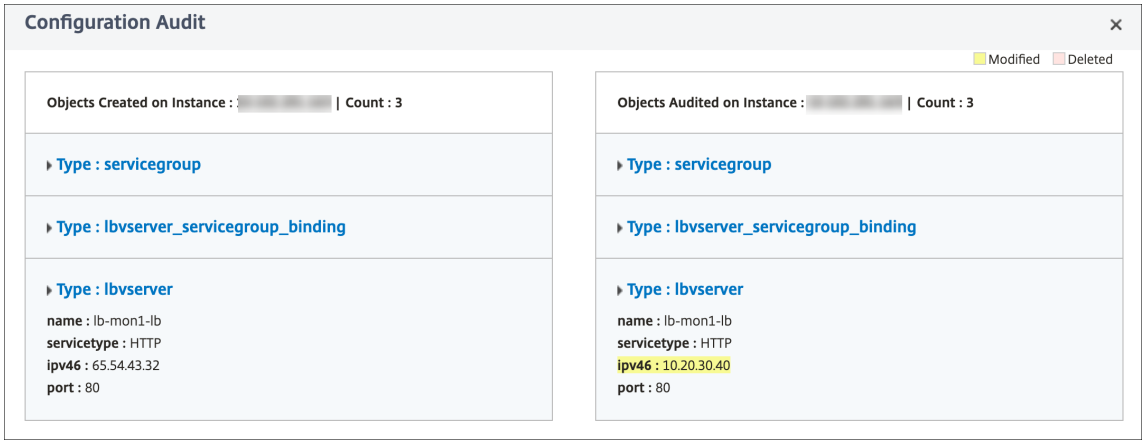
Vous pouvez comparer les modifications apportées par un pack de configuration StyleBook à la configuration ADC actuelle. Avec cette comparaison, vous pouvez effectuer les opérations suivantes :

- Détectez la dérive de configuration entre le pack de configuration StyleBook et la configuration ADC.
- Identifiez tous les objets modifiés et supprimés de ADC qui ne reflètent pas les modifications apportées par le pack de configuration.

Pour comparer les modifications du pack de configuration à la configuration des ADC, procédez comme suit.

1. Accédez à **Applications** > **StyleBooks** > **Configurations**.
2. Cliquez sur **Audit de configuration**.

   La page Audit de configuration affiche les objets créés et audités.

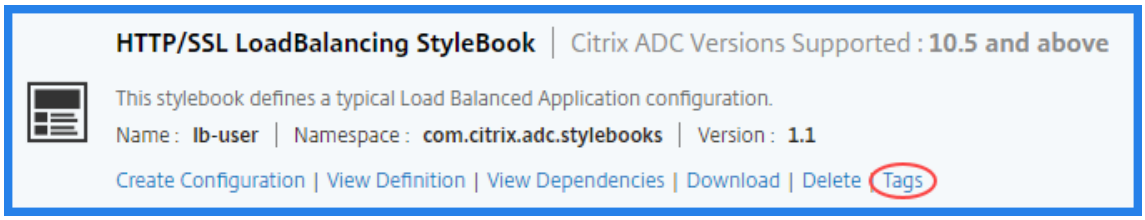


Créer une balise pour le StyleBook

Vous pouvez ajouter des balises à n'importe quel StyleBook dans Citrix ADM. Les balises sont des paires clé-valeur qui vous permettent de regrouper des StyleBooks à l'aide de critères différents. Vous pouvez utiliser ces balises lors de la recherche ou du filtrage de StyleBooks dans Citrix ADM.

Pour ajouter une balise au StyleBook :

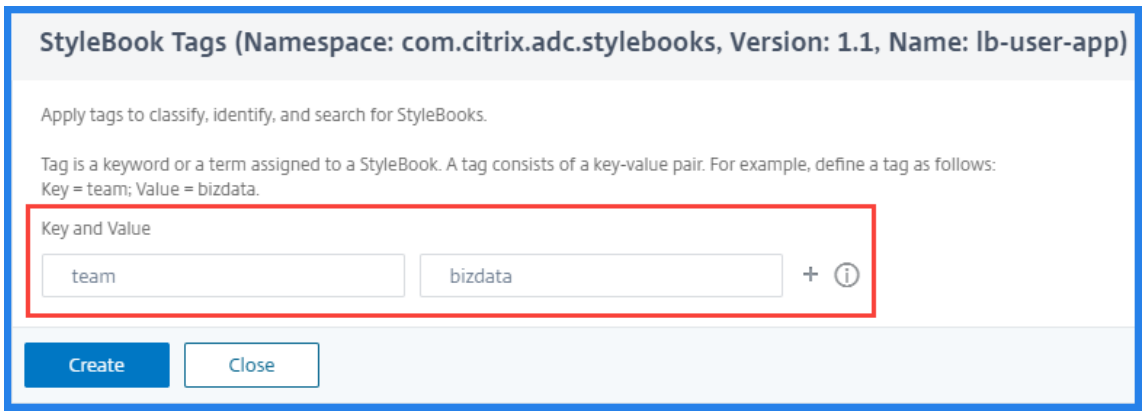
1. Accédez à **Applications** > **StyleBooks** .
2. Sélectionnez **Balises** dans le StyleBook pour lequel vous souhaitez ajouter des balises.



   Vous pouvez ajouter des balises à tous les types de StyleBooks.

3. Spécifiez les informations de **clé** et de **valeur** requises qui vous aident à filtrer le StyleBook.

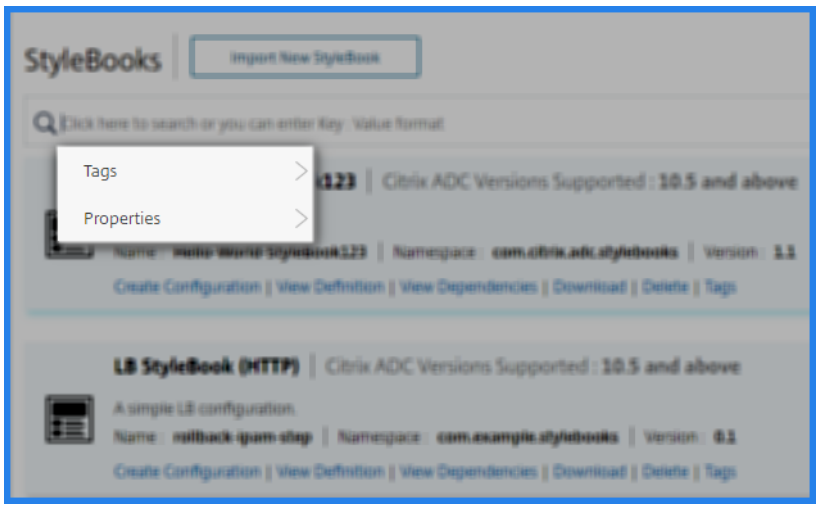
   Par exemple, key=Team et Value=BizData



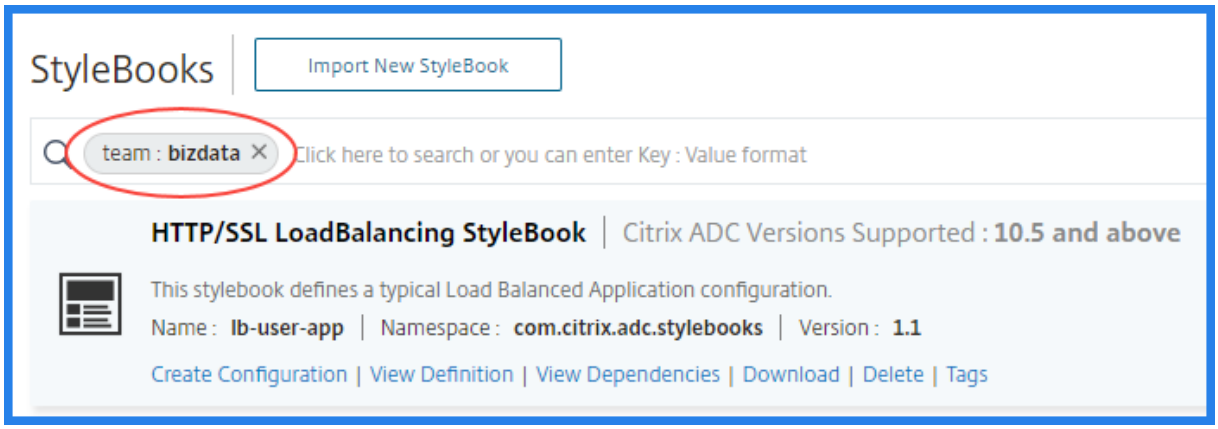
Pour ajouter d'autres balises, cliquez sur **+**.

4. Cliquez sur **Créer**.

Pour filtrer StyleBooks à l'aide de balises, dans la barre de recherche, cliquez sur **Balises** et sélectionnez clé et valeur dans la liste. Les StyleBooks correspondant à la balise spécifiée sont affichés.



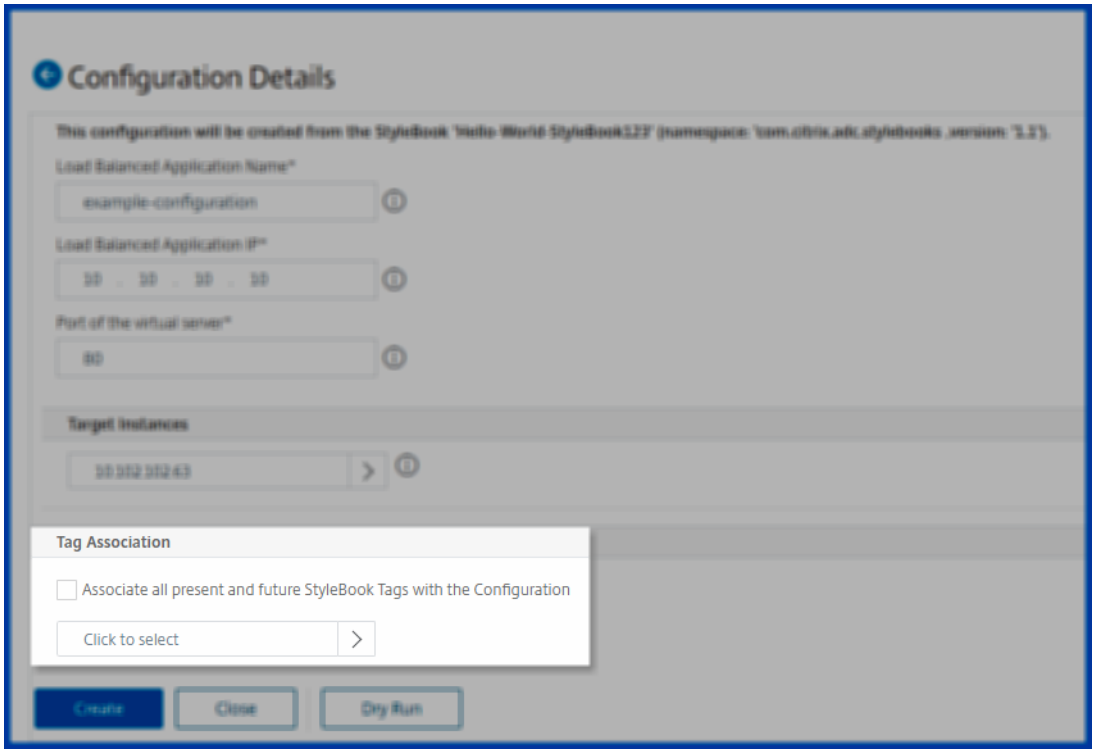
Voici un exemple de recherche pour les StyleBooks qui ont une balise où `key=team` et `value=bizdata` :



Vous pouvez associer les balises StyleBook à son pack de configuration. Ainsi, vous pouvez rechercher les packs de configuration à l'aide des balises StyleBook lui-même.

Lorsque vous créez un pack de configuration, utilisez l'une des options suivantes dans la section **Association de balises** :

- **Associer toutes les balises StyleBook présentes et futures à la configuration** : cette option associe toutes les balises StyleBook à un pack de configuration. Il veille également à associer les nouvelles balises que vous pourriez ajouter aux StyleBooks à l'avenir.
- **Sélectionner les balises** : cette option affiche les balises du StyleBook sélectionné. Vous pouvez sélectionner les balises StyleBook requises et les associer à un pack de configuration.



Importer et synchroniser les StyleBooks à partir du référentiel GitHub

February 1, 2024

Envisagez un scénario dans lequel vous utilisez des processus CI/CD pour votre développement. Ou, un scénario dans lequel vous gérez tous le code source de l'application et les objets de déploiement dans GitHub.

Dans le référentiel GitHub, vous avez peut-être créé plusieurs StyleBooks pour déployer les configurations Citrix ADC et gérer ces StyleBooks. Ces StyleBooks sont également requis dans Citrix Applications and Delivery Management (ADM). Vous pouvez désormais importer directement ces StyleBooks dans Citrix ADM. Vous n'avez pas besoin de les copier manuellement à partir de GitHub, puis de les télécharger dans Citrix ADM ou de synchroniser manuellement les fichiers dans ADM et GitHub.

Vous pouvez désormais définir un référentiel dans Citrix ADM qui représente un référentiel GitHub. Fournissez l'URL du référentiel GitHub ainsi que votre nom d'utilisateur et votre mot de passe (ou jeton d'API) créés dans GitHub. Cela signifie que seuls les utilisateurs autorisés disposant d'un compte valide dans GitHub peuvent importer et synchroniser les StyleBooks.

Après avoir créé le référentiel, vous pouvez synchroniser Citrix ADM avec votre référentiel GitHub. Citrix ADM se connecte à GitHub et importe les StyleBooks trouvés dans ce référentiel. ADM valide ensuite les StyleBooks et les ajoute à la liste des StyleBooks dans Citrix ADM. Les styleBooks ne sont pas

ajoutés à Citrix ADM s'ils échouent la validation. Corrigez les erreurs et validez les versions mises à jour dans votre dépôt GitHub. Plus tard, vous pouvez essayer de les importer ou de les synchroniser à nouveau dans Citrix ADM.

> **Remarque**
>
> - Les fichiers StyleBooks peuvent être importés et synchronisés depuis n'importe quelle branche d'un référentiel GitHub.
> - Vous pouvez également importer et synchroniser des StyleBooks auxquels des StyleBooks dépendants sont associés.
> - La synchronisation de StyleBooks à partir d'un référentiel GitHub doit être lancée manuellement à partir de l'interface graphique ou de l'API Citrix ADM. Autrement dit, actuellement, l'importation et la synchronisation de StyleBooks ne se produisent pas automatiquement en fonction de l'activité de validation de GitHub.

Ajouter un référentiel et importer StyleBooks depuis le référentiel GitHub

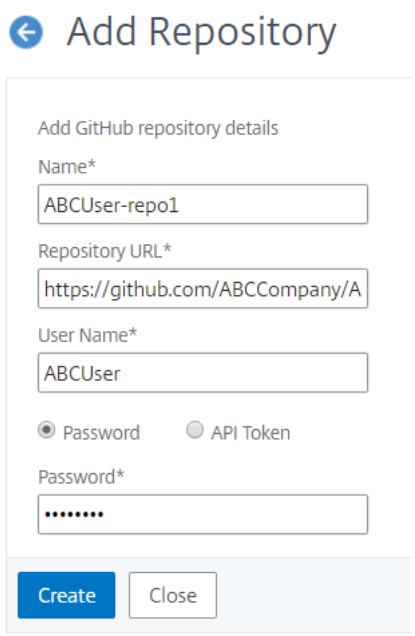
Avant de commencer, assurez-vous d'avoir un compte valide dans GitHub.

Vous pouvez importer des fichiers StyleBook vers ADM à partir de n'importe quel dossier du référentiel GitHub.

1. Dans Citrix ADM, accédez à **Applications** > **StyleBooks** > **Référentiels** .
2. Cliquez sur **Ajouter**. Dans la fenêtre **Ajouter un référentiel**, entrez les paramètres suivants :
   - **Nom**. Entrez le nom du référentiel. Ce nom peut être le même que le nom du référentiel dans GitHub ou un autre.
   - **URL du référentiel**. Tapez l'URL du référentiel GitHub.
   - **Nom d'utilisateur et mot de passe**. Saisissez le nom d'utilisateur et le mot de passe avec lequel vous accédez au compte GitHub.

   > **Remarque**
   >
   > Vous pouvez également fournir le jeton d'API à la place d'un mot de passe. Les jetons API peuvent être utilisés à la place d'un mot de passe pour GitHub sur HTTPS. Pour plus d'informations sur la création de jetons d'API pour votre référentiel GitHub, consultez la documentation GitHub relative à la création de jetons d'accès personnels.

3. Cliquez sur **Créer**.



Le référentiel est créé dans Citrix ADM.

4. Pour importer ou synchroniser StyleBooks, sélectionnez le référentiel dans la page **Référentiels**, puis cliquez sur **Synchroniser** .

Les autres actions que vous pouvez utiliser ici sont les suivantes :

- **Modifier**. Vous pouvez modifier l'URL, le nom d'utilisateur et le mot de passe (ou le jeton API) du référentiel.
- **Supprimer**. Vous pouvez supprimer le référentiel ainsi que tous les StyleBooks présents dans Citrix ADM qui ont été importés précédemment à partir de ce référentiel GitHub.

  > **Remarque**
  >
  > Vous ne pouvez pas supprimer un référentiel de Citrix ADM s'il a des StyleBooks auxquels ConfigPacks est associé. Tout d'abord, supprimez tous les packs de configuration de ces StyleBooks. Vous pouvez ensuite supprimer le référentiel de Citrix ADM pour nettoyer les StyleBooks de ce référentiel.

- **Réinitialiser**. Vous pouvez supprimer tous les StyleBooks dans Citrix ADM synchronisés à partir de ce référentiel sans réellement supprimer l'entrée de référentiel de Citrix ADM.
- **Liste des fichiers**. Vous pouvez voir une liste de tous les StyleBooks présents dans Citrix ADM provenant du référentiel GitHub.

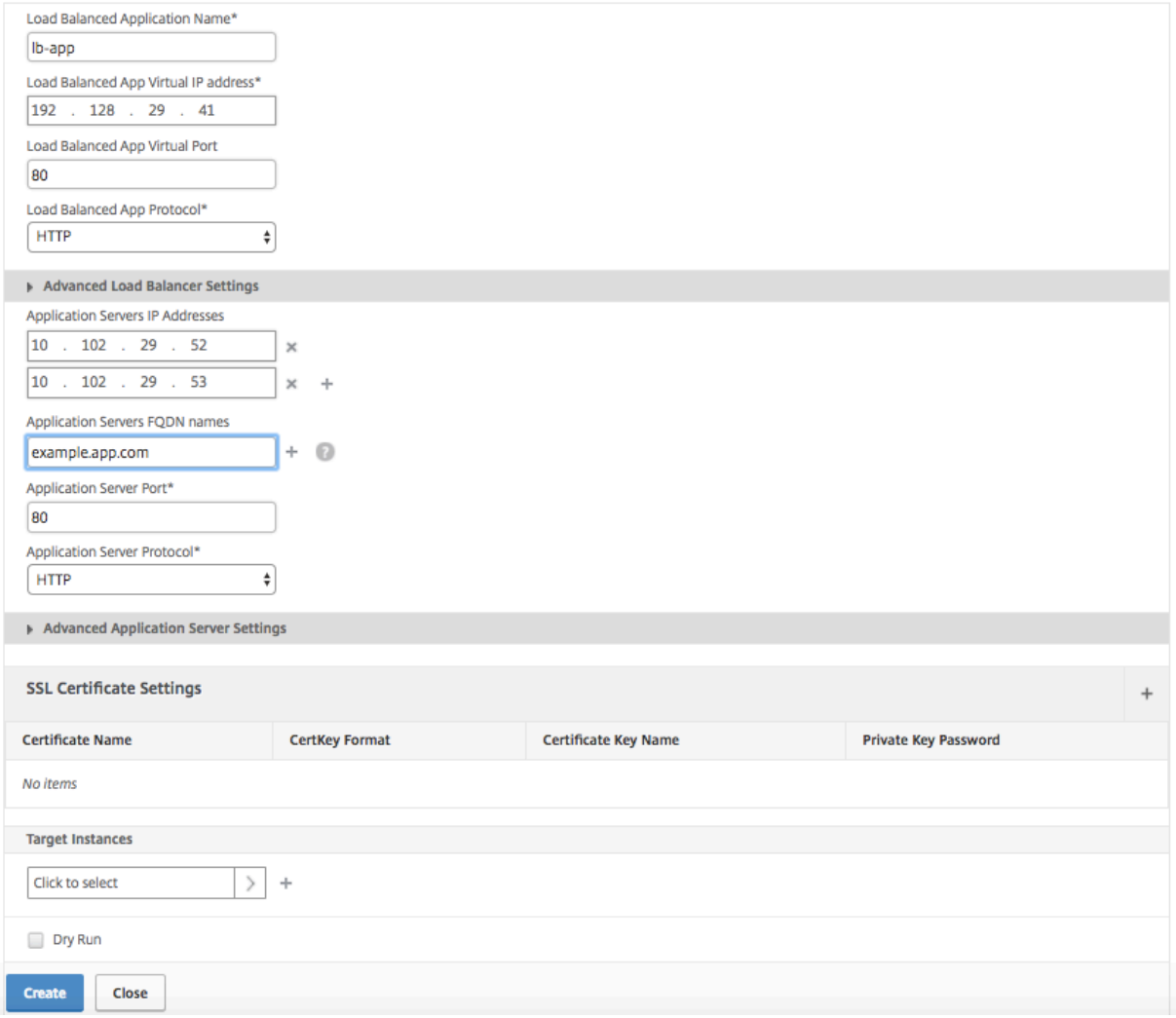
Utiliser les StyleBooks par défaut

February 1, 2024

Un ensemble de StyleBooks par défaut est fourni avec Citrix Application Delivery Management (ADM). Lorsque vous utilisez un StyleBook par défaut, vous devez spécifier des valeurs pour les paramètres du StyleBook et sélectionner les adresses IP des instances Citrix ADC où vous souhaitez exécuter la configuration. Après avoir soumis la configuration, Citrix ADM valide les valeurs des paramètres que vous avez spécifiées, crée un graphe de la configuration, se connecte aux instances Citrix ADC et exécute la configuration sur les instances.

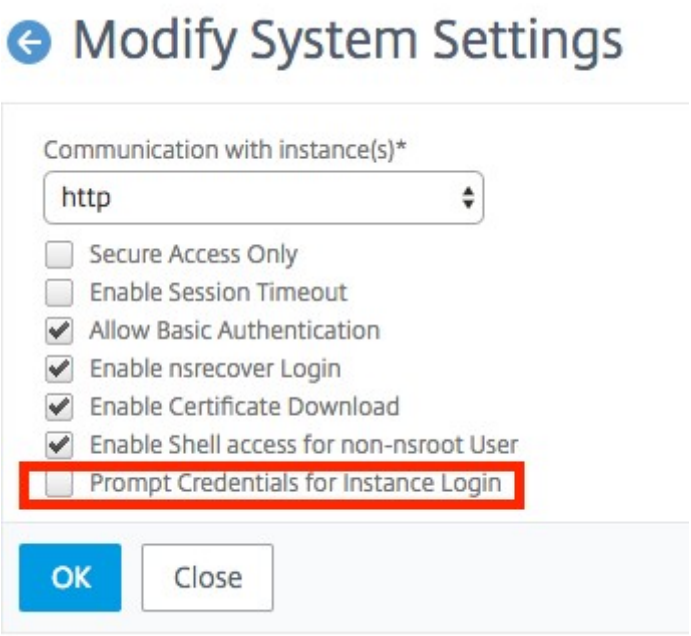
Pour créer une configuration à partir d'un StyleBook par défaut

1. Accédez à **Applications** > **Configurations > StyleBooks**. La page StyleBooks affiche tous les StyleBooks de Citrix ADM. Cette liste inclut les StyleBooks par défaut et personnalisés. Vous pouvez taper le nom du StyleBook dans le champ de recherche et appuyer sur la touche **Entrée**. Sinon, vous pouvez faire défiler la liste vers le bas pour trouver le StyleBook.
2. Cliquez sur **Créer une configuration**. Spécifiez les valeurs requises pour les paramètres.

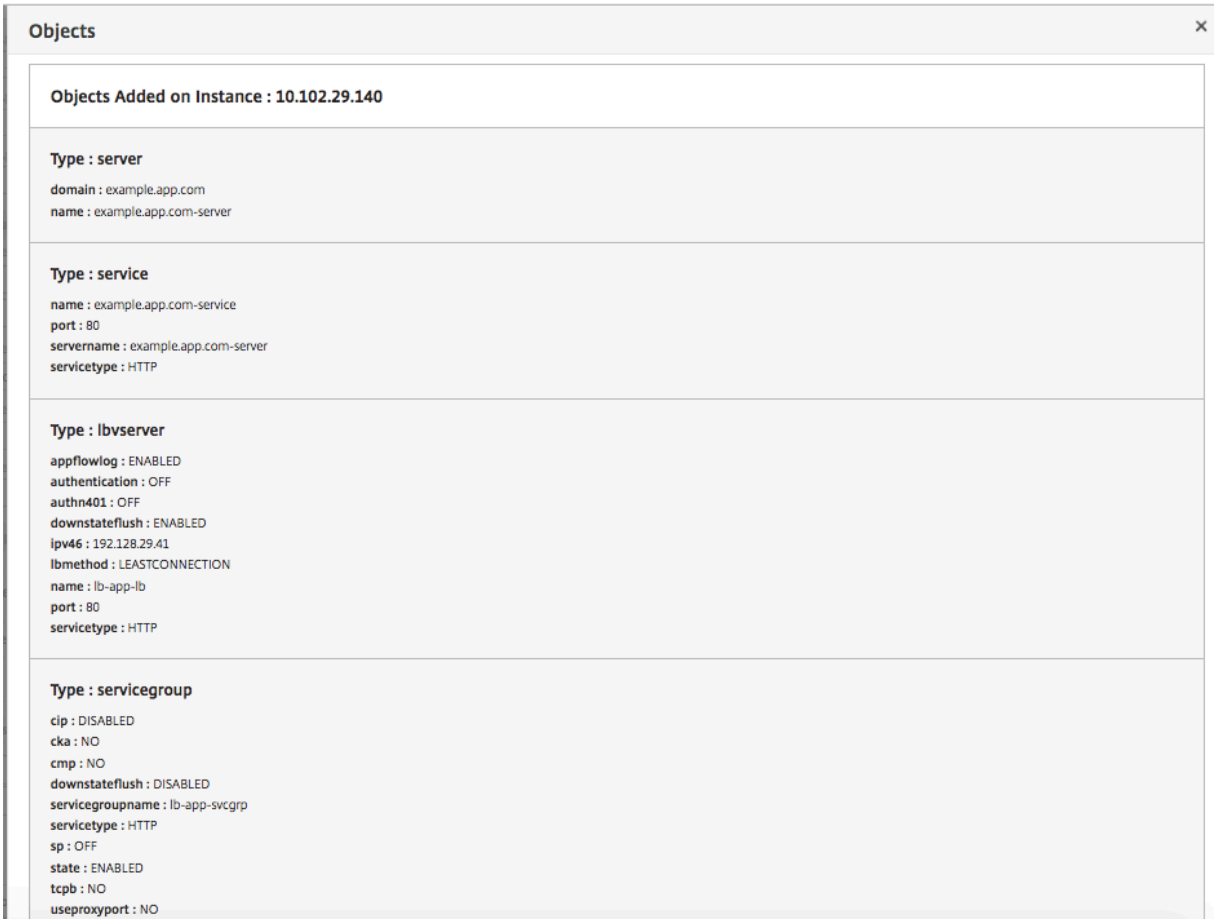


3.Sous **Instances cibles**, cliquez sur et sélectionnez l'adresse IP de l'instance Citrix ADC sur laquelle vous souhaitez exécuter la configuration. Si vous souhaitez exécuter cette configuration sur plusieurs instances, cliquez sur « + » pour ajouter d'autres instances.

Si l'option**Demander des informations d'identification pour la connexion à l'instance**est activée dans **Citrix ADM** > **Système** > **Modifier les paramètres système**> **Modifier les paramètres système**, vous êtes invité à entrer vos informations d'identification d'instance Citrix ADC lorsque vous exécutez la commande sur les instances Citrix ADC sélectionnées. Sinon, Citrix ADM utilise les informations d'identification d'instance stockées dans le profil d'instance pour se connecter à l'instance.



Si vous souhaitez tester ou valider votre configuration avant de l'exécuter sur l'instance Citrix ADC, sélectionnez **Exécution à sec**, puis cliquez sur **Créer**. Si votre configuration est valide, les objets créés sur la base des valeurs que vous avez fournies sont affichés.



4.Désactivez la case à cocher **Exécution à sec** et cliquez sur **Créer** pour créer la configuration et exécuter la configuration sur l'instance Citrix ADC. La configuration StyleBook que vous avez créée apparaît dans la liste des configurations, comme indiqué ci-dessous.

> **Remarque**
>
> Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter des instances Citrix ADC récemment découvertes dans Citrix ADM à la liste des instances disponibles dans cette fenêtre.

Vous pouvez désormais examiner, mettre à jour ou supprimer ce pack de configuration à l'aide de Citrix ADM.

Pare-feu d'application Web StyleBook

February 1, 2024

Citrix Web App Firewall est un pare-feu d'application Web (WAF) qui protège les applications et les

sites Web contre les attaques connues et inconnues, y compris toutes les menaces de couche d'application et de jour zéro.

Citrix ADM fournit désormais un StyleBook par défaut avec lequel vous pouvez créer plus facilement une configuration de pare-feu d'application sur les instances Citrix ADC.

Déploiement de configurations de pare-feu applic

La tâche suivante vous aide à déployer une configuration d'équilibrage de charge avec le pare-feu d'application et la stratégie de réputation IP sur les instances de Citrix ADC dans votre réseau d'entreprise.

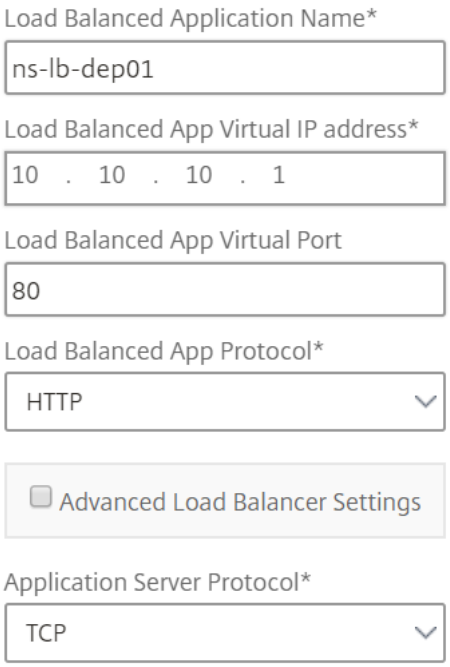
Pour créer une configuration LB avec les paramètres du pare-feu des applications :

1. Dans Citrix ADM, accédez à **Applications** > **Configurations** > **StyleBooks**. La page StyleBooks affiche tous les StyleBooks disponibles pour votre utilisation dans Citrix ADM. Faites défiler vers le bas et recherchez HTTP/SSL Load Balancing StyleBook avec stratégie de pare-feu d'application et stratégie de réputation IP. Vous pouvez également rechercher le StyleBook en tapant le nom sous la forme `lb-appfw`. Cliquez sur **Créer une configuration**.

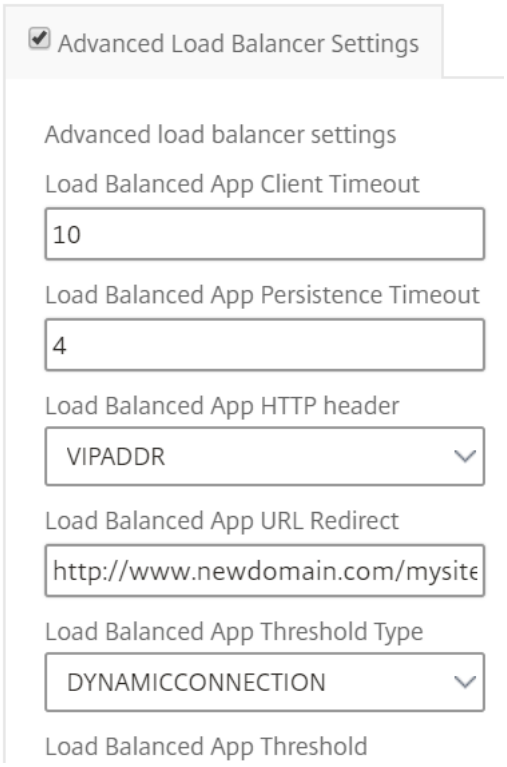
   Le StyleBook s'ouvre sous la forme d'une page d'interface utilisateur sur laquelle vous pouvez entrer les valeurs de tous les paramètres définis dans ce StyleBook.

2. Entrez des valeurs pour les paramètres suivants :

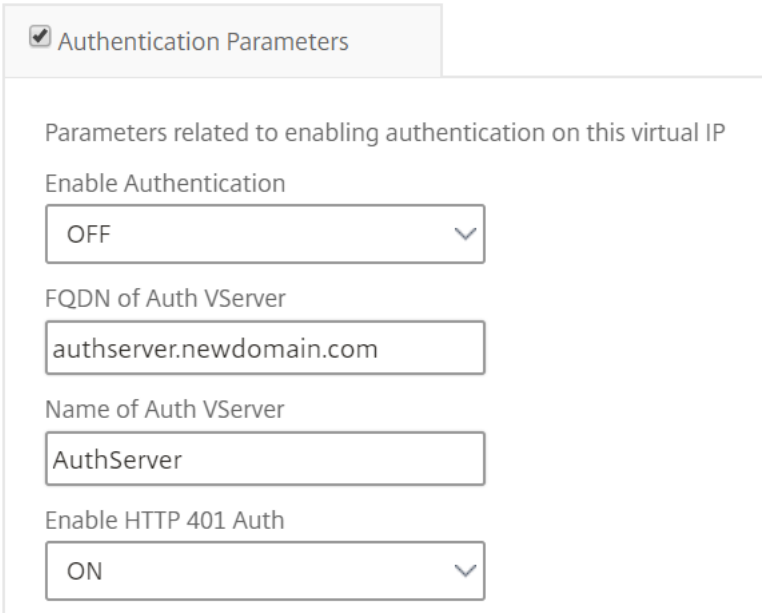
   - **Nom de l'application équilibrée de charge**. Nom de la configuration à répartition de charge avec pare-feu d'applications à déployer sur votre réseau.
   - **Adresse IP virtuelle de l'application équilibrée en charge**. Adresse IP virtuelle à laquelle l'instance Citrix ADC reçoit les demandes des clients.
   - **Port virtuel de l'application à charge équilibrée**. Le port TCP à utiliser par les utilisateurs pour accéder à l'application à charge équilibrée.
   - **Protocole d'application à charge équilibrée**. Sélectionnez le protocole frontal dans la liste.
   - **Protocole de serveur d'applications**. Sélectionnez le protocole du serveur d'applications.



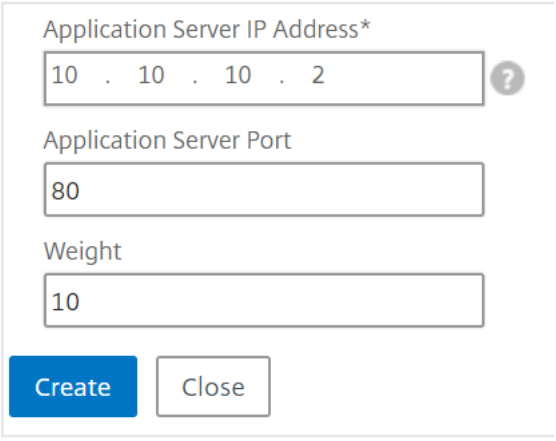
3. En option, vous pouvez activer et configurer les **paramètres avancés d'équilibrage**de charge.



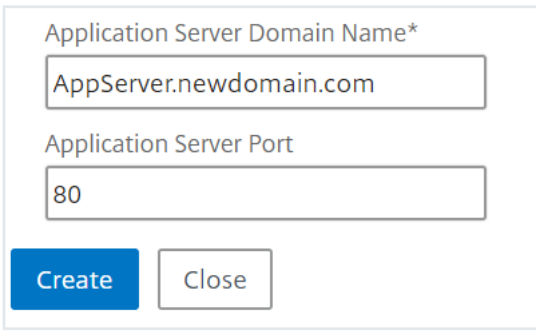
4. Vous pouvez également configurer un serveur d'authentification pour l'authentification du trafic pour le serveur virtuel d'équilibrage de charge.



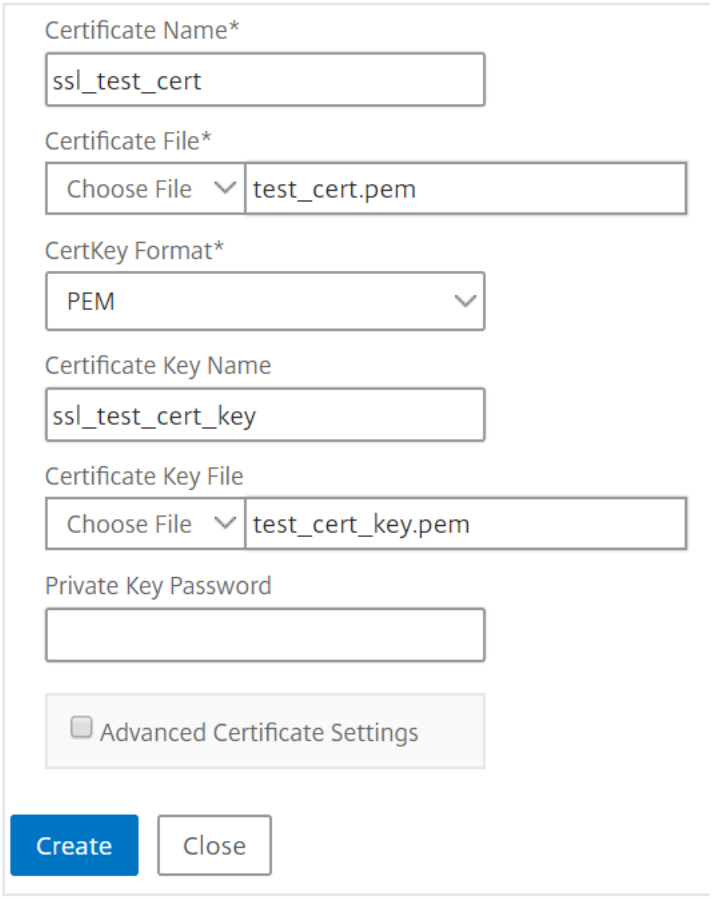
5. Cliquez sur « + » dans la section IP et ports du serveur pour créer des serveurs d'applications et les ports auxquels ils sont accessibles.



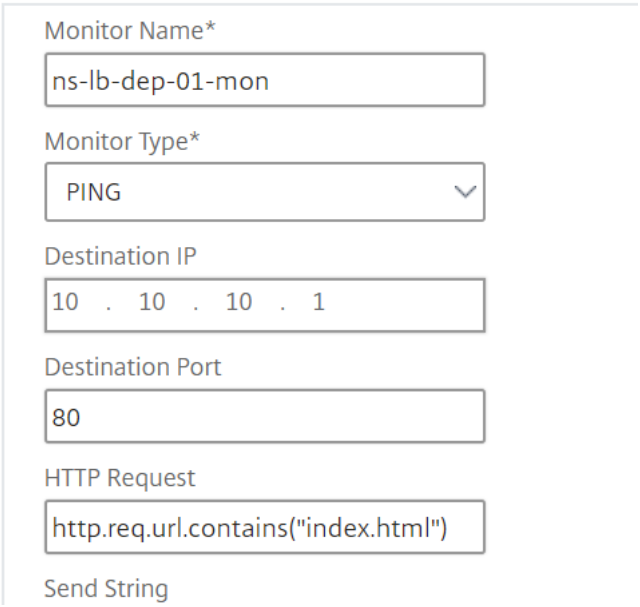
6. Vous pouvez également créer des noms de domaine complet pour les serveurs d'applications.



7. Vous pouvez également spécifier les détails du certificat SSL.



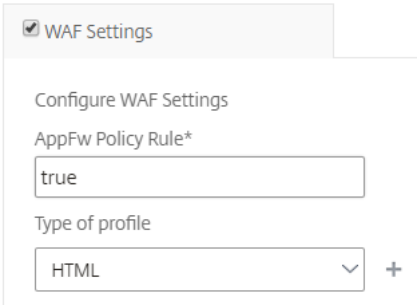
8. Vous pouvez également créer des moniteurs dans l'instance Citrix ADC cible.



9. Pour configurer un pare-feu d'application sur le serveur virtuel, activez les paramètres WAF.

   Assurez-vous que la règle de stratégie de pare-feu d'application est vraie si vous souhaitez ap-

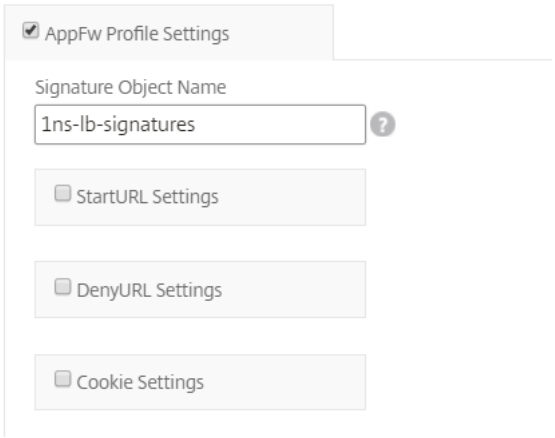
pliquer les paramètres du pare-feu de l'application à tout le trafic sur ce VIP. Sinon, spécifiez la règle de stratégie Citrix ADC pour sélectionner un sous-ensemble de demandes auxquelles appliquer les paramètres du pare-feu d'application. Ensuite, sélectionnez le type de profil à appliquer - HTML ou XML.



10. Vous pouvez également configurer des paramètres détaillés de profil de pare-feu d'application en activant la case à cocher Paramètres de profil du pare-feu d'application.
11. Si vous souhaitez configurer les signatures de pare-feu d'application, entrez le nom de l'objet de signature créé sur l'instance de Citrix ADC sur laquelle le serveur virtuel doit être déployé.

    > **Remarque**
    >
    > Vous ne pouvez pas créer un objet de signature à l'aide de ce StyleBook.

12. Ensuite, vous pouvez également configurer d'autres paramètres de profil de pare-feu d'application tels que les paramètres StarTURL, DenyURL et autres.



Pour plus d'informations sur le pare-feu d'application et les paramètres de configuration, voir Pare-feu d'application.

13. Dans la section **Instances cibles**, sélectionnez l'instance Citrix ADC sur laquelle déployer le serveur virtuel d'équilibrage de charge avec le pare-feu d'application.

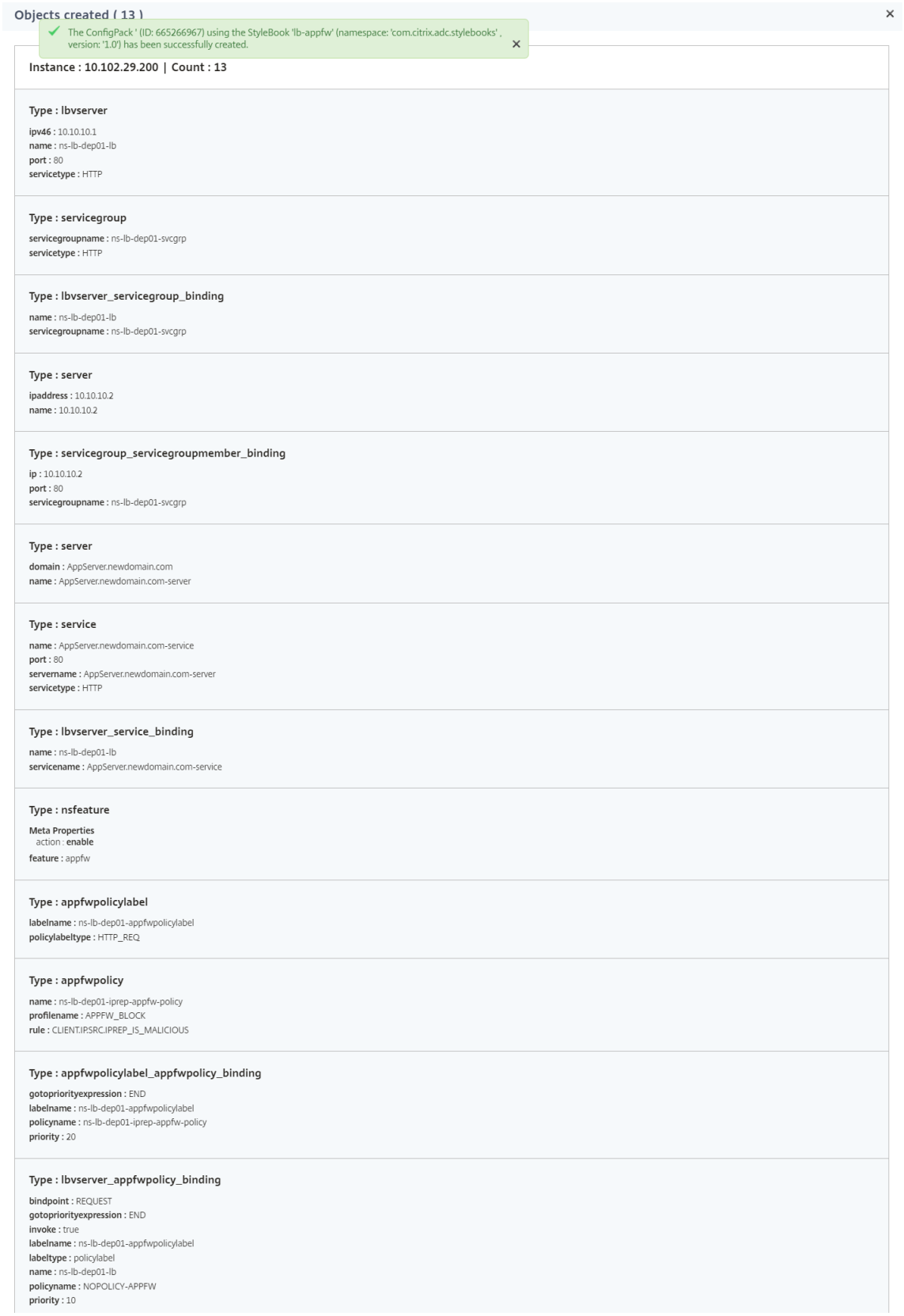
> **Remarque**
>
> Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter des instances Citrix ADC récemment découvertes dans Citrix ADM à la liste des instances disponibles dans cette fenêtre.

14. Vous pouvez également activer la **vérification de la réputation IP** pour identifier l'adresse IP qui envoie des demandes indésirables. Vous pouvez utiliser la liste de réputation IP pour rejeter préventivement les demandes provenant de l'IP avec la mauvaise réputation.
15. Cliquez sur **Créer** pour créer la configuration sur les instances Citrix ADC sélectionnées.

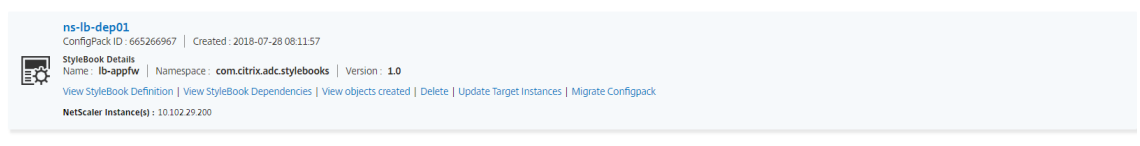
> **Conseil**
>
> Citrix vous recommande de sélectionner Dry Run pour vérifier les objets de configuration qui doivent être créés sur l'instance cible avant d'exécuter la configuration réelle sur l'instance.

Lorsque la configuration est correctement créée, le StyleBook crée le serveur virtuel d'équilibrage de charge requis, le serveur d'applications, les services, les groupes de services, les étiquettes de pare-feu d'application, les stratégies de pare-feu d'application et les lie au serveur virtuel d'équilibrage de charge.

La figure suivante montre les objets créés sur chaque serveur :



16. Pour afficher le ConfigPack créé sur Citrix ADM, accédez à **Applications** > **Configurations** .



Créer des profils WAF et BOT à l'aide de StyleBook

February 1, 2024

Lorsque vous pouvez sélectionner une stratégie pour une ressource API dans **API Gateway, elle**vous permet de définir les critères de sélection du trafic pour authentifier une demande d'API. En outre, il vous permet de configurer les stratégies de sécurité de l'API sur le trafic de l'API. Pour plus d'informations, consultez Gérer la passerelle d'API.

Vous pouvez configurer des stratégies WAF et BOT sur une ressource API. Avant de configurer une stratégie, assurez-vous de créer son profil dans Citrix Application Delivery Management (ADM). Utilisez les StyleBooks par défaut suivants pour créer un profil :

- API WAF Détection Stylebook
- API BOT Detection StyleBook

Créer un profil WAF à l'aide du StyleBook

Effectuez les opérations suivantes pour créer un profil WAF :

1. Dans Citrix ADM, accédez à **Applications** > **Configurations** > **StyleBooks**. Recherchez le StyleBook en tapant le nom en tant que `api-waf-profile`. Cliquez sur **Créer une configuration**.

   Le StyleBook s'ouvre en tant que page d'interface utilisateur sur laquelle vous pouvez entrer les valeurs de tous les paramètres définis dans ce StyleBook.

2. Spécifiez les valeurs pour les paramètres suivants :

   - **Nom du profil WAF API** - Nom permettant d'identifier un profil WAF.
   - **Type d'application** : ajoutez des types d'application au profil. Le profil WAF prend en charge les types d'application JSON et XML.

3. Facultatif, activez **Paramètres de sécurité** pour spécifier des vérifications de protection HTTP, JSON ou XML. Vous pouvez également spécifier une URL d'erreur vers le Citrix Web App Firewall. Pour plus d'informations, consultez Création d'un profil Web App Firewall.

4. Sélectionnez l'instance Citrix ADC cible ou le groupe d'instances sur lequel vous souhaitez déployer cette configuration.
5. Cliquez sur **Créer**.

Pour configurer une stratégie WAF, reportez-vous à la section Ajouter des stratégies à un déploiement d'API.

Créer un profil BOT à l'aide du StyleBook

Effectuez les opérations suivantes pour créer un profil BOT :

1. Dans Citrix ADM, accédez à **Applications** > **Configurations** > **StyleBooks**. Recherchez le StyleBook en tapant le nom en tant que `api-bot-profile`. Cliquez sur **Créer une configuration**.

   Le StyleBook s'ouvre en tant que page d'interface utilisateur sur laquelle vous pouvez entrer les valeurs de tous les paramètres définis dans ce StyleBook.
2. Dans **Nom du profil BOT**, spécifiez un nom pour identifier un profil BOT.
3. Facultatif, activez les options suivantes en fonction de vos besoins :

   - **Activer la vérification de la réputation IP** - Cette option identifie l'adresse IP qui envoie des demandes indésirables. Vous pouvez utiliser la liste de réputation IP pour rejeter préventivement les demandes provenant de l'IP avec la mauvaise réputation.
   - **Activer les signatures BOT** - Spécifiez le nom de la signature BOT. Il bloque les requêtes de la signature spécifiée.
   - **Autoriser la liste** - Spécifiez l'adresse IPv4 ou de sous-réseau (CIDR). Cette option permet au profil BOT de contourner les requêtes de l'adresse IPv4 ou de sous-réseau spécifiée.
   - **Refuser List** - Spécifiez l'adresse IPv4 ou de sous-réseau (CIDR). Cette option permet au profil BOT de bloquer les demandes provenant de l'adresse IPv4 ou de sous-réseau spécifiée.
4. Sélectionnez l'instance Citrix ADC cible ou le groupe d'instances sur lequel vous souhaitez déployer cette configuration.
5. Cliquez sur **Créer**.

Pour configurer une stratégie BOT, consultez la section Ajouter des stratégies à un déploiement d'API.

Masquer tous les StyleBooks par défaut

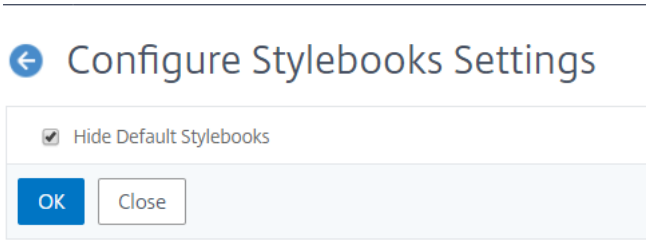
February 1, 2024

Citrix ADM répertorie tous les StyleBooks présents dans le système de dossiers Citrix ADM. La liste des StyleBooks inclut les StyleBooks par défaut et personnalisés qui peuvent être à la fois privés et publics. En tant qu'administrateur, vous souhaiterez peut-être masquer tous les StyleBooks par défaut. Vous pouvez autoriser vos utilisateurs à consulter et à accéder uniquement aux StyleBooks personnalisés créés par vous ou par les utilisateurs.

Citrix ADM vous permet d'afficher vos StyleBooks personnalisés et de masquer tous les StyleBooks par défaut fournis avec Citrix ADM. Une nouvelle option d'interface graphique permet de masquer tous les StyleBooks par défaut.

Pour masquer tous les StyleBooks par défaut :

1. Dans Citrix ADM, accédez à **Applications** > **Configurations > Paramètres.**
2. La page **Paramètres** affiche des informations indiquant si les StyleBooks par défaut sont visibles par les utilisateurs ou non.
3. Pour masquer les StyleBooks par défaut, cliquez sur l'icône d'édition en haut à droite.
4. Sur la page **Configurer les paramètres du StyleBook**, sélectionnez l'option **Masquer les StyleBooks par défaut** .
5. Cliquez sur **OK**.



La page **Configurer les paramètres StyleBook** est toujours visible pour les utilisateurs si vous n'avez pas choisi de masquer la page à l'aide de la fonction RBAC. Il se peut que les utilisateurs aient toujours la possibilité d'afficher les StyleBooks par défaut.

Pour masquer la page **Configurer les paramètres StyleBook** , vous devez créer une stratégie et attribuer cette stratégie aux utilisateurs qui ne doivent pas voir les StyleBooks par défaut.

Pour créer une stratégie RBAC :

1. Dans Citrix ADM, accédez à **Compte** > **Administration des utilisateurs** > **Stratégies d'accès**.

2. Cliquez sur **Add** pour créer une stratégie.
3. Entrez le nom de la stratégie.
4. Dans la section **Autorisations**, assurez-vous que l'option **Tout** > **Applications** > **Configuration** >**Paramètres** n'est pas sélectionnée, puis cliquez sur **OK**.

Après avoir créé des stratégies, vous devez créer des rôles, lier chaque rôle à une ou plusieurs stratégies et affecter des rôles à des groupes d'utilisateurs. Pour en savoir plus sur la façon d'associer des stratégies à des utilisateurs, consultez Configuration du contrôle d'accès basé sur les rôles.

Migrer la configuration de l'application Citrix ADC à l'aide de StyleBooks Configuration Builder

February 1, 2024

> **Remarque**
>
> Cette fonctionnalité est en avant-première technologique.

Le générateur de configuration StyleBooks est utilisé pour créer une configuration d'application StyleBook à partir d'une configuration Citrix ADC existante. Cette fonctionnalité automatise également la migration de la configuration de l'application d'une instance Citrix ADC vers une autre instance.

À l'aide de Configuration Builder, vous pouvez simplifier la création d'un StyleBook personnalisé. Cette fonctionnalité vous permet de créer un StyleBook sans connaissances approfondies de la grammaire et des constructions de StyleBooks. Sinon, la connaissance de la grammaire et des constructions de StyleBooks est nécessaire pour créer un StyleBook.

Le Générateur de configuration crée également un ConfigPack qui reflète la même configuration ADC sur une nouvelle instance ADC. Avec ce ConfigPack, la configuration ADC initiale d'une instance ADC peut être dupliquée sur une autre instance ADC. La source de configuration initiale peut être l'une des suivantes :

- **Une instance Citrix ADC :** spécifiez l'instance dans laquelle la configuration de l'application que vous souhaitez dupliquer est hébergée.

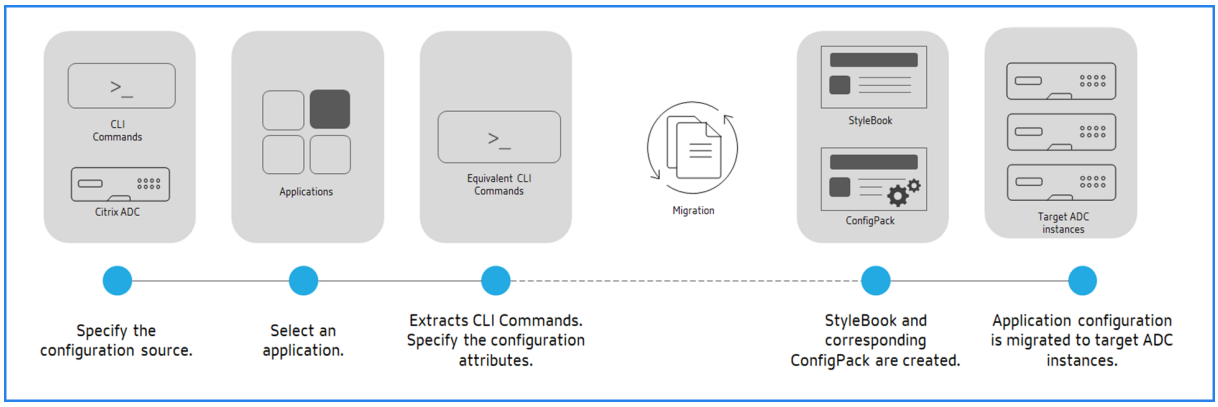
  Le Générateur de configuration convertit la configuration ADC en StyleBook et ConfigPack même si vous ne spécifiez pas l'instance cible. Vous pouvez ensuite utiliser ce configpack pour migrer la configuration ADC vers d'autres instances ADC.

- **Un ensemble de commandes CLI :** Collez la configuration à partir de `ns.conf` ou `Application config`.

Le générateur de configuration identifie la liste des applications distinctes intégrées dans la configuration source. Lorsque vous sélectionnez la configuration d'application qui vous intéresse, le Générateur de configuration extrait l'ensemble des commandes CLI pour l'application sélectionnée. Ces commandes CLI sont extraites de la configuration source. Il identifie également les attributs de déploiement et de configuration qui peuvent nécessiter votre entrée.

- **Attributs de déploiement** : vous pouvez afficher et modifier l'adresse IP et le port des serveurs virtuels, des services et des membres du groupe de services à partir de la configuration d'origine.
- **Attributs de configuration** : ces attributs peuvent être des mots de passe ou des certificats spécifiés dans la configuration source.

Après avoir spécifié les informations nécessaires, commencez à migrer ou à dupliquer la configuration de l'application sur une instance ADC cible.



Une fois que vous avez terminé la création et la migration de l'application, un ConfigPack est créé dans Citrix ADM avec son StyleBook correspondant. Ce ConfigPack représente la configuration de l'application sur l'instance ADC cible. Pour afficher le ConfigPack créé, accédez à **Applications** > **StyleBooks** > **Configurations** .

Fonctionnalités de Citrix ADC prises en charge

Le générateur de configuration StyleBook reconnaît et prend en charge les fonctionnalités Citrix ADC suivantes dans la configuration source :

- Commutation de contenu
- Équilibrage de charge
- Surveillance
- Déchargement SSL
- Limitation de débit
- Réécriture

- Répondeur
- Pare-feu pour applications Web (WAF)

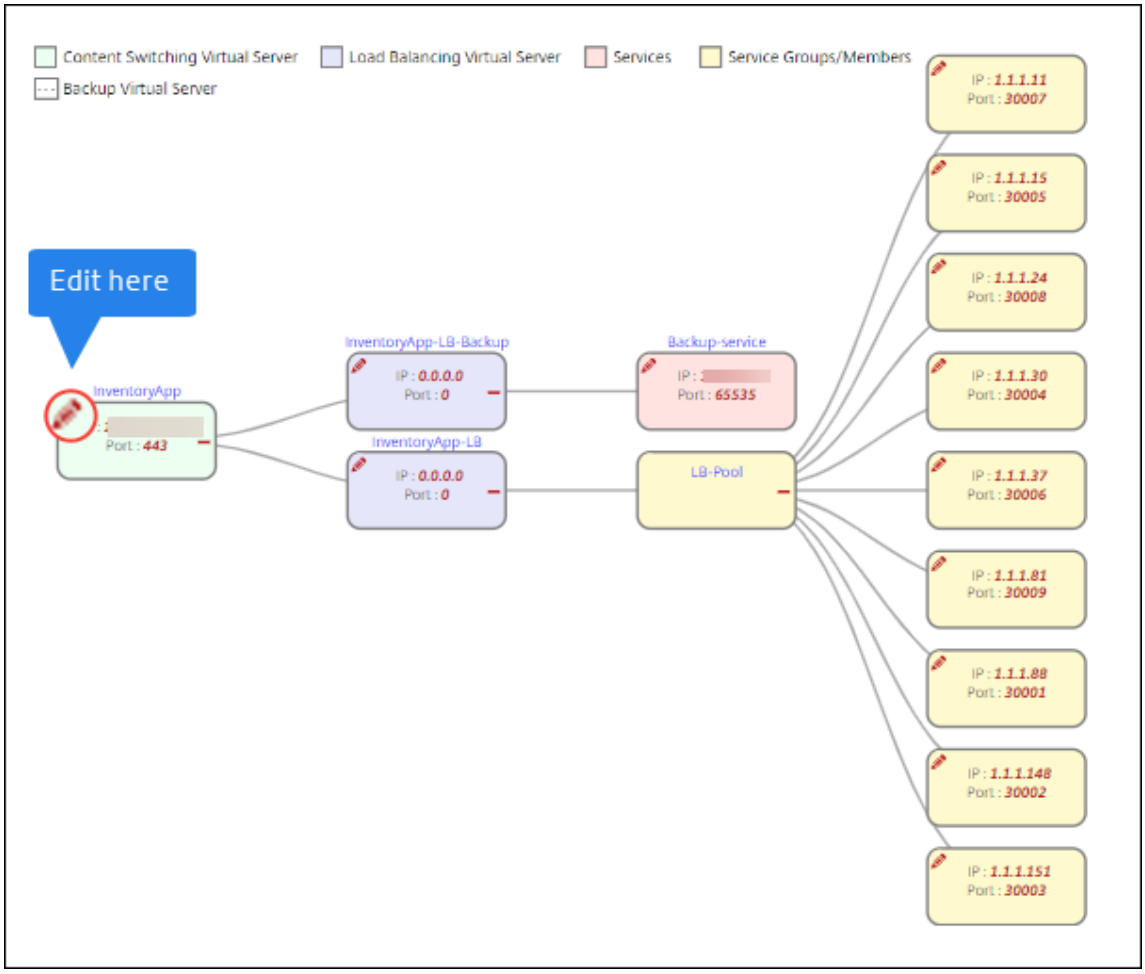
Créez un StyleBook pour migrer la configuration de l'application Citrix ADC

La procédure suivante permet de créer un StyleBook qui migre la migration de l'application Citrix ADC dans Citrix ADM :

1. Accédez à **Applications** > **StyleBooks** > **Configurations**.
2. Cliquez sur **Migrer la configuration ADC**.
3. Cliquez sur **Commencer**.
4. Dans **Spécifier la configuration**, sélectionnez la source de configuration :
    - **Importer depuis un ADC** : Cette option permet de découvrir les applications actives sur l'instance ADC sélectionnée.
    - **Importer à l'aide des commandes CLI** : Cette option analyse les commandes de la CLI et extrait les applications des commandes de la CLI.
5. Spécifiez l'**instance ADC source** à partir de laquelle vous souhaitez migrer ou dupliquer la configuration de l'application.
6. Spécifiez l'**instance ADC cible** vers laquelle vous souhaitez migrer ou dupliquer la configuration de l'application.
7. Dans **Définir une application**,
    a) Dans **Nom de l'application**, spécifiez le nom de l'application.
    b) Sélectionnez les serveurs virtuels à migrer.
    c) Cliquez sur **Suivant**.
8. Dans **Commandes CLI équivalentes**, passez en revue les commandes et cliquez sur **Suivant**.

    Ces commandes sont spécifiques à la configuration de l'application sélectionnée.
9. Dans **Attributs de déploiement**, vous pouvez afficher et modifier l'adresse IP et le port des serveurs virtuels, des services et des membres du groupe de services.

    Pour modifier l'adresse IP et le port, cliquez sur l'icône Modifier sur le serveur virtuel, le service ou le membre du groupe de services dans l'organigramme.



Cet onglet n'apparaît que dans les cas suivants :

- Les instances source et cible sont différentes.
- Importez des configurations à l'aide des commandes CLI.

10. Dans **Attributs de configuration**, spécifiez les détails nécessaires et cliquez sur **Suivant**.

    Cet onglet répertorie les secrets tels que les clés pour déchiffrer les mots de passe et les certificats.

    > **Remarque**
    >
    > Avant de commencer la migration, les configurations manquées ou non prises en charge sont affichées dans l'un des onglets suivants : Configurations non prises en charge
    >
    > **Configurations globales**
    >
    > **non prises en charge**
    >
    > Pour réussir la migration de ces configurations, vous devez appliquer les configurations manquantes ou non prises en charge séparément sur l'instance cible. Et, cliquez sur **Suiv-**

> **ant**.

11. Dans **Migrate**, spécifiez les détails StyleBook requis. Cliquez sur **Migrate**.

Limitations

- Les expressions nommées et `responderhtmlpages` mentionnées dans l'instance source ne sont pas identifiées. Assurez-vous de configurer les expressions nommées et `responderhtmlpages` sur l'instance cible avant la migration.
- Si la source dispose d'une configuration pour `servicegroup` et d'une liaison de surveillance comme suit :

  `bind serviceGroup <Name> <Port> -monitorName <Monitor_Name>`

  L'erreur suivante s'affiche :

  ```
  1  CLI Command conversion failed: 100 - No such command [{
  2   "errorcode": 1090, "message": "No such argument [XXX]", "
         severity": "ERROR"  }
  3  ]
  4  <!--NeedCopy-->
  ```

  Cette erreur se produit car Citrix ADC enregistre la liaison entre Service Group et Monitor dans un format non valide. Ce problème est résolu à partir de la version 12.1.52.15 de Citrix ADC.

Applications d'entreprise StyleBooks

February 1, 2024

Citrix ADM fournit les StyleBooks qui vous aident à déployer une configuration ADC pour des applications métier spécifiques. Pour plus d'informations sur ces StyleBooks, consultez les rubriques suivantes :

- StyleBook Google Apps SSO
- SSO Office 365 StyleBook
- StyleBook Microsoft Skype for Business
- StyleBook Microsoft Exchange
- Microsoft SharePoint StyleBook
- StyleBook proxy Microsoft ADFS

- StyleBook Oracle E-Business
- Pare-feu d'application Web StyleBook
- Créer des profils WAF et BOT à l'aide de StyleBook

StyleBook Google Apps SSO

February 1, 2024

Google Apps est un ensemble d'outils, de logiciels et de produits de cloud computing, de productivité et de collaboration développés par Google. L'authentification unique (SSO) permet aux utilisateurs d'accéder à toutes leurs applications cloud d'entreprise, y compris les administrateurs qui se connectent à la console d'administration, en se connectant en une seule fois pour tous les services à l'aide de leurs informations d'identification d'entreprise.

Le Citrix ADM SSO Google Apps StyleBook vous permet d'activer l'authentification unique pour Google Apps via des instances Citrix ADC. StyleBook configure l'instance Citrix ADC en tant que fournisseur d'identité SAML pour authentifier les utilisateurs pour accéder à Google Apps.

L'activation de l'authentification unique pour les applications Google dans une instance Citrix ADC à l'aide de ce StyleBook se traduit par les étapes suivantes :

1. Configuration du serveur virtuel d'authentification
2. Configuration d'une stratégie et d'un profil d'IdP SAML
3. Liaison de la stratégie et du profil au serveur virtuel d'authentification
4. Configuration d'un serveur d'authentification LDAP et d'une stratégie sur l'instance
5. Lier le serveur et la stratégie d'authentification LDAP à votre serveur virtuel d'authentification configuré sur l'instance

Détails de configuration :

Le tableau ci-dessous répertorie les versions logicielles minimales requises pour que cette intégration fonctionne correctement. Le processus d'intégration prendra également en charge les versions supérieures de la même.

Produit	Version minimale requise
Citrix ADC	Version 11.0, licence avancée/Premium

Les instructions suivantes supposent que vous avez déjà créé les entrées DNS externes ou internes appropriées pour acheminer les demandes d'authentification vers une adresse IP surveillée par Citrix ADC.

Déploiement des configurations Google apps StyleBook SSO :

La tâche suivante vous aide à déployer le Microsoft SSO Google Apps StyleBook sur votre réseau d'entreprise.

Pour déployer l'application Google StyleBook SSO

1. Dans Citrix ADM, accédez à **Applications** > **Configurations** >**StyleBooks**. La page StyleBooks affiche tous les StyleBooks disponibles pour votre utilisation dans Citrix ADM. Faites défiler vers le bas et trouvez **SSO Google Apps StyleBook**. Cliquez sur **Créer une configuration**.
2. Le StyleBook s'ouvre sous la forme d'une page d'interface utilisateur sur laquelle vous pouvez entrer les valeurs de tous les paramètres définis dans ce StyleBook.
3. Entrez des valeurs pour les paramètres suivants :

    a) **Nom de l'application**. Nom de la configuration SSO Google Apps à déployer sur votre réseau.

    b) **Authentification Adresse IP virtuelle**. Adresse IP virtuelle utilisée par le serveur virtuel d'authentification, d'autorisation et d'audit auquel la stratégie d'IdP SAML de Google Apps est liée.

    c) **Expression de règle SAML**. Par défaut, l'expression Citrix ADC Policy (PI) suivante est utilisée : HTTP.REQ.HEADER (« Referrer ») .CONTAINS (« google »). Mettez à jour ce champ avec une autre expression si votre besoin est différent. Cette expression de stratégie correspond au trafic auquel ces paramètres SSO SAML sont appliqués et s'assure que l'en-tête Referrer provient d'un domaine Google.

4. La section Paramètres d'IdP SAML vous permet de configurer votre instance Citrix ADC en tant que fournisseur d'identité SAML en créant le profil et la stratégie d'IdP SAML utilisés par le serveur virtuel d'authentification, d'autorisation et d'audit créé à l'étape 3.

    a) **Nom de l'émetteur SAML**. Dans ce champ, entrez le nom de domaine complet public de votre serveur virtuel d'authentification. Exemple : `https://<Citrix ADC Auth VIP>/saml/login`

    b) **ID du fournisseur de services (SP) SAML**. (facultatif) Le fournisseur d'identité Citrix ADC accepte les demandes d'authentification SAML provenant d'un nom d'émetteur qui correspond à cet identifiant.

    c) **URL du service client Assertion**. Entrez l'URL du fournisseur de services à laquelle le fournisseur d'identité Citrix ADC doit envoyer les assertions SAML après une authentification utilisateur réussie. L'URL du service client d'assertion peut être initiée sur le site serveur du fournisseur d'identité ou sur le site du fournisseur de services.

d) Vous pouvez saisir d'autres champs facultatifs dans cette section. Par exemple, vous pouvez définir les options suivantes :

i. Profil de liaison SAML (le profil par défaut est le profil « POST »).

ii. Algorithme de signature pour vérifier/signer les demandes/réponses SAML (par défaut est « RSA-SHA1 »).

iii. Méthode pour digérer le hachage pour les demandes/réponses SAML (par défaut est « SHA-1 »).

iv. Algorithme de chiffrement (AES256 par défaut) et autres paramètres.

> **Remarque**
>
> Citrix vous recommande de conserver les paramètres par défaut car ces paramètres ont été testés pour être compatibles avec Google Apps.

e) Vous pouvez également activer la case à cocher Attributs utilisateur pour entrer les détails de l'utilisateur tels que :

i. Nom de l'attribut utilisateur

ii. Expression Citrix ADC PI évaluée pour extraire la valeur de l'attribut

iii. Nom convivial de l'attribut

iv. Sélectionnez le format de l'attribut utilisateur.

Ces valeurs sont incluses dans l'assertion SAML émise. Vous pouvez inclure jusqu'à cinq ensembles d'attributs utilisateur dans une assertion émise par Citrix ADC à l'aide de ce StyleBook.

5. Dans la section Paramètres LDAP, entrez les informations suivantes pour authentifier les utilisateurs de Google Apps. Pour que les utilisateurs du domaine puissent se connecter à l'instance Citrix ADC à l'aide de leurs adresses e-mail professionnelles, vous devez configurer les éléments suivants :

a) **Base LDAP (Active Directory)**. Entrez le nom de domaine de base pour le domaine dans lequel les comptes d'utilisateur résident dans Active Directory (AD) pour lequel vous souhaitez autoriser l'authentification. Par exemple `dc=netscaler,dc=com`

b) **LDAP (Active Directory) Bind DN**. Ajoutez un compte de domaine (à l'aide d'une adresse e-mail pour faciliter la configuration) qui dispose des droits de parcourir l'arborescence AD. Par exemple,`cn=Manager,dc=netscaler,dc=com`

c) **Mot de passe du nom unique de liaison LDAP (Active Directory)**. Entrez le mot de passe du compte de domaine pour l'authentification.

d) Quelques autres champs que vous devez saisir dans cette section sont les suivants :

i. Adresse IP du serveur LDAP auquel Citrix ADC se connecte pour authentifier les utilisateurs

ii. Nom de domaine complet du serveur LDAP

> **Remarque**
>
> Vous devez spécifier au moins l'une des deux options ci-dessus : l'adresse IP du serveur LDAP ou le nom de domaine complet.

iii. Port serveur LDAP auquel Citrix ADC se connecte pour authentifier les utilisateurs (la valeur par défaut est 389).

iv. Nom d'hôte LDAP. Ceci est utilisé pour valider le certificat LDAP si la validation est activée (par défaut, il est désactivé).

v. Attribut de nom de connexion LDAP. L'attribut par défaut utilisé pour extraire les noms de connexion est « SamAccountName. »

vi. Autres paramètres LDAP divers facultatifs

6. Dans la section Certificat SSL SAML IdP, vous pouvez spécifier les détails du certificat SSL :

a) **Nom du certificat**. Entrez le nom du certificat SSL.

b) **Fichier de certificat**. Choisissez le fichier de certificat SSL dans le répertoire de votre système local ou sur Citrix ADM.

c) **Format CertKey**. Sélectionnez le format du certificat et des fichiers de clé privée dans la zone de liste déroulante. Les formats pris en charge sont les extensions .pem et .der.

d) **Nom de la clé de certificat**. Entrez le nom de la clé privée du certificat.

e) **Fichier clé du certificat**. Sélectionnez le fichier contenant la clé privée du certificat depuis votre système local ou depuis Citrix ADM.

f) Mot de**passe de clé privée**. Si votre fichier de clé privée est protégé par un mot de passe, saisissez-le dans ce champ.

g) Vous pouvez également activer la case à cocher Paramètres avancés du certificat pour saisir des détails tels que la période de notification d'expiration du certificat, activer ou désactiver le moniteur d'expiration des certificats.

7. Vous pouvez éventuellement sélectionner le certificat CA SSL IdP si le certificat IDP SAML saisi ci-dessus nécessite l'installation d'un certificat public CA sur Citrix ADC. Assurez-vous de sélectionner « Est un certificat CA » dans les paramètres avancés.

8. Vous pouvez éventuellement sélectionner le certificat SSL SAML SP pour spécifier le certificat SSL Google (clé publique) utilisé pour valider les demandes d'authentification de Google Apps (SAML SP).
9. Cliquez sur **Target Instances** et sélectionnez la ou les instances Citrix ADC sur lesquelles déployer cette configuration SSO Google Apps. Cliquez sur **Créer** pour créer la configuration et déployer la configuration sur les instances Citrix ADC sélectionnées.

> **Remarque**
>
> Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter des instances Citrix ADC récemment découvertes dans Citrix ADM à la liste des instances disponibles dans cette fenêtre.

Également,

> **Conseil**
>
> Citrix recommande qu'avant d'exécuter la configuration réelle, vous sélectionnez**Exécuter à sec**pour confirmer visuellement les objets de configuration créés sur les instances Citrix ADC cibles par le StyleBook.

SSO Office 365 StyleBook

February 1, 2024

Microsoft™ Office 365 est une suite d'applications de productivité et de collaboration basées sur le cloud fournies par Microsoft sur une base d'abonnement. Il inclut les applications serveur les plus populaires de Microsoft, telles qu'Exchange, SharePoint, Office et Skype for Business. L'authentification unique (SSO) permet aux utilisateurs d'accéder à toutes leurs applications cloud d'entreprise :

- Y compris les administrateurs qui se connectent à la console d'administration
- Connexion unique à tous les services Microsoft Office 365 à l'aide de leurs informations d'identification d'entreprise.

Le StyleBook SSO Office 365 vous permet d'activer l'authentification unique pour Microsoft Office 365 via des instances Citrix ADC. Vous pouvez désormais configurer l'authentification SAML avec Citrix ADC en tant que fournisseur d'identité SAML (IdP) et Microsoft Office 365 en tant que fournisseur de services SAML.

L'activation de l'authentification unique pour Microsoft Office 365 dans une instance Citrix ADC à l'aide de ce StyleBook implique les étapes suivantes :

1. Configuration du serveur virtuel d'authentification
2. Configuration d'une stratégie et d'un profil d'IDP SAML
3. Liaison de la stratégie et du profil au serveur virtuel d'authentification
4. Configuration d'un serveur d'authentification LDAP et d'une stratégie sur l'instance
5. Liez le serveur et la stratégie d'authentification LDAP à votre serveur virtuel d'authentification configuré sur l'instance.

Le tableau répertorie les versions logicielles minimales requises pour que cette intégration fonctionne correctement. Le processus d'intégration devrait également fonctionner avec des versions supérieures de celui-ci.
Produit	Version minimale requise
———	———————
Citrix ADC	11.0, licence avancée/premium

Les instructions suivantes supposent que vous avez déjà créé les entrées DNS externes et internes appropriées. Ces entrées sont essentielles pour acheminer les demandes d'authentification vers une adresse IP surveillée par Citrix ADC.

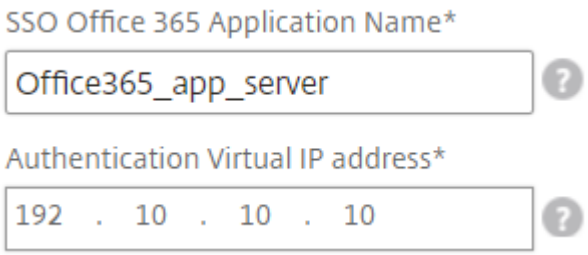
Les instructions suivantes vous aideront à implémenter le StyleBook SSO Office 365 dans votre réseau d'entreprise.

Pour déployer le SSO Microsoft Office 365 StyleBook

1. Dans Citrix Application Delivery Management (ADM), accédez à **Applications** > **StyleBooks** . La page **StyleBooks** affiche tous les StyleBooks disponibles pour votre utilisation dans Citrix ADM. Faites défiler l'écran vers le bas et trouvez **SSO Office 365 StyleBook**. Cliquez sur **Créer une configuration**.
2. Le StyleBook s'ouvre sous la forme d'une page d'interface utilisateur sur laquelle vous pouvez entrer les valeurs de tous les paramètres définis dans ce StyleBook.
3. Entrez des valeurs pour les paramètres suivants :

    a) **Nom de l'application**. Nom de la configuration SSO Microsoft Office 365 à déployer sur votre réseau.

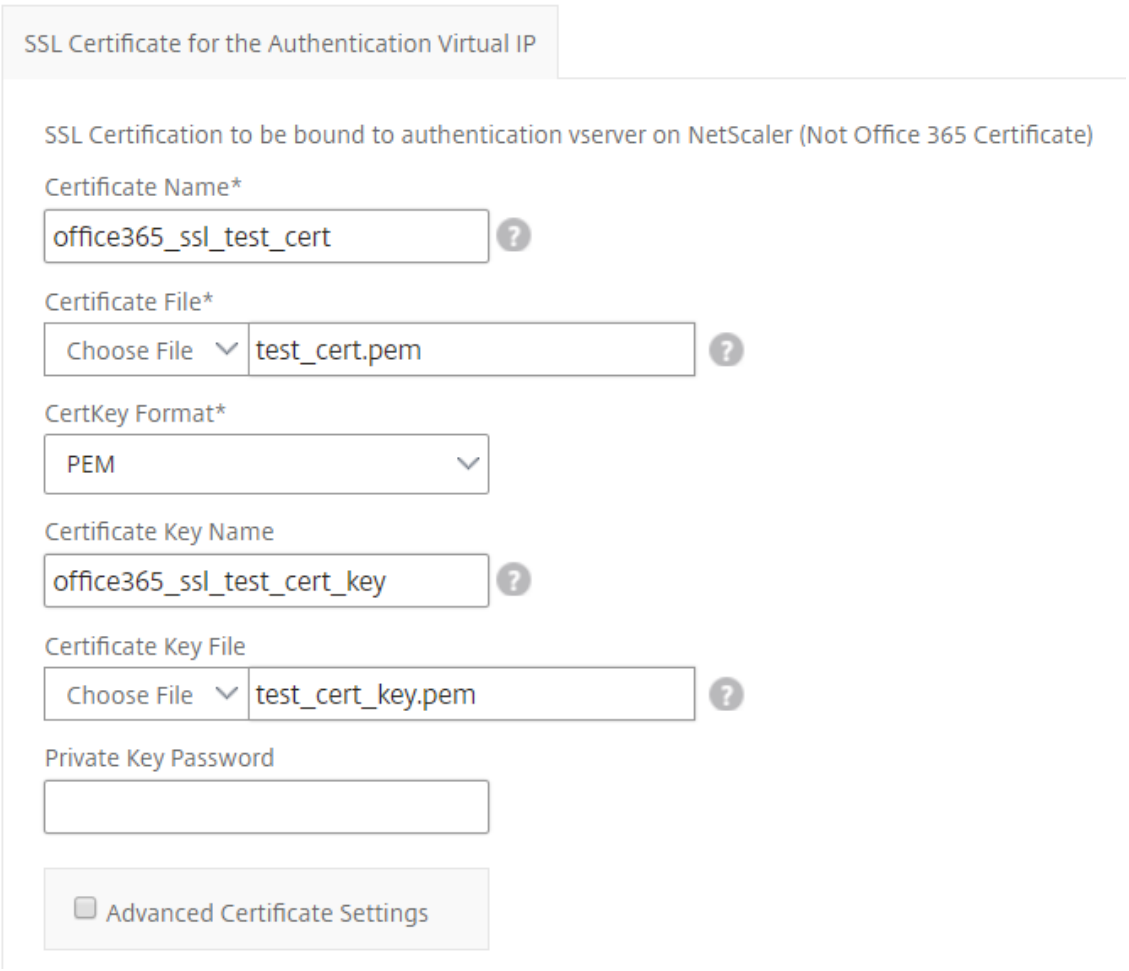
    b) **Authentification Adresse IP virtuelle**. Adresse IP virtuelle à utiliser par le serveur virtuel AAA auquel la stratégie IdP SAML de Microsoft Office 365 est liée.



4. Dans la section **Paramètres des certificats SSL**, entrez les noms du certificat SSL et la clé de certificat.

   > **Remarque**
   >
   > Il ne s'agit pas du certificat de fournisseur de services Office 365. Ce certificat SSL est lié au serveur d'authentification virtuel sur l'instance Citrix ADC.

5. Sélectionnez les fichiers correspondants dans votre dossier de stockage local. Vous pouvez également saisir le mot de passe de clé privée pour charger les clés privées chiffrées au format PEM.

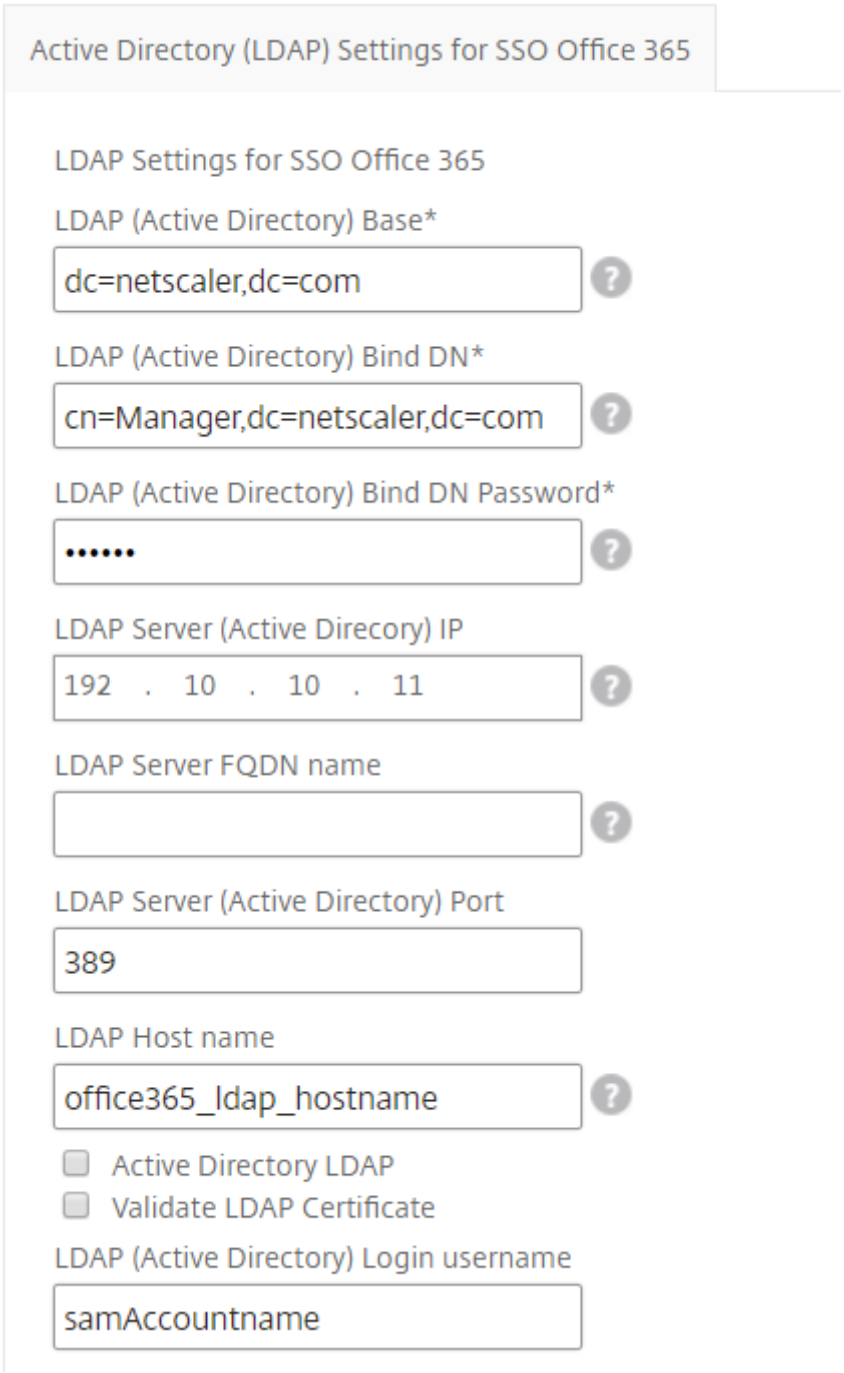


6. Vous pouvez également activer la case à cocher **Paramètres de certificat avancés**. Ici, vous pouvez entrer des détails tels que la période de notification d'expiration du certificat, activer ou désactiver le moniteur d'expiration du certificat.
7. Vous pouvez éventuellement cocher la case **Certificat de CA SSL pour l'adresse IP virtuelle d'authentification** si le certificat SSL nécessite l'installation d'un certificat public de l'autorité de certification sur Citrix ADC. Assurez-vous de choisir « Est un certificat CA » dans la section **Paramètres de certificat avancés** ci-dessus.
8. Dans la section **Paramètres LDAP pour SSO Office 365**, entrez les informations suivantes pour authentifier les utilisateurs Office 365. Pour permettre aux utilisateurs du domaine de se connecter à l'instance Citrix ADC à l'aide de leurs adresses e-mail professionnelles, configurez ce qui suit :

   - **Base LDAP (Active Directory)**. Entrez le nom de domaine de base du domaine dans lequel les comptes d'utilisateur résident dans Active Directory (AD) pour autoriser l'authentification. Par exemple, dc=netscaler, dc=com
   - **DN de liaison LDAP (Active Directory)**. Ajoutez un compte de domaine (à l'aide d'une adresse e-mail pour faciliter la configuration) qui dispose des droits de parcourir l'arborescence AD. Par exemple, CN=Manager, dc=netscaler, dc=com
   - **Mot de passe du nom unique de liaison LDAP (Active Directory)**. Entrez le mot de passe du compte de domaine pour l'authentification.
   - Quelques autres champs que vous devez saisir dans cette section sont les suivants :
     - Adresse IP du serveur LDAP auquel Citrix ADC se connecte pour authentifier les utilisateurs.
     - Nom de domaine complet du serveur LDAP.

       > **Remarque**
       >
       > Vous devez spécifier au moins l'une des deux options ci-dessus : l'adresse IP du serveur LDAP ou le nom de domaine complet.

     - Port serveur LDAP auquel Citrix ADC se connecte pour authentifier les utilisateurs (la valeur par défaut est 389). LDAPS utilise 636.
     - Nom d'hôte LDAP. Le nom d'hôte est utilisé pour valider le certificat LDAP si la validation est activée (elle est désactivée par défaut).
     - Attribut de nom de connexion LDAP. L'attribut par défaut utilisé pour extraire les noms de connexion est « sAMAccountName ».
     - Autres paramètres LDAP divers facultatifs.



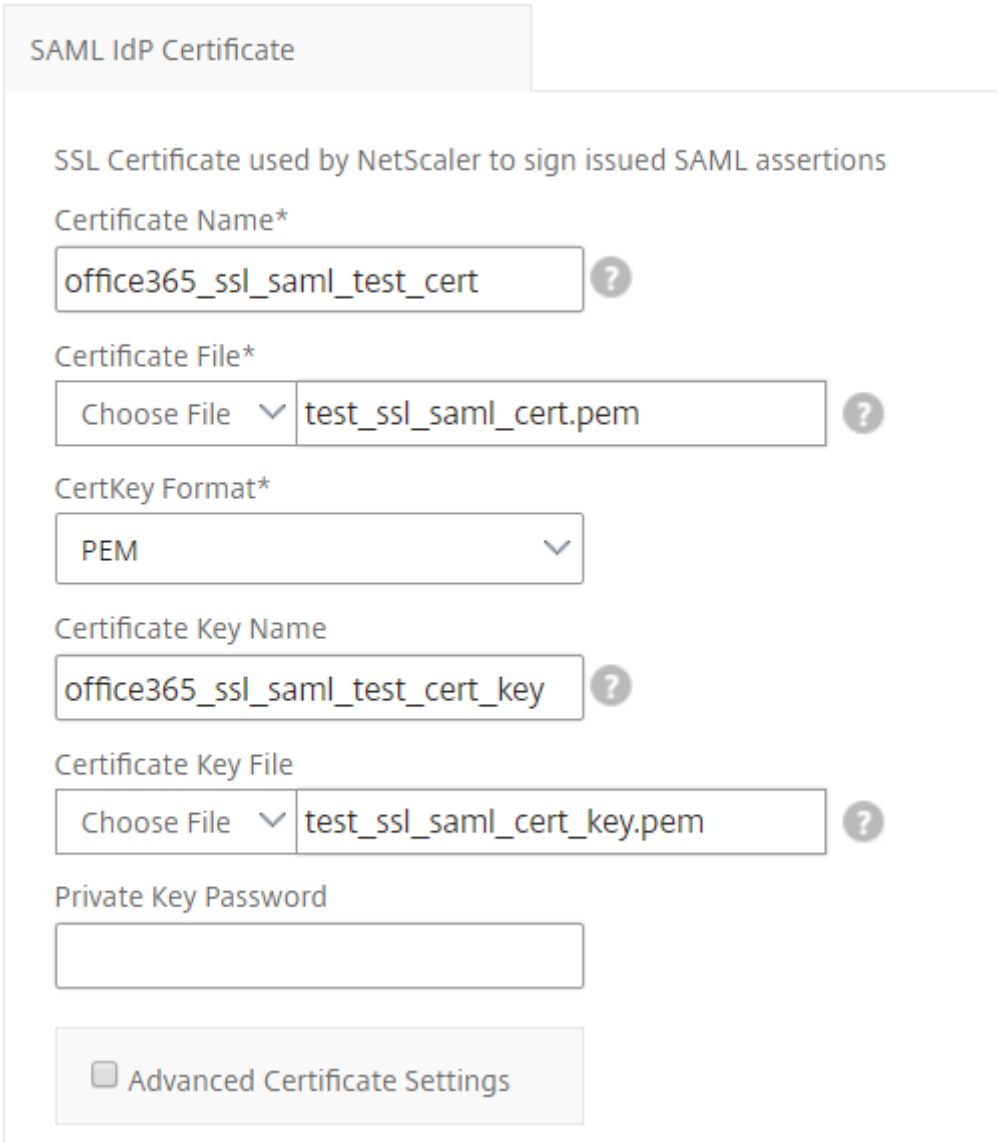
9. Dans la section **Certificat IdP SAML**, vous pouvez spécifier les détails des certificats SSL utilisés pour l'assertion SAML.

   - **Nom du certificat**. Entrez le nom du certificat SSL.
   - **Fichier de certificat**. Choisissez le fichier de certificat SSL dans le répertoire de votre système local.
   - **Format CertKey**. Sélectionnez le format du certificat et des fichiers de clé privée dans la

zone de liste déroulante. Les formats pris en charge sont les extensions de fichier .pem et .der.

- **Nom de la clé de certificat**. Entrez le nom de la clé privée du certificat.
- **Fichier clé du certificat**. Sélectionnez le fichier contenant la clé privée du certificat à partir de votre système local.
- Mot de**passe de clé privée**. Entrez le mot de passe qui protège votre fichier de clé privée.

Vous pouvez également activer la case à cocher **Paramètres de certificat avancés**. Ici, vous pouvez entrer des détails tels que la période de notification d'expiration du certificat, activer ou désactiver le moniteur d'expiration du certificat.

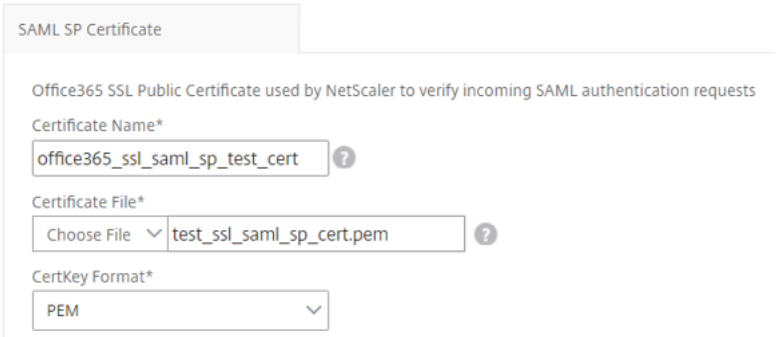


10. Le cas échéant, vous pouvez sélectionner un **certificat d'autorité de certification SAML IdP** si le certificat SAML IdP entré ci-dessus nécessite l'installation d'un certificat public d'autorité de

certification sur Citrix ADC. Assurez-vous de sélectionner **Est un certificat d'autorité de certification** dans la section **Paramètres de certificat avancés** ci-dessus.

11. Dans la section **Certificat SP SAML**, entrez les détails suivants pour le certificat public SSL Office 365. Ce certificat est utilisé par l'instance Citrix ADC pour vérifier les demandes d'authentification SAML entrantes.

    - **Nom du certificat**. Entrez le nom du certificat SSL.
    - **Fichier de certificat**. Choisissez le fichier de certificat SSL dans le répertoire de votre système local.
    - **Format CertKey**. Sélectionnez le format du certificat et des fichiers de clé privée dans la zone de liste déroulante. Les formats pris en charge sont les extensions de fichier .pem et .der.
    - Vous pouvez également activer la case à cocher **Paramètres de certificat avancés**. Ici, vous pouvez entrer des détails tels que la période de notification d'expiration du certificat, activer ou désactiver le moniteur d'expiration du certificat.



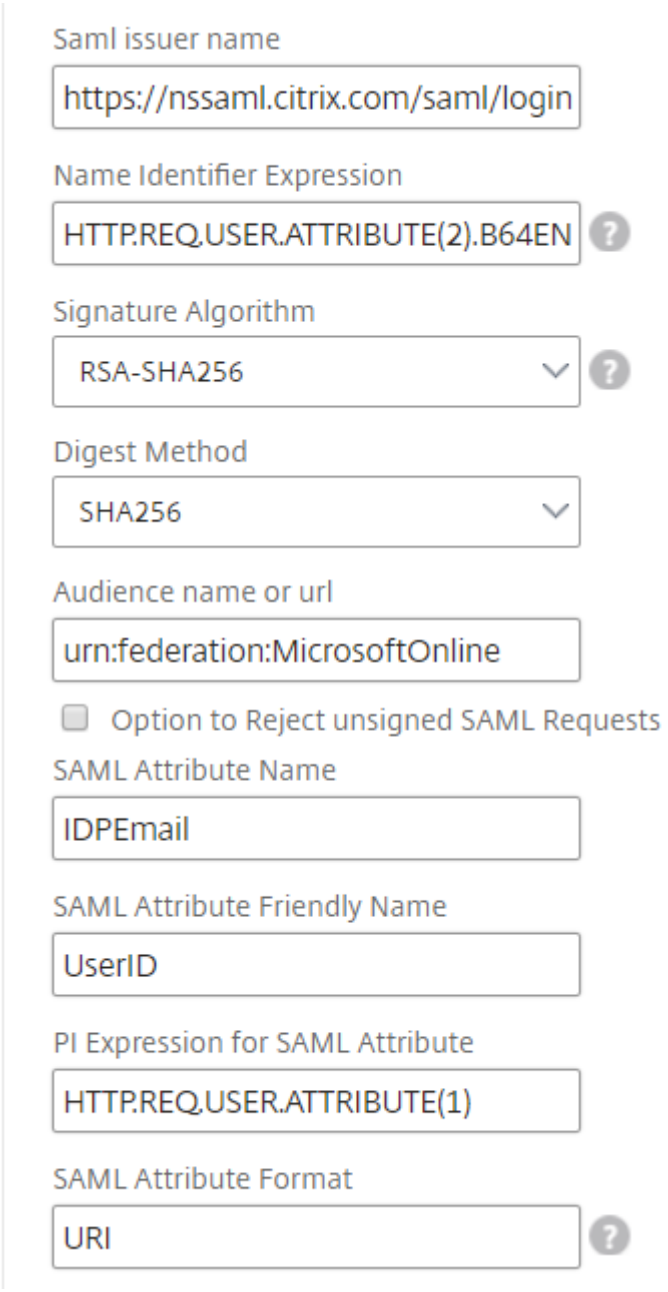
12. La section **Paramètres d'Idp SAML** vous permet de configurer votre instance Citrix ADC en tant que fournisseur d'identité SAML en créant le profil et la stratégie d'IDP SAML utilisés par le serveur virtuel AAA créé à l'étape 3.

    - **Nom de l'émetteur SAML**. Dans ce champ, saisissez le nom de domaine complet public de votre serveur virtuel d'authentification. Exemple : `https://<Citrix ADC Auth VIP>/saml/login`
    - **Expression d'identifiant de nom**. Tapez l'expression Citrix ADC qui est évaluée pour extraire le NameIdentifier SAML envoyé dans l'assertion SAML. Exemple : `"HTTP.REQ.USER.ATTRIBUTE(2).B64ENCODE"`
    - **Algorithme de signature** : sélectionnez l'algorithme pour vérifier/signer les requêtes/réponses SAML (la valeur par défaut est « RSA-SHA256 »).
    - **Méthode de digestion**. Sélectionnez la méthode de digestion du hachage pour les requêtes/réponses SAML (la valeur par défaut est « SHA256 »).

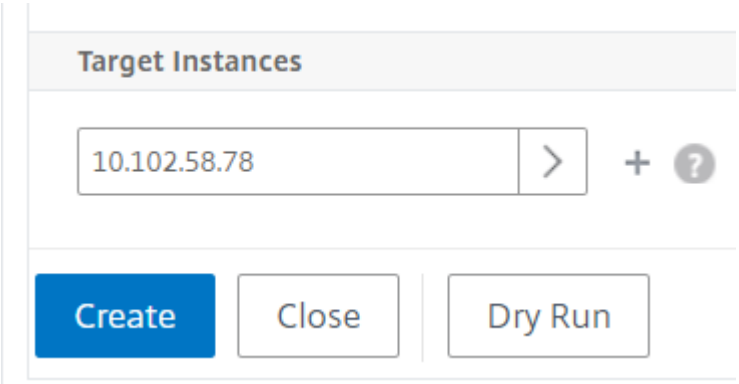
- **Nom du public**. Entrez le nom de l'entité ou l'URL qui représente le fournisseur de services (Microsoft Office 365).
- **ID du fournisseur de services (SP) SAML**. (facultatif) Le fournisseur d'identité Citrix ADC accepte les demandes d'authentification SAML provenant d'un nom d'émetteur qui correspond à cet identifiant.
- **URL du service client Assertion**. Entrez l'URL du fournisseur de services à laquelle le fournisseur d'identité Citrix ADC doit envoyer les assertions SAML après une authentification utilisateur réussie. L'URL du service client d'assertion peut être initiée sur le site serveur du fournisseur d'identité ou sur le site du fournisseur de services.
- Vous pouvez saisir d'autres champs facultatifs dans cette section. Par exemple, vous pouvez définir les options suivantes :
  - **Nom de l'attribut SAML**. Nom de l'attribut utilisateur envoyé dans l'assertion SAML.
  - **Nom convivial de l'attribut SAML**. Nom convivial de l'attribut utilisateur envoyé dans l'assertion SAML.
  - **Expression IP pour l'attribut SAML**. Par défaut, l'expression de stratégie (PI) Citrix ADC suivante est utilisée : HTTP.REQ.USER.ATTRIBUTE (1). Ce champ spécifie le premier attribut utilisateur envoyé par le serveur LDAP (mail) en tant qu'attribut d'authentification SAML.
  - Sélectionnez le format de l'attribut utilisateur.

  Ces valeurs sont incluses dans l'assertion SAML émise.

  > **Conseil**
  >
  > Citrix vous recommande de conserver les paramètres par défaut, car ces paramètres ont été testés pour fonctionner avec les applications Microsoft Office 365.



13. Cliquez sur **Instances cibles** et sélectionnez la ou les instances Citrix ADC sur lesquelles déployer cette configuration Microsoft Office 365 SSO. Cliquez sur **Créer** pour créer la configuration et déployer la configuration sur les instances Citrix ADC sélectionnées.



Conseil

Citrix recommande qu'avant d'exécuter la configuration réelle, vous sélectionnez**Exécuter à sec**pour afficher les objets de configuration créés sur les instances Citrix ADC cibles par le StyleBook.

StyleBook Microsoft Skype for Business

February 1, 2024

L'application Skype for Business 2015 s'appuie sur plusieurs composants externes pour fonctionner. Le réseau Skype for Business comprend divers systèmes, tels que les serveurs et leurs systèmes d'exploitation, les bases de données, les systèmes d'authentification et d'autorisation, les systèmes et infrastructures de réseau et les systèmes PBX téléphoniques. Skype for Business Server 2015 est disponible en deux versions, Standard Edition et Enterprise Edition. La principale différence réside dans la prise en charge des fonctionnalités de haute disponibilité qui ne sont incluses que dans l'édition Enterprise. Pour mettre en œuvre la haute disponibilité, plusieurs serveurs frontaux doivent être déployés dans un pool et les serveurs SQL doivent être mis en miroir.

Un déploiement Enterprise Edition permet de créer plusieurs serveurs avec des rôles différents.

Composants principaux

Les principaux composants de l'application Skype for Business 2015 sont les suivants :

- Serveurs frontaux
- Serveurs Edge
- Serveurs Director
- Serveurs de base de données (SQL)

Serveurs frontaux

Dans l'application Skype for Business, le serveur frontal est le serveur principal de votre réseau. Il fournit des liens et des services pour l'authentification des utilisateurs, l'enregistrement, la présence, le carnet d'adresses, les conférences audiovisuelles, le partage d'applications, la messagerie instantanée et les conférences Web. Si vous déployez Skype for Business 2015 édition Entreprise, la topologie consiste généralement en au moins deux serveurs frontaux équilibrés de charge dans un pool front-end avec un serveur de base de données qui héberge l'instance SQL Server contenant la base de données Skype for Business.

Serveurs Edge

Le déploiement de serveurs Edge pour Skype for Business est nécessaire si les utilisateurs externes qui ne sont pas connectés au réseau interne de votre organisation doivent pouvoir interagir avec les utilisateurs internes. Ces utilisateurs externes peuvent être des utilisateurs distants authentifiés et anonymes, des partenaires fédérés ou d'autres clients mobiles.

Il existe quatre types de rôles dans le serveur Skype For Business Edge :

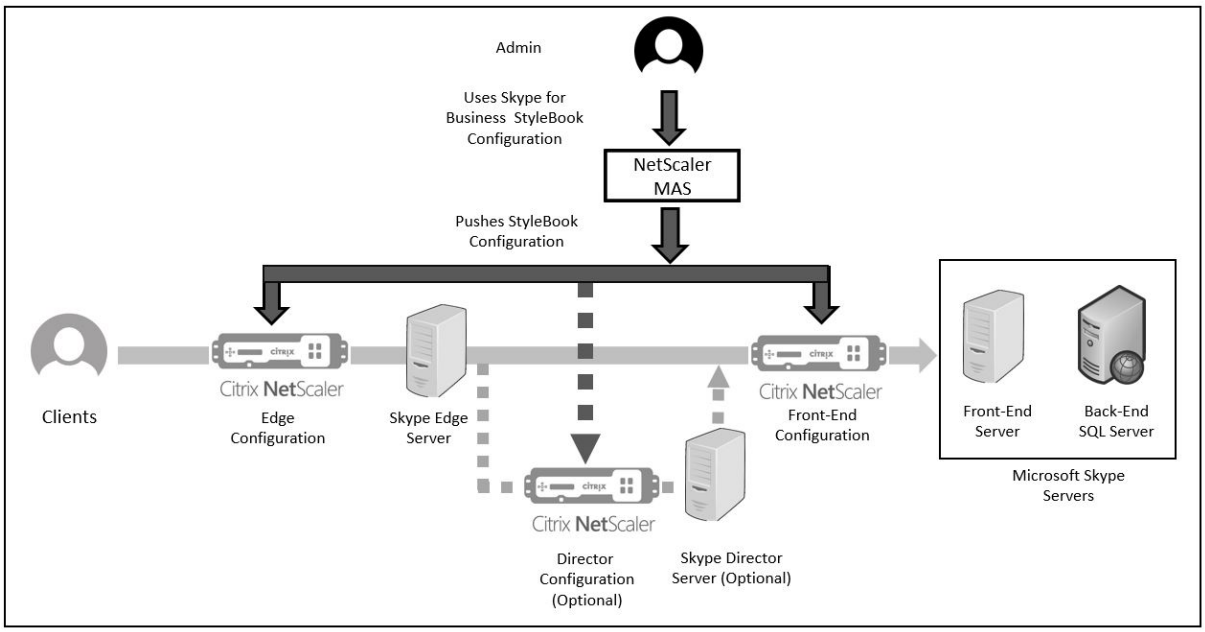
- Access Edge, qui gère le trafic SIP et authentifie les connexions externes, permet la connexion à distance et permet la connexion de fédération
- Web Conferencing, qui gère les paquets de conférence de données et permet aux utilisateurs externes d'accéder à Skype for Business
- A/V Conferencing, qui gère les paquets de conférence audio/vidéo et étend l'audio et la vidéo, le partage d'applications et le transfert de fichiers aux utilisateurs externes
- XMPP Proxy, qui gère les paquets XMPP, et permet aux serveurs ou clients basés sur XMPP de se connecter à Skype for Business.

Serveurs Director

La fonction principale du serveur Director dans Skype for Business 2015 est d'authentifier les points de terminaison et de « diriger » les utilisateurs vers le pool qui contient leur compte. Dans Skype for Business 2015, bien que le Director soit un rôle entièrement dédié et spécifique sur un serveur autonome, il s'agit d'un serveur facultatif. Cela facilite la sécurité en facilitant le déploiement ou la suppression des configurations.

Les directeurs sont particulièrement utiles lorsqu'il existe plusieurs pools, car ils fournissent un point de contact unique pour authentifier les points de terminaison. De plus, pour les utilisateurs distants, un Director sert de saut supplémentaire entre le pool Edge et le pool Front-End, ajoutant ainsi une couche de protection supplémentaire contre les attaques.

La figure suivante représente schématiquement le déploiement des serveurs Skype dans le réseau :



Configuration d'instances Citrix ADC dans une entreprise

Le tableau suivant répertorie les adresses IP utilisées dans l'exemple de configuration inclus dans les instructions ci-dessous :

Serveurs Skype for Business	Adresse IP virtuelle	Adresses IP du serveur	Instance Citrix ADC
Serveurs Edge	VIP externe - 192.20.20.20 VIP interne - 10.10.10.20	192.20.20.21 ; 192.20.20.22 10.10.10.21; 10.10.10.22	10.102.29.141
Serveurs frontaux	10.10.10.10	10.10.10.11 ; 10.10.10.12	10.102.29.60
Serveur Director	10.10.10.30	10.10.10.31; 10.10.10.32	10.102.29.93

Pour configurer des serveurs frontaux

1. Dans Citrix Application Delivery Management (ADM), accédez à **Applications** > **Configuration**, puis cliquez sur **Create New**. La page **Choisir un StyleBook** affiche tous les StyleBooks disponibles pour votre utilisation dans Citrix ADM. Faites défiler l'écran vers le bas et sélectionnez **Microsoft Skype for Business 2015 StyleBook**. Le StyleBook s'ouvre en tant que page d'

interface utilisateur sur laquelle vous pouvez entrer les valeurs de tous les paramètres définis dans ce StyleBook.

2. Dans la section **Serveur Edge**, entrez les adresses IP virtuelles (VIP) et les adresses IP de tous les serveurs Edge du réseau suivantes.

   a) Adresse VIP externe et adresses IP des serveurs Edge qui seront utilisés pour Access Edge, les conférences Web Edge et A/V Edge.
   b) Adresse VIP interne et adresses IP des serveurs Edge qui seront connectés au réseau interne.
   c) Deux serveurs Edge externes et deux serveurs internes sur votre réseau.

3. Dans la section **Serveur frontal**, entrez l'adresse IP du serveur frontal virtuel (VIP) qui doit être créé pour les serveurs front-end Skype for Business. Entrez également les adresses IP de tous les serveurs d'interface Skype for Business du réseau.
4. Dans la section **Director Server**, entrez l'adresse IP virtuelle (VIP) des serveurs Director à créer pour l'application Skype for Business. Entrez également les adresses IP de tous les serveurs Skype for Business Director du réseau. Créez au moins deux serveurs Director pour une haute disponibilité.
5. La section **Paramètres avancés** répertorie tous les ports par défaut configurés sur les instances Citrix ADC pour les trois serveurs Skype.

Le tableau suivant fournit une liste de tous les ports et protocoles par défaut :

Label	Port	Protocole	Description
Port HTTP	80	HTTP	Utilisé pour la communication entre les serveurs frontaux et les noms de domaine complets de la ferme Web lorsque le protocole HTTPS n'est pas utilisé.
Port HTTPS	443	HTTPS	Utilisé pour la communication entre les serveurs frontaux et les noms de domaine complets de la batterie Web.

Label	Port	Protocole	Description
Port interne AutoDiscover	4443	HTTPS	Communications inter-pool HTTPS (à partir du proxy inverse) et HTTPS Front-end pour la connexion AutoDiscover.
Port RPC	135	DCOM et appel de procédure à distance (RPC)	Utilisé pour les opérations basées sur DCOM telles que le déplacement d'utilisateurs, la synchronisation des réplicateurs d'utilisateurs et la synchronisation du carnet d'adresses.
Port SIP	5061	TCP (TLS)	Utilisé par les serveurs frontaux pour toutes les communications SIP internes.
Port de focus SIP	444	HTTPS, TCP	Utilisé pour la communication HTTPS entre le Focus (le composant qui gère l'état de la conférence Skype) et les serveurs individuels.
Port de groupe SIP	5071	TCP	Utilisé pour les demandes SIP entrantes pour l'application du groupe de réponse.
Port de partage d'applications SIP	5065	TCP	Utilisé pour les demandes d'écoute SIP entrantes pour le partage d'applications.

Label	Port	Protocole	Description
Port auxiliaire SIP	5072	TCP	Utilisé pour les demandes SIP entrantes pour le préposé (c'est-à-dire pour la conférence d'accès à distance).
Port d'annonce SIP Conf	5073	TCP	Utilisé pour les demandes SIP entrantes pour le service d'annonce de conférence sur le serveur Skype for Business (c'est-à-dire pour les téléconférences).
Port SIP CallPark	5075	TCP	Utilisé pour les requêtes SIP entrantes pour l'application CallPark.
Port d'admission d'appels SIP	448	TCP	Utilisé pour le contrôle d'admission des appels par le service de stratégie de bande passante du serveur Skype for Business.
Port TURN d'admission d'appel SIP	5080	TCP	Utilisé pour le contrôle d'admission des appels par le service de stratégie de bande passante pour le trafic Audio/Video Edge TURN.
Port de test audio SIP	5076	TCP	Utilisé pour les demandes SIP entrantes pour le service de test audio.

Label	Port	Protocole	Description
Port externe HTTPS	443	HTTPS	Utilisé pour les ports externes pour la communication SIP/TLS pour l'accès utilisateur à distance, l'accès à des conférences Web internes, et les communications multimédia STUN/TCP entrantes et sortantes pour accéder aux médias internes et aux sessions A/V.
Port interne HTTPS	443	HTTPS	Utilisé pour les ports internes pour la communication SIP/TLS pour l'accès utilisateur à distance, l'accès à des conférences Web internes, et les communications multimédia STUN/TCP entrantes et sortantes pour accéder aux médias internes et aux sessions A/V.
Port d'accès distant externe SIP	5061	TCP	Utilisé pour les ports externes pour la communication SIP/MTLS pour l'accès utilisateur à distance ou la fédération.

Label	Port	Protocole	Description
Port d'accès à distance interne SIP	5061	TCP	Utilisé pour les ports internes pour la communication SIP/MTLS pour l'accès utilisateur à distance ou la fédération.
Port UDP STUN externe SIP	3478	UDP	Utilisé pour les ports externes pour les communications multimédia entrantes et sortantes STUN/UDP.
Port UDP STUN interne SIP	3478	UDP	Utilisé pour les ports internes pour les communications multimédia entrantes et sortantes STUN/UDP.
Port de messagerie instantanée interne SIP	5062		Utilisé pour les ports internes pour l'authentification SIP/MTLS des communications de messagerie instantanée sortant via le pare-feu interne.
Port HTTP	80	TCP	Utilisé pour la communication initiale entre les directeurs et les FQDN de la ferme Web.
Port HTTPS	443	HTTPS	Utilisé pour la communication entre les directeurs et les noms de domaine complets de la batterie de serveurs Web.

Label	Port	Protocole	Description
Port interne AutoDiscover	4443	HTTPS	Utilisé pour les communications entre pools HTTPS (à partir de Reverse Proxy) et HTTPS Director pour la connexion AutoDiscover.
Port interne SIP	5061	TCP	Utilisé pour les communications internes entre les serveurs et pour les connexions client.

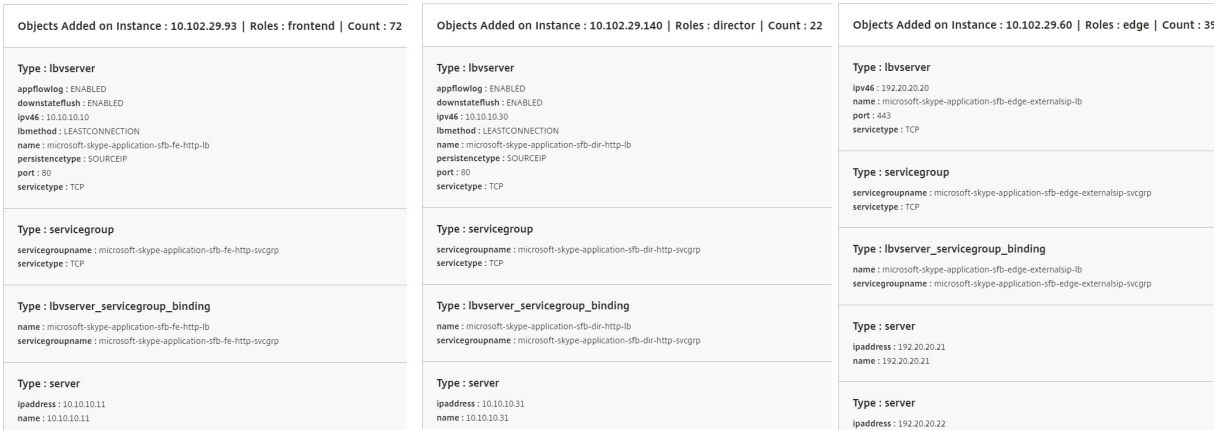
6. Dans la section **Instances cibles**, sélectionnez les trois instances Citrix ADC différentes sur lesquelles déployer les trois serveurs Skype for Business.

> **Remarque**
>
> Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter des instances Citrix ADC récemment découvertes dans Citrix ADM à la liste des instances disponibles dans cette fenêtre.

7.Cliquez sur**Créer** pour créer la configuration sur les instances Citrix ADC sélectionnées.

> **Conseil**
>
> Citrix vous recommande de sélectionner**Dry Run** pour vérifier les objets de configuration qui doivent être créés sur l'instance cible avant d'exécuter la configuration réelle sur l'instance.
>
> Lorsque la configuration est créée avec succès, le StyleBook crée 25 serveurs virtuels d'équilibrage de charge. En d'autres termes, pour chaque port, un serveur virtuel d'équilibrage de charge est défini avec un groupe de services, et le groupe de services est lié au serveur virtuel d'équilibrage de charge. La configuration ajoute également les serveurs frontaux en tant que membres du groupe de services et les lie au groupe de services. Le nombre de membres du groupe de services créés est égal au nombre de serveurs frontaux créés.

La figure suivante montre les objets créés sur chaque serveur :



StyleBook Microsoft Exchange

February 1, 2024

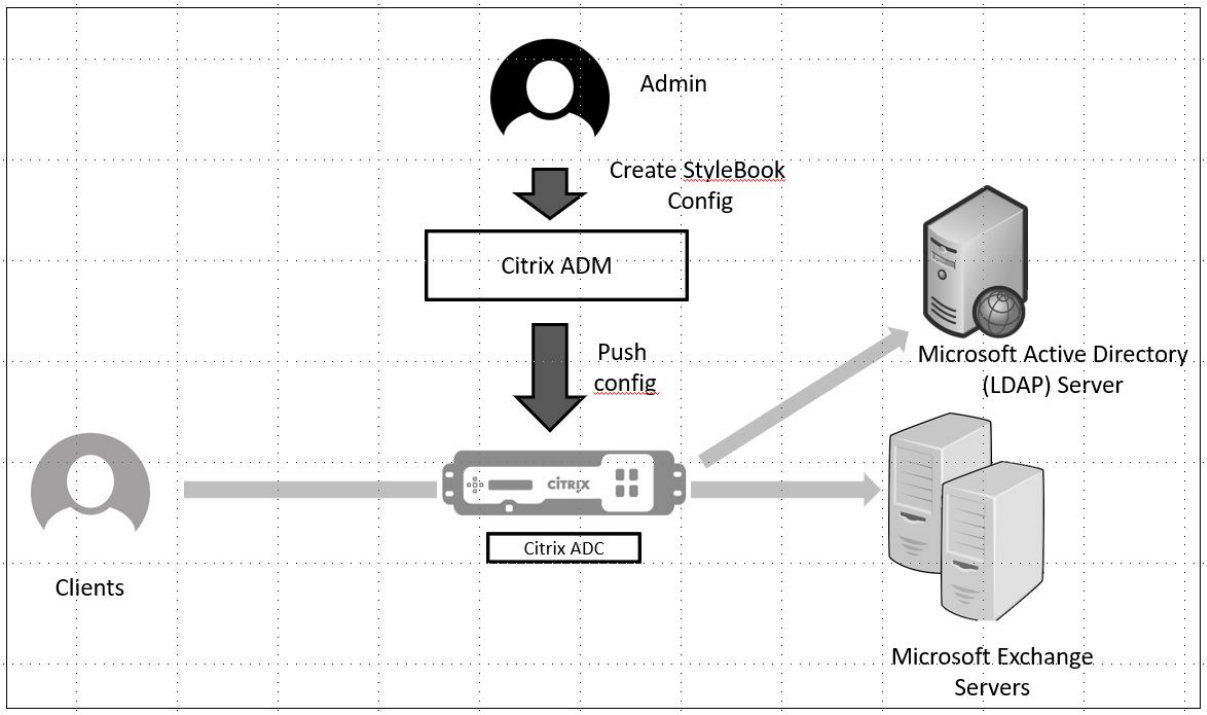
Vous pouvez utiliser le StyleBook de Microsoft Exchange 2016 pour déployer une configuration Citrix ADC qui optimise et sécurise une application d'entreprise Microsoft Exchange 2016 sur votre réseau. Microsoft Exchange 2016 est une application d'entreprise clé pour fournir des services de messagerie, de gestion des informations personnelles et de messagerie à vos employés et aux autres parties prenantes.

Fonctionnalités de Citrix ADC configurées à l'aide de Microsoft Exchange StyleBook

Le Microsoft Exchange 2016 StyleBook active et configure les fonctionnalités Citrix ADC suivantes pour les serveurs Microsoft Exchange 2016 :

- Équilibrage de charge : équilibrage de charge de base qui permet l'équilibrage de charge de plusieurs serveurs Exchange
- Commutation de contenu : commutation de contenu qui permet un accès IP unique et la redirection des requêtes vers les serveurs virtuels d'équilibrage de charge appropriés
- Réécriture : redirige les utilisateurs vers des pages sécurisées
- Déchargement SSL : décharge le traitement SSL vers Citrix ADC, réduisant ainsi la charge sur le serveur Exchange

La figure suivante représente schématiquement le déploiement des serveurs Exchange dans le réseau :



Conditions préalables

- Pour l'authentification basée sur des certificats, tous les hôtes adressables faisant partie de la configuration réseau doivent avoir des noms de domaine résolvables et pas uniquement des adresses IP.
- Assurez-vous que les ports SIP sont accessibles sur le serveur Microsoft Exchange 2016.

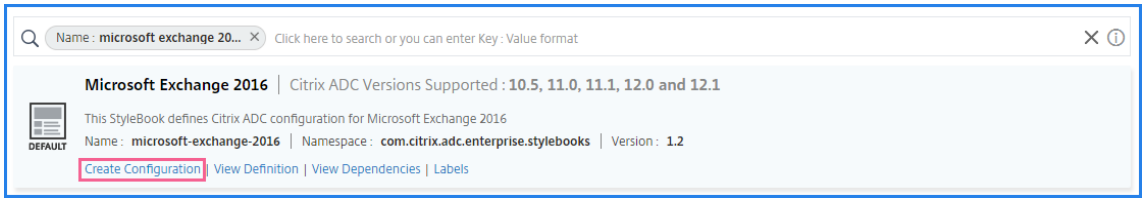
Configuration du StyleBook de Microsoft Exchange

Configurez le Microsoft Exchange StyleBook dans votre entreprise pour déployer la configuration Citrix ADC.

Pour configurer l'application Microsoft Exchange

1. **Dans Citrix ADM, accédez à**Applications**> StyleBooks.**
2. Recherchez **Microsoft Exchange 2016 StyleBook** et cliquez sur **Créer une configuration**.

   Le StyleBook apparaît sous la forme d'un formulaire d'interface utilisateur sur lequel vous pouvez saisir les valeurs de tous les paramètres définis dans ce StyleBook.



3. Entrez les détails des paramètres suivants :

   - **Nom de l'application Exchange** : nom de l'application Microsoft Exchange dans votre réseau
   - **Exchange VIP** : adresse IP virtuelle sur Citrix ADC qui reçoit les demandes des clients pour l'application Microsoft Exchange
   - **IP Exchange Server** : adresses IP de tous les serveurs Exchange du réseau.

     Si vous souhaitez ajouter d'autres adresses IP, cliquez sur l'icône plus (**+**). Habituellement, deux serveurs Exchange sont configurés dans le réseau.

4. Dans la section **Certificats Exchange**, téléchargez les certificats Exchange vers Citrix ADM. Entrez les noms du certificat et des fichiers clés et téléchargez-les depuis le stockage local. Vous pouvez également fournir un mot de passe de clé privée pour crypter le fichier clé.

   > **Remarque**
   >
   > Assurez-vous que les fichiers de certificat sont au format « .pem » ou « .der ». Citrix ADM rejette les fichiers d'autres formats.

   Si vous souhaitez spécifier les détails d'expiration du certificat ou tout autre paramètre avancé, sélectionnez **Paramètres de certificat avancés**.

5. Dans la section de **configuration de l'authentification Active Directory Exchange**, configurez les paramètres AD en entrant les données.

   - **Active Directory Authentication VIP** : adresse IP virtuelle utilisée pour créer et configurer le serveur virtuel AD (LDAP) sur une appliance Citrix ADC.
   - **Active Directory Server IP**- Adresse IP de votre Controller de domaine Active Directory.
   - **Chaîne de base Active Directory : chaîne**de base LDAP dans Active Directory. Par exemple, CN = Utilisateurs, DC=CTXNSSFB, DC=COM.
   - **Nom distinctif (DN) Active Directory LDAP** Bind : le nom distinctif (DN) LDAP Bind est utilisé pour lier cet objet au serveur LDAP (AD). Par exemple « CN = Administrateur, CN = Utilisateurs, dc=acme, dc=com »
   - Mot de**passe LDAP Bind Distinguished Name (DN) Active Directory** : le nom distinctif LDAP Bind (DN) est le mot de passe pour l'authentification AD

- Attribut de**nom d'utilisateur Active Directory : attribut** AD pour le nom d'utilisateur. Le Citrix ADC utilise l'attribut LDAP pour interroger les serveurs Active Directory externes. Par exemple, « SAMAccountName »
- **Nom d'attribut du groupe Active Directory** : noms d'attributs du groupe LDAP configurés sur le serveur LDAP. Par exemple, « MemberOf » pour l'attribut de groupe dans LDAP.
- **Nom de sous-attribut Active Directory** : noms de sous-attribut LDAP configurés sur le serveur LDAP. Par exemple, « cn » pour le sous-attribut dans LDAP.
- **Domaine d'authentification Active Directory** : nom de domaine AD/LDAP utilisé pour l'authentification. Par exemple, ctxnssfb.com.

6. Dans la section**Instances cibles**, sélectionnez l'instance Citrix ADC sur laquelle déployer cette configuration Exchange.

   > **Remarque**
   >
   > Si vous souhaitez afficher les instances Citrix ADC récemment découvertes, cliquez sur l'icône d'actualisation.

7. Cliquez sur **Créer** pour créer le fichier de configuration et exécuter la configuration sur l'instance Citrix ADC sélectionnée.

   Citrix vous recommande de sélectionner d'abord**Exécuter à sec**pour vérifier les objets de configuration créés sur l'instance cible avant d'exécuter la configuration réelle sur l'instance.

Lorsque la configuration a été créée avec succès, StyleBook a créé un serveur virtuel de commutation de contenu, cinq serveurs virtuels d'équilibrage de charge et une stratégie LDAP liée à un serveur virtuel d'authentification LDAP. En outre, les groupes de services correspondants sont créés et liés aux serveurs virtuels d'équilibrage de charge.

Microsoft SharePoint StyleBook

February 1, 2024

Microsoft SharePoint 2016 est une application d'entreprise clé qui fournit principalement un système de gestion et de stockage de documents, hautement configurable et pris en charge par tous les principaux navigateurs.

Vous pouvez utiliser le StyleBook de Microsoft SharePoint 2016 pour déployer une configuration Citrix ADC qui optimise et sécurise l'application d'entreprise Microsoft SharePoint 2016 sur votre réseau.

Conditions préalables

- Microsoft SharePoint 2016
- Citrix ADM, version 12.0 et versions ultérieures
- Citrix ADC, version 10.5 et ultérieure

Fonctionnalités de Citrix ADC configurées par le StyleBook de Microsoft SharePoint 2016

Vous pouvez utiliser le StyleBook de Microsoft SharePoint 2016 pour activer et configurer les fonctionnalités Citrix ADC suivantes pour Microsoft SharePoint 2016 :

- Équilibrage de charge
- Commutation de contenu
- Répondeur
- Réécriture
- Compression
- Mise en cache intégrée

Équilibrage de charge

L'équilibrage de charge Citrix ADC répartit uniformément les demandes vers les serveurs SharePoint principaux. La surveillance intelligente des serveurs dorsaux empêche l'envoi de demandes vers des serveurs défectueux.

Le StyleBook de SharePoint configure 12 serveurs virtuels d'équilibrage de charge, chacun dédié aux demandes d'équilibrage de charge pour un certain type de contenu, tel que des documents, des images, des fichiers audio, vidéo et d'autres types de fichiers.

Le SharePoint StyleBook prend désormais en charge le mode SSL de l'application SharePoint en configurant des serveurs virtuels LB basés sur SSL. Assurez-vous que SSL est sélectionné comme protocole frontal. Notez que le port virtuel est défini sur 443 par défaut. Vous pouvez également sélectionner SSL pour lier des groupes de services (serveurs d'applications SharePoint) aux serveurs virtuels d'équilibrage de charge cibles. Notez que le protocole principal est défini par défaut sur HTTP.

Commutation de contenu

La fonctionnalité de commutation de contenu est utilisée pour distribuer les demandes des clients sur plusieurs serveurs virtuels d'équilibrage de charge sur la base de types spécifiques de contenu SharePoint demandé (par exemple, des documents, des images et des fichiers audio ou vidéo). Le module de commutation de contenu dirige le trafic entrant vers un serveur virtuel d'équilibrage de

charge optimal capable de traiter ce type de contenu. Vous pouvez donc appliquer différentes stratégies d'optimisation à différents types de trafic. Par exemple, vous souhaiterez peut-être utiliser des stratégies de compression ou de mise en cache différentes pour les vidéos et pour les documents texte.

Répondeur

La fonctionnalité de répondeur d'une instance Citrix ADC peut être utilisée pour rediriger facilement les utilisateurs du protocole HTTP vers le protocole HTTPS. Le répondeur peut également être configuré pour fournir des pages d'erreur personnalisées. La stratégie Responder détermine les demandes (trafic) sur lesquelles une action doit être entreprise et lie chaque stratégie à un serveur virtuel d'équilibrage de charge. Le SharePoint StyleBook inclut une configuration qui redirige les utilisateurs des URL HTTP vers les URL HTTPS.

Réécrire

Le module de réécriture est utilisé pour modifier les en-têtes de demande/réponse, les URL ou le contenu à la volée. Ce module fonctionne en ligne avec le traitement du trafic et peut donc modifier le flux de trafic en fonction de cas d'utilisation particuliers. Par exemple, la réécriture peut donner accès au contenu demandé sans révéler de détails inutiles sur le serveur du site Web.

Dans le StyleBook de SharePoint, la fonction de réécriture est utilisée pour supprimer les en-têtes inutiles des demandes des utilisateurs.

Compression

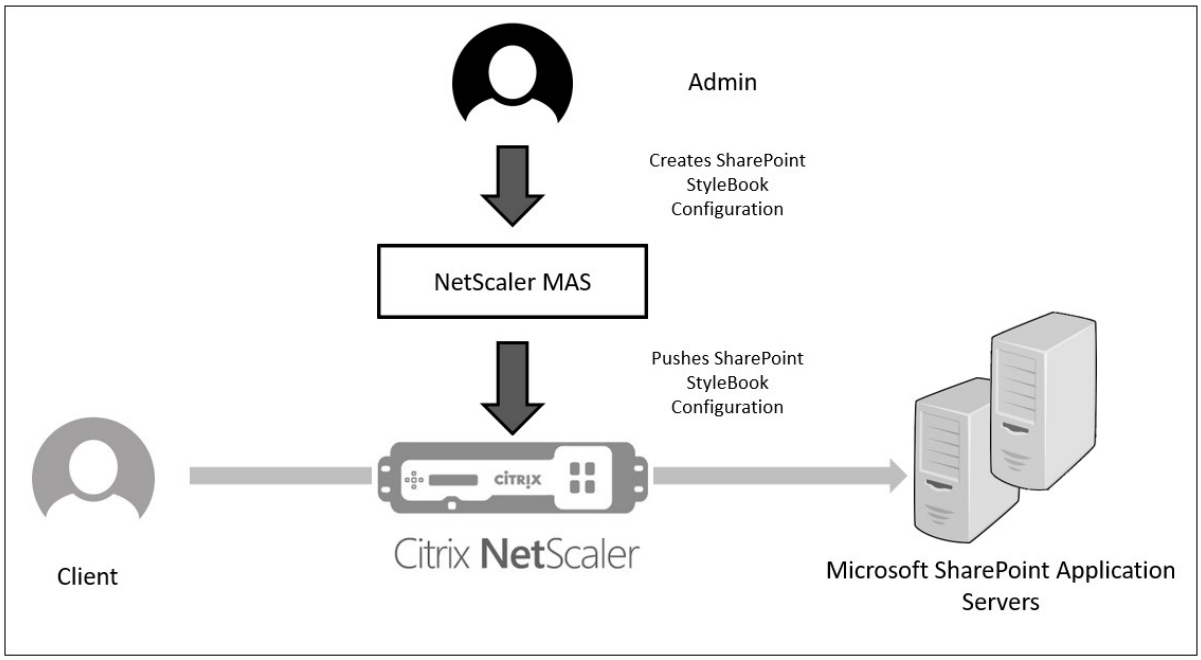
Le moteur de compression Citrix ADC identifie et compresse le contenu compressible. Ce processus améliore le temps de transmission des données et réduit les besoins en bande passante réseau des clients, tout en économisant des cycles de processeur sur les serveurs de contenu SharePoint. Une instance Citrix ADC peut compresser à la fois des données statiques et des données générées dynamiquement. Il applique l'algorithme de compression GZIP ou DEFLATE pour supprimer les informations superflues et répétitives des réponses du serveur et représenter les informations d'origine dans un format plus compact et efficace. La capacité du navigateur client à décompresser les données dépend de l'algorithme ou des algorithmes qu'il prend en charge : GZIP, DEFLATE ou les deux.

Une instance Citrix ADC est configurée pour compresser le texte dans des documents HTML, XML, texte brut, feuille de style en cascade (CSS) et Microsoft Office, mais ne compresse pas les images au format GIF ou JPG. Les principaux avantages du trafic compressé incluent la réduction des coûts de bande passante, la réduction de la latence du WAN et de meilleures performances des serveurs

Mise en cache intégrée

Le cache en mémoire Citrix ADC peut stocker des objets SharePoint afin de fournir rapidement le contenu fréquemment demandé aux utilisateurs. Le contenu mis en cache inclut les documents téléchargés et les fichiers audio, vidéo et image.

La figure suivante représente schématiquement le déploiement de serveurs SharePoint dans un réseau frontal par une instance Citrix ADC sur laquelle Citrix ADM est utilisé pour déployer une configuration SharePoint StyleBook.



Déploiement de configurations SharePoint StyleBook

La tâche suivante vous aidera à déployer le StyleBook Microsoft SharePoint 2016 sur votre réseau professionnel.

Pour déployer Microsoft SharePoint 2016 StyleBook :

1. Dans Citrix ADM, accédez à **Applications** > **Administration** > **Configuration**, puis cliquez sur **Créer un**nouveau.

   La page **Choisir un StyleBook** affiche tous les StyleBooks disponibles pour votre utilisation dans Citrix ADM.

2. Faites défiler l'écran vers le bas et sélectionnez **Microsoft SharePoint 2016 StyleBook**.

> **Remarque**
>
> Dans Citrix ADM, accédez à **Applications** > **Configurations** > **StyleBooks**. Faites défiler vers le bas pour trouver le **StyleBook de Microsoft SharePoint 2016**, puis cliquez sur **Créer une configuration**.

Le StyleBook s'ouvre en tant que formulaire d'interface utilisateur sur lequel vous pouvez entrer les valeurs de tous les paramètres définis dans ce StyleBook.

Entrez des valeurs pour les paramètres suivants :

a) **Nom de l'application SharePoint**. Nom de la configuration SharePoint à déployer sur votre réseau.

b) Adresse**IP virtuelle SharePoint**. Adresse IP virtuelle à laquelle l'instance Citrix ADC reçoit les demandes des clients pour l'application Microsoft SharePoint.

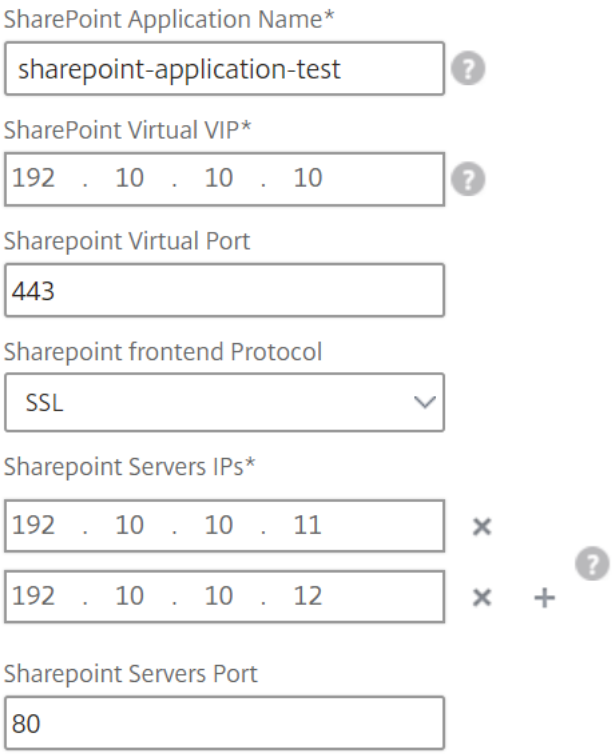
c) **Port virtuel SharePoint**. Le port TCP à utiliser par les utilisateurs pour accéder à l'application SharePoint

d) **Protocole frontend SharePoint**. Sélectionnez le protocole d'interface SharePoint dans la liste déroulante. Les options disponibles sont HTTP ou SSL.

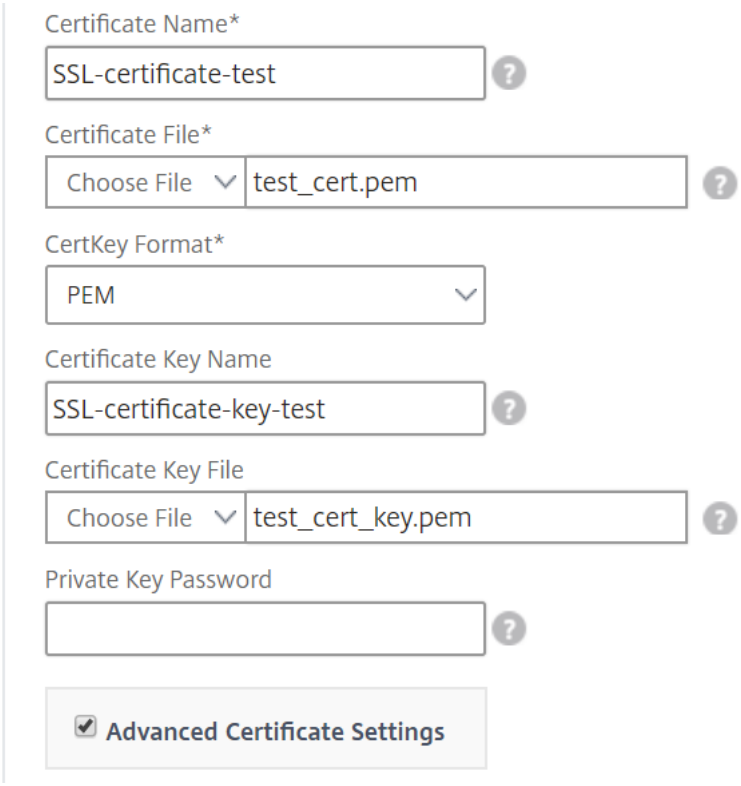
> **Remarque**
>
> Si vous sélectionnez SSL, assurez-vous que le paramètre de configuration de réécriture est activé dans la section Paramètres avancés de SharePoint de ce StyleBook.

e) **Adresses IP des serveurs SharePoint**. Adresses IP de tous les serveurs SharePoint du réseau.

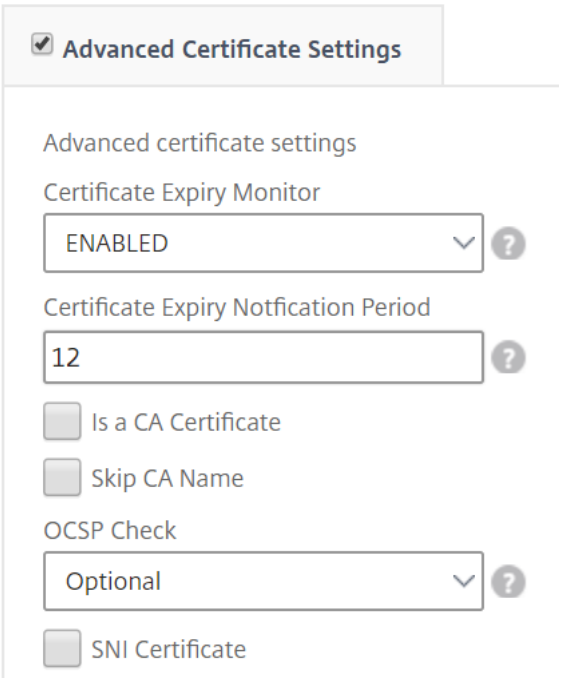
f) **Port des serveurs SharePoint**. Numéro de port TCP utilisé par les serveurs SharePoint. Par défaut, il s'agit de 80. Vous pouvez modifier cette valeur si nécessaire, mais assurez-vous que ce port est accessible sur les serveurs Microsoft SharePoint 2016.



3. Dans la section **Paramètres des certificats SSL**, cliquez sur + pour entrer le nom du certificat SSL, la clé de certificat, et sélectionnez les fichiers respectifs dans votre dossier de stockage local.

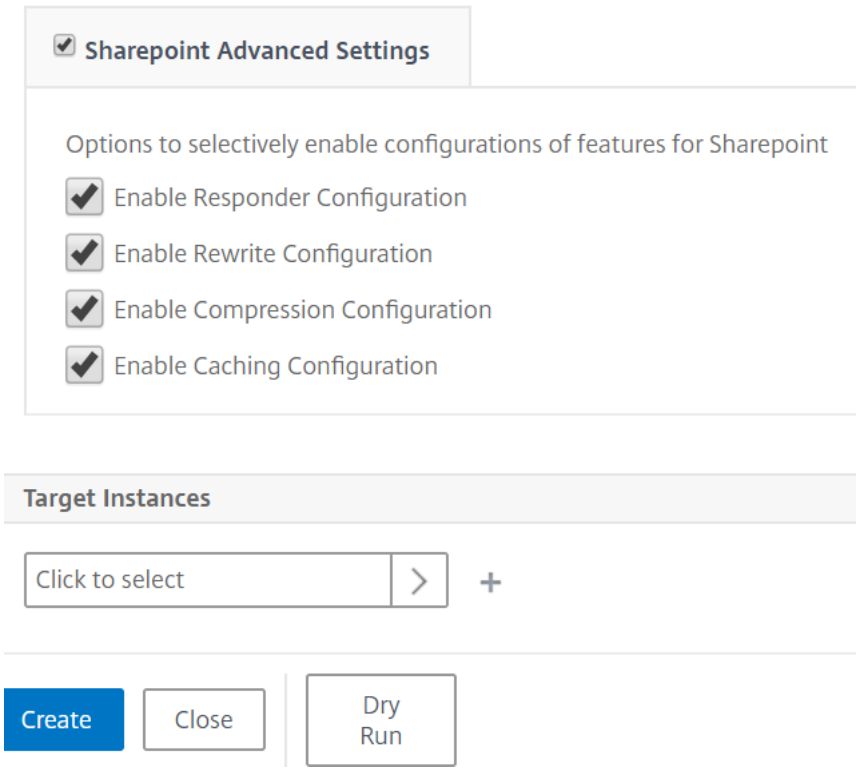


4. Vous pouvez également cliquer sur **Paramètres de certificat avancés** pour activer ou désactiver la surveillance de l'expiration des certificats SSL. Si vous activez la surveillance de l'expiration des certificats, définissez le nombre de jours afin que Citrix ADM émette une alarme après ces nombreux jours pendant lesquels le certificat est sur le point d'expirer. Vous avez également la possibilité de vérifier l'OCSP en tant que fonctionnalité facultative ou obligatoire.



5. La section **Paramètres avancés** de SharePoint vous permet d'activer les fonctionnalités de Citrix ADC qui seront configurées sur les instances de Citrix ADC. Bien que les fonctionnalités d'équilibrage de charge et de commutation de contenu soient configurées sur les instances par défaut, vous pouvez choisir les autres fonctionnalités, à savoir la configuration du répondeur, la configuration de réécriture, la configuration de compression et la configuration de mise en cache intégrée, que vous souhaitez configurer sur l'instance.
6. Cliquez sur **Target Instances** et sélectionnez l'instance Citrix ADC sur laquelle déployer cette configuration SharePoint. Cliquez sur **Créer** pour créer la configuration et déployer la configuration sur l'instance Citrix ADC sélectionnée.

   > **Remarque**
   >
   > Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter des instances Citrix ADC récemment découvertes dans Citrix ADM à la liste des instances disponibles dans cette fenêtre.



> **Remarque**
>
> Citrix recommande, avant d'exécuter la configuration proprement dite, de sélectionner **Dry Run** pour vérifier les objets de configuration qui seront créés sur l'instance cible.

Lorsque la configuration est créée et déployée avec succès, le StyleBook SharePoint crée un serveur virtuel de commutation de contenu et 12 serveurs virtuels d'équilibrage de charge. Il crée également

des stratégies et des groupes de services et les lie aux serveurs virtuels d'équilibrage de charge. Les stratégies créées dépendent des fonctionnalités sélectionnées dans le StyleBook lors de la création du pack de configuration.

Affichage des objets définis sur l'instance de Citrix ADC

Une fois le pack de configuration créé sur Citrix ADM, vous pouvez afficher tous les objets créés sur l'instance Citrix ADC pour le SharePoint StyleBook. Accédez à **Applications** > **Administration** > **Configuration**, puis cliquez sur **Afficher les objets créés** . La figure suivante montre certains des objets créés, avec les adresses IP spécifiées dans l'exemple illustré dans « Deploying SharePoint StyleBook Configurations from Citrix ADM. »

Type : lbvserver

appflowlog : DISABLED
backuppersistencetimeout : 20
downstateflush : DISABLED
ipv46 : 0.0.0.0
lbmethod : LEASTCONNECTION
name : sharepoint application test frontpage services lb
persistencebackup : SOURCEIP
persistencetype : COOKIEINSERT
port : 0
servicetype : HTTP
timeout : 20

Type : servicegroup

cip : DISABLED
cka : YES
cmp : NO
downstateflush : DISABLED
healthmonitor : NO
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp
servicetype : HTTP
sp : ON
state : ENABLED
tcpb : NO
useproxyport : NO
usip : NO

Type : lbvserver_servicegroup_binding

name : sharepoint-application-test-frontpage-services-lb
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.10.10.11
port : 80
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.10.10.12
port : 80
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

Type : csaction

name : sharepoint-application-test-cs-frontpage-services-csaction
targetlbvserver : sharepoint-application-test-frontpage-services-lb

Type : cspolicy

action : sharepoint-application-test-cs-frontpage-services-csaction
policyname : sharepoint-application-test-cs-frontpage-services-cspol
rule : HTTP.REQ.HEADER("X-Vermeer-Content-Type").EXISTS

Type : csvserver_cspolicy_binding

name : sharepoint-application-test-cs
policyname : sharepoint-application-test-cs-frontpage-services-cspol
priority : 10

StyleBook proxy Microsoft ADFS

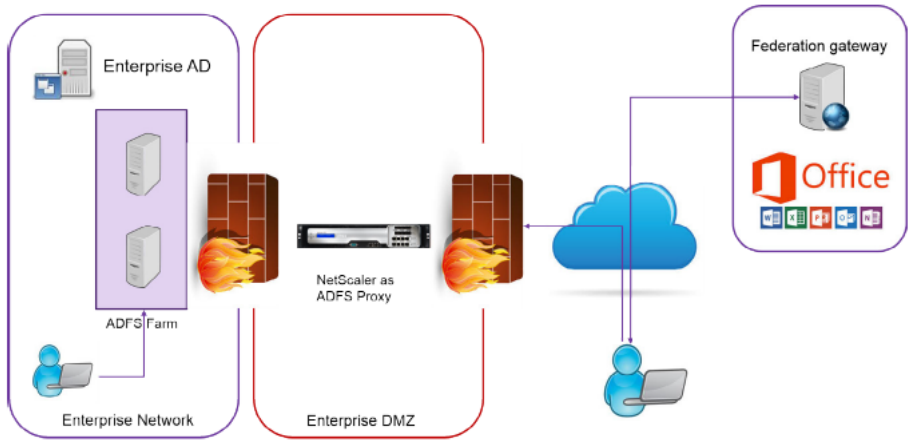
February 1, 2024

Le proxy Microsoft™ ADFS joue un rôle important en fournissant un accès par authentification unique aux ressources internes compatibles avec la fédération et aux ressources cloud. Office 365 est un exemple de ressources cloud. Le but du serveur proxy ADFS est de recevoir et de transférer des demandes vers des serveurs ADFS qui ne sont pas accessibles à partir d'Internet. Le proxy ADFS est un proxy inverse qui réside généralement dans le réseau de périmètre (DMZ) de votre organisation. Le proxy ADFS joue un rôle essentiel dans la connectivité des utilisateurs distants et l'accès aux applications.

Citrix ADC dispose de la technologie précise qui permet de sécuriser la connectivité, l'authentification et la gestion de l'identité fédérée. L'utilisation de Citrix ADC comme proxy ADFS évite de devoir déployer un composant supplémentaire dans la zone démilitarisée.

Le logiciel Microsoft ADFS Proxy StyleBook dans Citrix Application Delivery Management (ADM) vous permet de configurer un serveur proxy ADFS sur une instance Citrix ADC.

L'image suivante montre le déploiement d'une instance de Citrix ADC en tant que serveur proxy ADFS dans la zone DMZ d'entreprise.



Avantages de l'utilisation de Citrix ADC comme proxy ADFS

1. Répond à la fois aux besoins d'équilibrage de charge et de proxy ADFS
2. Prend en charge les scénarios d'accès utilisateur internes et externes
3. Prend en charge des méthodes complètes de pré-authentification
4. Offre une expérience d'authentification unique aux utilisateurs
5. Prend en charge les protocoles actifs et passifs

   a) Voici des exemples d'applications à protocole actif : Microsoft Outlook, Microsoft Skype for Business
   b) Voici des exemples d'applications à protocole passif : application Web Microsoft Outlook, navigateurs Web

6. Périphérique renforcé pour un déploiement basé sur DMZ
7. Ajoute de la valeur en utilisant des fonctionnalités supplémentaires de base de l'Citrix ADC ADC

   a) Commutation de contenu
   b) Déchargement SSL
   c) Réécriture
   d) Sécurité (Citrix ADC AAA)

Pour les scénarios basés sur un protocole actif, vous pouvez vous connecter à Office 365 et fournir vos informations d'identification. Microsoft Federation Gateway contacte le service ADFS (via le proxy ADFS) au nom du client de protocole actif. La passerelle soumet ensuite les informations d'identification à l'aide de l'authentification de base (401). Citrix ADC gère l'authentification du client avant l'accès au service ADFS. Après l'authentification, le service ADFS fournit un jeton SAML à Federation Gateway. La Federation Gateway, à son tour, soumet le jeton à Office 365 pour fournir un accès client.

Pour les clients passifs, l'ADFS Proxy StyleBook crée un compte utilisateur Kerberos Constrained Delegation (KCD). Le compte KCD est nécessaire pour que l'authentification SSO Kerberos puisse se connecter aux serveurs ADFS. Le StyleBook génère également une stratégie LDAP et une stratégie de session. Ces stratégies sont ultérieurement liées au serveur virtuel Citrix ADC AAA qui gère l'authentification pour les clients passifs.

Le StyleBook peut également garantir que les serveurs DNS du Citrix ADC sont configurés pour ADFS.

La section de configuration ci-dessous explique comment configurer Citrix ADC pour gérer l'authentification client basée sur des protocoles actifs et passifs.

Détails de la configuration

Le tableau ci-dessous répertorie les versions logicielles minimales requises pour que cette intégration soit déployée avec succès.

Produit	Version minimale requise
Citrix ADC	11.0, licence avancée/premium

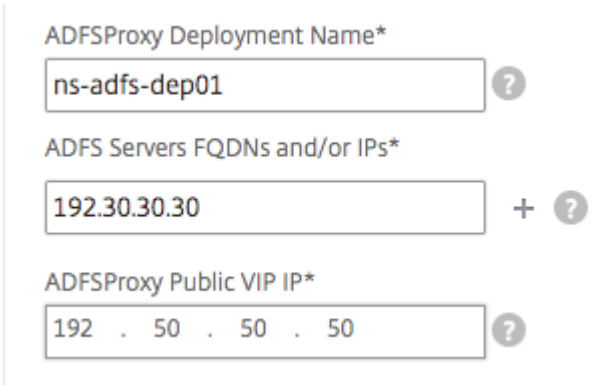
Les instructions suivantes supposent que vous avez déjà créé les entrées DNS externes et internes appropriées.

Déploiement de configurations StyleBook du proxy Microsoft ADFS depuis Citrix ADM

Les instructions suivantes vous aideront à implémenter le proxy Microsoft ADFS StyleBook dans votre réseau d'entreprise.

Pour déployer le proxy Microsoft ADFS StyleBook

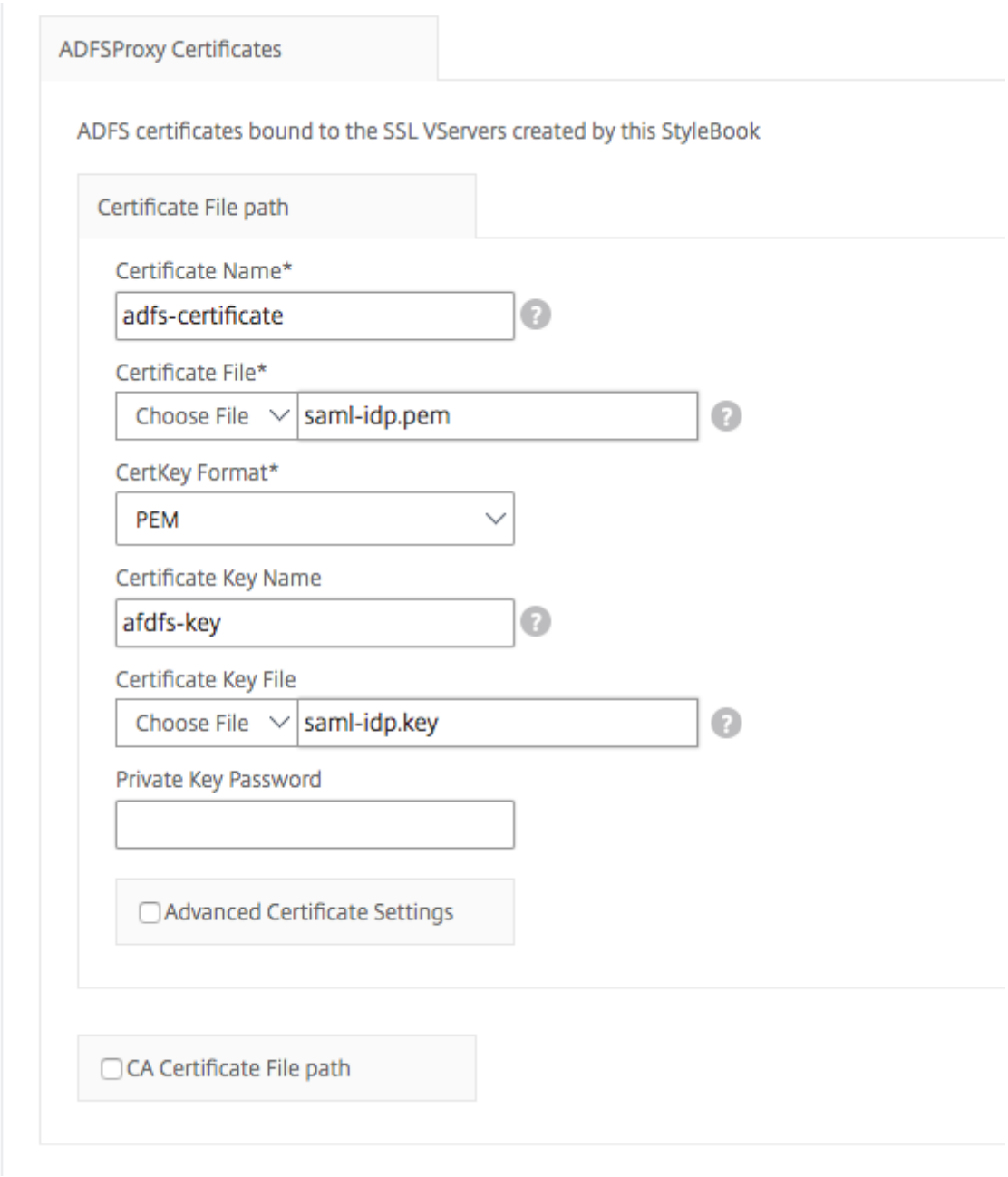
1. **Dans Citrix ADM, accédez à**Applications**> StyleBooks.** La page **StyleBooks** affiche tous les StyleBooks disponibles pour votre utilisation dans Citrix ADM.
2. Faites défiler l'écran vers le bas et trouvez le **StyleBook du proxy Microsoft ADFS**. Cliquez sur **Créer une configuration**.
   Le StyleBook s'ouvre sous la forme d'une page d'interface utilisateur sur laquelle vous pouvez saisir les valeurs de tous les paramètres définis dans ce StyleBook.
3. Entrez les valeurs des paramètres suivants :
   a) **Nom du déploiement du proxy ADFS**. Sélectionnez un nom pour la configuration du proxy ADFS déployée sur votre réseau.
   b) **FQDN ou IP des serveurs ADFS**. Entrez les adresses IP ou les noms de domaine complets (FQDN) de tous les serveurs ADFS du réseau.
   c) **IP VIP publique du proxy ADFS**. Tapez l'adresse IP virtuelle publique sur l'Citrix ADC qui fonctionne en tant que serveur proxy ADFS.



4. Dans la section **Certificats de proxy ADFS**, tapez les détails du certificat SSL et de la clé de certificat.

   Ce certificat SSL est lié à tous les serveurs virtuels créés sur l'instance Citrix ADC.

   Sélectionnez les fichiers correspondants dans votre dossier de stockage local. Vous pouvez également saisir le mot de passe de clé privée pour charger les clés privées chiffrées au format .pem.



Vous pouvez également activer la case à cocher **Paramètres de certificat avancés**. Vous pouvez saisir ici des informations telles que la période de notification d'expiration des certificats, activer ou désactiver le moniteur d'expiration des certificats.

5. Vous pouvez également activer la case à cocher **Certificat d'autorité de certification SSL** si le certificat SSL nécessite l'installation d'un certificat public d'autorité de certification sur Citrix ADC. Vérifiez que vous sélectionnez **Est un certificat d'autorité de certification** dans la section **Paramètres de certificat avancés**.
6. Activer l'authentification pour les clients actifs et passifs. Entrez le nom de domaine DNS utilisé

dans Active Directory pour l'authentification des utilisateurs. Vous pouvez ensuite configurer l'authentification pour les clients actifs ou passifs, ou les deux.

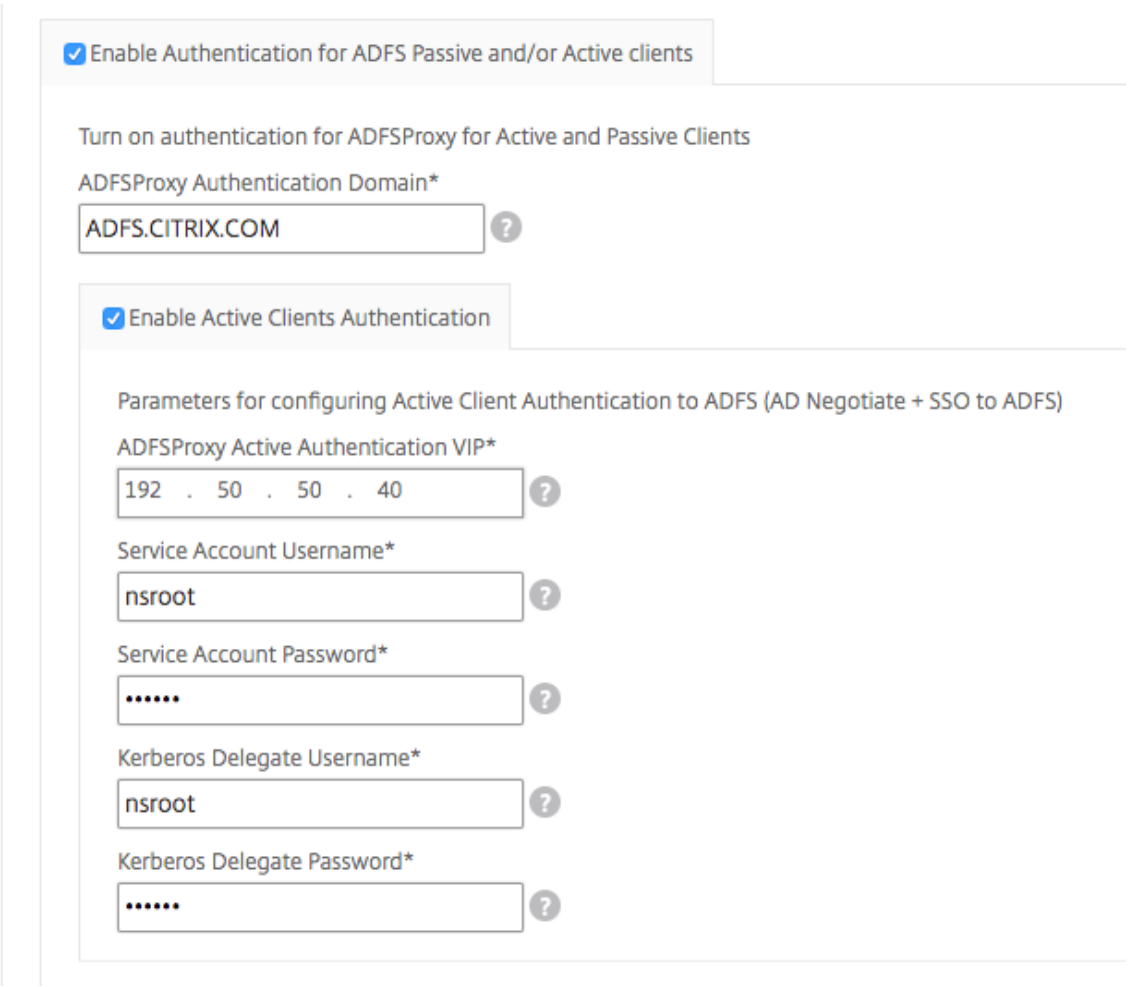
7. Entrez les informations suivantes pour activer l'authentification pour les clients actifs :

   > **Remarque**
   >
   > La configuration de la prise en charge des clients actifs est facultative.

   a) **Authentification active par proxy ADFS VIP**. Tapez l'adresse IP virtuelle du serveur d'authentification virtuel sur l'instance Citrix ADC sur laquelle les clients actifs sont redirigés pour l'authentification.

   b) Nom d'**utilisateur du compte de service** Entrez le nom d'utilisateur du compte de service utilisé par Citrix ADC pour authentifier vos utilisateurs auprès d'Active Directory.

   c) Mot de**passe du compte de service** Saisissez le mot de passe utilisé par Citrix ADC pour authentifier vos utilisateurs dans l'annuaire actif.



8. Configurez l'authentification pour les clients passifs en activant l'option correspondante et en configurant les paramètres LDAP.

> **Remarque**
>
> La configuration de la prise en charge des clients passifs est facultative.

Entrez les informations suivantes pour activer l'authentification pour les clients passifs :

a) **Base LDAP (Active Directory)**. Tapez le nom de domaine de base du domaine dans lequel les comptes d'utilisateur résident dans Active Directory (AD) pour autoriser l'authentification. Par exemple, dc=netscaler, dc=com

b) **DN de liaison LDAP (Active Directory)**. Ajoutez un compte de domaine (à l'aide d'une adresse e-mail pour faciliter la configuration) qui dispose des privilèges pour parcourir l'arborescence AD. Par exemple, CN=Manager, dc=netscaler, dc=com

c) **Mot de passe du nom unique de liaison LDAP (Active Directory)**. Entrez le mot de passe du compte de domaine pour l'authentification.

Quelques autres champs que vous devez saisir dans les valeurs de cette section sont les suivants :

d) **IP du serveur LDAP (Active Directory)**. Entrez l'adresse IP du serveur Active Directory pour que l'authentification AD fonctionne correctement.

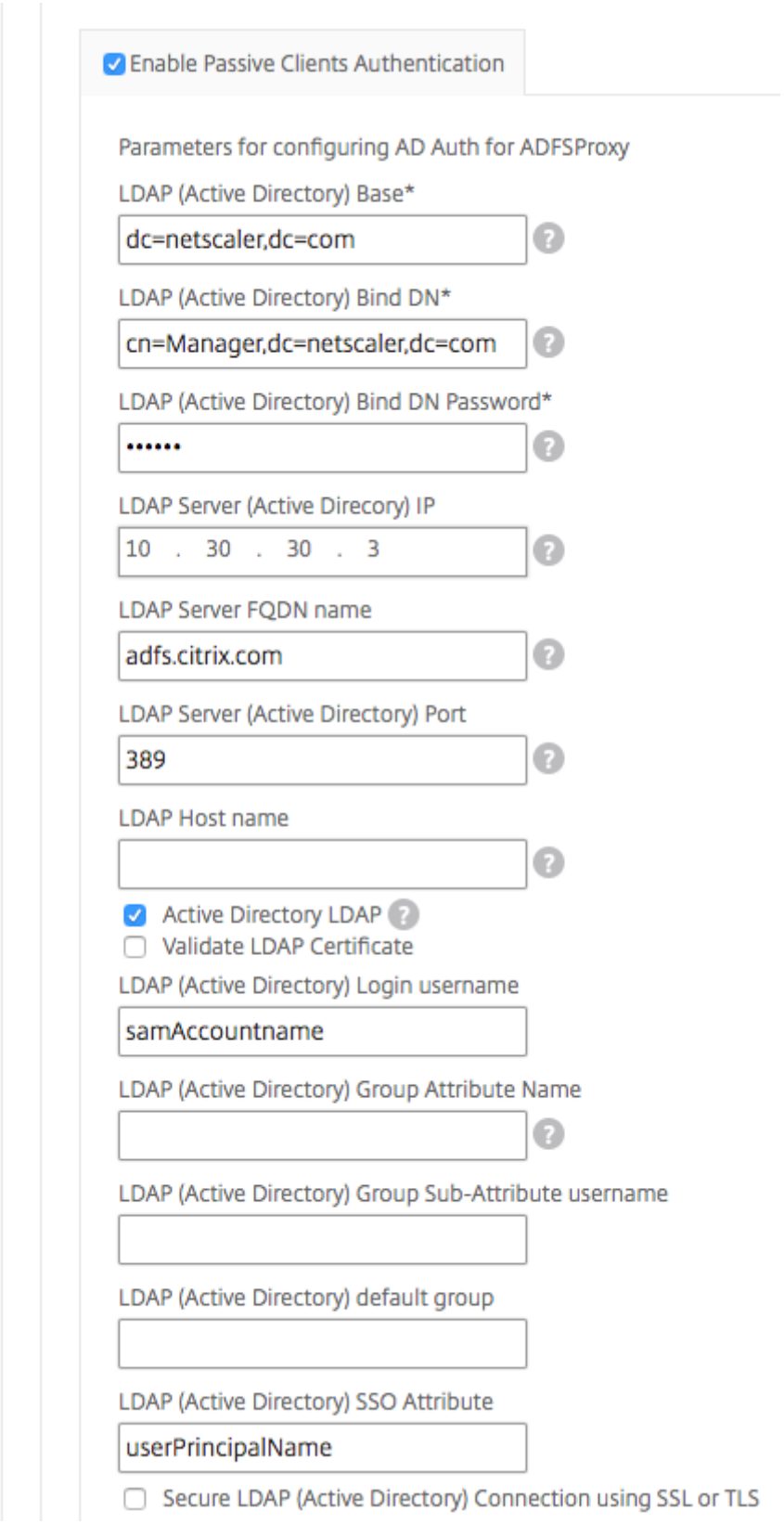
e) **Nom** de**domaine complet du serveur LDAP** . Entrez le nom de domaine complet du serveur Active Directory. Le nom FQDN est facultatif. Fournissez l'adresse IP comme à l'étape 1 ou le nom de domaine complet.

f) **Port Active Directory du serveur LDAP**. Par défaut, les ports TCP et UDP pour le protocole LDAP sont 389, tandis que le port TCP pour Secure LDAP est 636.

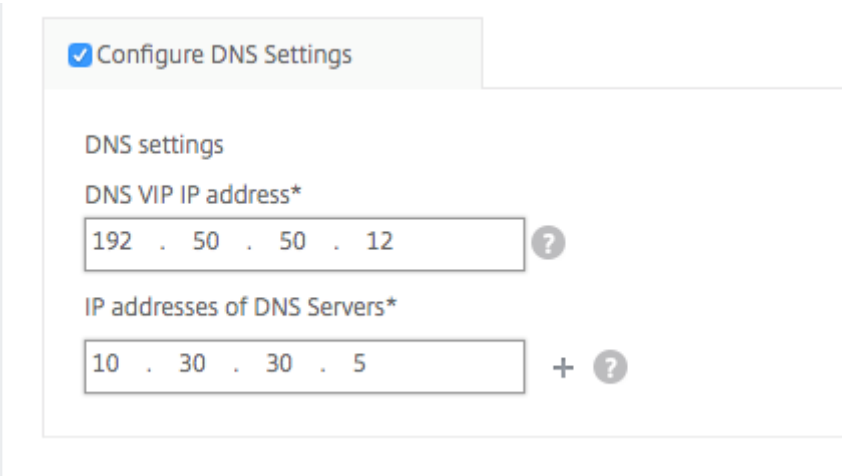
g) **Nom d'utilisateur de connexion LDAP (Active Directory)**. Entrez le nom d'utilisateur sous la forme « SAMAccountName ».

h) **VIP de l'authentification passive par proxy ADFS**. Entrez l'adresse IP du serveur virtuel proxy ADFS pour les clients passifs.

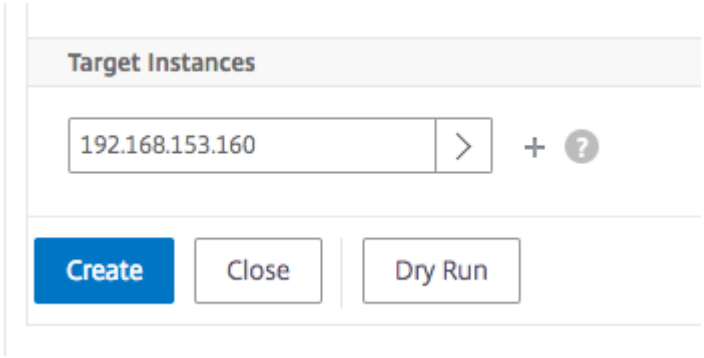
> **Remarque**
>
> Les champs marqués par « * » sont obligatoires.



9. Vous pouvez également configurer un VIP DNS pour vos serveurs DNS.



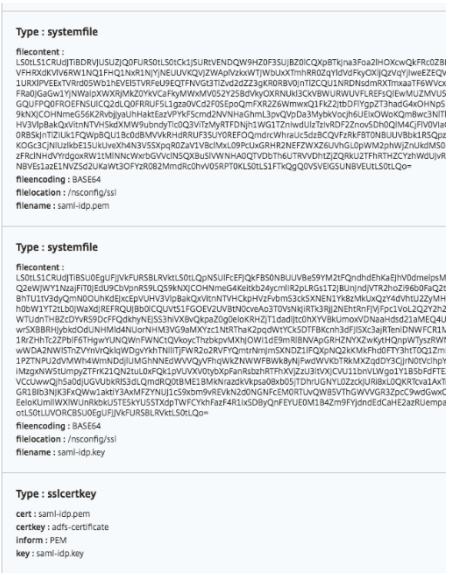
10. Cliquez sur **Instances cibles** et sélectionnez les instances Citrix ADC pour déployer cette configuration de proxy Microsoft ADFS. Cliquez sur **Créer** pour créer la configuration et déployer la configuration sur les instances Citrix ADC sélectionnées.



> **Remarque**
>
> Citrix recommande de sélectionner **Essai** avant d'exécuter la configuration réelle. Vous pouvez d'abord afficher les objets de configuration créés sur les instances Citrix ADC cibles par le StyleBook. Vous pouvez ensuite cliquer sur **Créer** pour déployer la configuration sur les instances sélectionnées.

Objets créés

Plusieurs objets de configuration sont créés lorsque la configuration du proxy ADFS est déployée sur l'instance Citrix ADC. L'image suivante affiche la liste des objets créés.



Objects Added on Instance : 192.168.153.160 | Count : 57

Type : nsfeature

Meta Properties
action : **enable**

feature : cs lb ssl rewrite aaa

Type : lbvserver

ipv46 : 192.50.50.12
name : ns-adfs-dep01-adfs-dns
port : 53
servicetype : DNS

Type : service

ip : 10.30.30.5
name : ns-adfs-dep01-dns-svc-1
port : 53
servicetype : DNS

Type : lbvserver_service_binding

name : ns-adfs-dep01-adfs-dns
servicename : ns-adfs-dep01-dns-svc-1

Type : authenticationnegotiateaction

domain : ADFS.CITRIX.COM
domainuser : nsroot
domainuserpasswd : nsroot
name : ns-adfs-dep01-negotiate-action

Type : authenticationpolicy

action : ns-adfs-dep01-negotiate-action
name : ns-adfs-dep01-negotiate-policy
rule : true

Type : aaakcdaccount

delegateduser : nsroot
kcdaccount : ns-adfs-dep01-adfs-auth401-kcd-
kcdpassword : nsroot
realmstr : ADFS.CITRIX.COM

Type : tmsessionaction

kcdaccount : ns-adfs-dep01-adfs-auth401-kcd-
name : ns-adfs-dep01-adfs-auth401-tmsession-action
persistentcookie : ON
persistentcookievalidity : 3
sso : ON

Type : tmsessionpolicy

action : ns-adfs-dep01-adfs-auth401-tmsession-action
name : ns-adfs-dep01-adfs-auth401-tmsession-policy
rule : ns_true

Type : authenticationvserver

authenticationdomain : ADFS.CITRIX.COM
failedlogintimeout : 1
ipv46 : 192.50.50.40
maxloginattempts : 255
name : ns-adfs-dep01-adfs-auth401-auth-vserver
port : 443
servicetype : SSL

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-adfs-auth401-auth-vserver

Type : authenticationvserver_authenticationpolicy_binding

name : ns-adfs-dep01-adfs-auth401-auth-vserver
policy : ns-adfs-dep01-negotiate-policy
priority : 10

Type : authenticationvserver_tmsessionpolicy_binding

name : ns-adfs-dep01-adfs-auth401-auth-vserver
policy : ns-adfs-dep01-adfs-auth401-tmsession-policy
priority : 10

Type : authenticationldapaction

authentication : ENABLED
authtimeout : 30
followreferrals : OFF
ldapbase : dc=netscaler,dc=com
ldapbinddn : cn=Manager,dc=netscaler,dc=com
ldapbinddnpassword : nsroot
ldaploginname : samAccountname
name : ns-adfs-dep01-ldap-action
passwdchange : DISABLED
sectype : PLAINTEXT
serverip : 10.30.30.3
serverport : 389
ssonameattribute : userPrincipalName
svrtype : AD
validateservercert : NO

Type : authenticationpolicy

action : ns-adfs-dep01-ldap-action
name : ns-adfs-dep01-ldap-policy
rule : true

Type : aaakcdaccount

kcdaccount : ns-adfs-dep01-adfs-ldap-kcd-acc
realmstr : ADFS.CITRIX.COM

Type : tmsessionaction

kcdaccount : ns-adfs-dep01-adfs-ldap-kcd-acc
name : ns-adfs-dep01-adfs-ldap-tmsession-action
persistentcookie : OFF
sso : ON

Type : tmsessionpolicy

action : ns-adfs-dep01-adfs-ldap-tmsession-action
name : ns-adfs-dep01-adfs-ldap-tmsession-policy
rule : ns_true

Type : authenticationvserver

authenticationdomain : ADFS.CITRIX.COM
failedlogintimeout : 1
ipv46 : 192.50.50.30
maxloginattempts : 255
name : ns-adfs-dep01-adfs-ldap-auth-vserver
port : 443
servicetype : SSL

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-adfs-ldap-auth-vserver

Type : authenticationvserver_authenticationpolicy_binding

name : ns-adfs-dep01-adfs-ldap-auth-vserver
policy : ns-adfs-dep01-ldap-policy
priority : 10

Type : authenticationvserver_tmsessionpolicy_binding

name : ns-adfs-dep01-adfs-ldap-auth-vserver
policy : ns-adfs-dep01-adfs-ldap-tmsession-policy
priority : 10

Type : csvserver

ipv46 : 192.50.50.50
name : ns-adfs-dep01-cs
port : 443
servicetype : SSL

Type : lbvserver

ipv46 : 192.50.50.50
name : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb
port : 445
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp

Type : server

ipaddress : 192.30.30.30
name : 192.30.30.30

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol
rule : HTTP.REQ.URL.CONTAINS("/adfs/services/trust") || HTTP.REQ.URL.CONTAINS("/federa

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol
priority : 9800

Type : lbvserver

appflowlog : ENABLED
authentication : ON
authenticationhost : ADFS.CITRIX.COM
authn401 : OFF
authnvsname : ns-adfs-dep01-adfs-ldap-auth-vserver
downstateflush : ENABLED
ipv46 : 192.50.50.50
lbmethod : LEASTCONNECTION
name : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb
port : 446
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-cspol
rule : HTTP.REQ.URL.CONTAINS("/adfs/ls/auth/integrated") || HTTP.REQ.URL.CONTAINS("/adfs/ls/wia")

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-cspol
priority : 9900

Type : lbvserver

appflowlog : ENABLED
authentication : OFF
authn401 : ON
authnvsname : ns-adfs-dep01-adfs-auth401-auth-vserver
downstateflush : ENABLED
ipv46 : 192.50.50.50
lbmethod : LEASTCONNECTION
name : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb
port : 444
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-cspol
rule : true

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-cspol
priority : 10000

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-cs

Type : rewritepolicylabel

labelname : ns-adfs-dep01-request-rewritepolicylabel
transform : HTTP_REQ

Type : rewritepolicylabel

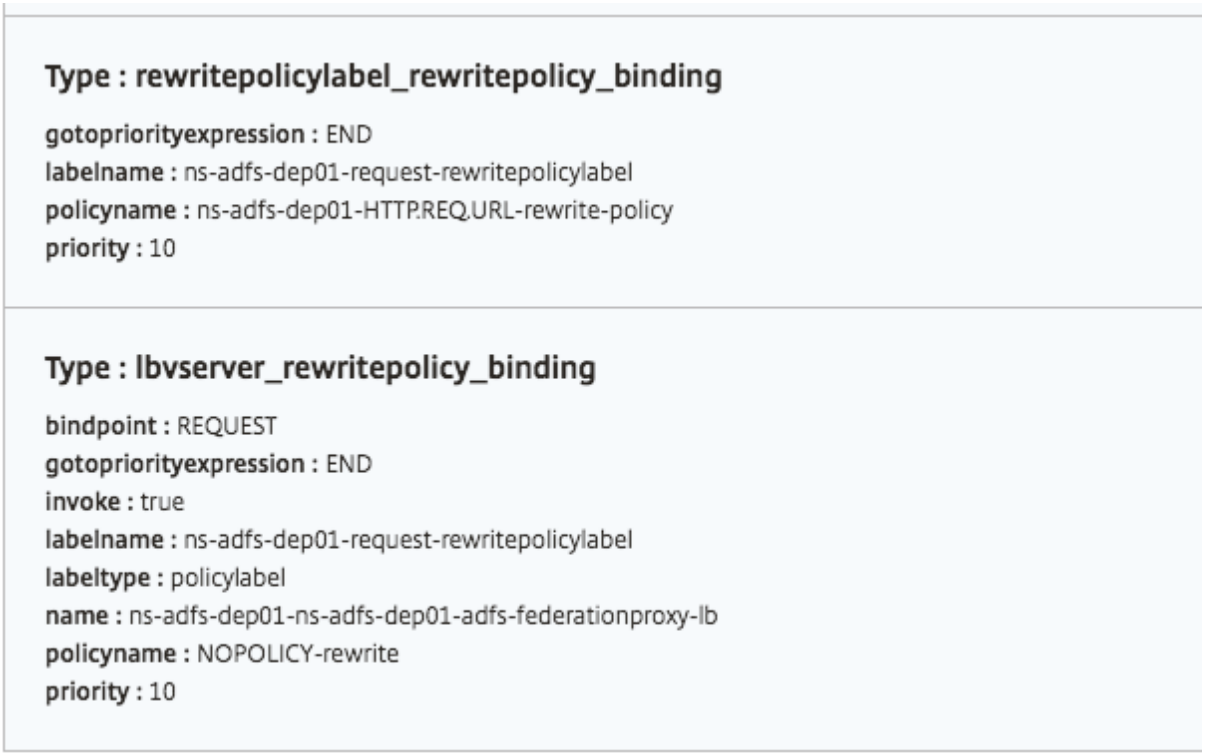
labelname : ns-adfs-dep01-response-rewritepolicylabel
transform : HTTP_RES

Type : rewriteaction

name : ns-adfs-dep01-HTTP.REQ.URL-rewrite-action
stringbuilderexpr : "/adfs/services/trust/proxymex"
target : HTTP.REQ.URL
type : REPLACE

Type : rewritepolicy

action : ns-adfs-dep01-HTTP.REQ.URL-rewrite-action
name : ns-adfs-dep01-HTTP.REQ.URL-rewrite-policy
rule : HTTP.REQ.URL.CONTAINS("/adfs/services/trust") && (!HTTP.REQ.URL.CONTAINS("/trust/proxymex"))



StyleBook Oracle E-Business

February 1, 2024

Oracle E-Business Suite est la suite la plus complète d'applications métier globales intégrées. Cette suite permet aux entreprises de prendre de meilleures décisions, de réduire les coûts et d'améliorer les performances. Elle comprend les applications suivantes.

- Planification des ressources de l'entreprise (ERP)
- Gestion de la relation client (CRM)
- Gestion de la chaîne d'approvisionnement (SCM)

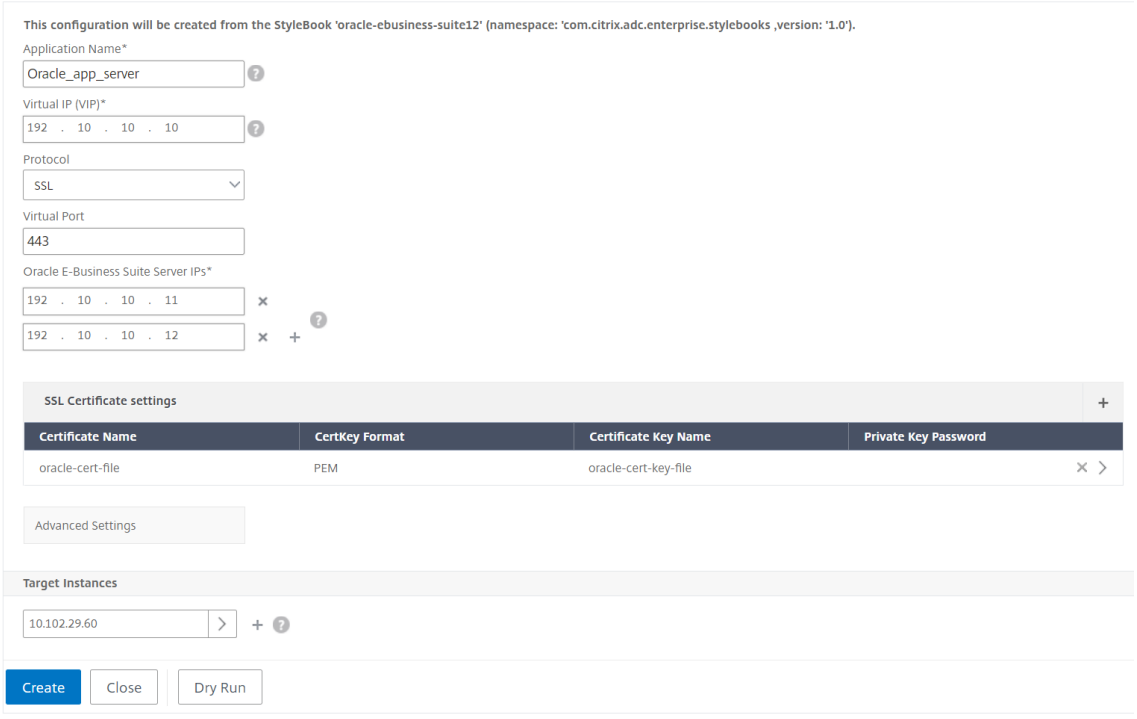
Ces applications informatiques sont développées ou acquises par Oracle. Le StyleBook d'Oracle E-Business Suite 12.2 vous permet de déployer la configuration sur les instances Citrix ADC sélectionnées.

Ce StyleBook crée une configuration d'équilibrage de charge qui comprend un serveur virtuel d'équilibrage de charge, un groupe de services et une liste de services. Il lie également les services au groupe de services et lie le groupe de services au serveur virtuel. Vous pouvez choisir une communication chiffrée en sélectionnant SSL et en fournissant les fichiers SSL et les fichiers clés de votre système local.

Pour créer une configuration pour Oracle E-Business Suite 12.2

1. Dans Citrix Application Delivery Management (ADM), accédez à **Applications** > **Configuration** > **StyleBooks**. La page **StyleBooks** affiche tous les StyleBooks disponibles dans votre Citrix ADM. Faites défiler l'écran vers le bas et sélectionnez **Oracle E-Business Suite 12.2**. Vous pouvez également utiliser l'option de recherche pour effectuer une recherche dans le StyleBook.
2. Cliquez sur **Créer une configuration** dans le panneau StyleBook.
3. Entrez le nom de l'application d'équilibrage de charge et l'adresse IP virtuelle dans la section des paramètres de l'équilibreur de charge.
4. Sélectionnez le protocole requis. Vous avez deux options ici - HTTP et HTTPS/SSL. Vous pouvez également saisir le numéro de port.
5. Entrez les adresses IP de tous les serveurs d'applications Oracle E-Business Suite du réseau qui doivent être équilibrés en termes de charge. Cliquez sur **+** pour ajouter d'autres adresses IP de serveur.
6. Dans la section **Paramètres des certificats SSL**, sélectionnez les fichiers correspondants dans votre stockage local. Vous pouvez également activer la case à cocher **Paramètres de certificat avancés**. Ici, vous pouvez configurer plus de détails tels que la période de notification d'expiration du certificat. Vous pouvez également activer ou désactiver le moniteur d'expiration des certificats.

   Sélectionnez l'instance Citrix ADC cible sur laquelle la configuration doit être créée, puis cliquez sur **Créer**.



> **Conseil**
>
> Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter des instances Citrix ADC récemment découvertes dans Citrix ADM à la liste des instances disponibles dans cette fenêtre. L'icône d'actualisation est actuellement disponible uniquement sur Citrix ADM.

Livres de style Citrix StoreFront

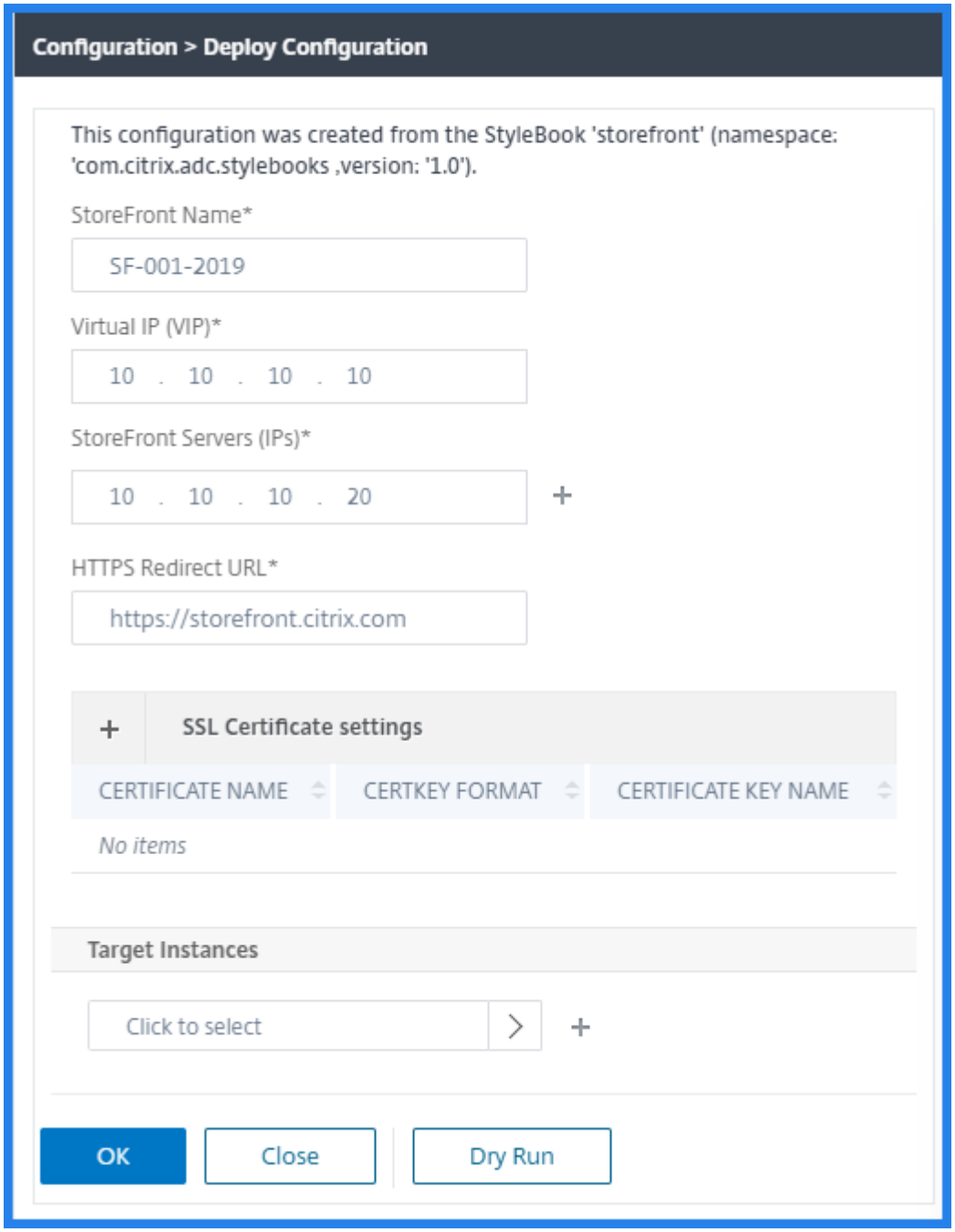
February 1, 2024

StoreFront est un magasin d'applications d'entreprise qui regroupe les applications et les bureaux des sites Citrix Virtual Apps and Desktops dans un magasin unique pour les utilisateurs. StoreFront authentifie les utilisateurs auprès des sites hébergeant des ressources et gère les magasins d'applications et les bureaux auxquels les utilisateurs accèdent. Il héberge votre magasin d'applications d'entreprise, ce qui vous permet de donner aux utilisateurs un accès en libre-service aux applications et aux postes de travail que vous mettez à leur disposition.

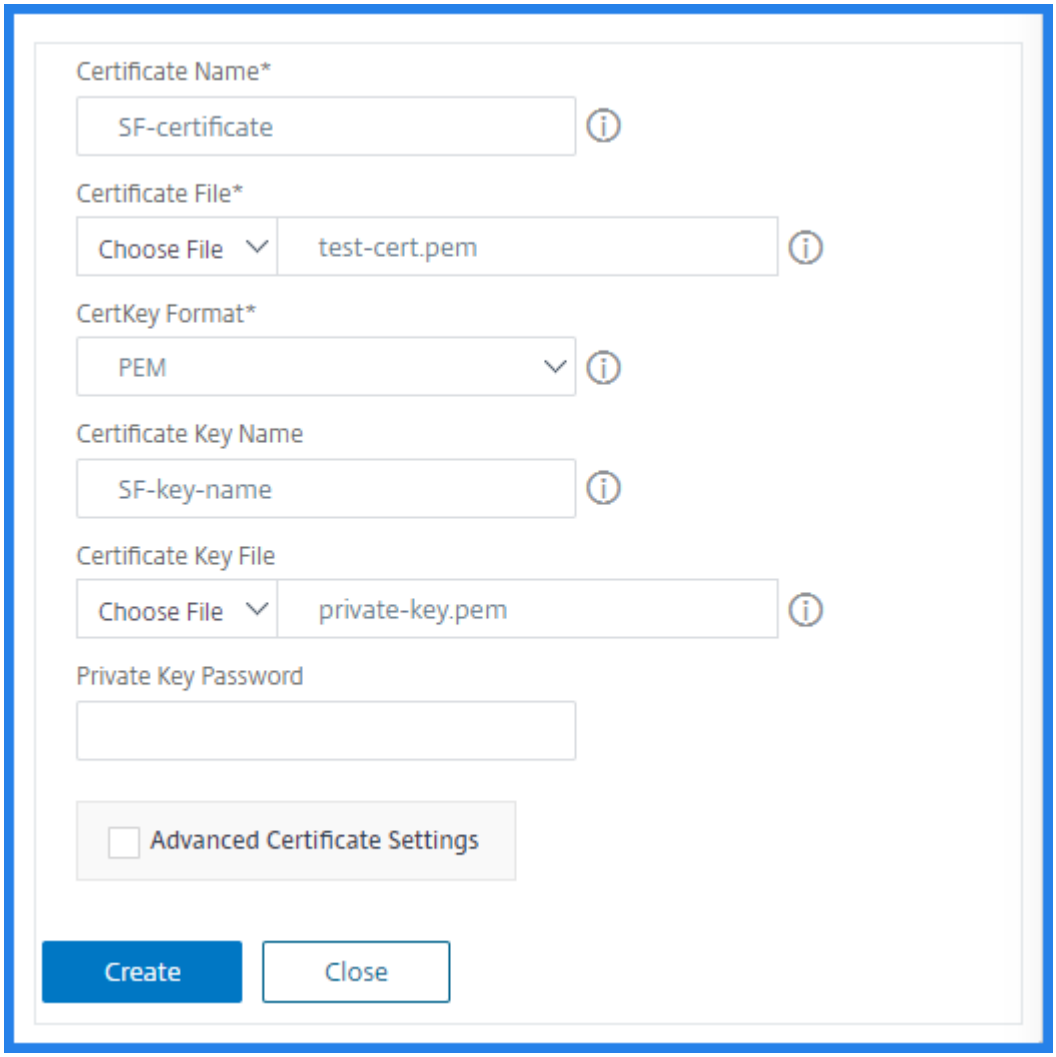
Ce StyleBook définit les configurations Citrix ADC pour les serveurs StoreFront. Avec ce StyleBook, vous pouvez configurer les serveurs StoreFront sur les instances Citrix ADC souhaitées. Vous pouvez choisir une communication chiffrée en sélectionnant SSL et en fournissant les fichiers SSL et les fichiers clés de votre système local.

Créer une configuration pour les applications Citrix StoreFront

1. Dans l'interface graphique Citrix ADM, accédez à **Applications > StyleBooks**.
2. Dans la barre de recherche, utilisez les propriétés **Nom** et recherchez `Citrix StoreFront`.
3. Dans le StyleBook Citrix StoreFront, cliquez sur Créer une configuration.
4. Spécifiez les détails suivants :
    - **Nom StoreFront** : Spécifiez le nom StoreFront. Le ConfigPack StoreFront est créé avec le même nom StoreFront.
    - **IP virtuelle (VIP)** : spécifiez l'adresse IP virtuelle à laquelle l'instance Citrix ADC reçoit les demandes du client.
    - **Serveurs StoreFront** : spécifiez les adresses IP des serveurs StoreFront que vous souhaitez configurer avec une instance Citrix ADC.
    - **URL de redirection HTTPS** : spécifiez l'URL HTTPS vers laquelle les requêtes HTTPS sont redirigées.



5. Dans la section **Paramètres des certificats SSL**, entrez les noms du certificat SSL et la clé du certificat.
6. Sélectionnez les fichiers correspondants dans votre dossier de stockage local. Vous pouvez également saisir le mot de passe de la clé privée pour spécifier les clés privées cryptées au format PEM.



7. Vous pouvez également activer la case à cocher **Paramètres de certificat avancés**. Ici, vous pouvez entrer des détails tels que la période de notification d'expiration du certificat, activer ou désactiver le moniteur d'expiration du certificat.
8. Facultatif, activez **la case à cocher Certificat d'autorité de certification SSL pour l'authentification IP virtuelle** si le certificat SSL nécessite l'installation d'un certificat public d'autorité de certification sur Citrix ADC. Assurez-vous de choisir **Est un certificat d'autorité de certification** dans la section **Paramètres de certificat avancés**.
9. Cliquez sur **Créer**.
10. Cliquez sur **Instances cibles** et sélectionnez les instances Citrix ADC sur lesquelles vous souhaitez configurer les serveurs StoreFront.
11. Cliquez sur **Créer** pour créer la configuration et déployer la configuration sur les instances Citrix ADC sélectionnées.

Créer et utiliser des StyleBooks personnalisés

February 1, 2024

Vous pouvez écrire votre propre StyleBook pour votre déploiement, l'importer dans Citrix Application Delivery Management (ADM) et créer des objets de configuration. Vous pouvez également utiliser l'API pour créer des configurations à partir de vos StyleBooks.

Ce document contient les informations suivantes :

Avant de commencer

Avant de commencer à créer des StyleBooks, assurez-vous de connaître les points suivants :

- API NITRO. Pour plus d'informations, consultez la documentation de l'API Nitro
- YAML

Les fichiers StyleBook utilisent le format YAML. Pour plus d'informations sur le format YAML, consultez Syntaxe YAML.

Voici une liste des instructions YAML dont vous devez tenir compte lors de la création de StyleBooks :

- YAML fait la distinction entre majuscules et minuscules.
- YAML nécessite une indentation appropriée
- Utilisez <spacebar> la touche pour créer une indentation appropriée. N'utilisez pas de <tab > clé. L'utilisation de <tab> la clé crée une erreur de compilation lors de l'importation de votre StyleBook vers MA Service
- N'utilisez pas de chaînes entre guillemets. N'incluez la chaîne entre guillemets que si une chaîne contient des signes de ponctuation (tirets, deux-points, etc.) Si vous souhaitez interpréter un nombre comme une chaîne, insérez-le entre guillemets ou utilisez la fonction intégrée str () de StyleBooks.
- Les littéraux tels que YES/Yes/yes/Y/y/NO/no/No/n/N, ON/On/on/OFF/Off/off et TRUE/true/truthy/-FALSE/False/false/falsely sont considérés comme des booléens et sont équivalents respectivement à true et false. Pour les interpréter comme des chaînes, incluez-les entre guillemets. Par exemple :
  - "YES"
  - "No"
  - "True"
  - "False"et ainsi de suite.

> **Remarque**
>
> Avant d'importer votre fichier StyleBook dans Citrix ADM, il est recommandé de vérifier si votre fichier est conforme au format YAML. Citrix vous recommande d'utiliser le validateur YAML intégré dans StyleBooks pour valider et importer le contenu YAML.
>
> Lors de la configuration de StyleBooks, vous ne pouvez utiliser que les ressources Nitro Configuration qui prennent en charge les opérations de **création** et de **suppression** (méthodes POST et DELETE HTTP). Pour plus d'informations, consultez la documentation sur les API Nitro.

Anatomie d'un StyleBook

Pour écrire des StyleBooks, vous devez comprendre la grammaire, la syntaxe et la structure des StyleBooks. Un StyleBook classique comporte les sections suivantes :

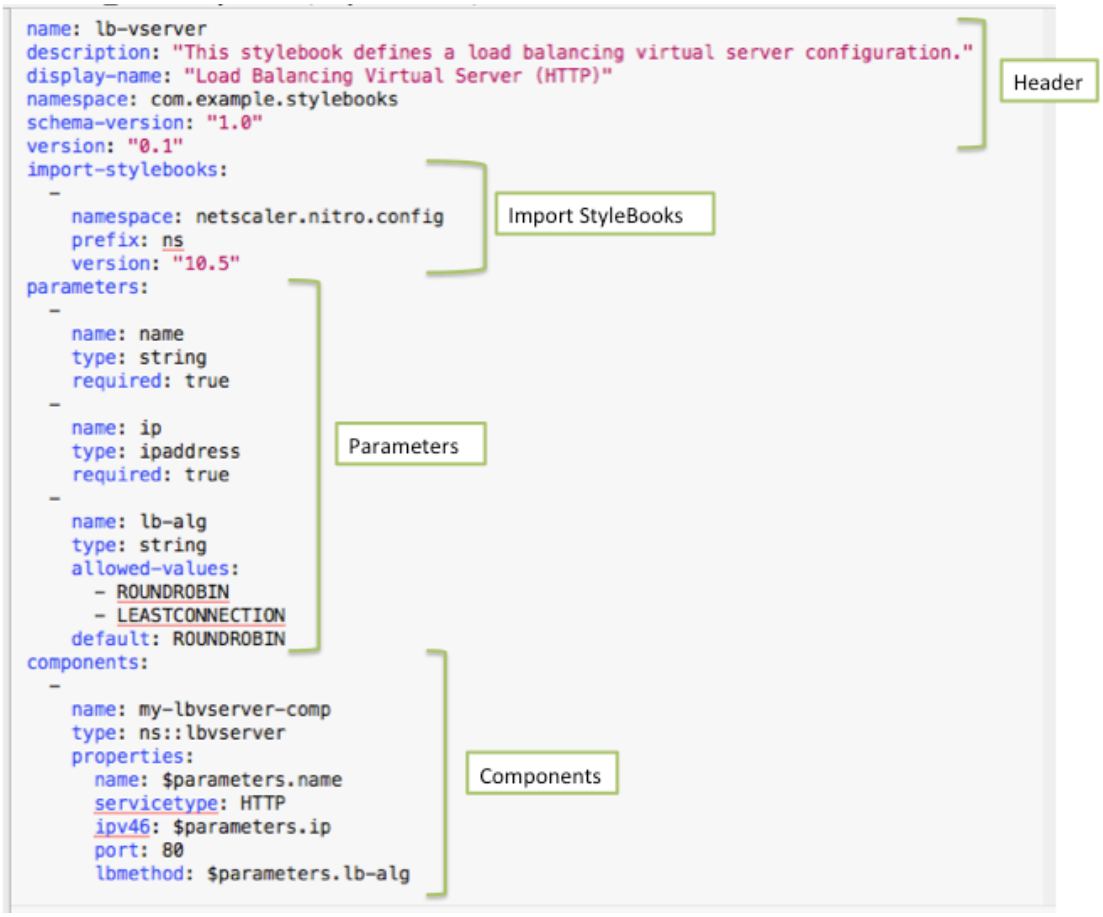
- **En-tête** : Cette section vous permet de définir l'identité d'un StyleBook et de décrire son rôle. Il s'agit d'une section obligatoire.
- **Importer des StyleBooks** : cette section vous permet de déclarer à quel autre StyleBook vous souhaitez faire référence depuis votre StyleBook actuel. L'importation de StyleBooks de configuration Citrix ADC NITRO ou d'autres StyleBooks est requise pour écrire un StyleBook. Il s'agit d'une section obligatoire.
- **Paramètres** : Cette section vous permet de définir les paramètres dont vous avez besoin dans votre StyleBook pour créer une configuration. Il décrit l'entrée que votre StyleBook prend. Il s'agit d'une section facultative.
- **Composants** : Cette section vous permet de définir les entités (objets de configuration) créées par le StyleBook pour une configuration spécifique. Cette section est considérée comme le cœur d'un StyleBook. Les composants utilisent généralement l'entrée fournie dans la section des paramètres pour adapter la configuration générée par le StyleBook. Il s'agit d'une section facultative.

  Un StyleBook peut comporter une section de paramètres, une section de composants, ou les deux. Un StyleBook contenant uniquement la section des paramètres est utile pour définir une liste de paramètres pouvant être utilisés par d'autres StyleBooks. Cela favorise la réutilisation des groupes de paramètres dans un ensemble de StyleBooks. Un StyleBook avec uniquement une section de composants peut être utilisé lorsque vous souhaitez spécifier les valeurs des attributs du StyleBook au lieu de définir des paramètres pour prendre en compte les entrées de l'utilisateur.
- **Sorties** : tandis que la section des paramètres définit les entrées du StyleBook, cette section facultative définit ses sorties. Dans cette section de sorties facultatives, vous pouvez spécifier

les composants que vous souhaitez exposer aux utilisateurs qui créent une configuration à partir de ce StyleBook et aux autres StyleBooks qui importent ce StyleBook. Les utilisateurs et les StyleBooks qui importent peuvent ensuite référencer les propriétés des composants exposés.

- **Opérations** : Un StyleBook peut contenir une section facultative pour activer Analytics dans Citrix ADM sur n'importe quel serveur virtuel faisant partie du StyleBook.

La figure suivante montre un contour simple d'un StyleBook.



Les exemples suivants vous aident à connaître la grammaire et la structure d'un StyleBook et à écrire des StyleBooks avec des niveaux de complexité croissants.

- StyleBook pour créer un serveur virtuel d'équilibrage de charge
- StyleBook pour créer une configuration d'équilibrage de charge de base
- Créer un StyleBook composite
- Personnalisez votre StyleBook en utilisant les attributs de l'interface

StyleBook pour créer un serveur virtuel d'équilibrage de charge

February 1, 2024

Dans cet exemple, vous concevez un StyleBook de base qui crée un serveur virtuel d'équilibrage de charge de type protocole HTTP et écoutant sur le port 80. Le nom du serveur virtuel, l'adresse IP et les paramètres de la méthode d'équilibrage de charge acceptent des valeurs définies par l'utilisateur, c'est-à-dire qu'il s'agit des paramètres du StyleBook.

En-tête

Les six premières lignes d'un StyleBook constituent la section d'en-tête. Dans cet exemple, la section d'en-tête est écrite comme suit :

```
name: lb-vserver
description: This StyleBook defines a load balancing virtual server
   configuration.
display-name: Load Balancing Virtual Server (HTTP)
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
<!--NeedCopy-->
```

La section d'en-tête inclut les informations suivantes :

- **nom** : nom pour ce StyleBook.
- **description** : Description définissant ce que fait ce StyleBook. Cette description apparaît sur Citrix ADM.
- **display-name** : nom descriptif du StyleBook qui apparaît sur Citrix ADM.
- **espace de noms** : un espace de noms fait partie d'un identificateur unique pour un StyleBook afin d'éviter les collisions de noms.
- **schema-version** : prend toujours la valeur « 1.0 » dans cette version.
- **version** : numéro de version du StyleBook. Vous pouvez modifier le numéro de version lorsque vous mettez à jour le StyleBook.

La combinaison du **nom** , de l'**espace** de noms et de la **version** identifie de manière unique un StyleBook dans le système. Vous ne pouvez pas avoir deux StyleBooks avec la même combinaison de nom, d'espace de noms et de version dans Citrix ADM. Cependant, vous pouvez avoir deux StyleBooks avec le même nom et la même version mais des espaces de noms différents, ou avec le même espace de noms et la même version mais des noms différents.

> **Remarque**
>
> Supposons que vous avez mis à jour votre StyleBook et que vous avez un numéro de version mis à jour. Maintenant, si vous faites référence (c'est-à-dire si vous importez) ce StyleBook dans d'autres StyleBooks, veillez à mettre à jour le numéro de version dans d'autres StyleBooks également, afin qu'ils utilisent la bonne version du StyleBook importé.

Importer des StyleBooks

La section qui suit l'en-tête s'appelle « import-stylebooks ». Dans cette section, vous devez déclarer l'espace de noms et le numéro de version de tout autre StyleBook auquel vous souhaitez faire référence dans votre StyleBook actuel. Cela vous permet d'importer et de réutiliser d'autres StyleBooks au lieu de recréer la même configuration dans votre propre StyleBook.

Dans cet exemple, la section import-stylebooks est écrite comme suit :

```
import-stylebooks:
 -
  namespace: netscaler.nitro.config
  prefix: ns
  version: "10.5"
<!--NeedCopy-->
```

Chaque StyleBook doit faire référence à l'espace de noms netscaler.nitro.config s'il utilise directement l'un des objets de configuration NITRO. Cet espace de noms contient tous les types de Citrix ADC NITRO, tels que LBVServer. Comme les versions 10.5 et ultérieures du logiciel sont prises en charge, vous pouvez utiliser votre StyleBook pour créer et exécuter des configurations sur n'importe quelle instance Citrix ADC exécutant la version 10.5 et les versions ultérieures.

Le préfixe utilisé dans la section import-stylebooks est un raccourci qui fait référence à la combinaison de l'espace de noms et de la version. Dans ce cas, ns fait référence à netscaler.nitro.config de la version 10.5. Dans les dernières sections de votre StyleBook, au lieu d'utiliser l'espace de noms et la version pour faire référence au StyleBook importé, vous pouvez utiliser la chaîne de préfixe choisie, par exemple ns, dans l'exemple ci-dessus.

La version utilisée dans les StyleBooks est la version NITRO de Citrix ADC. Un StyleBook basé sur Nitro version X peut être utilisé pour configurer n'importe quel Citrix ADC version X ou supérieure.

> **Remarque**
>
> Pour vous assurer que vos StyleBooks peuvent être utilisés pour configurer n'importe quelle instance Citrix ADC de la version 10.5 ou ultérieure, Citrix recommande que, pour une compatibilité maximale, vous importez l'espace de noms Nitro 10.5 dans vos StyleBooks qui utilisent directement les StyleBooks intégrés à Nitro (espace de noms : netscaler.nitro.config, version : 10.5).

Il est important qu'un StyleBook qui importe d'autres StyleBooks soit basé sur une version Nitro qui est à la même version ou supérieure que les StyleBooks qu'il importe. Par exemple, un StyleBook basé sur la version 10.5 de Nitro ne peut pas dépendre d'un StyleBook basé sur la version 11.1, ni l'utiliser ou l'importer. Mais un StyleBook basé sur la version 11.1 peut importer un StyleBook basé sur n'importe quelle version inférieure à 11.1.

Il est également possible qu'un StyleBook n'importe pas du tout l'espace de noms Nitro. Cela signifie qu'un StyleBook n'a pas besoin de définir directement les composants Nitro, mais peut importer (dépendre) les StyleBooks qui définissent les composants Nitro. Le StyleBook qui importe d'autres StyleBooks acquiert toujours la version Nitro la plus élevée dans la hiérarchie de ses dépendances et peut donc être utilisé pour configurer des Citrix ADC de cette version ou supérieure.

Paramètres

La section des paramètres vous permet de déclarer tous les paramètres dont vous avez besoin dans votre StyleBook. En tant que développeur de StyleBook, vous devez décider de l'entrée que vous souhaitez que les utilisateurs de votre StyleBook spécifient. Dans cet exemple, vous avez créé votre StyleBook de manière à ce que ses utilisateurs fournissent le nom du serveur virtuel, son adresse IP et la méthode d'équilibrage de charge.

La section des paramètres se présenterait comme suit :

```
parameters:
 -
  name: name
  type: string
  label: Application Name
  description: Name of the application configuration.
  required: true

 -
  name: ip
  type: ipaddress
  label: Application Virtual IP (VIP)
  description: Application VIP that the clients access.
  required: true

-
  name: lb-alg
  type: string
  label: LoadBalancing Algorithm
  description: Choose the load balancing algorithm (method) used for
     load balancing client request between the application servers.
  allowed-values:
   - ROUNDROBIN
   - LEASTCONNECTION
   default: ROUNDROBIN
<!--NeedCopy-->
```


> **Remarque**
>
> Si vous ne fournissez pas l'étiquette d'un paramètre, Citrix ADM utilise l'attribut name lors de l'affichage de ce paramètre. Vous devez toujours définir une étiquette pour vos paramètres afin de pouvoir contrôler leur affichage dans Citrix ADM.
>
> Toutefois, lors de l'utilisation des API, le paramètre est désigné par son nom.

Dans cette section, vous avez déclaré trois paramètres indiqués par leurs valeurs d'attribut **name** : **name** pour le nom du serveur virtuel, **ip** pour l'adresse IP du serveur virtuel, et **lb-alg** pour la méthode d'équilibrage de charge.

- **type**. Type de valeur que ces paramètres peuvent prendre. Par exemple, name et lb-alg peuvent prendre une valeur de chaîne et la valeur IP doit être de type adresse IP. Les paramètres d'un StyleBook peuvent être de l'un des types intégrés suivants :
- **chaîne**. Une panoplie de personnages. Si aucune longueur n'est spécifiée, la valeur de la chaîne peut prendre n'importe quel nombre de caractères. Toutefois, vous pouvez limiter la longueur d'un type de chaîne en utilisant les attributs min-length et max-length.
- **numéro**. Un nombre entier. Vous pouvez spécifier le nombre minimum et maximum que ce type peut prendre en utilisant les attributs min-value et max-value.
- **booléen**. Peut être vrai ou faux. Notez également que tous les littéraux sont considérés par YAML comme des booléens (par exemple, Oui ou Non).
- **ipaddress**. Chaîne qui représente une adresse IPv4 ou IPv6 valide.
- **port TCP**. Nombre compris entre 0 et 65535 qui représente un port TCP ou UDP.
- **password**. Une valeur de chaîne opaque/secrète. Lorsque Citrix ADM affiche une valeur pour ce paramètre, elle s'affiche sous la forme d'astérisques (*****).
- **Certfile**. Fichier de certificat.
- **fichier clé**. Fichier de clé privée du certificat.
- **fichier**. Un paramètre de ce type nécessite que l'utilisateur télécharge un fichier, par exemple un certificat ou un fichier clé.
- **objet**. Se compose de plusieurs éléments et chacun de ces éléments est un paramètre. Ce type peut être utilisé pour regrouper plusieurs paramètres associés sous un paramètre parent.
- **requis**. Indique si un paramètre est obligatoire ou facultatif. S'il est défini sur true, le paramètre est obligatoire et l'utilisateur doit fournir une valeur pour ce paramètre lors de la création de configurations à l'aide de ce StyleBook. Par défaut, tous les paramètres sont facultatifs. Dans cet exemple, le **nom** et l'**adresse IP** sont des paramètres obligatoires tandis que **lb-alg** est un paramètre facultatif dont la valeur par défaut est « ROUNDROBIN ».

Utilisez l'attribut **default** pour attribuer une valeur par défaut à un paramètre facultatif. Lors de la création d'une configuration, si un utilisateur ne spécifie aucune valeur, la valeur par défaut est utilisée. Par exemple, pour le paramètre **lb-alg**, la valeur par défaut est ROUNDROBIN.

Utilisez l'attribut **allowed-values** pour définir des valeurs spécifiques parmi lesquelles un utilisateur

peut choisir lors de la création d'une configuration. Dans cet exemple, vous avez spécifié deux valeurs pour le paramètre **lb-alg** : ROUNDROBIN et LEASTCONNECTION.

Lorsque vous importez votre StyleBook et l'utilisez, Citrix ADM affiche un formulaire avec ces trois paramètres. Les champs affichés pour name et ip permettent la saisie du type de valeur de chaîne et d'adresse IP, et le champ lb-alg est affiché sous forme de liste déroulante avec ROUNDROBIN sélectionné comme valeur par défaut.

> **Remarque**
>
> Outre les types intégrés, un paramètre peut avoir un autre type StyleBook. C'est une façon de réutiliser les paramètres définis dans d'autres StyleBooks.

Composants

La dernière section de ce StyleBook s'appelle la section Composants et est considérée comme la section la plus importante du StyleBook. Dans cette section, vous définissez les objets de configuration qui doivent être créés par le SyleBook.

Pour cet exemple, vous devez écrire la section des composants comme suit :

```
components:
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

Cet exemple ne contient qu'un seul composant. Les principaux attributs d'un composant sont le nom, le type et les propriétés. Le type d'un composant détermine les propriétés qu'il fournit. Les composants sont de deux types :

- **Type intégré**. Ce type est fourni par le système et vous n'avez pas à le définir. Par exemple, les types d'entités NITRO « lbvserver » ou « servicegroup ». Dans cet exemple, vous utilisez un type de composant intégré.
- **Type composite**. Ce type est le StyleBook que vous avez créé et importé dans Citrix ADM, ou le StyleBook par défaut fourni avec Citrix ADM. Vous pouvez en savoir plus sur les StyleBooks composites dans Créer un StyleBook composite.

Dans cet exemple, vous avez défini un composant appelé **lbvserver-comp**. Ce composant est du type **ns : :lbvserver** (un type Nitro intégré), où « ns » est le préfixe qui fait référence à l'es-

pace de noms netscaler.nitro.config et à la version 10.5 que vous avez spécifiés dans la section import-stylebooks, et « lbvserver » est une ressource Nitro dans cet espace de noms.

Les **propriétés** définies ici sont les attributs de la ressource « lbvserver ». Pour en savoir plus sur toutes les ressources Citrix ADC Nitro disponibles et leurs attributs, consultez la documentation de l'API REST Citrix ADC NITRO.

Les propriétés de cette section incluent les attributs obligatoires de la ressource « lbvserver » et vous permettent de spécifier des valeurs pour ces attributs. Dans cet exemple, vous spécifiez des valeurs statiques pour le type de service et le port alors que les propriétés name, ipv46 et lbmethod obtiennent leurs valeurs à partir des paramètres d'entrée. Dans le reste du StyleBook, vous pouvez faire référence aux noms de paramètres définis dans la section parameters à l'aide de l'expression **$parameters.<parameter-name>**, par exemple, **$parameters.ip**.

> **Remarque**
>
> Par convention, le préfixe « ns » est toujours utilisé pour désigner un espace de noms Citrix ADC Nitro dans la section « import-stylebooks ». Bien que ce ne soit pas obligatoire, Citrix recommande d'utiliser la même convention dans vos propres StyleBooks pour des raisons de cohérence.

Créez votre StyleBook

Maintenant que vous avez défini toutes les sections requises de ce StyleBook, regroupez-les toutes pour créer votre premier StyleBook. Copiez et collez le contenu du StyleBook dans un éditeur de texte, puis enregistrez le fichier sous le **nom lb-vserver.yaml**. Citrix vous recommande d'utiliser le validateur YAML intégré dans StyleBooks pour valider et importer le contenu YAML.

Le contenu complet du fichier lb-vserver.yaml est reproduit ci-dessous :

```yaml
name: lb-vserver
namespace: com.example.stylebook
version: "1.0"
display-name: Load Balancing Virtual Server (HTTP)
description: "This stylebook defines a very simple load balancing HTTP
   virtual server configuration"
schema-version: "1.0"

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  version: "10.5"
  prefix: ns
 -
  namespace: com.citrix.adc.stylebooks
  version: "1.0"
  prefix: stlb

parameters:
```



```
19   -
20    name: name
21    label: "Application Name"
22    description: "Give a name to the application configuration."
23    type: string
24    required: true
25   -
26    name: vip-ipaddress
27    label: "Load Balancer IP Address"
28    description: "The Application VIP that clients access"
29    type: ipaddress
30    required: true
31   -
32    name: lb-alg
33    label: LB Algorithm
34    description: Load Balancing Algorithm
35    type: string
36    default: ROUNDROBIN
37    allowed-values:
38     - ROUNDROBIN
39     - LEAST-CONNECTION
40
41 components:
42  -
43    name: lbvserver-comp
44    description: This StyleBook component (a Builtin Nitro StyleBook)
         builds a Citrix ADC load balancing virtual server configuration
         object.
45    type: ns::lbvserver
46    properties:
47     name: $parameters.name
48     ipv46: $parameters.vip-ipaddress
49     lbmethod: $parameters.lb-alg
50     servicetype: HTTP
51     port: 80
52 <!--NeedCopy-->
```

Pour commencer à utiliser votre StyleBook pour créer des configurations, vous devez l'importer dans Citrix ADM, puis l'utiliser. Pour plus d'informations, consultez Comment utiliser des StyleBooks définis par l'utilisateur.

Vous pouvez également importer ce StyleBook dans d'autres StyleBooks (à l'aide de la construction Import-Stylebooks). Vous pouvez également modifier ce StyleBook pour inclure plus de paramètres et de composants comme décrit dans la section suivante.

StyleBook pour créer une configuration d'équilibrage de charge de base

February 1, 2024

Dans l'exemple précédent, vous avez créé un StyleBook de base pour créer un serveur virtuel d'équilibrage de charge. Vous pouvez enregistrer ce StyleBook sous un autre nom, puis le mettre à jour pour inclure des paramètres et des composants supplémentaires pour une configuration de base d'équilibrage de charge. Enregistrez ce fichier StyleBook sous le **nom basic-lb-config.yaml**.

Dans cette section, vous allez concevoir un nouveau StyleBook qui crée une configuration d'équilibrage de charge comprenant un serveur virtuel d'équilibrage de charge, un groupe de services et une liste de services. Il lie également les services au groupe de services et lie le groupe de services au serveur virtuel.

En-tête

Pour créer ce StyleBook, vous devez commencer par mettre à jour la section d'en-tête. Cette section est similaire à celle que vous avez créée pour le serveur virtuel d'équilibrage de charge StyleBook. Dans la section d'en-tête, remplacez la valeur du **nom** par basic-lb-config. Mettez également à jour **la description** et le **nom d'affichage** pour décrire correctement ce StyleBook. Il n'est pas nécessaire de modifier l'espace de **noms** et les valeurs de **version** . Comme vous avez modifié le nom, la combinaison du nom, de l'espace de noms et de la version crée un identifiant unique pour ce StyleBook dans le système.

```
name: basic-lb-config
description: This StyleBook defines a simple load balancing
   configuration.
display-name: Load Balancing Configuration
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
<!--NeedCopy-->
```

Importer des StyleBooks

La section import-stylebooks reste la même. Il fait référence à l'espace de noms netscaler.nitro.config pour utiliser les objets de configuration Nitro.

```
import-stylebooks:
 -
 namespace: netscaler.nitro.config
 prefix: ns
 version: "10.5"
<!--NeedCopy-->
```


Paramètres

Vous devez mettre à jour la section des paramètres pour ajouter deux paramètres supplémentaires pour définir la liste des services ou serveurs et le port sur lequel les services écoutent. Les trois premiers paramètres, name, ip et lb-alg, restent les mêmes.

```
parameters:
 -
 name: name
 type: string
 label: Application Name
 description: Name of the application configuration
 required: true
  -
   name: ip
   type: ipaddress
   label: Application Virtual IP (VIP)
   description: Application VIP that the clients access
   required: true
  -
   name: lb-alg
   type: string
   label: LoadBalancing Algorithm
   description: Choose the load balancing algorithm used for load
      balancing client requests between the application servers.
     allowed-values:
     - ROUNDROBIN
     - LEASTCONNECTION
      default: ROUNDROBIN
  -
   name: svc-servers
   type: ipaddress[]
   label: Application Server IPs
   description: The IP addresses of all the servers of this application
   required: true
  -
   name: svc-port
   type: tcp-port
   label: Server Port
   description: The TCP port open on the application servers to receive
       requests.
   default: 80
<!--NeedCopy-->
```

Dans cet exemple, le paramètre **svc-servers** est ajouté pour accepter une liste d'adresses IP des services qui représentent les serveurs principaux de l'application. Ceci est un paramètre obligatoire comme indiqué par **requis : true**. Le deuxième paramètre, **svc-port**, indique le numéro de port sur lequel les serveurs écoutent. Le numéro de port par défaut est 80 pour le paramètre svc-port, s'il n'est pas spécifié par l'utilisateur.

Composants

Vous devez également mettre à jour la section des composants pour définir des composants supplémentaires afin qu'ils utilisent les deux nouveaux paramètres et créent la configuration complète d'équilibrage de charge.

Pour cet exemple, vous devez écrire la section des composants comme suit :

```
components:
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name + "-lb"
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg

components:
 -
  name: svcg-comp
  type: ns::servicegroup
  properties:
   name: $parameters.name + "-svcgrp"
   servicetype: HTTP

components:
 -
  name: lbvserver-svg-binding-comp
  type: ns::lbvserver_servicegroup_binding
  properties:
   name: $parent.parent.properties.name
   servicegroupname: $parent.properties.name
 -
  name: members-svcg-comp
  type: ns::servicegroup_servicegroupmember_binding
  repeat: $parameters.svc-servers
  repeat-item: srv
  properties:
   ip: $srv
   port: str($parameters.svc-port)
   servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

Dans cet exemple, le composant d'origine **lbvserver-comp** (de l'exemple précédent) possède désormais un composant enfant appelé **svcg-comp**. De plus, le composant **svcg-comp** contient deux composants enfants. L'imbrication d'un composant dans un autre composant permet au composant imbriqué de créer des objets de configuration en se référant aux attributs du composant parent. Le composant imbriqué peut créer un ou plusieurs objets pour chaque objet créé dans le composant parent.

Le composant **svcg-comp** est utilisé pour créer un groupe de services sur l'instance Citrix ADC en utilisant les valeurs fournies pour les attributs de la ressource « servicegroup ». Dans cet exemple, vous spécifiez une valeur statique pour le type de service, tandis que name obtient sa valeur à partir du paramètre d'entrée. Vous faites référence au **nom** du paramètre défini dans la section des paramètres en utilisant la notation **$parameters.name + "-svcgrp"**, où **-svcgrp** est ajouté (concaténé) au nom défini par l'utilisateur.

Le composant **svcg-comp** a deux composants enfants, **lbvserver-svg-binding-comp** et **members-svcg-comp**.

Le premier composant enfant, **lbvserver-svg-binding-comp**, est utilisé pour lier un objet de configuration entre le groupe de services créé par son composant parent et le serveur virtuel d'équilibrage de charge (lbvserver) créé par le composant parent du parent. La notation $parent, également appelée référence parente, est utilisée pour faire référence aux entités dans les composants parents. Par exemple, **servicegroupname : $parent.properties.name** fait référence au groupe de services créé par le composant parent **svcg-comp**, et **name : $parent.parent.properties.name** fait référence au serveur virtuel créé par le composant parent **lbvserver-comp**du parent.

Le composant **members-svcg** est utilisé pour lier des objets de configuration entre la liste des services au groupe de services créé par le composant parent. La création de plusieurs objets de configuration de liaison est réalisée en utilisant la construction de **répétition** de StyleBook pour parcourir la liste des serveurs spécifiés dans le paramètre **svc-servers**. Au cours de l'itération, ce composant StyleBook crée un objet de configuration Nitro de type **servicegroup_servicegroupmember_binding** pour chaque service (appelé srv dans la construction **repeat-item**) du groupe de services, et il définit l'attribut **IP de chaque objet de configuration Nitro sur l'adresse IP** du serveur correspondant.

En général, vous pouvez utiliser les constructions **repeat** et **repeat-item** d'un composant pour que ce composant génère plusieurs objets de configuration du même type. Vous pouvez attribuer un nom de variable à la construction **repeat-item**, par exemple, srv, pour désigner la valeur actuelle dans l'itération. Ce nom de variable est référencé dans les propriétés du même composant ou dans les composants enfants comme **$<varname>**, par exemple $srv.

Dans l'exemple ci-dessus, vous avez utilisé l'imbrication de composants les uns aux autres pour construire facilement cette configuration. Dans ce cas particulier, l'imbrication des composants n'était pas le seul moyen de créer la configuration. Vous auriez pu obtenir le même résultat sans imbrication, comme indiqué ci-dessous :

```
components:
 -
  name: members-svcg-comp
  type: ns::servicegroup_servicegroupmember_binding
  repeat: $parameters.svc-servers
  repeat-item: srv
  properties:
   ip: $srv
   port: str($parameters.svc-port)
```



```
    servicegroupname: $components.svcg-comp.properties.name
  -
   name: lbvserver-svg-binding-comp
   type: ns::lbvserver_servicegroup_binding
   properties:
    name: $components.lbvserver-comp.properties.name
    servicegroupname: $components.svcg-comp.properties.name
  -
   name: lbvserver-comp
   type: ns::lbvserver
   properties:
    name: $parameters.name + "-lb"
    servicetype: HTTP
    ipv46: $parameters.ip
    port: 80
    lbmethod: $parameters.lb-alg
  -
   name: svcg-comp
   type: ns::servicegroup
   properties:
   name: $parameters.name + "-svcgrp"
   servicetype: HTTP
<!--NeedCopy-->
```

Ici, tous les composants sont au même niveau (c'est-à-dire qu'ils ne sont pas imbriqués) mais le résultat obtenu (la configuration Citrix ADC générée) est le même que celui des composants imbriqués utilisés précédemment. En outre, l'ordre dans lequel les composants sont déclarés dans le StyleBook n'a pas d'incidence sur l'ordre de création des objets de configuration. Dans cet exemple, les composants **svcg-comp et**lbvserver-comp****, même s'ils ont été déclarés en dernier, doivent être construits avant de générer le deuxième composant **lbvserver-svg-binding-comp car le second composant contient**des références directes à ces composants.

> **Remarque**
>
> Par convention, les noms des StyleBooks, des paramètres, des substitutions, des composants et des sorties sont en minuscules. Lorsqu'ils contiennent plusieurs mots, ils sont séparés par un caractère « - ». Par exemple, « lb-bindings », « app-name », « rewrite-config », etc. Une autre convention consiste à suffixer les noms des composants avec la chaîne « -comp ».

Sorties

La dernière section que vous pouvez ajouter au nouveau StyleBook est la section des sorties dans laquelle vous spécifiez ce que ce StyleBook expose à ses utilisateurs (ou dans d'autres StyleBooks) après avoir été utilisé pour créer une configuration. Par exemple, vous pouvez spécifier dans la section des sorties d'exposer les objets de configuration lbvserver et servicegroup qui seraient créés par ce StyleBook.


```
outputs:
 -
  name: lbvserver-comp
  value: $components.lbvserver-comp
  description: The component that builds the Nitro lbvserver
     configuration object
 -
  name: servicegroup-comp
  value: $components.svcg-comp
  description: The component that builds the Nitro servicegroup
     configuration object
<!--NeedCopy-->
```

La section des sorties d'un StyleBook est facultative. Un StyleBook n'a pas besoin de renvoyer des sorties. Cependant, en renvoyant certains composants internes sous forme de sorties, cela donne aux StyleBooks qui importent ce StyleBook plus de flexibilité, comme vous pouvez le constater lors de la création d'un StyleBook composite.

> **Remarque**
>
> Il est recommandé d'exposer un composant entier du StyleBook dans la section des sorties, plutôt qu'une seule propriété d'un composant (par exemple, exposez l'intégralité de $components.lbvserver-comp plutôt que le nom $components.lbvserver-comp.properties.name). Ajoutez également une description à la sortie expliquant ce que représente la sortie spécifique.

Créez votre StyleBook

Maintenant que vous avez défini toutes les sections requises de ce StyleBook, regroupez-les toutes pour créer votre second StyleBook. Vous avez déjà enregistré ce fichier StyleBook en tant que **basic-lb-config.yaml**. Citrix vous recommande d'utiliser le validateur YAML intégré à la page StyleBooks pour valider et importer le contenu YAML.

Le contenu complet du fichier **basic-lb-config.yaml** est reproduit ci-dessous :

```
name: basic-lb-config
namespace: com.example.stylebooks
version: "0.1"
display-name: Load Balancing Configuration
description: This StyleBook defines a simple load balancing
   configuration.
schema-version: "1.0"

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  version: "10.5"
  prefix: ns
parameters:
 -
```



```
15    name: name
16    type: string
17    label: Application Name
18    description: Give a name to the application configuration.
19    required: true
20   -
21    name: ip
22    type: ipaddress
23    label: Application Virtual IP (VIP)
24    description: The Application VIP that clients access
25    required: true
26   -
27    name: lb-alg
28    type: string
29    label: LoadBalancing Algorithm
30    description: Choose the loadbalancing algorithm (method) used for
         loadbalancing client requests between the application servers.
31    allowed-values:
32       - ROUNDROBIN
33       - LEASTCONNECTION
34    default: ROUNDROBIN
35   -
36    name: svc-servers
37    type: ipaddress[]
38    label: Application Server IPs
39    description: The IP addresses of all the servers of this application
40    required: true
41
42  components:
43   -
44    name: lbvserver-comp
45    type: ns::lbvserver
46    properties:
47     name: $parameters.name + "-lb"
48     servicetype: HTTP
49     ipv46: $parameters.ip
50     port: 80
51     lbmethod: $parameters.lb-alg
52   -
53    name: svcg-comp
54    type: ns::servicegroup
55    properties:
56      servicegroupname: $parameters.name + "-svcgrp"
57      servicetype: HTTP
58
59   -
60    name: lbvserver-svg-binding-comp
61    type: ns::lbvserver_servicegroup_binding
62    properties:
63     name: $components.lbvserver-comp.properties.name
64     servicegroupname: $components.svcg-comp.properties.servicegroupname
65   -
66    name: members-svcg-comp
```



```
67    type: ns::servicegroup_servicegroupmember_binding
68    repeat: $parameters.svc-servers
69    repeat-item: srv
70    properties:
71     ip: $srv
72     port: 80
73     servicegroupname: $components.svcg-comp.properties.servicegroupname
74  outputs:
75  -
76    name: lbvserver-comp
77    value: $components.lbvserver-comp
78    description: The component that builds the Nitro lbvserver
         configuration object
79  -
80    name: servicegroup-comp
81    value: $components.svcg-comp
82    description: The component that builds the Nitro servicegroup
         configuration object
83  <!--NeedCopy-->
```

Pour commencer à utiliser votre StyleBook pour créer des configurations, vous devez l'importer dans Citrix ADM, puis l'utiliser. Pour plus d'informations, consultez Comment utiliser des StyleBooks définis par l'utilisateur.

Vous pouvez également importer ce StyleBook dans d'autres StyleBooks et utiliser ses propriétés comme décrit dans la section suivante.

Créer un StyleBook composite

February 1, 2024

Une caractéristique importante et puissante de StyleBooks est qu'ils peuvent être utilisés comme blocs de construction pour d'autres StyleBooks. Un StyleBook peut être importé dans un autre StyleBook et il peut être considéré comme un **type** utilisé par les composants du second StyleBook, similaire à un StyleBook intégré à Nitro.

Par exemple, vous pouvez utiliser le StyleBook **basic-lb-config** que vous avez créé dans la section précédente, pour créer un autre StyleBook appelé **composite-example** . Pour utiliser le StyleBook « basic-lb-config », vous devez l'importer dans le nouveau StyleBook dans la section import-stylebooks.

Créez votre StyleBook

Le nouveau StyleBook se présente comme suit :


```
name: composite-example
namespace: com.example.stylebooks
version: "0.1"
display-name: Load Balancing Virtual Server (HTTP/RoundRobin)
description: This StyleBook defines a RoundRobin load balancing
   configuration with a monitor.
schema-version: "1.0"
import-stylebooks:
  -
   namespace: netscaler.nitro.config
   version: "10.5"
   prefix: ns
  -
   namespace: com.example.stylebooks
   version: "0.1"
   prefix: stlb
parameters:
  -
    name: name
    type: string
    label: Application Name
    description: Give a name to the application configuration.
    required: true
  -
    name: ip
    type: ipaddress
    label: Application Virtual IP (VIP)
    description: The Application VIP that clients access
    required: true
  -
    name: svc-servers
    type: ipaddress[]
    label: Application Server IPs
    description: The IP addresses of all the servers of this
       application
    required: true

  -
    name: response-code
    type: string[]
    label: List of Response Codes
    description: List of Response Codes - Provide a list of response
       codes in integer.

components:
  -
    name: basic-lb-comp
    type: stlb::basic-lb-config
    description: This component's type is another StyleBook that builds
        the NetScaler lbvserver, servicegroups and services
       configuration objects.
    properties:
     name: $parameters.name
```



```
49        ip: $parameters.ip
50        svc-servers: $parameters.svc-servers
51     -
52        name: monit-comp
53        type: ns::lbmonitor
54        description: This component is a basic Nitro type (a Builtin
              StyleBook) that builds the NetScaler monitor configuration
              object.
55        properties:
56          monitorname: $parameters.name + "-mon"
57          type: HTTP
58          respcode: $parameters.response-code
59          httprequest: "'GET /'"
60          lrtm: ENABLED
61          secure: "YES"
62
63        components:
64           -
65             name: monit-svcgrp-bind-comp
66             type: ns::servicegroup_lbmonitor_binding
67             properties:
68               servicegroupname: $components.basic-lb-comp.outputs.
                     servicegroup-comp.properties.servicegroupname
69               monitor_name: $parent.properties.monitorname
70  <!--NeedCopy-->
```

Dans la section import-stylebooks, vous importez le StyleBook basic-lb-config en utilisant son espace de noms et sa version, désignés par le préfixe « stlb ».

Dans la section Composants, deux composants sont définis. Le premier composant est de type **stlb : :basic-lb-config**, où « basic-lb-config » est le nom du StyleBook que vous avez créé dans StyleBook pour créer une configuration d'équilibrage de charge de base. Les propriétés définies pour ce composant correspondent aux paramètres obligatoires déclarés dans le StyleBook basic-lb-config. Vous pouvez toutefois utiliser n'importe quel paramètre du StyleBook (obligatoire et facultatif). Au lieu de reconstruire un serveur lbvserver, un groupe de services et des liaisons de service et de groupe de services, vous importez le StyleBook qui fait tout cela en tant que composant et vous l'utilisez pour créer ces objets de configuration dans le nouveau StyleBook.

StyleBook ajoute un deuxième composant, « monit-comp », qui utilise les attributs de la ressource Nitro « lbmonitor » (un StyleBook intégré) pour créer un objet de configuration de moniteur. Il possède également un sous-composant « monit-svcgrp-bind-comp » pour créer l'objet de configuration de liaison qui lie le moniteur au groupe de services créé dans le premier composant. **Étant donné que le composant servicegroup créé dans le StyleBook « basic-lb-config » est exposé en tant que sortie, ce StyleBook peut y accéder à l'aide de l'expression $components.basic-lb-comp.outputs.servicegroup-comp.** Ceci est un exemple de la façon dont la section des sorties peut être utilisée par les StyleBooks d'importation pour avoir accès aux composants des StyleBooks importés auxquels ils n'auraient pas pu accéder autrement.

Ensuite, copiez et collez le contenu du StyleBook dans un éditeur de texte, puis enregistrez le fichier sous le **nom composite-example.yaml**. Assurez-vous de valider le contenu YAML avant d'importer le fichier dans Citrix ADM. Ensuite, importez-le dans Citrix ADM et créez une ou plusieurs configurations à l'aide de ce StyleBook.

Citrix vous recommande d'utiliser le validateur YAML intégré dans StyleBooks pour valider et importer le contenu YAML.

Utiliser les attributs de l'interface graphique dans un StyleBook personnalisé

February 1, 2024

Vous pouvez ajouter des attributs GUI dans la section Paramètres de votre StyleBook pour rendre les champs intuitifs lorsqu'ils sont affichés sur Citrix Application Delivery Management (ADM).

Exemple. Vous pouvez ajouter un nom descriptif au paramètre à l'aide de l'attribut label et ajouter une infobulle pour ce paramètre à l'aide de l'attribut description.

```
name: ip
label: Virtual Server IP Address
description: IP address of the virtual server that represents the load
   balanced application.
type: ipaddress
required: true
<!--NeedCopy-->
```

Exemple. Si vous avez un paramètre de type object, vous pouvez définir la mise en page à l'aide de l'attribut **gui** . Dans cet exemple, la mise en page est un objet pliable où les champs sont affichés en deux colonnes.

```
name: svcg-advanced
label: Advanced Application Server Settings
type: object
required: false
gui:
 collapse_pane: true
 columns: 2
<!--NeedCopy-->
```

Exemple. Certains StyleBooks sur Citrix ADM sont utilisés uniquement comme blocs de construction pour d'autres StyleBooks. Vous pouvez également ne pas vouloir que les utilisateurs créent des configurations directement à partir de ces StyleBooks. Parce que ces StyleBooks doivent être utilisés dans le cadre d'autres StyleBooks. Marquez le StyleBook comme privé pour vous assurer que le StyleBook n'est pas utilisé directement pour créer des configurations dans l'interface graphique Citrix ADM.


```
name: basic-lb-config
description: This stylebook defines a simple load balancing
   configuration.
display-name: Load Balancing Configuration
namespace: com.example.stylebooks
private: true
schema-version: "1.0"
version: "0.1"
<!--NeedCopy-->
```

Importer des StyleBooks personnalisés

February 1, 2024

Après avoir créé votre StyleBook, vous devez l'importer dans Citrix Application Delivery Management (ADM) pour l'utiliser. Citrix ADM vous permet d'importer un seul StyleBook sous forme YAML ou plusieurs fichiers StyleBook YAML sous la forme d'un bundle dans un formulaire .zip, .tgz ou .gz. Le système Citrix ADM valide vos StyleBooks lors de l'importation. Le StyleBook est maintenant prêt à être utilisé pour créer des configurations.

Citrix ADM dispose également d'un éditeur YAML intégré que vous pouvez utiliser pour composer le contenu de StyleBook YAML. L'éditeur YAML vous permet de valider vos constructions YAML à partir de l'interface graphique Citrix ADM elle-même. Vous n'avez pas besoin d'utiliser un outil distinct pour ces vérifications de validation. Le contenu est validé par rapport aux normes YAML et tout écart est mis en évidence. Vous pouvez ensuite corriger le contenu et essayer d'importer le StyleBook dans Citrix ADM. L'éditeur YAML intégré offre deux avantages lors de la rédaction de votre propre StyleBook.

- **Code couleur**. L'éditeur affiche le contenu StyleBook analysé selon les directives YAML, et le codage couleur vous aide à différencier facilement entre les clés et les valeurs définies dans le contenu YAML.
- **Validation YAML**. Le contenu est validé pour toutes les erreurs YAML lorsque vous saisissez et toute déviation est immédiatement mise en surbrillance. Cette validation vous permet d'écrire du texte conforme aux directives YAML avant même d'importer le StyleBook dans l'ADM.

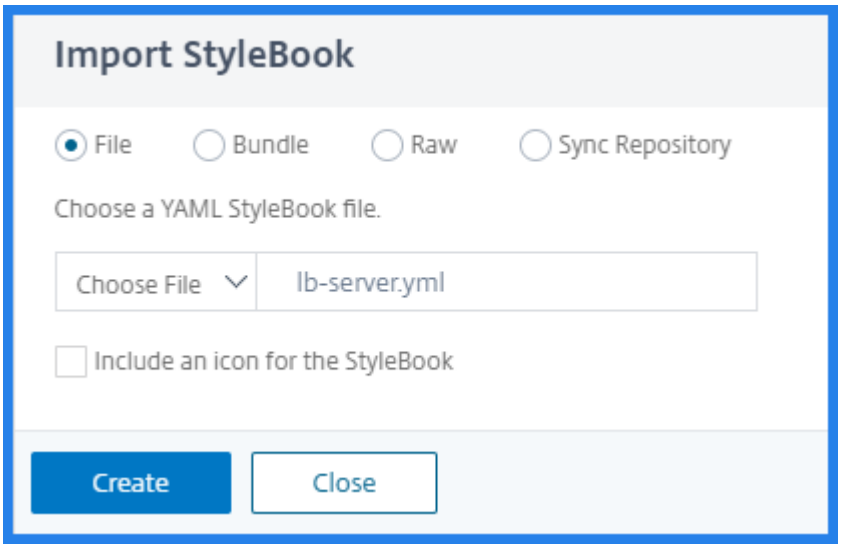
> **Remarque**
>
> Actuellement, l'éditeur valide le contenu conformément aux directives YAML. Il ne valide pas l'exactitude du code et les erreurs typographiques.

Pour importer votre StyleBook

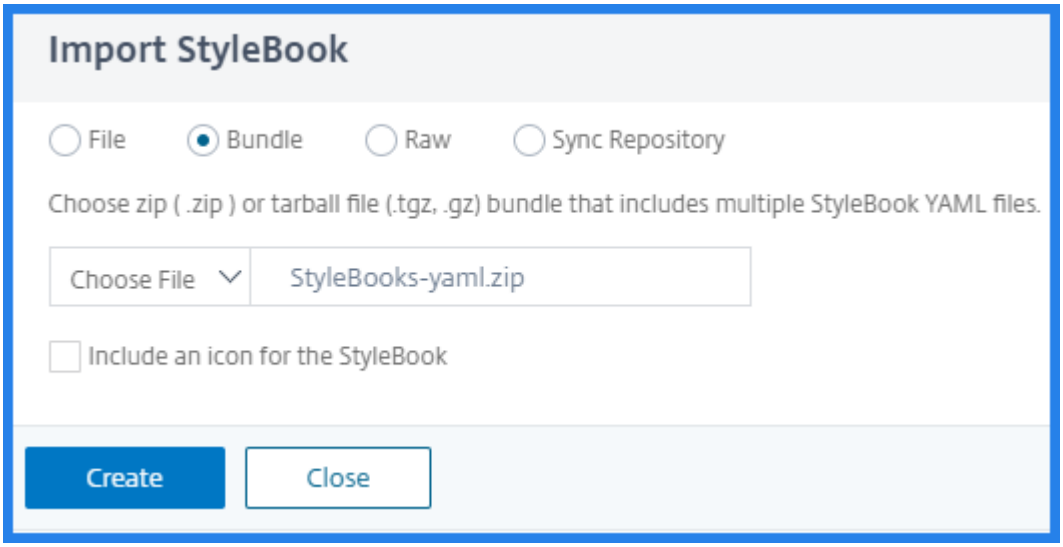
1. Dans Citrix ADM, accédez à **Applications** > **Configuration** > **StyleBooks**, puis cliquez sur **Importer un nouveau**StyleBook.
2. Cliquez sur l'une des options suivantes pour importer un StyleBook.

   - **Fichier** : sélectionnez le fichier requis ou l'ensemble de fichiers à partir de votre stockage local.

     > **Remarque**
     >
     > Dans cet exemple, importez le `lb-vserver.yml` StyleBook que vous avez créé dans StyleBook pour créer un serveur virtuel d'équilibrage de charge.

   - **Bundle** - Citrix ADM vous permet d'importer plusieurs StyleBooks au format YAML. Vous pouvez importer plusieurs fichiers YAML StyleBook compressés au format zip (.zip) ou tarball (.tgz, .gz).



Vous pouvez désormais inclure des icônes à chaque StyleBook de l'offre groupée. Assurez-vous d'avoir le dossier des ressources contenant des icônes au format PNG, GIF ou JPEG. Si le nom du fichier d'icônes correspond au nom de StyleBook, les icônes sont automatiquement mappées aux StyleBooks. Sinon, procédez comme suit :

a) Ajoutez le `icon_mapping.json` fichier dans le dossier ressources.

b) Mappez des StyleBooks et des icônes dans le `icon_mapping.json` fichier comme suit :

```
<StyleBook file name> : <icon file name>
<!--NeedCopy-->
```

Voici un exemple de pack StyleBook :

Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
resources	File folder					29-07-2020 07:25
.DS_Store	DS_STORE File	1 KB	No	7 KB	92%	18-08-2020 17:31
exchange.yaml	YAML File	2 KB	No	6 KB	78%	31-07-2020 11:37
sharepoint.yaml	YAML File	1 KB	No	1 KB	56%	29-07-2020 10:13
skype.yaml	YAML File	1 KB	No	1 KB	55%	29-07-2020 10:13

Le `resources` dossier contient les icônes requises.

Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
.DS_Store	DS_STORE File	1 KB	No	7 KB	96%	29-07-2020 11:55
exch.png	PNG File	3 KB	No	3 KB	0%	29-07-2020 07:20
icon_mapping.json	JSON File	1 KB	No	1 KB	7%	29-07-2020 07:28
sharepoint.jpeg	JPEG File	4 KB	No	4 KB	9%	29-07-2020 07:19
skype.png	PNG File	7 KB	No	7 KB	1%	29-07-2020 07:20

Dans cet exemple, `sharepoint.yaml` et `skype.yaml` les fichiers sont automatiquement mappés à `sharepoint.jpeg` et `skype.png` respectivement.

Pour `exchange.yaml` mapper à `exch.png`, spécifiez les éléments suivants dans le `icon_mapping.json` fichier :


```
{

"exchange.yaml":"exch.png"
 }

<!--NeedCopy-->
```

Si vous spécifiez l'`defaulticon` entrée, les StyleBooks sont mappés à l'icône par défaut, à moins qu'ils ne soient mappés à une autre icône.

```
defaulticon: <icon file name>
<!--NeedCopy-->
```

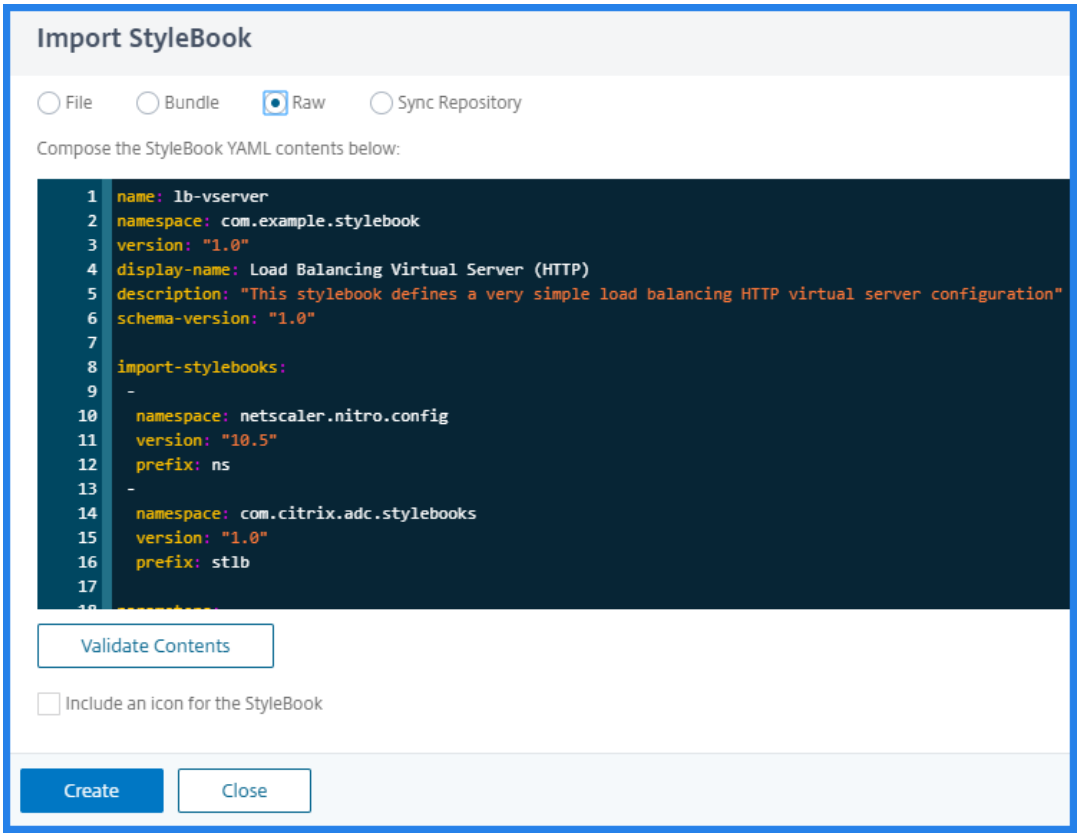
Dans **Application > StyleBooks**, les StyleBooks importés apparaissent avec les icônes mappées.

- **Raw** - Composez le contenu de votre StyleBook dans l'éditeur YAML.

  Vous pouvez valider le contenu du StyleBook pour vérifier les erreurs grammaticales du StyleBook. Pour valider le contenu du StyleBook, cliquez sur **Valider le contenu**.

  > **Remarque**
  >
  > Lors de la composition de StyleBook, assurez-vous de connaître les concepts suivants :
  >
  > - API NITRO
  > - YAML

  Pour plus d'informations sur la façon d'écrire vos propres StyleBooks, consultez Comment créer vos propres StyleBooks.



- **Référentiel de synchronisation** - Cette option répertorie les référentiels ajoutés à ADM. Sélectionnez le référentiel que vous souhaitez synchroniser avec ADM.

> **Remarque**
>
> Vous pouvez également copier et coller le contenu d'un fichier YAML StyleBook dans l'éditeur YAML.

3. Facultatif, sélectionnez une icône pour un StyleBook.

   Dans **Applications > StyleBook**, le StyleBook importé apparaît avec cette icône.

4. Cliquez sur **Créer**.

   Citrix ADM valide désormais votre StyleBook pour toutes les erreurs syntaxiques et sémantiques selon la grammaire StyleBook. Votre StyleBook n'est pas importé dans Citrix ADM s'il y a des erreurs.

   S'il n'y a aucune erreur, le StyleBook est correctement importé et répertorié sur la page **StyleBooks** . Vous pouvez identifier le StyleBook par le nom complet que vous avez défini dans la section d'en-tête du StyleBook.

> **Remarque**
>
> Si vous importez un ensemble de fichiers, Citrix ADM décompresse le dossier compressé et valide tous les StyleBooks.
> Le bundle n'est pas importé même si un fichier StyleBook échoue le test de validation.

Pour plus d'informations sur la grammaire StyleBook et la syntaxe des différentes constructions et attributs, voir Grammaire StyleBook.

5. Cliquez sur le lien **Créer une configuration** pour créer des configurations à partir de ce StyleBook.

   Le StyleBook s'ouvre en tant que page d'interface utilisateur sur laquelle vous pouvez entrer les valeurs de tous les paramètres définis dans ce StyleBook.

6. Spécifiez les valeurs requises pour les paramètres.

   Dans l'exemple suivant,

   a) Spécifiez le **nom de l'application** et l'**adresse IP de l'équilibreur** de charge.

   b) Sélectionnez l'**algorithme d'équilibrage** de charge dans la liste. Par défaut, **ROUNDROBIN** est sélectionné.

7. Sous **Instances cibles**, sélectionnez l'adresse IP de l'instance Citrix ADC sur laquelle vous souhaitez déployer la configuration.

   Vous pouvez également déployer la configuration sur plusieurs Citrix ADC, en spécifiant autant d'instances cibles que nécessaire.

8. Si vous souhaitez tester les objets de configuration Citrix ADC (NITRO) avant de déployer la configuration, cliquez sur **Exécuter à sec**.

   Si la configuration est valide, les objets de configuration sont créés en fonction des valeurs spécifiées.

   Dans cet exemple, le StyleBook ne crée qu'un seul objet de type `lbvserver`. Ce serveur d'équilibrage de charge était le seul composant défini dans cet exemple de base StyleBook.

   Plus tard, cliquez sur **Créer** pour déployer la configuration sur les instances Citrix ADC sélectionnées.

Une fois la configuration déployée avec succès, un nouveau pack de configuration apparaît dans la page **Configurations**.

> **Remarque**

> Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter des instances Citrix ADC récemment découvertes dans Citrix ADM à la liste des instances disponibles dans cette fenêtre.

Rechercher des StyleBooks personnalisés

Citrix ADM vous permet désormais de rechercher StyleBooks en fonction de leur type. Autrement dit, vous pouvez désormais rechercher des StyleBooks par défaut ou des StyleBooks personnalisés. Cette option est particulièrement utile lorsque vous devez rechercher vos StyleBooks définis par l'utilisateur parmi de nombreux StyleBooks par défaut.

Pour rechercher des StyleBooks personnalisés

1. Dans Citrix ADM, accédez à **Applications** > **Configurations** > **StyleBooks**.
2. Cliquez sur l'icône de recherche en haut à droite.
3. Dans la barre de recherche, sélectionnez **Type**, puis **Personnalisé** dans la sous-liste.
4. Citrix ADM affiche uniquement les StyleBooks définis par l'utilisateur.

Créer et modifier un pack de configuration

February 1, 2024

Dans Citrix Application Delivery Management (ADM), vous pouvez créer un pack de configuration à partir d'un StyleBook. Et, le pack de configuration est lié au StyleBook à partir duquel il est créé. Les mises à jour du pack de configuration sont effectuées via le StyleBook auquel il est lié.

Créer un pack de configuration

Effectuez les opérations suivantes pour créer un pack de configuration à partir d'un StyleBook :

1. Accédez à **Applications > StyleBooks > Configurations**.
2. Cliquez sur **Ajouter**.
3. Dans **Choisir des StyleBooks**, sélectionnez les StyleBooks requis à partir desquels vous souhaitez créer un pack de configuration.

   Cette page classe StyleBooks dans StyleBooks par défaut et personnalisés. Sélectionnez les onglets respectifs pour trouver les StyleBooks requis.

4. Spécifiez les détails requis, tels que le nom de l'application, l'adresse IP, le port ou le type de protocole.

   Les champs de l'interface graphique diffèrent d'un StyleBook à un autre StyleBook.

5. Dans **Instances cibles**, sélectionnez les instances ou les groupes d'instances dans lesquels vous souhaitez exécuter la configuration.

   > **Remarque**
   >
   > Vous pouvez déployer la configuration sur plusieurs Citrix ADC, en spécifiant autant d'instances cibles que nécessaire.

6. Cliquez sur **Exécuter à sec**.

   La page **Objets** affiche les objets qui sont créés, modifiés ou supprimés des instances Citrix ADC.

7. Cliquez sur **Créer**.

   Le pack de configuration apparaît dans la page **StyleBook > Configurations**.

Si vous souhaitez modifier les packs de configuration existants, sélectionnez-le et cliquez sur **Modifier**.

Modifier le StyleBook d'un pack de configuration

Parfois, vous devez mettre à jour le StyleBook pour ajouter des fonctionnalités ou résoudre un problème. Si vous avez déjà créé des packs de configuration à l'aide de l'ancien StyleBook, vous pouvez les mettre à jour pour utiliser le nouveau StyleBook mis à jour. Pour utiliser un nouveau StyleBook, modifiez le StyleBook existant du pack de configuration.

Prenons un exemple StyleBook **example-lb** qui déploie une configuration d'équilibrage de charge de base sur une instance ADC. Et, vous créez un pack de configuration CP1 à partir de ce StyleBook.

Lorsque vous souhaitez configurer des moniteurs avec la configuration de base de l'équilibrage de charge, vous avez besoin d'un nouveau StyleBook. Par conséquent, créez **exemple-lb-mon** StyleBook qui inclut la possibilité de configurer des moniteurs ainsi que la configuration de base de l'équilibreur de charge.

Après avoir créé un StyleBook, mettez à jour le pack de configuration existant CP1 pour ajouter des moniteurs. Pour ce faire, effectuez les opérations suivantes :

1. Accédez à **Applications > StyleBooks > Configurations**.
2. Sélectionnez le pack de configuration pour lequel vous souhaitez modifier le StyleBook.

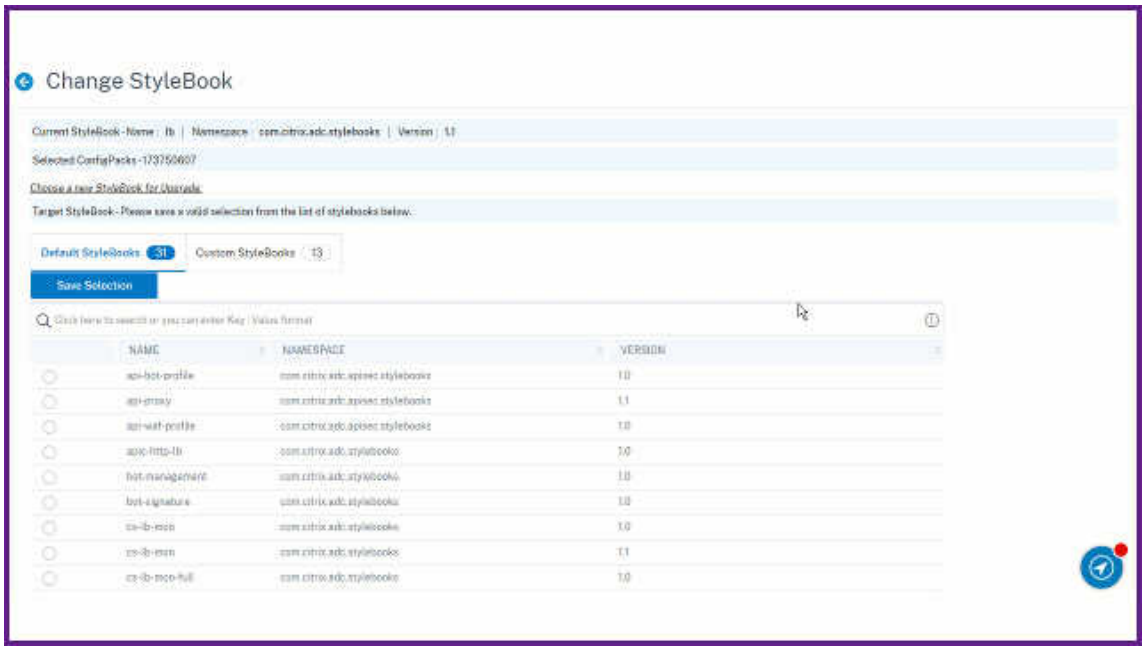
   Dans cet exemple, sélectionnez CP1 dans la liste.

3. Cliquez sur **Modifier le livre de style**.

4. Sélectionnez le StyleBook requis dans la liste. Cliquez ensuite sur **Enregistrer la sélection**.
5. Cliquez sur **Change**.

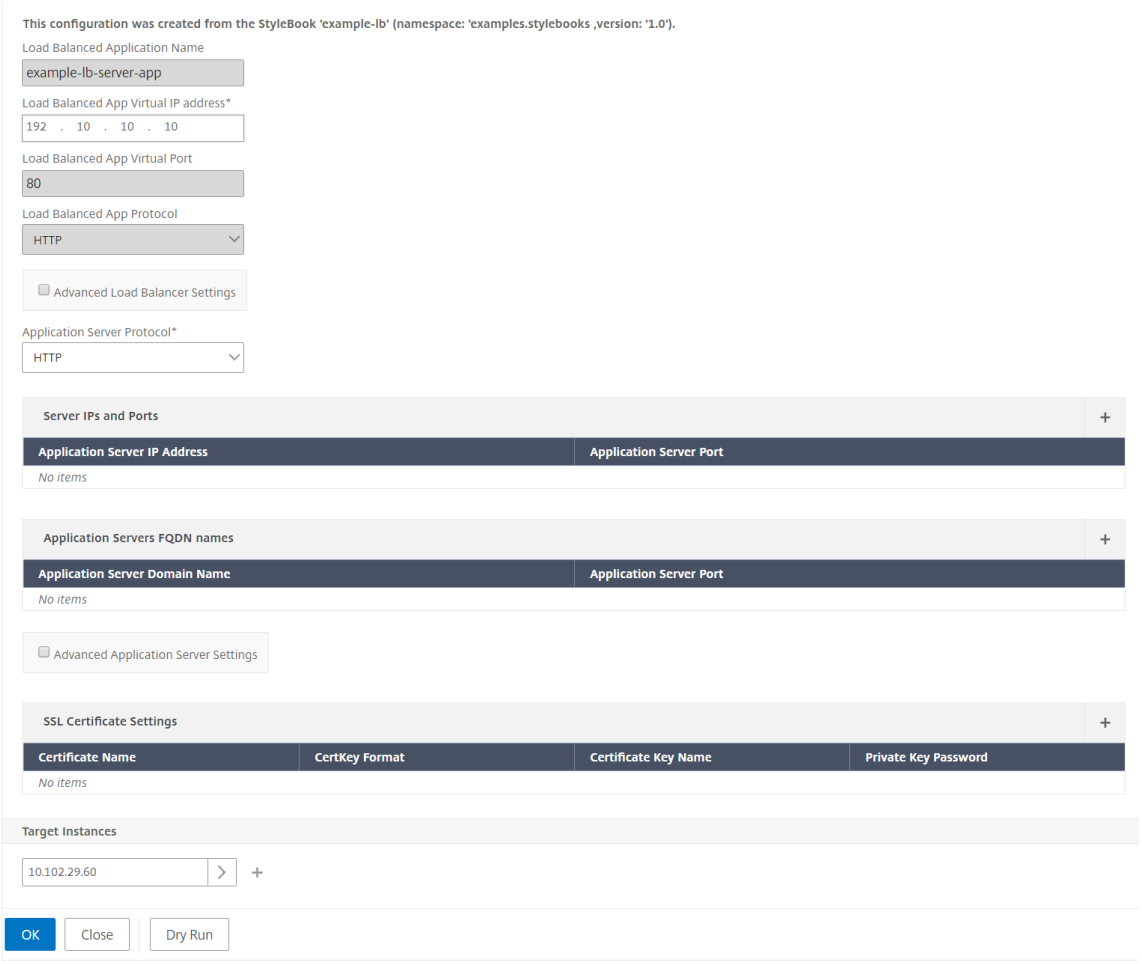
   Dans cet exemple, sélectionnez **exemple-lb-mon** dans la liste.

   Lorsque vous modifiez le StyleBook d'un pack de configuration, les paramètres du nouveau StyleBook peuvent avoir une structure différente de celle du StyleBook existant. Si la structure des paramètres est similaire à la précédente StyleBook, les valeurs des paramètres sont automatiquement conservées dans leurs champs respectifs. Sinon, seuls les paramètres ayant la même structure entre les deux StyleBooks sont transférés. Par exemple, le même nom de paramètre, le même type, le même paramètre parent, et plus encore.

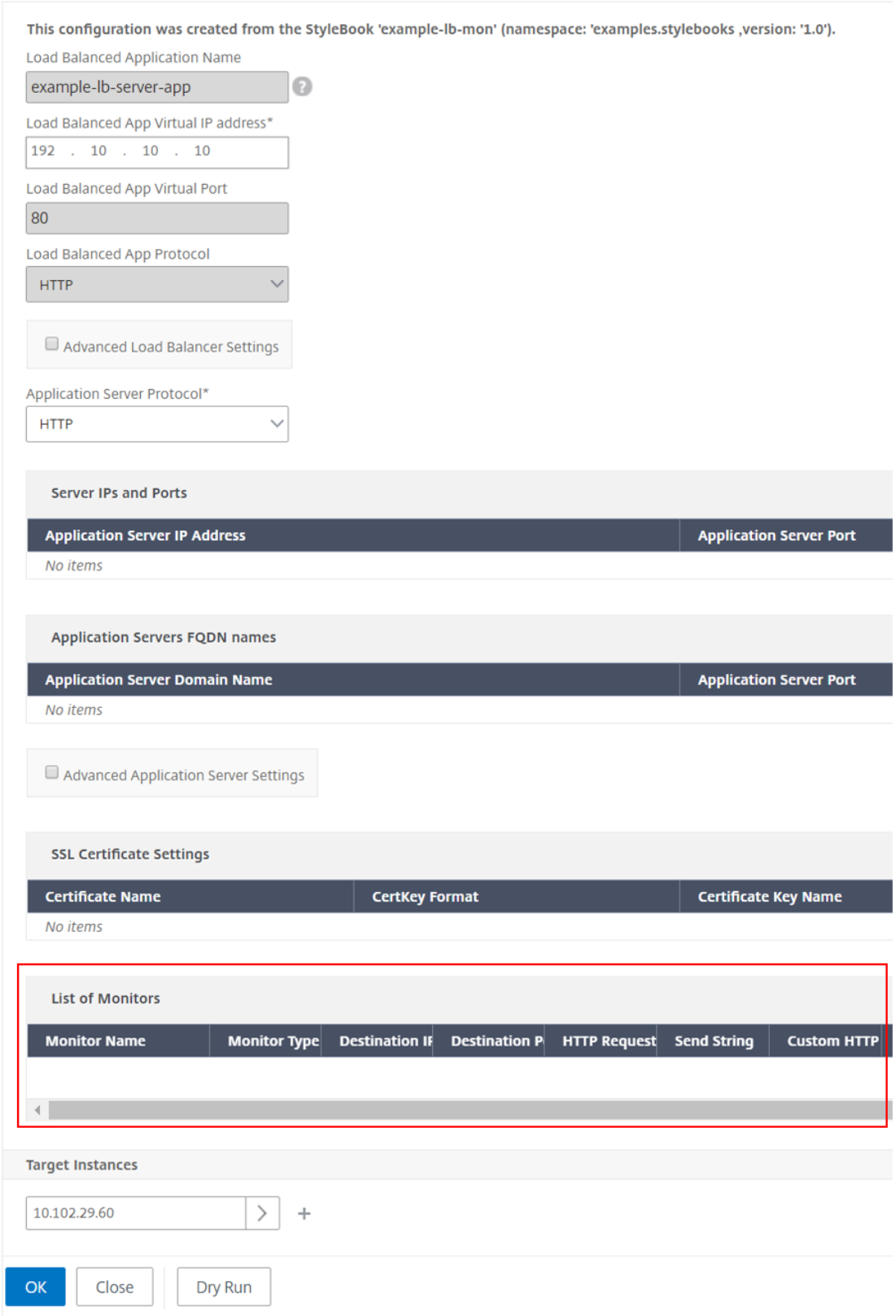


   Si de nouveaux paramètres obligatoires sont ajoutés dans le nouveau StyleBook, après avoir modifié le StyleBook, vous devez spécifier manuellement les valeurs de ces paramètres.

   Dans cet exemple, les paramètres qui apparaissent sur la page de configuration de l'**example-lb** StyleBook sont les suivants :



Les paramètres qui apparaissent sur la page de configuration du nouveau styleBook **example-lb-mon** sont les suivants :



Dans ce cas, les StyleBooks conservent les anciennes valeurs pour la configuration de base

de l'équilibreur de charge car le nouveau StyleBook n'a pas modifié les paramètres existants. Et, il ajoute seulement les nouveaux paramètres. Pour les paramètres du moniteur, spécifiez manuellement les valeurs requises.

6. Dans les **instances cibles**, passez en revue les instances sélectionnées et mettez à jour la liste si nécessaire.
7. Cliquez sur **Exécuter à sec**.

   La page **Objets** affiche les objets qui sont créés, modifiés ou supprimés des instances Citrix ADC.
8. Cliquez sur **OK**.

   Dans la page **StyleBook > Configurations**, la colonne **Nom du livre StyleBook** affiche le nouveau nom de StyleBook pour le pack de configuration sélectionné. Dans ce cas, il affiche **exemple-lb-mon**.

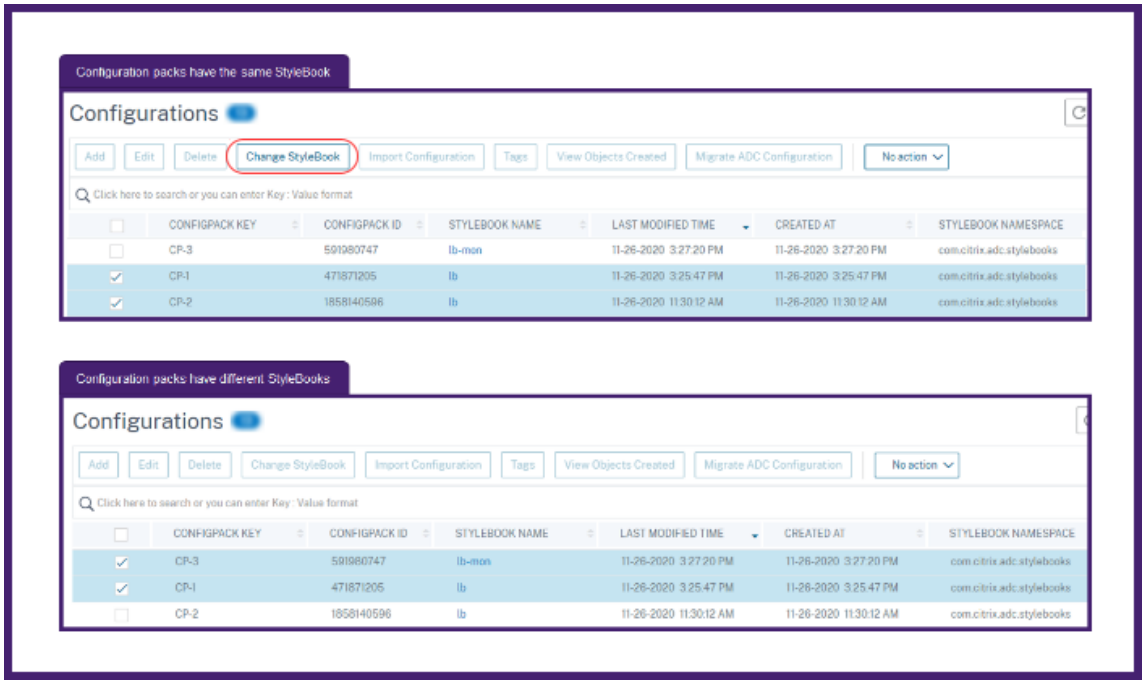
Modifier le StyleBook qui comporte plusieurs packs de configuration

Lorsque vous modifiez un StyleBook existant qui a plusieurs packs de configuration, procédez comme suit :

1. Importez un nouveau StyleBook dans ADM.

   Généralement, le nouveau StyleBook a le même nom et l'espace de noms avec une version supérieure à celle du StyleBook existant. Toutefois, vous pouvez ignorer cette étape si le nom, l'espace de noms ou la version sont différents.
2. Modifiez le StyleBook pour les packs de configuration associés au StyleBook existant.

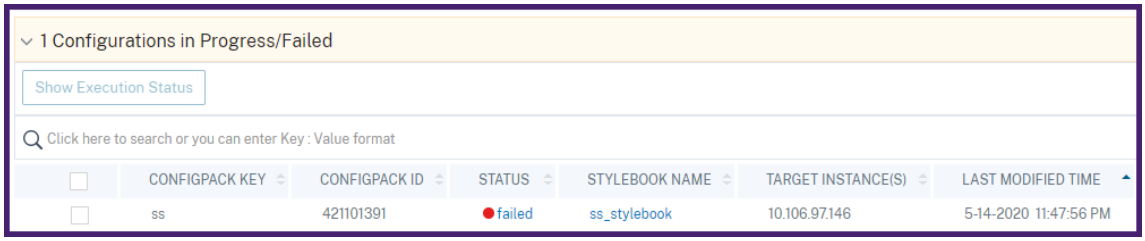
   Vous pouvez sélectionner **Modifier le livre de style** uniquement lorsque les packs de configuration sélectionnés sont associés au même StyleBook.



Pour les packs de configuration sélectionnés, l'ADM modifie correctement le StyleBook lorsque les conditions suivantes sont remplies :

- Tous les paramètres de configuration du StyleBook existant doivent être présents dans le StyleBook sélectionné.
- Les nouveaux paramètres du StyleBook sélectionné sont facultatifs.

Pour voir la progression des packs de configuration sélectionnés, sélectionnez **Configurations en cours ou en échec** dans la page **Configurations**.



3. Supprimez l'ancien StyleBook d'ADM une fois que tous les packs de configuration sont liés au nouveau StyleBook.

Exporter ou importer des packs de configuration

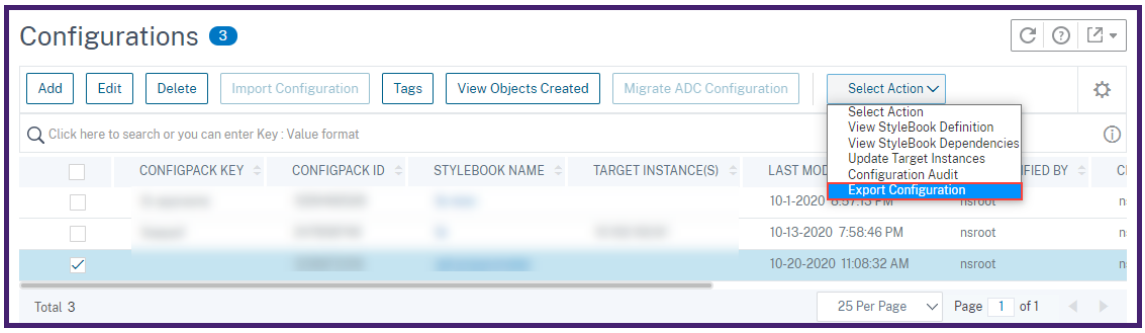
Vous pouvez exporter ou importer un pack de configuration tel que StyleBooks. Avec cette fonctionnalité, vous pouvez facilement partager la configuration de StyleBook à un autre serveur ADM. Lorsque vous exportez un pack de configuration, un `tgz` ou `zip` bundle se télécharge sur votre

ordinateur local. Ce bundle inclut un fichier JSON avec tous les paramètres définis dans un pack de configuration.

Exporter la configuration

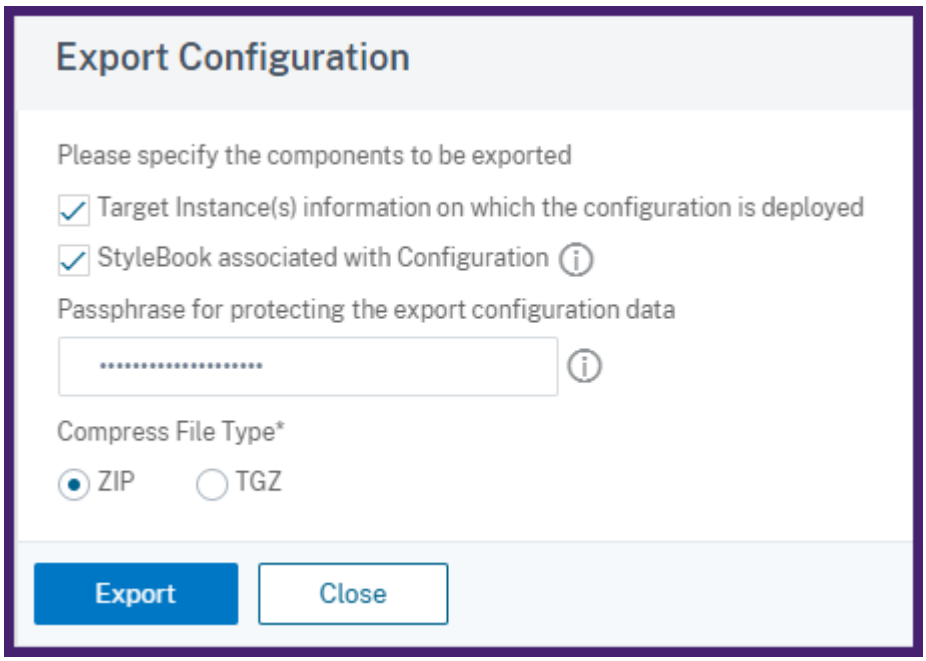
Pour exporter un pack de configuration, procédez comme suit :

1. Accédez à **Applications > StyleBooks > Configurations**.
2. Sélectionnez un pack de configuration que vous souhaitez exporter.
3. Dans **Sélectionner une action**, sélectionnez **Exporter la configuration**.



4. Dans le volet **Configuration d'exportation**, spécifiez les éléments suivants :

   - **Informations sur l'instance cible sur laquelle la configuration est déployée** : sélectionnez cette option pour inclure les informations des instances cibles dans le bundle d'exportation.
   - **StyleBook associé à Configuration** : sélectionnez cette option pour inclure le StyleBook dans l'offre groupée d'exportation.
   - **phrase secrète pour protéger les données de configuration d'exportation** : spécifiez une phrase secrète pour chiffrer le bundle d'exportation. Cette phrase secrète sécurise les données sensibles d'un pack de configuration.
   - **Compresser le type de fichier** : sélectionnez le type de fichier **ZIP** ou **TGZ** .



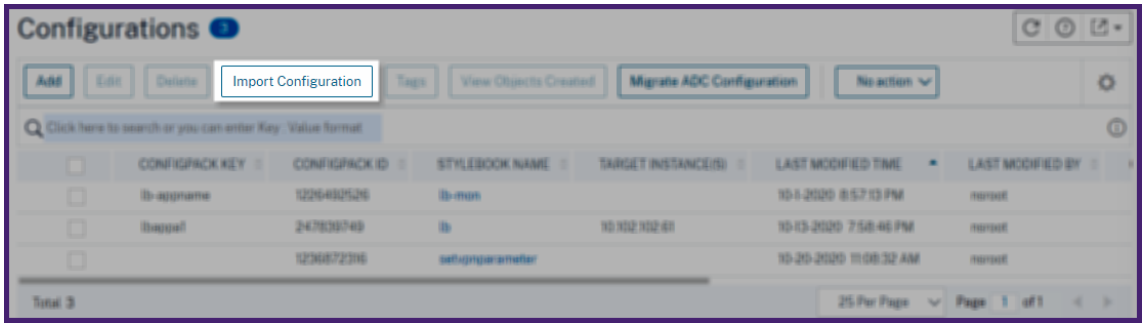
5. Cliquez sur **Exporter**.

   Enregistrez l'offre groupée d'exportation sur votre ordinateur local.

Configuration de l'importation

Vous pouvez importer un pack de configuration depuis votre ordinateur local vers un autre serveur ADM. Pour importer un pack de configuration, procédez comme suit :

1. Accédez à **Applications > StyleBooks > Configurations**.
2. Sélectionnez **Importer la configuration**.



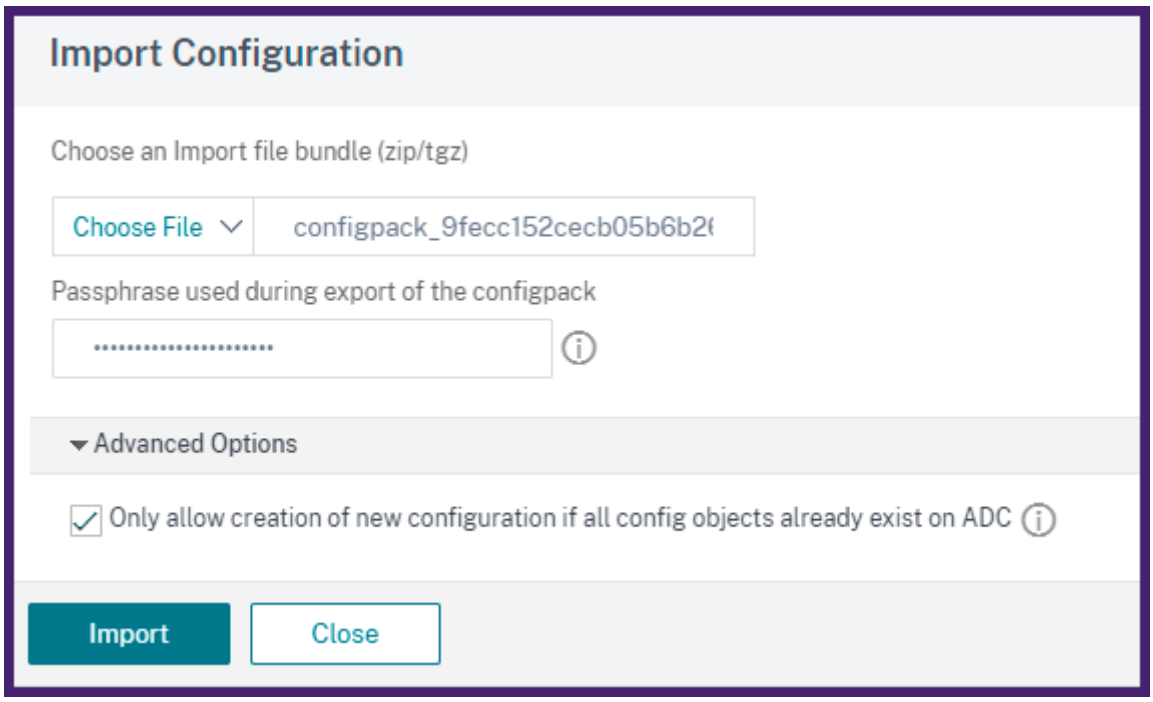
3. Choisissez le lot de fichiers d'importation à partir de votre ordinateur.
4. Utilisez la phrase secrète que vous avez spécifiée lors de l'exportation.
5. Facultatif, dans Options avancées, sélectionnez **Autoriser uniquement la création d'une nouvelle configuration si tous les objets de configuration existent déjà sur ADC**.

Cette option ne modifie pas les objets déjà créés sur l'instance ADC.

Considérez que vous avez ajouté la même instance ADC dans deux serveurs ADM. Et, vous souhaitez migrer un pack de configuration d'un serveur ADM vers un autre serveur. Utilisez cette option pour importer un pack de configuration sans modifier ses objets de configuration sur une instance ADC.

> **Important**
>
> Pour utiliser cette option, vérifiez que le groupe de configuration spécifié dispose des informations sur les instances cibles. Consultez la section Configuration de l'exportation.
>
> Cette option migre la configuration uniquement si tous les objets sont présents sur l'instance cible.

6. Cliquez sur **Importer**.



Lorsque vous importez un pack de configuration, l'ADM vérifie les éléments suivants :

- **StyleBook associé** : Si le StyleBook associé n'est pas dans l'ADM, il importe le StyleBook avec le pack de configuration.
- **Instances cibles** : recherchez les instances cibles et déploie la configuration sur les instances cibles spécifiées. Si les instances ADC mentionnées sont absentes dans l'ADM, le pack de configuration est importé sans instances cibles.
- **ADM source** : si vous importez un pack de configuration sur le même serveur ADM, le bundle sélectionné met à jour le pack de configuration existant.

Créez vos StyleBooks

Le contenu complet de **example-lb** StyleBook est fourni à titre de référence comme suit :

```
name: example-lb
namespace: examples.stylebooks
version: "1.0"
display-name: Basic Load Balancer App
description: This is an example StyleBook that creates a load balancer application
schema-version: "1.0"
import-stylebooks:
  -
    namespace: com.citrix.adc.stylebooks
    prefix: stlb
    version: "1.0"
parameters-default-sources:
  - stlb::lb
components:
  -
    name: lb-comp
    type: stlb::lb
    description: Uses the default lb StyleBook to build the typical lb configuration objects
    properties-default-sources:
      - $parameters
<!--NeedCopy-->
```

Le contenu complet de **example-lb-mon** StyleBook est fourni à titre de référence comme suit :

```
name: example-lb-mon
namespace: examples.stylebooks
version: "1.0"
description: This is an example StyleBook that creates a load balancer application with monitors
display-name: Basic Load Balancer App with Monitors
schema-version: "1.0"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
  -
    namespace: com.citrix.adc.stylebooks
    prefix: stlb
    version: "1.0"
  -
    namespace: com.citrix.adc.commontypes
    prefix: cmtypes
    version: "1.0"
parameters-default-sources:
  - stlb::lb
parameters:
```



```
23    -
24      name: monitors
25      label: "List of Monitors"
26      description: "List of Monitors to monitor Application Servers"
27      type: cmtypes::monitor[]
28  substitutions:
29    mon-name(appname, monname): $appname + "-mon-" + $monname
30  components:
31    -
32      name: lb-comp
33      type: stlb::lb
34      description: Uses the default lb StyleBook to build the typical lb
           configuration objects
35      properties-default-sources:
36        - $parameters
37    -
38      name: monitors-comp
39      type: cmtypes::monitor
40      condition: $parameters.monitors
41      repeat: $parameters.monitors
42      repeat-item: mon
43      repeat-index: ndx
44      description: Builds a list of Citrix ADC monitor objects and binds
           them to the servicegroup of this LB config
45      properties-default-sources:
46        - $mon
47      properties:
48          monitorname: $substitutions.mon-name($parameters.lb-appname,
              $mon.monitorname)
49      components:
50        -
51          name: monitor-svcg-binding-comp
52          condition:  $parameters.svc-servers
53          type: ns::servicegroup_lbmonitor_binding
54          properties:
55            servicegroupname: $components.lb-comp.outputs.servicegroup.
                properties.servicegroupname
56            monitor_name: $parent.properties.monitorname
57  <!--NeedCopy-->
```

Créer un StyleBook pour charger des fichiers vers Citrix ADM

February 1, 2024

Citrix Application Delivery Management (Citrix ADM) StyleBooks vous permettent de créer des configurations Citrix ADC qui peuvent inclure, entre autres, lors du téléchargement de fichiers de n'importe quel type depuis votre système de fichiers local vers l'instance Citrix ADC, à l'aide de l'interface graphique Citrix ADM ou des API. Ces fichiers peuvent être des exemples de fichiers de certificats ou

de fichiers de géolocalisation. Vous pouvez également spécifier le répertoire dans lequel télécharger ces fichiers.

Configuration de StyleBook

Voici un exemple de StyleBook qui décrit comment télécharger un fichier de géolocalisation sur l'instance Citrix ADC. Les fichiers géo sont généralement utilisés dans les configurations GSLB pour définir la proximité statique en fonction de l'emplacement géographique :

Créez votre StyleBook -1

```
name: upload-geolocations
namespace: com.citrix.adc.stylebooks.samples
version: "1.0"
display-name: GeoLocation File Upload
description: This StyleBook is used to upload a geolocation file to
   Citrix ADC
schema-version: "1.0"

import-stylebooks:
-
 namespace: netscaler.nitro.config
 version: "11.1"
 prefix: ns

parameters:
-
 name: locationfile
 label: Location File
 description: The system file path of the geolocation file on Citrix
    ADM
 type: file
 required: true

components:
-
 name: upload-file-comp
 type: ns::systemfile
 properties:
    filename: $parameters.locationfile.filename
    filelocation: "/var/netscaler/inbuilt_db/"
    filecontent: base64.encode($parameters.locationfile.contents)
<!--NeedCopy-->
```

> **Remarque**

> Le paramètre utilisé dans cet exemple est un fichier de type. Vous pouvez importer ce StyleBook dans Citrix ADM et l'utiliser pour télécharger des fichiers de géolocalisation.

Ce StyleBook exige que le fichier soit déjà présent dans Citrix ADM (par exemple, vous l'auriez déjà copié dans Citrix ADM à l'aide d'un utilitaire comme scp).
Si vous souhaitez télécharger un fichier vers des Citrix ADC via Citrix ADM sans le copier au préalable dans le système de fichiers Citrix ADM, vous pouvez créer un StyleBook qui comporte deux paramètres « chaîne », l'un permet de spécifier le nom de fichier à utiliser sur le Citrix ADC et l'autre pour spécifier le contenu de l'objet et utilisez ces deux paramètres dans les composants upload-file-comp. Voici une alternative à StyleBook pour télécharger un fichier de géolocalisation :

Créez votre StyleBook - 2

```
name: upload-geolocations-alt
namespace: com.citrix.adc.stylebooks.samples
version: "1.0"
display-name: GeoLocation File Upload
description: This StyleBook is used to upload a geolocation file to
   Citrix ADC
schema-version: "1.0"

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  version: "11.1"
  prefix: ns

parameters:
 -
  name: filename
  label: Location Filename
  description: The name of the location file on the Citrix ADC
  type: string
  required: true
 -
  name: filecontents
  label: Location File Contents
  description: The contents of the location file
  type: string
  required: true

components:
 -
  name: upload-file-comp
  type: ns::systemfile
  properties:
   filename: $parameters.filename
   filelocation: "/var/Citrix ADC/inbuilt_db/"
   filecontent: base64.encode($parameters.filecontents)
```



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

Création de configurations pour télécharger des fichiers

La procédure suivante crée une configuration sur une instance Citrix ADC sélectionnée qui téléchargerait un fichier de géolocalisation à l'aide du premier StyleBook décrit ci-dessus.

Pour créer une configuration pour le téléchargement de fichiers :

1. Dans Citrix ADM, accédez à **Applications** > **Configuration**, puis cliquez sur **Créer un nouveau**. La page Choisir un StyleBook affiche tous les StyleBooks disponibles dans votre Citrix ADM. Faites défiler vers le bas et sélectionnez le StyleBook que vous avez importé.

   Les paramètres du StyleBook apparaissent sous la forme d'une page d'interface utilisateur qui vous permet de saisir les valeurs de tous les paramètres définis dans ce StyleBook.
2. Entrez le nom de l'équilibreur de charge et l'adresse IP virtuelle dans la section des paramètres de base de l'équilibreur de charge.
3. Dans la section **Fichier de localisation**, entrez le nom ou l'emplacement du fichier.

   > **Remarque**
   >
   > Assurez-vous que dans Citrix ADM, le fichier se trouve sous le dossier du locataire actuel uniquement. Utilisez n'importe quel protocole de transfert de fichiers pour copier le fichier dans le système de fichiers Citrix ADM.

4. Vous pouvez être invité à fournir vos informations d'identification utilisateur avant d'accéder aux instances cibles.
5. Sélectionnez l'instance Citrix ADC cible sur laquelle la configuration doit être créée, puis cliquez sur **Créer**.

> **Remarque**
>
> Citrix vous recommande de sélectionner**Exécuter à sec**pour vérifier les objets de configuration créés sur l'instance cible avant d'exécuter la configuration réelle sur l'instance.

Lorsque la création du pack de configuration réussit, le fichier est enregistré sur le système de fichiers d'instance Citrix ADC à l'emplacement : /var/netscaler/inbuilt_db/

> **Remarque**
>
> Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter des instances Citrix ADC récemment découvertes dans Citrix ADM à la liste des instances disponibles dans cette fenêtre.

Utilisation de l'API Citrix ADM pour créer un pack de configuration

Vous pouvez également utiliser l'API Citrix ADM pour créer un pack de configuration qui télécharge des fichiers vers l'instance Citrix ADC sélectionnée. Pour plus d'informations sur l'utilisation des API, voirComment utiliser l'API pour créer des configurations afin de charger n'importe quel type de fichier.

Créer un StyleBook pour charger des fichiers de certificat SSL et de clé de certificat vers Citrix ADM

February 1, 2024

Lors de la création d'une configuration StyleBook qui utilise le protocole SSL, vous devez télécharger les fichiers de certificat SSL et les fichiers de clé de certificat conformément aux paramètres StyleBook. StyleBook vous permet de télécharger directement les fichiers SSL et les fichiers clés depuis votre système local à l'aide de l'interface graphique Citrix ADM. Vous pouvez également utiliser les API Citrix ADM pour télécharger des fichiers de certificat et des fichiers de clé qui sont déjà gérés par Citrix ADM.

Configuration de StyleBook

Ce document vous aide à créer votre propre StyleBook - **Serveur virtuel d'équilibrage de charge (SSL)**
avec des composants pour télécharger des certificats SSL et des fichiers clés. Le StyleBook fourni ici à titre d'exemple crée une configuration de serveur virtuel d'équilibrage de charge de base sur l'instance Citrix ADC sélectionnée. La configuration utilise le protocole SSL. Pour créer une configuration à l'aide de ce StyleBook, vous devez fournir le nom et l'adresse IP du serveur virtuel, sélectionner les paramètres de la méthode d'équilibrage de charge et télécharger le fichier de certificat et le fichier de clé de certificat pour le serveur virtuel, ou utiliser un fichier de certificat et un fichier de clé de certificat qui sont déjà présent dans Citrix ADM. Ils sont spécifiés dans la section « paramètres », comme indiqué ci-dessous :

```
parameters:
 -
  name: name
  type: string
  required: true
 -
  name: ip
  type: ipaddress
  required: true
```



```
10   -
11    name: lb-alg
12    type: string
13    allowed-values:
14      - ROUNDROBIN
15      - LEASTCONNECTION
16    default: ROUNDROBIN
17   -
18    name: certificate
19    label: "SSL Certificate File"
20    description: "The file name of the SSL certificate file"
21    type: certfile
22   -
23    name: key
24    label: "SSL Certificate Key File"
25    description: "The file name of the server certificate's private key
         file"
26    type: keyfile
27  <!--NeedCopy-->
```

Deux composants sont ensuite créés dans la section Composants du StyleBook, comme indiqué ci-dessous. Le composant « my-lbvserver-comp » est de type ns : :lbvserver, où :

- « ns » est le préfixe qui fait référence à l'espace de noms intégré netscaler.nitro.config et à la version 10.5 que vous avez spécifiés dans la section import-stylebooks.
- « lbvserver » est un StyleBook intégré dans cet espace de noms. Il correspond à la ressource serveur virtuel d'équilibrage de charge Citrix ADC NITRO du même nom.

Le deuxième composant « lbvserver-certificate-comp » est de type stlb vserver-certs-binds. Le préfixe « stlb » fait référence à l'espace de noms « com.citrix.adc.stylebooks » et à la version 1.0 spécifiée dans la section import-stylebooks du StyleBook. Si l'espace de noms « com.citrix.adc.stylebooks » peut être considéré comme un dossier, « vserver-certs-binds » est un autre StyleBook (ou un fichier) dans ce dossier. Les StyleBooks qui se trouvent dans l'espace de noms « com.citrix.adc.stylebooks » sont expédiés dans le cadre de Citrix ADM.

Le StyleBook « vserver-certs-binds » utilisé par les StyleBooks définis par l'utilisateur vous permet de configurer facilement les certificats en téléchargeant les fichiers de certificat et de clé sur l'instance Citrix ADC cible et en configurant la liaison des fichiers de certificat et de clé vers les serveurs virtuels appropriés. Les propriétés de ce composant sont - le nom du serveur virtuel lb et les noms des certificats SSL que vous fournissez lors de la création du pack de configuration.

```
1  components:
2   -
3    name: my-lbvserver-comp
4    type: ns::lbvserver
5    properties:
6     name: $parameters.name
7     servicetype: SSL
8     ipv46: $parameters.ip
```



```
    port: 443
    lbmethod: $parameters.lb-alg
  -
   name: lbvserver-certificate-comp
   type: stlb::vserver-certs-binds
   description: Binds lbvserver with server certificate
   properties:
    vserver-name: $components.my-lbvserver-comp.properties.name
    certificates:
     -
      cert-name: $parameters.name + "-lb-cert"
      cert-file: $parameters.certificate
      ssl-inform: PEM
      key-name: $parameters.name + "-key"
      key-file: $parameters.key
<!--NeedCopy-->
```

Lorsque vous utilisez l'API pour créer une configuration à partir d'un tel StyleBook, utilisez uniquement les noms de fichiers (pas le chemin complet du fichier). Ces fichiers devraient déjà être disponibles dans les dossiers de certificats et de fichiers clés sur Citrix ADM. Le fichier de certificat SSL téléchargé est stocké sur Citrix ADM dans le répertoire /var/mps/tenants/…Le répertoire /ns_ssl_certs et le fichier clé du certificat SSL sont stockés dans /var/mps/tenants/…Répertoire /ns_ssl_keys dans Citrix ADM.

Création de configurations pour télécharger des fichiers SSL

La procédure suivante crée une configuration de serveur virtuel d'équilibrage de charge de base sur une instance Citrix ADC sélectionnée à l'aide du protocole SSL du StyleBook spécifié ci-dessus. Vous pouvez utiliser cette procédure pour télécharger les fichiers de certificat SSL et les fichiers de clés de certificat dans Citrix ADM.

Pour créer une configuration pour le téléchargement de fichiers

1. Dans Citrix ADM, accédez à **Applications** > **Configuration > StyleBooks**.La page **StyleBooks** affiche tous les StyleBooks disponibles dans votre Citrix ADM.
2. Faites défiler vers le bas et sélectionnez **Serveur virtuel d'équilibrage de charge (SSL)ou tapez Serveur virtuel d'équilibrage de charge (SSL)**dans le champ de recherche et appuyez sur la touche**Entrée**.
3. Cliquez sur le lien **Créer une configuration** dans le panneau StyleBook.

   Les paramètres du StyleBook apparaissent sous la forme d'une page d'interface utilisateur qui vous permet de saisir les valeurs de tous les paramètres définis dans ce StyleBook.

4. Entrez le nom de l'équilibreur de charge et l'adresse IP virtuelle dans la section des paramètres de base de l'équilibreur de charge.
5. Dans la section **Paramètres des certificats SSL**, sélectionnez les fichiers correspondants dans votre dossier de stockage local. Vous pouvez également sélectionner les fichiers présents sur le Citrix ADM lui-même.
6. Sélectionnez l'instance Citrix ADC cible sur laquelle la configuration doit être créée, puis cliquez sur **Créer**.

> **Remarques :**
>
> Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter des instances Citrix ADC récemment découvertes dans Citrix ADM à la liste des instances disponibles dans cette fenêtre.
>
> Dans Citrix ADM, les StyleBooks par défaut suivants, fournis dans le cadre de Citrix ADM, vous permettent de créer un support SSL en téléchargeant les certificats et clés SSL.
>
> - StyleBook LoadBalancing HTTP/SSL (lb)
> - Équilibrage de charge HTTP/SSL (avec moniteurs) StyleBook (lb-mon)
> - Application de commutation de contenu HTTP/SSL avec moniteurs (cs-lb-mon)
> - Exemple d'application StyleBook utilisant les fonctionnalités CS, LB et SSL (sample-cs-app)
>
> Vous pouvez également créer vos propres StyleBooks qui utilisent les certificats SSL de la même manière que décrite dans le StyleBook ci-dessus

Créez votre StyleBook

Le contenu complet du fichier lb-vserver-ssl.yaml est illustré ci-dessous :

```
name: lb-vserver-ssl
description: "This stylebook defines a load balancing virtual server
   configuration."
display-name: "Load Balancing Virtual Server (SSL)"
namespace: com.example.ssl.stylebooks
schema-version: "1.0"
version: "0.1"

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  prefix: ns
  version: "10.5"
 -
  namespace: com.citrix.adc.stylebooks
  prefix: stlb
  version: "1.0"

parameters:
```



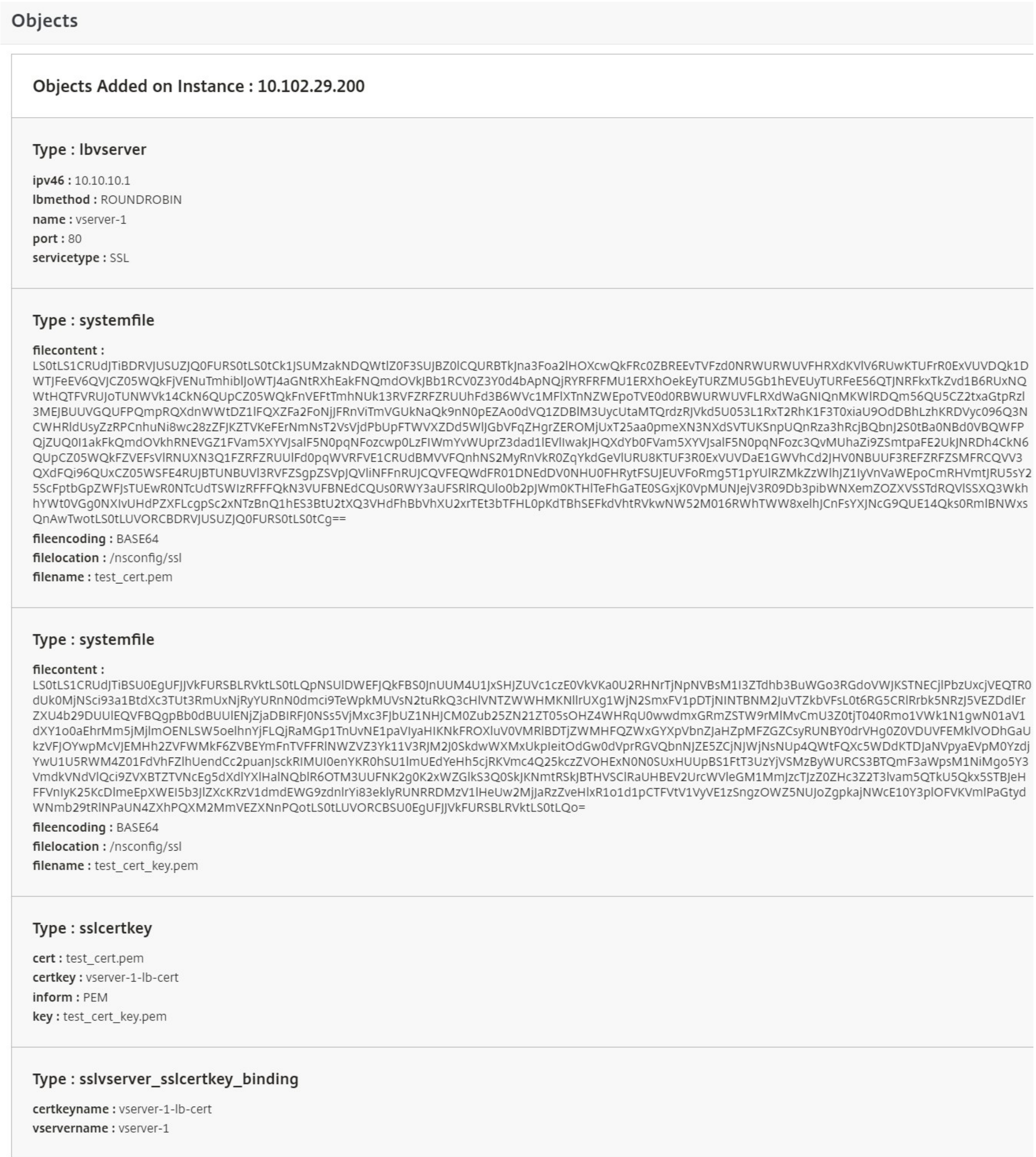
```
 -
  name: name
  type: string
  required: true
 -
  name: ip
  type: ipaddress
  required: true
 -
  name: lb-alg
  type: string
  allowed-values:
    - ROUNDROBIN
    - LEASTCONNECTION
  default: ROUNDROBIN
 -
  name: certificate
  label: "SSL Certificate File"
  description: "The file name of the SSL certificate file"
  type: certfile
 -
  name: key
  label: "SSL Certificate Key File"
  description: "The file name of the server certificate's private key
     file"
  type: keyfile

components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
  properties:
    name: $parameters.name
    servicetype: SSL
    ipv46: $parameters.ip
    port: 443
    lbmethod: $parameters.lb-alg
 -
  name: lbvserver-certificate-comp
  type: stlb::vserver-certs-binds
  description: Binds lbvserver with server certificate
  properties:
   vserver-name: $ components.my-lbvserver-comp.properties.name
   certificates:
    -
     cert-name: $parameters.name + "-lb-cert"
     cert-file: $parameters.certificate
     ssl-inform: PEM
     key-name: $parameters.name + "-key"
     key-file: $parameters.key
<!--NeedCopy-->
```


Utilisation de l'API Citrix ADM pour créer un pack de configuration

Vous pouvez également utiliser l'API Citrix ADM pour créer un pack de configuration qui télécharge les fichiers Cert et Key vers l'instance Citrix ADC sélectionnée. Pour plus d'informations sur l'utilisation des API, consultez Comment utiliser l'API pour créer des configurations afin de télécharger des fichiers de certificats et de clés .

Affichage des objets définis sur l'instance de Citrix ADC

Une fois le pack de configuration StyleBook créé sur Citrix ADM, cliquez sur **Afficher les objets créés** pour afficher tous les objets Citrix ADC créés sur l'instance Citrix ADC cible



Activer l'analyse et configurer les alarmes sur un serveur virtuel défini dans un StyleBook

February 1, 2024

Vous pouvez utiliser la construction des opérations pour configurer Citrix ADM Analytics afin de collecter des enregistrements Appflow sur tout ou partie des transactions de trafic gérées par tout composant de serveur virtuel faisant partie d'un StyleBook. Vous pouvez également utiliser cette construction pour configurer des alarmes afin d'obtenir un aperçu du trafic géré par le serveur virtuel.

L'exemple suivant montre une section Opérations d'un StyleBook :

```
operations:
  analytics:
   -
    name: lbvserver-ops
    properties:
    target: $components.basic-lb-comp.outputs.lbvserver
    filter: HTTP.REQ.URL.CONTAINS("catalog")
   -
    alarms:
     -
      name: lbvserver-alarm
      properties:
      target: $outputs.lbvserver
      email-profile: $parameters.emailprofile
      sms-profile: "NetScalerSMS"

    rules:
     -
      metric: "total_requests"
      operator: "greaterthan"
      value: 25
      period-unit: $parameters.period
     -
       metric: "total_bytes"
       operator: "lessthan"
       value: 60
       period-unit: "day"
<!--NeedCopy-->
```

Les attributs de la section Analytics sont utilisés pour demander à la fonctionnalité d'analyse Citrix ADM de collecter des enregistrements d'appflow sur un composant de serveur virtuel identifié par la propriété cible. Vous pouvez également spécifier une propriété de filtre qui accepte une expression de stratégie Citrix ADC pour filtrer les demandes pour lesquelles des enregistrements appflow sont collectés sur le serveur virtuel.

Lorsqu'un pack de configuration est créé à partir de ce StyleBook, la fonctionnalité d'analyse Citrix ADM est configurée pour collecter les enregistrements appflow sur les serveurs virtuels spécifiés lors de leur création lors de la création d'un pack de configuration.

Les attributs de la section alarmes permettent de définir des seuils pour générer des alarmes et envoyer des notifications sur le serveur virtuel identifié par la propriété cible. Dans l'exemple ci-dessus, les propriétés email-profile et sms-profile sont utilisées pour spécifier où les notifications doivent être envoyées. La section Règles définit les seuils. Par exemple, si le nombre total de demandes traitées

par le serveur virtuel est supérieur à 25 et pour une période définie par l'utilisateur, une alarme est définie et une notification est envoyée. L'«unité de période » indique la fréquence à laquelle une alarme est déclenchée. Il peut prendre la valeur du jour, de l'heure ou de la semaine.

Vous pouvez utiliser les opérateurs suivants pour comparer la valeur de mesure à la valeur de seuil :

- "greaterthan"for ">"
- "lessthan"for "<"
- "greaterthanequal"for ">="
- « lessthanequal » pour « <= »

Notez que StyleBooks utilise des noms d'API pour les mesures et non pas les noms affichés sur l'interface graphique d'analyse Citrix ADM.

Pour savoir comment afficher et analyser les données collectées sur des serveurs virtuels créés dans le cadre d'un pack de configuration, consultez la documentation d'analyse Citrix ADM.

Rôles d'instance

January 23, 2024

Dans Citrix Application Delivery Management (ADM), il peut y avoir un scénario dans lequel vous devez configurer plusieurs instances Citrix ADC pour une seule application, mais également dans lequel chaque instance ADC nécessite une configuration différente pour y être déployée. Un exemple de ce cas est le Microsoft Skype for Business StyleBook par défaut.

StyleBooks prend actuellement en charge la possibilité de créer un pack de configuration et d'appliquer la même configuration sur plusieurs instances Citrix ADC. Un tel scénario où la configuration est identique sur toutes les instances ADC, peut être appelé configuration symétrique.

Maintenant, avec la fonctionnalité « rôles d'instance » de StyleBooks, vous pouvez créer une configuration asymétrique, c'est-à-dire un pack de configuration qui peut être appliqué sur plusieurs instances ADC, mais avec des configurations différentes sur différentes instances ADC.

Lorsqu'une fonctionnalité StyleBook avec rôles d'instance est utilisée pour créer un pack de configuration, chaque instance ADC d'un pack de configuration peut se voir attribuer un rôle différent. Ce rôle détermine les objets de configuration du pack de configuration que l'instance ADC recevra.

Points à noter :

- L'ensemble des rôles d'instance dans un StyleBook sont définis lors de la création du StyleBook.
- Les rôles sont attribués à une instance ADC spécifique lors de la création ou de la mise à jour du pack de configuration.

Section Rôles de cible

Une nouvelle section dans un StyleBook appelée « rôles cibles » est introduite, dans laquelle tous les rôles pris en charge par le StyleBook sont déclarés.

Cette section est généralement placée après la section « Import-StyleBooks » d'un StyleBook et avant la section des paramètres.

Dans l'exemple StyleBook suivant, deux rôles sont définis dans la section « rôles cibles » : A et B.

```
target-roles:

  -
   name: A
   name: B
     min-targets: 2
     max-targets: 5
<!--NeedCopy-->
```

Vous pouvez voir que le rôle B définit également deux sous-propriétés facultatives, min-targets et max-targets.

Bien que ces deux sous-propriétés soient facultatives, min-targets spécifient le nombre minimum obligatoire d'instances ADC à attribuer à ce rôle lors de la création d'un pack de configuration à partir de ce StyleBook, et max-cibles spécifient le nombre maximal d'instances ADC pouvant être affectées à ce rôle lors de la création d'un à partir de ce StyleBook.

Si ces sous-propriétés ne sont pas spécifiées, le nombre d'instances ADC pouvant être configurées pour ce rôle n'est pas limité. Si min-targets = 0, la configuration associée à ce rôle est facultative et si min-targets = 1, cette configuration est obligatoire et au moins une instance ADC doit être configurée pour ce rôle.

Rôle « par défaut »

En plus des rôles explicitement définis, il existe un rôle implicite que tous les StyleBooks ont, et ce rôle est appelé comme rôle par défaut. Ce rôle peut être utilisé comme n'importe quel autre rôle dans un StyleBook. Lors de la création d'un pack de configuration, si une instance ADC n'est pas affectée avec un rôle spécifique, l'instance est implicitement affectée au rôle « par défaut ». L'instance recevra désormais tous les objets de configuration générés par les composants ayant le rôle « par défaut ».

Composants avec des rôles

Une fois les rôles qu'un StyleBook peut prendre en charge (y compris le rôle « par défaut ») définis, les rôles peuvent être utilisés dans la section des composants d'un StyleBook. Si vous souhaitez qu'

un composant soit déployé uniquement sur des instances ADC qui jouent un certain rôle, vous pouvez spécifier l'attribut role dans le cadre du composant, comme illustré dans l'exemple suivant d'un composant :

```
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
<!--NeedCopy-->
```

Dans l'exemple ci-dessus, le composant génère un « lbvserver » qui sera déployé sur les instances jouant le rôle A. Notez que l'attribut roles d'un composant est une liste et que plusieurs rôles peuvent être attribués à un composant. Ces rôles auraient été déclarés dans la section « rôles cibles » du StyleBook.

Remarque : Si un composant d'un StyleBook ne spécifie pas d'attribut de rôle, les objets de configuration générés par le composant sont créés sur toutes les instances Citrix ADC quel que soit leur rôle. Vous pouvez utiliser cette fonctionnalité efficacement pour créer des objets de configuration qui peuvent être appliqués à toutes les instances d'un pack de configuration.

Supposons qu'il existe un StyleBook avec deux rôles définis - A et B, et qui contient quatre composants.

- Le composant C1 a les rôles A et B
- Le composant C2 a le rôle B
- Aucun rôle n'est défini pour le composant C3
- Le composant C4 a le rôle « par défaut »

La section Composants de ce StyleBook est reproduite ci-dessous :

```
components:
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
      - B
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
  -
    name: C2
```



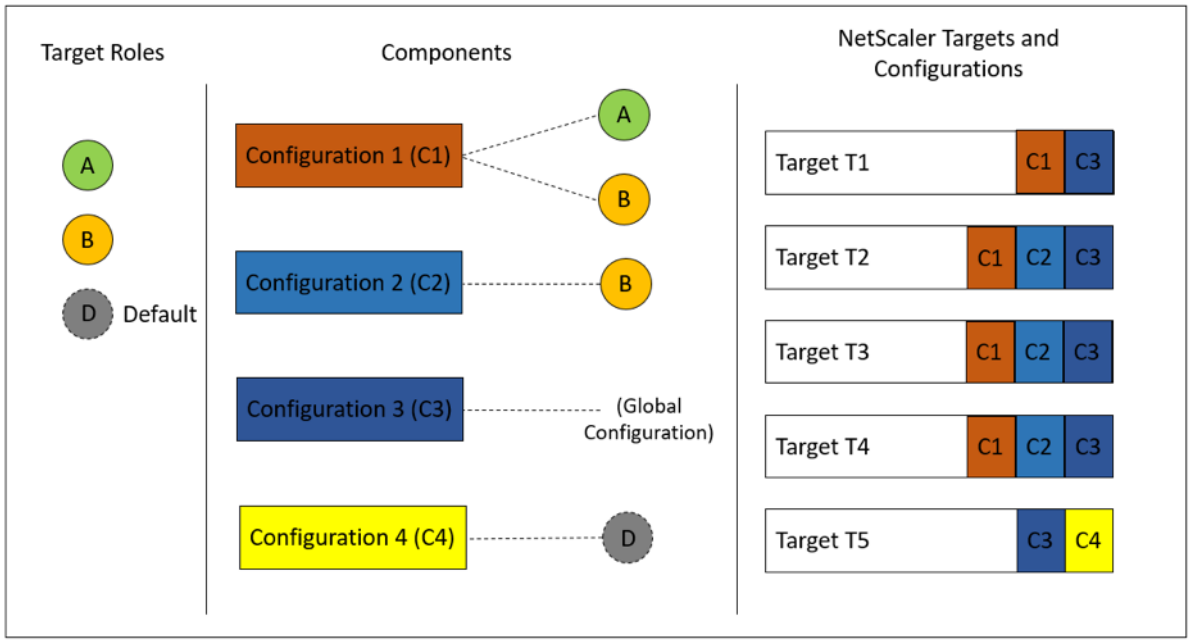
```
15      type: ns::lbvserver
16      roles:
17        - B
18      properties:
19        name: lb2
20        servicetype: HTTP
21        ipv46: 12.12.12.12
22        port: 80
23    -
24      name: C3
25      type: ns::lbvserver
26      properties:
27        name: lb3
28        servicetype: HTTP
29        ipv46: 13.13.13.13
30        port: 80
31    -
32      name: C4
33      type: ns::lbvserver
34      roles:
35        - default
36      properties:
37        name: lb4
38        servicetype: HTTP
39        ipv46: 14.14.14.14
40        port: 80
41  <!--NeedCopy-->
```

Notez que le composant C3 n'a pas de rôle défini, ce qui signifie que le composant est déployé sur toutes les instances, quel que soit leur rôle. D'autre part, le composant C4 a le rôle « default », ce qui signifie qu'il est appliqué à toute instance qui n'a pas de rôle explicite qui lui est assigné.

Maintenant, considérez que vous souhaitez créer un pack de configuration à l'aide de ce StyleBook et le déployer sur cinq instances ADC. À ce stade, vous pouvez affecter les rôles aux instances de la manière suivante :

- Le rôle A est attribué aux instances T1, T2, T3 et T4
- Le rôle B est attribué aux instances T2, T3 et T4
- Aucun rôle n'est attribué à l'instance T5

L'image suivante résume les attributions de rôle et montre la configuration résultante que chaque instance ADC recevra :



Notez que le composant C3 est déployé sur toutes les instances quel que soit le rôle, car ce composant ne possédait aucun attribut role.

Vous pouvez également utiliser la fonction « Exécuter à sec » lors de la création d'un pack de configuration pour afficher et vérifier l'attribution correcte des rôles et des objets de configuration qui seront créés sur chaque instance ADC.

Créez votre StyleBook

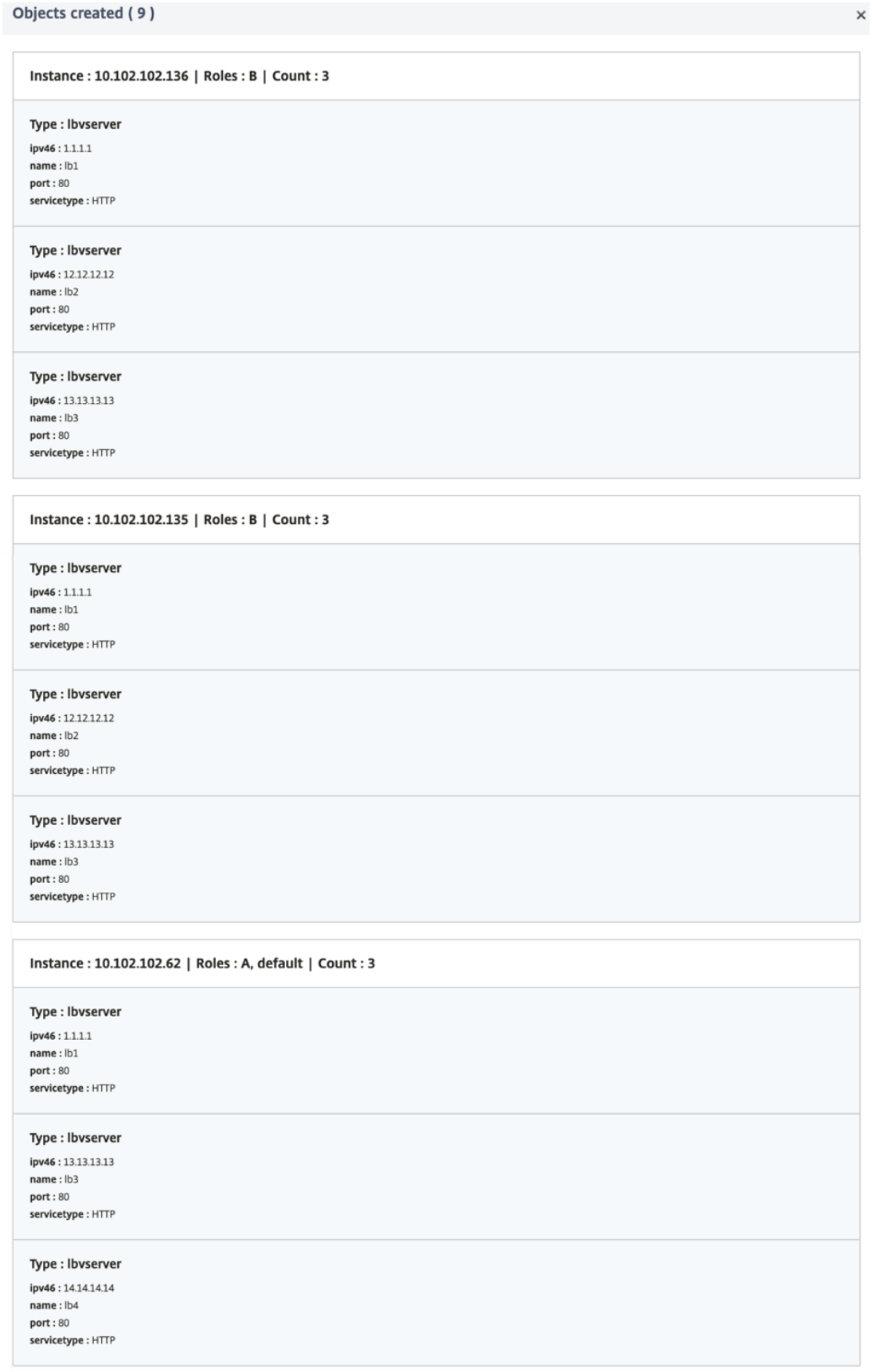
Le contenu complet du StyleBook « demo-target-roles » est fourni ci-dessous :

```
---
name: demo-target-roles
namespace: com.example.stylebooks
version: "1.2"
schema-version: "1.0"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
parameters:
  -
    name: appname
    type: string
    required: true
    key: true
target-roles:
  -
    name: A
```



```
  -
    name: B
    min-targets: 2
    max-targets: 5
components:
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
      - B
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
  -
    name: C2
    type: ns::lbvserver
    roles:
      - B
    properties:
      name: lb2
      servicetype: HTTP
      ipv46: 12.12.12.12
      port: 80
  -
    name: C3
    type: ns::lbvserver
    properties:
      name: lb3
      servicetype: HTTP
      ipv46: 13.13.13.13
      port: 80
  -
    name: C4
    type: ns::lbvserver
    roles:
      - default
    properties:
      name: lb4
      servicetype: HTTP
      ipv46: 14.14.14.14
      port: 80
<!--NeedCopy-->
```

L'image suivante montre les objets créés pour un exemple de pack de configuration :



Utilisation des API

Lorsque vous utilisez l'API REST, vous pouvez spécifier des rôles pour chaque instance ADC lors de la création ou de la mise à jour du pack de configuration comme suit. Dans le bloc « cibles », spécifiez l'UUID de l'instance Citrix ADC spécifique sur laquelle vous souhaitez déployer les composants individuels.

```
"targets": [
            {

             "id": "<ADC-UUID>",
             "roles": ["A"]
             }
 ,
           ]
<!--NeedCopy-->
```

Un exemple complet d'API REST est fourni à titre de référence.

POST/<ADM-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/1.2/demo-target-roles/configpacks

```
{

  "configpack": {

     "parameters": {

     "appname": "app1"
     }
 ,
     "targets": [
        {

          "id": "f53c35c3-a6bc-4619-b4b4-ad7ab6a94ddb",
        "roles": ["A"]
         }
 ,
        {

          "id": "c08caa1c-1011-48aa-b8c7-9aed1cd38ed0",
          "roles": ["A", "B"]
         }
 ,
        {

          "id": "88ac90cb-a5cb-445b-8617-f83d0ef6174e",
          "roles": ["A", "B"]
         }
 ,
        {

```



```
            "id": "bf7b0f74-7a83-4856-86f4-dcc951d3141e",
            "roles": ["A", "B"]
           }
 ,
         {

            "id": "fa5d97ab-ca29-4adf-b451-06e7a234e3da",
            "roles": ["default"]
           }

        ]
       }

 }

<!--NeedCopy-->
```

Créer un StyleBook pour effectuer des opérations non CRUD

February 1, 2024

StyleBooks gère les configurations de Citrix ADC en calculant les objets de configuration nécessaires sur les instances de Citrix ADC. Ces objets sont ajoutés, mis à jour ou supprimés de l'instance chaque fois que vous créez ou mettez à jour un ConfigPack. C'est à ce moment que vous spécifiez l'« état désiré. »

Toutefois, certains objets de configuration Citrix ADC prennent en charge quelques opérations autres que la création, la mise à jour ou la suppression (opérations CRUD). Par exemple, un objet d'équilibrage de charge (lbvserver) ou un objet de fonctionnalité Citrix ADC (nsfeature) peut prendre en charge l'opération « enable » ou « disable ». De même, les clés de certification Citrix ADC prennent en charge les opérations « link » et « unlink » pour lier ou dissocier un certificat à un autre certificat. Ces opérations sur les objets Citrix ADC sont appelées opérations non CRUD. Cette section décrit comment effectuer des opérations non CRUD sur des objets de configuration qui les prennent en charge à l'aide de StyleBooks.

> **Remarque**
>
> La liaison entre les objets de configuration (par exemple, lier une clé de certification à un serveur lbvserver) n'est pas considérée comme une opération non CRUD. En effet, les liaisons Nitro sont représentées en tant qu'objets de configuration à part entière. Ces objets sont créés et supprimés comme tout autre objet de configuration Citrix ADC.

Soutenir les opérations non CRUD

Une nouvelle construction appelée « méta-propriétés » est ajoutée dans le composant au même niveau que la construction « propriétés ». Le seul attribut pris en charge dans cette construction est actuellement appelé « action » Cet attribut peut prendre des valeurs telles que « enable » ou « disable » qui sont prises en charge par cet objet de configuration.

```
components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
  meta-properties
   action: enable
  properties:
    name: $parameters.name
    servicetype: HTTP
    ipv46: $parameters.ip
    port: 80
    lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

Dans l'exemple ci-dessus, le composant « my-lbvserver-comp » est du type « ns : :lbvserver ». Le « ns » est le préfixe qui fait référence à l'espace de noms netscaler.nitro.config et à la version 10.5 que vous avez spécifiés dans la section import-stylebooks. Le « lbvserver » est une ressource NITRO dans cet espace de noms. En tant qu'action implicite, le serveur lbvserver est d'abord créé par le StyleBook, puis l'opération « activer » est effectuée sur celui-ci.

L'action spécifiée dans les méta-propriétés est effectuée sur l'objet de configuration uniquement lors de la création du ConfigPack. Les mises à jour du ConfigPack n'effectuent pas d'actions non CRUD.

> **Remarque**
>
> La valeur de l'attribut action ne peut pas être une expression StyleBook évaluée dynamiquement.

Migrer le pack de configuration d'un StyleBook vers un autre StyleBook

February 1, 2024

Dans Citrix Application Delivery Management (ADM), les packs de configuration sont toujours liés au StyleBook à partir duquel ils sont créés. Toute mise à jour du pack de configuration peut être effectuée uniquement via le StyleBook à lequel le pack de configuration est lié. Citrix ADM vous permet désormais de migrer un pack de configuration existant vers un nouveau StyleBook. Le nouveau StyleBook

peut être une version plus originale du StyleBook actuel lié au pack de configuration. Vous pouvez également migrer le pack de configuration vers un StyleBook entièrement différent.

Par exemple, vous avez créé un StyleBook appelé **example-lb**. Ce StyleBook est utilisé pour déployer une configuration d'équilibrage de charge de base sur une instance Citrix ADC. Vous avez créé un pack de configuration CP1 à partir de ce StyleBook sur une instance Citrix ADC. Plus tard, vous avez réalisé que votre StyleBook n'inclut pas de configuration de surveillance. Vous avez donc créé un StyleBook appelé **example-lb-mon**. Ce StyleBook a la même configuration d'équilibrage de charge que l'exemple lb StyleBook, mais il ajoute la possibilité de configurer des moniteurs.

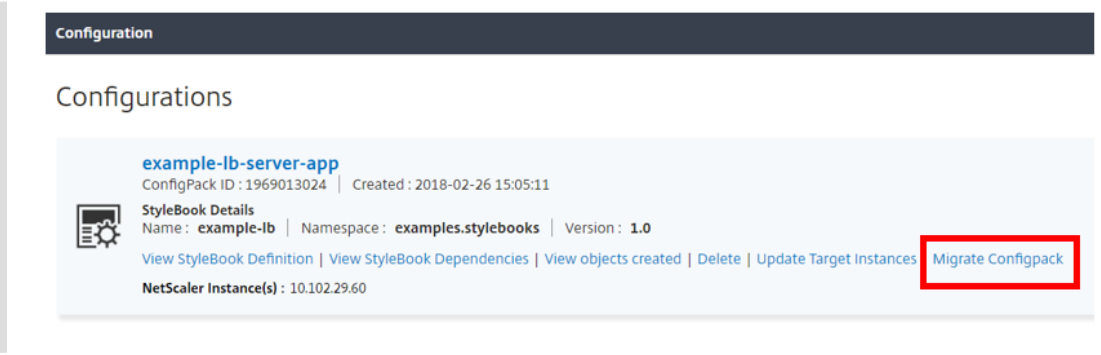
Vous souhaitez maintenant mettre à jour votre configuration existante qui a été créée dans le pack de configuration CP1 pour ajouter des moniteurs. Auparavant, vous deviez supprimer le pack de configuration CP1 et créer un pack de configuration CP2 à partir du nouveau StyleBook pour ajouter des moniteurs à votre configuration. La suppression de CP1 entraîne la suppression de toute la configuration créée dans le pack de configuration CP1 sur une ou plusieurs instances Citrix ADC. Auparavant, vous deviez recréer un nouveau pack de configuration via le nouveau StyleBook en tapant des valeurs pour tous les paramètres.

Au lieu de cela, vous pouvez désormais migrer le pack de configuration existant CP1 vers le nouveau styleBook example-lb-mon. Votre nouveau StyleBook peut configurer les détails des moniteurs. Seuls ces objets de configuration liés au moniteur sont ajoutés aux instances Citrix ADC où le pack de configuration a été déployé. Vous devez fournir juste les détails du moniteur maintenant. La configuration existante déployée sur les instances Citrix ADC qui n'a pas été modifiée reste inchangée.

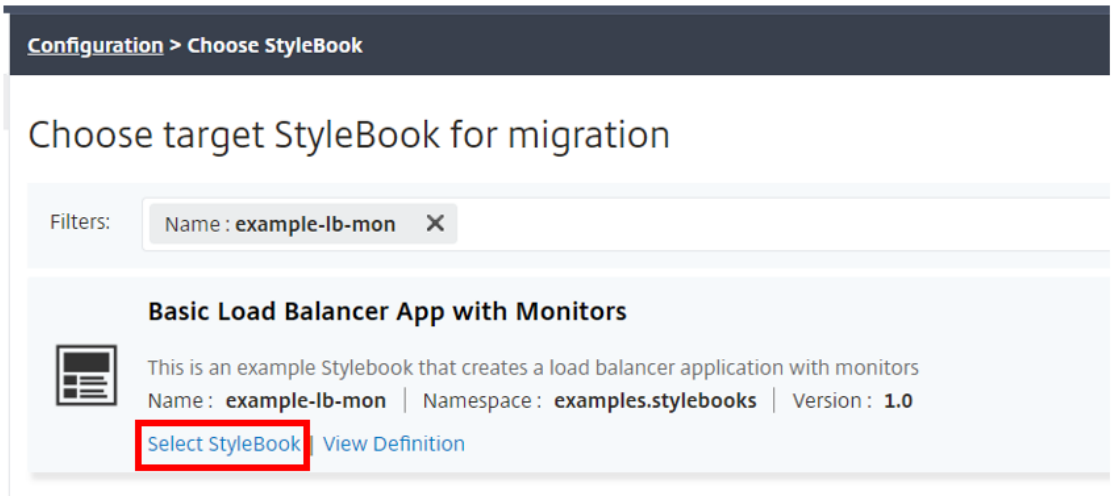
Migrer le pack de configuration

Pour migrer un pack de configuration créé à l'aide d'example-lb StyleBook vers example-lb-mon StyleBook

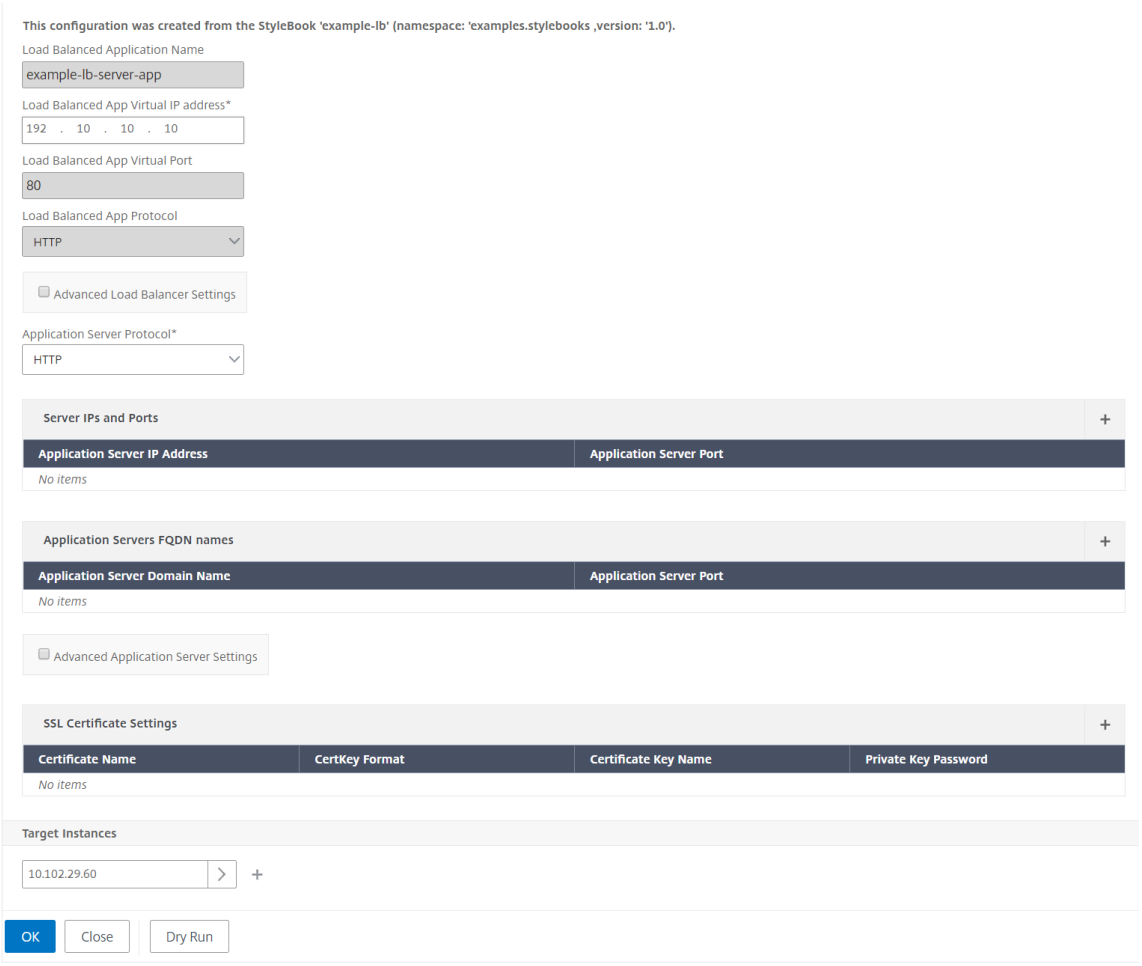
1. Dans Citrix ADM, accédez à **Applications** > **Configurations**. La page **Configurations** affiche tous les packs de configuration présents dans le système.
2. Faites défiler l'écran vers le bas pour trouver le pack de configuration **exemple-lb** que vous auriez créé précédemment, puis cliquez sur **Migrer Configpack**.



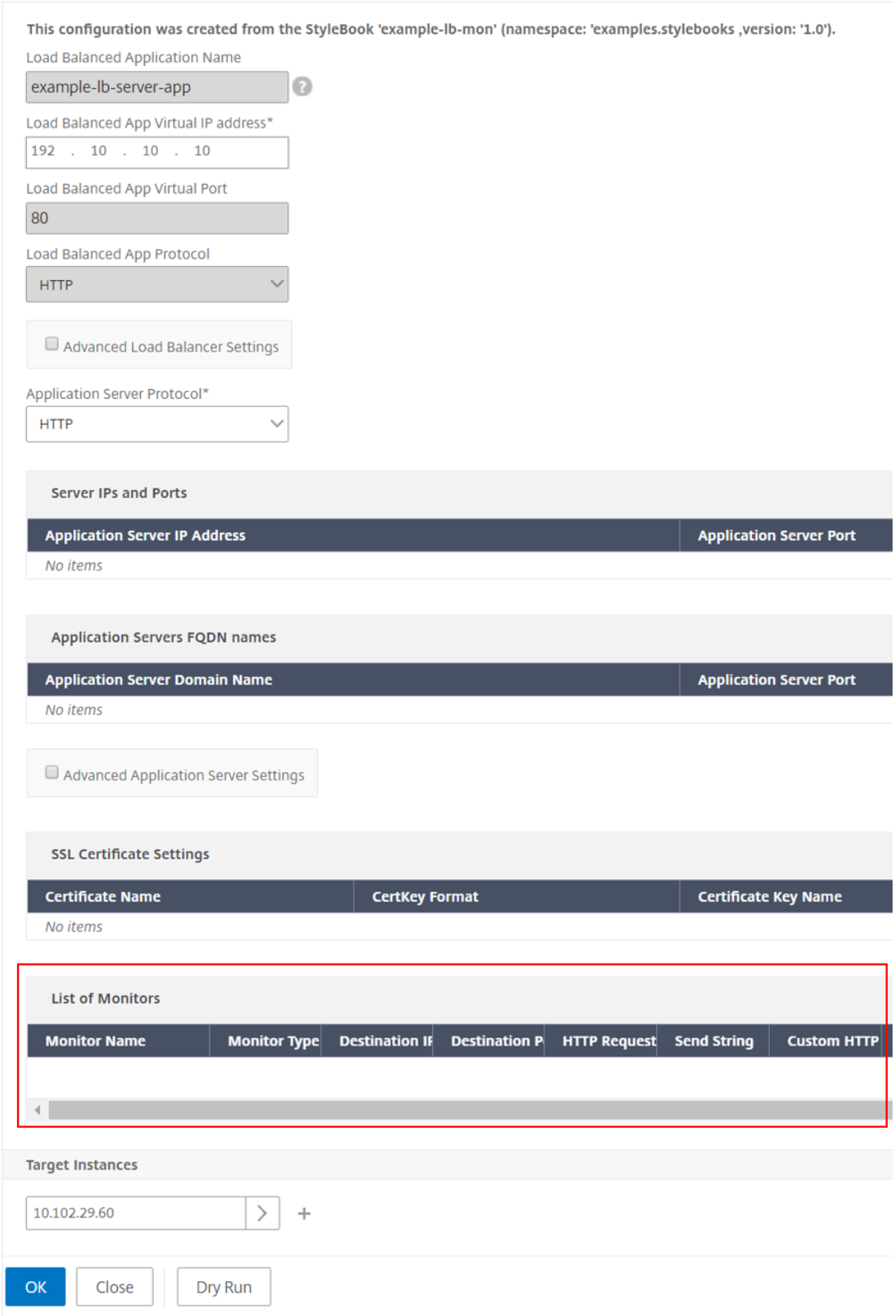
3. La page **Choisir le StyleBook cible pour la migration** s'ouvre et répertorie tous les StyleBooks disponibles dans Citrix ADM. Faites défiler la page vers le bas pour trouver l'**example-lb-mon** StyleBook et cliquez sur **Sélectionner StyleBook** . Vous pouvez également rechercher le StyleBook en tapant example-lb-mon.



Si vous migrez d'un StyleBook à un autre, tous les paramètres des deux StyleBooks peuvent ne pas avoir la même structure. Si la structure des paramètres est similaire, les valeurs précédentes sont automatiquement conservées dans les champs de paramètres. Certains paramètres du nouveau StyleBook peuvent être nouveaux ou leur structure peut être modifiée. Dans ce cas, vous devez renseigner manuellement les valeurs des paramètres StyleBook. Par exemple, l'image suivante montre les paramètres de l'example-lb StyleBook.



L'image suivante montre les paramètres après la migration du pack de configuration vers example-lb-mon StyleBook.



Dans ce cas, vous pouvez constater que les StyleBooks conservent les anciennes valeurs pour

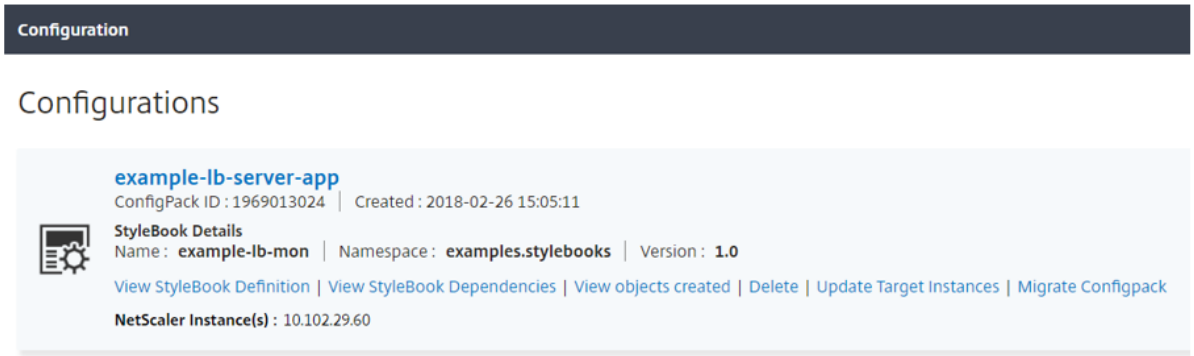
la configuration de base de l'équilibreur de charge. Toutefois, vous devez saisir manuellement les valeurs des paramètres du moniteur.

4. Saisissez les valeurs des nouveaux paramètres utilisés pour créer des moniteurs sur l'instance.
5. Sous **Instances cibles**, cliquez et sélectionnez l'adresse IP de l'instance Citrix ADC sur laquelle vous souhaitez exécuter la configuration. Notez que vous pouvez déployer la configuration sur plusieurs Citrix ADC, en spécifiant autant d'instances cibles que nécessaire.
6. Cliquez sur **Exécuter à sec**. La page **Objets** affiche les objets qui seraient récemment créés, modifiés ou supprimés de la ou des instances Citrix ADC.
7. Cliquez sur **Créer** pour créer ou mettre à jour la configuration des instances sélectionnées. Le pack de configuration est créé si les instances cibles sont nouvelles. Sinon, les configurations existantes déployées sur les instances sont mises à jour.

> **Remarque**
>
> Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter des instances Citrix ADC récemment découvertes. Ces instances sont donc immédiatement disponibles dans la liste des instances de cette fenêtre. L'icône d'actualisation est actuellement disponible uniquement sur Citrix ADM.

Vous pouvez également migrer un pack de configuration d'une version d'un StyleBook vers la version suivante. Ici aussi, vous devrez peut-être taper les valeurs de tous les nouveaux paramètres requis présents dans la nouvelle version. Vous pouvez également migrer le pack de configuration vers une version antérieure du StyleBook. Dans ce cas, les paramètres supplémentaires qui ne sont pas présents dans l'ancien StyleBook sont supprimés. La page **Objets** affiche tous les objets supprimés de la configuration.

Une fois la migration réussie, le ConfigPack est lié au nouveau StyleBook.



Vous pouvez voir que le nom du pack de configuration et l'ID du pack de configuration sont identiques à ceux précédents. Mais Citrix ADM met à jour le nom de StyleBook à example-lb-mon à partir de example-lb.

Créez vos StyleBooks

Le contenu complet de **example-lb**StyleBook est fourni ci-dessous à titre de référence :

```
name: example-lb
namespace: examples.stylebooks
version: "1.0"
display-name: Basic Load Balancer App
description: This is an example StyleBook that creates a load balancer
   application
schema-version: "1.0"
import-stylebooks:
  -
    namespace: com.citrix.adc.stylebooks
    prefix: stlb
    version: "1.0"
parameters-default-sources:
  - stlb::lb
components:
  -
    name: lb-comp
    type: stlb::lb
    description: Uses the default lb StyleBook to build the typical lb
       configuration objects
    properties-default-sources:
      - $parameters
<!--NeedCopy-->
```

Le contenu complet de **example-lb-mon** StyleBook est fourni ci-dessous à titre de référence :

```
name: example-lb-mon
namespace: examples.stylebooks
version: "1.0"
description: This is an example StyleBook that creates a load balancer
   application with monitors
display-name: Basic Load Balancer App with Monitors
schema-version: "1.0"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
  -
    namespace: com.citrix.adc.stylebooks
    prefix: stlb
    version: "1.0"
  -
    namespace: com.citrix.adc.commontypes
    prefix: cmtypes
    version: "1.0"
parameters-default-sources:
  - stlb::lb
parameters:
```



```
23    -
24      name: monitors
25      label: "List of Monitors"
26      description: "List of Monitors to monitor Application Servers"
27      type: cmtypes::monitor[]
28  substitutions:
29    mon-name(appname, monname): $appname + "-mon-" + $monname
30  components:
31    -
32      name: lb-comp
33      type: stlb::lb
34      description: Uses the default lb StyleBook to build the typical lb
           configuration objects
35      properties-default-sources:
36        - $parameters
37    -
38      name: monitors-comp
39      type: cmtypes::monitor
40      condition: $parameters.monitors
41      repeat: $parameters.monitors
42      repeat-item: mon
43      repeat-index: ndx
44      description: Builds a list of Citrix ADC monitor objects and binds
           them to the servicegroup of this LB config
45      properties-default-sources:
46        - $mon
47      properties:
48          monitorname: $substitutions.mon-name($parameters.lb-appname,
              $mon.monitorname)
49      components:
50        -
51          name: monitor-svcg-binding-comp
52          condition:  $parameters.svc-servers
53          type: ns::servicegroup_lbmonitor_binding
54          properties:
55            servicegroupname: $components.lb-comp.outputs.servicegroup.
                properties.servicegroupname
56            monitor_name: $parent.properties.monitorname
57  <!--NeedCopy-->
```

Utiliser l'API pour créer des configurations à partir de StyleBooks

February 1, 2024

Après avoir créé votre StyleBook, vous devez l'importer dans Citrix Application Delivery Management (ADM) pour l'utiliser soit à l'aide de Citrix ADM, soit à l'aide des API Citrix ADM. Citrix ADM valide votre StyleBook lorsque vous l'importez, et si la validation est réussie, votre StyleBook apparaît dans le catalogue Citrix ADM de StyleBooks, prêt à être utilisé pour créer des configurations.

Vous pouvez désormais utiliser les API StyleBook pour créer des configurations basées sur ce StyleBook. Vous pouvez utiliser n'importe quel outil tel que l'outil de ligne de commande curl ou l'extension de navigateur Chrome Postman pour envoyer des requêtes HTTP à Citrix ADM.

Exemple 1

Considérez le StyleBook « lb-vserver » que vous avez créé dans StyleBook pour créer un serveur virtuel d'équilibrage de charge. Utilisez l'API REST pour créer un pack de configuration à partir de ce StyleBook comme suit :

```
POST

https://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/lb-vserver/configpacks

<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

  "configpack":
  {

    "parameters": {

      "name": "lb1",
      "ip": "10.102.117.31"
     }
 ,
    "target_devices":
    [
      {

        "id": "deecee30-f478-4446-9741-a85041903410"
       }

    ]
 }

 }

<!--NeedCopy-->
```

Dans cette requête HTTP, l'id (par exemple, « deecee30-f478-4446-9741-a85041903410 ») est l'ID d'instance de l'instance Citrix ADC sur laquelle le serveur virtuel d'équilibrage de charge lb1 avec l'adresse IP 10.102.117.31 est créé. L'ID d'instance de l'instance Citrix ADC est extrait de Citrix ADM.

Pour obtenir l'ID d'une instance gérée par Citrix ADM, vous pouvez utiliser les API Citrix ADM. Par ex-

emple, pour récupérer l'ID d'instance d'une instance Citrix ADC dont l'adresse IP est 192.168.153.160, vous pouvez utiliser l'API suivante :

```
GET https://<MAS-IP>/nitro/v1/config/ns?filter=ip_address
   :192.168.153.160
<!--NeedCopy-->
```

```
Accept: application/json
<!--NeedCopy-->
```

La réponse contient l'ID de la charge utile :

```
200
OK
Content-Type: application/json
{

  "errorcode": 0,
  "message": "Done",
  "operation": "get",
  "resourceType": "ns",
  "username": "nsroot",
  "tenant_name": "Owner",
  "resourceName": "",
  "ns":
  [
    {

    "is_grace": "false",
    "hostname": "",
    "std_bw_config": "0",
    "gateway_deployment": "false",
    ..."id": "deecee30-f478-4446-9741-a85041903410",
    ...
    }

 ]
 }

<!--NeedCopy-->
```

Si le pack de configuration est créé avec succès, vous recevez la réponse HTTP suivante :

```
200 OK
Content-Type: application/json
{

  "configpack":
  {

    "config_id": "1460806080"
   }

```



```
 }

<!--NeedCopy-->
```

Vous avez créé votre premier pack de configuration qui est identifié de manière unique à l'aide de l'ID 1460806080. Vous pouvez utiliser cet ID pour interroger, mettre à jour ou supprimer la configuration.

Exemple 2

Vous pouvez utiliser le même StyleBook pour créer un autre pack de configuration et l'exécuter sur des instances Citrix ADC identiques ou différentes. Dans cet exemple, créez une autre configuration et fournissez un nom et une adresse IP différents pour le serveur virtuel et spécifiez LEASTCONNECTION comme méthode d'équilibrage de charge. Déployez cette configuration sur deux instances Citrix ADC.

La requête HTTP est la suivante :

```
POST

https://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/lb-vserver/configpacks
<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

  "configpack":
  {

    "parameters":
    {

      "name": "lb2",
      "ip": "10.102.117.32",
      "lb-alg": "LEASTCONNECTION"
     }
 ,
    "target_devices"
    [
     {
 "id": "deecee30-f478-4446-9741-a85041903410" }
 ,
     {
 "id": "debecc60-d589-4557-8632-a74032802412" }

    ]
   }
```



```
26
27  }
28
29 <!--NeedCopy-->
```

Dans cette requête HTTP, le serveur virtuel d'équilibrage de charge lb2 avec l'adresse IP 10.102.117.32 est créé sur les deux instances Citrix ADC représentées par les ID « deecee30-f478-4446-9741-a85041903410 » et « debecc60-d589-4557-8632-a74032802412 ».

En cas de création réussie du pack de configuration, la réponse HTTP suivante est reçue :

```
1  200 OK
2  Content-Type: application/json
3  {
4
5     "configpack":
6    {
7
8       "config_id": "1657696292"
9     }
10
11  }
12
13 <!--NeedCopy-->
```

Ce nouveau pack de configuration a un ID différent 165769629. Vous pouvez mettre à jour ou supprimer cette configuration à l'aide de cet ID.

Exemple 3

Considérez le StyleBook « basic-lb-config » que vous avez créé dans StyleBook pour créer une configuration d'équilibrage de charge de base. Utilisez l'API REST pour créer un pack de configuration à partir de ce StyleBook comme suit :

```
1  POST
2
3  http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example
      .stylebooks/0.1/basic-lb-config/configpacks
4  <!--NeedCopy-->
```

```
1  Content-Type: application/json
2  Accept: application/json
3  {
4
5    "configpack":
6    {
7
8      "parameters":
9      {
10
```



```
        "name": "myapp",
        "ip": "10.70.122.25",
        "svc-servers":
        ["192.168.100.11","192.168.100.12"],
         "svc-port": 8080
       }
  ,
     "target_devices":
     [
      {

       "id": "deecee30-f478-4446-9741-a85041903410"
       }
  ,
      {

       "id": "debecc60-d589-4557-8632-a74032802412"
       }

     ]
    }

  }

<!--NeedCopy-->
```

Dans cette requête HTTP, la configuration d'équilibrage de charge est exécutée sur deux instances Citrix ADC. Vous pouvez ouvrir une session sur ces instances Citrix ADC pour vérifier si un serveur virtuel et un groupe de services avec deux services liés sont créés.

Exemple 4

Prenons l'**exemple composite StyleBook composite** que vous avez créé dans Créer un StyleBook composite. Utilisez l'API REST pour créer un pack de configuration à partir de ce StyleBook comme suit :

```
POST http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/composite-example/configpacks
<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

  "configpack":
  {

    "parameters": {

      "name": "myapp",
```



```
11         "ip": "2.2.2.2",
12         "svc-servers": ["10.102.29.52","10.102.29.53"]
13       }
14   ,
15      "target_devices":
16      [
17      {
18
19        "id": "deecee30-f478-4446-9741-a85041903410"
20       }
21   ,
22      {
23
24        "id": "debecc60-d589-4557-8632-a74032802412"
25       }
26
27      ]
28    }
29
30   }
31
32   <!--NeedCopy-->
```

Dans cette requête HTTP, la configuration est créée sur deux instances Citrix ADC représentées par leurs ID. Si vous ouvrez une session sur les instances Citrix ADC, vous pouvez afficher les objets de configuration créés par le StyleBook « basic-lb-config » qui a été importé dans le StyleBook « composite-example ». Vous pouvez également voir un nouveau moniteur HTTP appelé « myapp-mon » qui faisait partie du StyleBook « composite-example ».

En cas de création réussie du pack de configuration, la réponse HTTP suivante est reçue :

```
1  200 OK
2  Content-Type: application/json{
3
4    "configpack": {
5
6      "config_id": "4917276817"
7     }
8
9   }
10
11  <!--NeedCopy-->
```

Mise à jour d'une configuration

Pour mettre à jour cette configuration, par exemple, en ajoutant un nouveau serveur principal avec l'adresse IP 10.102.29.54 au serveur virtuel d'équilibrage de charge myapp, utilisez l'API pour mettre à jour un pack de configuration comme suit :


```
PUT http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/composite-example/configpacks/4917276817
<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

  "configpack": {

    "parameters": {

      "name": "myapp",
      "ip": "2.2.2.2",
      "svc-servers": ["10.102.29.52","10.102.29.53","10.102.29.54"]
    }
 ,
  "target_devices":
  [
    {

    "id": "deecee30-f478-4446-9741-a85041903410"
     }
 ,
  {

    "id": "debecc60-d589-4557-8632-a74032802412"
   }

]
 }

 }

<!--NeedCopy-->
```

En cas de mise à jour réussie du pack de configuration, la réponse HTTP suivante est reçue :

```
200 OK
Content-Type: application/json
{

   "configpack": {

     "config-id": "4917276817"
   }

 }

<!--NeedCopy-->
```


Suppression d'une configuration

Pour supprimer cette configuration (de toutes les instances Citrix ADC), vous pouvez utiliser l'API pour supprimer un pack de configuration comme suit :

```
DELETE http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/composite-example/configpacks/4917276817
<!--NeedCopy-->
```

```
Accept: application/json
<!--NeedCopy-->
```

En cas de suppression réussie du pack de configuration, la réponse HTTP suivante est reçue :

```
200 OK
Content-Type: application/json
{

   "configpack": {

     "config_id": "4917276817"
   }

 }

<!--NeedCopy-->
```

Vous pouvez vous connecter à l'instance Citrix ADC et vérifier que tous les objets de configuration qui font partie de ce pack de configuration ont été supprimés.

Si vous souhaitez supprimer la configuration d'instances Citrix ADC spécifiques au lieu de toutes, utilisez l'opération de pack de configuration de mise à jour décrite ci-dessus et modifiez l'attribut « target_devices » dans la charge utile JSON pour supprimer les ID d'instance Citrix ADC spécifiques.

Utiliser l'API pour créer des configurations pour charger des fichiers de certificat et de clé

February 1, 2024

Utilisez les API StyleBook pour créer des configurations basées sur ce StyleBook. Vous pouvez utiliser n'importe quel outil tel que l'outil de ligne de commande curl ou l'extension du navigateur Chrome Postman pour envoyer des requêtes HTTP à Citrix Application Delivery Management (ADM).

Prenons l'exemple StyleBook que vous avez créé pour télécharger les fichiers de certificat et de clé dans Comment créer un StyleBook pour télécharger des fichiers de certificat et de clé de certificat

SSL vers Citrix ADM. Utilisez l'API REST pour créer un pack de configuration à partir de ce StyleBook comme suit :

```
POST

https://<MAS_IP_Address>/stylebook/nitro/v1/config/stylebooks/com.
   citrix.adc.stylebooks/1.0/lb-mon/configpacks?mode=async
<!--NeedCopy-->
```

```
Content-Type: application/jsonAccept: application/json {

   "configpack": {

       "parameters": {

           "lb-appname": "lbmon",
           "lb-virtual-ip": "13.1.11.10",
           "lb-virtual-port": "80",
           "lb-service-type": "HTTP",
           "svc-service-type": "HTTP",
           "svc-servers": [
               {

                   "ip": "14.1.1.15",
                   "port": "80"         }

      ],
           "certificates": [
               {

                   "cert-name": "server_cert",
                   "cert-file": "server_cert.pem",
                   "ssl-inform": "PEM",
                   "key-name": "server_key",
                   "key-file": "server_key.pem",
                   "cert-password": "secret",
                   "cert-advanced": {

                       "is-ca-cert": false,
                       "skip-ca-name": false
           }

         }

      ],
           "lb-advanced": {

               "flush-on-state-down": "ENABLED",
               "auth-params": {

                   "authentication": "OFF",
                   "authentication-http-401": "OFF"
         }
```



```
45  ,
46                  "appflow-log": "ENABLED",
47                  "algorithm": "LEASTCONNECTION"
48          }
49  ,
50              "svcg-advanced": {
51
52                  "svc-client-ip": "DISABLED",
53                  "svc-use-source-ip": "NO",
54                  "svc-use-proxy-port": "NO",
55                  "svc-surge-protection": "OFF",
56                  "svc-client-keepalive": "NO",
57                  "svc-tcp-buffering": "NO",
58                  "svc-compression": "NO",
59                  "svc-state": "ENABLED",
60                  "svc-downstate-flush": "DISABLED",
61                  "svc-enable-health-monitor": "NO"
62          }
63
64       }
65  ,
66          "targets": [
67              {
68
69                  "id": "8c158e7a-0087-423f-91b0-0ccf16de552a"
70          }
71
72       ]
73     }
74
75  }
76
77  <!--NeedCopy-->
```

Ce pack de configuration est identifié de manière unique à l'aide de l'ID 8c158e7a-0087-423f-91b0-0ccf16de552a. Vous pouvez utiliser cet ID pour interroger, mettre à jour ou supprimer la configuration. En cas de mise à jour réussie du pack de configuration, les fichiers de certificat et de clé sont téléchargés sur le système de fichiers Citrix ADM.

Utiliser l'API pour créer des configurations pour télécharger n'importe quel type de fichier

February 1, 2024

Vous pouvez également utiliser l'API Citrix Application Delivery Management (ADM) pour créer un pack de configuration qui charge des fichiers vers l'instance Citrix ADC sélectionnée.

Prenons l'exemple StyleBook que vous avez créé pour télécharger des fichiers de tout type

dansComment créer un StyleBook pour télécharger des fichiers vers le service Citrix ADC MA. Comme dans l'exemple dans la rubrique ci-dessus, créez un pack de configuration et spécifiez la valeur du paramètre « locationfile » comme chemin d'accès au fichier d'emplacement sur Citrix ADM.
Utilisez l'API REST pour créer un pack de configuration à partir de ce StyleBook comme suit :

```
POST

https://<mas_ip>/stylebook/nitro/v1/config/stylebooks/com.citrix.adc.
   stylebooks.samples/1.0/upload-geolocations/configpacks
<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

   "configpack":
   {

      "parameters": {

         "locationfile": "/var/mps/tenants/root/files/ /
          custom_geolocations.csv"
      }
 ,
      "targets": [
         {

            "id": "5e540839-cd6c-437e-ac53-7d49bc2602b5"
       }

    ]
   }

 }

<!--NeedCopy-->
```

Utiliser l'API pour importer des StyleBooks personnalisés

February 1, 2024

Vous pouvez désormais utiliser les API StyleBook pour importer des StyleBooks personnalisés dans Citrix Application Delivery Management (ADM). Utilisez l'API REST pour créer un pack de configuration à partir de ce StyleBook comme suit dans n'importe quel outil tel que l'outil de ligne de commande curl ou l'extension du navigateur Chrome Postman. Par exemple, vous pouvez importer un StyleBook nommé exemple-lb qui peut être utilisé pour créer une configuration d'équilibrage de charge sur une

instance Citrix ADC.

```
HTTP Method: POST
URL: http://<mas-ip>/stylebook/nitro/v1/config/stylebooks
Headers:
Content-Type: application/json
Accept: application/json
RequestBody:
{

       "stylebook":
  {

     "file_name": "example-lb.yaml",
     "source": "<base64-contents>",
     "encoding": "base64"
   }

 }

<!--NeedCopy-->
```

où, la valeur de l'attribut « source », est l'encodage base64 du contenu de votre fichier StyleBook. Vous pouvez coller le contenu YAML de votre fichier StyleBook dans un outil en ligne, par exemple, https://www.browserling.com/tools/file-to-base64 pour obtenir la chaîne base64 que vous pouvez ensuite utiliser comme valeur pour l'attribut « source » ci-dessus.

À l'aide de cet appel API, vous pouvez également télécharger un fichier tarball compressé (fichier .tgz) contenant plusieurs fichiers StyleBook en une seule opération API. Pour ce faire, changez simplement l'attribut file_name par le nom de fichier .tgz et la valeur de l'attribut source par le codage base64 du contenu de votre fichier .tgz.

Une fois l'API exécutée avec succès dans l'outil, vous obtenez la réponse suivante qui indique que le StyleBook a été importé dans Citrix ADM.

```
200 OK
<!--NeedCopy-->
```

Corps de réponse :

```
{


  "stylebook":
{


    "name": "example-lb",

    "namespace": "com.example.stylebook",

```



```
    "version": "1.0"

   }


 }

<!--NeedCopy-->
```

Utiliser l'API pour télécharger des StyleBooks personnalisés

February 1, 2024

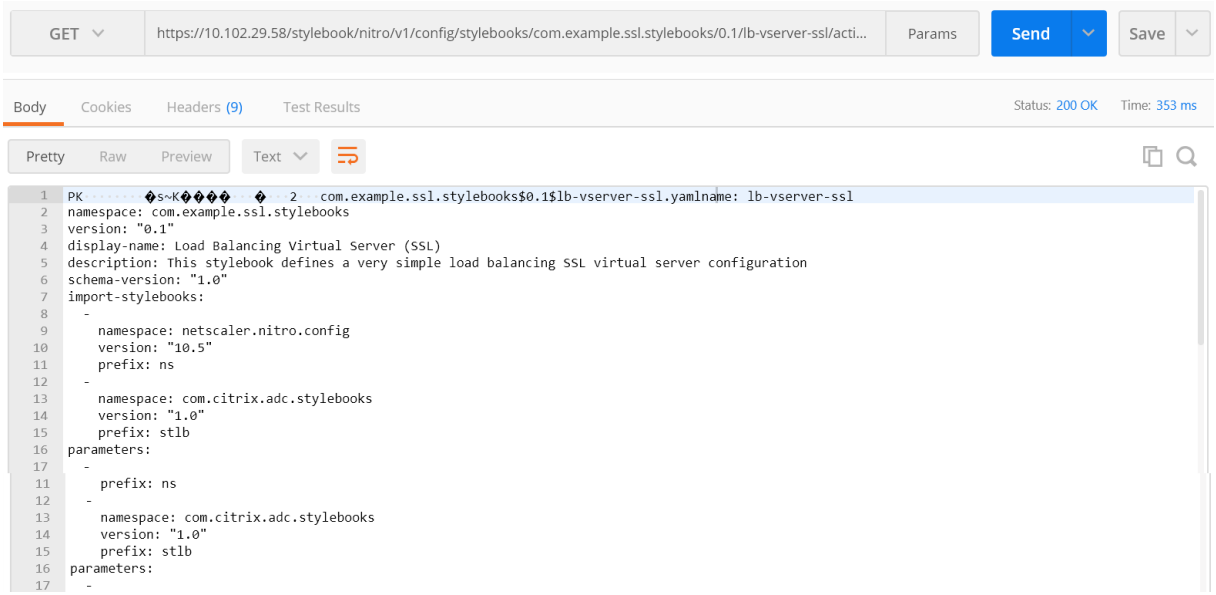
Vous pouvez télécharger un StyleBook personnalisé en fournissant l'API REST StyleBooks suivante :

```
GET

https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks/<NAMESPACE>/<
   VERSION>/<NAME>/actions/download
<!--NeedCopy-->
```

Vous pouvez exécuter l'API dans n'importe quel outil tel que l'outil de ligne de commande curl ou l'extension de navigateur Postman Chrome après avoir modifié les champs d'adresse IP, de nom, de version et d'espace de noms.

```
GET

https://10.102.29.58/stylebook/nitro/v1/config/stylebooks/com.example.
   ssl.stylebooks/0.1/lb-vserver-ssl/actions/download`
<!--NeedCopy-->
```

Le StyleBook au format .yaml est téléchargé.



Utiliser l'API pour supprimer des StyleBooks personnalisés

February 1, 2024

Vous pouvez supprimer le StyleBook personnalisé en fournissant l'API REST StyleBooks suivante :

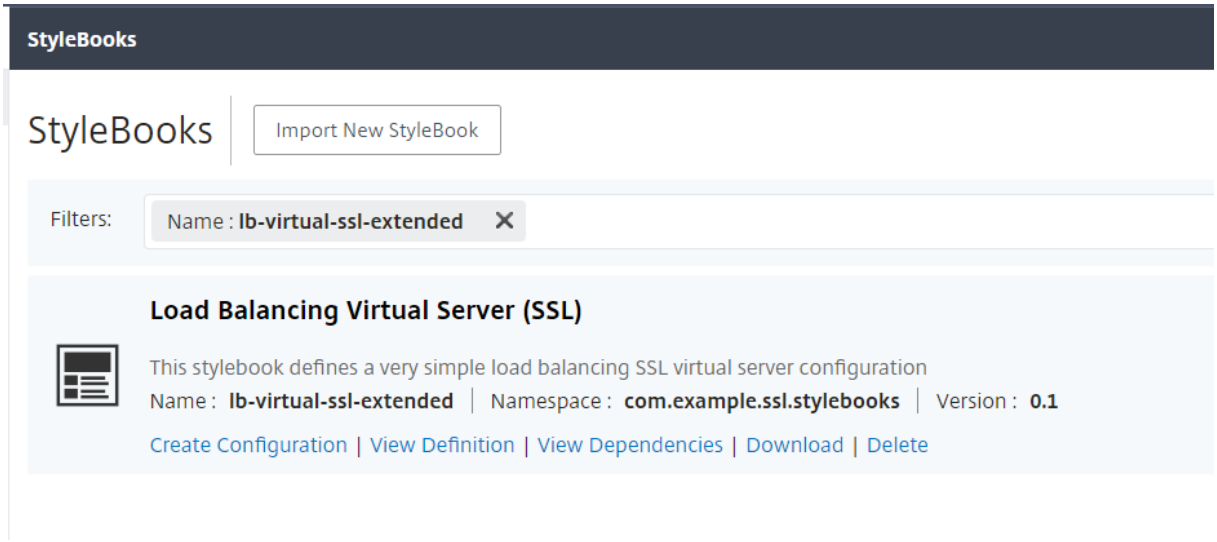
```
DELETE

https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks/<NAMESPACE>/<
    VERSION>/<NAME>?dependencies=true
<!--NeedCopy-->
```

Si le paramètre de requête dépendances de l'URL n'est pas fourni ou si sa valeur est définie sur false, les dépendances StyleBook ne sont pas supprimées (seul le StyleBook lui-même est supprimé).

Lorsque vous recevez un code d'état de réponse HTTP 200, cela signifie que le StyleBook personnalisé (et ses dépendances) est correctement supprimé de Citrix ADM.

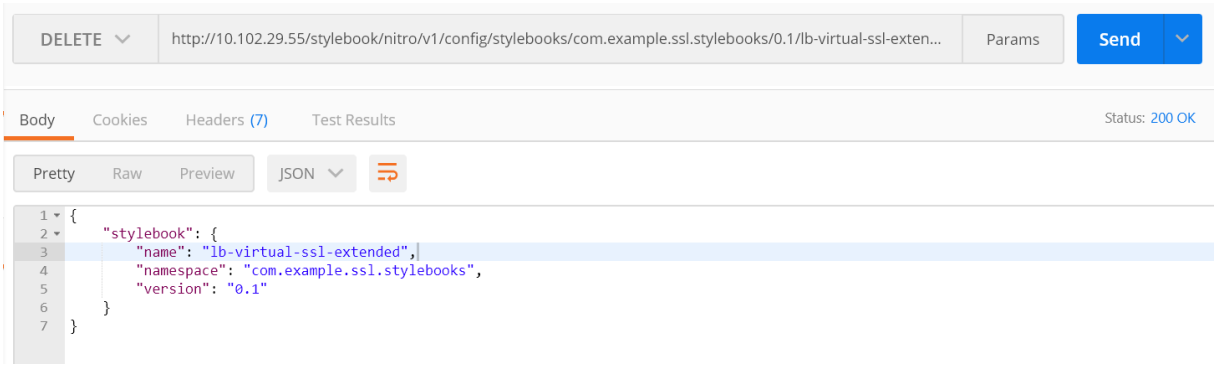
> **Remarque**
>
> Vous ne pouvez pas supprimer un StyleBook personnalisé qui possède d'autres StyleBooks dans le service MA qui en dépendent.

Par exemple, supposons que vous avez créé un StyleBook nommé « lb-virtual-ssl-extended » dans Citrix ADM. Vous avez ensuite décidé de supprimer ce StyleBook.

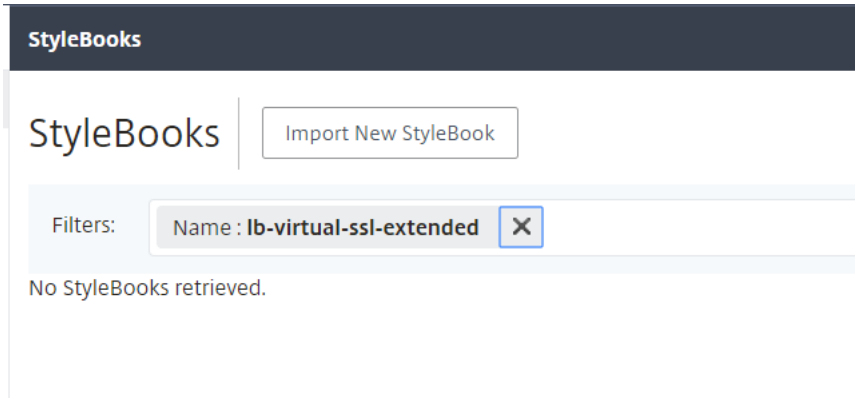


Vous pouvez exécuter l'API dans n'importe quel outil tel que l'outil de ligne de commande curl ou l'extension de navigateur Postman Chrome après avoir modifié les champs d'adresse IP, de nom, de version et d'espace de noms.

SUPPRIMER https://10.102.29.55/stylebook/nitro/v1/config/stylebooks/com.example.ssl.stylebooks/0.1/lb-virtual-ssl-extended?dependencies=false



Le StyleBook est supprimé de Citrix ADM.



Grammaire de StyleBooks

February 1, 2024

Vous pouvez concevoir vos propres StyleBooks, les importer dans Citrix Application Delivery Management (ADM), puis les utiliser pour créer des configurations à l'aide de l'interface graphique Citrix ADM ou à l'aide d'API. Pour pouvoir créer vos propres StyleBooks, vous devez d'abord comprendre la grammaire et la syntaxe des différentes constructions et attributs que vous pouvez utiliser.

Ce document décrit les différentes constructions et références que vous pouvez utiliser lors de la création de StyleBooks.

Cliquez sur le nom d'une section, d'une construction ou d'une référence dans le tableau ci-dessous pour afficher les détails.

[Header](/fr-fr/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/header-section.html)	[Importer des StyleBooks](/fr-fr/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/import-stylebooks-section.html)
[Parameters](/fr-fr/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/parameters-section.html)	[Parameters-default-sources construct](/fr-fr/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/parameters-default-sources-construct.html)
[Substitutions](/fr-fr/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/substitutions.html)	[Components](/fr-fr/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/components.html)
[Propriétés facultatives](/fr-fr/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/optional-properties.html)	[Composants d'assistance](/fr-fr/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/helper-components.html)
[Propriétés, sources par défaut](/fr-fr/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/properties-default-sources.html)	[Composants imbriqués](/fr-fr/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/nested-components.html)
[Conditionner la construction](/fr-fr/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/condition-construct.html)	[Construction repeat](/fr-fr/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/repeat-construct.html)
[Construction repeat-condition](/fr-fr/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/repeat-condition-construct.html)	[Outputs](/fr-fr/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/outputs.html)
[Répétitions imbriquées](/fr-fr/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-

grammar/nested-repeats.html) | [Référence parent](/fr-fr/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/parent-reference.html) |
| [Référence des paramètres](/fr-fr/netscaler-application-delivery-management-software/13/stylebooks/stylebook
grammar/parameter-reference.html) | [Référence des substitutions](/fr-fr/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/substitutions-reference.html) |
| [Référence des composants](/fr-fr/netscaler-application-delivery-management-software/13/stylebooks/styleboo
grammar/components-reference.html) | [Operations](/fr-fr/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/operations.html) |
[Référence de variable](/fr-fr/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/variable-reference.html)	[Alarms](/fr-fr/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/alarms.html)
[Analytics](/fr-fr/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/analytics.html)	[Fonctions intégrées](/fr-fr/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/built-in-functions.html)
[Expressions](/fr-fr/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/expressions.html)	[Détection des dépendances](/fr-fr/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/dependency-detection.html)
Interpolations sur place

> **Remarque**
>
> Lorsque vous définissez un élément de répétition, un indice de répétition ou des arguments de fonctions de substitution, n'utilisez pas les mots réservés suivants pour nommer une variable définie par l'utilisateur, $<var-name>
>
> - livre de style, paramètres, substitutions, composants, propriétés, sorties, parent, self, opérations, analyses, alarmes
> - repeat-item, repeat-item-0, repeat-item-1, repeat-item-2
> - indice de répétition, indice de répétition 0, indice de répétition 1, indice de répétition 2
> - default
> - rôles, rôle, cibles, cible
> - context, parent-context, parent_context

Pour plus d'informations et des exemples sur la façon de concevoir vos propres StyleBooks, consultez Comment créer vos propres StyleBooks.

En-tête

February 1, 2024

Les six premières lignes d'un StyleBook constituent la section d'en-tête. Cette section vous permet de définir l'identité d'un StyleBook et de décrire son rôle. Il s'agit d'une section obligatoire.

Le tableau suivant décrit les attributs de la section d'en-tête :

|Attribut| Description|
—	—
nom	Un nom permettant d'identifier le StyleBook. Cet attribut est obligatoire.
display-name	Un nom descriptif pour le StyleBook. Ce nom apparaît sur l'interface graphique Citrix ADM. Il s'agit d'un attribut facultatif.
description	Un texte de description définit ce que fait ce StyleBook. Cette description apparaît sur l'interface graphique ADM. Il s'agit d'un attribut facultatif. **Remarque :** Il s'agit d'un fragment HTML et vous pouvez utiliser des balises HTML pour personnaliser les titres ou insérer des images à l'aide de la balise <img> contenant des URL ou des images intégrées.
auteur	L'auteur, la personne ou l'organisation qui crée le StyleBook. Il s'agit d'un attribut facultatif.
espace de noms	Un espace de noms fait partie de l'identifiant unique d'un StyleBook afin d'éviter les collisions de noms. Un espace de noms peut être n'importe quelle chaîne, mais il est recommandé de l'utiliser pour nommer la société, le service ou l'unité qui a créé ou possède un ensemble de StyleBooks. Par exemple, vous pouvez utiliser le format suivant : <company>.<department>.<unit>.stylebooks. Il s'agit d'un attribut obligatoire.
version	Numéro de version du StyleBook. Vous pouvez modifier le numéro de version lorsque vous mettez à jour un StyleBook. Les StyleBooks de différentes versions peuvent coexister ensemble. Il s'agit d'un attribut obligatoire.
version du schéma	Version du schéma StyleBooks. Il prend la valeur « 1.0 » dans la version actuelle de Citrix ADM. Il s'agit d'un attribut obligatoire.
privé	Si cet attribut est défini sur true, le StyleBook ne s'affiche pas sur l'interface graphique Citrix ADM. Il s'agit d'un paramètre utile pour les StyleBooks qui sont des éléments de base pour d'autres StyleBooks et qui ne sont pas destinés à être utilisés directement par les utilisateurs. Il s'agit d'un attribut facultatif. Sa valeur par défaut est false.

Exemple :

```
1      name: lb
2      description: "This stylebook defines a sample load balancing
      configuration."
3      display-name: "Load Balancing StyleBook (HTTP)"
4      author: Mike Smith (ACME Infra team)
5      namespace: com.example.stylebooks
6      schema-version: "1.0"
7      version: "0.1"
8  <!--NeedCopy-->
```

La combinaison du nom, de l'espace de noms et de la version identifie de manière unique un Style-

Book dans le système. Vous ne pouvez pas avoir deux StyleBooks avec la même combinaison de nom, d'espace de noms et de version dans Citrix ADM. Cependant, vous pouvez avoir deux StyleBooks avec le même nom et la même version mais des espaces de noms différents, ou avec le même espace de noms et la même version mais des noms différents.

Importer des StyleBooks

February 1, 2024

Il s'agit de la deuxième section de votre StyleBook et vous permet de déclarer à quel autre StyleBook vous souhaitez faire référence à partir de votre StyleBook actuel. Cela vous permet d'importer et de réutiliser d'autres StyleBooks au lieu de recréer la même configuration dans votre propre StyleBook. Il s'agit d'une section obligatoire.

Vous devez déclarer l'**espace de noms** et le numéro de **version** du ou des StyleBook auxquels vous souhaitez faire référence dans votre StyleBook actuel. Chaque StyleBook doit faire référence à l'espace de noms netscaler.nitro.config s'il utilise directement l'un des objets de configuration NITRO. Cet espace de noms contient tous les types NITRO Citrix ADC, tels que le service lbvserver ou le moniteur. StyleBooks for Citrix ADC versions 10.5 et ultérieures sont pris en charge, ce qui signifie que vous pouvez utiliser votre StyleBook pour créer et exécuter des configurations sur n'importe quelle instance Citrix ADC exécutant la version 10.5 ou ultérieure.

L'attribut **préfixe** utilisé dans la section import-stylebooks est un raccourci qui fait référence à la combinaison de l'espace de noms et de la version. Par exemple, le préfixe « ns » peut être utilisé pour faire référence à l'espace de noms netscaler.nitro.config avec la version 10.5. Dans les sections ultérieures de votre StyleBook, au lieu d'utiliser l'espace de noms et la version chaque fois que vous souhaitez faire référence à un StyleBook avec cet espace de noms et cette version, vous pouvez simplement utiliser la chaîne de préfixe choisie avec le nom du StyleBook pour l'identifier de manière unique.

Exemple :

```
      import-stylebooks:
       -
         namespace: netscaler.nitro.config
         version: "10.5"
         prefix: ns
      -
       namespace: com.acme.stylebooks
        version: "0.1"
        prefix: stlb
<!--NeedCopy-->
```

Dans l'exemple ci-dessus, le premier préfixe défini s'appelle ns et fait référence à l'espace de noms netscaler.nitro.config et à la version 10.5. Le deuxième préfixe défini s'appelle stlb et fait référence à

l'espace de noms com.acme.stylebooks et à la version 0.1.

Après avoir défini un préfixe, chaque fois que vous souhaitez faire référence à un type ou à un StyleBook appartenant à un espace de noms et à une version spécifiques, vous pouvez utiliser la notation **<namespace-shorthand>::<type-name>**. Par exemple, **ns : :lbvserver fait référence au type lbvserver** défini dans l'espace de noms netscaler.nitro.config, version 10.5.

De même, si vous voulez faire référence à un StyleBook avec la version « 0.1 » dans l'espace de noms com.acme.stylebooks, vous pouvez utiliser la notation **stlb::<stylebook-name>**.

> **Remarque**
>
> Par convention, le préfixe « ns » est utilisé pour faire référence à l'espace de noms NITRO de Citrix ADC.

Paramètres

February 1, 2024

Cette section vous permet de définir tous les paramètres dont vous avez besoin dans votre StyleBook pour créer une configuration. Il décrit l'entrée que votre StyleBook prend. Bien que cette section soit facultative, la plupart des StyleBook peuvent en avoir besoin. Vous pouvez considérer la section Paramètres pour définir les champs des utilisateurs qui utilisent le StyleBook pour créer une configuration sur une instance Citrix ADC.

Lorsque vous importez votre StyleBook dans Citrix ADM et que vous l'utilisez pour créer une configuration, l'interface graphique utilise cette section du StyleBook pour afficher un formulaire. Ce formulaire prend une entrée pour les valeurs de paramètre définies.

La section suivante décrit les attributs que vous devez spécifier pour chaque paramètre de cette section :

'**nom**'

Nom du paramètre que vous souhaitez définir. Vous pouvez spécifier un nom alphanumérique.

Le nom doit commencer par un alphabet et peut inclure plus d'alphabets, de nombres, de trait d' union (-) ou de trait de soulignement (_).

Lorsque vous écrivez un StyleBook, vous pouvez utiliser cet attribut « name » pour faire référence au paramètre dans d'autres sections en utilisant la notation $parameters. <name>.

Obligatoire ? Oui

‘étiquette’

Chaîne affichée dans l’interface graphique d’ADM en tant que nom de ce paramètre.

Obligatoire ? Non

‘description’

Chaîne d’aide qui décrit à quoi sert le paramètre. L’interface graphique ADM affiche ce texte lorsque l’utilisateur clique sur l’icône d’aide associée à ce paramètre.

Obligatoire ? Non

‘type’

Type de valeur que ces paramètres peuvent prendre. Les paramètres peuvent être de l’un des types intégrés
suivants :

- string : un tableau de caractères. Si aucune longueur n’est spécifiée, la valeur de la chaîne peut prendre n’importe quel nombre de caractères. Toutefois, vous pouvez limiter la longueur d’un type de chaîne en utilisant les attributs min-length et max-length.
- `number` : nombre entier. Vous pouvez spécifier le nombre minimum et maximum que ce type peut prendre en utilisant les attributs min-value et max-value.
- **`boolean`** : Peut être vrai ou faux. YAML considère tous les littéraux comme des booléens (par exemple, Oui ou Non).
- `ipaddress` : chaîne représentant une adresse IPv4 ou IPv6 valide.
- `tcp-port` : nombre compris entre 0 et 65535 qui représente un port TCP ou UDP.
- `password` : Représente une valeur de chaîne opaque/secrète. Lorsque l’interface graphique ADM affiche une valeur pour ce paramètre, elle est affichée sous forme d’astérisques (*****).
- `certfile` : Représente un fichier de certificat. Cette valeur vous permet de charger les fichiers directement à partir de votre système local lorsque vous créez une configuration StyleBook à l’aide de l’interface graphique ADM. Le fichier de certificat téléchargé est stocké dans le répertoire `/var/mps/tenants/\<tenant_path>/ns_ssl_certs` d’ADM.

  Le fichier de certificat est ajouté à la liste des certificats gérés par ADM.
- `keyfile` : Représente un fichier de clé de certificat. Cette valeur vous permet de charger le fichier directement à partir de votre système local lorsque vous créez une configuration StyleBook à l’aide de l’interface graphique ADM. Le fichier de certificat téléchargé est stocké dans le répertoire `/var/mps/tenants/\<tenant_path>/ns_ssl_keys` d’ADM.

Le fichier de clé de certificat est ajouté à la liste des clés de certificat gérées par ADM.

- `file` : Représente un fichier.
- `object` : Ce type est utilisé lorsque vous souhaitez regrouper plusieurs paramètres associés sous un élément parent. Spécifiez le paramètre parent le type comme « objet ». Un paramètre de type « objet » peut avoir une section « paramètres » imbriquée pour décrire les paramètres qu'il contient.
- `another StyleBook` : lorsque vous utilisez ce type de paramètre, ce paramètre s'attend à ce que sa valeur soit sous la forme des paramètres définis dans le StyleBook indiquant son type.

Un paramètre peut également avoir un `type` qui est la liste des types. Pour ce faire, ajoutez `[]` à la fin du type. Par exemple, si l'`type` attribut est `string[]`, ce paramètre prend une liste de chaînes en entrée. Vous pouvez fournir une, deux ou plusieurs chaînes pour ce paramètre lors de la création d'une configuration à partir de ce StyleBook.

Obligatoire ? Oui

'réseau'

Pour `type: ipaddress`, vous pouvez spécifier l'`network` attribut pour allouer automatiquement une adresse IP à partir d'un réseau ADM IPAM.

ADM alloue automatiquement une adresse IP à partir de l'attribut `network` lorsque vous créez une configuration StyleBook.

Exemple :

```
        name: virtual-ip
        label: "Load Balancer IP Address"
        type: ipaddress
        network: "network-1"
        required: true
<!--NeedCopy-->
```

Dans cet exemple, le `virtual-ip` champ alloue automatiquement une adresse IP à partir de `network-1`.L'adresse IP est libérée sur le réseau lorsque la configuration est supprimée.

'allocation dynamique'

L'`dynamic-allocation` attribut est ajouté dans la définition du paramètre de `type: ipaddress`. Utilisez cet attribut pour répertorier dynamiquement les réseaux ADM IPAM. Cet attribut peut prendre **`true`** soit soit **`false`** en entrée. Pour `type: ipaddress`, spécifiez l'`dynamic-allocation: true` attribut pour répertorier dynamiquement les réseaux ADM IPAM

qui sont dans ADM. Dans le formulaire de création du pack de configuration, vous pouvez effectuer les opérations suivantes :

1. Sélectionnez le réseau IPAM requis dans la liste.
2. Spécifiez une adresse IP que vous souhaitez allouer à partir du réseau IPAM sélectionné.

   Si aucune adresse IP n'est spécifiée, l'ADM alloue automatiquement une adresse IP à partir du réseau IPAM sélectionné.

Exemple :

```
  -
    name: virtual-ip
    label: "Load Balancer IP Address"
    type: ipaddress
    dynamic-allocation: true
    required: true
<!--NeedCopy-->
```

Dans cet exemple, le `virtual-ip` champ répertorie les réseaux ADM IPAM qui sont dans ADM. Sélectionnez un réseau dans la liste pour allouer automatiquement une adresse IP à partir du réseau. L'adresse IP est libérée sur le réseau lorsque la configuration est supprimée.

'clé'

Spécifiez true ou false pour indiquer si ce paramètre est un paramètre clé pour le StyleBook.

Un StyleBook ne peut avoir qu'un seul paramètre défini comme paramètre « key ».

Lorsque vous créez des configurations différentes à partir du même StyleBook (sur des instances ADC identiques ou
différentes), chaque configuration a une valeur différente ou unique pour ce
paramètre.

La valeur par défaut est false.

Obligatoire ? Non

« requis »

Spécifiez true ou false pour indiquer si un paramètre est obligatoire ou facultatif. S'il est défini sur true, le paramètre est obligatoire et l'utilisateur doit fournir une valeur pour ce paramètre lors de la création de configurations.

L'interface graphique ADM oblige l'utilisateur à fournir une valeur valide pour ce paramètre.

La valeur par défaut est false.

Obligatoire ? Non

« valeurs allouées »

Utilisez cet attribut pour définir une liste de valeurs valides pour un paramètre, lorsque le type est défini sur « string. »

Lors de la création d'une configuration à partir de l'interface graphique ADM, l'utilisateur est invité à sélectionner une valeur de paramètre dans cette liste.

> **Remarque**
>
> Si vous souhaitez afficher les valeurs de la liste sous forme d'options radio, définissez l'`layout` attribut.

Exemple 1 :

```
-
      name: ipaddress
      type: string
      allowed-values:
            -  SOURCEIP
            -  DEST IP
            -  NONE
<!--NeedCopy-->
```

Exemple 2 :

```
-
      name: TCP Port
      type: tcp-port
      allowed-values:
            -  80
            -  81
            -  8080
<!--NeedCopy-->
```

Exemple 3 :

Liste de `tcp-ports`, où chaque élément de la liste ne peut avoir que des valeurs spécifiées dans `allowed-values`.

```
-
      name: tcpports
      type: tcp-port[]
      allowed-values:
            -  80
            -  81
            -  8080
            -  8081
<!--NeedCopy-->
```


Obligatoire ? Non

« par défaut »

Utilisez cet attribut pour affecter une valeur par défaut à un paramètre facultatif. Lorsqu'un utilisateur crée une configuration sans spécifier de valeur, la valeur par défaut est utilisée.

Le paramètre ne prend aucune valeur si les conditions suivantes sont remplies :

- Le paramètre n'a pas de valeur par défaut.
- Un utilisateur ne fournit pas de valeur pour le paramètre.

Exemple 1 :

```
-
      name: timeout
      type: number
      default: 20
<!--NeedCopy-->
```

Exemple 2 :

Pour répertorier les valeurs par défaut du paramètre :

```
-
      name: protocols
      type: string[]
      default:
            -  TCP
            -  UDP
            -  IP
<!--NeedCopy-->
```

Exemple 3 :

```
-
      name: timeout
      type: number
      default: 20
<!--NeedCopy-->
```

Exemple 4:

```
-
      name: tcpport
      type: tcp-port
      default: 20
<!--NeedCopy-->
```

Obligatoire ? Non

« modèle »

Utilisez cet attribut pour définir un motif (expression régulière) pour les valeurs valides de ce paramètre, lorsque le type du paramètre est « string. »

Exemple :

```
-
      name: appname
      type: string
      pattern: "[a-z]+"
<!--NeedCopy-->
```

Obligatoire ? Non

‘Min-valeur’

Utilisez cet attribut pour définir la valeur minimale pour les paramètres de type `number` ou `tcp-port`.

Exemple :

```
-
      name: audio-port
      type: tcp-port
      min-value: 5000
<!--NeedCopy-->
```

Les `min-value` nombres peuvent être négatifs. Cependant, le `min-value` for `tcp-port` doit être positif.

Obligatoire ? Non

‘max-value’

Utilisez cet attribut pour définir la valeur maximale des paramètres de type `number` ou `tcp-port`.

Assurez-vous que la valeur maximale est supérieure à la valeur minimale, si elle est définie.

Exemple :

```
-
      name: audio-port
      type: tcp-port
      min-value: 5000
      max-value: 15000
<!--NeedCopy-->
```


Obligatoire ? Non

‘min-longueur’

Utilisez cet attribut pour définir la longueur minimale des valeurs acceptées pour un paramètre de type « string. »

Assurez-vous que la longueur minimale des caractères définis comme valeurs est supérieure ou égale à zéro.

Exemple :

```
-
      name: appname
      type: string
      min-length: 3
<!--NeedCopy-->
```

Obligatoire ? Non

‘longueur’

Utilisez cet attribut pour définir la longueur maximale des valeurs acceptées pour un paramètre de type « string. »

Assurez-vous que la longueur maximale des valeurs est supérieure ou égale à la longueur des caractères définis dans `min-length`.

Exemple :

```
-
      name: appname
      type: string
      max-length: 64
<!--NeedCopy-->
```

Obligatoire ? Non

‘min-items’

Utilisez cet attribut pour définir le nombre minimal d’éléments d’un paramètre qui est une liste.

Assurez-vous que le nombre minimum d’articles est supérieur ou égal à zéro.

Exemple :


```
-
      name: server-ips
      type: ipaddress[]
      min-items: 2
<!--NeedCopy-->
```

Obligatoire ? Non

‘max-items’

Utilisez cet attribut pour définir le nombre maximal d’éléments dans un paramètre qui est une liste.

Assurez-vous que le nombre maximal d’éléments est supérieur au nombre minimal d’éléments si défini.

Exemple :

```
-
      name: server-ips
      type: ipaddress[]
      min-items: 2
      max-items: 250
<!--NeedCopy-->
```

Obligatoire ? Non

‘gui’

Utilisez cet attribut pour personnaliser la disposition du paramètre dans l’interface graphique ADM.

Obligatoire ? Non

‘colonnes’

Cet attribut est un sous-attribut de l’attribut `gui`. Utilisez cet attribut pour définir le nombre de colonnes pour afficher les `type: object[]` paramètres dans l’interface graphique ADM.

Obligatoire ? Non

‘updatable’

Cet attribut est un sous-attribut de l’`gui` attribut. Utilisez cet attribut pour spécifier si le paramètre peut être mis à jour après la création de la configuration. Définissez cet attribut uniquement sur des types de paramètres simples tels que chaîne, booléenne ou nombre.

Si la valeur est définie sur **false**, le champ paramètre est grisé lorsque vous mettez à jour la configuration.

Obligatoire ? Non

‘collapse_pane’

Cet attribut est un sous-attribut de l’attribut gui. Utilisez cet attribut pour spécifier si le volet définissant la disposition de ce paramètre d’objet est réductible.

Si la valeur est définie sur true, l’utilisateur peut développer ou réduire les paramètres enfants sous ce paramètre parent.

Exemple :

```
gui:

 collapse_pane: true

 columns: 2
<!--NeedCopy-->
```

Exemple de section complète des paramètres :

```
parameters:

   -

      name: name

      label: Name

      description: Name of the application

      type: string

      required: true

   -

      name: ip

      label: IP Address

      description: The virtual IP address used for this application

      type: ipaddress

      required: true

   -
```



```
28
29        name: svc-servers
30
31        label: Servers
32
33        type: object[]
34
35        required: true
36
37        parameters:
38
39          -
40
41                name: svc-ip
42
43                label: Server IP
44
45                description: The IP address of the server
46
47                type: ipaddress
48
49                required: true
50
51          -
52
53                name: svc-port
54
55                label: Server Port
56
57                description: The TCP port of the server
58
59                type: tcp-port
60
61                default: 80
62
63          -
64
65                name: lb-alg
66
67                label: LoadBalancing Algorithm
68
69                type: string
70
71                allowed-values:
72
73                   - ROUNDROBIN
74
75                   - LEASTCONNECTION
76
77                default: ROUNDROBIN
78
79          -
80
```



```
                name: enable-healthcheck

                label: Enable HealthCheck?

                type: boolean

                default: true
<!--NeedCopy-->
```

Voici un exemple qui définit tous les attributs d'une liste et les valeurs expliquées dans les sections précédentes :

```
        -
                name: features-list

                type: string[]

                min-length: 1

                max-length: 3

                min-items: 1

                max-items: 3

                pattern: "[A-Z]+"

                allowed-values:

                  - SP

                  - LB

                  - CS

                default:

                  - LB
<!--NeedCopy-->
```

'mise en page '

Cet attribut est un sous-attribut de l'attribut `gui`. Utilisez cet attribut pour afficher les valeurs de liste sous forme de boutons radio. Définissez l'`layout` attribut sur `radio` dans la section des paramètres d'une définition StyleBook. Elle s'applique au paramètre qui possède l'`allowed-values` attribut. Lorsque vous créez un pack de configuration, l'interface graphique ADM affiche les valeurs de la `allowed-values` liste sous forme de boutons radio.

Exemple :


```
-
    gui:
        layout: radio
    allowed-values:
        - One
        - Two
        - Three
<!--NeedCopy-->
```

Les valeurs Un, Deux et Trois apparaissent sous forme de boutons radio dans l'interface graphique ADM.

'paramètres-dépendants'

Cet attribut est un sous-attribut de l'attribut `gui`. Il contrôle dynamiquement l'apparence du paramètre ou sa valeur initiale dans l'écran de configuration StyleBook en fonction de la valeur spécifiée dans un autre paramètre.

Spécifiez cet attribut sur un paramètre source qui contrôle le comportement du paramètre sur le formulaire. Vous pouvez inclure plusieurs conditions qui contrôlent d'autres paramètres. Par exemple, un paramètre source `protocol` peut avoir un paramètre dépendant `certificate`, qui n'apparaît que si la valeur du `protocol` paramètre est `SSL`.

Chaque condition peut avoir les attributs suivants :

- **target-parameter** : spécifiez le paramètre cible auquel cette condition s'applique.
- **matching-values** : spécifiez la liste des valeurs du paramètre source qui déclenche l'action.
- **action** : spécifiez l'une des actions suivantes sur le paramètre ciblé :
  - `read-only` : le paramètre est en lecture seule.
  - `show` : le paramètre apparaît dans le formulaire s'il est masqué.
  - `hide` : le paramètre est supprimé du formulaire.
  - `set-value` : la valeur du paramètre est définie sur la valeur spécifiée dans l'attribut value.
- **value** : valeur du paramètre cible si l'action est `set-value`.

Lorsqu'une entrée utilisateur correspond aux valeurs spécifiées sur le paramètre source, l'apparence ou la valeur du paramètre cible change en fonction de l'action spécifiée.

Exemple :

```
-
    name: lb-virtual-port
```



```
    label: "Load Balanced App Virtual Port"
    description: "TCP port representing the Load Balanced application"
    type: tcp-port
    gui:
      updatable: false
      dependent-parameters:
            -
              matching-values:
                - 80
              target-parameter: $parameters.lb-service-type
              action: set-value
              allowed-values:
              - HTTP
              - TCP
              - UDP

    default: 80

<!--NeedCopy-->
```

Dans cet exemple, le paramètre dépendant est spécifié sous le paramètre `lb-virtual-port` (paramètre source).

Lorsque la valeur du paramètre source est définie sur `80`, le paramètre `lb-service-type` déclenche l'action `set-value`. Par conséquent, un utilisateur est autorisé à sélectionner l'une des options suivantes :

- HTTP
- TCP
- UDP

Parameters-default-sources construct

February 1, 2024

Vous pouvez utiliser cette construction pour réutiliser les définitions de paramètres d'autres StyleBooks.

Imaginons un scénario dans lequel un paramètre ou un groupe de paramètres est utilisé à plusieurs reprises dans plusieurs StyleBooks. **Pour éviter de redéfinir ces paramètres, chaque fois que vous souhaitez créer un nouveau StyleBook, vous pouvez les définir une fois, puis importer leurs définitions dans les StyleBooks qui ont besoin de ces paramètres à l'aide de la construction parameters-default-sources.**

Par exemple, si plusieurs de vos StyleBooks doivent configurer une adresse IP virtuelle, vous devrez peut-être définir les mêmes paramètres liés aux adresses IP virtuelles dans chaque nouveau Style-

Book que vous créez. Au lieu de cela, vous pouvez créer un StyleBook distinct appelé, par exemple, « vip-params » dans lequel vous définissez tous les paramètres associés, comme indiqué dans l'exemple suivant :

```
1       -
2       name: vip-params
3       namespace: com.acme.commontypes
4       version: "1.0"
5       description: This StyleBook defines a typical virtual IP config.
6       private: true
7       schema-version: "1.0"
8       parameters:
9         -
10            name: lb-appname
11            label: Load Balanced Application Name
12           description: Name of the Load Balanced application
13            type: string
14            required: true
15        -
16            name: lb-virtual-ip
17            label: Load Balanced App Virtual IP address
18            description: Virtual IP address representing the Load
      Balanced application
19            type: ipaddress
20            required: true
21        -
22            name: lb-virtual-port
23            label: Load Balanced App Virtual Port
24            description: TCP port representing the Load Balanced
      application
25            type: tcp-port
26            default: 80
27        -
28            name: lb-service-type
29            label: Load Balanced App Protocol
30            description: Protocol used for the Load Balanced application
      .
31            type: string
32            default: HTTP
33            required: true
34            allowed-values:
35                 - HTTP
36                 - SSL
37                 - TCP
38  <!--NeedCopy-->
```

Ensuite, vous pouvez créer d'autres StyleBooks utilisant ces paramètres. Voici un exemple d'un tel StyleBook.

```
1       -
2       name: acme-biz-app
3       namespace: com.acme.stylebooks
```



```
4       version: "1.0"
5       description: This stylebook defines the Citrix ADC configuration
      for Biz App
6       schema-version: "1.0"
7       import-stylebooks:
8         -
9             namespace: com.acme.commontypes
10            prefix: cmtypes
11            version: "1.0"
12      parameters-default-sources:
13            - cmtypes::vip-params
14      parameters:
15          -
16            name: monitorname
17            label: Monitor Name
18            description: Name of the monitor
19            type: string
20            required: true
21          -
22            name: type
23            label: Monitor Type
24            description: Type of the monitor
25            type: string
26            required: true
27            allowed-values:
28              - PING
29              - TCP
30              - HTTP
31              - HTTP-ECV
32              - TCP-ECV
33              - HTTP-INLINE
34  <!--NeedCopy-->
```

Dans StyleBook, acme-biz-app, tout d'abord, l'espace de noms et la version du styleBook vip-params sont importés à l'aide de la section « import-stylebooks ». Ensuite, la construction **parameters-default-sources** est ajoutée et le nom StyleBook, c'est-à-dire vip-params, est spécifié. Cela a le même effet que de définir les paramètres du styleBook vip-params directement dans ce StyleBook.

Vous pouvez inclure des paramètres de plusieurs StyleBooks, car les parameters-default-sources sont une liste et chaque élément de la liste doit être un StyleBook.

En plus d'inclure des paramètres provenant d'autres StyleBooks, vous pouvez également définir vos propres paramètres en utilisant la section des paramètres. La liste complète des paramètres du StyleBook est la combinaison de paramètres inclus dans d'autres StyleBooks et de paramètres définis dans ce StyleBook. Par conséquent, l'expression **$parameters** fait référence à cette combinaison de paramètres.

Notez que si un paramètre est défini à la fois dans un StyleBook importé et dans le StyleBook actuel, la définition du StyleBook actuel remplace la définition importée depuis un autre StyleBook. Vous pouvez l'utiliser efficacement en personnalisant certains paramètres importés si nécessaire, tout en

utilisant les autres paramètres importés tels quels.

La construction parameters-default-sources peut également être utilisée dans les paramètres imbriqués comme indiqué :

```
parameters:
    -
      name: vip-details
      label: Virtual IP details
      description: Details of the Virtual IP
      type: object
      required: true
      parameters-default-sources:
              - cmtypes::vip-params
<!--NeedCopy-->
```

Cela revient à ajouter les paramètres des paramètres vip-params de StyleBook directement en tant que paramètres enfants du paramètre vip-details dans ce StyleBook.

Substitutions

February 1, 2024

La section substitutions est utilisée pour définir des noms abrégés pour des expressions complexes qui peuvent être utilisés dans le reste du StyleBook afin de faciliter la lecture du StyleBook. Ils sont également utiles lorsque la même expression ou valeur est répétée plusieurs fois dans le StyleBook, par exemple une valeur constante. L'utilisation d'un nom de substitution pour cette valeur vous permet de mettre à jour uniquement la valeur de substitution lorsque cette valeur doit être modifiée plutôt que de la mettre à jour à chaque emplacement où elle apparaît dans le StyleBook, ce qui pourrait être sujet à des erreurs.

Les substitutions sont également utilisées pour définir des correspondances entre les valeurs, comme décrit dans des exemples plus loin dans ce document.

Chaque substitution dans la liste est composée d'une clé et d'une valeur.La valeur peut être une valeur simple, une expression, une fonction ou une carte.

Dans l'exemple suivant, deux substitutions sont définies. Le premier est « http-port » qui peut être utilisé comme abrégé pour 8181. En utilisant une substitution, vous pouvez désigner cela dans le reste du StyleBook comme **$substitutions.http-port** au lieu de 8181.

substitutions :

http-port : 8181

Cela vous permet de spécifier un nom mnémonique à un numéro de port et de définir ce numéro de port en un seul endroit dans le StyleBook, quel que soit le nombre de fois qu'il est utilisé. Si vous

voulez modifier le numéro de port en 8080, vous pouvez le modifier dans la section de substitution, et la modification prendra effet partout où le nom mnémonique http-port est utilisé. L'exemple suivant montre comment une substitution est utilisée dans un composant.

```
components:
 -
     name: my-lbvserver-comp
     type: ns::lbvserver
     properties:
          name: $parameters.name + "-lb"
          servicetype: HTTP
          ipv46: $parameters.ip
          port: \*\*$substitutions.http-port\*\*
          lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

Une substitution peut également être une expression complexe. L'exemple suivant montre comment deux substitutions utilisent des expressions.

```
substitutions:
  app-rule: HTTP.REQ.HEADER("X-Test-Application").EXISTS
  app-name: str("acme-") + $parameters.name + str("-app")
<!--NeedCopy-->
```

Une expression de substitution peut également utiliser des expressions de substitution existantes, comme indiqué dans l'exemple suivant.

```
substitutions:
  http-port: 8181
  app-name: str("acme-") + $parameters.name + str($substitutions.http-
    port) + str("-app")
<!--NeedCopy-->
```

Les cartes sont une autre fonctionnalité utile des substitutions, dans lesquelles vous pouvez associer des clés à des valeurs. Voici un exemple de substitution de carte.

```
substitutions:
    secure-port:
        true: int("443")
        false: int("80")
    secure-protocol:
        true: SSL
        false: HTTP
<!--NeedCopy-->
```

L'exemple suivant montre comment utiliser les cartes secure-port et secure-protocol.

```
components:
 -
     name: my-lbvserver-comp
     type: ns::lbvserver
     properties:
```



```
6            name: $parameters.name + "-lb"
7            servicetype: $substitutions.secure-protocol[$parameters.is-
     secure]
8            ipv46: $parameters.ip
9            port: $substitutions.secure-port[$parameters.is-secure]
10           lbmethod: $parameters.lb-alg
11 <!--NeedCopy-->
```

Cela implique que si l'utilisateur de StyleBook spécifie la valeur booléenne « true » au paramètre is-secure, ou coche la case correspondant à ce paramètre dans l'interface graphique Citrix ADM, la propriété servicetype de ce composant est affectée à la valeur **SSL** et la propriété port est a attribué la valeur **443**. Toutefois, si l'utilisateur spécifie « false » pour ce paramètre ou désactivez la case à cocher correspondante dans l'interface graphique de Citrix ADM, la propriété servicetype reçoit la valeur **HTTP** et le port reçoit la valeur **80** .

L'exemple suivant montre comment utiliser les substitutions en tant que fonction. Une fonction de substitution peut prendre un ou plusieurs arguments.Les arguments doivent être de type simple par exemple, string, number, ipaddress, booléen et autres types.

substitutions :

form-lb-name(name): $name + "-lb"

Dans cet exemple, nous définissons une fonction de substitution « form-lb-name » qui prend un argument de chaîne appelé « name » ** et l'utilise pour créer une nouvelle chaîne qui suffixe « -lb » à la chaîne dans l'argument name. Une expression utilisant cette fonction de substitution peut être écrite comme suit :

$substitutions.form-lb-name("my")

qui renvoie « my-lb »

Prenons un autre exemple :

substitutions :

cspol-priority(priority): 10100 - 100 * $priority

La substitution cspol-priority est une fonction qui prend un argument appelé priority et l'utilise pour calculer une valeur. Dans le reste du StyleBook, cette substitution peut être utilisée comme illustré dans l'exemple suivant :

```
1 components:
2   -
3     name: cspolicy-binding-comp
4     type: ns::csvserver_cspolicy_binding
5     condition: not $parameters.is-default
6     properties:
7          name: $parameters.csvserver-name
8          policyname: $components.cspolicy-comp.properties.policyname
```



```
          priority: $substitutions.cspol-priority($parameters.pool.
    priority)
<!--NeedCopy-->
```

La substitution peut également être composée d'une clé et d'une valeur. La valeur peut être une valeur simple, une expression, une fonction, une carte, une liste ou un dictionnaire.

Voici un exemple de substitution appelée 'slist'dont la valeur est une liste :

```
substitutions:
  slist:
    - a
    - b
    - c
<!--NeedCopy-->
```

La valeur d'une substitution peut également être un dictionnaire de paires clé-valeur comme on le voit dans l'exemple suivant d'une substitution appelée 'sdict'ci-dessous :

```
substitutions:
  sdict:
    a: 1
    b: 2
    c: 3
<!--NeedCopy-->
```

Vous pouvez créer des attributs plus complexes en combinant les listes et les dictionnaires. Par exemple, une substitution appelée « slistofdict » renvoie une liste de paires clé-valeur.

```
  slistofdict:
    -
      a: $parameters.cs1.lb1.port
      b: $parameters.cs1.lb2.port
    -
      a: $parameters.cs2.lb1.port
      b: $parameters.cs2.lb2.port
<!--NeedCopy-->
```

Mais, dans l'exemple suivant, une substitution « sdictoflist » renvoie une paire clé-valeur, où la valeur elle-même est une autre liste.

```
  sdictoflist:
    a:
      - 1
      - 2
    b:
      - 3
      - 4
<!--NeedCopy-->
```

Dans les composants, ces substitutions peuvent être utilisées dans les constructions de condition, de propriétés, de répétition, de condition.

L'exemple suivant d'un composant montre comment une substitution peut être utilisée lors de la spécification des propriétés :

```
    properties:
      a: $substitutions.slist
      b: $substitutions.sdict
      c: $substitutions.slistofdict
      d: $substitutions.sdictoflist
<!--NeedCopy-->
```

Un cas d'utilisation pour définir une substitution dont la valeur est une liste ou un dictionnaire est lorsque vous configurez un serveur virtuel de commutation de contenu et plusieurs serveurs virtuels d'équilibrage de charge. Puisque tous les serveurs virtuels lb liés au même serveur virtuel cs peuvent avoir une configuration identique, vous pouvez utiliser la liste de substitution et le dictionnaire pour créer cette configuration afin d'éviter de répéter cette configuration pour chaque serveur virtuel lb.

L'exemple suivant montre la substitution et le composant dans les cs-lb-mon StyleBooks pour créer une configuration de serveur virtuel de commutation de contenu. Lors de la construction des propriétés de cs-lb-mon StyleBooks, la substitution complexe « lb-properties » spécifie les propriétés des serveurs virtuels lb associés au serveur virtuel cs. La substitution « lb-properties » est une fonction qui prend le nom, le type de service, l'adresse IP virtuelle, le port et les serveurs comme paramètres et génère une paire clé-valeur comme valeur. Dans le composant « cs-pools », nous assignons la valeur de cette substitution au paramètre lb-pool pour chaque pool.

```
substitutions:
  cs-port[]:
    true: int("80")
    false: int("443")
  lb-properties(name, servicetype, vip, port, servers):
    lb-appname: $name
    lb-service-type: $servicetype
    lb-virtual-ip: $vip
    lb-virtual-port: $port
    svc-servers: $servers
    svc-service-type: $servicetype
    monitors:
      -
        monitorname: $name
        type: PING
        interval: $parameters.monitor-interval
        interval_units: SEC
        retries: 3
components:
  -
    name: cs-pools
    type: stlb::cs-lb-mon
    description: | Updates the cs-lb-mon configuration with the
    different pools provided. Each pool with rule result in a dummy LB
    vserver, cs action, cs policy, and csvserver_cspolicy_binding
    configuration.
```



```
24      condition: $parameters.server-pools
25      repeat: $parameters.server-pools
26      repeat-item: pool
27      repeat-condition: $pool.rule
28      repeat-index: ndx
29      properties:
30        appname: $parameters.appname + "-cs"
31        cs-virtual-ip: $parameters.vip
32        cs-virtual-port: $substitutions.cs-port($parameters.protocol == "
       HTTP")
33        cs-service-type: $parameters.protocol
34        pools:
35          -
36            lb-pool: $substitutions.lb-properties($pool.pool-name, "HTTP"
       , "0.0.0.0", 0, $pool.servers)
37            rule: $pool.rule
38            priority: $ndx + 1
39  <!--NeedCopy-->
```

Carte de substitution :

Vous pouvez créer des substitutions qui associent des clés à des valeurs. Par exemple, imaginez un scénario dans lequel vous souhaitez définir le port par défaut (valeur) à utiliser pour chaque protocole (clé). Pour cette tâche, écrivez une carte de substitution comme suit.

```
1  substitutions:
2       port:
3            HTTP: 80
4            DNS: 53
5            SSL: 443
6  <!--NeedCopy-->
```

Dans cet exemple, HTTP est mappé à 80, DNS est mappé à 53 et SSL est mappé à 443. Pour récupérer le port d'un certain protocole donné en tant que paramètre, utilisez l'expression

$substitutions.port[$parameters.protocol]

L'expression renvoie une valeur basée sur le protocole spécifié par l'utilisateur.

- Si la clé est HTTP, l'expression renvoie 80
- Si la clé est DNS, l'expression renvoie 53
- Si la clé est SSL, l'expression renvoie 443
- Si la clé n'est pas présente dans la carte, l'expression ne renvoie aucune valeur

Composants

February 1, 2024

La construction Components d'un StyleBook est considérée comme la section la plus importante du StyleBook. Dans cette section, vous définissez les objets de configuration qui doivent être créés. À l'aide de cette construction, vous pouvez créer un ou plusieurs objets de configuration du même type.

La construction des composants peut utiliser l'entrée fournie dans la section des paramètres pour adapter la configuration générée par le StyleBook. Cette section est facultative, bien que la plupart des StyleBooks aient une section sur les composants.

Le tableau suivant décrit les principaux attributs d'un composant.

|Attribut| Description|
—	—
nom	Le nom du composant. Vous pouvez spécifier un nom alphanumérique. Le nom doit commencer par un alphabet et peut inclure des alphabets, des chiffres, un tiret (-) ou un trait de soulignement (_) supplémentaires.
description	Description du rôle de ce composant dans le StyleBook.
type	Le type détermine les propriétés que ce composant fournit. Les composants ont deux types de types : **Type intégré** : Ce type est fourni par le système et vous n'avez pas à le définir, par exemple, les types d'entités NITRO « lbvserver » ou « servicegroup ». Lorsqu'un composant dispose d'un attribut type intégré, il crée un objet de configuration de ce type sur l'Citrix ADC. Par exemple, si un composant fait référence au type intégré « lbvserver », ce composant crée un serveur virtuel d'équilibrage de charge sur l'instance de Citrix ADC qui est la cible de la configuration. **Type composite** : ce type fait référence à un StyleBook existant que vous avez créé et importé dans Citrix ADM. Lorsqu'un composant possède un attribut de type composite, il crée tous les objets de configuration, qui sont spécifiés dans le StyleBook référencé, sur l'instance Citrix ADC qui est la cible de la configuration. Cela vous permet de combiner plusieurs StyleBooks où chaque StyleBook crée une partie de la configuration finale. Pour plus d'informations sur les StyleBooks composites, voir [Créer un StyleBook composite](/fr-fr/netscaler-application-delivery-management-software/13/stylebooks/how-to-create-custom-stylebooks).
propriétés	Les sous-attributs qui peuvent être utilisés pour un attribut de type de composant. Les propriétés valides pour un composant sont dictées par son type. Pour un type intégré, il s'agit des propriétés ou des attributs de l'objet Nitro correspondant. Pour un composant dont le type est un autre StyleBook, c'est-à-dire un type composite, les propriétés correspondent aux paramètres définis dans ce StyleBook.

Exemple :

```
components:
   -
     name: my-lbvserver-comp
     type: ns::lbvserver
     properties:
```



```
6           name: $parameters.name
7           servicetype: HTTP
8           ipv46: $parameters.ip
9           port: 80
10          lbmethod: $parameters.lb-alg
11  <!--NeedCopy-->
```

Dans cet exemple, vous avez défini un composant appelé my-lbvserver-comp. Ce composant est du type ns : :lbvserver (un type intégré), où « ns » est le préfixe qui fait référence à l'espace de noms netscaler.nitro.config et à la version 10.5 que vous avez spécifié dans la section import-stylebooks, et « lbvserver » est une ressource NITRO dans cet espace de noms.

Les propriétés de cette section incluent quatre attributs obligatoires et un attribut facultatif (lb-method) de la ressource « lbvserver » et vous permettent de spécifier des valeurs pour ces attributs. Dans cet exemple, vous spécifiez des valeurs statiques pour le type de service et le port alors que les propriétés name, ipv46 et lbmethod obtiennent leurs valeurs à partir des paramètres d'entrée. Vous vous référez aux noms de paramètres définis dans la section des paramètres en utilisant $parameters.<name> notation, par exemple, $parameters.ip.

> **Remarque**
>
> Vous devez utiliser des minuscules pour les noms d'attributs des types de ressources NITRO (les propriétés de ses composants). Sinon, l'importation d'un StyleBook échouera.

Composants d'assistance

February 1, 2024

L'utilisation principale de la section des composants dans un StyleBook est de générer des objets de configuration via des types intégrés de Nitro ou un autre StyleBook qui crée les objets de configuration réels. Les composants d'assistance ne construisent pas d'objets de configuration par eux-mêmes. Les composants auxiliaires prennent les entrées d'autres sections, telles que les objets de paramètres, les propriétés d'autres composants ou les sorties d'autres composants, et les transforment en d'autres formes. Cela peut être utilisé ultérieurement par d'autres composants pour générer les objets de configuration réels. Un composant d'assistance peut être de deux types : un type d'objet ou un autre StyleBook qui ne contient pas de section de composant.

L'exemple suivant illustre un extrait d'un StyleBook utilisé pour créer un serveur d'équilibrage de charge avec moniteur (lb-mon-comp) sur une instance de Citrix ADC.

```
1  parameters:
2    -
3      name: appname
```



```
    type: string
  -
    name: ips
    type: ipaddress[]
  -
    name: vip
    type: ipaddress

components:
  -
    name: help-comp
    type: cmtypes::server-ip-port-params
    repeat:
      repeat-list: $parameters.ips
      repeat-item: server-ip
    properties:
      ip: $server-ip
      port: 80
 -
    name: lb-mon-comp
    type: stlb::lb-mon
    properties:
      lb-appname: $parameters.appname
      lb-virtual-ip: $parameters.vip
      lb-virtual-port: 80
      lb-service-type: HTTP
      svc-service-type: HTTP
      svc-servers: $components.help-comp.properties
<!--NeedCopy-->
```

La section Paramètres vous permet d'entrer le nom de l'application et les adresses IP des serveurs d'équilibrage de charge. Dans la section du composant lb-mon-comp, le paramètre svc-servers de lb-mon StyleBook attend une liste d'objets où chaque élément possède deux sous-paramètres : ip et port.

Cependant, la section paramètres de ce StyleBook accepte uniquement les adresses IP du serveur via $parameters.ips. Le StyleBook suppose que tous les serveurs s'exécutent sur le port 80. Pour créer la configuration d'équilibrage de charge à l'aide de lb-mon StyleBook, vous devez transformer le fichier $parameters.ips en une liste d'objets. Ceci est réalisé à l'aide du composant d'assistance, help-comp dans l'exemple ci-dessus. Le composant help-comp est du type server-ip-port-params StyleBook. Ce StyleBook ne comporte aucun composant. Par conséquent, il ne crée aucun objet de configuration. Le help-comp crée une liste répétée sur $parameters.ips et construit un objet composé d'une adresse IP et d'un port (défini sur une valeur statique de 80) pour chaque élément de $parameters.ips. Ainsi, help-comp transforme une liste d'adresses IP en une liste d'objets qui peuvent être utilisés ultérieurement dans lb-mon-comp pour attribuer la propriété svc-servers. Le résultat de la commande help-comp est attribué à la propriété svc-servers de lb-mon-comp.

Propriétés facultatives

February 1, 2024

Dans certains cas, la valeur d'une propriété d'un composant provient d'une expression, qui peut être une expression simple, telle qu'une référence de paramètre, ou une expression plus complexe. La définition de cette valeur de propriété est facultative dans le composant. Vous pouvez choisir de définir la valeur de la propriété uniquement si l'expression renvoie une valeur réelle, sinon vous pouvez choisir de ne pas définir cette propriété.

Par exemple, considérez que l'une des propriétés que vous souhaitez définir est la méthode lbmethod (algorithme d'équilibrage de charge) d'un composant dont le type est ns : :lbvserver. La valeur de la propriété lbmethod est extraite d'une valeur de paramètre fournie par l'utilisateur, comme indiqué ci-dessous :

```
components
  -
      name: lbvserver_comp
      type: ns::lbvserver
      properties:
        name: $parameters.lb-appname + "-lb"
        servicetype: $parameters.lb-service-type
        ipv46: $parameters.lb-virtual-ip
        port: 80
        lbmethod: $parameters.lb-advanced.algorithm
<!--NeedCopy-->
```

Maintenant, considérez que le paramètre **lb-advanced.algorithm** est un paramètre facultatif. Et, si l'utilisateur ne fournit pas de valeur pour ce paramètre parce qu'il est facultatif, l'expression **$parameters.lb-advanced.algorithm** est évaluée à valeur vide. Par conséquent, une valeur non valide est transmise pour la propriété lbmethod. Afin d'éviter une telle situation, vous pouvez annoter la propriété comme facultative en suffixant son nom avec « ? » comme suit :

```
components
   -
     name: lbvserver_comp
     type: ns::lbvserver
     properties:
       name: $parameters.lb-appname + "-lb"
       servicetype: $parameters.lb-service-type
       ipv46: $parameters.lb-virtual-ip
       port: 80
       lbmethod?: $parameters.lb-advanced.algorithm
<!--NeedCopy-->
```

L'utilisation de « ? » omet la propriété si l'expression sur le droit n'évalue rien, ce qui équivaudrait, dans ce cas, à un composant défini comme suit :


```
components
  -
    name: lbvserver_comp
    type: ns::lbvserver
    properties:
      name: $parameters.lb-appname + "-lb"
      servicetype: $parameters.lb-service-type
      ipv46: $parameters.lb-virtual-ip
      port: 80
<!--NeedCopy-->
```

Comme **lbmethod** est facultatif, son omission en fait un composant valide. Notez que lbmethod peut prendre sa valeur par défaut si elle est définie dans son type « ns : :lbvserver ».

Properties-Default-Sources, construction

February 1, 2024

La construction properties-default-sources est analogue à la construction parameters-default-sources. Alors que la construction parameters-default-sources permet la réutilisation de paramètres existants (provenant d'autres StyleBooks) dans un StyleBook, la construction properties-default-sources permet à l'utilisateur de spécifier les propriétés d'un composant en fonction de sources existantes.

Les propriétés d'un composant peuvent être réparties dans différentes sections du StyleBook. Par exemple, les propriétés peuvent provenir de paramètres d'objets, de substitutions renvoyant un objet, de propriétés d'autres composants ou de sorties d'autres composants. Dans ce cas, vous devez redéfinir les propriétés qui apparaissent dans d'autres sections du StyleBook dans la définition du composant. Il est clair que cela est redondant et peut entraîner des erreurs. Pour résoudre ce problème, la construction properties-default-sources peut être utilisée. La construction properties-default-sources est une liste dans laquelle chaque élément identifie une source pour certaines propriétés du composant.

Par exemple, considérez un composant qui crée une configuration lbvserver. Ce composant doit définir les propriétés du serveur lbvserver comme suit.

```
parameters:
  -
    name: lb
    type: ns::lbvserver
components:
  -
    name: lb-comp
    type: ns::lbvserver
    properties:
```



```
      name: $parameters.lb.name
      ipv46: $parameters.lb.ipv46
      port: $parameters.lb.port
      servicetype: $parameters.lb.servicetype
      lbmethod: $parameters.lb.lbmethod
<!--NeedCopy-->
```

Dans l'exemple ci-dessus, observez que les valeurs de toutes les propriétés définies dans la section composants sont extraites de l'objet $parameters.lb. Bien qu'elles soient extraites d'une seule source, les propriétés sont à nouveau définies dans le StyleBook. En outre, si un nouveau sous-paramètre de l'objet $parameters.lb pertinent pour la configuration du lbvserver est ajouté, vous devez mettre à jour le composant lb-comp pour ajouter la nouvelle propriété correspondant au nouveau sous-paramètre.

Pour éviter de redéfinir les propriétés et récupérer toutes les propriétés pertinentes d'un composant sans les énumérer explicitement dans la section propriétés, la construction properties-default-sources peut être utilisée. L'exemple ci-dessus peut être écrit comme suit.

```
parameters:
  -
    name: lb
    type: ns::lbvserver
components:
  -
    name: lb-comp
    type: ns::lbvserver
    properties-default-sources:
      - $parameters.lb
<!--NeedCopy-->
```

Dans l'exemple ci-dessus, l'utilisation de la construction properties-default-sources entraîne une réduction de la taille de la définition du composant, ce qui vous permet de définir un composant de manière concise. De plus, chaque fois que la source des propriétés du composant change, les modifications sont reflétées automatiquement. Par exemple, lorsqu'une nouvelle propriété, par exemple « persistencetype », est ajoutée à l'objet $parameters.lb, cette propriété est ajoutée à la configuration de lb-comp par défaut puisque persistencetype est une propriété de lbvserver. Ainsi, la construction properties-default-sources fournit une interface dynamique pour définir les composants sans se soucier des changements qui se produisent dans les sources des propriétés du composant.

Calcul des propriétés du composant

Cette section explique comment les propriétés sont récupérées si la construction properties-default-sources est utilisée dans un composant. Tout d'abord, le compilateur StyleBooks identifie la liste des propriétés d'un composant en fonction de son type (dans l'exemple ci-dessus, lbvserver). Ensuite, le compilateur récupère ces propriétés à partir des multiples sources dans l'ordre dans lequel elles

sont définies (dans la section properties-default-sources du composant). Si une propriété existe dans plusieurs sources, la propriété apparaissant dans la dernière source a priorité sur les autres. Enfin, une propriété récupérée à l'aide de la construction properties-default-sources peut être remplacée dans la section propriétés du composant. Il est important de noter que la définition d'une section de composant doit au moins comporter une section properties-default-sources ou une section de propriétés. Il peut avoir les deux.

Composants imbriqués

February 1, 2024

L'imbrication d'un composant dans un autre composant permet au composant imbriqué de créer ses objets de configuration en se référant aux objets de configuration ou au contexte créé par le composant parent. Le composant imbriqué peut créer un ou plusieurs objets pour chaque objet créé dans le composant parent. L'imbrication d'un composant dans un autre composant n'indique aucune relation entre les objets de configuration créés. L'imbrication permet aux composants de créer plus facilement des objets de configuration dans un contexte existant des composants parents.

Exemple :

```
components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
   properties:
      name: $parameters.name + "-lb"
      servicetype: HTTP
      ipv46: $parameters.ip
      port: 80
      lbmethod: $parameters.lb-alg
      components:
        -
         name: my-svcg-comp
         type: ns::servicegroup
         properties:
            name: $parameters.name + "-svcgrp"
            servicetype: HTTP
         components:
            -
              name: lbvserver-svg-binding-comp
              type: ns::lbvserver_servicegroup_binding
              properties:
                name: $parent.parent.properties.name
                servicegroupname: $parent.properties.name
                  -
                    name: members-svcg-comp
```



```
                    type: ns::servicegroup_servicegroupmember_binding
                    repeat:
                      repeat-list: $parameters.svc-servers
                      repeat-item: srv
                    properties:
                      ip: $srv
                      port: str($parameters.svc-port)
                      servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

Dans cet exemple, l'imbrication à plusieurs niveaux est utilisée. Le composant my-lbvserver-comp possède un composant enfant appelé my-svcg-comp. Et, le composant my-svcg-comp a deux composants enfants à l'intérieur. Le composant my-svcg-comp est utilisé pour créer un objet de configuration de groupe de services sur l'instance de Citrix ADC en fournissant des valeurs aux attributs du type de ressource NITRO intégré « servicegroup. » Le premier composant enfant du composant my-svcg, lbvserver-svg-binding-comp, est utilisé pour lier le groupe de services créé par son composant parent au serveur virtuel d'équilibrage de charge (lbvserver) créé par le composant parent du composant parent. La notation $parent, également appelée référence parente, est utilisée pour faire référence aux entités dans les composants parents. Le deuxième composant enfant, members-svcg-comp, est utilisé pour lier la liste des services au groupe de services créé par le composant parent. La liaison est obtenue en utilisant la construction de répétition de StyleBook pour parcourir la liste des services spécifiés pour le paramètre svc-servers. Pour plus d'informations sur les constructions de répétition, voir Répétition de construction.

Vous pouvez également créer les mêmes objets de configuration sans utiliser l'imbrication de composants. Pour plus d'informations et d'exemples, consultez StyleBook pour créer une configuration d'équilibrage de charge de base.

Conditionner la construction

February 1, 2024

Vous pouvez rendre un composant conditionnel à l'aide d'une structure de condition. La valeur d'une construction conditionnelle est une expression booléenne dont la valeur est vraie ou fausse. Si la condition est vraie, le composant est utilisé pour créer ses objets de configuration. Si la condition est fausse, le composant est ignoré et aucun objet de configuration n'est créé par son intermédiaire. L'expression booléenne est souvent basée sur des valeurs de paramètres.

Exemple :

```
components:
      -
        name: servicegroup-comp
```



```
        type: ns::servicegroup
        condition: $parameters.svc-server-ips
        properties:
              name: $parameters.name + "-svcgrp"
              servicetype: HTTP
<!--NeedCopy-->
```

Dans cet exemple, si l'utilisateur spécifie une valeur pour le paramètre facultatif svc-server-ips, le composant, servicegroup-comp, est traité par le moteur StyleBook. Si la condition est fausse, c'est-à-dire si l'utilisateur ne fournit pas de valeur à ce paramètre, une valeur nulle est affectée à ce paramètre et est évaluée à false, le moteur StyleBook ignore la présence de ce composant et aucun groupe de services n'est créé.

Notez que l'expression booléenne peut être basée sur n'importe quelle expression valide prise en charge dans StyleBooks (par exemple, si un autre composant est présent ou si un paramètre a une certaine valeur).

L'exemple suivant génère l'objet de configuration de type NITRO ns::systemfile si la condition est évaluée comme vraie.

Exemple :

```
    components
         -
           name: pem_key_files
           type: ns::systemfile
           condition: "$components.der-certificate-files-comp or
    $components.pem-certificate-files-comp"
           properties:
                 filecontent: $certificate.keyfile.contents
                 fileencoding: "BASE64"
                 filelocation: "/nsconfig/ssl"
                 filename: $certificate.keyfile.filename
<!--NeedCopy-->
```

Dans cet exemple, la condition est une expression « OR » complexe, dans laquelle vous souhaitez que cet objet de configuration soit créé par le StyleBook uniquement si deux autres composants du StyleBook ont été traités (non ignorés), créant ainsi une dépendance entre les composants.

Construction repeat

February 1, 2024

Vous pouvez utiliser la construction **répétée** d'un composant pour créer plusieurs objets de configuration du même type.

Dans l'exemple suivant, le composant **members-svcg-comp** est utilisé pour lier la liste des services au groupe de services créé par le composant parent. Pour créer un objet de configuration qui lie chaque serveur au groupe de services, utilisez la construction de **répétition** pour parcourir la liste des services spécifiés pour le paramètre **svc-servers**. Au cours de l'itération, le composant crée un objet NITRO de type **servicegroup_servicegroupmember_binding** pour chaque service (appelé **srv** dans la construction **répét-item**) dans le groupe de services, et il définit l'attribut **ip** de chaque objet NITRO sur l'adresse IP du service correspondant.

Exemple :

```
components:
  -
      name: my-lbvserver-comp
      type: ns::lbvserver
      properties:
           name: $parameters.name + "-lb"
           servicetype: HTTP
           ipv46: $parameters.ip
           port: 80
           lbmethod: $parameters.lb-alg
          components:
                -
                   name: my-svcg-comp
                   type: ns::servicegroup
                   properties:
                        name: $parameters.name + "-svcgrp"
                        servicetype: HTTP
                  components:
                         -
                         name: lbvserver-svg-binding-comp
                         type: ns::lbvserver\servicegroup\binding
                         properties:
                               name: $parent.parent.properties.name
                               servicegroupname: $parent.properties.
    name
                         -
                         name: members-svcg-comp
                         type: ns::servicegroup\servicegroupmember\
    binding
                         repeat:
                           repeat-list: $parameters.svc-servers
                           repeat-item: srv
                         properties:
                                ip: $srv
                                port: $parameters.svc-port
                                servicegroupname: $parent.properties.
    name
<!--NeedCopy-->
```

La **répétition** est un objet en soi, et **repeat-list et**repeat-item** sont des attributs de l'objet répété.

- repeat-list est un attribut obligatoire qui identifie la liste sur laquelle le composant itère.

- repeat-item est facultatif et est utilisé pour donner un nom convivial à l'élément actif dans l'itération.

S'il n'est pas spécifié, l'élément en cours est accessible à l'aide de l'expression**$repeat-item**. Le dernier composant de l'exemple ci-dessus peut également être écrit comme suit :

```
1            -
2            name: members-svcg-comp
3            type: ns::servicegroup_servicegroupmember_binding
4            repeat:
5              repeat-list: $parameters.svc-servers
6            properties:
7                   ip: $repeat-item
8                   port: $parameters.svc-port
9                   servicegroupname: $parent.properties.name
10 <!--NeedCopy-->
```

En plus de pouvoir faire référence à l'élément en cours en itérant sur une liste, il est également possible de faire référence à l'index actuel de l'élément de la liste à l'aide de **repeat-index**. Dans l'exemple suivant, **repeat-index** est utilisé pour calculer un numéro de port basé sur l'index actuel :

```
1              name: services
2              type: ns::service
3              repeat:
4                 repeat-list: $parameters.app-services
5                 repeat-item: srv
6              properties:
7                  ip: $parameters.app-ip
8                  port: $parameters.base-port + repeat-index
9                  servicegroupname: $parent.properties.name
10 <!--NeedCopy-->
```

Comme pour la construction**repeat-item**, vous pouvez attribuer un nom de variable différent pour faire référence à l'index actuel de l'itération. L'exemple précédent est équivalent à l'exemple suivant :

```
1      -
2              name: services
3              type: ns::service
4              repeat:
5                 repeat-list: $parameters.app-services
6                 repeat-item: srv
7                 repeat-index: idx
8              properties:
9                  ip: $parameters.app-ip
10                 port: $parameters.base-port + $idx
11                 servicegroupname: $parent.properties.name
12 <!--NeedCopy-->
```


Construction repeat-condition

February 1, 2024

La construction à conditions répétées est évaluée à chaque itération d'une construction répétée et le résultat détermine s'il faut créer l'objet de configuration au cours de cette itération ou passer à l'itération suivante. L'exemple suivant montre l'utilisation de la construction repeat-condition :

Exemple :

```
components
   -
      name: der-key-files-comp
      type: ns::systemfile
      repeat:
      repeat-list: $parameters.certificates
      repeat-item: certificate
        repeat-condition: $certificate.ssl-inform == DER
        properties:
         filecontent: base64($certificate.keyfile.contents)
         fileencoding: BASE64
         filelocation: /nsconfig/ssl
         filename: $certificate.keyfile.file
<!--NeedCopy-->
```

Dans cet exemple, le composant der-key-files-comp effectue une itération sur tous les certificats fournis par l'utilisateur, mais il crée uniquement des objets de configuration qui correspondent à des certificats avec un codage DER. Dans chaque itération, l'expression de condition de répétition est évaluée pour tester si l'encodage de certificat est de type DER. S'il n'est pas de type DER, aucun objet de configuration n'est créé dans l'itération en cours et l'itération passe au certificat suivant de la liste.

Répétitions imbriquées

February 1, 2024

Avec la construction répétitive imbriquée, vous pouvez avoir plusieurs constructions répétées dans chaque composant en fonction de la définition du composant. Envisagez une répétition imbriquée de deux niveaux. Pour chaque élément de la liste extérieure (première liste de répétitions), vous pouvez créer une liste de répétition pour tous les éléments de la liste intérieure (deuxième liste de répétitions). Le compilateur StyleBook prend en charge jusqu'à trois répétitions imbriquées. Chaque niveau de répétition est associé à des attributs repeat-item et repeat-index. Les attributs repeat-item et repeat-index sont tous deux facultatifs. En outre, chaque répétition peut également spécifier une condition de répétition.

Exemple :

```
parameters:
  -
      name: vips
      type: ipaddress[]
  -
      name: vip-ports
      type: tcp-port[]
components:
  -
      name: lbvservers-comp
      type: ns::lbvserver
      repeat:
         repeat-list: $parameters.vips
         repeat-item: ip
         repeat:
              repeat-list: $parameters.vip-ports
              repeat-item: port
      properties:
         name: str("lb-") + str($ip) + '-' + str($port)
         servicetype: HTTP
         ipv46: $ip
         port: $port
<!--NeedCopy-->
```

Dans l'exemple ci-dessus, pour chaque élément de $parameters.vips, nous procédons à une itération sur tous les éléments de $parameters.vip-ports. Ainsi, pour chaque adresse IP spécifiée dans $parameters.vips, nous créons des objets de configuration lbvserver pour tous les ports spécifiés dans $parameters.vip-ports. La section des propriétés définit le nom de l'objet avec « lb » comme préfixe pour la combinaison de l'adresse IP et du port. Par conséquent, pour chaque itération, $ip + $port définit une combinaison unique d'adresse IP et de numéro de port.

Si l'attribut repeat-item n'est pas fourni, le compilateur génère une valeur par défaut pour celui-ci. Les valeurs par défaut pour repeat-item sont : $repeat-item, $repeat-item-1, $repeat-item-2 respectivement pour chaque niveau de répétition. De même, si l'attribut repeat-index n'est pas fourni, le compilateur génère une valeur par défaut pour celui-ci. Les valeurs par défaut pour repeat-index sont : $repeat-index, $repeat-index-1 et $repeat-index-2 respectivement pour chaque niveau de répétition.

L'exemple suivant décrit la convention de dénomination en l'absence d'attributs repeat-item et repeat-index dans un objet de répétition imbriqué.

Exemple :

```
components:
-
     name: lbvservers-comp
     type: ns::lbvserver
     repeat:
```



```
          repeat-list: $parameters.vips
          repeat:
             repeat-list: $parameters.vip-ports
      properties:
         name: str("lb-") + str($repeat-item) + '-' + str($repeat-item
     -1)
         servicetype: HTTP
         ipv46: $repeat-item
         port: $repeat-item-1
<!--NeedCopy-->
```

Sorties

February 1, 2024

Dans la section des sorties, vous spécifiez ce qu'un StyleBook expose à ses utilisateurs une fois qu'il a créé avec succès tous les objets de configuration. La section des sorties d'un StyleBook est facultative. Un StyleBook n'a pas besoin de renvoyer des sorties. Cependant, en renvoyant certains composants internes sous forme de sortie, cela donne à tous les StyleBooks qui les importent plus de flexibilité, comme vous pouvez le voir lors de la création d'un StyleBook composite.

Le tableau suivant décrit les attributs utilisés dans la section des sorties.

Attribut	Description	Mandatory
nom	Le nom de la sortie correspondant à l'objet de configuration que vous souhaitez exposer.	Oui
description	Chaîne de texte décrivant la sortie.	Non
valeur	Cet attribut indique comment extraire la valeur renvoyée par un StyleBook.	Oui

Exemple :

```
outputs:
 -
   name: lbvserver
   description: LBVServer component
   value: $components.my-lbvserver-comp
 -
```



```
    name: svc-grp
      description: ServiceGroup name
      value: $components.my-svcg.properties.name
<!--NeedCopy-->
```

Dans cet exemple, vous exposez le composant **lbvserver** et le **nom** du groupe de services qui seraient créés par le StyleBook. La valeur de la sortie appelée **lbvserver** est le composant **my-lbvserver-comp**. **De même, la valeur de la sortie appelée**svc-grp**est le nom du groupe de services créé par le composant my-svcg.**

Référence des paramètres

February 1, 2024

Dans la construction des composants, vous vous référez aux paramètres définis dans la section des paramètres à l'aide de la notation `$parameters.<parametername>`. Si `<parametername>` contient lui-même des paramètres (lorsque le type est objet), vous devez utiliser la notation `$parameters.<parametername>.<sub-parametername>`, etc.

Exemple :

```
parameters:
  -
    name: name
    label: Name
    type: string
    required: true
     -
      name: vip
      label: Virtual IP and Port
      type: object
      required: true
      parameters:
        -
          name: ip
          label: Virtual IP
          description: The Virtual IP Address
          type: ipaddress
          required: true
            -
              name: port
              label: The Virtual Port
              description: The TCP port for the Virtual IP
              type: tcp-port
              default: 80
components:
  -
    name: my-lbvserver-comp
```



```
    type: ns::lbvserver
    properties:
       name: $parameters.name
       servicetype: HTTP
       ipv46: $parameters.vip.ip
       port: $parameters.vip.port
<!--NeedCopy-->
```

Référence parent

February 1, 2024

Si vous utilisez des composants imbriqués, vous pouvez faire référence au composant parent en utilisant la notation $parent. Si le composant parent construit plusieurs objets de configuration à l'aide de la construction de répétition, et dans chaque itération, les composants enfants créent d'autres objets de configuration, la notation $parent fait toujours référence à l'itération actuelle du composant parent. Par exemple, $parent.properties.name fait référence à la propriété name de l'objet de configuration créé dans l'itération en cours par le parent.

Exemple :

```
components:
 -
   name: my-lbvserver-comp
   type: ns::lbvserver
   properties:
     name: $parameters.name + "-lb"
     servicetype: HTTP
     ipv46: $parameters.ip
     port: 80
     lbmethod: $parameters.lb-alg
     components:
       -
         name: my-svcg-comp
         type: ns::servicegroup
         properties:
           name: $parameters.name + "-svcgrp"
           servicetype: HTTP
           components:
            -
              name: lbvserver-svg-binding-comp
              type: ns::lbvserver_servicegroup_binding
              properties:
                 name: $parent.parent.properties.name
                 servicegroupname: $parent.properties.name
                   -
                     name: members-svcg-comp
                     type: ns::servicegroup_servicegroupmember_binding
```



```
                      repeat: $parameters.svc-servers
                      repeat-item: srv
                      properties:
                        ip: $srv
                        port: str($parameters.svc-port)
                        servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

Vous pouvez également naviguer vers le haut dans la hiérarchie des composants en accédant aux propriétés des parents jusqu'aux composants de niveau supérieur. Par exemple, le nom de la propriété du composant **lbvserver-svg-binding-comp** tire sa valeur du nom de propriété du parent de son composant parent, le composant**my-lbvserver-comp**, à l'aide de la notation **$parent.parent**.

Référence des composants

February 1, 2024

Dans la construction des composants, vous faites référence au composant de niveau supérieur dans le StyleBook en utilisant la notation **$components.<componentname>**. S'il y a des composants imbriqués dans un composant de niveau supérieur, la notation utilisée est **$components.<componentname>.comp name>** pour y faire référence, et ainsi de suite.

Exemple :

```
components:
 -
    name: my-lbvserver-comp
     type: ns::lbvserver
     properties:
           name: $parameters.name + "-lb"
           servicetype: HTTP
           ipv46: $parameters.ip
           port: 80
           lbmethod: $parameters.lb-alg
  -
     name: my-svcg-comp
     type: ns::servicegroup
     properties:
          name: $parameters.name + "-svcgrp"
          servicetype: HTTP
 -
     name: members-svcg-comp
     type: ns::servicegroup_servicegroupmember_binding
     repeat: $parameters.svc-servers
     repeat-item: srv
     properties:
        ip: $srv
          port: str($parameters.svc-port)
```



```
25            servicegroupname: $components.my-svcg-comp.properties.name
26   -
27       name: lbvserver-svg-binding-comp
28       type: ns::lbvserver_servicegroup_binding
29       properties:
30              name: $components.my-lbvserver-comp.properties.name
31              servicegroupname: $components.my-svcg-comp.properties.name
32  <!--NeedCopy-->
```

Dans cet exemple, les composants **my-svcg-comp** et **my-lbvserver-comp** doivent être construits avant de construire le dernier composant **lbvserver-svg-binding-comp** car il y a des références à ces composants dans ce dernier composant. Ces références sont fournies en utilisant les références de composants désignées par **$components.<componentname>**.

Référence des substitutions

February 1, 2024

Dans la section composants ou la section opérations, vous faites référence aux substitutions définies dans la section substitutions à l'aide de la notation **$substitutions.<substitution-name>**. Par exemple, **$substitutions.http-port**.

Si une substitution est une carte, vous pouvez faire référence à un élément de la carte sous la forme **$substitutions.<substitutions-name>[<map-key>]**. Par exemple, **$substitutions.protocol-map[$parameters.port]**.

Référence de variable

February 1, 2024

Lorsque vous utilisez les constructions repeat-item et repeat-item dans des composants pour créer plusieurs objets de configuration, vous pouvez attribuer un nom de variable à la construction repeat-item. Cette variable peut ensuite être référencée dans les propriétés de ce composant ou dans les composants enfants à l'aide de la notation **$\<varname\>**. Notez que lorsque la construction repeat est utilisée sans la construction repeat-item dans un composant, une variable par défaut appelée $repeat-item peut être utilisée pour accéder aux éléments d'itération.

Exemple :

```
1  components:
2    -
3      name: server-members-comp
```



```
    type: ns::server
    condition: $parameters.svc-server-domain-names
    repeat: $parameters.svc-server-domain-names
    repeat-item: server-name
    properties:
      name: $server-name + "-server"
      domain: $server-name
    components:
      -
         name: service-members-comp
         type: ns::service
         properties:
           name: $server-name + "-service"
           servername: $parent.properties.name
           servicetype: $parameters.svc-service-type
           port: $parameters.svc-server-port
<!--NeedCopy-->
```

Dans l'exemple ci-dessus, un nom de variable, nom_serveur, est affecté à la construction d'élément répétitif. Ce nom de variable est mentionné dans les propriétés du même composant ainsi que dans les composants enfants **$\<varname\>**.

Opérations

February 1, 2024

Operations est une section facultative dans un StyleBook. Dans cette section, vous pouvez configurer les analyses Citrix Application Delivery Management (ADM) pour collecter des enregistrements AppFlow sur toutes ou certaines des transactions de trafic. Le serveur virtuel créé sur une instance Citrix ADC à l'aide du StyleBook gère ces transactions de trafic. Dans cette section, vous pouvez également configurer Citrix ADM pour déclencher des alarmes lorsque certaines conditions de trafic sont remplies sur un serveur virtuel.

Vous pouvez configurer Citrix ADM via StyleBooks pour collecter des statistiques de trafic à partir de divers Citrix ADM Insights répertoriés comme suit :

- Web Insight
- Security Insight
- HDX Insight
- Citrix Gateway Insight.

Les serveurs virtuels pris en charge sont l'équilibrage de charge, la commutation de contenu et les serveurs virtuels VPN.

Activez Web Insight et Security Insight ou l'un d'entre eux pour l'analyse sur un serveur virtuel d'

équilibrage de charge ou de commutation de contenu. Toutefois, pour les serveurs virtuels VPN, vous devez activer HDX Insight et Citrix Gateway Insight ou l'un d'entre eux.

Tout Citrix ADM Insight activé sur les instances Citrix ADC via StyleBooks utilise le protocole IPFIX (AppFlow) pour envoyer les données des instances à Citrix ADC.

En outre, lorsque vous activez Web Insight, les mesures côté client sont activées sur l'équilibrage de charge et les serveurs virtuels de commutation de contenu. Lorsque les mesures côté client sont activées, ADM capture les mesures de temps de chargement et de rendu des pages HTML par injection HTML. À l'aide de ces mesures, les administrateurs peuvent identifier les problèmes de latence L7.

Exemple 1 :

L'exemple suivant montre comment écrire la section des opérations dans un StyleBook pour activer HDX Insight et Citrix Gateway Insight sur un serveur virtuel VPN :

```
name: simple-vpn-ops
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
description: Test StyleBook to enable hdxinsight and gatewayinsight on
   a VPN vserver
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    version: "10.5"
    prefix: ns
components:
    -
        name: vpnvserver-comp
        type: ns::vpnvserver
        properties:
            name: str("vpn-") + str($current-target.ip)
            servicetype: SSL
            ipv46: 1.1.21.37
            port: 443
operations:
    analytics:
        -
            name: comp-ops
            properties:
                target: $components.vpnvserver-comp
                filter: "true"
                insights:
                  -
                   type: hdxinsight**
                    -
                      type: gatewayinsight
outputs:
  -
    name: myvpns
    value: $components.vpnvserver-comp
```



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

Exemple 2 :

L'exemple suivant montre comment écrire la section Opérations dans un StyleBook pour activer Web Insight et Security Insight sur un serveur virtuel d'équilibrage de charge :

```
name: simple-lb-ops
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
description: Test StyleBook to enable webinsight and securityinsight on
    LB vserver
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    version: "10.5"
    prefix: ns
components:
    -
        name: lbvserver-comp
        type: ns::lbvserver
        properties:
            name: str("lb-") + str($current-target.ip)
            servicetype: HTTP
            ipv46: 1.1.21.37
            port: 80
operations:
    analytics:
        -
            name: comp-ops
            properties:
                target: $components.lbvserver-comp
                filter: "true"
                 insights:
                 -
                  type: webinsight
                   -
                  type: securityinsight
outputs:
  -
    name: mylbs
    value: $components.lbvserver-comp
<!--NeedCopy-->
```

Analytics

February 1, 2024

La sous-section Analytics de la section Opérations a une structure similaire à celle de la section Composants. Chaque élément de la section d'analyse est utilisé pour configurer la fonctionnalité Citrix ADM Analytics pour un ou plusieurs serveurs virtuels créés par le StyleBook.

Un élément de la section Analytics possède les attributs suivants :

Attribut	Description	Mandatory
nom	Nom de l'élément d'analyse.	Oui
description	Chaîne de texte décrivant ce qu'est cet élément.	Non
condition	Expression booléenne. Lorsque cette condition est évaluée à faux, l'ensemble de l'élément d'analyse est ignoré.	Non
répétition	Répète sur une liste.	Non
condition de répétition	Expression booléenne. Si l'expression donne la valeur false, l'itération en cours est ignorée.	Non
article répété	Nom de l'élément dans l'itération en cours.	Non
indice de répétition	Nom de la valeur d'index de l'itération en cours.	Non
propriétés	La liste des propriétés des analyses.	Oui
target	L'une des propriétés de la liste. L'expression cible est le nom d'un serveur virtuel, configuré sur Citrix ADC, pour lequel les analyses seront collectées.	Oui

Attribut	Description	Mandatory
filtre	L'une des propriétés de la liste. La valeur de cet attribut est une expression de stratégie avancée Citrix ADC qui est utilisée pour filtrer les requêtes sur le serveur virtuel pour lesquelles les analyses seront collectées. Par défaut, les données d'analyse sont collectées sur tout le trafic passant par le serveur virtuel.	Non

Exemple :

```
operations:

  analytics:

    -

    name: lbvserver-ops-comp

    properties:

    target: $components-basic-lb-comp.outputs.lbvserver-name

    filter: HTTP.REQ.URL.CONTAINS("catalog")
<!--NeedCopy-->
```

Chaque attribut de la section Analytics est utilisé pour indiquer à la fonctionnalité Citrix ADM Analytics de configurer les instances Citrix ADC pour collecter les enregistrements Appflow sur le serveur virtuel identifié par la propriété cible.

Alarmes

February 1, 2024

La sous-section alarmes de la section des opérations présente une structure similaire et les mêmes attributs que dans la sous-section d'analyse. La seule différence est dans l'attribut properties. Pour obtenir la liste de tous les attributs (autres que l'attribut de propriétés), consultez Analytics.

Les propriétés suivantes sont disponibles dans une sous-section alarmes :

Attribut	Description	Mandatory
target	Expression qui évalue le nom d'un serveur virtuel, configuré sur Citrix ADC, pour lequel les alarmes sont configurées.	Oui
profil de courrier électronique	Nom d'un profil de messagerie défini dans la fonctionnalité Citrix ADM Analytics et contenant une liste d'adresses e-mail que vous souhaitez notifier lorsque l'alarme est déclenchée.	Non (un profil e-mail ou un profil sms doit être défini)
profil sms-	Nom d'un profil SMS défini dans la fonctionnalité Citrix ADM Analytics et contenant une liste de numéros de téléphone que vous souhaitez notifier lorsque l'alarme est déclenchée.	Non (un profil e-mail ou un profil sms doit être défini)
rules	Liste de règles définissant les conditions qui déclencheraient une alarme pour le serveur virtuel défini par la propriété cible.	Oui
métrique	Un attribut de règle. Le nom d'une métrique que vous souhaitez suivre concernant le serveur virtuel Citrix ADC.	Oui
opérateur	Un attribut de règle. Opérateur à utiliser pour comparer la mesure à la valeur. Les opérateurs valides sont « supérieur à » et « inférieur à ».	Oui

Attribut	Description	Mandatory
valeur	Un attribut de règle. La valeur seuil à laquelle la métrique est comparée à l'aide de l' opérateur. Si la valeur de la métrique dépasse ce seuil, les alarmes associées sont déclenchées.	Oui
unité de période	Attribut d'une règle. Fréquence à laquelle alerter les utilisateurs si la règle d'alarme est respectée. Cela peut contenir la valeur du jour, de l' heure ou de la semaine. Cela signifie que si la règle est respectée, une alarme sera envoyée une fois par unité de période (par exemple, une fois par jour).	Oui

Le tableau suivant fournit une liste des mesures qui sont suivies concernant le serveur virtuel Citrix ADC.

Compteurs|Description|Desription détaillée|Calcul de Citrix ADM
|—|—|—|—|
|Pour un serveur virtuel VPN :|
total_requests|Nombre total de lancements de sessions VPN|Nombre total de sessions actives sur ce serveur virtuel VPN démarrées pendant un intervalle de temps spécifié par l'utilisateur.|Compteur croissant de façon monotone, incrémenté à chaque lancement de nouvelle session|
app_count	Nombre de lancements d'applications VPN	Nombre total d'applications VPN uniques sur ce serveur virtuel VPN lancées pendant un intervalle de temps spécifié par l'utilisateur.	Augmenter le compteur de façon monotone à chaque lancement d'une nouvelle application
app_launch_duration	Durée de lancement de l'application VPN	Durée moyenne de lancement d' une application (en millisecondes)	Valeur moyenne calculée sur les durées de lancement de toutes les applications VPN lancées sur ce serveur virtuel VPN
Autres serveurs virtuels (CS, LB, Auth, GSLB)		
Total_Requests	Nombre de requêtes	Nombre de requêtes client sur ce serveur virtuel depuis le dernier redémarrage de l'appliance ou depuis la création du serveur virtuel, selon la date la plus récente.	Compteur monotone croissant, incrémenté à chaque nouvelle requête vers ce serveur

virtuel. |
|total_bytes|bytes|Nombre total d'octets transférés du serveur virtuel vers Citrix ADM sur l'intervalle de temps spécifié. |Compteur monotone croissant pour tenir compte du nombre total d'octets servis par ce serveur virtuel. |
|Application_Response_time|Temps de réponse|Temps de réponse moyen du serveur virtuel. |Valeur moyenne des temps de réponse de toutes les demandes reçues par ce serveur virtuel depuis le dernier redémarrage de l'appliance (ou depuis la création du serveur virtuel), selon la dernière éventualité. |

Exemple d'une section d'alarmes dans un StyleBook :

```
operations:
alarms:
 -
  name:lbvserver_alarm
  properties:
  target: $outputs.lbvserver
  email-profile: $parameters.emailprofile
  sms-profile: "NetScalerSMS"
     rules:
      -
        metric: "total_requests"
        operator: "greaterthan"
        value: 25
        period-unit: weekly
        -
          metric: "total_bytes"
          operator: "lessthan"
          value: 1024
          period-unit: day

<!--NeedCopy-->
```

Expressions

February 1, 2024

L'une des caractéristiques les plus puissantes d'un StyleBook est l'utilisation d'expressions. Vous pouvez utiliser des expressions StyleBooks dans différents scénarios pour calculer des valeurs dynamiques. L'exemple suivant est une expression permettant de concaténer une valeur de paramètre avec une chaîne littérale.

Exemple :

```
$parameters.appname + "-mon"
<!--NeedCopy-->
```


Cette expression récupère le paramètre nommé appnameet le concatène avec la chaîne −mon.

Les types d'expressions suivants sont pris en charge :

Expressions arithmétiques

- Ajout (+)
- Soustraction (-)
- Multiplication (*)
- Division (/)
- Module (%)

Exemples :

- Ajouter deux nombres : $parameters.a + $parameters.b
- Multiplier deux nombres : $parameters.a * 10
- Trouver le reste après la division d'un nombre par un autre :

`15%10` Résultats en 5

Expressions de chaîne

- Concaténer deux chaînes (+)

Exemple :

Concaténer deux chaînes : str (« app- ») + $parameters.appname

Liste des expressions

Fusionne deux listes (+)

Exemple :

- Concaténer deux listes : $parameters.external-servers + $parameters.internal-servers
- Si `$parameters.ports-1` vaut [80, 81] et `$parameters.port-2` est [81, 82], `$parameters.ports-1 + $parameters.ports-2` s'affiche sous forme de liste [80, 81, 81, 82].

Expressions relationnelles

- **==**: Teste si deux opérandes sont égaux et renvoie vrai s'ils sont égaux, sinon renvoie faux.

- **!** = : Teste si deux opérandes sont différents et renvoie true s'ils sont différents, sinon renvoie false.
- ** : Retourne true si le premier opérande est supérieur au second opérande, sinon renvoie false.
- **>=** : Retourne true si le premier opérande est supérieur ou égal au second opérande, else renvoie false.
- **<** : Renvoie true si le premier opérande est inférieur au second opérande, sinon renvoie false.
- **<=** : Retourne true si le premier opérande est inférieur ou égal au second opérande, else renvoie false.

Exemple :

- Utilisation de l'opérateur Equality : `$parameters.name = = "abcd"`
- Utilisation de l'opérateur d'inégalité : `$parameters.name != "default"`
- Exemples pour d'autres opérateurs relationnels
  - 10 > 9
  - 10 >= 10
  - 0 < 9
  - 10 <= 9
  - 10 == 10
  - 10 != 1

Expressions logiques - booléenne

- **et** : L'opérateur logique 'et'. Si les deux opérandes sont vrais, le résultat est vrai, sinon il est faux.
- **ou** : l'opérateur logique 'ou'. Si l'un des opérandes est vrai, le résultat est vrai, sinon il est faux.
- **not**: opérateur unaire. Si l'opérande est vrai, le résultat est faux, et le sens inverse.
- **in**: Teste si le premier argument est une sous-chaîne du second argument
- **in** : Teste si un élément fait partie d'une liste

> **Remarque**
>
> Vous pouvez utiliser des expressions de type dans lesquelles les chaînes sont converties en nombres et les nombres sont convertis en chaînes. De même, vous pouvez convertir `tcp-port` en un nombre, et une adresse IP peut être convertie en une chaîne.
>
> Utilisez un délimiteur avant et après tout opérateur. Vous pouvez utiliser les délimiteurs suivants :

- Devant un opérateur : `space`, `tab`, `comma`, `(`, `)`, `[`, `]`
- Après un opérateur : `space`, `tab`, `(`, `[`

Par exemple :

- `abc + def`
- `100 % 10`
- `10 > 9`

Expressions de chaîne verbatim

Vous pouvez utiliser des chaînes textuelles lorsque les caractères spéciaux d'une chaîne doivent prendre leur forme littérale. Ces chaînes peuvent contenir des caractères d'échappement, des barres obliques inverses, des guillemets, des parenthèses, des espaces blancs, des crochets, etc. Dans les chaînes textuelles, l'interprétation habituelle des caractères spéciaux est ignorée. Tous les caractères de la chaîne sont conservés dans leur forme littérale.

Dans StyleBooks, vous pouvez inclure des expressions de stratégie Citrix ADC dans leur forme littérale à l'aide de chaînes textuelles. Les expressions de stratégie contiennent généralement des caractères spéciaux. Sans chaînes textuelles, vous devez échapper à des caractères spéciaux en divisant les chaînes en sous-chaînes.

Pour créer une chaîne textuelle, encapsulez une chaîne entre des caractères spéciaux comme suit :

```
~{
 string }
 ~
<!--NeedCopy-->
```

Vous pouvez utiliser des chaînes textuelles n'importe où dans le StyleBook.

> **Remarque**
>
> N'utilisez pas la séquence de caractères `}  ~` dans une chaîne d'entrée car cette séquence indique la fin d'une chaîne textuelle.

Exemple :

```
 ~{
 HTTP.REQ.COOKIE.VALUE("jsessionid") ALT HTTP.REQ.URL.BEFORE_STR("=").
    AFTER_STR(";jsessionid=") ALT HTTP.REQ.URL.AFTER_STR(";jsessionid="
    ) }
 ~
<!--NeedCopy-->
```


Expressions cibles

Dans une définition StyleBook, vous pouvez utiliser l'`$current-target` expression pour faire référence à l'instance ADC cible actuelle. Pour faire référence spécifiquement à l'adresse IP de l'instance ADC cible, utilisez cette expression comme suit :

```
$current-target.ip
<!--NeedCopy-->
```

Exemple :

```
components:
 -
  name: lb-comp
  type: ns::lbvserver
  properties:
    name: $current-target.ip + "-lbvserver"
<!--NeedCopy-->
```

Dans cet exemple, le nom de l'`lbvserver` est construit avec l'adresse IP de l'instance ADC cible.

Validation du type d'expression

Le moteur StyleBook permet une vérification de type plus forte pendant la compilation, c'est-à-dire que les expressions utilisées lors de l'écriture du StyleBook sont validées lors de l'importation de StyleBook lui-même plutôt que lors de la création du pack de configuration.

Toutes les références aux paramètres, substitutions, composants, propriétés des composants, sorties des composants, variables définies par l'utilisateur (élément répété, index répété, arguments aux fonctions de substitution) et ainsi de suite sont toutes validées pour leur existence et leur type.

Exemple de contrôles de type :

Dans l'exemple suivant, le type attendu de propriété port de `lbvserver` StyleBook est `tcp-port`. Dans Citrix Application Delivery Management (ADM), les validations de type se produisent au moment de la compilation (au moment de l'importation). Le compilateur trouve cette chaîne et ne `tcp-port` sont pas des types compatibles et, par conséquent, le compilateur StyleBook affiche une erreur et ne parvient pas à importer ou à migrer un StyleBook.

```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: str("80")
      servicetype: HTTP
```



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

Pour compiler ce StyleBook avec succès, déclarez ce qui suit en tant que nombre dans le compilateur :

```
port: 80
```

Exemple de marquage d'expressions non valides :

Dans les versions antérieures, lorsqu'une expression non valide était affectée à un nom de propriété, le compilateur ne détectait pas d'expressions non valides et autorisait l'importation des StyleBooks dans Citrix ADM. Maintenant, si ce StyleBook est importé dans Citrix ADM, le compilateur identifie ces expressions non valides et l'indique. Par conséquent, le StyleBook ne parvient pas à importer vers Citrix ADM.

Dans cet exemple, l'expression affectée à la propriété name dans le `lb-sg-binding-comp` composant est : `$components.lbvserver-comp.properties.lbvservername`. Cependant, il n'y a aucune propriété appelée `lbvservername` dans le composant `lbvserver-comp`. Dans les versions précédentes de Citrix ADM, le compilateur aurait autorisé cette expression et l'aurait importée avec succès. L'échec réel se produirait lorsqu'un utilisateur souhaite créer un pack de configuration à l'aide de ce StyleBook. Toutefois, ce type d'erreur est identifié lors de l'importation et le StyleBook n'est pas importé dans Citrix ADM. Corrigez manuellement ces erreurs et importez les StyleBooks.

```
Components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: 80
      servicetype: HTTP
  -
    name: sg-comp
    type: ns::servicegroup
    properties:
      servicegroupname: mysg
      servicetype: HTTP
  -
    name: lb-sg-binding-comp
    type: ns::lbvserver_servicegroup_binding
    condition: $parameters.create-binding
    properties:
      name: $components.lbvserver-comp.properties.lbvservername
      servicegroupname: $components.sg-comp.properties.servicegroupname
<!--NeedCopy-->
```


Listes d'indexation

Les éléments d'une liste sont maintenant accessibles en les indexant directement :

Expression	Description
`$components.test-lbs[0]`	Fait référence au premier élément du composant test-lbs
`$components.test-lbs[0].properties.p1`	Fait référence à la propriété p1 du premier élément du composant test-lbs
`$components.lbcomps[0].outputs.servicegroups[1].properties.servicegroupname`	Fait référence à `servicegroupname` la propriété du deuxième élément dans le `servicegroups` composant, qui est une sortie du premier élément du `lbcomps` composant

Interpolations sur place

February 2, 2024

Il est désormais possible de remplacer une ou plusieurs parties d'une chaîne à l'aide d'une ou plusieurs expressions StyleBook. Lorsque ces expressions de chaîne sont évaluées par le compilateur StyleBook, la partie de la chaîne qui utilise une expression StyleBook est remplacée par la valeur de l'expression. Pour inclure des expressions StyleBook dans une chaîne, nous utilisons la notation suivante :

"…%{…}%…"

où les caractères entre "%{ "and "}%"forment une expression StyleBook. Ces expressions sont appelées « interpolations sur place. »

Par exemple, la chaîne « lb-%{$parameters.appname}%-svc » est une expression de chaîne avec interpolation sur place d'une expression StyleBook. La valeur de l'expression de chaîne dépend de la valeur de l'expression d'interpolation. Considérez que **$parameters.appname** est affecté avec "app1."L'expression de chaîne est ensuite évaluée à **lb-app1-svc**. Cela permet aux valeurs de ne pas être codées en dur dans des expressions de chaîne, mais d'être évaluées en fonction des valeurs définies par l'utilisateur.

Un cas d'utilisation pratique des interpolations sur place consiste à paramétrer les expressions de stratégie dans StyleBooks. Imaginons un scénario dans lequel vous souhaitez écrire une expression de stratégie qui vérifie si l'URL HTTP contient un mot spécifique, par exemple « jpeg ».

Pour cela, vous écrivez une expression de stratégie comme suit : “HTTP.REQ.URL.CONTAINS(\“jpeg\”)”.

Maintenant, si vous souhaitez paramétrer l’objet dans l’URL HTTP, vous pouvez ajouter un paramètre de chaîne dans le StyleBook, par exemple $parameters.url-object. L’expression de stratégie doit être écrite en fonction de ce paramètre. Pour ce faire, vous utilisez la concaténation de chaînes pour obtenir le résultat. L’expression ressemblerait à :

str(“HTTP.REQ.URL.CONTAINS(\’”+ $parameters.url-object + “\”)”)

Si $parameter.url-object est assigné « csv », l’expression ci-dessus correspond à “HTTP.REQ.URL.CONTAINS(\ “csv\”)”. Cependant, cette expression n’est pas facile à lire. Pour faciliter la lecture et la compréhension de ce paramétrage, vous pouvez utiliser des interpolations sur place.

L’expression avec interpolation sur place est maintenant :

str(“HTTP.REQ.URL.CONTAINS(%{quotewrap($parameters.url-object)}%)”)

Dans l’expression ci-dessus, vous avez utilisé une expression d’interpolation qui ajoute les guillemets internes autour de la valeur du $parameters.url-object. Le résultat de cette expression est identique à celui ci-dessus, mais il semble plus intuitif et plus proche du résultat réel.

Types autorisés à l’intérieur des interpolations

Vous pouvez utiliser des expressions qui génèrent des valeurs des types suivants dans les interpolations : booléen, nombre, port TCP, adresse IP et chaîne. La valeur générée est automatiquement transformée en chaîne lorsque les interpolations sont remplacées par le résultat.

Les expressions de chaîne peuvent comporter 0, 1 ou plusieurs interpolations. Dans une interpolation séquentielle, différentes parties de l’expression de chaîne peuvent être remplacées par différentes expressions StyleBook. Par exemple, la chaîne lb-%{$parameters.appname}%-%{$parameters.vip}% renvoie “lb-app1-1.1.1.1”, si $parameters.appname est “app1”et $parameters.vip est “1.1.1.1”

Les expressions de chaîne prennent également en charge les interpolations imbriquées. Autrement dit, une expression d’interpolation peut être imbriquée dans une autre expression d’interpolation afin que la valeur d’une expression puisse devenir une entrée dans la seconde expression.

Par exemple, considérez une chaîne “%{lb-%{$parameters.port + 1}%}%”

La chaîne interne, “**%{$parameters.port + 1}%”returns “lb-81”si $parameters.port**est égal à 80. Ici, cette expression est imbriquée dans une autre expression d’interpolation.

Le tableau suivant décrit les différents types d’interpolations avec des exemples et des résultats correspondants. Les valeurs des paramètres utilisés dans les exemples sont les suivantes :

- $parameters.appname: “lb1”
- $parameters.vip: “1.1.1.1”

- $parameters.n1: 1
- $parameters.n2: 3

Interpolations simples

Expression	Résultat
lb-%{$parameters.appname}%-def	lb-lb1-def

Conversions automatiques de type

Expression	Résultat
lb-%{1}%	lb-1
lb-%{$parameters.vip}%	lb-1.1.1.1
lb-%{true}%	lb-True

Interpolations séquentielles

Expression	Résultat
%{$parameters.appname}%-%{str($parameters.appname)}%	lb1-lb1
lb-%{1}%-%{2}%	lb-1-2

Interpolations imbriquées

Expression	Résultat
%{abc-%{$parameters.n1 + 1}%}%	abc-2

Expression	Résultat
str(“%{abc-%{$parameters.n1}%}%-%{$parameters.n2}%”)	bc-1-3

Interpolations avec quotewrap

Expression	Résultat
str(“%{quotewrap(abcd)}%”) str(“%{quotewrap(https://)} %+HTTP.REQ.HOSTNAME+HTTP.REQ.URL")	“abcd “«code class=”language-plaintext highlighter-rouge”>https://”+HTTP.REQ.HOSTNAME+HTTP.REQ.URL</code>

Caractères d’échappement dans les interpolations

Si les caractères “%{“or “}%”font partie de la chaîne, vous devez fournir “\”comme caractère d’échappement afin que le compilateur StyleBook ne les évalue pas comme des balises d’interpolation.

Exemple :

str(“%{\%{ + str($parameters.vip) + }\%}%”) returns “%{1.1.1.1}%”if $parameters.vip is 1.1.1.1

Le tableau suivant décrit quelques expressions supplémentaires et leurs résultats :

Catégorie	Expression	Résultat
Escaping interpolations	str(“%{str($parameters.n1) + }\%}%”)	1}%
	lb-%{str($parameters.n1) + }\%}%	lb-1}%
	”%{str($parameters.n1) + \” }\%\”}%”	1}%

Fonctions intégrées

February 1, 2024

Les expressions dans StyleBooks peuvent utiliser des fonctions intégrées.

Par exemple, vous pouvez utiliser la fonction intégrée, `str()` pour transformer un nombre en chaîne.

```
str($parameters.order)
```

Ou, vous pouvez utiliser la fonction intégrée, **`int()`** pour transformer une chaîne en un entier.

```
int($parameters.priority)
```

Voici la liste des fonctions intégrées prises en charge dans les expressions StyleBook avec des exemples de leur utilisation :

str()

La fonction `str()` transforme l'argument input en une valeur de chaîne.

Types d'arguments autorisés :

- `string`
- `number`
- `TCP-port`
- **`boolean`**
- `IP address`

Exemples :

- La fonction `"set-"+ str(10)` renvoie `"set-10"`.
- La `str(10)` fonction renvoie `10`.
- La `str(1.1.1.1)` fonction renvoie `1.1.1.1`.
- La `str(T rue)` fonction renvoie `"T rue"`.
- La fonction `str(ADM)` renvoie `"mas"`.

int()

La fonction **`int()`** prend une chaîne, un nombre, une adresse IP ou `tcpport` comme argument et renvoie un entier.

Exemples :

- La fonction `int("10")` renvoie `10`.
- La `int(10)` fonction renvoie `10`.
- La fonction `int(ip('0.0.4.1'))` renvoie `1025`.

bool()

La fonction `bool()` prend n'importe quel type comme argument. Si la valeur de l'argument est **`false`**, vide ou absente, cette fonction renvoie **`false`**.

Sinon, elle renvoie **`true`**.

Exemples :

- La fonction `bool(true)` renvoie **`true`**.
- La fonction `bool(false)` renvoie **`false`**.
- La fonction `bool($parameters.a)` renvoie **`false`** si `$parameters.a` est **`false`**, vide ou absent.

len()

La fonction `len()` prend une chaîne ou une liste comme argument, et renvoie le nombre de caractères dans une chaîne ou le nombre d'éléments d'une liste.

Exemple 1 :

Si vous définissez une substitution comme suit :

```
items: ["123", "abc", "xyz"]
```

La `len($substitutions.items)` fonction renvoie 3

Exemple 2 :

La fonction `len("Citrix ADM")` renvoie `10`.

Exemple 3 :

Si `$parameters.vips` a les valeurs `['1.1.1.1', '1.1.1.2', '1.1.1.3']`, la fonction `len($parameters.vips)` renvoie 3.

min()

La fonction `min()` prend soit une liste, soit une série de nombres ou `tcp-ports` comme arguments, et renvoie le plus petit élément.

Exemples avec une série de numéros/ports tcp :

- La fonction `min(80, 100, 1000)` renvoie `80`.
- La `min(-20, 100, 400)` fonction renvoie `-20`.
- La `min(-80, -20, -10)` fonction renvoie `-80`.
- La fonction `min(0, 100, -400)` renvoie `-400`.

Exemples avec une liste de numéros/tcp-ports :

- Le support `$parameters.ports` est une liste de `tcp-ports` et a les valeurs : `[80, 81, 8080]`.

  La fonction `min($parameters.ports)` renvoie `80`.

max()

La fonction `max()` prend une liste ou une série de nombres ou `tcp-ports` comme arguments, et renvoie le plus grand élément.

Exemples avec une série de numéros/ports tcp :

- La fonction `max(80, 100, 1000)` renvoie `1000`.
- La `max(-20, 100, 400)` fonction renvoie `400`.
- La `max(-80, -20, -10)` fonction renvoie `-10`.
- La fonction `max(0, 100, -400)` renvoie `100`.

Exemples avec une liste de numéros/tcp-ports :

- Le support `$parameters.ports` est la liste de `tcp-ports` et a les valeurs : `[80, 81, 8080]`.

  La fonction `max($parameters.ports)` renvoie `8080`.

bin()

La fonction `bin()` prend un nombre comme argument, et renvoie une chaîne qui représente le nombre au format binaire.

Exemples d'expressions :

La fonction `bin(100)` renvoie `0b1100100`.

oct()

La fonction `oct()` prend un nombre comme argument, et renvoie une chaîne qui représente le nombre au format octal.

Exemples d'expressions :

La fonction `oct(100)` renvoie `0144`.

hex()

La fonction `hex()` prend un nombre comme argument, et renvoie une chaîne minuscule qui représente le nombre au format hexadécimal.

Exemples d'expressions :

La fonction `hex(100)` renvoie `0x64`.

lower()

La fonction `lower()` prend une chaîne comme argument et renvoie la même chaîne en minuscules.

Exemple :

La fonction `lower("ADM")` renvoie `adm`.

upper()

La fonction `upper()` prend une chaîne comme argument et renvoie la même chaîne en majuscules.

Exemple :

La fonction `upper("Citrix ADM")` renvoie `CITRIX ADM`.

sum()

La fonction `sum()` prend une liste de nombres ou `tcpports` comme arguments et renvoie la somme des nombres dans la liste.

Exemple 1 :

Si vous définissez une substitution comme suit :
substitutions :

```
list-of-numbers = [11, 22, 55]
```

La fonction `sum($substitutions.list-of-numbers)` renvoie 88.

Exemple 2 :

Si `$parameters.ports` est `[80, 81, 82]`, la fonction `sum($parameters.ports)` renvoie `243`.

pow()

La fonction `pow()` prend deux nombres comme arguments et renvoie un nombre qui représente le premier argument soulevé à la puissance du second.

Exemple :

La fonction `pow(3,2)` renvoie `9`.

ip()

La fonction `ip()` prend un entier, une chaîne ou une adresse IP comme argument et renvoie l'adresse IP en fonction de la valeur d'entrée.

Exemples :

- Spécifiez une adresse IP dans la fonction `ip`:

  La fonction `ip(3.1.1.1)` renvoie `3.1.1.1`.

- Spécifiez une chaîne dans la fonction `ip`:

  La fonction `ip('2.1.1.1')` renvoie `2.1.1.1`

- Spécifiez un entier dans la fonction `ip`:

  - La fonction `ip(12)` renvoie `0.0.0.12`.
  - Lorsque vous spécifiez un entier en tant que chaîne dans la fonction `ip`, il renvoie une adresse IP équivalente de l'entrée.

    La fonction `ip('1025')` renvoie `0.0.4.1`.

  Cette fonction prend également en charge les opérations d'addition et de soustraction entières et renvoie une adresse IP résultante.

  - Addition : La fonction `ip(1025)+ ip(12)` renvoie `0.0.4.13`.
  - Soustraction : La fonction `ip('1025')- ip(12)` renvoie `0.0.3.245`.
  - Combiner l'addition et la soustraction : `ip('1.1.1.1')+ ip('1.1.1.1')- ip(2)` renvoie `2.2.2.0`.

base64.encode()

La fonction `base64.encode()` prend un argument de chaîne et renvoie la chaîne codée base64.

Exemple :

La fonction `base64.encode("abcd")` renvoie `YWJjZA==`.

base64.decode()

La fonction `base64.decode` prend une chaîne codée base64 comme argument et renvoie la chaîne décodée.

Exemple :

La fonction `base64.decode("YWJjZA==")` renvoie `abcd`.

exists()

La fonction `exists()` prend un argument de n'importe quel type et renvoie un booléen. La valeur renvoyée est `True` si l'entrée a une valeur quelconque. La valeur de retour est `False` Si l'argument input n'a pas de valeur (c'est-à-dire, aucune valeur).

Considérez que `$parameters.monitor` est un paramètre facultatif. Si vous fournissez une valeur à ce paramètre lors de la création d'un pack de configuration, la fonction exist (`$parameters.monitor`) renvoie `True`.

Sinon, elle renvoie `False`.

filter()

La fonction `filter()` prend deux arguments.

Argument 1 : fonction de substitution qui prend un argument et renvoie une valeur booléenne.

Argument 2 : une liste.

La fonction renvoie un sous-ensemble de la liste d'origine où chaque élément est évalué `True` lorsqu'il est passé à la fonction de substitution dans le premier
argument.

Exemple :

Supposons que nous ayons défini une fonction de substitution comme suit.

Substitutions :

`x(a): $a != 81`

Cette fonction renvoie True si la valeur d'entrée n'est pas égale à `81`. Sinon, elle renvoie `False`.

Supposons que `$parameters.ports` est `[81, 80, 81, 89]`.

`filter($substitutions.x, $parameters.ports)` renvoie `[80, 89]` en supprimant toutes les occurrences de `81` de de la liste.

if-then-else()

La fonction **`if`**`-then-`**`else`**`()` prend trois arguments.

Argument 1 : Expression booléenne

Argument 2 : Toute expression

Argument 3 : Toute expression (facultatif)

Si l'expression de l'argument 1 est évaluée à `True`, la fonction renvoie la valeur de l'expression fournie en tant qu'argument 2.

Sinon, si l'argument 3 est fourni, la fonction renvoie la valeur de l'expression dans l'argument 3.

Si l'argument 3 n'est pas fourni, la fonction renvoie `no`.

Exemple 1 :

La fonction **`if`**`-then-`**`else`**`($parameters.servicetype == HTTP, 80, 443)` renvoie `80` si `$parameters.servicetype` a la valeur `HTTP`. Sinon, la fonction renvoie `443`.

Exemple 2 :

La fonction **`if`**`-then-`**`else`**`($parameters.servicetype == HTTP, $parameters.hport, $parameters.sport)` renvoie la valeur de `$parameters.hport` si `$parameters.servicetype` a une valeur `HTTP`.

Sinon, la fonction renvoie la valeur de `$parameters.sport`.

Exemple 3 :

`if``-then-`**`else`**`($parameters.servicetype == HTTP, 80)` renvoie `80` si `$parameters.servicetype` a la valeur `HTTP`.

Sinon, la fonction ne renvoie aucune valeur.

join()

La fonction `join()` prend deux arguments :

Argument 1 : liste de nombres `tcp-ports`, de chaînes ou d'adresses IP

Argument 2 : chaîne de délimiteur (facultatif)

Cette fonction rejoint les éléments de la liste fournie en argument un dans une chaîne, où chaque élément est séparé par la chaîne de délimiteur fournie en argument deux. Si l'argument deux n'est pas fourni, les éléments de la liste sont joints sous la forme d'une seule chaîne.

Exemple :

- `$parameters.ports` est `[81, 82, 83]`.
  - Avec l'argument de délimiteur :

    La fonction `join($parameters.ports, '-')` renvoie `81-82-83`.
  - Sans argument de délimiteur :

    La fonction `join($parameters.ports)` renvoie `818283`.

split()

La fonction `split()` divise une chaîne d'entrée en plusieurs listes en fonction des séparateurs spécifiés. Si aucun séparateur ou vide (`''`) n'est spécifié, cette fonction considère l'espace comme un séparateur et divise la chaîne en listes.

Exemples :

- La fonction `split('Example_string_split', 's')` renvoie `['Example_','tring_','plit']`.
- La `split('Example string split')` fonction renvoie `['Example','string','split']`.
- La `split('Example string split', '')` fonction renvoie `['Example','string','split']`.
- La `split('Example string')` fonction renvoie `['Example','string']`.

  Cette fonction considère les espaces continus comme un seul espace.

map()

La fonction `map()` prend deux arguments ;

Argument 1 : N'importe quelle fonction

Argument 2 : Une liste d'éléments.

La fonction renvoie une liste où chaque élément de la liste est le résultat de l'application de la fonction `map()` (argument un) à l'élément correspondant dans l'argument deux.

Fonctions autorisées dans l'argument 1 :

- Fonctions intégrées qui prennent un argument :

  ```
  base64.encode, base64.decode, bin, bool, exists, hex, int, ip,
  len, lower, upper, oct, quotewrap, str, trim, upper, url.encode,
  url.decode
  ```

- Fonctions de substitution qui prennent au moins un argument.

Exemple :

Supposons que $parameters.nums est `[81, 82, 83]`.

- Mapper à l'aide d'une fonction intégrée, str

  La fonction `map(str, $parameters.nums)` renvoie `["81", "82", "83"]`

  Le résultat de la fonction map est la liste des chaînes où chaque élément est une chaîne est calculée en appliquant la fonction str sur l'élément correspondant dans la liste d'entrée ($parameters.nums).

- Carte utilisant une fonction de substitution

  - Substitutions :

    ```
    add-10(port): $port + 10
    ```

  - Expression :

    La fonction `map($substitutions.add-10, $parameters.nums)` renvoie une liste de nombres : `[ 91, 92, 93 ]`

Le résultat de cette fonction de carte est une liste de nombres, chaque élément est calculé en appliquant la fonction de substitution `$substitutions.add-10` sur l'élément correspondant dans la liste d'entrée (`$parameters.nums`).

quotewrap()

La fonction `quotewrap()` prend une chaîne comme argument et renvoie une chaîne après avoir ajouté un caractère de guillemets doubles avant et après la valeur d'entrée.

Exemple :

La fonction `quotewrap("ADM")` renvoie `"mas"`

replace()

La fonction `replace()` prend trois arguments :

Argument 1 : chaîne

Argument 2 : chaîne ou liste

Argument 3 : chaîne (facultatif)

La fonction remplace toutes les occurrences de l'argument deux par l'argument trois dans l'argument un.

Si l'argument trois n'est pas fourni, toutes les occurrences de l'argument deux sont supprimées de l'argument 1 (en d'autres termes, remplacées par une chaîne vide).

Remplacez une sous-chaîne par une autre sous-chaîne :

- La `replace('abcdef', 'def', 'xyz')` fonction renvoie `abcxyz`.

  Toutes les occurrences de `def` sont remplacées par `xyz`.

- `replace('abcdefabc', 'def')` renvoie `abcabc`.

  Comme il n'y a pas de troisième argument, `def` est supprimé de la chaîne résultante.

Spécifiez la liste de caractères que vous souhaitez remplacer dans une chaîne.

```
$parameters.spl_chars = ['@', '#', '!', '%']
```

Cette liste contient les valeurs qui doivent être remplacées dans une chaîne d'entrée.

La `replace('An#example@to%replace!characters', $parameters.spl_chars, '_')` fonction renvoie `An_example_to_replace_characters`.

La chaîne de sortie comporte un trait de soulignement (_) au lieu des caractères spécifiés dans la `$parameters.spl_chars` liste.

trim()

La fonction `trim()` renvoie une chaîne dans laquelle les espaces de début et de fin sont retirés de la chaîne d'entrée.

Exemple :

La `trim('abc ')` fonction renvoie `abc`.

truncate()

La fonction `truncate()` prend deux arguments :

Argument 1 : chaîne

Argument 2 : nombre

La fonction renvoie une chaîne dans laquelle la chaîne d'entrée de l'argument 1 est tronquée à la longueur spécifiée par l'argument 2.

Exemple :

`truncate('Citrix ADM', 6)` renvoie `Citrix`.

distinct()

La fonction `distinct()` extrait des éléments uniques d'une entrée de liste.

Exemples :
Si `$parameters.input_list` est `['ADM', 'ADC', 'VPX', 'ADC', 'ADM', 'CPX']`, la fonction `distinct($parameters.input_list)` renvoie `['ADM', 'ADC', 'VPX', 'CPX']`.

url.encode()

La fonction `url.encode()` renvoie une chaîne où les caractères sont transformés en utilisant le jeu de caractères ASCII selon RFC 3986.

Exemple :

La `url.encode("a/b/c")` fonction renvoie `a%2Fb%2Fc`.

url.decode()

La fonction `url.decode()` renvoie une chaîne où l'argument encodé URL est décodé en une chaîne régulière selon RFC 3986.

Exemple :

La `url.decode("a%2Fb%2Fc")` fonction renvoie `a/b/c`.

is-ipv4()

La fonction `is-ipv4()` prend une adresse IP comme argument et renvoie le booléen `True` si l'adresse IP est au format IPv4.

La `is-ipv4(10.10.10.10)` fonction renvoie `True`

is-ipv6()

La fonction `is-ipv6()` prend une adresse IP comme argument et renvoie le booléen `True` si l'adresse IP est au format IPv6.

La fonction `is-ipv6(2001:DB8::)` renvoie `True`

startswith()

La fonction `startswith()` détermine si une chaîne commence par un préfixe donné. Cette fonction nécessite deux arguments de chaîne obligatoires.

```
startswith(str, sub_str)
```

Cette fonction retourne `True` lorsque la chaîne (`str`) commence par la sous-chaîne (`sub_str`).

Exemples :

- La `startswith('Citrix', 'Ci')` fonction renvoie `True`.
- La fonction `startswith('Citrix', 'iC')` renvoie `False`
- La fonction `startswith('Citrix', 'Ab')` renvoie `False`

endswith()

La fonction `endswith()` détermine si une chaîne se termine par un suffixe donné. Cette fonction nécessite deux arguments de chaîne obligatoires.

```
endswith(str, sub_str)
```

Cette fonction renvoie `True` lorsque la chaîne (`str`) se termine par la sous-chaîne (`sub_str`).

Exemples :

- La fonction `endswith('Citrix', 'ix')` renvoie `True`.
- La `endswith('Citrix', 'Ix')` fonction renvoie `False`.
- La `endswith('Citrix', 'ab')` fonction renvoie `False`.

contains()

La fonction `contains()` détermine si une chaîne contient une sous-chaîne donnée. Cette fonction nécessite deux arguments de chaîne obligatoires.

```
contains(str, sub_str)
```

Cette fonction renvoie `True` lorsque la sous-chaîne (`sub_str`) est contenue n'importe où dans la chaîne (`str`).

Exemple :

- La `contains('Citrix', 'tri')` fonction renvoie `True`.
- La `contains('Citrix', 'Ci')` fonction renvoie `True`.
- La `contains('Citrix', 'ti')` fonction renvoie `False`

substring()

Utilisez la fonction `substring()` pour extraire une sous-chaîne d'une chaîne.

```
substring(str, start_index, end_index)
```

Cette fonction nécessite les deux arguments obligatoires et un argument entier facultatif.

- `str` (Obligatoire)
- `start_index` (Obligatoire)
- `end_index` (Facultatif)

Cette fonction renvoie la sous-chaîne de la chaîne (`str`) qui se trouve entre les positions d'index spécifiées. Si vous ne spécifiez pas la position d'index de fin, la fonction extrait la sous-chaîne de l'index de début à la fin de la chaîne.

> **Remarque**
>
> Lorsque vous spécifiez `end_index`, la sous-chaîne exclut le caractère à la position `end_index` .

Exemple :

- La fonction `substring('Citrix', 2)` renvoie `trix`
- La fonction `substring('Citrix', 10)` renvoie (")

  Dans cet exemple, la fonction renvoie une chaîne vide car elle a une position `start_index` non valide.

- La fonction `substring('Citrix', 2, 4)` renvoie `tr`

  Dans cet exemple, la fonction extrait les caractères compris entre 2 et 4 positions d'index.

- La fonction `substring('Citrix', -3)` renvoie `rix`

  Si vous souhaitez extraire les caractères qui se trouvent à la fin de la chaîne, spécifiez une valeur négative pour l'argument `start_index`.

  Dans cet exemple, la fonction extrait la sous-chaîne qui inclut les trois derniers caractères de la chaîne.

Détection des dépendances

February 1, 2024

Les composants d'un StyleBook peuvent faire référence aux propriétés ou aux sections d'autres composants du même StyleBook. Les composants sont des blocs complets en eux-mêmes et ils peuvent ne pas être écrits dans le même ordre que celui dans lequel ils doivent être exécutés. Le compilateur StyleBook vérifie l'ordre dans lequel les composants sont écrits, puis les exécute dans un ordre logique.

Exemple :

```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: 80
      servicetype: HTTP
 -
    name: lb-sg-binding-comp
    type: ns::lbvserver_servicegroup_binding
    condition: $parameters.create-binding
    properties:
      name: $components.lbvserver-comp.properties.name
      servicegroupname: $components.sg-comp.properties.servicegroupname
-
    name: sg-comp
    type: ns::servicegroup
    properties:
      servicegroupname: mysg
      servicetype: HTTP
<!--NeedCopy-->
```

Dans l'exemple ci-dessus, trois composants sont définis - **lbvserver-comp**, **lb-sg-binding-comp**et **sg-comp**. Lorsque ce StyleBook est exécuté, le lbvserver-comp est d'abord créé. Le lb-sg-binding-comp fait référence aux propriétés lbvserver-comp, mais il ne peut pas être créé ensuite, bien qu'il

s'agisse du deuxième composant défini dans le StyleBook. En effet, le lb-sg-binding-comp dépend également du sg-comp qui n'a pas encore été créé. Par conséquent, le compilateur réorganise les composants de manière à ce que les dépendances d'un composant soient résolues au moment où un composant est créé, et exécute cette liste réorganisée de composants. L'ordre d'exécution du StyleBook ci-dessus est le suivant : lbvserver-comp, sg-comp et lb-sg-binding-comp.

Ainsi, l'auteur d'un StyleBook n'a pas besoin de s'inquiéter de l'ordre correct des composants. Les composants peuvent apparaître dans n'importe quel ordre. Le compilateur calcule l'ordre d'exécution correct des composants en fonction de la façon dont les composants se réfèrent. Notez que cette détection et cette réorganisation des dépendances fonctionnent également pour les sections de substitution et de sortie.

Dépendances cycliques

Comme un composant peut faire référence à un autre composant, il est possible qu'un cycle de dépendances soit introduit dans la définition du StyleBook. Par exemple, si le composant A fait référence à une propriété définie dans le composant B, qui fait encore référence à une propriété définie dans le composant A. Ce type de dépendance est appelé dépendances cycliques. Les dépendances cycliques ne peuvent pas être résolues automatiquement. L'auteur du StyleBook doit corriger manuellement la définition du StyleBook pour éliminer ces dépendances cycliques. Le compilateur sera en mesure d'identifier les dépendances cycliques - si elles existent, et de les signaler.

L'exemple suivant montre une dépendance cyclique des composants :

```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: $components.lb-sg-binding-comp.properties.name
      ipv46: 10.102.190.15
      port: 80
      servicetype: HTTP
  -
    name: lb-sg-binding-comp
    type: ns::lbvserver_servicegroup_binding
    condition: $parameters.create-binding
    properties:
     name: mylb
      servicegroupname: $components.sg-comp.properties.servicegroupname
  -
    name: sg-comp
    type: ns::servicegroup
    properties:
      servicegroupname: mysg
      servicetype: $components.lbvserver-comp.properties.servicetype
<!--NeedCopy-->
```


Dans l'exemple ci-dessus, il existe trois composants : **lbvserver-comp, lb-sg-binding-comp et sg-comp. lbvserver-comp**dépend de **lb-sg-binding-comp, lb-sg-binding comp dépend**de sg-comp et **sg-comp dépend de lbvserver-comp**. Ici, un cycle de dépendances entre ces composants est formé et cela ne peut pas être résolu automatiquement. Par conséquent, ce StyleBook ne peut pas être exécuté. Le compilateur StyleBook détecte cela et empêche l'importation de StyleBook dans Citrix ADM.

Gestion des instances

February 1, 2024

Les instances sont des appliances Citrix Application Delivery Controller (ADC) que vous pouvez gérer, surveiller et dépanner à l'aide de Citrix Application Delivery Management (ADM). Vous devez ajouter des instances à Citrix ADM pour les surveiller. Vous pouvez ajouter des instances lorsque vous configurez Citrix ADM ou version ultérieure. Une fois que vous avez ajouté des instances à Citrix ADM, elles sont interrogées en permanence pour collecter des informations qui peuvent être utilisées ultérieurement pour résoudre des problèmes ou en tant que données de reporting.

Les instances peuvent être regroupées sous la forme d'un groupe statique ou d'un bloc IP privé. Un groupe statique d'instances peut être utile lorsque vous souhaitez exécuter des tâches spécifiques telles que des tâches de configuration, etc. Un bloc IP privé regroupe vos instances en fonction de leur emplacement géographique.

Ajouter une instance

Vous pouvez ajouter des instances lors de la configuration du serveur Citrix ADM pour la première fois ou plus tard. Pour ajouter des instances, vous devez spécifier le nom d'hôte ou l'adresse IP de chaque instance Citrix ADC, ou une plage d'adresses IP.

Pour savoir comment ajouter une instance à Citrix ADM, consultez la section Ajouter des instances à Citrix ADM.

Lorsque vous ajoutez une instance au serveur Citrix ADM, le serveur s'ajoute implicitement comme destination d'interruption pour l'instance et collecte l'inventaire de l'instance. Pour en savoir plus, consultez Comment Citrix ADM découvre les instances.

Après avoir ajouté une instance, vous pouvez la supprimer en accédant à **Réseaux**> **Tableau de bord** et en cliquant sur **Toutes les instances**. Sur la page Instances, sélectionnez l'instance à supprimer et cliquez sur **Supprimer**.

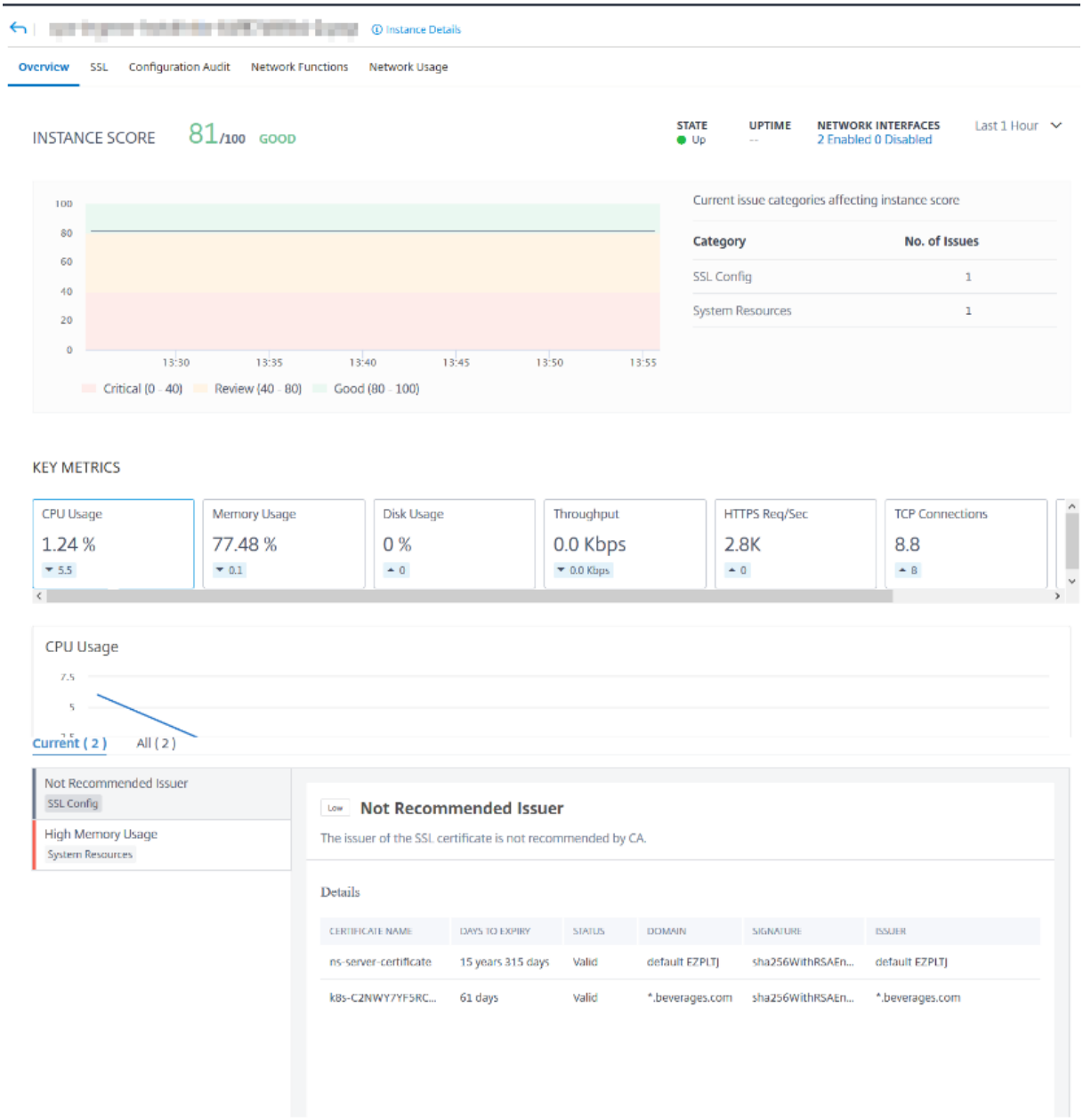
Comment utiliser le tableau de bord de l'instance

Le tableau de bord par instance de Citrix ADM affiche les données sous forme de tableau et de graphique pour l'instance sélectionnée. Les données collectées à partir de votre instance lors du processus de sondage sont affichées sur le tableau de bord.

Par défaut, chaque minute, les instances gérées sont interrogées pour la collecte de données. Les informations statistiques telles que l'état, les requêtes HTTP par seconde, l'utilisation du processeur, l'utilisation de la mémoire et le débit sont collectées en continu à l'aide des appels NITRO. En tant qu'administrateur, vous pouvez afficher toutes ces données collectées sur une seule page, identifier les problèmes dans l'instance et prendre des mesures immédiates pour les corriger.

Pour afficher le tableau de bord d'une instance spécifique, accédez à **Réseaux** > **Instances**. Dans le résumé, choisissez le type d'instance, puis sélectionnez l'instance à afficher et cliquez sur **Tableau de bord**.

L'illustration suivante fournit une vue d'ensemble des différentes données affichées sur le tableau de bord par instance :



- **Vue d'ensemble**. L'onglet Vue d'ensemble affiche l'utilisation du processeur et de la mémoire de l'instance choisie. Vous pouvez également afficher les événements générés par l'instance et les données de débit. Les informations spécifiques à l'instance, telles que l'adresse IP, son matériel et ses versions LOM, les détails du profil, le numéro de série, la personne à contacter, etc. sont également affichées ici. En faisant défiler vers le bas, les fonctionnalités sous licence disponibles sur l'instance choisie ainsi que les modes configurés sur celle-ci.

  Pour plus d'informations, consultez Détails de l'instance.

- Tableau de**bord SSL**. Vous pouvez utiliser l'onglet SSL du tableau de bord par instance pour afficher ou contrôler les détails des certificats SSL, des serveurs virtuels SSL et des protocoles SSL

de l'instance que vous avez choisie. Vous pouvez cliquer sur les « chiffres » dans les graphiques pour afficher plus de détails.

- **Audit de configuration**. Vous pouvez utiliser l'onglet Audit de configuration pour afficher toutes les modifications de configuration qui se sont produites sur l'instance choisie. L ' **état enregistré de la configuration NetScaler et les diagrammes de dérive de configurationNetScaler du tableau de bord affichent des informations détaillées sur les modifications de configuration**enregistrées par rapport aux configurations non enregistrées.
- **Fonctions réseau**. À l'aide du tableau de bord des fonctions réseau, vous pouvez surveiller l'état des entités configurées sur l'instance Citrix ADC sélectionnée. Vous pouvez afficher des graphiques pour vos serveurs virtuels qui affichent des données telles que les connexions client, le débit et les connexions aux serveurs.
- **Utilisation du réseau**. Vous pouvez consulter les données de performance réseau de l'instance sélectionnée dans l'onglet Utilisation du réseau. Vous pouvez afficher des rapports pendant une heure, un jour, une semaine ou un mois. La fonction de curseur de chronologie peut être utilisée pour personnaliser la durée des rapports réseau générés. Par défaut, seuls huit rapports sont affichés, mais vous pouvez cliquer sur l'icône « plus » dans le coin inférieur droit de l'écran pour ajouter un rapport de performance supplémentaire.

Surveiller les sites distribués à l'échelle mondiale

February 1, 2024

En tant qu'administrateur réseau, vous devrez peut-être surveiller et gérer les instances réseau déployées sur des sites géographiques. Toutefois, il n'est pas facile d'évaluer les besoins du réseau lors de la gestion des instances réseau dans des datacenters répartis géographiquement.

Les géomaps de Citrix Application Delivery Management (ADM) vous fournissent une représentation graphique de vos sites et répartit votre expérience de surveillance réseau par géographie. Avec les géomaps, vous pouvez visualiser la distribution de votre instance réseau par emplacement et surveiller les problèmes réseau.

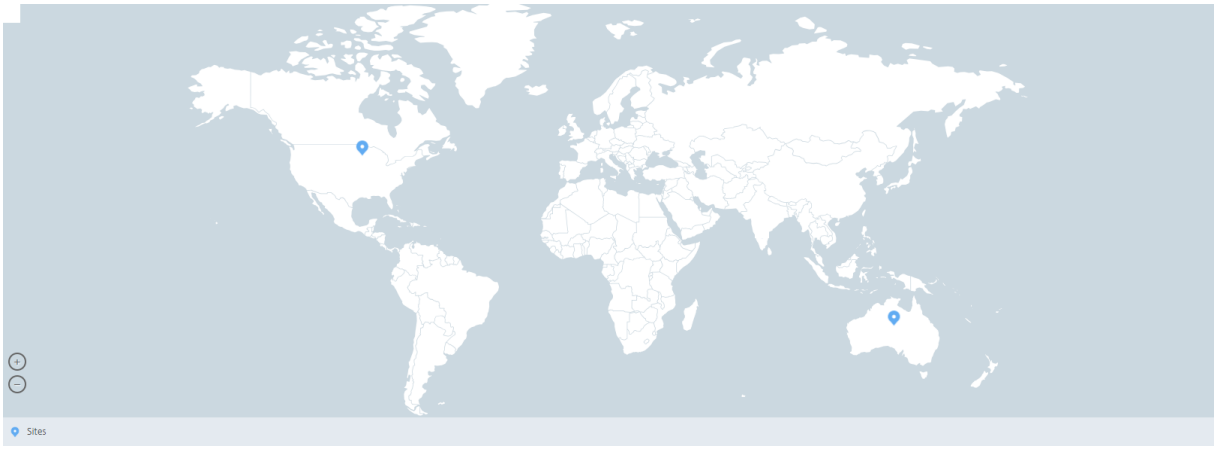
La section suivante explique comment surveiller les centres de données dans Citrix ADM.

Le site Citrix ADM est un regroupement logique d'instances de Citrix Application Delivery Controller (ADC) dans un emplacement géographique spécifique. Par exemple, lorsqu'un site est affecté à Amazon Web Services (AWS) et un autre site peut être affecté à Azure™. Un autre site est hébergé dans les locaux du locataire. Citrix ADM gère et surveille toutes les instances Citrix ADC connectées à tous les sites. Vous pouvez utiliser Citrix ADM pour surveiller et collecter des données Syslog, AppFlow, SNMP et toutes les données de ce type provenant des instances gérées.

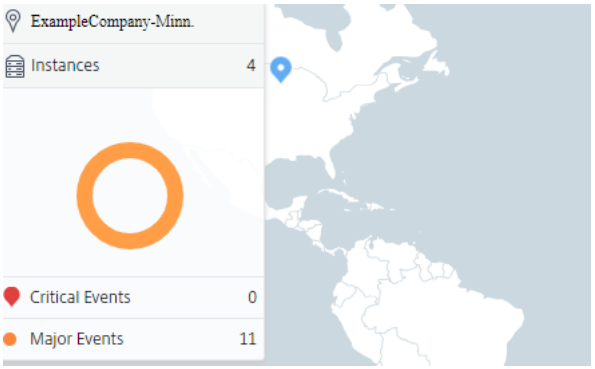
Geomaps dans Citrix ADM vous fournit une représentation graphique de vos sites. Geomaps décompose également votre expérience de surveillance réseau par zone géographique. Avec les géomaps, vous pouvez visualiser la distribution de votre instance réseau par emplacement et surveiller tous les problèmes réseau. Vous pouvez accéder à la page **Réseaux** > **Tableau de bord** pour obtenir une représentation visuelle des sites créés sur la carte du monde.

Cas d'utilisation

Un opérateur de téléphonie mobile de premier plan, ExampleCompany, s'appuyait sur des fournisseurs de services privés pour héberger ses ressources et ses applications. L'entreprise possédait déjà deux sites, l'un à Minneapolis aux États-Unis et l'autre à Alice Springs en Australie. Dans cette image, vous pouvez voir que deux marqueurs représentent les deux sites existants.



Les marqueurs affichent également un nombre, qui indique le nombre d'applications dans chaque site. Vous pouvez cliquer sur ces marqueurs pour plus d'informations sur chaque site.

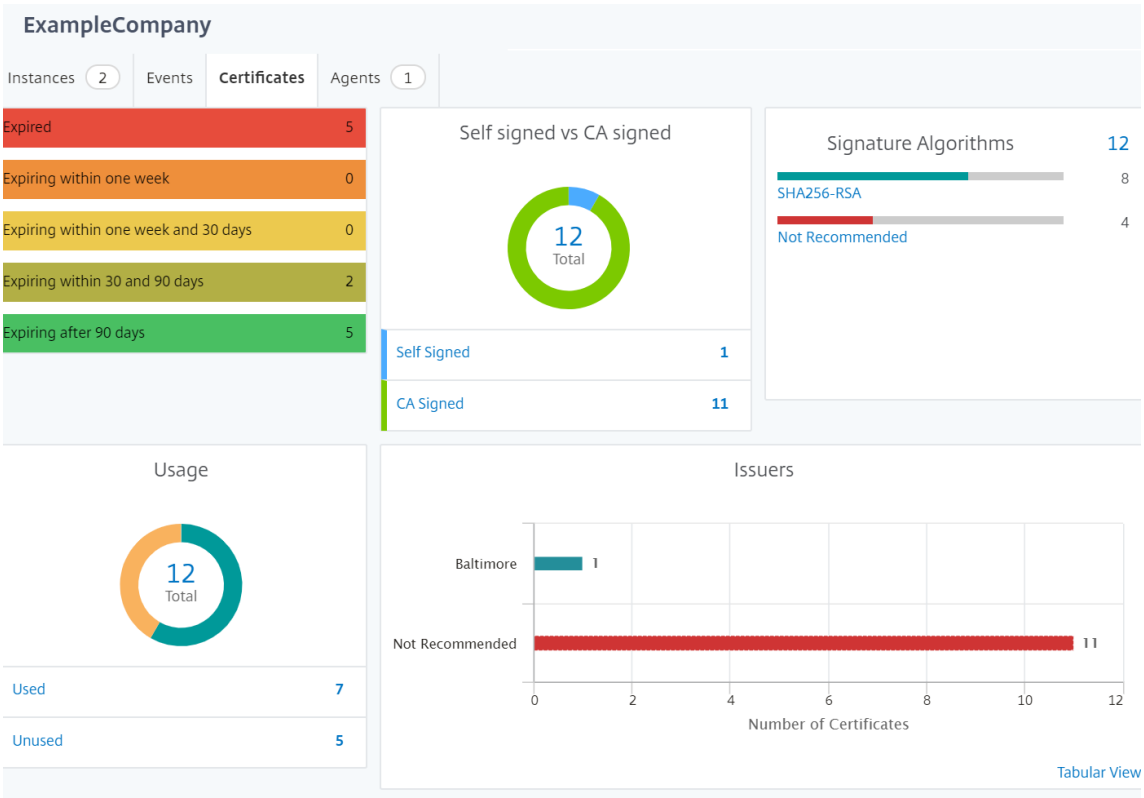


Cliquez sur les onglets pour afficher plus d'informations :

- Onglet**Instances** : affichez les informations suivantes dans cet onglet :
  - Adresse IP de chaque instance réseau
  - Type d'instance

  - Nombre d'événements critiques sur eux
  - Événements significatifs et tous les événements générées sur une instance Citrix ADC.

- Onglet**Événements** : consultez la liste des événements critiques et significatifs signalés sur les instances.
- Onglet**Certificats** : affichez les informations suivantes dans cet onglet :
  - Liste des certificats de toutes les instances
  - État d'expiration
  - Informations vitales et les 10 principales instances de nombreux certificats utilisés.
- Onglet**Agents** : affichez la liste des agents auxquels les instances sont liées.



Configuration des géomaps

ExampleCompany a décidé de créer un troisième site à Bangalore, en Inde. L'entreprise souhaitait tester le cloud en déchargeant certaines de ses applications informatiques internes les moins critiques vers le bureau de Bangalore. L'entreprise a décidé d'utiliser les services de cloud computing d'AWS.

En tant qu'administrateur, vous devez d'abord créer un site, puis ajouter les instances Citrix ADC dans Citrix ADM. Vous devez également ajouter l'instance au site, ajouter un agent et lier l'agent au site. Citrix ADM reconnaît ensuite le site auquel appartiennent l'instance Citrix ADC et l'agent.

Pour plus d'informations sur l'ajout d'instances Citrix ADC, consultez la section Ajout d'instances.

Pour créer des sites :

Créez des sites avant d'ajouter des instances dans Citrix ADM. Fournir des informations de localisation vous permet de localiser le site avec précision.

Accédez à **Réseaux** > **Sites**, puis cliquez sur**Ajouter**.

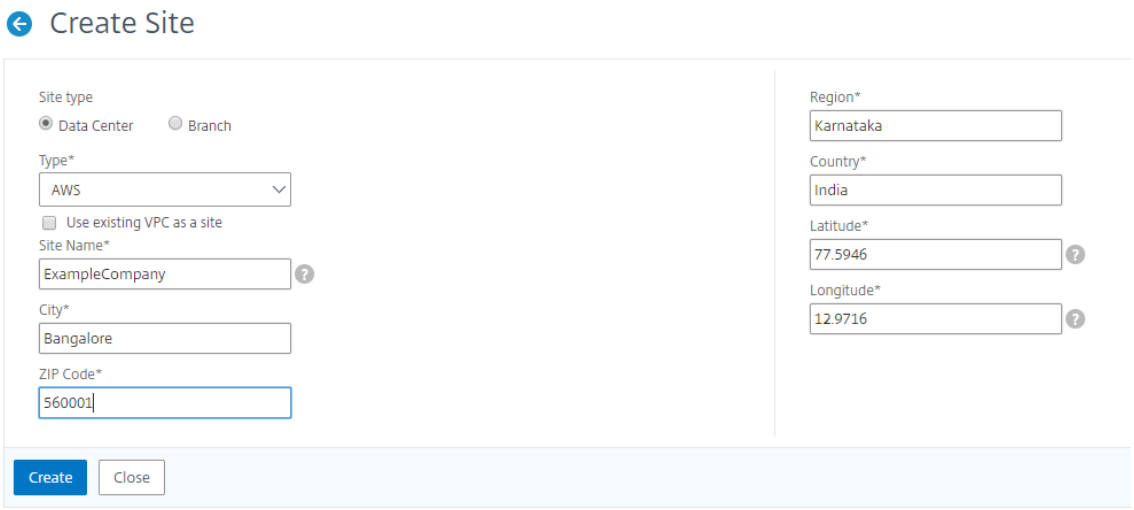
1. Dans la page**Créer un site**, spécifiez les informations suivantes :
    a) **Type de site** : Sélectionnez un **centre de données**.

    > **Remarque**
    >
    > Le site peut fonctionner comme centre de données principal ou comme succursale. Choisissez en conséquence.

    b) **Type** : Sélectionnez AWS comme fournisseur de cloud dans la liste.

    > **Remarque**
    >
    > Cochez la case **Utiliser un VPC existant comme site** en conséquence.

    c) **Nom du site** : entrez le nom du site.
    d) **Ville** : entrez la ville.
    e) **Code postal** : entrez le code postal.
    f) **Région** : entrez la région.
    g) **Pays** : Tapez le pays
    h) **Latitude** : saisissez la latitude de l'emplacement.
    i) **Longitude** : saisissez la longitude de l'emplacement.
2. Cliquez sur**Créer**.

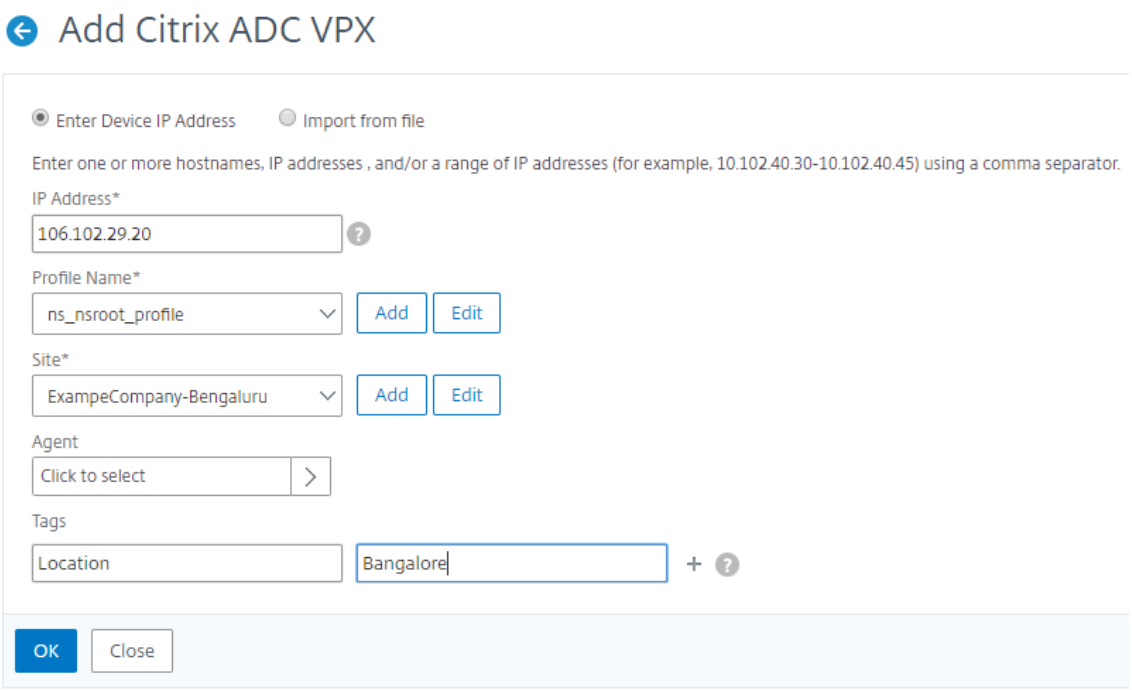


Pour ajouter des instances et sélectionner des sites :

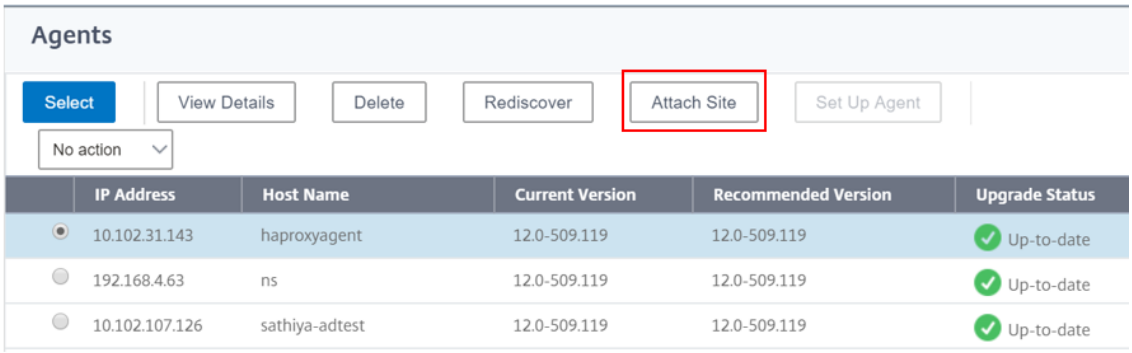
Après avoir créé des sites, vous devez ajouter des instances dans Citrix ADM. Vous pouvez sélectionner le site précédemment créé, ou vous pouvez également créer un site et associer l'instance.

Après avoir créé des sites, vous devez ajouter des instances dans Citrix ADM. Vous pouvez sélectionner le site précédemment créé, ou vous pouvez également créer un site et associer l'instance.

1. Dans Citrix ADM, accédez à **Réseaux** > **Instances**.
2. Sélectionnez le type d'instance à créer, puis cliquez sur **Ajouter**.
3. Sur la page **Ajouter Citrix ADC VPX**, tapez l'adresse IP et sélectionnez le profil dans la liste.
4. Sélectionnez le site dans la liste. Vous pouvez cliquer sur le signe + à côté **du champ Site** pour créer un site ou cliquer sur l'icône de modification pour modifier les détails du site par défaut.
5. Cliquez sur la flèche droite et sélectionnez l'agent dans la liste qui s'affiche.



6. Après avoir choisi l'agent, vous devez l'associer au site. Cette étape permet à l'agent d'être lié au site. Sélectionnez l'agent et cliquez sur **Joindre le site**.

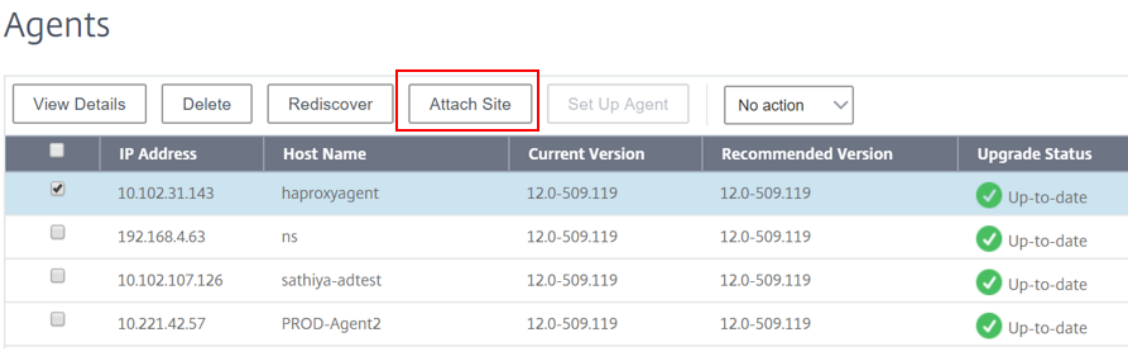


1. Sélectionnez le site dans la liste et cliquez sur **Enregistrer**.
1. Cliquez sur **OK**.

Vous pouvez également attacher un agent à un site en accédant à **Réseaux** > **Agents** .

Pour associer un agent Citrix ADM au site :

1. Dans Citrix ADM, accédez à **Réseaux** > **Agents** .
2. Sélectionnez l'agent, puis cliquez sur **Joindre le site**.



1. Vous pouvez associer le site et cliquer sur **Enregistrer**.

Citrix ADM commence à surveiller les instances de Citrix ADC ajoutées dans le site Bangalore ainsi que les instances des deux autres sites.

Comment créer des balises et affecter des instances

February 1, 2024

Citrix Application Delivery Management (ADM) vous permet désormais d'associer vos instances Citrix Application Delivery Controller (ADC) à des balises. Une balise est un mot-clé ou un terme à un mot que vous pouvez affecter à une instance. Les balises ajoutent des informations supplémentaires sur l'instance. Les balises peuvent être considérées comme des métadonnées qui permettent de décrire une instance. Les balises vous permettent de classer et de rechercher des instances en fonction de ces mots-clés spécifiques. Vous pouvez également affecter plusieurs balises à une seule instance.

Les cas d'utilisation suivants vous aident à comprendre comment le balisage des instances vous aide à mieux les surveiller.

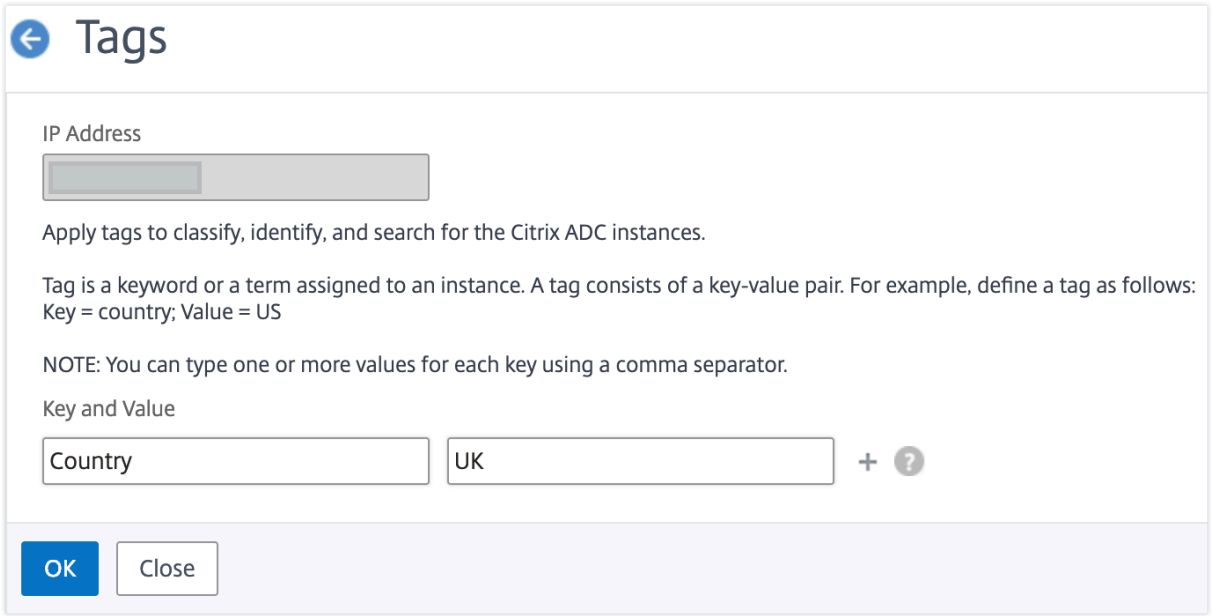
- **Cas d'utilisation 1** : Vous pouvez créer une balise pour identifier toutes les instances au Royaume-Uni. Ici, vous pouvez créer une balise avec la clé « Pays » et la valeur « UK ». Cette balise vous aide à rechercher et à surveiller toutes ces instances au Royaume-Uni.
- **Cas d'utilisation 2** : vous souhaitez rechercher des instances qui se trouvent dans l'environnement intermédiaire. Ici, vous pouvez créer une balise avec la clé « Purpose » et la valeur « Staging_ns. » Cette balise vous permet de séparer toutes les instances utilisées dans l'environnement intermédiaire des instances dont les requêtes client sont exécutées à travers elles.
- **Cas d'utilisation 3** : Considérez une situation où vous souhaitez connaître la liste des instances Citrix ADC qui se trouvent dans la zone « Swindon » au Royaume-Uni et que vous possédez, David T. Vous pouvez créer des balises pour toutes ces exigences et l'affecter à toutes les instances qui satisfont à ces conditions.

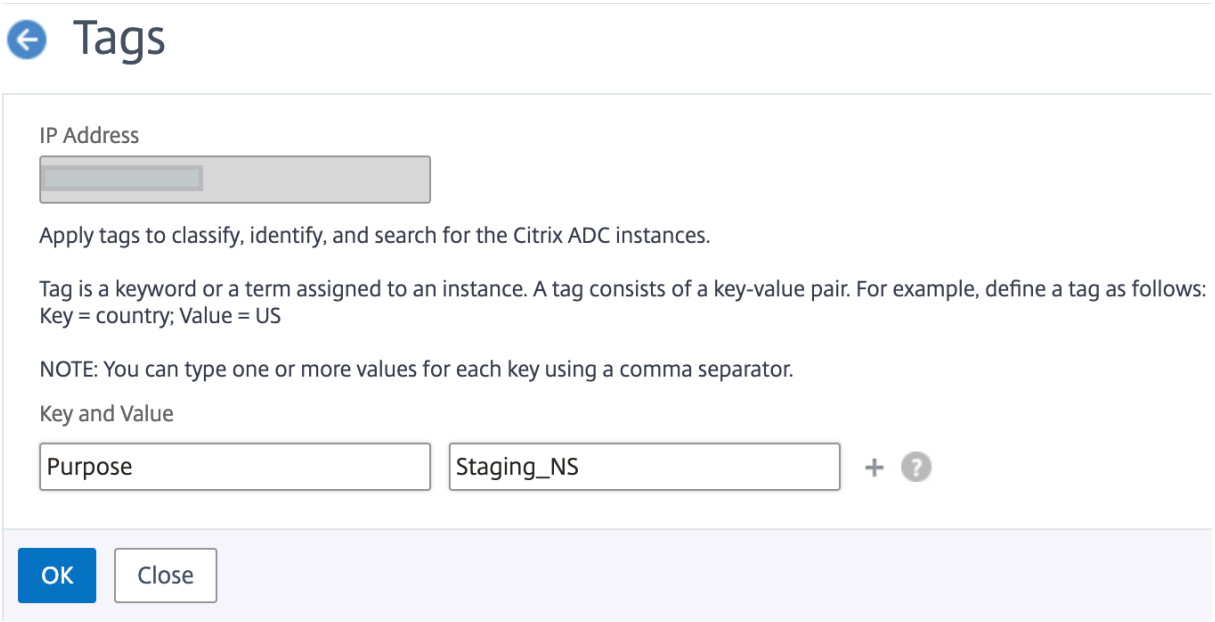
Pour affecter des balises à l'instance Citrix ADC VPX :

1. Dans Citrix ADM, accédez à **Réseaux** > **Instances** > **Citrix ADC**.
2. Sélectionnez l'onglet **Citrix ADC VPX**.
3. Sélectionnez le Citrix VPX requis.
4. Cliquez sur **Balises**.
5. Créez des balises et cliquez sur **OK**.

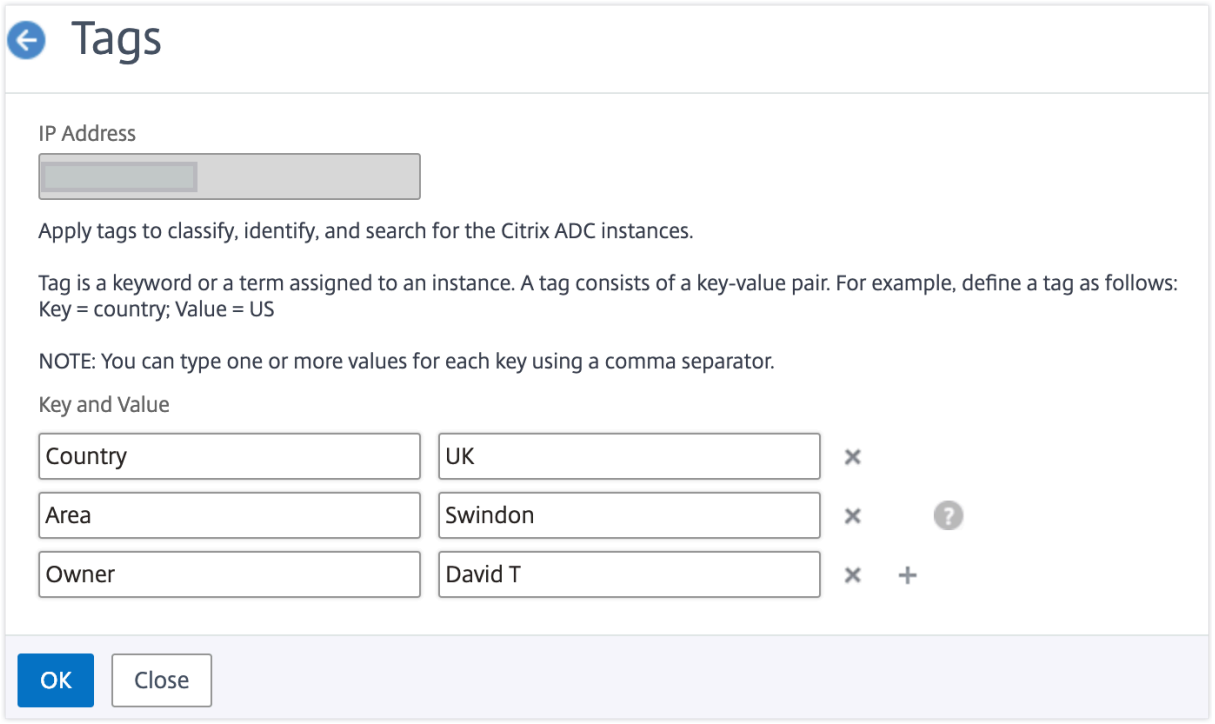
La fenêtre **Balises** qui s'affiche vous permet de créer vos propres paires « clé-valeur » en affectant des valeurs à chaque mot clé que vous créez.

Par exemple, les images suivantes montrent quelques mots clés créés et leurs valeurs. Vous pouvez ajouter vos propres mots clés et saisir une valeur pour chaque mot clé.



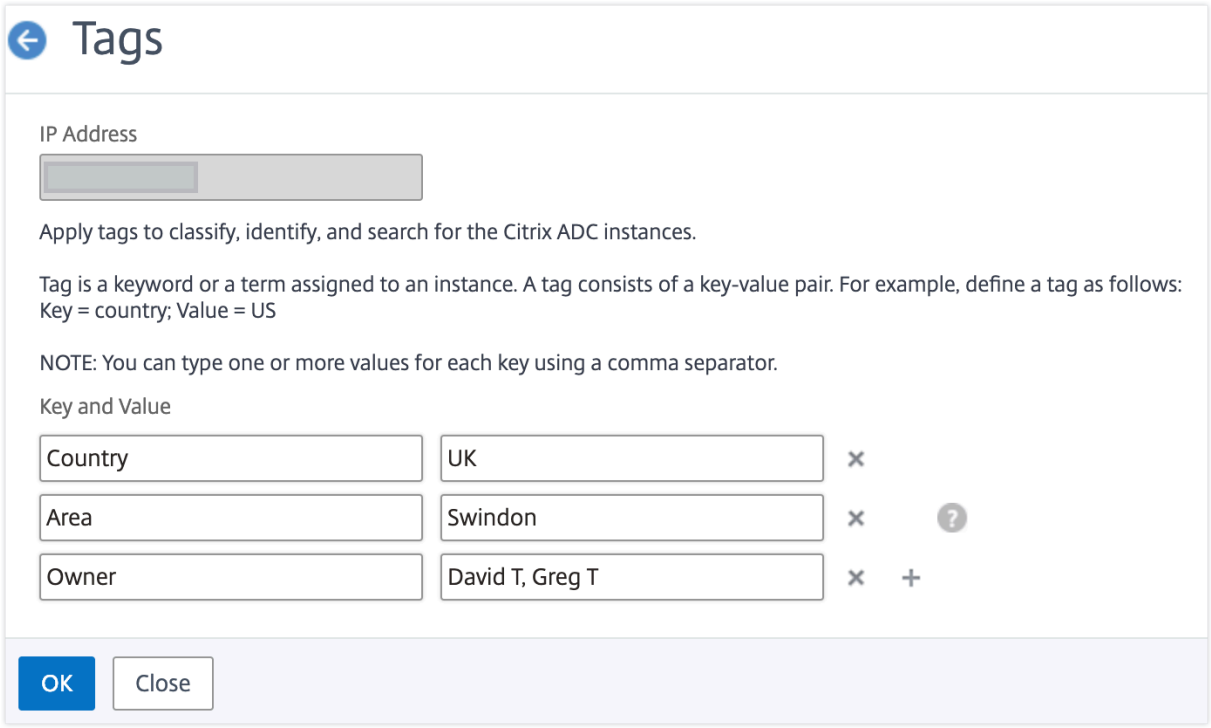


Vous pouvez également ajouter plusieurs balises en cliquant sur « +. » L'ajout de balises multiples et significatives vous permet de rechercher efficacement les instances.



Vous pouvez ajouter plusieurs valeurs à un mot-clé en les séparant par des virgules.

Par exemple, vous attribuez le rôle d'administrateur à un autre collègue, Greg T. Vous pouvez ajouter son nom en le séparant par une virgule. L'ajout de plusieurs noms vous aide à rechercher par l'un des noms ou par les deux noms. Citrix ADM reconnaît les valeurs séparées par des virgules en deux valeurs différentes.



Pour en savoir plus sur la façon de rechercher des instances en fonction de balises, consultez Comment rechercher des instances à l'aide de valeurs de balises et de propriétés.

> **Remarque**
>
> Vous pouvez ajouter ultérieurement de nouvelles balises ou supprimer des balises existantes. Il n'y a aucune restriction quant au nombre de balises que vous créez.

Procédure de recherche d'instances à l'aide de valeurs de balises et de propriétés

February 1, 2024

Dans certains cas, Citrix Application Delivery Management (ADM) gère de nombreuses instances Citrix ADC. En tant qu'administrateur, vous pouvez avoir la possibilité de rechercher dans l'inventaire des instances en fonction de certains paramètres. Citrix ADM offre désormais une fonctionnalité de recherche améliorée pour rechercher un sous-ensemble d'instances Citrix ADC en fonction des paramètres que vous définissez dans le champ de recherche. Vous pouvez rechercher les instances en fonction de deux critères : les balises et les propriétés.

- **Étiquettes**. Les balises sont des termes ou des mots clés que vous pouvez attribuer à une instance Citrix ADC pour ajouter une description supplémentaire sur l'instance Citrix ADC. Vous

pouvez désormais associer vos instances Citrix ADC à des balises. Ces balises peuvent être utilisées pour mieux identifier et rechercher sur les instances Citrix ADC.

- **Propriétés**. Chaque instance Citrix ADC ajoutée dans Citrix ADM a quelques paramètres ou propriétés par défaut associés à cette instance. Par exemple, chaque instance a son propre nom d'hôte, adresse IP, version, ID hôte, ID de modèle matériel, etc. Vous pouvez rechercher des instances en spécifiant des valeurs pour n'importe laquelle de ces propriétés.

Par exemple, imaginez une situation dans laquelle vous souhaitez connaître la liste des instances Citrix ADC qui sont sur la version 12.0 et qui sont dans l'état UP. Ici, la version et l'état de l'instance sont définis par les propriétés par défaut.

Outre la version 12.0 et l'état UP des instances, vous pouvez également rechercher les instances qui vous appartiennent. Vous pouvez créer une balise « Propriétaire » et attribuer une valeur « David T » à cette balise. Pour plus d'informations sur la façon de créer et d'attribuer des balises, consultez Comment créer des balises et attribuer à des instances.

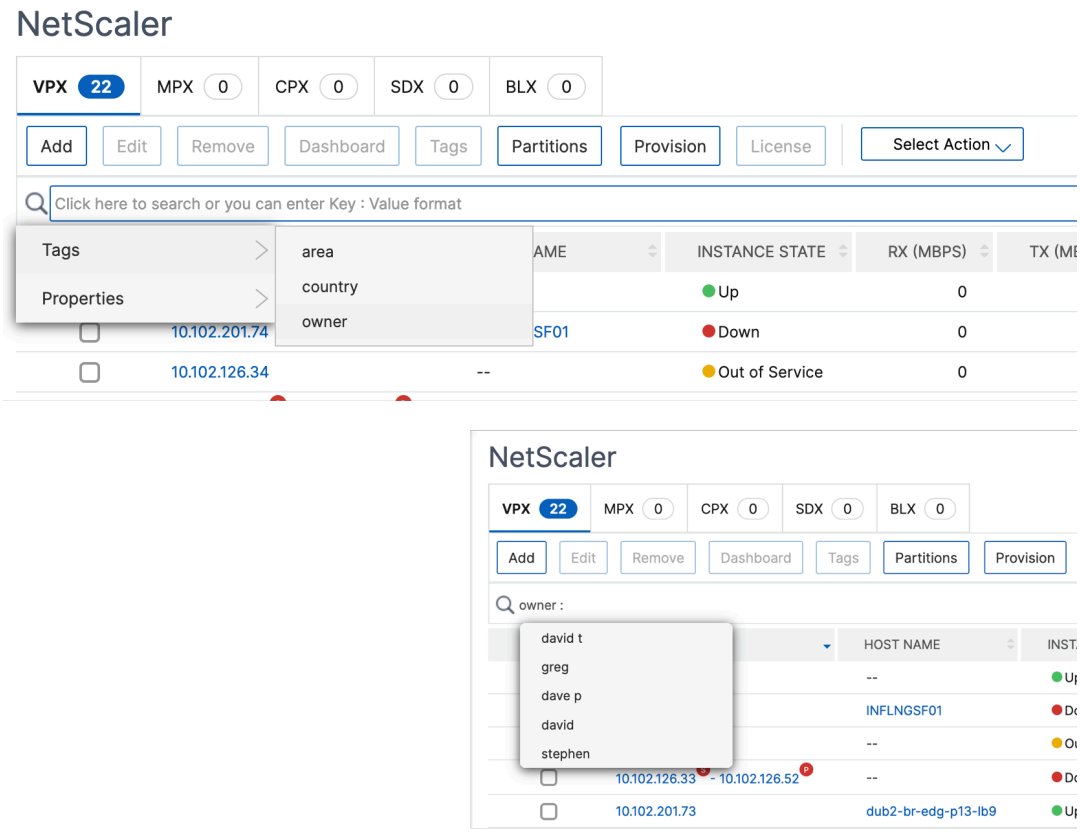
Vous pouvez utiliser une combinaison de balises et de propriétés pour créer vos propres critères de recherche.

Pour rechercher des instances Citrix ADC VPX

1. Dans Citrix ADM, accédez à l'onglet **Réseaux** > **Instances** > **Citrix ADC** > **VPX**.
2. Cliquez sur le champ de recherche. Vous pouvez créer une expression de recherche en utilisant des balises ou des propriétés ou en combinant les deux.

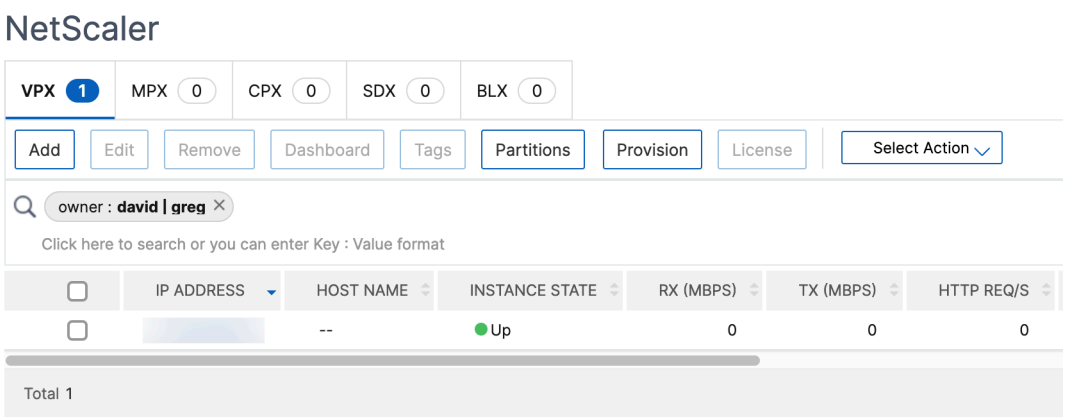
   Les exemples suivants montrent comment utiliser efficacement l'expression de recherche pour rechercher l'instance.

   a) Sélectionnez l'option **Balises** et sélectionnez **Propriétaire**. Sélectionnez « David T. »

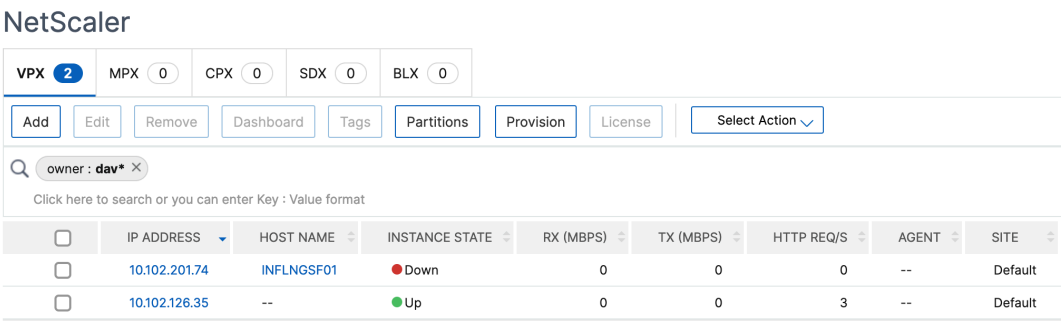


Citrix ADM prend en charge les expressions régulières et les caractères génériques dans les expressions de recherche.

b) Vous pouvez utiliser des expressions régulières pour élargir les critères de recherche. Par exemple, vous souhaitez rechercher des instances appartenant à David ou à Stephen. Dans ce cas, vous pouvez taper les valeurs en les séparant par une expression « | ».



c) Vous pouvez également utiliser des caractères génériques pour remplacer ou représenter un ou plusieurs caractères. Par exemple, vous pouvez `Dav*` taper pour rechercher toutes les instances appartenant à David T et Dave P.



> **Remarque**
>
> Pour plus d'informations sur les expressions régulières et les caractères génériques et sur leur utilisation, cliquez sur l'icône « Informations » dans la barre de recherche.

Gérer les partitions d'administration des instances Citrix ADC

February 1, 2024

Vous pouvez configurer des partitions d'administration sur vos instances de Citrix Application Delivery Controller (ADC) de sorte que différents groupes de votre organisation se voient attribuer des partitions différentes sur la même instance de Citrix ADC. Un administrateur réseau peut être affecté pour gérer plusieurs partitions sur plusieurs instances Citrix ADC.

Citrix Application Delivery Management (ADM) offre un moyen transparent de gérer toutes les partitions appartenant à un administrateur à partir d'une console unique. Vous pouvez gérer ces partitions sans perturber d'autres configurations de partitions.

Pour permettre à plusieurs utilisateurs de gérer différentes partitions d'administration, vous devez créer des groupes, puis affecter des utilisateurs et des partitions à ces groupes. Chaque utilisateur peut afficher et gérer uniquement les partitions du groupe auquel il appartient. Chaque partition d'administration est considérée comme une instance dans Citrix ADM. Lorsque vous découvrez une instance Citrix ADC, les partitions d'administration configurées sur cette instance Citrix ADC sont automatiquement ajoutées au système.

Considérez que vous avez deux instances Citrix VPX avec deux partitions configurées sur chaque instance. Par exemple, l'instance Citrix ADC 10.102.216.49 a Partition_1, Partition_2 et Partition_3, et l'instance Citrix ADC 10.102.29.120 a p1 et p2 comme illustré dans l'image suivante.

Pour afficher les partitions, accédez à**Réseaux > Instances > Citrix ADC > VPX**, puis cliquez sur **Partitions**.

Vous pouvez affecter user-p1 les partitions suivantes : 10.102.29.120-p1 et 10.102.216.49-Partition_1.

Vous pouvez également attribuer à user-p2 la gestion des partitions 10.102.29.80-p2, 10.102.216.49-Partition_2 et 10.102.216.49-Partition_3.

Ensuite, vous devez créer les deux utilisateurs, user-p1 et user-p2, et vous devez affecter les utilisateurs aux groupes que vous avez créés pour eux.

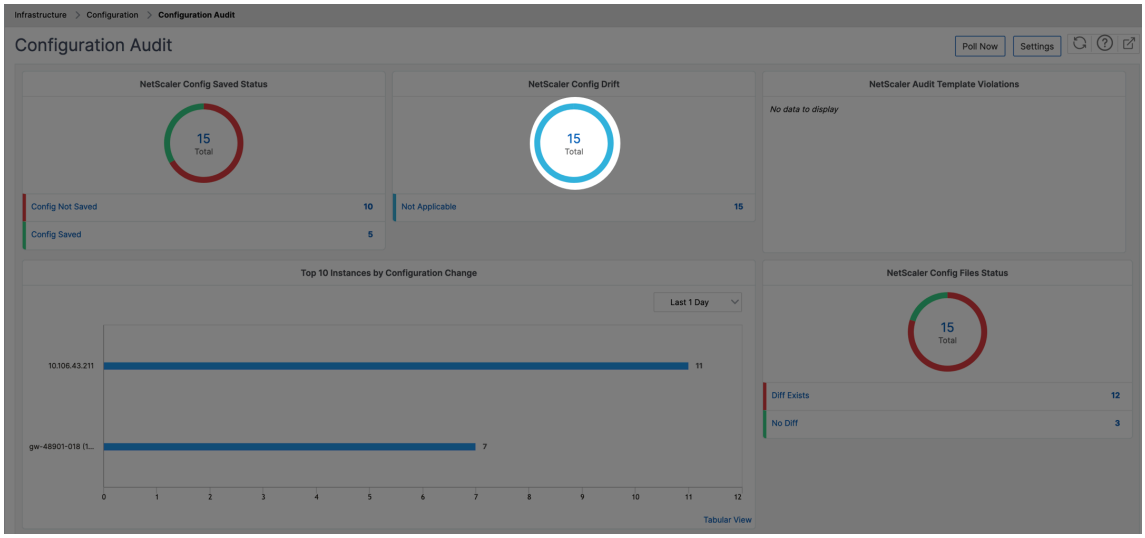
Tout d'abord, vous devez créer deux groupes avec les autorisations appropriées (par exemple : permissions admin) et inclure les instances de partition admin requises dans chaque groupe. Par exemple, créez le groupe système partition1-admin et ajoutez les partitions d'administration Citrix ADC 10.102.29.120-p1 et 10.102.216.49-Partition_1 à ce groupe. Créez également le groupe système partition2-admin et ajoutez les partitions d'administration Citrix ADC 10.102.29.120-p2, 10.102.216.49-Partition_2 et 10.102.216.49-Partition_3 et à ce groupe.

Après avoir créé la partition admin, vous pouvez également utiliser la fonction de différence d'historique des révisions et le modèle d'audit pour la fonctionnalité de partition admin à des fins d'audit

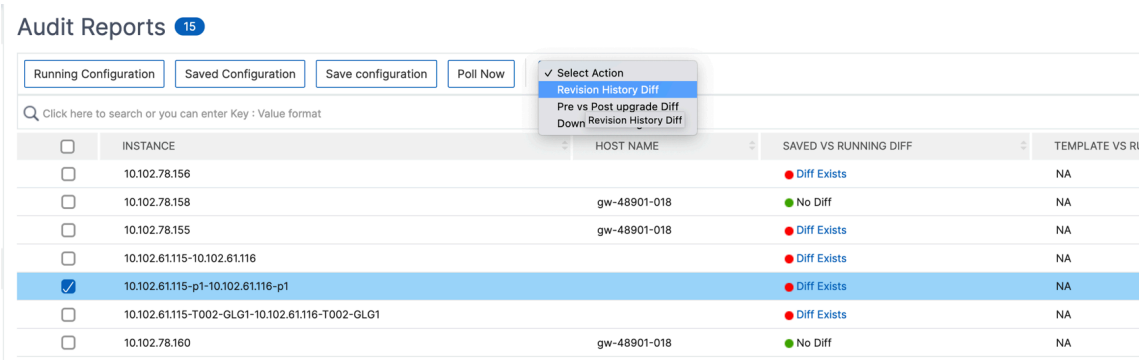
La différence d'historique des révisions pour la partition d'administration vous permet d'afficher la différence entre les cinq derniers fichiers de configuration pour une instance Citrix ADC partitionnée. Vous pouvez comparer les fichiers de configuration les uns aux autres (exemple Révision de configuration - 1 avec Révision de configuration -2) ou avec la configuration en cours d'exécution/enregistrée avec Révision de configuration. Avec les différences de configuration, les configurations de correction sont également affichées. Vous pouvez exporter toutes les commandes correctives dans votre dossier local et corriger les configurations.

Pour afficher la différence dans l'historique des révisions :

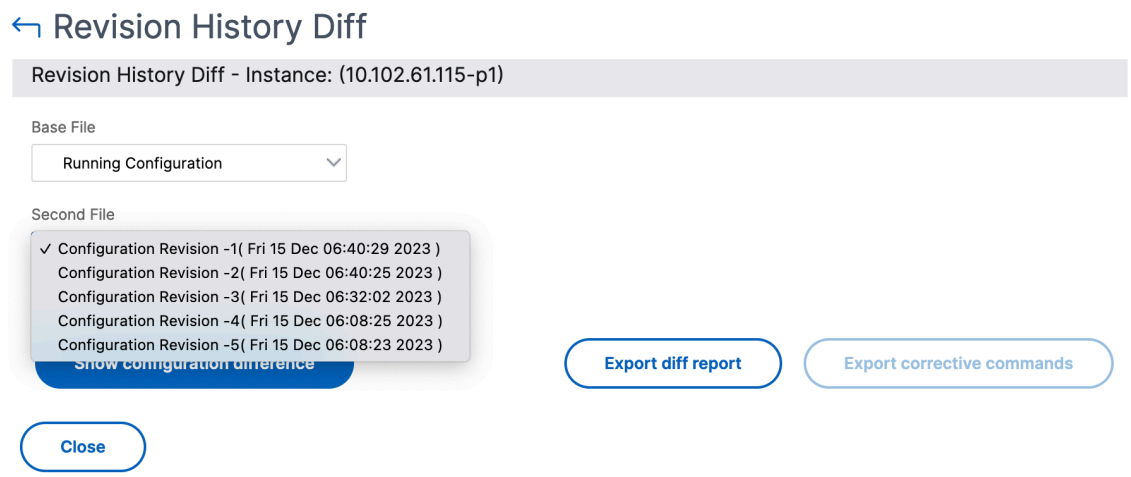
1. Accédez à **Réseaux > Audit de configuration.** Cliquez à l'intérieur du graphique en donut qui représente l'état de configuration de l'instance. Dans la page **Rapports d'audit** qui s'ouvre, cliquez sur l'instance Citrix ADC partitionnée.



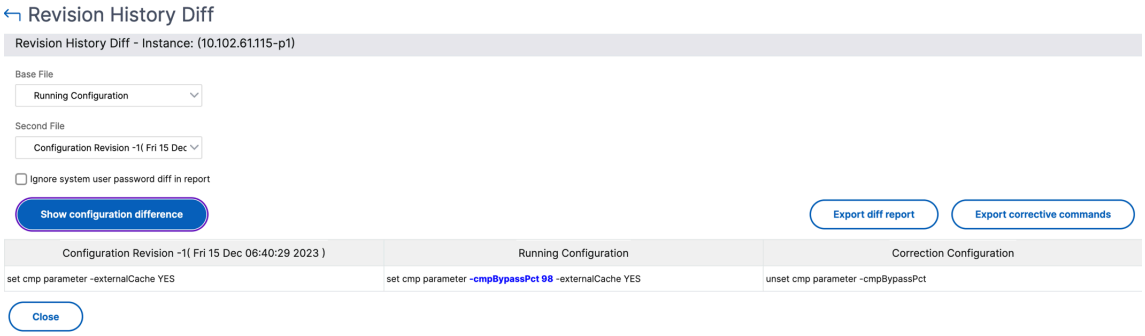
2. Dans le menu **Action**, cliquez sur **Diff Historique des révisions.**



3. Dans la page **Diff de l'historique des révisions**, sélectionnez les fichiers que vous souhaitez comparer. Par exemple, comparez la configuration enregistrée avec la révision de configuration -1, puis cliquez sur **Afficher la différence de configuration**.



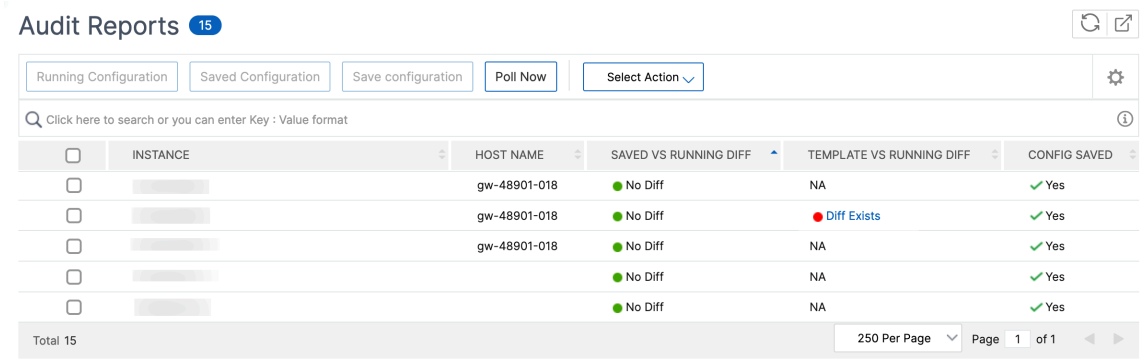
4. Vous pouvez ensuite afficher la différence entre les cinq derniers fichiers de configuration pour l'instance Citrix ADC partitionnée sélectionnée, comme indiqué ci-dessous. Vous pouvez également afficher les commandes de configuration corrective et exporter ces commandes correctives dans votre dossier local. Ces commandes correctives sont les commandes qui doivent être exécutées sur le fichier de base pour obtenir la configuration à l'état souhaité (fichier de configuration utilisé à des fins de comparaison).



Les modèles d'audit pour la partition vous permettent de créer un modèle de configuration personnalisé et de l'associer à une instance de partition. Toute variation de la configuration d'exécution de l'instance avec le modèle d'audit est affichée dans la colonne **Template vs Running diff** de la page **Rapports d'audit** . Outre les différences de configuration, les configurations de correction sont également affichées. Vous pouvez également exporter toutes les commandes correctives dans votre dossier local et corriger les configurations.

Pour afficher la différence entre le modèle et l'exécution :

1. Dans la page **Rapports d'audit**, cliquez sur l'instance Citrix ADC partitionnée.



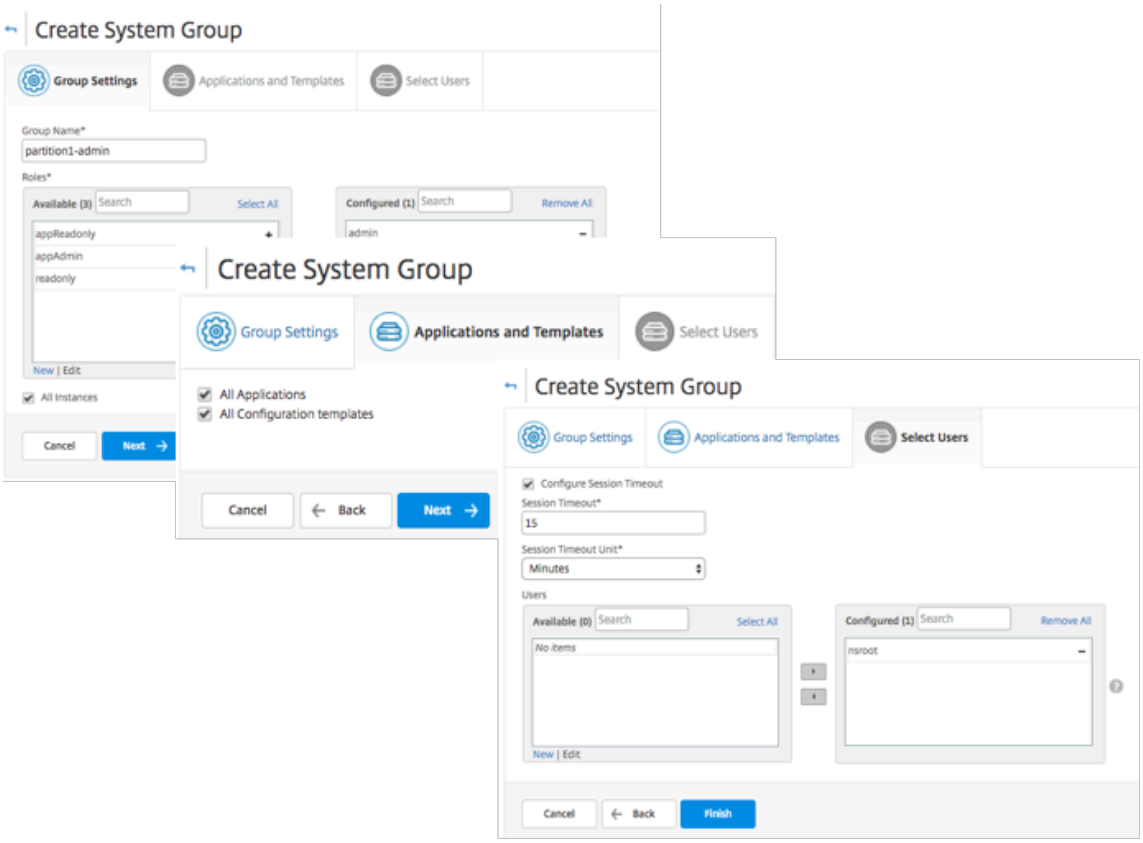
2. S'il y a une différence entre le modèle d'audit et la différence en cours d'exécution, la différence est affichée sous la forme d'un lien hypertexte. Cliquez sur le lien hypertexte pour afficher les différences s'il y en a. Avec les différences de configuration, les configurations de correction sont également affichées. Vous pouvez également exporter toutes les commandes correctives dans votre dossier local et corriger les configurations.

Pour créer des groupes :

1. Accédez à **Système > Administration des utilisateurs > Groupes**, puis cliquez sur **Ajouter**.
2. Dans la page **Créer un utilisateur système**, spécifiez les éléments suivants :
   - Onglet**Paramètres du groupe** : entrez le nom du groupe et les autorisations de rôle. Pour autoriser l'accès à des instances spécifiques, désactivez la case à cocher**Toutes les instances** , puis choisissez vos instances sur la page **Sélectionner les instances** .

- **Onglet Applications et modèles** : vous pouvez choisir d'utiliser ce groupe dans toutes les applications et tous les modèles de configuration.
- **Onglet Sélectionner les utilisateurs : sélectionnez les utilisateurs que vous souhaitez ajouter à ce groupe.** Vous pouvez cliquer sur le lien **Nouveau** dans le tableau **Disponible** pour créer de nouveaux utilisateurs. Vous pouvez également configurer le délai d'expiration de la session, dans lequel vous pouvez configurer la période pendant laquelle un utilisateur peut rester actif.

3. Cliquez sur **Terminer**.



Pour créer des utilisateurs :

1. Accédez à**Système > Administration des utilisateurs > Utilisateurs**, puis cliquez sur **Ajouter**.
2. Dans la page**Créer un utilisateur système**, spécifiez le nom d'utilisateur et le mot de passe. Vous pouvez éventuellement activer l'authentification externe et configurer le délai d'expiration de la session.
3. Attribuez l'utilisateur à un groupe en ajoutant le nom du groupe de la liste**Disponible** à la liste**configurée** .
4. Cliquez sur**Créer**.

Maintenant, déconnectez-vous et ouvrez une session avec les informations d'identification de l'utilisateur p1. Vous pouvez afficher et gérer uniquement les partitions d'administration qui vous sont attribuées pour gérer et surveiller.

Créer une paire haute disponibilité Citrix ADC

January 23, 2024

Une paire Citrix ADC High Availability (HA) peut assurer un fonctionnement ininterrompu en cas de panne ou de panne réseau. Vous pouvez créer une paire HA d'instances ADC à l'aide de Citrix ADM. Pour de plus amples informations, consultez la section Haute disponibilité Citrix ADC.

Pour créer une paire HA d'instances ADC dans Citrix ADM, procédez comme suit :

1. Accédez à **Réseaux > Instances > Citrix ADC**.
2. Sélectionnez une instance ADC dans la liste avec laquelle vous souhaitez créer une paire HA.

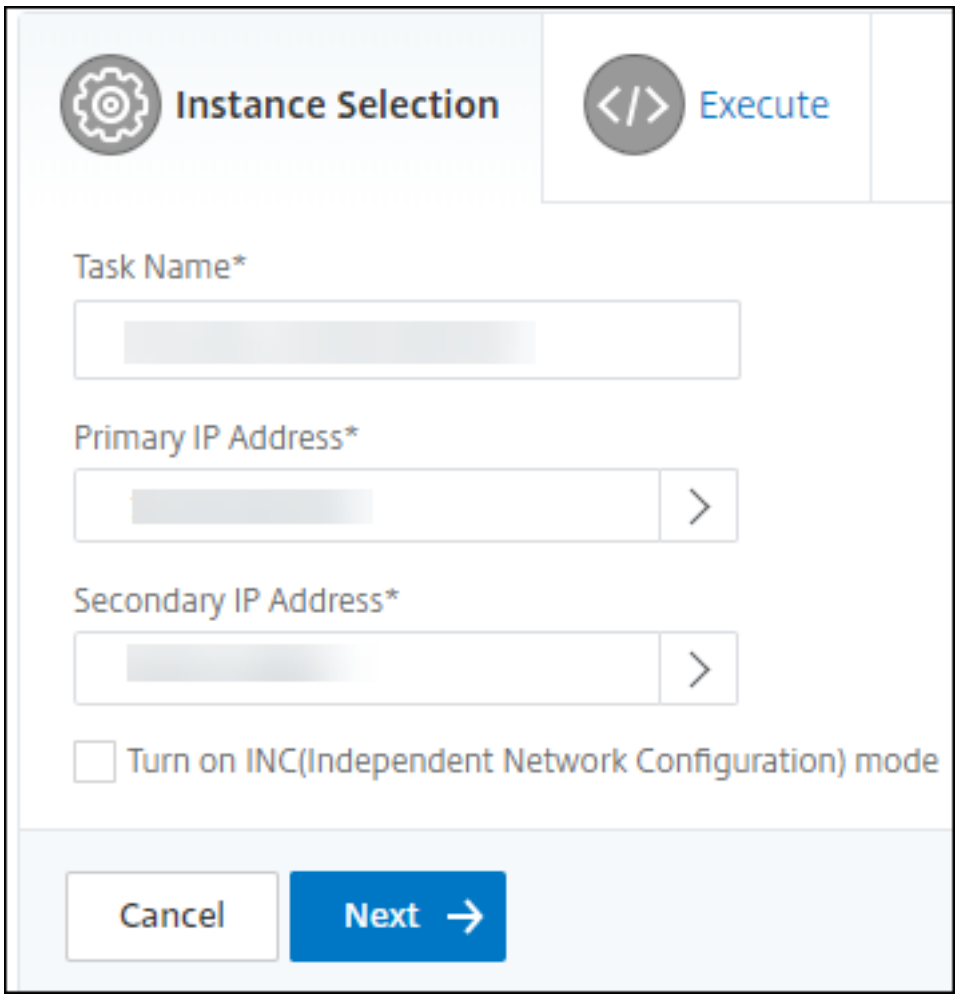
   L'instance sélectionnée devient une instance principale de la paire HA.
3. Cliquez sur Sélectionner **une action > Créer une paire HA**.
4. Dans **Sélection d'instance**, effectuez les opérations suivantes :

   a) Dans **Adresse IP secondaire**, cliquez pour sélectionner une instance secondaire.

   b) Sélectionnez une instance ADC que vous souhaitez configurer comme instance secondaire dans la paire HA.

   c) Facultatif, sélectionnez **Activer le mode INC (Independent Network Configuration)** si vous avez les instances de la paire HA dans deux sous-réseaux.

   d) Cliquez sur **Suivant**.



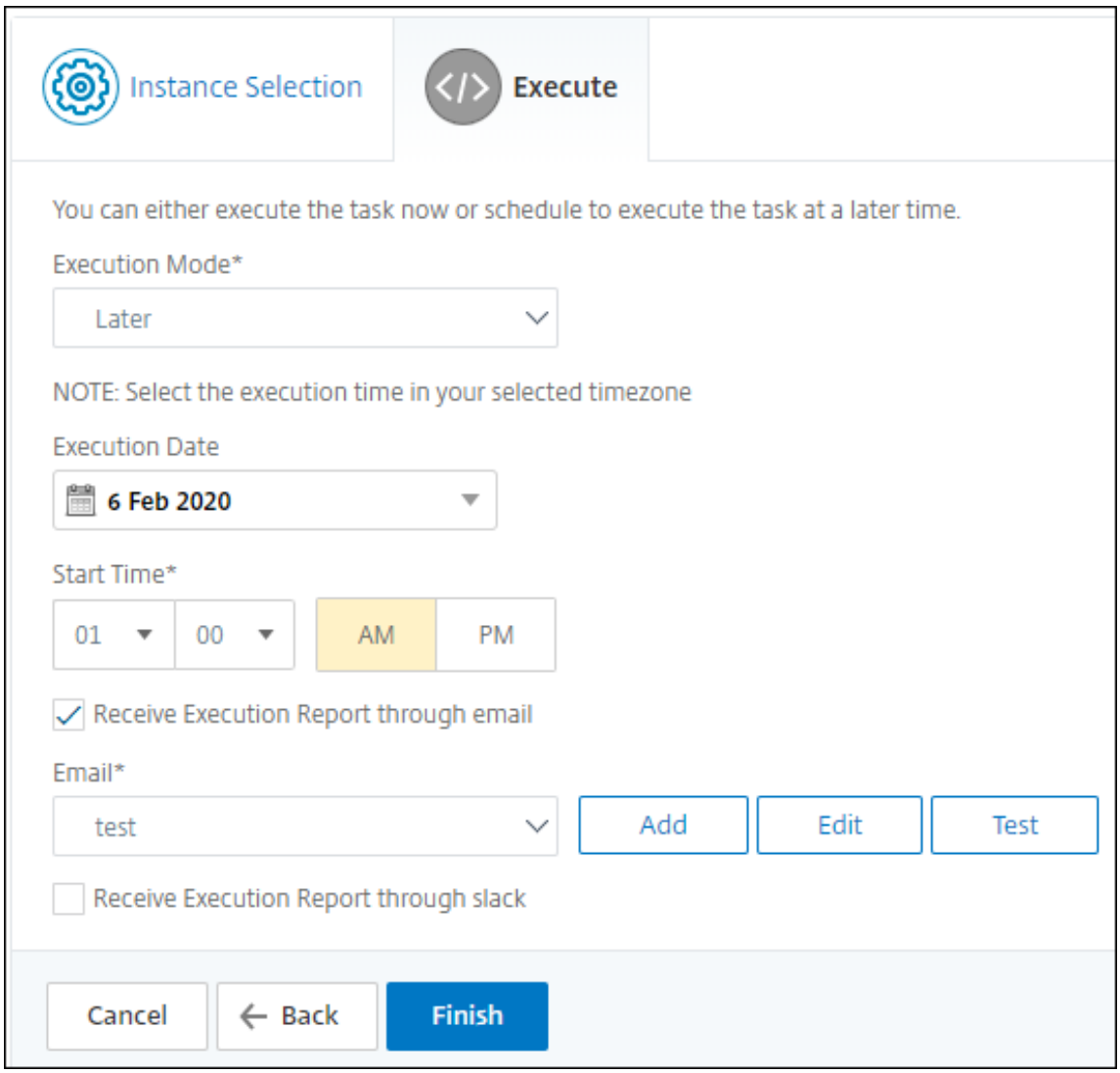
5. Dans **Execute**, vous pouvez décider de créer une paire HA maintenant ou ultérieurement.

   a) Dans **Mode d'exécution**, sélectionnez l'un des modes d'exécution suivants :

      - **Maintenant** - Sélectionnez cette option pour créer une paire HA maintenant.
      - **Plus tard** - Sélectionnez cette option pour créer une paire HA à une date et à une heure spécifiques.

   b) Si vous avez sélectionné **Plus tard** dans la liste **Mode d'exécution**, sélectionnez **Date d'exécution** et **Heure de début** lorsque vous souhaitez exécuter cette tâche.

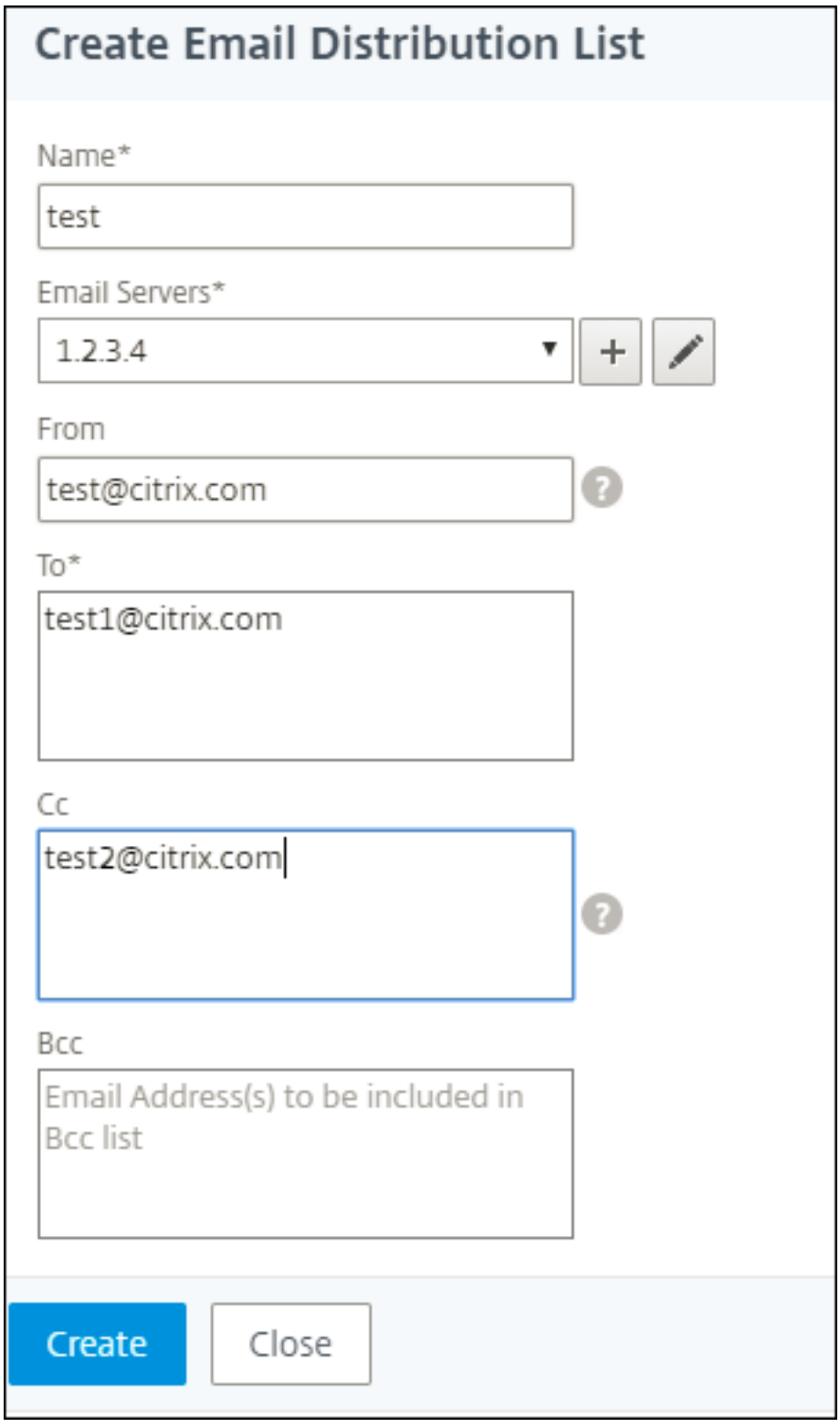
      > **Remarque**
      >
      > L'heure d'exécution s'affiche dans le fuseau horaire défini dans Citrix ADM.



Vous pouvez recevoir un rapport d'exécution de cette tâche via les éléments suivants :

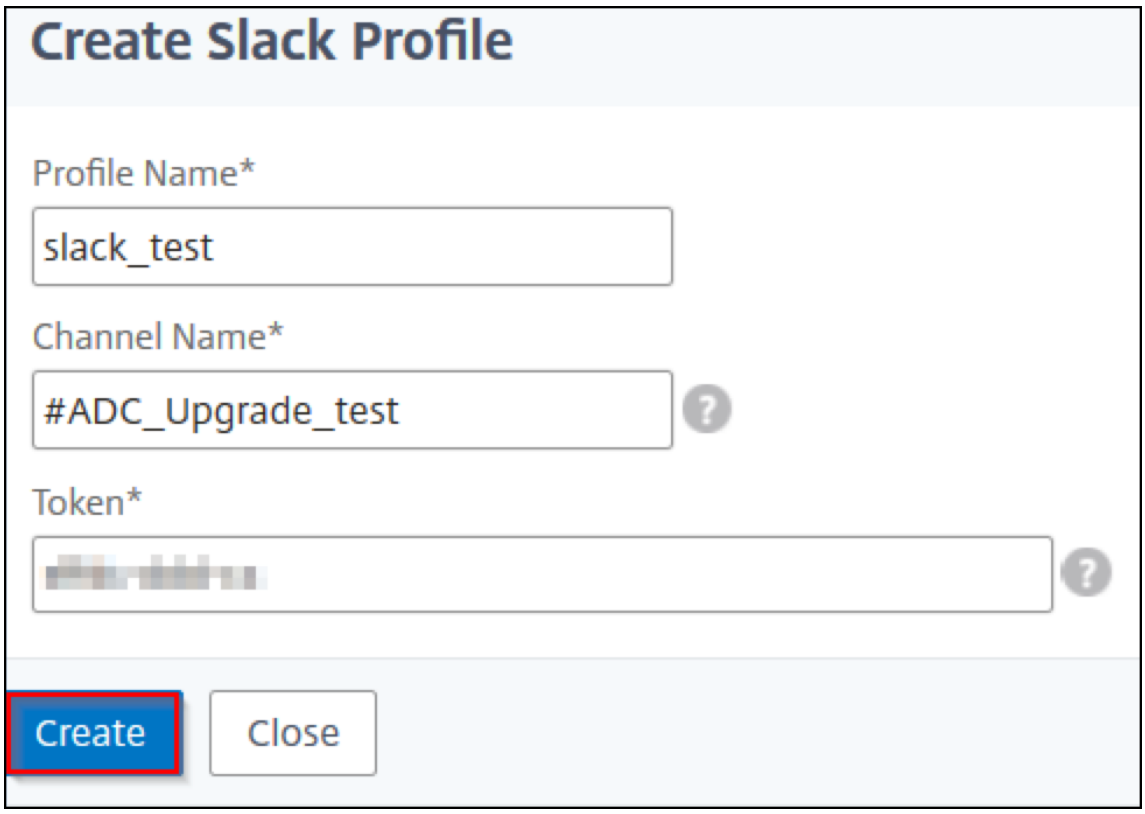
- **Courrier électronique** : sélectionnez la distribution d'e-mails dans la liste.

  Pour ajouter une liste de distribution, cliquez sur **Ajouter**. Spécifiez les paramètres requis pour ajouter la liste de distribution et cliquez sur **Créer**.



- **Slack** : sélectionnez le profil Slack dans la liste.

  Pour ajouter un profil Slack, cliquez sur **Ajouter**. Spécifiez **le nom du profil**, le **nom de la chaîne**et le **jeton**, puis cliquez sur **Créer**.



Sauvegarder et restaurer des instances Citrix ADC

February 1, 2024

Vous pouvez sauvegarder l'état actuel d'une instance Citrix ADC et utiliser ultérieurement les fichiers sauvegardés pour la restaurer dans le même état. Sauvegardez toujours une instance avant de la mettre à niveau ou pour des raisons de précaution. Une sauvegarde d'un système stable vous permet de le restaurer à un point stable s'il devient instable.

Il existe plusieurs façons d'effectuer des sauvegardes et des restaurations sur une instance Citrix ADC. Vous pouvez sauvegarder et restaurer manuellement les configurations Citrix ADC à l'aide de l'interface graphique et de l'interface de ligne de commande. Vous pouvez également utiliser Citrix ADM pour effectuer des sauvegardes automatiques et des restaurations manuelles.

Citrix ADM sauvegarde l'état actuel de vos instances Citrix ADC gérées à l'aide d'appels NITRO et des protocoles Secure Shell (SSH) et Secure Copy (SCP).

Citrix ADM crée une sauvegarde complète et restaure les types d'instance Citrix ADC suivants :

- Citrix SDX
- Citrix VPX

- Citrix MPX
- Citrix BLX

Pour plus d'informations, consultez Sauvegarder et restaurer une instance ADC .

> **Remarque**
>
> - Assurez-vous que le profil Citrix ADM dispose de l'accès administrateur à la sauvegarde et à la restauration des instances ADC.
> - À partir de Citrix ADM, vous ne pouvez pas effectuer l'opération de sauvegarde et de restauration sur un cluster Citrix ADC.
> - Vous ne pouvez pas utiliser le fichier de sauvegarde provenant d'une instance pour restaurer une autre instance.

Les fichiers sauvegardés sont stockés en tant que fichier TAR compressé dans le répertoire suivant :

```
/var/mps/tenants/root/device_backup/
<!--NeedCopy-->
```

Pour éviter les problèmes dus à la non-disponibilité de l'espace disque, vous pouvez enregistrer un maximum de 50 fichiers de sauvegarde par instance ADC dans ce répertoire.

Pour sauvegarder et restaurer des instances Citrix ADC, vous devez d'abord configurer les paramètres de sauvegarde sur Citrix ADM. Après avoir configuré les paramètres, vous pouvez sélectionner une ou plusieurs instances Citrix ADC et créer une sauvegarde des fichiers de configuration dans ces instances. Si nécessaire, vous pouvez également restaurer les instances de Citrix ADC à l'aide de ces fichiers sauvegardés.

Configurer les paramètres de sauvegarde d'instance

La page **Paramètres de sauvegarde d'instance** vous permet de configurer les paramètres sur Citrix ADM pour sauvegarder une instance Citrix ADC sélectionnée ou plusieurs instances :

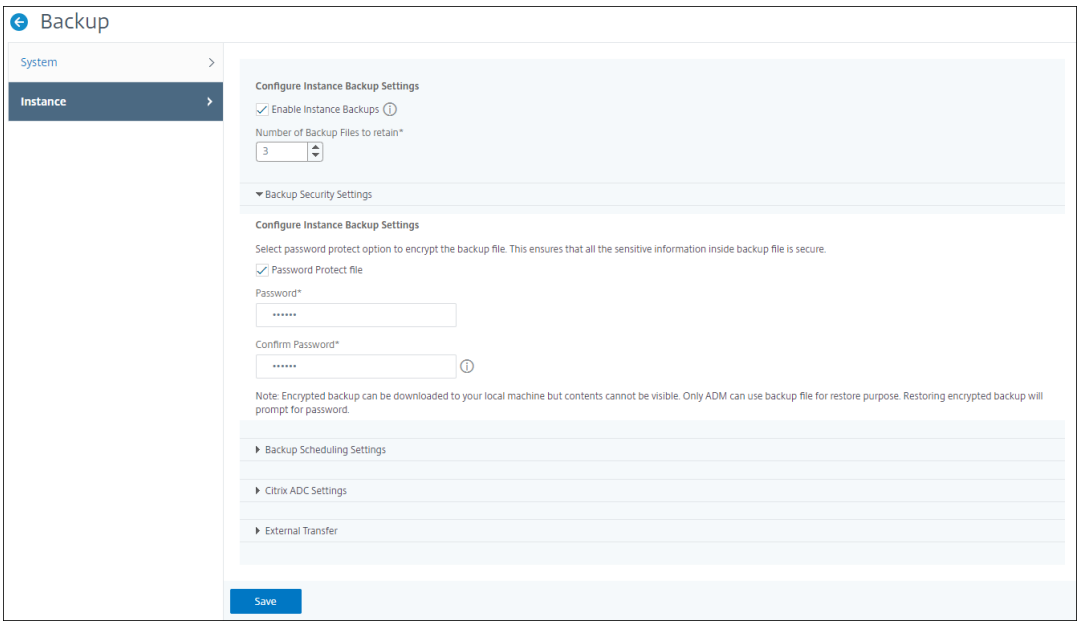
1. Dans Citrix ADM, accédez à **Système** > **Administration**.
2. Dans **Sauvegarde**, sélectionnez **Configurer la sauvegarde du système et de l'instance**.
3. Sélectionnez **Instance** et spécifiez les éléments suivants :
    - **Activer les sauvegardes d'instance** : par défaut, Citrix ADM est activé pour effectuer des sauvegardes d'instances Citrix ADC. Désactivez cette option si vous ne souhaitez pas créer de fichiers de sauvegarde pour les instances.

- **Fichier de protection par mot**de passe : (facultatif) Sélectionnez l'option de protection par mot de passe pour chiffrer le fichier de sauvegarde. Le chiffrement du fichier de sauvegarde garantit la sécurité de toutes les informations sensibles contenues dans le fichier de sauvegarde.

  > **Remarque**
  >
  > Vous pouvez télécharger le fichier de sauvegarde chiffré sur votre ordinateur local, mais vous ne pouvez pas ouvrir le fichier avec l'interface graphique Citrix ADM ni avec un éditeur de texte. Vous êtes invité à fournir le mot de passe lors de la restauration du fichier de sauvegarde chiffré. Vous pouvez toutefois ouvrir un fichier de sauvegarde non chiffré sur votre système.

- **Nombre de fichiers de sauvegarde à conserver** : spécifiez le nombre de fichiers de sauvegarde à conserver dans Citrix ADM. Vous pouvez conserver jusqu'à 50 fichiers de sauvegarde par instance ADC. La valeur par défaut est trois fichiers de sauvegarde.

  > **Remarque**
  >
  > Chaque fichier de sauvegarde tient compte de certaines exigences en matière de stockage. Citrix vous recommande de stocker un nombre optimal de fichiers de sauvegarde Citrix ADC sur Citrix ADM en fonction de vos besoins.

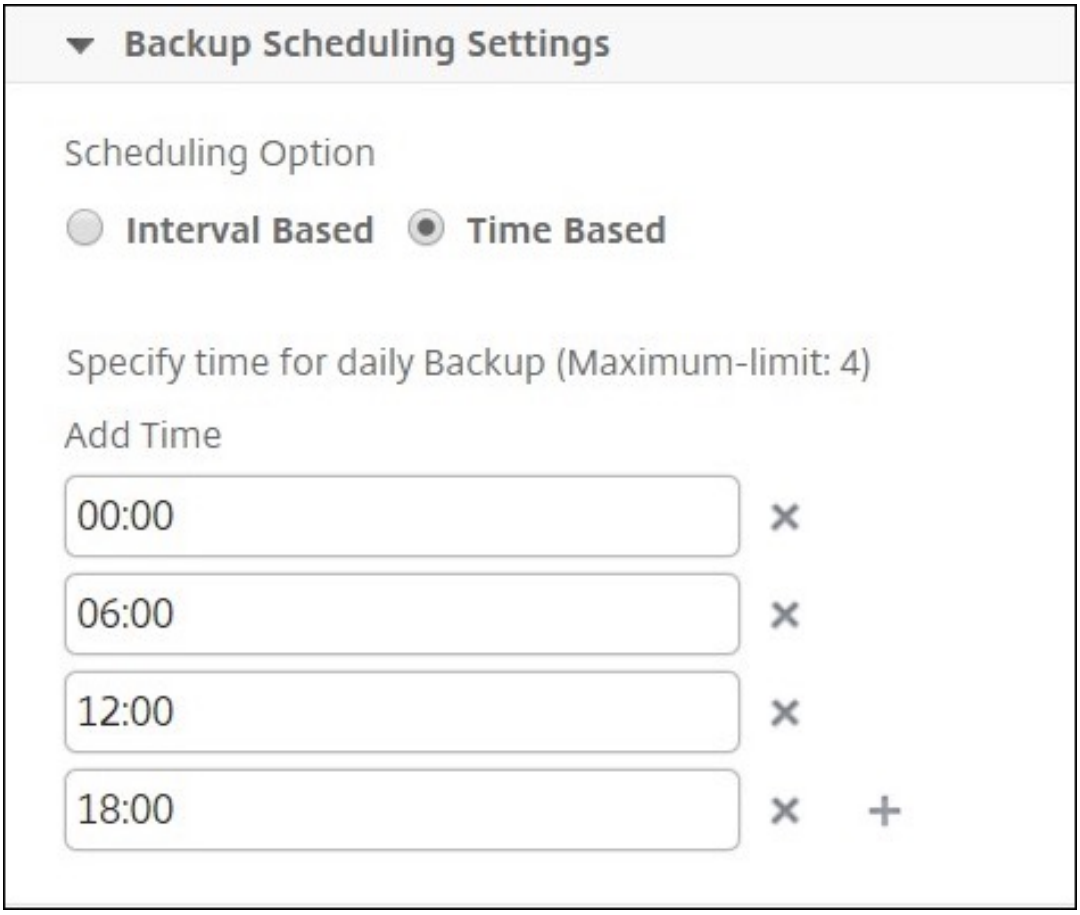


- **Paramètres de planification des sauvegardes** : (facultatif) Deux options sont disponibles pour créer des fichiers de sauvegarde, mais vous ne pouvez utiliser qu'une seule option à la fois :

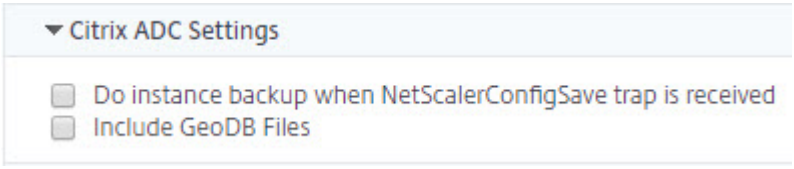
  a) L'option de planification de sauvegarde par défaut est « basée sur l'intervalle. » Un

fichier de sauvegarde est créé dans Citrix ADM après l'expiration de l'intervalle spécifié. L'intervalle de sauvegarde par défaut est de 12 heures.

b) Vous pouvez également modifier le type de sauvegardes planifiées en fonction du temps. Dans cette option, spécifiez l'heure au format `hours:minutes` pour sauvegarder des instances à l'heure spécifiée. Citrix ADM permet à un maximum de quatre sauvegardes quotidiennes sur les instances.



- **Paramètres de Citrix ADC** : (facultatif) Par défaut, Citrix ADM ne crée pas de fichier de sauvegarde lorsqu'il reçoit l'interruption « NetScalerConfigSave ». Toutefois, vous pouvez activer l'option pour créer un fichier de sauvegarde chaque fois qu'une instance Citrix ADC envoie un piège « NetScalerConfigSave » à Citrix ADM. Une instance Citrix ADC envoie « NetScalerConfigSave » chaque fois que la configuration sur l'instance est enregistrée.
- **Fichiers de géodatabase** : (facultatif) Par défaut, Citrix ADM ne sauvegarde pas les fichiers de géodatabase. Vous pouvez également activer l'option pour créer une sauvegarde de ces fichiers.



- **Transfert externe :**(facultatif) Citrix ADM vous permet de transférer les fichiers de sauvegarde d'instance Citrix ADC vers un emplacement externe :

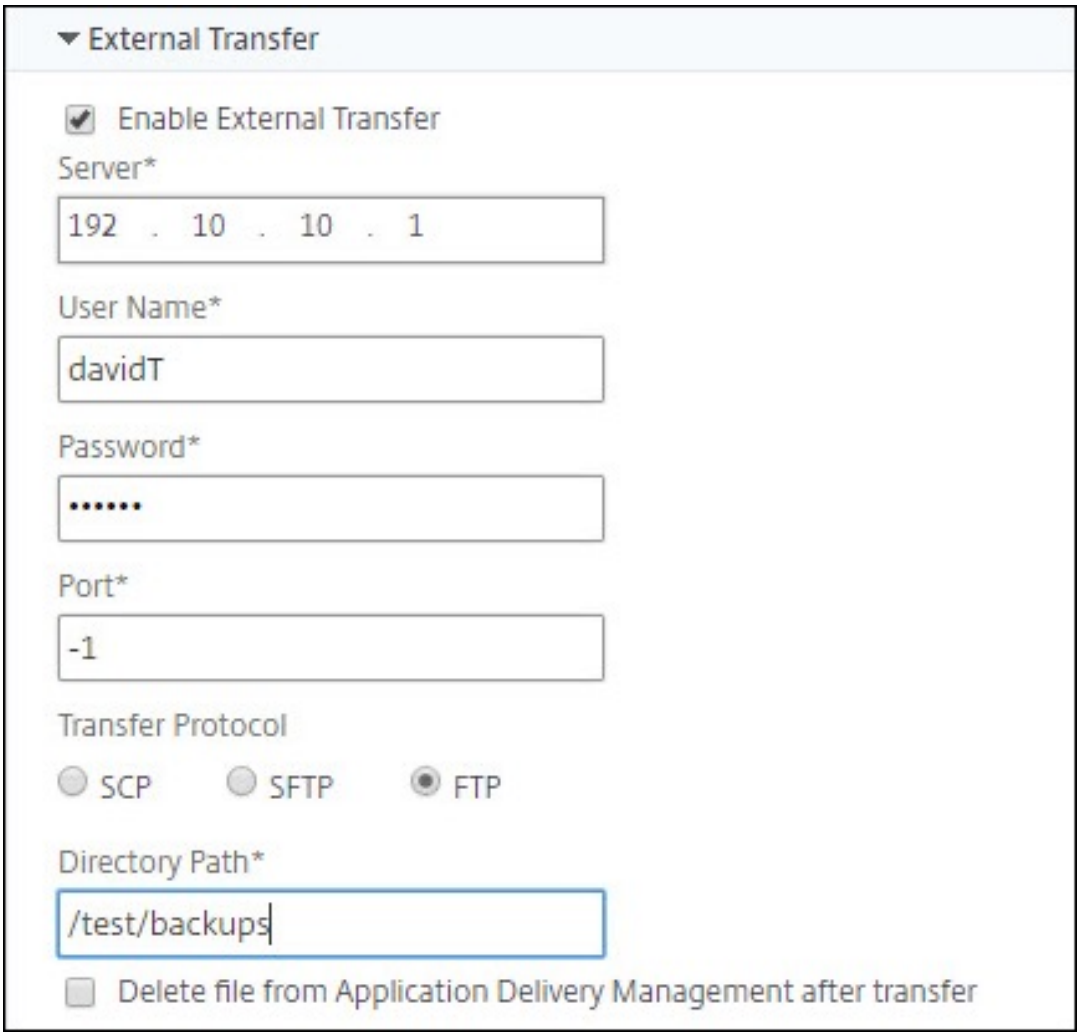
  a) Spécifiez l'adresse IP de l'emplacement.

  b) Spécifiez le nom d'utilisateur et le mot de passe du serveur externe vers lequel vous souhaitez transférer les fichiers de sauvegarde.

  c) Spécifiez le protocole de transfert et le numéro de port.

  d) Vous pouvez spécifier le chemin d'accès au répertoire où le fichier doit être stocké.

  e) Facultatif, vous pouvez également supprimer le fichier de sauvegarde de Citrix ADM après l'avoir transféré sur le serveur externe.



> **Remarque**
>
> Citrix ADM envoie un piège SNMP ou une notification Syslog à lui-même en cas d'échec de sauvegarde pour l'une des instances Citrix ADC sélectionnées.

Créer une sauvegarde pour une instance Citrix ADC sélectionnée à l'aide de Citrix ADM

Effectuez cette tâche si vous souhaitez sauvegarder une ou plusieurs instances Citrix ADC sélectionnées :

1. Dans Citrix ADM, accédez à**Réseaux** >**Instances**. Sous**Instances**, sélectionnez le type d'instances (Citrix VPX, par exemple) à afficher à l'écran.
2. Sélectionnez l'instance à sauvegarder.
    - Pour les instances MPX, VPX et BLX, sélectionnez **Sauvegarder/Restaurer** dans la liste **Sélectionner une action** .
    - Pour une instance SDX, cliquez sur **Sauvegarde/Restaurer**.
3. Dans la page **Fichiers de sauvegarde**, cliquez sur **Sauvegarder**.
4. Vous pouvez spécifier s'il faut chiffrer votre fichier de sauvegarde pour plus de sécurité. Vous pouvez entrer votre mot de passe ou utiliser le mot de passe global que vous avez précédemment spécifié sur la page Paramètres de sauvegarde d'instance.
5. Cliquez sur **Continuer**.

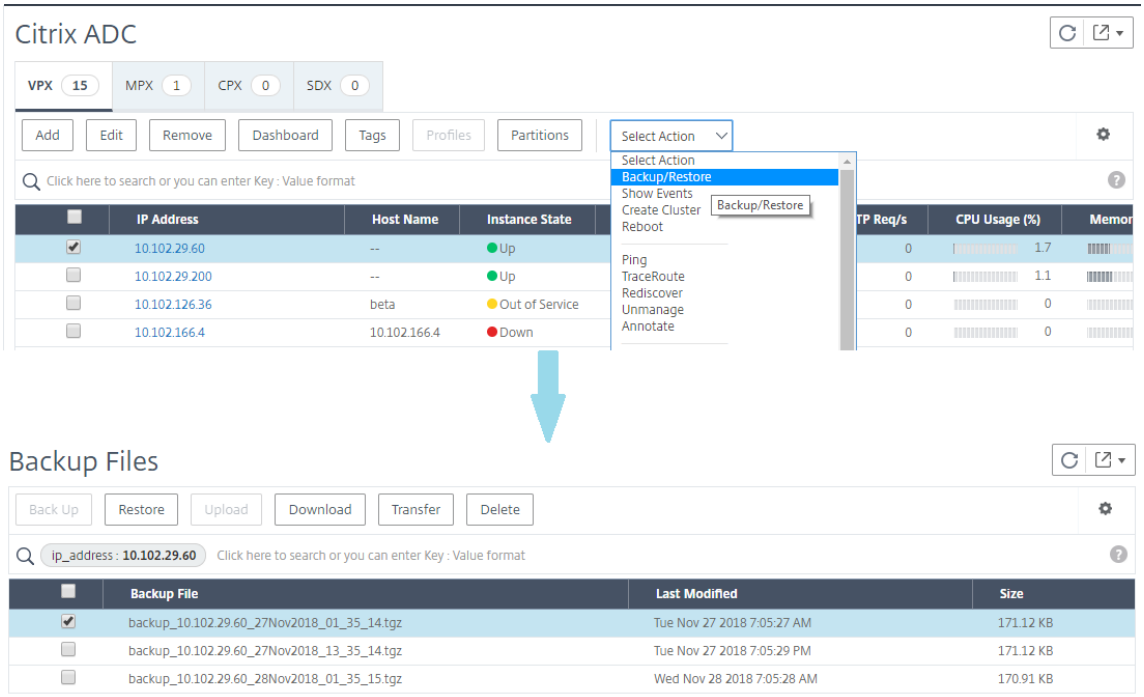
Restaurer une instance Citrix ADC à l'aide de Citrix ADM

> Remarque :
>
> Si vous avez des instances Citrix ADC dans une paire HA, vous devez prendre en compte les points suivants :
>
> - Restaurez la même instance à partir de laquelle le fichier de sauvegarde a été créé. Par exemple, considérons un scénario selon lequel une sauvegarde a été effectuée à partir de l'instance principale de la paire HA. Au cours du processus de restauration, assurez-vous de restaurer la même instance, même si elle n'est plus l'instance principale.
> - Lorsque vous lancez le processus de restauration sur l'instance ADC principale, vous ne pouvez pas accéder à l'instance principale et l'instance secondaire est remplacée par **STAYSECONDARY**. Une fois le processus de restauration terminé sur l'instance principale, l'instance ADC secondaire passe du mode **STAYSECONDARY** au mode **ENABLED** et fait à nouveau partie de la paire HA. Vous pouvez vous attendre à un temps d'arrêt possible sur l'instance

> principale jusqu'à ce que le processus de restauration soit terminé.

Effectuez cette tâche pour restaurer une instance Citrix ADC à l'aide du fichier de sauvegarde que vous avez créé précédemment :

1. Accédez à**Réseaux** >**Instances**, sélectionnez l'instance à restaurer, puis cliquez sur**Afficher la sauvegarde**.
2. Dans la page**Fichiers de sauvegarde**, sélectionnez le fichier de sauvegarde contenant les paramètres à restaurer, puis cliquez sur**Restaurer**.



Restaurer une appliance Citrix ADC SDX à l'aide de Citrix ADM

Dans Citrix ADM, la sauvegarde de l'appliance Citrix ADC SDX comprend les éléments suivants :

- Instances Citrix ADC hébergées sur l'appliance
- Certificats et clés SSL SVM
- Paramètres d'élagage de l'instance (au format XML)
- Paramètres de sauvegarde de l'instance (au format XML)
- Paramètres du sondage sur les certificats SSL (au format XML)
- Fichier db SVM
- Fichiers de configuration Citrix ADC des appareils présents sur SDX
- Images de génération Citrix ADC
- Images Citrix ADC XVA, ces images sont stockées à l'emplacement suivant : `/var/mps/sdx_images/`

- Image d'ensemble SDX unique (SVM+XS)
- Images d'instances tierces (si provisionnées)

Restaurez votre appliance Citrix ADC SDX à la configuration disponible dans le fichier de sauvegarde. Lors de la restauration de l'appliance, l'intégralité de la configuration actuelle est supprimée.

Si vous restaurez l'appliance Citrix ADC SDX à l'aide d'une sauvegarde d'un autre dispositif Citrix ADC SDX, assurez-vous d'ajouter les licences et configurez les paramètres réseau du service de gestion de l'appliance pour qu'ils correspondent aux paramètres du fichier de sauvegarde avant de démarrer le processus de restauration.

Avant de restaurer l'appliance SDX, assurez-vous que la variante de l'appliance SDX sauvegardée est la même que l'appliance. Vous ne pouvez pas restaurer à partir d'une variante de plate-forme différente.

> **Remarque**
>
> Avant de restaurer une appliance SDX RMA, assurez-vous que la version sauvegardée est identique ou supérieure à la version RMA.

Pour restaurer l'appliance SDX à partir du fichier sauvegardé :

1. Dans l'interface utilisateur graphique Citrix ADM, accédez à **Réseaux > Instances > Citrix ADC**.
2. Cliquez sur **Sauvegarde/Restaurer**.
3. Sélectionnez le fichier de sauvegarde de la même instance que vous souhaitez restaurer.
4. Cliquez sur **Reconditionner la sauvegarde**.

   Lorsque l'appliance SDX est sauvegardée, les fichiers et les images XVA sont stockés séparément pour économiser la bande passante réseau et l'espace disque. Par conséquent, vous devez reconditionner le fichier sauvegardé avant de restaurer l'appliance SDX.

   Lorsque vous reconditionnez le fichier de sauvegarde, il inclut tous les fichiers sauvegardés ensemble pour restaurer l'appliance SDX. Le fichier de sauvegarde reconditionné garantit la restauration réussie de l'appliance SDX.
5. Sélectionnez le fichier de sauvegarde qui est réemballé et cliquez sur **Restaurer**.

Forcer un basculement sur incident à l'instance secondaire Citrix ADC

February 1, 2024

Vous pouvez forcer un basculement si, par exemple, vous devez remplacer ou mettre à niveau l'instance principale Citrix Application Delivery Controller (ADC). Vous pouvez forcer le basculement à partir de l'instance principale ou secondaire. Lorsque vous forcez un basculement sur l'instance principale, la principale devient la secondaire et la secondaire devient la principale. Le basculement forcé n'est possible que lorsque l'instance principale peut déterminer que l'instance secondaire est active.

Un basculement forcé n'est ni propagé ni synchronisé. Pour consulter l'état de la synchronisation après un basculement forcé, vous pouvez consulter l'état de l'instance.

Un basculement forcé échoue dans l'une des circonstances suivantes :

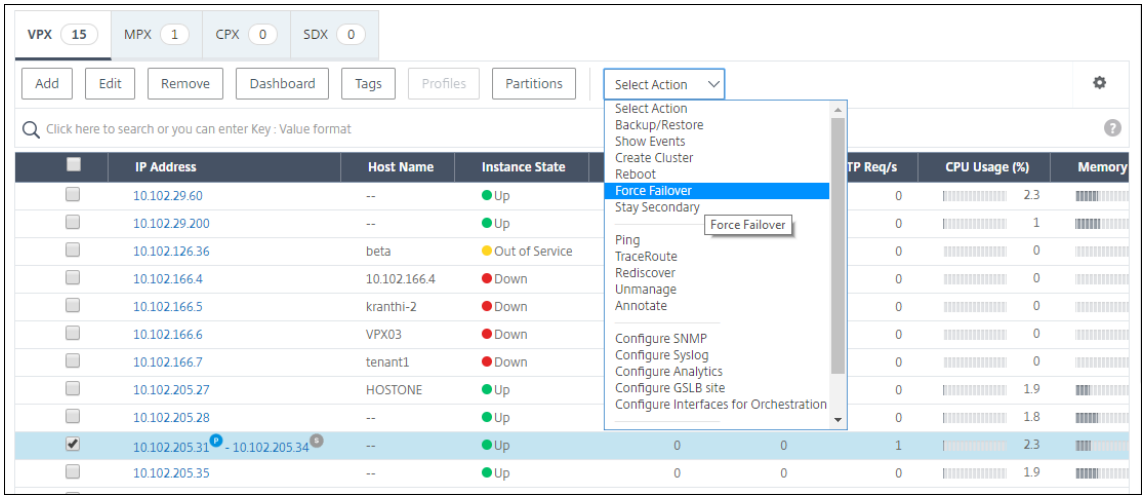
- Vous forcez le basculement sur un système autonome.
- L'instance secondaire est désactivée ou inactive. Si l'instance secondaire est inactive, vous devez attendre que son état soit activé pour forcer un basculement.
- L'instance secondaire est configurée pour rester secondaire.

L'instance Citrix ADC affiche un message d'avertissement si elle détecte un problème potentiel lorsque vous exécutez la commande force failover. Le message inclut les informations qui ont déclenché l'avertissement et demande une confirmation avant de continuer.

Vous pouvez forcer un basculement sur une instance principale ou secondaire.

Pour forcer un basculement sur incident vers l'instance Citrix ADC secondaire à l'aide de Citrix ADM :

1. Dans Citrix Application Delivery Management (ADM), accédez à **Réseaux > Instances > Citrix ADC > onglet VPX**, puis sélectionnez une instance.
2. Sélectionnez les instances d'une configuration HA à partir des instances répertoriées sous le type d'instance sélectionné.
3. Dans le menu **Action**, sélectionnez **Force Failover.**
4. Cliquez sur **Oui** pour confirmer l'action de basculement forcé.



Forcer une instance Citrix ADC secondaire à rester secondaire

February 1, 2024

Dans une configuration HA, le nœud secondaire peut être forcé de rester secondaire quel que soit l'état du nœud principal.

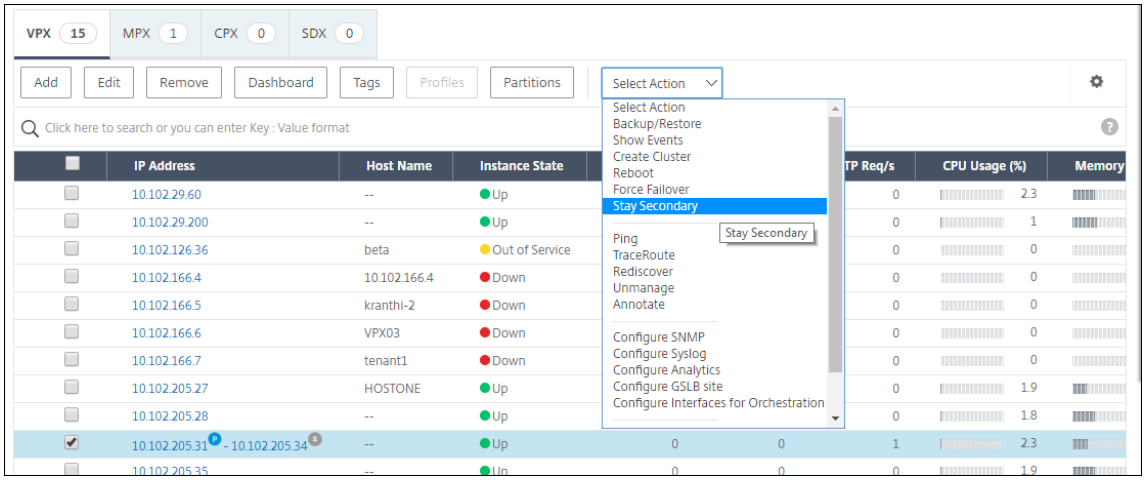
Par exemple, supposons que le nœud principal doit être mis à niveau et que le processus prend quelques secondes. Pendant la mise à niveau, le nœud principal peut tomber en panne pendant quelques secondes, mais vous ne voulez pas que le nœud secondaire prenne le relais. Vous souhaitez qu'il reste le nœud secondaire même s'il détecte une défaillance dans le nœud principal.

Lorsque vous forcez le nœud secondaire à rester secondaire, il reste secondaire même si le nœud principal tombe en panne. En outre, lorsque vous forcez l'état d'un nœud dans une paire HA à rester secondaire, il ne participe pas aux transitions de machines d'état HA. L'état du nœud est affiché en tant que STAYSECONDARY.

> **Remarque**
>
> Lorsque vous forcez un système à rester secondaire, le processus de forçage n'est ni propagé ni synchronisé. Elle affecte uniquement le nœud sur lequel vous exécutez la commande.

Pour configurer une instance Citrix ADC secondaire pour qu'elle reste secondaire à l'aide de Citrix ADM :

1. Dans Citrix Application Delivery Management (ADM), accédez à l'onglet **Réseaux** > **Instances** > **Citrix ADC** > **VPX**, puis sélectionnez une instance.
2. Sélectionnez les instances d'une configuration HA à partir des instances répertoriées sous le type d'instance sélectionné.
3. Dans le menu **Action**, sélectionnez **Rester secondaire**.
4. Cliquez sur **Oui** pour confirmer l'exécution de l'action « Rester secondaire ».



Créer des groupes d'instances

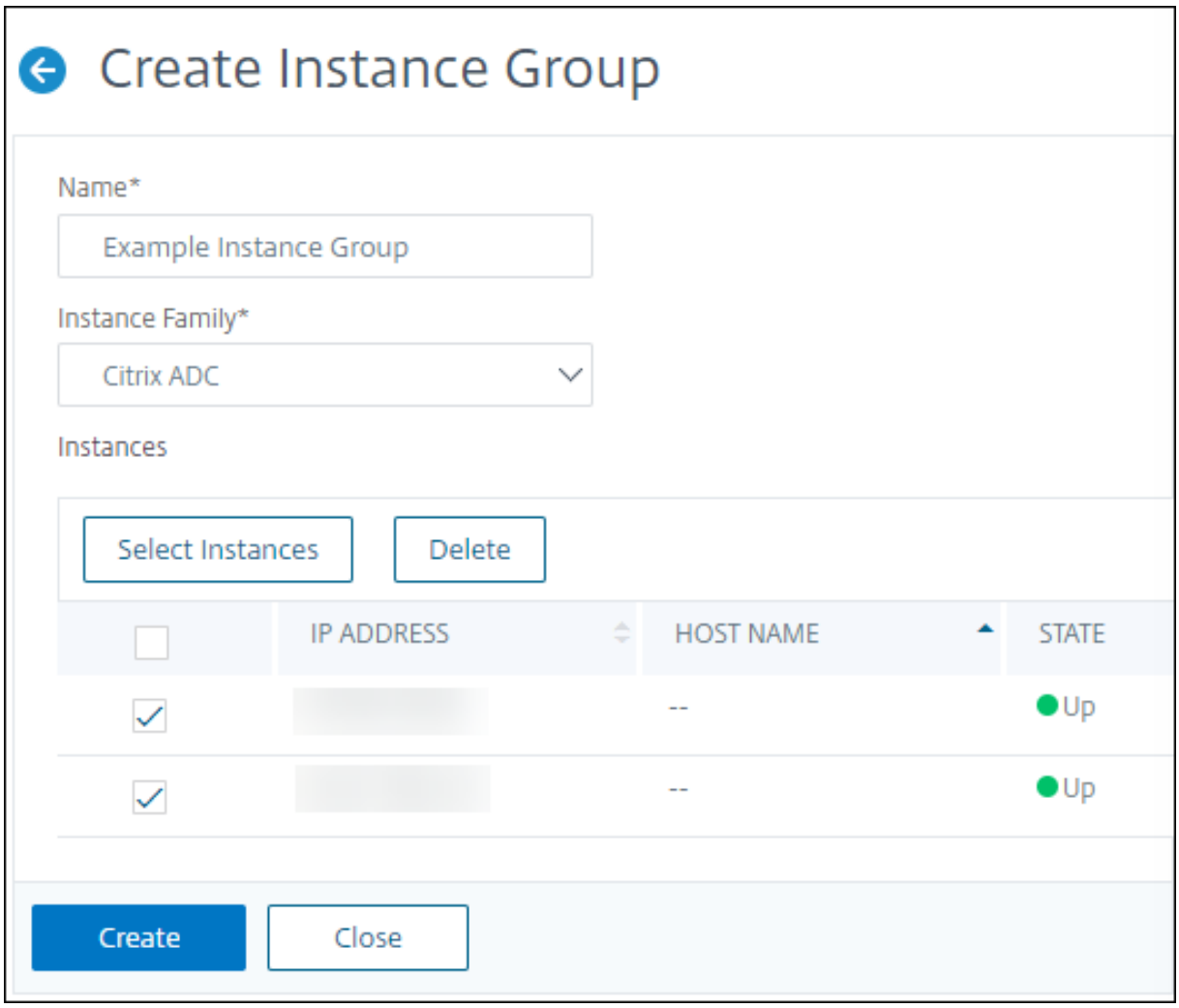
February 1, 2024

Pour créer un groupe d'instances, vous devez d'abord ajouter toutes vos instances Citrix ADC à Citrix ADM. Une fois les instances ajoutées avec succès, créez des groupes d'instances en fonction de leur famille d'instances. La création d'un groupe d'instances vous permet de mettre à niveau, de sauvegarder ou de restaurer les instances groupées en une seule fois.

Pour créer un groupe d'instances à l'aide de Citrix ADM

1. Dans Citrix ADM, accédez à **Réseaux** > **Groupes d'instances**, puis cliquez sur **Ajouter** .
2. Spécifiez un nom à votre groupe d'instances et sélectionnez **Citrix ADC** dans la liste **Famille d'instances**.
3. Cliquez sur **Sélectionner des instances**. Sur la page **Select Instances**, sélectionnez les instances que vous souhaitez regrouper et cliquez sur **Sélectionner**.

   Le tableau répertorie les instances sélectionnées et leurs détails. Si vous souhaitez supprimer une instance du groupe, sélectionnez-la dans le tableau et cliquez sur **Supprimer** .
4. Cliquez sur **Créer**.



Provisionner des instances VPX ADC sur SDX à l'aide d'ADM

February 1, 2024

Vous pouvez provisionner une ou plusieurs instances VPX ADC sur l'appliance SDX à l'aide de Citrix ADM. Le nombre d'instances que vous pouvez déployer dépend de la licence que vous avez achetée. Si le nombre d'instances ajoutées est égal au nombre spécifié dans la licence, l'ADM vous empêche de provisionner davantage d'instances Citrix ADC.

Avant de commencer, assurez-vous d'ajouter une instance SDX dans ADM où vous souhaitez provisionner des instances VPX.

Pour provisionner une instance VPX, procédez comme suit :

1. Accédez à **Réseaux > Instances > Citrix ADC**.

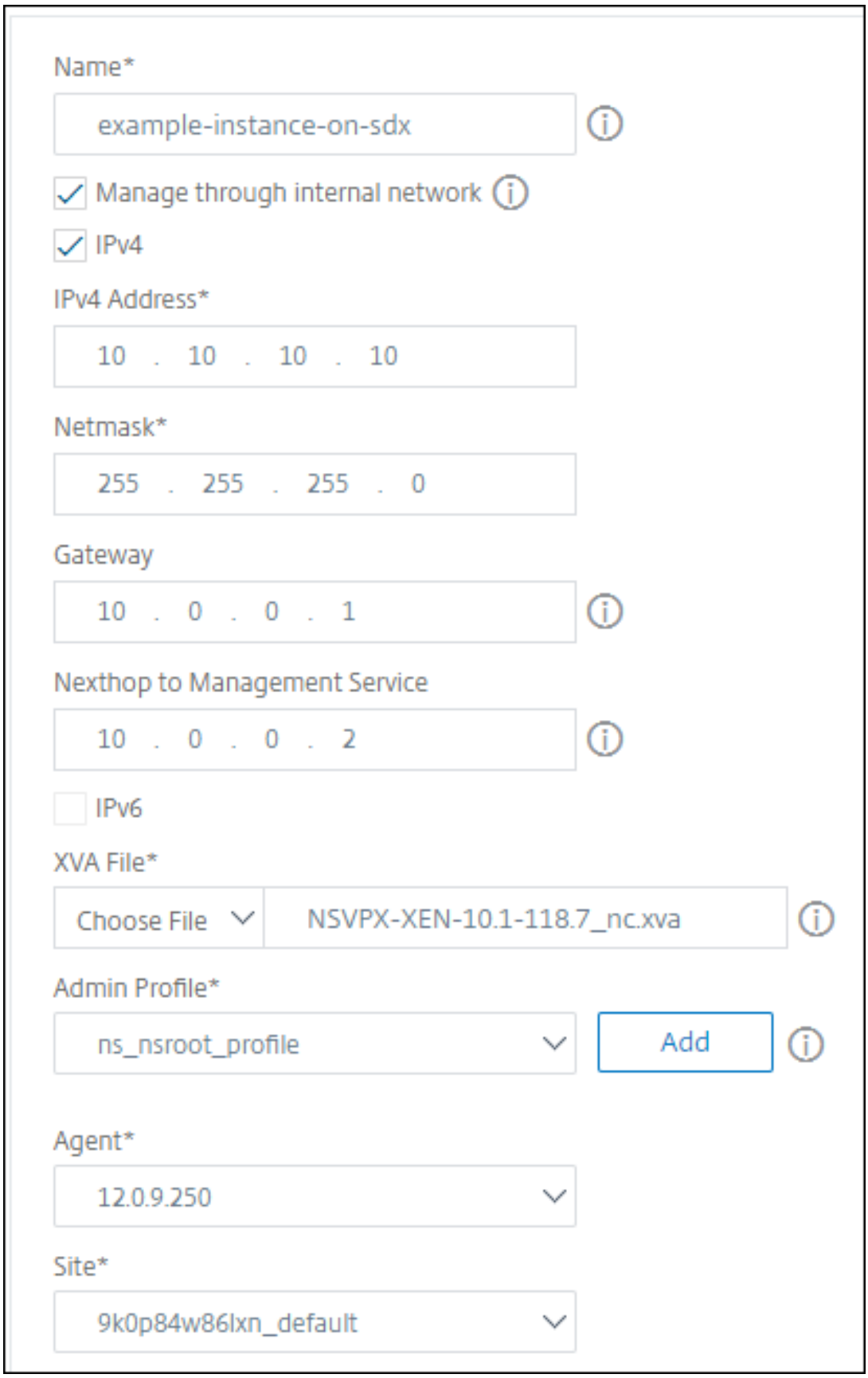
2. Dans l'onglet **SDX**, sélectionnez une instance SDX dans laquelle vous souhaitez provisionner une instance VPX.
3. Dans **Sélectionner une action**, sélectionnez **Provisionner VPX**.

Étape 1 - Ajouter une instance VPX

L'ADM utilise les informations suivantes pour configurer les instances VPX dans une appliance SDX :

- **Nom** : spécifiez un nom à une instance ADC.
- Établir un réseau de communication entre SDX et VPX. Pour ce faire, sélectionnez les options requises dans la liste :
  - **Gérer via le réseau interne** - Cette option établit un réseau interne pour une communication entre ADM et une instance VPX.
  - **Adresse IP** - Vous pouvez sélectionner une adresse **IPv4** ou **IPv6** ou les deux pour gérer l'instance Citrix VPX. Une instance VPX ne peut avoir qu'une seule adresse IP de gestion (également appelée Citrix ADC IP). Vous ne pouvez pas supprimer l'adresse IP Citrix ADC.

    Pour l'option sélectionnée, attribuez un masque de réseau, une passerelle par défaut et un saut suivant au serveur ADM pour l'adresse IP.
- **XVA File** - Sélectionnez le fichier XVA à partir duquel vous souhaitez provisionner une instance VPX. Utilisez l'une des options suivantes pour sélectionner le fichier XVA.
  - **Local** - Sélectionnez le fichier XVA de votre ordinateur local.
  - **Appliance** - Sélectionnez le fichier XVA dans un navigateur de fichiers ADM.
- **Profil d'administrateur** - Ce profil permet d'accéder au provisionnement des instances VPX. Avec ce profil, ADM récupère les données de configuration d'une instance. Si vous devez ajouter un profil, cliquez sur **Ajouter**.
- **Agent** - Sélectionnez l'agent auquel vous souhaitez associer les instances
- **Site** - Sélectionnez le site où vous souhaitez ajouter l'instance.



Étape 2 - Allouer des licences

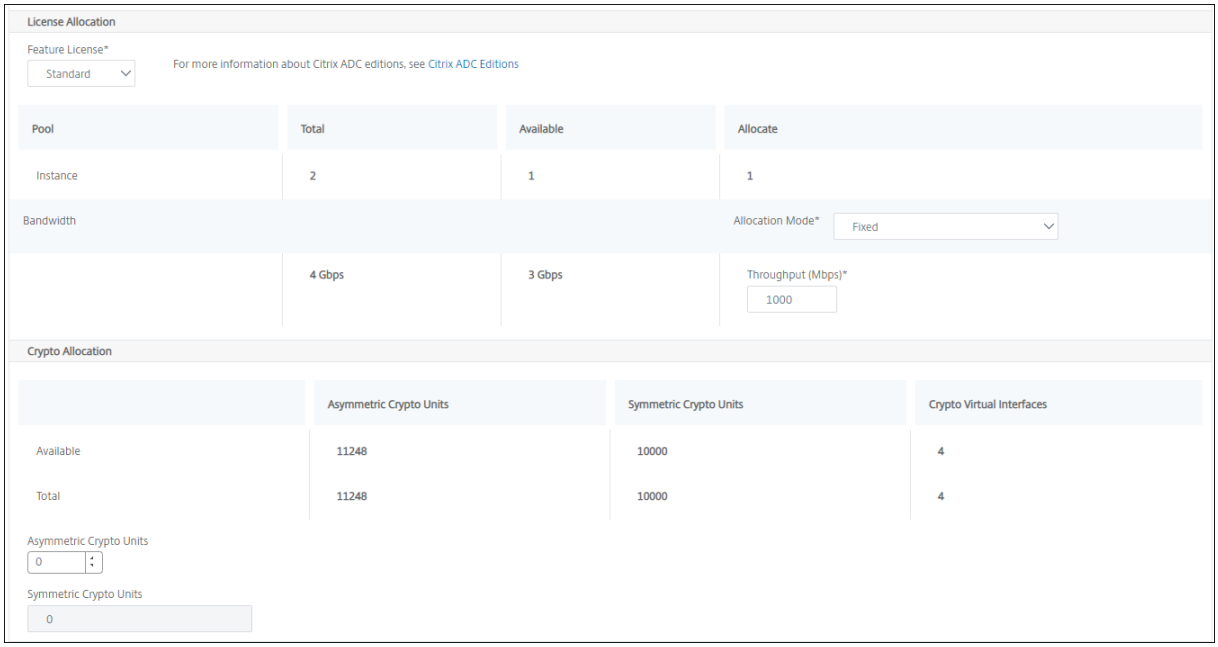
Dans la section **Allocation de licences**, spécifiez la licence VPX. Vous pouvez utiliser des licences Standard, Advanced et Premium.

- **Mode d'allocation** - Vous pouvez choisir les modes **Fixe** ou **Burstable** pour le pool de bande passante.

  Si vous choisissez le mode **Burstable**, vous pouvez utiliser une bande passante supplémentaire lorsque la bande passante fixe est atteinte.

- **Débit** - Affectez le débit total (en Mbps) à une instance.

> **Remarque**
>
> Achetez une licence distincte (SDX 2-Instance Add-On Pack pour Secure Web Gateway) pour les instances Citrix Secure Web Gateway (SWG) sur les appliances SDX. Ce pack d'instances est différent de la licence de plate-forme SDX ou du pack d'instances SDX.
>
> Pour plus d'informations, consultez Déploiement d'une instance Citrix Secure Web Gateway sur une appliance SDX.



À partir de la version SDX 12.0 57.19, l'interface pour gérer la capacité de chiffrement a changé. Pour plus d'informations, consultez Gérer la capacité de chiffrement.

Étape 3 - Allouer les ressources

Dans la section **Allocation de ressources**, allouez des ressources à une instance VPX pour maintenir le trafic.

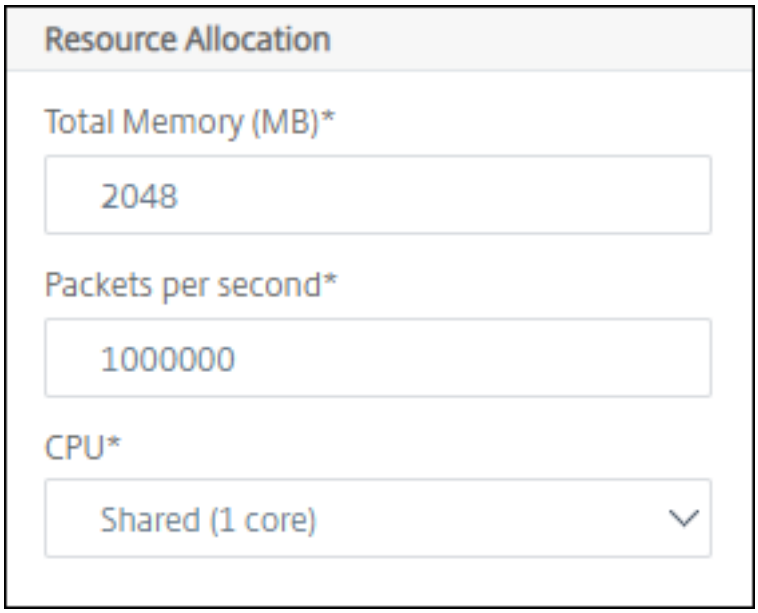
- **Mémoire totale (Mo)** - Affectez la mémoire totale à une instance. La valeur minimale est 2048 Mo.
- **Paquets par seconde** - Spécifiez le nombre de paquets à transmettre par seconde.
- **CPU** - Spécifiez le nombre de cœurs de CPU à une instance. Vous pouvez utiliser des cœurs CPU partagés ou dédiés.

  Lorsque vous sélectionnez un cœur partagé pour une instance, les autres instances peuvent utiliser le noyau partagé au moment de la pénurie de ressources.

  Redémarrez les instances sur lesquelles les cœurs CPU sont réaffectés pour éviter toute dégradation des performances.

  Si vous utilisez la plate-forme SDX 25000xx, vous pouvez affecter 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 unique groupée 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
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 40G et SDX 14100 40 G	12	10	10
SDX 14020 FIPS, SDX 14030 FIPS, SDX 14040 FIPS, SDX 14060 FIPS, SDX 14080 FIPS et SDX 14100. FIPS	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	5
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	13
15000-50G	16	14	7

> **Remarque**
>
> Sur la plate-forme SDX 26xxx, un maximum de 26 cœurs de CPU peuvent être affectés à une instance VPX. Si des unités crypto sont affectées à l'instance, le nombre maximal de cœurs dépend du nombre d'unités de crypto 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. Pour 26000 unités crypto, le provisionnement d'instance VPX échoue en raison de l'absence d'espace pour ajouter des interfaces de données.

Étape 4 - Ajouter l'administration d'instance

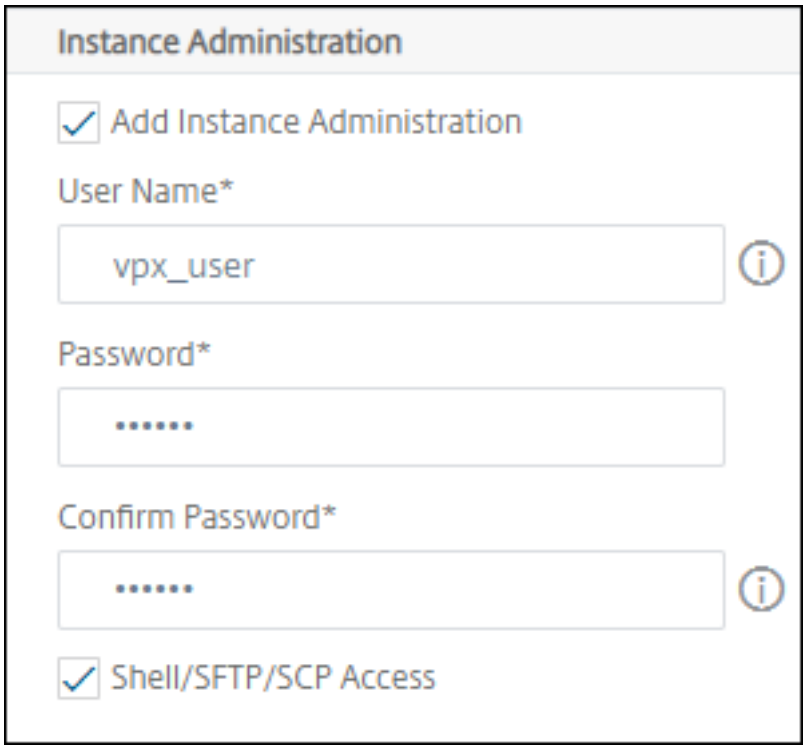
Vous pouvez créer un utilisateur administrateur pour l'instance VPX. Pour ce faire, sélectionnez **Ajouter une administration d'instance** dans la section **Administration de l'instance**.

Spécifiez les détails suivants :

- **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** : spécifiez le mot de passe du nom d'utilisateur.
- **Accès Shell/Sftp/SCP** : Accès autorisé à l'administrateur de l'instance Citrix ADC. Cette option est sélectionnée par défaut.



Étape 5 - Spécifier les paramètres réseau

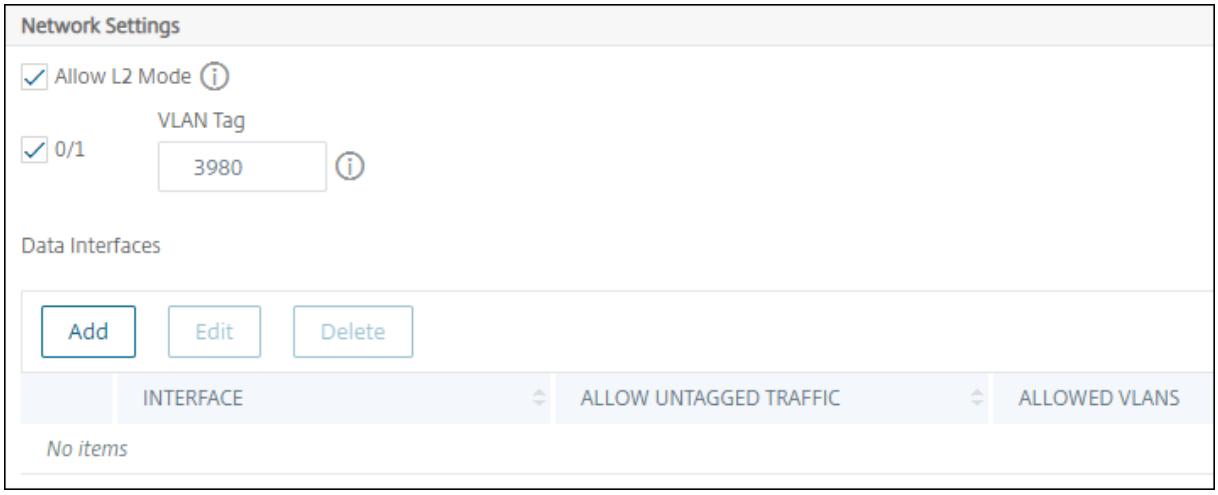
Sélectionnez les paramètres réseau requis pour une instance :

- **Autoriser le mode L2 dans les paramètres réseau** : 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, vous devez vous connecter à l'instance et désactiver le mode L2 à partir de cette instance. Sinon, tous les autres modes Citrix ADC peuvent être désactivés après le redémarrage de l'instance.

- **0/1** - Dans la **balise VLAN**, spécifiez un ID VLAN pour l'interface de gestion.
- **0/2** - Dans la **balise VLAN**, spécifiez un ID VLAN pour l'interface de gestion.

Par défaut, les interfaces **0/1** et **0/2** sont sélectionnées.



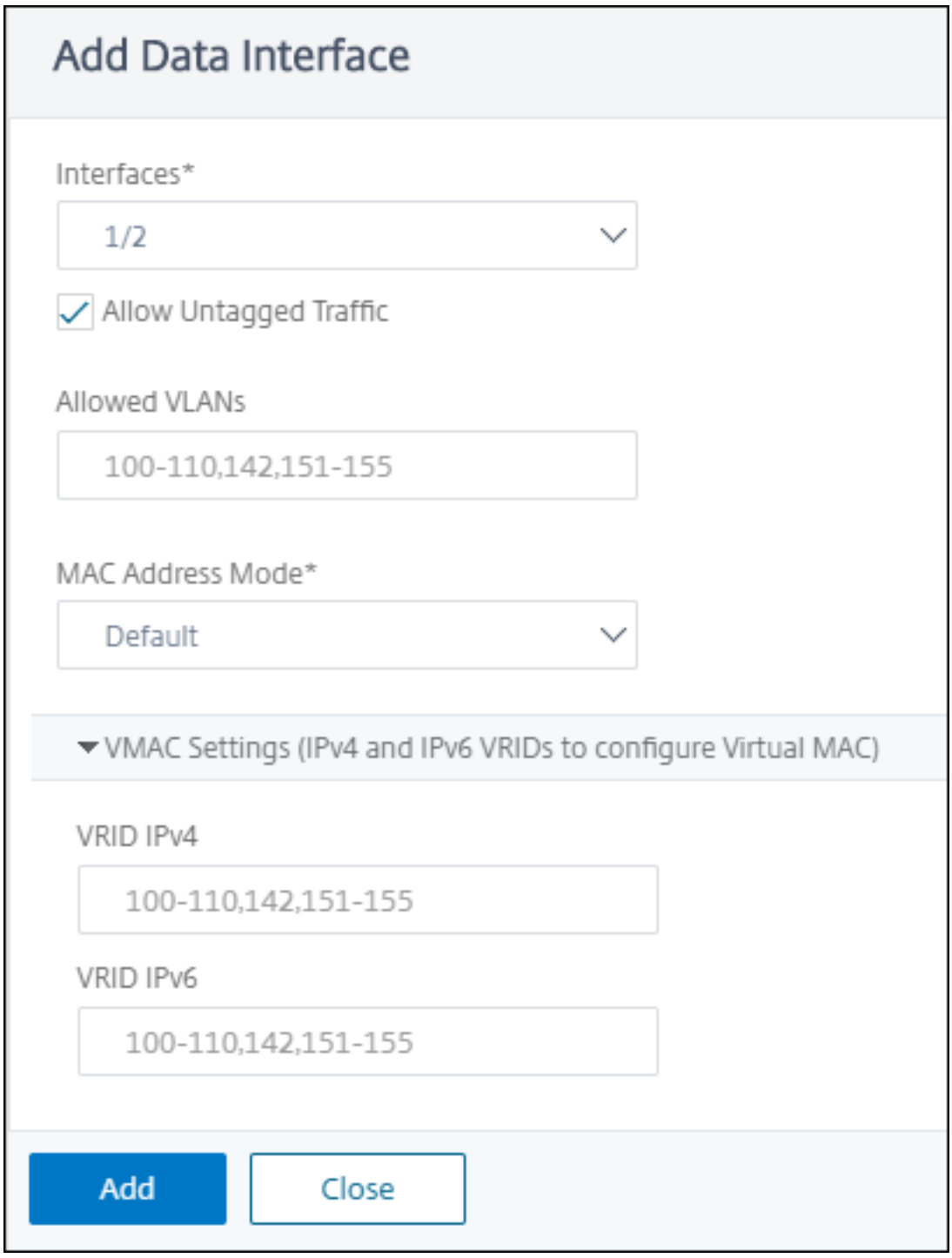
Dans **Interfaces de données**, cliquez sur **Ajouter** pour ajouter des interfaces de données et spécifiez les éléments suivants :

- **Interfaces** - Sélectionnez l'interface dans la liste.

  > **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.
  >
  > Par exemple, la première interface que vous associez à instance-1 est l'interface SDX 1/4, elle apparaît sous la forme d'interface 1/1 lorsque vous affichez les paramètres de l'interface dans cette instance. Cette interface indique qu'il s'agit de la première interface que vous avez associée à instance-1.

- **VLAN autorisés :** spécifiez une liste d'ID VLAN pouvant être associés à une instance Citrix ADC.
- **Mode d'adresse MAC** - Affectez une adresse MAC à une instance. Sélectionnez l'une des options suivantes :
  - **Valeur par défaut** - Citrix Workspace 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'ensemble d'adresses MAC de base 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** - Le VRID IPv4 qui identifie le VMAC. Valeurs possibles : 1—255. Pour plus d'informations, consultez Configuration de vMac sur une interface.

- VRID IPV6 - Le VRID IPv6 qui identifie le VMAC. Valeurs possibles : 1—255. Pour plus d'informations, consultez Configuration de vMac sur une interface.



Cliquez sur **Ajouter**.

Étape 6 - Spécifier les paramètres du VLAN de gestion

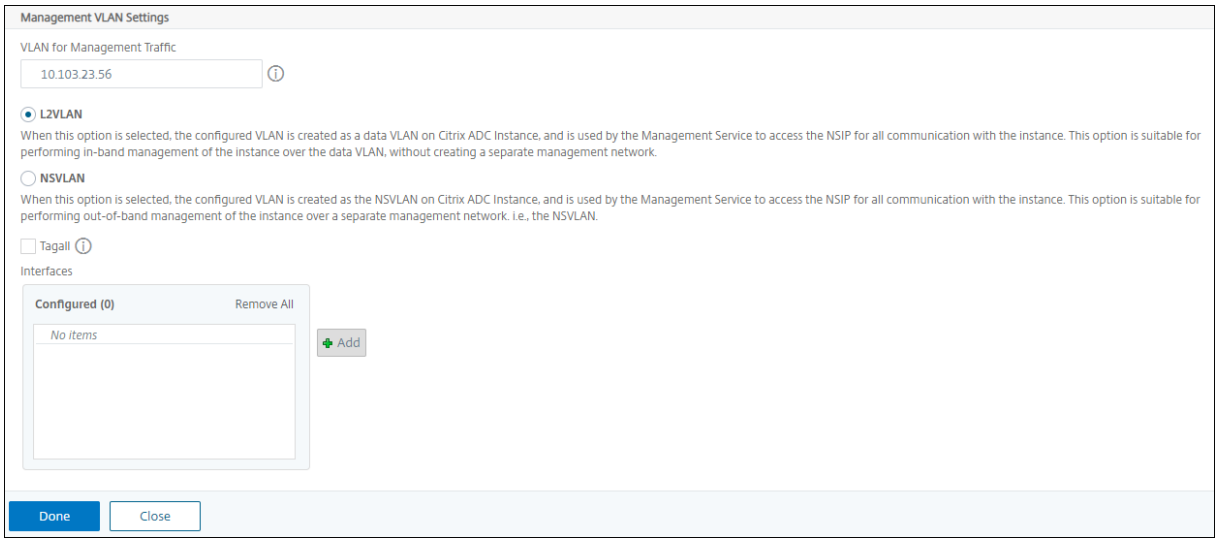
Le service de gestion et l'adresse de gestion (NSIP) de l'instance VPX se trouvent dans le même sous-réseau, et la communication se fait via une interface de gestion.

Si le service de gestion et l'instance se trouvent dans des sous-réseaux différents, spécifiez un ID VLAN pendant que vous provisionnez une instance VPX. Par conséquent, l'instance est accessible sur le réseau lorsqu'elle est active.

Si votre déploiement nécessite que le NSIP est accessible uniquement via l'interface sélectionnée lors du provisionnement de l'instance VPX, sélectionnez **NSVLAN**. Et, le NSIP devient inaccessible via d'autres interfaces.

- 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 la version XVA VPX `9.3-53.4` et ultérieure.

> **Important**
>
> - Vous ne pouvez pas modifier ce paramètre après avoir configuré l'instance VPX.
> - La commande `clear config full` de l'instance VPX supprime la configuration du VLAN si **NSVLAN** n'est pas sélectionnée.

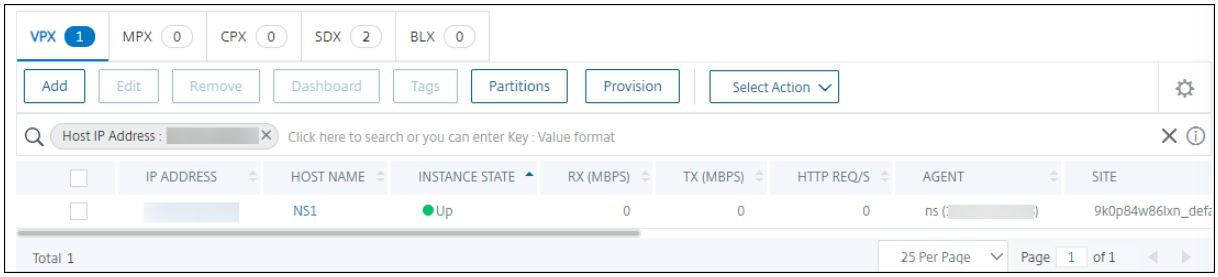


Cliquez sur **Terminé** pour provisionner une instance VPX.

Afficher l'instance VPX provisionnée

Pour afficher l'instance nouvellement provisionnée, procédez comme suit :

1. Accédez à **Réseaux > Instances > Citrix ADC**.
2. Dans l'onglet **VPX**, recherchez une instance à l'aide de la propriété d'**adresse IP de l'hôte** et spécifiez l'adresse IP de l'instance SDX.



Redécouvrir plusieurs instances Citrix VPX

February 1, 2024

Vous pouvez redécouvrir plusieurs instances Citrix VPX dans votre configuration de Citrix Application Delivery Management (ADM). Vous pouvez également redécouvrir plusieurs instances Citrix VPX lorsque vous souhaitez afficher les derniers états et configurations de ces instances. Le serveur Citrix ADM redécouvre toutes les instances Citrix VPX et vérifie si les instances de Citrix Application Delivery Controller (ADC) sont accessibles.

Pour redécouvrir plusieurs instances Citrix VPX :

1. Dans un navigateur Web, tapez l'adresse IP du serveur Citrix ADM (par exemple, http://192.168.100.1).
2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur. Les informations d'identification de l'administrateur par défaut sont `nsroot` et `nsroot`.
3. Accédez à **Réseaux** > **Instances** > **Citrix ADC** > onglet **VPX** et sélectionnez les instances que vous souhaitez redécouvrir.
4. Dans le menu **Sélectionner une action**, cliquez sur **Redécouvrir**.
5. Lorsque le message de confirmation de l'exécution de l'utilitaire Redécouvrir s'affiche, cliquez sur **Oui**.

   L'écran signale la progression de la redécouverte de chacune des instances Citrix VPX.

Annuler l'administration d'une instance

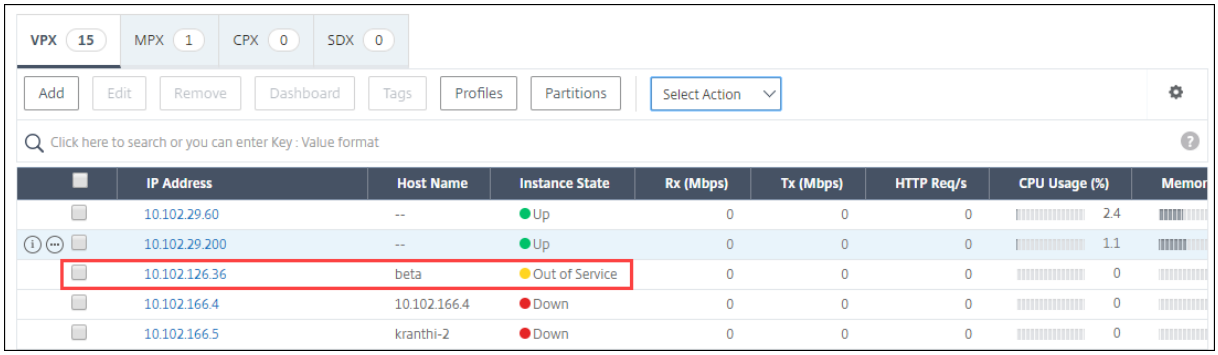
February 1, 2024

Si vous souhaitez arrêter l'échange d'informations entre Citrix Application Delivery Management (ADM) et les instances de votre réseau, vous pouvez annuler la gestion des instances.

Pour annuler la gestion d'une instance :

Accédez à **Réseaux** > **Instances** > **Citrix ADC** > onglet **VPX**. Dans la liste des instances, cliquez avec le bouton droit sur une instance, puis sélectionnez **Ne pas gérer**, ou sélectionnez l'instance et, dans la liste **Sélectionner une action**, sélectionnez **Ne pas gérer**.

L'état de l'instance sélectionnée devient **Absence de service**, comme illustré dans la figure suivante.



L'instance n'est plus gérée par Citrix ADM et n'échange plus de données avec Citrix ADM.

Tracer la route jusqu'à une instance

February 1, 2024

En traçant l'itinéraire d'un paquet depuis Citrix Application Delivery Management (ADM) vers une instance, vous pouvez trouver des informations telles que le nombre de sauts nécessaires pour atteindre l'instance. Traceroute trace le chemin du paquet de la source à la destination. Il affiche la liste des sauts réseau ainsi que le nom d'hôte et l'adresse IP de chaque entité de la route.

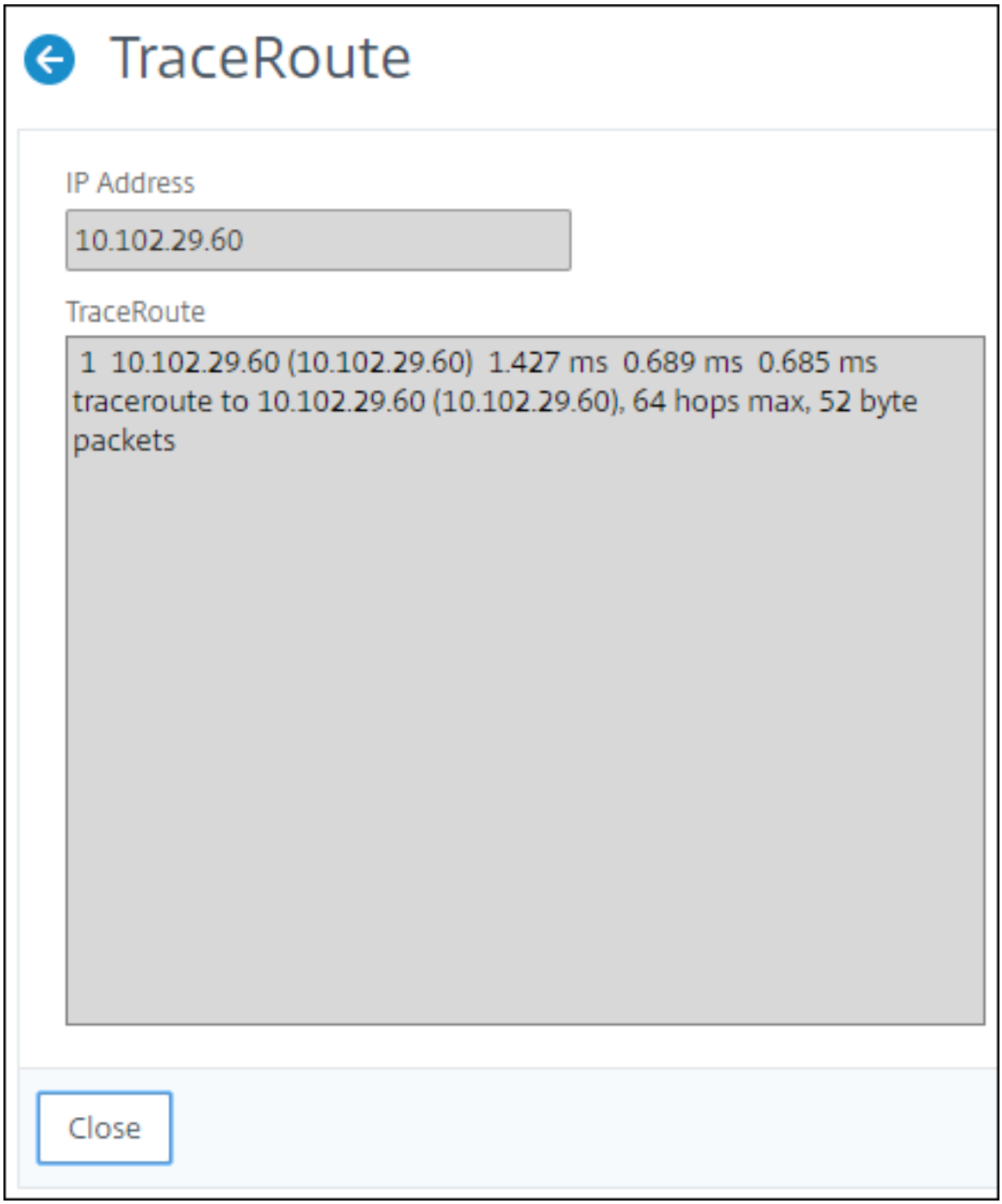
Traceroute enregistre également le temps qu'un paquet prend pour voyager d'un saut à l'autre. En cas d'interruption du transfert de paquets, traceroute indique où se situe le problème.

Pour tracer la route d'une instance :

1. Dans Citrix ADM, accédez à l'onglet **Réseaux** > **Instances** > **Citrix ADC** > **VPX**.

2. Dans la liste des instances, cliquez avec le bouton droit sur une instance, puis sélectionnez **TraceRoute** ou sélectionnez l'instance et, dans le menu **Sélectionner une action**, cliquez sur **TraceRoute**.

La boîte de message **TraceRoute** indique l'itinéraire vers l'instance et la durée, en millisecondes, consommée par chaque saut.



Avis de mise à

February 1, 2024

En tant qu'administrateur réseau, vous pouvez gérer de nombreuses instances ADC exécutées sur différentes versions d'ADC dans NetScaler ADM. La surveillance du cycle de vie de chaque instance ADC peut être une tâche lourde. Vous devez consulter la matrice des produits Citrixet identifier les instances ADC qui atteignent ou ont atteint la fin de vie (EOL) ou la fin de la maintenance (EOM). Ensuite, planifiez leur mise à niveau.

Les conseils de mise à niveau vous aident à surveiller le cycle de vie de vos instances ADC. Il identifie les instances qui atteignent l'EOL/EOM et vous pouvez planifier les mises à niveau de l'ADC avant la date EOL ou EOM.

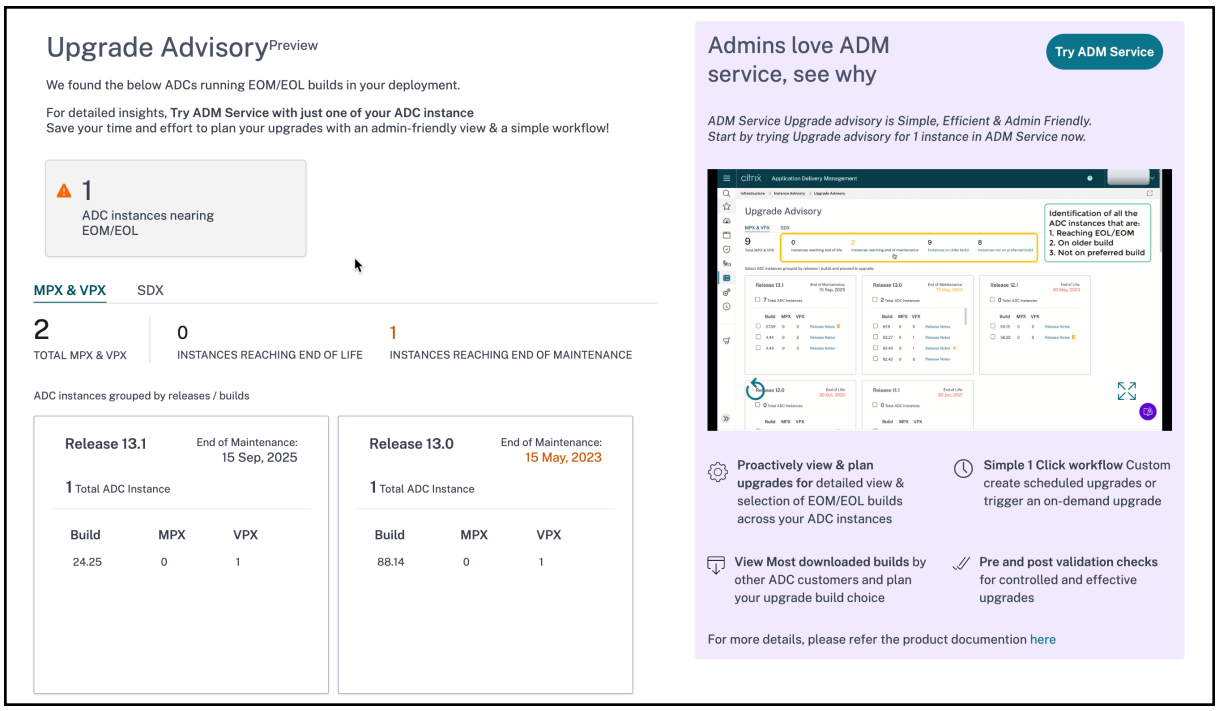
Upgrade Advisory analyse les versions des ADC et fournit une vue des versions EOM/EOL de vos instances ADC.

Vous pouvez sélectionner et intégrer l'une des instances ADC au service ADM. Cliquez sur **Essayer le service ADM**et intégrez une instance ADC pour obtenir des informations détaillées. Pour plus d'informations sur la fonctionnalité consultative de mise à niveau du service ADM, prévisualisez l'animation gif sur la page des **conseils de mise à niveau** .

Consulter l'avis de mise

Naviguez **Réseaux > Avis d'instance > Avis de mise à niveau** et affichez les informations suivantes :

- Nombre total d'instances ADC.
- Les instances atteignant la fin de la vie.
- Instances atteignant la fin de la maintenance.



La page **Avis de mise à niveau** regroupe les instances ADC en fonction de leurs versions.

Avis de sécurité

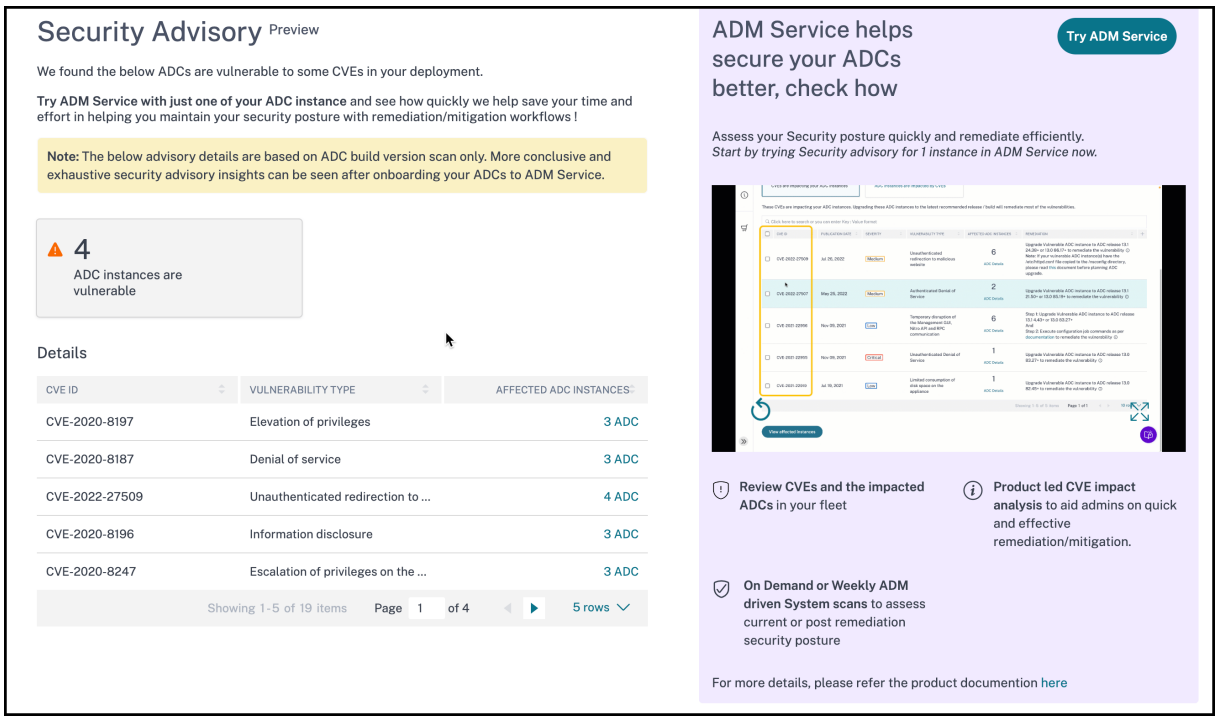
February 1, 2024

Une infrastructure sûre, sécurisée et résiliente est la ligne de vie de toute organisation. Les entreprises doivent suivre les nouvelles vulnérabilités et expositions courantes (CVE) et évaluer l'impact des CVE sur leur infrastructure. Ils doivent également comprendre et planifier les mesures d'atténuation et de correction pour résoudre les vulnérabilités.

L'avis de sécurité de NetScaler ADM met en évidence les CVE Citrix qui mettent en danger vos instances ADC.

Afficher l'avis de sécurité

Pour accéder à l'**avis de sécurité**, accédez à **Réseaux > Avis d'instance > Avis de sécurité**. Vous pouvez consulter l'état de vulnérabilité de toutes les instances ADC que vous gérez via NetScaler ADM.



Security Advisory effectue uniquement une analyse de la version ADC pour vérifier la présence de CVE et un tableau indiquant le nombre de CVE ayant un impact sur les instances ADC s'affiche.

- **ID CVE** : ID du CVE impactant les instances.
- **Type de vulnérabilité** : type de vulnérabilité pour ce CVE.
- **Instances ADC concernées : nombre d'instances**sur lesquelles l'ID CVE a un impact.

Pour vérifier le type de vulnérabilité d'un CVE particulier et obtenir des informations sur l'atténuation et la correction permettant de résoudre la vulnérabilité, sélectionnez l'une des instances ADC, cliquez sur **Essayer le service ADM** et intégrez l'instance ADC au service ADM. Pour plus d'informations sur la fonction d'avis de sécurité du service ADM, prévisualisez l'animation GIF sur la page **de l'avis de sécurité** .

Événements

February 1, 2024

Lorsque l'adresse IP d'une instance de Citrix Application Delivery Controller (ADC) est ajoutée à Citrix Application Delivery Management (ADM), Citrix ADM envoie un appel NITRO et s'ajoute implicitement comme destination d'interruption pour que l'instance reçoive ses interruptions ou événements.

Les événements représentent des occurrences d'événements ou d'erreurs sur une instance Citrix ADC

gérée. Par exemple, en cas de défaillance du système ou de modification de la configuration, un événement est généré et enregistré sur le serveur Citrix ADM. Les événements reçus dans Citrix ADM s'affichent sur la page Récapitulatif des événements (**Réseaux** > **Événements**) et tous les événements actifs sont affichés dans la page Messages d'événements (**Réseaux** > **Événements** > **Messages**d'événements).

Citrix ADM vérifie également les événements générés sur les instances pour former des alarmes de différents niveaux de gravité. Ces alarmes sont ensuite affichées sous forme de messages, dont certains peuvent nécessiter une attention immédiate. Par exemple, les défaillances du système peuvent être classées comme une gravité d'événement « critique » et devraient être corrigées immédiatement.

Vous pouvez configurer des règles pour surveiller des événements spécifiques. Les règles facilitent la surveillance des événements, qui peuvent être nombreux, générés dans l'ensemble de votre infrastructure Citrix ADC.

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 : gravité, instances Citrix ADC, catégorie, objets de défaillance, commandes de configuration et messages.

Vous pouvez également vous assurer que plusieurs notifications sont déclenchées pour un événement pendant un intervalle de temps spécifique, jusqu'à ce que l'événement soit effacé. Par mesure supplémentaire, vous pouvez personnaliser votre e-mail avec une ligne d'objet et un message utilisateur spécifiques, et télécharger une pièce jointe.

Utiliser le tableau de bord des événements

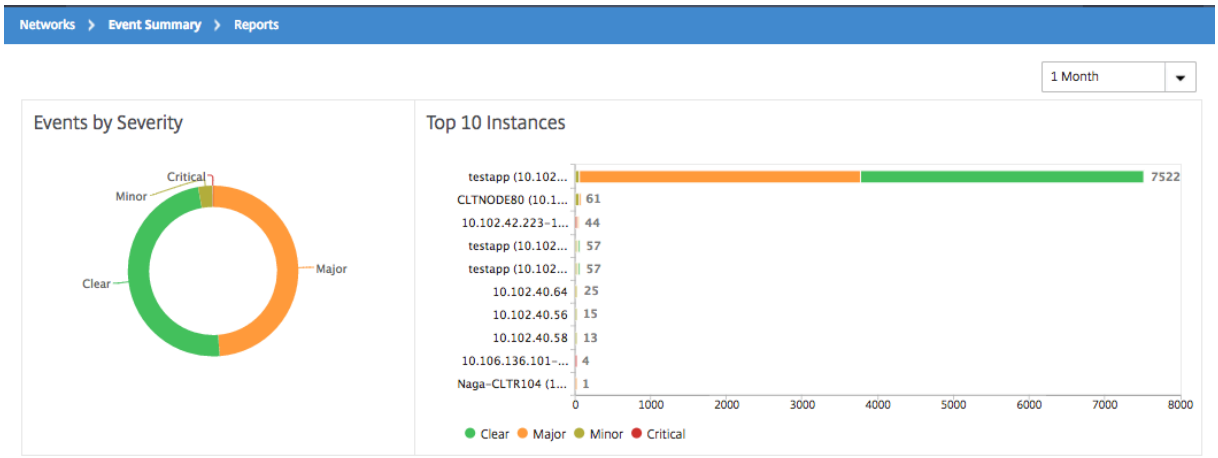
February 1, 2024

En tant qu'administrateur réseau, vous pouvez consulter des informations telles que les modifications de configuration, les conditions de connexion, les défaillances matérielles, les violations des seuils et les modifications de l'état des entités sur vos instances Citrix Application Delivery Controller (ADC), ainsi que les événements et leur gravité sur des instances spécifiques. Vous pouvez utiliser le tableau de bord des événements de Citrix Application Delivery Management (ADM) pour consulter les rapports générés contenant des informations détaillées sur la gravité des événements critiques sur toutes vos instances Citrix ADC.

Pour afficher les détails sur le tableau de bord des événements :

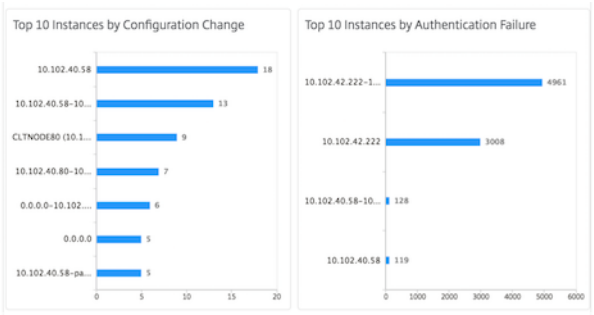
Accédez à **Réseaux** > **Événements** > **Rapports**.

Le graphique 10 principaux périphériques du tableau de bord affiche un rapport des 10 instances les plus importantes selon le nombre d'événements générés sur elles. Vous pouvez cliquer sur une instance sur le graphique pour afficher plus de détails sur la gravité de l'événement.

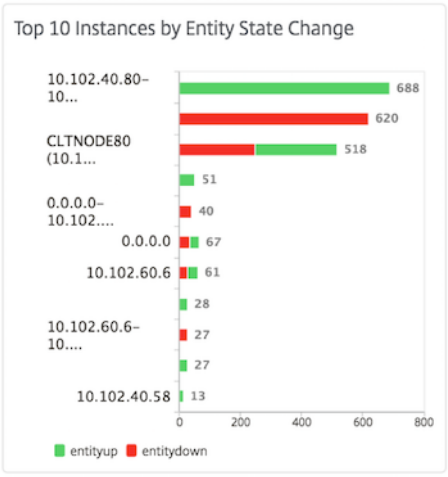


Vous pouvez afficher plus de détails en accédant au type d'instance Citrix ADC (**Réseaux** > **Événements** > **Rapports** > **Citrix ADC/Citrix ADC SDX/ Citrix ADC SD-WAN WO**) pour afficher les éléments suivants :

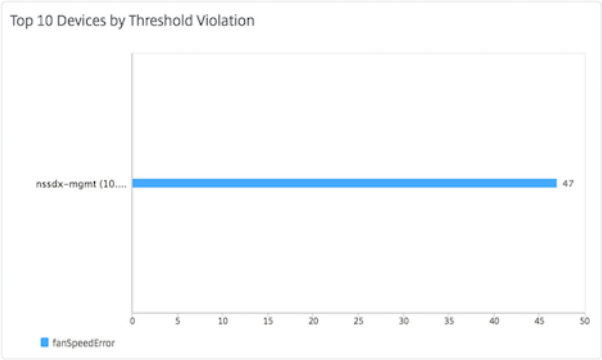
- Top 10 des périphériques par défaillance matérielle
- Les 10 principaux appareils par changement de configuration
- Top 10 des appareils par échec d'authentification



- Top 10 des périphériques par modification de l'état de l'entité



- Top 10 des appareils par violation de seuil



Définir l'âge de l'événement pour les événements

February 1, 2024

Vous pouvez définir l'option d'âge de l'événement pour spécifier l'intervalle de temps (en secondes). Citrix ADM surveille les appliances jusqu'à la durée définie et génère un événement uniquement si l'âge de l'événement dépasse la durée définie.

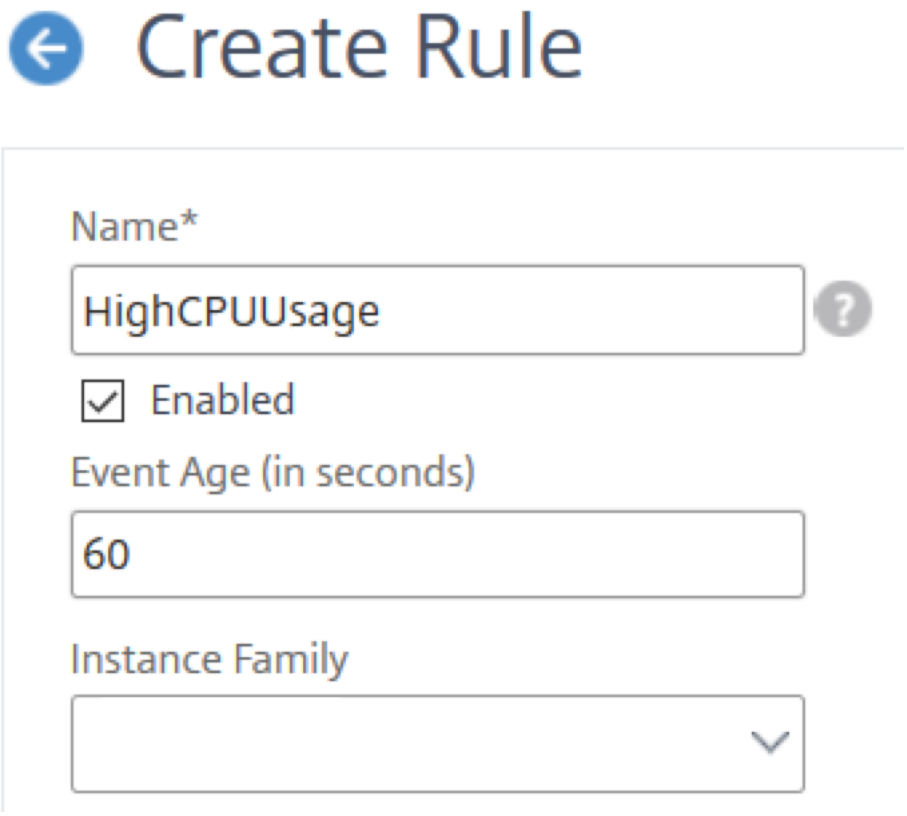
> Remarque :
>
> La valeur minimale de l'âge de l'événement est de 60 secondes. Si vous gardez le champ **Âge** de l'événement vide, la règle d'événement est appliquée immédiatement après l'événement.

Par exemple, imaginez que vous souhaitez gérer différentes appliances ADC et recevoir une notification par e-mail lorsque l'un de vos serveurs virtuels tombe en panne pendant 60 secondes ou plus. Vous pouvez créer une règle d'événement avec les filtres nécessaires et définir l'âge d'événement de

la règle sur 60 secondes. Ensuite, chaque fois qu'un serveur virtuel reste en panne pendant 60 secondes ou plus, vous recevez une notification par e-mail contenant des détails tels que le nom de l'entité, le changement d'état et l'heure.

Pour définir l'âge des événements dans Citrix ADM :

1. Dans Citrix ADM, accédez à **Réseaux** > **Événements** > **Règles**, puis cliquez sur **Ajouter**.
2. Dans la page **Créer une règle**, définissez les paramètres de la règle.
3. Spécifiez l'âge de l'événement en secondes.



Veillez à définir tous les interruptions associées dans la section **Catégorie** et également à définir la gravité respective dans la section **Gravité** lorsque vous définissez l'âge de l'événement. Dans l'exemple précédent, sélectionnez les `entityofs` interruptions `entityupentitydown`, et.

Planifier un filtre d'événement

February 1, 2024

Après avoir créé un filtre pour votre règle, si vous ne souhaitez pas que le serveur ADM (Citrix Application Delivery Management) envoie une notification chaque fois que l'événement généré satisfait aux

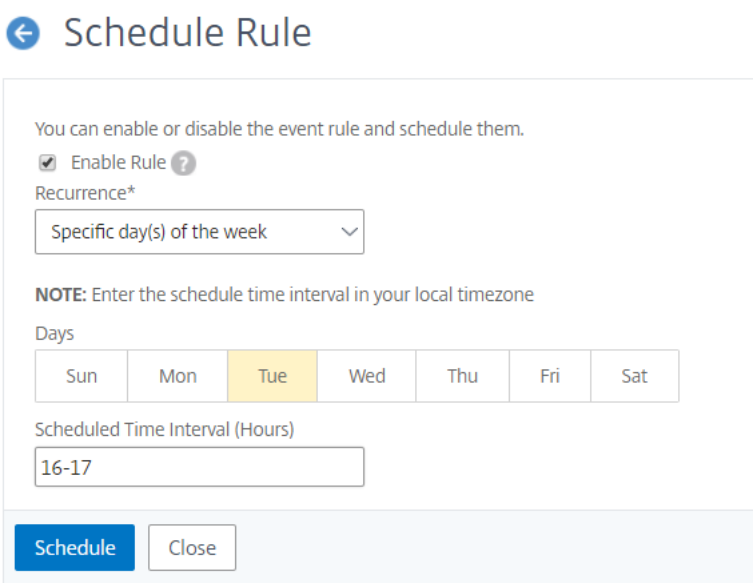
critères de filtre, vous pouvez programmer le filtre pour qu'il se déclenche uniquement à des intervalles de temps spécifiques, tels que quotidiens, hebdomadaires ou mensuels.

Par exemple, si vous avez planifié une activité de maintenance système pour différentes applications sur vos instances à des moments différents, les instances peuvent générer plusieurs alarmes.

Si vous avez configuré un filtre pour ces alarmes et activé les notifications par e-mail pour ces filtres, le serveur envoie un grand nombre de notifications par e-mail lorsque Citrix ADM reçoit ces interruptions. Si vous souhaitez que le serveur envoie ces notifications par e-mail uniquement pendant une période spécifique, vous pouvez le faire en planifiant un filtre.

Pour planifier un filtre à l'aide de Citrix ADM :

1. Dans Citrix ADM, accédez à **Réseaux** > **Événements** > **Règles** .
2. Sélectionnez la règle pour laquelle vous souhaitez planifier un filtre, puis cliquez sur **Afficher la planification**.
3. Dans la page **Règle programmée**, cliquez sur **Planifier** et spécifiez les paramètres suivants :
    - **Activer la règle** —Activez cette case à cocher pour activer la règle d'événement planifié.
    - **Récurrence** : intervalle auquel planifier la règle. Sélectionnez un jour spécifique de la semaine ou une date spécifique dans un mois.
    - **Jours** : sélectionnez le jour de la semaine pour exécuter la règle. Vous pouvez sélectionner plusieurs jours.
    - **Dates** : saisissez les dates. Vous pouvez taper plusieurs dates en tant que valeurs séparées par des virgules.
    - **Intervalle de temps planifié (heures)** —Heures, à laquelle programmer la règle (utilisez le format 24 heures).
4. Cliquez sur **Planifier**.



Définir des notifications par e-mail répétées pour les événements

February 1, 2024

Pour vous assurer que tous les événements critiques sont traités et qu'aucune notification par e-mail importante n'est manquée, vous pouvez choisir d'envoyer des notifications par e-mail répétées pour les règles d'événements qui répondent aux critères que vous avez sélectionnés. Par exemple, si vous avez créé une règle d'événement pour les instances qui impliquent des défaillances de disque et que vous souhaitez être averti jusqu'à ce que le problème soit résolu, vous pouvez choisir de recevoir des notifications par e-mail répétées sur ces événements.

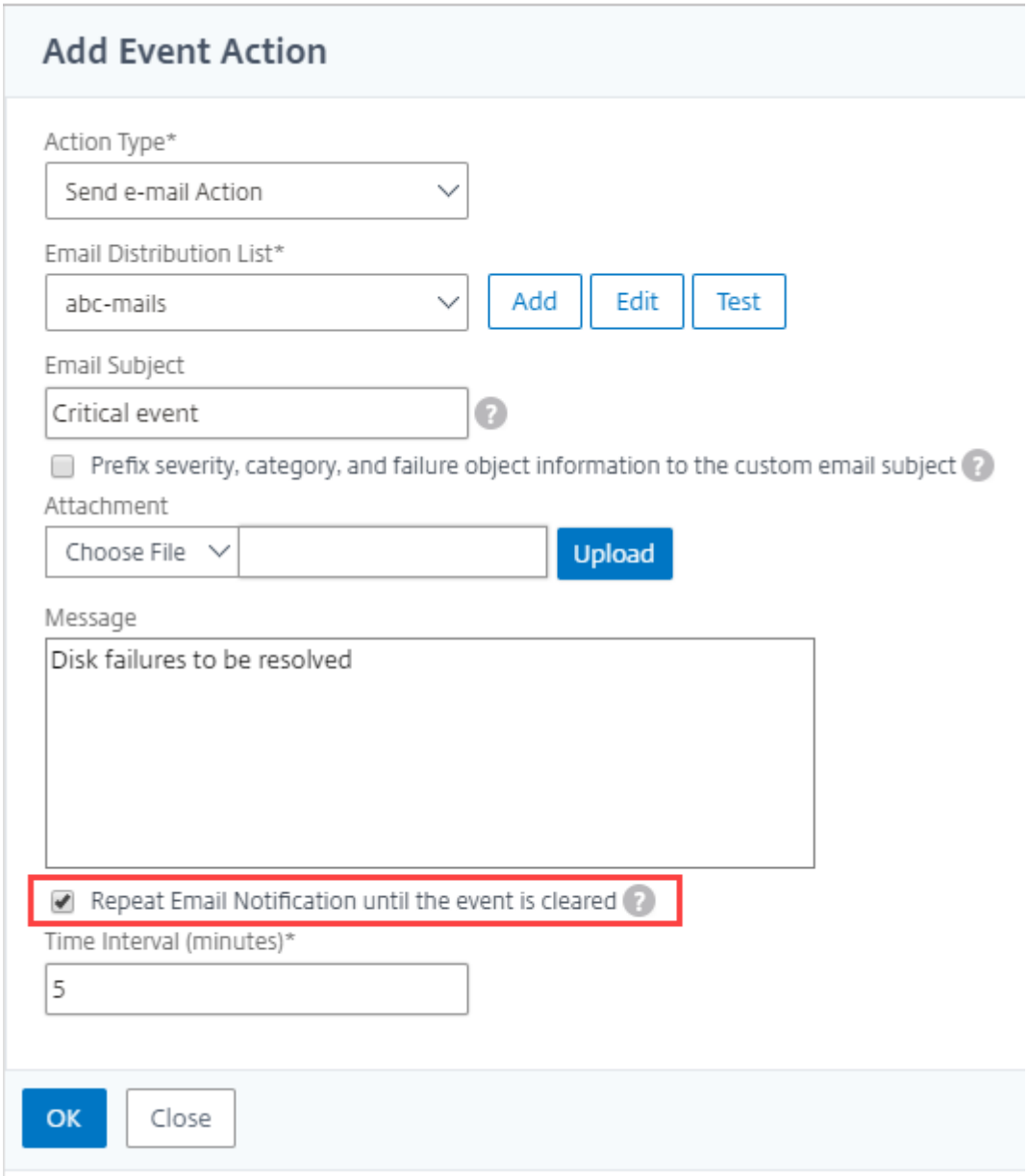
Ces notifications par e-mail sont envoyées à plusieurs reprises, à des intervalles prédéfinis, jusqu'à ce que le destinataire reconnaisse avoir vu la notification ou que la règle d'événement soit effacée.

> **Remarque**
>
> Les événements ne peuvent être effacés automatiquement que si un piège « clair » équivalent est défini et envoyé depuis votre instance Citrix Application Delivery Controller (ADC).
>
> Pour effacer manuellement un événement, vous pouvez effectuer les opérations suivantes :
>
> - Accédez à **Réseaux > Événements > Récapitulatif**des événements, choisissez une **catégorie**et sélectionnez un événement dans la catégorie, puis cliquez sur **Effacer**.
> - Vous pouvez également accéder à **Réseaux > Événements > Messages d'événements**.

> Choisissez un type d'instance, puis sélectionnez un événement dans la grille ci-dessous et cliquez sur **Effacer**.

Pour définir des notifications par e-mail répétées à partir de Citrix ADM :

1. Dans Citrix Application Delivery Management (ADM), accédez à **Réseaux** > **Événements** > **Règles**, puis cliquez sur **Ajouter** pour créer une règle.
2. Dans la page **Créer une règle**, définissez les paramètres de la règle.
3. Sous Actions relatives aux **règles d'événement**, cliquez sur **Ajouter une action**. Sélectionnez ensuite **Envoyer une action par e-mail** dans la liste déroulante **Type d'action** et sélectionnez une liste de **distribution par e-mail**.
4. Vous pouvez également ajouter une ligne d'objet personnalisée et un message utilisateur, et télécharger une pièce jointe à votre e-mail lorsqu'un événement entrant correspond à la règle configurée.
5. Activez la case à cocher **Répéter la notification par e-mail jusqu'à ce que l'événement soit désactivée**.



Suppression d'événements

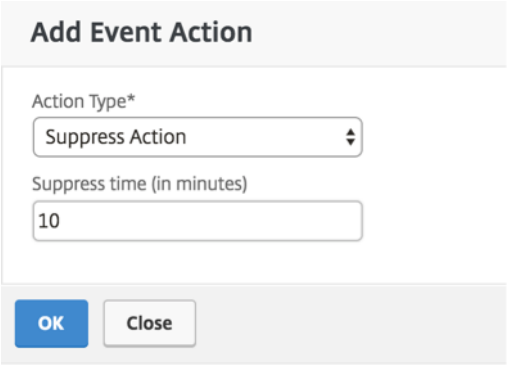
February 1, 2024

Lorsque vous choisissez l'**action d'événement Supprimer**l'action, vous pouvez configurer une période, en minutes, pour laquelle un événement est supprimé ou supprimé. Vous pouvez supprimer l'événement pendant au moins 1 minute.

> Remarque :
>
> Vous pouvez également configurer le temps de suppression comme 0 minutes et cela signifie temps infini. Si vous ne spécifiez aucune durée de temps, Citrix ADM considère l'heure de suppression comme zéro et n'expire jamais.

Pour supprimer des événements à l'aide de Citrix ADM :

1. Dans Citrix Application Delivery Management (ADM), accédez à **Réseaux** > **Événements** > **Règles**. Cliquez sur **Ajouter**.
2. Spécifiez tous les paramètres requis pour créer une règle.
3. Sous **Actions de règle d'événement**, cliquez sur **Ajouter une action** pour affecter des actions de notification à l'événement.
4. Dans la page **Ajouter une action d'événement**, sélectionnez **Supprimer** une **action dans la liste déroulante Type d'action** et spécifiez la période, en minutes, pendant laquelle un événement doit être supprimé.
5. Cliquez sur **OK**.



Créer des règles d'événement

February 1, 2024

Vous pouvez configurer des règles pour surveiller des événements spécifiques. Les règles facilitent la surveillance d'un grand nombre d'événements générés dans votre infrastructure.

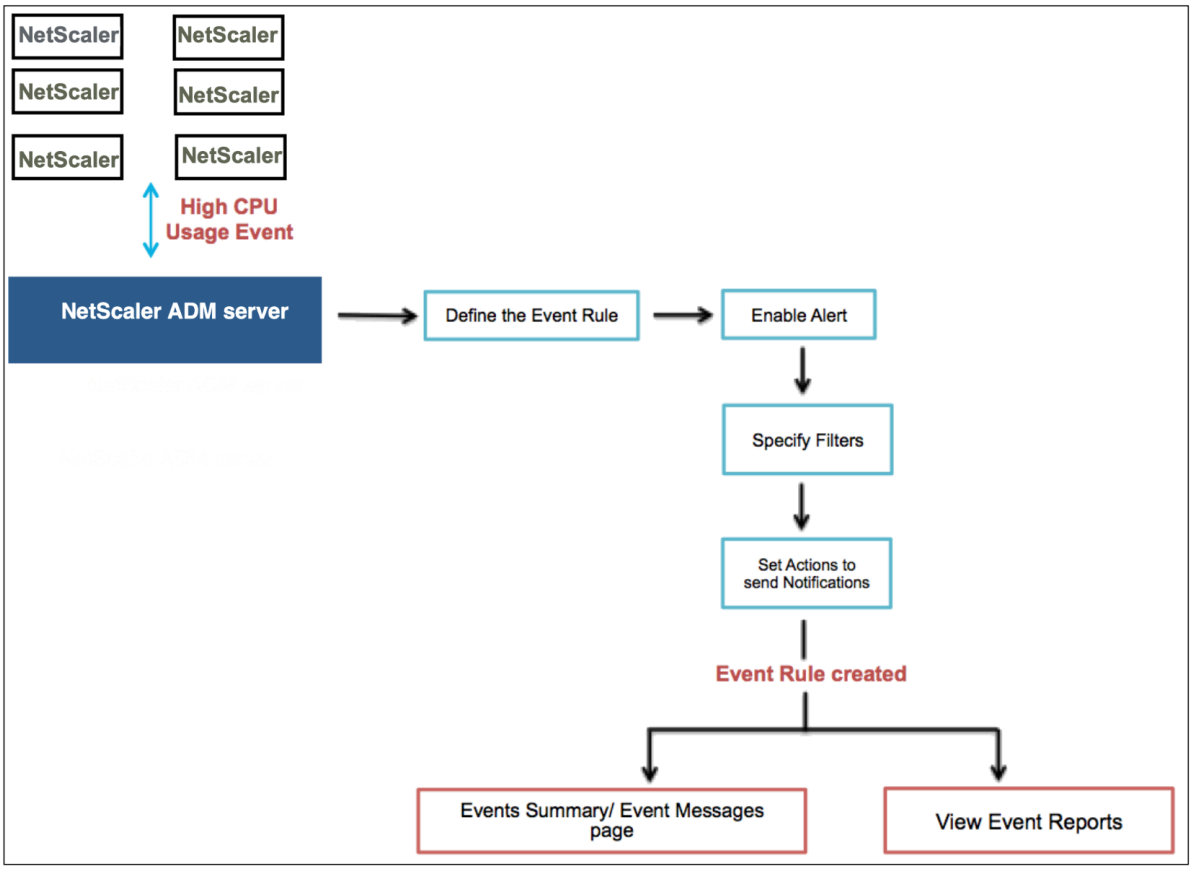
Vous pouvez filtrer un ensemble d'événements en configurant des règles avec des conditions spécifiques et en affectant des actions aux règles. Lorsque les événements générés répondent aux critères de filtre de la règle, l'action associée à la règle est exécutée. Les conditions pour lesquelles vous pouvez créer des filtres sont : gravité, instances Citrix Application Delivery Controller (Citrix ADC), catégorie, objets de défaillance, commandes de configuration et messages.

Vous pouvez affecter les actions suivantes aux événements :

- **Action d'envoi d'un e-mail** : envoyez un e-mail pour les événements qui correspondent aux critères du filtre.
- **Envoyer une action d'interruptions** : envoyer ou transférer des interruptions SNMP vers une destination d'interruptions externe
- **Exécuter l'action de commande** : Exécutez une commande lorsqu'un événement entrant répond à la règle configurée.
- **Exécuter une action de travail** : Exécuter une tâche concerne les événements qui correspondent aux critères de filtre que vous avez spécifiés.
- **Supprimer l'action** : supprime supprimer un événement pour une période spécifique.
- **Envoyer des notifications Slack** : envoyez des notifications sur le canal Slack configuré pour les événements qui correspondent aux critères du filtre.
- **Envoyer des notifications PagerDuty** : envoyez des notifications d'événements en fonction des configurations de PagerDuty pour les événements qui correspondent aux critères de filtre.
- **Envoyer des notifications ServiceNow** : générer automatiquement des incidents ServiceNow pour un événement qui correspond aux critères de filtre.

Pour plus d'informations, voir Ajouter des actions de règle d'événement

Vous pouvez également renvoyer les notifications à un intervalle spécifié jusqu'à ce qu'un événement soit effacé. Et vous pouvez personnaliser l'e-mail avec une ligne d'objet spécifique, un message utilisateur et une pièce jointe.



Par exemple, en tant qu'administrateur, vous pouvez surveiller les événements « utilisation élevée du processeur » pour des instances Citrix ADC spécifiques si ces événements peuvent entraîner une panne de vos instances Citrix ADC. Vous pouvez :

- Créez une règle pour surveiller les instances et spécifier une action qui vous envoie une notification par e-mail lorsqu'un événement de la catégorie « utilisation élevée du processeur » se produit.
- Planifiez l'exécution de la règle à une heure précise, par exemple entre 11 h et 23 h 00, afin de ne pas être averti chaque fois qu'un événement est généré.

La configuration d'une règle d'événement implique les tâches suivantes :

1. Définissez la règle
2. Choisissez la gravité de l'événement détecté par la règle
3. Spécifiez la catégorie de l'événement
4. Spécifier les instances Citrix ADC auxquelles la règle s'applique
5. Sélectionner des objets d'échec
6. Spécifier des filtres avancés

7. Spécifier les actions à effectuer lorsque la règle détecte un événement

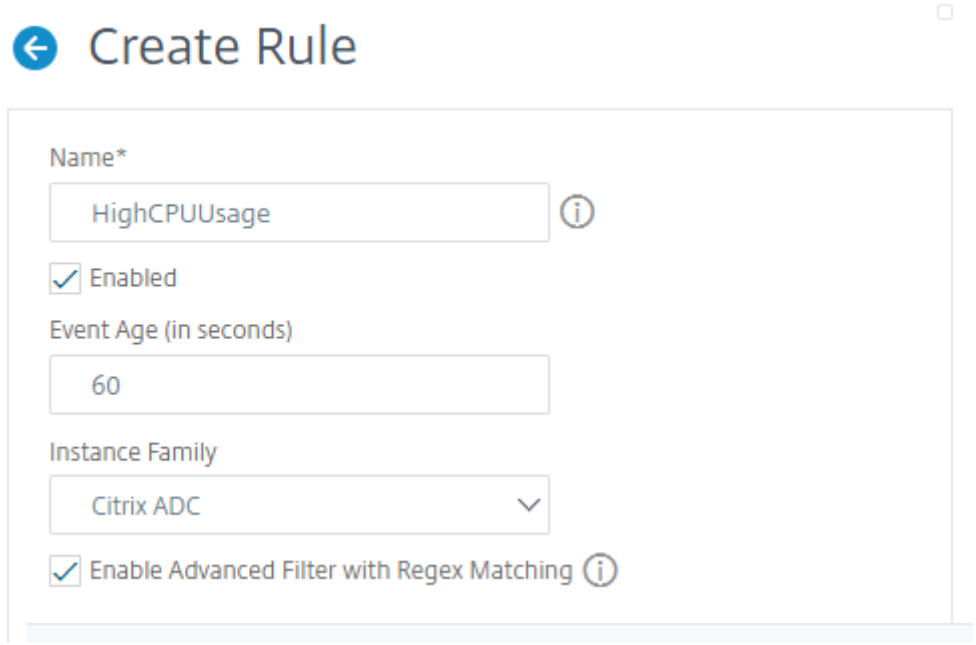
Étape 1 - Définir une règle d'événement

Accédez à **Réseaux** > **Événements** > **Règles**, puis cliquez sur **Ajouter** . Si vous souhaitez activer votre règle, activez la case à cocher **Activer la règle**.

Vous pouvez définir l'option **Event Age** pour spécifier l'intervalle de temps (en secondes) après lequel Citrix ADM actualise une règle d'événement.

> Remarque :
>
> La valeur minimale de l'âge de l'événement est de 60 secondes. Si vous conservez le champ **Âge** de l'événement vide, la règle d'événement est appliquée immédiatement après l'événement.

Sur la base de l'exemple ci-dessus, vous souhaiterez peut-être être averti par e-mail chaque fois que votre instance Citrix ADC connaît un événement « utilisation élevée du processeur » pendant 60 secondes ou plus. Vous pouvez définir l'âge de l'événement à 60 secondes, de sorte que chaque fois que votre instance Citrix ADC subit un événement « utilisation élevée du processeur » pendant 60 secondes ou plus, vous receviez une notification par e-mail contenant les détails de l'événement.



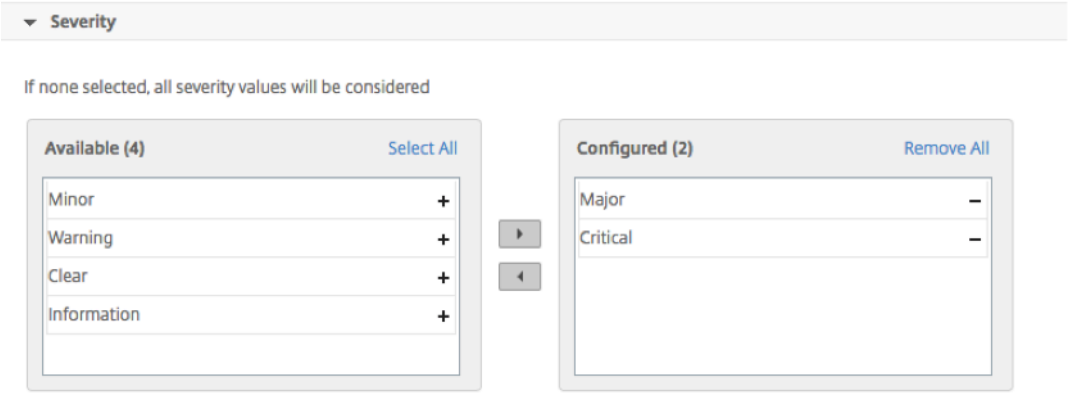
Vous pouvez également filtrer les règles d'événement par **famille d'instances** pour suivre l'instance Citrix ADC à partir de laquelle Citrix ADM reçoit un événement.

Si vous souhaitez inclure une expression régulière autre que la correspondance de formes avec un astérisque (*), sélectionnez **Activer le filtre avancé avec correspondance régulière**.

Étape 2 - Choisir la gravité de l'événement

Vous pouvez créer des règles d'événement qui utilisent les paramètres de gravité par défaut. La gravité indique la gravité actuelle des événements auxquels vous souhaitez ajouter la règle des événements.

Vous pouvez définir les niveaux de gravité suivants : Critique, Majeur, Mineur, Avertissement, Effacer et Informations.

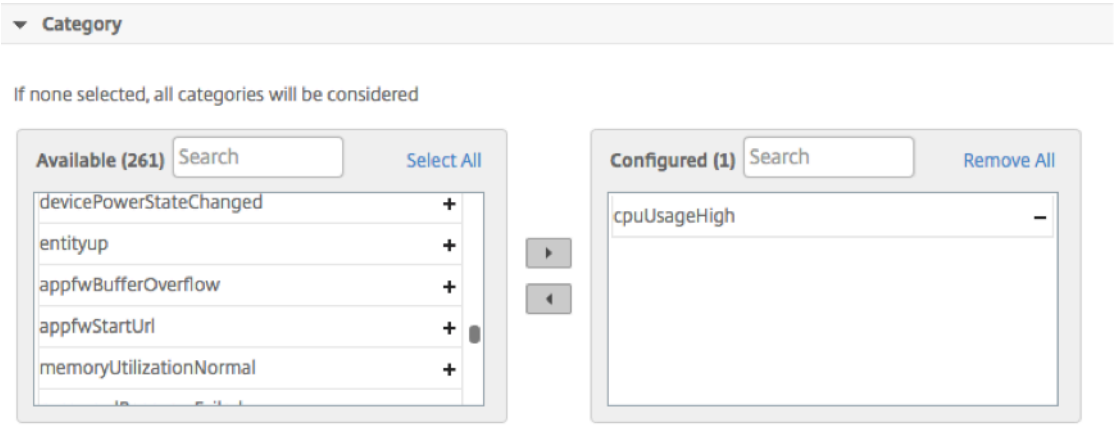


> **Remarque**
>
> Vous pouvez configurer la gravité des événements génériques et spécifiques à Advanced. Pour modifier la gravité des événements pour les instances Citrix ADC gérées sur Citrix ADM, accédez à **Réseaux** > **Événements** > **Paramètres**des événements. Choisissez la **catégorie** pour laquelle vous souhaitez configurer la gravité de l'événement, puis cliquez sur **Configurer la gravité** . Attribuez un nouveau niveau de gravité et cliquez sur **OK**.

Étape 3 - Spécifiez la catégorie d'événement

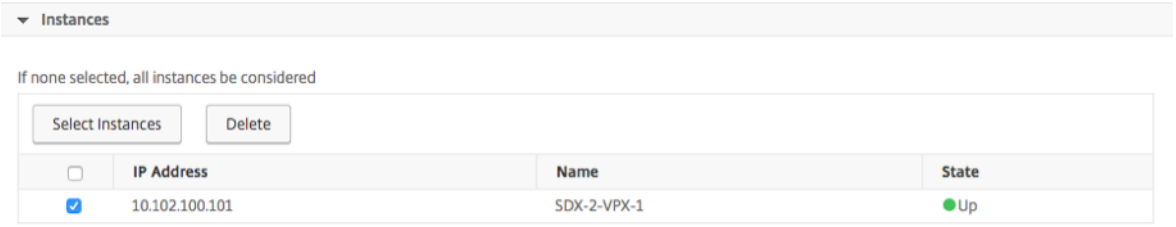
Vous pouvez spécifier la ou les catégories des événements générés par vos instances Citrix ADC. Toutes les catégories sont créées sur des instances Citrix ADC. Ces catégories sont ensuite mappées avec Citrix ADM qui peut être utilisé pour définir des règles d'événements. Sélectionnez la catégorie à prendre en compte et déplacez-la de la table **Disponible** vers la table **configurée**.

Dans l'exemple ci-dessus, vous devrez choisir « CPUusageHigh » comme catégorie d'événement dans le tableau affiché.



Étape 4 - Spécifier les instances de Citrix ADC

Sélectionnez les adresses IP des instances Citrix ADC pour lesquelles vous souhaitez définir la règle d'événement. Dans la section **Instances**, cliquez sur **Sélectionner des instances**. Dans la page **Sélectionner des instances**, choisissez vos instances, puis cliquez sur **Sélectionner** .



Étape 5 - Sélectionner les objets de défaillance

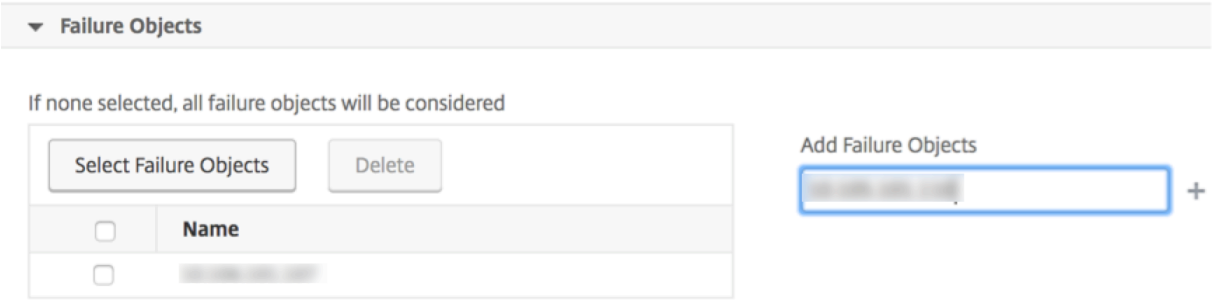
Vous pouvez sélectionner un objet de défaillance dans la liste fournie ou ajouter un objet de défaillance pour lequel un événement a été généré. Vous pouvez également spécifier une expression régulière pour ajouter des objets de défaillance. En fonction de l'expression régulière spécifiée, les objets défaillants sont automatiquement ajoutés à la liste. Les objets d'échec sont des instances d'entité ou des compteurs pour lesquels un événement a été généré.

> **Important**
>
> Pour répertorier les objets d'échec à l'aide d'une expression régulière, sélectionnez **Activer le filtre avancé avec correspondance d'expressions régulières** à l'étape 1.

L'objet d'échec affecte la façon dont un événement est traité et s'assure qu'il reflète exactement le problème tel qu'il a été notifié. Ce filtre vous permet de suivre rapidement les problèmes liés aux objets défaillants et d'identifier la cause d'un problème. Par exemple, si un utilisateur rencontre des

problèmes de connexion, l'objet d'échec est le nom d'utilisateur ou le mot de passe, tel que `nsroot`.

Cette liste peut contenir des noms de compteur pour tous les événements liés au seuil, des noms d'entité pour tous les événements liés à l'entité, des noms de certificats pour les événements liés au certificat, etc.

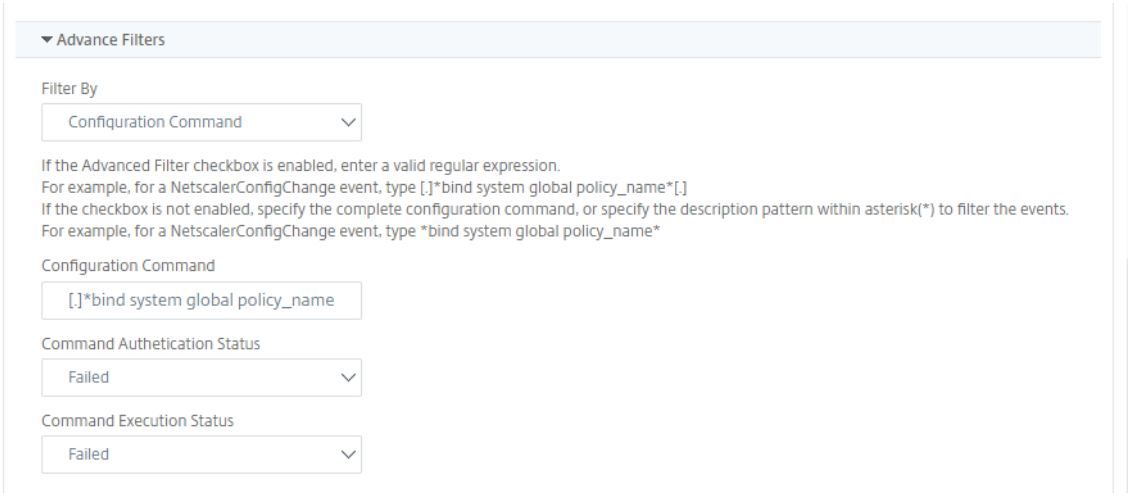


Étape 6 - Spécifier les filtres avancés

Vous pouvez filtrer davantage une règle d'événement en :

- **Commandes de configuration** : vous pouvez spécifier la commande de configuration complète ou spécifier une expression régulière pour filtrer les événements.

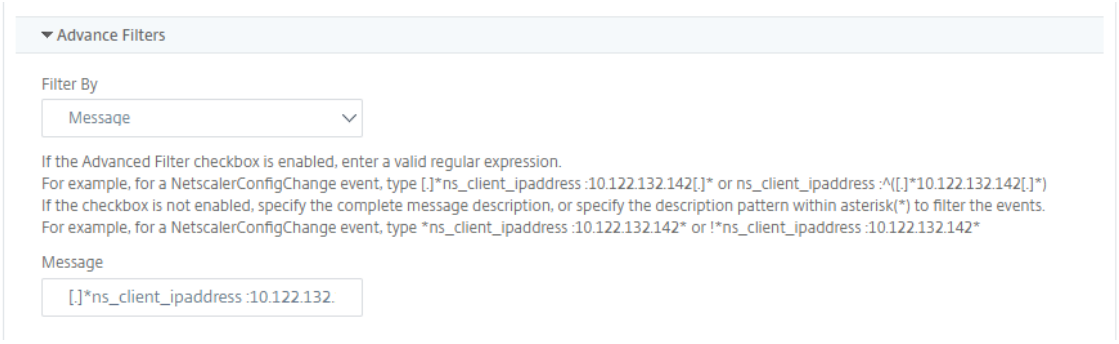
  Vous pouvez également filtrer la règle d'événement en fonction de l'état d'authentification de la commande et/ou de son état d'exécution. Par exemple, pour un `NetscalerConfigChange event`, tapez `[.]*bind system global policy_name[.]*`.



- **Messages** : vous pouvez spécifier la description complète du message ou spécifier une expression régulière pour filtrer les événements.
  Par exemple, pour un `NetscalerConfigChange` événement, tapez `[.]*ns_client_ipaddress`


```
:10.122.132.142[.]* or ns_client_ipaddress :^([.]*10.122.132.142[.]*)
```

.



Étape 7 - Ajouter des actions de règle d'événement

Vous pouvez ajouter des actions de règle d'événement pour affecter des actions de notification à un événement. Ces notifications sont envoyées ou exécutées lorsqu'un événement répond aux critères de filtre définis ci-dessus. Vous pouvez ajouter les actions d'événement suivantes :

- Envoyer un e-mail Action
- Envoyer une action de piège
- Exécuter l'action de commande
- Exécuter une action de travail
- Supprimer l'action
- Envoyer des notifications Slack
- Envoyer des notifications PagerDuty
- Envoyer des notifications ServiceNow

Pour définir une action de règle d'événement de messagerie électronique

Lorsque vous choisissez le type d'action d'action Envoyer un e-mail, un e-mail est déclenché lorsque les événements répondent aux critères de filtre définis. Vous devrez soit créer une liste de distribution d'e-mails en fournissant les détails du serveur de messagerie ou du profil de messagerie, soit sélectionner une liste de distribution d'e-mails que vous avez précédemment créée.

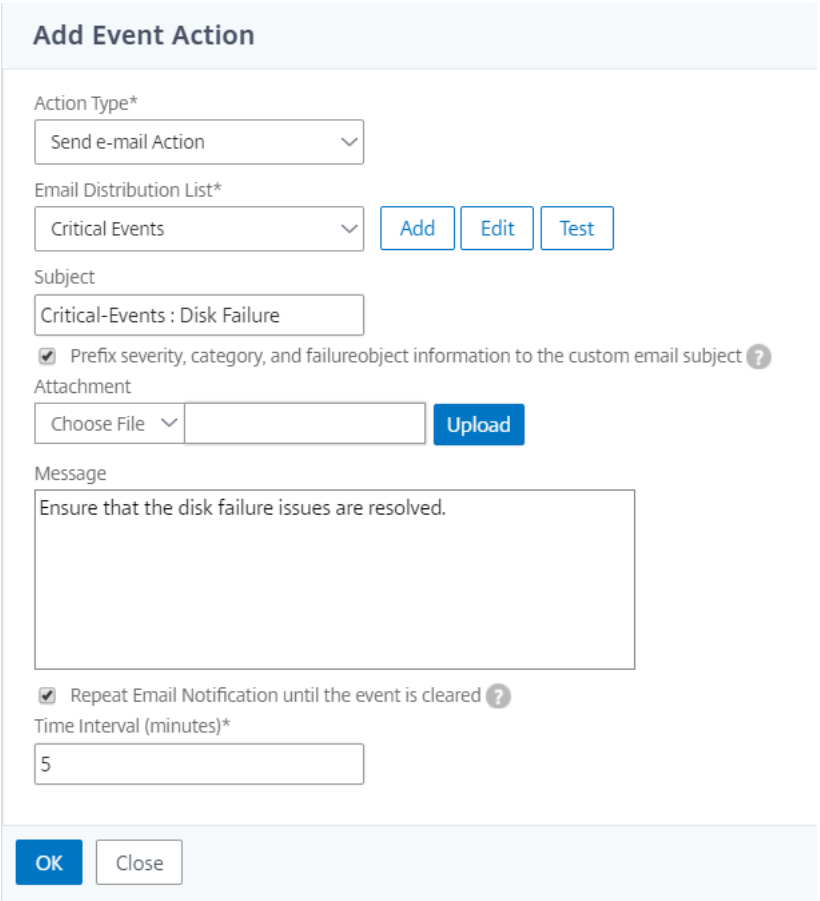
En raison du nombre élevé de serveurs virtuels configurés dans Citrix ADM, vous pouvez recevoir un nombre élevé d'e-mails chaque jour. Les e-mails ont une ligne d'objet par défaut qui fournit des informations sur la gravité de l'événement, la catégorie de l'événement et l'objet de la défaillance. Mais la ligne d'objet ne contient aucune information sur le nom du serveur virtuel d'où proviennent ces

événements. Vous avez maintenant la possibilité d'inclure des informations supplémentaires, telles que le nom de l'entité affectée, c'est-à-dire le nom de l'objet défaillant.

Vous pouvez également ajouter une ligne d'objet personnalisée et un message utilisateur, et télécharger une pièce jointe à votre e-mail lorsqu'un événement entrant correspond à la règle configurée.

Lors de l'envoi d'e-mails pour les notifications d'événements, vous pouvez envoyer un e-mail de test pour tester les paramètres configurés. Le bouton « Tester » vous permet désormais d'envoyer un e-mail de test après avoir configuré un serveur de messagerie, les listes distribuées associées et d'autres paramètres. Cette fonctionnalité garantit que les paramètres fonctionnent correctement.

Vous pouvez également vous assurer que tous les événements critiques sont traités et qu'aucune notification par e-mail importante n'est oubliée, en cochant la case **Répéter la notification par e-mail jusqu'à ce que l'événement soit effacé** pour envoyer des notifications par e-mail répétées concernant les règles d'événement répondant aux critères que vous avez sélectionnés. Par exemple, si vous avez créé une règle d'événement pour les instances qui impliquent des défaillances de disque et que vous souhaitez être averti jusqu'à ce que le problème soit résolu, vous pouvez choisir de recevoir des notifications par e-mail répétées sur ces événements.



Pour définir une action de règle d'événement d'interruption

Lorsque vous choisissez le type **d'action d'événement Envoyer une action d'interruption**, les interruptions SNMP sont envoyées ou transférées vers une destination d'interruption externe. En définissant une liste de distribution des interruptions (ou une destination et des détails sur le profil des interruptions), des messages d'interruption sont envoyés à des auditeurs d'interruptions spécifiques lorsque les événements répondent aux critères de filtre définis.

Pour définir l'action Exécuter la commande

Lorsque vous choisissez l'**action événementielle Run Command** Action, vous pouvez créer une commande ou un script qui peut être exécuté sur Citrix ADM pour les événements correspondant à un critère de filtre particulier.

Vous pouvez également définir les paramètres suivants pour le script **Run Command Action** :

Paramètre	Description
$source	Ce paramètre correspond à l'adresse IP source de l'événement reçu.
Catégorie $	Ce paramètre correspond au type de pièges défini dans la catégorie du filtre
$entité	Ce paramètre correspond aux instances ou aux compteurs d'entités pour lesquels un événement a été généré. Il peut inclure les noms de compteur pour tous les événements liés aux seuils, les noms d'entités pour tous les événements liés aux entités et les noms de certificats pour tous les événements liés aux certificats.
$severity	Ce paramètre correspond à la gravité de l'événement.
$failureobj	L'objet Failure affecte la façon dont un événement est traité et garantit que l'objet Failure reflète le problème exact tel qu'il a été notifié. Cela peut être utilisé pour détecter rapidement les problèmes et identifier la raison de l'échec, au lieu de simplement signaler les événements bruts.

> **Remarque**
>
> Pendant l'exécution de la commande, ces paramètres sont remplacés par des valeurs réelles.

Par exemple, considérez que vous souhaitez définir une action de commande d'exécution lorsque l'état d'un serveur virtuel d'équilibrage de charge est **Arrêté**. En tant qu'administrateur, vous pouvez envisager de proposer une solution rapide en ajoutant un autre serveur virtuel. Dans Citrix ADM, vous pouvez :

- Écrivez un fichier script (.sh).

  Voici un exemple de fichier de script (.sh) :

```
#!/bin/sh
source=$1
failureobj=$2
payload='{
"params":{
"warning":"YES" }
,"lbvserver":{
"name":"'$failureobj'","servicetype":"HTTP","ipv46":"x.x.x.x","
   port":"80","td":"","m":"IP","state":"ENABLED","rhistate":"
   PASSIVE","appflowlog":"ENABLED","
bypassaaaa":"NO","retainconnectionsoncluster":"NO","comment":"" }
 }
'
url="http://$source/nitro/v1/config/lbvserver"
curl --insecure -basic -u nsroot:nsroot -H "Content-type:
   application/json" -X POST -d $payload $url

<!--NeedCopy-->
```

- Enregistrez le fichier .sh dans n'importe quel emplacement persistant de l'agent Citrix ADM. Par exemple, `/var`.
- Indiquez l'emplacement du fichier .sh dans Citrix ADM à exécuter lorsque les critères de règle sont remplis.

Pour définir l'action **Exécuter la commande** pour créer un nouveau serveur virtuel :

1. Définissez la règle
2. Sélectionnez la gravité de l'événement
3. Sélectionnez la catégorie d'événement : **entitydown**
4. Sélectionnez l'instance sur laquelle le serveur virtuel est configuré
5. Sélectionnez ou créez un objet de défaillance pour le serveur virtuel
6. Sous **Actions des règles d'événement**, cliquez sur **Ajouter une action** et sélectionnez **Exécuter une action de commande** dans la liste des **types d'action** .

7. Sous **Liste d'exécution des commandes**, cliquez sur **Ajouter**.

   La page Créer une liste de distribution de commandes s'affiche.

   a) Dans **Nom du profil**, spécifiez un nom de votre choix

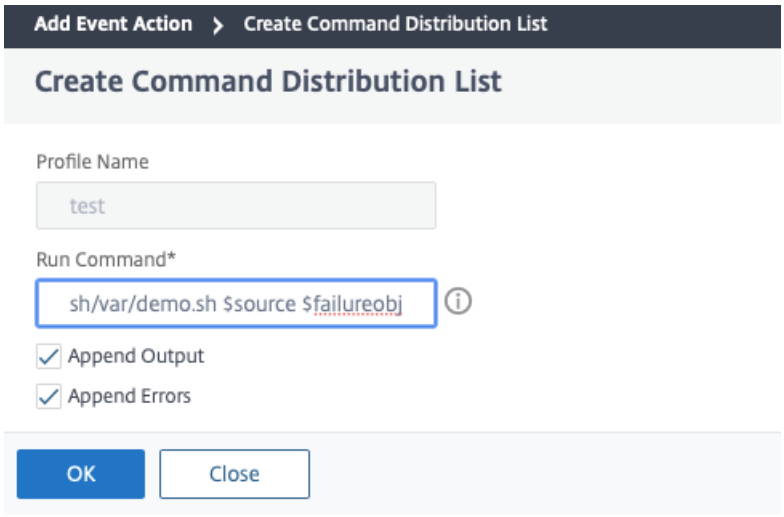
   b) Dans **Exécuter la commande**, spécifiez l'emplacement de l'agent Citrix ADM, où le script doit être exécuté. Par exemple : `/sh/var/demo.sh $source $failureobj`.

   c) Sélectionnez **Ajouter la sortie** et **Ajouter les erreurs**

   > **Remarque**
   >
   > Vous pouvez activer les options **Ajout de sortie** et **Ajout d'erreurs** si vous souhaitez stocker la sortie et les erreurs générées (le cas échéant) lorsque vous exécutez un script de commande dans les fichiers journaux du serveur Citrix ADM. Si vous n'activez pas ces options, Citrix ADM supprime toutes les sorties et erreurs générées lors de l'exécution du script de commande.

   d) Cliquez sur **Créer**.

8. Dans la page **Ajouter une action d'événement**, cliquez sur **OK** .

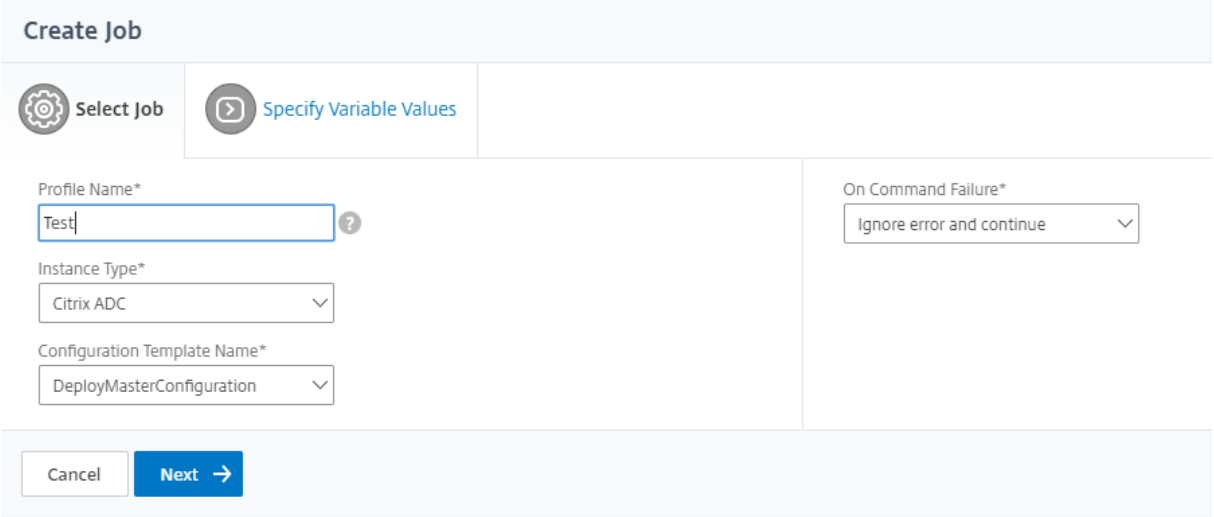


> **Remarque**
>
> Vous pouvez activer les options **Ajout de sortie** et **Ajout d'erreurs** si vous souhaitez stocker la sortie et les erreurs générées (le cas échéant) lorsque vous exécutez un script de commande dans les fichiers journaux du serveur Citrix ADM. Si vous n'activez pas ces options, Citrix ADM supprime toutes les sorties et erreurs générées lors de l'exécution du script de commande.

Pour définir l'action de `Execute` travail

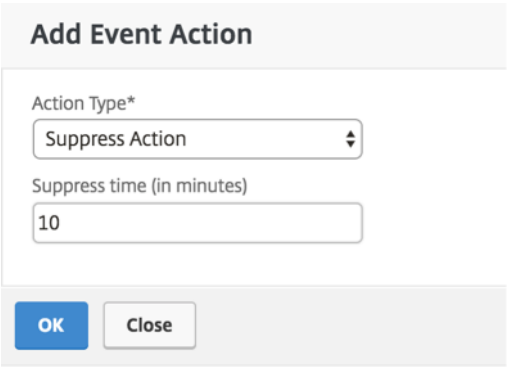
En créant un profil avec des tâches de configuration, un travail est exécuté en tant que travail intégré ou personnalisé pour les instances Citrix ADC, Citrix ADC SDX et Citrix SD-WAN WO, pour les événements et les alarmes correspondant aux critères de filtre que vous avez spécifiés.

1. Sous **Actions de règle d'événement**, cliquez sur **Ajouter une action** et sélectionnez **Exécuter une action de travail** dans la liste déroulante **Type d'action** .
2. Créez un profil avec une tâche à exécuter lorsque les événements répondent aux critères de filtre définis.
3. Lors de la création d'une tâche, spécifiez un nom de profil, le type d'instance, le modèle de configuration et l'action que vous souhaitez effectuer en cas d'échec des commandes de la tâche.
4. En fonction du type d'instance sélectionné et du modèle de configuration choisi, spécifiez vos valeurs de variables et cliquez sur **Terminer** pour créer le travail.



Pour définir l'action Supprimer

Lorsque vous choisissez l'**action d'événement Supprimer** l'action, vous pouvez configurer une période, en minutes, pendant laquelle un événement est supprimé ou supprimé. Vous pouvez supprimer l'événement pendant au moins 1 minute.



Pour définir des notifications Slack à partir de Citrix ADM

Configurez le canal Slack requis en fournissant le nom du profil et l'URL du webhook dans l'interface graphique Citrix ADM. Les notifications d'événement sont ensuite envoyées à ce canal. Vous pouvez configurer plusieurs canaux Slack pour recevoir ces notifications

1. Dans Citrix ADM, accédez à**Réseaux**>**Événements**>**Règles**, puis cliquez sur**Ajouter**pour créer une règle.
2. Dans la page **Créer une règle**, définissez les paramètres de règle tels que la gravité et la catégorie. Sélectionnez les instances ainsi que les objets de défaillance qui doivent être surveillés.
3. Sous **Actions relatives aux règles d'événement**, cliquez sur **Ajouter une action**. Sélectionnez ensuite **Envoyer des notifications Slack** dans la liste des **types d'action**, puis sélectionnez **Liste des profils Slack**.
4. Vous pouvez également ajouter une liste de profils Slack en cliquant sur **Ajouter** en regard du champ **Liste des profils Slack**.
5. Entrez les paramètres suivants pour créer une liste de profils :

    a) **Nom du profil**. Entrez un nom pour la liste de profils à configurer sur Citrix ADM

    b) **Nom de la chaîne**. Entrez le nom de la chaîne Slack à laquelle les notifications d'événements doivent être envoyées.

    c) **URL du webhook**. Entrez l'URL du webhook de la chaîne que vous avez saisie précédemment. Les webhooks entrants sont un moyen simple de publier des messages provenant de sources externes dans Slack. L'URL est liée en interne au nom du canal et toutes les notifications d'événement sont envoyées à cette URL pour être publiées sur le canal Slack désigné. Voici un exemple de webhook : https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK

6. Cliquez sur **Créer**, puis sur **OK** dans la fenêtre **Ajouter une action d'événement** .

> **Remarque**
>
> Vous pouvez également ajouter les profils Slack en accédant à **Système** > **Notifications** > **Profils Slack**. Cliquez sur **Ajouter** et créez le profil comme décrit dans la section précédente.

Vous pouvez consulter l'état des profils Slack que vous avez créés.

Votre règle d'événement est maintenant créée avec des filtres appropriés et des actions de règle d'événement bien définies.

Pour définir les notifications PagerDuty à partir de Citrix ADM

Vous pouvez ajouter un profil PagerDuty en tant qu'option dans Citrix ADM pour surveiller les notifications d'incident en fonction de vos configurations PagerDuty. PagerDuty vous permet de configurer les notifications par e-mail, SMS, notification push et appel téléphonique sur le numéro enregistré.

Avant d'ajouter un profil PagerDuty dans Citrix ADM, assurez-vous d'avoir terminé les configurations requises dans PagerDuty. Pour plus d'informations, consultez la documentation de PagerDuty.

Vous pouvez sélectionner votre profil PagerDuty comme l'une des options pour obtenir des notifications pour les fonctionnalités suivantes :

- **Événements** : liste des événements générés pour les instances Citrix ADC.
- **Licences** : liste des licences actuellement actives, sur le point d'expirer, etc.
- **Certificats SSL** : liste des certificats SSL ajoutés aux instances Citrix ADC.

Pour ajouter un profil PagerDuty dans ADM :

1. Ouvrez une session sur Citrix ADM à l'aide des informations d'identification de l'administrateur.
2. Accédez à **Système** > **Notifications** > **Profils PagerDuty**.
3. Cliquez sur **Ajouter** pour créer un profil.
4. Dans la page Créer un profil PagerDuty :
   a) Indiquez le nom de profil de votre choix.
   b) Entrez la **clé d'intégration**.
      Vous pouvez obtenir la clé d'intégration sur votre portail PagerDuty.
   c) Cliquez sur **Créer**.

Cas d'utilisation :

Envisagez un scénario dans lequel vous :

- souhaitez envoyer des notifications à votre profil PagerDuty.
- J'ai configuré l'appel téléphonique comme option dans PagerDuty pour recevoir des notifications.
- vous souhaitez recevoir des alertes d'appels téléphoniques pour les événements Citrix ADC.

Pour configurer :

a) Accédez à **Événements** > **Règles**

b) Sur la page **Créer une règle**, configurez tous les autres paramètres pour créer une règle.

c) Sous **Actions de création de règles**, cliquez sur **Ajouter une action**.

La page **Ajouter une action d'événement** s'affiche.

i. Sous **Type d'action**, sélectionnez **Envoyer les notifications PagerDuty**.

ii. Sélectionnez votre profil PagerDuty et cliquez sur **OK**.

Une fois la configuration terminée, chaque fois qu'un nouvel événement est généré pour l'instance Citrix ADC, vous recevrez un appel téléphonique. À partir de l'appel téléphonique, vous pouvez décider de :

- Reconnaissez l'événement
- Marquez-le comme résolu
- Transférer à un autre membre de l'équipe

Pour générer automatiquement des incidents ServiceNow à partir de Citrix ADM

Vous pouvez générer automatiquement des incidents ServiceNow pour les événements Citrix ADM en sélectionnant le profil ServiceNow sur l'interface graphique Citrix ADM. Vous devez choisir le profil ServiceNow dans Citrix ADM pour configurer une règle d'événement.

Avant de configurer une règle d'événement pour générer automatiquement des incidents ServiceNow, intégrez Citrix ADM à une instance ServiceNow. Pour plus d'informations, consultez Configurer l'adaptateur ITSM pour ServiceNow.

Pour configurer une règle d'événement, accédez à **Événements** > **Règles** .

1. Sur la page **Créer une règle**, configurez tous les autres paramètres pour créer une règle.
2. Sous **Actions de création de règles**, cliquez sur **Ajouter une action**.

   La page **Ajouter une action d'événement** s'affiche.

   a) Dans **Type d'action**, sélectionnez **Envoyer des notifications ServicNow**.

b) Dans le **profil ServiceNow**, sélectionnez le profil **Citrix_Workspace_SN** dans la liste.

c) Cliquez sur **OK**.

Modifier la gravité signalée des événements qui se produisent sur les instances Citrix ADC

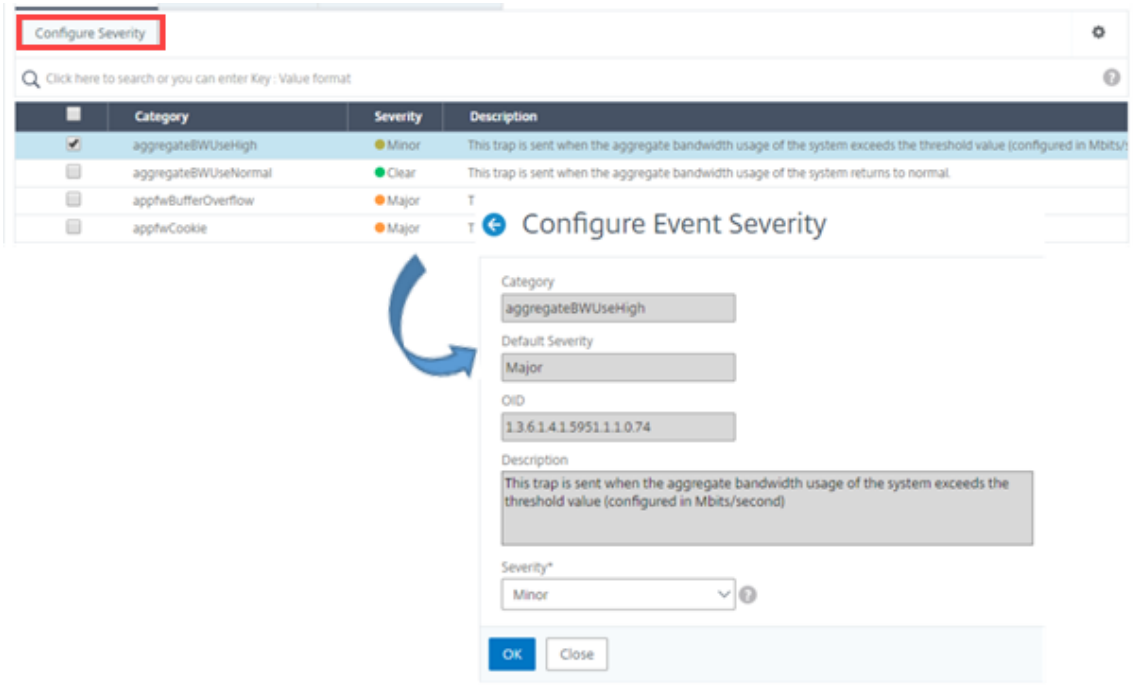
February 1, 2024

Vous pouvez gérer les rapports d'événements générés sur tous vos appareils, de sorte que vous pouvez afficher les détails d'événements concernant un événement particulier sur une instance particulière et afficher les rapports en fonction de la gravité de l'événement. Vous pouvez créer des règles d'événement qui utilisent les paramètres de gravité par défaut, et vous pouvez modifier les paramètres de gravité. Vous pouvez configurer la gravité des événements génériques et spécifiques à l'entreprise.

Vous pouvez définir les niveaux de gravité suivants : Critique, Majeur, Mineur, Avertissement et Clair.

Pour modifier la gravité de l'événement :

1. Accédez à **Réseaux > Événements > Paramètres d'événement**.
2. Cliquez sur l'onglet correspondant au type d'instance de Citrix Application Delivery Controller (ADC) que vous souhaitez modifier. Sélectionnez ensuite la catégorie dans la liste et cliquez sur **Configurer la gravité**.
3. Dans **Configurer la gravité de l'événement**, sélectionnez le niveau de gravité dans la liste déroulante.
4. Cliquez sur **OK**.

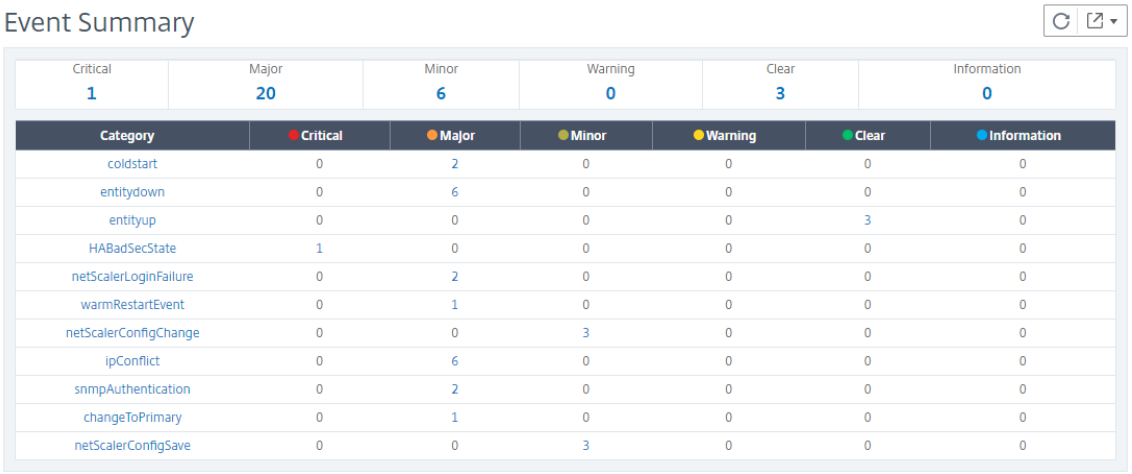


Afficher le résumé des événements

February 1, 2024

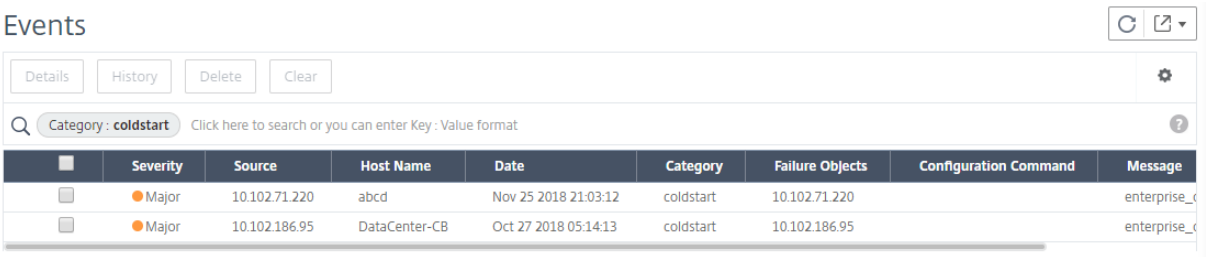
Vous pouvez désormais afficher une page Récapitulatif des événements pour surveiller les événements et les interruptions reçus sur votre serveur ADM (Application Delivery Management) Citrix. Accédez à **Réseaux** > **Événements**. La page Récapitulatif des événements affiche les informations suivantes sous forme de tableau :

- **Résumé de tous les événements reçus par Citrix ADM**. Les événements sont répertoriés par catégorie et les différentes sévérité sont affichées dans différentes colonnes : Critique, Majeur, Mineur, Avertissement, Effacer et Informations. Par exemple, un événement critique se produit lorsqu'une instance de Citrix Application Delivery Controller (ADC) s'arrête et arrête d'envoyer des informations au serveur Citrix ADM. Pendant l'événement, une notification est envoyée à un administrateur, expliquant la raison pour laquelle l'instance est en panne, la durée pendant laquelle elle a été arrêtée, etc. L'événement est ensuite enregistré sur la page Résumé des événements, sur laquelle vous pouvez consulter un résumé et accéder aux détails de l'événement.



- **Nombre de pièges reçus pour chaque catégorie**. Nombre de pièges reçus, classés par gravité. Par défaut, chaque interruption envoyée à partir d'instances Citrix ADC à Citrix ADM a une gravité attribuée, mais en tant qu'administrateur réseau, vous pouvez spécifier sa gravité dans l'interface graphique Citrix ADM.

Si vous cliquez sur un type de catégorie ou une interruption, vous accédez à la page **Événements**, sur laquelle des filtres tels que Catégorie et Gravité sont présélectionnés. Cette page affiche plus d'informations sur l'événement, telles que l'adresse IP et le nom d'hôte de l'instance Citrix ADC, la date à laquelle l'interruption a été reçue, la catégorie, les objets d'échec, l'exécution de la commande de configuration et la notification de message.



Afficher les sévérité des événements et les détails des interruptions SNMP

February 1, 2024

Lorsque vous créez un événement et ses paramètres dans Citrix Application Delivery Management (ADM), vous pouvez afficher l'événement immédiatement sur la page Récapitulatif des événements. De même, vous pouvez afficher et surveiller l'intégrité, le temps de fonctionnement, les modèles et les versions de toutes les instances de Citrix Application Delivery Controller (ADC) ajoutées à votre

serveur Citrix ADM en détail dans le tableau de bord de l'infrastructure.

Dans le tableau de bord Infrastructure, vous pouvez désormais masquer les valeurs non pertinentes afin de pouvoir afficher et surveiller plus facilement les informations telles que les événements par gravité, intégrité, temps de fonctionnement, modèles et version des instances Citrix ADC en détail.

Par exemple, les événements présentant un niveau de gravité **critique** peuvent se produire rarement. Toutefois, lorsque ces événements critiques se produisent sur votre réseau, vous souhaiterez peut-être étudier plus en détail, dépanner et surveiller où et quand l'événement s'est produit. Si vous sélectionnez tous les niveaux de gravité sauf Critique, le graphique affiche uniquement les occurrences des événements critiques. En outre, en cliquant sur le graphique, vous accédez à la page **Événements basés sur la gravité**, où vous pouvez voir tous les détails concernant le moment où un événement critique s'est produit pendant la durée sélectionnée : la source de l'instance, la date, la catégorie et la notification de message envoyée lorsque l'événement critique s'est produit.

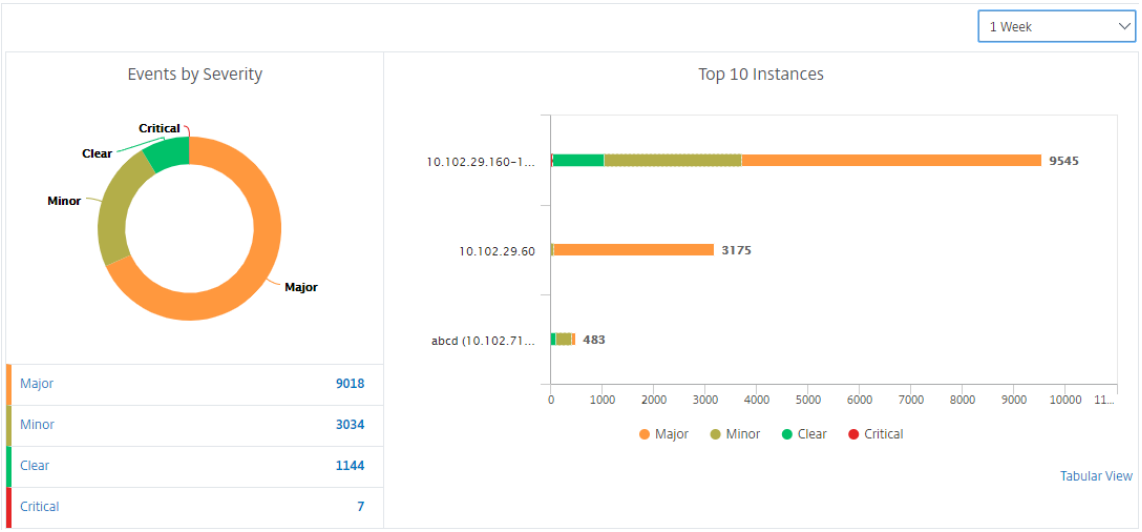
De même, vous pouvez afficher l'intégrité d'une instance Citrix VPX sur le tableau de bord. Vous pouvez masquer le temps pendant lequel l'instance était en cours d'exécution et afficher uniquement les heures où elle était hors service. En cliquant sur le graphique, vous accédez à la page de cette instance, où le filtre *hors service* est déjà appliqué, et voyez des détails tels que le nom d'hôte, le nombre de requêtes HTTP reçues par seconde, l'utilisation du processeur, etc. Vous pouvez également sélectionner l'instance et consulter le tableau de bord de l'instance Citrix particulière pour plus de détails.

Pour sélectionner des événements spécifiques par gravité dans Citrix ADM :

1. Connectez-vous à Citrix ADM à l'aide de vos informations d'identification d'administrateur.
2. Accédez à **Réseaux > Tableau de bord**

   Ou

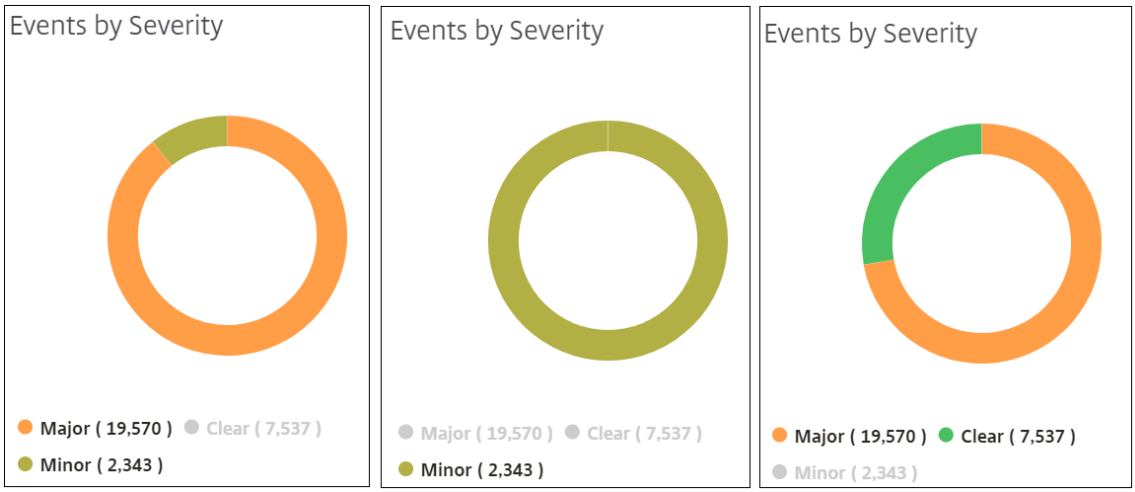
   Accédez à **Réseaux > Événements > Rapports**.
3. Dans le menu situé dans le coin supérieur droit de la page, sélectionnez la durée pour laquelle vous souhaitez afficher les événements par gravité.



4. Le graphique **Événements par gravité**affiche une représentation visuelle de tous les événements par gravité. Différents types d'événements sont représentés sous forme de sections colorées différentes, et la longueur de chaque section correspond au nombre total d'événements de ce type de gravité.
5. Vous pouvez cliquer sur chaque section du graphique en donut pour afficher la page **Événements basés sur la gravité** correspondante, qui affiche les détails suivants pour la gravité sélectionnée pour la durée sélectionnée :

   - Source de l'instance
   - Données de l'événement
   - Catégorie d'événements générés par l'instance Citrix ADC
   - Notification de message envoyée

   > **Remarque**
   >
   > Sous le diagramme en beignet, vous pouvez voir une liste des gravités qui sont représentées dans le graphique. Par défaut, un graphique en donut affiche tous les événements de tous les types de gravité. Par conséquent, tous les types de gravité de la liste sont mis en surbrillance. Vous pouvez basculer les types de gravité pour afficher et surveiller plus facilement la gravité de votre choix.



Pour afficher les détails des interruptions SNMP Citrix ADC sur Citrix ADM :

Vous pouvez désormais afficher les détails de chaque interruption SNMP reçue de ses instances Citrix ADC gérées sur le serveur Citrix ADM dans la page **Paramètres d'événement**. Accédez à **Réseaux** > **Événements** > **Paramètres d'événement**. Pour une interruption spécifique reçue de votre instance, vous pouvez afficher les détails suivants sous forme de tableau :

- **Catégorie** : spécifie la catégorie de l'instance à laquelle appartient l'événement.
- **Gravité** - La gravité de l'événement est indiquée par les couleurs et son type de gravité.
- **Description** - Spécifie les messages associés à l'événement.

Par exemple, dans le cas d'un événement de la catégorie **MonRespTimeoutBelowThresh**, la description du piège s'affiche sous la forme « Ce piège est envoyé lorsque le délai de réponse d'une sonde de surveillance revient à la normale, inférieur au seuil défini ».

Afficher et exporter les messages syslog Citrix ADC

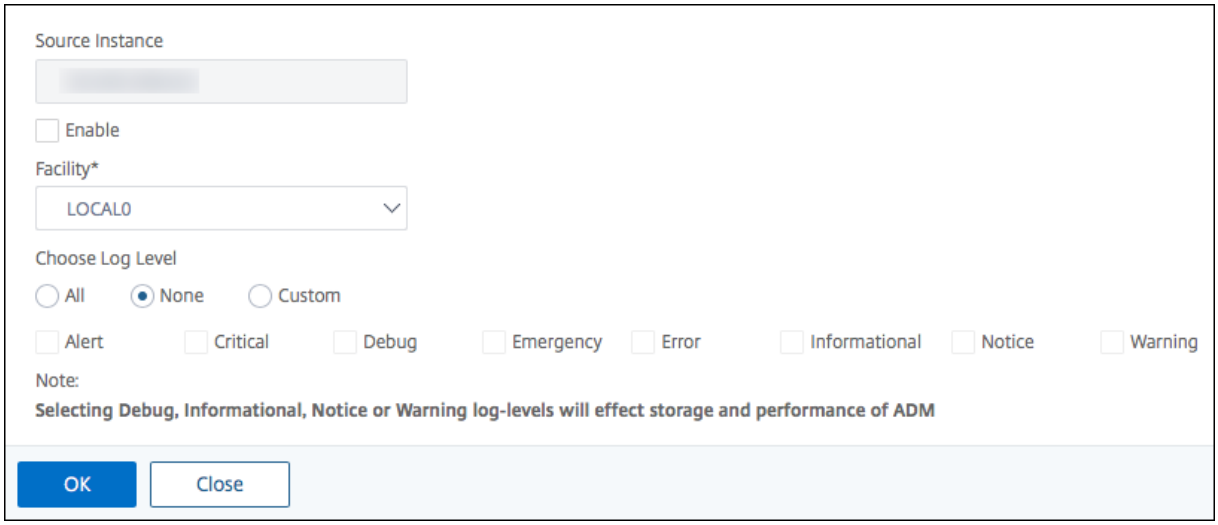
February 1, 2024

À partir de votre logiciel ADM, vous pouvez surveiller les événements syslog générés sur vos instances Citrix Application Delivery Controller (ADC). Pour cela, vous devez configurer ADM en tant que serveur syslog pour vos instances Citrix ADC. Après avoir configuré ADM, tous les messages syslog sont redirigés des instances ADC vers ADM.

Configurer ADM en tant que serveur syslog

Procédez comme suit pour configurer ADM en tant que serveur syslog :

1. À partir de l'interface graphique ADM, accédez à **Réseaux > Instances**.
2. Sélectionnez l'instance Citrix ADC à partir de laquelle vous souhaitez que les messages syslog soient collectés et affichés dans Citrix ADM.
3. Dans la liste **Sélectionner une action**, sélectionnez **Configurer Syslog**.
4. Cliquez sur **Activer**.
5. Dans la liste déroulante **Installation**, sélectionnez une ressource locale ou au niveau de l'utilisateur.
6. Sélectionnez le niveau de journalisation requis pour les messages Syslog.
7. Cliquez sur **OK**.

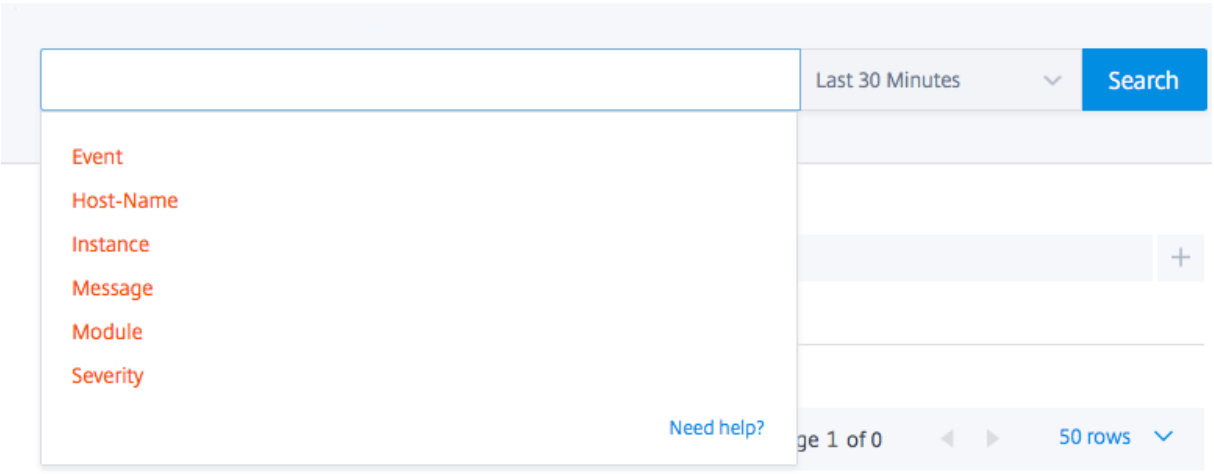


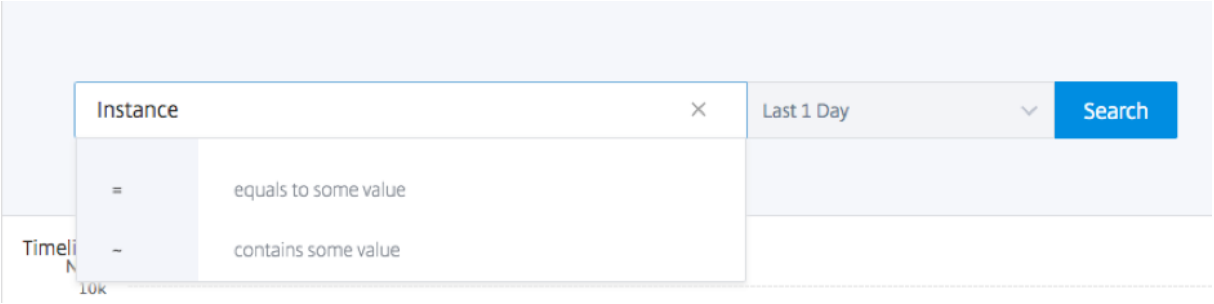
Ces étapes configurent toutes les commandes syslog dans l'instance de Citrix ADC et Citrix ADM commence à recevoir les messages syslog.

Afficher et rechercher des messages syslog

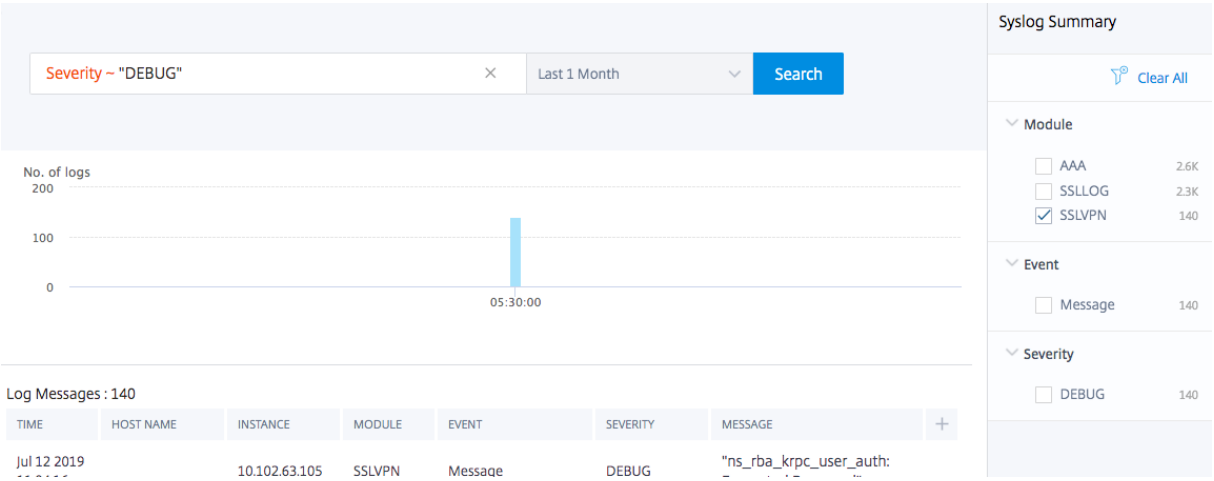
Vous pouvez afficher tous vos messages syslog générés sur vos instances Citrix ADC gérées. Les messages syslog sont stockés dans la base de données de manière centralisée et sont disponibles sous **Réseaux > Evénements > Messages Syslog** à des fins d'audit. Vous pouvez combiner ces informations de journalisation et dériver des rapports pour les analyses à partir des données collectées.

De plus, vous pouvez utiliser des filtres pour affiner les résultats de recherche des messages syslog et trouver exactement ce que vous cherchez et en temps réel. Cliquez sur **Besoin d'aide ?** pour ouvrir l'aide de recherche intégrée.





Ensuite, ajoutez le terme de recherche. Pour certaines catégories, une liste préremplie de termes de recherche s'affiche. Par défaut, la durée de recherche est de 1 jour. Vous pouvez modifier la plage d'heure et de dates en cliquant sur la flèche vers le bas. Vous pouvez affiner votre recherche en sélectionnant des options dans le volet **Récapitulatif Syslog**.

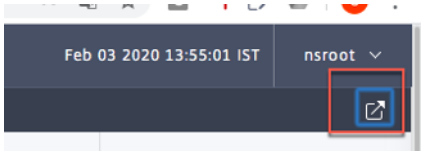


Exporter et planifier les messages syslog

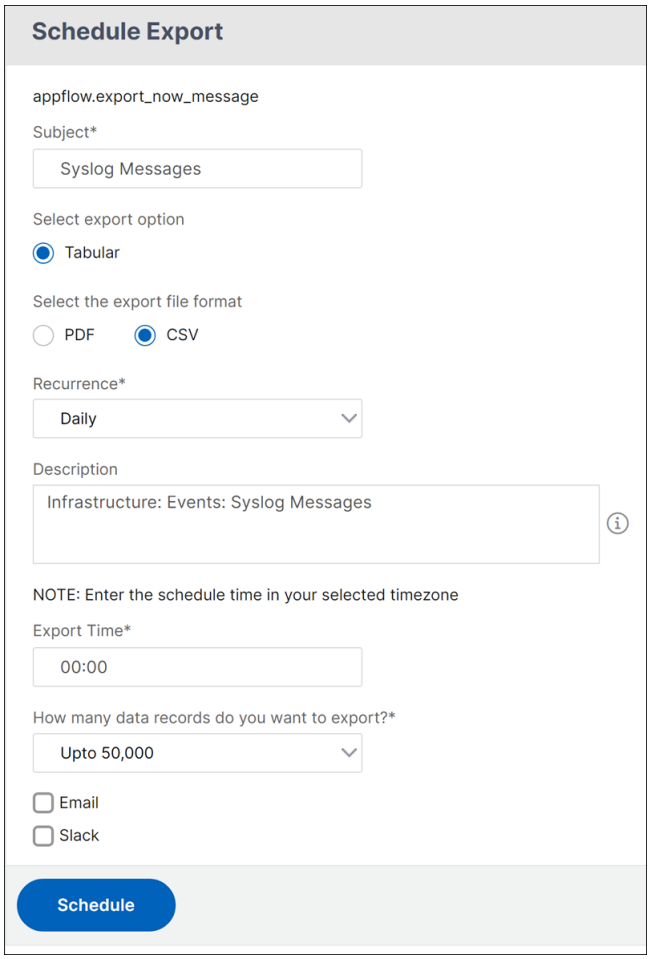
Vous pouvez afficher les messages syslog sans vous connecter à ADM, en planifiant une exportation de tous les messages syslog reçus sur le serveur. Vous pouvez exporter les messages syslog générés

sur vos instances ADC aux formats PDF, CSV, PNG et JPEG. Vous pouvez planifier l'exportation de ces rapports vers des adresses e-mail spécifiées ou un compte Slack à différents intervalles.

Pour exporter et planifier les messages du journal, cliquez sur l'icône en forme de flèche dans le coin supérieur droit.



- Pour exporter les messages du journal, cliquez sur **Exporter les rapports > Exporter maintenant**, sélectionnez le format requis, puis cliquez sur **Exporter**.
- Pour planifier l'exportation des messages syslog, cliquez sur **Exporter les rapports > Planifier le rapport**, puis définissez les paramètres requis. Vous pouvez recevoir le rapport par courriel ou par Slack.



Supprimer les messages Syslog

February 1, 2024

Lorsqu'il est configuré en tant que serveur syslog, Citrix Application Delivery Management (ADM) reçoit tous les messages syslog qui lui sont envoyés par les instances de Citrix Application Delivery Controller (ADC) configurées. Il se peut que vous ne vouliez pas voir un grand nombre de messages. Par exemple, il se peut que vous ne souhaitiez pas voir tous les messages de niveau informatif. Vous pouvez maintenant ignorer certains des messages syslog qui ne vous intéressent pas. Vous pouvez supprimer certains messages Syslog entrant dans Citrix ADM en configurant certains filtres. Citrix ADM supprime tous les messages correspondant aux critères. Ces messages supprimés n'apparaissent pas sur l'interface graphique Citrix ADM et ces messages ne sont pas non plus stockés dans la base de données Citrix ADM du client.

Vous pouvez supprimer certains messages Syslog enregistrés qui arrivent dans Citrix ADM en configurant certains filtres. Les deux filtres qui peuvent être utilisés pour supprimer les messages syslog sont la gravité et la facilité. Vous pouvez également supprimer les messages provenant d'une instance Citrix ADC particulière ou de plusieurs instances. Vous pouvez également fournir un modèle de texte pour Citrix ADM pour rechercher et supprimer des messages. Citrix ADM supprime tous les messages correspondant aux critères. Ces messages supprimés n'apparaissent pas sur l'interface graphique Citrix ADM et ne sont pas non plus stockés dans la base de données client. Par conséquent, une bonne quantité d'espace est économisée sur le serveur de stockage.

Voici quelques cas d'utilisation pour supprimer les messages Syslog :

- Si vous souhaitez ignorer tous les messages de niveau d'information, supprimez le niveau 6 (informationnel)
- Si vous souhaitez uniquement enregistrer les conditions d'erreur du pare-feu, supprimez tous les niveaux autres que le niveau 3 (erreurs)

Suppression des messages syslog en créant des filtres

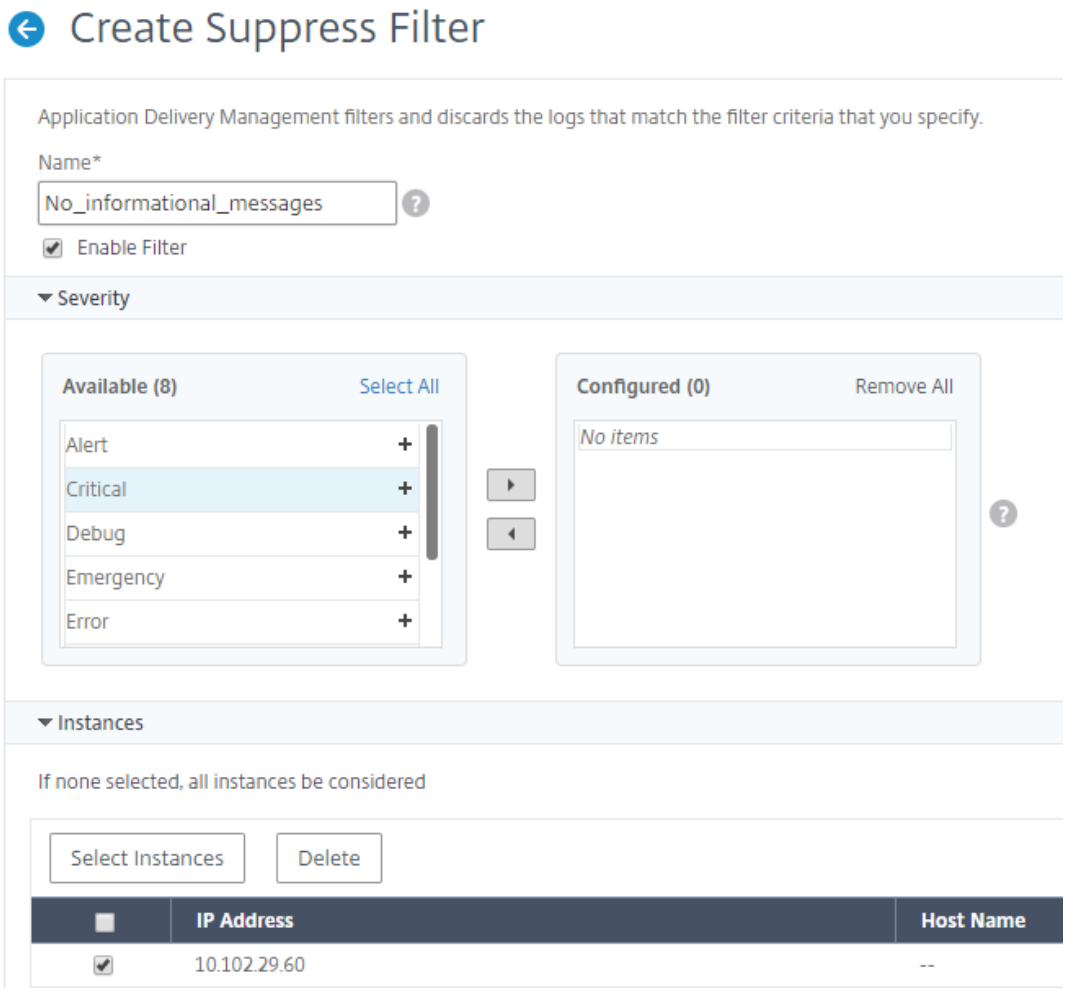
1. Dans Citrix ADM, accédez à **Réseaux** > **Événements** > **Messages Syslog** > **Supprimer le filtre**.
2. Sur la page **Créer un filtre de suppression**, mettez à jour les informations suivantes :
   a) **Nom** : entrez le nom du filtre.

> **Remarque**
>
> Si différents utilisateurs ont un accès différent à plusieurs instances Citrix ADC, différents filtres doivent être créés pour différentes instances, car les utilisateurs ne peu-

> vent voir que les filtres dans lesquels ils ont accès à toutes les instances.

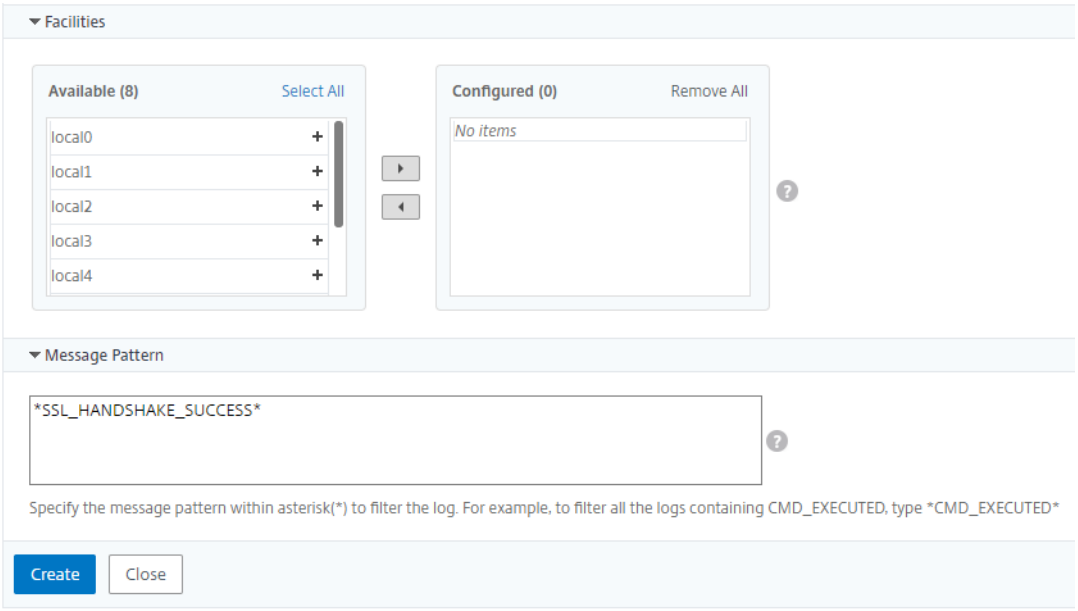
b) **Gravité** : sélectionnez et ajoutez les niveaux de journalisation pour lesquels vous devez supprimer les messages. Par exemple, si vous ne souhaitez pas voir les messages d'information qui arrivent, vous pouvez sélectionner Informationnel pour supprimer ces messages.

c) **Instances** : sélectionnez les instances Citrix ADC sur lesquelles les messages syslog ont été configurés.



d) **Installations** - Sélectionnez la ressource pour supprimer les messages en fonction de la source qui les génère.

e) **Modèle de message** : vous pouvez également saisir un modèle de texte entouré d'un astérisque (*) pour supprimer les messages. Les messages sont recherchés pour la chaîne de modèle de texte et les messages qui contiennent ce modèle sont supprimés.



Désactivation du filtre

Pour autoriser l'affichage des messages sur Citrix ADM, vous devez désactiver le filtre.

1. Accédez à **Réseaux** > **Événements** > **Messages Syslog** > **Supprimer le filtre**, puis sur la page **Supprimer le filtre**, sélectionnez le filtre et cliquez sur **Modifier**.
2. Dans la page **Configurer Supprimer le filtre**, **désactivez la case à cocher Activer le filtre** pour désactiver le filtre.

Configurer les paramètres de nettoyage pour les événements d'instance

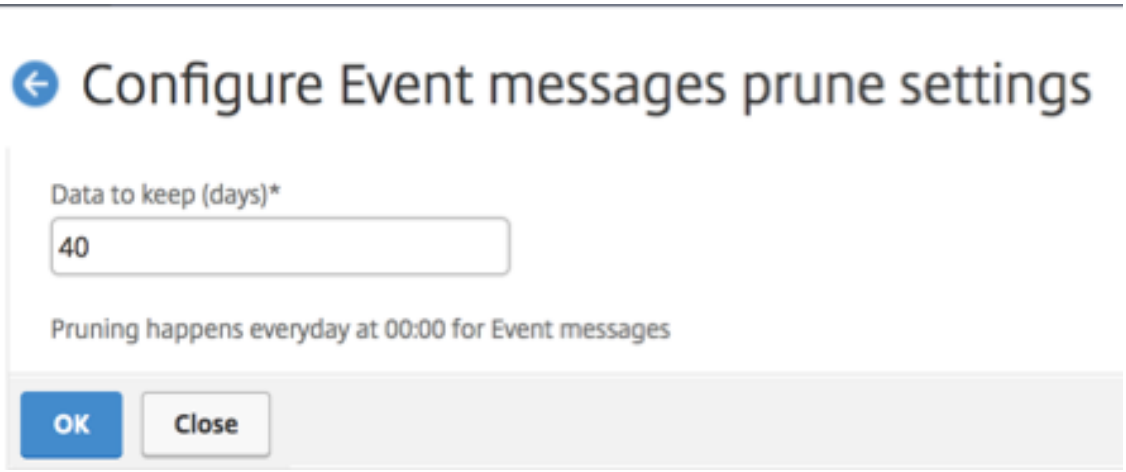
February 1, 2024

Les instances de Citrix Application Delivery Controller (ADC) gérées par votre serveur Citrix Application Delivery Management (ADM) envoient des données de messages d'événements en continu pour être stockées sur Citrix ADM. Vous pouvez spécifier l'intervalle pendant lequel Citrix ADM conserve les données de reporting réseau, les événements, les journaux d'audit et les journaux de tâches. Par défaut, ces données sont nettoyées toutes les 24 heures (à 00.00 heures).

> **Remarque**
>
> La valeur que vous pouvez spécifier ne peut pas dépasser 40 jours ni être inférieure à 1 jour.

Pour configurer les paramètres nettoyer pour les événements d'instance :

1. Accédez à **Système** > **Administration système**.
2. Sous **Paramètres de nettoyage**, cliquez sur **Paramètres de nettoyage des événements d'instance**.
3. Entrez l'intervalle de temps, en jours, pour lequel vous souhaitez conserver les données sur le serveur Citrix ADM et cliquez sur**OK**.



Gestion des certificats SSL

February 1, 2024

Toute organisation ou site Web individuel nécessitant le traitement d'informations confidentielles ou sensibles doit posséder un certificat SSL. Le certificat SSL sur un serveur Web permet de garantir l'authenticité du serveur Web au client qui se connecte. Il authentifie non seulement l'identité d'un site Web, mais aide également à générer la clé de session, qui est utilisée ultérieurement pour le chiffrement de la session entière.

Un certificat SSL (Secure Socket Layer), qui fait partie de toute transaction SSL, est un formulaire de données numérique (X509) qui identifie une société (domaine) ou un individu. Le certificat possède un composant de clé publique visible par tout client qui souhaite lancer une transaction sécurisée avec le serveur. La clé privée correspondante, qui réside en toute sécurité sur l'appliance Citrix Application Delivery Controller (ADC), est utilisée pour effectuer le chiffrement et le déchiffrement des clés asymétriques (ou des clés publiques).

Citrix Application Delivery Management (ADM) vous fournit une console unifiée pour automatiser l'installation, la mise à jour, la suppression, la liaison et le téléchargement des certificats SSL. Il aide à conserver la réputation du site Web et la confiance des clients. Citrix ADM simplifie désormais tous les aspects de la gestion des certificats pour vous. Grâce à une console unifiée, vous pouvez configurer

des stratégies automatisées pour garantir l'émetteur recommandé, la force clé, le protocole et les algorithmes conformément aux stratégies informatiques de l'organisation. Ce faisant, vous pouvez surveiller de près les certificats inutilisés ou sur le point d'expirer.

Vous pouvez obtenir un certificat SSL et une clé de l'une des manières suivantes :

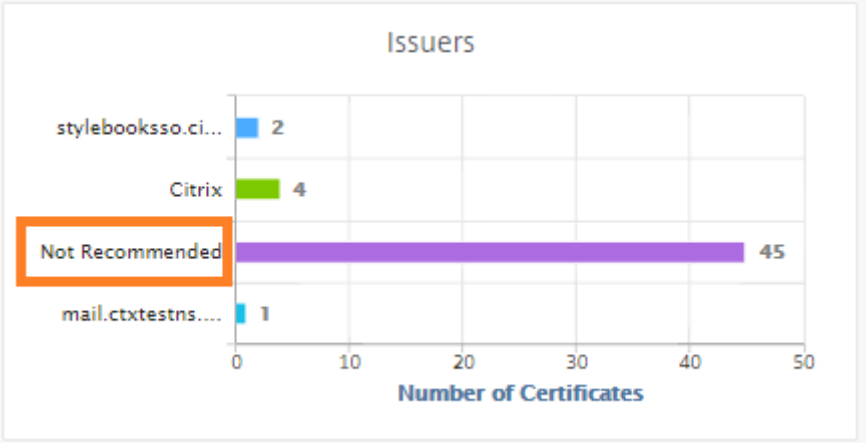
- À partir d'une autorité de certification (CA) autorisée, telle que Verisign
- En générant un nouveau certificat SSL et une nouvelle clé sur l'appliance Citrix ADC

Paramètres de stratégie SSL d'entreprise

Chaque entreprise dispose de sa propre stratégie SSL et définit les exigences auxquelles tous les certificats SSL doivent respecter. La sécurité a toujours été l'une des principales priorités de tous les utilisateurs de l'entreprise et, par conséquent, les paramètres SSL jouent un rôle important.

Par exemple, une société ABC exige que tous les certificats aient une puissance de clé minimale de 2 048 bits et plus. Les certificats doivent être autorisés par une autorité de certification ou des émetteurs de confiance. Les administrateurs doivent vérifier tous ces paramètres SSL pour s'assurer que les certificats respectent la stratégie de l'entreprise. Il est fastidieux de vérifier chaque certificat manuellement. Pour surmonter ce scénario, Citrix ADM vous aide à configurer les paramètres de stratégie SSL d'entreprise et affiche tout certificat de non-conformité avec la balise « Non recommandé ».

Vous pouvez afficher le résumé des certificats de non-conformité (non recommandé) dans le tableau de bord SSL.

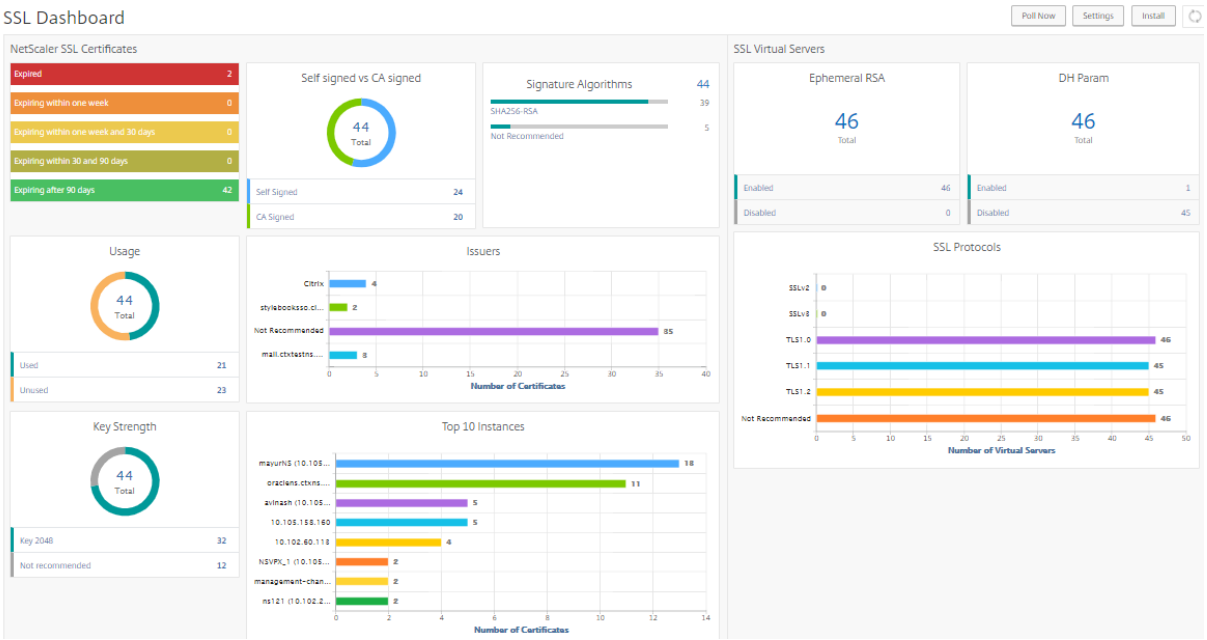


> **Remarque**
>
> Les certificats « Non recommandés » sont classés en fonction de différents paramètres, et vous pouvez les afficher dans les composants pertinents.

Fonctionnement du certificat Citrix ADM

SSL Dashboard fournit une présentation visuelle de tous les certificats SSL installés sur différentes instances Citrix ADC. Le tableau de bord SSL inclut les informations suivantes pour chaque certificat installé sur les instances Citrix ADC. Il est classé en fonction des éléments suivants :

- **Auto-signé vs CA signé.** La section auto-signé vs CA signé vous aide à séparer les certificats en certificats auto-signés et certificats signés par l'autorité de certification.
- **Algorithmes de signature.** Cette section sépare les certificats SSL en fonction des algorithmes de signature utilisés pour le chiffrement.
- **Utilisation.** Cette section sépare vos certificats SSL en fonction des certificats utilisés et non utilisés. Les certificats inutilisés nécessitent une attention particulière car ils ont pu être manqués pour être liés aux serveurs virtuels.
- **Émetteurs.** Cette section sépare les certificats SSL en fonction de l'émetteur des certificats.
- **La force de la clé.** Cette section sépare les certificats SSL en fonction de la force de clé d'une clé privée.
- **Les 10 premières instances.** Cette section fournit les détails des 10 principales instances Citrix ADC en fonction du nombre de certificats SSL installés.



Cas d'utilisation de la gestion des certificats SSL

Les cas d'utilisation suivants décrivent comment utiliser le certificat SSL pour gérer et surveiller les certificats sur plusieurs instances Citrix ADC.

Installer les certificats SSL

Imaginez que vous disposez d'une flotte d'instances Citrix ADC, sur lesquelles vous devez déployer les certificats SSL requis. Citrix ADM vous fournit une console unifiée pour déployer les certificats SSL sur plusieurs instances Citrix ADC en une seule tentative.

Par exemple, vous pouvez installer certains certificats SSL sur une ou plusieurs instances Citrix ADC. Avec cette approche, vous pouvez minimiser l'intervention manuelle d'installation du certificat SSL sur chaque instance Citrix ADC. Vous pouvez effectuer une installation groupée de certificats SSL sur une ou plusieurs instances Citrix ADC.

Pour obtenir un résumé des certificats SSL, connectez-vous à **Citrix ADM**, puis accédez à **Réseaux > Dashboard SSL**.

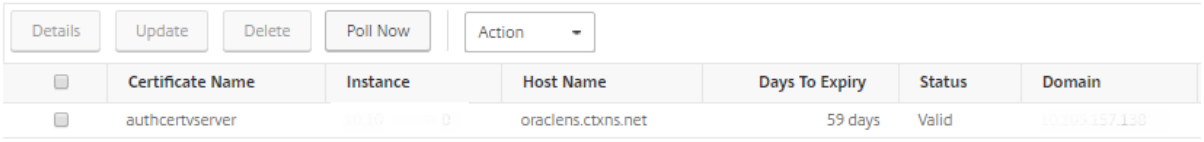
Paramètres de notification pour l'expiration du certificat

Dans ce cas d'utilisation, vous pouvez disposer de nombreux certificats sur plusieurs instances Citrix ADC, et le suivi de l'expiration de chaque certificat devient une surcharge. C'est un travail fastidieux pour vous de suivre chaque certificat manuellement et de le mettre à jour avant son expiration. Pour éviter de tels scénarios, vous pouvez configurer Citrix ADM pour envoyer les notifications ou alertes aux profils e-mail, pager, Slack ou ServiceNow configurés. De cette façon, vous pouvez rester au courant des dates d'expiration des certificats et renouveler les certificats bien avant les dates d'expiration.

Par exemple, vous pouvez oublier de suivre le certificat qui arrive à expiration. Et le certificat expire provoquant une panne de service, ce qui peut affecter de nombreuses applications pour les utilisateurs. Avec les paramètres de notification d'expiration de certificat ADM, vous pouvez éviter de tels scénarios imprévus.

Vous pouvez afficher le récapitulatif et suivre les certificats qui sont en voie d'expiration dans le tableau de **bord SSL**.

Pour afficher le rapport sur les certificats expirant dans une durée quelconque, vous pouvez cliquer sur la vignette pour obtenir les détails de tous ces certificats expirant dans cette fenêtre.



Renouvellement des certificats

Vous pouvez maintenant renouveler les certificats de Citrix ADM. Vous pouvez renouveler les certificats existants ou créer les certificats basés sur les éléments suivants :

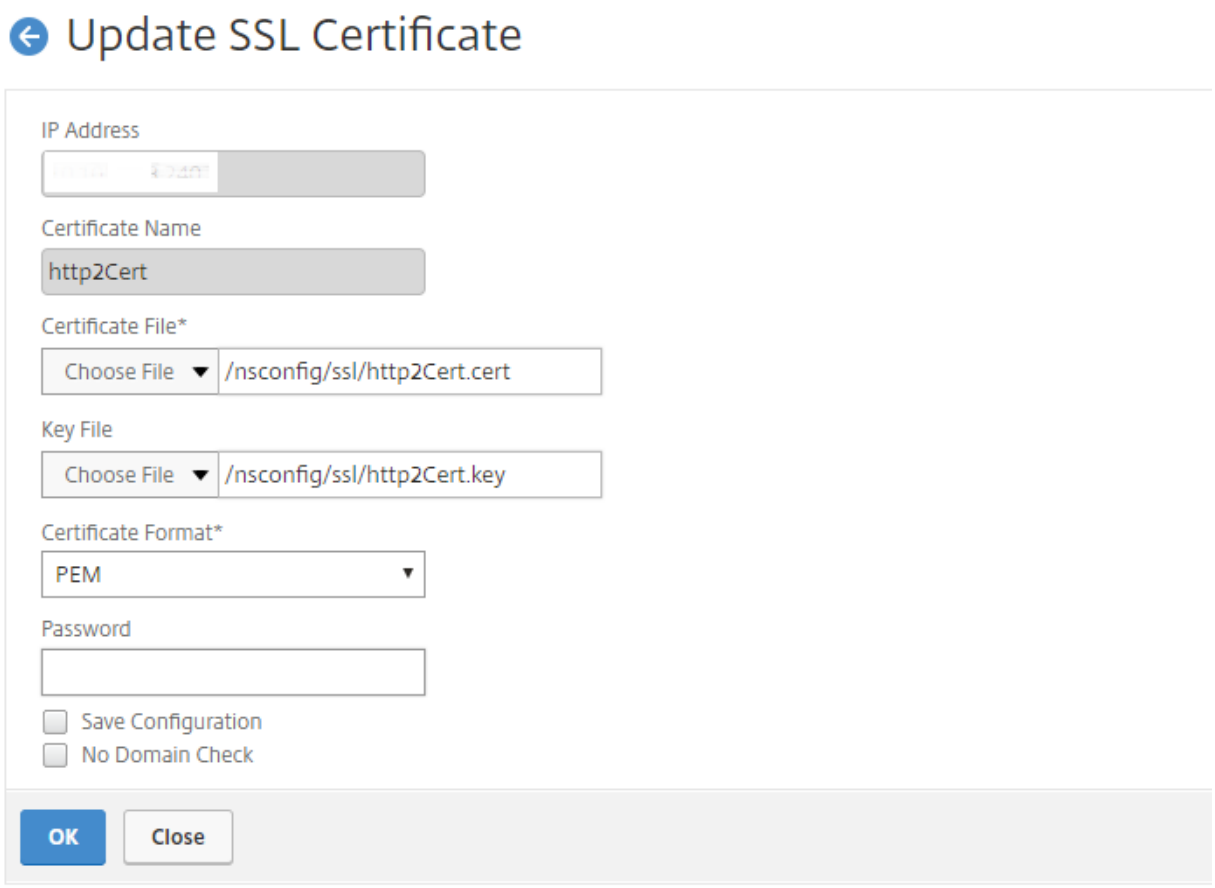
Mettre à jour le certificat existant Dans ce cas d'utilisation, vous devez mettre à jour un certificat existant une fois que vous recevez un certificat renouvelé de l'autorité de certification (CA). Vous pouvez désormais mettre à jour les certificats existants à partir de Citrix ADM sans vous connecter aux instances Citrix ADC.

Par exemple, il peut y avoir des modifications ou des modifications aux certificats existants. L'AC émet des certificats renouvelés. Au lieu d'accéder à l'appliance Citrix ADC, vous pouvez maintenant mettre à jour le certificat SSL à partir de Citrix ADM.

Pour mettre à jour un certificat, connectez-vous à Citrix ADM, puis accédez à **Réseaux > Tableau de bord SSL**.

Sélectionnez le certificat que vous souhaitez mettre à jour, puis cliquez sur **Mettre à jour**.

Vous avez la possibilité de mettre à jour les champs pertinents du certificat sélectionné à partir de Citrix ADM.

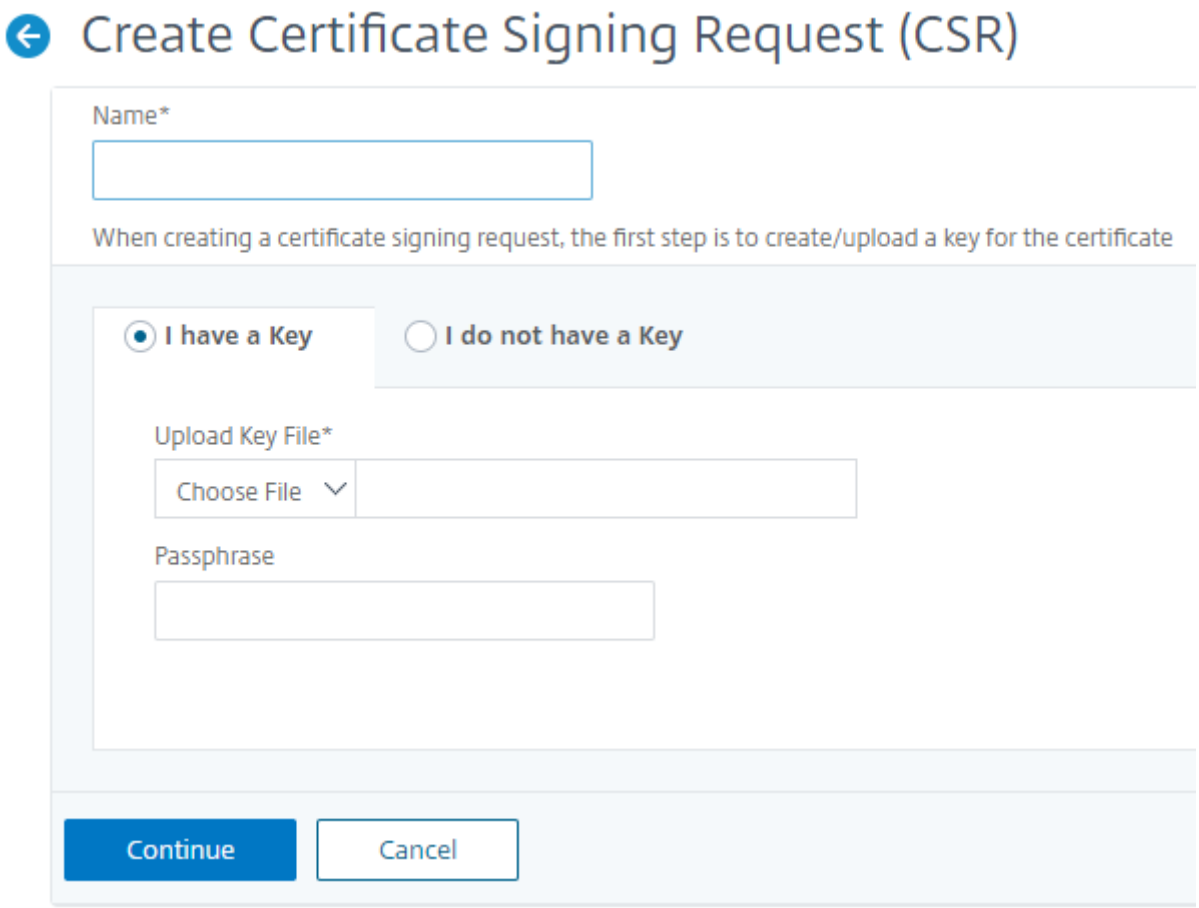


Créer une demande de signature de certificat Imaginez un cas d'utilisation où l'un des certificats SSL ne respecte pas les stratégies de l'organisation. Vous souhaitez obtenir un nouveau certificat auprès de l'autorité de certification. Vous pouvez désormais générer une demande de signature de

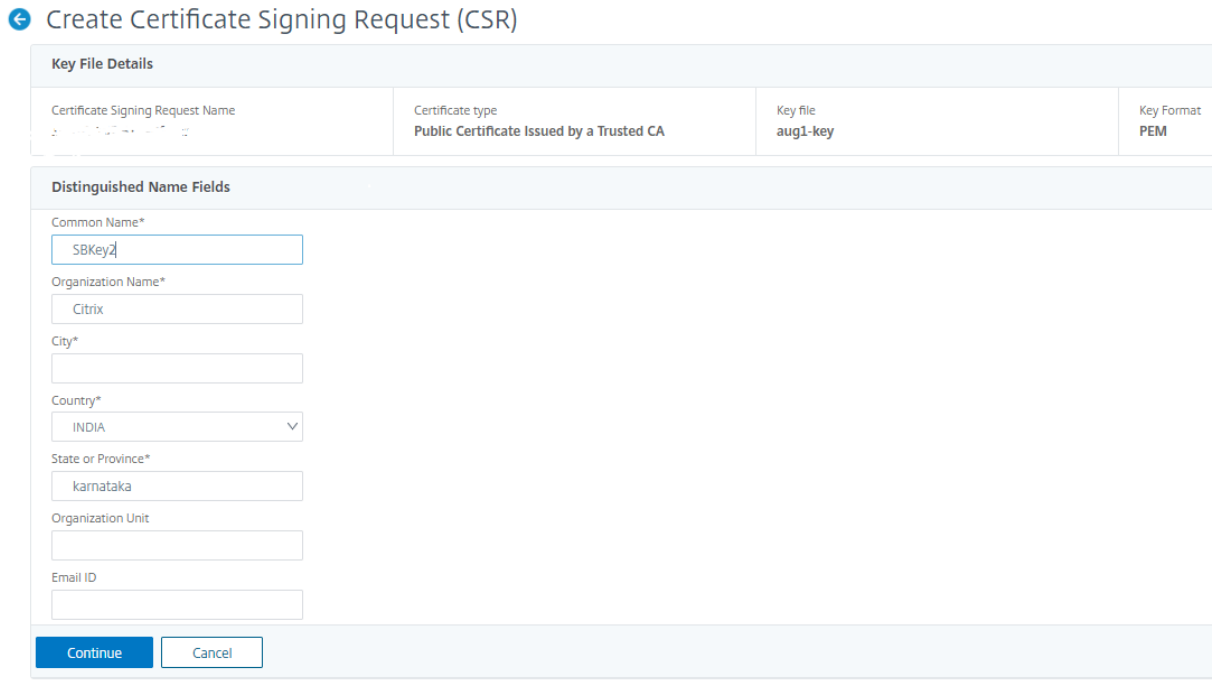
certificat (CSR) à partir de Citrix ADM. Un CSR et une clé publique peuvent être envoyés à une autorité de certification pour obtenir le certificat SSL.

Pour déterminer et créer la CSR, sélectionnez le certificat souhaité et cliquez sur **Créer un CSR**.

Vous devez avoir une paire de valeurs de clé publique ou privée. Pour télécharger une clé, cliquez sur **Choisir un fichier** et sélectionnez dans la liste. Pour créer une clé, sélectionnez **Je n'ai pas d'option Clé** et spécifiez les paramètres pertinents.

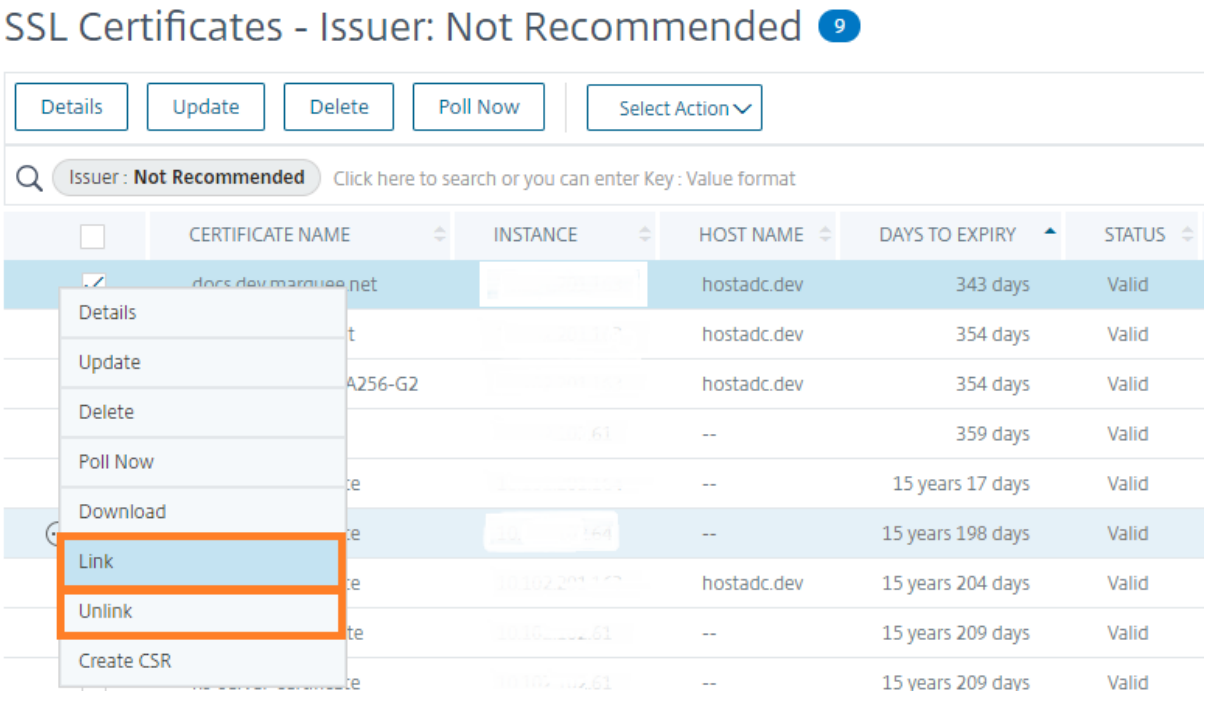


Pour donner plus de détails sur la clé sélectionnée, comme Nom commun, Nom de l'organisation, Ville, Pays, État, Unité Org et Email ID pour créer la CSR.



Lier et dissocier les certificats SSL

Vous pouvez lier plusieurs certificats SSL les uns aux autres pour créer un ensemble de certificats. Pour lier un certificat à un autre certificat, l'émetteur du premier certificat doit correspondre au domaine du second certificat.

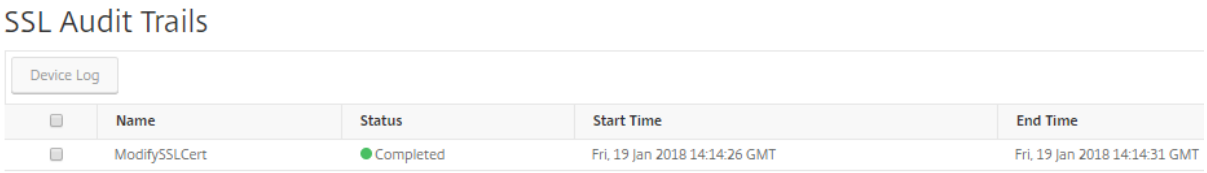


Journaux d'audit

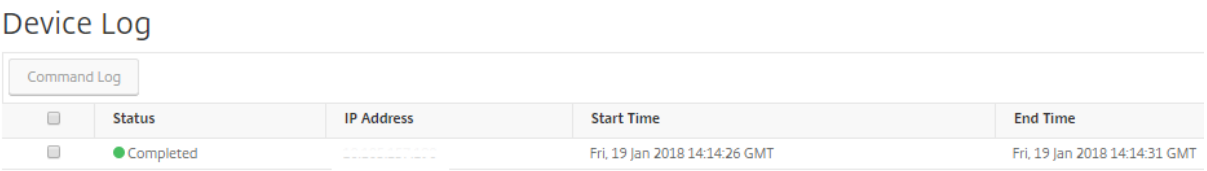
Les journaux d'audit sont un ensemble de fichiers journaux texte générés par Citrix ADM. Il affiche un historique des certificats SSL ajoutés, modifiés et modifiés à l'aide de Citrix ADM pour l'appliance Citrix ADC spécifique. Les journaux d'audit affichent également l'adresse IP de l'appliance Citrix ADC, l'état, l'heure de début et l'heure de fin de l'opération particulière.

Dans cet exemple, vous pouvez vérifier la modification apportée au certificat particulier au cours d'une période donnée. Vous avez également la possibilité d'afficher l'historique des modifications apportées au certificat sur le journal des périphériques et le journal des commandes.

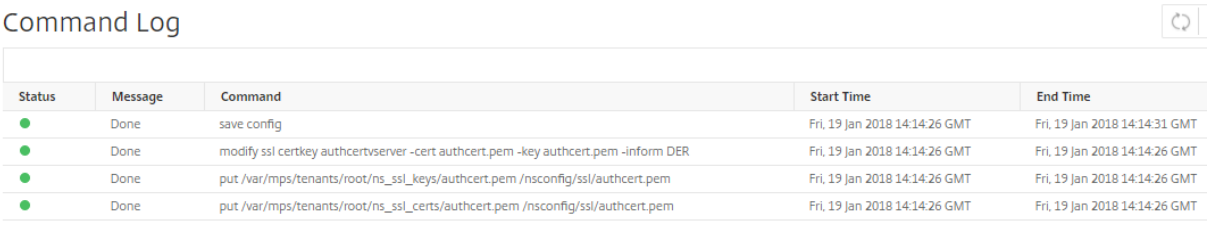
Pour déterminer les informations des certificats SSL, dans le tableau de **bord SSL**, cliquez sur **Journal d'audit**. Le récapitulatif de l'application inclut l'état des certificats SSL avec Heure de début et Heure de fin.



Pour déterminer les informations de l'appliance Citrix ADC d'un certificat SSL particulier, activez la case à cocher certificat appropriée de votre choix. Cliquez sur **Journal des périphériques**.



Pour afficher les informations sur le type de commande et le message, cliquez sur **Journal des commandes**.



Utiliser le tableau de bord SSL

February 1, 2024

Vous pouvez utiliser le tableau de bord des certificats SSL de Citrix Application Delivery Management (ADM) pour afficher des graphiques qui vous aident à suivre les émetteurs de certificats, leurs principaux atouts et les algorithmes de signature. Le tableau de bord des certificats SSL affiche également des graphiques indiquant les éléments suivants :

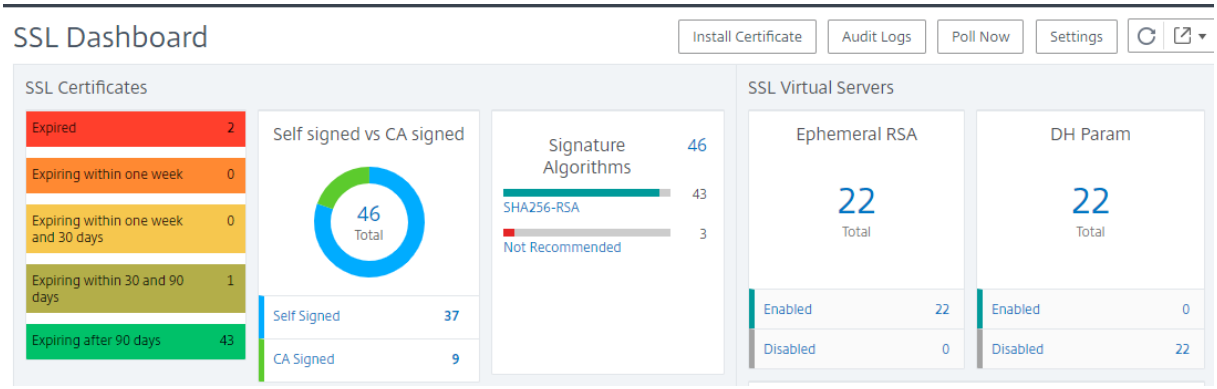
- Nombre de jours après lesquels les certificats expirent
- Nombre de certificats utilisés et non utilisés
- Nombre de certificats autosignés et signés par une autorité de certification
- Nombre d'émetteurs
- Des algorithmes de signature
- Protocoles SSL
- 10 instances les plus importantes par nombre de certificats utilisés

Pour surveiller les certificats SSL

Vous pouvez utiliser le tableau de bord SSL sur Citrix ADM pour surveiller vos certificats si votre société a une stratégie SSL dans laquelle vous avez défini certaines exigences en matière de certificats SSL telles que tous les certificats doivent avoir une force clé minimale de 2048 bits et une autorité de certification de confiance doit l'autoriser.

Dans un autre exemple, vous avez peut-être téléchargé un nouveau certificat mais oublié de le lier à un serveur virtuel. Le tableau de bord SSL met en évidence les certificats SSL utilisés ou non. Dans la section **Utilisation** , vous pouvez voir le nombre de certificats installés et le nombre de certificats utilisés. Vous pouvez cliquer sur le graphique pour voir le nom du certificat, l'instance sur laquelle il est utilisé, sa validité, son algorithme de signature, etc.

Pour surveiller les certificats SSL dans Citrix ADM, accédez à**Réseaux**> Tableau de **bord SSL**.



Citrix ADM vous permet d'interroger les certificats SSL et d'ajouter immédiatement tous les certificats SSL des instances à Citrix ADM. Pour ce faire,

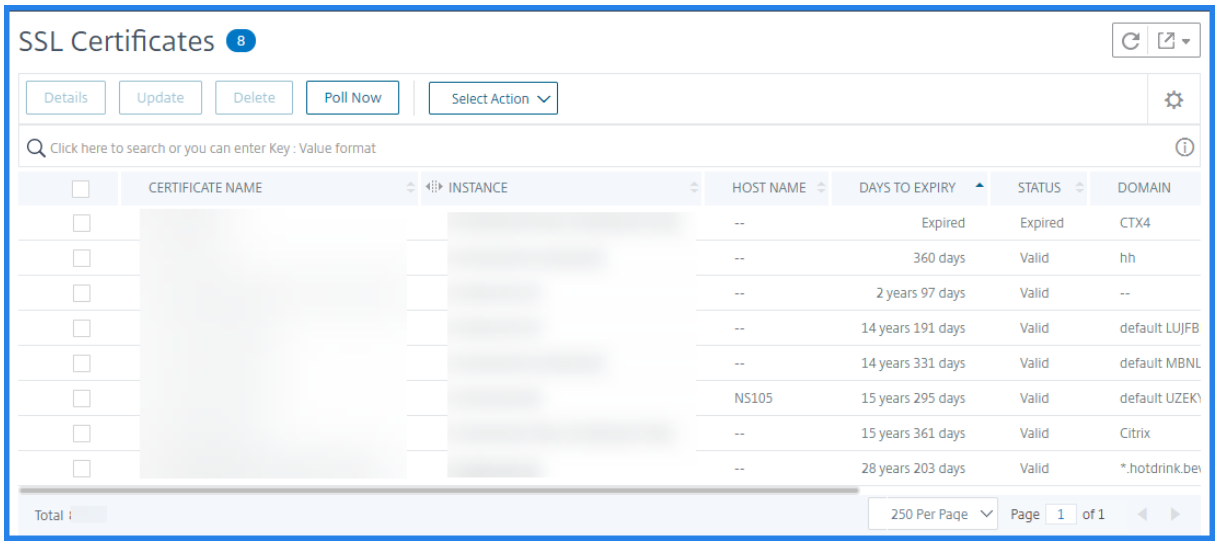
1. Accédez à **Réseaux**> Tableau de**bord SSL**.
2. Cliquez sur **Interroger maintenant**.

   Sur la page **Poll Now**, vous pouvez interroger toutes les instances ADC gérées ou sélectionner des instances spécifiques.
3. Cliquez sur **Démarrer l'interrogation**.

Dans **SSL Dashboard**, vous pouvez surveiller les certificats SSL ADC, les serveurs virtuels SSL et les protocoles SSL.

Vous pouvez cliquer sur les mesures du tableau de bord pour afficher les détails relatifs aux certificats SSL, aux serveurs virtuels SSL ou aux protocoles SSL.

Par exemple, lorsque vous cliquez sur le numéro sous **Autosigné vs CA signé** dans le tableau de bord, l'interface graphique ADM affiche tous les certificats SSL sur les instances Citrix ADC.



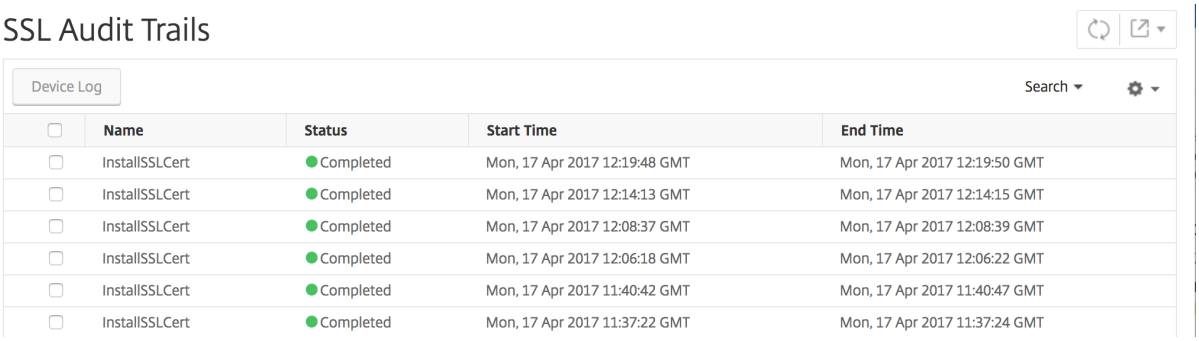
Le tableau de bord SSL Citrix ADM affiche également la distribution des protocoles SSL qui s'exécutent sur vos serveurs virtuels. En tant qu'administrateur, vous pouvez spécifier les protocoles que vous souhaitez surveiller via la stratégie SSL. Pour plus d'informations, reportez-vous à la section Configuration des stratégies SSL. Les protocoles pris en charge sont SSLv2, SSLv3, TLS 1.0, TLS 1.1, TLS 1.2 et TLS 1.3. Les protocoles SSL utilisés sur les serveurs virtuels apparaissent sous forme de graphique à barres. Cliquez sur un protocole spécifique pour afficher la liste des serveurs virtuels utilisant ce protocole.

Un graphique en anneau apparaît une fois que les clés Diffie-Hellman (DH) ou Ephemeral RSA sont activées ou désactivées sur le tableau de bord SSL. Ces clés permettent une communication sécurisée avec les clients d'exportation même si le certificat serveur ne prend pas en charge les clients d'exportation, comme dans le cas d'un certificat 1024 bits. Cliquez sur le graphique approprié pour afficher la liste des serveurs virtuels sur lesquels les clés DH ou Ephemeral RSA sont activées.

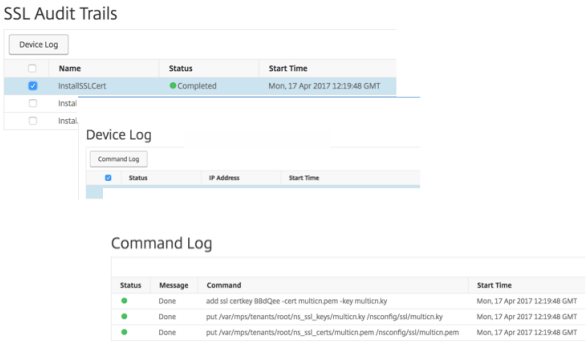
Pour afficher les pistes d'audit des certificats SSL

Vous pouvez désormais afficher les détails du journal des certificats SSL sur Citrix ADM. Les détails du journal affichent les opérations effectuées à l'aide de certificats SSL sur Citrix ADM, telles que : installation de certificats SSL, liaison et dissociation de certificats SSL, mise à jour de certificats SSL et suppression de certificats SSL. Les informations de piste d'audit sont utiles lors de la surveillance des modifications de certificat SSL effectuées sur une application avec plusieurs propriétaires.

Pour afficher un journal d'audit pour une opération particulière effectuée sur Citrix ADM à l'aide de certificats SSL, accédez à **Réseaux** > Tableau de **bord SSL** > et cliquez sur **Journaux d'audit**.



Pour une opération particulière effectuée à l'aide d'un certificat SSL, vous pouvez afficher son état, l'heure de début et l'heure de fin. En outre, vous pouvez afficher l'instance sur laquelle l'opération a été effectuée et les commandes s'exécutent sur cette instance.



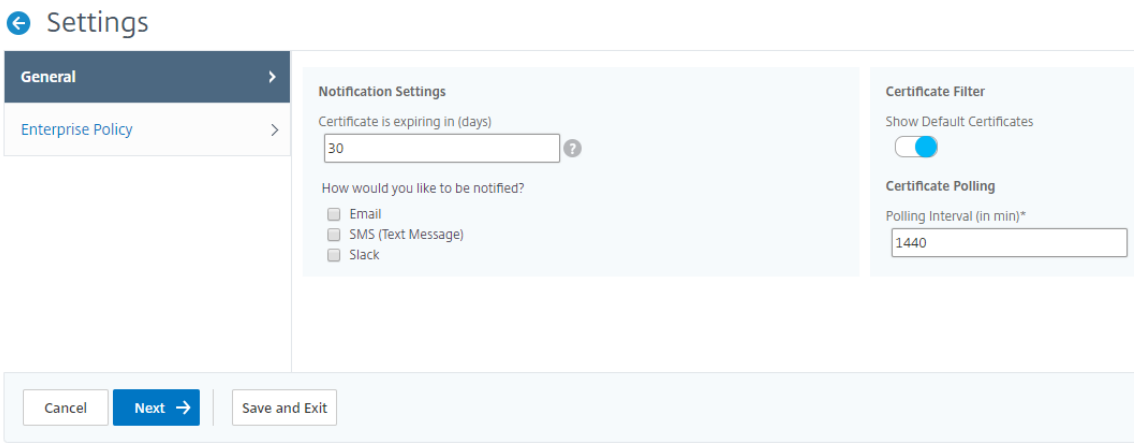
Pour exclure les certificats Citrix ADC par défaut sur le tableau de bord SSL

Citrix ADM vous permet d'afficher ou de masquer les certificats Citrix ADC par défaut qui s'affichent dans les graphiques SSL Dashboard en fonction de vos préférences. Par défaut, tous les certificats sont affichés sur le tableau de bord SSL, y compris les certificats par défaut.

Pour afficher ou masquer les certificats par défaut sur le tableau de bord SSL :

1. Accédez à **Réseaux** > **Tableau de bord SSL** dans l'interface graphique Citrix ADM.
2. Sur la page **Tableau de bord SSL**, cliquez sur **Paramètres**.

3. Dans la page **Paramètres**, sélectionnez **Général** .
4. Entrez le nombre de jours d'expiration du certificat pour recevoir une notification concernant l'expiration du certificat.
5. Sélectionnez la méthode de notification et créez les profils correspondants.
6. Dans la section **Filtre de certificat**, désactivez la case à cocher **Afficher les certificats par défaut** et cliquez sur **Enregistrer et quitter**.



Afficher, télécharger et télécharger des fichiers SSL

Pour afficher les fichiers SSL sur Citrix ADM, accédez à **Réseaux > Tableau de bord SSL > Fichiers SSL sur Citrix ADM**.

Dans cette page, vous pouvez afficher, télécharger et télécharger les fichiers suivants sur Citrix ADM :

- Certificats SSL
- Clés SSL
- CSR SSL

Pour afficher et télécharger des fichiers SSL sur une instance Citrix ADC, accédez à **Réseaux > Tableau de bord SSL > Fichiers SSL sur Citrix ADC**.

> **Important**
>
> Pour activer le téléchargement des fichiers SSL à partir d'instances ADC, activez la fonctionnalité **Certificats SSL d'instance**. Pour plus d'informations, consultez Activer ou désactiver les fonctionnalités ADM.

Configurer les notifications pour l'expiration du certificat SSL

February 1, 2024

En tant qu'administrateur de la sécurité, vous pouvez configurer des notifications pour vous informer de l'expiration prochaine des certificats et pour inclure des informations sur les instances de Citrix Application Delivery Controller (ADC) qui utilisent ces certificats. En activant les notifications, vous pouvez renouveler vos certificats SSL à temps.

Par exemple, vous pouvez définir une notification par e-mail pour envoyer une liste de distribution par e-mail 30 jours avant l'expiration de votre certificat.

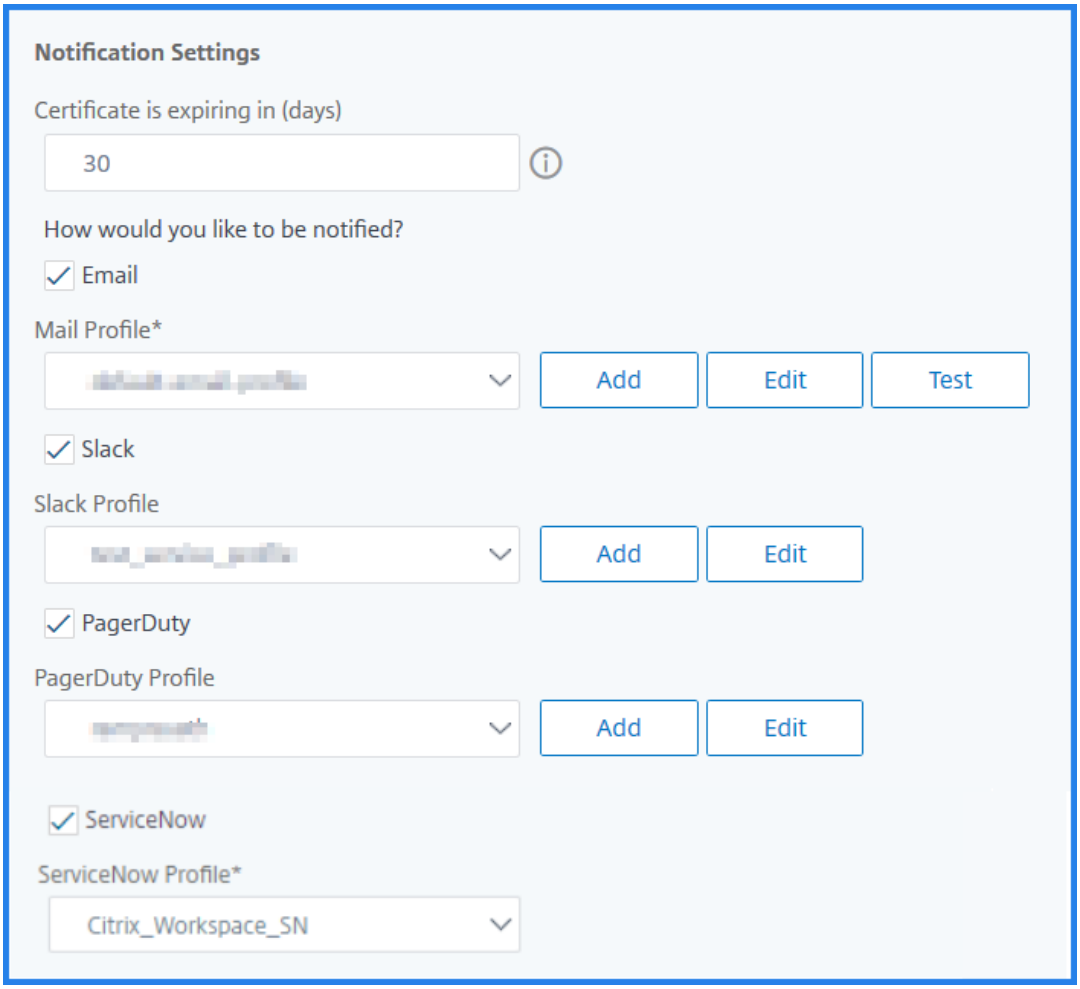
Pour configurer des notifications à partir de Citrix ADM :

1. Dans Citrix Application Delivery Management (ADM), accédez à **Réseaux > Tableau de bord SSL**.
2. Dans la page **Tableau de bord SSL**, cliquez sur **Paramètres** .
3. Sur la page **Paramètres SSL**, cliquez sur l'icône **Modifier**.
4. Dans la section **Paramètres de notification**, indiquez à quel moment vous souhaitez envoyer la notification en termes de nombre de jours avant la date d'expiration.
5. Choisissez le type de notification que vous souhaitez envoyer. Sélectionnez le type de notification et la liste de distribution dans le menu déroulant. Les types de notification sont les suivants :

    - **E-mail** : spécifiez un serveur de messagerie et les détails du profil. Un e-mail est déclenché lorsque vos certificats sont sur le point d'expirer.
    - **SMS** —Spécifiez un serveur de service de messages courts (SMS) et les détails du profil. Un message SMS est déclenché lorsque vos certificats sont sur le point d'expirer.
    - **Slack** - Spécifiez les détails du profil Slack.
    - **Alertes PagerDuty** - Spécifiez un profil PagerDuty. En fonction des paramètres de notification configurés dans votre portail PagerDuty, une notification est envoyée lorsque vos certificats sont sur le point d'expirer.
    - **ServiceNow** - Une notification est envoyée au profil ServiceNow par défaut lorsque vos certificats sont sur le point d'expirer.

        > **Important**
        >
        > Assurez-vous que l'adaptateur ITSM Citrix Cloud est configuré pour ServiceNow et

> intégré à Citrix ADM. Pour de plus amples informations, consultez Intégrer Citrix ADM à l'instance ServiceNow.



6. Cliquez sur **Enregistrer et quitter**.

Citrix ADM envoie désormais l'interruption d'expiration de certificat SSL au serveur de destination d'interruption externe lorsque vos certificats SSL sont expirés. Citrix ADM envoie une interruption lorsque les deux conditions suivantes sont remplies :

- Vous avez configuré le nombre de jours pour l'expiration du certificat dans la page des paramètres du tableau de bord SSL .
- Vous avez ajouté la destination du piège.

Vous pouvez définir des destinations d'interruptions en accédant à **Système > SNMP > Destinations des interruptions**. Tapez l'adresse IP du serveur SNMP de destination où les interruptions sont envoyées. Entrez le numéro de port et tapez « public » (sans guillemets) comme chaîne de communauté.

Mettre à jour un certificat installé

February 1, 2024

Après avoir reçu un certificat renouvelé de l'autorité de certification (CA), vous pouvez mettre à jour les certificats existants à partir de Citrix Application Delivery Management (ADM) sans avoir à ouvrir une session à des instances Citrix Application Delivery Controller (ADC) individuelles.

Pour mettre à jour un certificat SSL, une clé ou les deux à partir de Citrix ADM :

1. Dans Citrix ADM, accédez à **Réseaux** > **Tableau de bord SSL**.
2. Cliquez sur l'un des graphiques pour afficher la liste des certificats SSL.
3. Sur la page **Certificats SSL**, sélectionnez un certificat et cliquez sur **Mettre à jour**. Vous pouvez également cliquer sur le certificat SSL pour afficher ses détails, puis cliquez sur **Mettre à jour** dans le coin supérieur droit de la page **Certificat SSL**.
4. Sur la page **Mettre à jour le certificat SSL**, apportez les modifications requises au certificat, à la clé ou aux deux, puis cliquez sur **OK** .

Installer des certificats SSL sur une instance Citrix ADC

February 1, 2024

Avant d'installer des certificats SSL sur des instances ADC (Citrix Application Delivery Controller), assurez-vous que les certificats sont émis par des autorités de certification approuvées. Assurez-vous également que la force de clé des clés de certificat est de 2048 bits ou plus et que les clés sont signées à l'aide d'algorithmes de signature sécurisés.

Pour installer un certificat SSL à partir d'une autre instance Citrix ADC :

Vous pouvez également importer un certificat à partir d'une instance Citrix ADC choisie et l'appliquer à d'autres instances Citrix ADC ciblées à partir de l'interface graphique de Citrix Application Delivery Management (ADM).

1. Accédez à **Réseaux** > **Tableau de bord SSL**.
2. Dans l'angle supérieur droit du tableau de bord SSL, cliquez sur **Installer**.
3. Dans la page **Installer le certificat SSL sur les instances Citrix ADC**, spécifiez les paramètres suivants :

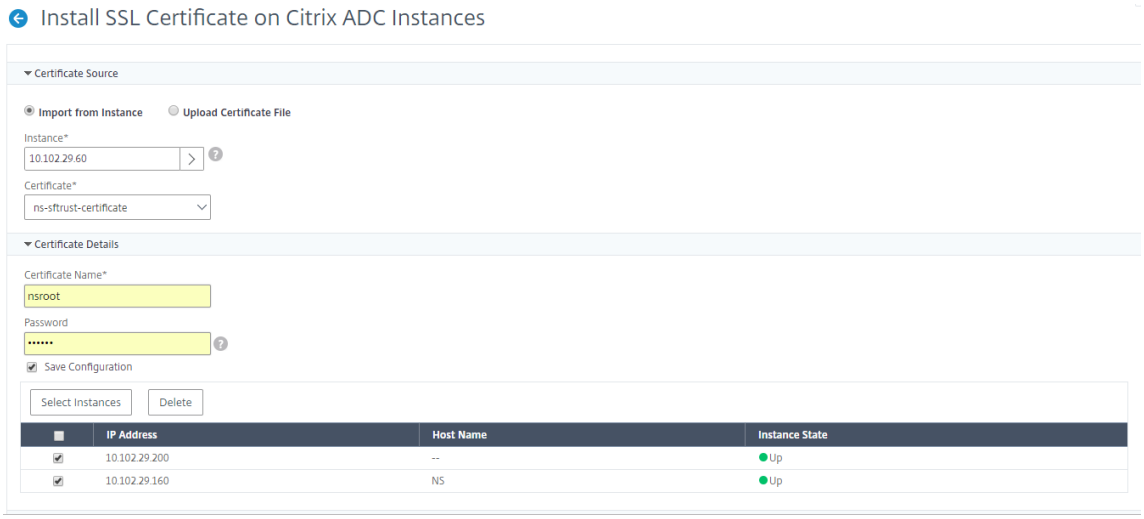
    a) Source du certificat
    Sélectionnez l'option **Importer à partir d'une instance**.

- Choisissez l'**instance** à partir de laquelle vous souhaitez importer le certificat.
- Choisissez le **certificat** dans la liste de tous les fichiers de certificats SSL de l'instance.

b) Détails du certificat

- **Nom du certificat**. Spécifiez le nom de la clé de certificat.
- **Mot de passe**. Mot de passe pour crypter la clé privée. Vous pouvez utiliser cette option pour télécharger des clés privées chiffrées.

4. Cliquez sur **Sélectionner les instances** pour sélectionner les instances Citrix ADC sur lesquelles vous souhaitez installer vos certificats.
5. Cliquez sur **OK**.



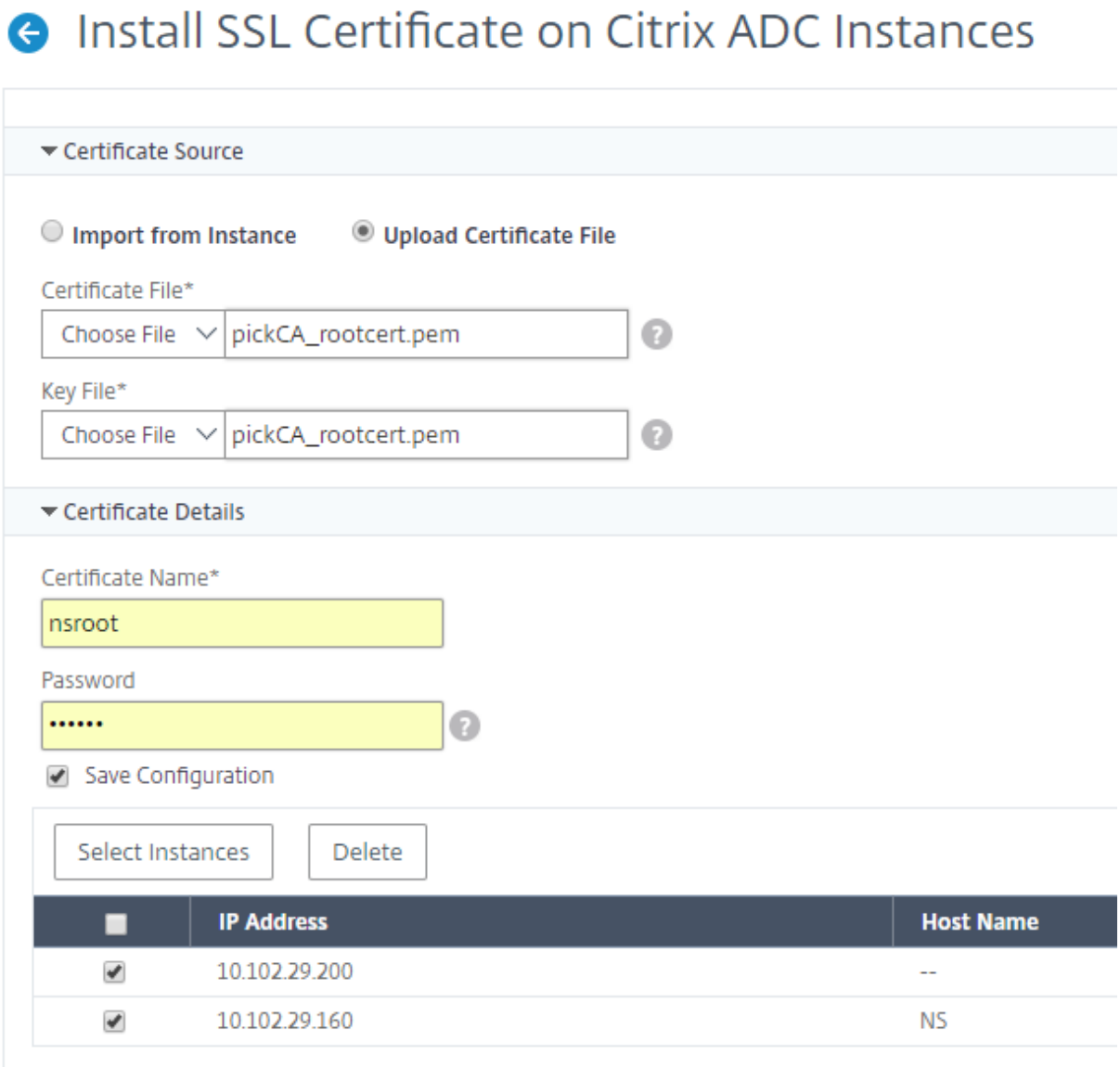
Pour installer un certificat SSL à partir de Citrix ADM :

1. Dans Citrix ADM, accédez à **Réseaux** > **Tableau de bord SSL**.
2. Dans l'angle supérieur droit du tableau de bord, cliquez sur **Installer**.
3. Sur la page **Installer le certificat SSL sur Citrix ADC Instance**, sélectionnez **Télécharger le fichier de certificats** et spécifiez les paramètres suivants :

- **Fichier de certificat** : chargez un fichier de certificat SSL en sélectionnant **Local** (votre machine locale) ou **Appliance** (le fichier de certificat doit être présent sur l'instance virtuelle Citrix ADM).
- **Fichier clé** : téléchargez le fichier clé.
- **Nom du certificat** —Spécifiez le nom de la clé de certificat.
- **Mot de passe** : mot de passe pour crypter la clé privée. Vous pouvez utiliser cette option pour télécharger des clés privées chiffrées.

- **Sélectionner les instances** : sélectionnez les instances Citrix ADM sur lesquelles vous souhaitez installer vos certificats.

4. Pour enregistrer la configuration en vue d'une utilisation ultérieure, activez la case à cocher **Enregistrer la configuration**.
5. Cliquez sur **OK**.



Créer une demande de signature de certificat (CSR)

February 1, 2024

Une demande de signature de certificat (CSR) est un bloc de texte chiffré qui est généré sur le serveur sur lequel le certificat sera utilisé. Il contient des informations qui seront incluses dans le certificat, telles que le nom de votre organisation, le nom commun (nom de domaine), la localité et le pays.

Pour créer un CSR à l'aide de Citrix ADM :

1. Dans Citrix Application Delivery Management (ADM), accédez à **Réseaux** > **Tableau de bord SSL**.
2. Cliquez sur l'un des graphiques pour afficher la liste des certificats SSL installés, puis sélectionnez le certificat pour lequel vous souhaitez créer un CSR et sélectionnez **Créer CSR** dans la liste **Sélectionner une action**.
3. Dans la page **Créer une demande de signature de certificat (CSR)**, spécifiez un nom pour la CSR.
4. Procédez comme suit :
    - **Télécharger une clé** : sélectionnez l'option **J'ai une clé** . Pour télécharger votre fichier de clé, sélectionnez **Local** (votre machine locale) ou **Appliance** (le fichier de clé doit être présent sur l'instance virtuelle Citrix ADM).
    - **Créer une clé** - Sélectionnez l'option Je n'ai pas de clé, puis spécifiez les paramètres suivants :

Algorithme de chiffrement	Type de clé. Par exemple, RSA.
Nom du fichier clé	Nom du fichier dans lequel la clé RSA est stockée.
Taille de la clé	Taille de la clé en bits.
Valeur de l'exposant public	Choisissez **3** ou **F4** dans la liste déroulante fournie. Cette valeur fait partie de l'algorithme de chiffrement requis pour créer votre clé RSA.
Format clé	Par défaut, PEM est sélectionné. PEM est le format de clé recommandé pour votre certificat SSL.
Algorithme d'encodage PEM	Dans la liste déroulante, sélectionnez l'algorithme (**DES** ou **DES3**) à utiliser pour chiffrer la clé RSA générée. Si vous sélectionnez cet algorithme, vous devrez fournir un mot de passe PEM.
Passphrase PEM	Si vous avez choisi l'algorithme de codage PEM, entrez un mot de passe.
Confirmer la phrase secrète PEM	Confirmez votre mot de passe PEM.

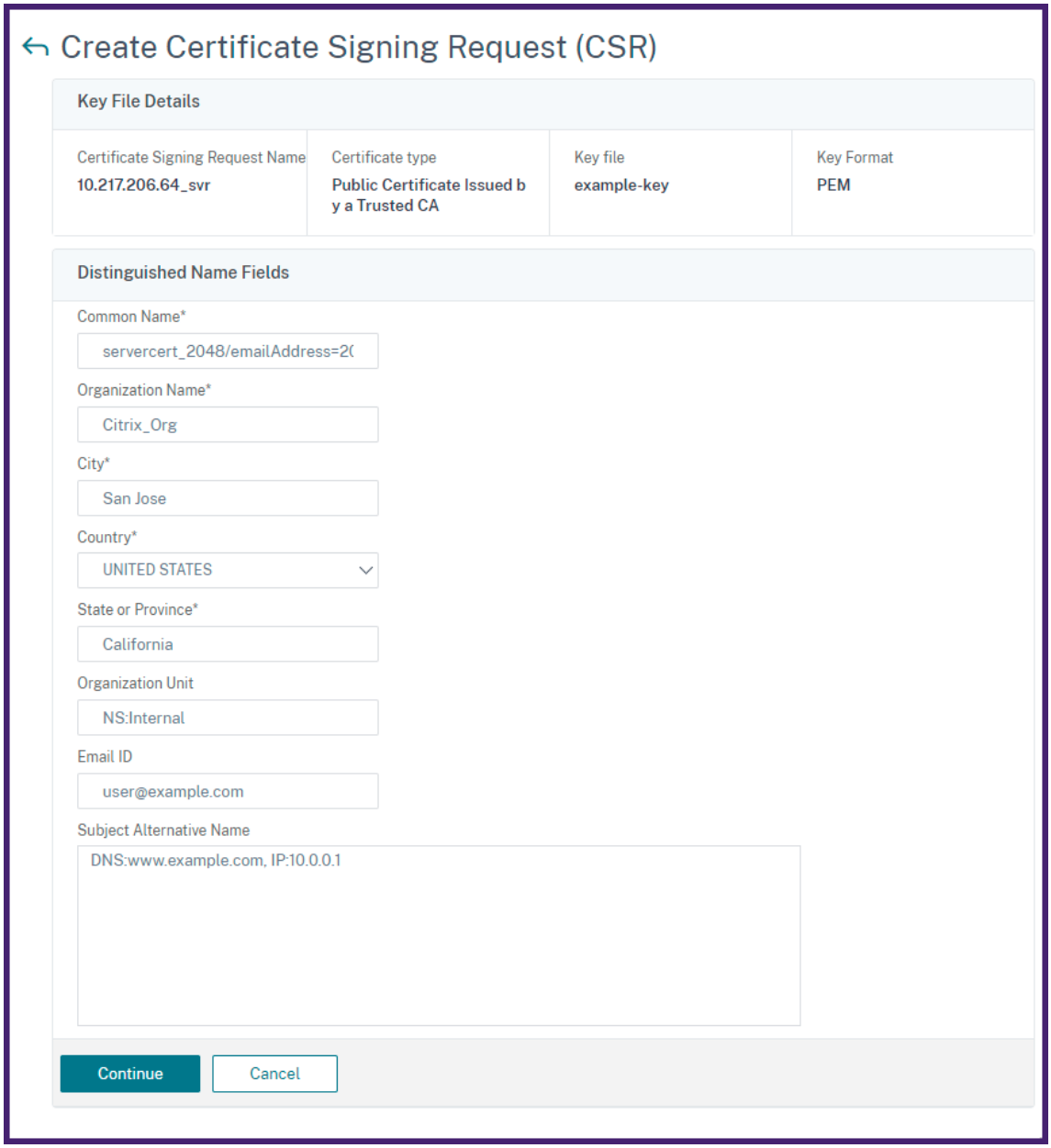
5. Cliquez sur **Continue**.
6. Sur la page suivante, fournissez plus de détails.

   La plupart des champs ont des valeurs par défaut extraites de l'objet du certificat sélectionné. L'objet contient des détails tels que le nom commun, le nom de l'organisation, l'état et le pays.

   Dans le champ **Nom alternatif de l'objet**, vous pouvez spécifier plusieurs valeurs, telles que des noms de domaine et des adresses IP avec un seul certificat. Les noms alternatifs d'objet vous aident à sécuriser plusieurs domaines avec un seul certificat.

   Spécifiez les noms de domaine et les adresses IP dans le format suivant :

```
DNS:<Domain name>, IP:<IP address>
<!--NeedCopy-->
```

Dans cet exemple, il sécurise `10.0.0.1` et `www.example.com`.

Vérifiez les champs et cliquez sur **Continuer**.

> **Remarque**
>
> La plupart des autorités de certification acceptent les soumissions de certificats par courriel. L'autorité de certification renvoie un certificat valide à l'adresse e-mail à partir de laquelle vous soumettez le CSR.

Lier et dissocier les certificats SSL

February 1, 2024

Vous créez un ensemble de certificats en liant plusieurs certificats entre eux. Pour lier un certificat à un autre certificat, l'émetteur du premier certificat doit correspondre au domaine du second certificat. Par exemple, si vous souhaitez lier le certificat A au certificat B, l'« émetteur » du certificat A doit correspondre au « domaine » du certificat B.

Pour lier un certificat SSL à un autre certificat à l'aide de Citrix ADM :

1. Dans Citrix Application Delivery Management (ADM), accédez à **Réseaux** > **Tableau de bord SSL**.
2. Cliquez sur l'un des graphiques pour afficher la liste des certificats SSL.
3. Sélectionnez le certificat que vous souhaitez lier, puis sélectionnez **Lien** dans la liste déroulante **Action** .
4. Dans la liste des certificats correspondants, sélectionnez le certificat auquel vous souhaitez lier, puis cliquez sur **OK**.

> **Remarque**
>
> Si aucun certificat correspondant n'est trouvé, le message suivant s'affiche : Aucun certificat trouvé à lier.

Pour dissocier un certificat SSL à l'aide de Citrix ADM :

1. Dans Citrix ADM, accédez à **Réseaux** > **Tableau de bord SSL**.
2. Cliquez sur l'un des graphiques pour afficher la liste des certificats SSL.
3. Choisissez l'un des certificats liés, puis sélectionnez **Dissocier dans** la liste déroulante **Action** .
4. Cliquez sur **OK**.

> **Remarque**
>
> Si le certificat sélectionné n'est pas lié à un autre certificat, le message suivant s'affiche : Le certificat n'a pas de lien d'autorité de certification.

Configurer une stratégie d'entreprise

February 1, 2024

Vous pouvez configurer une stratégie d'entreprise et ajouter toutes les autorités de certification approuvées, des algorithmes de signature sécurisés et sélectionner la force de clé recommandée pour vos clés de certificat dans Citrix Application Delivery Management (ADM). Si l'un des certificats installés sur votre instance Citrix Application Delivery Controller (ADC) n'a pas été ajouté à la stratégie d'entreprise, le tableau de bord des certificats SSL affiche l'émetteur de ces certificats comme **Non recommandé**.

De plus, si la force de la clé du certificat ne correspond pas à la force de clé recommandée dans la stratégie d'entreprise, le tableau de bord des certificats SSL affiche la force de ces clés comme **Non recommandée** .

Pour configurer une stratégie d'entreprise sur Citrix ADM :

1. Dans Citrix ADM, accédez à **Infrastructure** > Tableau de **bord SSL**, puis cliquez sur **Paramètres**.
2. Sur la page Paramètres SSL, cliquez sur l'icône **Modifier** pour ajouter toutes les autorités de certification de confiance, les algorithmes de signature sécurisée et sélectionner la force de clé recommandée pour vos certificats et clés.
3. Cliquez sur **Enregistrer** pour enregistrer votre stratégie d'entreprise.

Interroger les certificats SSL à partir d'instances Citrix ADC

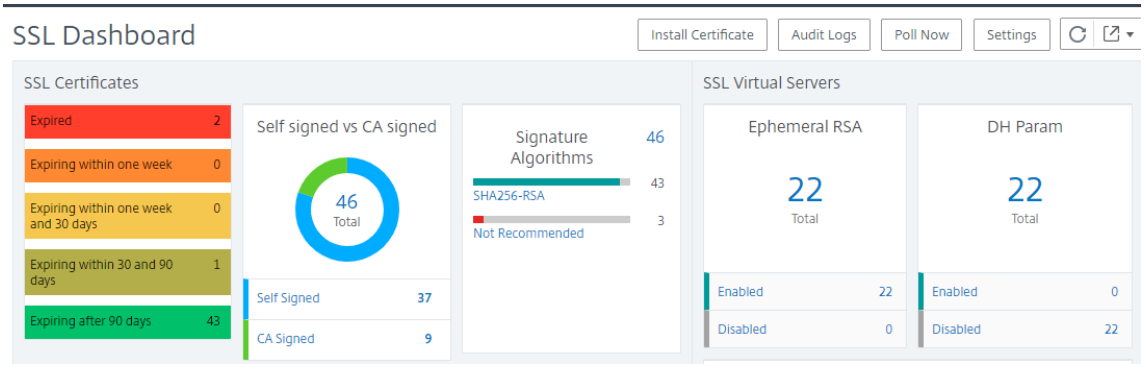
February 1, 2024

Citrix Application Delivery Management (ADM) interroge automatiquement les certificats SSL toutes les 24 heures à l'aide d'appels NITRO et du protocole Secure Copy (SCP). Vous pouvez également interroger manuellement les certificats SSL pour découvrir les certificats SSL nouvellement ajoutés sur les instances de Citrix Application Delivery Controller (ADC). L'interrogation de toutes les instances Citrix ADC certificats SSL place une lourde charge sur le réseau.

Au lieu d'interroger les certificats SSL de tous les instances Citrix ADC, vous pouvez interroger manuellement uniquement les certificats SSL d'une ou plusieurs instances sélectionnées.

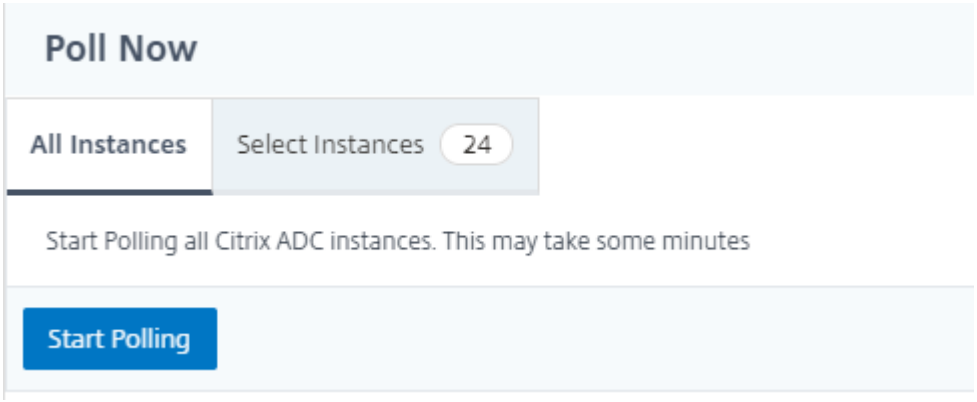
Pour interroger des certificats SSL sur des instances Citrix ADC :

1. Dans Citrix ADM, accédez à **Réseaux** > **Tableau de bord SSL**.
2. Dans la page **Tableau de bord SSL**, dans le coin supérieur droit, cliquez sur **Sondage maintenant** .

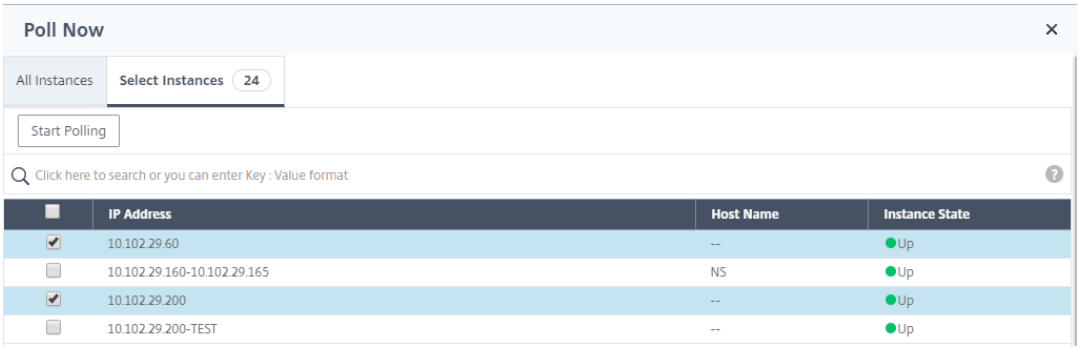


3. La page **Poll Now** s'affiche et vous permet d'interroger toutes les instances Citrix ADC du réseau ou d'interroger des instances sélectionnées.

   a) Pour interroger les certificats SSL de toutes les instances Citrix ADC, sélectionnez l'onglet **Toutes les instances** et cliquez sur **Démarrer**le sondage.



   b) Pour interroger des instances spécifiques, sélectionnez l'onglet **Sélectionner**des**instances**, sélectionnez les instances dans la liste, puis cliquez sur **Interroger maintenant**.



Configurer la gestion des adresses IP (IPAM)

February 1, 2024

ADM IPAM vous permet d'attribuer et de libérer automatiquement des adresses IP dans les configurations gérées par ADM. Vous pouvez attribuer des adresses IP à partir de réseaux ou de plages d'adresses IP définies à l'aide des fournisseurs IP suivants :

- Fournisseur IPAM intégré à ADM.
- Solution IPAM Infoblox. Pour plus d'informations, consultez Infoblox DDI.

Actuellement, vous pouvez utiliser ADM IPAM dans :

- **StyleBooks** : attribuez automatiquement des adresses IP aux serveurs virtuels lorsque vous créez des configurations.
- **Ingress de Kubernetes** : Affectez automatiquement une adresse IP virtuelle à une configuration d'entrée dans un cluster Kubernetes.

Vous pouvez également suivre les adresses IP allouées et disponibles dans chaque réseau ou plage d'adresses IP gérée par ADM.

Ajouter un fournisseur d'adresses IP externe

ADM dispose d'un fournisseur IPAM intégré pour gérer les adresses IP et les plages d'adresses IP. Si vous souhaitez ajouter une solution de fournisseur IP externe dans ADM, effectuez les opérations suivantes :

1. Accédez à **Réseaux > IPAM**.
2. Dans **Fournisseurs**, cliquez sur **Ajouter**.
3. Spécifiez les informations suivantes pour ajouter un fournisseur IP :
    - **Nom** : spécifiez le nom du fournisseur IP à utiliser dans ADM.
    - **Fournisseur** : sélectionnez un fournisseur d'adresses IP dans la liste.
    - **URL** : spécifiez l'URL de la solution IPAM qui attribue des adresses IP dans l'environnement ADM.
    - **Nom d'utilisateur** : spécifiez le nom d'utilisateur pour vous connecter à la solution IPAM.
    - **Mot de passe** : spécifiez le mot de passe pour vous connecter à la solution IPAM.
4. Cliquez sur **Ajouter**.

Ajouter un réseau

Ajoutez un réseau pour utiliser IPAM avec les configurations gérées ADM.

1. Accédez à **Réseaux > IPAM**.

2. Dans **Réseaux**, cliquez sur **Ajouter**.
3. Spécifiez les détails suivants :
   - **Nom du réseau** : spécifiez le nom du réseau pour identifier le réseau dans ADM.
   - **Fournisseur** : sélectionnez le fournisseur dans la liste.

     Cette liste affiche les fournisseurs ajoutés dans ADM.
   - **Type de réseau** : sélectionnez la **plage IP** ou le **CIDR** dans la liste en fonction de vos besoins.
   - **Valeur réseau** : spécifiez la valeur du réseau.

     > **Remarque**
     >
     > ADM IPAM prend uniquement en charge les adresses IPv4.

     Pour la **plage IP**, spécifiez la valeur du réseau au format suivant :

     ```
     <first-IP-address>-<last-IP-address>
     <!--NeedCopy-->
     ```

     Exemple :

     ```
     10.0.0.20-10.0.0.100
     <!--NeedCopy-->
     ```

     Pour **CIDR**, spécifiez la valeur du réseau au format suivant :

     ```
     <IP-address>/<subnet-mask>
     <!--NeedCopy-->
     ```

     Exemple :

     ```
     10.70.124.0/24
     <!--NeedCopy-->
     ```
4. Cliquez sur **Créer**.

Afficher les adresses IP allouées

Pour afficher plus de détails sur les adresses IP allouées à partir du réseau IPAM, procédez comme suit :

1. Accédez à **Réseaux > IPAM**.
2. Dans l'onglet **Réseaux**, cliquez sur **Afficher toutes les adresses IP allouées**.

   Ce volet affiche l'adresse IP, le nom du fournisseur, le fournisseur et la description. Il affiche également les détails de la ressource qui a réservé cette adresse IP :

- **Module** : Affiche le module ADM qui réserve l'adresse IP. Par exemple, si l'adresse IP est réservée par StyleBooks, cette colonne affiche StyleBooks comme module.
- **Type de ressource** : Affiche le type de ressource dans ce module. Pour le module StyleBooks, seul le type de ressource configurations utilise le réseau IPAM.
- **ID de ressource** : affiche l'ID de ressource avec un lien. Cliquez sur ce lien pour accéder à la ressource qui utilise l'adresse IP. Pour le type de ressource de configuration, l'ID de ressource s'affiche en tant qu'ID du pack de configuration.

> **Remarque**
>
> Si vous souhaitez libérer l'adresse IP, sélectionnez l'adresse IP à publier et cliquez sur **Libérer les adresses IP allouées**.

Tâches de configuration

February 1, 2024

Le processus de gestion de la configuration Citrix Application Delivery Management (Citrix ADM) garantit la réplication correcte des modifications de configuration, des mises à niveau du système et d' autres activités de maintenance sur plusieurs instances Citrix Application Delivery Controller (ADC) du réseau.

Citrix ADM vous permet de créer des tâches de configuration qui vous aident à effectuer toutes ces activités facilement sur plusieurs appareils en une seule tâche. Les tâches de configuration et les modèles simplifient les tâches administratives les plus répétitives en une seule tâche sur Citrix ADM. Une tâche de configuration contient un ensemble de commandes de configuration que vous pouvez exécuter sur un ou plusieurs appareils gérés.

Les tâches de configuration peuvent soit utiliser des commandes SSH pour effectuer des commandes de configuration, soit utiliser SCP pour copier des fichiers depuis localement ou vers une autre appliance. Par exemple, nous pouvons planifier un basculement HA ou une mise à niveau HA.

Vous pouvez créer une tâche de configuration à l'aide de l'une des quatre options suivantes dans Citrix ADM. Utilisez l'une de ces options pour créer une source réutilisable de commandes et d'instructions au système pour exécuter un travail de configuration.

1. Modèle de configuration
2. Instance
3. Fichier
4. Enregistrer et lire

Modèle de configuration

Vous pouvez créer des modèles de configuration tout en créant un travail et en enregistrant un ensemble de commandes de configuration en tant que modèle. Lorsque vous enregistrez ces modèles sur la page Créer des travaux, ils s'affichent automatiquement dans la page Créer un modèle.

> **Remarque**
> L'option **Renommer** est désactivée pour les modèles de configuration par défaut. Vous pouvez toutefois renommer les modèles de configuration personnalisés.

Vous pouvez utiliser l'un des modèles suivants :

Éditeur de configuration : vous pouvez utiliser l'éditeur de configuration pour saisir des commandes CLI, enregistrer la configuration en tant que modèle et l'utiliser pour configurer des tâches.

Modèle intégré : Vous pouvez choisir parmi une liste de modèles de configuration. Ces modèles fournissent les syntaxes des commandes CLI et vous permettent de spécifier des valeurs pour les variables. Les modèles intégrés sont répertoriés, avec leur description dans le tableau ci-dessous. Vous pouvez planifier une tâche à l'aide de l'option de modèle intégrée. Une tâche est un ensemble de commandes de configuration que vous pouvez exécuter sur une ou plusieurs instances gérées. Par exemple, vous pouvez utiliser l'option de modèle intégrée pour planifier une tâche de configuration des serveurs syslog. Vous pouvez également choisir d'exécuter le travail immédiatement ou de planifier l'exécution ultérieure.

Instance

Vous pouvez effectuer une mise à niveau groupée unique de vos instances Citrix SDX exécutant Citrix ADC version 11.0 et ultérieure. Pour effectuer une mise à niveau groupée unique, vous utilisez une tâche intégrée dans Citrix ADM. Vous pouvez également mettre à niveau une instance Citrix ADC en extrayant la configuration en cours d'exécution ou une configuration enregistrée et en exécutant les commandes sur une autre instance Citrix ADC du même type. Cela vous permet de répliquer la configuration d'une instance sur l'autre.

Fichier

Vous pouvez télécharger un fichier de configuration à partir de votre machine locale et créer des tâches.

Avantages de l'utilisation d'un fichier

- Vous pouvez utiliser n'importe quel fichier texte pour créer une source réutilisable de commandes de configuration.

- Aucun type de formatage n'est requis.
- Le fichier peut être enregistré sur votre ordinateur local.

Vous pouvez créer et enregistrer un nouveau fichier ou importer un fichier existant et exécuter les commandes.

Enregistrer et lire

À l'aide de Create job, vous pouvez entrer vos propres commandes CLI, ou vous pouvez utiliser le bouton Enregistrer et lire pour obtenir les commandes d'une session Citrix ADC. Lorsque vous exécutez le travail, les modifications apportées au fichier ns.conf sur l'instance sélectionnée sont enregistrées et copiées dans Citrix ADM.

Articles connexes

- Comment utiliser la commande SCP (put) dans les tâches de configuration
- Comment utiliser des variables dans les tâches de configuration
- Comment créer des tâches de configuration à partir de commandes correctives
- Comment utiliser les modèles de configuration pour créer des modèles d'audit
- Comment utiliser l'enregistrement et la lecture pour créer des tâches de configuration
- Comment faire pour utiliser le modèle de configuration maître sur Citrix ADM

Créer une tâche de configuration

February 1, 2024

Une tâche est un ensemble de commandes de configuration que vous pouvez créer et exécuter sur une ou plusieurs instances gérées. Vous pouvez créer des tâches pour apporter des modifications de configuration entre les instances, répliquer des configurations sur plusieurs instances de votre réseau et des tâches de configuration d'enregistrement et de lecture à l'aide de l'interface graphique Citrix Application Delivery Management (ADM) et les convertir en commandes CLI.

Vous pouvez utiliser la fonctionnalité Travaux de configuration de Citrix ADM pour créer une tâche de configuration, envoyer des notifications par e-mail et vérifier les journaux d'exécution des tâches créées.

Pour créer une tâche de configuration sur Citrix ADM :

1. Accédez à **Réseaux > Travaux de configuration**.

2. Cliquez sur **Créer un travail**.
3. Sur la page **Créer une tâche**, sous l'onglet **Sélectionner la configuration**, spécifiez le nom de la tâche et sélectionnez le **type d'instance** dans la liste.
4. Dans la liste **Source de configuration**, sélectionnez le modèle de tâche de configuration que vous souhaitez créer. Ajoutez les commandes du modèle sélectionné.

    - Vous pouvez saisir les commandes ou importer les commandes existantes à partir des modèles de configuration enregistrés.
    - Vous pouvez également ajouter plusieurs modèles de types différents dans l'éditeur de configuration lors de la création d'une tâche dans les tâches de configuration.
    - Dans la liste **Source de configuration**, sélectionnez les différents modèles, puis faites-les glisser dans l'éditeur de configuration. Les types de modèles peuvent être le **modèle de configuration**, **le modèle intégré**, la **configuration principale**, l'**enregistrement et la lecture**, l'**instance** et **le fichier**.

    > **Remarque**
    >
    > Si vous ajoutez le modèle `Deploy Master Configuration Job` pour la première fois, ajoutez un modèle de type différent, puis l'ensemble du modèle de tâche devient un type `Master Configuration`.

    Vous pouvez également réorganiser et réorganiser les commandes dans l'éditeur de configuration. Vous pouvez déplacer la commande d'une ligne à l'autre en faisant glisser la ligne de commande. Vous pouvez également déplacer ou réorganiser la ligne de commande d'une ligne à n'importe quelle ligne cible en changeant simplement le numéro de ligne de commande dans la zone de texte. Vous pouvez également réorganiser et réorganiser la ligne de commande lors de la modification du travail de configuration.

    Vous pouvez définir des variables qui vous permettent d'affecter des valeurs différentes pour ces paramètres ou d'exécuter un travail sur plusieurs instances. Vous pouvez consulter toutes les variables que vous avez définies lors de la création ou de la modification d'un travail de configuration dans une vue consolidée unique. Cliquez sur l'onglet**Aperçu des variables** pour prévisualiser les variables dans une vue consolidée unique que vous avez définie lors de la création ou de la modification d'une tâche de configuration.

    Vous pouvez personnaliser les commandes d'annulation pour chaque commande de l'éditeur de configuration. Pour spécifier vos commandes personnalisées, activez l'option de restauration personnalisée.

    > **Important**
    >
    > Pour que la restauration personnalisée prenne effet, exécutez l'assistant de **création de**

> **tâche** . Et dans l'onglet **Exécuter**, sélectionnez l'option Annuler **les commandes réussies dans** la liste En cas d'**échec de commande** .

5. Dans l'onglet **Sélectionner des instances**, sélectionnez les instances sur lesquelles vous souhaitez exécuter l'audit de configuration.

    a) Dans une paire Citrix ADC haute disponibilité, vous pouvez exécuter un travail de configuration local sur un nœud principal ou secondaire. Sélectionnez le nœud sur lequel vous souhaitez exécuter la tâche.

    - **Exécuter sur les nœuds principaux** - Sélectionnez cette option pour exécuter le travail uniquement sur les nœuds principaux.
    - **Exécuter sur les nœuds secondaires** - Sélectionnez cette option pour exécuter le travail uniquement sur les nœuds secondaires.

    Vous pouvez également choisir le nœud principal et le nœud secondaire pour exécuter le même travail de configuration. Si vous ne sélectionnez ni nœud principal ni secondaire, le travail de configuration s'exécute automatiquement sur le nœud principal.

6. Dans l'onglet **Spécifier les valeurs variables**, vous disposez de deux options :

    a) Téléchargez le fichier d'entrée pour entrer les valeurs des variables que vous avez définies dans vos commandes, puis téléchargez le fichier sur le serveur Citrix ADM.

    b) Entrez des valeurs communes pour les variables que vous avez définies pour toutes les instances

    c) Cliquez sur **Suivant**.

Pour envoyer un e-mail et une notification Slack pour une tâche :

Un e-mail et une notification Slack sont désormais envoyés chaque fois qu'une tâche est exécutée ou planifiée. La notification comprend des détails tels que le succès ou l'échec du travail ainsi que les détails pertinents.

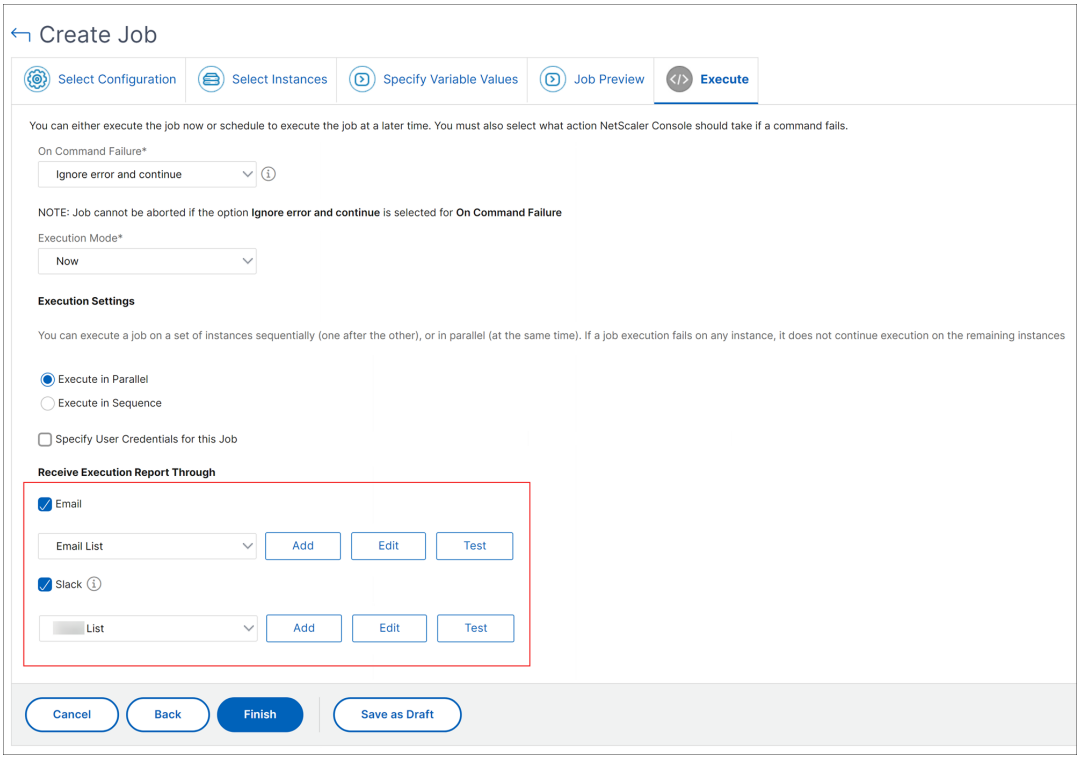
1. Accédez à **Réseaux**>**Travaux de configuration**.
2. Sélectionnez le travail que vous souhaitez activer la notification par e-mail et Slack, puis cliquez sur **Modifier**.
3. Dans l'onglet **Exécuter**, accédez au volet **Recevoir le rapport d'exécution via** :

    - Cochez la case **E-mail** et choisissez la liste de distribution d'e-mails à laquelle vous souhaitez envoyer le rapport d'exécution.

      Si vous souhaitez ajouter une liste de distribution d'e-mails, cliquez sur **Ajouter** et spécifiez les détails du serveur de messagerie.

- Cochez la case **Slack** et choisissez le canal Slack auquel vous souhaitez envoyer le rapport d'exécution.

  Si vous souhaitez ajouter un profil Slack, cliquez sur **Ajouter** et spécifiez le **nom du profil**, le **nom du canal** et le **jeton** du canal Slack requis.



4. Cliquez sur **Terminer**.

Pour envoyer un e-mail et une notification Slack pour une tâche :

Un e-mail et une notification Slack sont désormais envoyés chaque fois qu'une tâche est exécutée ou planifiée. La notification comprend des détails tels que le succès ou l'échec du travail ainsi que les détails pertinents.

1. Accédez à **Réseaux**>**Travaux de configuration**.
2. Sélectionnez le travail que vous souhaitez activer la notification par e-mail et Slack, puis cliquez sur **Modifier**.
3. Dans l'onglet **Exécuter**, accédez au volet **Recevoir le rapport d'exécution via** :

   - Cochez la case **E-mail** et choisissez la liste de distribution d'e-mails à laquelle vous souhaitez envoyer le rapport d'exécution.

     Si vous souhaitez ajouter une liste de distribution d'e-mails, cliquez sur **Ajouter** et spécifiez les détails du serveur de messagerie.

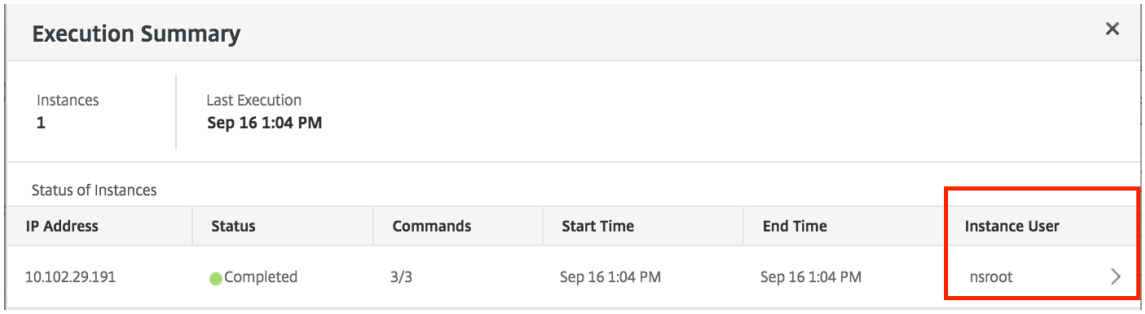
- Cochez la case **Slack** et choisissez le canal Slack auquel vous souhaitez envoyer le rapport d'exécution.

  Si vous souhaitez ajouter un profil Slack, cliquez sur **Ajouter** et spécifiez le **nom du profil**, le **nom du canal** et le **jeton** du canal Slack requis.

4. Cliquez sur **Terminer**.

Pour afficher les détails du récapitulatif d'exécution :

1. Accédez à **Réseaux** > **Travaux de configuration**.
2. Sélectionnez le travail que vous souhaitez afficher le résumé de l'exécution, puis cliquez sur **Détails**.
3. Cliquez sur **Résumé de l'exécution** pour afficher :
   - L'état de l'instance sur l'exécution de la tâche
   - Les commandes s'exécutent sur le travail
   - L'heure de début et de fin de la tâche, et
   - Nom de l'utilisateur de l'instance



Utiliser l'enregistrement et la lecture pour créer des tâches de configuration

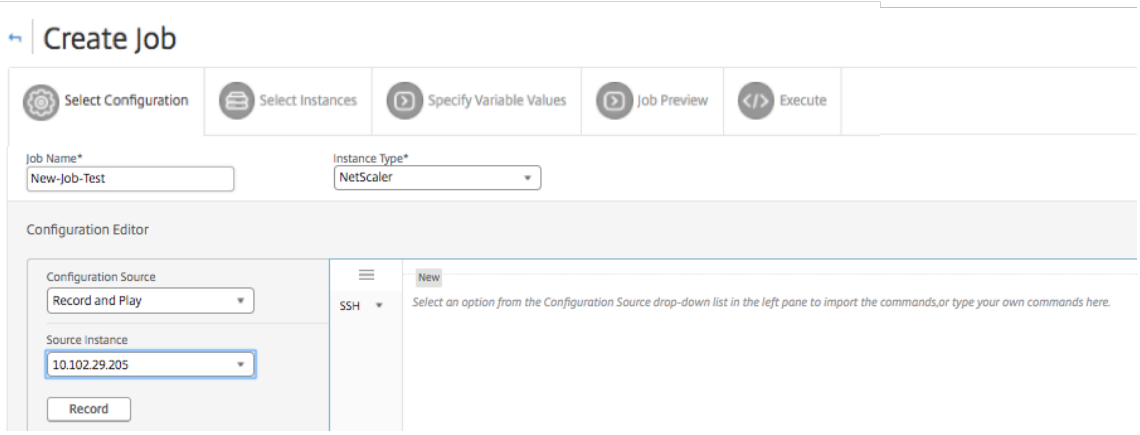
February 1, 2024

Si vous êtes habitué à utiliser l'interface graphique Citrix ADC pour configurer une instance Citrix ADC, il peut parfois être difficile de rappeler les commandes CLI exactes pour créer une tâche de configuration et l'exécuter sur plusieurs instances Citrix ADC.

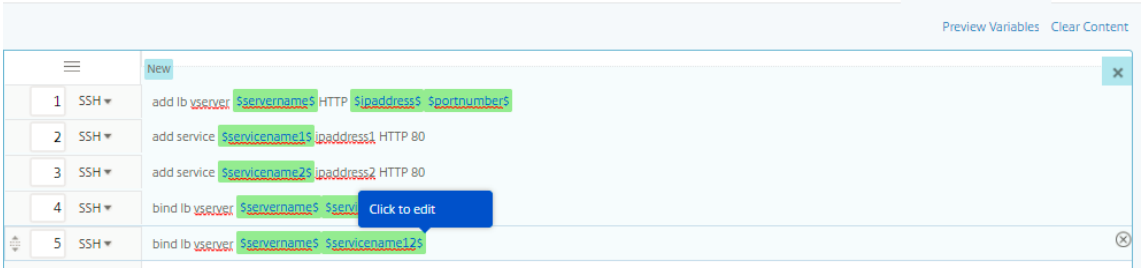
Citrix ADM vous permet d'enregistrer les tâches de configuration effectuées à l'aide de l'interface graphique d'une instance Citrix ADC et de les convertir en commandes CLI. Vous pouvez ensuite créer une tâche de configuration à partir de ces commandes CLI et exécuter cette tâche sur plusieurs instances.

Pour enregistrer la configuration de l'interface graphique et la convertir en tâche de configuration

1. Accédez à **Réseaux** > **Travaux de configuration**, puis cliquez sur **Créer un travail** .
2. Spécifiez le nom de la tâche et le type d'instance.
3. Dans la liste **Source de configuration**, sélectionnez **Record and Play**, puis sélectionnez l'instance source à partir de laquelle vous souhaitez enregistrer la configuration. Cliquez sur **Enregistrer**.



4. L'**interface graphique Citrix ADC** s'ouvre. Configurez les fonctionnalités et paramètres que vous souhaitez que la tâche de configuration contienne. Fermez ensuite la fenêtre de l'interface graphique Citrix ADC et cliquez sur **Arrêter** dans l'**éditeur de configuration**. Les commandes apparaissent sous la forme d'un lien dans le volet gauche. Faites glisser les commandes vers le volet droit, puis cliquez sur **Suivant**.



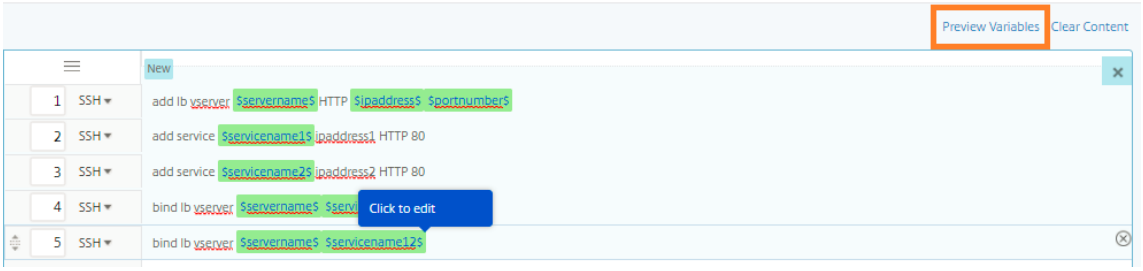
Vous pouvez ensuite réorganiser les commandes dans l'éditeur de configuration selon les besoins. Vous pouvez déplacer la commande d'une ligne à l'autre en faisant glisser la ligne de commande. Vous pouvez également déplacer ou réorganiser la ligne de commande d'une ligne à n'importe quelle ligne cible en changeant simplement le numéro de ligne de commande dans la zone de texte.

5. Vous pouvez consulter toutes les variables que vous avez définies lors de la création ou de la modification d'un travail de configuration dans une vue consolidée unique.

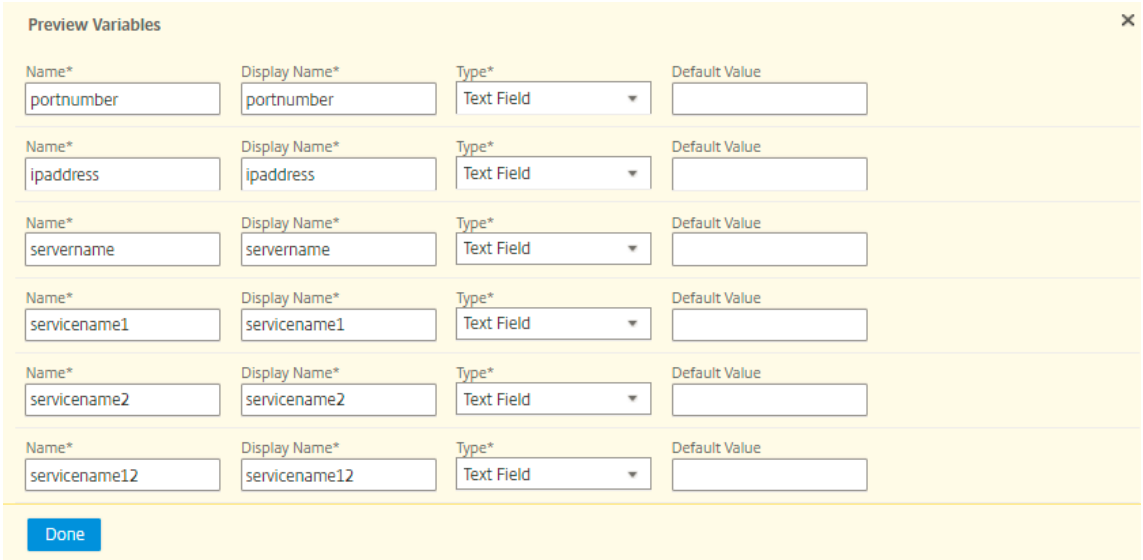
6. Pour afficher toutes les variables dans une seule vue consolidée, procédez de l'une des manières suivantes :

   - Lors de la création d'une tâche de configuration, accédez à **Réseaux > Tâches de configuration**, puis sélectionnez **Créer une tâche**. Sur la page **Créer un travail**, vous pouvez consulter toutes les variables que vous avez ajoutées lors de la création du travail de configuration.
   - Lorsque vous modifiez une tâche de configuration, accédez à **Réseau > Tâches de configuration**, sélectionnez le nom de la tâche et cliquez sur **Modifier**. Sur la page **Configurer la tâche**, vous pouvez consulter toutes les variables qui ont été ajoutées lors de la création de la tâche de configuration.

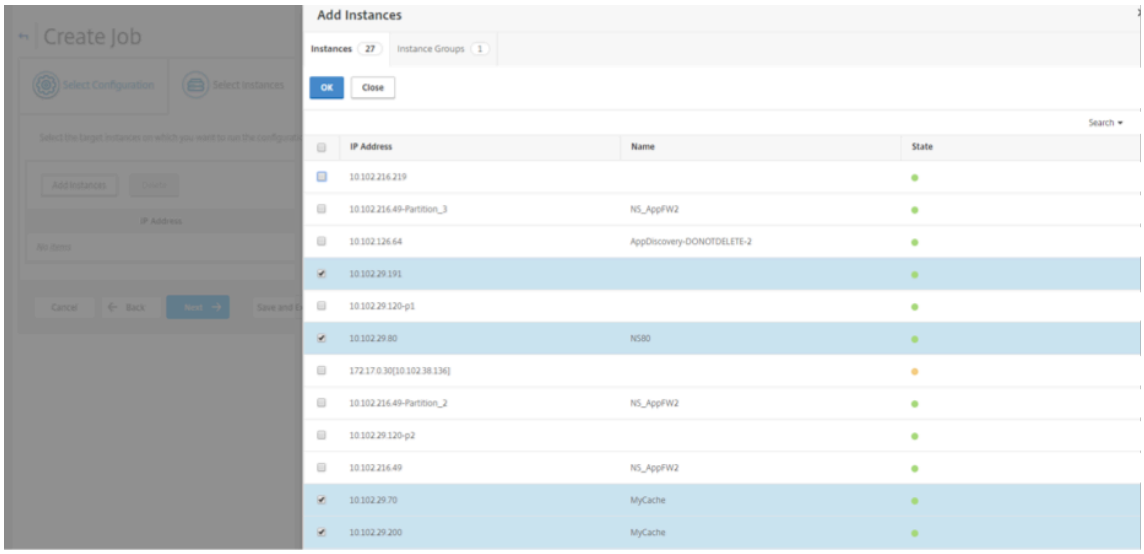
7. Vous pouvez ensuite cliquer sur l'onglet **Aperçu des variables** pour prévisualiser les variables dans une vue consolidée unique que vous avez définie lors de la création ou de la modification d'un travail de configuration.



8. Une nouvelle fenêtre contextuelle apparaît et affiche tous les paramètres des variables telles que Nom, Nom d'affichage, Type et valeur par défaut dans un format tabulaire. Vous pouvez également modifier et modifier ces paramètres. Cliquez sur le bouton **Terminé** après avoir modifié l'un des paramètres.



9. Cliquez sur**Ajouter des instances**et sélectionnez les instances sur lesquelles vous souhaitez exécuter le travail de configuration. Cliquez sur**OK**, puis sur**Suivant**.



10. Si vous avez spécifié des variables dans les commandes, sous l'onglet**Spécifier des valeurs variables**, sélectionnez l'une des options suivantes pour spécifier des variables pour vos instances :

    - **Télécharger le fichier d'entrée pour les valeurs des variables :** cliquez sur**Télécharger le fichier clé d'entrée**pour télécharger un fichier d'entrée. Dans le fichier d'entrée, entrez des valeurs pour les variables que vous avez définies dans vos commandes, puis téléchargez le fichier sur le serveur Citrix ADM.
    - **Valeurs de variables communes pour toutes les instances** : entrez des valeurs pour les variables. Les variables varient en fonction du modèle sélectionné.

    Les fichiers d'entrée contenant les valeurs des variables sont conservés (avec le même nom de fichier) dans les tâches de configuration. Vous pouvez afficher et modifier ces fichiers d'entrée que vous avez utilisés et chargés précédemment lors de la création ou de la modification des tâches de configuration.

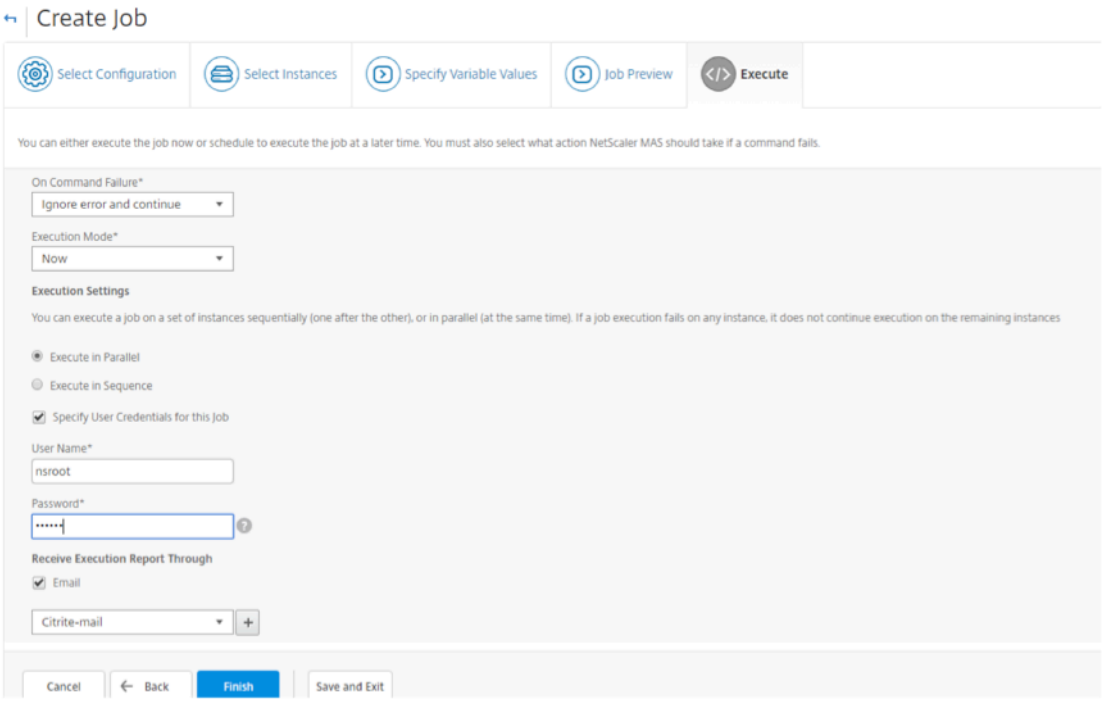
    Pour afficher les travaux de configuration d'exécution lors de la création d'un travail de configuration, accédez à **Réseau > Travaux de configuration**, puis cliquez sur **Créer un travail**. Dans la page **Créer une tâche**. Dans l'onglet **Spécifier les valeurs des variables**, sélectionnez l'option **Valeurs de variables communes pour toutes les instances** pour afficher les fichiers téléchargés. Pour modifier les fichiers d'entrée, téléchargez le fichier d'entrée, puis modifiez et chargez les fichiers (en conservant le même nom de fichier).

    Pour afficher les travaux de configuration déjà exécutés lors de la modification d'un travail de configuration, accédez à **Réseau > Travaux de configuration**, sélectionnez le nom du travail et cliquez sur **Modifier**. Dans la page **Configurer la tâche**, sous l'onglet **Spécifier les valeurs de**

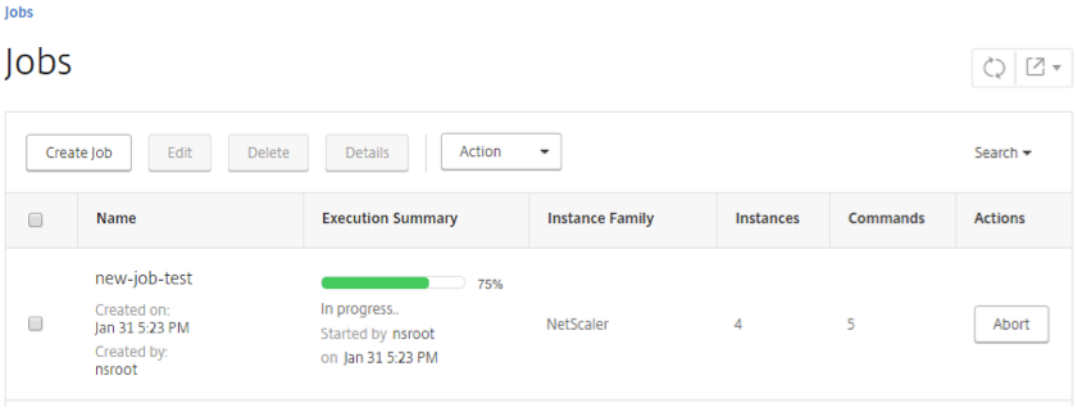
variable, sélectionnez l'option **Valeurs variables communes pour toutes les instances** pour afficher les fichiers chargés. Pour modifier les fichiers d'entrée, téléchargez le fichier d'entrée, puis modifiez et téléchargez les fichiers (en conservant le même nom de fichier) .10.Sous l'onglet **Aperçu des tâches**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances.

11. Sous l'onglet**Aperçu du travail**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances.
12. Sous l'onglet**Exécuter**, vous pouvez choisir d'exécuter votre travail maintenant ou de le programmer pour qu'il soit exécuté ultérieurement. Vous pouvez également choisir l'action que Citrix ADM doit prendre en cas d'échec de la commande.

    Vous pouvez également choisir d'autoriser les utilisateurs autorisés à exécuter des travaux sur vos instances gérées, et vous pouvez choisir d'envoyer une notification par e-mail concernant le succès ou l'échec de la tâche, ainsi que d'autres détails.



13. Sur la page **Tâches**, vous pouvez ensuite afficher la progression de l'exécution de votre tâche de configuration sur toutes les instances.



Utiliser les tâches de configuration pour répliquer la configuration d'une instance vers plusieurs instances

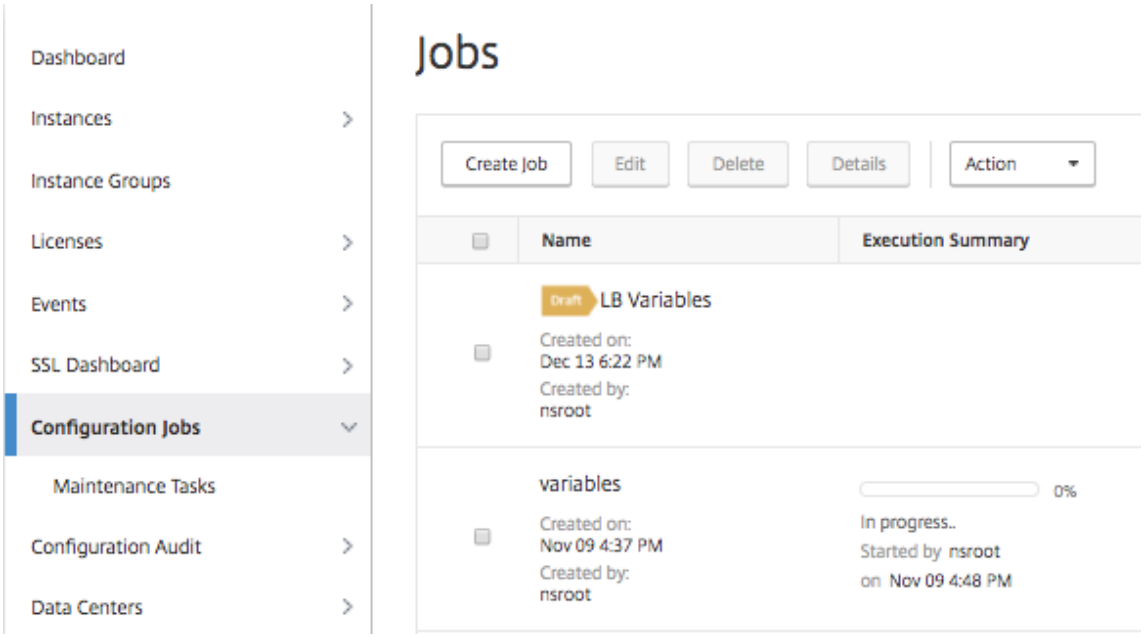
February 1, 2024

Vous pouvez utiliser la fonctionnalité Configuration Jobs de Citrix ADM pour extraire une configuration particulière d'une instance Citrix ADC et la répliquer sur plusieurs instances.

Par exemple, vous avez peut-être configuré à la fois l'équilibrage de charge et l'optimisation frontale (FEO) sur une instance Citrix ADC pour votre déploiement. Toutefois, vous souhaitez désormais répliquer uniquement la configuration FEO sur d'autres instances Citrix ADC.

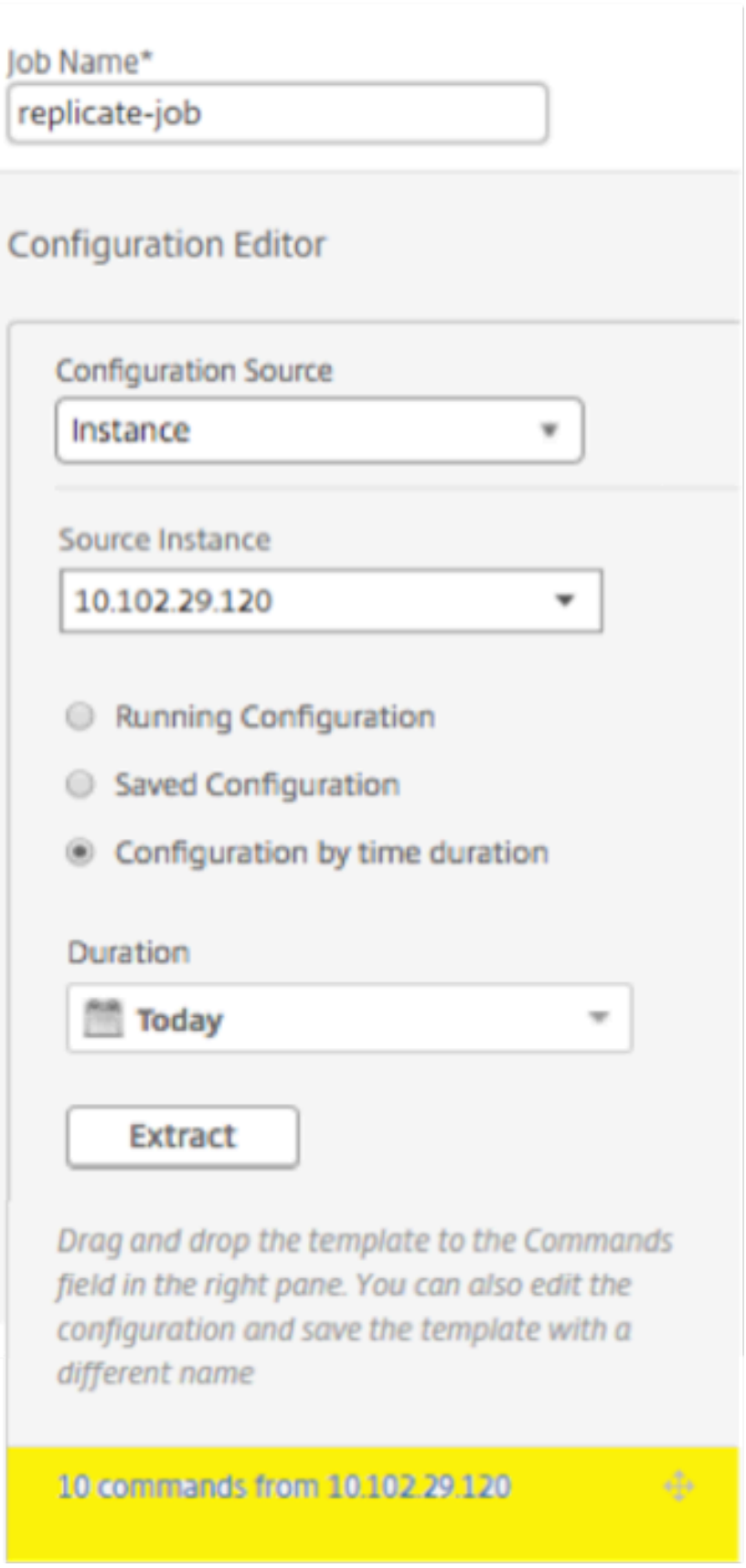
Pour récupérer et répliquer la configuration d'une instance vers d'autres instances Citrix ADC :

1. Accédez à **Réseaux** > **Travaux de configuration**, puis cliquez sur **Créer un travail** .



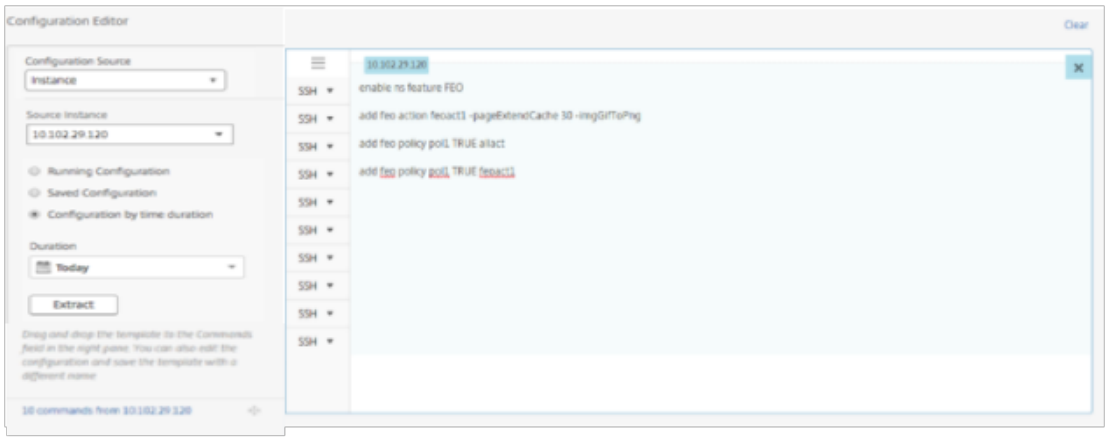
2. Spécifiez le nom de la tâche et le type d'instance.
3. Sélectionnez **Instance** comme **source de configuration** et sélectionnez l'instance source dont vous souhaitez répliquer la configuration. Sélectionnez le type de configuration que vous souhaitez extraire. Si vous sélectionnez « Configuration par durée de temps », définissez la période pendant laquelle vous avez exécuté cette configuration, puis cliquez sur **Extraire**.

   Le nombre de commandes exécutées sur cette instance pendant la durée sélectionnée est affiché à l'écran comme mis en surbrillance dans l'image suivante.



4. Faites glisser les commandes vers le champ **Commandes** dans le volet droit.

Conservez uniquement les commandes liées à FEO et supprimez manuellement les commandes liées à l'équilibrage de charge ou les commandes liées à toute autre configuration, puis cliquez sur **Suivant**.



5. Cliquez sur **Ajouter des instances** et ajoutez les instances sur lesquelles vous souhaitez appliquer la configuration FEO. Cliquez sur **OK**, puis sur **Suivant**.
6. Si vous avez spécifié des variables dans les commandes, dans l'onglet Spécifier les valeurs des variables, cliquez sur **Télécharger le fichier clé d'entrée**. Dans le fichier téléchargé, spécifiez les valeurs des variables, puis chargez le fichier sur Citrix ADM.
7. Sous l'onglet **Aperçu des tâches**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances.
8. Sous l'onglet **Exécuter**, cliquez sur **Terminer** pour exécuter le travail sur les instances Citrix ADC sélectionnées.

Utiliser des variables dans les tâches de configuration

February 1, 2024

Un travail de configuration est un ensemble de commandes de configuration que vous pouvez exécuter sur une ou plusieurs instances gérées. Lorsque vous exécutez la même configuration sur plusieurs instances, vous pouvez utiliser des valeurs différentes pour les paramètres utilisés dans votre configuration. Vous pouvez définir des variables qui vous permettent d'affecter des valeurs différentes pour ces paramètres ou d'exécuter un travail sur plusieurs instances.

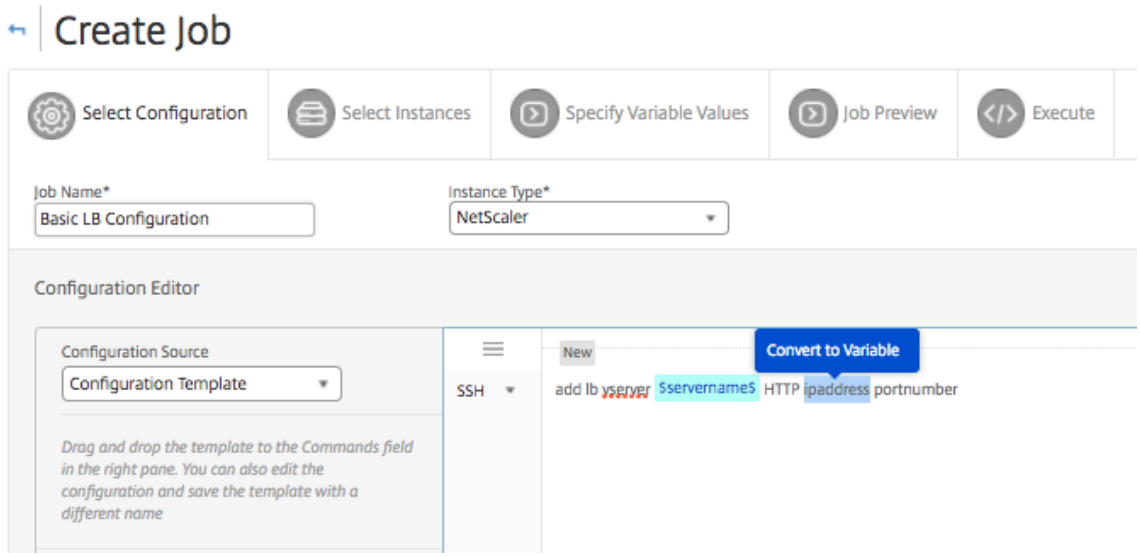
Par exemple, envisagez une configuration d'équilibrage de charge de base dans laquelle vous ajoutez un serveur virtuel d'équilibrage de charge, ajoutez deux services et liez les services au serveur virtuel. À présent, vous souhaiterez peut-être avoir la même configuration sur deux instances, mais avec des valeurs différentes pour le serveur virtuel, les noms de services et les adresses IP. Vous pouvez utiliser la fonctionnalité de tâches de configuration pour y parvenir en utilisant des variables pour définir les noms et les adresses IP du serveur virtuel et des services.

Dans cet exemple, les commandes et variables suivantes sont utilisées :

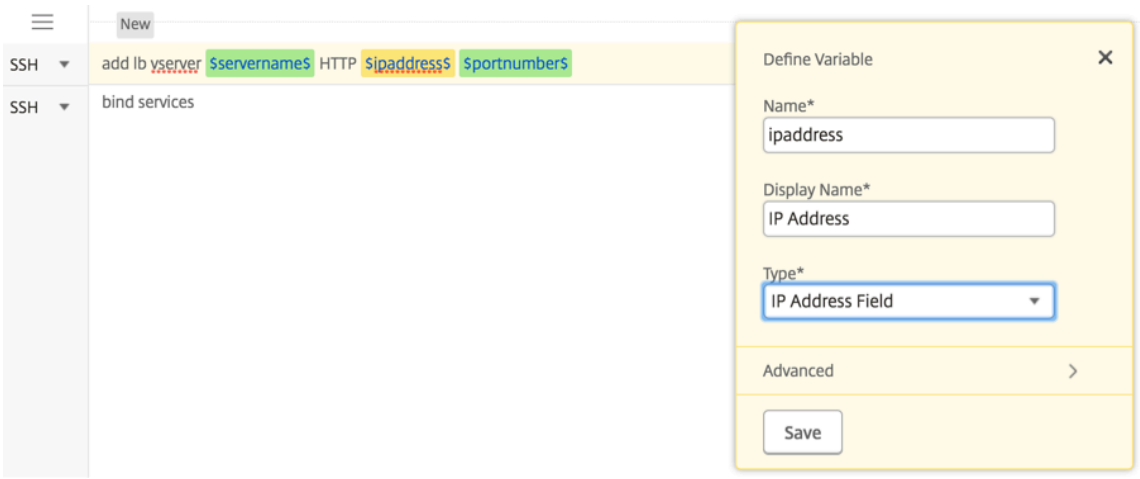
```
add lb vserver <servername> HTTP <ipaddress> <portnumber>
add service <servicename1> <ipaddress1> HTTP 80
add service <servicename2> <ipaddress2> HTTP 80
bind lb vserver <servername> <servicename1>
bind lb vserver <servername> <servicename2>
```

Pour créer une tâche de configuration en définissant des variables dans Citrix ADM :

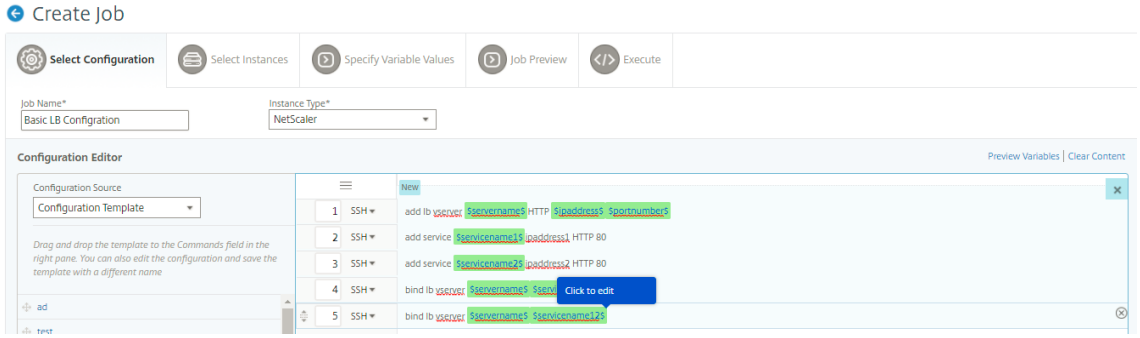
1. Accédez à **Réseaux** > **Travaux de configuration**.
2. Cliquez sur **Créer une tâche**.
3. Sur la page **Créer une tâche**, sélectionnez les paramètres de tâche personnalisés tels que le nom de la tâche, le type d'instance et le type de configuration.
4. Dans l'Éditeur de configuration, tapez les commandes pour ajouter un serveur virtuel d'équilibrage de charge, deux services et lier les services au serveur virtuel. Double-cliquez pour sélectionner les valeurs que vous souhaitez convertir en variable, puis cliquez sur **Convertir en variable**. Par exemple, sélectionnez l'adresse IP du serveur d'équilibrage de charge `*ipaddress *`, puis cliquez sur **Convertir en variable** comme illustré dans l'image suivante.



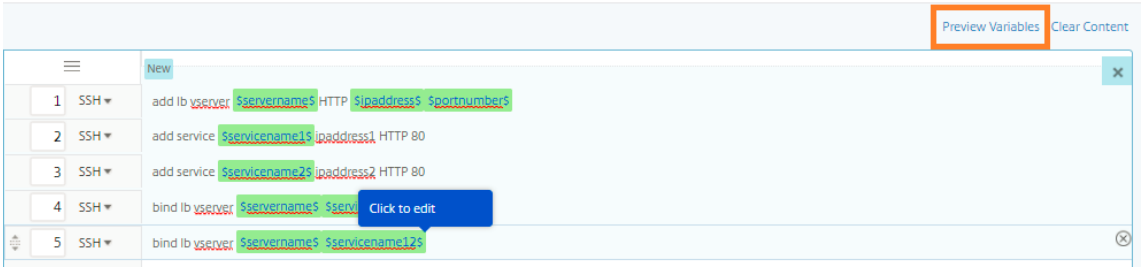
5. Une fois que vous voyez des signes dollar enferment la valeur de la variable, cliquez sur la variable pour spécifier davantage les détails de la variable, tels que le nom, le nom complet et le type. Vous pouvez également cliquer sur l'option **Avancé** si vous souhaitez spécifier une valeur par défaut pour votre variable. Cliquez sur **Enregistrer**, puis sur **Suivant**.



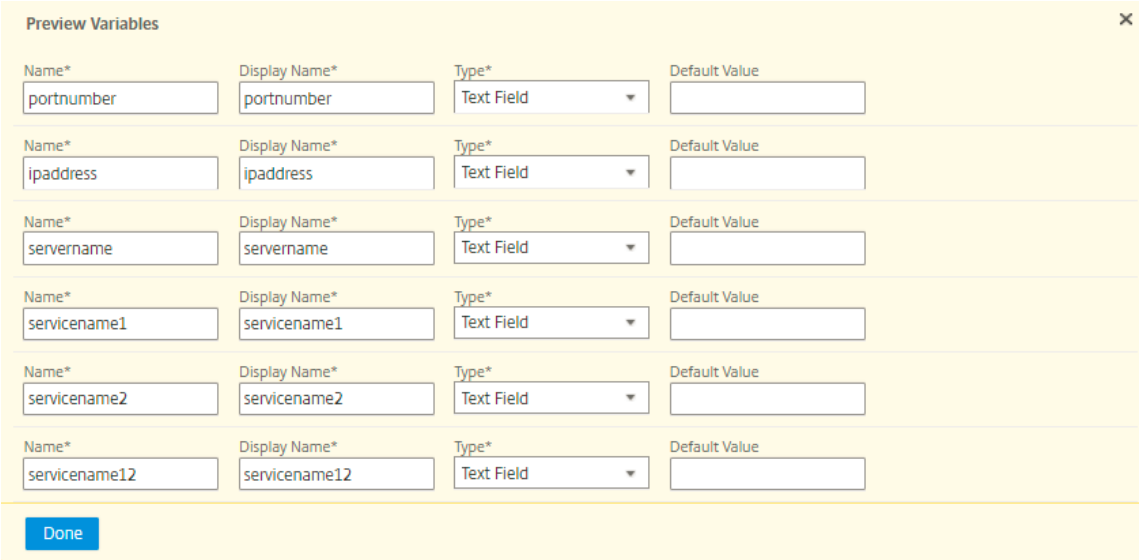
Tapez le reste de vos commandes et définissez toutes les variables.



6. Vous pouvez consulter toutes les variables que vous avez définies lors de la création ou de la modification d'un travail de configuration dans une vue consolidée unique.
7. Pour afficher toutes les variables dans une seule vue consolidée, procédez de l'une des manières suivantes :
   - Lors de la création d'une tâche de configuration, accédez à **Réseaux > Tâches de configuration**, puis sélectionnez **Créer une tâche**. Sur la page **Créer un travail**, vous pouvez consulter toutes les variables que vous avez ajoutées lors de la création du travail de configuration.
   - Lorsque vous modifiez une tâche de configuration, accédez à **Réseau > Tâches de configuration**, sélectionnez le nom de la tâche et cliquez sur **Modifier**. Sur la page **Configurer la tâche**, vous pouvez consulter toutes les variables qui ont été ajoutées lors de la création de la tâche de configuration.
8. Vous pouvez ensuite cliquer sur l'onglet **Aperçu des variables** pour prévisualiser les variables dans une vue consolidée unique que vous avez définie lors de la création ou de la modification d'un travail de configuration.



9. Une nouvelle fenêtre contextuelle apparaît et affiche tous les paramètres des variables telles que Nom, Nom d'affichage, Type et valeur par défaut dans un format tabulaire. Vous pouvez également modifier et modifier ces paramètres. Cliquez sur le bouton **Terminé** après avoir modifié l'un des paramètres.



10. Vous pouvez ensuite réorganiser les commandes dans l'éditeur de configuration selon les besoins. Vous pouvez déplacer la commande d'une ligne à l'autre en faisant glisser la ligne de commande. Vous pouvez également déplacer ou réorganiser la ligne de commande d'une ligne à n'importe quelle ligne cible en changeant simplement le numéro de ligne de commande dans la zone de texte.
11. Sélectionnez les instances sur lesquelles vous souhaitez exécuter le travail de configuration.
12. Dans l'onglet **Spécifier les valeurs variables**, sélectionnez l'option **Télécharger le fichier d'entrée pour les valeurs variables**, puis cliquez sur **Télécharger le fichier clé d'entrée**. Dans notre exemple, vous devrez spécifier le nom du serveur sur chaque instance, les adresses IP du serveur et des services, les numéros de port et les noms de service. Enregistrez le fichier et téléchargez-le. Si vos valeurs ne sont pas définies avec précision, le système peut déclencher une erreur.
13. Le fichier de clé d'entrée est téléchargé sur votre système local et vous pouvez le modifier en spécifiant les valeurs des variables pour chaque instance Citrix ADC que vous avez sélectionnée précédemment et en cliquant sur **Télécharger pour télécharger** le fichier de clé d'entrée sur Citrix ADM. Cliquez sur **Suivant**. Le fichier de clé en entrée est téléchargé sur votre système local et vous pouvez le modifier en spécifiant les valeurs de variable pour chaque instance Citrix ADC que vous avez sélectionnée précédemment.

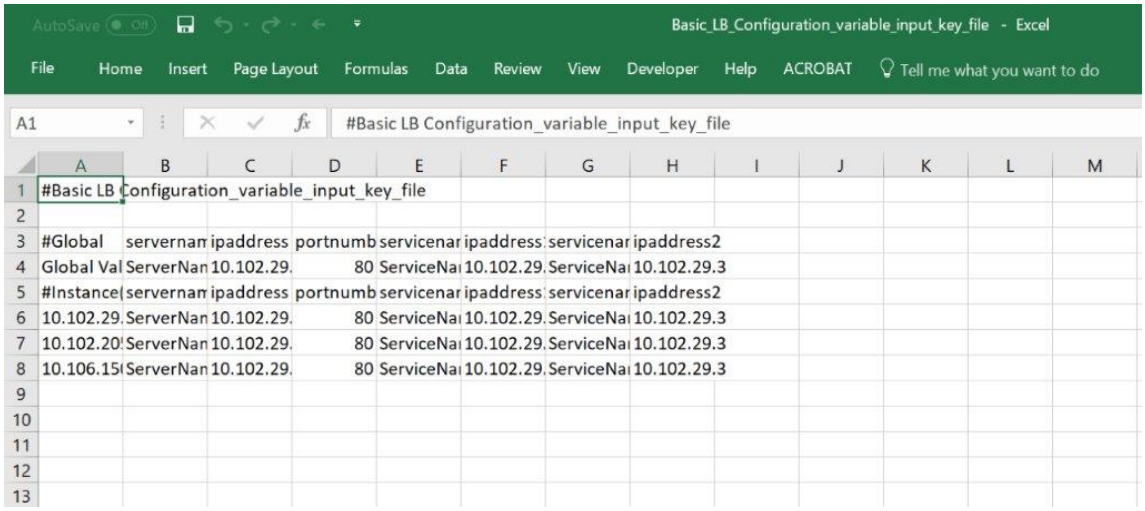
    > **Remarque** Dans le fichier clé en entrée, les variables sont définies à trois niveaux :
    >
    > - Au niveau mondial
    > - Au niveau du groupe d'instances
    > - Niveau de l'instance

    Les variables globales sont des valeurs variables appliquées à toutes les instances. Les valeurs des variables au niveau du groupe d'instances sont appliquées à toutes les instances définies

dans un groupe. Les valeurs des variables au niveau de l'instance ne sont appliquées qu'à une instance spécifique.

Citrix ADM donne la priorité aux valeurs au niveau de l'instance. Si aucune valeur n'est fournie aux variables pour les instances individuelles, Citrix ADM utilise la valeur fournie au niveau du groupe. Si aucune valeur n'est fournie au niveau du groupe, Citrix ADM utilise la valeur variable fournie au niveau global. Si vous fournissez une entrée pour une variable sur les trois niveaux, Citrix ADM utilise la valeur de niveau d'instance comme valeur par défaut.

14. Cliquez sur **Télécharger** pour télécharger le fichier clé d'entrée sur Citrix ADM. Cliquez sur **Suivant**.



> **Important**
>
> Lorsque vous téléchargez un fichier CSV à partir d'un Mac, le Mac stocke le fichier CSV avec des points-virgules au lieu de virgules. Cela entraînera l'échec de la configuration lorsque vous téléchargez le fichier d'entrée et exécutez le travail. Si vous utilisez un Mac, utilisez un éditeur de texte pour apporter les modifications nécessaires, puis téléchargez le fichier.

15. Vous pouvez également attribuer des valeurs de variables communes à toutes les instances et cliquer sur**Télécharger** pour télécharger le fichier clé d'entrée vers Citrix ADM.

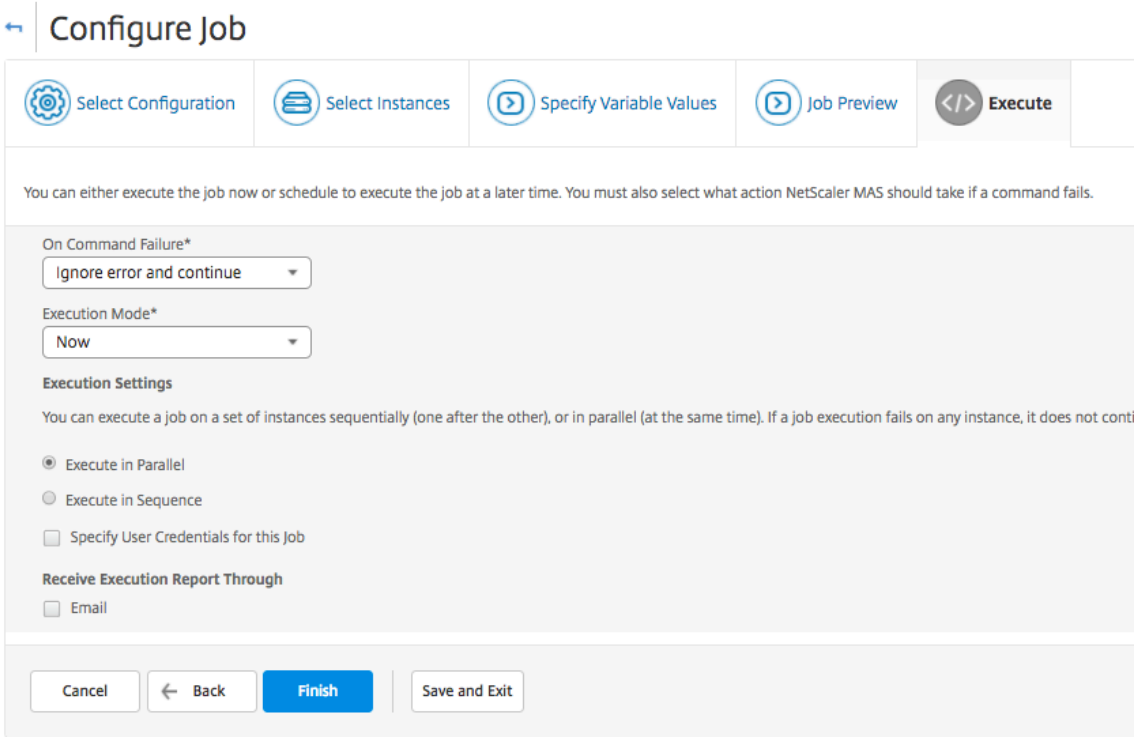
    Les fichiers d'entrée de clé contenant les valeurs des variables sont conservés (avec le même nom de fichier) dans les tâches de configuration. Vous pouvez afficher et modifier ces fichiers d'entrée que vous avez utilisés et chargés précédemment lors de la création ou de la modification des tâches de configuration.

    Pour afficher les travaux de configuration d'exécution lors de la création d'un travail de configuration, accédez à **Réseau > Travaux de configuration**, puis cliquez sur **Créer un travail**. Dans la page **Créer une tâche**. Dans l'onglet **Spécifier les valeurs des variables**, sélectionnez l'option **Valeurs de variables communes pour toutes les instances** pour afficher les fichiers

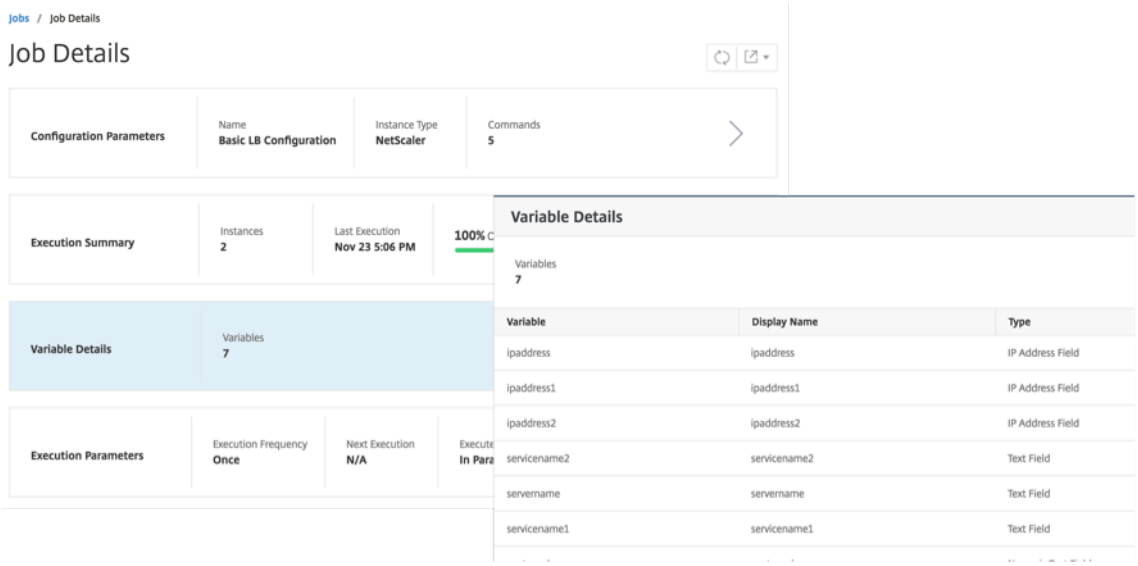
téléchargés. Pour modifier les fichiers d'entrée, téléchargez le fichier d'entrée, puis modifiez et chargez les fichiers (en conservant le même nom de fichier).

Pour afficher les travaux de configuration déjà exécutés lors de la modification d'un travail de configuration, accédez à **Réseau > Travaux de configuration**, sélectionnez le nom du travail et cliquez sur **Modifier**. Dans la page **Configurer la tâche**, sous l'onglet **Spécifier les valeurs de variable**, sélectionnez l'option **Valeurs variables communes pour toutes les instances** pour afficher les fichiers chargés. Pour modifier les fichiers d'entrée, téléchargez le fichier d'entrée, puis modifiez et chargez les fichiers (en conservant le même nom de fichier).

16. Sous l'onglet **Aperçu des tâches**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances.
17. Dans l'onglet **Exécuter**, vous pouvez choisir d'exécuter votre travail maintenant ou de le planifier ultérieurement. Vous pouvez également choisir l'action que Citrix ADM doit prendre si la commande échoue et si vous souhaitez envoyer une notification par e-mail concernant le succès ou l'échec de la tâche ainsi que d'autres détails.



Après avoir configuré vos tâches et les exécuter, vous pouvez voir les détails du travail en accédant à **Réseaux** > **Travaux de configuration** et sélectionnez le travail que vous venez de configurer. Cliquez sur **Détails**, puis cliquez sur **Détails des variables** pour afficher la liste des variables ajoutées à votre travail.



> **Remarque**
>
> Les valeurs que vous avez fournies pour les variables à l'**ÉTAPE 5** sont conservées par Citrix ADM lorsque vous enregistrez la tâche et la quittez, ou lorsque vous planifiez l'exécution d'une tâche ultérieurement.

Créer des tâches de configuration à partir de commandes correctives

February 1, 2024

Vous pouvez utiliser la fonctionnalité de modèle d'audit dans Citrix Application Delivery Management (ADM) pour surveiller les modifications de configuration des instances Citrix ADC gérées et résoudre les erreurs de configuration.

Le flux de travail typique pour l'audit des modifications de configuration à l'aide de modèles d'audit se compose des étapes suivantes :

1. Créez un modèle d'audit avec un ensemble de commandes Citrix ADC valides/attendues pour auditer les configurations d'instance.
2. Sélectionnez les instances Citrix ADC sur lesquelles vous souhaitez exécuter le modèle d'audit pour vérifier les différences entre la configuration en cours d'exécution et les configurations attendues.
3. Comprendre les commandes différentielles/correctrices et utiliser la fonctionnalité « Create Job » pour obtenir les configurations de l'instance à l'état souhaité

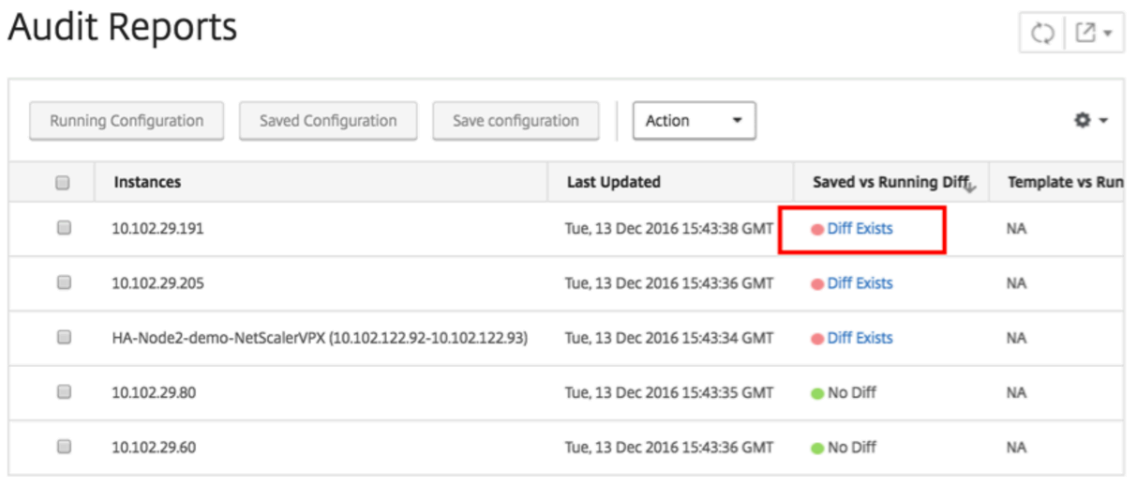
Imaginez un scénario dans lequel plusieurs administrateurs gèrent cinq instances Citrix ADC. Tous ces administrateurs mettent à jour la configuration de l'instance existante au fur et à mesure que des modifications sont nécessaires. Le super administrateur veut s'assurer qu'un certain ensemble de configuration importante reste intact, indépendamment des modifications apportées par d'autres administrateurs. Dans ce cas d'utilisation, le super administrateur crée un modèle de configuration censé être présent sur les instances Citrix ADC et l'exécute sur les instances. Citrix ADM compare la configuration du modèle d'audit à la configuration en cours d'exécution et signale toute incompatibilité dans le tableau de bord **Audit de configuration**.

Si vous remarquez une modification de la configuration de certaines instances, vous pouvez utiliser la fonctionnalité de commandes correctives Citrix ADM pour créer une tâche de configuration avec les commandes de configuration modifiées et corrigées pour des instances Citrix ADC spécifiques.

S'il existe une différence entre la configuration du modèle d'audit et la configuration en cours d'exécution, un message d'état **Différent existe** apparaît sur la page **Rapport d'audit** . En cliquant sur le lien **Diff Exist**, vous accédez à la page **Configuration Diff**, où vous pouvez afficher la commande corrective. Vous pouvez également utiliser ces commandes correctives pour créer un travail de configuration et l'exécuter sur les instances Citrix ADC spécifiques pour les ramener à la configuration souhaitée.

Pour créer une tâche de configuration à partir de commandes correctives sur Citrix ADM

1. Accédez à **Réseaux** > **Audit de configuration**.
2. Sur la page **Audit de configuration**, cliquez à l'intérieur de l'un des deux graphiques en donut pour accéder à la page **Rapports d'audit** .
3. Cliquez sur le lien **Diff Exists** (sous la colonne **Saved vs Running Diff** du tableau) pour l'instance pour laquelle vous souhaitez corriger les commandes de configuration. La page **Configuration Diff** apparaît, répertoriant les différences entre la configuration enregistrée, la configuration en cours d'exécution et la configuration de correction pour cette instance.



4. Cliquez sur **Créer un travail** pour accéder à la page **Créer un travail**, sur laquelle les commandes correctives ont été préremplies. Pour obtenir des instructions sur la façon de créer un travail de configuration, consultez Comment créer un travail de configuration sur Citrix ADM.

Répliquer la configuration en cours d'exécution et enregistrée d'une instance Citrix ADC vers une autre

February 1, 2024

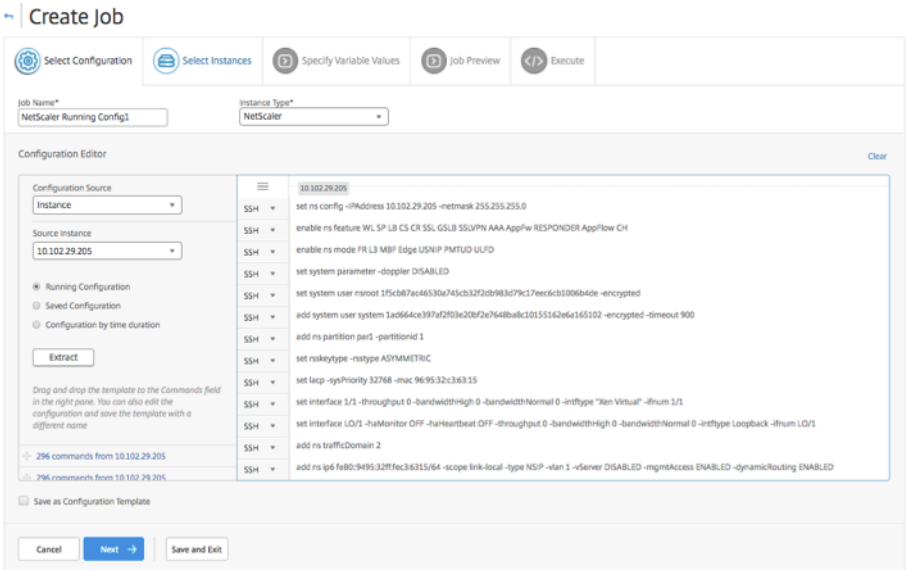
24 mai 2018

Vous pouvez désormais répliquer la configuration d'une instance Citrix ADC sur d'autres instances. Lorsque vous configurez une tâche dans Citrix ADM, sélectionnez une instance comme source de configuration et choisissez la configuration en cours d'exécution ou enregistrée de l'instance sélectionnée.

Par exemple, lorsque vous sélectionnez **Configuration en cours d'exécution** et que vous cliquez sur **Extraire**, Citrix ADM envoie une demande à l'instance de Citrix ADC sélectionnée pour localiser la configuration en cours d'exécution et l'affiche sous forme de modèle. Vous pouvez faire glisser le modèle dans le champ **Commandes** du volet de droite. Vous pouvez modifier les commandes, les paramètres et les instances.

Pour répliquer les commandes de configuration en cours d'exécution et enregistrées d'une instance vers une autre instance sur Citrix ADM :

1. Accédez à **Réseaux** > **Tâches de configuration**, puis cliquez sur **Créer une tâche**.
2. Spécifiez le nom de la tâche et le type d'instance. Par exemple, spécifiez *Citrix ADC RunningConfig1* comme nom de votre tâche et le type d'instance comme *Citrix ADC*.
3. Sélectionnez **Instance** comme **source de configuration**, sélectionnez l'instance source dont vous souhaitez répliquer la configuration sur d'autres instances.
4. Vous voyez les trois options suivantes :
   - Configuration en cours d'exécution
   - Configuration enregistrée
   - Configuration par durée
5. Choisissez **Exécution de la configuration**, puis cliquez sur **Extraire**. Le nombre de commandes de configuration exécutées sur cette instance s'affiche.



6. Faites glisser les commandes dans le champ **Commandes** dans le volet droit.
7. Vous pouvez modifier les commandes dans le champ Commandes. Par exemple, si les commandes extraites doivent configurer une instance Citrix ADC. Cela peut inclure l'ajout de partitions,

la configuration de l'équilibrage de charge, la liaison du serveur d'équilibrage de charge aux services, etc. Vous pouvez modifier vos commandes, pour configurer vos nouvelles instances Citrix ADC sans partitions. Donc, pour supprimer les partitions, supprimez manuellement les commandes liées à la création de partitions et cliquez sur **Suivant**.

8. Cliquez sur **Ajouter des instances** et ajoutez les instances sur lesquelles vous souhaitez appliquer les commandes de configuration en cours d'exécution. Cliquez sur **OK**, puis sur **Suivant**.
9. Si vous avez spécifié des variables dans les commandes, sous l'onglet **Spécifier les valeurs de variable**, cliquez sur **Télécharger le fichier de clé d'entrée** . Dans le fichier téléchargé, spécifiez les valeurs des variables, puis chargez le fichier sur Citrix ADM.
10. Sous l'onglet **Aperçu des tâches**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances.

11. Dans l'onglet **Exécuter**, vous pouvez choisir d'exécuter votre travail maintenant ou de le planifier pour qu'il soit exécuté ultérieurement. Vous pouvez également choisir l'action que Citrix ADM doit prendre la commande échoue et si vous souhaitez envoyer une notification par e-mail concernant le succès ou l'échec de la tâche ainsi que d'autres détails.

Réutiliser les travaux de configuration d'exécution

February 1, 2024

Les tâches de configuration vous permettent de créer un ensemble de commandes de configuration que vous pouvez exécuter sur une ou plusieurs instances gérées. Vous pouvez également exécuter le même ensemble de tâches de configuration enregistrées après avoir modifié les commandes, les paramètres, la source de configuration et les instances de la tâche. Ceci est utile lorsque les mêmes ensembles de commandes doivent être exécutés sur une instance différente, ou lorsque la tâche rencontre une erreur et arrête l'exécution ultérieure.

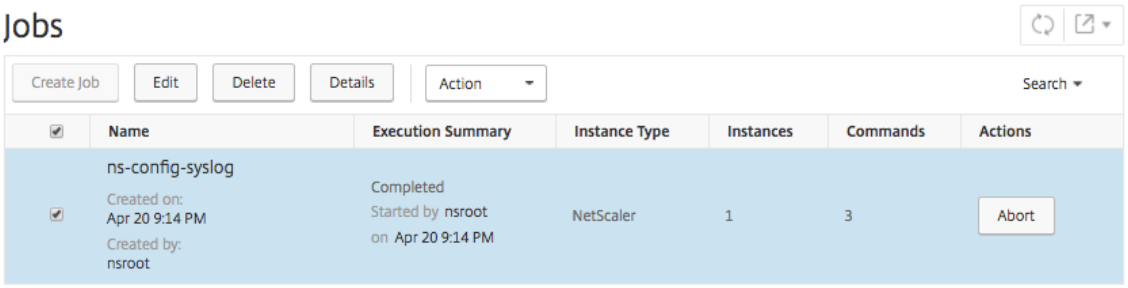
Citrix Application Delivery Management (ADM) fournit une fonction permettant d'exécuter à nouveau les travaux terminés. Avec cette fonction, les travaux exécutés complètement peuvent être exécutés à nouveau sans modifier le nom de la tâche.

> **Remarque** Vous pouvez réexécuter uniquement les tâches qui sont exécutées lorsque le mode d'exécution est « Maintenant ».

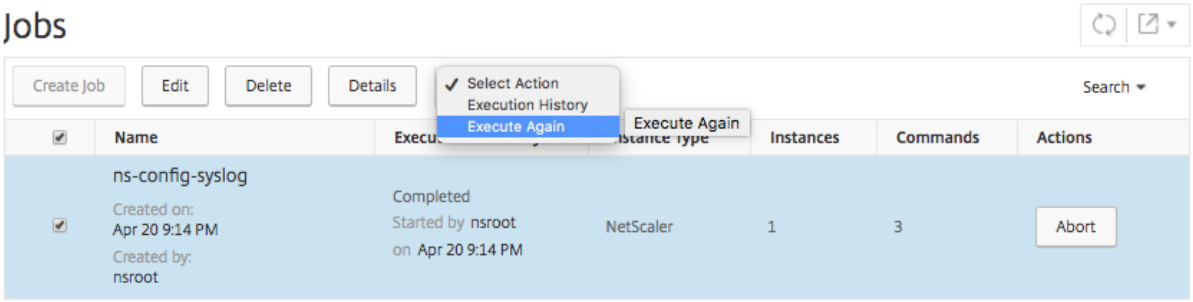
Pour modifier les tâches terminées :

1. À partir de la page d'accueil Citrix ADM, accédez à **Réseaux > Travaux de configuration**.

2. Dans la page **Tâches**, sélectionnez un travail qui affiche le résumé de l'exécution comme terminé, puis cliquez sur **Modifier** . Vous pouvez également modifier une tâche de configuration planifiée.
3. Sur la page **Configurer la tâche**, vous pouvez voir que le nom de la tâche et le type d'instance ne sont pas modifiables. Vous pouvez modifier d'autres champs tels que la source de configuration, ajouter des instances, modifier les valeurs des variables et définir les paramètres d'exécution.
4. Cliquez sur **Terminer** pour exécuter à nouveau la tâche de configuration.



> **Remarque**
>
> Vous pouvez également sélectionner la tâche et cliquer à nouveau sur **Exécuter** pour exécuter la tâche sans modifier la source, l'instance et les commandes. Ceci est utile lorsque vous devez exécuter le même ensemble de commandes sur les mêmes instances. Parfois, le travail peut rencontrer une erreur transitoire du côté serveur, et vous devrez peut-être exécuter à nouveau la tâche.



Planifier les tâches créées à l'aide de modèles intégrés

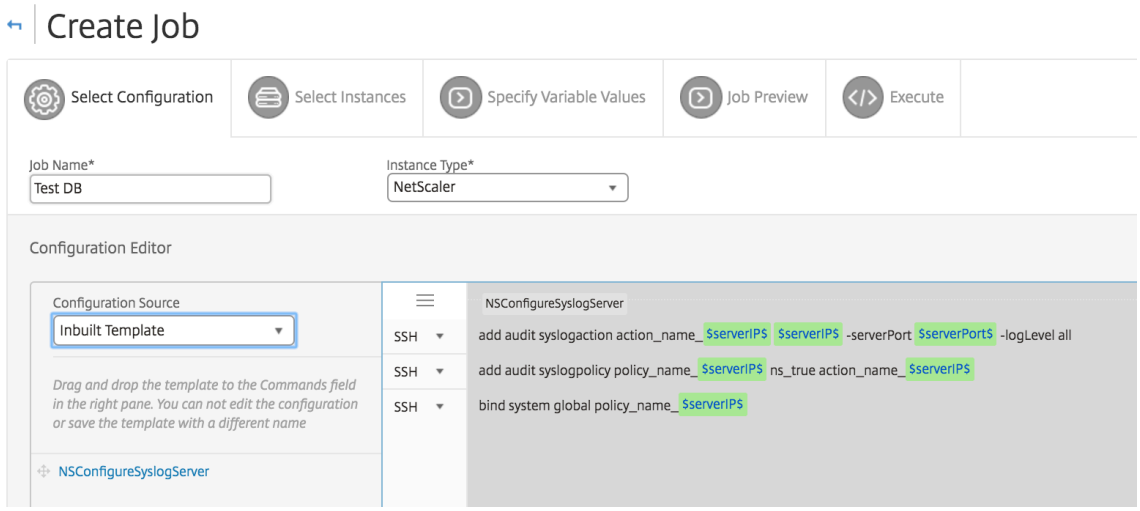
February 1, 2024

Vous pouvez planifier une tâche à l'aide de l'option de modèle intégrée. Une tâche est un ensemble de commandes de configuration que vous pouvez exécuter sur une ou plusieurs instances gérées. Par

exemple, utilisez l'option de modèle intégrée pour planifier une tâche de configuration des serveurs syslog. Vous pouvez également choisir d'exécuter le travail immédiatement ou de planifier l'exécution ultérieure.

Pour planifier un travail à l'aide de modèles intégrés dans Citrix Application Delivery Management (ADM)

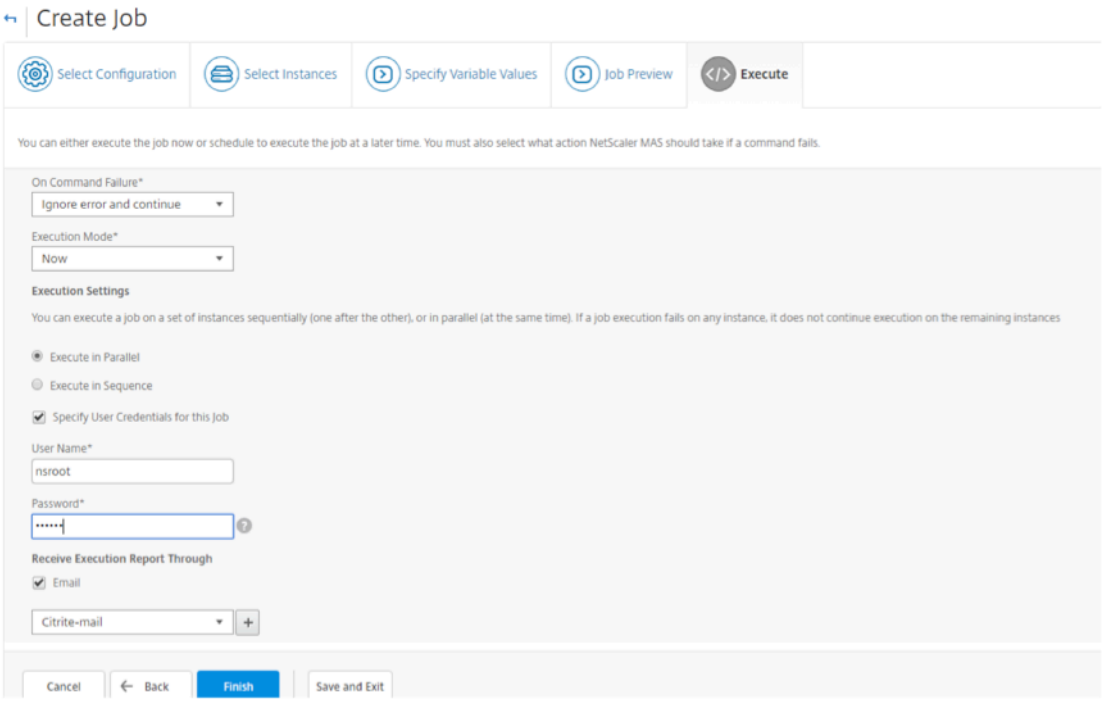
1. Dans Citrix ADM, accédez à **Réseaux** > Tâches **de configuration, puis**cliquez sur **Créer une**tâche.
2. Dans la page **Créer un travail**, sous l'onglet **Sélectionner une configuration**, spécifiez le **nom du travail** et sélectionnez le **type d'instance** dans la liste déroulante.
3. Sélectionnez **Modèle intégré** dans la liste déroulante **Source de configuration**. Faites glisser la commande ***NSConfiguresySlogServer** vers le volet droit, puis cliquez sur **Suivant**.



4. Sous l'onglet **Sélectionner des instances**, cliquez sur **Ajouter** des instances, sélectionnez les instances sur lesquelles vous souhaitez exécuter le travail, puis cliquez sur **OK** .
5. Cliquez sur **Suivant**. Dans l'onglet **Spécifier les valeurs des variables**, sélectionnez l'une des options suivantes pour spécifier des variables pour vos instances :
   - **Valeurs de variables à partir d'un fichier** d'entrée : téléchargez un fichier d'entrée pour entrer des valeurs pour les variables que vous avez définies dans vos commandes. Chargez ensuite le fichier sur le serveur Citrix ADM.
   - **Valeurs de variables communes pour toutes les instances** —Spécifiez l'adresse IP et le port du serveur Syslog.
6. Sous l'onglet **Aperçu des tâches**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances.

7. Cliquez sur **Suivant**.
8. Sous l'onglet **Exécuter**, définissez les conditions suivantes :
   - **En cas d'échec de commande** - Si une commande échoue, vous pouvez choisir d'ignorer les erreurs et de continuer à exécuter la tâche ou d'arrêter l'exécution ultérieure de la tâche. Choisissez l'action à exécuter dans la liste déroulante.
   - **Mode d'exécution** - Vous pouvez exécuter le travail maintenant ou planifier son exécution ultérieure. Si vous souhaitez planifier le travail ultérieurement, vous devez spécifier les paramètres de fréquence d'exécution pour ce travail. Choisissez la planification à suivre dans la liste déroulante.
9. Vous pouvez également exécuter un travail sur un ensemble d'instances séquentiellement ou en parallèle en sélectionnant la méthode requise sous **Paramètres d'exécution**. Si l'exécution d'une tâche échoue sur une instance, elle ne se poursuit pas sur les instances restantes.

   Vous pouvez choisir d'autoriser les utilisateurs autorisés à exécuter des tâches sur vos instances gérées. Une notification par e-mail peut également être envoyée concernant le succès ou l'échec du travail, ainsi que d'autres détails.
10. Cliquez sur **Terminer**.



Utiliser les tâches de maintenance pour mettre à niveau les instances Citrix ADC SDX

February 1, 2024

Vous pouvez effectuer une mise à niveau groupée de vos instances Citrix ADC SDX exécutant Citrix ADC version 11.0 et ultérieure. Pour effectuer une mise à niveau groupée unique, vous utilisez une tâche intégrée dans Citrix ADM.Avec cette tâche intégrée, vous pouvez mettre à niveau Citrix ADC SDX Management Service, Citrix Hypervisor, ainsi que les packs et correctifs supplémentaires pour Citrix Hypervisor.

Pour mettre à niveau des instances Citrix ADC SDX à l'aide de Citrix ADM :

1. Accédez à **Réseaux > Tâches de configuration > Tâches de maintenance**.
2. Cliquez sur **Créer une tâche**. Dans la page **Créer un travail**, sélectionnez la tâche intégrée **Mettre à niveau Citrix ADC SDX** pour mettre à niveau vos instances Citrix ADC SDX. Cliquez sur **Continuer**.
3. Sur la page **Mettre à niveau les appliances Citrix ADC**, dans l'onglet **Sélection d'instance**, spécifiez le **nom de la tâche**et cliquez sur **Ajouter des instances.**
4. Sélectionnez les instances ou groupes d'instances cibles que vous souhaitez mettre à niveau.
5. Après avoir ajouté les instances Citrix ADC ou les groupes d'instances, cliquez sur**Suivant** pour démarrer la validation préalable à la mise à niveau sur les instances sélectionnées. L'écran indique la progression de la pré-validation de chacune des instances Citrix ADC.
6. Sur la page**Modifier la mise à niveau Citrix ADC Appliance (s)**, sélectionnez l'onglet**Mise à niveau**. Dans le menu déroulant**Image logicielle**, sélectionnez**Local**(votre machine locale) ou**Appliance**(le fichier de construction doit être présent sur Citrix ADM).
7. Vous pouvez également voir si des instances présentent des erreurs de mise à niveau de pré-validation. Ces erreurs sont affichées sous forme de message. Les messages indiquent les erreurs liées à l'espace disque, au disque dur et à la personnalisation de l'utilisateur. Si vous ne souhaitez pas continuer avec les instances qui ont échoué la vérification de mise à niveau de pré-validation, vous pouvez supprimer les instances. Pour supprimer les instances, sélectionnez-les et cliquez sur**Supprimer.**
8. Sous l'onglet**Planifier la tâche**, vous pouvez également définir les détails d'exécution dans lesquels vous pouvez effectuer le processus de mise à niveau maintenant ou le planifier pour une date ultérieure. Vous pouvez également choisir de sauvegarder votre instance Citrix ADC SDX, de recevoir un rapport d'exécution par e-mail ou d'effectuer une mise à niveau en deux étapes pour les nœuds dans HA.

La mise à niveau en deux étapes pour les nœuds dans HA vous donne la possibilité d'effectuer la mise à niveau immédiatement ou de planifier une heure pour les nœuds à mettre à jour les uns après les autres.La synchronisation et la propagation des nœuds sont désactivées jusqu'à ce que les deux nœuds soient correctement mis à niveau.

Création de tâches de configuration pour les instances Citrix SD-WAN WANOP

February 1, 2024

Une tâche est un ensemble de commandes de configuration que vous pouvez créer et planifier sur une ou plusieurs instances gérées. Pour les instances Citrix SD-WAN WANOP, vous pouvez utiliser les options suivantes pour créer des tâches :

- **Modèle de configuration** : vous pouvez utiliser l'éditeur de configuration pour saisir des commandes CLI, enregistrer la configuration en tant que modèle et l'utiliser pour configurer des tâches.
- **Modèle intégré** : Vous pouvez choisir parmi une liste de modèles de configuration. Ces modèles fournissent les syntaxes des commandes CLI et vous permettent de spécifier des valeurs pour les variables. Les modèles intégrés sont répertoriés, avec leur description dans le tableau ci-dessous.
- **Fichier** : Vous pouvez télécharger un fichier de configuration à partir de votre machine locale et créer des tâches.

Une fois qu'un travail est créé, vous pouvez choisir d'exécuter le travail immédiatement ou de planifier l'exécution ultérieure. Vous pouvez également définir la fréquence d'exécution

Modèle intégré	Description
EnableCloudBridgeWANOpt	Active le trafic via l'appliance Citrix SD-WAN WANOP.
DisableCloudBridgeWANOpt	Désactive le trafic via l'appliance Citrix SD-WAN WANOP.
RestartCloudBridgeWANOpt	Redémarre l'appliance WANOP Citrix SD-WAN.
RestoreConfig	Restaure la configuration de l'appliance Citrix SD-WAN WANOP.

Modèle intégré	Description
AddLink	La création ou la définition de liens permettent à l'appliance SD-WAN WANOP d'éviter la congestion et les pertes sur les liaisons et de modeler le trafic. Vous pouvez définir la bande passante maximale envoyée ou reçue sur la liaison et également spécifier qu'il s'agit du trafic côté LAN ou WAN.
ConfigureBandwidth	Définit les limites de bande passante et les autres paramètres de gestion de bande passante
AddUser	Ajoute un nouvel utilisateur auquel vous pouvez attribuer des privilèges.
AddUserAdvancedPlatform	Ajout d'un nouvel utilisateur vous permet d'attribuer des privilèges non disponibles dans le `AddUser` modèle.
AddService-class	Crée une classe de service pour l'appliance WANOP Citrix SD-WAN avec un ou plusieurs filtres de classes de service et l'active.
SetApplication	Définit la définition du classificateur d'applications.
AddorRemoveVideoCachingPorts	Ajoute ou supprime le numéro de port sur lequel la source vidéo peut envoyer ou recevoir des données. Le port par défaut est 80.
RemoveVideoCachingSource	Supprime une ou plusieurs sources de mise en cache vidéo. Spécifiez l'adresse IP de la source vidéo ou le nom de domaine.
RemoveAllVideoCaching	Supprime toutes les sources de mise en cache vidéo disponibles.
VideoCachingState	Active ou désactive la fonctionnalité de mise en cache vidéo sur les appliances Citrix SD-WAN WANOP.
ClearVideoCaching	Efface le cache vidéo ou les statistiques de mise en cache vidéo.
SetVideoCaching	Définit la taille maximale des objets mis en cache. Un objet supérieur à cette limite n'est pas mis en cache. Par défaut, la taille maximale de l'objet de mise en cache est de 100 Mo.

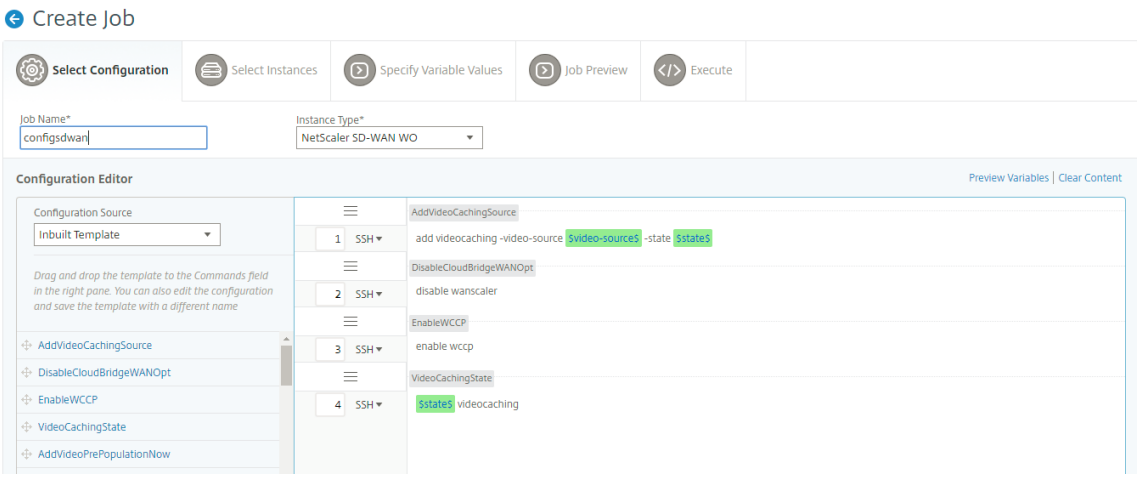
Modèle intégré	Description
AddVideoCachingSource	Ajoute l'adresse IP ou le nom de domaine de la source vidéo. Inclut des options permettant d'activer ou de désactiver la mise en cache vidéo pour cette source.
ConfigureRemoteLicenseServer	Configure le serveur de licences centralisé. Spécifiez le modèle de serveur de licences, l'adresse IP et le numéro de port.
ConfigureLocalLicenseServer	Définit l'emplacement du serveur de licences comme étant local.
InstallCACert	Installe les certificats d'autorité de certification sur l'appliance WANOP Citrix SD-WAN. Spécifiez le nom du certificat, le nom du fichier et le mot de passe du keystore.
InstallCombinedCerKey	Installe un fichier de paire de clés de certificat SSL combiné.
InstallSeperateCertKey	Installe le certificat SSL et la clé sous forme de fichiers distincts.
EnableWCCP	Active le mode de déploiement WCCP.
AddWCCPServiceGroup	Ajoute une nouvelle définition de groupe de services WCCP pour l'appliance Citrix SD-WAN WANOP.
DisableWCCP	Désactive le mode de déploiement WCCP.
AddTrafficShapingPolicy	Crée une stratégie de régulation du trafic pour l'appliance Citrix SD-WAN. La stratégie contrôle la bande passante réseau.
SetTrafficShapingPolicy	Modifie la stratégie de mise en forme du trafic pour l'appliance WANOP Citrix SD-WAN. La stratégie contrôle la bande passante réseau.
AddVideoPrePopulation	Crée une entrée de pré-remplissage vidéo, qui vous permet de télécharger et de mettre en cache une vidéo à l'avance. Vous pouvez également spécifier à quel moment mettre en cache une vidéo.
UpdateVideoPrePopulation	Modifie une entrée de préremplissage vidéo, qui indique à quel moment mettre en cache une vidéo.

Modèle intégré	Description
AddVideoPrePopulationNow	Configure la prépopulation vidéo, ce qui vous permet de télécharger et de mettre en cache une vidéo immédiatement. Vous pouvez contrôler la façon dont vous souhaitez télécharger et mettre en cache des vidéos à partir de l'URL ou des URL.
VideoPrePopulationState	Modifie, démarre, met à jour ou supprime le pré-remplissage vidéo.
ConfigureSyslogServer	Définit l'adresse IP et le numéro de port du serveur Syslog.
ConfigureAlert	Configure le niveau d'alerte.

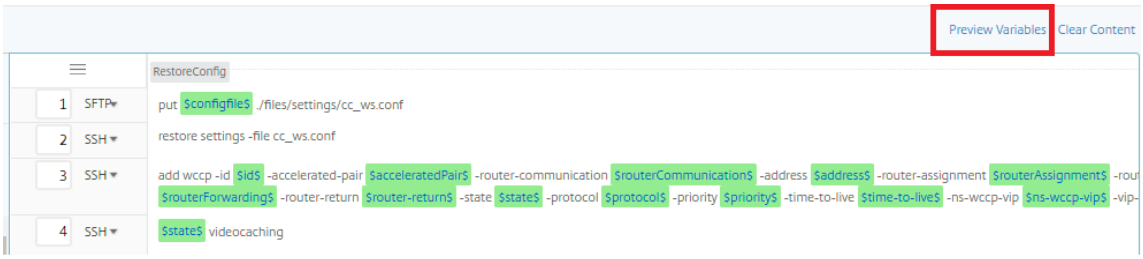
Pour créer une tâche de configuration pour les instances WANOP Citrix SD-WAN :

1. Dans Citrix ADM, accédez à **Réseaux**> **Tâches de configuration**, puis cliquez sur **Créer une tâche**.
2. Dans la page **Créer un travail**, sous l'onglet **Sélectionner une configuration**, spécifiez le **nom du travail** .
3. Dans le champ **Type d'instance**, sélectionnez **Citrix SD-WAN WO** .
4. Dans la liste déroulante **Source de configuration**, sélectionnez une option pour créer un travail.

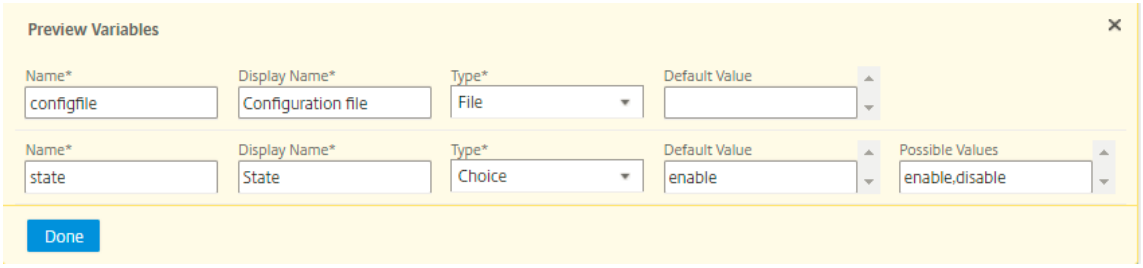
> **Remarque**
>
> Sélectionnez **Enregistrer en tant que modèle de configuration** et spécifiez un nom pour enregistrer la configuration en tant que modèle et la réutiliser.



5. Vous pouvez consulter toutes les variables que vous avez définies lors de la création ou de la modification d'un travail de configuration dans une vue consolidée unique.
6. Pour afficher toutes les variables dans une seule vue consolidée, procédez de l'une des manières suivantes :
   - Lors de la création d'une tâche de configuration, accédez à **Réseaux > Tâches de configuration**, puis sélectionnez **Créer une tâche**. Sur la page **Créer un travail**, vous pouvez consulter toutes les variables que vous avez ajoutées lors de la création du travail de configuration.
   - Lorsque vous modifiez une tâche de configuration, accédez à **Réseau > Tâches de configuration**, sélectionnez le nom de la tâche et cliquez sur **Modifier**. Sur la page **Configurer la tâche**, vous pouvez consulter toutes les variables qui ont été ajoutées lors de la création de la tâche de configuration.
7. Vous pouvez ensuite cliquer sur l'onglet **Aperçu des variables** pour prévisualiser les variables dans une vue consolidée unique que vous avez définie lors de la création ou de la modification d'un travail de configuration.

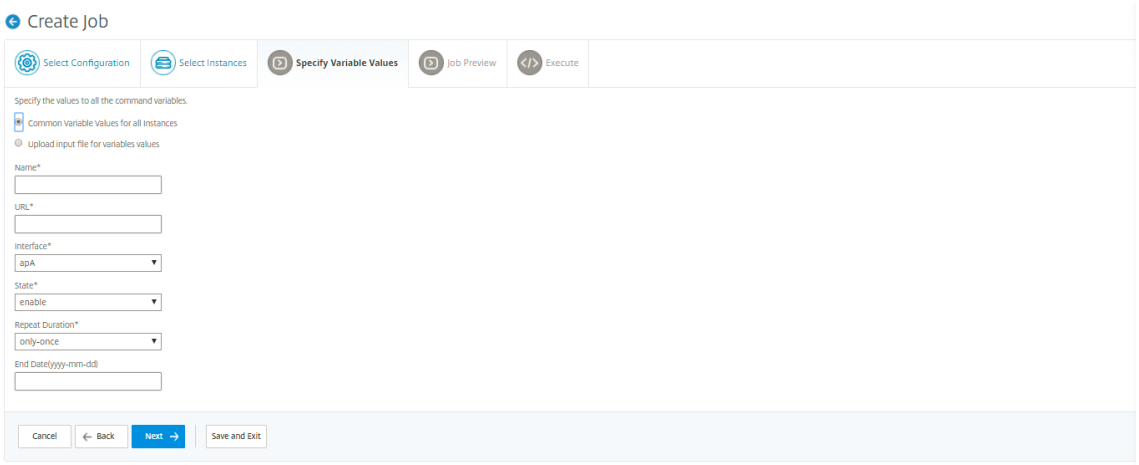


8. Une nouvelle fenêtre contextuelle apparaît et affiche tous les paramètres des variables telles que Nom, Nom d'affichage, Type et valeur par défaut dans un format tabulaire. Vous pouvez également modifier et modifier ces paramètres. Cliquez sur le bouton **Terminé** après avoir modifié l'un des paramètres.



9. Cliquez **sur**Suivant , puis sur l'onglet **Sélectionner des instances** , cliquez sur **Ajouter des instances.** Sélectionnez les instances sur lesquelles vous souhaitez exécuter la tâche, puis cliquez sur **OK** .
10. Cliquez sur**Suivant**, puis sur l'onglet**Spécifier les valeurs de variable**, sélectionnez l'une des options suivantes pour spécifier des variables pour vos instances :

- **Télécharger le fichier d'entrée pour les valeurs des variables :** cliquez sur**Télécharger le fichier clé d'entrée**pour télécharger un fichier d'entrée. Dans le fichier d'entrée, entrez des valeurs pour les variables que vous avez définies dans vos commandes, puis téléchargez le fichier sur le serveur Citrix ADM.
- **Valeurs de variables communes pour toutes les instances** : entrez des valeurs pour les variables. Les variables varient en fonction du modèle sélectionné.



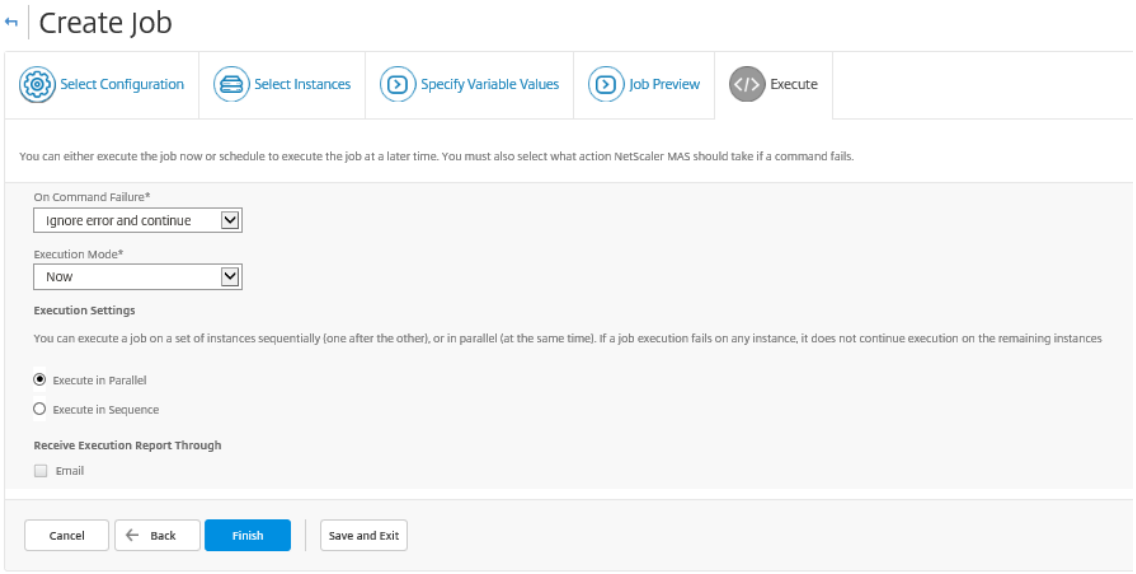
Les fichiers d'entrée contenant les valeurs des variables sont conservés (avec le même nom de fichier) dans les tâches de configuration. Vous pouvez afficher et modifier ces fichiers d'entrée que vous avez utilisés et chargés précédemment lors de la création ou de la modification des tâches de configuration.

Pour afficher les travaux de configuration exécutés lors de la création d'un travail de configuration, accédez à **Réseau > Travaux de configuration**, puis cliquez sur **Créer un travail**. Dans la page**Créer une tâche**. Sous l'onglet**Spécifier les valeurs variables**, sélectionnez l'option**Valeurs variables communes pour toutes les instances** pour afficher les fichiers téléchargés. Pour modifier les fichiers d'entrée, téléchargez le fichier d'entrée, puis modifiez et chargez les fichiers (en conservant le même nom de fichier).

Pour afficher les travaux de configuration déjà exécutés lors de la modification d'un travail de configuration, accédez à **Réseau > Travaux de configuration**, sélectionnez le nom du travail et cliquez sur **Modifier**. Dans la page**Configurer le travail**, sous l'onglet**Spécifier les valeurs**de**variable, sélectionnez l'option Valeurs variables communes pour toutes les instances** pour afficher les fichiers téléchargés. Pour modifier les fichiers d'entrée, téléchargez le fichier d'entrée, puis modifiez et téléchargez les fichiers (en conservant le même nom de fichier)

11. Cliquez sur **Suivant**, sous l'onglet **Aperçu du travail**, vous pouvez évaluer et vérifier les commandes à exécuter en tant que tâche.
12. Cliquez sur **Suivant**, sous l'onglet **Exécuter**, définissez les conditions suivantes :

- **En cas d'échec d'une commande** : Que faire en cas d'échec d'une commande : ignorez les erreurs et poursuivez le travail, ou arrêtez toute exécution ultérieure du travail. Choisissez une action dans la liste déroulante.
- **Mode d'exécution** : exécutez le travail immédiatement ou planifiez l'exécution pour une durée ultérieure. Si vous planifiez l'exécution pour une période ultérieure, vous devez spécifier les paramètres de fréquence d'exécution pour la tâche. Choisissez la planification à suivre dans la liste déroulante **Fréquence d'exécution**.



13. Sous **Paramètres d'exécution**, sélectionnez cette option pour exécuter le travail de manière séquentielle (l'un après l'autre) ou en parallèle (en même temps).
14. Pour qu'un rapport d'exécution de travail soit envoyé par e-mail à une liste de destinataires, activez la case à cocher **E-mail** dans la section **Recevoir le rapport d'exécution par le biais**. Dans la liste déroulante qui s'affiche, choisissez une liste de distribution de courrier électronique. Pour créer une liste de distribution d'e-mails, cliquez sur l'icône **+** et entrez les adresses e-mail des destinataires, ainsi que les détails du serveur de messagerie.
15. Cliquez sur **Terminer**.

Utiliser le modèle de configuration maître

February 1, 2024

L'utilisation d'un modèle de configuration principal est une option flexible pour créer et déployer une configuration maître sur plusieurs instances Citrix ADC.

En tant qu'administrateur, vous pouvez modifier la configuration et enregistrer les licences, certificats et autres fichiers sur l'instance ADC. Vous pouvez enregistrer la nouvelle configuration en tant que modèle de configuration maître (fichier .conf).

Pour enregistrer votre modèle de configuration maître à partir d'une instance ADC, vous pouvez effectuer l'une des opérations suivantes :

- À l'invite de commandes, entrez **save ns config**. La configuration est enregistrée dans la mémoire FLASH de l'instance dans le fichier /nsconfig/ns.conf.
- À partir de l'interface graphique de l'instance, accédez à **Diagnostics** > **Afficher la configuration**. Choisissez le type de configuration que vous souhaitez enregistrer. Par exemple, si vous souhaitez enregistrer la configuration enregistrée de votre instance, sélectionnez **Configuration enregistrée**.Cliquez sur le lien **Enregistrer le texte dans un fichier** pour enregistrer le fichier 'ns.conf'sur votre machine locale.

Lorsque vous déployez le modèle de configuration maître à l'aide du modèle de configuration 'DeployMasterConfiguration'lors de la création d'une tâche, vous pouvez le personnaliser davantage pour chaque instance ADC spécifique en ajoutant plus de commandes, en modifiant des commandes existantes et en fournissant différentes valeurs de variables dans le fichier d'entrée.

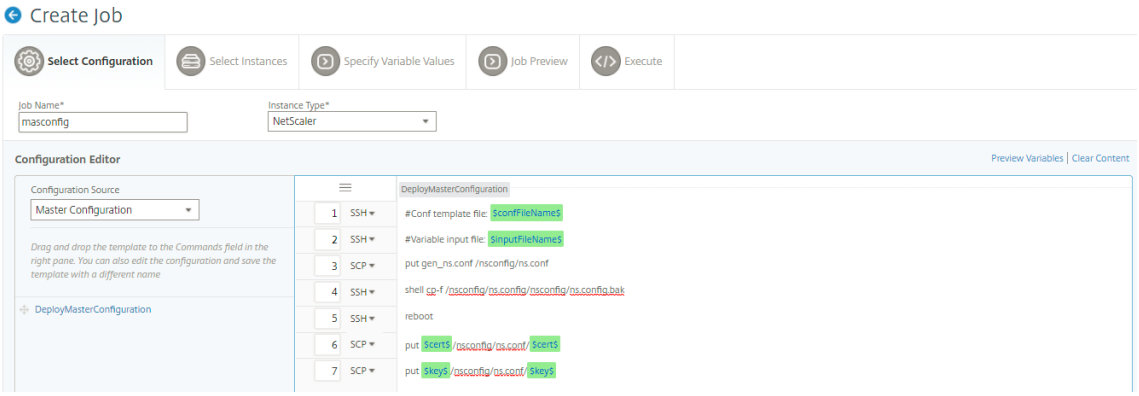
Par exemple, en tant qu'administrateur, vous pouvez télécharger des clés de certificat sur vos instances ADC en plus du fichier ns.conf et déployer la configuration principale sur eux également.

> **Important**
>
> Vous ne pouvez pas exécuter un travail de configuration à l'aide du modèle DeployMasterConfiguration sur les instances Citrix ADC CPX, les instances configurées dans un cluster ou sur des instances ADC partitionnées.

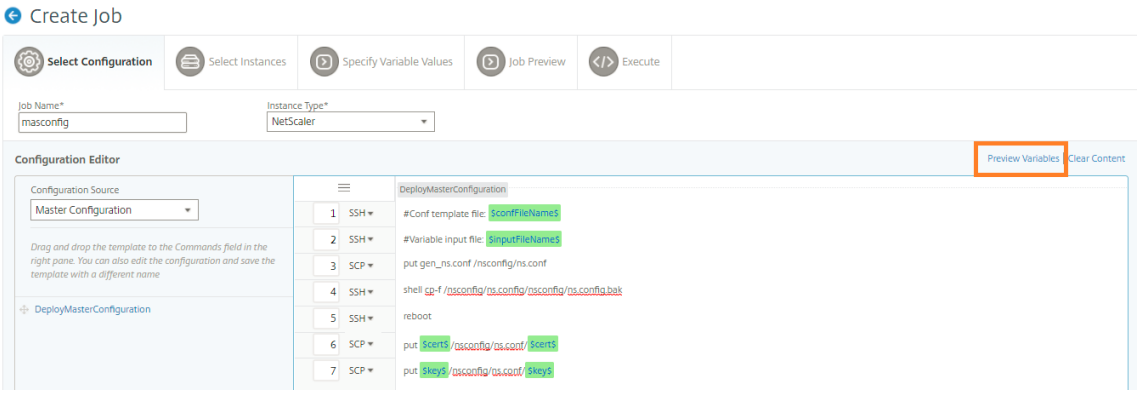
Pour créer une tâche de configuration à l'aide du modèle de configuration Master Config sur Citrix ADM :

1. Dans Citrix ADM, accédez à **Réseaux** > **Tâches de configuration**, puis cliquez sur **Créer une tâche**.
2. Dans la page **Créer un travail**, sous l'onglet **Sélectionner une configuration**, spécifiez le **nom du travail** et sélectionnez le **type d'instance** dans la liste déroulante.
3. Sélectionnez **Configuration principale** dans la liste déroulante **Source de configuration**. Faites glisser les commandes du modèle DeployMasterConfiguration vers le volet droit. Vous pouvez également ajouter, modifier ou supprimer des commandes dans le volet droit. Cliquez sur **Suivant**.

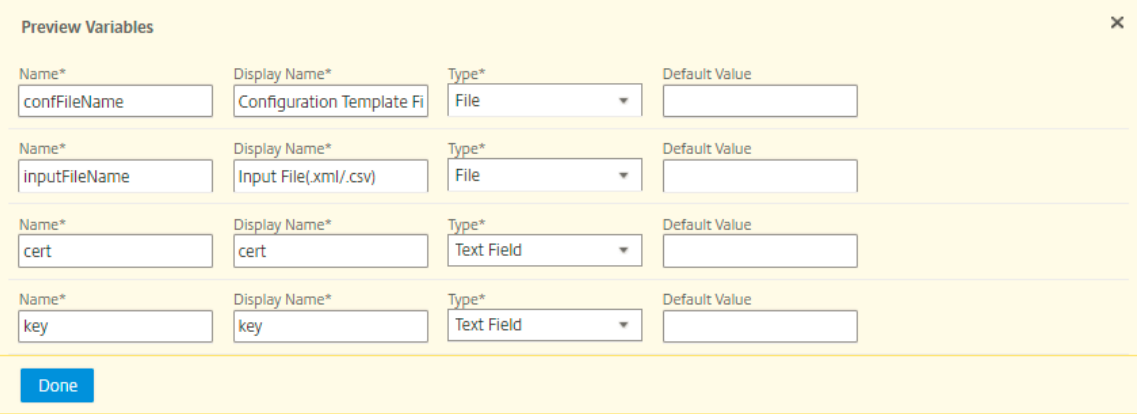
> **Remarque**
>
> Vous pouvez ajouter des commandes ***put*** pour ajouter des fichiers d'entrée à votre modèle. Dans notre exemple, nous devons télécharger des fichiers de certificat et de clé en plus du fichier de modèle de configuration et des fichiers d'entrée de variables.



4. Vous pouvez consulter toutes les variables que vous avez définies lors de la création ou de la modification d'un travail de configuration dans une vue consolidée unique.
5. Pour afficher toutes les variables dans une seule vue consolidée, procédez de l'une des manières suivantes :
   - Lors de la création d'une tâche de configuration, accédez à **Réseaux > Tâches de configuration**, puis sélectionnez **Créer une tâche**. Sur la page **Créer un travail**, vous pouvez consulter toutes les variables que vous avez ajoutées lors de la création du travail de configuration.
   - Lorsque vous modifiez une tâche de configuration, accédez à **Réseau > Tâches de configuration**, sélectionnez le nom de la tâche et cliquez sur **Modifier**. Sur la page **Configurer la tâche**, vous pouvez consulter toutes les variables qui ont été ajoutées lors de la création de la tâche de configuration.
6. Vous pouvez ensuite cliquer sur l'onglet **Aperçu des variables** pour prévisualiser les variables dans une vue consolidée unique que vous avez définie lors de la création ou de la modification d'un travail de configuration.



7. Une nouvelle fenêtre contextuelle apparaît et affiche tous les paramètres des variables telles que Nom, Nom d'affichage, Type et valeur par défaut dans un format tabulaire. Vous pouvez également modifier et modifier ces paramètres. Cliquez sur le bouton **Terminé** après avoir modifié l'un des paramètres.



8. Sélectionnez les instances sur lesquelles vous souhaitez exécuter le travail de configuration, puis cliquez sur **Suivant**.
9. Dans l'onglet **Spécifier les valeurs des variables**, chargez les éléments suivants :

   - **Fichier de modèle de configuration (.conf)** : téléchargez le fichier .conf que vous avez extrait d'une instance ADC.
   - **Télécharger le fichier d'entrée (.xml/csv)** - Téléchargez le fichier d'entrée avec les valeurs des variables que vous avez définies dans vos commandes.

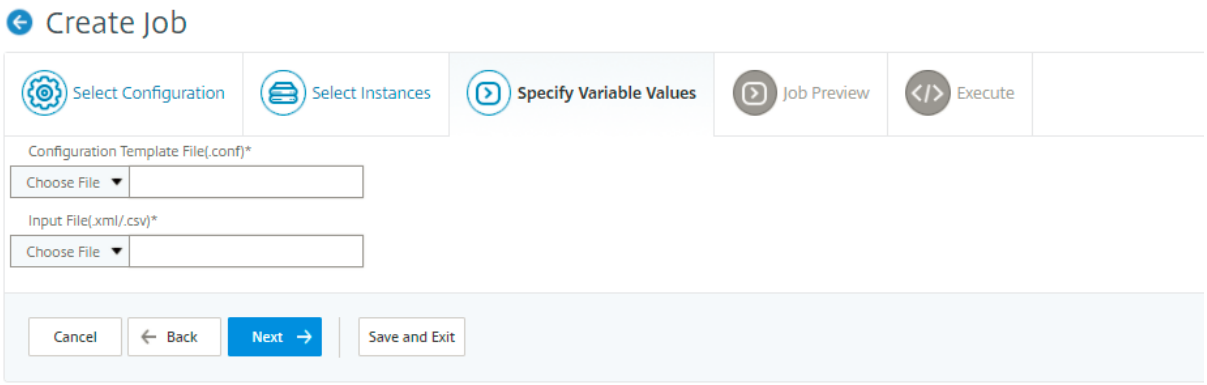
   Un exemple de fichier XML est fourni ici pour votre utilisation. Assurez-vous que les fichiers xml contiennent les détails correspondant aux instances ADC que vous utilisez.

```
<?xml version="1.0" encoding="UTF-8" ?>

<properties>

<!--

```



```
Provide inputs for all the parameters defined in the master config file.

- global. This tag contains all the common parameters and value.

- devicegroup. This tag contains all the instance group specific parameters and values.

If the same parameters are defined in global and instance tags, the instance specific parameters value will take precedence over the instance group. The instance group specific parameters value will take precedence over global parameters in the execution.

- name. This attribute represents the name of the instance group.

- device. This tag contains all the instance specific parameters and value.

If the same parameters are defined in global and instance tags, the instance specific parameters value will take precedence in the execution.

- name. This attribute represents the IP Address of the instance. Host name is not supported for the attibute.

HA pair should be represented as <primaryip>-<secondaryip>. Example 10.102.2.1-10.102.2.2

In the template file, the parameter name must be specified within the dollar sign,Example: $NSIP$, $CC_Trap_Dest$ and parameters names are case sensitive.
-->

<global>

</global>
<devicegroup name="BLR_DEVS">
</devicegroup>
<device name="10.106.101.209">
<param name="IP" value="10.106.101.209"/>
</device>

<!-- HA PAIR-->
<!--<device name="10.102.43.154-10.102.43.155">
<param name="NSIP" value="10.102.43.154"/>
<param name="HostName" value="NS43HA"/>
<param name="LBSERVER" value="haserver43http"/>
<param name="SNMPTrapDest" value="10.102.43.130"/>
</device>-->
</properties>

<!--NeedCopy-->
```


10. Cliquez sur **Suivant**.

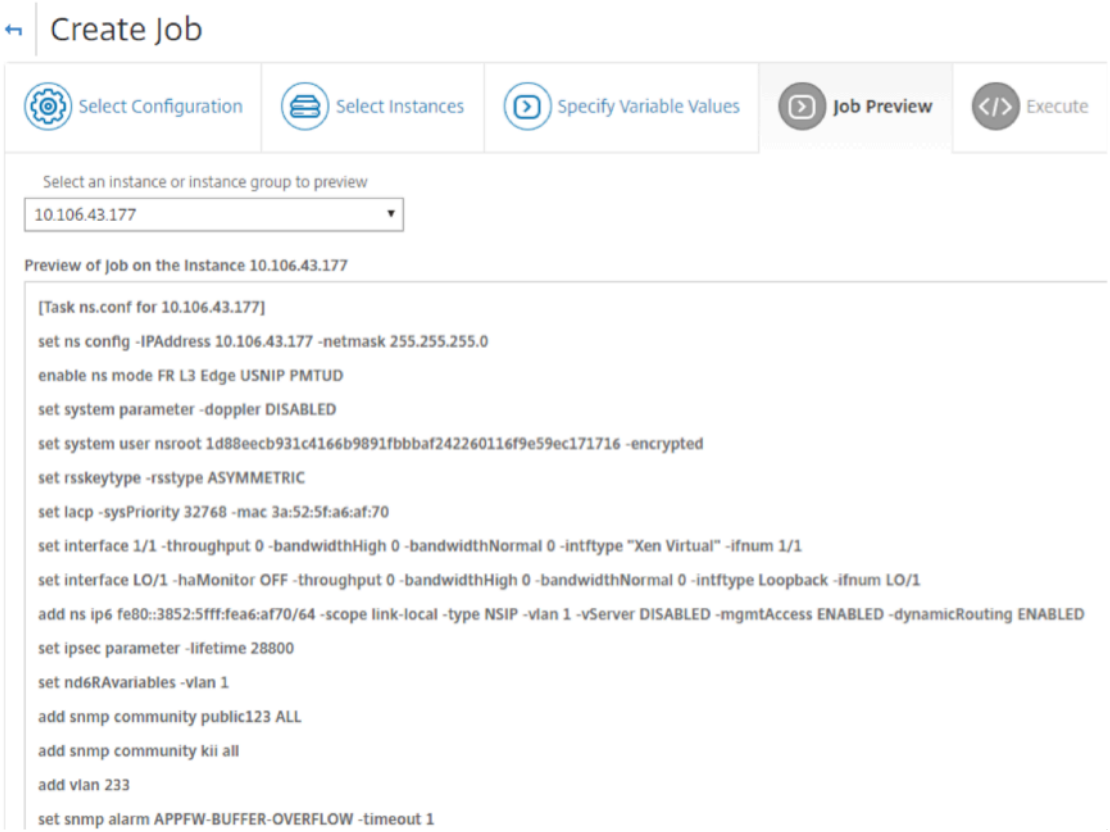


Les fichiers d'entrée contenant les valeurs des variables sont conservés (avec le même nom de fichier) dans les tâches de configuration. Vous pouvez afficher et modifier ces fichiers d'entrée que vous avez utilisés et chargés précédemment lors de la création ou de la modification des tâches de configuration.

Pour afficher les travaux de configuration d'exécution lors de la création d'un travail de configuration, accédez à **Réseau > Travaux de configuration**, puis cliquez sur **Créer un travail**. Dans la page **Créer une tâche**. Dans l'onglet **Spécifier les valeurs des variables**, sélectionnez l'option **Valeurs de variables communes pour toutes les instances** pour afficher les fichiers téléchargés. Pour modifier les fichiers d'entrée, téléchargez le fichier d'entrée, puis modifiez et chargez les fichiers (en conservant le même nom de fichier).

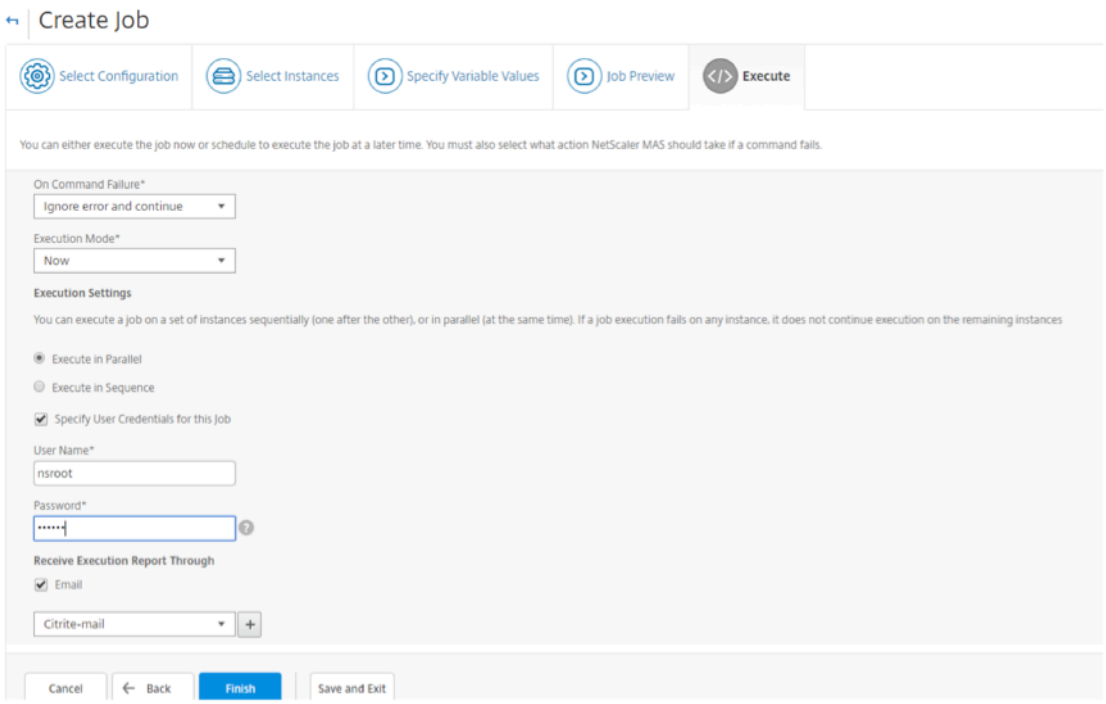
Pour afficher les travaux de configuration déjà exécutés lors de la modification d'un travail de configuration, accédez à **Réseau > Travaux de configuration**, sélectionnez le nom du travail et cliquez sur **Modifier**. Dans la page **Configurer la tâche**, sous l'onglet **Spécifier les valeurs de variable**, sélectionnez l'option **Valeurs variables communes pour toutes les instances** pour afficher les fichiers chargés. Pour modifier les fichiers d'entrée, téléchargez le fichier d'entrée, puis modifiez et chargez les fichiers (en conservant le même nom de fichier).

1. Sous l'onglet **Aperçu des tâches**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances, puis cliquez sur **Suivant** .



2. Dans l'onglet **Exécuter**, vous pouvez choisir d'exécuter votre tâche maintenant ou de la planifier pour qu'elle soit exécutée ultérieurement. Vous pouvez également choisir l'action que Citrix ADM doit prendre en cas d'échec de la commande.

   Vous pouvez également choisir d'autoriser les utilisateurs autorisés à exécuter des travaux sur vos instances gérées, et vous pouvez choisir d'envoyer une notification par e-mail concernant le succès ou l'échec de la tâche, ainsi que d'autres détails.



Après avoir exécuté votre travail, vous pouvez voir les détails de la tâche en accédant à**Réseaux** > Tâches**de configuration**et en sélectionnant le travail que vous avez configuré. Cliquez sur**Détails**, puis sur**Récapitulatif de l'exécution** pour afficher les détails de votre tâche. Cliquez sur l'instance pour afficher les **journaux des commandes** pour voir les commandes exécutées sur la tâche.

Command Log

Status	Command	Message
✓	put /var/mps/tenants/root/config_mgmt/MySSLCert.crt /nsconfig/ssl/MySSLCert.crt	Done
✓	put /var/mps/tenants/root/config_mgmt/MySSLCertKey.key /nsconfig/ssl/MySSLCertKey.key	Done
✓	shell cp -f /nsconfig/ns.conf /nsconfig/ns.conf.bak	Done
✓	#Conf template file: NS12_0_41_Template.conf	Done
✓	#Variable input file: NS12_0_41_AnswerKey.xml	Done
✓	put /var/mps/tenants/root/config_mgmt/ns_##7A818EB30E94FAA36144CC5F0782E06A13C3122F6BC67B32190444FC6F06.conf /nsconfig/ns.conf	Done
✓	shell	Done
✓	reboot	Done

Utiliser les tâches pour mettre à niveau les instances de Citrix ADC

February 1, 2024

Vous pouvez utiliser Citrix Application Delivery Management (ADM) pour mettre à niveau une ou plusieurs instances Citrix ADC. Vous devez connaître le cadre de licences et les types de licences avant de mettre à niveau une instance.

Lorsque vous mettez à niveau votre instance Citrix ADC en créant un travail de maintenance, effectuez la vérification de pré-validation sur les instances que vous souhaitez mettre à niveau.

1. **Rechercher des personnalisations** - Sauvegardez vos personnalisations et supprimez-les des instances. Vous pouvez réappliquer les personnalisations sauvegardées après la mise à niveau de l'instance.
2. **Vérifiez l'utilisation du disque** : si le dossier `/var` possède moins de 6 Go d'espace et que le dossier `/flash` contient moins de 200 Mo d'espace, nettoyez l'espace disque. Vérifiez les chemins de dossier suivants pour nettoyer l'espace disque :

   - `/var/nstrace`
   - `/var/log`
   - `/var/nslog`
   - `/var/tmp/support`
   - `/var/core`
   - `/var/crash`
   - `/var/nsinstall`
   - `/var/netscaler/nsbackup`

3. **Rechercher des problèmes matériels de disque** - Résolvez les problèmes matériels, le cas échéant.

Vous pouvez mettre à niveau une paire ADC HA en deux étapes :

1. Créez un travail de mise à niveau et exécutez immédiatement sur l'un des nœuds ou planifiez plus tard.
2. Planifiez ultérieurement l'exécution du travail de mise à niveau sur le nœud restant. Assurez-vous de planifier ce travail après la mise à niveau du nœud initial.

Lorsque vous mettez à niveau une paire ADC HA, tenez compte des points suivants :

- Le nœud secondaire est mis à niveau en premier.
- La synchronisation et la propagation des nœuds sont désactivées jusqu'à ce que les deux nœuds soient correctement mis à niveau.
- Une fois la mise à niveau réussie de la paire HA, un message d'erreur apparaît dans l'historique des exécutions. Ce message s'affiche si vos nœuds de la paire HA se trouvent sur des versions ou des versions différentes. Ce message indique que la synchronisation entre le nœud principal et le nœud secondaire est désactivée.

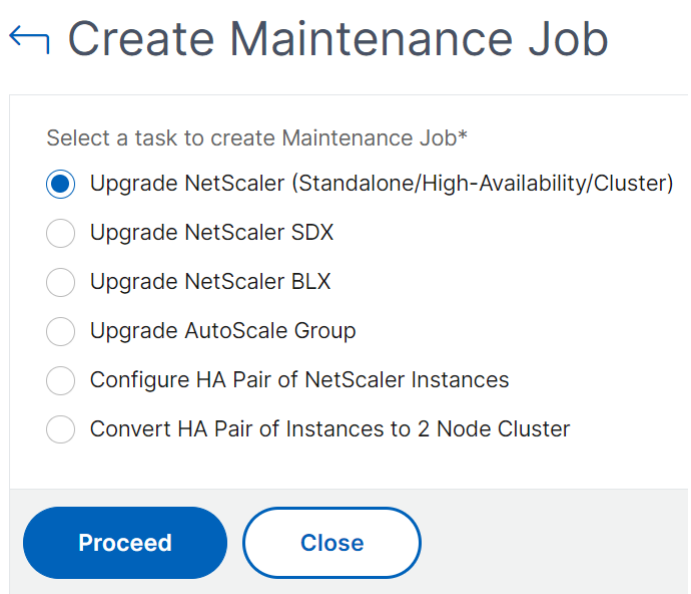
Lorsque vous mettez à niveau un cluster ADC, l'ADM effectue une validation préalable à la mise à niveau sur l'instance spécifiée uniquement. Avant de procéder à la mise à niveau, vérifiez et résolvez les problèmes de personnalisation, d'utilisation du disque et de matériel sur les nœuds du cluster.

Créer un travail de maintenance de mise à niveau pour mettre à niveau des instances ADC

> **Remarque**
>
> La mise à niveau ADC d'une version supérieure à une version inférieure n'est pas prise en charge Par exemple, si votre instance Citrix ADC est 13.0 82.x, vous ne pouvez pas rétrograder l'instance ADC vers 13.0 79.x ou toute autre version antérieure.

1. Dans Citrix ADM, accédez à **Réseaux** > Tâches de **configuration > Tâches** de **maintenance**. Cliquez sur le bouton **Créer un travail**.

2. Dans **Create Maintenance Jobs**, sélectionnez **Mettre à niveau Citrix ADC (Standalone/High-Availability/Cluster)** et cliquez sur **Proceed**.



3. Dans **Sélectionner une instance**, tapez le nom de votre choix pour **Nom de la tâche**.
4. Cliquez sur **Ajouter des instances** pour ajouter des instances ADC à mettre à niveau.

- Pour mettre à niveau une paire HA, spécifiez l'adresse IP d'un nœud principal ou secondaire.
- Pour mettre à niveau un cluster, spécifiez l'adresse IP du cluster.

5. Cliquez sur **Suivant** pour lancer la validation préalable à la mise à niveau sur les instances sélectionnées.

   L'onglet **Validation préalable à la mise à niveau** affiche les instances ayant échoué. Vous pouvez supprimer les instances ayant échoué et cliquer sur **Suivant**.

   Si l'espace disque est insuffisant sur une instance, vous pouvez vérifier et nettoyer l'espace disque. Reportez-vous à la section Nettoyer l'espace disque ADC.

   > **Important**
   >
   > Si vous spécifiez l'adresse IP du cluster, l'ADM effectue la validation préalable à la mise à niveau uniquement sur l'instance spécifiée et non sur les autres nœuds du cluster.

6. Facultatif, dans **Scripts personnalisés**, spécifiez les scripts à exécuter avant et après une mise à niveau d'instance. Utilisez l'une des méthodes suivantes pour exécuter les commandes :

   Les scripts personnalisés sont utilisés pour vérifier les modifications avant et après une mise à niveau d'instance ADC. Par exemple :

   - Version d'instance avant et après la mise à niveau.
   - État des interfaces, des nœuds haute disponibilité, des serveurs virtuels et des services avant et après la mise à niveau.
   - Les statistiques des serveurs et services virtuels.
   - Les routes dynamiques.

   Une mise à niveau d'instance comporte plusieurs étapes. Vous pouvez désormais spécifier ces scripts à exécuter dans les étapes suivantes :

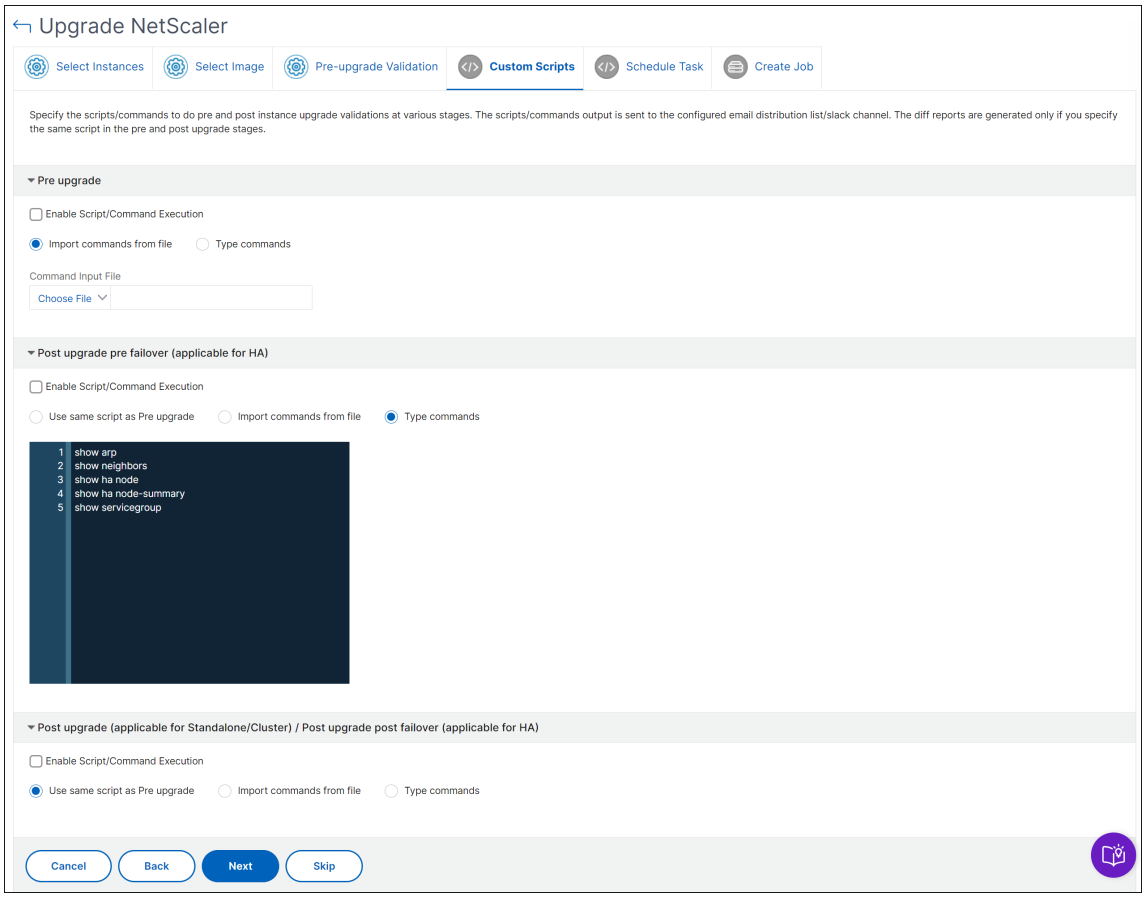
   - **Avant mise à niveau** : le script spécifié s'exécute avant la mise à niveau d'une instance.
   - **Après mise à niveau avant basculement (applicable pour HA)** : Cette étape s'applique uniquement au déploiement haute disponibilité. Le script spécifié s'exécute après la mise à niveau des nœuds, mais avant leur basculement.
   - **Après mise à niveau (applicable pour autonome)/Après mise à niveau après basculement (applicable pour HA)** : Le script spécifié s'exécute après la mise à niveau d'une instance dans le déploiement autonome. Dans le déploiement haute disponibilité, le script s'exécute après la mise à niveau des nœuds et leur basculement sur incident.

> **Remarque**
>
> Assurez-vous d'activer l'exécution du script aux étapes requises. Sinon, les scripts spécifiés ne s'exécutent pas.

Vous pouvez importer un fichier script ou taper des commandes directement dans l'interface graphique ADM.

- **Importer les commandes à partir du fichier** : sélectionnez le fichier d'entrée de commande à partir de votre ordinateur local.
- **Commandes de type** : entrez les commandes directement sur l'interface graphique.

Dans les étapes de post-mise à niveau, vous pouvez utiliser le même script spécifié dans l'étape de pré-mise à niveau.



7. Dans **Planifier la tâche**, sélectionnez l'une des options suivantes :
   - **Mise à niveau maintenant** - Le travail de mise à niveau s'exécute immédiatement.
   - **Planifier plus tard** - Sélectionnez cette option pour exécuter ce travail de mise à niveau ultérieurement. Spécifiez la **date d'exécution** et l'**heure de début** lorsque vous souhaitez mettre à niveau les instances.

Si vous souhaitez mettre à niveau une paire ADC HA en deux étapes, sélectionnez **Effectuer une mise à niveau en deux étapes pour les nœuds en haute disponibilité**.

Spécifiez la **date d'exécution** et l'**heure de début** lorsque vous souhaitez mettre à niveau une autre instance de la paire HA.

8. Dans **Créer une tâche**, spécifiez les détails suivants :

   a) Sélectionnez l'une des options suivantes dans la liste des **images logicielles** :

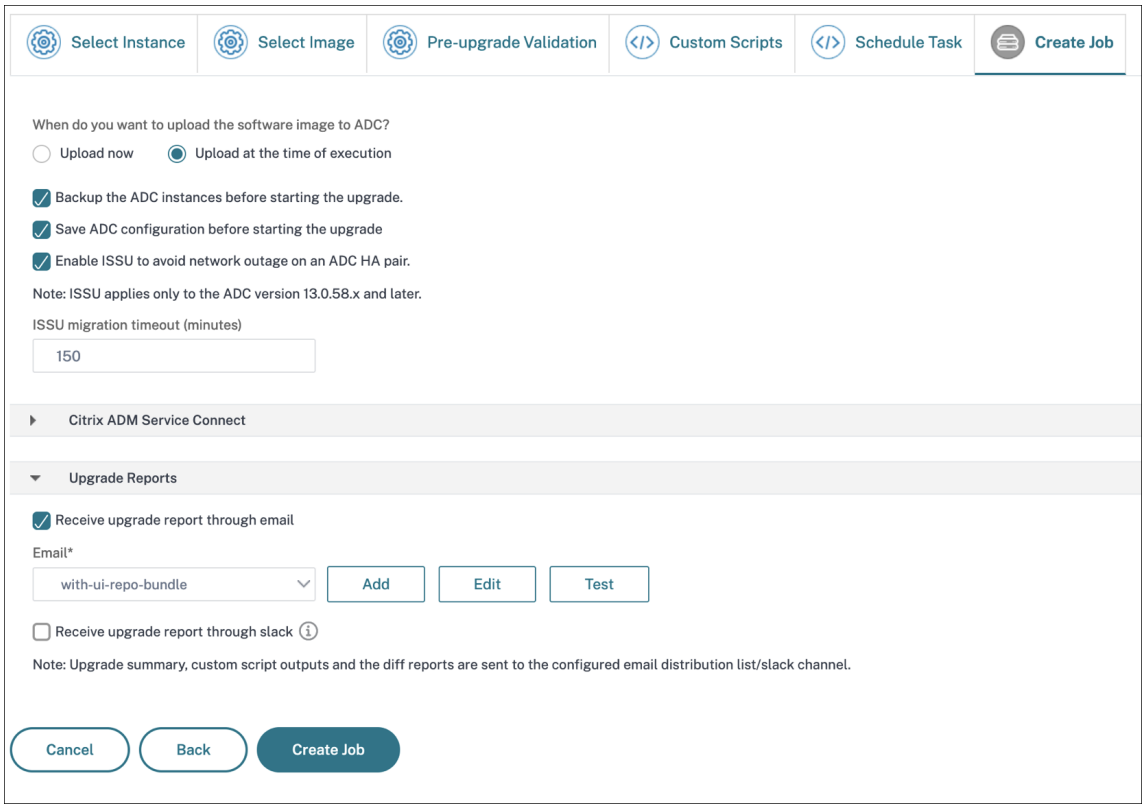
      - **Local** : sélectionnez le fichier de mise à niveau de l'instance sur votre machine locale.
      - **Appliance** : sélectionnez le fichier de mise à niveau de l'instance dans un navigateur de fichiers ADM. L'interface graphique ADM affiche les fichiers d'instance présents sur `/var/mps/ns_images`.

   b) Spécifiez le moment où vous souhaitez télécharger l'image sur une instance :

      - **Télécharger maintenant** - Sélectionnez cette option pour télécharger l'image immédiatement. Toutefois, le travail de mise à niveau s'exécute à l'heure planifiée.
      - **Télécharger au moment de l'exécution** - Sélectionnez cette option pour télécharger l'image au moment de l'exécution de la tâche de mise à niveau.

   - **Nettoyer l'image logicielle à partir de Citrix ADC lors de la mise à niveau réussie** - Sélectionnez cette option pour effacer l'image téléchargée dans l'instance ADC après la mise à niveau de l'instance.
   - **Sauvegardez les instances ADC avant de commencer la mise à niveau.** - Crée une sauvegarde des instances ADC sélectionnées.
   - **Maintenir le statut principal et secondaire des nœuds HA après la mise à niveau** : sélectionnez cette option si vous souhaitez que le travail de mise à niveau lance un basculement après la mise à niveau de chaque nœud. De cette façon, le travail de mise à niveau conserve l'état principal et secondaire des nœuds.
   - **Enregistrer la configuration ADC avant de commencer la mise à niveau** - Enregistre la configuration ADC en cours d'exécution avant la mise à niveau des instances ADC.
   - **Permet à ISSU d'éviter une panne réseau sur une paire ADC HA** - ISSU garantit la mise à niveau zéro temps d'arrêt sur une paire ADC haute disponibilité. Cette option fournit une fonctionnalité de migration qui respecte les connexions existantes lors de la mise à niveau. Ainsi, vous pouvez mettre à niveau une paire ADC HA sans temps d'arrêt. Spécifiez le délai de migration ISSU en minutes.
   - **Recevoir le rapport d'exécution par e-mail** - Envoie le rapport d'exécution par e-mail. Pour ajouter une liste de distribution d'e-mails, voir Créer une liste de distribution d'e-mails.

- **Recevoir le rapport d'exécution via la marge** - Envoie le rapport d'exécution en marge. Pour ajouter un profil Slack, consultez Créer un profil Slack.



9. Cliquez sur **Créer une tâche**.

Le travail de mise à niveau apparaît dans **Réseaux > Travail de configuration > Tâche de maintenance**. Lorsque vous modifiez une tâche existante, vous pouvez basculer vers n'importe quel onglet si les champs obligatoires sont déjà remplis. Par exemple, si vous êtes dans l'onglet **Sélectionner une configuration**, vous pouvez basculer vers l'onglet **Aperçu des travaux**.

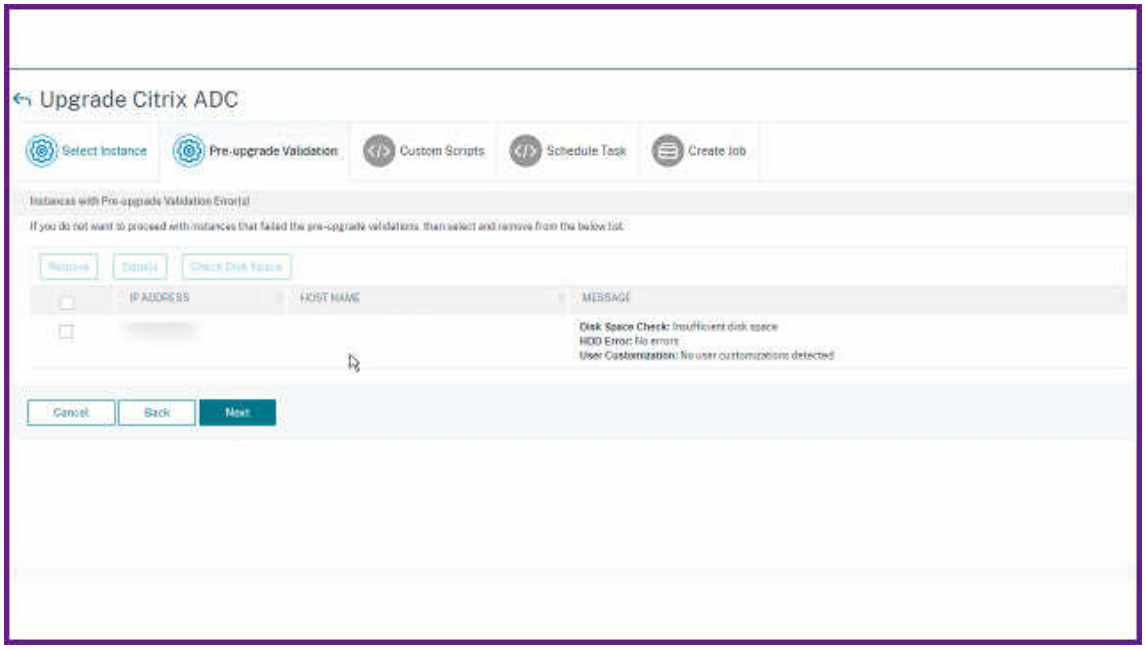
Nettoyer l'espace disque ADC

Si vous rencontrez un problème d'espace disque insuffisant lors de la mise à niveau d'une instance ADC, nettoyez l'espace disque à partir de l'interface graphique d'ADM elle-même.

1. Dans l'onglet **Validation préalable à la mise à niveau**, sélectionnez l'instance qui présente le problème d'espace disque.
2. Sélectionnez **Vérifier l'espace disque**.

   Ce volet affiche le disque de l'instance qui dispose d'un espace insuffisant. Il affiche également la quantité de mémoire utilisée et disponible sur le disque.
3. Dans le volet **Vérifier l'espace disque**, sélectionnez l'instance qui nécessite un nettoyage.

4. Cliquez sur **Nettoyage de disque**.



5. Sélectionnez les fichiers que vous souhaitez effacer.
6. Cliquez sur **Supprimer**

Télécharger un rapport de diff consolidé d'une tâche de mise à niveau ADC

Vous pouvez télécharger un rapport diff d'une tâche de mise à niveau ADC si des scripts personnalisés sont spécifiés. Un rapport diff contient les différences entre les sorties du script pré-mise à niveau et post-mise à niveau. Avec ce rapport, vous pouvez déterminer quelles modifications ont eu lieu sur l'instance ADC après mise à niveau.

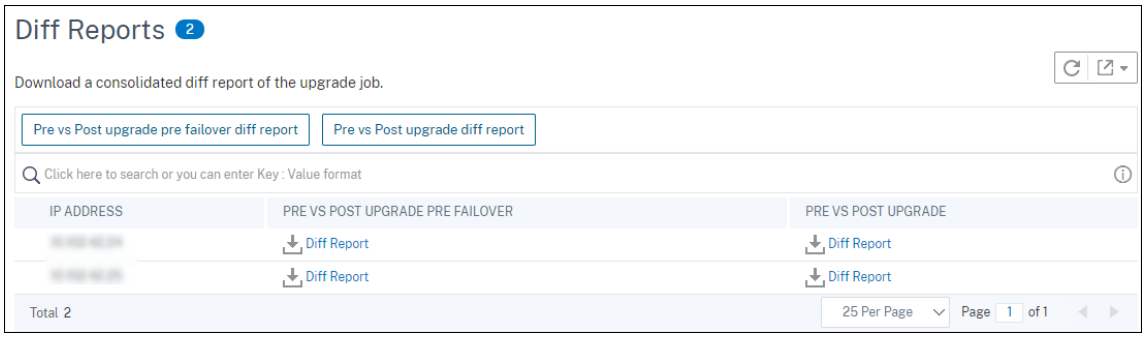
> **Remarque**
>
> Le rapport diff n'est généré que si vous spécifiez le même script dans les étapes de pré-mise à niveau et de post-mise à niveau.

Pour télécharger un rapport diff d'une tâche de mise à niveau, procédez comme suit :

1. Accédez à **Réseaux > Tâches de configuration > Tâches de maintenance**.
2. Sélectionnez le travail de mise à niveau pour lequel vous souhaitez télécharger un rapport de diff.
3. Cliquez sur **Rapports de différé**.
4. Dans **Rapports Diff**, téléchargez un rapport de diff consolidé du travail de mise à niveau sélectionné.

Dans cette page, vous pouvez télécharger l'un des rapports diff suivants :

- **Rapport de différentiel pré-basculement avant la mise à niveau et après mise à niveau**
- **Rapport de diff pré vs post mise à niveau**



Utiliser des modèles de configuration pour créer des modèles d'audit

February 1, 2024

Vous pouvez désormais utiliser des commandes de configuration précédemment enregistrées en tant que modèles de configuration pour créer des modèles d'audit qui peuvent être appliqués à des instances Citrix ADC spécifiques. Lors de la création d'un modèle d'audit, vous pouvez faire glisser des modèles de configuration précédemment enregistrés dans le champ Commandes et modifier le modèle en fonction de vos besoins. Vous pouvez ensuite appliquer le modèle d'audit à des instances Citrix ADC spécifiques. Citrix ADM compare ces instances avec le modèle d'audit et signale toute incompatibilité. Ce processus vous aide à identifier les erreurs et à les corriger en temps opportun.

Vous pouvez créer des modèles de configuration tout en créant un travail et en enregistrant un ensemble de commandes de configuration en tant que modèle. Lorsque vous enregistrez ces modèles sur la page **Créer des tâches**, ils s'affichent automatiquement sur la page **Créer un modèle** .

Par exemple, envisagez une configuration d'équilibrage de charge de base pour laquelle vous ajoutez un serveur virtuel d'équilibrage de charge, ajoutez deux services et liez les services au serveur virtuel.

Cet exemple utilise les commandes suivantes :

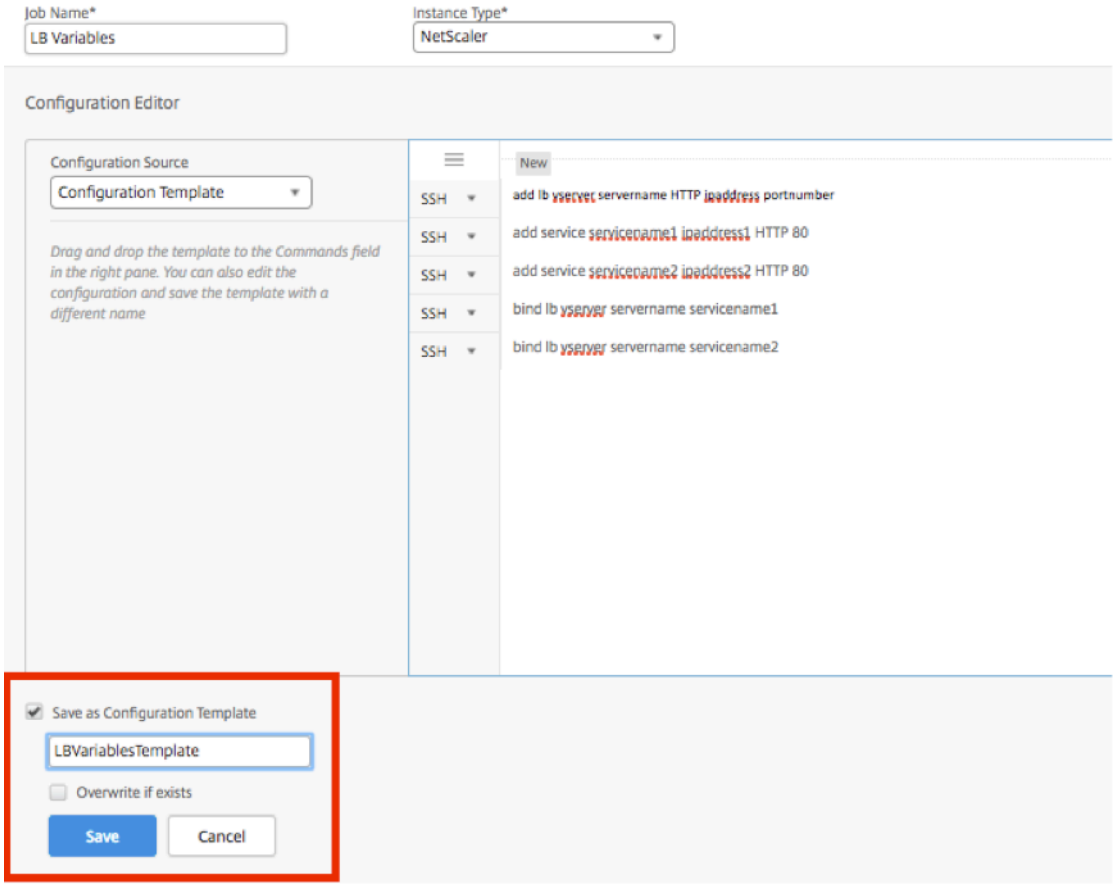
```
add lb vserver >servername> HTTP <ipaddress portnumber>

add service <servicename1 ipaddress1> HTTP 80

add service <servicename2 ipaddress2> HTTP 80

bind lb vserver <servername servicename1>
```



```
bind lb vserver <servername servicename2>
```

Pour enregistrer un modèle de configuration dans Citrix ADM :

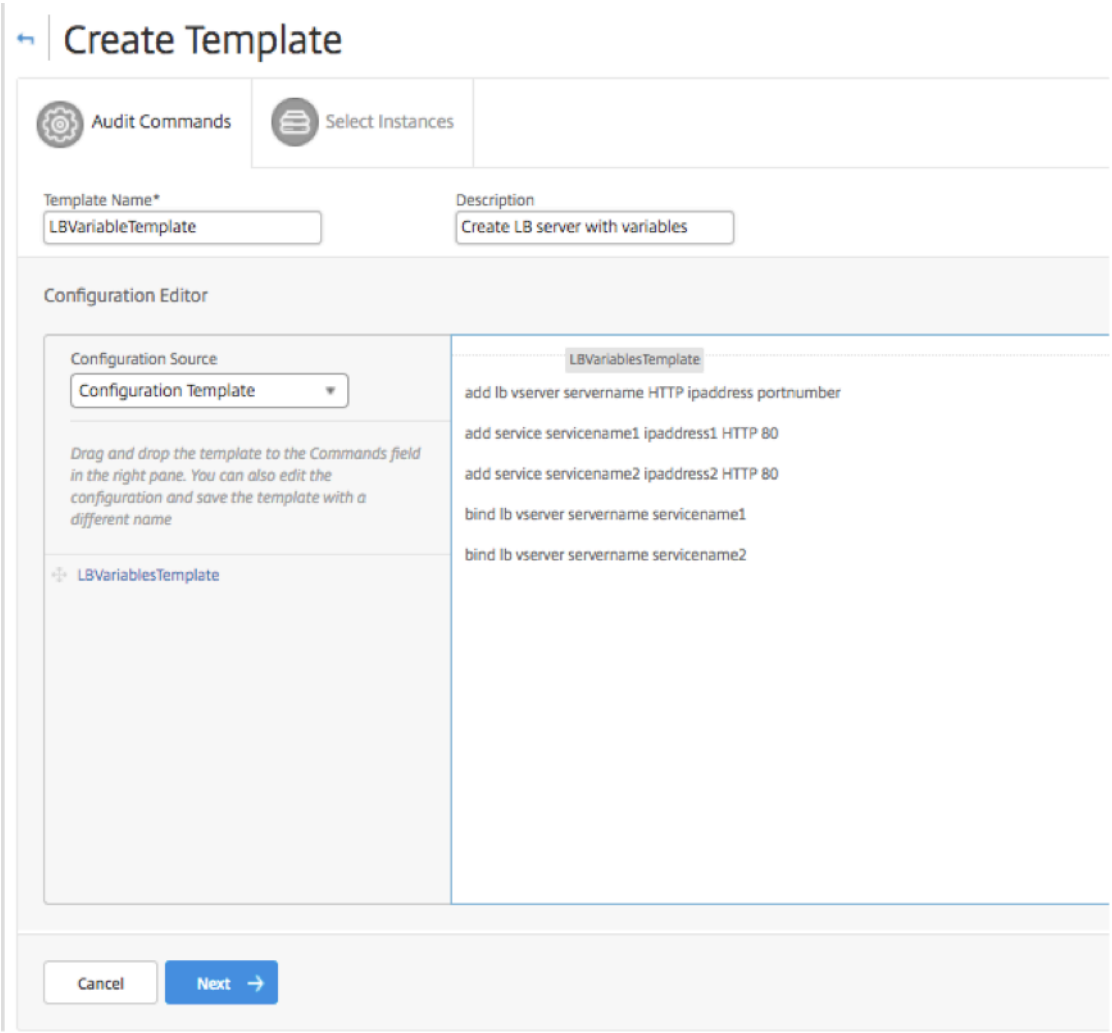
1. Accédez à **Réseaux** > **Tâches de configuration**, puis cliquez sur **Créer une tâche**.
2. Sur la page **Créer un travail**, spécifiez le nom du travail et le type d'instance.
3. Choisissez **Modèle de configuration** comme source de configuration et, dans le champ **Commandes**, saisissez des commandes telles que celles de l'exemple ci-dessus.
4. Activez la case à cocher **Enregistrer en tant que modèle de configuration** et indiquez un nom pour votre modèle. Vous pouvez choisir d'écraser d'autres modèles qui existent avec le même nom.
5. Cliquez sur **Enregistrer**.



Pour utiliser un modèle de configuration pour créer un modèle d'audit dans Citrix ADM :

1. Accédez à **Réseaux** > **Audit de configuration** > **Modèles d'audit**, puis cliquez sur **Ajouter**.
2. Dans la page **Créer un modèle**, spécifiez un nom pour le nom du modèle et entrez une description.

3. Dans la liste **Source de configuration**, sélectionnez **Modèle de configuration**, puis faites glisser le modèle dans le champ Commandes dans le volet droit. Vous pouvez également modifier la configuration et enregistrer le modèle sous un autre nom. Cliquez sur **Suivant**.
4. Dans l'onglet **Sélectionner des instances**, cliquez sur **Ajouter des instances** et ajoutez les instances sur lesquelles vous souhaitez exécuter la configuration. Cliquez sur **OK**.
5. Cliquez sur **Terminer**.



Le modèle d'audit apparaît dans la liste Modèles d'audit et est exécuté toutes les 12 heures par rapport aux configurations des instances spécifiées.

Utiliser la commande SCP (put) dans les tâches de configuration

February 1, 2024

Vous pouvez utiliser la fonctionnalité Tâches de configuration de Citrix ADM pour créer des tâches de configuration, envoyer des notifications par e-mail et consulter les journaux d'exécution des tâches créées. Une tâche est un ensemble de commandes de configuration que vous pouvez créer et exécuter sur une seule instance gérée ou sur plusieurs instances gérées. Par exemple, vous pouvez utiliser des tâches de configuration pour les mises à niveau des appareils.

Les tâches de configuration dans Citrix ADM utilisent les commandes SSH (Secure Shell) pour configurer les instances, et vous pouvez configurer une tâche de configuration pour utiliser Secure Copy (SCP) pour transférer des fichiers en toute sécurité. SCP est basé sur le protocole SSH. L'une des commandes **SCP** que vous pouvez inclure dans une tâche de configuration est la commande « put ». Vous pouvez utiliser la commande « put » dans les tâches de configuration pour télécharger ou transférer un ou plusieurs fichiers stockés dans un répertoire local de votre système vers Citrix ADM, puis vers un répertoire sur l'instance ou les instances Citrix ADC.

> **Remarque** Le fichier est chargé sur Citrix ADM puis copié (placé) dans les instances Citrix ADC sélectionnées. Le fichier téléchargé est stocké dans Citrix ADM et est supprimé uniquement lorsque le travail est supprimé. Ceci est nécessaire pour les travaux planifiés pour s'exécuter plus tard.

La commande a la syntaxe suivante :

```
put <local_filename> <remote_path/remote_filename>
```

Où,

<local_filename> est le nom du fichier local à télécharger.

<remote_path / remote_filename> est le chemin d'accès à un répertoire distant et le nom à attribuer au fichier lorsqu'il est copié dans ce répertoire.

Lors de la création du travail de configuration, vous pouvez convertir les paramètres de nom de fichier local et distant en variables. Cela vous permet d'affecter différents fichiers à ces paramètres pour le même ensemble d'instances Citrix ADC chaque fois que vous exécutez le travail. En outre, lorsque vous utilisez un fichier à plusieurs endroits dans une tâche et si vous souhaitez renommer le fichier, vous pouvez redéfinir la variable au lieu de changer le nom du fichier à tous les endroits.

Pour utiliser la commande put pour télécharger des fichiers dans une tâche de configuration :

1. Accédez à **Réseaux** > **Travaux de configuration**.
2. Sur la page **Travaux**, cliquez sur **Créer un travail** .
3. Dans la page **Créer un travail**, entrez le nom du travail dans le champ Nom du travail et, dans le volet **Éditeur de configuration**, entrez la commande « put ».

   Par exemple, si vous souhaitez créer un travail de configuration qui copie un fichier de certificat SSL enregistré sur votre système local vers plusieurs instances Citrix ADC, vous pouvez ajouter

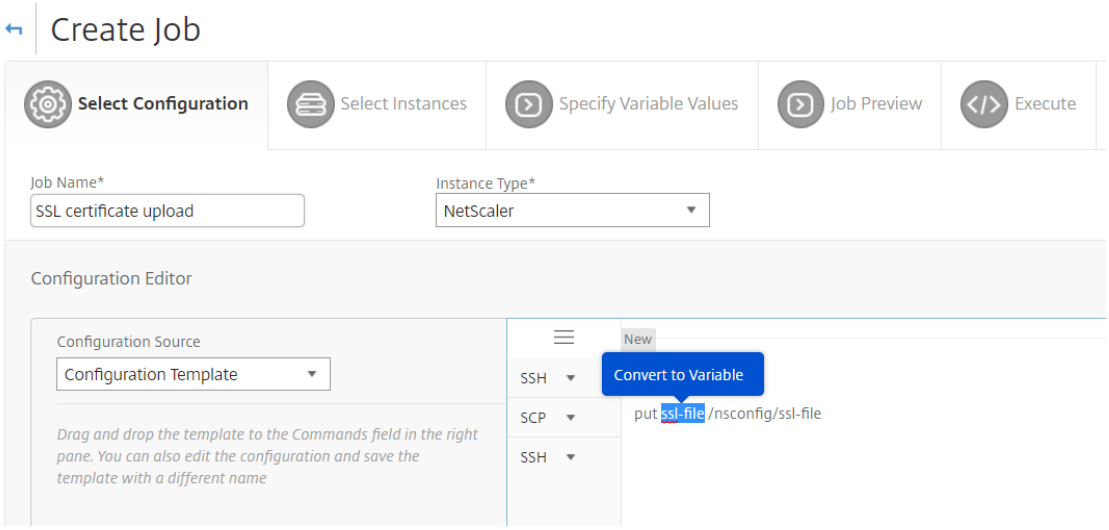
une commande « put » qui utilise une variable au lieu du nom d'un fichier particulier et définir le type de variable comme « fichier ».

```
put ssl-file /nsconfig/ssl-file
```

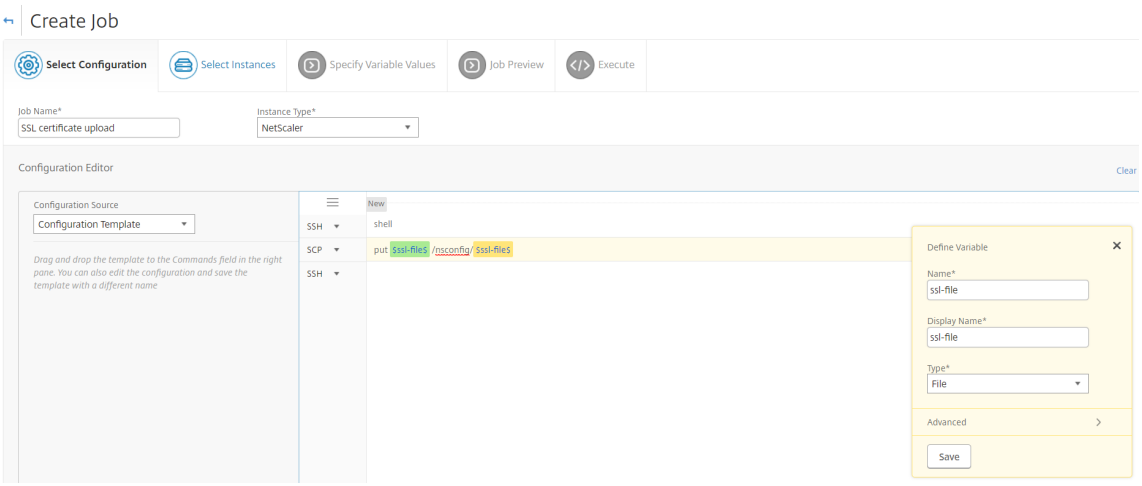
Dans cet exemple,

- `ssl-file` - Il s'agit du nom du fichier qui doit être téléchargé dans l'instance Citrix ADC.
- `/nsconfig/ssl-file` - Il s'agit du dossier de destination de l'instance où le `ssl-file` sera placé après l'exécution de la tâche.

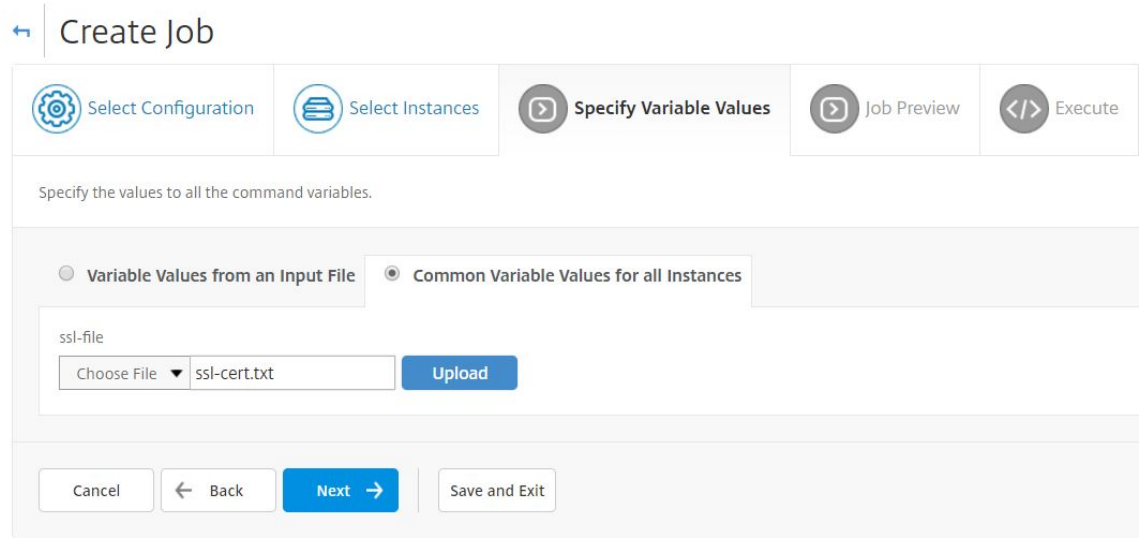
4. Dans la commande que vous avez saisie, sélectionnez le nom de fichier que vous souhaitez convertir en variable, puis cliquez sur**Convertir en variable**, comme illustré dans la figure suivante.



5. Vérifiez que le nom du fichier est entouré de signes dollar (indiquant qu'il s'agit maintenant d'une variable), puis cliquez sur la variable.
6. Spécifiez les détails de la variable, tels que le nom, le nom complet et le type.
7. Dans la liste déroulante **Type**, sélectionnez **Fichier**. Cliquez sur **Enregistrer**. La déclaration de la variable en tant que type « Fichier » vous permet de télécharger des fichiers vers Citrix ADM.

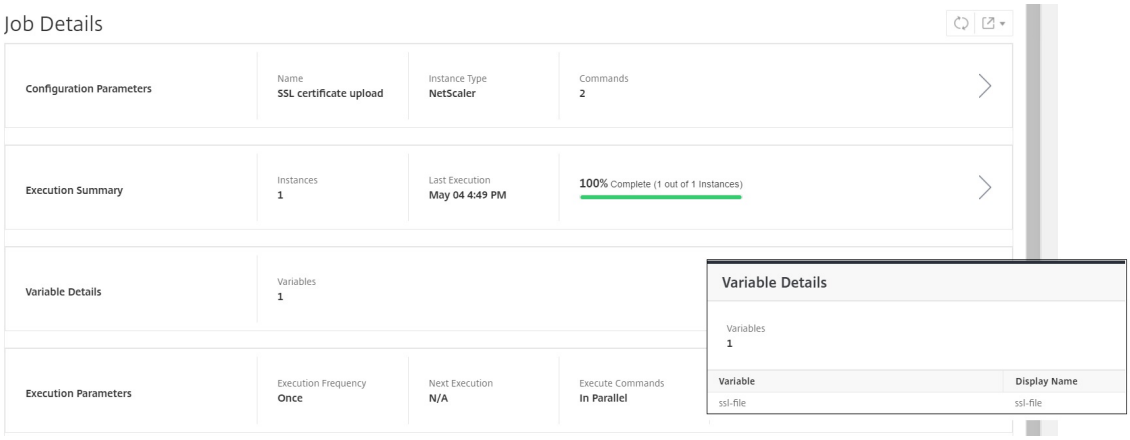


8. Cliquez sur **Suivant** et sélectionnez les instances Citrix ADC dans lesquelles copier les fichiers.
9. Sous l'onglet **Spécifier les valeurs** de **variables, sélectionnez Valeurs de variables communes pour toutes les instances** section, sélectionnez le fichier dans le stockage local de votre système, cliquez sur Télécharger pour**télécharger**le fichier dans Citrix ADM, puis cliquez sur**Suivant**.



10. Sous l'onglet**Aperçu des tâches**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances.
11. Sous l'onglet**Exécuter**, vous pouvez exécuter le travail maintenant ou planifier son exécution ultérieure. Vous pouvez également choisir l'action que Citrix ADM doit prendre en cas d'échec de la commande. Vous pouvez également créer une notification par e-mail pour recevoir une notification sur le succès ou l'échec de la tâche, ainsi que d'autres détails. Cliquez sur **Terminer**.
12. Vous pouvez afficher les détails de la tâche en accédant à**Réseaux** > Tâces de**configuration**et en sélectionnant la tâche que vous avez configurée. Cliquez sur **Détails**, puis sur**Détails des**

variablespour répertorier les variables ajoutées à votre tâche.



Replanifier les tâches configurées à l'aide de modèles intégrés

February 1, 2024

Vous pouvez replanifier une tâche que vous avez planifiée à l'aide de modèles intégrés dans Citrix Application Delivery Management (ADM). Par exemple, vous pouvez modifier l'action que Citrix ADM doit effectuer en cas d'échec d'une commande. Si vous avez précédemment choisi d'ignorer une erreur et de continuer, vous pouvez la modifier pour annuler toutes les commandes réussies en cas d'échec d'une commande.

Pour replanifier un travail configuré à l'aide de modèles intégrés dans Citrix ADM

1. Dans Citrix ADM, accédez à **Réseaux** > **Travaux de configuration**.
2. Sélectionnez le travail à modifier, ajouter ou supprimer des instances, spécifiez des valeurs variables, puis modifiez les actions d'exécution et les paramètres.
3. Cliquez sur **Terminer** pour replanifier la tâche.

> **Remarque**
>
> Vous pouvez également sélectionner la tâche et cliquer sur **Exécuter à nouveau** pour exécuter la tâche sans modifier la source, l'instance et les commandes. Cette fonctionnalité est utile lorsque vous devez exécuter le même ensemble de commandes sur les mêmes instances. Parfois, le travail peut rencontrer une erreur transitoire du côté serveur, et vous devrez peut-être exécuter à nouveau la tâche.

Réutiliser les modèles d'audit de configuration dans les tâches de configuration

February 1, 2024

En tant qu'administrateur, vous pouvez désormais enregistrer les commandes de configuration sous la forme d'un ensemble de modèles de configuration réutilisables lorsque vous créez une tâche et exécutez un audit de configuration. Le modèle de configuration créé et enregistré dans Configuration Jobs est disponible dans Configuration Audit pour créer un modèle d'audit qui peut être appliqué à des instances Citrix ADC spécifiques. De même, le modèle d'audit créé dans le module Configuration Audit est disponible dans les tâches de configuration afin que vous puissiez exécuter le modèle en tant que tâche de configuration. Toute modification apportée au modèle est désormais visible dans les modules Jobs de configuration et Configuration Audit.

Auparavant, la tâche de configuration et les modèles d'audit de configuration devaient être créés séparément pour la même configuration et enregistrés dans des fichiers différents. Cela a entraîné une duplication des efforts lors de la création et de la maintenance des modèles.

Citrix Application Delivery Management (ADM) vous permet d'enregistrer ce modèle dans le système afin que le modèle d'audit soit également disponible dans les tâches de configuration. Les modèles d'audit peuvent désormais être utilisés pour créer des tâches de configuration. De cette façon, les modèles peuvent être utilisés de manière interchangeable entre les tâches de configuration et les audits de configuration.

Par exemple, envisagez une configuration d'équilibrage de charge de base pour laquelle vous ajoutez un serveur virtuel d'équilibrage de charge, ajoutez deux services et liez les services au serveur virtuel.

Cet exemple utilise les commandes suivantes :

```
add lb vserver servername HTTP ipaddress portnumber

add service servicename1 ipaddress1 HTTP 80

add service servicename2 ipaddress2 HTTP 80

bind lb vserver servername servicename1

bind lb vserver servername servicename2
<!--NeedCopy-->
```


Création d'un modèle dans les audits de configuration et réutilisation dans les travaux de configuration

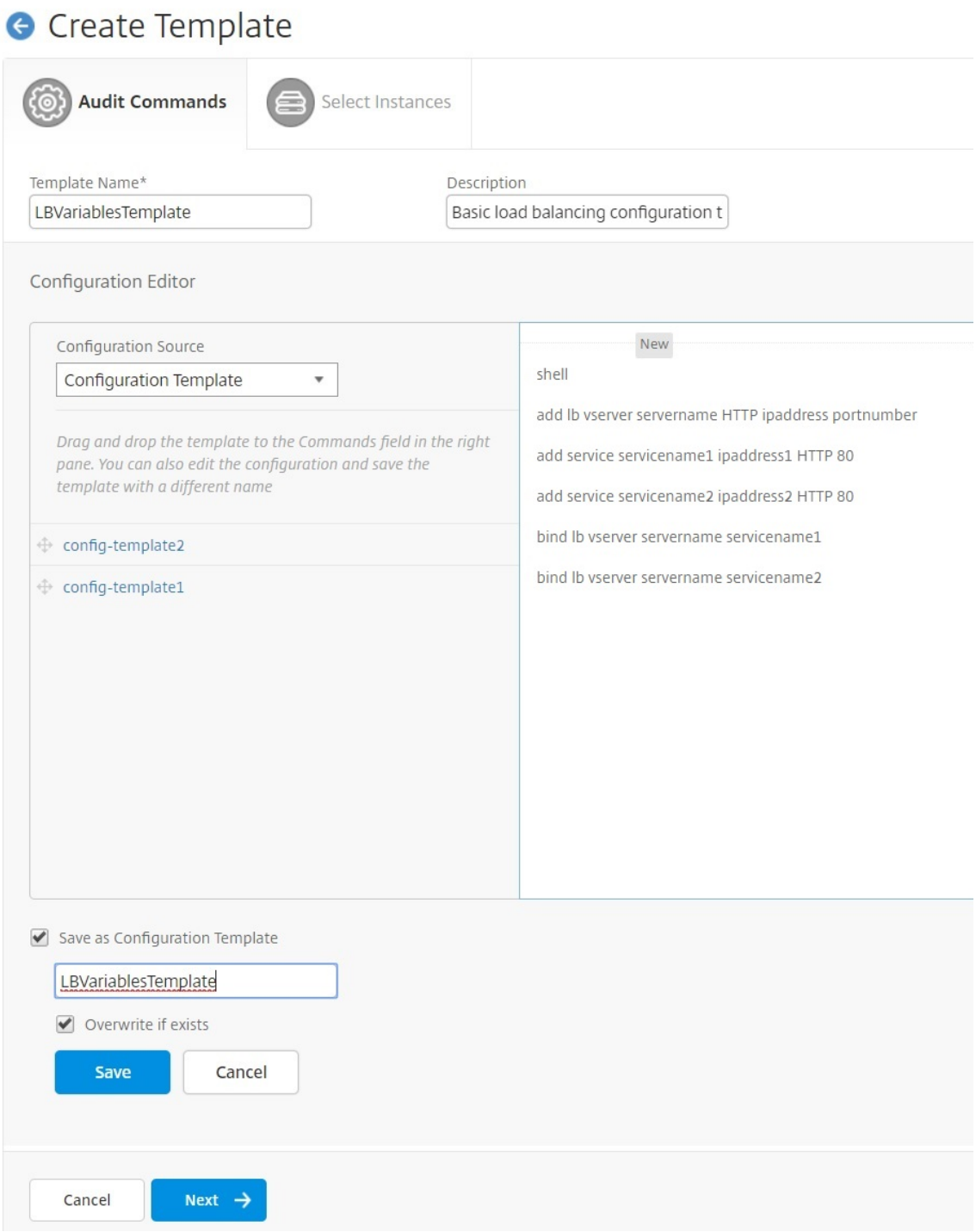
Effectuez la tâche suivante pour créer un modèle dans le module d'audit de configuration et le réutiliser dans le module de tâches de configuration.

Pour créer un modèle d'audit :

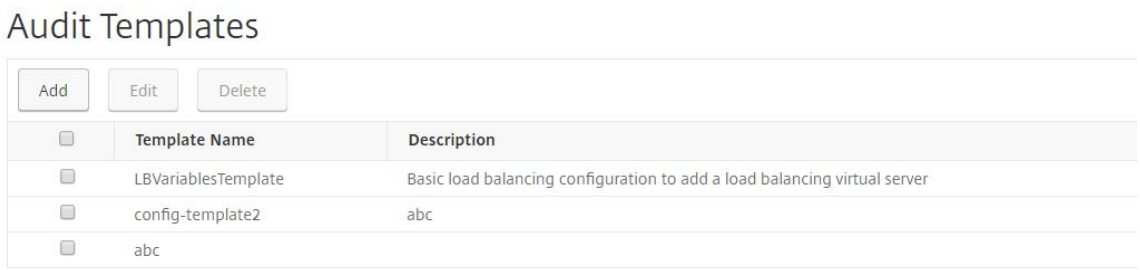
1. Dans Citrix ADM, accédez à**Réseaux > Audit de configuration > Modèle d'audit**, puis cliquez sur**Ajouter**.
2. Dans la page**Créer un modèle**, spécifiez le nom du modèle. Vous pouvez également ajouter plus d'informations sur le modèle dans le champ **Description**.
3. Dans le volet **Commandes**, entrez les commandes de l'exemple.
4. Activez la case à cocher**Enregistrer en tant que modèle de configuration**et spécifiez un nom pour votre modèle. Par exemple, vous pouvez nommer ce modèle comme « LBVariablesTemplate. » Vous pouvez choisir d'écraser d'autres modèles qui existent avec le même nom.

   > **Remarque** Le nom du modèle d'audit peut être identique au nom du modèle de configuration.

5. Cliquez sur**Enregistrer**, puis sur **Suivant**.



6. Cliquez sur **Suivant**.
7. Dans l'onglet **Sélectionner les instances**, sélectionnez les **instances Citrix ADC** sur lesquelles vous souhaitez exécuter ces commandes de configuration et cliquez sur **Terminer**. Le nouveau modèle est désormais visible dans la liste des modèles d'audit.



8. Lorsque vous souhaitez exécuter ces commandes de configuration, accédez à **Réseaux > Travaux de configuration**, puis cliquez sur **Créer un travail**. Le modèle d'audit que vous avez créé précédemment est répertorié en tant que modèle de configuration.

Pour réutiliser le modèle d'audit dans les tâches de configuration :

1. Entrez un nom pour la tâche, sélectionnez le type d'instance, puis faites glisser le modèle vers le volet des commandes.

   Lors de la création du travail de configuration, vous pouvez convertir les paramètres de nom de fichier local et distant en variables. Cela vous permet d'affecter différents fichiers à ces paramètres pour le même ensemble d'instances Citrix ADC chaque fois que vous exécutez le travail.

2. Dans la commande que vous avez saisie, sélectionnez le nom de fichier à convertir en variable, puis cliquez sur**Convertir en variable.**

3. Dans l'onglet **Sélectionner** les instances, sélectionnez les instances sur lesquelles vous souhaitez exécuter ces commandes.

4. Si vous avez spécifié des variables dans les commandes, dans l'onglet **Spécifier les valeurs de variable**, sélectionnez l'une des options suivantes pour spécifier des variables pour vos instances :

   - Valeurs de variables à partir d'un fichier d'entrée : téléchargez un fichier d'entrée pour saisir les valeurs des variables que vous avez définies dans vos commandes, puis chargez le fichier sur le serveur Citrix ADM.
   - Valeurs de variables communes à toutes les instances : spécifiez l'adresse IP et le port du serveur Syslog.

5. Dans l'onglet **Aperçu des tâches**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances et cliquer sur **Suivant**.

6. Dans l'onglet **Exécuter**, cliquez sur **Terminer** pour exécuter le travail de configuration. Maintenant, si vous souhaitez ajouter un autre service à ce serveur d'équilibrage de charge et lier

le service au serveur, vous pouvez modifier les commandes dans la page de commande et les enregistrer.

7. Accédez à **Modèles d'audit** et cliquez sur **Ajouter**.
8. Faites glisser le modèle « LBVariablesTemplate » vers le volet des commandes. Vous pouvez voir que le modèle a été mis à jour avec les nouvelles commandes.

Le modèle d'audit apparaît dans la liste Modèles d'audit et est exécuté toutes les 12 heures par rapport aux configurations des instances spécifiées. Vous pouvez désormais créer des modèles et les réutiliser entre les tâches de configuration et les modules d'audit de configuration.

Importer et exporter des modèles de configuration

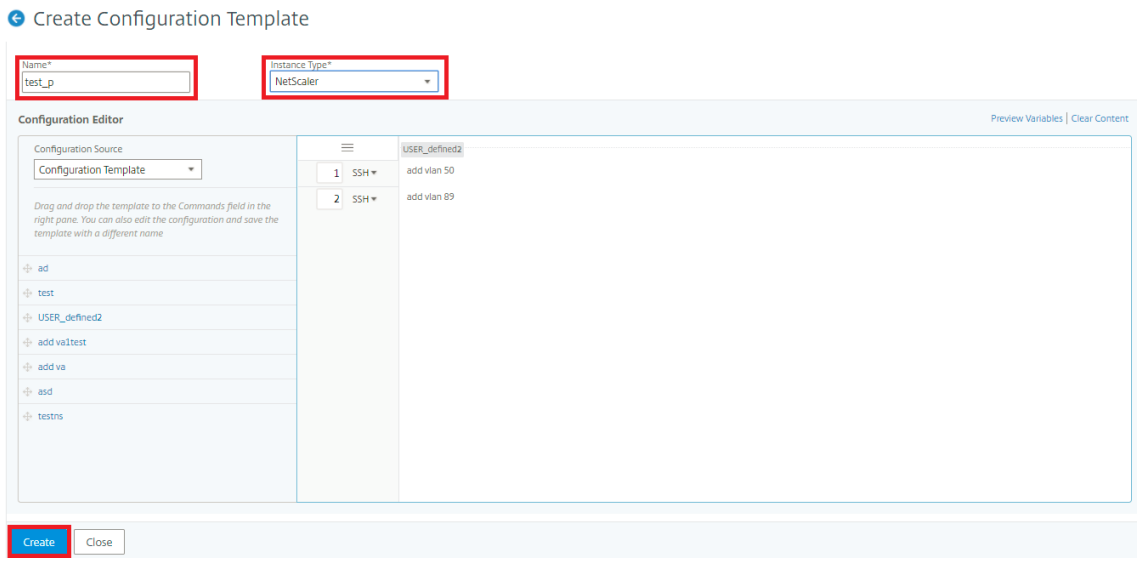
February 1, 2024

Vous pouvez exporter les modèles de configuration depuis n'importe quel Citrix Application Delivery Management (ADM). Vous pouvez également importer le fichier dans le même Citrix ADM ou dans un autre Citrix ADM à tout moment à l'avenir. Les données des modèles de configuration (telles que les commandes de configuration, les définitions de variables et les paramètres) ne sont pas perdues.

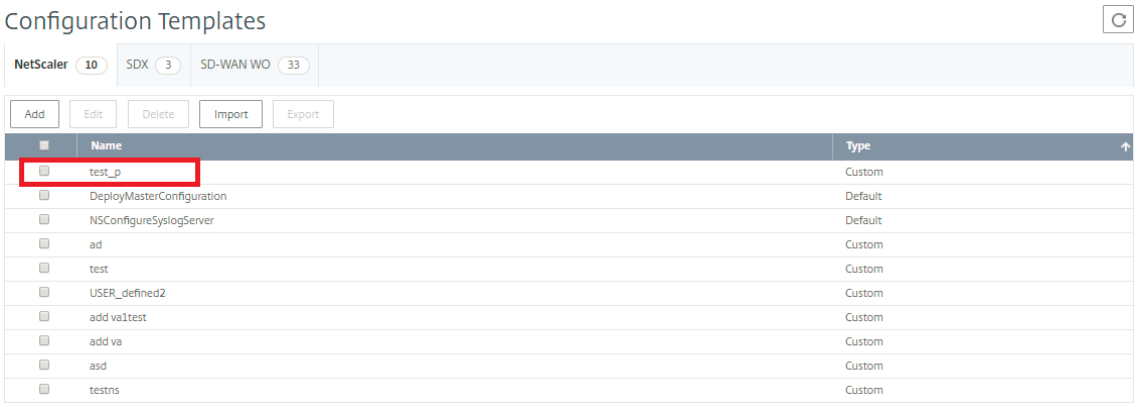
Vous pouvez exporter les modèles de configuration dans un format de fichier **.json** et les enregistrer dans le dossier local. Vous pouvez importer un modèle de configuration. fichiers**json** dans Citrix ADM. Ce fichier est peut-être nouveau ou celui que vous avez exporté depuis le même Citrix ADM ou un autre Citrix ADM.

Pour exporter les modèles de configuration :

1. Accédez à **Réseaux > Tâches de configuration > Modèles de configuration**.
2. Cliquez sur le bouton **Ajouter** pour créer le modèle de configuration.
3. Dans la page **Créer un modèle de configuration**, spécifiez le nom du modèle de configuration et choisissez le type d'instance. Sous **Éditeur de**configuration, sélectionnez la source de configuration comme Modèle de configuration dans le menu déroulant. Vous pouvez faire glisser les modèles de configuration existants vers l'éditeur de configuration. Cliquez sur **Créer**.



4. Accédez à **Réseaux > Travaux de configuration > Modèles de configuration** pour afficher les modèles créés dans la liste des modèles de configuration.

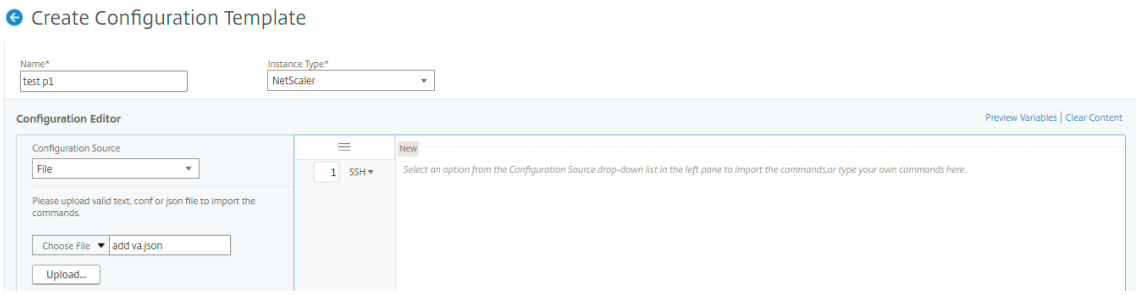


5. Sélectionnez le modèle de configuration nouvellement créé et cliquez sur le bouton **Exporter**.

Le modèle de configuration correspondant est téléchargé sur votre système local au format **.json**.

Pour importer les modèles de configuration :

1. Accédez à **Réseaux > Travaux de configuration > Modèles de configuration** et cliquez sur le bouton **Importer** . Sélectionnez le chemin où vous avez le. **json** du modèle de configuration et téléchargez le. fichiers**json**. Il est fortement recommandé de télécharger le. fichiers**json** que vous avez déjà exportés.
2. Vous pouvez également importer le modèle de configuration à l'aide de l'option **Fichier** dans l'Éditeur de configuration.
3. Sélectionnez **Fichier** dans le menu déroulant de l'**éditeur de configuration**.
4. Sélectionnez **Choisir un fichier** (**.json**) à partir de votre système local et téléchargez le modèle de configuration. fichiers**json**.



Remarque

- Chaque nouveau modèle importé est enregistré avec une nouvelle chaîne d'identification.
- Vous ne pouvez importer les modèles de configuration que si le fichier est enregistré dans le. format**json** . Si vous importez les modèles de configuration autres que les fichiers **.json** depuis votre système local, une erreur s'affiche et l'importation des fichiers échoue.

Tâches de maintenance

February 1, 2024

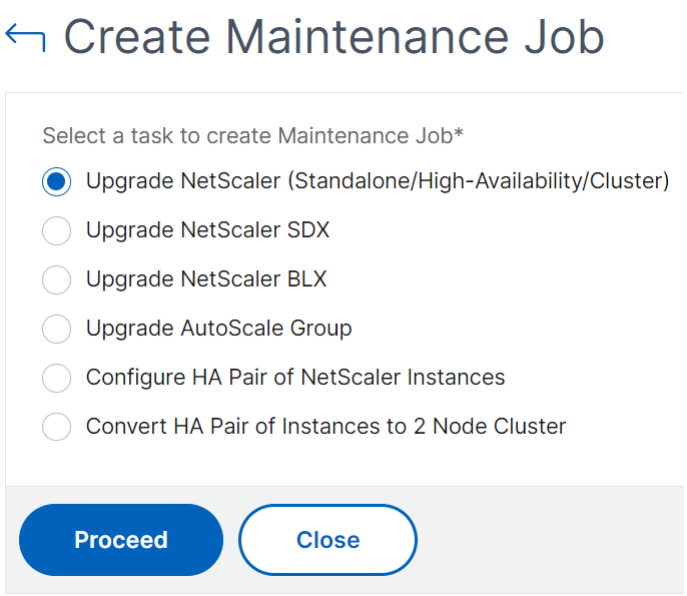
Vous pouvez créer les tâches de maintenance suivantes à l'aide de Citrix ADM. Vous pouvez ensuite planifier les tâches de maintenance à une date et à une heure spécifiques.

- Mettre à niveau les instances de Citrix ADC
- Mettre à niveau les instances Citrix ADC SD WAN-WO
- Mettre à niveau les instances Citrix ADC SDX
- Mettre à niveau les instances Citrix ADC dans le groupe Autoscale
- Configurer la paire HA d'instances Citrix ADC
- Convertir une paire d'instances HA en cluster à 2 nœuds

Planifier la mise à niveau des instances Citrix ADC

1. Dans Citrix ADM, accédez à **Réseaux** > Tâches de **configuration > Tâches** de **maintenance**. Cliquez sur le bouton **Créer un travail**.

2. Dans **Create Maintenance Jobs**, sélectionnez **Mettre à niveau Citrix ADC (Standalone/High-Availability/Cluster)** et cliquez sur **Proceed**.



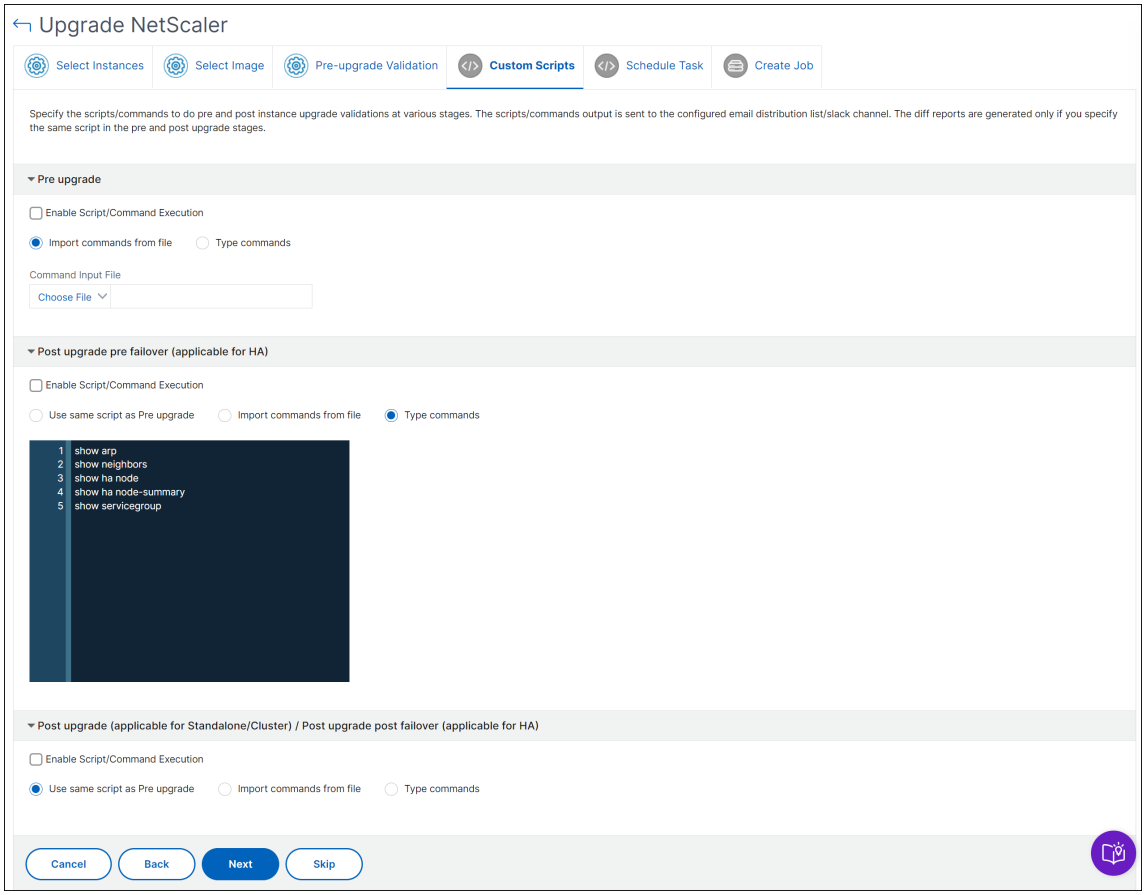
3. Dans **Sélectionner une instance**, tapez le nom de votre choix pour **Nom de la tâche**.
4. Cliquez sur **Ajouter des instances** pour ajouter des instances ADC à mettre à niveau.
   - Pour mettre à niveau une paire HA, spécifiez l'adresse IP du nœud principal ou secondaire. Toutefois, il est recommandé d'utiliser l'instance principale pour mettre à niveau la paire HA.
   - Pour mettre à niveau un cluster, spécifiez l'adresse IP du cluster.
5. Cliquez sur **Suivant** pour lancer la validation préalable à la mise à niveau sur les instances sélectionnées.

   L'onglet **Validation préalable à la mise à niveau** affiche les instances ayant échoué. Supprimez les instances en échec et cliquez sur **Suivant**.

> **Important**
>
> Si vous spécifiez l'adresse IP du cluster, l'ADM effectue la validation préalable à la mise à niveau uniquement sur l'instance spécifiée et non sur les autres nœuds du cluster.

6. Facultatif, dans **Scripts personnalisés**, spécifiez les scripts à exécuter avant et après une mise à niveau d'instance. Utilisez l'une des méthodes suivantes pour exécuter les commandes :

   - **Importer des commandes à partir d'un fichier** - Sélectionnez le fichier d'entrée de commandes à partir de votre ordinateur local.
   - **Tapez des commandes** - Saisissez des commandes directement sur l'interface graphique.



Vous pouvez utiliser des scripts personnalisés pour vérifier les modifications avant et après la mise à niveau d'une instance. Par exemple :

- Version de l'instance avant et après la mise à niveau.
- État des interfaces, des nœuds haute disponibilité, des serveurs virtuels et des services avant et après la mise à niveau.
- Les statistiques des serveurs et services virtuels.
- Les routes dynamiques.

7. Dans **Planifier la tâche**, sélectionnez l'une des options suivantes :

   - **Mise à niveau maintenant** - Le travail de mise à niveau s'exécute immédiatement.
   - **Planifier plus tard** - Sélectionnez cette option pour exécuter ce travail de mise à niveau ultérieurement. Spécifiez la **date d'exécution** et l'**heure de début** lorsque vous souhaitez mettre à niveau les instances.

     Si vous souhaitez mettre à niveau une paire ADC HA en deux étapes, sélectionnez **Effectuer une mise à niveau en deux étapes pour les nœuds en haute disponibilité**.

     Spécifiez la **date d'exécution** et l'**heure de début** lorsque vous souhaitez mettre à niveau une autre instance de la paire HA.

8. Dans **Créer une tâche**, spécifiez les détails suivants :

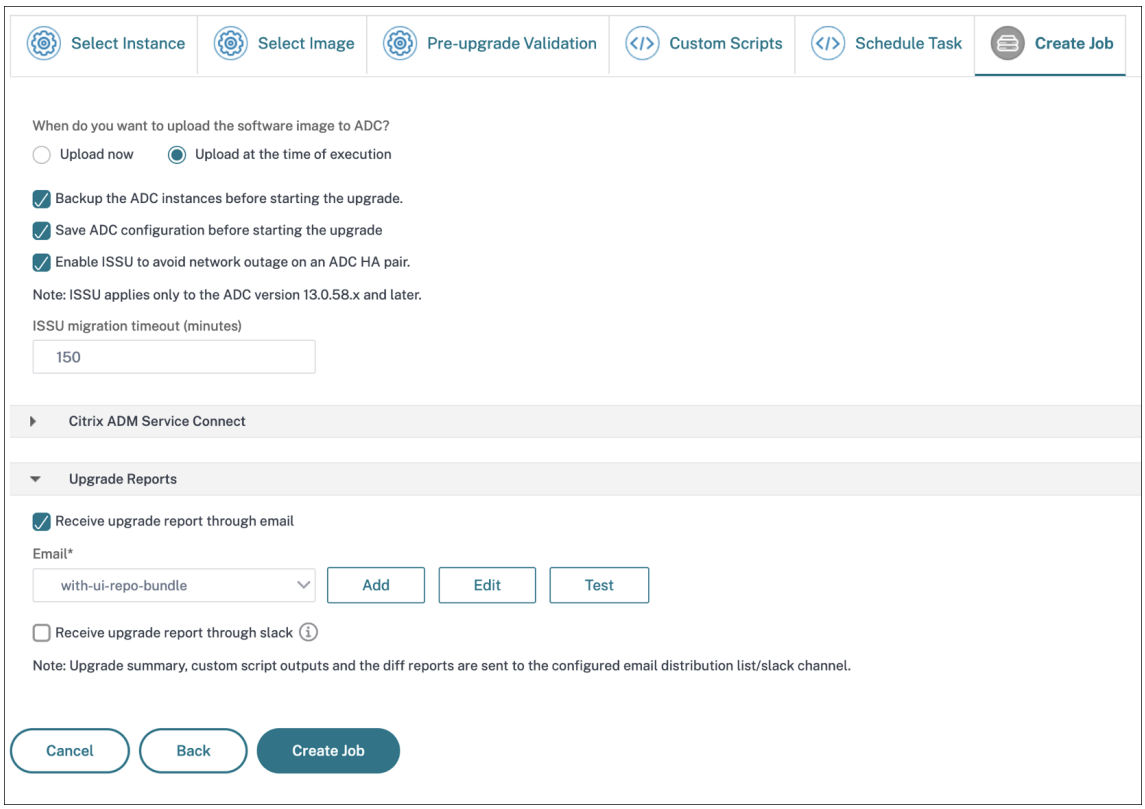
   a) Sélectionnez l'une des options suivantes dans la liste des **images logicielles** :

      - **Local** : sélectionnez le fichier de mise à niveau de l'instance sur votre machine locale.
      - **Appliance** : sélectionnez le fichier de mise à niveau de l'instance dans un navigateur de fichiers ADM. L'interface graphique ADM affiche les fichiers d'instance présents sur `/var/mps/mps_images`.

   b) Spécifiez le moment où vous souhaitez télécharger l'image sur une instance :

      - **Télécharger maintenant** - Sélectionnez cette option pour télécharger l'image immédiatement. Toutefois, le travail de mise à niveau s'exécute à l'heure planifiée.
      - **Télécharger au moment de l'exécution** - Sélectionnez cette option pour télécharger l'image au moment de l'exécution de la tâche de mise à niveau.

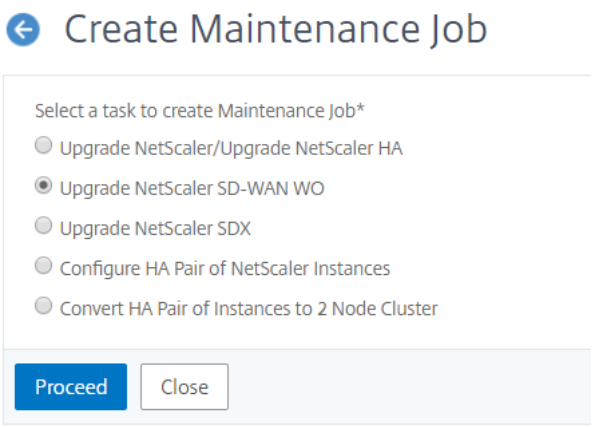
   - **Nettoyer l'image logicielle à partir de Citrix ADC lors de la mise à niveau réussie** - Sélectionnez cette option pour effacer l'image téléchargée dans l'instance ADC après la mise à niveau de l'instance.
   - **Sauvegardez les instances ADC avant de commencer la mise à niveau.** - Crée une sauvegarde des instances ADC sélectionnées.
   - **Recevoir le rapport d'exécution par e-mail** - Envoie le rapport d'exécution par e-mail. Pour ajouter une liste de distribution d'e-mails, voir Créer une liste de distribution d'e-mails.
   - **Recevoir le rapport d'exécution via la marge** - Envoie le rapport d'exécution en marge. Pour ajouter un profil Slack, consultez Créer un profil Slack.



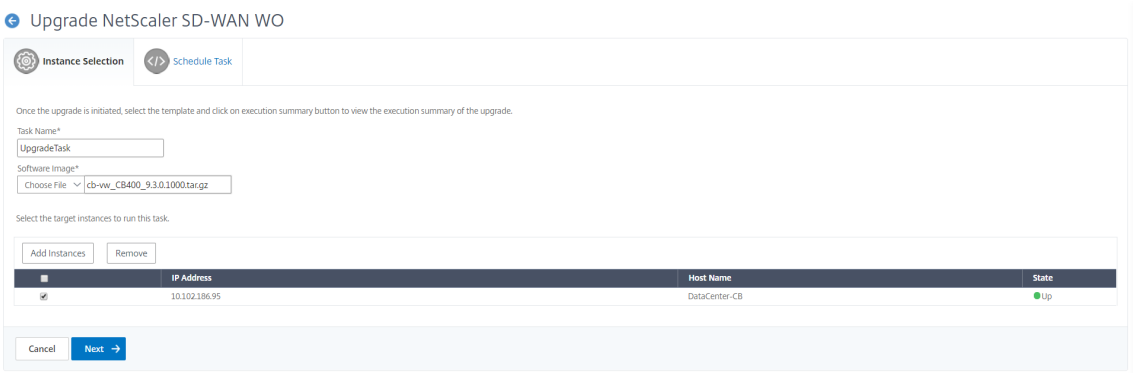
9. Cliquez sur **Créer un travail**.

Planifier la mise à niveau des instances WO SD-WAN Citrix ADC

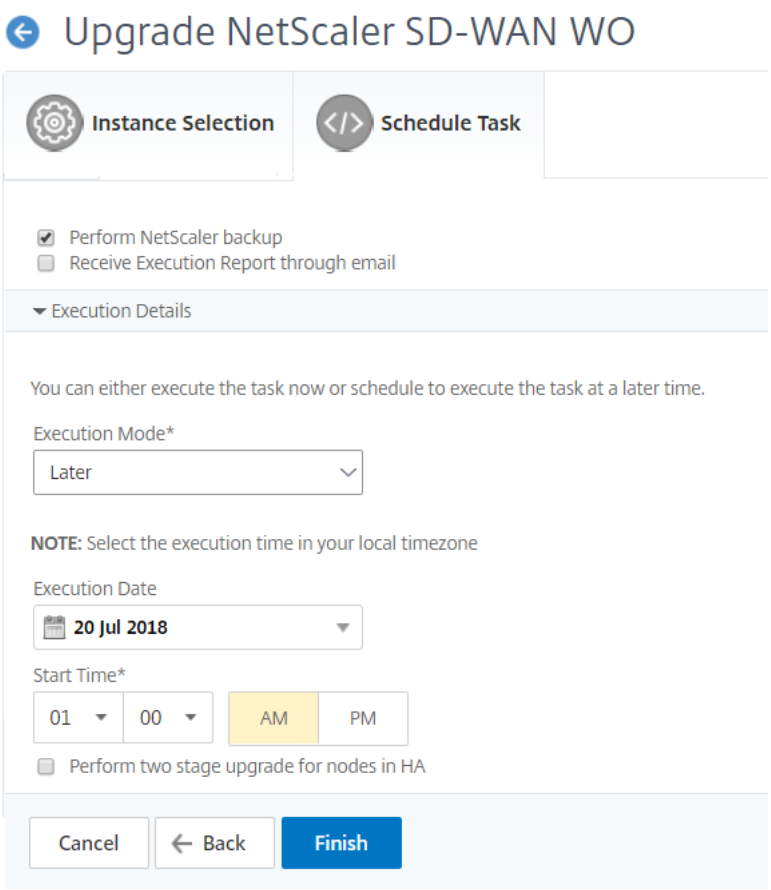
1. Accédez à **Réseaux** > **Travaux de configuration** > **Travaux de maintenance** . Cliquez sur le bouton **Créer une tâche**.
2. Sur la page **Créer une tâche de maintenance**, sélectionnez **Mettre à niveau Citrix ADC SD-WAN WO** et cliquez sur **Continuer**.



3. Dans la page **Mettre à niveau Citrix ADC SD-WAN WO**, dans l'onglet **Sélection d'instance**, ajoutez un **nom de tâche**. Dans la liste des images logicielles, sélectionnez Local (votre machine locale) ou Appliance (le fichier de génération doit être présent sur l'appliance virtuelle Citrix ADM). Ajoutez les instances WO SD-WAN Citrix ADC sur lesquelles vous souhaitez exécuter le processus de mise à niveau. Cliquez sur **Suivant**.



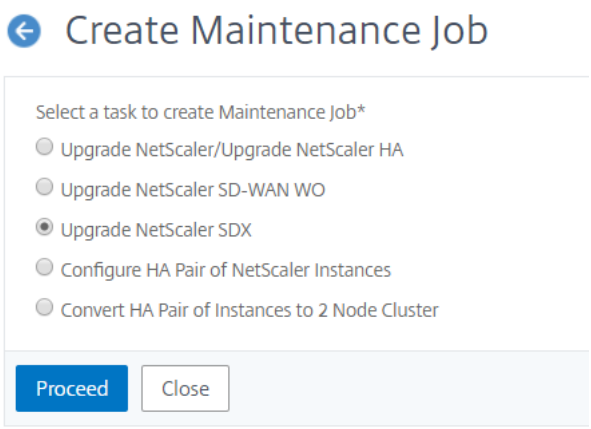
4. Pour mettre à niveau l'instance WO SD-WAN Citrix ADC maintenant, sélectionnez **Maintenant** dans la liste **Mode d'exécution**. Cliquez sur **Terminer**.
5. Pour mettre à niveau l'instance WO SD-WAN Citrix ADC ultérieurement, sélectionnez **Plus tard** dans la liste**Mode d'exécution**. Vous pouvez ensuite choisir la date d'exécution et l'heure de début de la mise à niveau de l'instance WO SD-WAN Citrix ADC.
6. Vous pouvez activer la notification par e-mail pour recevoir le rapport d'exécution de la mise à niveau de l'instance WO Citrix ADC SD-WAN. Activez la case à cocher **Recevoir le rapport d'exécution par e-mail** pour activer la notification par e-mail.
7. Sélectionnez l'icône **+** pour créer la liste de distribution d'e-mails.



8. Dans la page **Créer une liste de distribution de courrier électronique**, spécifiez un nom pour la liste de distribution de courrier électronique. Ajoutez le serveur de messagerie SMTP à utiliser pour envoyer des notifications par e-mail au serveur de messagerie. Dans la zone **De**, ajoutez l'adresse e-mail à partir de laquelle envoyer des messages. Dans la zone **À**, ajoutez l'adresse e-mail ou les adresses auxquelles vous souhaitez envoyer des messages. Vous pouvez également ajouter une ou plusieurs adresses e-mail auxquelles envoyer des copies et des copies des messages sans afficher ces adresses dans les messages ou les copies. Cliquez sur **Créer**. Après avoir créé la liste de distribution d'e-mails, cliquez sur **Terminer** pour terminer le processus de configuration.

Planifier la mise à niveau des instances Citrix ADC SDX

1. Dans Citrix ADM, accédez à **Réseaux** > Tâches de **configuration > Tâches** de **maintenance**. Cliquez sur le bouton **Créer une tâche**.
2. Sur la page **Créer un travail de maintenance**, sélectionnez **Mettre à niveau Citrix ADC SDX**, puis cliquez sur **Continuer** .



3. Sur la page **Mettre à niveau le matériel SDX Citrix ADC**, dans l'onglet **Sélection d'instance**, ajoutez un **nom de tâche**. Dans la liste des images logicielles, sélectionnez Local (votre machine locale) ou Appliance (le fichier de génération doit être présent sur l'appliance virtuelle Citrix ADM). Ajoutez les instances Citrix ADC SDX sur lesquelles vous souhaitez exécuter le processus de mise à niveau. Cliquez sur **Suivant**.
4. Vous pouvez activer la notification par e-mail pour recevoir le rapport d'exécution de la mise à niveau de l'instance SDX Citrix ADC. Activez la case à cocher **Recevoir le rapport d'exécution par e-mail** pour activer la notification par e-mail.
5. Sélectionnez l'icône **+** pour créer la liste de distribution d'e-mails.
6. Pour mettre à niveau l'instance Citrix ADC SDX dès maintenant, sélectionnez **Maintenant** dans la liste des **modes d'exécution**. Cliquez sur **Terminer**.
7. Pour mettre à niveau l'instance Citrix ADC SDX ultérieurement, sélectionnez **Plus tard** dans la liste **Mode d'exécution**. Vous pouvez ensuite choisir la date d'exécution et l'heure de début de la mise à niveau de l'instance SDX Citrix ADC.
8. Dans la page **Créer une liste de distribution de courrier électronique**, spécifiez un nom pour la liste de distribution de courrier électronique. Ajoutez le serveur de messagerie SMTP à utiliser pour envoyer des notifications par e-mail au serveur de messagerie. Dans la zone **De**, ajoutez l'adresse e-mail à partir de laquelle envoyer des messages. Dans la zone **À**, ajoutez l'adresse e-mail ou les adresses auxquelles vous souhaitez envoyer des messages. Vous pouvez également ajouter une ou plusieurs adresses e-mail auxquelles envoyer des copies et des copies des messages sans afficher ces adresses dans les messages ou les copies. Cliquez sur **Créer**. Après avoir créé la liste de distribution d'e-mails, cliquez sur **Terminer** pour terminer le processus de configuration.

Planifier la mise à niveau du groupe Auto Scale

Procédez comme suit pour mettre à niveau toutes les instances des services cloud qui font partie du groupe Autoscale :

1. Dans Citrix ADM, accédez à **Réseaux > Travaux de configuration > Travaux de maintenance**. Cliquez sur le bouton **Créer un travail**.
2. Dans la page **Créer des travaux de maintenance**, sélectionnez **Mettre à niveau le groupe de mise à niveau automatique**, puis cliquez sur **Continuer** .
3. Dans l'onglet **Paramètres de mise à niveau** :
   a) Sélectionnez le **groupe Autoscale** que vous souhaitez mettre à niveau.
   b) Dans **Image**, sélectionnez la version de Citrix ADC. Cette image est la version existante des instances Citrix ADC du groupe Autoscale.
   c) Dans **Citrix ADC Image**, parcourez le fichier de version de Citrix ADC vers lequel vous souhaitez effectuer la mise à niveau.

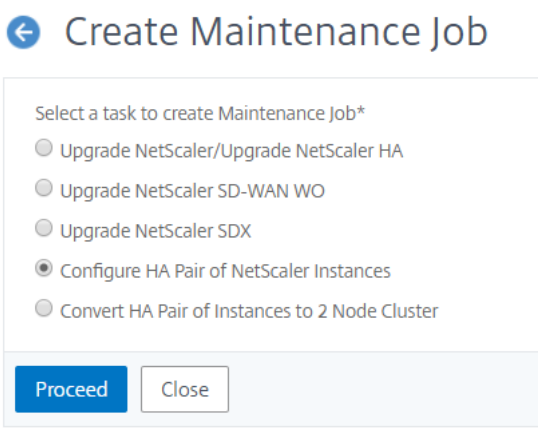
      Si vous cochez la **case Mise à niveau**progressive, la tâche de mise à niveau attend l'expiration de la période de connexion de drain spécifiée.
   d) Cliquez sur **Suivant**.
4. Dans l'onglet **Planifier la tâche** :
   a) Sélectionnez l'une des options suivantes dans la liste Mode d'exécution :
      - **Maintenant :**pour démarrer immédiatement la mise à niveau des instances Citrix ADC.
      - **Plus tard :** pour démarrer la mise à niveau des instances Citrix ADC ultérieurement.
   b) Si vous sélectionnez l'option **Plus tard**, sélectionnez la date d'exécution et l'heure de début lorsque vous souhaitez démarrer la tâche de mise à niveau.

   Vous pouvez également activer les notifications par e-mail et par slack pour recevoir le rapport d'exécution de la mise à niveau du groupe Autoscale. Cliquez sur la la case à cocher **Recevoir le rapport d'exécution par courrier électronique** et la case à cocher **Recevoir le rapport d'exécution via Slack** pour activer les notifications.
5. Cliquez sur **Terminer**.

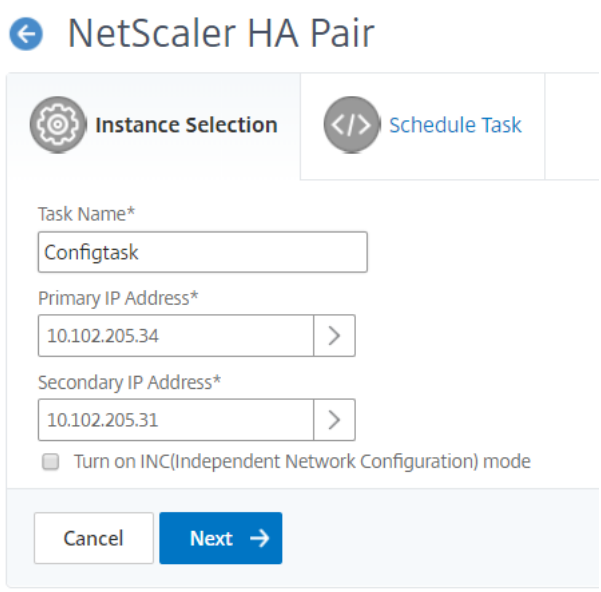
Planifier la configuration de la paire HA d'instances Citrix ADC

1. Dans Citrix ADM, accédez à **Réseaux** > Tâches de **configuration > Tâches** de **maintenance**. Cliquez sur le bouton **Créer une tâche**.

2. Sur la page **Créer une tâche de maintenance**, sélectionnez **Configurer HA Pair of Citrix ADC Instances** et cliquez sur **Continuer**.



3. Dans la page **Citrix ADC HA Paire**, dans l'onglet **Sélection d'instance**, ajoutez un **nom de tâche**. Entrez l'adresse IP principale et l'adresse secondaire, puis cliquez sur **Suivant**.



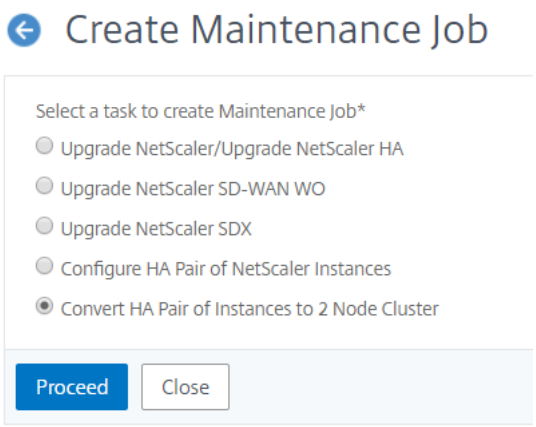
4. Sous l'onglet **Planifier la tâche**, vous pouvez choisir de configurer la paire Citrix ADC HA maintenant ou ultérieurement.
5. Pour configurer la paire Citrix ADC HA dès maintenant, sélectionnez **Maintenant** dans la liste des **modes d'exécution**. Vous pouvez activer la notification par e-mail pour recevoir le rapport d'exécution de la paire Citrix ADC HA. Activez la case à cocher **Recevoir le rapport d'exécution par e-mail** pour activer la notification par e-mail.
6. Pour configurer ultérieurement la paire Citrix ADC HA, sélectionnez **Plus tard** dans la liste **Mode d'exécution**. Vous pouvez ensuite choisir la date eExecution et l'heure de début. Vous pouvez activer la notification par e-mail pour recevoir le rapport d'exécution de la paire Citrix ADC HA.

Activez la case à cocher **Recevoir le rapport d'exécution par e-mail** pour activer la notification par e-mail.

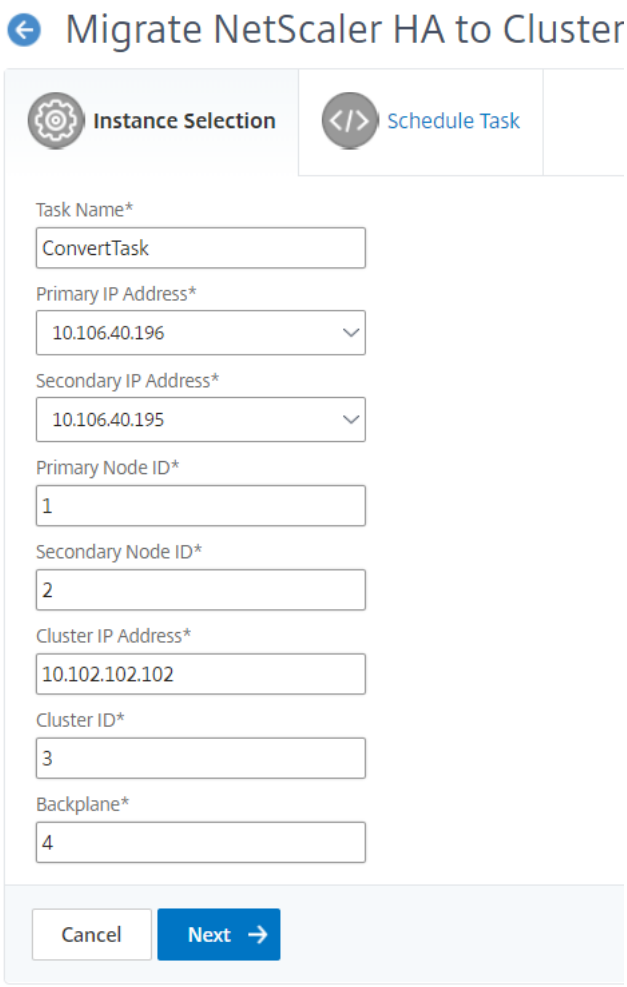
7. Sélectionnez l'icône **+** pour créer la liste de distribution d'e-mails.
8. Sur la page **Créer une liste de distribution d'e-mails**, indiquez un **nom** pour la liste de distribution d'e-mails. Ajoutez le serveur de messagerie SMTP à utiliser pour envoyer des notifications par e-mail au serveur de messagerie. Dans la zone **De**, ajoutez l'adresse e-mail à partir de laquelle vous souhaitez envoyer les messages. Dans la zone **À**, ajoutez l'adresse e-mail ou les adresses auxquelles vous souhaitez envoyer des messages. Vous pouvez également ajouter une ou plusieurs adresses e-mail auxquelles envoyer des copies et des copies des messages sans afficher ces adresses dans les messages ou les copies. Cliquez sur **Créer**. Après avoir créé la liste de distribution d'e-mails, cliquez sur **Terminer** pour terminer le processus de configuration.

Planifier la conversion d'une paire d'instances HA en cluster

1. Dans Citrix ADM, accédez à **Réseaux** > Tâches de **configuration > Tâches** de **maintenance**. Cliquez sur le bouton **Créer une tâche**.
2. Sur la page **Créer un travail de maintenance**, sélectionnez **Convertir une paire d'instances HA en cluster à 2 nœuds**, puis cliquez sur **Continuer** .



3. Sur la page **Migrer Citrix ADC HA vers le cluster**, dans l'onglet **Sélection d'instance**, ajoutez un **nom de tâche**. Spécifiez l'adresse IP principale, l'adresse secondaire, l'ID du nœud principal, l'ID du nœud secondaire, l'adresse IP du cluster, l'ID du cluster et le backplane. Cliquez sur **Suivant**.



4. Sous l'onglet **Planifier la tâche**, vous pouvez choisir de migrer la HA Citrix ADC vers Cluster maintenant ou une version ultérieure.
5. Pour configurer ultérieurement la paire Citrix ADC HA, sélectionnez **Plus tard** dans la liste **Mode d'exécution**. Vous pouvez ensuite choisir la date d'exécution et l'heure de début. Vous pouvez activer la notification par e-mail pour recevoir le rapport d'exécution de la paire Citrix ADC HA. Activez la case à cocher **Recevoir le rapport d'exécution par e-mail** pour activer la notification par e-mail.
6. Sélectionnez l'icône **+** pour créer la liste de distribution d'e-mails.
7. Dans la page **Créer une liste de distribution de courrier électronique**, spécifiez un nom pour la liste de distribution de courrier électronique. Ajoutez le serveur de messagerie SMTP à utiliser pour envoyer des notifications par e-mail au serveur de messagerie. Dans la zone **De**, ajoutez l'adresse e-mail à partir de laquelle vous souhaitez envoyer les messages. Dans la zone **À**, ajoutez l'adresse e-mail ou les adresses auxquelles vous souhaitez envoyer des messages. Vous pouvez également ajouter une ou plusieurs adresses e-mail auxquelles envoyer des copies et des

copies des messages sans afficher ces adresses dans les messages ou les copies. Cliquez sur **Créer**. Après avoir créé la liste de distribution d'e-mails, cliquez sur **Terminer** pour terminer le processus de configuration.

Audit de configuration

February 1, 2024

Ce document comprend :

- Création de modèles d'audit
- Affichage des rapports d'audit
- Modifications de configuration d'audit entre les instances
- Obtenir des conseils de configuration sur la configuration réseau
- Comment interroger l'audit de configuration des instances Citrix ADC

Créer des modèles d'audit

February 1, 2024

Vous voulez vous assurer que certaines configurations s'exécutent sur des instances spécifiques pour des performances optimales de votre réseau. Vous souhaitez également surveiller les modifications de configuration sur les instances de Citrix Application Delivery Controller (ADC) gérées, résoudre les erreurs de configuration et restaurer les configurations non enregistrées après un arrêt soudain du système. Vous pouvez créer des modèles d'audit avec des configurations spécifiques que vous souhaitez auditer sur certaines instances. Citrix Application Delivery Management (Citrix ADM) compare ces instances avec le modèle d'audit et signale s'il y a une incompatibilité dans la configuration.Chaque fois qu'il y a une incompatibilité de configuration, Citrix ADM génère un rapport de diff de configuration, qui vous permet de résoudre les problèmes et de corriger les modifications de configuration indésirables.

Vous pouvez automatiser l'exécution du modèle d'audit en

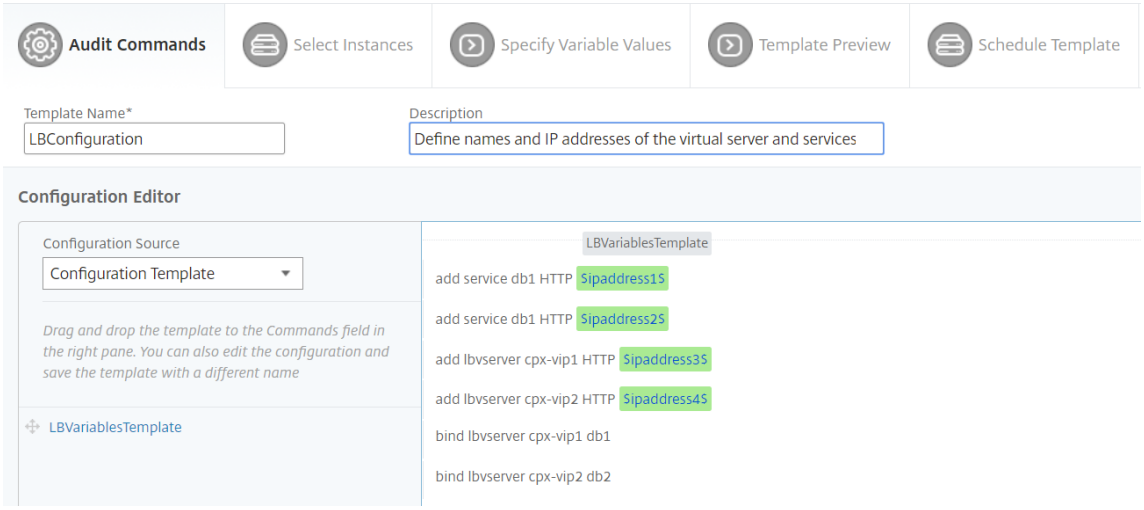
- Planification de l'heure à laquelle le modèle doit être exécuté
- Définition de la fréquence à laquelle Citrix ADM doit exécuter le modèle. Vous pouvez exécuter le modèle tous les jours, un jour spécifique d'une semaine ou à une date spécifique d'un mois.

Vous avez également la possibilité d'envoyer le rapport de comparaison généré par Citrix ADM à des adresses e-mail spécifiées que vous pouvez configurer. Cette option permet à votre utilisateur de recevoir le rapport sous la forme d'une pièce jointe et il n'est pas nécessaire que l'utilisateur se connecte à Citrix ADM pour exporter les rapports manuellement.

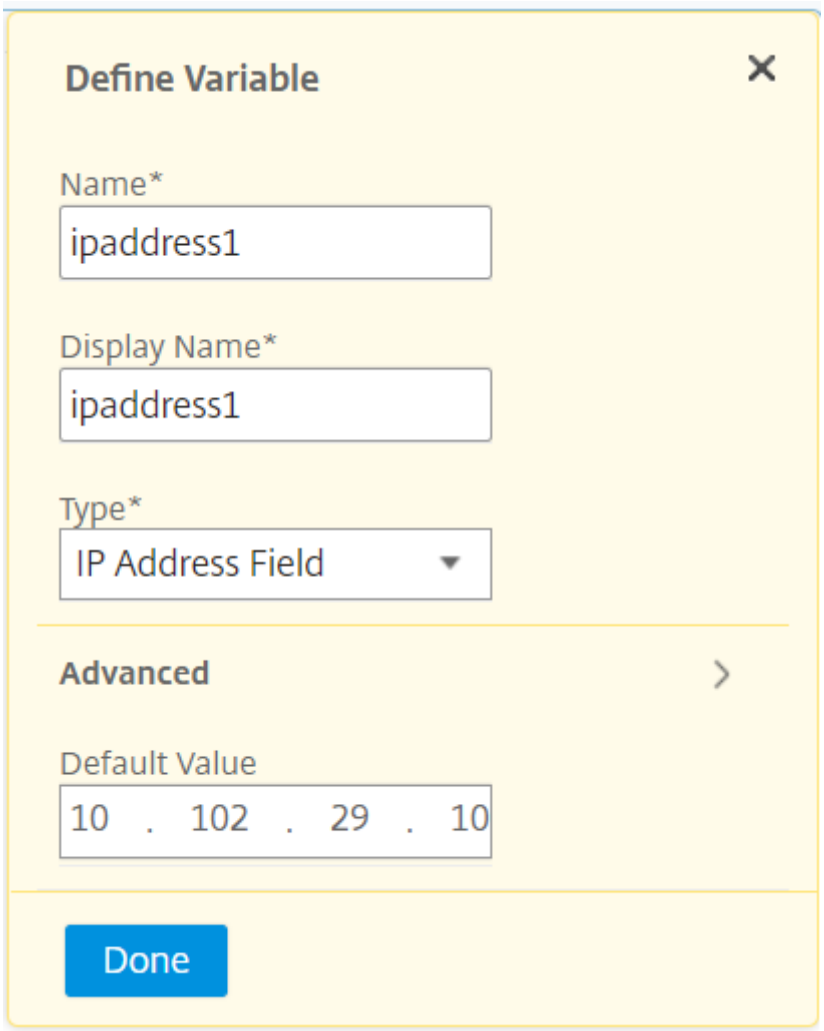
> **Remarque**
> L'option **Renommer** est désactivée pour les modèles de configuration par défaut. Vous pouvez toutefois renommer les modèles de configuration personnalisés.

Pour créer des modèles d'audit :

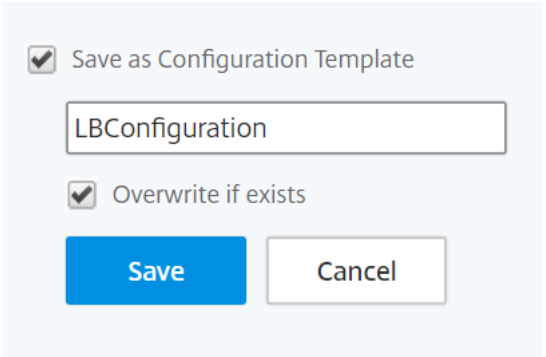
1. Accédez à **Réseaux** > **Audit de configuration** > **Modèles d'audit**, puis cliquez sur **Ajouter**.
2. Dans la page**Créer un modèle**et dans l'onglet**Commandes d'audit**, spécifiez le nom du modèle et sa description.
3. Sur la page **Éditeur de configuration**, saisissez vos commandes et enregistrez-les en tant que modèle de configuration. Vous pouvez également faire glisser un modèle existant du volet gauche vers l'éditeur.
4. Sélectionnez les valeurs que vous souhaitez convertir en variable, puis cliquez sur **Convertir en variable**. Par exemple, sélectionnez l'adresse IP du serveur d'équilibrage de charge « ipaddress1 », puis cliquez sur **Convertir en variable**. La variable est maintenant entourée de « $ » comme indiqué dans l'image ci-dessous.



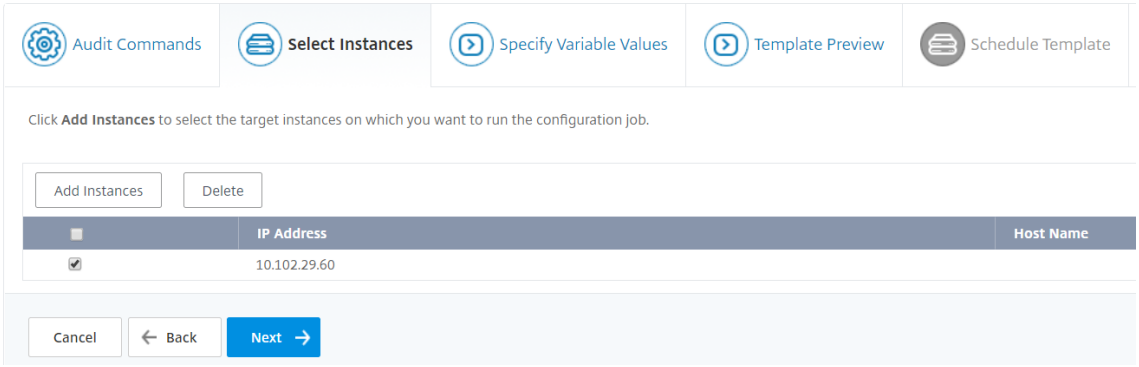
Dans la fenêtre **Définir une variable**, définissez les propriétés de cette variable - nom, nom d'affichage et type de la variable. Cliquez sur l'option**Avancé** si vous souhaitez spécifier une valeur par défaut pour votre variable.



Vous pouvez également enregistrer les commandes en tant que modèle de configuration.



5. Cliquez sur **Enregistrer**, puis sur **Suivant**.
6. Dans l'onglet **Sélectionner les instances**, sélectionnez les instances sur lesquelles vous souhaitez exécuter l'audit de configuration et cliquez sur **Suivant**.

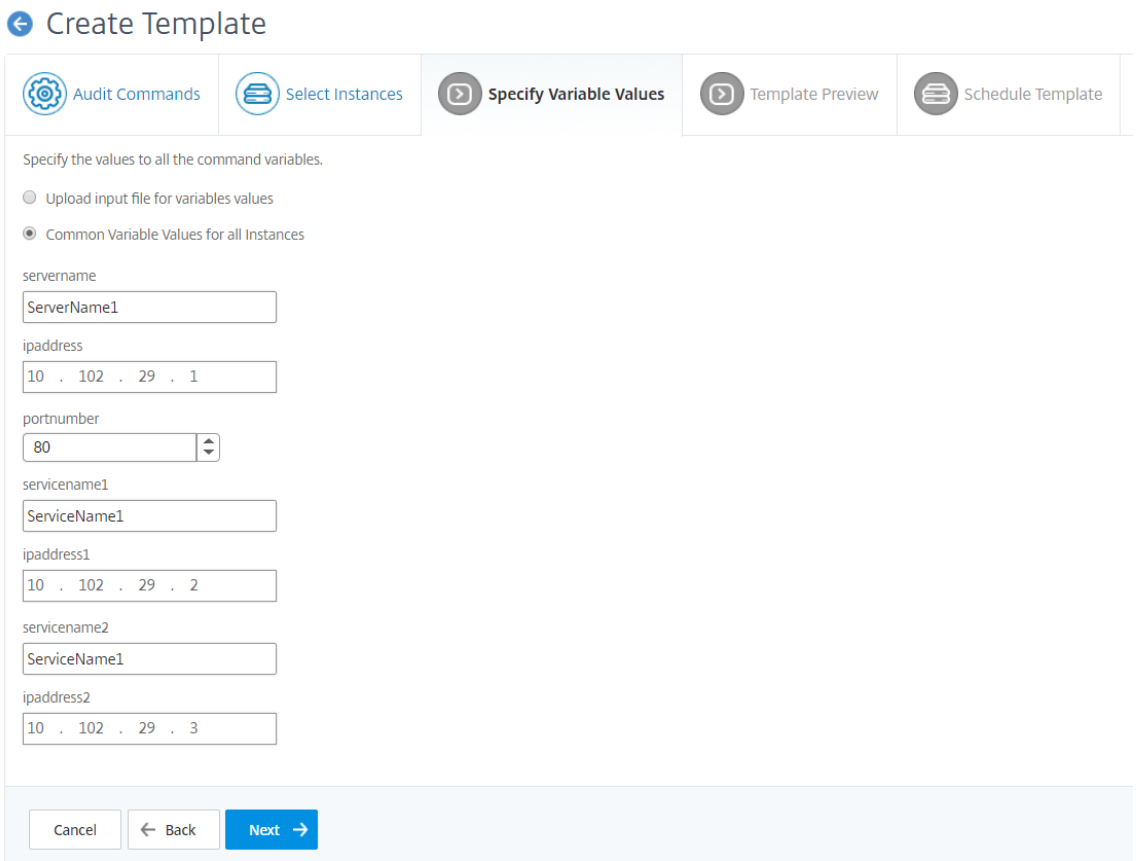


7. Dans l'onglet **Spécifier les valeurs variables**, vous disposez de deux options :

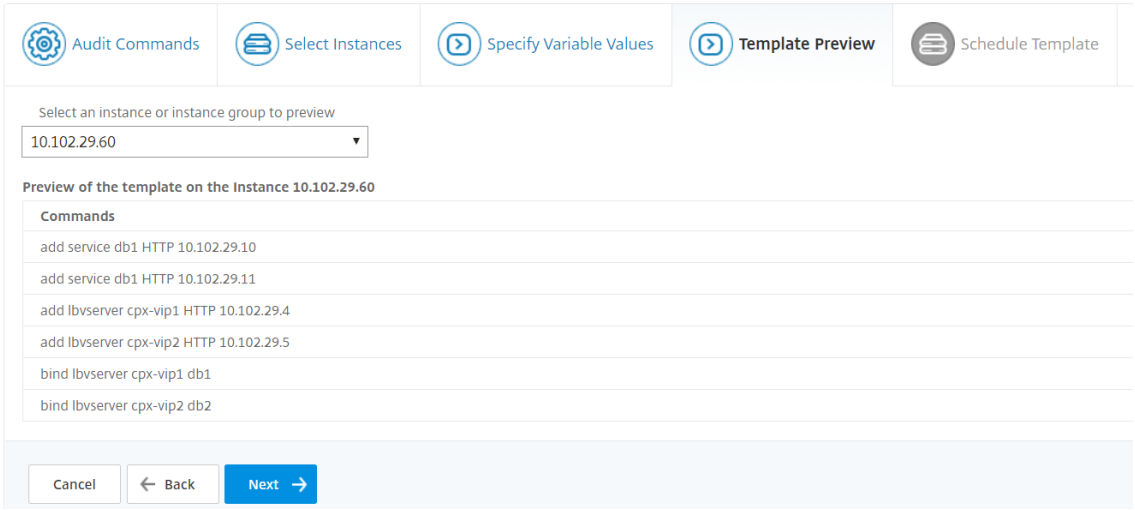
   a) Téléchargez le fichier d'entrée pour entrer les valeurs des variables que vous avez définies dans vos commandes, puis téléchargez le fichier sur le serveur Citrix ADM

   b) Entrez des valeurs communes pour les variables que vous avez définies pour toutes les instances

8. Cliquez sur **Suivant**.



9. Dans l'onglet **Aperçu du modèle**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances. Cliquez sur **Suivant**.



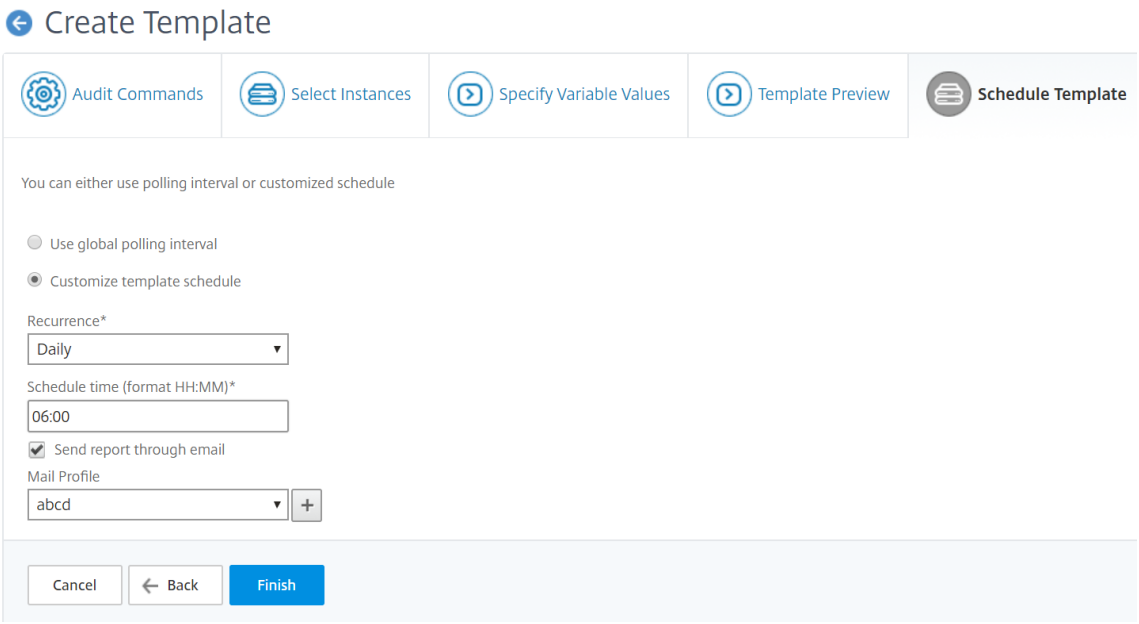
10. Dans l'onglet **Modèle de planification**, vous disposez des options suivantes pour planifier l'exécution du modèle et configurer l'adresse de messagerie pour envoyer le rapport de diff.

    - **Utilisez l'intervalle d'interrogation global**. Sélectionnez cette option pour exécuter le modèle sur les instances à un moment configuré globalement sur Citrix ADM.

      > **Remarque**
      >
      > Pour configurer l'intervalle d'interrogation global dans Citrix ADM, accédez à **Réseaux** > **Audit de configuration** > **Modèles d'audit,** puis cliquez sur **Intervalle d'interrogation globale**. Dans le champ **Intervalle d'interrogation**, entrez les minutes auxquelles Citrix ADM doit interroger globalement les instances.

    - **Personnaliser la planification du modèle**. Utilisez cette option pour configurer l'heure et la fréquence auxquelles les modèles doivent être exécutés
    - **Envoyer un rapport par courrier électronique**. Utilisez cette option pour configurer le profil de messagerie auquel le rapport diff doit être envoyé en tant que pièce jointe.

11. Cliquez sur **Terminer**.



Le modèle d'audit apparaît dans la liste **Modèles d'audit** et est exécuté à l'heure planifiée par rapport aux configurations dans les instances spécifiées.

Afficher les rapports d'audit

February 1, 2024

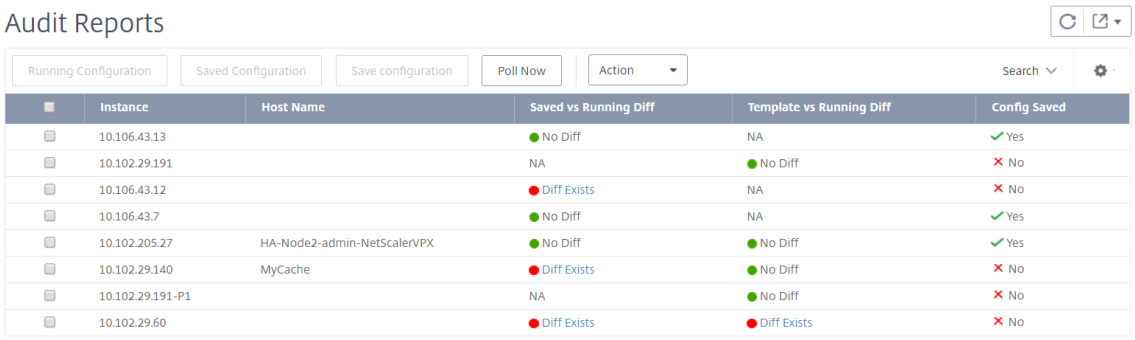
Citrix Application Delivery Management (Citrix ADM) vous permet d'afficher et de télécharger le rapport d'audit de configuration dans la section Audit de configuration.La section Audit de configuration vous permet d'exporter le rapport de synthèse sur toutes les instances et par instance, et vous permet également d'exporter un rapport de diff granulaire pour chaque paire de modèles d'instance.

Les modèles d'audit qui apparaissent dans la liste Modèles d'audit sont exécutés à l'heure planifiée sur les configurations des instances spécifiées. Le graphique **NetScaler Config Drift** du tableau de bord de l'**audit de configuration** affiche des détails de haut niveau sur les modifications de configuration enregistrées par rapport aux configurations non enregistrées. Lorsque vous cliquez sur le graphique de**dérive de configuration NetScaler**, la page **Rapports d'audit** qui suit affiche une liste d'instances indiquant à la fois « Diff Exists » et « No Diff ». Vous pouvez télécharger les rapports diff affichés par Citrix ADM.

Citrix ADM fournit également une option pour planifier l'exportation automatique du rapport diff en tant que pièce jointe de messagerie. Pour plus d'informations sur la façon de planifier l'exportation des rapports, consultez Création de modèles d'audit.

Pour exporter des rapports d'audit de configuration :

1. Dans Citrix ADM, accédez à **Réseaux** > **Audit de configuration**.
2. Sur la page **Configuration Audit**, cliquez dans le graphique **NetScaler Config Drift**.
3. La page **Rapports d'audit** répertorie les instances qui présentent une différence. La page affiche également une liste d'instances qui ne présentent aucune différence dans leurs configurations en cours d'exécution.

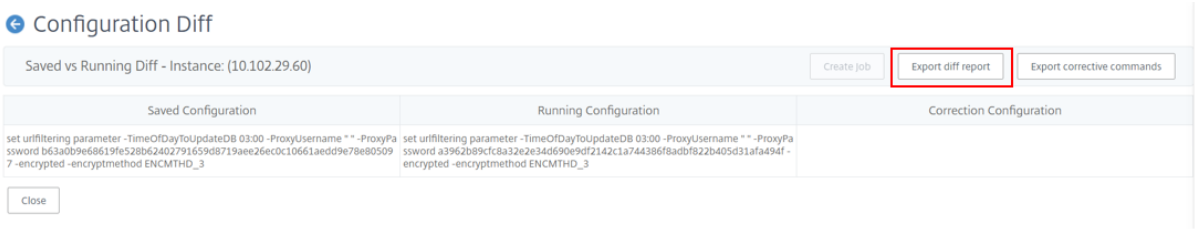


Dans l'image, vous pouvez voir que pour certains cas, un diff est présent uniquement dans **Sauvegardé vs Running Diff** et pour certains cas, un diff est présent uniquement dans **Template vs Running Diff**. Dans certains cas, des différences existent à la fois entre **Saved et Running Diff** et entre **Template et Running Diff .**

Sauvegardé vs Exécution Diff

Vous pouvez afficher un rapport de diff entre la configuration enregistrée sur l'instance et la configuration en cours d'exécution sur cette instance. Par exemple, cliquez sur **Diff Exists** pour une instance sous **Saved vs Running Diff.**

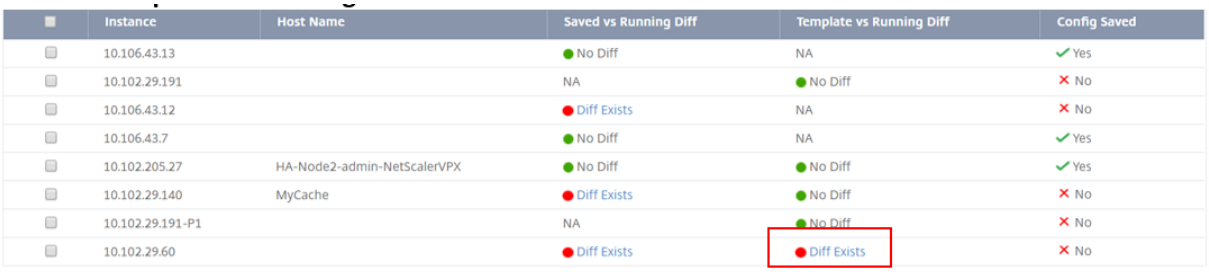
Ici, vous pouvez voir un rapport pour la configuration enregistrée par rapport à l'exécution de diff de configuration pour cette instance.



Cliquez sur **Exporter le rapport diff** pour télécharger un fichier .csv du rapport diff. Vous pouvez également cliquer sur Exporter les commandes correctives pour exporter les commandes dans un fichier .txt. Vous pouvez ensuite exécuter les commandes sur l'instance Citrix ADM associée à partir des tâches de configuration pour corriger la configuration dans cette instance.

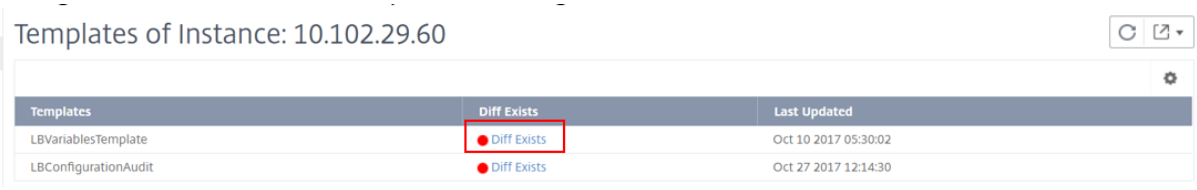
Modèle vs Courir Diff

Le **modèle vs Running Diff** inclut tous les modèles autres que **Sauvegardé vs Running Diff**, qui est le modèle par défaut. Vous pouvez afficher la différence qui existe entre le modèle et la configuration en cours d'exécution.Par exemple, cliquez sur **Diff Exists** pour l'une des instances sous **Modèle vs Running Diff.**



Instance	Host Name	Saved vs Running Diff	Template vs Running Diff	Config Saved
10.106.43.13		No Diff	NA	Yes
10.102.29.191		NA	No Diff	No
10.106.43.12		Diff Exists	NA	No
10.106.43.7		No Diff	NA	Yes
10.102.205.27	HA-Node2-admin-NetScalerVPX	No Diff	No Diff	Yes
10.102.29.140	MyCache	Diff Exists	No Diff	No
10.102.29.191-P1		NA	No Diff	No
10.102.29.60		Diff Exists	Diff Exists	No

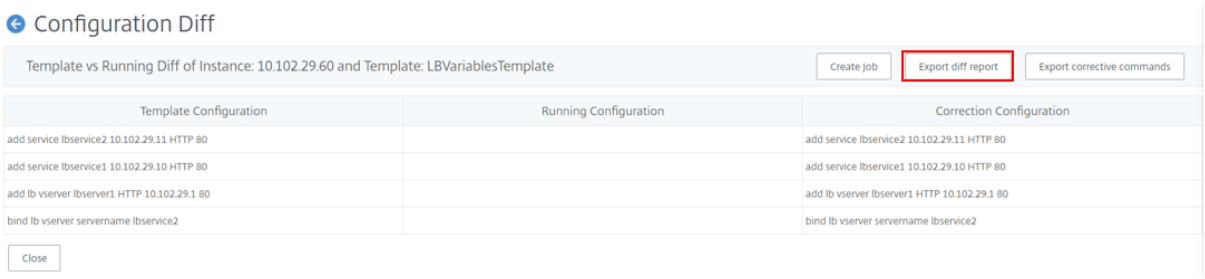
Maintenant, vous pouvez voir que deux modèles affichent diff et que l'instance Citrix ADM a une configuration différente de celle que le modèle recherche.



Templates of Instance: 10.102.29.60

Templates	Diff Exists	Last Updated
LBVariablesTemplate	Diff Exists	Oct 10 2017 05:30:02
LBConfigurationAudit	Diff Exists	Oct 27 2017 12:14:30

Cliquez à nouveau sur**Diff Exists**. L'image suivante montre la configuration recherchée par le modèle et la configuration en cours d'exécution vide, car aucune commande de ce type n'a été configurée ou n'a été supprimée. Vous pouvez également voir les configurations de correction ou les commandes à exécuter pour corriger la configuration.



Configuration Diff

Template vs Running Diff of Instance: 10.102.29.60 and Template: LBVariablesTemplate

Create Job | Export diff report | Export corrective commands

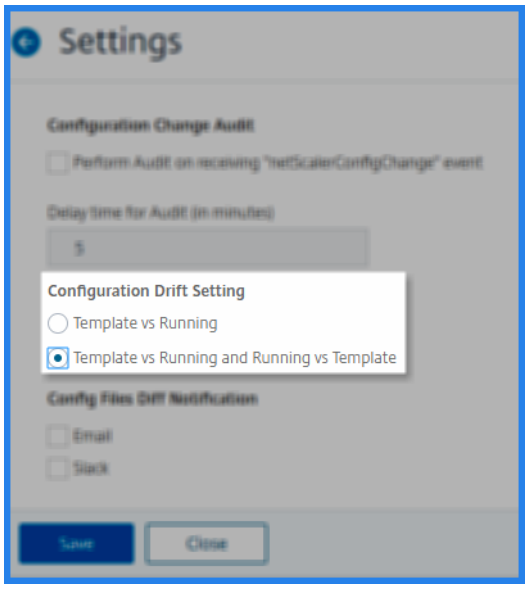
Template Configuration	Running Configuration	Correction Configuration
add service lbservice2 10.102.29.11 HTTP 80		add service lbservice2 10.102.29.11 HTTP 80
add service lbservice1 10.102.29.10 HTTP 80		add service lbservice1 10.102.29.10 HTTP 80
add lb vserver lbserver1 HTTP 10.102.29.1 80		add lb vserver lbserver1 HTTP 10.102.29.1 80
bind lb vserver servername lbservice2		bind lb vserver servername lbservice2

Close

Vous pouvez également utiliser le paramètre de dérive Template vs Running et Running vs template, pour comparer la configuration des deux façons :

- Compare la configuration du modèle d'audit avec la configuration en cours d'exécution sur l'instance.
- Compare la configuration en cours d'exécution sur l'instance avec le modèle d'audit.

Par défaut, le paramètre Template vs. running drift est sélectionné. Pour modifier le paramètre de dérive, dans l'interface graphique d'ADM, sélectionnez **Paramètres** dans la page **Vérification de la configuration**.



Cliquez sur **Exporter le rapport diff** pour télécharger un fichier .csv du rapport diff. Vous pouvez également cliquer sur **Exporter les commandes correctives** pour exporter les commandes dans un fichier .txt. Vous pouvez ensuite exécuter les commandes dans l'interface de ligne de commande pour corriger la configuration dans cette instance.

L'image suivante montre un exemple de fichier diff .csv téléchargé sur votre système :

#Template vs Running Diff of Instance: 10.102.29.60 and Template: LBVariablesTemplate		
Template Configuration	Running Configuration	Correction Configuration
add service lbservice2 10.102.29.11 HTTP 80		add service lbservice2 10.102.29.11 HTTP 80
add service lbservice1 10.102.29.10 HTTP 80		add service lbservice1 10.102.29.10 HTTP 80
add lb vserver lbserver1 HTTP 10.102.29.1 80		add lb vserver lbserver1 HTTP 10.102.29.1 80
bind lb vserver servername lbservice2		bind lb vserver servername lbservice2

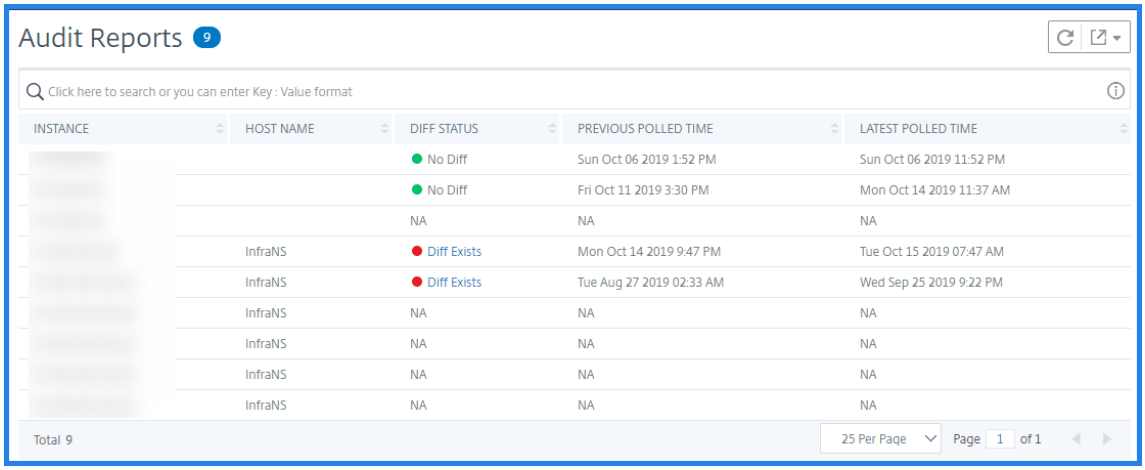
Afficher les rapports d'audit de l'état des fichiers

À l'aide du graphique **Citrix ADC File Status**, vous pouvez vérifier si des fichiers sont ajoutés, modifiés ou supprimés dans le `nsconfig` dossier. Par exemple : si le fichier de licence est mis à jour sur une instance ADC, vous pouvez vérifier la date de la dernière mise à jour de ce fichier et prendre les mesures appropriées.

Pour exporter les rapports d'audit d'état des fichiers pour les instances de Citrix ADC :

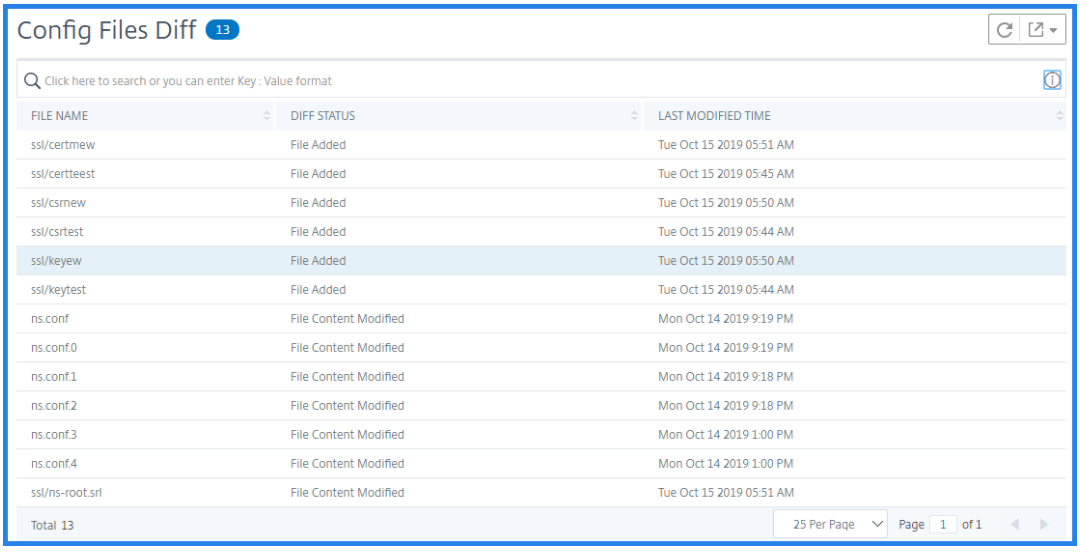
1. Dans Citrix ADM, accédez à **Réseaux** > **Audit de configuration**.
2. Dans la page **Audit de configuration**, cliquez dans le graphique **État du fichier Citrix ADC** .

   La page **Rapports d'audit** répertorie les instances ayant le statut Diff.



Le **statut de différence** est calculé pour l'intervalle entre l'**heure interrogée précédente** et la **dernière heure interrogée**. Le **statut de différence** peut être l'un des suivants :

- **Diff existe** - Cet état indique que les fichiers ont changé dans le dossier `nsconfig` d'une instance depuis l'**heure d'interrogation précédente**. Pour afficher ce qui a changé sur le fichier, cliquez sur **Diff Exists**.



- **No Diff** - Cet état indique que les fichiers du dossier `nsconfig` n'ont pas changé depuis l'heure d'interrogation précédente.
- **NA** - Ce statut indique que la surveillance de l'état du fichier n'est pas applicable. Ce statut apparaît lorsque Citrix ADM n'interroge pas l'instance. Par exemple, lorsqu'une instance est ajoutée récemment ou que l'état de l'instance est inactif, l'interrogation de l'instance

ne se produit pas.

Modifications de configuration d'audit entre les instances

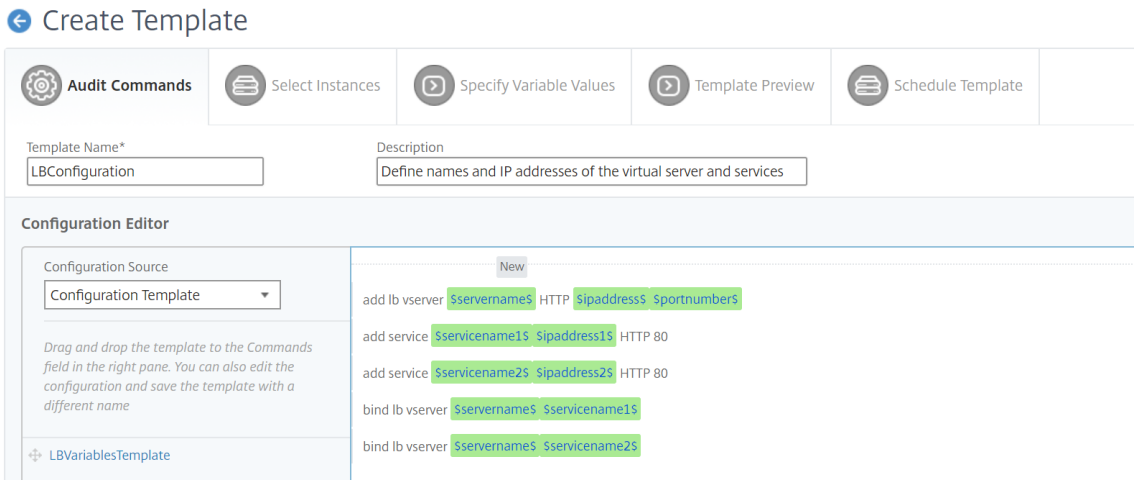
February 1, 2024

Vous voulez vous assurer que certaines configurations s'exécutent sur des instances spécifiques pour des performances optimales de votre réseau. Vous souhaitez également surveiller les modifications de configuration sur les instances de Citrix Application Delivery Controller (ADC) gérées, résoudre les erreurs de configuration et restaurer les configurations non enregistrées après un arrêt soudain du système. Vous pouvez créer des modèles d'audit avec des configurations spécifiques que vous souhaitez exécuter sur certaines instances. Citrix Application Delivery Management (Citrix ADM) compare ces instances avec le modèle d'audit et signale en cas de non-concordance dans la configuration. Cela vous permet de dépanner et de corriger les erreurs.

Vous pouvez automatiser l'exécution du modèle d'audit en planifiant l'heure à laquelle le modèle doit s'exécuter. Vous pouvez également définir la fréquence à laquelle Citrix ADM doit exécuter le modèle. Vous pouvez exécuter le modèle tous les jours, un jour spécifique d'une semaine ou à une date spécifique d'un mois. Vous avez également la possibilité d'envoyer le rapport diff généré par Citrix ADM aux adresses e-mail spécifiées que vous pouvez configurer. Par cette option, votre utilisateur reçoit le rapport en tant que pièce jointe et il n'est pas nécessaire que l'utilisateur se connecte à Citrix ADM pour vérifier manuellement les rapports.

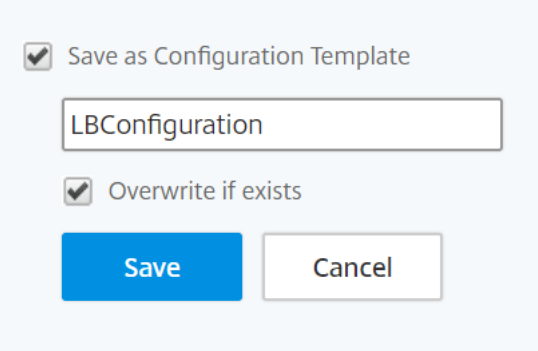
Pour créer des modèles d'audit :

1. Accédez à**Réseaux > Audit de configuration > Modèles d'audit**, puis cliquez sur**Ajouter**.
2. Dans la page**Créer un modèle**et dans l'onglet**Commandes d'audit**, spécifiez le nom du modèle et sa description.
3. Dans l'**Éditeur de configuration**, tapez vos commandes et enregistrez les commandes en tant que modèle de configuration. Vous pouvez également faire glisser un modèle existant à partir du volet gauche de l'éditeur.
4. Sélectionnez les valeurs que vous souhaitez convertir en variable, puis cliquez sur **Convertir en variable**. Par exemple, sélectionnez l'adresse IP du serveur d'équilibrage de charge `ipaddress`, puis cliquez sur**Convertir en variable**comme indiqué dans l'image ci-dessous.

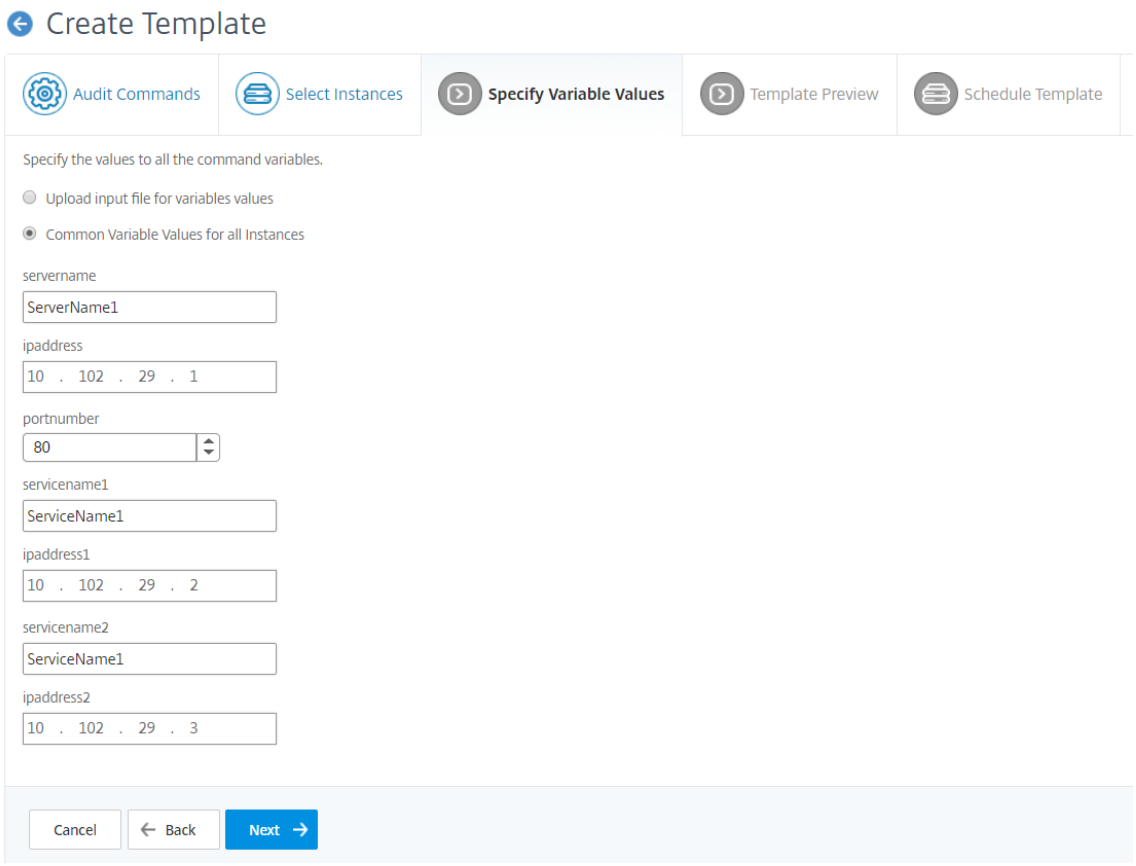


Cliquez sur l'option**Avancé** si vous souhaitez spécifier une valeur par défaut pour votre variable.

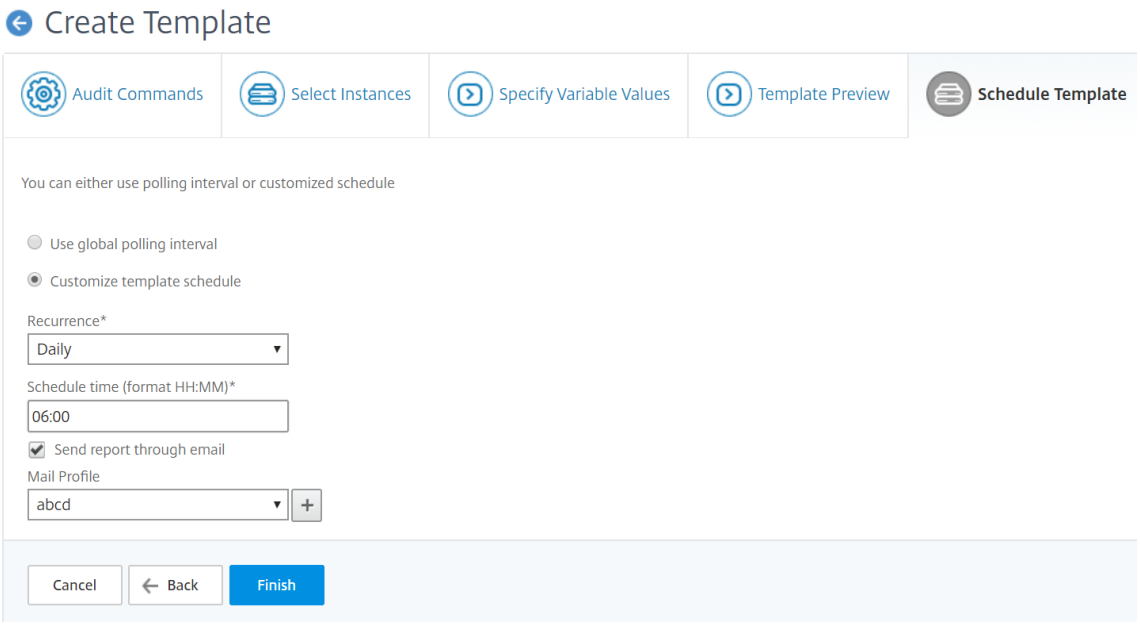
Vous pouvez également enregistrer les commandes en tant que modèle de configuration.



5. Cliquez sur **Enregistrer**, puis sur **Suivant**.
6. Dans l'onglet **Select Instances**, sélectionnez les instances sur lesquelles vous souhaitez exécuter l'audit de configuration.
7. Dans l'onglet **Spécifier les valeurs variables**, vous disposez de deux options :
   a) Téléchargez le fichier d'entrée pour entrer les valeurs des variables que vous avez définies dans vos commandes, puis téléchargez le fichier sur le serveur Citrix ADM
   b) Entrez des valeurs communes pour les variables que vous avez définies pour toutes les instances
8. Cliquez sur **Suivant**.



9. Dans l'onglet **Aperçu du modèle**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances. Cliquez sur **Suivant**.
10. Dans l'onglet **Modèle de calendrier**, vous disposez de trois options pour automatiser l'exécution du modèle et l'adresse e-mail pour envoyer le rapport de comparaison.
    - **Utilisez l'intervalle d'interrogation global**. Sélectionnez cette option pour exécuter le modèle sur les instances à un moment configuré globalement sur Citrix ADM
    - **Personnaliser la planification du modèle**. Utilisez cette option pour configurer l'heure et la fréquence auxquelles les modèles doivent être exécutés
    - **Envoyer un rapport par courrier électronique**. Utilisez cette option pour configurer le profil de messagerie auquel le rapport diff doit être envoyé en tant que pièce jointe.
11. Cliquez sur **Terminer**.

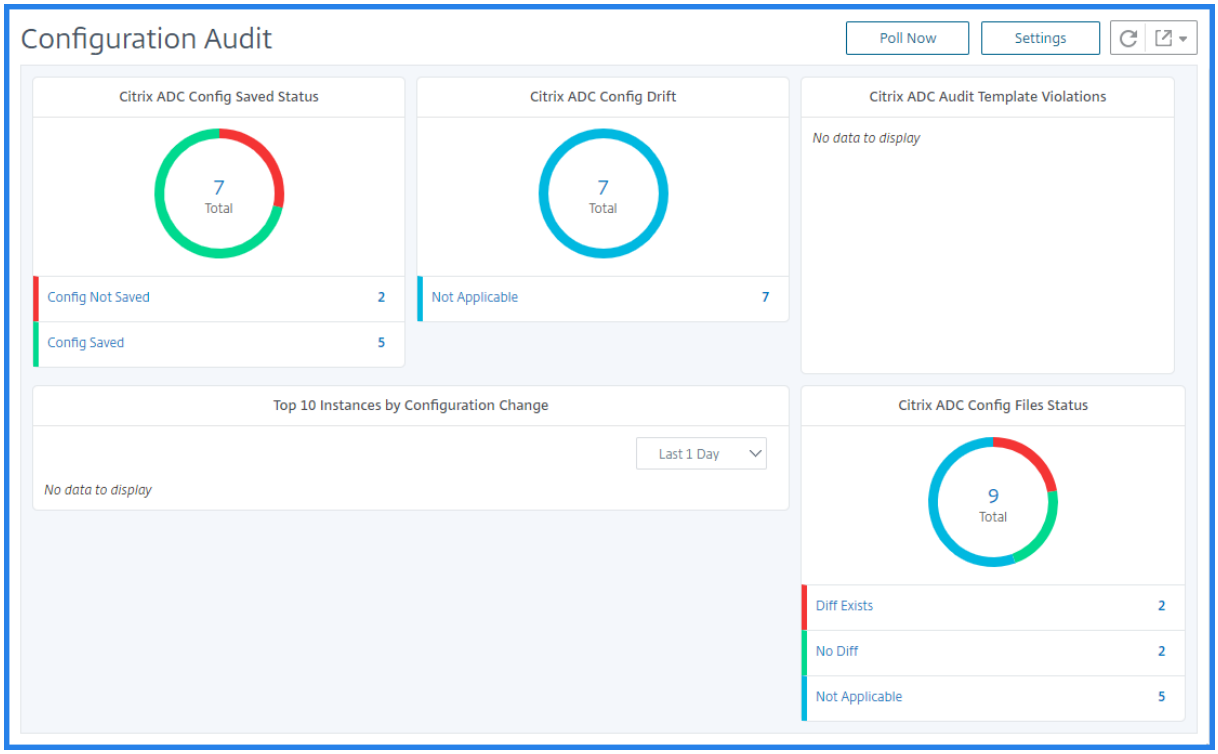


Le modèle d'audit apparaît dans la liste Modèles d'audit et est exécuté à l'heure planifiée par rapport aux configurations dans les instances spécifiées.

Afficher les détails des modifications de configuration

Vous pouvez également utiliser le tableau de bord Vérification de la configuration pour afficher des détails de haut niveau sur les modifications de configuration telles que :

- Les dix principales instances par changement de configuration
- Nombre de configurations enregistrées et non enregistrées
- Le fichier ajouté, supprimé ou modifié dans le `nsconfig` dossier

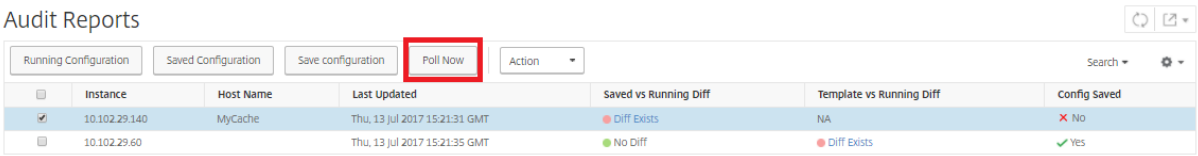


Citrix ADM vous permet également d'interroger manuellement les audits de configuration et ajoute immédiatement tous les audits de configuration des instances à Citrix ADM. Pour ce faire, accédez à **Réseaux**>**Vérification de la configuration,** cliquez sur **Interroger maintenant,** la page contextuelle **Interroger maintenant** vous permet d'interroger toutes les instances Citrix ADC du réseau ou d'interroger les instances sélectionnées.

Vous pouvez également forcer un audit sur une instance. Pour ce faire, cliquez sur l'un des graphiques suivants :

- **État enregistré de la configuration Citrix ADC Config**
- **Dérive de configuration Citrix ADC**

Sur la page **Rapports d'audit**, sélectionnez l'instance et, dans la liste **Action**, sélectionnez **Interroger maintenant** .



Le graphique **État du fichier de configuration Citrix ADC** vous indique l'état des fichiers Citrix ADC présents dans le `nsconfig` dossier. Citrix ADM enregistre et compare les modifications apportées aux fichiers dans le dossier `nsconfig` et affiche les différences. Reportez-vous à la section Afficher les rapports d'audit du statut des fichiers

Définir les notifications d'audit de configuration

1. Accédez à **Réseaux** > **Audit de configuration**.
2. Dans la page **Audit de configuration**, cliquez sur **Paramètres** .
3. Sur la page **Paramètres de notification**, cliquez sur l'icône **Modifier** pour activer les paramètres de notification.
4. Cochez la case **Activé**, puis choisissez une liste de distribution d'e-mails dans la liste déroulante. Vous pouvez également créer une liste de distribution d'e-mails en cliquant sur l'icône **+** et en spécifiant les détails du serveur de messagerie.

Obtenir des conseils de configuration sur la configuration du réseau

February 1, 2024

Vous configurez vos instances de Citrix Application Delivery Controller (ADC) avec des configurations optimales afin d'obtenir des performances optimales sur vos applications. Toutefois, certaines configurations peuvent ne pas être des configurations standard, ce qui peut affecter les performances de vos applications.

Pour vous aider à optimiser les performances de votre application, Citrix Application Delivery Management (Citrix ADM) analyse la configuration de l'instance Citrix ADC et vous fournit des recommandations. Vous pouvez appliquer les configurations recommandées à partir de Citrix ADM.

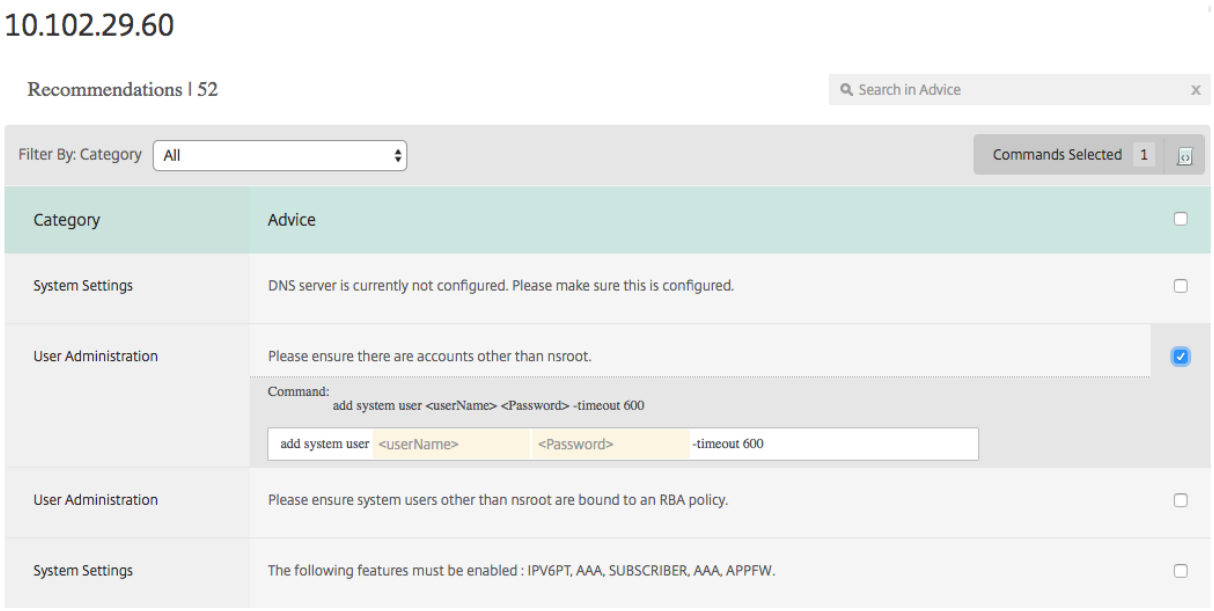
Pour analyser l'instance de Citrix ADC :

1. Accédez à **Réseaux** > **Audit deconfiguration > Conseil de configuration** .
2. Procédez comme suit :

   - Cliquez sur **Charger le fichier de configuration** et téléchargez le fichier de configuration de votre instance réseau.

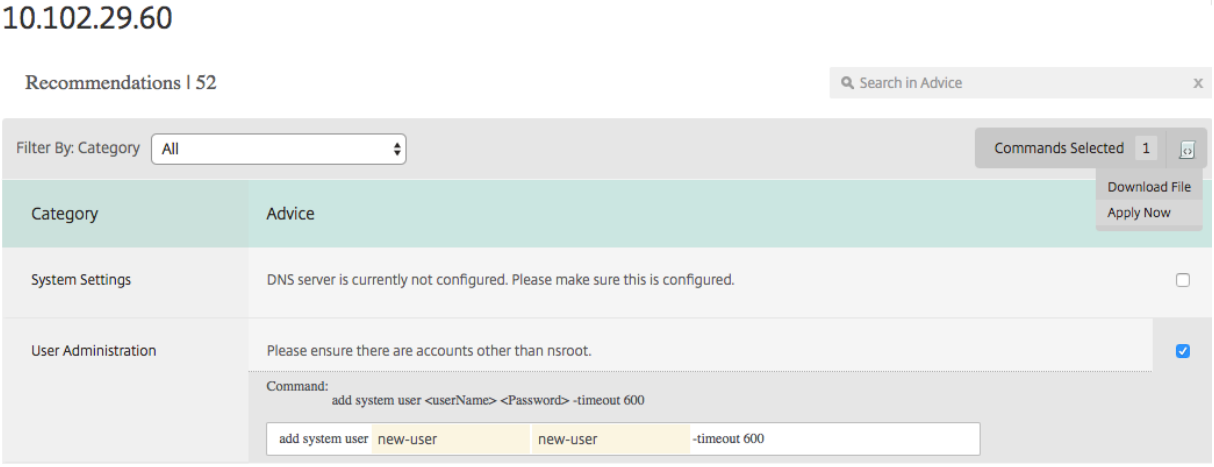
   - Cliquez sur **Sélectionner un périphérique** et sélectionnez l'instance Citrix ADC que vous souhaitez analyser.

Citrix ADM analyse la configuration de votre instance et fournit une liste de recommandations de configuration, comme indiqué dans l'image suivante. Cochez la case située en regard d'un conseil de configuration pour afficher les commandes correctives.

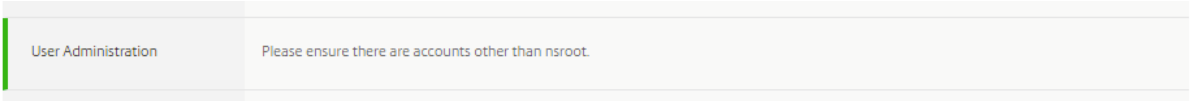


Si vous souhaitez mettre à jour votre configuration, spécifiez les valeurs des variables dans les commandes correctives et cliquez sur **Appliquer maintenant** comme indiqué dans l'image suivante.

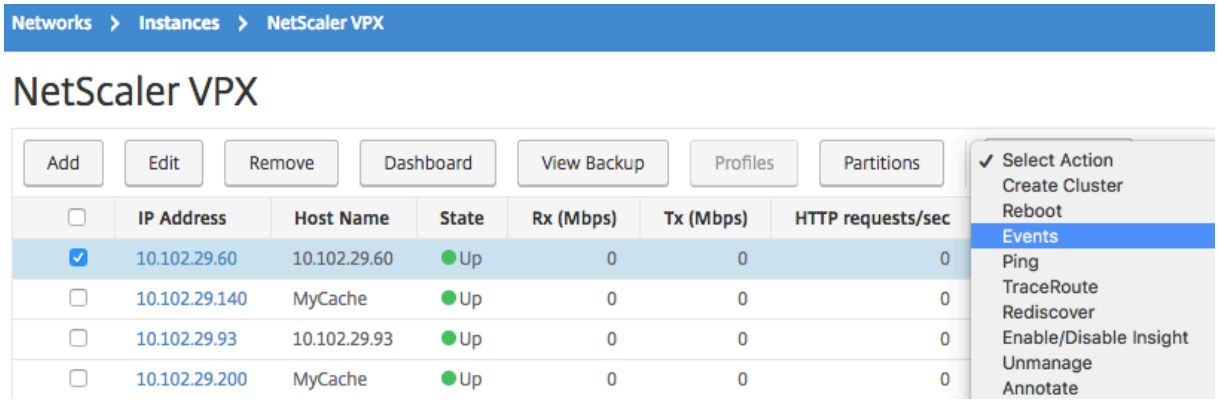
> **Remarque**
>
> Les commandes répertoriées ici ne sont que des recommandations. Un utilisateur disposant d'un accès en lecture et en écriture peut modifier n'importe quelle commande à l'aide de cette fonctionnalité. Assurez-vous d'accorder un accès privilégié limité aux utilisateurs qui, selon vous, ne doivent pas modifier les commandes.



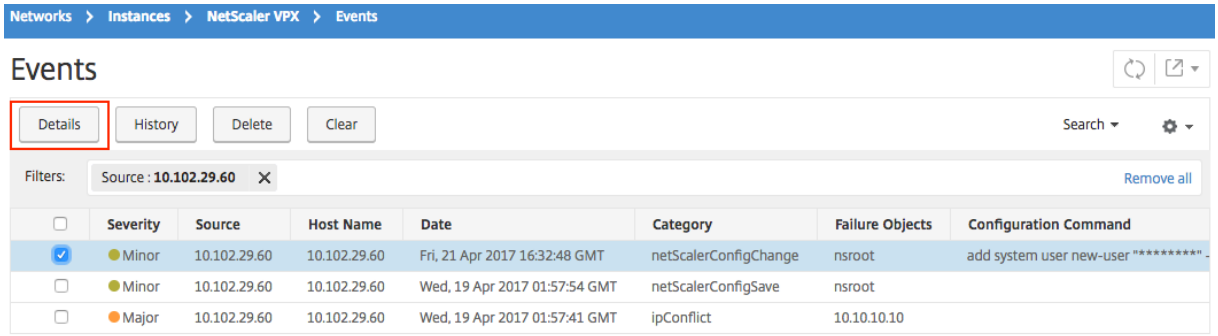
Lorsque la commande est exécutée avec succès sur l'instance réseau, la case à cocher en regard de l'avis disparaît.



Si vous souhaitez afficher les détails des commandes exécutées sur votre instance réseau, accédez à **Réseaux > Instances > <Instance_Type\>**, sélectionnez l'adresse IP de l'instance, puis cliquez sur **Événements** dans la liste déroulante **Actions** .



Sur la page **Événements**, vous pouvez afficher les détails de la modification de configuration.



Audit de configuration d'interrogation des instances Citrix ADC

February 1, 2024

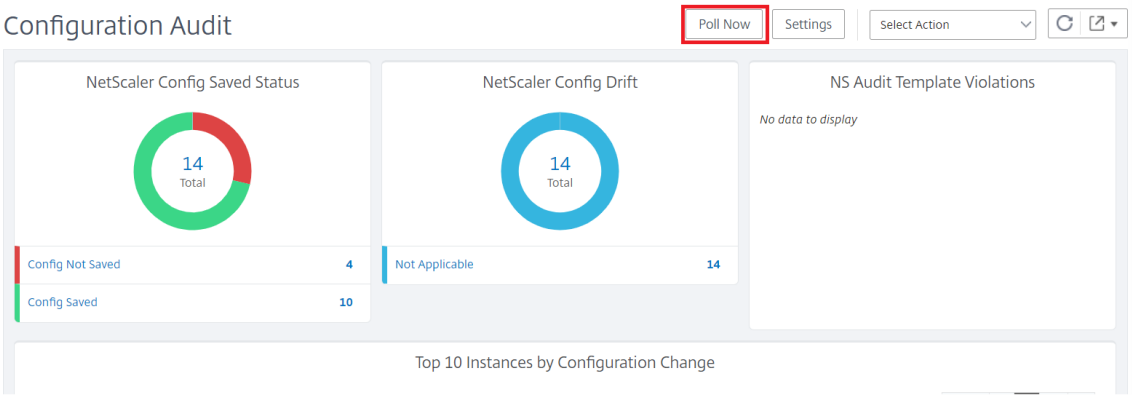
Citrix Application Delivery Management (Citrix ADM) interroge automatiquement les audits de configuration toutes les 10 heures pour rechercher les modifications de configuration qui se produisent sur les instances de Citrix Application Delivery Controller (ADC). Vous pouvez également interroger manuellement les audits de configuration pour découvrir les modifications récentes, mais l'interrogation de toutes les instances de Citrix ADC entraîne une lourde charge sur le réseau.

Au lieu d'interroger l'ensemble de l'audit de configuration des instances Citrix ADC, vous pouvez interroger manuellement uniquement les audits de configuration d'une ou plusieurs instances sélectionnées.

Pour interroger les audits de configuration des instances Citrix ADC :

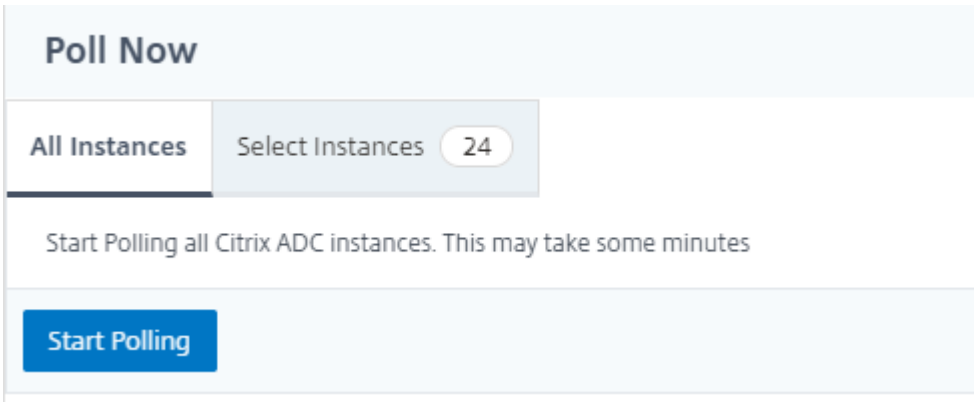
1. Dans Citrix ADM, accédez à **Réseaux** > **Audit de configuration**.

2. Dans la page **Audit de configuration**, dans le coin supérieur droit, cliquez sur **Sondage maintenant** .



3. La page **Interroger maintenant** apparaît, vous donnant la possibilité d'interroger toutes les instances Citrix ADC dans le réseau ou d'interroger les instances sélectionnées.

   a) Pour interroger toutes les instances Citrix ADC, sélectionnez l'onglet **Toutes les instances** et cliquez sur **Démarrer l'interrogation**.



   b) Pour interroger des instances spécifiques, sélectionnez l'onglet **Sélectionner**des**instances**, sélectionnez les instances dans la liste, puis cliquez sur**Interroger maintenant**.

Générer un diff d'audit de configuration pour les interruptions SNMP ConfigChange

February 1, 2024

Chaque fois qu'il y a une modification de configuration dans une instance de Citrix Application Delivery Controller (ADC) dans le réseau, le fichier de configuration est mis à jour. L'instance envoie une interruption SNMP ConfigChange à Citrix Application Delivery Management (Citrix ADM). Vous pouvez activer Citrix ADM pour effectuer un audit de configuration sur cette instance lorsque l'instance envoie une interruption SNMP ConfigChange.

S'il existe une différence entre la configuration du modèle d'audit et la configuration en cours d'exécution, un message d'état Différent existe apparaît sur la page Rapport d'audit . En cliquant sur le lien Diff Exist, vous accédez à la page Configuration Diff, où vous pouvez afficher la commande corrective. Vous pouvez utiliser ces commandes correctives pour créer un travail de configuration et l'exécuter sur les instances Citrix ADC spécifiques. Lorsque vous exécutez le travail de configuration, les instances sont ramenées à la configuration souhaitée. Pour plus d'informations sur la façon de créer un travail de configuration à partir de commandes correctives, consultez Comment créer des travaux de configuration à partir de commandes correctives sur Citrix ADM.

Pour exécuter des modèles d'audit de configuration lors de la réception de l'interruption SNMP ConfigChange :

Citrix ADM vous permet d'activer l'option permettant d'exécuter le modèle d'audit de configuration dans Citrix ADM.

1. Dans Citrix ADM, accédez à **Réseaux** > **Audit de configuration**.
2. Cliquez sur**Paramètres** dans la page **Vérification de la configuration**.
3. Cliquez sur l'icône de modification dans la section **Paramètres d'audit des modifications de configuration**.
4. Cochez la case **Effectuer un audit de configuration lors de la réception de l'événement NetScalerConfigChange** .

> **Remarque**
>
> Il s'agit d'un paramètre global pour toutes les instances. Citrix ADM effectue un audit de configuration pour chaque instance sur laquelle il recevra les interruptions SNMP NetScalerConfigChange à l'avenir.

1. Dans le champ **Délai d'exécution du modèle d'audit** (en minutes), saisissez les minutes. Citrix ADM exécute le modèle d'audit de configuration sur l'instance de Citrix ADC après ce délai lorsqu'il reçoit l'interruption SNMP ConfigChange par cette instance.

Fonctions réseau

February 1, 2024

À l'aide de la fonctionnalité Network Functions, vous pouvez surveiller l'état des entités configurées sur vos instances Citrix Application Delivery Controller (ADC) gérées. Vous pouvez afficher des statistiques telles que les détails de transaction, les détails de connexion et le débit d'un serveur virtuel d'équilibrage de charge. Vous pouvez également activer ou désactiver les entités lorsque vous planifiez une maintenance.

Le tableau de bord Network Functions fournit les graphiques suivants :

- Les 5 meilleurs serveurs virtuels avec le plus grand nombre de connexions client
- Les 5 meilleurs serveurs virtuels avec le plus grand nombre de connexions
- Les 5 meilleurs serveurs virtuels avec un débit maximal (Mo/sec)
- Les 5 derniers serveurs virtuels présentant le débit le plus faible (Mo/sec)
- Les 5 meilleures instances avec la plupart des serveurs virtuels
- État des serveurs virtuels
- État de santé des serveurs virtuels d'équilibrage de charge
- Protocoles

Générer des rapports pour les entités d'équilibrage de charge

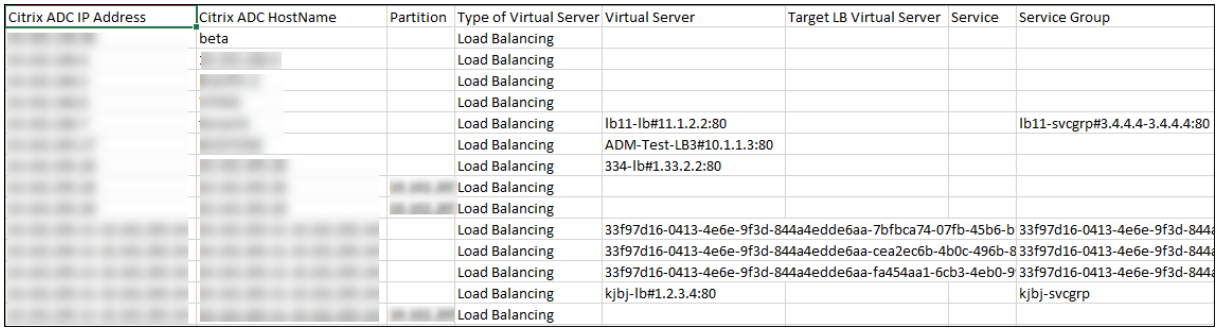
February 1, 2024

Citrix Application Delivery Management (ADM) vous permet de consulter les rapports des entités d'instance Citrix Application Delivery Controller (ADC) à tous les niveaux. Il existe deux types de rapports que vous pouvez télécharger dans Citrix ADM > Network Functions : les rapports consolidés et les rapports individuels.

Rapports consolidés : vous pouvez télécharger et consulter un rapport consolidé ou résumé pour toutes les entités gérées sur des instances Citrix ADC.

Ce rapport vous permet d'avoir une vue de haut niveau du mappage entre les instances Citrix ADC, les partitions et les entités d'équilibrage de charge correspondantes (serveurs virtuels, groupes de services et services) présentes sur le réseau.

L'image suivante montre un exemple de rapport récapitulatif.



Citrix ADC IP Address	Citrix ADC HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
	beta		Load Balancing				
			Load Balancing				
			Load Balancing				
			Load Balancing				
			Load Balancing	lb11-lb#11.1.2.2:80			lb11-svcgrp#3.4.4.4-3.4.4.4:80
			Load Balancing	ADM-Test-LB3#10.1.1.3:80			
			Load Balancing	334-lb#1.33.2.2:80			
			Load Balancing				
			Load Balancing				
			Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-7bfbca74-07fb-45b6-b			33f97d16-0413-4e6e-9f3d-844
			Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-cea2ec6b-4b0c-496b-8			33f97d16-0413-4e6e-9f3d-844
			Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-fa454aa1-6cb3-4eb0-9			33f97d16-0413-4e6e-9f3d-844
			Load Balancing	kjbj-lb#1.2.3.4:80			kjbj-svcgrp
			Load Balancing				

Le rapport consolidé est au format CSV. Les entrées de chaque colonne sont décrites comme suit :

- **Adresse IP NetScaler : l'adresse IP**de l'instance Citrix ADC est affichée dans le rapport
- Nom d'**hôte NetScaler : le nom**d'hôte est affiché dans le rapport.
- **Partition** : l'adresse IP de la partition administrative est affichée
- **Serveur virtuel** : <name_of_the_virtual_server>#virtual_IP_address :port_number
- **Services** : <name_of_the_service>#service-IP_address:port_number
- **Groupes de services** : <name_of_service_group>#membre_serveur1_adresse_IP:port, adresse_IP_de_serveur2_adresse_IP:port, membre_serveur3_adresse_IP:port,…, Adresse IP du membre du serveur : port

> **Remarque**
>
> - Si aucun nom d'hôte n'est disponible, l'adresse IP correspondante s'affiche.
> - Les colonnes vides indiquent que les entités respectives ne sont pas configurées pour cette instance Citrix ADC.

Rapports individuels : vous pouvez également télécharger et consulter des rapports indépendants de toutes les instances et entités. Par exemple, vous pouvez télécharger un rapport concernant uniquement les serveurs virtuels d'équilibrage de charge, les services d'équilibrage de charge ou les groupes de services d'équilibrage de charge.

Citrix ADM vous permet de télécharger le rapport instantanément. Vous pouvez également planifier la génération du rapport à une heure fixe une fois par jour, une fois par semaine ou une fois par mois.

Générer un rapport d'équilibrage de charge combiné

1. Dans Citrix ADM, accédez à **Réseaux** > **Fonctions réseau** > **Équilibrage de charge.**
2. Sur la page **Équilibrage de charge**,  .
3. Sur la page **Exporter** qui s'ouvre, vous disposez de deux options pour afficher le rapport :

a) Sélectionnez **l'onglet Exporter maintenant** et cliquez sur **OK**.

   Le rapport consolidé est téléchargé sur votre système.

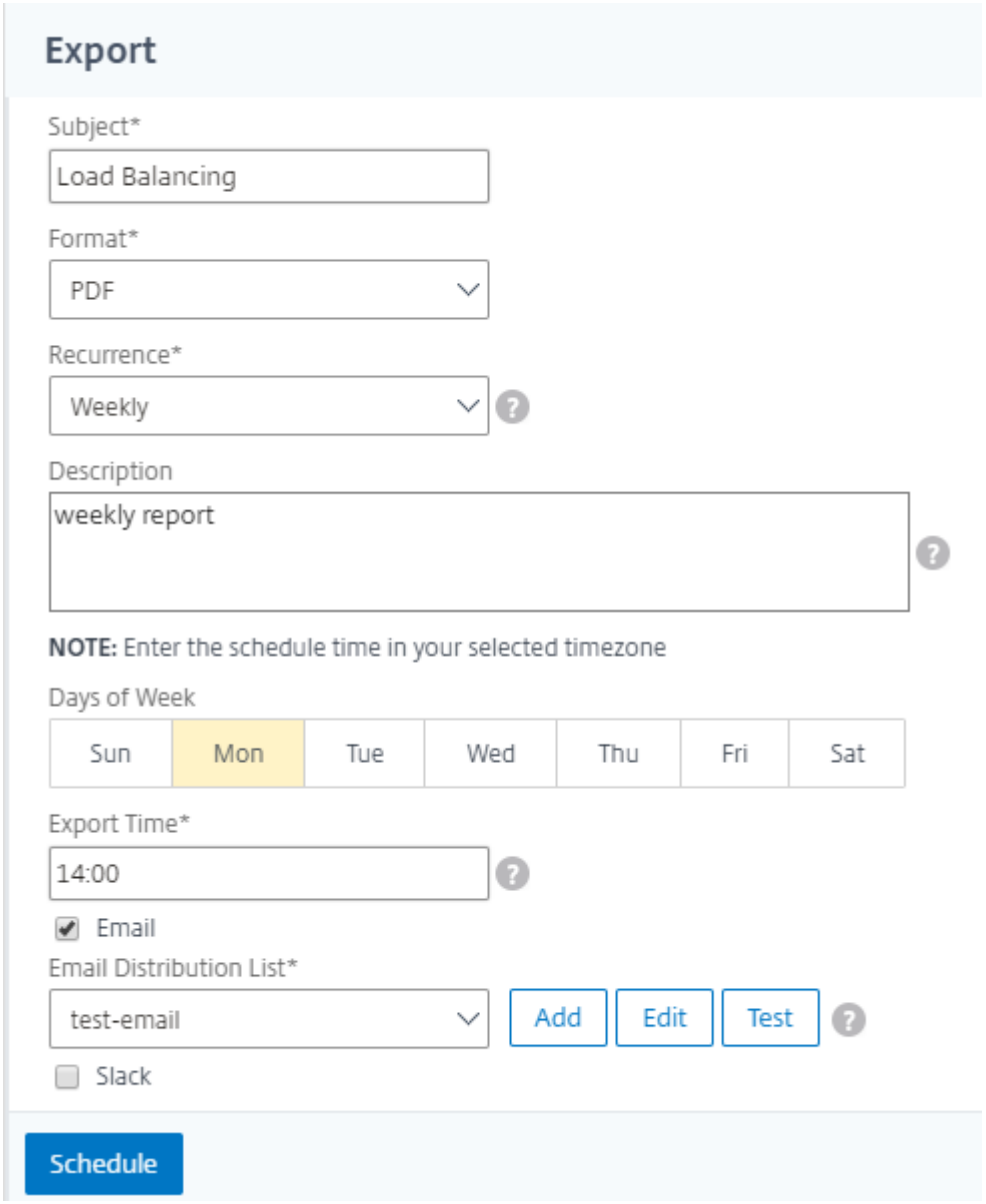
b) Sélectionnez l'onglet **Planifier le rapport** pour planifier la génération et l'exportation du rapport à intervalles réguliers. Spécifiez les paramètres de récurrence de génération de rapport et créez un profil de messagerie vers lequel le rapport est exporté.

   i. **Récurrence** : sélectionnez **Quotidien**, **Hebdomadaire**ou **Mensuel** dans la liste déroulante.

   ii. Durée de**récurrence** : entrez l'heure sous la forme Heure:Minute au format 24 heures.

   iii. **Profil de messagerie** : sélectionnez un profil dans la liste déroulante ou cliquez sur **+** pour créer un profil de messagerie.

> **Remarque**
>
> Si vous sélectionnez Périodicité **hebdomadaire**, veillez à sélectionner les jours de semaine pendant lesquels vous souhaitez que le rapport soit planifié.



Remarque

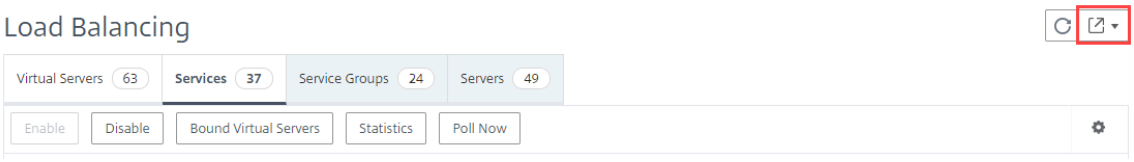
Si vous sélectionnez Récurrence **mensuelle**, assurez-vous de saisir tous les jours où vous souhaitez que le rapport soit planifié, séparés par des virgules.

Générer un rapport d'entité d'équilibrage de charge individuel

Vous pouvez générer et exporter un rapport individuel pour un type particulier d'entité associé aux instances. Par exemple, considérez un scénario dans lequel vous souhaitez afficher une liste de tous les services d'équilibrage de charge du réseau.

1. Dans Citrix ADM, accédez à **Réseaux** > **Fonctions réseau** > **Équilibrage de charge > Services.**

2. Sur la page **Services**, cliquez sur le bouton **Exporter** en haut à droite.



   a) Sélectionnez **l'onglet Exporter maintenant** si vous souhaitez générer et afficher le rapport en ce moment.

   b) Sélectionnez **Planifier l'exportation** pour planifier la génération et l'exportation du rapport à intervalles réguliers.

> **Remarque**
>
> Vous pouvez uniquement télécharger les rapports ou les exporter sous forme de pièces jointes à un courrier électronique. Vous ne pouvez pas afficher les rapports sur l'interface graphique Citrix ADM.

Exporter ou planifier l'exportation des rapports sur les fonctions réseau

February 1, 2024

Vous pouvez générer un rapport complet pour certaines fonctions réseau telles que l'équilibrage de charge, la commutation de contenu, la redirection de cache, l'équilibrage de charge globale du serveur (GSLB), l'authentification et Citrix Gateway dans Citrix Application Delivery Management (ADM). Ce rapport vous permet d'avoir une vue de haut niveau du mappage entre les instances Citrix ADC, les partitions et les entités liées correspondantes (serveurs virtuels, groupes de services et services) présentes dans le réseau. Vous pouvez exporter ces rapports au format .csv.

Le rapport affiche les données de serveur virtuel suivantes :

- Adresse IP NetScaler
- Nom d'hôte
- Données de partition
- Nom du serveur virtuel
- Type de serveur virtuel
- Serveur virtuel
- Serveur virtuel LB cible

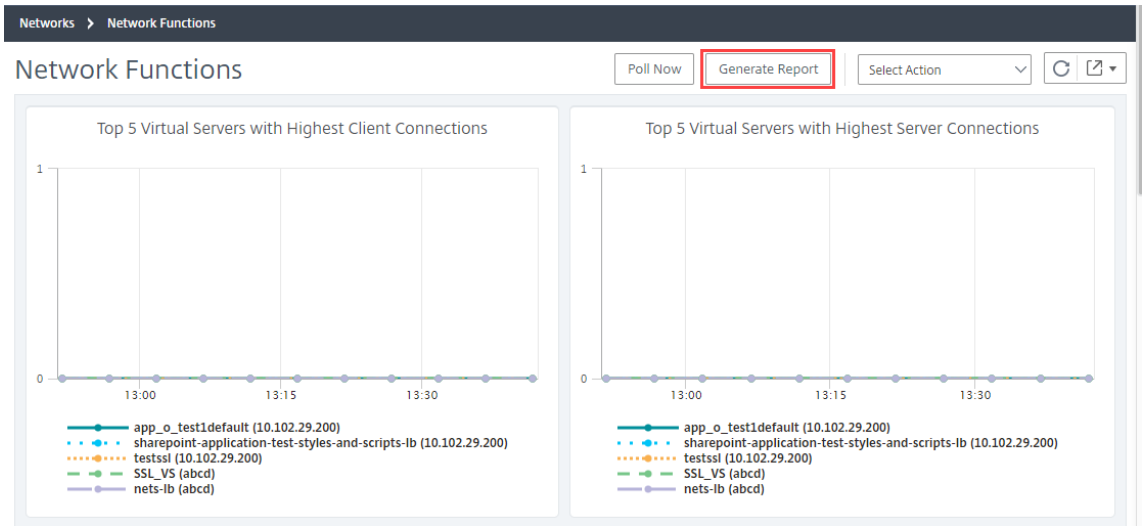
> **Remarque**
>
> Pour les serveurs virtuels de commutation de contenu et de redirection de cache, la colonne Serveur virtuel Target LB répertorie tous les serveurs LB, c'est-à-dire à la fois les serveurs par défaut et les serveurs basés sur des stratégies.
>
> - Nom du service
> - Nom du groupe de services

Vous pouvez planifier l'exportation de ces rapports vers des adresses e-mail spécifiées à des intervalles différents.

> **Remarque**
>
> - Pour les serveurs virtuels GSLB, le rapport des fonctions réseau affiche uniquement les serveurs virtuels GSLB et les services associés.
> - Pour les serveurs virtuels de commutation de contenu et de redirection de cache, le rapport affiche uniquement les liaisons vers les serveurs LB associés.
> - Les serveurs virtuels SSL ne sont pas répertoriés dans ce rapport car une liste distincte de serveurs virtuels SSL n'est pas gérée sur Citrix ADM.
> - Lorsqu'un nouveau rapport est généré, les anciens rapports sont automatiquement supprimés de votre compte.
> - Vous ne pouvez pas générer de rapport sur les fonctions réseau pour HAProxy.

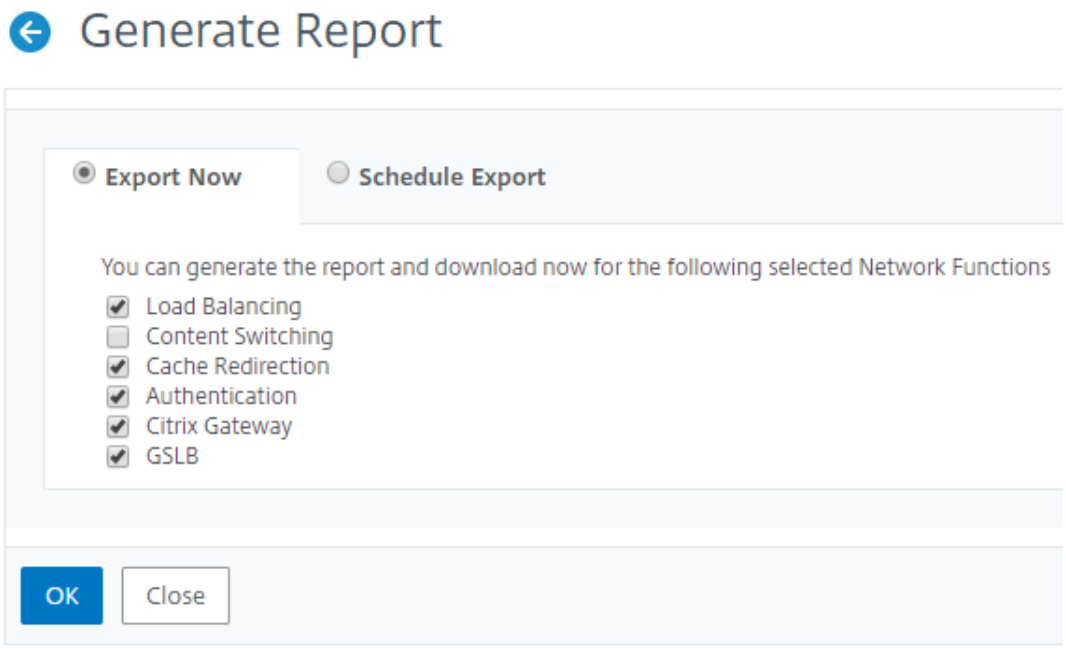
Pour exporter et planifier des rapports sur les fonctions réseau :

1. Accédez à**Réseaux > Fonctions réseau**.
2. Dans la page**Fonctions réseau**, dans le volet droit, cliquez sur**Générer un rapport**dans le coin supérieur droit de la page.



3. Sur la page **Générer un rapport**, vous disposez des 2 options suivantes :

   a) Sélectionnez **l'onglet Exporter maintenant** et cliquez sur **OK**. Le rapport est téléchargé sur votre système.



   L'image suivante montre un exemple de rapport de fonctions réseau.

NetScaler ADC IP Address	NetScaler ADC HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
10.	10.		Load Balancing	lb_test_1#10.10.10.10:80		adm_metric_collector_svc_10.106.171.41#10.106	
10.	10.		Load Balancing	lbvs_511#51.1.1.1:80		test_1#10.102.61.105:80	
10.	10.		Load Balancing	lbvs_521#52.1.1.1:80		test_1#10.102.61.105:80	
10.	10.		Load Balancing	SG_HS_DNS_MON#1.2.22.2:80			sc1
10.	10.		Load Balancing	SG_HS_DNS_MONgdvfffs#1.3.4.5:80			
10.	10.		Load Balancing	atest94#1.1.1.11:80			
10.	10.		Load Balancing	lbvs1_101#1.10.1.1:80			
10.	10.		Load Balancing	lbvs1_1010#1.10.1.10:80			
10.	10.		Load Balancing	lbvs1_10100#1.10.1.100:80			
10.	10.		Load Balancing	lbvs1_10101#1.10.1.101:80			
10.	10.		Load Balancing	lbvs1_10102#1.10.1.102:80			
10.	10.		Load Balancing	lbvs1_10103#1.10.1.103:80			

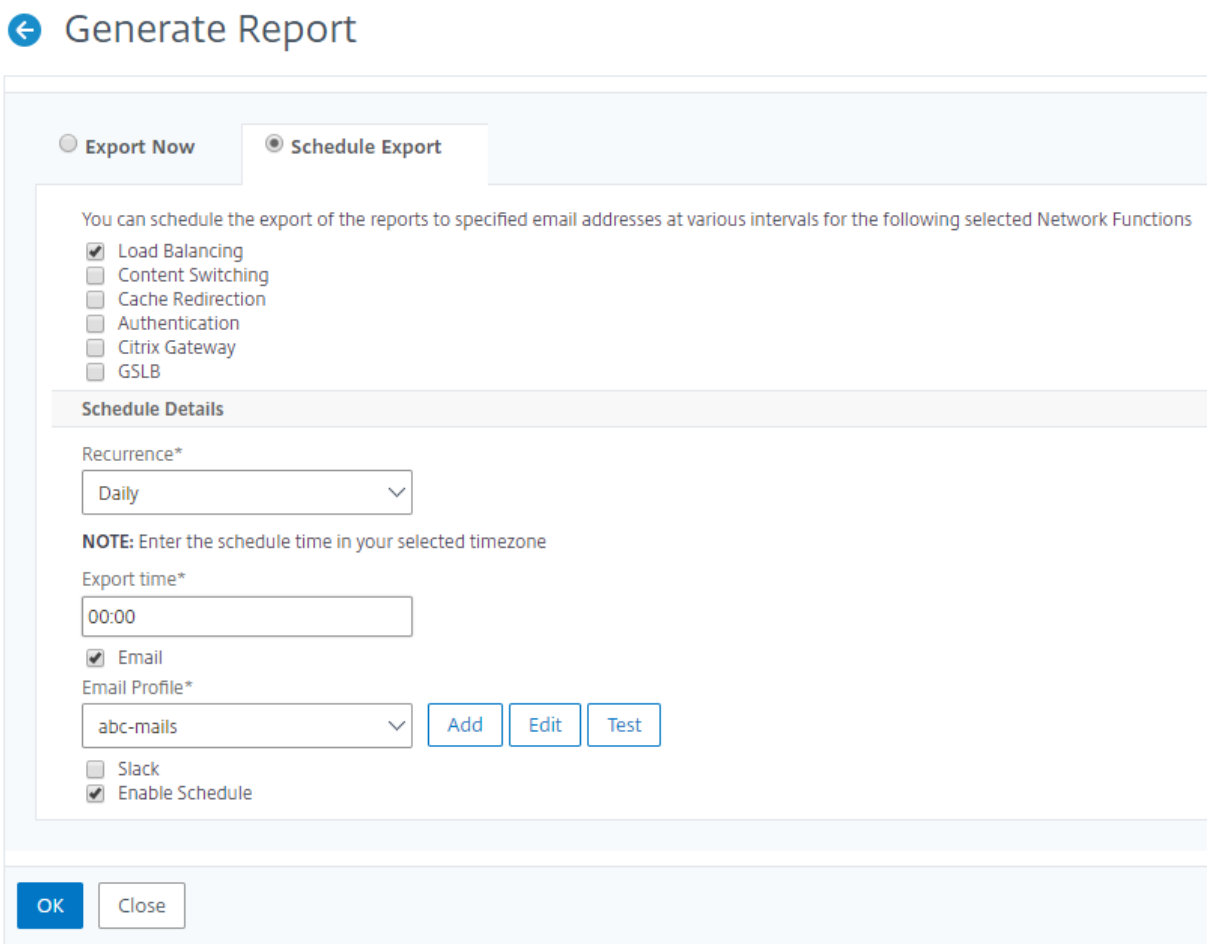
   b) Sélectionnez**l'onglet Planifier le rapport**pour planifier la génération et l'exportation du rapport à intervalles réguliers. Spécifiez les paramètres de récurrence de génération de rapport et créez un profil de messagerie vers lequel le rapport est exporté.

      i. **Récurrence** : sélectionnez**Quotidien**,**Hebdomadaire**ou**Mensuel**dans la zone de liste déroulante.

      ii. **Heure de récurrence**- Entrez l'heure en tant que Heure : Minute au format 24 heures.

      iii. **Profil de messagerie** : sélectionnez un profil dans la liste déroulante ou cliquez sur**+** pour créer un profil de messagerie.

Cliquez sur **Activer la planification pour planifier** votre rapport, puis cliquez sur **OK**. En cochant la case **Activer la planification**, vous pouvez générer les rapports sélectionnés.



Rapports sur le réseau

February 1, 2024

Vous pouvez optimiser l'utilisation des ressources en surveillant les rapports de votre réseau sur Citrix Application Delivery Management (Citrix ADM). Il se peut que vous ayez un déploiement distribué avec de nombreuses applications déployées à plusieurs emplacements. Pour garantir des performances optimales de vos applications, vous avez également déployé plusieurs instances de Citrix Application Delivery Controller (Citrix ADC) pour équilibrer la charge, changer de contenu ou compresser le trafic. Les performances réseau peuvent avoir un impact sur les performances de l'application. Pour continuer à maintenir les performances de vos applications, vous devez surveiller régulièrement les performances de votre réseau et vous assurer que toutes les ressources sont utilisées de manière optimale.

Citrix ADM vous permet désormais de générer des rapports non seulement pour des instances au niveau global, mais aussi pour des entités telles que les serveurs virtuels et les interfaces réseau. La

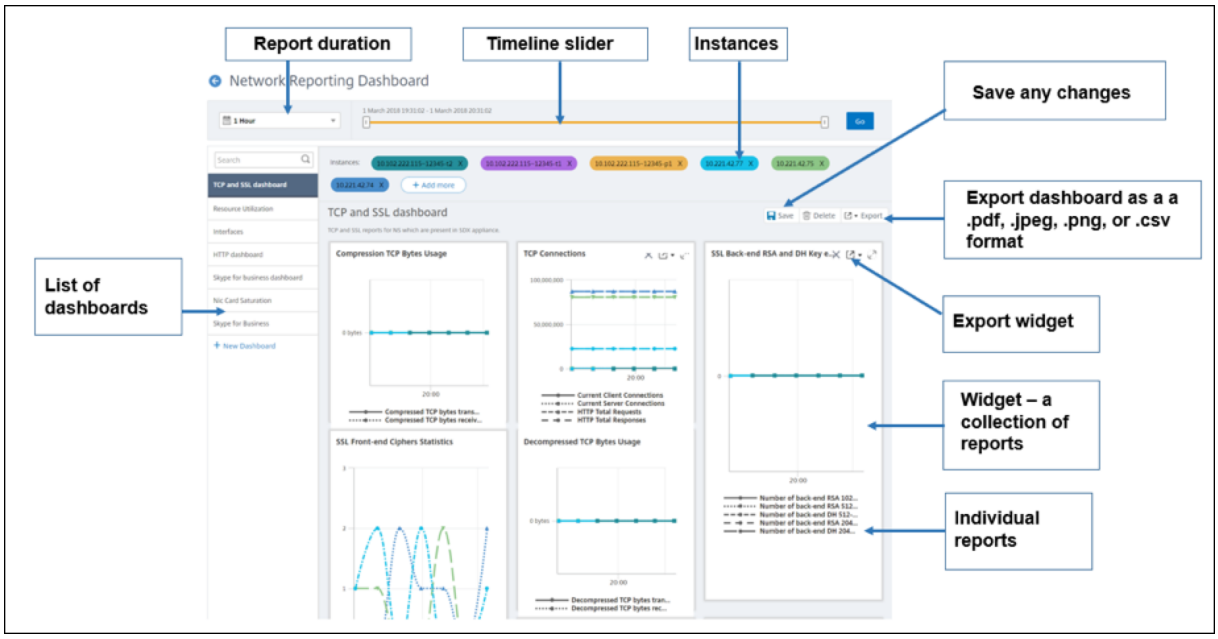
famille d'instances comprend les instances Citrix ADC et SD-WAN. Les serveurs virtuels pour lesquels vous pouvez générer des rapports sont les suivants :

- Serveurs, services et groupes de services d'équilibrage de charge
- Serveurs de commutation de contenu
- Serveurs de redirection du cache
- Équilibrage global de la charge de service (GSLB)
- Authentification
- Citrix Gateway

Le tableau de bord des rapports réseau de Citrix ADM est hautement personnalisable. Vous pouvez désormais créer plusieurs tableaux de bord pour différentes instances, serveurs virtuels et autres entités.

Tableau de bord de rapports réseau

L'image suivante appelle les différentes fonctionnalités du tableau de bord :



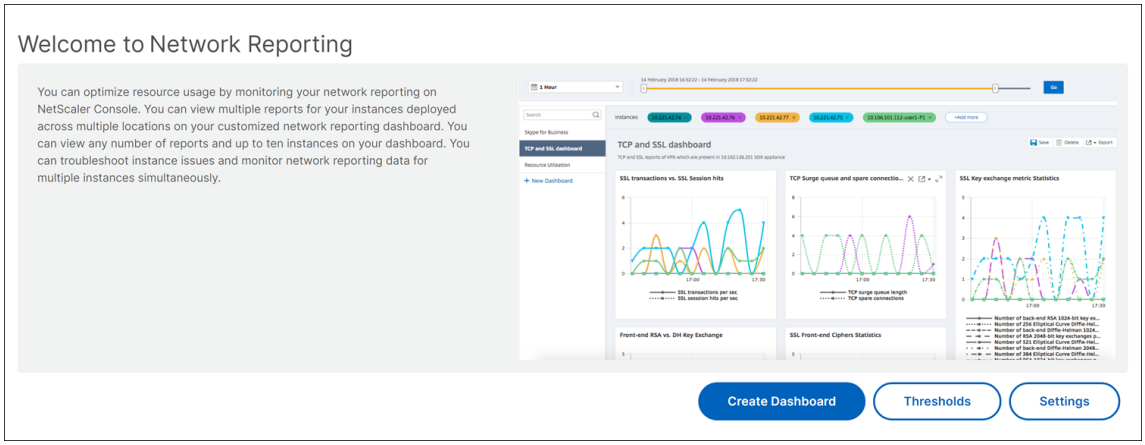
- Le panneau de gauche répertorie tous les tableaux de bord personnalisés créés dans Citrix ADM. Vous pouvez cliquer sur l'un d'eux pour afficher les différents rapports que le tableau de bord est composé. Par exemple, un tableau de bord TCP et SSL contient divers rapports liés aux protocoles TCP et SSL.
- Vous pouvez personnaliser chaque tableau de bord avec plusieurs widgets pour afficher différents rapports. Un widget représente un rapport sur le tableau de bord, c'est-à-dire une collection de rapports plus associés. Par exemple, un rapport d'utilisation des octets TCP compressés contient des rapports sur les octets TCP compressés transférés et reçus par seconde.

- Vous pouvez afficher les rapports pendant une heure, un jour, une semaine ou un mois. En outre, vous pouvez désormais utiliser l'option du curseur de chronologie pour personnaliser la durée des rapports générés sur Citrix ADM.
- Vous pouvez supprimer un rapport en cliquant sur « X ». Vous pouvez également exporter le rapport au format .pdf, .jpeg, .png ou .csv vers votre système. Vous pouvez également planifier l'heure et la récurrence du moment où le rapport doit être généré. Vous pouvez également configurer une liste de distribution de courrier électronique à laquelle les rapports doivent être envoyés.
- La section Instances en haut du tableau de bord répertorie les adresses IP de toutes les instances pour lesquelles le rapport est généré.
- Vous pouvez supprimer des instances en cliquant sur « X » ou ajouter d'autres instances aux rapports. Toutefois, Citrix ADM vous permet actuellement d'afficher des rapports pour 10 instances.
- Vous pouvez également exporter l'intégralité du tableau de bord au format .pdf, .jpeg, .png ou .csv vers votre système. Toutes les modifications apportées au tableau de bord doivent être enregistrées. Cliquez sur Enregistrer pour enregistrer vos modifications.

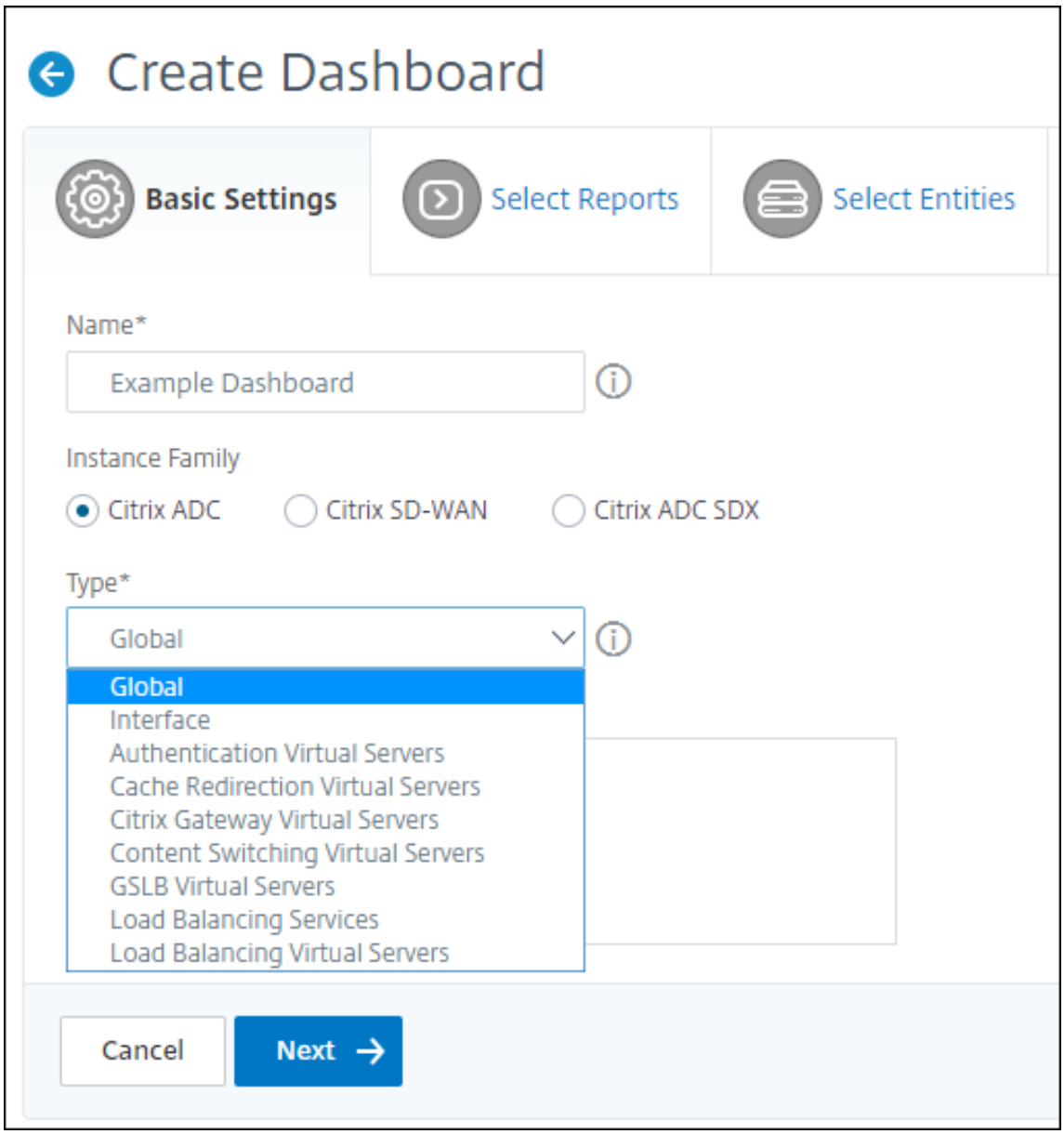
La section suivante explique en détail les tâches de création d'un tableau de bord, de génération de rapports et d'exportation de rapports.

Pour afficher ou créer un tableau de bord :

1. Dans Citrix ADM, accédez à **Réseaux** > **Network Reporting**.



2. Pour afficher les tableaux de bord existants, cliquez sur **Afficher le tableau de bord**. La page **Tableau de bord** Network Reporting s'ouvre et vous permet d'afficher tous vos tableaux de bord et widgets de rapport.
3. Pour créer un tableau de bord, cliquez sur **Nouveau tableau de bord**. La page Créer un tableau de bord s'ouvre.



4. Dans l'onglet Paramètres de base, entrez les détails suivants :

   a) **Nom**. Entrez le nom du tableau de bord.

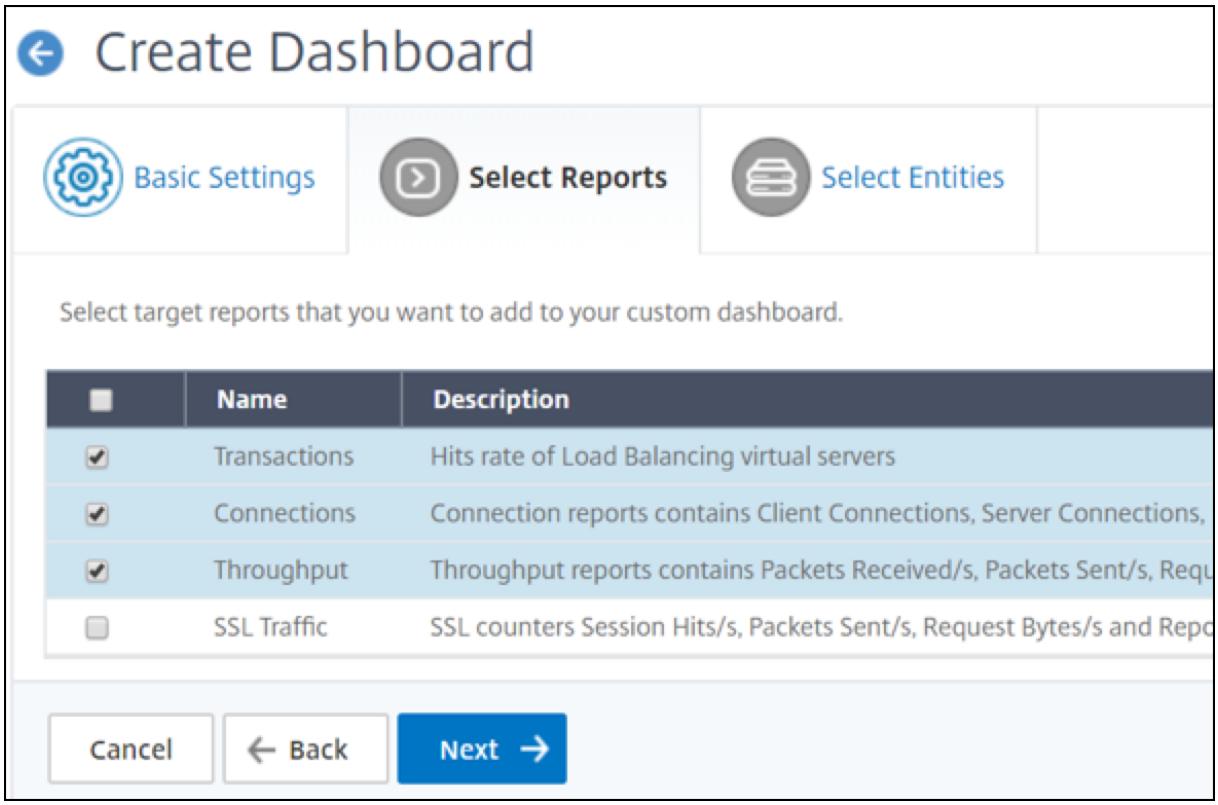
   b) **Famille d'instances**. Sélectionnez le type d'instance - Citrix ADC, Citrix SD-WAN ou Citrix ADC SDX.

   c) **Type**. Sélectionnez le type d'entité pour lequel vous souhaitez générer des rapports. Dans cet exemple, sélectionnez des serveurs virtuels d'équilibrage de charge.

   d) **Descriptif**. Entrez une description claire pour le tableau de bord.

5. Cliquez sur **Suivant**. Tous les rapports pris en charge pour l'instance et l'entité spécifique s'affichent.

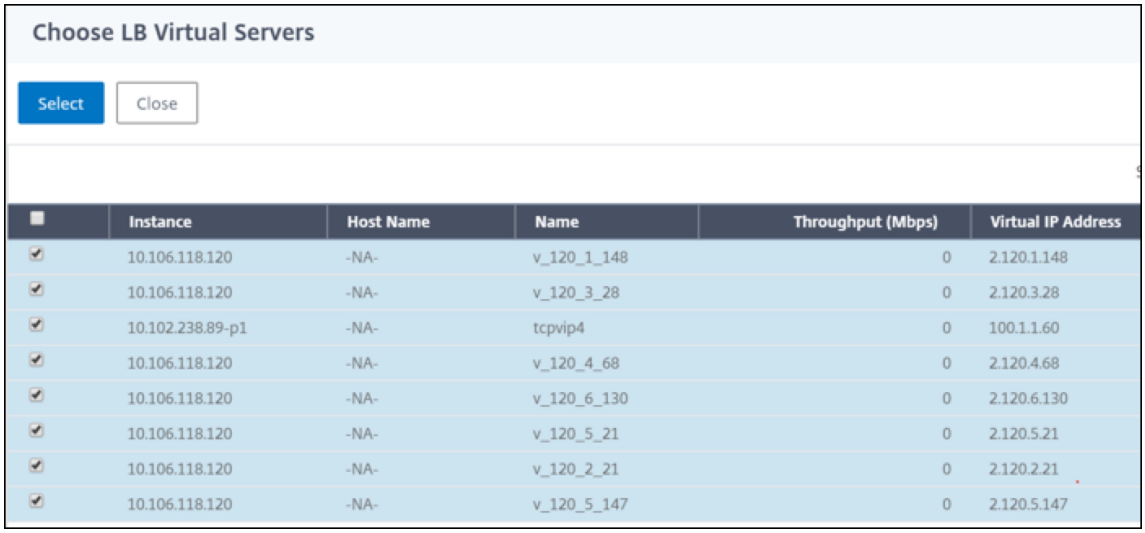
6. Dans l'onglet **Sélectionner des rapports**, sélectionnez les rapports requis. Dans cet exemple, vous pouvez sélectionner les transactions, les connexions et le débit. Cliquez sur **Suivant**.



1. Dans l'onglet **Sélectionner les entités**, cliquez sur **Ajouter** .

   Une fenêtre apparaît avec la liste des entités en fonction du type d'entité sélectionné dans l'onglet **Paramètres de base**. Dans cet exemple, la fenêtre **Choose LB Virtual Servers** s'affiche.

2. Sélectionnez les entités que vous souhaitez surveiller.



3. Cliquez sur **Créer**.

Le tableau de bord est créé et affiche tous les rapports que vous avez sélectionnés.

> **Remarque**
>
> Actuellement, les modifications que vous apportez aux légendes ou aux filtres ne peuvent pas être enregistrées.

Exportation de rapports réseau

Bien que vous puissiez exporter des rapports de widgets aux formats .pdf, .png, .jpeg ou .csv, vous pouvez exporter l'intégralité des tableaux de bord uniquement aux formats .pdf, .jpeg ou .png.

> **Remarque**
>
> Vous ne pouvez pas exporter de rapports dans Citrix ADM si vous disposez d'autorisations en lecture seule. Vous avez besoin d'une autorisation de modification pour pouvoir créer un fichier dans Citrix ADM et pour pouvoir exporter le fichier.

Pour exporter des rapports de tableau de bord :

1. Accédez à **Réseaux** > **Rapports réseau**
2. Cliquez sur **Afficher les tableaux de bord** pour afficher tous les tableaux de bord que vous avez créés.
3. Dans le volet gauche, cliquez sur un tableau de bord. Dans cet exemple, cliquez sur **Tableau de bord 1**.
4. Cliquez sur le bouton d'exportation en haut à droite de la page.
5. Sous l'onglet **Exporter maintenant**, sélectionnez le format requis, puis cliquez sur **Exporter**.

   Sur la page **Exporter**, vous pouvez effectuer l'une des opérations suivantes :
6. Sélectionnez l'onglet **Exporter maintenant** . Pour afficher et enregistrer le rapport au format PDF, JPEG, PNG ou CSV.
7. Sélectionnez l'onglet **Planifier l'exportation**. Pour planifier le rapport tous les jours, hebdomadaires ou mensuels et envoyer le rapport par e-mail ou message de marge.

   Vous pouvez planifier une exportation récurrente de la page du tableau de bord **Network Reporting** . Par exemple, vous pouvez définir une option permettant de générer un rapport de tableau de bord chaque semaine pour l'heure précédente à un moment donné. Le rapport est alors généré chaque semaine et indique l'état du tableau de bord. Le rapport remplace l'horodatage, s'il est défini par l'utilisateur.

> **Remarque**
>
> - si vous sélectionnez Récurrence hebdomadaire, assurez-vous de sélectionner les jours de la semaine sur lesquels vous souhaitez que le rapport soit planifié.
> - Si vous sélectionnez Récurrence mensuelle, assurez-vous de saisir tous les jours où vous souhaitez que le rapport soit planifié, séparés par des virgules.

Lorsque vous planifiez des rapports réseau, vous pouvez personnaliser le titre du rapport en saisissant une chaîne de texte dans le champ **Objet** . Le rapport créé à l'heure planifiée a cette chaîne comme nom.

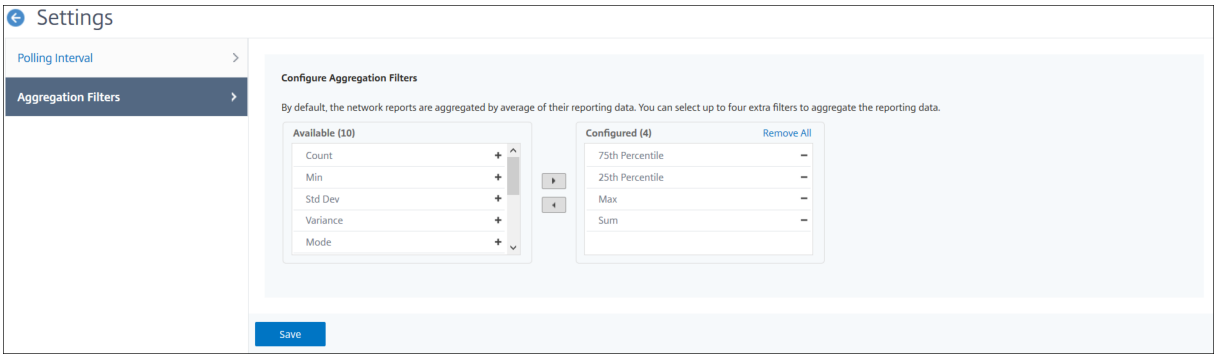
Par exemple, pour les rapports réseau provenant d'un serveur virtuel particulier, vous pouvez taper le sujet comme « authentication-reports-10.106.118.120 », où 10.106.118.120 est l'adresse IP du serveur virtuel surveillé.

> **Remarque**
>
> Actuellement, cette option n'est disponible que lorsque vous planifiez l'exportation de rapports. Vous ne pouvez pas ajouter un en-tête au rapport lorsque vous les exportez instantanément.

Afficher les données de reporting réseau en appliquant des agrégations

Vous pouvez appliquer des agrégations aux données de performances réseau et afficher les performances des applications sur le tableau de bord. Vous pouvez également exporter les résultats en fonction de vos besoins. À l'aide de ces agrégations appliquées aux données, vous pouvez analyser et vous assurer que toutes les ressources sont utilisées de manière optimale. Accédez à **Réseau > Rapports réseau** et sélectionnez la durée d'un jour ou plus pour obtenir l'option **Afficher par** .

Dans les données moyennes existantes, vous pouvez appliquer des agrégations en sélectionnant l'option dans la liste **Voir par**. Lorsque vous appliquez l'agrégation, les données sont mises à jour pour chaque mesure du tableau de bord. Cliquez sur **Paramètres**, puis sélectionnez **Filtres d'agrégation**.



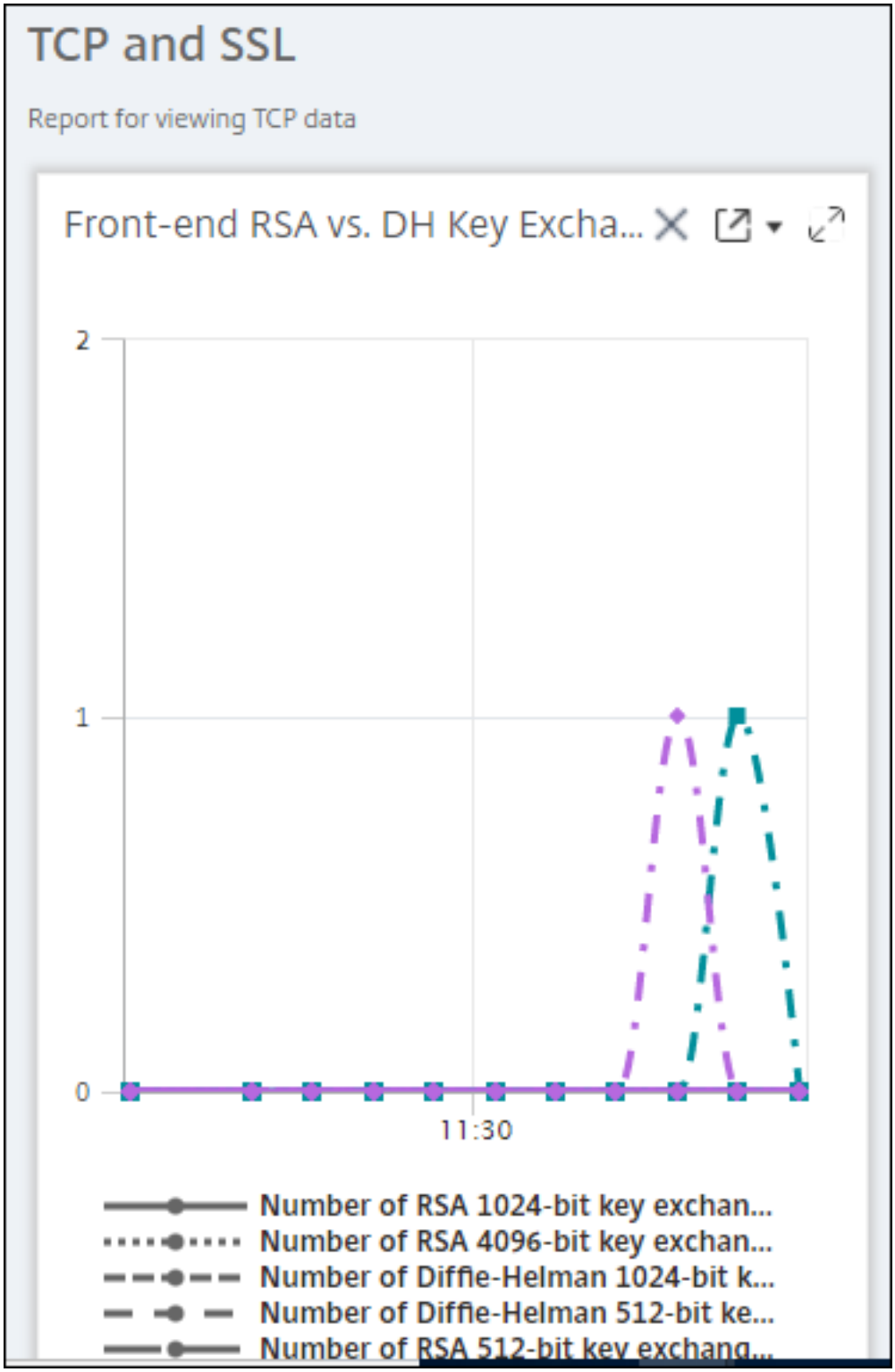
Les agrégations que vous pouvez ajouter sont les suivantes :

- Nombre
- Max
- Min
- Somme
- Dev Std
- Variance
- Mode
- Médiane
- 25e centile
- 75e centile
- 95e centile
- 99e centile
- Premier
- Dernier

Vous pouvez ajouter jusqu'à 4 options d'agrégation au tableau de bord. Après avoir ajouté les options d'agrégation, Citrix ADM prend environ 1 heure pour générer des rapports pour les options d'agrégation sélectionnées.

Pour exporter des rapports de widget :

1. Accédez à **Réseaux** > **Rapports réseau.**
2. Cliquez sur **Afficher les tableaux de bord** pour afficher tous les tableaux de bord que vous avez créés.
3. Dans le volet gauche, cliquez sur un tableau de bord. Dans cet exemple, cliquez également sur **Skype for Business**.
4. Sélectionnez un widget. Par exemple, sélectionnez **Load Balancing Virtual Server Transactions**.
5. Cliquez sur le bouton Exporter dans le coin supérieur droit de la page
6. Sous l'onglet **Exporter maintenant**, sélectionnez le format requis, puis cliquez sur **Exporter**.



Comment faire pour gérer les seuils pour les rapports réseau sur Citrix ADM

Pour surveiller l'état d'une instance Citrix ADC, vous pouvez définir des seuils sur les compteurs et recevoir des notifications lorsqu'un seuil est dépassé. Sur Citrix ADM, vous pouvez configurer des seuils et les afficher, les modifier et les supprimer.

Par exemple, vous pouvez recevoir une notification par e-mail lorsque le compteur de connexions d'un serveur virtuel de commutation de contenu atteint une valeur spécifiée. Vous pouvez définir un seuil pour un type d'instance spécifique. Vous pouvez également choisir les rapports que vous souhaitez générer pour des mesures de compteur spécifiques à partir de l'instance choisie.

Lorsque la valeur d'un compteur dépasse ou tombe en dessous (comme spécifié par la règle) la valeur seuil, un événement de la gravité spécifiée est généré pour signaler un problème lié aux performances. Lorsque la valeur du compteur revient à une valeur que vous considérez normale, l'événement est effacé. Pour afficher ces événements, accédez à **Réseaux** > **Événements** > **Rapports** . Sur la page Rapports, vous pouvez cliquer sur le donut **Événements par gravité** pour afficher les événements par gravité.

Vous pouvez également associer une action à un seuil tel que l'envoi d'un e-mail ou d'un message SMS en cas de violation du seuil.

Pour créer un seuil :

1. Dans Citrix ADM, accédez à **Réseaux** > **Rapports réseau** > **Seuils** . Sous **Seuils**, cliquez sur **Ajouter**.
2. Sur la page **Créer un seuil**, spécifiez les informations suivantes :

    - **Nom**. Nom du seuil.
    - **Type d'instance**. Choisissez Citrix ADC ou Citrix SD-WAN WO.
    - **Nom du rapport**. Nom du rapport de performance qui fournit des informations sur ce seuil.

3. Vous pouvez également définir des règles pour spécifier à quel moment un événement doit être généré ou supprimé. Vous pouvez spécifier les informations suivantes dans la section **Configurer la règle** :

    - **Métrique**. Sélectionnez la métrique pour laquelle vous souhaitez définir un seuil.
    - **Comparateur**. Sélectionnez un comparateur pour vérifier si la valeur surveillée est supérieure ou égale, inférieure ou égale à la valeur seuil.
    - **Valeur seuil**. Entrez la valeur pour laquelle la gravité de l'événement est calculée. Par exemple, vous souhaiterez peut-être générer un événement présentant une gravité critique si la valeur surveillée pour les connexions client actuelles atteint 80 %. Dans ce cas, tapez 80 comme valeur de seuil. Vous pouvez afficher les événements de « gravité critique » en

accédant à **Réseaux** > **Événements** > **Rapports**. Sur la page Rapports, vous pouvez cliquer sur le donut **Événements par gravité** pour afficher les événements par gravité.

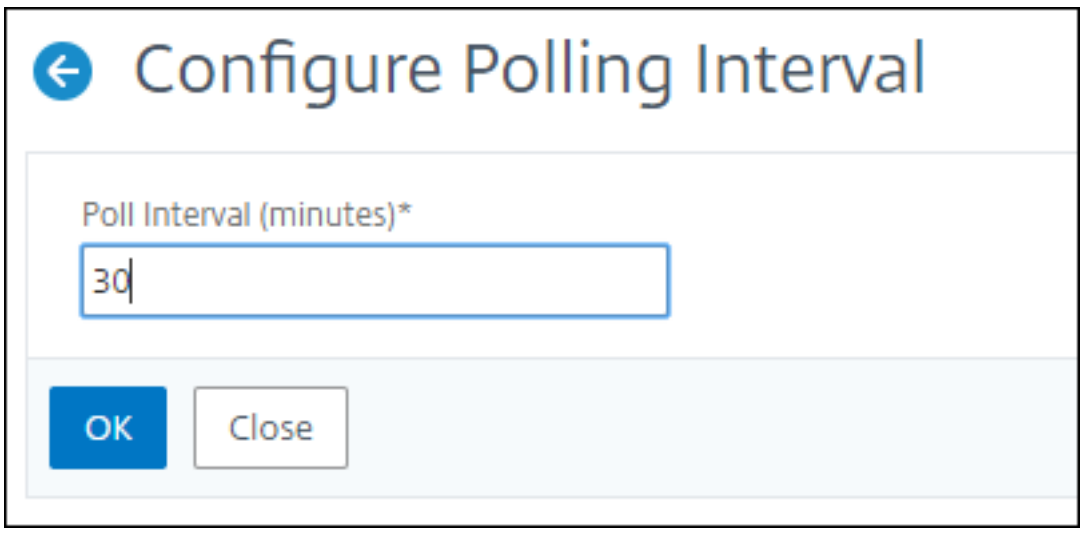
- **Valeur claire**. Entrez la valeur qui indique à quel moment effacer la valeur. Par exemple, vous pouvez supprimer le seuil des connexions client actuelles lorsque la valeur surveillée atteint 50 %. Dans ce cas, saisissez 50 comme valeur claire.
- **Gravité de l'événement** Sélectionnez le niveau de sécurité que vous souhaitez définir pour la valeur de seuil.

4. Choisissez l'adresse IP de la ou des instances pour lesquelles vous souhaitez définir le seuil.
5. Vous pouvez également ajouter un **message d'événement**. Tapez un message que vous souhaitez afficher lorsque le seuil est atteint. Citrix ADM ajoute la valeur surveillée et la valeur de seuil à ce message.
6. Sélectionnez**Activer**pour activer le seuil pour générer des alarmes.
7. Vous pouvez également configurer des **actions** telles que les notifications par e-mail ou Slack ou les notifications par e-mail et Slack.
8. Cliquez sur **Créer**.

Définir l'intervalle d'interrogation des performances pour les rapports réseau

Par défaut, toutes les 5 minutes, les appels NITRO recueillent des données de performances pour les rapports réseau. ADM récupère les statistiques d'instance telles que les informations de compteur et les agrège en fonction de la minute, de l'heure, du jour ou de la semaine. Vous pouvez afficher ces données agrégées dans des rapports prédéfinis.

Pour définir l'intervalle d'interrogation des performances, accédez à **Réseaux** > **Rapport réseau, puis**cliquez sur**Configurer l'intervalle d'interrogation**. Votre intervalle de scrutin ne peut pas être inférieur à 5 minutes ou supérieur à 60 minutes.



Configuration des paramètres de nettoyage des rapports réseau

Vous pouvez configurer l'intervalle de purge des données de rapport réseau dans Citrix ADM. Ce paramètre limite la quantité de données de rapport réseau stockées dans la base de données du serveur Citrix ADM. Par défaut, le nettoyage se produit toutes les 24 heures (à 01.00 heures) pour le réseau qui rapporte des données historiques.

> **Remarque**
>
> La valeur que vous pouvez spécifier ne peut pas dépasser 90 jours ou être inférieure à 1 jour.

Utiliser les journaux d'audit ADM pour gérer et surveiller votre infrastructure

February 1, 2024

Vous pouvez utiliser le service Citrix ADM pour suivre tous les événements sur ADM et les événements Syslog générés sur les instances ADC gérées par ADM. Ces messages peuvent vous aider à gérer et à surveiller votre infrastructure. Mais les messages de journal ne constituent une excellente source d'informations que si vous les consultez, et ADM simplifie la procédure de révision des messages de journal.

Vous pouvez utiliser des filtres pour rechercher les messages du syslog et du journal d'audit d'ADM. Les filtres vous aident à affiner vos résultats et à trouver exactement ce que vous recherchez en temps réel. L'aide à la recherche intégrée vous guide pour filtrer les journaux. Une autre façon d'afficher les messages du journal consiste à les exporter aux formats PDF, CSV, PNG et JPEG. Vous pouvez planifier l'exportation de ces rapports vers des adresses e-mail spécifiées à différents intervalles.

Vous pouvez consulter les types de messages de journal suivants à partir de l'interface graphique d'ADM :

- Journaux d'audit relatifs aux instances ADC
- Journaux de vérification liés à ADM
- journaux d'audit des applications

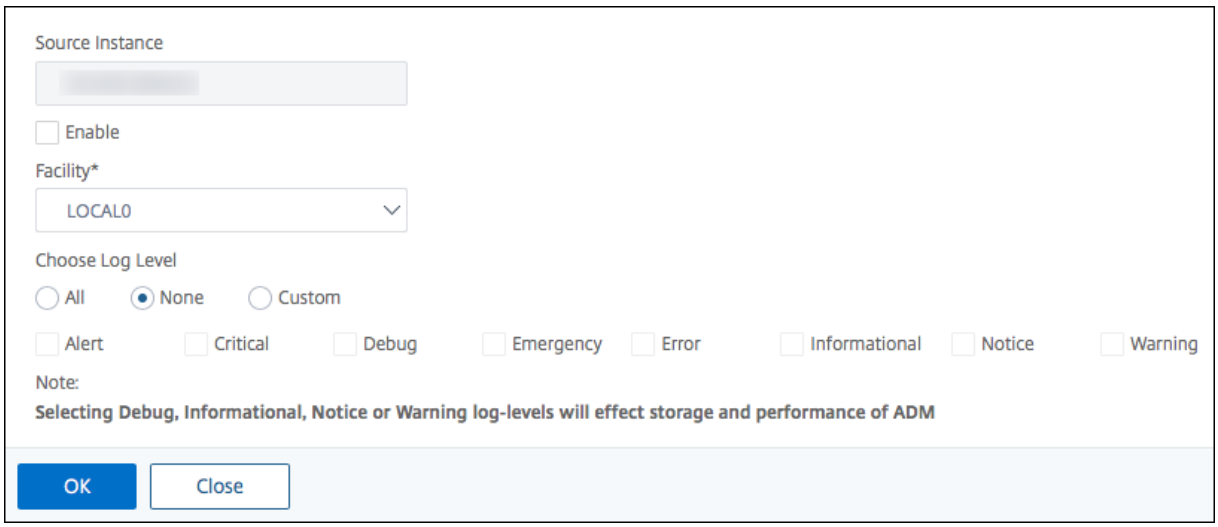
Journaux d'audit relatifs aux instances ADC

Avant de pouvoir afficher les messages syslog relatifs à l'instance ADC depuis ADM, configurez le service Citrix ADM en tant que serveur syslog pour votre instance Citrix ADC. Une fois la configuration terminée, tous les messages syslog sont redirigés de l'instance vers ADM.

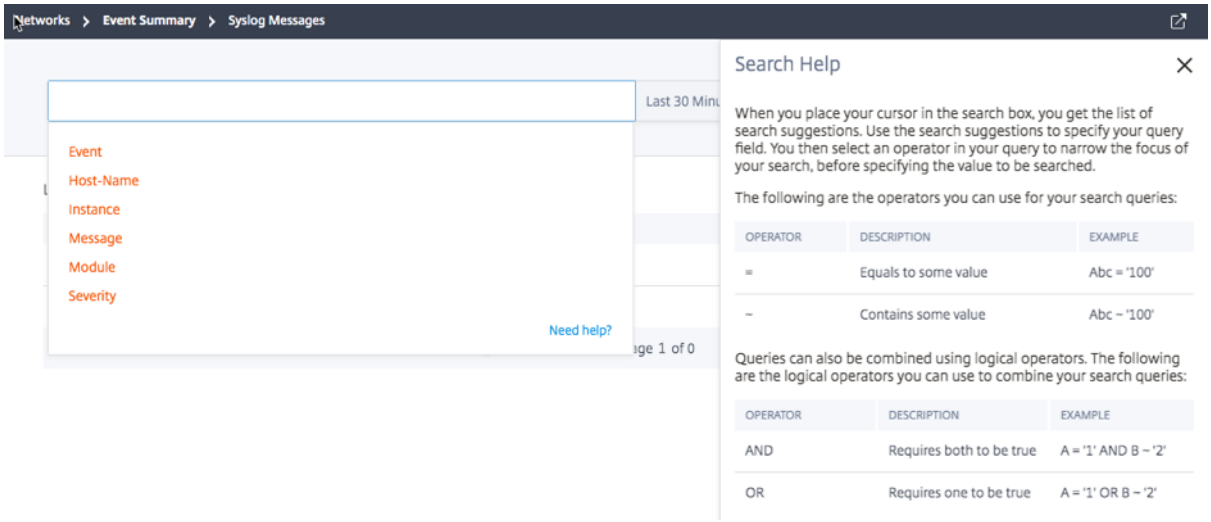
Configurer le service ADM en tant que serveur Syslog

Procédez comme suit pour configurer ADM en tant que serveur syslog :

1. À partir de l'interface graphique ADM, accédez à **Réseaux > Instances**.
2. Sélectionnez l'instance Citrix ADC à partir de laquelle vous souhaitez que les messages syslog soient collectés et affichés dans Citrix ADM.
3. Dans la liste **Sélectionner une action**, sélectionnez **Configurer Syslog**.
4. Cliquez sur **Activer**.
5. Dans la liste déroulante **Installation**, sélectionnez une ressource locale ou au niveau de l'utilisateur.
6. Sélectionnez le niveau de journalisation requis pour les messages Syslog.
7. Cliquez sur **OK**.



Ces étapes configurent toutes les commandes syslog dans l'instance de Citrix ADC et Citrix ADM commence à recevoir les messages syslog. Vous pouvez afficher les messages en accédant à **Réseaux > Événements > Messages Syslog**. Cliquez sur **Besoin d'aide ?** pour ouvrir l'aide de recherche intégrée. Pour plus d'informations, consultez Afficher et exporter des messages Syslog.

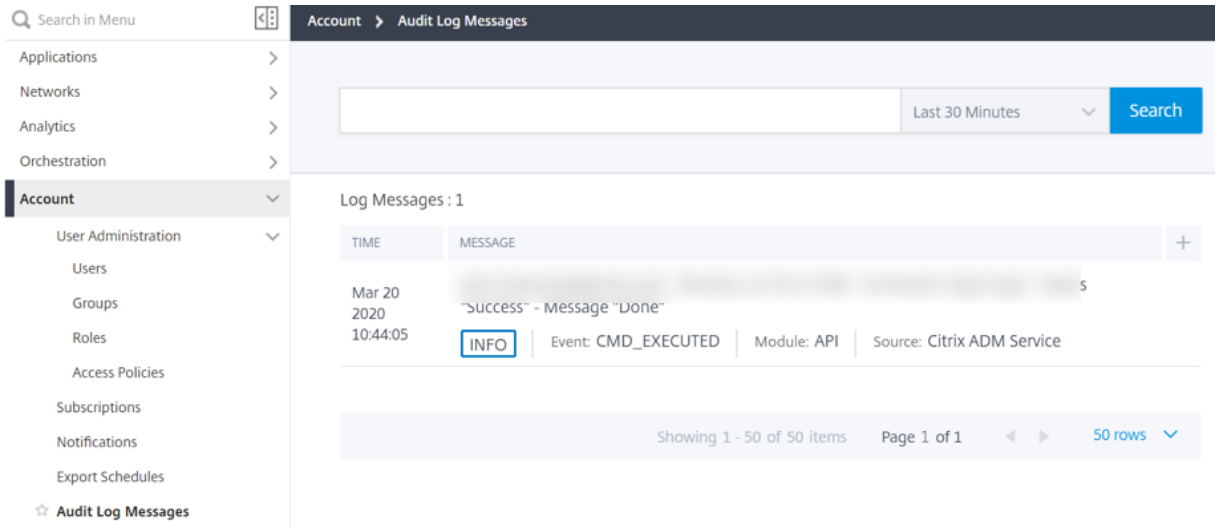


Pour exporter les messages du journal, cliquez sur l'icône en forme de flèche dans le coin supérieur droit.

Ensuite, cliquez sur **Exporter maintenant** ou **Planifier l'exportation**. Pour plus d'informations, consultez Afficher et exporter des messages Syslog.

Journaux de vérification liés à ADM

Sur la base de règles préconfigurées, ADM génère des messages de journal d'audit pour tous les événements sur, ce qui vous aide à surveiller l'intégrité de votre infrastructure. Pour afficher tous les messages du journal d'audit présents dans l'ADM, accédez à **Système > Messages du journal d'audit**.



Pour exporter les messages du journal, cliquez sur l'icône en forme de flèche dans le coin supérieur droit.

Journaux d'audit relatifs aux applications

Vous pouvez afficher les messages du journal d'audit pour toutes les applications ADM ou pour une application spécifique.

- Pour afficher tous les messages du journal d'audit pour toutes les applications présentes dans l'ADM, accédez à **Réseaux->Fonctions réseau >Audit**.
- Pour afficher les messages du journal d'audit pour une application spécifique dans ADM, accédez à **Application > Tableau de bord > double-cliquez sur le serveur virtuel > Journal d'audit**.

Analytics

February 1, 2024

La fonctionnalité Citrix ADM Analytics fournit un moyen simple et évolutif d'examiner diverses informations Citrix ADC afin d'analyser et d'améliorer les performances des applications. Vous pouvez utiliser une ou plusieurs fonctionnalités d'analyse simultanément sur Citrix ADM.

Le tableau suivant décrit diverses fonctionnalités d'analyse prises en charge sur Citrix ADM :

Fonctionnalité d'analyse	Description
Web Insight	Web Insight offre une visibilité sur les applications Web d'entreprise et vous permet de surveiller toutes les applications Web dans Citrix ADC. En tant qu'administrateur, vous pouvez voir la surveillance intégrée et en temps réel des applications.
HDX Insight	HDX Insight offre une visibilité de bout en bout pour le trafic ICA passant par Citrix ADC. HDX Insight vous permet d'afficher en temps réel les mesures de latence du client et du réseau, les rapports historiques, les données de performance de bout en bout et de résoudre les problèmes de performances.

Fonctionnalité d'analyse	Description
Gateway Insight	Gateway Insight offre une visibilité sur les défaillances rencontrées par tous les utilisateurs, quel que soit le mode d'accès, au moment de la connexion à Citrix Gateway.
Security Insight	Security Insight fournit une solution sur un seul écran pour vous aider à évaluer l'état de sécurité de votre application et à prendre des mesures correctives pour sécuriser vos applications.
SSL Insight	SSL Insight offre une visibilité sur les transactions Web sécurisées (HTTPS) et vous permet de surveiller toutes les applications Web sécurisées dans Citrix ADC. En tant qu'administrateur, vous pouvez voir la surveillance intégrée, en temps réel et historique des transactions Web sécurisées.
TCP Insight	TCP Insight fournit une solution simple et évolutive pour surveiller les mesures des techniques d'optimisation et des stratégies (ou algorithmes) de contrôle de la congestion utilisées dans les instances de Citrix ADC afin d'éviter la congestion du réseau lors de la transmission de données.
Video Insight	La fonctionnalité Video Insight fournit une solution simple et évolutive pour surveiller les mesures des techniques d'optimisation vidéo utilisées par les appliances Citrix ADC afin d'améliorer l'expérience client et l'efficacité opérationnelle.
WAN Insight	L'analyse WAN Insight permet aux administrateurs de surveiller facilement le trafic WAN accéléré et non accéléré qui circule entre le centre de données et les appliances d'optimisation WAN des succursales. WAN Insight offre également une visibilité sur les clients, les applications et les succursales du réseau afin de résoudre efficacement les problèmes réseau.

Exigences en matière de licence

February 1, 2024

Le tableau suivant décrit les exigences en matière de licences sur les instances Citrix ADC pour consulter les différents rapports d'analyse sur Citrix ADM :

Fonctionnalités Citrix ADM Analytics	Exigence de licence Citrix ADC
Web Insight	Le rapport Web Insight sur Citrix ADM est pris en charge sur toutes les éditions de licence Citrix ADC (Standard/Advanced/Premium).
HDX Insight	Le rapport HDX Insight sur Citrix ADM est pris en charge sur toutes les licences Citrix ADC suivantes : Advanced Edition (pour les rapports de moins d'une heure) ou Premium Edition (pour des rapports illimités). **Remarque** l'édition de licence standard n'est pas prise en charge.
Security Insight	Le rapport Security Insight sur Citrix ADM est pris en charge sur Premium Edition ou Advanced Edition avec une licence App Firewall. **Remarque** l'édition de licence standard et la licence de pare-feu d'application autonome ne sont pas prises en charge.
SSL Insight	Le rapport SSL Insight sur Citrix ADM est pris en charge sur toutes les éditions de licence Citrix ADC (Standard/Advanced/Premium).
Gateway Insight	Le rapport Gateway Insight sur Citrix ADM est pris en charge sur toutes les licences Citrix ADC suivantes : Advanced Edition (pour les rapports de moins d'une heure) ou Premium Edition (pour des rapports illimités). **Remarque** l'édition de licence standard n'est pas prise en charge.
TCP Insight	Le rapport TCP Insight est pris en charge sur toutes les éditions de licence Citrix ADC (Standard/Advanced/Premium).

Fonctionnalités Citrix ADM Analytics	Exigence de licence Citrix ADC
Video Insight	Le rapport Video Insight sur Citrix ADM est pris en charge sur l'édition Citrix ADC Premium (série VPX-T 1000, VPX-T).
WAN Insight	Le rapport WAN Insight sur Citrix ADM est pris en charge sur Citrix SD-WAN WO Edition (WAN Optimization Edition).

Vue d'ensemble de Logstream

February 1, 2024

Les instances Citrix ADC génèrent des enregistrements AppFlow et constituent un point de contrôle central pour tout le trafic d'applications dans le centre de données. IPFIX et Logstream sont les protocoles qui transportent ces enregistrements AppFlow des instances de Citrix ADC vers Citrix ADM. Pour plus d'informations, voir AppFlow.

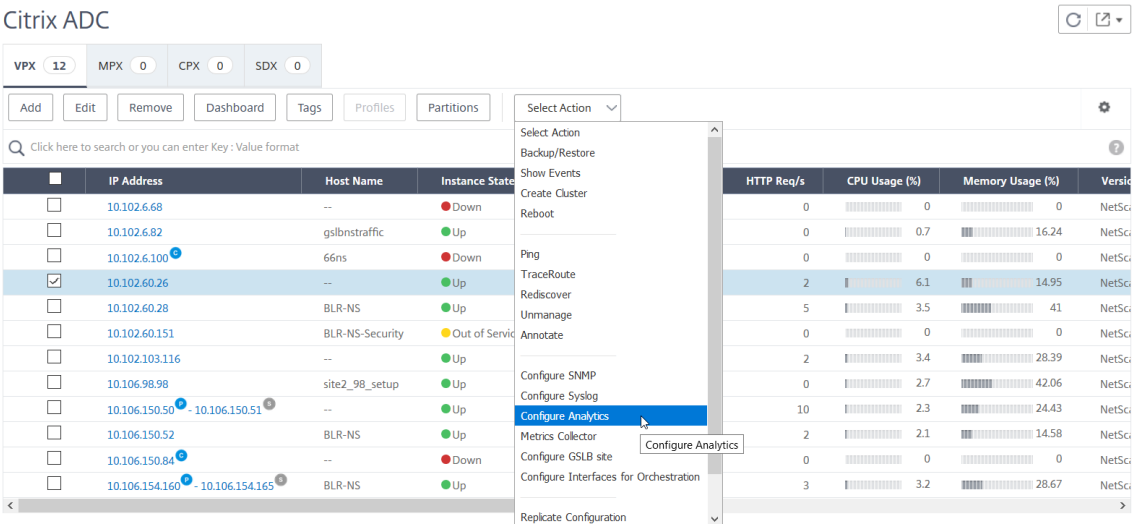
- IPFIX est un standard ouvert Internet Engineering Task Force (IETF) défini dans la RFC 5101. IPFIX utilise le protocole UDP qui est un protocole de transport peu fiable utilisé pour le flux de données dans une direction. Comme IPFIX utilise le protocole UDP, le respect de la norme IPFIX permet de traiter davantage de ressources dans Citrix ADM.
- Logstream est un protocole appartenant à Citrix qui est utilisé comme l'un des modes de transport pour transférer efficacement les données du journal d'analyse des instances de Citrix ADC vers Citrix ADM. Logstream utilise un protocole TCP fiable et nécessite moins de ressources pour traiter les données.

Pour Citrix ADC entre **11.1 Build 47.14 et 11.1 Build 62.8**, Logstream est le mode de transport par défaut pour activer Web Insight (HTTP) et IPFIX est le seul mode de transport pour activer d'autres informations. Pour la version **12.0 à la dernière version** de Citrix ADC, vous pouvez sélectionner **Logstream**ou **IPFIX**comme mode de transport.

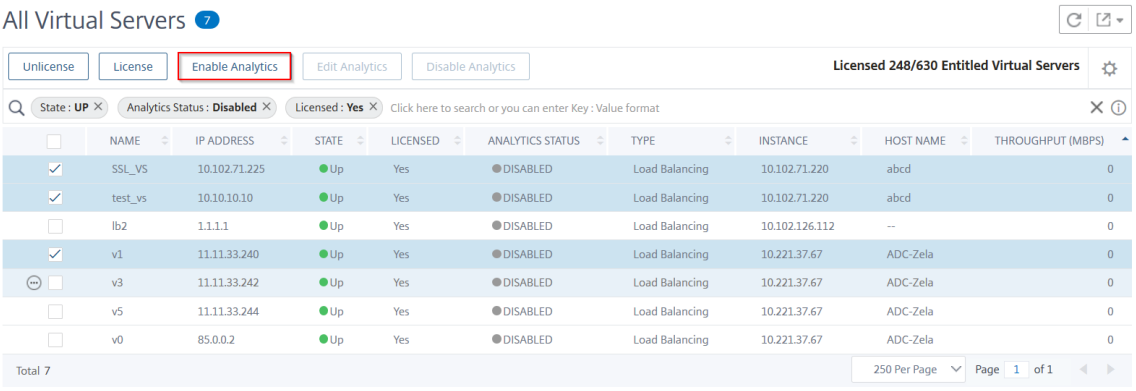
Activer Logstream comme mode de transport

1. Accédez à **Réseaux > Instances**, puis sélectionnez l'instance ADC que vous souhaitez activer l'analyse.

2. Dans la liste **Sélectionner une action**, sélectionnez **Configurer Analytics**.



3. Sélectionnez les serveurs virtuels, puis cliquez sur **Activer Analytics**.



4. Dans la fenêtre **Activer Analytics** :

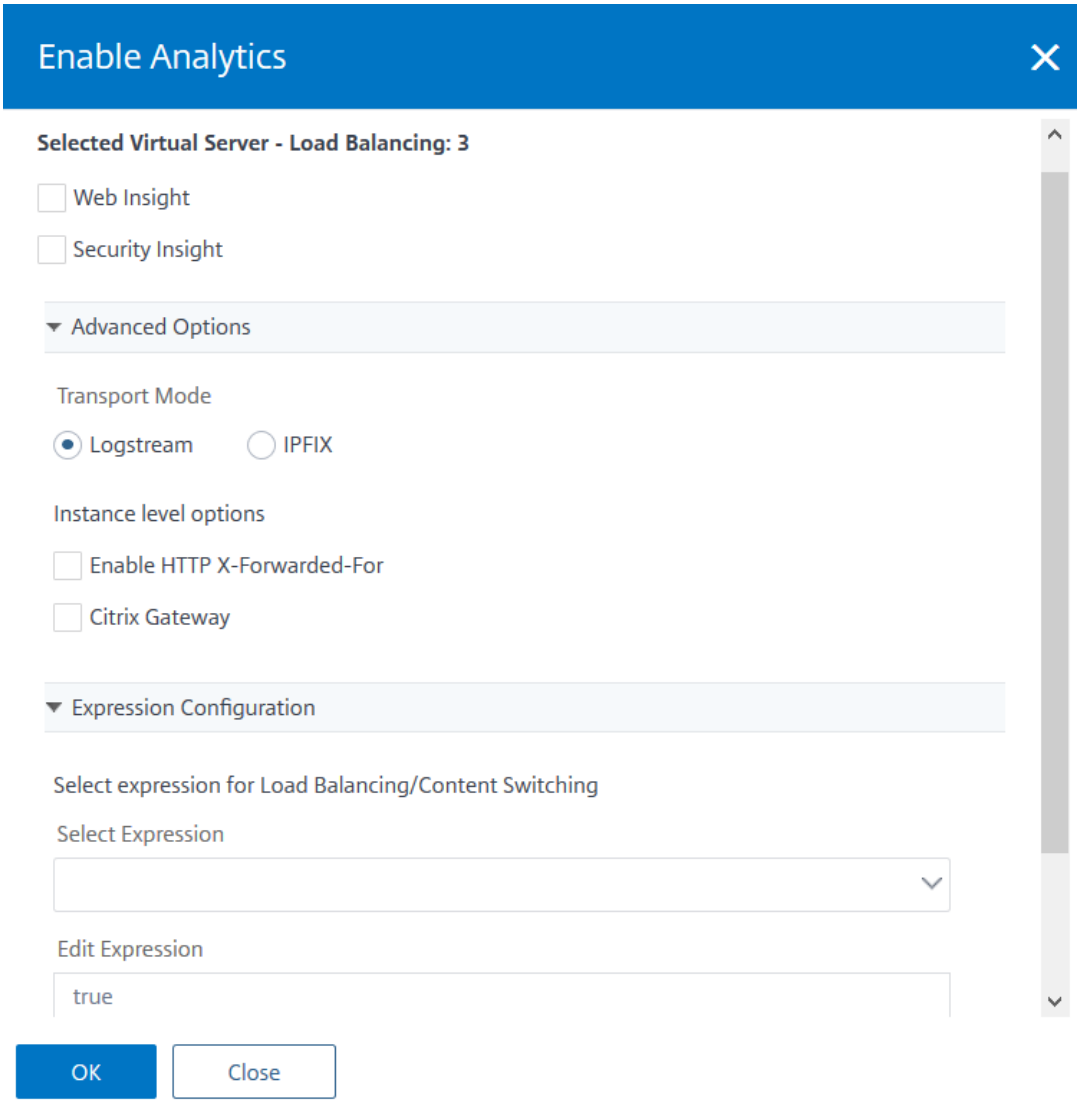
   a) Sélectionnez les types d'informations (Web Insight ou Security Insight)

   b) Sélectionnez **Logstream** comme mode de transport

> **Remarque**
>
> Pour Citrix ADC entre **11.1 Build 47.14 et 11.1 Build 62.8**, Logstream est le mode de transport par défaut pour activer Web Insight (HTTP) et IPFIX est le seul mode de transport pour activer d'autres informations. Pour la version **12.0 à la dernière version** de Citrix ADC, vous pouvez sélectionner **Logstream**ou **IPFIX**comme mode de transport.

   c) L'expression est true par défaut

   d) Cliquez sur **OK**.



Remarque

- Si vous sélectionnez des serveurs virtuels qui ne sont pas sous licence, Citrix ADM octroie d'abord des licences à ces serveurs virtuels, puis active les analyses
- Pour les partitions d'administration, seul **Web Insight** est pris en charge
- Pour les serveurs virtuels tels que la redirection du cache , l'authentification et le GSLB , vous ne pouvez pas activer les analyses. Un message d'erreur s'affiche

Le tableau suivant décrit les fonctionnalités de Citrix ADM qui prend en charge Logstream en tant que mode de transport :

Fonctionnalité	IPFIX	Logstream
Web Insight	•	•
Security Insight	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	Non pris en charge	•
CR Insight	•	•
Réputation IP	•	•
AppFirewall	•	•
Mesure côté client	•	•
Syslog/Auditlog	•	•

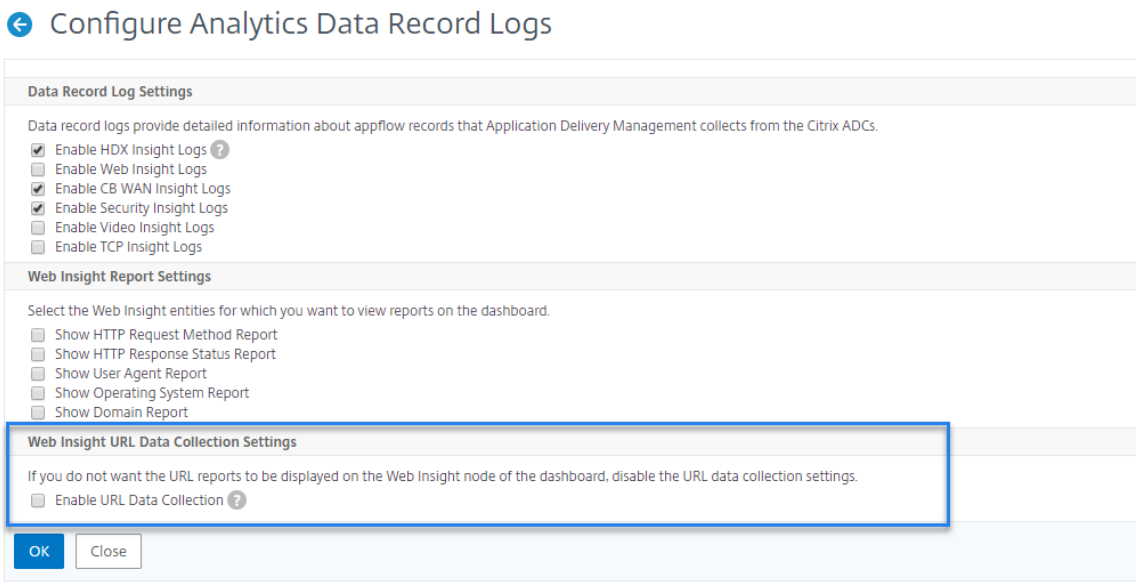
Désactiver la collecte de données d'URL

February 1, 2024

Vous pouvez désactiver la collecte de données d'URL si vous ne souhaitez pas que les rapports d'URL s'affichent sur le nœud Web Insight du tableau de bord dans Citrix Application Delivery Management (ADM).

Pour désactiver la collecte de données d'URL à partir de Citrix ADM

1. Dans Citrix ADM, accédez à **Analytics** > **Paramètres**, puis cliquez sur **Configurer les journaux des enregistrements de données Analytics**.
2. Dans la section **Paramètres de collecte de données URL Web Insight**, si l'option **Activer la collecte de données URL** est cochée, désactivez la case à cocher.
3. Cliquez sur **OK**.



Créer des seuils et des alertes

February 1, 2024

Vous pouvez définir des seuils et des alertes pour surveiller l'état d'une instance Citrix ADC. Vous pouvez définir des seuils sur les compteurs et surveiller les instances et les entités sur les instances gérées.

Lorsque la valeur d'un compteur dépasse le seuil, Citrix Application Delivery Management (ADM) génère un événement pour signifier un problème lié aux performances. Lorsque la valeur du compteur correspond à la valeur d'effacement spécifiée dans le seuil, l'événement est effacé, ce qui signifie que le seuil particulier est revenu à son état normal.

Vous pouvez également associer une action au seuil. Les actions incluent l'envoi d'une alerte, d'un e-mail ou d'une notification par SMS. Lorsque le seuil est atteint, Citrix ADM effectue l'action que vous définissez automatiquement, comme l'activation d'une alerte et l'envoi d'une notification par e-mail ou SMS.

Pour créer un seuil et une alerte à l'aide de Citrix ADM :

1. Dans Citrix ADM, accédez à **Analytics** > **Paramètres** > **Seuils**. Sous **Seuils**, cliquez sur **Ajouter**.
2. Sur la page **Créer des seuils**, spécifiez les informations suivantes :
    - **Nom** : nom pour configurer le seuil.

- **Type de trafic** : type de trafic pour lequel vous souhaitez configurer le seuil.
- **Entité** : catégorie ou type de ressource pour lequel vous souhaitez configurer le seuil.
- **Clé de référence** : valeur générée automatiquement en fonction du type de trafic et de l'entité sélectionnés.
- **Durée** : intervalle pour lequel vous souhaitez configurer le seuil.
- **Configurer la règle** : règle de la mesure pour laquelle vous souhaitez configurer le seuil.
- **Paramètres de notification** - Activez le seuil et recevez des notifications via différents canaux tels que les e-mails, slack ou messages SMS lorsque le seuil est dépassé.

3. Cliquez sur **Créer**.

Pour l'aperçu HDX, vous pouvez également définir plusieurs seuils pour lesquels une alerte est générée uniquement si toutes les entités du seuil configuré sont violées.

Configurer des seuils adaptatifs

February 1, 2024

La fonctionnalité de seuil adaptative définit la valeur de seuil pour le nombre maximal de visites sur chaque URL. Si le nombre maximal de visites sur une URL est supérieur à la valeur seuil définie pour l'URL, un message Syslog est envoyé à un serveur Syslog externe. L'intervalle entre les valeurs de seuil peut être exprimé en jours ou en semaines.

La valeur seuil est calculée comme suit :

Valeur seuil = **Nombre maximum de visites * Multiplicateur de seuil**

Où :

- Le nombre maximal de visites est le nombre maximum de visites sur une URL.
- Le multiplicateur de seuil est une valeur entière que vous définissez (par défaut : 2).

Pour créer un seuil adaptatif à l'aide de Citrix ADM

1. Dans Citrix ADM, accédez à **Analytics** > **Paramètres** > **Seuils adaptatifs**, puis cliquez sur **Ajouter**.
2. Dans la page **Seuils adaptatifs**, spécifiez les paramètres suivants :
    - **Nom : nom** du seuil

- **Entité** - URL
- **Durée** - Durée du seuil (jour ou semaine)
- **Multiplicateur de seuil** : entier défini par l'utilisateur qui est multiplié par le nombre maximal de visites de l'URL spécifiée afin d'obtenir le seuil adaptatif pour l'URL.

Configurer la persistance de la base de données

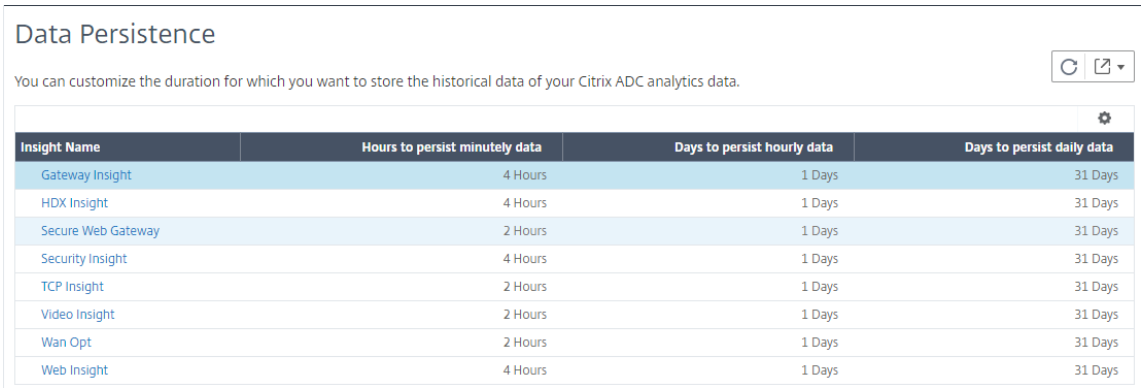
February 1, 2024

Configurer la persistance de la base de données dans Citrix Application Delivery Management (ADM) vous permet de personnaliser la durée de stockage des données historiques de vos données d'analyse Citrix ADC. Vous pouvez choisir les types de persistance de base de données suivants pour les données historiques de vos analyses :

- Des heures pour conserver les données minutieusement
- Jours pendant lesquels les données horaires doivent être conservées
- Jours pendant lesquels conserver les données quotidiennes

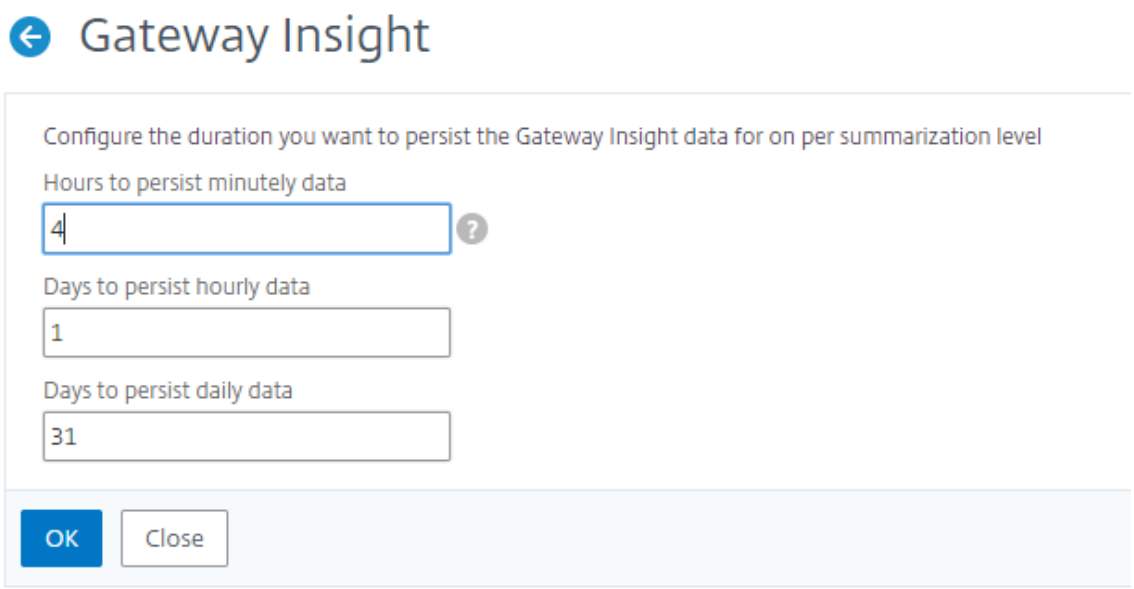
Pour configurer la persistance de la base de données

1. Accédez à > **Analytics** > **Paramètres** > **Persistance de la base**de données.
2. Cliquez sur le type d'aperçu que vous souhaitez configurer la persistance de la base de données.



Insight Name	Hours to persist minutely data	Days to persist hourly data	Days to persist daily data
Gateway Insight	4 Hours	1 Days	31 Days
HDX Insight	4 Hours	1 Days	31 Days
Secure Web Gateway	2 Hours	1 Days	31 Days
Security Insight	4 Hours	1 Days	31 Days
TCP Insight	2 Hours	1 Days	31 Days
Video Insight	2 Hours	1 Days	31 Days
Wan Opt	2 Hours	1 Days	31 Days
Web Insight	4 Hours	1 Days	31 Days

3. Spécifiez la durée pendant laquelle vous souhaitez conserver les données Insight sur Citrix ADM. Par exemple, pour Gateway Insight, vous pouvez stocker les données historiques de vos analyses pendant 2 heures, ou les données horaires pendant 1 jour.



Diagnostics en libre-service pour Analytics

February 1, 2024

Citrix Application Delivery Management (ADM) effectue des diagnostics en libre-service pour identifier les problèmes de licence et de configuration sur les instances gérées pour les fonctionnalités d'analyse suivantes :

- Web Insight
- HDX Insight
- Gateway Insight
- Security Insight
- Analyses de proxy de transfert SSL

Les diagnostics en libre-service s'exécutent toutes les 12 heures et génèrent un rapport de diagnostic si des problèmes sont détectés pour chacune des fonctionnalités d'analyse spécifiées. Le rapport de diagnostic fournit les sources des problèmes, les types de problèmes et les actions correctives pour les résoudre. Les diagnostics en libre-service vous aident à identifier et à résoudre les problèmes plus rapidement.

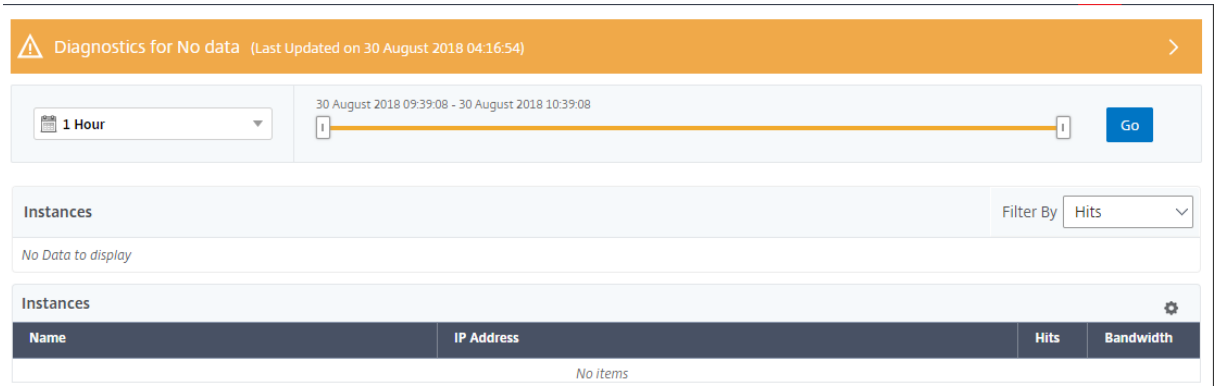
Par exemple, si la stratégie AppFlow n'est pas liée à un serveur virtuel ou qu'un serveur virtuel n'est pas sous licence, Citrix ADM n'obtient pas les données souhaitées pour la surveillance Web Insight. Le

diagnostic en libre-service identifie les problèmes et génère un rapport de diagnostic. Vous pouvez consulter le rapport de diagnostic pour vérifier les problèmes et effectuer les actions correctives.

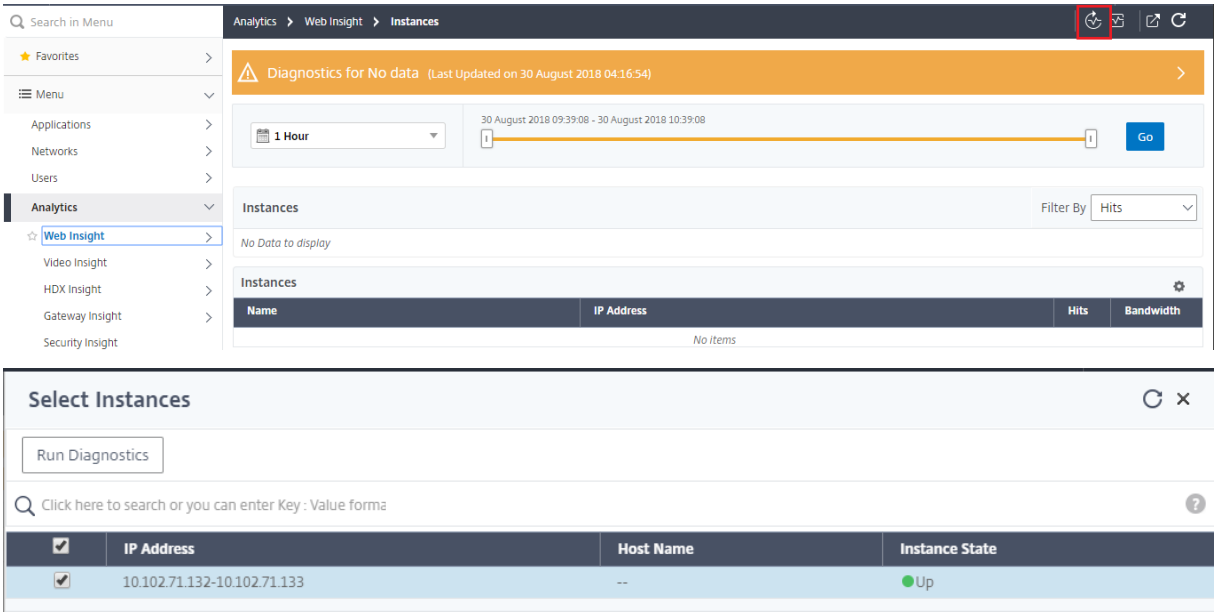
Voir le rapport de diagnostic

Pour afficher les rapports de diagnostic pour les fonctionnalités d'analyse spécifiées, vous devez accéder au nœud d'analyse respectif dans le tableau de bord de Citrix ADM.

Par exemple, pour afficher le rapport de diagnostic pour Web Insight, accédez à **Analytics > Web Insight**. Sur la page Web Insight, sélectionnez l'icône **Afficher les diagnostics**.



Vous pouvez également exécuter un diagnostic instantané si vous souhaitez vérifier les problèmes. Cliquez sur **Exécuter les diagnostics**. Choisissez les instances et sélectionnez **Exécuter les diagnostics**.



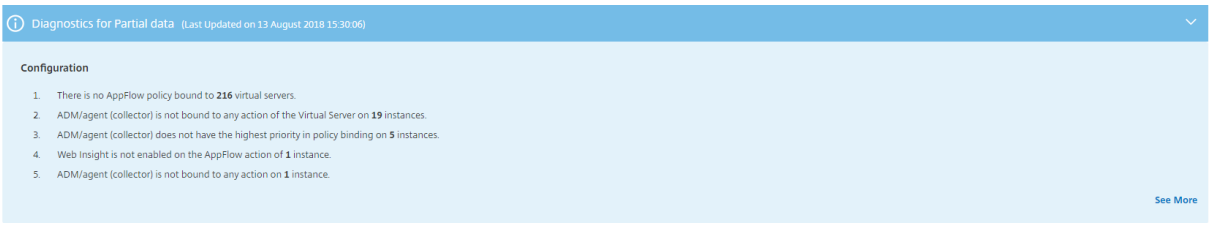
Analyser le rapport de diagnostic

Les diagnostics en libre-service affichent le rapport de diagnostic sur fond orange ou bleu en fonction de l'importance des problèmes.

Le rapport de diagnostic sur fond orange indique une criticité plus élevée que sur fond bleu.

Par exemple, cinq serveurs virtuels sont configurés sur votre instance Citrix ADC. Si vous n'avez activé les paramètres AppFlow sur aucun serveur virtuel, Citrix ADM ne reçoit pas le trafic Web Insight et Security Insight à des fins d'analyse. Les diagnostics en libre-service identifient les problèmes de configuration comme critiques. Les rapports de diagnostic s'affichent en arrière-plan orange dans les fonctionnalités Web Insight et Security Insight.

Si vous avez activé AppFlow sur l'un des serveurs virtuels, Citrix ADM reçoit des données à des fins d'analyse. Vous voyez le rapport de diagnostic en arrière-plan bleu car au moins un serveur virtuel envoie du trafic pour analyse.

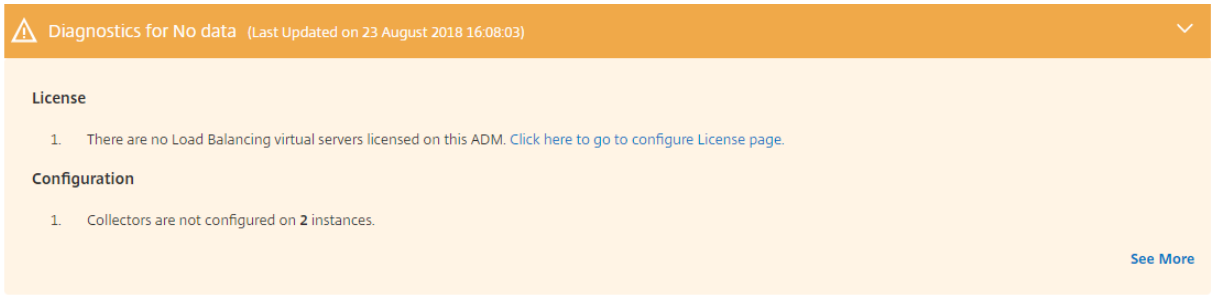


> **IMPORTANT** : Les diagnostics en libre-service ne vérifient pas le flux de trafic. Il vérifie uniquement les problèmes de licence ou de configuration associés aux fonctionnalités d'analyse spécifiées sur les instances gérées. Parfois, vous ne voyez aucune donnée d'analyse car aucun trafic actif ne passe par des serveurs virtuels.

Le rapport de diagnostic comporte une page de résumé et une page d'informations détaillées.

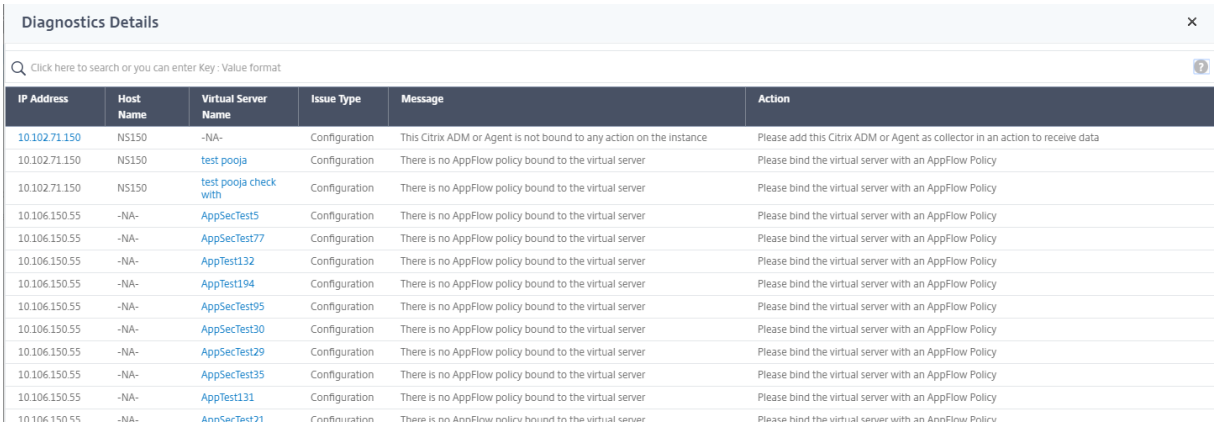
La page de résumé fournit une vue d'ensemble des types de problèmes (licence ou configuration). La page peut contenir des liens hypertexte qui vous dirigent vers les pages de configuration pertinentes.

Par exemple, s'il n'y a pas de serveurs virtuels d'équilibrage de charge sous licence sur votre Citrix ADM, la page de résumé fournit un lien hypertexte qui vous dirige vers la page **Licences système**.

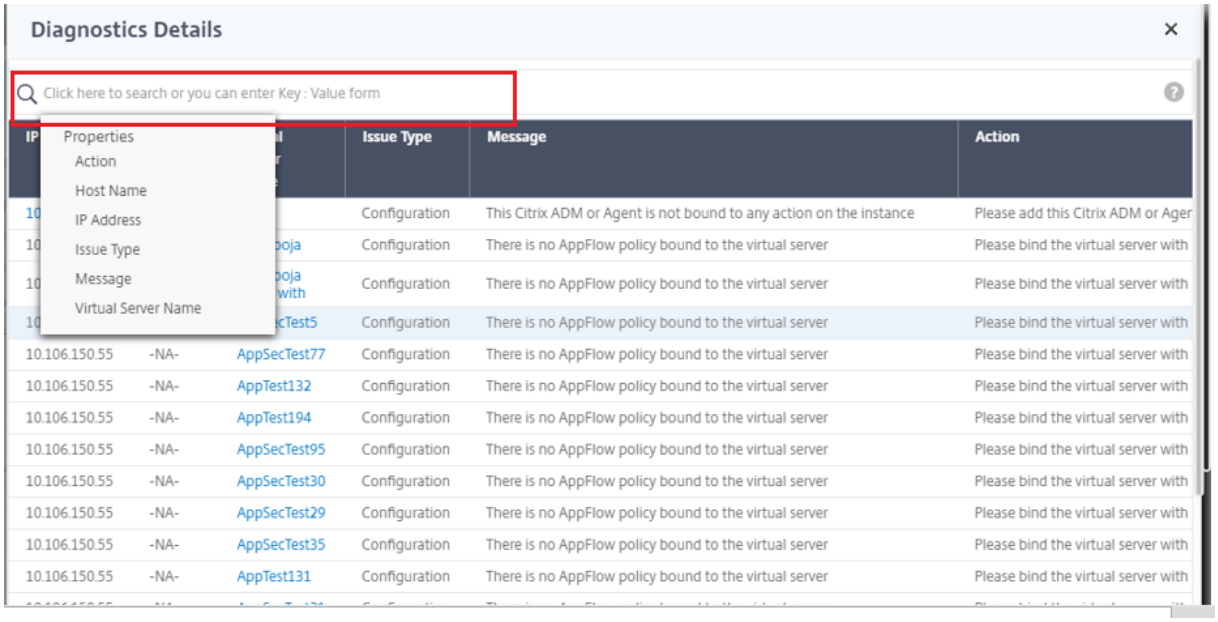


Pour afficher les informations détaillées sur les problèmes, cliquez sur **Voir plus** sur la page récapitulative.

La page d'informations détaillées fournit des informations complètes sur les problèmes et recommande les actions que vous devez effectuer. Vous pouvez cliquer sur le lien hypertexte correspondant à chaque problème pour configurer l'instance gérée ou le serveur virtuel.



Vous pouvez également rechercher les problèmes en fonction de l'action, du nom d'hôte, de l'adresse IP et du type de problème, etc.



Après avoir résolu les problèmes, vous devez exécuter un diagnostic instantané pour générer le dernier rapport de diagnostic.

Web Insight

February 1, 2024

Web Insight permet aux administrateurs de surveiller toutes les applications Web desservies par les instances de Citrix ADC. En tant qu'administrateur, vous pouvez obtenir une surveillance intégrée et en temps réel des applications à partir d'instances de Citrix ADC. Web Insight fournit des informations critiques telles que la latence du réseau client et le temps de réponse du serveur, garantissant ainsi la surveillance et l'amélioration des performances des applications. Les données utilisées pour l'analyse sont capturées à partir de chaque transaction HTTP, HTTPS traitée par l'instance de Citrix ADC. Les données d'analyse vous permettent d'analyser les performances des instances Citrix ADC, de l'application, de l'URL, du client et du serveur dans votre environnement.

Voici quelques-uns des cas d'utilisation que vous pouvez afficher les données à l'aide de Web Insight :

- La liste des clients qui connaissent une latence élevée lors de l'accès à une application telle que SharePoint
- La meilleure application qui a eu le plus de succès en une heure
- La liste des applications et des URL accessibles depuis les clients
- Le système d'exploitation et le navigateur utilisés par un client particulier
- Applications ou serveurs qui envoient le plus de réponses liées aux erreurs
- Problèmes d'accessibilité avec un client particulier
- Problèmes d'accessibilité pour une partie ou l'ensemble des applications d'un client particulier
- Peu de pages d'une application sont lentes à partir d'un client particulier et d'un serveur backend
- L'application est lente lorsqu'elle est accessible à partir d'un client particulier et d'un serveur principal

Vous pouvez activer Web Insight pour un serveur virtuel spécifique sur une instance sélectionnée afin de surveiller le trafic sur votre application Web. La fonctionnalité Web Insight fournit ensuite des statistiques pour le serveur virtuel dans Citrix ADM.

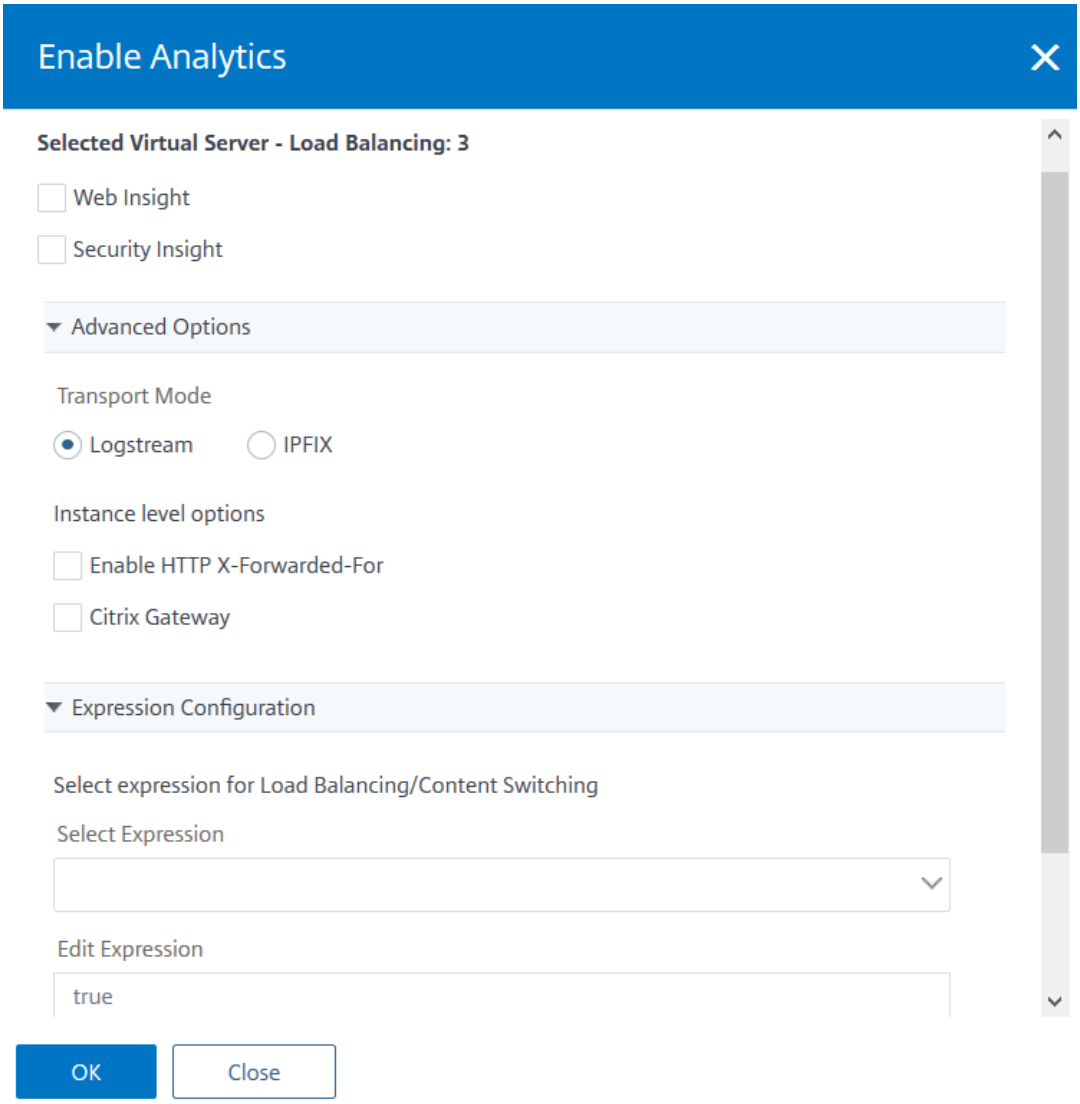
Pour activer Web Insight :

Si votre Citrix ADM est **13.0 Build 41.x ou version ultérieure** :

1. Accédez à **Réseaux** > **Instances** > **Citrix ADC**, puis sélectionnez le type d'instance. Par exemple, VPX.
2. Sélectionnez l'instance et dans la liste **Sélectionner une action**, cliquez sur **Configurer Analytics**.
3. Dans la page **Configurer l'analyse sur les serveurs virtuels**, sélectionnez le serveur virtuel, puis cliquez sur **Activer l'analyse**.
4. Dans la fenêtre **Activer Analytics** :
   a) Sélectionnez **Web Insight**
   b) Sélectionnez **Logstream** comme mode de transport

      > **Remarque**
      >
      > Pour Citrix ADC 12.0 ou version antérieure, **IPFIX** est l'option par défaut pour le mode de transport. Pour Citrix ADC 12.0 ou version ultérieure, vous pouvez sélectionner **Logstream** ou **IPFIX** comme mode de transport.
      >
      > Pour plus d'informations sur IPFIX et Logstream, consultez la section Présentation de Logstream .

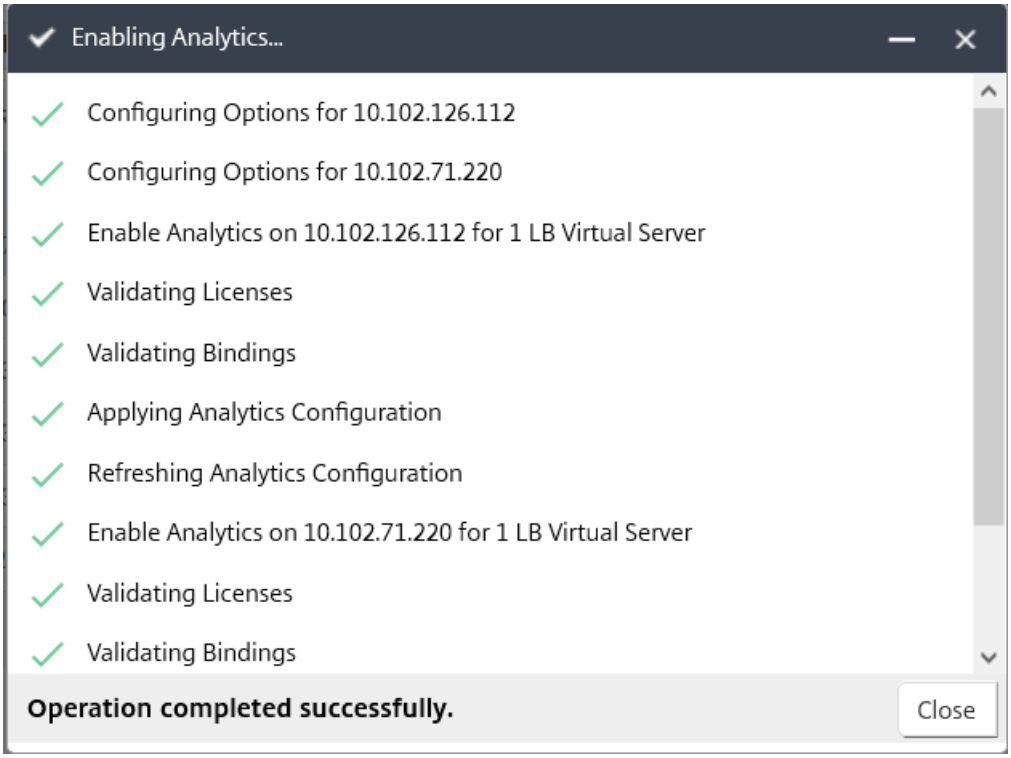
   c) L'expression est true par défaut
   d) Cliquez sur **OK**.



Remarque

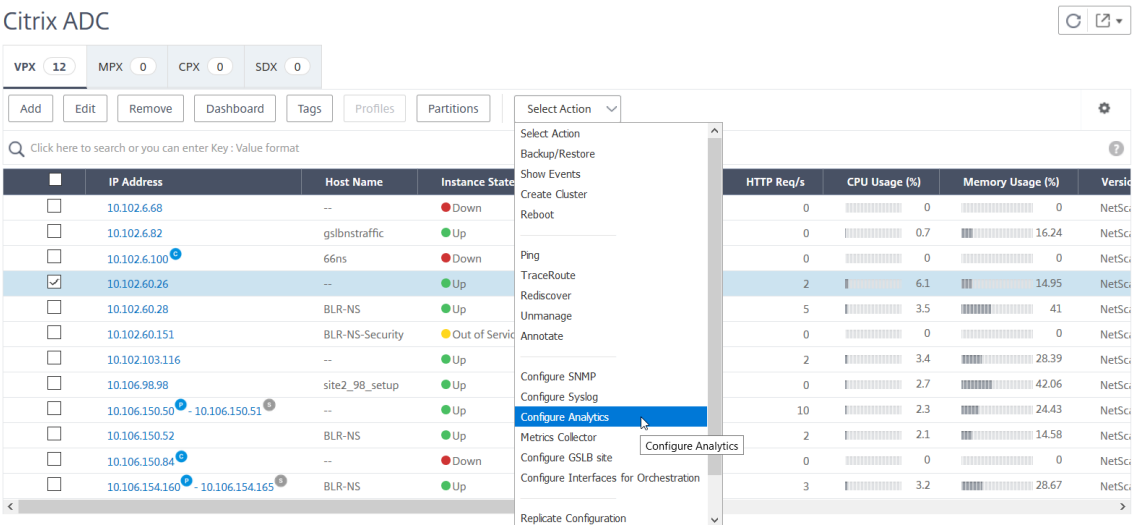
- Si vous sélectionnez des serveurs virtuels qui ne sont pas sous licence, Citrix ADM octroie d'abord des licences à ces serveurs virtuels, puis active les analyses
- Pour les partitions d'administration, seul **Web Insight** est pris en charge
- Pour les serveurs virtuels tels que la redirection du cache , l'authentification et le GSLB , vous ne pouvez pas activer les analyses. Un message d'erreur s'affiche.

Après avoir cliqué sur **OK**, Citrix ADM traite pour activer les analyses sur les serveurs virtuels sélectionnés.



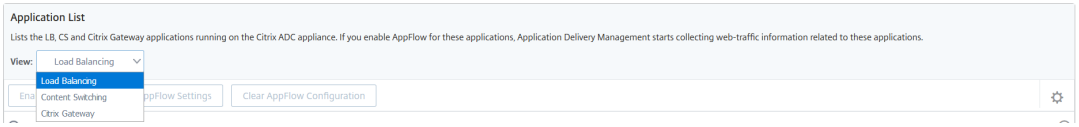
Si votre Citrix ADM est **13.0 Build 36.27 ou une version antérieure** :

1. Accédez à **Réseaux** > **Instances** > **Citrix ADC**, puis sélectionnez l'instance Citrix ADC sur laquelle vous souhaitez activer l'analyse.
2. Dans la liste **Sélectionner une action**, sélectionnez **Configurer Analytics**.

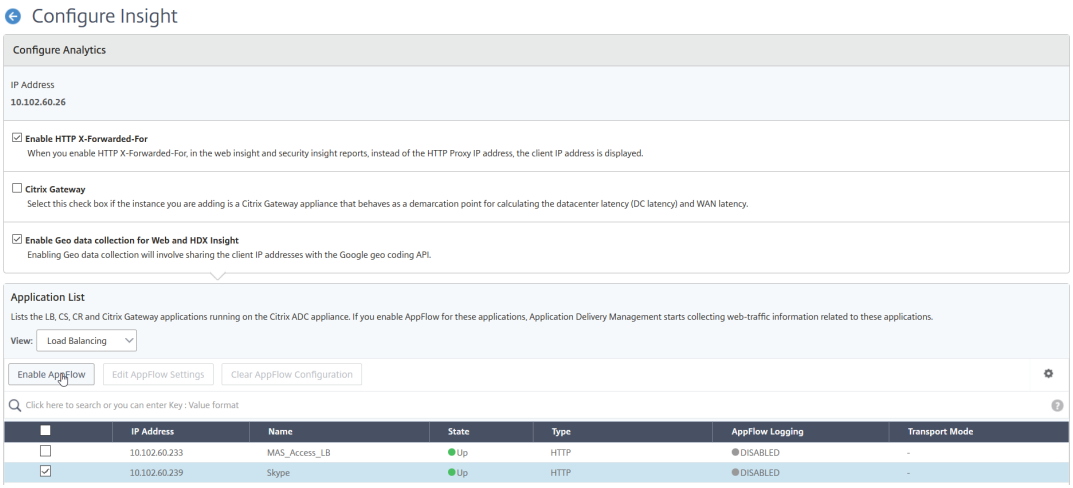


3. Sur la page **Configurer Insight** :

   a) Sélectionnez la **liste des applications** pour l'équilibrage de charge ou la commutation de contenu.



b) Sélectionnez le serveur virtuel et cliquez sur **Activer AppFlow**.

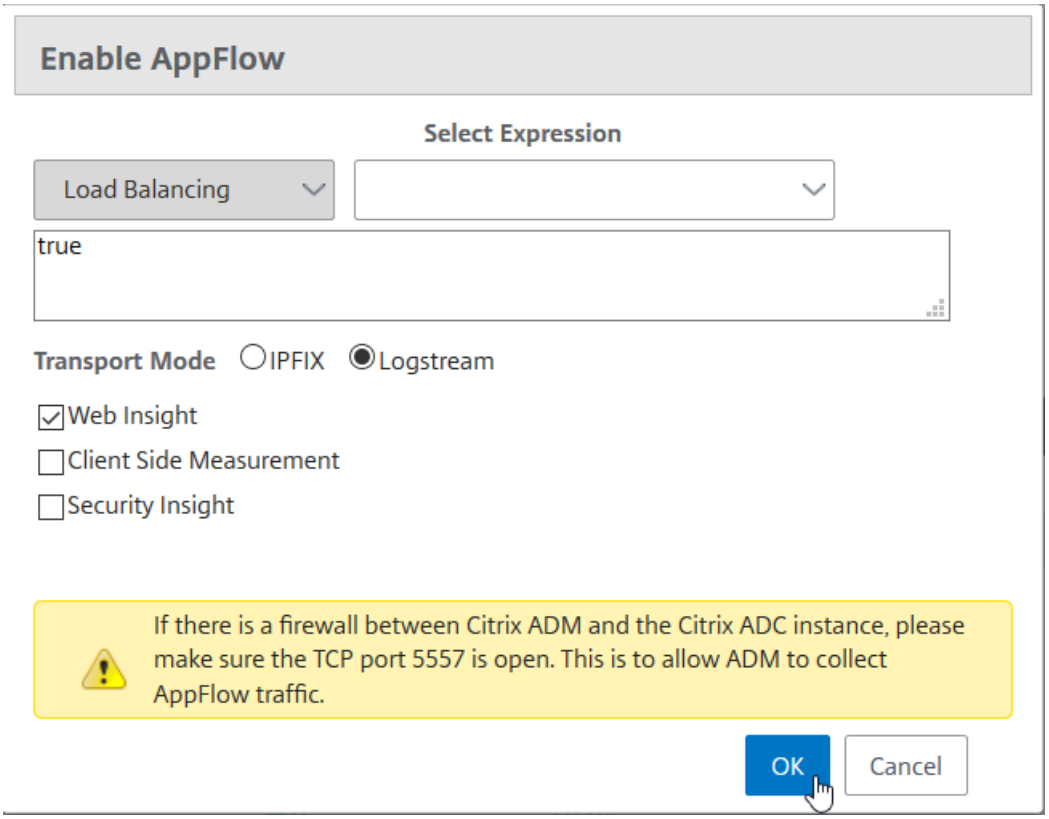


4. Dans la boîte de dialogue Activer AppFlow :

   - Entrez **true** dans la zone de texte
   - Sélectionnez **Logstream** comme mode de transport

     > Remarque : Citrix vous recommande de sélectionner Logstream comme mode de transport.

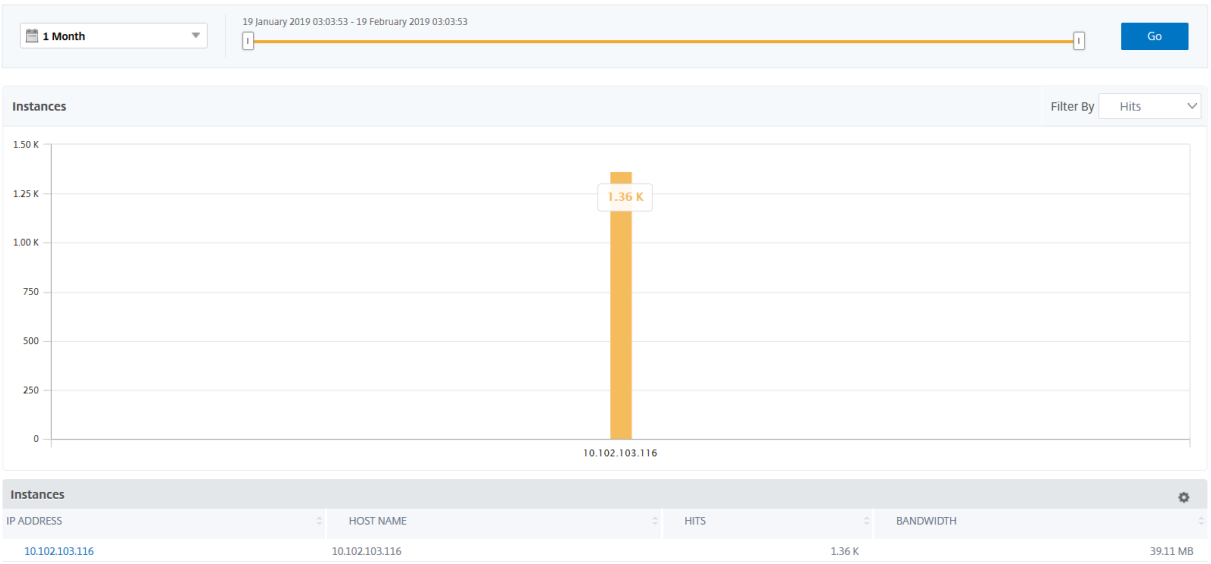
   - Sélectionnez **Web Insight** et cliquez sur **OK**.



Analyser les problèmes liés aux applications Web

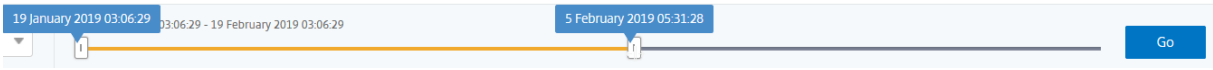
L'un des problèmes courants qu'un administrateur doit identifier est les problèmes de latence. En tant qu'administrateur, vous devez déterminer si le problème de latence provient du réseau serveur, du réseau client ou du temps de réponse du serveur. À l'aide de Citrix ADM, vous pouvez identifier ces informations en accédant à **Analytics** > **Web Insight** .

Lorsque vous accédez à **Analytics** > **Web Insight**, il affiche les instances Citrix ADC activées avec Web Insight. Vous pouvez afficher les informations détaillées pour les instances telles que l'adresse IP, le nom d'hôte, le nombre total d'accès et la bande passante.



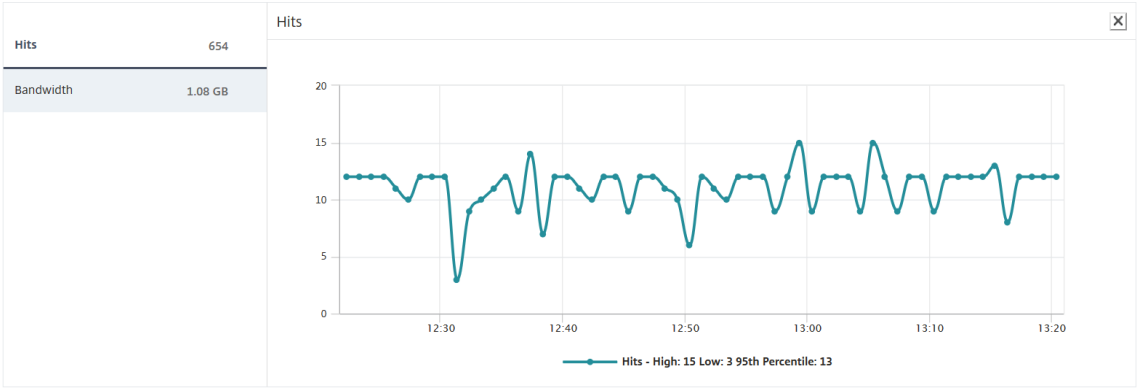
À l'aide de la liste, vous pouvez sélectionner la durée pour afficher les informations relatives aux instances.

Vous pouvez également utiliser le curseur pour personnaliser la durée du temps et cliquer sur **Aller** pour afficher les résultats.

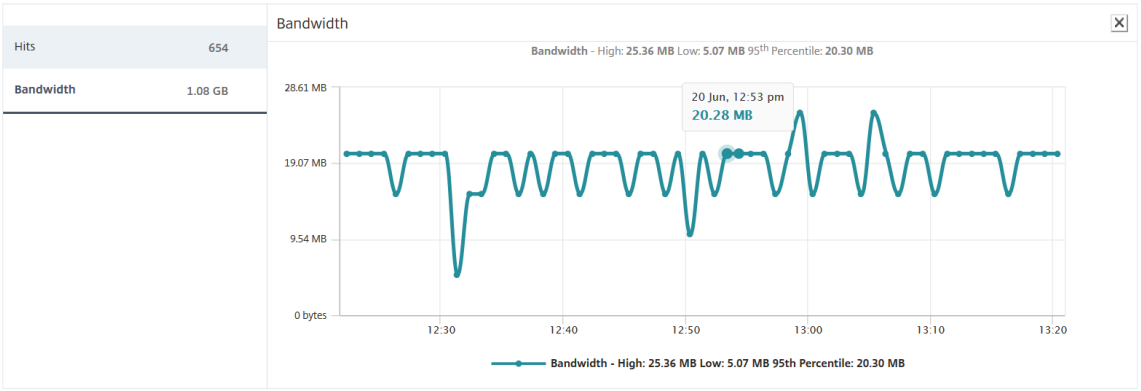


Lorsque vous cliquez sur le graphique ou l'adresse IP de l'instance, les informations détaillées sur l'instance s'affichent. Vous pouvez afficher des informations sur les éléments suivants :

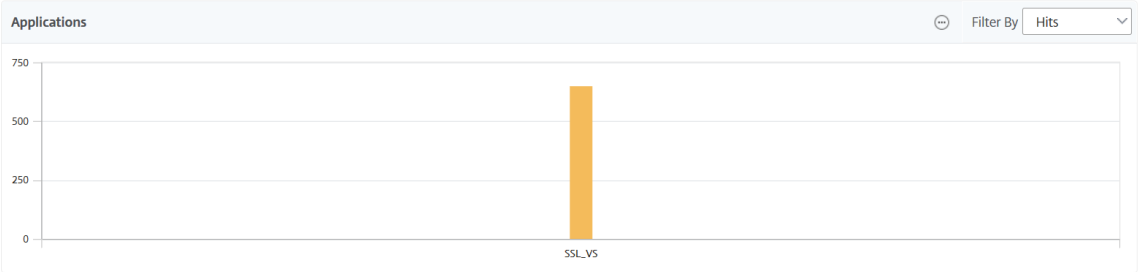
- **Nombre total de visites**



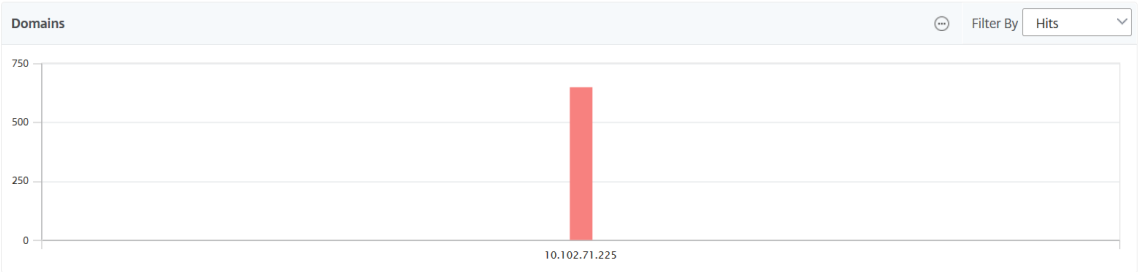
- **Bande passante**



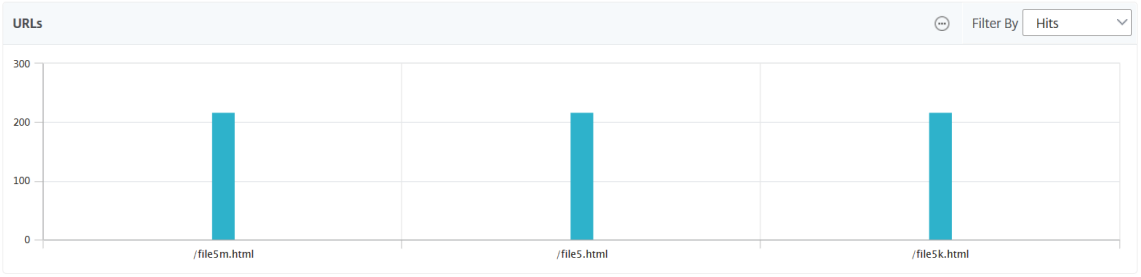
- **Applications**



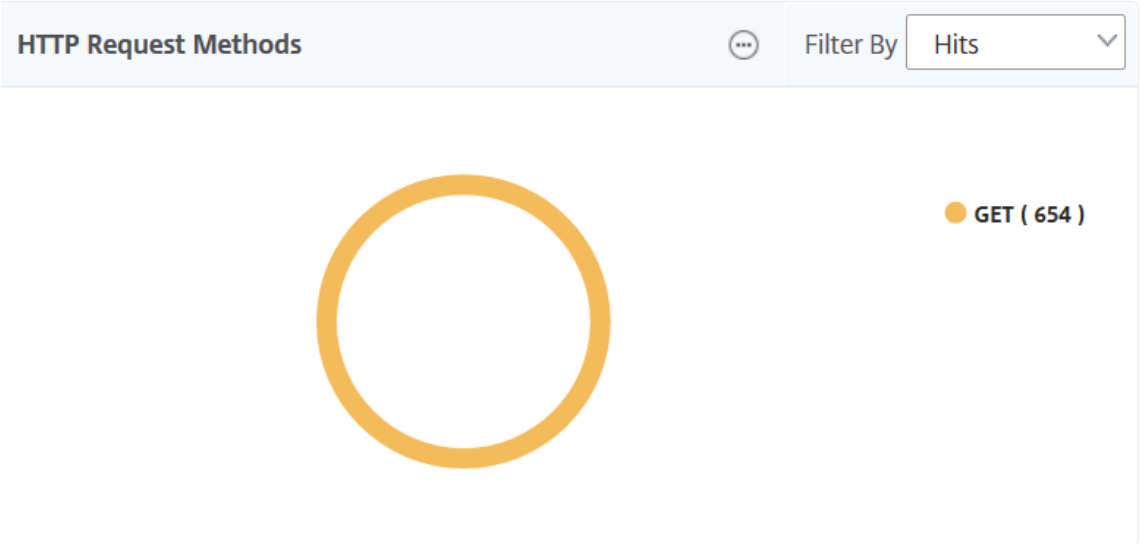
- **Domaines**



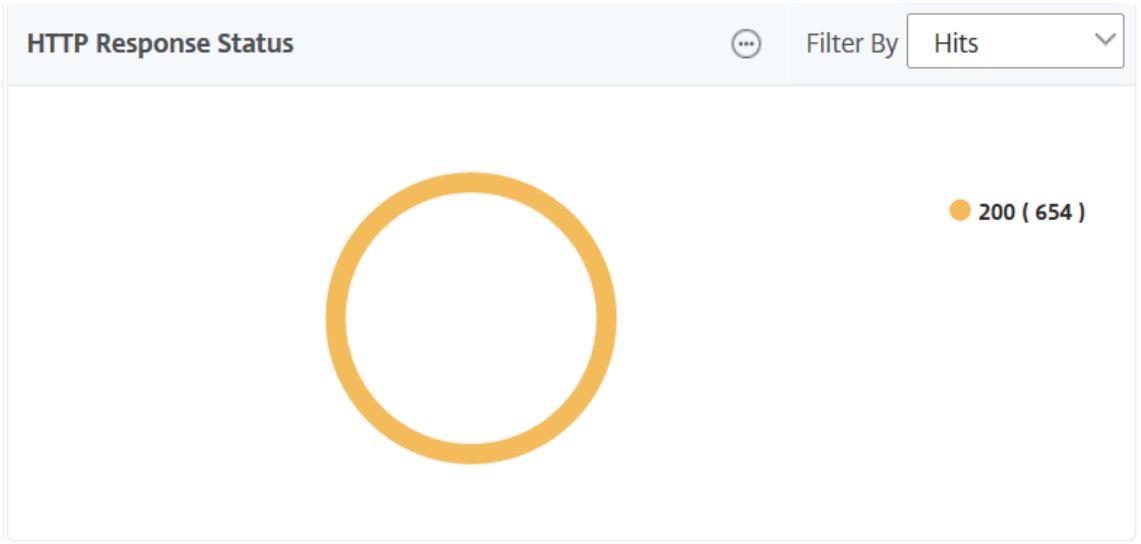
- **URL**



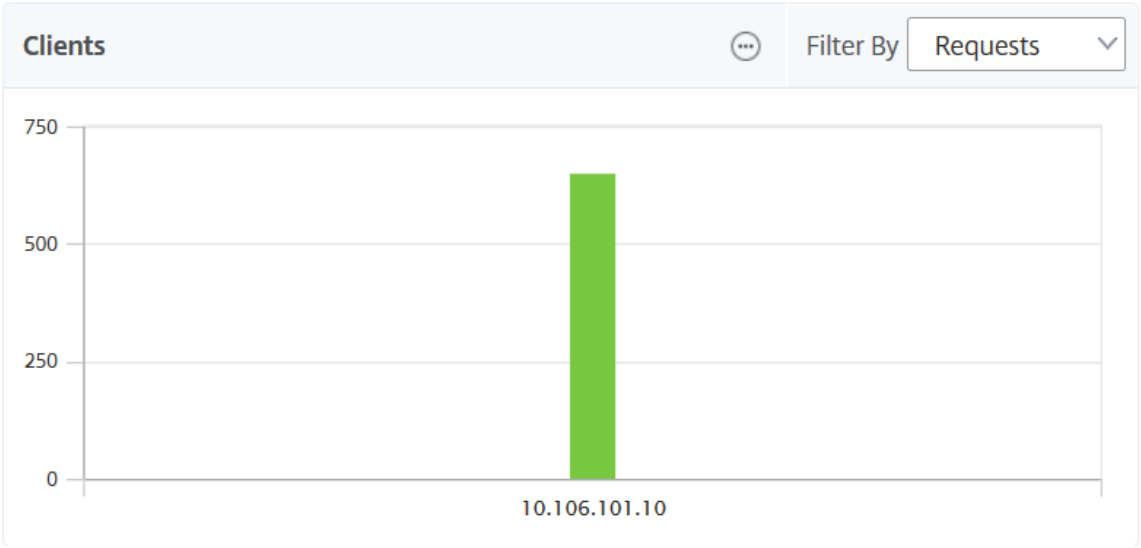
- **Méthodes de requête HTTP**



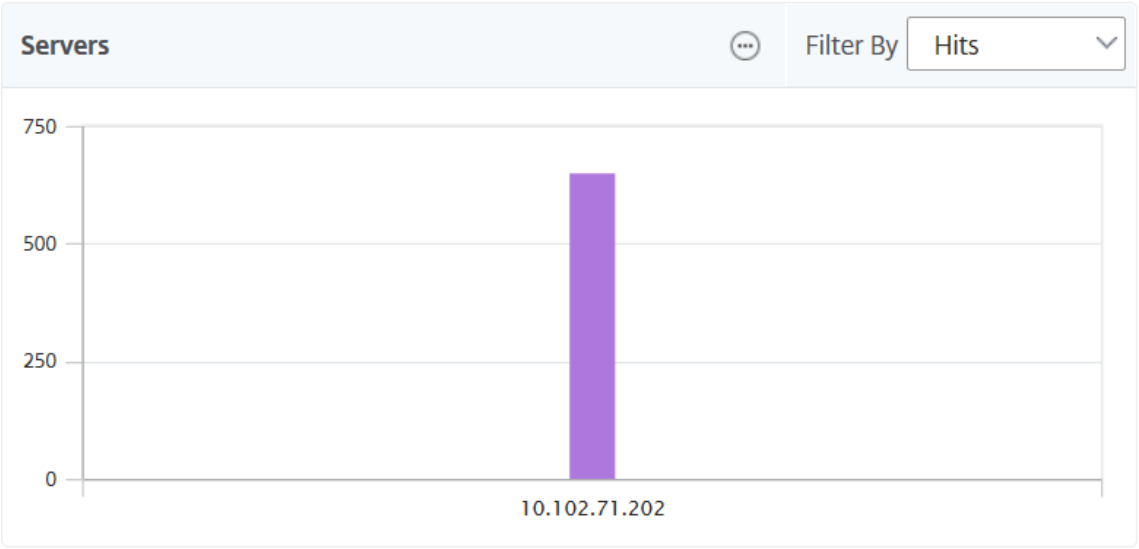
- **État de la réponse HTTP**



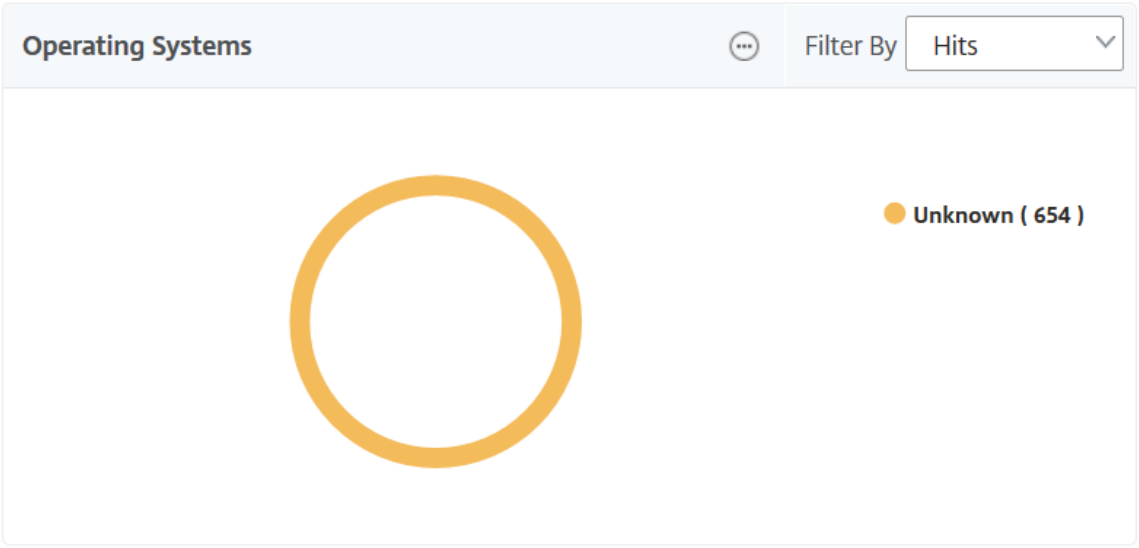
- **Clientèle**



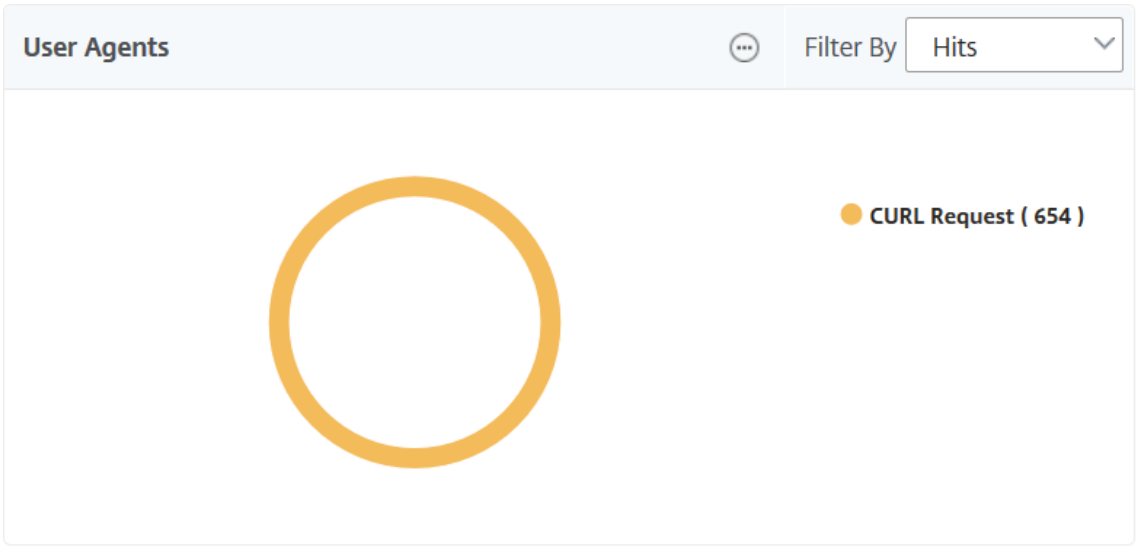
- **Serveurs**



- **Systèmes d'exploitation**

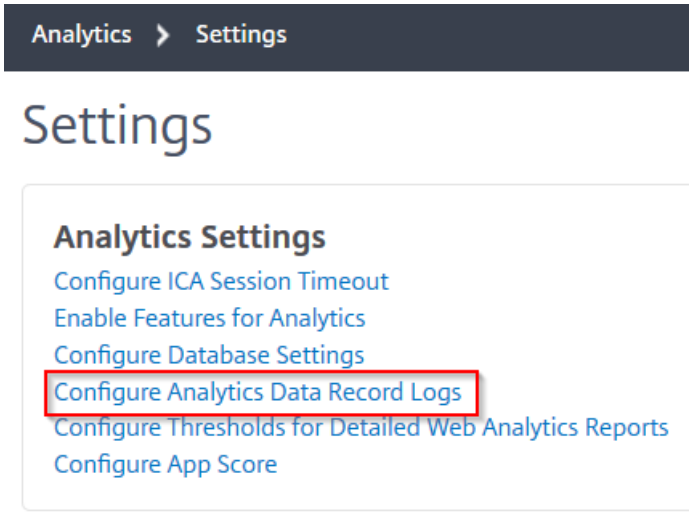


- **Agents utilisateur**

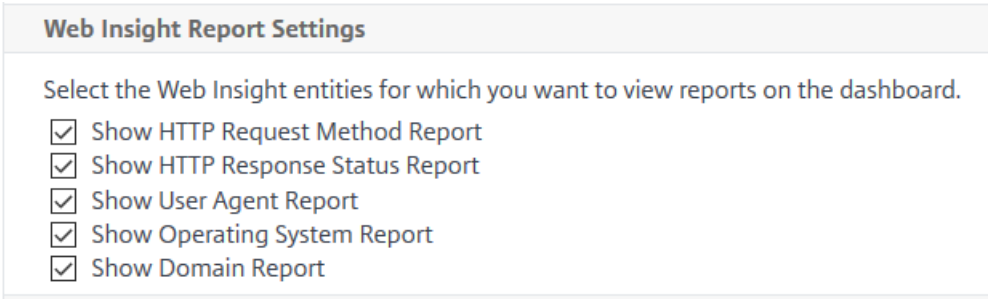


Vous pouvez également sélectionner **des entités Web Insight** pour lesquelles vous souhaitez afficher des rapports sur l'interface graphique.

1. Accédez à **Analytics** > **Web Insight** > **Paramètres** .
2. Cliquez sur **Configurer les journaux des enregistrements de données Analytics**.



3. Sous **Paramètres de rapport Web Insight**, sélectionnez les entités que vous souhaitez afficher des rapports sur l'interface graphique.



4. Cliquez sur **OK**.

Pour effectuer une analyse plus poussée, vous pouvez cliquer sur chaque catégorie d'informations sous Web Insight dans l'interface graphique. Par exemple, si vous souhaitez vérifier les problèmes pour les serveurs configurés :

1. Accédez à **Analytics** > **Web Insight** > **Serveurs**.
2. La page Serveurs s'affiche avec tous les serveurs configurés.
3. Cliquez sur l'adresse IP du graphique. Vous pouvez également cliquer sur l'adresse IP dans le tableau.

La vue d'aperçu détaillée du serveur sélectionné s'affiche. Dans cette vue, vous pouvez rechercher plusieurs informations telles que :

- Nombre total de visites reçues par le serveur
- Bande passante
- Délai de traitement du serveur
- Latence réseau du serveur
- Serveurs virtuels configurés pour le serveur
- Nombre total de clients accédant au serveur
- Nombre total de codes de réponse fournis par le serveur

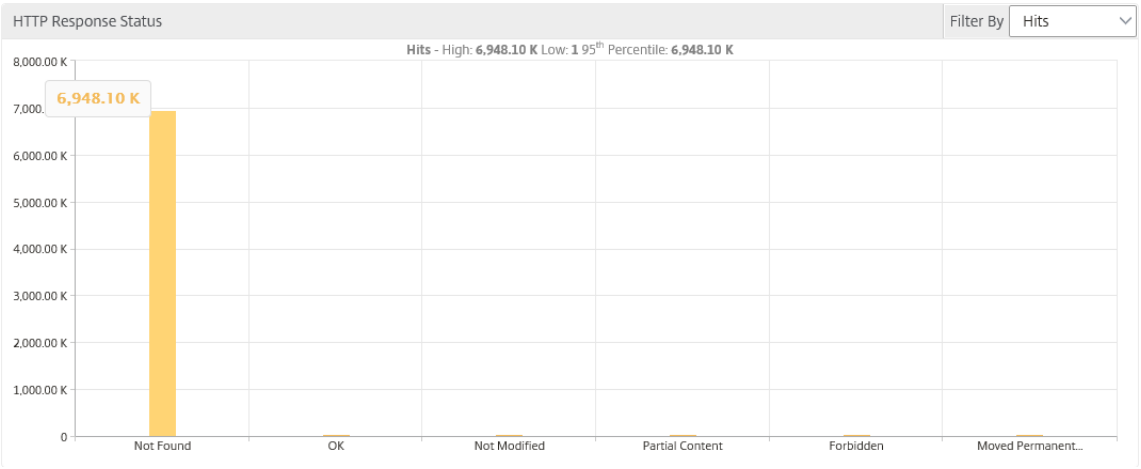
Cas d'utilisation 1 - Erreur interne du serveur

Considérez un scénario selon lequel vos utilisateurs rencontrent une erreur d'inaccessibilité 500 pour votre application Web. L'erreur 500 (introuvable) est une erreur d'état de réponse HTTP qui indique un problème sur le serveur Web, mais le serveur n'indique pas le problème explicitement. Pour identifier et analyser le problème réel :

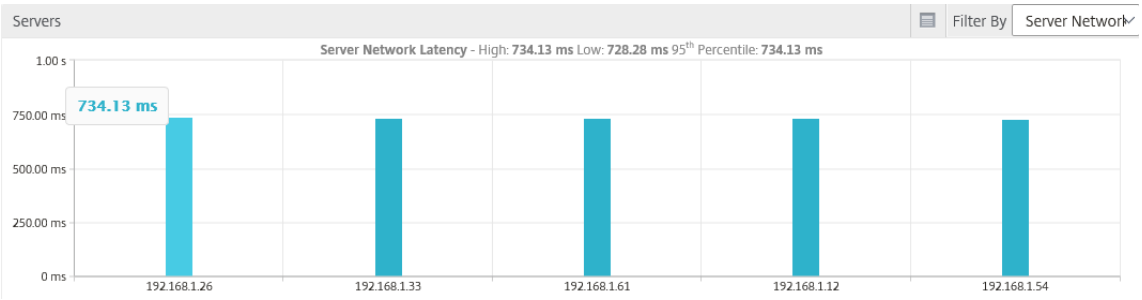
1. Accédez à **Analytics** > **Web Insight** > **État des réponses**.

   La page du tableau de bord s'affiche. Le tableau de bord fournit les mesures que vous pouvez utiliser pour analyser le succès et l'échec des transactions HTTP traitées.

2. Cliquez sur **Non trouvé** dans le graphique.



3. Faites défiler vers le bas pour afficher le **graphique Serveurs**et, dans la liste **Filtrer par**, sélectionnez **Latence réseau du serveur**.



Le graphique indique que chaque serveur d'applications a rencontré un problème lors de la récupération de l'application Web et donc le temps de réponse pour le serveur Web est augmenté. Le problème peut être lié au fait que le serveur Web ne répond à aucune demande d'un serveur.

Cas d'utilisation 2 - L'utilisateur connaît une lenteur dans l'accès à l'application Web

Considérez un scénario selon lequel votre application Web est hébergée par 10 serveurs Web différents. Lorsque plusieurs utilisateurs accèdent à l'application en même temps, un ou plusieurs utilisateurs peuvent rencontrer une lenteur de l'application. En tant qu'administrateur, vous devez analyser les scénarios suivants pour comprendre la cause première du problème :

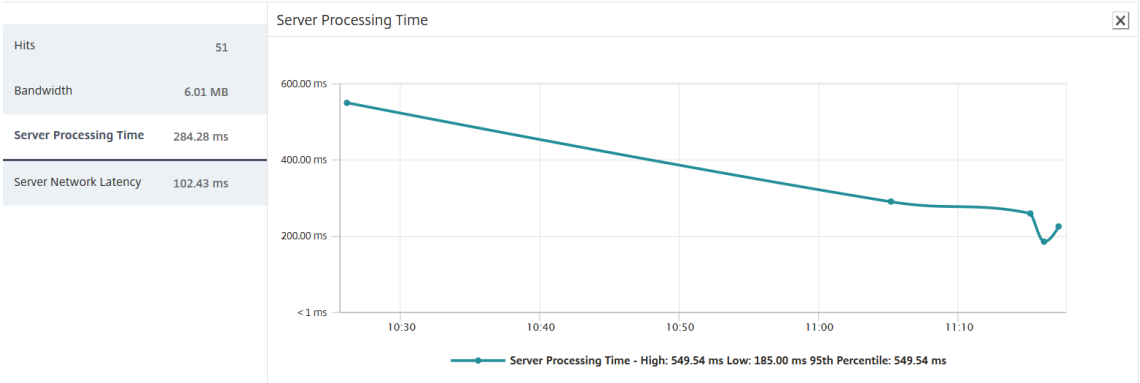
Scénario 1 - Temps de traitement du serveur :

Lorsque plusieurs requêtes touchent les 10 serveurs Web en même temps, le temps nécessaire pour charger la requête diffère en fonction de :

- Nombre de demandes dans la file d'attente.
- Bande passante consommée par chaque requête pour traiter la transaction HTTP.

Le graphique du serveur peut vous aider à comprendre le temps de traitement de chaque serveur pour la demande traitée par les serveurs. De même, le graphique de l'application affiche les accès, le temps de réponse et la bande passante consommée par chaque transaction HTTP.

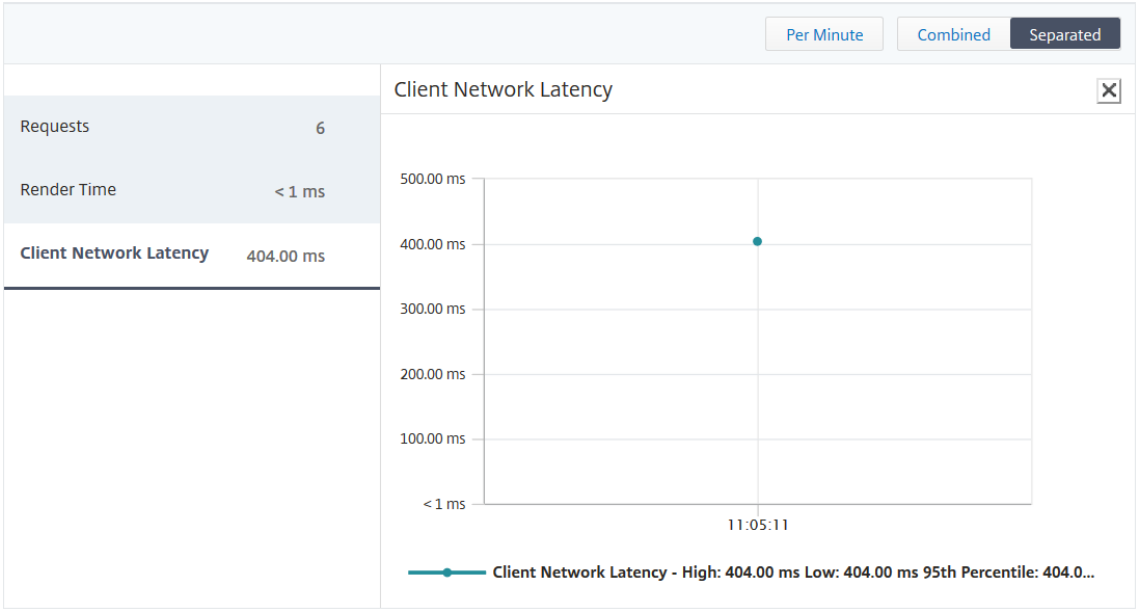
1. Accédez à **Analytics** > **Web Insight** > **Serveurs**.
2. Sélectionnez le serveur dans le graphique.
3. Cliquez sur **Temps de traitement du serveur** pour analyser le temps de traitement du serveur.



Scénario 2 - Latence du client :

Le temps de réponse et le nombre total d'accès pour l'application peuvent être la raison de la lenteur de l'accès à l'application. Vous pouvez vérifier la latence du réseau client et analyser les mesures de latence du réseau client. Pour analyser la cause première :

1. Accédez à **Analytics** > **Web Insight** > **Clients** .
2. Sélectionnez le client dans le graphique.
3. Cliquez sur **Latence réseau client** pour analyser la latence élevée.



Dans cet exemple, en tant qu'administrateur, vous pouvez voir que la cause principale du problème provient du réseau client car la latence du réseau client indique un niveau élevé.

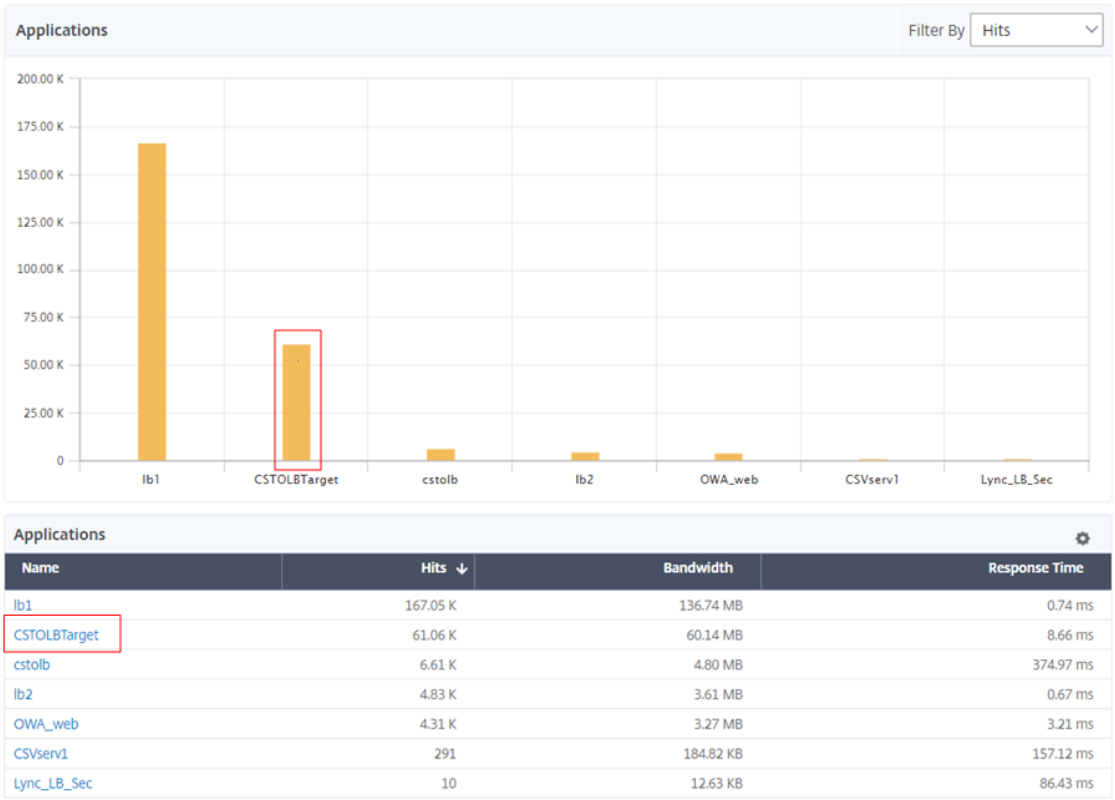
Cas d'utilisation 3 - Lenteur dans l'accès à l'application Web

Considérez un scénario selon lequel vous disposez de serveurs Web pour les utilisateurs Windows et de serveurs Web pour les utilisateurs Mac, et vos utilisateurs signalent une lenteur dans l'accès à l'application Web. En tant qu'administrateur, vous savez que vous avez :

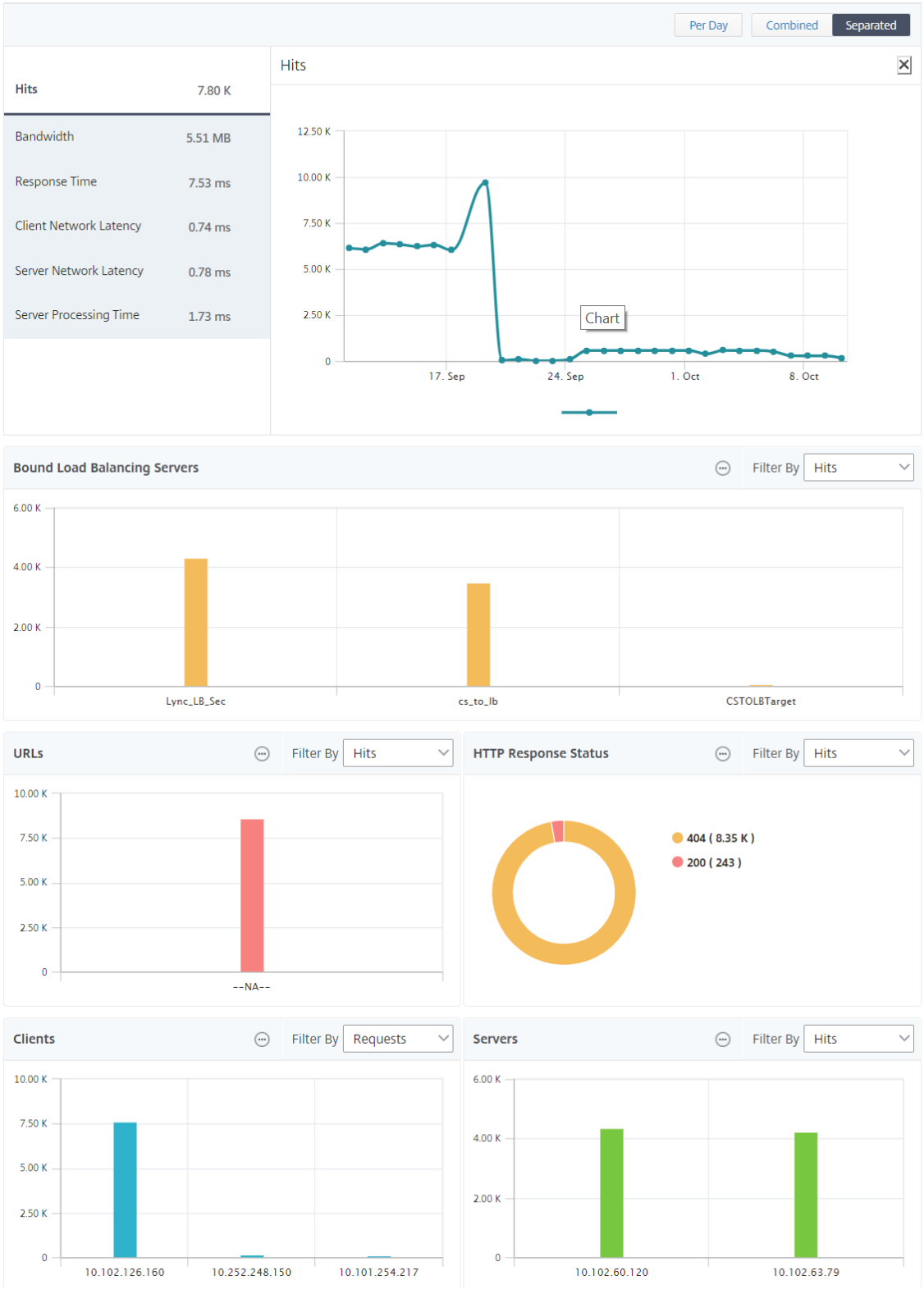
- Configuration d'un serveur virtuel de commutation de contenu pour les utilisateurs Windows.
- Configuration d'un serveur virtuel de commutation de contenu pour les utilisateurs Mac.
- Configuration des services associés liés aux serveurs virtuels pour rediriger les demandes basées sur les utilisateurs Windows et Mac.

Pour analyser la cause première du problème de lenteur de l'application Web :

1. Accédez à **Analytics** > **Web Insight** > **Applications**
2. Sélectionnez le serveur virtuel de commutation de contenu.
   Par exemple, l'application « CStolbTarget » dans l'image est un serveur virtuel de commutation de contenu lié à d'autres serveurs virtuels d'équilibrage de charge



3. Cliquez sur le serveur virtuel de commutation de contenu pour afficher l'autre serveur virtuel d'équilibrage de charge. Vous pouvez également cliquer sur le nom de l'application dans le tableau.



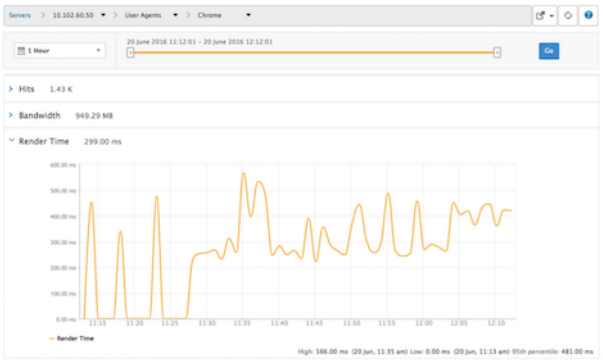
Vous pouvez également cliquer sur les serveurs d'équilibrage de charge liés pour afficher les détails Web Insight de ces applications.

Analyser des informations pour les navigateurs et les systèmes d'exploitation

Vous pouvez utiliser Web Insight pour vous aider à séparer les problèmes de latence L7 et à comprendre l'utilisation des appareils mobiles. En tant qu'administrateur, les informations peuvent vous aider à comprendre les différentes prises de système d'exploitation au sein de votre base d'utilisateurs.

Accédez à **Analytics** > **Web Insight** > **Système d'exploitation** pour voir pourquoi l'accès des utilisateurs est lent et si cela est dû à une incompatibilité entre certains navigateurs. Vous pouvez également voir quels systèmes d'exploitation sont utilisés sur certains clients et quels navigateurs sont accessibles. Vous pouvez comparer le temps de rendu sur les différents navigateurs et effectuer une exploration vers le bas à un navigateur particulier pour identifier les pages d'application qui sont associées au temps de rendu le plus élevé pour ce navigateur.

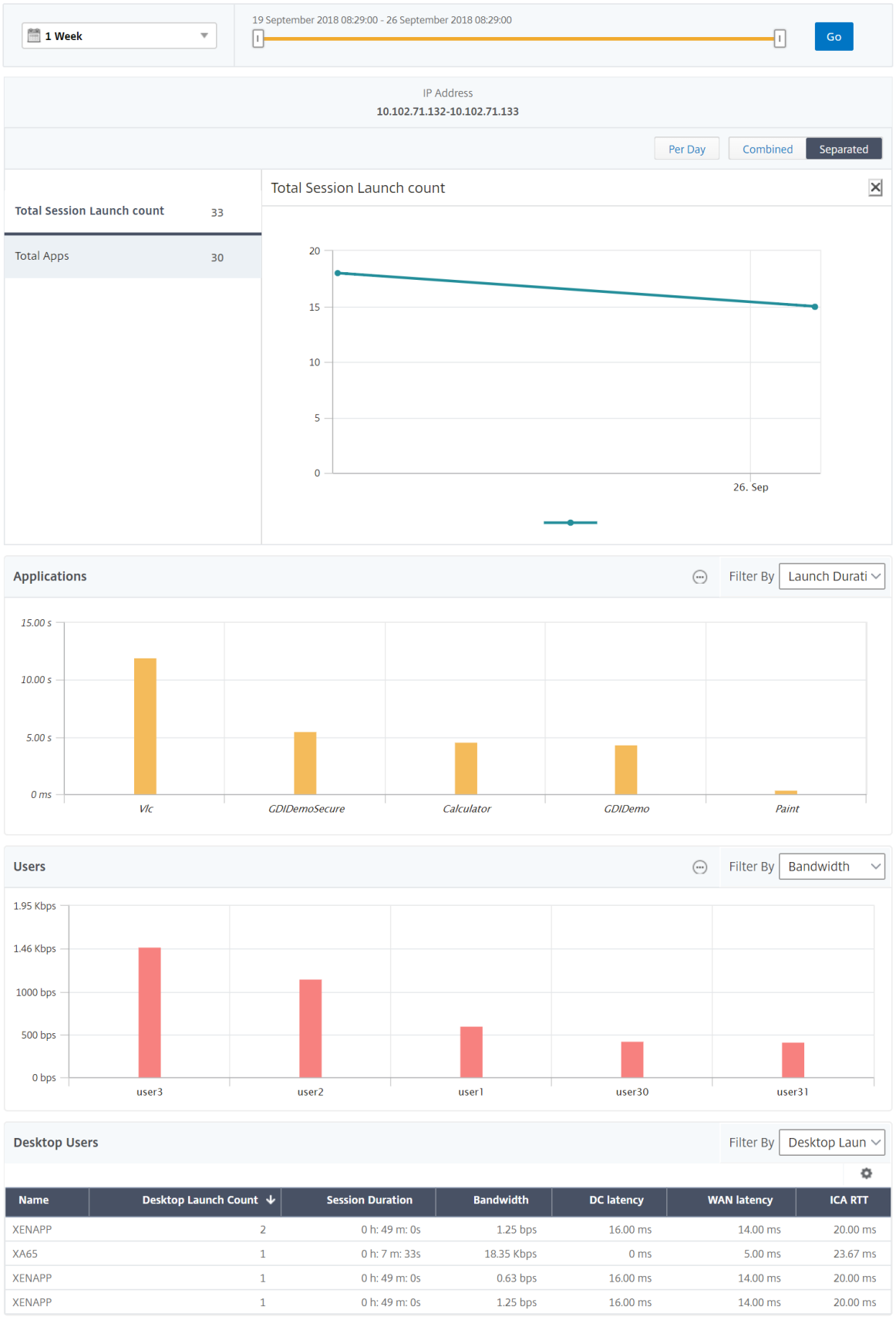
Par exemple, vous pouvez sélectionner **Google Chrome** et voir les temps de rendu correspondants pour les différentes pages URL d'une application particulière.



Instances Citrix ADC déployées en mode haute disponibilité

Citrix ADM fournit des rapports pour les instances ADC déployées en mode haute disponibilité. Les rapports agrégés pour les instances en mode haute disponibilité sont pris en charge dans toutes les analyses.

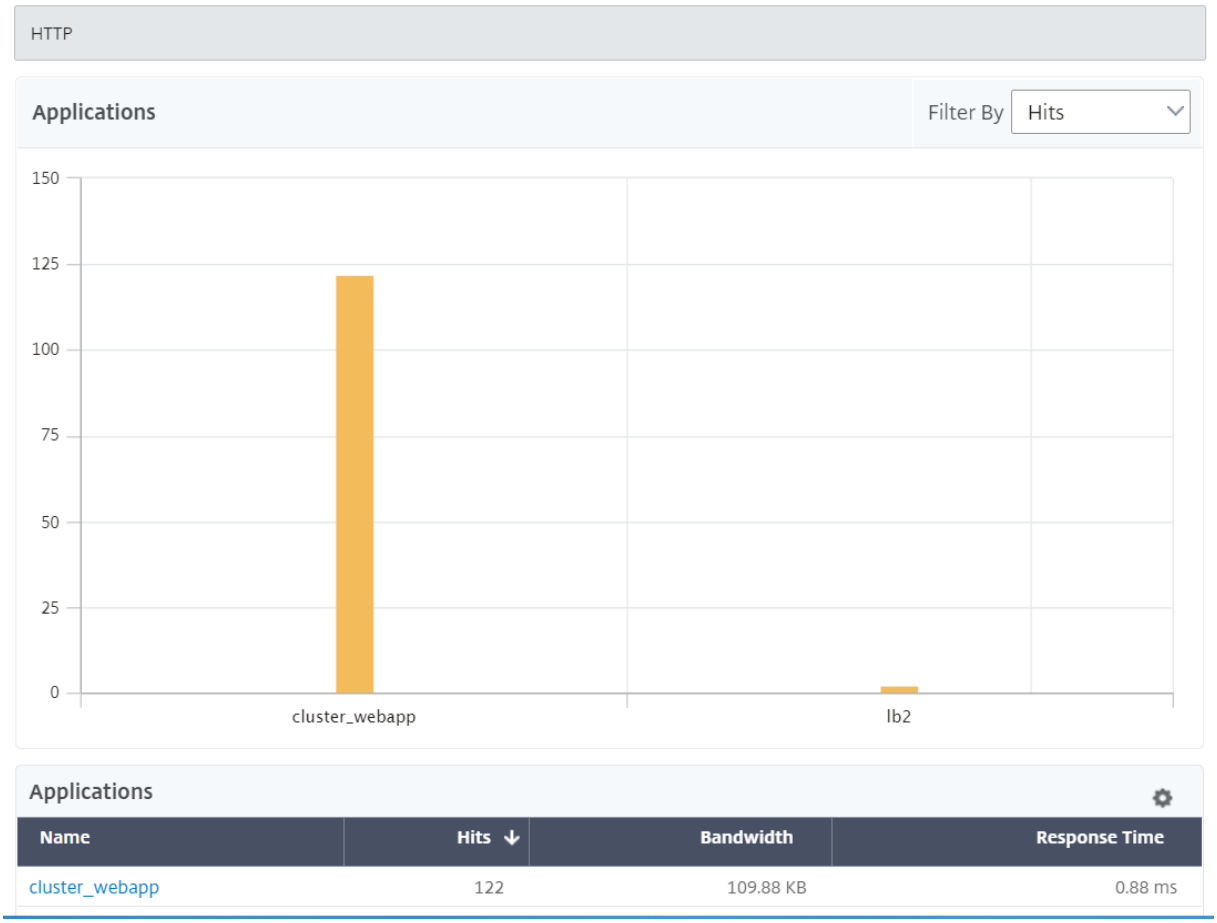
Vous pouvez cliquer sur le nom des instances qui sont en haute disponibilité pour afficher plus de détails.



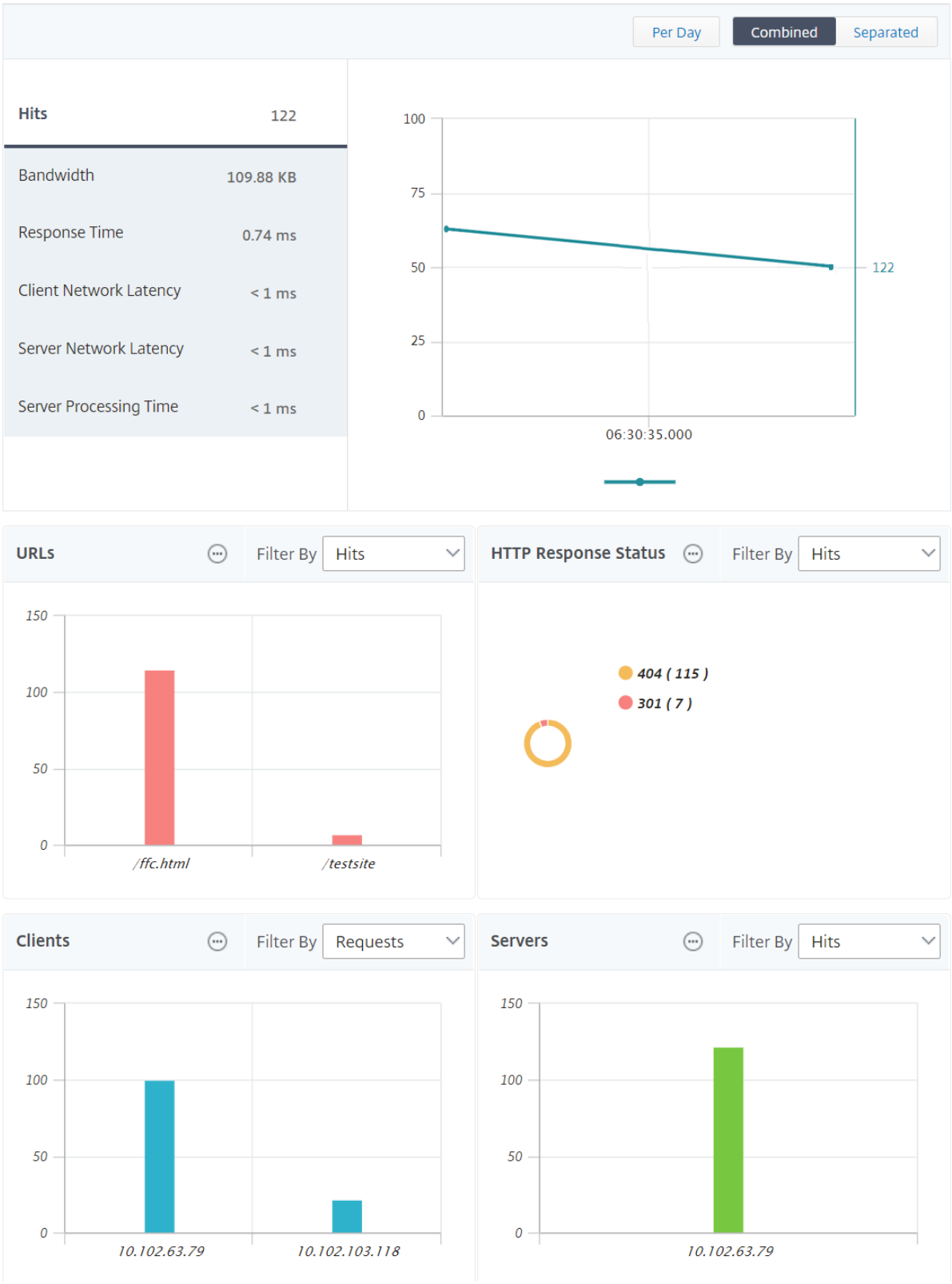
Name	Desktop Launch Count	Session Duration	Bandwidth	DC latency	WAN latency	ICA RTT
XENAPP	2	0 h: 49 m: 0s	1.25 bps	16.00 ms	14.00 ms	20.00 ms
XA65	1	0 h: 7 m: 33s	18.35 Kbps	0 ms	5.00 ms	23.67 ms
XENAPP	1	0 h: 49 m: 0s	0.63 bps	16.00 ms	14.00 ms	20.00 ms
XENAPP	1	0 h: 49 m: 0s	1.25 bps	16.00 ms	14.00 ms	20.00 ms

Instances Citrix ADC déployées en mode cluster

Citrix ADM fournit des rapports pour les instances ADC déployées en mode cluster. Les rapports agrégés pour les instances en mode cluster sont pris en charge dans toutes les analyses.



Vous pouvez également cliquer sur le **nom d'hôte CLIP** pour afficher tous les détails sur les instances ADC déployées en mode cluster.



> **Remarque**
>
> - Toutes les données précédemment collectées avant la mise à niveau vers Citrix ADM 12.1 build 503.x restent affichées en tant que rapports indépendants pendant la période jusqu'à ce que les données persistent.
> - Pour les instances ADC déployées en mode cluster, l'ID de domaine d'observation/les noms de domaine d'observation sont remplacés par le nom d'hôte CLIP et CLIP. Toutes les données précédemment collectées continuent de déclarer l'ID de domaine d'observation/nom de domaine d'observation.

Configuration de la carte géographique Web Insight

La fonctionnalité Geomaps de Citrix ADM affiche l'utilisation des applications Web sur différents emplacements géographiques sur une carte. Les administrateurs peuvent utiliser ces informations pour comprendre les tendances de l'utilisation des applications et pour la planification des capacités.

Geo map fournit des informations sur les mesures suivantes spécifiques à un pays, un état et une ville :

- Nombre total de visites : nombre total d'accès à une application.
- Bande passante : bande passante totale consommée lors du traitement des demandes des clients
- Temps de réponse : Temps moyen nécessaire pour envoyer des réponses aux demandes des clients.

Les géomaps fournissent des informations qui peuvent être utilisées pour traiter plusieurs cas d'utilisation tels que les suivants :

- Région ayant le nombre maximal de clients accédant à une application
- Région ayant le temps de réponse le plus élevé
- Région qui consomme le plus de bande passante

Citrix ADM vous offre une option pour configurer des géomaps pour les adresses IP privées ou les adresses IP publiques.

Configurer les géomaps pour les adresses IP privées

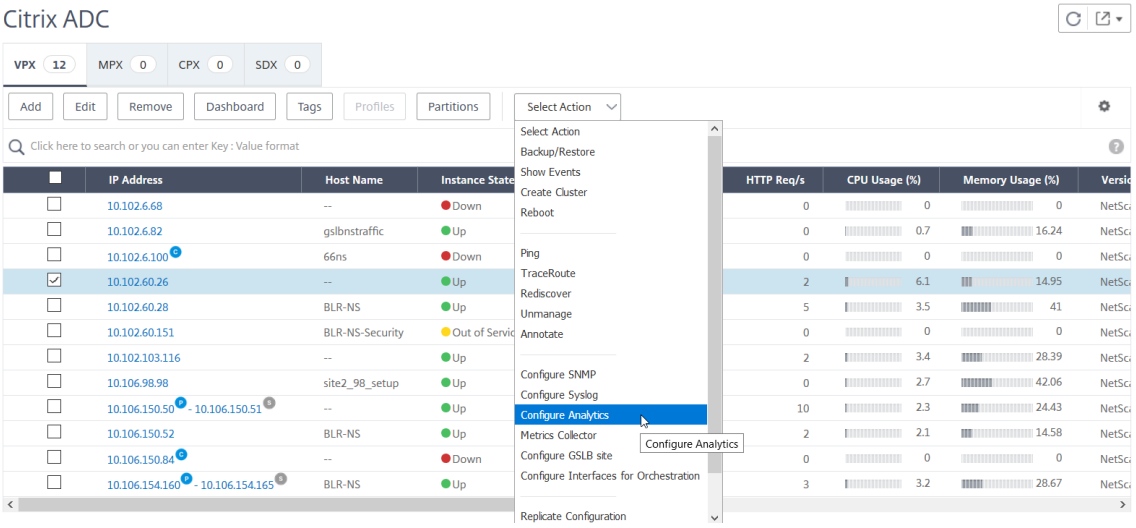
> **Remarque**
>
> La procédure suivante s'applique uniquement si votre Citrix ADM est **13.0 Build 36.27 ou une version antérieure**. Pour Citrix ADM **13.0 Build 41.x ou version ultérieure**, la collecte de don-

> nées géographiques est automatiquement activée lorsque vous activez Web Insight.

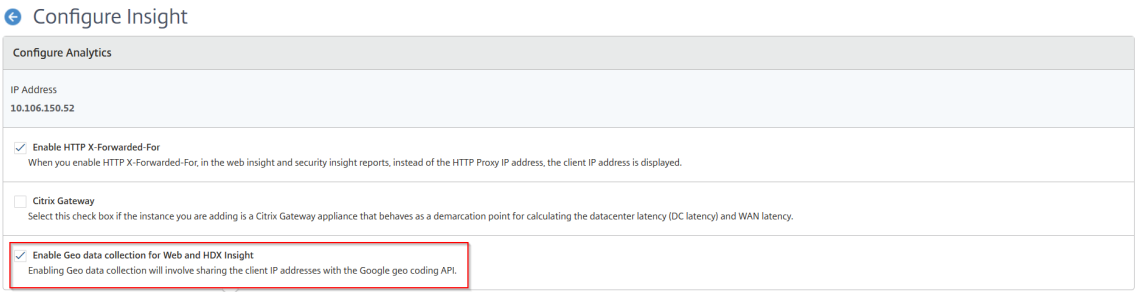
Pour afficher le trafic d'applications Web provenant d'adresses IP privées sur la carte géographique, vous devez d'abord créer des blocs d'adresses IP privées, puis activer la collecte des données géographiques.

Pour activer la collecte de données géographiques :

1. Accédez à **Réseaux** > **Instances** > **Citrix ADC**, puis sélectionnez l'instance de Citrix ADC.
2. Dans la liste **Sélectionner une action**, sélectionnez **Configurer Analytics**.



3. Sur la page **Configurer Insight**, sélectionnez **Activer la collecte de données Geo pour Web et HDX Insight** .



Créer un bloc IP privé Citrix ADM peut reconnaître l'emplacement d'un client lorsque l'adresse IP privée du client est ajoutée au serveur Citrix ADM. Par exemple, si l'adresse IP d'un client se situe dans la plage d'un bloc d'adresse IP privé associé à la ville A, Citrix ADM reconnaît que le trafic provient de la ville A pour ce client.

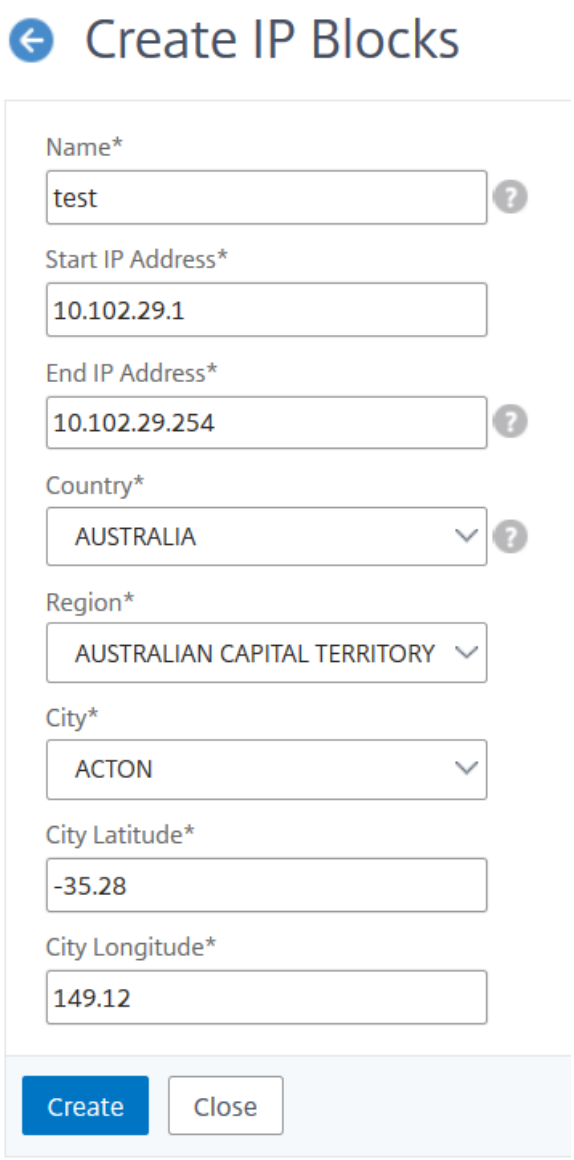
Pour créer un bloc IP :

1. Dans Citrix ADM, accédez à **Analytics** > **Paramètres** > **Blocs IP**, puis cliquez sur **Ajouter** .

2. Dans la page **Créer des blocs IP**, spécifiez les paramètres suivants :

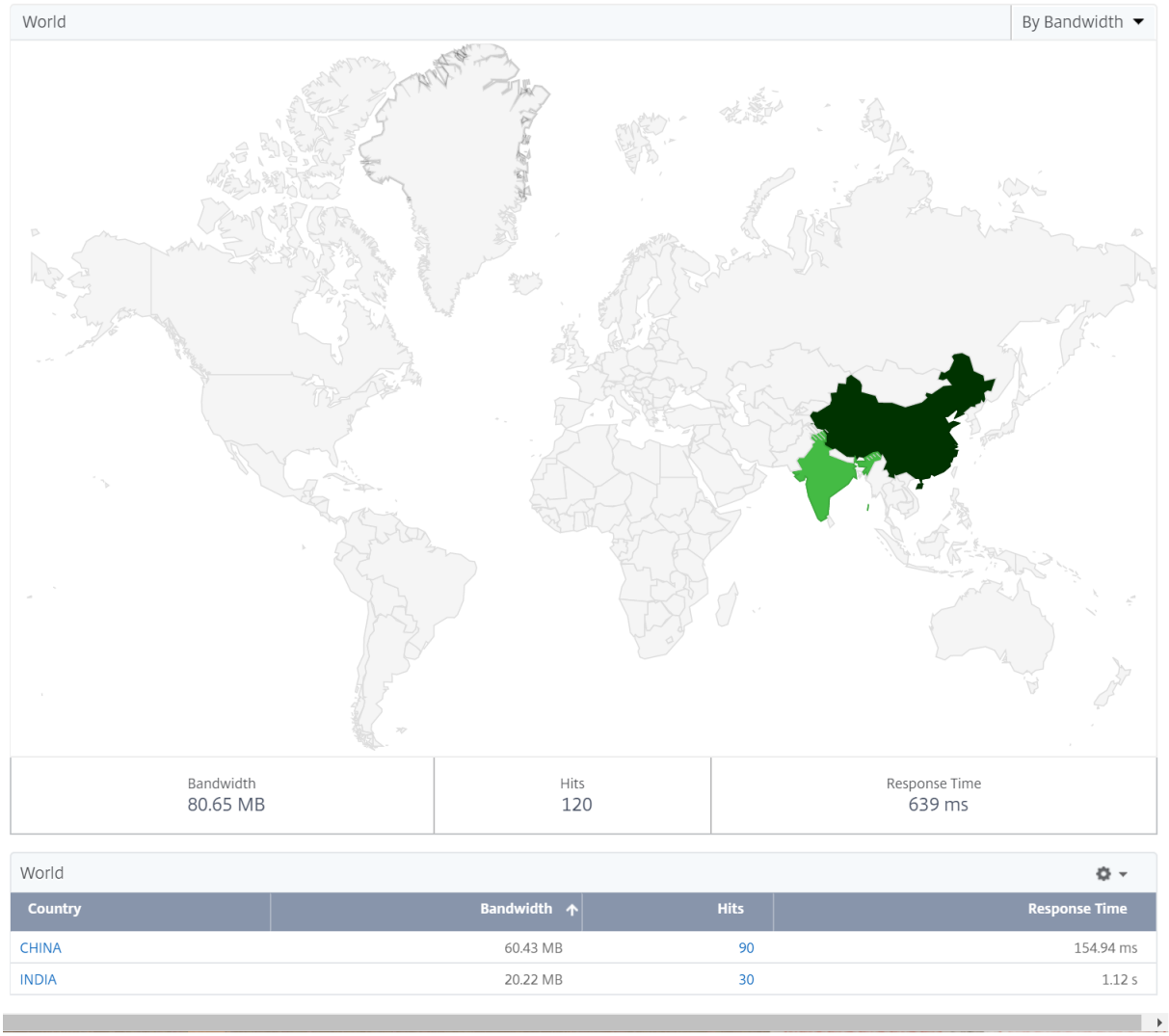
    - **Nom**. Spécifiez un nom pour le bloc d'adresses IP privées
    - **Adresse IP de départ**. Spécifiez la plage d'adresses IP la plus basse pour le bloc d'adresses IP.
    - **Adresse IP de fin**. Spécifiez la plage d'adresses IP la plus élevée pour le bloc d'adresses IP.
    - **Pays**. Sélectionnez le pays dans la liste.
    - **Région**. En fonction du pays, la région est renseignée automatiquement, mais vous pouvez sélectionner votre région.
    - **Ville**. En fonction de la région, la ville est renseignée automatiquement, mais vous pouvez sélectionner votre ville.
    - **Latitude de la ville** et **longitude de la ville**. En fonction de la ville que vous sélectionnez, la latitude et la longitude sont renseignées automatiquement.

3. Cliquez sur **Créer** pour terminer.



Blocs IP publics Citrix ADM peut également reconnaître l'emplacement d'un client si le client utilise une adresse IP publique. Citrix ADM possède son fichier CSV d'emplacement intégré qui correspond à l'emplacement basé sur la plage d'adresses IP du client. Pour utiliser le bloc IP public, la seule exigence est d'activer la collecte de **données géographiques** sur la page **Configure Insight** .

> Remarque
>
> Citrix ADM a besoin d'une connexion Internet pour afficher les géomaps d'un lieu géographique particulier. Une connexion Internet est également nécessaire pour exporter le GeoMap aux formats .pdf, .png ou .jpg.



Pour exporter le rapport de ce tableau de bord :

Pour exporter le rapport de cette page, cliquez sur l'icône **Exporter** en haut à droite de cette page. Sur la page **Exporter**, vous pouvez effectuer l'une des opérations suivantes :

1. Sélectionnez l'onglet **Exporter maintenant** . Pour afficher et enregistrer le rapport au format PDF, JPEG, PNG ou CSV.
2. Sélectionnez l'onglet **Planifier l'exportation**. Pour planifier le rapport sur une base quotidienne, hebdomadaire ou mensuelle et l'envoyer par e-mail ou par message Slack.

> **Remarque**
>
> - Si vous sélectionnez Périodicité **hebdomadaire**, veillez à sélectionner les jours de semaine pendant lesquels vous souhaitez que le rapport soit planifié.
> - Si vous sélectionnez Périodicité **mensuelle**, veillez à saisir tous les jours, séparés par des

> virgules, pendant lesquels vous voulez que le rapport soit planifié.

Configurer les seuils

Vous pouvez créer des seuils et le recevoir une notification chaque fois que la valeur seuil est franchie. Dans un déploiement classique, vous pouvez définir des seuils pour :

- Suivez les différents indicateurs des applications
- Faciliter la planification
- Recevez une notification chaque fois que la valeur métrique de l'application dépasse le seuil défini

Pour configurer le seuil :

1. Accédez à **Analytics** > **Paramètres** > **Seuils** .
2. Sur la page **Seuils**, cliquez sur **Ajouter**.

   La page **Créer un seuil** s'affiche.
3. Spécifiez les détails suivants :

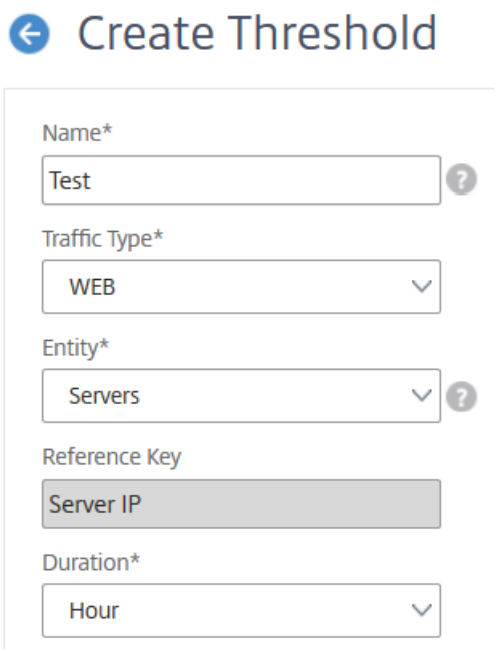
   a) **Nom** : spécifiez un nom pour créer un événement.

   b) **Type de trafic** - Dans la liste, sélectionnez WEB.

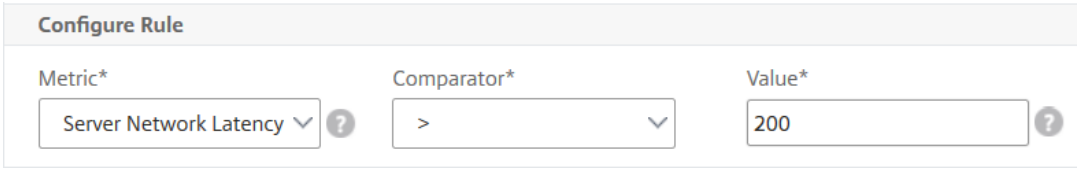
   c) **Entité** - Dans la liste, sélectionnez la catégorie ou le type de ressource. Par défaut, « applications » est sélectionné comme entité.

   d) **Clé de référence** : une clé de référence est générée automatiquement en fonction du type de trafic et de l'entité que vous avez sélectionnés.

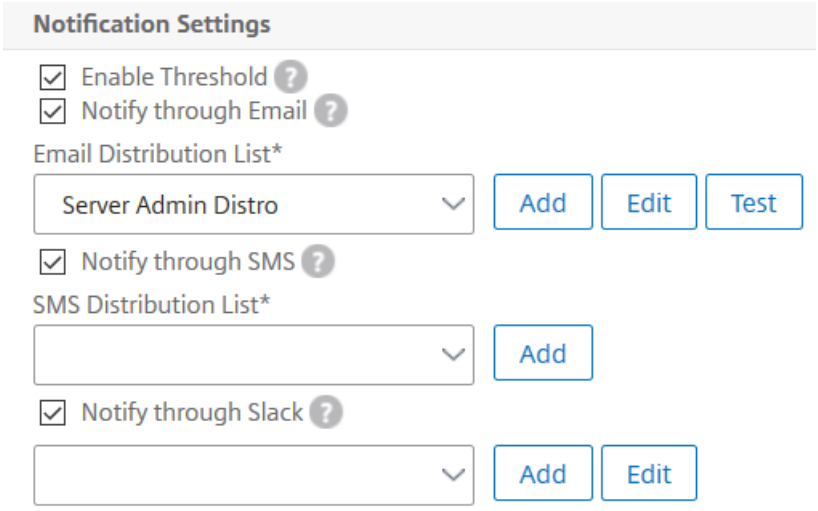
   e) **Durée** - Dans la liste, sélectionnez l'intervalle de temps pour lequel vous souhaitez surveiller l'entité. Vous pouvez surveiller les entités pendant une heure, une journée ou une semaine.



f) Dans la section **Configurer la règle**, créez une règle en choisissant la mesure, un comparateur requis et indiquez une valeur de seuil.



g) Dans la section **Paramètres des notifications**, sélectionnez **Activer le seuil** et le mode d'alerte pour lequel vous souhaitez recevoir les alertes.



4. Cliquez sur **Créer**.

Résoudre les problèmes liés à Web Insight

Pour plus de détails, consultez le document de dépannage Résoudre les problèmes liés à Web Insight.

Résoudre les problèmes liés à Web Insight

February 1, 2024

Avec le tableau de bord Citrix ADM Web Insight, vous pouvez visualiser l'utilisation de vos applications et surveiller toutes les applications Web que les instances de Citrix ADC desservent. À l'aide de Web Insight, les instances ADC envoient des données de transaction HTTP et SSL à l'ADM configuré en tant que collecteur AppFlow. AppFlow est la norme d'exportation de flux utilisée pour identifier et collecter les données d'application et de transaction dans l'infrastructure réseau.

Ce document vous aide à résoudre les problèmes courants liés au déploiement de Web Insight.

Problèmes liés aux rapports de tableau de bord Citrix ADM Web Insight

Si le tableau de bord ADM Web Insight (**GUI ADM > Analytics > Web Insight**) ne parvient pas à afficher les rapports, le problème peut être l'un des suivants :

- Problème de configuration de Web Insight
- Problème de connectivité entre Citrix ADC et Citrix ADM
- Problème de compteur
- Problème de licence
- Problème d'identification du point d'observation
- Problème de paramètres AppFlow manquants

Problème de configuration : Citrix ADM Web Insight n'affiche pas de rapports

Procédez comme suit pour résoudre ce problème :

1. Assurez-vous que la fonctionnalité AppFlow est activée dans l'instance de Citrix ADC. Pour plus de détails, consultez Activation d'AppFlow.
2. Vérifiez la configuration de Web Insight dans l'instance ADC :
    a) Exécutez la commande `show running | grep -i <appflow_policy>` pour vérifier la configuration de Web Insight sur la stratégie. Assurez-vous que le type de

liaison est `REQUEST`. Pa exemple : `bind lb vserver afsanity -policy afp -priority 100 -type REQUEST`

b) Exécutez la commande `show appflow action` pour vérifier la configuration de Web Insight lors de l'action. Assurez-vous que l'`-webinsight` option est activée

c) Vérifiez correctement le paramètre `appflowlog` dans le serveur virtuel LB/CS/CR. Assurez-vous que ce paramètre est activé.

Problème de connectivité entre Citrix ADC et Citrix ADM : Citrix ADM Web Insight n'affiche pas de rapports

Procédez comme suit pour résoudre ce problème :

1. Vérifiez l'état du collecteur AppFlow dans Citrix ADC. Pour de plus amples informations, consultez Comment vérifier l'état de la connectivité entre Citrix ADC et AppFlow Collector.
2. Sur l'interface graphique ADC, vérifiez si les stratégies AppFlow obtiennent des hits. Exécutez la commande `show appflow policy <policy_name>` pour vérifier les succès de stratégie AppFlow. Vous pouvez également accéder à **Système > AppFlow > Stratégies** dans l'interface graphique pour vérifier les accès à la stratégie AppFlow.
3. Validez tout pare-feu bloquant les ports AppFlow 4739 ou 5557.

Problème de compteur : Citrix ADM Web Insight n'affiche pas les rapports

Procédez comme suit pour résoudre ce problème :

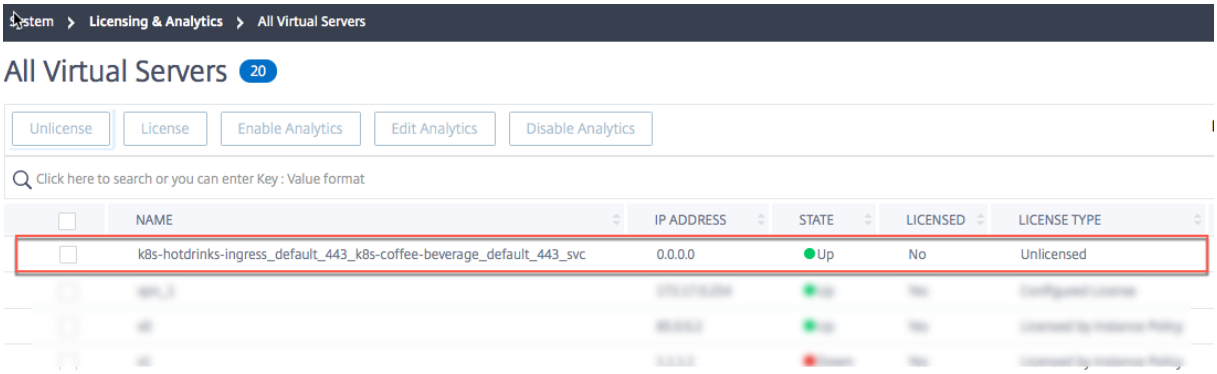
1. Assurez-vous qu'il n'y a aucun problème de configuration et de connectivité AppFlow. Pour plus d'informations, consultez les sections de solution de cette rubrique pour les problèmes de configuration et de connectivité entre Citrix ADC et Citrix ADM.
2. Sur l'instance ADC, à l'invite shell, exécutez la commande `nsconmsg -g appflow_tmpl -d current` et vérifiez les compteurs suivants :

   - `appflow_tmpl_v4_l7_clt2ns_complete`
   - `appflow_tmpl_v4_l7_srvr2ns_complete`
   - `appflow_tmpl_v46_ulfd_client_eot`
   - `appflow_tmpl_v46_ulfd_server_eot`

   Si l'un des compteurs est manquant, effectuez une trace sur l'instance ADC. Ensuite, vérifiez que la transaction est terminée et que la réponse est envoyée par le serveur d'origine. Si la transaction est correcte et que certains compteurs sont manquants, signalez un bogue.

Problème de licence : Citrix ADM Web Insight n'affiche pas de rapports

Avec ce problème, la licence du serveur virtuel particulier pour lequel vous souhaitez afficher le rapport Web Insight apparaît « Non » sous **Système > Licences & Analytics > Configurer la licence**.



Procédez comme suit pour résoudre ce problème :

1. Dans l'instance ADC, assurez-vous que les accès à la stratégie AppFlow augmentent et que l'instance envoie des enregistrements AppFlow à ADM
2. Vérifiez si le serveur virtuel correspondant est sous licence. Si le serveur virtuel n'est pas sous licence, ADM supprime les enregistrements AppFlow. Par conséquent, les rapports Web Insight ne s'affichent pas.

Problème d'ID de point d'observation : Citrix ADM Web Insight n'affiche pas les rapports

Ce problème apparaît car l'identifiant du point d'observation n'est pas unique.

> Remarque :
> Un ID de point d'observation est l'identifiant du Citrix ADC à partir duquel les enregistrements AppFlow sont exportés. Par défaut, l'adresse IP Citrix ADC est l'ID du point d'observation.

Procédez comme suit pour résoudre ce problème :

1. Dans l'instance ADC, assurez-vous que les accès à la stratégie AppFlow augmentent et que l'instance met fin aux enregistrements AppFlow vers ADM.
2. Vérifiez si le serveur virtuel correspondant est sous licence.
3. Assurez-vous que la configuration n'est pas copiée d'une instance ADC vers une autre. Une fois copiée, la configuration peut créer un problème d'ID d'exportateur, entraînant la suppression des enregistrements AppFlow par l'ADM.
4. Connectez-vous à l'instance ADC et exécutez la commande `unset appflow param -observationpointId`.

Problème de paramètres AppFlow manquants : Citrix ADM Web Insight n'affiche pas les rapports

Ce problème se produit car ADM supprime les enregistrements AppFlow en raison de données manquantes.

Procédez comme suit pour résoudre ce problème :

1. Assurez-vous que dans l'instance ADC, les accès à la stratégie AppFlow augmentent et que l'instance met fin aux enregistrements AppFlow vers ADM.
2. Vérifiez si le serveur virtuel correspondant est sous licence.
3. Assurez-vous que la configuration n'est pas copiée d'une instance ADC vers une autre. Une fois copiée, la configuration peut créer un problème d'ID d'exportateur, entraînant la suppression des enregistrements AppFlow par l'ADM.
4. Assurez-vous que les paramètres AppFlow suivants sont activés sur l'instance ADC :

   a) `HTTP method logging`
   b) `HTTP domain name logging`
   c) `HTTP URL logging`
   d) `HTTP host logging`
   e) `HTTP Content-Type header logging`

Problèmes divers de Citrix ADM Web Insight

- **Problème** : sur le client HTTP, la page ne se charge pas lorsque AppFlow est activé.
- **Solution** : procédez comme suit pour résoudre ce problème :

  1. Dans la commande d'action AppFlow, désactivez la fonctionnalité « PageTracking » `set appflow action <name> -pageTracing disable`. Cette action n'a aucun effet sur la fonctionnalité.

  Si le problème n'est pas résolu, procédez comme suit :

  1. Dans la même action, désactivez la `clientsidemeasurement` fonction `set appflow action <name> -clientsidemeasurements disable`. Si cette étape résout le problème, capturez des traces sur l'instance ADC et déposez un bogue.

- **Problème** : l'appliance ADC se bloque lorsque AppFlow est activé.
- **Solution** : procédez comme suit pour résoudre ce problème :

Si backtrace (BT) a des fonctions AppFlow, le problème peut se trouver dans la fonctionnalité AppFlow. Si le BT est dans un code spécifique à l'entité, le problème peut être dans les entités qui utilisent AppFlow pour envoyer des données aux collecteurs.

Dans ce dernier cas, désactivez toute configuration AppFlow spécifique à la fonctionnalité et vérifiez. Ne désactivez pas la fonctionnalité AppFlow globalement car cette étape ne donne pas beaucoup d'informations sur le problème.

Résolution des problèmes liés à l'utilisation

Vérifiez les compteurs AppFlow suivants pour tout problème lié à AppFlow ou Web Insight.

Comptoir	Description
appflow_tot_record_drop	Les enregistrements AppFlow ont été abandonnés en raison d'un collecteur non valide. Cela se produit généralement lorsque la configuration du collecteur change et que les connexions existantes utilisent l'ancienne configuration du collecteur.
lstream_tot_trans_written	Ce compteur doit être incrémenté pour chaque transaction qui doit être enregistrée.
lstream_sent	Ce compteur est incrémenté pour chaque journal de transactions envoyé.

HDX Insight

February 1, 2024

HDX Insight fournit une visibilité de bout en bout du trafic HDX vers Citrix Virtual Apps and Desktop passant par Citrix ADC. Il permet également aux administrateurs d'afficher en temps réel les mesures de latence des clients et du réseau, les rapports historiques, les données de performance de bout en bout et de résoudre les problèmes de performances. La disponibilité des données de visibilité en temps réel et historiques permet à Citrix Application Delivery Management (ADM) de prendre en charge une grande variété de cas d'utilisation.

Pour que des données apparaissent, vous devez activer AppFlow sur vos serveurs virtuels Citrix Gateway. AppFlow peut être fourni par le protocole IPFIX ou la méthode LogStream.

> **Remarque**

> Pour autoriser l'enregistrement des calculs du temps aller-retour de l'ICA, activez les paramètres de stratégie suivants :

- Calcul de l'ICA aller-retour
- Intervalle de calcul aller-retour ICA
- Calcul de l'aller-retour ICA pour les connexions au ralenti

Si vous cliquez sur un utilisateur individuel, vous pouvez voir chaque session HDX, active ou terminée, effectuée par l'utilisateur dans la période sélectionnée. D'autres informations incluent plusieurs statistiques de latence et la bande passante consommée pendant la session. Vous pouvez également obtenir des informations sur la bande passante à partir de canaux virtuels individuels tels que l'audio, le mappage de l'imprimante et le mappage du lecteur client.

> **Remarque**
>
> Lorsque vous créez un groupe, vous pouvez affecter des rôles au groupe, fournir un accès au niveau de l'application au groupe et affecter des utilisateurs au groupe. Citrix ADM Analytics prend désormais en charge l'autorisation basée sur l'adresse IP virtuelle. Vos utilisateurs peuvent désormais voir des rapports pour tous les Insights uniquement pour les applications (serveurs virtuels) pour lesquelles ils sont autorisés. Pour plus d'informations sur les groupes et l'affectation d'utilisateurs au groupe, consultez Configurer des groupes.

Vous pouvez également accéder à **HDX Insight** > **Applications** et cliquer sur **Durée de lancement** pour afficher le temps nécessaire au lancement de l'application. Vous pouvez également consulter l'agent utilisateur de tous les utilisateurs connectés en accédant à**HDX Insight**-> Users.

> **Remarque**HDX insight prend en charge les partitions d'administration configurées dans les instances de Citrix ADC exécutées sur la version 12.0 du logiciel.

Les clients légers suivants prennent en charge HDX Insight :

- Clients légers WYSE basés sur Windows
- Clients légers basés sur WYSE Linux
- Clients légers WYSE Thinos
- Clients légers basés sur Ubuntu 10Zig

Identification de la cause première des problèmes de performances lentes

Scénario 1

L'utilisateur rencontre des retards lors de l'accès à Citrix Virtual Apps and Desktops.

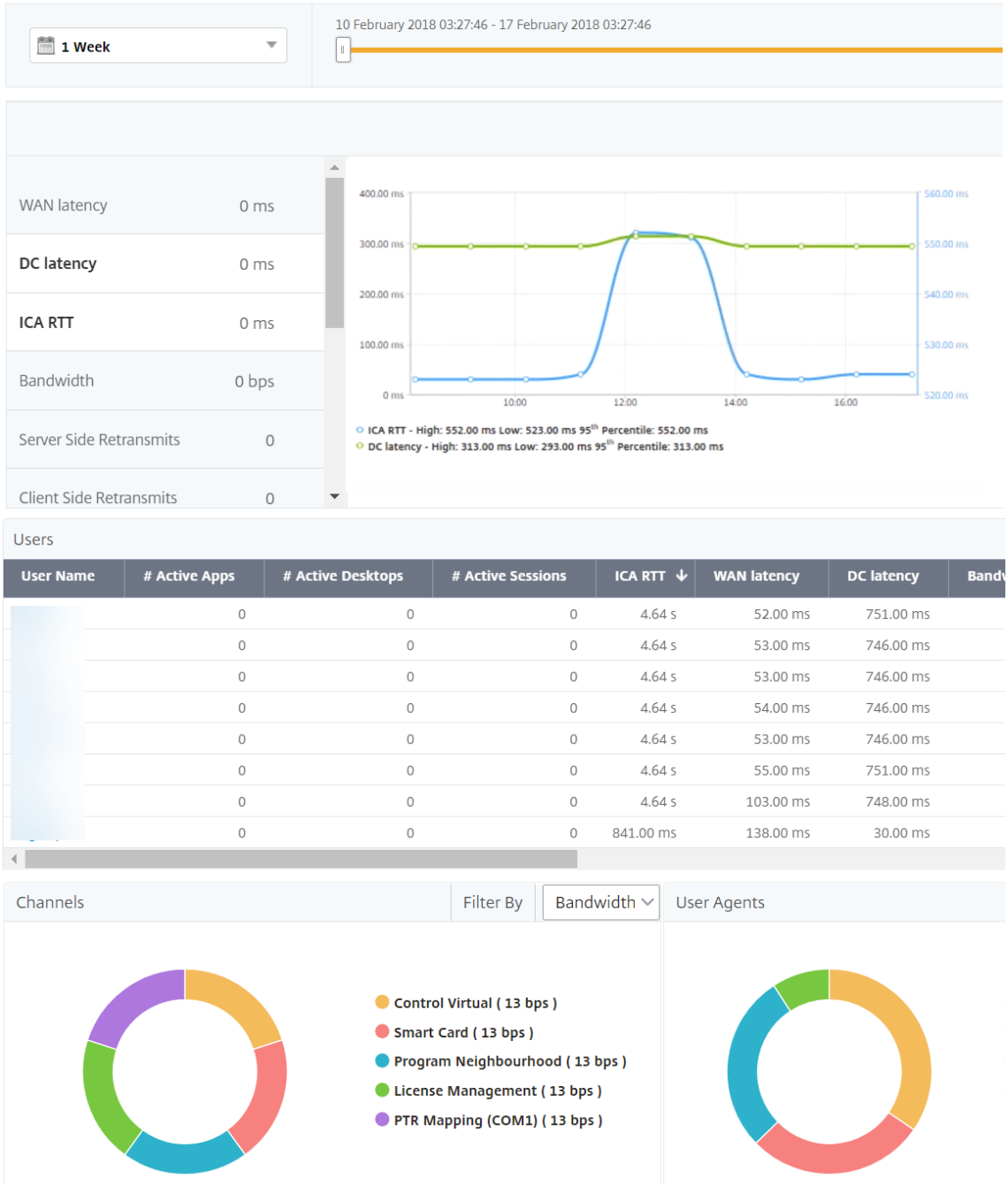
Les retards peuvent être dus à une latence sur le réseau du serveur, à des retards de trafic ICA causés par le réseau du serveur ou à une latence sur le réseau client.

Pour identifier la cause première du problème, analysez les indicateurs suivants :

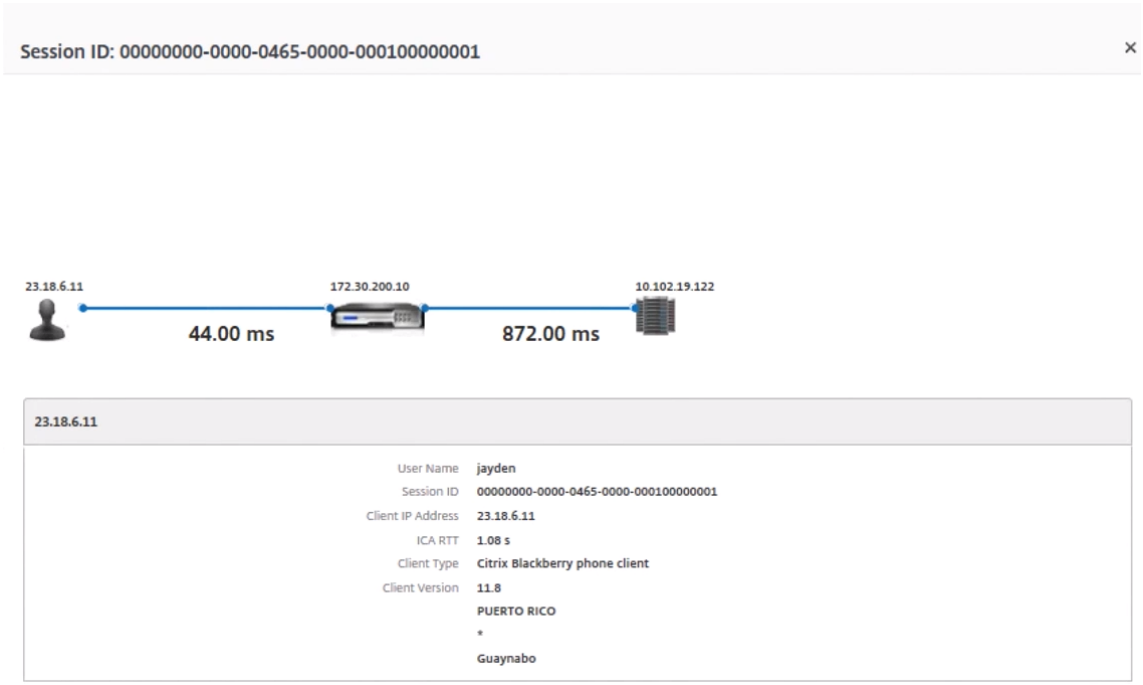
- Latence WAN
- Latence DC
- Délai d'hôte

Pour afficher les mesures client :

1. Sous l'onglet **Analytics**, accédez à **HDX Insight** > **Utilisateurs**.
2. Faites défiler vers le bas et sélectionnez le nom d'utilisateur et sélectionnez la période dans la liste. La période peut être d'un jour, d'une semaine, d'un mois, ou vous pouvez même personnaliser la période pour laquelle vous souhaitez voir les données.
3. Le graphique affiche sous forme de graphique les valeurs de latence ICA RTT et DC de l'utilisateur pour la période spécifiée.



4. Dans le tableau **Sessions en cours**, placez le curseur de la souris sur la valeur **RTT** et notez les valeurs de retard de l'hôte, de latence CC et de latence WAN.
5. Dans le tableau**Sessions en cours**, cliquez sur le symbole de diagramme de saut pour afficher des informations sur la connexion entre le client et le serveur, y compris les valeurs de latence.



Résumé **Dans cet exemple, la**latence DC**est de 751 millisecondes, la**latence WAN**de 52 millisecondes et les retards hôtes de 6 secondes.** Cela indique que l'utilisateur connaît un retard dû à la latence moyenne causée par le réseau du serveur.

Scénario 2

L'utilisateur rencontre un retard lors du lancement d'une application sur Citrix Virtual App ou Desktop

Ce retard peut être dû à une latence sur le réseau du serveur, à des retards de trafic ICA-causés par le réseau du serveur, à une latence sur le réseau client ou au temps nécessaire pour lancer une application.

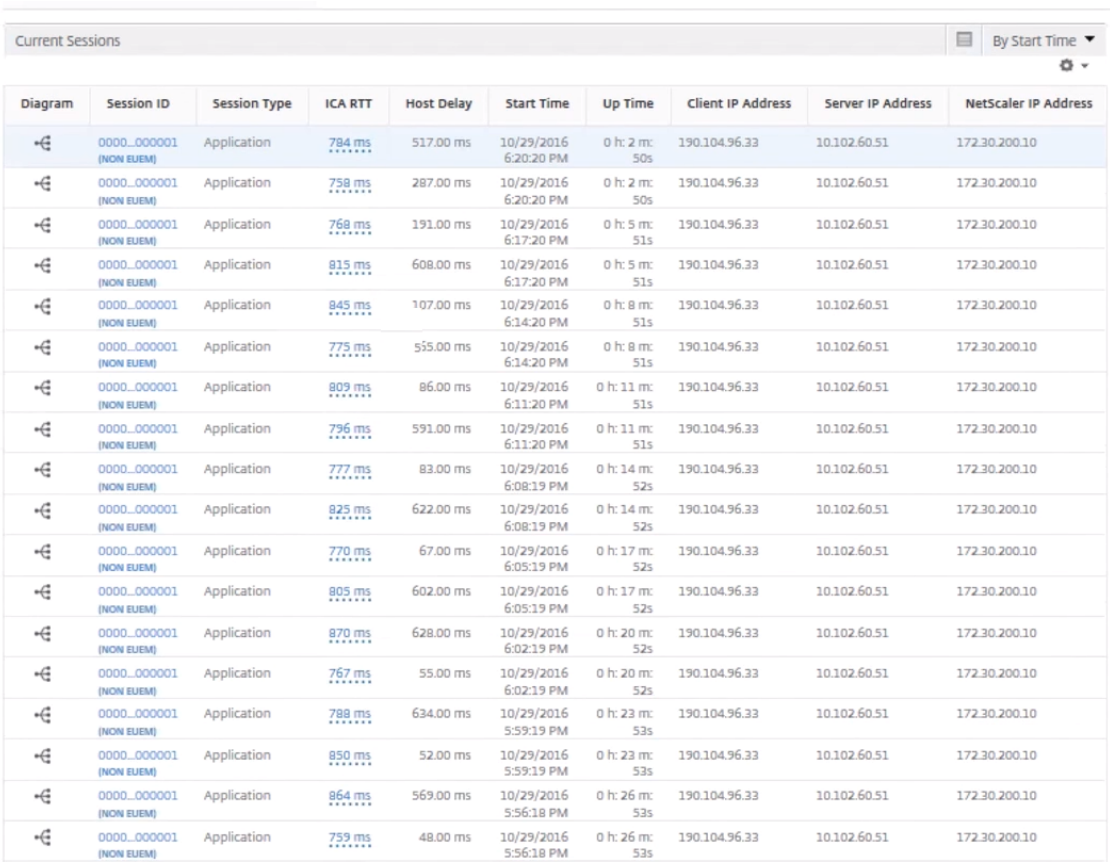
Pour identifier la cause première du problème, analysez les indicateurs suivants :

- Latence WAN
- Latence DC
- Retard de l'hôte

Pour afficher les mesures utilisateur :

1. Dans l'onglet **Analytics**, accédez à **HDX Insight** > **Users**.
2. Faites défiler la page vers le bas et cliquez sur le nom d'utilisateur.

3. Dans la représentation graphique, notez les valeurs de latence WAN, de latence DC et de RTT pour la session particulière.
4. Dans le tableau **Sessions en cours**, notez que le délai d'hôte est élevé.



Current Sessions — By Start Time

Diagram	Session ID	Session Type	ICA RTT	Host Delay	Start Time	Up Time	Client IP Address	Server IP Address	NetScaler IP Address
	0000...000001 (NON EUEM)	Application	784 ms	517.00 ms	10/29/2016 6:20:20 PM	0 h: 2 m: 50s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	758 ms	287.00 ms	10/29/2016 6:20:20 PM	0 h: 2 m: 50s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	768 ms	191.00 ms	10/29/2016 6:17:20 PM	0 h: 5 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	815 ms	608.00 ms	10/29/2016 6:17:20 PM	0 h: 5 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	845 ms	107.00 ms	10/29/2016 6:14:20 PM	0 h: 8 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	775 ms	535.00 ms	10/29/2016 6:14:20 PM	0 h: 8 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	809 ms	86.00 ms	10/29/2016 6:11:20 PM	0 h: 11 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	796 ms	591.00 ms	10/29/2016 6:11:20 PM	0 h: 11 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	777 ms	83.00 ms	10/29/2016 6:08:19 PM	0 h: 14 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	825 ms	622.00 ms	10/29/2016 6:08:19 PM	0 h: 14 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	770 ms	67.00 ms	10/29/2016 6:05:19 PM	0 h: 17 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	805 ms	602.00 ms	10/29/2016 6:05:19 PM	0 h: 17 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	870 ms	628.00 ms	10/29/2016 6:02:19 PM	0 h: 20 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	767 ms	55.00 ms	10/29/2016 6:02:19 PM	0 h: 20 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	788 ms	634.00 ms	10/29/2016 5:59:19 PM	0 h: 23 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	850 ms	52.00 ms	10/29/2016 5:59:19 PM	0 h: 23 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	864 ms	569.00 ms	10/29/2016 5:56:18 PM	0 h: 26 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	759 ms	48.00 ms	10/29/2016 5:56:18 PM	0 h: 26 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10

Résumé Dans cet exemple, la **latence CC** est de 1 milliseconde, la **latence WAN** est de 12 millisecondes, mais le **délai hôte** est de 517 millisecondes. Le RTT élevé avec des latences DC et WAN faibles indique une erreur d'application sur le serveur hôte.

> **Remarque**HDX Insight affiche également plus de mesures utilisateur, telles que la gigue WAN et les retransmet côté serveur si vous utilisez Citrix ADM exécutant le logiciel 11.1 build 51.21 ou version ultérieure. Pour afficher ces mesures, accédez à **Analytics** > **HDX Insight** > **Utilisateurs**, puis sélectionnez un nom d'utilisateur. Les mesures utilisateur apparaissent dans le tableau en regard du graphique.

Géomaps pour HDX Insight

La fonctionnalité Citrix ADM Geomaps affiche l'utilisation des applications dans différents emplacements géographiques sur une carte. Les administrateurs peuvent utiliser ces informations pour comprendre les tendances de l'utilisation des applications dans divers emplacements géographiques.

Vous pouvez configurer Citrix ADM pour afficher les cartes géographiques d'un emplacement géographique ou d'un réseau local particulier en spécifiant la plage d'adresses IP privées (adresses IP de début et de fin) de l'emplacement.

Vous pouvez également afficher les détails historiques et actifs des utilisateurs à partir des cartes géographiques dans HDX Insight. Accédez à **Analytics** > **HDX Insight**, puis dans la section **Monde** de la carte, cliquez sur le pays ou la région dont vous souhaitez voir les détails. Vous pouvez approfondir la hiérarchie vers le bas pour afficher les informations par ville et par état.

Pour configurer une géomap pour les centres de données :

Sous l'onglet **Analytics**, accédez à **Paramètres** > **Blocs IP** pour configurer les géomaps pour un emplacement particulier.

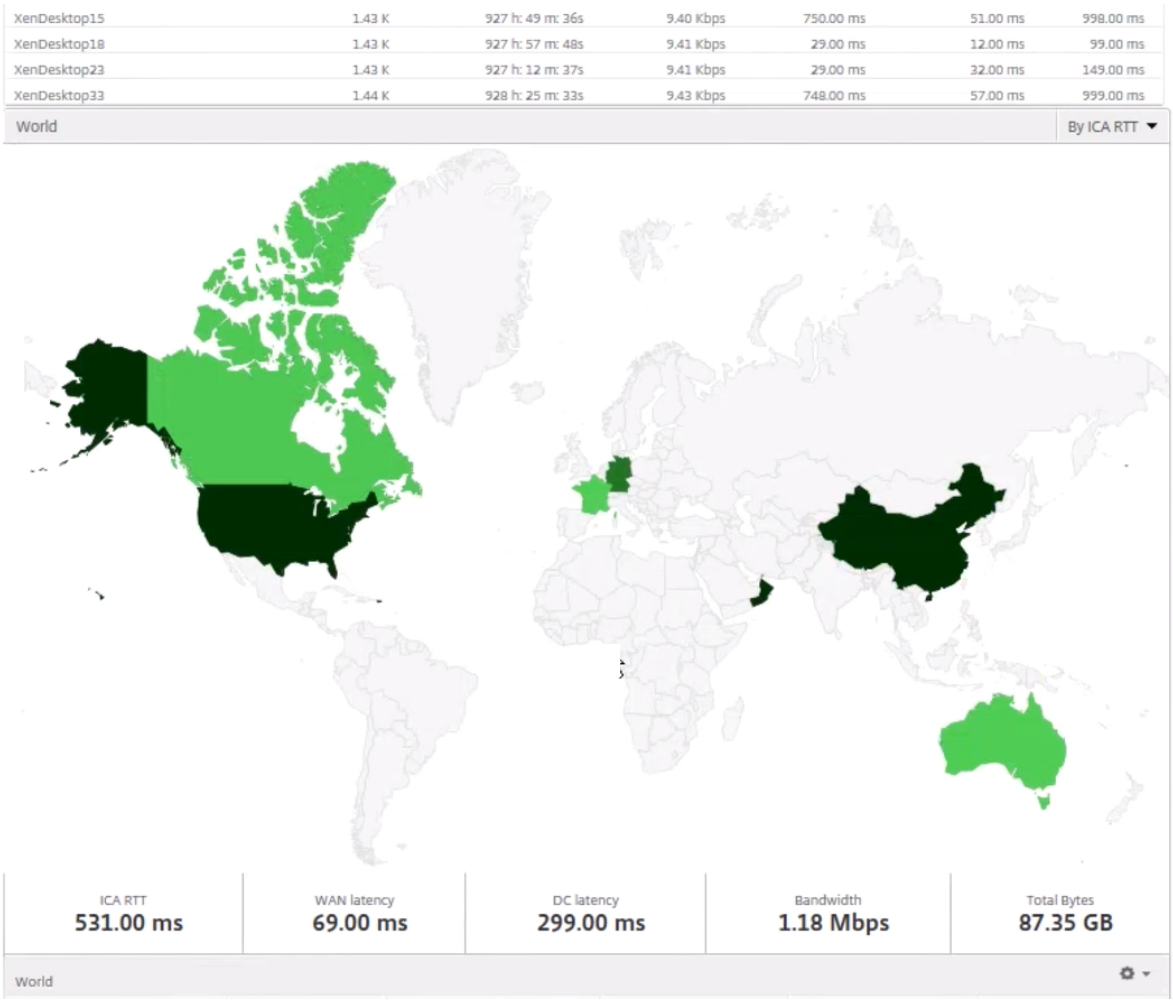
Cas d'utilisation

Imaginez un scénario dans lequel l'organisation ABC a deux succursales, l'une à Santa Clara et l'autre en Inde.

Les utilisateurs de Santa Clara utilisent l'appliance Citrix Gateway sur Sclara.x.com pour accéder au trafic VPN. Les utilisateurs indiens utilisent l'appliance Citrix Gateway sur India.x.com pour accéder au trafic VPN.

Pendant un intervalle de temps particulier, disons de 10 heures à 17 heures, les utilisateurs de Santa Clara se connectent à Sclara.x.com pour accéder au trafic VPN. La plupart des utilisateurs accèdent au même Citrix Gateway, ce qui entraîne un retard dans la connexion au VPN, de sorte que certains utilisateurs se connectent à India.x.com au lieu de Sclara.x.com.

Un administrateur Citrix ADC qui analyse le trafic peut utiliser la fonctionnalité de cartographie géographique pour afficher le trafic dans le bureau de Santa Clara. La carte montre que le temps de réponse dans le bureau de Santa Clara est élevé, car le bureau de Santa Clara dispose d'une seule appliance Citrix Gateway grâce à laquelle les utilisateurs peuvent accéder au trafic VPN. L'administrateur peut donc décider d'installer un autre Citrix Gateway, de sorte que les utilisateurs disposent de deux appliances Citrix Gateway locales via lesquelles accéder au VPN.



Limitations

Si les instances Citrix ADC disposent d'une licence Advanced, les seuils définis sur Citrix ADM pour HDX Insight ne seront pas déclenchés car les données analytiques sont collectées pendant une heure seulement.

Activation de la collecte de données HDX Insight

February 1, 2024

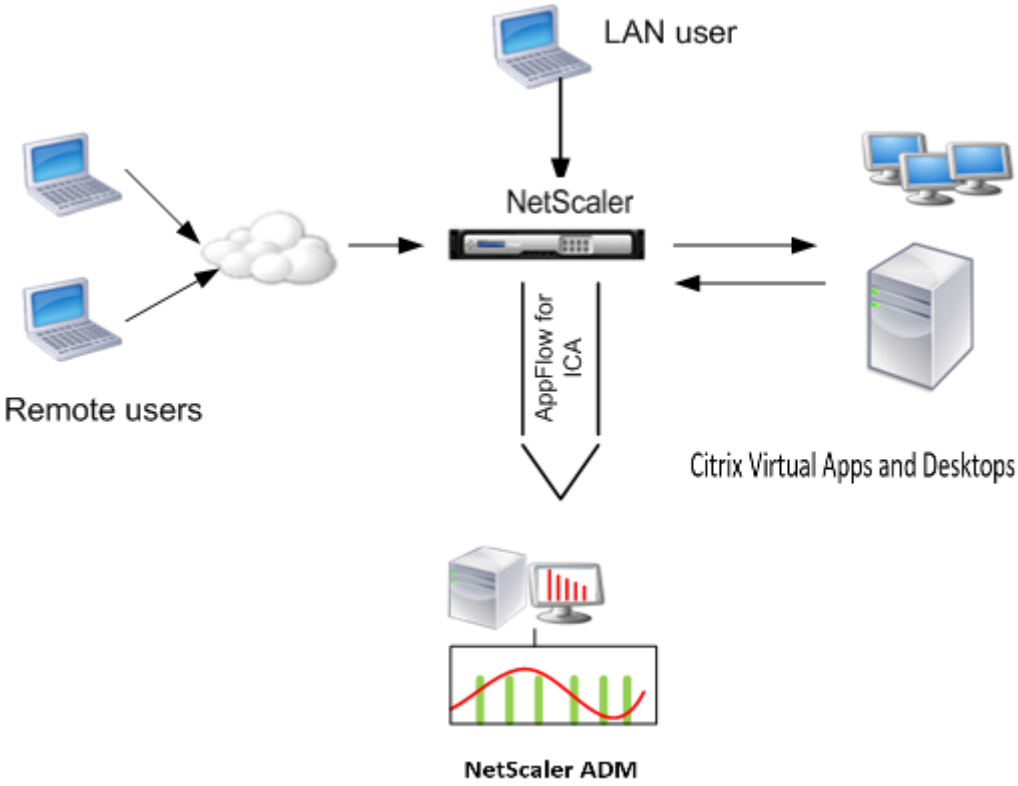
HDX Insight permet au service informatique d'offrir une expérience utilisateur exceptionnelle en offrant une visibilité de bout en bout sans précédent sur le trafic ICA qui passe par les instances Citrix ADC ou les appliances Citrix SD-WAN, et fait partie de Citrix Application Delivery Management (ADM) Analytics. HDX Insight offre des fonctionnalités de veille décisionnelle et d'analyse des défaillances convaincantes et puissantes pour le réseau, les postes de travail virtuels, les applications et la structure applicative. HDX Insight peut à la fois trier instantanément les problèmes des utilisateurs, collecter des données sur les connexions de bureau virtuel et générer des enregistrements AppFlow et les présenter sous forme de rapports visuels.

La configuration permettant la collecte de données dans Citrix ADC diffère selon la position de l'appliance dans la topologie de déploiement.

Activation de la collecte de données pour la surveillance des Citrix ADC déployés en mode utilisateur LAN

Les utilisateurs externes qui accèdent aux applications Citrix Virtual App and Desktop doivent s'authentifier sur Citrix Gateway. Toutefois, les utilisateurs internes peuvent ne pas avoir besoin d'être redirigés vers Citrix Gateway. En outre, dans un déploiement en mode transparent, l'administrateur doit appliquer manuellement les stratégies de routage afin que les demandes soient redirigées vers l'appliance Citrix ADC.

Pour surmonter ces difficultés et pour que les utilisateurs LAN se connectent directement aux applications Citrix Virtual App et Desktop, vous pouvez déployer l'appliance Citrix ADC en mode utilisateur LAN en configurant un serveur virtuel de redirection de cache, qui agit comme un proxy SOCKS sur l'appliance Citrix Gateway.



> **Remarque** L'appliance Citrix ADM et Citrix Gateway résident dans le même sous-réseau.

Pour surveiller les appliances Citrix ADC déployées dans ce mode, ajoutez d'abord l'appliance Citrix ADC à l'inventaire NetScaler Insight, activez AppFlow, puis consultez les rapports sur le tableau de bord.

Après avoir ajouté l'appliance Citrix ADC à l'inventaire Citrix ADM, vous devez activer AppFlow pour la collecte de données.

> **Remarque**
>
> - Sur une instance ADC, vous pouvez accéder à **Système > AppFlow > Collecteurs**, pour vérifier si le collecteur (Citrix ADM) est ou non. L'instance Citrix ADC envoie des enregistrements AppFlow à Citrix ADM à l'aide de NSIP. Mais l'instance utilise son SNIP pour vérifier la connectivité avec Citrix ADM. Assurez-vous donc que le SNIP est configuré sur l'instance.
> - Vous ne pouvez pas activer la collecte de données sur un Citrix ADC déployé en mode utilisateur LAN à l'aide de l'utilitaire de configuration Citrix ADM.
> - Pour des informations détaillées sur les commandes et leur utilisation, consultez la sectionRéférence des commandes.
> - Pour plus d'informations sur les expressions de stratégie, consultez la sectionPolitiques et expressions.

Pour configurer la collecte de données sur un appliance Citrix ADC à l'aide de l'interface de ligne de commande :

À l'invite de commandes, procédez comme suit :

1. Connectez-vous à une appliance.
2. Ajoutez un serveur virtuel de redirection de cache proxy avec l'IP et le port proxy, et spécifiez le type de service HDX.

```
add cr vserver <name> <servicetype> [<ipaddress> <port>] [-
   cacheType <cachetype>] [ - cltTimeout <secs>]
<!--NeedCopy-->
```

Exemple

```
add cr vserver cr1 HDX 10.12.2.2 443 – cacheType FORWARD –
   cltTimeout 180
<!--NeedCopy-->
```

> **Remarque :** Si vous accédez au réseau LAN à l'aide d'une appliance Citrix Gateway, ajoutez une action à appliquer selon une stratégie correspondant au trafic VPN.

```
add vpn trafficAction <name> <qual> [-HDX ( ON or OFF )]

add vpn trafficPolicy <name> <rule> <action>
<!--NeedCopy-->
```

Exemple

```
add vpn trafficAction act1 tcp -HDX ON

add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
<!--NeedCopy-->
```

3. Ajoutez Citrix ADM en tant que collecteur AppFlow sur l'appliance Citrix ADC.

```
add appflow collector <name> -IPAddress <ip_addr>
<!--NeedCopy-->
```

Example:

‘‘‘

add appflow collector MyInsight -IPAddress 192.168.1.101

‘‘‘

4. Créez une action AppFlow et associez le collecteur à l'action.

```
add appflow action <name> -collectors <string>
```

Exemple :


```
add appflow action act -collectors MyInsight
```

5. Créez une stratégie AppFlow pour spécifier la règle de génération du trafic.

   ```
   add appflow policy <policyname> <rule> <action>
   ```

   Exemple :

   ```
   add appflow policy pol true act
   ```

6. Liez la stratégie AppFlow à un point de liaison global.

   ```
   bind appflow global <policyname> <priority> -type <type>
   ```

   Exemple :

   ```
   bind appflow global pol 1 -type ICA_REQ_DEFAULT
   ```

   > **Remarque**
   >
   > La valeur de type doit être ICA_REQ_OVERRIDE ou ICA_REQ_DEFAULT pour s'appliquer au trafic ICA.

7. Définissez la valeur du paramètre FlowRecordInterval pour AppFlow sur 60 secondes.

   ```
   set appflow param -flowRecordInterval 60
   ```

   Exemple :

   ```
   set appflow param -flowRecordInterval 60
   ```

8. Enregistrez la configuration. Type : `save ns config`

Activation de la collecte de données pour les appliances Citrix Gateway déployées en mode saut unique

Lorsque vous déployez Citrix Gateway en mode à saut unique, il se trouve à la périphérie du réseau. L'instance Gateway fournit des connexions ICA proxy à l'infrastructure de mise à disposition des ordinateurs de bureau. Le déploiement à saut unique est le déploiement le plus simple et le plus courant. Le mode à saut unique assure la sécurité lorsqu'un utilisateur externe essaie d'accéder au réseau interne d'une organisation.
En mode saut unique, les utilisateurs accèdent aux appliances Citrix ADC via un réseau privé virtuel (VPN).

Pour commencer à collecter les rapports, vous devez ajouter l'appliance Citrix Gateway à l'inventaire Citrix Application Delivery Management (ADM) et activer AppFlow sur ADM.

Pour activer la fonctionnalité AppFlow à partir de Citrix ADM :

1. Dans un navigateur Web, tapez l'adresse IP du Citrix ADM (par exemple, http://192.168.100.1).
2. Dans **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Accédez à **Réseaux** > **Instances**, puis sélectionnez l'instance Citrix ADC que vous souhaitez activer l'analyse.
4. Dans la liste **Sélectionner une action**, sélectionnez **Configurer Analytics**.
5. Sélectionnez les serveurs virtuels VPN, puis cliquez sur **Activer les analyses**.
6. Sélectionnez **HDX Insight**, puis **ICA**.
7. Cliquez sur **OK**.

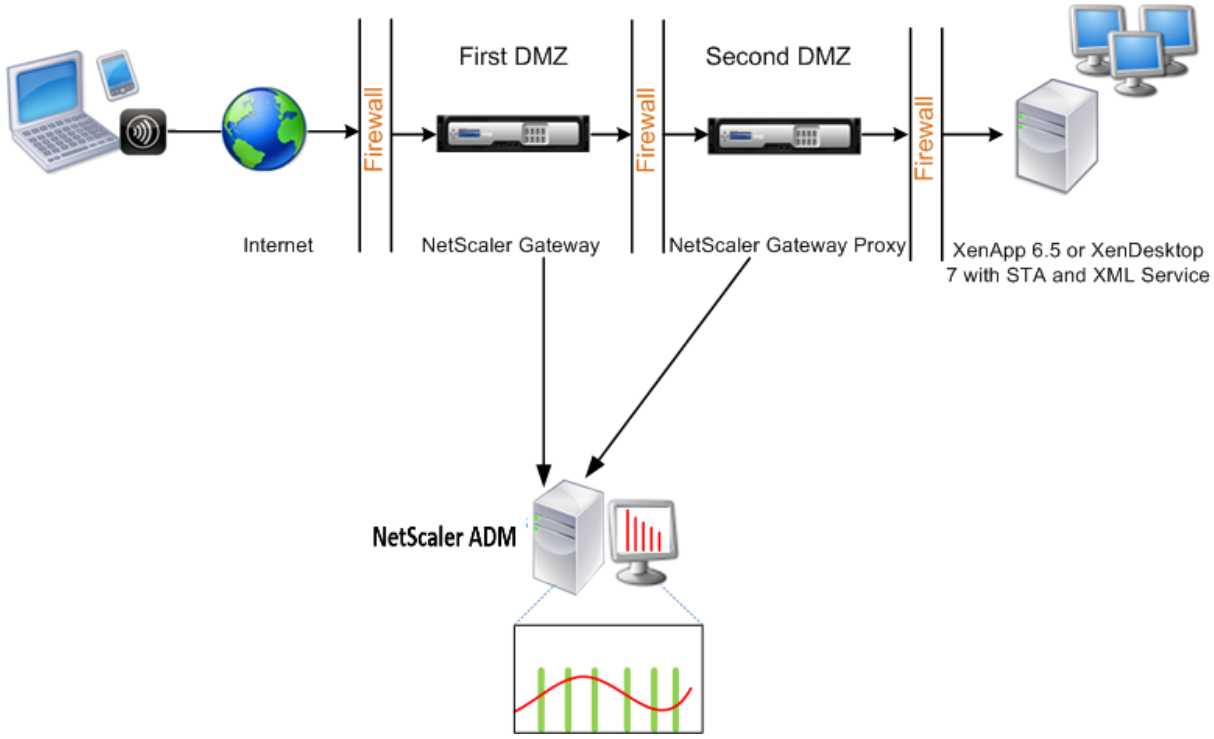
> **Remarque**
>
> lorsque vous activez AppFlow en mode saut unique, les commandes suivantes s'exécutent en arrière-plan. Ces commandes sont explicitement spécifiées ici à des fins de dépannage.

```
1  -  add appflow collector <name> -IPAddress <ip_addr>
2
3  -  add appflow action <name> -collectors <string>
4
5  -  set appflow param -flowRecordInterval <secs>
6
7  -  disable ns feature AppFlow
8
9  -  enable ns feature AppFlow
10
11 -  add appflow policy <name> <rule> <expression>
12
13 -  set appflow policy <name> -rule <expression>
14
15 -  bind vpn vserver <vsname> -policy <string> -type <type> -priority <
      positive_integer>
16
17 -  set vpn vserver <name> -appflowLog ENABLED
18
19 -  save ns config
```

Les données de canal virtuel EUEM font partie des données HDX Insight que Citrix ADM reçoit des instances de Gateway. Le canal virtuel EUEM fournit les données sur ICA RTT. Si le canal virtuel EUEM n'est pas activé, les données HDX Insight restantes sont toujours affichées sur Citrix ADM.

Activation de la collecte de données pour les appliances Citrix Gateway déployées en mode double saut

Le mode double saut Citrix Gateway offre une protection supplémentaire au réseau interne d'une organisation car un attaquant doit pénétrer plusieurs zones de sécurité ou zones démilitarisées (DMZ) pour atteindre les serveurs du réseau sécurisé. Si vous souhaitez analyser le nombre de sauts (appliances Citrix Gateway) à travers lesquels les connexions ICA passent, ainsi que les détails sur la latence sur chaque connexion TCP et son rapport avec la latence ICA totale perçue par le client, vous devez installer Citrix ADM afin que les appliances Citrix Gateway rapporter ces statistiques de l'état civil.



Citrix Gateway dans la première DMZ gère les connexions utilisateur et exécute les fonctions de sécurité d'un VPN SSL. Cette passerelle Citrix Gateway chiffre les connexions utilisateur, détermine comment les utilisateurs sont authentifiés et contrôle l'accès aux serveurs du réseau interne.

Citrix Gateway dans la deuxième DMZ sert de périphérique proxy Citrix Gateway. Cette passerelle Citrix Gateway permet au trafic ICA de traverser la deuxième zone démilitarisée pour terminer les connexions utilisateur à la batterie de serveurs.

Le Citrix ADM peut être déployé soit dans le sous-réseau appartenant à l'appliance Citrix Gateway dans la première zone démilitarisée, soit dans le sous-réseau appartenant à la seconde zone démilitarisée de l'appliance Citrix Gateway. Dans l'image ci-dessus, Citrix ADM et Citrix Gateway de la première DMZ sont déployés dans le même sous-réseau.

En mode double saut, Citrix ADM collecte les enregistrements TCP d'une appliance et les enregistrements ICA de l'autre appliance. Une fois que vous avez ajouté les appliances Citrix Gateway à l'

inventaire Citrix ADM et activé la collecte de données, chacune des appliances exporte les rapports en suivant le nombre de sauts et l'ID de la chaîne de connexion.

Pour que Citrix ADM identifie l'appliance qui exporte des enregistrements, chaque appliance est spécifiée avec un nombre de sauts et chaque connexion est spécifiée avec un ID de chaîne de connexion. Le nombre de sauts représente le nombre d'appliances Citrix Gateway via lesquelles le trafic circule d'un client vers les serveurs. L'ID de chaîne de connexion représente les connexions de bout en bout entre le client et le serveur.

Citrix ADM utilise le nombre de sauts et l'ID de chaîne de connexion pour corréler les données des appliances Citrix Gateway et générer les rapports.

Pour surveiller les appliances Citrix Gateway déployées dans ce mode, vous devez d'abord ajouter Citrix Gateway à l'inventaire Citrix ADM, activer AppFlow sur Citrix ADM, puis afficher les rapports sur le tableau de bord Citrix ADM.

Configurer HDX Insight sur les serveurs virtuels utilisés pour Optimal Gateway

Étapes à suivre pour configurer HDX Insight sur les serveurs virtuels utilisés pour Optimal Gateway :

1. Accédez à **Réseaux** > **Instances**, puis sélectionnez l'instance Citrix ADC que vous souhaitez activer l'analyse.
2. Dans la liste **Sélectionner une action**, sélectionnez **Configurer Analytics**.
3. Sélectionnez le serveur virtuel VPN configuré pour l'authentification, puis cliquez sur **Activer les analyses**.
4. Sélectionnez **HDX Insight**, puis **ICA**.
5. Sélectionnez d'autres options avancées selon vos besoins.
6. Cliquez sur **OK**.
7. Répétez les étapes 3 à 6 sur l'autre serveur virtuel VPN.

Activer la collecte de données sur Citrix ADM

Si vous activez Citrix ADM pour commencer à collecter les détails ICA à partir des deux appliances, les détails collectés sont redondants. Il s'agit des deux appliances qui signalent les mêmes mesures. Pour remédier à cette situation, vous devez activer AppFlow pour ICA sur l'une des premières appliances Citrix Gateway, puis activer AppFlow pour TCP sur la seconde appliance. Ce faisant, l'une des appliances exporte les enregistrements ICA AppFlow et l'autre exporte les enregistrements TCP AppFlow. Cela permet également d'économiser le temps de traitement lors de l'analyse du trafic ICA.

Pour activer la fonctionnalité AppFlow à partir de Citrix ADM :

1. Dans un navigateur Web, tapez l'adresse IP du Citrix ADM (par exemple, http://192.168.100.1).
2. Dans **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Accédez à **Réseaux** > **Instances**, puis sélectionnez l'instance Citrix ADC que vous souhaitez activer l'analyse.
4. Dans la liste **Sélectionner une action**, sélectionnez **Configurer Analytics**.
5. Sélectionnez les serveurs virtuels VPN, puis cliquez sur **Activer les analyses**.
6. Sélectionnez **HDX** Insight, puis **sélectionnez** ICA **ou TCP pour le trafic ICA ou** le trafic TCP respectivement.

   > **Remarque**
   >
   > Si la journalisation AppFlow n'est pas activée pour les services ou groupes de services respectifs sur l'appliance Citrix ADC, le tableau de bord Citrix ADM n'affiche pas les enregistrements, même si la colonne Insight indique Activé.

7. Cliquez sur **OK**.

Configuration des appliances Citrix Gateway pour exporter des données

Après avoir installé les appliances Citrix Gateway, vous devez configurer les paramètres suivants sur les appliances Citrix Gateway pour exporter les rapports vers Citrix ADM :

- Configurez les serveurs virtuels des appliances Citrix Gateway dans la première et la deuxième zone démilitarisée pour communiquer entre eux.
- Liez le serveur virtuel Citrix Gateway dans la deuxième zone DMZ au serveur virtuel Citrix Gateway dans la première zone DMZ.
- Activez le double saut sur Citrix Gateway dans la deuxième DMZ.
- Désactivez l'authentification sur le serveur virtuel Citrix Gateway dans la deuxième DMZ.
- Permettre à l'une des appliances Citrix Gateway d'exporter des enregistrements ICA
- Activez l'autre appliance Citrix Gateway pour exporter des enregistrements TCP :
- Activez le chaînage des connexions sur les deux appliances Citrix Gateway.

Configurer Citrix Gateway à l'aide de l'interface de ligne de commande :

1. Configurez le serveur virtuel Citrix Gateway dans la première zone DMZ pour qu'il communique avec le serveur virtuel Citrix Gateway dans la deuxième zone DMZ.


```
add vpn nextHopServer <name> <nextHopIP> <nextHopPort> [-secure (
    ON or OFF)] [-imgGifToPng]

add vpn nextHopServer nh1 10.102.2.33 8443 –secure ON
```

2. Liez le serveur virtuel Citrix Gateway dans la deuxième zone DMZ au serveur virtuel Citrix Gateway dans la première zone DMZ. Exécutez la commande suivante sur Citrix Gateway dans la première DMZ :

```
bind vpn vserver <name> -nextHopServer <name>

bind vpn vserver vs1 -nextHopServer nh1
```

3. Activez le double saut et AppFlow sur Citrix Gateway dans la deuxième DMZ.

```
set vpn vserver <name> [- doubleHop ( ENABLED or DISABLED )] [-
     appflowLog ( ENABLED or DISABLED )]

set vpn vserver vpnhop2 –doubleHop ENABLED –appFlowLog ENABLED
```

4. Désactivez l'authentification sur le serveur virtuel Citrix Gateway dans la deuxième DMZ.

```
set vpn vserver <name> [-authentication (ON or OFF)]

set vpn vserver vs -authentication OFF
```

5. Activez l'une des appliances Citrix Gateway pour exporter des enregistrements TCP.

```
bind vpn vserver <name> [-policy <string> -priority <
    positive_integer>] [-type <type>]

bind vpn vserver vpn1 -policy appflowpol1 -priority 101 –type
    OTHERTCP_REQUEST
```

6. Activez l'autre appliance Citrix Gateway pour exporter des enregistrements ICA :

```
bind vpn vserver <name> [-policy <string> -priority <
    positive_integer>] [-type <type>]

bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
    ICA_REQUEST
```

7. Activez le chaînage des connexions sur les deux appliances Citrix Gateway :

```
set appFlow param [-connectionChaining (ENABLED or DISABLED)]

set appflow param -connectionChaining ENABLED
```

Configurer Citrix Gateway avec l'utilitaire de configuration :

1. Configurez Citrix Gateway dans la première DMZ pour communiquer avec Citrix Gateway dans

la deuxième DMZ et lier Citrix Gateway dans la deuxième DMZ à Citrix Gateway dans la première DMZ.

a) Sous l'onglet**Configuration**, développez**Citrix Gateway** et cliquez sur**Serveurs virtuels**.

b) Dans le volet droit, double-cliquez sur le serveur virtuel et, dans le groupe Avancé, développez**Applications publiées**.

c) Cliquez sur **Serveur de saut suivant** et liez un serveur de saut suivant à la deuxième appliance Citrix Gateway.

2. Activez le double saut sur Citrix Gateway dans la deuxième DMZ.

a) Sous l'onglet**Configuration**, développez**Citrix Gateway** et cliquez sur**Serveurs virtuels**.

b) Dans le volet droit, double-cliquez sur le serveur virtuel, puis dans le groupe **Paramètres de base**, cliquez sur l'icône Modifier.

c) Développez plus, sélectionnez **Double saut** et cliquez sur **OK**.

3. Désactivez l'authentification sur le serveur virtuel sur Citrix Gateway dans la deuxième zone démilitarisée.

a) Dans l'onglet **Configuration** , développez **Citrix Gateway** et cliquez sur **Virtual Servers** .

b) Dans le volet droit, double-cliquez sur le serveur virtuel, puis dans le groupe **Paramètres de base**, cliquez sur l'icône Modifier.

c) Développez**Plus**et**désactivez Activer l'authentification**.

4. Activez l'une des appliances Citrix Gateway pour exporter des enregistrements TCP.

a) Dans l'onglet **Configuration** , développez **Citrix Gateway** et cliquez sur **Virtual Servers** .

b) Dans le volet droit, double-cliquez sur le serveur virtuel et dans le groupe Avancé, développez Stratégies.

c) Cliquez sur l'icône + et dans la liste **Choisir une stratégie**, sélectionnez **AppFlow** et dans la liste **Choisir un type**, sélectionnez **Autre demande TCP**.

d) Cliquez sur **Continuer**.

e) Ajoutez une liaison de stratégie, puis cliquez sur**Fermer**.

5. Activez l'autre appliance Citrix Gateway pour exporter des enregistrements ICA :

a) Dans l'onglet **Configuration** , développez **Citrix Gateway** et cliquez sur **Virtual Servers** .

b) Dans le volet droit, double-cliquez sur le serveur virtuel et dans le groupe **Avancé**, développez **Stratégies**.

c) Cliquez sur l'icône + et dans la liste **Choisir une stratégie**, sélectionnez AppFlow et dans la liste Choisir un type, sélectionnez **Autre demande TCP**.

d) Cliquez sur **Continuer**.

e) Ajoutez une liaison de stratégie, puis cliquez sur**Fermer**.

6. Activez le chaînage des connexions sur les deux appliances Citrix Gateway.

a) Sous l'onglet **Configuration**, accédez à **Système** > **Appflow**.

b) Dans le volet droit, dans le groupe **Paramètres**, double-cliquez sur **Modifier les paramètres Appflow**.

c) Select **Chaîne de connexion** et cliquez sur **OK**.

7. Configurez Citrix Gateway dans la première DMZ pour communiquer avec Citrix Gateway dans la deuxième DMZ et lier Citrix Gateway dans la deuxième DMZ à Citrix Gateway dans la première DMZ.

a) Sous l'onglet Configuration, développez **Citrix Gateway** et cliquez sur **Serveurs virtuels**.

b) Dans le volet droit, double-cliquez sur le serveur virtuel, puis dans le**groupe Avancé** , développez**Applications publiées**.

c) Cliquez sur **Serveur de saut suivant** et liez un serveur de saut suivant à la deuxième appliance Citrix Gateway.

8. Activez le double saut sur Citrix Gateway dans la deuxième DMZ.

a) Sous l'onglet Configuration, développez **Citrix Gateway** et cliquez sur **Serveurs virtuels**.

b) Dans le volet droit, double-cliquez sur le serveur virtuel, puis dans le groupe **Paramètres de base**, cliquez sur l'icône Modifier.

c) Développez Plus, sélectionnez **Double saut**, puis cliquez sur **OK**.

9. Désactivez l'authentification sur le serveur virtuel sur Citrix Gateway dans la deuxième zone démilitarisée.

a) Dans l'onglet Configuration , développez Citrix Gateway et cliquez sur **Virtual Servers** .

b) Dans le volet droit, double-cliquez sur le serveur virtuel, puis dans le groupe **Paramètres de base**, cliquez sur l'icône Modifier.

c) Développez**Plus**et**désactivez Activer l'authentification**.

10. Activez l'une des appliances Citrix Gateway pour exporter des enregistrements TCP.

a) Sous l'onglet Configuration, développez **Citrix Gateway** et cliquez sur **Serveurs virtuels**.

b) Dans le volet droit, double-cliquez sur le serveur virtuel, puis dans le groupe Avancé , développez**Stratégies**.

c) Cliquez sur l'icône**+** et dans la liste Choisir une stratégie , sélectionnez AppFlow, puis dans la liste **Choisir un type**, sélectionnez**Autre demande TCP**.

d) Cliquez sur **Continuer**.

e) Ajoutez une liaison de stratégie, puis cliquez sur**Fermer**.

11. Activez l'autre appliance Citrix Gateway pour exporter des enregistrements ICA.

a) Sous l'onglet Configuration, développez **Citrix Gateway** et cliquez sur **Serveurs virtuels**.

b) Dans le volet droit, double-cliquez sur le serveur virtuel et, dans le groupe Avancé, développez**Stratégies**.

c) Cliquez sur l'icône**+** et, dans la liste**Choose Policy** , sélectionnez AppFlow, puis dans la liste **Choose Type** , sélectionnez**Autre demande TCP**.

d) Cliquez sur **Continuer**.

e) Ajoutez une liaison de stratégie, puis cliquez sur**Fermer**.

12. Activez le chaînage des connexions sur les deux appliances Citrix Gateway.

Activer la collecte de données pour la surveillance des Citrix ADC déployés en mode transparent

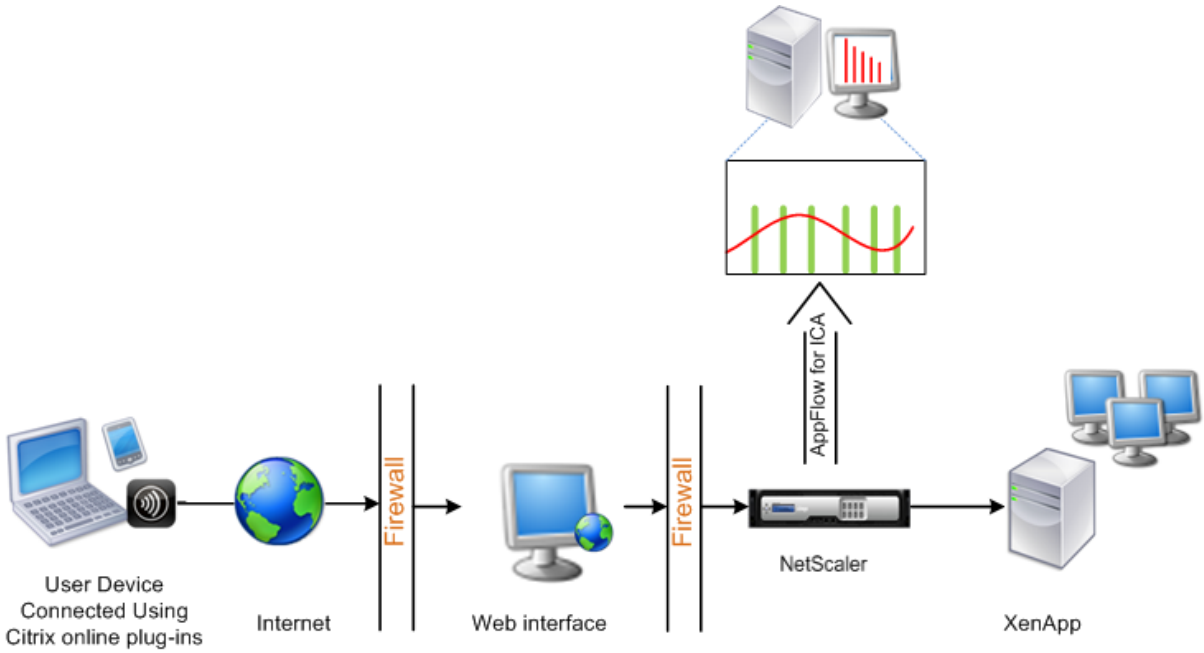
Lorsqu'un Citrix ADC est déployé en mode transparent, les clients peuvent accéder directement aux serveurs, sans aucun serveur virtuel intermédiaire. Si une appliance Citrix ADC est déployée en mode transparent dans un environnement Citrix Virtual Apps and Desktop, le trafic ICA n'est pas transmis via un VPN.

Après avoir ajouté Citrix ADC à l'inventaire Citrix ADM, vous devez activer AppFlow pour la collecte de données. L'activation de la collecte de données dépend du périphérique et du mode. Dans ce cas, vous devez ajouter Citrix ADM en tant que collecteur AppFlow sur chaque appliance Citrix ADC, et vous devez configurer une stratégie AppFlow pour collecter tout le trafic ICA ou spécifique qui circule via l'appliance.

> **Remarque**
>
> - Vous ne pouvez pas activer la collecte de données sur un Citrix ADC déployé en mode transparent à l'aide de l'utilitaire de configuration Citrix ADM.
> - Pour des informations détaillées sur les commandes et leur utilisation, consultez la sectionRéférence des commandes.
> - Pour plus d'informations sur les expressions de stratégie, consultez la sectionPolitiques et

> expressions.

La figure suivante illustre le déploiement réseau d'un Citrix ADM lorsqu'un Citrix ADC est déployé en mode transparent :



Pour configurer la collecte de données sur un appliance Citrix ADC à l'aide de l'interface de ligne de commande :

À l'invite de commandes, procédez comme suit :

1. Connectez-vous à une appliance.
2. Spécifiez les ports ICA sur lesquels l'appliance Citrix ADC écoute le trafic.

```
set ns param --icaPorts <port>...
```

Exemple :

```
set ns param -icaPorts 2598 1494
```

> **Remarque**
>
> - Vous pouvez spécifier jusqu'à 10 ports à l'aide de cette commande.
> - Le numéro de port par défaut est 2598. Vous pouvez modifier le numéro de port selon vos besoins.

3. Ajoutez NetScaler Insight Center en tant que collecteur AppFlow sur l'appliance Citrix ADC.


```
add appflow collector <name> -IPAddress <ip_addr>
```

Exemple :

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

> **Remarque** Pour afficher les collecteurs AppFlow configurés sur l'appliance Citrix ADC, utilisez la commande**show appflow collector**.

4. Créez une action AppFlow et associez le collecteur à l'action.

```
add appflow action <name> -collectors <string> ...
```

Exemple :

add AppFlow action act-collectors MyInsight

5. Créez une stratégie AppFlow pour spécifier la règle de génération du trafic.

```
add appflow policy <policyname> <rule> <action>
```

Exemple :

```
add appflow policy pol true act
```

6. Liez la stratégie AppFlow à un point de liaison global.

```
bind appflow global <policyname> <priority> -type <type>
```

Exemple :

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

> **Remarque**
>
> La valeur de**type** doit être ICA_REQ_OVERRIDE ou ICA_REQ_DEFAULT pour s'appliquer au trafic ICA.

7. Définissez la valeur du paramètre FlowRecordInterval pour AppFlow sur 60 secondes.

```
set appflow param -flowRecordInterval 60
```

Exemple :

```
set appflow param -flowRecordInterval 60
```

8. Enregistrez la configuration. Type : `save ns config`

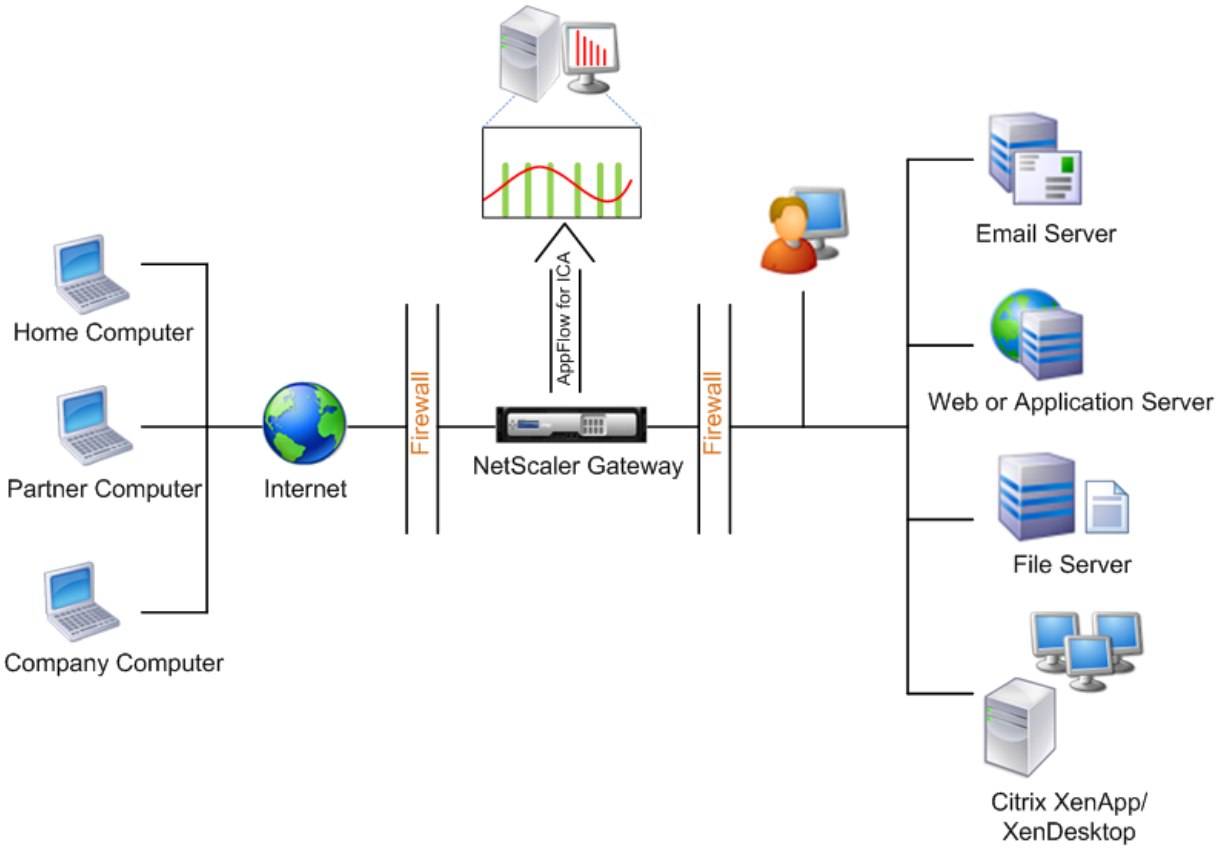
‘‘

Activer la collecte de données pour les appliances Citrix Gateway déployées en mode à saut unique

February 1, 2024

Lorsque vous déployez Citrix Gateway en mode à saut unique, il se trouve à la périphérie du réseau. L'instance Gateway fournit des connexions ICA proxy à l'infrastructure de mise à disposition des ordinateurs de bureau. Le déploiement à saut unique est le déploiement le plus simple et le plus courant. Le mode à saut unique assure la sécurité lorsqu'un utilisateur externe essaie d'accéder au réseau interne d'une organisation.
En mode saut unique, les utilisateurs accèdent aux appliances Citrix ADC via un réseau privé virtuel (VPN).

Pour commencer à collecter les rapports, vous devez ajouter l'appliance Citrix Gateway à l'inventaire Citrix Application Delivery Management (ADM) et activer AppFlow sur ADM.



Pour activer la fonctionnalité AppFlow à partir d'ADM :

1. Accédez à **Infrastructure** > **Instances**, puis sélectionnez l'instance Citrix ADC que vous souhaitez activer l'analyse.

2. Dans la liste **Action**, sélectionnez **Activer/Désactiver Insight**.
3. Sélectionnez les **serveurs virtuels VPN**, puis cliquez sur **Activer AppFlow**.
4. Dans le champ **Activer AppFlow**, tapez **true** et sélectionnez **ICA**.
5. Cliquez sur **OK**.

> **Remarque**
>
> Lorsque vous activez AppFlow en mode saut unique, les commandes suivantes s'exécutent en arrière-plan. Ces commandes sont explicitement spécifiées ici à des fins de dépannage.
>
> - `add appflow collector \<name\> -IPAddress \<ip\\_addr\>`
> - `add appflow action \<name\> -collectors \<string\>`
> - `set appflow param -flowRecordInterval \<secs\>`
> - `disable ns feature AppFlow`
> - `enable ns feature AppFlow`
> - `add appflow policy \<name\> \<rule\> \<expression\>`
> - `set appflow policy \<name\> -rule \<expression\>`
> - `bind vpn vserver \<vsname\> -policy \<string\> -type \<type\> >-priority \<positive\\_integer\>`
> - `set vpn vserver \<name\> -appflowLog ENABLED`
> - `save ns config`

Les données de canal virtuel EUEM font partie des données HDX Insight que Citrix ADM reçoit des instances de Gateway. Le canal virtuel EUEM fournit les données sur ICA RTT. Si le canal virtuel EUEM n'est pas activé, les données HDX Insight restantes sont toujours affichées sur Citrix ADM.

Activer la collecte de données pour surveiller les Citrix ADC déployés en mode transparent

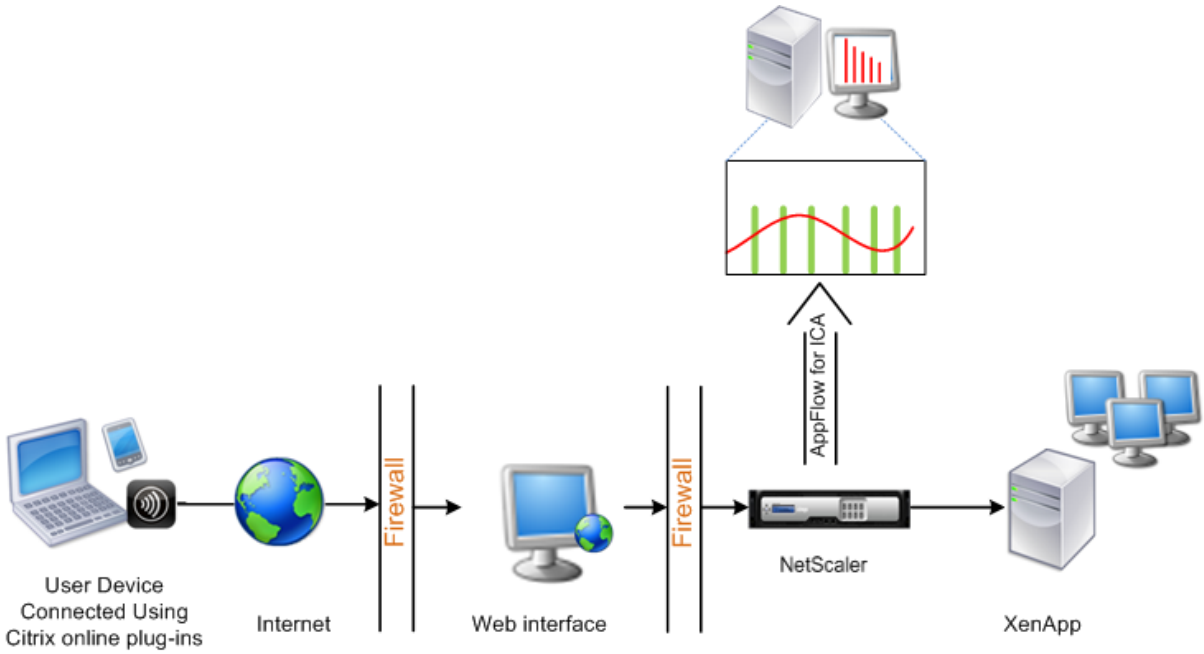
February 1, 2024

Lorsqu'un Citrix ADC est déployé en mode transparent, les clients peuvent accéder directement aux serveurs, sans aucun serveur virtuel intermédiaire. Si un Citrix ADC est déployé en mode transparent dans un environnement Citrix Virtual Apps and Desktops, le trafic ICA n'est pas transmis via un VPN.

Après avoir ajouté Citrix ADC à l'inventaire Citrix ADM, vous devez activer AppFlow pour la collecte de données. L'activation de la collecte de données dépend du périphérique et du mode. Dans ce cas, vous devez ajouter Citrix ADM en tant que collecteur AppFlow sur chaque instance de Citrix ADC, et vous devez configurer une stratégie AppFlow pour collecter tout le trafic ICA ou un trafic spécifique qui traverse l'appliance.

> **Remarque**
>
> - Vous ne pouvez pas activer la collecte de données sur un Citrix ADC déployé en mode transparent à l'aide de l'utilitaire de configuration Citrix ADM.
> - Pour des informations détaillées sur les commandes et leur utilisation, consultez la sectionRéférence des commandes.
> - Pour plus d'informations sur les expressions de stratégie, consultez la sectionPolitiques et expressions.

La figure suivante illustre le déploiement réseau d'un Citrix ADM lorsqu'un Citrix ADC est déployé en mode transparent :



Pour configurer la collecte de données sur un appliance Citrix ADC à l'aide de l'interface de ligne de commande :

À l'invite de commandes, procédez comme suit :

1. Connectez-vous à une appliance.
2. Spécifiez les ports ICA sur lesquels l'appliance Citrix ADC écoute le trafic.

```
set ns param --icaPorts \<port\>...
<!--NeedCopy-->
```

Exemple :


```
set ns param -icaPorts 2598 1494
<!--NeedCopy-->
```

> **Remarque**
>
> - Vous pouvez spécifier jusqu'à 10 ports à l'aide de cette commande.
> - Le numéro de port par défaut est 2598. Vous pouvez modifier le numéro de port selon vos besoins.

3. Ajoutez NetScaler Insight Center en tant que collecteur AppFlow sur l'instance Citrix ADC.

```
add appflow collector <name> -IPAddress <ip_addr>
<!--NeedCopy-->
```

Exemple :

```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```

> **Remarque** Pour afficher les collecteurs AppFlow configurés sur l'instance Citrix ADC, utilisez la commande **show appflow collector**.

4. Créez une action AppFlow et associez le collecteur à l'action.

```
add appflow action <name> -collectors <string> ...
<!--NeedCopy-->
```

Exemple :

```
add appflow action act -collectors MyInsight
<!--NeedCopy-->
```

5. Créez une stratégie AppFlow pour spécifier la règle de génération du trafic.

```
add appflow policy <policyname> <rule> <action>
<!--NeedCopy-->
```

Exemple :

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. Liez la stratégie AppFlow à un point de liaison global.

```
bind appflow global <policyname> <priority> -type <type>
<!--NeedCopy-->
```

Exemple :

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--NeedCopy-->
```


> **Remarque**
>
> La valeur de**type** doit être ICA_REQ_OVERRIDE ou ICA_REQ_DEFAULT pour s'appliquer au trafic ICA.

7. Définissez la valeur du paramètre FlowRecordInterval pour AppFlow sur 60 secondes.

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

8. Enregistrez la configuration.

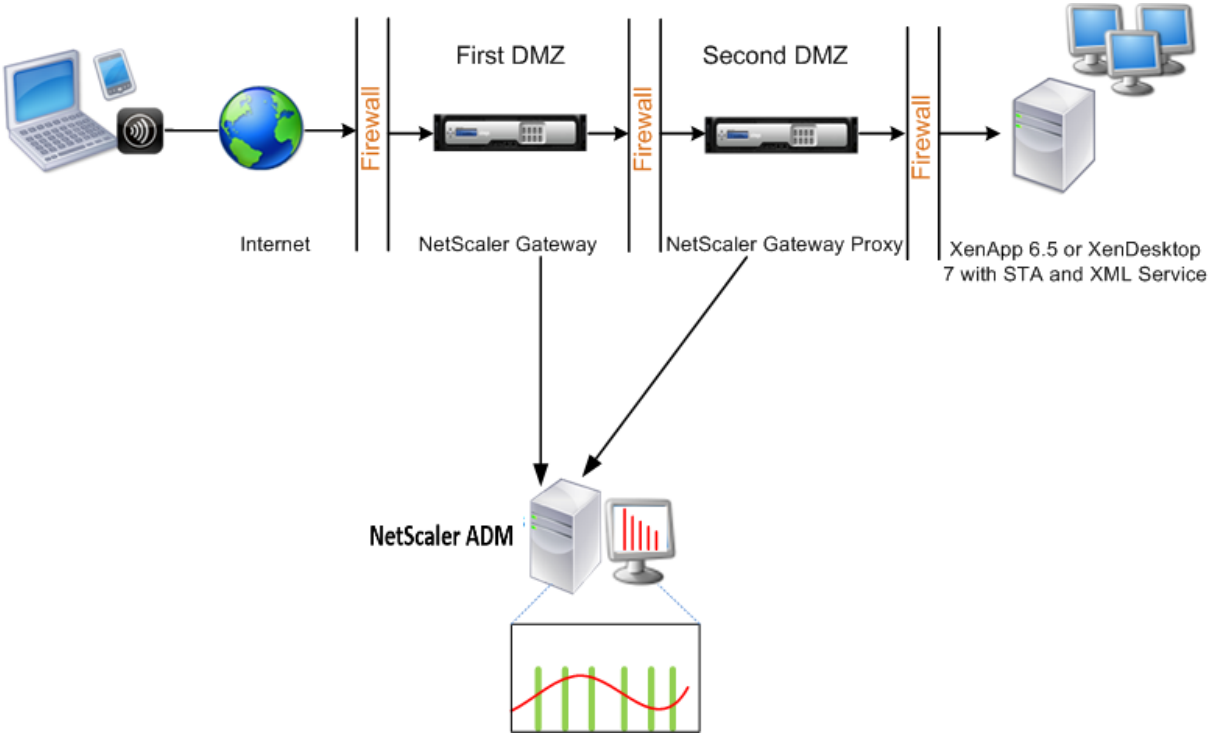
```
save ns config
<!--NeedCopy-->
```

Activer la collecte de données pour les appliances Citrix Gateway déployées en mode double saut

February 1, 2024

Le mode double saut Citrix Gateway fournit une protection supplémentaire au réseau interne d'une organisation, car un attaquant devrait pénétrer plusieurs zones de sécurité ou zones démilitarisées (DMZ) pour atteindre les serveurs du réseau sécurisé. Si vous souhaitez analyser le nombre de sauts (appliances Citrix Gateway) à travers lesquels les connexions ICA passent, ainsi que les détails sur la latence sur chaque connexion TCP et son rapport avec la latence ICA totale perçue par le client, vous devez installer Citrix ADM afin que les appliances Citrix Gateway rapporter ces statistiques de l'état civil.

Figure 3. Citrix ADM déployé en mode double saut



Citrix Gateway dans la première DMZ gère les connexions utilisateur et exécute les fonctions de sécurité d'un VPN SSL. Cette passerelle Citrix Gateway chiffre les connexions utilisateur, détermine comment les utilisateurs sont authentifiés et contrôle l'accès aux serveurs du réseau interne.

Citrix Gateway dans la deuxième DMZ sert de périphérique proxy Citrix Gateway. Cette passerelle Citrix Gateway permet au trafic ICA de traverser la deuxième zone démilitarisée pour terminer les connexions utilisateur à la batterie de serveurs.

Le Citrix ADM peut être déployé soit dans le sous-réseau appartenant à l'appliance Citrix Gateway dans la première zone démilitarisée, soit dans le sous-réseau appartenant à la seconde zone démilitarisée de l'appliance Citrix Gateway. Dans l'image ci-dessus, Citrix ADM et Citrix Gateway de la première DMZ sont déployés dans le même sous-réseau.

En mode double saut, Citrix ADM collecte les enregistrements TCP d'une appliance et les enregistrements ICA de l'autre appliance. Après avoir ajouté les appliances Citrix Gateway à l'inventaire Citrix ADM et activé la collecte des données, chaque appliance exporte les rapports en gardant le suivi du nombre de sauts et de l'ID de chaîne de connexion.

Pour que Citrix ADM identifie l'appliance qui exporte des enregistrements, chaque appliance est spécifiée avec un nombre de sauts et chaque connexion est spécifiée avec un ID de chaîne de connexion. Le nombre de sauts représente le nombre d'appliances Citrix Gateway via lesquelles le trafic circule d'un client vers les serveurs. L'ID de chaîne de connexion représente les connexions de bout en bout entre le client et le serveur.

Citrix ADM utilise le nombre de sauts et l'ID de chaîne de connexion pour corréler les données des

appliances Citrix Gateway et générer les rapports.

Pour surveiller les appliances Citrix Gateway déployées dans ce mode, vous devez d'abord ajouter Citrix Gateway à l'inventaire Citrix ADM, activer AppFlow sur Citrix ADM, puis afficher les rapports sur le tableau de bord Citrix ADM.

Activer la collecte de données sur Citrix ADM

Si vous activez Citrix ADM pour commencer à collecter les détails ICA à partir des deux appliances, les détails collectés sont redondants. Il s'agit des deux appliances qui signalent les mêmes mesures. Pour remédier à cette situation, vous devez activer AppFlow pour TCP sur l'un des premiers dispositifs Citrix Gateway, puis activer AppFlow pour ICA sur le second dispositif. Ce faisant, l'une des appliances exporte les enregistrements ICA AppFlow et l'autre exporte les enregistrements TCP AppFlow. Cela permet également d'économiser le temps de traitement lors de l'analyse du trafic ICA.

Pour activer la fonctionnalité AppFlow à partir de Citrix ADM :

1. Accédez à **Infrastructure > Instances** et sélectionnez l'instance Citrix ADC pour laquelle vous souhaitez activer les analyses.
2. Dans la liste **Action**, sélectionnez **Activer/Désactiver Insight**.
3. Sélectionnez les serveurs virtuels VPN, puis cliquez sur **Activer AppFlow**.
4. Dans le champ **Activer AppFlow**, tapez **true**et sélectionnez **ICA/TCP** pour le trafic ICA un trafic TCP respectivement.

   > **Remarque**
   >
   > Si la journalisation AppFlow n'est pas activée pour les services ou groupes de services sur l'appliance Citrix ADC, le tableau de bord Citrix ADM n'affiche pas les enregistrements, même si la colonne Insight affiche Activé.

5. Cliquez sur **OK**.

Configurer les appliances Citrix Gateway pour exporter des données

Après avoir installé les appliances Citrix Gateway, vous devez configurer les paramètres suivants sur les appliances Citrix Gateway pour exporter les rapports vers Citrix ADM :

- Configurez les serveurs virtuels des appliances Citrix Gateway dans la première et la deuxième zone démilitarisée pour communiquer entre eux.
- Liez le serveur virtuel Citrix Gateway dans la deuxième zone DMZ au serveur virtuel Citrix Gateway dans la première zone DMZ.

- Activez le double saut sur Citrix Gateway dans la deuxième DMZ.
- Désactivez l'authentification sur le serveur virtuel Citrix Gateway dans la deuxième DMZ.
- Permettre à l'une des appliances Citrix Gateway d'exporter des enregistrements ICA
- Activez l'autre appliance Citrix Gateway pour exporter des enregistrements TCP :
- Activez le chaînage des connexions sur les deux appliances Citrix Gateway.

Configurer Citrix Gateway à l'aide de l'interface de ligne de commande :

1. Configurez le serveur virtuel Citrix Gateway dans la première zone DMZ pour qu'il communique avec le serveur virtuel Citrix Gateway dans la deuxième zone DMZ.

add vpn nextHopServer [**-secure**(ON OFF)] [**-imgGifToPng**] ...

```
add vpn nextHopServer nh1 10.102.2.33 8443 –secure ON
<!--NeedCopy-->
```

2. Liez le serveur virtuel Citrix Gateway dans la deuxième zone DMZ au serveur virtuel Citrix Gateway dans la première zone DMZ. Exécutez la commande suivante sur Citrix Gateway dans la première DMZ :

   bind vpn vserver <name> **-nextHopServer** <name>

```
bind vpn vserver vs1 -nextHopServer nh1
<!--NeedCopy-->
```

3. Activez le double saut et AppFlow sur Citrix Gateway dans la deuxième DMZ.

set vpn vserver [**- doubleHop** (ENABLED DISABLED)] [**- appflowLog** (ENABLED DISABLED)]

```
set vpn vserver vpnhop2 –doubleHop ENABLED –appFlowLog ENABLED
<!--NeedCopy-->
```

4. Désactivez l'authentification sur le serveur virtuel Citrix Gateway dans la deuxième DMZ.

set vpn vserver [**-authentication** (ON OFF)]

```
set vpn vserver vs -authentication OFF
<!--NeedCopy-->
```


5. Activez l'une des appliances Citrix Gateway pour exporter des enregistrements TCP.

   bind vpn vserver<name> [**-policy**<string> **-priority**<positive_integer>] [**-type**<type>]

```
bind vpn vserver vpn1 -policy appflowpol1 -priority 101  – type
   OTHERTCP_REQUEST
<!--NeedCopy-->
```

6. Activez l'autre appliance Citrix Gateway pour exporter des enregistrements ICA :

   bind vpn vserver<name> [**-policy**<string> **-priority**<positive_integer>] [**-type**<type>]

```
bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
   ICA_REQUEST
<!--NeedCopy-->
```

7. Activez le chaînage des connexions sur les deux appliances Citrix Gateway :

set appFlow DISABLED)]
param [**-connectionChaining** (ENABLED

```
set appflow param -connectionChaining ENABLED
<!--NeedCopy-->
```

Configuration de Citrix Gateway à l'aide de l'utilitaire de configuration :

1. Configurez Citrix Gateway dans la première DMZ pour communiquer avec Citrix Gateway dans la deuxième DMZ et lier Citrix Gateway dans la deuxième DMZ à Citrix Gateway dans la première DMZ.

   a) Sous l'onglet**Configuration**, développez**Citrix Gateway** et cliquez sur**Serveurs virtuels**.

   b) Dans le volet droit, double-cliquez sur le serveur virtuel et, dans le groupe Avancé, développez**Applications publiées**.

   c) Cliquez sur **Serveur de saut suivant** et liez un serveur de saut suivant à la deuxième appliance Citrix Gateway.

2. Activez le double saut sur Citrix Gateway dans la deuxième DMZ.

   a) Sous l'onglet**Configuration**, développez**Citrix Gateway** et cliquez sur**Serveurs virtuels**.

   b) Dans le volet droit, double-cliquez sur le serveur virtuel, puis dans le groupe **Paramètres de base**, cliquez sur l'icône Modifier.

   c) Développez**Plus**, sélectionnez**Double saut**et cliquez sur**OK**.

3. Désactivez l'authentification sur le serveur virtuel sur Citrix Gateway dans la deuxième zone démilitarisée.

a) Dans l'onglet **Configuration** , développez **Citrix Gateway** et cliquez sur **Virtual Servers** .

b) Dans le volet droit, double-cliquez sur le serveur virtuel, puis dans le groupe **Paramètres de base**, cliquez sur l'icône Modifier.

c) Développez**Plus**et**désactivez Activer l'authentification**.

4. Activez l'une des appliances Citrix Gateway pour exporter des enregistrements TCP.

a) Dans l'onglet **Configuration** , développez **Citrix Gateway** et cliquez sur **Virtual Servers** .

b) Dans le volet droit, double-cliquez sur le serveur virtuel et dans le groupe Avancé, développez Stratégies.

c) Cliquez sur l'icône + et, dans la liste**Choisir une stratégie**, sélectionnez**AppFlow**, puis dans la liste déroulante**Choisir un type**, sélectionnez**Autre demande TCP**.

d) Cliquez sur **Continuer**.

e) Ajoutez une liaison de stratégie, puis cliquez sur**Fermer**.

5. Activez l'autre appliance Citrix Gateway pour exporter des enregistrements ICA :

a) Dans l'onglet **Configuration** , développez **Citrix Gateway** et cliquez sur **Virtual Servers** .

b) Dans le volet droit, double-cliquez sur le serveur virtuel et, dans le groupe**Avancé**, développez**Stratégies**.

c) Cliquez sur l'icône + et, dans la liste déroulante**Choisir une stratégie**, sélectionnez**AppFlow**et, dans la liste déroulante Choisir un type, sélectionnez**Autre demande TCP**.

d) Cliquez sur **Continuer**.

e) Ajoutez une liaison de stratégie, puis cliquez sur**Fermer**.

6. Activez le chaînage des connexions sur les deux appliances Citrix Gateway.

a) Sous l'onglet**Configuration**, accédez à**Système > Appflow**.

b) Dans le volet droit, dans le groupe **Paramètres**, cliquez sur **Modifier les paramètres de flux d'applications**.

c) Select **Chaîne de connexion** et cliquez sur **OK**.

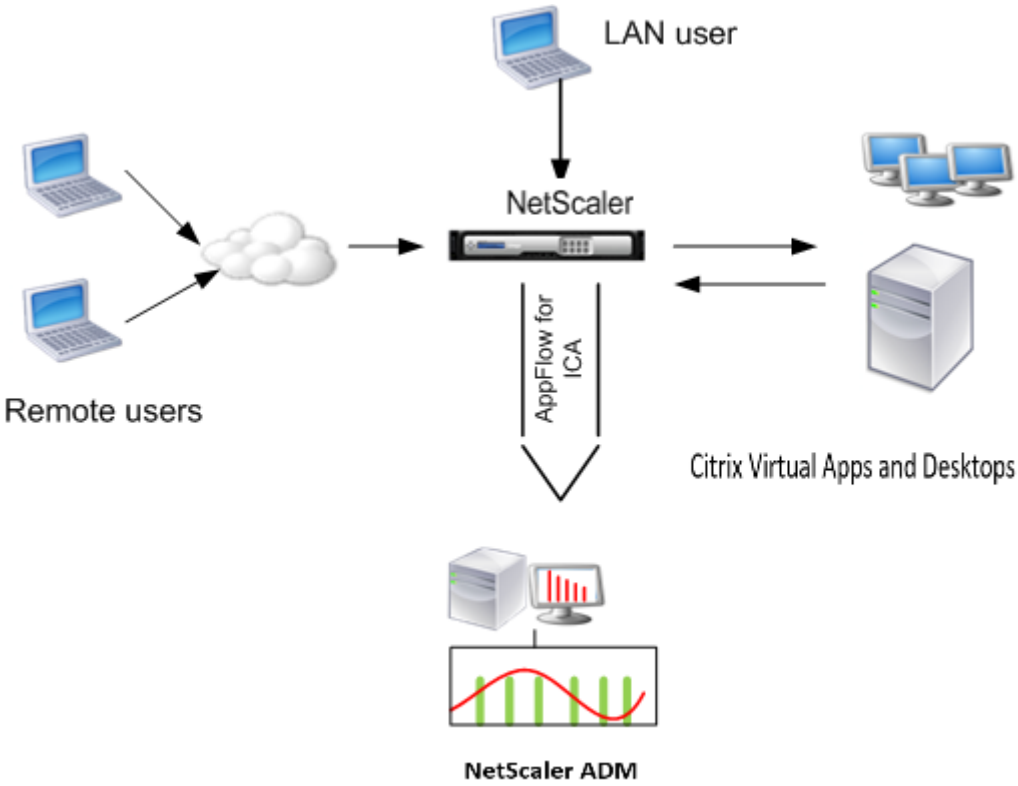
Activer la collecte de données pour surveiller les Citrix ADC déployés en mode utilisateur LAN

February 1, 2024

Les utilisateurs externes qui accèdent aux applications Citrix Virtual App ou Desktop doivent s'authentifier sur Citrix Gateway. Toutefois, les utilisateurs internes peuvent ne pas avoir besoin d'être redirigés vers Citrix Gateway. En outre, dans un déploiement en mode transparent, l'administrateur doit appliquer manuellement les stratégies de routage afin que les demandes soient redirigées vers l'appliance Citrix ADC.

Pour surmonter ces difficultés et pour que les utilisateurs LAN se connectent directement aux applications Citrix Virtual Apps and Desktops, vous pouvez déployer l'appliance Citrix ADC en mode utilisateur LAN en configurant un serveur virtuel de redirection de cache, qui agit en tant que proxy SOCKS sur l'appliance Citrix Gateway.

Figure 4. Citrix ADM déployé en mode utilisateur LAN



Remarque L'appliance Citrix ADM et Citrix Gateway résident dans le même sous-réseau.

Pour surveiller les appliances Citrix ADC déployées dans ce mode, ajoutez d'abord l'appliance Citrix ADC à l'inventaire NetScaler Insight, activez AppFlow, puis consultez les rapports sur le tableau de bord.

Après avoir ajouté l'appliance Citrix ADC à l'inventaire Citrix ADM, vous devez activer AppFlow pour la collecte de données.

> **Remarque**
>
> - Vous ne pouvez pas activer la collecte de données sur un Citrix ADC déployé en mode utilisateur LAN à l'aide de l'utilitaire de configuration Citrix ADM.
> - Pour des informations détaillées sur les commandes et leur utilisation, consultez la section Référence des commandes .
> - Pour plus d'informations sur les expressions de stratégie, voir Stratégies et expressions .

Pour configurer la collecte de données sur un appliance Citrix ADC à l'aide de l'interface de ligne de commande :

À l'invite de commandes, procédez comme suit :

1. Connectez-vous à une appliance.
2. Ajoutez un serveur virtuel de redirection de cache proxy avec l'IP et le port proxy, et spécifiez le type de service HDX.

```
add cr vserver <name> <servicetype> [<ipaddress> <port>] [-
   cacheType <cachetype>] [ - cltTimeout <secs>]
<!--NeedCopy-->
```

Exemple :

```
add cr vserver cr1 HDX 10.12.2.2 443 – cacheType FORWARD –
   cltTimeout 180
<!--NeedCopy-->
```

> **Remarque** Si vous accédez au réseau LAN à l'aide d'une appliance Citrix Gateway, ajoutez une action à appliquer par une stratégie correspondant au trafic VPN.

```
add vpn trafficAction** \<name\> \<qual\> \[-HDX ( ON | OFF )\]

add vpn trafficPolicy** \<name\> \<rule\> \<action\>
<!--NeedCopy-->
```

Exemple :

```
add vpn trafficAction act1 tcp -HDX ON

add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
<!--NeedCopy-->
```

3. Ajoutez Citrix ADM en tant que collecteur AppFlow sur l'appliance Citrix ADC.

```
add appflow collector** \<name\> \*\*-IPAddress\*\* \\<ip\\_addr
   \\>
<!--NeedCopy-->
```


Exemple :

```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```

4. Créez une action AppFlow et associez le collecteur à l'action.

```
add appflow action** \<name\> \*\*-collectors\*\* \<string\> ...
<!--NeedCopy-->
```

Exemple :

```
add appflow action act -collectors MyInsight
<!--NeedCopy-->
```

5. Créez une stratégie AppFlow pour spécifier la règle de génération du trafic.

```
add appflow policy** \<policyname\> \<rule\> \<action\>
<!--NeedCopy-->
```

Exemple :

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. Liez la stratégie AppFlow à un point de liaison global.

```
bind appflow global** \<policyname\> \<priority\> \*\*-type\*\* \<
   type\>
<!--NeedCopy-->
```

Exemple :

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--NeedCopy-->
```

> **Remarque**
>
> La valeur de type doit être ICA_REQ_OVERRIDE ou ICA_REQ_DEFAULT pour s'appliquer au trafic ICA.

7. Définissez la valeur du paramètre FlowRecordInterval pour AppFlow sur 60 secondes.

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

Exemple :

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

8. Enregistrez la configuration.


```
save ns config
<!--NeedCopy-->
```

Créer des seuils et configurer des alertes pour HDX Insight

February 1, 2024

HDX Insight on Citrix Application Delivery Management (ADM) vous permet de surveiller le trafic HDX transitant par les instances Citrix ADC. Citrix ADM vous permet de définir des seuils sur différents compteurs utilisés pour surveiller le trafic Insight. Vous pouvez également configurer des règles et créer des alertes dans Citrix ADM.

Le type de trafic HDX est associé à diverses entités telles que les applications, les postes de travail, les passerelles, les licences et les utilisateurs. Chaque entité peut contenir différentes mesures qui leur sont associées. Par exemple, l'entité d'application est associée à divers accès, à la bande passante consommée par l'application et au temps de réponse du serveur. Une entité utilisateur peut être associée à la latence WAN, à la latence DC, à la RTT ICA et à la bande passante consommée par un utilisateur.

La gestion des seuils pour HDX Insight dans Citrix ADM vous a permis de créer des règles de manière proactive et de configurer des alertes chaque fois que les seuils définis sont dépassés. Cette gestion des seuils est désormais étendue pour configurer un groupe de règles de seuil. Vous pouvez désormais surveiller le groupe au lieu de suivre des règles individuelles. Un groupe de règles de seuil comprend une ou plusieurs règles de seuil définies par l'utilisateur pour des mesures choisies parmi des entités telles que des utilisateurs, des applications et des postes de travail. Chaque règle est surveillée par rapport à une valeur attendue que vous entrez lors de la création de la règle. Dans le cas d'une entité utilisateur, le groupe de seuil peut également être associé à une géolocalisation.

Une alerte est générée sur Citrix ADM uniquement si toutes les règles du groupe de seuils configuré sont violées. Par exemple, vous pouvez surveiller une application en fonction du nombre total de lancements de sessions et également du nombre de lancements d'applications sous la forme d'un groupe de seuil. Une alerte est générée uniquement si les deux règles ne sont pas respectées. Cela vous permet de définir des seuils plus réalistes pour une entité.

Voici quelques exemples :

- Règle de seuil1 : la RTT ICA (métrique) pour les utilisateurs (entité) doit être <= 100 ms
- Règle de seuil2 : la latence WAN (métrique) pour les utilisateurs (entité) doit être <= 100 ms

Un exemple de groupe de seuil peut être : {Règle de seuil 1 + Règle de seuil 2}

Pour créer une règle, vous devez d'abord sélectionner l'entité que vous souhaitez surveiller. Choisissez ensuite une mesure lors de la création d'une règle. Par exemple, vous pouvez sélectionner l'entité d'applications, puis sélectionner Nombre total de lancement de session ou Nombre de lancement d'applications. Vous pouvez créer une règle pour chaque combinaison d'une entité et d'une métrique. Utilisez les comparateurs fournis (>, <, >= et <=) et saisissez une valeur seuil pour chaque métrique.

> **Remarque**
>
> Si vous ne souhaitez pas surveiller plusieurs entités au sein d'un même groupe, vous devez créer un groupe de règles de seuil distinct pour chaque entité.

Lorsque la valeur d'un compteur dépasse la valeur d'un seuil, Citrix ADM génère un événement pour signaler un dépassement de seuil, et une alerte est créée pour chaque événement.

Vous devez configurer la façon dont vous recevez l'alerte. Vous pouvez activer l'affichage de l'alerte sur Citrix ADM et/ou recevoir l'alerte par e-mail ou par SMS sur votre appareil mobile. Pour les deux dernières actions, vous devez configurer le serveur de messagerie ou le serveur SMS sur Citrix ADM.

Les groupes de seuils peuvent également être liés aux géolocalisations pour la surveillance géographique spécifique de l'entité utilisateur.

Exemples de cas d'utilisation

ABC Inc. est une entreprise mondiale qui a des bureaux dans plus de 50 pays. L'entreprise dispose de deux centres de données, l'un à Singapour et l'autre en Californie qui hébergent Citrix Virtual Apps and Desktops. Les employés de l'entreprise accèdent aux Citrix Virtual Apps and Desktops dans le monde entier à l'aide de Citrix Gateway et de la redirection basée sur Citrix GSLB. Eric, l'administrateur Citrix Virtual Apps and Desktops pour ABC Inc. souhaite suivre l'expérience utilisateur de tous leurs bureaux afin d'optimiser la distribution des applications et des postes de travail pour un accès en tout lieu et en tout temps. Eric souhaite également vérifier les métriques de l'expérience utilisateur comme les RTT ICA, les latences, et augmenter les écarts de manière proactive.

Les utilisateurs d'ABC Inc. ont une présence distribuée. Certains utilisateurs sont situés à proximité du centre de données, tandis que d'autres sont situés plus loin du centre de données. Comme la base d'utilisateurs est largement distribuée, les mesures et les seuils correspondants varient également d'un endroit à l'autre. Par exemple, le RTT de l'ICA pour un site proche du centre de données peut être de 5 à 10 ms, alors qu'il peut être identique pour un site distant d'environ 100 ms.

Grâce à la gestion des groupes de règles de seuil pour HDX Insight, Eric peut définir des groupes de règles de seuil géo-spécifiques pour chaque emplacement et être alerté par e-mail ou SMS en cas de violation par zone. Eric est également capable de combiner le suivi de plusieurs mesures au sein d'un groupe de règles de seuil et de limiter la cause profonde aux problèmes de capacité, le cas échéant. Eric est désormais en mesure de suivre de manière proactive tout écart sans avoir à se soucier de la

complexité de la recherche manuelle à travers toutes les mesures du portefeuille Citrix Virtual Apps and Desktops.

Pour créer un groupe de règles de seuil et configurer des alertes pour HDX Insight à l'aide de Citrix ADM :

1. Dans Citrix ADM, accédez à **Analytics** > **Paramètres** > **Seuils**. Dans la page **Seuils** qui s'ouvre, cliquez sur **Ajouter**.
2. Sur la page **Créer des seuils et des alertes**, spécifiez les informations suivantes :

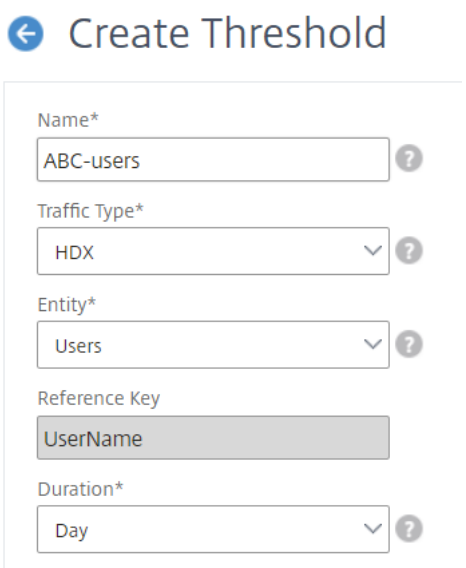
   a) **Nom**. Entrez un nom pour créer un événement pour lequel Citrix ADM génère une alerte.

   b) **Type de trafic**. Dans la zone de liste, sélectionnez HDX.

   c) **Entité**. Dans la zone de liste, sélectionnez la catégorie ou le type de ressource. Les entités diffèrent pour chaque type de trafic sélectionné précédemment.

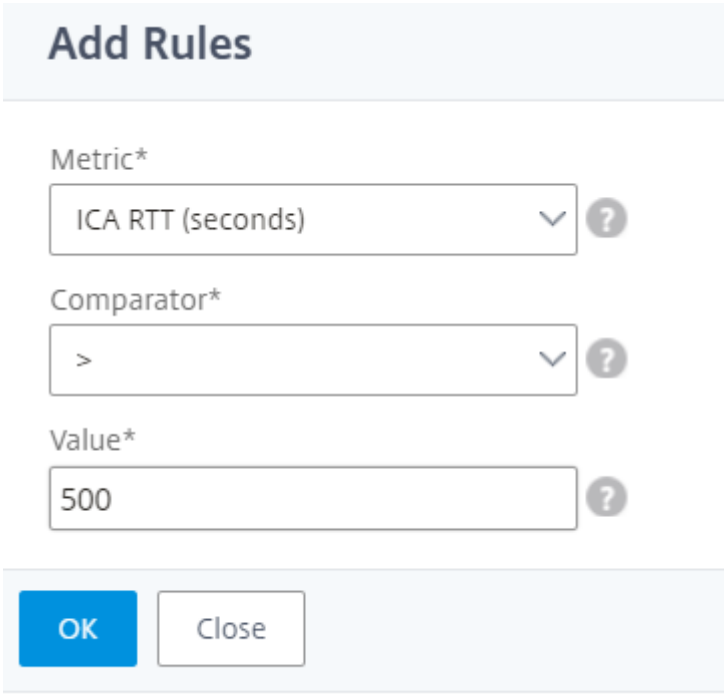
   d) **Clé de référence**. Une clé de référence est automatiquement générée en fonction du type de trafic et de l'entité que vous avez sélectionnés.

   e) **Durée**. Dans la zone de liste, sélectionnez l'intervalle de temps pendant lequel vous souhaitez surveiller l'entité. Vous pouvez surveiller les entités pendant une heure, une journée ou une semaine.

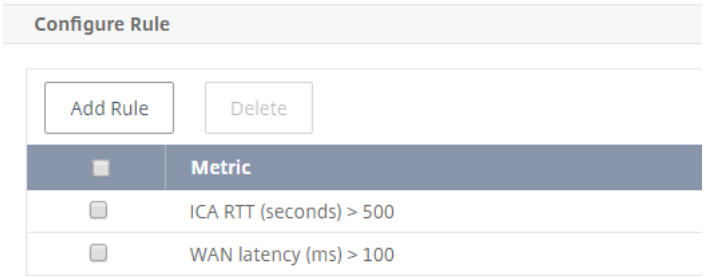


3. Création d'un groupe de règles de seuil pour toutes les entités :

   Pour le trafic HDX, vous devez créer une règle en cliquant **sur Ajouter une règle.**Entrez les valeurs dans la fenêtre contextuelle **Ajouter des règles** qui s'ouvre.

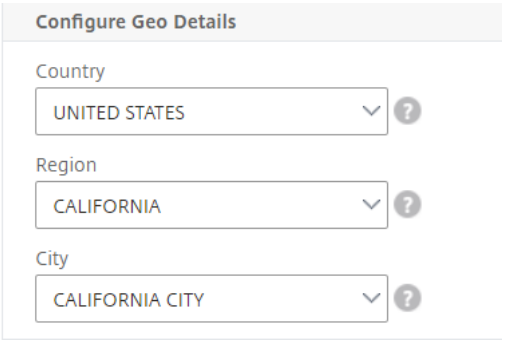


Vous pouvez créer plusieurs règles pour surveiller chaque entité. La création de plusieurs règles dans un seul groupe vous permet de surveiller les entités sous la forme d'un groupe de règles de seuil au lieu de règles individuelles. Cliquez sur **OK** pour fermer la fenêtre.



4. Configuration du balisage de géolocalisation pour l'entité Utilisateurs

   Vous pouvez également créer une alerte basée sur l'emplacement pour l'entité utilisateur dans la section **Configurer les détails géographiques**. L'image suivante montre un exemple de création d'un balisage basé sur la géolocalisation pour surveiller les performances de latence WAN pour les utilisateurs de la côte ouest des États-Unis.



5. Cliquez sur **Activer les seuils** pour permettre à Citrix ADM de commencer à surveiller les entités.
6. Vous pouvez également configurer des actions telles que les notifications par e-mail et les notifications par SMS.
7. Cliquez sur **Créer** pour créer un groupe de règles de seuil.

Affichage des rapports et des mesures HDX Insight

February 1, 2024

HDX insights fournit une visibilité complète des rapports et des mesures relatifs au trafic HDX sur vos instances Citrix ADC.

Vous pouvez afficher les métriques HDX de n'importe quelle entité sélectionnée. Les vues comprennent les catégories d'entités suivantes :

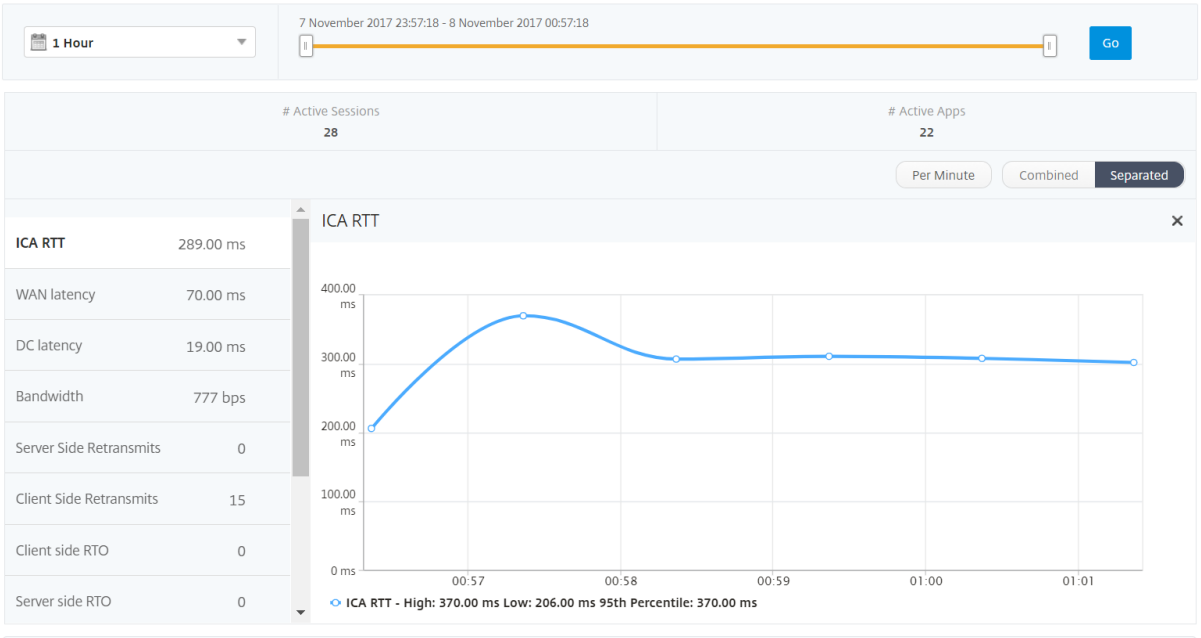
- **Utilisateurs** : affiche les rapports de tous les utilisateurs accédant à Citrix Virtual App ou Desktop dans l'intervalle de temps sélectionné.
- **Applications**: affiche les rapports relatifs au nombre total d'applications et toutes les informations pertinentes connexes, telles que le nombre total de fois que les applications ont été lancées dans l'intervalle de temps spécifié.
- **Instances** : affiche les rapports sur les instances Citrix ADC qui agissent comme des passerelles pour le trafic entrant.
- **Bureaux** : affiche les rapports des bureaux utilisés dans la période sélectionnée.
- **Licences** : affiche les rapports pour le nombre total de licences VPN SSL utilisées dans le créneau horaire spécifié.

> **Remarque**
>
> La valeur Licences ne s'applique pas aux appliances Citrix SD-WAN.

Rapports et mesures d'affichage des utilisateurs

Les rapports et les mesures de cette vue sont affichés par les utilisateurs Citrix Virtual Apps et Desktop.

Accédez à **Analytics** > **HDX Insight** > **Utilisateurs**.



Les rapports et mesures d'affichage utilisateur se composent des sections suivantes :

- Vue récapitulative
- Par vue utilisateur
- Vue par session utilisateur

Vue récapitulative

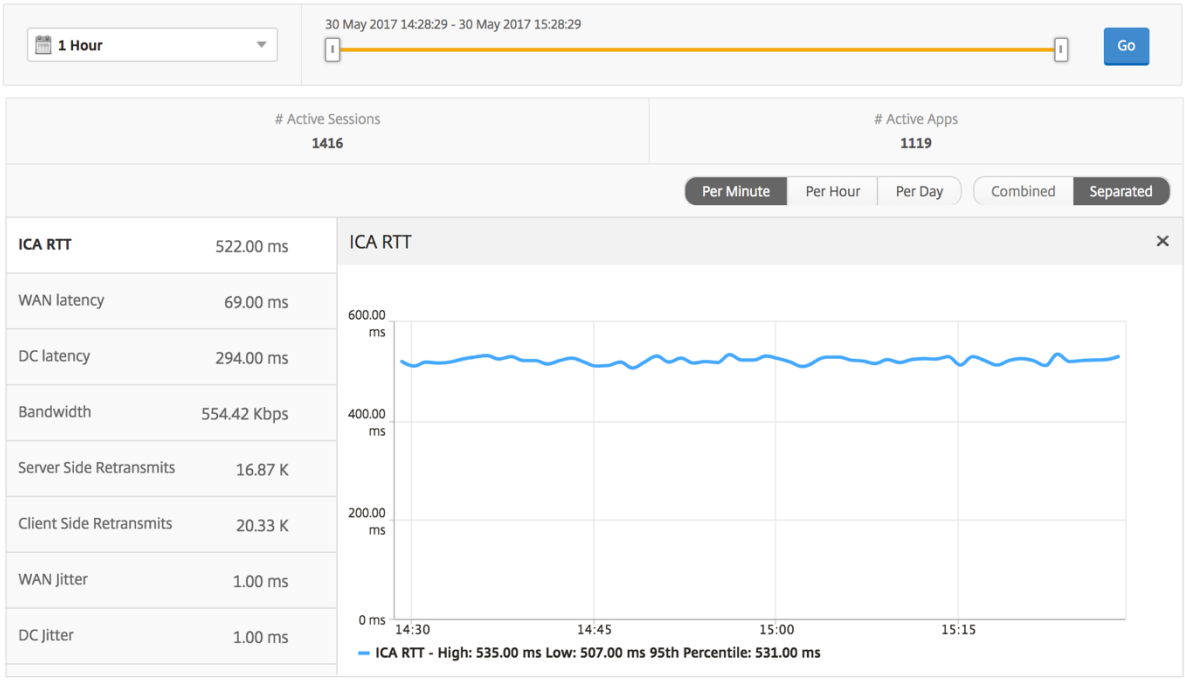
La vue récapitulative affiche les rapports de tous les utilisateurs qui se sont connectés au cours de la chronologie sélectionnée. Toutes les métriques/rapports de cette vue affichent les valeurs qui leur correspondent pour la période sélectionnée, sauf indication contraire.

Pour modifier la période sélectionnée :

1. Utilisez la liste de périodes ou le curseur temporel pour définir l'intervalle de temps souhaité.
2. Cliquez sur **Go**.

Graphique linéaire

Métriques	Description
Nombre de sessions actives	Ce nombre indique le nombre de sessions Citrix Virtual Apps and Desktops actives.
Nbre d'applications actives	Ce nombre indique le nombre de sessions actives de Citrix Virtual App.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps ou Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre Citrix Gateway et les serveurs VDI, CVAD ou StoreFront.
Bande passante	Nombre total d'octets par seconde pris pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et serveur back-end.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit sur la connexion entre Citrix ADC et le serveur back-end.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.



Rapport récapitulatif de l'utilisateur Voici les mesures spécifiques à ce rapport.

Mesures	Description
Nombre de sessions actives	Ce nombre indique le nombre de sessions Citrix Virtual App and Desktop actives.
Nbre d'applications actives	Ce nombre indique le nombre de sessions actives de Citrix Virtual App.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps ou Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre Citrix Gateway et les serveurs VDI, CVAD ou StoreFront.
Bande passante	Nombre total d'octets par seconde pris pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et serveur back-end.

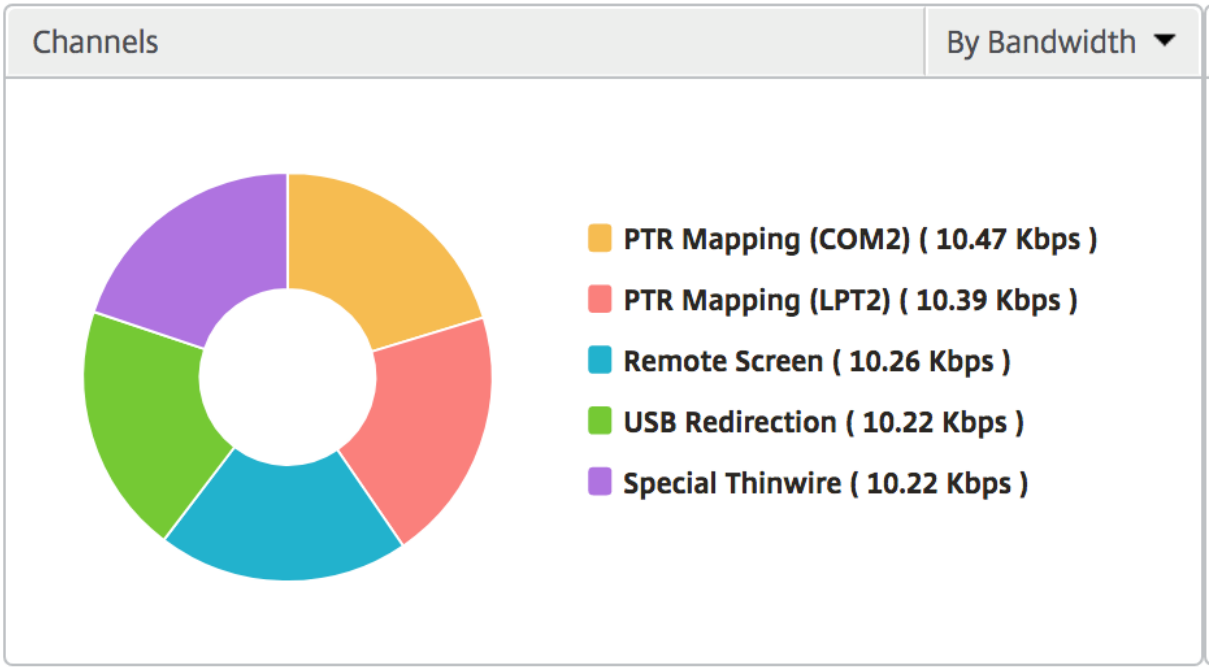
Mesures	Description
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
RTO rapide côté client	Nombre de fois où le délai de retransmission s' est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s' est produit sur la connexion entre Citrix ADC et le serveur back-end.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.
Nb total d'applications lancées	Total des applications lancées par l'utilisateur au cours de la période sélectionnée.
Nb total d'octets	Nombre total d'octets consommés par l' utilisateur pendant la période sélectionnée.
Ordinateurs de bureau actifs	Nombre total de Citrix Virtual Desktops actifs au cours d'un intervalle de temps donné.

Users

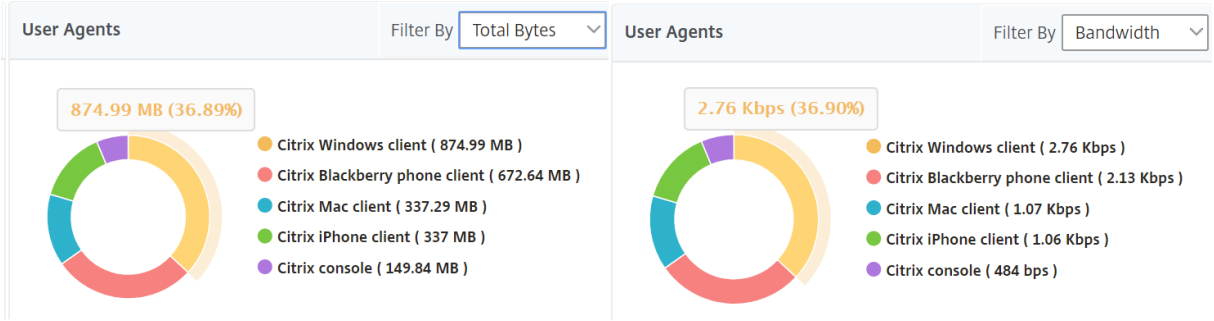
Search

User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT	WAN latency	DC latency	Bandwidth	Server Side Retransmits	Cl
liam	59	59	118	999.00 ms	57.00 ms	751.00 ms	47.25 Kbps	3.74 K	
jayden	59	59	118	999.00 ms	52.00 ms	751.00 ms	47.06 Kbps	3.71 K	
florinl	59	0	59	997.00 ms	52.00 ms	754.00 ms	23.66 Kbps	1.88 K	
ramas	59	0	59	997.00 ms	778.00 ms	1.00 ms	7.03 Kbps	0	
omerp	59	0	59	997.00 ms	57.00 ms	754.00 ms	23.80 Kbps	1.89 K	
grahmm	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.80 Kbps	1.89 K	
ryan	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.69 Kbps	1.88 K	
rajivs	59	0	59	801.00 ms	11.00 ms	1.00 ms	23.97 Kbps	0	
alexisc	117	0	118	622.00 ms	56.00 ms	392.00 ms	47.67 Kbps	1.88 K	
juan	59	59	118	169.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
lennoxl	59	0	59	169.00 ms	31.00 ms	30.00 ms	23.86 Kbps	0	
daniel	59	59	118	149.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
woojunek	58	0	59	149.00 ms	31.00 ms	30.00 ms	23.85 Kbps	0	
parkerf	59	0	59	149.00 ms	31.00 ms	30.00 ms	23.88 Kbps	0	
randyb	59	59	118	99.00 ms	11.00 ms	29.00 ms	47.71 Kbps	0	
bradp	177	0	177	74.00 ms	27.00 ms	1.00 ms	71.75 Kbps	0	

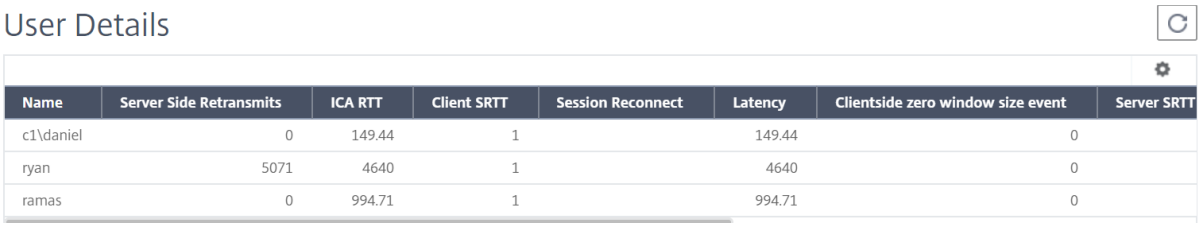
Canaux Les canaux représentent la bande passante globale ou le nombre total d'octets consommés par chaque canal virtuel ICA sous la forme d'un graphique en anneau. Vous pouvez également trier les mesures par bande passante ou Nombre total d'octets.



Agents utilisateurs Les agents utilisateurs représentent la bande passante globale/nombre total d'octets consommés par chaque client récepteur sous la forme d'un graphique en donut. Chaque segment coloré du graphique représente un client destinataire. La longueur du segment dépend du nombre d'utilisateurs qui lancent leurs applications sur ce client récepteur. Vous pouvez également trier les mesures par bande passante ou par nombre total d'octets.



Cliquez sur chaque segment pour afficher les détails des utilisateurs utilisant ce client récepteur.



Name	Server Side Retransmits	ICA RTT	Client SRTT	Session Reconnect	Latency	Clientside zero window size event	Server SRTT
c1\daniel	0	149.44	1		149.44	0	
ryan	5071	4640	1		4640	0	
ramas	0	994.71	1		994.71	0	

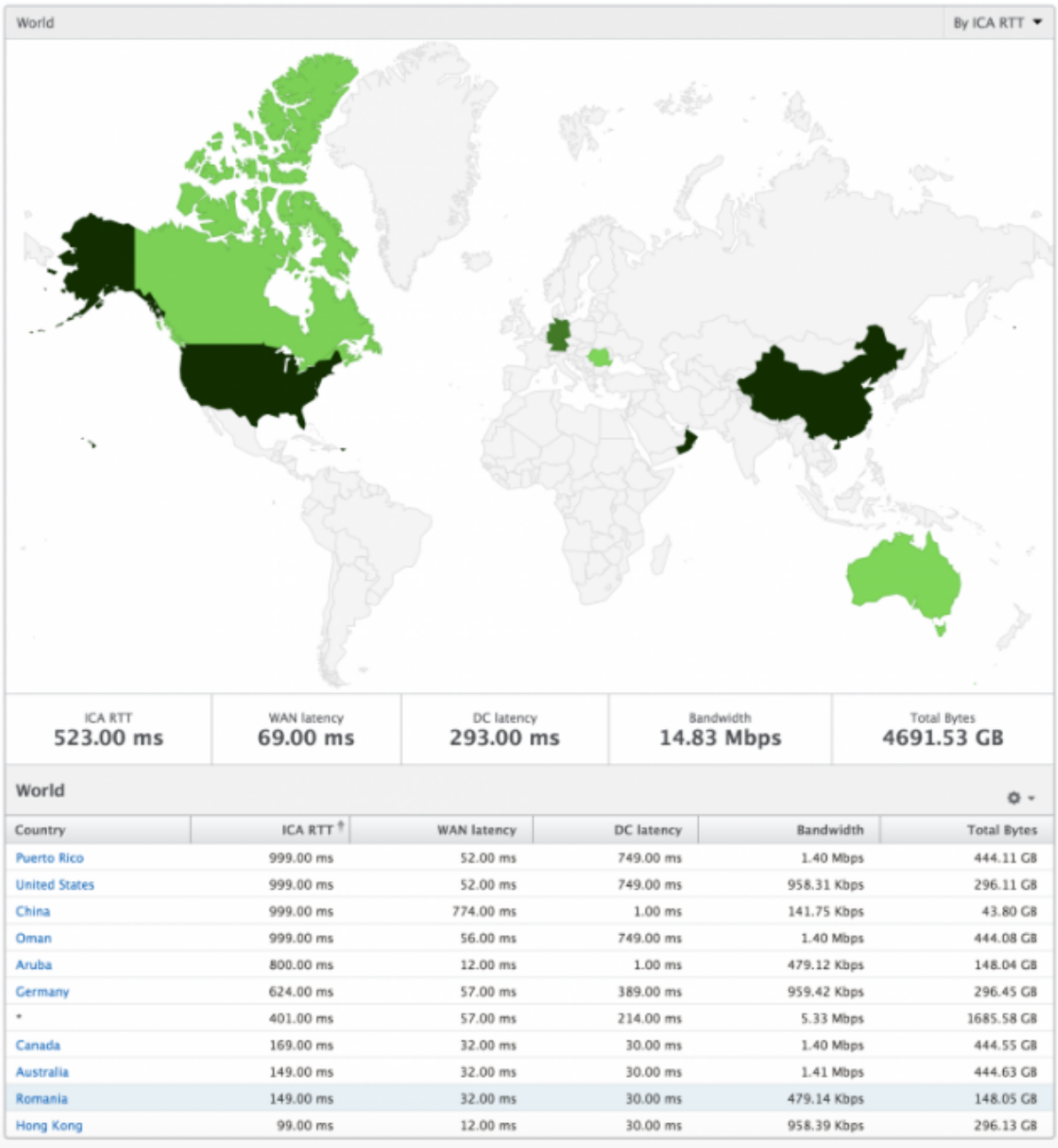
Nombre de violations des seuils Les mesures de nombre de violations des seuils représentent le nombre de seuils violés au cours de la période sélectionnée.

Carte du monde La vue Carte du monde dans HDX insights permet aux administrateurs de visualiser les détails des utilisateurs historiques et actifs d'un point de vue géographique. Les administrateurs peuvent avoir une vue du monde du système, accéder à un pays particulier et plus loin dans les villes en cliquant simplement sur la région. Les administrateurs peuvent approfondir l'exploration vers le bas pour afficher les informations par ville et par État. À partir de Citrix ADM version 12.0 et ultérieure, vous pouvez effectuer une exploration vers le bas vers les utilisateurs connectés à partir d'un emplacement géographique.

Les détails suivants peuvent être consultés sur la carte du monde dans un aperçu HDX, et la densité de chaque mesure est affichée sous la forme d'une carte thermique :

- RTT ICA
- Latence WAN
- Latence DC
- Bande passante

- Nb total d'octets



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

Vue par utilisateur

La vue par utilisateur fournit des rapports détaillés sur l'expérience utilisateur final pour un utilisateur sélectionné particulier.

Pour accéder aux mesures spécifiques d'un utilisateur :

1. Connectez-vous à votre Citrix ADM à l'aide d'un navigateur Web pris en charge.

2. Accédez à **Analytics** > **HDX Insight** > **Utilisateurs**.
3. Sélectionnez un utilisateur particulier dans le rapport récapitulatif Utilisateurs.

Graphique linéaire Le graphique en courbes affiche le résumé de toutes les mesures pour l'utilisateur sélectionné particulier pendant la période sélectionnée.

Rapport Sessions en cours/terminées Ce rapport est pertinent pour toutes les sessions utilisateur en cours/terminées pour l'utilisateur sélectionné. Ces mesures peuvent être triées par heure de début, reconnexions de session et nombre d'ACR.

Mesures	Description
ID de session	Une identité unique pour une session ICA.
Type de session	Application/Bureau.
État	Vert/rouge pour les sessions actives/inactives.
Délai d'hôte	Délai moyen du trafic ICA transitant par les Citrix ADC causé par le réseau du serveur.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Bande passante de session	La bande passante consommée par la session quel que soit l'intervalle de temps.
Octets par intervalle	Nombre d'octets consommés par la session pendant cet intervalle de temps particulier.
Start Time	Heure de début de la session.
Temps d'activité	Durée de la session.
Adresse IP cliente	IP de l'utilisateur final.
Adresse IP du serveur	Adresse IP du serveur Backend/Citrix Virtual App.
Adresse IP NetScaler	IP de gestion NetScaler (NSIP).
Type de client	Type de Receiver - Client Windows Citrix et ainsi de suite
Version du client	Version du Receiver.
MSI	Boolean (Oui/Non). Indique si la session est multiflux ICA.
Reconnexions de session	Nombre de fois où la session s'est reconnectée.

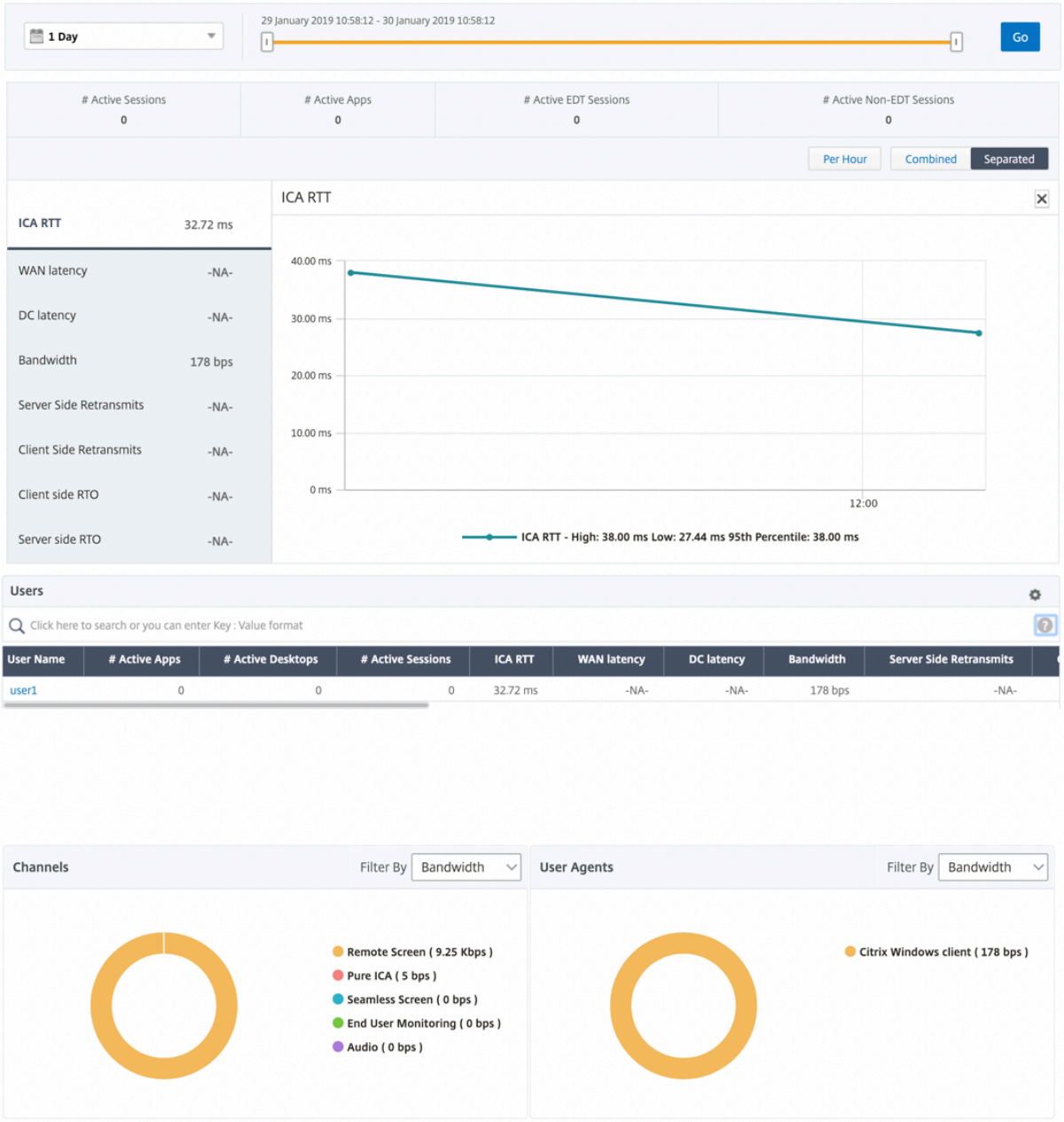
Mesures	Description
Nb d'ACR	Nombre total de fois où un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, le mode utilisateur/transparent de Citrix Gateway.
Pays	Pays à partir duquel la session a été créée.
Région	Région à partir de laquelle la session a été créée.
City	Ville à partir de laquelle la session a été créée.
État de l'USB	Actif/Inactif -Vert/Rouge.
Nombre d'instances USB acceptées	Le nombre d'instances USB acceptées.
Nombre d'instances USB rejetées	Le nombre d'instances USB rejetées.
Nombre d'instances USB arrêtées	Le nombre d'instances USB arrêtées.
Nom d'hôte du client	Le nom d'hôte du client.
Nombre de basculements HA	Nombre de fois où le basculement HA s'est produit.
Motif de la résiliation	Affiche la raison de l'arrêt d'une session. Par exemple, délai d'expiration de session ICA, session terminée par l'utilisateur.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps ou Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre Citrix Gateway et les serveurs VDI, CVAD ou StoreFront.
Nb total d'octets	Nombre total d'octets consommés par l'utilisateur pendant la période sélectionnée.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et serveur back-end.

Mesures	Description
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit sur la connexion entre Citrix ADC et le serveur back-end.

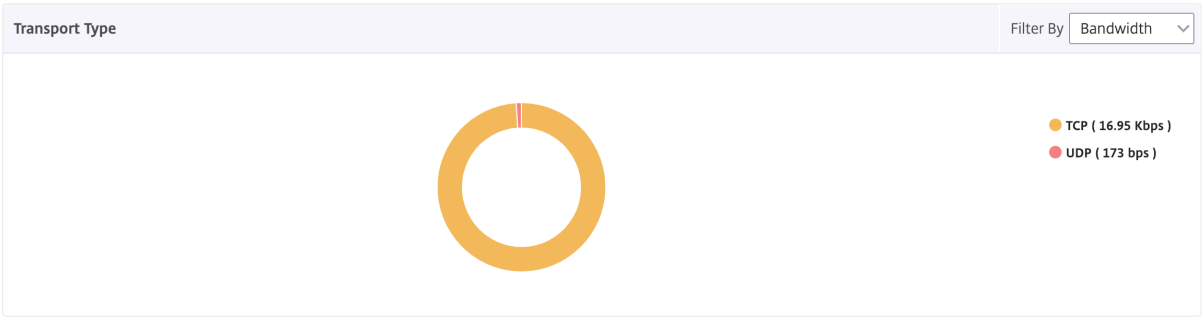
Prise en charge de l'EDT dans HDX insights

Citrix Application Delivery Management (ADM) prend désormais en charge le transport de données éclairé (EDT) pour afficher les analyses pour HDX Insight. En d'autres termes, ADM prend désormais en charge les protocoles UDP et TCP. La prise en charge d'EDT pour Citrix Gateway garantit une expérience utilisateur haute définition en session des bureaux virtuels pour les utilisateurs exécutant Citrix Receiver.

HDX Insight affiche désormais le nombre de sessions EDT et de sessions non EDT dans le rapport des sessions actives. Le tableau Utilisateurs affiche un rapport détaillé de tous les utilisateurs du système. Le tableau présente des mesures telles que la latence WAN, la latence DC, les retransmissions, les RTO et certaines de ces mesures ne sont pas disponibles pour les utilisateurs qui ont des sessions EDT car elles sont calculées à partir de la pile TCP actuellement. Par conséquent, ils apparaissent comme « NA ».



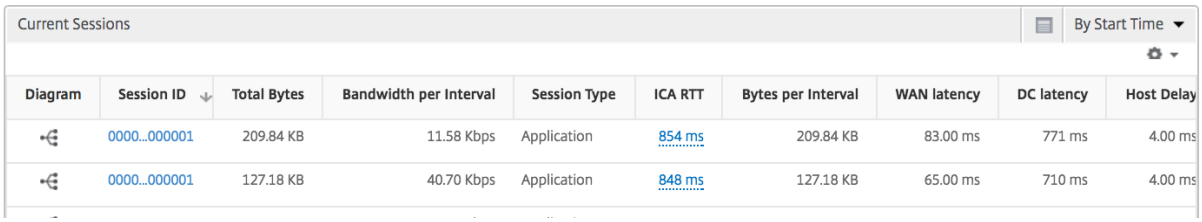
Un nouveau graphique en anneau a été introduit pour vous permettre de voir la bande passante consommée par l'utilisateur ainsi que le nombre total d'octets en fonction du type de protocole utilisé par les utilisateurs.

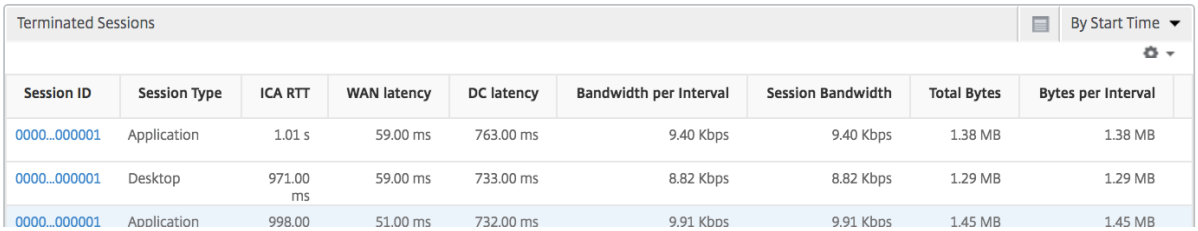


> **Remarque**
>
> EDT dans HDX Insight est pris en charge sur Citrix ADM à partir de la version 12.1 build 50.28 et est disponible sur les instances ADC à partir de la version 12.1 build 49.23.

Mesures HDX Insight disponibles à partir de Citrix ADM 12.0 et versions ultérieures :

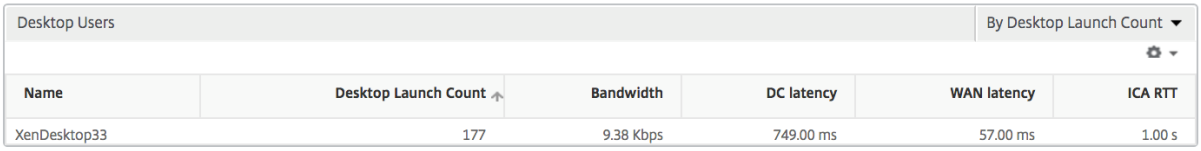
Latence côté client L7	La latence moyenne L7 observée entre le client ICA et l'instance de Citrix ADC. Cette mesure est utile dans le cas de périphériques non Citrix présents dans le chemin de remise.
Latence côté serveur L7	Latence moyenne L7 observée entre l'appareil Citrix ADC et l'application virtuelle Citrix. Cette mesure est utile dans le cas de périphériques non Citrix présents dans le chemin de remise.
Latence maximale de violation	La valeur la plus élevée de la latence L7 lorsqu'un dépassement d'un seuil défini pour un intervalle de temps défini se produit.
Latence moyenne des violations	Valeur moyenne de la latence L7 lorsque le système est dans un état « Latence L7 violée ».
Nombre de franchissements de seuil L7	Nombre de fois qu'une violation du seuil L7 s'est produite.



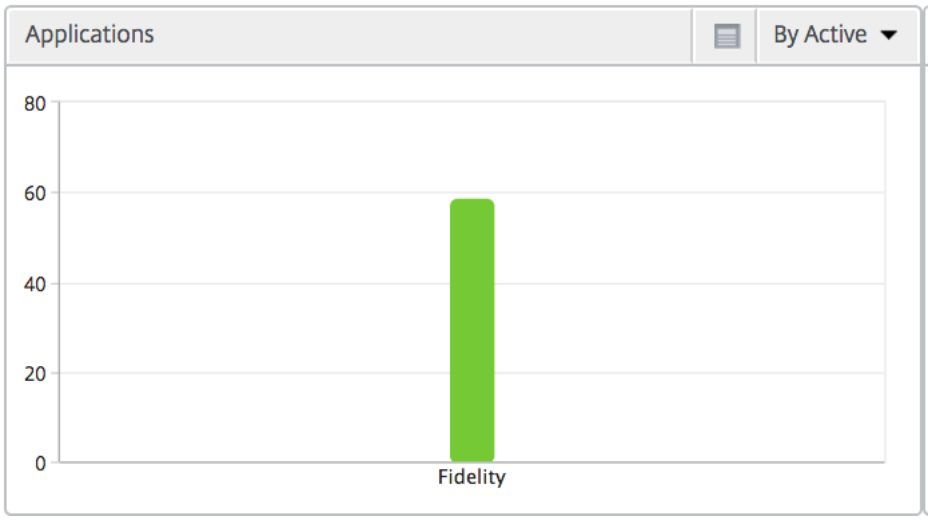


Utilisateurs de bureau Ce tableau donne un aperçu des sessions Citrix Virtual Desktop pour un utilisateur particulier. Ces mesures peuvent être triées par nombre de lancements de postes de travail et bande passante.

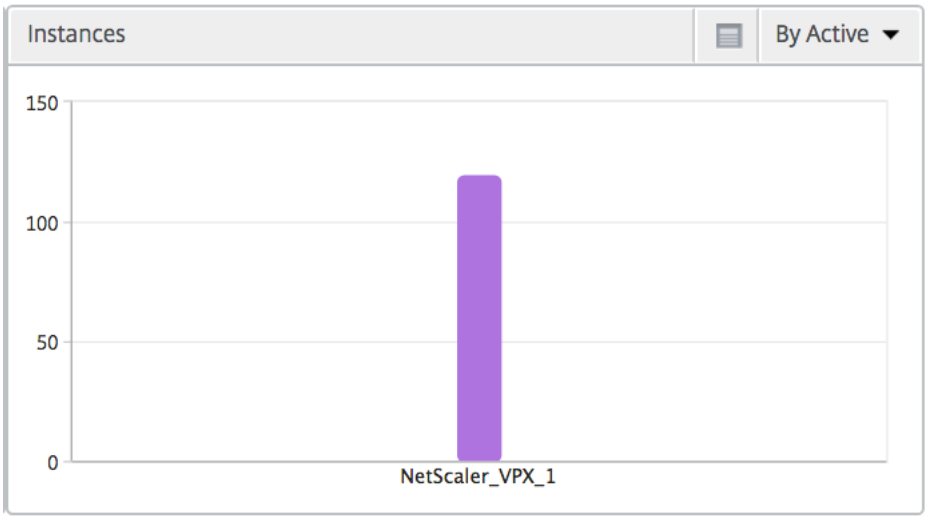
Mesures	Description
Nom	Nom du bureau virtuel Citrix.
Nombre de lancements de bureaux	Nombre de fois que l'ordinateur de bureau a été lancé.
Bande passante	Nombre total d'octets par seconde pris pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre Citrix Gateway et les serveurs VDI, CVAD ou StoreFront.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps ou Desktops respectivement.



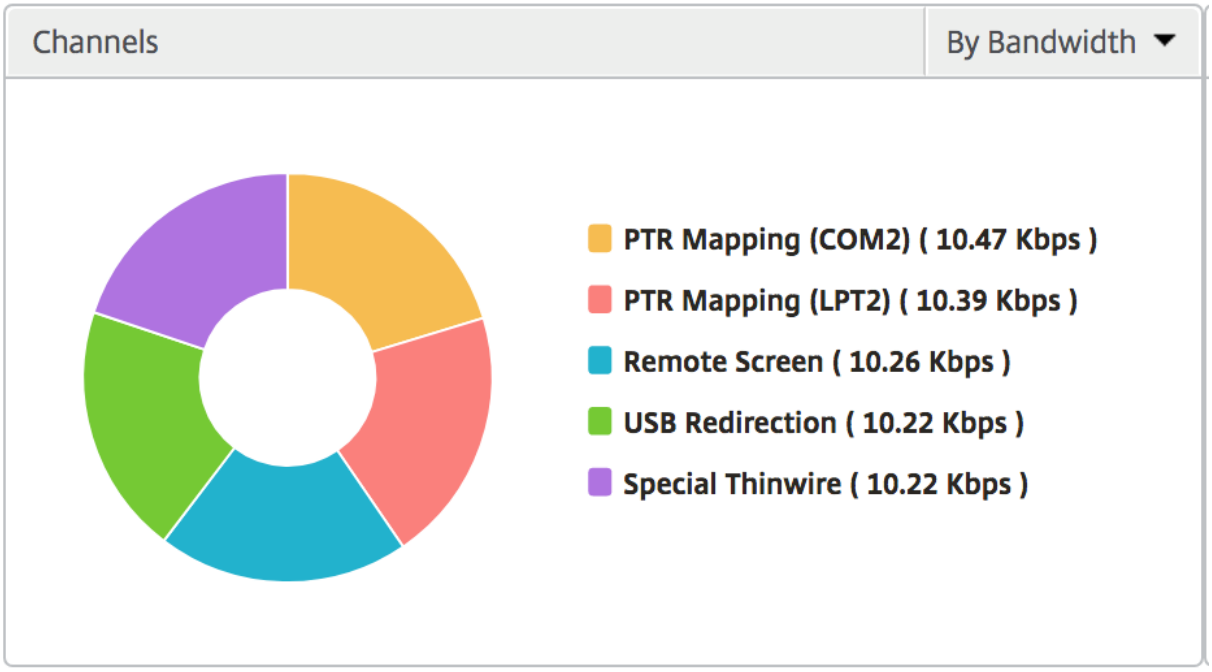
Applications Graphique à barres représentant les applications triées par Active, nombre total de lancements de session, nombre total de lancements d'applications et durée de lancement.



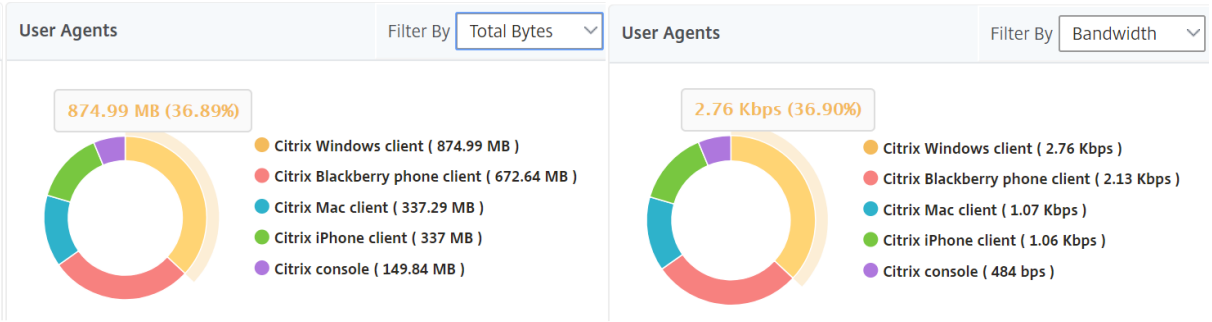
Instances Graphique à barres représentant les instances Citrix ADC triées par applications actives et totales



Canaux Les canaux représentent la bande passante globale ou le nombre total d'octets consommés par chaque canal virtuel ICA sous la forme d'un graphique en anneau. Vous pouvez également trier les mesures par bande passante ou Nombre total d'octets.



Agents utilisateurs Les agents utilisateurs représentent la bande passante globale/nombre total d'octets consommés par chaque point final sous la forme d'un graphique en donut. Vous pouvez également trier les mesures par bande passante ou Nombre total d'octets.



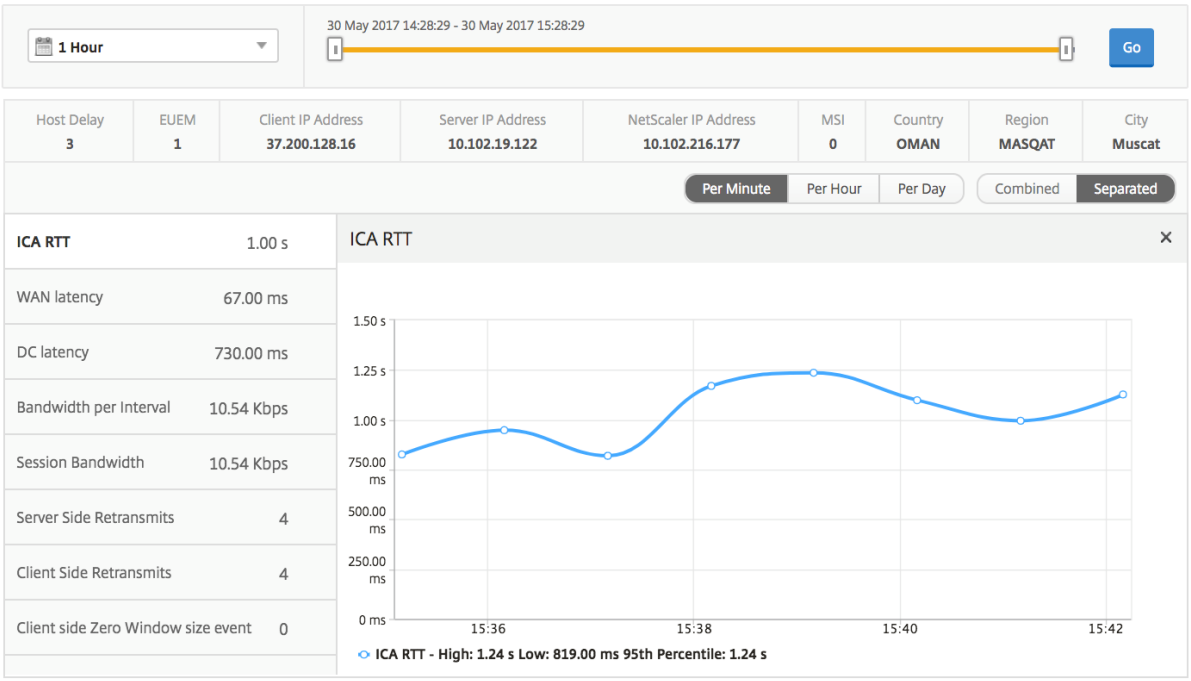
Par vue de session utilisateur La vue par session utilisateur fournit des rapports pour la session d'un utilisateur sélectionné particulier.

Pour afficher les mesures de la session d'un utilisateur sélectionné :

1. Accédez à **Analytics** > **HDX Insight** > **Utilisateurs**.
2. Select un utilisateur particulier dans la section **Rapport récapitulatif de l'utilisateur**.
3. Sélectionnez une session dans la colonne **Sessions en cours** ou **Sessions terminées** .

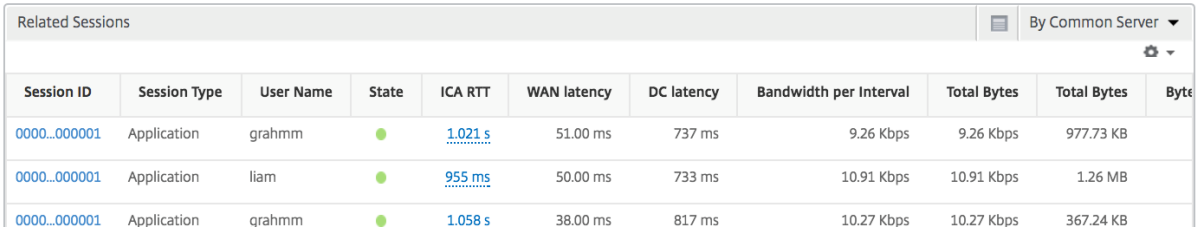
Graphique chronologique

Mesures	Description
Reconnexions de session	Ce nombre indique le nombre de sessions Citrix Virtual Apps and Desktops actives.
Nb d'ACR	Ce nombre indique le nombre de sessions actives de Citrix Virtual App.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lorsqu'il interagit avec une application ou un bureau hébergé respectivement sur Citrix Virtual Apps ou Desktops.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre Citrix Gateway et les serveurs VDI, CVAD ou StoreFront.
Bande passante de session	La bande passante consommée par la session quel que soit l'intervalle de temps.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et serveur back-end.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit sur la connexion entre Citrix ADC et le serveur back-end.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.



Application active La section **Applications actives** affiche les applications actives de l'utilisateur sélectionné. Ces applications peuvent également être triées en fonction du nombre de sessions actives et des durées de lancement.

Sessions connexes La section Sessions associées affiche les sessions associées des sessions de l'utilisateur sélectionné. La relation peut être sélectionnée comme serveurs communs ou Citrix ADC commun.



Rapports et mesures d'affichage des applications

Les rapports et les mesures de cette vue sont axés sur Citrix Virtual Apps.

Pour accéder à la vue Application :

1. Accédez à **Analytics** > **HDX Insight** > **Applications**.

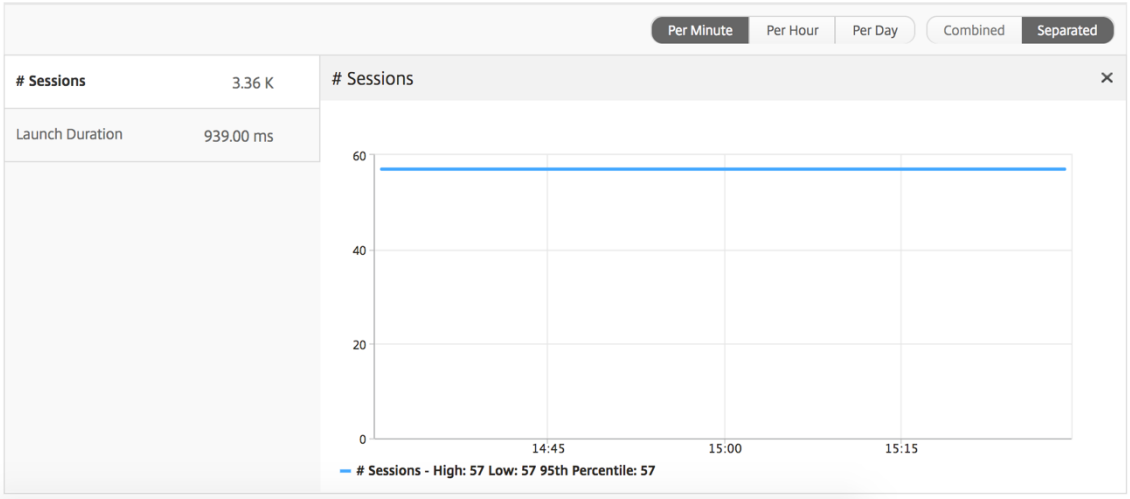
Vue récapitulative

La vue récapitulative affiche les rapports de toutes les applications qui sont connectées au cours de la chronologie sélectionnée.

Toutes les métriques/rapports, sauf mention explicite, auront les valeurs qui leur correspondent pour la période de sélection.

Graphique linéaire

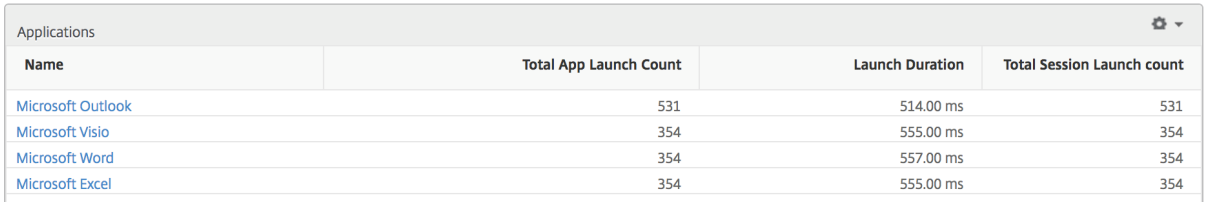
Métriques	Description
Nombre de sessions	Nombre total de séances pendant un intervalle de temps donné.
Durée du lancement	Temps moyen requis pour lancer une application.



Rapport récapitulatif des applications

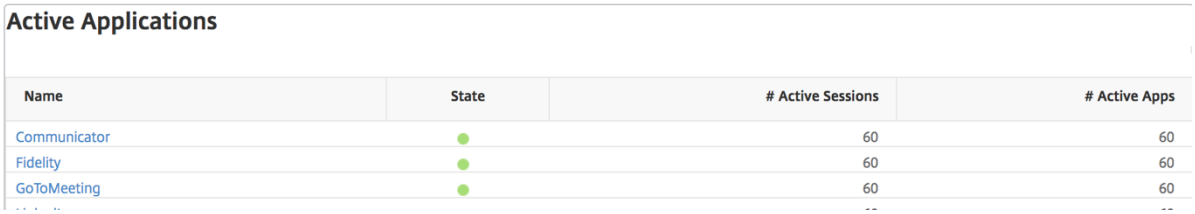
Métriques	Description
Nom	Nom de l'application virtuelle Citrix.
Nb total de sessions lancées	Nombre total de sessions Citrix Virtual App actives au cours de l'intervalle de temps donné.

Métriques	Description
Nb total d'applications lancées	Nombre total d'applications Citrix Virtual App lancées au cours de l'intervalle de temps donné.
Durée de lancement	Temps moyen requis pour lancer Citrix Virtual Apps.



Rapport d'application active

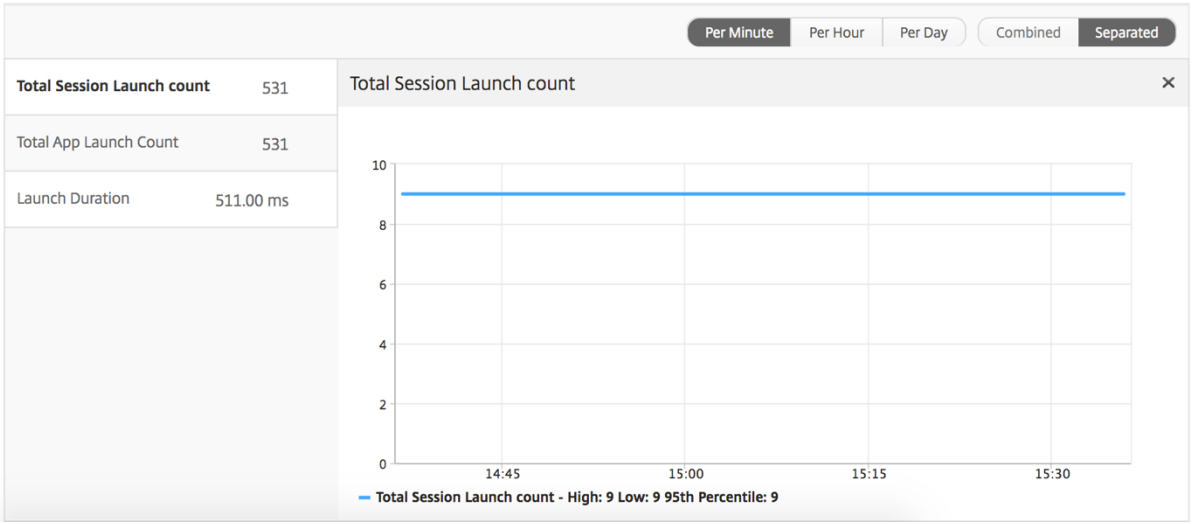
Métriques	Description
Nom	Nom de l'application virtuelle Citrix.
État	Affiche l'état de l'application : Vert-Actif, Rouge-Inactif
Nombre de sessions actives	Nombre de sessions utilisateur actives utilisant cette application pendant un intervalle de temps donné.
Nombre d'applications actives	Nombre de sessions actives pour cette application.



Rapport sur les seuils Le rapport sur les seuils représente le nombre de seuils franchis lorsque l'*entité* est sélectionnée comme application au cours de la période sélectionnée. Pour plus d'informations, consultez comment créer des seuils.

Graphique linéaire

Métriques	Description
Nombre de sessions actives	Ce nombre indique le nombre de sessions Citrix Virtual Apps and Desktops actives.
Durée du lancement	Temps moyen requis pour lancer une application.



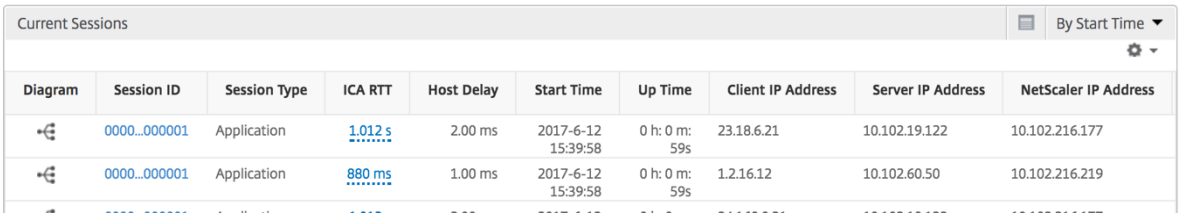
Rapport des sessions en cours

Métriques	Description
ID de session	Une identité unique pour une session ICA.
Type de session	Application/Bureau.
État	Vert/rouge pour les sessions actives/inactives.
Délai d'hôte	Délai moyen du trafic ICA transitant par les Citrix ADC causé par le réseau du serveur.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Bande passante de session	La bande passante consommée par la session quel que soit l'intervalle de temps.
Octets par intervalle	Nombre d'octets consommés par la session pendant cet intervalle de temps particulier.
Start Time	Heure de début de la session.
Temps d'activité	Durée de la session.

Métriques	Description
Adresse IP cliente	IP de l'utilisateur final.
Adresse IP du serveur	Adresse IP du serveur Backend/Citrix Virtual App.
Adresse IP NetScaler	IP de gestion NetScaler (NSIP).
Type de client	Type de Receiver - Client Windows Citrix et ainsi de suite
Version du client	Version du Receiver.
MSI	Boolean (Oui/Non). Indique si la session est multiflux ICA.
Reconnexions de session	Nombre de fois où la session s'est reconnectée.
Nb d'ACR	Nombre total de fois où un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, le mode utilisateur/transparent de Citrix Gateway.
Pays	Pays à partir duquel la session a été créée.
Région	Région à partir de laquelle la session a été créée.
City	Ville à partir de laquelle la session a été créée.
État de l'USB	Actif/Inactif -Vert/Rouge.
Nombre d'instances USB acceptées	Le nombre d'instances USB acceptées.
Nombre d'instances USB rejetées	Le nombre d'instances USB rejetées.
Nombre d'instances USB arrêtées	Le nombre d'instances USB arrêtées.
Nom d'hôte du client	Le nom d'hôte du client.
Nombre de basculements HA	Nombre de fois où le basculement HA s'est produit.
Motif de la résiliation	Affiche la raison de l'arrêt d'une session. Par exemple, délai d'expiration de session ICA, session terminée par l'utilisateur.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lorsqu'il interagit avec une application ou un bureau hébergé respectivement sur Citrix Virtual Apps ou Desktops.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.

Métriques	Description
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre Citrix Gateway et les serveurs VDI, CVAD ou StoreFront.
Nb total d'octets	Nombre total d'octets consommés par l'utilisateur pendant la période sélectionnée.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et serveur back-end.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit sur la connexion entre Citrix ADC et le serveur back-end.
Nom d'utilisateur	Nom d'utilisateur de l'utilisateur accédant à cette application virtuelle Citrix particulière.
ID de session	Identifiant unique pour la session Citrix Virtual App.
Type de session	Sera « Application ».
État	État de la session : vert pour actif, rouge pour inactif.
Latence maximale de violation	La valeur la plus élevée de la latence L7 lorsqu'un dépassement d'un seuil défini pour un intervalle de temps défini se produit.
Latence moyenne des violations	Valeur moyenne de la latence L7 lorsque le système est dans un état « Latence L7 violée ».
Nombre de franchissements de seuil L7	Nombre de fois qu'une violation du seuil L7 s'est produite.

Métriques	Description
Latence côté client L7	La latence moyenne L7 observée entre le client ICA et l'instance de Citrix ADC. Cette mesure est utile dans le cas de périphériques non Citrix présents dans le chemin de remise.
Latence côté serveur L7	Latence moyenne L7 observée entre l'appareil Citrix ADC et l'application virtuelle Citrix. Cette mesure est utile dans le cas de périphériques non Citrix présents dans le chemin de remise.



Par vue de session d'application

L'affichage par session d'application affiche les rapports pour une session d'application sélectionnée particulière.

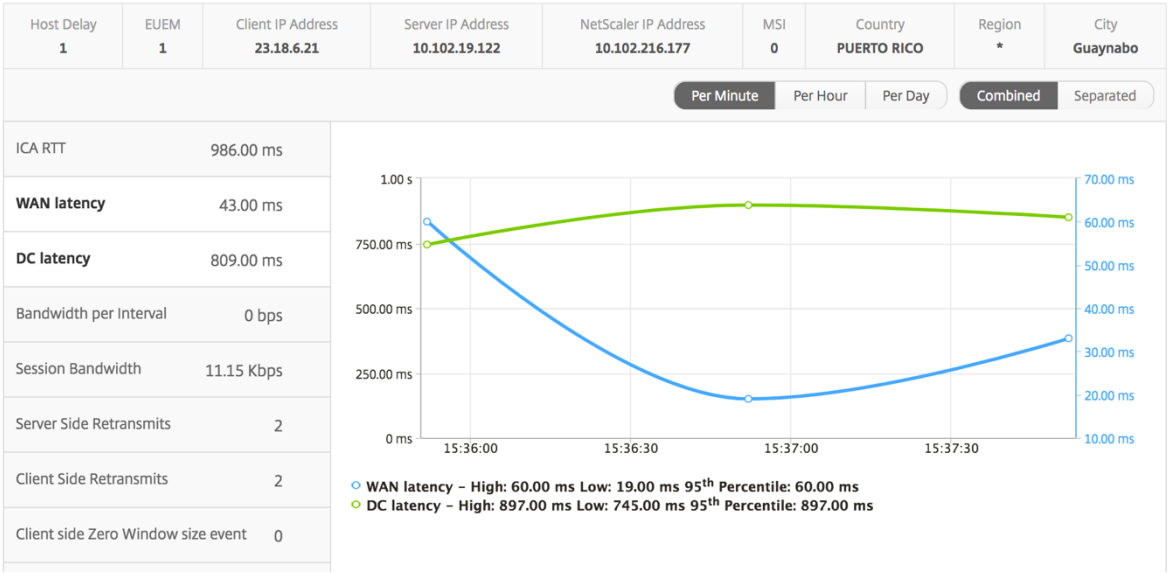
Pour afficher les rapports de session :

1. Connectez-vous à votre Citrix ADM à l'aide d'un navigateur Web pris en charge.
2. Accédez à **Analytics** > **HDX Insight** > **Applications**.
3. Sélectionnez un utilisateur particulier dans le rapport récapitulatif des applications.
4. Sélectionné une session à partir du rapport des sessions en cours.

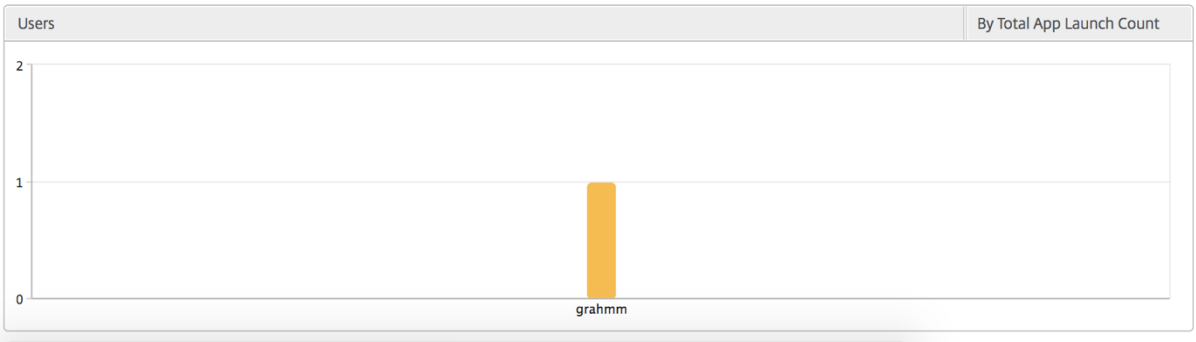
Graphique linéaire

Métriques	Description
Reconnexions de session	Nombre de fois où la session s'est reconnectée.
Nb d'ACR	Nombre total de fois où un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.

Métriques	Description
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Événement de taille de fenêtre nulle côté serveur	Latence causée par le côté serveur du réseau. C'est-à-dire, de Citrix ADC aux serveurs back-end.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et serveur back-end.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
Bande passante de session	La bande passante consommée par la session quel que soit l'intervalle de temps.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit sur la connexion entre Citrix ADC et le serveur back-end.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.



Graphique à barres utilisateur Le graphique à barres de l'utilisateur représente les utilisateurs connectés à cette application particulière.



Rapports et mesures d'affichage du Bureau

Les rapports et les mesures de cette vue sont axés sur les Citrix Virtual Desktops.

Pour accéder à la vue Bureau :

1. Connectez-vous à votre Citrix ADM à l'aide d'un navigateur Web pris en charge.
2. Accédez à **Analytics** > **HDX Insight** > **Bureau** .

Vue récapitulative

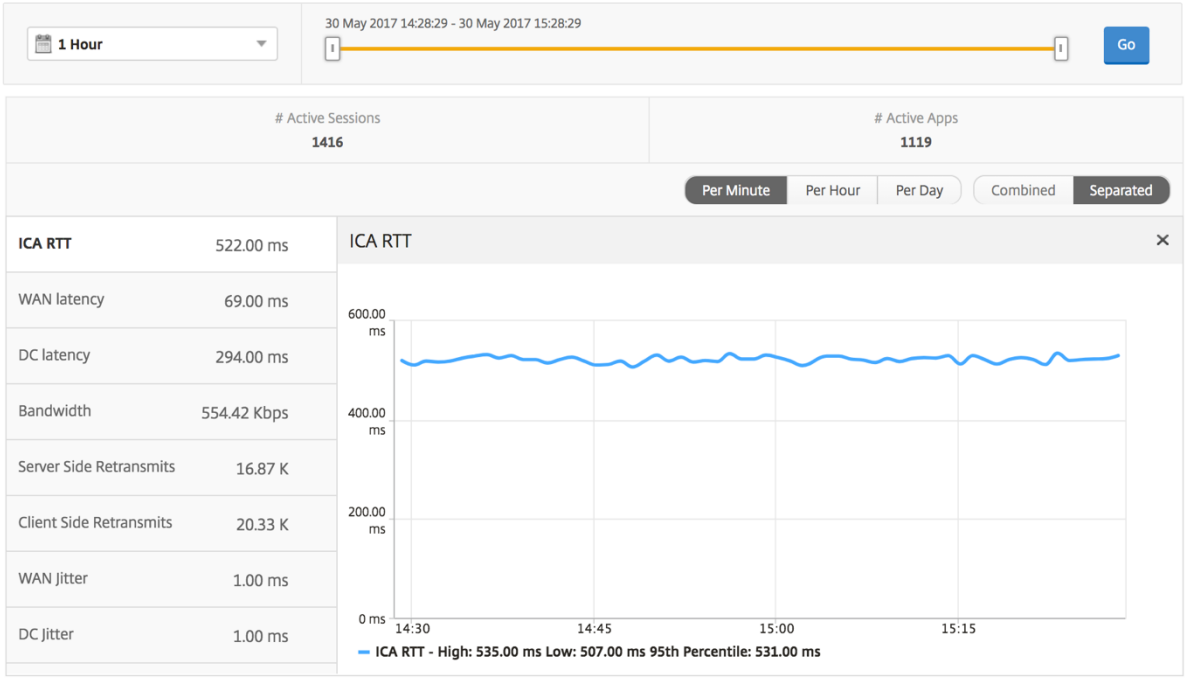
La vue récapitulative affiche les rapports de tous les Citrix Virtual Desktops qui sont connectés au cours de la chronologie sélectionnée.

Toutes les métriques/rapports, sauf mention explicite, auront les valeurs qui leur correspondent pour la période de sélection.

Graphique linéaire

Métriques	Description
Nombre de sessions actives	Ce nombre indique le nombre de sessions Citrix Virtual Apps and Desktops actives.
Nbre d'applications actives	Ce nombre indique le nombre de sessions actives de Citrix Virtual App.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre Citrix Gateway et les serveurs VDI, CVAD ou StoreFront.
Bande passante	Nombre total d'octets par seconde pris pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et serveur back-end.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit sur la connexion entre Citrix ADC et le serveur back-end.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.

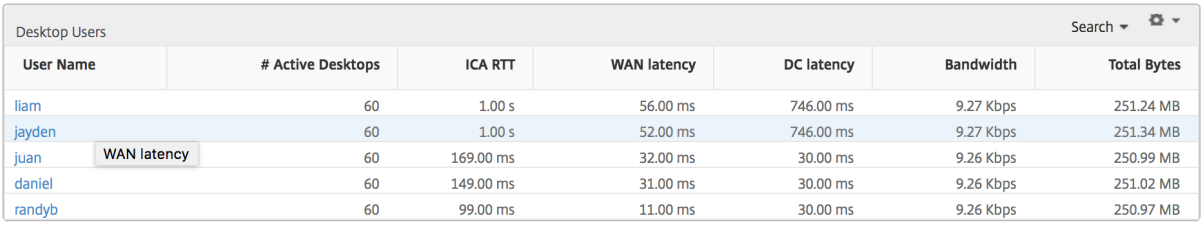
Métriques	Description
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.



Rapport récapitulatif du bureau

Métriques	Description
Active Sessions	Nombre total de sessions Citrix Virtual Desktop actives au cours d'un intervalle de temps donné.
Ordinateurs de bureau actifs	Nombre total de Citrix Virtual Desktops actifs au cours d'un intervalle de temps donné.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre Citrix Gateway et les serveurs VDI, CVAD ou StoreFront.

Métriques	Description
Bande passante	Nombre total d'octets par seconde pris pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Nb total d'octets	Nombre total d'octets consommés par l'utilisateur pendant la période sélectionnée.



Rapport sur les seuils Le rapport de seuil représente le nombre de seuils dépassés lorsque l'*entité* est sélectionnée en tant que Bureau au cours de la période sélectionnée. Pour plus d'informations, consultez comment créer des seuils.

Par vue Bureau

La vue par poste de travail fournit des rapports détaillés sur l'expérience utilisateur pour un Citrix Virtual Desktop sélectionné.

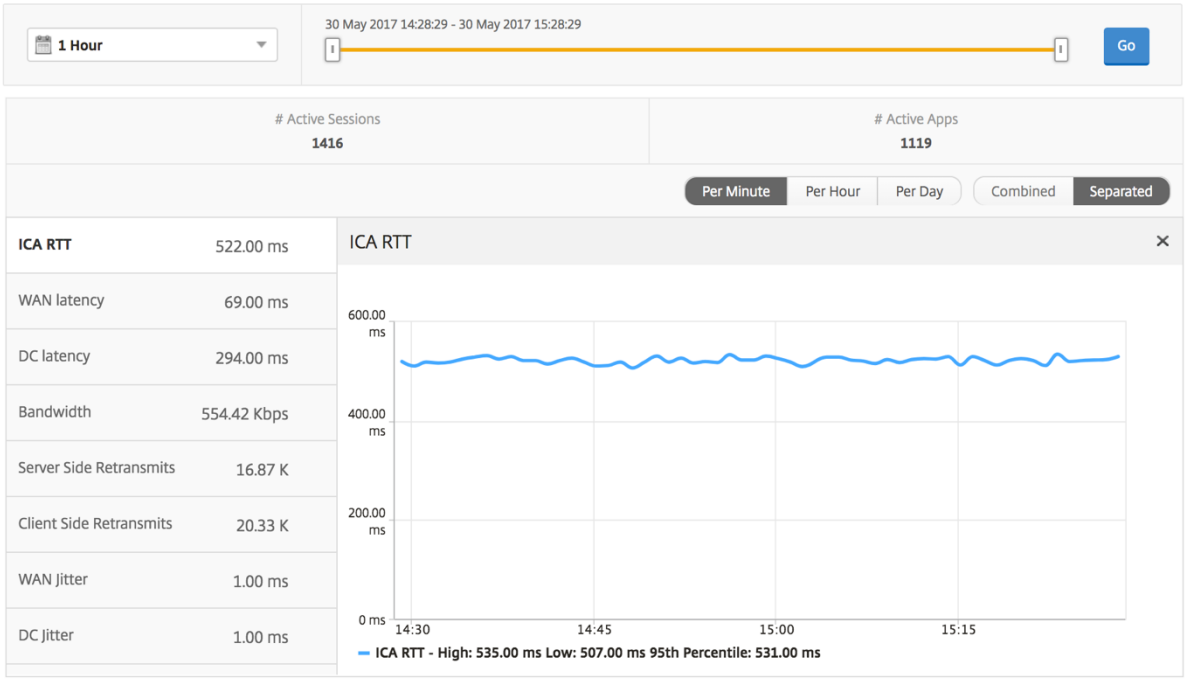
Pour accéder à la vue Bureau spécifique :

1. Connectez-vous à votre Citrix ADM à l'aide d'un navigateur Web pris en charge.
2. Accédez à **Analytics > HDX Insight > Bureau**.
3. Sélectionnez un **poste de travail** particulier dans le **rapport récapitulatif des ordinateurs de bureau**.

Graphique linéaire

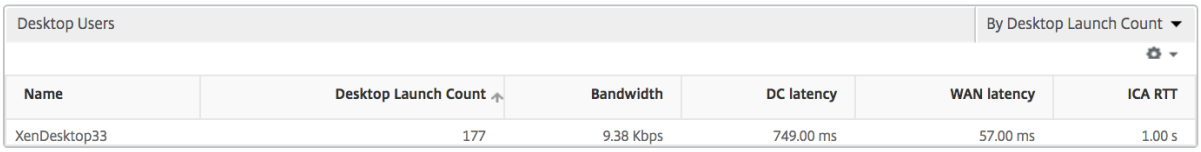
Métriques	Description
Nombre de sessions actives	Ce nombre indique le nombre de sessions Citrix Virtual Apps and Desktops actives.
Nbre d'applications actives	Ce nombre indique le nombre de sessions actives de Citrix Virtual App.

Métriques	Description
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre Citrix Gateway et les serveurs VDI, CVAD ou StoreFront.
Bande passante	Nombre total d'octets par seconde pris pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et serveur back-end.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit sur la connexion entre Citrix ADC et le serveur back-end.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.



Rapport Utilisateurs de bureau Ce tableau donne un aperçu des sessions Citrix Virtual Desktop pour un utilisateur particulier. Ces mesures peuvent être triées par nombre de lancements de postes de travail et bande passante.

Mesures	Description
Nom	Nom du bureau virtuel Citrix.
Nombre de lancements de bureaux	Nombre de fois que l'ordinateur de bureau a été lancé.
Bande passante	Nombre total d'octets par seconde pris pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre Citrix Gateway et les serveurs VDI, CVAD ou StoreFront.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.



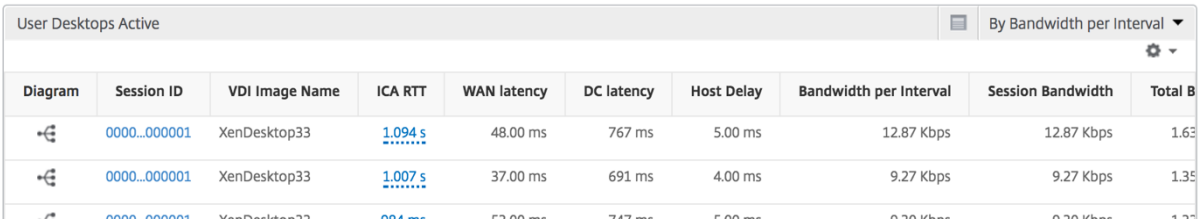
Rapport Actif/Inactif des postes de travail utilisateur Les mesures suivantes peuvent être triées en fonction de la bande passante par intervalle, des reconnexions de session et du nombre d'ACR.

Mesures	Description
ID de session	Une identité unique pour une session ICA.
Type de session	Application/Bureau.
État	Vert/rouge pour les sessions actives/inactives.
Délai d'hôte	Délai moyen du trafic ICA transitant par les Citrix ADC causé par le réseau du serveur.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Bande passante de session	La bande passante consommée par la session quel que soit l'intervalle de temps.
Octets par intervalle	Nombre d'octets consommés par la session pendant cet intervalle de temps particulier.
Start Time	Heure de début de la session.
Temps d'activité	Durée de la session.
Adresse IP cliente	IP de l'utilisateur final.
Adresse IP du serveur	Adresse IP du serveur Backend/Citrix Virtual App.
Adresse IP NetScaler	IP de gestion NetScaler (NSIP).
Type de client	Type de Receiver - Client Windows Citrix et ainsi de suite
Version du client	Version du Receiver.
MSI	Boolean (Oui/Non). Indique si la session est multiflux ICA.
Reconnexions de session	Nombre de fois où la session s'est reconnectée.
Nb d'ACR	Nombre total de fois où un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.

Mesures	Description
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, le mode utilisateur/transparent de Citrix Gateway.
Pays	Pays à partir duquel la session a été créée.
Région	Région à partir de laquelle la session a été créée.
City	Ville à partir de laquelle la session a été créée.
État de l'USB	Actif/Inactif -Vert/Rouge.
Nombre d'instances USB acceptées	Le nombre d'instances USB acceptées.
Nombre d'instances USB rejetées	Le nombre d'instances USB rejetées.
Nombre d'instances USB arrêtées	Le nombre d'instances USB arrêtées.
Nom d'hôte du client	Le nom d'hôte du client.
Nombre de basculements HA	Nombre de fois où le basculement HA s'est produit.
Motif de la résiliation	Affiche la raison de l'arrêt d'une session. Par exemple, délai d'expiration de session ICA, session terminée par l'utilisateur.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre Citrix Gateway et les serveurs VDI, CVAD ou StoreFront.
Nb total d'octets	Nombre total d'octets consommés par l'utilisateur pendant la période sélectionnée.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et serveur back-end.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.

Mesures	Description
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit sur la connexion entre Citrix ADC et le serveur back-end.
Nom de l'image VDI	Nom du Citrix Virtual Desktops auquel l'utilisateur est connecté

Diagramme



Par vue de session Bureau

La vue par session de bureau fournit des rapports pour une session Citrix Virtual Desktops sélectionnée.

Pour accéder à la vue de session Bureau :

1. Connectez-vous à votre Citrix ADM à l'aide d'un navigateur Web pris en charge.
2. Accédez à **Analytics > HDX Insight > Bureau**.
3. Sélectionnez un poste de travail particulier dans le **rapport récapitulatif des postes**de travail.
4. Sélectionnez une session dans le rapport des sessions en cours.

Graphique chronologique La vue par session utilisateur fournit des rapports pour la session d'un utilisateur sélectionné particulier.

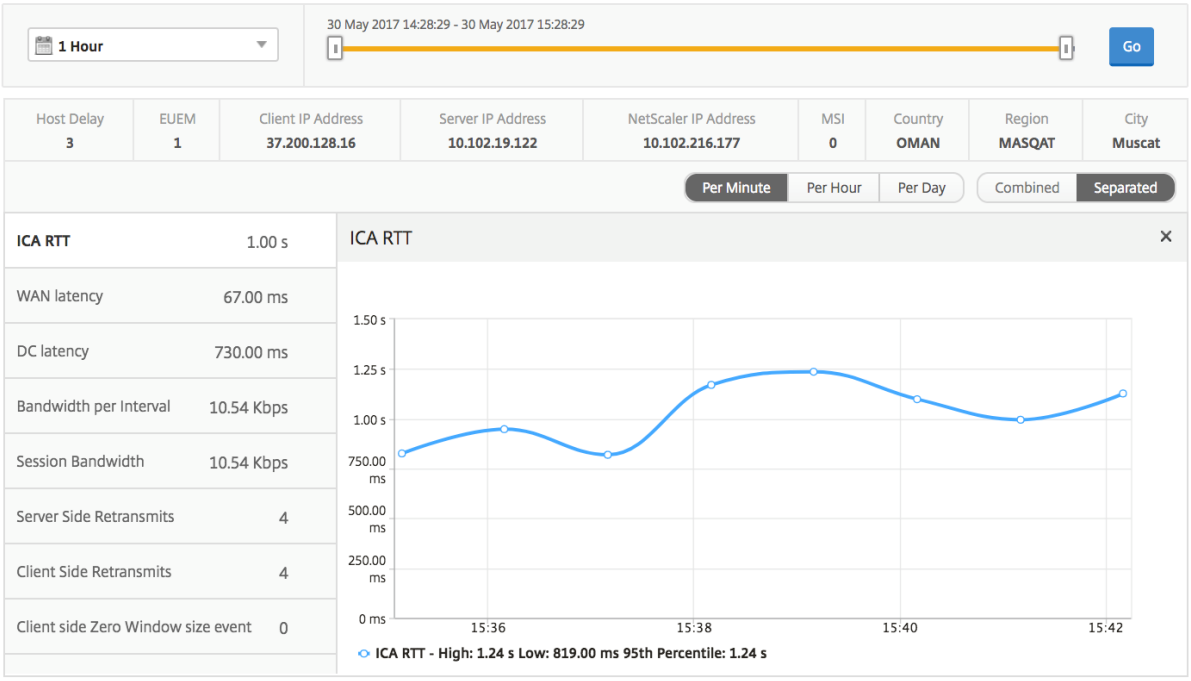
Pour afficher les mesures de la session d'un utilisateur sélectionné :

1. Connectez-vous à votre Citrix ADM à l'aide d'un navigateur Web pris en charge.

2. Accédez à **Analytics** > **HDX Insight** > **Utilisateurs**.
3. Select un utilisateur particulier dans la section **Rapport récapitulatif de l'utilisateur**.
4. Sélectionnez une session dans la colonne **Sessions en cours** ou **Sessions terminées** .

Mesures	Description
Reconnexions de session	Ce nombre indique le nombre de sessions Citrix Virtual Apps and Desktops actives.
Nb d'ACR	Ce nombre indique le nombre de sessions actives de Citrix Virtual App.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre Citrix Gateway et les serveurs VDI, CVAD ou StoreFront.
Bande passante de session	La bande passante consommée par la session quel que soit l'intervalle de temps.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et serveur back-end.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit sur la connexion entre Citrix ADC et le serveur back-end.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.

Mesures	Description
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.

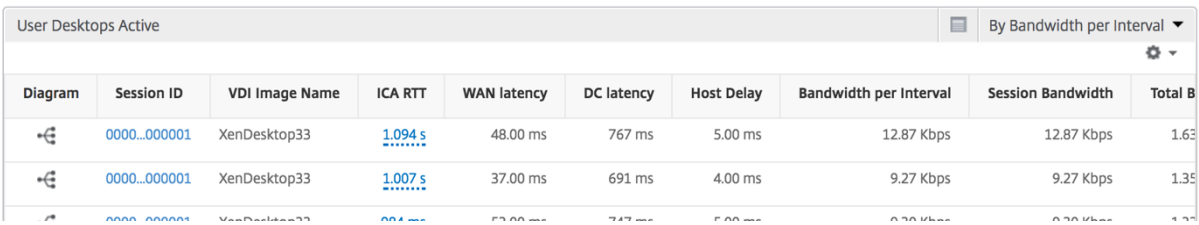


Rapport sur les sessions de bureau associées Les mesures suivantes peuvent être triées en fonction de la bande passante par intervalle, des reconnexions de session et du nombre d'ACR.

Mesures	Description
ID de session	Une identité unique pour une session ICA.
Type de session	Application/Bureau.
État	Vert/rouge pour les sessions actives/inactives.
Délai d'hôte	Délai moyen du trafic ICA transitant par les Citrix ADC causé par le réseau du serveur.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Bande passante de session	La bande passante consommée par la session quel que soit l'intervalle de temps.
Octets par intervalle	Nombre d'octets consommés par la session pendant cet intervalle de temps particulier.

Mesures	Description
Start Time	Heure de début de la session.
Temps d'activité	Durée de la session.
Adresse IP cliente	IP de l'utilisateur final.
Adresse IP du serveur	Adresse IP du serveur Backend/Citrix Virtual App.
Adresse IP NetScaler	IP de gestion NetScaler (NSIP).
Type de client	Type de Receiver - Client Windows Citrix et ainsi de suite
Version du client	Version du Receiver.
MSI	Boolean (Oui/Non). Indique si la session est multiflux ICA.
Reconnexions de session	Nombre de fois où la session s'est reconnectée.
Nb d'ACR	Nombre total de fois où un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, le mode utilisateur/transparent de Citrix Gateway.
Pays	Pays à partir duquel la session a été créée.
Région	Région à partir de laquelle la session a été créée.
City	Ville à partir de laquelle la session a été créée.
État de l'USB	Actif/Inactif -Vert/Rouge.
Nombre d'instances USB acceptées	Le nombre d'instances USB acceptées.
Nombre d'instances USB rejetées	Le nombre d'instances USB rejetées.
Nombre d'instances USB arrêtées	Le nombre d'instances USB arrêtées.
Nom d'hôte du client	Le nom d'hôte du client.
Nombre de basculements HA	Nombre de fois où le basculement HA s'est produit.
Motif de la résiliation	Affiche la raison de l'arrêt d'une session. Par exemple, délai d'expiration de session ICA, session terminée par l'utilisateur.

Mesures	Description
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre Citrix Gateway et les serveurs VDI, CVAD ou StoreFront.
Nb total d'octets	Nombre total d'octets consommés par l'utilisateur pendant la période sélectionnée.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et serveur back-end.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit sur la connexion entre Citrix ADC et le serveur back-end.



Rapports et mesures de vue d'instance

Les rapports et les métriques de la vue d'instance sont axés sur les instances Citrix ADC.

Pour accéder à la vue Instance :

1. Connectez-vous à votre Citrix ADM à l'aide d'un navigateur Web pris en charge.
2. Accédez à **Analytics > HDX Insight > Instances**.

Les rapports et mesures de vue d'instance comprennent les sections suivantes :

- Vue récapitulative de l'instance
- Vue par instance

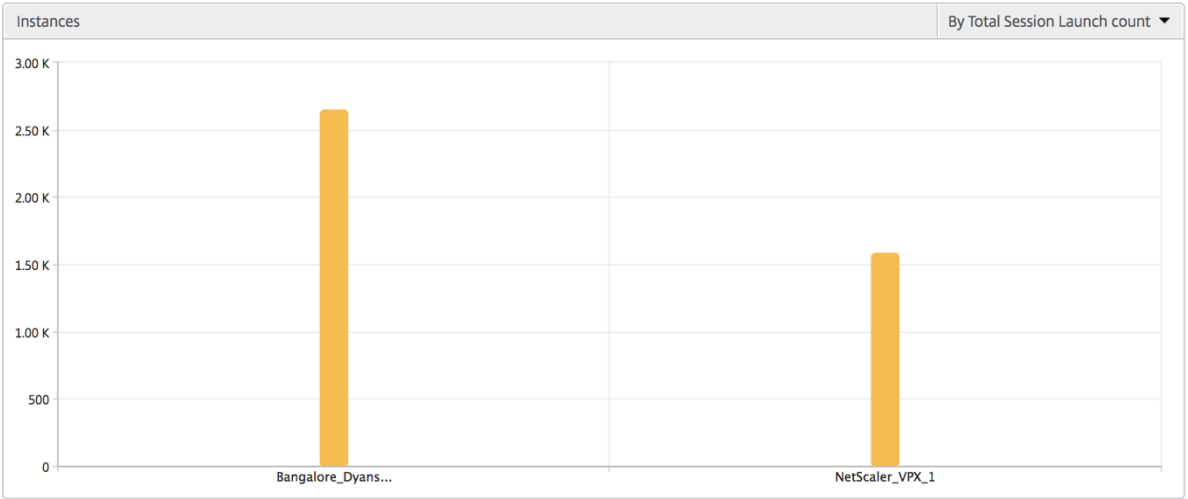
Vue récapitulative de l'instance

Cette vue est appelée vue récapitulative car elle affiche les rapports pour toutes les instances Citrix ADC qui sont ajoutées à Citrix ADM.

Toutes les métriques/rapports ci-dessous, sauf mention explicite, auront les valeurs qui leur correspondent pour la période sélectionnée.

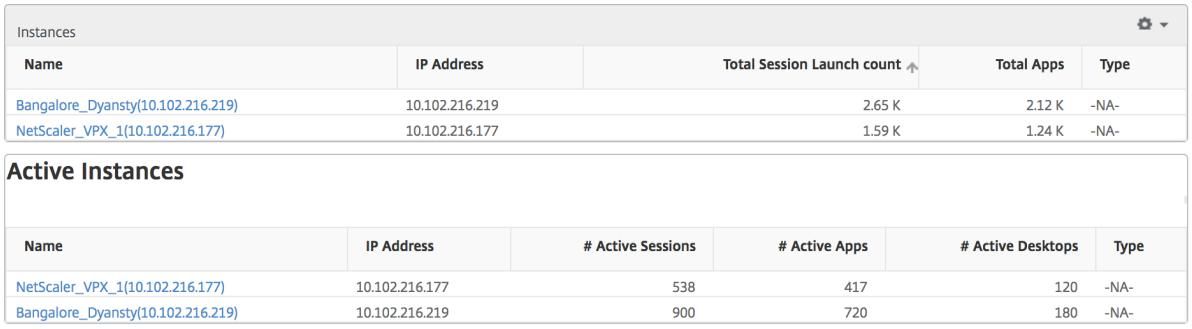
Graphique à barres d'instance

Ce graphique affiche l'instance par rapport au nombre total de lancement de session	Total des applications qui peuvent être sélectionnées dans la liste en haut à droite du canevas du graphique.



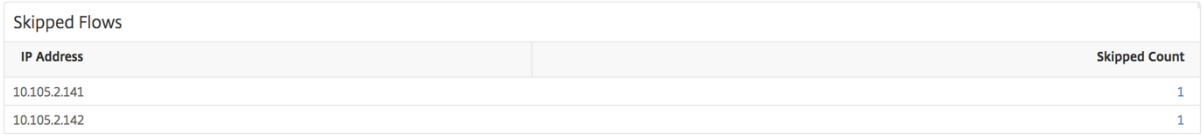
Rapport récapitulatif des instances et des instances actives

Métriques	Description
Nom	Nom d'hôte de l'instance Citrix ADC.
Adresse IP	Adresse IP NetScaler.
Nb total de sessions lancées	Nombre total de sessions utilisateur uniques créées au cours d'un intervalle de temps donné.
Nb total d'applis	Nombre total d'applications uniques lancées pendant un intervalle de temps donné.
Type	S/O



Rapport sur les seuils L'état des seuils représente le nombre de seuils dépassés lorsque l'*entité* est sélectionnée en tant qu'instance dans la période sélectionnée. Pour plus d'informations, consultez comment créer des seuils.

Flux ignorés Un flux ignoré est un enregistrement qui a ignoré l'analyse de la connexion ICA. Cela peut se produire pour plusieurs raisons, telles que l'utilisation de versions non prises en charge de Citrix Virtual Apps and Desktop, la version non prise en charge du type de récepteur ou de récepteur, etc. Ce tableau montre l'adresse IP et le nombre de flux ignorés. Ces récepteurs peuvent ne pas faire partie des récepteurs de liste blanche. Par conséquent, ces sessions sont ignorées de la surveillance.

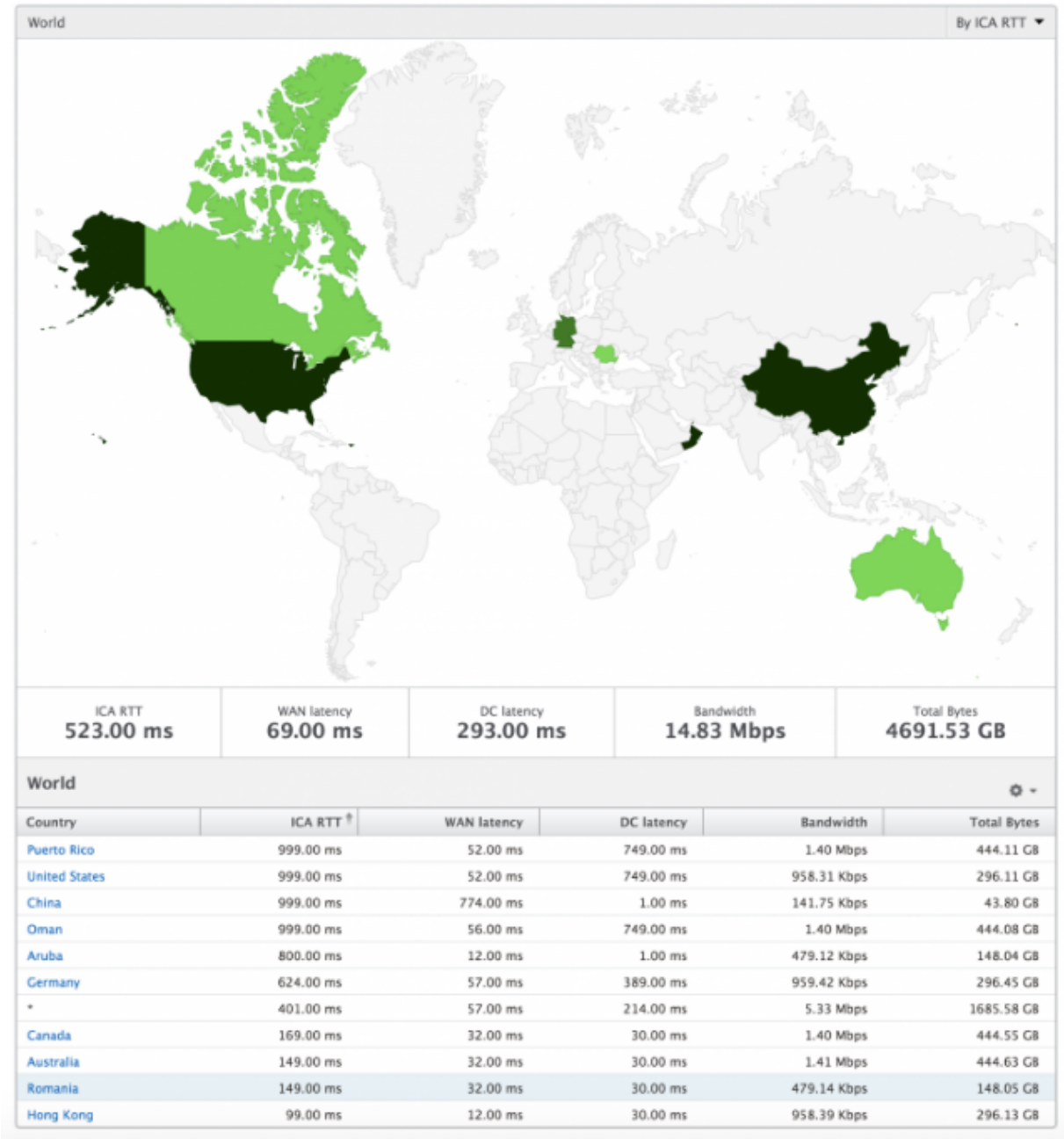


Vue du monde La vue Carte du monde dans HDX insights permet aux administrateurs de visualiser les détails des utilisateurs historiques et actifs d'un point de vue géographique. Les administrateurs peuvent avoir une vue du monde du système, une exploration vers un pays particulier et plus loin dans

les villes ainsi qu'en cliquant simplement sur la région. Les administrateurs peuvent approfondir l'exploration vers le bas pour afficher les informations par ville et par État. À partir de Citrix ADM version 12.0 et ultérieure, vous pouvez effectuer une exploration vers le bas vers les utilisateurs connectés à partir d'un emplacement géographique.

Les détails suivants peuvent être consultés sur la carte du monde dans un aperçu HDX, et la densité de chaque mesure est affichée sous la forme d'une carte thermique :

- RTT ICA
- Latence WAN
- Latence DC
- Bande passante
- Nb total d'octets



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

Vue par instance

La vue par instance fournit des rapports détaillés sur l'expérience utilisateur final pour une instance Citrix ADC sélectionnée particulière.

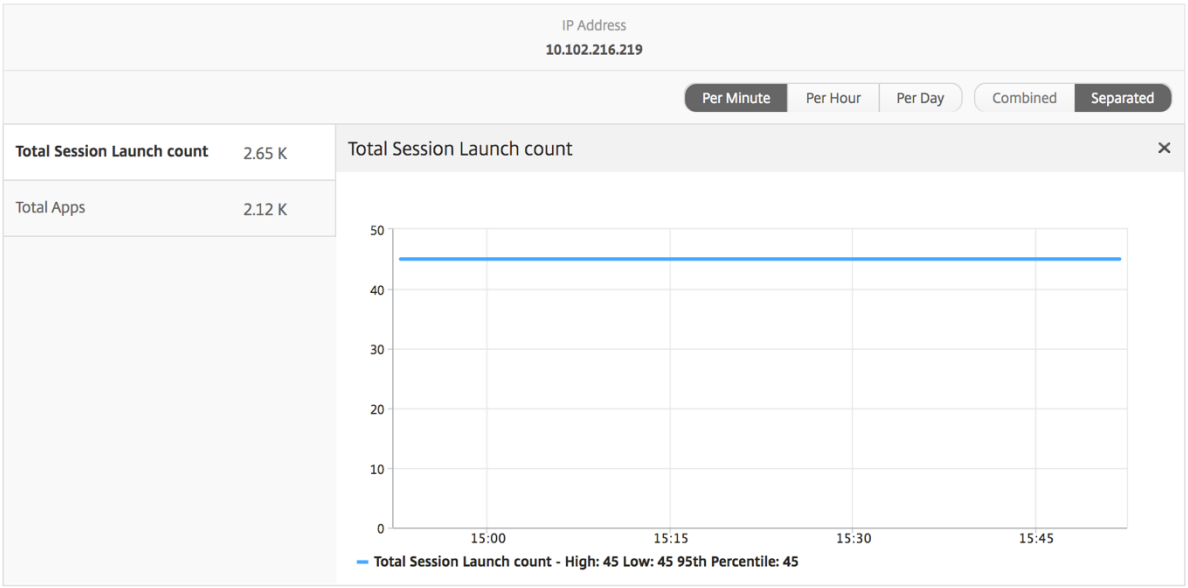
Pour accéder à la vue d'instance :

1. Connectez-vous à votre Citrix ADM à l'aide d'un navigateur Web pris en charge.
2. Accédez à **Analytics > HDX Insight > Instances**.

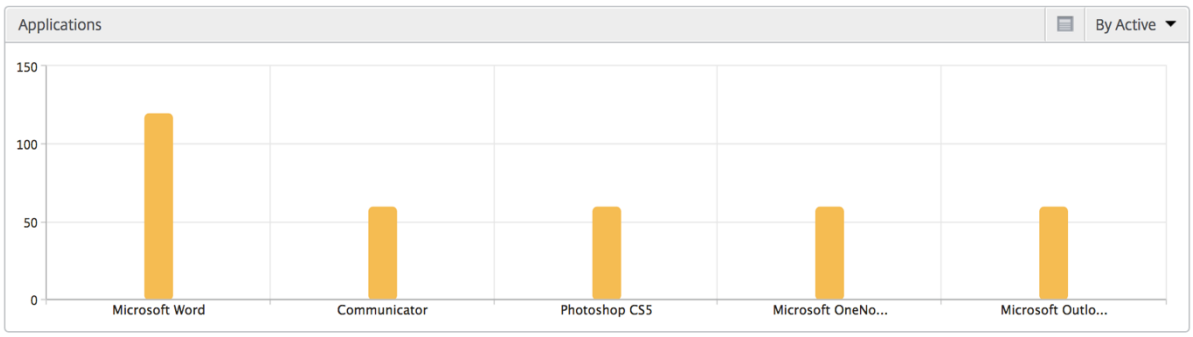
3. Sélectionnez une instance particulière dans le **rapport de synthèse des instances**.

Graphique linéaire

Métriques	Description
Adresse IP	Cela représente l'adresse IP NetScaler de l'instance sélectionnée.
Nombre total de lancements de session	Nombre total de sessions Citrix Virtual App actives au cours de l'intervalle de temps donné.
Nb total d'applis	Nombre total d'applications uniques lancées pendant un intervalle de temps donné.

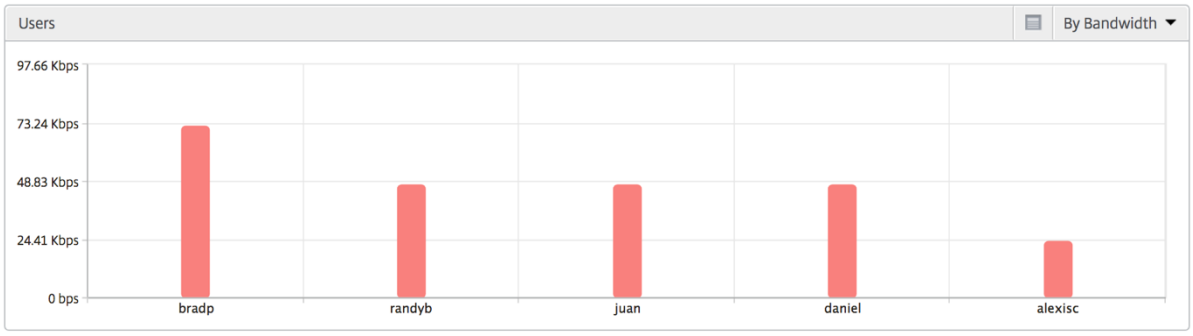


Graphique à barres des applications Affiche les 5 premières applications en fonction des critères suivants : applications actives, nombre total de lancements de session, nombre total de lancements d'applications ou durée de lancement.



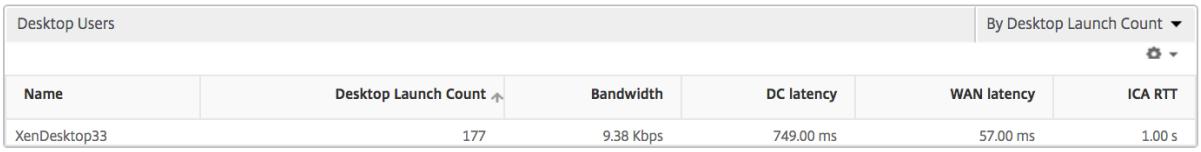
Graphique à barres des utilisateurs Le graphique à barres Utilisateurs affiche les 5 premiers utilisateurs selon les critères suivants

- Bande passante
- Latence WAN
- Latence DC
- RTT ICA



Rapport Utilisateurs de bureau Ce tableau donne un aperçu des sessions Citrix Virtual Desktop pour un utilisateur particulier. Ces mesures peuvent être triées par nombre de lancements de postes de travail et bande passante.

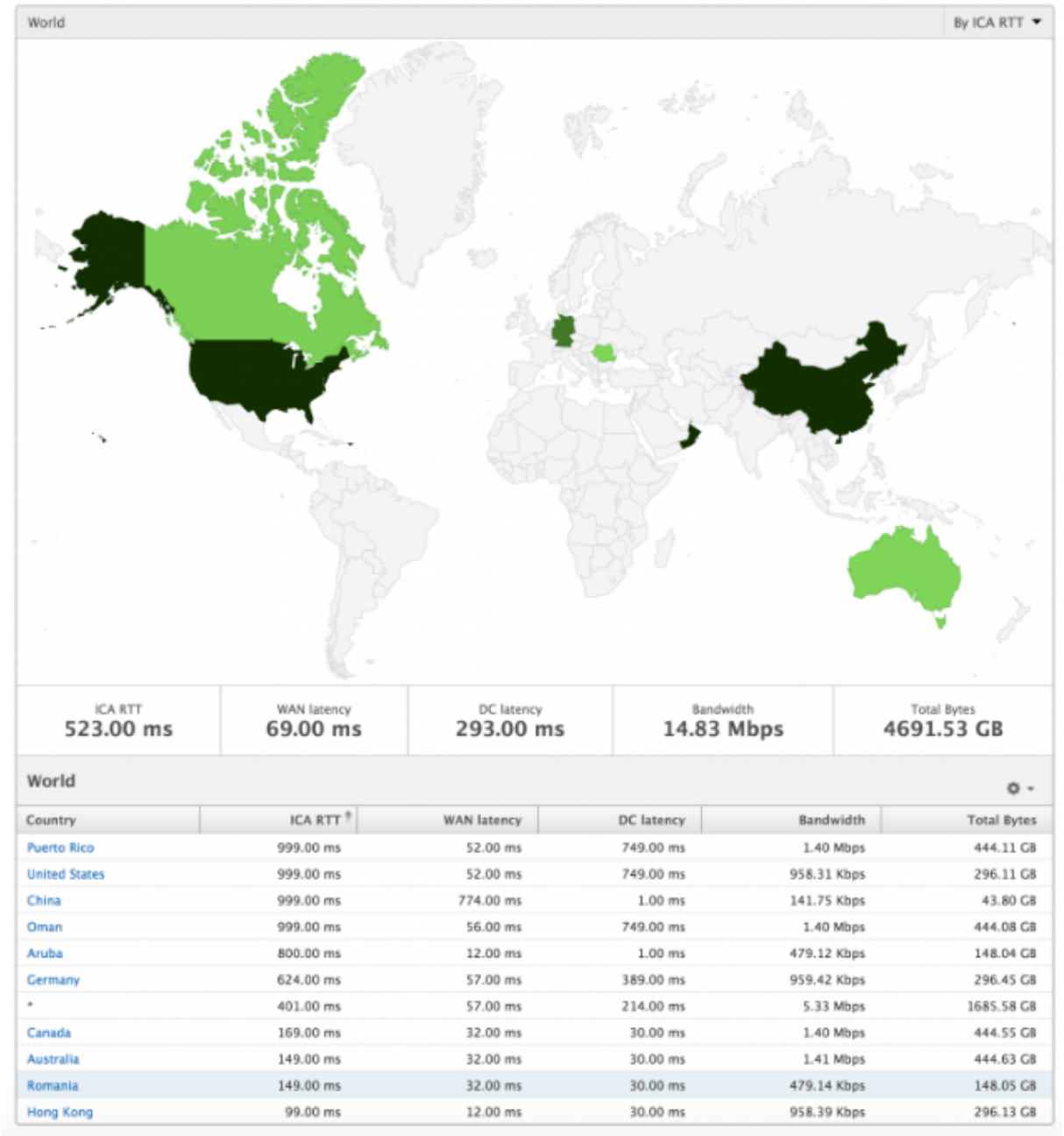
Mesures	Description
Nom	Nom du bureau virtuel Citrix.
Nombre de lancements de bureaux	Nombre de fois que l'ordinateur de bureau a été lancé.
Bande passante	Nombre total d'octets par seconde pris pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre Citrix Gateway et les serveurs VDI, CVAD ou StoreFront.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.



Vue du monde La vue Carte du monde dans HDX insights permet aux administrateurs de visualiser les détails des utilisateurs historiques et actifs d'un point de vue géographique. Les administrateurs peuvent avoir une vue du monde du système, une exploration vers un pays particulier et plus loin dans les villes ainsi qu'en cliquant sur la région. Les administrateurs peuvent approfondir leurs recherches pour afficher les informations par ville et par État. À partir de Citrix ADM version 12.0 et ultérieure, vous pouvez effectuer une exploration vers le bas vers les utilisateurs connectés à partir d'un emplacement Geo.

Les détails suivants peuvent être consultés sur la carte du monde dans un aperçu HDX, et la densité de chaque mesure est affichée sous la forme d'une carte thermique :

- RTT ICA
- Latence WAN
- Latence DC
- Bande passante
- Nb total d'octets



Rapports et mesures d'affichage des licences

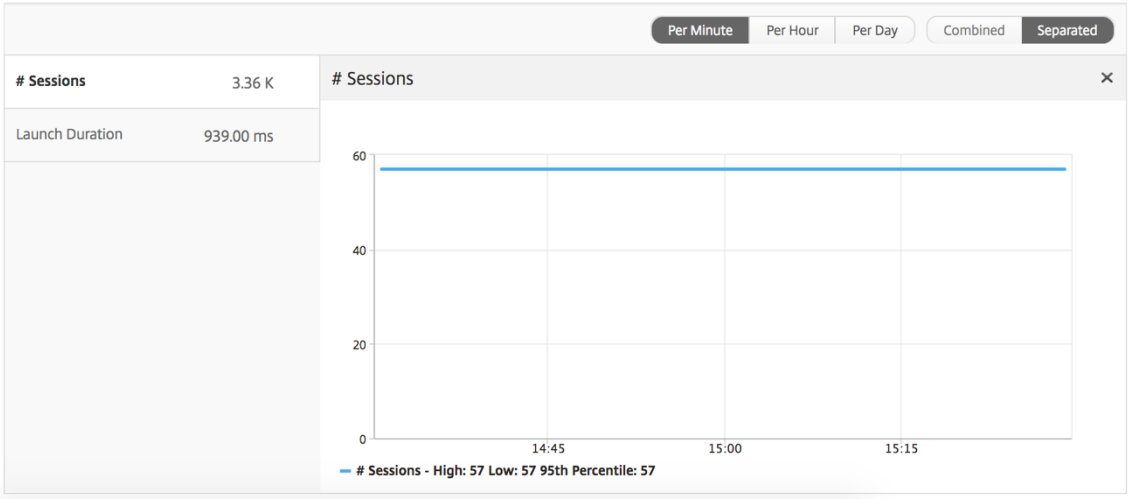
La vue de licence donne des détails sur les informations de licence Citrix Gateway.

Pour accéder à la vue Licence :

1. Connectez-vous à votre Citrix ADM à l'aide d'un navigateur Web pris en charge.
2. Accédez à **Analytics > HDX Insight > Licences**.

Graphique linéaire

Métriques	Description
Licences utilisées	Les licences CCU Citrix Gateway utilisées pendant la chronologie sélectionnée. Chaque nombre représente le nombre de sessions utilisateur. Cela est indépendant des sessions d'application et de bureau lancées par cet utilisateur.
Nombre total de licences	Nombre total de licences Citrix Gateway CCU disponibles pour le client.



Rapport sur les seuils Le rapport de seuil représente le nombre de seuils dépassés lorsque l'*entité* est sélectionnée en tant que Licence au cours de la période sélectionnée. Pour plus d'informations, consultez comment créer des seuils.

Rapports et mesures d'affichage des applications

February 1, 2024

Les rapports et les mesures de cette vue sont axés sur Citrix Virtual Apps.

Pour accéder à la vue Application :

1. Accédez à **Analytics** > **HDX Insight** > **Applications**.

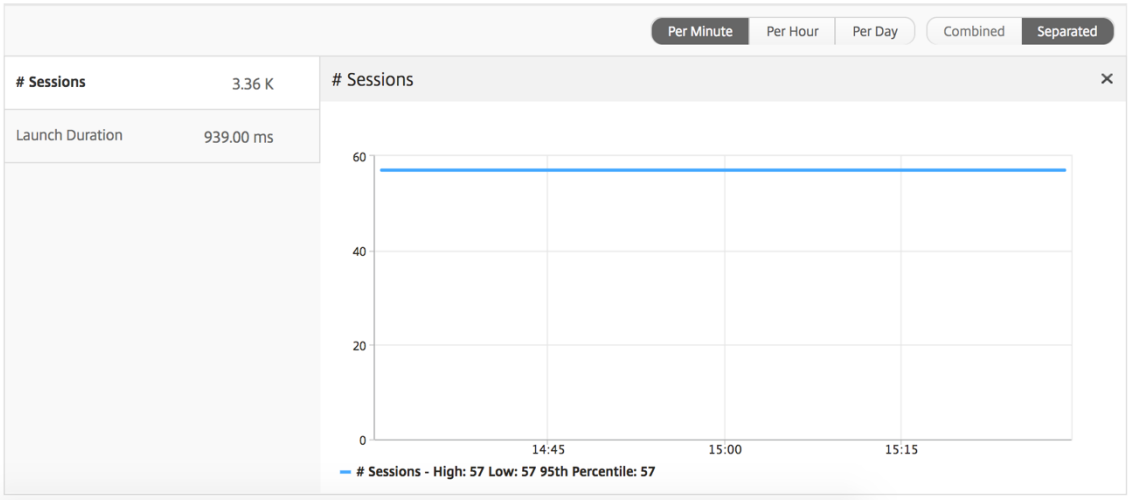
Vue récapitulative

La vue récapitulative affiche les rapports de toutes les applications qui sont connectées au cours de la chronologie sélectionnée.

Toutes les métriques/rapports ci-dessous, sauf mention explicite, auront les valeurs qui leur correspondent pour la période sélectionnée.

Graphique linéaire

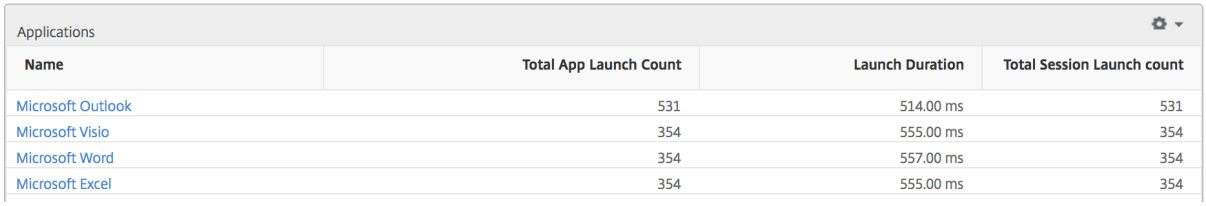
Métriques	Description
Nombre de sessions	Nombre total de séances pendant un intervalle de temps donné.
Durée du lancement	Temps moyen requis pour lancer une application.



Rapport récapitulatif des applications

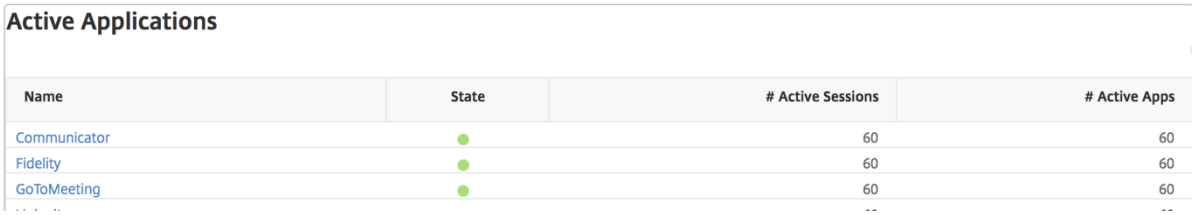
Métriques	Description
Nom	Nom de l'application virtuelle Citrix.
Nb total de sessions lancées	Nombre total de sessions Citrix Virtual App actives au cours de l'intervalle de temps donné.
Nb total d'applications lancées	Nombre total d'applications Citrix Virtual App lancées au cours de l'intervalle de temps donné.

Métriques	Description
Durée de lancement	Temps moyen requis pour lancer Citrix Virtual Apps.



Rapport d'application active

Métriques	Description
Nom	Nom de l'application virtuelle Citrix.
État	Affiche l'état de l'application : Vert-Actif, Rouge-Inactif
Nombre de sessions actives	Nombre de sessions utilisateur actives utilisant cette application pendant un intervalle de temps donné.
Nombre d'applications actives	Nombre de sessions actives pour cette application.

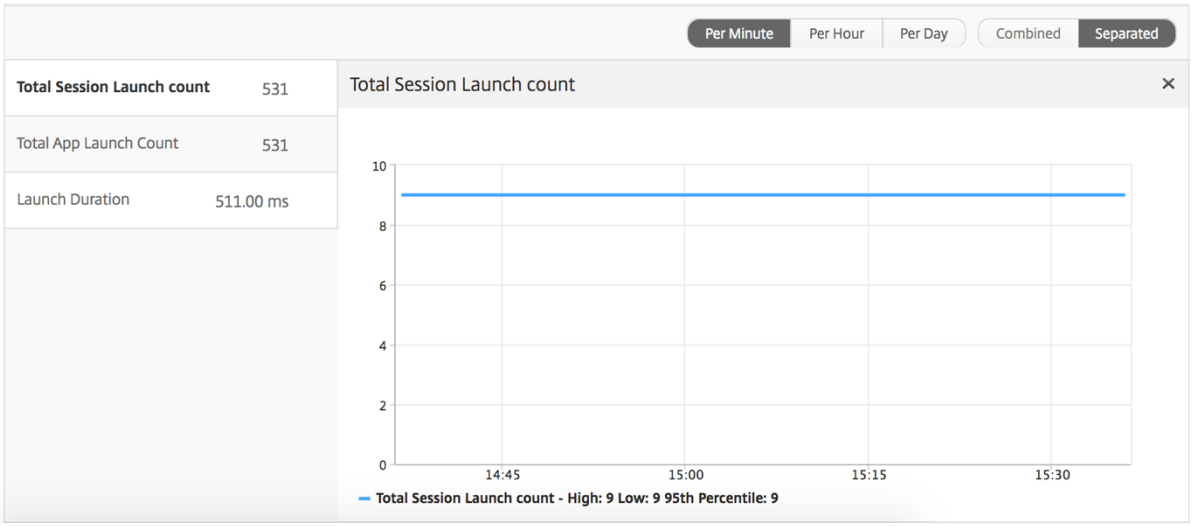


Rapport sur les seuils

Le rapport sur les seuils représente le nombre de seuils franchis lorsque l'*entité* est sélectionnée comme application au cours de la période sélectionnée. Pour plus d'informations, consultez comment créer des seuils et des alertes .

Graphique linéaire

Métriques	Description
Nombre de sessions actives	Ce nombre indique le nombre de sessions Citrix Virtual Apps and Desktops actives.
Durée du lancement	Temps moyen requis pour lancer une application.



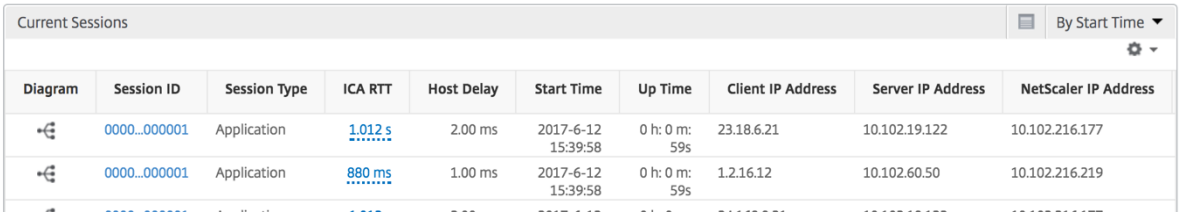
Rapport des sessions en cours

Métriques	Description
ID de session	Une identité unique pour une session ICA.
Type de session	Application/Bureau.
État	Vert/rouge pour les sessions actives/inactives.
Délai d'hôte	Délai moyen du trafic ICA transitant par les Citrix ADC causé par le réseau du serveur.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Bande passante de session	La bande passante consommée par la session quel que soit l'intervalle de temps.
Octets par intervalle	Nombre d'octets consommés par la session pendant cet intervalle de temps particulier.

Métriques	Description
Start Time	Heure de début de la session.
Temps d'activité	Durée de la session.
Adresse IP cliente	IP de l'utilisateur final.
Adresse IP du serveur	Adresse IP du serveur Backend/Citrix Virtual App.
Adresse IP NetScaler	IP de gestion NetScaler (NSIP).
Type de client	Type de Receiver - Client Windows Citrix et ainsi de suite
Version du client	Version du Receiver.
MSI	Boolean (Oui/Non). Indique si la session est multiflux ICA.
Reconnexions de session	Nombre de fois où la session s'est reconnectée.
Nb d'ACR	Nombre total de fois où un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, le mode utilisateur/transparent de Citrix Gateway.
Pays	Pays à partir duquel la session a été créée.
Région	Région à partir de laquelle la session a été créée.
City	Ville à partir de laquelle la session a été créée.
État de l'USB	Actif/Inactif -Vert/Rouge.
Nombre d'instances USB acceptées	Le nombre d'instances USB acceptées.
Nombre d'instances USB rejetées	Le nombre d'instances USB rejetées.
Nombre d'instances USB arrêtées	Le nombre d'instances USB arrêtées.
Nom d'hôte du client	Le nom d'hôte du client.
Nombre de basculements HA	Nombre de fois où le basculement HA s'est produit.
Motif de la résiliation	Affiche la raison de l'arrêt d'une session. Par exemple, délai d'expiration de session ICA, session terminée par l'utilisateur.

Métriques	Description
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de Citrix ADC aux serveurs back-end.
Nb total d'octets	Nombre total d'octets consommés par l'utilisateur pendant la période sélectionnée.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et serveur back-end.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit sur la connexion entre Citrix ADC et le serveur back-end.
Nom d'utilisateur	Nom d'utilisateur de l'utilisateur accédant à cette application virtuelle Citrix particulière.
ID de session	Identifiant unique pour la session Citrix Virtual App.
Type de session	Sera « Application ».
État	État de la session : vert pour actif, rouge pour inactif.

Métriques	Description
Latence maximale de violation	La valeur la plus élevée de la latence L7 lorsqu'un dépassement d'un seuil défini pour un intervalle de temps défini se produit.
Latence moyenne des violations	Valeur moyenne de la latence L7 lorsque le système est dans un état « Latence L7 violée ».
Nombre de franchissements de seuil L7	Nombre de fois qu'une violation du seuil L7 s'est produite.
Latence côté client L7	La latence moyenne L7 observée entre le client ICA et l'instance de Citrix ADC. Cette mesure est utile pour les périphériques non Citrix présents dans le chemin de remise.
Latence côté serveur L7	Latence moyenne L7 observée entre l'appareil Citrix ADC et l'application virtuelle Citrix. Cette mesure est utile pour les périphériques non Citrix présents dans le chemin de remise.



Par vue de session d'application

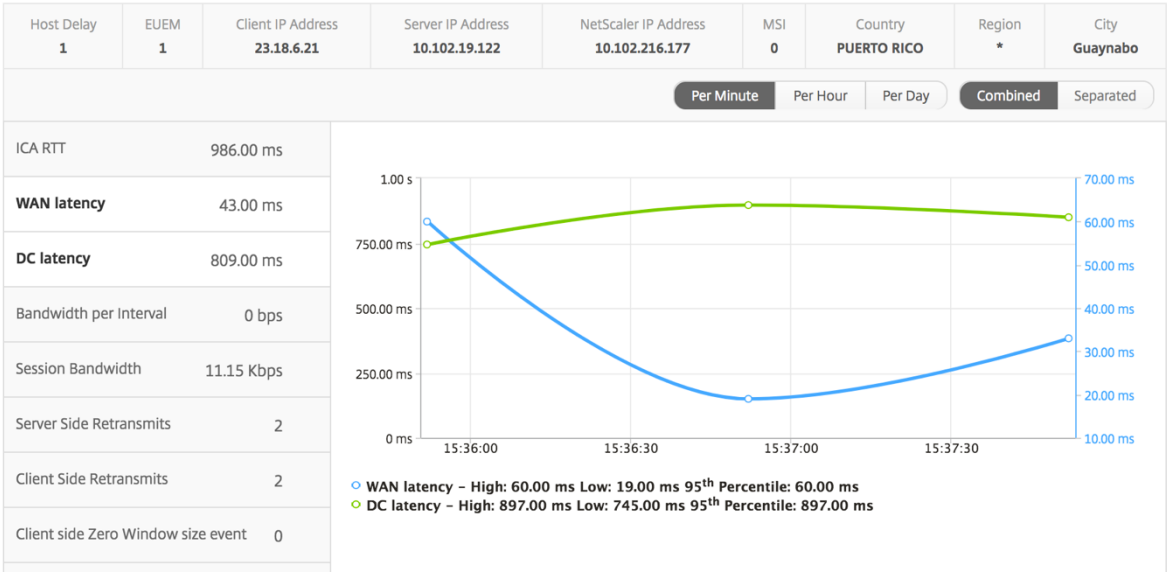
L'affichage par session d'application affiche les rapports pour une session d'application sélectionnée particulière.

Pour afficher les rapports de session :

1. Accédez à **Analytics** > **HDX Insight** > **Applications**.
2. Sélectionnez un utilisateur particulier dans le rapport récapitulatif des applications.
3. Sélectionné une session à partir du rapport des sessions en cours.

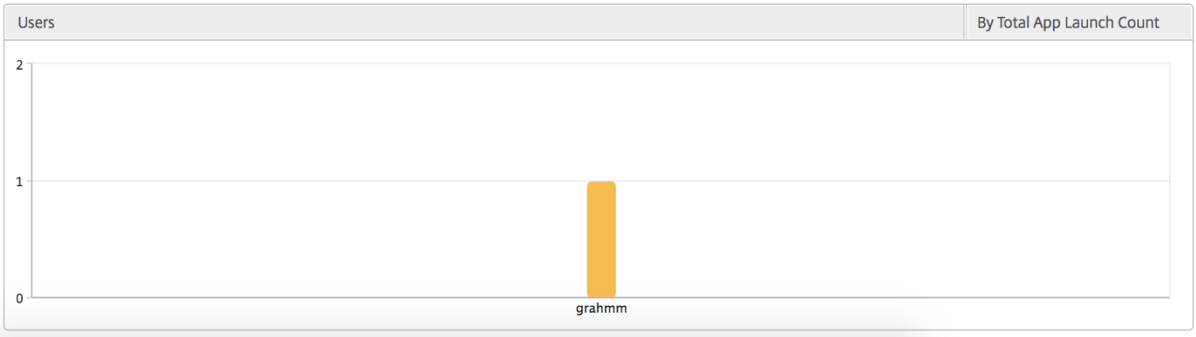
Graphique linéaire

Métriques	Description
Reconnexions de session	Nombre de fois où la session s'est reconnectée.
Nb d'ACR	Nombre total de fois où un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Événement de taille de fenêtre nulle côté serveur	Latence causée par le côté serveur du réseau. C'est-à-dire, de Citrix ADC aux serveurs back-end.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et serveur back-end.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
Bande passante de session	La bande passante consommée par la session quel que soit l'intervalle de temps.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit sur la connexion entre Citrix ADC et le serveur back-end.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.



Graphique à barres utilisateur

Le graphique à barres de l'utilisateur représente les utilisateurs connectés à cette application particulière.



Rapports et mesures d'affichage du Bureau

February 1, 2024

Les rapports et les mesures de cette vue sont axés sur les Citrix Virtual Desktops.

Pour accéder à la vue Bureau :

1. Accédez à **Analytics** > **HDX Insight** > **Bureau** .

Vue récapitulative

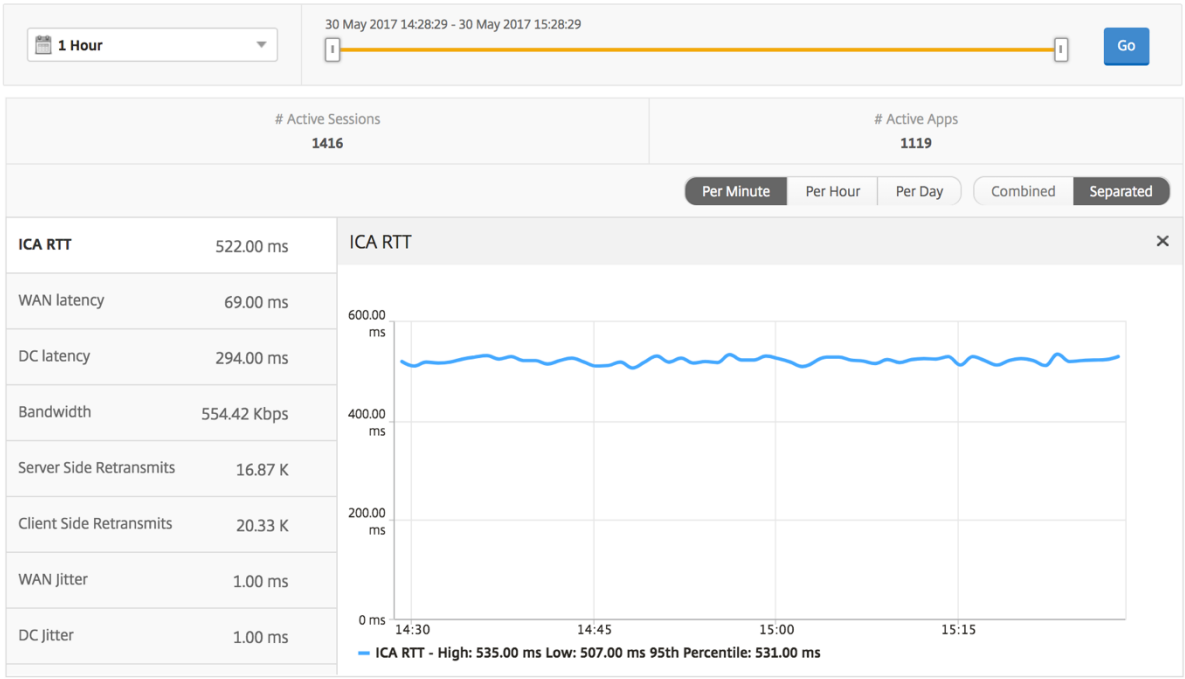
La vue récapitulative affiche les rapports de tous les Citrix Virtual Desktops qui sont connectés au cours de la chronologie sélectionnée.

Toutes les métriques/rapports, sauf mention explicite, auront les valeurs qui leur correspondent pour la période de sélection.

Graphique linéaire

Métriques	Description
Nombre de sessions actives	Ce nombre indique le nombre de sessions Citrix Virtual Apps and Desktops actives.
Nbre d'applications actives	Ce nombre indique le nombre de sessions actives de Citrix Virtual App.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de Citrix ADC aux serveurs back-end.
Bande passante	Nombre total d'octets par seconde pris pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et serveur back-end.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.

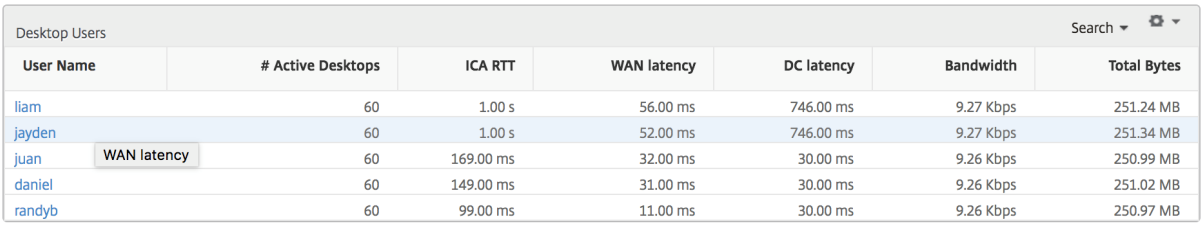
Métriques	Description
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit sur la connexion entre Citrix ADC et le serveur back-end.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.



Rapport récapitulatif du bureau

Métriques	Description
Active Sessions	Nombre total de sessions Citrix Virtual Desktop actives au cours d'un intervalle de temps donné.
Ordinateurs de bureau actifs	Nombre total de Citrix Virtual Desktops actifs au cours d'un intervalle de temps donné.

Métriques	Description
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de Citrix ADC aux serveurs back-end.
Bande passante	Nombre total d'octets par seconde pris pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Nb total d'octets	Nombre total d'octets consommés par l'utilisateur pendant la période sélectionnée.



Rapport sur les seuils

Le rapport de seuil représente le nombre de seuils dépassés lorsque l'*entité* est sélectionnée en tant que Bureau au cours de la période sélectionnée. Pour plus d'informations, consultez comment créer des seuils et des alertes .

Par vue de bureau

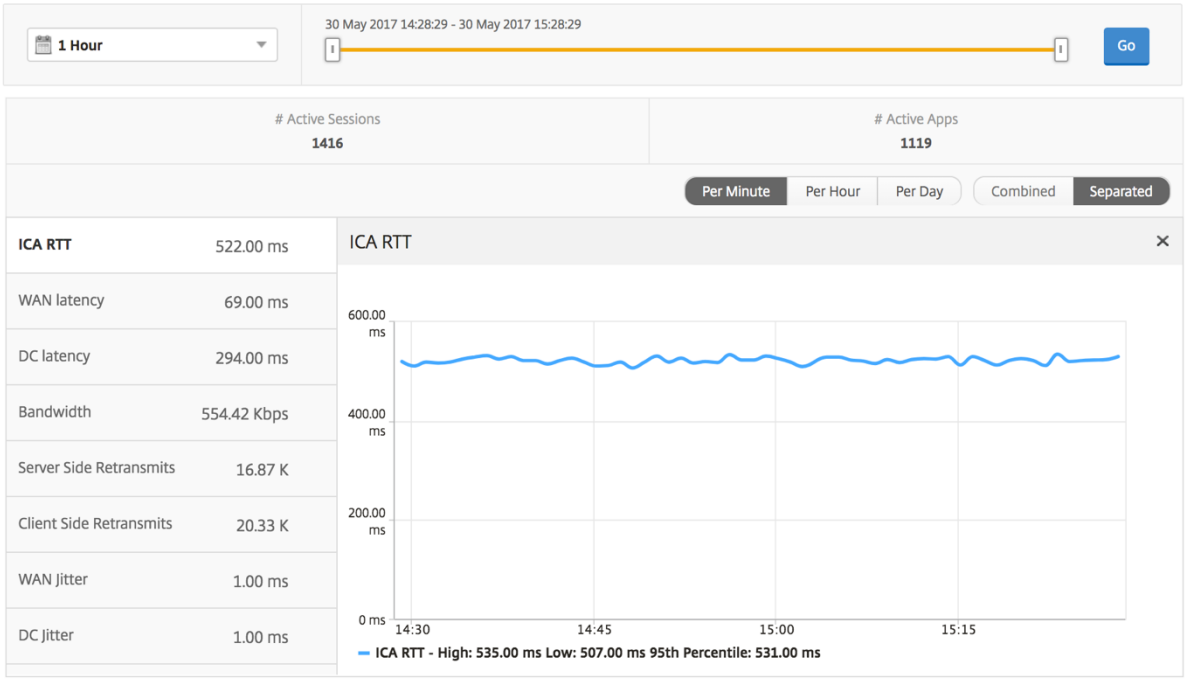
La vue par poste de travail fournit des rapports détaillés sur l'expérience utilisateur pour un Citrix Virtual Desktop sélectionné.

Pour accéder à la vue Bureau spécifique :

1. Accédez à **Analytics > HDX Insight > Bureau**.
2. Sélectionnez un **poste de travail** particulier dans le **rapport récapitulatif des ordinateurs de bureau**.

Graphique linéaire

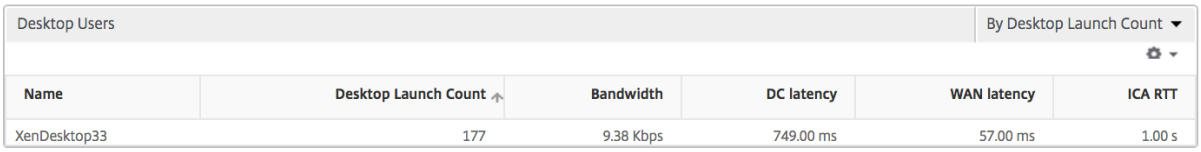
Métriques	Description
Nombre de sessions actives	Ce nombre indique le nombre de sessions Citrix Virtual Apps and Desktops actives.
Nbre d'applications actives	Ce nombre indique le nombre de sessions actives de Citrix Virtual App.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de Citrix ADC aux serveurs back-end.
Bande passante	Nombre total d'octets par seconde pris pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et serveur back-end.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit sur la connexion entre Citrix ADC et le serveur back-end.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.



Rapport sur les utilisateurs du bureau

Ce tableau donne un aperçu des sessions Citrix Virtual Desktop pour un utilisateur particulier. Ces mesures peuvent être triées par nombre de lancements de postes de travail et bande passante.

Mesures	Description
Nom	Nom du bureau virtuel Citrix.
Nombre de lancements de bureaux	Nombre de fois que l'ordinateur de bureau a été lancé.
Bande passante	Nombre total d'octets par seconde pris pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de Citrix ADC aux serveurs back-end.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.



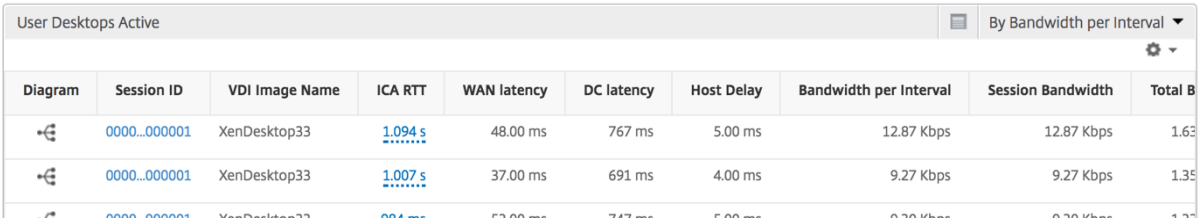
Rapport actif/inactif sur les postes de travail utilisateur

Les mesures suivantes peuvent être triées en fonction de la bande passante par intervalle, des reconnexions de session et du nombre d'ACR.

Mesures	Description
ID de session	Une identité unique pour une session ICA.
Type de session	Application/Bureau.
État	Vert/rouge pour les sessions actives/inactives.
Délai d'hôte	Délai moyen du trafic ICA transitant par les Citrix ADC causé par le réseau de serveurs.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Bande passante de session	La bande passante consommée par la session quel que soit l'intervalle de temps.
Octets par intervalle	Nombre d'octets consommés par la session pendant cet intervalle de temps particulier.
Start Time	Heure de début de la session.
Temps d'activité	Durée de la session.
Adresse IP cliente	IP de l'utilisateur final.
Adresse IP du serveur	Adresse IP du serveur Backend/Citrix Virtual App.
Adresse IP NetScaler	IP de gestion NetScaler (NSIP).
Type de client	Type de Receiver - Client Windows Citrix et ainsi de suite
Version du client	Version du Receiver.
MSI	Boolean (Oui/Non). Indique si la session est multiflux ICA.
Reconnexions de session	Nombre de fois où la session s'est reconnectée.
Nb d'ACR	Nombre total de fois où un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.

Mesures	Description
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, le mode utilisateur/transparent de Citrix Gateway.
Pays	Pays à partir duquel la session a été créée.
Région	Région à partir de laquelle la session a été créée.
City	Ville à partir de laquelle la session a été créée.
État de l'USB	Actif/Inactif -Vert/Rouge.
Nombre d'instances USB acceptées	Le nombre d'instances USB acceptées.
Nombre d'instances USB rejetées	Le nombre d'instances USB rejetées.
Nombre d'instances USB arrêtées	Le nombre d'instances USB arrêtées.
Nom d'hôte du client	Le nom d'hôte du client.
Nombre de basculements HA	Nombre de fois où le basculement HA s'est produit.
Motif de la résiliation	Affiche la raison de l'arrêt d'une session. Par exemple, délai d'expiration de session ICA, session terminée par l'utilisateur.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lorsqu'il interagit avec une application ou un bureau hébergé respectivement sur Citrix Virtual Apps ou Desktops.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de Citrix ADC aux serveurs back-end.
Nb total d'octets	Nombre total d'octets consommés par l'utilisateur pendant la période sélectionnée.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et serveur back-end.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.

Mesures	Description
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit sur la connexion entre Citrix ADC et le serveur back-end.
Nom de l'image VDI	Nom du Citrix Virtual Desktops auquel l'utilisateur est connecté
Diagramme	



Par vue de session de bureau

La vue par session de bureau fournit des rapports pour une session Citrix Virtual Desktops sélectionnée.

Pour accéder à la vue de session Bureau :

1. Accédez à **Analytics** > **HDX Insight** > **Bureau** .
2. Sélectionnez un poste de travail particulier dans le **rapport récapitulatif des postes**de travail.
3. Sélectionnez une session dans le rapport des sessions en cours.

Graphique chronologique

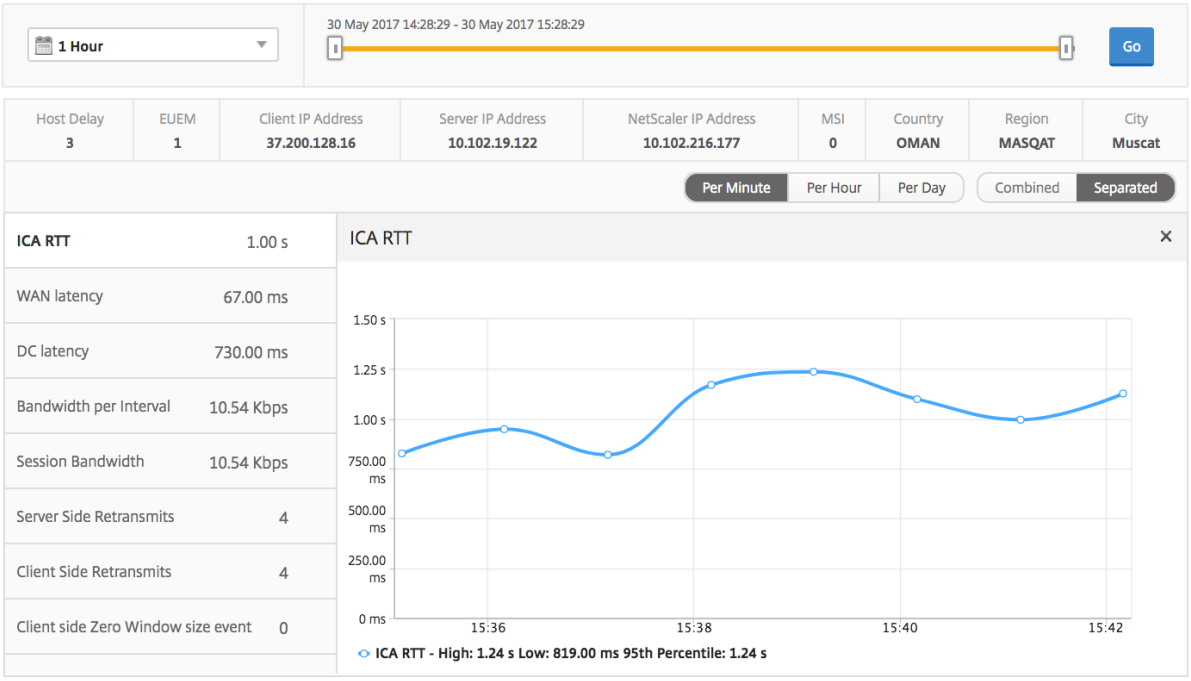
La vue par session utilisateur fournit des rapports pour la session d'un utilisateur sélectionné particulier.

Pour afficher les mesures de la session d'un utilisateur sélectionné :

1. Accédez à **Analytics** > **HDX Insight** > **Utilisateurs**.
2. Select un utilisateur particulier dans la section **Rapport récapitulatif de l'utilisateur**.
3. Sélectionnez une session dans la colonne **Sessions en cours** ou **Sessions terminées** .

Mesures	Description
Reconnexions de session	Ce nombre indique le nombre de sessions Citrix Virtual App and Desktop actives.
Nb d'ACR	Ce nombre indique le nombre de sessions actives de Citrix Virtual App.
RTT ICA	L'ICA RTT est le décalage d'écran que l'utilisateur ressent lorsqu'il interagit avec une application ou un poste de travail hébergés respectivement sur Citrix Virtual Apps and Desktops.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de Citrix ADC aux serveurs back-end.
Bande passante de session	La bande passante consommée par la session quel que soit l'intervalle de temps.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et serveur back-end.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit sur la connexion entre Citrix ADC et le serveur back-end.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.

Mesures	Description
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.



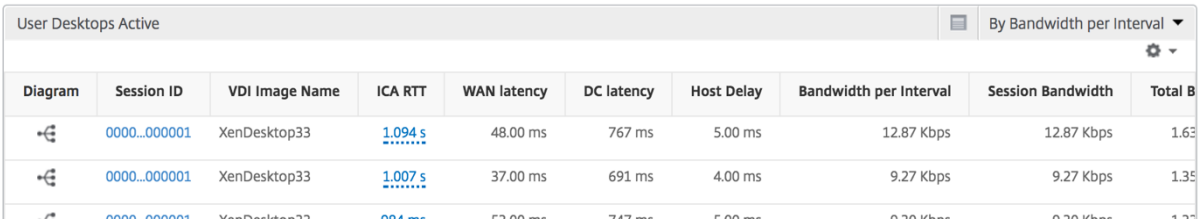
Rapport sur les sessions de bureau associées

Les mesures suivantes peuvent être triées en fonction de la bande passante par intervalle, des reconnexions de session et du nombre d'ACR.

Mesures	Description
ID de session	Une identité unique pour une session ICA.
Type de session	Application/Bureau.
État	Vert/rouge pour les sessions actives/inactives.
Délai d'hôte	Délai moyen du trafic ICA transitant par les Citrix ADC causé par le réseau du serveur.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Bande passante de session	La bande passante consommée par la session quel que soit l'intervalle de temps.

Mesures	Description
Octets par intervalle	Nombre d'octets consommés par la session pendant cet intervalle de temps particulier.
Start Time	Heure de début de la session.
Temps d'activité	Durée de la session.
Adresse IP cliente	IP de l'utilisateur final.
Adresse IP du serveur	Adresse IP du serveur Backend/Citrix Virtual App.
Adresse IP NetScaler	IP de gestion NetScaler (NSIP).
Type de client	Type de Receiver - Client Windows Citrix et ainsi de suite
Version du client	Version du Receiver.
MSI	Boolean (Oui/Non). Indique si la session est multiflux ICA.
Reconnexions de session	Nombre de fois où la session s'est reconnectée.
Nb d'ACR	Nombre total de fois où un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, le mode utilisateur/transparent de Citrix ADC Gateway.
Pays	Pays à partir duquel la session a été créée.
Région	Région à partir de laquelle la session a été créée.
City	Ville à partir de laquelle la session a été créée.
État de l'USB	Actif/Inactif -Vert/Rouge.
Nombre d'instances USB acceptées	Le nombre d'instances USB acceptées.
Nombre d'instances USB rejetées	Le nombre d'instances USB rejetées.
Nombre d'instances USB arrêtées	Le nombre d'instances USB arrêtées.
Nom d'hôte du client	Le nom d'hôte du client.
Nombre de basculements HA	Nombre de fois où le basculement HA s'est produit.
Motif de la résiliation	Affiche la raison de l'arrêt d'une session. Par exemple, délai d'expiration de session ICA, session terminée par l'utilisateur.

Mesures	Description
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps ou Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de Citrix ADC aux serveurs back-end.
Nb total d'octets	Nombre total d'octets consommés par l'utilisateur pendant la période sélectionnée.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et serveur back-end.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit sur la connexion entre Citrix ADC et le serveur back-end.
Nom de l'image VDI	Nom du Citrix Virtual Desktops auquel l'utilisateur est connecté

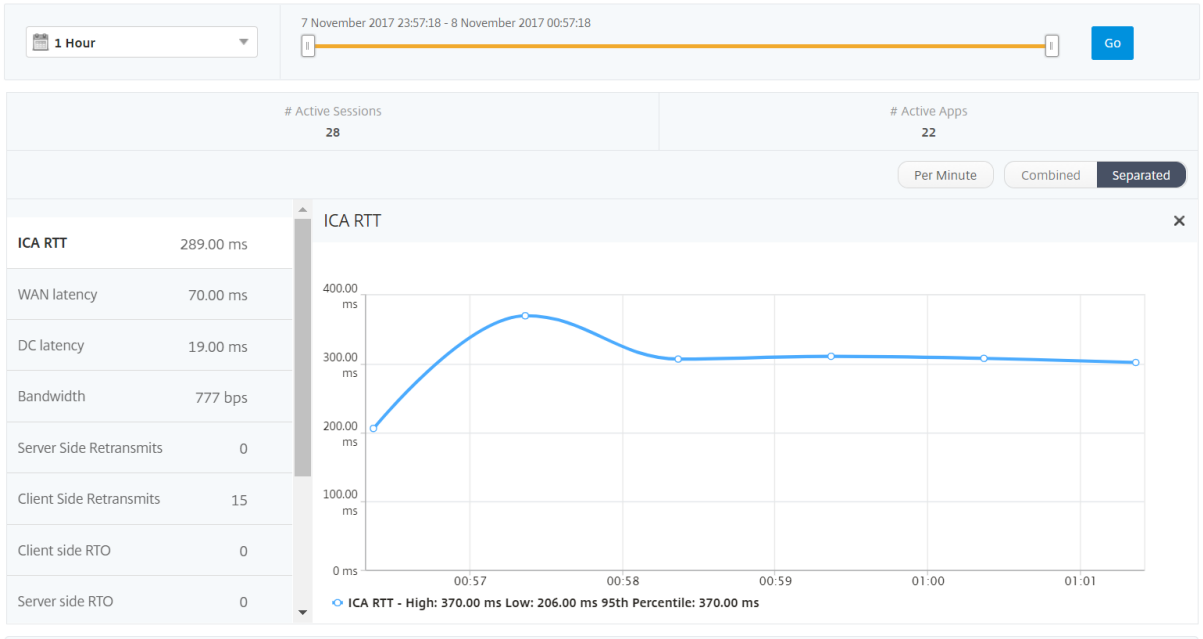


Afficher les rapports et les mesures de l'utilisateur

February 1, 2024

Les rapports et les mesures de cette vue sont affichés par les utilisateurs Citrix Virtual Apps et Desktop.

Accédez à **Analytics** > **HDX Insight** > **Utilisateurs**.



Vue récapitulative

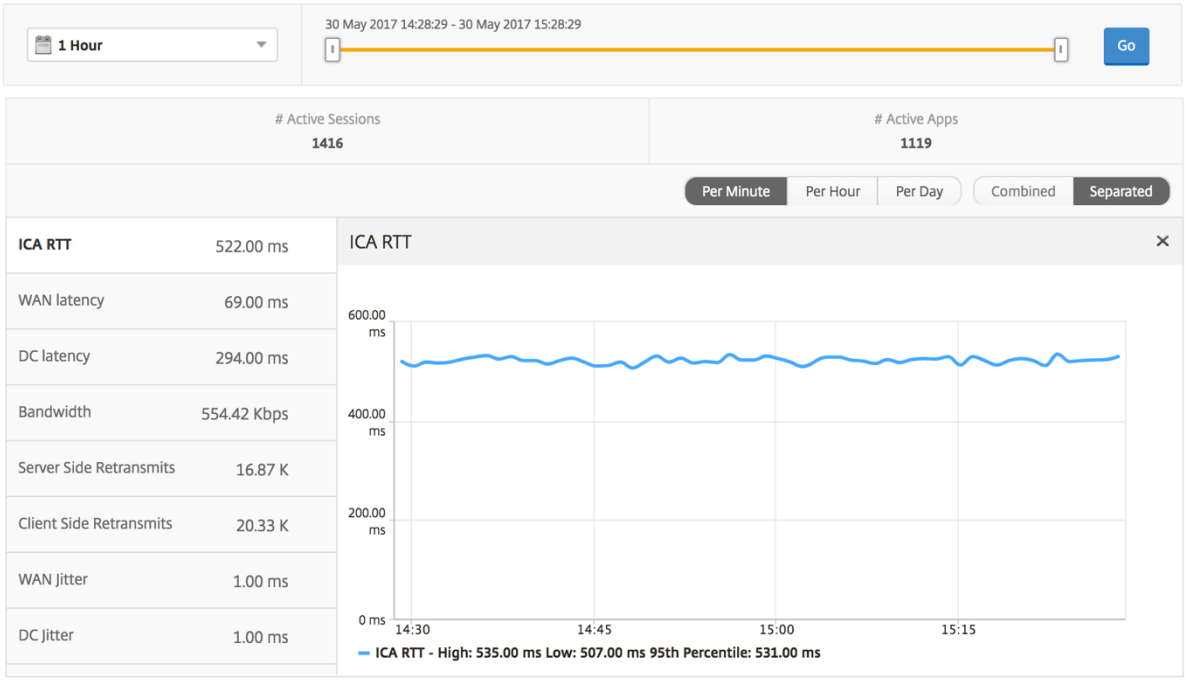
La vue récapitulative affiche les rapports de tous les utilisateurs qui se sont connectés au cours de la chronologie sélectionnée. Toutes les métriques/rapports de cette vue affichent les valeurs qui leur correspondent pour la période sélectionnée, sauf indication contraire.

Pour modifier la période sélectionnée :

1. Utilisez la liste de périodes ou le curseur temporel pour définir l'intervalle de temps souhaité.
2. Cliquez sur **Go**.

Graphique linéaire

Métriques	Description
Nombre de sessions actives	Ce nombre indique le nombre de sessions Citrix Virtual App and Desktop actives.
Nbre d'applications actives	Ce nombre indique le nombre de sessions actives de Citrix Virtual App.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps ou Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire de Citrix ADC aux serveurs principaux.
Bande passante	Nombre total d'octets par seconde pris pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de la retransmission s'est produit sur la connexion entre Citrix ADC et le serveur principal.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.



Rapport récapitulatif de l'utilisateur

Voici les mesures spécifiques à ce rapport.

Mesures	Description
Nombre de sessions actives	Ce nombre indique le nombre de sessions Citrix Virtual App and Desktop actives.
Nbre d'applications actives	Ce nombre indique le nombre de sessions actives de Citrix Virtual App.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps ou Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire de Citrix ADC aux serveurs principaux.
Bande passante	Nombre total d'octets par seconde pris pour la communication de bout en bout pendant l'intervalle de temps sélectionné.

Mesures	Description
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
RTO rapide côté client	Nombre de fois où le délai de retransmission s' est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de la retransmission s'est produit sur la connexion entre Citrix ADC et le serveur principal.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.
Nb total d'applications lancées	Total des applications lancées par l'utilisateur au cours de la période sélectionnée.
Nb total d'octets	Nombre total d'octets consommés par l' utilisateur pendant la période sélectionnée.
Ordinateurs de bureau actifs	Nombre total de Citrix Virtual Desktops actifs au cours d'un intervalle de temps donné.

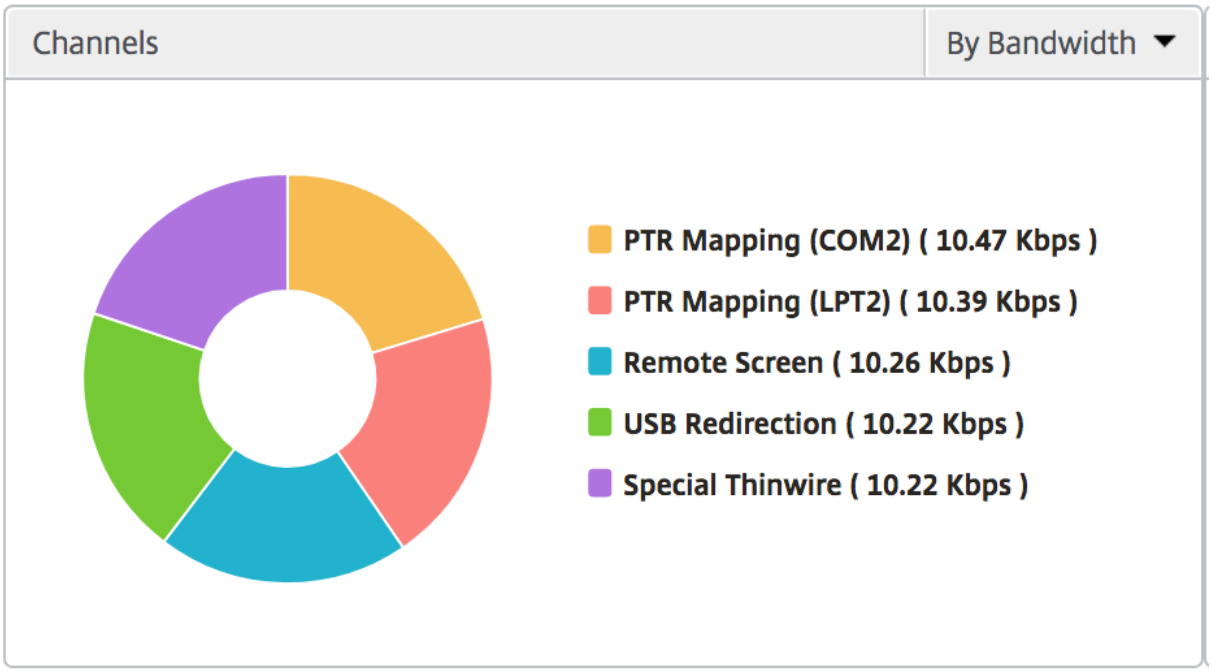
Users

Search

User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT	WAN latency	DC latency	Bandwidth	Server Side Retransmits	Cl
liam	59	59	118	999.00 ms	57.00 ms	751.00 ms	47.25 Kbps	3.74 K	
jayden	59	59	118	999.00 ms	52.00 ms	751.00 ms	47.06 Kbps	3.71 K	
florinl	59	0	59	997.00 ms	52.00 ms	754.00 ms	23.66 Kbps	1.88 K	
ramas	59	0	59	997.00 ms	778.00 ms	1.00 ms	7.03 Kbps	0	
omerp	59	0	59	997.00 ms	57.00 ms	754.00 ms	23.80 Kbps	1.89 K	
grahmm	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.80 Kbps	1.89 K	
ryan	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.69 Kbps	1.88 K	
rajivs	59	0	59	801.00 ms	11.00 ms	1.00 ms	23.97 Kbps	0	
alexisc	117	0	118	622.00 ms	56.00 ms	392.00 ms	47.67 Kbps	1.88 K	
juan	59	59	118	169.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
lennoxl	59	0	59	169.00 ms	31.00 ms	30.00 ms	23.86 Kbps	0	
daniel	59	59	118	149.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
woojunek	58	0	59	149.00 ms	31.00 ms	30.00 ms	23.85 Kbps	0	
parkerf	59	0	59	149.00 ms	31.00 ms	30.00 ms	23.88 Kbps	0	
randyb	59	59	118	99.00 ms	11.00 ms	29.00 ms	47.71 Kbps	0	
bradp	177	0	177	74.00 ms	27.00 ms	1.00 ms	71.75 Kbps	0	

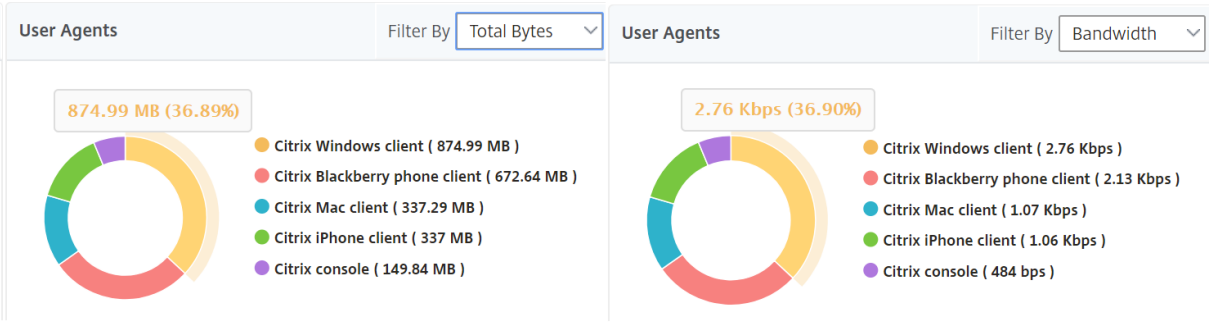
Canaux

Les canaux représentent la bande passante globale ou le nombre total d'octets consommés par chaque canal virtuel ICA sous la forme d'un graphique en anneau. Vous pouvez également trier les mesures par bande passante ou Nombre total d'octets.



Agents utilisateurs

Les agents utilisateurs représentent la bande passante globale/nombre total d'octets consommés par chaque point final sous la forme d'un graphique en donut. Vous pouvez également trier les mesures par bande passante ou Nombre total d'octets.



Nombre de violations des seuils

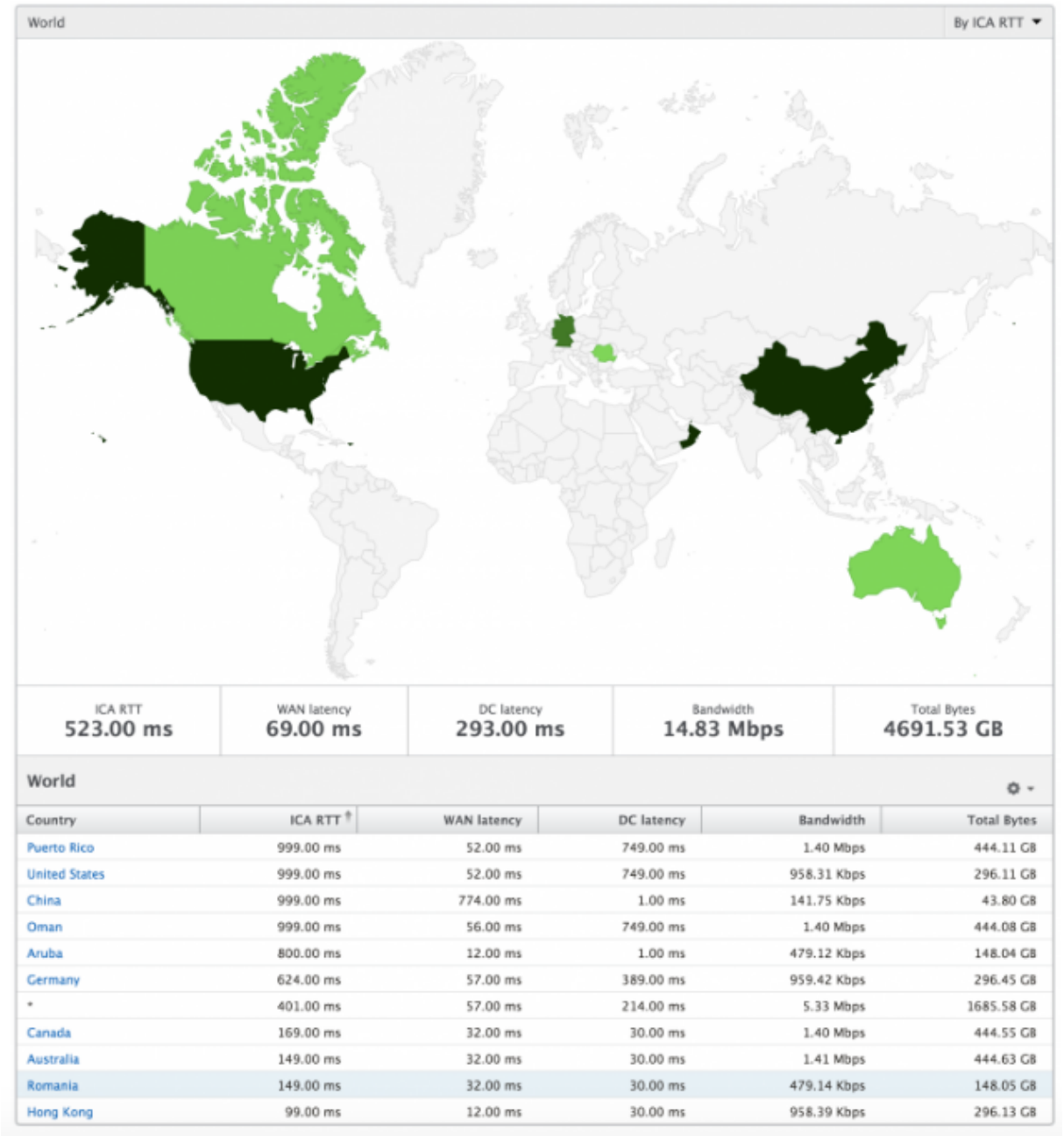
Les mesures de nombre de violations des seuils représentent le nombre de seuils violés au cours de la période sélectionnée. Pour plus d'informations, découvrez comment créer des seuils et des alertes.

Carte du monde

La vue Carte du monde dans HDX insights permet aux administrateurs de visualiser les détails des utilisateurs historiques et actifs d'un point de vue géographique. Les administrateurs peuvent avoir une vue du monde du système, une exploration vers un pays particulier et plus loin dans les villes ainsi qu'en cliquant sur la région. Les administrateurs peuvent approfondir leurs recherches pour afficher les informations par ville et par État. À partir de Citrix ADM version 12.0 et ultérieure, vous pouvez effectuer une exploration vers le bas vers les utilisateurs connectés à partir d'un emplacement Geo.

Les détails suivants peuvent être consultés sur la carte du monde dans un aperçu HDX, et la densité de chaque mesure est affichée sous la forme d'une carte thermique :

- RTT ICA
- Latence WAN
- Latence DC
- Bande passante
- Nb total d'octets



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

Par vue utilisateur

La vue par utilisateur fournit des rapports détaillés sur l'expérience utilisateur final pour un utilisateur sélectionné particulier.

Pour accéder aux mesures spécifiques d'un utilisateur :

1. Accédez à **Analytics** > **HDX Insight** > **Utilisateurs**.
2. Sélectionnez un utilisateur particulier dans le rapport récapitulatif Utilisateurs.

Graphique linéaire

Le graphique en courbes affiche le résumé de toutes les mesures pour l'utilisateur sélectionné particulier pendant la période sélectionnée.

Rapport Sessions en cours/terminées

Ce rapport est pertinent pour toutes les sessions utilisateur en cours/terminées pour l'utilisateur sélectionné. Ces mesures peuvent être triées par heure de début, reconnexions de session et nombre d'ACR.

Mesures	Description
ID de session	Une identité unique pour une session ICA.
Type de session	Application/Bureau.
État	Vert/rouge pour les sessions actives/inactives.
Délai d'hôte	Délai moyen du trafic ICA transitant par les Citrix ADC causé par le réseau de serveurs.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Bande passante de session	La bande passante consommée par la session quel que soit l'intervalle de temps.
Octets par intervalle	Nombre d'octets consommés par la session pendant cet intervalle de temps particulier.
Start Time	Heure de début de la session.
Temps d'activité	Durée de la session.
Adresse IP cliente	IP de l'utilisateur final.
Adresse IP du serveur	Adresse IP du serveur Backend/Citrix Virtual App.
Adresse IP NetScaler	IP de gestion NetScaler (NSIP).
Type de client	Type de Receiver - Client Windows Citrix et ainsi de suite
Version du client	Version du Receiver.
MSI	Boolean (Oui/Non). Indique si la session est multiflux ICA.
Reconnexions de session	Nombre de fois où la session s'est reconnectée.

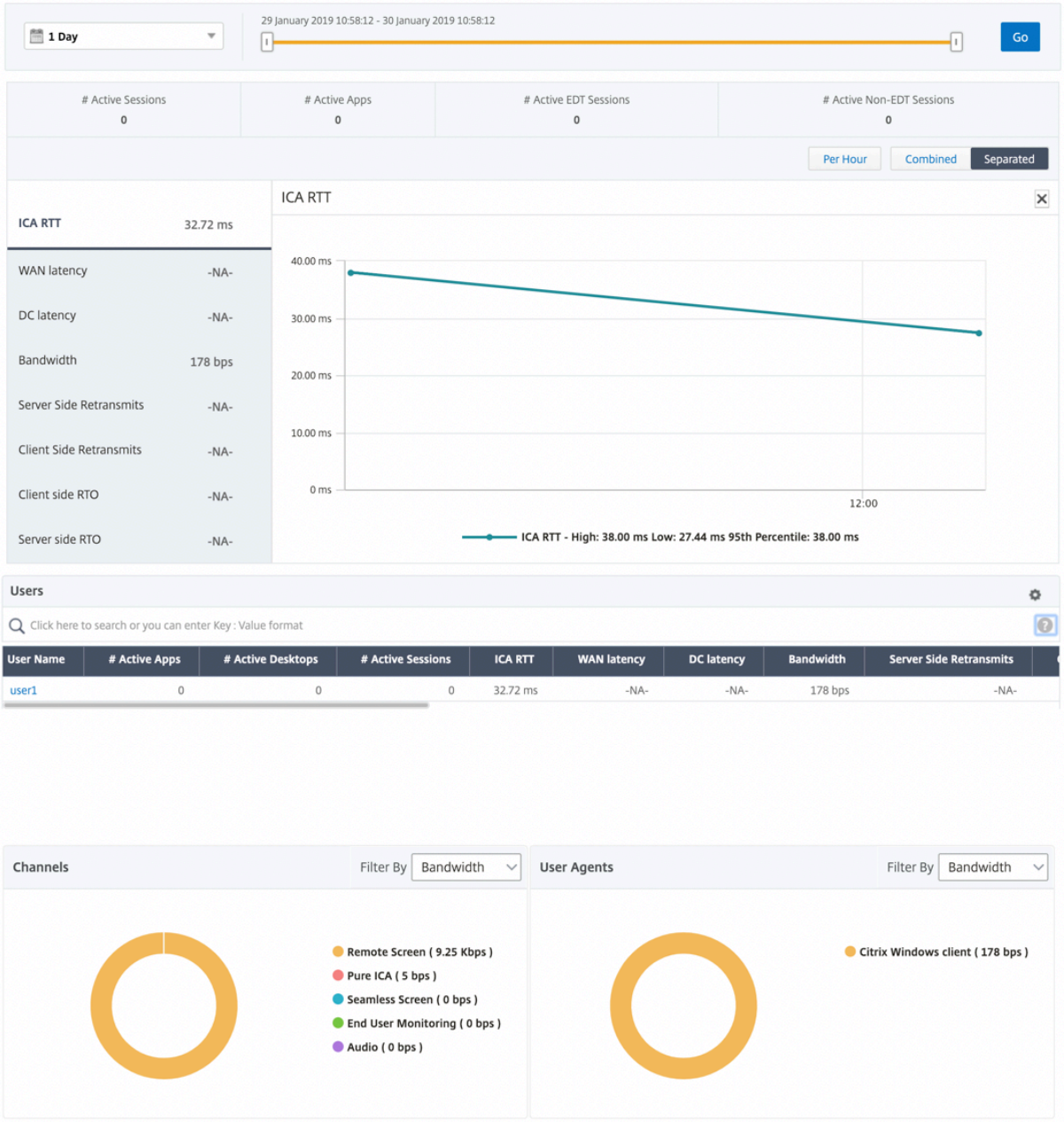
Mesures	Description
Nb d'ACR	Nombre total de fois où un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, le mode utilisateur/transparent de Citrix Gateway.
Pays	Pays à partir duquel la session a été créée.
Région	Région à partir de laquelle la session a été créée.
City	Ville à partir de laquelle la session a été créée.
État de l'USB	Actif/Inactif -Vert/Rouge.
Nombre d'instances USB acceptées	Le nombre d'instances USB acceptées.
Nombre d'instances USB rejetées	Le nombre d'instances USB rejetées.
Nombre d'instances USB arrêtées	Le nombre d'instances USB arrêtées.
Nom d'hôte du client	Le nom d'hôte du client.
Nombre de basculements HA	Nombre de fois où le basculement HA s'est produit.
Motif de la résiliation	Affiche la raison de l'arrêt d'une session. Par exemple, délai d'expiration de session ICA, session terminée par l'utilisateur.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps ou Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire de Citrix ADC aux serveurs principaux.
Nb total d'octets	Nombre total d'octets consommés par l'utilisateur pendant la période sélectionnée.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et le serveur principal.

Mesures	Description
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de la retransmission s'est produit sur la connexion entre Citrix ADC et le serveur principal.

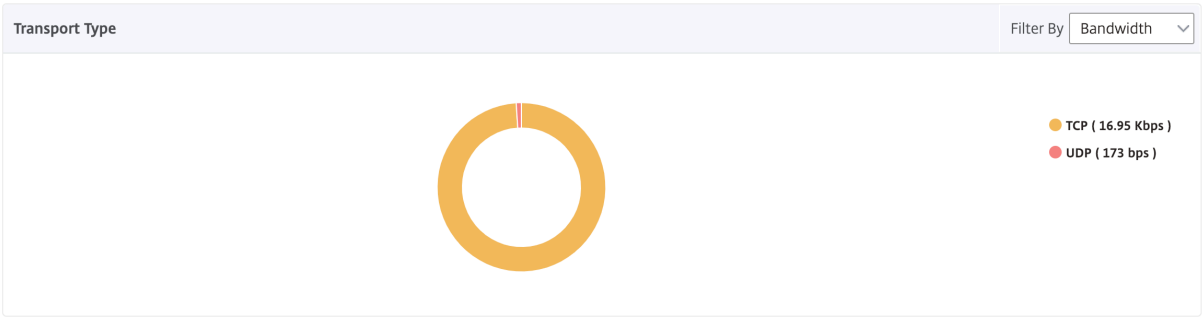
Prise en charge de l'EDT dans HDX insights

Citrix Application Delivery Management (ADM) prend désormais en charge le transport de données éclairé (EDT) pour afficher les analyses pour HDX Insight. En d'autres termes, ADM prend désormais en charge les protocoles UDP et TCP. La prise en charge d'EDT pour Citrix Gateway garantit une expérience utilisateur haute définition en session des bureaux virtuels pour les utilisateurs exécutant Citrix Receiver.

HDX Insight affiche désormais le nombre de sessions EDT et de sessions non EDT dans le rapport des sessions actives. Le tableau Utilisateurs affiche un rapport détaillé de tous les utilisateurs du système. Le tableau présente des indicateurs tels que la latence WAN, la latence DC, les retransmissions et les RTO. Certaines de ces statistiques ne sont pas disponibles pour les utilisateurs disposant de sessions EDT, car elles sont actuellement calculées à partir de la pile TCP. Par conséquent, ils apparaissent comme « NA ».

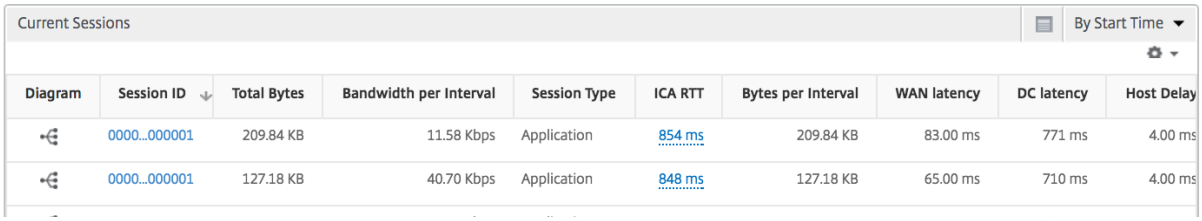


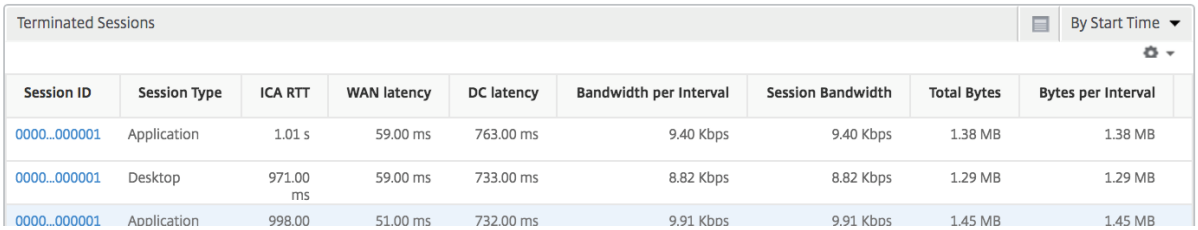
Un nouveau graphique en anneau a été introduit pour vous permettre de voir la bande passante consommée par l'utilisateur ainsi que le nombre total d'octets en fonction du type de protocole utilisé par les utilisateurs.



Mesures HDX Insight disponibles à partir de Citrix ADM 12.0 et versions ultérieures :

Latence côté client L7	La latence moyenne L7 observée entre le client ICA et l'instance de Citrix ADC. Cette mesure est utile dans le cas de périphériques non Citrix présents dans le chemin de remise.
Latence côté serveur L7	Latence moyenne L7 observée entre l'appareil Citrix ADC et l'application virtuelle Citrix. Cette mesure est utile dans le cas de périphériques non Citrix présents dans le chemin de remise.
Latence maximale de violation	La valeur la plus élevée de la latence L7 lorsqu'un dépassement d'un seuil défini pour un intervalle de temps défini se produit.
Latence moyenne des violations	Valeur moyenne de la latence L7 lorsque le système est dans un état « Latence L7 violée ».
Nombre de franchissements de seuil L7	Nombre de fois qu'une violation du seuil L7 s'est produite.

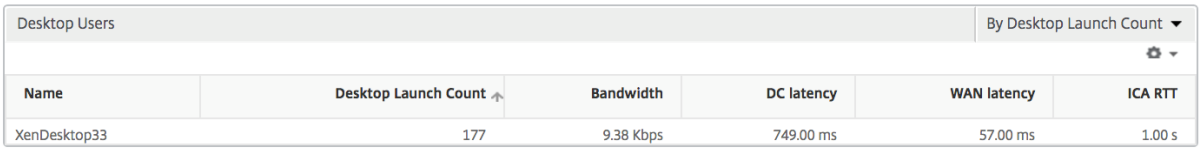




Utilisateurs de bureau

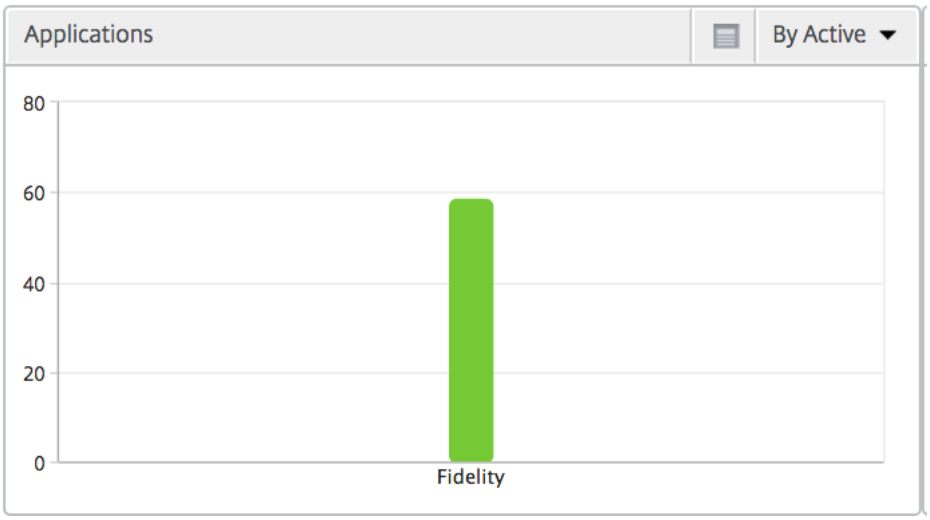
Ce tableau donne un aperçu des sessions Citrix Virtual Desktop pour un utilisateur particulier. Ces mesures peuvent être triées par nombre de lancements de postes de travail et bande passante.

Mesures	Description
Nom	Nom du bureau virtuel Citrix.
Nombre de lancements de bureaux	Nombre de fois que l'ordinateur de bureau a été lancé.
Bande passante	Nombre total d'octets par seconde pris pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire de Citrix ADC aux serveurs principaux.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps ou Desktops respectivement.



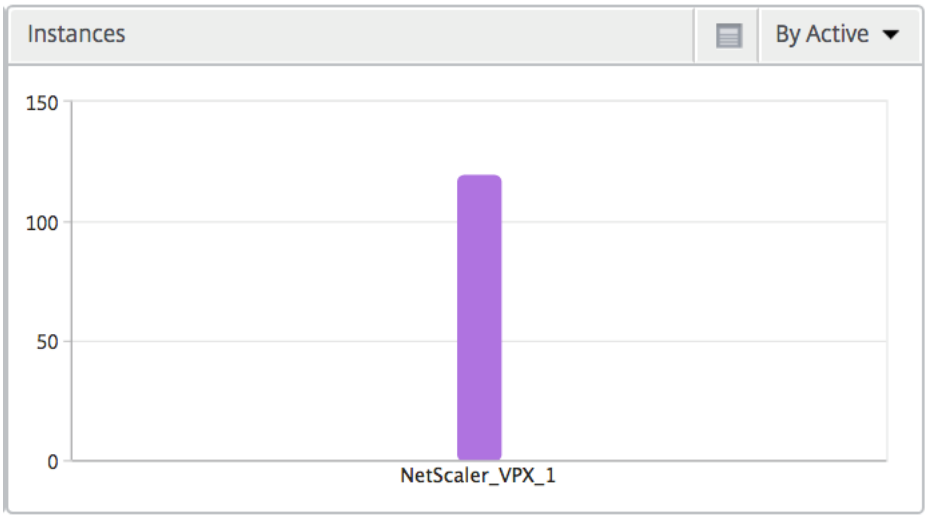
Applications

Graphique à barres représentant les applications triées par Active, nombre total de lancements de session, nombre total de lancements d'applications et durée de lancement.



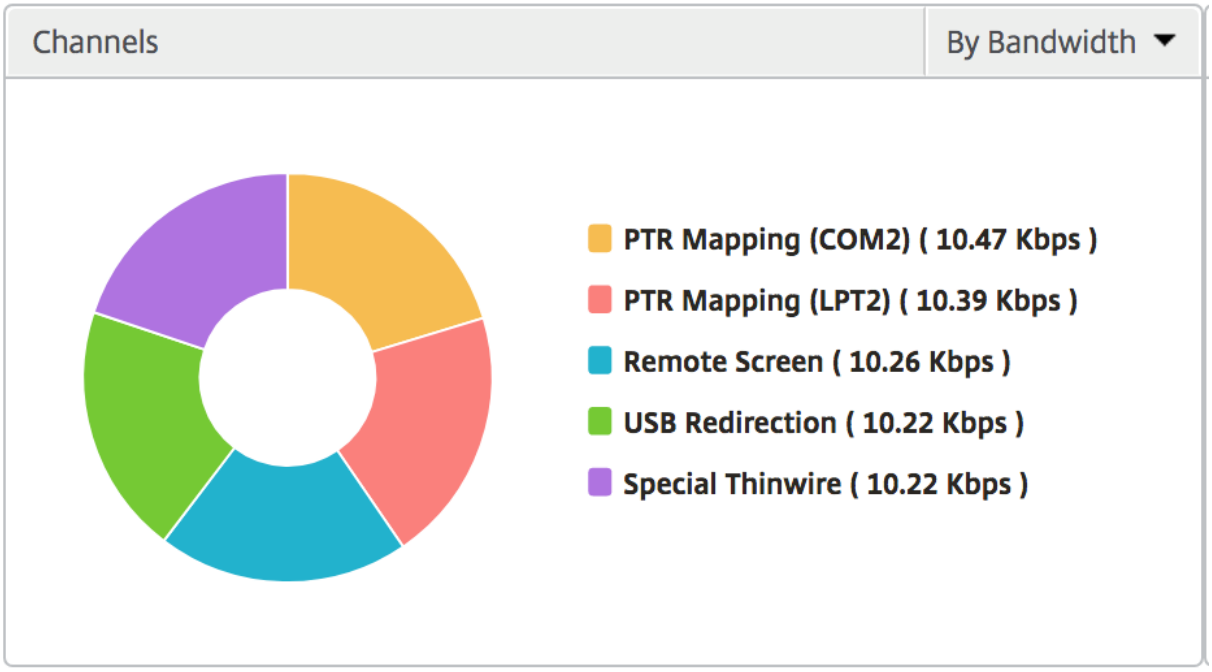
Instances

Graphique à barres représentant les instances Citrix ADC triées par applications actives et par nombre total d'applications



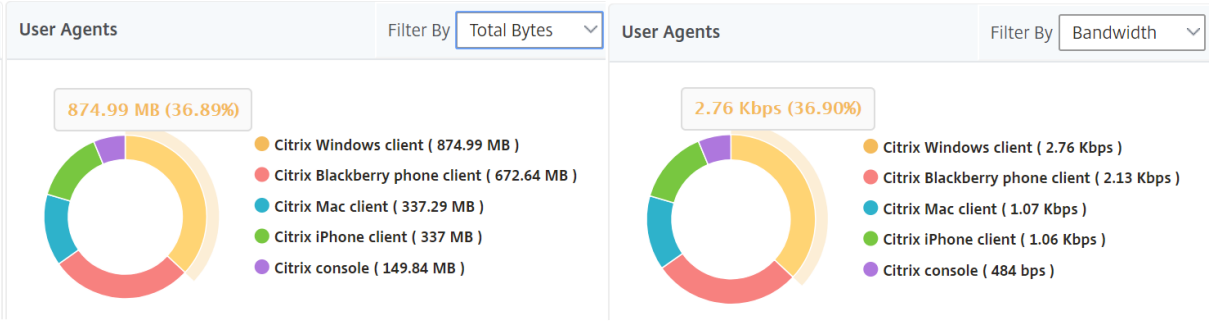
Canaux

Les canaux représentent la bande passante globale ou le nombre total d'octets consommés par chaque canal virtuel ICA sous la forme d'un graphique en anneau. Vous pouvez également trier les mesures par bande passante ou Nombre total d'octets.



Agents utilisateurs

Les agents utilisateurs représentent la bande passante globale/nombre total d'octets consommés par chaque point final sous la forme d'un graphique en donut. Vous pouvez également trier les mesures par bande passante ou Nombre total d'octets.



Par vue de session utilisateur

La vue par session utilisateur fournit des rapports pour la session d'un utilisateur sélectionné particulier.

Pour afficher les mesures de la session d'un utilisateur sélectionné :

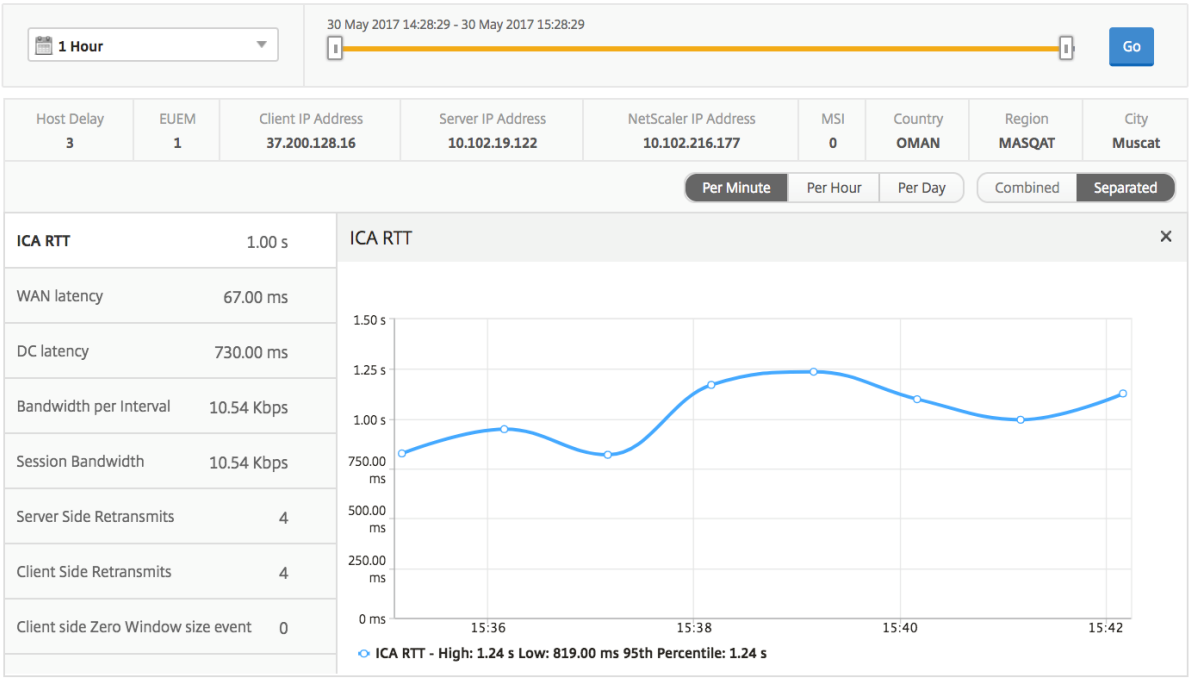
1. Accédez à **Analytics** > **HDX Insight** > **Utilisateurs**.
2. Select un utilisateur particulier dans la section **Rapport récapitulatif de l'utilisateur**.

3. Sélectionnez une session dans la colonne **Sessions en cours** ou **Sessions terminées** .

Graphique chronologique

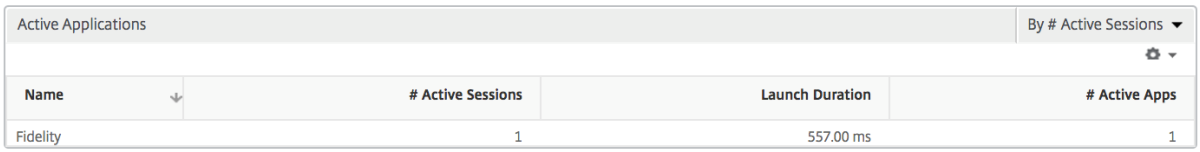
Mesures	Description
Reconnexions de session	Ce nombre indique le nombre de sessions Citrix Virtual App and Desktop actives.
Nb d'ACR	Ce nombre indique le nombre de sessions actives de Citrix Virtual App.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps ou Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire de Citrix ADC aux serveurs principaux.
Bande passante de session	La bande passante consommée par la session quel que soit l'intervalle de temps.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de la retransmission s'est produit sur la connexion entre Citrix ADC et le serveur principal.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.

Mesures	Description
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.



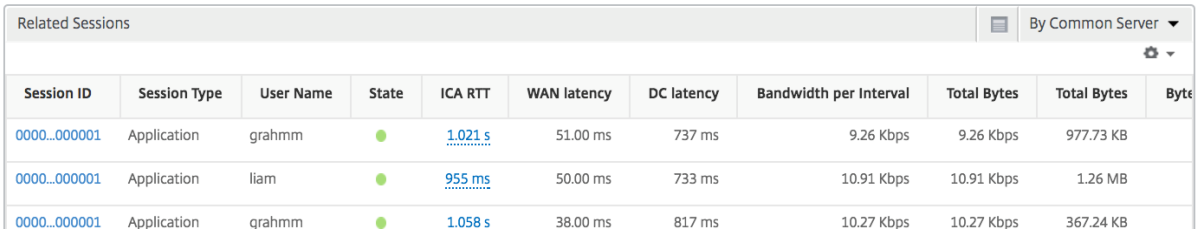
Application active

La section **Applications actives** affiche les applications actives de l'utilisateur sélectionné. Ces applications peuvent également être triées en fonction du nombre de sessions actives et des durées de lancement.



Sessions connexes

La section Sessions associées affiche les sessions associées des sessions de l'utilisateur sélectionné. La relation peut être sélectionnée comme serveurs communs ou Citrix ADC commun.



Rapports et mesures d'affichage d'instance

February 1, 2024

Les rapports et les métriques de la vue d'instance sont axés sur les instances Citrix ADC.

Pour accéder à la vue d'instance :

1. Accédez à **Analytics** > **HDX Insight** > **Instances**.

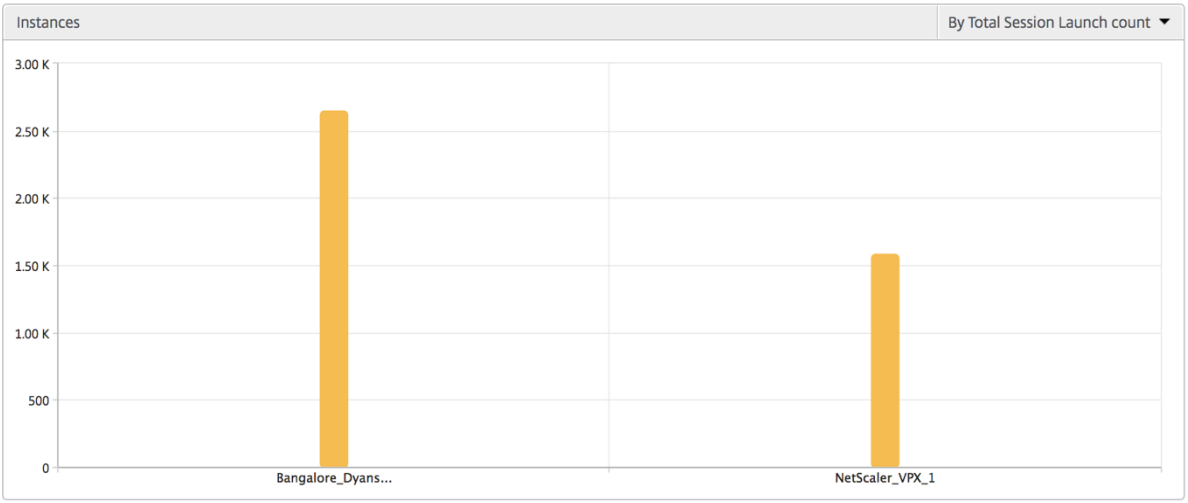
Vue récapitulative de l'instance

Cette vue est appelée vue récapitulative car elle affiche les rapports pour toutes les instances Citrix ADC qui sont ajoutées à Citrix ADM.

Toutes les métriques/rapports, sauf mention explicite, auront les valeurs qui leur correspondent pour la période sélectionnée.

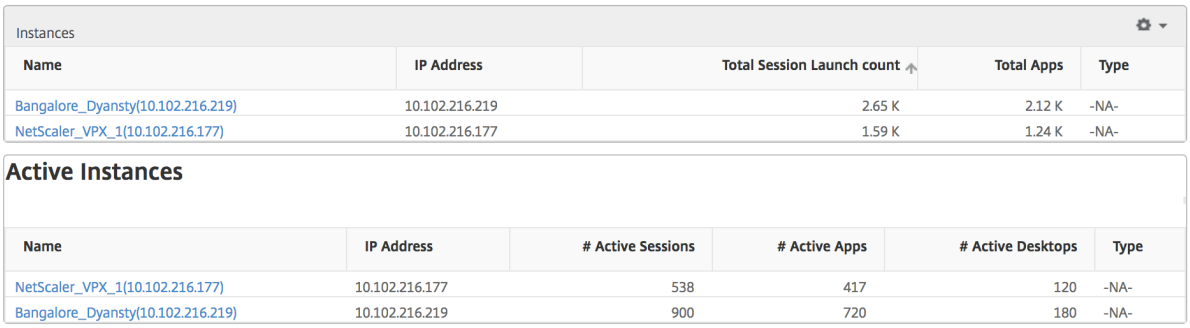
Graphique à barres d'instance

Ce graphique affiche l'instance par rapport au nombre total de lancement de session et au nombre total d'applications qui peuvent être sélectionnées dans la liste en haut à droite du canevas du graphique.



Rapport récapitulatif des instances et des instances actives

Métriques	Description
Nom	Nom d'hôte de l'instance Citrix ADC.
Adresse IP	Adresse IP NetScaler.
Nb total de sessions lancées	Nombre total de sessions utilisateur uniques créées au cours d'un intervalle de temps donné.
Nb total d'applis	Nombre total d'applications uniques lancées pendant un intervalle de temps donné.
Type	S/O



Instances

Name	IP Address	Total Session Launch count	Total Apps	Type
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	2.65 K	2.12 K	-NA-
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	1.59 K	1.24 K	-NA-

Active Instances

Name	IP Address	# Active Sessions	# Active Apps	# Active Desktops	Type
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	538	417	120	-NA-
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	900	720	180	-NA-

Rapport sur les seuils

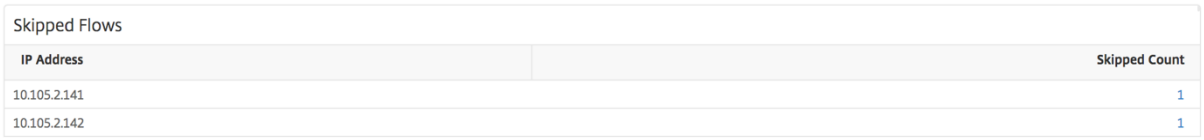
L'état des seuils représente le nombre de seuils dépassés lorsque l'*entité* est sélectionnée en tant qu'instance dans la période sélectionnée. Pour plus d'informations, consultez comment créer des

seuils et des alertes .

Flux ignorés

Un flux ignoré est un enregistrement qui a ignoré l'analyse de la connexion ICA. Cela peut se produire pour plusieurs raisons, telles que l'utilisation de versions non prises en charge de Citrix Virtual Apps and Desktops, d'une version non prise en charge du type Receiver ou Receiver, etc. Ce tableau indique l'adresse IP et le nombre de flux ignorés. Ces récepteurs peuvent ne pas faire partie des récepteurs de liste blanche. Par conséquent, ces sessions sont ignorées de la surveillance.

Voir **Erreur ! Référence de lien hypertexte non valide** pour plus de détails sur les problèmes liés à l'analyse ICA.


Skipped Flows

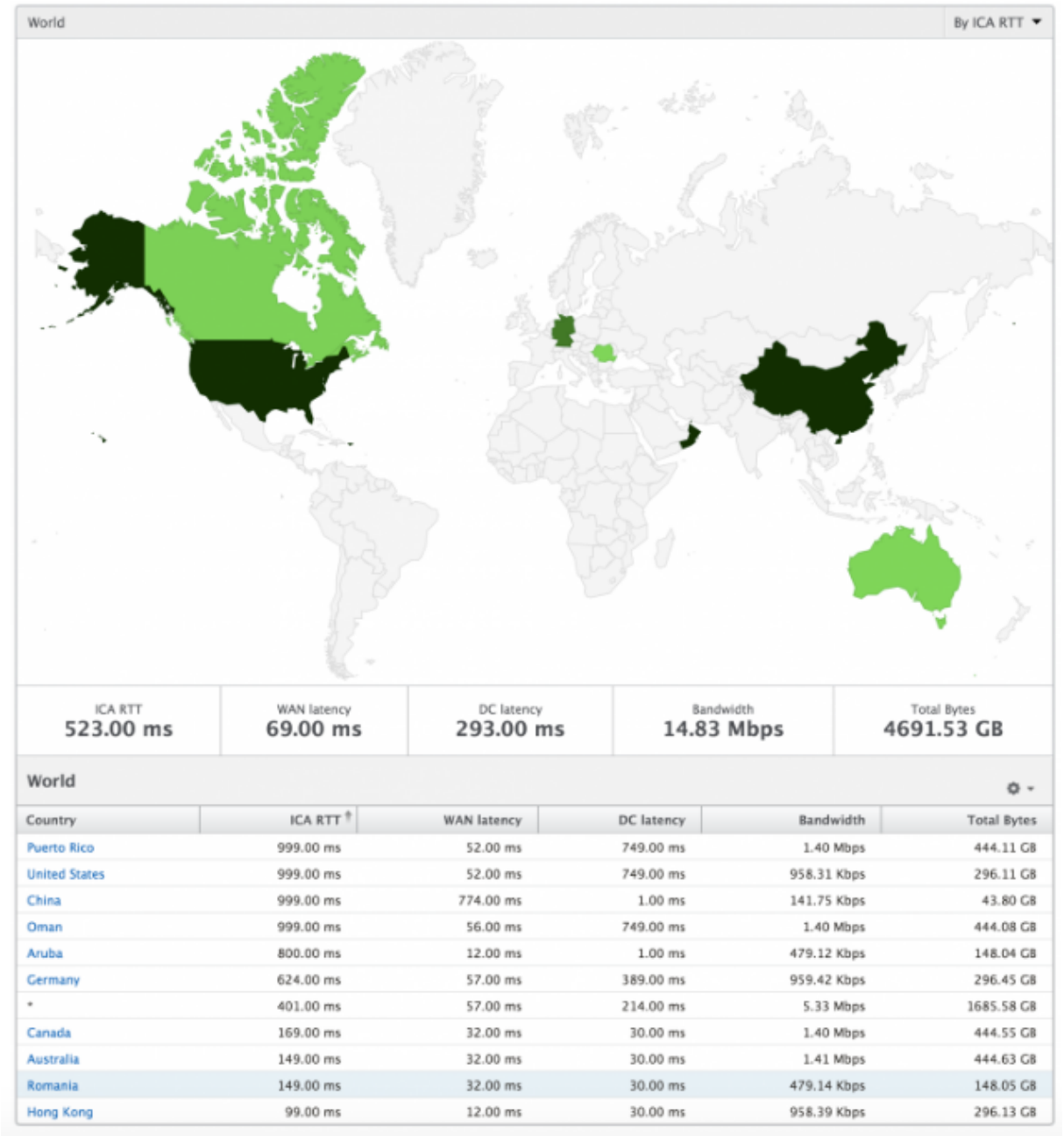
IP Address	Skipped Count
10.105.2.141	1
10.105.2.142	1

Vue du monde

La vue Carte du monde dans HDX insights permet aux administrateurs de visualiser les détails des utilisateurs historiques et actifs d'un point de vue géographique. Les administrateurs peuvent avoir une vue du monde du système, une exploration vers un pays particulier et plus loin dans les villes ainsi qu'en cliquant sur la région. Les administrateurs peuvent approfondir l'exploration vers le bas pour afficher les informations par ville et par État. À partir de Citrix ADC version 12.0 et ultérieure, vous pouvez effectuer une exploration vers le bas vers les utilisateurs connectés à partir d'un emplacement géographique.

Les détails suivants peuvent être consultés sur la carte du monde dans un aperçu HDX, et la densité de chaque mesure est affichée sous la forme d'une carte thermique :

- RTT ICA
- Latence WAN
- Latence DC
- Bande passante
- Nb total d'octets



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

Vue par instance

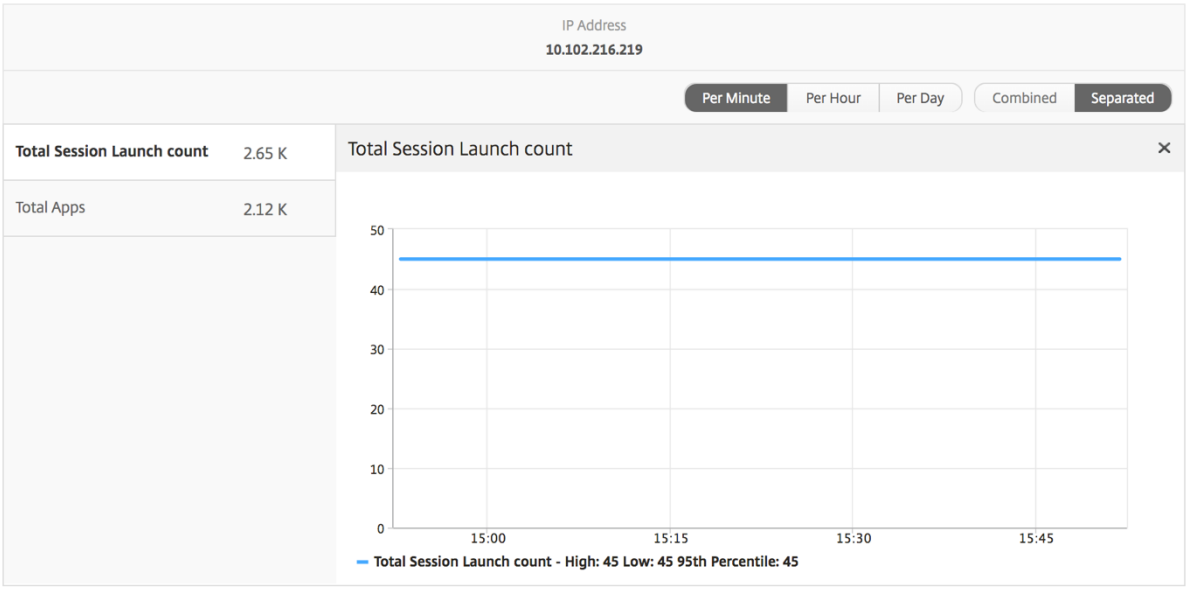
La vue par instance fournit des rapports détaillés sur l'expérience utilisateur final pour une instance Citrix ADC sélectionnée particulière.

Pour accéder à la vue d'instance :

1. Accédez à **Analytics** > **HDX Insight** > **Instances**.
2. Sélectionnez une instance particulière dans le **rapport de synthèse des instances**.

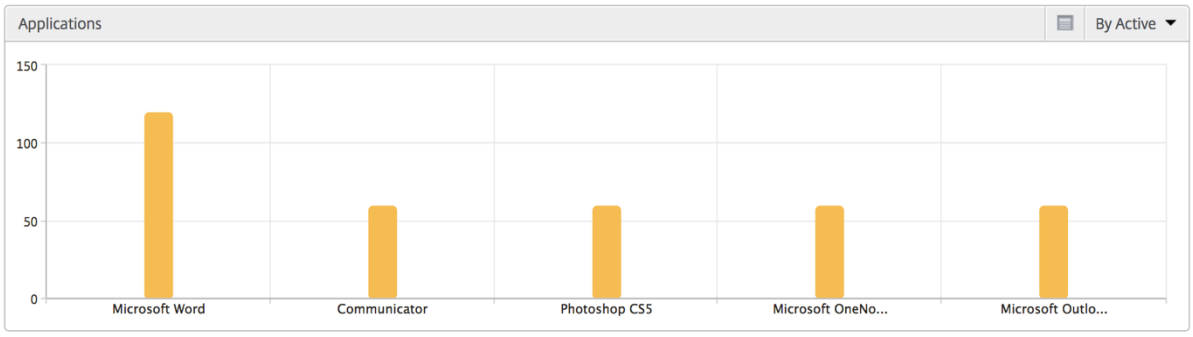
Graphique linéaire

Métriques	Description
Adresse IP	Cela représente l'adresse IP NetScaler de l'instance sélectionnée.
Nombre total de lancements de session	Nombre total de sessions Citrix Virtual App actives au cours de l'intervalle de temps donné.
Nb total d'applis	Nombre total d'applications uniques lancées pendant un intervalle de temps donné.



Graphique à barres des applications

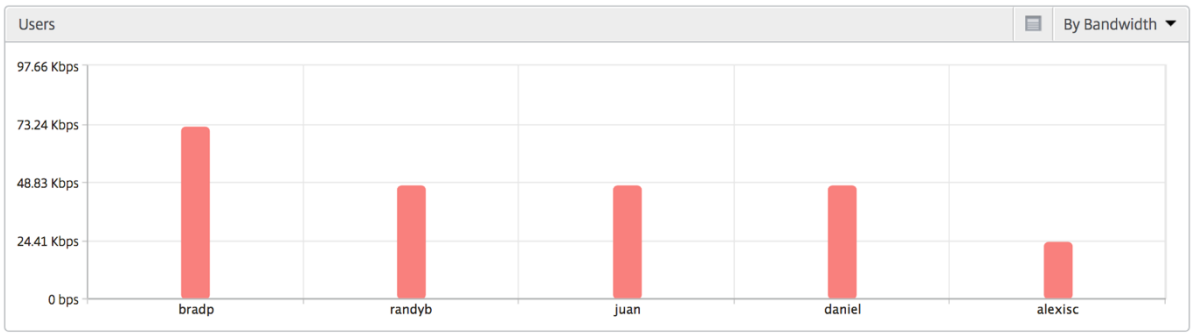
Affiche les 5 premières applications en fonction des critères suivants : applications actives, nombre total de lancements de session, nombre total de lancements d'applications ou durée de lancement.



Graphique à barres des utilisateurs

Le graphique à barres Utilisateurs affiche les 5 premiers utilisateurs selon les critères suivants

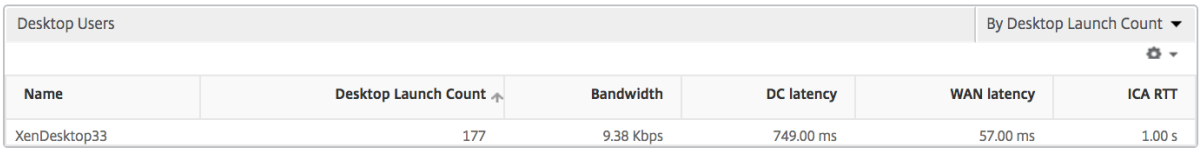
- Bande passante
- Latence WAN
- Latence DC
- RTT ICA



Rapport sur les utilisateurs du bureau

Ce tableau donne un aperçu des sessions Citrix Virtual Desktop pour un utilisateur particulier. Ces mesures peuvent être triées par nombre de lancements de postes de travail et bande passante.

Mesures	Description
Nom	Nom du bureau virtuel Citrix.
Nombre de lancements de bureaux	Nombre de fois que l'ordinateur de bureau a été lancé.
Bande passante	Nombre total d'octets par seconde pris pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de Citrix ADC aux serveurs back-end.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps ou Desktops respectivement.

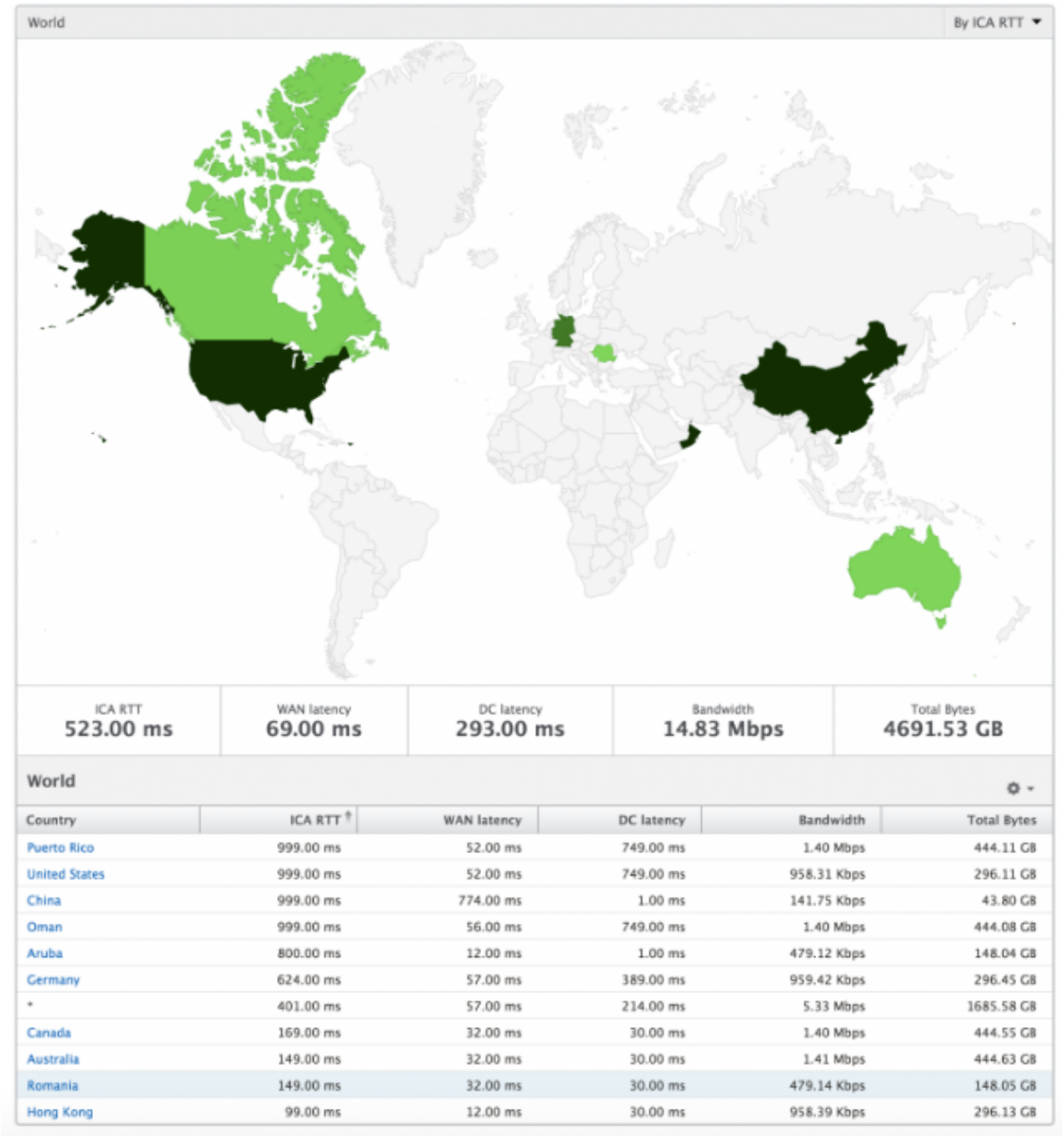


Vue du monde

La vue Carte du monde dans HDX insights permet aux administrateurs de visualiser les détails des utilisateurs historiques et actifs d'un point de vue géographique. Les administrateurs peuvent avoir une vue du monde du système, accéder à un pays particulier et plus loin dans les villes en cliquant sur la région. Les administrateurs peuvent approfondir l'exploration vers le bas pour afficher les informations par ville et par État. À partir de Citrix ADM version 12.0 et ultérieure, vous pouvez effectuer une exploration vers le bas vers les utilisateurs connectés à partir d'un emplacement géographique.

Les détails suivants peuvent être consultés sur la carte du monde dans un aperçu HDX, et la densité de chaque mesure est affichée sous la forme d'une carte thermique :

- RTT ICA
- Latence WAN
- Latence DC
- Bande passante
- Nb total d'octets



Rapports et mesures d'affichage des licences

February 1, 2024

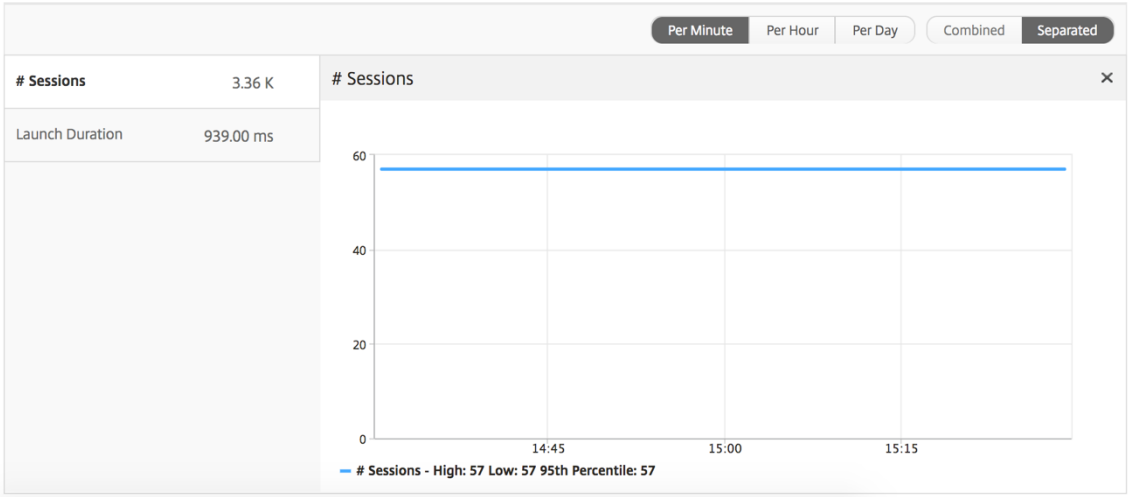
La vue de licence donne des détails sur les informations de licence Citrix Gateway.

Pour accéder à la vue des licences :

1. Accédez à **Analytics** > **HDX Insight** > **Licences** .

Graphique linéaire

Métriques	Description
Licences utilisées	Les licences CCU Citrix Gateway utilisées pendant la chronologie sélectionnée. Chaque nombre représente le nombre de sessions utilisateur. Cela est indépendant des sessions d'application et de bureau lancées par cet utilisateur.
Nombre total de licences	Nombre total de licences Citrix Gateway CCU disponibles pour le client.



Rapport sur les seuils

Le rapport de seuil représente le nombre de seuils dépassés lorsque l'*entité* est sélectionnée en tant que Licence au cours de la période sélectionnée. Pour plus d'informations, consultez comment créer des seuils et des alertes .

Résoudre les problèmes HDX Insight

February 1, 2024

Si la solution HDX Insight ne fonctionne pas comme prévu, le problème peut provenir de l'un des éléments suivants. Reportez-vous aux listes de contrôle dans les sections correspondantes pour le dépannage.

- Configuration de HDX Insight.
- Connectivité entre Citrix ADC et Citrix ADM.
- Génération d'enregistrements pour le trafic HDX/ICA dans Citrix ADC.
- Population des enregistrements dans Citrix ADM.

Liste de contrôle de configuration HDX Insight

- Assurez-vous que la fonctionnalité AppFlow est activée dans Citrix ADC. Pour plus de détails, consultez Activation d'AppFlow.
- Vérifiez la configuration HDX Insight dans la configuration en cours d'exécution de Citrix ADC.

  Exécutez la commande `show running | grep -i <appflow_policy>` pour vérifier la configuration HDX Insight. Assurez-vous que le type de liaison est ICA REQUEST. Par exemple ;

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
  ```

  Pour le mode transparent, le type de liaison doit être ICA_REQ_DEFAULT. Par exemple ;

  ```
  bind appflow global afp 100 END -type ICA_REQ_DEFAULT
  ```

- Pour le déploiement d'une passerelle d'accès ou d'un saut unique, assurez-vous que la stratégie HDX Insight AppFlow est liée au serveur virtuel VPN, où le trafic HDX/ICA circule.
- Pour le mode transparent ou le mode utilisateur LAN, assurez-vous que les ports ICA 1494 et 2598 sont définis.
- Vérifiez le paramètre `appflowlog` dans Citrix Gateway ou le serveur virtuel VPN est activé pour le déploiement Access Gateway ou à double saut. Pour plus de détails, consultez Activation d'AppFlow pour les serveurs virtuels.
- Cochez « Connection Chaining » est activé dans Citrix ADC double saut. Pour plus de détails, reportez-vous à la section Configuration des dispositifs Citrix Gateway pour exporter des données.
- Après le basculement HA si les détails HDX Insight sont analysés, cochez le paramètre ICA « enableSRonHAFailover » est activé. Pour plus de détails, consultez la section Fiabilité de session sur la paire haute disponibilité Citrix ADC.

Liste de contrôle de la connectivité entre Citrix ADC et Citrix ADM

- Vérifiez l'état du collecteur AppFlow dans Citrix ADC. Pour de plus amples informations, consultez Comment vérifier l'état de la connectivité entre Citrix ADC et AppFlow Collector.
- Vérifiez les hits de stratégie AppFlow HDX Insight.

  Exécutez la commande `show appflow policy <policy_name>` pour vérifier les succès de stratégie AppFlow.

  Vous pouvez également accéder à **Système > AppFlow > Stratégies** dans l'interface graphique pour vérifier les accès à la stratégie AppFlow.
- Validez tout pare-feu bloquant les ports AppFlow 4739 ou 5557.

Génération d'enregistrement pour le trafic HDX/ICA dans Citrix ADC

Exécutez la commande `tail -f /var/log/ns.log | grep -i "default ICA Message"` pour la validation du journal. En fonction des journaux générés, vous pouvez utiliser ces informations pour le dépannage.

- Journal : **connexion ICA d'analyse ignorée - HDX Insight non pris en charge pour cet hôte**

  Cause : Versions de Citrix Virtual Apps and Desktops non prises en charge

  Solution : mettez à niveau les serveurs Citrix Virtual Apps and Desktops vers une version prise en charge.
- Journal : **Type de client reçu 0x53, NON pris en charge**

  Cause : Version non prise en charge de Citrix Workspace

  Solution : mettez à niveau Citrix Workspace vers une version prise en charge. Pour plus d'informations, consultez l'application Citrix Workspace.
- Journal : **Erreur de Expand Packet - Ignorer tout le traitement hdx pour ce flux**

  Cause : problème de décompression du trafic ICA

  Solution : Aucun rapport n'est disponible pour cette session ICA tant qu'une nouvelle session n'est pas établie.
- Journal : **Transition non valide : NS_ICA_ST_FLOW_INIT/NS_ICA_EVT_INVALID -> NS_ICA_ST_UNINIT**

  Cause : problème lors de l'analyse de la poignée de main ICA

  Solution : Aucun rapport n'est disponible pour cette session ICA en particulier tant qu'une nouvelle session n'est pas établie.

- Log : **RTT EUEM ICA manquant**

  Cause : Impossible d'analyser les données de canal de surveillance de l'expérience utilisateur final

  Solution : Assurez-vous que le service de surveillance de l'expérience utilisateur final est démarré sur les serveurs Citrix Virtual Apps and Desktops. Assurez-vous que vous utilisez les versions prises en charge de l'application Citrix Workspace.

- Journal : **en-tête de canal non valide**

  Cause : Impossible d'identifier l'en-tête du canal

  Solution : Aucun rapport n'est disponible pour cette session ICA en particulier tant qu'une nouvelle session n'est pas établie.

- Log : **code d'évitement**

  Si vous voyez l'une des valeurs suivantes pour le code d'évitement, les détails Insight sont analysés.

  > Le code d'évitement 0 indique que l'enregistrement a été exporté avec succès depuis Citrix ADC.

Code d'évitement	Message d'erreur	Cause de l'erreur
100	NS_ICA_ERR_NULL_FRAG	Erreur lors de la gestion des fragments ICA, probablement en raison de conditions de mémoire
101	NS_ICA_ERR_INVALID_HS_CMD	Commande de prise de contact non valide reçue
102	NS_ICA_ERR_REDUC_PARAM_CNT	Paramètre non valide spécifié pour l'initialisation de l'expandeur V3
103	NS_ICA_ERR_REDUC_INIT	Impossible d'initialiser correctement le module d'extension V3
104	NS_ICA_ERR_REDUC_PARAM_BYTES	Nombre d'octets insuffisant pour affecter un codeur à un canal
105	NS_ICA_ERR_INVALID_CHANNEL	Numéro de canal ICA non valide
106	NS_ICA_ERR_INVALID_DECODER	Décodeur non valide spécifié pour un canal

Code d'évitement	Message d'erreur	Cause de l'erreur
107	NS_ICA_ERR_INVALID_TW_PARAM	Nombre de paramètres non valide spécifié sur le canal Thinwire
108	NS_ICA_ERR_INVALID_TW_DECODER	Décodeur non valide pour le canal Thinwire
109	NS_ICA_ERR_REDUC_NO_DECODER	Aucun décodeur défini pour le canal
110	NS_ICA_ERR_REDUC_V3_EXPANDER	Impossible d'étendre les données de canal
111	NS_ICA_ERR_REDUC_BYTES_V3_OOR	Erreur d'extension : Octets consommés plus que le nombre d'octets disponibles
112	NS_ICA_ERR_REDUC_BYTES_OOR	Erreur : dépassement de données non compressées
113	NS_ICA_ERR_REDUC_INVALID_CMD	Commande Undefined Expander
114	NS_ICA_ERR_CGP_FILL_HOLE	Erreur lors de la gestion des trames CGP séparées
115	NS_ICA_ERR_MEM_NSB_ALLOC	Erreur d'allocation de NSB — due à des conditions de mémoire insuffisantes
116	NS_ICA_ERR_MEM_REDUC_CTX_ALLOC	Erreur d'allocation de mémoire pour le contexte de l'extension
117	NS_ICA_ERR_ICA_OLD_SERVER	Ancien serveur, blocs de fonctionnalités non pris en charge
118	NS_ICA_ERR_PIR_MANY_FRAG	La requête Packet Init est fragmentée, impossible à traiter
119	NS_ICA_ERR_INIT_ICA_CAPS	Erreur d'initialisation de la capacité ICA
120	NS_ICA_ERR_NO_MSI_SUPPORT	L'hôte ne prend pas en charge la fonctionnalité MSI. Indique pour les versions de XenApp inférieures à 6.5 ou les versions de XenDesktop inférieures à 5.0
121	NS_ICA_ERR_CGP_INVALID_CMD	Commande CGP non valide détectée

Code d'évitement	Message d'erreur	Cause de l'erreur
122	NS_ICA_ERR_INSUFFICENT_CHANNEL_BYTES	Nombre d'octets insuffisant sur le canal
123	NS_ICA_ERR_CHANNEL_DATA	Données incorrectes sur le canal EUEM, CONTROL ou SEAMLESS
124	NS_ICA_ERR_INVALID_PURE_CMD	Commande non valide reçue lors du traitement de données de canal ICA pures
125	NS_ICA_ERR_INVALID_PURE_LEN1	Longueur non valide détectée lors du traitement de données de canal ICA pures
126	NS_ICA_ERR_INVALID_PURE_LEN	Longueur non valide détectée lors du traitement des données de canal PURE ICA
127	NS_ICA_ERR_INVALID_CLNT_DATA	Longueur de données non valide reçue du client
128	NS_ICA_ERR_MSI_GUID_SZ	Erreur dans la taille du GUID MSI
129	NS_ICA_ERR_INVALID_CHANNEL_HEADER	En-tête de canal incorrect détecté
130	NS_ICA_ERR_CGP_PARSE_RECONNECT	La récupération de la session reconnectée a échoué
131	NS_ICA_ERR_DISABLE_SR_NON_RECONNECT	Erreur lors de la désactivation de SR
132	NS_ICA_ERR_REDUC_NOT_V3	Version du réducteur ICA non prise en charge
133	NS_ICA_ERR_HS_COMPRESSION_DISABLED	Compression désactivée, non respectée par l'hôte
134	NS_ICA_ERR_IDENT_PROTO	Impossible d'identifier le protocole ICA ou CGP, vu avec des récepteurs incorrects
135	NS_ICA_ERR_INVALID_SIGNATURE	Signature ICA ou chaîne magique incorrecte
136	NS_ICA_ERR_PARSE_RAW	Erreur lors de l'analyse du paquet de négociation ICA
137	NS_ICA_ERR_INCOMPLETE_PKT	Paquet incomplet reçu lors de la négociation

Code d'évitement	Message d'erreur	Cause de l'erreur
138	NS_ICA_ERR_ICAFRAME_TOO_LARGE	La trame ICA est trop grande, dépasse 1460 octets
139	NS_ICA_ERR_FORWARD	Erreur lors du transfert des données ICA
140	NS_ICA_ERR_MAX_HOLES	Impossible de traiter la commande CGP car elle est divisée au-delà de la limite prise en charge
141	NS_ICA_ERR_ASSEMBLE_FRAME	Impossible de remonter correctement le cadre ICA
142	NS_ICA_ERR_UNSUPPORTED_RECEIVER_VERSION	Analyse ICA ignorée pour ce récepteur (client) car il n'est pas dans la liste d'autorisation
143	NS_ICA_ERR_LOOKUP_RECONNECT_ID	Impossible de détecter l'état d'analyse pour le cookie de reconnexion du client
144	NS_ICA_ERR_SYNCUP_RECONNECT_ID	Longueur de cookie de reconnexion non valide détectée après la reconnexion du client
145	NS_ICA_ERR_INVALID_RECONNECT_ID	Le cookie reconnecte le client a manqué la contrainte nécessaire
146	NS_ICA_ERR_INVALID_CLIENT_VERSION	Chaîne de version de récepteur non valide reçue du client
147	NS_ICA_ERR_UNKNOWN_CLIENT_PRODUCT_ID	Product_ID non valide reçu du client
148	NS_ICA_ERR_V3_HDR_CORRUPT_LEN	Longueur de canal non valide après l'extension
149	NS_ICA_ERR_SPECIAL_THINWIRE	Erreur de décompression
150	NS_ICA_ERR_SEAMLESS_INSUFFBYTE	Octets insuffisants rencontrés pour une commande transparente
151	NS_ICA_ERR_EUEM_INSUFFBYTE	Nombre d'octets insuffisant pour la commande EUEM

Code d'évitement	Message d'erreur	Cause de l'erreur
152	NS_ICA_ERR_SEAMLESS_INVALID_EVENT	Événement non valide pour l'analyse transparente des canaux
153	NS_ICA_ERR_CTRL_INVALID_EVENT	Événement non valide pour l'analyse du canal CTRL
154	NS_ICA_ERR_EUEM_INVALID_EVENT	Événement non valide pour l'analyse du canal EUEM
155	NS_ICA_ERR_USB_INVALID_EVENT	Événement non valide pour l'analyse du canal USB
156	NS_ICA_ERR_PURE_INVALID_EVENT	Événement non valide pour l'analyse de canal pure
157	NS_ICA_ERR_VCP_INVALID_EVENT	Événement non valide pour l'analyse des canaux virtuels
158	NS_ICA_ERR_ICAP_INVALID_EVENT	Événement non valide pour l'analyse des données ICA
159	NS_ICA_ERR_CGPP_INVALID_EVENT	Événement non valide pour l'analyse des données CGP
160	NS_ICA_ERR_BASICCRYPT_INVALIDSTATE	État non valide pour une commande crypt dans le chiffrement de base
161	NS_ICA_ERR_BASICCRYPT_INVALIDCRYPTCMD	Commande crypt non valide dans le chiffrement de base
162	NS_ICA_ERR_ADVCRYPT_INVALIDSTATE	État non valide pour une commande crypt dans le chiffrement RC5
163	NS_ICA_ERR_ADVCRYPT_INVALIDCRYPTCMD	Commande crypt non valide dans le chiffrement RC5
164	NS_ICA_ERR_ADVCRYPT_ENC	Erreur dans le chiffrement/déchiffrement RC5
165	NS_ICA_ERR_ADVCRYPT_DEC	Erreur dans le chiffrement/déchiffrement RC5
166	NS_ICA_ERR_SERVER_NOT_REDUCER_V3	Le serveur ne prend pas en charge Reducer version 3
167	NS_ICA_ERR_CLIENT_NOT_REDUCER_V3	Le client ne prend pas en charge Reducer version 3
168	NS_ICA_ERR_ICAP_INSUFFBYTE	Nombre d'octets inattendu dans la poignée de main ICA

Code d'évitement	Message d'erreur	Cause de l'erreur
169	NS_ICA_ERR_HIGHER_RECONSEQ	Numéro de séquence de reprise CGP plus élevé à partir des reconnexions de post homologues
170	NS_ICA_ERR_DESCSRINFO_ABSENT	Impossible de restaurer l'état d'analyse ICA après la reconnexion
171	NS_ICA_ERR_NSAP_PARSING	Erreur lors de l'analyse des données du canal Insight
172	NS_ICA_ERR_NSAP_APP	Erreur lors de l'analyse des détails de l'application à partir Insight données du canal
173	NS_ICA_ERR_NSAP_ACR	Erreur lors de l'analyse des détails ACR à partir des données du canal Insight
174	NS_ICA_ERR_NSAP_SESSION_END	Erreur lors de l'analyse des détails de fin de session à partir Insight données de canal
175	NS_ICA_ERR_NON_NSAP_SN	L'analyse ICA sur le nœud de service a été ignorée en raison de l'absence de prise en charge du canal Insight
176	NS_ICA_ERR_NON_NSAP_CLIENT	NSAP n'est pas pris en charge par le client
177	NS_ICA_ERR_NON_NSAP_SERVER	NSAP n'est pas pris en charge par le VDA
178	NS_ICA_ERR_NSAP_NEG_FAIL	Erreur lors de la négociation des données NSAP
179	NS_ICA_ERR_SN_RECONNECT_TKT_FETCH	Erreur lors de la récupération du service reconnecte le ticket dans le nœud de service
180	NS_ICA_ERR_SN_HIGHER_RECONSEQ	Erreur lors de la réception d'un numéro de séquence de reconnexion supérieur dans le nœud

Code d'évitement	Message d'erreur	Cause de l'erreur
181	NS_ICA_ERR_DISABLE_HDXINSIGHT_NONSAP	Erreur lors de la désactivation de HDX Insight pour les connexions non-NSAP

Exemples de journaux :

```
Jan 9 22:57:02 <local0.notice> 10.106.40.223 01/09/2020:22:57:02 GMT
 ns-223 0-PPE-2 : default ICA Message 1234 0 : "Session setup data
 send: Session GUID [57af35043e624abab409f5e6af7fd22c], Client IP/
Port [10.105.232.40/52314], Server IP/Port [10.106.40.215/2598], MSI
 Client Cookie [Non-MSI], Session setup time [01/09/2020:22:56:49
GMT], Client Type [0x0052], Receiver Version [19.12.0.23], User [
user1], Client [10.105.232.40], Server [WIN2K12-215], Ctx Flags [0
x8820220228], Track Flags [0x1775010c3fc], Skip Code [0]"
```

```
Jan 9 22:55:41 <local0.notice> 10.106.40.223 01/09/2020:22:55:41
GMT ns-223 0-PPE-0 : default ICA Message 156 0 : "Skipping ICA flow
: Session GUID [4e3a91175ebcbe686baf175eec7e0200], Client IP/Port
 [10.105.232.40/60059], Server IP/Port [10.106.40.219/2598], MSI
Client Cookie [Non-MSI], Session setup time [01/09/2020:22:55:39
GMT], Client Type [0x0052], Receiver Version [19.12.0.23], User [
user1], Client [10.105.232.40], Server [10.106.40.219], Ctx Flags [0
x8820220008], Track Flags [0x1600010c040], Skip Code [171]"
```

Compteurs d'erreurs

Différents compteurs sont capturés par analyse ICA. Le tableau suivant répertorie les différents compteurs pour l'analyse ICA.
Exécutez la commande `nsconmsg –g hdx –d statswt0`pour afficher les détails du compteur.

Nom du compteur HDX	Motif	Catégorie (Statistiques/Erreur/-Diagnostics)
hdx_tot_ica_conn	Indique le nombre total de connexions Pure ICA détectées par NS. Incrémenté chaque fois qu'une connexion ICA basée sur la signature ICA d'un PCB client est détectée.	Statistiques
hdx_tot_cgp_conn	Indique le nombre total de connexions CGP détectées par NS (Session Reliability ON). Incrémenté chaque fois qu'une connexion CGP basée sur la signature CGP d'un PCB client est détectée.	Statistiques
hdx_dbgsym tot_udt_conn	Indique le nombre total de connexions ICA UDP détectées par NS	Statistiques
hdx_dbgsym tot_nsap_conn	Indique le nombre total de connexions prises en charge par NSAP détectées par NS	Statistiques
hdx_tot_skip_conn	Indique le nombre de connexions ICA qui ont été ignorées par l'analyseur en raison d'une signature ICA ou CGP non valide.	Statistiques
hdx_dbgsym active_conn	Nombre total de connexions EDT/CGP/ICA actives à cet instant.	Statistiques
hdx_dbgsym active_nsap_conn	Nombre total de connexions EDT/CGP/ICA NSAP actives à cet instant.	Statistiques
hdx_dbgsym skip_appflow_disabled	Nombre total d'instances où AppFlow a été détaché d'une session en raison de la désactivation d'AppFlow	Statistiques/Diagnostics
hdx_dbgsym transparent_user	Nombre total d'accès utilisateur transparents	Statistiques/Diagnostics

Nom du compteur HDX	Motif	Catégorie (Statistiques/Erreur/-Diagnostics)
hdx_bg_ag_user	Nombre total d'accès utilisateur Access Gateway	Statistiques/Diagnostics
hdx_bg_lan_user	Nombre total d'accès en mode utilisateur LAN	Statistiques/Diagnostics
hdx_basic_enc	Indique le nombre de connexions ICA utilisant le chiffrement de base	Statistiques/Diagnostics
hdx_advanced_enc	Indique le nombre de connexions ICA utilisant le chiffrement avancé basé sur RC5	Statistiques/Diagnostics
dx_dbg_wanscaler_on_clientside	Nombre total de connexions CGP/ICA avec Citrix SD-WAN côté client	Statistiques/Diagnostics
hdx_dbg_wanscaler_on_serverside	Nombre total de connexions CGP/ICA avec Citrix SD-WAN côté serveur	Statistiques/Diagnostics
hdx_dbg_reconnected_session	Nombre total de demandes de reconnexion du client sans erreur Citrix ADC	Statistiques/Diagnostics
hdx_dbg_host_rejected_ns_reconnect	Nombre total d'hôtes rejetés demandes de reconnexion par client	Statistiques/Diagnostics
hdx_euem_available	Indique le nombre de connexions pour lesquelles le canal de surveillance de l'expérience utilisateur final est disponible. Le canal de surveillance de l'expérience utilisateur final est nécessaire pour collecter des statistiques telles que ICA RTT.	Statistiques/Diagnostics
hdx_err_disabled_sr	La fiabilité de session est désactivée à l'aide du bouton `nsapimgr`.La session ne fonctionne pas pour cette session.	Erreur

Nom du compteur HDX	Motif	Catégorie (Statistiques/Erreur/-Diagnostics)
hdx_err_skip_no_msi	La fonctionnalité MSI du serveur XA/XD est absente. Cela indique une ancienne version du serveur, HDX Insight ignore cette connexion.	Error
hdx_err_skip_old_server	Ancienne version de serveur non prise en charge	Erreur
hdx_err_clnt_not_whitelist	Le récepteur client n'est pas dans la liste d'autorisation, HDX Insight ignore cette connexion	Erreur
hdx_sm_ica_cam_channel_disabled	Nombre total de NS_ICA_CAM_CHANNEL désactivés via la stratégie SmartAccess	Diagnostics
hdx_sm_ica_usb_channel_disabled	Nombre total de NS_ICA_USB_CHANNEL désactivés via la stratégie SmartAccess	Diagnostics
hdx_sm_ica_clip_channel_disabled	Nombre total de NS_ICA_CLIP_CHANNEL désactivés via la stratégie SmartAccess	Diagnostics
hdx_sm_ica_ccm_channel_disabled	Nombre total de NS_ICA_CCM_CHANNEL désactivés via la stratégie SmartAccess	Diagnostics
hdx_sm_ica_cdm_channel_disabled	Nombre total de NS_ICA_CDM_CHANNEL désactivés via la stratégie SmartAccess	Diagnostics
hdx_sm_ica_com1_channel_disabled	Nombre total de NS_ICA_COM1_CHANNEL désactivés via la stratégie SmartAccess	Diagnostics

Nom du compteur HDX	Motif	Catégorie (Statistiques/Erreur/-Diagnostics)
hdx_sm_ica_com2_channel_disabled	Nombre total de NS_ICA_COM2_CHANNEL désactivés via la stratégie SmartAccess	Diagnostics
hdx_sm_ica_cpm_channel_disabled	Nombre total de NS_ICA_CPM_CHANNEL désactivés via la stratégie SmartAccess	Diagnostics
hdx_sm_ica_lpt1_channel_disabled	Nombre total de NS_ICA_LPT1_CHANNEL désactivés via la stratégie SmartAccess	Diagnostics
hdx_sm_ica_lpt2_channel_disabled	Nombre total de NS_ICA_LPT2_CHANNEL désactivés via la stratégie SmartAccess	Diagnostics
dx_dbgsym sm_ica_msi_disabled	Nombre total de cas où MSI est désactivé via la stratégie SmartAccess	Diagnostics
hdx_sm_ica_file_channel_disabled	Le nombre total de NS_ICA_FILE_CHANNEL est désactivé via la stratégie SmartAccess	Diagnostics
hdx_db_usb_accept_device	Nombre total de périphériques USB acceptés	Diagnostics
hdx_dbgsym usb_reject_device	Nombre total de périphériques USB rejetés	Diagnostics
hdx_dbgsym usb_reset_endpoint	Nombre total de points de terminaison USB réinitialisés	Diagnostics
hdx_dbgsym usb_reset_device	Nombre total de périphériques USB réinitialisés	Diagnostics
hdx_db_usb_stop_device	Nombre total de périphériques USB arrêtés	Diagnostics
hdx_dbgsym usb_stop_device_response	Nombre total de réponses provenant de périphériques USB arrêtés	Diagnostics

Nom du compteur HDX	Motif	Catégorie (Statistiques/Erreur/-Diagnostics)
hdx_db_usb_device_gone	Nombre total de périphériques USB disparus	Diagnostics
hdx_dbg_usb_device_stopped	Nombre total de périphériques USB arrêtés	Diagnostics

nstrace validation

Vérifiez le protocole CFLOW pour voir tous les enregistrements AppFlow sortant de Citrix ADC.

Population d'enregistrements dans Citrix ADM liste de contrôle

- Exécutez la commande `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: ica_"` et vérifiez les journaux pour confirmer que Citrix ADM reçoit des enregistrements AppFlow.
- Confirmez que l'instance Citrix ADC est ajoutée à Citrix ADM.
- Validez que le serveur virtuel Citrix Gateway/VPN est sous licence Citrix ADM.
- Assurez-vous que le réglage des paramètres multi-sauts est activé pour le double saut.
- Assurez-vous que Citrix Gateway est autorisé pour le deuxième saut dans le déploiement à double saut.

Avant de contacter le support technique Citrix

Pour une résolution rapide, assurez-vous de disposer des informations suivantes avant de contacter le support technique Citrix :

- Détails du déploiement et de la topologie du réseau.
- Versions de Citrix ADC et de Citrix ADM.
- Versions du serveur Citrix Virtual Apps and Desktops.
- Versions de Client Receiver
- Nombre de sessions ICA actives lorsque le problème s'est produit.
- Bundle de support technique capturé en exécutant la commande `show techsupport` à l'invite de commande Citrix ADC.
- Pack de support technique capturé pour Citrix ADM.

- Traces de paquets capturées sur tous les Citrix ADC.
  Pour démarrer une trace de paquets, tapez, `start nstrace -size 0'`
  Pour arrêter une trace de paquets, tapez, `stop nstrace`
- Collectez les entrées de la table ARP du système en exécutant la commande `show arp`.

Problèmes connus

Reportez-vous aux notes de publication de Citrix ADC pour connaître les problèmes connus sur HDX Insight.

Gateway Insight

February 1, 2024

Dans un déploiement Citrix Gateway, la visibilité des détails d'accès d'un utilisateur est essentielle pour résoudre les problèmes d'échec d'accès. En tant qu'administrateur réseau, vous souhaitez savoir quand un utilisateur n'est pas en mesure de se connecter à Citrix Gateway, ainsi que connaître l'activité de l'utilisateur et les raisons de l'échec de connexion. Ces informations ne sont généralement pas disponibles sauf si l'utilisateur envoie une demande de résolution.

Gateway Insight offre une visibilité sur les défaillances rencontrées par tous les utilisateurs, quel que soit le mode d'accès, au moment de la connexion à Citrix Gateway. Vous pouvez consulter la liste de tous les utilisateurs disponibles, le nombre d'utilisateurs actifs, le nombre de sessions actives, ainsi que les octets et les licences utilisés par tous les utilisateurs à tout moment. Vous pouvez consulter l'analyse des points de terminaison (EPA), l'authentification, l'authentification unique (SSO) et les échecs de lancement d'applications pour un utilisateur. Vous pouvez également consulter les détails des sessions actives et interrompues d'un utilisateur.

Gateway Insight fournit également une visibilité sur les raisons de l'échec du lancement d'applications pour les applications virtuelles. Cela améliore votre capacité à résoudre tout type de problème d'échec de connexion ou de lancement d'application. Vous pouvez afficher le nombre d'applications lancées, le nombre de sessions totales et actives, le nombre total d'octets et la bande passante consommée par les applications. Vous pouvez afficher les détails des utilisateurs, des sessions, de la bande passante et des erreurs de lancement d'une application.

Vous pouvez consulter le nombre de passerelles, le nombre de sessions actives, le nombre total d'octets et la bande passante utilisés par toutes les passerelles associées à une appliance Citrix Gateway à tout moment. Vous pouvez afficher les échecs de l'EPA, de l'authentification, de l'authentification unique et du lancement d'application pour une Gateway. Vous pouvez également afficher les détails de tous les utilisateurs associés à une Gateway et leur activité d'ouverture de session.

Tous les messages du journal sont stockés dans la base de données Citrix ADM, afin que vous puissiez consulter les détails des erreurs pour n'importe quelle période. Vous pouvez également afficher un résumé des échecs d'ouverture de session et déterminer à quel stade du processus d'ouverture de session un échec s'est produit.

Points à noter

- Gateway Insight est pris en charge sur les déploiements suivants :
  - Access Gateway
  - Unified Gateway
- La version et la version de Citrix ADM doivent être identiques ou ultérieures à celles de l'appliance Citrix Gateway.
- Une heure de rapports Gateway Insight peut être affichée pour les instances Citrix ADC dotées d'une licence avancée. Une licence Premium est un must afficher les rapports Gateway Insight au-delà d'une heure.

Limitations

- Citrix Gateway ne prend pas en charge Gateway Insight lorsque la méthode d'authentification est configurée en tant qu'authentification basée sur un certificat.
- Pour les rapports Gateway Insight, les informations de géolocalisation ne sont pas fournies par l'appliance Citrix ADC.
- Les connexions utilisateur réussies, la latence et les détails au niveau de l'application pour les applications et les bureaux ICA virtuels sont visibles uniquement sur le tableau de bord des utilisateurs HDX Insight.
- En mode double saut, la visibilité des défaillances sur l'appliance Citrix Gateway dans la deuxième zone démilitarisée n'est pas disponible.
- Les problèmes d'accès au bureau RDP (Remote Desktop Protocol) ne sont pas signalés.
- Gateway Insight est pris en charge pour les types d'authentification suivants. Si un autre type d'authentification est utilisé, vous pouvez constater certaines incohérences dans Gateway Insight.
  - Stockage local
  - LDAP
  - RADIUS
  - TACACS

- SAML
- OTP natif

Activer Gateway Insight

Pour activer Gateway Insight pour votre appliance Citrix Gateway, vous devez d'abord ajouter l'appliance Citrix Gateway à Citrix ADM. Vous devez ensuite activer AppFlow pour le serveur virtuel représentant l'application VPN. Pour plus d'informations sur l'ajout d'un appareil à Citrix ADM, consultez la section Ajout d'appareils.

> **Remarque**
>
> Pour afficher les échecs d'analyse du point de terminaison (EPA) dans Citrix ADM, vous devez activer l'authentification, l'autorisation et l'audit AppFlow dans la journalisation du nom d'utilisateur sur l'appliance Citrix Gateway.

La procédure suivante pour activer l'aperçu de la Gateway s'applique si votre Citrix ADM est **13.0 Build 36.27** :

1. Accédez à **Réseaux** >**Instances**et sélectionnez l'instance pour laquelle vous souhaitez activer AppFlow.
2. Dans la liste **Sélectionner une action**, sélectionnez **Configurer Analytics**.
3. Dans la page **Configurer Insight**, sous **Configurer Analytics**, sélectionnez **Citrix Gateway**.
4. Sélectionnez le serveur virtuel, puis cliquez sur **Activer AppFlow**.
5. Dans l'écran **Activer AppFlow**, dans la liste **Sélectionner une expression**, cliquez sur true.
6. En regard de **Mode transport**, activez la case à cocher **Logstream** .

   > **Remarque**
   >
   > Vous pouvez choisir **IPFIX** ou **Logstream** comme mode de transport.
   >
   > Pour plus d'informations sur **IPFIX** et **Logstream**, voir Présentation de **Logstream**.

7. Cliquez sur **OK**.

Pour Citrix ADM version 13.0 Build 41.x ou ultérieure

1. Accédez à **Réseaux** > **Instances**, puis sélectionnez l'instance.
2. Dans la liste **Sélectionner une action**, sélectionnez **Configurer Analytics**.
3. Sélectionnez le serveur virtuel et cliquez sur **Activer les analyses**.

4. Sous **Options avancées** :
    a) Sélectionner **Logstream**
    b) Sélectionnez **Citrix Gateway**
5. Cliquez sur **OK**.

Activer l'authentification AppFlow, l'autorisation et l'audit de la journalisation des noms d'utilisateur sur une appliance Citrix Gateway à l'aide de l'interface graphique

1. Accédez à **Configuration > Système > AppFlow > Paramètres**, puis cliquez sur **Modifier les paramètres AppFlow**.
2. Dans l'écran **Configurer les paramètres d'AppFlow**, sélectionnez **Nom d'utilisateur AAA**, puis cliquez sur **OK.**

Affichage des rapports Gateway Insight

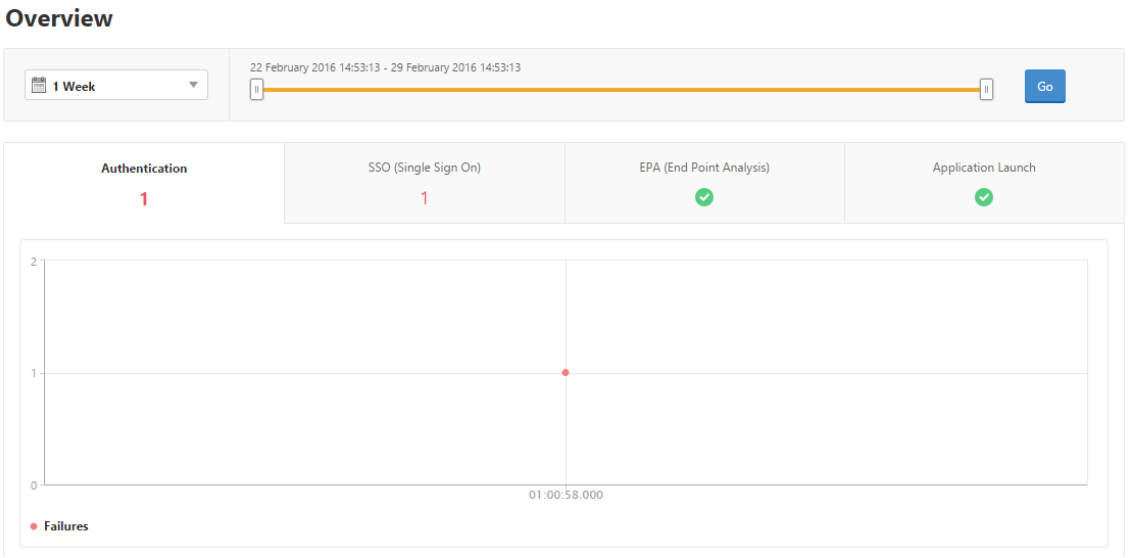
Dans Citrix ADM, vous pouvez consulter les rapports de tous les utilisateurs, applications et passerelles associés aux appliances Citrix Gateway, ainsi que les détails d'un utilisateur, d'une application ou d'une passerelle en particulier. Dans la section **Présentation**, vous pouvez afficher les échecs de l'EPA, de l'authentification unique, de l'authentification et du lancement d'application. Vous pouvez également afficher un résumé des différents modes de session utilisés par les utilisateurs pour ouvrir une session, des types de clients et du nombre d'utilisateurs connectés chaque heure.

> **Remarque**
>
> Lorsque vous créez un groupe, vous pouvez affecter des rôles au groupe, fournir un accès au niveau de l'application au groupe et affecter des utilisateurs au groupe. Citrix ADM Analytics prend désormais en charge l'autorisation basée sur l'adresse IP virtuelle. Vos utilisateurs peuvent désormais voir des rapports pour tous les Insights uniquement pour les applications (serveurs virtuels) pour lesquelles ils sont autorisés. Pour plus d'informations sur les groupes et l'affectation d'utilisateurs au groupe, consultez Configurer des groupes.

Pour afficher les échecs d'EPA, d'authentification unique, d'authentification, d'autorisation et de lancement d'application

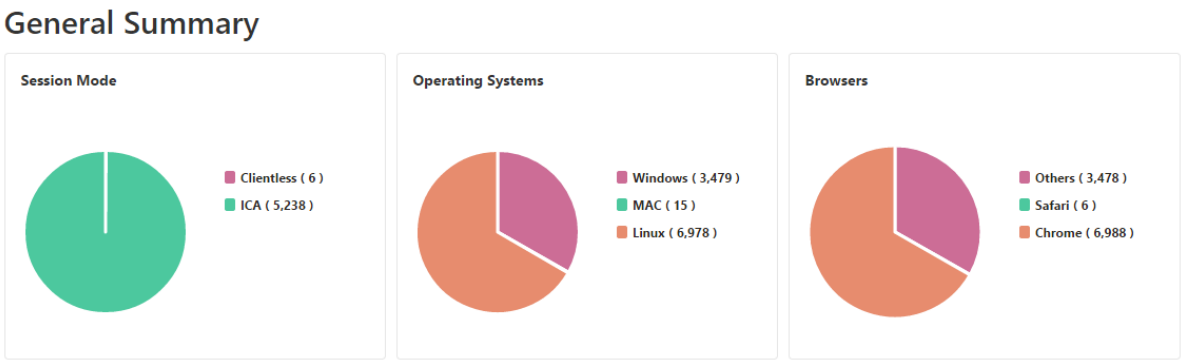
1. Dans Citrix ADM, accédez à **Analytics > Gateway Insight**.
2. Sélectionnez la période pour laquelle vous souhaitez afficher les détails de l'utilisateur. Vous pouvez utiliser le curseur temporel pour personnaliser davantage la période sélectionnée. Cliquez sur **Go**.

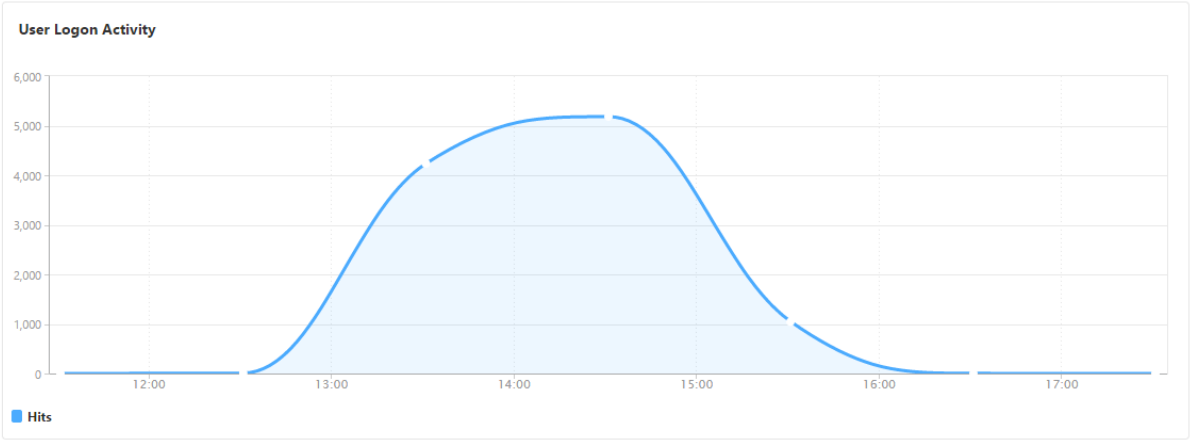
3. Cliquez sur les onglets EPA (End Point Analysis), Authentification, Autorisation, SSO (Single Sign On) ou Lancement d'application pour afficher les détails de l'échec.



Pour afficher un résumé des modes de session, des clients et du nombre d'utilisateurs

Dans Citrix ADM, accédez à **Analytics > Gateway Insight**, faites défiler vers le bas pour afficher les rapports.





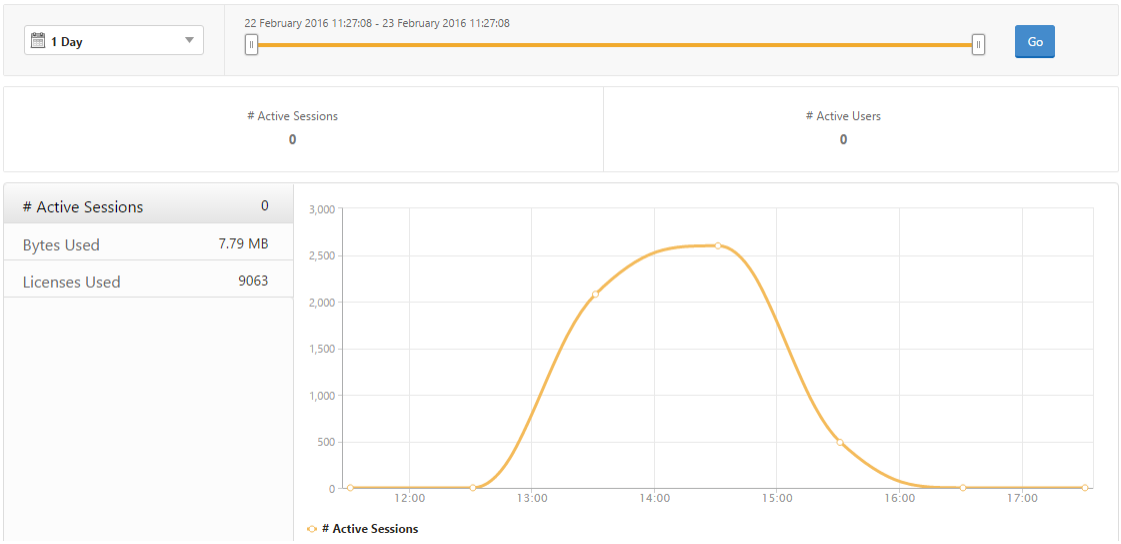
Affichage des rapports Gateway Insight pour les utilisateurs

Vous pouvez consulter les rapports relatifs aux éléments suivants :

- Tous les utilisateurs associés aux appliances Citrix Gateway.
- Échec de lancement de l'EPA, de l'authentification, de l'authentification unique et de l'application pour un utilisateur.
- Détails des sessions actives et terminées pour un utilisateur.
- Les types de modes de session tels que Tunnel complet, VPN sans client et proxy ICA.

Pour afficher les détails de l'utilisateur

1. Dans Citrix ADM, accédez à **Analytics > Gateway Insight > Utilisateurs**.
2. Sélectionnez la période pour laquelle vous souhaitez afficher les détails de l'utilisateur. Vous pouvez utiliser le curseur temporel pour personnaliser davantage la période sélectionnée. Cliquez sur **Go**.
3. Vous pouvez afficher le nombre d'utilisateurs actifs, le nombre de sessions actives, d'octets et de licences utilisés par tous les utilisateurs au cours de la période.

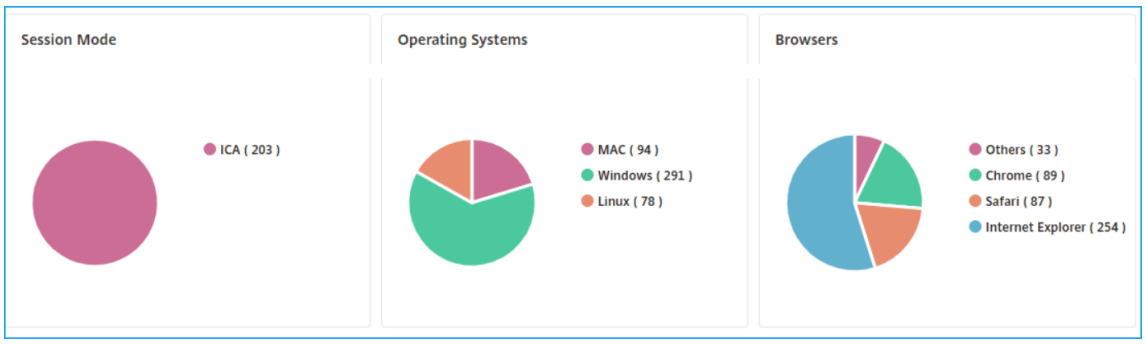


Faites défiler vers le bas pour afficher la liste des utilisateurs disponibles et des utilisateurs actifs.

User Name	Total Bytes	# Sessions Used
user1	191.94 KB	11
user10	0	4
user100	2.81 KB	4
user1000	42.66 KB	5
user1001	2.11 KB	4
user1002	4.22 KB	4
user1003	4.22 KB	4

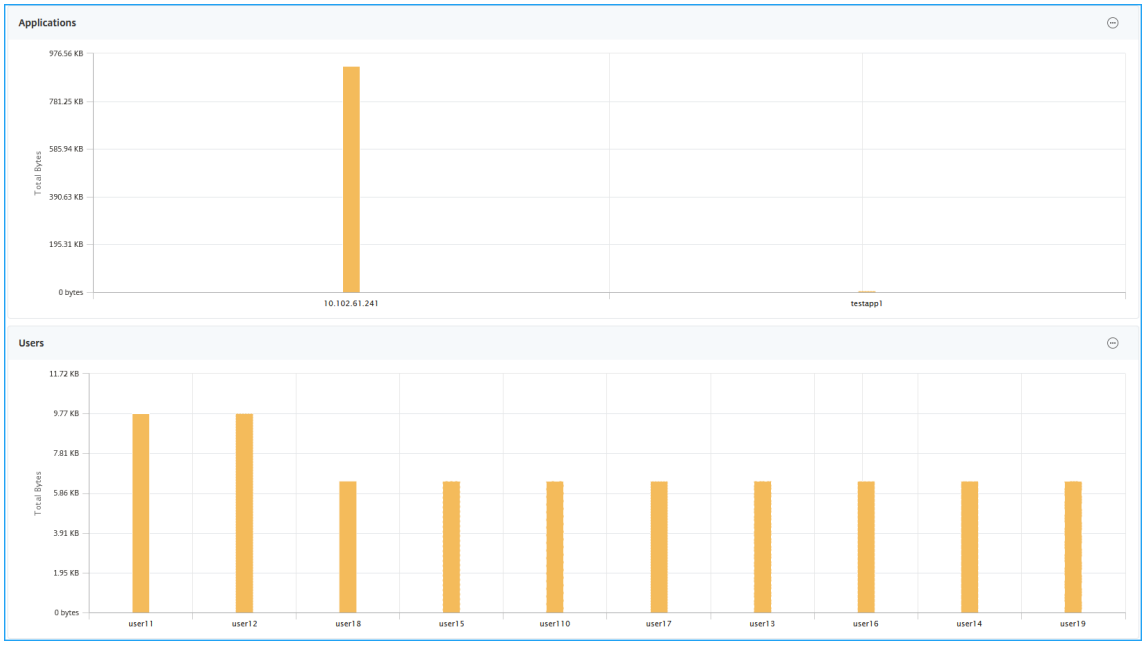
Sous l'onglet **Utilisateurs** ou **Utilisateurs actifs**, cliquez sur un utilisateur pour afficher les détails de l'utilisateur suivants :

- **Détails de l'utilisateur** - Vous pouvez afficher des informations pour chaque utilisateur associé aux appliances de passerelle ADC. Accédez à **Analytics** > **Gateway Insight** > **Utilisateurs** et cliquez sur un utilisateur pour afficher les informations relatives à l'utilisateur sélectionné, comme le mode session, le système d'exploitation et les navigateurs.

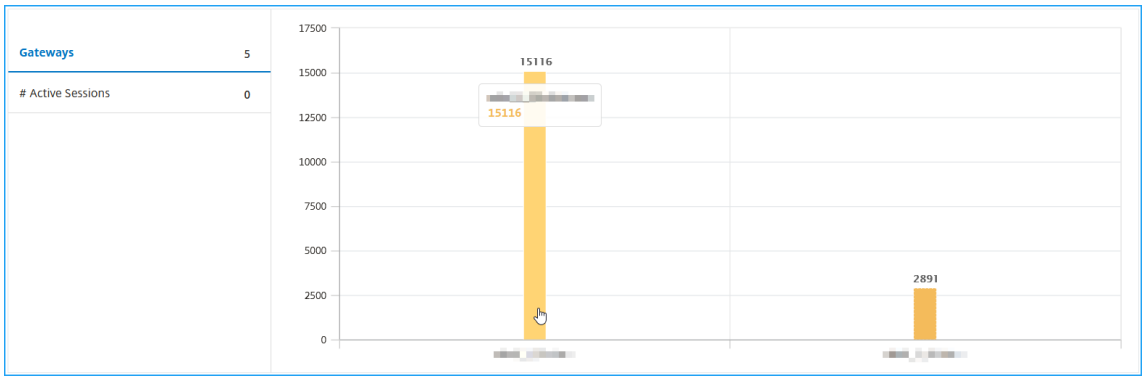


- **Utilisateurs et applications pour la passerelle sélectionnée** - Accédez à **Analytics** > **Gate-**

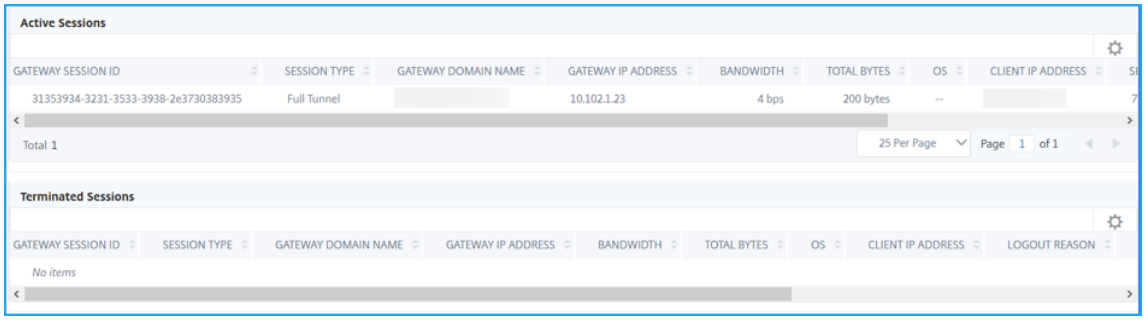
way Insight > **Gateway** et cliquez sur un nom de domaine de passerelle pour afficher les 10 principales applications et les 10 principaux utilisateurs associés à la passerelle sélectionnée.



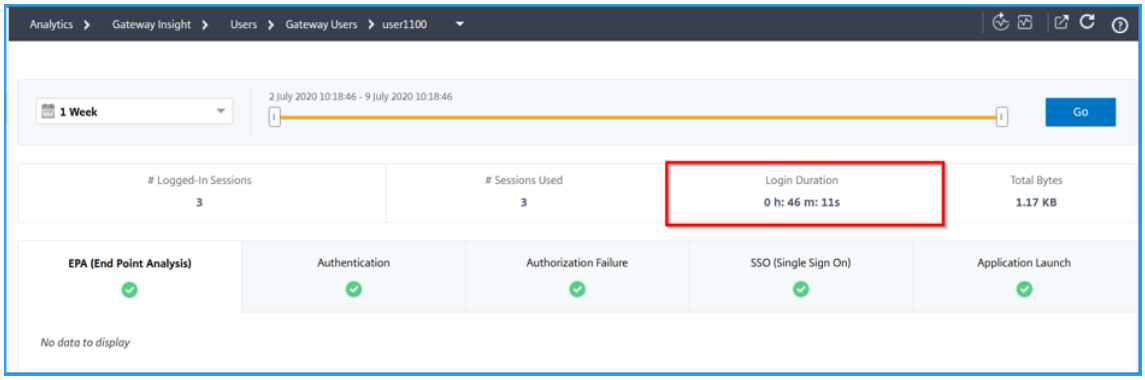
- **Afficher plus d'option pour les applications et les utilisateurs** : pour plus de 10 applications et utilisateurs, vous pouvez cliquer sur l'icône Plus dans Applications et utilisateurs pour afficher tous les détails des utilisateurs et applications associés à la passerelle sélectionnée.
- **Afficher les détails en cliquant sur le graphique à barres** —Lorsque vous cliquez sur un graphique à barres, vous pouvez afficher les détails pertinents. Par exemple, accédez à **Analytics > Gateway Insight > Gateway** et cliquez sur le graphique à barres de passerelle pour afficher les détails de la passerelle.



- L'utilisateur **Sessions actives et Sessionsterminées**.



- Le nom de domaine de la passerelle et l'adresse IP de la passerelle dans les **sessions actives**.
- Durée de connexion de l'utilisateur.



- Raison de la session de déconnexion de l'utilisateur. Les raisons de déconnexion peuvent être :
  - Session expirée
  - Déconnecté en raison d'une erreur interne
  - Déconnecté en raison de la session inactive expiré
  - L'utilisateur s'est déconnecté
  - L'administrateur a arrêté la session

Affichage des rapports Gateway Insight pour les applications

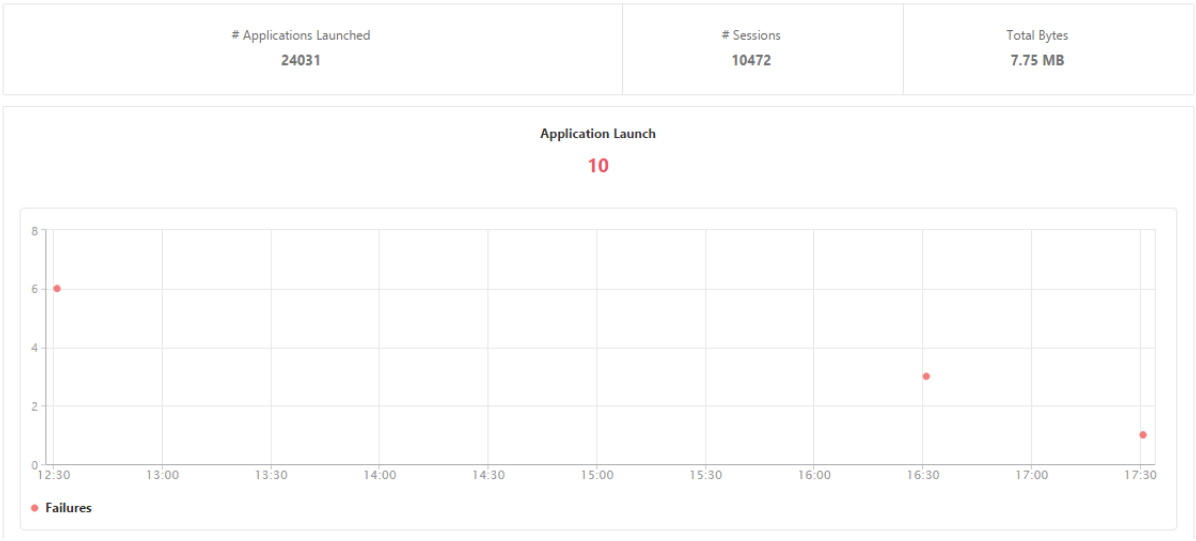
Vous pouvez afficher le nombre d'applications lancées, le nombre de sessions totales et actives, le nombre total d'octets et la bande passante consommés par les applications. Vous pouvez afficher les détails des utilisateurs, des sessions, de la bande passante et des erreurs de lancement d'une application.

Pour afficher les détails de l'application

1. Dans Citrix ADM, accédez à **Analytics > Gateway Insight > Applications**.

2. Sélectionnez la période pour laquelle vous souhaitez afficher les détails de l'application. Vous pouvez utiliser le curseur temporel pour personnaliser davantage la période sélectionnée. Cliquez sur **Go**.

Vous pouvez désormais afficher le nombre d'applications lancées, le nombre de sessions totales et actives, le nombre total d'octets et la bande passante consommés par les applications.



Faites défiler vers le bas pour afficher le nombre de sessions, la bande passante et le nombre total d'octets consommés par ICA et d'autres applications.

Name	# Sessions	Bandwidth	Total Bytes
10.102.61.249	3972	52 bps	3.79 MB
c.go-mpulse.net	2	0 bps	1.53 KB
cdn.kendostatic.com	1	0 bps	805
code.jquery.com	1	0 bps	1.51 KB
engtools.citrite.net	2	0 bps	160
onebug.citrite.net	2	1 bps	86.21 KB

Sous l'onglet **Autres applications**, vous pouvez cliquer sur une application dans la colonne **Nom** pour afficher les détails de cette application.

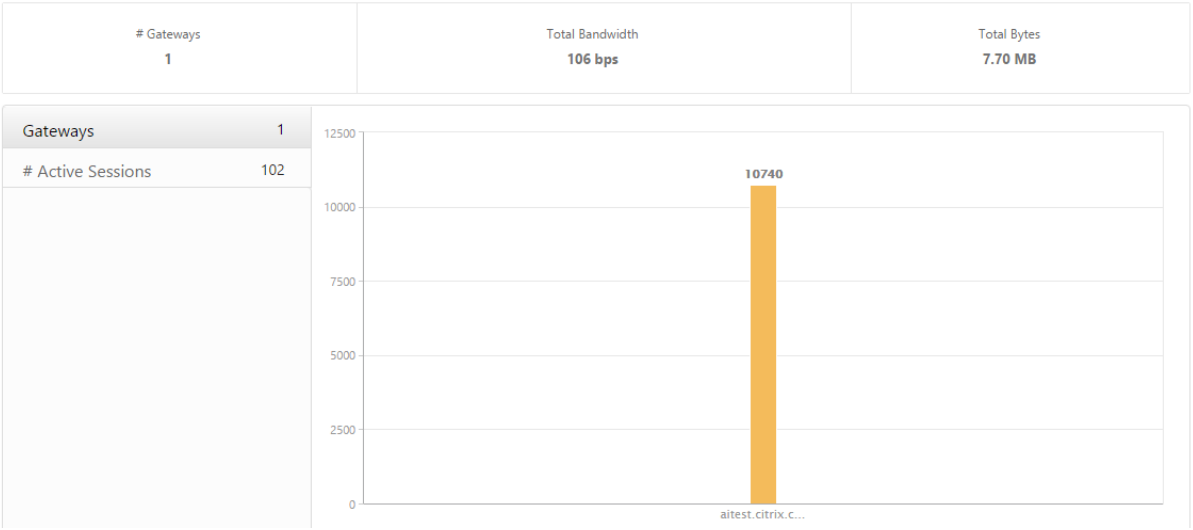
Affichage des rapports Gateway Insight pour les passerelles

Vous pouvez consulter le nombre de passerelles, le nombre de sessions actives, le nombre total d'octets et la bande passante utilisés par toutes les passerelles associées à une appliance Citrix Gateway à tout moment. Vous pouvez afficher les échecs de l'EPA, de l'authentification, de l'authentification unique et du lancement d'application pour une Gateway. Vous pouvez également afficher les détails de tous les utilisateurs associés à une Gateway et leur activité d'ouverture de session.

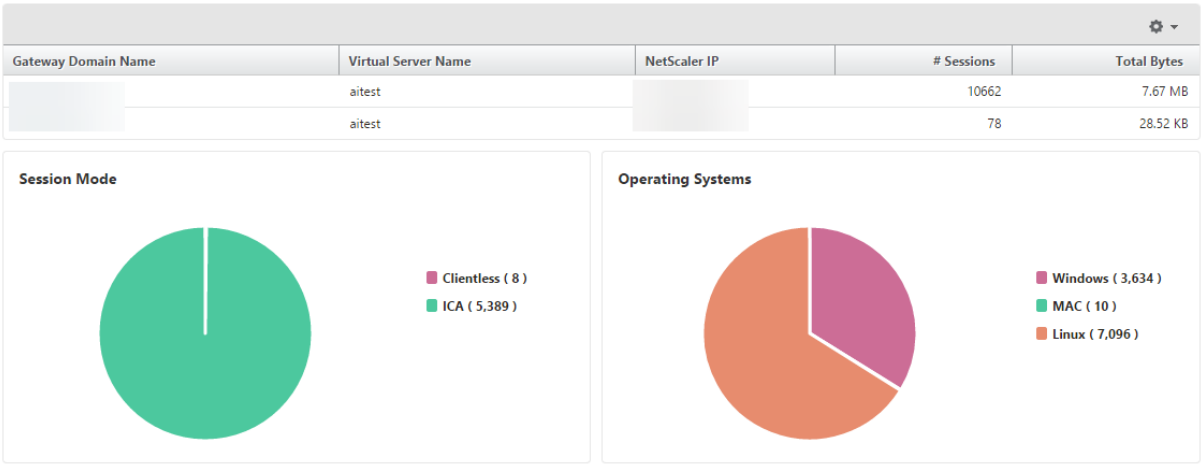
Pour afficher les détails de la Gateway

1. Dans **Citrix ADM**, accédez à **Analytics > Gateway Insight > Passerelles**.
2. Sélectionnez la période pour laquelle vous souhaitez afficher les détails de la Gateway. Vous pouvez utiliser le curseur temporel pour personnaliser davantage la période sélectionnée. Cliquez sur **Go**.

Vous pouvez désormais afficher à tout moment le nombre de passerelles, le nombre de sessions actives, le nombre total d'octets et la bande passante utilisés par toutes les passerelles associées à une appliance Citrix Gateway.



Faites défiler vers le bas pour afficher les détails de la Gateway tels que le nom de domaine de la passerelle, le nom du serveur virtuel, l'adresse IP NetScaler, les modes de session et le nombre total d'octets.



Vous pouvez cliquer sur une Gateway dans la colonne **Nom de domaine de la Gateway** pour afficher les échecs de l'EPA, de l'authentification, de l'authentification unique et du lancement d'application,

ainsi que d'autres détails pour une passerelle.

Exportation de rapports

Vous pouvez enregistrer les rapports Gateway Insight avec tous les détails affichés dans l'interface graphique au format PDF, JPEG, PNG ou CSV sur votre ordinateur local. Vous pouvez également planifier l'exportation des rapports vers des adresses e-mail spécifiées à différents intervalles.

> **Remarque**
>
> - Les utilisateurs disposant d'un accès en lecture seule ne peuvent pas exporter de rapports.
> - Les rapports de carte géographique sont exportés uniquement si Citrix ADM dispose d'une connexion Internet.

Pour exporter un rapport

1. Dans l'onglet **Tableau de bord**, dans le volet droit, cliquez sur le bouton **d'exportation** .
2. Sous **Exporter maintenant**, sélectionnez le format requis, puis cliquez sur **Exporter**.

Pour planifier l'exportation :

1. Dans l'onglet **Tableau de bord**, dans le volet droit, cliquez sur le bouton **d'exportation** .
2. Sous **Planifier l'exportation**, spécifiez les détails et cliquez sur **Planifier**.

Pour ajouter un serveur de messagerie ou une liste de distribution de messagerie :

1. Dans l'onglet **Configuration**, accédez à **Système** > **Notifications** > **E-mail**.
2. Dans le volet droit, sélectionnez **Serveur de messagerie**pour ajouter un serveur de messagerie ou sélectionnez Liste de **distribution de messagerie pour créer une liste** de distribution de messagerie.
3. Spécifiez les détails et cliquez sur **Créer**.

Pour exporter l'intégralité du tableau de bord Gateway Insight :

1. Dans l'onglet **Tableau de bord**, dans le volet droit, cliquez sur le bouton **d'exportation** .
2. Sous **Exporter maintenant**, sélectionnez Format **PDF**, puis cliquez sur **Exporter**.

Cas d'utilisation de Gateway Insight

Les cas d'utilisation suivants montrent comment utiliser Gateway Insight pour gagner en visibilité sur les détails d'accès, les applications et les passerelles des utilisateurs sur les dispositifs Citrix Gateway.

Un utilisateur ne peut pas se connecter à l'appliance Citrix Gateway ou aux serveurs Web internes

En tant qu'administrateur Citrix Gateway, vous surveillez les appliances Citrix Gateway via Citrix ADM et vous souhaitez savoir pourquoi un utilisateur ne parvient pas à se connecter ou à quel stade du processus de connexion l'échec s'est produit.

Citrix ADM vous permet d'afficher les détails des erreurs de connexion de l'utilisateur aux étapes suivantes du processus de connexion :

- Authentification
- Analyse des points finaux (EPA)
- Single Sign-On

Dans Citrix ADM, vous pouvez rechercher un utilisateur en particulier, puis afficher tous les détails de cet utilisateur.

Pour rechercher un utilisateur :

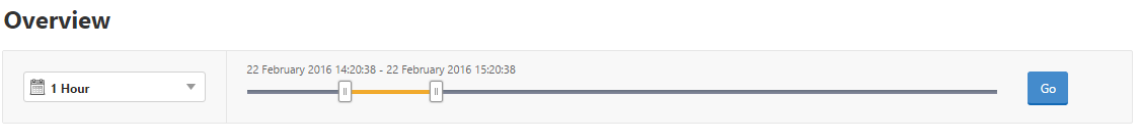
Dans Citrix ADM, accédez à **Analytics > Gateway Insight** et, dans la zone de texte **Search for Users**, spécifiez l'utilisateur que vous souhaitez rechercher.

Échec de l'authentification

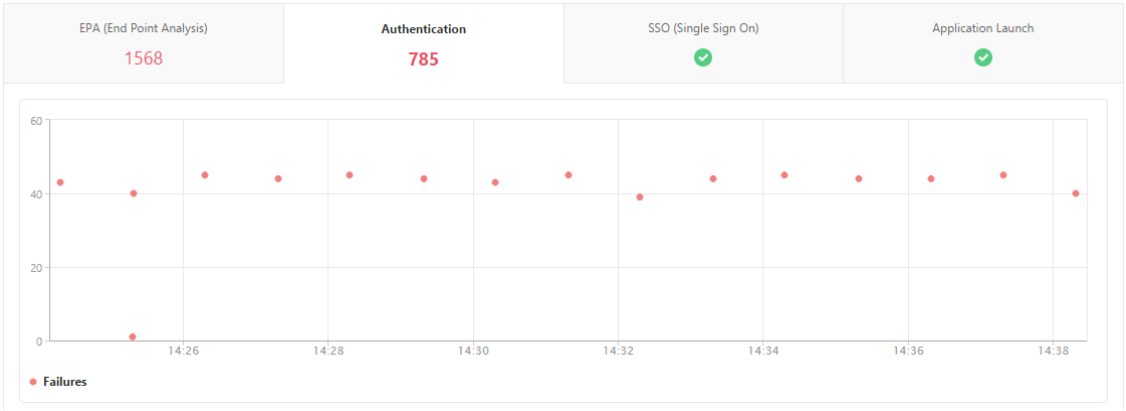
Vous pouvez afficher les erreurs d'authentification telles que les informations d'identification incorrectes ou l'absence de réponse du serveur d'authentification. Vous pouvez également voir le facteur à l'origine de l'échec de l'authentification.

Pour afficher les détails de l'échec d'authentification :

1. Dans Citrix ADM, accédez à **Analytics > Gateway Insight**.
2. Dans la section **Vue d'ensemble**, sélectionnez la période pour laquelle vous souhaitez afficher les erreurs d'authentification. Vous pouvez utiliser le curseur temporel pour personnaliser davantage la période sélectionnée. Cliquez sur **Go**.



3. Cliquez sur l'onglet **Authentification** . Vous pouvez consulter le nombre d'erreurs d'authentification à tout moment dans le graphique **des échecs** .



Faites défiler la page vers le bas pour afficher les détails de chaque erreur d'authentification, **tels que Nom d'utilisateur, Adresse IP du client, Heure de l'erreur, Type d'authentification, Adresse IP du serveur**d'authentification, etc., à partir du tableau du même onglet. La colonne **Description de l'erreur** du tableau indique la raison de l'échec de connexion et la colonne **État** indique le nième facteur à l'origine de l'échec.

IP ADDRESS	VPN	CS VIRTUAL SERVER	ERROR TIME	ERROR DESCRIPTION	ERROR COUNT	STATE	AUTHEN
183	vpnvserver		15/03/2019, 06:30:04	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Server timed out	4	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Server timed out	3	2nd Factor	RADIUS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	1	2nd Factor	RADIUS
111	vpnvip		19/03/2019, 06:30:04	Bad(format) password passed to nsaaad	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	3	1st Factor	LDAP
183	vpnvserver		13/04/2019, 06:30:28	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Account is disabled	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	Local
183	vpnvserver		12/04/2019, 06:30:13	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Bad(format) password passed to nsaaad	5	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	4	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	4	1st Factor	RADIUS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	22	1st Factor	RADIUS
88	_XD_10.217.205.88_443		15/03/2019, 06:30:04	Bad(format) password passed to nsaaad	1	1st Factor	LDAP

Vous pouvez cliquer sur un utilisateur dans la colonne **Nom d'utilisateur** pour afficher les erreurs d'authentification et d'autres détails pour cet utilisateur. Vous pouvez personnaliser le tableau pour ajouter ou supprimer des colonnes à l'aide de l'icône des paramètres.

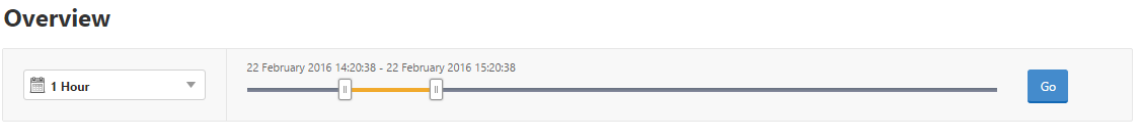
Échec de l'EPA

Vous pouvez afficher les échecs de l'EPA au stade de la pré-authentification ou de la post-authentification.

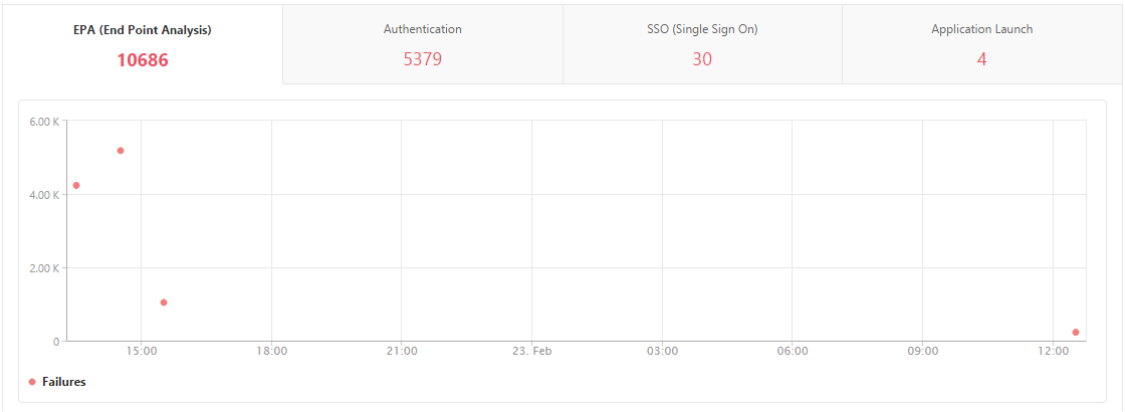
> **Important :**
>
> - Les défaillances EPA ne sont signalées que lorsque des expressions classiques sont configurées.
> - Les échecs EPA ne sont pas signalés si l'expression avancée est configurée dans la stratégie de pré-authentification ou de post-authentification.
> - Les défaillances EPA ne sont pas signalées si l'EPA est configuré comme l'un des facteurs d'un flux d'authentification nFactor.

Pour afficher les détails des échecs EPA :

1. Dans Citrix ADM, accédez à **Analytics > Gateway Insight**.
2. Dans la section Vue d'ensemble, sélectionnez la période pour laquelle vous souhaitez afficher les erreurs EPA. Vous pouvez utiliser le curseur temporel pour personnaliser davantage la période sélectionnée. Cliquez sur **Go**.



3. Cliquez sur l'onglet **EPA (End Point Analysis)**. Vous pouvez afficher le nombre d'erreurs EPA à tout moment dans le graphique **Failures**.



Faites défiler la page vers le bas pour afficher les détails de chaque erreur EPA, tels que le **nom d'utilisateur, l'adresse IP NetScaler, l'adresse IP de la passerelle, le VPN, l'heure d'erreur, le nom de la stratégie, le nom de domaine de passerelle,** etc., dans le tableau du même onglet. La colonne **Description de l'erreur** du tableau affiche la raison de l'échec EPA et la colonne **Nom de la stratégie** affiche la stratégie qui a entraîné l'échec.

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	Policy Name	EPA Method	Gateway Domain Name
user1097	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1098	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1491	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1633	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 3:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user17	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1774	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user197	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com

Vous pouvez cliquer sur un utilisateur dans la colonne **Nom d'utilisateur** pour afficher les erreurs EPA et d'autres détails pour cet utilisateur. Vous pouvez personnaliser le tableau pour ajouter ou supprimer des colonnes à l'aide de la flèche vers le bas.

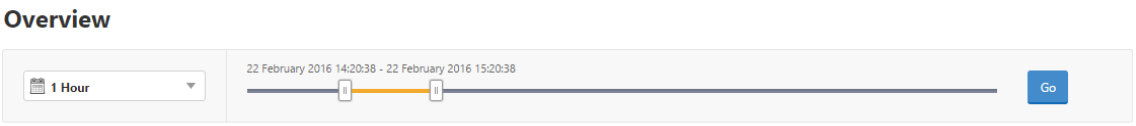
> **Remarque**
>
> Citrix Gateway ne signale pas les échecs EPA lorsque l'expression « ClientSecurity » est configurée en tant que règle de stratégie de session VPN.

Défaillances SSO

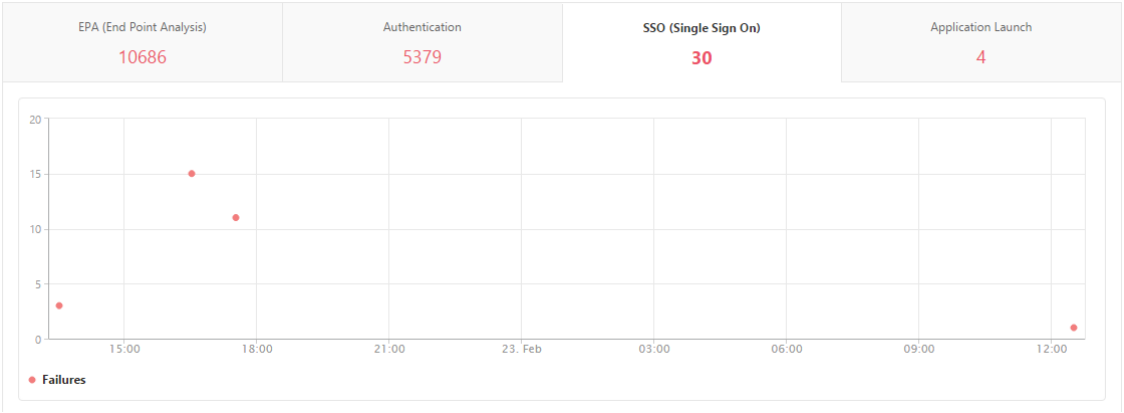
Vous pouvez consulter tous les échecs SSO à tout moment pour un utilisateur accédant à n'importe quelle application via l'appliance Citrix Gateway.

Pour afficher les détails des défaillances SSO :

1. Dans Citrix ADM, accédez à **Analytics > Gateway Insight**.
2. Dans la section Vue d'ensemble, sélectionnez la période pour laquelle vous souhaitez afficher les erreurs d'SSO. Vous pouvez utiliser le curseur temporel pour personnaliser davantage la période sélectionnée. Cliquez sur **Go**.



3. Cliquez sur l'onglet **SSO (Single Sign On)**. Vous pouvez afficher le nombre d'erreurs SSO à tout moment dans le graphique Failures.



Faites défiler vers le bas pour afficher les détails de chaque erreur d'authentification seule (**nom d'utilisateur, adresse IP NetScaler, heure d'erreur, description de l'erreur, nom de la ressource,** etc.) dans le tableau du même onglet.

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	SSO Method	Gateway Domain Name
user11	10.102.61.201	10.102.61.210	10.144.2.35	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 5:30:54 PM	Single Sign ON failed	11	NTLM	aitest.citrix.com
user5	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/23/2016, 12:30:54 PM	Single Sign ON failed	1	Basic	aitest.citrix.com
user31	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user23	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 4:30:54 PM	Single Sign ON failed	15	NTLM	aitest.citrix.com

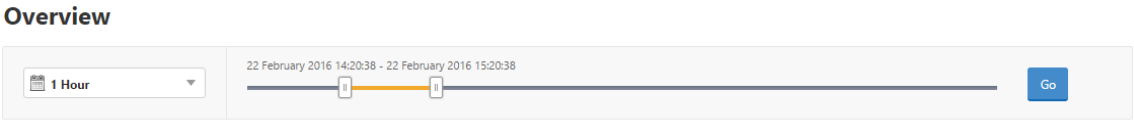
Vous pouvez cliquer sur un utilisateur dans la colonne **Nom d'utilisateur** pour afficher les erreurs SSO et d'autres détails pour cet utilisateur. Vous pouvez personnaliser le tableau pour ajouter ou supprimer des colonnes à l'aide de la flèche vers le bas.

Après une connexion réussie à Citrix Gateway, un utilisateur n'est pas en mesure de lancer une application virtuelle

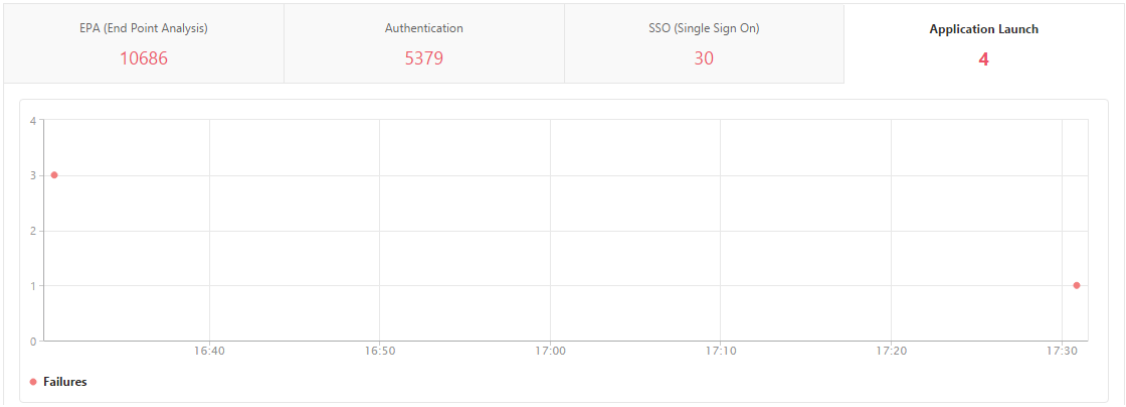
En cas d'échec de lancement de l'application, vous pouvez obtenir une visibilité sur les raisons, telles que le serveur STA (Secure Ticket Authority) inaccessible ou le serveur Citrix Virtual App, ou le ticket STA non valide. Vous pouvez afficher l'heure à laquelle l'erreur s'est produite, les détails de l'erreur et la ressource pour laquelle la validation STA a échoué.

Pour afficher les détails de l'échec de lancement de l'application :

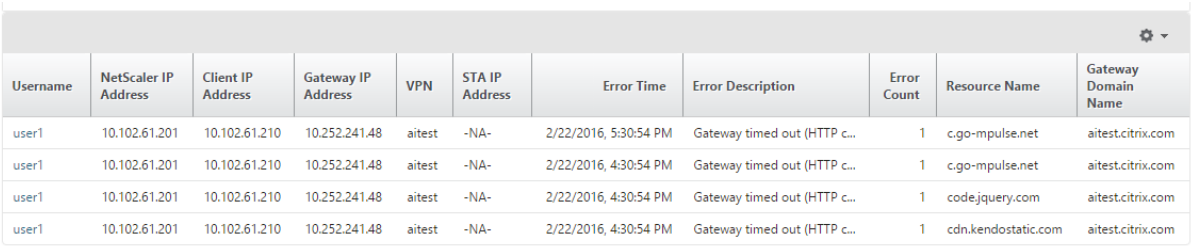
1. Dans Citrix ADM, accédez à **Analytics > Gateway Insight**.
2. Dans la section **Vue d'ensemble**, sélectionnez la période pour laquelle vous souhaitez afficher les erreurs d'SSO. Vous pouvez utiliser le curseur temporel pour personnaliser davantage la période sélectionnée. Cliquez sur **Go**.



3. Cliquez sur l'onglet **Lancement de l'application**. Vous pouvez afficher le nombre d'échecs de lancement d'application à tout moment dans le graphique **Échec**.



Faites défiler vers le bas pour afficher les détails de chaque erreur de lancement d'application, telles que l'**adresse IP NetScaler, le temps d'erreur, la description de l'erreur, le nom de ressource, le nom de domaine de la passerelle**, etc., dans le tableau du même onglet. La colonne **Description de l'erreur** du tableau affiche l'adresse IP du serveur STA et la colonne **Nom de la ressource** affiche les détails de la ressource pour laquelle la validation STA a échoué.



Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	STA IP Address	Error Time	Error Description	Error Count	Resource Name	Gateway Domain Name
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 5:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	code.jquery.com	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	cdn.kendostatic.com	aitest.citrix.com

Vous pouvez cliquer sur un utilisateur dans la colonne **Nom d'utilisateur** pour afficher les erreurs de lancement de l'application et d'autres détails pour cet utilisateur. Vous pouvez personnaliser le tableau pour ajouter ou supprimer des colonnes à l'aide de la flèche vers le bas.

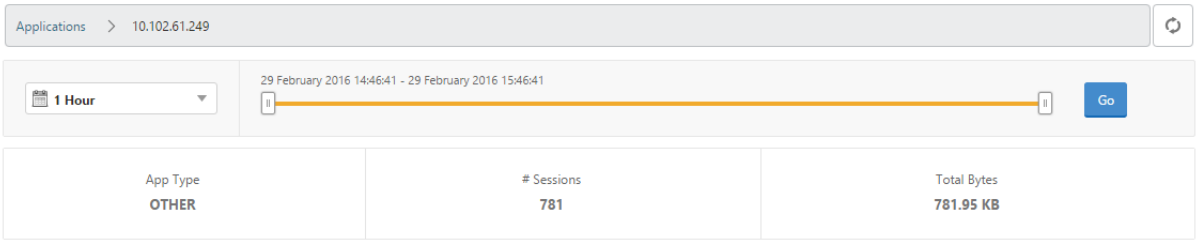
Après avoir lancé une nouvelle application avec succès, un utilisateur souhaite afficher le nombre total d'octets et de bande passante consommés par cette application

Une fois que vous avez lancé une nouvelle application avec succès, dans Citrix ADM, vous pouvez afficher le total des octets et de la bande passante consommés par cette application.

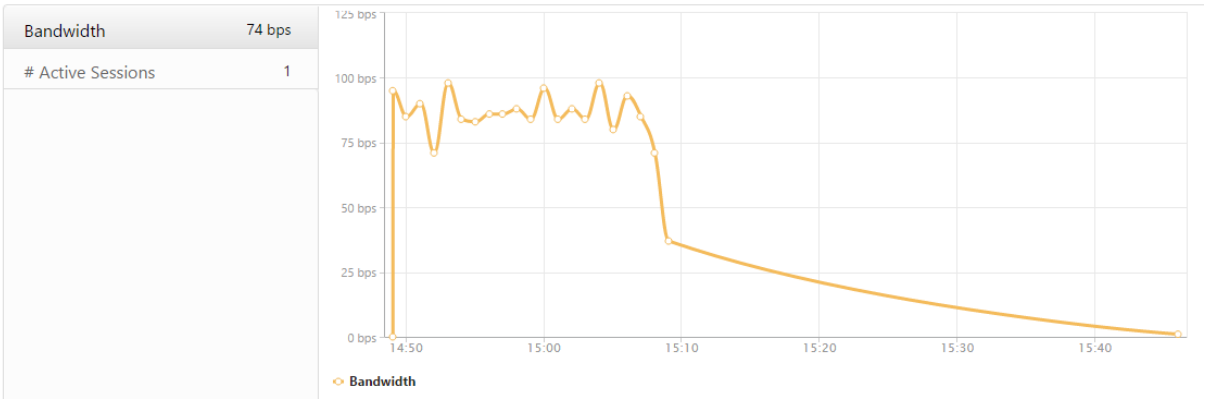
Pour afficher le nombre total d'octets et de bande passante consommés par une application :

Dans Citrix ADM, accédez à **Analytics > Gateway Insight > Applications**, faites défiler vers le bas et, sous l'onglet **Autres applications**, cliquez sur l'application pour laquelle vous souhaitez afficher les détails.

Vous pouvez afficher le nombre de sessions et le nombre total d'octets consommés par cette application.



Vous pouvez également afficher la bande passante consommée par cette application.



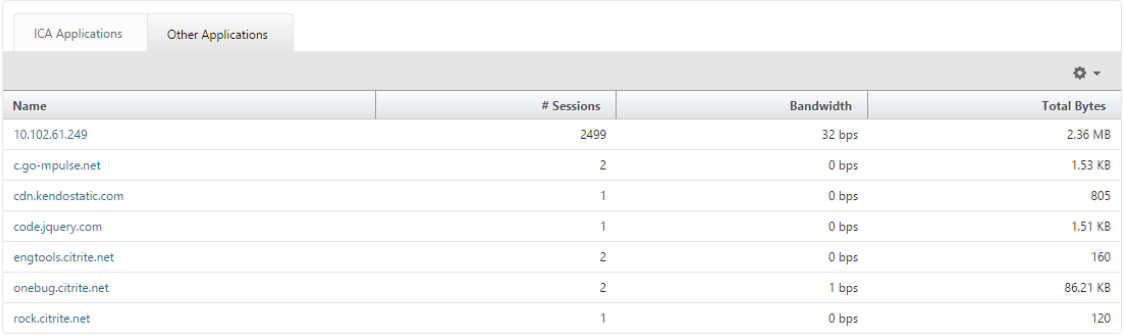
Un utilisateur s'est connecté à Citrix Gateway avec succès, mais ne peut pas accéder à certaines ressources réseau dans le réseau interne

Avec Gateway Insight, vous pouvez déterminer si l'utilisateur a accès aux ressources réseau ou non. Vous pouvez également afficher le nom de la stratégie qui a entraîné l'échec.

Pour afficher l'accès utilisateur aux ressources :

1. Dans Citrix ADM, **accédez à Analytics > Gateway Insight > Applications**.

2. Sur l'écran qui apparaît, faites défiler l'écran vers le bas et dans l'onglet **Autres applications**, sélectionnez l'application à laquelle l'utilisateur n'a pas pu se connecter.



Name	# Sessions	Bandwidth	Total Bytes
10.102.61.249	2499	32 bps	2.36 MB
c.go-mpulse.net	2	0 bps	1.53 KB
cdn.kendostatic.com	1	0 bps	805
code.jquery.com	1	0 bps	1.51 KB
engtools.citrite.net	2	0 bps	160
onebug.citrite.net	2	1 bps	86.21 KB
rock.citrite.net	1	0 bps	120

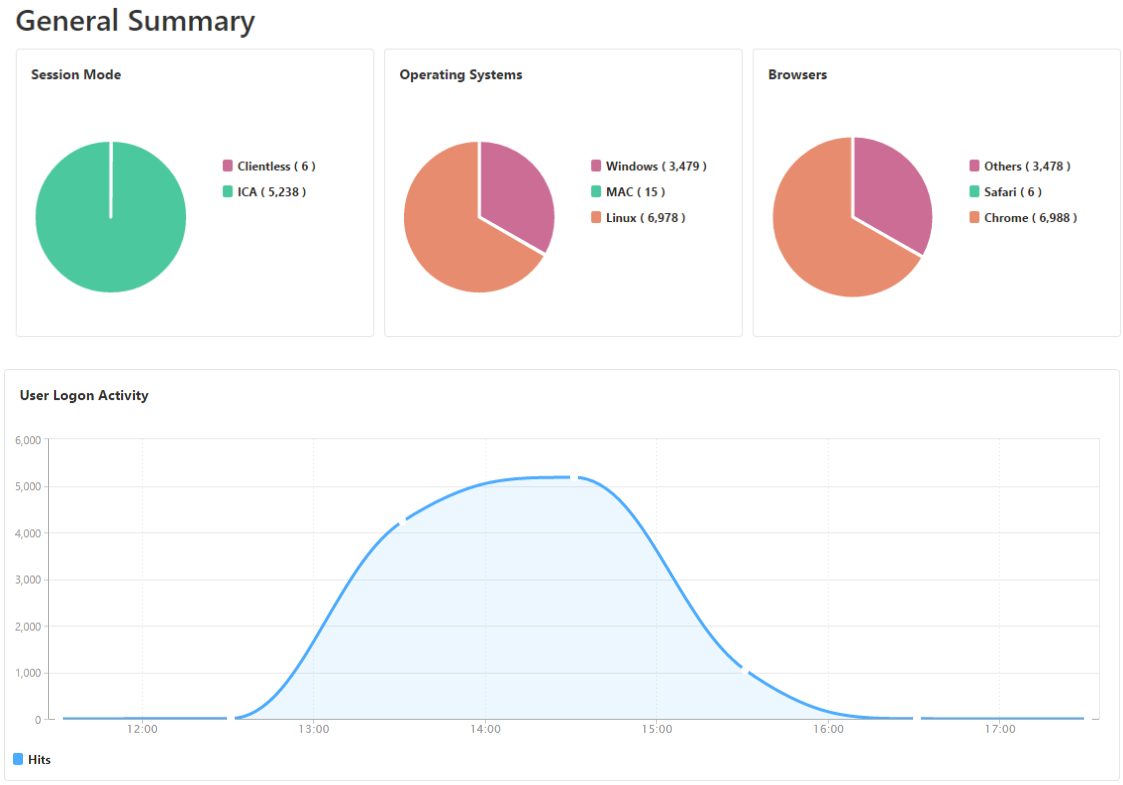
3. Faites défiler la page vers le bas et dans le tableau **Utilisateurs**, tous les utilisateurs ayant accès à cette application sont affichés.

Différents utilisateurs peuvent utiliser différents déploiements Citrix Gateway ou se connecter à Citrix Gateway via différents modes d'accès. L'administrateur doit être en mesure d'afficher les détails sur les types de déploiement et les modes d'accès

Avec Gateway Insight, vous pouvez afficher un résumé des différents modes de session utilisés par les utilisateurs pour ouvrir une session, les types de clients et le nombre d'utilisateurs connectés chaque heure. Vous pouvez également déterminer si le déploiement d'un utilisateur est une passerelle unifiée ou un déploiement Citrix Gateway classique. Pour les déploiements de Gateway unifiée, vous pouvez afficher le nom et l'adresse IP du serveur virtuel de commutation de contenu et le nom du serveur virtuel VPN.

Pour afficher le résumé des modes de session, du type de clients et du nombre d'utilisateurs connectés, procédez comme suit :

1. Dans Citrix ADM, accédez à **Analytics > Gateway Insight**.
2. Dans la section **Vue d'ensemble**, faites défiler la page vers le bas pour afficher les graphiques **Mode session, Systèmes d'exploitation, Navigateurs** et **Activité d'ouverture de session utilisateur** affichent les différents modes de session utilisés par les utilisateurs pour ouvrir une session, les types de clients et le nombre d'utilisateurs connectés toutes les heures.



Résoudre les problèmes liés à Gateway Insight

February 1, 2024

Si la solution Gateway Insight ne fonctionne pas comme prévu, le problème peut provenir de l'un des éléments suivants. Reportez-vous aux listes de contrôle dans les sections correspondantes pour le dépannage.

- Configuration de Gateway Insight.
- Problème de connectivité entre Citrix ADC et Citrix ADM.
- Génération d'enregistrements dans Citrix ADC.
- Validations dans Citrix ADM.

Liste de contrôle de la configuration Gateway Insight

- Assurez-vous que la fonctionnalité AppFlow est activée dans l'appliance Citrix ADC. Pour plus de détails, consultez Activation d'AppFlow.
- Vérifiez la configuration Gateway Insight dans la configuration en cours d'exécution Citrix ADC.

Exécutez la commande `show running | grep -i <appflow_policy>` pour vérifier la configuration de Gateway Insight. Assurez-vous que le type de liaison est REQUEST. Par exemple ;

```
bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
<!--NeedCopy-->
```

Le type de liaison OTHERTCP_REQUEST est également requis pour Gateway Insight.

```
bind vpn vserver afsanity -policy afp -priority 100 -type
   OTHERTCP_REQUEST
<!--NeedCopy-->
```

- Pour un déploiement à saut unique, Access Gateway ou Unified Gateway, assurez-vous que la stratégie Gateway Insight AppFlow est liée au serveur virtuel VPN, où le trafic VPN circule. Pour plus de détails, voir Activation de la collecte de données HDX Insight
- Pour le double-saut, Gateway Insight doit être configuré sur les deux sauts.
- Vérifiez le paramètre `appflowlog` dans le serveur virtuel Citrix Gateway/VPN. Pour plus de détails, consultez Activation d'AppFlow pour les serveurs virtuels.

Liste de contrôle de la connectivité entre Citrix ADC et Citrix ADM

- Vérifiez l'état du collecteur AppFlow dans Citrix ADC. Pour de plus amples informations, consultez Comment vérifier l'état de la connectivité entre Citrix ADC et AppFlow Collector.
- Vérifiez les accès à la stratégie AppFlow Gateway Insight.

  Exécutez la commande `show appflow policy <policy_name>` pour vérifier les succès de stratégie AppFlow.

  Vous pouvez également accéder à **Système > AppFlow > Stratégies** dans l'interface graphique pour vérifier les accès à la stratégie AppFlow.
- Validez tout pare-feu bloquant les ports AppFlow 4739 ou 5557.

Liste de contrôle de la génération d'enregistrements dans Citrix ADC

- Exécutez la commande `nsconmsg -d stats -g ai_tot` et vérifiez les incréments de statistiques dans Citrix ADC.
- Capturez `nstrace logs` et vérifiez la présence de paquets CFLOW pour confirmer que Citrix ADC exporte des enregistrements AppFlow.

> **Remarque :**
>
> Les `nstrace logs` sont obligatoires uniquement pour IPFIX. Pour Logstream, les journaux nstrace ne confirment pas si l'appliance ADC a exporté les enregistrements AppFlow.

Validation des enregistrements dans Citrix ADM

- Exécutez la commande `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: vpn_"` pour vérifier les journaux pour confirmer que Citrix ADM reçoit des enregistrements AppFlow.
- Assurez-vous que l'instance Citrix ADC est ajoutée à Citrix ADM.
- Assurez-vous que le serveur virtuel Citrix Gateway/VPN est sous licence dans Citrix ADM.

Validation des journaux Logstream dans Citrix ADM

La validation des données Logstream reçues par Citrix ADM peut être effectuée à l'aide des méthodes suivantes :

- **Activation de la journalisation des enregistrements de données dans Citrix ADM**

  Une fois activé, les journaux peuvent être vus dans le fichier /var/mps/log/mps_afdecoder.log

- **Activation de la journalisation de bibliothèque ULFD**

  Exécutez la commande `/mps/decoder_enable_debug`

  Les journaux sont capturés dans `/var/ulflog/libulfd.log`

  Vous pouvez désactiver la journalisation à l'aide de la commande `/mps/decoder_disable_debug`

Compteurs Gateway Insight

Les compteurs Gateway Insight suivants sont disponibles.

- ai_tot_preauth_epa_export
- ai_tot_auth_export
- ai_tot_auth_session_id_update_export
- ai_tot_postauth_epa_export
- ai_tot_vpn_update_export
- ai_tot_ica_fileinfo_export
- ai_tot_app_launch_failure
- ai_tot_logout_export

- ai_tot_skip_appflow_export
- ai_tot_sso_appflow_export
- ai_tot_authz_appflow_export
- ai_tot_appflow_pol_eval_failure
- ai_tot_vpn_export_state_mismatch
- ai_tot_appflow_disabled
- ai_tot_appflow_pol_eval_in_gwinsight
- ai_tot_app_launch_success

Enregistrements AppFlow dans le journal Citrix ADC

À partir de la version 13.0 build 71.x, vous pouvez vérifier les journaux Citrix ADC pour vérifier si les enregistrements AppFlow sont exportés. Le niveau de journal par défaut de `syslogparams` capture tous les journaux d'erreurs et d'informations. Dans le cas où vous ne trouvez pas d'indice sur les erreurs, activez tous les niveaux de journalisation, y compris DEBUG, `syslogparams` pour capturer même les journaux DEBUG.

Journaux d'échantillons

```
<local0.info> ... GMT 0-PPE-0 : default SSLVPN Message 147 0 : "
    GwInsight: Sent auth record Func=ns_sslvpn_export_auth_data Username
    =<name> Clientip=<ip>:<port> Destip=0:80 SessSeq=0 Sessid=<sessid>
    Gwip=<ip>:443 StatusCode=0 CSappid=0 CSAppname=(null) VPNfqdn=<
    vpnfqdn> Authtype=3 EPAid=(null) AuthStage=1 AuthDuration=309
    AuthAgent=<auth_server_ip> Groupname= Policyname=<name>
    CurfactorPolname=<name> NextfactorPolname= CSecExpr= Devicetype
    =16777219 Deviceid=0 email="
<local0.err> ... GMT 0-PPE-0 : default SSLVPN Message 143 0 : "GwInsight
    : Func=ns_aaa_copy_email_id_to_vpn_record input hash_attrs_len is
    zero"
<local0.err> ... GMT 0-PPE-0 : default SSLVPN Message 148 0 : "GwInsight
    : Func=update_session_appflow_collector pcb or session is NULL"
<local0.info> ... GMT 0-PPE-0 : default SSLVPN Message 165 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<> Clientip=<ip>:<port> Destip
    =<ip>:80 SessSeq=1 Sessid=<sessid> Gwip=<ip>:443 StatusCode=0
    CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=0 SessState
    =2 SessMode=2 IIP=0 AppByteCount=0 ReqURL=/Citrix/Store
Web BackendServername= SSOurl= email="
SSO logs:
<!--NeedCopy-->
```

```
<local0.info> ... GMT 0-PPE-0 : default SSLVPN Message 463 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
    Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
```



```
    =150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=1
    SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
    BackendServername=<> SSOurl= email="
<!--NeedCopy-->
```

```
<local0.info> ... GMT 0-PPE-0 : default SSLVPN Message 582 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
    Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
    =150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=3
    SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
    BackendServername=<> SSOurl= email="
<!--NeedCopy-->
```

```
<local0.info> ... GMT 0-PPE-0 : default SSLVPN Message 513 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
    Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
    =150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=2
    SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
    BackendServername=<> SSOurl= email="
<!--NeedCopy-->
```

```
<local0.info> ... GMT 0-PPE-0 : default SSLVPN Message 29796 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
    Destip=<ip>:443 SessSeq=c Sessid=<sessid> Gwip=<ip>:443 StatusCode
    =155 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=6
    SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
    BackendServername=<> SSOurl= email="
<!--NeedCopy-->
```

Contactez le support technique Citrix

Pour une résolution rapide, assurez-vous de disposer des informations suivantes avant de contacter le support technique Citrix :

- Détails du déploiement et de la topologie du réseau.
- Versions de Citrix ADC et de Citrix ADM.
- Offre groupée de support technique pour Citrix ADC et Citrix ADM.
- `nstrace` lors du problème.

Problèmes connus

Consultez les notes de mise à jour de Citrix ADC pour les problèmes connus sur Gateway Insight.

Security Insight

February 1, 2024

> Remarque
>
> Si votre version Citrix ADM est antérieure à **13.0-79.x**, vous pouvez afficher des informations sur la sécurité en accédant à **Analytics > Sécurité > Security Insight**. Pour la version **13.0-79.x ou ultérieure**, vous pouvez afficher les détails de la violation WAF en accédant à **Analytics > Sécurité > Violations de sécurité > Vue d'ensemble de l'application** et en cliquant sur **WAF** sous **Répartition des applications par**.

Les applications Web et de services Web exposées à Internet sont devenues de plus en plus vulnérables aux attaques. Pour protéger les applications contre les attaques, vous avez besoin d'une visibilité sur la nature et l'étendue des menaces passées, présentes et imminentes, de données exploitables en temps réel sur les attaques et de recommandations en matière de contre-mesures. Security Insight fournit une solution sur un seul écran pour vous aider à évaluer l'état de sécurité de votre application et à prendre des mesures correctives pour sécuriser vos applications.

> **Remarque**
>
> Security Insight est pris en charge sur Citrix Application Delivery Management (ADM) avec les appliances Citrix ADC exécutant sur la version 11.0 Build 65.31 et ultérieure.

Fonctionnement de Security Insight

Security Insight est une solution intuitive d'analyse de la sécurité basée sur un tableau de bord qui vous donne une visibilité totale sur l'environnement de menace associé à vos applications. Des informations sur la sécurité sont incluses dans Citrix ADM et elles génèrent périodiquement des rapports basés sur vos configurations de sécurité système Application Firewall et Citrix ADC. Les rapports contiennent les renseignements suivants pour chaque application :

- **Indice de menace.** Système de classement à un chiffre indiquant la criticité des attaques sur l'application, que l'application soit protégée ou non par une appliance Citrix ADC. Plus les attaques sur une application sont critiques, plus l'indice de menace pour cette application est élevé. Les valeurs varient de 1 à 7.

  L'indice des menaces est basé sur les informations d'attaque. Les informations relatives à l'attaque, telles que le type de violation, la catégorie d'attaque, l'emplacement et les détails du client, vous donnent un aperçu des attaques visant l'application. Les informations de violation sont envoyées à Citrix ADM uniquement lorsqu'une violation ou une attaque se produit. De nombreuses failles et vulnérabilités conduisent à un indice de menace élevé.

- **Indice de sécurité.** Système de notation à un chiffre indiquant la manière dont vous avez configuré en toute sécurité les instances Citrix ADC pour protéger les applications contre les menaces et les vulnérabilités externes. Plus les risques pour la sécurité d'une application sont faibles, plus l'indice de sécurité est élevé. Les valeurs varient de 1 à 7.

  L'index de sécurité tient compte à la fois de la configuration du pare-feu de l'application et de la configuration de sécurité du système Citrix ADC. Pour un indice de sécurité élevé, les deux configurations doivent être solides. Par exemple, si des contrôles rigoureux du pare-feu des applications sont en place mais que les mesures de sécurité du système Citrix ADC, telles qu'un mot de passe fort pour l'`nsroot` utilisateur, n'ont pas été adoptées, les applications se voient attribuer une valeur d'indice de sécurité faible.

- **Informations exploitables.** Informations dont vous avez besoin pour abaisser l'indice de menace et augmenter l'indice de sécurité, ce qui améliore considérablement la sécurité des applications. Par exemple, vous pouvez consulter des informations sur les violations, les configurations de sécurité existantes et manquantes pour le pare-feu des applications et d'autres fonctionnalités de sécurité, le taux d'attaque des applications, etc.

Configurer Security Insight

Citrix ADM prend en charge Security Insight à partir de toutes les instances Citrix ADC sur lesquelles un pare-feu d'application est configuré.

Pour configurer des informations de sécurité sur une instance ADC, configurez d'abord un profil de pare-feu d'application et une stratégie de pare-feu d'application. Bien que vous puissiez ensuite lier la stratégie de pare-feu d'application globalement, Citrix recommande que la stratégie soit liée au serveur virtuel.

Pour afficher les analyses sur Citrix ADM, activez la fonctionnalité AppFlow sur l'instance, configurez un collecteur, une action et une stratégie AppFlow, et liez la stratégie globalement. Ici aussi, bien que vous puissiez ensuite lier la stratégie de pare-feu de l'application globalement, Citrix recommande que la stratégie soit liée au serveur virtuel. Citrix vous recommande également d'utiliser Citrix ADM pour déployer des configurations AppFlow sur les instances ADC. Lorsque vous configurez le collecteur, vous devez spécifier l'adresse IP du serveur Citrix ADM sur lequel vous souhaitez surveiller les rapports.

Pour configurer des informations de sécurité sur une instance Citrix ADC :

1. Exécutez les commandes suivantes pour configurer un profil et une stratégie de pare-feu d'application et lier la stratégie de pare-feu d'application globalement ou au serveur virtuel d'équilibrage de charge.

add appfw profile [**-defaults** (basic advanced)]

set appfw profile <name> [**-startURLAction** <startURLAction> …]

add appfw policy <name> <rule> <profileName>

bind appfw global <policyName> <priority>

ou,

bind lb vserver <lb vserver> **-policyName** <policy> **-priority** <priority>

```
add appfw profile pr_appfw -defaults advanced
set  appfw profile pr_appfw -startURLaction log stats learn
add appfw policy pr_appfw_pol "HTTP.REQ.HEADER("Host").EXISTS"
   pr_appfw
bind appfw global pr_appfw_pol 1
or,
bind lb vserver outlook – policyName pr_appfw_pol – priority “20
   ”
<!--NeedCopy-->
```

2. Exécutez les commandes suivantes pour activer la fonctionnalité AppFlow, configurer un collecteur, une action et une stratégie AppFlow et lier la stratégie globalement ou au serveur virtuel d'équilibrage de charge :

add appflow collector <name> **-IPAddress** <ipaddress>

set appflow param DISABLED)]
[**-SecurityInsightRecordInterval**]
[**-SecurityInsightTraffic** (ENABLED

add appflow action <name> **-collectors** <string>

add appflow policy <name> <rule> <action>

bind appflow global <policyName> <priority> [<gotoPriorityExpression>] [**-type** <type>]

ou,

bind lb vserver <vserver> **-policyName** <policy> **-priority** <priority>

```
add appflow collector col -IPAddress 10.102.63.85
set appflow param  -SecurityInsightRecordInterval 600 -
   SecurityInsightTraffic ENABLED
add appflow action act1 -collectors col
add appflow action af_action_Sap_10.102.63.85 -collectors col
add appflow policy pol1 true act1
```



```
6  add appflow policy af_policy_Sap_10.102.63.85 true
       af_action_Sap_10.102.63.85
7  bind appflow global pol1 1 END -type REQ_DEFAULT
8  or,
9  bind lb vserver Sap  – policyName af_action_Sap_10.102.63.85  –
       priority  “ 20 ”
10 <!--NeedCopy-->
```

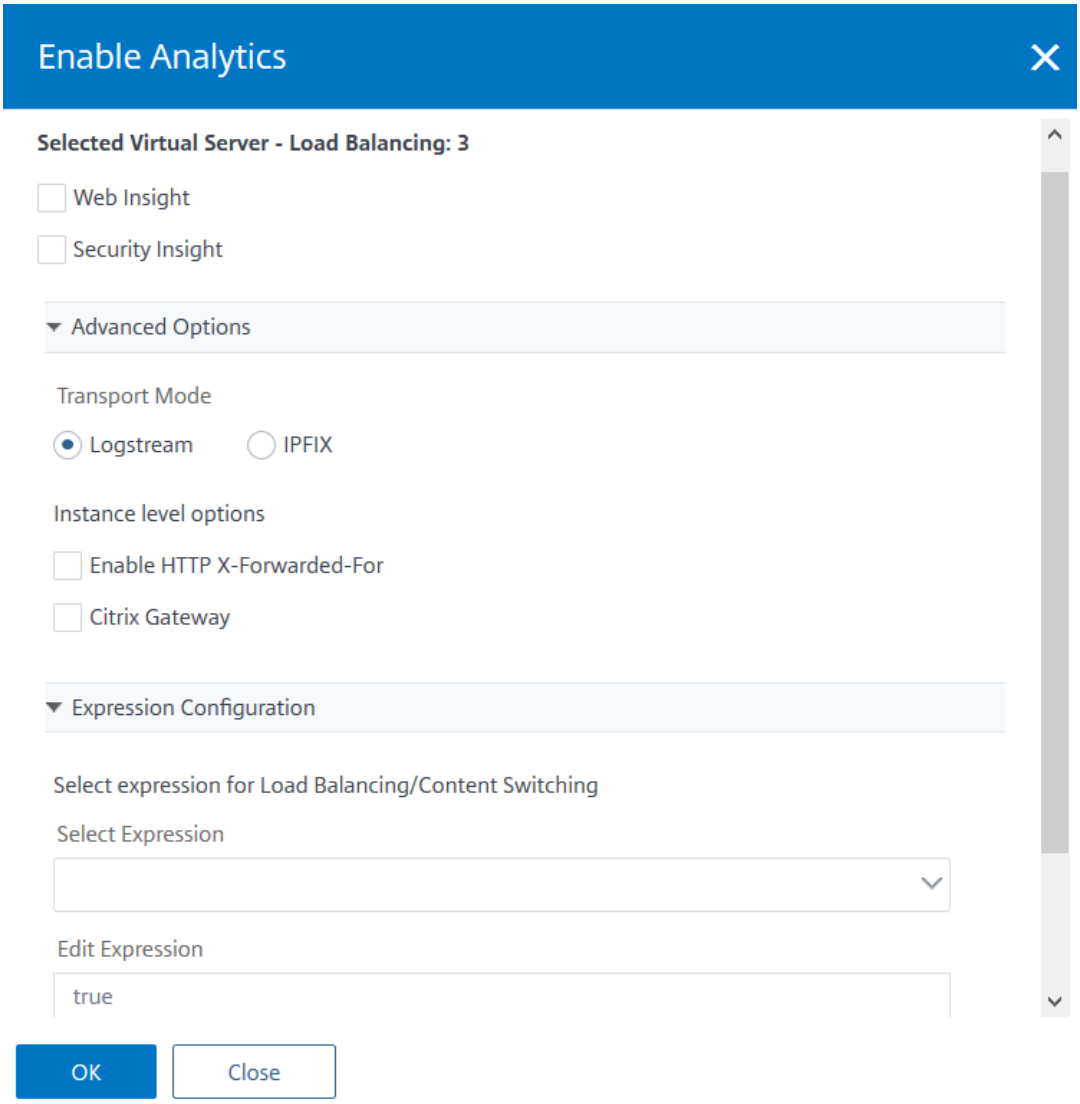
Pour activer Security Insight à partir de Citrix ADM :

Si votre Citrix ADM est **13.0 Build 41.x** :

1. Accédez à **Réseaux** > **Instances** > **Citrix ADC**, puis sélectionnez le type d'instance. Par exemple, VPX.
2. Sélectionnez l'instance et dans la liste **Sélectionner une action**, cliquez sur **Configurer Analytics**.
3. Sur la page **Configurer les analyses sur des serveurs virtuels**, sélectionnez le serveur virtuel et cliquez sur **Activer les analyses**.
4. Dans la fenêtre **Activer Analytics** :
   a) Sélectionnez **Insight de la sécurité**
   b) Sélectionnez **Logstream** comme mode de transport

      > **Remarque**
      >
      > Pour Citrix ADC 12.0 ou version antérieure, **IPFIX** est l'option par défaut pour le mode de transport. Pour Citrix ADC 12.0 ou version ultérieure, vous pouvez sélectionner **Logstream** ou **IPFIX** comme mode de transport.
      >
      > Pour plus d'informations sur IPFIX et Logstream, consultez la section Présentation de Logstream .

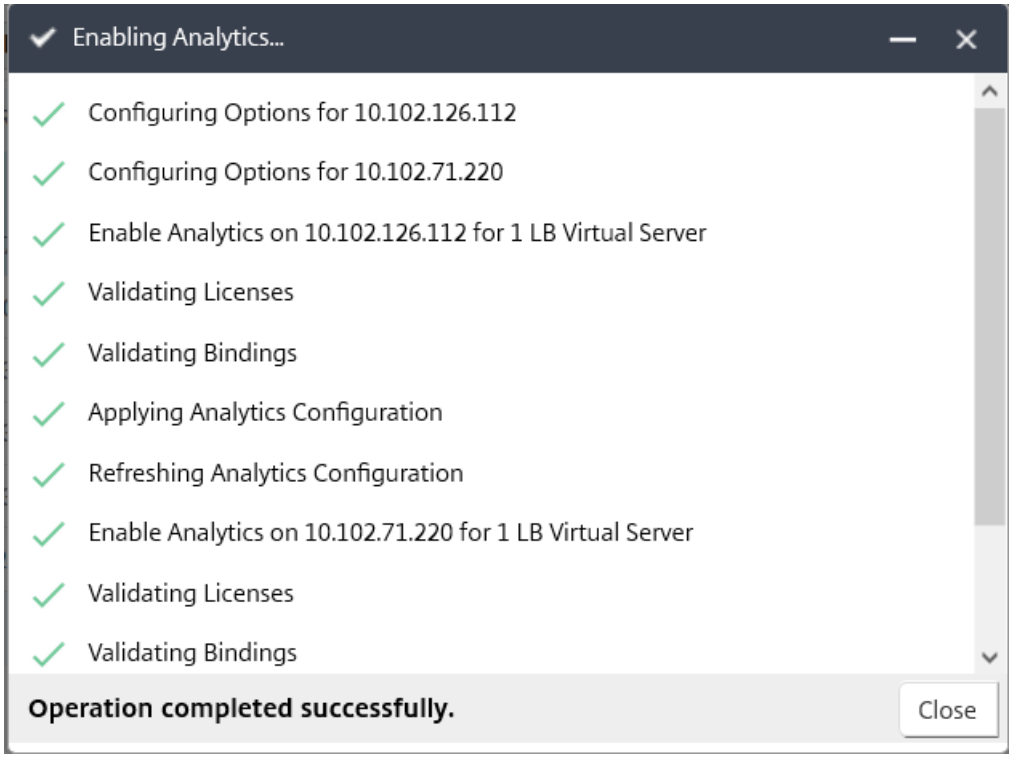
   c) L'expression est true par défaut
   d) Cliquez sur **OK**.



Remarque

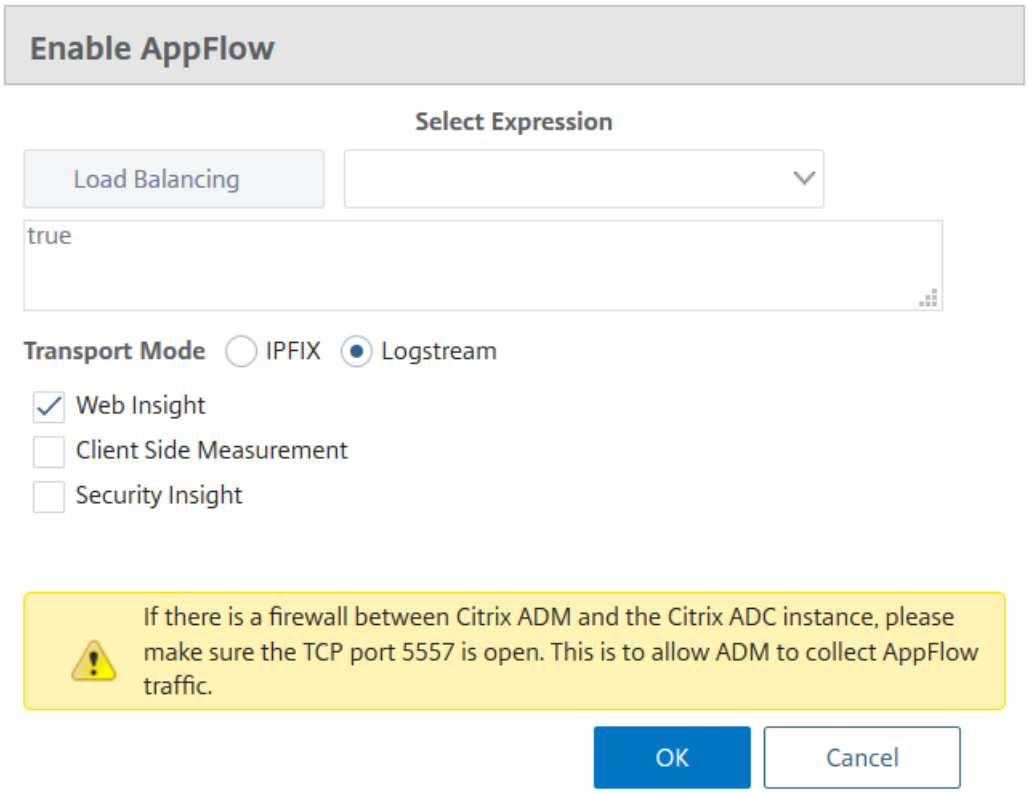
- Si vous sélectionnez des serveurs virtuels qui ne sont pas sous licence, Citrix ADM octroie d'abord des licences à ces serveurs virtuels, puis active les analyses
- Pour les partitions d'administration, seul **Web Insight** est pris en charge
- Pour les serveurs virtuels tels que la redirection du cache , l'authentification et le GSLB , vous ne pouvez pas activer les analyses. Un message d'erreur s'affiche.

Après avoir cliqué sur **OK**, Citrix ADM traite pour activer les analyses sur les serveurs virtuels sélectionnés.



Si votre Citrix ADM est **13.0 Build 36.27** :

1. Accédez à **Réseaux** > **Instances**, puis sélectionnez l'instance Citrix ADC que vous souhaitez activer AppFlow.
2. Dans la liste **Sélectionner une action**, sélectionnez **Configurer Analytics**.
3. Sélectionnez les serveurs virtuels, puis cliquez sur **Activer AppFlow**.
4. Dans le champ **Activer AppFlow**, tapez **true**et sélectionnez **Security Insight**.
5. Cliquez sur **OK**.



> **Remarque**
>
> Lorsque vous créez un groupe, vous pouvez affecter des rôles au groupe, fournir un accès au niveau de l'application au groupe et affecter des utilisateurs au groupe. Citrix ADM Analytics prend désormais en charge l'autorisation basée sur l'adresse IP virtuelle. Vos utilisateurs peuvent désormais voir des rapports pour tous les Insights uniquement pour les applications (serveurs virtuels) pour lesquelles ils sont autorisés. Pour plus d'informations sur les groupes et l'affectation d'utilisateurs au groupe, consultez Configurer des groupes.

Afficher les emplacements géographiques pour les rapports Security Insight

Les rapports Security Insight incluent les emplacements géographiques exacts d'où proviennent les demandes des clients. Vous pouvez afficher les emplacements géographiques dans Citrix ADM. Le fichier de base de données géo intégré dans Citrix ADC contient la plupart des adresses IP publiques. Le fichier est disponible à l'emplacement **/var/netscaler/inbuilt_db** dans Citrix ADC.

Pour activer les emplacements géographiques :

Exécutez les commandes suivantes pour activer la journalisation géographique et la journalisation au format CEF :

- **add locationFile** <Complete path with the DB filename>

- **définir les paramètres appfw -GeolocationLogging ON**
- **définir les paramètres appfw -CEFLogging ON**

Si aucune adresse IP n'est disponible dans le fichier de base de données géo, vous pouvez ajouter l'adresse IP de l'emplacement géographique. Avec l'adresse IP, vous pouvez également ajouter le nom de la ville/état/pays ainsi que les coordonnées de latitude et de longitude de chaque emplacement.

Ouvrez le fichier de base de données géo avec un éditeur de texte, tel que l'éditeur vi, et ajoutez une entrée pour chaque emplacement.

L'entrée doit être dans le format suivant :

```
\<start IP\>,\<end IP\>,,\<country\>,\<state\>,,\<city\>,,longitude,
latitude
```

Par exemple, les opérations suivantes peuvent être effectuées :

```
4.17.142.224,4.17.142.239,,US,New York,,Harrison,,73.7304,41.0568
<!--NeedCopy-->
```

Réputation de la propriété intellectuelle

Vous pouvez utiliser NetScaler Insight Center pour surveiller et gérer la réputation IP de votre trafic entrant. Vous pouvez configurer des stratégies pour ajouter d'autres adresses IP comme étant malveillantes et créer une liste de blocs personnalisée.

Pour en savoir plus sur la configuration et l'utilisation de la réputation IP, consultez Réputation IP.

Surveillance de la réputation IP

La fonctionnalité Réputation IP fournit des informations relatives aux attaques sur les adresses IP malveillantes. Par exemple, il signale le score de réputation IP, la catégorie de réputation IP, le temps d'attaque de réputation IP, l'adresse IP du périphérique et des détails sur l'adresse IP du client.

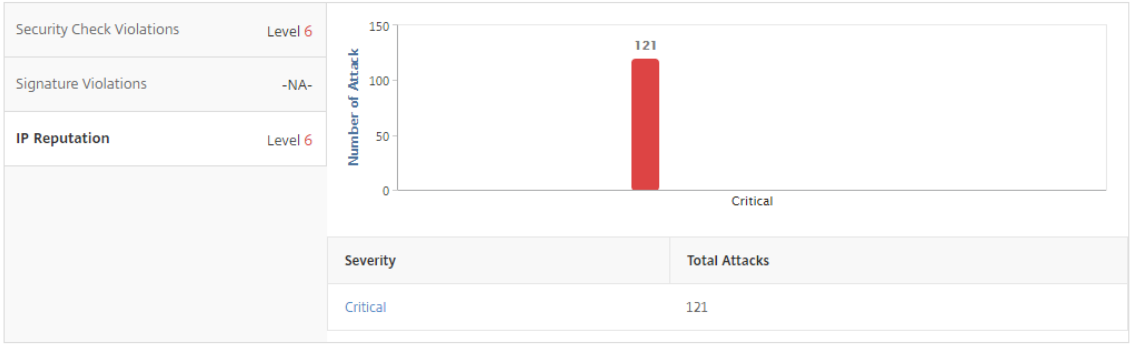
Le score de réputation IP indique le risque associé à une adresse IP. Le score a les suivantes sont les plages :

Score de réputation IP	Niveau de risque
1–20	Risque élevé
21–40	Suspect
41–60	Risque modéré
61–80	Risque faible

Score de réputation IP	Niveau de risque
81–100	Fiable

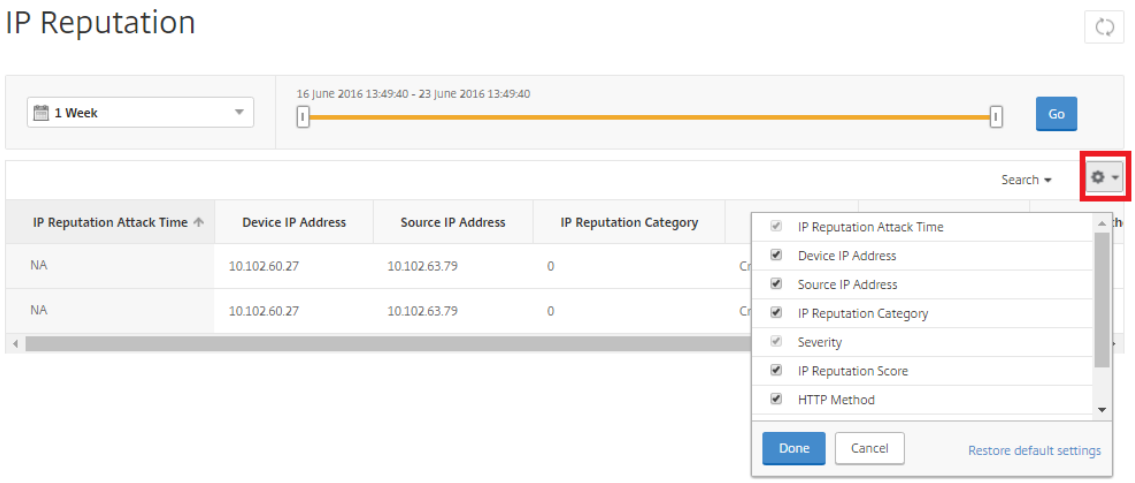
Pour surveiller la réputation d'IP :

1. Accédez à **Analytics**> **Security Insight**, puis sélectionnez l'application que vous souhaitez surveiller.
2. Dans l'onglet **Index des menaces**, sélectionnez **Réputation IP.**



3. Sélectionnez une gravité pour afficher plus de détails sur les attaques qui se trouvaient à ce niveau. Vous pouvez cliquer sur le graphique à barres ou dans le tableau sous le graphique.
4. Sélectionnez la période pour laquelle vous souhaitez afficher les détails. Vous pouvez utiliser le curseur temporel pour personnaliser davantage la période sélectionnée. Ensuite, cliquez sur **Aller**.

5. Pour personnaliser l'affichage, cliquez sur le bouton Paramètres.



Seuils

Vous pouvez définir et consulter les seuils relatifs à l'indice de sécurité et à l'indice de menace des applications dans Security Insight.

Pour définir un seuil :

1. Accédez à **Analytics** > **Paramètres** > **Seuils**, puis sélectionnez **Ajouter**.
2. Sélectionnez le type de trafic comme **Sécurité** dans le champ **Type de trafic** et saisissez les informations requises dans les autres champs appropriés tels que le nom, la durée et l'entité.
3. Dans la section **Configurer une règle**, utilisez les champs Mesure, Comparateur et Valeur pour définir un seuil.

   Par exemple, "Threat Index"*">"*"5"
4. Dans les **Paramètres de notification**, sélectionnez le type de notification.
5. Cliquez sur **Créer**.

Pour afficher les franchissement des seuils :

1. Accédez à **Analytics** > **Security Insight** > **Périphériques**, puis sélectionnez l'instance Citrix ADC.
2. Dans la section **Application**, vous pouvez afficher le nombre de violations de seuil survenues pour chaque serveur virtuel dans la colonne **Violation de seuil** .

Cas d'utilisation de Security Insight

Les cas d'utilisation suivants décrivent comment utiliser les informations de sécurité pour évaluer l'exposition aux menaces des applications et améliorer les mesures de sécurité.

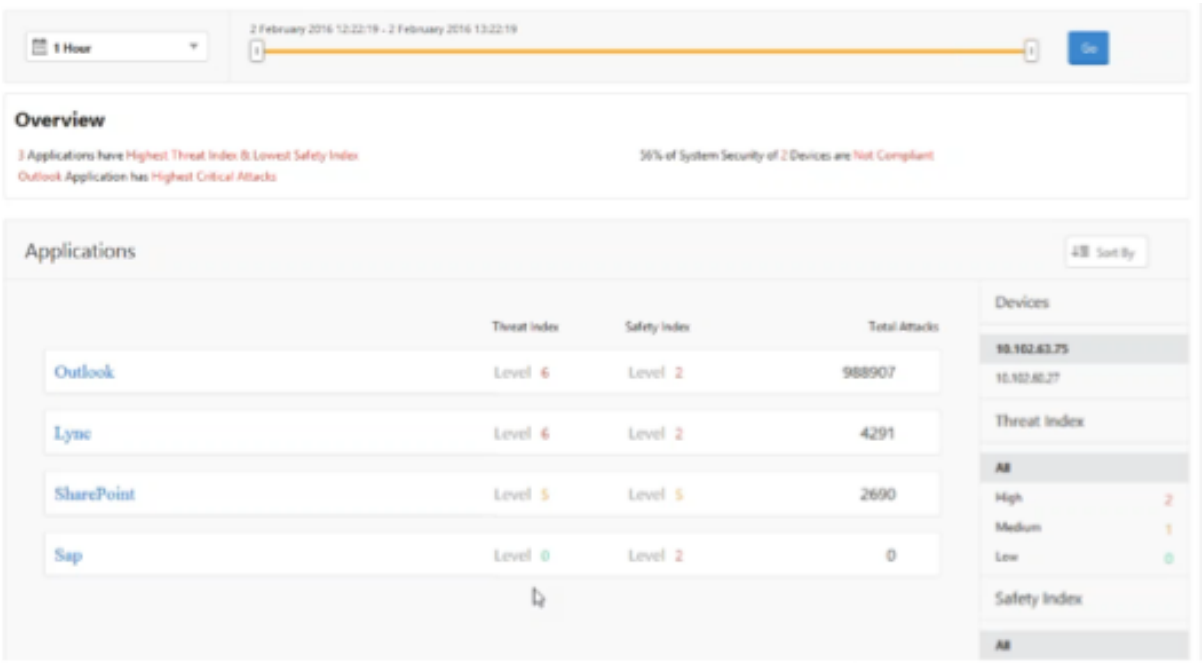
Obtenez une vue d'ensemble de l'environnement des menaces

Dans ce cas d'utilisation, vous disposez d'un ensemble d'applications exposées à des attaques et vous avez configuré Citrix ADM pour surveiller l'environnement de menace. Vous devez consulter fréquemment l'indice de menace, l'indice de sécurité, ainsi que le type et la gravité des attaques que les applications ont pu subir, afin de pouvoir vous concentrer d'abord sur les applications qui nécessitent le plus d'attention. Le tableau de bord d'informations sur la sécurité fournit un résumé des menaces rencontrées par vos applications pendant la période de votre choix et pour un périphérique Citrix ADC sélectionné. Il affiche la liste des applications, leurs indices de menace et de sécurité, ainsi que le nombre total d'attaques pour la période choisie.

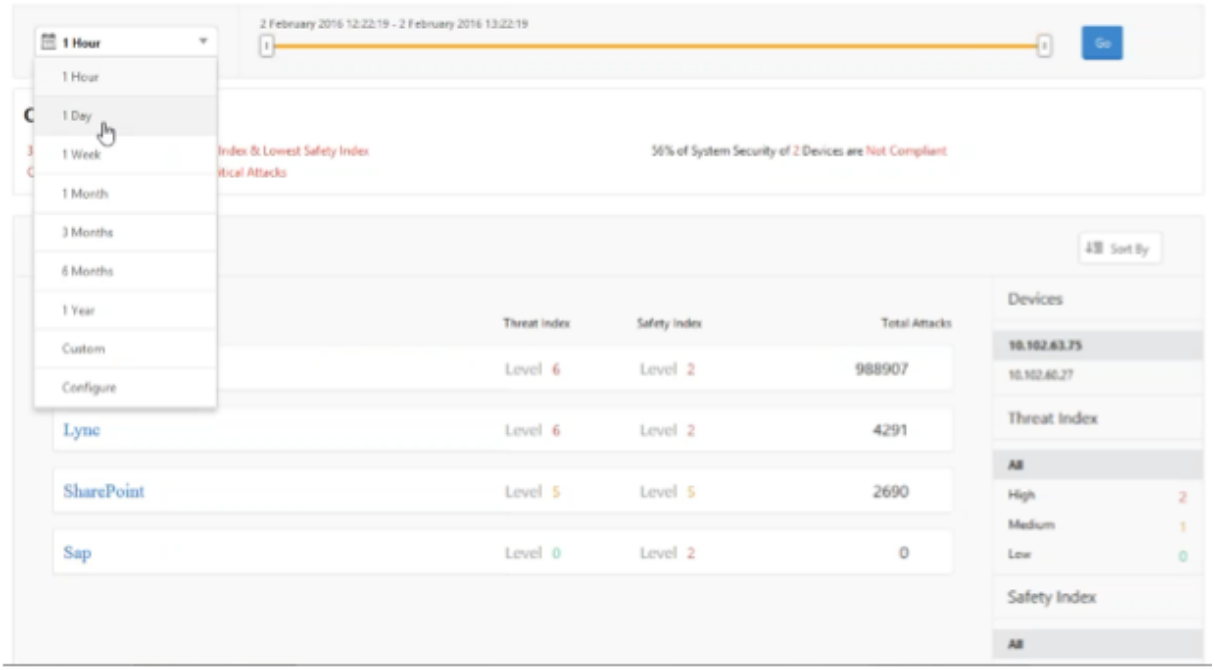
Par exemple, vous pouvez surveiller Microsoft Outlook, Microsoft Lync, SharePoint et une application SAP, et vous pouvez consulter un résumé de l'environnement de menace pour ces applications.

Pour obtenir un résumé de l'environnement de menace, ouvrez une session sur **Citrix ADM**, puis accédez à **Analytics > Security Insight**.

Les informations clés sont affichées pour chaque application. La période par défaut est de 1 heure.



Pour afficher les informations d'une période différente, sélectionnez une période dans la liste située en haut à gauche.



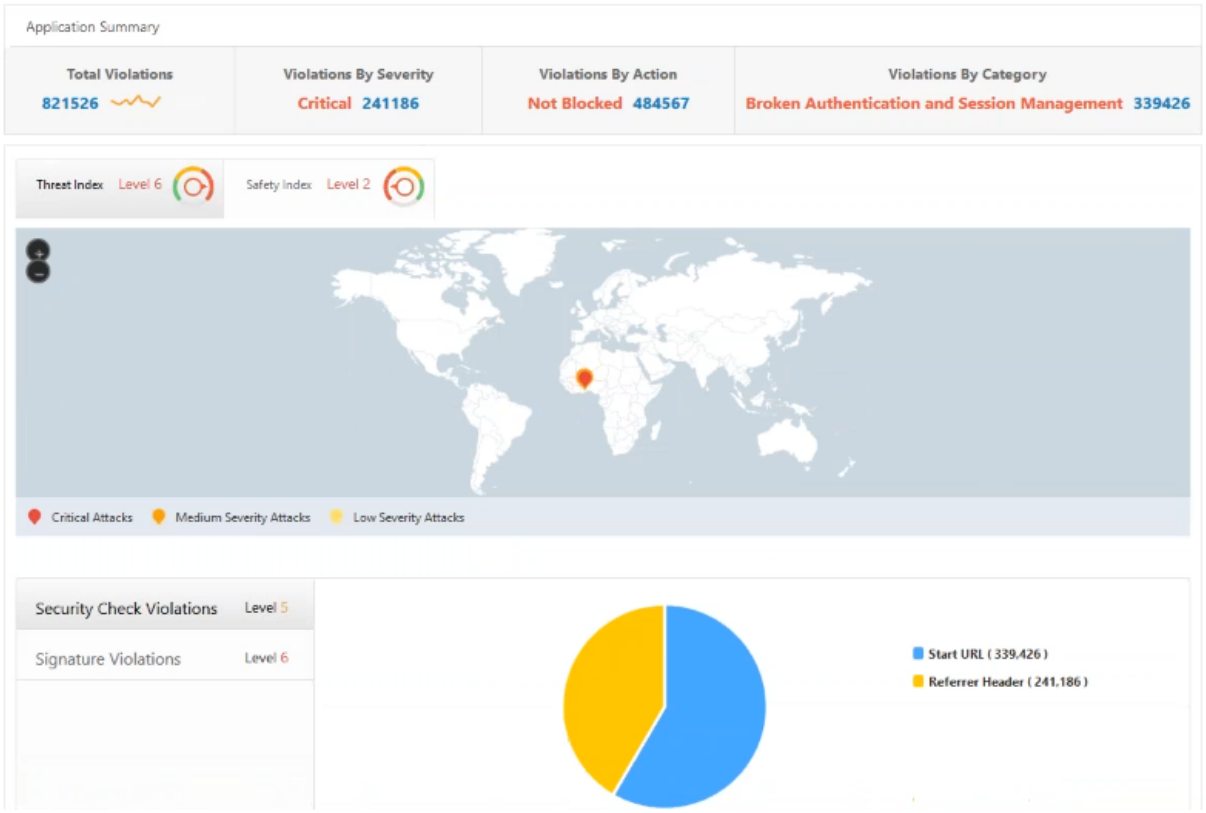
Pour afficher un résumé pour une autre instance Citrix ADC, sous **Périphériques**, cliquez sur l'adresse IP de l'instance Citrix ADC. Pour trier la liste des applications par colonne donnée, cliquez sur l'en-tête de colonne.

Déterminer l'exposition aux menaces d'une application

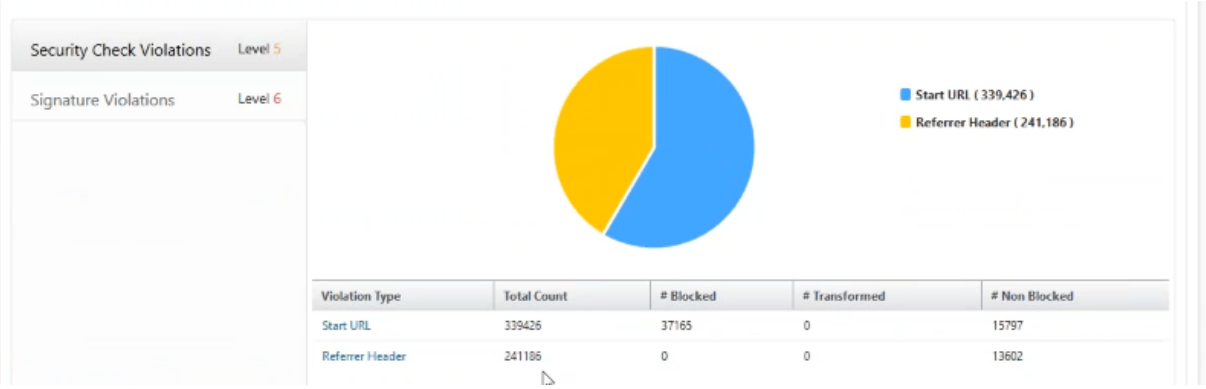
Pour identifier les applications qui ont un indice de menace élevé et un indice de sécurité faible dans le tableau de bord Security Insight, vous souhaitez déterminer l'exposition aux menaces avant de décider de les sécuriser. Autrement dit, vous voulez déterminer le type et la gravité des attaques qui ont dégradé leurs valeurs d'index. Vous pouvez déterminer l'exposition à la menace d'une application en consultant le résumé de l'application.

Dans cet exemple, Microsoft Outlook a une valeur d'indice de menace de 6 et vous voulez savoir quels facteurs contribuent à cet indice de menace élevé.

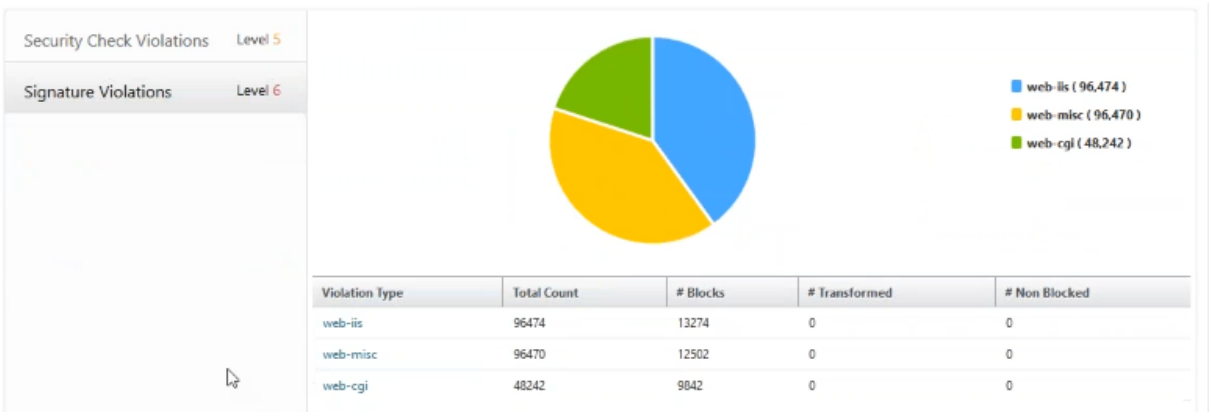
Pour déterminer l'exposition à la menace de Microsoft Outlook, dans le tableau de bord **Security Insight**, cliquez sur **Outlook** . Le résumé de l'application inclut une carte qui identifie l'emplacement géographique du serveur.



Cliquez sur **Index des menaces > Violations de vérification de sécurité** et consultez les informations de violation qui s'affichent.



Cliquez sur **Violations de signature** et consultez les informations de violation qui s'affichent.

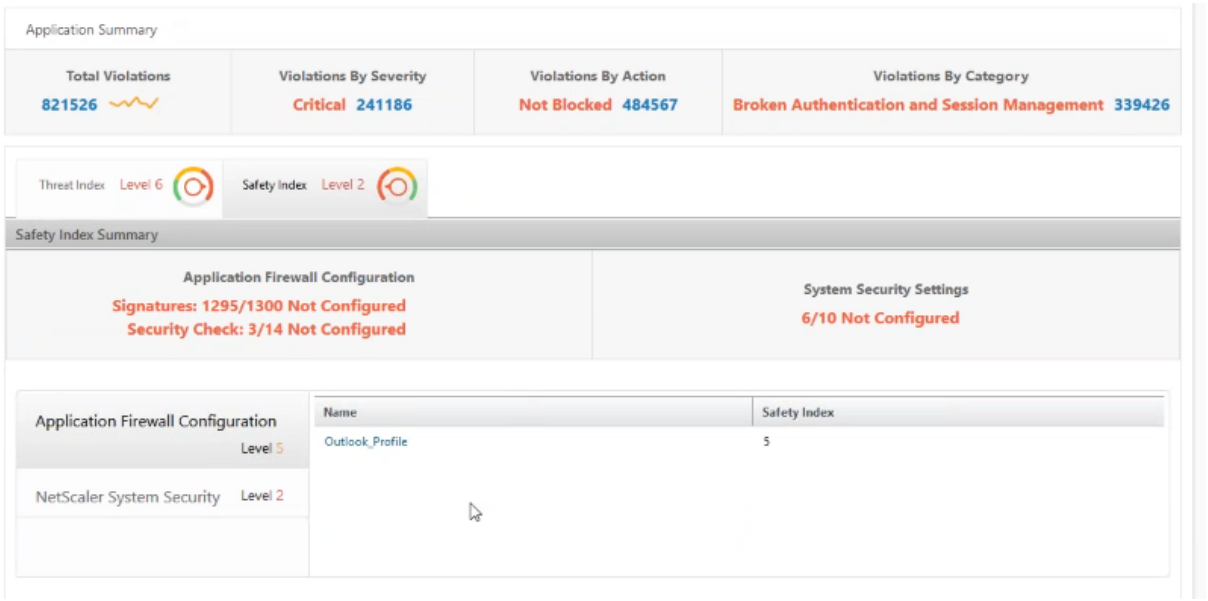


Déterminer la configuration de sécurité existante et manquante pour une application

Après avoir examiné l'exposition aux menaces d'une application, vous souhaitez déterminer quelles configurations de sécurité des applications sont en place et quelles configurations sont manquantes pour cette application. Vous pouvez obtenir ces informations en consultant le résumé de l'indice de sécurité de l'application.

Le résumé de l'indice de sécurité fournit des informations sur l'efficacité des configurations de sécurité suivantes :

- **Configuration du pare-feu des applications.** Indique le nombre d'entités de signature et de sécurité qui ne sont pas configurées.
- **Sécurité du système NetScaler.** Indique combien de paramètres de sécurité système ne sont pas configurés.

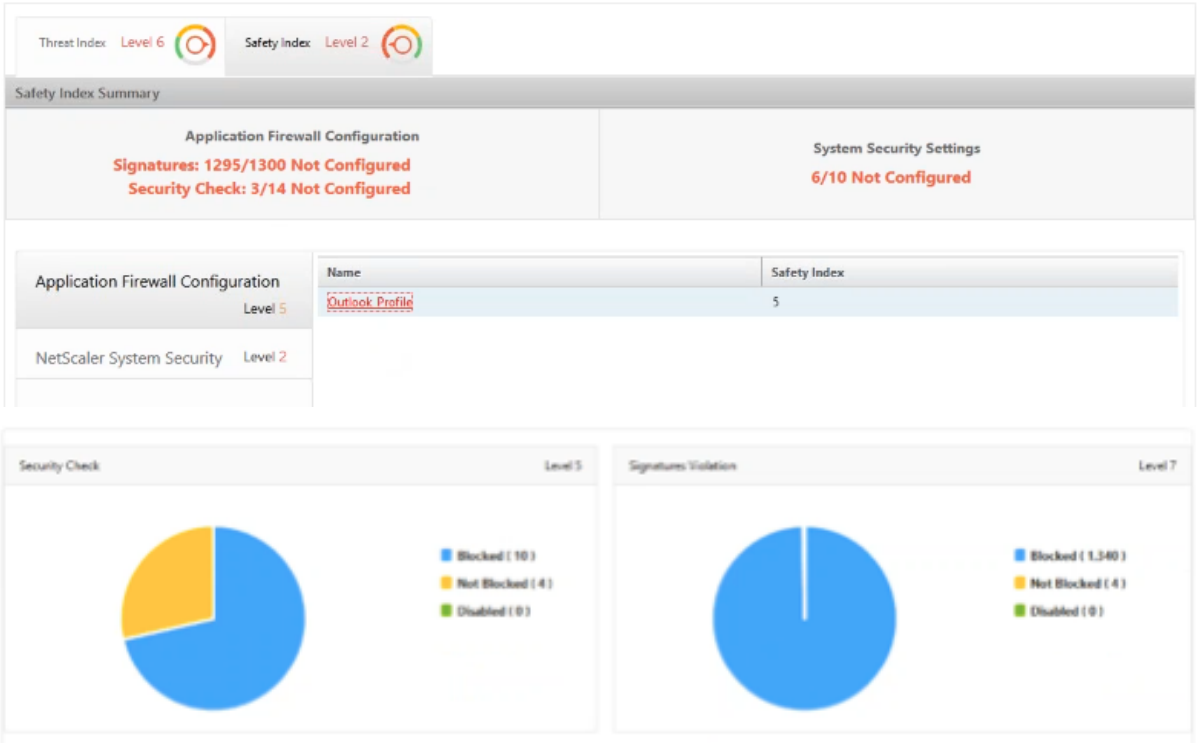


Dans le cas d'utilisation précédent, vous avez examiné l'exposition aux menaces de Microsoft Outlook,

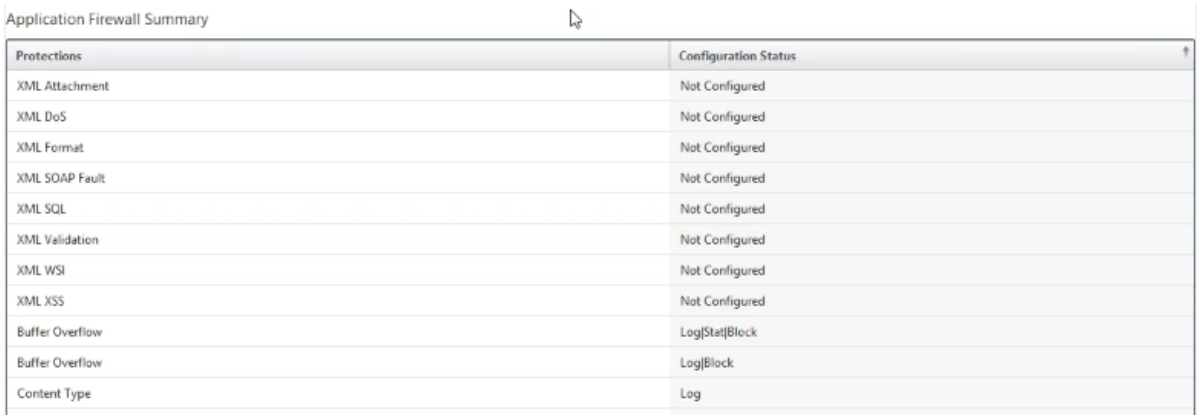
qui a une valeur d'indice de menace de 6. Maintenant, vous voulez savoir quelles configurations de sécurité sont en place pour Outlook et quelles configurations peuvent être ajoutées pour améliorer son indice de menace.

Dans le tableau de bord **Security Insight**, cliquez sur **Outlook**, puis cliquez sur l'onglet **Safety Index**. Examiner les renseignements fournis dans la zone **Résumé de l'indice de sécurité**.

Sur le nœud **Configuration du pare-feu d'application**, cliquez sur **Outlook_Profile** et vérifiez les informations de vérification de sécurité et de violation de signature dans les graphiques à secteurs.



Vérifiez l'état de configuration de chaque type de protection dans le tableau récapitulatif du pare-feu de l'application. Pour trier le tableau d'une colonne, cliquez sur l'en-tête de colonne.

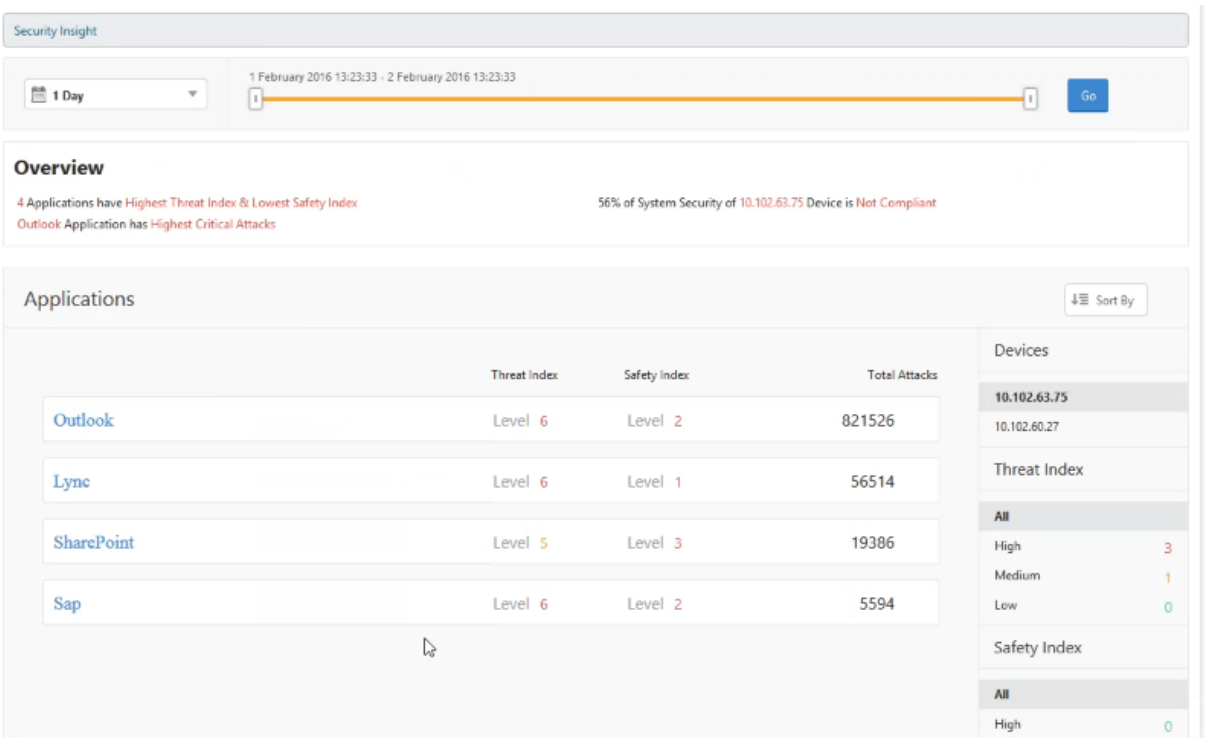


Cliquez sur le nœud **NetScaler System Security** et passez en revue les paramètres de sécurité du système et les recommandations Citrix pour améliorer l'index de sécurité des applications.

Identifier les applications nécessitant une attention immédiate

Les applications qui nécessitent une attention immédiate sont celles qui présentent un indice de menace élevé et un indice de sécurité faible.

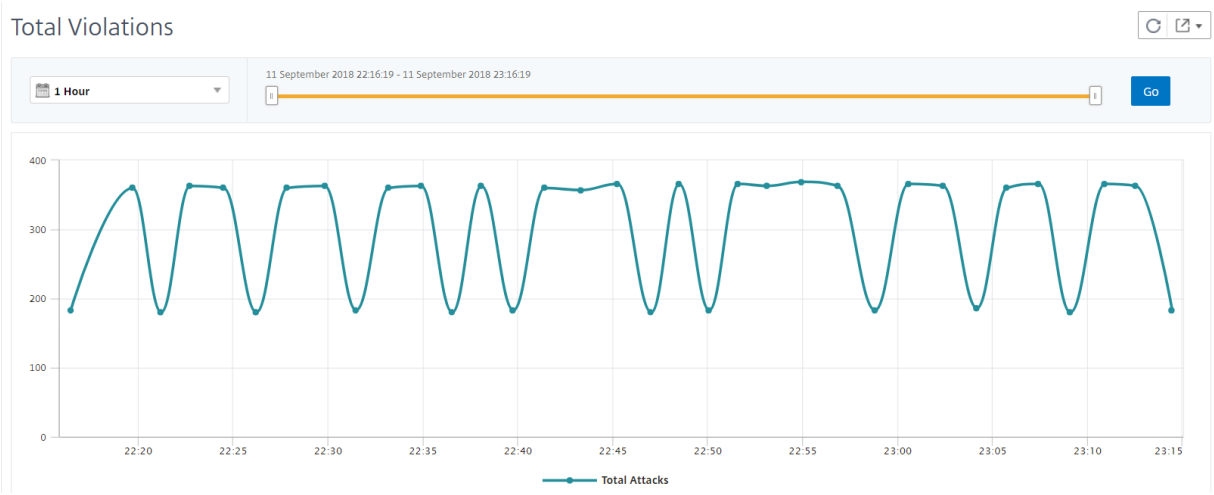
Dans cet exemple, Microsoft Outlook et Microsoft Lync ont une valeur d'indice de menace élevée de 6, mais Lync a le plus faible des deux index de sécurité. Par conséquent, vous devrez peut-être concentrer votre attention sur Lync avant d'améliorer l'environnement de menace pour Outlook.



Déterminer le nombre d'attaques dans un temps donné

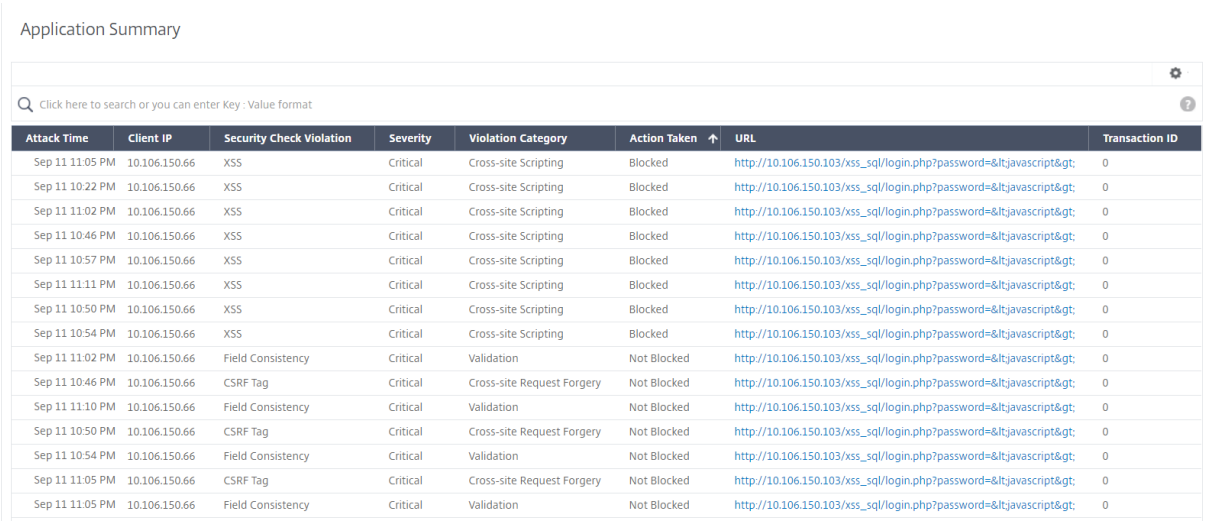
Vous pouvez déterminer le nombre d'attaques survenues sur une application donnée à un moment donné ou étudier le taux d'attaque pour une période donnée.

Sur **la page Security Insight**, cliquez sur n'importe quelle application et dans le **Résumé de l'application**, cliquez sur le nombre de violations. La page Total des violations affiche les attaques de manière graphique pendant une heure, un jour, une semaine et un mois.

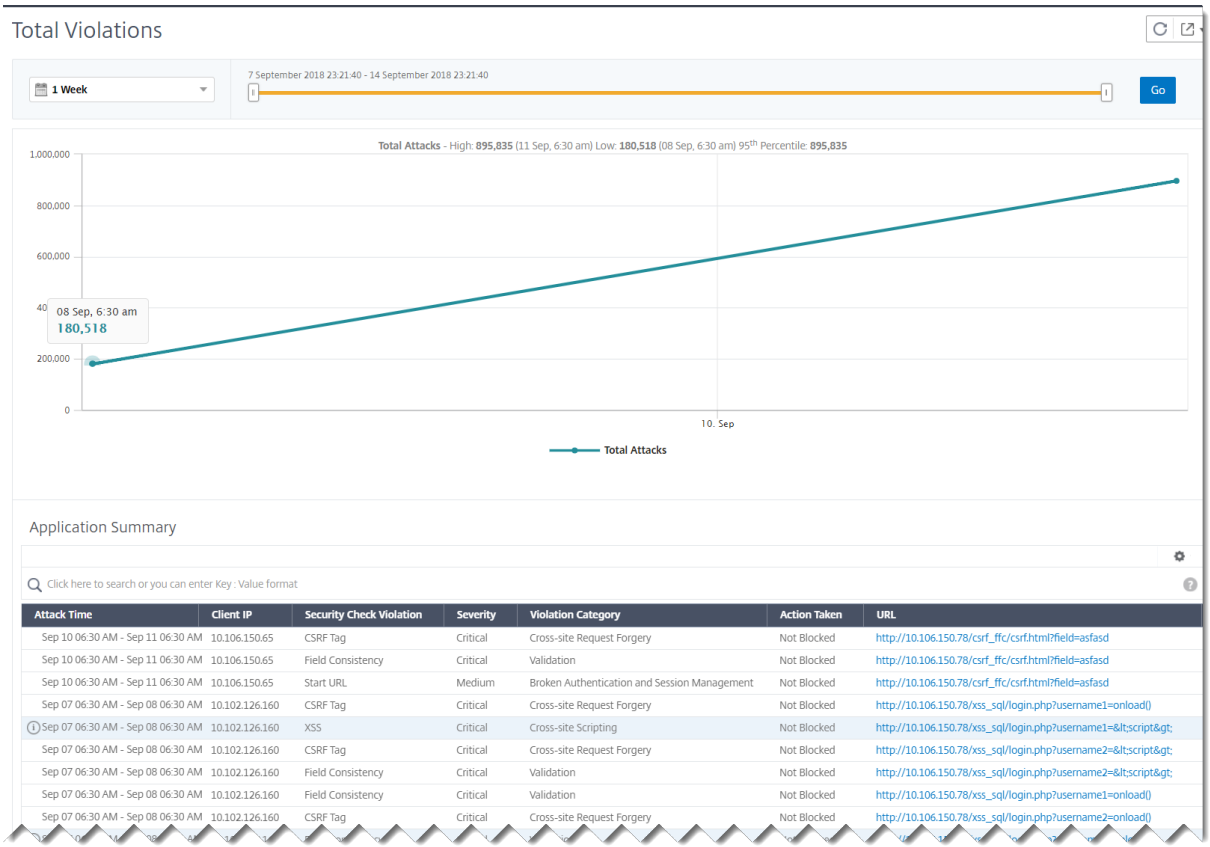


Le tableau Récapitulatif des applications fournit des détails sur les attaques. Certains d'entre eux sont les suivants :

- Temps d'attaque
- Adresse IP du client à partir duquel l'attaque s'est produite
- Gravité
- Catégorie de violation
- URL d'origine de l'attaque, et d'autres détails.



Bien que vous puissiez toujours afficher l'heure de l'attaque dans un rapport horaire comme indiqué dans l'image, vous pouvez maintenant afficher la plage de temps d'attaque pour les rapports agrégés, même pour les rapports quotidiens ou hebdomadaires. Si vous sélectionnez « 1 jour » dans la liste de périodes, le rapport Security Insight affiche toutes les attaques qui sont agrégées et le temps d'attaque est affiché dans une plage d'une heure. Si vous choisissez « 1 semaine » ou « 1 mois », toutes les attaques sont agrégées et le temps d'attaque est affiché dans une plage d'un jour.

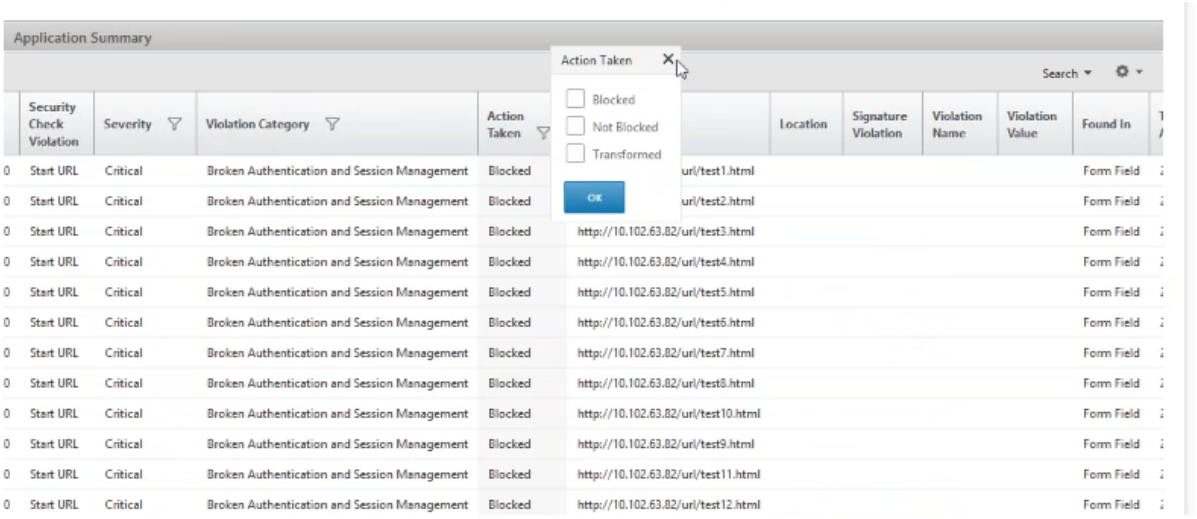


Obtenir des informations détaillées sur les violations de sécurité

Vous pouvez afficher la liste des attaques sur une application et obtenir des informations sur le type et la gravité des attaques, les actions entreprises par l'instance Citrix ADC, les ressources demandées et la source des attaques.

Par exemple, vous pouvez déterminer le nombre d'attaques sur Microsoft Lync bloquées, les ressources demandées et les adresses IP des sources.

Sur le tableau de **bord Security Insight**, cliquez sur **Lync > Nombre total de violations**. Dans le tableau, cliquez sur l'icône de filtre dans l'en-tête de colonne **Action prise**, puis sélectionnez **Bloqué** .



Pour plus d'informations sur les ressources demandées, consultez la colonne **URL**. Pour plus d'informations sur les sources des attaques, consultez la colonne **IP du client** .

Afficher les détails des expressions du journal

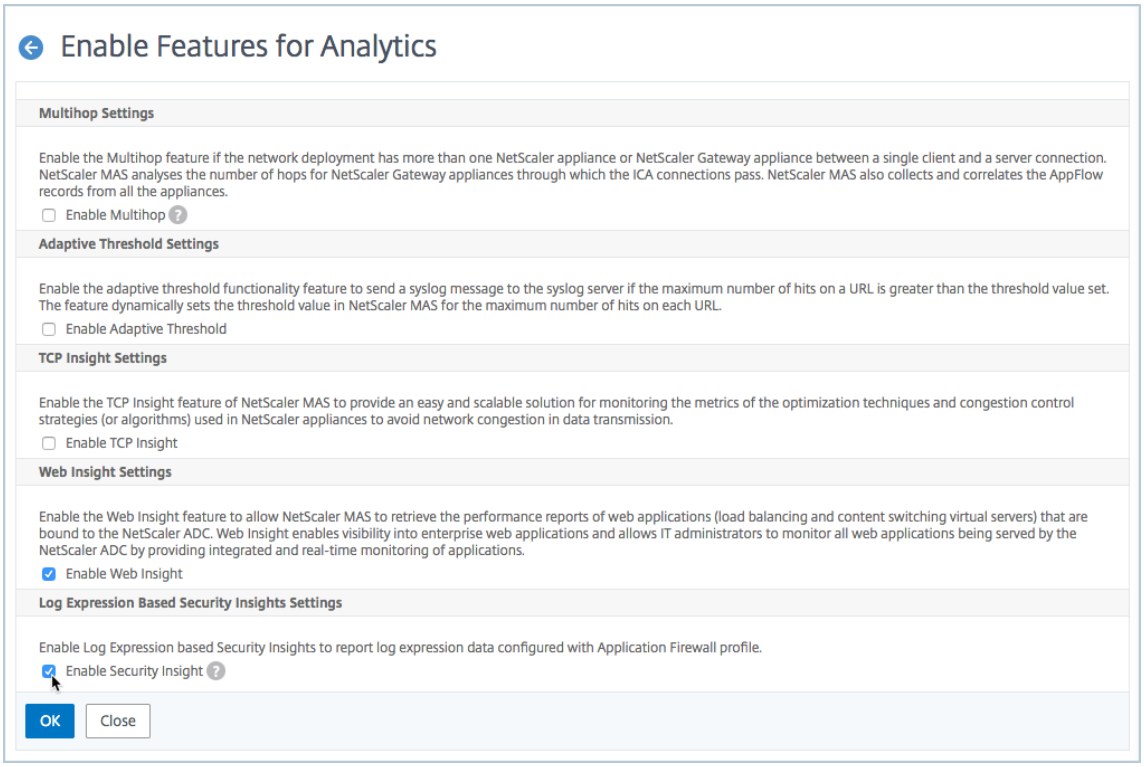
Les instances de Citrix ADC utilisent des expressions de journal configurées avec le profil de pare-feu d'application pour prendre des mesures en cas d'attaques sur une application de votre entreprise. Dans Security Insight, vous pouvez afficher les valeurs renvoyées pour les expressions de journal utilisées par l'instance de Citrix ADC. Ces valeurs incluent l'en-tête de la requête, le corps de la requête, etc. Outre les valeurs d'expression de journal, vous pouvez également afficher le nom de l'expression de journal et le commentaire de l'expression de journal définie dans le profil Application Firewall que l'instance de Citrix ADC a utilisée pour exécuter l'attaque.

Conditions préalables Assurez-vous que vous :

- Configurez les expressions de journal dans le profil du pare-feu d'application. Pour plus d'informations, consultez la section Pare-feu d'application .

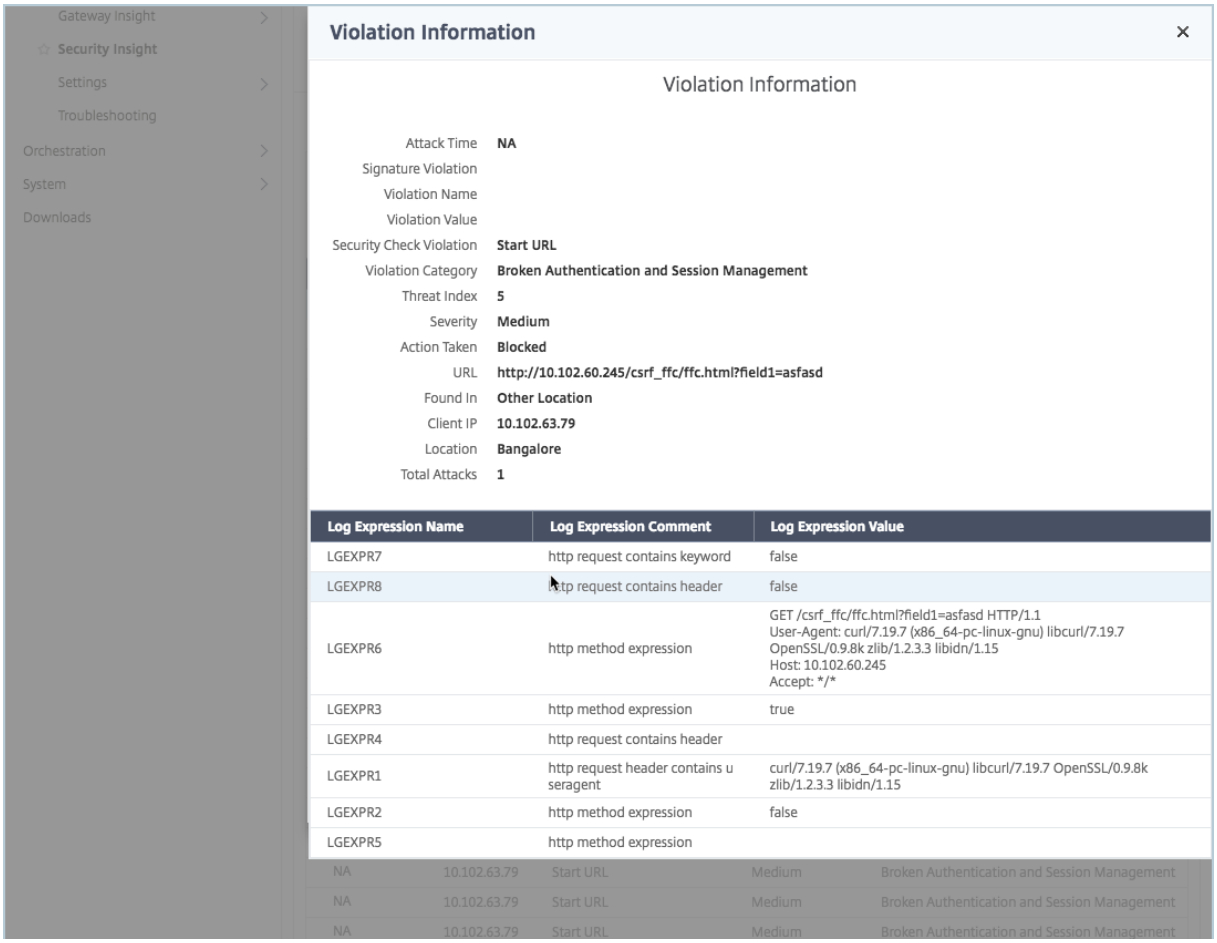
- Activez le paramètre Security Insights basé sur l'expression de journal dans Citrix ADM. Procédez comme suit :

  1. Accédez à **Analytics > Paramètres** , puis cliquez sur **Activer les fonctionnalités pour Analytics** .
  2. Dans la page Activer la fonctionnalité pour Analytics, sélectionnez **Activer Security Insight** dans la section **Log Expression Security Insight Setting**, puis cliquez sur **OK**.



Par exemple, vous pouvez afficher les valeurs de l'expression de journal renvoyée par l'instance de Citrix ADC pour l'action qu'elle a effectuée pour une attaque sur Microsoft Lync dans votre entreprise.

Dans le tableau de bord Security Insight, accédez à **Lync > Total des violations**. Dans le **tableau Résumé de l'application**, cliquez sur l'URL pour afficher les détails complets de la violation dans la page **Informations sur la violation**, y compris le nom de l'expression de journal, le commentaire et les valeurs renvoyées par l'instance Citrix ADC pour l'action.



Mettre en surbrillance les modèles de violation pour le pare-feu d'application Web (WAF)

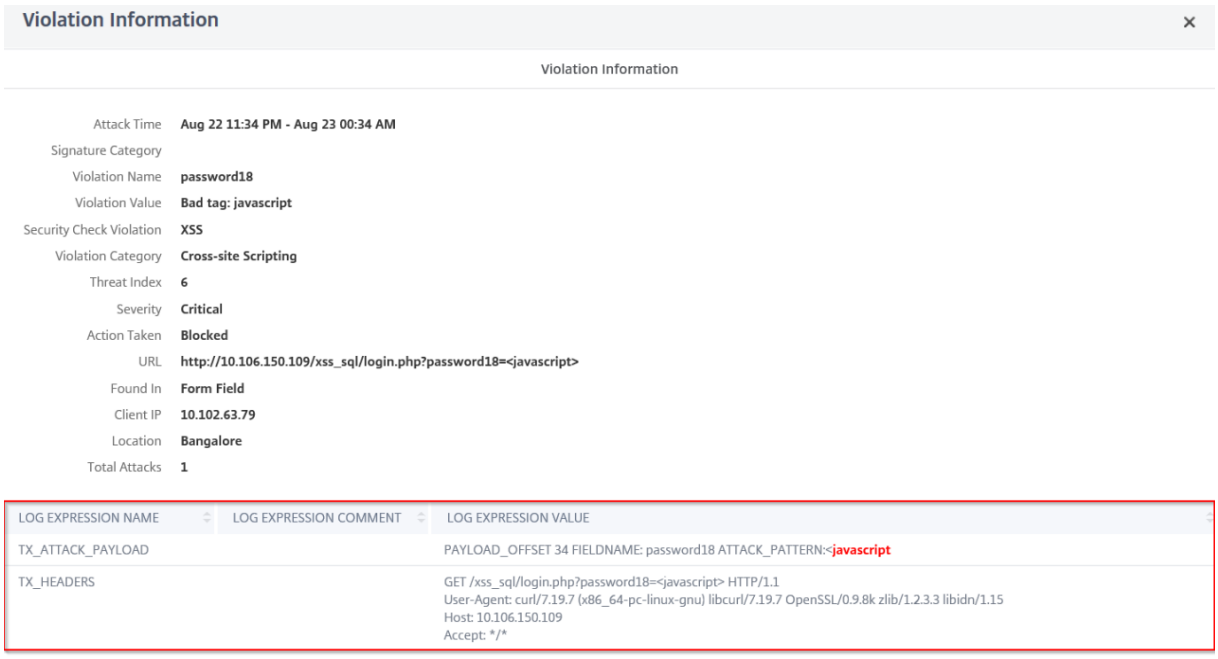
Vous pouvez désormais obtenir des détails sur les attaques telles que les en-têtes HTTP et la charge utile HTTP pour dépanner ou analyser les attaques. Pour obtenir des détails sur les attaques, vous devez mettre à jour le « VerboseLogLevel » dans le profil de pare-feu d'application, à l'aide de la commande suivante :

```
Set appfw profile <profile_name> -VerboseLogLevel (pattern|patternPayload
|patternPayloadHdr)
```

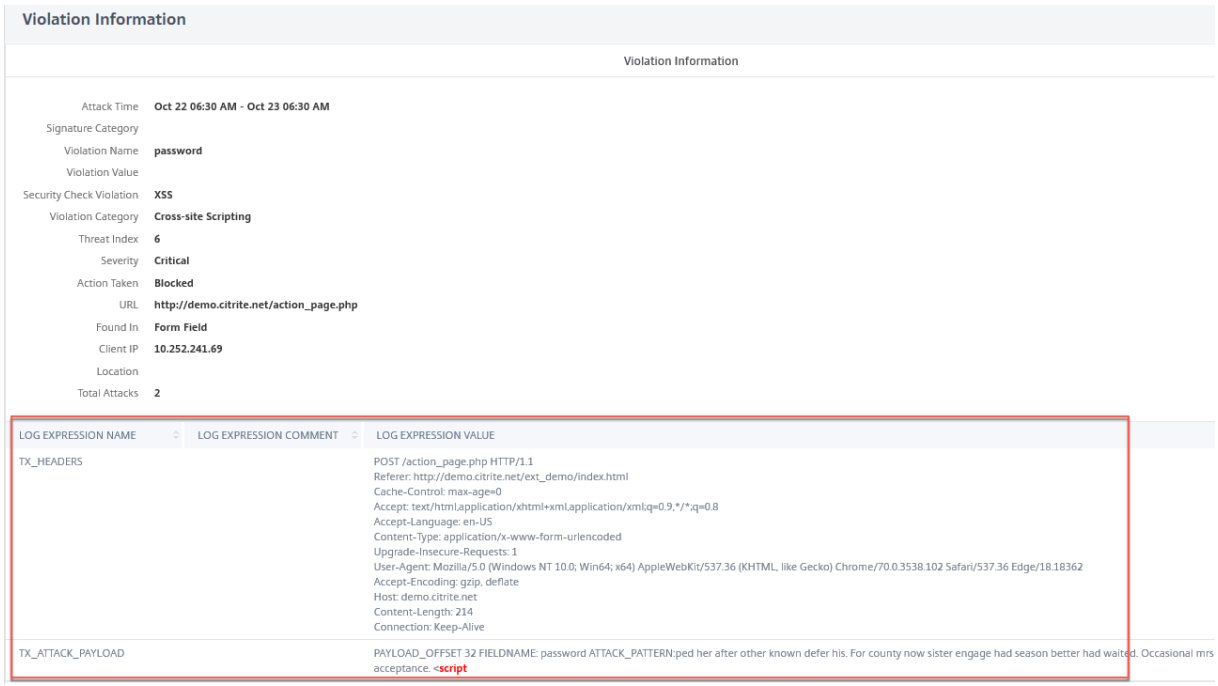
- `pattern` - Seul le motif de violation est enregistré
- `patternPayload` - Modèle de violation +150 octets de valeur d'élément de champ avant le modèle d'attaque sont enregistrés
- `patternPayloadHdr` - Modèle de violation + 150 octets de valeur d'élément de champ avant le modèle d'attaque + les en-têtes de requête HTTP sont consignés

Basé sur la configuration « VerboseLogLevel », Citrix ADM affiche les enregistrements d'expression de journal détaillés.

L'image suivante est un exemple qui met en évidence le modèle d'attaque pour la requête GET :



L'image suivante est un exemple qui met en évidence le modèle d'attaque pour la requête POST :



Dans ces deux exemples :

- **FIELDNAME** fait référence au nom de champ correspondant au modèle d'attaque.
- **PAYLOAD_OFFSET** fait référence au décalage d'attaque dans la charge utile réelle.

- **ATTACK_PATTERN** met en évidence le modèle d'attaque et inclut 150 octets de charge utile de préfixe dans la valeur.

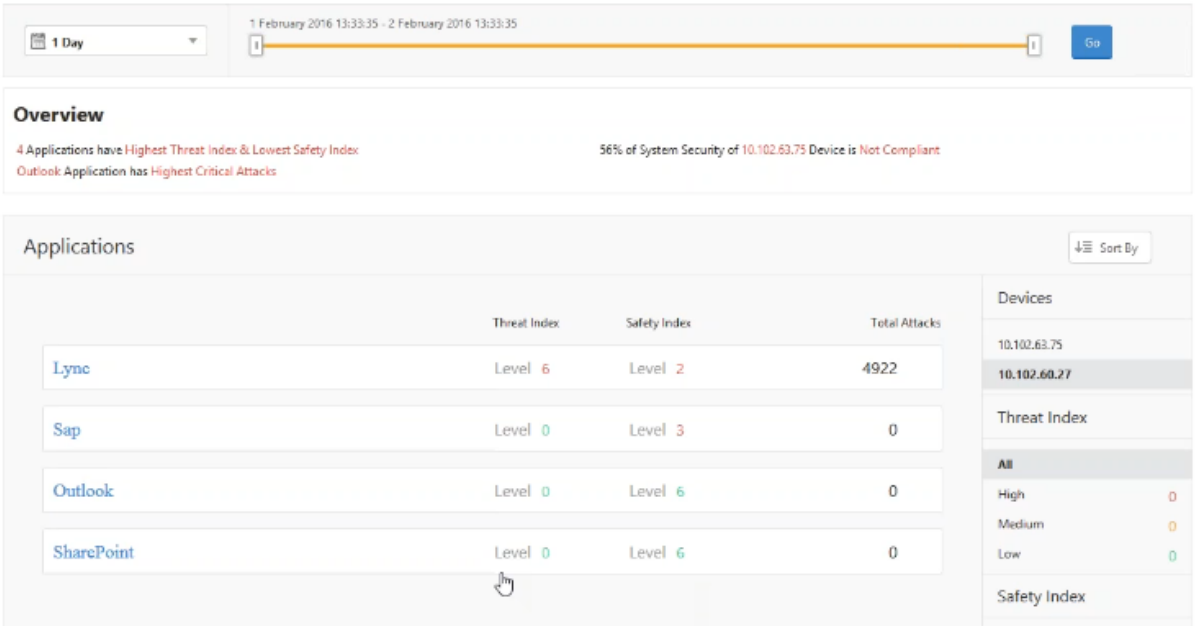
Pour plus d'informations sur la configuration du niveau de journal détaillé dans Citrix ADC, consultez Facilité de dépannage avec les journaux du pare-feu d'application Web.

Déterminer l'indice de sécurité avant de déployer la configuration

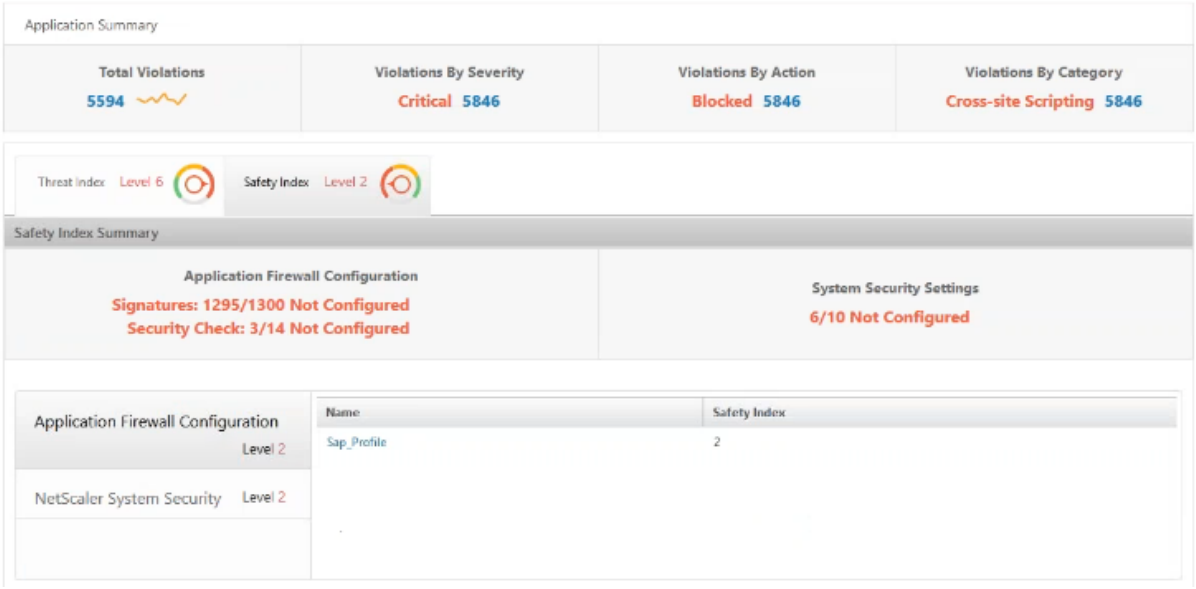
Des violations de sécurité se produisent après le déploiement de la configuration de sécurité sur une instance Citrix ADC, mais vous pouvez évaluer l'efficacité de la configuration de sécurité avant de la déployer.

Par exemple, vous pouvez évaluer l'indice de sécurité de la configuration de l'application SAP sur l'instance Citrix ADC avec l'adresse IP 10.102.60.27.

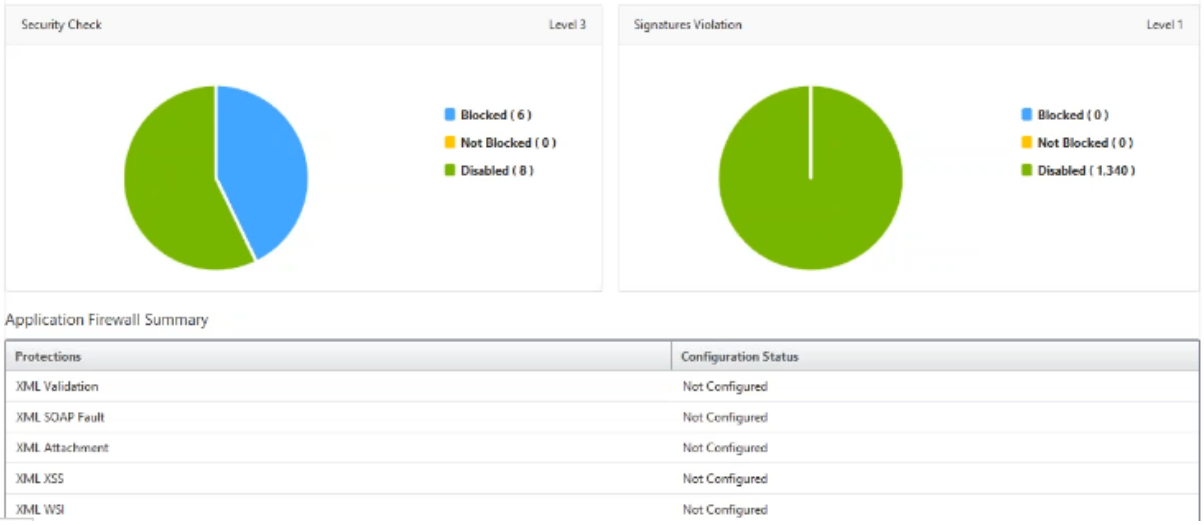
Dans le tableau de bord **Security Insight**, sous **Périphériques**, cliquez sur l'adresse IP de l'instance Citrix ADC que vous avez configurée. Vous pouvez voir que l'indice de menace et le nombre total d'attaques sont 0. L'index des menaces est un reflet direct du nombre et du type d'attaques sur l'application. Aucune attaque indique que l'application n'est soumise à aucune menace.



Cliquez sur **SAP > Indice de sécurité > Profil SAP_et** évaluez les informations relatives à l'indice de sécurité qui s'affichent.



Dans le résumé du pare-feu de l'application, vous pouvez afficher l'état de configuration des différents paramètres de protection. Si un paramètre est défini pour consigner ou si un paramètre n'est pas configuré, un indice de sécurité inférieur est attribué à l'application.



Bot

February 1, 2024

> Remarque
>
> Si votre version Citrix ADM est antérieure à **13.0-79.x**, vous pouvez afficher les informations

> sur les robots en accédant à **Analytics > Sécurité > Bot Insight**. Pour la version **13.0-79.x ou ultérieure**, vous pouvez afficher les détails du robot en accédant à **Analytics > Sécurité > Violations de sécurité > Vue d'ensemble de l'application** et en cliquant sur **Bot** sous **Répartition des applications par**.

Un bot est un logiciel qui effectue automatiquement certaines actions répétitives à un rythme beaucoup plus rapide qu'un humain. Plus de 35 % de votre trafic Web est composé de robots et 80 % des entreprises sont victimes d'attaques de robots. Ils peuvent interagir avec une page Web, soumettre des formulaires, cliquer sur des liens, numériser du texte ou télécharger du contenu. Les robots peuvent accéder à des vidéos, publier des commentaires et tweeter sur les plateformes de réseaux sociaux. Certains bots peuvent même tenir des conversations de base avec des utilisateurs humains. Ils sont connus sous le nom de chatbots.

Un bot qui effectue un service utile ou utile tel que le service à la clientèle, les chatbots, les bots de recherche sont connus comme de bons bots. Certains robots malveillants peuvent extraire ou télécharger du contenu à partir d'un site Web, voler les informations d'identification des utilisateurs, diffuser du contenu de spam et effectuer divers autres types de cyberattaques. Ces bots malveillants sont connus sous le nom de mauvais bots. Il est essentiel d'identifier les robots malveillants et de protéger votre appareil contre les attaques de sécurité avancées. Vous pouvez y parvenir en utilisant un système de gestion de bot.
Pour plus d'informations sur les robots, consultez la section Gestion des robots .

Configurer les techniques de détection de bot dans Citrix ADC

Dans Citrix ADC, vous pouvez configurer des techniques de détection des robots pour détecter le trafic de robots entrant. Voici les techniques de bot que vous configurez dans l'instance de Citrix ADC :

- **List d'autorisation**. Cette règle dispose d'une liste d'URL et d'expressions de stratégie pour évaluer si un ensemble spécifique de bons bots pouvant accéder à votre ressource Web.
- **Liste de blocage**. Cette règle dispose d'une liste d'URL et d'expressions de stratégie pour évaluer si un ensemble spécifique de bots défectueux peut accéder à votre site Web.
- **Réputation IP**. Cette règle détecte si le trafic de bot entrant est une adresse IP malveillante.
- **Empreinte digitale de l'appareil**. Cette règle détecte si le trafic de bot entrant possède l'identifiant d'empreinte digitale de l'appareil dans l'en-tête de la demande entrante et les attributs de navigateur d'un trafic de bot client entrant.
- **Limitation du débit**. Ce taux de règle limite les demandes multiples provenant du même client.
- **Signatures**. Cette règle détecte et bloque les robots en fonction de la détection des signatures. Il empêche également les URL non autorisées qui grattent les sites Web, forcent les connexions brutes et les bots qui détectent des vulnérabilités.

- **Pièges à robots**. Cette règle détecte les robots accédant au script activé sur la page Web.
- **TPS**. Cette règle détecte le trafic entrant sous forme de robots si le nombre maximal de demandes et le pourcentage d'augmentation des demandes dépassent l'intervalle de temps configuré.

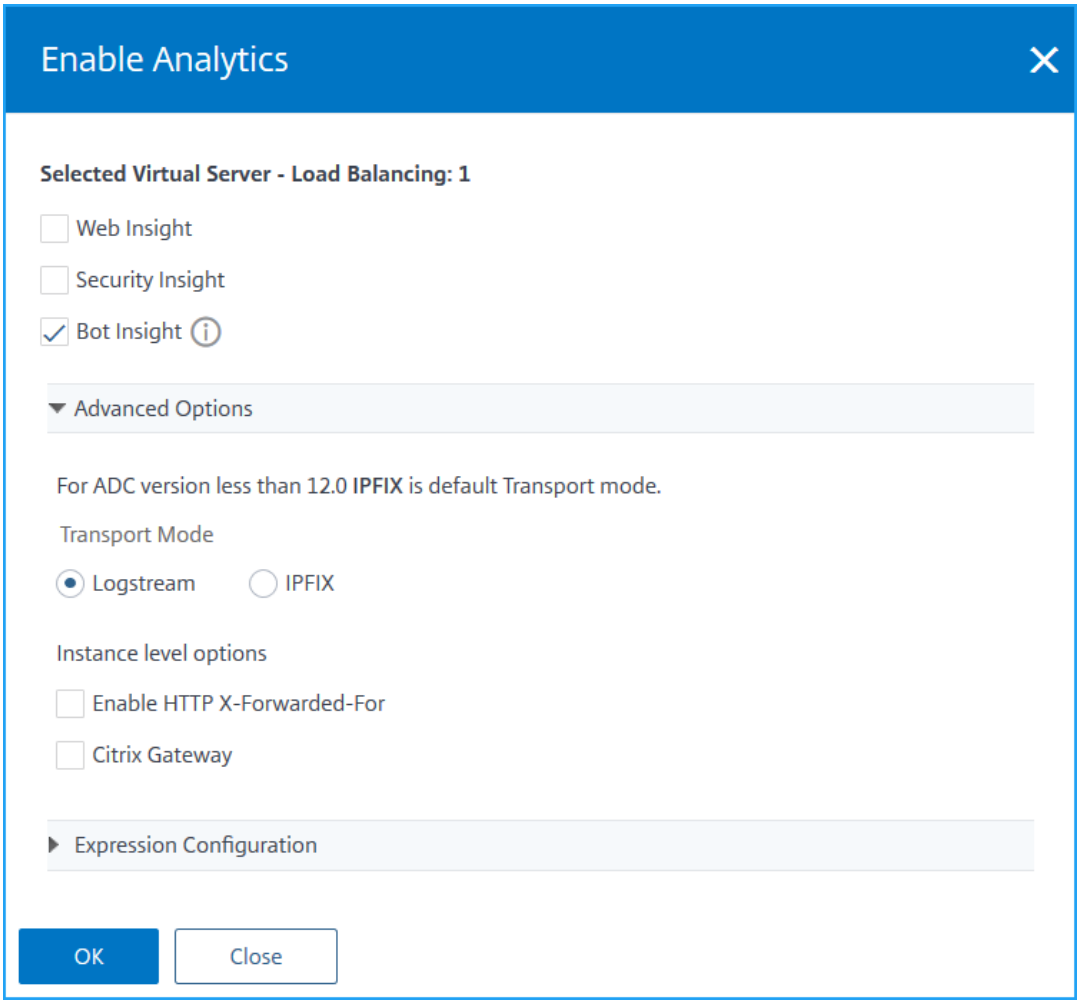
Pour plus d'informations sur la configuration de la gestion des bots, consultez Configurer la gestion des bots.

Utilisation de Bot Insight dans Citrix ADM

Après avoir configuré la gestion des bots dans Citrix ADC, vous devez activer **Bot Insight** sur les serveurs virtuels pour afficher les informations dans Citrix ADM.

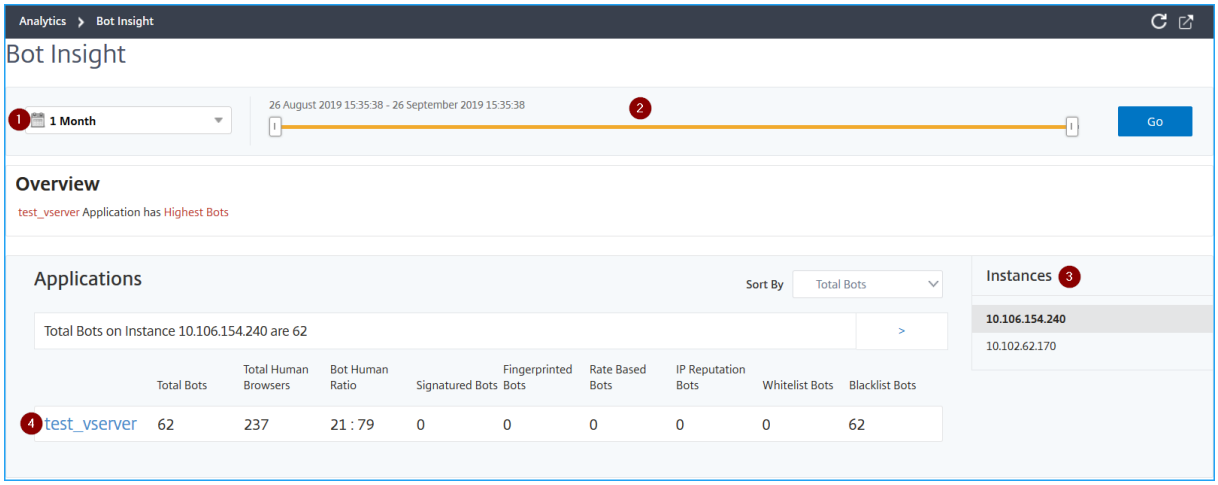
Pour activer **Bot Insight** :

1. Accédez à **Réseaux** > **Instances** > **Citrix ADC** et sélectionnez le type d'instance. Par exemple, VPX.
2. Sélectionnez l'instance et, dans la liste **Sélectionner une action**, sélectionnez **Configurer Analytics**.
3. Sélectionnez le serveur virtuel et cliquez sur **Activer les analyses**.
4. Dans la fenêtre **Activer Analytics** :
    a) Sélectionnez **Bot Insight**
    b) Sous **Option avancée**, sélectionnez **Logstream**.



c) Cliquez sur **OK**.

Après avoir activé **Bot Insight**, accédez à **Analytics** > **Bot Insight**.



1 - Liste horaire pour voir les détails du bot

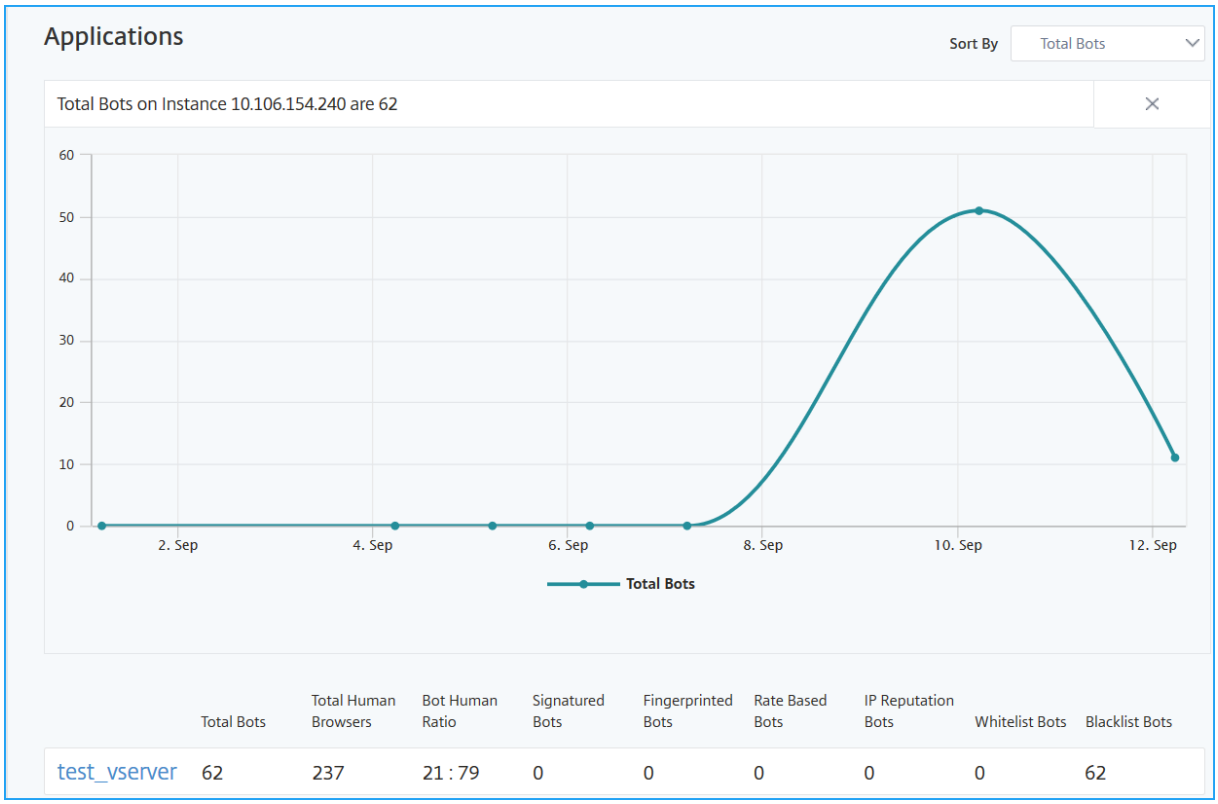
2 —Faites glisser le curseur pour sélectionner une plage de temps spécifique et cliquez sur **OK** pour afficher les résultats personnalisés

3 —Nombre total d'instances affectées par les bots

4 —Serveur virtuel pour l'instance sélectionnée avec un nombre total d'attaques de bots

- **Nombre total de bots** : indique le nombre total d'attaques de robots (y compris toutes les catégories de robots) détectées sur le serveur virtuel.
- **Nombre total de navigateurs humains** : indique le nombre total d'utilisateurs humains accédant au serveur virtuel.
- **Bot Human Ratio** —Indique le rapport entre les utilisateurs humains et les bots accédant au serveur virtuel.
- **Bots de signature**, **Bot à empreintes digitales**, **Robots basés sur le taux**, **Robots de réputation IP**, **Robots de liste d'autorisation et**bots de liste de blocage—**Indique le nombre total d'attaques de robots** se sont produites en fonction de la catégorie de bot configurée. Pour plus d'informations sur la catégorie de robots, consultez Configurer les techniques de détection des bots dans Citrix ADC.

5 - Cliquez sur **>** pour afficher les détails du bot sous forme de graphique.

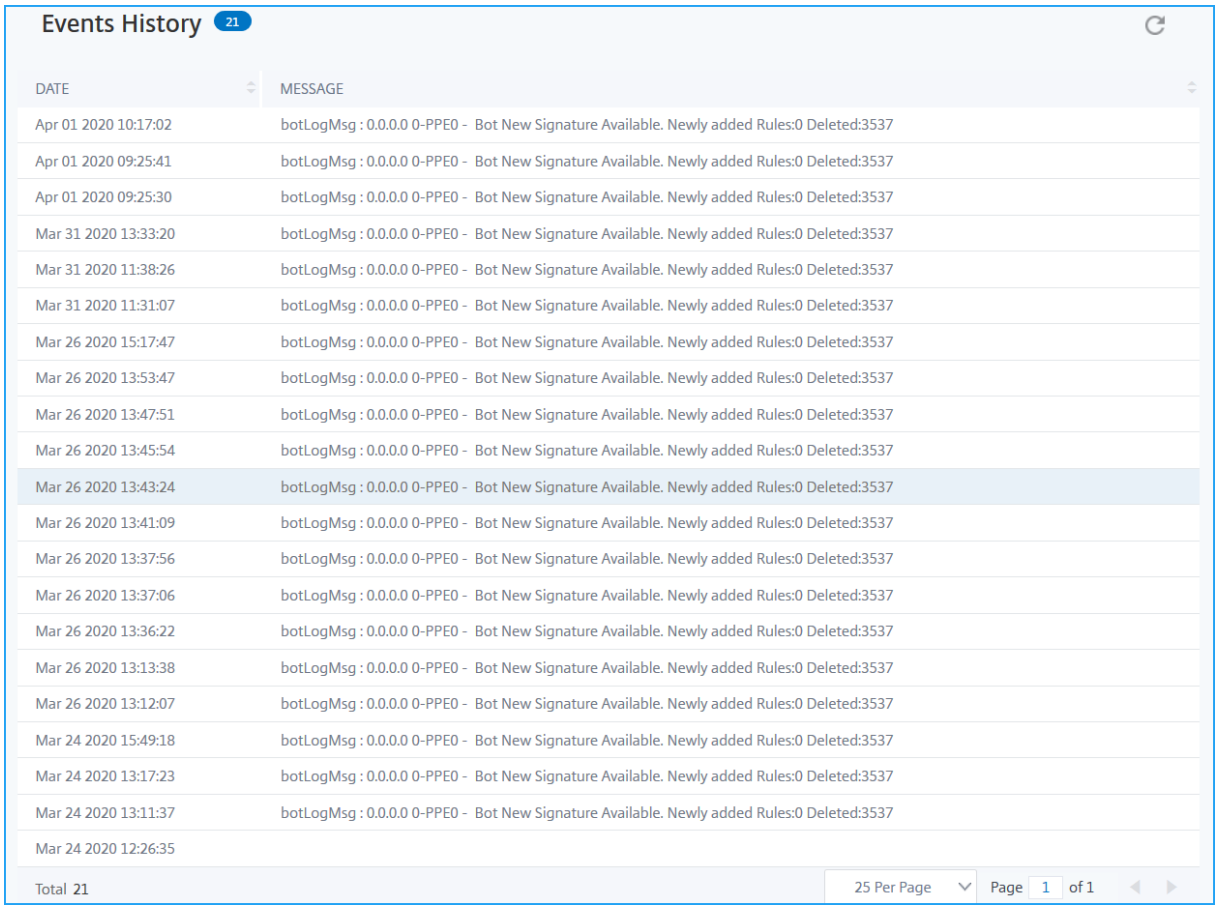


Afficher l'historique des événements

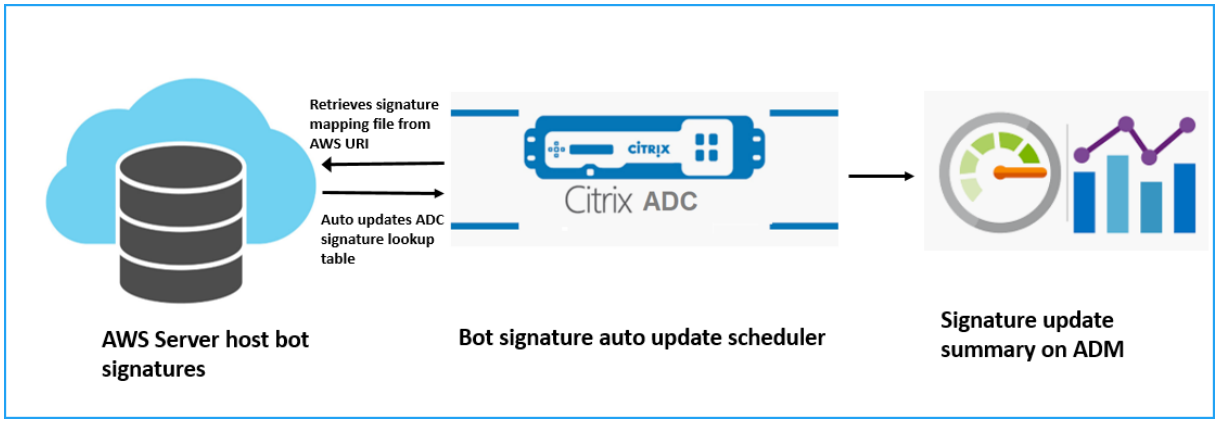
Vous pouvez consulter les mises à jour des signatures du bot dans l'**historique des événements**, lorsque :

- De nouvelles signatures de bot sont ajoutées dans les instances de Citrix ADC.
- Les signatures de bot existantes sont mises à jour dans les instances de Citrix ADC.

Vous pouvez sélectionner la durée dans la page d'aperçu des robots pour afficher l'historique des événements.



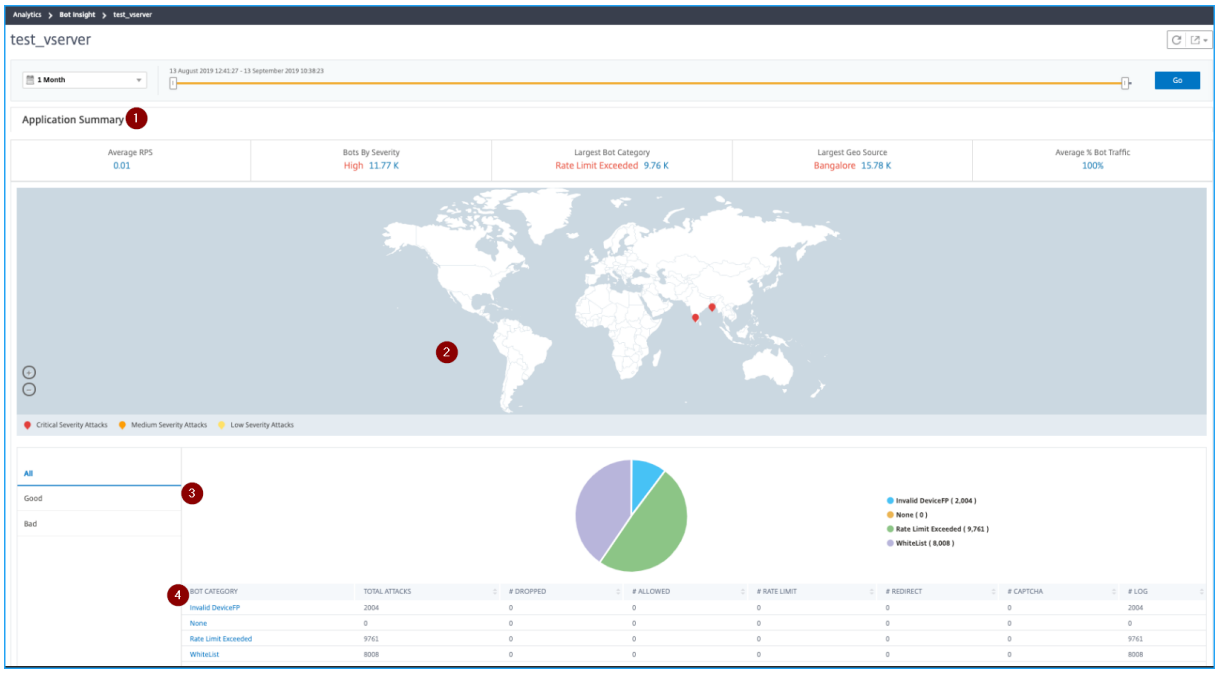
Le diagramme suivant montre comment les signatures de bot sont récupérées à partir du cloud AWS, mises à jour sur Citrix ADC et afficher le résumé de la mise à jour des signatures sur Citrix ADM.



1. Le planificateur de mise à jour automatique de la signature du bot récupère le fichier de mappage à partir de l'URI AWS.
2. Vérifie les dernières signatures du fichier de mappage avec les signatures existantes dans l'appliance ADC.
3. Télécharge les nouvelles signatures depuis AWS et vérifie l'intégrité de la signature.
4. Met à jour les signatures de bots existantes avec les nouvelles signatures dans le fichier de signature du bot.
5. Génère une alerte SNMP et envoie le résumé de la mise à jour des signatures à Citrix ADM.

Afficher les robots

Cliquez sur le serveur virtuel pour afficher le **résumé de l'application**.



1 —Fournit les détails du résumé de la demande, tels que :

- **RPS moyen** : indique le nombre moyen de demandes de transaction de bot par seconde (RPS) reçues sur les serveurs virtuels.
- **Bots par gravité** : indique que les transactions de bot les plus élevées ont eu lieu en fonction de la gravité. La gravité est classée en fonction de la gravité **critique**, **élevée**, **moyenne**et **faible**.

  Par exemple, si les serveurs virtuels comportent 11 770 robots de gravité élevée et 1 550 robots de gravité critique, Citrix ADMaffiche Critical 1,55**K sous Bots par gravité.**
- **Catégorie de bot la plus grande** —Indique les attaques de bot les plus élevées ont eu lieu en fonction de la catégorie de bot.

  Par exemple, si les serveurs virtuels ont 8000 bots répertoriés comme bloqués, 5000 bots répertoriés comme autorisés et 10000 bots de limite atteinte, Citrix ADM affiche la **limite atteinte 10 000** sous **Catégorie de bot la plus grande**.
- **Source géo la plus importante** : indique que les attaques de bot les plus élevées ont eu lieu en fonction d'une région.

  Par exemple, si les serveurs virtuels sont victimes de 5 000 attaques de robots à Santa Clara, de 7 000 attaques de robots à Londres et de 9 000 attaques de robots à Bangalore, Citrix ADM **affiche Bangalore 9** K **sous**la catégorie Largest Geo Source.
- **% moyen du trafic de bots** —Indique le ratio homme-bot.

2 —Affiche la gravité des attaques de robots en fonction des emplacements sur la carte

3 —Affiche les types d'attaques de bots (bonnes, mauvaises et toutes)

4 —Affiche le nombre total d'attaques de bots ainsi que les actions configurées correspondantes. Par exemple, si vous avez configuré :

- Plage d'adresses IP (192.140.14.9 à 192.140.14.254) en tant que bots de liste de blocs et sélectionné Drop comme action pour ces plages d'adresses IP
- Plage IP (192.140.15.4 à 192.140.15.254) en tant que bots de liste de blocage et sélectionné pour créer un message de journal en tant qu'action pour ces plages IP

  Dans ce scénario, Citrix ADM affiche :

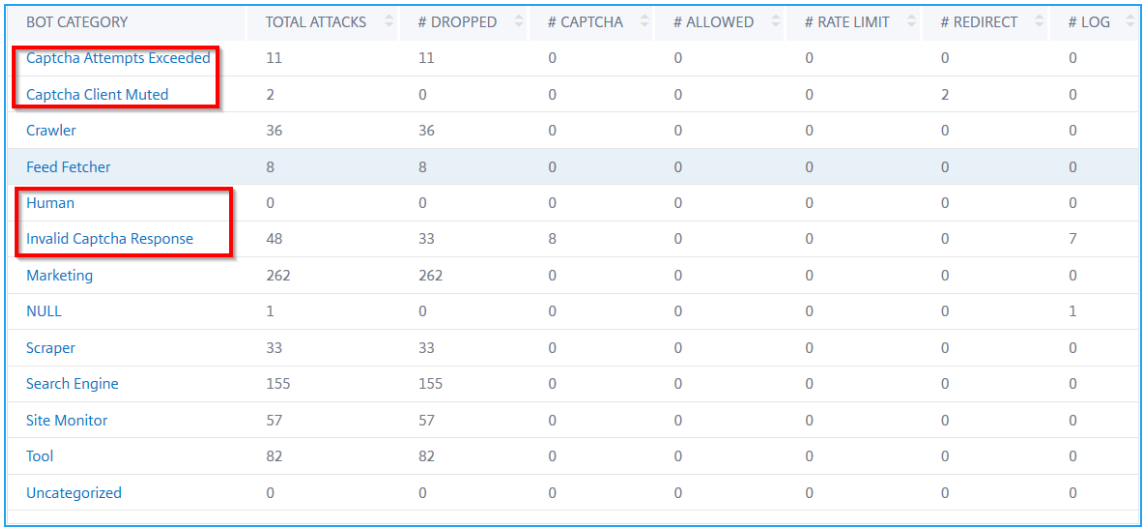
  - Total des bots listés par bloc
  - Nombre total de bots sous **Dropés**
  - Nombre total de robots **enregistrés**

Voir les robots CAPTCHA

Dans les pages Web, les CAPTCHA sont conçus pour identifier si le trafic entrant provient d'un humain ou d'un robot automatisé. Pour afficher les activités CAPTCHA dans Citrix ADM, vous devez configurer CAPTCHA en tant qu'action bot pour les techniques de réputation IP et de détection d'empreintes digitales de périphérique dans une instance de Citrix ADC. Pour plus d'informations, consultez la section Gestion des bots.

Voici les activités CAPTCHA que Citrix ADM affiche dans Bot insights :

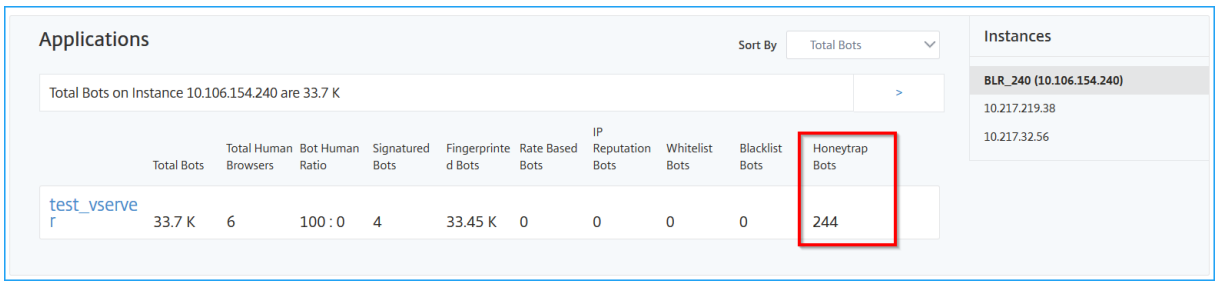
- Tentatives de**captcha dépassées** —**Indique le nombre maximum de tentatives** CAPTCHA effectuées après un échec de connexion
- **Client Captcha muet** —Indique le nombre de demandes client abandonnées ou redirigées parce que ces demandes ont été détectées comme de mauvais robots plus tôt dans le cadre du défi CAPTCHA
- **Humain** —Indique les entrées de captcha effectuées par les utilisateurs humains
- **Réponse captcha non valide** : indique le nombre de réponses CAPTCHA incorrectes reçues du robot ou de l'humain, lorsque Citrix ADC envoie un défi CAPTCHA



BOT CATEGORY	TOTAL ATTACKS	# DROPPED	# CAPTCHA	# ALLOWED	# RATE LIMIT	# REDIRECT	# LOG
Captcha Attempts Exceeded	11	11	0	0	0	0	0
Captcha Client Muted	2	0	0	0	0	2	0
Crawler	36	36	0	0	0	0	0
Feed Fetcher	8	8	0	0	0	0	0
Human	0	0	0	0	0	0	0
Invalid Captcha Response	48	33	8	0	0	0	7
Marketing	262	262	0	0	0	0	0
NULL	1	0	0	0	0	0	1
Scraper	33	33	0	0	0	0	0
Search Engine	155	155	0	0	0	0	0
Site Monitor	57	57	0	0	0	0	0
Tool	82	82	0	0	0	0	0
Uncategorized	0	0	0	0	0	0	0

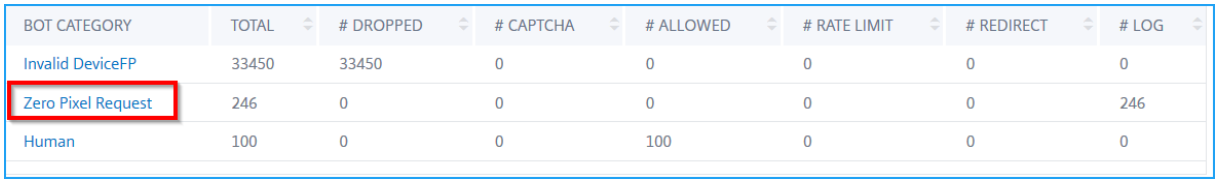
Voir les robots de piégeage de bot

Pour afficher les interruptions de bot dans Citrix ADM, vous devez configurer l'interruption de bot dans l'instance Citrix ADC. Pour plus d'informations, consultez la section Gestion des bots.



Pour identifier les interruptions des robots, un script est activé dans la page Web et ce script est caché à l'humain, mais pas aux bots. Citrix ADM identifie et signale les interruptions de robot, lorsque ce script est accessible par les robots.

Cliquez sur le serveur virtuel et sélectionnez **Zero Pixel Request**

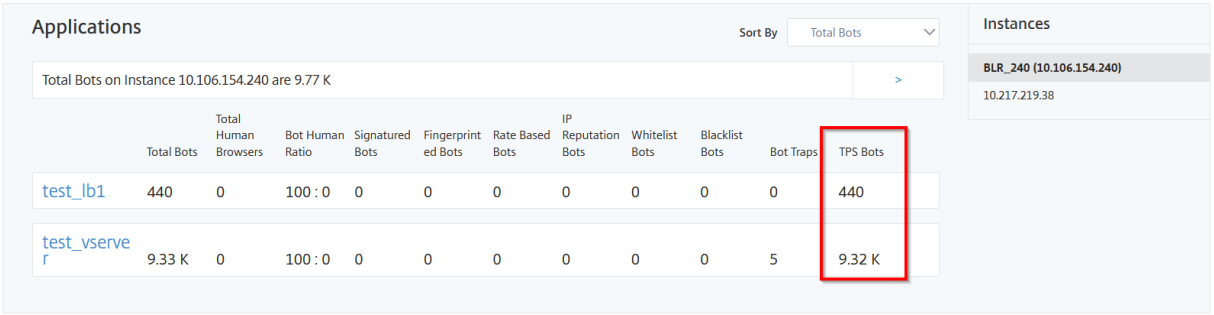


Voir les robots TPS

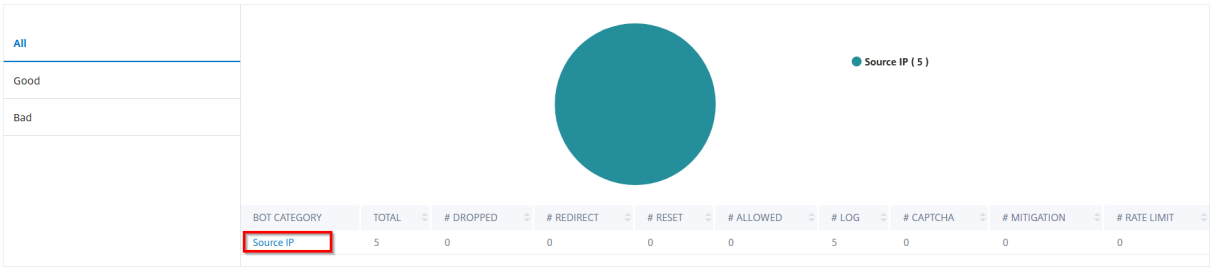
Voici les catégories de bot TPS que vous pouvez afficher dans Citrix ADM :

- IP source
- Localisation géographique
- Hôte
- Adresse URL

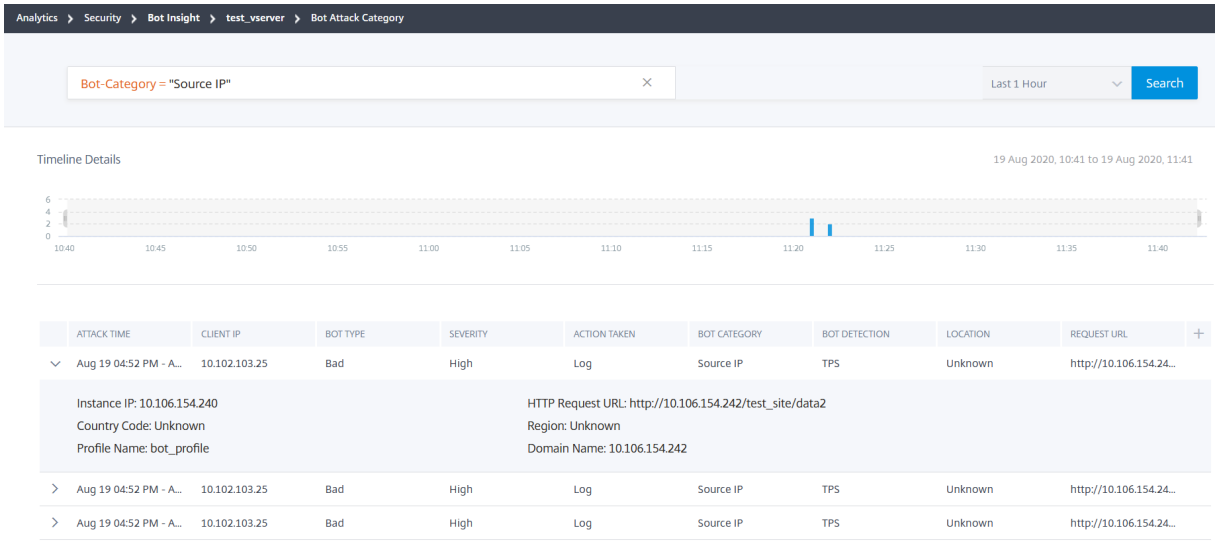
Cliquez sur le serveur virtuel pour afficher les robots TPS.



Cliquez sur la **catégorie de bot TPS** pour afficher les détails du robot.



La page de détails s'affiche.



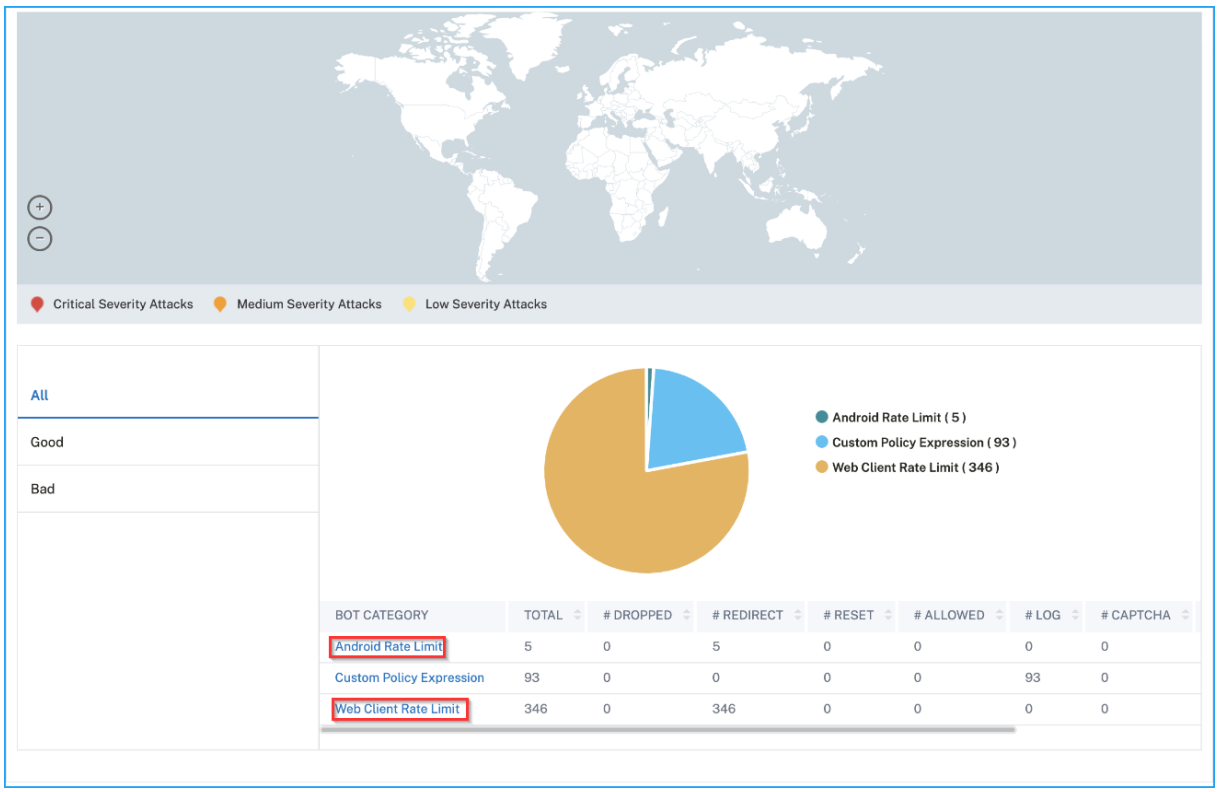
Afficher les catégories de robots pour les applications mobiles (Android)

Pour afficher les robots des applications mobiles (Android), vous devez configurer la technique de détection d'empreintes digitales dans Citrix ADC. Pour plus d'informations, consultez Configurer la technique d'empreinte digitale de l'appareil pour les applications mobiles.

Après avoir configuré les paramètres dans Citrix ADC, vous pouvez afficher les catégories de robots suivantes dans Citrix ADM :

- Limite de débit client Web
- Limite de débit Android
- Périphérique client Web
- Appareil Android

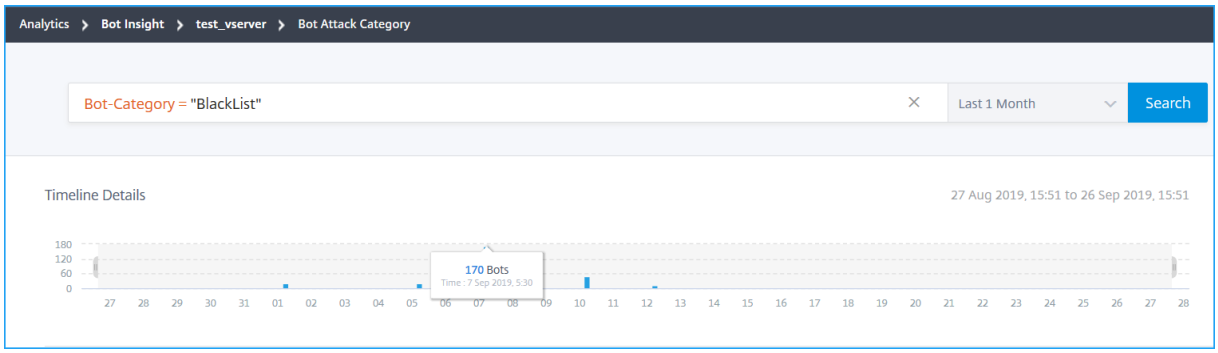
Cliquez sur le serveur virtuel pour afficher les catégories de robots applicables à l'application mobile.



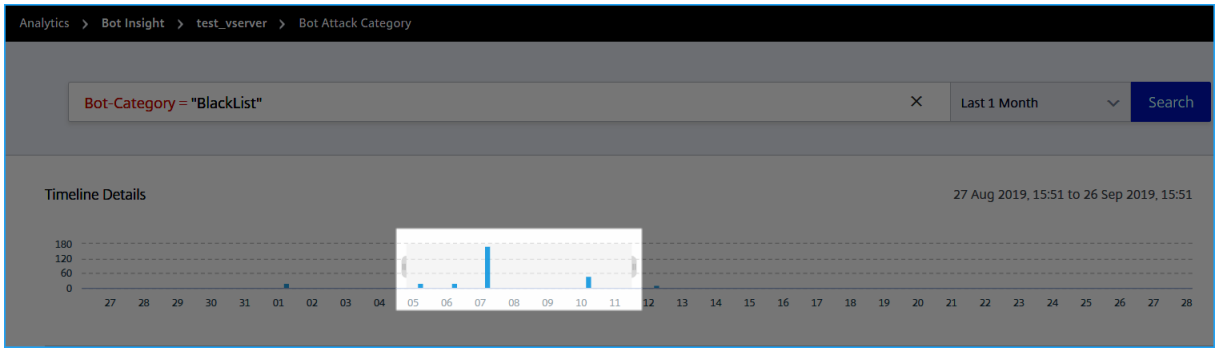
Afficher les détails du bot

Pour plus de détails, cliquez sur le type d'attaque de bot sous **Catégorie de bot**. Par exemple, si vous souhaitez afficher les détails des attaques de robots répertoriées en bloc, cliquez sur **Liste de blocage** sous **Catégorie de bot**.

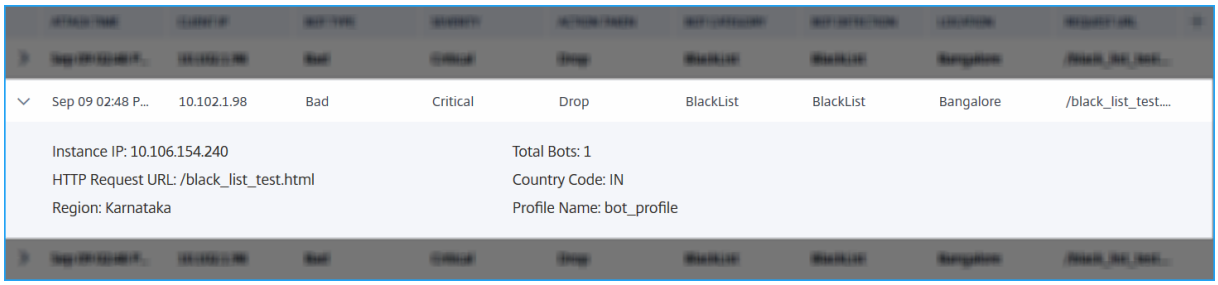
Les détails tels que le temps d'attaque et le nombre total d'attaques par bot sont affichés.



Vous pouvez également faire glisser le graphique à barres pour sélectionner la plage de temps spécifique à afficher pour les attaques de robots.



Pour obtenir des informations supplémentaires sur l'attaque de bot, cliquez pour développer.



- **IP de l'instance** —Indique l'adresse IP de l'instance Citrix ADC
- **Total Bots** —Indique le nombre total d'attaques de bots se sont produites pendant cette période.
- **URL de requête HTTP** —Indique l'URL configurée pour être répertoriée en bloc
- **Code pays** —Indique le pays où l'attaque par bot s'est produite
- **Région** —Indique la région où l'attaque du bot s'est produite
- **Nom du profil** —Indique le nom du profil que vous avez fourni lors de la configuration

Recherche avancée

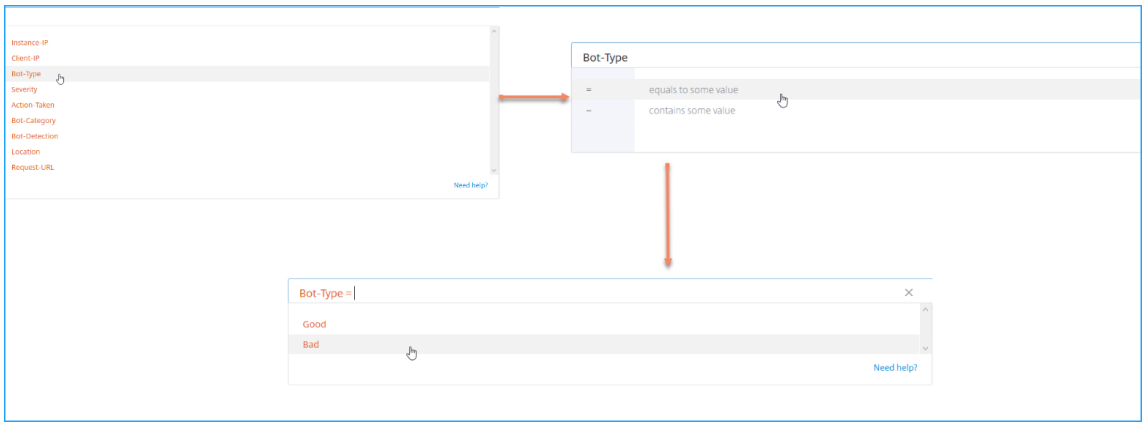
Vous pouvez également utiliser la zone de texte de recherche et la liste des durées, où vous pouvez afficher les détails du bot selon vos besoins. Lorsque vous cliquez sur le champ de recherche, celui-ci affiche la liste suivante de suggestions de recherche.

- **Instance-IP : adresse IP** de l'instance Citrix ADC
- **Client-IP** —Adresse IP du client
- **Type de bot** : type de bot, bon ou mauvais
- **Severity** —Gravité de l'attaque de bot
- **Action-Taken** –action entreprise après l'attaque du bot, par exemple Drop, Aucune action, Redirection

- **Bot-Category** –catégorie de l'attaque de bot, telle que liste de blocage, liste d'autorisation, empreinte digitale, etc. En fonction d'une catégorie, vous pouvez y associer une action de bot
- **Bot-Detection** —Types de détection de bot (liste de blocage, liste d'autorisation, etc.) que vous avez configurés sur l'instance Citrix ADC
- **Lieu** —Région/pays où l'attaque du bot s'est produite
- **Request-URL** —URL qui contient les attaques de bot possibles

Vous pouvez également utiliser des opérateurs dans vos requêtes de recherche pour affiner le focus de votre recherche. Par exemple, si vous souhaitez voir tous les robots malveillants :

1. Cliquez sur le champ de recherche et sélectionnez **Bot-Type**
2. Cliquez à nouveau sur le champ de recherche et sélectionnez l'opérateur **=**
3. Cliquez à nouveau sur la zone de recherche et sélectionnez **Bad**
4. Cliquez sur **Rechercher** pour afficher les résultats



Afficher les détails des violations de sécurité des applications

February 1, 2024

Les applications Web exposées à Internet sont devenues très vulnérables aux attaques. Citrix ADM vous permet de visualiser les détails des violations exploitables pour protéger les applications contre les attaques. Accédez à **Analytics** > **Sécurité> Violations** de sécurité pour une solution à volet unique pour :

- Visualisez les applications avec une visibilité totale sur les détails des menaces associés à la fois dans les informations de sécurité et les informations sur les robots

- Accéder aux violations de sécurité des applications en fonction de ses catégories telles que **Network**, **Bot**et **WAF**
- Prendre des mesures correctives pour sécuriser les applications

La page **Violations de sécurité** comporte les options suivantes :

- **Vue d'ensemble des applications** : affiche une vue d'ensemble des applications qui présentent des violations totales, des violations totales de WAF et de bot, des violations par pays, etc. Pour plus d'informations, consultez Vue d'ensemble de l'application.
- **Toutes les violations** : affiche les détails de la violation de sécurité de l'application. Pour plus d'informations, consultez Toutes les violations.

Conditions préalables

Vérifiez que **Metrics Collector** est activé. Par défaut, **Metrics Collector** est activé sur l'instance de Citrix ADC. Pour plus d'informations, consultez Configurer l'analyse intelligente des applications.

SSL Insight

February 1, 2024

SSL Insight fournit une visibilité sur les transactions Web sécurisées (HTTPS) et permet aux administrateurs informatiques de surveiller toutes les applications Web sécurisées desservies par l'Citrix ADC en fournissant une surveillance intégrée et en temps réel et historique des transactions Web sécurisées. Avec cette visibilité, l'administrateur peut évaluer les éléments suivants :

- **Déterminer l'impact des modifications de configuration sur l'utilisation par les clients** : l'administrateur peut comprendre l'impact sur les clients d'une modification de configuration, telle que la désactivation de SSLv3 ou la suppression d'un chiffrement tel que RC4-MD5. Cela peut être fait en évaluant les données de transaction historiques sur ce protocole et en chiffrement.
- **Quantifier les performances du client** : l'administrateur peut comprendre l'impact sur le temps de réponse de l'application en fonction des chiffres/protocoles SSL utilisés ou des certificats négociés.
- **Sécurité des applications** : évaluez si l'une des applications a des transactions exécutées sur des protocoles de sécurité faibles, des chiffrements ou une faible force de clé.

Lorsque SSL Analytics est activé sur une instance Citrix ADC, les statistiques SSL sont enregistrées et consignées pour chaque transaction SSL. Les statistiques montrent les détails du flux SSL. En outre,

chaque connexion réussie est enregistrée et affichée par Citrix Application Delivery Management (ADM)
Analytics.

SSL Insight fournit les informations critiques suivantes, affichées par Citrix ADM Analytics :

- Version du protocole SSL négociée
- Chiffrement négocié et force du chiffrement
- Algorithme de hachage de signature du certificat utilisé
- Type et taille du certificat
- Erreurs SSL frontales et dorsales

> **Remarque**
>
> Pour des connexions SSL réussies, la journalisation SSL AppFlow a lieu à la fin de chaque transaction.

Conditions préalables

- L'instance Citrix ADC sur laquelle vous souhaitez configurer SSL Insight doit exécuter le logiciel Citrix ADC version 11.1 51.21 et supérieure. Exécutez les commandes suivantes sur l'instance ADC exécutant 11.1 51.21 pour activer Logstream en tant que type de transport pour SSL Insight.

1. `enable ns mode ulfd`
2. `add ulfd server <IP Address of the ADM>`

   Pour les instances ADC exécutant la version 12.0 et supérieure, sélectionnez Logstream comme type de transport tout en activant AppFlow à partir d'ADM.

- La version et le build de Citrix ADM doivent être égaux ou supérieurs à la version et au build de Citrix ADC. Par exemple, si vous avez installé Citrix ADM 11.1 build 61.7, assurez-vous d'avoir installé Citrix ADC 11.1 build 60.14 ou version antérieure.

Configurer SSL Insight

Les mesures SSL Insight sont incluses dans les rapports Web Insight si vous activez les éléments suivants :

- Activez AppFlow pour Web Insight sur chaque instance de Citrix ADC.
- Activez le mode ULFD sur chaque instance de Citrix ADC.
- Activez les paramètres AppFlow requis sur chaque instance de Citrix ADC.

Activer la fonctionnalité AppFlow

> **Remarque**
>
> Vous pouvez activer la fonctionnalité AppFlow à partir de Citrix ADM ou de chaque instance Citrix ADC.

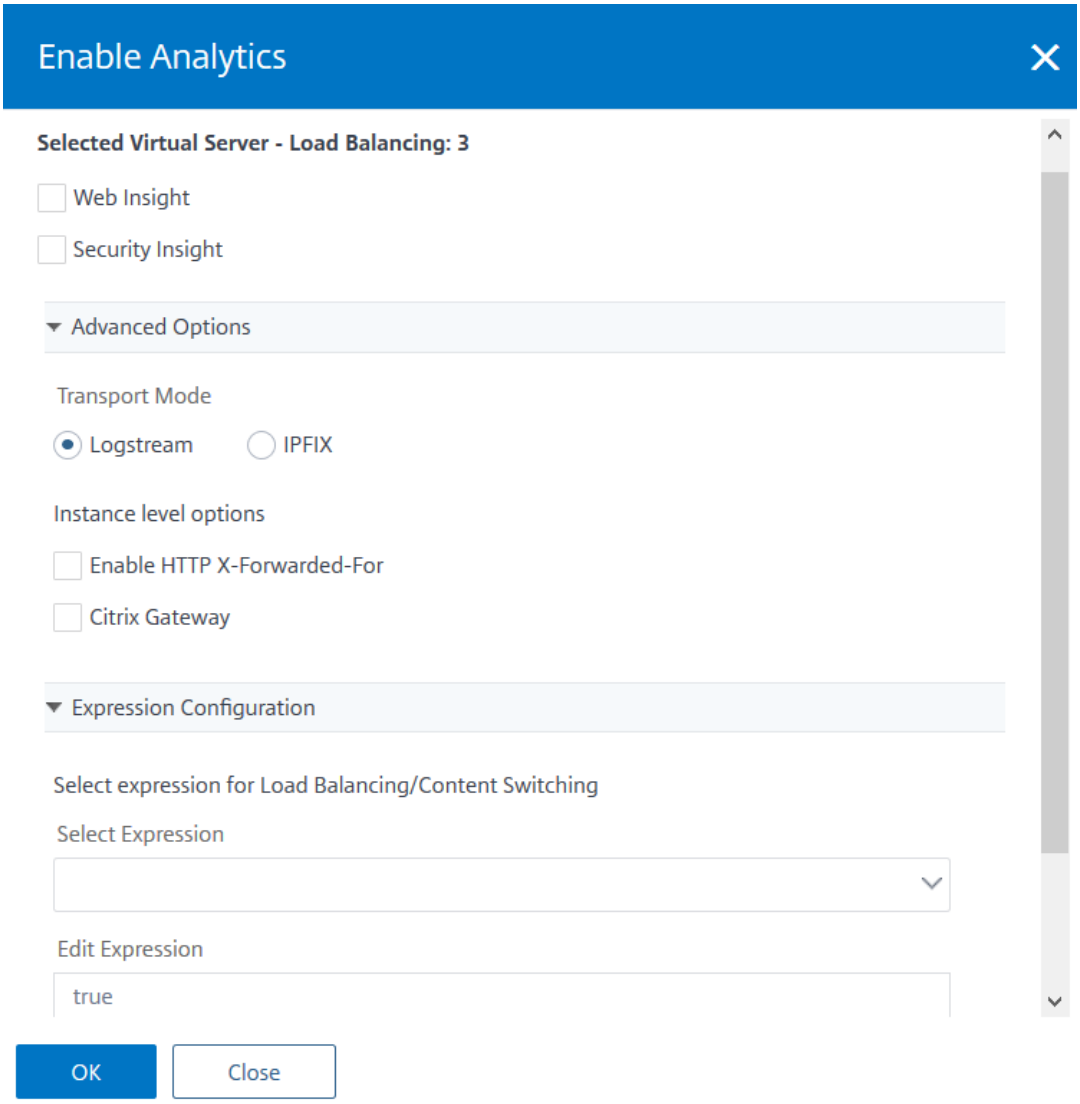
Pour activer la fonctionnalité AppFlow à partir de Citrix ADM :

Si votre Citrix ADM est **13.0 Build 41.x ou version ultérieure** :

1. Accédez à **Réseaux** > **Instances** > **Citrix ADC**, puis sélectionnez le type d'instance. Par exemple, VPX.
2. Sélectionnez l'instance et dans la liste **Sélectionner une action**, cliquez sur **Configurer Analytics**.
3. Dans la page **Configurer l'analyse sur les serveurs virtuels**, sélectionnez le serveur virtuel, puis cliquez sur **Activer l'analyse**.
4. Dans la fenêtre **Activer Analytics** :
   a) Sélectionnez **Web Insight**
   b) Sélectionnez **Logstream** comme mode de transport

      > **Remarque**
      >
      > Pour Citrix ADC 12.0 ou version antérieure, **IPFIX** est l'option par défaut pour le mode de transport. Pour Citrix ADC 12.0 ou version ultérieure, vous pouvez sélectionner **Logstream** ou **IPFIX** comme mode de transport.
      >
      > Pour plus d'informations sur IPFIX et Logstream, consultez la section Présentation de Logstream .

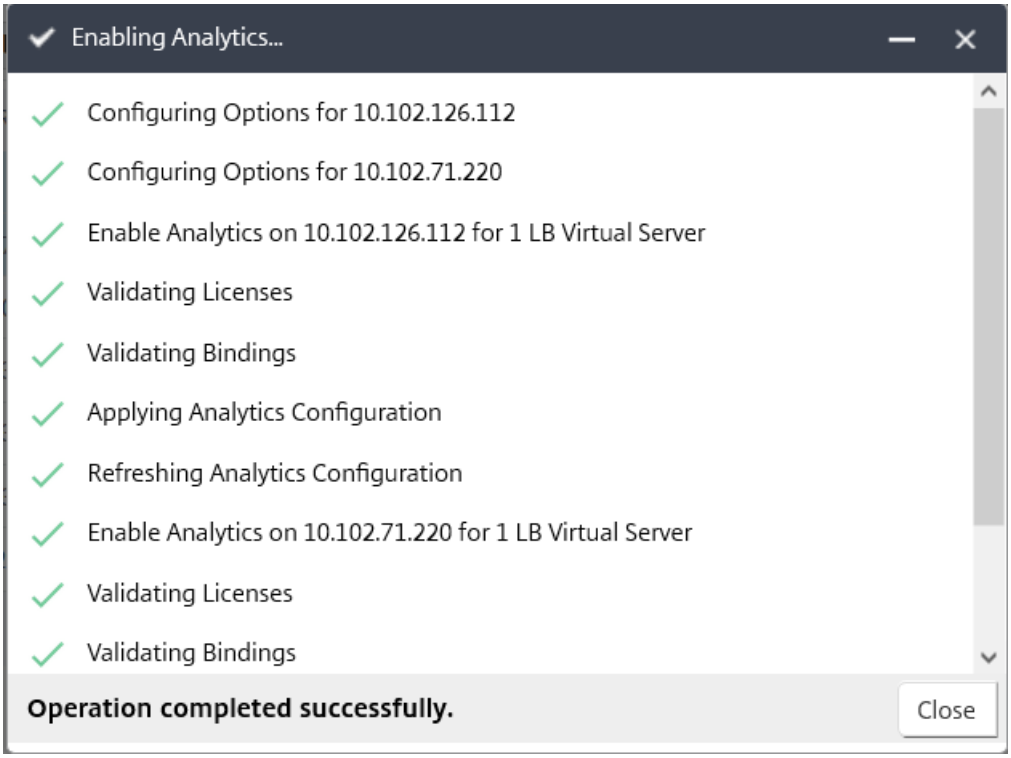
   c) L'expression est true par défaut
   d) Cliquez sur **OK**.



Remarque

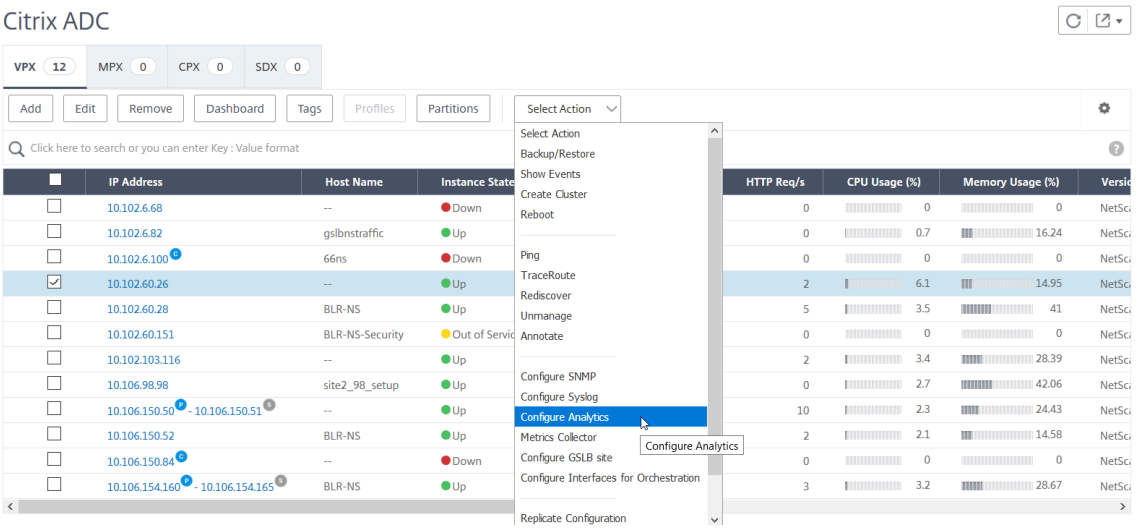
- Si vous sélectionnez des serveurs virtuels qui ne sont pas sous licence, Citrix ADM octroie d'abord des licences à ces serveurs virtuels, puis active les analyses
- Pour les partitions d'administration, seul **Web Insight** est pris en charge
- Pour les serveurs virtuels tels que la redirection du cache , l'authentification et le GSLB , vous ne pouvez pas activer les analyses. Un message d'erreur s'affiche.

Après avoir cliqué sur **OK**, Citrix ADM traite pour activer les analyses sur les serveurs virtuels sélectionnés.



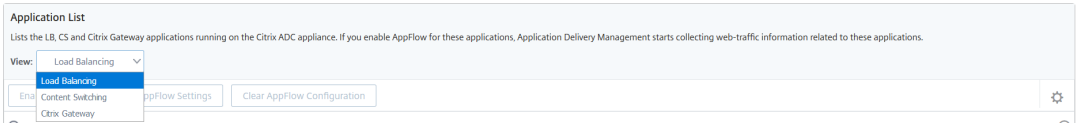
Si votre Citrix ADM est **13.0 Build 36.27 ou une version antérieure** :

1. Accédez à **Réseaux** > **Instances** > **Citrix ADC**, puis sélectionnez l'instance Citrix ADC sur laquelle vous souhaitez activer l'analyse.
2. Dans la liste **Sélectionner une action**, sélectionnez **Configurer Analytics**.

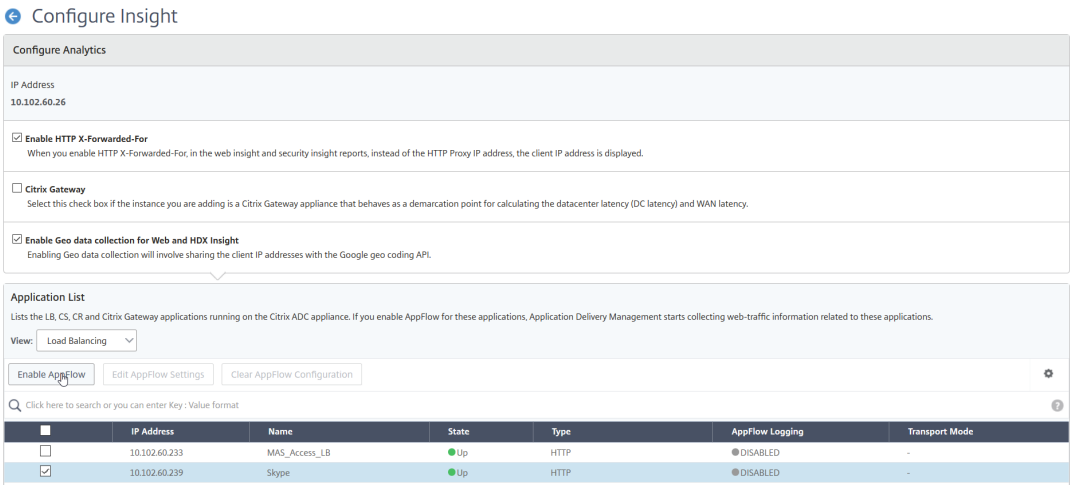


3. Sur la page **Configurer Insight** :

   a) Sélectionnez la **liste des applications** pour l'équilibrage de charge ou la commutation de contenu.



b) Sélectionnez le serveur virtuel et cliquez sur **Activer AppFlow**.

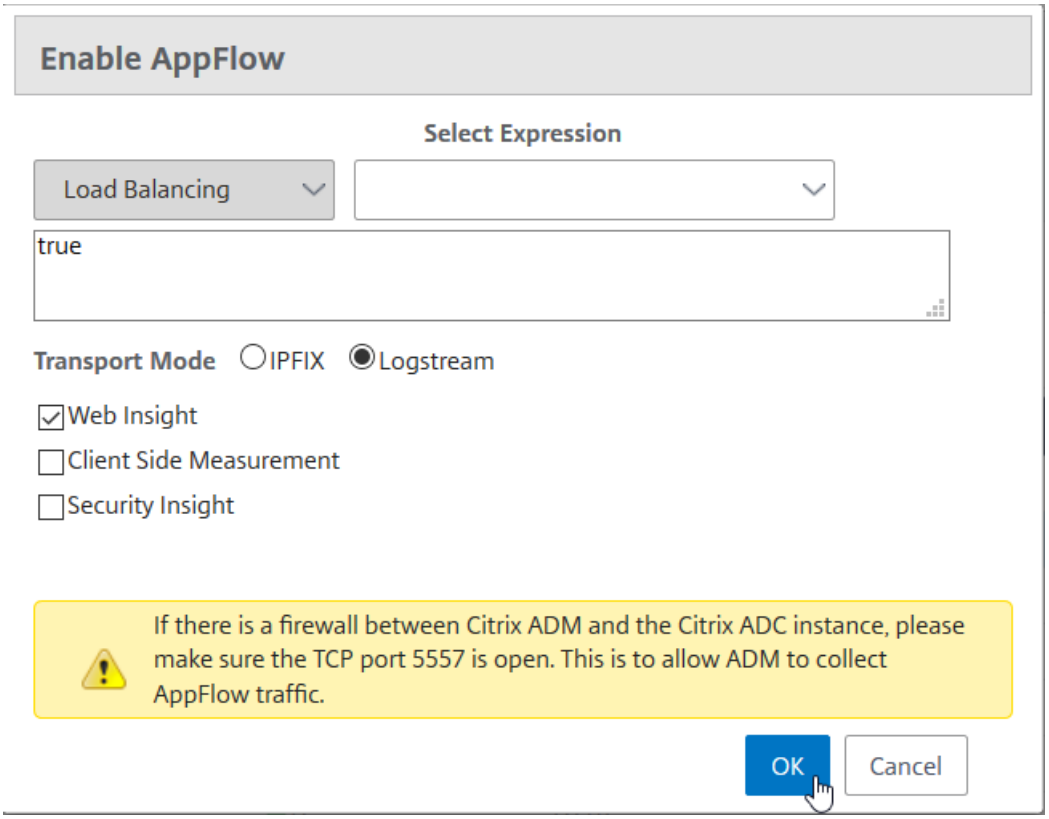


4. Dans la boîte de dialogue Activer AppFlow :

   - Entrez **true** dans la zone de texte
   - Sélectionnez **Logstream** comme mode de transport

     > Remarque : Citrix vous recommande de sélectionner Logstream comme mode de transport.

   - Sélectionnez **Web Insight** et cliquez sur **OK**.



Pour activer la fonctionnalité AppFlow à l'aide de l'interface utilisateur graphique Citrix ADC :

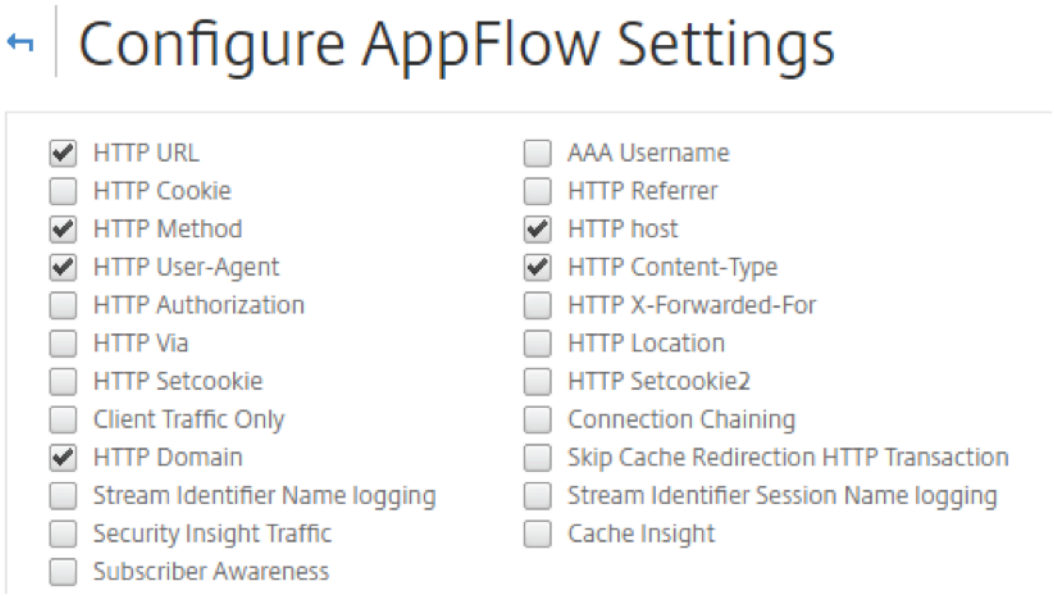
Dans l'interface graphique d'une instance Citrix ADC, accédez à **Configuration** > **Système** > **Paramètres**, cliquez sur **Configurer les fonctionnalités avancées**, puis sélectionnez **AppFlow**.

Activer les paramètres SSL Insight

Sur chaque instance Citrix ADC, vous devez activer certains paramètres HTTP pour afficher les enregistrements SSL Insight dans Citrix ADM.

Pour activer les paramètres SSL Insight à partir de l'utilitaire de configuration Citrix ADC :

1. Accédez à **Configuration** > **Système** > **AppFlow**, puis cliquez sur **Modifier les paramètres d'AppFlow**.
2. Cochez les cases suivantes : **Domaine HTTP**, **Hôte HTTP**, **Méthode HTTP**, **URL HTTP**, **Agent utilisateur HTTP**, Type de **contenu HTTP**.
3. Cliquez sur **OK**.



Afficher les métriques SSL Insight

Les mesures SSL Insight dans Citrix ADM fournissent une vue détaillée des performances des transactions SSL servies par les instances Citrix ADC. Vous pouvez afficher les mesures SSL Insight au niveau du client, du serveur ou de l'application, ainsi que les mesures des transactions de succès et d'échec SSL. À l'aide de ces mesures, vous pouvez analyser et optimiser vos paramètres **HTTPS Citrix ADC** et vos paramètres de certificat SSL, et suivre les problèmes de performances.

> **Remarque**
>
> Lorsque vous créez un groupe, vous pouvez affecter des rôles au groupe, fournir un accès au niveau de l'application au groupe et affecter des utilisateurs au groupe. Citrix ADM Analytics prend désormais en charge l'autorisation basée sur l'adresse IP virtuelle. Vos utilisateurs peuvent désormais voir des rapports pour tous les Insights uniquement pour les applications (serveurs virtuels) pour lesquelles ils sont autorisés. Pour plus d'informations sur les groupes et l'affectation d'utilisateurs au groupe, consultez Configurer des groupes.

Pour surveiller les mesures SSL Insight dans Citrix ADM :

Vous pouvez afficher les mesures SSL pour :

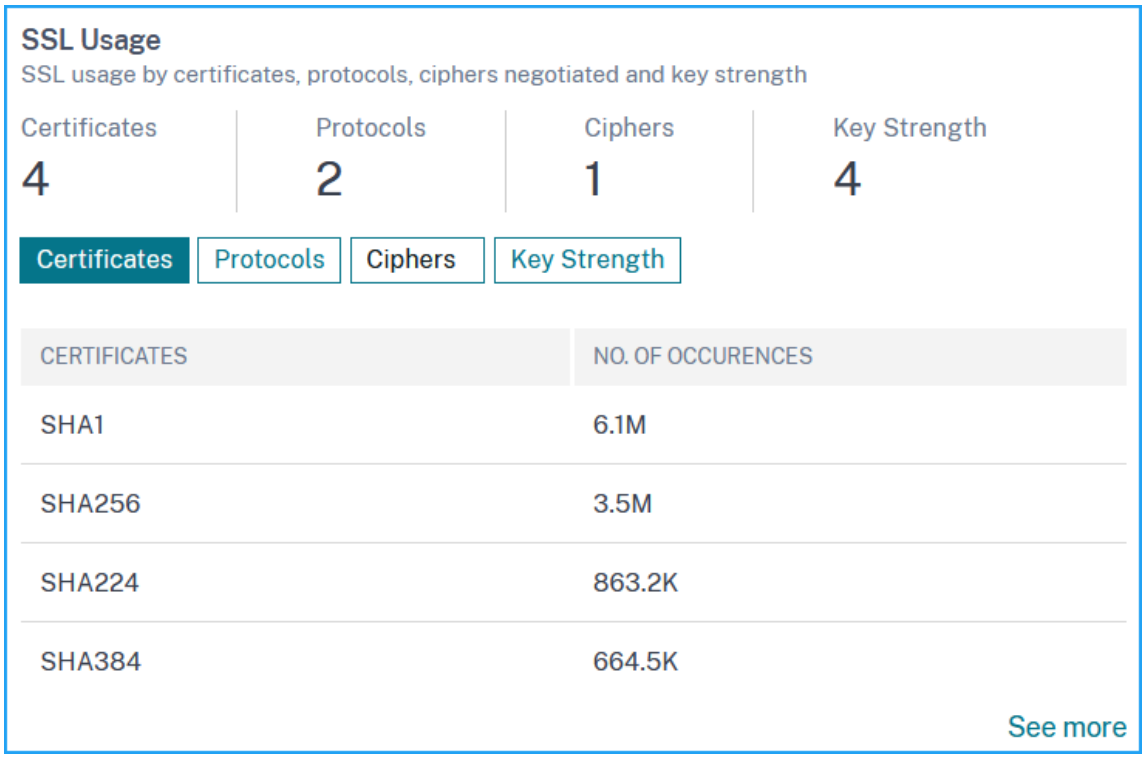
- Une application. Accédez à **Applications > Tableau de bord**, cliquez sur une application, puis sélectionnez l'onglet **Web Insight** pour afficher les mesures détaillées. Pour plus d'informations, consultez Analyse de l'utilisation des applications.
- Toutes les applications. Accédez à **Applications > Web Insight** et cliquez sur **les onglets Applications** et **clients** pour afficher les mesures SSL.

Cas d'utilisation : obtenir un aperçu des transactions SSL

Le cas d'utilisation suivant décrit comment utiliser SSL Insight pour évaluer l'utilisation de divers paramètres SSL et améliorer les mesures de sécurité.

Considérez que vous disposez d'un ensemble d'applications qui utilisent des transactions SSL (HTTPS) pour la communication et que vous avez configuré Citrix ADM pour surveiller les composants SSL. Il se peut que vous deviez examiner fréquemment les demandes afin que vous puissiez d'abord vous concentrer sur les applications qui nécessitent le plus d'attention. Le tableau de bord **Web Insight** d'une ou de toutes les applications fournit un résumé des paramètres SSL suivants sous **Erreurs SSL** et **utilisation SSL** :

- Certificats SSL
- Protocoles SSL
- Chiffrement SSL
- Force des clés SSL
- Défaillance SSL —Frontal
- Échec SSL —Back end

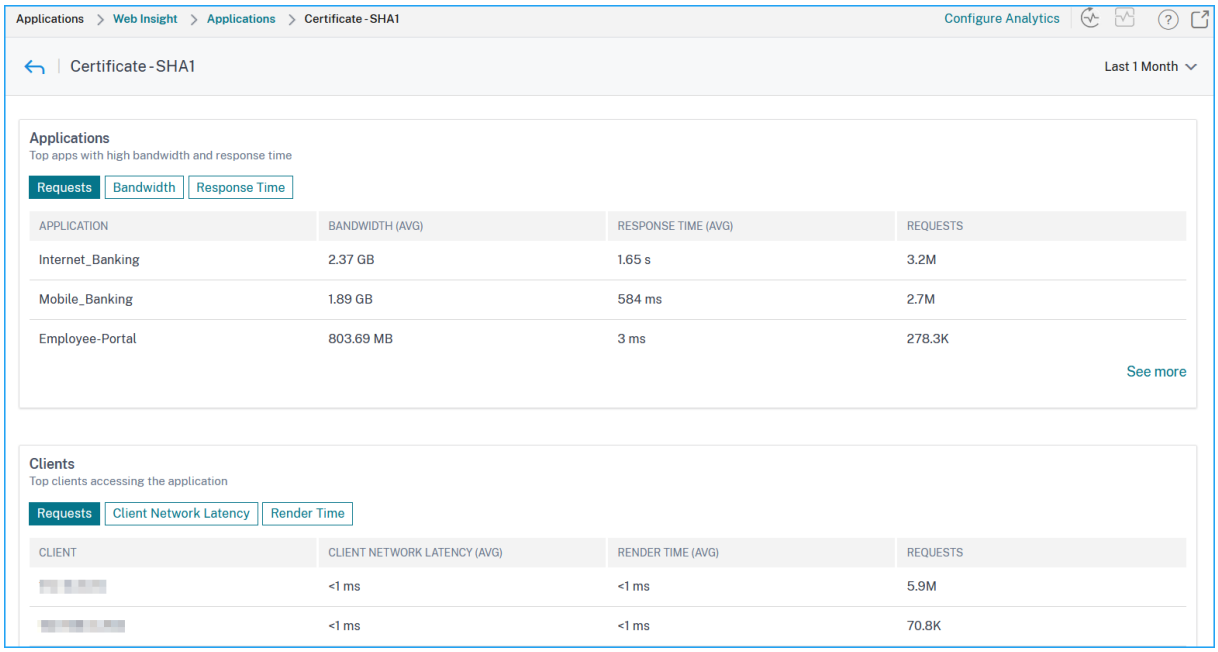


Vous pouvez cliquer sur chaque onglet pour afficher les détails.

Cas d'utilisation : métriques SSL pour les clients

Vous pouvez voir la liste des clients (identifiés par leur adresse IP) et le nombre total d'occurrences par client. Accédez à **Applications > Web Insight** et sélectionnez l'onglet **Clients** pour afficher les détails sous **Utilisation SSL**.

Cliquez sur une mesure pour afficher les détails et sous **Clients**, cliquez sur n'importe quelle adresse IP du client pour afficher les mesures SSL du client sélectionné.



TCP Insight

February 1, 2024

La fonctionnalité TCP Insight de Citrix Application Delivery Management (ADM) fournit une solution simple et évolutive pour surveiller les mesures des techniques d'optimisation et des stratégies (ou algorithmes) de contrôle de la congestion utilisées dans les appliances Citrix ADC afin d'éviter la congestion réseau dans la transmission des données. Cette fonctionnalité utilise la fonctionnalité « TCP Speed Report », qui mesure les performances de téléchargement ou de chargement de fichiers TCP avec et sans optimisation TCP.

Vous pouvez consulter les principales mesures de la **couche de transport** , telles que le volume de données, le débit et la vitesse, et utiliser ces informations pour mesurer le volume de trafic desservi par les instances Citrix ADC et valider les avantages de l'optimisation TCP. Des ventilations par direction de flux (du client vers Citrix ADC et Citrix ADC vers le serveur d'origine), du port TCP et du réseau local virtuel sont fournies pour les mesures ci-dessus.

Conditions préalables

Avant de commencer à configurer la fonctionnalité TCP Insight, assurez-vous que les conditions préalables suivantes sont remplies :

- Les instances Citrix ADC s'exécutent sur la version logicielle 11.1 build 51.21 ou ultérieure.
- Vous avez installé Citrix ADM s'exécutant sur la version 11.1 build 51.21 ou ultérieure du logiciel.
- Tous les serveurs virtuels configurés pour une application sont sous licence pour la gestion et la surveillance sur Citrix ADM.
  Pour plus d'informations sur les licences Citrix ADM, consultez la section Licences.

Activation de TCP Insight

Avant de pouvoir afficher les métriques TCP Insight, vous devez activer la fonctionnalité sur Citrix ADM.

Pour activer TCP Insight :

1. Dans un navigateur Web, tapez l'adresse IP de l'appliance virtuelle Citrix ADM (par exemple, http://192.168.100.1).
2. Dans **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Accédez à **Analytics** > **Paramètres**, puis cliquez sur **Activer les fonctionnalités pour Analytics** .
4. Sur la page **Activer les fonctionnalités pour Analytics**, sélectionnez **Activer TCP Insight** .
5. Dans la fenêtre de confirmation, cliquez sur **OK**.

Afficher les métriques TCP Insight dans Citrix ADM

Après avoir activé TCP Insight dans Citrix ADM, vous pouvez afficher les informations clés de la couche de transport telles que le mode de trafic (données Internet ou mobiles), le volume de données, le débit, les interfaces, les ports, la vitesse de téléchargement moyenne, la vitesse de téléchargement moyenne.

Pour afficher les mesures TCP Insight dans Citrix ADM :

Accédez à **Analytics** > **TCP Insight** .

Vous pouvez placer le pointeur de la souris sur les graphiques à barres pour afficher le volume de données des techniques de transport correspondantes. Vous pouvez également afficher le volume de données et d'autres mesures dans le tableau situé sous le graphique.

> **Remarque** Vous pouvez personnaliser les mesures affichées dans le graphique à l'aide de l'icône des paramètres du tableau. Vous pouvez également sélectionner la période à laquelle les mesures se rapportent et utiliser le curseur temporel pour ajuster la période.

Vous pouvez également consulter des mesures concernant des éléments tels que les interfaces, les ports et les débits en les sélectionnant dans la liste **TCP Insight** .

Cas d'utilisation

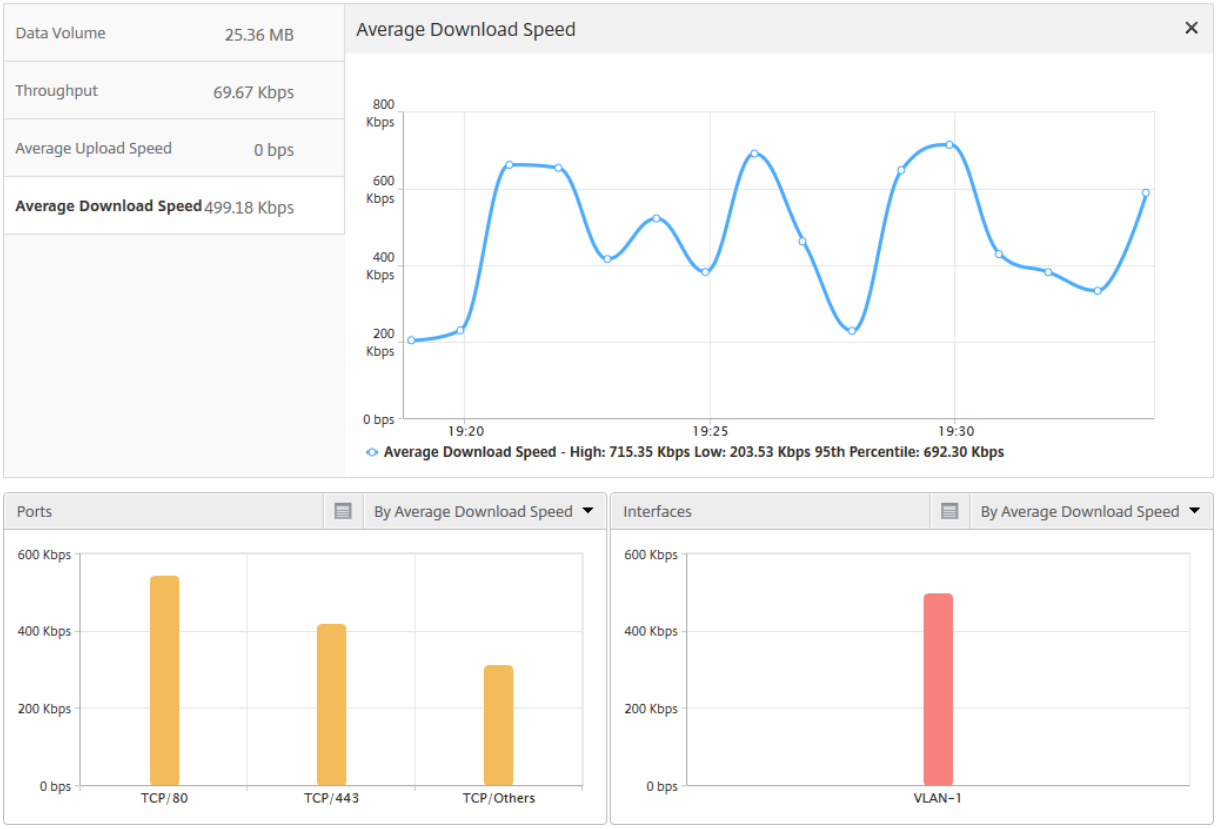
Les cas d'utilisation suivants illustrent certaines des manières d'utiliser TCP Insight sur les appliances Citrix ADC :

- Évaluez les avantages de l'optimisation TCP
- Régler les paramètres TCP
- Mesurer l'impact de l'optimisation TCP sur le volume de trafic

Évaluez les avantages de l'optimisation TCP

Dans quelle mesure l'optimisation TCP de Citrix ADC bénéficie-t-elle réellement à un réseau mobile (radio) ou d'entreprise (Internet) ? Vous pouvez visualiser la vitesse des transferts de données effectués via TCP et comparer les performances optimisées et non optimisées. Ces mesures sont affichées séparément pour les directions de téléchargement et de téléchargement (toujours côté radio/client), et pour différents ports de destination, HTTP (80) et HTTPS (443).
En examinant les métriques TCP Insight, vous pouvez quantifier l'amélioration de la vitesse obtenue grâce à l'optimisation des flux TCP.

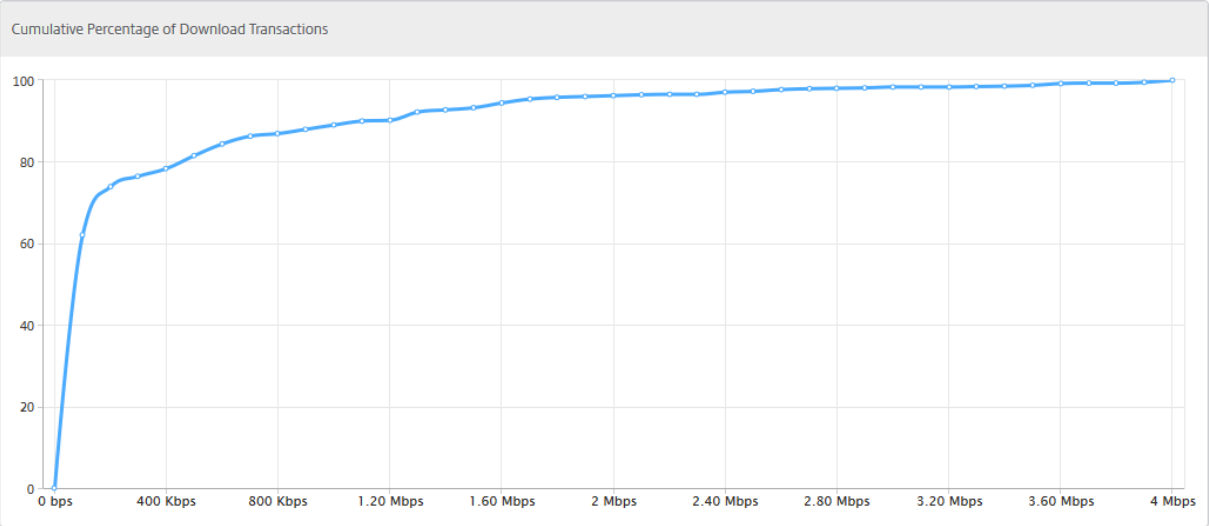
Pour afficher un résumé de ces paramètres, connectez-vous à Citrix ADM et cliquez sur l'onglet **TCP Insight**. Ensuite, cliquez sur **Côtés** et sélectionnez **Internet** ou **Radio** dans le graphique à barres ou dans le tableau situé sous le graphique.



Régler les paramètres TCP

L'utilisation de différents profils TCP peut générer des sorties différentes pour le même trafic. Dans de telles situations, vous pouvez consulter et comparer les mesures de vitesse des périodes pendant lesquelles Citrix ADC exécute différents profils d'optimisation TCP. Vous pouvez utiliser les résultats pour ajuster les paramètres TCP afin d'accélérer la transmission et développer un profil TCP qui maximise l'expérience perçue par les utilisateurs sur un réseau client spécifique.

Pour afficher les rapports, connectez-vous à Citrix ADM. Ensuite, sous l'onglet **TCP Insight**, cliquez sur **Taux de débit**et sélectionnez le débit souhaité dans le graphique à barres ou dans le tableau sous le graphique.

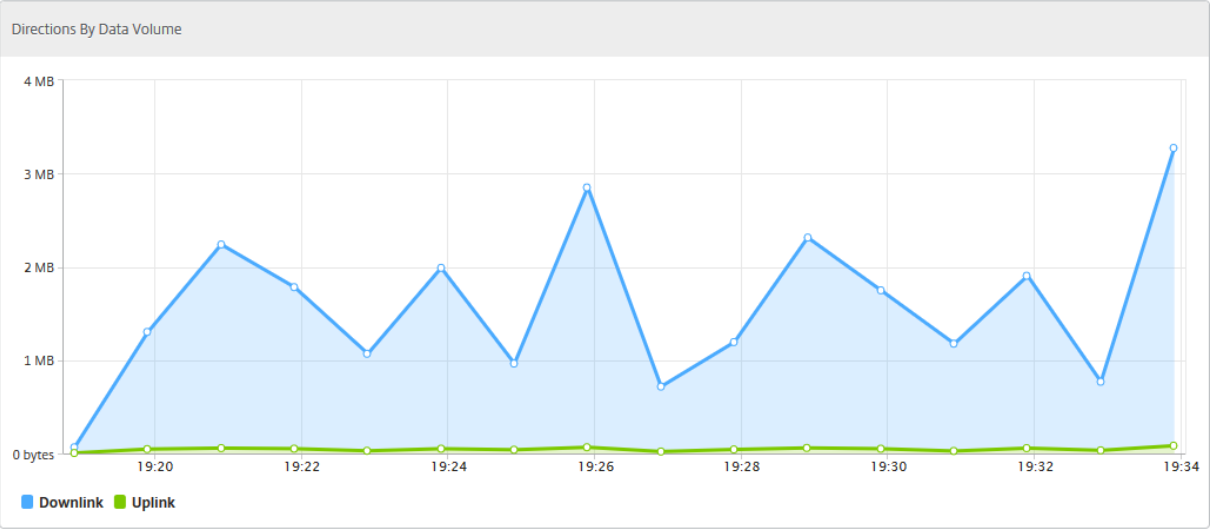


Mesurer l'impact de l'optimisation TCP sur le volume de trafic

Les mesures du volume/débit de données de la couche IP gérées par une instance Citrix ADC peuvent être comparées entre différentes périodes afin d'évaluer l'effet de l'optimisation TCP sur la consommation de données des abonnés. Les mesures peuvent être appliquées séparément pour chaque côté du réseau (côté radio ou côté Internet), pour différents segments de trafic (délimités par différentes interfaces ou VLAN), pour chaque direction (liaison descendante ou liaison montante) et pour différents ports de destination (HTTP et HTTPS). La comparaison peut être utilisée pour confirmer que l'optimisation du protocole TCP encourage les abonnés à consommer davantage de données.

Pour obtenir un résumé des mesures, connectez-vous à Citrix ADM et, dans l'onglet **TCP Insight**, cliquez sur **Sides**, puis sélectionnez **Internet** ou **Radio** dans le graphique à barres ou dans le tableau situé sous le graphique.

Vous pouvez également sélectionner une autre période dans la liste des heures. Vous pouvez personnaliser la période à l'aide du curseur de période.



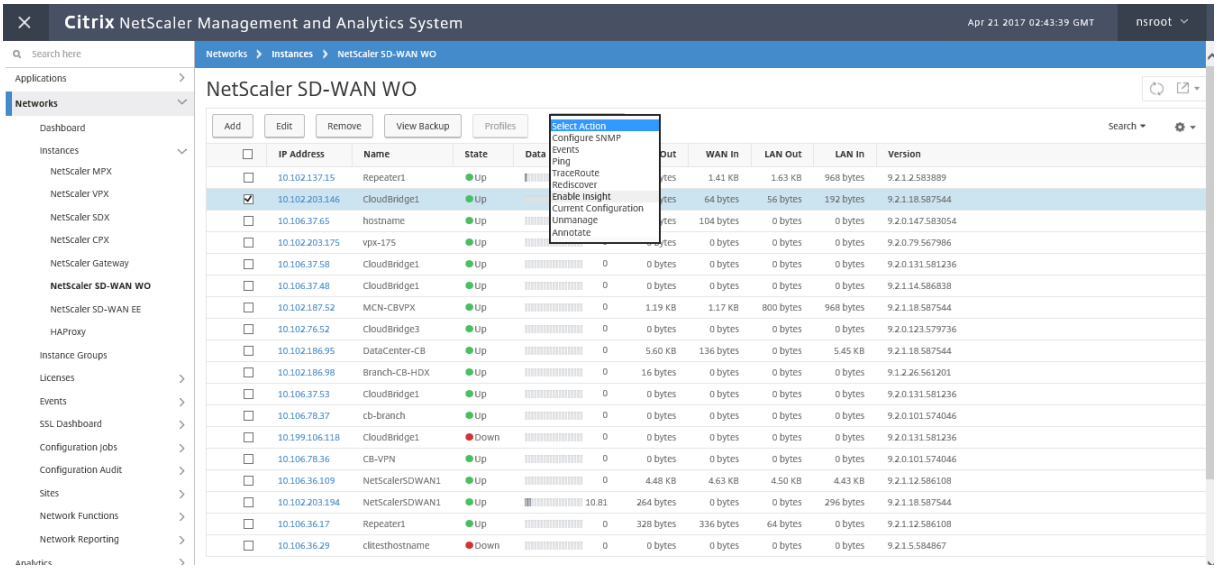
WAN Insight

February 1, 2024

Les appliances d'optimisation WAN (WO) Citrix SD-WAN optimisent la livraison de nombreuses applications via le WAN, en améliorant l'efficacité du flux de données sur le réseau entre le datacenter et les sites de succursales.

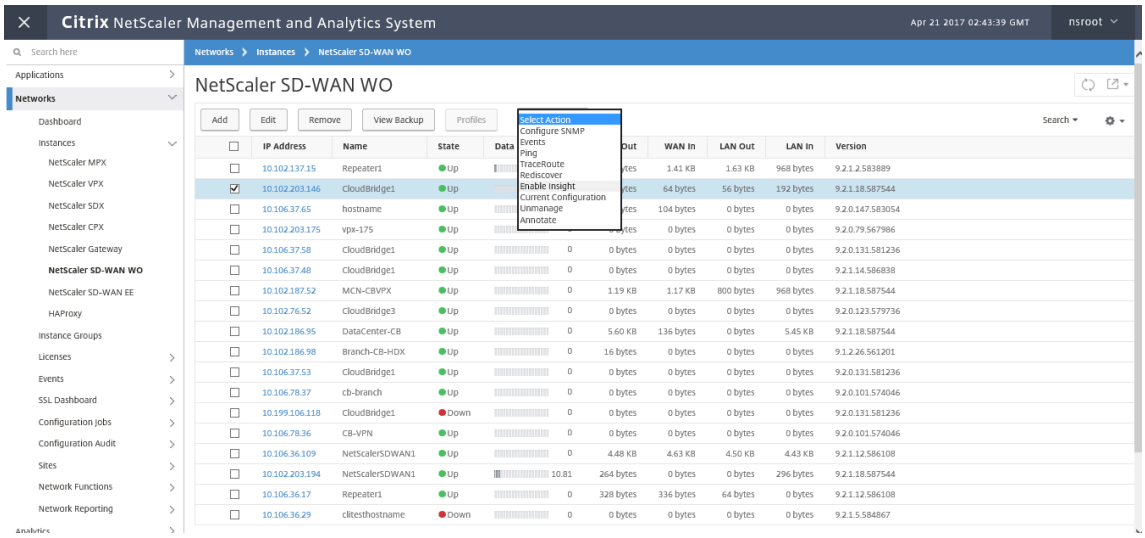
L'analyse WAN Insight permet aux administrateurs de surveiller facilement le trafic WAN accéléré et non accéléré qui circule entre les appliances d'optimisation WAN du centre de données et des succursales. WAN Insight offre une visibilité sur les clients, les applications et les succursales du réseau afin de résoudre efficacement les problèmes réseau. Les rapports en direct et historique vous permettent de résoudre les problèmes de manière proactive, le cas échéant.

L'activation de l'analyse sur l'appliance d'optimisation WAN du centre de données permet à Citrix ADM de collecter des données et de fournir des rapports et des statistiques pour le datacenter et les appliances d'optimisation WAN de branche.



Pour activer les analyses sur l'appliance d'optimisation WAN :

1. Accédez à **Réseaux**> **Instances** > **Citrix SD-WAN**, puis sélectionnez l'instance WO SD-WAN.

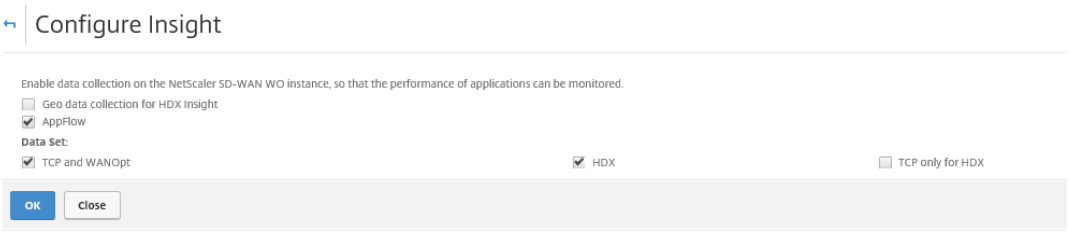


2. **Dans la liste Sélectionner une action**, sélectionnez**Configurer Analytics**.
3. Sélectionnez les paramètres suivants selon les besoins :

   - **Collecte de données géo pour HDX Insight** : partage l'adresse IP du client avec l'API Google Geo.

   - **AppFlow** : Commence à collecter des données à partir d'instances d'optimisation WAN.

     - **TCP et WANopt**: fournit des rapports **TCP et WANopt** Insight .
     - **HDX** : fournit des rapports HDX Insight.
     - **TCP uniquement pour HDX** : fournit TCP uniquement pour les rapports HDX Insight.



4. Cliquez sur **OK**.

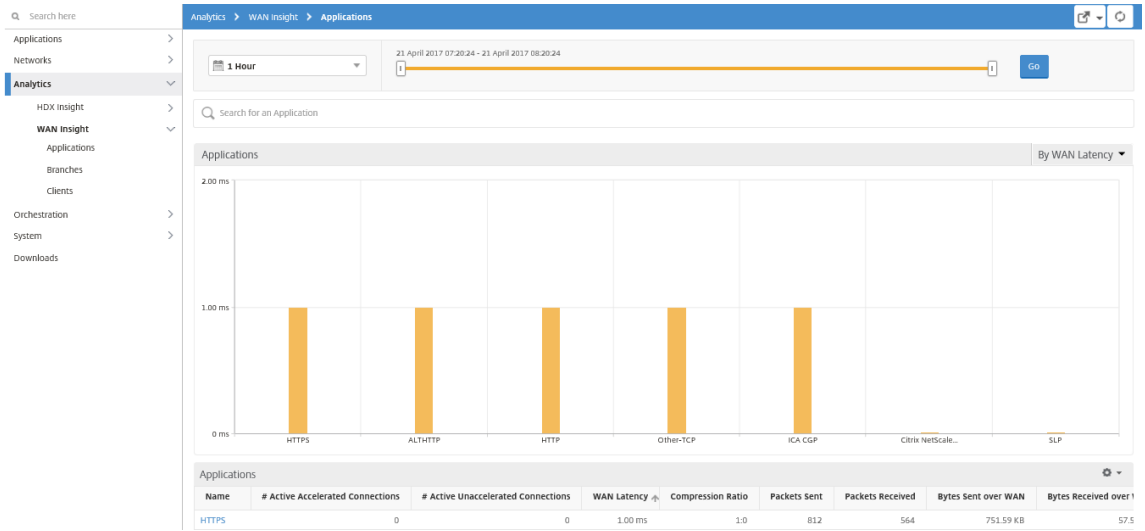
Pour afficher les rapports WAN Insight :

1. Accédez à **Analytics** > **WAN Insight** .

> **Remarque**
>
> L'option WAN Insight n'est visible qu'après avoir ajouté une instance SD-WAN WO à Citrix ADM.

Vous pouvez consulter les rapports suivants :

- **Applications** : affiche les statistiques d'utilisation et de performance de toutes les applications pendant la durée sélectionnée.
- **Branches** : affiche les statistiques d'utilisation et de performances de toutes les appliances de branche d'optimisation WAN.
- **Clients** : affiche les statistiques d'utilisation et de performance de tous les clients accédant aux appliances d'optimisation WAN, dans chaque branche.



Les mesures suivantes sont affichées :

Métrique	Description
Connexions accélérées actives	Nombre de connexions WAN actives accélérées.
Connexions actives non accélérées	Nombre de connexions WAN actives qui ne sont pas accélérées.
Latence WAN	Retard, en millisecondes, ressenti par l'utilisateur lorsqu'il interagit avec une application.
Taux de compression	Rapport de compression des données entre la succursale et les appliances du centre de données pour la durée sélectionnée.
Paquets envoyés	Nombre de paquets que l'appliance d'optimisation WAN a envoyés sur le réseau pendant la durée sélectionnée.
Paquets reçus	Nombre de paquets que l'appliance d'optimisation WAN a reçus du réseau pendant la durée sélectionnée.
Octets envoyés sur le WAN	Nombre d'octets que l'appliance d'optimisation de Citrix WAN a envoyés sur le réseau étendu pendant la durée sélectionnée.
Octets reçus sur le WAN	Nombre d'octets que l'appliance d'optimisation WAN a reçus du WAN pendant la durée sélectionnée.
LAN RTO	Nombre de fois où l'appliance d'optimisation WAN a dépassé le délai de retransmission vers le réseau local pendant la durée sélectionnée.
RTO WAN	Nombre de fois que l'appliance d'optimisation du WAN a dépassé le délai de retransmission vers le WAN pendant la durée sélectionnée.
Retransmettre des paquets (LAN)	Nombre de paquets que l'appliance d'optimisation WAN a retransmis au réseau LAN pendant la durée sélectionnée.
Retransmettre des paquets (WAN)	Nombre de paquets que l'appliance d'optimisation WAN a retransmis au réseau WAN pendant la durée sélectionnée.

Video Insight

February 1, 2024

La fonctionnalité Video Insight fournit une solution simple et évolutive pour surveiller les indicateurs des techniques d'optimisation vidéo utilisées par les appliances Citrix ADC afin d'améliorer l'expérience client et l'efficacité opérationnelle, offrant des avantages tels que :

- Gérez le réseau en cas de congestion aux heures de pointe.
- Améliorez la cohérence de la lecture vidéo et réduisez le blocage vidéo.
- Activez de nouvelles offres de services vidéo (par exemple, des services vidéo en rafale).
- Permettez aux clients de sélectionner la meilleure qualité vidéo durable.
- Offrez une expérience utilisateur cohérente à l'abonné.

Tout en optimisant le trafic vidéo, l'appliance Citrix ADC utilise un mécanisme spécial pour accélérer dynamiquement le débit vidéo et une technique d'échantillonnage aléatoire pour estimer les économies réalisées grâce à la technique d'optimisation. Pour plus d'informations sur la fonctionnalité d'optimisation vidéo Citrix ADC, consultez Optimisation vidéo.Lorsque vous intégrez l'appliance Citrix ADC à Citrix Application Delivery Management (ADM), il recueille des informations clés à partir des données vidéo qui transitent par l'appliance Citrix ADC. Vous pouvez utiliser ces informations pour comparer les performances optimisées et non optimisées du trafic vidéo ABR, déterminer les économies dues à l'optimisation, etc.

> **Remarque**
>
> Les statistiques des sessions non optimisées fournies dans Citrix ADM correspondent aux sessions sélectionnées pour un échantillonnage aléatoire dans l'appliance Citrix ADC. Pour plus d'informations sur l'échantillonnage aléatoire, voir Optimisation vidéo.

Video Insight dans Citrix ADM fournit des mesures pour les types de trafic vidéo suivants :

- Vidéos à téléchargement progressif (PD) via HTTP
- Vidéos ABR via HTTP
- Vidéos ABR via HTTPS
- Vidéos YouTube ABR sur QUIC

Configuration de Video Insight

> **Remarque**
>
> Video Insight est pris en charge sur les instances Citrix ADC dotées d'une licence Citrix ADC Premium. La licence Citrix ADC Premium est prise en charge pour les plates-formes Citrix ADC Telco (VPX T1000 et VPX-T).

Pour configurer Video Insight sur une instance Citrix ADC, activez d'abord la fonctionnalité AppFlow, configurez un collecteur, une action et une stratégie AppFlow et liez la stratégie globalement. Lorsque vous configurez le collecteur, vous devez spécifier l'adresse IP du serveur Citrix ADM sur lequel vous souhaitez surveiller les rapports.

Pour configurer des informations vidéo sur une instance Citrix ADC, exécutez les commandes suivantes pour configurer un profil et une stratégie AppFlow et lier la stratégie AppFlow globalement.

add appflow collector <name> **-IPAddress** <ipaddress> **-port** <port_number> **-Transport** logstream

set appflow param -**videoInsight** ENABLED

add appflow action <name> **-collectors** <string> **-videoAnalytics** ENABLED

add appflow policy <name> <rule> <action>

bind appflow global <policyName> <priority> [<gotoPriorityExpression>] [**-type** <type>]

enable ns mode `ulfd`

enable feature AppFlow

Sample

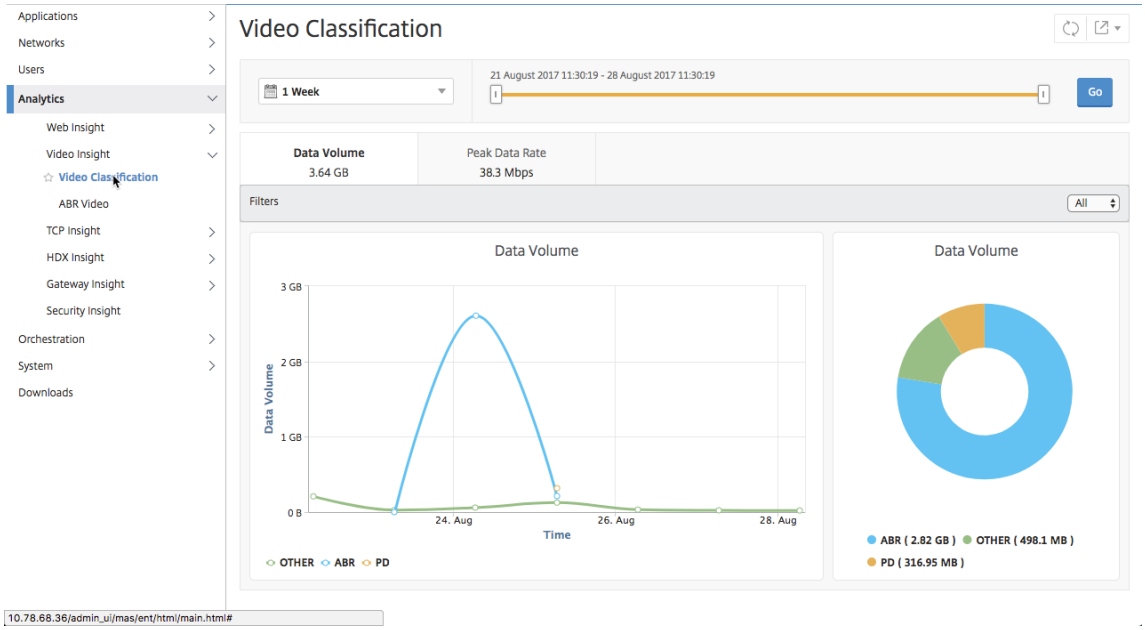
```
add appflow collector col1 -IPAddress 10.106.76.15 -port 5557 -
    Transport logstream
set appflow param -videoInsight ENABLED
add appflow action act1 -collectors col1 -videoAnalytics ENABLED
add appflow policy appol true act1
bind appflow global appol 1
enable ns mode ulfd
enable feature appflow
<!--NeedCopy-->
```

Affichage des métriques Video Insight dans Citrix ADM

Après avoir activé Video Insight dans Citrix ADM, vous pouvez afficher des mesures d'optimisation vidéo telles que la classification vidéo, le volume de données, le débit de pointe et les lectures vidéo ABR. Ces mesures vous aident à analyser votre réseau et à optimiser les vidéos pour améliorer l'expérience des abonnés, l'efficacité opérationnelle et d'autres critères de performance.

Pour afficher les mesures Video Insight dans Citrix ADM :

1. Dans un navigateur Web, tapez l'adresse IP de l'appliance virtuelle Citrix ADM (par exemple, http://192.168.100.1).
2. Dans **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Accédez à **Analytics > Insight vidéo**.



> **Remarque**
>
> Les valeurs fournies par la légende **OTHER** dans les graphiques représentent les données non ABR et non-DP du trafic vidéo en fonction du filtre que vous avez sélectionné :
>
> - **All** –Somme des données non-ABR (HTTP, HTTPS et QUIC) et non-PD (HTTP) dans le trafic vidéo.
> - **HTTP** —Somme des données non ABR et non PD dans le trafic vidéo.
> - **HTTPS** : somme des données vidéo non ABR dans le trafic vidéo.
> - **QUIC** —Somme des données vidéo non ABR dans le trafic vidéo.

Afficher l'efficacité du réseau

February 1, 2024

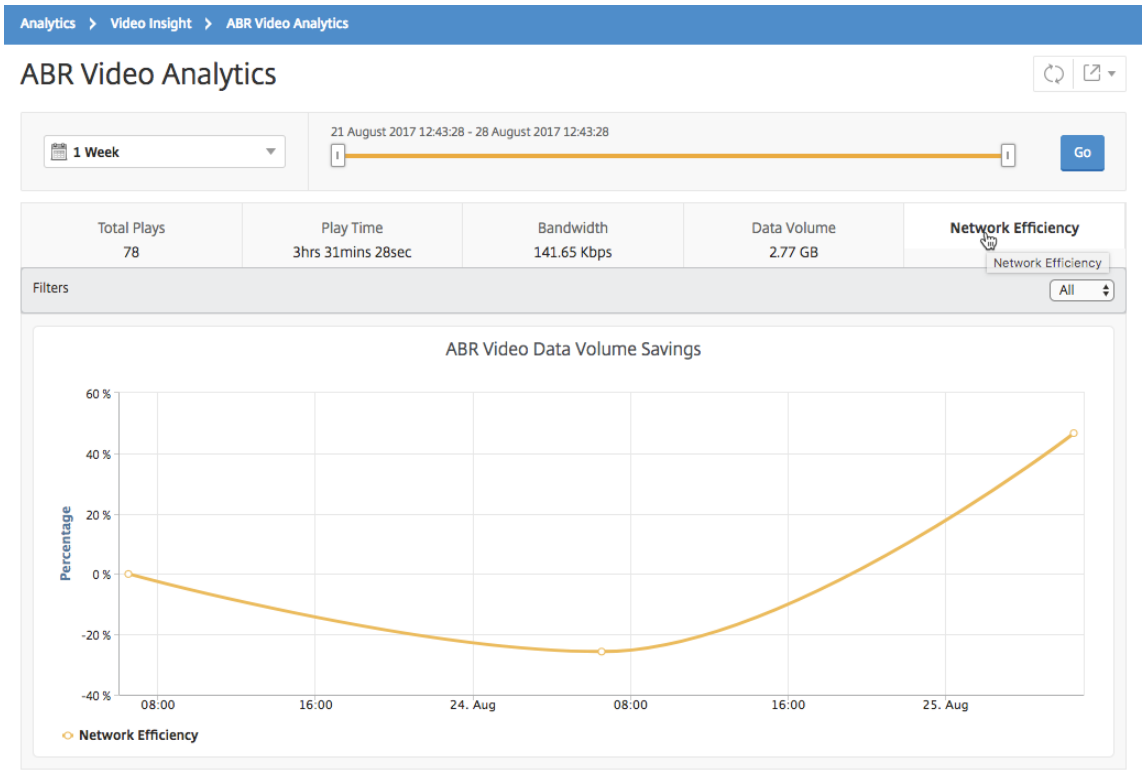
Pour une période donnée, Citrix Application Delivery Management (ADM) fournit un graphique qui montre le rapport entre les sessions vidéo optimisées et non optimisées dans la période. Il affiche

également le pourcentage de bande passante économisé grâce à l'optimisation. Le pourcentage de bande passante économisée est calculé à l'aide de la formule suivante :

Pourcentage de bande passante sauvegardée = Volume de **données vidéo ABR optimisé moyen/-Moyenne du volume de données vidéo ABR non optimisé**.

Pour voir le pourcentage de bande passante économisé grâce à l'optimisation :

1. Accédez à **Analytics > Video Insight**, puis cliquez sur **ABR Video.**
2. Dans le volet droit, sélectionnez une période dans la liste. Vous pouvez personnaliser davantage la période en utilisant le curseur temporel.
3. Cliquez sur **Aller** et sélectionnez l'onglet **Efficacité réseau**.



Comparer le volume de données utilisé par les vidéos ABR optimisées et non optimisées

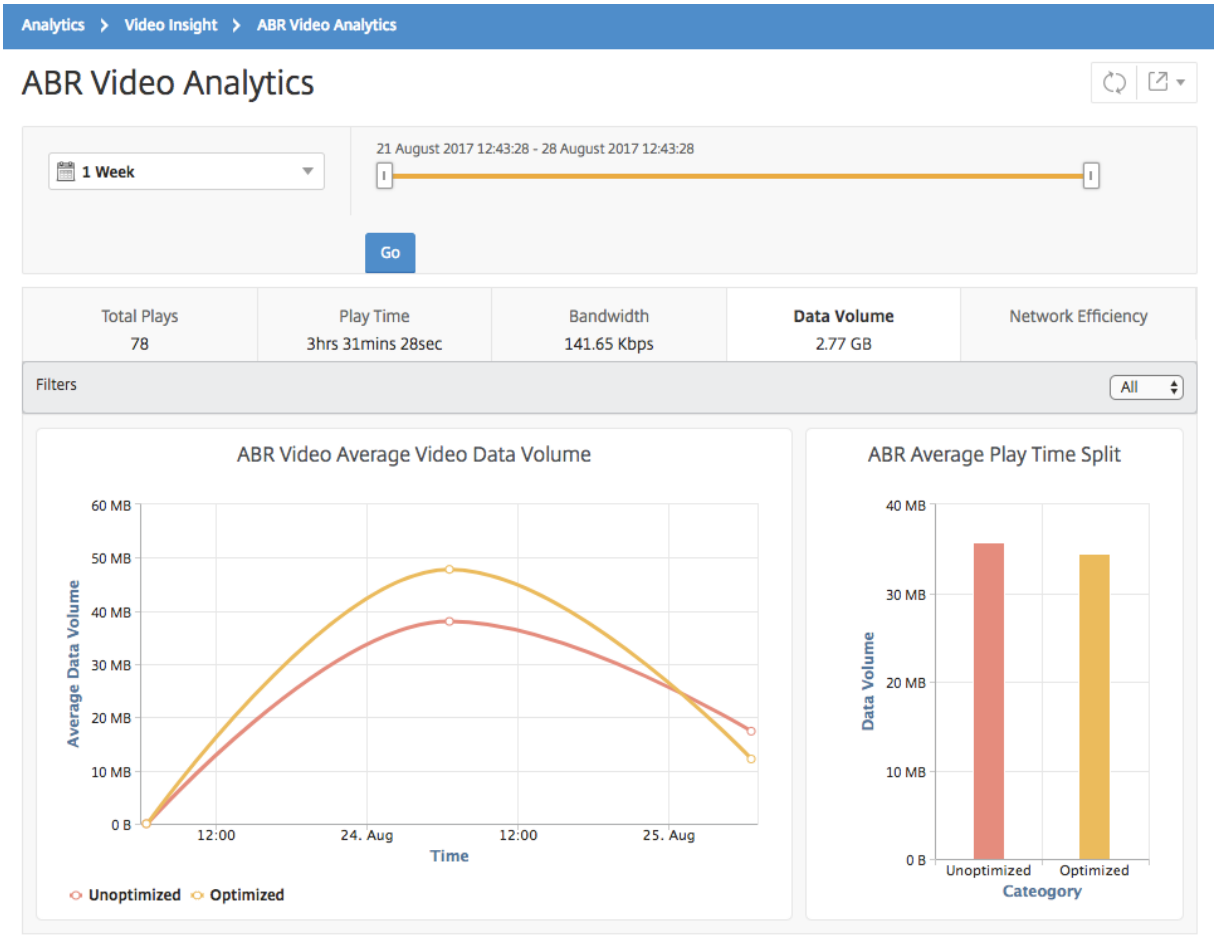
February 1, 2024

Pour une période donnée, Citrix Application Delivery Management (ADM) affiche le volume de données utilisé par les vidéos ABR optimisées et non optimisées, de sorte que vous pouvez comparer les deux volumes.

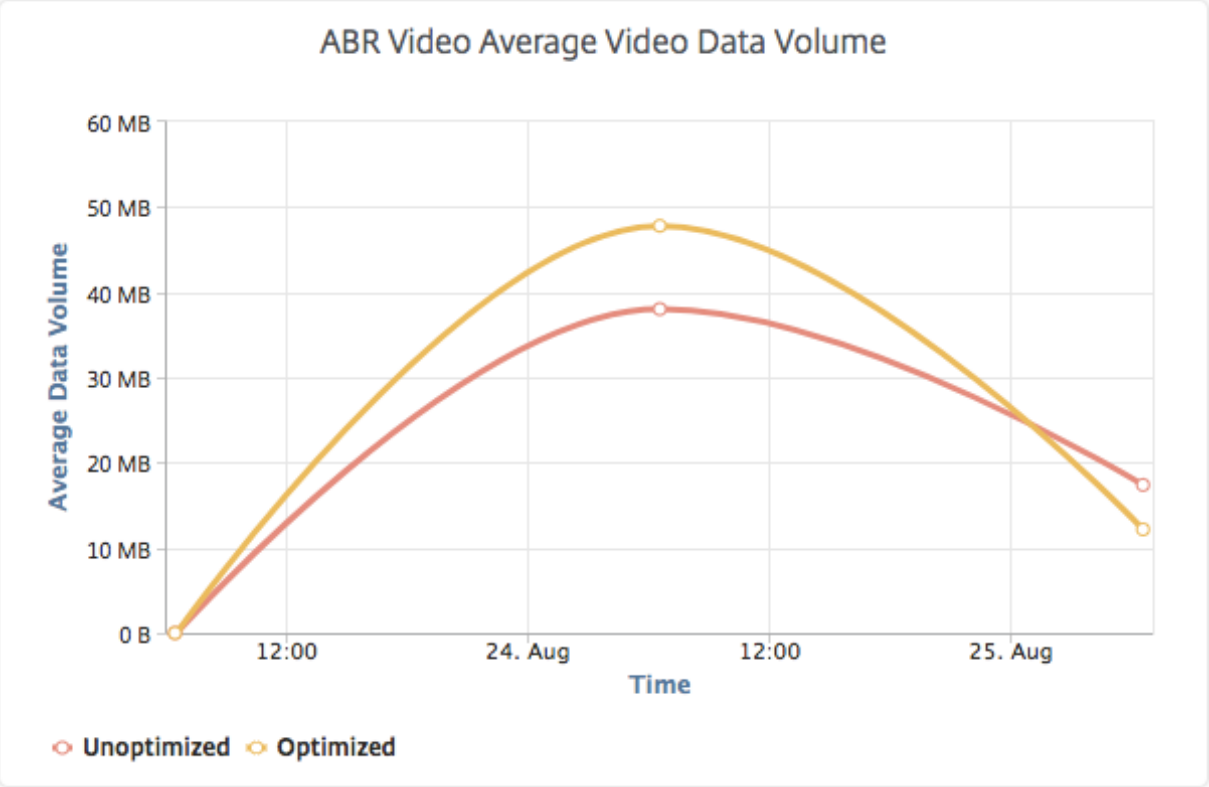
Pour voir le volume de données utilisé par les vidéos ABR :

1. Accédez à **Analytics > Video Insight**, puis cliquez sur **ABR Video.**
2. Dans le volet droit, sélectionnez une période dans la liste. Vous pouvez personnaliser davantage la période en utilisant le curseur temporel.
3. Cliquez sur **Aller** et sélectionnez l'onglet **Volume de données**.

Vous pouvez utiliser la liste **Filtres** pour sélectionner les vidéos HTTP, HTTPS ou QUIC ABR.



L'onglet **Volume de données** fournit un graphique linéaire et un graphique circulaire décrivant le volume de données moyen utilisé par les vidéos ABR et le volume de données consommé par les vidéos ABR optimisées et non optimisées de votre réseau pour la période sélectionnée. Vous pouvez placer le pointeur de la souris sur le graphique linéaire pour afficher le volume moyen de données utilisé pendant une période donnée :



Afficher le type de vidéos diffusées en continu et le volume de données consommé à partir de votre réseau

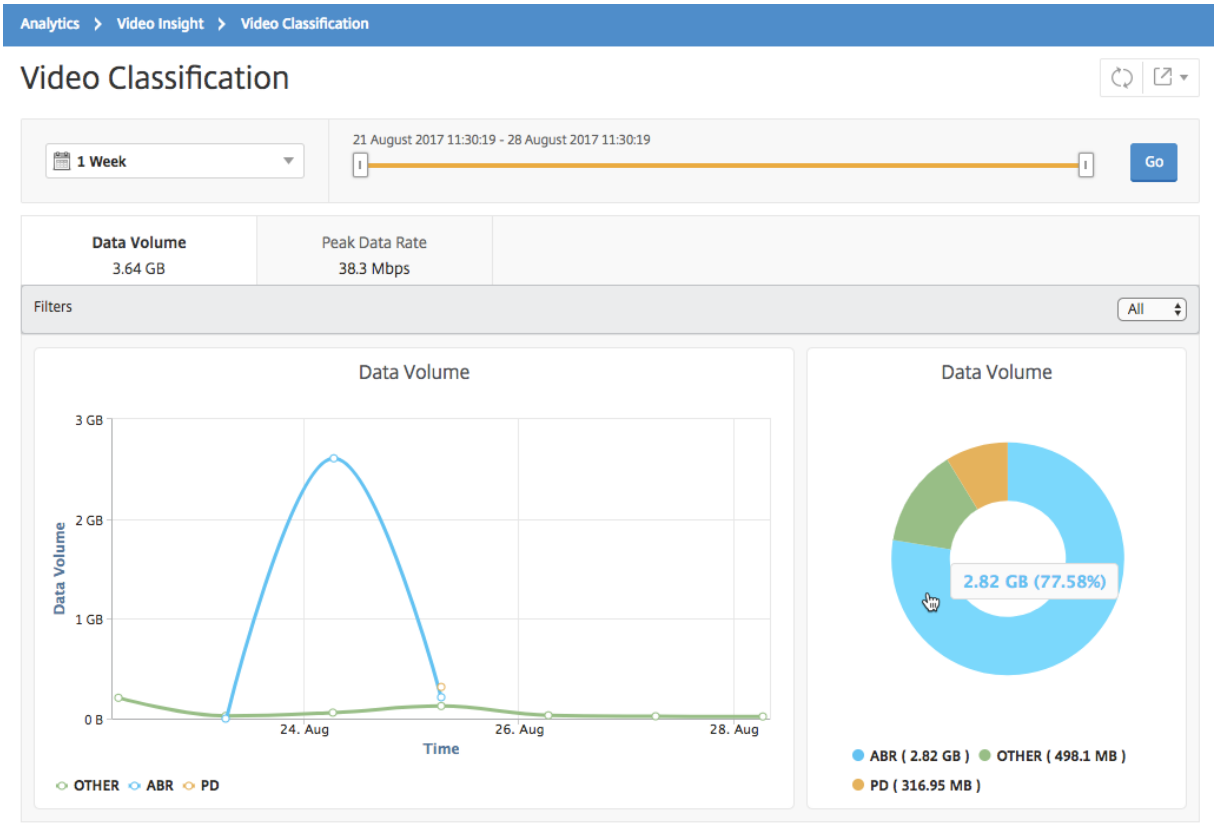
February 1, 2024

L'appliance Citrix ADC détecte le trafic vidéo crypté ou non crypté sur votre réseau et le type de streaming vidéo (DP ou ABR). Citrix Application Delivery Management (ADM) affiche ces mesures et le volume de données consommé par le trafic vidéo pendant une période définie.

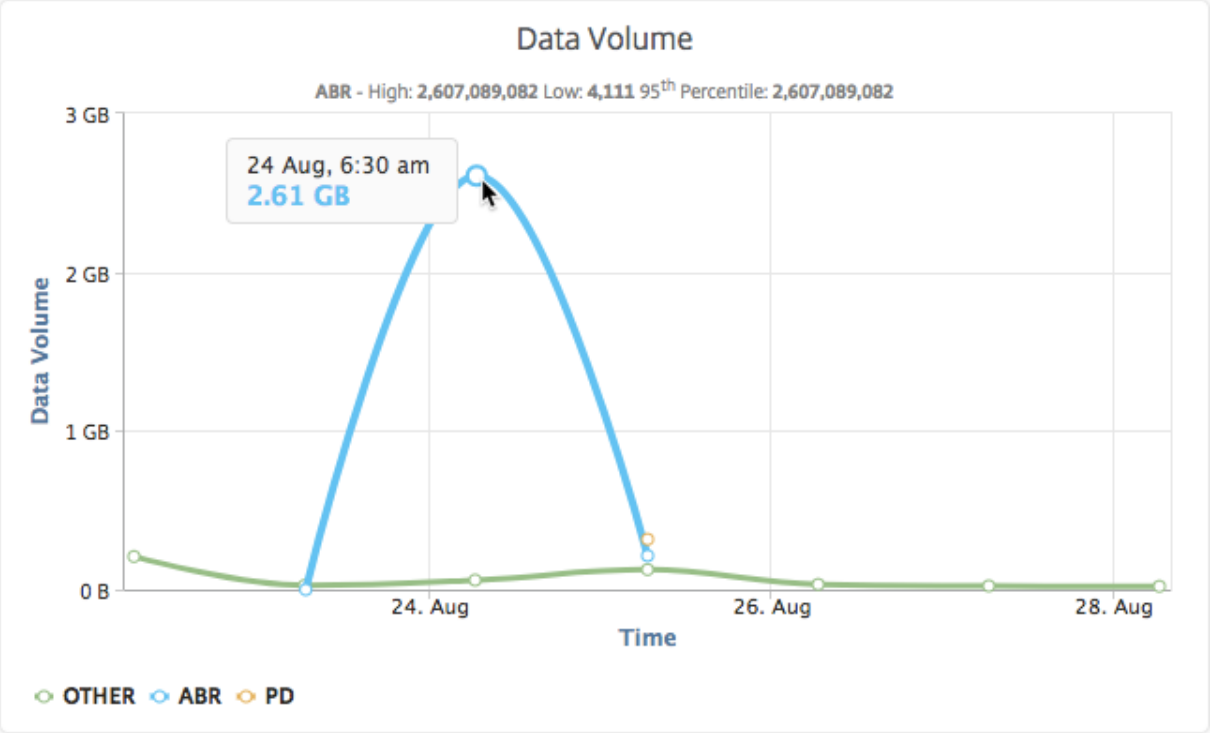
Pour voir les types de vidéos et le volume de données consommé :

1. Accédez à **Analytics > Video Insight** et cliquez sur **Classification des vidéos**.
2. Dans le volet droit, sélectionnez une période dans la liste. Vous pouvez personnaliser davantage la période en utilisant le curseur temporel.
3. Cliquez sur **OK**.

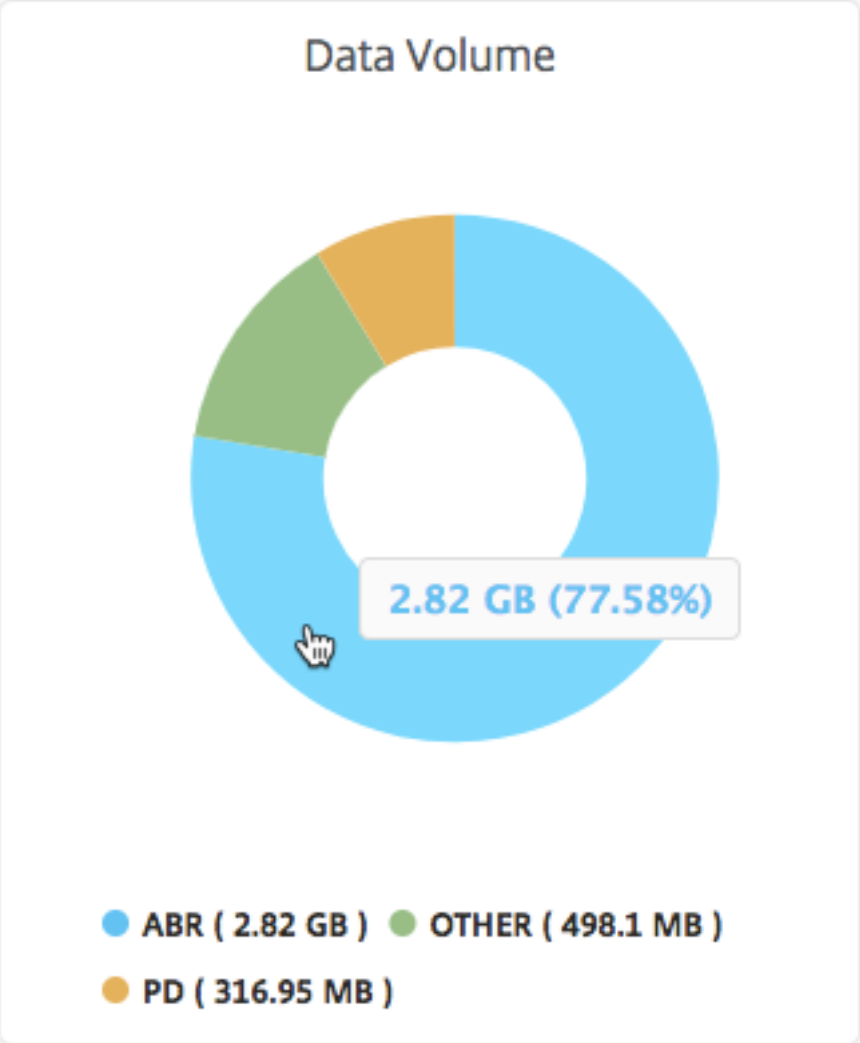
Vous pouvez utiliser la liste **Filtres** pour sélectionner le trafic HTTP, HTTPS ou QUIC.



L'onglet **Volume de données** fournit un graphique linéaire et un graphique circulaire indiquant les types de flux de trafic vidéo à partir de votre réseau et le volume de données consommé par votre réseau. Vous pouvez placer le pointeur de la souris sur le graphique linéaire pour afficher les données consommées pendant une période donnée :



En outre, vous pouvez placer le pointeur de la souris sur le graphique à secteurs pour afficher le pourcentage de volume de données consommé par un type particulier de trafic vidéo.



Comparer le temps de lecture optimisé et non optimisé des vidéos ABR

February 1, 2024

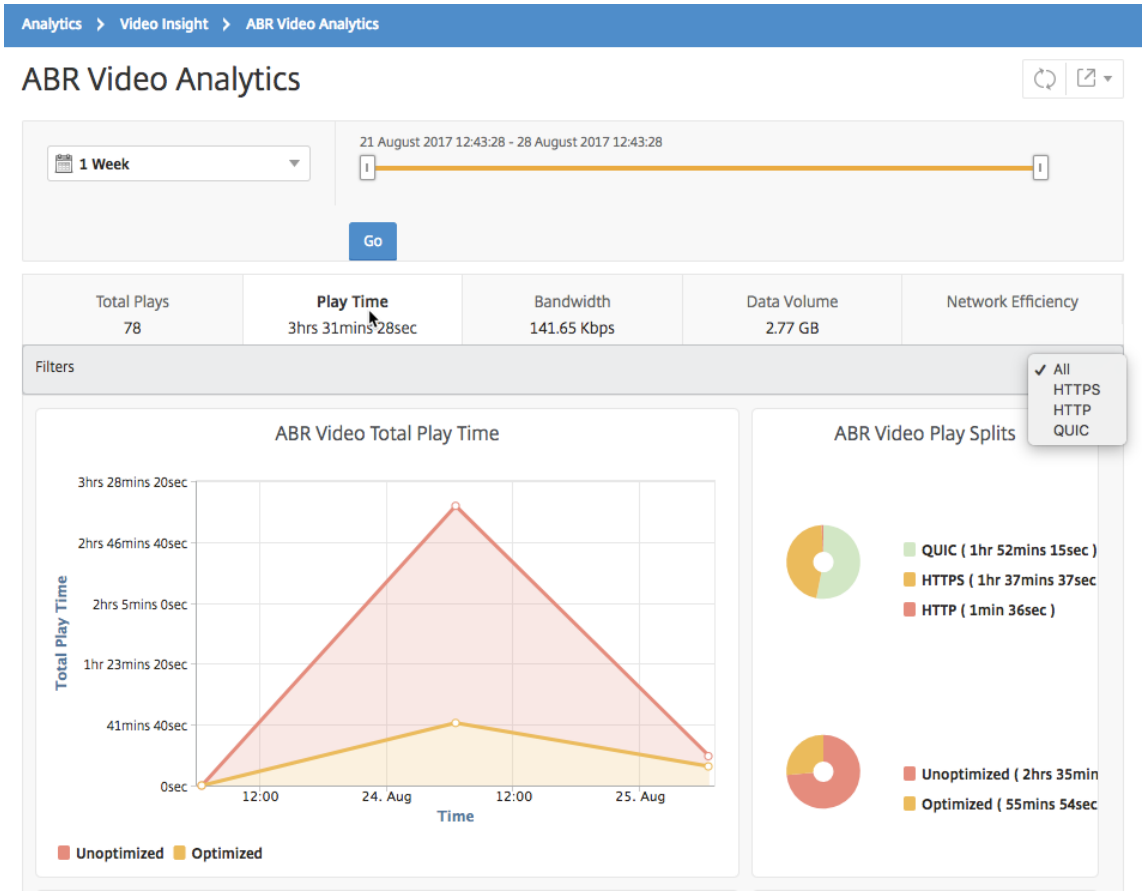
Pour une période donnée, Citrix Application Delivery Management (ADM) fournit la durée de lecture des vidéos ABR et vous permet également de comparer la durée de lecture des vidéos ABR optimisées et non optimisées de votre réseau.

Pour consulter le temps de jeu :

1. Accédez à **Analytics > Video Insight** et cliquez sur **ABR Video.**
2. Dans le volet droit, sélectionnez une période dans la liste. Vous pouvez personnaliser davantage la période en utilisant le curseur temporel.

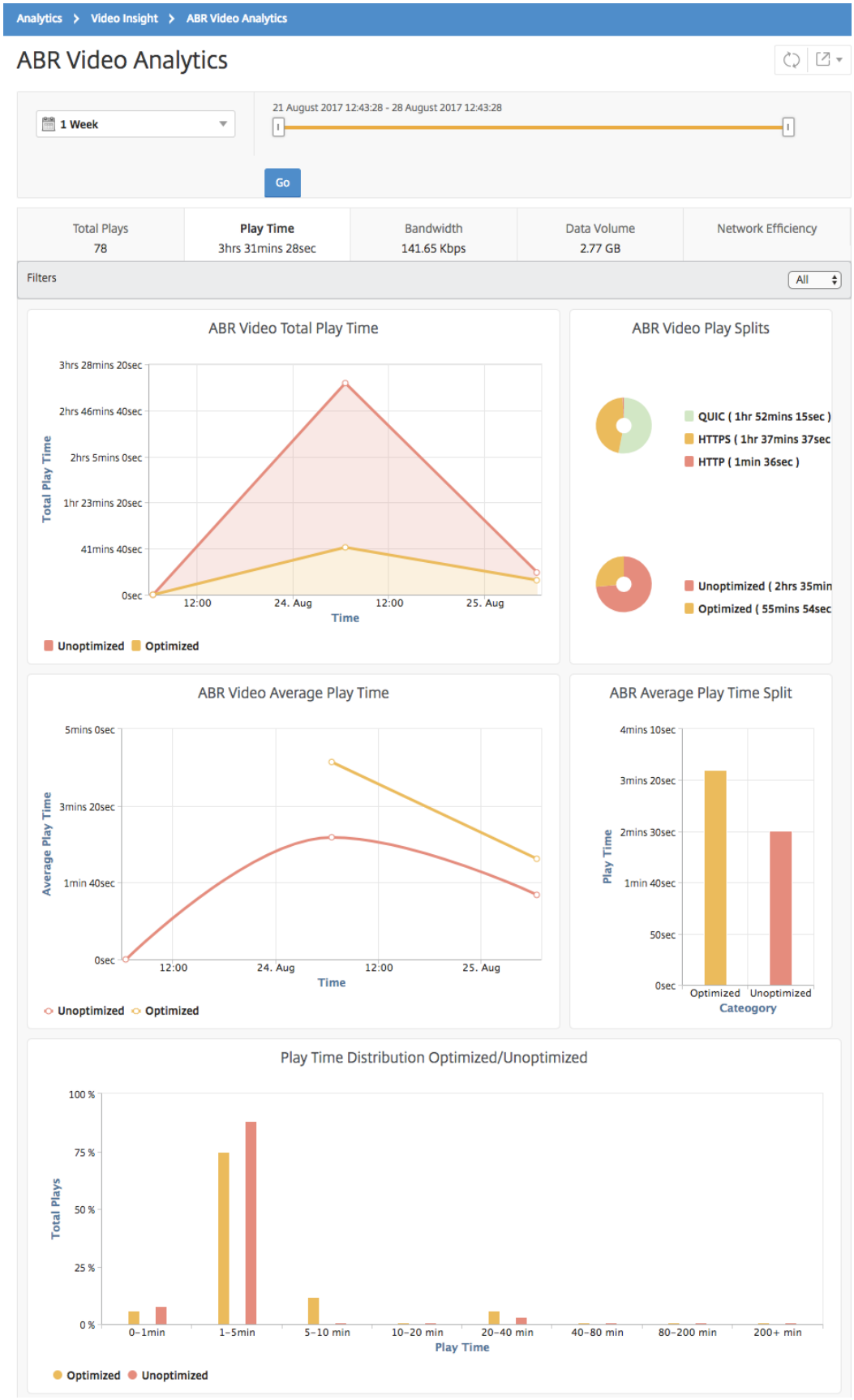
3. Cliquez sur **Aller** et sélectionnez l'onglet **Temps de lecture**.

   Vous pouvez utiliser la liste **Filtres** pour sélectionner les vidéos HTTP, HTTPS ou QUIC ABR.



Pour la période sélectionnée, l'onglet **Temps de lecture** fournit un graphique linéaire et un graphique à secteurs décrivant les éléments suivants :

- Temps total de lecture des vidéos ABR depuis votre réseau
- Durée totale de lecture des lectures optimisées et non optimisées de vidéos ABR à partir de votre réseau pendant la période sélectionnée
- Durée de lecture totale des vidéos ABR cryptées et non cryptées
- Durée moyenne de lecture des vidéos ABR
- Durée de lecture moyenne des lectures optimisées et non optimisées de vidéos ABR
- Durée de lecture moyenne des vidéos ABR cryptées et non cryptées
- Distribution du temps de lecture entre les vidéos ABR optimisées et non optimisées



Comparer la consommation de bande passante des vidéos ABR optimisées et non optimisées

February 1, 2024

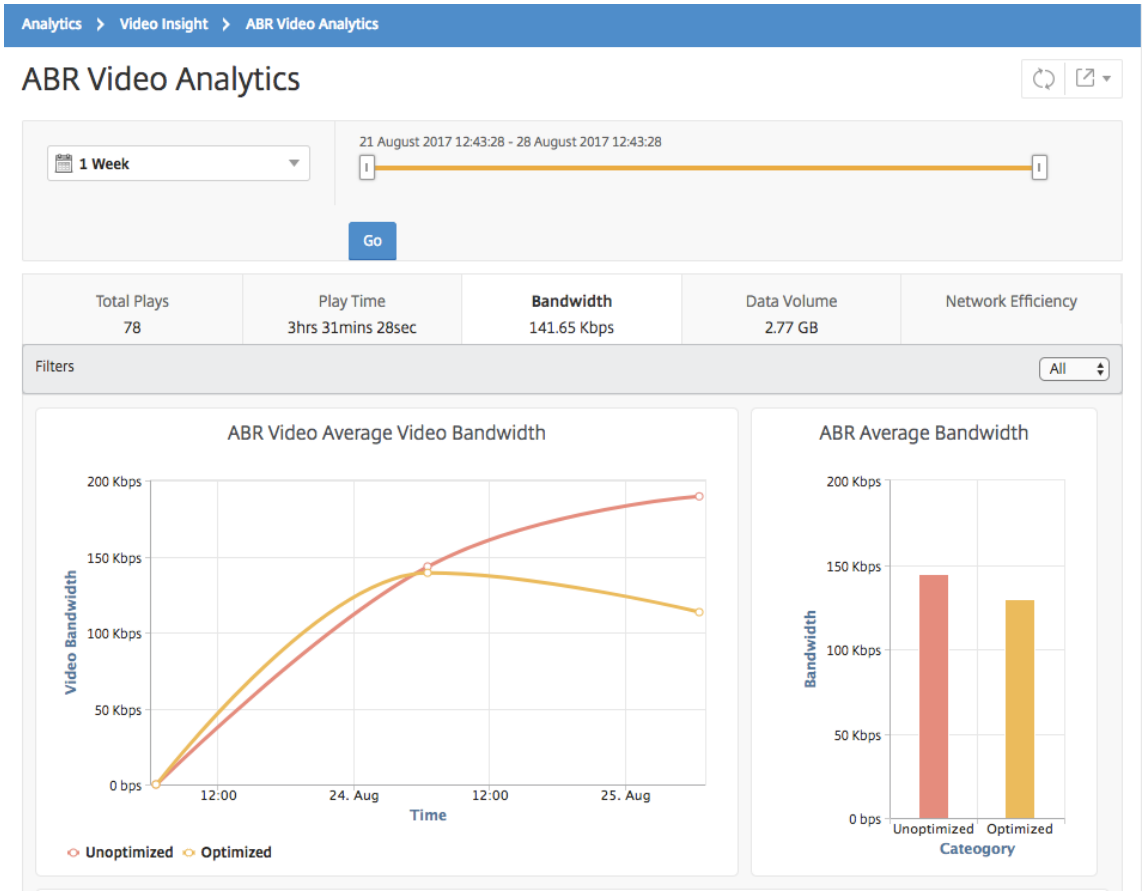
Pour une période donnée, Citrix Application Delivery Management (ADM) fournit la bande passante consommée par les vidéos ABR optimisées et non optimisées et vous permet également de comparer la bande passante consommée par les vidéos ABR optimisées et non optimisées dans votre réseau en fonction des éléments suivants :

- Temps de jeu
- Volume de données

Pour consulter la consommation de bande passante :

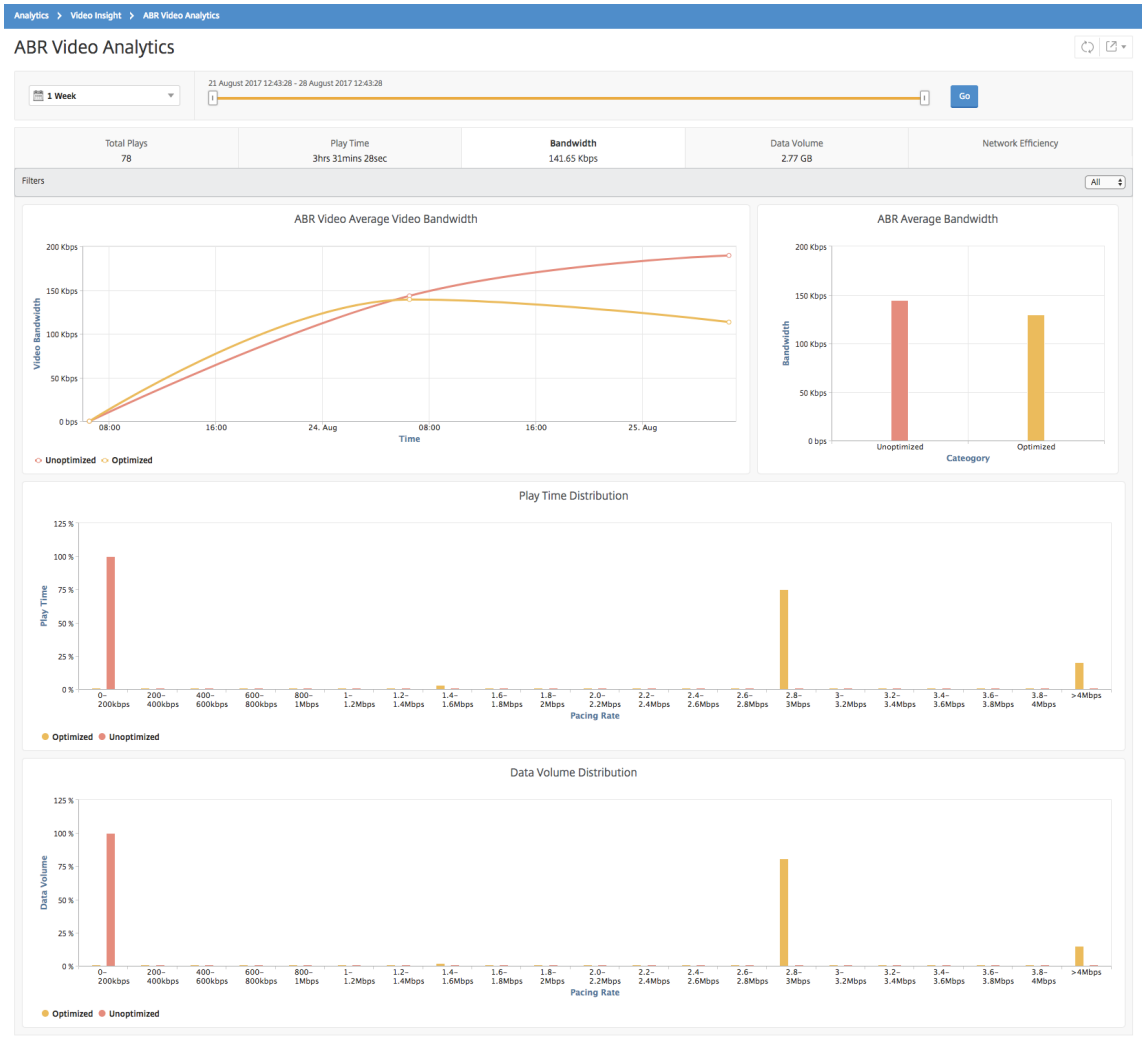
1. Accédez à **Analytics > Video Insight** et cliquez sur **ABR Video Analytics**.
2. Dans le volet droit, sélectionnez une période dans la liste. Vous pouvez personnaliser davantage la période en utilisant le curseur temporel.
3. Cliquez sur **Aller** et sélectionnez l'onglet **Bande passante**.

   Vous pouvez utiliser la liste **Filtres** pour sélectionner les vidéos HTTP, HTTPS ou QUIC ABR.



Pour la période sélectionnée, l'onglet **Bande passante** fournit un graphique linéaire et un graphique à secteurs décrivant les éléments suivants :

- Bande passante moyenne consommée par les vidéos ABR optimisées et non optimisées.
- Bande passante consommée en fonction de la répartition du temps de lecture entre les vidéos ABR optimisées et non optimisées.
- Bande passante consommée en fonction du volume de données distribué entre les vidéos ABR optimisées et non optimisées.



Comparer le nombre optimisé et non optimisé de lectures de vidéos ABR

February 1, 2024

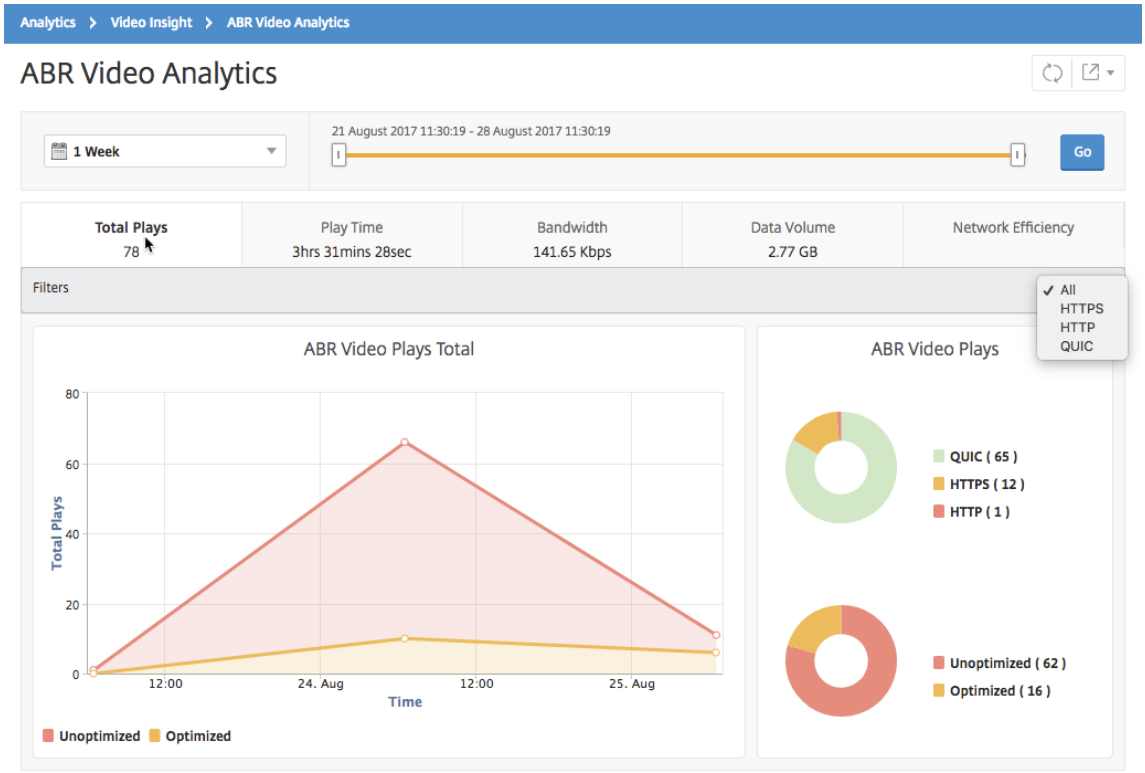
Pour une période donnée, Citrix Application Delivery Management (ADM) affiche le nombre de lectures de vidéos ABR et vous permet de comparer le nombre de lectures optimisées et non optimisées dans votre réseau.

Pour voir le nombre de parties :

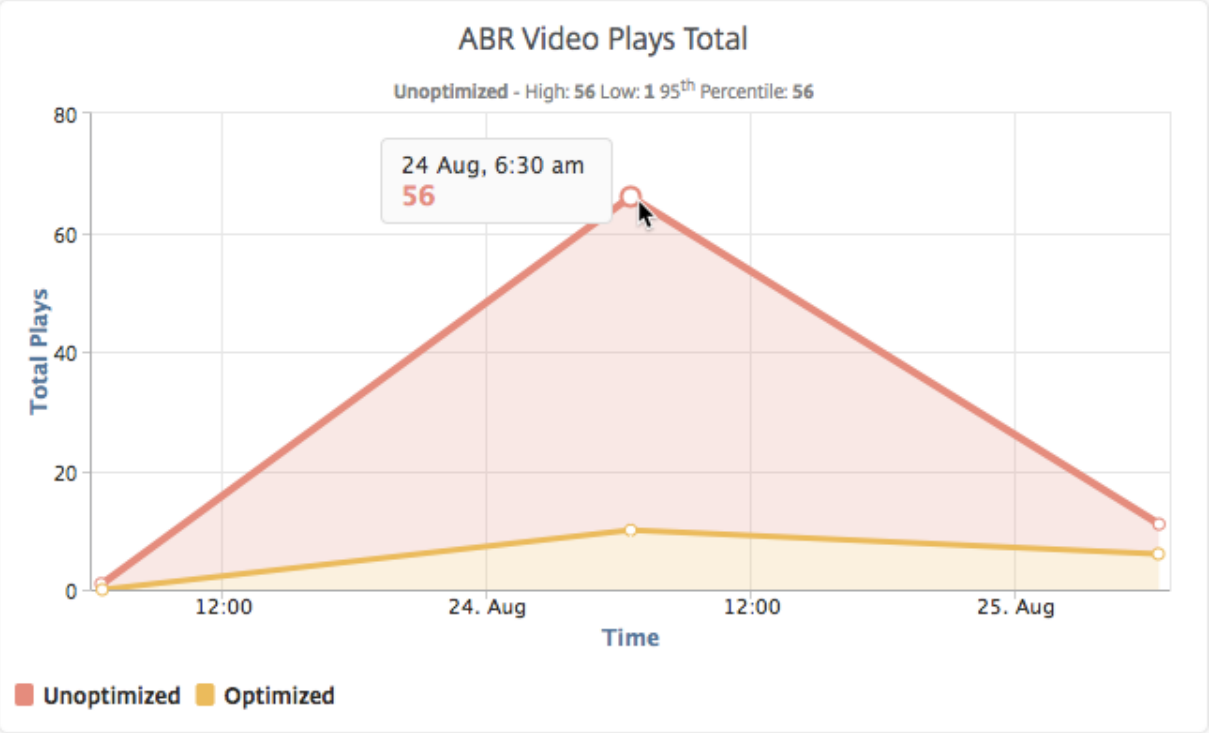
1. Accédez à **Analytics > Video Insight**, puis cliquez sur **ABR Video Analytics**.
2. Dans le volet droit, sélectionnez une période dans la liste. Vous pouvez personnaliser davantage la période en utilisant le curseur temporel.

3. Cliquez sur **Aller** et sélectionnez l'onglet **Nombre de Lecture**.

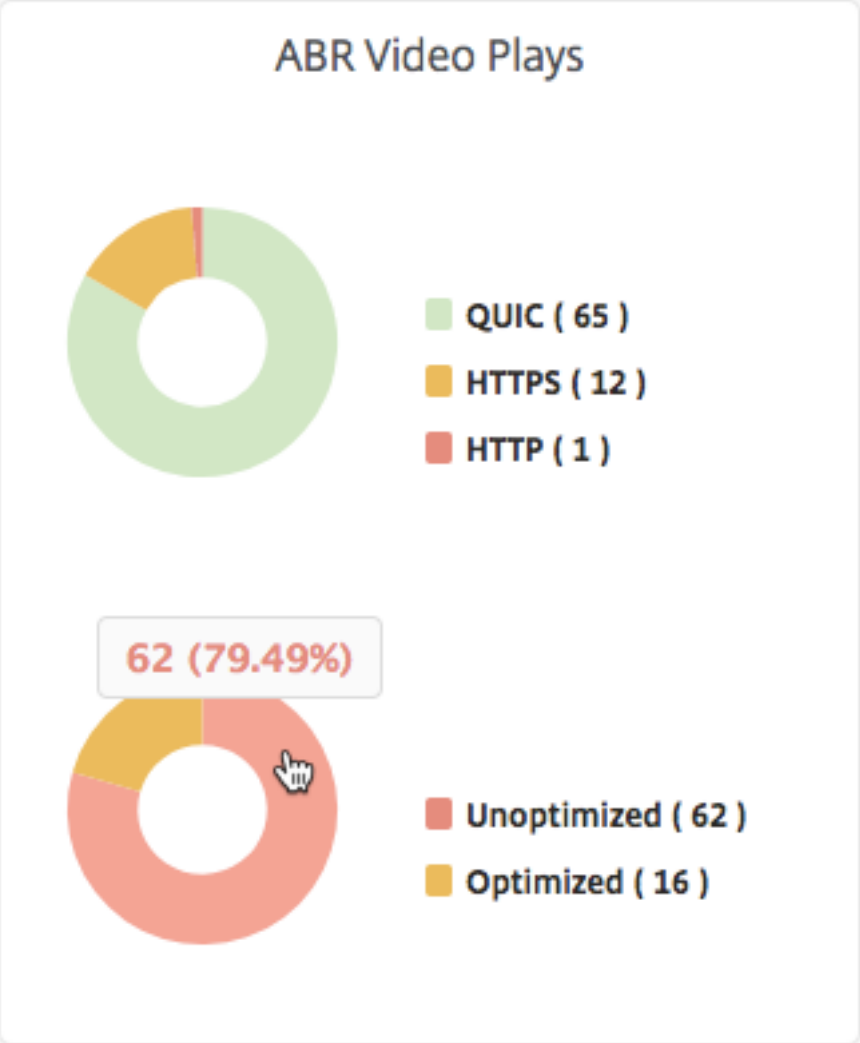
   Vous pouvez utiliser la liste **Filtres** pour sélectionner les vidéos HTTP, HTTPS ou QUIC ABR.



L'onglet **Nombre de lectures** fournit un graphique linéaire et un graphique à secteurs décrivant le nombre de lectures de vidéos ABR de votre réseau et le nombre de lectures optimisées et non optimisées de vidéos ABR de votre réseau pour la période sélectionnée. Vous pouvez placer le pointeur de la souris sur le graphique linéaire pour afficher le nombre de lectures au cours d'une période donnée :



En outre, vous pouvez pointer votre souris sur le graphique à secteurs pour afficher le pourcentage de lectures optimisées et non optimisées et le pourcentage de vidéos ABR chiffrées et non chiffrées pour la période sélectionnée.



Afficher le débit de données de pointe pour une période spécifique

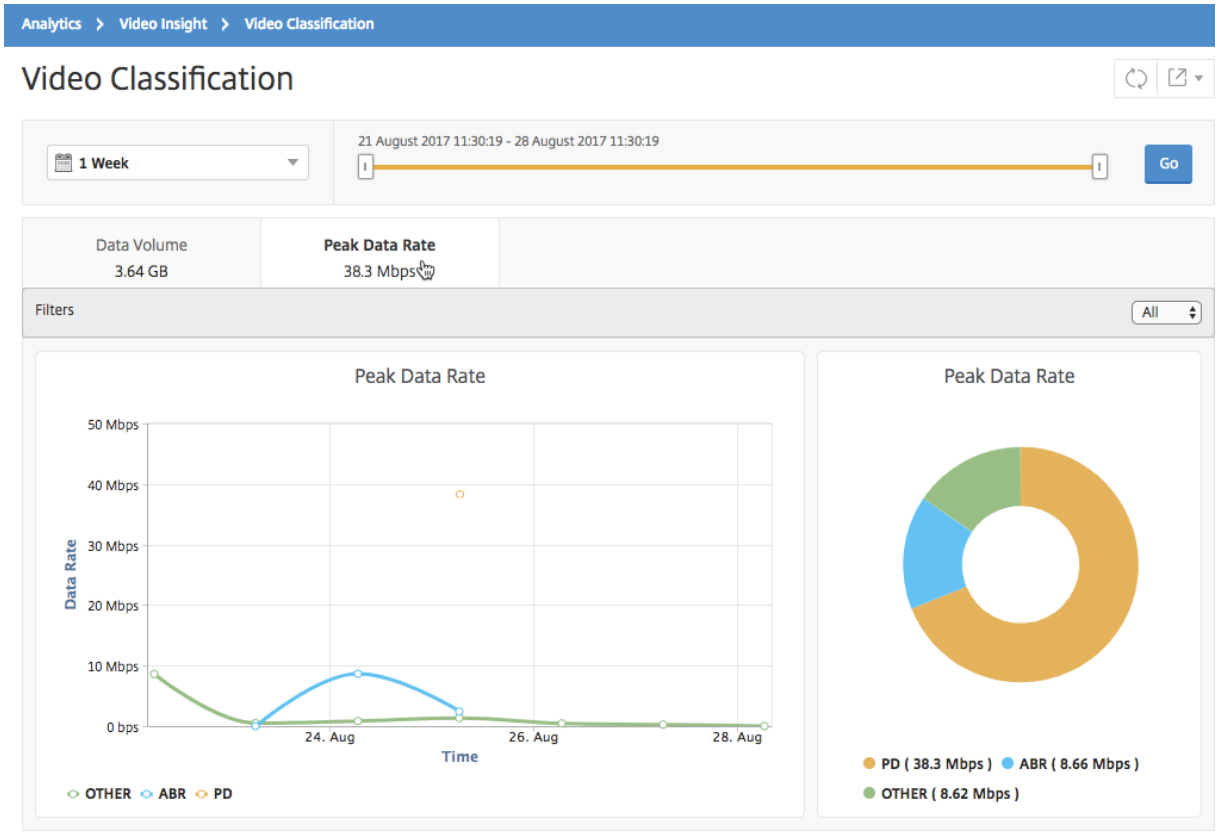
February 1, 2024

Citrix Application Delivery Management (ADM) vous indique le débit de pointe ou le débit de données du trafic vidéo sur votre réseau.

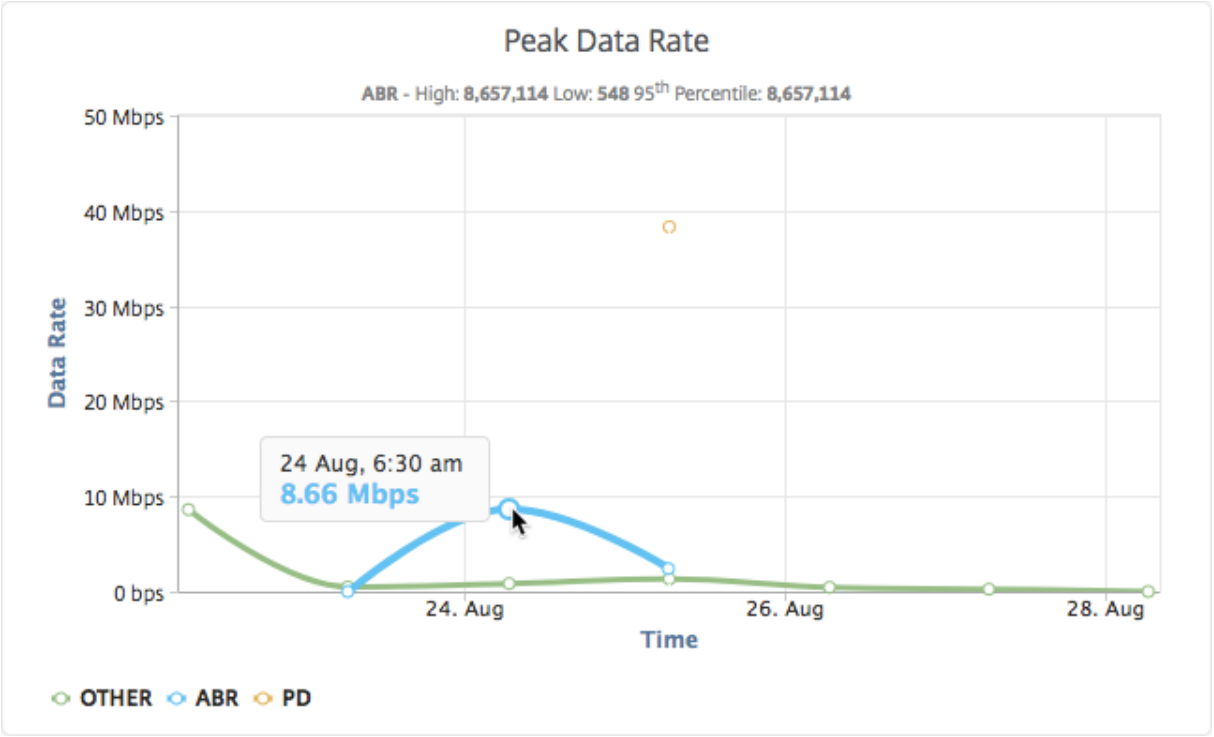
Pour voir le débit de données maximal du trafic vidéo :

1. Accédez à **Analytics > Video Insight**, puis cliquez sur **Classification des vidéos**.
2. Dans le volet droit, sélectionnez une période dans la liste. Vous pouvez personnaliser davantage la période en utilisant le curseur temporel.
3. Cliquez sur **Aller** et sélectionnez l'onglet **Taux de données de pointe**.

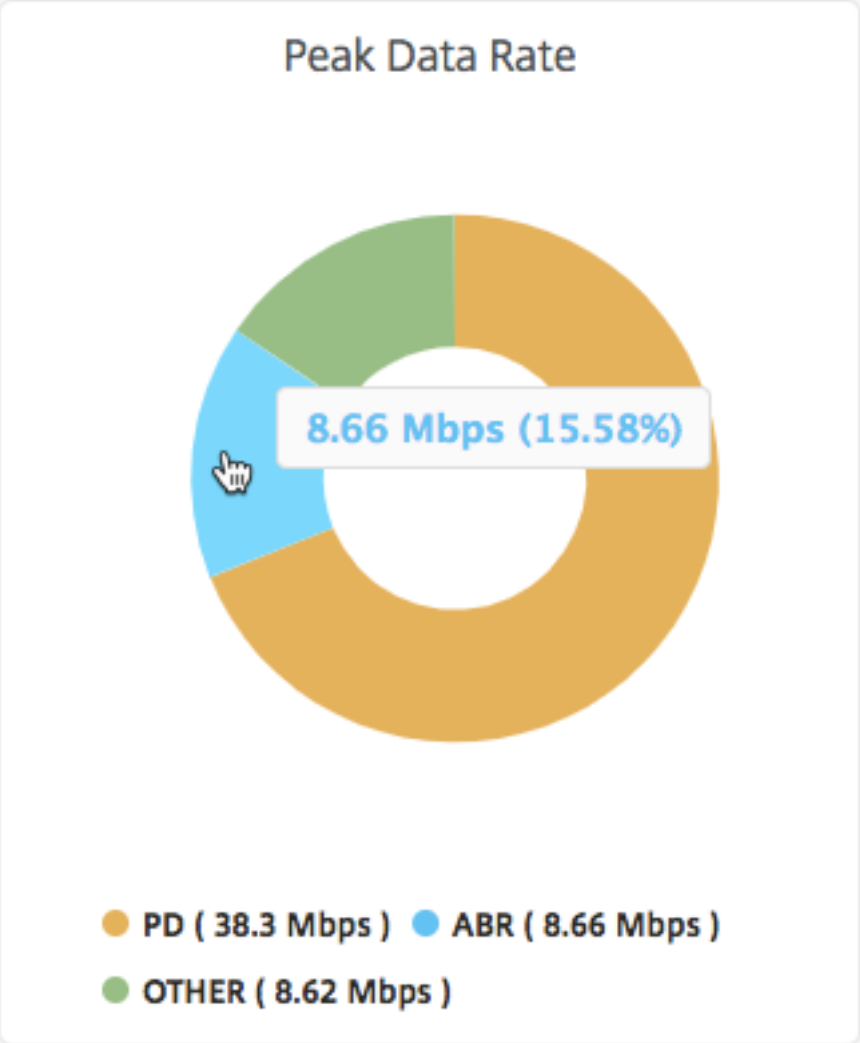
Vous pouvez utiliser la liste **Filtres** pour sélectionner le trafic HTTP, HTTPS ou QUIC.



L'onglet **Taux de crête de données** fournit un graphique linéaire et un graphique circulaire décrivant le débit de données de pointe du type de flux vidéo en continu à partir de votre réseau et le débit de données de pointe du trafic vidéo sur votre réseau pendant la période sélectionnée. Vous pouvez placer le pointeur de la souris sur le graphique linéaire pour afficher le débit de données maximal pendant une période donnée.



En outre, vous pouvez pointer votre souris sur le graphique à secteurs pour afficher le pourcentage du débit de données de pointe consommé par le type de trafic vidéo diffusé pendant la période sélectionnée.



Analyses de proxy de transfert SSL

February 1, 2024

Une appliance Citrix ADC située à la périphérie du réseau de l'entreprise fait office de proxy Internet. L'appliance peut fonctionner en mode proxy transparent ou en mode proxy explicite et propose des contrôles pour intercepter le trafic Internet, y compris HTTPS. La décision d'intercepter, de contourner ou de bloquer toute demande est prise en fonction des stratégies configurées sur l'appliance. Un utilisateur est authentifié avant de se connecter au réseau de l'entreprise. Toutes les demandes et réponses sont marquées à l'utilisateur et les activités de l'utilisateur sont enregistrées dans l'appliance. Pour plus d'informations, consultez Citrix SSL Forward Proxy.

Lorsque vous intégrez Citrix Application Delivery Management (ADM) à une appliance Citrix ADC, l'activité utilisateur consignée et les enregistrements suivants sur l'appliance sont exportés vers Citrix

ADM à l'aide de logstream. Citrix ADM rassemble et présente des informations sur les activités des utilisateurs, telles que les sites Web visités et la bande passante dépensée. Il signale également l'utilisation de la bande passante et les menaces détectées, telles que les logiciels malveillants et les sites de phishing. Vous pouvez utiliser ces indicateurs clés pour surveiller votre réseau et prendre des mesures correctives avec l'appliance Citrix ADC.

Pour intégrer une appliance Citrix ADC à Citrix ADM :

1. Sur l'appliance Citrix ADC, lors de la configuration du proxy SSL Forward, activez **Analytics** et fournissez les détails de l'instance Citrix ADM que vous souhaitez utiliser pour les analyses.
2. Dans Citrix ADM, ajoutez l'appliance Citrix ADC en tant qu'instance à Citrix ADM. Pour plus d'informations, consultez Ajouter des instances à Citrix ADM.

Tableaux de bord

February 1, 2024

Citrix Application Delivery Management (ADM) fournit deux tableaux de bord, le tableau de bord du **trafic sortant et le tableau de borddes utilisateurs**. Ces tableaux de bord affichent plusieurs graphiques qui résument les sites Web ou les applications accessibles depuis le réseau d'entreprise ainsi que les activités effectuées par les utilisateurs de votre réseau.

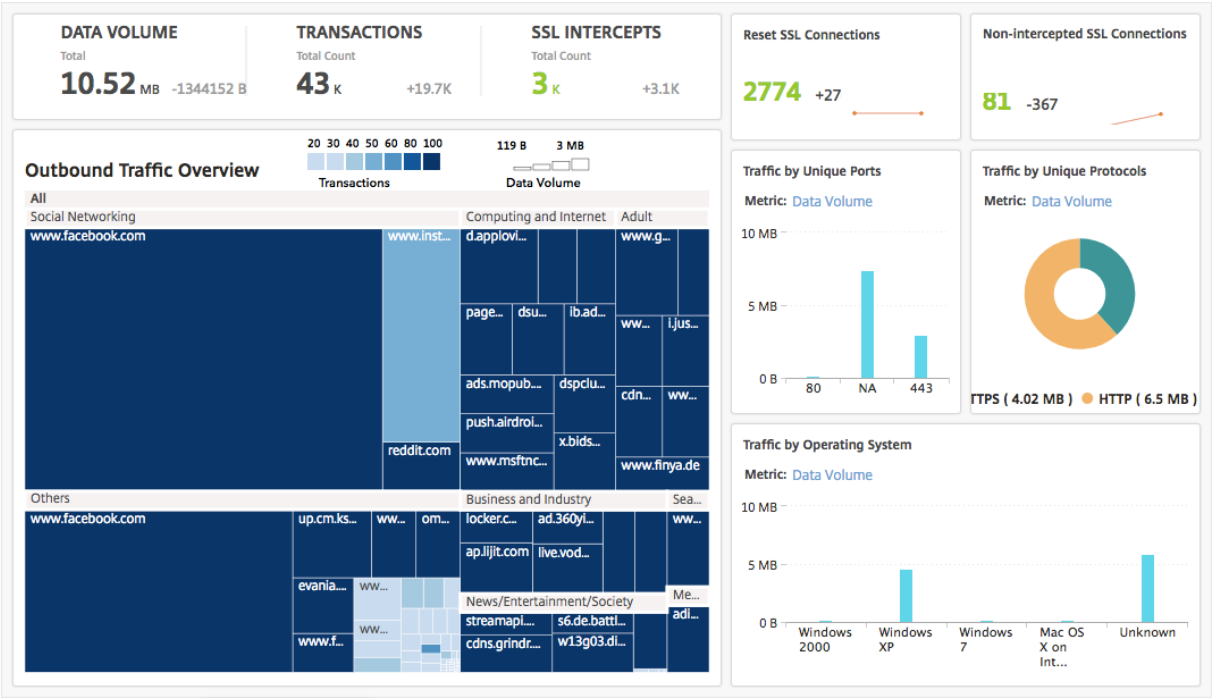
Tableau de bord du trafic sortant

Le tableau de **bord du trafic sortant** fournit un résumé des URL ou des domaines auxquels vous accédez depuis votre réseau. Il fournit une vue globale de toutes les URL ou domaines en fonction du nombre de transactions ou du volume de données consommé par les URL ou les domaines.
Il fournit également des détails tels que les suivants :

1. Quantité de bande passante consommée par les URL ou les domaines auxquels vous accédez depuis votre réseau.
2. Nombre de transactions qui se sont produites lors de l'accès aux URL et aux domaines à partir de votre réseau.
3. Nombre de connexions SSL interceptées par l'appliance Citrix ADC lors des transactions.
4. Nombre de connexions SSL non interceptées par l'appliance Citrix ADC lors des transactions.
5. Nombre de connexions SSL réinitialisées par l'appliance Citrix ADC lors des transactions.

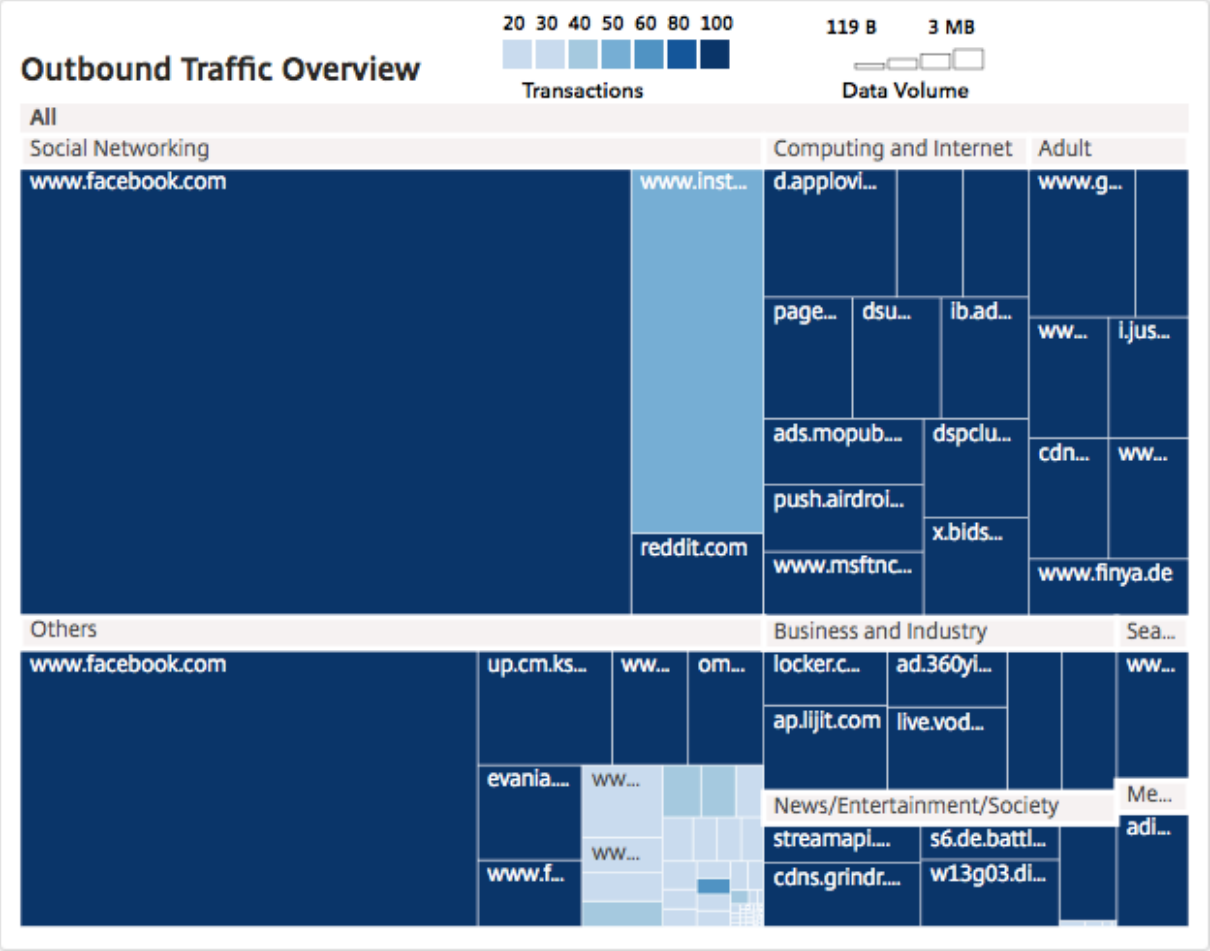
6. Quantité de trafic Web transmis, en fonction du port utilisé pour transmettre le trafic, du protocole utilisé par le trafic Web et des systèmes d'exploitation clients utilisés pour transmettre le trafic.

Pour accéder au tableau de bord du trafic sortant, accédez à **Applications > Tableau de bord du trafic sortant**.



Afficher le trafic sortant du réseau

Le tableau de **bord Trafic sortantcomprend un volet Aperçu du trafic sortant**. Dans le volet**Vue d'ensemble du trafic sortant**, Citrix ADM regroupe les URL ou domaines accessibles en catégories, telles que Shopping, Actualités, Réseaux sociaux, etc. Le volet**Aperçu du trafic sortant** affiche les URL ou les domaines auxquels vous accédez depuis votre réseau sous forme de nœuds dans les catégories d'URL. Les nœuds sont dimensionnés en fonction du volume de données consommé lors de l'accès à l'URL ou au domaine. La couleur du nœud indique le nombre de transactions qui se sont produites lors de l'accès à l'URL ou au domaine.



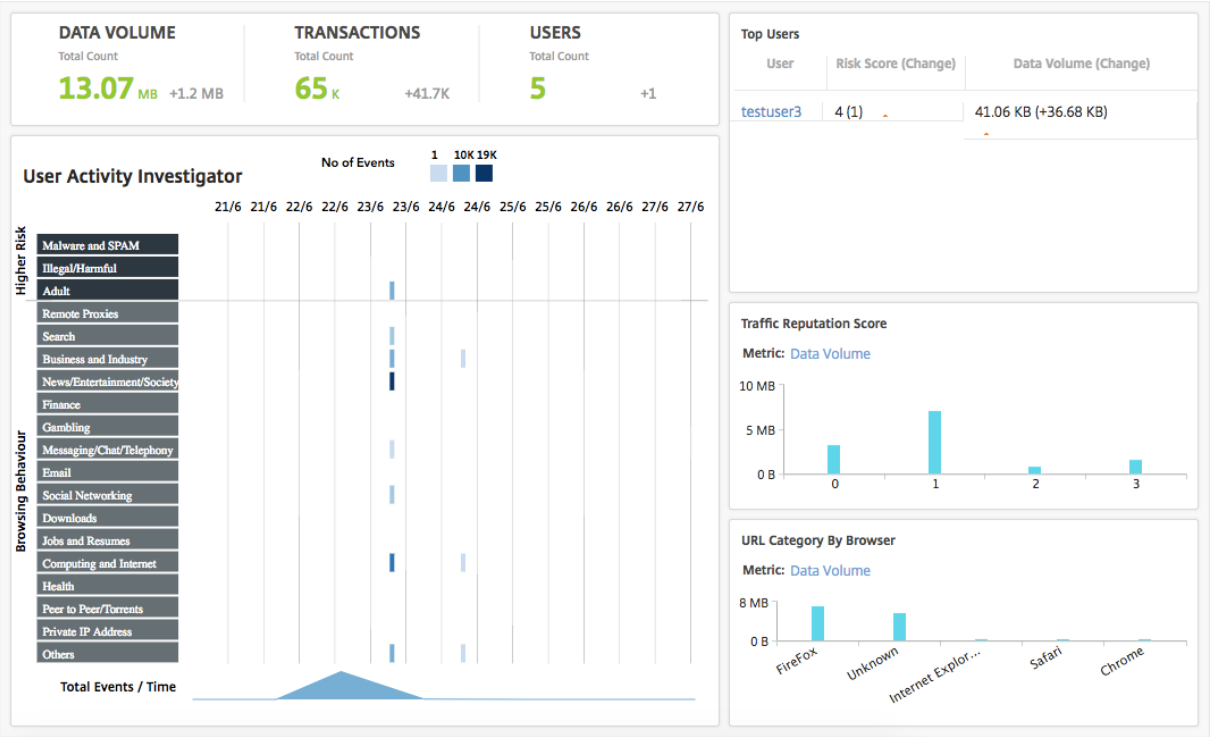
Vous pouvez cliquer sur une catégorie pour filtrer les graphiques afin d'afficher les détails liés à la catégorie pour la période spécifiée.

Tableau de bord utilisateur

Le **tableau de bord des utilisateurs** affiche un récapitulatif des activités effectuées par les utilisateurs dans votre entreprise. Il fournit des indicateurs clés que vous pouvez utiliser pour déterminer les éléments suivants :

1. Comportement de navigation des utilisateurs de votre entreprise.
2. Catégories d'URL auxquelles les utilisateurs de votre entreprise accèdent.
3. Les cinq principaux utilisateurs, en fonction de leurs scores de risque et de la bande passante qu'ils consomment. Pour plus d'informations sur le score de risque, voir Score de risque.
4. Navigateurs utilisés pour accéder aux URL ou aux domaines.
5. Montant du trafic Web généré par les utilisateurs, en fonction du score de réputation de trafic.

Pour accéder au Tableau de **bord utilisateur**, accédez à **Utilisateurs > Tableau de bord**.

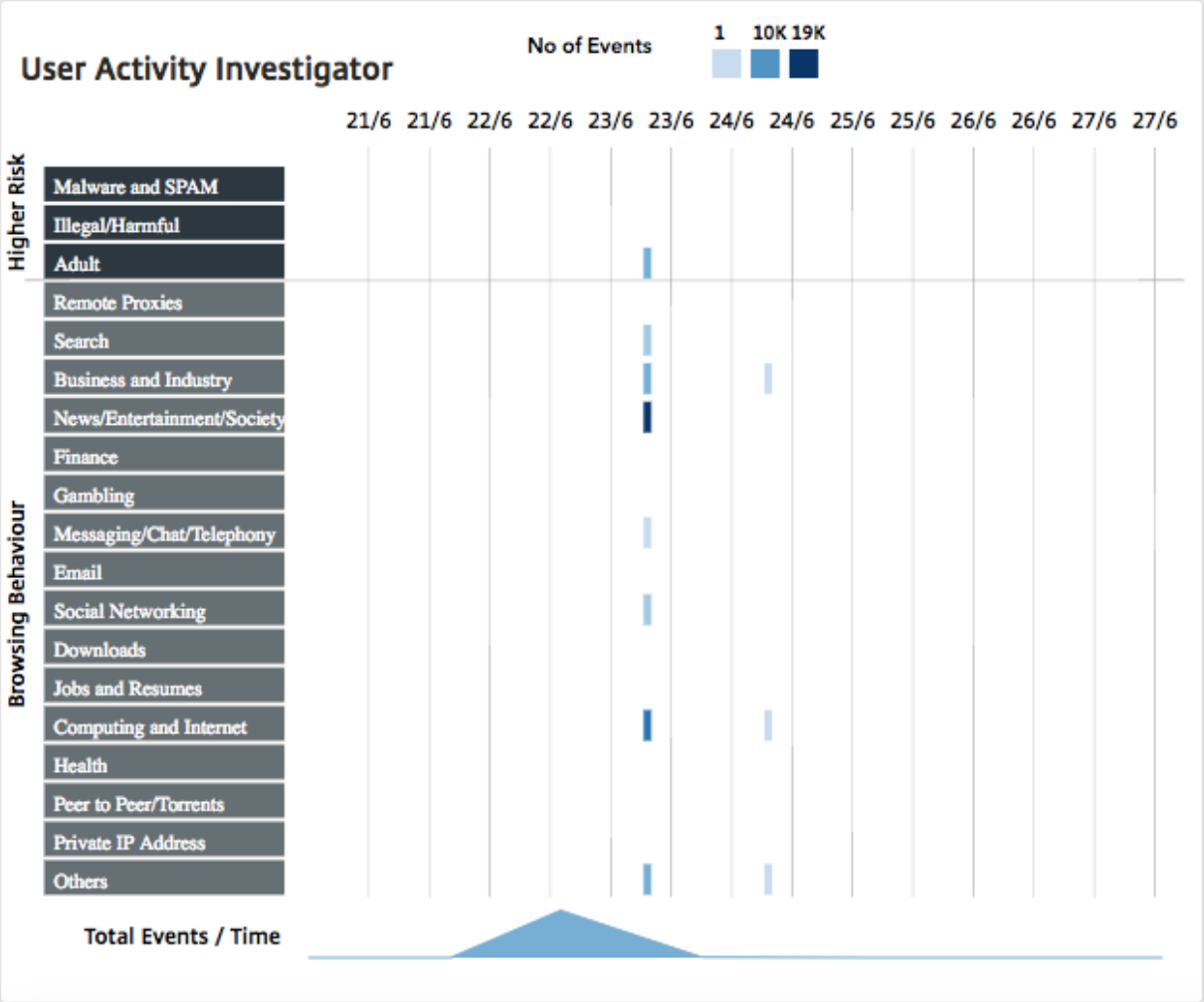


Vous pouvez cliquer sur un utilisateur dans le volet **Utilisateurs les plus importants** pour filtrer les graphiques afin d'afficher les détails de l'activité Web effectuée par l'utilisateur dans la période spécifiée.

Enquêteur d'activité utilisateur

Le **tableau de bord del'utilisateur comprend un volet de recherche d'activité utilisateur** qui affiche diverses activités Web effectuées par les utilisateurs. Il affiche les catégories d'URL auxquelles les utilisateurs accèdent pendant la période sélectionnée, ainsi que les différents événements déclenchés par catégorie d'URL. Vous pouvez cliquer sur les événements pour obtenir les détails du niveau de transaction.

L'**enquêteur d'activité utilisateur** affiche des informations clés telles que le comportement de navigation de l'utilisateur, les activités à haut risque de l'utilisateur et les événements déclenchés, par catégorie d'URL. Les événements sont présentés sous forme de légendes rectangulaires sur le graphique. Chacune des légendes est agrégée à intervalles d'une minute si la durée sélectionnée est d'une heure, et à intervalles d'une heure si la durée sélectionnée est d'un jour.



Ces légendes sont agrégées et sont codées par couleur en fonction du nombre d'événements qui se sont produits. Vous pouvez placer le pointeur de la souris sur une légende pour afficher des détails tels que l'heure et le nombre d'événements agrégés pour la légende sélectionnée. Vous pouvez personnaliser la période du graphique en sélectionnant une heure dans la liste des périodes.

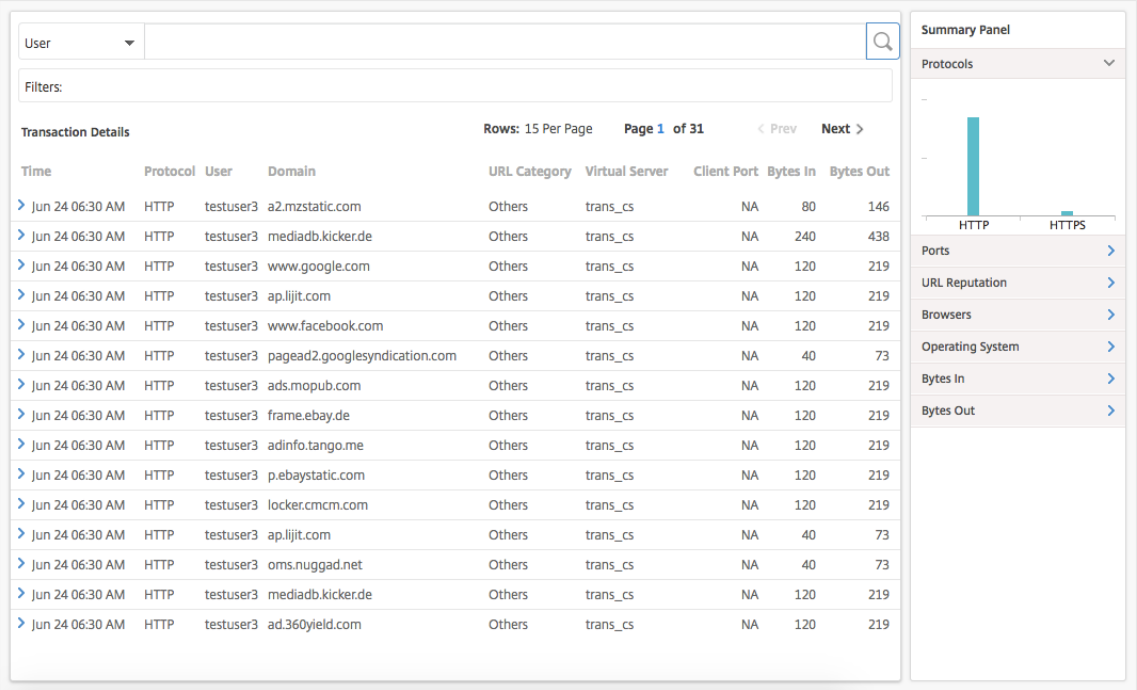
Vous pouvez cliquer sur les événements pour accéder plus en détail aux transactions.

Transactions des utilisateurs

La page Transactions utilisateur affiche les détails des transactions utilisateur dans votre réseau. Il fournit des informations au niveau des transactions, telles que :

1. Heure à laquelle la transaction a eu lieu
2. Protocole utilisé pour la transaction
3. Nom d'utilisateur
4. Domaine accédé par l'utilisateur

5. Catégorie d'URL
6. Serveur proxy utilisé pour intercepter la transaction
7. Détails du port client
8. Octets entrants
9. Octets sortants



Panneau récapitulatif Le **panneau de synthèse** affiche toutes les mesures des transactions qui sont visibles dans le volet **Détails de la transaction** . Ce panneau vous permet de trier et d'afficher les transactions dans le volet **Détails des transactions** en sélectionnant ou en désélectionnant les indicateurs. Le **panneau de synthèse** affiche les mesures suivantes :

Mesures	Description
Protocoles	Protocoles utilisés dans les transactions
Ports	Ports utilisés pour les transactions
Réputation d'URL	Score de réputation d'URL
Navigateurs	Navigateurs utilisés pour les transactions
Système d'exploitation	Système d'exploitation utilisé pour les transactions
Octets entrants	Quantité de données reçues via l'appliance Citrix ADC.

Mesures	Description
Octets sortants	Quantité de données envoyées via l'appliance Citrix ADC.

Score de risque

Le score de risque est un système de notation utilisé dans Citrix ADM pour déterminer les risques associés aux utilisateurs de votre entreprise. Citrix ADM attribue un score de risque basé sur le score de réputation d'URL attribué par l'appliance Citrix ADC pour les URL consultées par les utilisateurs de votre réseau. Pour plus d'informations sur le score de réputation d'URL, consultez Score de réputationd'URL. Le tableau suivant décrit les scores de risque attribués par Citrix ADM.

Cote de risque	Description
1	L'activité Web de l'utilisateur n'est pas perçue comme une menace ou n'est pas anormale.
2	L'activité Web de l'utilisateur ne présente aucune menace perçue ou n'est pas anormale, mais l'utilisateur accède à des « sites inconnus », pour lesquels aucun score de réputation d'URL n'est attribué.
3	Aucune menace n'est détectée dans l'activité Web de l'utilisateur, mais celui-ci a tenté d'accéder à des sites potentiellement vulnérables ou affiliés à des sites potentiellement vulnérables.
4	Utilisateur potentiellement compromis.
5	L'activité Web de l'utilisateur est anormale et l'utilisateur a accédé à des sites malveillants connus.

Cas d'utilisation

February 1, 2024

Surveillance des interceptions SSL

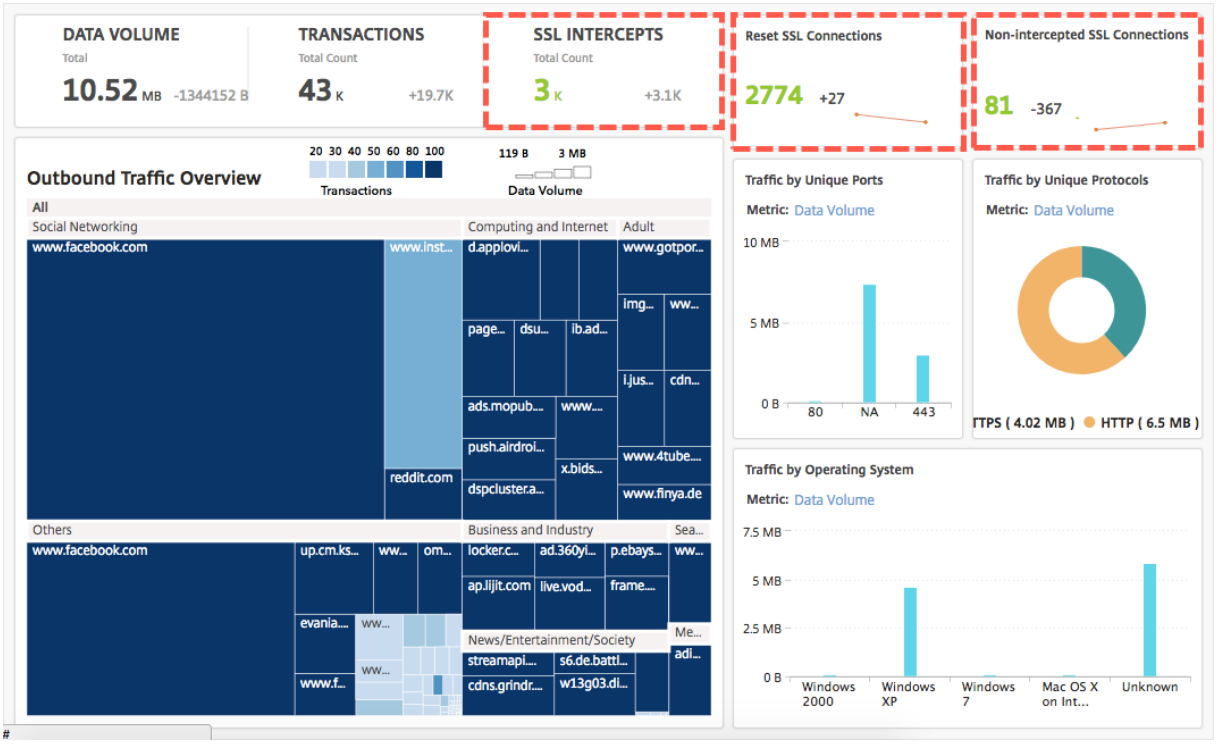
Une appliance Citrix ADC vous permet d'inspecter votre trafic sortant crypté. Vous pouvez intercepter, contourner ou bloquer toute requête HTTPS en fonction des stratégies configurées sur l'appliance. Citrix Application Delivery Management (ADM) fournit les détails suivants sur les connexions SSL dans le tableau de **bord du trafic sortant** pour une période sélectionnée :

- Nombre de connexions SSL interceptées, non interceptées et réinitialisées par l'appliance Citrix ADC
- Détails de la transaction des connexions SSL

À l'aide de ces détails, vous pouvez affiner les stratégies de votre appliance Citrix ADC afin d'inspecter efficacement le trafic sortant chiffré. Pour plus d'informations, consultez Citrix SSL Forward Proxy.

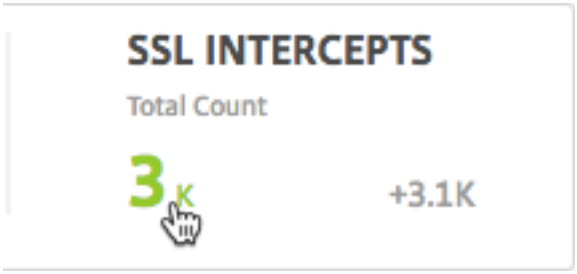
Pour afficher le nombre de connexions SSL interceptées, non interceptées et réinitialisées :

Accédez à **Applications > Tableau de bord du trafic sortant**.Le tableau de bord du trafic hors-bord affiche le nombre de connexions SSL interceptées, non interceptées et réinitialisées.

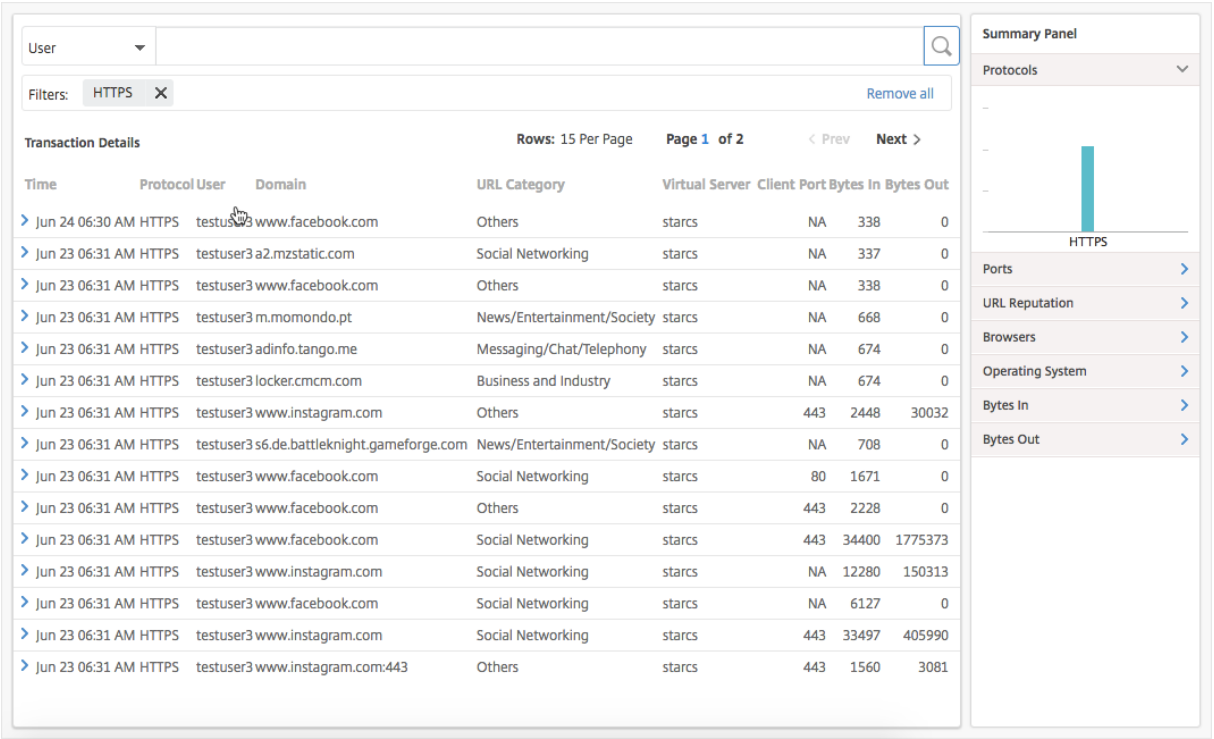


Pour afficher les détails de transaction des connexions SSL interceptées :

1. Accédez à **Applications > Tableau de bord du trafic sortant**.
2. Dans le tableau de **bord du trafic hors-bord**, cliquez sur le nombre total dans la section **INTERCEPTS SSL** .



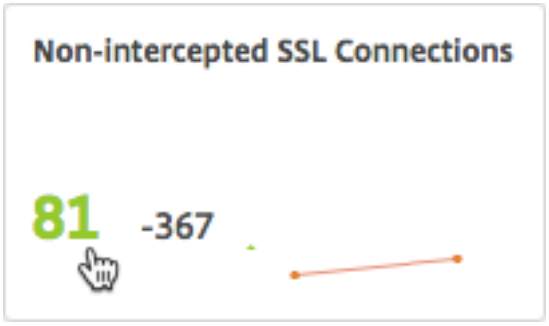
Les détails de transaction des connexions SSL interceptées au cours de la période sélectionnée sont affichés sur la page **Détails de la transaction**.



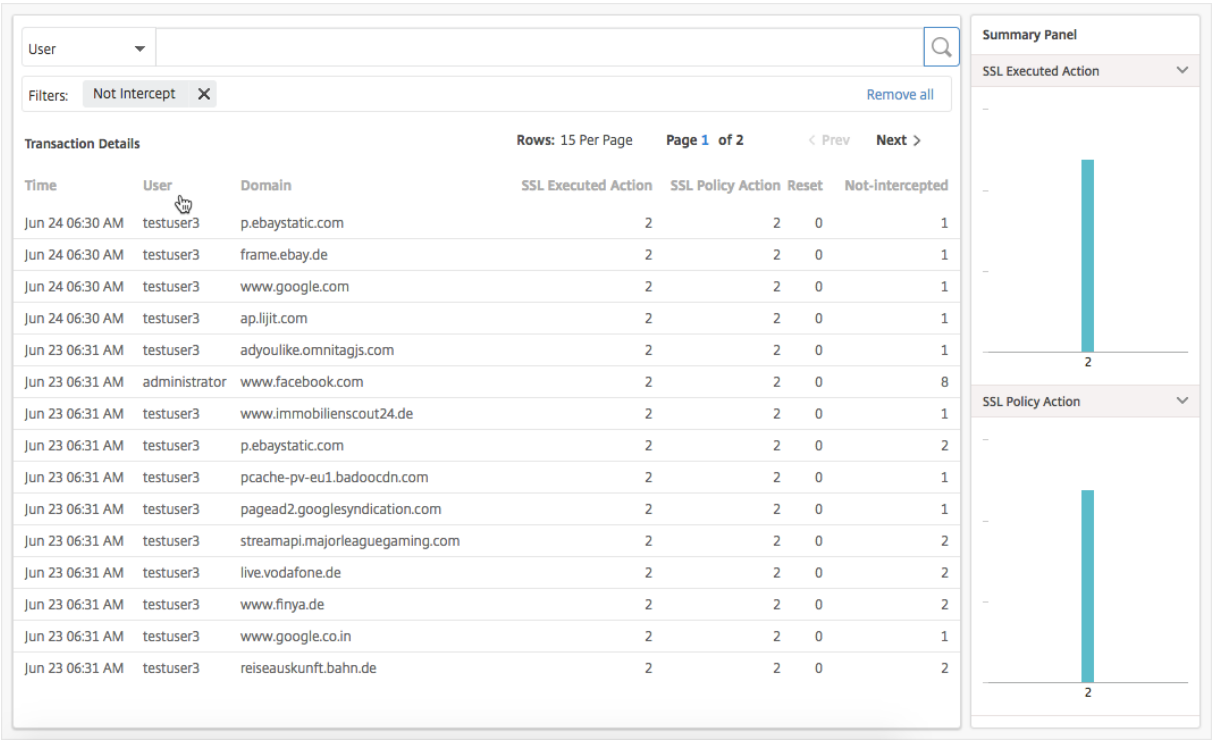
Vous pouvez également filtrer les détails des transactions par utilisateur et par catégorie d'URL.

Pour consulter les détails des transactions relatives aux connexions SSL sur lesquelles le trafic n'a pas été intercepté, procédez comme suit :

1. Accédez à **Applications > Tableau de bord du trafic sortant**.
2. Dans le tableau de **bord du trafic hors-bord**, cliquez sur le nombre total dans la section **Connexions SSL non interceptées** .



Les détails de transaction des connexions SSL sur lesquelles le trafic n'a pas été intercepté pendant la période sélectionnée apparaissent dans la page **Détails de la transaction**.

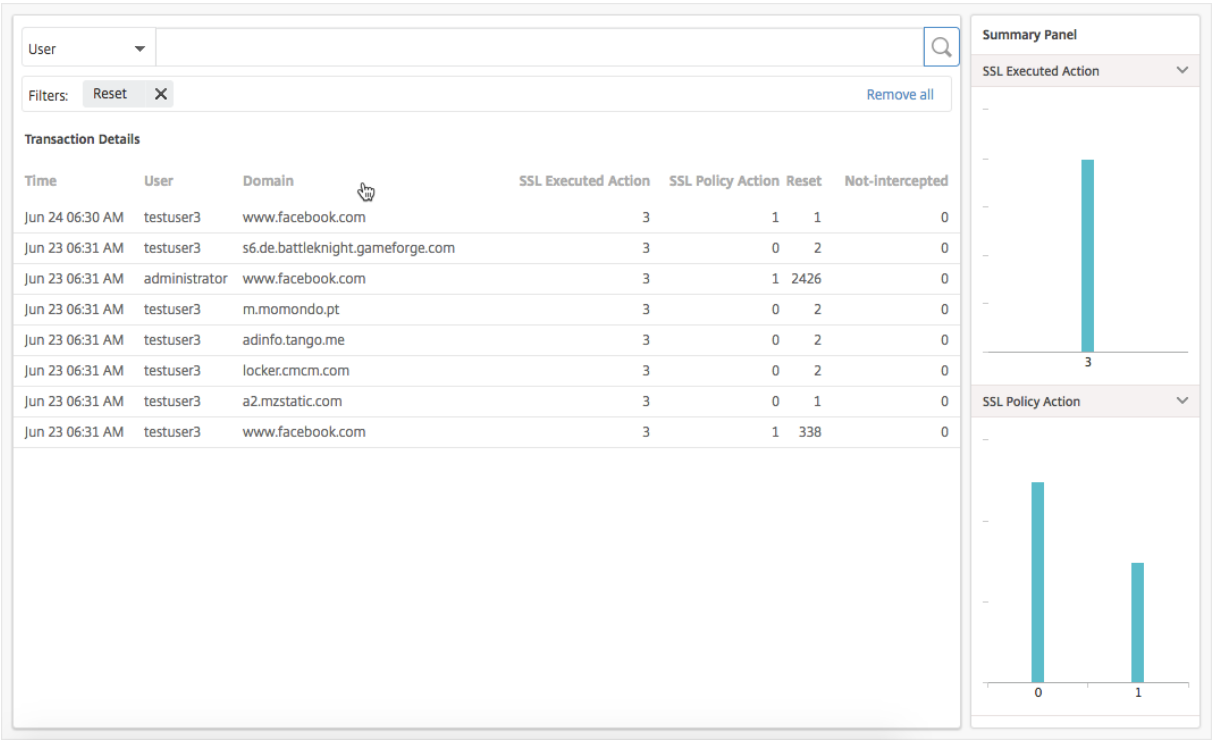


Vous pouvez également filtrer les détails des transactions par utilisateur et par catégorie d'URL.

Pour afficher les détails des transactions des connexions SSL qui sont réinitialisées, procédez comme suit :

1. Accédez à **Applications > Tableau de bord du trafic sortant**.
2. Dans le tableau de **bord du trafic hors-bord**, cliquez sur le nombre total dans la section **Réinitialiser les connexions SSL** .

Les détails de transaction des connexions SSL sur lesquelles le trafic n'a pas été intercepté pendant la période sélectionnée apparaissent sur la page **Détails de la transaction**.



Vous pouvez également filtrer les détails des transactions en fonction de l'utilisateur et de la catégorie d'URL.

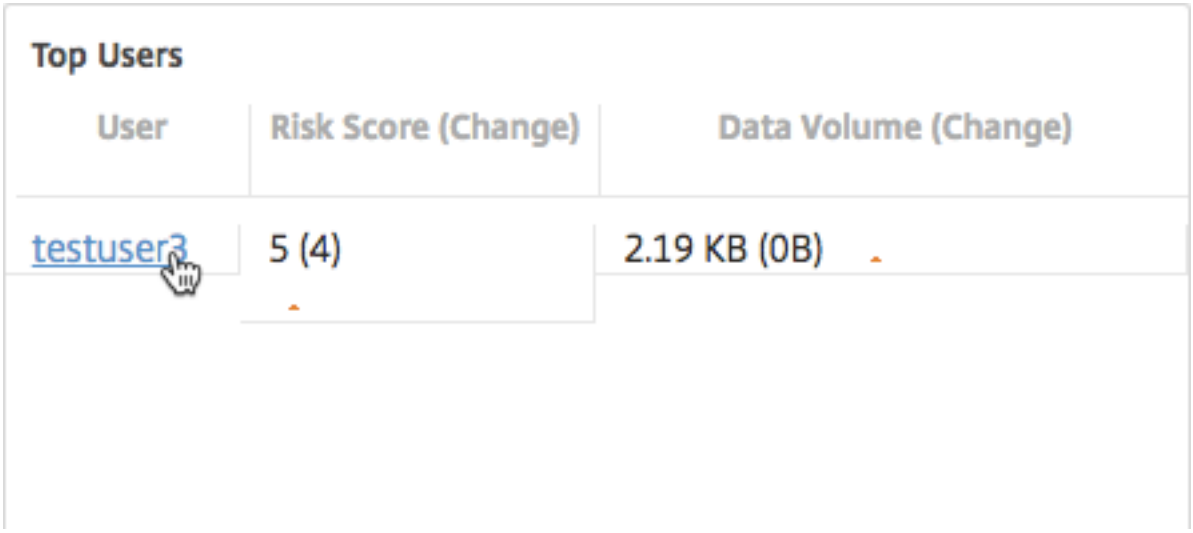
Inspection des terminaux

Les stratégies que vous avez configurées sur une appliance Citrix ADC spécifient la manière dont l'appliance enregistre toutes les activités des utilisateurs effectuées dans votre entreprise. Citrix ADM fournit des mesures clés que vous pouvez utiliser pour déterminer :

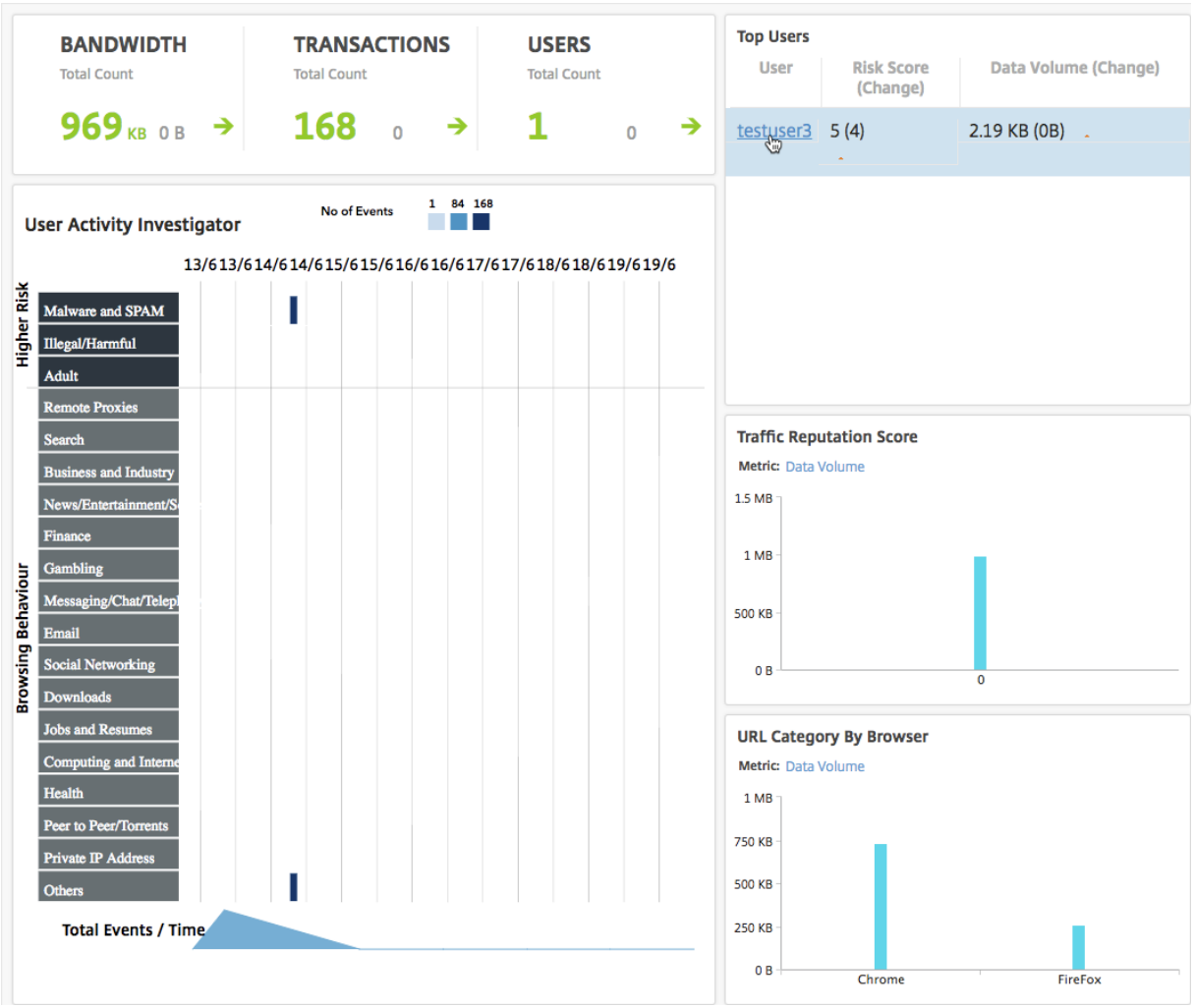
1. Comportement de navigation des utilisateurs de votre entreprise.
2. Catégories d'URL auxquelles les utilisateurs de votre entreprise accèdent.

3. Les cinq principaux utilisateurs, en fonction de leurs scores de risque et de la bande passante qu'ils consomment. Pour plus d'informations sur les scores de risque, consultez Score de risque.
4. Navigateurs utilisés pour accéder aux URL ou aux domaines.
5. Montant du trafic Web généré par les utilisateurs, en fonction du score de réputation de trafic.

Par exemple, si un utilisateur avec l'ID utilisateur testuser3 accède constamment à des sites liés à des logiciels malveillants dans votre entreprise, Citrix ADM identifie l'utilisateur en tant qu'utilisateur d'activité à haut risque et lui attribue un score de risque plus élevé. Les informations testuser3 sont affichées dans la section **Utilisateurs les plus importants** du tableau de **bord des utilisateurs**.

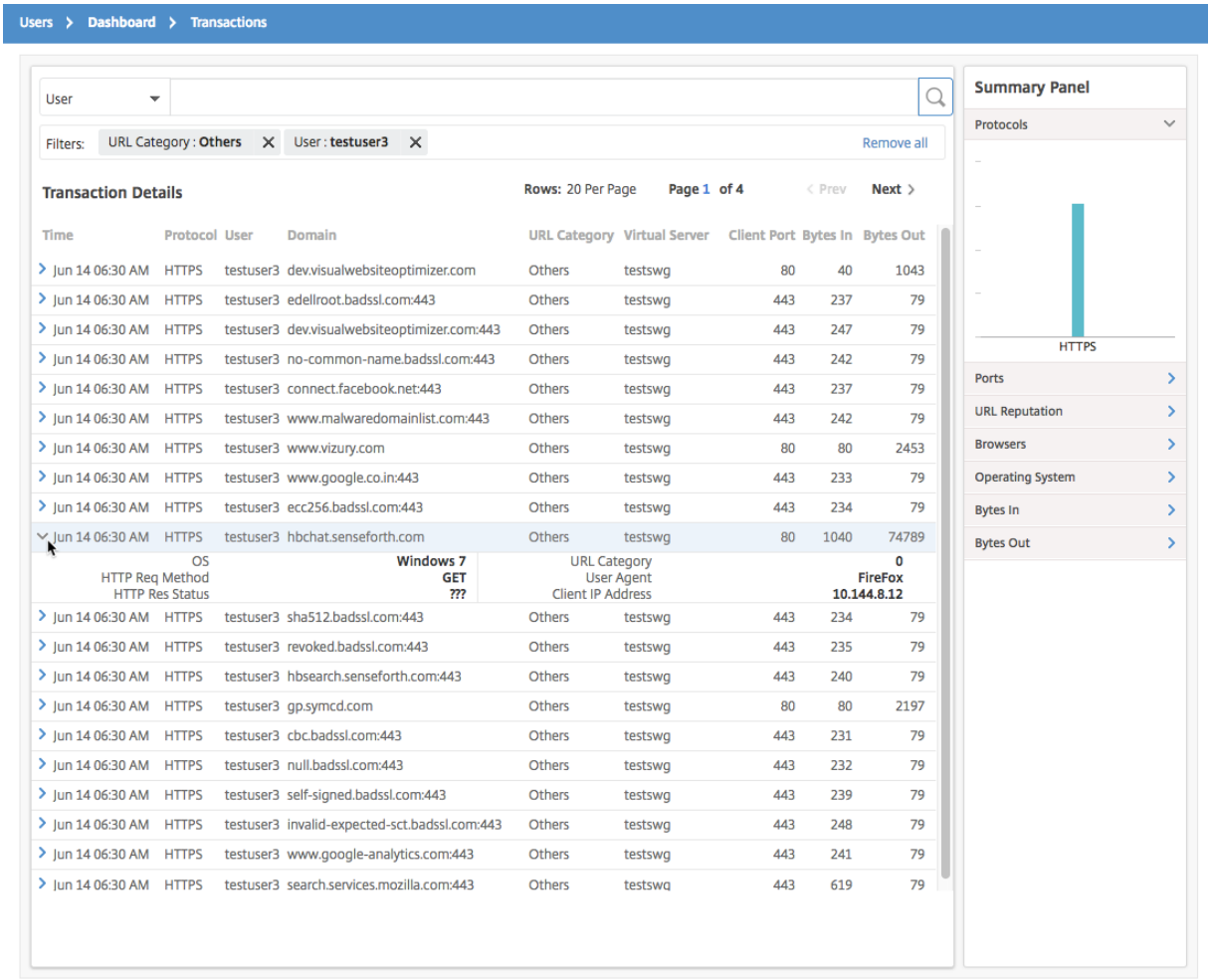


Vous pouvez cliquer sur testuser3 pour filtrer le **tableau de bord utilisateur** afin d'afficher toutes les mesures clés liées à testuser3.



Dans le volet **Enquête sur l'activité de l'utilisateur**, l'activité à haut risque de testuser3 s'affiche sous forme d'événements dans les catégories d'URL respectives.

Vous pouvez survoler les événements pour afficher le nombre d'événements et cliquer sur événements pour analyser les transactions qui se sont produites pendant les événements.

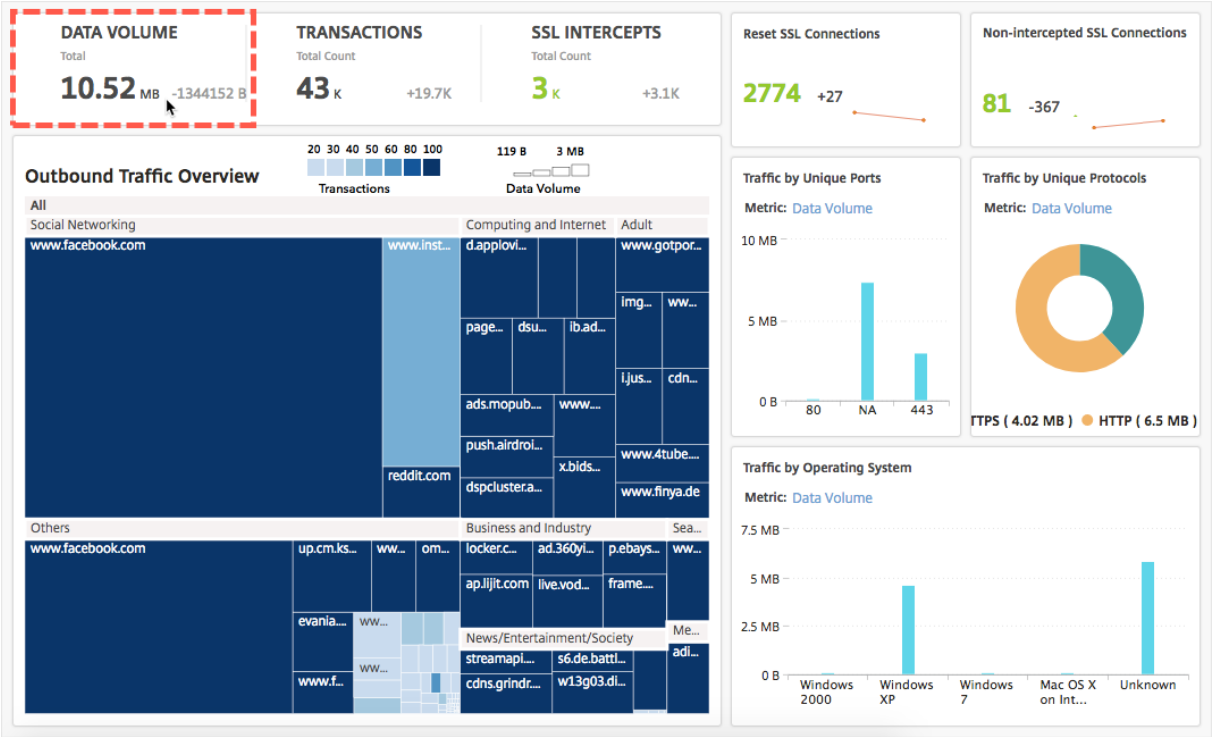


Grâce à ces informations, vous pouvez déterminer si votre système est infecté par des logiciels malveillants, ou bien comprendre le modèle de consommation de bande passante de l'utilisateur et affiner vos stratégies Citrix ADC. Pour plus d'informations, consultez la documentation Citrix SSL Forward Proxy.

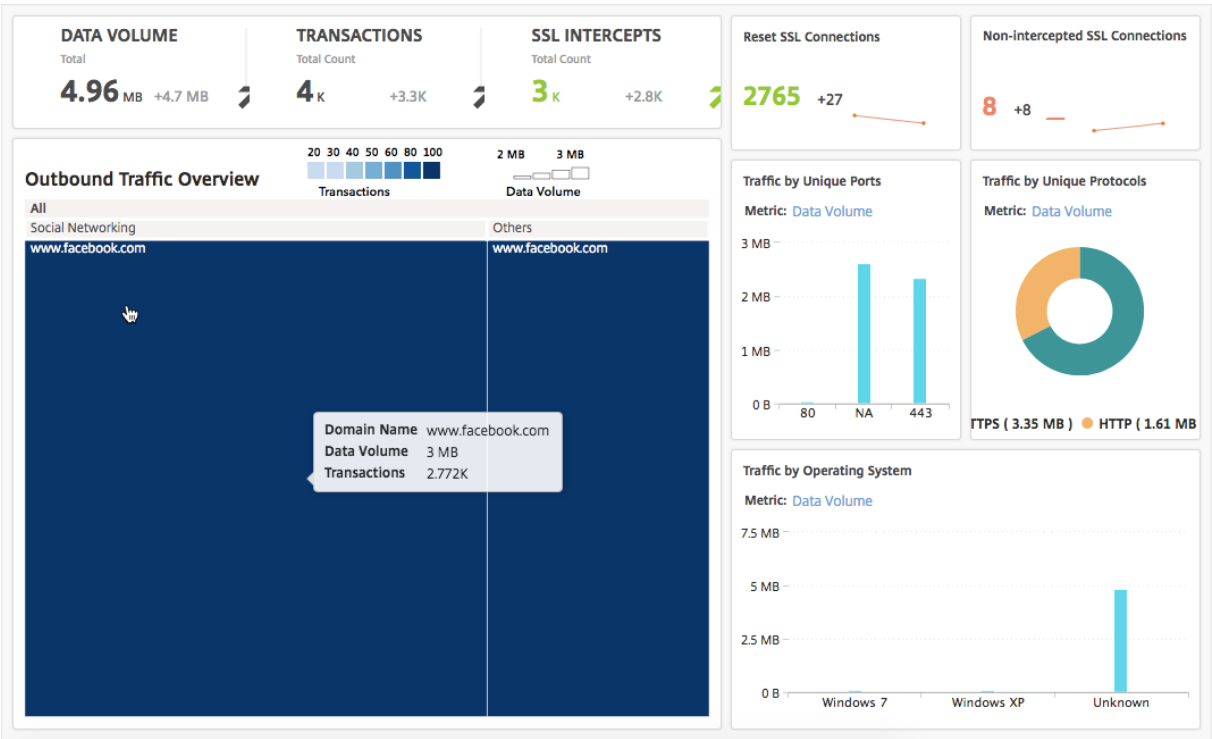
Rapports sur la consommation de bande passante

Le Tableau de **bord du trafic sortant** et le Tableau de **bord des utilisateurs** fournissent plusieurs graphiques qui résument les sites Web ou les applications accessibles à partir du réseau d'entreprise, ainsi que les activités effectuées par les utilisateurs de votre réseau.

Le tableau de **bord du trafic sortant** fournit les détails de la consommation du volume de données par les URL ou les domaines auxquels vous avez accédé depuis votre réseau. Accédez à **Applications > Tableau de bord du trafic sortant**, où les détails du volume de données sont affichés dans la section **Volume de données** .

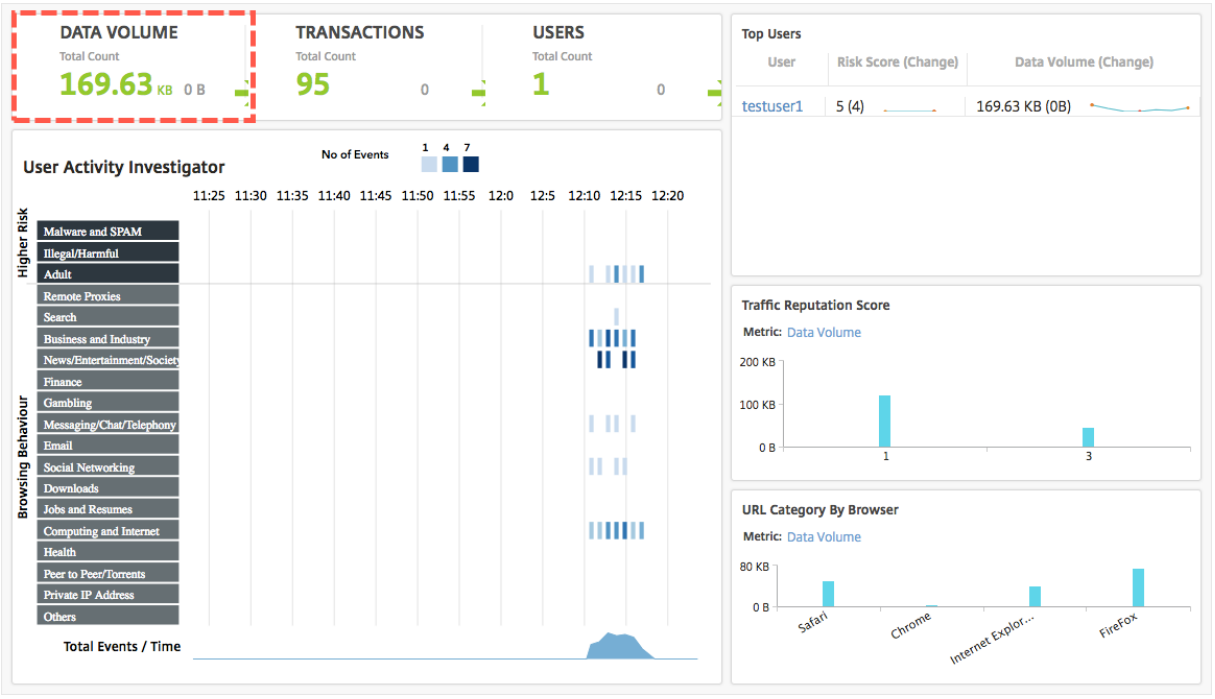


Dans le volet **Vue d'ensemble du trafic sortant**, vous pouvez cliquer sur un domaine ou une URL pour afficher les détails du volume de données consommé par le domaine ou l'URL.

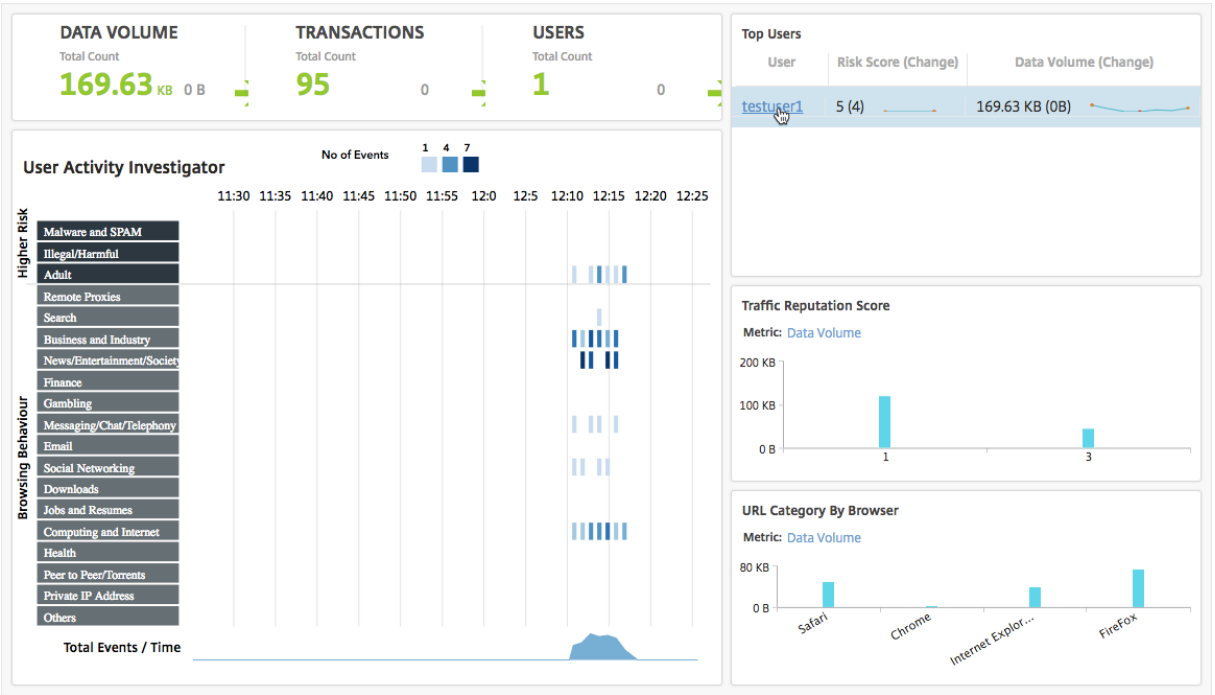


Le **tableau de bord utilisateur** fournit des détails sur la bande passante consommée par les utilisateurs de votre réseau. Accédez à **Utilisateurs > Tableau de bord** pour afficher les détails de la bande

passante consommée par les utilisateurs dans la section **VOLUME DE DONNÉES** du **Tableau de bord utilisateur**.



Vous pouvez afficher les détails de la bande passante consommée par un utilisateur en le sélectionnant dans la section **Utilisateurs les plus importants**. La section **VOLUME DE DONNÉES** et les autres mesures clés du graphique sont filtrées pour l'utilisateur sélectionné.



En utilisant ces détails, vous pouvez comprendre la consommation de bande passante et la raison de

la consommation. Par exemple, si un utilisateur accède à des sites Web de réseaux sociaux et que cela a entraîné une forte consommation de bande passante, l'administrateur peut accéder à l'appliance Citrix ADC et configurer une fonctionnalité de liste d'URL pour contrôler l'accès aux sites Web. Pour plus d'informations, consultez la rubrique Cas d'utilisation : Filtrage d'URL à l'aide d'un jeu d'URL personnalisé.

Affichage de la distribution du trafic sortant

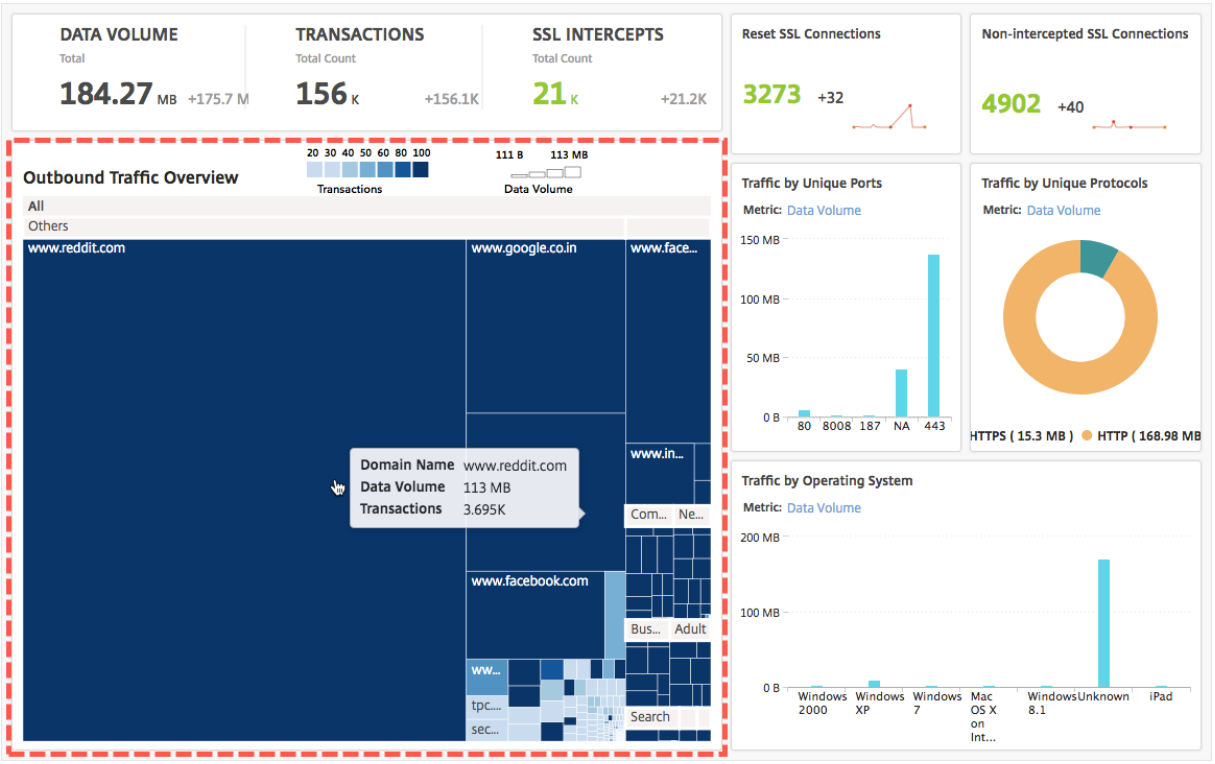
L'appliance Citrix ADC fournit des fonctionnalités de catégorisation et de filtrage d'URL que vous pouvez utiliser pour classer les URL accessibles depuis votre réseau. Dans Citrix ADM, le tableau de **bord du trafic sortant** inclut un volet **Présentation du trafic sortant**. Dans le volet **Vue d'ensemble du trafic sortant**, Citrix ADM regroupe les URL ou domaines accessibles en catégories, telles que Shopping, Actualités, Mobile, etc. pour afficher la distribution du trafic sortant dans votre réseau. Pour une période donnée, vous pouvez cliquer sur l'URL pour comprendre :

1. Bande passante consommée en accédant à l'URL
2. Transactions survenues lors de l'accès à l'URL
3. Nombre de connexions SSL qui ont été interceptées, non interceptées et réinitialisées lors de l'accès à l'URL

Grâce à ces informations, vous pouvez comprendre le schéma du trafic sortant et prendre des décisions correctives, par exemple s'il faut bloquer certaines URL.

Pour consulter la distribution du trafic sortant :

Accédez à **Applications > Tableau de bord du trafic sortant**.Le tableau de **bord du trafic hors-bord** affiche les URL dans le volet **Présentation du trafic sortant** :



Si vous souhaitez afficher les détails d'une URL particulière, sélectionnez l'URL.

À l'aide de ces informations, vous pouvez comprendre le modèle de trafic sortant et contrôler votre trafic réseau à l'aide d'un filtre d'URL configuré sur votre appliance Citrix ADC. Pour plus d'informations, consultez Filtrage d'URL.

Orchestration

February 1, 2024

Dans le cadre d'un réseau défini par logiciel (SDN), un contrôleur d'application logicielle gère un réseau et ses activités plutôt que le matériel qui prend en charge le réseau. En d'autres termes, le SDN permet aux administrateurs réseau de virtualiser une connectivité réseau physique en une connectivité réseau logique et de gérer les services réseau à l'aide d'un outil de gestion centralisée basé sur un logiciel. Le SDN permet aux ingénieurs réseau et aux administrateurs de répondre à l'évolution rapide des besoins de l'entreprise.

Bien que les avantages les plus connus du SDN soient la programmabilité du trafic, une plus grande agilité, la capacité de créer une supervision réseau basée sur des stratégies et la mise en œuvre de l'automatisation du réseau, certains des avantages spécifiques du SDN sont énumérés ci-dessous :

- Approvisionnement réseau centralisé

- Sécurité réseau accrue au niveau granulaire
- Coûts d'exploitation réduits
- Niveaux accrus d'abstraction du cloud
- Diffusion de contenu garantie
- Réduction des temps d'arrêt du réseau

Citrix Application Delivery Management (ADM) prend en charge le SDN dans le réseau des entreprises en s'intégrant aux contrôleurs SDN de différents fournisseurs. Citrix ADM prend en charge VMware NSX Manager et Cisco Application Policy Infrastructure Controller (APIC).

VMware NSX Manager

Citrix ADM s'intègre à la plate-forme de virtualisation réseau VMware pour automatiser le déploiement, la configuration et la gestion des services Citrix ADC. Cette intégration évite les complexités traditionnelles associées à la topologie de réseau physique, permettant aux administrateurs vSphere/vCenter de déployer par programmation les services Citrix ADC plus rapidement.

VMware NSX Manager présente des pare-feu logiques, des commutateurs, des routeurs, des ports et d'autres éléments de réseau pour permettre la mise en réseau virtuelle entre divers hyperviseurs, systèmes de gestion du cloud et matériels réseau associés. Il prend également en charge la mise en réseau externe et les services de sécurité.

La fonctionnalité Cloud Orchestration de Citrix ADM permet l'intégration des produits Citrix ADC avec VMware NSX et offre les fonctionnalités suivantes :

- Possibilité d'allouer un VPX à la demande préprovisionné à une certaine Gateway Edge dans le cadre de l'insertion de service.
- Possibilité de configurer des fonctionnalités avancées de Citrix ADC telles que SSL et CS ainsi que l'équilibrage de charge de base via des modèles d'application sur les instances qui s'exécutent dans l'environnement NSX.
- Possibilité de désallouer un VPX d'une certaine Gateway Edge dans le cadre de la suppression de service et de réaffecter le même VPX pour une autre Gateway Edge.
- Possibilité de déployer rapidement les fonctions Citrix ADC à partir de la console vCenter dans le cadre du flux de travail de déploiement de toute l'infrastructure requise pour une application.

Avantages :

- Allocation automatisée et à la demande de nouveaux services ADC dans le cadre d'un flux de travail de déploiement d'applications

- Configuration simplifiée des fonctionnalités ADC avancées spécifiques à l'application grâce à des modèles d'application
- Séparation des tâches multilocataires et modèle de consommation en libre-service tout en offrant aux administrateurs du cloud un point de contrôle unique
- Intégration plus facile avec les API Citrix ADM, qui aident à prendre en charge les utilisations futures imprévues.

Pour plus d'informations sur la façon de configurer VMware NSX Manager sur Citrix ADM, consultez Intégration de dispositifs Citrix ADC à VMware NSX Manager.

Mode hybride ACI Cisco

Cisco ACI a introduit la prise en charge du mode hybride dans la version 1.3 (2f). En mode hybride, vous pouvez effectuer l'automatisation du réseau via l'APIC (Application Policy Infrastructure Controller), tout en déléguant la configuration L4-L7 à Citrix ADM, qui agit en tant que Gestionnaire de périphériques dans l'APIC.

La solution Citrix ADC Hybrid Mode est prise en charge par un package de périphériques en mode hybride et Citrix ADM. Vous devez télécharger le package de périphérique en mode hybride dans l'APIC. Pour plus d'informations, consultezAutomatisation Citrix ADC à l'aide de Citrix ADM en mode hybride de Cisco ACI.

OpenStack : intégration d'instances Citrix ADC

February 1, 2024

La fonctionnalité Cloud Orchestration de Citrix Application Delivery Management (ADM) permet l'intégration des produits Citrix ADC avec la plate-forme OpenStack. En utilisant cette fonctionnalité avec la plate-forme OpenStack, les utilisateurs d'OpenStack peuvent utiliser la fonction d'équilibrage de charge (LBaaS) du Citrix ADC. Après cela, les utilisateurs OpenStack peuvent déployer leurs configurations d'équilibrage de charge à partir d'OpenStack dans l'instance de Citrix ADC.

Les sections suivantes fournissent une brève description des fonctionnalités du workflow d'intégration Citrix ADM et OpenStack.

Pilote Citrix ADC pour LBaaS OpenStack Neutron

Le plug-in OpenStack Neutron LBAAs inclut un pilote Citrix ADC qui permet à OpenStack de communiquer avec Citrix ADM. OpenStack utilise ce pilote pour transférer toute configuration d'équilibrage

de charge effectuée via les API LBAaS à Citrix ADM, qui crée la configuration d'équilibrage de charge sur les instances Citrix ADC souhaitées. OpenStack utilise également le pilote pour appeler Citrix ADM à intervalles réguliers afin de récupérer l'état des différentes entités (telles que les VIP et les pools) de toutes les configurations d'équilibrage de charge à partir des Citrix ADC. Le logiciel de pilote Citrix ADC pour la plate-forme OpenStack est fourni avec Citrix ADM. Pour télécharger et installer les pilotes, vous devez d'abord installer Citrix ADM et lancer l'application.

Enregistrement de Citrix ADM et OpenStack entre eux

Vous devez d'abord enregistrer les informations OpenStack sur Citrix ADM. Spécifiez l'adresse IP du Controller OpenStack et les informations d'identification de l'utilisateur d'administration du cloud, ainsi que les informations d'identification de l'utilisateur du pilote ADC OpenStack Citrix. Vous pouvez ensuite spécifier les mêmes informations d'identification de connexion dans la section Citrix ADC_Driver du fichier de configuration Neutron (neutron.conf) afin que le pilote Citrix ADC dans OpenStack puisse se connecter à Citrix ADM pendant les configurations LB.

Une fois OpenStack et Citrix ADM enregistrés les uns avec les autres, les deux peuvent se parler. En outre, les utilisateurs OpenStack peuvent utiliser leurs informations d'identification existantes dans OpenStack pour se connecter à l'interface utilisateur Citrix ADM afin de vérifier les performances de leurs configurations LB dans les Citrix ADC.

Locataires dans OpenStack

Dans OpenStack, un client est également appelé projet. Un locataire est un groupe d'utilisateurs ; un locataire ou un projet peut également être défini comme un ensemble de ressources (calcul, réseau, stockage, etc.) attribuées à un groupe isolé d'utilisateurs.

Stratégies de placement

Les stratégies de placement offrent la flexibilité nécessaire pour décider de l'instance Citrix ADC utilisée dans chaque configuration d'équilibrage de charge créée par les utilisateurs. Alternativement, Citrix ADM propose également une option permettant d'affecter une instance Citrix ADC en fonction des locataires OpenStack.

Paquets de services

Les packages de services sont des ensembles qui relient des stratégies/SLA, des spécifications de configuration des appareils ou du provisionnement automatique et des stratégies de locataire/de placement. Un package de services est généralement défini en termes de stratégies d'isolation fournies au locataire.

Voici quelques points relatifs aux packages de services :

- Un locataire ne peut pas participer à plus d'un ensemble de services.
- Plusieurs locataires peuvent être associés au même package de services.
- Dans un service package défini pour le provisionnement automatique, les instances virtuelles Citrix ADC peuvent être créées à partir d'un seul type de plate-forme (sur la plate-forme SDX ou sur la plate-forme OpenStack Compute).

Fonctionnalités prises en charge sur LBaaS V1 et LBaaS V2

Alors que le pilote LBaaS V1 dans OpenStack prend en charge les opérations à partir de l'interface utilisateur OpenStack Horizon, le pilote LBaaS V2 ne prend en charge que les opérations en ligne de commande.

La liste suivante répertorie les fonctionnalités prises en charge sur LBaaS V1 et LBaaS V2 sur OpenStack :

- LBaaS V1
  - Équilibrage de charge
- LBaaS V2
  - Équilibrage de charge
  - Déchargement SSL avec les certificats gérés par **Barbican**, le gestionnaire de clés dans OpenStack
  - Ensembles de certificats (y compris les autorités de certification intermédiaires)
  - Support SNI

Ce document fournit des informations sur :

- Scénario de cas d'utilisation
- Intégration de Citrix ADM avec OpenStack Workflow
- Prerequisites
- Tâches de pré-configuration dans Citrix ADM et OpenStack
- Étapes de configuration pour LBaaS V1 à l'aide d'Horizon
- Étapes de configuration pour LBaaS V2 à l'aide de la ligne de commande
- Provisionnement manuel de l'instance Citrix ADC VPX sur OpenStack
- Intégration de Citrix ADM avec OpenStack Heat Services
- Surveillance des applications OpenStack dans Citrix ADM

Scénario de cas d'utilisation

Le scénario d'utilisation suivant explique le flux de travail d'intégration de Citrix ADM à la plate-forme OpenStack :

Une entreprise, Example-Cloud-Provider, a utilisé des composants OpenStack pour configurer un cloud afin de fournir une infrastructure à ses locataires. Steve est l'administrateur de ce fournisseur de cloud, tandis que Tom est un locataire de l'infrastructure cloud de l'Example-Cloud-Provider. L'organisation de Tom, Example-Sportsonline.com, nécessite deux serveurs S1 et S1, et Tom nécessite également un périphérique Citrix ADC dédié pour équilibrer la charge du trafic entre les serveurs S1 et S2 sur la plate-forme OpenStack.

Pour répondre à cette exigence, Steve doit installer et configurer OpenStack et Citrix ADM, et les préparer à être compatibles les uns avec les autres. Steve doit créer un compte locataire nommé Example-SportsOnline dans OpenStack, puis allouer des ressources au compte locataire. Steve doit également créer différents identifiants de connexion (utilisateurs) pour Example-SportsOnline afin de gérer ses ressources et sa configuration. Tom peut désormais créer les deux serveurs S1 et S2 sur OpenStack pour gérer le trafic dans son organisation.

Steve doit enregistrer les détails OpenStack auprès de Citrix ADM et configurer le pilote LBaaS Citrix ADC dans le composant réseau OpenStack, Neutron. Une fois l'enregistrement terminé, Citrix ADM affiche les détails de tous les locataires dans OpenStack. Steve peut sélectionner Example-SportsOnline dans la liste qui souhaite les fonctionnalités de Citrix ADC LBaaS et configurer Tom pour obtenir un Citrix ADC dédié alloué pour ses configurations d'équilibrage de charge dans Citrix ADM.

Pour cela, Steve peut soit provisionner une instance Citrix ADC VPX sur la couche de calcul (Nova) d'OpenStack à l'aide de l'interface utilisateur Citrix ADM, soit permettre à MAS de provisionner automatiquement une instance Citrix ADC VPX à la demande, lorsque Tom effectue sa configuration LB dans OpenStack. Dans les deux cas, Citrix ADM gère l'instance VPX. Pour ce faire, Steve crée un package de service dans Citrix ADM, et définit les conditions du package de service qui ont été convenues dans le SLA avec Tom. Par exemple, Steve sélectionne la stratégie d'isolement « dédiée » pour fournir une instance dédiée pour fournir des configurations d'équilibrage de charge à Tom. Autrement dit, Steve sélectionne une instance non partagée pour Tom dans le package de services. Il attribue ensuite de nombreuses instances Citrix ADC VPX au service package, et associe Example-SportsOnline, ainsi que d'autres locataires, qui ont besoin d'un Citrix ADC dédié au service package. Par conséquent, lorsque Tom effectue sa première configuration d'équilibrage de charge, Citrix ADM attribue l'une des instances Citrix ADC VPX du service package à Example-SportsOnline et déploie également sa configuration dans ce Citrix ADC.

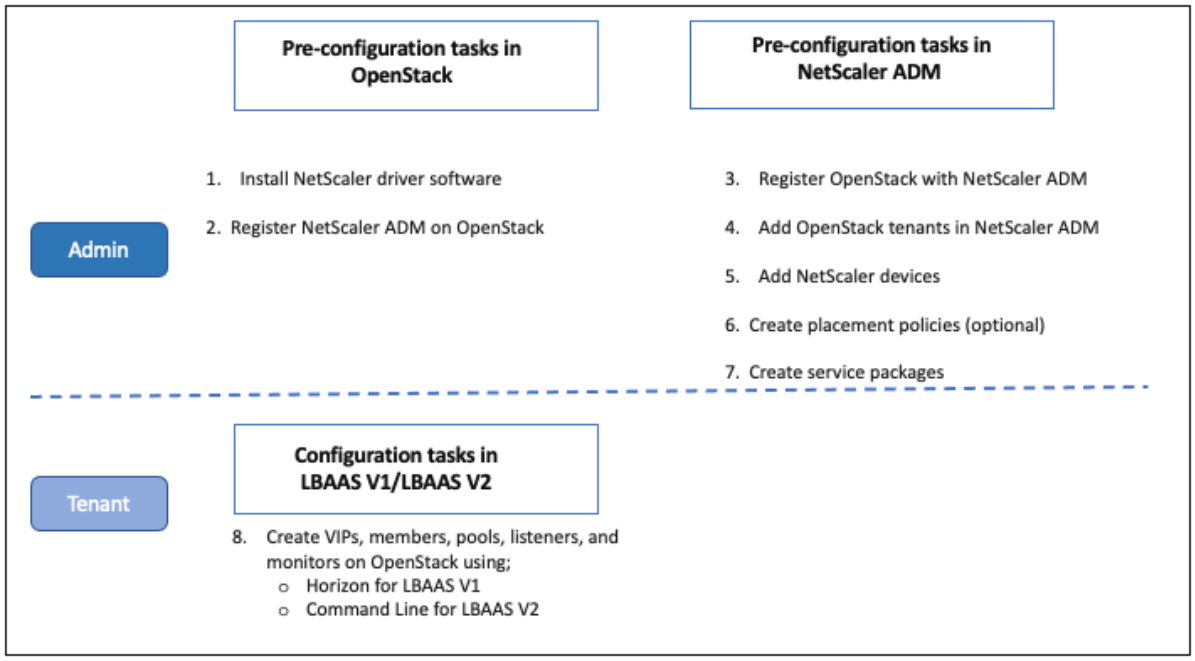
Tom peut désormais créer des configurations d'équilibrage de charge en créant des pools, des adresses IP virtuelles (VIP) et des moniteurs de santé à l'aide d'OpenStack LBAAS/UI. Les pools et les VIP dans OpenStack sont déployés en tant que groupes de services et serveurs virtuels sur l'instance de Citrix ADC. Tom peut également créer des moniteurs de santé pour surveiller les serveurs et

envoyer le trafic des applications uniquement aux serveurs qui sont UP à tout moment et accessibles depuis Citrix ADC.

La configuration d'équilibrage de charge créée dans OpenStack est désormais implémentée sur l'instance de Citrix ADC. Une fois entièrement configurée, l'instance Citrix ADC VPX reprend ensuite la fonctionnalité d'équilibrage de charge et commence à accepter le trafic de l'application et équilibre la charge le trafic entre les serveurs S1 et S2 créés par Tom.

Intégration de Citrix ADM avec OpenStack Workflow

L'organigramme suivant illustre le flux de travail que vous devez suivre lorsque vous configurez LBaaS V1 et LBaaS V2.



Conditions préalables

February 1, 2024

Avant d'intégrer l'instance virtuelle Citrix ADC à la plate-forme OpenStack, assurez-vous que les conditions suivantes sont remplies :

Configuration logicielle requise pour Citrix ADM et OpenStack

- Citrix ADM 13.0 est installé sur un poste de travail Hypervisor pris en charge qui répond à la configuration matérielle minimale requise.
- Les composants OpenStack sont installés et en cours d'exécution.
- Citrix ADM 13.0 prend en charge les versions d'OpenStack suivantes : **Newton**, **Ocata**, **Pike**et **Queens**.

Configuration matérielle requise pour Citrix ADM

Assurez-vous que les ressources informatiques virtuelles suivantes sont sur votre serveur OpenStack pour installer des instances virtuelles Citrix ADC :

Composant	Exigences
RAM	8 GB
CPU virtuel	8
Espace de stockage	500 GB
Interfaces réseau virtuelles	1
Débit	1 Gbit/s ou 100 Mbit/s

> **Remarque**
>
> Les besoins en mémoire et en disque dur spécifiés sont pour le déploiement de Citrix ADM sur la plate-forme OpenStack, étant donné qu'aucune autre machine virtuelle ne s'exécute sur l'hôte. La configuration matérielle requise pour OpenStack dépend du nombre de machines virtuelles qui s'y exécutent.

Tâches de pré-configuration dans Citrix ADM et OpenStack

February 1, 2024

Cette section vous aide à effectuer les tâches de pré-configuration avant de configurer Citrix Application Delivery Management (ADM) et OpenStack.

Installation de Citrix ADM

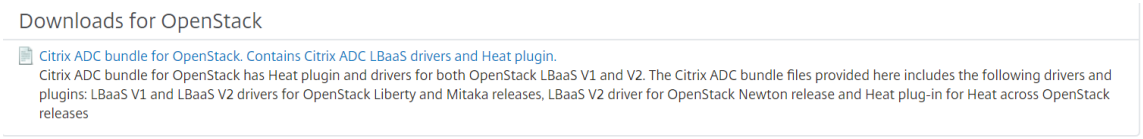
Installez Citrix ADM sur un Hypervisor pris en charge. Pour plus d'informations sur la façon de télécharger et d'installer Citrix ADM, consultez Déploiement de Citrix ADM.

Installation du pilote Citrix ADC et enregistrement de Citrix ADM sur OpenStack

Téléchargez l'offre groupée Citrix ADC pour OpenStack à partir de la page Téléchargements Citrix ADM.

Pour installer le pilote Citrix ADC sur la plate-forme OpenStack à l'aide de l'interface graphique Citrix ADM :

1. Dans Citrix ADM, cliquez sur **Téléchargements**. La page **Téléchargements** de Citrix ADM fournit des liens pour télécharger le **bundle Citrix ADC pour le logiciel OpenStack** requis pour les versions **Newton**, **Ocata**et **Pike** OpenStack.
2. Téléchargez le dernier fichier tar du bundle Citrix ADC dans un répertoire temporaire (par exemple, /tmp) dans OpenStack Controller. Ce bundle inclut le pilote LBaaS V2 et le plug-in Heat pour toutes les versions d'OpenStack.



3. Exécutez la commande suivante pour extraire les fichiers du fichier tar du pilote Citrix ADC :
   `tar -xvzf <name_of_tar_file>`
4. Si vous avez un OpenStack <Release Name> setup, à l'invite, tapez la commande suivante :

   `cd <Release Name>`

   Exemple :

   `cd Newton`
5. Exécutez la commande suivante pour installer le pilote et spécifier l'adresse IP Citrix ADM, le mot de passe du pilote Citrix ADC que vous avez configuré lorsque vous avez enregistré OpenStack auprès de Citrix ADM et le protocole :

   `./install.sh --ip=<NetScaler_MAS_IP> --password=<password> --protocol=<protocol> --neutron-lbaas-path <neutron-lbaas-directory-path>`

   Exemple pour la configuration d'OpenStack à nœud unique :

   `./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --neutron-lbaas-path=/opt/stack/neutron-lbaas`

Exemple de configuration d'OpenStack à plusieurs nœuds :

```
./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --
neutron-lbaas-path=/usr/lib/python2.7/site-packages
```

> **Remarque**
>
> La fourniture du chemin d'accès au `neutron-lbaas` répertoire du système est facultative. La fourniture du chemin d'accès peut aider le script à trouver les pilotes.
>
> Une fois que Citrix ADM est enregistré avec succès sur OpenStack, vous pouvez vous connecter à Citrix ADM à l'aide de vos informations d'identification utilisateur OpenStack.
>
> Une fois que Citrix ADM est enregistré avec succès sur OpenStack, redémarrez les services OpenStack Neutron.

Enregistrement d'OpenStack avec Citrix ADM

Pour enregistrer OpenStack auprès de Citrix ADM à l'aide de l'interface graphique Citrix ADM :

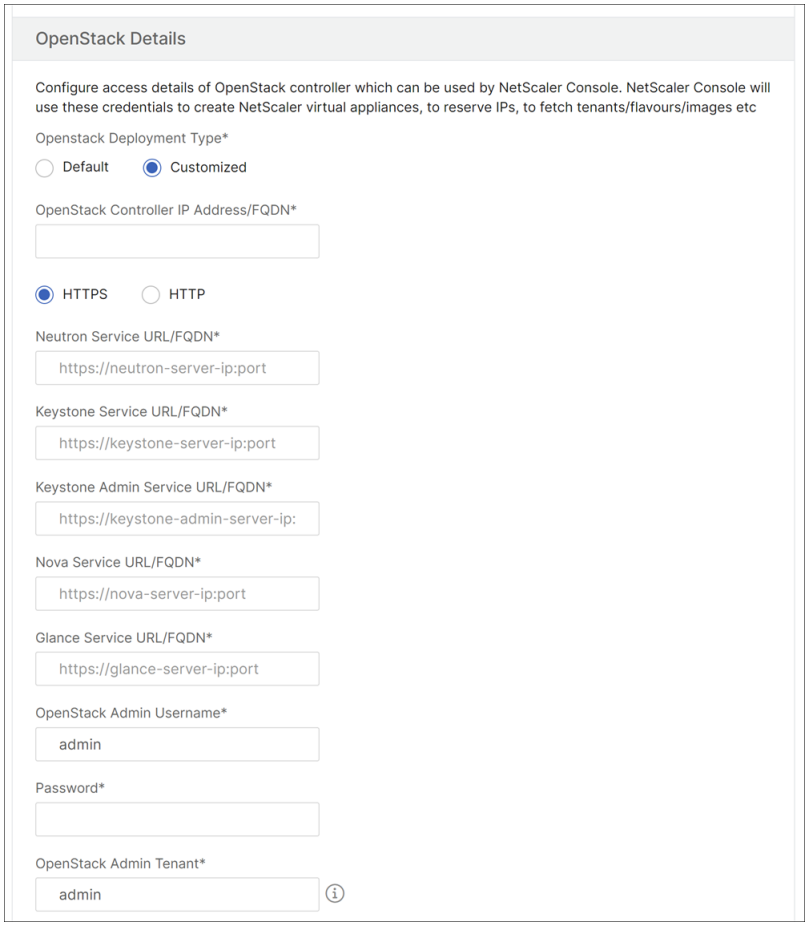
1. Dans Citrix ADM, accédez à**Orchestration** >**Cloud Orchestration**>**OpenStack**.
2. Cliquez sur **Configurer les paramètres OpenStack**.
3. Dans la page **Configurer les paramètres OpenStack**, vous pouvez définir les paramètres pour configurer OpenStack dans Citrix ADM. Vous avez deux options ici - Par défaut et Personnalisé.

   Pour les versions Newton et **Ocata** d'OpenStack, vous pouvez utiliser un type de déploiement par défaut ou personnalisé. Mais pour la version Pike, vous devez utiliser un type de déploiement personnalisé pour enregistrer OpenStack auprès de Citrix ADM.

- **Type de déploiement par défaut**

  Sélectionnez **Par défaut**, si les services OpenStack s'exécutent sur les ports par défaut. Par exemple, le portail par défaut pour les services Neutron est 9696, le portail par défaut pour les services Keystone est 5000.

1. Adresse IP du contrôleur OpenStack : adresse IP du contrôleur OpenStack (le service **KeyStone** et le service **Neutron** doivent tous deux être accessibles sur cette adresse IP). Par exemple, entrez l'adresse IP 10.102.205.23.
2. Nom d'utilisateur Admin OpenStack : nom d'utilisateur administratif du contrôleur OpenStack. Par exemple, entrez admin1.
3. Mot de passe : mot de passe de l'utilisateur administratif du contrôleur OpenStack.
4. OpenStack Admin Tenant : nom du locataire administratif sur OpenStack. Par exemple, entrez admin.

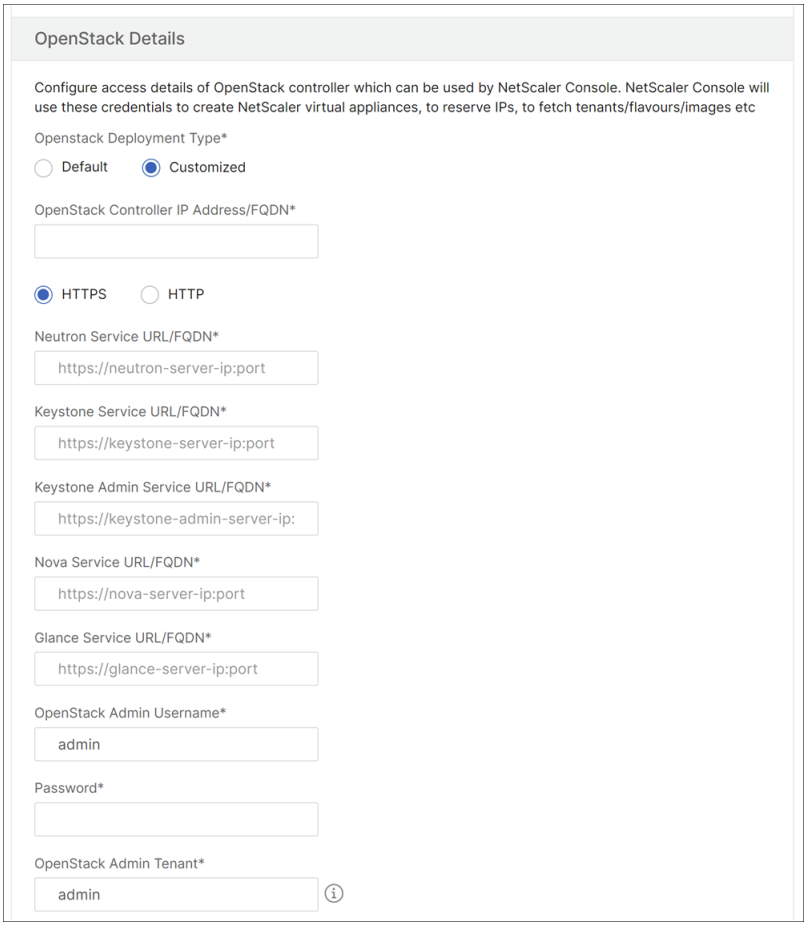


- **Type de déploiement personnalisé**

  Sélectionnez le type de déploiement comme **personnalisé** si les services OpenStack s'exécutent sur des ports différents des ports par défaut. Si ces services sont exécutés sur des ports différents, spécifiez-les ici. L'enregistrement des versions d'OpenStack Newton et **Ocata** auprès de Citrix ADM est différent de l'enregistrement de la version OpenStack Pike.

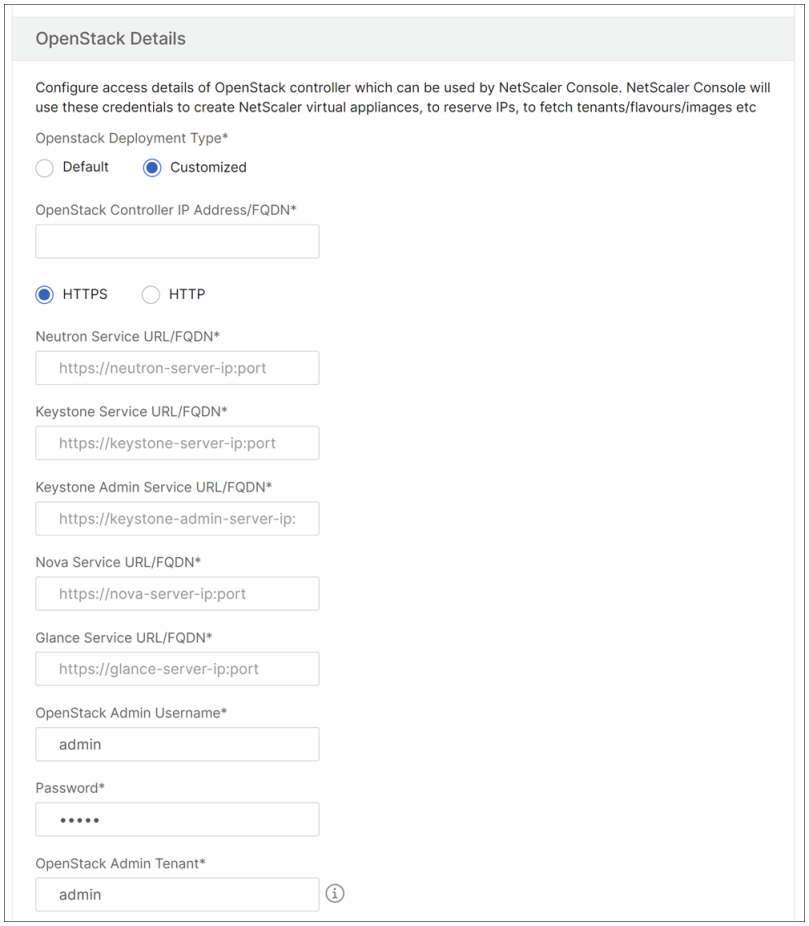
  Newton et Ocata Version d'OpenStack :

  1. Spécifiez les numéros de port pour les différents services OpenStack si vous enregistrez la version Newton d'OpenStack.
  2. Spécifiez le nom d'utilisateur, le mot de passe et le nom d'utilisateur du locataire d'administration OpenStack comme vous l'avez indiqué précédemment dans les paramètres **par défaut** .

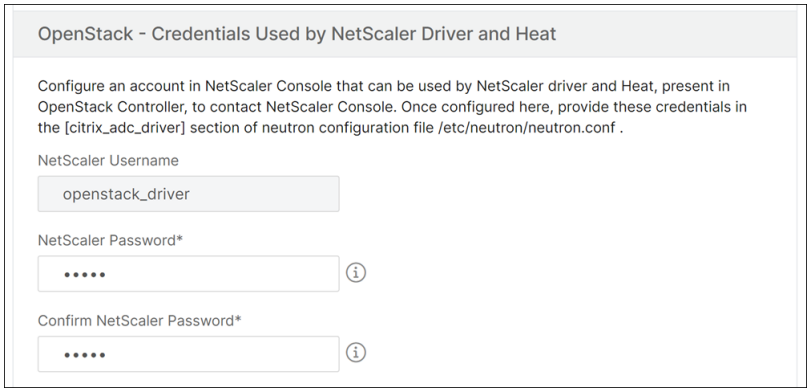


Pike Release d'OpenStack :

Si vous enregistrez la version Pike d'OpenStack, entrez les détails des services OpenStack comme indiqué dans l'image suivante. Vous devez également spécifier le nom d'utilisateur, le mot de passe et le nom d'utilisateur du locataire d'administration OpenStack comme indiqué dans les paramètres par défaut.



1. Dans la section**OpenStack Neutron LBaaS - Informations d'identification utilisées par Citrix ADC Driver**, définissez le mot de passe du pilote Citrix ADC pour le compte d'utilisateur du pilote ADC OpenStack Citrix. Citrix ADM authentifie les appels à partir du pilote ADC OpenStack Citrix à l'aide de ces informations d'identification. Vous devez spécifier le même mot de passe lorsque vous exécutez le script d'installation du pilote Citrix ADC dans le contrôleur OpenStack.



2. Cliquez sur **OK**.

Création d'un locataire sur OpenStack

Créez un projet ou un locataire sur OpenStack, ajoutez des utilisateurs au projet ou au locataire et attribuez des rôles à tous les utilisateurs. **KeyStone**, le service d'identité d'OpenStack fournit des services d'authentification pour chaque service OpenStack. Le service d'authentification utilise une combinaison de domaines, de projets (locataires), d'utilisateurs et de rôles.

Pour plus d'informations sur la création d'un projet et sur l'exécution d'autres tâches dans OpenStack, consultez la documentation d'OpenStack sur http://docs.openstack.org/.

Ajout de locataires OpenStack

1. Dans Citrix ADM, accédez à**Orchestration** >**Cloud Orchestration**> **OpenStack** >**Locataires OpenStack**, puis cliquez sur**Ajouter**.
2. Dans la page **Ajouter des locataires OpenStack**, cliquez sur **+Ajouter**, puis sélectionnez le locataire OpenStack.
3. Cliquez sur **OK**.

Selon que vous utilisez une instance pré-provisionnée ou le provisionnement automatique de l'instance lorsque vous intégrez OpenStack, procédez à l'une des deux tâches suivantes :

- Préprovisionner les périphériques Citrix ADC
- Provisionner automatiquement les appareils Citrix ADC VPX sur OpenStack

Provisionnement des périphériques Citrix ADC

Selon que vous utilisez une instance pré-provisionnée ou le provisionnement automatique de l'instance lorsque vous intégrez OpenStack, procédez à l'une des deux tâches suivantes :

- Préprovisionner les périphériques Citrix ADC
- Provisionner automatiquement les appareils Citrix ADC VPX sur OpenStack

Préprovisionnement des périphériques Citrix ADC

Installez le périphérique Citrix ADC sur l'une des plates-formes hyperviseurs telles que Citrix Hypervisor, KVM ou ESX, et ajoutez l'instance à Citrix ADM. Citrix ADM gère ensuite ce périphérique qui équilibre la charge du trafic dans les serveurs.

Pour ajouter une instance Citrix ADC VPX existante dans Citrix ADM :

1. Dans Citrix ADM, accédez à**Infrastructure** >**Instances** >**Citrix ADC VPX**, puis cliquez sur**Ajouter**.

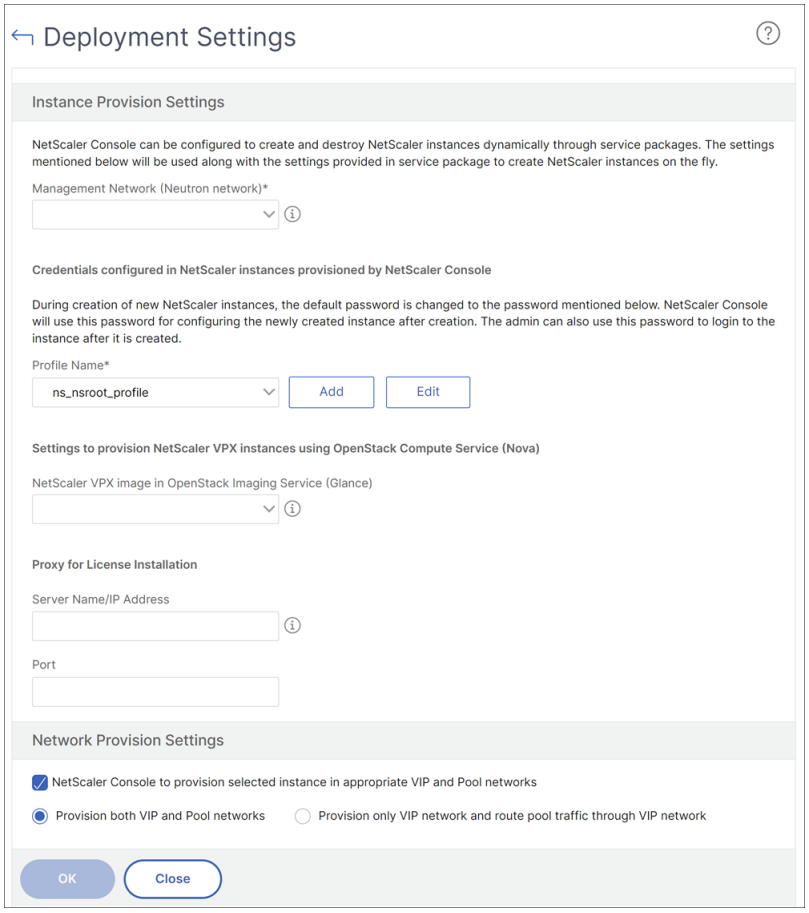
2. Sur la page**Ajouter un Citrix ADC VPX**, spécifiez l'adresse IP de l'instance Citrix ADC VPX et sélectionnez un profil d'instance dans la liste**Nom du profil**. Le profil d'instance contient les informations d'identification utilisées pour ouvrir une session au Citrix ADC VPX. Vous pouvez également créer un profil d'instance en cliquant sur l'icône +. Cliquez sur **OK**.

Provisionnement automatique des périphériques Citrix ADC

Téléchargez l'image d'instance Citrix ADC requise à partir de la page de téléchargement Citrix, puis téléchargez-la sur Glance, le service OpenStack Imaging. La disponibilité d'une image sur Glance vous permet de configurer une instance Citrix ADC à la demande lors de l'attribution de l'instance au locataire.

Pour provisionner automatiquement les périphériques Citrix ADC VPX sur OpenStack :

1. Dans Citrix ADM, accédez à **Orchestration** > **Cloud Orchestration** > **OpenStack**.
2. Cliquez sur**Paramètres de déploiement**.
3. Définissez les paramètres suivants :
    a) Réseau de gestion : sélectionnez le réseau de gestion sur OpenStack, auquel le Citrix ADC VPX provisionné automatiquement est connecté.
    b) Nom du profil : sélectionnez le profil dans la liste déroulante. Citrix ADM utilise le mot de passe contenu dans ce profil pour configurer de nouvelles instances Citrix ADC VPX provisionnées automatiquement.
    c) Licences : fournissez les codes d'accès aux licences Citrix ADM utilisés pour attribuer des licences aux nouvelles instances Citrix ADC auto-provisionnées. Citrix ADM provisionne les instances Citrix ADC sur le calcul OpenStack dans le réseau de gestion, puis déclenche l'installation de licence sur ces instances à l'aide du code de licence spécifié. L'instance Citrix ADC télécharge ensuite les fichiers de licences à partir du site Web Citrix à l'aide du code d'accès de licence spécifié ici.
    d) Citrix ADC VPX Image in Glance : sélectionnez l'image Citrix ADC VPX disponible dans OpenStack Glance qui est utilisée pour créer une instance VPX Citrix ADC.
    e) Paramètres proxy : fournit des détails sur le serveur proxy Citrix ADC pour l'installation des licences. Cela peut être nécessaire lorsque Citrix ADC n'a pas accès direct à Internet via le réseau de gestion.
4. Cliquez sur **OK**.



Création d'un service package dans Citrix ADM

Pour créer des packages de services pour un locataire dans Citrix ADM :

1. Dans Citrix ADM, accédez à **Orchestration** > **Cloud Orchestration** > **OpenStack** > **Service Packages**, puis cliquez sur **Ajouter**.
2. Dans la page **Service Package**, spécifiez les paramètres suivants :
   a) Name : nom du package de service. Par exemple, entrez SVC-PKG-GOLD.
   b) Allocation d'instance Citrix ADC : type d'allocation d'instance défini dans le package de services basé sur lequel les ressources d'instance Citrix ADC sont allouées à un locataire. Sélectionnez **Dédié**. Pour plus d'informations sur les stratégies, consultez Stratégies d'isolation des packages de services.
   c) Provisioning d'instance Citrix ADC : sélectionnez **Instance existante**pour allouer une instance Citrix ADC existante à un locataire. Si vous souhaitez créer des instances Citrix ADC pendant la configuration elle-même, sélectionnez **Create Instance OnDemand**.
   d) Citrix ADC Instance Type - sélectionnez **Citrix ADC VPX**.

> **Remarque**
>
> Sélectionnez Citrix ADC VPX pour allouer des instances Citrix ADC préprovisionnées hébergées sur la plate-forme SDX.

3. Cliquez sur **Continuer** pour associer un locataire à un package de services.

> **Remarque**
>
> Activer le **provisionnement de la paire d'instances Citrix ADC pour la haute disponibilité**, si vous déployez les instances Citrix ADC en mode haute disponibilité.

4. **Dans la section Affecter des instances**, cliquez sur **Ajouter**, puis sélectionnez l'instance Citrix ADC que vous souhaitez affecter au locataire, puis cliquez sur **Continuer**.
5. Dans la section **Affecter des locataires OpenStack ou des stratégies de placement**, sous **Locataires OpenStack**, cliquez sur **Ajouter,** puis sélectionnez le locataire.
6. Cliquez sur **Continuer**, puis sur **Terminé**.

> **Remarque**
>
> Si la stratégie n'est pas trouvée, le mécanisme de secours est rétabli et Citrix ADM attribue des instances Citrix ADC en fonction des locataires. Si le locataire ne fait partie d'aucun package de services, Citrix ADM affiche un message d'erreur indiquant : « Le locataire <admin> ne fait partie d'aucun Service Package et il n'y a aucun Service Package par défaut. »

Création de stratégies de placement (facultatif)

Les stratégies d'isolation ne sont pas uniquement basées sur les locataires. Vous pouvez créer des stratégies de placement flexibles, où elles sont basées non seulement sur le nom ou l'ID du locataire, mais également sur d'autres attributs personnalisés.

Pour créer des stratégies de placement pour un locataire dans Citrix ADM :

1. Dans Citrix ADM, accédez à **Orchestration** > **Cloud Orchestration** > **OpenStack** > **Stratégie de placement**, puis cliquez sur **Ajouter**.
2. Dans la page **Ajouter une stratégie de placement**, définissez les paramètres suivants :
    a) Nom : entrez un nom pour la stratégie de placement
    b) Exemples d'expressions : sélectionnez un exemple d'expression dans la liste. Ces exemples sont utiles pour élaborer la stratégie de placement.
    c) Expression : une expression booléenne est renseignée dans ce champ en fonction de l'exemple d'expression que vous avez sélectionné dans le champ précédent. Modifiez les noms des champs selon vos besoins.

3. Cliquez sur **OK**.

Activation du trafic des instances Citrix ADC vers les serveurs principaux via le réseau client

Par défaut, dans le workflow d'orchestration OpenStack, les instances Citrix ADC sont liées dynamiquement à l'équilibreur de charge ou aux réseaux clients et aux réseaux membres ou serveurs.

Dans certains déploiements, les serveurs sont également accessibles via les réseaux clients et peuvent être routés via la Gateway client. Dans de tels cas, les instances Citrix ADC ne doivent pas être liées aux réseaux de serveur, mais elles doivent être liées uniquement aux réseaux clients.

Effectuez le paramètre suivant pour configurer le trafic via la Gateway client.

Accédez à **Orchestration** > **Cloud Orchestration** > **OpenStack** > **Paramètres de déploiement**, puis sélectionnez l'option **Provisionner uniquement le réseau VIP et acheminer le trafic de pool via le réseau VIP**.

Citrix ADM configure ensuite l'instance Citrix ADC sur les réseaux clients en ajoutant un SNIP dans ce réseau et ajoute une route par défaut à la Gateway réseau client. Cela permet à l'instance d'atteindre les serveurs via la Gateway client.

Provisionnement automatique des périphériques Citrix ADC VPX déployés sur la plate-forme Citrix ADC SDX

Ajoutez la plate-forme Citrix ADC SDX dans Citrix ADM, de sorte que Citrix ADM provisionne les instances sur cette plate-forme à la demande.

Pour provisionner automatiquement les instances Citrix ADC déployées sur la plate-forme Citrix ADC SDX :

1. Dans l'interface graphique Citrix ADM, accédez à**Réseaux** >**Instances** >**Citrix ADC SDX**, puis cliquez sur**Ajouter** pour ajouter une plate-forme Citrix ADC SDX.
2. Accédez à **Orchestration** > **Cloud Orchestration** > **OpenStack** > **Paramètres de déploiement.**
3. Dans**la section Réseau**de gestion, sélectionnez le réseau de gestion sur OpenStack auquel le SDX Citrix ADC provisionné automatiquement est connecté.
    a) Dans**Nom du profil**, sélectionnez le profil dans la liste déroulante. Citrix ADM utilise le mot de passe contenu dans ce profil pour configurer de nouvelles instances Citrix ADC VPX provisionnées automatiquement.
    b) Cliquez sur **OK**.

4. Pour provisionner la plate-forme Citrix ADC SDX dans OpenStack, accédez à**Orchestration** >**Cloud Orchestration**>**OpenStack**>**Service Package**.

    a) Cliquez sur**Ajouter** pour créer un nouveau service package.

    b) Entrez le nom du package de services.

    c) Dans le champ**Allocation d'instance Citrix ADC**, sélectionnez**Dédié**.

    d) Dans le champ**Citrix ADC Instance Provisioning**, sélectionnez**Create Instance OnDemand**et dans le champ**Auto Provisioning Platform**, sélectionnez**Citrix ADC SDX**.

    e) Par défaut, seules les instances Citrix ADC VPX sont provisionnées sur la plate-forme SDX Citrix ADC.

    f) Cliquez sur **Continuer**.

    g) Dans la section**Paramètres de mise en service automatique**, définissez les propriétés**des ressources** .

        i. Champ de **débit** . Entrez 1000 Mbps.

        ii. Champ**Version de Citrix ADC**. Dans la liste, sélectionnez la bonne version de l'image Citrix ADC VPX présente sur la plate-forme Citrix ADC SDX.

    h) Dans la section**Plates-formes SDX Citrix ADC**, cliquez sur**Ajouter** pour ajouter la plate-forme SDX au service package.

    i) Cliquez sur **Continuer**.

    j) Dans la section **Configurer les locataires d'OpenStack**, cliquez sur**Ajouter** pour ajouter les locataires. Vous pouvez également ajouter de nouveaux locataires en cliquant sur**Nouveau**.

    k) Cliquez sur**Terminé**.

5. Les implémentations de l'API LBaaS V2 sont effectuées à l'aide de commandes LBaaS Neutron. Connectez-vous à n'importe quel client Neutron et exécutez les tâches de configuration. Pour plus d'informations sur la façon d'exécuter des commandes de configuration, consultezConfiguration de LBaaS V2 à l'aide de la ligne de commande.

Configurer LBaaS V1 à l'aide d'Horizon

February 1, 2024

Tom peut désormais se connecter au portail OpenStack Horizon, créer un pool LBaaS et sélectionner un sous-réseau dans lequel se trouvent tous les membres de ce pool. Tom doit ajouter une adresse IP

virtuelle (VIP) et attribuer cette adresse VIP au pool qu'il a créé. Tom peut également effectuer cette opération en ligne de commande ou via des API. Les clients externes pour les serveurs de Tom peuvent se connecter à cette adresse VIP, qui est hébergée sur l'Citrix ADC attribué, et Citrix ADC distribue toutes les requêtes aux membres du pool sur les ports configurés.

Les membres du pool LBaaS sont les serveurs équilibrés de charge qui sont ajoutés au pool sélectionné. Tom peut attribuer un poids et un port à chacun de ces membres.

Les moniteurs de santé sont utilisés pour surveiller la santé et le bon fonctionnement de tous les membres du pool. Tom peut créer un modèle de surveillance de l'état de santé dans OpenStack en spécifiant les limites de délai, de délai d'expiration et de nouvelle tentative, ainsi qu'en spécifiant la méthode, le chemin de l'URL et les codes HTTP attendus en cas de succès. Après avoir créé un moniteur, Tom doit associer le moniteur au pool précédemment créé.

Pour plus d'informations sur la façon de créer des pools et d'autres tâches de configuration LBaaS dans OpenStack, consultez la documentation OpenStack.

> **Important**
>
> LBaaS V1 n'est pas pris en charge dans la version Liberty d'OpenStack. Pour plus d'informations, consultez les notes de version d'OpenStack.

Configurer LBaaS V2 à l'aide de la ligne de commande

February 1, 2024

Le LBaaS V2 prend en charge le déchargement SSL avec des certificats gérés par **Barbican** , des ensembles de certificats (y compris des autorités de certification intermédiaires), la prise en charge du SNI ainsi que les fonctionnalités habituelles d'équilibrage de charge. LBAaS V2 prend uniquement en charge l'interface de ligne de commande pour exécuter les tâches de configuration. Les implémentations de l'API LBaaS V2 sont effectuées à l'aide de commandes LBaaS Neutron.

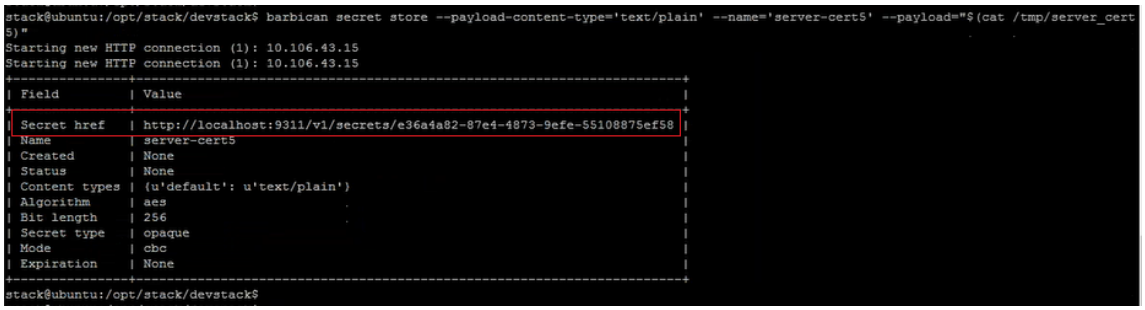
> **Remarque**
>
> Téléchargez le certificat et la clé vers le service **Barbican** lorsque vous avez besoin de la fonction de déchargement SSL. Effectuez les étapes 1, 2 et 3 si le déchargement SSL est pris en charge, sinon continuez à partir de l'étape 4 pour créer un équilibreur de charge, un écouteur, un pool et un membre.

1. Téléchargez le certificat vers le service **Barbican** à l'aide de la commande suivante :

```
barbican secret store --payload-content-type <content_type> --name
    <certificate_name> --payload<certificate_location>
<!--NeedCopy-->
```


Exemple :

```
barbican secret store --payload-content-type='text/plain' --name='
    hp_server_certificate' --payload=" hp_server/tmp/
    server_certificate"
<!--NeedCopy-->
```



2. Téléchargez la clé vers le service **Barbican** à l'aide de la commande suivante :

```
barbican secret store --payload-content-type <content_type> --name
     <key_name> --payload<key_location>
<!--NeedCopy-->
```

Exemple :

```
barbican secret store -- payload-content-type='text/plain' --name=
    'shp_server_key' --payload="hp-server/tmp/server_key"
<!--NeedCopy-->
```

> **Remarque**
>
> Lorsque vous exécutez ces deux commandes **Barbican** pour charger le certificat et la clé, les champs href Secret fournissent un emplacement ou une URL. C'est là que le certificat et la clé sont stockés sur le système sur lequel OpenStack est installé. Copiez ces liens et fournissez ces liens en tant que paramètres lorsque vous créez le conteneur sur le service **Barbican** à l'étape 3.

3. Créez un conteneur dans le service **Barbican** pour stocker le certificat et la clé à l'aide de la commande suivante :

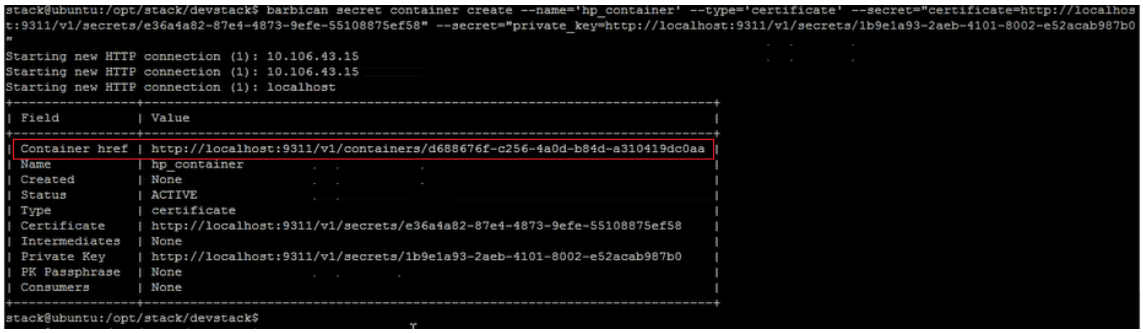
   Dans la commande, remplacez avec l'URL que vous avez obtenue dans le champ Secret href

lorsque vous avez téléchargé le certificat. De même, remplacez avec l'URL que vous avez obtenue dans le champ Secret href lorsque vous avez téléchargé la clé.

```
barbican secret container create --name<container_name> --type<
    container_type> --secret<certificate_url> --secret<key_url>
<!--NeedCopy-->
```

Exemple :

```
barbican secret container create --name='hp_container' --type='
    certificate' --secret="`certificate=http://localhost:9311/v1/
    secrets/e36a4a82-87e4-4873-9efe-55108875ef58 --secret="
    private_key=http://localhost:9311/v1/secrets/1b9e1a93-2aeb
    -4101-8002-e52acab987b0`"
<!--NeedCopy-->
```



Copiez la valeur href du conteneur. Vous devez fournir le lien vers le conteneur lors de la création de l'écouteur à l'étape 6.

4. Définissez les variables d'environnement dans OpenStack. Les variables permettent aux commandes du client OpenStack de communiquer avec les services OpenStack.

   Exemple :

   export OS_PASSWORD-hp

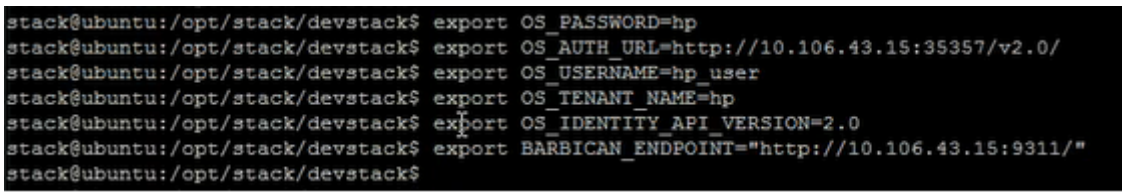
   export OS_AUTH_URL=http://10.106.43.15:35357/v2.0/

   export OS_USERNAME=hp_user

   export OS_TENANT_NAME=hp

   export OS_IDENTITY_API_VERSION=2.0

   export BARBICAN_ENDPOINT="http://10.106.43.15:9311/"



> **Remarque**
>
> Définissez ces variables pour chaque session SSH avant d'exécuter d'autres commandes. Pour plus d'informations sur les variables d'environnement OpenStack, consultez Variables d'environnement OpenStack.

5. Créez un équilibreur de charge à l'aide de la commande suivante :

```
neutron lbaas-loadbalancer-create --name <loadbalancer-name>  <
    subnet-name> --provider <netscaler>
<!--NeedCopy-->
```

Exemple :

```
neutron lbaas-loadbalancer-create --name hp-lb-test hp-sub1 --
    provider netscaler
<!--NeedCopy-->
```

```
stack@ubuntu:/opt/stack/devstack$ neutron lbaas-loadbalancer-create --name hp-lb-test hp-sub1 --provider netscaler
Created a new loadbalancer:
+---------------------+--------------------------------------+
| Field               | Value                                |
+---------------------+--------------------------------------+
| admin_state_up      | True                                 |
| description         |                                      |
| id                  | 746d730b-3b63-418f-a816-d8dd5472963c |
| listeners           |                                      |
| name                | hp-lb-test                           |
| operating_status    | OFFLINE                              |
| provider            | netscaler                            |
| provisioning_status | PENDING_CREATE                       |
| tenant_id           | 0f30b93cd0cd4482b92d033e1628aa8f     |
| vip_address         | 15.0.0.27                            |
| vip_port_id         | 36636748-15c1-4ec3-9328-496ee74e64fc |
| vip_subnet_id       | 0bb433c4-4b90-4de0-803f-9df92aa46ac4 |
+---------------------+--------------------------------------+
stack@ubuntu:/opt/stack/devstack$
```

L'état passe de PENDING_CREATE à ACTIVE après la création de l'équilibreur de charge.

```
+--------------------------------------+------------+-------------+---------------------+-----------+
| id                                   | name       | vip_address | provisioning_status | provider  |
+--------------------------------------+------------+-------------+---------------------+-----------+
| 0d5e8e17-41c2-41bb-aab5-2b3f8f5af4c5 | hp-lb8     | 15.0.0.25   | ACTIVE              | netscaler |
| 1092f752-aa25-4262-aacc-014725fe2921 | hp_lb3     | 15.0.0.19   | ACTIVE              | netscaler |
| 41dbe490-6d9c-4ce5-8d88-bb55953f5961 | hp-lb7     | 15.0.0.24   | ACTIVE              | netscaler |
| 746d730b-3b63-418f-a816-d8dd5472963c | hp-lb-test | 15.0.0.27   | ACTIVE              | netscaler |
| 9d65f6a4-5be5-44fd-a4bd-0808084557b0 | hp-lb1     | 15.0.0.18   | ACTIVE              | netscaler |
| cf8ee4b7-a9f5-41c5-a76a-cd2520e0a7a3 | hp-lb6     | 15.0.0.23   | ACTIVE              | netscaler |
| f7f7dd6e-28eb-40f2-b26c-e541138c6a06 | hp-lb4     | 15.0.0.20   | ERROR               | netscaler |
+--------------------------------------+------------+-------------+---------------------+-----------+
```

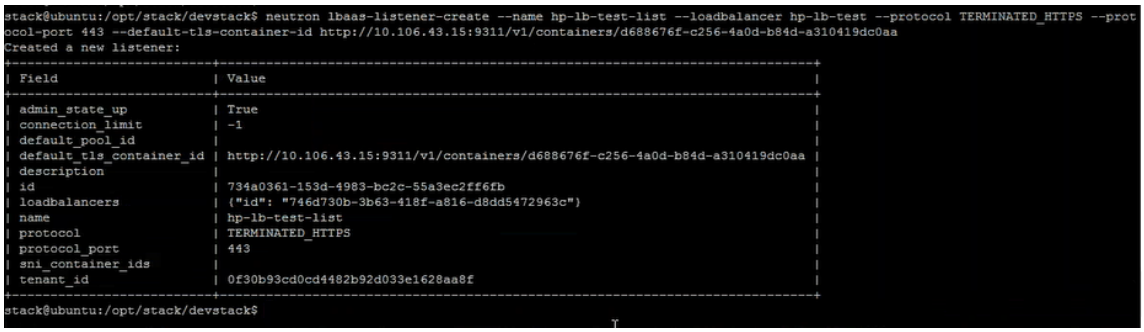
6. Créez un écouteur à l'aide de la commande suivante :

```
neutron lbaas-listener-create --loadbalancer <loadbalancer-name>
    --name <listener-name> --protocol <protocol_type> --protocol-
    port <port_number> --default-tls-container-id<container_url>
<!--NeedCopy-->
```

Exemple :


```
neutron lbaas-listener-create --name hp-lb-test-list  --
    loadbalancer hp-lb-test --protocol TERMINATED_HTTPS --protocol-
    port 443 --default-tls-container-id `http://10.106.43.15:9311/
    v1/containers/d688676f-c256-4a0d-b84d-a310419dc0aa`
<!--NeedCopy-->
```

> **Remarque**
>
> Si vous créez un écouteur sans prise en charge du déchargement SSL, exécutez la commande suivante sans fournir d'emplacements au conteneur :
>
> `neutron lbaas-listener-create --loadbalancer <loadbalancer-name> --name <listener-name> --protocol <protocol_type> --protocol-port <port_number>`

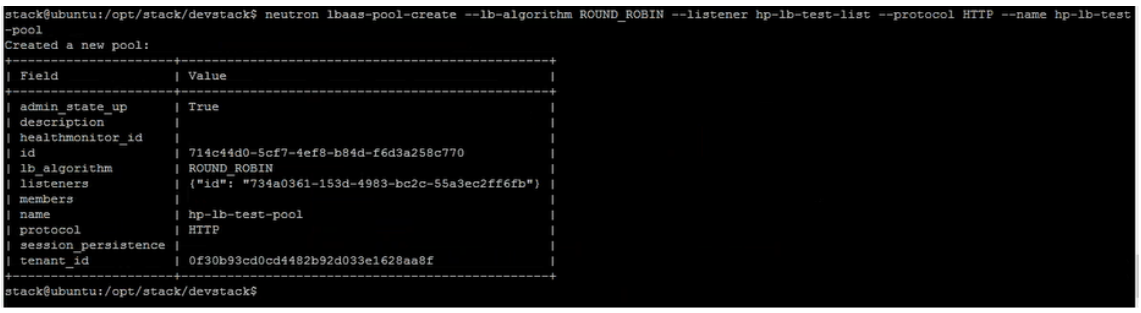


7. Créez un pool à l'aide de la commande suivante :

```
neutron lbaas-pool-create --lb-algorithm <algorithm_type> --
    listener <listener-name> --protocol <protocol_type> --name <
    pool-name>
<!--NeedCopy-->
```

Exemple :

```
neutron lbaas-pool-create --lb-algorithm LEAST_CONNECTIONS --
    listener demolistener --protocol http --name demopool
<!--NeedCopy-->
```

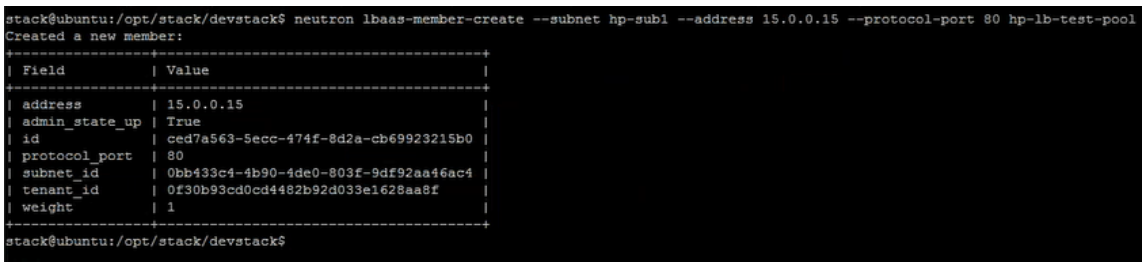


8. Créez un membre à l'aide de la commande suivante :


```
neutron lbaas-member-create  --subnet <subnet-name> --address <ip-address of the web server> --protocol-port <port_number>  <pool-name>
<!--NeedCopy-->
```

Exemple :

```
neutron lbaas-member-create --subnet hp-sub1 --address 15.0.0.15 --protocol-port 80 hp-lb-test-pool
<!--NeedCopy-->
```



Surveillance des applications OpenStack dans Citrix ADM

Vos locataires peuvent se connecter à Citrix Application Delivery Management (ADM) à l'aide de leurs informations d'identification OpenStack pour surveiller les VIP et les pools créés à partir d'OpenStack à partir de n'importe quel navigateur. L'URL doit être au format suivant :

`http://<mas_ip>/<admin_ui>/mas/ent/html/cc_tenant_main.html`

Où, `mas-ip-address`, est l'adresse IP Citrix ADM enregistrée auprès de OpenStack.

> **Remarque**
>
> - Les VIP OpenStack correspondent aux serveurs virtuels dans Citrix ADM.
> - Les pools OpenStack correspondent aux groupes de services dans Citrix ADM.
> - Les membres du pool OpenStack correspondent aux membres du groupe de services dans Citrix ADM.

Configurer la commutation de contenu de couche 7

February 1, 2024

Citrix Application Delivery Management (ADM) orchestre avec OpenStack pour configurer les fonctionnalités de commutation de couche 7 (L7) ou de commutation basée sur le contenu sur des instances Citrix ADC. La commutation de contenu diffère du simple équilibrage de charge en ce sens que des

types spécifiques de requêtes peuvent être dirigés vers des serveurs spécifiques. Lorsque les configurations L7 sont créées dans OpenStack avec une instance Citrix ADC en tant que fournisseur, Citrix ADM affecte une instance Citrix ADC et déploie des configurations de commutation de contenu et de répondeur correspondant aux configurations L7. Les instances de Citrix ADC peuvent ensuite distribuer et équilibrer la charge des demandes utilisateur en fonction des caractéristiques de couche applicative des demandes.

La fonction d'équilibrage de charge de la couche 7 (L7) d'OpenStack combine l'équilibrage de charge et la commutation de contenu pour optimiser la diffusion de types spécifiques de contenu. Cela améliore les performances de l'équilibreur de charge en exécutant uniquement les stratégies applicables au contenu. L'équilibrage de charge de couche 7 facilite également l'efficacité de l'infrastructure applicative. La possibilité de séparer le contenu en fonction du type, de l'URI ou des données permet une meilleure allocation des ressources physiques dans l'infrastructure applicative. Par exemple, un utilisateur final naviguant vers `http://example-sports.com/about-us` est servi par un pool de serveurs hébergeant du contenu sur l'entreprise et les services, tandis qu'un utilisateur naviguant vers `http://example-sports.com/shopping-cart-football` est servi par un pool différent de serveurs qui permet aux utilisateurs d'effectuer des achats en ligne.

Dans la commutation L7, un équilibreur de charge est implémenté en tant que serveur virtuel de commutation de contenu qui accepte les requêtes HTTP des utilisateurs et les distribue aux serveurs d'applications. La commutation L7 ou la commutation de contenu vous permet de disposer d'un point d'entrée unique pour accéder à divers services dorsaux (par exemple, non seulement aux applications Web, aux portails de services Web, aux courriers électroniques, mais également à la gestion mobile, au contenu dans différentes langues, etc.). En d'autres termes, vous pouvez fournir une adresse IP publique pour tous les services que vous offrez à vos utilisateurs.

Contrairement à l'équilibrage de charge de niveau inférieur, la commutation de couche 7 ne nécessite pas que tous les serveurs du pool disposent du même contenu. Une configuration d'équilibreur de charge utilisant la commutation L7 s'attend à ce que les applications ou les serveurs principaux de différents pools aient un contenu différent. Les commutateurs L7 peuvent diriger les requêtes sur la base de l'URI, de l'hôte, des en-têtes HTTP ou tout autre élément du message de l'application. Les serveurs d'applications servent essentiellement des types spécifiques de contenu. Par exemple, un serveur ne peut servir que des images, un autre peut exécuter des langages de script côté serveur, tels que PHP et ASP, et un autre peut servir du contenu statique tel que HTML, CSS et JavaScript.

Règles L7

Les attributs suivants sont définis dans une règle pour évaluer le trafic et sont comparés aux valeurs définies dans la règle :

- Nom d'hôte : le nom d'hôte dans la requête HTTP est comparé au paramètre value de la règle. Par exemple, « www.example-sports.com ».

- chemin : la partie chemin de l'URI HTTP est comparée au paramètre value de la règle. Par exemple, « www.example-sports.com/shopping-cart/football_pump.html »
- file_type : la dernière partie de l'URI est comparée au paramètre value de la règle. Par exemple, txt, html, jpg, PNG, xls et autres.
- header : l'en-tête défini dans le paramètre clé est comparé au paramètre value de la règle.
- cookie : le cookie nommé par le paramètre clé est comparé au paramètre value de la règle. La valeur du champ d'en-tête de demande de cookie contient une paire nom/valeur d'informations stockées pour cette URL ; la syntaxe générale est la suivante : Cookie : nom=valeur. Par exemple, une règle qui recherche un cookie nommé « stores » dont la valeur commence par « football- » ressemblera à ceci : type = Cookie, compare_type=startsWith, key = stores value = football-.

Types de comparaison

Lors de l'évaluation du trafic, la stratégie L7 compare les expressions suivantes aux attributs définis dans la règle.

- regex : correspondance d'expressions régulières de type Perl
- starts_with : chaîne commençant par
- ends_with : La chaîne se termine par
- contains : La chaîne contient
- equal_to : Chaîne égale à

> **Remarque**
>
> Les attributs nom d'hôte, chemin d'accès, en-tête et cookie prennent en charge tous les types de comparaison, mais l'attribut file_type ne prend en charge que regex et equal_to.

Stratégies L7

Une stratégie L7 traite le trafic HTTP entrant et renvoie une valeur « vraie » lorsque toutes les règles définies dans la stratégie sont respectées.

Dans toute stratégie L7, toutes les règles sont logiquement associées à un opérateur AND. Une demande doit respecter toutes les règles pour que la stratégie renvoie une valeur « vraie ». L'action entreprise par l'équilibreur de charge est basée sur la valeur renvoyée par la stratégie. Vous pouvez créer une deuxième stratégie avec la même action pour réaliser une opération OR logique entre les règles.

Par exemple, vous pouvez créer une stratégie dans laquelle la requête HTTP entrante peut contenir les mots « EXAMPLE-SPORTS », « SPORTS-FOOTBALL » ou « EXAMPLE-FOOTBALL », afin que l'équilibreur de charge prenne les mesures appropriées pour transmettre ces demandes au pool de serveurs de la société de commerce électronique Example-Sports pour diffuser le contenu demandé. Vous pouvez créer une autre stratégie qui prend la même action, mais qui correspond à « exemple sport », « exemple sports-football » ou « exemple football. » Lorsqu'un utilisateur envoie une requête HTTP avec l'un de ces six mots clés, l'équilibreur de charge transmet la demande au serveur Example-Sports.

Selon les règles définies dans la stratégie, une stratégie L7 peut effectuer l'une des actions suivantes :

- Rediriger vers le pool : transmettez la demande au pool de serveurs d'applications identifié par les règles associées à la stratégie L7. En d'autres termes, vous pouvez créer une règle d'application pour diriger les demandes vers un pool d'équilibreurs de charge spécifique en fonction du nom de domaine. Par exemple, vous pouvez créer une règle qui dirige certaines demandes vers example-football.com vers pool_1, et d'autres demandes vers example-sports-online_purchase.com vers pool_2.
- Redirection vers une URL : envoyez au client une réponse HTTP de redirection dans laquelle l'en-tête de la réponse de localisation contient le nouvel emplacement. Le navigateur mettra à jour la barre d'adresse avec le nouvel emplacement et émettra une nouvelle demande. Les cas d'utilisation sont nombreux. Par exemple, si l'adresse d'un site Web a changé, vous pouvez rediriger les demandes vers la nouvelle adresse au lieu de les supprimer. Ou, pendant la maintenance du site Web, vous pouvez rediriger les utilisateurs vers un site en lecture seule.
- Rejeter - Rejette la demande et n'effectue aucune autre action. Par exemple, vous pouvez renvoyer une réponse 401 non autorisée pour refuser l'accès aux utilisateurs pour les pages Web restreintes.

Une configuration de commutation de contenu se compose d'un serveur virtuel de commutation de contenu, d'une configuration d'équilibrage de charge consistant en serveurs et services virtuels d'équilibrage de charge, et de stratégies de commutation de contenu. Après avoir créé votre serveur virtuel de commutation de contenu et vos stratégies, vous liez chaque stratégie au serveur virtuel de commutation de contenu. Lorsque vous liez la stratégie au serveur virtuel de commutation de contenu, vous spécifiez le serveur virtuel d'équilibrage de charge cible. Lorsqu'une demande atteint le serveur virtuel de commutation de contenu, le serveur virtuel applique les stratégies de commutation de contenu associées à cette demande. La priorité de la stratégie définit l'ordre dans lequel les stratégies liées au serveur virtuel de commutation de contenu sont évaluées.

Tout pool doté de l'ID d'écouteur peut être affecté en tant que pool par défaut de serveurs virtuels vers lesquels le trafic est redirigé. Le pool est étroitement lié à un écouteur et n'est associé à un auditeur que par la mise en œuvre d'une stratégie L7. Un pool peut également être créé directement sous un équilibreur de charge sans nécessairement être lié à un auditeur. Dans ce cas, le pool est créé dans un

état « pending_create ». Les stratégies L7 étant étroitement liées aux auditeurs, une stratégie L7 contenant l'ID du pool doit être créée et mise en œuvre pour que le pool devienne « actif » et commence à recevoir des demandes de trafic.

Un pool peut être desservi par plusieurs stratégies L7, mais il reste dans l'état « actif » si au moins une stratégie y est attachée. Lorsque la dernière stratégie est supprimée, le pool revient à l'état « pending_create » jusqu'à ce qu'une autre stratégie soit créée et associée à celle-ci. Si le pool lui-même est supprimé, toutes les requêtes HTTP qu'il aurait reçues autrement sont redirigées vers le pool par défaut.

Mappage entre les stratégies OpenStack L7 et les entités Citrix ADC

OpenStack	Entité Citrix ADC	Description
Stratégie L7 avec action REDIRECT_TO_POOL	Stratégie de commutation de contenu > Action de commutation de contenu	Citrix ADM crée une stratégie de commutation de contenu liée au serveur virtuel de commutation de contenu et associée à une action de commutation de contenu spécifiant le pool cible de serveurs d'applications pour la récupération de contenu et la présentation à l'utilisateur.
Stratégie L7 avec action REDIRECT_TO_URL	Stratégie du répondeur > Action du répondeur	Citrix ADM crée une stratégie de répondeur liée au serveur virtuel de commutation de contenu et associée à une action de répondeur qui spécifie l'URL cible à présenter aux utilisateurs.
Stratégie L7 avec action REJECT	Stratégie de répondeur > Supprimer la demande	Citrix ADM crée une stratégie de répondeur liée au serveur virtuel de commutation de contenu et associée à une action de répondeur qui supprime la demande.

Si l'action d'une stratégie L7 qui évalue « true » redirige le trafic vers un pool qui est à l'état « create_pending », Citrix ADM implémente le pool spécifié avec un serveur virtuel d'équilibrage de charge. Citrix ADM crée une stratégie de commutation de contenu à partir de la stratégie L7 et utilise l'action de commutation de contenu correspondante pour rediriger les demandes vers le serveur virtuel d'équilibrage de charge associé à ce pool. Si une seconde stratégie L7 redirige vers le même pool, Citrix ADM crée une stratégie de commutation de contenu et une action de commutation de contenu pour rediriger le trafic vers le serveur virtuel d'équilibrage de charge existant associé au pool.

Positionnement des stratégies

L'évaluation des stratégies L7 dans OpenStack est déterminée par leurs priorités. Dans OpenStack, par défaut, les stratégies se voient attribuer des priorités dans l'ordre dans lequel elles sont créées. La stratégie créée en premier est numérotée « 1 », et les stratégies créées par la suite sont numérotées consécutivement. Vous pouvez toutefois modifier les priorités des stratégies et leur attribuer des priorités différentes. Les stratégies sont toujours évaluées dans l'ordre de leurs priorités. La première stratégie qui correspond à une requête spécifique est toujours exécutée en premier.

Lors de la création de stratégies, notez les points suivants :

- Si vous attribuez à une nouvelle stratégie la même priorité qu'une stratégie existante, la nouvelle stratégie prend cette priorité. La priorité de la stratégie existante est abaissée. Si nécessaire, les priorités des autres stratégies sont également abaissées afin de conserver l'ordre dans lequel les stratégies sont évaluées.
- Si vous créez une nouvelle stratégie sans spécifier de poste, la nouvelle stratégie sera simplement ajoutée à la liste.
- Si vous créez une nouvelle stratégie et que vous lui attribuez une position supérieure au nombre de stratégies figurant déjà dans la liste, la nouvelle stratégie sera ajoutée à la liste, c'est-à-dire qu'elle aura toujours la priorité disponible suivante. Par exemple, s'il existe trois stratégies A, B et C avec les priorités 1,2 et 3, et si vous créez une stratégie et que vous attribuez une priorité de 8, la priorité de la nouvelle stratégie devient 4.
- Si vous ajoutez une stratégie à la liste ou si vous supprimez une stratégie de la liste, les valeurs de position de la stratégie sont réorganisées à partir de 1 sans omettre de chiffres. Par exemple, si la stratégie A, B, C et D a des valeurs de position de 1, 2, 3 et 4 et si vous supprimez la stratégie B de la liste, la stratégie C prend désormais la deuxième position et la stratégie D prend la troisième position.

Dans Citrix ADM, il existe toujours une stratégie par défaut associée à un `csvserver` avec une priorité de 1. Cette stratégie par défaut spécifie le nombre de connexions TCP qu'un `lbvserver` traite à un moment donné. Par conséquent, lorsque les stratégies de répondeur et les stratégies de commutation de contenu correspondantes sont créées dans Citrix ADC, elles reçoivent toujours une priorité

1 supérieure à la priorité de la stratégie L7 correspondante. Par exemple, lorsqu'une stratégie L7 avec une priorité de 1 est évaluée et qu'une stratégie de commutation de contenu est créée avec une priorité de 2. De même, lorsqu'une stratégie L7 avec une priorité de 2 est évaluée et qu'une stratégie de réponse est créée avec une priorité de 3.

Dans OpenStack, la stratégie « rejet » ou « redirect_to_url » est d'abord évaluée, puis la stratégie « redirect_to_pool » est évaluée. Dans une instance de Citrix ADC, les stratégies de répondeur sont toujours évaluées en premier pour supprimer la demande ou présenter à l'utilisateur une adresse Web redirigée, et les stratégies de commutation de contenu sont évaluées en dernier. Cet ordre d'évaluation ne provoque généralement aucun conflit si les stratégies de changement de contenu et de réponse s'excluent mutuellement. En d'autres termes, deux stratégies L7 ne doivent pas avoir des expressions identiques. Les expressions dérivées sont ajoutées dans les stratégies de répondeur et de changement de contenu pour éviter de tels conflits. Par exemple, écrivez une expression pour rejeter toutes les demandes sur "sports-football.com"et une autre expression pour autoriser les requêtes à "example-sports-football.com."Créez les stratégies L7 de sorte que toutes les stratégies de réponse pour rejeter la demande soient organisées en haut de la liste d'évaluation, suivies des stratégies de réponse pour le web direct, suivies des stratégies de changement de contenu.

Dans Citrix ADM, il existe toujours une stratégie par défaut associée à un `csvserver` avec une priorité de 1. Cette stratégie par défaut spécifie le nombre de connexions TCP qu'un `lbvserver` traite à un moment donné. Par conséquent, lorsque les stratégies de répondeur et les stratégies de commutation de contenu correspondantes sont créées dans Citrix ADC, elles reçoivent toujours une priorité 1 supérieure à la priorité de la stratégie L7 correspondante. Par exemple, lorsqu'une stratégie L7 avec une priorité de 1 est évaluée et qu'une stratégie de commutation de contenu est créée avec une priorité de 2. De même, lorsqu'une stratégie L7 avec une priorité de 2 est évaluée et qu'une stratégie de réponse est créée avec une priorité de 3.

Dans OpenStack, la stratégie « rejet » ou « redirect_to_url » est d'abord évaluée, puis la stratégie « redirect_to_pool » est évaluée. Dans Citrix ADC, les stratégies de réponse sont toujours évaluées en premier pour supprimer la demande ou présenter à l'utilisateur une adresse Web redirigée, et les stratégies de commutation de contenu sont évaluées en dernier. Cet ordre d'évaluation ne provoque généralement aucun conflit si les stratégies de changement de contenu et de réponse s'excluent mutuellement. En d'autres termes, il n'y a pas deux stratégies L7 qui ont des expressions similaires. Des expressions dérivées similaires sont ajoutées dans les stratégies de répondeur et de changement de contenu pour éviter de tels conflits. Par exemple, écrivez une expression pour rejeter toutes les demandes sur "sports-football.com"et une autre expression pour autoriser les requêtes à "example-sports-football.com."Créez les stratégies L7 de sorte que toutes les stratégies de réponse pour rejeter la demande soient organisées en haut de la liste d'évaluation, suivies des stratégies de réponse pour le web direct, suivies des stratégies de changement de contenu.

Tâches de configuration

Les implémentations de la stratégie et des actions L7 sont effectuées via les commandes Neutron LBaaS.

Définissez les variables d'environnement dans OpenStack et créez l'équilibreur de charge (par exemple, LB1). Une fois l'équilibreur de charge correctement créé, créez le module d'écoute et les pools (par exemple, L1, P1 et P2), puis ajoutez des membres et des moniteurs aux pools. Par exemple, P1 est le pool par défaut pour L1, tandis que P2 est le pool lié à LB1 et gérant les serveurs d'applications.

Pour plus d'informations sur la façon de configurer LBaaS V2 à l'aide de la ligne de commande, consultez Configuration de LBaaS V2 à l'aide de la ligne de commande.

Les commandes suivantes créent les stratégies et définissent les actions spécifiques :

Créer une stratégie L7 pour supprimer les demandes

```
neutron lbaas-l7policy-create --name <L7 policy name> --listener <
    listener name> --action<action-name>
```

Exemple :

neutron lbaas-l7policy-create –name policy11 –action REJECT –listener L1

La commande ci-dessus crée et lie policy11, une stratégie de répondeur, au serveur de commutation de contenu pour rejeter les demandes. Aucune règle n'ayant été créée pour cette stratégie, celle-ci est considérée comme « fausse » et la demande est rejetée.

Créer une stratégie L7 pour rediriger les demandes vers une URL particulière

```
neutron lbaas-l7policy-create --name <L7 policy name> --listener <
    listener name> --action <action-name> --redirect-url <redirect-url>
```

Exemple :

neutron lbaas-l7policy-create –name policy12 –action REDIRECT_TO_URL –listener admin-list1 –redirect-url `http://example-sports/about-us.html`

La commande ci-dessus crée une action de répondeur pour rediriger les demandes vers une URL, crée une stratégie de répondeur avec action et lie cette stratégie au serveur virtuel de commutation de contenu.

```
neutron lbaas-l7rule-create --type HOST_NAME --compare-type CONTAINS --
    value <value-string> <L7 policy name>

neutron lbaas-l7rule-create --type PATH --compare-type CONTAINS --value
     <value-string> <L7 policy name>
```

Les deux règles ci-dessus peuvent être connectées à un opérateur AND pour dériver l'expression de la stratégie de répondeur.

Créer une stratégie L7 pour rediriger les demandes vers un pool

```
neutron lbaas-l7policy-create --name <L7 policy name> --listener <
    listener name> --action <action-name> --redirect-pool <redirect-pool
    >
```

Exemple :

neutron lbaas-l7policy-create –name policy13 –action REDIRECT_TO_POOL –listener admin-list1 –redirect-pool admin-pool2

S'il s'agit de la première stratégie L7, la commande ci-dessus implémente P2 en même temps que LB1, crée l'action de redirection de commutation de contenu et redirige les demandes vers LB1. Si P2 existe déjà, la commande crée l'action de redirection de commutation de contenu et redirige les requêtes vers LB1.

Provisioning manuel de l'instance Citrix ADC VPX sur OpenStack

February 1, 2024

Dans certains réseaux d'entreprise, les instances Citrix ADC VPX ne peuvent pas se connecter au serveur de licences Citrix pour télécharger automatiquement les licences, pour des raisons de sécurité. Dans un tel scénario, vous devez déployer manuellement des instances Citrix ADC VPX sur la plate-forme OpenStack. À l'aide du code d'accès à la licence que vous avez reçu de Citrix, téléchargez la licence Citrix ADC VPX appropriée et enregistrez-la sur votre système local.

Pour provisionner manuellement une instance Citrix ADC VPX sur OpenStack :

1. Installez le logiciel de pilote Citrix ADC et enregistrez Citrix Application Delivery Management (ADM) sur OpenStack
    a) Dans Citrix ADM, accédez à **Orchestration** > **Cloud Orchestration** > **OpenStack**.
    b) Cliquez sur **Configurer les paramètres OpenStack**. Dans la page **Configurer les paramètres OpenStack**, vous pouvez définir les paramètres pour configurer OpenStack dans Citrix ADM. Vous avez deux options ici : par **défaut** et **Personnalisé** .
    c) Sélectionnez **Par défaut**, si les services OpenStack s'exécutent sur les ports par défaut.
2. Accédez à **Orchestration** > **Cloud Orchestration** > **OpenStack**, puis cliquez sur **Paramètres de déploiement**.
    a) **Réseau de gestion** : sélectionnez le réseau de gestion sur OpenStack, auquel le Citrix ADC VPX provisionné automatiquement est connecté.

b) **Nom du profil** : sélectionnez le profil dans la liste déroulante. Citrix ADM utilise le mot de passe contenu dans ce profil pour configurer de nouvelles instances Citrix ADC VPX provisionnées automatiquement.

c) Citrix ADC VPX Image in Glance : sélectionnez l'image Citrix ADC VPX disponible dans OpenStack Glance qui est utilisée pour créer une instance VPX Citrix ADC. La liste déroulante affiche uniquement les images présentes sur OpenStack Glance.

3. Dans Citrix ADM, accédez à **Orchestration** > **Cloud Orchestration** > **OpenStack** > **Service Packages**, puis cliquez sur **Ajouter**.
4. Dans la page **Service Package**, spécifiez les paramètres suivants :

a) **Nom** : nom du package de service. Par exemple, entrez SVC-PKG-GOLD.

b) **Allocation d'instance Citrix ADC** - sélectionnez **Dédié** ou **Partitionné** comme type d'allocation d'instance défini dans le package de services.

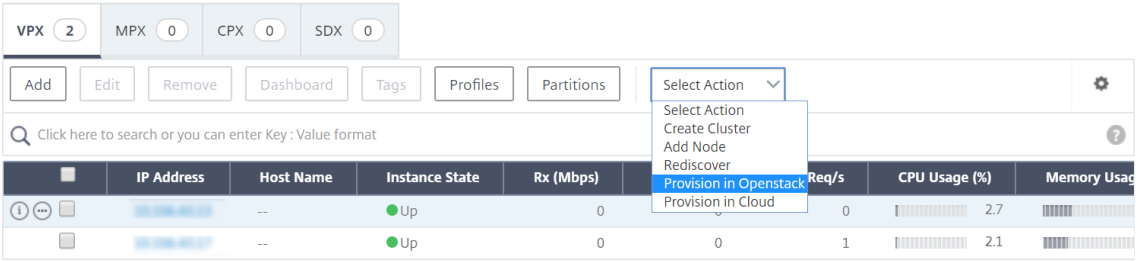
c) **Citrix ADC Instance Provisioning** : sélectionnez **Create Instance OnDemand** pour créer des instances Citrix ADC lors de la configuration elle-même.

d) **Plateforme de provisionnement automatique** - sélectionnez **OpenStack Compute**. Par défaut, Citrix ADC VPX sera sélectionné comme type d'instance.

e) **Affecter des locataires OpenStack ou des stratégies de placement**- section, sous Locataires OpenStack, cliquez sur **Ajouter**, puis sélectionnez le locataire.

f) Cliquez sur **Continuer**, puis sur **Terminé**.

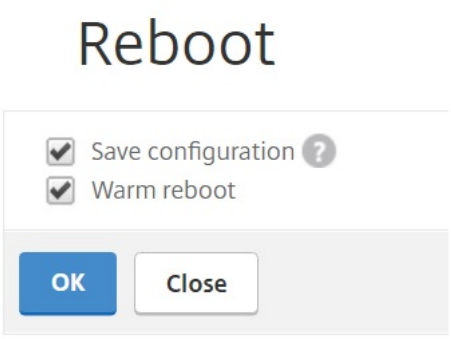
5. Accédez à **Système** > **Administration système** > **Modifier les paramètres système** et sélectionnez **http** dans la liste déroulante.
6. Accédez à **Réseaux** > **Instances** > **Citrix ADC VPX**.
7. Dans la page **Citrix ADC VPX**, cliquez sur la liste déroulante **Admin** et sélectionnez **Provisionner le périphérique**.



a) Sur la page **Device Provisioning**, entrez le nom du périphérique et sélectionnez le service package que vous avez créé à l'étape précédente.

b) Cliquez sur **OK**.

8. Accédez à l'onglet **Orchestration** > **Cloud Orchestration** > **OpenStack** > **Requêtes**. Sélectionnez la demande et cliquez sur **Tâches** pour afficher les tâches. Lorsque l'état de la tâche devient **Terminé**, cela signifie que le Citrix ADC VPX est provisionné dans Citrix ADM.
9. Accédez à**Réseaux** >**Instances** >**Citrix ADC VPX** pour vérifier que l'instance Citrix ADC VPX s'affiche dans la page Citrix ADC VPX.
10. Cliquez sur l'instance Citrix ADC VPX. Lorsque l'instance Citrix ADC VPX s'ouvre dans la fenêtre de votre navigateur, connectez-vous à l'instance. Accédez à **Configuration** > **Système** > **Licences**et ajoutez manuellement la nouvelle licence. Pour plus d'informations sur la façon d'ajouter une nouvelle licence, consultezVue d'ensemble des licences Citrix ADC.
11. Redémarrez l'instance Citrix ADC VPX.



12. Après quelques minutes, vous pouvez vous connecter à OpenStack et dans**System** >**Instances**, vous pouvez voir que l'instance Citrix ADC VPX est déployée sur OpenStack.
13. Les implémentations de l'API LBaaS V2 sont effectuées à l'aide de commandes LBaaS Neutron. Connectez-vous à n'importe quel client Neutron et exécutez les tâches de configuration. Pour plus d'informations sur la façon d'exécuter des commandes de configuration, consultezConfiguration de LBaaS V2 à l'aide de la ligne de commande.

Provisionnement de l'instance Citrix ADC VPX sur OpenStack à l'aide de StyleBook

February 1, 2024

Dans le workflow d'orchestration OpenStack, Citrix Application Delivery Management (ADM) utilise désormais `os-cs-lb-mon` StyleBook pour déployer des configurations LBAaS sur des instances Citrix ADC attribuées au client OpenStack. Un pack de configuration est créé pour chaque équilibreur de charge créé par l'utilisateur OpenStack.

L'utilisation de StyleBooks pour la configuration dans un workflow OpenStack offre les avantages suivants :

- Meilleure visualisation en visualisant tous les objets de configuration.
- Fiabilité grâce à la restauration.
- Prise en charge de divers types d'instance Citrix ADC (Citrix ADC HA, partitions, VPX, CPX, MPX et autres).
- Personnalisation à l'aide de vos propres StyleBooks pour déployer la configuration pour les locataires OpenStack.

En tant qu'administrateur Citrix ADM, accédez à **Applications** > **Configurations** pour afficher le pack de configuration déployé sur l'instance Citrix ADC.
Vous pouvez effectuer les tâches suivantes :

- Faites défiler l'écran pour afficher le pack `os-cs-lb-mon` de configuration déployé pour l'équilibreur de charge.
- Cliquez sur **Afficher la définition** dans le panneau `os-cs-lb-mon` StyleBook pour vérifier la configuration déployée sur les instances.
- Cliquez sur **Afficher l'objet** pour afficher la liste des objets ou entités Citrix ADC déployés sur les instances.

Points à noter avant de Provisioning des instances à l'aide de StyleBooks

A partir de Citrix ADM 12.1 build 49.23, l'architecture d'un workflow d'orchestration OpenStack a été mise à jour. Le workflow utilise désormais Citrix ADM StyleBooks pour configurer les instances Citrix ADC. Si vous effectuez une mise à niveau vers Citrix ADM 12.1 build 49.23 à partir de la version 12.0 ou de la version 12.1 build 48.18, vous devez exécuter le script de migration suivant :

```
/mps/scripts/migration_scripts/migrate_configurations.py
<!--NeedCopy-->
```

- L'exécution du script de migration crée des packs de configuration du `os-cs-lb-mon` StyleBook correspondant aux configurations OpenStack existantes.
- L'exécution de ce script de migration est obligatoire si des configurations OpenStack ont été déployées à partir de ces versions antérieures.
- Vous pouvez déployer de nouvelles configurations sur les instances à l'aide du `os-cs-lb-mon` StyleBook uniquement après avoir exécuté le script de migration à partir de la version 12.1 build 49.23.
- Toutes les configurations tentées à partir d'OpenStack échouent jusqu'à ce que le script de migration soit exécuté.

> **Remarque**
>
> - Une fois que vous exécutez le script de migration, vous ne pouvez pas passer à la version précédente de Citrix ADM.
> - Assurez-vous d'avoir mis à niveau les pilotes Citrix ADC pour OpenStack LBaaS V2 vers la dernière version. Utilisez les fichiers groupés Citrix ADC fournis avec la dernière version de Citrix ADM 13.0.

Les implémentations de l'API LBaaS V2 sont effectuées à l'aide de commandes LBaaS Neutron. Connectez-vous à n'importe quel client Neutron et exécutez les tâches de configuration. Pour plus d'informations sur la façon d'exécuter des commandes de configuration, consultezConfiguration de LBaaS V2 à l'aide de la ligne de commande.

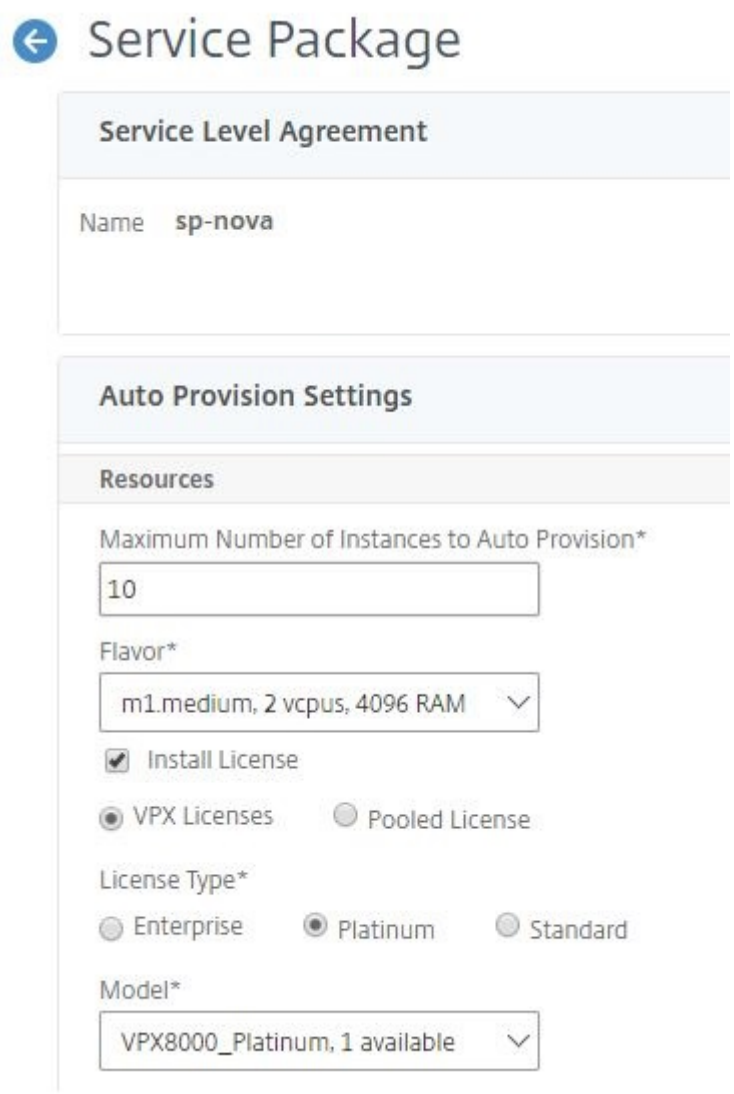
Prise en charge des licences d'enregistrement et de récupération VPX et des licences groupées pour l'environnement OpenStack

February 1, 2024

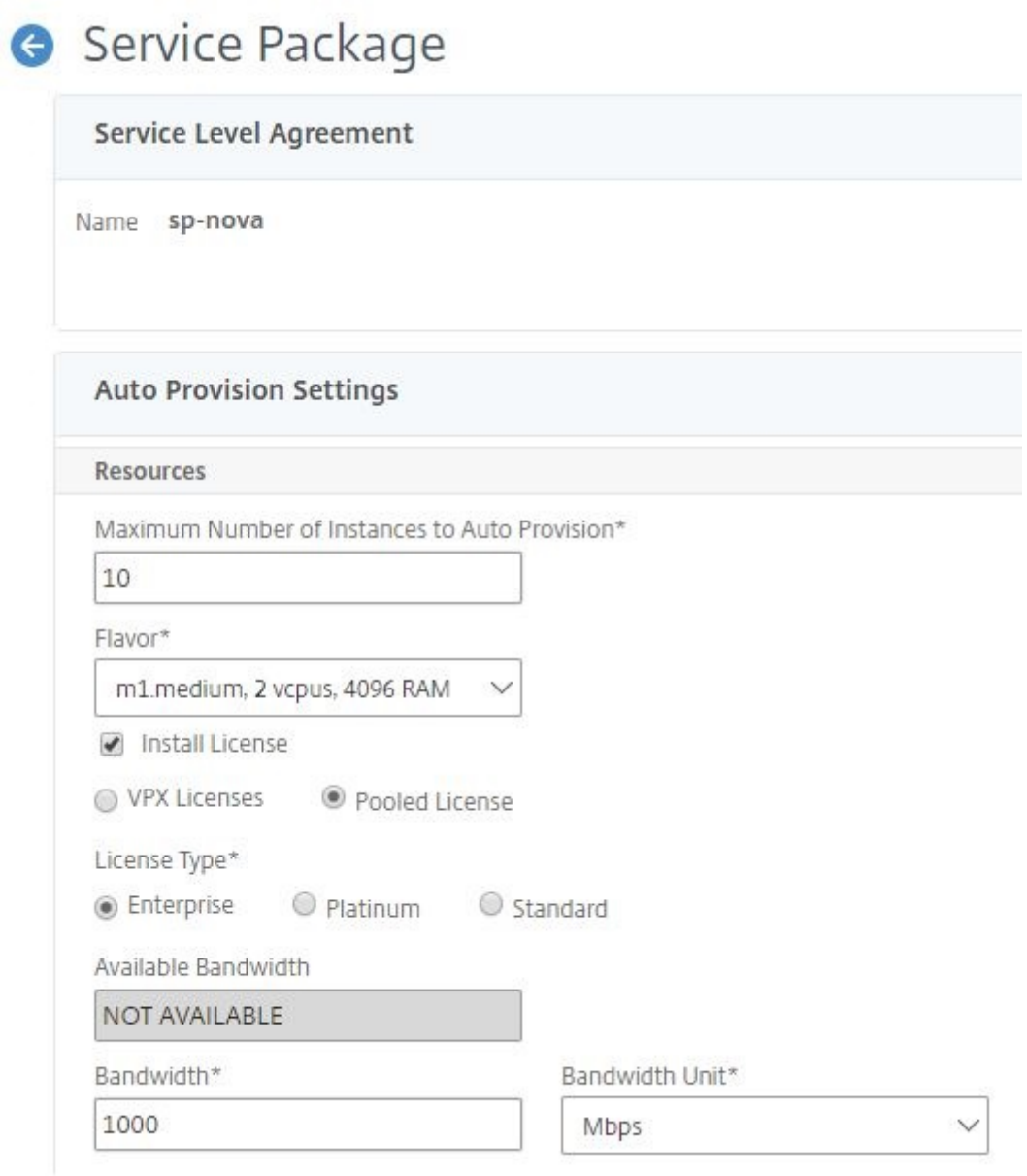
Dans le workflow d'orchestration OpenStack, Citrix Application Delivery Management (ADM) crée des instances Citrix ADC VPX à la demande lorsque vous sélectionnez un service package avec **OpenStack Compute**. Maintenant, la page Service Package de la fonctionnalité Orchestration de Citrix ADM est améliorée pour fournir la licence requise pour être installée sur les instances Citrix ADC VPX créées à la demande. Les licences fournies peuvent être soit une licence d'enregistrement et de départ VPX ou une licence groupée.

Pour utiliser cette fonctionnalité, vous devez d'abord télécharger les licences dans Citrix ADM, puis créer des packages de services qui utilisent le calcul OpenStack.

- S'il s'agit d'une licence d'enregistrement et de départ, vous pouvez choisir la licence à installer parmi les différentes licences disponibles.



- S'il s'agit d'une licence de pool, vous pouvez sélectionner à la fois la bande passante et le type d'édition de licence à installer.



Chaque fois que vous déployez votre premier équilibreur de charge avec Citrix ADM en tant que fournisseur, Citrix ADM crée l'instance Citrix ADC VPX et installe la licence spécifiée dans le service package sur l'instance nouvellement créée.

En outre, lorsque vous supprimez une instance d'équilibrage de charge existante, cette instance n'est plus nécessaire. L'instance est désaffectée et la licence est renvoyée à Citrix ADM. Cela permet une utilisation optimale des licences disponibles dans Citrix ADM.

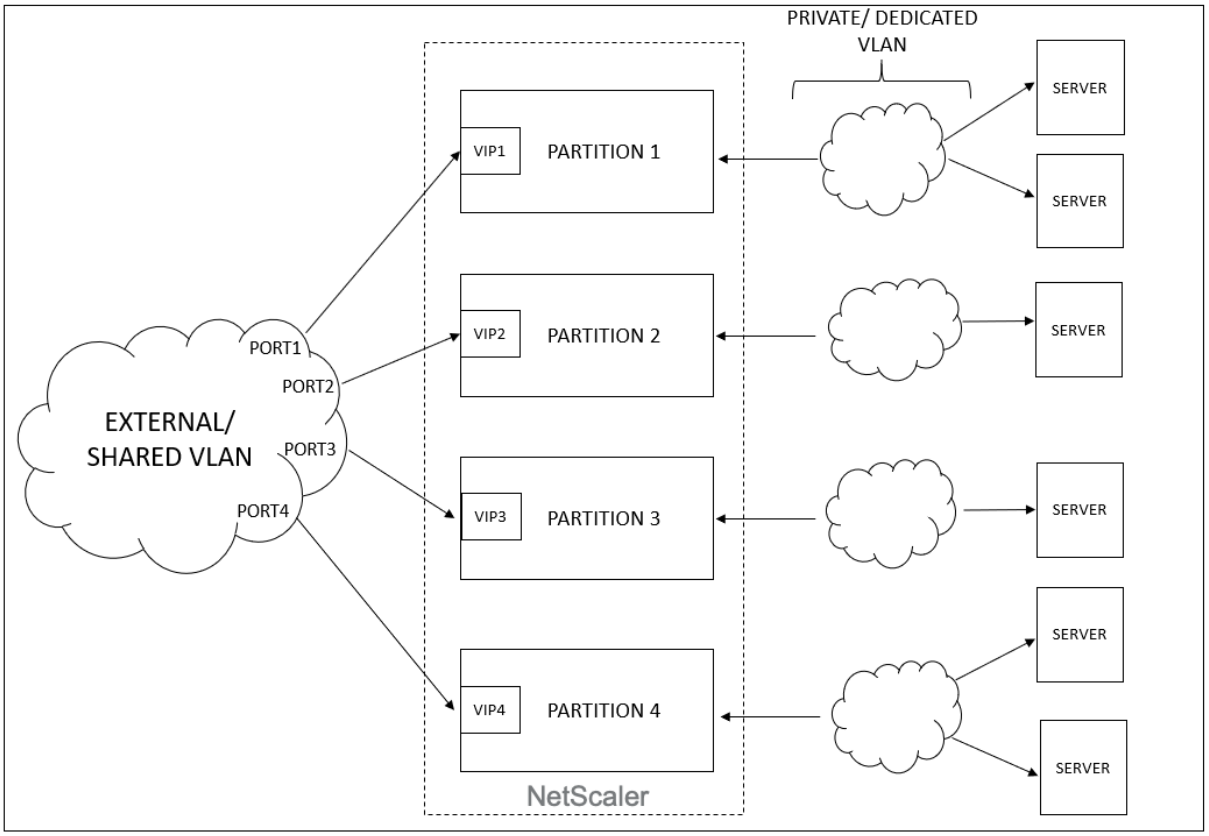
> **Remarque**
>
> Lorsque Citrix ADM est déployé en mode haute disponibilité, considérez que les licences sont téléchargées sur l'ADM actif ou principal Citrix, MAS-HA-1. Lorsque vous déployez la première

> demande et que Citrix ADM crée les instances Citrix ADC VPX, l'instance extrait les licences requises de MAS-HA-1. À un moment ultérieur, supposons que le Citrix ADM secondaire, MAS-HA-2, qui n'a pas les licences est actif maintenant. L'instance ADC VPX ne peut pas retirer la licence de MAS-HA-2 maintenant et, par conséquent, l'instance ne peut pas être créée pour les nouveaux utilisateurs.
>
> Dans ce cas, assurez-vous que MAS-HA-1 est UP et qu'il est maintenant le nœud principal actuel. Autrement dit, basculer manuellement l'Citrix ADM de MAS-HA-2 vers MAS-HA-1. Après cela, vous devez réessayer la configuration à partir d'OpenStack et les instances seront recréées avec des licences appropriées. Pour plus d'informations sur la prise en charge des licences dans le déploiement haute disponibilité Citrix ADM, consultez Haute disponibilité.

Prise en charge du VLAN partagé pour les partitions d'administration

February 1, 2024

Pour les locataires qui se connectent à partir de réseaux privés, Citrix Application Delivery Management (ADM) prend en charge la stratégie d'isolement afin que chaque locataire dispose de sa propre partition dédiée, d'un VLAN dédié et de serveurs dédiés. Pour les locataires qui se connectent à partir de réseaux publics, un VLAN dédié nécessitera trop d'adresses IP pour être utilisé. Un VLAN partagé contourne ce problème en créant une adresse IP virtuelle sur chaque partition, créant ainsi un seul sous-réseau IP.



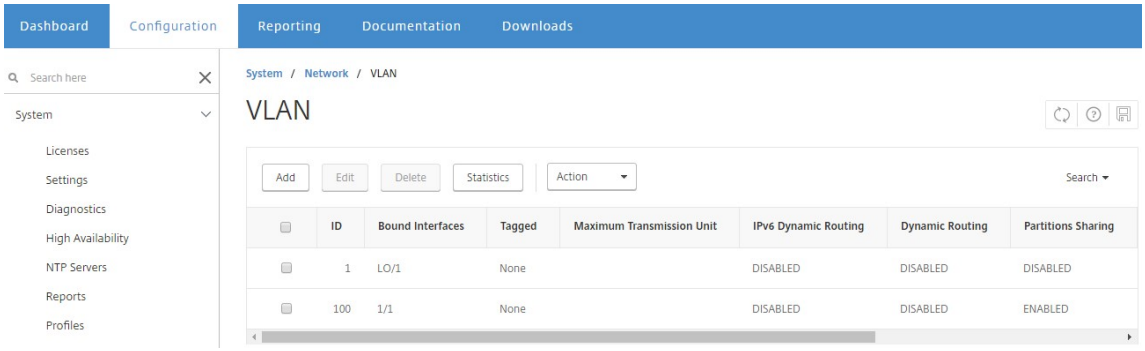
Lorsqu'un locataire configure un VIP ou un écouteur, une partition d'administrateur est créée dans le périphérique Citrix ADC pour ce locataire. Toute la configuration de l'équilibreur de charge est poussée vers la partition d'administration qui est créée. Si le locataire utilise un réseau partagé ou un réseau externe pour créer un équilibreur de charge, le VLAN de ce réseau est ajouté et la fonctionnalité de partage est activée. Lorsqu'un autre locataire utilise le même réseau partagé pour créer son équilibreur de charge, le VLAN n'est pas ajouté à l'Citrix ADC, mais le VLAN est également lié à la deuxième partition. Ainsi, tout locataire qui utilise le même réseau partagé obtient une partition qui est liée au même VLAN.

Citrix ADM prend en charge l'adresse MAC de destination virtuelle. Lorsque les locataires partagent un VLAN, Citrix ADM attribue différentes adresses MAC à la partition sur le périphérique Citrix ADC. Cela permet de partager un VLAN entre des partitions ou entre tous les locataires et tous les domaines de trafic.

Configuration du VLAN partagé à partir d'une instance Citrix ADC

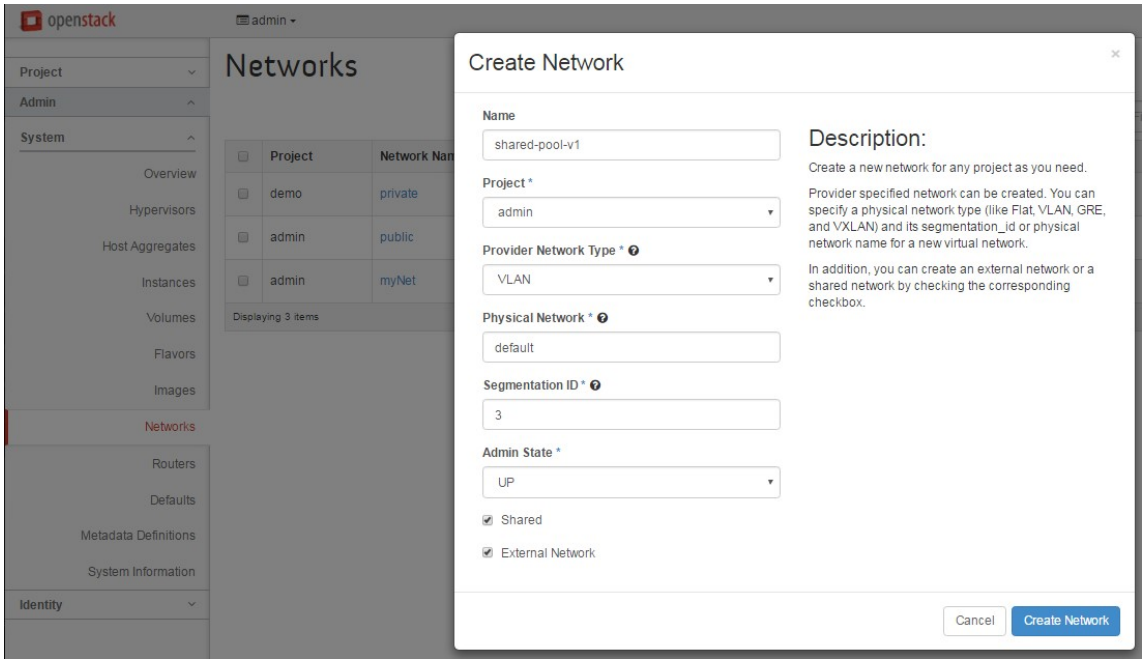
1. Dans une instance Citrix ADC, accédez à **Configuration** > **Système** > **Réseau** > **VLAN**, sélectionnez un profil VLAN, puis cliquez sur **Modifier** pour définir le paramètre de partage de partition.
2. Dans la page **Configurer le VLAN**, activez la case à cocher **Partage de partitions**.

3. Cliquez sur **OK**.



Configuration du VLAN partagé à partir d'OpenStack Orchestration

1. Dans OpenStack, accédez à **Admin** > **Système** > **Réseaux**, puis cliquez sur **Créer un réseau**.
2. Dans **Create Network**, définissez les paramètres suivants :
   a) Nom : entrez le nom du réseau
   b) Projet : sélectionnez un projet dans la liste déroulante
   c) Type de réseau du fournisseur : sélectionnez le **VLAN** dans la liste déroulante. Cela définit que le réseau virtuel est établi en tant que VLAN.
   d) Réseau physique : le réseau physique par défaut est sélectionné ici. Vous pouvez le modifier.
   e) État de l'administrateur : par défaut, l'état administratif du réseau est UP
   f) Sélectionnez Réseau **partagé** et **externe** pour définir que le VLAN est partagé et utilise un réseau externe.
3. Cliquez sur **Créer un réseau**.



Flux de travail de licence d'essai

February 1, 2024

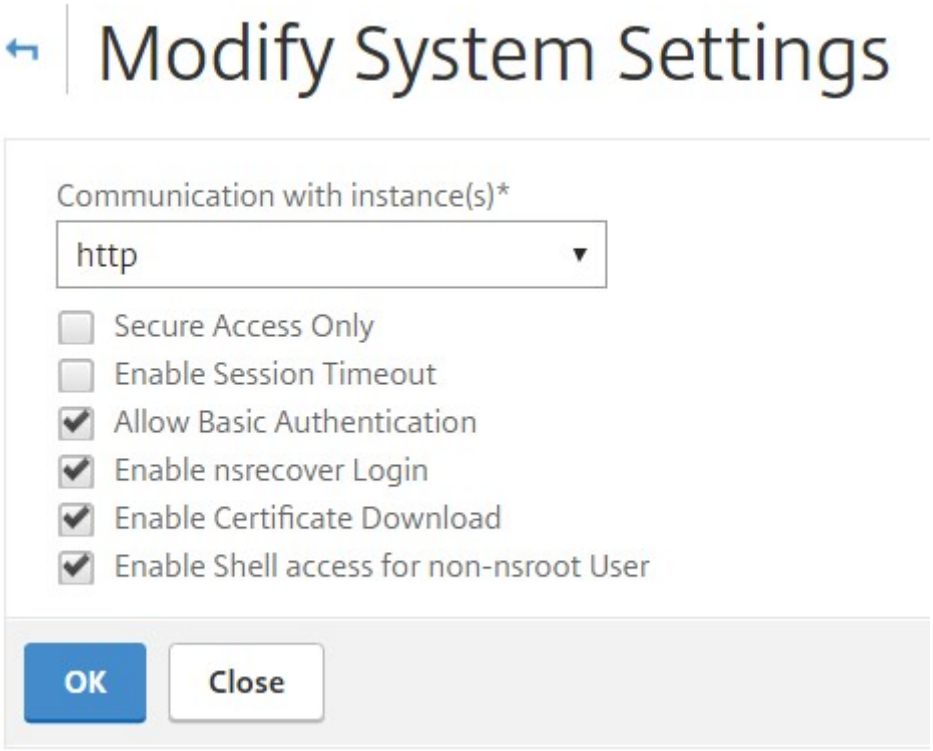
Lors du provisionnement automatique de l'instance Citrix ADC VPX à l'aide de l'orchestration OpenStack, Citrix Application Delivery Management (ADM) utilise OpenStack Compute pour lancer une instance Citrix ADC VPX. L'instance Citrix ADC VPX récemment provisionnée contacte le portail de licences Citrix lors de la configuration et utilise le code d'accès de licence pour télécharger et installer automatiquement les fichiers de licences.

Licences d'essai

Le personnel du support technique utilise des licences d'essai lorsqu'il installe des périphériques Citrix ADM et Citrix ADC VPX sur le terrain. Une licence d'essai ou d'évaluation pour Citrix ADC VPX est valide pendant 90 jours. S'il est nécessaire d'évaluer plus d'un Citrix ADC ou de prolonger le test après 90 jours, une nouvelle licence d'évaluation doit être demandée. Au lieu de l'installation automatique des fichiers de licence d'essai, Citrix ADM vous propose une solution alternative. Vous pouvez télécharger manuellement les fichiers de licence et les installer sur Citrix ADC VPX pour terminer l'installation de l'instance.

Si Citrix ADC VPX ne peut pas se connecter à Internet, configurez Citrix ADM pour qu'il agisse en tant que serveur proxy pour Citrix Licensing Portal et installez les fichiers de licence.

Les instances Citrix ADC VPX disposant d'une licence d'essai peuvent communiquer avec Citrix ADM sur HTTP uniquement. Pour configurer la communication HTTP dans Citrix ADM, accédez à**Système** >**Administration système**, puis cliquez sur**Modifier les paramètres système**. Sélectionnez **http** dans la liste déroulante pour définir la méthode de communication, puis cliquez sur**OK**.



Intégration avec les services OpenStack Heat

February 1, 2024

Les LBaaS OpenStack Neutron permettent des services d'équilibrage de charge de base, tels que l'équilibrage de charge, le déchargement SSL et la commutation de contenu, pour les applications. LBAaS est géré via une API REST, et l'API permet aux locataires d'effectuer des appels REST pour créer, mettre à jour et supprimer des objets LBaaS. Étant donné que LBaaS fournit des services d'équilibrage de charge, il n'autorise pas l'utilisation des fonctionnalités Citrix ADC plus avancées au cours du processus d'orchestration. Le plug-in Citrix ADC Heat surmonte cette limitation.

Service d'orchestration thermique

Le service d'orchestration OpenStack Heat permet de déployer des applications cloud complexes sur la base de modèles. Le modèle d'orchestration Heat (HOT) décrit l'infrastructure d'une application cloud sous forme de fichiers texte lisibles et inscriptibles par des humains, et pouvant être gérés par des outils de contrôle de version. Le langage structuré YAML est utilisé pour écrire ces modèles. Le modèle HOT vous permet de créer la plupart des types de ressources OpenStack et spécifie les relations entre les ressources définies dans celui-ci. Le plug-in Citrix ADC Heat vous permet de configurer les fonctionnalités ADC (Advanced Application Delivery Controller) sur n'importe quelle instance Citrix ADC.

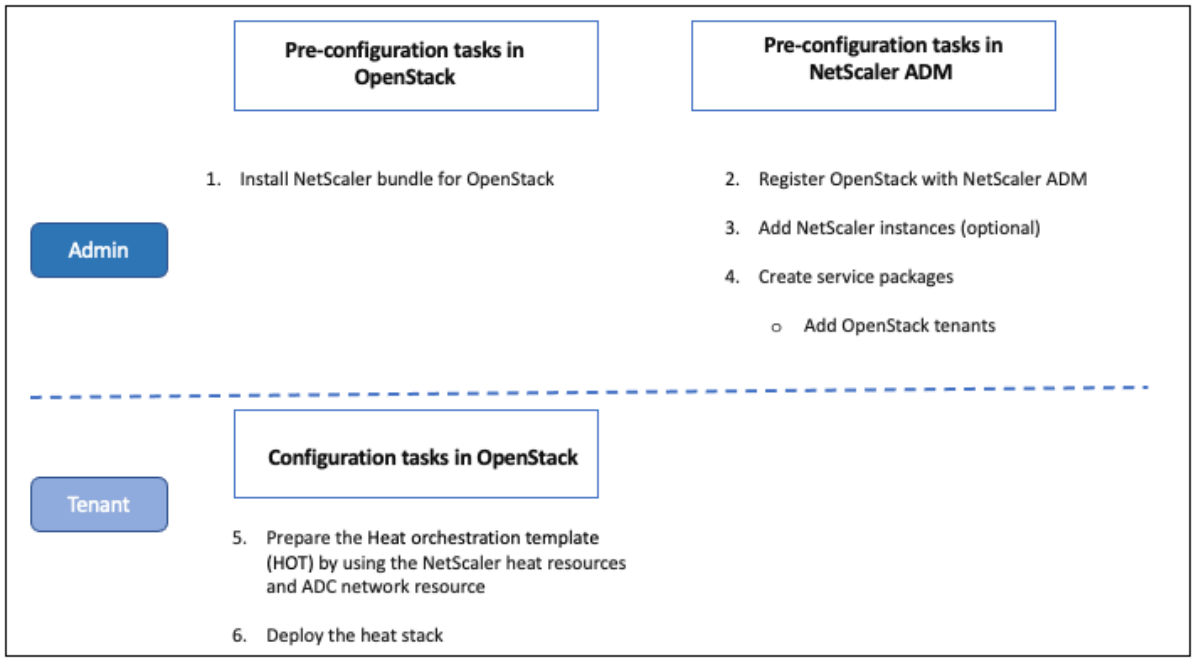
Citrix ADC StyleBooks

Citrix Application Delivery Management (ADM) StyleBooks peut être utilisé pour créer et configurer des fonctionnalités Citrix ADC. Tout comme les modèles Heat, les StyleBooks sont également écrits en YAML. Un StyleBooks distinct peut être créé pour chaque fonctionnalité, et un StyleBooks unique peut être utilisé pour déployer des configurations sur plusieurs instances Citrix ADC.

Lors de l'intégration de Citrix ADC avec OpenStack, Citrix ADM publie tous les StyleBooks Citrix ADM en tant que ressource dans le service Heat. Cela inclut à la fois les StyleBooks livrés avec Citrix ADM et les StyleBooks créés par l'utilisateur à un moment ultérieur.Le modèle Heat vous permet de configurer les fonctionnalités avancées des Citrix ADC à l'aide de ces ressources StyleBooks.

Workflow pour configurer des instances Citrix ADC à l'aide de la chaleur

L'organigramme suivant illustre le workflow de déploiement de la pile de chaleur :



Effectuez les tâches suivantes en tant qu'administrateur de cloud :

Pour configurer les services Heat dans OpenStack :

1. Télécharger les offres groupées Citrix ADC pour OpenStack

   Installez les bundles Citrix ADC dans OpenStack. Dans Citrix ADM, accédez à **Téléchargements** et téléchargez les bundles de pilotes Citrix ADC, dézippez les bundles et copiez le contenu du dossier Heat dans le répertoire des ressources du moteur Heat dans OpenStack. Le chemin d'accès au répertoire est le suivant :

   /opt/stack/heat/heat/engine/resources/netscaler_resources

2. Créez une section « netscaler_plugin » dans le fichier heat.conf et mettez à jour les paramètres suivants dans cette section :

   [netscaler_plugin]

   a) Lorsque la communication est HTTP, les paramètres sont mis à jour comme suit :

   NMAS_BASE_URI=<http://10.146.103.45:80>

   NMAS_USERNAME=

   NMAS_PASSWORD=

   b) Lorsque la communication est en https, les paramètres sont mis à jour comme suit :

   NMAS_BASE_URI=https://common_name_used_in_certificate

   NMAS_USERNAME=<openstack_driver_username

NMAS_PASSWORD=<openstack_driver_password>

SSL_CERT_VERIFY=<True_or_False>

CERT_FILE_PATH= <path_of_the_certificate_file>

Si l'utilisateur définit ssl_cert_verify comme étant « False », Citrix ADM envoie verify=false dans les appels de requête, ce qui désactive la validation du certificat SSL. Si ssl_cert_verify est défini sur « True » et que l'entrée cert_file_path est présente, Citrix ADM envoie ce chemin dans le paramètre de vérification de la requête, sinon Citrix ADM envoie verify=true.

> **Remarque**
>
> Pour le déploiement de Citrix ADM en mode « Haute disponibilité », mettez à jour les paramètres suivants dans le fichier heat.conf :
>
> NMAS_BASE_URI= <IP address of the front-end virtual server>

3. Redémarrez le service Heat dans OpenStack.

   Lorsque vous redémarrez les services Citrix ADC Heat dans OpenStack, tous les Citrix ADM StyleBooks définis sont importés dans Heat en tant que ressources. En outre, la ressource réseau Citrix ADC et la ressource de certificat sont importées dans OpenStack en tant que ressources Citrix ADC Heat.

4. Enregistrez Citrix ADM avec OpenStack.

   a) Dans Citrix ADM, accédez à **Orchestration** > **Cloud Orchestration** > **OpenStack**, puis cliquez sur **Configurer les paramètres OpenStack**.

   b) Dans la page **Configurer les paramètres OpenStack**, vous pouvez définir les paramètres pour configurer OpenStack. Deux options s'offrent à vous : par défaut et personnalisé.

   c) Sélectionnez **Par défaut** si les services OpenStack s'exécutent sur les ports par défaut. Entrez les paramètres suivants :

      i. Adresse IP du contrôleur OpenStack

      ii. Nom d'utilisateur administrateur

      iii. Mot de passe

      iv. Locataire administrateur OpenStack

      v. Pilote Citrix ADC et mot de passe Heat

   > **Remarque Il**

> s'agit du même mot de passe (NMAS_PASSWORD) que vous avez entré dans le fichier heat.conf.

5. Créez des packages de services et définissez les SLA avec votre locataire.

   Un locataire est créé dans Citrix ADM pour chaque utilisateur lors de l'enregistrement OpenStack, et les informations de locataire sont utilisées à la fois par le pilote LBaaS et par le plug-in Heat. Le plug-in Heat utilise ces informations pour contacter Citrix ADM afin d'importer StyleBooks en tant que ressources Heat dans OpenStack.

   > **Remarque**
   >
   > Pour plus d'informations sur la création de packages de services et d'autres tâches de préconfiguration dans Citrix ADM et OpenStack, consultez la section Intégration de Citrix ADM à OpenStack Platform.

6. Notez que tous les StyleBooks pertinents dans Citrix ADM sont importés dans OpenStack Heat en tant que ressources. Notez également que la ressource réseau Citrix ADC et la ressource de certificat Citrix ADC sont importées dans OpenStack Heat en tant que ressources.

   > **Remarque**
   >
   > Actuellement, vous ne pouvez utiliser que les StyleBooks livrés avec Citrix ADM.

   Votre locataire peut désormais créer le modèle Heat dans OpenStack, entrer les valeurs des paramètres Heat requis et déployer la pile Heat. Lorsque la pile Heat est déployée, la configuration est transmise à Citrix ADM et les instances Citrix ADC requises sont configurées.

Pour préparer le modèle de chaleur et lancer la pile de chaleur :

1. Dans OpenStack, le locataire peut créer un modèle d'orchestration Heat (HOT) à l'aide des ressources Heat.
2. Dans OpenStack Horizon, l'administrateur du client peut accéder à**Projet** >**Orchestration** >**Stacks** pour créer le modèle Heat et lancer le Heat Stack. Il existe deux manières de créer HOT :

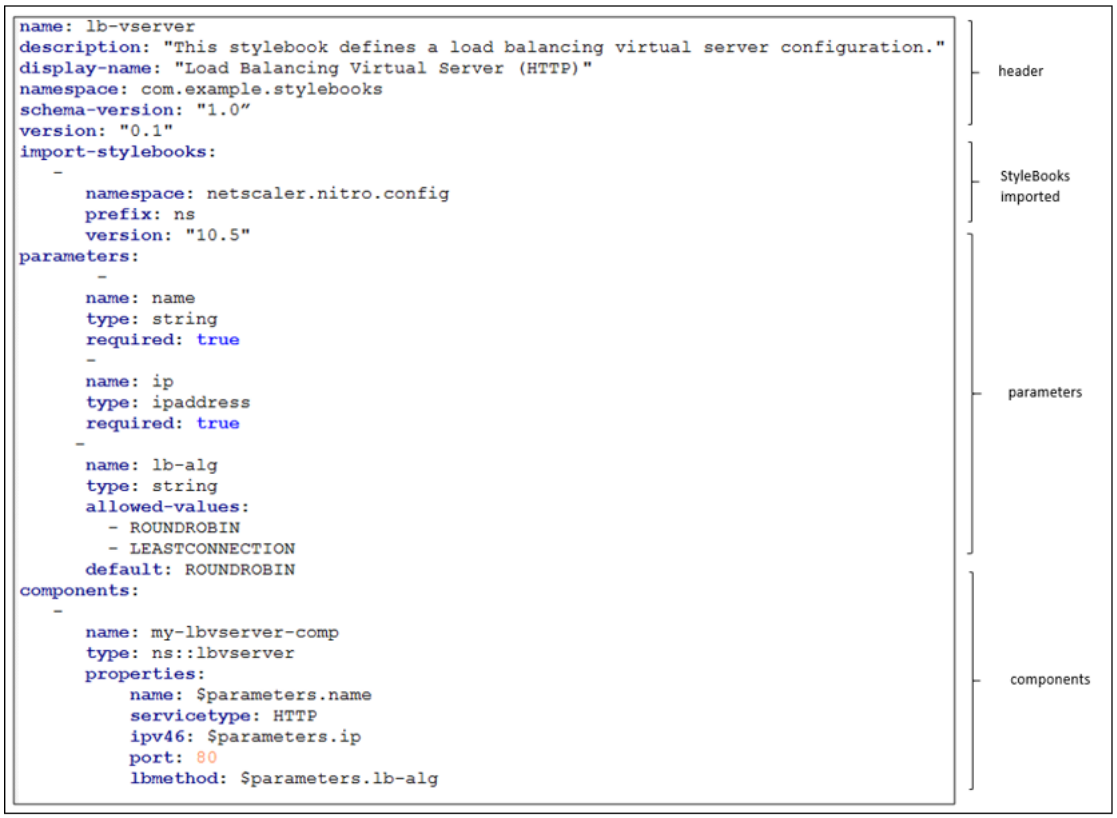
   - **Fichier** : sélectionnez le modèle mis à jour dans le répertoire local
   - **Saisie directe** : copiez et collez le contenu YAML du modèle dans la fenêtre

   > **Remarque**
   >
   > Une fois le stack déployé avec succès, le locataire peut le mettre à jour à l'aide du modèle Change Stack. Mais les informations de sous-réseau et l'adresse IP virtuelle (VIP) fournies initialement lors de la création de la pile ne peuvent pas être modifiées.

Une fois que le locataire a déployé la pile, accédez à**Orchestration** >**Cloud Orchestration**>**OpenStack**>**Demandes** dans Citrix ADM pour observer les listes de tâches. En outre, accédez à**Applications** >**Configuration** dans Citrix ADM pour observer que les instances Citrix ADC sont correctement configurées sous la forme de packs de configuration StyleBooks.

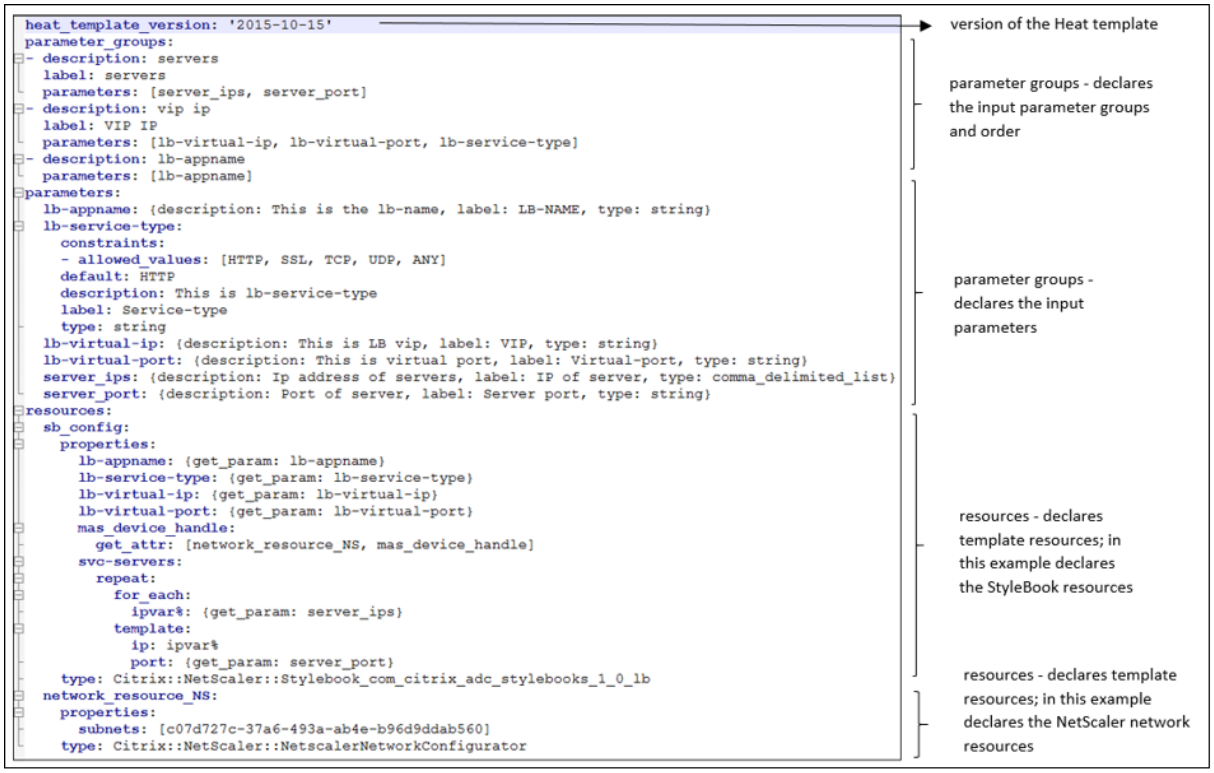
Exemple d'un Citrix ADM StyleBooks :

L'image suivante montre un exemple de construction d'un Citrix ADM StyleBooks et explique brièvement les composants. Pour plus d'informations sur les StyleBooks Citrix ADM et sur la façon d'utiliser les StyleBooks livrés, consultez StyleBooks.



Exemple d'un modèle de chaleur :

L'image suivante montre la structure d'un modèle de chaleur défini dans YAML et pointe vers les ressources StyleBooks et Citrix ADC importées en tant que ressources de chaleur.



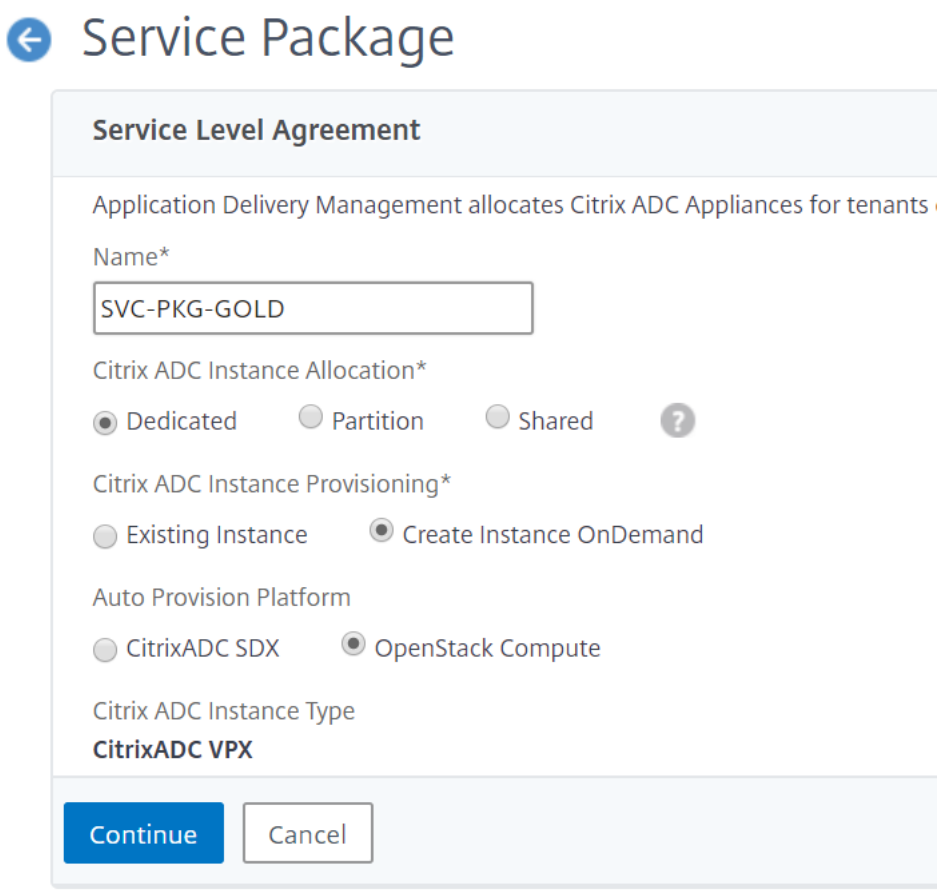
Pour plus d'informations sur les services Heat et la façon de créer des modèles, consultez ladocumentation OpenStack Heat.

Stratégies d'isolement des packages de services

February 1, 2024

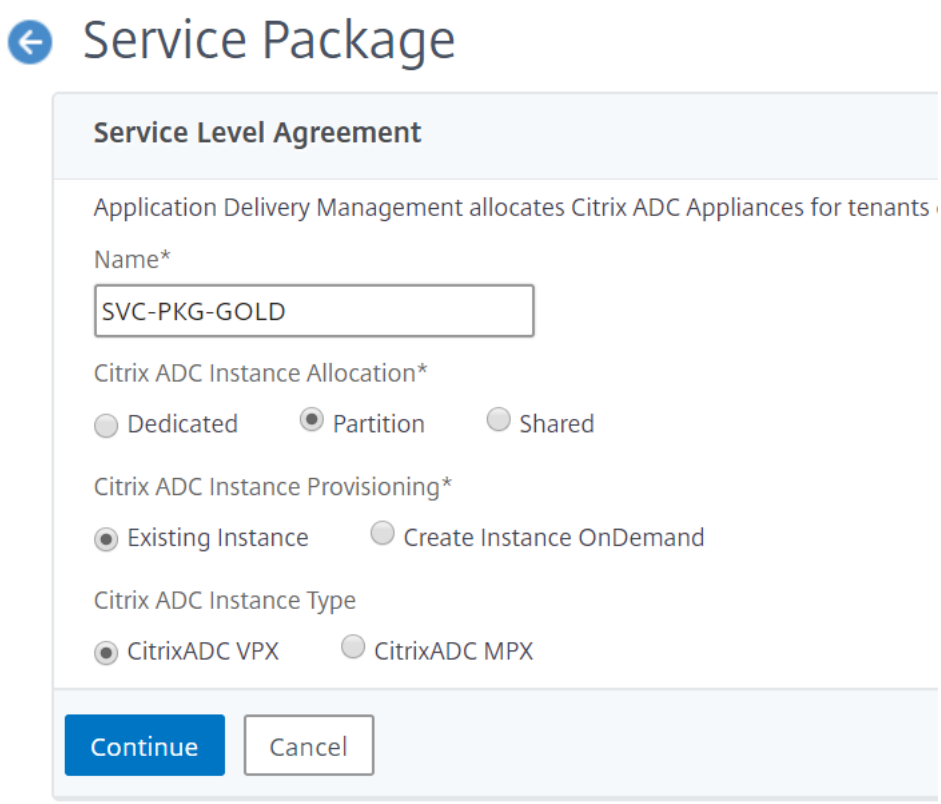
Stratégie d'isolement dédiée

Chaque locataire associé au package de service Citrix Application Delivery Management (ADM) d'une stratégie dédiée se voit attribuer une instance Citrix ADC parmi les instances qui font partie de ce service package. Cette instance Citrix ADC affectée n'est pas partagée avec d'autres locataires.



Stratégie d'isolement de partition

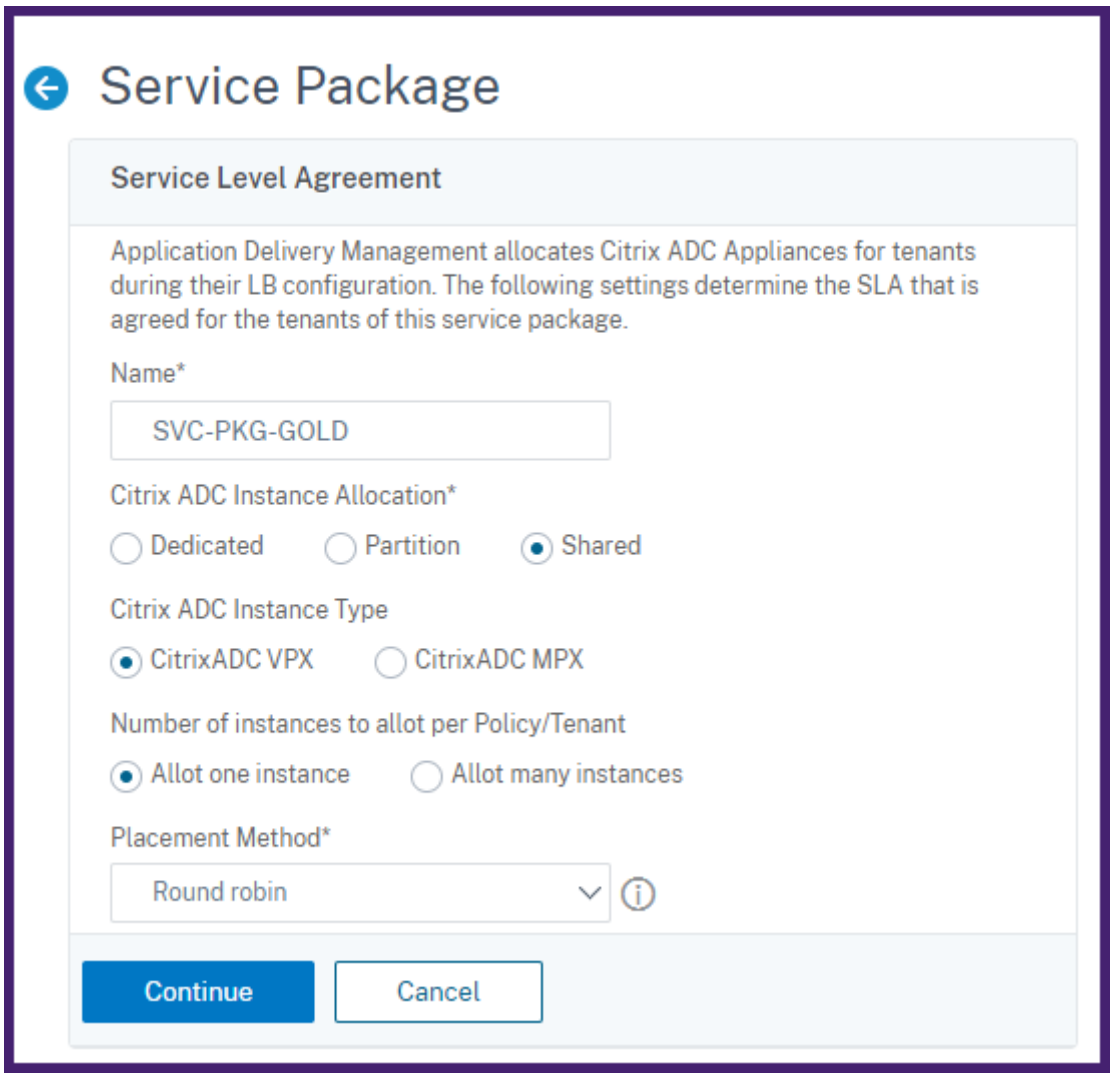
Chaque locataire associé au service package de stratégie de partition se voit attribuer une partition d'administration logique dédiée d'une instance Citrix ADC qui fait partie du service package.



Stratégie d'isolement partagée

Les locataires associés au service package partagent les instances Citrix ADC qui font partie du service package. Toutes les configurations d'un locataire sont affectées à une instance Citrix ADC. Dans ce mode, les configurations de plusieurs locataires peuvent être hébergées sur la même instance de Citrix ADC. Vous pouvez sélectionner **Citrix ADC VPX** ou **Citrix ADC MPX** comme type de périphérique. Vous pouvez choisir d'utiliser une seule instance Citrix ADC ou plusieurs instances au service package. Autrement dit, plusieurs locataires peuvent partager une ou plusieurs instances virtuelles du périphérique Citrix ADC.

> **Remarque**
>
> Ajouter des instances Citrix ADC SDX dans les packages de service en tant qu'instances Citrix ADC VPX uniquement, car un Citrix ADC SDX dispose d'un VPX Citrix ADC.



Remarque

Vous pouvez également créer des stratégies de placement flexibles, dans lesquelles les stratégies ne sont pas uniquement basées sur le nom ou l'ID du locataire, mais également sur d'autres attributs personnalisés. Pour plus d'informations sur les stratégies de placement flexibles, consultezAllocation flexible des appareils basée sur des règles.

Attribution de périphériques flexible basée sur des règles

February 1, 2024

Citrix Application Delivery Management (ADM) attribue des instances virtuelles Citrix ADC aux locataires, en fonction des contrats de niveau de service convenus avec les locataires. L'attribution d'instances virtuelles aux locataires crée une relation un-à-un entre l'instance et le locataire,

dans laquelle un locataire ne peut être affecté qu'à un seul package de services dans le centre de données.

Dans certaines situations, les locataires peuvent nécessiter plus d'une instance, ou l'attribution d'instances peut ne pas être basée sur les locataires comme critère, mais sur d'autres facteurs tels que l'ID réseau ou l'application. Dans de tels cas, Citrix ADM vous permet de définir avec précision des stratégies de placement basées sur des expressions définies par l'utilisateur afin d'affecter une configuration d'équilibrage de charge à l'une des instances gérées.

Les stratégies de placement offrent la flexibilité nécessaire pour décider de l'instance Citrix ADC utilisée dans chaque configuration d'équilibrage de charge créée par les utilisateurs. Les stratégies de placement flexibles dans Citrix ADM fournissent une option ajoutée à la méthode existante d'attribution d'instances Citrix ADC en fonction des locataires.

> **Remarque**
>
> Vous pouvez attribuer des instances aux locataires manuellement ou utiliser des stratégies de placement pour attribuer des instances en fonction des expressions créées. Vous ne pouvez pas utiliser ces deux méthodes simultanément sur un même package de services.

Les stratégies de placement sont basées sur des expressions booléennes définies sur les propriétés des principaux objets de configuration LBaaS, tels que les pools et les équilibreurs de charge. L'interface utilisateur de stratégie de placement dans Citrix ADM fournit des expressions prédéfinies que vous pouvez choisir pour définir une stratégie personnalisée. Vous pouvez créer plusieurs stratégies de placement pour différentes expressions. Ainsi, chaque locataire peut disposer de plusieurs appareils définis selon ses besoins.

Vous devez d'abord sélectionner une expression correspondant à un objet racine qui doit être configuré ultérieurement. L'objet racine peut être un objet pool dans le cas de LBaaS V1, et un objet d'équilibrage de charge dans le cas de LBaaS V2. Ainsi, les placements basés sur la stratégie Citrix ADM sont pris en charge pour les API LBaaS V1 et V2. Ces stratégies de placement sont ensuite associées aux packages de services. Une fois que l'objet racine est placé dans une instance, les objets successifs du modèle sont ajoutés à l'instance.

Par exemple, l'objet de configuration du pool peut avoir les propriétés suivantes :

- tenant_id
- nom
- description
- protocol
- lb_method
- subnet_id

- subname_name
- admin_state_up
- état
- network_id
- network_type
- segmentation_id
- subnet_cidr
- subnet_gateway_ip

Les exemples suivants présentent certaines expressions qui utilisent les propriétés du pool pour définir une expression pour la stratégie :

1. Expression de stratégie basée sur le nom de pool

```
config["pools"]["name"] =="high-end-pool"
<!--NeedCopy-->
```

2. Expression de stratégie basée sur le nom de sous-réseau de pool

```
config ["pools"]["subnet_name"] == "us-west-payment-subnet1"
<!--NeedCopy-->
```

3. Expression de stratégie basée sur le nom du sous-réseau d'équilibrage de charge

```
config["loadbalancers"]["subnet_name"] == "mas-subnet"
<!--NeedCopy-->
```

Ajout d'une stratégie de placement

1. Dans la page d'accueil de Citrix ADM, accédez à **Orchestration** > **Cloud Orchestration** > **Stratégie de placement**, puis cliquez sur **Ajouter**.
2. Dans la page **Ajouter une stratégie de placement**, définissez les paramètres suivants :
   a) Nom : entrez un nom pour la stratégie de placement
   b) Expressions fréquemment utilisées : sélectionnez une expression dans la liste déroulante.
   c) Expression : une expression logique (booléenne) est renseignée dans ce champ en fonction de l'expression que vous avez sélectionnée dans le champ précédent. Modifiez les noms des champs selon vos besoins.

> **Remarque**
>
> Lorsque vous créez plusieurs stratégies, assurez-vous qu'elles sont exclusives les unes aux autres.

3. Cliquez sur **OK**.
4. Accédez à **Orchestration** > **Cloud Orchestration** > **OpenStack** > **Service Packages**, puis cliquez sur **Ajouter**.
5. Sur la page **Service Package**, définissez les paramètres suivants :

   a) Nom : entrez le nom du package de services

   b) Stratégie d'isolation : sélectionnez **une stratégie partagée**

   Dans la stratégie d'isolement partagée, la configuration d'équilibrage de charge d'un locataire coexiste avec la configuration d'équilibrage de charge des autres locataires de l'appareil alloué au locataire.

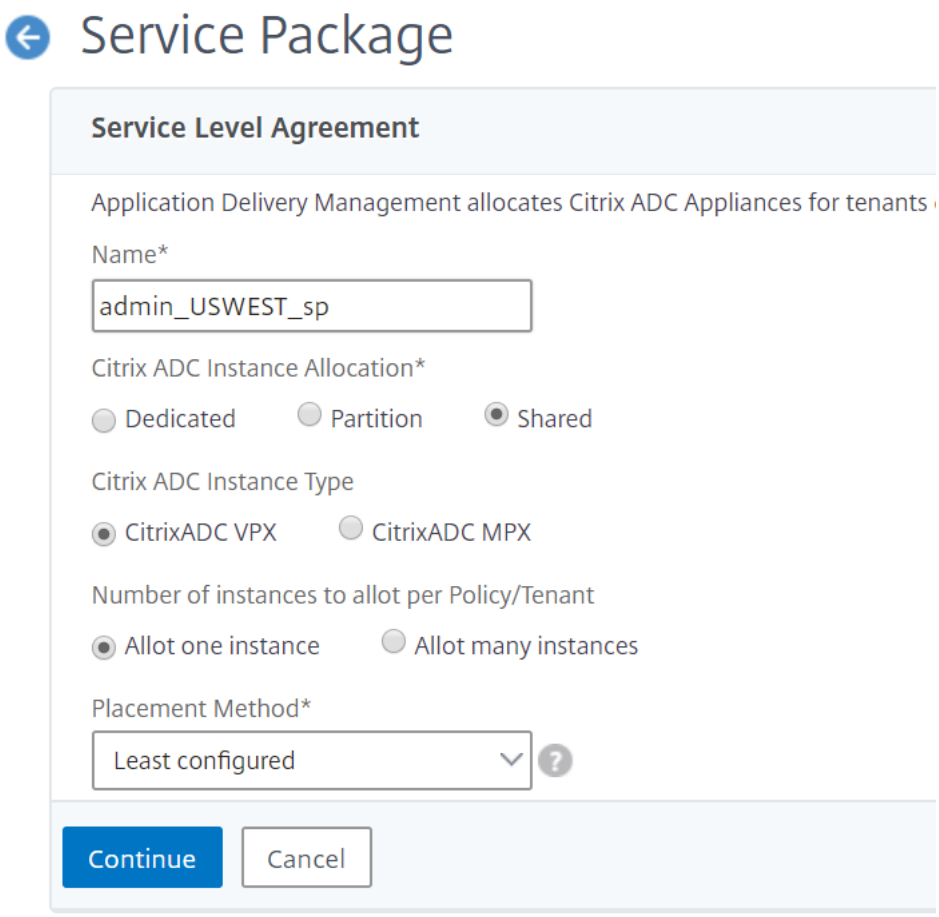
   c) Type de périphérique : sélectionnez un **Citrix ADC VPX** ou **Citrix ADC MPX**préprovisionné

   Sélectionnez **Allocation d'un périphérique** si vous souhaitez que toutes les configurations d'équilibrage de charge d'un locataire soient liées à un périphérique. Sélectionnez **Allocation de plusieurs périphériques** si vous souhaitez que chaque configuration d'équilibreur de charge d'un locataire soit distribuée sur plusieurs périphériques en fonction des stratégies de placement.

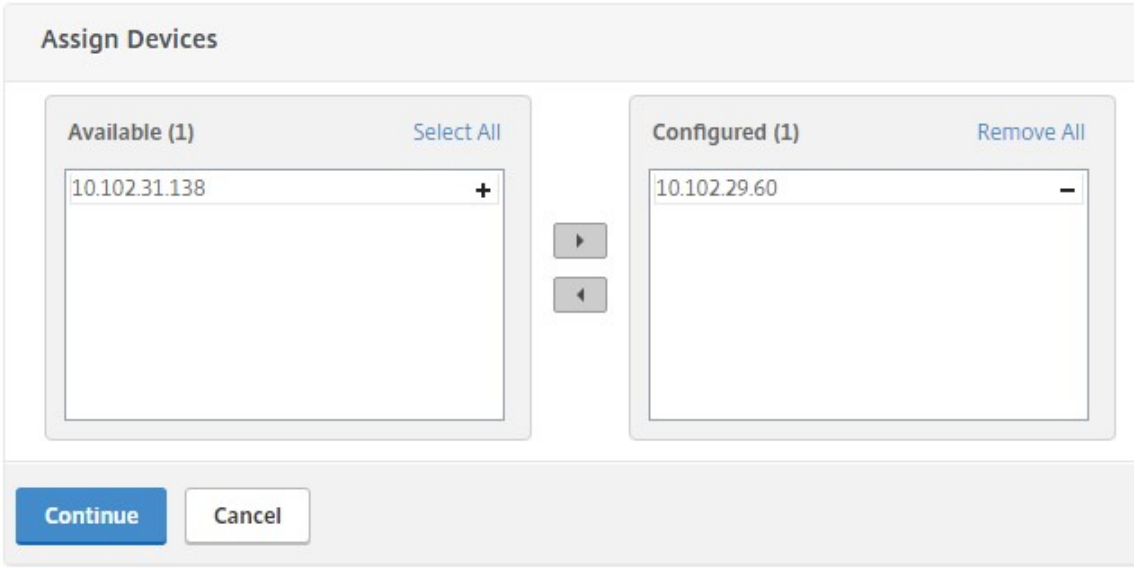
   > **Remarque**
   >
   > Citrix ADC SDX doit être ajouté dans les packages de service en tant qu'instances Citrix ADC VPX uniquement, car un Citrix ADC SDX possède un VPX Citrix ADC.

   d) Méthode de placement - sélectionnez **Moins configurés**

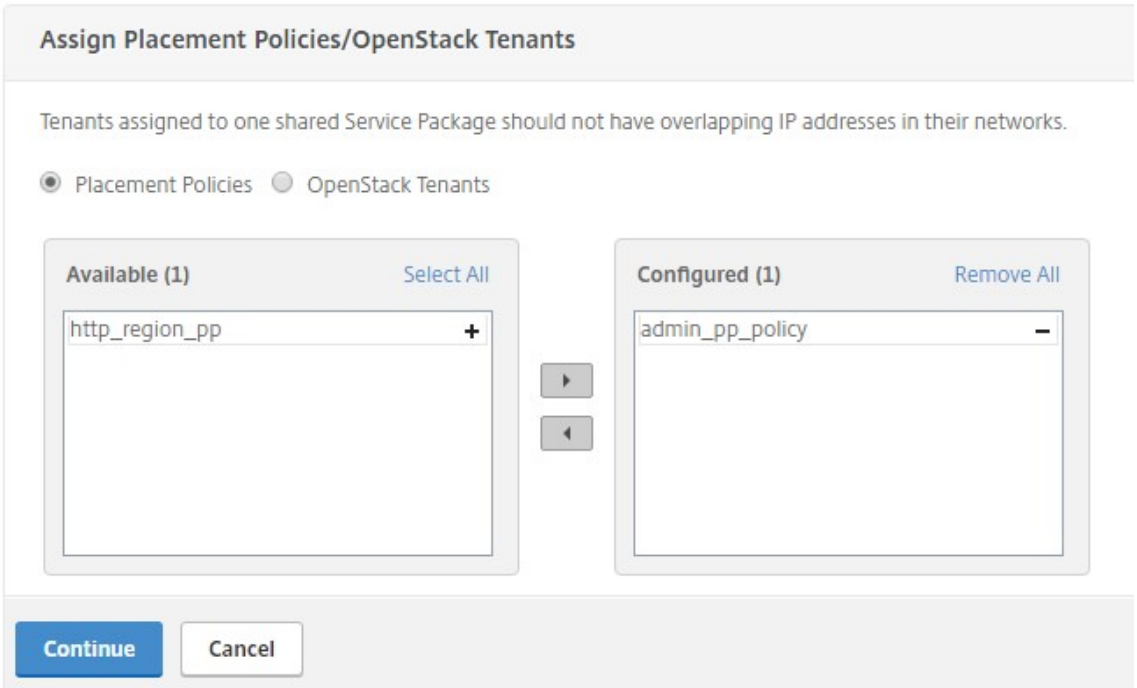
Lorsque Moins configurés est sélectionné, l'instance Citrix ADC qui a le moins de membres de pool configuré à ce moment est choisie comme périphérique pour le locataire.



6. Cliquez sur **Continuer**.
7. Dans la section **Affecter des périphériques**, ajoutez les périphériques Citrix ADC disponibles à la liste des périphériques configurés.



8. Cliquez sur **Continuer**.
9. Dans la section **Affecter des stratégies de placement/Locataires OpenStack**, ajoutez la stratégie de placement que vous avez créée précédemment.



> **Remarque**
>
> Si la stratégie n'est pas trouvée, le mécanisme de secours est rétabli et Citrix ADM attribue des instances Citrix ADC en fonction des locataires. Si le locataire ne fait partie d'aucun package de services, Citrix ADM affiche un message d'erreur indiquant :

> « Le locataire ne `admin` fait partie d'aucun Service Package et il n'y a aucun Service Package par défaut ».

10. Cliquez sur **Continuer**, puis sur **Terminé**.

NSX Manager : Provisioning manuel des instances Citrix ADC

February 1, 2024

Citrix Application Delivery Management (ADM) s'intègre à la plate-forme de virtualisation réseau VMware pour automatiser le déploiement, la configuration et la gestion des services Citrix ADC. Cette intégration évite les complexités traditionnelles associées à la topologie de réseau physique, permettant aux administrateurs vSphere/vCenter de déployer par programmation les services Citrix ADC plus rapidement.

Cet article fournit une liste des tâches que vous devez effectuer sur VMware NSX Manager et sur Citrix ADM.

> **Remarque**
>
> Assurez-vous que VMware NSX for vSphere 6.2 et versions ultérieures est installé et configuré, et que les passerelles périphériques, les machines DLR et les machines virtuelles qui doivent être équilibrées de charge sont déjà créés.

Conditions préalables

- Installez VMware ESXi version 4.1 ou ultérieure avec du matériel répondant à la configuration minimale requise.
- Installez VMware Client sur une station de travail de gestion qui répond à la configuration système minimale requise.
- Installez VMware OVF Tool (requis pour VMware ESXi version 4.1) sur une station de travail de gestion répondant à la configuration minimale requise.
- Installez Citrix ADM sur l'un des hyperviseurs pris en charge.

  Pour connaître les tâches d'installation de Citrix ADM build 13.0, sur l'un des hyperviseurs pris en charge, reportez-vous à la section Déploiement de Citrix ADM.

Configuration matérielle requise pour VMware ESXi

Le tableau suivant répertorie les ressources informatiques virtuelles dont vous avez besoin sur votre serveur VMware ESXi pour installer une appliance virtuelle Citrix ADM.

Composant	Exigences
RAM	8 GB
CPU virtuel	8
Espace de stockage	500 GB
Interfaces réseau virtuelles	1
Débit	1 Gbit/s

> **Remarque**
>
> Les exigences en matière de mémoire et de disque dur spécifiées ci-dessus concernent le déploiement de Citrix ADM sur le serveur VMware ESXi, étant donné qu'aucune autre machine virtuelle ne s'exécute sur l'hôte. La configuration matérielle requise pour le serveur VMware ESXi dépend du nombre de machines virtuelles qui s'y exécutent.

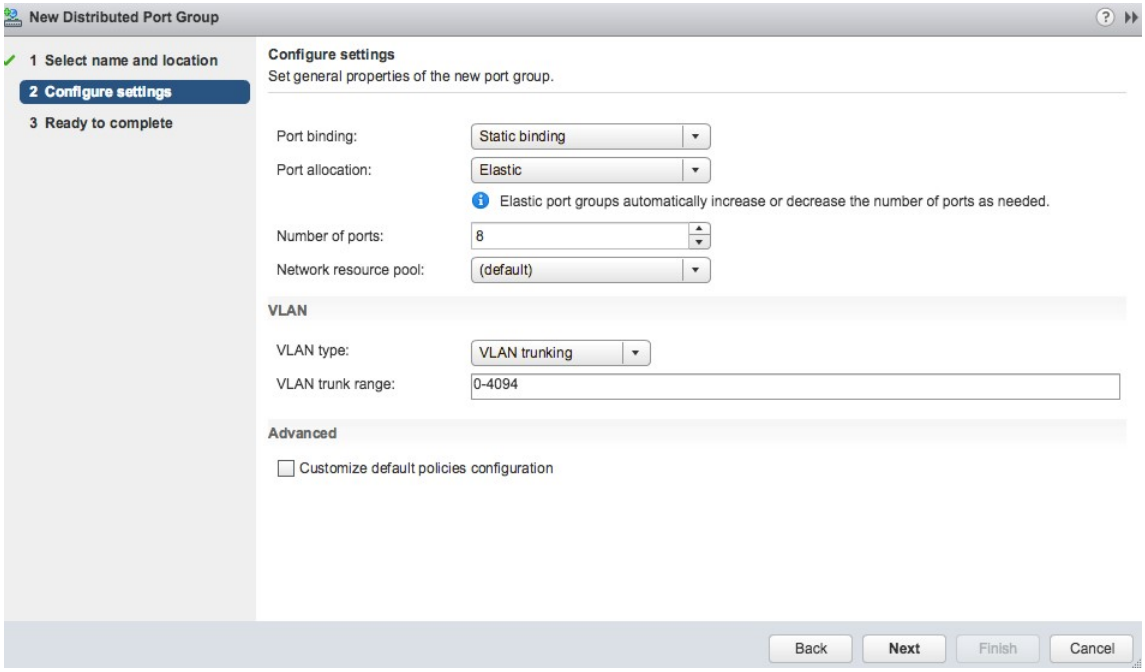
Configuration de VMware NSX

- Créez un pool d'instances Citrix ADC VPX de différentes capacités, qui sont ajoutées aux différents services packages.

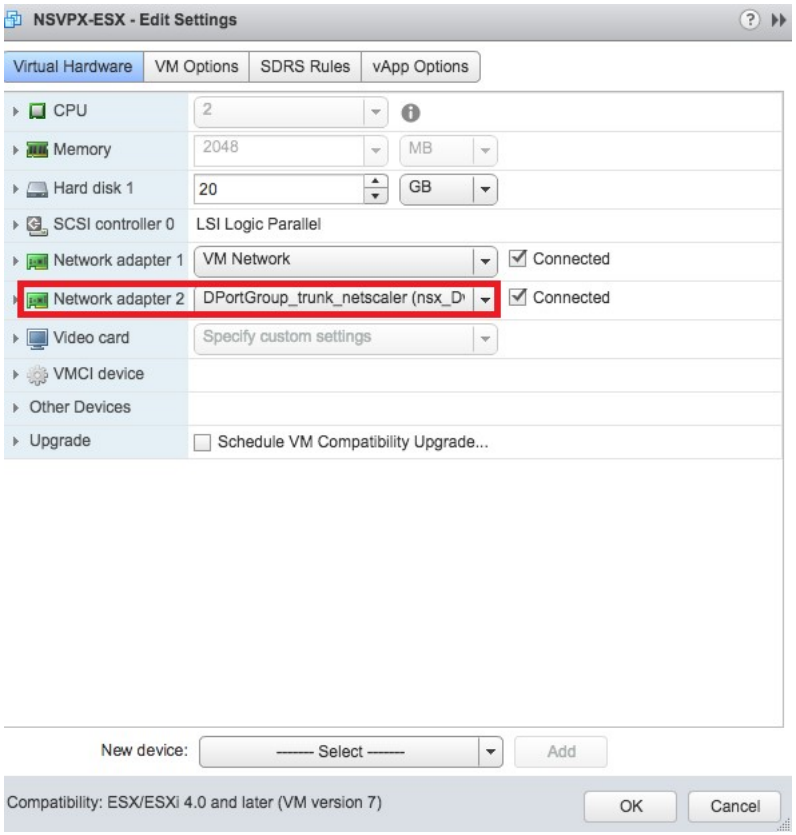
Par exemple :

- Créez cinq instances Citrix ADC VPX de VPX1000 (1 Gbit/s). Ces instances sont ajoutées au package de service Gold.
- Créez cinq instances Citrix ADC VPX de VPX10 (10 Mbit/s). Ces instances sont ajoutées au package de service Bronze.

1. Dans vSphere Client, accédez à **Networking**et créez un groupe de ports de type VLAN Trunking avec plage, par exemple, 101-105 (vous pouvez même fournir la plage complète, mais créer un groupe de ports de type VLAN pour uniquement les VLAN requis).

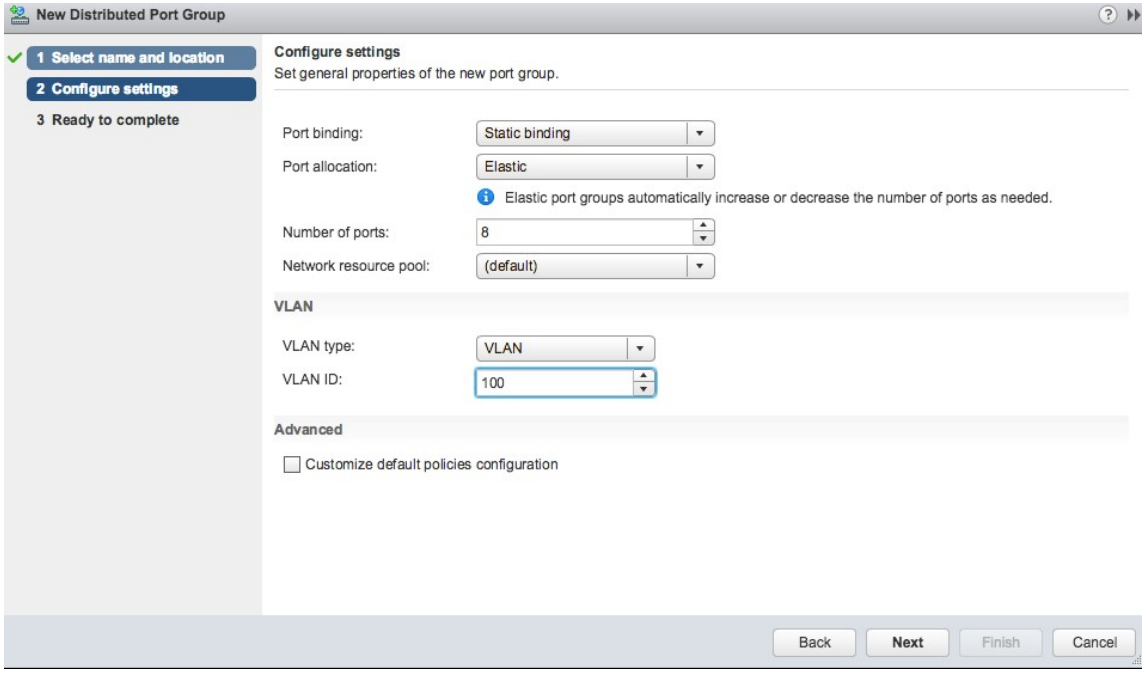


2. Créez une nouvelle interface pour chaque instance Citrix ADC VPX et attachez-la au groupe de ports de jonction de la plage de VLAN créé ci-dessus.



3. Dans vSphere Client, accédez à **Mise en réseau**et créez un groupe de ports de type VLAN.

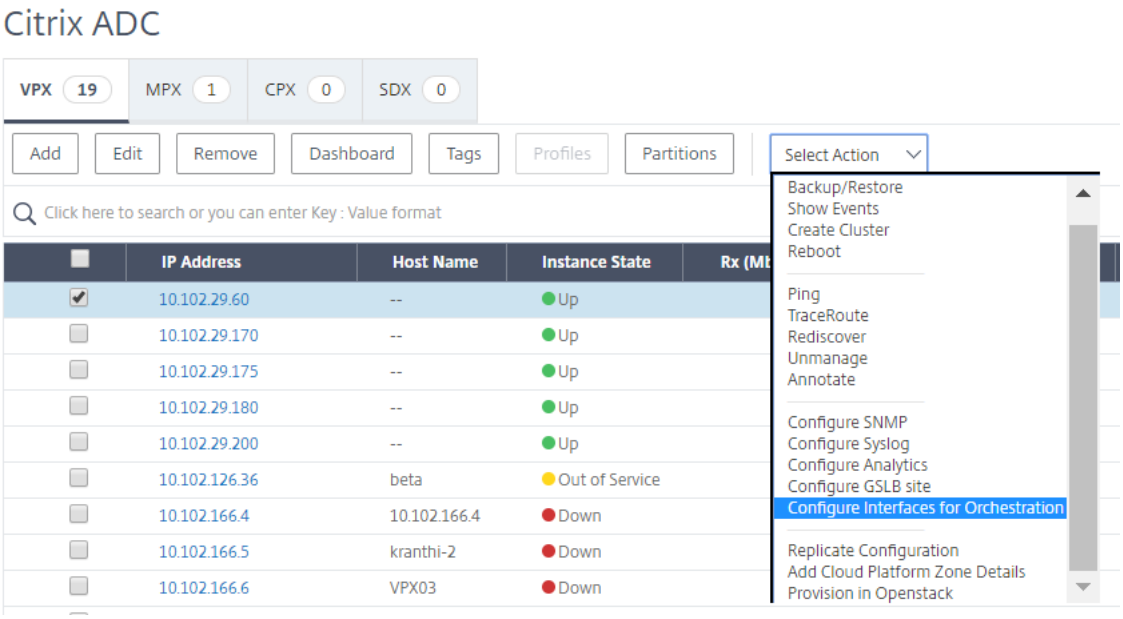
Par exemple, si le groupe de ports tronqués initial a été créé avec la plage 101 à 105, créez cinq groupes de ports VLAN un par VLAN, c'est-à-dire un groupe de ports avec VLAN 101, un autre avec VLAN102, etc., jusqu'à VLAN 105.



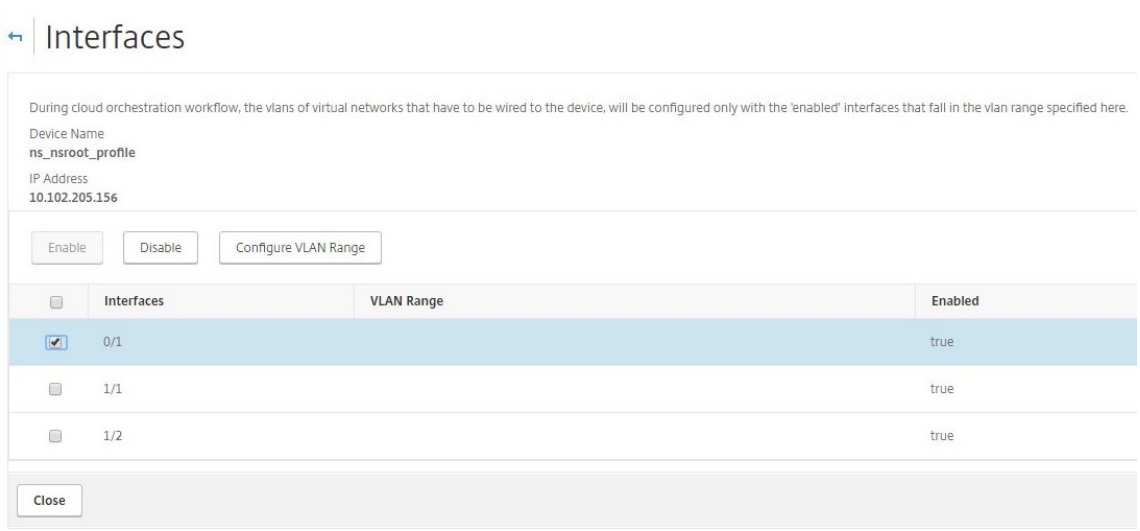
Ajout d'une instance Citrix ADC VPX dans Citrix ADM

Ajoutez des instances Citrix ADC VPX dans Citrix ADM et spécifiez la plage de VLAN du groupe tronqué pour chaque périphérique.

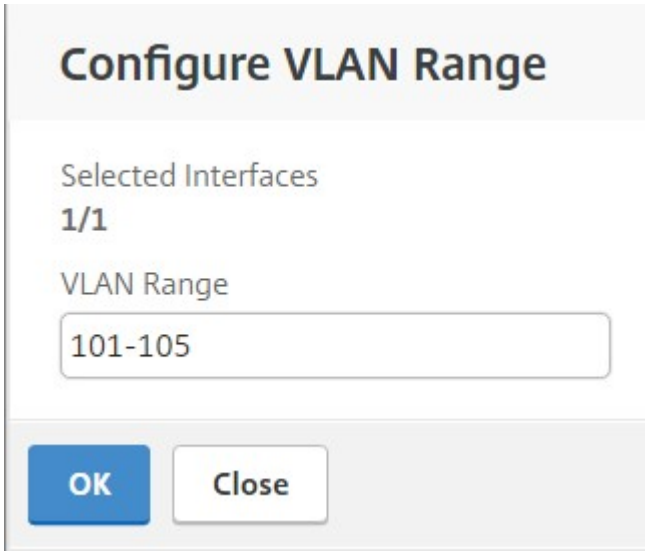
1. Dans Citrix ADM, accédez à **Infrastructure** > **Instances** > **Citrix ADC VPX**, puis cliquez sur **Ajouter**.
2. Sur la page **Ajouter un Citrix ADC VPX**, spécifiez les noms d'hôte des instances, l'adresse IP de chaque instance ou une plage d'adresses IP, puis sélectionnez un profil d'instance dans la liste **Profile Name**. Vous pouvez également créer un profil d'instance en cliquant sur l'icône +.
3. Cliquez sur **OK**.
4. Sélectionnez l'instance Citrix ADC VPX nouvellement ajoutée dans la liste de la page **Citrix ADC VPX**, puis cliquez sur le bouton flèche vers le bas dans le champ **Action**. Sélectionnez **Configurer les interfaces pour l'orchestration**.



5. Sur la page **Interfaces**, sélectionnez l'interface de gestion, puis cliquez sur **Désactiver**pour désactiver le VLAN de la liaison à l'interface de gestion.



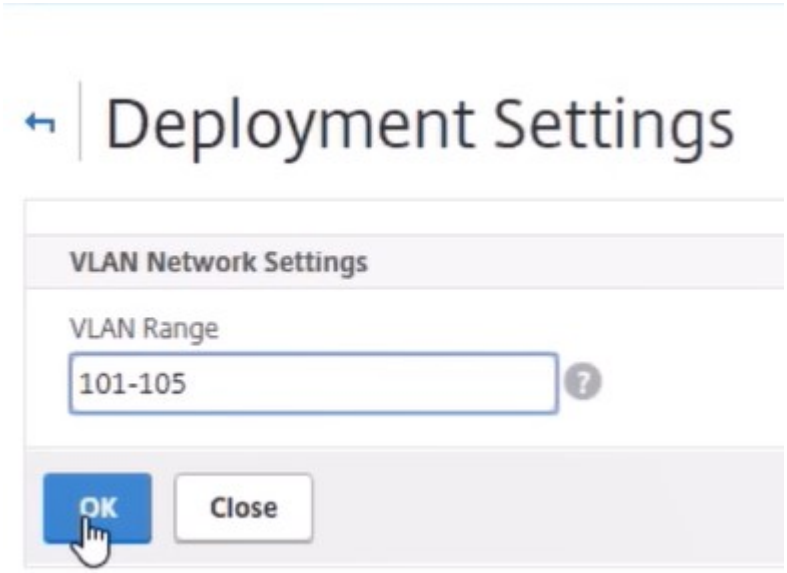
6. Sur la page **Interfaces**, sélectionnez l'interface requise, puis cliquez sur **Configurer VLAN Range**.
7. Entrez la plage de VLAN configurée dans NSX Manager, cliquez sur **OK**, puis cliquez sur **Fermer**.



Enregistrement de VMware NSX Manager auprès de Citrix ADM

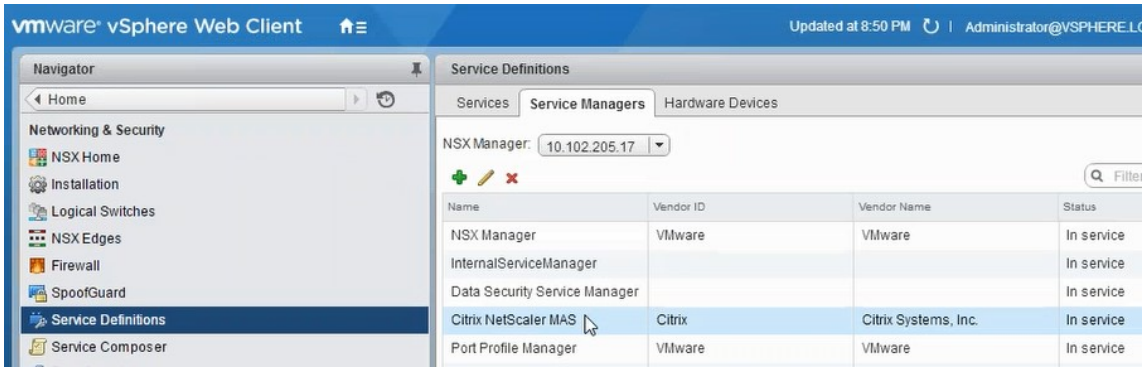
Enregistrez VMware NSX manager auprès de Citrix ADM pour créer un canal de communication entre eux.

1. Dans Citrix ADM, accédez à**Orchestration** >**SDN Orchestration**>**VMware NSX Manager** dans la liste déroulante, puis cliquez sur**Configurer les paramètres de NSX Manager**.
2. Dans la page **Configurer les paramètres de NSX Manager**, définissez les paramètres suivants :
   a) Adresse IP de NSX Manager : adresse IP de NSX Manager.
   b) Nom d'utilisateur de NSX Manager : nom d'utilisateur administratif de NSX Manager.
   c) Mot de passe - Mot de passe de l'utilisateur administratif de NSX Manager.
3. Dans le **compte Citrix ADM utilisé par NSX Manager** section, définissez le nom d'utilisateur et le mot de passe du pilote Citrix ADC pour NSX Manager. Citrix ADM authentifie les demandes de configuration d'équilibrage de charge à partir de NSX Manager à l'aide de ces informations d'identification d'ouverture de session.
4. Cliquez sur **OK**.
5. Accédez à **Orchestration** > **Système** > **Paramètres de déploiement.** Fournissez la plage de VLAN configurée dans le groupe de ports tronqués.



6. Ouvrez une session sur NSX Manager sur vSphere Web Client et accédez à **Définitions de service> Gestionnaire**de services.

   Vous pouvez afficher Citrix Citrix ADM comme l'un des gestionnaires de services. Cela indique que l'enregistrement réussit et qu'un canal de communication est établi entre le gestionnaire NSX et Citrix ADM.

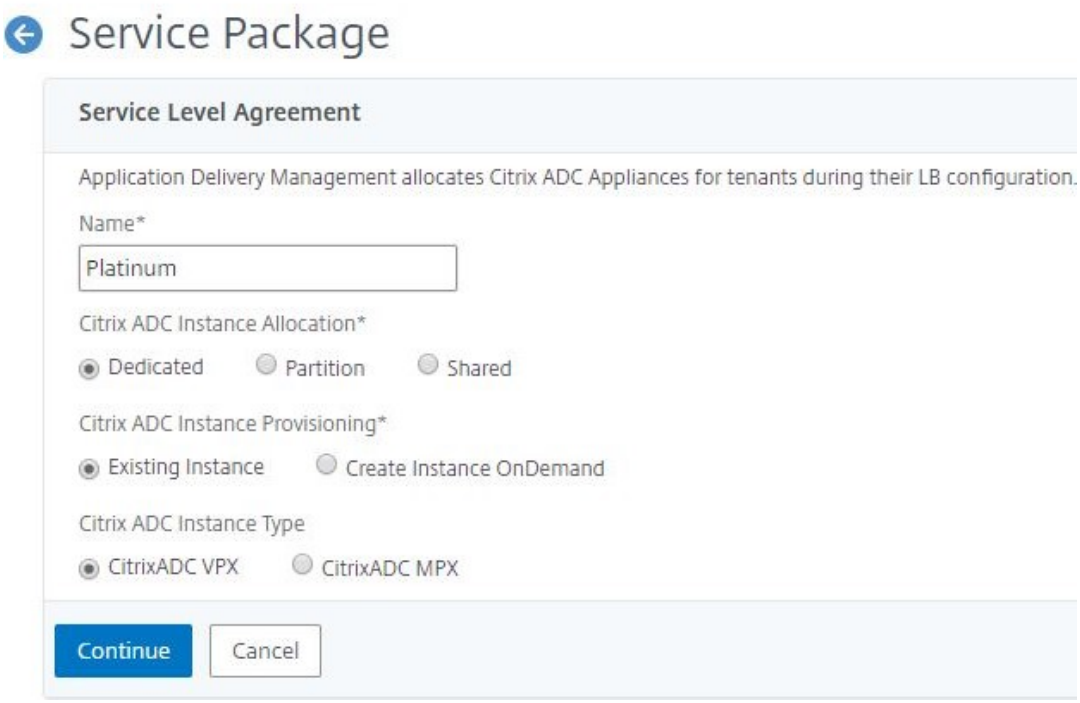


Création d'un Service Package dans Citrix ADM

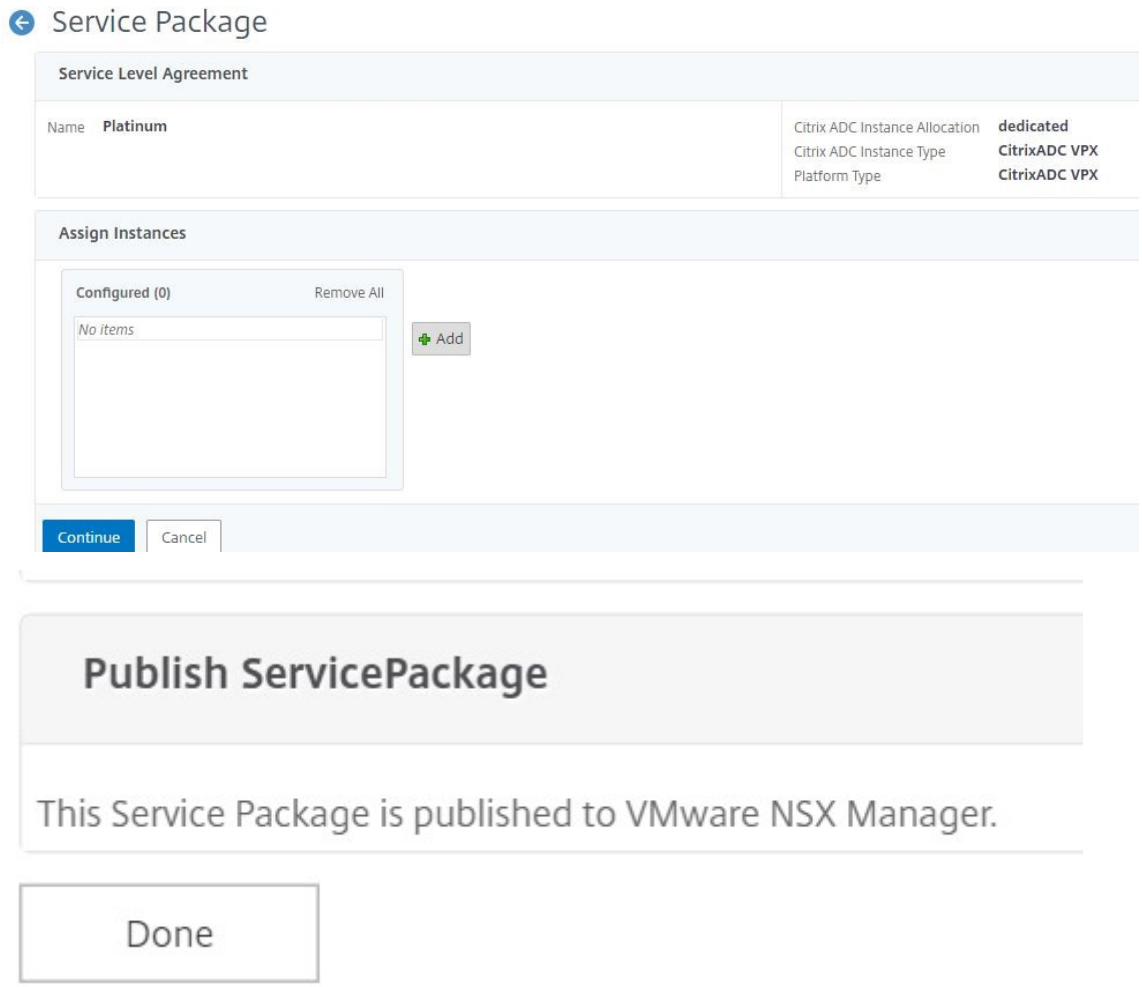
1. Dans Citrix ADM, accédez à**Orchestration** >**SDN Orchestration**>**VMware NSX Manager**> **Service Packages**, puis cliquez sur **Ajouter** pour ajouter un nouveau service package.
2. Dans la page **Service Package**, dans la section **Paramètres de base**, définissez les paramètres suivants :
   a) Nom : entrez le nom d'un package de services
   b) Stratégie d'isolement : par défaut, la stratégie d'isolement est définie sur Dédié
   c) Type de périphérique : par défaut, le type de périphérique est défini sur Citrix ADC VPX

> **Remarque**
>
> Ces valeurs sont définies par défaut dans cette version et vous ne pouvez pas les modifier.

d) Cliquez sur **Continuer**.



3. Dans la section **Affecter des périphériques**, sélectionnez le VPX préconfiguré pour ce package, puis cliquez sur **Continuer**.
4. Dans la section **Publier le service package**, cliquez sur **Continuer** pour publier le service package sur VMware NSX, puis cliquez sur **Terminé**.



Cette procédure configure un package de service dans NSX Manager. Plusieurs périphériques peuvent être ajoutés à un service et plusieurs tronçons peuvent utiliser le même service package pour décharger l'instance Citrix ADC VPX vers Citrix ADM.

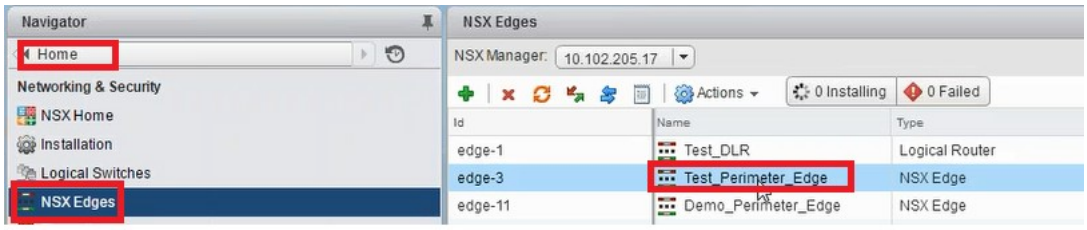
5. Ouvrez une session sur NSX Manager sur vSphere Web Client et accédez à **Définitions de service** > **Services**.

   Vous pouvez voir que le package de service Citrix ADM est enregistré.

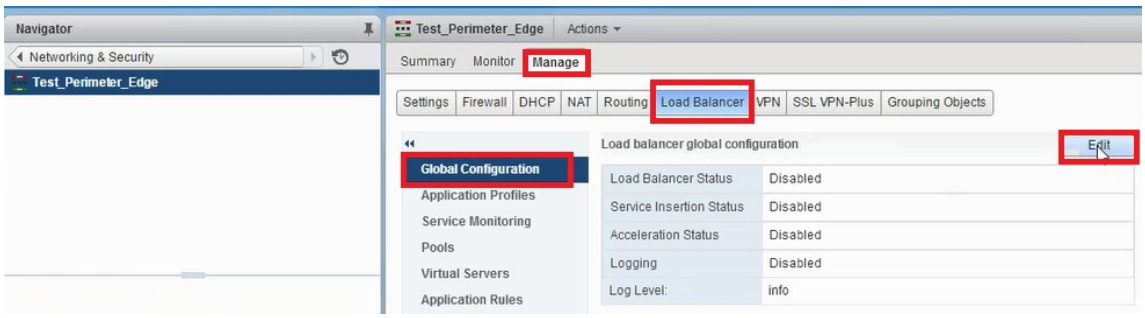
Exécution de l'insertion du service d'équilibrage de charge pour Edge

Effectuer l'insertion du service d'équilibrage de charge sur la Gateway NSX Edge créée précédemment (déchargez la fonction d'équilibrage de charge de NSX LB vers Citrix ADC).

1. Dans NSX Manager, accédez à **Accueil** > **NSX Edge**, puis sélectionnez la Gateway périphérique que vous avez configurée.

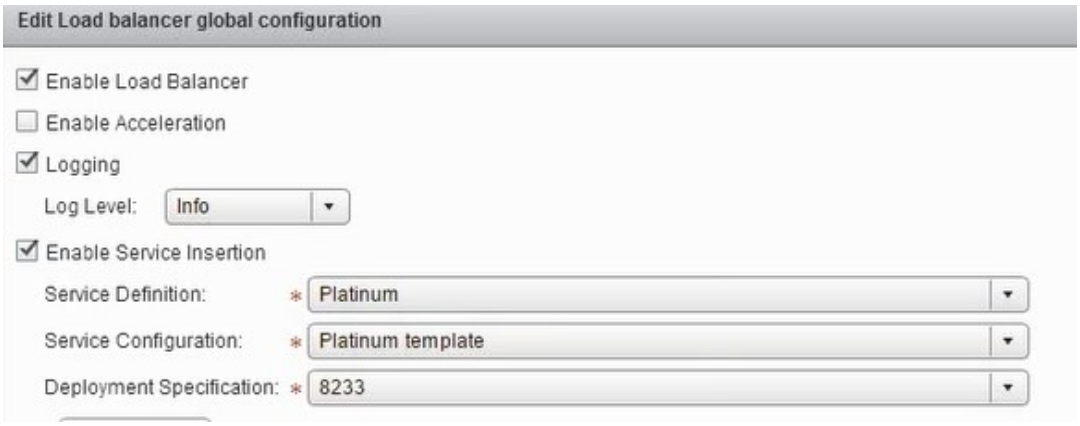


2. Cliquez sur **Gérer**, puis sur l'onglet **Équilibreur** de charge, sélectionnez **Configuration globale**, puis cliquez sur **Modifier**.

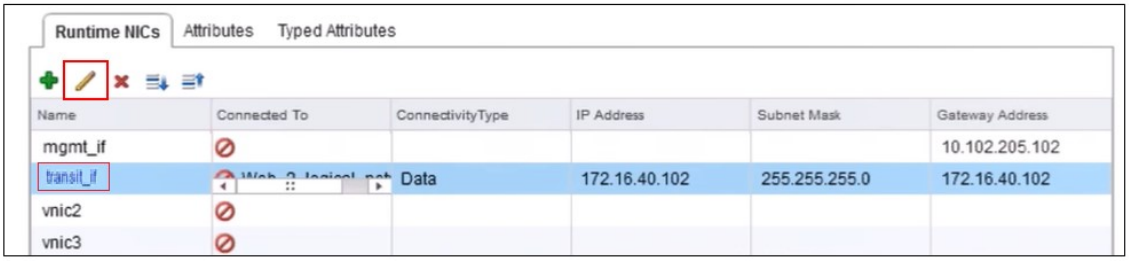


3. Sélectionnez **Activer l'équilibreur**de charge, **Journalisation**, **Activer l'insertion de service** pour les activer.

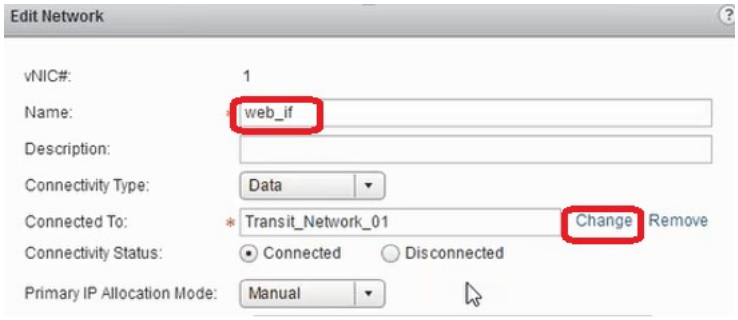
   a) Dans **Définition de service,** sélectionnez le package de service qui a été créé dans Citrix ADM et publié sur NSX Manager.



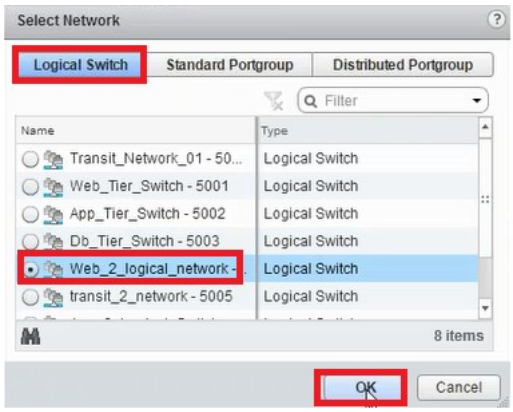
4. Sélectionnez les cartes réseau d'exécution existantes et cliquez sur l'icône Modifier pour modifier les cartes réseau d'exécution qui doivent être connectées lorsque Citrix ADC VPX est alloué.



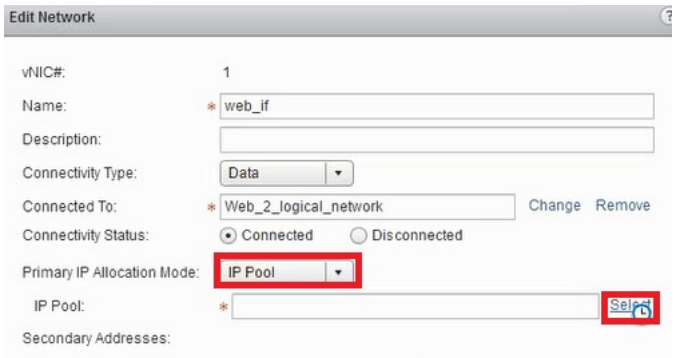
5. Modifiez le nom de la carte réseau, spécifiez le type de connectivité en tant que **données**, puis cliquez sur **Modifier**.



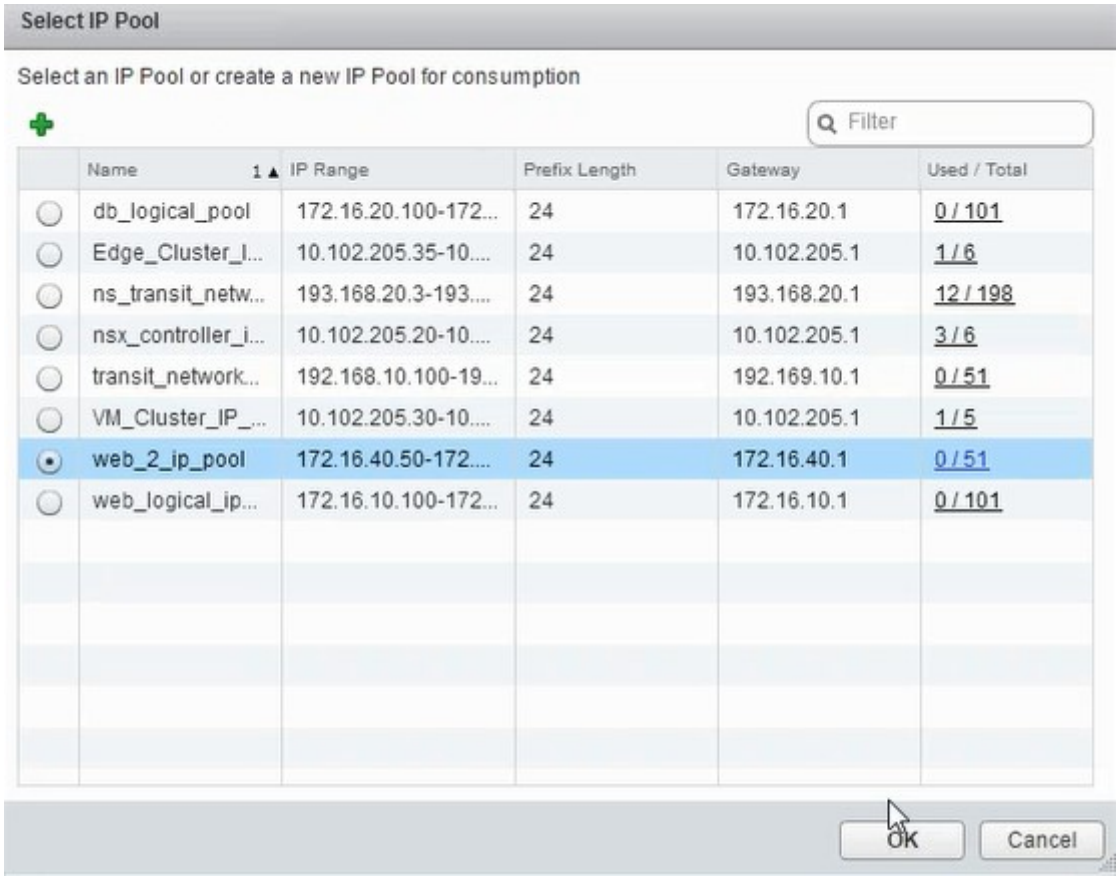
6. Sélectionnez le commutateur logique Web approprié.



7. Dans le **mode d'allocation IP primaire**, sélectionnez Pool IP dans la liste déroulante, puis cliquez sur le bouton flèche vers le bas dans le champ Pool IP.



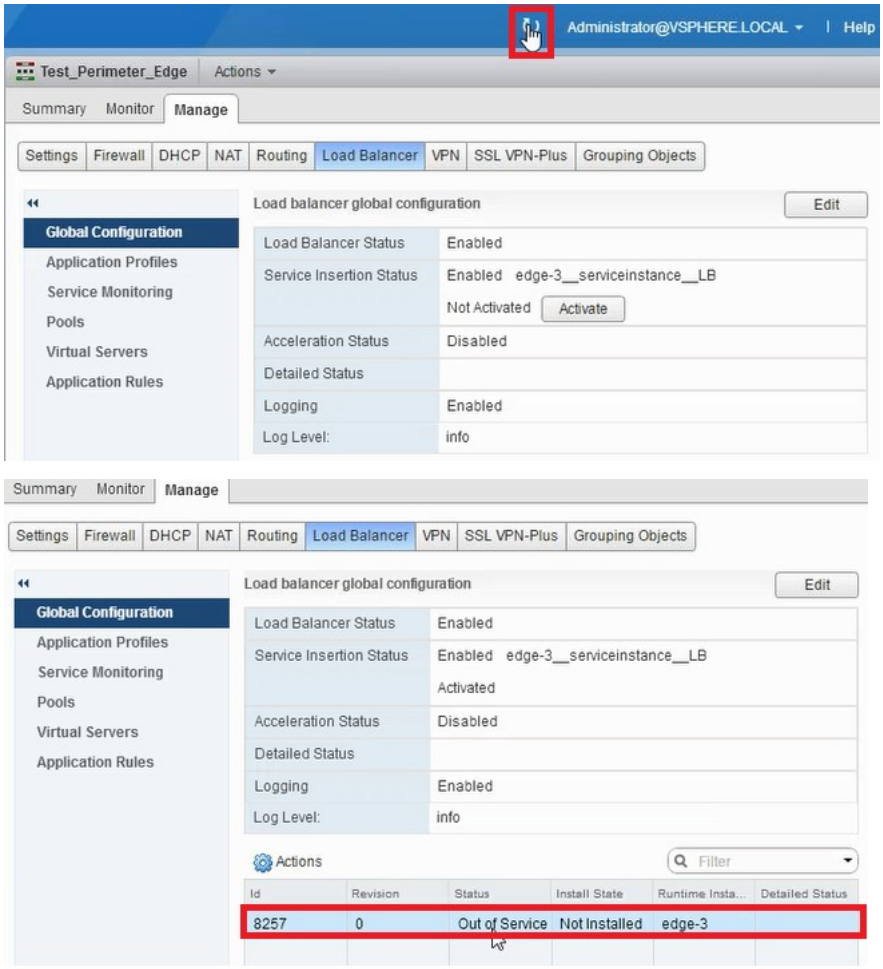
8. Dans la fenêtre **Sélectionner un pool d'adresses IP**, sélectionnez le pool d'adresses IP approprié, puis cliquez sur **OK**.



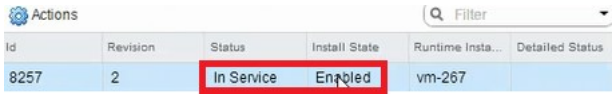
L'adresse IP est acquise et est définie comme adresse IP réseau source dans l'appliance Citrix ADC VPX. Une Gateway L2 est créée dans NSX Manager pour mapper le VXLAN au VLAN.

> **Remarque**
>
> Toutes les interfaces de données sont connectées en tant que cartes réseau d'exécution et font partie des interfaces pour DLR.

9. Actualisez la vue pour voir la création de l'heure d'exécution.



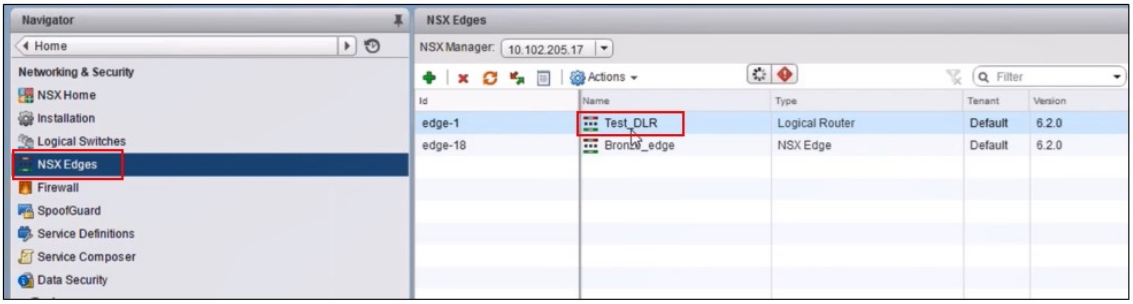
10. Une fois la machine virtuelle démarrée, la valeur de l'état passe à **En service** et celle de l'état d'installation passe à **Activé**.



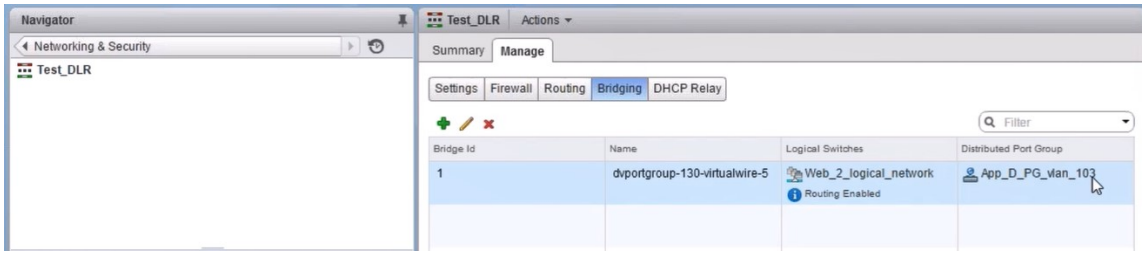
> **Remarque**
>
> Dans Citrix ADM, accédez à **Orchestration** > **Demandes** pour afficher les détails de progression de l'insertion du service LB.

Affichage de la passerelle L2 sur NSX Manager

1. Ouvrez une session sur NSX Manager sur vSphere Web Client, accédez à **NSX Edge**et sélectionnez le DLR créé.



2. Dans la page DLR, accédez à **Gérer** > **Bridging**. Vous pouvez voir la Gateway L2 affichée dans la liste.

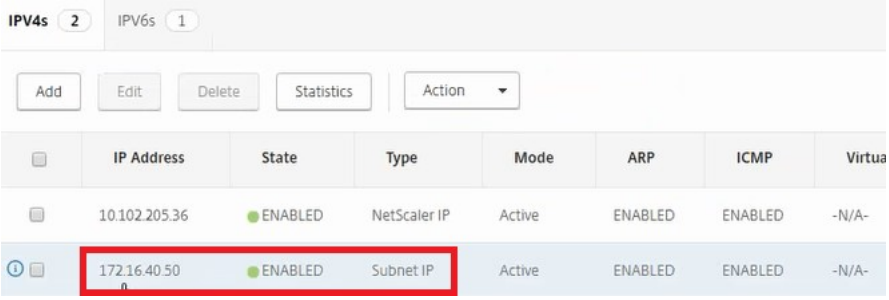


> **Remarque**
>
> Une Gateway L2 est créée pour chaque interface de données.

Affichage de Citrix ADC alloué

1. Ouvrez une session sur l'instance Citrix ADC VPX à l'aide de l'adresse IP affichée dans Citrix ADM.Ensuite, accédez à **Configuration** > **Système** > **Mise en réseau**. Dans le volet droit, vous pouvez voir que les deux adresses IP sont ajoutées. Cliquez sur le lien hypertexte de l'adresse IP pour afficher les détails.

L'adresse IP du sous-réseau est identique à l'adresse IP de l'interface Web ajoutée dans le NSX.



2. Accédez à **Configuration** > **Système** > **Licences** pour afficher les licences appliquées à cette instance.

Configuration de l'instance Citrix ADC VPX à l'aide de StyleBook

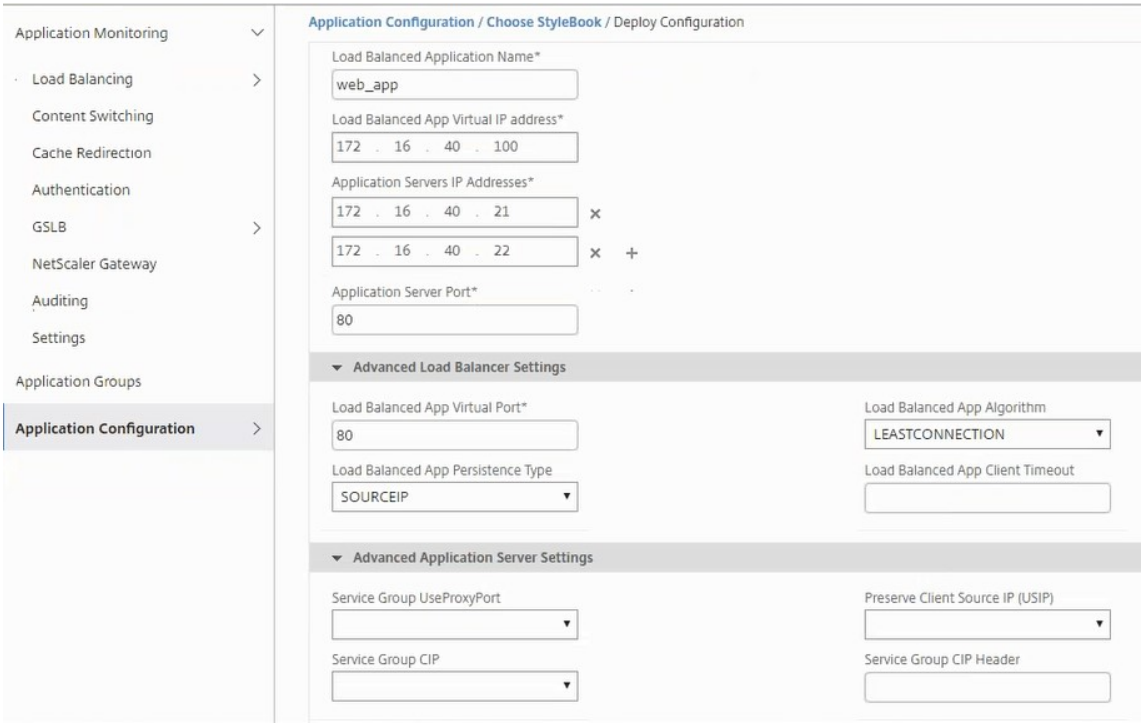
1. Dans Citrix ADM, accédez à **Orchestration** > **SDN Orchestration** > **Configurer NSX Manager** > **Edge Gateways**.

   Notez l'adresse IP de l'instance Citrix ADC qui est attribuée à la passerelle Edge respective sur laquelle la configuration d'équilibrage de charge via StyleBooks doit être appliquée.

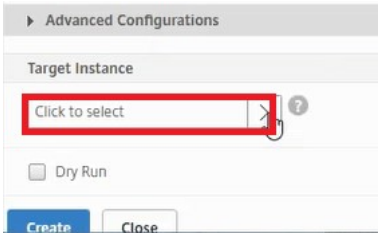
2. Créez un nouveau StyleBook. Accédez à **Applications** > **Configuration**, importez le StyleBook et sélectionnez le StyleBook dans la liste.

   Pour créer un nouveau StyleBook, voir Créer votre propre StyleBook.

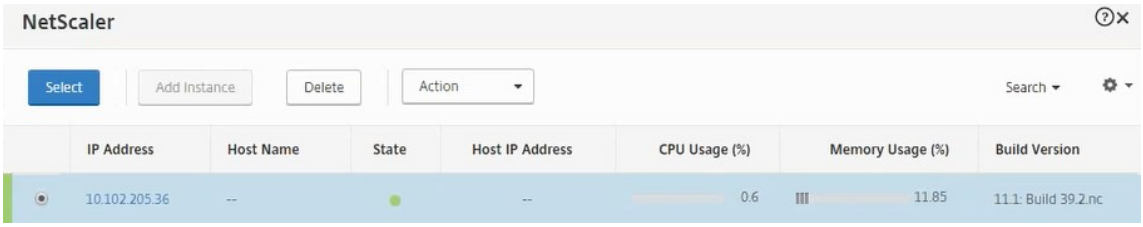
3. Spécifiez des valeurs pour tous les paramètres requis.



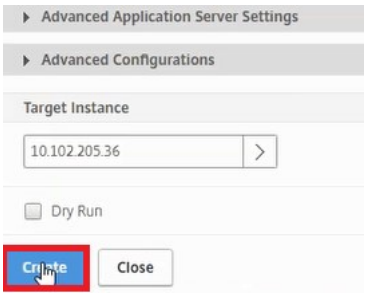
4. Spécifiez l'instance Citrix ADC VPX sur laquelle vous souhaitez exécuter ces paramètres de configuration.



5. Sélectionnez l'instance IP mentionnée précédemment, puis cliquez sur **Sélectionner**.

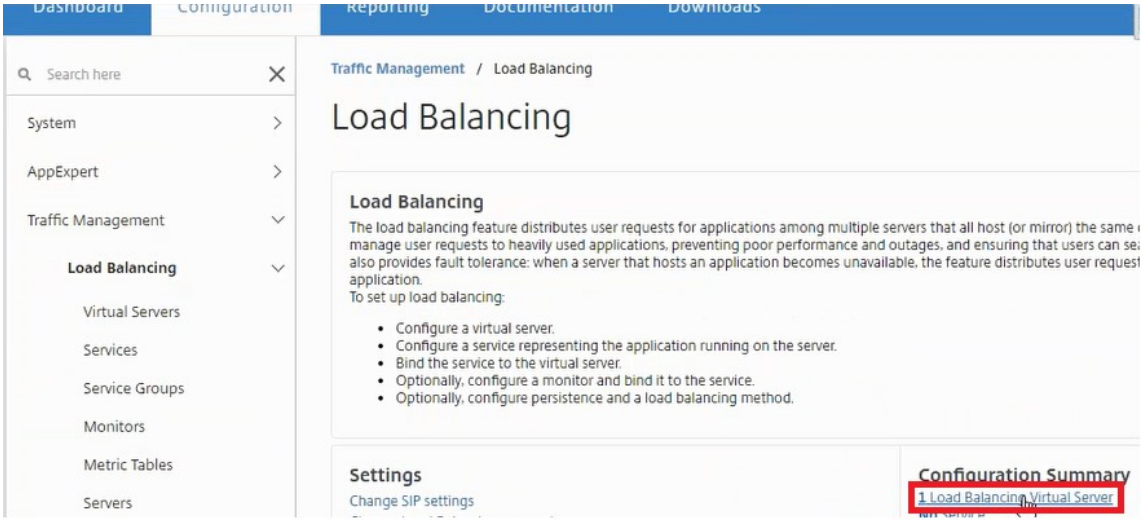


6. Cliquez sur **Créer** pour appliquer la configuration sur le périphérique sélectionné.

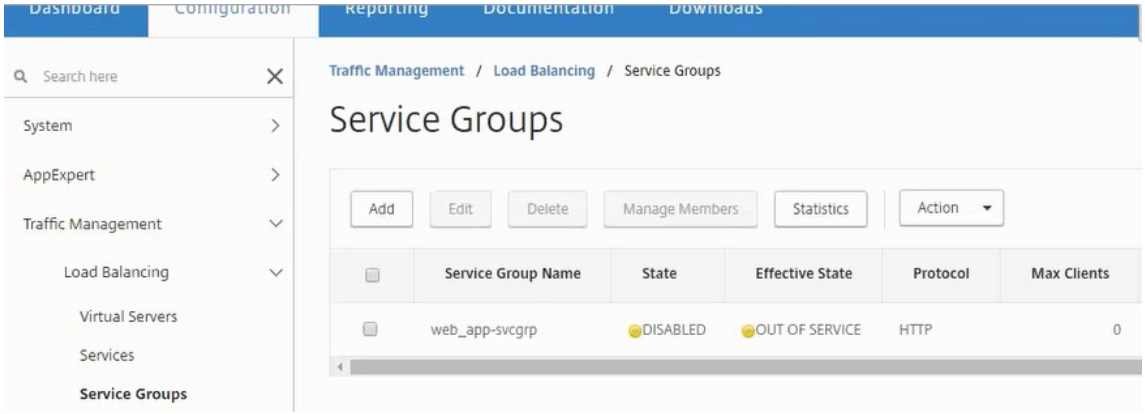


Affichage de la configuration de l'équilibreur de charge

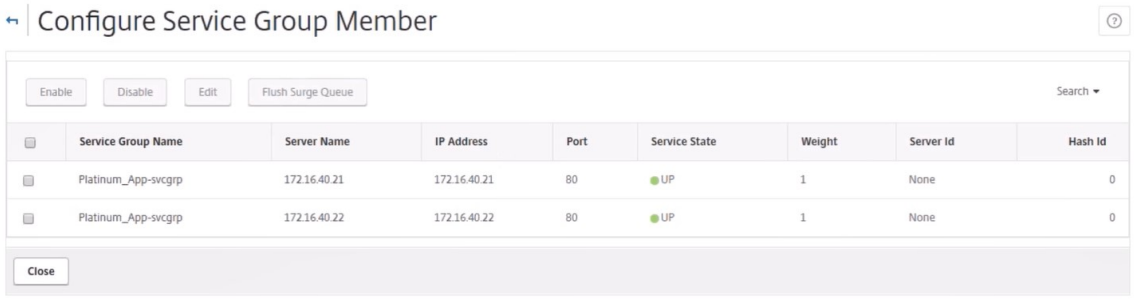
1. Ouvrez une session sur l'instance Citrix ADC VPX, accédez à **Configuration** > **Gestion du trafic** > **Équilibrage de charge** pour afficher le serveur virtuel d'équilibrage de charge créé.



Vous pouvez également afficher les groupes de services créés.



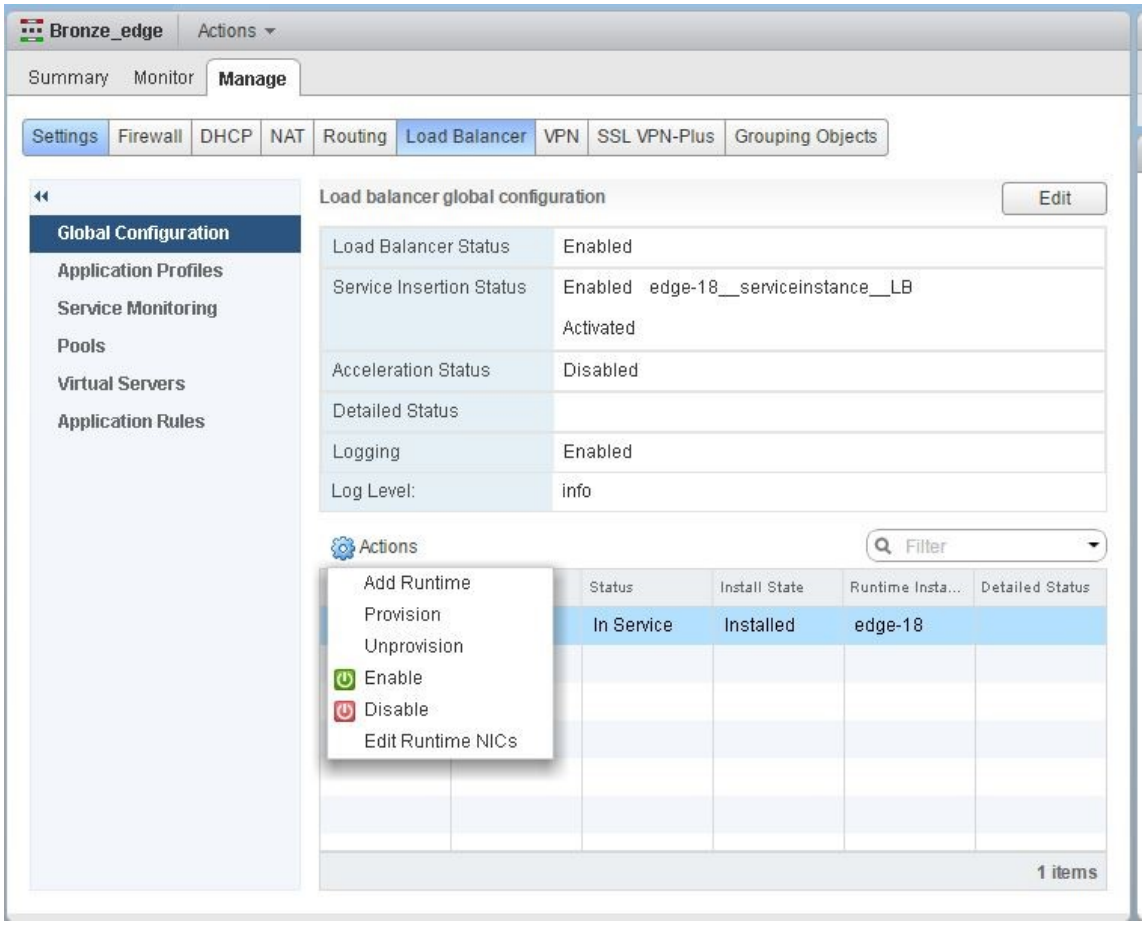
2. Sélectionnez le groupe de services, puis cliquez sur **Gérer les membres**. La page **Configurer un membre de groupe de services** affiche les membres associés au groupe de services.



Suppression du service d'équilibrage de charge

1. Dans Citrix ADM, accédez à **Applications** > **Configuration**, puis cliquez sur l'icône **X** pour supprimer la configuration de l'application.
2. Ouvrez une session sur NSX Manager sur vSphere Web Client et accédez à la Gateway périphérique à laquelle l'instance Citrix ADC VPX est connectée.
3. Accédez à **Gérer** > **Équilibreur de charge** > **Configuration globale**, cliquez avec le bouton droit sur l'entrée d'exécution, puis cliquez sur **Déprovisionner**.

> **Remarque**
>
> Gateways Edge dans Citrix ADM correspond à des entrées d'exécution dans NSX manager.



L'instance Citrix ADC VPX est rendue hors service.

4. Dans Citrix ADM, accédez à **Orchestration** > **SDN Orchestration** > **Configurer NSX Manager** > **Edge Gateways**. Vérifiez que le mappage respectif de Edge Gateway avec l'instance supprimée n'est pas présent.

NSX Manager : Provisioning automatique des instances Citrix ADC

February 1, 2024

Vue d'ensemble

Citrix Application Delivery Management (ADM) s'intègre à la plate-forme de virtualisation réseau VMware pour automatiser le déploiement, la configuration et la gestion des services Citrix ADC. Cette intégration évite les complexités traditionnelles associées à la topologie de réseau physique,

permettant aux administrateurs vSphere/vCenter de déployer par programmation les services Citrix ADC plus rapidement.

Lors de l'insertion et de la suppression du service d'équilibrage de charge sur VMware NSX Manager, Citrix ADM provisionnent et détruit dynamiquement les instances de Citrix ADC. Ce Provisioning dynamique nécessite l'automatisation des attributions de licences Citrix ADC VPX dans Citrix ADM. Lorsque les licences Citrix ADC sont téléchargées vers Citrix ADM, Citrix ADM joue le rôle de serveur de licences.

Conditions préalables

> **Remarque**
>
> Cette intégration est prise en charge uniquement pour **VMware NSX for vSphere 6.1 ou version antérieure**.

- Citrix ADM, version 13.0 installation en haute disponibilité et installé sur ESX.
- Citrix ADC VPX, version 13.0
- Licences Citrix ADC VPX pour les instances Citrix ADC VPX, version 13.0
- Installez VMware ESXi version 4.1 ou ultérieure avec du matériel répondant à la configuration minimale requise.
- Installez VMware Client sur une station de travail de gestion qui répond à la configuration système minimale requise.
- Installez VMware OVF Tool (requis pour VMware ESXi version 4.1) sur une station de travail de gestion répondant à la configuration minimale requise.

Déploiement haute disponibilité des instances Citrix ADM et Citrix ADC

Pour provisionner le programme d'installation de Citrix ADM HA, installez le fichier image Citrix ADM que vous avez téléchargé à partir du site de téléchargement Citrix. Pour plus d'informations sur la façon de configurer Citrix ADM HA, consultez Déploiement de Citrix ADM en haute disponibilité.

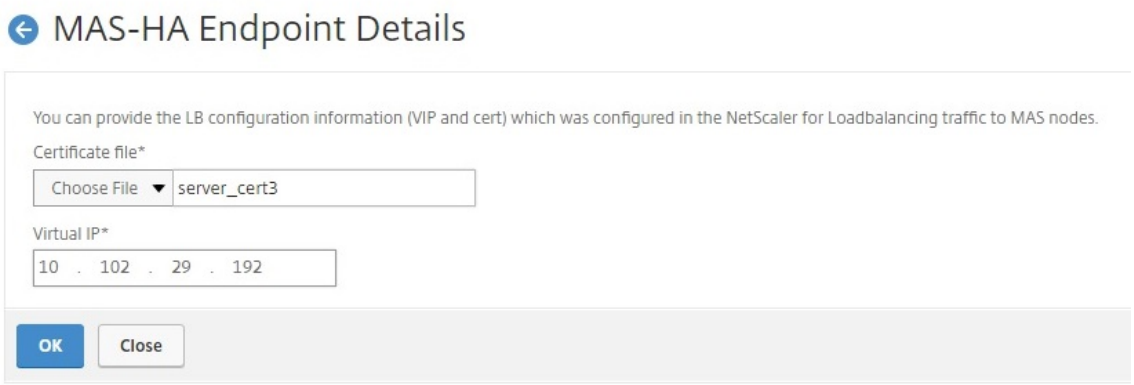
Configuration des détails du point de terminaison Citrix ADM HA

Pour intégrer VMware NSX Manager à Citrix ADM déployé en mode HA, vous devez d'abord entrer l'adresse IP virtuelle de l'instance d'équilibrage de charge Citrix ADC. Vous devez également télécharger le fichier de certificat présent sur le serveur virtuel d'équilibrage de charge de Citrix ADC vers le système de fichiers Citrix ADM.

Pour fournir des informations de configuration d'équilibrage de charge dans Citrix ADM :

1. Dans le nœud Citrix ADM HA, accédez à **Système** > **Déploiement**.
2. Cliquez sur **Paramètres HA** dans le coin supérieur droit et dans la page **Paramètres MAS-HA**, cliquez sur **Détails du point de terminaison MAS-HA**.

3. Sur la page **Détails du point de terminaison MAS-HA**, téléchargez le même certificat qui est déjà présent sur l'instance d'équilibrage de charge Citrix ADC.
4. Entrez l'adresse IP virtuelle de l'instance d'équilibrage de charge Citrix ADC et cliquez sur **OK**.



Enregistrement de VMware NSX Manager auprès de Citrix ADM

Lorsque vous configurez deux serveurs Citrix ADM en haute disponibilité, les deux nœuds de serveur sont en mode actif-passif. Ouvrez une session sur le nœud serveur Citrix ADM principal pour enregistrer VMware NSX manager auprès de Citrix ADM dans HA, afin de créer un canal de communication entre eux.

Pour enregistrer VMware NSX manager auprès de Citrix ADM dans HA :

1. Dans le nœud serveur Citrix ADM principal, accédez à **Orchestration** > **SDN Orchestration** > **VMware NSX Manager**.
2. Cliquez sur **Configurer les paramètres de NSX Manager**.
3. Dans la page **Configurer les paramètres de NSX Manager**, définissez les paramètres suivants :
   a) Adresse IP de NSX Manager : adresse IP de NSX Manager.
   b) Nom d'utilisateur de NSX Manager : nom d'utilisateur administratif de NSX Manager.

c) Mot de passe - Mot de passe de l'utilisateur administratif de NSX Manager.

4. Dans la section Compte Citrix ADM utilisé par NSX Manager, définissez le mot de passe du pilote Citrix ADC pour NSX Manager.
5. Cliquez sur **OK**.

Chargement de licences dans Citrix ADM

Chargez les licences Citrix ADC VPX vers Citrix ADM, afin que Citrix ADM puisse automatiquement allouer des licences aux instances lors de l'orchestration avec NSX.

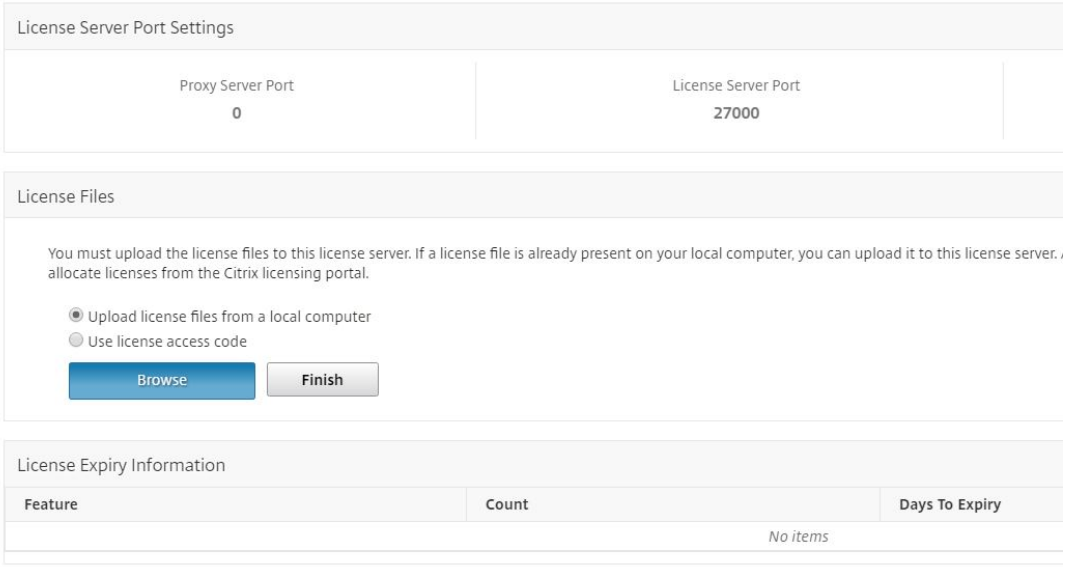
Pour installer des fichiers de licence sur Citrix ADM :

1. Dans Citrix ADM, accédez à **Réseaux** > **Licences.**
2. Dans la section **Fichiers de licence**, sélectionnez l'une des options suivantes :

   a) **Télécharger des fichiers de licences à partir d'un ordinateur local** : si un fichier de licence est déjà présent sur votre ordinateur local, vous pouvez le télécharger sur Citrix ADM. Pour ajouter des fichiers de licence, cliquez sur **Parcourir** et sélectionnez le fichier de licence (.lic) que vous souhaitez ajouter. Cliquez ensuite sur **Terminer**.

   b) **Utiliser le code d'accès aux licences** - Citrix envoie par e-mail le code d'accès à la licence pour les licences que vous achetez. Pour ajouter des fichiers de licence, entrez le code d'accès à la licence dans la zone de texte, puis cliquez sur **Obtenir des licences**.

   > **Remarque**
   >
   > À tout moment, vous pouvez ajouter d'autres licences à Citrix ADM à partir des paramètres de licence.



Téléchargement d'images Citrix ADC VPX dans Citrix ADM

Ajoutez les images Citrix ADC à Citrix ADM afin que Citrix ADM utilise ces images comme défini dans le service package.

Pour charger des images Citrix ADC VPX dans Citrix ADM :

1. Dans Citrix ADM, accédez à **Orchestration** > **SDN Orchestration** > **VMware NSX Manager** > **Images ESX NSVPX**.
2. Cliquez sur **Télécharger**, puis sélectionnez le package zip Citrix ADC VPX dans le dossier de stockage local.

Création de Service Packages dans Citrix ADM

Créez des packages de services dans Citrix ADM pour définir l'ensemble de SLA, qui indique comment les ressources Citrix ADC sont allouées.

Pour créer des packages de service dans Citrix ADM :

1. Dans Citrix ADM, accédez à **Orchestration** > **SDN Orchestration** > **VMware NSX Manager** > **Service Packages**, puis cliquez sur **Ajouter** pour ajouter un nouveau service package.
2. Dans la page **Service Package**, dans la section **Paramètres de base**, définissez les paramètres suivants :

    a) Nom : nom d'un package de services

    b) Stratégie d'isolement - sélectionnez **Dédié**

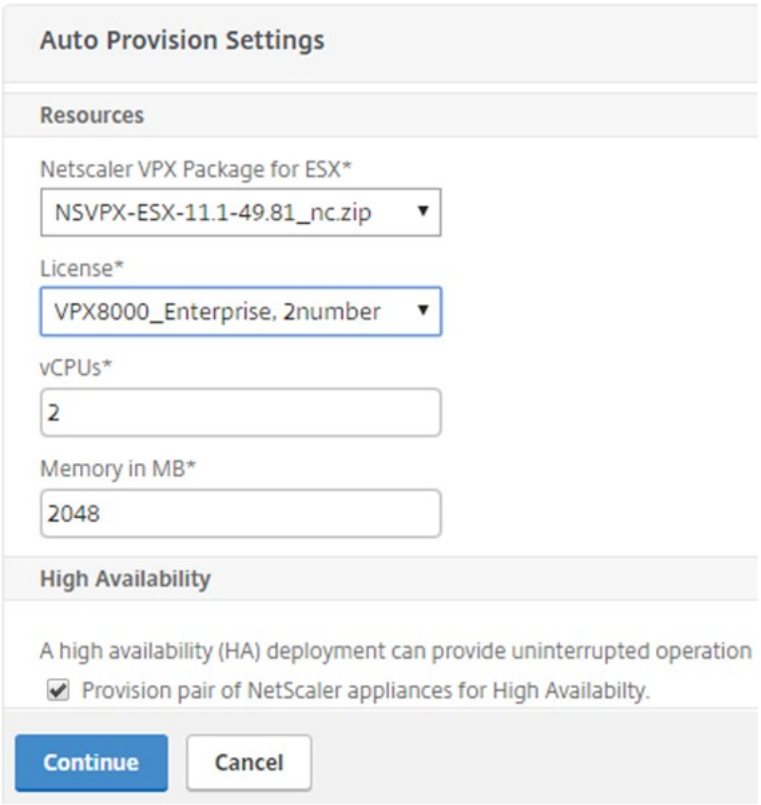
c) Provisioning d'instance Citrix ADC - sélectionnez **Créer une instance à la demande**

d) Plateforme de provisionnement automatique - sélectionnez **CitrixADC SDX**

e) Cliquez sur **Continue**.

3. Dans la section **Paramètres de provisionnement automatique**, sélectionnez le package zip Citrix ADC VPX récemment téléchargé pour le déployer sur la plate-forme NSX, sélectionnez la licence correspondante, puis cliquez sur **Continuer**.

> **Remarque**
>
> Dans **la section Haute disponibilité**, cochez la case pour provisionner les instances Citrix ADC pour HA.



> **Remarque**
>
> Le nom de la licence affiché dans la zone de liste illustrée dans la figure ci-dessus, VPX8000_Advanced, numéro 2 est un exemple et est expliqué comme suit :
>
> - VPX - la licence consiste à déployer des instances Citrix ADC VPX
> - 8000 - la bande passante consommable est de 8 Go
> - Avancé - Citrix fournit trois types de licences : Standard, Advanced et Premium

> - 2 nombre - deux instances Citrix ADC VPX peuvent être déployées à l'aide de cette licence
>
> Le nom de la licence affichée dans la zone de liste**Licence** dépend de la licence que vous avez achetée auprès de Citrix.

4. Cliquez sur **Continue**.
5. Le package de services est publié sur NSX Manager. Dans NSX Manager, accédez à **Définitions de service** > **Gestionnaires de service**. Vous pouvez afficher Citrix ADM comme l'un des gestionnaires de services. Cela indique que l'enregistrement est réussi et que la communication bidirectionnelle est établie entre le gestionnaire NSX et Citrix ADM.

> **Remarque**
>
> Pour Citrix ADM en déploiement haute disponibilité, les licences sont chargées uniquement dans le nœud de serveur de licences Citrix ADM. Les nœuds Citrix ADM sont en mode actif-passif.

Exécution de l'insertion du service d'équilibrage de charge pour Edge

Effectuez l'insertion du service d'équilibrage de charge sur la passerelle NSX Edge existante, c'est-à-dire déchargez la fonction d'équilibrage de charge de l'équilibreur de charge NSX vers Citrix ADC.

Pour insérer un service d'équilibrage de charge sur NSX Edge Gateway :

1. Dans NSX Manager, accédez à **Accueil** > **Mise en réseau et sécurité** > **NSX Edges**, puis double-cliquez pour sélectionner la passerelle Edge que vous avez configurée.
2. Cliquez sur **Gérer**, puis sur l'onglet **Équilibreur** de charge, sélectionnez **Configuration globale**, puis cliquez sur **Modifier**.
3. Sélectionnez **Activer l'équilibreur de charge** et **Activer l'insertion de services** pour les activer.
4. Dans **Définition du service**, sélectionnez le package de service qui a été publié sur NSX Manager.
5. Configurez une carte réseau virtuelle pour l'interface de gestion et une ou plusieurs cartes réseau virtuelles pour les interfaces de données. Sélectionnez les réseaux à gérer et les données en conséquence.

> **Remarque**
>
> Sélectionnez l'option Pool IP en mode Allocation IP principale. Citrix ADM ne prend pas en charge l'allocation manuelle ou DHCP des adresses IP.

6. Cliquez sur l'icône d'actualisation pour voir la création de l'heure d'exécution.

> **Remarque**
>
> Étant donné que vous déployez deux instances Citrix ADC VPX dans le déploiement HA, deux temps d'exécution sont créés dans le gestionnaire NSX.
>
> Vous devrez peut-être actualiser l'écran pour afficher les temps d'exécution affichés à l'écran.

7. Sélectionnez l'heure d'exécution, cliquez sur **Actions**, puis sélectionnez **Installer** dans le menu contextuel. Pour HA, répétez cette opération pour l'autre temps d'exécution également.
8. Lorsque les deux machines virtuelles démarrent, la valeur de Status passe à « En service » et celle de Install State passe à « Enabled ».

   > **Remarque**
   >
   > Vous devrez peut-être actualiser l'écran pour afficher le changement d'état.

9. Dans Citrix ADM, accédez à **Orchestration** > **Demandes** pour afficher les détails de progression de l'insertion de service. Vous pouvez voir qu'une demande de création et de mise à jour de l'heure d'exécution a été envoyée à Citrix ADM. Lorsque l'heure d'exécution a été mise à jour, sélectionnez la demande et cliquez sur le bouton **Tâches** pour afficher que Citrix ADM a été ajouté dans NSX Manager.

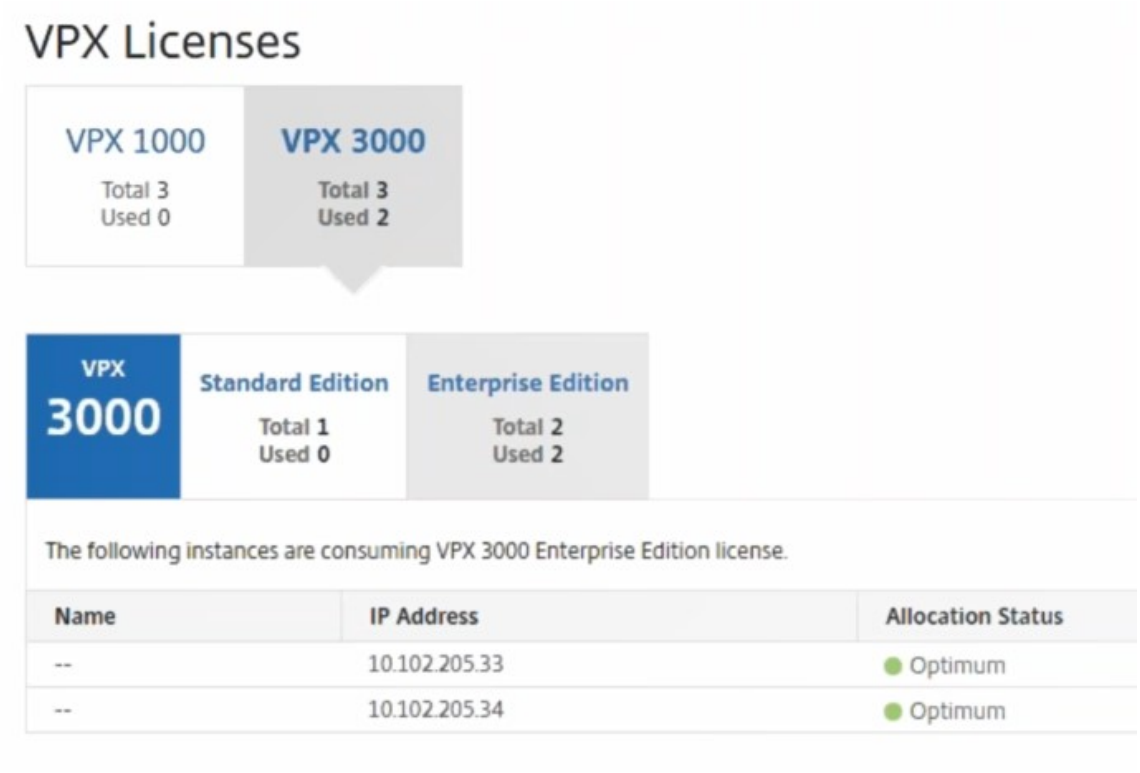
   Pour HA, il y aura deux demandes pour créer et mettre à jour deux fois d'exécution dans Citrix ADM. Lorsque les deux temps d'exécution ont été mis à jour, sélectionnez les deux demandes et cliquez sur le bouton **Tâches** pour afficher que deux nœuds Citrix ADM HA ont été ajoutés dans NSX Manager.

10. Dans Citrix ADM, accédez à **Orchestration** > **SDN Orchestration** > **VMware NSX Manager** > **Edge Gateways**. Dans le panneau de droite, vous pouvez afficher que Citrix ADC VPX a été ajouté à NSX Edge Gateway.

    Pour HA, vous pouvez voir que deux instances Citrix ADC VPX en mode HA ont été ajoutées à la passerelle NSX Edge.

11. Dans Citrix ADM, accédez à **Réseaux** > **Licences > LicencesVPX Licences**. Sélectionnez la licence Citrix ADC VPX et l'édition que vous avez installée.

    Les instances Citrix ADC VPX qui sont en mode HA consomment deux licences et l'état s'affiche à l'écran comme ci-dessous.



Lorsque l'insertion du service est terminée, vous pouvez utiliser StyleBooks pour configurer les instances Citrix ADC selon l'une des deux méthodes suivantes :

- Configuration des services d'équilibrage de charge sur Citrix ADC VPX dans l'interface graphique VMware NSX Manager
- Configuration des services d'équilibrage de charge sur Citrix ADC VPX dans l'interface graphique Citrix ADM

Configuration des services d'équilibrage de charge sur Citrix ADC VPX dans l'interface graphique VMware NSX Manager

Effectuez la tâche suivante pour activer la configuration des services d'équilibrage de charge sur le périphérique de Gateway NSX Edge à l'aide de StyleBooks intégrés.

Dans NSX Manager, accédez à **Accueil** > **Mise en réseau et sécurité** > **NSX Edges**, puis double-cliquez pour sélectionner la passerelle Edge que vous avez configurée.

Création de pools et de membres de pool

Créez un pool de serveurs et de membres de capacités différentes.

1. Cliquez sur **Gérer**, puis sur l'onglet **Load Balancer**, sélectionnez **Pools**, puis cliquez sur l'icône « **+** » pour ajouter un nouveau pool et définir les paramètres suivants :

   a) Nom : nom du nouveau pool

   b) Algorithme - Sélectionnez un algorithme dans la liste déroulante sur laquelle le pool sera sélectionné.

   c) Moniteurs - Assurez-vous que le moniteur de service est réglé sur default_http_monitor

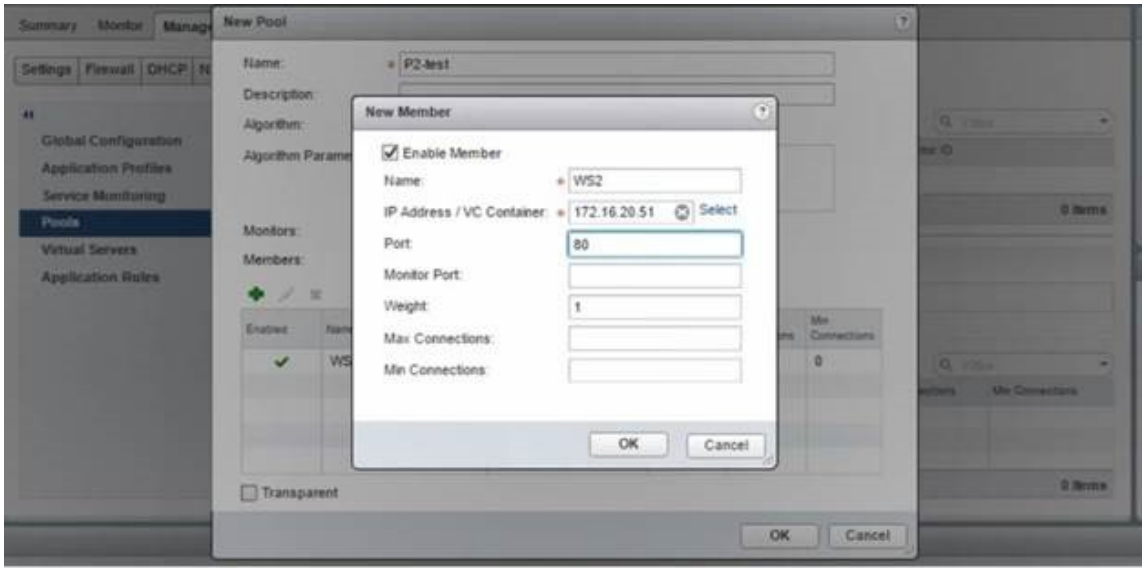
   d) Membres - Cliquez sur « + » pour ajouter des membres au pool et entrez les paramètres requis dans la fenêtre Nouveau membre.

      i. Nom : nom du membre

      ii. Adresse IP/conteneur VC - Cliquez sur Sélectionner pour sélectionner l'objet dans la liste disponible ou entrez l'adresse IP de l'objet.

2. Cliquez sur **OK**.

   Ajoutez autant de membres que nécessaire.



Création de serveurs virtuels

Créez un ensemble de serveurs virtuels et attribuez un pool à chaque serveur virtuel.

1. Cliquez sur **Gérer**, puis sur l'onglet Équilibreur de charge, sélectionnez **Serveurs virtuels**, puis cliquez sur l'icône "**+**"pour ajouter un serveur virtuel et définissez les paramètres suivants :

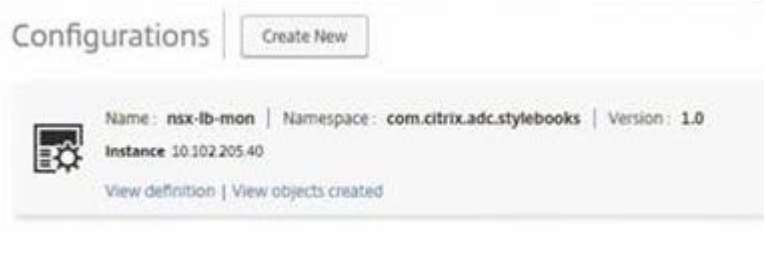
   a) Profil d'application : par défaut, le profil de service que vous avez créé dans Citrix ADM s'affiche.

b) Name : nom du serveur virtuel.

c) Adresse IP : cliquez sur Sélectionner pour sélectionner un pool d'adresses IP existant ou créer un nouveau pool d'adresses IP.

d) Pool par défaut : sélectionnez le pool par défaut dans la liste déroulante.

2. Cliquez sur **OK**.
3. Dans Citrix ADM, accédez à **Orchestration** > **Demandes** pour afficher les détails de l'avancement de la création de service sur une ou plusieurs instances Citrix ADC sélectionnées.
4. Dans Citrix ADM, accédez à **Applications** > **Configuration**et vérifiez que le pack de `nsx-lb-mon` configuration a été créé.



Configuration des services d'équilibrage de charge sur Citrix ADC VPX dans l'interface graphique Citrix ADM

Déployez des configurations d'équilibrage de charge sur l'instance Citrix ADC à l'aide de Citrix ADM StyleBooks. Pour HA, la configuration est déployée sur les deux instances Citrix ADC qui sont en HA.

Pour créer des packs de configuration via StyleBooks :

1. Dans Citrix ADM, accédez à **Applications** > **Configuration** > **Créer un nouveau**, puis sélectionnez le **StyleBook HTTP/SSL LoadBalancing (with Monitors)** dans la liste. Le StyleBook s'ouvre en tant que page d'interface utilisateur sur laquelle vous entrez les valeurs de tous les paramètres définis dans ce StyleBook.
2. Spécifiez des valeurs pour tous les paramètres requis.
3. Sélectionnez l'instance Citrix ADC VPX cible qui est provisionnée dans l'environnement NSX, puis cliquez sur **Créer** pour appliquer la configuration sur le périphérique sélectionné. Pour le déploiement HA, sélectionnez les instances en mode HA.

Vérification de la création de serveurs virtuels et de groupes de services dans les instances Citrix ADC VPX

Vous pouvez afficher que les groupes de services et les serveurs virtuels sont créés en vous connectant à l'instance Citrix ADC VPX.

Pour afficher les groupes de services et les serveurs virtuels :

1. Ouvrez une session sur l'instance Citrix ADC VPX. Pour le déploiement HA, vous devez ouvrir une session sur les deux instances Citrix ADC qui sont en HA.
2. Accédez à **Configuration** > **Système** > **Mise en réseau**. Dans le volet droit, vous pouvez voir les adresses IP ajoutées. Cliquez sur le lien hypertexte de l'adresse IP pour afficher les détails. Vous pouvez constater que l'adresse IP du sous-réseau est identique à l'adresse IP de l'interface Web ajoutée dans NSX.
3. Accédez ensuite à **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** et affichez les détails du serveur virtuel.
4. Accédez ensuite à **Groupes de services et affichez** les détails des groupes de services.
5. Enfin, accédez à **Configuration** > **Système** > **Licences** pour afficher les licences appliquées à cette instance.

Suppression des services d'équilibrage de charge

Lorsque les services d'équilibrage de charge ne sont plus requis sur les instances Citrix ADC VPX déployées sur le gestionnaire NSX, vous pouvez supprimer les insertions de service effectuées précédemment.

Pour supprimer la configuration et l'insertion de service :

1. Dans Citrix ADM, accédez à **Applications** > **Configuration**, sélectionnez la configuration de l'application créée, puis supprimez la configuration en cliquant sur l'icône « X ».
2. Dans NSX Manager, accédez à la Gateway périphérique à laquelle l'instance Citrix ADC VPX est connectée. Accédez à **Gérer** > **Équilibreur de chargeConfiguration globale**, cliquez avec le bouton droit sur l'entrée d'exécution, puis cliquez sur**Déprovisionner**. La machine virtuelle est rendue hors service.
3. Dans Citrix ADM, accédez à **Orchestration** > **Cloud Orchestration** > **Edge Gateways**. Assurez-vous qu'il n'existe pas de mappage respectif de la passerelle Edge à l'instance supprimée

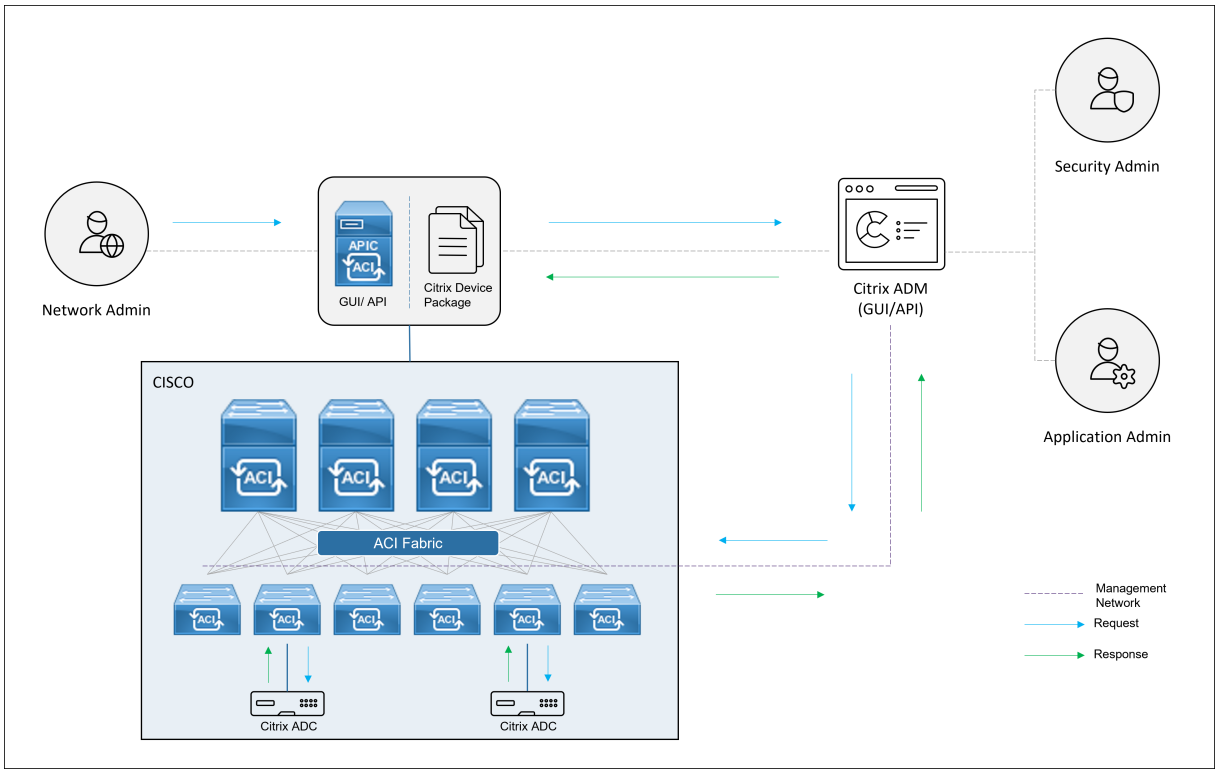
Automatisation Citrix ADC à l'aide de Citrix ADM en mode hybride ACI Cisco

February 1, 2024

Cisco ACI a introduit la prise en charge du mode hybride dans la version 1.3 (2f). En mode hybride, vous pouvez automatiser le réseau via l'Application Policy Infrastructure Controller (APIC), tout en déléguant la configuration L4-L7 à Citrix Application Delivery Management (ADM), qui agit en tant que gestionnaire de périphériques dans l'APIC.

La solution Citrix ADC Hybrid Mode est prise en charge par un package de périphériques en mode hybride et Citrix ADM. Vous devez télécharger le package de périphérique en mode hybride dans l'APIC. Ce package fournit toutes les entités configurables réseau L2-L3 à partir de Citrix ADC. La parité des applications est mappée par StyleBook de Citrix ADM à l'APIC. En d'autres termes, StyleBook sert de référence entre les configurations L2-L3 et L4-L7 pour une application donnée. Vous devez fournir un nom StyleBook lors de la configuration des entités réseau à partir de l'APIC pour Citrix ADC.

L'illustration suivante fournit une vue d'ensemble de Citrix ADC dans une solution en mode hybride :



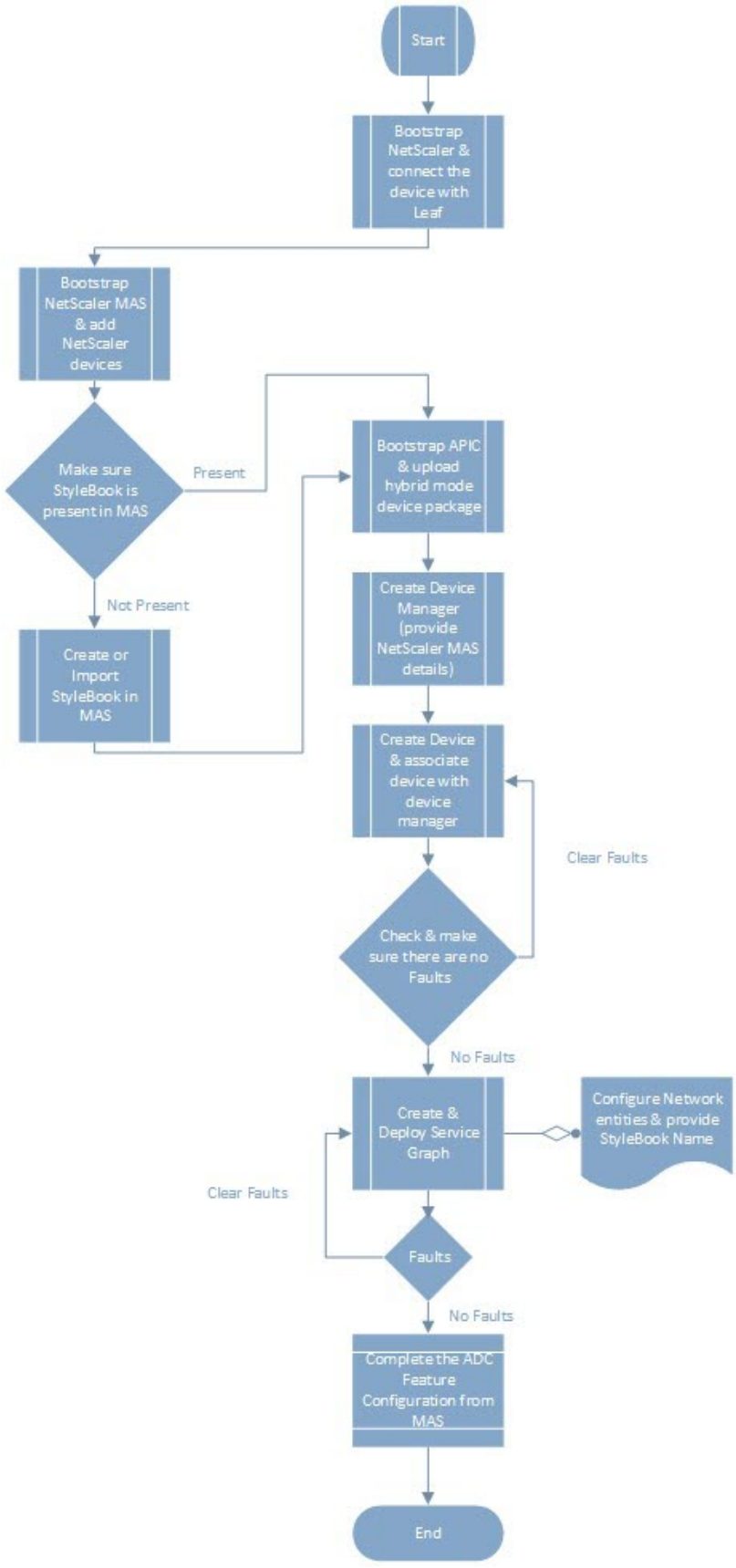
En mode hybride, la configuration de Citrix ADC est effectuée dans les deux phases suivantes :

1. L'assemblage du réseau est effectué à partir du Cisco APIC

2. La configuration est effectuée à partir de Citrix ADM

Pour toute application donnée, un administrateur réseau doit fournir des détails spécifiques au réseau, tels que les adresses IP, le port, le VLAN (automatisé), etc., dans le cadre de la création et du déploiement du graphique de service dans l'APIC Cisco. Ces détails de configuration sont ensuite transmis à Citrix ADM via le package de l'appareil, et Citrix ADM les traite en interne et configure le Citrix ADC. Un administrateur d'application crée la configuration liée à l'ADC de l'application à l'aide de StyleBook dans Citrix ADM, puis ces configurations sont transmises de Citrix ADM vers Citrix ADC. Le Cisco APIC et le Citrix ADM communiquent avec l'ADC via le réseau de gestion.

Le diagramme suivant montre un flux de travail Citrix ADC dans la solution hybride :



Conditions préalables

February 1, 2024

Assurez-vous que :

- Vous avez une connaissance conceptuelle des composants Cisco ACI et des Citrix ADC.
  - Pour plus d'informations sur Cisco ACI et ses composants, consultez la documentation produit à l'adresse suivante :http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.
  - Pour plus d'informations sur les Citrix ADC, consultez la documentation produit Citrix ADC à l'adresse :http://docs.citrix.com/.
- Tous les composants requis de Cisco ACI, y compris un Cisco APIC dans le centre de données, sont configurés et configurés. Pour plus d'informations sur Cisco ACI et ses composants, consultez la documentation produit à l'adresse suivante :http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.
- Vous avez installé Citrix ADC 11.1 ou version ultérieure.
- Vous avez configuré les Citrix ADC dans Cisco ACI afin qu'ils puissent être gérés à l'aide de l'APIC Cisco.
- Vous avez déployé Citrix Application Delivery Management (ADM) dans votre environnement. Pour de plus amples informations, consultez Citrix ADM 13.0.
- La connectivité de gestion d'APIC à Citrix ADM et ADC est établie.
- Prenez note de :
  - Interfaces de connexion et adresses IP utilisées pour la gestion et la connectivité des chemins de données.
  - Détails du commutateur Leaf-switch : adresses IP Citrix ADC, ports, interfaces, etc.

> **Remarque**
>
> Dans cette version, la solution en mode hybride prend en charge Citrix ADC dans un contexte unique, c'est-à-dire que les partitions d'administration ne sont pas prises en charge.

Configurer Citrix ADC en mode hybride à l'aide de Cisco APIC et Citrix ADM

February 1, 2024

Effectuez les tâches suivantes pour configurer un Citrix ADC en mode hybride à l'aide de Cisco APIC et de Citrix Application Delivery Management (ADM) :

1. Ajoutez des instances Citrix ADC dans votre structure à Citrix ADM. Pour obtenir des instructions, consultez la section Ajout d'une instance à Citrix ADM.
2. Utilisez Citrix ADM pour créer un StyleBook pour l'application. Pour obtenir des instructions, consultez Création d'un StyleBook pour l'application à l'aide de Citrix ADM.
3. Importez le package de périphériques en mode hybride Citrix ADC dans Cisco APIC. Pour obtenir des instructions, reportez-vous à la section Importation du package de périphériques en mode hybride Citrix ADC dans Cisco APIC
4. Ajoutez Citrix ADM en tant que gestionnaire de périphériques dans l'APIC Cisco. Pour obtenir des instructions, reportez-vous à la section Ajout de Citrix ADM en tant que gestionnaire de périphériques dans Cisco APIC
5. Utilisez Cisco APIC pour ajouter un périphérique Citrix ADC dans Cisco ACI. Pour obtenir des instructions, reportez-vous à la section Ajout de Citrix ADC en tant que périphérique dans Cisco ACI
6. Créez et déployez un modèle de graphe de service. Pour obtenir des instructions, consultez Création et déploiement d'un graphique de service
7. Configurez les paramètres L4-L7 à l'aide de StyleBook dans Citrix ADM. Pour obtenir des instructions, voir Configurer le paramètre L4-L7 à l'aide de StyleBook à partir de Citrix ADM
8. Attacher ou détacher les événements de point de terminaison de l'APIC Cisco. Pour plus d'informations, consultez Attachement ou détachement d'événements de point de terminaison d'APIC

Créer un StyleBook pour une application à l'aide de Citrix ADM

February 1, 2024

Un StyleBook est un modèle de configuration que vous pouvez utiliser pour créer et gérer des configurations Citrix ADC pour n'importe quelle application. Vous pouvez créer un StyleBook pour configurer

une fonctionnalité Citrix ADC spécifique, telle que l'équilibrage de charge, le déchargement SSL ou la commutation de contenu. Vous pouvez concevoir un StyleBook pour créer des configurations pour un déploiement d'application d'entreprise tel que Microsoft Exchange ou Lync. Pour plus d'informations, consultez StyleBooks.

Vous pouvez créer votre propre StyleBook pour votre application ou modifier et utiliser l'APIC-HTTP-LB StyleBook fourni avec Citrix Application Delivery Management (ADM).

Pour créer votre propre StyleBook pour votre application dans Citrix ADM, consultez Comment créer vos propres StyleBooks.

Lors de la création du StyleBook, assurez-vous de suivre le modèle de graphe de service de l'APIC dans le StyleBook. En d'autres termes, le graphique de service de l'APIC pour n'importe quelle application suit le modèle du consommateur et du fournisseur connectés via une fonction ADC. Le consommateur et le fournisseur sont représentés sous la forme d'un groupe terminal (EPG) et entretiennent une relation individuelle. Le même modèle doit également être suivi dans StyleBook, où le fournisseur EPG doit être représenté en tant que groupe de services et chaque point final en tant que membre du groupe de services. Le nœud de fonction ADC doit être représenté par un serveur virtuel (par exemple, un serveur virtuel d'équilibrage de charge) et il doit exister une relation 1:1 entre le serveur virtuel et le groupe de services.

Cela capture essentiellement l'essence du graphe de service et vous permet de gérer l'événement d'attachement ou de détachement depuis l'APIC, où un événement d'attachement lie le point final au groupe de services correspondant et un événement de détachement le dissocie. Vous devez vous assurer que le graphique de service et le StyleBook sont identiques pour une automatisation fluide des configurations réseau L2-L3 aux configurations L4-l7 dotées de fonctionnalités ADC.

Importer le package de périphériques en mode hybride Citrix ADC dans Cisco APIC

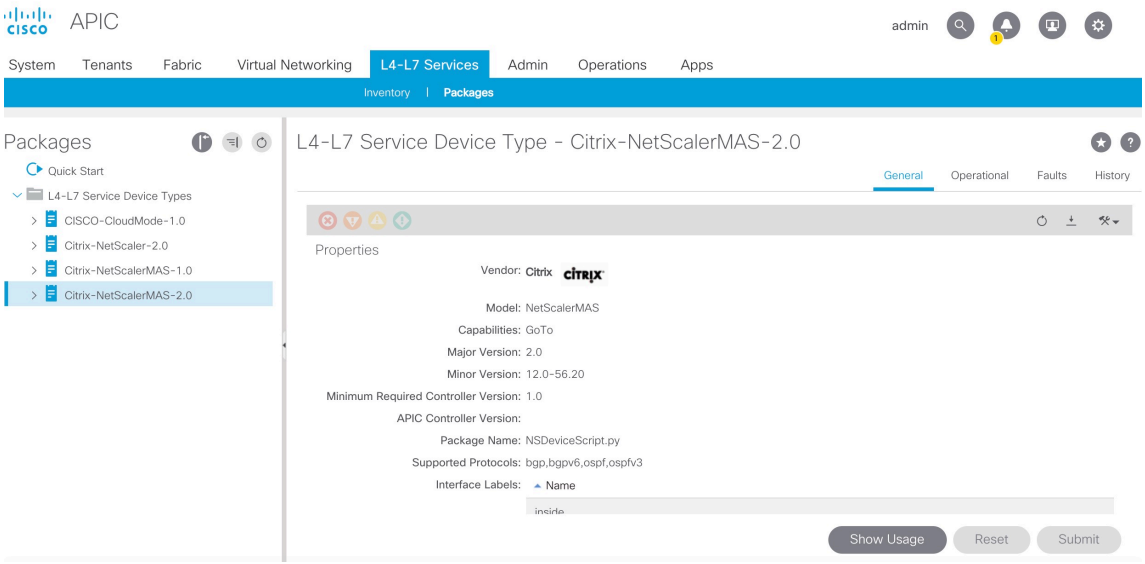
February 1, 2024

Le package de périphériques en mode hybride est un package léger comparé à un mode entièrement géré. Seuls les paramètres réseau L2-L3 sont disponibles via le modèle de périphérique. Le modèle de périphérique ne comporte qu'une seule fonction ADC générique définie, et quatre profils de fonctions basés sur le déploiement de Citrix ADC dans la structure (par exemple, un bras et deux bras et le même avec RHI). Le nom du package Périphérique en mode **hybride est NetScaler Hybrid Mode Device package 12.0 Build 56.20**. Recherchez le package d'appareils en mode hybride sur le site de téléchargement Citrix, téléchargez-le et importez le package d'appareils dans l'APIC.

> **Remarque**
>
> L'ensemble de dispositifs en mode hybride peut coexister avec un ensemble de dispositifs en mode entièrement géré.

Pour importer le package de périphériques en mode hybride dans l'APIC à l'aide de l'interface graphique APIC, procédez comme suit :

1. Dans la barre de menu, cliquez sur l'onglet **Services L4-L7** et sélectionnez le panneau **Packages**.
2. Dans le volet de **navigation**, cliquez avec le bouton droit sur **Types de périphériques L4-L7** et sélectionnez **Importer un package de périphériques**.
3. Dans la boîte de dialogue **Importer le package de périphériques**, cliquez sur **Parcourir** pour sélectionner le package de périphériques en mode hybride Citrix ADC téléchargé.
4. Cliquez sur **Envoyer**.
   Après avoir importé avec succès le package de périphériques dans l'APIC, dans le volet de **navigation**, vous pouvez afficher les détails du package de périphériques en cliquant sur le nom de l'appareil.



> **Important**
>
> Après avoir importé le package de l'appareil, assurez-vous que l'APIC ne présente aucun défaut. Vous pouvez afficher les défauts en cliquant sur l'onglet **Défauts** dans la fenêtre Types de périphériques.

Ajouter Citrix ADM en tant que gestionnaire de périphériques dans Cisco APIC

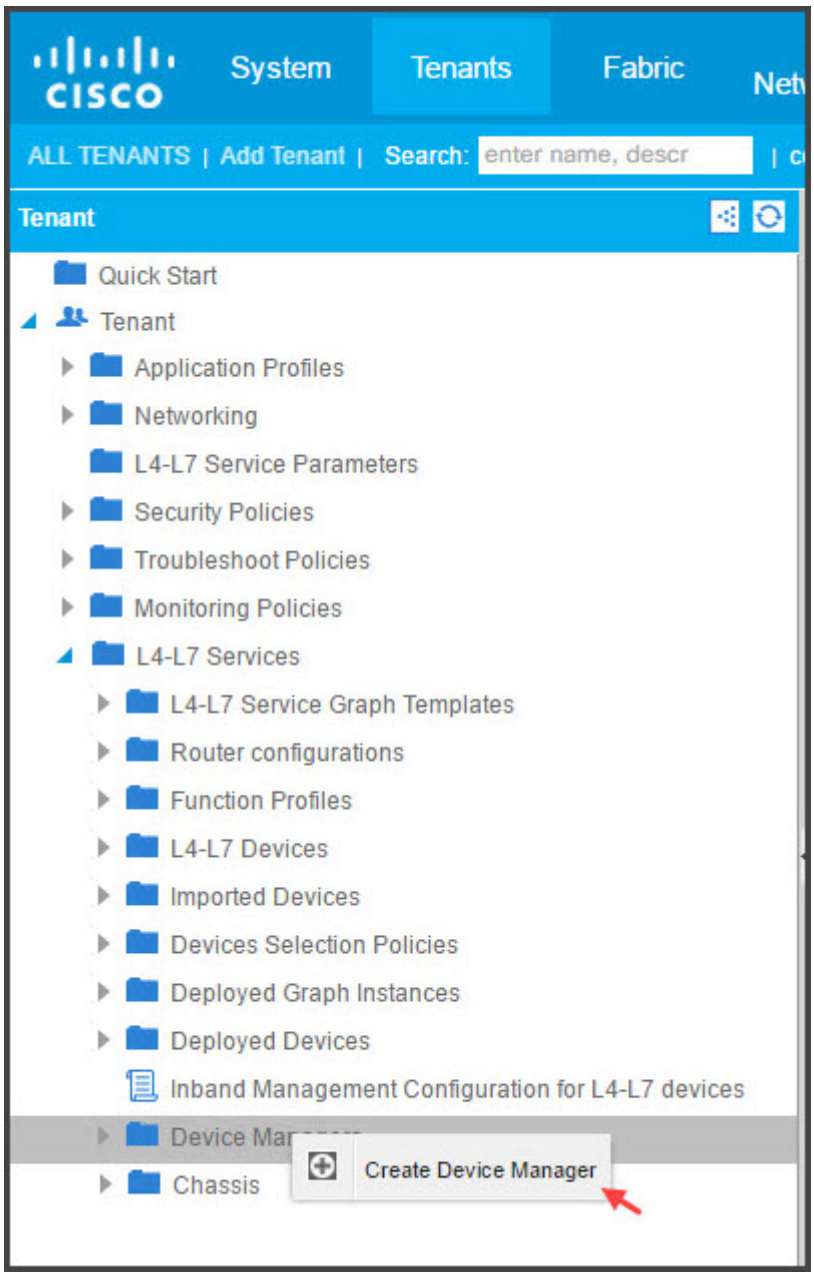
February 1, 2024

24 mai 2018

Citrix Application Delivery Management (ADM) agit en tant que gestionnaire de périphériques centralisé pour Citrix ADC déployé sur Cisco ACI. Vous devez ajouter Citrix ADM en tant que gestionnaire de périphériques dans l'APIC Cisco.

Pour ajouter Citrix ADM en tant que gestionnaire de périphériques dans l'APIC à l'aide de l'interface graphique APIC :

1. Dans la barre de menus, accédez à **Locataires > Tous les Locataires**.
2. Dans le volet **Travail**, double-cliquez sur le nom du locataire.
3. Dans le volet de **navigation**, sélectionnez ***tenant_name* > Services L4-L7**.
4. Cliquez avec le bouton droit sur **Gestionnaires de périphériques**, puis cliquez sur **Créer un gestionnaire de périphériques**.



5. Dans la boîte de dialogue **Créer le Gestionnaire de périphériques**, procédez comme suit :

   a) Dans le champ **Nom du Gestionnaire de périphériques**, entrez un nom pour le déploiement Citrix ADM que vous souhaitez enregistrer en tant que gestionnaire de périphériques.

   b) Dans la liste déroulante **Gestion EPG**, sélectionnez l'EPG de gestion.

   c) Dans la liste déroulante **Type de Gestionnaire de périphériques**, sélectionnez **Citrix-DevMGR-1.0**.

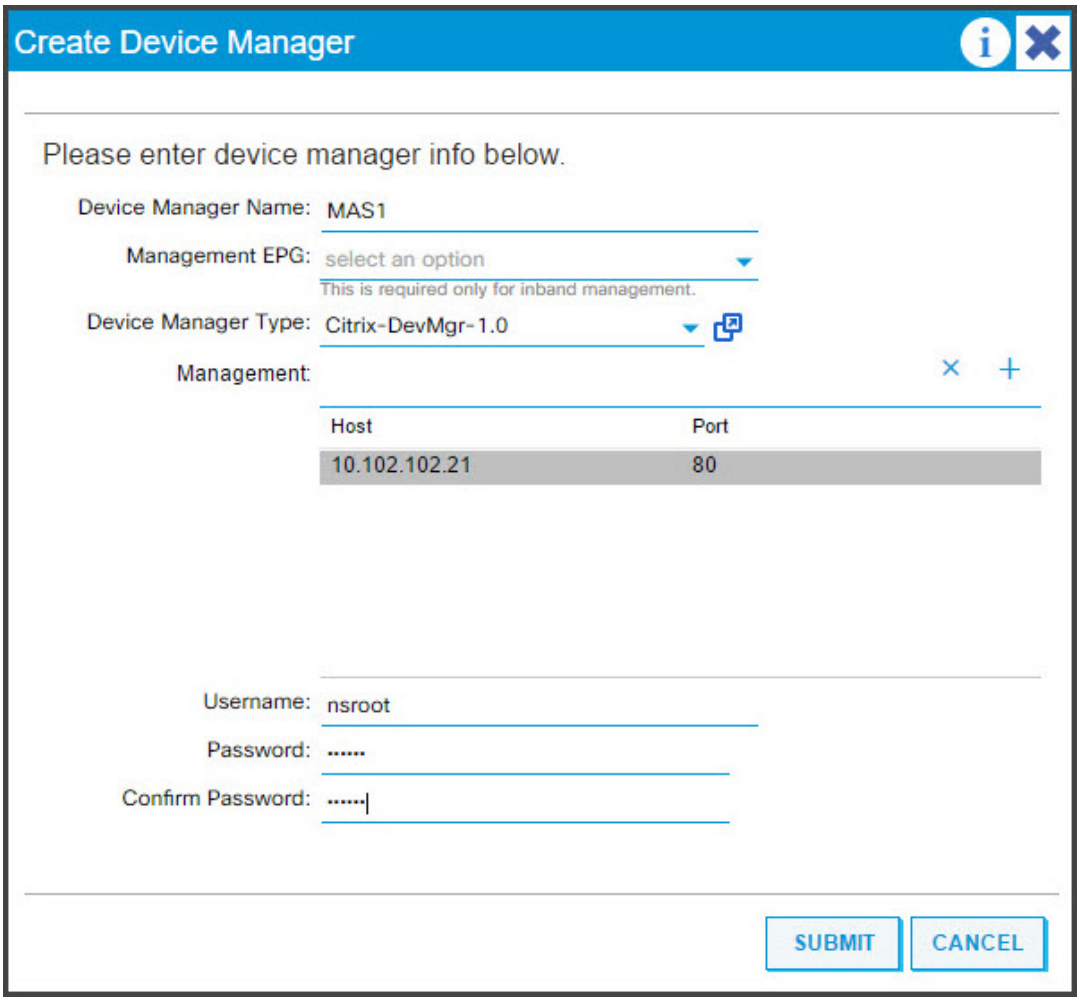
   d) Dans le champ **Gestion**, cliquez sur **+** et ajoutez les détails de l'adresse IP et du port du

déploiement Citrix ADM.

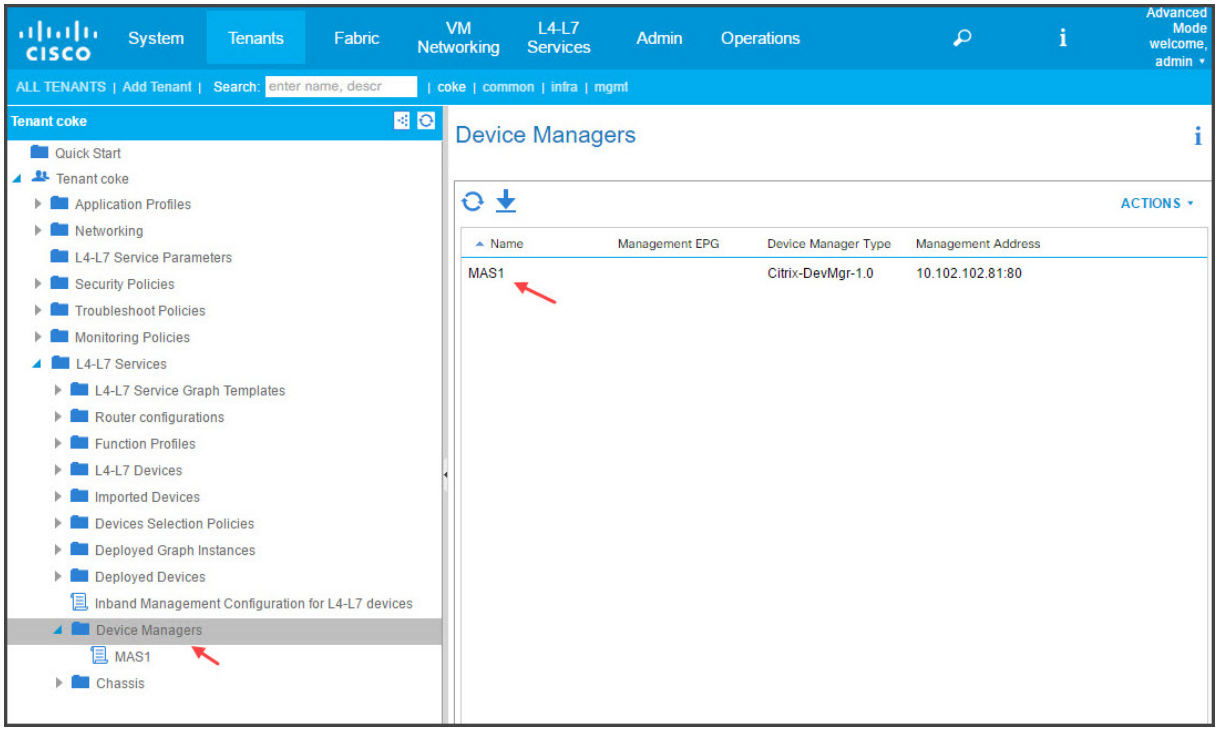
e) Dans le champ **Nom d'utilisateur**, entrez le nom d'utilisateur pour accéder à Citrix ADM.

f) Dans les champs **Mot de passe** et **Confirmer le mot** de passe, entrez le mot de passe pour accéder à Citrix ADM.

g) Cliquez sur **SUBMIT**.



Une fois que Citrix ADM est correctement enregistré en tant que gestionnaire de périphériques dans l'APIC, le gestionnaire de périphériques est ajouté et s'affiche dans le volet de **navigation**. Pour afficher le gestionnaire de périphériques enregistré, dans le volet de navigation, accédez à ***nom_tenant* > Services L4-L7 > Gestionnaire de périphériques**.



Remarque

Assurez-vous qu'il n'y a aucun problème de connectivité entre l'APIC Cisco et Citrix ADM et que vous fournissez les mêmes informations d'identification que vous utilisez pour accéder à Citrix ADM. Assurez-vous également que le compte dispose de privilèges d'administrateur.

Important

Après avoir importé le package de l'appareil, assurez-vous que l'APIC ne présente aucun défaut. Vous pouvez afficher les défauts en cliquant sur l'onglet **Défauts** dans la fenêtre Types de périphériques.

Vous pouvez également enregistrer Citrix ADM en tant que gestionnaire de périphériques à l'aide d'API. Voici un exemple de charge utile XML qui montre comment vous pouvez utiliser des API pour ajouter Citrix ADM en tant que gestionnaire de périphériques.

```
<polUni>
    <fvTenant name="coke">
        <vnsDevMgr name="MAS1">
            <vnsRsDevMgrToMDevMgr tDn="uni/infra/mDevMgr-Citrix-DevMgr-1.0" />
            <vnsCMgmts name="devMgmt" host="10.102.102.81" port="80"/>
            <vnsCCred name="username" value="nsroot"/>
            <vnsCCredSecret name="password" value="*****("/>
        </vnsDevMgr>
    </fvTenant>
</polUni>
```


Ajouter Citrix ADC en tant que périphérique dans Cisco ACI à l'aide d'APIC

February 1, 2024

Vous devez ajouter un Citrix ADC en tant que périphérique L4-L7 à l'APIC pour l'automatisation du réseau. L'APIC effectue l'assemblage réseau entre Leaf et le périphérique Citrix ADC, en fonction du graphique de service déployé. Vous devez configurer les paramètres de base de la configuration du périphérique, tels que les adresses IP de gestion de la configuration, le gestionnaire de périphériques et les informations d'identification.

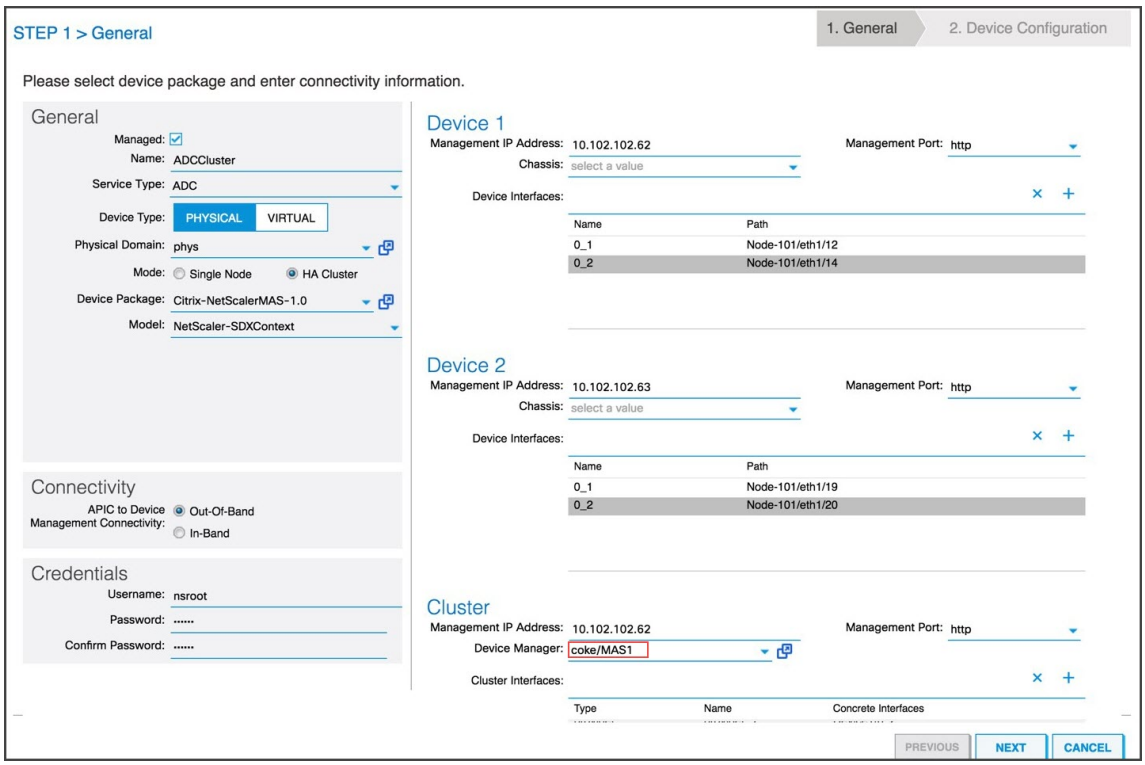
Pour enregistrer le Citrix ADC en tant que périphérique dans l'APIC à l'aide de l'interface graphique APIC :

1. Dans la barre de menus, accédez à **Locataires > Tous les Locataires**.
2. Dans le volet **Travail**, double-cliquez sur le nom du locataire.
3. Dans le volet de **navigation**, sélectionnez ***tenant_name* > Services L4-L7 > Appareils L4-L7**.
4. Dans le volet Travail, sélectionnez **Actions > Créer des périphériques L4-L7**.
5. Dans la boîte de dialogue **Créer des périphériques L4-L7**, dans la section **Général**, procédez comme suit :
    a) Cochez la case **Géré** .
    b) Dans le champ **Nom**, entrez le nom de l'appareil.
    c) Dans la liste déroulante **Type de service**, sélectionnez **ADC**.
    d) Dans le champ **Type de périphérique**, sélectionnez **Physique**.

    > **Remarque**
    >
    > Assurez-vous que pour VMware ESX, vous sélectionnez Virtual et associez le domaine Virtual Machine Manager (VMM) correspondant.

    e) Dans la liste déroulante **Domaine physique**, sélectionnez le domaine physique.
    f) Dans le champ **Mode**, sélectionnez **Nœud unique** ou **Cluster HA**, selon vos besoins.
    g) Dans la liste déroulante **Device Package**, sélectionnez **Citrix-NetScalerMAS-1.0**.
    h) Dans la liste déroulante **Modèle**, sélectionnez le modèle de périphérique. Par exemple, Citrix ADC-MPX ou Citrix ADC-VPX.
6. Dans la section **Connectivité**, sélectionnez **Out-Of-Bandou In-Band**dans le champ**Connectivity APIC to Device Management**, en fonction de la configuration de Citrix ADC dans la structure.

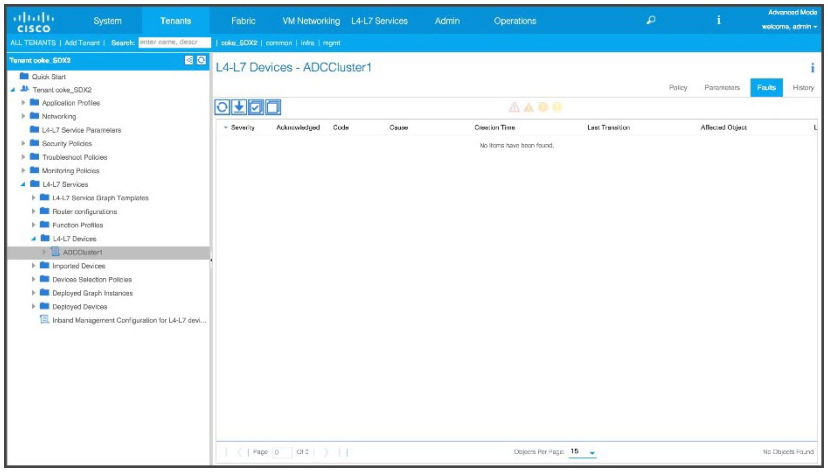
7. Dans la section **Informations d'identification**, spécifiez le nom d'utilisateur et le mot de passe pour l'accès au périphérique.
8. Dans les sections **Appareil 1** et **Appareil 2**, respectivement, terminez la configuration liée à la gestion.
9. Dans la section **Cluster**, complétez la configuration liée à la gestion du cluster. Assurez-vous que dans la liste déroulante **Device Manager**, vous sélectionnez le gestionnaire de périphériques que vous avez créé dans Ajout de Citrix ADM en tant que gestionnaire de périphériques dans Cisco APIC



10. Cliquez sur **SUIVANT**. La page Configuration de l'appareil s'affiche. Le package de périphériques en mode hybride ne fournit pas de détails de configuration spécifiques au périphérique et au cluster, tels que la haute disponibilité, les fonctionnalités et les modes d'activation/désactivation, la configuration pour NTP, SNMP, les alarmes SNMP, etc. Ces configurations doivent être effectuées à l'aide de Citrix ADM.
11. Cliquez sur **FINISH**. Lorsque vous avez correctement enregistré l'appareil dans l'APIC, l'appareil est ajouté et s'affiche dans le volet de navigation. Pour afficher l'appareil enregistré, dans le volet de navigation, accédez à ***tenant_name* > Services L4-L7 > Appareils L4-L7 > Device_name**.

> **Important**
>
> Après avoir enregistré l'appareil, assurez-vous que l'APIC ne présente aucun défaut. Vous

> pouvez afficher les défauts en cliquant sur l'onglet **Défauts** dans le volet de **travail** .



Vous pouvez également enregistrer un périphérique Citrix ADC à l'aide d'API. Voici un exemple de charge utile XML pour ajouter un périphérique L4-L7 :

```
<polUni>

    <fvTenant name="coke">

    <vnsLDevVipname="ADCCluster1"funcType="GoTo" svcType="ADC">

     <vnsRsMDevAtt tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0" />

     <vnsRsALDevToPhysDomP tDn="uni/phys-phys"/>

     <vnsCMgmt name="devMgmt"host="10.102.102.67"port="80"/>

     <vnsCCred name="username" value="nsroot"/>

     <vnsCCredSecret name="password" value="****"/>

     <vnsRsALDevToDevMgr tnVnsDevMgrName="MAS1"/>

     <vnsCDev name="ADC1" devCtxLbl="C1">

     <vnsCIf name="1_1">

     <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1
        /33]"/>

     </vnsCIf>

     <vnsCIf name="1_2">

     <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1
        /35]"/>

```



```
31        </vnsCIf>
32
33        <vnsCMgmt name="devMgmt" host="10.102.102.65" port="80"/>
34
35        <vnsCCred name="username" value="nsroot"/>
36
37        <vnsCCredSecret name="password" value="****"/>
38
39        </vnsCDev>
40
41        <vnsCDev name="ADC2" devCtxLbl="C1">
42
43        <vnsCIf name="1_1">
44
45        <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1
              /34]"/>
46
47        </vnsCIf>
48
49        <vnsCIf name="1_2">
50
51        <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1
              /36]"/>
52
53        </vnsCIf>
54
55        <vnsCMgmt name="devMgmt" host="10.102.102.66" port="80"/>
56
57        <vnsCCred name="username" value="nsroot"/>
58
59        <vnsCCredSecret name="password" value="****"/>
60
61        </vnsCDev>
62
63        <vnsLIf name="outside">
64
65        <vnsRsMetaIf tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/
              mIfLbl-outside"/>
66
67        <vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC1/
              cIf-1_1"/>
68
69        <vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC2/
              cIf-1_1"/>
70
71        </vnsLIf>
72
73        <vnsLIf name="inside">
74
75        <vnsRsMetaIf tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/
              mIfLbl-inside"/>
76
77        <vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC1/
```



```
            cIf-1_2"/>
78
79          <vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC2/
               cIf-1_2"/>
80
81          </vnsLIf>
82
83          </vnsLDevV
84
85          </fvTenant>
86
87          </polUni>
```

Créer et déployer un graphique de service

February 1, 2024

Vous devez utiliser des modèles de graphique de service Cisco APIC dans APIC pour créer et déployer les Citrix ADC. Assurez-vous d'utiliser le profil de fonction ADC lors de la création et du déploiement d'un graphique de service.

Une fois le graphique configuré dans l'APIC, l'APIC automatise la configuration des périphériques sur la base des définitions de fonctions, de la connectivité des périphériques à la structure et des entités configurées dans le cadre du déploiement du graphique. L'APIC automatise également la configuration réseau, telle que l'allocation de VLAN et sa liaison, dans le cadre de la création du graphe de service, et la configuration est supprimée une fois que vous supprimez le graphique de l'APIC.

Un graphe de service est représenté sous la forme de deux niveaux ou plus d'une application, la fonction de service appropriée étant insérée entre eux. Un graphe de service est inséré entre les EPG source et destination par un contrat.

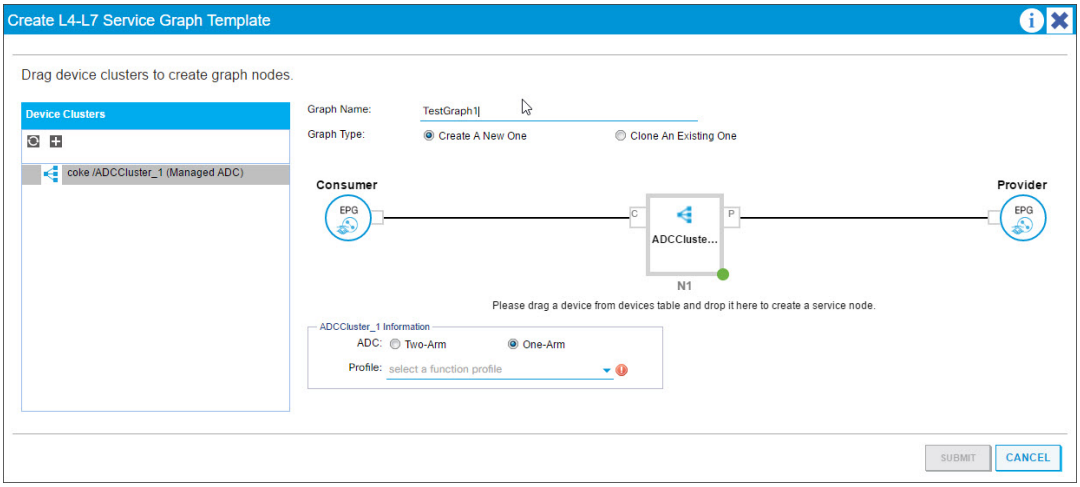
Pour créer un graphique de service à l'aide de l'interface graphique APIC, procédez comme suit :

1. Dans la barre de menus, accédez à **Locataires > Tous les Locataires**.
2. Dans le volet **Travail**, double-cliquez sur le nom du locataire.
3. Dans le volet de **navigation**, sélectionnez ***tenant_name* > L4-L7 Services > L4-L7 Service Graph Templates**.
4. Dans le volet **Travail**, sélectionnez **Actions > Créer un modèle de diagramme de service L4-L7**.
5. Dans la boîte de dialogue **Créer un modèle de graphe de service L4-L7**, dans la section Clusters de périphériques, sélectionnez un cluster de périphériques et procédez comme suit :

a) Dans le champ **Nom du graphique**, entrez le nom du modèle de graphe de service.

b) Dans le champ **Type de graphique**, sélectionnez **Créer un nouveau**graphique.

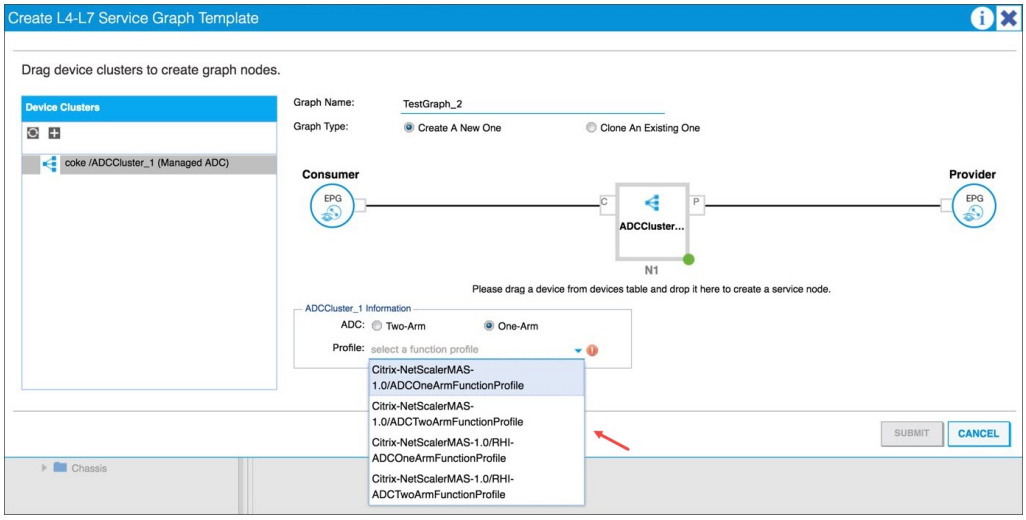
c) Dans la section **Device Cluster**, faites glisser l'appareil et déposez-le entre le groupe de points de terminaison du consommateur et le groupe de points de terminaison du fournisseur pour créer un nœud de service.



d) Dans la section <***L4-L7device_name information***>, procédez comme suit :

i. Dans le champ **ADC**, sélectionnez **un bras** ou **deux bras**, selon le mode de déploiement de l'Citrix ADC dans l'atelier.

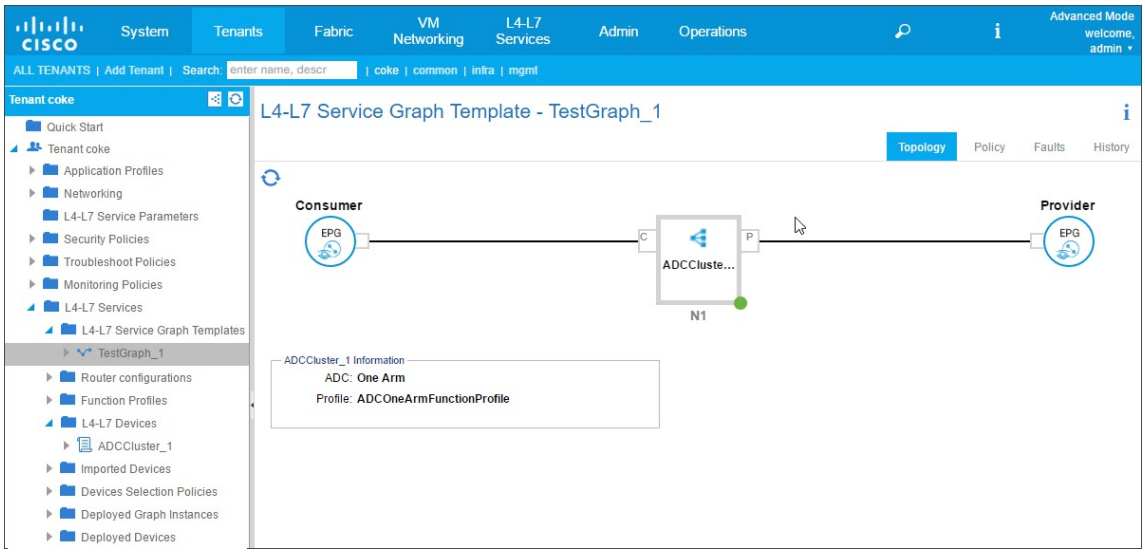
ii. Dans la liste déroulante **Profil**, sélectionnez le profil de fonction fourni dans le package de périphériques.



iii. Cliquez sur **SUBMIT**.

6. Dans le volet **de navigation**, cliquez sur le modèle de graphe de service. L'écran présente une topologie graphique du modèle de graphe de service.

> **Remarque**
>
> Le Cisco APIC prend en charge la notion de connecteurs, et ces connecteurs sont visibles dans le nœud ADCCluster. Les connecteurs définissent la direction du trafic réseau et le script de périphérique qui lie dynamiquement le VLAN alloué à une adresse IP virtuelle (VIP) ou IP de sous-réseau (SNIP), selon que la connexion est externe ou interne. Les VLAN sont également liés à des interfaces spécifiques utilisées pour le trafic entrant et sortant.

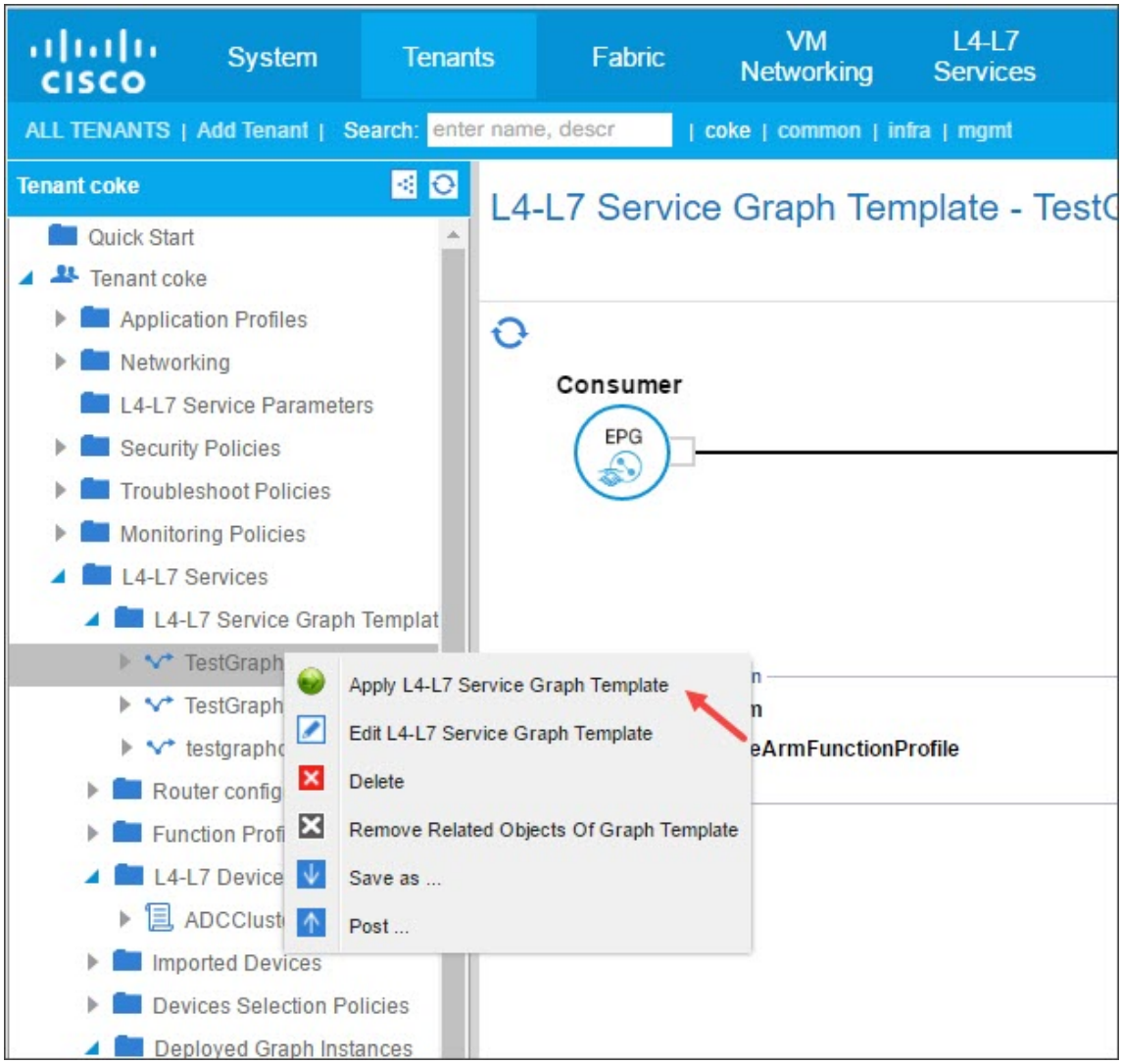


Application du modèle Service Graph aux groupes de points de terminaison

Après avoir créé le modèle de graphe de service, vous devez appliquer le modèle de graphique de service créé à l'aide de l'interface graphique APIC.

Pour appliquer le modèle de graphique des services, procédez comme suit :

1. Dans la barre de menus, accédez à **Locataires > Tous les Locataires**.
2. Dans le volet **Travail**, double-cliquez sur le nom du locataire.
3. Dans le volet de navigation, choisissez ***tenant_name* > L4-L7 Services > L4-L7 Service Graph Templates**.
4. Cliquez avec le bouton droit sur le ***template_name*** et cliquez sur **Appliquer le modèle de graphe de service L4-L7**.

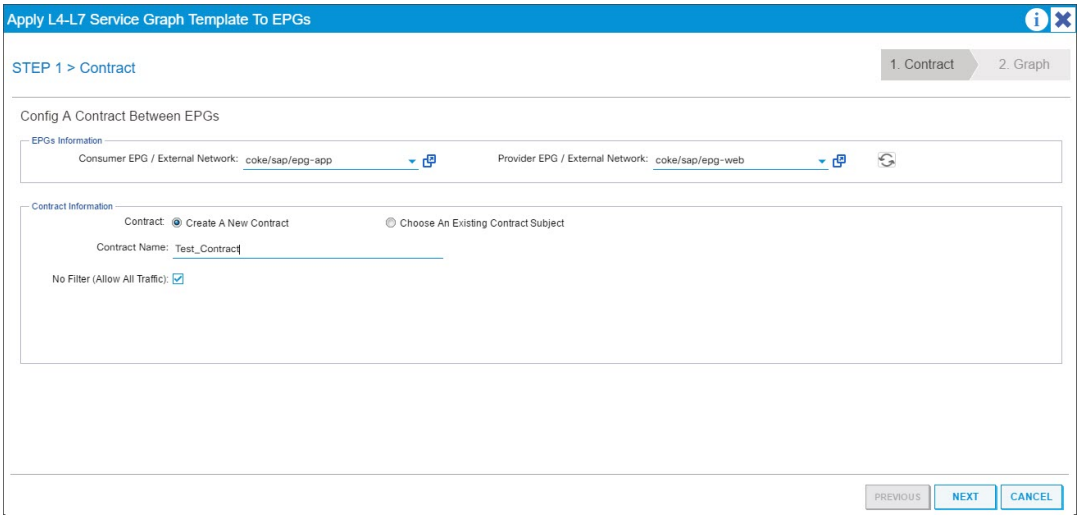


5. Dans la boîte de dialogue **Appliquer le modèle de graphe de service L4-L7 aux EPG**, dans la section **Informations EPG**, renseignez les champs suivants :

   a) Dans la liste déroulante **Consumer EPG/External Network**, sélectionnez le groupe de terminaux consommateurs.

   b) Dans la liste déroulante **Provider EPG/External Network**, sélectionnez le groupe de terminaux fourni.

   c) Dans la section **Informations sur le contrat**, renseignez les champs appropriés. Les informations du contrat sont spécifiques à l'APIC Cisco et sont configurées dans le cadre des stratégies de sécurité associées aux EPG.



d) Cliquez sur **Suivant**.

e) Dans la liste déroulante **Modèle de graphique**, sélectionnez le modèle de graphique de service que vous avez créé.

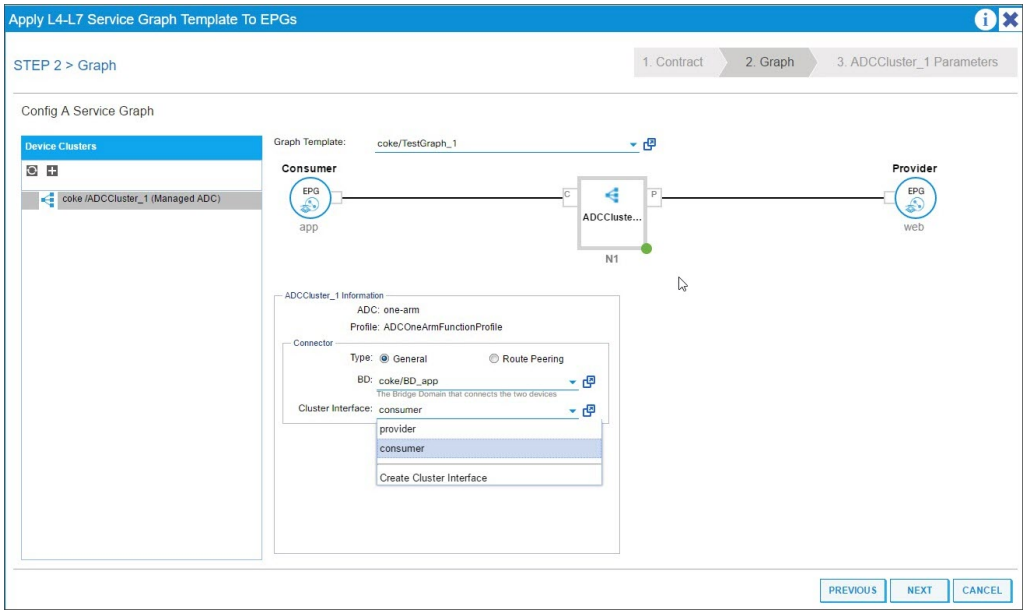
f) Dans la section **Connecteur**, procédez comme suit :

   i. Dans le champ **Type**, sélectionnez Général.

   ii. Dans la liste déroulante **BD**, sélectionnez le domaine du pont. Les détails du connecteur font partie du domaine de pont qui fait partie du modèle d'infrastructure Cisco APIC.

   iii. Dans la liste déroulante **Interface de cluster**, sélectionnez l'interface de cluster appropriée pour le domaine de pont sélectionné.

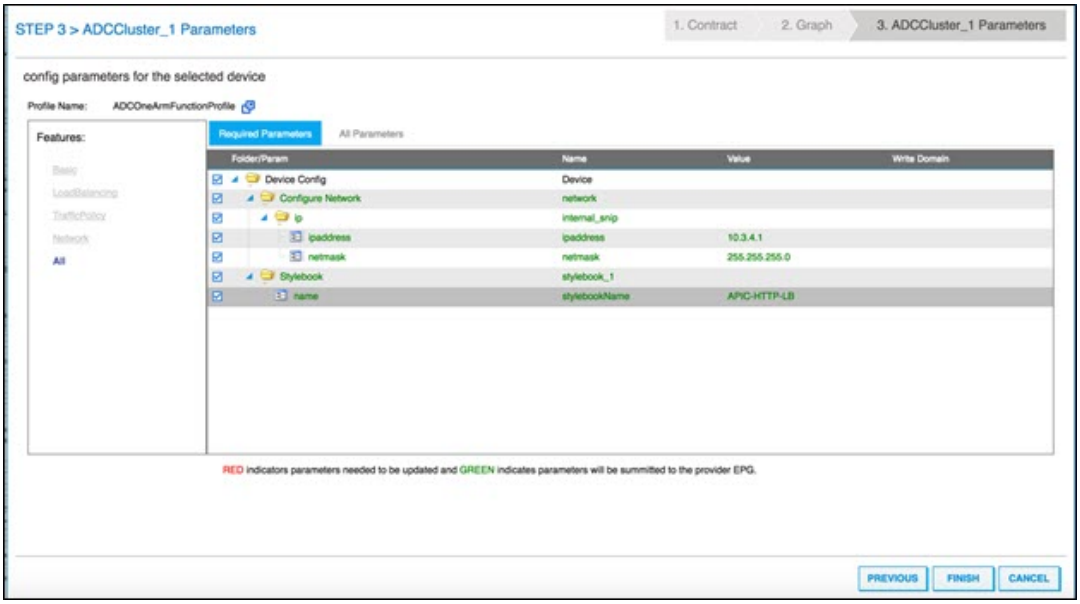
   L'APIC Cisco utilise les domaines de pont sélectionnés pour le trafic de chemin de données entre le périphérique Citrix ADC et la structure, comme requis par le modèle de graphe de service sélectionné.



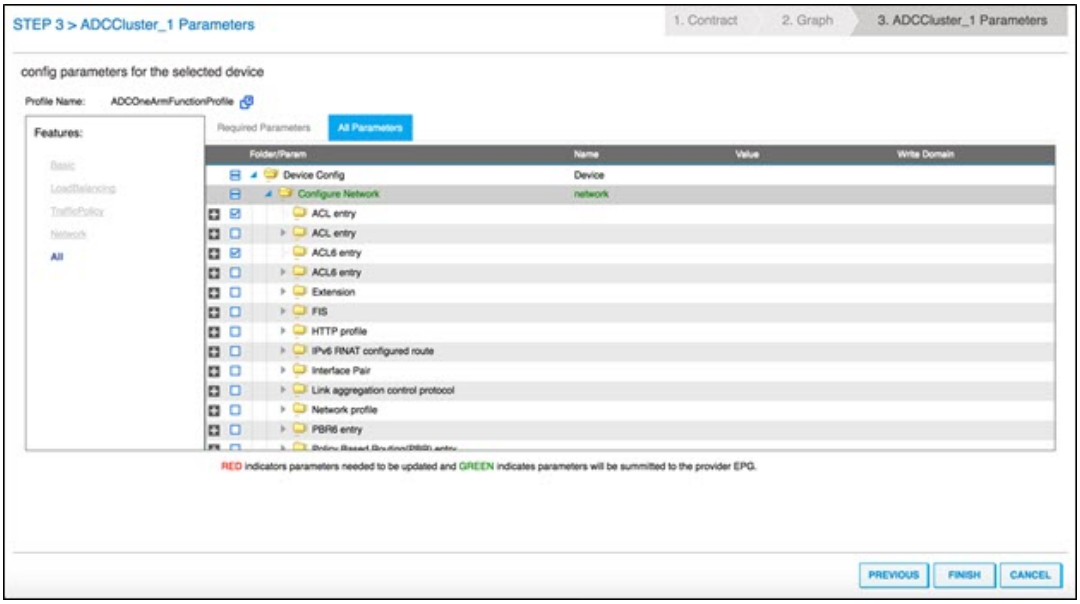
iv. Cliquez sur **Suivant**.

Sur l'écran **Paramètres**, dans l'onglet **Paramètres requis**, entrez les détails spécifiques à la L2-L3, tels que l'adresse IP requise par le profil. L'autre paramètre clé est le nom StyleBook. Il peut s'agir du StyleBook **APIC-HTTP-LB** intégré fourni dans Citrix Application Delivery Management (ADM), ou vous pouvez fournir le nom du StyleBook que vous avez créé dans Création d'un StyleBook pour l'application à l'aide de Citrix ADM

> **Remarque**
>
> Le nom StyleBook lie les détails du graphe de service à la configuration L4-L7 créée avec Citrix ADM pour une application donnée.



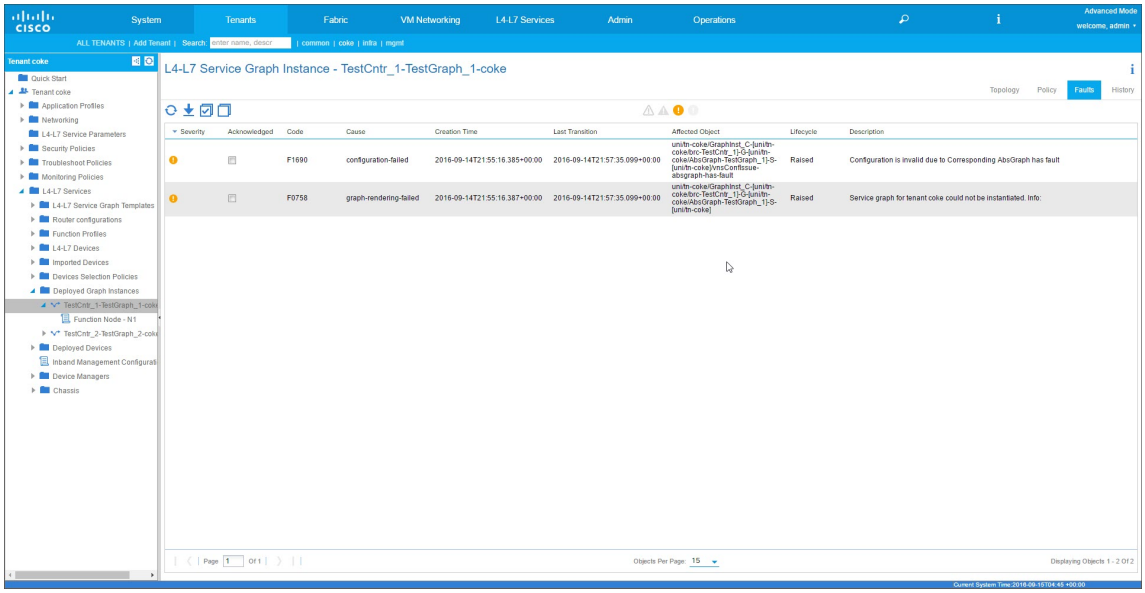
L'interface graphique Cisco APIC vous permet de filtrer les paramètres sur la base de fonctionnalités (par exemple, l'équilibrage de charge). Vous pouvez afficher et définir tous les paramètres obligatoires dans l'onglet **Paramètres requis**, et vous pouvez afficher et définir tous les autres paramètres liés à la fonctionnalité dans l'onglet **Tous les paramètres** .



> **Remarque**
>
> Par défaut, un profil à bras unique intégré nécessite que vous fournissiez des informations SNIP telles que l'adresse IP et le masque de réseau. Vous pouvez afficher d'autres paramètres réseau en cliquant sur **Tous les paramètres** et en développant l'arborescence **Configurer le réseau** dans l'interface graphique Cisco APIC. Cette liste répertorie tous les paramètres réseau pris en charge par Citrix ADC. Vous pouvez instancier n'importe quelle entité et fournir des valeurs pour les attributs répertoriés à partir de l'interface graphique Cisco APIC.

6. Cliquez sur **Terminer**.

> **Important**
>
> Après avoir appliqué le modèle de graphe de service, assurez-vous que le graphe déployé ne présente aucune erreur. Vous pouvez afficher les défauts en cliquant sur l'onglet **Défauts** dans le volet de **travail** .



Dans le cadre du déploiement Service Graph, le package de périphérique en mode hybride transmet les détails de configuration de l'APIC Cisco vers l'Citrix ADM. Citrix ADM traite en interne ces configurations vers l'Citrix ADC respectif et renvoie la réponse à l'APIC. Un déploiement de graphe réussi n'aura pas de problème, et le Citrix ADC est correctement mis en réseau avec la structure pour le graphique correspondant.

L'APIC prend en charge différentes façons de configurer et de déployer des graphiques à l'aide d'API, et le déploiement de graphiques inclut diverses dépendances sur certaines constructions spécifiques à APIC, telles que le locataire, le contrat, le VLAN et l'espace de noms.

L'exemple d'approche suivant illustre l'une des manières d'utiliser les API de l'APIC pour créer et déployer des graphes L4 à L7, en supposant que les artefacts spécifiques à l'APIC sont déjà configurés dans l'APIC.

> **Important**
>
> Assurez-vous d'utiliser ces charges utiles XML comme référence et d'apporter les modifications appropriées au code XML avant de les utiliser dans votre environnement.

Voici un exemple de création et de déploiement du graphe de service à l'aide d'API :

a) Créer un profil d'application

b) Créer les détails d'un graphique de service

c) Joindre le graphique de service à un contrat

Voici un exemple de charge utile XML pour créer un AppProfile. AppProfile contient des EPG, et le fournisseur EPG contient les entités spécifiques à Citrix ADC, les attributs et leurs valeurs. Dans l'exemple de charge utile XML suivant, les entités réseau spécifiques à Citrix ADC telles que le NSIP sont créées avec un ensemble d'attributs et un nom de StyleBook.


```
<polUni>
    <fvTenant name="coke">
        <!-- Application Profile -->
        <fvAp dn="uni/tn-coke/ap-sap" name="sap">
            <!-- EPG 1  -->
            <fvAEPg dn="uni/tn-coke/ap-sap/epg-web" name="web">
                <fvRsBd tnFvBDName="BD_web" />
                <!-- --------- CONFIG PAYLOAD ---------------- -->
                <vnsFolderInst ctrctNameOrLbl="Ctrct1" graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="Network" name="Network">
                    <vnsFolderInst ctrctNameOrLbl="Ctrct1" graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="nsip" name="snip1">
                        <vnsParamInst key="ipaddress" name="ip1" value="110.110.110.2"/>
                        <vnsParamInst key="netmask" name="netmask1" value="255.255.255.0"/>
                        <vnsParamInst key="type" name="tye" value="SNIP"/>
                        <vnsParamInst key="dynamicrouting" name="dynamicrouting" value="DISABLED"/>
                        <vnsParamInst key="hostroute" name="hostroute" value="DISABLED"/>
                    </vnsFolderInst>
                    <vnsFolderInst ctrctNameOrLbl="Ctrct1" graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="nsip" name="snip2">
                        <vnsParamInst key="ipaddress" name="ip2" value="220.220.220.2"/>
                        <vnsParamInst key="netmask" name="netmask2" value="255.255.255.0"/>
                        <vnsParamInst key="type" name="tye" value="SNIP"/>
                        <vnsParamInst key="dynamicrouting" name="dynamicrouting" value="DISABLED"/>
                        <vnsParamInst key="hostroute" name="hostroute" value="DISABLED"/>
                    </vnsFolderInst>
                </vnsFolderInst>
                <vnsFolderInst ctrctNameOrLbl="Ctrct1" graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="Stylebook" name="stylebook_1">
                    <vnsParamInst name="stylebookName" key="name" value="APIC-HTTP-LB"/>
                </vnsFolderInst>
                <vnsFolderInst ctrctNameOrLbl="Ctrct1" graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="internal_network" name="internal_network">
                    <vnsCfgRelInst name="internal_network_key" key="internal_network_key" targetName="Network/snip1"/>
                </vnsFolderInst>
                <vnsFolderInst ctrctNameOrLbl="Ctrct1"
```



```
        graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="
        external_network" name="external_network">
32                      <vnsCfgRelInst name="external_network_key" key
        ="external_network_key" targetName="Network/snip2"/>
33                  </vnsFolderInst>
34                  <vnsFolderInst ctrctNameOrLbl="Ctrct1"
        graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="mFCngStylebook
        " name="mFCngStylebook_1">
35                      <vnsCfgRelInst name="Stylebook_key" key="
        Stylebook_key" targetName="stylebook_1"/>
36                  </vnsFolderInst>
37                  <!-- ------- END CONFIG PAYLOAD -------------- -->
38                  <fvSubnet ip="110.110.110.110/24" scope="shared"/>
39                  <fvRsProv tnVzBrCPName="Ctrct1"></fvRsProv>
40                  <fvRsDomAtt tDn="uni/phys-sepg" />
41                  <fvRsPathAtt tDn="topology/pod-1/paths-101/pathep
        -[eth1/38]" encap="vlan-3703" instrImedcy="immediate"/>
42              </fvAEPg>
43              <!-- EPG 2 -->
44              <fvAEPg dn="uni/tn-coke/ap-sap/epg-app"  name="app">
45                  <fvRsCons tnVzBrCPName="Ctrct1"/>
46                  <fvRsBd tnFvBDName="BD_app" />
47                  <fvSubnet ip="220.220.220.220/24" scope="shared"/>
48                  <fvRsPathAtt tDn="topology/pod-1/paths-101/pathep
        -[eth1/37]" encap="vlan-3704" instrImedcy="immediate"/>
49                  <fvRsDomAtt tDn="uni/phys-sepg" />
50              </fvAEPg>
51          </fvAp>
52      </fvTenant>
53  </polUni>
54  <!--NeedCopy-->
```

Voici un exemple de charge utile XML pour créer des détails de graphe de service :

```
1   <polUni>
2       <fvTenant name="coke">
3           <vnsAbsGraph name = "Graph1">
4               <vnsAbsTermNodeProv name = "Input1">
5                   <vnsAbsTermConn name = "C1"></vnsAbsTermConn>
6               </vnsAbsTermNodeProv>
7               <vnsAbsNode name="ADC" funcType="GoTo">
8                   <vnsAbsFuncConn name = "outside" attNotify="true">
9                       <vnsRsMConnAtt tDn="uni/infra/mDev-Citrix-
        NetScalerMAS-1.0/mFunc-ADCFunction/mConn-external" />
10                  </vnsAbsFuncConn>
11                  <vnsAbsFuncConn name = "inside" attNotify="true">
12                      <vnsRsMConnAtt tDn="uni/infra/mDev-Citrix-
        NetScalerMAS-1.0/mFunc-ADCFunction/mConn-internal" />
13                  </vnsAbsFuncConn>
14                  <vnsRsNodeToMFunc tDn="uni/infra/mDev-Citrix-
        NetScalerMAS-1.0/mFunc-ADCFunction"/>
15                  <vnsRsDefaultScopeToTerm tDn="uni/tn-coke/AbsGraph
        -Graph1/AbsTermNodeProv-Input1/outtmnl"/>
```



```
                <vnsRsNodeToAbsFuncProf tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/absFuncProfContr/absFuncProfGrp-ADCOneArmServiceProfileGroup/absFuncProf-ADCOneArmFunctionProfile"/>
                <vnsRsNodeToLDev tDn="uni/tn-coke/lDevVip-ADCCluster1"/>
            </vnsAbsNode>
            <vnsAbsTermNodeCon name = "Output1">
                <vnsAbsTermConn name = "C6"></vnsAbsTermConn>
            </vnsAbsTermNodeCon>
            <vnsAbsConnection name = "CON1">
                <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph-Graph1/AbsTermNodeCon-Output1/AbsTConn" />
                <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph-Graph1/AbsNode-ADC/AbsFConn-outside" />
            </vnsAbsConnection>
            <vnsAbsConnection name = "CON2">
                <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph-Graph1/AbsNode-ADC/AbsFConn-inside" />
                <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph-Graph1/AbsTermNodeProv-Input1/AbsTConn" />
            </vnsAbsConnection>
        </vnsAbsGraph>
    </fvTenant>
</polUni>
<!--NeedCopy-->
```

Voici un exemple de charge utile XML pour attacher le graphique de service à un contrat :

```
<polUni>
    <fvTenant name="coke">
        <vzBrCP name="Ctrct1">
            <vzSubj name="http">
                <vzRsSubjGraphAtt tnVnsAbsGraphName="Graph1"/>
            </vzSubj>
        </vzBrCP>
    </fvTenant>
</polUni>
<!--NeedCopy-->
```

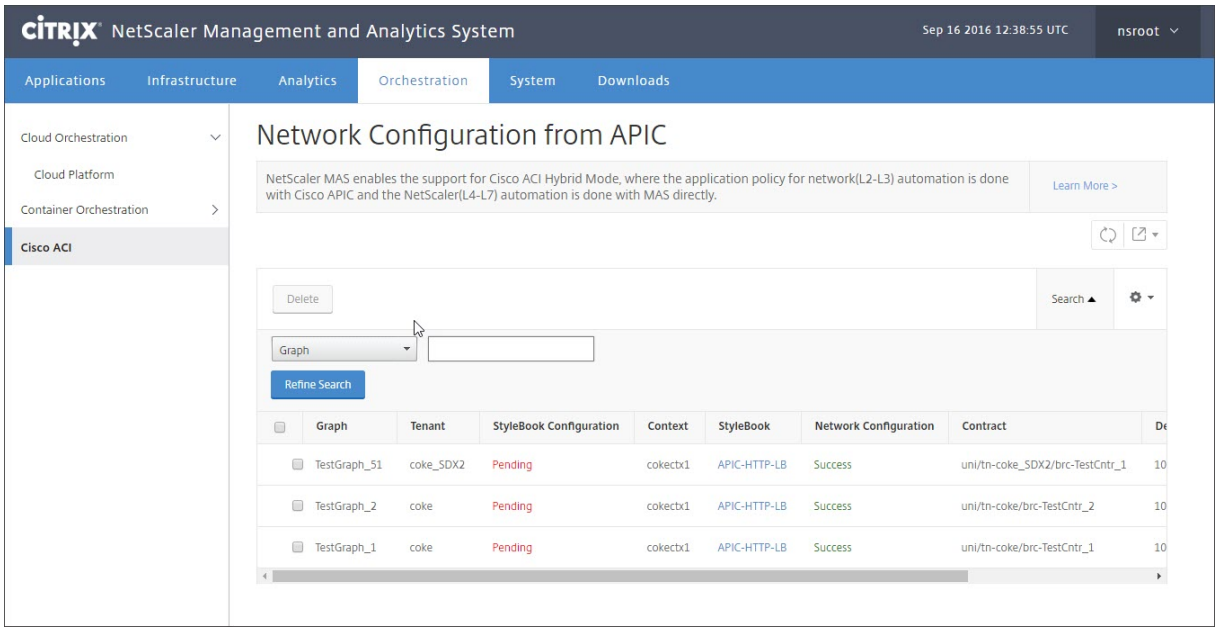
Configurer les paramètres L4-L7 à partir de Citrix ADM à l'aide de StyleBook

February 1, 2024

24 mai 2018

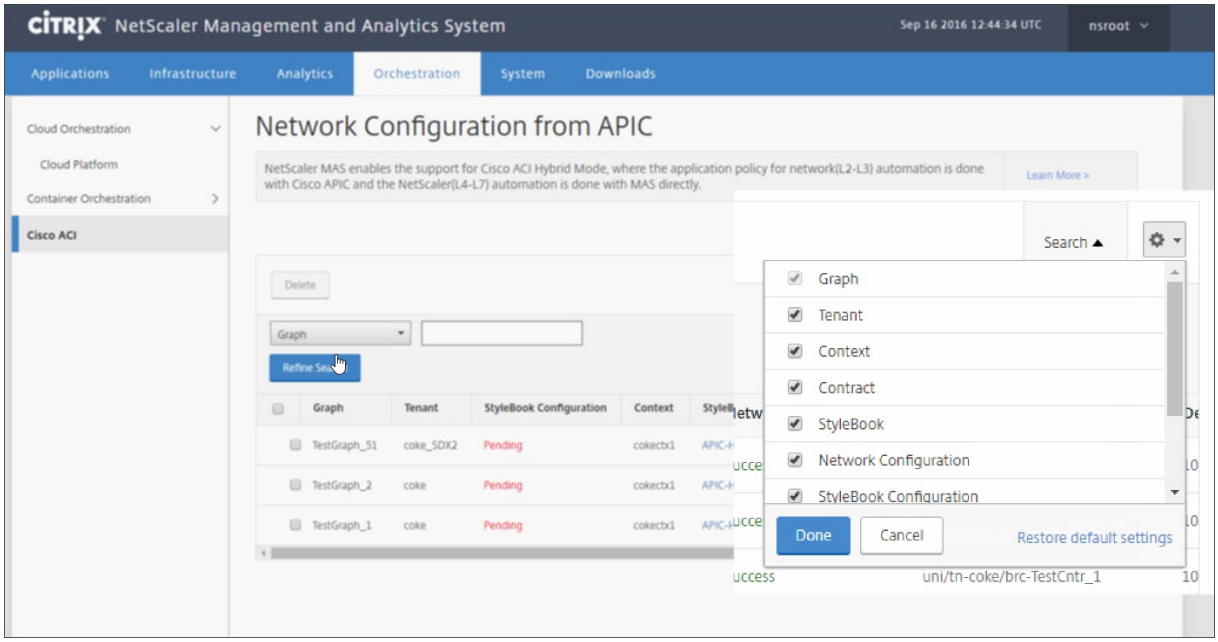
Dans Citrix Application Delivery Management (ADM), vous pouvez afficher les détails du graphique

de service déployé dans l'onglet **Orchestration**, sous **Cisco ACI**. La vue tabulaire affiche les détails du graphique de service tels que le nom du graphique, le nom du locataire, le contexte, le nom du StyleBook et l'état de la configuration du réseau.



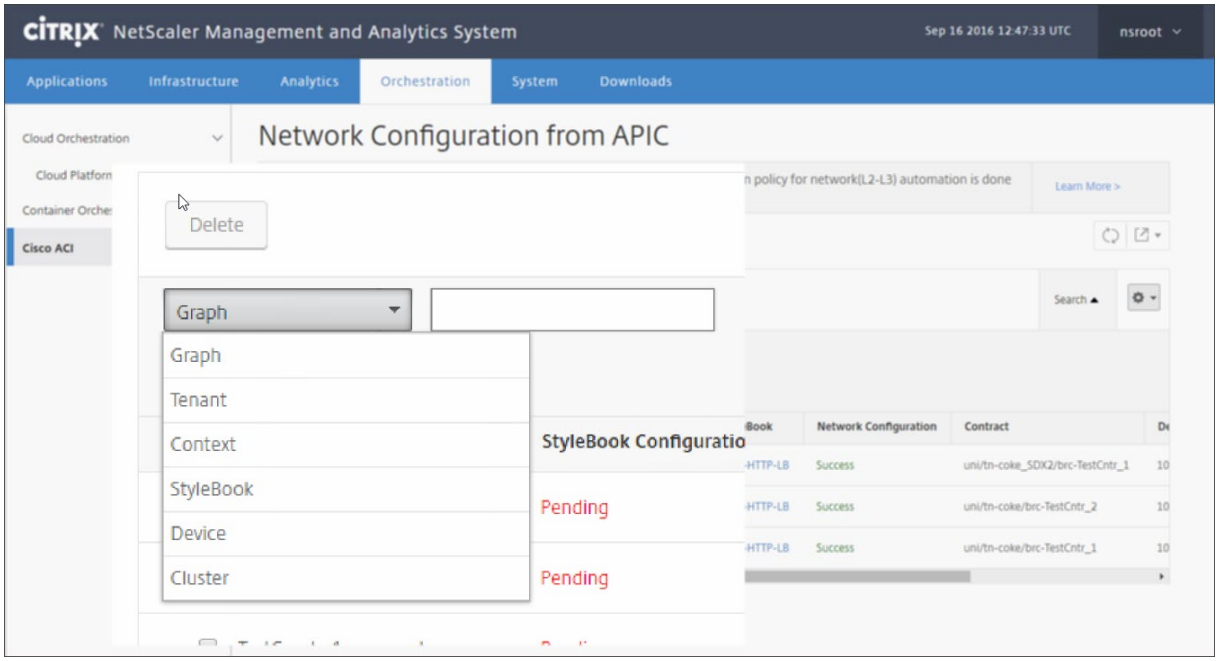
> **Remarque**
>
> Si le graphe est supprimé de l'APIC Cisco, la configuration correspondante est supprimée du périphérique, y compris la configuration L4-L7.

En outre, la vue tabulaire vous permet de trier n'importe quelle colonne affichée dans le tableau et de filtrer les données à l'aide de l'option Rechercher. Vous pouvez également personnaliser les détails des colonnes en sélectionnant ou en désélectionnant les noms des colonnes dans la liste déroulante :



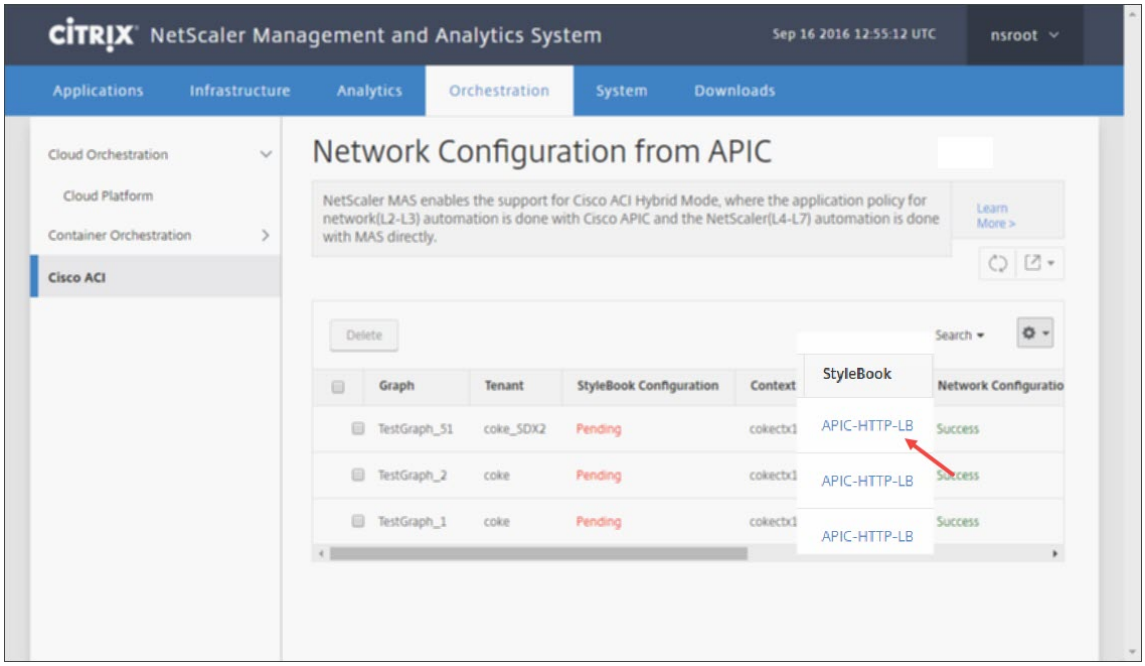
Vous pouvez également cliquer sur le bouton **Rechercher** et utiliser les options de recherche pour filtrer les données. Vous pouvez sélectionner n'importe quelle colonne dans la liste déroulante et saisir une valeur correspondante pour filtrer les données affichées dans le tableau.

> **Remarque**
>
> La fonctionnalité de recherche distingue les majuscules et minuscules et vous devez fournir les critères de recherche exacts.

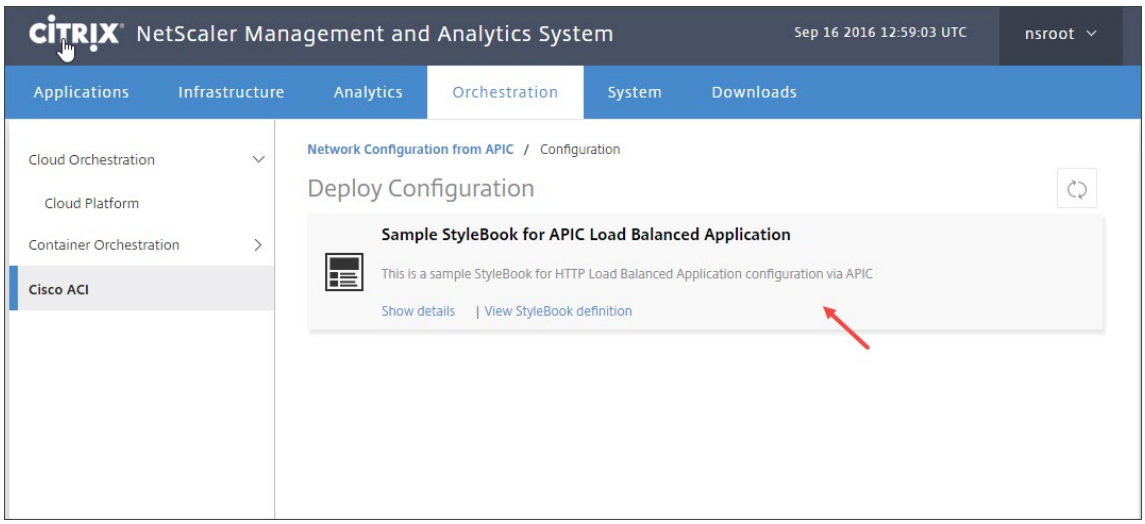


Pour déployer la configuration L4-L7 à l'aide de StyleBook dans Citrix ADM :

1. Cliquez sur le nom du StyleBook qui apparaît sous forme d'URL dans la vue tabulaire.



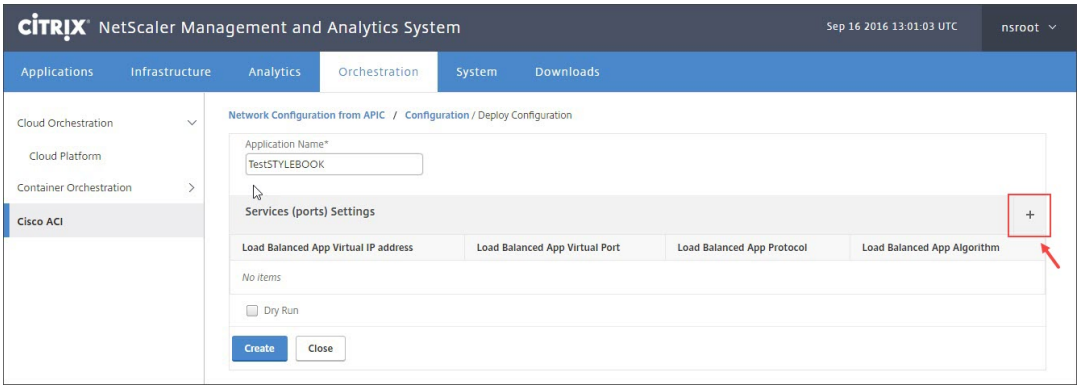
2. Dans la fenêtre Configuration, double-cliquez sur **StyleBook**.



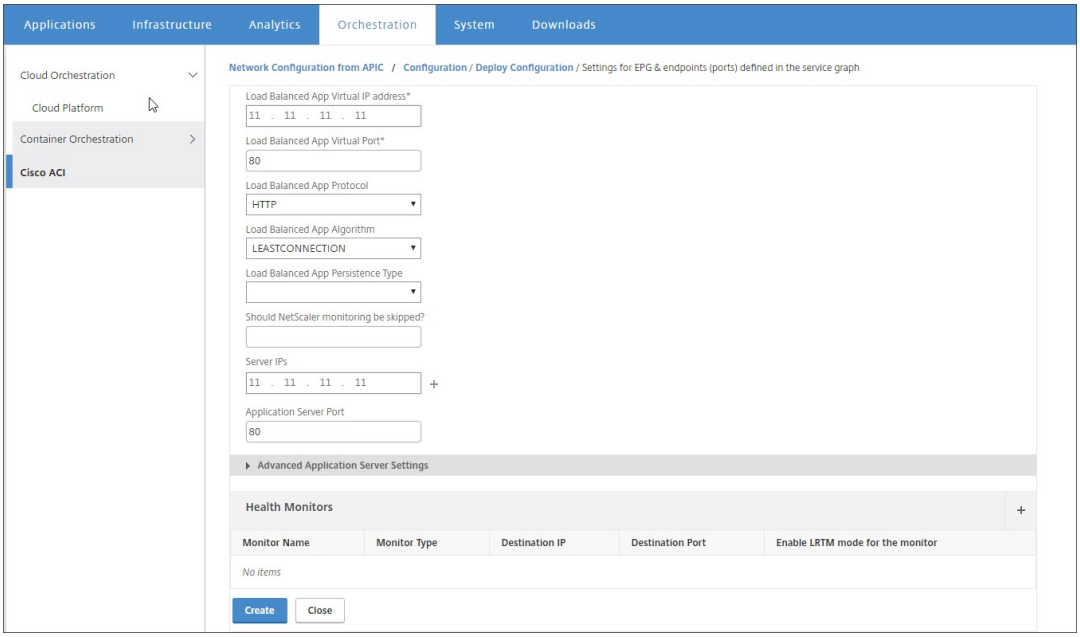
3. Dans la fenêtre Configuration du déploiement, procédez comme suit :

   a) Dans le champ **Nom de l'application**, entrez le nom de la configuration des fonctionnalités ADC qui correspond au graphe de service de l'application dans l'APIC.

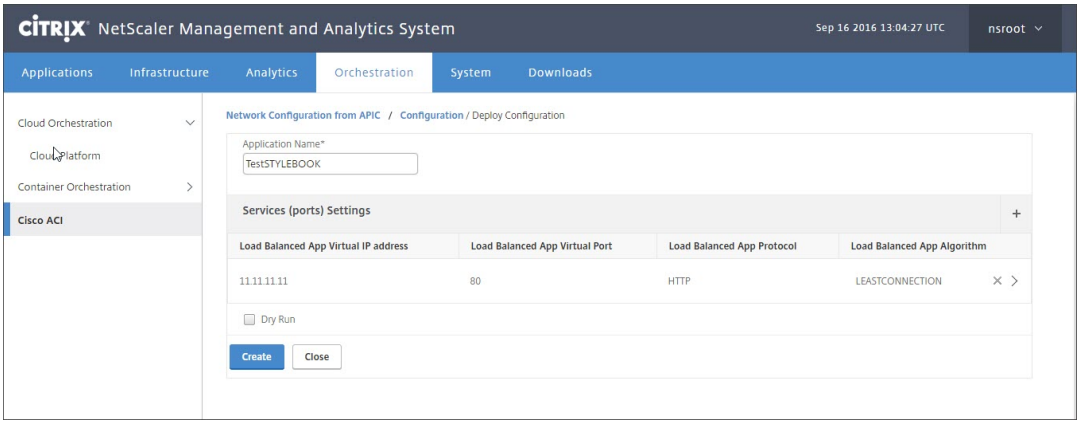
   b) Dans la section Paramètres du service (ports), cliquez sur **+**.



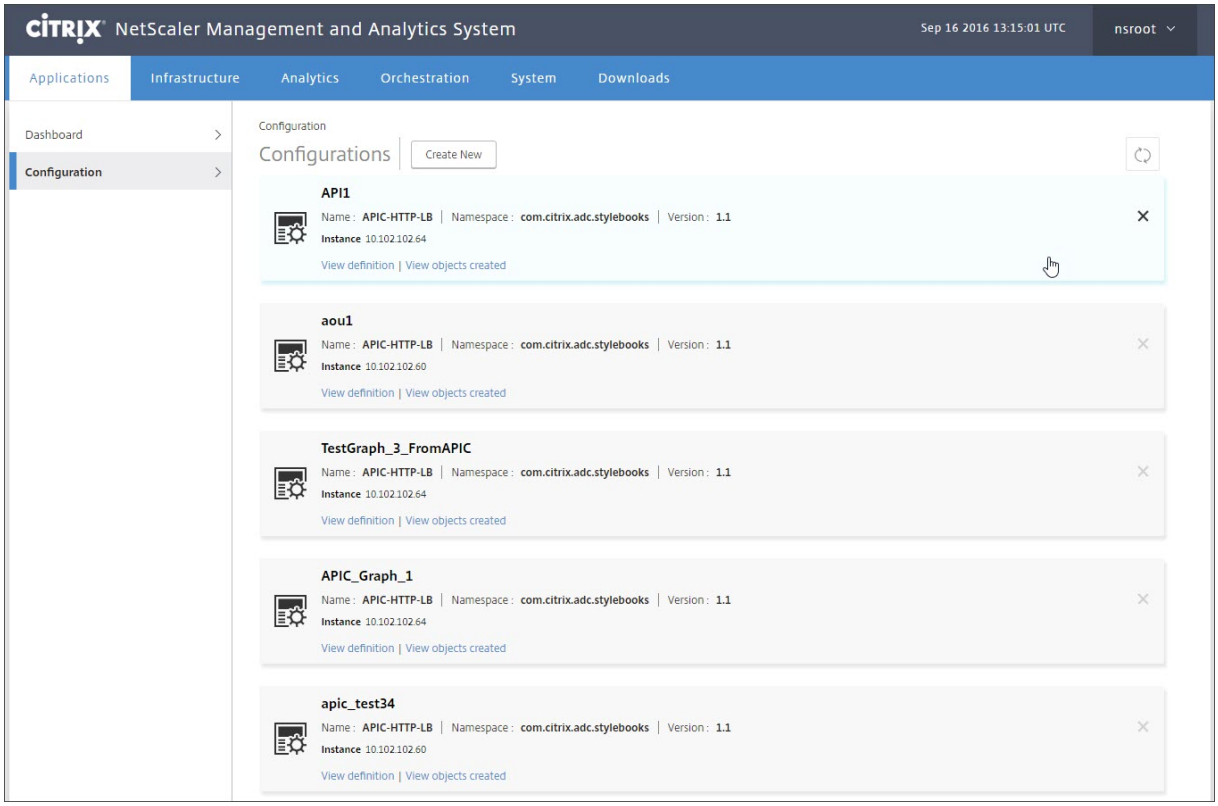
c) Dans les **paramètres pour l'EPG et les points de terminaison (ports) définis dans la fenêtre du graphique des services**, entrez les valeurs du paramètre renseigné à partir du StyleBook et cliquez sur **Créer**.



d) Cliquez sur **Créer**.



La configuration L4-L7 spécifiée dans le StyleBook est déployée, dans Citrix ADM. Vous pouvez afficher la configuration StyleBoook à partir de l'onglet **Application**, en accédant à **Application > Configuration**.



Attacher et détacher les événements de point de terminaison d'APIC

February 1, 2024

La solution en mode hybride gère implicitement l'attachement ou le détachement des événements de point de terminaison du Cisco APIC. Lorsque l'APIC Cisco déclenche un événement de point de terminaison attachement, le servicegroup_servicegroupmember_binding est automatiquement déclenché par le StyleBook dans Citrix Application Delivery Management (ADM), et le point de terminaison est délié lors de l'événement de point de terminaison détacher.

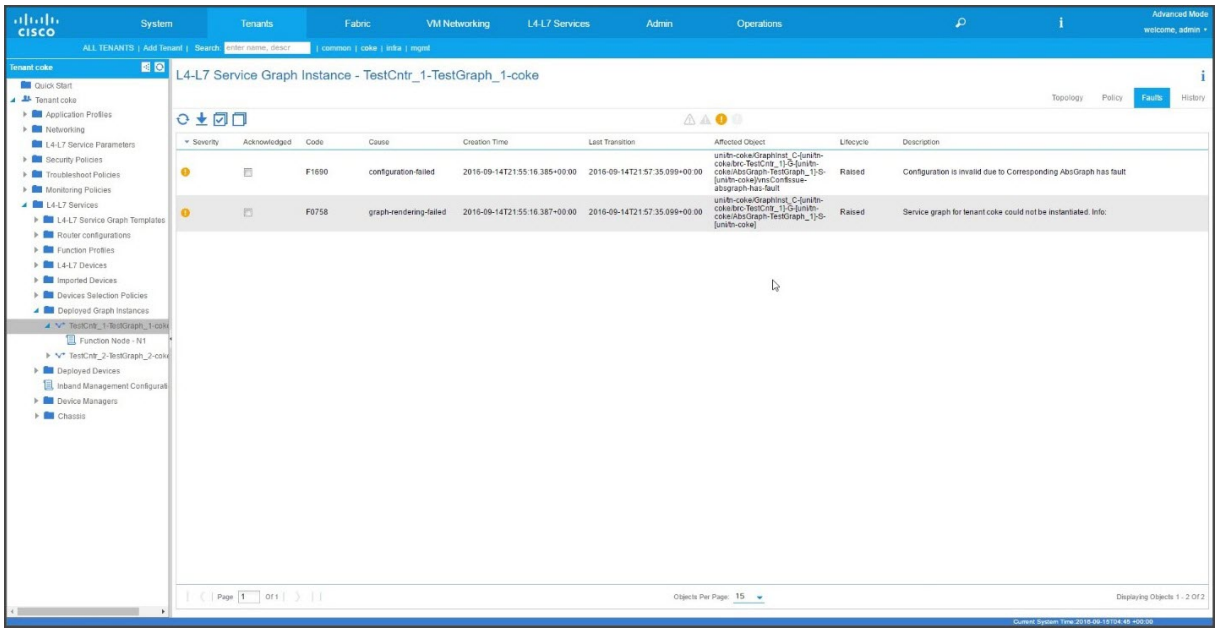
En outre, si vous n'avez pas déployé la configuration L4-L7 dans citrix ADM avant que l'événement de point de terminaison d'attache ou de détachement ne soit déclenché dans Cisco l'APIC, la solution conservera les adresses IP d'attache dans la base de données. Ces adresses IP sont liées au groupe de services correspondant après la création du groupe de services via StyleBook.

Rapports d'erreurs APIC

February 1, 2024

Lorsque vous déployez un package de périphériques Citrix ADC dans Cisco ACI, le Cisco APIC signale toute défaillance. Vous pouvez afficher les rapports d'erreurs à n'importe quel niveau de l'APIC (par exemple, périphérique, locataire, EPG ou graphique de service). La capture d'écran ci-dessous montre un rapport d'erreur au niveau de l'appareil. Pour plus d'informations sur les défauts, consultez http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/faults/guide/b_APIC_Faults_Errors/b_IFC_Faults_Errors_chapter_01.html.

Sélectionnez une entité APIC et cliquez sur l'onglet **Faults** pour afficher les erreurs signalées par l'APIC pour cette entité.



Journaux générés par Citrix ADM

February 1, 2024

Citrix Application Delivery Management (ADM) fournit une journalisation complète qui peut aider à résoudre les problèmes. Les journaux générés (**admin.log**) sont situés à : **/var/controlcenter/log/**

Vous pouvez ouvrir une session sur Citrix ADM et utiliser l'interpréteur de commandes pour accéder à la structure de répertoire Citrix ADM. Voici un exemple d'extrait d'un journal Citrix ADM pour le déploiement de graphe d'un APIC.


```
    2016-06-29 10:58:33,816 DEBUG APIC Config  = {
(0, '', 5230): {
'dn': u'uni/vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[uni/tn-coke_SDX2]-ctx-cokectx1', 'state': 1, 'transaction': 0, 'ackedstate': 0, 'tenant': 'coke_SDX2', 'ctxName': 'cokectx1', 'value': {
(10, '', 'ADCHybridMode_1_Consumer_1'): {
'state': 1, 'transaction': 0, 'cifs': {
'ADCHybridMode_1_Device_1': '1_1' }
, 'ackedstate': 0 }
, (7, '', '2129920_32778'): {
'state': 1, 'tag': 273, 'type': 1, 'ackedstate': 0, 'transaction': 0 }
, (1, '', 5790): {
'transaction': 0, 'ackedstate': 0, 'value': {
(3, 'ADCFunction', 'N1'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(4, 'mFCngNetwork', 'mFCngnetwork'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(6, 'Network_key', 'network_key'): {
'state': 1, 'transaction': 0, 'target': 'network', 'ackedstate': 0 }
 }
 }
, (4, 'internal_network', 'internal_network'): {
'connector': 'provider', 'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(6, 'internal_network_key', 'internal_network_key'): {
'state': 1, 'transaction': 0, 'target': 'network/internal_snip', 'ackedstate': 0 }
 }
 }
, (2, 'external', 'consumer'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(9, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
'state': 1, 'transaction': 0, 'target': 'ADCHybridMode_1_Consumer_1_2129920_32778', 'ackedstate': 0 }
 }
 }
, (4, 'mFCngStylebook', 'mFCngStylebook'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(6, 'Stylebook_key', 'Stylebook_key'): {
'state': 1, 'transaction': 0, 'target': 'stylebook_1', 'ackedstate': 0
    }
 }
 }
, (2, 'internal', 'provider'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(9, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
'state': 1, 'transaction': 0, 'target': 'ADCHybridMode_1_Consumer_1_2129920_32778', 'ackedstate': 0 }
 }
 }
 }
 }
```



```
 }
, 'state': 1, 'absGraph': 'HybridModeGraph_1', 'rn': u'vGrp-[uni/tn-coke_SDX2/GraphInst_C-[uni/tn-coke_SDX2/brc-TestCntr_3]-G-[uni/tn-coke_SDX2/AbsGraph-HybridModeGraph_1]-S-[uni/tn-coke_SDX2]]' }
, (4, 'Network', 'network'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(4, 'nsip', 'internal_snip'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(5, 'type', 'type'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'SNIP' }
, (5, 'hostroute', 'hostroute'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'DISABLED' }
, (5, 'ipaddress', 'ipaddress'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': '10.1.1.1' }
, (5, 'dynamicrouting', 'dynamicRouting'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'ENABLED' }
, (5, 'netmask', 'netmask'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': '255.255.255.0' }
 }
 }
 }
 }
, (8, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
'state': 1, 'transaction': 0, 'vif': 'ADCHybridMode_1_Consumer_1', 'ackedstate': 0, 'encap': '2129920_32778' }
, (4, 'Stylebook', 'stylebook_1'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(5, 'name', 'stylebookName'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'APIC-HTTP-LB' }
 }
 }
 }
, 'txid': 10000 }
 }

   2016-06-29 10:58:33,816 DEBUG get Graph Return details = {
'graphDN': u'uni/vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[uni/tn-coke_SDX2]-ctx-cokectx1', (1, '', 5790): {
'state': 1, 'graphrn': u'vGrp-[uni/tn-coke_SDX2/GraphInst_C-[uni/tn-coke_SDX2/brc-TestCntr_3]-G-[uni/tn-coke_SDX2/AbsGraph-HybridModeGraph_1]-S-[uni/tn-coke_SDX2]]' }
, 'tenantName': 'coke_SDX2', 'StyleBookName': 'APIC-HTTP-LB', 'graphInstanceName': 'HybridModeGraph_1', 'context': 'cokectx1', 'graphInstanceId': 5790 }

   2016-06-29 10:58:33,827 DEBUG SUCCESS created track 2.0
   2016-06-29 10:58:33,833 DEBUG SUCCESS updated track with new task 2
   2016-06-29 10:58:33,851 DEBUG SUCCESS updated track with new task 1
   2016-06-29 10:58:33,867 DEBUG fn_wrapper:long_operation_thread_id:<eventlet.greenthread.GreenThread object at 0x80aa5c7d0>
   2016-06-29 10:58:33,867 DEBUG +++++++ Service Audit Call for Device
```



```
            Details  = 10.102.102.62 +++++++++++++++++
88      2016-06-29 10:58:33,867 DEBUG Inside APIC Cred Col If = 2
89      2016-06-29 10:58:33,867 DEBUG Host name from device =
           ADCHybridMode_1
90      "InProgress","message":null,"replication_status":"","target":"
           10.102.102.81","operation":"POST","entity_type":"apic","
           entity_id":null }
91    }
92
93      2016-06-29 10:58:44,141 DEBUG  Save config  Response = {
94    "errorcode": 0, "message": "Done", "severity": "NONE"  }
95
96      2016-06-29 10:58:44,141 DEBUG +++++++++ getContextAwareFlag = True
97      2016-06-29 10:58:44,141 DEBUG +++++ get context tenant name from
           Config ++++++
98      2016-06-29 10:58:44,141 DEBUG +++++ getContextTenantName = {
99    'state': 1, 'ctxName': 'cokectx1', 'tenant': 'coke_SDX2', 'vdev': 5230
         }
100   ++++++
101     2016-06-29 10:58:44,142 DEBUG Service health details = {
102   }
103   collection length = 0
104     2016-06-29 10:58:44,142 DEBUG Count details Total = 0 Up = 0 Down =
           0
105     2016-06-29 10:58:44,142 DEBUG Health Score details Up = 0
106     2016-06-29 10:58:44,142 DEBUG Service HEALTH final collection  = {
107   ((0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1')): {
108   'faults': [], 'state': 0, 'health': ([(0, '', 5230), (1, '', 5790),
           (3, 'ADCFunction', 'N1')], 0) }
109   }
110
111     2016-06-29 10:58:44,142 DEBUG ++++++getServiceHealth Fault List =
           []
112     2016-06-29 10:58:44,142 DEBUG Service HEALTH final response  = {
113   'devs': 'ADCHybridMode_1_Device_1', 'faults': [], 'state': 0, 'health'
           : [([(0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1')], 0)] }
114
115     2016-06-29 10:58:44,236 DEBUG RESPONSE from NSLOGOUT = {
116   "errorcode": 0, "message": "Done", "severity": "NONE"  }
117   , sessionId = ##
           D2EAFA7CFCD73119E6C5E78D8BCB2E842829C971C1DC7E99850949DAE0029F2191B5E7EDF2764
118     2016-06-29 10:58:44,237 DEBUG +++++ Faults respCol   = {
119   '10.102.102.62': {
120   '10.102.102.62': {
121   u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
         u'NONE', 'operation_name': 'add_op' }
122   }
123   , (7, '', '2129920_32778'): {
124   'vlan': {
125   u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
         u'NONE', 'operation_name': 'add_op' }
126   }
```



```
127   , (((0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1'), (2, '
          internal', 'provider')), 'nsip'): {
128   'vlan_nsip_binding': {
129   u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
          u'NONE', 'operation_name': 'bind_op' }
130    }
131   , (((0, '', 5230), (4, 'Network', 'network')), (4, 'nsip', '
          internal_snip')): {
132   'nsip': {
133   u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
          u'NONE', 'operation_name': 'add_op' }
134    }
135   , (): {
136    }
137   , (8, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
138   'vlan_interface_binding': {
139   u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
          u'NONE', 'operation_name': 'bind_op' }
140    }
141    }
142
143      2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg
             = Done, statusCode = add_op
144      2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg
             = Done, statusCode = add_op
145      2016-06-29 10:58:44,237 DEBUG Fault details oprName = bind_op,
          erMsg = Done, statusCode = bind_op
146      2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg
             = Done, statusCode = add_op
147      2016-06-29 10:58:44,238 DEBUG Fault details oprName = bind_op,
          erMsg = Done, statusCode = bind_op
148      2016-06-29 10:58:44,238 DEBUG +++++++++++++++ ServiceAudit response
          = {
149   'faults': [], 'state': 0, 'health': [] }
150
151      2016-06-29 10:58:44,238 DEBUG APIC Graph Details = {
152   'graphDN': u'uni/vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[
          uni/tn-coke_SDX2]-ctx-cokectx1', (1, '', 5790): {
153   'state': 1, 'graphrn': u'vGrp-[uni/tn-coke_SDX2/GraphInst_C-[uni/tn-
          coke_SDX2/brc-TestCntr_3]-G-[uni/tn-coke_SDX2/AbsGraph-
          HybridModeGraph_1]-S-[uni/tn-coke_SDX2]]' }
154   , 'tenantName': 'coke_SDX2', 'StyleBookName': 'APIC-HTTP-LB', '
          graphInstanceName': 'HybridModeGraph_1', 'context': 'cokectx1', '
          graphInstanceId': 5790 }
155
156      2016-06-29 10:58:44,242 DEBUG Journal Processing: Database task:
          create apic_graph
157      2016-06-29 10:58:44,264 DEBUG SUCCESS created task 2
158      2016-06-29 10:58:44,269 DEBUG SUCCESS updated track with new task 2
159      2016-06-29 10:58:44,308 DEBUG +++++++ get IP and Connector
          collection from Config with type 22 for attach & detach event
          ++++++
160      2016-06-29 10:58:44,308 DEBUG ----- connector with IP List = {
```



```
161   0: [], 1: [], 3: [] }
162
163      2016-06-29 10:58:44,308 DEBUG ----- attachIpList = [] dettachIpList
             = []
164      2016-06-29 10:58:44,308 DEBUG ----- In _attachDettachIps
            attachIpList = [] dettachIpList = []
165      2016-06-29 10:58:44,312 DEBUG ----- In _attachDettachIps row = {
166    'deviceIP': u'10.102.102.62', 'responseToAPIC': None, 'graphDN': u'uni
        /vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[uni/tn-
        coke_SDX2]-ctx-cokectx1', 'apicGraphState': None, 'serviceGroupName
        ': None, 'configPackId': None, 'tenantName': u'coke_SDX2', '
        styleBookName': u'APIC-HTTP-LB', 'graphInstanceName': u'
        HybridModeGraph_1', 'context': u'cokectx1', 'serviceGroupPort':
        None, 'graphInstanceId': 5790, 'createDate': None, 'serviceGroupIP'
        : None }
167
168  <!--NeedCopy-->
```

Journaux générés par le package de périphériques en mode hybride

February 1, 2024

Le package de périphériques Citrix ADC Hybrid Mode génère des journaux liés à la configuration et des journaux liés à la surveillance. Les journaux générés se trouvent à l'adresse **/data/devicescript/Citrix.NetScalerMas.1.0/logs**.

Voici un exemple de fragment de **debug.log**d'un Cisco APIC :

```
1      2016-06-28 03:06:53.879767 DEBUG Thread-20 18723 [10.102.102.62,
          24063] Device manager details ip = 10.102.102.81, port = 80
2      2016-06-28 03:06:53.879856 DEBUG Thread-20 18724 [10.102.102.62,
          24063] +++++++++++++++ serviceAudit  request ++++++++++++++++++
3      2016-06-28 03:06:53.879929 DEBUG Thread-20 18725 [10.102.102.62,
          24063] ++++++++++ getStyleBookObjects ++++++++++++
4      2016-06-28 03:06:53.879995 DEBUG Thread-20 18726 [10.102.102.62,
          24063] NMAS collection A3 = (4, 'Stylebook', 'stylebook_1') B3 =
           {
5    'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
6    (5, 'name', 'stylebookName'): {
7    'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'APIC-HTTP-LB'
         }
8     }
9     }
10
11     2016-06-28 03:06:53.880045 DEBUG Thread-20 18727 [10.102.102.62,
          24063] NMAS collection styleBookName= APIC-HTTP-LB
12     2016-06-28 03:06:53.880093 DEBUG Thread-20 18728 [10.102.102.62,
          24063] NMAS collection retCol= {
```



```
13  'Stylebook': 'APIC-HTTP-LB', 'tuple': ((0, '', 5230), (4, 'Stylebook',
        'stylebook_1')) }
14
15     2016-06-28 03:06:53.880140 DEBUG Thread-20 18729 [10.102.102.62,
          24063]  ++++ devMgrStyleBookUrl = http://10.102.102.81/stylebook
          /nitro/v1/config/stylebooks/com.citrix.adc.stylebooks/1.1/APIC-
          HTTP-LB
16     2016-06-28 03:06:54.135240 DEBUG Thread-20 18730 [10.102.102.62,
          24063]  ++++ Response from styleBookresCode serviceAudit = {
17  u'stylebook': {
18  u'uses_builtin_namespaces': {
19  u'netscaler.nitro.config': u'10.5' }
20  , u'name': u'APIC-HTTP-LB', u'used_by_stylebooks': [], u'namespace': u
       'com.citrix.adc.stylebooks', u'source': u'---\nname: APIC-HTTP-LB\
       nnamespace: com.citrix.adc.stylebooks\nversion: "1.1"\ndisplay-name
       : "Sample StyleBook for APIC Load Balanced Application"\
       ndescription: "This is a sample StyleBook for HTTP Load Balanced
       Application configuration via APIC"\nschema-version: "1.0"\nimport-
       stylebooks: \n  - \n    namespace: netscaler.nitro.config\n
       prefix: ns\n    version: "10.5"\n  - \n    namespace: "com.citrix.
       adc.stylebooks"\n    prefix: "stlb"\n    version: "1.1"\nparameters
       -default-sources:\n  - stlb::APIC-ROOT\nsubstitutions:\n  lb-name(
       appname, port): $appname + "-" + str($port) + "-lb"\n  sg-name(
       appname, port): $appname + "-" + str($port) + "-sg"\n
       healthmonitor[]:\n    true: "NO"\n    false: "YES"\ncomponents: \n
        - \n    name: lbvserver\n    type: ns::lbvserver\n    repeat:
       $parameters.app-services\n    repeat-item: app\n    properties: \
       n      name: $substitutions.lb-name($parameters.appname, $app.
       virtual-port)\n      ipv46: $app.virtual-ip\n      port: $app.
       virtual-port\n      servicetype: $app.protocol\n      lbmethod?:
       $app.algorithm\n      persistencetype?: $app.persistence\n  - \n
        name: svcgrp\n    type: ns::servicegroup\n    repeat: $parameters.
       app-services\n    repeat-item: app\n    properties: \n      name:
       $substitutions.sg-name($parameters.appname, $app.virtual-port)\
       n      servicetype: $app.protocol\n      useproxyport?: $app.sg-
       advanced.useproxyport\n      usip?: $app.sg-advanced.usip\n
       cip?: $app.sg-advanced.cip\n      cipheader?: $app.sg-advanced.
       cipheader\n      healthmonitor?: $substitutions.healthmonitor($app.
       skip_healthmonitor)\n    components: \n      -\n        name:
       lbvserver-svg-binding\n        type: ns::
       lbvserver_servicegroup_binding\n        properties: \n
       name: $substitutions.lb-name($parameters.appname, $app.virtual-port
       )\n          servicegroupname: $parent.properties.name\n      - \
       n        name: svg-members\n        type: ns::
       servicegroup_servicegroupmember_binding\n        condition: $app.
       server-ips\n        repeat: $app.server-ips\n        repeat-item:
       serverip\n        properties: \n          ip: $serverip\n
       port: $app.server-port\n          servicegroupname: $parent.
       properties.name\noutputs: \n  - \n    name: lbvservers\n    value:
       $components.lbvserver\n  - \n    name: servicegroups\n    value:
       $components.svcgrp', u'version': u'1.1', u'uses_stylebooks': [{
21  u'version': u'1.1', u'namespace': u'com.citrix.adc.stylebooks', u'name
       ': u'APIC-ROOT' }
```



```
22  ] }
23   }
24
25      2016-06-28 03:06:54.359142 DEBUG Thread-20 18731 [10.102.102.62,
           24063]  ++++ Dev Mgr request details devMgrUrl = http://
           10.102.102.81/admin/v1/apic
26      2016-06-28 03:06:54.359221 DEBUG Thread-20 18732 [10.102.102.62,
           24063]  ++++ Response from Device Mgr serviceAudit = {
27  "APIC":[] }
28
29      2016-06-28 03:06:54.359266 DEBUG Thread-20 18733 [10.102.102.62,
           24063] ++++++++++++++ serviceAudit response = {
30  "APIC":[] }
31
32      2016-06-28 03:06:54.359306 DEBUG Thread-20 18734 [10.102.102.62,
           24063] ++++++++++++++ serviceAudit response headers content type
           = application/json; charset=utf-8
33      2016-06-28 03:06:54.359394 DEBUG Thread-20 18735 [10.102.102.62,
           24063] ++++++++++++++ serviceAudit response headers = {
34  'content-length': '11', 'job_id': 'ctxt-f4db2883-e42c-4262-a35f-04628
       c4ad5ea', 'x-content-type-options': 'nosniff', 'transfer-encoding':
        'chunked', 'connection': 'close', 'date': 'Wed, 29 Jun 2016
       10:58:33 GMT', 'x-frame-options': 'SAMEORIGIN', 'content-type': '
       application/json; charset=utf-8' }
35
36      2016-06-28 03:06:54.359480 DEBUG Thread-20 18736 [10.102.102.62,
           24063] ++++++++++++++ pollingURL = http://10.102.102.81/admin/v1
           /journalcontexts/ctxt-f4db2883-e42c-4262-a35f-04628c4ad5ea
37      2016-06-28 03:06:54.359713 DEBUG Thread-20 18737 [10.102.102.62,
           24063] ++++++++++++++ pollingStatus = True, pollingTime = 0
38      2016-06-28 03:06:54.483228 DEBUG Thread-20 18738 [10.102.102.62,
           24063] ++++++++++++++ pollingResponse json = {
39  u'journalcontext': {
40  u'status': u'In Progress', u'scopes': [], u'entity_id': None, u'name':
        u'Create apic', u'operation': u'POST', u'entity_type': u'apic', u'
       service_name': u'admin', u'start_time': u'2016-06-29T10
       :58:33.760565', u'is_default': u'false', u'end_time': None, u'
       target': u'10.102.102.81', u'message': None, u'id': u'ctxt-f4db2883
       -e42c-4262-a35f-04628c4ad5ea', u'replication_status': u'' }
41   }
42
43      2016-06-28 03:07:04.493074 DEBUG Thread-20 18739 [10.102.102.62,
           24063] ++++++++++++++ pollingStatus = True, pollingTime = 1
44      2016-06-28 03:07:04.587595 DEBUG Thread-20 18767 [10.102.102.62,
           24063] ++++++++++++++ pollingResponse json = {
45  u'journalcontext': {
46  u'status': u'In Progress', u'scopes': [], u'entity_id': None, u'name':
        u'Create apic', u'operation': u'POST', u'entity_type': u'apic', u'
       service_name': u'admin', u'start_time': u'2016-06-29T10
       :58:33.760565', u'is_default': u'false', u'end_time': None, u'
       target': u'10.102.102.81', u'message': None, u'id': u'ctxt-f4db2883
       -e42c-4262-a35f-04628c4ad5ea', u'replication_status': u'' }
47   }
```



```
48
49      2016-06-28 03:07:14.597812 DEBUG Thread-20 18790 [10.102.102.62,
           24063] +++++++++++++++ pollingStatus = True, pollingTime = 2
50      2016-06-28 03:07:14.692590 DEBUG Thread-20 18791 [10.102.102.62,
           24063] +++++++++++++++ pollingResponse json = {
51   u'journalcontext': {
52   u'status': u'Finished', u'scopes': [], u'entity_id': None, u'name': u'
        Create apic', u'operation': u'POST', u'entity_type': u'apic', u'
        service_name': u'admin', u'start_time': u'2016-06-29T10
        :58:33.760565', u'is_default': u'false', u'end_time': u'2016-06-29
        T10:58:44.486919', u'target': u'10.102.102.81', u'message': u'Done'
        , u'id': u'ctxt-f4db2883-e42c-4262-a35f-04628c4ad5ea', u'
        replication_status': u'' }
53    }
54
55      2016-06-28 03:07:14.692932 DEBUG Thread-20 18793 [10.102.102.62,
           24063] Attempts 1
56      2016-06-28 03:07:14.693031 DEBUG Thread-20 18794 [10.102.102.62,
           24063] Cluster (u'uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1', (0,
            '', 5230)), transaction: 0
57      2016-06-28 03:07:14.693147 DEBUG Thread-20 18795 [10.102.102.62,
           24063] Attempts for {
58   'name': 'ADCHybridMode_1', 'host': '10.102.102.62', 'virtual': False,
        'devs': {
59   'ADCHybridMode_1_Device_1': {
60   'state': 0, 'virtual': False, 'manager': {
61   'hosts': {
62   '10.102.102.81': {
63   'port': 80 }
64    }
65   , 'name': 'NMAS_1', 'creds': {
66   'username': 'nsroot', 'password': '<hidden>' }
67    }
68   , 'version': '11.0', 'host': '10.102.102.62', 'port': 80, 'creds': {
69   'username': 'nsroot', 'password': '<hidden>' }
70    }
71    }
72   , 'manager': {
73   'hosts': {
74   '10.102.102.81': {
75   'port': 80 }
76    }
77   , 'name': 'NMAS_1', 'creds': {
78   'username': 'nsroot', 'password': '<hidden>' }
79    }
80   , 'contextaware': True, 'port': 80, 'creds': {
81   'username': 'nsroot', 'password': '<hidden>' }
82    }
83    is 0
84      2016-06-28 03:07:14.693339 DEBUG Thread-20 18796 [10.102.102.62,
           24063] Deleting (u'uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1',
           (0, '', 5230))
85      2016-06-28 03:07:14.693379 DEBUG Thread-20 18797 [10.102.102.62,
```



```
           24063] pending: False, delete: False, txId: None
86      2016-06-28 03:07:14.693517 DEBUG Thread-20 18798 [10.102.102.62,
           24063] Faults: []
87      2016-06-28 03:07:14.693558 DEBUG Thread-20 18799 [10.102.102.62,
           24063] Health: []
88      2016-06-28 03:07:14.693914 DEBUG Thread-20 18800 [10.102.102.62,
           24063] Send num: 761, type: 220, len: 382
89  <!--NeedCopy-->
```

Package de périphériques Citrix ADC en mode Cloud Orchestrator de Cisco ACI

February 1, 2024

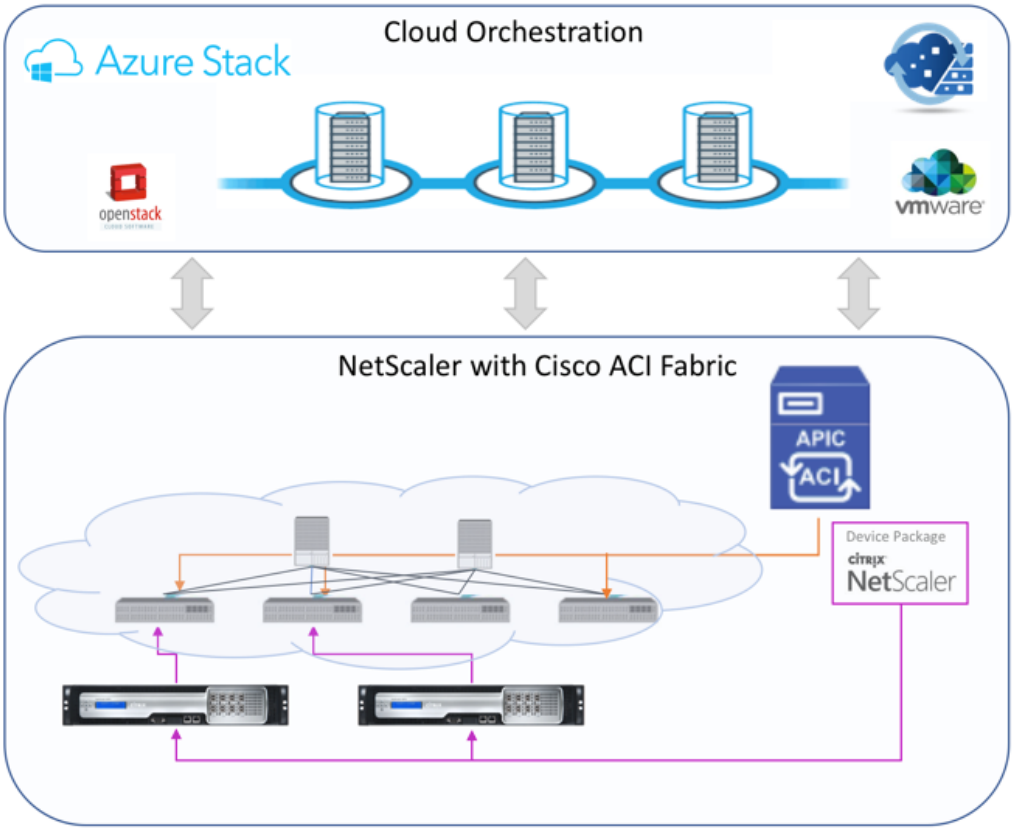
Avec Application Policy Infrastructure Controller (APIC) version 3.1, Citrix ADC et Cisco ACI étendent le portefeuille d'intégration conjoint pour fournir une nouvelle solution répondant aux besoins des clients. Le nouveau mode d'intégration, le mode ACI Cloud Orchestrator*, simplifie les intégrations L4-L7 en supprimant la complexité de la configuration grâce à des paramètres normalisés. La solution fonctionne de manière transparente pour automatiser les services L4-L7, atteindre les objectifs de déploiement d'applications agiles, de flexibilité opérationnelle et de simplicité.

Le mode orchestrateur de cloud Cisco ACI à l'aide de la solution Citrix ADC offre les avantages suivants :

- L'automatisation des services L4-L7 réduit les erreurs humaines.
- L'intégration prédéfinie de la solution Cisco ACI vous aide à réduire le temps de déploiement et augmente les performances des applications, telles que les applications Web, les machines virtuelles et SQL.
- Visibilité entièrement intégrée sur la santé des applications telles que les applications Web, les machines virtuelles et SQL sur les composants réseau physiques et virtuels.

Le mode Orchestrator cloud ACI vous offre désormais plus de choix pour utiliser la nouvelle interface graphique APIC simplifiée directement ou en sélectionnant n'importe quel orchestrateur de cloud, tel que Cisco Cloud Center, Windows Azure Pack, OpenStack, vRealize ou tout autre en fonction de vos préférences. Cette nouvelle modification est réalisée en exposant un ensemble d'attributs ADC en tant que schéma ADC. Ces attributs sont mappés dans les profils de fonction des packages d'appareils. Vous pouvez fournir des valeurs pour ces attributs lors du Provisioning du service ADC par l'orchestrateur de cloud (Cisco Cloud Center ou Wireless Application Protocol (WAP)).

L'illustration suivante fournit une vue d'ensemble de Citrix ADC dans une solution d'orchestration cloud :

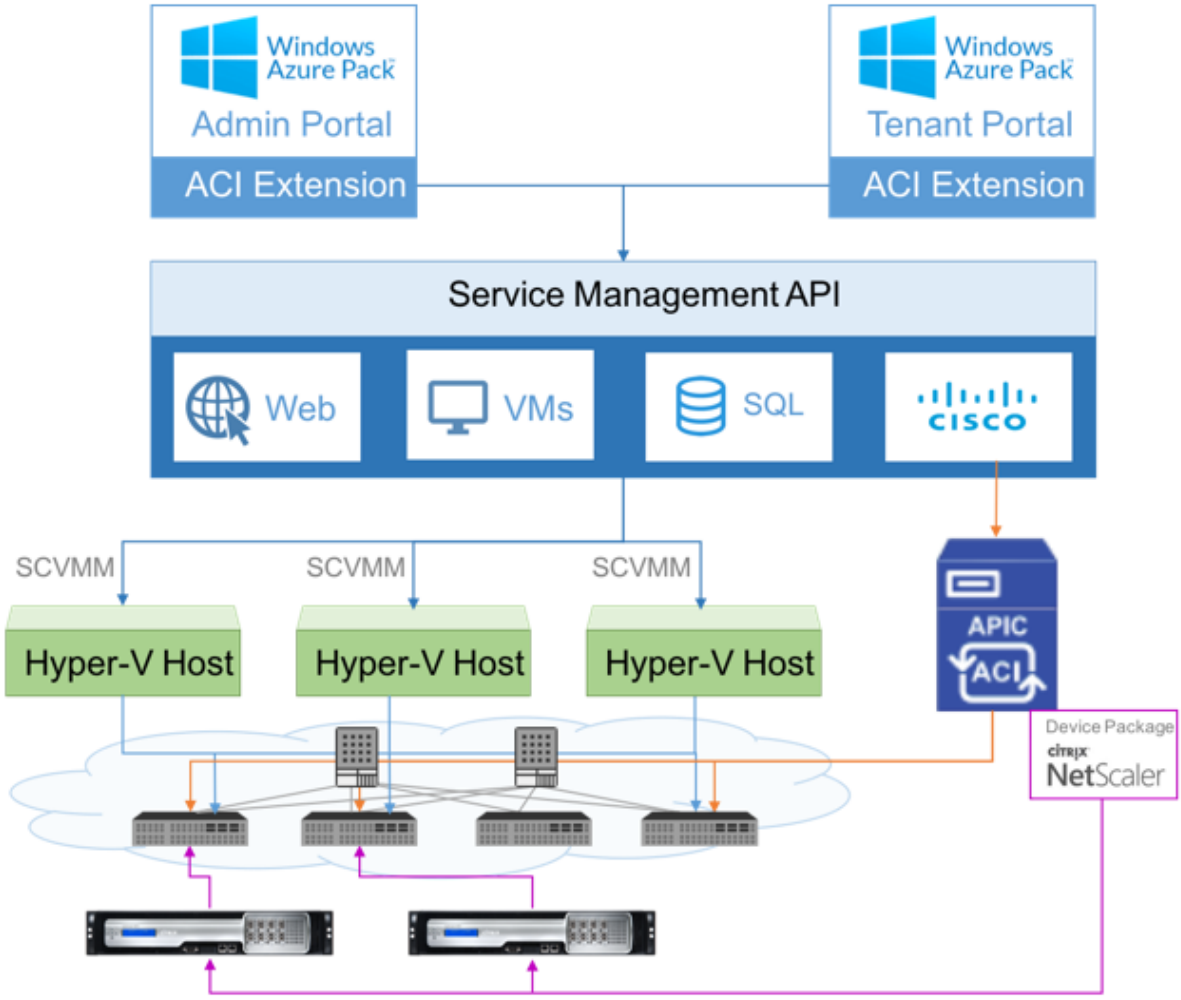


La solution en mode d'orchestrateur de cloud utilisant Microsoft Azure Pack implique de nombreux points d'intégration, tels qu'Azure Pack vers Cisco APIC, Cisco APIC vers System Central Virtual Machine Manager (SCVMM) et Cisco APIC vers Citrix ADC. En tant que locataire dans le cloud privé, vous pouvez activer le NAT, fournir des services réseau et ajouter un équilibreur de charge.

Azure Pack prend en charge les portails des locataires et des administrateurs, et chacun d'eux possède son propre ensemble d'opérations pouvant être effectuées.

- En tant qu'administrateur, vous pouvez effectuer des tâches administratives telles que l'enregistrement ACI, la plage d'adresses IP virtuelles, l'association d'appareils Citrix ADC avec le cloud de machines virtuelles et la création de comptes d'utilisateurs locataires.
- En tant que locataire, vous pouvez effectuer des tâches telles que vous connecter au portail locataire Azure Pack et configurer le réseau, les domaines de pont et le routage et le transfert virtuels (VRF), et pouvez utiliser les fonctionnalités d'équilibrage de charge Citrix ADC et RNAT.

L'illustration suivante fournit une vue d'ensemble d'Azure Pack dans une solution en mode cloud :



Important

- L'administrateur du cloud peut faciliter la tâche avec le schéma L4-L7 pris en charge par l'APIC et toute modification supplémentaire peut être effectuée par l'administrateur APIC directement dans l'APIC. Cela vous permet de configurer et de déployer Citrix ADC au même niveau que l'ensemble des fonctionnalités prises en charge.
- Les locataires peuvent déployer plusieurs adresses VIP avec différents ports pour le même réseau. Vous devez vous assurer que la combinaison IP et port est unique.
- Le package d'appareils Citrix ADC prend uniquement en charge le déploiement à contexte unique. Chaque locataire reçoit une instance Citrix ADC dédiée.
- Le protocole d'application sans fil (WAP) prend en charge les appliances Citrix ADC MPX et les appliances Citrix ADC VPX (y compris les instances Citrix ADC VPX déployées sur la plate-forme Citrix ADC SDX).

Le package d'appareils en mode orchestrateur cloud prend en charge à la fois le mode entièrement géré et le mode gestionnaire de services. Le package de mode entièrement géré prend en charge une grande variété de profils de fonction, tels que l'équilibrage de charge simple, la commutation de contenu, le déchargement SSL et d'autres profils. Ces profils de fonction couvrent un ensemble complet de fonctionnalités et le mode de déploiement de Citrix ADC. De même, le package de périphériques en mode gestionnaire de services prend en charge la configuration à un et deux bras et le déploiement de Citrix ADC à l'aide d'APIC. Citrix Application Delivery Management (ADM) agit en tant que gestionnaire de services pour APIC et vous pouvez utiliser Citrix ADM pour configurer les paramètres Citrix ADC L4-L7.

> **Remarque**
>
> En mode gestionnaire de services (mode hybride), vous ne pouvez pas réutiliser ou réattribuer la même adresse IP du serveur, qui est déjà présente dans l'appliance Citrix ADC.

Le profil de fonction du mode Orchestrator Cloud possède un ensemble de paramètres mappés au schéma ADC des APIC et l'orchestrateur utilise ces paramètres. L'orchestrateur de cloud fournit les valeurs des paramètres ADC (VIP, tout en provisionnant Citrix ADC via APIC). L'orchestrateur communique avec les API de l'APIC et transmet les détails spécifiques à l'ADC dans le cadre de la charge utile d'un profil de fonction spécifique. En interne, APIC extrait les valeurs et les transmet au package de périphérique qui configure l'Citrix ADC en interne.

Pour plus d'informations sur la liste complète des schémas ADC, qui sont pris en charge par les API Cisco, reportez-vous au Guide de déploiement des services Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 3.x and earlier).

Le package de périphériques en mode entièrement géré prend en charge les profils de fonctions suivants :

1. LB-HTTP-One-Arm-ProfileCM
2. LB-HTTP-Two-Arm-ProfileCM
3. LB-HTTP-Two-Arm-ServiceBackendProfileCM
4. CS-HTTP-LB-Service-ProfileCM
5. CS-SSL-LB-Service-ProfileCM
6. LB-SSL-ProfileCM
7. SSLVServerProfileInlineModeCM
8. WebVServerProfileWithRHICM
9. WebInlineVServerProfileWithRHICM
10. WebAnywhereVServerProfileWithRHIC

11. SSLVServerProfileForAnywhereModeCM
12. SSLAnywhereServerProfileCM
13. WebVServerProfileCM
14. WebInlineVServerProfileCM
15. WebAnywhereVServerProfileCM
16. CSLBServerProfileCM
17. GSLBServerProfileCM
18. CMPServerProfileCM
19. CRServerProfileC
20. DNSServerProfileCM
21. DSServerProfileCM
22. ICServerProfileCM
23. SSLVPNServerProfileCM
24. AppFWServerProfileCM
25. AAAServerProfileCM
26. AAASyslogServerProfileCM
27. IPv6WebInlineVServerProfileCM

Le package d'appareils en mode de gestion des services prend en charge les profils de fonction du mode cloud suivants :

1. ADCOneArmFunctionProfileCM
2. AADCTwoArmFunctionProfileCM
3. RHI-ADCOneArmFunctionProfileCM
4. RHI-ADCTwoArmFunctionProfileCM

Citrix ADC prend en charge les profils de fonction mentionnés ci-dessus. L'APIC prend en charge un sous-ensemble de ces paramètres dans le schéma ADC. Si des attributs non pris en charge par Cisco ACI sont présents dans le profil de fonction, vous devez cloner le profil de fonction du mode orchestrateur de cloud et fournir les valeurs pour tous les attributs non pris en charge par APIC et enregistrer les attributs. Plus tard, l'orchestrateur peut utiliser le profil de fonction récemment cloné.

Le package d'appareils en mode Citrix Cloud prend en charge Citrix ADC 12.0 et le mode gestionnaire de services utilise également Citrix ADM 12.0. Le package de l'appareil a changé la version du modèle

de 1.0 à 2.0 et peut être utilisé comme nouvelle installation. Le package d'appareils en mode Orchestrator Cloud ne peut pas être mis à niveau à partir des versions précédentes du package d'appareils car la version du modèle a

Les packages d'appareils en mode Orchestrator Cloud peuvent également être utilisés dans le cadre d'un déploiement régulier. Le package n'oblige pas l'utilisateur à provisionner Citrix ADC via un orchestrateur de cloud. Le package de l'appareil est compatible uniquement avec APIC et APIC avec un orchestrateur de cloud.

Gérer la configuration de Kubernetes Ingress dans Citrix ADM

February 1, 2024

Kubernetes (K8s) est une plate-forme d'orchestration de conteneurs open source qui automatise le déploiement, la mise à l'échelle et la gestion des applications cloud natives.

Kubernetes fournit la fonctionnalité d'entrée qui permet au trafic client en dehors du cluster d'accéder aux microservices d'une application exécutée au sein du cluster Kubernetes. Les instances ADC peuvent servir d'entrée aux applications exécutées au sein d'un cluster Kubernetes. Les instances ADC peuvent équilibrer la charge et le contenu acheminer le trafic Nord-Sud des clients vers n'importe quel microservice au sein du cluster Kubernetes.

> **Remarque**
>
> - Citrix ADM prend en charge la fonctionnalité Ingress sur les clusters avec Kubernetes version 1.14 et versions ultérieures.
> - Citrix ADM prend en charge les appliances Citrix ADC VPX et MPX en tant que périphériques d'entrée.
> - Dans l'environnement Kubernetes, la charge de l'instance Citrix ADC équilibre uniquement le type de service « NodePort ».

Vous pouvez configurer plusieurs instances ADC pour qu'elles agissent en tant que périphériques d'entrée sur le même cluster ou sur différents clusters ou espaces de noms. Après avoir configuré les instances, vous pouvez affecter chaque instance à différentes applications en fonction de la stratégie d'entrée.

Vous pouvez créer et déployer une configuration d'entrée à l'aide de Kubernetes `kubectl` ou d'API. Vous pouvez également configurer et déployer une entrée depuis Citrix ADM.

Vous pouvez spécifier les aspects suivants de l'intégration de Kubernetes dans ADM :

- **Cluster** : vous pouvez enregistrer ou annuler l'enregistrement des clusters Kubernetes pour lesquels ADM peut déployer des configurations d'entrée. Lorsque vous enregistrez un cluster

dans Citrix ADM, spécifiez les informations du serveur d'API Kubernetes. Sélectionnez ensuite un agent ADM capable d'atteindre le cluster Kubernetes et de déployer des configurations d'entrée.

- **Stratégies** : les stratégies d'entrée sont utilisées pour sélectionner l'instance ADC en fonction du cluster ou de l'espace de noms pour déployer une configuration d'entrée. Spécifiez les informations relatives au cluster, au site et à l'instance lorsque vous ajoutez une stratégie.
- **Configuration d'entrée** —Cette configuration est la configuration de Kubernetes Ingress, qui inclut les règles de commutation de contenu et les chemins d'URL correspondants des microservices et de leurs ports. Vous pouvez également spécifier les certificats SSL/TLS (pour décharger le traitement SSL sur l'instance ADC) à l'aide des ressources secrètes Kubernetes.

Citrix ADM mappe automatiquement les configurations d'entrée aux instances ADC à l'aide des stratégies d'entrée.

Pour chaque configuration d'entrée réussie, Citrix ADM génère un StyleBook ConfigPack. Le ConfigPack représente la configuration ADC appliquée à l'instance ADC qui correspond à la configuration Ingress. Pour afficher le ConfigPack, accédez à **Applications > StyleBooks > Configurations**.

Avant de commencer

Pour utiliser des instances Citrix ADC en tant qu'appareils d'entrée sur des clusters Kubernetes, assurez-vous d'avoir :

- Cluster Kubernetes en place.
- Cluster Kubernetes enregistré dans Citrix ADM.

Configurer Citrix ADM avec un jeton secret pour gérer un cluster Kubernetes

Pour que Citrix ADM puisse recevoir des événements de Kubernetes, vous devez créer un compte de service dans Kubernetes pour Citrix ADM. Et, configurez le compte de service avec les autorisations RBAC nécessaires dans le cluster.

1. Créez un compte de service pour Citrix ADM. Par exemple, le nom du compte de service peut être `citrixadm-sa`. Pour créer un compte de service, reportez-vous à la section Utiliser plusieurs comptes de service.
2. Utilisez le rôle `cluster-admin` pour lier le compte de service Citrix ADM. Cette liaison octroie un `ClusterRole` à un compte de service à travers le cluster. Voici un exemple de commande pour lier un rôle `cluster-admin` au compte de service.


```
kubectl create clusterrolebinding citrixadm-sa-admin --clusterrole
   =cluster-admin --serviceaccount=default:citrixadm-sa
<!--NeedCopy-->
```

Après avoir lié le compte de service Citrix ADM au rôle `cluster-admin`, le compte de service dispose de l'accès à l'échelle du cluster. Pour plus d'informations, consultez la section `kubectl` Créer `clusterrolebinding`.

3. Obtenez le jeton à partir du compte de service créé.

   Par exemple, exécutez la commande suivante pour afficher le jeton du compte de service `citrixadm-sa`:

```
kubectl describe sa citrixadm-sa
<!--NeedCopy-->
```

4. Exécutez la commande suivante pour obtenir la chaîne secrète du jeton :

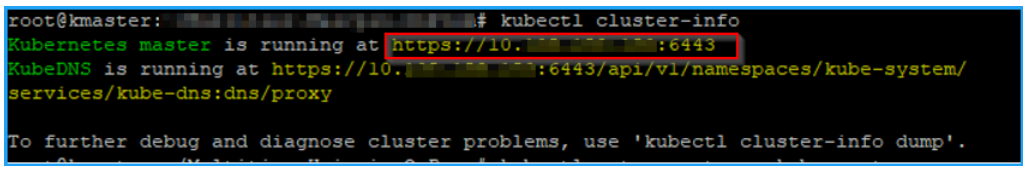
```
kubectl describe secret <token-name>
<!--NeedCopy-->
```

Ajoutez le cluster Kubernetes dans Citrix ADM

Après avoir configuré un agent Citrix ADM et configuré des itinéraires statiques, vous devez enregistrer le cluster Kubernetes dans Citrix ADM.

Pour enregistrer le cluster Kubernetes :

1. Ouvrez une session sur Citrix ADM avec les informations d'identification de l'administrateur.
2. Accédez à **Orchestration** > **Kubernetes** > **Cluster**.
   La page Clusters s'affiche.
3. Cliquez sur **Ajouter**.
4. Dans la page **Ajouter un cluster**, spécifiez les paramètres suivants :
   a) **Nom** - Indiquez un nom de votre choix.
   b) **URL du serveur API** - Vous pouvez obtenir les détails de l'URL du serveur API à partir du nœud principal Kubernetes.
      i. Sur le nœud principal Kubernetes, exécutez la commande `kubectl cluster-info`.



ii. Entrez l'URL qui s'affiche pour **"Kubernetes master est en cours d'exécution à."**

c) **Jeton d'authentification** : spécifiez la chaîne du jeton d'authentification obtenue lorsque vous configurez Citrix ADM pour gérer un cluster Kubernetes. Le jeton d'authentification est requis pour valider l'accès pour la communication entre le cluster Kubernetes et Citrix ADM. Pour générer un jeton d'authentification :

i. Sur le nœud principal Kubernetes, exécutez les commandes suivantes :

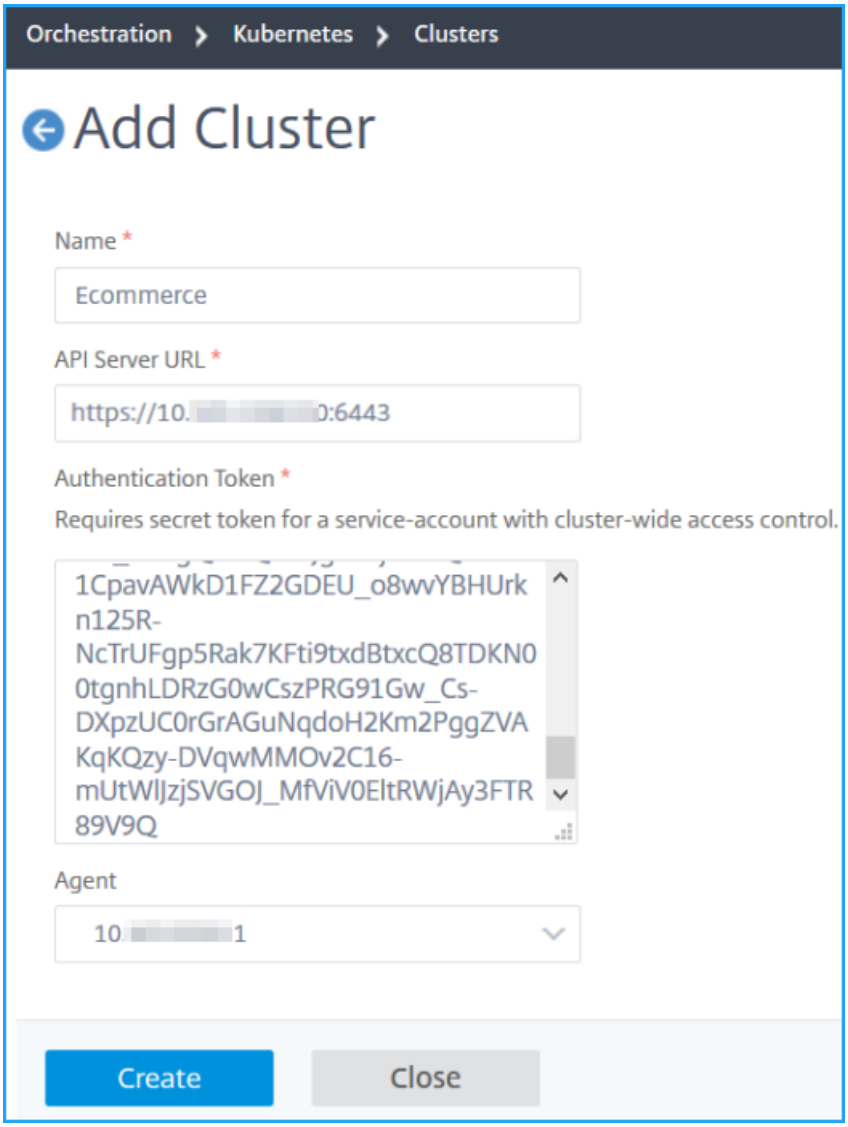
```
kubectl describe secret <token-name>
<!--NeedCopy-->
```

ii. Copiez le jeton généré et collez-le en tant que jeton d'authentification

Pour plus d'informations, consultez la documentation Kubernetes .

d) Sélectionnez l'agent dans la liste.

e) Cliquez sur **Créer**.



Définir une stratégie d'entrée

La stratégie d'entrée décide quel Citrix ADC est utilisé pour déployer une configuration d'entrée, en fonction du cluster d'entrée ou de l'espace de noms.

1. Accédez à **Orchestration > Kubernetes > Stratégie**.
2. Cliquez sur **Add** pour créer une stratégie.
    a) Spécifiez le nom de la stratégie.
    b) Définissez **les conditions** pour déployer la configuration d'entrée sur un cluster Kubernetes. Ces conditions sont généralement basées sur le cluster d'entrée et l'espace de noms.

c) Dans le panneau Infrastructure,

- **Site** : sélectionnez un site dans la liste.
- **Instance** : sélectionnez l'instance ADC dans la liste.

Les listes **Site** et **Instance** renseignent les options en fonction de la sélection du cluster dans le panneau **Conditions** .

Ces listes affichent les sites ou les instances associés à l'agent Citrix ADM configuré avec le cluster Kubernetes.

d) Dans **Choisir un réseau**, sélectionnez le réseau à partir duquel ADM attribue automatiquement les adresses IP virtuelles à une configuration d'entrée.

Cette liste affiche les réseaux créés dans **Réseaux > IPAM**.

e) Cliquez sur **Créer**.

Déployer la configuration Ingress

Vous pouvez déployer la configuration Ingress à partir de Kubernetes à l'aide de `kubectl`, de l'API Kubernetes ou d'autres outils. Vous pouvez également déployer la configuration Ingress directement depuis Citrix ADM.

1. Accédez à **Orchestration > Kubernetes > Ingresses**.
2. Cliquez sur **Ajouter**.
3. Dans le champ **Créer une entrée**, spécifiez les détails suivants :

   a) Spécifiez le nom de l'entrée.

   b) Dans **Cluster**, sélectionnez le cluster Kubernetes sur lequel vous souhaitez déployer une entrée.

   c) Sélectionnez l'**espace de noms du cluster** dans la liste. Ce champ répertorie les espaces de noms présents dans le cluster Kubernetes spécifié.

   d) Facultatif, sélectionnez **Affectation automatique de l'adresse IP frontale**.

   e) Sélectionnez **Protocole d'entrée** dans la liste. Si vous sélectionnez **HTTPS**, spécifiez un **secret TLS**.

   Ce secret intègre la ressource secrète Kubernetes qui intègre le certificat HTTPS et la clé privée.

   Une entrée HTTPS nécessite un secret basé sur TLS configuré sur le cluster Kubernetes. Spécifiez les champs `tls.crt` et `tls.key` pour inclure respectivement le certificat de serveur et la clé de certificat.

f) Pour le routage du contenu, spécifiez les informations suivantes :

- **Chemins d'URL** : spécifiez le chemin d'accès associé au service et au port Kubernetes.
- **Service Kubernetes** : spécifiez le service souhaité.
- **Port** - Spécifiez le port de service.
- **Méthode LB** : sélectionnez la méthode d'équilibrage de charge préférée pour le service Kubernetes sélectionné.

  La méthode sélectionnée met à jour la spécification d'entrée avec une annotation appropriée. Par exemple, si vous sélectionnez la méthode **ROUNDROBIN**, l'annotation Citrix s'affiche comme suit :

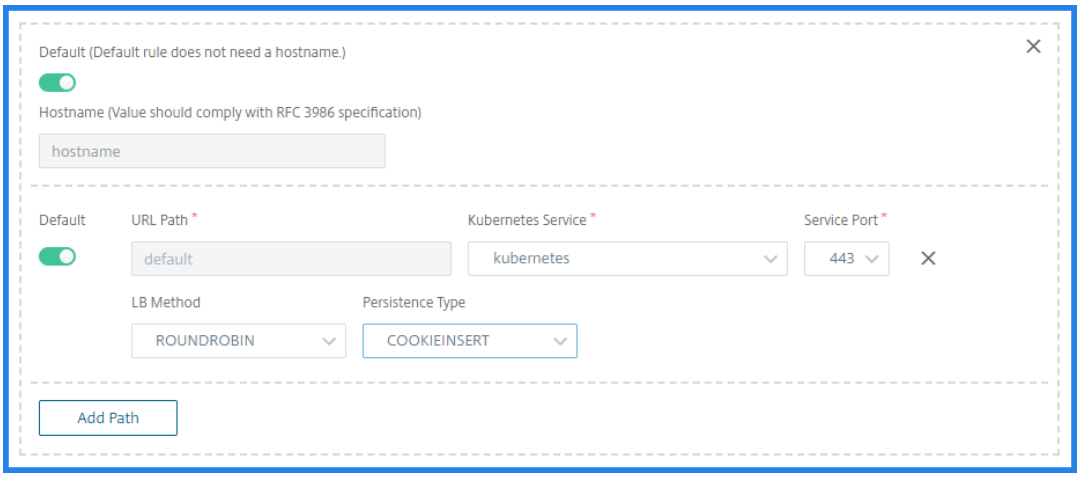
```
1  "lbmethod":"ROUNDROBIN"
2  <!--NeedCopy-->
```

- **Type de persistance :** sélectionnez le type de persistance d'équilibrage de charge préféré pour le service Kubernetes sélectionné.

  Le type de persistance sélectionné met à jour la spécification d'entrée avec une annotation appropriée. Par exemple, si vous sélectionnez **COOKIEINSERT**, l'annotation Citrix s'affiche comme suit :

```
1  "persistenceType":"COOKIEINSERT"
2  <!--NeedCopy-->
```

Cliquez sur **Ajouter** pour ajouter d'autres chemins d'URL et ports à la configuration d'entrée.



Après le déploiement, la configuration d'entrée redirige le trafic client vers un service spécifique en fonction des éléments suivants :

- Le chemin d'accès et le port d'URL demandés.

- La méthode LB et le type de persistance définis.

> **Remarque**
>
> Les services Kubernetes utilisés dans une configuration d'entrée sont censés être de type NodePort.

g) Facultatif, spécifiez une **description d'entrée**.

h) cliquez sur **Déployer**

Si vous souhaitez revoir la configuration avant le déploiement, cliquez sur **Generate Ingress Spec**. La configuration d'entrée spécifiée s'affiche au format YAML. Après avoir examiné la configuration, cliquez sur **Déployer**.

> **Remarque**
> Appliquez des licences aux serveurs virtuels créés à l'aide de configurations d'entrée. Pour appliquer une licence, effectuez les opérations suivantes :
>
> 1. Accédez à **Système > Licences et analyses**.
> 2. Sous **Récapitulatif des licences du serveur virtuel**, activez la **sélection automatique des serveurs virtuels**.

Capacité du pool de Citrix ADC

February 1, 2024

La capacité mise en commun Citrix ADC vous permet de partager des licences de bande passante ou d'instance entre différents facteurs de forme ADC. Pour les instances basées sur un abonnement à un processeur virtuel, vous pouvez partager la licence de processeur virtuel entre les instances. Utilisez cette capacité groupée pour les instances qui se trouvent dans le centre de données ou les clouds publics. Lorsqu'une instance n'a plus besoin des ressources, elle vérifie la capacité allouée dans le pool commun. Réutilisez la capacité libérée vers d'autres instances ADC qui ont besoin de ressources.

Vous pouvez utiliser les licences groupées pour optimiser l'utilisation de la bande passante en garantissant l'allocation de bande passante nécessaire à une instance et pas plus que ce dont elle a besoin. Augmentez ou diminuez la bande passante allouée à une instance au moment de l'exécution sans affecter le trafic. Avec les licences de capacité groupée, vous pouvez automatiser le Provisioning des instances.

Comment fonctionnent les licences de capacité groupées Citrix ADC

La capacité mise en pool Citrix ADC comprend les composants suivants :

- Les instances Citrix ADC, qui peuvent être classées dans les catégories suivantes :
  - Matériel à capacité nulle
  - Instances VPX autonomes ou instances CPX ou BLX
- Pool de bande passante
- Pool d'instances
- Citrix ADM configuré en tant que serveur de licences

Matériel à capacité nulle

Lorsqu'elles sont gérées via la capacité mise en pool Citrix ADC, les instances MPX et SDX sont appelées « matériel à capacité nulle », car ces instances ne peuvent pas fonctionner tant qu'elles n'ont pas extrait les ressources de la bande passante et des pools d'instances. Ainsi, ces plates-formes sont également appelées appliances MPX-Z et SDX-Z.

Le matériel à capacité nulle nécessite une licence de plate-forme pour pouvoir extraire la bande passante et une licence d'instance du pool commun.

> **Remarque**
>
> L'abonnement à une licence d'instance n'est pas requis pour les instances MPX. Reportez-vous au tableau 1 de cette page pour connaître la capacité groupée prise en charge pour les instances MPX et SDX. Voir le tableau 5 pour connaître les exigences de licence pour différents facteurs de formulaire MPX et SDX.

Gérer et installer les licences de plateforme

Vous devez installer une licence de plate-forme manuellement, en utilisant le numéro de série du matériel ou le code d'accès à la licence. Une fois qu'une licence de plate-forme est installée, elle est verrouillée sur le matériel et ne peut pas être partagée entre les instances matérielles Citrix ADC à la demande. Toutefois, vous pouvez déplacer manuellement la licence de plate-forme vers une autre instance matérielle Citrix ADC.

Les instances ADC MPX exécutant le logiciel ADC version 11.1 build 54.14 ou ultérieure et les instances SDX ADC exécutant 11.1 build 58.13 ou version ultérieure prennent en charge la capacité groupée ADC. Pour en savoir plus, voir le **tableau 1. Capacité groupée prise en charge pour les instances MPX et SDX**.

Instances Citrix ADC VPX autonomes

Les instances Citrix ADC VPX exécutant le logiciel Citrix ADC version 11.1 Build 54.14 et ultérieure sur les hyperviseurs suivants prennent en charge la capacité mise en commun :

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM

Les instances Citrix ADC VPX exécutant le logiciel Citrix ADC version 12.0 Build 51.24 et ultérieures sur les hyperviseurs et plates-formes cloud suivants prennent en charge la capacité mise en commun :

- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

> **Remarque**
>
> Pour activer la communication entre Citrix ADM et Microsoft Azure ou AWS, un tunnel IPSEC doit être configuré. Pour plus d'informations, consultez Ajouter des instances Citrix ADC VPX déployées dans le cloud à Citrix ADM.
> Contrairement au matériel à capacité nulle, VPX ne nécessite pas de licence de plate-forme. Pour traiter le trafic, il doit extraire la bande passante et une licence d'instance du pool.

Instances Citrix ADC CPX autonomes

Les instances Citrix ADC CPX déployées sur un hôte Docker prennent en charge la capacité en pool. Contrairement au matériel à capacité nulle, CPX ne nécessite pas de licence de plate-forme. Une seule instance CPX consommant jusqu'à 1 Gbit/s de débit extrait seulement 1 instance et aucune bande passante du pool de licences. Par exemple, considérez que vous avez 20 instances CPX avec un pool de bande passante de 20 Gbit/s. Si l'une des instances CPX consomme un débit de 500 Mbit/s, le pool de bande passante reste 20 Gbit/s pour les 19 instances CPX restantes.

Si la même instance CPX commence à consommer un débit de 1500 Mbit/s, le pool de bande passante a 19,5 Gbit/s pour les 19 instances CPX restantes.

Pour les licences de pool, vous pouvez ajouter plus de bande passante uniquement en multiples de 10 Mbps.

Instances Citrix ADC BLX autonomes

Les instances Citrix ADC BLX prennent en charge les licences à capacité groupée. Une instance BLX Citrix ADC ne nécessite pas de licence de plate-forme. Pour traiter le trafic, une instance Citrix ADC BLX doit extraire la bande passante et une licence d'instance du pool.

Pool de bande passante

Le pool de bande passante est la bande passante totale qui peut être partagée par les instances Citrix ADC, physiques et virtuelles. Le pool de bande passante comprend des pools distincts pour chaque édition logicielle (Standard, Advanced et Premium). Une instance Citrix ADC donnée ne peut pas avoir de bande passante provenant de différents pools récupérés simultanément. Le pool de bande passante à partir duquel il peut extraire la bande passante dépend de l'édition logicielle pour laquelle il est licencié.

Pool d'instances

Le pool d'instances définit le nombre d'instances VPX ou d'instances CPX ou BLX pouvant être gérées via la capacité groupée Citrix ADC ou le nombre d'instances VPX dans une instance SDX-Z.

Lorsqu'elle est retirée du pool, une licence déverrouille les ressources de l'instance MPX-Z, SDX-Z, VPX, CPX et BLX, y compris les CPU/PE, les cœurs SSL, les paquets par seconde et la bande passante.

> **Remarque**
>
> Le service de gestion d'un SDX-Z ne consomme pas d'instance.

Serveur de licences Citrix ADM

La capacité mise en pool Citrix ADC utilise Citrix ADM configuré en tant que serveur de licences pour gérer les licences de capacité regroupées : licences de pool de bande passante et licences de pool d'instances. Vous pouvez utiliser le logiciel Citrix ADM pour gérer les licences de capacité groupées sans licence ADM.

Lors de la récupération de licences à partir d'un pool de bande passante et d'instances, le facteur de forme Citrix ADC et le numéro de modèle matériel sur un matériel à capacité nulle déterminent

- La bande passante minimale et le nombre d'instances qu'une instance Citrix ADC doit extraire avant d'être fonctionnelle.
- La bande passante maximale et le nombre d'instances qu'un Citrix ADC peut extraire.

- L'unité de bande passante minimale pour chaque sortie de bande passante. L'unité de bande passante minimale est la plus petite unité de bande passante qu'un Citrix ADC doit extraire d'un pool. Toute extraction doit être un multiple entier de l'unité de bande passante minimale. Par exemple, si l'unité de bande passante minimale d'un Citrix ADC est de 1 Gbit/s, 100 Gbit/s peuvent être récupérés, mais pas 200 Mbit/s ou 150,5 Gbit/s. L'unité de bande passante minimale est différente de la largeur de bande minimale requise. Une instance Citrix ADC ne peut fonctionner qu'après avoir obtenu une licence avec au moins la bande passante minimale. Une fois la bande passante minimale atteinte, l'instance peut extraire plus de bande passante avec l'unité de bande passante minimale.

Les tableaux 1, 2, 3 et 4 résument la bande passante maximale, la bande passante minimale et l'unité de bande passante minimale pour toutes les instances Citrix ADC prises en charge. Le tableau 5 résume les exigences de licence pour différents facteurs de forme pour toutes les instances Citrix ADC prises en charge :

Tableau 1 Capacité groupée prise en charge pour les instances MPX et SDX

Ligne de produits	Bande passante maximale (Gbit/s)	Bande passante minimale (Gbps)	Instances minimales	Nombre maximum d'instances	Unité de bande passante minimale
MPX 5900Z	10	1	S/O	S/O	1 Gbit/s
MPX 8005Z	15	5	S/O	S/O	1 Gbit/s
MPX 8900Z	33	5	SO	SO	1 Gbit/s
MPX 8900Z FIPS	33	5	SO	SO	1 Gbit/s
MPX 14000Z series	100	20	SO	SO	1 Gbit/s
MPX 14000Z 40G series	100	20	S/O	S/O	1 Gbit/s
MPX 14000Z FIPS series	100	20	S/O	S/O	1 Gbit/s
MPX 14000Z 40S series	100	20	S/O	S/O	1 Gbit/s
MPX 15000Z series	120	20	S/O	S/O	1 Gbit/s

Ligne de produits	Bande passante maximale (Gbit/s)	Bande passante minimale (Gbps)	Instances minimales	Nombre maximum d' instances	Unité de bande passante minimale
MPX 15000Z FIPS series	120	20	S/O	S/O	1 Gbit/s
MPX 15000Z 50G series	120	20	S/O	S/O	1 Gbit/s
MPX 115XX series	42	15	S/O	S/O	1 Gbit/s
MPX 22000Z series	120	40	S/O	S/O	1 Gbit/s
MPX 24000Z series	150	100	S/O	S/O	1 Gbit/s
MPX 25000Z 40G	200	100	S/O	S/O	1 Gbit/s
MPX 25000ZA	200	100	S/O	S/O	1 Gbit/s
MPX 26000Z series	200	100	S/O	S/O	1 Gbit/s
MPX 26000Z 100G series	200	100	S/O	S/O	1 Gbit/s
MPX 26000Z 50S series	200	100	S/O	S/O	1 Gbit/s
SDX 8015Z	15	7	1	5	1 Gbit/s
SDX 8900Z	33	10	2	7	1 Gbit/s
SDX 115XX series	42	8	2	20	1 Gbit/s
SDX 14000Z series	100	10	2	25	1 Gbit/s
SDX 14000Z 40G series	100	10	2	25	1 Gbit/s
SDX 14000Z 40S series	100	20	10	25	1 Gbit/s

Ligne de produits	Bande passante maximale (Gbit/s)	Bande passante minimale (Gbps)	Instances minimales	Nombre maximum d'instances	Unité de bande passante minimale
SDX 14000Z FIPS series	100	10	2	25	1 Gbit/s
SDX 15000Z 50G	120	10	2 (Remarque : 5 instances pour les versions inférieures à 13.0 47.x)	55	1 Gbit/s
SDX 15000Z	120	10	2 Remarque : 5 instances pour les versions inférieures à 13.0 47.x)	55	1 Gbit/s
SDX 22000Z series	120	20	20	80	1 Gbit/s
SDX 25000Z 40G	200	50	10	115	1 Gbit/s
SDX 25000ZA	200	50	10	115	1 Gbit/s
SDX 26000Z 100G	200	50	10	115	1 Gbit/s
SDX 26000Z	200	50	10	115	1 Gbit/s
SDX 26000Z 50S	200	50	10	115	1 Gbit/s
Série SDX 24000Z	150	50	10	80	1 Gbit/s

> Remarque
>
> La bande passante minimale et les instances sont applicables aux instances SDX exécutant les versions suivantes et supérieures : 11.1 64.x, 12.0 63.x, 12.1 54.x et 13.0 41.x.
>
> La quantité minimale d'achat est différente de la configuration minimale requise.

Tableau 2. Capacité groupée prise en charge pour les instances CPX

Ligne de produits	Bande passante maximale (Gbit/s)	Bande passante minimale (Mbps)	Instances minimales	Nombre maximum d'instances	Unité de bande passante minimale
CPX	10	10	1	1	10 Mbit/s

Tableau 3. Capacité groupée prise en charge pour les instances VPX sur les hyperviseurs et les services cloud

Service hyper-viseur/cloud	Bande passante maximale (Gbit/s)	Bande passante minimale (Mbps)	Instances minimales	Nombre maximum d'instances	Unité de bande passante minimale
Citrix Hypervisor	40 Gbits/s	10 Mbit/s	1	1	10 Mbit/s
VMware ESXI	100 Gbit/s	10 Mbit/s	1	1	10 Mbit/s
Linux KVM	100 Gbit/s	10 Mbit/s	1	1	10 Mbit/s
Microsoft Hyper-V	3 Gbits/s	10 Mbit/s	1	1	10 Mbit/s
AWS	30 Gbit/s	10 Mbit/s	1	1	10 Mbit/s
Azure	10 Gbit/s	10 Mbit/s	1	1	10 Mbit/s
Google Cloud	10 Gbit/s	10 Mbit/s	1	1	10 Mbit/s

> Remarque
>
> La quantité minimale d'achat est différente de la quantité minimale requise pour le système.

Tableau 4. Capacité groupée prise en charge pour les instances BLX

Ligne de produits	Bande passante maximale (Gbit/s)	Bande passante minimale (Mbps)	Instances minimales	Nombre maximum d'instances	Unité de bande passante minimale
BLX	100	10	1	1	10 Mbit/s

Tableau 5. Exigence de licence pour différents facteurs de forme

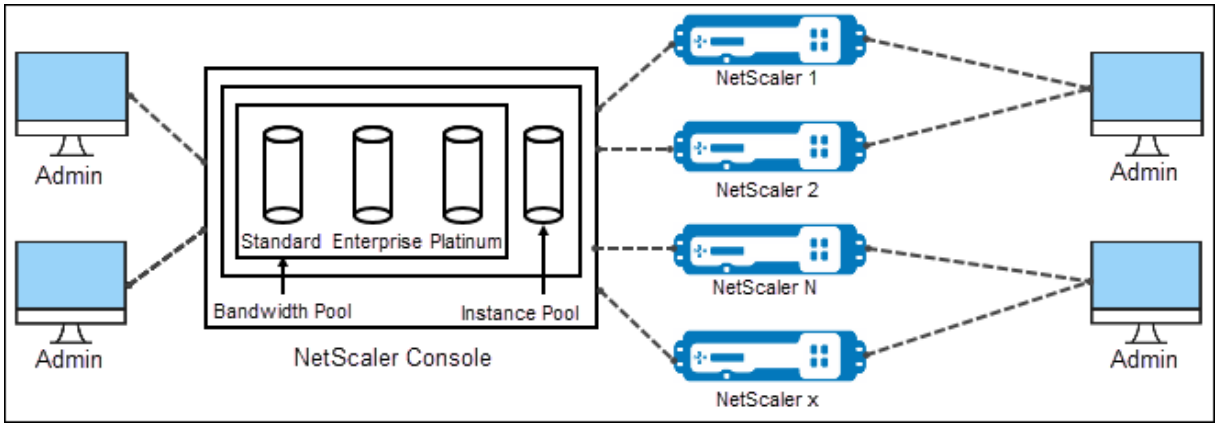
Ligne de produits	Achat de matériel à capacité nulle	Abonnement Bandwidth & Edition	Abonnement aux instances
MPX	Licence requise	Licence requise	-
SDX	Licence requise	Licence requise	Licence requise
VPX	-	Licence requise	Licence requise
CPX	-	-	Licence requise
BLX	-	Licence requise	Licence requise

Configurer la capacité du pool de Citrix ADC

February 1, 2024

Pour utiliser la capacité mise en pool ADC, configurez Citrix ADM en tant que serveur de licences pour les instances ADC requises. Les instances ADC enregistrent et extraient les licences auprès de l'ADM. Vous pouvez effectuer les tâches suivantes dans l'interface graphique d'ADM :

- Chargez les fichiers de licences de capacité groupée (bande passante et pool d'instances) sur le serveur de licences.
- Allouer des licences du pool de licences aux instances Citrix ADC à la demande.
- Consultez les licences des instances Citrix ADC (MPX-Z /SDX-Z/VPX/CPX/BLX) en fonction de la capacité minimale et maximale de l'instance.
- Configurez la capacité mise en pool pour les instances FIPS Citrix ADC afin d'archiver ou de retirer des licences.



Versions matérielles et logicielles prises en charge

Pour connaître les versions matérielles et logicielles prises en charge pour la capacité mise en pool, reportez-vous à la section Capacité groupée Citrix ADC.

États de capacité groupée ADC

Les états de capacité groupée indiquent l'exigence de licence sur une instance ADC. Les instances ADC configurées avec une capacité groupée affichent l'un des états suivants :

- **Optimum** : l'instance fonctionne avec une capacité de licence appropriée.
- **Incompatibilité de capacité** : l'instance est en cours d'exécution avec une capacité inférieure à celle configurée par l'utilisateur.
- **Grace** : l'instance est exécutée sur une licence de grâce.
- **Grace & Mismatch** : L'instance est exécutée en mode de grâce mais avec une capacité inférieure à celle configurée par l'utilisateur.
- **Non disponible** : l'instance n'est pas enregistrée auprès d'ADM pour la gestion, ou la communication NITRO entre ADM et les instances ne fonctionne pas.
- **Non alloué** : la licence n'est pas allouée dans l'instance.

Étape 1 - Appliquer des licences dans ADM

1. Dans Citrix ADM, accédez à **Réseaux** > **Licences**.
2. Dans la section **Fichiers de licence**, sélectionnez **Ajouter un fichier de licence** et sélectionnez l'une des options suivantes :

- **Téléchargez des fichiers de licence à partir d'un ordinateur local**. Si un fichier de licence est déjà présent sur votre ordinateur local, vous pouvez le télécharger sur ADM.
- **Utilisez le code d'accès de licence**. Spécifiez le code d'accès à la licence que vous avez achetée auprès de Citrix. Sélectionnez ensuite **Obtenir des licences**. Sélectionnez ensuite **Terminer**.

> **Remarque**
>
> À tout moment, vous pouvez ajouter d'autres licences à ADM à partir des **paramètres de licence**.

3. Cliquez sur **Terminer**.

   Les fichiers de licence sont ajoutés à ADM. L'onglet **Informations d'expiration de licence** répertorie les licences présentes dans l'ADM et les jours restants avant l'expiration.

4. Dans **Fichiers de licences**, sélectionnez un fichier de licence que vous souhaitez appliquer et cliquez sur **Appliquer les licences**.

   Cette action permet aux instances ADC d'utiliser la licence sélectionnée comme capacité groupée.

Étape 2 - Enregistrez Citrix ADM en tant que serveur de licences

Pour enregistrer ADM en tant que serveur de licences sur une instance Citrix ADC, suivez l'une des procédures suivantes :

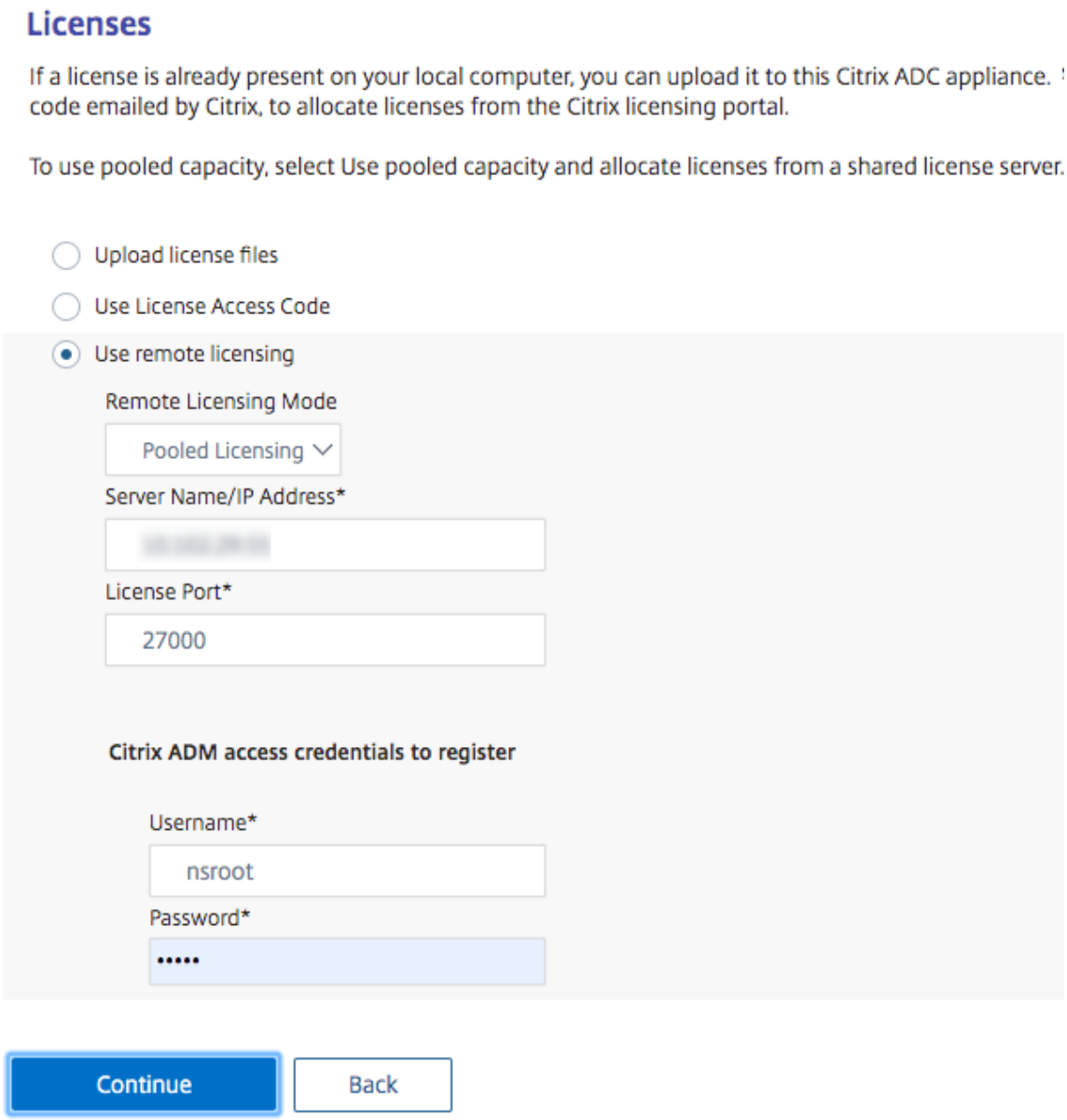
- Utiliser l'interface graphique
- Utiliser l'interface de ligne de commande

Utiliser l'interface graphique pour enregistrer ADM en tant que serveur de licences

Dans l'interface graphique ADC, enregistrez le serveur ADM en tant que serveur de licences.

1. Connectez-vous à l'interface graphique Citrix ADC.
2. Accédez à **Système** > **Licences** > **Gérer les licences**.
3. Cliquez sur **Ajouter une nouvelle licence**.
4. Sélectionnez **Utiliser les licences à distance**, puis sélectionnez le mode de licence à distance dans la liste.
5. Dans le champ **Nom du serveur/adresse IP**, spécifiez l'adresse IP du serveur ADM.
6. Sélectionnez **Enregistrer auprès de Citrix ADM**.

7. Entrez vos informations d'identification ADM pour enregistrer une instance auprès de Citrix ADM et cliquez sur **Continuer**.



8. Dans **Allouer des licences**, sélectionnez l'édition de la licence et spécifiez la bande passante requise.

   Pour la première fois, allouez des licences dans Citrix ADC. Vous pouvez ultérieurement modifier ou libérer l'allocation de licence à partir de l'interface graphique d'ADM.

9. Cliquez sur **Obtenir licences**.

> **Important**
>
> Redémarrez l'instance à chaud si vous modifiez l'édition de la licence. Les modifications

> de configuration ne prennent effet que lorsque vous redémarrez l'instance.

Utiliser la CLI pour ajouter ADM en tant que serveur de licences

Si une instance ADC ne possède pas d'interface graphique, utilisez les commandes CLI suivantes pour ajouter le serveur ADM en tant que serveur de licences :

1. Connectez-vous à la console ADC.
2. Ajoutez l'adresse IP du serveur ADM :

```
> add ns licenseserver <adm-server-IP-address> -port <adm-server-port-number>
<!--NeedCopy-->
```

3. Affichez la bande passante de licence disponible sur le serveur de licences :

```
> sh ns licenseserverpool
<!--NeedCopy-->
```

4. Allouez la bande passante de licence à partir de l'édition de licence requise :

```
> set ns capacity -unit gbps -bandwidth <specify-license-bandwidth > edition <specify-license-edition>
<!--NeedCopy-->
```

   L'édition de licence peut être **Standard**, **Enterprise** ou **Platinum**.

   > **Important**
   >
   > Warm redémarrez l'instance si vous modifiez l'édition de la licence.
   >
   > ```
   > reboot -w
   > ```
   >
   > Les modifications de configuration ne prennent effet que lorsque vous redémarrez l'instance.

Étape 3 - Attribuer des licences groupées aux instances ADC

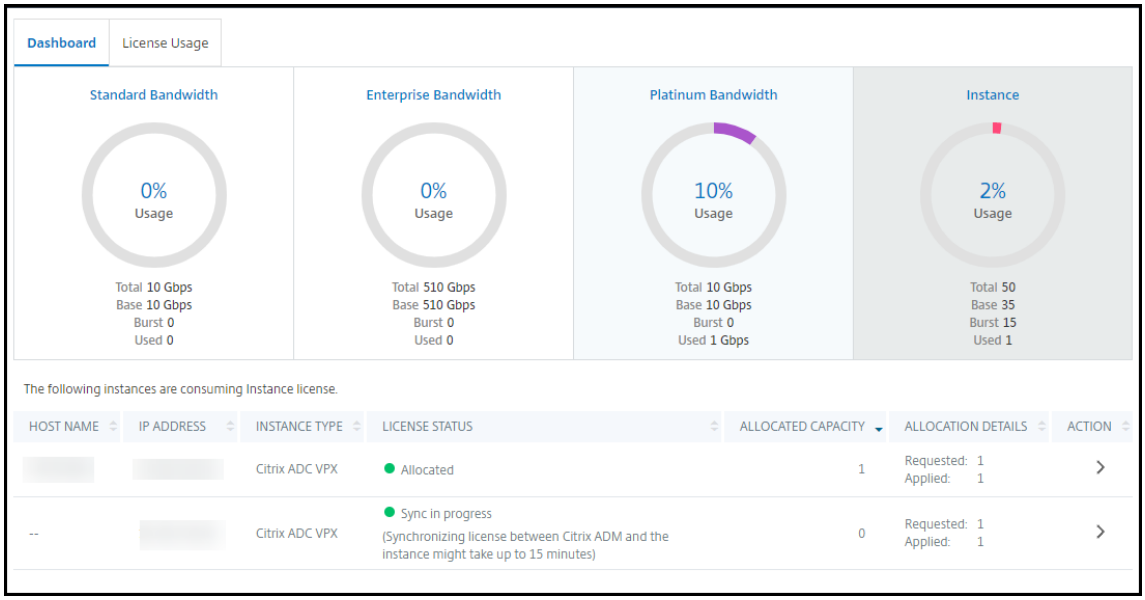
Pour allouer des licences de capacité groupées à partir de l'interface graphique d'ADM :

1. Connectez-vous à Citrix ADM.
2. Accédez à **Réseaux > Licences > Licences de bande passante > Capacité groupée**.

   La capacité d'instance FIPS n'apparaît que si vous téléchargez des licences d'instance FIPS vers ADM.
3. Cliquez sur le pool de licences que vous souhaitez gérer.

> **Remarque**
>
> Le champ **Capacité allouée** ne reflète pas immédiatement la bande passante modifiée. Le changement de bande passante prend effet après le redémarrage à chaud de l'ADC.
>
> Dans **Détails de l'allocation**, les champs **Demandéet Appliqué** sont mis à jour lorsque vous modifiez l'allocation de bande passante de l'instance.

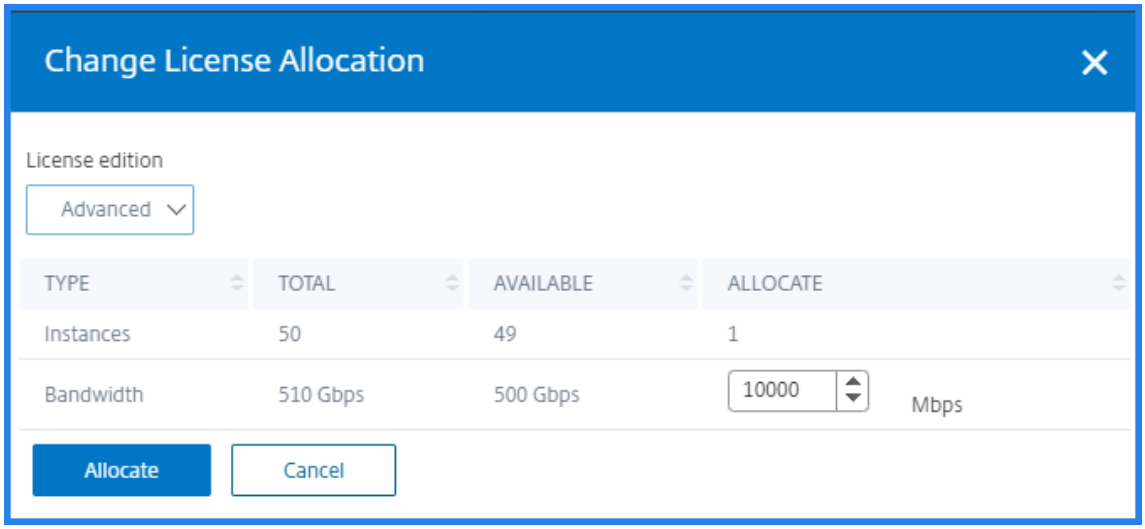
4. Sélectionnez une instance ADC dans la liste des instances disponibles en cliquant sur le bouton **>**.



La colonne **État de la licence** affiche les messages d'état d'attribution de licences correspondants.

> **Remarque**
>
> L'onglet **Instances non gérées** affiche les instances qui sont découvertes mais non gérées dans Citrix ADM.
>
> 
>

5. Cliquez sur **Change allocation** ou **Release allocation** pour modifier l'allocation de licence.
6. Une fenêtre contextuelle contenant les licences disponibles sur le serveur de licences s'affiche.
7. Vous pouvez choisir la bande passante ou l'allocation d'instance à l'instance en définissant les options de liste Allouer. Après avoir effectué vos sélections, cliquez sur **Allouer**.
8. Vous pouvez également modifier l'édition de licence allouée à partir des options de la liste de la **fenêtre Modifier l'allocation de licence**.



> **Remarque**
>
> Redémarrez à chaud une instance si vous modifiez l'édition de la licence.

Configurer la capacité mise en pool sur les instances ADC

Vous pouvez configurer des licences de capacité groupées sur les instances ADC suivantes :

- Instances ADC MPX-Z
- Instances ADC VPX
- Paire haute disponibilité ADC

Instances Citrix ADC MPX-Z

MPX-Z est l'appliance ADC MPX à capacité regroupée. MPX-Z prend en charge la mise en pool de bande passante pour les licences Premium, Advanced ou Standard Edition.

MPX-Z nécessite des licences de plate-forme avant de pouvoir se connecter au serveur de licences. Vous pouvez installer la licence de plate-forme MPX-Z de l'une des manières suivantes :

- Téléchargement du fichier de licence à partir d'un ordinateur local.
- En utilisant le numéro de série du matériel de l'instance.
- Le code d'accès à la licence de la section **Système** > **Licences** de l'interface graphique de l'instance.

Si vous supprimez la licence de plate-forme MPX-Z, la fonctionnalité de capacité groupée est désactivée. Les licences d'instance sont publiées sur le serveur de licences.

Vous pouvez modifier dynamiquement la bande passante d'une instance MPX-Z sans redémarrer. Un redémarrage n'est requis que si vous souhaitez modifier l'édition de la licence.

> **Remarque**
>
> Lorsque vous redémarrez l'instance, elle extrait automatiquement les licences groupées requises pour sa capacité configurée.

Instances Citrix ADC VPX

Une instance ADC VPX activée pour la capacité mise en commun peut extraire des licences à partir d'un pool de bande passante (éditions Premium/Avancées/Standard). Vous pouvez utiliser l'interface graphique ADC pour extraire des licences à partir du serveur de licences.

Vous pouvez modifier dynamiquement la bande passante d'une instance VPX sans redémarrer. Un redémarrage n'est requis que si vous souhaitez modifier l'édition de la licence.

> **Remarque**
>
> Lorsque vous redémarrez l'instance, les licences de capacité groupées configurées sont automatiquement extraites du serveur ADM.

Paire haute disponibilité Citrix ADC

Avant de commencer, assurez-vous que le serveur ADM est configuré en tant que serveur de licences. Pour plus d'informations, consultez Configurer ADM en tant que serveur de licences.

Pour les instances ADC configurées en mode haute disponibilité, vous devez configurer la capacité groupée sur chaque nœud de la paire haute disponibilité. Pour les nœuds principal et secondaire, vous devez allouer des licences de même capacité. Par exemple, si vous voulez une capacité de 1 Gbit/s pour chaque instance de la paire HA, vous avez besoin du double de la capacité (2 Gbit/s) du pool commun. Vous pouvez ensuite allouer une capacité de 1 Gbit/s à chaque nœud.

Pour allouer une licence de pool à chaque nœud de la paire, suivez les étapes indiquées dans Allouer des licences groupées aux instances ADC. Allouez d'abord la licence au premier nœud, puis répétez les mêmes étapes pour attribuer la licence au second nœud.

Configurer un serveur ADM uniquement en tant que serveur de licences groupé

February 1, 2024

En tant qu'administrateur, vous ne pouvez configurer un serveur ADM qu'en tant que serveur de licences groupé. Avec cette configuration, le serveur ADM reçoit uniquement les données de licence des instances ADC.

Parfois, vous pouvez avoir le mandat réglementaire qui exige de restreindre les données des instances ADC de quitter la zone de réglementation. Dans de telles situations, vous pouvez déployer une instance locale d'un serveur ADM sur site dans votre zone réglementaire pour utiliser les fonctionnalités de gestion, de surveillance et d'analyse. Lorsque vous suivez la même approche pour utiliser la fonctionnalité de licences groupées, vous devez répartir les licences groupées entre différents serveurs de licences ADM. Cette approche ne vous offre pas la flexibilité d'allouer des licences groupées entre vos instances ADC déployées dans le monde entier.

Par conséquent, configurez le serveur ADM uniquement en tant que serveur de licences groupé. Le serveur ADM reçoit uniquement les données de licence de toutes les instances ADC. Ainsi, vous pouvez respecter le mandat réglementaire et allouer dynamiquement des licences de capacité groupée entre des instances ADC déployées dans le monde entier.

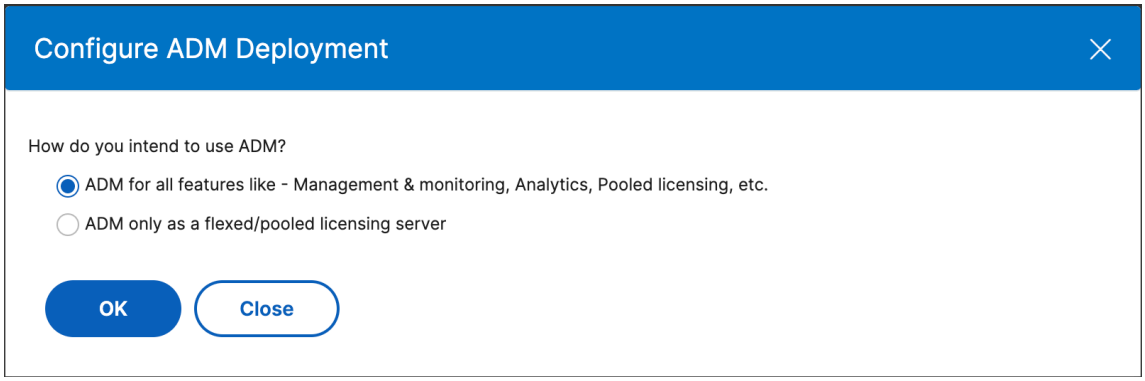
Ce document explique comment configurer un serveur ADM uniquement en tant que serveur de licences groupé.

Comment configurer un serveur ADM uniquement en tant que serveur de licences groupé

Avant de commencer, assurez-vous qu'aucune instance ADC n'est ajoutée à un serveur ADM. Ajoutez les instances ADC uniquement après avoir terminé l'étape 4.

Pour configurer un serveur ADM uniquement pour le serveur de licences groupé, procédez comme suit :

1. Accédez à **Système > Administration**.
2. Dans la section **Configurations système**, sélectionnez **Déploiement du système**.
3. Dans le **déploiement ADM**, sélectionnez **ADM uniquement en tant que serveur de licences groupé**.



4. Cliquez sur **OK**.

   Cette action conserve uniquement la fonctionnalité de licence groupée et désactive les fonctionnalités ADM suivantes :

   - Sauvegarde ADM
   - Gestion d'événements
   - Gestion des certificats SSL
   - Rapports sur le réseau
   - Fonctions réseau
   - Audit de configuration

   > **Remarque**
   >
   > Par défaut, la fonctionnalité d'analyse ADM est désactivée. Assurez-vous de désactiver cette fonctionnalité si vous l'avez activée.

   Dans la zone de confirmation, cliquez sur **Oui**.

   L'interface graphique ADM affiche désormais uniquement la fonctionnalité de gestion des licences groupées. Et, les entités restantes n'apparaissent pas.

5. Après avoir configuré ADM uniquement pour la fonction de licence, ajoutez des instances ADC dans la page **Réseaux > Instances**.

> **Remarque**
>
> - Vous pouvez ajouter une instance ADC dans un ou plusieurs serveurs ADM. Lorsque vous modifiez le mot de passe de telles instances ADC, veillez à mettre à jour le mot de passe sur tous les serveurs ADM où l'instance est découverte.
> - Un utilisateur peut toujours effectuer certaines opérations sur les fonctionnalités désactivées dans l'interface graphique ADM. Par exemple, l'interrogation des événements et la sauvegarde ADC. En tant que super-administrateur, Si vous souhaitez restreindre de telles opérations, désactivez les accès utilisateur pour les autres administrateurs à l'aide d'une stratégie d'accès appropriée. Pour plus d'informations, consultez Configurer les stratégies d'accès sur Citrix ADM.

Mettre à niveau une licence perpétuelle dans Citrix ADC VPX vers une capacité mise en commun Citrix ADC

February 1, 2024

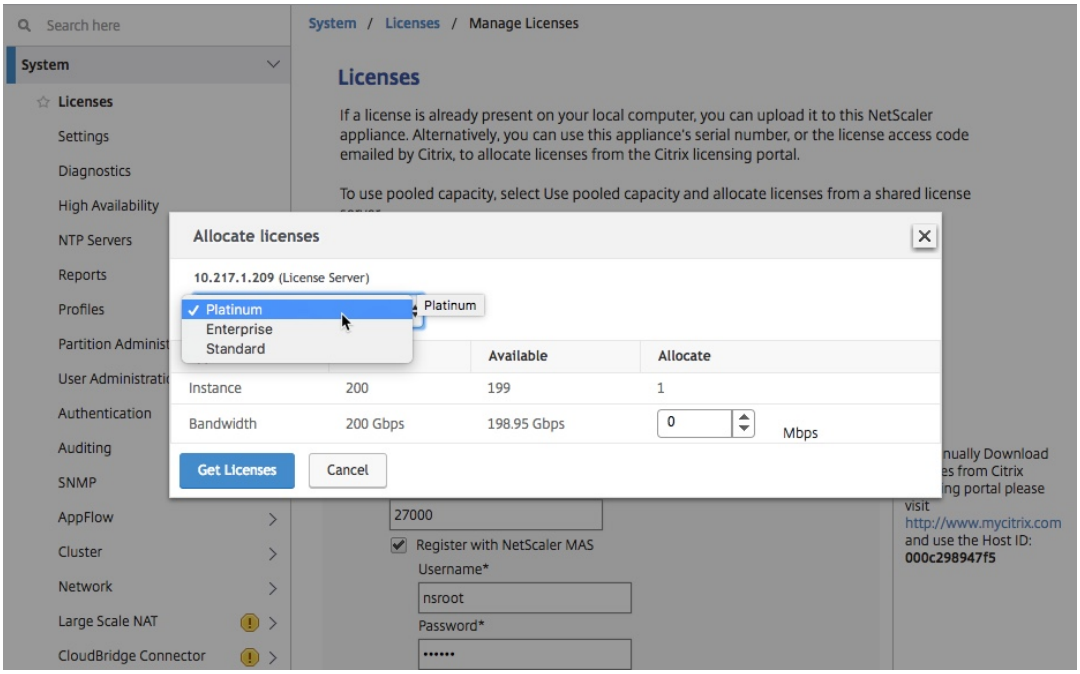
Les instances Citrix ADC VPX avec licence perpétuelle peuvent être mises à niveau vers une licence de capacité groupée ADC. La mise à niveau vers une licence de capacité groupée vous permet d'allouer des licences du pool de licences aux instances VPX à la demande. Vous pouvez également configurer une licence de capacité groupée pour les instances ADC configurées en mode haute disponibilité. Pour configurer la licence de capacité groupée pour les instances VPX en mode haute disponibilité, reportez-vous à la section Mise à niveau de la licence perpétuelle dans la paire haute disponibilité Citrix ADC VPX vers la capacité groupée Citrix ADC.

Conditions préalables

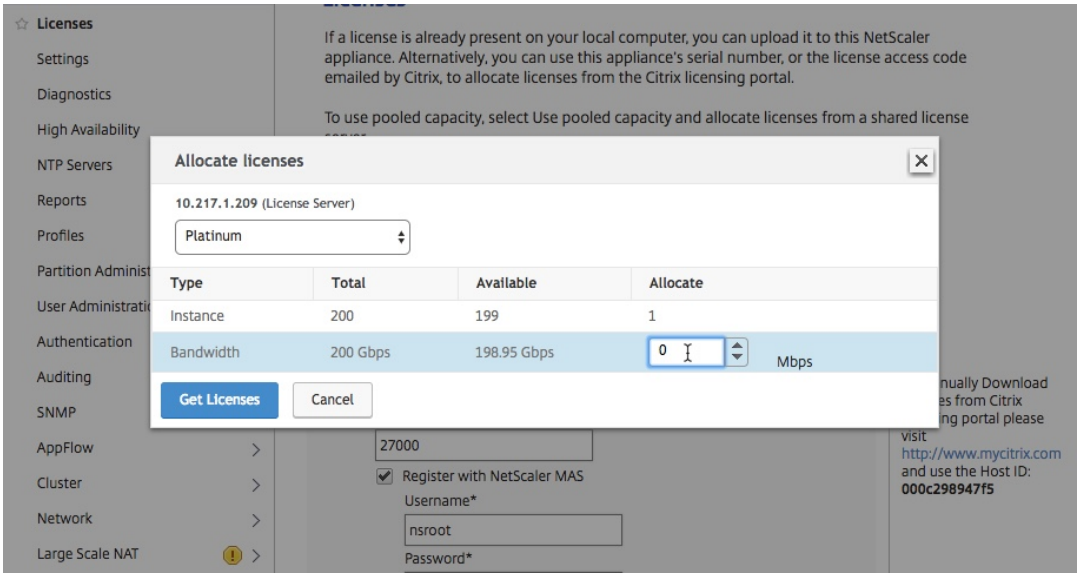
Assurez-vous de mettre à niveau l'instance VPX vers la version 12.0.56.x.

Pour mettre à niveau la capacité mise en commun Citrix ADC :

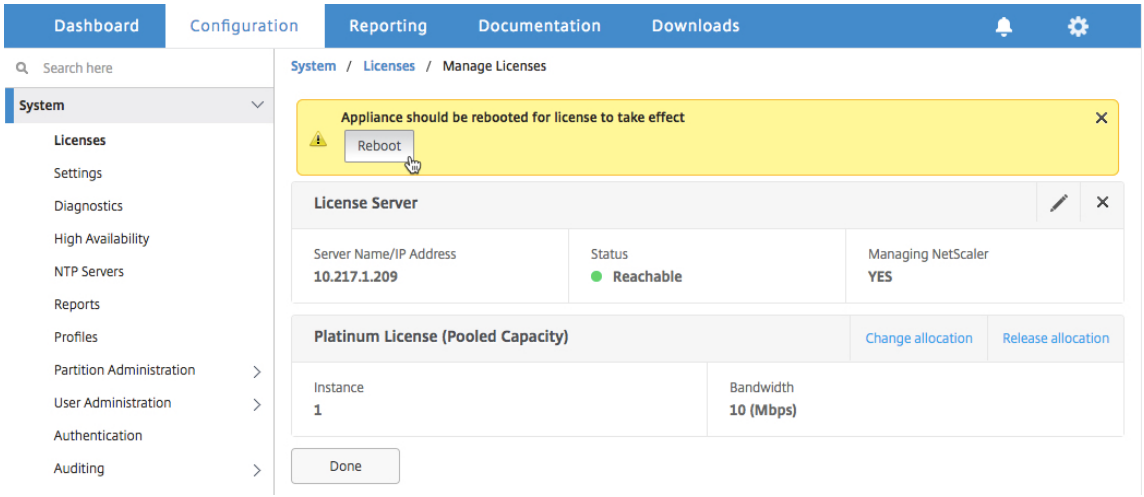
1. Dans un navigateur Web, saisissez l'adresse IP de l'instance VPX, par exemple http://192.168.100.1.
2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification de l'administrateur.
3. Sur la page **Bienvenue**, cliquez sur **Continuer**.
4. Sous l'onglet Configuration, accédez à **Système > Licences**, puis cliquez sur **Gérer les licences**.
5. Sur la page **Licences**, cliquez sur **Ajouter une nouvelle licence**.
6. Sur la page **Licences**, choisissez **Utiliser les licences distantes** et procédez comme suit :
    a) Dans la liste déroulante **Mode de gestion des licences à distance**, choisissez **Licences groupées**.
    b) Dans le champ **Nom du serveur/Adresse IP**, entrez les détails du serveur de licences.
    c) Assurez-vous que la case à cocher **Enregistrer auprès de Citrix ADM** est activée et entrez les informations d'identification Citrix ADM si vous souhaitez gérer les licences de pool de votre instance via ADM.
    d) Cliquez sur **Continuer**.
7. Dans la fenêtre **Allouer des licences**, procédez comme suit :
    a) Sélectionnez l'édition de licence dans la liste déroulante.



b) Affectez la bande passante à l'appliance Citrix ADC à partir du menu **Allouer** et cliquez sur **Obtenir des licences**.



8. Lorsque vous y êtes invité, cliquez sur **Redémarrer** pour redémarrer l'appliance.



9. Dans la boîte de dialogue Confirmer, cliquez sur **Oui** .
10. Après le redémarrage de l'instance VPX, connectez-vous à l'instance. Sur la page **Bienvenue**, cliquez sur **Continuer**.

    La page **Licences** affiche toutes les fonctionnalités qui sont concédées sous licence sur l'appliance Citrix ADC VPX. Cliquez sur **X**.
11. Accédez à **Système > Licences** et cliquez sur **Gérer les licences**.

    Sur la page **Gérer les licences**, vous pouvez afficher les détails du serveur de licences, de l'édition de licence et de la bande passante allouée.

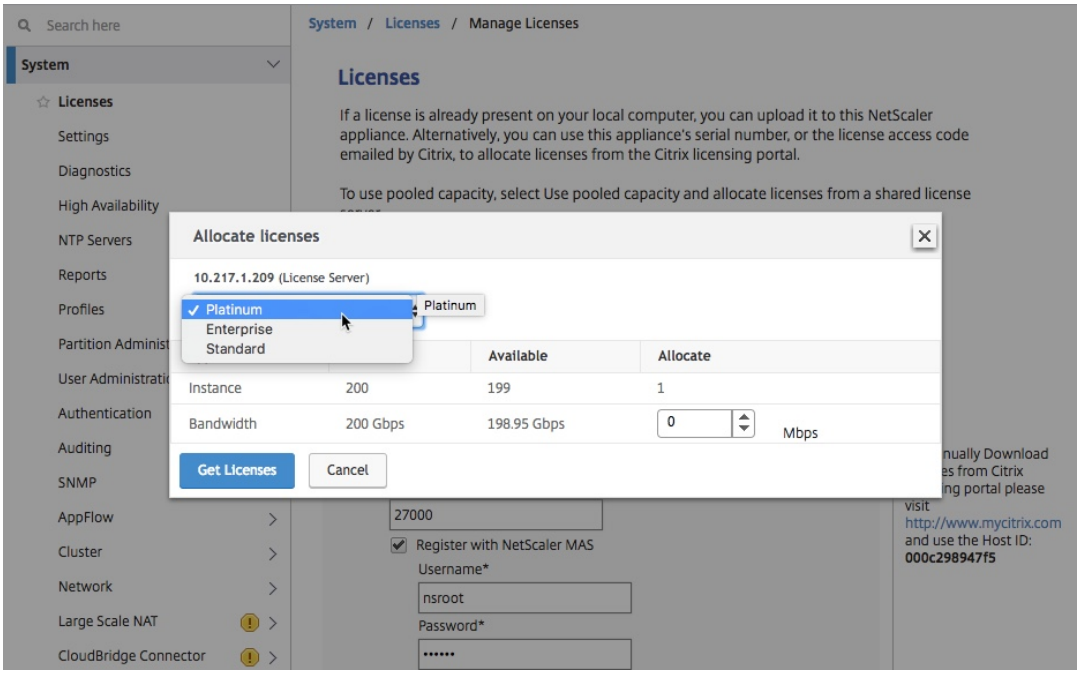
Mettre à niveau la licence perpétuelle dans la paire haute disponibilité Citrix ADC VPX vers la capacité mise en commun Citrix ADC

Pour les instances VPX configurées en mode haute disponibilité, vous devez configurer la capacité groupée sur les instances principale et secondaire de la paire HA. Pour les instances principales et secondaires, vous devez allouer des licences de même capacité. Par exemple, si vous voulez une capacité de 1 Gbit/s pour chaque instance de la paire HA, vous avez besoin du double de la capacité (2 Gbit/s) du pool commun. Vous pouvez ensuite allouer une capacité de 1 Gbit/s chacune aux instances principale et secondaire de la paire HA.

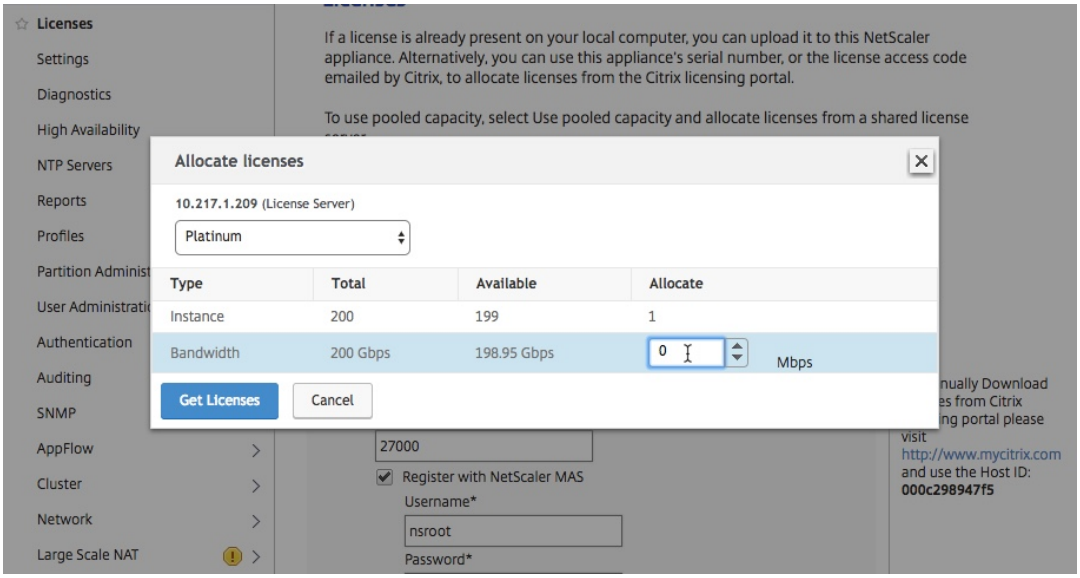
Pour mettre à niveau une configuration Citrix ADC VPX HA existante vers la capacité mise en pool Citrix ADC :

1. Ouvrez une session sur l'instance VPX secondaire (nœud 2). Dans un navigateur Web, tapez l'adresse IP de l'appliance Citrix ADC, par exemple `http://192.168.100.1`.
2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification de l'administrateur.

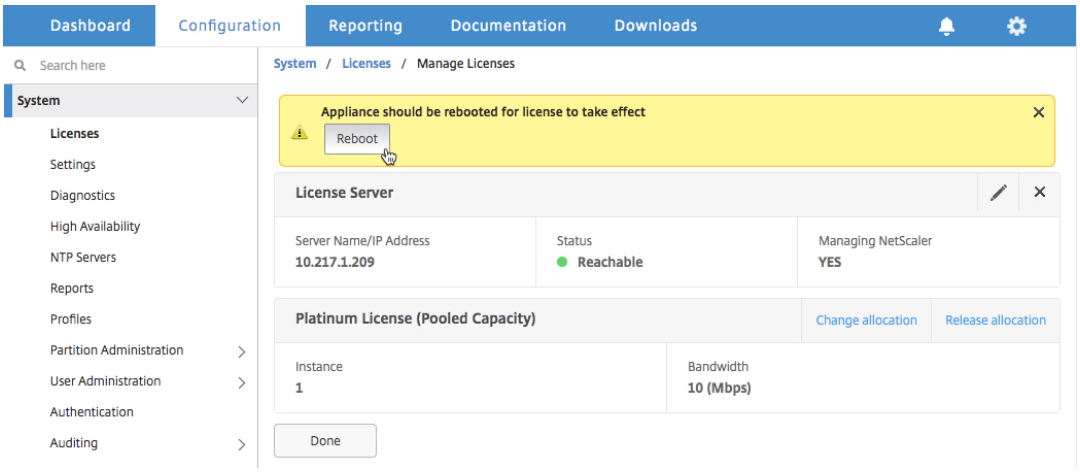
3. Sur la page **Bienvenue**, cliquez sur **Continuer**.
4. Dans l'onglet Configuration, accédez à **Système** > **Licences** et cliquez sur **Gérer les licences** .
5. Sur la page **Licences**, cliquez sur **Ajouter une nouvelle licence**.
6. Sur la page **Licences**, choisissez **Utiliser les licences distantes** et procédez comme suit :
   a) Dans la liste déroulante **Mode de gestion des licences à distance**, choisissez **Licences groupées**.
   b) Dans le champ **Nom du serveur/Adresse IP**, entrez les détails du serveur de licences.
   c) Assurez-vous que la case à cocher **Enregistrer auprès de Citrix ADM** est activée et entrez les informations d'identification ADM, si vous souhaitez gérer les licences de pool de votre instance via Citrix ADM.
   d) Cliquez sur **Continuer**.
7. Dans la fenêtre Allouer des licences, procédez comme suit :
   a) Sélectionnez l'édition de licence dans la liste déroulante.



   b) Affectez la bande passante à l'appliance Citrix ADC à partir du menu **Allouer** et cliquez sur **Obtenir des licences**.



c) Lorsque vous y êtes invité, cliquez sur **Redémarrer** pour redémarrer l'instance à chaud.



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

   L'instance VPX redémarre.

   Lorsque vous y êtes invité, cliquez sur Redémarrer pour redémarrer l'appliance. Une fois que l'appliance est opérationnelle avec la nouvelle licence, forcez un basculement en tapant `force ha failover`. Ce basculement garantit que la paire HA est en bon état.

9. Ouvrez une session sur l'instance VPX principale existante (nœud 1) et redémarrez-la. Effectuez les étapes suivantes.

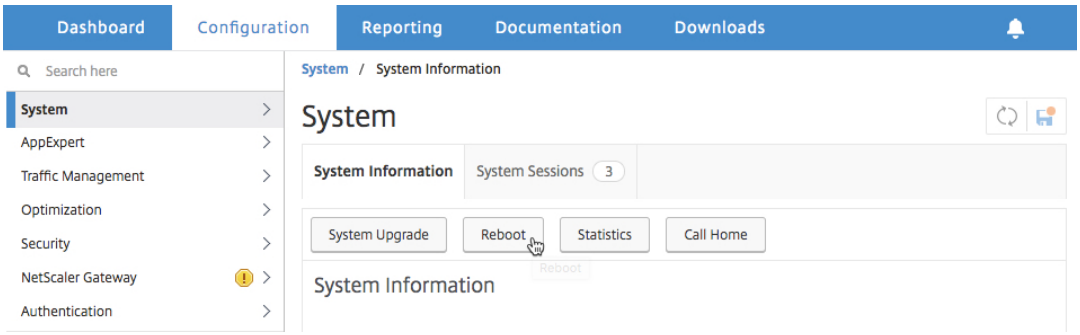
   a) Dans un navigateur Web, tapez l'adresse IP de l'appliance Citrix ADC, par exemple http://192.168.100.1.

   b) Dans les champs **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification de l'administrateur.

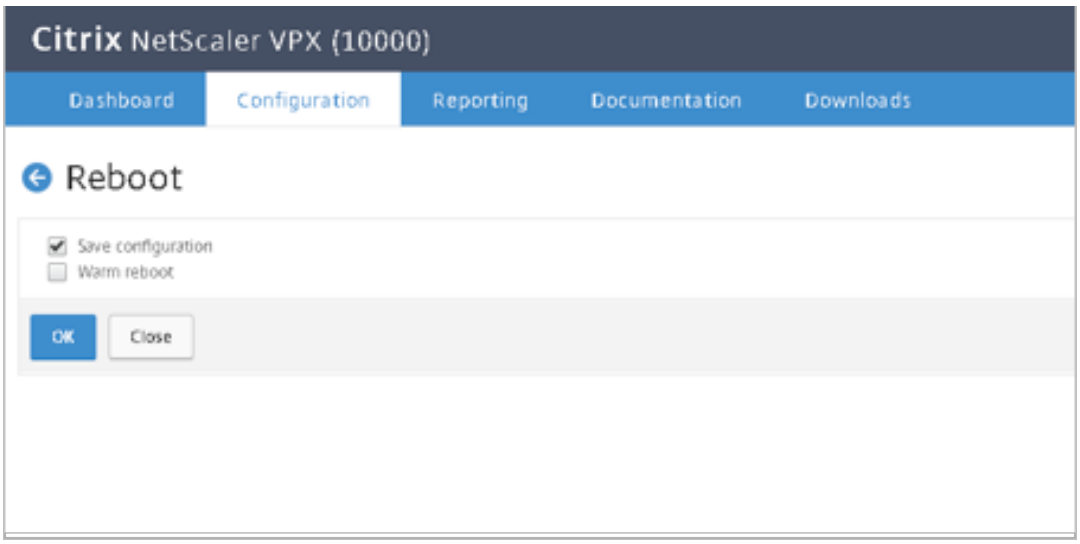
c) Sur la page **Bienvenue**, cliquez sur **Continuer**.

d) Dans l'onglet **Configuration**, cliquez sur **Système**.

e) Sur la page **Système**, cliquez sur **Redémarrer**.



f) Sur la page **Redémarrage**, sélectionnez **Redémarrage à chaud** et cliquez sur **OK**.



Après le redémarrage du nœud 1, il devient l'instance secondaire de la paire HA. Si vous souhaitez remplacer l'instance principale et secondaire de la paire HA par votre configuration de paire HA d'origine, forcez un basculement. Exécutez la commande suivante sur n'importe quelle instance de la paire HA :

‘‘‘

```
force ha failover
```

10. Pour vérifier que l'instance VPX est mise à niveau vers une licence de capacité groupée, connectez-vous aux instances principale et secondaire et effectuez les étapes suivantes.

a) Sur la page **Bienvenue**, cliquez sur **Continuer**.

b) Sous l'onglet Configuration, accédez à **Système > Licences**, puis cliquez sur **Gérer les licences**. Sur la page **Gérer les licences**, vous pouvez afficher les détails du serveur de

licences, de l'édition de licence et de la bande passante allouée.

Mise à niveau d'une licence perpétuelle dans Citrix ADC MPX vers Citrix ADC Pooled Capacity

February 1, 2024

L'appliance Citrix ADC MPX avec licence perpétuelle peut être mise à niveau vers la licence Citrix ADC Pooled Capacity. La mise à niveau vers la licence Citrix ADC Pooled Capacity vous permet d'allouer des licences à partir du pool de licences aux appliances Citrix ADC à la demande. Vous pouvez également configurer la licence Citrix ADC Pooled Capacity pour les instances Citrix ADC configurées en mode haute disponibilité. Pour configurer la licence de capacité groupée Citrix ADC pour les instances Citrix ADC MPX en mode haute disponibilité, reportez-vous à la section Mise à niveau de la licence perpétuelle dans la paire haute disponibilité Citrix ADC MPX vers la capacité groupée Citrix ADC.

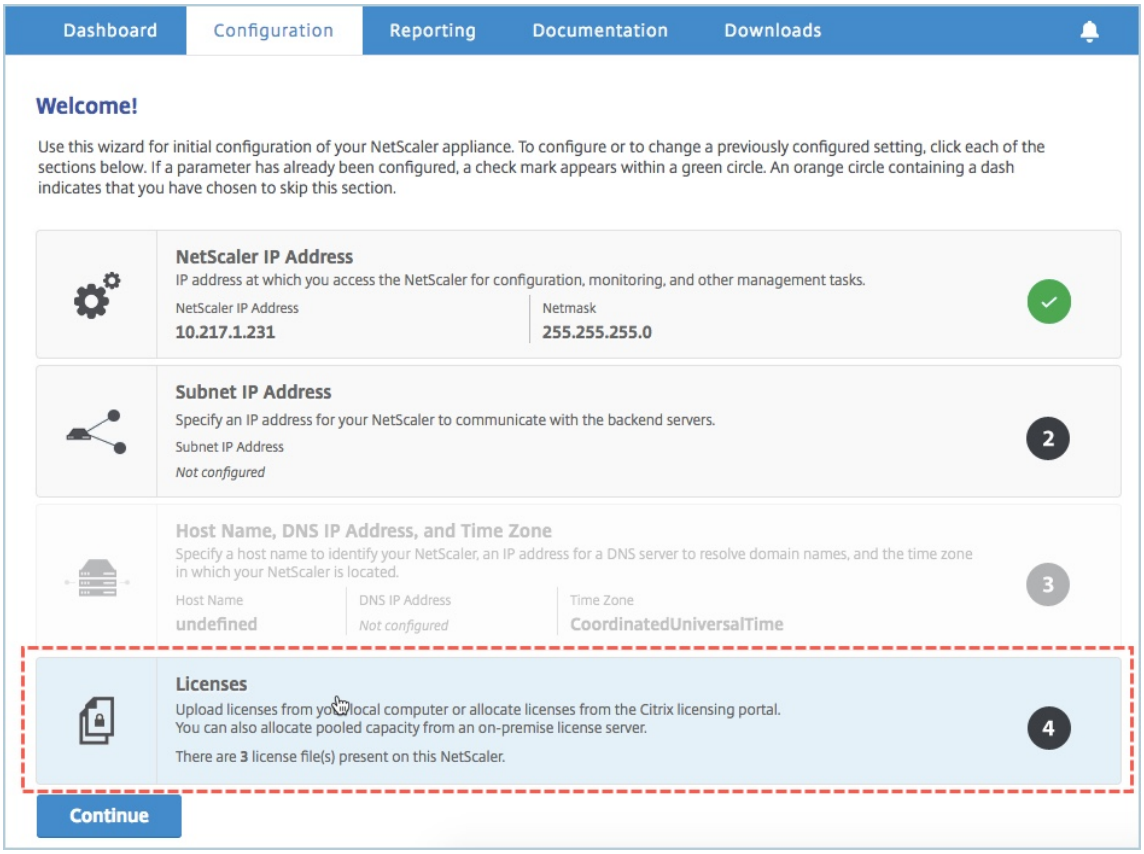
> **Remarque**
>
> La conversion d'une licence perpétuelle à une licence de capacité groupée est un processus à sens unique pour l'octroi d'une licence. Vous ne pouvez pas rétablir la licence de capacité groupée à perpétuelle.
>
> **Important**
>
> Pour mettre à niveau l'appliance Citrix ADC MPX vers la licence Citrix ADC Pooled Capacity, vous devez télécharger la licence MPX-Z vers l'appliance.

Pour effectuer la mise à niveau vers la capacité groupée Citrix ADC :

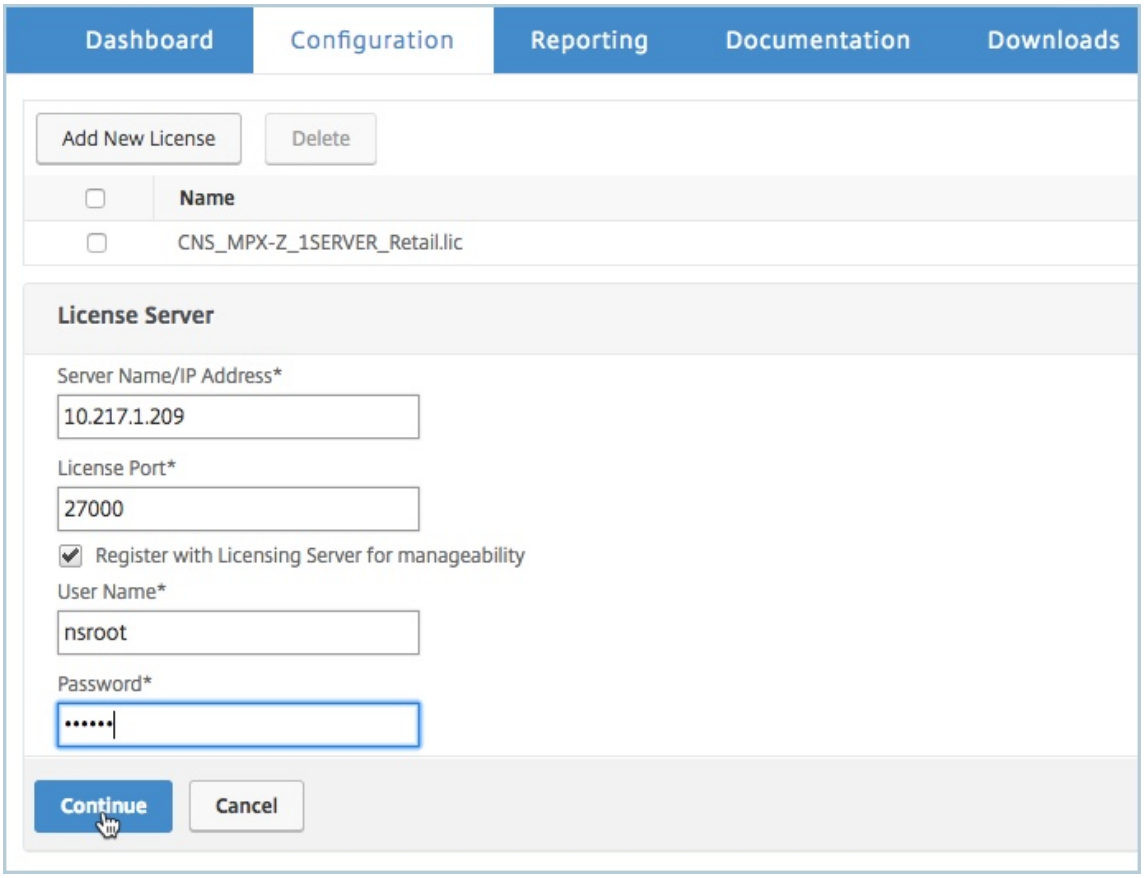
1. Dans un navigateur Web, tapez l'adresse IP de l'appliance Citrix ADC, par exemple http://192.168.100.1.
2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification de l'administrateur.
3. Sur la page **Bienvenue**, cliquez sur **Continuer**.
4. Téléchargez la licence à capacité nulle (licence MPX-Z). Sous l'onglet Configuration, accédez à **Système** > **Licences**.
5. Dans le volet d'informations, cliquez sur **Gérer les licences** , puis sur Ajouter une **nouvelle licence** .
6. Dans la page **Licences**, sélectionnez **Charger des fichiers de licence** et cliquez sur **Parcourir** pour sélectionner la licence de capacité nulle de votre machine locale.
7. Une fois la licence téléchargée, cliquez sur **Redémarrer** pour redémarrer l'appliance.

> **Avertissement**
>
> Après l'application de la licence MPX-Z, les fonctionnalités, y compris le déchargement SSL sur l'appliance, deviennent sans licence. L'appliance arrête le traitement des demandes HTTPS.
>
> Si l'option **Accès sécurisé uniquement** est activée sur l'appliance avant la mise à niveau, vous ne pouvez pas vous connecter à l'appliance via l'interface graphique Citrix ADM, à l'aide de HTTPS.

8. Sur la page **Confirmer**, cliquez sur **Oui**.
9. Après le redémarrage de l'appliance, connectez-vous à l'appliance.
10. Sur la page d'accueil, cliquez sur la section **Licences**.



11. Dans la section **Serveur de licences**, procédez comme suit :



a) Dans le champ **Nom du serveur/Adresse IP**, entrez les détails du serveur de licences.

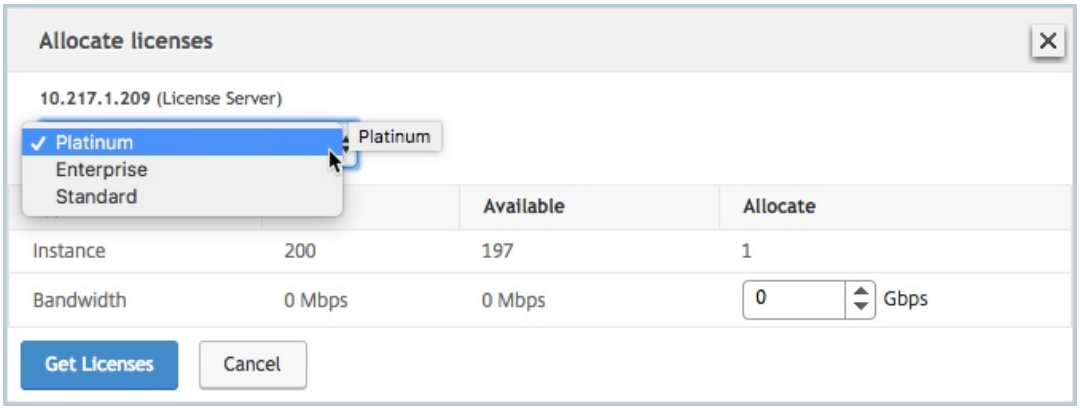
b) Dans le champ **Port de licence**, entrez le port du serveur de licences. Valeur par défaut : 27000.

c) Si vous souhaitez gérer les licences de pool de votre instance via Citrix ADM, activez la case à cocher **Enregistrer auprès du serveur de licences pour faciliter la gestion** et entrez les informations d'identification ADM.

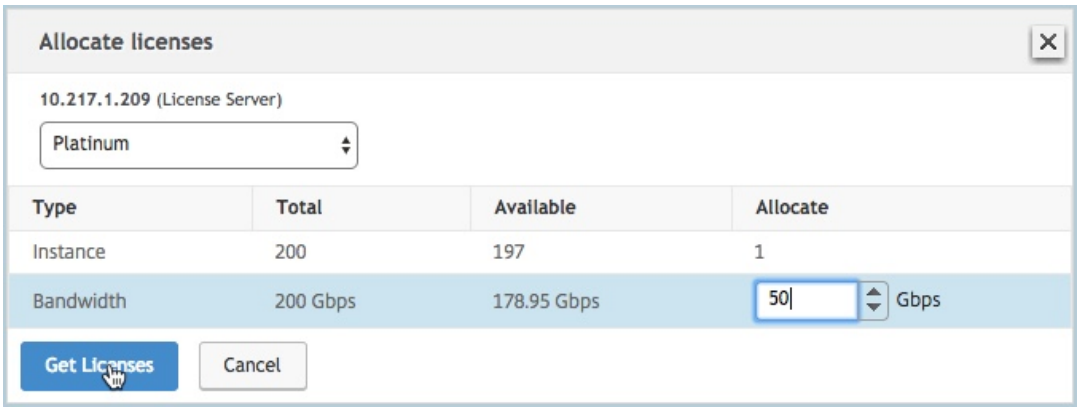
d) Cliquez sur **Continuer**.

12. Dans la fenêtre Allouer des licences, procédez comme suit :

a) Sélectionnez l'édition de licence dans la liste déroulante.



b) Affectez la bande passante à l'appliance Citrix ADC à partir du menu **Allouer** et cliquez sur **Obtenir des licences**.



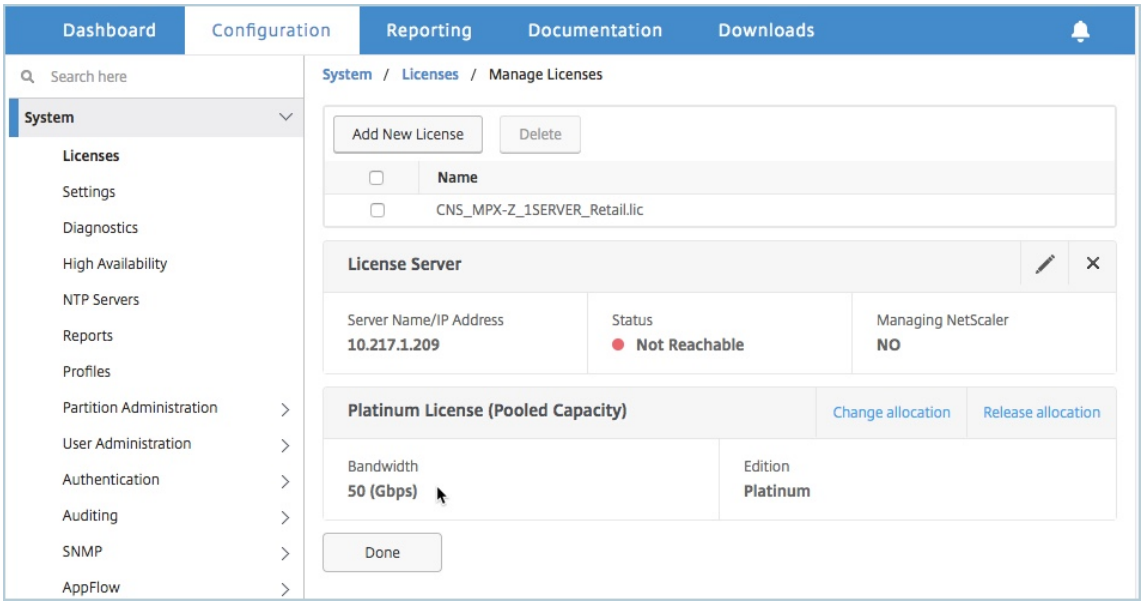
c) Lorsque vous y êtes invité, cliquez sur **Redémarrer** pour redémarrer l'appliance.

13. Une fois que l'appliance Citrix ADC MPX redémarre, connectez-vous à l'appliance Citrix ADC MPX. Sur la page **Bienvenue**, cliquez sur **Continuer**.

    La page **Licences** répertorie toutes les fonctionnalités sous licence.

14. Accédez à **Système > Licences** et cliquez sur **Gérer les licences**.

    Sur la page **Gérer les licences**, vous pouvez afficher les détails du serveur de licences, de l'édition de licence et de la bande passante allouée.



Mise à niveau de la licence perpétuelle dans la paire haute disponibilité Citrix ADC MPX vers la capacité mise en commun Citrix ADC

Pour les dispositifs MPX configurés en mode haute disponibilité, vous devez configurer la capacité groupée sur les instances ADC principale et secondaire de la paire HA. Allouez des licences de même capacité aux instances Citrix ADC principales et secondaires de la paire HA. Par exemple, si vous voulez une capacité de 1 Gbit/s pour chaque instance de la paire HA, vous devez allouer une capacité de 2 Gbit/s à partir du pool commun. Avec une capacité de 2 Gbit/s, vous pouvez allouer 1 Gbit/s chacune aux instances Citrix ADC principale et secondaire de la paire HA.

> **Important**
>
> Pour mettre à niveau l'appliance Citrix ADC MPX afin d'utiliser la licence Citrix ADC Pooled Capacity, vous devez télécharger le MPX-Z sur l'appliance.

Conditions préalables

Assurez-vous de télécharger la licence MPX-Z sur les instances principale et secondaire de la paire HA.

Pour télécharger la licence MPX-Z sur les instances Citrix ADC MPX dans la paire HA :

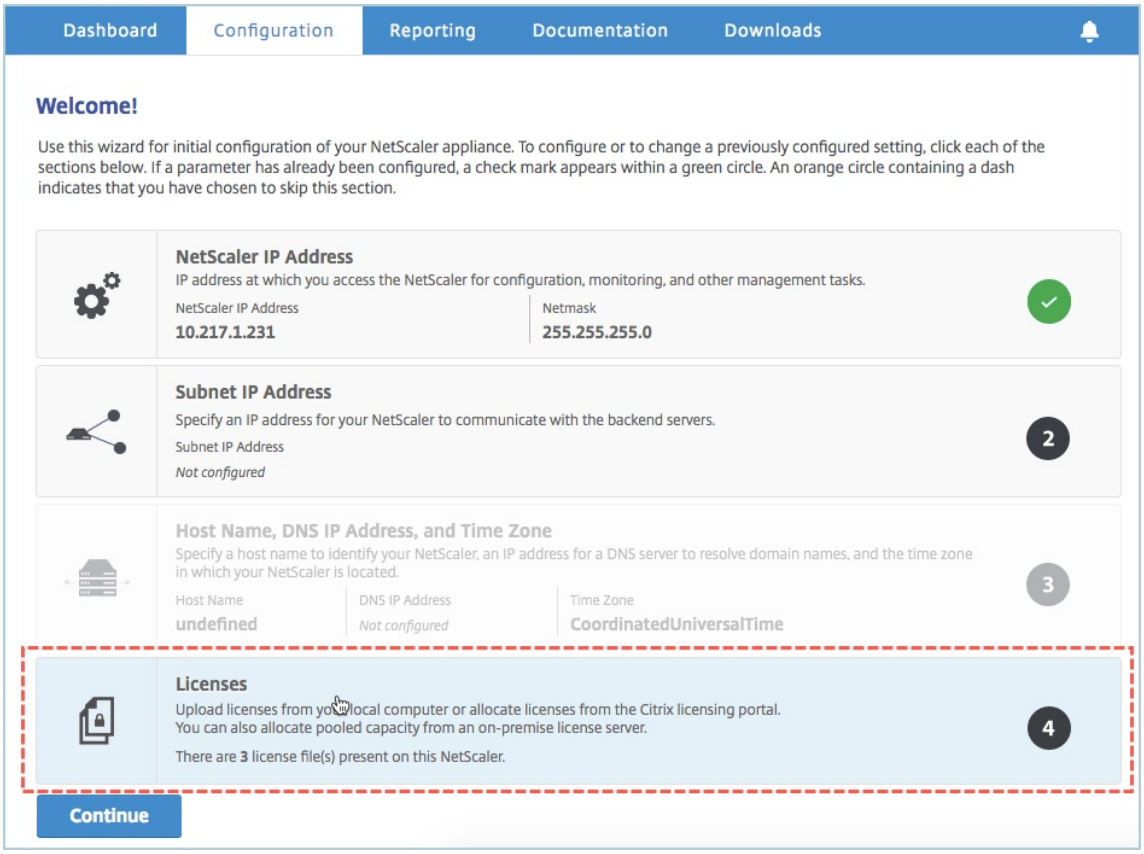
1. Dans un navigateur Web, saisissez l'adresse IP de l'appliance, telle que http://192.168.100.1.
2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification de l'administrateur.
3. Sur la page **Bienvenue**, cliquez sur **Continuer**.

4. Téléchargez la licence à capacité nulle (licence MPX-Z). Sous l'onglet **Configuration**, accédez à **Système > Licences**.
5. Dans le volet d'informations, cliquez sur **Gérer les licences**, cliquez sur **Ajouter une nouvelle licence**.
6. Dans la page **Licences**, sélectionnez **Charger des fichiers de licence** et cliquez sur **Parcourir** pour sélectionner la licence de capacité nulle de votre machine locale.

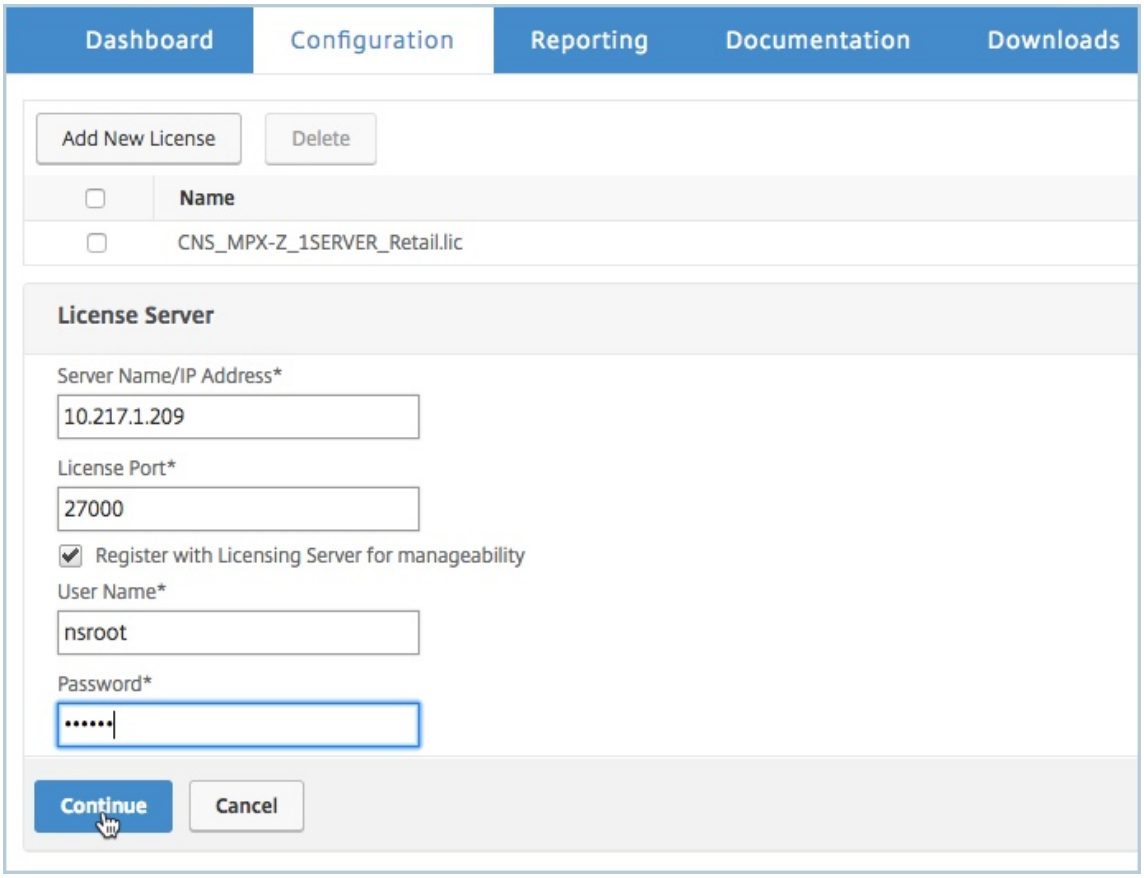
   Une fois la licence téléchargée, vous êtes invité à redémarrer l'appliance.
7. Cliquez sur **Redémarrer** pour redémarrer l'appliance.
8. Sur la page **Confirmer**, cliquez sur **Oui**.

Pour mettre à niveau une configuration HA existante vers la capacité groupée Citrix ADC :

1. Connectez-vous à l'instance secondaire Citrix ADC MPX. Dans un navigateur Web, tapez l'adresse IP de l'appliance Citrix ADC, par exemple http://192.168.100.1.
2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification de l'administrateur.
3. Sur la page d'**accueil** , cliquez sur la section **Licences** .



4. Dans la section **Serveur de licences**, procédez comme suit :



a) Dans le champ **Nom du serveur/Adresse IP**, entrez les détails du serveur de licences.

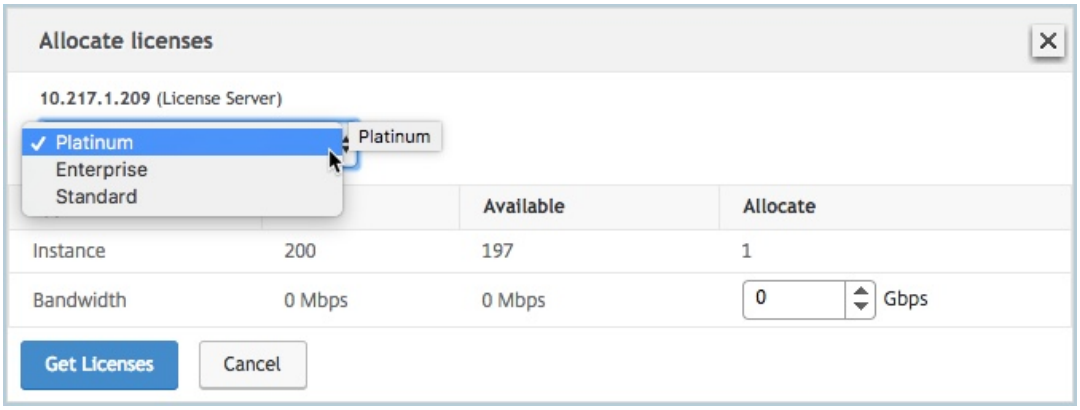
b) Dans le champ **Port de licence**, entrez le port du serveur de licences. Valeur par défaut : 27000.

c) Si vous souhaitez gérer les licences de pool de votre instance via Citrix ADM, activez la case à cocher **Enregistrer auprès du serveur de licences pour la gérabilité** et entrez les informations d'identification ADM.

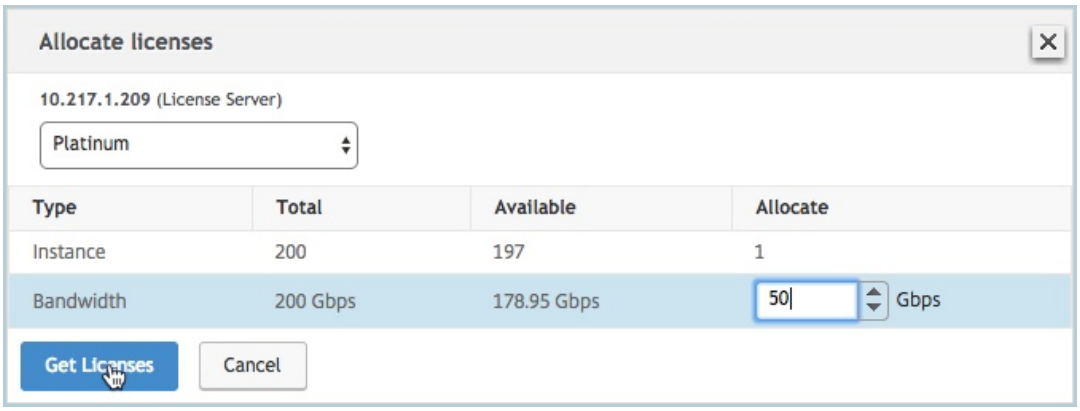
d) Cliquez sur **Continuer**.

5. Dans la fenêtre **Allouer des licences**, procédez comme suit :

a) Sélectionnez l'édition de licence dans la liste déroulante.



b) Affectez la bande passante à l'appliance Citrix ADC à partir du menu **Allouer** et cliquez sur **Obtenir des licences**.



c) Lorsque vous y êtes invité, cliquez sur Redémarrer pour **redémarrer** l'appliance. Une fois que l'appliance est opérationnelle avec la nouvelle licence, forcez un basculement en tapant `force ha failover`. Ce basculement garantit que la paire HA est en bon état.

6. Connectez-vous à l'appliance Citrix ADC MPX principale existante et redémarrez l'appliance. Procédez comme suit :

   a) Dans un navigateur Web, tapez l'adresse IP de l'appliance Citrix ADC, par exemple http://192.168.100.1.

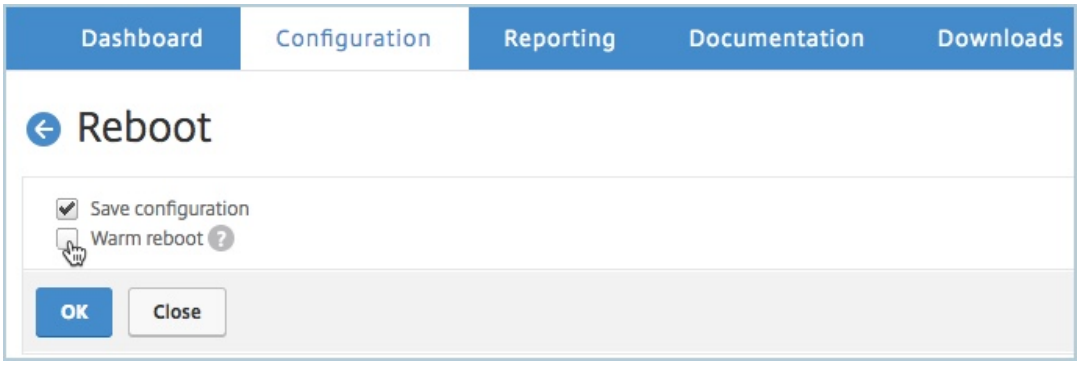
   b) Dans les champs **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification de l'administrateur.

   c) Sur la page **Bienvenue**, cliquez sur **Continuer**.

   d) Dans l'onglet **Configuration**, cliquez sur **Système**.

   e) Sur la page **Système**, cliquez sur **Redémarrer**.

   f) Sur la page **Redémarrage**, sélectionnez **Redémarrage à chaud** et cliquez sur **OK**.



Après le redémarrage de l'appliance Citrix ADC MPX principale, il devient l'appliance Citrix ADC MPX secondaire dans la paire HA. Si vous souhaitez remplacer l'instance principale et secondaire de la paire HA par votre configuration de paire HA d'origine, forcez un basculement. Exécutez la commande suivante sur n'importe quelle instance de la paire HA :

```
1 > force ha failover
2 <!--NeedCopy-->
```

Mettre à niveau une licence perpétuelle dans un SDX Citrix ADC vers une capacité groupée Citrix ADC

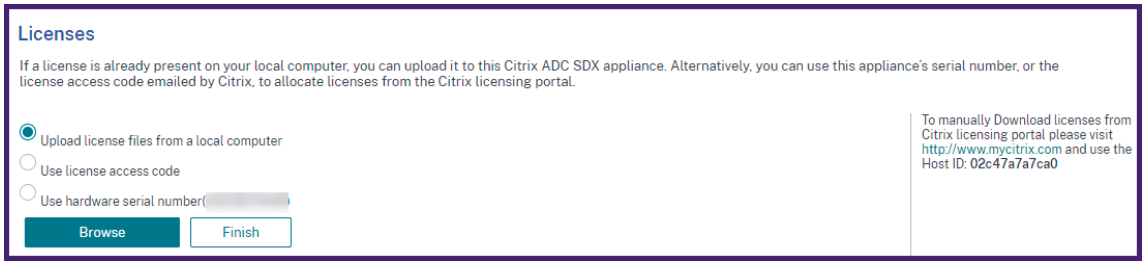
February 1, 2024

Une appliance Citrix ADC SDX avec licence perpétuelle peut être mise à niveau vers une licence Citrix ADC Pooled Capacity. La mise à niveau vers la licence Citrix ADC Pooled Capacity vous permet d'allouer des licences à partir du pool de licences aux appliances Citrix ADC à la demande. Vous pouvez également configurer la licence de capacité groupée ADC pour les instances Citrix ADC configurées en mode haute disponibilité.

> **Remarque**
>
> La conversion d'une licence perpétuelle à une licence de capacité groupée est un processus de droits de licence unidirectionnel. Vous ne pouvez pas rétablir la licence de capacité groupée à perpétuel.
>
> **Important**
>
> - Pour mettre à niveau l'appliance SDX vers la licence Citrix ADC Pooled Capacity, vous devez télécharger la licence SDX-Z sur l'appliance.
> - Assurez-vous que vous disposez de l'autorisation d'ajouter des instances ADC dans ADM.

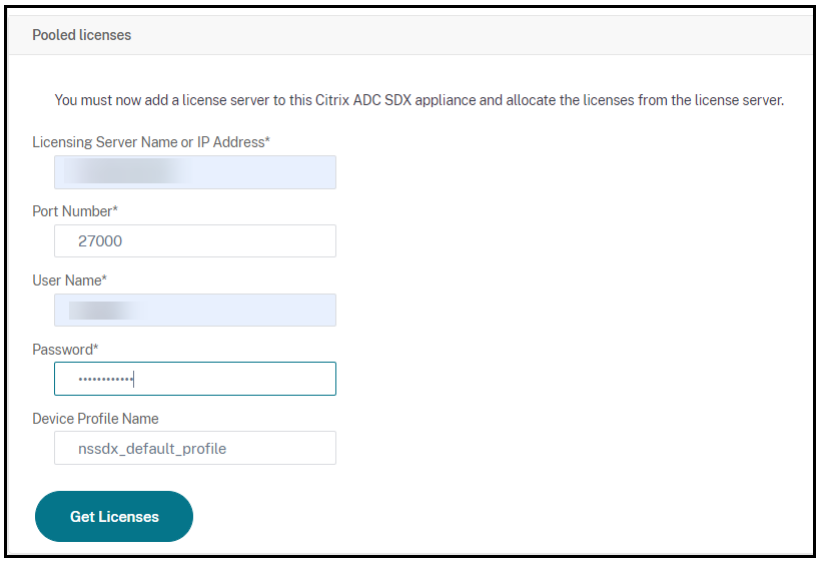
Pour effectuer la mise à niveau vers la capacité groupée Citrix ADC :

1. Dans un navigateur Web, tapez l'adresse IP de l'appliance SDX, par exemple http://192.168.100.1.
2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification de l'administrateur.
3. Sur la page **Bienvenue**, cliquez sur **Continuer**.
4. Téléchargez la licence à capacité nulle. Sous l'onglet Configuration, accédez à **Système** > **Licences**.
5. Sur la page **Gérer les licences**, cliquez sur **Ajouter un fichier de licence**.
6. Dans la page **Licences**, sélectionnez **Charger des fichiers de licence à partir d'un ordinateur local** et cliquez sur **Parcourir** pour sélectionner la licence à capacité nulle de votre machine locale. Puis, cliquez sur **Terminer**.



Une fois la licence à capacité zéro appliquée correctement, la section **Licences groupées** apparaît sur la page **Licences**.

7. Dans la section **Licences groupées**, procédez comme suit :



   a) Dans le champ **Nom du serveur de licences ou Adresse IP**, entrez les détails du serveur de licences.

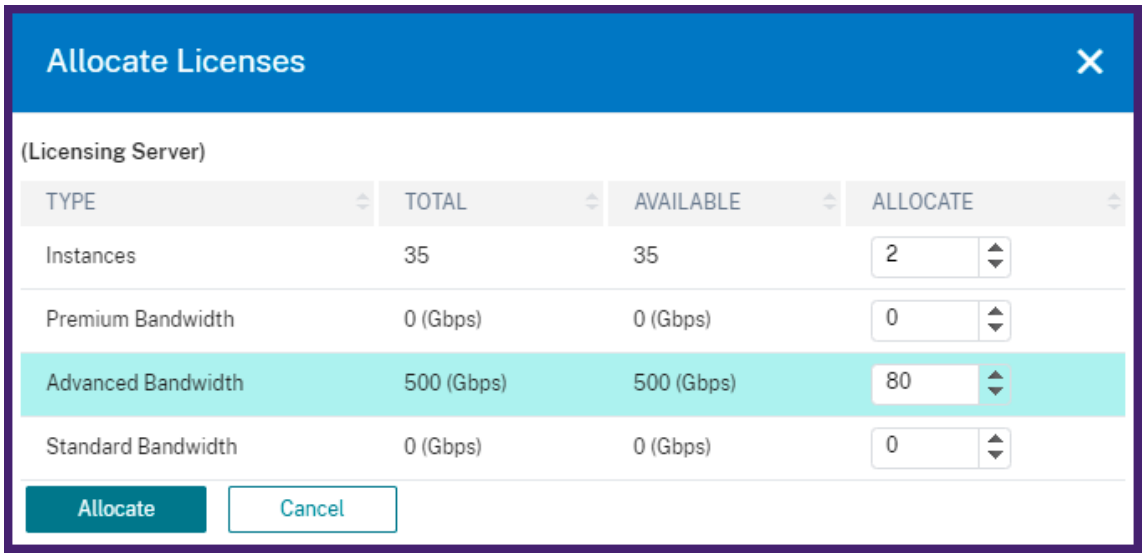
Si vous souhaitez configurer le serveur ADM en tant que serveur de licences, spécifiez l'adresse IP du serveur ADM.

Si vous utilisez un agent pour communiquer avec le serveur ADM, spécifiez l'adresse IP de l'agent ADM.

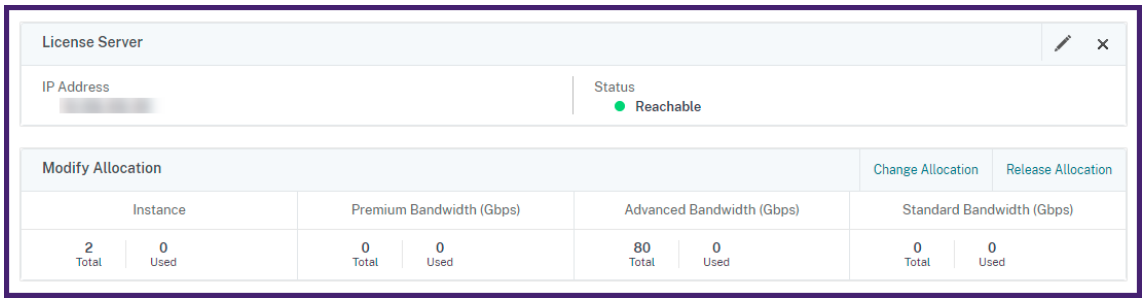
b) Dans le champ **Numéro de port**, entrez le port du serveur de licences. Valeur par défaut : 27000.

c) Cliquez sur **Obtenir licences**.

8. Dans la fenêtre **Allouer les licences**, spécifiez les instances et la bande passante requises, puis cliquez sur **Allouer**.



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**
>
> La mise à niveau d'une licence perpétuelle vers une capacité groupée ne nécessite pas le redémarrage de l'appliance SDX.

Capacité mise en commun Citrix ADC sur les instances Citrix ADC en mode cluster

February 1, 2024

Vous pouvez configurer la capacité mise en commun Citrix ADC sur les instances Citrix ADC configurées en tant que cluster. Les conditions préalables à la configuration de la capacité mise en commun sur les instances Citrix ADC en mode cluster sont les suivantes :

- Les instances s'exécutent individuellement dans un mode de licence à capacité groupée pour former le cluster.
- Toutes les instances doivent être exécutées avec la même bande passante.
- Toutes les instances ont retiré la capacité groupée du même Citrix Application Delivery Management (ADM).
- Les nouvelles instances ne peuvent pas être ajoutées à un cluster Citrix ADC existant, sauf si leur capacité et les configurations Citrix ADM sont identiques à celles des instances existantes du cluster.

Toute récupération de capacité à partir du cluster Citrix ADC affecte la même capacité à tous les nœuds de cluster et la bande passante de récupération = Bande passante fournie* nombre de nœuds.

Par exemple, si vous extrayez 50 Mbit/s de bande passante à partir du cluster Citrix ADC et que le cluster comprend 12 instances, chaque instance reçoit automatiquement 50 Mbit/s. Et, 600 Mbps sont sortis du pool.

> **Remarque**
>
> Si une ou plusieurs instances du cluster ne répondent pas, le cluster continue de traiter le trafic avec la capacité des instances restantes.

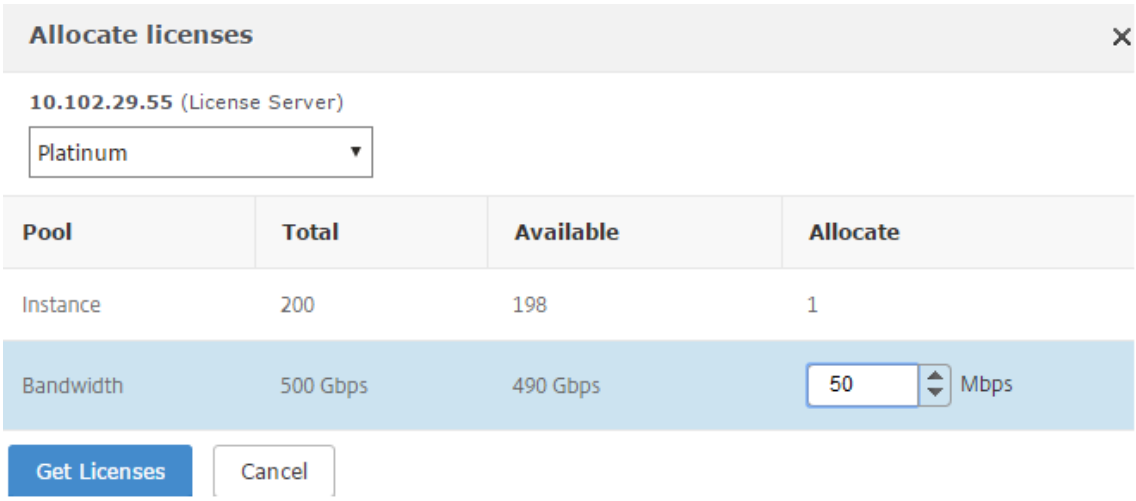
Allouer une capacité groupée ADC à un cluster ADC

Attribuez des licences à chaque nœud de cluster séparément. Parce que les commandes de propagation et de synchronisation des licences entre les nœuds du cluster sont désactivées.

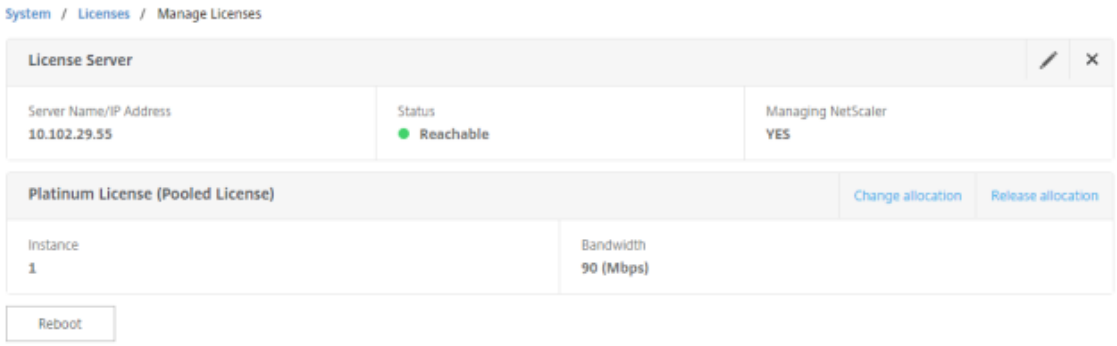
Répétez la procédure suivante sur chaque nœud de cluster :

1. Dans un navigateur Web, tapez l'adresse IP Citrix ADC (NSIP). Par exemple, `http://192.168.100.1`.
2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.

3. Dans l'onglet **Configuration**, accédez à **Système > Licences > Gérer les licences**, cliquez sur **Ajouter une nouvelle licence** et sélectionnez **Utiliser les licences groupées**.
4. Entrez le nom ou l'adresse du serveur de licences dans le champ **Nom du serveur/Adresse IP**.
5. Si vous souhaitez gérer les licences de pool de votre instance via Citrix ADM, activez la case à cocher **Enregistrer auprès de Citrix ADM pour la gérabilité** et entrez les informations d'identification ADM.
6. Sélectionnez l'édition de la licence et la bande passante requise, puis cliquez sur **Obtenir des licences**.

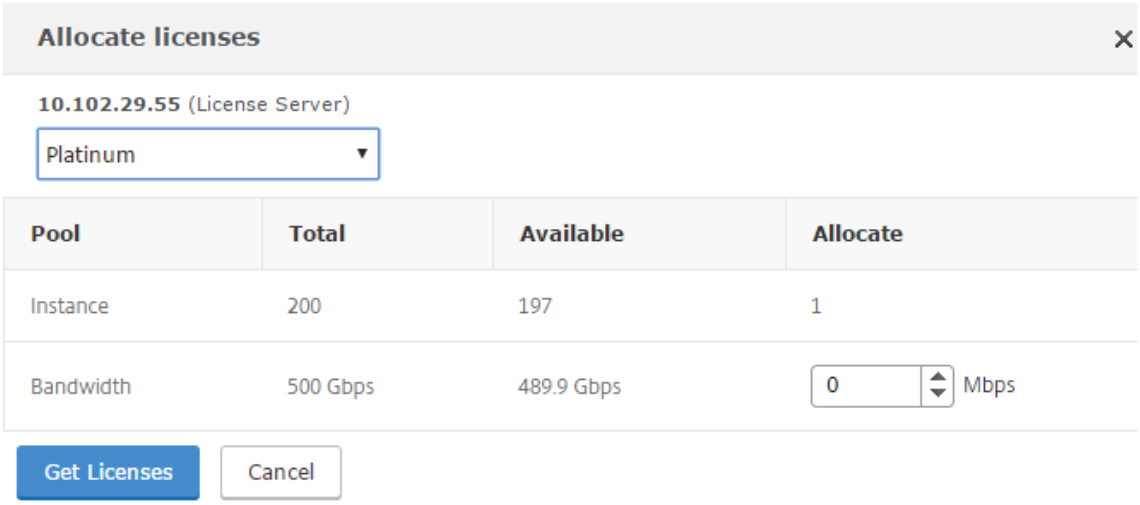


7. Vous pouvez modifier ou libérer l'allocation de licence en sélectionnant **Modifier l'allocation** ou **Libérer l'allocation** .



8. Si vous cliquez sur **Modifier l'allocation**, une fenêtre contextuelle affiche les licences disponibles sur le serveur de licences.

> **Remarque**
>
> L'allocation de bande passante doit être un multiple intégral de l'unité de bande passante minimale du facteur de forme correspondant.



9. Vous pouvez allouer de la bande passante ou des instances à l'instance Citrix ADC à partir de la liste déroulante **Allouer**. Cliquez ensuite sur **Obtenir des licences**.
10. Vous pouvez choisir l'édition de licence et la bande passante requise dans les listes déroulantes de la fenêtre contextuelle.

> **Remarque**
>
> Un redémarrage n'est pas nécessaire si vous modifiez l'allocation de bande passante, mais un redémarrage à chaud est requis si vous modifiez l'édition de la licence.

Allouer une capacité groupée ADC à un cluster ADC à l'aide de l'interface de ligne de commande

Attribuez des licences à chaque nœud de cluster séparément. Parce que les commandes de propagation et de synchronisation des licences entre les nœuds du cluster sont désactivées.

Répétez la procédure suivante sur chaque nœud de cluster :

1. Dans un client SSH, entrez l'adresse IP Citrix ADC (NSIP) et connectez-vous à l'aide des informations d'identification de l'administrateur.
2. Pour ajouter un serveur de licences, entrez la commande suivante :

```
1 add ns licenseserver (<licenseServerIP> | <serverName>) [-port <
     port number >]
2 <!--NeedCopy-->
```

```
> add ns licenseserver 10.102.29.97 -port 27000
 Done
```

3. Pour afficher les licences disponibles sur le serveur de licences, entrez la commande suivante :


```
sh licenseserverpool
<!--NeedCopy-->
```

```
> sh licenseserverpool
        Instance Total                  : 0
        Instance Available              : 0
        Standard Bandwidth Total        : 0 Mbps
        Standard Bandwidth Availabe     : 0 Mbps
        Enterprise Bandwidth Total      : 0 Mbps
        Enterprise Bandwidth Available  : 0 Mbps
        Platinum Bandwidth Total        : 0 Mbps
        Platinum Bandwidth Available    : 0 Mbps
        VPX25S Total                    : 1
        VPX25S Available                : 1
        VPX200E Total                   : 1
        VPX200E Available               : 1
        VPX1000S Total                  : 1
        VPX1000S Available              : 1
        VPX8000E Total                  : 2
        VPX8000E Available              : 1
 Done
```

4. Pour attribuer une licence à l'appliance Citrix ADC VPX, entrez la commande suivante :

```
set capacity  –platform V[S/E/P][Bandwidth]
<!--NeedCopy-->
```

```
> set capacity -platform VE8000
Warning: The configuration changes will not take effect until the system is rebooted
```

Contrôle de l'intégrité

February 1, 2024

Le serveur de licences surveille en permanence l'intégrité de l'instance à capacité groupée Citrix ADC. Les instances communiquent par le biais de messages périodiques au serveur de licences. Si quelques messages consécutifs ne sont pas reçus, le serveur de licences signale que la connectivité a été perdue.

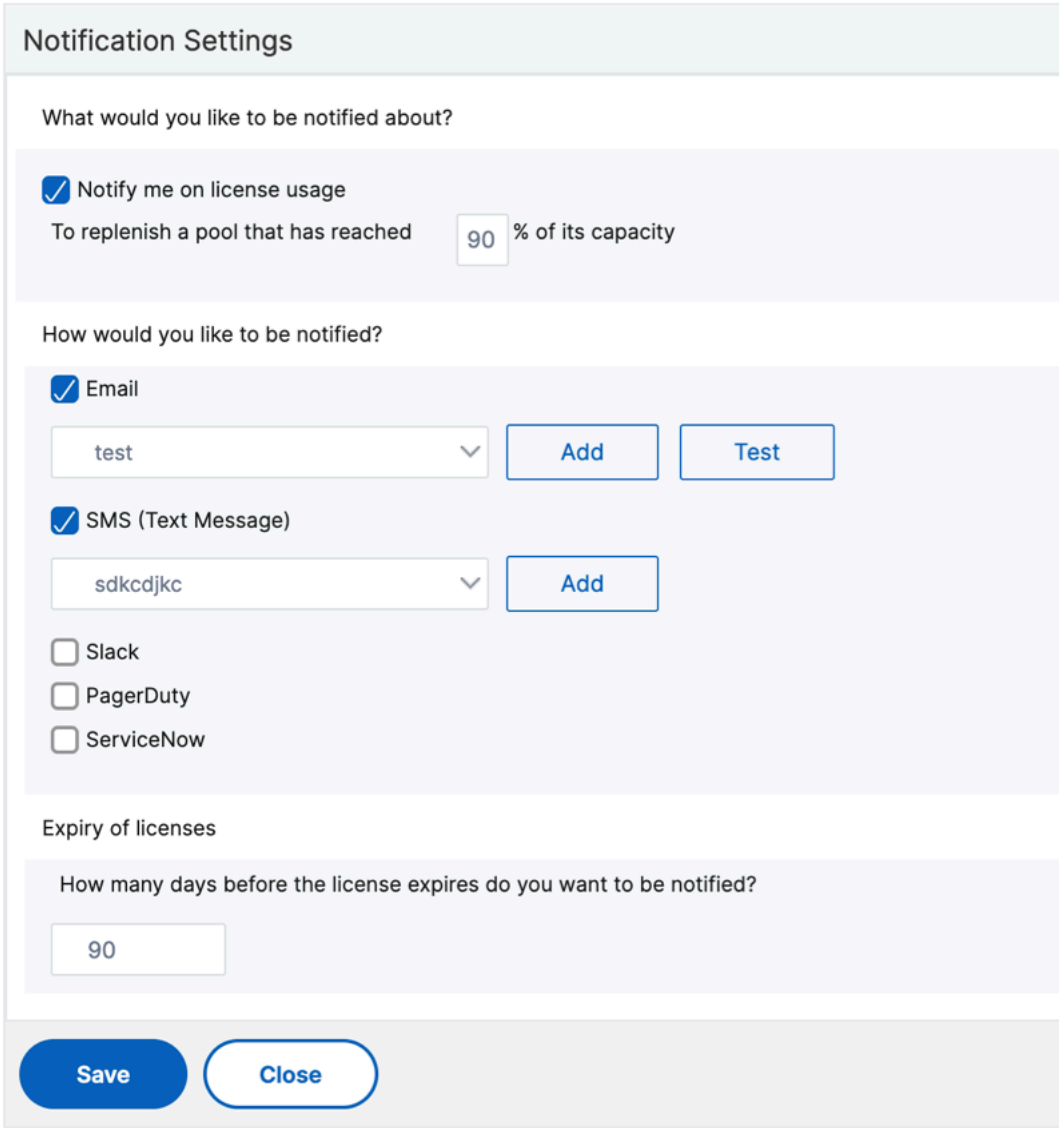
Vous pouvez créer des notifications personnalisées pour compléter les alarmes par défaut.

Période de grâce

Lorsqu'une instance à capacité groupée Citrix ADC est dans un état sain et que le serveur de licences cesse de répondre, l'instance continue de fonctionner avec la capacité actuelle pendant 30 jours. Si la connectivité au serveur de licences n'est pas restaurée après 30 jours, l'instance perd sa capacité et arrête le traitement du trafic.

Notifications et alarmes

Les notifications peuvent être activées à partir de Citrix Application Delivery Management (ADM) pour toute action effectuée sur l'instance. Outre les paramètres de notification personnalisés, certaines alarmes sont configurées par défaut. Par exemple : pour configurer une alarme pour réapprovisionner un pool qui a épuisé un certain pourcentage de sa capacité, accédez à **Infrastructure** > **Licence** > **Paramètres > Paramètres** de **notification** et cliquez sur le bouton Modifier.



Comportements attendus lorsque des problèmes surviennent

February 1, 2024

Voici les comportements attendus des serveurs de licences et des instances Citrix ADC lorsqu'ils éprouvent les problèmes décrits :

Le serveur de licences cesse de répondre

> **Avertissement**
>
> Le serveur de licences ne répond pas. Citrix ADC continue de fonctionner avec la capacité actuelle pendant 30 jours. Après 30 jours, si la connectivité au serveur de licences n'est pas restaurée, Citrix ADC perd sa capacité actuelle et arrête le traitement du trafic.

Si le serveur de licences cesse de répondre, l'instance Citrix ADC entre dans la période de grâce jusqu'à ce que la connectivité soit restaurée.

L'instance à capacité groupée Citrix ADC activée cesse de répondre

Si l'instance à capacité groupée Citrix ADC cesse de répondre et que le serveur de licences est dans un état sain, le serveur de licences vérifie toutes les licences de l'instance Citrix ADC après 10 minutes. Lorsque l'instance redémarre, elle envoie une demande pour extraire toutes les licences du serveur de licences.

Le serveur de licences et l'instance à capacité groupée Citrix ADC cessent de répondre

Si le serveur de licences et l'instance Citrix ADC à capacité groupée redémarrent et rétablit la connexion, le serveur de licences vérifie toutes ses licences après 10 minutes, et les instances Citrix ADC groupées capacité activées retirent automatiquement les licences une fois le redémarrage terminé.

L'instance à capacité groupée Citrix ADC s'arrête gracieusement

Lors d'un arrêt gracieux, vous pouvez choisir de vérifier les licences dans ou de conserver les licences qui ont été allouées avant l'arrêt gracieux. Si vous choisissez de vérifier les licences dans, l'instance Citrix ADC à capacité groupée activée n'est pas sous licence après son redémarrage. Si vous choisissez de conserver les licences, elles sont archivées sur le serveur de licences lorsque l'instance s'arrête. Une fois l'instance redémarrée, elle rétablit la connexion avec le serveur de licences et récupère les licences comme spécifié dans la configuration enregistrée.

Si le système redémarre et que la récupération échoue en raison de l'absence de capacité disponible dans le pool, Citrix ADC vérifie l'inventaire des licences de pool ADM (Application Delivery Management) Citrix et retire toute capacité disponible. Une alarme SNMP est déclenchée pour notifier cette condition à l'utilisateur si Citrix ADC n'est pas en cours d'exécution avec la pleine capacité conformément à la configuration. Si aucune capacité n'est disponible dans le pool de bande passante, l'instance activée de capacité du pool devient sans licence.

Le réseau perd la connectivité

> **Message d'erreur (syslog)**
>
> Le serveur de licences ne répond pas.

Si le serveur de licences et les instances à capacité groupée Citrix ADC sont dans des états sains mais que la connectivité réseau est perdue, les instances continuent à fonctionner avec leur capacité actuelle pendant 30 jours. Après 30 jours, si la connectivité au serveur de licences n'est pas restaurée, les instances perdent leur capacité et arrêtent le traitement du trafic, et le serveur de licences contrôle toutes ses licences. Une fois que le serveur de licences rétablit la connectivité avec les instances Citrix ADC, les instances retirent à nouveau les licences.

Configurer les contrôles d'expiration pour les licences de capacité du pool

February 1, 2024

Vous pouvez désormais configurer le seuil d'expiration des licences pour les licences à capacité groupée Citrix ADC. En définissant des seuils, Citrix Application Delivery Management (ADM) envoie des notifications par e-mail ou SMS lorsqu'une licence doit expirer. Une interruption SNMP et une notification sont également envoyées lorsque la licence a expiré sur Citrix ADM.

Un événement est généré lorsqu'une notification d'expiration de licence est envoyée et cet événement peut être consulté sur Citrix ADM.

Pour configurer les contrôles d'expiration de licence :

1. Accédez à **Réseaux** > **Licences**.
2. Dans la page **Paramètres de licence**, sous la section**Informations d'expiration de licence**, vous trouverez les détails des licences qui vont expirer :
    - **Fonctionnalité** : Type de licence qui va expirer.
    - **Nombre** : nombre de serveurs virtuels ou d'instances qui seront affectés.

- **Jours jusqu'à l'expiration** : Nombre de jours avant l'expiration de la licence.

3. Dans la section**Paramètres de notification**, cliquez sur l'icône **Modifier** et spécifiez le seuil d'alerte. Vous pouvez définir un pourcentage de capacité de licences groupées à utiliser pour notifier les administrateurs.
4. Choisissez le type de notification que vous souhaitez envoyer en cochant la case appropriée. Les types de notification sont les suivants :
   a) **Profil de messagerie** : Spécifiez un serveur de messagerie et les détails du profil. Un e-mail est déclenché lorsque vos licences sont sur le point d'expirer.
   b) **Profil SMS** : Spécifiez un serveur de service de messages courts (SMS) et les détails du profil. Un message SMS est déclenché lorsque vos licences sont sur le point d'expirer.
5. Ensuite, indiquez quand vous souhaitez envoyer la notification en termes de nombre de jours avant l'expiration de la licence.
6. Cliquez sur **Enregistrer**.

> **Remarque**
>
> Lorsque vous ajoutez de nouvelles licences au pool, les instances Citrix ADC utilisent les nouvelles licences à l'expiration de leurs licences existantes.

Enregistrez-vous et consultez les licences Citrix ADC VPX et BLX

February 1, 2024

Vous pouvez allouer des licences VPX et BLX à des instances Citrix ADC à la demande auprès de Citrix Application Delivery Management (ADM). Le logiciel ADM stocke et gère les licences, qui ont un cadre de licences qui fournit un provisionnement de licences évolutif et automatisé. Une instance peut extraire la licence auprès de Citrix ADM lorsqu'elle est provisionnée. Lorsqu'une instance est supprimée ou détruite, l'instance récupère sa licence au logiciel Citrix ADM.

Conditions préalables

Assurez-vous que les conditions préalables suivantes sont remplies :

- Vous utilisez une image Citrix ADC VPX exécutant la version 12.0 du logiciel.
  Par exemple : NSVPX-ESX-12.0-xx.xx_NC.zip
- Vous avez installé Citrix ADM exécutant la version 12.0.
  Par exemple : MAS-ESX-12.0-xx.xx.zip

> **Remarque**
>
> Pour gérer les licences VPX existantes par Citrix ADM, vous devez réhéberger les licences vers Citrix ADM.

Installation de licences dans Citrix ADM

> **Remarque**
>
> Avant d'installer les licences, redémarrez l'appliance virtuelle Citrix ADM si vous avez modifié l'édition du logiciel ou la bande passante.

Pour installer des fichiers de licence sur Citrix ADM :

1. Dans un navigateur Web, tapez l'adresse IP du Citrix ADM (par exemple, http://192.168.100.1).
2. Dans Nom d'utilisateur et Mot de passe, entrez les informations d'identification de l'administrateur.
3. Accédez à **Réseaux** > **Licences**.
4. Dans la section **Fichiers de licence**, sélectionnez l'une des options suivantes :

   - **Télécharger des fichiers de licences à partir d'un ordinateur local** : si un fichier de licence est déjà présent sur votre ordinateur local, vous pouvez le télécharger sur Citrix ADM. Pour ajouter des fichiers de licence, cliquez **sur**Parcourir et sélectionnez le fichier de licence (.lic) que vous souhaitez ajouter. Cliquez ensuite sur **Terminer**.
   - **Utiliser le code d'accès à la licence** - Citrix envoie par e-mail le code d'accès à la licence pour les licences que vous achetez.
     Pour ajouter des fichiers de licence, entrez le code d'accès à la licence dans la zone de texte, puis cliquez sur **Obtenir des licences** .

   > **Remarque**
   >
   > Assurez-vous d'être connecté à Internet avant d'utiliser le code d'accès à la licence pour installer les licences.

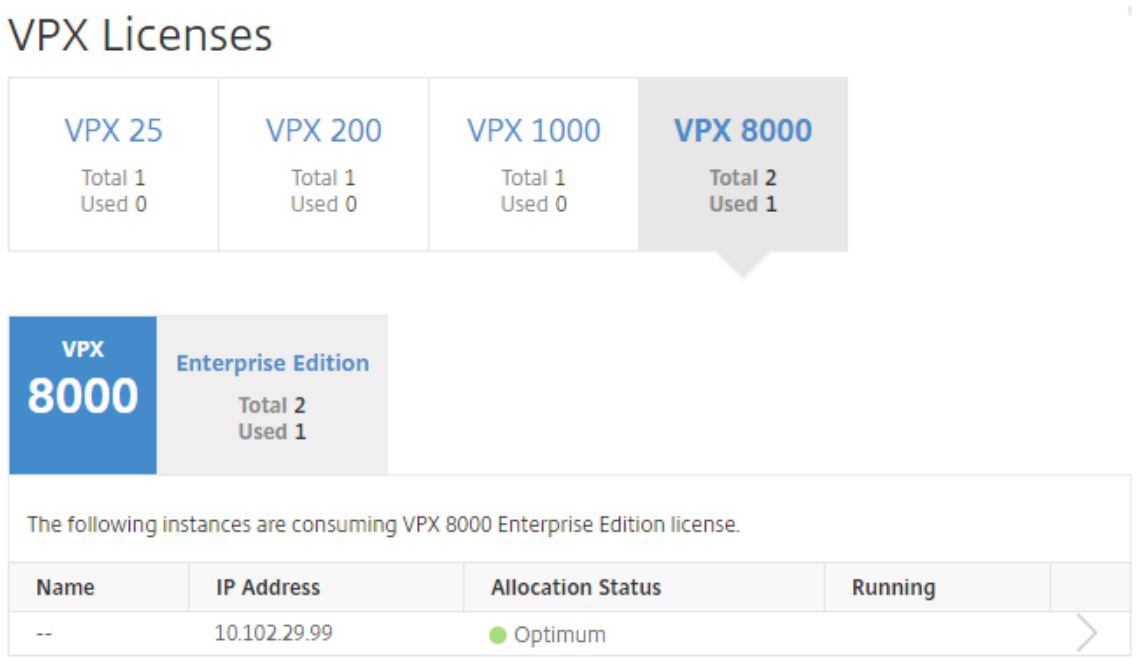
   À tout moment, vous pouvez ajouter d'autres licences à Citrix ADM à partir des paramètres de licence.

Vérification

Vous pouvez afficher les licences disponibles et allouées dans l'interface graphique Citrix ADM.

Pour afficher les licences :

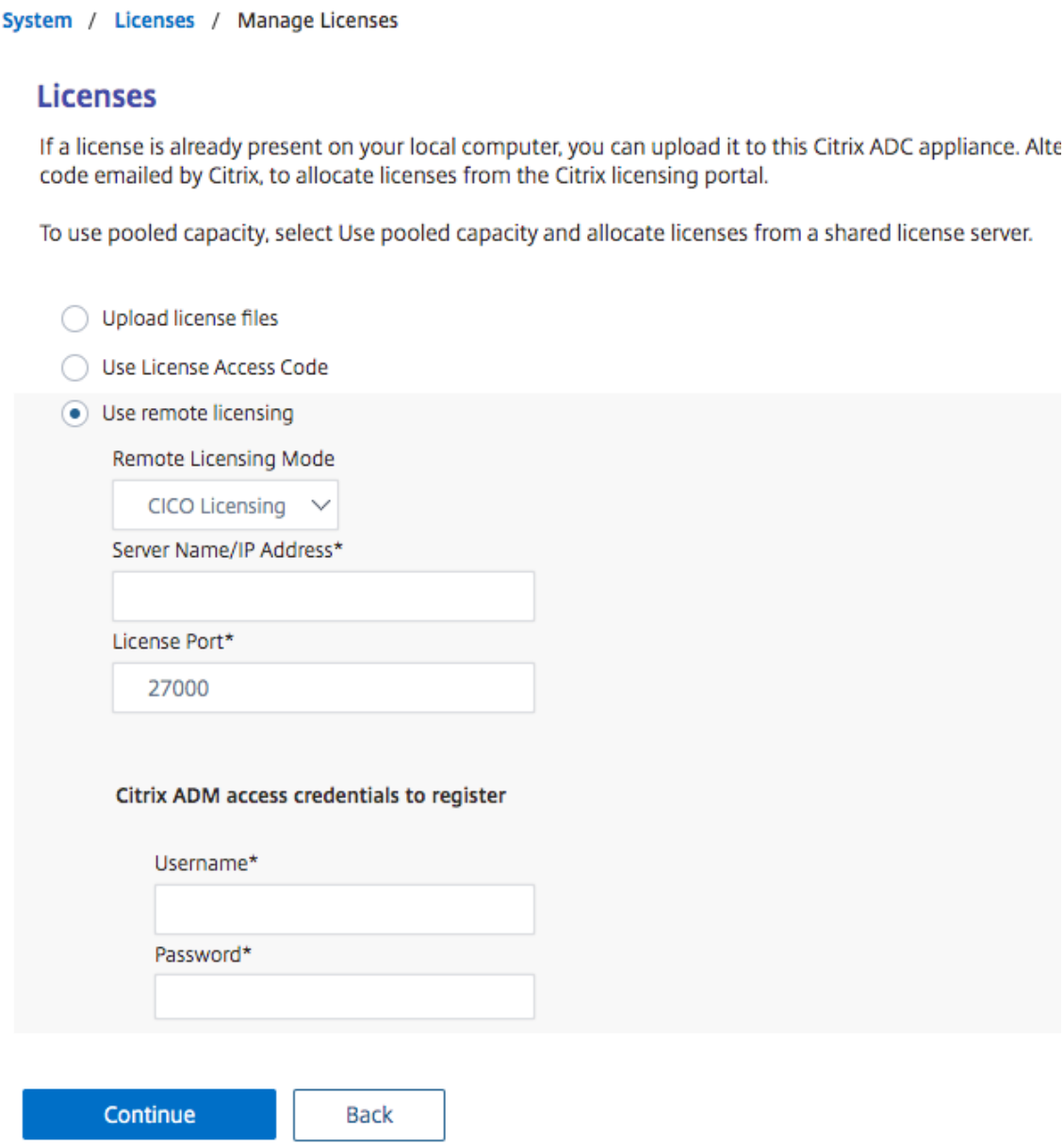
1. Dans un navigateur Web, tapez l'adresse IP de Citrix ADM (par exemple, http://192.168.100.1).
2. Dans **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Sous l'onglet Configuration, accédez à **Réseaux**> **Licences** > **Licences VPX.**



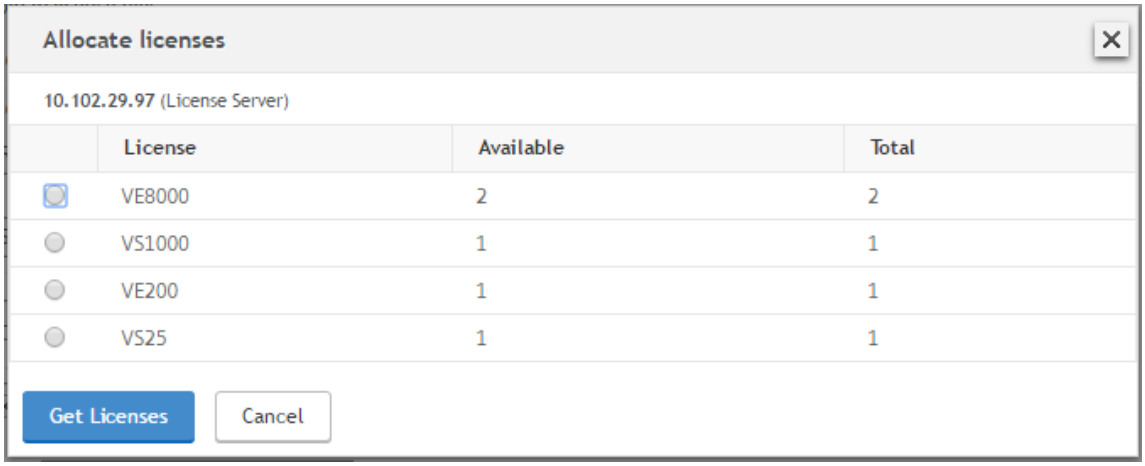
4. Vous pouvez afficher les licences allouées dans le tableau sous la section Licences disponibles.

Allouer des licences VPX et BLX à une instance ADC à l'aide de l'interface graphique Citrix ADC

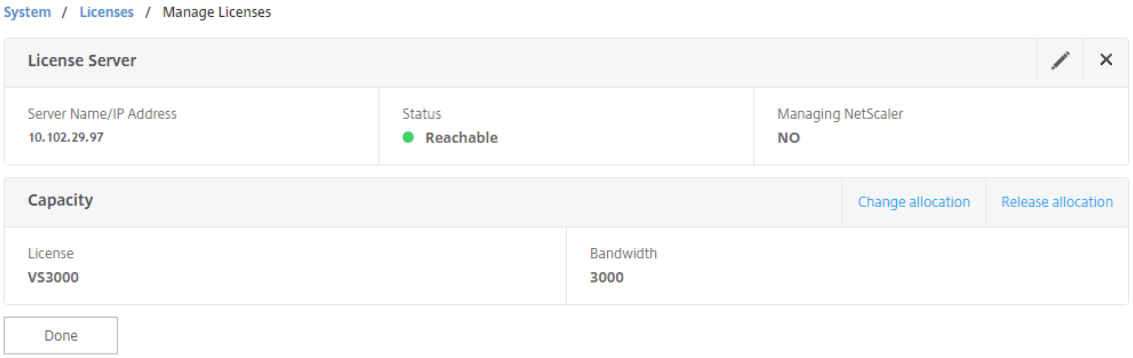
1. Dans un navigateur Web, tapez l'adresse IP de l'instance Citrix ADC (par exemple, http://192.168.100.1).
2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Sous l'onglet Configuration, accédez à **Système > Licences > Gérer les licences**, cliquez sur **Ajouter une nouvelle licence**, puis sélectionnez **Utiliser les licences à distance > Licences CICO**.
4. Entrez les détails du serveur de licences dans le **champ Nom du serveur/Adresse IP** .
5. Dans les champs **Nom d'utilisateur** et **Mot de passe** de l'écran ci-dessus, entrez les informations d'identification Citrix ADM et cliquez sur **Continuer**.



6. Sélectionnez l'édition de licence avec la bande passante requise, cliquez sur **Obtenir des licences**.



7. Cliquez sur **Redémarrer**, votre instance Citrix ADC redémarre.
8. Vous pouvez modifier ou libérer l'allocation de licence en accédant à **Système** > **Licences** > **Gérer les licences**, puis en sélectionnant **Modifier l'allocation** ou **Release allocation.**



9. Si vous cliquez sur **Modifier l'allocation**, une fenêtre contextuelle affiche les licences disponibles sur le serveur de licences. Sélectionnez la licence requise, cliquez sur **Obtenir des licences**.

Allouer des licences VPX et BLX à une instance ADC à l'aide de l'interface de ligne de commande Citrix ADC

1. Dans un client SSH, entrez l'adresse IP de l'instance Citrix ADC et ouvrez une session à l'aide des informations d'identification de l'administrateur.
2. Pour ajouter un serveur de licences, entrez la commande suivante :

```
add ns licenseserver (<licenseServerIP> | <serverName>) [-port <
    port number >]
<!--NeedCopy-->
```

```
> add ns licenseserver 10.102.29.97 -port 27000
 Done
```

3. Pour afficher les licences disponibles sur le serveur de licences, entrez la commande suivante :

```
sh licenseserverpool
<!--NeedCopy-->
```

```
> sh licenseserverpool
        Instance Total                  : 0
        Instance Available              : 0
        Standard Bandwidth Total        : 0 Mbps
        Standard Bandwidth Availabe     : 0 Mbps
        Enterprise Bandwidth Total      : 0 Mbps
        Enterprise Bandwidth Available  : 0 Mbps
        Platinum Bandwidth Total        : 0 Mbps
        Platinum Bandwidth Available    : 0 Mbps
        VPX25S Total                    : 1
        VPX25S Available                : 1
        VPX200E Total                   : 1
        VPX200E Available               : 1
        VPX1000S Total                  : 1
        VPX1000S Available              : 1
        VPX8000E Total                  : 2
        VPX8000E Available              : 1
 Done
```

4. Pour attribuer une licence à l'appliance Citrix ADC, entrez la commande suivante :

```
set capacity  –platform V[S/E/P][Bandwidth]
<!--NeedCopy-->
```

```
> set capacity -platform VE8000
Warning: The configuration changes will not take effect until the system is rebooted
```

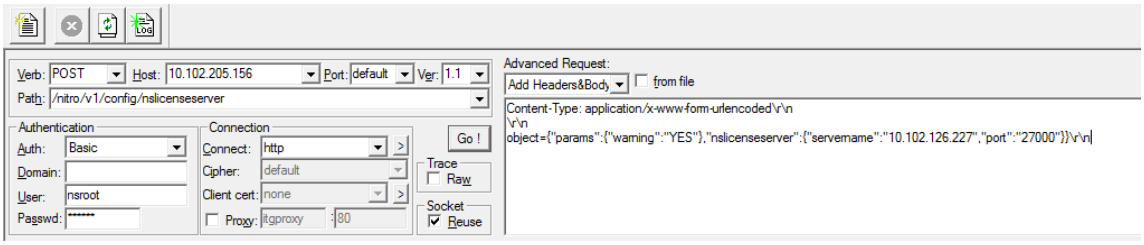
Allouer des licences VPX et BLX à une instance ADC à l'aide de l'API

Dans un navigateur Web ou un client API, connectez-vous à l'instance Citrix ADC à l'aide des informations d'identification de l'administrateur.

Pour ajouter un serveur de licences :

1. Définissez le type de demande sur **Valider**.
2. Définissez le chemin vers /nitro/v1/config/nslicensingserver.
3. Définissez la charge utile comme suit :

```
content-type: application/x-www-form-urlencoded\r\n
\r\n
object= {
  " params " ;{
 warning " : " yes "  }
 , " nslicensing server " ;{
 servername " : " <Citrix ADM IP> " , " port " : " 27000 "  }
  }
 \r\n
<!--NeedCopy-->
```

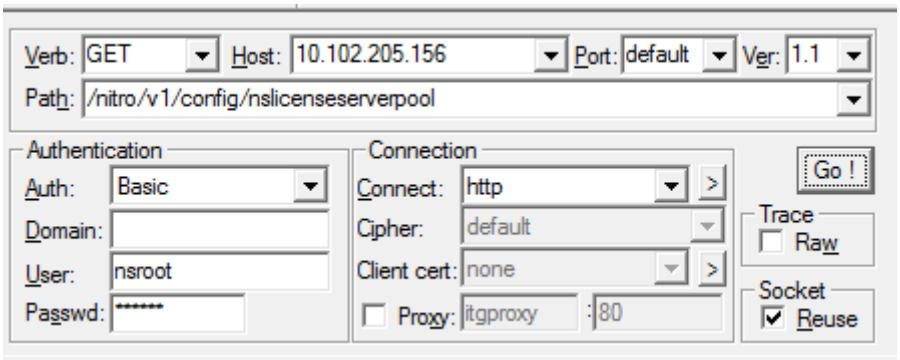


Citrix ADM répond à la demande. L'exemple de réponse suivant montre un succès.

```
RESPONSE: **************\n
HTTP/1.1 201 Created\r\n
Date: Fri, 06 Jan 2017 19:03:21 GMT\r\n
Server: Apache\r\n
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Pragma: no-cache\r\n
Content-Length: 57\r\n
Content-Type: application/json; charset=utf-8\r\n
\r\n
{ "errorcode": 0, "message": "Done", "severity": "NONE" }
finished.
```

Pour afficher les licences disponibles sur le serveur de licences :

1. Définissez le type de demande sur **Get**.
2. Définissez le chemin d'accès à /nitro/v1/config/nslicenseserverpool



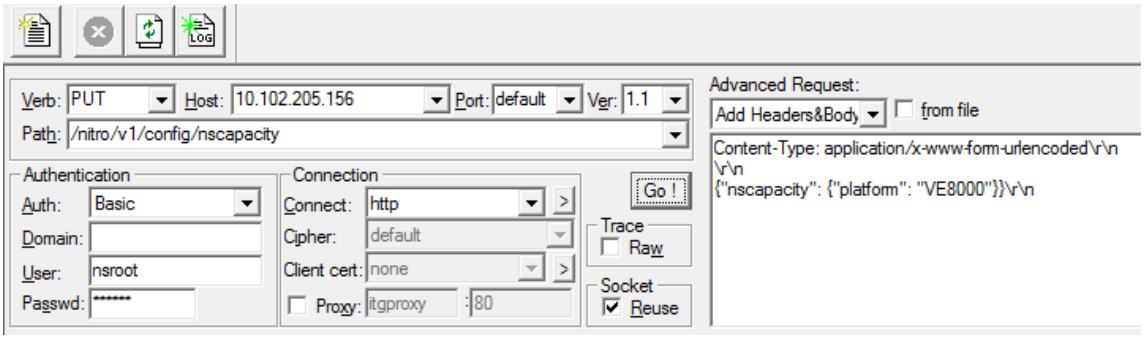
Citrix ADM répond à la demande. L'exemple de réponse suivant montre le succès et la liste des licences disponibles sur le serveur de licences.

RESPONSE: **********\n
HTTP/1.1 200 OK\r\n
Date: Fri, 06 Jan 2017 19:18:54 GMT\r\n
Server: Apache\r\n
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Pragma: no-cache\r\n
Content-Length: 1874\r\n
Content-Type: application/json; charset=utf-8\r\n
\r\n
{ "errorcode": 0, "message": "Done", "severity": "NONE", "nslicenseserverpool": { "instancetotal": 0, "instanceavailable": 0, "standardbandwidthtotal":
0, "standardbandwidthavailable": 0, "enterprisebandwidthtotal": 0, "enterprisebandwidthavailable": 0, "platinumbandwidthtotal": 0, "platinumbandwidthav
ailable": 0, "cpxinstancetotal": 0, "cpxinstanceavailable": 0, "vpx1stotal": 0, "vpx1savailable": 0, "vpx1ptotal": 0, "vpx1pavailable": 0, "vpx5stotal"
: 0, "vpx5savailable": 0, "vpx5ptotal": 0, "vpx5pavailable": 0, "vpx10stotal": 0, "vpx10savailable": 0, "vpx10etotal": 0, "vpx10eavailable": 0, "vpx10p
total": 0, "vpx10pavailable": 0, "vpx25stotal": 0, "vpx25savailable": 0, "vpx25etotal": 0, "vpx25eavailable": 0, "vpx25ptotal": 0, "vpx25pavailable": 0
, "vpx50stotal": 0, "vpx50savailable": 0, "vpx50etotal": 0, "vpx50eavailable": 0, "vpx50ptotal": 0, "vpx50pavailable": 0, "vpx100stotal": 0, "vpx100sav
ailable": 0, "vpx100etotal": 0, "vpx100eavailable": 0, "vpx100ptotal": 0, "vpx100pavailable": 0, "vpx200stotal": 0, "vpx200savailable": 0, "vpx200etota
l": 0, "vpx200eavailable": 0, "vpx200ptotal": 0, "vpx200pavailable": 0, "vpx500stotal": 0, "vpx500savailable": 0, "vpx500eto
tal": 0, "vpx500eavailable": 0, "vpx500ptotal": 0, "vpx500pavailable": 0, "vpx1000stotal": 0, "vpx1000savailable": 0, "vpx1000etotal": 0, "vpx1000eavail
able": 0, "vpx1000ptotal": 0, "vpx1000pavailable": 0, "vpx2000ptotal": 0, "vpx2000pavailable": 0, "vpx3000stotal": 0, "vpx3000savailable": 0, "vpx3000e
total": 0, "vpx3000eavailable": 0, "vpx3000ptotal": 0, "vpx3000pavailable": 0, "vpx4000ptotal": 0, "vpx4000pavailable": 0, "vpx5000stotal": 0, "vpx5000
savailable": 0, "vpx5000etotal": 0, "vpx5000eavailable": 0, "vpx5000ptotal": 0, "vpx5000pavailable": 0, "vpx8000stotal": 1, "vpx8000savailable": 1, "vp
x8000etotal": 2, "vpx8000eavailable": 1, "vpx8000ptotal": 1, "vpx8000pavailable": 1 } }
finished.

Pour attribuer une licence à l'appliance Citrix ADC :

1. Définissez le type de demande sur **Valider**.
2. Définissez le chemin vers /nitro/v1/config/nscapacity.
3. Définissez la charge utile comme suit :

```
content-type: application/x-www-form-urlencoded\r\n
\r\n
{
  " nscapacity:{
  " platform " : " VE8000 "  }
   }
 \r\n
<!--NeedCopy-->
```

Citrix ADM répond à la demande. L'exemple de réponse suivant montre un succès.

```
RESPONSE: **************\n
HTTP/1.1 200 OK\r\n
Date: Fri, 06 Jan 2017 19:16:21 GMT\r\n
Server: Apache\r\n
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Pragma: no-cache\r\n
Content-Length: 57\r\n
Content-Type: application/json; charset=utf-8\r\n
\r\n
{ "errorcode": 0, "message": "Done", "severity": "NONE" }
finished.
```

Mettre à jour l'adresse IP d'un serveur de licences

Vous pouvez mettre à jour l'adresse IP du serveur de licences dans les instances VPX et BLX, sans aucun impact sur la bande passante de licence allouée sur l'instance et la perte de données.

Mise à jour à l'aide de l'interface de ligne de commande : pour mettre à jour l'adresse IP du serveur de licences à l'aide de l'interface de ligne de commande,

```
add licenseserver <licensing server IP address> -forceUpdateIP
```

Cette commande se connecte au nouveau serveur et libère les ressources associées au serveur de licences précédent.

Mise à jour à l'aide de l'interface graphique : pour mettre à jour l'adresse IP du serveur de licences à l'aide de l'interface graphique, accédez à **Système > Licences > Gérer les licences**, cliquez sur **Ajouter une nouvelle licence**. Pour plus d'informations, consultez Allouer des licences VPX et BLX à une instance ADC à l'aide de l'interface graphique Citrix ADC.

Configurer les contrôles d'expiration pour les licences d'enregistrement et de sortie Citrix ADC VPX et BLX

Vous pouvez désormais configurer le seuil d'expiration des licences Citrix ADC VPX et BLX. En définissant des seuils, Citrix ADM envoie des notifications par e-mail ou SMS lorsqu'une licence doit expirer. Un trap SNMP et une notification sont également envoyés lorsque la licence a expiré sur Citrix ADM.

Un événement est généré lorsqu'une notification d'expiration de licence est envoyée et cet événement peut être consulté sur Citrix ADM.

Pour configurer les contrôles d'expiration de licence :

1. Accédez à **Réseaux** > **Licences**.
2. Dans la page**Paramètres de licence**, sous la section**Informations d'expiration de licence**, vous trouverez les détails des licences qui vont expirer :
    - **Fonctionnalité** : Type de licence qui va expirer.
    - **Nombre** : nombre de serveurs virtuels ou d'instances affectés.
    - **Jours jusqu'à l'expiration** : Nombre de jours avant l'expiration de la licence.
3. Dans la section**Paramètres de notification**, cliquez sur l'icône**Modifier**et spécifiez le seuil d'alerte. Vous pouvez définir un pourcentage de capacité de licences groupées à utiliser pour notifier les administrateurs.
4. Choisissez le type de notification que vous souhaitez envoyer en cochant la case appropriée. Les types de notification sont les suivants :
    a) **Profil de messagerie** : Spécifiez un serveur de messagerie et les détails du profil. Un e-mail est déclenché lorsque vos licences sont sur le point d'expirer.
    b) **Profil SMS** : Spécifiez un serveur de service de messages courts (SMS) et les détails du profil. Un message SMS est déclenché lorsque vos licences sont sur le point d'expirer.
5. Ensuite, indiquez quand vous souhaitez envoyer la notification en termes de nombre de jours avant l'expiration de la licence.
6. Cliquez sur **Enregistrer**.

Licences de processeur virtuel Citrix ADC

February 1, 2024

Les administrateurs de centres de données tels que vous optent pour de nouvelles technologies qui simplifient les fonctions réseau tout en réduisant les coûts et en améliorant l'évolutivité. La nouvelle architecture de centre de données doit inclure au minimum les fonctionnalités suivantes :

- Réseau défini par logiciel (SDN)
- Virtualisation des fonctions réseau (NFV)
- Virtualisation de réseau (NV)
- Micro-services

Un tel mouvement nécessite également que les exigences logicielles soient dynamiques, flexibles et agiles pour répondre aux besoins commerciaux en constante évolution. Les licences devraient également être gérées par un outil de gestion centralisé offrant une visibilité complète de l'utilisation.

Licences de processeur virtuel pour Citrix ADC VPX

Auparavant, les licences Citrix ADC VPX étaient attribuées en fonction de la consommation de bande passante par les instances. Un Citrix ADC VPX est limité à l'utilisation d'une bande passante spécifique et d'autres mesures de performance en fonction de l'édition de licence à laquelle il est lié. Pour augmenter la bande passante disponible, vous devez passer à une édition de licence qui fournit davantage de bande passante. Dans certains scénarios, la bande passante requise peut être moindre, mais elle est plus importante pour d'autres performances L7, telles que le protocole SSL, le TPS, le débit de compression, etc. La mise à niveau de la licence Citrix ADC VPX peut ne pas convenir dans de tels cas. Mais vous devrez peut-être encore acheter une licence avec une large bande passante pour débloquer les ressources système requises pour un traitement intense en CPU. Citrix ADM prend désormais en charge l'allocation de licences à l'instance Citrix ADC en fonction des exigences du processeur virtuel.

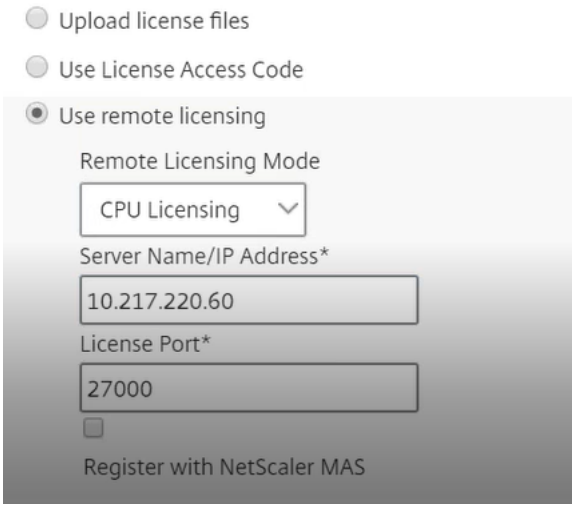
Dans la fonctionnalité de licence basée sur l'utilisation du processeur virtuel, la licence spécifie le nombre de processeurs auxquels un Citrix ADC VPX particulier a droit. Ainsi, le Citrix ADC VPX peut extraire des licences uniquement pour le nombre de processeurs virtuels s'exécutant sur celui-ci à partir du serveur de licences. Citrix ADC VPX récupère les licences en fonction du nombre de CPU s'exécutant dans le système. Citrix ADC VPX ne prend pas en compte les processeurs inactifs lors de l'extraction des licences.

Similaire à la capacité de licence mise en commun et aux fonctionnalités de licence CICO, le serveur de licences Citrix ADM gère un ensemble distinct de licences CPU virtuelles. Ici aussi, les trois éditions gérées pour les licences de processeurs virtuels sont Standard, Advanced et Premium. Ces éditions déverrouillent le même ensemble de fonctionnalités que celles déverrouillées par les éditions pour les licences de bande passante.

Il peut y avoir un changement dans le nombre de processeurs virtuels ou lors d'un changement dans l'édition de la licence. Dans ce cas, vous devez toujours arrêter l'instance avant de lancer une demande pour un nouvel ensemble de licences. Redémarrez le Citrix ADC VPX après avoir retiré les licences.

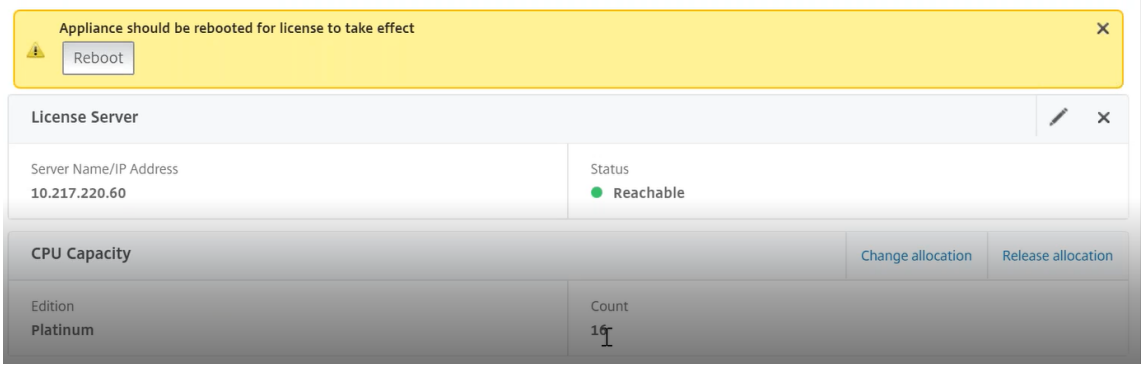
Pour configurer le serveur de licences dans Citrix ADC VPX à l'aide de l'interface graphique :

1. Dans Citrix ADC VPX, accédez à **Système** > **Licences** et cliquez sur **Gérer les licences**.
2. Sur la page **Licence**, cliquez sur **Ajouter une nouvelle licence**.
3. Sur la page **Licences**, sélectionnez l'option **Utiliser les licences à distance** .
4. Sélectionnez les **licences CPU** dans la liste des **modes de licence à distance** .
5. Entrez l'adresse IP du serveur de licences et le numéro de port.
6. Cliquez sur **Continuer**.



> **Remarque**
>
> Vous devez toujours enregistrer l'instance Citrix ADC VPX auprès de Citrix ADM. Si ce n'est déjà fait, activez **Enregistrer auprès de Citrix ADM** et saisissez les informations d'identification de connexion Citrix ADM.

7. Dans la fenêtre **Allouer des licences**, sélectionnez le type de licence. La fenêtre affiche le total et les processeurs virtuels disponibles, ainsi que les processeurs qui peuvent être alloués. Cliquez sur **Obtenir licences**.
8. Cliquez sur **Redémarrer** sur la page suivante pour demander les licences.



> **Remarque**
>
> Vous pouvez également libérer la licence actuelle et vérifier à partir d'une autre édition. Par exemple, vous exécutez déjà une licence d'édition Standard sur votre instance. Vous pouvez libérer cette licence, puis vérifier à partir de Advanced Edition.

Configuration du serveur de licences dans la licence Citrix ADC VPX à l'aide de l'interface de ligne de commande CLI

Dans la console Citrix ADC VPX, tapez les commandes suivantes pour les deux tâches suivantes :

1. Pour ajouter le serveur de licences au Citrix ADC VPX :

```
add licenseserver <IP address of the license server>
<!--NeedCopy-->
```

2. Pour demander les licences :

```
set capacity -vcpu - edition premium
<!--NeedCopy-->
```

   Lorsque vous y êtes invité, redémarrez l'instance en tapant la commande suivante :

```
reboot -w
<!--NeedCopy-->
```

Mettre à jour l'adresse IP d'un serveur de licences

Vous pouvez mettre à jour l'adresse IP du serveur de licences dans l'instance VPX, sans aucun impact sur la bande passante de licence allouée à l'instance et sans perte de données. Pour mettre à jour l'adresse IP du serveur de licences, tapez la commande suivante sur l'instance VPX :

```
add licenseserver <licensing server IP address> -forceUpdateIP
```

Cette commande se connecte au nouveau serveur et libère les ressources associées au serveur de licences précédent.

Gestion des licences de processeur virtuel sur Citrix ADM

1. Dans Citrix ADM, accédez à **Réseaux** > **Licences > Licences** de **processeur virtuel**.
2. La page affiche les licences allouées pour chaque type d'édition de licence.
3. Cliquez sur le chiffre dans chaque beignet pour afficher les instances Citrix ADC qui utilisent cette licence.

Licence de processeur virtuel pour Citrix ADC CPX

Lors du provisionnement de l'instance Citrix ADC CPX, vous pouvez configurer l'instance Citrix ADC CPX pour extraire les licences du serveur de licences en fonction de l'utilisation du processeur sur l'instance.

Citrix ADC CPX s'appuie sur le serveur de licences, exécuté sur Citrix ADM, pour gérer les licences. Citrix ADC CPX extrait les licences du serveur de licences lors de son démarrage. Les licences sont réarchivées sur le serveur de licences lorsque le Citrix ADC CPX s'arrête.

Vous pouvez télécharger Citrix ADC CPX depuis le Docker App Store. Sur l'hôte Docker, pour télécharger Citrix ADC CPX, exécutez la commande suivante :

```
docker pull store/citrix/netscalercpx: [version]
```

Il existe trois types de licences disponibles pour les licences CPX :

1. Licences d'abonnement au processeur virtuel prises en charge pour CPX et VPX
2. Licences de capacité groupée
3. Licences CP1000 prenant en charge un ou plusieurs vCPU pour CPX uniquement

Pour configurer des licences d'abonnement vCPU lors du Provisioning de l'instance CPX Citrix ADC :

Spécifiez le nombre de licences vCPU utilisées par l'instance CPX Citrix ADC.

- Cette valeur est entrée en tant que variable d'environnement via Docker, Kubernetes ou Mesos/-Marathon.
- La variable cible est « CPX_CORES ». Le CPX peut prendre en charge de 1 à 16 cœurs.

Pour spécifier 2 cœurs, vous pouvez exécuter la commande docker run comme suit :

```
1 docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
    -e EULA=yes -e CPX_CORES=2
```



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

Lors du Provisioning d'une instance Citrix ADC CPX, définissez le serveur de licences Citrix ADC en tant que variable d'environnement dans la commande **docker run** comme indiqué ci-dessous :

```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
   -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
   LS_PORT> cpx:11.1
<!--NeedCopy-->
```

Où,

- *<LS_IP_ADDRESS>* est l'adresse IP du serveur de licences Citrix ADC.
- *<LS_PORT>* est le port du serveur de licences Citrix ADC. Par défaut, le port est 27000.

> **Remarque**
>
> Par défaut, l'instance CPX Citrix ADC extrait la licence du pool d'abonnements vCPU. L'instance CPX extrait un nombre « n » de licences si l'instance fonctionne avec « n » processeurs.

Pour configurer les licences Citrix ADC Pooled Capacity ou CP1000 lors du Provisioning de l'instance CPX Citrix ADC :

Si vous souhaitez récupérer les licences de l'instance CPX à l'aide du pool de licences (basé sur la bande passante) ou du pool privé CPX (CP1000 ou basé sur un pool privé), vous devez fournir les variables d'environnement en conséquence.

Par exemple, les opérations suivantes peuvent être effectuées :

```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
   -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
   LS_PORT> -e PLATFORM=CP1000 cpx:11.1
<!--NeedCopy-->
```

CP1000. Cette commande déclenche l'extraction depuis le pool CP1000 (pool privé CPX). L'instance CPX Citrix ADC extrait ensuite le nombre « n » d'instances pour le nombre « n » de cœurs spécifiés pour CPX_CORES. Le cas d'utilisation le plus courant est de spécifier n = 1 pour une extraction d'une instance unique. Les cas d'utilisation du CPX multicœur examinent « n » processeurs virtuels (où « n » est compris entre 1 et 7).

```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
   -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
   LS_PORT> -e BANDWIDTH=2000 cpx:11.1
<!--NeedCopy-->
```

Capacité mise en commun. Cette commande extrait une licence du pool d'instances et consomme 1 000 Mbit/s de bande passante provenant du pool de bande passante Premium, tout en permettant à

CPX de fonctionner jusqu'à 2 000 Mbit/s.Dans les licences groupées, les 1000 premiers Mbps ne sont pas facturés.

> **Remarque**
>
> Spécifiez le nombre de processeurs virtuels correspondant à la bande passante cible souhaitée lors du retrait du pool de bande passante, comme indiqué dans le tableau suivant :

Nombre de cœurs (vCPU)	Bande passante maximale
1	1000 Mbit/s
2	2000 Mbits/s
3	3 500 Mbit/s
4	5000 Mbits/s
5	6500 Mbits/s
6	8000 Mbits/s
7	9300 Mbit/s

Gérer les instances Citrix SD-WAN

February 1, 2024

Citrix ADM vous permet de surveiller, de gérer et d'afficher les analyses des appliances Citrix SD-WAN dans votre réseau. Le tableau d'interopérabilité suivant fournit des informations sur les fonctionnalités de Citrix ADM actuellement prises en charge dans chacune des éditions de la plate-forme Citrix SD-WAN.

Matrice d'interopérabilité des éditions de la plate-forme Citrix SD-WAN et des fonctionnalités Citrix ADM

Édition Plate-forme	Détection	Configuration	Surveillance	Reporting (rapports réseau)	Gestion des événe-ments	HDX Insight	WAN Insight
Citrix SD-WAN WANOP	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Citrix SD-WAN SE	Oui	Non	Non	Non	Non	Non	Non
Citrix SD-WAN PE	Oui	Non	Non	Non	Non	Oui	Non

Versions Citrix SD-WAN prises en charge par Citrix ADM

Édition Plateforme	Version Citrix SD-WAN	Version de Citrix ADM
Citrix SD-WAN WANOP	Citrix CloudBridge 7.4 et versions ultérieures	Citrix ADM 11.0 et versions ultérieures
Citrix SD-WAN SE	Citrix SD-WAN 9.3.0 et versions ultérieures	Citrix ADM 12.0.53.8 et versions ultérieures
Citrix SD-WAN PE	Citrix SD-WAN 9.3.0 et versions ultérieures	Citrix ADM 12.0.53.8 et versions ultérieures

Vous pouvez ajouter une appliance WANOP Citrix SD-WAN en tant qu'instance gérée sur Citrix ADM. Pour plus d'informations, consultez Ajouter des instances à Citrix ADM. Vous pouvez afficher les informations WAN, HDX, Network Reports et Event Reports pour les instances WANOP Citrix SD-WAN.

Citrix ADM permet aux appliances Citrix SD-WAN Standard Edition (SE) et Enterprise Edition (EE) de s'enregistrer en tant qu'instances gérées sur Citrix ADM.

Pour ajouter une appliance Citrix SD-WAN SE/PE/AE à Citrix ADM, configurez Citrix ADM en tant que collecteur AppFlow sur les appliances Citrix SD-WAN SE/PE/AE. L'appliance Citrix SD-WAN SE/PE/AE s'ajoute en tant qu'instance gérée sur Citrix ADM. L'appliance SD-WAN SE/PE/AE envoie ensuite les données d'analyse à Citrix ADM.

Vous pouvez définir Citrix ADM en tant que collecteur AppFlow sur chaque périphérique SE/PE/AE SD-WAN individuellement, ou utiliser Citrix SD-WAN Center pour exporter la configuration vers les appliances gérées.

Pour plus d'informations, consultez la section Ajout d'instances Citrix SD-WAN SE/PE/AE dans Citrix ADM.

Pour une appliance Citrix SD-WAN PE, vous pouvez afficher des enregistrements de données HDX ou des données multi-sauts, en fonction de la configuration AppFlow. Une appliance Citrix SD-WAN SE fournit uniquement des données multi-sauts. Pour plus d'informations, consultez Affichage des rapports et des mesures HDX Insight et Affichage des données d'analyse pour un déploiement multi-sauts.

Cette page fournit des liens d'accès rapide vers les rubriques que vous pouvez consulter pour configurer Citrix ADM et gérer vos appliances WANOP SD-WAN à l'aide de Citrix ADM.

Présentation de Citrix ADM

À propos de Citrix ADM

Architecture

Comment Citrix ADM découvre des instances

Comment Citrix ADM communique avec les instances gérées

Déploiement Citrix ADM

Déployer Citrix ADM avec Citrix Hypervisor

Déployer Citrix ADM avec Microsoft Hyper-V

Déployer Citrix ADM avec VMware ESXi

Déployer Citrix ADM avec le serveur KVM Linux

Déployer Citrix ADM en mode haute disponibilité

Migrer de NetScaler Insight Center vers Citrix ADM

Intégrer Citrix ADM avec Director

Gestion des instances

Comment ajouter des instances à Citrix ADM

Comment créer des groupes d'instances sur Citrix ADM

Comment faire pour sauvegarder et restaurer une instance à l'aide de Citrix ADM

Gestion de la configuration

Comment créer des tâches de configuration à partir de commandes correctives sur Citrix ADM

Procédure de planification des tâches créées à l'aide de modèles intégrés dans Citrix ADM

Replanifier des travaux configurés à l'aide de modèles intégrés dans Citrix ADM

Comment réutiliser les tâches de configuration exécutées

Analytics

WAN Insight

HDX Insight

Comment afficher les rapports réseau pour les instances WANOP Citrix SD-WAN

Comment configurer des seuils adaptatifs

Comment configurer la synthèse des bases de données pour Analytics

Comment créer des seuils et des alertes à l'aide de Citrix ADM

Gestion des événements

Comment faire pour définir l'âge des événements pour Citrix ADM

Procédure de planification d'un filtre d'événement à l'aide de Citrix ADM

Comment faire pour définir des notifications par e-mail répétées pour des événements à partir de Citrix ADM

Comment faire pour supprimer des événements à l'aide de Citrix ADM

Comment afficher les rapports d'événements pour les instances WANOP Citrix SD-WAN

Comment faire pour modifier la gravité signalée des événements qui se produisent sur des instances Citrix ADC

Comment afficher le résumé des événements dans Citrix ADM

Comment faire pour afficher la gravité des événements et les biais des interruptions SNMP sur le tableau de bord de l'infrastructure de Citrix ADM

Authentification

Comment mettre en cascade des serveurs d'authentification externes

Comment ajouter des serveurs d'authentification RADIUS

Comment ajouter des serveurs d'authentification LDAP

Comment ajouter des serveurs d'authentification TACACS

Comment extraire un groupe de serveurs d'authentification dans Citrix ADM

Comment activer l'authentification locale de secours

Système Citrix ADM

Gestion du système Citrix ADM

Procédure de mise à niveau de Citrix ADM

Comment faire pour générer un fichier de support technique pour Citrix ADM

Comment faire pour sauvegarder et restaurer votre serveur Citrix ADM dans un déploiement à serveur unique

Comment faire pour sauvegarder et restaurer une configuration Citrix ADM dans une paire HA

Comment faire pour activer l'accès Shell pour les utilisateurs non par défaut dans Citrix ADM

Comment faire pour configurer le serveur NTP sur Citrix ADM

Comment faire pour configurer les paramètres SSL pour Citrix ADM

Comment faire pour configurer l'intervalle de purge Syslog pour Citrix ADM

Comment afficher les informations d'audit de Citrix ADM

Comment faire pour configurer les paramètres de notification système de Citrix ADM

Comment surveiller l'utilisation du processeur, de la mémoire et du disque de Citrix ADM

Comment faire pour configurer un groupe de chiffrement pour Citrix ADM

Procédure de création d'interruptions SNMP, de gestionnaires et d'utilisateurs sur Citrix ADM

Comment faire pour attribuer un nom d'hôte à un serveur Citrix ADM

Comment faire pour configurer les paramètres de nettoyage du système pour Citrix ADM

Comment faire pour configurer les paramètres de sauvegarde système à l'aide de Citrix ADM

Comment faire pour configurer et afficher les alarmes système sur Citrix ADM

Ajouter des instances Citrix SD-WAN

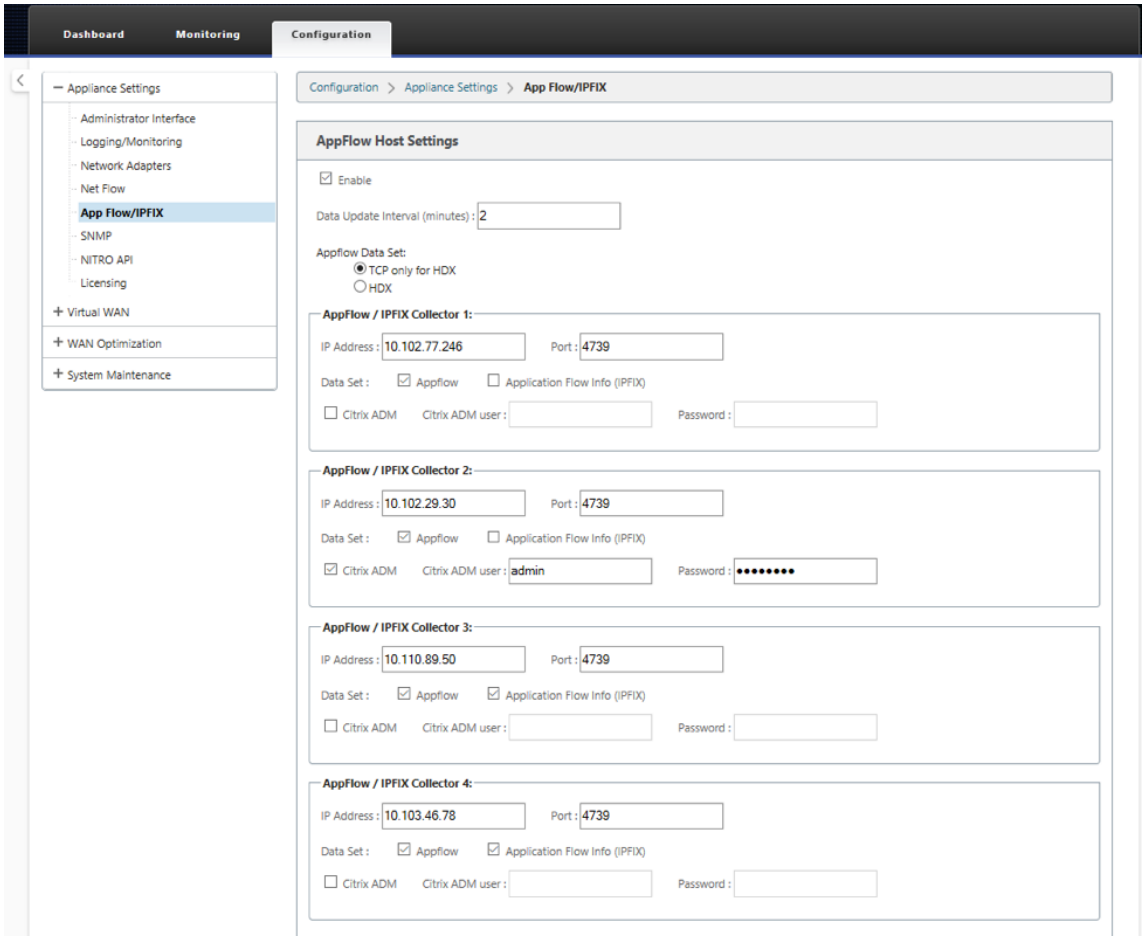
February 1, 2024

Configurez Citrix ADM en tant que collecteur AppFlow sur l'appliance Citrix SD-WAN SE/PE pour ajouter ces instances dans Citrix ADM.Les appliances Citrix SD-WAN SE/PE/AE sont enregistrées en tant qu'instances gérées sur Citrix ADM et leurs enregistrements AppFlow sont collectés. Pour une appliance Citrix SD-WAN PE, vous pouvez activer le modèle **TCP uniquement pour HDX** ou le modèle **HDX**. Le modèle **TCP uniquement pour HDX** fournit des données multi-sauts. Le modèle **HDX** fournit des données HDX, il doit être activé uniquement sur l'appliance Data Center.

Vous pouvez configurer Citrix ADM en tant que collecteur AppFlow sur l'appliance SE/PE/AE SD-WAN, ou vous pouvez configurer Citrix ADM en tant que collecteur AppFlow à l'aide du Centre SD-WAN et exporter la configuration vers les appliances gérées par celui-ci.

Pour configurer Citrix ADM en tant que collecteur AppFlow sur une appliance Citrix SD-WAN SE/PE/AE :

1. Dans l'interface Web SD-WAN SE/PE/AE, accédez à **Configuration** > **Appflow/IPfix**
2. Choisissez **Activer**.



3. Dans le champ **Intervalle de mise à jour des données**, spécifiez l'intervalle de temps, en minutes, auquel les rapports AppFlow sont exportés vers le collecteur AppFlow.

> **Remarque**
>
> Si Citrix ADM est le collecteur AppFlow, l'intervalle de mise à jour des données doit être de 1 minute.

4. Procédez comme suit :
   - Choisissez **HDX** pour envoyer des données d'aperçu HDX au collecteur AppFlow. Cela doit être activé sur les appliances de branche.
   - Choisissez **TCP uniquement pour HDX,** pour envoyer des données multi-sauts au collecteur AppFlow.

   > **Remarque**
   >
   > L'option de modèle**HDX** est disponible uniquement pour l'appliance Citrix SD-WAN PE, elle doit être activée sur l'appliance Data Center

5. Dans le champ **Adresse IP**, tapez l'adresse IP du système de collecte AppFlow externe (serveur Citrix ADM).
6. Dans le champ **Port**, tapez le numéro de port sur lequel le système collecteur AppFlow externe écoute. La valeur par défaut est 4739.
7. Activez la case à cocher **Citrix ADM** pour spécifier que Citrix ADM est le collecteur AppFlow.

   > **Remarque**
   >
   > - Citrix ADM ne prend actuellement pas en charge la collection IPFIX.
   > - Vous pouvez ajouter jusqu'à quatre collecteurs AppFlow. Citrix ADM ou tout collecteur AppFlow prenant en charge le protocole IPFIX.

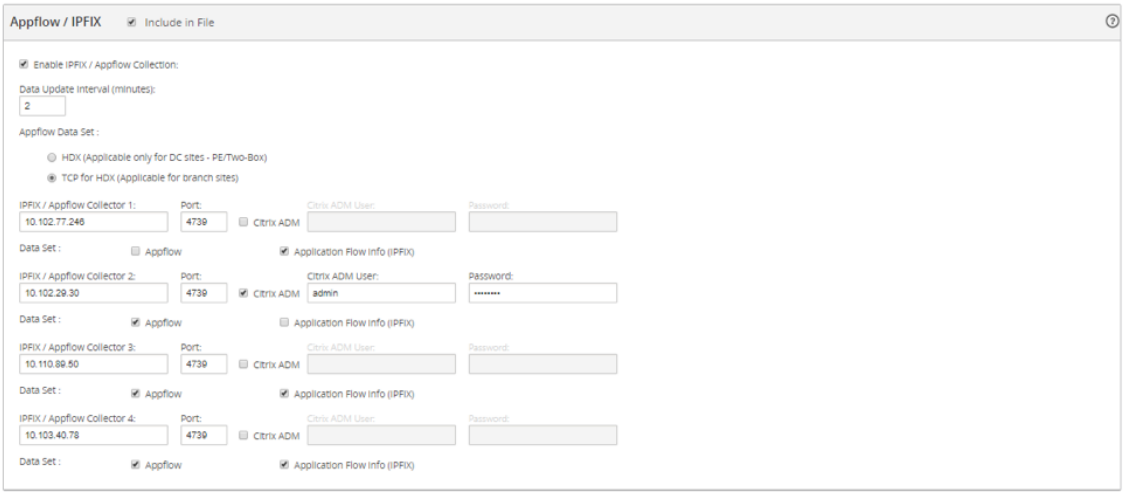
8. Entrez les informations d'identification du serveur Citrix ADM
9. Cliquez sur **Appliquer les paramètres**.

Les appliances Citrix SD-WAN SE/PE sont découvertes et répertoriées sur Citrix ADM. Les appliances Citrix SD-WAN SE/PE envoient les données d'analyse à Citrix ADM. Pour plus d'informations, consultez AppFlow et IPFIX.

Pour configurer Citrix ADM en tant que collecteur AppFlow à l'aide de Citrix SD-WAN Center :

1. Dans l'interface utilisateur de gestion du Citrix SD-WAN Center, accédez à **Configuration** > Paramètres de **l'appliance**.
2. Accédez à la section **AppFlow/IPFIX** et choisissez **Inclure dans le fichier**.

3. Sélectionnez **Activer IPFIX/AppFlow Collection**.



4. Dans le champ **Intervalle** de **mise à jour des données**, spécifiez l'intervalle de temps, en minutes, auquel les rapports AppFlow sont exportés vers le collecteur AppFlow.

> **Remarque**
>
> Si Citrix ADM est le collecteur AppFlow, l'intervalle de mise à jour des données doit être de 1 minute.

5. Procédez comme suit :

   - Choisissez **HDX** pour envoyer des données d'aperçu HDX au collecteur AppFlow.
   - Choisissez **TCP pour HDX,** pour envoyer des données d'informations multi-sauts au collecteur AppFlow. Cela doit être activé sur les appliances de branche.

> **Remarque**
>
> L'option de modèle**HDX** est disponible uniquement pour l'appliance Citrix SD-WAN PE, elle doit être activée sur l'appliance Data Center.

6. Dans le champ **IPFIX/AppFlow Collector**, tapez l'adresse IP du système de collecte AppFlow externe (serveur Citrix ADM).
7. Dans le champ **Port**, tapez le numéro de port sur lequel le système collecteur AppFlow externe écoute. La valeur par défaut est 4739.
8. Activez la case à cocher **Citrix ADM** pour spécifier que Citrix ADM est le collecteur AppFlow.
9. Entrez les informations d'identification du serveur Citrix ADM.

> **Remarque**

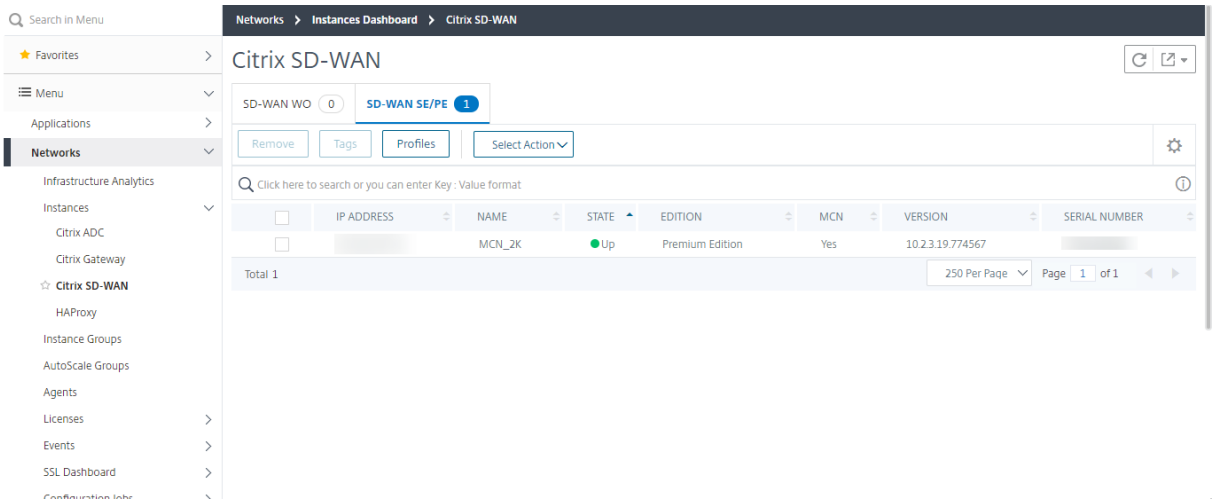
> Vous pouvez ajouter jusqu'à quatre collecteurs AppFlow. Citrix ADM ou tout collecteur AppFlow prenant en charge le protocole IPFIX.

10. Enregistrez et exportez la configuration vers les appliances gérées.

    Pour plus d'informations, consultez Comment configurer et exporter les paramètres du dispositif vers des dispositifs gérés.

Pour plus d'informations sur la configuration de Citrix ADM en tant que collecteur AppFlow à l'aide de Citrix SD-WAN Center, AppFlow et IPFIX.

Les appliances Citrix SD-WAN SE/PE sont découvertes et répertoriées par Citrix ADM.Les appliances Citrix SD-WAN SE/PE sont découvertes et répertoriées dans Citrix ADM. Pour afficher les appliances Citrix SD-WAN SE/PE découvertes, dans l'interface Web Citrix ADM, accédez à **Réseaux** > **Instances** > **Citrix SD-WAN** et sélectionnez **SD-WAN SE/PE/AE**.



Vous pouvez afficher l'adresse IP, le nom, l'état actuel, l'édition du logiciel et la version des appliances découvertes. Vous pouvez également voir si l'appliance est un nœud de Controller maître (MCN) ou non.

Vous pouvez effectuer les actions suivantes :

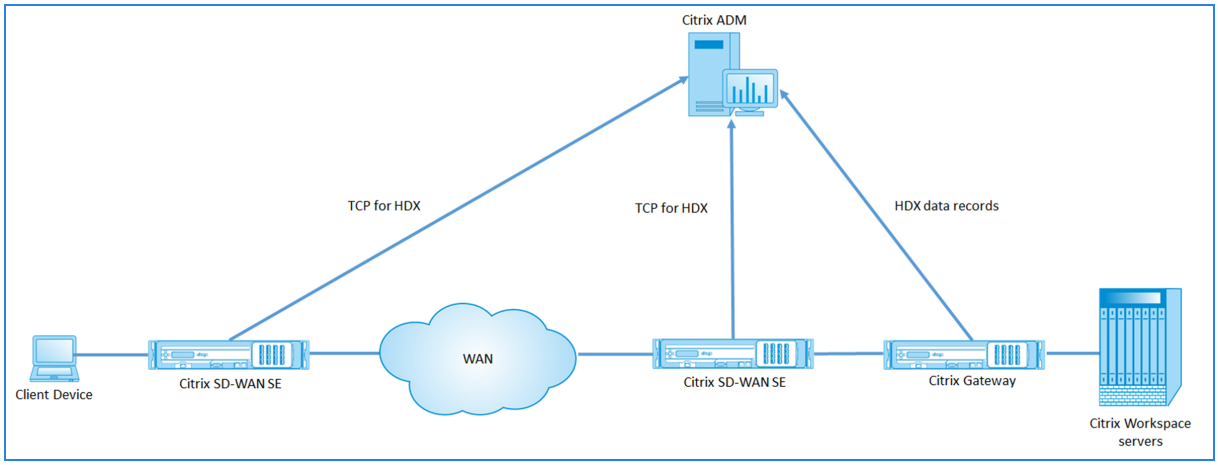
- Afficher et supprimer les profils d'instance.
- Supprimez des instances de Citrix ADM.
- Redécouvrez les instances.

Pour une appliance Citrix SD-WAN PE, vous pouvez afficher des enregistrements de données HDX ou des données multi-sauts, en fonction de la configuration AppFlow. Une appliance Citrix SD-WAN SE fournit uniquement des données multi-sauts. Pour plus d'informations, consultez Affichage des rapports et des mesures HDX Insight et Affichage des données d'analyse Citrix SD-WAN pour un déploiement multi-sauts.

Afficher les données d'analyse Citrix SD-WAN pour un déploiement multi-sauts

February 1, 2024

Un déploiement de réseau à sauts multiples comporte plusieurs appareils entre le client et le serveur, comme illustré dans la figure suivante. Dans ce type de déploiement, les appliances Citrix SD-WAN SE et Citrix Gateway sont ajoutés à Citrix ADM et AppFlow est activé.



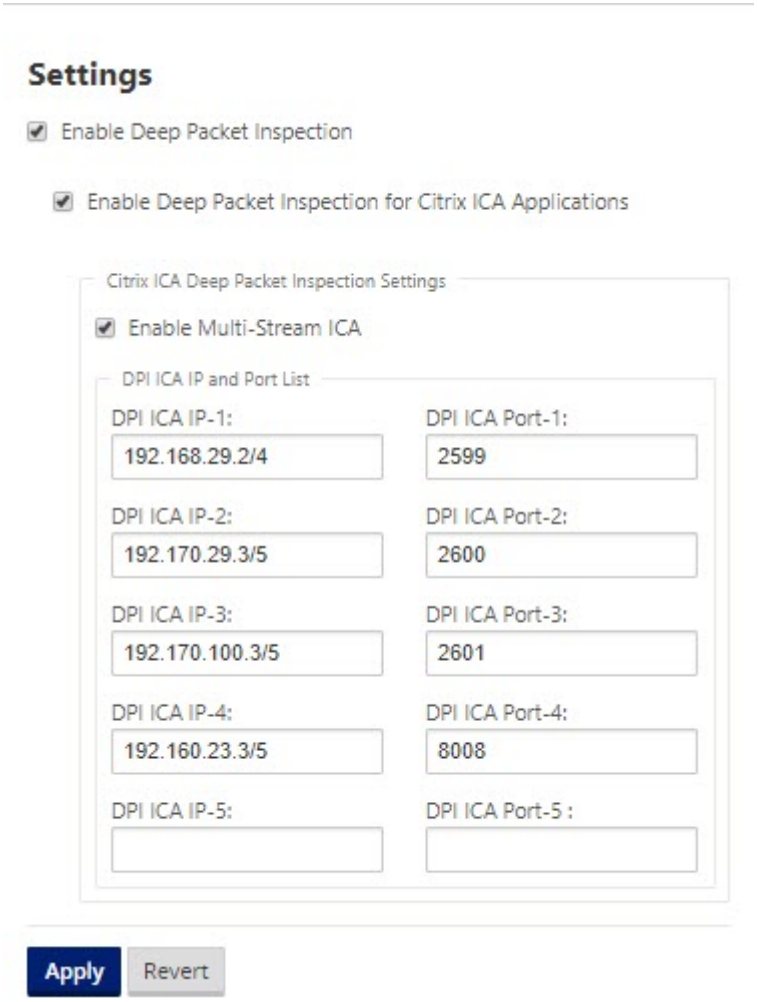
Citrix ADM identifie l'appliance à partir de laquelle il reçoit les données, en fonction du nombre de sauts et de l'ID de chaîne de connexion. Le nombre de sauts représente le nombre d'appareils par lesquels le trafic circule du client vers le serveur. L'ID de chaîne de connexion représente les connexions de bout en bout entre le client et le serveur.

Citrix ADM utilise le nombre de sauts et l'ID de chaîne de connexion pour corréler les données des appliances et génère les rapports.

Pour que les appliances Citrix SD-WAN SE envoient les données d'analyse à Citrix ADM, vous devez configurer l'adresse IP virtuelle de Citrix Gateway comme adresse IP DPI ICA et définir le numéro de port DPI ICA sur 443.

Pour configurer les paramètres DPI de l'ICA :

1. ****Dans l'interface utilisateur de l'appliance Citrix SD-WAN SE, accédez **à l'éditeur de configuration> Avancé ** Global > **Applications ** Paramètres****
2. Sélectionnez **Activer l'inspection approfondie des paquets > Activer l'inspectionapprofondie des paquets pour les applications Citrix ICA > Activer l'inspectionICA multi-flux**



3. Dans le champ **DPI ICA IP-1**, entrez l'adresse IP virtuelle et le préfixe Citrix Gateway.
4. Dans le champ **DPI ICA Port-1**, entrez le numéro de port 443.
5. Cliquez sur **Appliquer** et exportez la configuration vers l'appliance à l'aide du processus de gestion des modifications.

Dans Citrix ADM, pour chaque session ICA active, vous pouvez afficher un diagramme de session dans HDX Insight. Les diagrammes de session fournissent des informations détaillées sur les appareils situés sur le chemin de connexion. Ils fournissent également un aperçu de la latence côté client/côté serveur entre un périphérique réseau et son prochain saut immédiat. Ces informations vous permettent d'identifier la cause première du retard et de résoudre les problèmes de performances.

Citrix SD-WAN SE n'envoie pas d'enregistrements de données HDX. Il fournit uniquement des informations TCP pour HDX. Les données HDX insights sont fournies par les périphériques HDX insights de votre réseau (par exemple, Citrix ADC ou Citrix Gateway).

L'appliance Citrix SD-WAN PE peut envoyer des données TCP pour HDX ou des données d'information HDX, en fonction de la configuration AppFlow de l'appliance.Le modèle HDX doit être activé sur l'

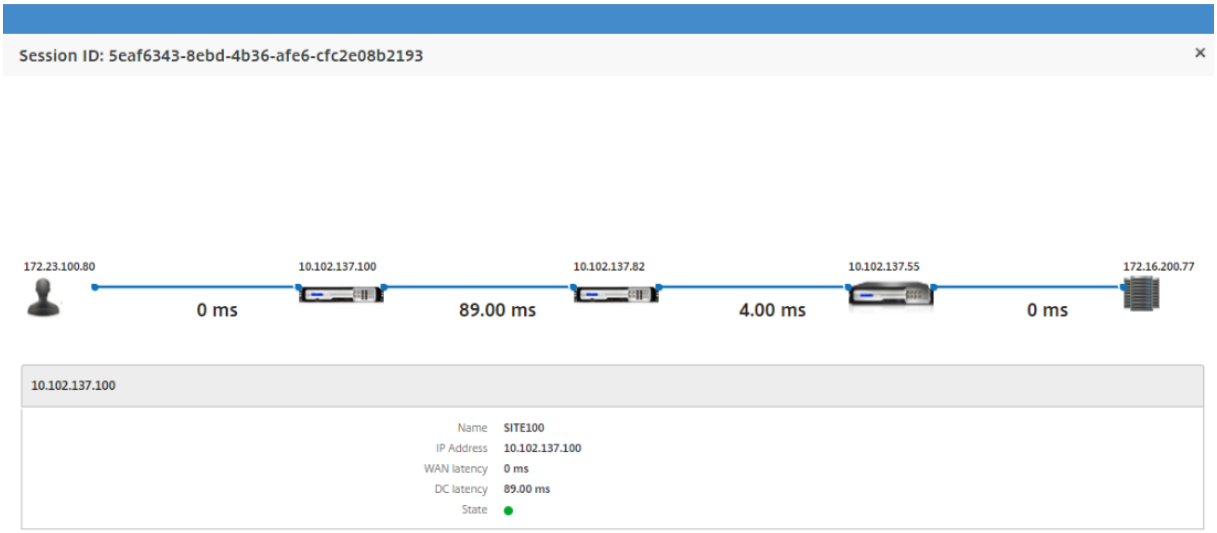
appliance Data Center.

> **Remarque**
>
> Dans un déploiement à sauts multiples, assurez-vous qu'un seul des périphériques réseau envoie des données HDX Insight. Les autres périphériques réseau peuvent envoyer du TCP pour les données HDX.

Pour afficher les données multi-sauts, procédez comme suit :

Dans l'interface Web Citrix ADM, accédez àHDX Insight****> Utilisateurs ** Sessions en **cours ou HDX **Insight**** Applications****Sessions en cours** et cliquez sur l'icône de diagramme.****

Le diagramme de topologie du réseau apparaît.



Cliquez sur n'importe quel élément du réseau pour afficher plus d'informations.

> **Remarque**
>
> Les informations affichées dépendent de l'élément de réseau sélectionné.

Les paramètres suivants apparaissent pour les appliances Citrix :

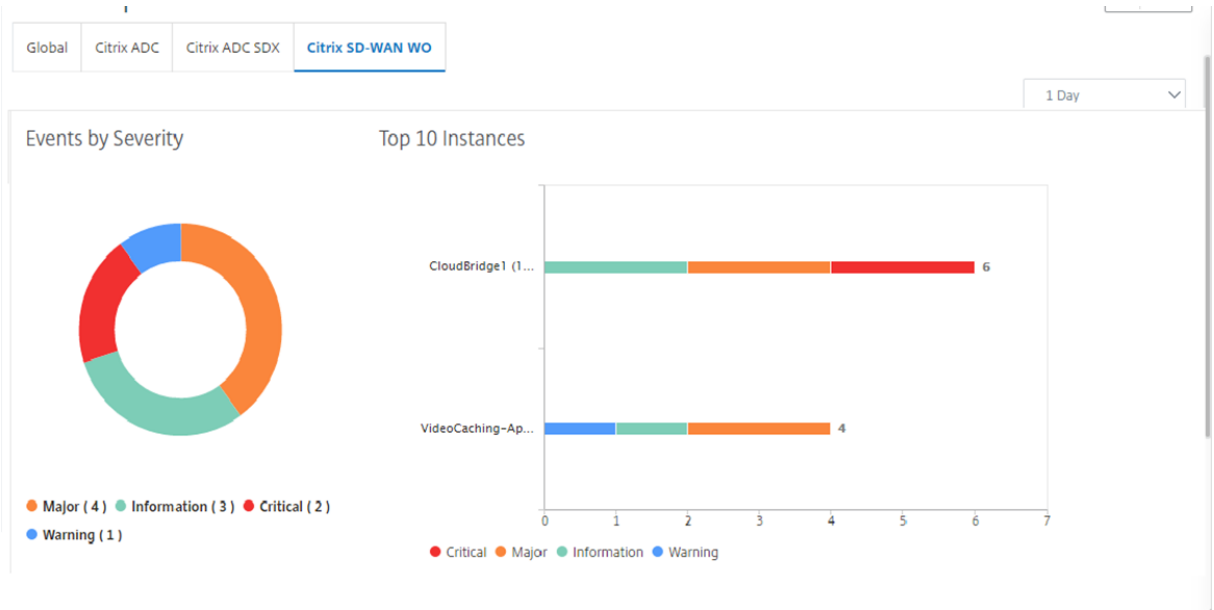
- **Nom** : nom de l'appliance Citrix.
- **Adresse IP** : adresse IP de l'appliance.
- **Latence WAN** : latence causée par le côté client du réseau. C'est-à-dire de l'appliance Citrix à l'utilisateur final.
- **Latence DC** : latence causée par le côté serveur du réseau. C'est-à-dire de l'appliance Citrix aux serveurs principaux.
- **État : État**d'accessibilité de l'appareil.

Voir les rapports d'événements des instances de Citrix SD-WAN WANOP

February 1, 2024

Vous pouvez afficher les événements des 10 premières instances WANOP SD-WAN sous forme de représentation graphique en accédant à **Réseaux** > **Événements** > **Rapports** et en sélectionnant **Citrix SD-WAN WO**.

Les événements sont affichés en fonction de leur gravité pour chaque instance, vous pouvez cliquer sur chaque gravité pour en savoir plus sur le nombre d'événements, le moment où ils se sont produits et la catégorie à laquelle ils appartiennent.



Afficher les rapports réseau des instances de Citrix SD-WAN WANOP

February 1, 2024

Vous pouvez afficher les rapports liés au réseau d'optimisation WAN dans Citrix ADM, à l'aide de ces données, vous pouvez résoudre les problèmes réseau ou analyser le comportement de vos périphériques Citrix SD-WAN WANOP. Vous pouvez consulter les rapports de statistiques réseau de vos périphériques d'optimisation WAN au cours des dernières heures, une journée, une semaine ou un mois.

Vous pouvez consulter les rapports suivants :

Rapports	Description
Accélération	Utilisez ce rapport pour analyser le schéma du trafic accéléré (KBPS par classe de service) et le nombre de connexions TCP accélérées passant par l'appliance d'optimisation WAN. Cela inclut le nombre de connexions TCP passant par le périphérique d'optimisation WAN qui subissent une accélération, le nombre de connexions ouvertes et semi-fermées sélectionnées pour l'accélération et le nombre de connexions semi-ouvertes qui sont candidates pour accélération.
Passer la connexion	Utilisez ce rapport pour afficher les connexions non accélérées du périphérique d'optimisation WAN.
Classe de service	Utilisez ce rapport pour afficher les économies de bande passante envoyées et recevoir en fonction du type de classe de service défini pour le périphérique d'optimisation WAN.
Application	Utilisez ce rapport pour afficher le volume de données envoyé et reçu en bits par seconde pour les applications exécutées sur le périphérique d'optimisation WAN.
Utilisation de l'UC	Utilisez ce rapport pour afficher l'utilisation de l'UC du périphérique d'optimisation WAN sous forme de pourcentage.

Rapports	Description
Augmentation de la capacité	Utilisez ce rapport pour afficher le taux de compression d'envoi cumulé pour le périphérique d'optimisation WAN.
Réduction des données	Utilisez ce rapport pour afficher la transmission et recevoir des économies de bande passante en pourcentage. Vous pouvez également analyser la bande passante de transmission et recevoir séparément des valeurs d'économie de bande passante pour le périphérique d'optimisation WAN.
Utilisation des liens	Utilisez ce rapport pour afficher l'utilisation du lien de transmission et recevoir l'utilisation du lien pour l'optimisation du réseau étendu sous forme de pourcentage.
Utilisation du plugin	Utilisez ce rapport pour afficher le nombre de plugins connectés au périphérique d'optimisation WAN.
Perte de paquets	Utilisez ce rapport pour afficher les paquets envoyés par lien et les paquets reçus reçus par lien pour les liens définis dans le périphérique d'optimisation WAN.
Débit	Utilisez ce rapport pour afficher le volume de liaison envoyé et le volume de liaison reçu en bits par seconde pour le périphérique d'optimisation WAN.
QoS	Utilisez ce rapport pour afficher le volume QOS envoyé et QOS Recevoir en bits par seconde pour le périphérique d'optimisation WAN.

Pour afficher les rapports réseau WANOP Citrix SD-WAN :

1. Dans Citrix ADM, accédez à **Réseaux**> **Network Reporting** > **Citrix SD-WAN WO**.
2. Dans la liste déroulante **Nom** du rapport, sélectionnez un rapport à afficher.
3. **Dans la liste déroulante Instances**, sélectionnez l'instance WANOP Citrix SD-WAN pour laquelle vous souhaitez afficher le rapport.
4. Dans la liste déroulante **Durée**, sélectionnez l'intervalle de temps.

5. Cliquez sur **Exécuter**.

Sauvegarder les instances de Citrix SD-WAN WANOP

February 1, 2024

Vous pouvez sauvegarder l'état actuel d'une instance et utiliser ultérieurement les fichiers sauvegardés pour restaurer l'instance au même état. Il est recommandé de sauvegarder une instance avant de la mettre à niveau ou pour des raisons de précaution. Une sauvegarde d'un système stable vous permet de restaurer le système à un point stable au cas où il devient instable. Il existe plusieurs façons d'effectuer des sauvegardes et des restaurations sur une instance WANOP Citrix SD-WAN. Vous pouvez également sauvegarder et restaurer des instances à l'aide de l'interface graphique, de l'interface de ligne de commande ou utiliser Citrix ADM pour effectuer des sauvegardes. Citrix ADM sauvegarde l'état actuel de vos instances WANOP Citrix SD-WAN gérées à l'aide des appels NITRO, du protocole SSH (Secure Shell) et du protocole SCP (Secure Copy).

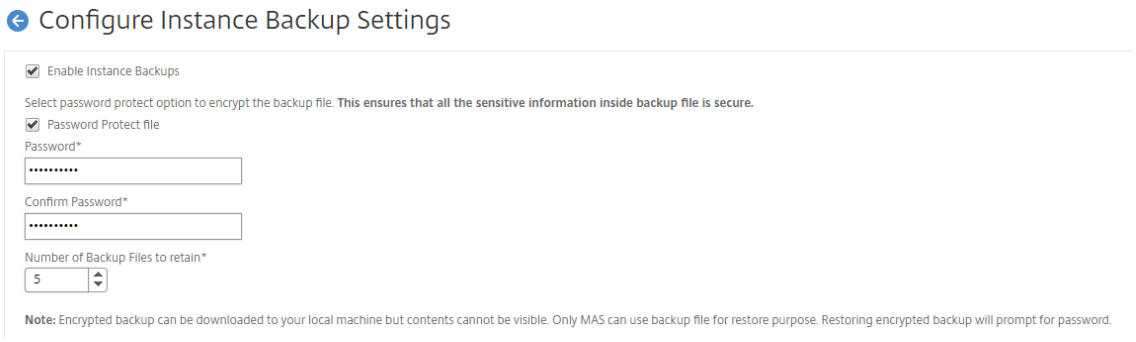
Configuration des paramètres de sauvegarde d'instance

Avant d'effectuer une sauvegarde de l'instance WANOP Citrix SD-WAN dans Citrix ADM, vous devez configurer les paramètres de sauvegarde d'instance sur Citrix ADM.

Pour configurer les paramètres de sauvegarde d'instance :

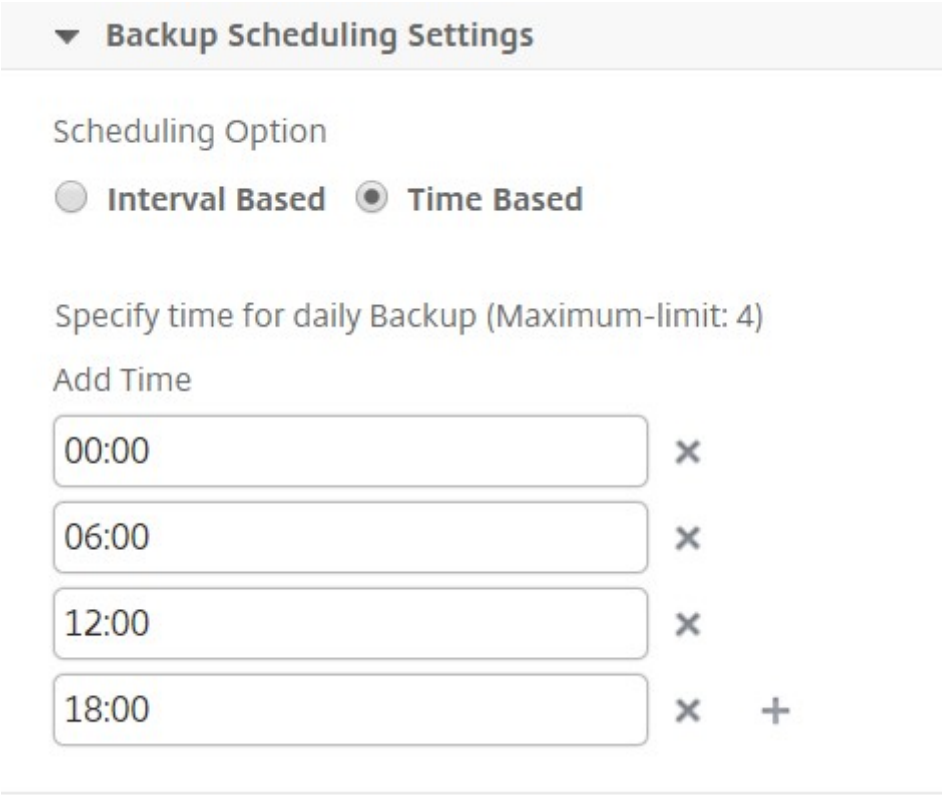
1. Dans Citrix ADM, accédez à **Système** > **Administration système**. Dans le volet droit, sous Paramètres de **sauvegarde, sélectionnez Paramètres**de **sauvegarde d'instance**.
2. Sélectionnez **Activer les sauvegardes d'instance**. Cette option est activée par défaut.
3. Sélectionnez **Mot de passe Protect File** pour chiffrer le fichier de sauvegarde. Le chiffrement du fichier de sauvegarde garantit la sécurité des informations sensibles contenues dans le fichier de sauvegarde.
4. Dans le champ **Nombre de fichiers de sauvegarde à conserver**, spécifiez le nombre de fichiers de sauvegarde à conserver dans Citrix ADM. Vous pouvez conserver jusqu'à 50 fichiers de sauvegarde.

   > **Remarque**
   >
   > Chaque fichier de sauvegarde nécessite une certaine exigence de stockage. Citrix vous recommande de stocker un nombre optimal de fichiers de sauvegarde sur Citrix ADM en fonction de vos besoins.



5. Définissez les paramètres de planification de sauvegarde. Choisissez l'une des options suivantes :

   - **Basé sur l'intervalle** : un fichier de sauvegarde est créé dans Citrix ADM après l'expiration de l'intervalle spécifié. L'intervalle de sauvegarde par défaut est de 12 heures.
   - **Basé sur le temps** - Vous pouvez spécifier l'heure dans le format « heures:minutes » à laquelle la sauvegarde doit se produire. Citrix ADM permet jusqu'à quatre sauvegardes quotidiennes sur les instances.



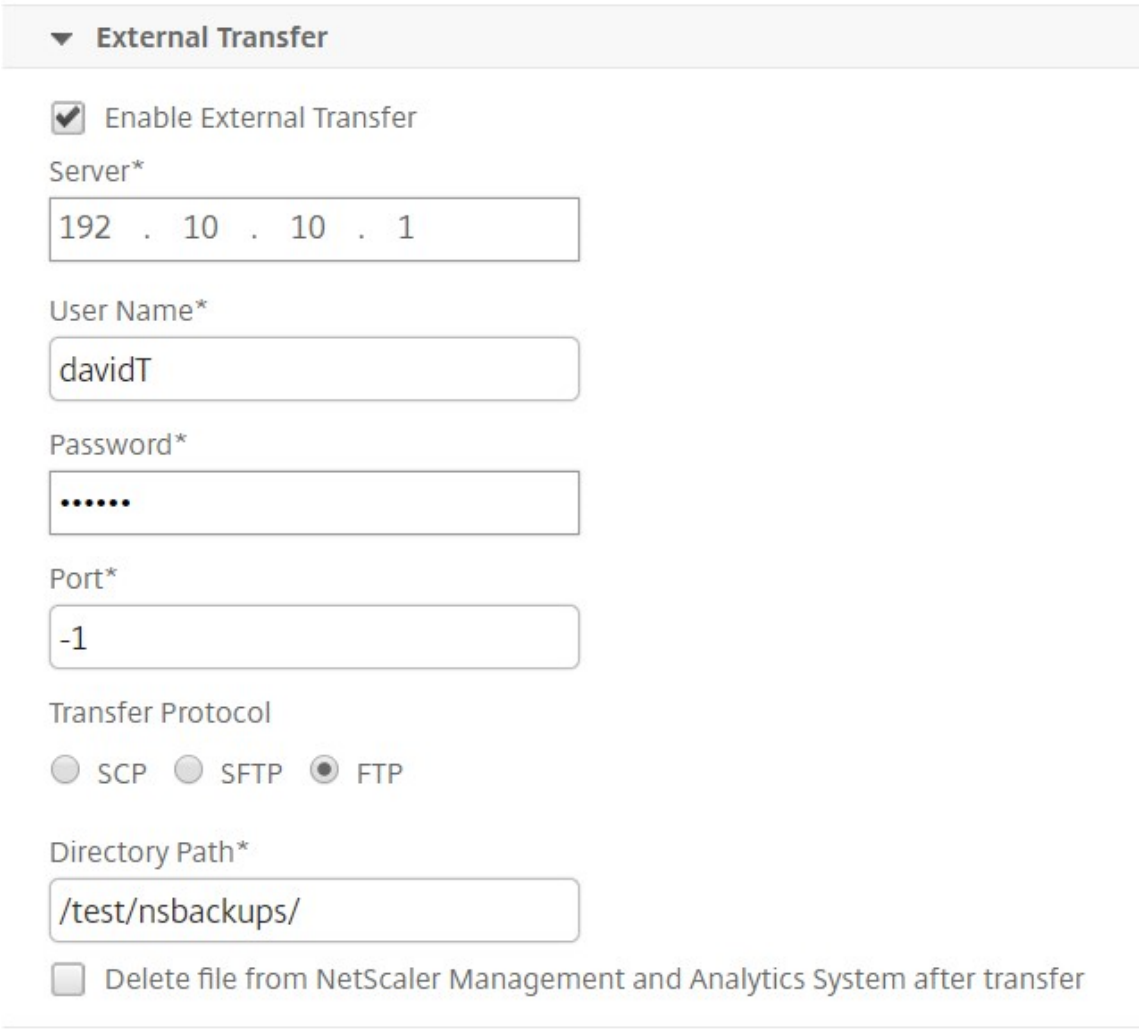
> **Remarque**
>
> Ignorez la section **Paramètres Citrix ADC** ; ces paramètres ne sont pas applicables aux instances WANOP Citrix SD-WAN.

6. Sélectionnez **Activer le transfert externe** pour transférer les fichiers de sauvegarde d'instance

vers un emplacement externe. Entrez les valeurs des champs suivants :

- **Serveur** : adresse IP du serveur externe.
- **Nom d'**utilisateur : nom d'utilisateur du serveur externe
- **Mot de passe** : Mot de passe du serveur externe.
- **Port** : numéro de port utilisé pour communiquer avec le serveur externe.
- **Protocole de transfert** : Protocole à utiliser pour transférer les fichiers de sauvegarde de Citrix ADM vers le serveur externe.

Vous pouvez également supprimer le fichier de sauvegarde de Citrix ADM après l'avoir transféré sur le serveur externe.



7. Cliquez sur **OK**.

> **Remarque**
>
> Citrix ADM envoie un piège SNMP ou une notification Syslog à lui-même en cas d'échec de sauvegarde pour l'une des instances WANOP Citrix SD-WAN sélectionnées.

Création d'une sauvegarde d'une instance WANOP Citrix SD-WAN

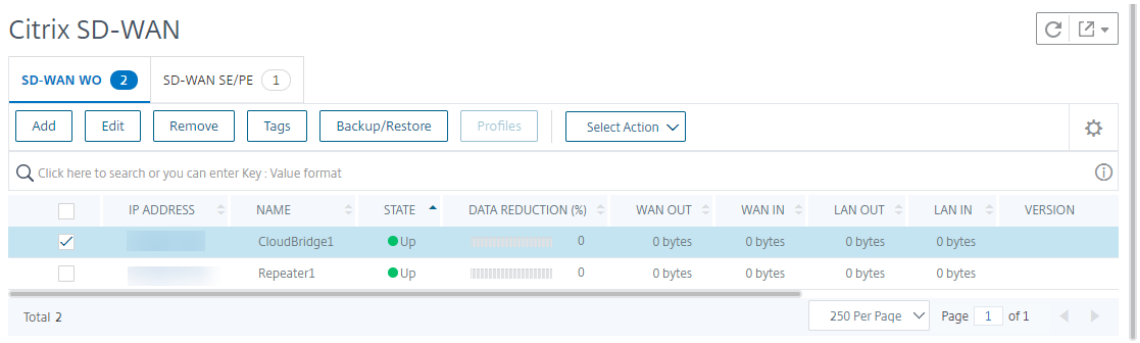
La procédure de création d'une sauvegarde pour l'instance WANOP Citrix SD-WAN s'applique à un utilisateur administrateur, à l'aide du profil nsroot par défaut.

Pour plus d'informations sur, comment un utilisateur personnalisé peut reprendre la sauvegarde d'une instance WANOP Citrix SD-WAN, reportez-vous à la section Création d'une sauvegarde d'instance WANOP Citrix SD-WAN pour les utilisateurs personnalisés de cette rubrique.

Assurez-vous qu'une instance Citrix SD-WAN WANOP est ajoutée à Citrix ADM. Pour plus d'informations, reportez-vous à la section Ajout d'une instance à Citrix ADM.

Pour créer une sauvegarde pour l'instance WANOP Citrix SD-WAN :

1. Dans Citrix ADM, accédez à **Réseaux** > **Instances** > **Citrix SD-WAN**.
2. Dans **SD-WAN WO**, sélectionnez l'instance WANOP Citrix SD-WAN à sauvegarder, puis cliquez sur **Sauvegarde/Restaurer**.



3. Dans la page **Fichiers de sauvegarde**, cliquez sur **Sauvegarder**.
4. Chiffrez votre fichier de sauvegarde à l'aide de l'une des options suivantes :
   - Sélectionnez **Fichier protégé par mot de passe** et entrez un mot de passe pour chiffrer les fichiers de sauvegarde.
   - Sélectionnez **Utiliser le mot de passe global** pour utiliser le mot de passe global que vous avez spécifié sur la page des paramètres de sauvegarde de l'instance.
5. Cliquez sur **Créer une sauvegarde**

Création d'une sauvegarde de l'instance WANOP Citrix SD-WAN pour les utilisateurs personnalisés

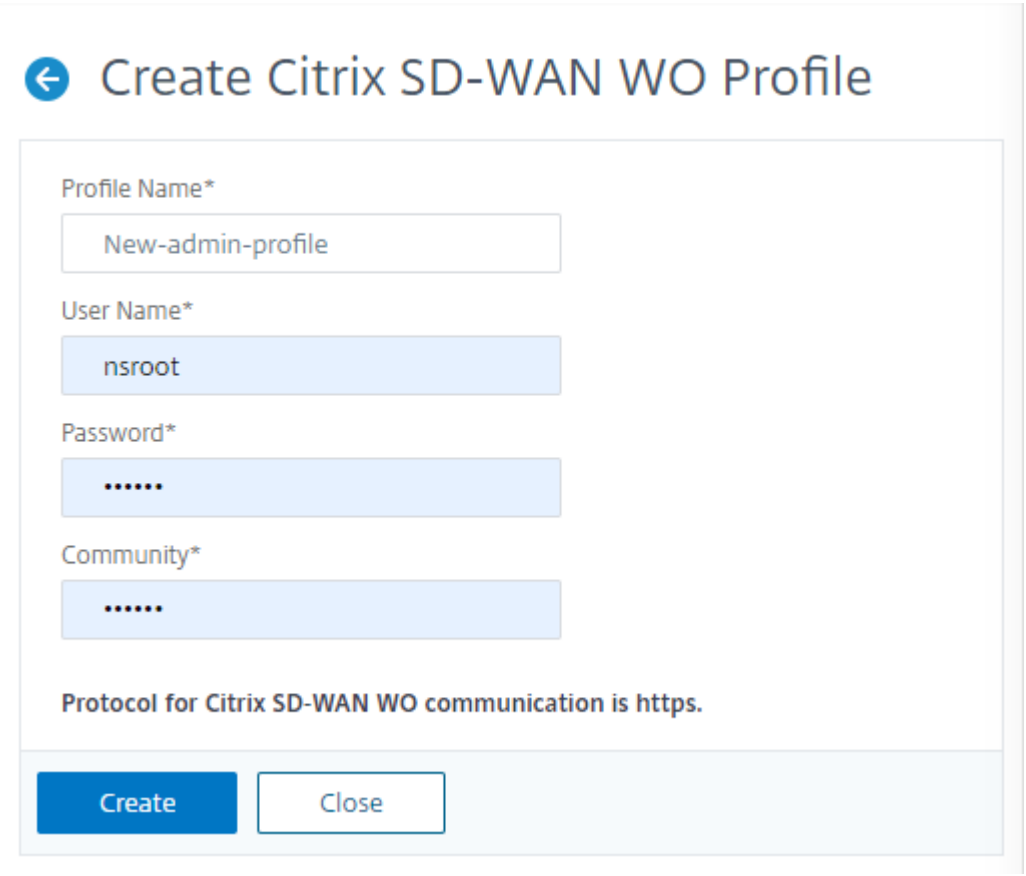
Si vous avez créé un utilisateur personnalisé avec des privilèges d'administrateur dans l'instance WANOP Citrix SD-WAN, suivez la procédure suivante pour ajouter une instance et reprendre cette instance à l'aide de Citrix ADM.

L'opération de sauvegarde par les utilisateurs personnalisés n'est pas prise en charge sur les plates-formes WANOP SD-WAN 400/800/1000WS/2000/2000WS/3000/4000/5000/4100/5100.

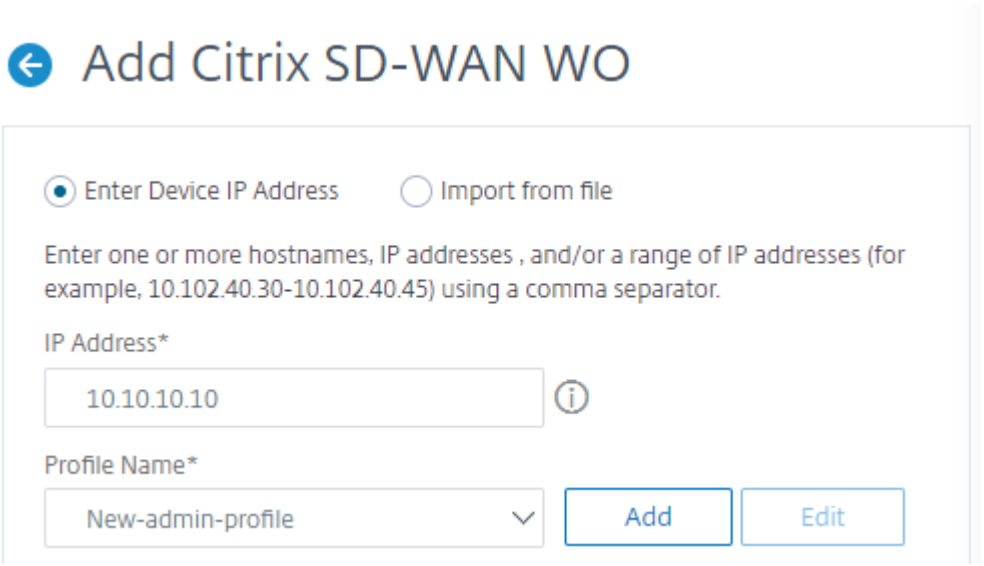
> **Remarque**
>
> Citrix vous recommande d'utiliser le profil nsroot par défaut, lors de la création de la sauvegarde des plates-formes avancées Citrix SD-WAN dans Citrix ADM.

Pour ajouter une instance WANOP Citrix SD-WAN et effectuer une sauvegarde pour un utilisateur personnalisé :

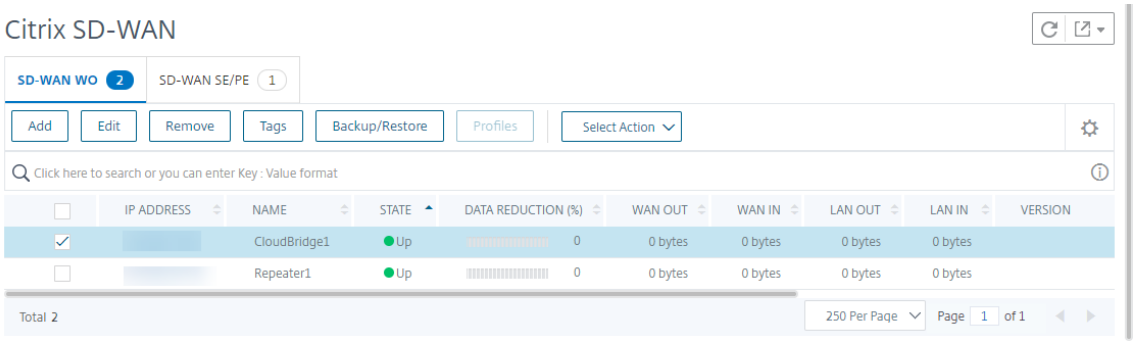
1. Dans Citrix ADM, accédez à **Réseaux** > **Instances** > **Citrix SD-WAN** et sélectionnez **SD WAN WO**.
2. Cliquez sur **Ajouter**.
3. Dans le champ **Adresse IP**, entrez l'adresse IP de l'instance WANOP Citrix SD-WAN.
4. Cliquez sur **Ajouter** en regard **du champ Nom du profil** pour créer un nouveau profil. La fenêtre **Créer un profil de WO Citrix SD-WAN** apparaît.



5. Dans le **champ Nom du profil**, entrez un nom pour le profil.
6. Dans le champ **Nom d'utilisateur**, entrez le nom d'utilisateur de l'utilisateur personnalisé que vous créez sur l'instance WANOP SD-WAN.
7. Dans le **champ Mot de passe**, entrez le mot de passe que vous avez défini pour l'utilisateur personnalisé dans l'instance WANOP SD-WAN.
8. Dans le champ **Communauté**, entrez la chaîne de communication SNMP configurée sur l'appliance WANOP SD-WAN. (par exemple : public)
9. Cliquez sur **Créer**.
10. Dans le champ **Nom du profil**, sélectionnez le profil nouvellement créé et cliquez sur **OK**.



11. Accédez à **Réseaux** > **Instances** > **Citrix SD-WAN**.
12. Dans **SD-WAN WO**, sélectionnez l'instance WANOP Citrix SD-WAN que vous venez d'ajouter, puis cliquez sur**Sauvegarde/Restaurer**.



13. Dans la page **Fichiers de sauvegarde**, cliquez sur **Sauvegarder**.
14. Chiffrez votre fichier de sauvegarde à l'aide de l'une des options suivantes :

    - Sélectionnez **Fichier protégé par mot de passe** et entrez un mot de passe pour chiffrer les fichiers de sauvegarde.
    - Sélectionnez **Utiliser le mot de passe global** pour utiliser le mot de passe global que vous avez spécifié sur la page des paramètres de sauvegarde de l'instance.

Remarque

Vous pouvez télécharger le fichier de sauvegarde chiffré sur votre ordinateur local, mais vous ne pouvez pas afficher son contenu. Seul Citrix ADM peut utiliser ces fichiers de sauvegarde à des fins de restauration. La restauration d'une sauvegarde cryptée demandera le mot de passe.

15. Cliquez sur **Créer une sauvegarde**.

Important

```
1. Pour une appliance Citrix SD-WAN WANOP VPX, Citrix ADM
   sauvegarde uniquement le fichier de configuration CB Broker
   .
```

a) Pour une plate-forme WANOP Citrix SD-WAN avancée, Citrix ADM sauvegarde les éléments suivants : ·

- Fichier de configuration du broker CB
- Fichier de configuration NTP
- DNS
- Fichier de configuration SNMPD
- Fichier de configuration Syslog
- Certificat SSL, clés et stratégies
- Fichier de base de données SVM
- Composants (au format XML)
- Ressources (au format XML)

Les fichiers sauvegardés dans les dossiers respectifs sont répertoriés dans le tableau suivant. Notez que si un nom de dossier est suivi d'un « * », tous les fichiers de ce dossier sont sauvegardés.

Répertoire	Sous-répertoire ou fichiers
/br_broker/	CB-6bbb660A/ ws.conf
/etc/	resolv.conf
/mps/	mps_devices.xml
/mpsconfig/	ssl/*, ntp.conf, snmpd.conf, syslog.conf
/mpsdb/	mpsdb_dump.sql
/ns/	NS-6CBB660A/*

/var/	mps/policy/, *mps/ssl_certs/ sdx_default_ssl_cert, mps/ssl_keys/ sdx_default_ssl_key, mps/tenants/*

Gérer les instances HaProxy

February 1, 2024

HAProxy est un équilibreur de charge open source qui peut équilibrer la charge n'importe quel service TCP ou HTTP. Pour plus d'informations sur HAProxy, reportez-vous à la section http://www.haproxy.org/.

Citrix Application Delivery Management (Citrix ADM) prend en charge HaProxy version 1.4.24 ou ultérieure. Lorsque vous ajoutez un hôte sur lequel vous avez provisionné les instances HAProxy à Citrix ADM, Citrix ADM détecte les instances HAProxy sur l'hôte et vous permet de les surveiller. Il vous montre les types d'informations suivants sur la configuration HaProxy sur les instances :

- Frontend —Comment les demandes doivent être transmises au back-end.
- Backend —Ensemble de serveurs qui reçoivent les demandes transférées.
- Serveurs : serveurs parmi lesquels la charge HaProxy équilibre le trafic.

Pour plus d'informations, consultez http://www.haproxy.org/download/1.7/doc/configuration.txt.

Citrix ADM fournit également un tableau de bord des applications HAProxy sur lequel vous pouvez surveiller les frontends en temps réel. Pour plus d'informations, consultez Tableau de bord de l'application HAProxy.

Ajouter des instances HAProxy à Citrix ADM

February 1, 2024

Dans Citrix Application Delivery Management (Citrix ADM), vous devez ajouter manuellement les détails de l'hôte sur lequel vous avez provisionné l'instance HaProxy. Après avoir ajouté ces détails, Citrix ADM découvre automatiquement les instances HaProxy provisionnées sur l'hôte et les ajoute à Citrix ADM Inventory. Il découvre également tous les fronts, backends et serveurs configurés sur les instances HaProxy, et traite les fronts comme des applications découvertes.

Conditions préalables

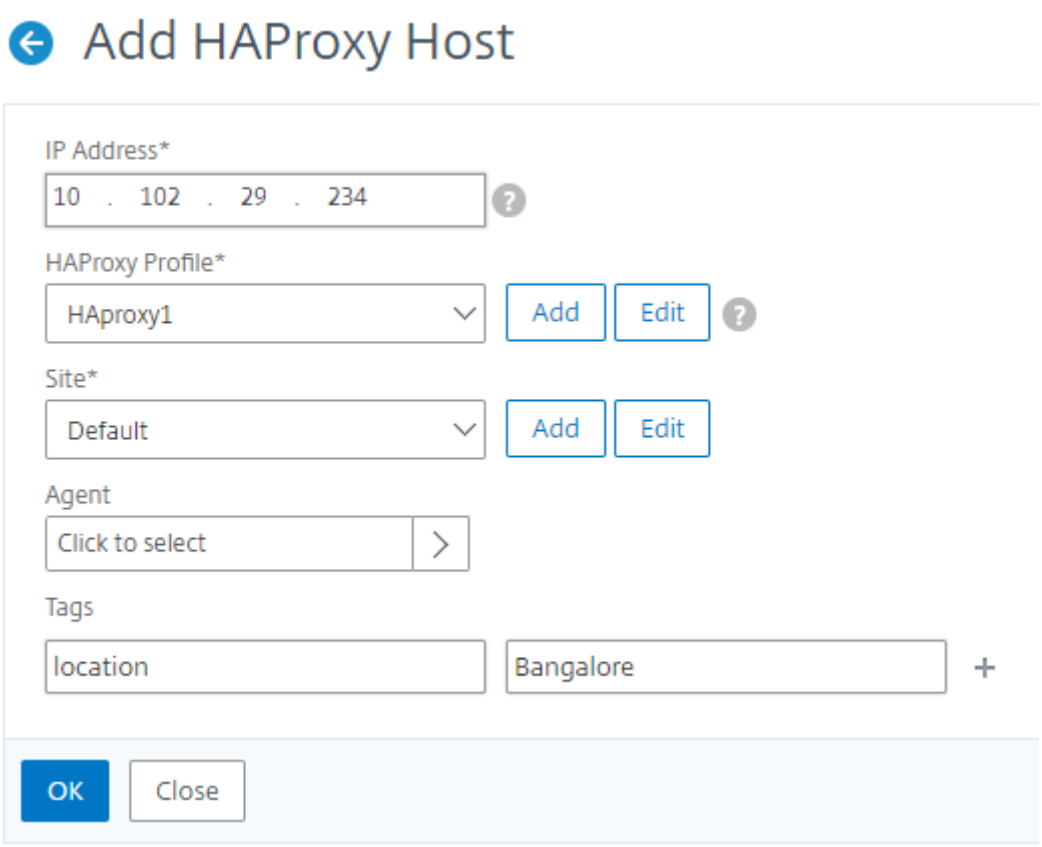
Assurez-vous d'avoir :

- Déploiement d'une instance HaProxy sur un hôte dans votre déploiement. Pour plus d'informations, consultez http://www.haproxy.org/#docs.
- Identifiée et décidé du nombre de fronts pour lesquels vous souhaitez afficher les statistiques d'application sur le tableau de bord de l'application HAProxy. Par défaut, le tableau de bord des applications HaProxy affiche les statistiques de 30 applications découvertes. Pour plus d'informations sur HAProxy App Dashboard, voir Tableau de bord de l'application HAProxy Si vous souhaitez afficher les statistiques de plus de 30 applications découvertes, vous devez acheter une licence distincte. Pour plus d'informations, consultez la section Licences tierces.

> **Important**
>
> Citrix ADM nécessite l'accès à l'hôte pour découvrir les instances HaProxy qui s'y trouve. Vous pouvez fournir l'accès à Citrix ADM en fournissant la paire de clés SSH de l'hôte ou en utilisant le mot de passe de l'hôte. Si vous souhaitez fournir un accès à l'aide de la paire de clés SSH, assurez-vous de générer la paire de clés privées et publiques SSH dans l'hôte et d'ajouter la clé publique aux clés autorisées sur l'hôte. En outre, le compte d'utilisateur SSH doit disposer d'autorisations de superutilisateur.

Pour ajouter une instance HaProxy à Citrix ADM :

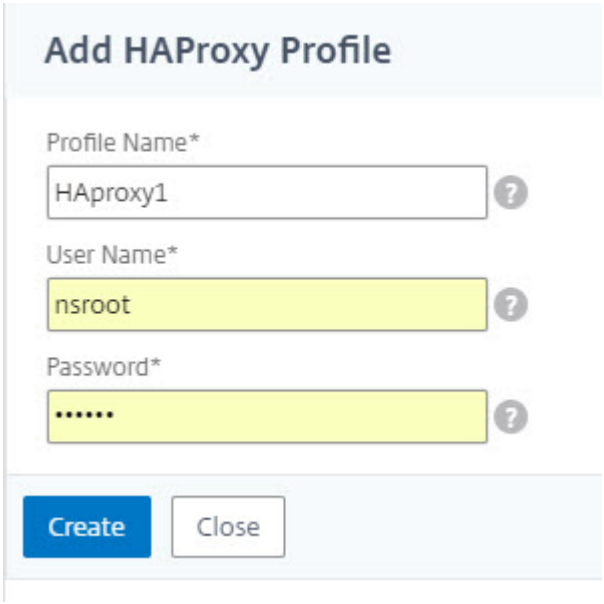
1. Accédez à **Réseaux** > **Instances**. Sous **Instances**, sélectionnez **HAProxy** et cliquez sur **Ajouter**.
2. Dans la boîte de dialogue **Ajouter un hôte HaProxy**, procédez comme suit :



1. Dans le champ **Adresse IP**, entrez l'adresse IP de l'hôte sur lequel vous avez provisionné les instances HAProxy.

    a) Dans le menu **Profil HaProxy**, sélectionnez un profil HaProxy existant ou créez et sélectionnez un nouveau profil HaProxy. Pour créer un profil HaProxy, cliquez sur **Ajouter**.

        i. Dans la boîte de dialogue **Ajouter un profil HAProxy**, procédez comme suit :



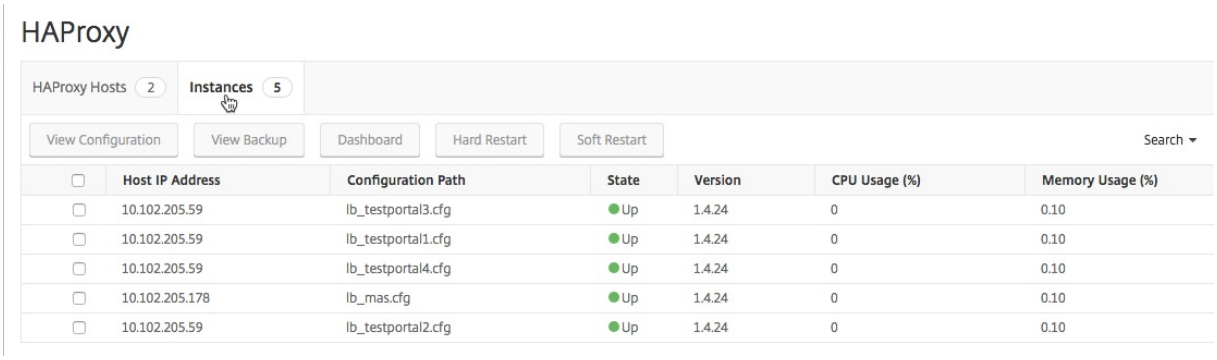
i. Dans le champ **Nom du profil**, entrez le nom du profil.

ii. Dans les champs **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'utilisateur de l'hôte.

iii. Cliquez sur **Créer**.

2. Dans le menu **Site**, sélectionnez un site HaProxy. Pour créer et ajouter un nouveau site au menu, cliquez sur **Ajouter**.
3. Dans le menu **Agent**, sélectionnez un agent.
4. Dans les champs Balises, saisissez les valeurs de manière appropriée.
5. Cliquez sur **OK**.

Citrix ADM détecte les instances HAProxy mises en service sur l'hôte et vous pouvez afficher toutes les instances HAProxy sous l'onglet **Instances**.



Affichage de la configuration d'une instance HaProxy

Pour afficher la configuration d'une instance HAProxy dans Citrix ADM, accédez à **Réseaux** > **Instances** > **HAProxy** et, sous l'onglet, **Instances**, sélectionnez l'instance HAProxy et cliquez sur **Afficher la configuration**.

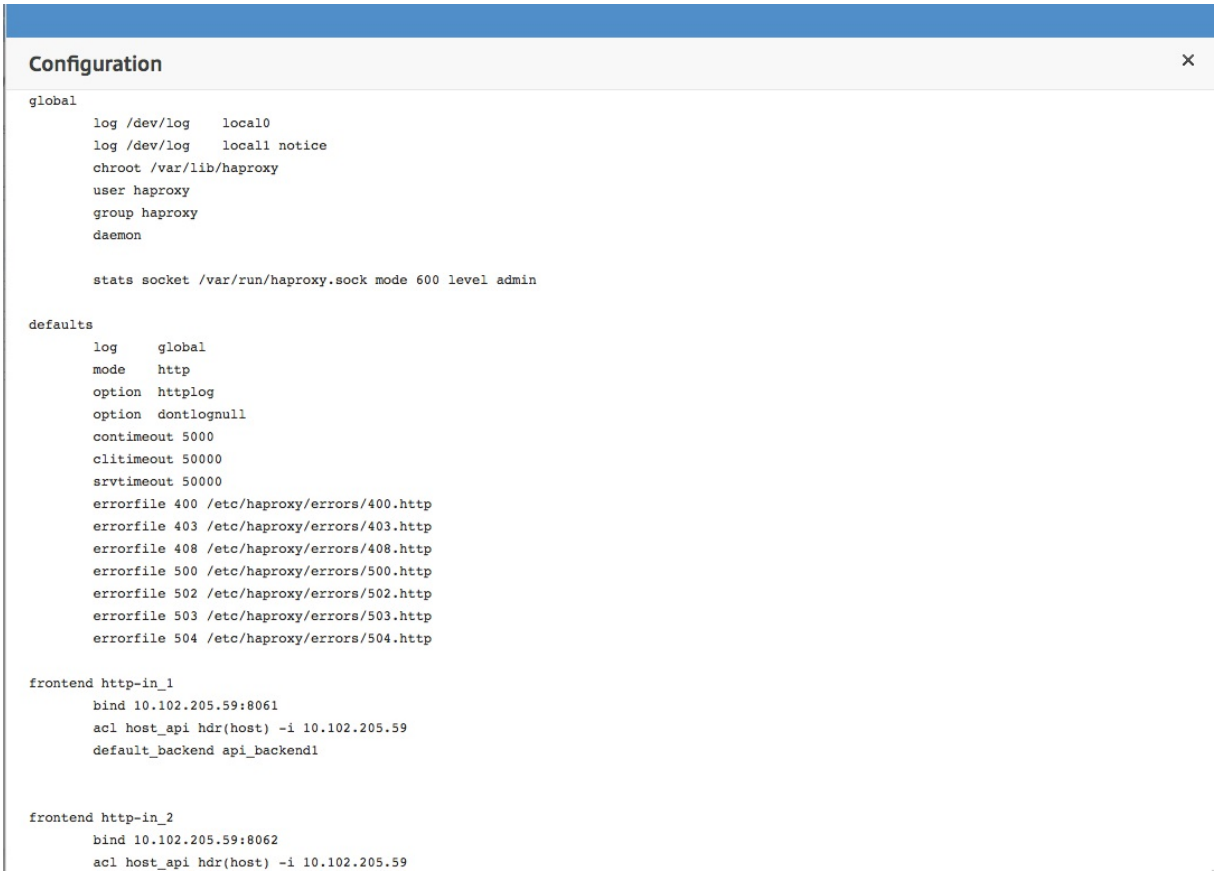


Tableau de bord de l'application HaProxy

February 1, 2024

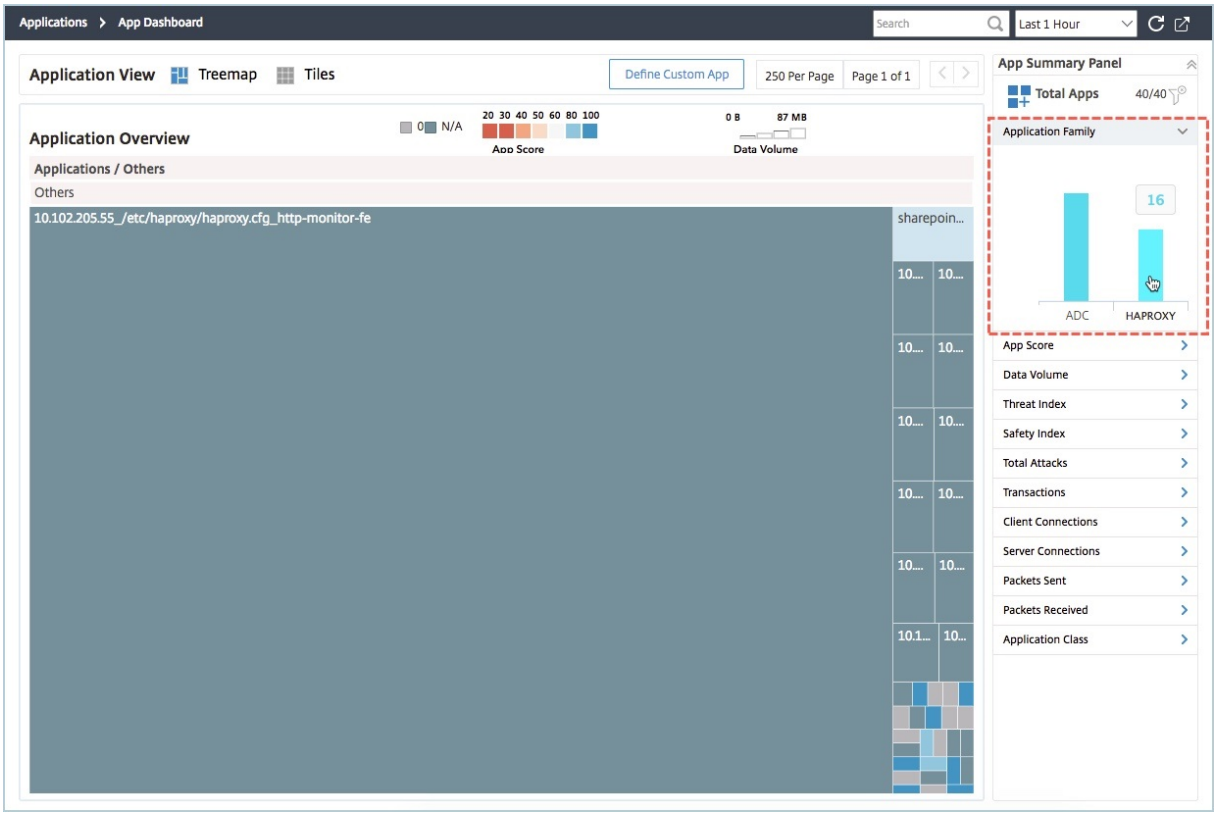
Le tableau de bord des applications fournit des statistiques en temps réel de tous les fronts HaProxy surveillés par Citrix Application Delivery Management (Citrix ADM). Il répertorie les fronts en tant qu'applications discrètes et fournit des informations sur les transactions, le débit et les sessions sur les applications.

> **Important**
>
> Assurez-vous d'activer les **statistiques** dans le fichier de configuration de l'instance HaProxy. Pour activer les **statistiques**, modifiez votre fichier de configuration HaProxy et, après la section

> des valeurs par défaut, ajoutez une entrée similaire à celle de l'exemple suivant :

```
    listen stats :9000  # Listen on localhost:9000
    mode http
    stats enable  # Enable stats page
    stats hide-version  # Hide HAProxy version
    stats realm Haproxy\ Statistics  # Title text for popup window
    stats uri /haproxy_stats  # Stats URI
    stats auth Username:Password  # Authentication credentials
<!--NeedCopy-->
```

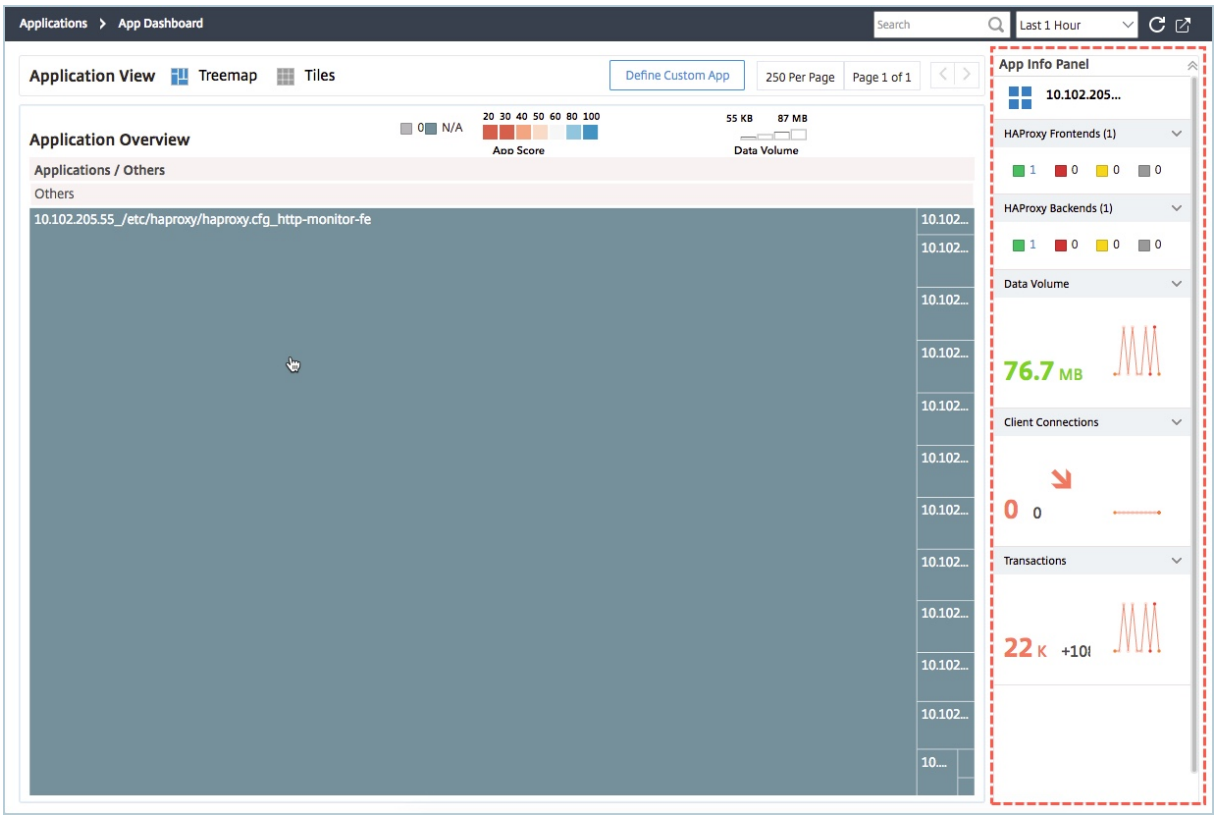
Pour accéder à l'application HAProxy sur le tableau de bord des applications dans Citrix ADM, après avoir ajouté les instances HAProxy à Citrix ADM, accédez à **Applications** > **Tableau de bord**. Vous pouvez filtrer le tableau de bord pour afficher uniquement l'application HAProxy. Pour filtrer le tableau de bord, sélectionnez **HAPROXY** affiché sous la section **Famille d'applications** dans le panneau Informations récapitulatives de l'application.



Afficher les mesures clés de l'application HaProxy

Le panneau **Infos sur l'application** est au premier niveau lorsque vous effectuez une exploration vers le bas sur une application HaProxy. Il affiche les métriques et les composants clés de l'application, ainsi que son état. Par exemple, pour toute application HaProxy sélectionnée, le panneau **Infos sur l'application** affiche le nombre total de fronts HaProxy, le nombre total de backend HaProxy, le volume

de données, la tendance des connexions client et les transactions. Pour afficher les mesures clés de l'application HaProxy, cliquez sur la vignette de l'application **HaProxy** dans le tableau de bord de l'application. Le panneau **Informations sur l'application** remplace ensuite le panneau **Résumé de l'application** .

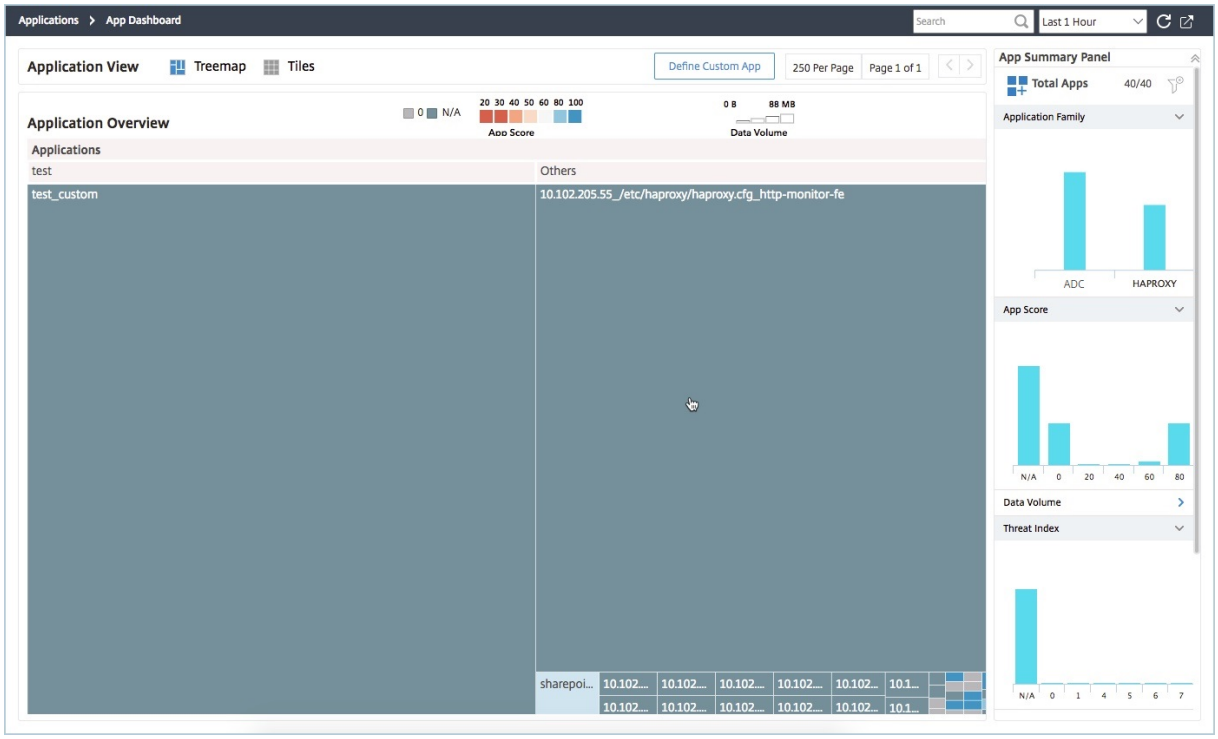


Voir les performances en temps réel de l'application HaProxy

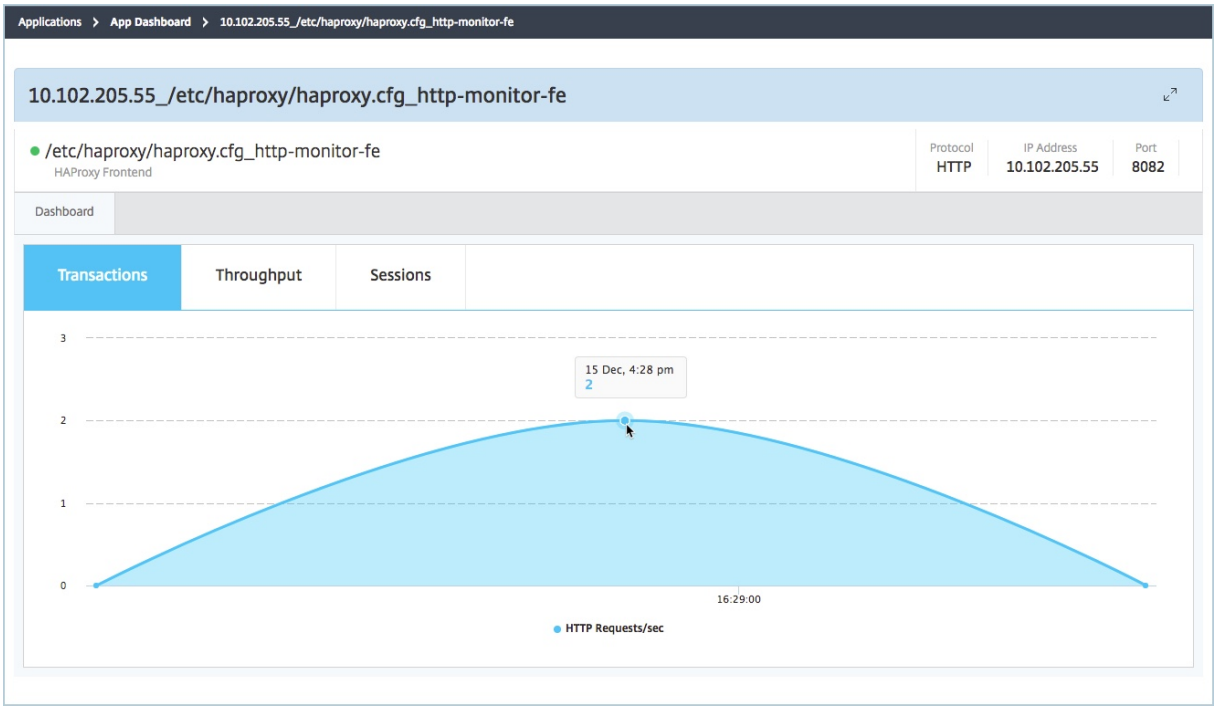
Citrix ADM vous permet de visualiser les performances en temps réel de vos applications HaProxy. Il fournit les détails suivants en temps réel de l'application HaProxy sélectionnée :

- **Transactions.** Transactions effectuées par l'application.
- **Débit.** Débit de l'application.
- **Sessions.** Nombre de sessions établies par la demande.

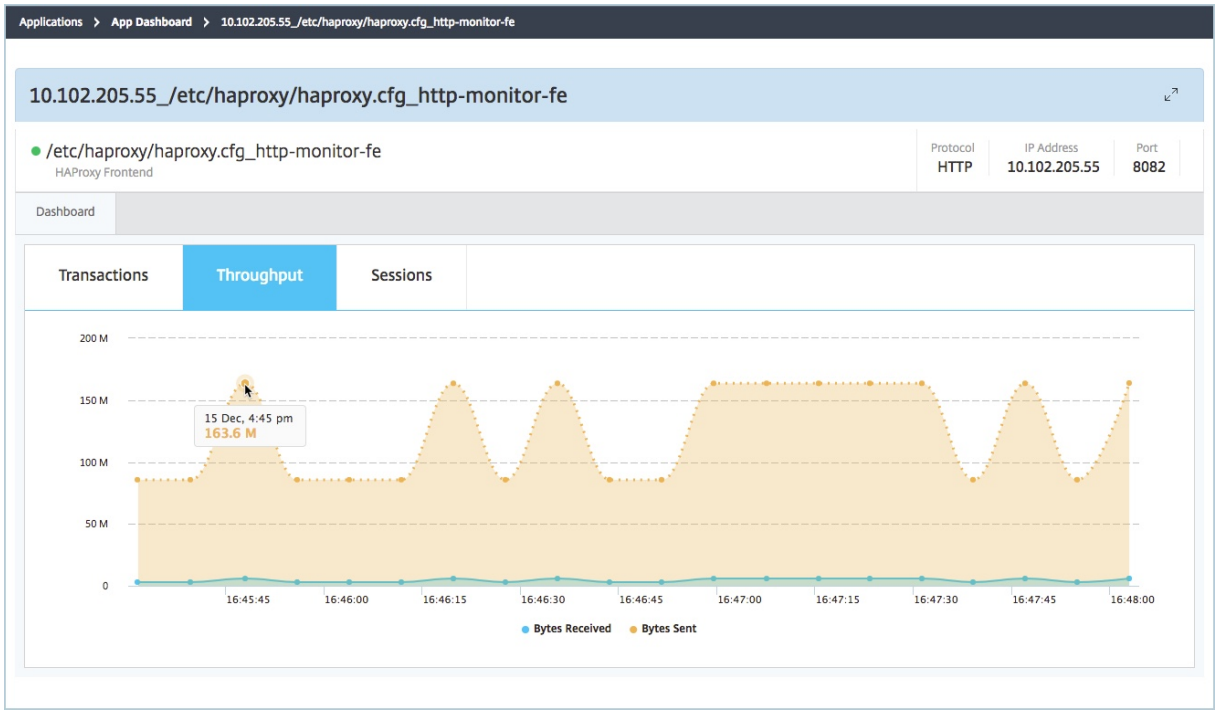
Pour afficher les performances en temps réel de votre application HAProxy, dans le Tableau de **bord des applications**, double-cliquez sur la vignette de l'application HAProxy.



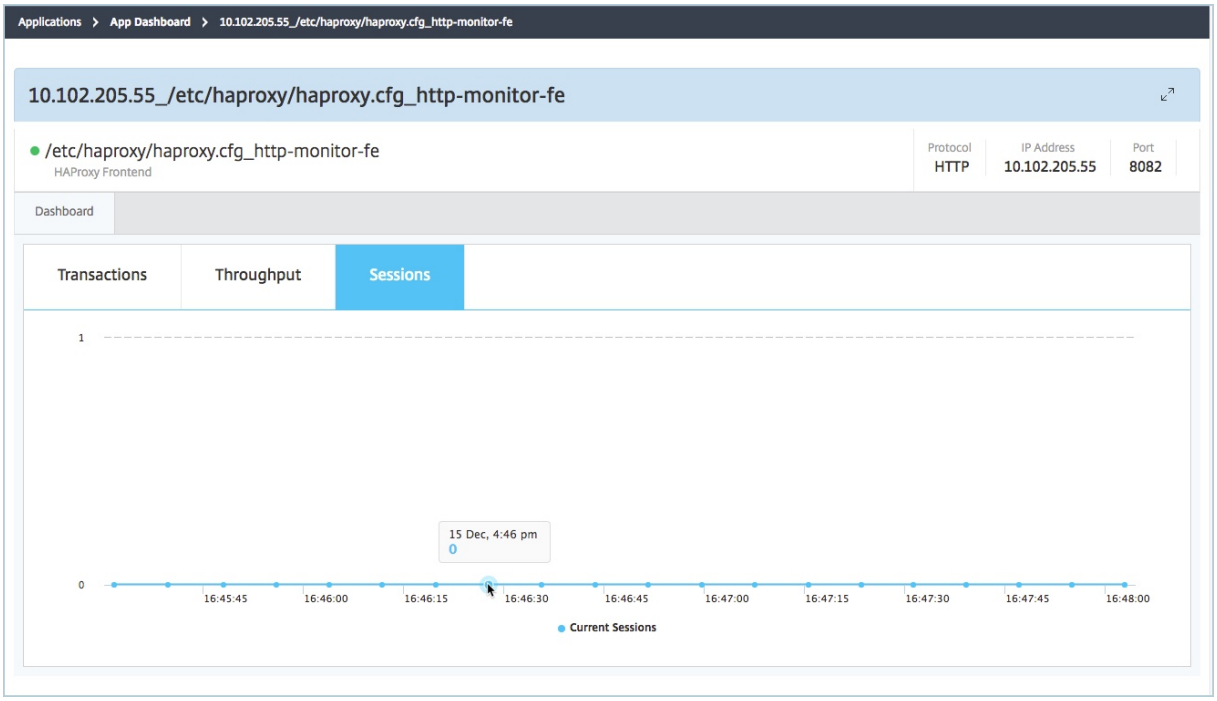
Par défaut, l'onglet **Transactions** est sélectionné et les transactions en temps réel effectuées par l'application sont affichées.



Pour afficher le débit en temps réel de l'application, cliquez sur l'onglet **Débit**.



Vous pouvez cliquer sur l'onglet **Sessions** pour afficher en temps réel le nombre de sessions établies par l'application.

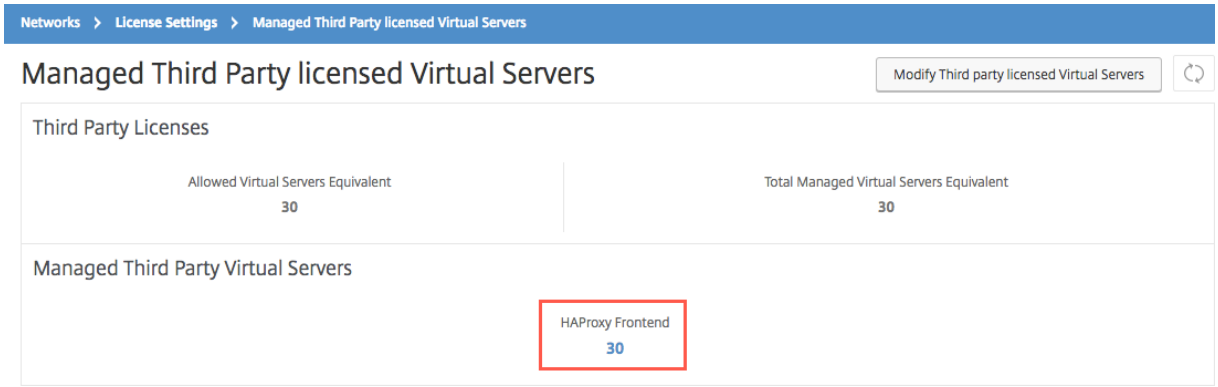


Licences tierces

February 1, 2024

Après avoir ajouté les hôtes à Citrix Application Delivery Management (Citrix ADM), Citrix ADM découvre automatiquement les instances HaProxy mises en service sur les hôtes et les ajoute à Citrix ADM Inventory. Il découvre également tous les fronts, backends et serveurs configurés sur les instances HaProxy et considère les fronts comme des applications découvertes.

Vous pouvez gérer et surveiller toutes les applications découvertes, mais par défaut, le tableau de bord des applications HaProxy affiche les statistiques des applications pour 30 applications découvertes. Pour plus d'informations sur le tableau de bord des applications HaProxy, consultez Tableau de bord des applications HaProxy. Si vous souhaitez afficher les statistiques d'application de plus de 30 applications découvertes, vous devez acheter une licence distincte.



Les licences pour plus de fronts sont disponibles dans des packs de serveurs virtuels de 100. Vous pouvez obtenir une licence valide et l'installer à l'aide de l'interface graphique Citrix ADM.

Installer les licences tierces

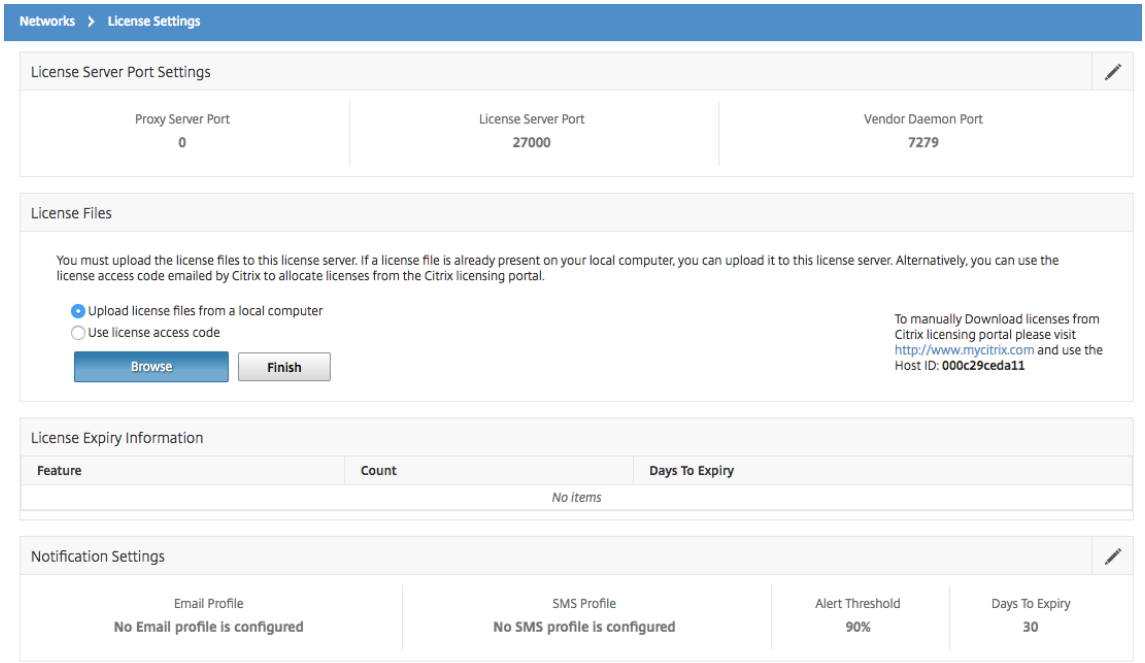
Vous pouvez installer une licence sur Citrix ADM pour afficher les statistiques d'application de plus de 30 applications découvertes.

Pour installer une licence :

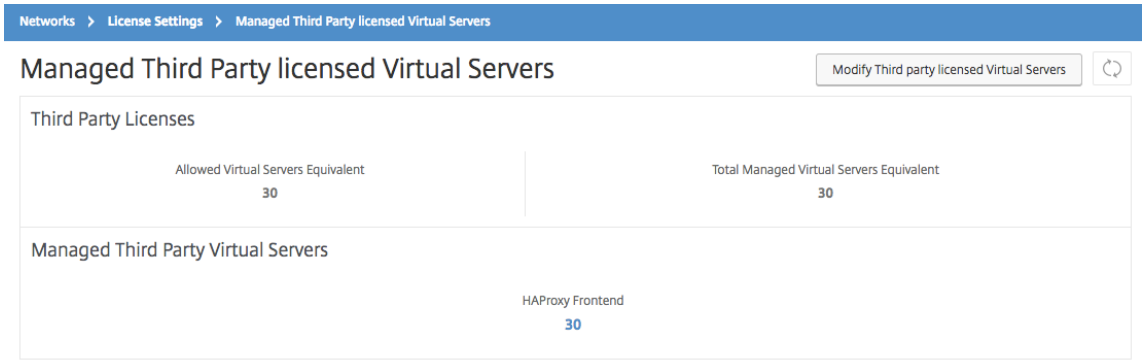
1. Accédez à **Réseaux** > **Licences**.
2. Dans la section **Fichiers de licence**, sélectionnez l'une des options suivantes :
   - **Téléchargez les fichiers de licence depuis un ordinateur local.** Si une licence est déjà présente sur votre ordinateur local, cliquez sur Parcourir et sélectionnez le fichier de licence (.lic) que vous souhaitez utiliser pour allouer vos licences. Cliquez sur **Terminer**.

- **Utiliser le code d'activation de licence** - Citrix envoie par e-mail la clé de licence de la licence que vous avez achetée. Entrez la clé de licence dans la zone de texte, puis cliquez sur **Obtenir des licences**.

> **Remarque**
>
> Si vous sélectionnez cette option, Citrix ADM doit être connecté à Internet ou un serveur proxy doit être disponible.



Vous pouvez vérifier les licences installées sur votre Citrix ADM en accédant à **Réseaux** > **Licences > Licencestierces**.



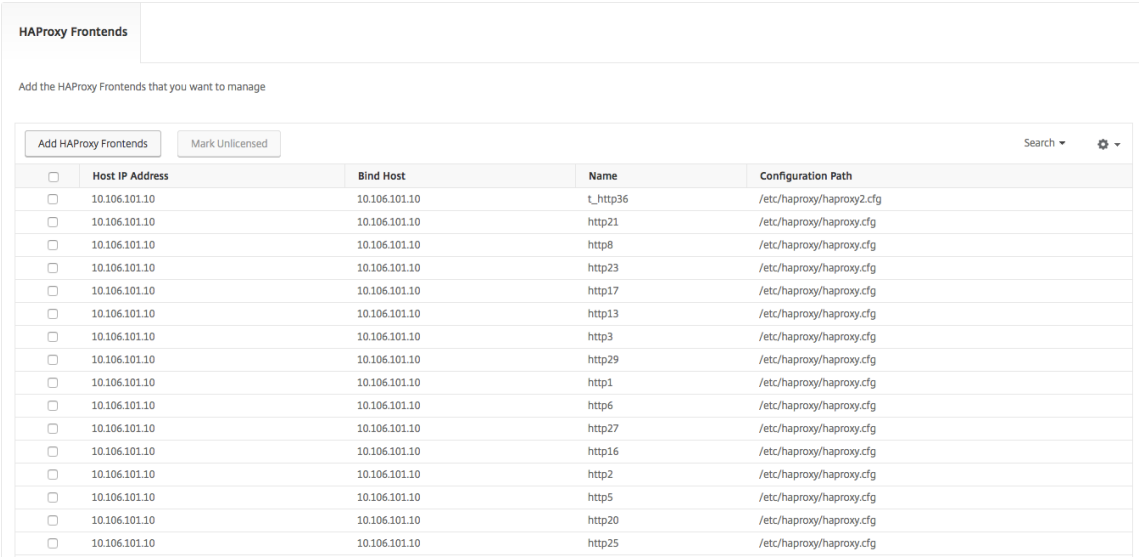
Gérer les licences tierces

Citrix ADM sélectionne de manière aléatoire les applications découvertes dans les instances HaProxy et les octroie automatiquement des licences. Si vous souhaitez modifier les applications découvertes

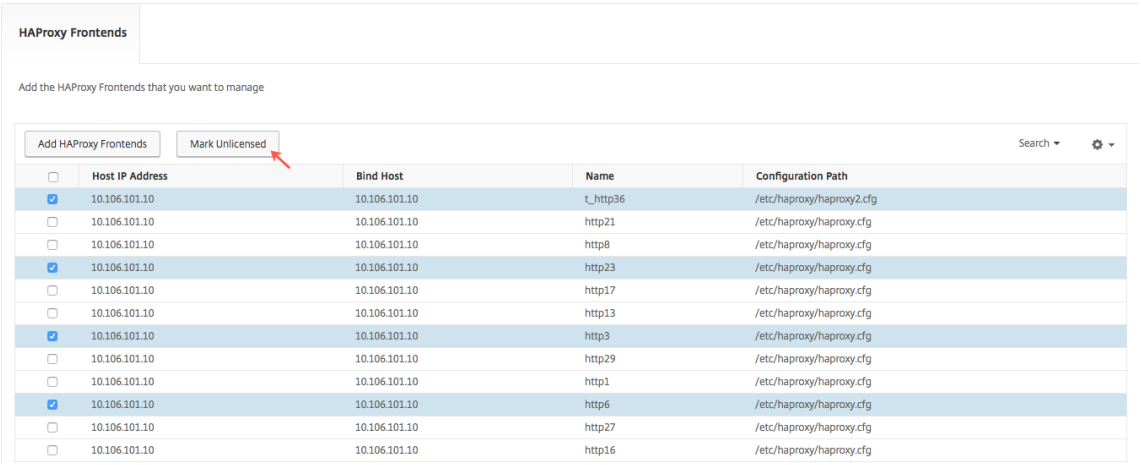
sélectionnées, vous devez annuler manuellement la licence des applications découvertes sous licence, puis allouer les licences aux applications découvertes que vous souhaitez mettre sous licence.

Pour gérer les licences tierces :

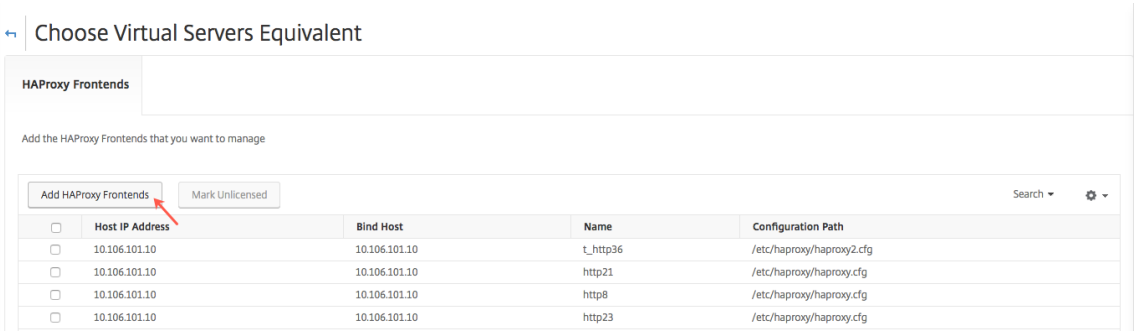
1. Accédez à **Réseaux** > **Licences > Licencestierces**et cliquez sur**Modifier les serveurs virtuels sous licence tierce partie**. Le tableau de bord affiche les fronts gérés.



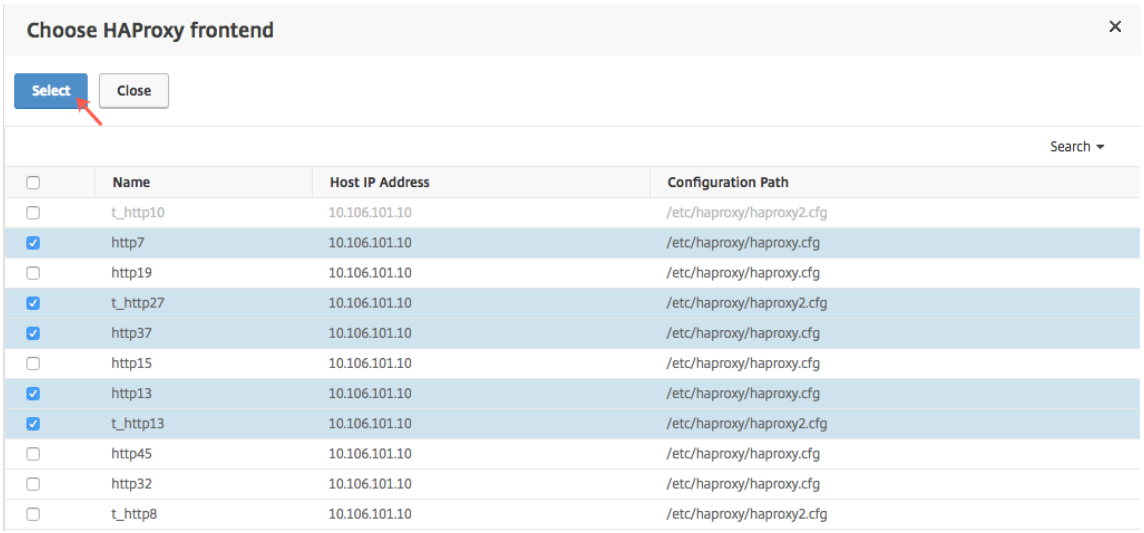
2. Sélectionnez les fronts dans la liste, **Marquer sans licence**, puis cliquez sur **Terminer** pour libérer les licences.



3. Après avoir libéré les licences, ou si vous avez déjà des licences disponibles, cliquez sur **Ajouter des frontends HaProxy**.



4. Dans la boîte de dialogue **Choose HaProxy Frontend**, sélectionnez les fronts sans licence dans la liste et cliquez sur **Sélectionner**.



5. Cliquez sur **Terminer maintenant**.

Contrôle d'accès basé sur les rôles pour les instances HaProxy

February 1, 2024

Citrix Application Delivery Management (Citrix ADM) utilise le contrôle d'accès basé sur les rôles (RBAC) fin pour contrôler l'accès aux objets de configuration. Par exemple, vous pouvez créer des utilisateurs et leur donner accès à des instances particulières de HaProxy, et vous pouvez spécifier une autorisation d'affichage/lecture seule pour le tableau de bord de l'application HaProxy. Pour plus d'informations, consultez Contrôle d'accès basé sur les rôles dans Citrix ADM.

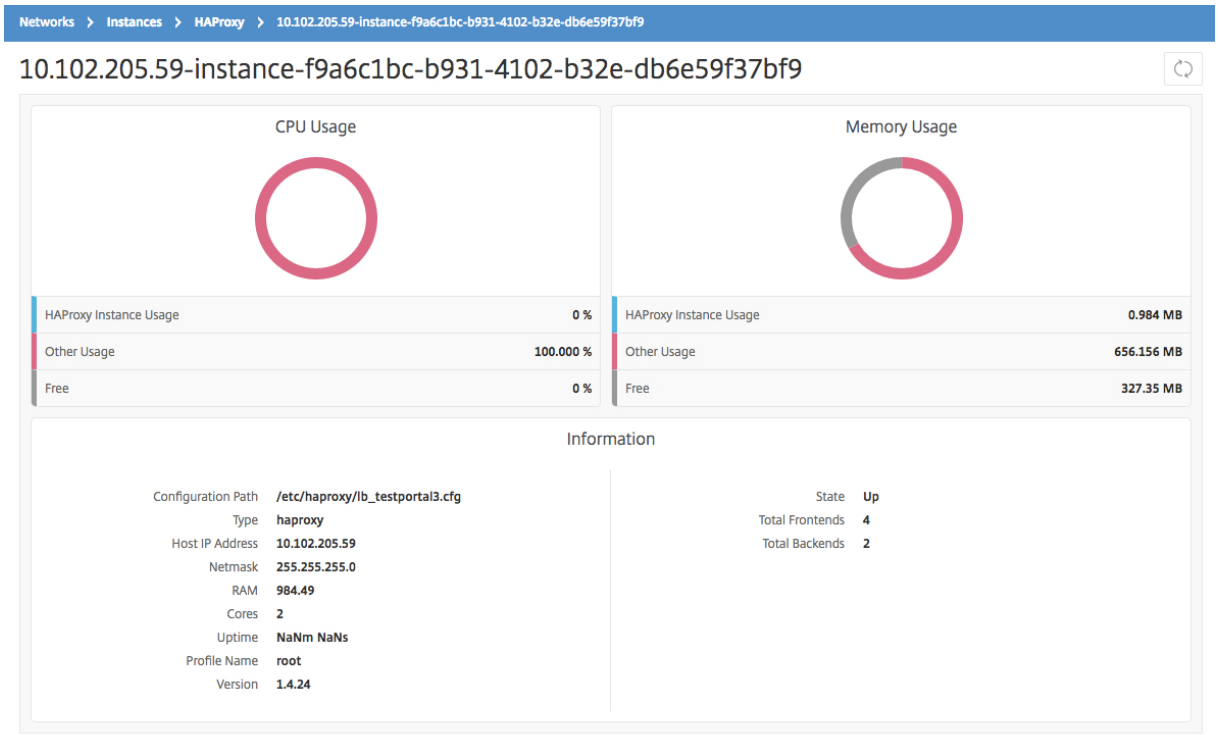
Surveiller les instances HaProxy

February 1, 2024

Le tableau de bord HAProxy dans Citrix Application Delivery Management (Citrix ADM) affiche des graphiques qui vous aident à suivre l'utilisation du processeur et de la mémoire d'une instance HAProxy. Le tableau de bord affiche également des graphiques indiquant les éléments suivants :

- Pourcentage de CPU utilisé par l'instance HAProxy sur l'hôte.
- Pourcentage de CPU utilisé par d'autres entités sur l'hôte.
- Pourcentage de CPU restant sur l'hôte.
- Pourcentage de mémoire utilisée par l'instance HAProxy sur l'hôte.
- Pourcentage de mémoire utilisée par d'autres entités sur l'hôte.
- Pourcentage de mémoire restante sur l'hôte.

Pour surveiller une instance HAProxy dans Citrix ADM, accédez à l'onglet **Réseaux** > **Instances** > **HAProxy** > **Instances**, sélectionnez l'instance HAProxy, puis cliquez sur **Tableau de bord**.



Afficher les détails des fronts configurés sur les instances HaProxy

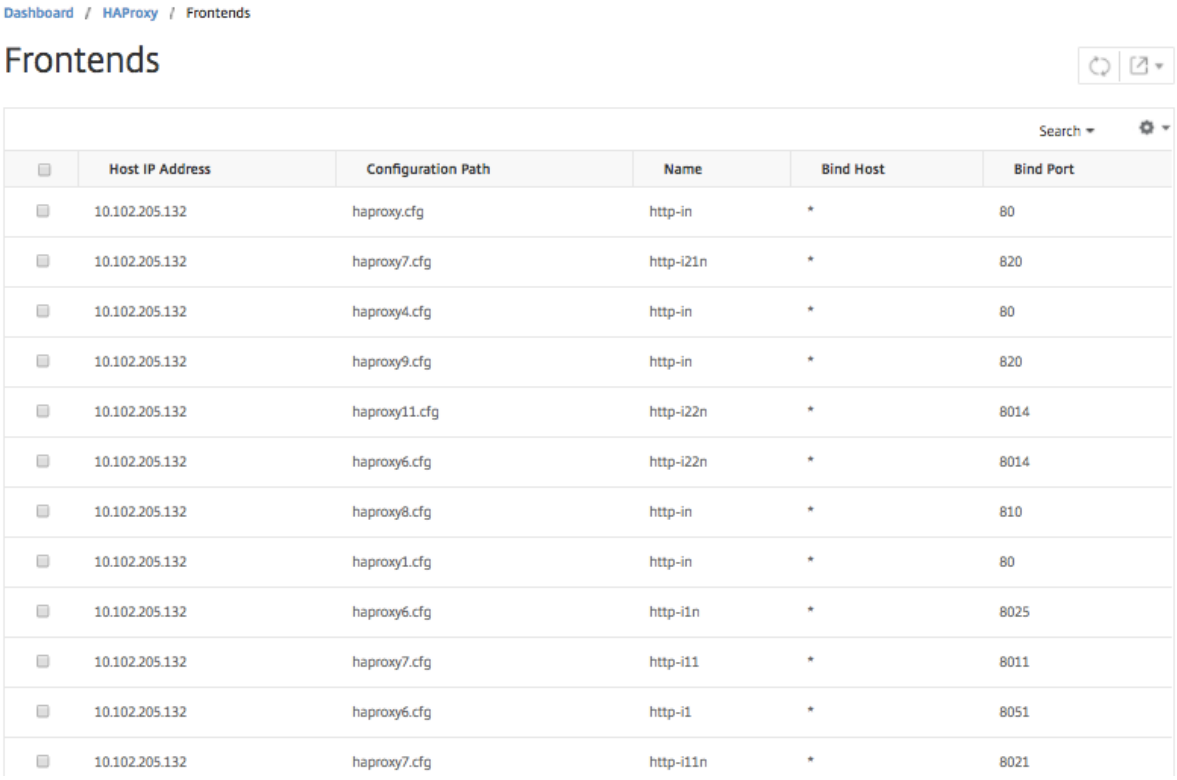
February 1, 2024

Citrix Application Delivery Management (Citrix ADM) signale les détails suivants sur le frontal configuré sur une instance HAProxy :

- **Adresse IP de l'hôte**. Adresse IP de l'hôte
- **Chemin de configuration**.Chemin de configuration absolu de l'instance HaProxy sur l'hôte.
- **Nom**. Nom de l'extrémité frontale qui gère le trafic entrant.
- **Lier l'hôte**. Adresse IP à laquelle le front end est lié.
- **Port de liaison**. Port auquel le front end est lié.

Pour afficher le frontal configuré sur les instances HaProxy :

Dans Citrix ADM, accédez à **Réseaux > Fonctions réseau > HAProxy > Frontends**.



Host IP Address	Configuration Path	Name	Bind Host	Bind Port
10.102.205.132	haproxy.cfg	http-in	*	80
10.102.205.132	haproxy7.cfg	http-i21n	*	820
10.102.205.132	haproxy4.cfg	http-in	*	80
10.102.205.132	haproxy9.cfg	http-in	*	820
10.102.205.132	haproxy11.cfg	http-i22n	*	8014
10.102.205.132	haproxy6.cfg	http-i22n	*	8014
10.102.205.132	haproxy8.cfg	http-in	*	810
10.102.205.132	haproxy1.cfg	http-in	*	80
10.102.205.132	haproxy6.cfg	http-i1n	*	8025
10.102.205.132	haproxy7.cfg	http-i11	*	8011
10.102.205.132	haproxy6.cfg	http-i1	*	8051
10.102.205.132	haproxy7.cfg	http-i11n	*	8021

Afficher les détails des back-end configurés sur les instances HaProxy

February 1, 2024

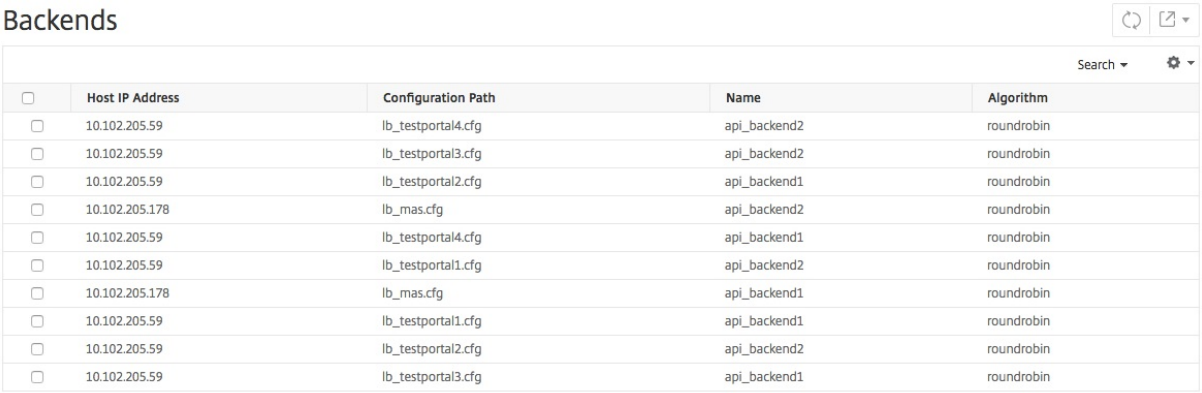
Citrix Application Delivery Management (Citrix ADM) signale les détails suivants d'une application back-end configurée sur une instance HAProxy :

- **Adresse IP de l'hôte**. Adresse IP de l'hôte.
- **Chemin de configuration**. Chemin d'instance HAProxy sur l'hôte.

- **Nom**. Nom du back-end vers lequel le trafic est transféré.
- **Algorithme**. Algorithme d'équilibrage de charge utilisé pour équilibrer le trafic.

Pour afficher le backend configuré sur les instances HaProxy :

Dans Citrix ADM, accédez à **Réseaux** > **Fonctions réseau** > **HAProxy** > **Backends**.



Afficher les détails des serveurs configurés sur les instances HaProxy

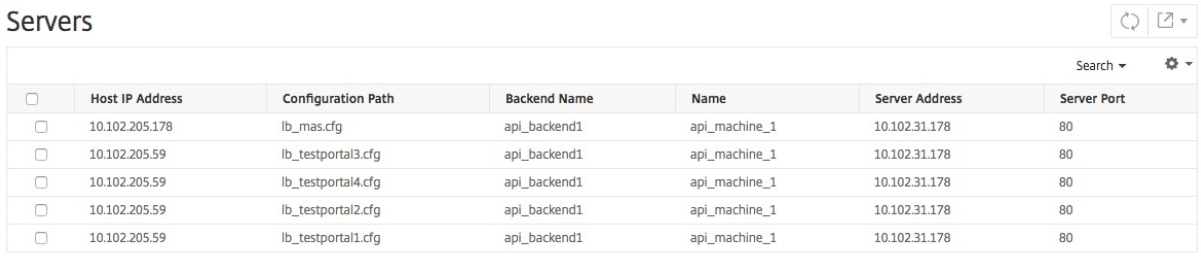
February 1, 2024

Citrix Application Delivery Management (Citrix ADM) signale les détails suivants des serveurs configurés sur une instance HAProxy :

- **Adresse IP de l'hôte**. Nom de l'hôte.
- **Chemin de configuration**.Chemin absolu du fichier de configuration d'instance HaProxy sur l'hôte.
- **Nom du backend**. Nom du backend dans la configuration HaProxy.
- **Nom**. Nom du serveur dans la configuration HAProxy.
- **Adresse du serveur**. Adresse IP du serveur.
- **Port serveur**. Port utilisé par le serveur.

Pour afficher les serveurs configurés sur les instances HaProxy :

Dans Citrix ADM, accédez à **Réseaux** > **Fonctions réseau** > **HAProxy** > **Serveurs**.

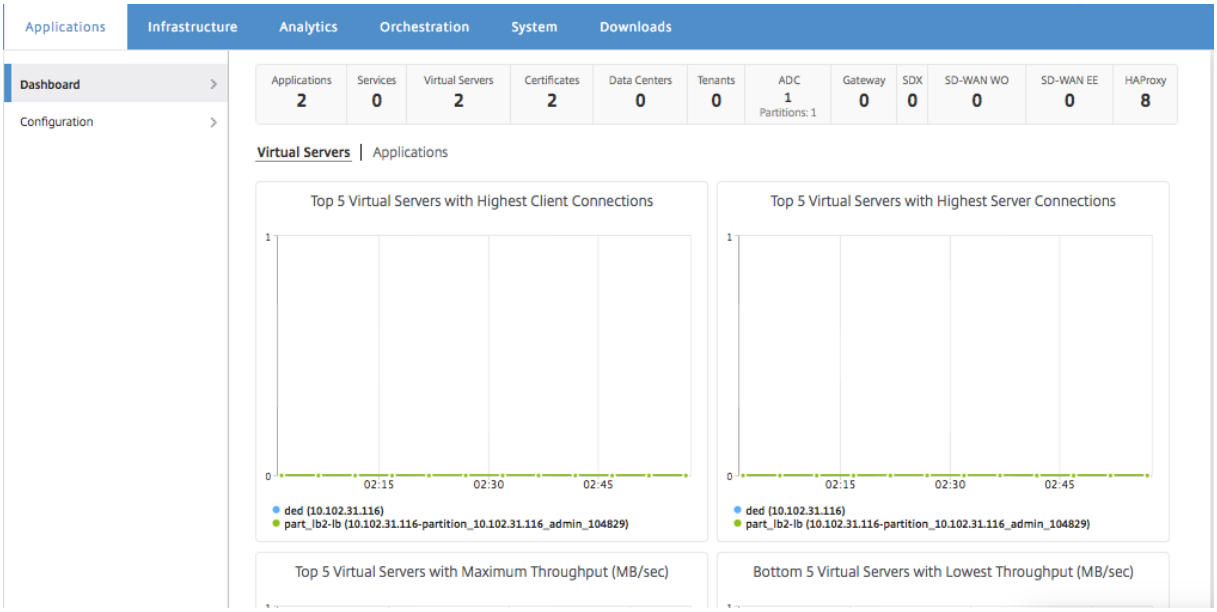


Afficher les instances HaProxy avec le plus grand nombre de fronts ou de serveurs

February 1, 2024

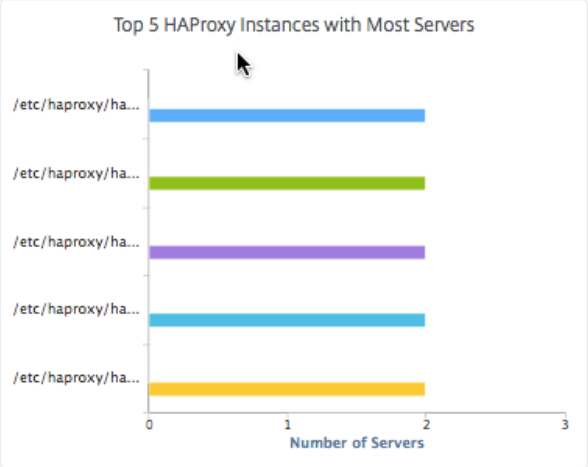
Dans le tableau de **bord**des applications, Citrix Application Delivery Management (Citrix ADM) affiche le nombre d'instances HaProxy qu'il découvre et répertorie les cinq premières instances HaProxy configurées avec le plus grand nombre de serveurs ou de fronts.

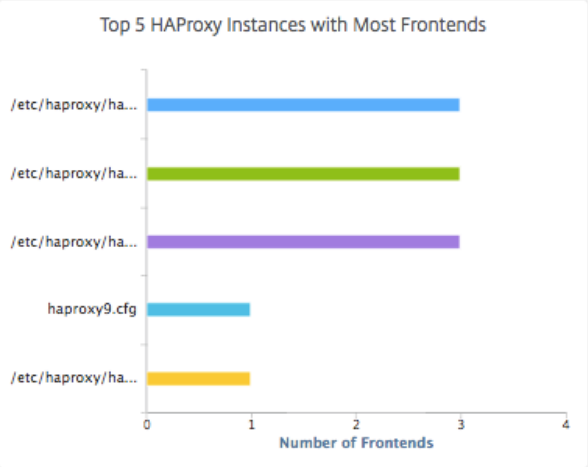
Pour afficher le tableau de **bord des applications**, dans Citrix ADM, accédez à **Applications** > **Tableau de bord**.



Le nombre d'instances HAProxy découvertes par Citrix ADM est affiché dans la ligne supérieure :

Pour afficher la liste des cinq premières instances HProxy configurées avec le plus grand nombre de fronts ou le plus grand nombre de serveurs, faites défiler le tableau de bord vers le bas :





Redémarrer une instance HAProxy

February 1, 2024

Pour redémarrer une instance HaProxy à partir de l'interface graphique Citrix Application Delivery Management (Citrix ADM), vous pouvez sélectionner un redémarrage dur ou un redémarrage progressif.

Redémarrage dur

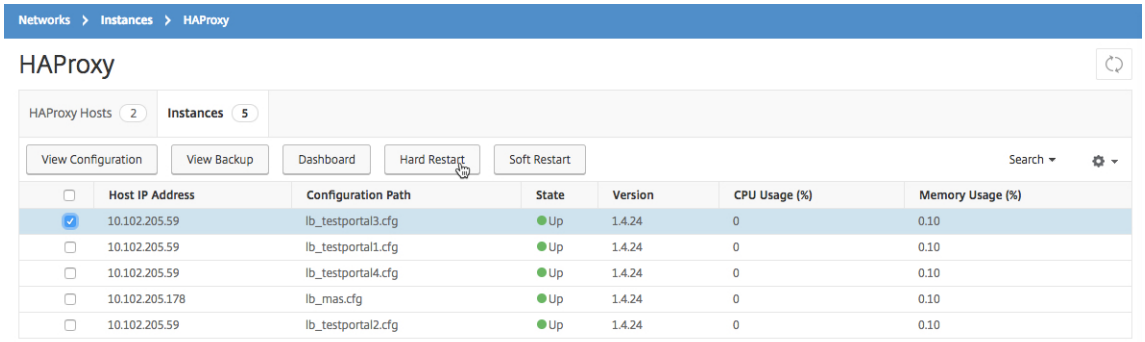
Le redémarrage dur interrompt le processus HAProxy sur l'instance et ferme toutes les connexions établies. Après le redémarrage, un nouveau processus HProxy est créé et les nouvelles connexions suivantes sont traitées par le nouveau processus HaProxy.

Redémarrage progressif

Le redémarrage progressif délie le processus HAProxy du port d'écoute, mais le processus HAProxy continue de traiter les connexions existantes jusqu'à leur fermeture. Un nouveau processus HaProxy est créé pour traiter les nouvelles connexions.

Pour redémarrer une instance HaProxy, procédez comme suit :

1. Accédez à **Réseaux** > **Instances** > **HAProxy** et cliquez sur l'onglet **Instance**.
2. Sous l'onglet **Instance**, sélectionnez l'instance HAProxy que vous souhaitez redémarrer.
3. Cliquez sur **Redémarrer dur** pour redémarrer l'instance HAProxy ou cliquez sur **Redémarrer logiciel** pour redémarrer l'instance HAProxy.



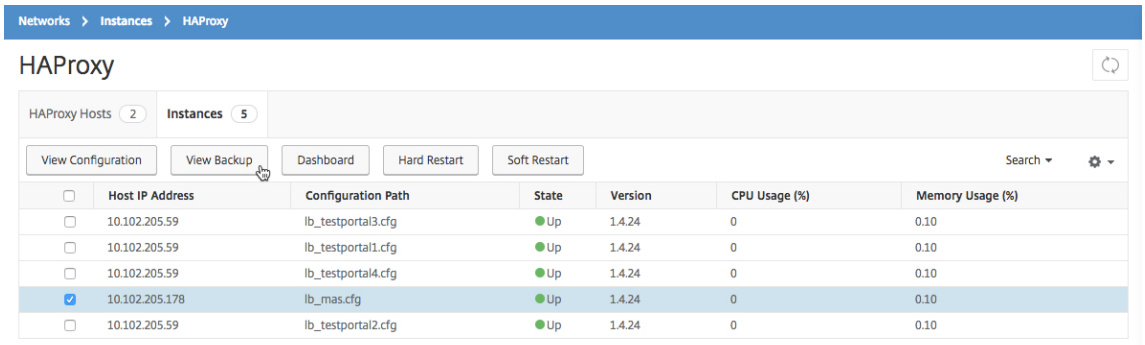
Sauvegarder et restaurer une instance HaProxy

February 1, 2024

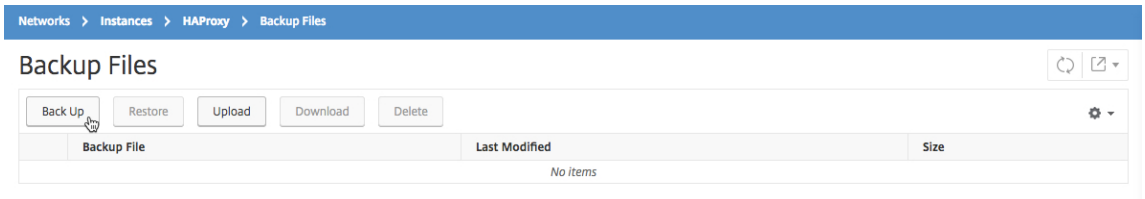
Vous pouvez sauvegarder l'état actuel d'une instance HAProxy dans un fichier de configuration HAProxy. Si l'instance devient instable, vous pouvez utiliser le fichier sauvegardé pour restaurer l'instance à son état stable.

Pour sauvegarder une instance HaProxy à l'aide de Citrix ADM :

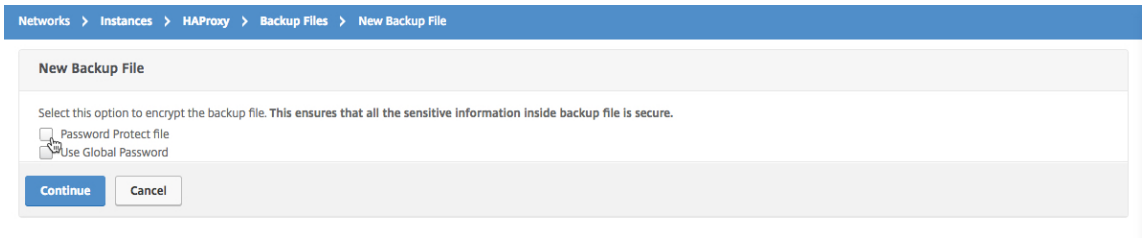
1. Dans Citrix Application Delivery Management (Citrix ADM), accédez à **Réseaux > Instances > HAProxy**.
2. Dans la page **HaProxy**, cliquez sur l'onglet **Instances**.
3. Sélectionnez l'instance HAProxy à sauvegarder, puis cliquez sur **Afficher la sauvegarde**.



4. Sur la page **Fichiers de sauvegarde** , cliquez **sur Sauvegarder.**



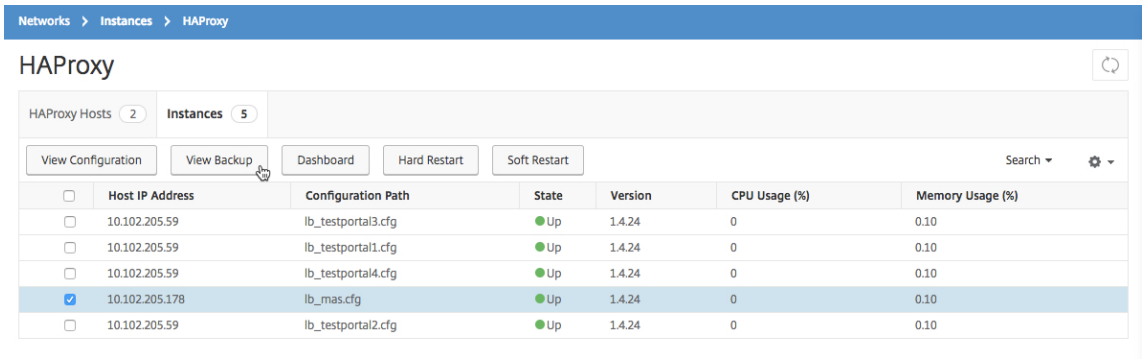
5. Vous pouvez choisir de chiffrer votre fichier de sauvegarde pour plus de sécurité.



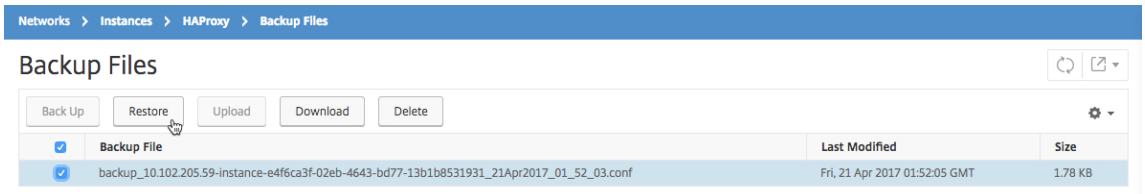
6. Cliquez sur **Continuer**.

Pour restaurer une instance à l'aide de Citrix ADM :

1. Accédez à **Réseaux** > **Instances** > **HAProxy**.
2. Sur la page **HaProxy**, cliquez sur l'onglet **Instances**.
3. Sélectionnez l'instance à restaurer, puis cliquez sur **Afficher la sauvegarde**.



4. Dans la page **Fichiers de sauvegarde**, sélectionnez le fichier de sauvegarde à restaurer, puis cliquez sur **Restaurer**.



> **Remarque**
>
> Lorsque vous restaurez une instance, le logiciel Citrix ADM redémarre l'instance HAProxy.

Modifier le fichier de configuration HaProxy

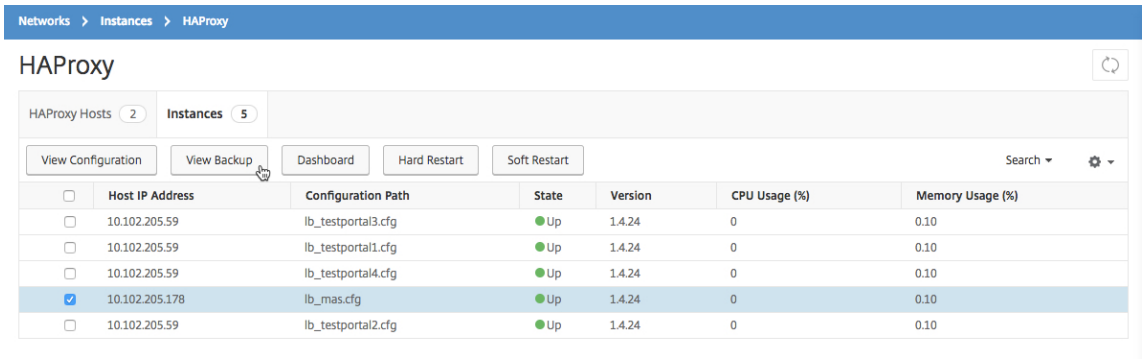
February 1, 2024

Vous pouvez mettre à jour les paramètres frontal, backend, serveur et autres paramètres dans le fichier de configuration HaProxy existant. Pour modifier le fichier de configuration HaProxy :

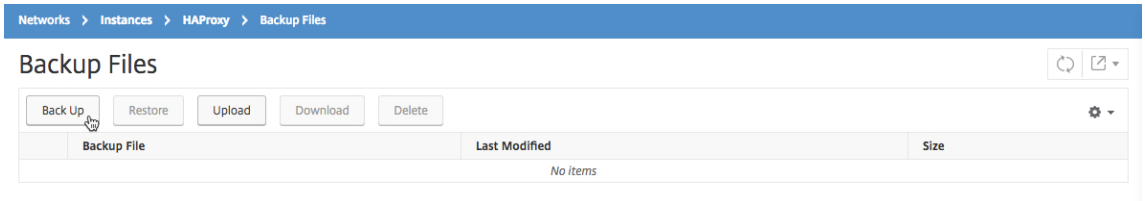
- Sauvegardez le fichier de configuration HaProxy.
- Téléchargez le fichier de configuration de sauvegarde HaProxy et modifiez-le hors connexion.
- Télécharger le fichier de configuration HaProxy mis à jour dans Citrix Application Delivery Management (Citrix ADM)
- Restaurez l'instance HaProxy avec le fichier de sauvegarde mis à jour.

Pour modifier le fichier de configuration HAProxy à l'aide de Citrix ADM :

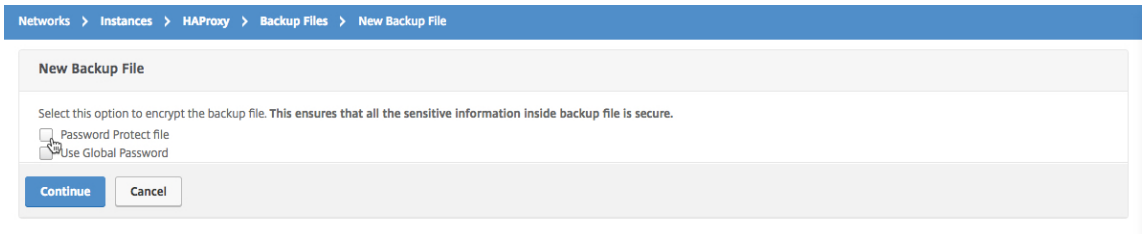
1. Dans Citrix ADM, accédez à **Réseaux** > **Instances** > **HAProxy**.
2. Sur la page **HaProxy**, cliquez sur l'onglet **Instances**.
3. Sélectionnez l'instance HAProxy à sauvegarder, puis cliquez sur **Afficher la sauvegarde**.



4. Sur la page **Fichiers de sauvegarde**, cliquez sur **Sauvegarder**.

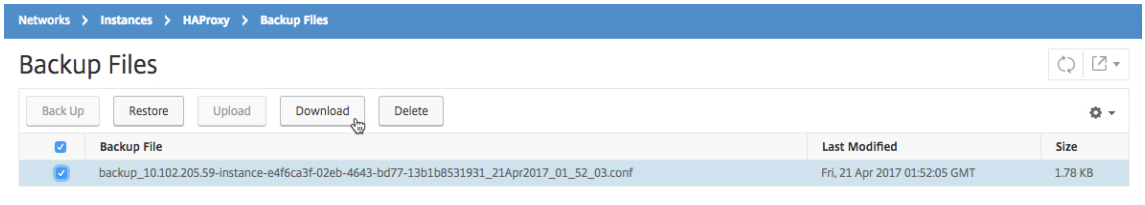


5. Cliquez sur **Continuer**.

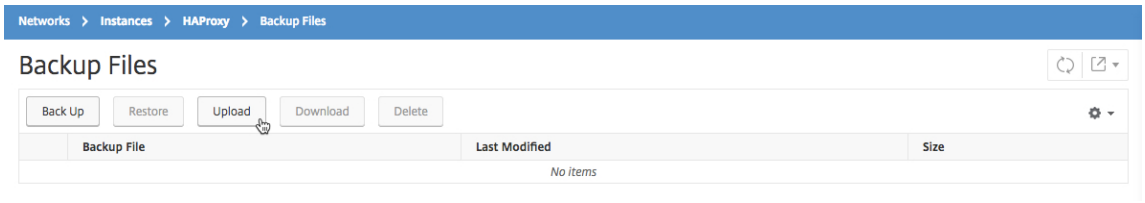


> **Remarque**
>
> Ne chiffrez pas le fichier de sauvegarde.

6. Sur la page **Fichiers de sauvegarde**, sélectionnez le fichier de sauvegarde et cliquez sur **Télécharger**.



7. À l'aide d'un éditeur de texte, modifiez le fichier de configuration HAProxy.
8. Dans la page **Fichiers de sauvegarde**, cliquez sur **Télécharger** pour parcourir et sélectionner le fichier de configuration HaProxy mis à jour.



   Une fois le fichier de configuration HaProxy mis à jour téléchargé, il est répertorié sur la page **Fichiers de sauvegarde**.
9. Sélectionnez le fichier de configuration HaProxy mis à jour et cliquez sur **Restaurer**.

Gérer les paramètres système

February 1, 2024

Le tableau suivant décrit la liste des options disponibles sous **Système** > **Administration** :

Configurations réseau

Configurations réseau	Options	Description
Adresse IP, deuxième carte réseau, nom d'hôte et serveur proxy	Adresse IP	Affiche les détails de l'adresse IP de configuration réseau Citrix ADM qui sont utilisés pour déployer Citrix ADM

Configurations réseau	Options	Description
	Deuxième carte réseau	Permet de configurer une deuxième carte réseau pour isoler l'accès à la gestion Citrix ADM. Pour plus d'informations, consultez Configurer une double carte réseau pour accéder à Citrix ADM
	Nom d'hôte	Permet d'attribuer un nom d'hôte à Citrix ADM. Pour plus d'informations, consultez Attribuer un nom d'hôte à un serveur Citrix ADM
	Serveur proxy	Permet de configurer ADM en tant que serveur proxy. Pour plus d'informations, consultez Citrix ADM en tant que serveur proxy d'API
Itinéraires statiques		Vous permet de configurer des itinéraires statiques pour établir une connexion entre les instances Citrix ADM et Citrix ADC VPX
Serveurs NTP		Garantit que l'horloge Citrix ADM possède les mêmes paramètres de date et d'heure que les autres serveurs du réseau. Pour plus d'informations, consultez Configurer le serveur NTP
Informations sur les ports ADM		Permet de comprendre quel port doit être ouvert pour la communication entre les instances ADM et ADC ou SD-WAN. Pour plus d'informations, consultez Ports pris en charge

Configurations système

Configurations système	Options	Description
Système, fuseau horaire, URL autorisées et message du jour	Paramètres de base	Permet de modifier les paramètres système tels que l'activation de la connexion `nsrecover`, l'activation du délai d'expiration de session, etc.
	Fuseau horaire	Vous permet de modifier le fuseau horaire à utiliser dans Citrix ADM. Le fuseau horaire par défaut est UTC
	Liste des URL autorisées	Permet de configurer des URL pour envoyer des demandes ininterrompues à ADM. Vous pouvez le configurer avec la valeur « none » si aucune URL à ajouter
	Message du jour	Vous permet de créer un message de bienvenue dans Citrix ADM. Vous pouvez utiliser cette fonctionnalité pour définir des messages de rappel pour vous-même ou pour l'utilisateur qui ouvre une session sur Citrix ADM. Cliquez sur **Activer le message**, saisissez le message dans la zone de message, puis cliquez sur **Enregistrer**
Afficher les empreintes digitales d'ADM		Vous permet de copier l'identifiant d'empreinte numérique unique de Citrix ADM pour commencer à utiliser Service Graph

Configurations système	Options	Description
Configurer l'identité du client		Permet de protéger les ressources réseau en autorisant uniquement les clients ou utilisateurs authentifiés à accéder à son réseau. Pour plus d'informations, consultez Gouvernance des données
Paramètres CUXIP		Si vous cochez cette case, les statistiques d'utilisation sont collectées dans le seul but d'améliorer l'interface graphique. Les données reçues ne sont utilisées que par les ingénieurs Citrix et ne sont partagées avec personne.

Maintenance du système

Maintenance du système	Description
Mettre à niveau Citrix ADM	Permet de mettre à niveau Citrix ADM via l'interface graphique. Pour plus d'informations, consultez Mettre à niveau
Redémarrer Citrix ADM	Vous permet de redémarrer Citrix ADM
Arrêter Citrix ADM	Vous permet d'arrêter Citrix ADM
Récupération d'urgence	Permet d'afficher les informations du nœud de reprise après sinistre. Pour plus d'informations, consultez Configurer la reprise après sinistre

Nettoyage des données

Nettoyage des données	Options	Description
Élagage des données du système et de l'instance	System	Permet de limiter la quantité de données de reporting stockées dans la base de données du serveur Citrix ADM. Pour plus d'informations, voir Configurer les paramètres d'nettoyer du système
	Événements d'instance	Vous permet de limiter les données de rapport sur les messages d'événements stockées dans Citrix ADM
	Syslog d'instance	Permet de limiter la quantité de données syslog stockées dans la base de données. Pour plus d'informations, voir Configurer les paramètres d'élagage de Syslog d'instance
	Rapports sur le réseau	Vous permet de limiter les données de reporting réseau stockées dans Citrix ADM

Sauvegarde

Sauvegarde	Options	Description
Configuration de la sauvegarde du système et de l'instance	System	Permet de configurer les paramètres de sauvegarde initiaux avant d'effectuer une sauvegarde système. Pour plus d'informations, voir Paramètres de sauvegarde du système

Sauvegarde	Options	Description
	Instance	Permet de configurer les paramètres sur Citrix ADM pour sauvegarder une ou plusieurs instances Citrix ADC sélectionnées. Pour plus d'informations, consultez Configurer les paramètres de sauvegarde d'instance

Notifications d'événements

Notifications d'événements	Options	Description
Configuration de la notification et du résumé des événements	Notification d'événement	Vous pouvez envoyer des notifications à des groupes d'utilisateurs sélectionnés pour plusieurs fonctions liées au système. Ces fonctions système sont organisées en catégories d'événements telles que SystemReboot, StatusPoll, SystemState, etc. Vous pouvez configurer Citrix Application Delivery Management (ADM) pour vous envoyer des notifications par e-mail, SMS ou Slack. Cela garantit que vous êtes informé de toute activité au niveau du système, telle que le dépassement de la capacité de stockage des données ou l'échec de la sauvegarde.
	Résumé de l'événement	Vous permet d'obtenir un rapport consolidé sur les événements importants liés au système et aux fonctionnalités

Paramètres SSL

Paramètres SSL	Description
Installer le certificat SSL	Vous permet d'installer un certificat SSL et un fichier de clé SSL
Afficher le certificat SSL	Vous permet de consulter les détails du certificat SSL
Configurer les paramètres SSL	Pour plus d'informations, voir Configurer les paramètres SSL
Certificats SSL	Vous permet de charger, de télécharger ou de supprimer un certificat SSL ou un fichier de clé SSL
Groupes de chiffrement	Pour plus d'informations, consultez Configurer un groupe de chiffrement

Configurer les fonctionnalités

Configurer les fonctionnalités	Description
Désactiver ou activer des fonctionnalités	Vous pouvez activer ou désactiver des fonctionnalités dans Citrix ADM. Pour plus d'informations, voir Activer ou désactiver les fonctionnalités ADM

Configurer les paramètres de sauvegarde du système

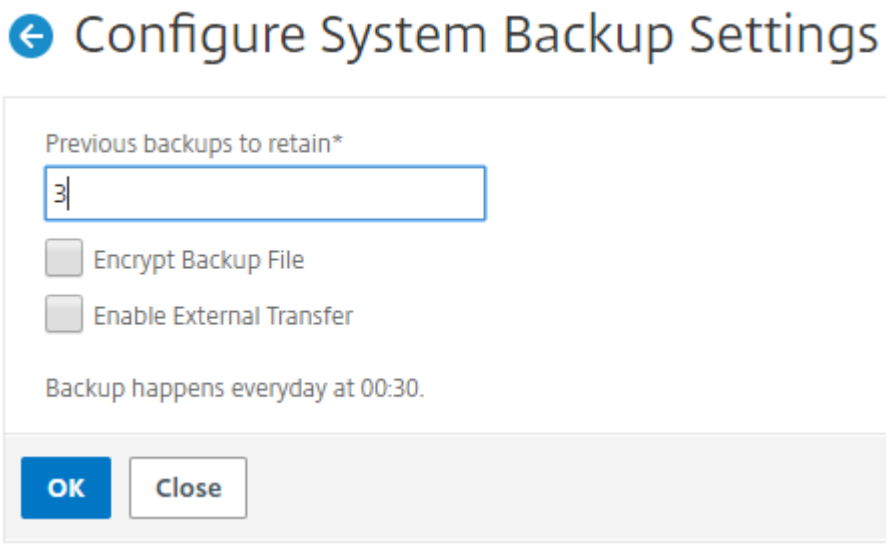
February 1, 2024

Définissez vos paramètres de sauvegarde système initiaux avant de devoir sauvegarder et restaurer le système Citrix Application Delivery Management (ADM).

1. Accédez à **Système** > **Administration système**. Sous **Paramètres de sauvegarde**, cliquez sur **Paramètres de sauvegarde système**.
2. Dans la page **Configurer les paramètres de sauvegarde du système**, spécifiez les éléments suivants :

- Nombre de sauvegardes à conserver. Vous ne pouvez conserver qu'un maximum de 10 sauvegardes.
- Chiffrez le fichier de sauvegarde.
- Activez le transfert externe. Vous pouvez transférer une copie d'une copie de votre fichier de sauvegarde vers un autre système par mesure de précaution. Lorsque vous souhaitez restaurer la configuration, vous devez d'abord télécharger le fichier sur le serveur Citrix ADM, puis effectuer l'opération de restauration. Spécifiez le serveur, le nom d'utilisateur et le mot de passe, le port, le protocole de transfert à utiliser et le chemin d'accès au répertoire. Pour en savoir plus sur le transfert externe, consultez Transférer un fichier de sauvegarde Citrix ADM vers un système externe.

3. Cliquez sur **OK**.



Configurer un serveur NTP

February 1, 2024

Vous pouvez configurer un serveur NTP (Network Time Protocol) dans Citrix Application Delivery Management (ADM) pour synchroniser son horloge avec le serveur NTP. La configuration d'un serveur NTP garantit que l'horloge Citrix ADM possède les mêmes paramètres de date et d'heure que les autres serveurs du réseau.

Pour configurer un serveur NTP sur Citrix ADM :

1. Accédez à **Système** > **Serveurs NTP**, puis cliquez sur **Ajouter**.

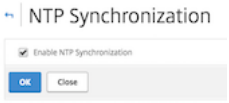
2. Dans la page **Créer un serveur NTP**, entrez les détails suivants :

   - **Nom du serveur/adresse IP** —Entrez le nom de domaine ou l'adresse IP du serveur NTP. Le nom ou l'adresse IP ne peuvent pas être modifiés après avoir ajouté le serveur NTP.
   - Intervalle**minimum d'interrogation** : spécifiez la valeur minimale de l'intervalle entre les messages NTP transmis, en secondes sous la forme d'une puissance de 2. Par exemple, si vous souhaitez que l'intervalle minimal d'interrogation soit de 64 secondes, qui peut être exprimé par 2^6, saisissez 6.
   - Intervalle**maximum d'interrogation**: spécifiez la valeur maximale de l'intervalle entre les messages NTP transmis, en secondes sous la forme d'une puissance de 2. Par exemple, si vous souhaitez que l'intervalle d'interrogation maximal soit de 256 secondes, ce qui peut être exprimé sous la forme 2^8, entrez 8.
   - **Identifiant de clé** : entrez l'identifiant de clé qui peut être utilisé pour l'authentification par clé symétrique auprès du serveur NTP. N'ajoutez pas d'identifiant de clé si vous choisissez de sélectionner Autokey.
   - **Autokey** : sélectionnez **Autokey** si vous souhaitez utiliser l'authentification par clé publique avec le serveur NTP. Ne sélectionnez pas si vous souhaitez ajouter un identifiant clé.
   - **Préféré** —Sélectionnez cette option si vous souhaitez spécifier ce serveur NTP comme serveur préféré pour la synchronisation des horloges. Cela ne s'applique que si plusieurs serveurs sont configurés.

3. Cliquez sur **Créer**.

Pour activer la synchronisation NTP sur Citrix ADM :

1. Accédez à **Système > Serveurs NTP**.
2. Cliquez sur **Synchronisation NTP** et **activez la case à cocher Activer la synchronisation NTP**.
3. Cliquez sur **OK**.



> Remarque
>
> Vous pouvez trouver les messages de journalisation NTP dans le répertoire /var/log dans le fichier `/var/log/ntpd.log` fichier.

Mettre à niveau Citrix Application Delivery Management (ADM)

February 1, 2024

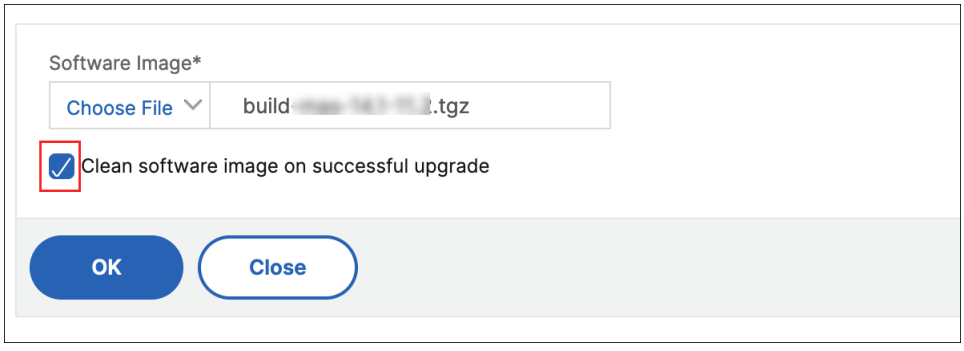
Chaque version de Citrix ADM offre des fonctionnalités nouvelles et mises à jour avec des fonctionnalités améliorées. Une liste complète des améliorations est répertoriée dans les notes de mise à jour accompagnant l'annonce de publication. Prenez le temps de lire les notes de mise à jour avant de mettre à jour le logiciel. Il est important de comprendre le cadre de licences et les types de licences avant de commencer à mettre à niveau.

Pour mettre à niveau Citrix ADM :

1. Accédez à **Système** > **Administrations système**. Sous le sous-titre **Administration du système**, cliquez sur **Mettre à niveau Citrix ADM**.
2. Sur la page Mettre à niveau Citrix ADM, chargez un nouveau fichier image en sélectionnant **Local** (votre ordinateur local) ou **Appliance**.

   > **Remarque**
   >
   > Lorsque vous sélectionnez **Appliance**, assurez-vous que l'image de mise à niveau est disponible `/var/mps/mps_images` dans NetScaler ADM.

   Par défaut, l'image logicielle est nettoyée après une mise à niveau réussie.
3. Cliquez sur **OK**.



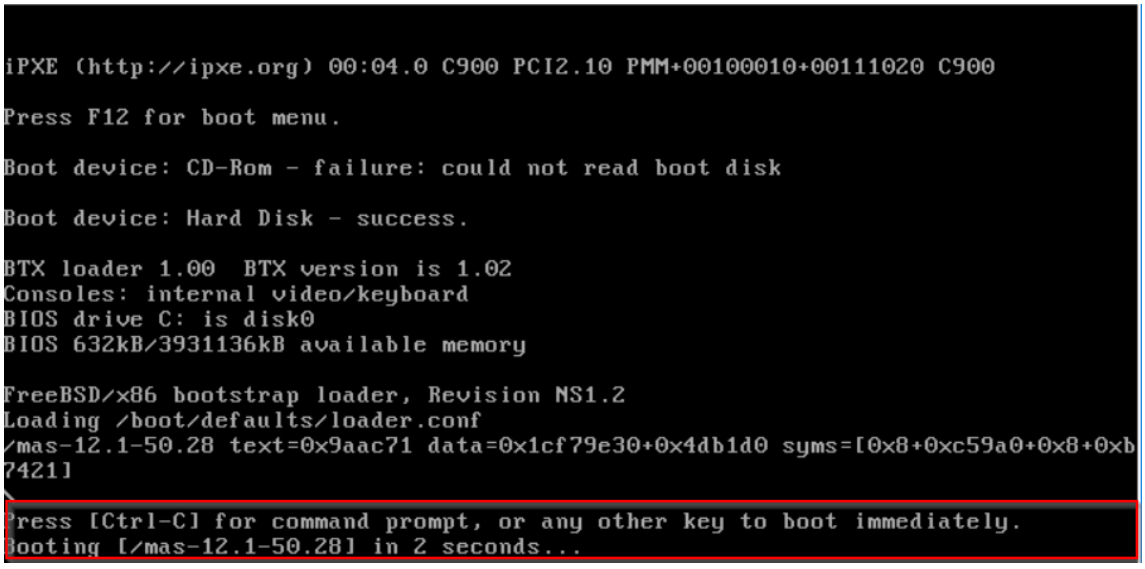
Comment réinitialiser le mot de passe pour Citrix ADM

February 1, 2024

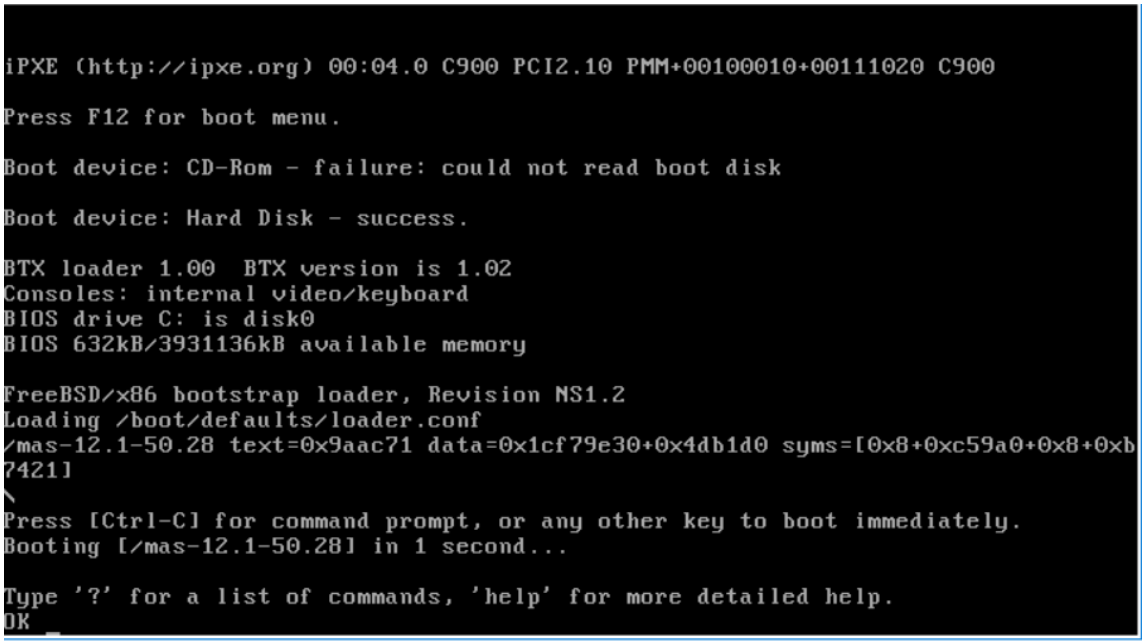
La procédure de réinitialisation du mot de passe pour Citrix ADM peut différer selon les hyperviseurs sur lesquels il est hébergé. Si vous avez modifié votre mot de passe par défaut et souhaitez rétablir le mot de passe par défaut, vous pouvez réinitialiser le mot de passe en redémarrant le nœud Citrix ADM.

Citrix Hypervisor utilisant XenCenter :

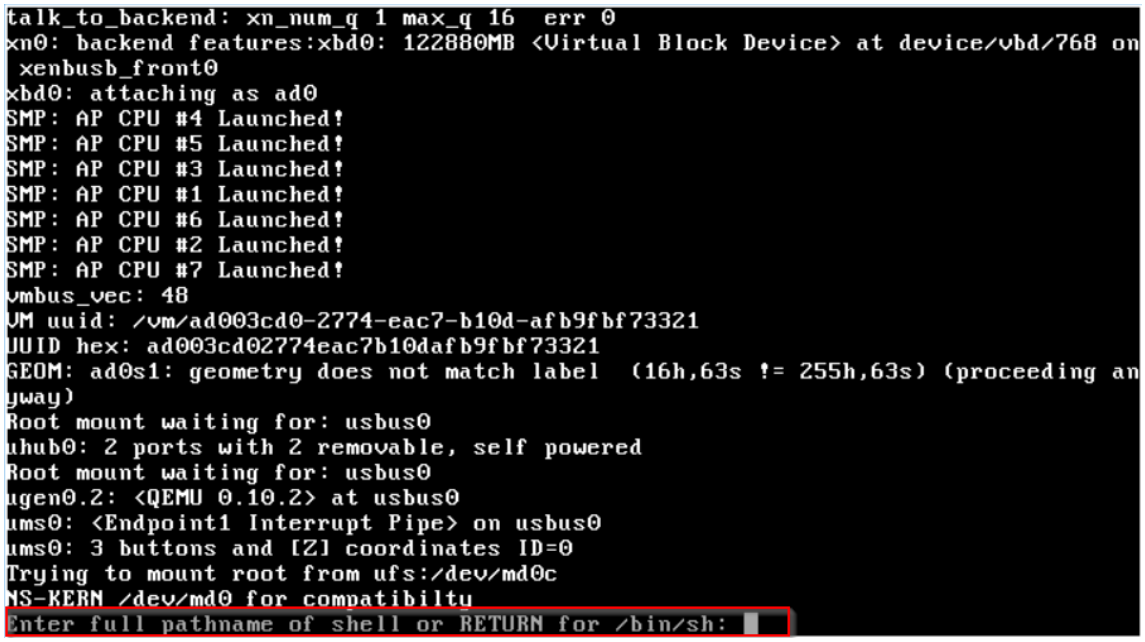
1. Connectez-vous à Citrix Hypervisor à l'aide de XenCenter.
2. Sélectionnez le nœud Citrix ADM, cliquez avec le bouton droit de la souris et sélectionnez **Redémarrer**.
3. Sous l'onglet **Console**, appuyez sur **CTL +C** pour interrompre la séquence de démarrage.



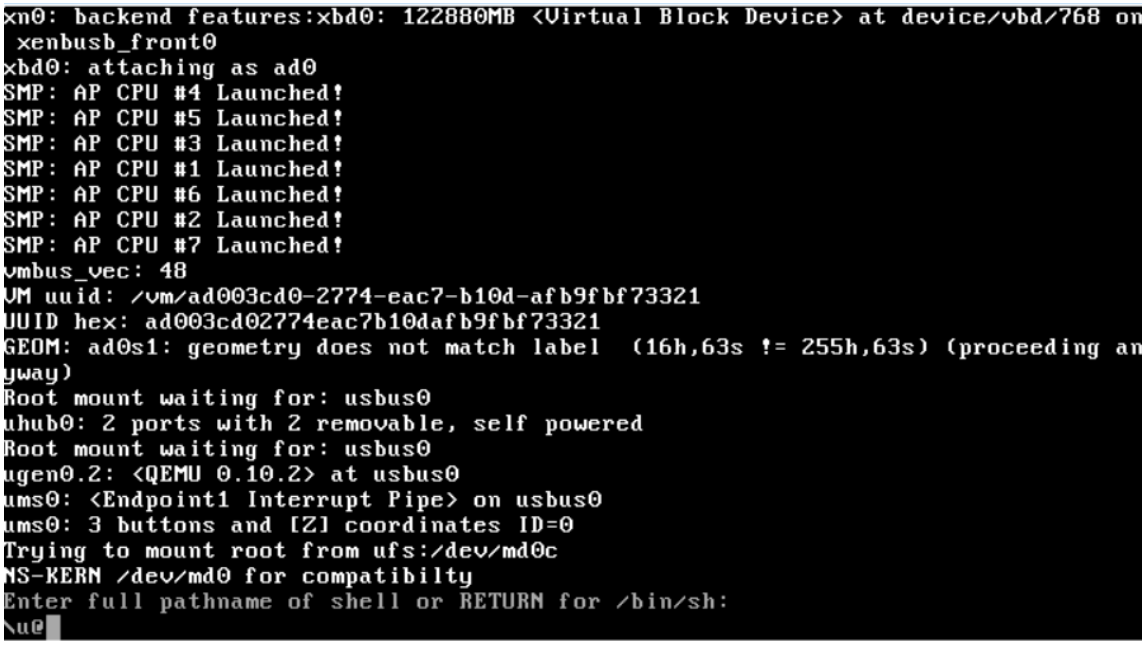
4. Exécutez la commande **boot -s** à l'invite OK.



Citrix ADM redémarre et affiche le message suivant :

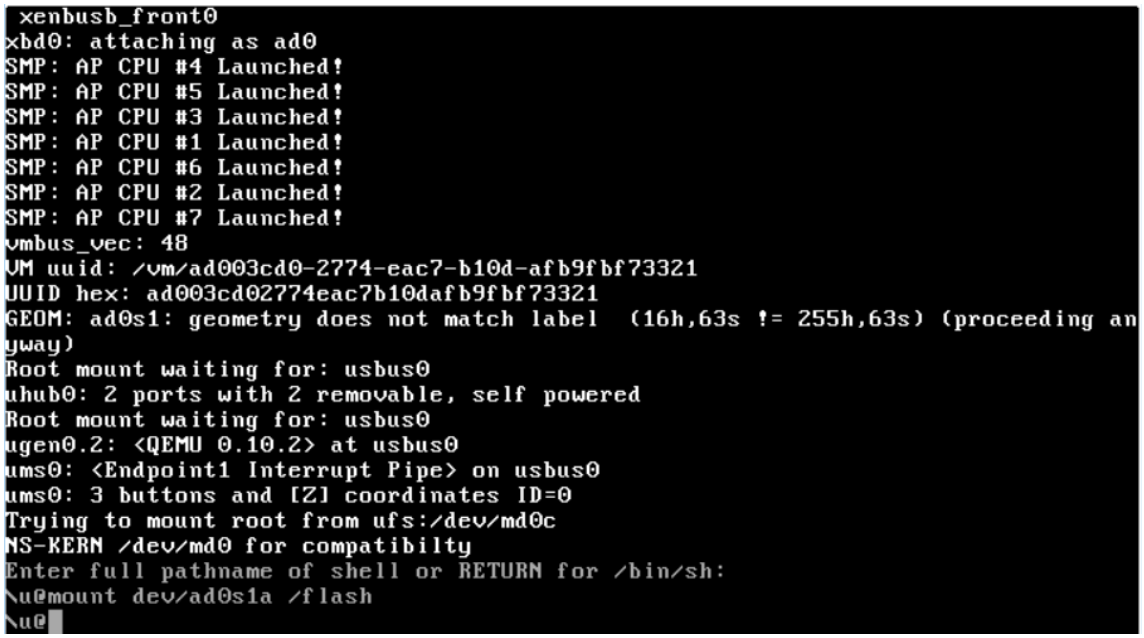


5. Appuyez sur **Entrée** pour obtenir l'invite /u@.



6. Montez la partition flash à l'aide de la commande suivante :

   ```
   mount dev/ad0s1a /flash
   ```



7. Créez un fichier à l'aide de la commande suivante :

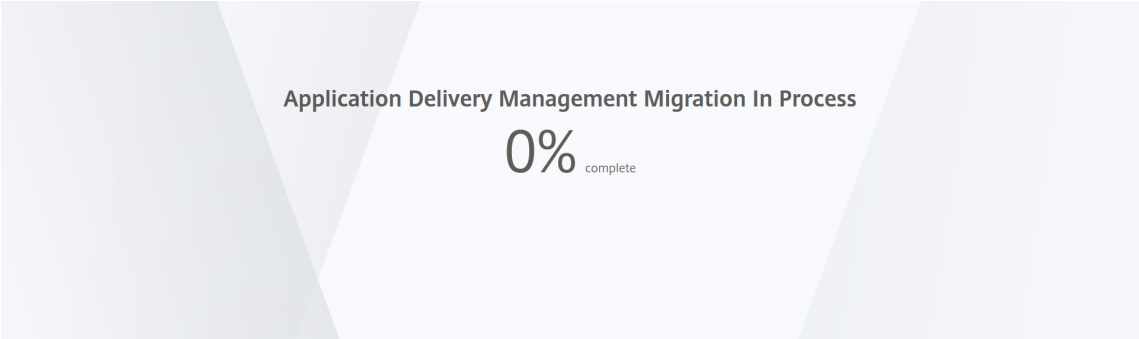
   ```
   touch /flash/mpsconfig/.recover
   ```

   Le mot de passe est maintenant réinitialisé au mot de passe par défaut.

8. Exécutez la commande **Reboot** pour redémarrer Citrix ADM.


```
xbd0: attaching as ad0
SMP: AP CPU #4 Launched!
SMP: AP CPU #5 Launched!
SMP: AP CPU #3 Launched!
SMP: AP CPU #1 Launched!
SMP: AP CPU #6 Launched!
SMP: AP CPU #2 Launched!
SMP: AP CPU #7 Launched!
vmbus_vec: 48
VM uuid: /vm/ad003cd0-2774-eac7-b10d-afb9fbf73321
UUID hex: ad003cd02774eac7b10dafb9fbf73321
GEOM: ad0s1: geometry does not match label  (16h,63s != 255h,63s) (proceeding an
yway)
Root mount waiting for: usbus0
uhub0: 2 ports with 2 removable, self powered
Root mount waiting for: usbus0
ugen0.2: <QEMU 0.10.2> at usbus0
ums0: <Endpoint1 Interrupt Pipe> on usbus0
ums0: 3 buttons and [Z] coordinates ID=0
Trying to mount root from ufs:/dev/md0c
NS-KERN /dev/md0 for compatibilty
Enter full pathname of shell or RETURN for /bin/sh:
\u@mount dev/ad0s1a /flash
\u@touch /flash/mpsconfig/.recover
\u@reboot
```

9. Accédez à l'interface graphique Citrix ADM et attendez que le redémarrage soit terminé.



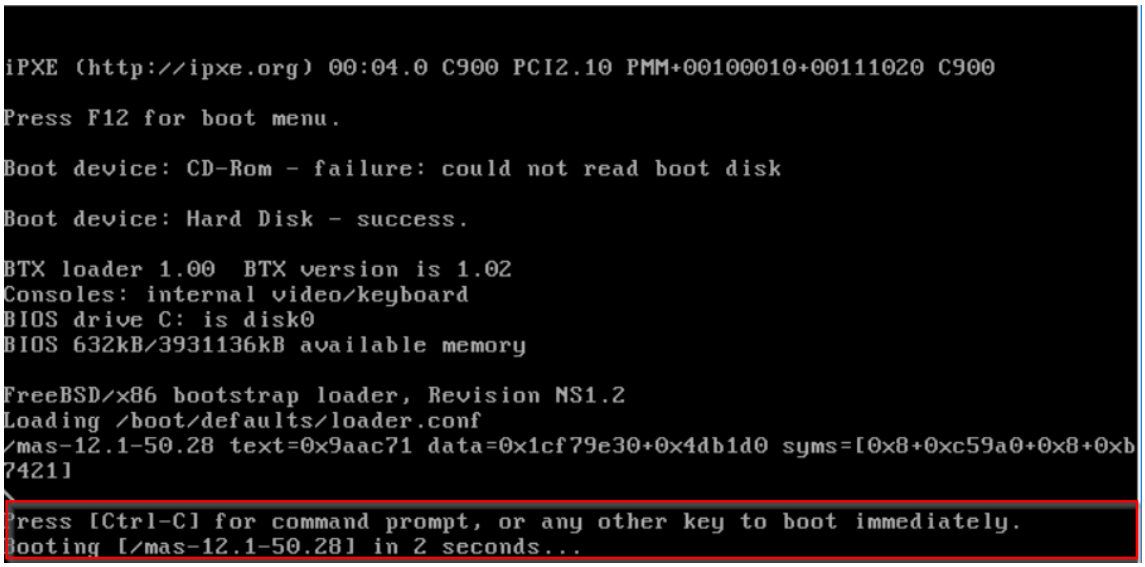
Vous pouvez maintenant utiliser les informations d'identification *nsroot/nsroot* pour ouvrir une session à partir de l'interface graphique et *nsrecover/nsroot* pour ouvrir une session à partir de l'Hypervisor.

> Remarque
>
> Après le redémarrage, si le mot de passe n'a pas été réinitialisé au mot de passe par défaut, répétez la même procédure (étape 1 à étape 7). Exécutez ensuite les commandes suivantes et redémarrez Citrix ADM :
>
> - `rm /flash/mpsconfig/master.passwd`
> - `rm –rf /etc/passwd`

Esx utilisant vSphere :

1. Connectez-vous à ESX à l'aide de vSphere.
2. Sélectionnez le nœud Citrix ADM, cliquez avec le bouton droit, puis sélectionnez **Redémarrer**.

3. Sous l'onglet **Console**, appuyez sur **CTL +C** pour interrompre la séquence de démarrage.



4. Exécutez la commande **boot -s** dans l'invite OK.

   Le Citrix ADM redémarre.

5. Appuyez sur **Entrée** pour obtenir l'invite /u@.

6. Montez la partition flash à l'aide de la commande suivante :

   ```
   mount dev/da0s1a /flash
   ```

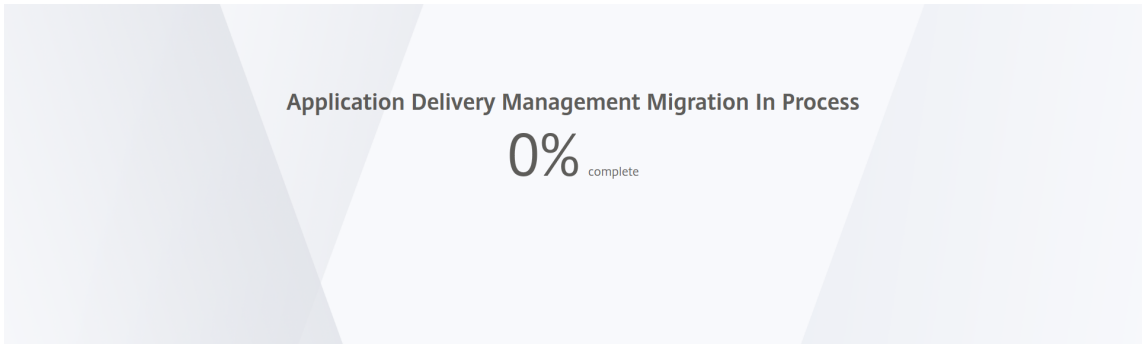
7. Créez un fichier à l'aide de la commande suivante :

   ```
   touch /flash/mpsconfig/.recover
   ```

   Le mot de passe est maintenant réinitialisé au mot de passe par défaut.

8. Exécutez la commande **Reboot** pour redémarrer Citrix ADM.

9. Accédez à l'interface graphique Citrix ADM et attendez que le redémarrage soit terminé.

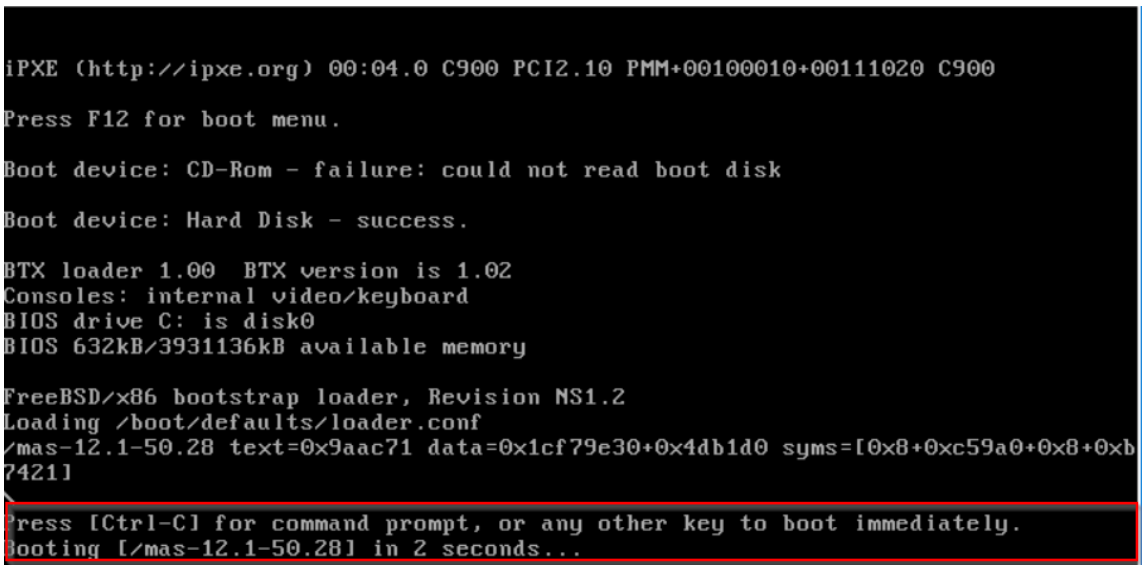


   Vous pouvez désormais utiliser les informations d'identification *nsroot/nsroot* pour ouvrir une session à partir de l'interface graphique et *nsrecover/nsroot* pour ouvrir une session à partir du serveur ESX.

> Remarque
>
> Après le redémarrage, si le mot de passe n'a pas été réinitialisé au mot de passe par défaut, répétez la même procédure (étape 1 à étape 7). Exécutez ensuite les commandes suivantes et redémarrez Citrix ADM :
>
> - `rm /flash/mpsconfig/master.passwd`
> - `rm –rf /etc/passwd`

Hyper-V utilisant le gestionnaire Hyper-V :

1. Connectez-vous à Hyper-V à l'aide du gestionnaire Hyper-V.
2. Sélectionnez le nœud Citrix ADM, cliquez avec le bouton droit, puis sélectionnez **Redémarrer**.
3. Sous l'onglet **Console**, appuyez sur **CTL +C** pour interrompre la séquence de démarrage.



4. Exécutez la commande **boot -s** à l'invite OK.

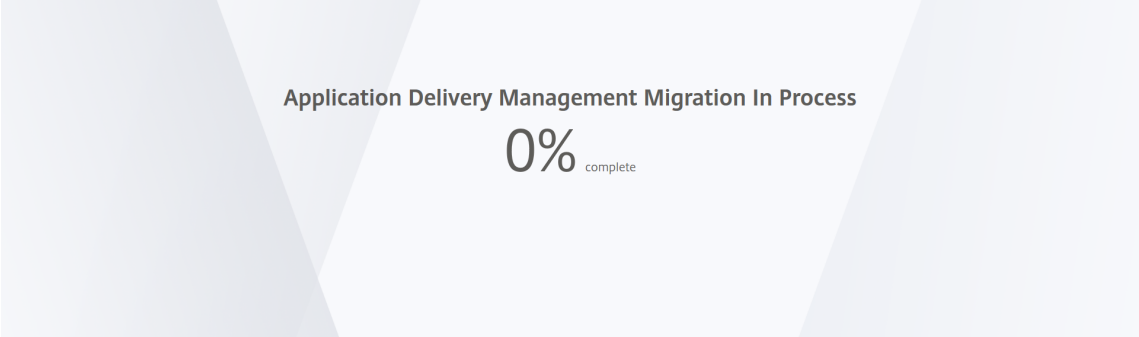
   Le Citrix ADM redémarre.
5. Appuyez sur **Entrée** pour obtenir l'invite /u@.
6. Montez la partition flash à l'aide de la commande suivante :

   ```
   mount dev/ad0s1a /flash
   ```
7. Créez un fichier à l'aide de la commande suivante :

   ```
   touch /flash/mpsconfig/.recover
   ```

   Le mot de passe est maintenant réinitialisé au mot de passe par défaut.
8. Exécutez la commande **Reboot** pour redémarrer Citrix ADM.

9. Accédez à l'interface graphique Citrix ADM et attendez que le redémarrage soit terminé.



Vous pouvez maintenant utiliser les informations d'identification *nsroot/nsroot* pour ouvrir une session à partir de l'interface graphique et *nsrecover/nsroot* pour ouvrir une session à partir du gestionnaire hyper-v.

> Remarque
>
> Après le redémarrage, si le mot de passe n'a pas été réinitialisé au mot de passe par défaut, répétez la même procédure (étape 1 à étape 7). Exécutez ensuite les commandes suivantes et redémarrez Citrix ADM :
>
> - `rm /flash/mpsconfig/master.passwd`
> - `rm –rf /etc/passwd`

Serveur KVM Linux (SSH to KVM Server à l'aide de n'importe quel client SSH) :

1. Connectez-vous à Citrix ADM à l'aide d'un client SSH sur le serveur KVM.
2. Redémarrez Citrix ADM.
3. Appuyez sur **CTL + C** pour interrompre la séquence de démarrage peu après l'affichage du message **Loading /boot/defaults/loader.conf**.
4. À l'invite OK, exécutez la commande suivante :

   ```
   set console='comconsole,vidconsole'
   ```

5. Exécutez la commande **boot -s** pour redémarrer Citrix ADM.
6. Une fois que le message **Enter full path of shell ou RETURN for /bin/sh :** s'affiche, appuyez sur **Entrée** pour obtenir l'invite /u@.
7. Montez la partition flash à l'aide de la commande suivante :

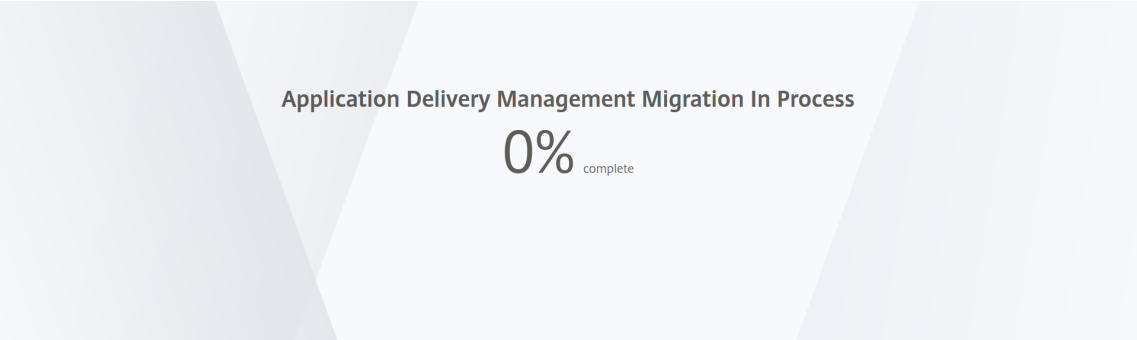
   ```
   mount dev/vtbd0s1a /flash
   ```

8. Créez un fichier à l'aide de la commande suivante :

   ```
   touch /flash/mpsconfig/.recover
   ```

   Le mot de passe est maintenant réinitialisé au mot de passe par défaut.

9. Exécutez la commande **Reboot** pour redémarrer Citrix ADM.
10. Accédez à l'interface graphique Citrix ADM et attendez que le redémarrage soit terminé.



Vous pouvez désormais utiliser les informations d'identification *nsroot/nsroot* pour ouvrir une session à partir de l'interface graphique et *nsrecover/nsroot* pour ouvrir une session à partir de la console SSH.

> Remarque
>
> Après le redémarrage, si le mot de passe n'a pas été réinitialisé au mot de passe par défaut, répétez la même procédure (étape 1 à étape 7). Exécutez ensuite les commandes suivantes et redémarrez Citrix ADM :
>
> - `rm /flash/mpsconfig/master.passwd`
> - `rm –rf /etc/passwd`

Configurer une carte réseau double pour accéder à Citrix ADM

February 1, 2024

Vous pouvez configurer une deuxième carte réseau pour isoler l'accès de gestion à Citrix ADM. À l'aide de cette deuxième fonctionnalité de carte réseau, en fonction de vos besoins, vous pouvez choisir la manière dont vous souhaitez isoler le trafic reçu et envoyé via Citrix ADM.

Envisagez un scénario dans lequel vous souhaitez isoler le trafic pour :

- Réalisez toutes les communications entre Citrix ADM et ses instances Citrix ADC gérées sur un seul réseau.
- Bénéficiez d'un accès de gestion à Citrix ADM sur un autre réseau.

Dans ce scénario, en tant qu'administrateur, vous pouvez :

- Configurez une adresse IP pour le trafic entre Citrix ADM et ses instances Citrix ADC gérées.

- Configurez une autre adresse IP pour gérer le logiciel Citrix ADM afin d'effectuer toutes les tâches administratives du logiciel.

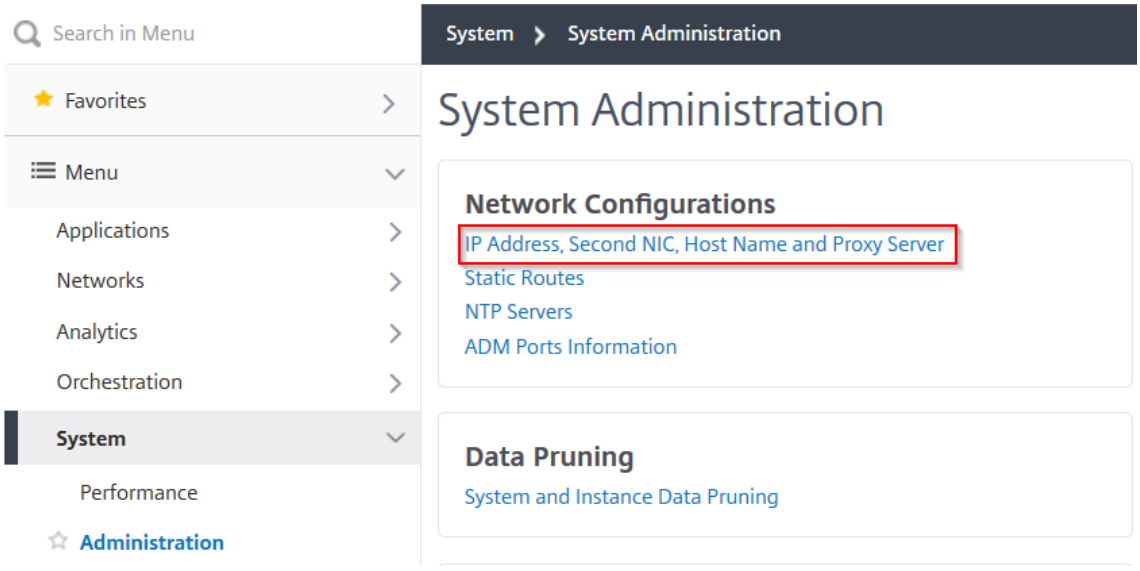
> **Remarque**
>
> Si Citrix ADM est configuré en tant que paire HA, l'adresse IP de gestion configurée sur la deuxième carte réseau est associée au nœud principal.

Conditions préalables

- Assurez-vous d'avoir déployé et configuré **Citrix ADM 13.0 Build 47.x ou version ultérieure** sur l'hyperviseur (Citrix Hypervisor, Microsoft Hyper-V, Linux KVM ou VMware ESXi).
- Assurez-vous d'avoir ajouté la deuxième carte réseau sur l'hyperviseur (Citrix Hypervisor, Microsoft Hyper-V, Linux KVM ou VMware ESXi).

Configurer une deuxième carte réseau dans Citrix ADM

1. Connectez-vous à l'interface graphique d'ADM.
2. Accédez à **Système** > **Administration** .
3. Sous **Configuration réseau**, cliquez sur **Adresse IP, Deuxième carte réseau, Nom d'hôte et Serveur proxy**.



La page **de configuration réseau** s'affiche.

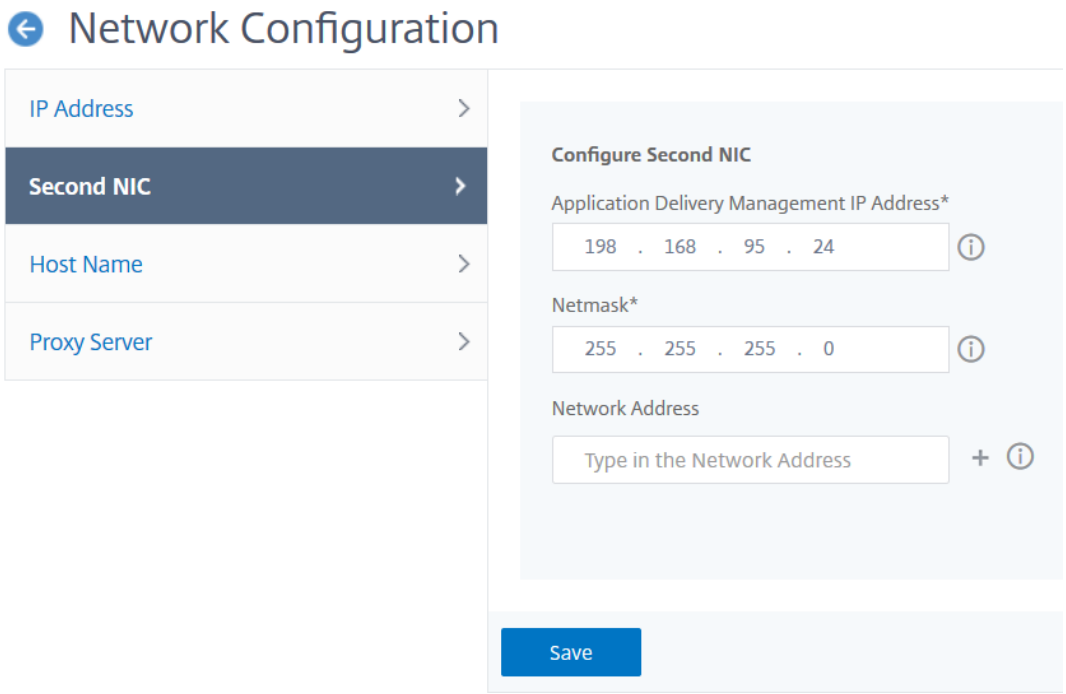
4. Cliquez sur l'onglet Deuxième carte réseau et configurez les paramètres suivants :

a) **Adresse IP de gestion de la mise à disposition des applications** —Entrez une adresse IP valide pour accéder à Citrix ADM. Vous pouvez utiliser cette adresse IP pour accéder à Citrix ADM, en plus de l'adresse IP de gestion existante.

b) **Masque réseau** —Entrez l'adresse du masque de réseau pour spécifier l'hôte réseau. L'adresse par défaut est 255.255.255.0.

c) **Adresse réseau** —Entrez une adresse IP pour ajouter une entrée de route pour Citrix ADM. Cliquez sur **+** pour ajouter d'autres adresses IP. Ce champ est facultatif.

d) Cliquez sur **Enregistrer**.



Configurer l'intervalle de purge de syslog

February 1, 2024

Syslog est un protocole standard de journalisation. Il comprend deux composants : le module d'audit Syslog, qui s'exécute sur l'instance Citrix Application Delivery Controller (ADC), et le serveur Syslog, qui peut s'exécuter soit sur le système d'exploitation FreeBSD sous-jacent de l'instance Citrix ADC, soit sur un système distant. SYSLOG utilise User Datagram Protocol (UDP) pour le transfert de données.

Syslog permet d'isoler le système qui génère les informations et le système qui stocke les informations. Vous pouvez consolider les informations de journalisation et obtenir des informations à partir

des données collectées. Vous pouvez également configurer syslog pour consigner différents types d'événements.

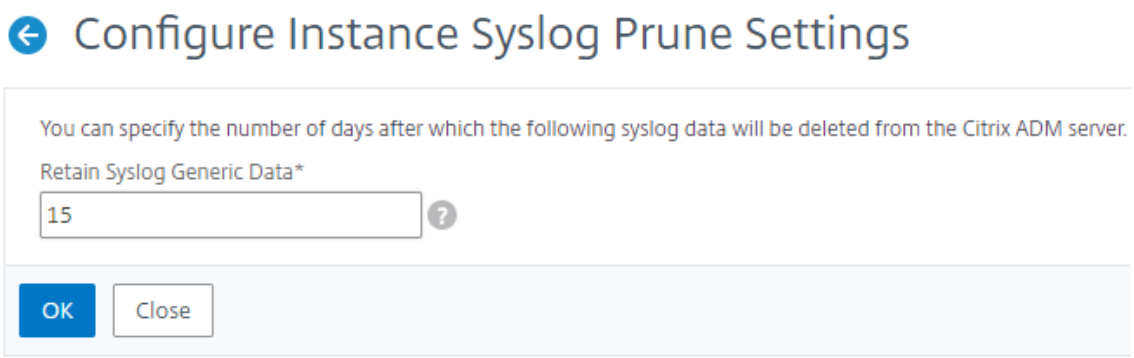
Pour limiter la quantité de données syslog stockées dans la base de données, vous pouvez spécifier l'intervalle auquel vous souhaitez nettoyer les données syslog.Vous pouvez spécifier le nombre de jours après lesquels les données syslog suivantes seront supprimées de Citrix Application Delivery Management (ADM) :

- Données Syslog génériques
- Données AppFirewall
- Données Citrix Gateway

Vous pouvez également configurer l'intervalle de nettoyage de Citrix Gateway par type de syslog. Cet intervalle de nettoyage a priorité sur l'intervalle de nettoyage configuré pour conserver les données Citrix Gateway.

Pour configurer les paramètres d'intervalle de nettoyage de syslog pour Citrix ADM :

1. Accédez à **Système > Administration**.Sous **Nettoyage des données**, cliquez sur **Nettoyage des données système et instance**, puis cliquez sur **Syslog d'instance**.
2. Dans la page **Configurer les paramètres Syslog de nettoyage d'instance**, spécifiez **Conserver les données génériques Syslog (jours)**. Tapez le nombre de jours pendant lesquels Citrix ADM conserve les messages syslog génériques.



Configurer les paramètres de nettoyer système et d'un nettoyer d'événement

February 1, 2024

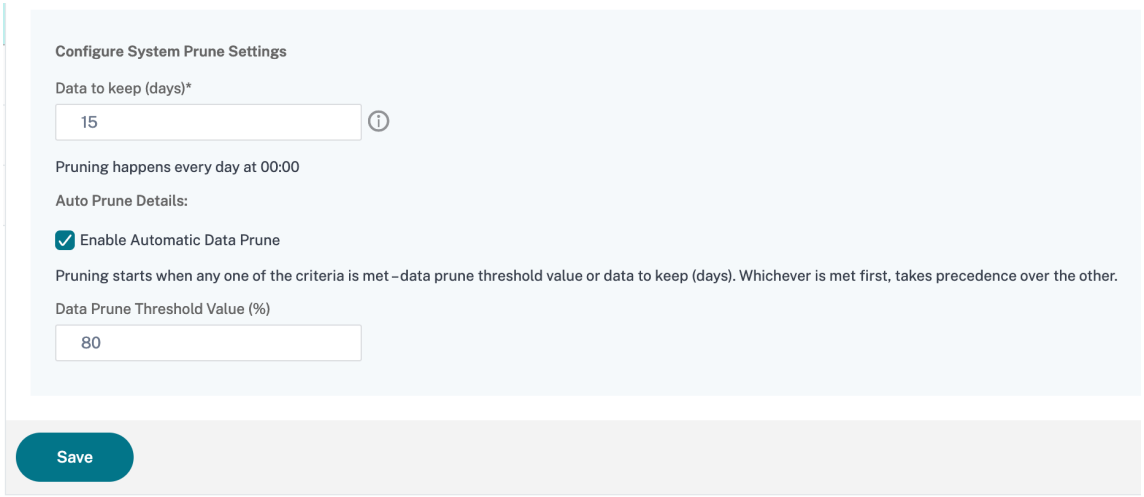
Pour limiter la quantité de données de reporting stockées dans votre base de données logicielle Citrix Application Delivery Management (ADM), vous pouvez les nettoyer. Vous pouvez spécifier l'intervalle

pendant lequel Citrix ADM conserve les données de reporting réseau, les événements, les journaux d'audit et les journaux de tâches. Par défaut, ces données sont nettoyées toutes les 24 heures (à 00.00 heures).

> Remarque
>
> La valeur que vous spécifiez ne peut pas dépasser 30 jours ou être inférieure à 15 jours.

Pour configurer les paramètres de nettoyage du système pour les rapports de performances à l'aide de Citrix ADM :

1. Accédez à **Système** > **Administration**. Sous **Nettoyage des données**, cliquez sur **Nettoyage des données du système et de l'instance**.
2. Dans la page**Configurer les paramètres de nettoyage du système**, spécifiez le nombre de jours pendant lesquels les données doivent être conservées, puis cliquez sur**OK**.



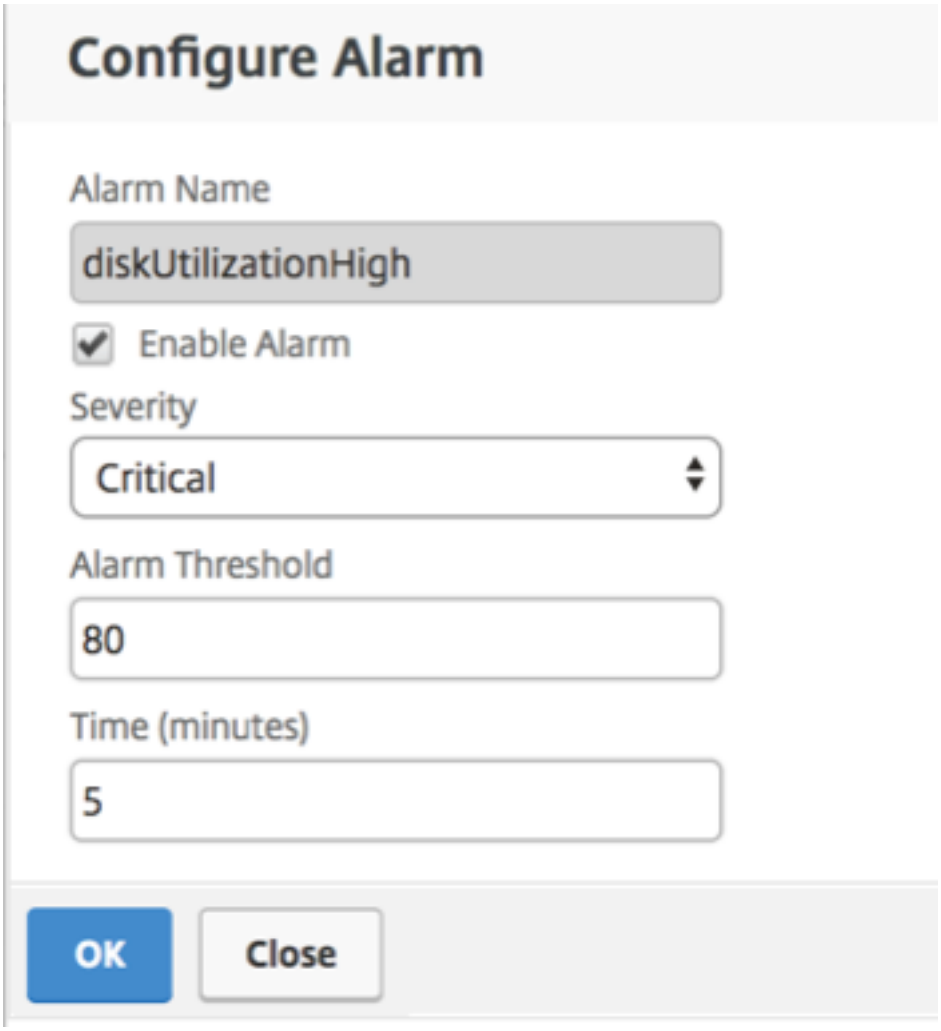
Vous pouvez activer le nettoyage automatique en cochant la case**Activer le nettoyage automatique des données**. Une alarme est déclenchée et un e-mail est envoyé lorsque l'utilisation du disque dépasse la **valeur seuil de nettoyage des données**configurée. Pour modifier le pourcentage d'espace disque (seuil de nettoyage), cliquez sur **Modifier**.

> Remarque
>
> Le nettoyage commence lorsque l'un des critères est satisfait : valeur de seuil de nettoyage des données ou données à conserver (jours). Celui qui est atteint en premier a la priorité sur l'autre.

Vous pouvez configurer et activer l'alarme **DiskUtilizationHigh** (par défaut) et spécifier les éléments suivants :

- **Gravité**, telle que Critique.
- **Seuil d'alarme**. Entrez la valeur pour laquelle la gravité de l'événement est calculée.

- **Heure**. Durée (en minutes) après laquelle vous voulez déclencher l'alarme.



Configurer les paramètres d'appel d'événements à l'aide de Citrix ADM

Pour limiter la quantité de données des messages d'événement stockées dans votre base de données Citrix ADM, vous pouvez spécifier l'intervalle pour lequel vous souhaitez que Citrix ADM conserve les données de rapport réseau, les événements, les journaux d'audit et les journaux des tâches. Par défaut, ces données sont nettoyées toutes les 24 heures (à 00.00 heures).

- Accédez à **Système > Administration > Elagage des données**, puis cliquez sur **Elagage des données système et instance**. Cliquez sur **Événements d'instance**.
- Entrez l'intervalle de temps, en jours, pour lequel vous souhaitez conserver les données sur le serveur Citrix ADM, puis cliquez sur **Enregistrer**.

Activer l'accès shell pour les utilisateurs non par défaut

February 1, 2024

Vous pouvez activer l'accès shell pour les utilisateurs autres que par défaut dans Citrix Application Delivery Management (ADM). Vous pouvez utiliser cette fonctionnalité pour activer et configurer le mode de communication avec les instances.

> **Remarque**
>
> Par défaut, l'accès shell est désactivé pour les utilisateurs autres que par défaut.

Pour activer l'accès shell pour les utilisateurs autres que par défaut dans Citrix ADM :

1. Dans Citrix ADM, accédez à **Système** > **Administration système**.
2. Dans **Paramètres système**, cliquez sur **Modifier les paramètres système**.
3. Sur la page **Modifier les paramètres système**, configurez les paramètres suivants :
   - **Communication avec les instances** : sélectionnez le protocole de communication.
   - **Accès sécurisé** : activez l'accès sécurisé pour Citrix ADM.
   - **Activer le délai d'expiration de la session** : spécifiez la période pendant laquelle vous souhaitez conserver une session inactive.
   - **Autoriser l'authentification de base** - Autoriser le service de gestion à accepter les informations d'identification fournies à l'aide du protocole d'authentification de base.
   - **Activer nsrecover Login** - Activer la connexion `nsrecover` sur le service de gestion.
   - **Activer le téléchargement de certificats** : vous permet de télécharger des certificats à partir de l'Citrix ADC ajouté.
   - **Activer l'accès à l'environnement de ligne de commande pour un utilisateur non nsroot** - Activer l'accès à l'environnement de ligne de commande pour les utilisateurs autres que par défaut dans Citrix ADM.
   - **Demander les informations d'identification utilisateur pour la connexion à l'instance** - Autoriser les utilisateurs à entrer leurs informations d'identification utilisateur lors de la connexion à des instances à partir de Citrix ADM.
4. Cliquez sur **OK**.

Récupérer des serveurs Citrix ADM inaccessibles

February 1, 2024

Citrix Application Delivery Management (ADM) fournit désormais un outil de maintenance de base de données pour effectuer le nettoyage de la base de données système. Vous pouvez maintenant lancer l'outil utilitaire Citrix ADM pour vous connecter au système de fichiers, supprimer quelques composants et rendre la base de données accessible. Le script de récupération Citrix ADM est un outil qui aide à récupérer de l'espace dans le système de fichiers en effaçant les tables et fichiers de base de données anciens ou inutilisés. L'outil vous aide à parcourir les tables et les fichiers de la base de données par étapes successives et affiche l'espace occupé sur le système de fichiers par les éléments respectifs. Une fois que vous avez sélectionné les tables de base de données et les fichiers à supprimer, l'outil les supprime du système de fichiers après confirmation.

Comment faire pour utiliser le script de récupération de base de données Citrix ADM pour un déploiement autonome Citrix ADM

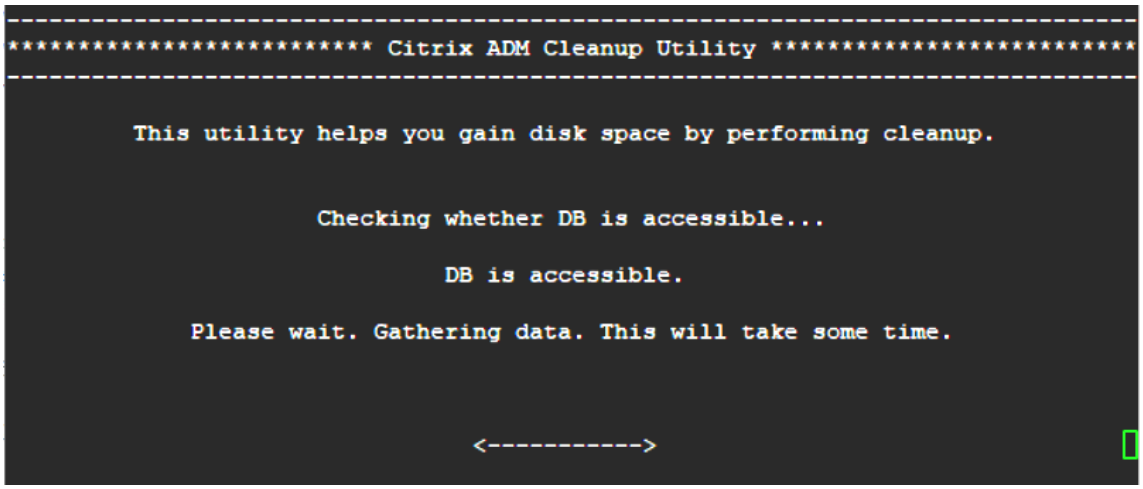
Utilisez la procédure suivante dans un déploiement Citrix ADM serveur unique pour vous connecter au système de fichiers, supprimer quelques composants et rendre la base de données accessible, puis effectuer les opérations de restauration.

1. À l'aide d'un client SSH ou de la console de votre hyperviseur, connectez-vous à Citrix ADM et tapez la commande suivante :

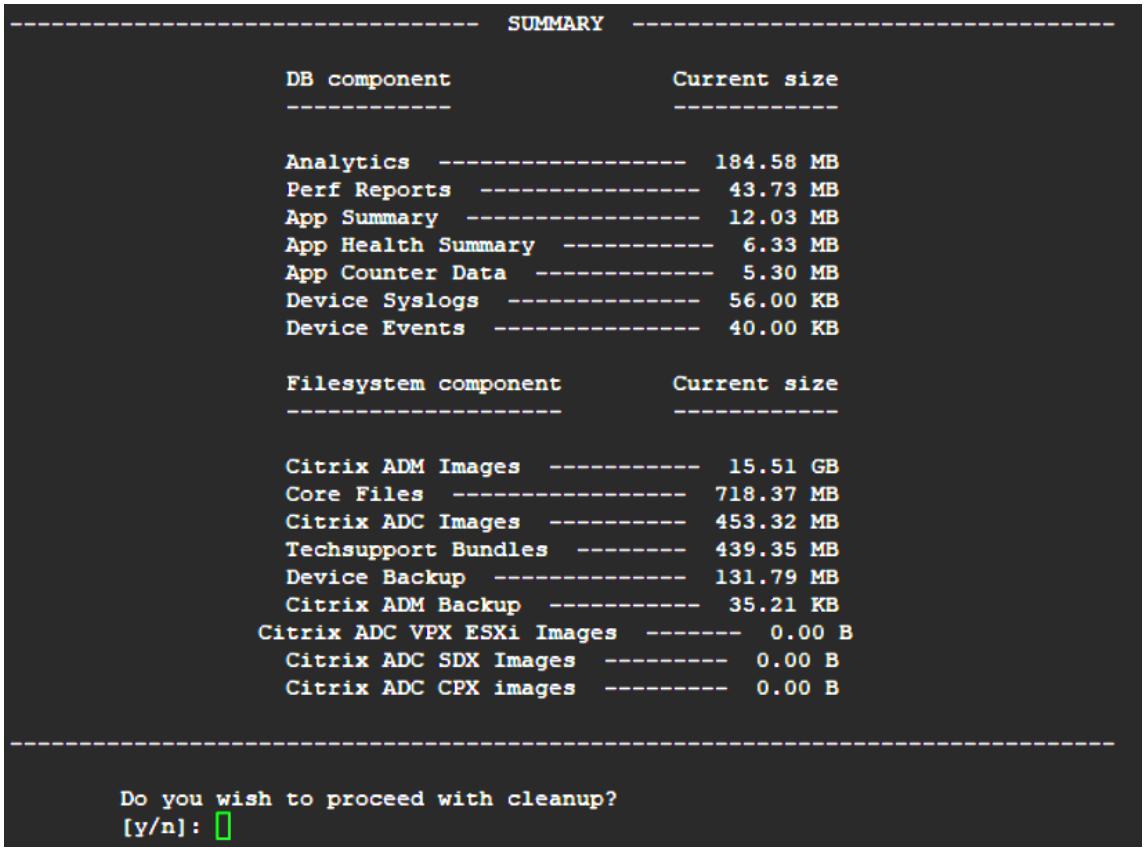
```
Last login: Fri Nov 30 09:51:19 2018 from 10.252.241.100
Have a nice daybash-3.2# /mps/mas_recovery/mas_recovery.py
```

2. Lorsque l'écran affiche un message d'avertissement pour arrêter quelques processus Citrix ADM, tapez « y » et appuyez sur la touche **Entrée**.

   L'écran suivant apparaît alors que le système détermine les composants de la base de données que vous pouvez supprimer sans affecter les fichiers principaux du système.



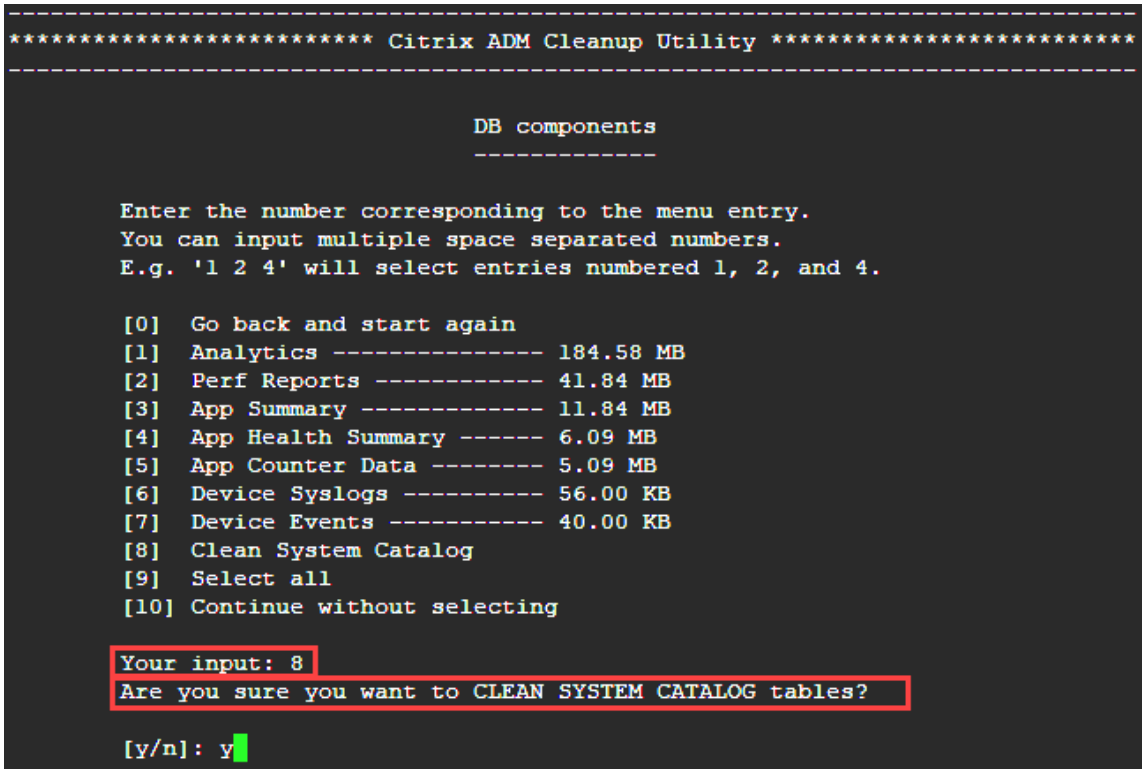
3. L'écran affiche la liste des fichiers de la base de données. Tapez « y » et appuyez sur la touche Entrée pour commencer le processus de nettoyage.



4. Vous pouvez sélectionner le composant de base de données spécifique qui doit être nettoyé et saisir le numéro correspondant. Appuyez sur la touche **Entrée** .

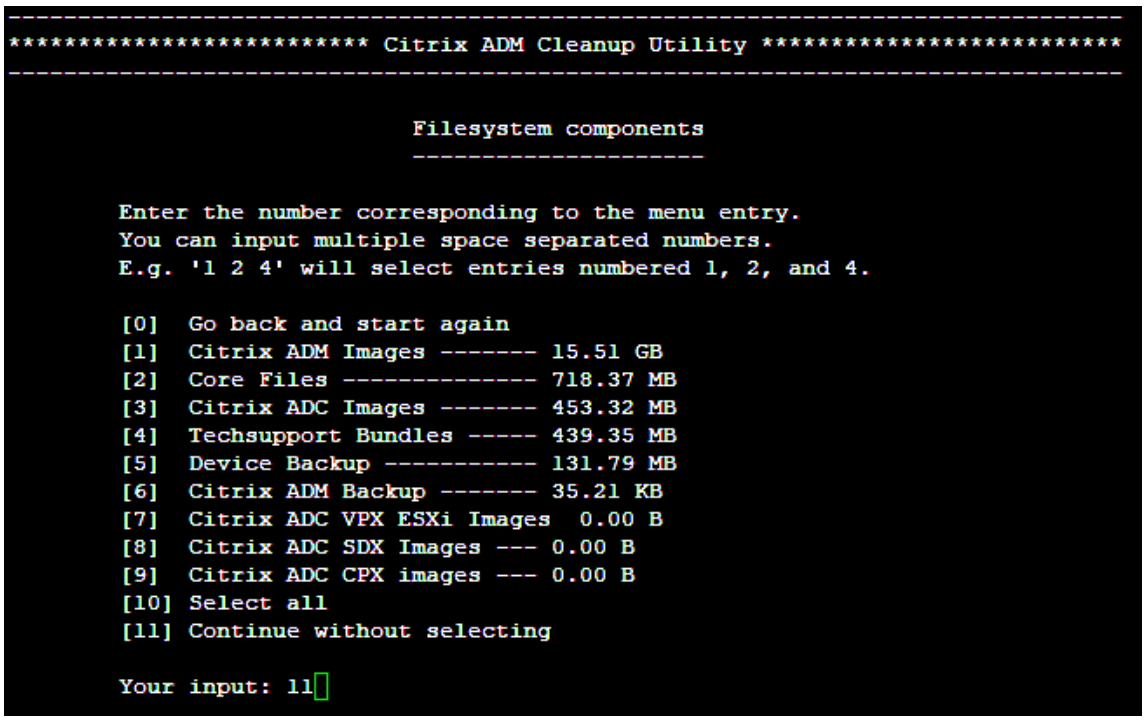
   Par exemple, pour effectuer le nettoyage du catalogue système, sélectionnez l'option 8 dans le menu de sélection des **composants DB** et tapez « y », puis appuyez sur la touche **Entrée** pour poursuivre le nettoyage du catalogue système.

   > **Remarque**
   >
   > Citrix ADM inclut des tables utilisateur appelées catalogue système. Le catalogue système est un emplacement dans la base de données Citrix ADM où un système de gestion de base de données relationnelle stocke les métadonnées de schéma, telles que des informations sur les tables et les colonnes et les enregistrements internes. Les tables du catalogue système sont comme des tables régulières qui peuvent accumuler des lignes gonflées et mortes au fil du temps et, par conséquent, nécessitent un nettoyage périodique pour des performances optimales. C'est une bonne pratique de tenir régulièrement ces tableaux. L'activité libère non seulement de l'espace disque, mais améliore également les performances globales de la base de données et, par conséquent, de l'Citrix ADM.

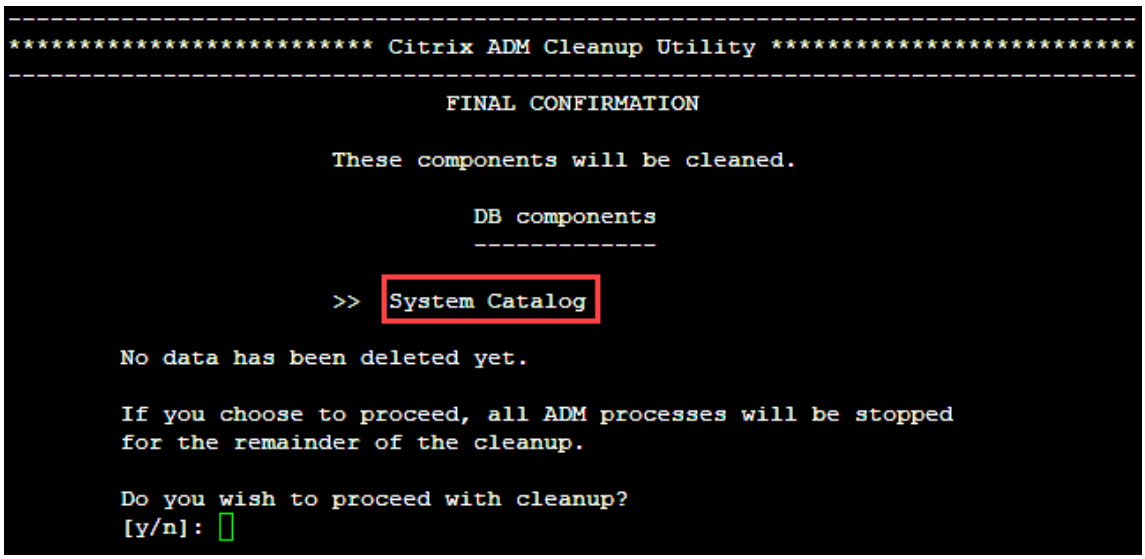


L'utilitaire de nettoyage vous permet de nettoyer les composants de base de données et les composants de fichiers. Vous pouvez sélectionner n'importe quel composant de fichier en saisissant un chiffre compris entre « 1 » et « 9 », ou en tapant « 11 » et en appuyant sur la touche Entrée pour nettoyer le composant de base de données.

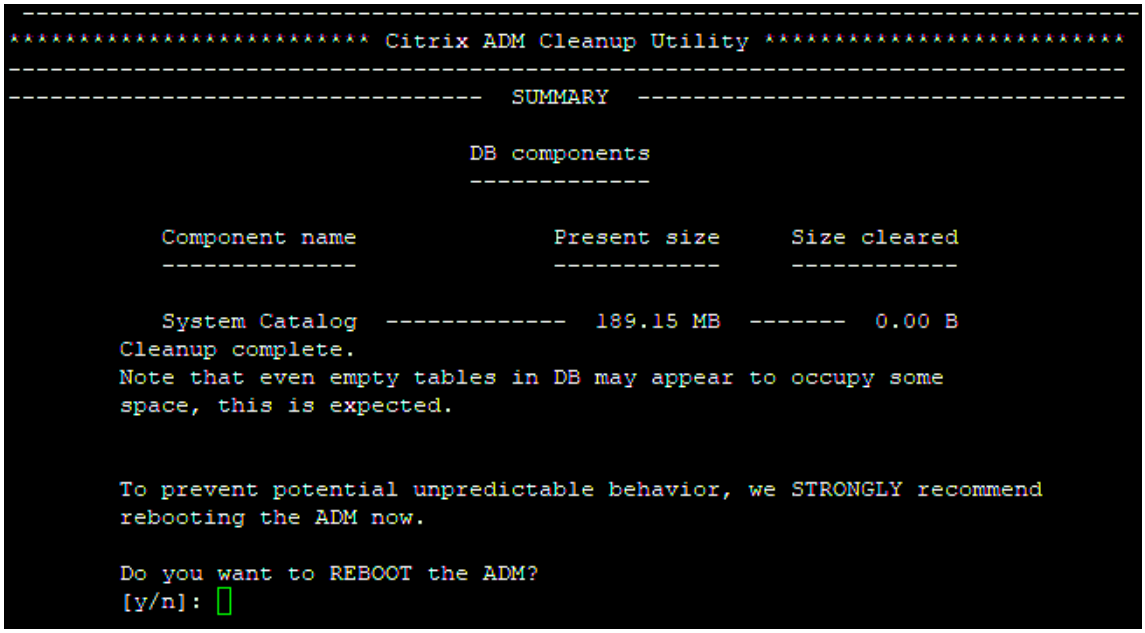
> **Remarque**
>
> Le nombre « 11 » indique que vous n'avez sélectionné aucun composant de fichier à nettoyer et que vous continuez à nettoyer le composant de base de données antérieurement sélectionné. Dans cet exemple, il s'agit du « catalogue système ».



5. Tapez « y » et appuyez à nouveau sur la touche **Entrée** sur l'écran de confirmation final.



Le catalogue du système est nettoyé, ce qui peut prendre du temps en fonction de la taille de la table qu'il contient. Une fois le processus terminé, un écran récapitulatif s'affiche.



6. Tapez « y » et appuyez sur la touche **Entrée** pour redémarrer Citrix ADM.

   Assurez-vous de redémarrer Citrix ADM après le nettoyage du système. Attendez environ 30 minutes pour que les opérations de base de données internes se terminent après le redémarrage de Citrix ADM. Vous devriez alors pouvoir vous connecter à la base de données Citrix ADM. Si ce n'est pas le cas, exécutez à nouveau le script de récupération pour libérer plus d'espace. Lorsque Citrix ADM est opérationnel, il doit fonctionner comme prévu.

   > **Remarque**
   >
   > La taille actuelle de la table de catalogue système n'est jamais égale à zéro après le nettoyage. En effet, seules les lignes vides sont supprimées de la table et la table peut avoir des entrées valides même après leur nettoyage.

Comment faire pour utiliser le script de récupération de base de données Citrix ADM pour un déploiement haute disponibilité Citrix ADM

Le système de base de données pour les serveurs Citrix ADM dans un déploiement à haute disponibilité est en mode de synchronisation continue. Lors de l'utilisation du nouvel outil de récupération de base de données, vous n'avez pas besoin de répliquer la procédure sur les deux serveurs Citrix ADM.

1. À l'aide d'un client SSH ou d'une console d'hyperviseur, connectez-vous au nœud principal.
2. Exécutez la commande suivante :

   ```
   /mps/mas_recovery/mas_recovery.py
   ```

3. Suivez la procédure de l'étape 2 disponible pour le script de récupération de déploiement autonome Citrix ADM

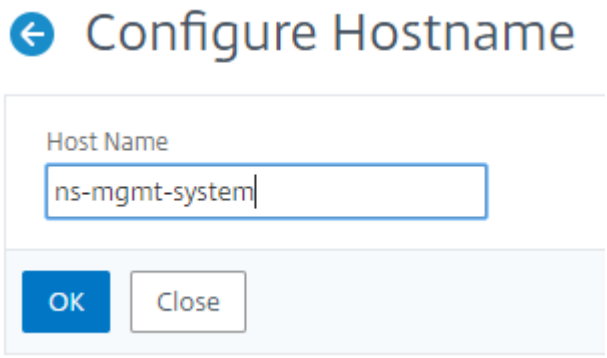
Attribuer un nom d'hôte à un serveur Citrix ADM

February 1, 2024

Pour identifier un serveur Citrix Application Delivery Management (ADM), vous pouvez lui attribuer un nom d'hôte. Le nom d'hôte s'affiche sur la licence universelle pour Citrix ADM.

Pour attribuer un nom d'hôte à un serveur Citrix ADM :

1. Dans Citrix ADM, accédez à **Système** > **Administration système**.
2. Sous **Paramètres système**, cliquez sur **Modifier le nom d'hôte**.
3. Dans la page **Configurer le nom d'hôte**, entrez un nom d'hôte et cliquez sur **OK**.



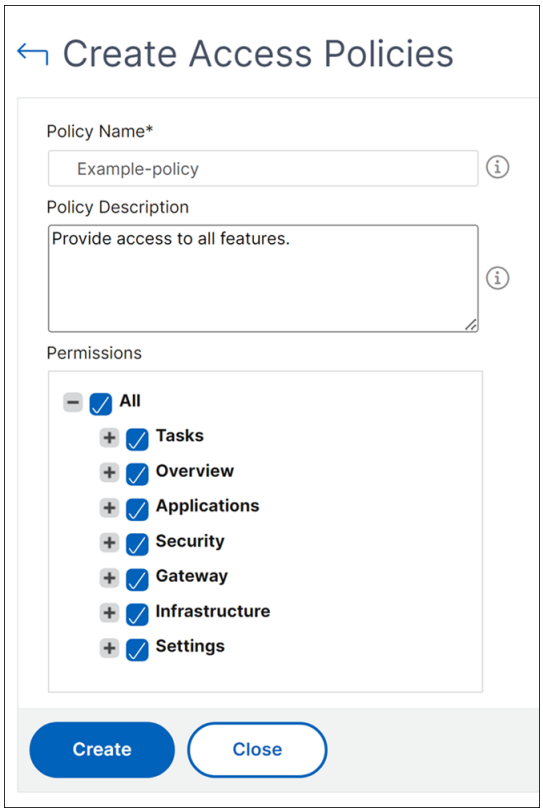
Sauvegarder et restaurer votre serveur Citrix ADM

February 1, 2024

Vous pouvez effectuer des sauvegardes périodiques de votre serveur Citrix ADM. Vous pouvez sauvegarder et restaurer les fichiers de configuration, les détails de l'instance, les données système, etc.

> **Important**
>
> Citrix vous recommande de restaurer le serveur ADM à l'aide d'une sauvegarde de la même version. Par exemple, si la version ADM est 13.0, utilisez la sauvegarde ADM 13.0 pour restaurer le serveur.
>
> L'accès des utilisateurs à la sauvegarde et à la restauration du serveur ADM est limité. La page **Système > Fichiers de sauvegarde** s'affiche uniquement pour les utilisateurs qui ont accès à toutes les fonctionnalités ADM. Un utilisateur ne peut accéder à cette page que si sa stratégie d'accès dispose de toutes les autorisations. Généralement, les superutilisateurs ont accès à toutes

les fonctionnalités ADM.



Pour plus d'informations, voir Configurer les stratégies d'accès.

Avant de procéder à la mise à niveau, sauvegardez les fichiers de configuration du serveur ADM pour des raisons de précaution.

La sauvegarde comprend les composants suivants :

- Fichiers de configuration Citrix ADM :
  - SNMP
  - Fichiers de configuration du serveur Syslog
  - Fichiers NTP
  - Certificats SSL
  - Fichiers du Centre de contrôle
- Sauvegardes des instances Citrix ADC gérées par le serveur Citrix ADM.
- Modèles d'audit de configuration.
- Données système stockées dans la base de données :
  - Liste des locataires et des utilisateurs créée.

  - Configuration du serveur d'authentification externe (LDAP, RADIUS, etc.).
  - Tâches de configuration et modèles de tâches créés.
- Données d'infrastructure et d'application stockées dans la base de données :
  - Données provenant d'instances Citrix ADC ajoutées et gérées.
  - Détails du profil d'instance, détails de version, détails du groupe d'instances, etc.
  - Application statique (groupe de serveurs virtuels) créée par l'administrateur.
- Paramètres SNMP.

> **Remarque**
>
> Les données Analytics, les événements, les licences ADM et les messages syslog sont exclus de la sauvegarde.

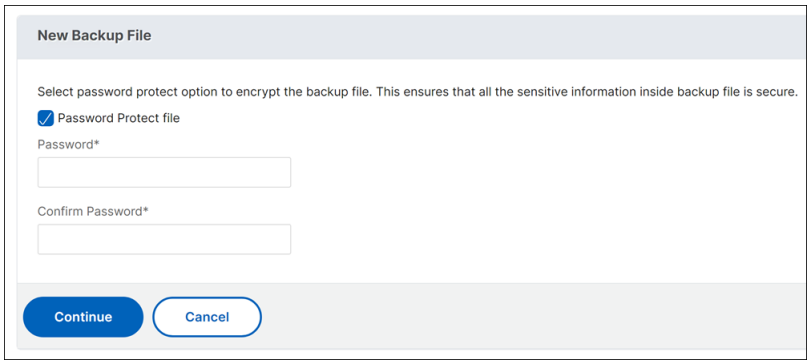
Sauvegardez la configuration Citrix ADM

Par défaut, le serveur Citrix ADM sauvegarde la configuration toutes les 24 heures (à 00,30 heures). Vous pouvez également planifier et sélectionner l'heure de la sauvegarde. Vous pouvez également déplacer une copie du fichier sauvegardé vers un autre système.

La sauvegarde est stockée sous forme de fichier TAR compressé qui peut également être crypté. Par défaut, trois fichiers de sauvegarde sont conservés dans le serveur. Pour éviter tout problème d'espace disque faible, vous pouvez stocker un maximum de 10 fichiers de sauvegarde sur votre serveur Citrix ADM. Toutefois, Citrix vous recommande de stocker certaines copies de vos fichiers de sauvegarde sur le serveur ou de transférer les fichiers vers un autre système par mesure de précaution.

Pour sauvegarder une configuration Citrix ADM :

1. Accédez à **Système > Fichiers de sauvegarde**, puis cliquez sur **Sauvegarder**.
2. Pour chiffrer le fichier de sauvegarde, activez la case à cocher **Password Protect file**, puis fournissez un mot de passe pour chiffrer le fichier.

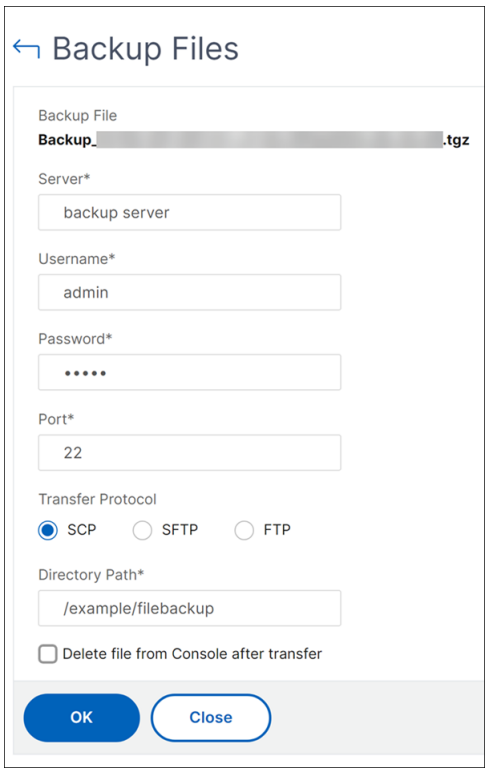


Transférer un fichier de sauvegarde Citrix ADM vers un système externe

Vous pouvez transférer une copie du fichier de sauvegarde vers un autre système par mesure de précaution. Lorsque vous souhaitez restaurer la configuration, téléchargez d'abord le fichier sur le serveur Citrix ADM, puis effectuez l'opération de restauration.

Pour transférer un fichier de sauvegarde Citrix ADM :

1. Accédez à **Système > Fichiers de sauvegarde**.
2. Sélectionnez le fichier de sauvegarde que vous souhaitez déplacer vers un autre système, puis cliquez sur **Transférer**.
3. Sur la page **Fichiers de sauvegarde**, spécifiez les paramètres suivants :
    - **Serveur** : adresse IP du système sur lequel vous souhaitez transférer le fichier sauvegardé.
    - **Nom d'utilisateur et mot de passe** : informations d'identification utilisateur du nouveau système sur lequel les fichiers sauvegardés sont copiés.
    - **Port** : numéro de port du système vers lequel les fichiers sont transférés.
    - **Protocole de transfert** : protocole utilisé pour effectuer le transfert du fichier de sauvegarde. Vous pouvez sélectionner les protocoles SCP, SFTP ou FTP pour transférer le fichier sauvegardé.
    - **Chemin d'accès au répertoire** : emplacement dans lequel le fichier sauvegardé est transféré sur le nouveau système.
4. Vous pouvez supprimer le fichier de sauvegarde de Citrix ADM après le transfert en cochant la case **Supprimer le fichier de Application Delivery Management après le transfert**.
5. Cliquez sur **OK** pour effectuer le transfert.



> **Remarque**
>
> Pour enregistrer une copie du fichier de sauvegarde sur votre système local, accédez à **Système > Fichiers de sauvegarde**, sélectionnez le fichier à copier, puis cliquez sur **Télécharger**.

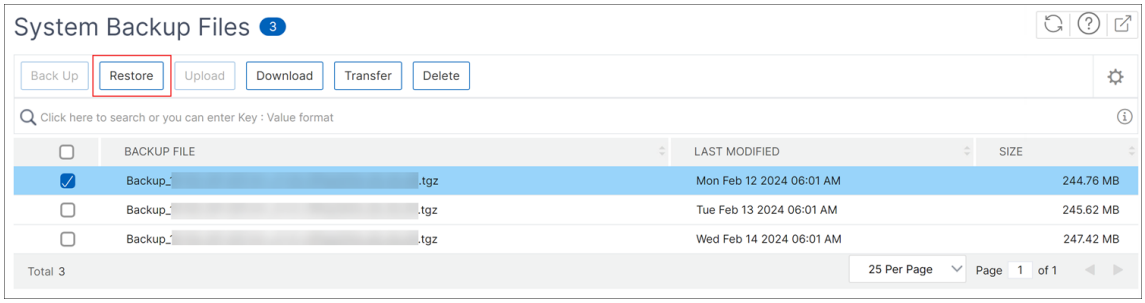
Restaurer la configuration Citrix ADM à partir d'un fichier de sauvegarde

Lorsque vous restaurez la configuration Citrix ADM à partir d'un fichier précédemment sauvegardé, l'opération de restauration efface le fichier de sauvegarde, puis restaure la configuration. L'opération de restauration supprime la configuration existante et la remplace par la configuration du fichier de sauvegarde.

> **Remarque**
>
> L'opération de restauration échoue si le fichier de sauvegarde est renommé ou si le contenu du fichier de sauvegarde est modifié.

Pour restaurer une configuration Citrix ADM à partir d'un fichier de sauvegarde :

1. Accédez à**Système > Fichiers de sauvegarde**.
2. Sélectionnez le fichier de sauvegarde à restaurer, puis cliquez sur **Restaurer**.



3. Dans la boîte de dialogue de confirmation, cliquez sur **Oui**.

> **Remarque**
>
> Pour restaurer la configuration à partir d'un fichier de sauvegarde stocké dans un système externe, téléchargez le fichier de sauvegarde sur le serveur ADM avant d'effectuer l'opération de restauration. Pour télécharger le fichier, accédez à **Système > Fichiers de sauvegarde**, puis cliquez sur **Télécharger**.

Afficher les informations d'audit

January 23, 2024

Syslog est un protocole standard de journalisation. Il comprend deux composants : le module d'audit Syslog, qui s'exécute sur l'instance Citrix Application Delivery Controller (ADC), et le serveur Syslog, qui peut s'exécuter soit sur le système d'exploitation FreeBSD sous-jacent de l'instance Citrix ADC, soit sur un système distant. SYSLOG utilise User Datagram Protocol (UDP) pour le transfert de données.

Syslog permet d'isoler le système qui génère les informations et le système qui stocke les informations. Vous pouvez consolider les informations de journalisation et obtenir des informations à partir des données collectées. Vous pouvez également configurer syslog pour consigner différents types d'événements.

Vous pouvez surveiller les messages Syslog générés par un périphérique Citrix ADC si vous configurez l'appareil pour rediriger les messages Syslog vers Citrix Application Delivery Management (ADM). Vous pouvez planifier une tâche pour créer des serveurs Syslog qui génèrent différents types de données Syslog à l'aide de la fonctionnalité de modèles intégrés de Citrix ADM.

Tout d'abord, configurez un serveur syslog vers lequel l'instance peut envoyer des informations de journal. Ensuite, spécifiez le format de date et d'heure pour l'enregistrement des messages du journal.

Pour configurer un serveur Syslog sur Citrix ADM :

1. Accédez à **Système** > **Audit**. Sous **Résumé de la configuration**, sélectionnez **Serveurs Syslog.** Vous pouvez également accéder à **Système** > **Audit > ServeursSyslog**.
2. **Sur la page**Serveur Syslog**, cliquez sur Ajouter.**
3. Dans la page **Créer un serveur Syslog**, entrez les valeurs suivantes :
    - **Nom** : nom du serveur Syslog.
    - **Adresse IP** : adresse IP du serveur Syslog.
    - **Port : port** du serveur Syslog.
4. Choisissez les niveaux de journalisation (Tous, Aucun ou Personnalisé). En conséquence, sélectionnez les niveaux de gravité.
5. Cliquez sur**Créer**.

Pour configurer le format de date et d'heure Syslog sur Citrix ADM, procédez comme suit :

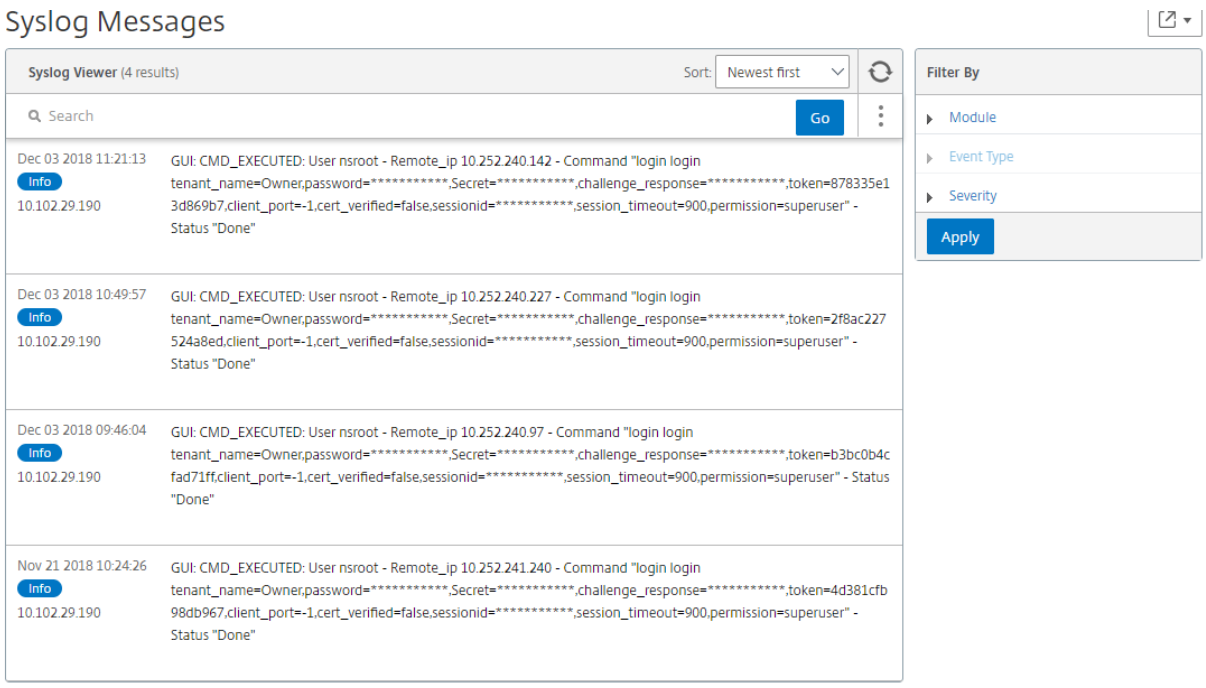
1. Accédez à **Système** > **Audit**. Dans **Résumé de la configuration**, sélectionnez **Serveurs Syslog**.
2. Dans la page **Serveur Syslog**, sélectionnez un serveur syslog, puis cliquez sur **Paramètres Syslog**.
3. Dans la page **Configurer les paramètres Syslog**, spécifiez le format de date et d'heure.
4. Cliquez sur **OK**.

Pour afficher les messages Syslog sur Citrix ADM :

Vous pouvez désormais consulter tous vos messages Syslog générés sur vos instances Citrix ADC gérées si vous avez configuré votre instance pour rediriger les messages Syslog vers le serveur Citrix ADM. Les messages Syslog sont stockés de manière centralisée dans la base de données du serveur Citrix ADM et seront disponibles sur le Syslog Viewer à des fins d'audit. Vous pouvez consolider ces informations de journalisation et dériver des rapports analytiques à partir des données collectées.

Vous pouvez filtrer ces informations par module, type d'événement et gravité. Vous pouvez également configurer syslog pour consigner différents types d'événements.

Pour afficher le **visualiseur Syslog**, accédez à **Système** > **Audit**. Sur la page **Audit**, sous **Messages d'audit**, sélectionnez **Messages Syslog**. Choisissez les filtres appropriés pour afficher les messages du journal de votre système.



Configurer les paramètres SSL

February 1, 2024

SSL (Secure Socket Layer) et TLS (Transport Layer Security) sont des protocoles de mise en réseau de sécurité couramment utilisés qui fournissent une communication chiffrée entre les utilisateurs et les serveurs. Vous pouvez configurer les paramètres SSL sur Citrix Application Delivery Management (ADM) et spécifier le type de clients qui se connectent au système.

Pour configurer les paramètres SSL pour Citrix ADM :

1. Accédez à **Système** > **Administration système**. Sous **Paramètres système**, cliquez sur **Configurer les paramètres SSL**.
2. Sur la page **Paramètres SSL**, passez en revue les paramètres de protocole actuels et les suites de chiffrement appliquées au système.
3. Pour modifier les paramètres du protocole, accédez à **Modifier les paramètres** > **Paramètres du protocole** et apportez les modifications souhaitées.
4. Pour modifier les suites de chiffrement appliquées, accédez à **Modifier les paramètres** > **Suites de chiffrement** et apportez les modifications souhaitées.
5. Cliquez sur **OK**, puis sur **Fermer**.

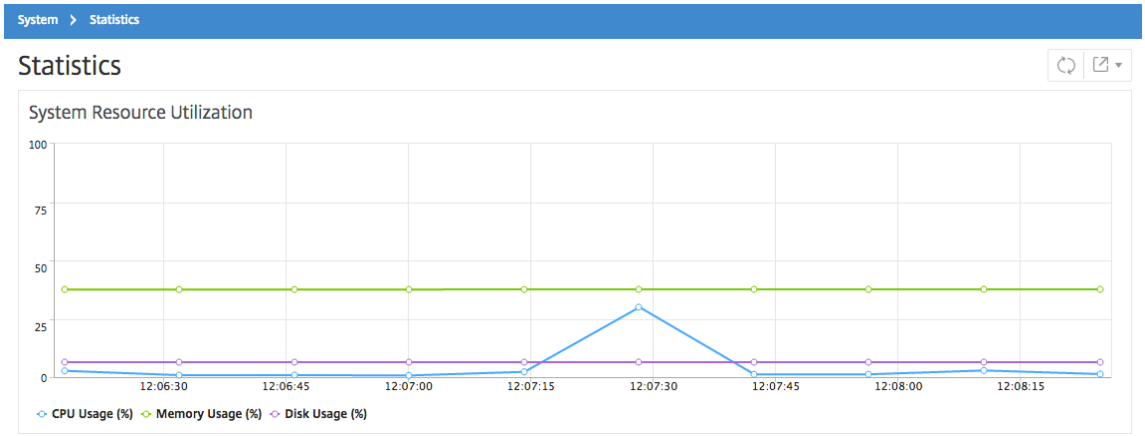
Surveiller l'utilisation du processeur, de la mémoire et du disque

January 23, 2024

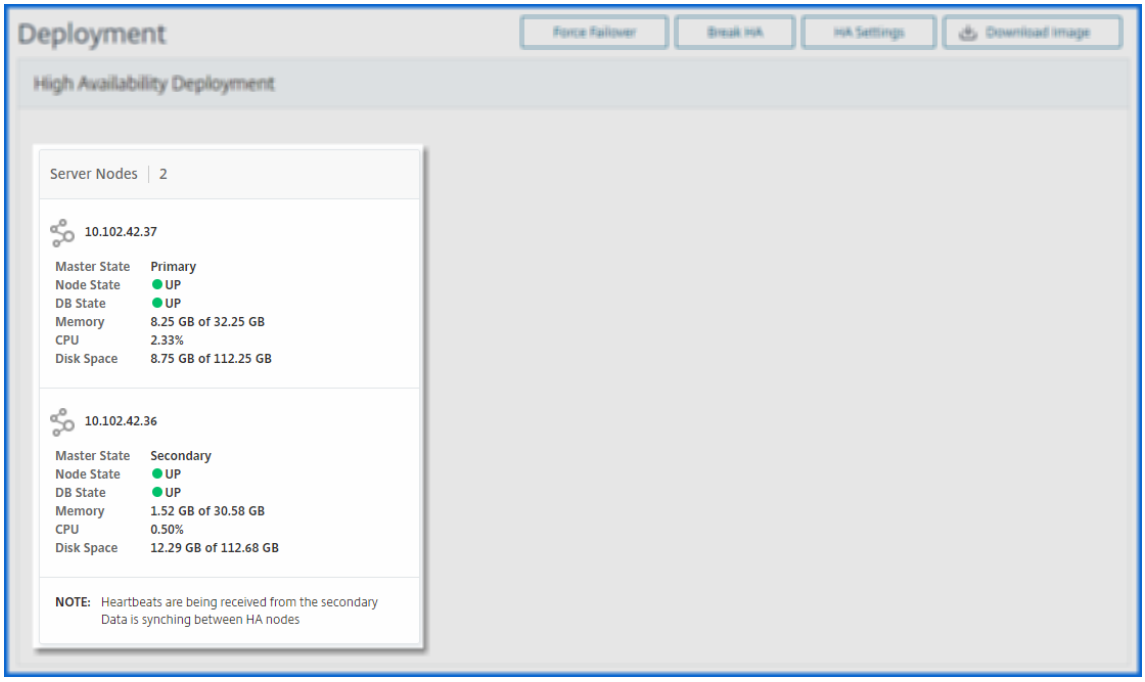
Vous pouvez utiliser les informations conservées dans les journaux et les statistiques. Ces informations sont également affichées dans des rapports qui vous aident à configurer et à gérer Citrix Application Delivery Management (ADM).

Pour surveiller l'utilisation du processeur, de la mémoire et du disque

- **Déploiement autonome.** Accédez à **Système** > **Statistiques**. Vous pouvez afficher en temps réel les graphiques d'utilisation du processeur, de la mémoire et du disque.



- **Déploiement haute disponibilité.** Accédez à **Système** > **Déploiement**. Les statistiques relatives à la mémoire, au processeur, à l'espace disque et aux instances gérées sont affichées numériquement comme illustré dans la figure suivante :



Configurer les paramètres de notification

January 23, 2024

Vous pouvez sélectionner un type de notification pour recevoir des notifications pour les fonctionnalités suivantes :

- **Événements** : liste des événements générés pour les instances Citrix ADC. Pour plus d'informations, consultez la section Ajouter des actions de règle d'événement.
- **Licences** : liste des licences actuellement actives, sur le point d'expirer, etc. Pour plus d'informations, consultez la section L'expiration de la licence Citrix ADM.
- **Certificats SSL** : liste des certificats SSL ajoutés aux instances Citrix ADC. Pour plus d'informations, consultez La date d'expiration du certificat SSL

ADM prend en charge les types de notification suivants :

- E-mail
- SMS
- Slack
- PagerDuty
- ServiceNow

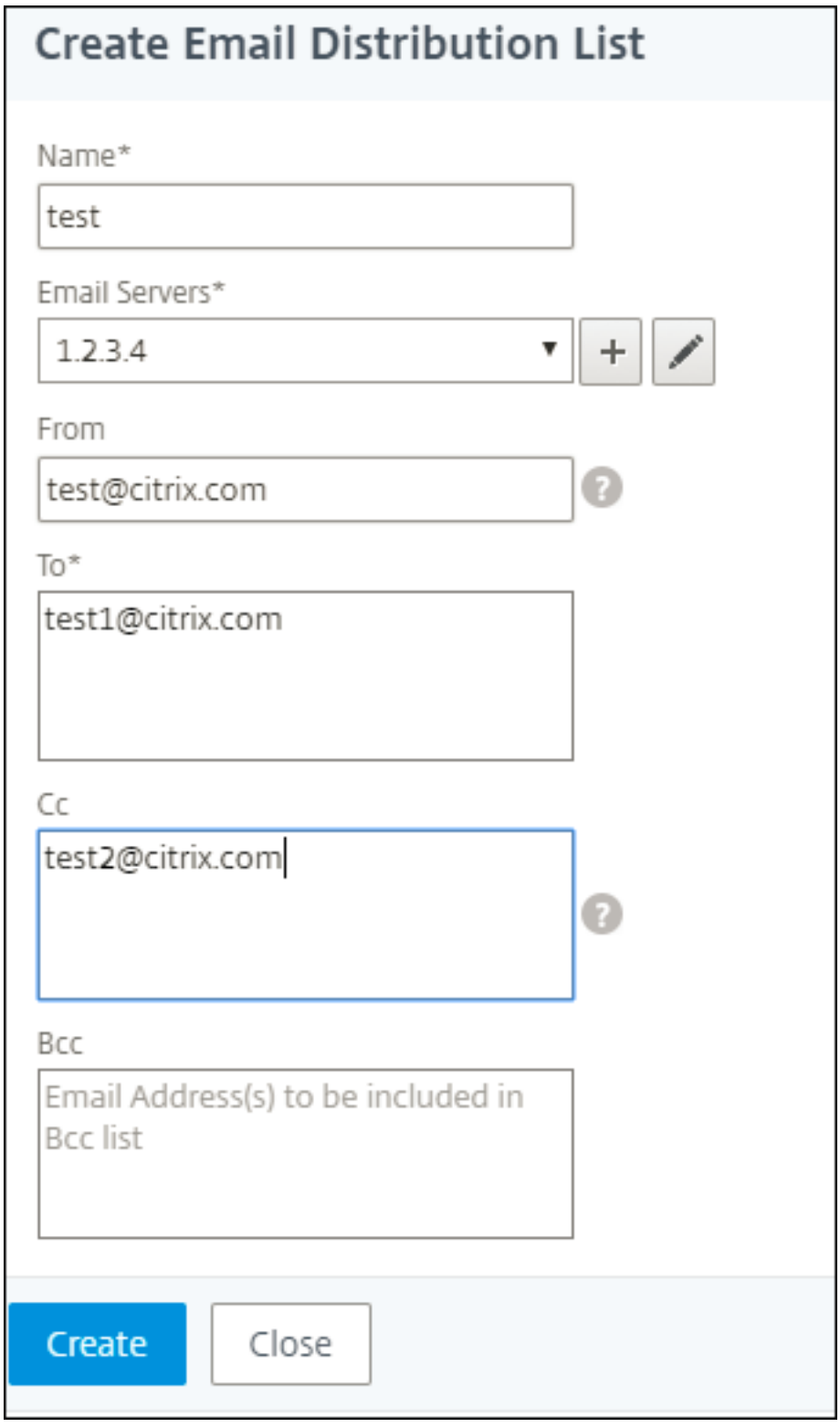
Pour chaque type de notification, l'interface graphique ADM affiche la liste ou le profil de distribution configuré. L'ADM envoie des notifications à la liste de distribution ou au profil sélectionné.

Création d'une liste de distribution par e-mail

Pour recevoir des notifications par e-mail pour les fonctions ADM, vous devez ajouter un serveur de messagerie et une liste de distribution.

Pour créer une liste de distribution d'e-mails, procédez comme suit :

1. Accédez à **Système > Notifications**.
2. Dans **E-mail**, cliquez sur **Ajouter**.
3. Dans **Créer une liste de distribution d'e-mails**, spécifiez les informations suivantes :
    - **Nom** : spécifiez le nom de la liste de distribution.
    - **Serveur de messagerie** : sélectionnez le serveur de messagerie qui envoie les notifications par e-mail. Si vous souhaitez ajouter un serveur de messagerie, cliquez sur **Ajouter**.
    - **De** : spécifiez l'adresse e-mail à partir de laquelle ADM doit envoyer des messages.
    - **À** - Spécifiez les adresses e-mail auxquelles ADM doit envoyer des messages.
    - **Cc** - Spécifiez les adresses e-mail auxquelles ADM doit envoyer les copies des messages.
    - **Bcc** - Spécifiez les adresses e-mail auxquelles ADM doit envoyer des copies de messages sans afficher les adresses.



4. Cliquez sur **Créer**.

Répétez cette procédure pour créer plusieurs listes de distribution d'e-mails. L'onglet **E-mail** affiche toutes les listes de distribution d'e-mails présentes dans ADM.

Création d'une liste de distribution de SMS

Pour recevoir des notifications par SMS pour les fonctions ADM, vous devez ajouter un serveur SMS et des numéros de téléphone.

Pour configurer les paramètres de notification SMS, procédez comme suit :

1. Accédez à **Système > Notifications**.
2. Dans **SMS**, cliquez sur **Ajouter**.
3. Dans **Créer une liste de distribution de SMS**, spécifiez les informations suivantes :
   - **Nom** : spécifiez le nom de la liste de distribution.
   - **Serveur SMS** : sélectionnez le serveur SMS qui envoie les notifications par SMS.
   - **À** : Spécifiez le numéro de téléphone auquel ADM doit envoyer des messages.
4. Cliquez sur **Créer**.

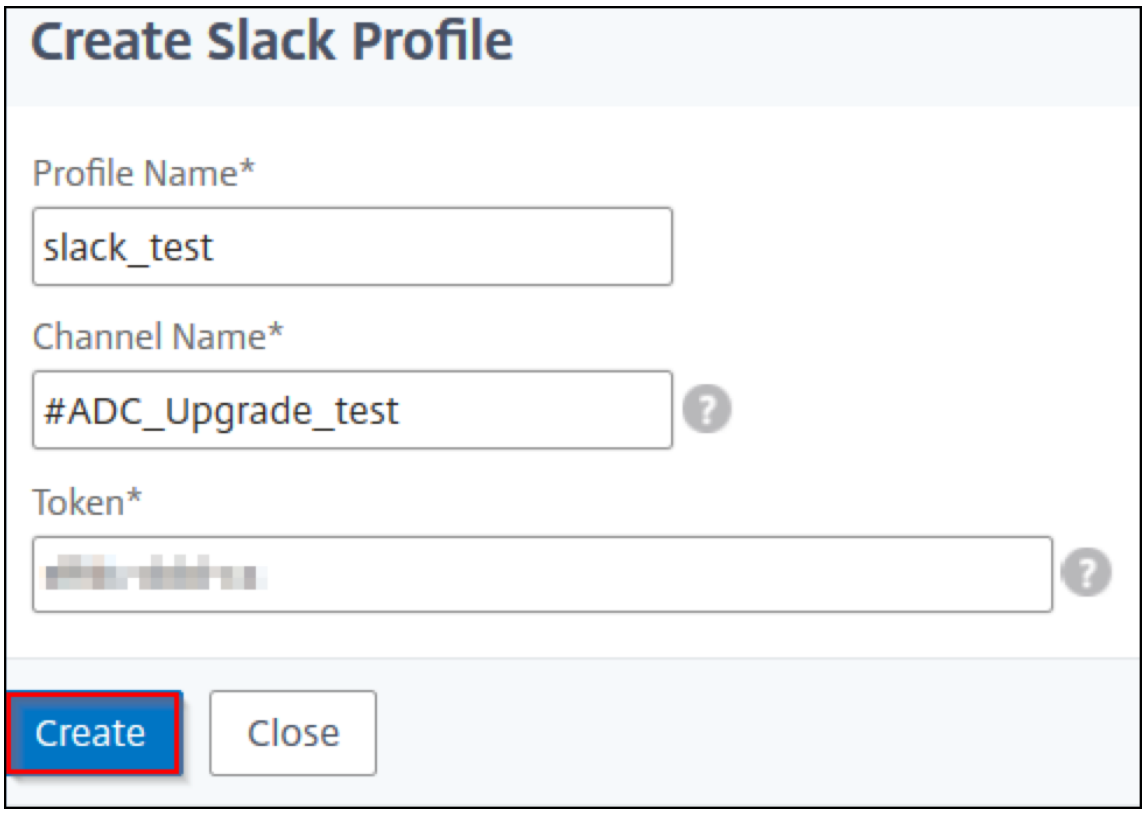
Répétez cette procédure pour créer plusieurs listes de distribution de SMS. L'onglet **SMS** affiche toutes les listes de distribution de SMS présentes dans ADM.

Créer un profil Slack

Pour recevoir des notifications Slack concernant les fonctions ADM, vous devez créer un profil Slack.

Pour créer un profil Slack, procédez comme suit :

1. Accédez à **Système > Notifications**.
2. Dans **Slack**, cliquez sur **Ajouter**.
3. Dans **Créer un profil Slack**, spécifiez les informations suivantes :
   - **Nom du profil** - Spécifiez le nom du profil. Ce nom apparaît dans la liste des profils Slack.
   - **Nom de la chaîne** : spécifiez le nom de la chaîne Slack à laquelle ADM doit envoyer des notifications.
   - **URL du webhook** : spécifiez l'URL du webhook de la chaîne. Les webhooks entrants sont un moyen simple de publier des messages provenant de sources externes dans Slack. L'URL est liée en interne au nom de la chaîne. Et, toutes les notifications d'événement sont envoyées à cette URL sont postées sur le canal Slack désigné. Voici un exemple de webhook : https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK



4. Cliquez sur **Créer**.

Répétez cette procédure pour créer plusieurs profils Slack. L'onglet **Slack** affiche tous les profils Slack présents dans ADM.

Création d'un profil PagerDuty

Vous pouvez ajouter un profil PagerDuty pour surveiller les notifications d'incidents en fonction des configurations de PagerDuty. PagerDuty vous permet de configurer les notifications par e-mail, SMS, notification push et appel téléphonique sur un numéro enregistré.

Avant d'ajouter un profil PagerDuty dans Citrix ADM, assurez-vous d'avoir terminé les configurations requises dans PagerDuty. Pour commencer à utiliser PagerDuty, consultez la documentation de PagerDuty.

Pour créer un profil PagerDuty, procédez comme suit :

1. Accédez à **Système > Notifications**.
2. Dans **PagerDuty**, cliquez sur **Ajouter**.
3. Dans **Créer un profil PagerDuty**, spécifiez les informations suivantes :
    - **Nom du profil** - Spécifiez le nom de profil de votre choix.

- **Clé d'intégration** : spécifiez la clé d'intégration. Vous pouvez obtenir cette clé sur votre portail PagerDuty.

4. Cliquez sur **Créer**.

Pour plus d'informations, consultez Services et intégrations dans la documentation PagerDuty.

Répétez cette procédure pour créer plusieurs profils PagerDuty. L'onglet **PagerDuty** affiche tous les profils PagerDuty présents dans ADM.

Afficher le profil ServiceNow

Lorsque vous souhaitez activer les notifications ServiceNow pour les événements Citrix ADC et les événements ADM, vous devez intégrer Citrix ADM avec ServiceNow à l'aide du connecteur ITSM. Pour de plus amples informations, consultez Intégrer Citrix ADM à l'instance ServiceNow.

Pour afficher et vérifier le profil ServiceNow, procédez comme suit :

1. Accédez à **Système > Notifications**.
2. Dans **ServiceNow**, sélectionnez le profil **Citrix_Workspace_SN** dans la liste.
3. Cliquez sur **Tester** pour générer automatiquement un ticket ServiceNow et vérifier la configuration.

   Si vous souhaitez afficher les tickets ServiceNow dans l'interface graphique Citrix ADM, sélectionnez **ServiceNow Tickets**.

Générer un fichier de support technique

February 1, 2024

Citrix vous recommande de générer une archive des données et des statistiques de Citrix Application Delivery Management (ADM) avant de contacter le support technique pour résoudre un problème. L'archive est un fichier TAR que vous pouvez envoyer à l'équipe de support technique.

> **Remarque**
>
> Pour les serveurs Citrix ADM en mode haute disponibilité, vous pouvez générer un fichier de support technique à partir de l'un des serveurs. Citrix vous conseille de ne pas utiliser l'adresse IP du serveur virtuel d'équilibrage de charge pour générer le fichier de support technique.

Pour configurer et envoyer un fichier de support technique depuis Citrix ADM :

1. Accédez à **Système** > **Diagnostics** > **Support technique**, puis cliquez sur **Générer un fichier de support technique**.
2. Dans la page **Générer un fichier de support**, sélectionnez les options suivantes :

- **Collecter les journaux de débogage** : sélectionnez cette option pour collecter les journaux `afdecoder`.
- **Durée** : entrez la durée pendant laquelle les journaux de débogage doivent être collectés. Cette option ne s'affiche que si vous activez l'option **Collecter les journaux de débogage**.
- **Collecter la distribution des données** : sélectionnez cette option pour collecter des journaux distincts et divers à partir de la base de données.

```
1  The archive file is created as a TAR file.
2
3  For example, the archive file that is created might be named as
      follows:   Citrix_ADM_<ADM_IP_address>_<DDMMYY>_<time_stamp>.
      tar.gz
```

1. Vous pouvez envoyer les fichiers de support technique à l'équipe de support de deux manières :

   a) Vous pouvez télécharger le fichier depuis l'interface graphique d'ADM vers votre stockage local, puis utiliser un navigateur Web pour le télécharger vers CIS.

   b) Vous pouvez également télécharger les fichiers de support technique sur le site Web Citrix Insight Services (CIS) en exécutant un script sur la console ADM.

      i. À l'aide de SSH, connectez-vous à la console ADM.

      ii. Passez à l'invite Shell et tapez :

      /mps/collector_upload.pl

La commande complète est donnée ci-dessous avec les attributs que vous devez fournir :

```
1  /mps/collector_upload.pl [-proxy [<proxy_user>:<proxy_password>@]<
      proxy_host>:<proxy_port>] [-user <user>] [-password <password>] [-sr
       <sr>] [-description <description>] [-debug] <file>
2  <!--NeedCopy-->
```

L'avantage de l'exécution du script Perl est que vous n'avez pas à télécharger le fichier de support technique d'ADM sur votre système local, puis à le télécharger sur CIS. En option, vous pouvez télécharger le fichier vers CIS directement à l'aide d'un proxy de la console ADM.

Assurez-vous d'avoir un compte sur CIS. Vous pouvez utiliser les informations d'identification de votre compte Citrix pour télécharger des fichiers vers CIS.

Et si vous n'avez pas de serveur proxy ? Ou que faire si vous rencontrez des problèmes avec les proxys de transfert SSL ? (Cela peut se produire si le script Perl ne fait pas confiance au certificat racine du

serveur proxy.)
Vous pouvez toujours télécharger le fichier directement depuis le shell ADM vers CIS.

> **Remarque**
>
> Vous pouvez toujours télécharger le fichier et l'envoyer par e-mail à l'équipe de support technique Citrix si ADM ne parvient pas à télécharger le fichier vers CIS depuis la console. Vous pouvez également télécharger le fichier depuis ADM sur votre stockage local, puis utiliser un navigateur Web pour le télécharger vers CIS.

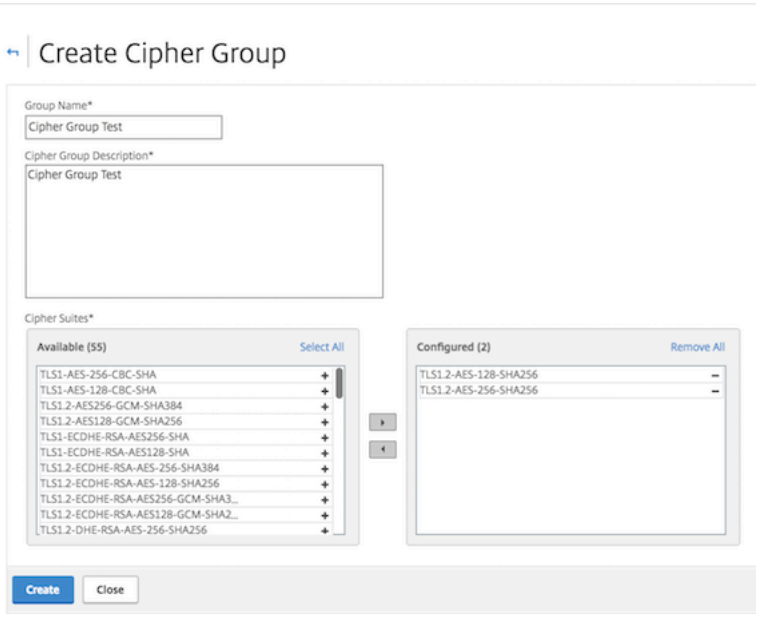
Configurer un groupe de chiffrement

January 23, 2024

Un groupe de chiffrement est un ensemble de suites de chiffrement que vous liez à un serveur virtuel, un service ou un groupe de services SSL sur l'instance ADC (Citrix Application Delivery Controller). Une suite de chiffrement comprend un protocole, un algorithme d'échange de clés (Kx), un algorithme d'authentification (Au), un algorithme de cryptage (Enc) et un algorithme de code d'authentification de message (Mac).

Pour ajouter un groupe de chiffrement sur Citrix ADM :

1. Accédez à **Système** > **Administration**
2. Sous **Paramètres SSL**, cliquez sur **Groupes de chiffrement**
3. Cliquez sur **Ajouter**.
4. Dans la page **Créer un groupe de chiffrement**, entrez les détails suivants :
    - **Nom du groupe** : nom du groupe de chiffrement.
    - **Description du groupe de chiffrement** —Fournissez une description de votre groupe de chiffrement.
    - **Suites de chiffrement** : cliquez sur Ajouter pour sélectionner les suites de chiffrement dans la liste des suites de chiffrement disponibles, puis déplacez les suites de chiffrement sélectionnées (ou toutes) vers la liste des suites de chiffrement configurées.
5. Cliquez sur **Créer**.



Créer une destination d'interruptions SNMP, une communauté de gestionnaires et des utilisateurs

February 1, 2024

Chaque fois qu'une condition anormale se produit sur Citrix ADM, une interruption SNMP est générée. Les interruptions sont ensuite envoyées à un périphérique distant appelé serveur de destination d'interruptions ou *destination d'interruptions SNMP*. Ici, Citrix ADM est configuré en tant que destination d'interruption. Vous pouvez interroger l'agent SNMP pour obtenir des informations spécifiques au système à partir d'un périphérique distant appelé *gestionnaire SNMP*. L'agent recherche ensuite les données demandées dans la base d'informations de gestion (MIB) et envoie les données au gestionnaire SNMP.

Pour créer une destination d'interruption SNMP sur Citrix ADM :

1. Accédez à **Système** > **SNMP** > **Destinations d'interruptions**.
2. Sous **Interruptions SNMP**, cliquez sur **Ajouter** pour créer une interruption SNMP, puis spécifiez les détails suivants :
    - **Version.** Sélectionnez la version SNMP à utiliser.
    - **Serveur de destination.** Nom ou adresse IP de la destination de l'interception.
    - **Port.** Entrez le port de destination du piège. Le port est défini sur 162 par défaut.

- **Communauté.** Spécifiez la chaîne communautaire à utiliser lors de l'envoi d'un trap à l'auditeur trap.

3. Cliquez sur **Créer**.

> **Remarque**
>
> Si vous créez une destination d'interruption SNMP v3, spécifiez les informations d'identification utilisateur SNMP auxquelles vous souhaitez lier l'interruption. Pour ajouter des informations d'identification utilisateur SNMP, cliquez sur **Insérer**, puis ajoutez l'utilisateur dans la liste des utilisateurs SNMP disponibles.

Pour créer une communauté de gestionnaires SNMP, procédez comme suit :

1. Accédez à **Système** > **SNMP** > **Gestionnaires**.
2. Sous **Gestionnaire SNMP**, cliquez sur **Ajouter** pour créer une communauté de gestionnaires SNMP, puis spécifiez les détails suivants :
   - **Gestionnaire SNMP.** Entrez le nom ou l'adresse IP du gestionnaire SNMP.
   - **Communauté.** Spécifiez la chaîne de communauté à utiliser lors de l'envoi d'interruptions à l'auditeur de trappes.
3. Vous pouvez éventuellement cocher la case **Activer le réseau de gestion** pour spécifier le masque de **réseau, qui est le masque**de sous-réseau du réseau du gestionnaire SNMP.
4. Cliquez sur **Créer**.

Pour créer un utilisateur SNMP, procédez comme suit :

1. Accédez à **Système** > **SNMP** > **Utilisateurs**.
2. Sous **Utilisateur SNMP**, cliquez sur **Ajouter**.
3. Entrez le nom d'utilisateur et attribuez un niveau de sécurité à l'utilisateur depuis le menu.
4. En fonction du niveau de sécurité que vous avez attribué à l'utilisateur, fournissez des protocoles d'authentification supplémentaires, tels que des protocoles d'authentification, des mots de passe de confidentialité et attribuez des vues SNMP.

Configurer et afficher les alarmes système

February 1, 2024

Vous pouvez activer et configurer un ensemble d'alarmes pour surveiller l'intégrité de vos serveurs Citrix Application Delivery Management (ADM). Vous devez configurer les alarmes système pour vous

assurer que vous êtes au courant de tout problème système critique ou majeur. Par exemple, vous pouvez être averti si l'utilisation de l'UC est élevée ou s'il y a plusieurs échecs de connexion au serveur. Pour certaines catégories d'alarmes, telles que CPUUsageHigh ou MemoryUsageHigh, vous pouvez définir des seuils et définir la gravité (critique ou majeure, par exemple) pour chacune d'entre elles. Pour certaines catégories, telles que InventoryFailed ou LoginFailure, vous ne pouvez définir que la gravité. Lorsque le seuil est enfreint pour une catégorie d'alarme (par exemple, MemoryUsageHigh) ou lorsqu'un événement se produit correspondant à la catégorie d'alarme (par exemple, **LoginFailure**), un message est enregistré dans le système et vous pouvez afficher le message sous la forme d'un message syslog. Vous pouvez également configurer les notifications pour recevoir un e-mail ou un SMS correspondant à vos paramètres d'alarme.

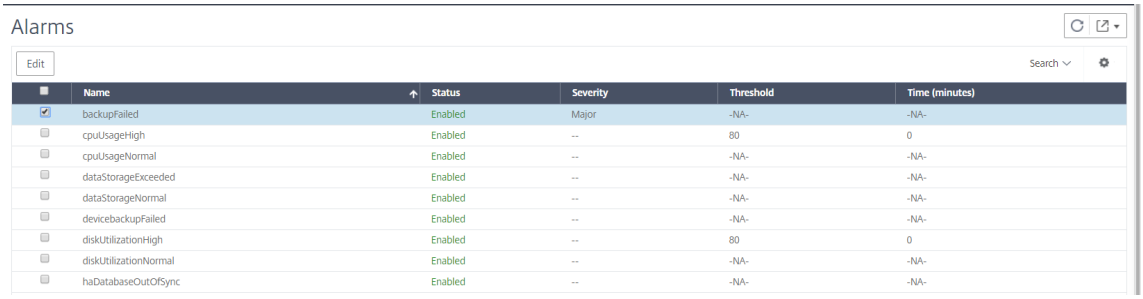
Vous pouvez attribuer ou modifier la gravité d'une alarme. Les niveaux de gravité que vous pouvez attribuer sont Critique, Majeur, Mineur, Avertissement et Informatif.

Considérez un scénario dans lequel vous souhaitez surveiller chaque fois qu'une tentative de sauvegarde a échoué. Vous pouvez activer l'alarme BackupFailed et lui attribuer une gravité, telle que Major. Chaque fois que Citrix ADM tente de sauvegarder les fichiers système et lorsque la tentative échoue, une alarme est déclenchée. Vous pouvez afficher le message sur Citrix ADM ou recevoir des notifications par e-mail ou SMS.

Pour configurer l'alarme, vous devez sélectionner l'alarme BackupFailed et spécifier le niveau de gravité Major. L'alarme est activée par défaut.

Pour configurer et afficher une alarme système à l'aide de Citrix ADM :

1. Accédez à **Système > SNMP**. Cliquez sur **Alarmes** dans le coin supérieur droit.



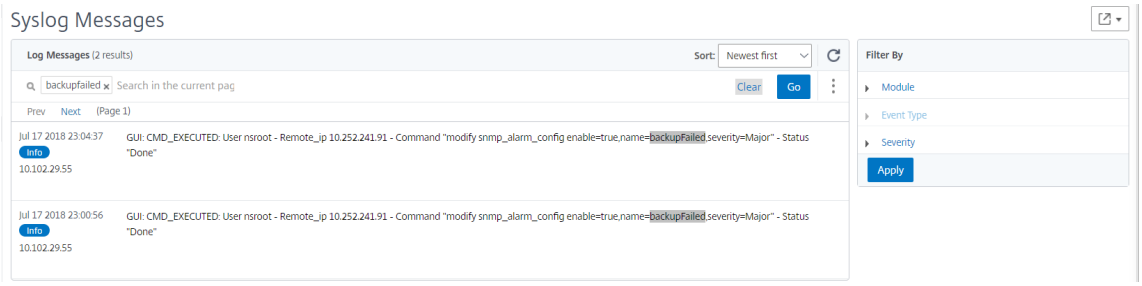
2. Sélectionnez l'alarme à configurer (par exemple, BackupFailed) et cliquez sur **Modifier** pour modifier ses paramètres.
3. L'alarme est activée par défaut. Attribuez un niveau de gravité (exemple : Majeur), puis cliquez sur **OK**.

> **Remarque**
>
> Pour certaines alarmes, vous ne pouvez pas définir de seuil.
> Lorsque l'alarme est déclenchée, vous pouvez afficher l'événement généré sous la forme d'un

> message syslog.

Pour afficher l'événement généré par l'alarme BackupFailed à l'aide de Citrix ADM :

1. Accédez à **Système** > **Audit**.
2. Dans la page **Audit**, sous **Messages d'audit**, sélectionnez **Messages Syslog**.
3. Dans le champ de recherche, saisissez le nom de l'alarme.
   Dans cet exemple, vous pouvez voir qu'un événement a été généré pour une tentative de sauvegarde ayant échoué.



   Vous pouvez également définir des notifications pour vous envoyer un e-mail ou un SMS (Short Message Service) lorsqu'une alarme est déclenchée. Pour plus d'informations sur la façon de configurer les notifications système, consultez Comment configurer les paramètres de notification système de Citrix ADM.

Citrix ADM en tant que serveur proxy API

February 1, 2024

En plus de pouvoir recevoir des demandes d'API REST NITRO pour ses propres fonctionnalités de gestion et d'analyse, Citrix Application Delivery Management (Citrix ADM) peut fonctionner en tant que serveur proxy API REST pour ses instances gérées. Au lieu d'envoyer des demandes d'API directement aux instances gérées, les clients d'API REST peuvent envoyer les demandes d'API à Citrix ADM. Citrix ADM peut faire la différence entre les demandes d'API auxquelles il doit répondre et les demandes d'API qu'il doit transférer inchangées à une instance gérée.

En tant que serveur proxy API, Citrix ADM vous offre les avantages suivants :

- **Validation des demandes d'API**. Citrix ADM valide toutes les demandes d'API par rapport aux stratégies de sécurité configurées et de contrôle d'accès basé sur les rôles (RBAC). Citrix ADM est également conscient des locataires et veille à ce que l'activité API ne dépasse pas les limites des locataires.

- **Audit centralisé**. Citrix ADM gère un journal d'audit de toutes les activités d'API liées à ses instances gérées.
- **Gestion de session**. Citrix ADM libère les clients API de la tâche consistant à gérer des sessions avec des instances gérées.

Fonctionnement de Citrix ADM en tant que serveur proxy API

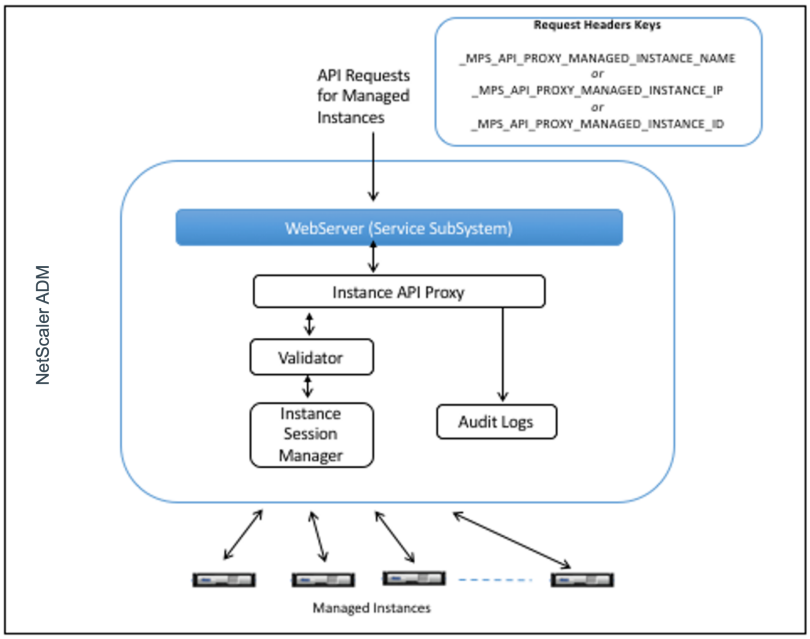
Lorsque vous souhaitez que Citrix ADM transporte une requête à une instance gérée, vous configurez le client API pour inclure l'un des en-têtes HTTP suivants dans la requête API :

Valeur d'en-tête	Description
_MPS_API_PROXY_MANAGED_INSTANCE_NAME	Nom de l'instance gérée.
_MPS_API_PROXY_MANAGED_INSTANCE_IP	Adresse IP de l'instance gérée.
_MPS_API_PROXY_MANAGED_INSTANCE_ID	ID de l'instance gérée.
_MPS_API_PROXY_TIMEOUT	Valeur du délai d'expiration pour une demande d'API NITRO. Définissez la valeur du délai d'attente en secondes. Lorsque vous définissez un délai d'expiration proxy, ADM attend la durée spécifiée avant d'expiration de la demande.
_MPS_API_PROXY_MANAGED_INSTANCE_USERNAME	Nom d'utilisateur pour accéder à l'instance ADC gérée.
_MPS_API_PROXY_MANAGED_INSTANCE_PASSWORD	Mot de passe permettant d'accéder à l'instance ADC gérée.
_MPS_API_PROXY_MANAGED_INSTANCE_SESSID	ID de session pour accéder à l'instance gérée.

> **Remarque**
>
> Dans **Système > Administration > Configurations système > Paramètres de base**, si vous sélectionnez **Demander les informations d'identification pour la connexion à l'instance**, assurez-vous de configurer le nom d'utilisateur et le mot de passe d'une instance gérée. Vous pouvez également spécifier l'ID de session d'instance.

La présence de l'un de ces en-têtes HTTP permet à Citrix ADM d'identifier une requête API comme une requête qu'elle doit transférer à une instance gérée. La valeur de l'en-tête permet à Citrix ADM d'identifier l'instance gérée vers laquelle il doit transférer la demande.

Ce flux est représenté dans la figure suivante :



Comme indiqué dans la figure ci-dessus, lorsque l'un de ces en-têtes HTTP apparaît dans une requête, Citrix ADM traite la demande comme suit :

1. Sans modifier la demande, Citrix ADM transmet la demande au moteur proxy de l'API d' instance.
2. Le moteur proxy de l'API d'instance transmet la demande d'API à un validateur et consigne les détails de la demande d'API dans le journal d'audit.
3. Le validateur s'assure que la demande ne viole pas les stratégies de sécurité configurées, les stratégies RBAC, les limites de location, etc. Il effectue des vérifications supplémentaires, telles qu'une vérification pour déterminer si l'instance gérée est disponible.

Si la demande d'API est valide et peut être transférée à l'instance gérée, Citrix ADM identifie une session qui est gérée par le Gestionnaire de session d'instance, puis envoie la demande à l'instance gérée.

> **Remarque**
>
> Assurez-vous que l'option **Invite les informations d'identification pour la connexion d'instance** est désactivée. Pour ce faire :
>
> 1. Accédez à **Système > Administration**.
> 2. Dans **Configurations système**, sélectionnez **Système, Fuseau horaire, URL autorisées et Message du jour**.

Comment utiliser Citrix ADM en tant que serveur proxy API

Les exemples suivants montrent les demandes d'API REST qu'un client API envoie à un serveur Citrix ADM dont l'adresse IP est 192.0.2.5. Citrix ADM est requis pour transférer les demandes, inchangées, vers une instance gérée avec l'adresse IP 192.0.2.10. Tous les exemples utilisent l'en-tête _MPS_API_PROXY_MANAGED_INSTANCE_IP.

Avant d'envoyer les demandes d'API Citrix ADM, le client API doit :

- Connectez-vous à Citrix ADM
- Obtenir un ID de session
- Incluez l'ID de session dans les demandes d'API suivantes.

La demande d'API d'ouverture de session est de la forme suivante :

```
    POST /nitro/v1/config/login
    Content-Type: application/json

    {

        "login": {

            "username":"nsroot",
            "password":"nsroot"
          }

     }

<!--NeedCopy-->
```

Citrix ADM répond à la demande d'ouverture de session avec une réponse qui inclut l'ID de session. L'exemple de corps de réponse suivant affiche un ID de session :

```
{


  "errorcode": 0,

  "message": "Done",

  "operation": "add",

  "resourceType": "login",

  "username": "***********",

  "tenant_name": "Owner",

  "resourceName": "nsroot",

  "login": [
```



```
19
20      {
21
22
23        "tenant_name": "Owner",
24
25        "permission": "superuser",
26
27        "session_timeout": "36000",
28
29        "challenge_token": "",
30
31        "username": "",
32
33        "login_type": "",
34
35        "challenge": "",
36
37        "client_ip": "",
38
39        "client_port": "-1",
40
41        "cert_verified": "false",
42
43        "sessionid": "##
       D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D",
44
45        "token": "b2f3f935e93db6a"
46       }
47
48
49    ]
50
51   }
52
53  <!--NeedCopy-->
```

Exemple 1 : Récupérer des statistiques de serveur virtuel d'équilibrage de charge

Le client doit envoyer à Citrix ADM une demande d'API du formulaire suivant :

```
1      GET /nitro/v1/stat/lbvserver
2      Content-type: application/json
3      _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
4      SESSID: ##
          D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
5   <!--NeedCopy-->
```

Où la valeur de l'en-tête de cookie est l'ID de session renvoyé par l'appel d'API de connexion. Et la valeur de _MPS_API_PROXY_MANAGED_INSTANCE_IP est l'adresse IP de l'ADC.

Exemple 2 : Créer un serveur virtuel d'équilibrage de charge

Le client doit envoyer à Citrix ADM une demande d'API du formulaire suivant :

```
1     POST /nitro/v1/config/lbvserver/sample_lbvserver
2     Content-type: application/json
3     Accept-type: application/json
4     _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
5     SESSID: ##
          D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
6
7     {
8
9          "lbvserver":{
10
11             "name":"sample_lbvserver",
12             "servicetype":"HTTP",
13             "ipv46":"10.102.1.11",
14             "port":"80"
15          }
16
17      }
18
19 <!--NeedCopy-->
```

Exemple 3 : Modifier un serveur virtuel d'équilibrage de charge

Le client doit envoyer à Citrix ADM une demande d'API du formulaire suivant :

```
1     PUT /nitro/v1/config/lbvserver
2     Content-type: application/json
3     Accept-type: application/json
4     _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
5     SESSID: ##
          D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
6
7     {
8
9        "lbvserver":{
10
11            "name":"sample_lbvserver",
12            "appflowlog":"DISABLED"
13         }
14
15      }
16
17 <!--NeedCopy-->
```


Exemple 4 : Suppression d'un serveur virtuel d'équilibrage de charge

Le client doit envoyer à Citrix ADM une demande d'API du formulaire suivant :

```
1     DELETE /nitro/v1/config/lbvserver/sample_lbvserver
2     Accept-type: application/json
3     _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
4     SESSID: ##
         D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
5
6  <!--NeedCopy-->
```

Exemple 5 : Télécharger l'interface de ligne de commande exécutant la configuration sur l'ADC

Le client doit envoyer à Citrix ADM une demande d'API du formulaire suivant :

```
1     GET /nitro/v1/config/nsrunningconfig
2     Accept-type: application/json
3     _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
4     SESSID: ##
         D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
5
6  <!--NeedCopy-->
```

Visualiser les problèmes à l'aide d'Infrastructure Analytics

February 1, 2024

L'un des principaux objectifs des administrateurs réseau est de surveiller les instances Citrix ADC. Les instances ADC offrent des informations intéressantes sur l'utilisation et les performances des applications et des postes de travail auxquels elles accèdent. Les administrateurs doivent surveiller l'instance ADC et analyser les flux d'application traités par chaque instance ADC. Ils peuvent résoudre tous les problèmes probables de configuration, d'installation, de connectivité, de certificats et autres qui pourraient avoir un impact sur l'utilisation ou les performances de l'application. Par exemple, un changement soudain dans le modèle de trafic de l'application peut être dû à un changement de configuration SSL comme la désactivation d'un protocole SSL. Les administrateurs doivent être en mesure d'identifier rapidement la corrélation entre ces points de données afin de garantir les éléments suivants :

- La disponibilité des applications est optimale
- Il n'y a aucun problème de consommation de ressources, de matériel, de capacité ou de modification de configuration

- Il n'y a aucun inventaire inutilisé
- Il n'y a pas de certificats expirés

La fonction Infrastructure Analytics simplifie le processus d'analyse des données en corrélant plusieurs sources de données et en les quantifiant en un score mesurable qui définit l'état de santé d'une instance. Grâce à cette fonctionnalité, les administrateurs disposent d'un point de contact unique qui leur permet de savoir s'il existe un problème, d'en déterminer l'origine et d'effectuer les corrections probables.

Analyse de l'infrastructure

La fonctionnalité d'analyse de l'infrastructure de Citrix Application Delivery Management (ADM) rassemble toutes les données collectées à partir des instances de Citrix ADC et les quantifie dans un **score d'instance** qui définit l'intégrité des instances. Le score d'instance est résumé sur une vue tabulaire ou sous forme de visualisation de cercle. La fonctionnalité Analytics d'infrastructure vous aide à visualiser les facteurs qui ont entraîné ou peuvent entraîner un problème sur les instances. Cette visualisation vous aide également à déterminer les actions à effectuer pour éviter que le problème ne se reproduise.

Score d'instance

Le score d'une instance indique l'état de santé d'une instance ADC. Un score de 100 signifie une instance parfaitement saine et sans aucun problème. Le score de l'instance capture les différents niveaux de problèmes potentiels sur l'instance. Il s'agit d'une mesure quantifiable de la santé de l'instance et de multiples « indicateurs de santé » contribuent au score.

Les**indicateurs de santé** sont les éléments de base du score de l'instance, où le score est calculé périodiquement pendant une « période de surveillance » prédéfinie, sur la base de tous les indicateurs détectés dans cette fenêtre temporelle. Actuellement, Infrastructure Analytics calcule le score de l'instance une fois par heure sur la base des données collectées auprès des instances.
Un indicateur peut être défini comme toute activité (un événement ou un problème) appartenant à l'une des catégories suivantes sur les instances.

- Indicateurs de ressources système
- Indicateurs d'événements critiques
- Indicateurs de configuration SSL
- Indicateurs d'écart de configuration

Indicateurs de santé

- Indicateurs des ressources du système

  Vous trouverez ci-dessous les problèmes critiques de ressources système qui peuvent survenir sur les instances Citrix ADC et surveillés par Citrix ADM.

  - Utilisation**élevée du processeur**. L'utilisation du processeur a dépassé le seuil supérieur dans l'instance Citrix ADC.
  - **Utilisation élevée de la mémoire**. L'utilisation de la mémoire a dépassé le seuil supérieur dans l'instance Citrix ADC.
  - **Utilisation élevée du disque**. L'utilisation du disque a dépassé le seuil supérieur dans l'instance Citrix ADC.
  - **Erreurs de disque**. Des erreurs se produisent sur le disque dur 0 ou le disque dur 1 de l'hyperviseur sur lequel l'instance ADC est installée.
  - **Panne de courant**. L'alimentation est tombée en panne ou s'est déconnectée de l'instance ADC.
  - **Échec de la carte SSL**. La carte SSL installée sur l'instance est défectueuse.
  - **Erreurs de flash**. Des erreurs Compact Flash sont détectées sur l'instance Citrix ADC.
  - **Rejets NIC**. Les paquets ignorés par la carte NIC ont franchi la valeur de seuil supérieure dans l'instance de Citrix ADC.

Pour plus d'informations sur ces erreurs de ressources système, consultez Le tableau de bord de l'instance.

- Indicateurs d'événements critiques

  Les événements critiques suivants sont identifiés par les événements relevant de la fonction de gestion des événements d'ADM qui sont configurés avec une gravité critique.

  - **Échec de synchronisation HA**. La synchronisation de la configuration entre les instances ADC en haute disponibilité a échoué sur le serveur secondaire.
  - **HA pas de battements**de cœur. Le serveur principal d'une paire d'instances ADC en haute disponibilité ne reçoit pas les battements cardiaques du serveur secondaire.
  - **Son état secondaire est mauvais**. Le serveur secondaire d'une paire d'instances ADC en haute disponibilité est dans l'état secondaire Inactif, Inconnu ou Stay.
  - **Incompatibilité de version HA**. La version des images du logiciel ADC installées sur une paire d'instances ADC en haute disponibilité ne correspond pas.

- **Échec de synchronisation du cluster**. La synchronisation de la configuration entre les instances ADC en mode cluster a échoué.
- **Incompatibilité entre les versions du cluster**. La version des images du logiciel ADC installées sur les instances ADC en mode cluster ne correspond pas.
- **Échec de propagation du cluster**. La propagation des configurations vers toutes les instances d'un cluster a échoué.

> **Remarque**
>
> Vous pouvez disposer de votre liste d'événements SNMP critiques en modifiant les niveaux de gravité des événements. Pour plus d'informations sur la façon de modifier les niveaux de gravité, consultez Modifier la gravité signalée des événements qui se produisent sur les instances Citrix ADC.

Pour plus d'informations sur les événements dans Citrix ADM, consultez la section Événements.

- Indicateurs de configuration SSL
  - **Force de touche non recommandée**. La principale force des certificats SSL n'est pas conforme aux normes Citrix
  - **Emetteur non recommandé**. L'émetteur du certificat SSL n'est pas recommandé par Citrix.
  - **Les certificats SSL ont expiré**. Le certificat SSL installé dans l'instance ADC a expiré.
  - **Expiration des certificats SSL arrivée à échéance**. Le certificat SSL installé dans l'instance ADC est sur le point d'expirer dans la semaine qui vient.
  - **Algorithmes non recommandés**. Les algorithmes de signature des certificats SSL installés dans l'instance ADC ne sont pas conformes aux normes Citrix.

Pour plus d'informations sur les certificats SSL, consultez Tableau de bord SSL.

- Indicateurs d'écart de configuration
  - **Modèle de dérive de configuration**. Il existe une dérive (modifications non enregistrées) dans la configuration par rapport aux modèles d'audit que vous avez créés avec des configurations spécifiques que vous souhaitez auditer sur certaines instances.
  - **Config Drift par défaut**. Il y a une dérive (modifications non enregistrées) dans la configuration à partir des fichiers de configuration par défaut.

Pour plus d'informations sur les écarts de configuration et sur la façon d'exécuter des rapports d'audit pour vérifier les écarts de configuration, voir Afficher les rapports d'audit .

Voir les problèmes de capacité ADC

Lorsqu'une instance ADC a consommé la plus grande partie de sa capacité disponible, la suppression de paquets peut se produire lors du traitement du trafic client. Ce problème provoque de faibles performances dans une instance ADC. En comprenant ces problèmes de capacité de l'ADC, vous pouvez attribuer des licences supplémentaires de manière proactive afin de stabiliser les performances de l'ADC.

Pour afficher les problèmes de capacité de l'ADC,

1. Accédez à **Réseaux > Analyse de l'infrastructure**.
2. Développez l'instance pour laquelle vous souhaitez afficher les problèmes de capacité.

L'ADM interroge ces événements toutes les cinq minutes à partir de l'instance ADC et affiche les baisses de paquets ou les incréments de compteur de limite de vitesse s'il existe. Les problèmes sont classés selon les paramètres de capacité suivants :

- **Limite de débit atteinte** : nombre de paquets abandonnés dans l'instance une fois la limite de débit atteinte.
- **Limite de processeur PE atteinte** : nombre de paquets déposés sur toutes les cartes réseau une fois que la limite du processeur PE est atteinte.
- **Limite PPS atteinte** : nombre de paquets abandonnés dans l'instance une fois la limite PPS atteinte.
- **Limite de débit SSL** : nombre de fois que la limite de débit SSL est atteinte.
- **Limite de débit SSL TPS** : nombre de fois que la limite SSL TPS est atteinte.

L'ADM calcule le score de l'instance sur le seuil de capacité défini.

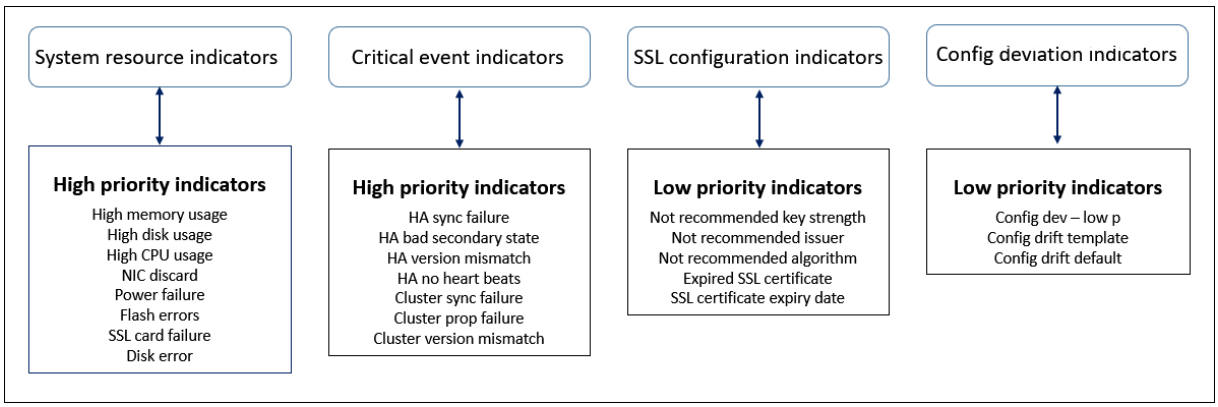
- Seuil bas —Incrément de compteur de perte ou de limite de débit de 1 paquet
- Seuil élevé : 10000 paquets baisse ou incrément du compteur de limite de taux

Par conséquent, lorsqu'une instance ADC dépasse le seuil de capacité, le score de l'instance est affecté.

Lorsque des paquets tombent ou que le compteur de limite de débit augmente, un événement est généré dans `ADCCapacityBreach` cette catégorie. Pour afficher ces événements, accédez à **Comptes > Événements système**.

Valeur des indicateurs de santé

Les indicateurs sont classés en indicateurs hautement prioritaires et en indicateurs de faible priorité sur la base de leurs valeurs, comme suit :



Les indicateurs de santé d'un même groupe d'indicateurs ont des poids différents qui leur sont attribués. Un indicateur peut contribuer davantage à la baisse du score d'instance qu'un autre indicateur. Par exemple, une utilisation élevée de la mémoire fait baisser le score de l'instance davantage qu'une utilisation élevée du disque, une utilisation élevée du processeur et la suppression de la carte réseau. Si un plus grand nombre d'indicateurs sont détectés sur une instance, le score de l'instance est faible.

La valeur d'un indicateur est calculée selon les règles suivantes. On dit que l'indicateur est détecté de l'une des trois manières suivantes :

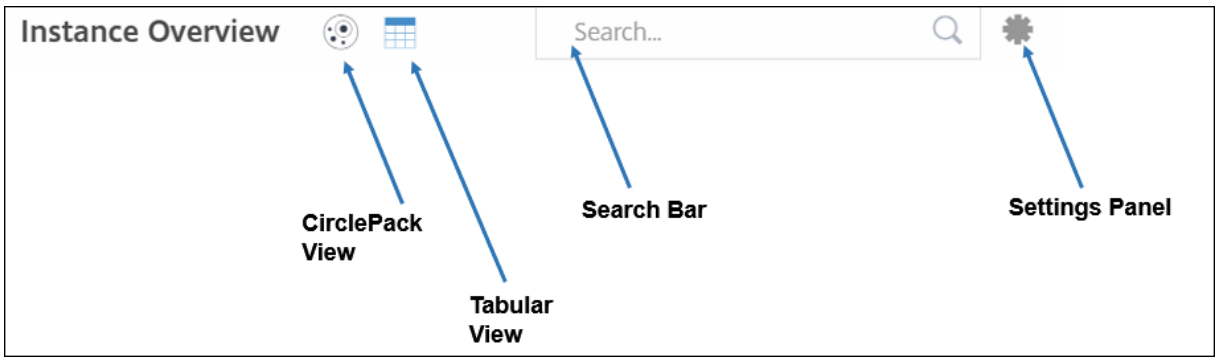
1. **Sur la base d'une activité**. Par exemple, un indicateur de ressources système est déclenché en cas de panne de courant sur l'instance, et cet indicateur réduit la valeur du score de l'instance. Lorsque l'indicateur est effacé, la pénalité est effacée et le score de l'instance augmente.
2. **Sur la base de la violation de la valeur seuil**. Par exemple, un indicateur de ressources système est déclenché lorsque la carte NIC rejette des paquets et que le seuil est dépassé.
3. **Sur la base de la violation du seuil bas et du seuil supérieur**. Ici, un indicateur peut être déclenché de deux manières :
    - Lorsque la valeur de l'indicateur se situe entre des seuils bas et haut, auquel cas une pénalité partielle est appliquée au score de l'instance.
    - Lorsque la valeur dépasse le seuil supérieur, auquel cas une pénalité complète est appliquée au score de l'instance.
    - Aucune pénalité n'est appliquée au score de l'instance si la valeur tombe en dessous d'un seuil bas.

Par exemple, l'utilisation du processeur est un indicateur de ressources système déclenché lorsque la valeur d'utilisation franchit le seuil bas et également lorsque la valeur franchit le seuil supérieur.

Tableau de bord de l'analyse de l'infrastructure

Accédez à **Réseaux** > **Analyse de l'infrastructure** .

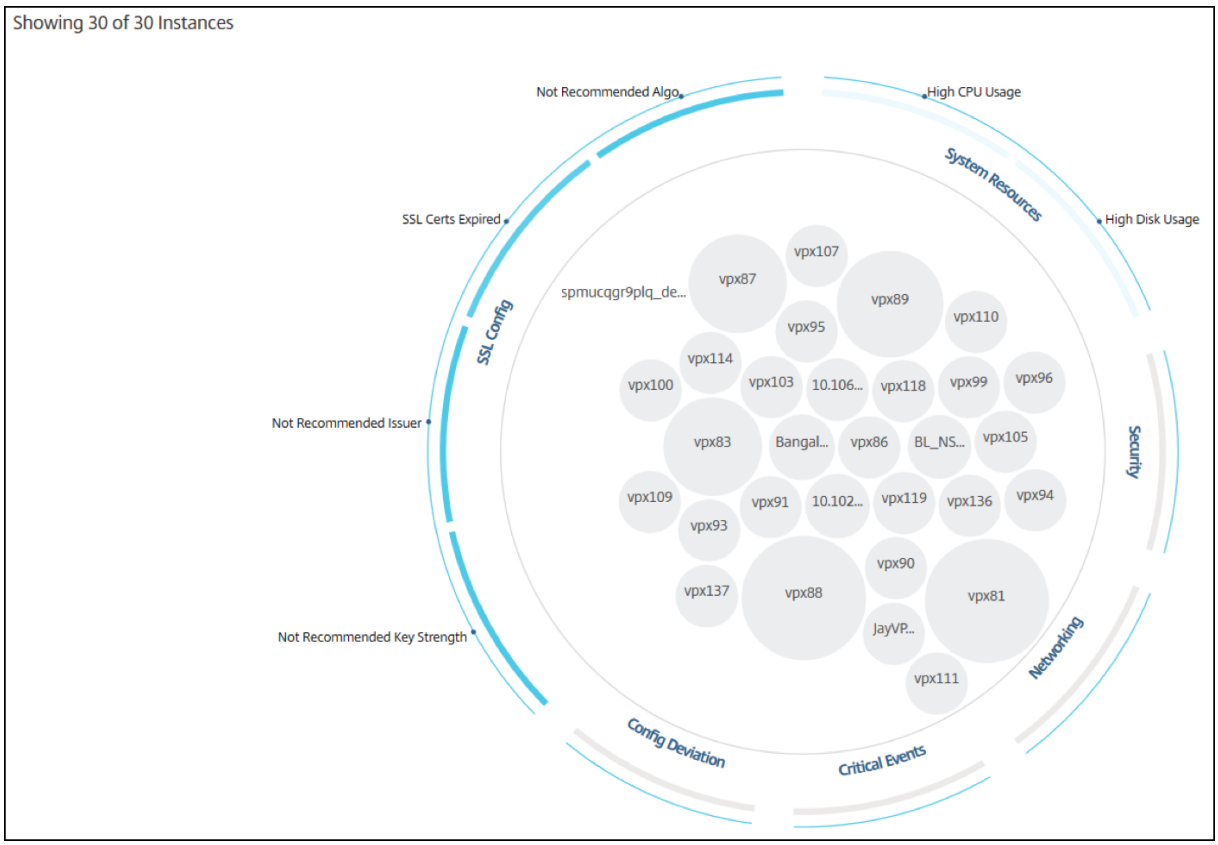
L'analyse de l'infrastructure peut être affichée au format **Circle Pack** ou **Tabulaire** . Vous pouvez basculer entre les deux formats.



- Dans la vue tabulaire, vous pouvez rechercher une instance en tapant le nom d'hôte ou l'adresse IP dans la barre de recherche.
- Par défaut, la page Infrastructure Analytics affiche le panneau de synthèse sur le côté droit de la page.
- Cliquez sur l'icône **Paramètres** pour afficher le panneau des **paramètres** .
- Dans les deux formats d'affichage, le panneau de synthèse affiche les détails de toutes les instances de votre réseau.

Vue du pack de cercle

Les diagrammes de regroupement de cercles présentent les groupes d'instances sous la forme de cercles Ils présentent souvent des hiérarchies dans lesquelles les petits groupes d'instances sont soit colorés de la même manière que les autres groupes de la même catégorie, soit imbriqués dans des groupes plus importants. Les packs de cercles représentent des ensembles de données hiérarchiques et montrent différents niveaux de la hiérarchie et comment ils interagissent les uns avec les autres.



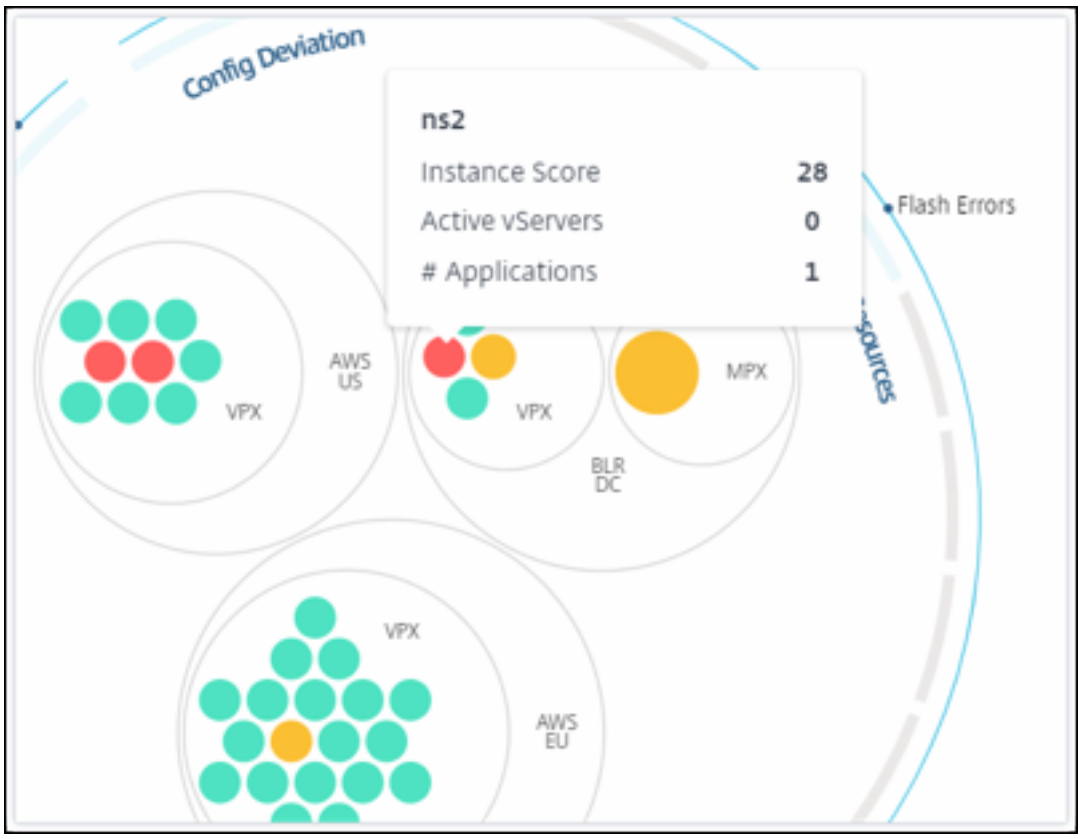
Cercles d'instance

Couleur Chaque instance est représentée dans Circle Pack sous la forme d'un cercle coloré. La couleur du cercle indique l'état de santé de cette instance.

- **Vert** : le score de l'instance est compris entre 100 et 80. L'instance est saine.
- **Jaune** : le score de l'instance se situe entre 80 et 50 ; certains problèmes ont été remarqués et doivent être revus.
- **Rouge** : le score de l'instance est inférieur à 50. L'instance est dans une phase critique car plusieurs problèmes ont été détectés sur cette instance.

taille. La taille de ces cercles colorés indique le nombre de serveurs virtuels configurés sur cette instance. Un cercle plus grand indique qu'il existe un plus grand nombre de serveurs virtuels.

Vous pouvez placer le pointeur de la souris sur chacun des cercles d'instance (cercles colorés) pour afficher un résumé. L'infobulle de survol affiche le nom d'hôte de l'instance, le nombre de serveurs virtuels actifs et le nombre d'applications configurées sur cette instance.

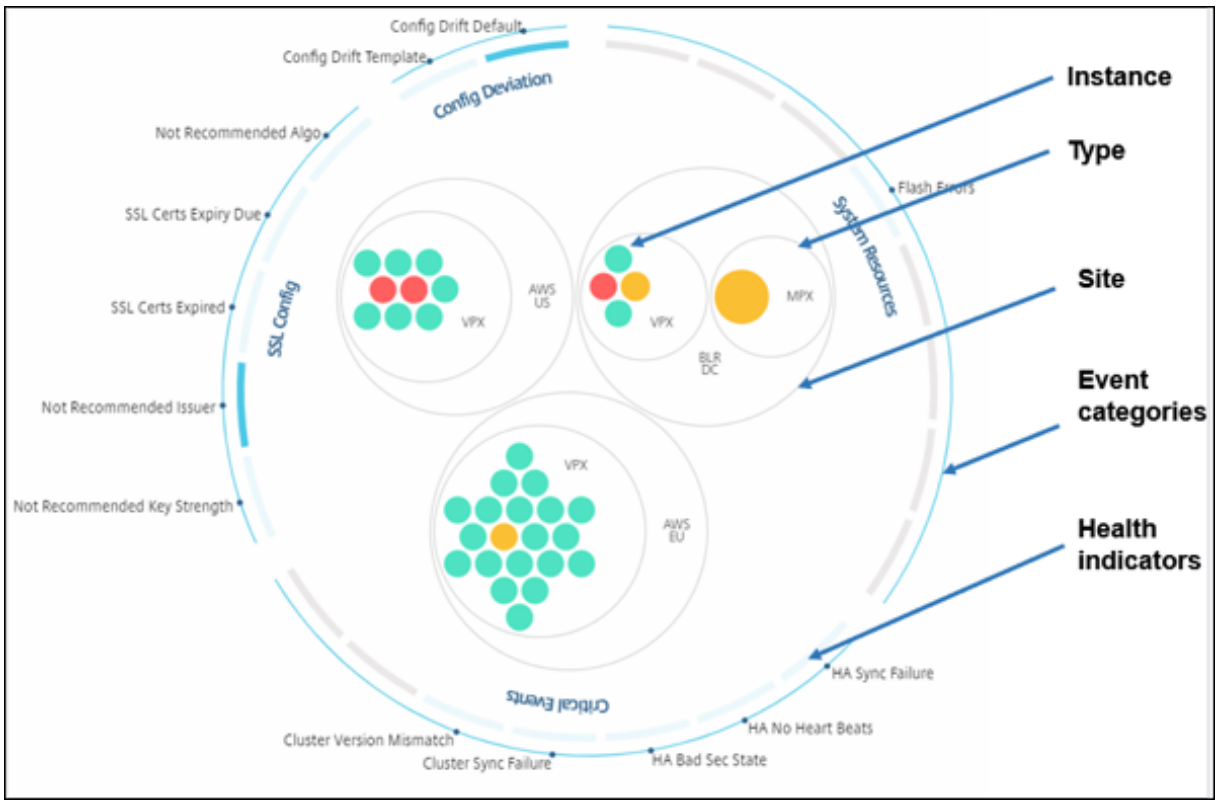


Cercles d'instance groupés

Au départ, le Circle Pack comprend des cercles d'instance qui sont regroupés, imbriqués ou regroupés dans un autre cercle en fonction des critères suivants :

- le site où ils sont déployés
- le type d'instances déployées : VPX, MPX, SDX et CPX
- le modèle virtuel ou physique de l'instance ADC
- la version de l'image ADC installée sur les instances

L'image suivante montre un Circle Pack où les instances sont d'abord regroupées par site ou centre de données où elles sont déployées, puis regroupées en fonction de leur type, VPX et MPX.

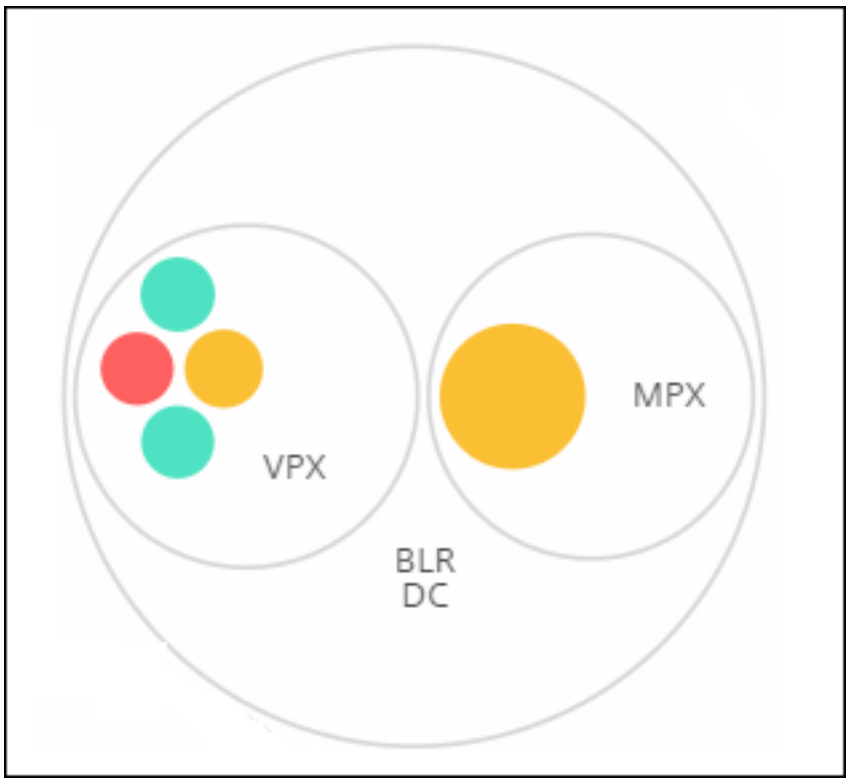


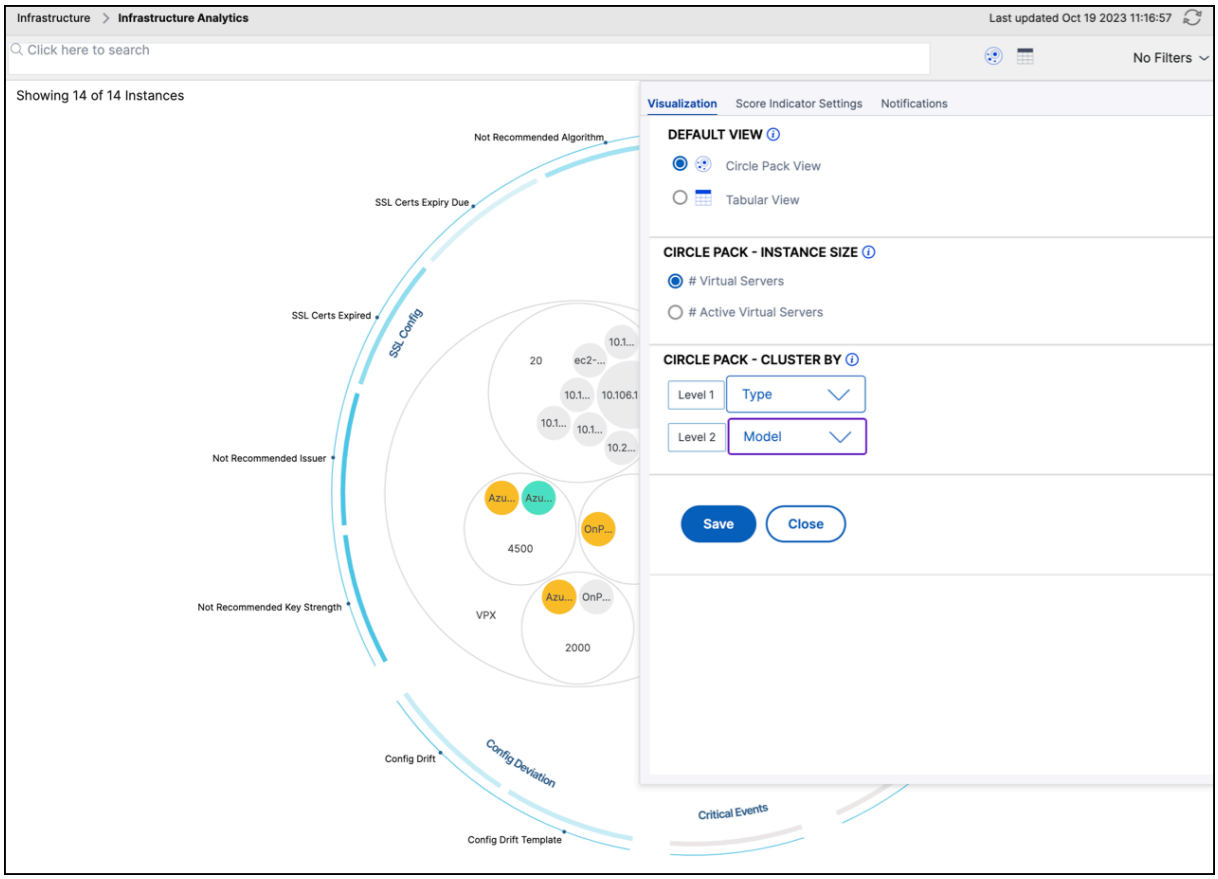
Tous ces cercles imbriqués sont délimités par deux cercles extérieurs. Les deux cercles extérieurs représentent les quatre catégories d'événements surveillés par Citrix ADM (ressources système, événements critiques, configuration SSL et écart de configuration) et les indicateurs de santé correspondants.

Cercles d'instance en cluster

Citrix ADM surveille de nombreuses instances. Pour faciliter la surveillance et la maintenance de ces instances, Infrastructure Analytics vous permet de les regrouper à deux niveaux. En d'autres termes, les groupes d'instances peuvent être imbriqués dans un autre groupe.

Par exemple, le centre de données BLR dispose de deux types d'instances ADC : VPX et MPX, qui y sont déployées. Vous pouvez d'abord regrouper les instances ADC en fonction de leur type, puis toutes les instances en fonction du site où elles sont regroupées. Vous pouvez désormais identifier facilement le nombre de types d'instances déployés sur les sites que vous gérez.

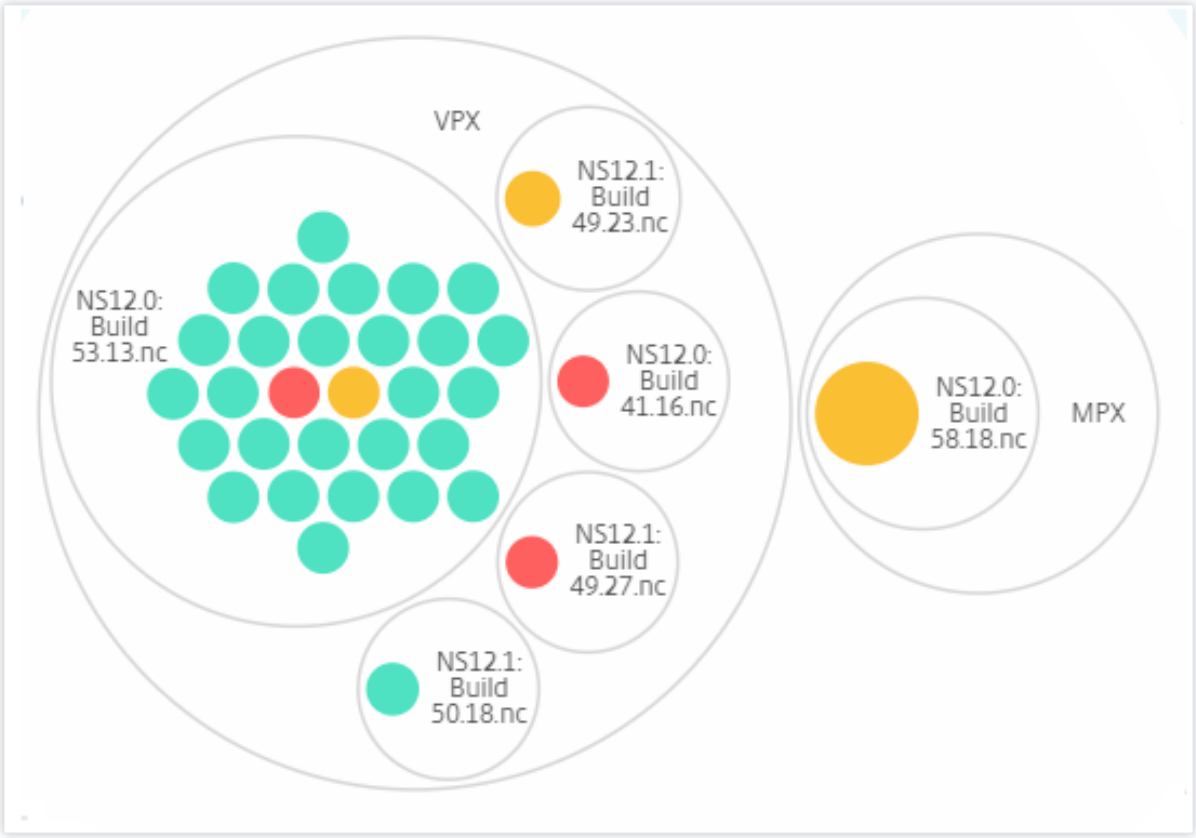




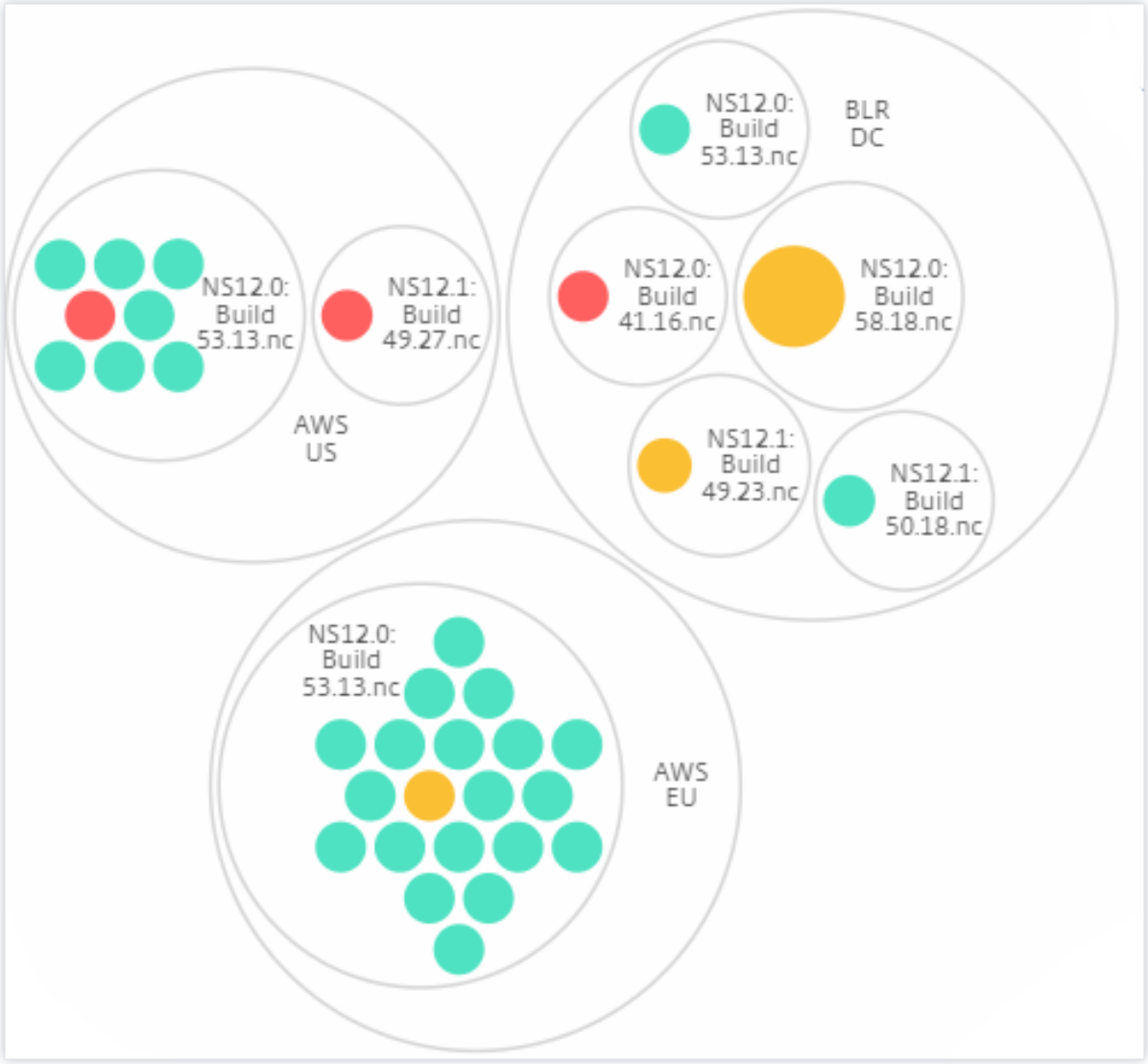
Quelques autres exemples de regroupement à deux niveaux sont les suivants :

Site et modèle :

Type et version :

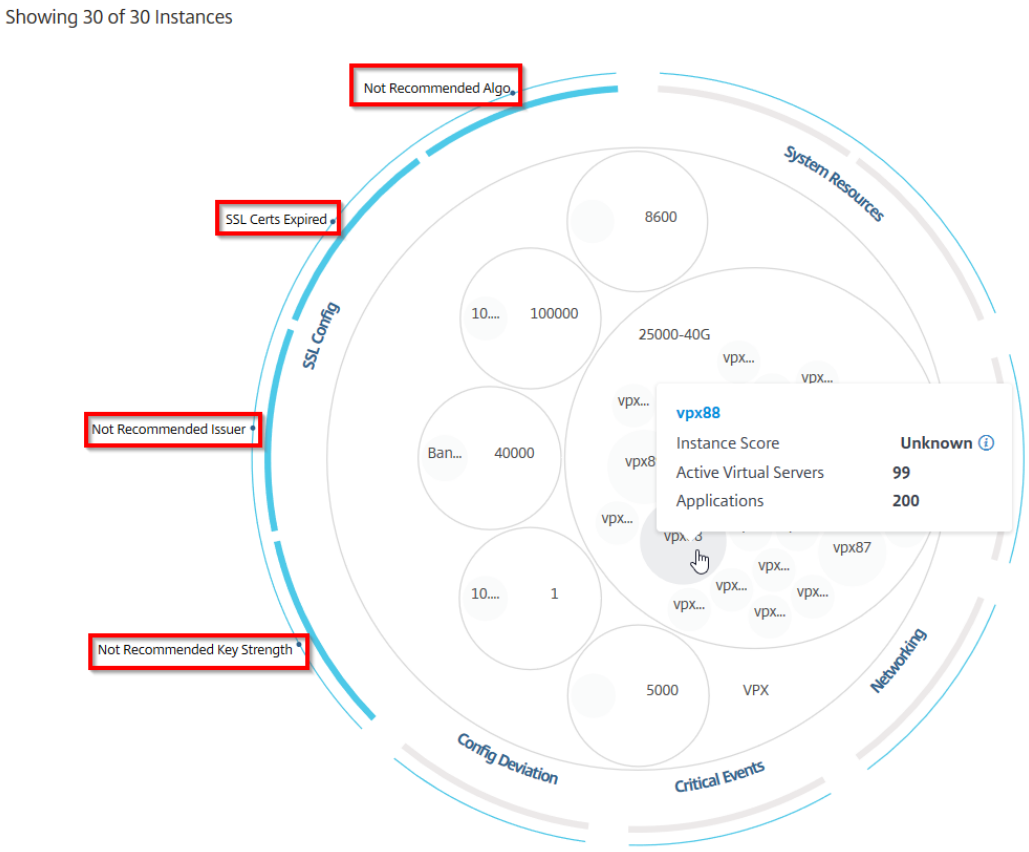


Site et version :

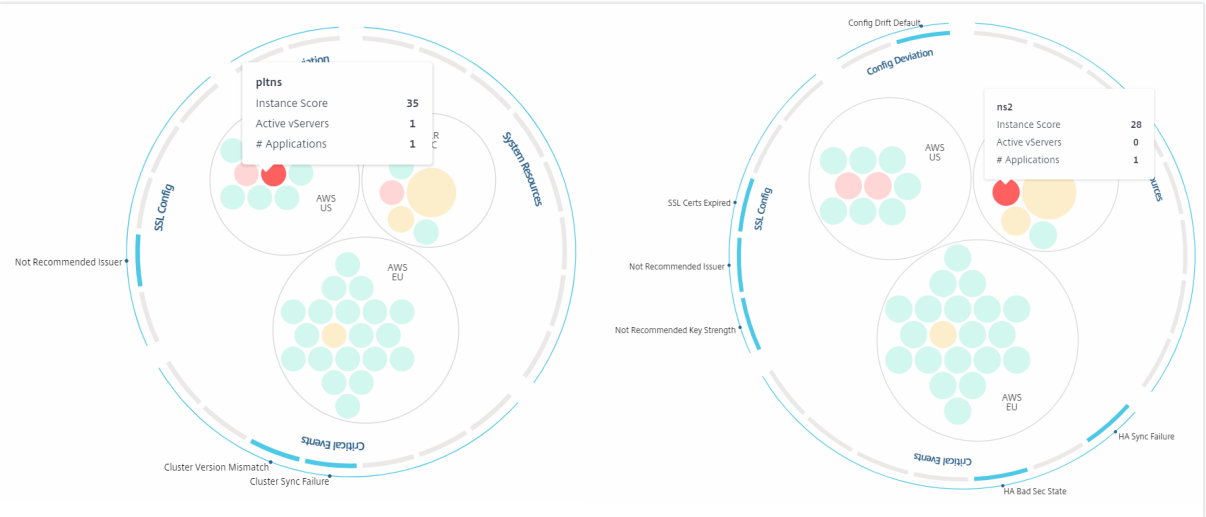


Comment utiliser Circle Pack

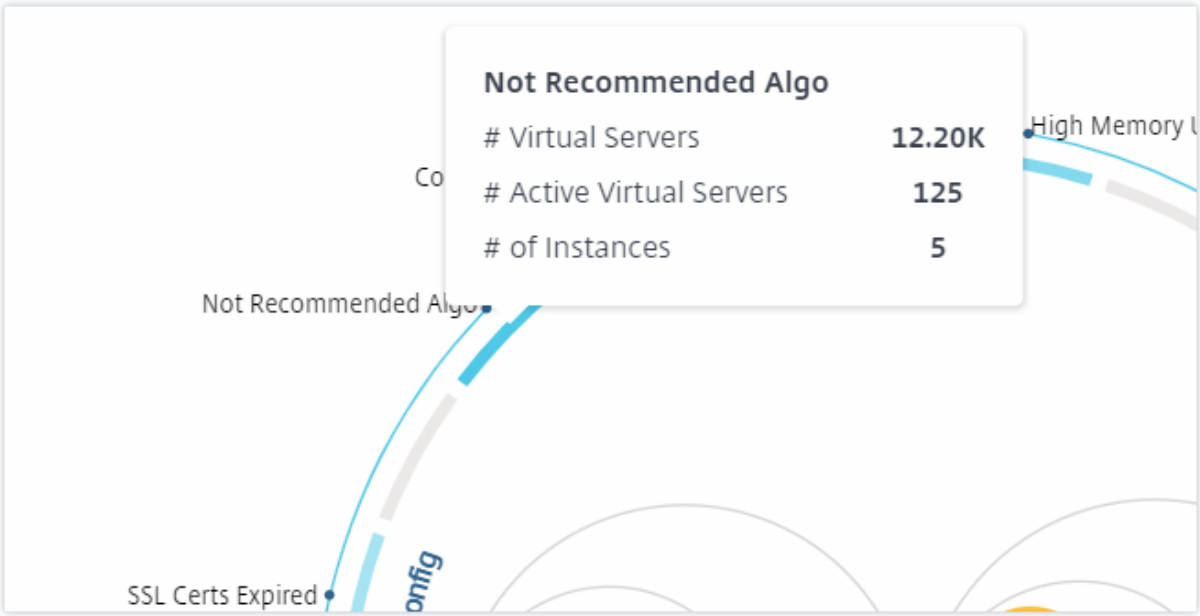
Cliquez sur chacun des cercles colorés pour mettre en surbrillance cette instance.



Selon les événements qui se sont produits dans ce cas, seuls ces indicateurs de santé sont mis en évidence sur les cercles extérieurs. Par exemple, les deux images suivantes du Circle Pack affichent différents ensembles d'indicateurs de risque, bien que les deux instances soient dans un état critique.



Vous pouvez également cliquer sur les indicateurs de santé pour obtenir plus de détails sur le nombre d'instances qui ont signalé cet indicateur de risque. Par exemple, cliquez sur `Not recommended Algo` pour afficher le rapport récapitulatif de cet indicateur de risque.

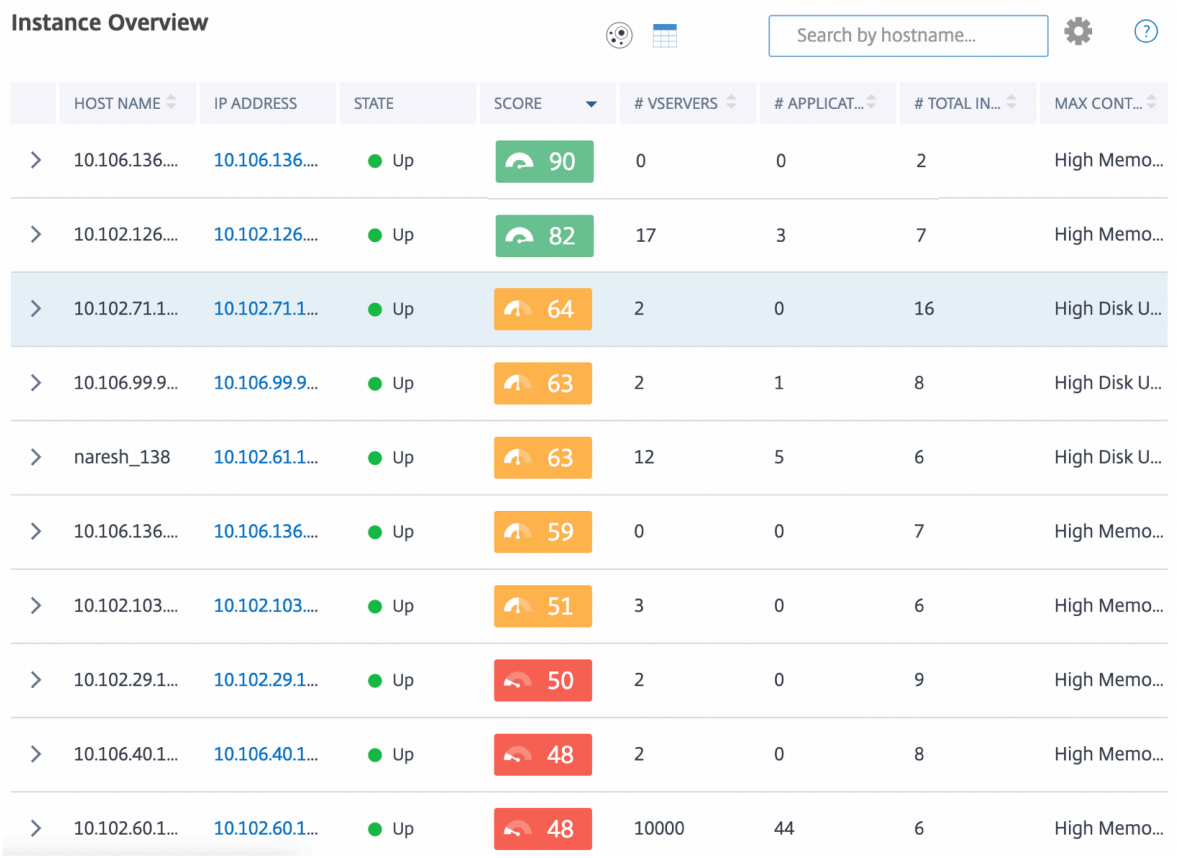


Vue tabulaire

La vue tabulaire affiche les instances et les détails de ces instances dans un format tabulaire. Les détails qui s'affichent sont les suivants :

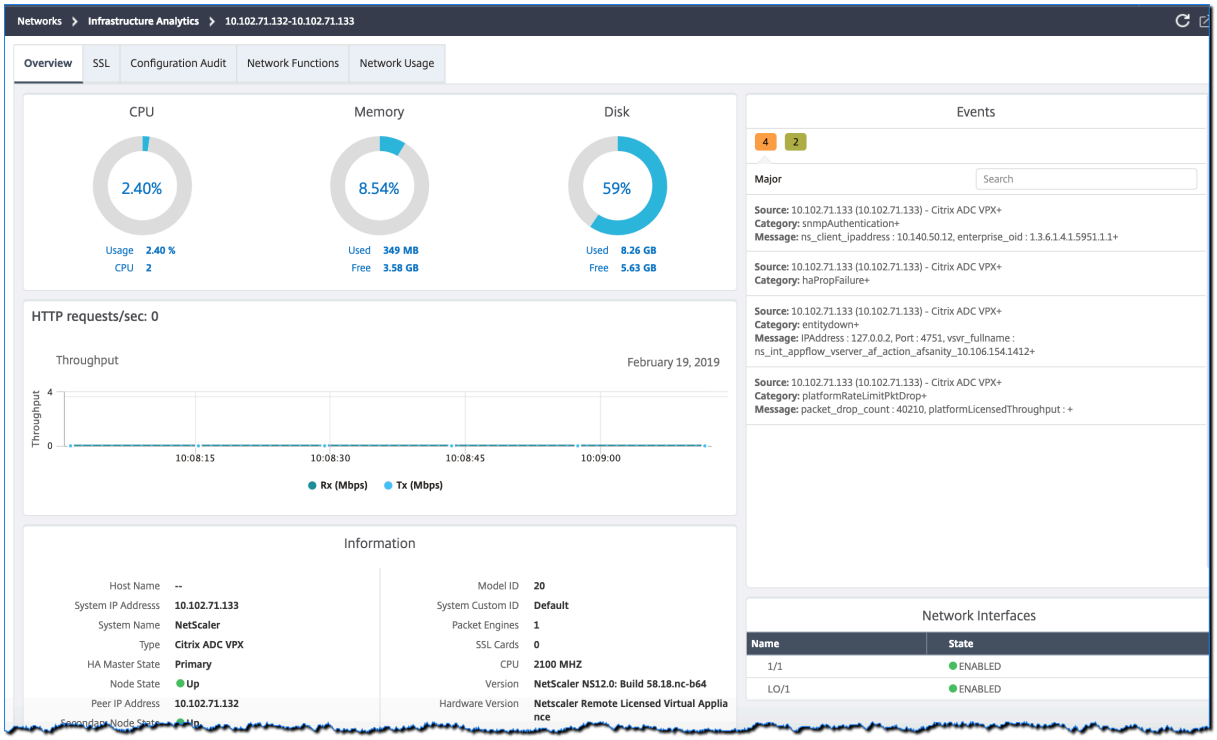
- Nom d'hôte de l'instance
- L'adresse IP de l'instance
- État de l'instance
- Score d'instance
- Nombre de serveurs virtuels configurés sur cette instance
- Nombre d'applications configurées sur cette instance
- Nombre total d'indicateurs de risque
- L'événement qui contribue le plus à la baisse du score de l'instance

Les instances qui se trouvent dans un état critique figurent en haut du tableau, suivies par les instances qui doivent être examinées, puis par les instances les plus saines.

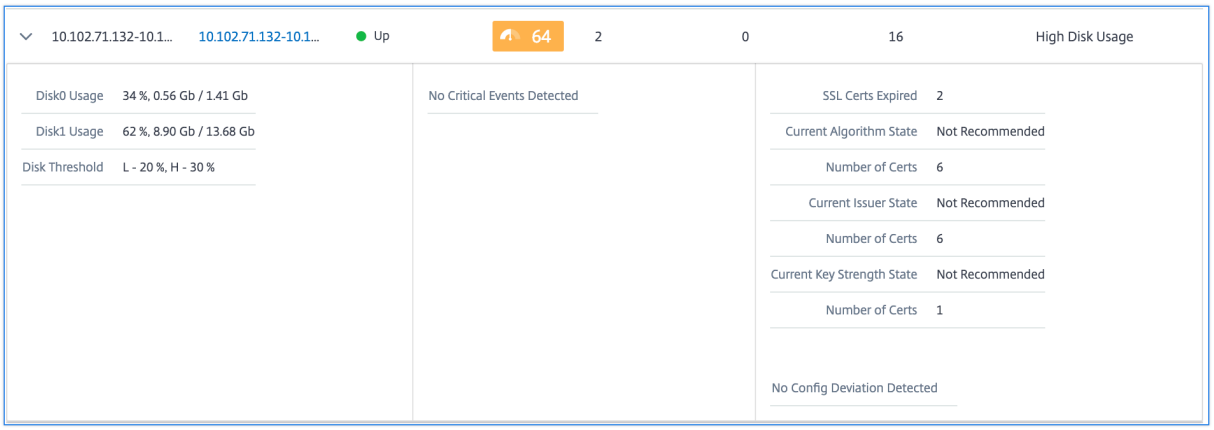


HOST NAME	IP ADDRESS	STATE	SCORE	# VSERVERS	# APPLICAT...	# TOTAL IN...	MAX CONT...
10.106.136....	10.106.136....	Up	90	0	0	2	High Memo...
10.102.126....	10.102.126....	Up	82	17	3	7	High Memo...
10.102.71.1...	10.102.71.1...	Up	64	2	0	16	High Disk U...
10.106.99.9...	10.106.99.9...	Up	63	2	1	8	High Disk U...
naresh_138	10.102.61.1...	Up	63	12	5	6	High Disk U...
10.106.136....	10.106.136....	Up	59	0	0	7	High Memo...
10.102.103....	10.102.103....	Up	51	3	0	6	High Memo...
10.102.29.1...	10.102.29.1...	Up	50	2	0	9	High Memo...
10.106.40.1...	10.106.40.1...	Up	48	2	0	8	High Memo...
10.102.60.1...	10.102.60.1...	Up	48	10000	44	6	High Memo...

Cliquez sur l'adresse IP de l'instance dans la vue tabulaire pour afficher plus de détails sur cette instance sous forme d'affichage du tableau de bord. Le tableau de bord de l'instance présente une vue d'ensemble de l'instance dans laquelle vous pouvez voir le CPU, la mémoire et l'utilisation du disque de l'instance. Vous pouvez également afficher les détails relatifs à la gestion des certificats SSL, à l'audit de configuration, aux fonctions réseau et à un rapport réseau qui indique l'utilisation détaillée de l'instance sur le réseau. Faites défiler la page vers le bas pour voir la liste des fonctionnalités et des modes activés sur cette instance.



Vous pouvez également cliquer sur la flèche au début de chaque ligne pour développer la ligne et obtenir plus de détails.



La ligne de tableau étendue affiche les erreurs survenues sur l'instance pour toutes les catégories. Dans l'exemple ci-dessus, vous pouvez voir qu'il y a eu des erreurs dans les ressources système, la configuration SSL et des écarts dans les fichiers de configuration. Mais aucun événement critique n'a été signalé depuis cette instance.

Comment utiliser le panneau récapitulatif

Le **panneau récapitulatif** vous aide à vous concentrer efficacement et rapidement sur les instances nécessitant une révision ou un état critique. Le panneau est divisé en trois onglets : vue d'ensemble,

informations sur l'instance et profil de trafic. Les modifications que vous apportez dans ce panneau modifient l'affichage dans les formats Circle Pack et Tabular. Les sections suivantes décrivent ces onglets plus en détail. Les exemples présentés dans les sections suivantes vous aident à utiliser efficacement les différents critères de sélection pour analyser les problèmes signalés par les instances.

Vue d'ensemble :

L'onglet **Vue d'ensemble** vous permet de surveiller les instances en fonction des erreurs matérielles, de l'utilisation, des certificats expirés et d'indicateurs similaires pouvant survenir dans les instances. Les indicateurs que vous pouvez surveiller ici sont les suivants :

- Utilisation UC
- Utilisation de la mémoire
- Utilisation du disque
- Pannes du système
- Événements critiques
- Expiration des certificats SSL

Les exemples suivants illustrent comment vous pouvez interagir avec le panneau **Vue d'ensemble** pour isoler les instances qui signalent des erreurs.

Exemple 1 : Afficher les instances dont l'état est en cours de révision :

Cochez la case **Vérifier** pour afficher uniquement les instances qui ne signalent pas d'erreurs critiques, mais qui nécessitent tout de même une attention particulière.

Les histogrammes du panneau **Vue d'ensemble** représentent un nombre agrégé d'instances en fonction d'événements liés à une utilisation élevée du processeur, à une utilisation élevée de la mémoire et à une utilisation élevée du disque. Les histogrammes sont notés à 10 %, 20 %, 30 %, 40 %, 50 %, 60 %, 70 %, 80 %, 90 % et 100 %. Passez le pointeur de votre souris sur l'un des graphiques à barres. La légende au bas du graphique indique la plage d'utilisation et le nombre d'instances comprises dans cette plage. Vous pouvez également cliquer sur le graphique à barres pour afficher toutes les instances de cette plage.

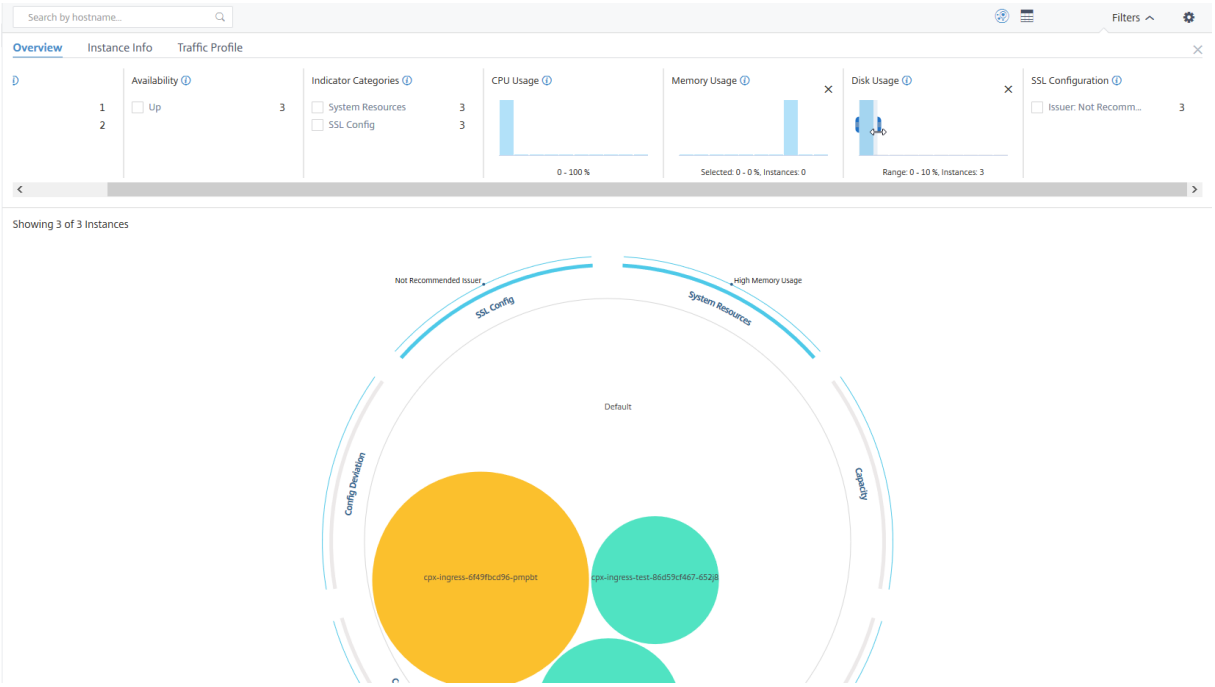
Exemple 2 : Afficher les instances qui consomment entre 10 % et 20 % de la mémoire allouée :

Dans la section Utilisation de la mémoire, cliquez sur le graphique à barres. La légende indique que la plage sélectionnée est comprise entre 10 et 20 % et que 29 instances fonctionnent dans cette plage.

Vous pouvez également sélectionner plusieurs plages dans ces histogrammes.

Exemple 3 : affichez les instances qui consomment beaucoup d'espace disque dans plusieurs plages :

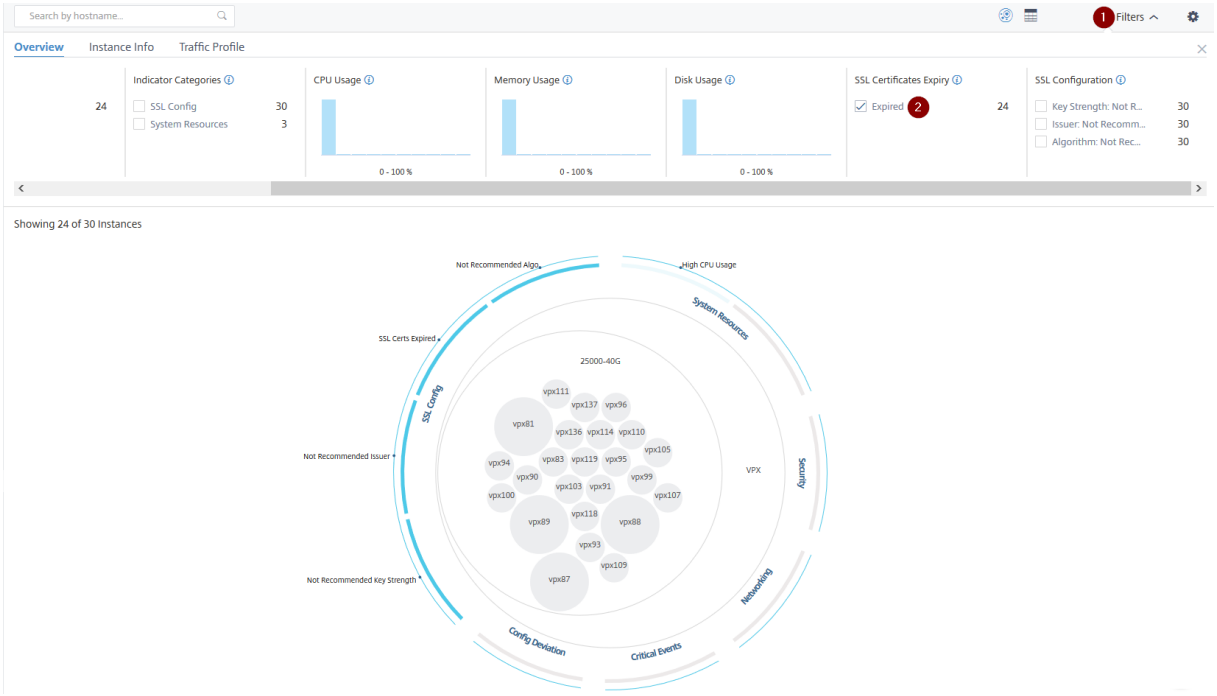
Pour afficher les instances qui ont consommé de l'espace disque entre 0 et 10 %, faites glisser le pointeur de la souris sur les deux plages.



> **Remarque**
>
> Cliquez sur « X » pour supprimer la sélection. Vous pouvez également cliquer sur **Réinitialiser** pour supprimer plusieurs sélections.

Les graphiques à barres horizontales du panneau **Vue d'ensemble** indiquent le nombre d'instances qui signalent des erreurs système, des événements critiques et l'état d'expiration des certificats SSL. Cochez la case pour afficher ces instances.

Exemple 4 : Afficher les instances pour les certificats SSL expirés :



1 - Cliquez sur la liste **Filtre**.

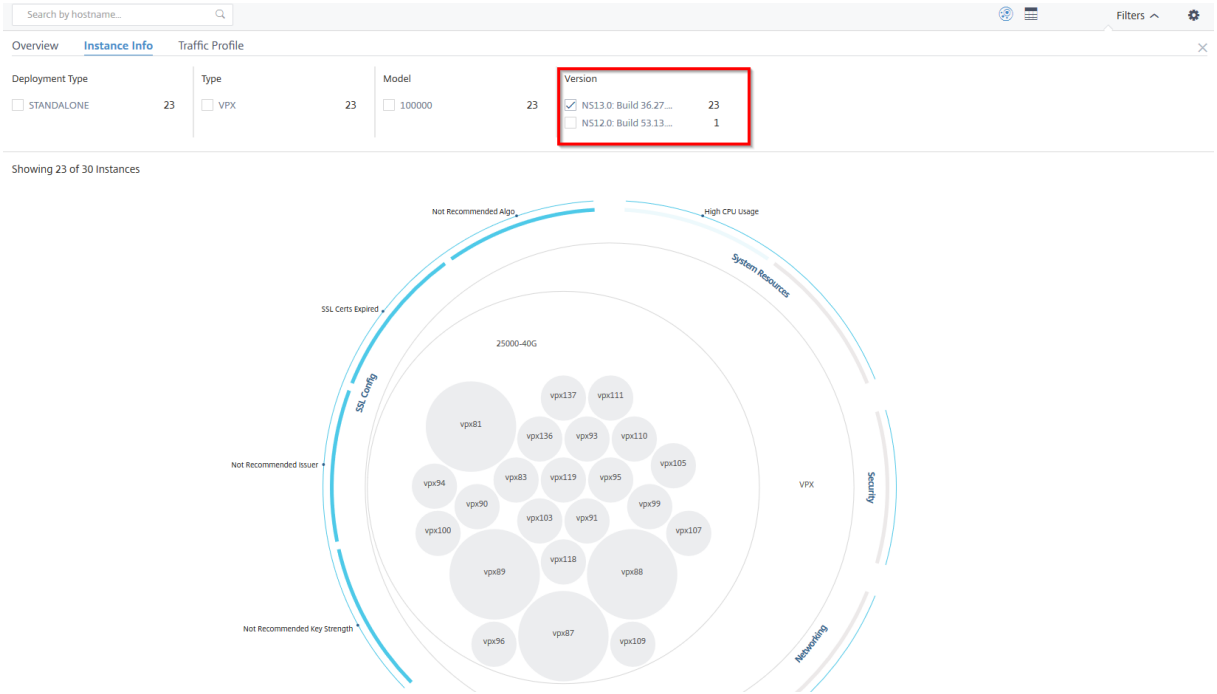
2 - Dans la section **Expiration des certificats SSL**, cochez la case **Expiré** pour afficher les instances.

Infos sur l'instance

Le panneau **Informations sur l'instance** vous permet de visualiser les instances en fonction du type de déploiement, du type d'instance, du modèle et de la version du logiciel. Vous pouvez sélectionner plusieurs cases à cocher pour affiner votre sélection.

Exemple 5 : Afficher les instances ADC VPX avec un numéro de build spécifique :

Sélectionnez la version à afficher.



Profil de trafic

Les histogrammes du panneau **Profil de trafic** représentent un nombre agrégé d'instances en fonction du débit autorisé sur les instances, du nombre de demandes, de connexions et de transactions gérées par les instances. Sélectionnez le graphique à barres pour afficher les instances comprises dans cette plage.

Exemple 6 : Afficher les instances prenant en charge les connexions TCP :

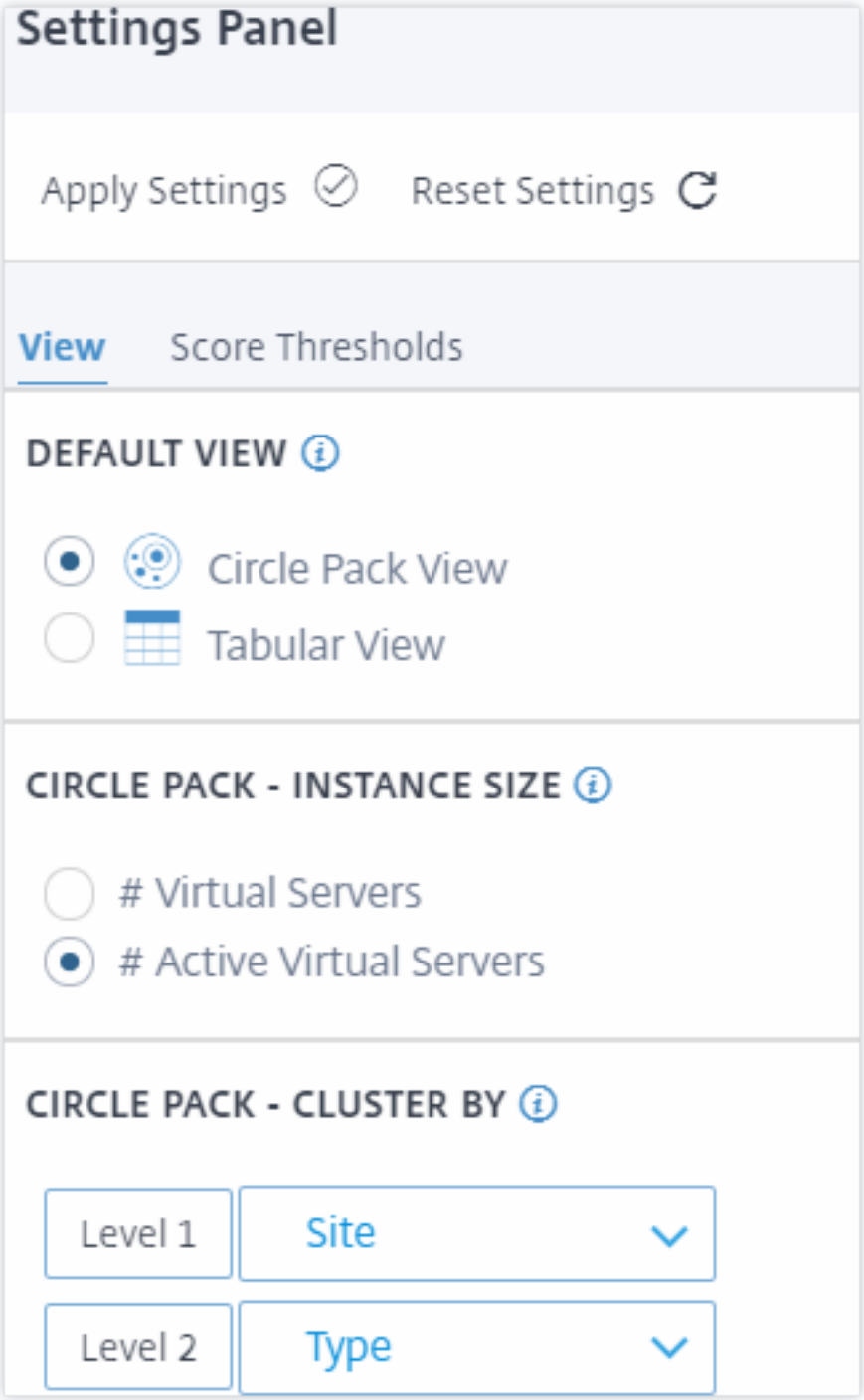
L'image suivante montre le nombre d'instances prenant en charge les connexions TCP.

Comment utiliser le panneau des paramètres

Le panneau **Paramètres** vous permet de définir la vue par défaut de l'analyse de l'infrastructure. Il vous permet également de définir les valeurs de seuil basses et supérieures pour une utilisation élevée du processeur, une utilisation élevée du disque et une utilisation élevée de la mémoire. Le panneau des paramètres est divisé en deux onglets : Afficher et Seuils de score.

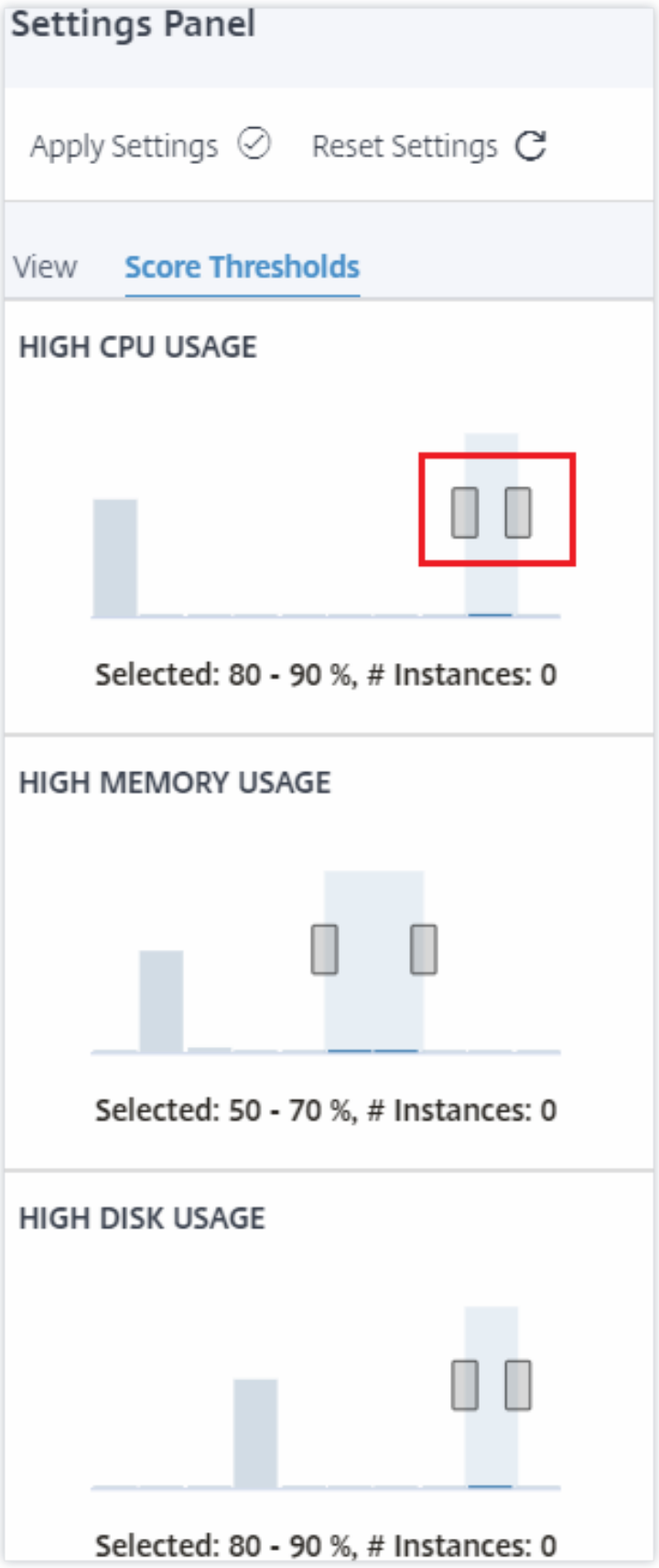
View

- **Vue par défaut**. Sélectionnez **Circle Pack** ou le format tabulaire comme affichage par défaut sur la page d'analyse. Le format que vous sélectionnez est celui que vous voyez chaque fois que vous accédez à la page dans Citrix ADM.
- **Circle Pack : taille de l'instance**. Indiquez la taille du cercle d'instances en fonction du nombre de serveurs virtuels ou du nombre de serveurs virtuels actifs.
- **Empilement de cercles - Cluster par**. Décidez de la mise en cluster à deux niveaux des cercles d'instance. Pour plus d'informations sur le clustering d'instances, voir Cercles d'instances en cluster.



Seuils de score

Vous pouvez modifier les valeurs de seuil bas et haut pour une utilisation élevée du processeur, de la mémoire et du disque en fonction des besoins de trafic de votre organisation. Faites glisser les poignées dans chacun des histogrammes de sélection pour définir les valeurs.



> **Remarque**
>
> Cliquez sur **Appliquer les paramètres** pour appliquer ces modifications ou cliquez sur **Réinitialiser** pour supprimer toutes les modifications.

Comment visualiser les données sur le tableau de bord

Grâce à Infrastructure Analytics, les administrateurs réseau peuvent désormais identifier les instances nécessitant le plus d'attention en quelques secondes. Pour comprendre plus en détail la visualisation des données, considérons le cas de Chris, un administrateur réseau d'ExampleCompany.

Chris gère de nombreuses instances Citrix ADC dans l'organisation. Quelques-unes des instances traitent un trafic élevé, et Chris doit les surveiller de près. Chris remarque que quelques instances à fort trafic ne traitent plus l'intégralité du trafic qui les traverse. Pour analyser cette réduction, Chris devait auparavant lire plusieurs rapports de données provenant de diverses sources. Chris a dû passer plus de temps à essayer de corréler les données manuellement et de déterminer quelles instances ne sont pas dans un état optimal et nécessitent une attention particulière.

Chris utilise la fonctionnalité Infrastructure Analytics pour visualiser l'état de santé de toutes les instances.

Les deux exemples suivants illustrent comment Infrastructure Analytics aide Chris dans les activités de maintenance :

Exemple 1 - Pour surveiller le trafic SSL :

Chris remarque sur le Circle Pack qu'une instance a un score d'instance faible et que cette instance est dans l'état « Critique ». Chris clique sur cette instance pour voir quel est le problème. Le résumé de l'instance indique qu'il y a une défaillance de la carte SSL sur cette instance et que l'instance n'est pas en mesure de traiter le trafic SSL (le trafic SSL a été réduit). Chris extrait cette information et envoie un rapport à l'équipe pour qu'elle examine le problème immédiatement.

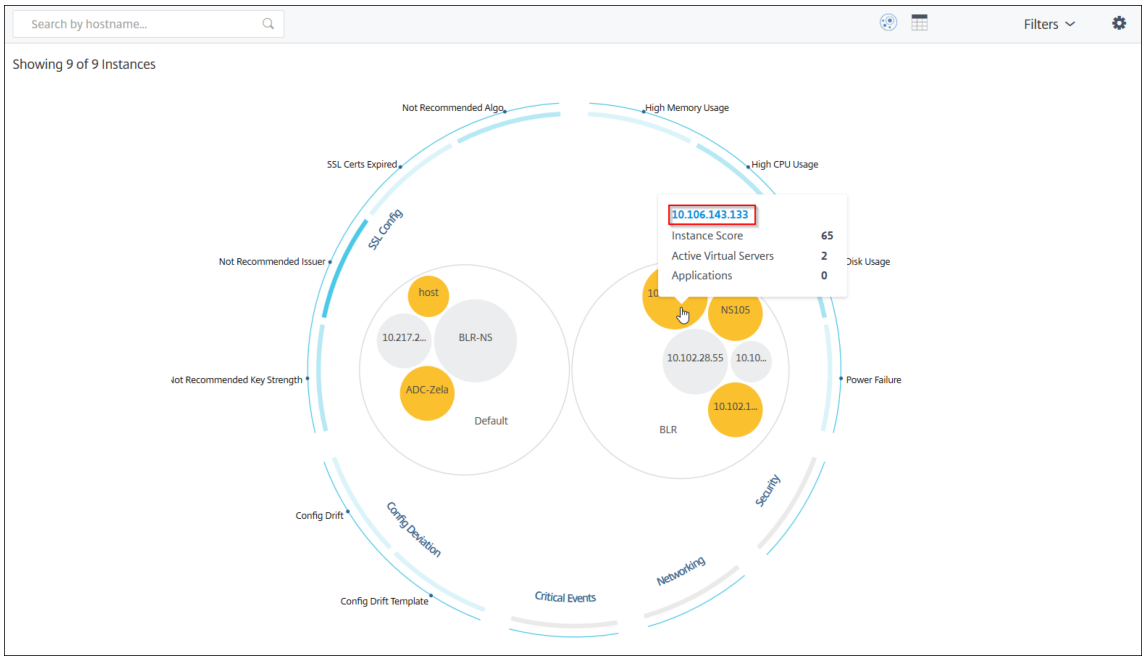
Exemple 2 - Pour surveiller les modifications de configuration :

Chris remarque également qu'une autre instance est dans l'état « Review » et qu'il y a eu une déviation de configuration récemment. Lorsque Chris clique sur l'indicateur de risque d'écart de configuration, Chris remarque que des modifications de configuration liées à RC4 Cipher, SSL v3, TLS 1.0 et TLS 1.1 ont été apportées, ce qui peut être dû à des problèmes de sécurité. Chris remarque également que le profil de trafic des transactions SSL pour cette instance a été réduit. Chris exporte ce rapport et l'envoie à l'administrateur pour en savoir plus.

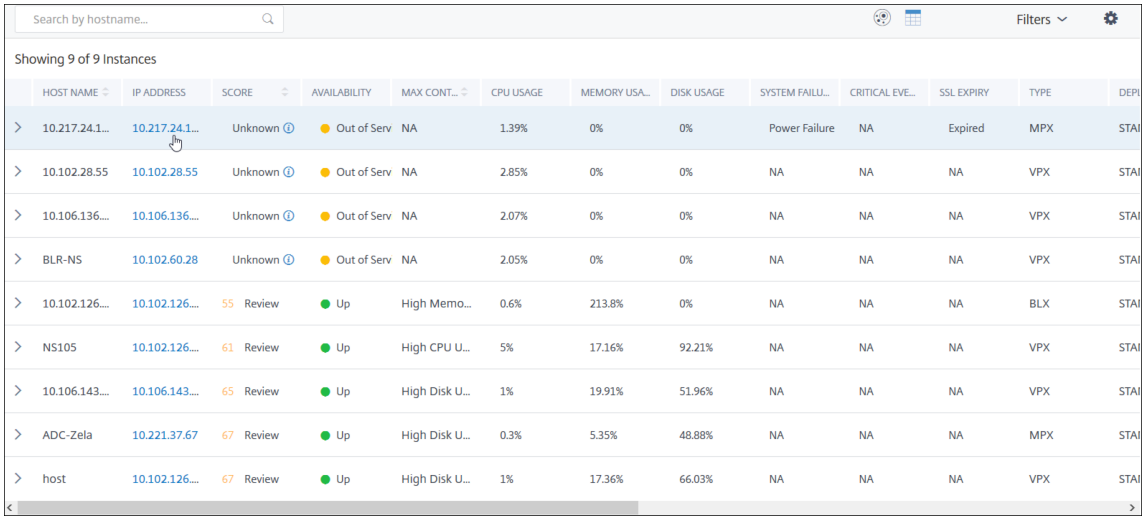
Afficher les détails de l'instance dans Infrastructure Analytics

February 1, 2024

1. Accédez à **Réseaux** > **Analyse de l'infrastructure**
2. Cliquez sur la vue du pack de cercle et sélectionnez l'adresse IP.



Vous pouvez également cliquer sur une adresse IP dans la vue tabulaire.



- **Nom d'hôte** : indique le nom d'hôte attribué à l'instance ADC
- **Adresse IP** : indique l'adresse IP de l'instance ADC

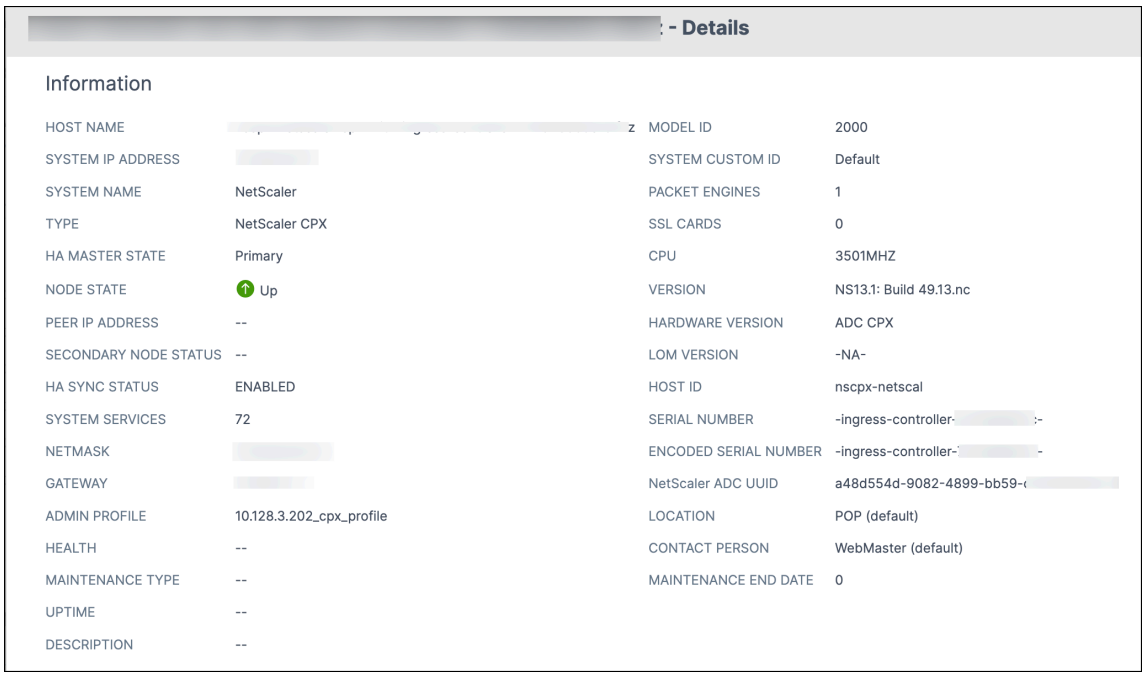
- **Score** —Indique le score de l'instance ADC et le statut (Critical, Good et Fair)
- **Disponibilité** : indique l'état de l'instance ADC, tel que **Up**, **Down**ou **Hors service**.
- **Contribution maximale** : indique la catégorie de problème pour laquelle l'instance ADC a le nombre maximal d'erreurs.
- **Utilisation du processeur** : indique le pourcentage actuel du processeur utilisé par l'instance
- **Utilisation de la mémoire** : indique le % de mémoire actuellement utilisé par l'instance
- **Utilisation du disque** : indique le pourcentage de disque actuellement utilisé par l'instance
- **Défaillance du système** : indique le nombre total d'erreurs pour le système d'instance
- **Evénements critiques** : indique la catégorie d'événement dans laquelle l'instance Citrix ADC a le maximum d'événements
- **Expiration SSL** —Indique l'état du certificat SSL installé sur l'instance ADC
- **Type** : indique le type d'instance ADC tel que VPX, SDX, MPX ou CPX
- **Déploiement** : indique si l'instance ADC est déployée en tant qu'instance autonome ou en tant que paire HA
- **Modèle** : indique le numéro de modèle de l'instance ADC
- **Version** : indique la version et le numéro de build de l'instance ADC
- **Débit** : indique le débit réseau actuel de l'instance ADC
- **Demande HTTPS/sec** : indique les demandes HTTPS actuelles reçues par l'instance ADC
- **Connexion TCP** —Indique les connexions TCP actuelles établies
- **Transaction SSL** : indique les transactions SSL en cours traitées par l'instance ADC
- **Site** : indique le nom du site sur lequel l'instance ADC est déployée.

> **Remarque**
>
> Toutes les 5 minutes, les valeurs actuelles relatives à l'utilisation du processeur, de la mémoire, de l'utilisation du disque, du débit, etc. sont mises à jour.

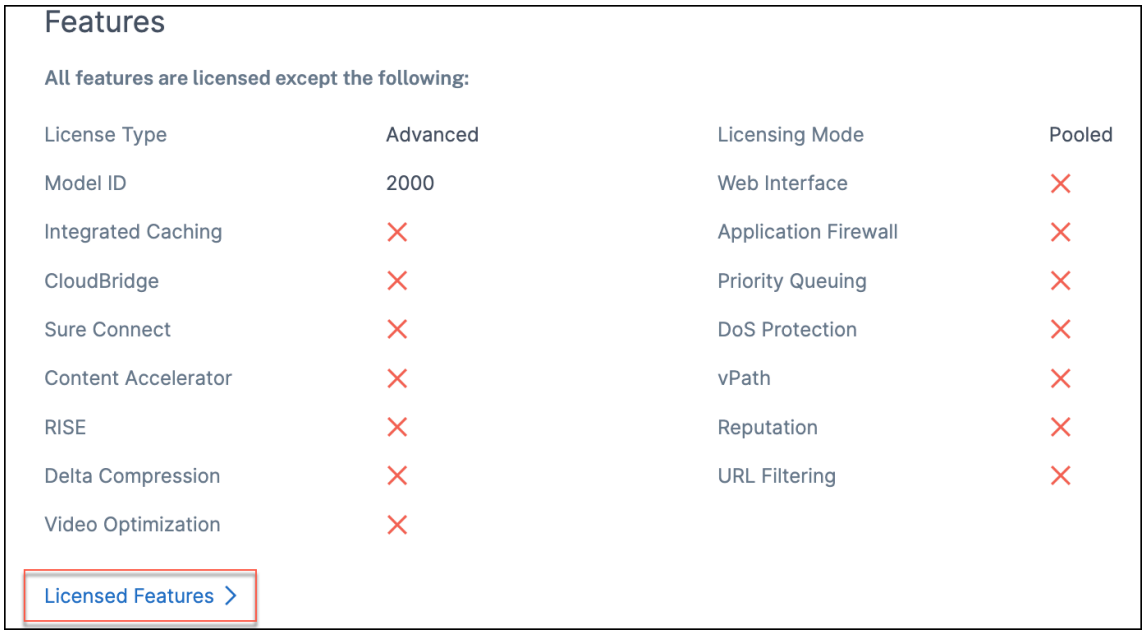
Cliquez sur **Détails de l'instance** pour afficher les détails.

Les détails suivants s'affichent :

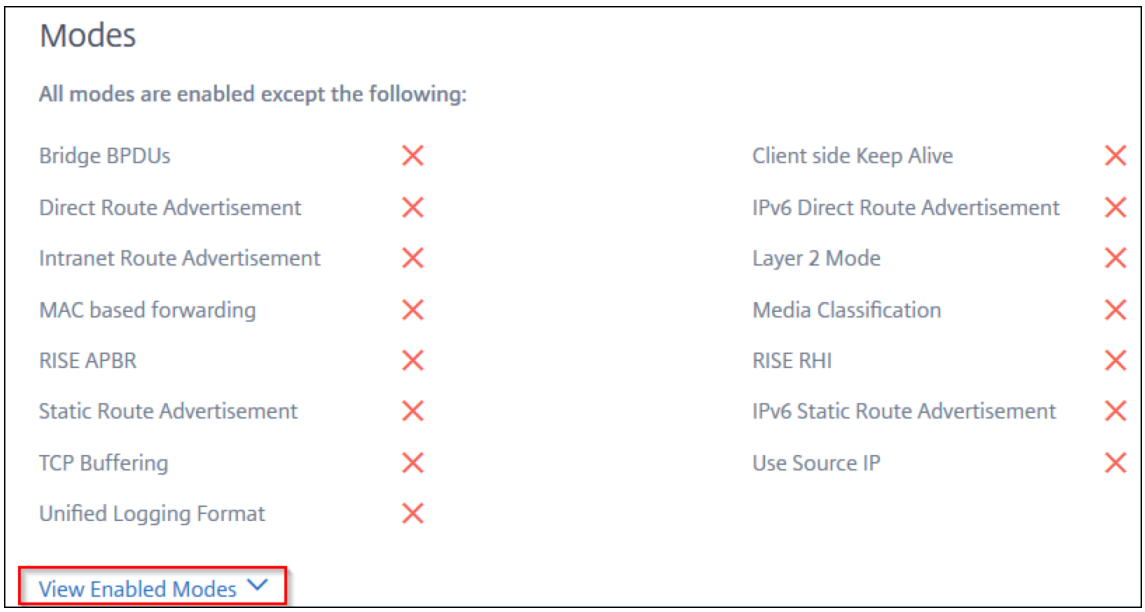
- **Informations** : détails de l'instance tels que le type d'instance, le type de déploiement, la version et le modèle.



- **Fonctionnalités** : par défaut, les fonctionnalités qui ne sont pas sous licence sont affichées. Cliquez sur **Fonctionnalités sous licence** pour afficher les fonctionnalités sous licence.

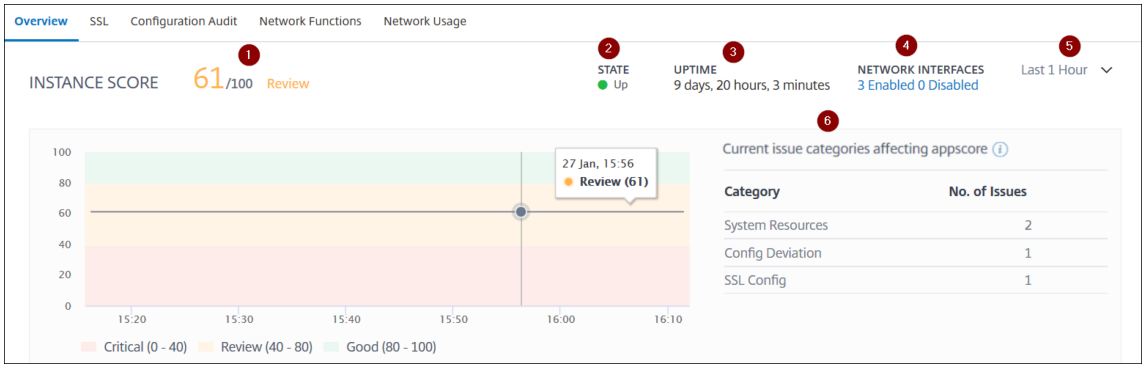


- **Modes** : par défaut, tous les modes désactivés sur l'instance sont affichés. Cliquez sur **Afficher les modes activés** pour afficher les modes activés sur l'instance.



Le tableau de bord de l'instance présente un aperçu de l'instance dans lequel vous pouvez consulter les informations suivantes :

- **Score d'instance**



1 —Indique le score actuel de l'instance Citrix ADC pour la durée sélectionnée. Le score final est calculé comme **100 moins le total des pénalités**. Le graphique affiche les plages de score pour la durée sélectionnée.

2 —Indique l'état de l'instance de Citrix ADC, par exemple **Up**, **Down**et **Out of Service**.

3 —Indique la durée pendant laquelle l'instance de Citrix ADC est en cours d'exécution.

4 —Indique le nombre total d'interfaces réseau activées et désactivées pour l'instance. Cliquez pour afficher les détails tels que le nom de l'interface réseau et son état (activé ou désactivé).

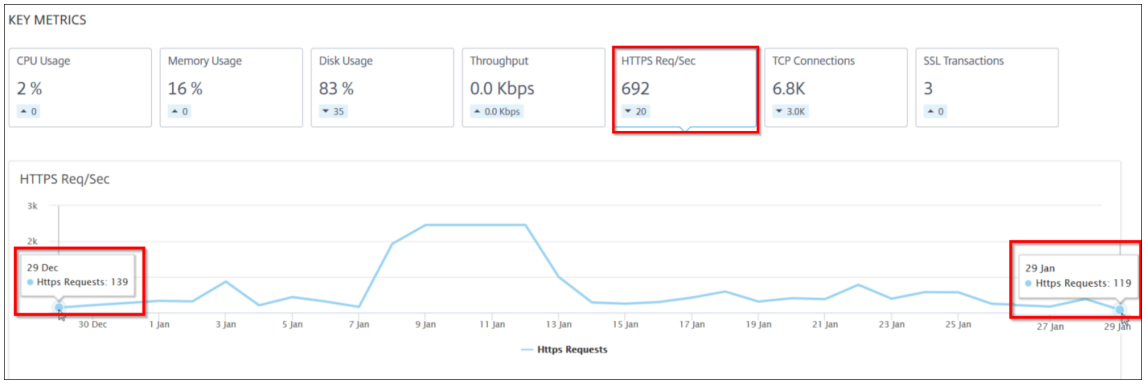
5 —Sélectionnez la durée dans la liste pour afficher les détails de l'instance.

6 —Affiche le nombre total de problèmes et la catégorie de problèmes de l'instance ADC.

- **Indicateurs clés**

Cliquez sur chaque onglet pour afficher les détails. Dans chaque mesure, vous pouvez afficher la valeur moyenne et la valeur de différence pour l'heure sélectionnée.

L'image suivante est un exemple de HTTPS Req/Sec et la durée sélectionnée est de 1 heure. La valeur **692** est la valeur HTTPS Req/Sec moyenne pour une durée d'un mois et la valeur **20** est la valeur de différence. Dans le graphique, la première valeur est **139** et la dernière valeur est **119**. La valeur de la différence est de **139** —**119 = 20**.



Vous pouvez afficher les mesures d'instance suivantes dans un format graphique pour la durée sélectionnée :

- **Utilisation du processeur** : % de CPU moyen de l'instance pendant la durée sélectionnée (s'affiche à la fois pour le processeur par paquets et pour le processeur de gestion).
- **Utilisation de la mémoire** : % d'utilisation moyenne de la mémoire de l'instance pendant la durée sélectionnée.
- **Utilisation du disque** : pourcentage d'espace disque moyen de l'instance pendant la durée sélectionnée.
- **Débit** : débit réseau moyen traité par l'instance pendant la durée sélectionnée.
- **Demande HTTPS/sec** : nombre moyen de requêtes HTTPS reçues par l'instance pendant la durée sélectionnée.
- Connexions**TCP** —**Les connexions** TCP moyennes établies par le client et le serveur pendant la durée sélectionnée.
- **Transactions SSL** : transactions SSL moyennes traitées par l'instance pendant la durée sélectionnée.

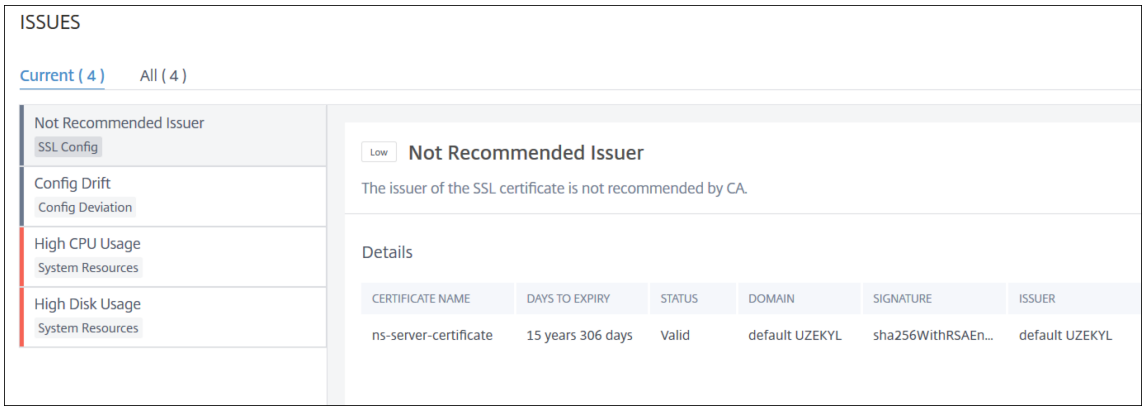
- **Problèmes**

Vous pouvez consulter les problèmes suivants qui se produisent dans l'instance Citrix ADC :

Catégorie de problème	Description	Problèmes
Ressources système	Affiche tous les problèmes liés à la ressource système Citrix ADC tels que CPU, mémoire, utilisation du disque.	– Utilisation élevée du processeur – Utilisation élevée de la mémoire – Utilisation élevée du disque – Défaillances de cartes SSL – Panne de courant – Erreur de disque – Erreur Flash – Rejets de cartes réseau
Configuration SSL	Affiche tous les problèmes liés à la configuration SSL sur l'instance Citrix ADC.	– Les certificats SSL ont expiré – Émetteur non recommandé – Algorithme non recommandé – Intensité clé non recommandée
Déviation de configuration	Affiche tous les problèmes liés aux tâches de configuration appliquées dans l'instance Citrix ADC.	– Dérive de configuration – Running vs Template
Événements critiques	Affiche tous les événements critiques liés aux instances Citrix ADC configurées dans une paire HA et dans un cluster.	– Défaillance de l'hélice du cluster – Échec de la synchronisation du cluster – Incompatibilité des versions du cluster

Catégorie de problème	Description	Problèmes
Réseau	Affiche les problèmes opérationnels qui se produisent dans les instances.	– HA : mauvais état secondaire – HA Pas de battements de chaleur – Échec de synchronisation HA – Incompatibilité de version HA Pour plus d'informations, consultez Analyse d'infrastructure améliorée avec de nouveaux indicateurs.

Cliquez sur chaque onglet pour analyser et résoudre le problème. Par exemple, considérez qu'une instance présente les erreurs suivantes pour la durée sélectionnée :



- L'onglet **Actuel** affiche les problèmes qui affectent actuellement le score de l'instance.
- L'onglet **Tout** affiche tous les problèmes infra détectés pour la durée sélectionnée.

Afficher les problèmes de capacité dans une instance ADC

February 1, 2024

Lorsqu'une instance ADC a consommé la plus grande partie de sa capacité disponible, la suppression de paquets peut se produire lors du traitement du trafic client. Ce problème provoque de faibles performances dans une instance ADC. En comprenant ces problèmes de capacité de l'ADC, vous pouvez

allouer de manière proactive des licences supplémentaires afin de stabiliser les performances de l'ADC.

Dans la **vue Circle Pack**, vous pouvez afficher les problèmes de capacité d'instance ADC s'il existe.

Pour afficher les problèmes de capacité de l'ADC,

1. Accédez à **Réseaux > Analyse de l'infrastructure**.
2. Sélectionnez la vue du pack de cercles.

> **Remarque**
>
> Dans **Infrastructure Analytics**, les vues circulaires et tabulaires affichent les événements et les problèmes survenus au cours de la dernière heure.

L'illustration suivante suggère que les problèmes de capacité existent dans l'instance sélectionnée :

Les problèmes sont classés selon les paramètres de capacité suivants :

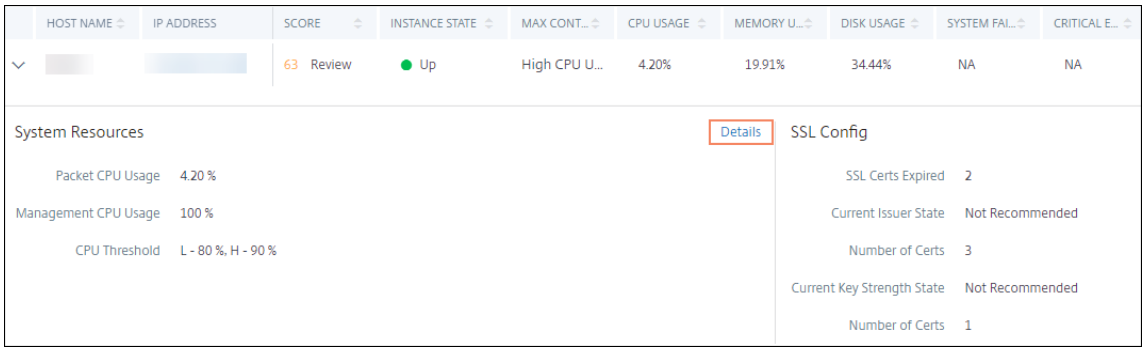
- **Limite de débit atteinte** : nombre de paquets abandonnés dans l'instance une fois la limite de débit atteinte.
- **Limite de processeur PE atteinte** : nombre de paquets déposés sur toutes les cartes réseau une fois que la limite du processeur PE est atteinte.
- **Limite de PPS atteinte** : nombre de paquets abandonnés dans l'instance une fois la limite de PPS atteinte.

- **Limite de débit SSL** : nombre de fois que la limite de débit SSL est atteinte.
- **Limite de débit SSL TPS** : nombre de fois que la limite SSL TPS est atteinte.

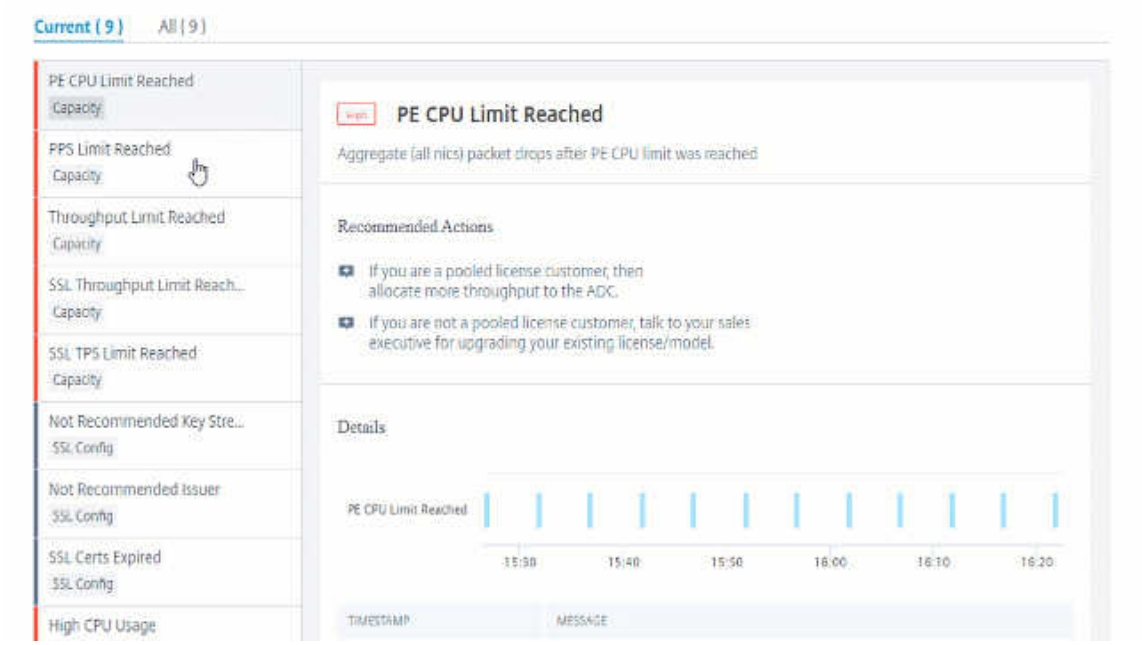
Afficher les actions recommandées pour résoudre les problèmes de capacité

L'ADM recommande des actions susceptibles de résoudre les problèmes de capacité. Pour afficher les actions recommandées, effectuez les opérations suivantes :

1. Dans **Réseaux > Analyse de l'infrastructure**, sélectionnez la vue tabulaire.
2. Sélectionnez l'instance qui présente des problèmes de capacité et cliquez sur **Détails**.



3. Sur la page de l'instance, faites défiler l'écran jusqu'à la section **Problèmes** .
4. Sélectionnez chaque problème et consultez les actions recommandées pour résoudre les problèmes de capacité.



L'ADM interroge ces événements toutes les cinq minutes à partir de l'instance ADC et affiche les baisses de paquets ou les incréments de compteur de limite de vitesse s'il existe.

L'ADM calcule le score de l'instance sur le seuil de capacité défini.

- **Seuil bas** —Incrément de compteur de perte ou de limite de débit de 1 paquet
- **Seuil élevé** : 10000 paquets baisse ou incrément du compteur de limite de taux

Par conséquent, lorsqu'une instance ADC dépasse le seuil de capacité, le score d'instance est affecté.

Lorsque des paquets tombent ou que le compteur de limite de débit augmente, un événement est généré dans `ADCCapacityBreach` cette catégorie. Pour afficher ces événements, accédez à **Comptes > Événements système**.

Analyse de l'infrastructure améliorée avec de nouveaux indicateurs

February 1, 2024

À l'aide de Citrix ADM Infrastructure Analytics, vous pouvez :

- Consultez un nouvel ensemble de problèmes opérationnels qui se produisent dans les instances Citrix ADC.
- Consultez les messages d'erreur et consultez les recommandations pour résoudre les problèmes.

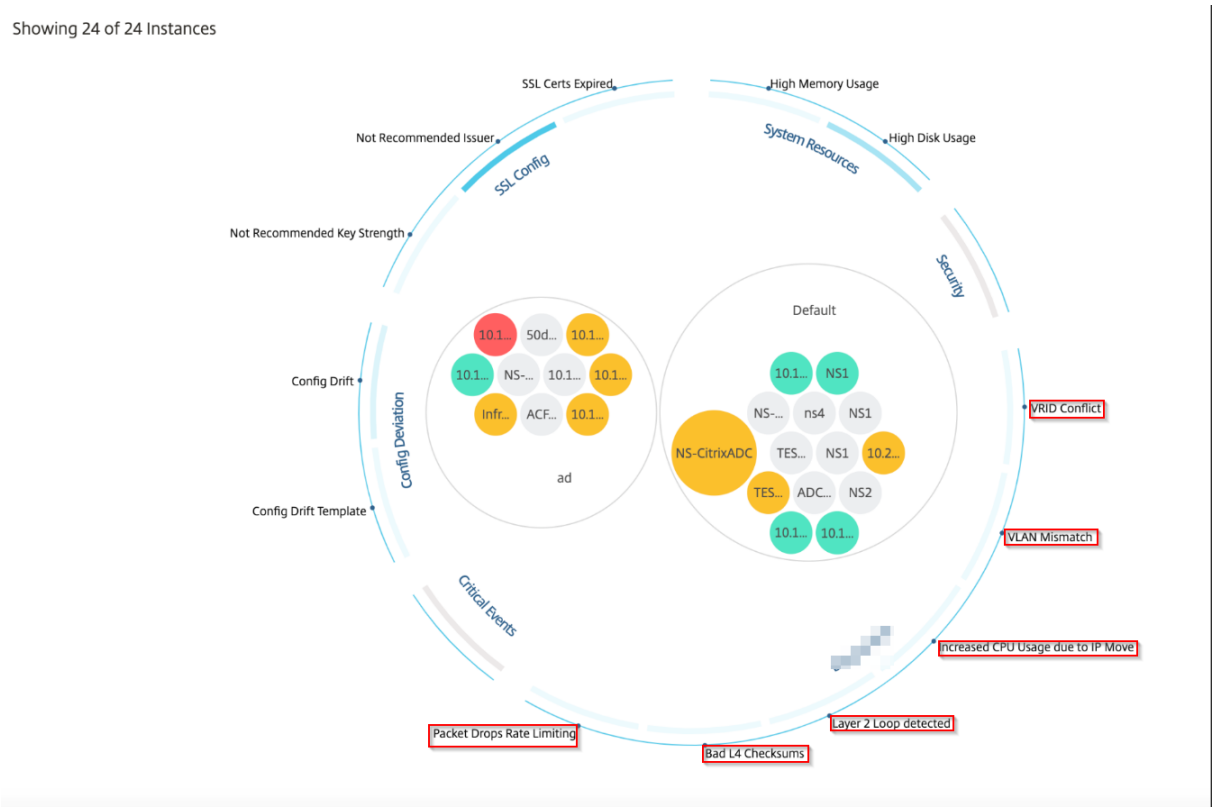
En tant qu'administrateur, vous pouvez rapidement identifier la cause première des problèmes et analyser les problèmes.

> **Remarque**
>
> Les indicateurs de règles ne sont pas supportés pour :
>
> - Instances Citrix ADC configurées en mode cluster.
> - Instances Citrix ADC configurées avec des partitions d'administration.

Dans Citrix ADM, accédez à **Réseaux** > **Analyse de l'infrastructure** pour afficher les indicateurs suivants :

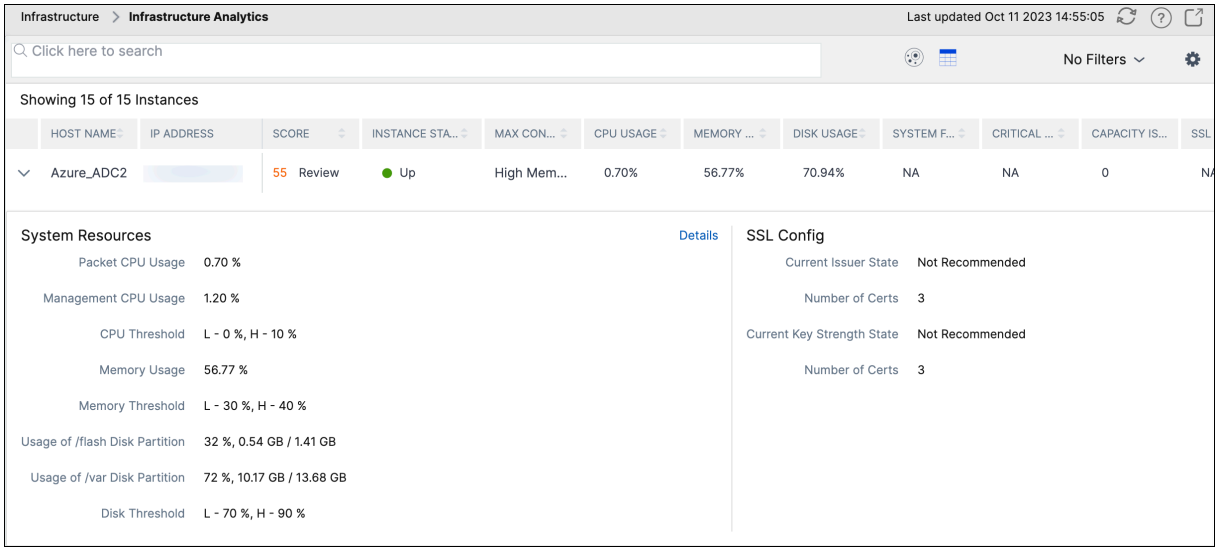
Nom de l'indicateur dans Infrastructure Analytics	Description
Échec de l'allocation de port	Détecte lorsque Citrix ADC utilise SNIP pour communiquer avec une nouvelle connexion au serveur et que le nombre total de ports disponibles sur ce SNIP est épuisé. L'action recommandée consiste à ajouter un autre SNIP dans le même sous-réseau.
Aucune configuration d'itinéraire par défaut	Détecte lorsque le trafic est interrompu en raison de la non-disponibilité des itinéraires.
Conflit d'IP	Détecte si une même adresse IP est configurée ou appliquée sur deux instances ou plus d'un réseau.
Conflit VRID	Détecte lorsque des problèmes d'accès intermittents se produisent pour le VRID spécifié.
Inadéquation du VLAN	Détecte si des erreurs se produisent lors de la configuration du VLAN lié aux sous-réseaux IP.
Attaque de petite fenêtre TCP	Détecte lorsqu'une attaque de petite fenêtre est en cours. Cette alerte est purement informative, car l'ADC atténue déjà cette attaque.
Seuil de contrôle tarifaire	Détecte lorsque des paquets sont abandonnés en fonction du seuil de contrôle de débit configuré.
Limite de persistance	Détecte le moment où un maximum d'accès est imposé à la mémoire Citrix ADC.
Incompatibilité du nom de site GSLB	Détecte les échecs de synchronisation de la configuration GSLB en raison d'une incompatibilité entre les noms de sites.
En-tête IP mal formé	Détecte lorsque les contrôles de santé sur les paquets IPv4 échouent.
Sommes de contrôle L4 incorrectes	Détecte lorsque la validation de la somme de contrôle pour les paquets TCP échoue.
Augmentation de l'utilisation du processeur en raison du déplacement d'IP	Détecte si un grand nombre de Mac doivent être mis à jour.
Direction excessive des paquets	Détecte les niveaux élevés de gestion des paquets logiciels dus à l'utilisation d'un type de clé RSS asymétrique.

Nom de l'indicateur dans Infrastructure Analytics	Description
Boucle de couche 2	Détecte la présence de boucles de couche 2 dans le réseau.
Tagged VLAN mismatch	Détecte lorsque des paquets VLAN balisés sont reçus sur une interface non balisée.



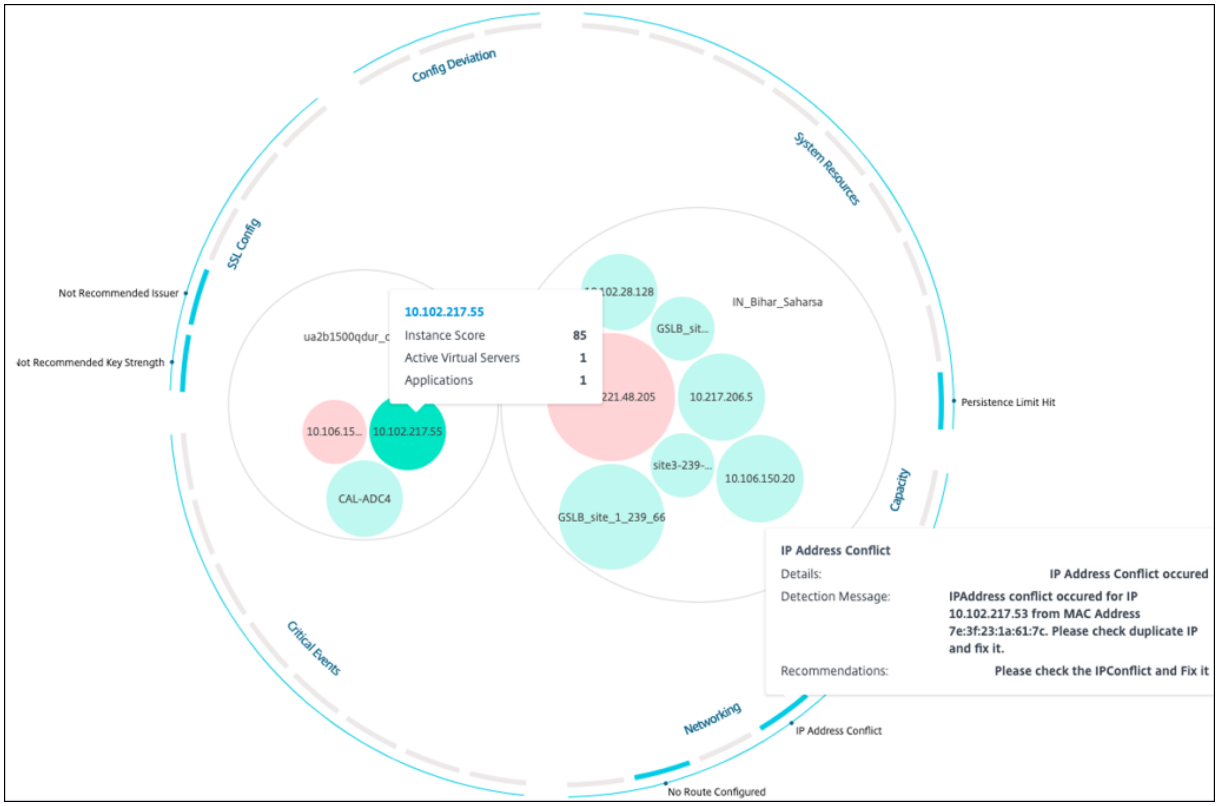
Vue tabulaire

Vous pouvez également afficher les anomalies à l'aide de l'option Vue tabulaire dans **Infrastructure Analytics**. Accédez à **Réseaux** > **Analyse de l'infrastructure**, puis cliquez sur la pour afficher toutes les instances gérées. Cliquez sur › pour plus de détails.



Afficher les détails d'une anomalie

Par exemple, si vous souhaitez afficher les détails d'un **conflit d'adresses IP** sur le réseau, cliquez sur l'anomalie qui s'affiche pour le conflit d'adresses IP pour afficher les détails.



- **Détails** - Indique quelle anomalie est détectée
- **Message de détection** - Indique l'adresse MAC pour laquelle l'adresse IP a le conflit

- **Recommandations** - Indique l'élément d'action pour résoudre ce conflit d'adresse IP

FAQ

February 1, 2024

Cette section fournit la FAQ sur les fonctionnalités suivantes de Citrix Application Delivery Management (Citrix ADM). Cliquez sur le nom d'une fonctionnalité dans le tableau suivant pour afficher la liste des questions fréquentes relatives à cette fonctionnalité.

Analytics	Authentification	Gestion de la configuration
Gestion des certificats	Déploiement	Déploiement (reprise après sinistre)
Gestion des événements	Gestion des instances	StyleBooks
Gestion du système		

Analytics

Est-il nécessaire d'activer le canal virtuel EUEM sur les instances Citrix Gateway déployées en mode à saut unique ?

Les données de canal virtuel EUEM font partie des données HDX Insight que Citrix ADM reçoit des instances de Gateway. Le canal virtuel EUEM fournit les données sur ICA RTT. Si le canal virtuel EUEM n'est pas activé, les données HDX Insight restantes sont toujours affichées sur Citrix ADM.

Le canal virtuel EUEM est un service par défaut exécuté sur des applications Citrix Virtual Desktop (VDA). S'il n'est pas en cours d'exécution, démarrez le processus « Citrix End User Experience Monitoring » dans les services VDA.

Comment activer Citrix ADM pour surveiller le trafic des applications Web et des postes de travail virtuels ?

1. Accédez à **Infrastructure** > **Instances** > **Citrix ADC**, puis sélectionnez l'instance Citrix ADC sur laquelle vous souhaitez activer Analytics.
2. Dans la liste **Sélectionner une action**, sélectionnez **Configurer Analytics**.

3. Dans la page **Configurer Analytics** qui s'ouvre, sélectionnez tous les serveurs virtuels sur lesquels vous souhaitez activer les analyses, puis cliquez sur **Activer AppFlow**. Pour plus de détails, consultez Comment activer Analytics sur les instances.

> Remarque
>
> Pour les instances Citrix ADC de version 11.0, version 65.30 et versions ultérieures, il n'existe aucune option sur Citrix ADM pour activer Security Insight explicitement. Assurez-vous de configurer les paramètres AppFlow sur les instances Citrix ADC, de sorte que Citrix ADM commence à recevoir le trafic Security Insight avec le trafic Web Insight. Pour plus d'informations sur la façon de définir les paramètres AppFlow sur les instances Citrix ADC, consultezPour définir les paramètres AppFlow à l'aide de l'utilitaire de configuration.

Après avoir ajouté les instances de Citrix ADC, Citrix ADM commence-t-il automatiquement à collecter des informations analytiques ?

Non. Activez l'analyse sur les serveurs virtuels hébergés dans les instances Citrix ADC qui sont gérées par Citrix ADM. Pour plus de détails, consultez Comment activer les analyses sur les instances .

Est-il nécessaire d'accéder à l'appliance Citrix ADC individuelle pour activer l'analyse ?

Non. Toute la configuration est effectuée à partir de l'interface utilisateur Citrix ADM, qui répertorie les serveurs virtuels hébergés sur l'instance Citrix ADC spécifique. Pour plus de détails, consultez Comment activer les analyses sur les instances .

Quels sont les types de serveurs virtuels qui peuvent être répertoriés sur une instance Citrix ADC pour activer les analyses ?

Actuellement, l'interface utilisateur de Citrix ADM répertorie les serveurs virtuels suivants pour activer les analyses :

- Serveur virtuel d'équilibrage de charge
- Serveur virtuel de commutation de contenu
- Serveur virtuel VPN
- Serveur virtuel de redirection de cache

Comment attacher un disque supplémentaire à Citrix ADM ?

Pour attacher un disque supplémentaire à Citrix ADM :

1. Arrêtez la machine virtuelle Citrix ADM.

2. Dans l'hyperviseur, attachez un disque supplémentaire de la taille de disque requise à la machine virtuelle Citrix ADM.

   Par exemple, Considérons que vous souhaitez augmenter l'espace disque à 200 Go, dans une machine virtuelle Citrix ADM de 120 Go. Dans ce scénario, vous devez associer un espace disque de 200 Go au lieu de 80 Go. Les 200 Go d'espace disque nouvellement attachés seront utilisés pour stocker les données de base de données, les fichiers journaux Citrix ADM. L'espace disque existant de 120 Go est utilisé pour stocker les fichiers principaux, les fichiers journaux du système d'exploitation, etc.

3. Démarrez la machine virtuelle Citrix ADM.

Que voulez-vous dire par les collecteurs ne sont pas configurés sur les instances Citrix ADC ?

Un collecteur reçoit les enregistrements AppFlow générés par l'appliance Citrix ADC.

Citrix ADM reçoit le trafic Security Insight et Web Insight des instances Citrix ADC lorsque la fonctionnalité AppFlow est activée. Lorsque vous activez la fonctionnalité AppFlow sur une instance Citrix ADC, vous devez spécifier au moins un collecteur auquel les enregistrements AppFlow sont envoyés. Si les collecteurs ne sont pas configurés sur les instances Citrix ADC, Citrix ADM ne reçoit pas le trafic provenant des instances.

Par exemple, cinq instances Citrix ADC sont ajoutées à Citrix ADM. Si aucun collecteur n'est spécifié pour deux instances, aucun trafic ne circule vers Citrix ADM. Les diagnostics en libre-service détectent le problème et affichent le problème comme « Les collecteurs ne sont pas configurés sur 2 instances. »

Pour plus d'informations sur la façon de configurer la fonctionnalité AppFlow, consultez Configuration de la fonctionnalité AppFlow.

Qu'est-ce que l'activation des mesures côté client ?

Lorsque les mesures côté client sont activées, ADM capture les mesures de temps de chargement et de rendu des pages HTML par injection HTML. À l'aide de ces mesures, les administrateurs peuvent identifier les problèmes de latence L7.

Authentification

Qu'est-ce que l'équilibrage de charge des demandes d'authentification ?

La fonction d'équilibrage de charge du serveur d'authentification permet à Citrix ADM d'équilibrer la charge des demandes d'authentification qui sont dirigées vers les serveurs d'authentification ex-

ternes. L'équilibrage de charge des serveurs d'authentification garantit que la charge d'authentification est répartie entre plusieurs serveurs d'authentification et évite ainsi la surcharge d'un serveur d'authentification. Vous pouvez créer un service d'authentification pour vous connecter à votre serveur d'authentification externe existant et obtenir des informations utilisateur à partir de celui-ci à l'aide de protocoles d'authentification tels que LDAP, RADIUS ou TACACS.

Pourquoi avons-nous besoin de mettre en cascade des serveurs d'authentification externes ?

Les serveurs d'authentification externes en cascade fournissent un traitement d'authentification ininterrompu, permettant l'accès aux utilisateurs légitimes en cas de défaillance d'un serveur d'authentification. Il n'existe aucune limite quant aux types de serveurs d'authentification que vous pouvez mettre en cascade. Vous pouvez disposer de tous les serveurs RADIUS, de tous les serveurs LDAP ou d'une combinaison de serveurs RADIUS et LDAP.

Combien de serveurs d'authentification externes puis-je mettre en cascade ?

Vous pouvez mettre en cascade jusqu'à 32 serveurs d'authentification externes dans Citrix ADM.

Ai-je une alternative lorsque l'authentification externe échoue ?

Il peut arriver que l'authentification externe échoue complètement, même si vous avez monté en cascade plusieurs serveurs. Par exemple, les serveurs externes peuvent devenir inaccessibles ou les informations d'identification d'un nouvel utilisateur peuvent n'avoir été saisies dans aucun des serveurs d'authentification externes. Pour empêcher le verrouillage des utilisateurs dans une telle situation, vous pouvez activer l'authentification locale de secours. Pour plus de détails, consultez Authentification locale de secours.

Qu'est-ce que l'authentification locale de secours ?

L'authentification locale de secours est une option permettant d'authentifier vos utilisateurs localement en cas d'échec de l'authentification externe. Si l'authentification externe échoue, Citrix ADM accède à la base de données utilisateur locale pour authentifier vos utilisateurs.

Dans Citrix ADM, accédez à **Système** > **Authentification** > **Configuration de l'authentification**. Sur cette page, vous pouvez ajouter plusieurs serveurs d'authentification externes en cascade et sélectionner l'option **Activer l'authentification locale de secours**.

Qu'est-ce qu'une extraction de groupes d'utilisateurs externes ?

Si vous avez ajouté des serveurs externes pour authentifier les utilisateurs, vous pouvez importer (extraire) des groupes d'utilisateurs existants dans Citrix ADM. Vous devez importer des groupes d'utilisateurs une seule fois et leur accorder une autorisation de groupe plutôt que d'importer des utilisateurs individuels et de leur accorder des autorisations individuelles. Il n'est pas nécessaire de recréer les utilisateurs sur Citrix ADM.

Pourquoi devons-nous attribuer des autorisations de groupe ?

Lorsque vous utilisez la fonctionnalité d'équilibrage de charge de Citrix ADC, vous pouvez intégrer Citrix ADM à des serveurs d'authentification externes et importer des informations de groupe d'utilisateurs à partir des serveurs d'authentification. Connectez-vous à Citrix ADM et créez manuellement les mêmes informations de groupe dans Citrix ADM et attribuez des autorisations à ces groupes. L'autorisation utilisateur et groupe d'utilisateurs est gérée dans Citrix ADM et non dans le serveur externe. Les utilisateurs disposent de différentes autorisations d'accès basées sur les rôles sur les serveurs externes. Configurez également les mêmes autorisations pour les utilisateurs dans Citrix ADM. Au lieu de configurer les autorisations individuellement pour chaque utilisateur, vous pouvez configurer une autorisation au niveau du groupe afin que les membres du groupe d'utilisateurs puissent accéder à des services spécifiques sur les serveurs virtuels à charge équilibrée. Les autorisations typiques que vous pouvez attribuer sont des autorisations pour gérer les instances Citrix ADC, les instances Citrix SDX, les serveurs virtuels, etc., afin que les utilisateurs de ce groupe puissent gérer uniquement ces instances ou serveurs virtuels. Vous pouvez modifier ultérieurement les autorisations accordées aux utilisateurs au niveau du groupe. Vous pouvez même supprimer un ou plusieurs groupes d'utilisateurs ; les autres utilisateurs du groupe continuent de fonctionner sur Citrix ADM.

Gestion de la configuration

Puis-je effectuer la configuration de plusieurs instances Citrix ADC simultanément à l'aide de Citrix ADM ?

Oui, vous pouvez utiliser des tâches de configuration pour effectuer la configuration sur plusieurs instances de Citrix ADC.

Que sont les tâches de configuration sur Citrix ADM ?

Une tâche est un ensemble de commandes de configuration que vous pouvez créer et exécuter sur une ou plusieurs instances gérées. Vous pouvez créer des tâches pour apporter des modifications de configuration entre les instances, répliquer les configurations sur plusieurs instances de votre réseau

et enregistrer et lire des tâches de configuration à l'aide de l'interface utilisateur graphique Citrix ADM. Vous pouvez également convertir les tâches enregistrées en commandes CLI.

Vous pouvez utiliser la fonctionnalité Travaux de configuration de Citrix ADM pour créer une tâche de configuration, envoyer des notifications par e-mail et vérifier les journaux d'exécution des tâches créées.

Puis-je planifier des tâches à l'aide de modèles intégrés dans Citrix ADM ?

- Oui ! Vous pouvez planifier une tâche à l'aide de l'option de modèle intégrée. Une tâche est un ensemble de commandes de configuration que vous pouvez exécuter sur une ou plusieurs instances gérées. Par exemple, vous pouvez utiliser l'option de modèle intégrée pour planifier une tâche de configuration des serveurs syslog. Vous pouvez choisir d'exécuter le travail immédiatement ou de planifier l'exécution ultérieure.

Vous pouvez enregistrer la configuration d'une tâche créée précédemment et l'exécuter à nouveau après avoir modifié les commandes, les paramètres, la source de configuration et les instances ciblées. Ceci est utile lorsque le même ensemble de commandes doit être exécuté sur une instance différente, ou lorsque le travail rencontre une erreur et arrête l'exécution ultérieure.

Gestion des certificats

La suppression des certificats SSL de Citrix ADM conduit-elle à la suppression des certificats des instances Citrix ADC ?

Non

Déploiement

Quels sont le nom d'utilisateur et le mot de passe par défaut ?

- Une fois la configuration réseau initiale terminée, vous pouvez vous connecter à Citrix ADM à partir de l'hyperviseur ou de la console SSH, en utilisant le nom d'utilisateur et le mot de passe par défaut (nsrecover/nsroot).
- Le nom d'utilisateur et le mot de passe par défaut pour se connecter à partir de l'interface graphique sont *nsroot/nsroot*.

Comment modifier le mot de passe par défaut ?

Pour modifier le mot de passe :

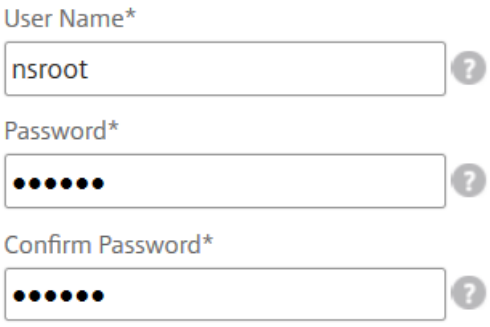
1. Dans Citrix ADM, accédez à **Système** > **Administration des utilisateurs** > **Utilisateurs**.

   La page Utilisateurs s'affiche.

2. Sélectionnez le nom d'utilisateur **nsroot** et cliquez sur **Modifier**.

   La page Configurer l'utilisateur système s'affiche.

3. Sélectionnez **Modifier le mot de passe** et créez un mot de passe de votre choix.



4. Cliquez sur **OK**.

   Vous pouvez maintenant utiliser le nouveau mot de passe pour vous connecter à partir de l'interface graphique et de l'Hypervisor ou de la console SSH.

   > Remarque
   >
   > Vous ne pouvez pas modifier le nom d'utilisateur.

Comment réinitialiser le mot de passe ?

Vous pouvez consulter cette documentation pour réinitialiser le mot de passe.

Dans une paire HA, si le mot de passe est modifié dans le nœud principal et si l'option Break HA paire est sélectionnée ultérieurement, quel est le comportement ?

Vous pouvez vous connecter aux deux nœuds autonomes à l'aide de votre nouveau mot de passe.

Si deux serveurs autonomes ont des mots de passe différents, quel est l'impact du déploiement de ces deux serveurs en paire HA ?

Il est recommandé d'avoir un mot de passe par défaut pour les deux serveurs lorsque vous déployez deux serveurs autonomes sur une paire HA.

La configuration HA est terminée, mais l'interface utilisateur du nœud principal n'est pas accessible. Quelle peut être la raison ?

Quelques minutes sont nécessaires pour que la configuration soit prise en compte. Vous pouvez réessayer d'y accéder au bout de quelques minutes.

La configuration HA est terminée, mais l'interface graphique de l'adresse IP flottante n'est pas accessible. Quelle peut être la raison ?

Après la configuration de la haute disponibilité, vous devez d'abord accéder à l'interface graphique du nœud principal et terminer le déploiement. Pour plus d'informations, consultez Déployer le nœud principal et le nœud secondaire en tant que paire haute disponibilité. Une fois le déploiement terminé, le serveur redémarre et se prépare pour le déploiement haute disponibilité. Vous pouvez ensuite accéder à l'interface graphique de l'adresse IP flottante.

Quelle base de données est prise en charge dans Citrix ADM autonome et Citrix ADM HA ?

Citrix ADM autonome et Citrix ADM HA prennent en charge PostgreSQL.

Quelle est la perte de données potentielle pour le nœud secondaire ?

Le nœud secondaire écoute les messages de pulsation que le nœud principal envoie via la base de données Citrix ADM. Si le nœud secondaire ne reçoit pas les pulsations pendant plus de 180 secondes, le nœud secondaire effectue une vérification basée sur SSH sur le nœud principal. Si le battement de cœur et la vérification basée sur SSH échouent, le nœud principal est considéré comme étant hors service.

Dans ce scénario, le nœud secondaire prend le relais en tant que nœud principal et la période de 180 secondes peut être considérée comme la perte de données possible pour le nœud secondaire.

Que se passe-t-il si le nœud principal est en panne ?

Le nœud secondaire prend le relais et devient le nœud principal.

Comment réinstaller le nœud défaillant ?

Il est recommandé d'installer une nouvelle version de machine virtuelle. Pour réinstaller :

1. Brisez la paire HA. Accédez à **Système** > **Déploiement**

   La page de déploiement s'affiche. Cliquez sur **Break HA**
2. Supprimez le nœud défaillant de l'Hypervisor.
3. Importez le fichier image .XVA dans l'hyperviseur.
4. Dans l'onglet Console, configurez Citrix ADM avec les configurations réseau initiales. Pour plus d'informations, consultez Enregistrer et déployer le premier serveur (nœud principal) et Enregistrer et déployer le deuxième serveur (nœud secondaire).
5. Redéployez la paire HA.

Citrix ADM prend-il en charge le stockage SAN ?

Citrix vous recommande d'héberger le disque dur virtuel Citrix ADM sur un stockage local. Lorsqu'il est hébergé sur des périphériques de stockage dans un SAN, Citrix ADM peut ne pas fonctionner comme prévu. Le déploiement d'ADM sur le SAN n'est donc pas pris en charge.

Citrix ADM prend en charge un disque supplémentaire ?

Oui. Une nouvelle installation de la paire Citrix ADM HA alloue 120 Go de stockage par défaut. Pour plus de 120 Go de stockage, vous pouvez ajouter un disque supplémentaire pour un maximum de 3 To de stockage. L'ajout de plusieurs disques supplémentaires n'est pas pris en charge.

Après avoir désactivé la paire HA, qu'advient-il de l'adresse IP flottante configurée ?

L'adresse IP flottante n'est plus accessible et vous devez redéployer la paire haute disponibilité.

Puis-je donner une autre adresse IP flottante pendant le redéploiement ?

Oui. Vous pouvez configurer une nouvelle adresse IP flottante.

Pourquoi l'interface utilisateur du nœud secondaire n'est-elle pas accessible ?

Le nœud secondaire est uniquement un serveur de réplica en lecture et agit en tant que nœud principal uniquement si le nœud principal est en panne pour une raison quelconque. Citrix recommande

d'accéder à l'interface utilisateur du nœud principal ou à l'interface graphique de l'adresse IP flottante.

Si le nœud principal est hors service pendant une longue période, les configurations peuvent-elles toujours être effectuées à l'aide de l'interface graphique d'adresse IP flottante ?

Oui. Vous pouvez continuer à effectuer des configurations et les configurations sont enregistrées dans le nœud secondaire. Après le retour du nœud principal, toutes les configurations sont synchronisées.

S'il est nécessaire de modifier l'adresse IP du nœud principal ou l'adresse IP du nœud secondaire ou l'adresse IP flottante à l'avenir (par exemple, en la changeant en IPv6), quelles sont les solutions recommandées ?

La modification des adresses IP dans la paire HA n'est pas prise en charge sans casser la paire HA.

Pour mettre à jour l'adresse IP du nœud principal ou du nœud secondaire :

1. Brisez la paire HA. Accédez à **Système** > **Déploiement**.

   La page Déploiement s'affiche. Cliquez sur **Break HA**

   a) Ouvrez une session sur le nœud principal à l'aide d'un client SSH ou à partir de l'hyperviseur.

   b) Utilisez `nsrecover` comme nom d'utilisateur et entrez le mot de passe que vous avez défini.

   c) Entrez **networkconfig**. Exécutez la procédure de l'**étape 3** disponible dans Enregistrer et déployer le premier serveur (nœud principal).

      Lors de la configuration réseau initiale, vous pouvez fournir une adresse IP différente.

   d) Effectuez la même procédure pour le nœud secondaire et continuez avec la procédure de l'**étape 3** disponible dans Enregistrer et déployer le deuxième serveur (nœud secondaire).

Pour mettre à jour l'adresse IP flottante :

1. Accédez à **Système** > **Déploiement**.

   La page Déploiement s'affiche.

   a) Cliquez sur **Paramètres HA**.

   b) Cliquez sur **Configurer l'adresse IP flottante pour le mode haute disponibilité**.

   c) Entrez l'adresse IP flottante et cliquez sur **OK**.

ADM prend en charge les processeurs AMD ?

Non. ADM ne prend pas en charge les processeurs AMD.

Déploiement (reprise après sinistre)

Quelle est la fréquence de la réplication entre le site principal et le site de reprise après sinistre ?

La réplication entre le site principal et le site de reprise après sinistre s'effectue en temps réel.

Après avoir lancé le script de sauvegarde sur le site de reprise après sinistre, le site de reprise après sinistre devient-il le site principal temporaire, jusqu'à ce que le site principal soit restauré et pleinement opérationnel ?

Non. Le site de reprise après sinistre deviendra désormais le site principal. Pour rétablir la paire HA en tant que site principal, reportez-vous à la section Rétablir les configurations sur le site principal d'origine

Si l'option Break HA paire est sélectionnée, les deux nœuds fonctionnent comme un serveur autonome. Étant donné que la prise en charge de la reprise après sinistre ne s'applique pas au serveur autonome, qu'advient-il du site DR si la paire Break HA est sélectionnée

Si vous sélectionnez l'option Break HA pair, la réplication entre le site principal et le site DR est interrompue. Vous devez reconfigurer le site DR dans le cadre du redéploiement de la paire HA.

Gestion des événements

Comment puis-je suivre tous les événements qui ont été générés sur mes instances Citrix ADC gérées à l'aide de Citrix ADM ?

En tant qu'administrateur réseau, vous pouvez afficher des détails tels que les modifications de configuration, les conditions de connexion, les défaillances matérielles, les violations de seuil et les changements d'état d'entité sur vos instances Citrix ADC, ainsi que les événements et leur gravité sur des instances spécifiques. Vous pouvez utiliser le tableau de bord des événements Citrix ADM pour afficher les rapports générés pour les détails de gravité des événements critiques sur toutes vos instances Citrix ADC.

Quelles sont les règles de l'événement ?

À l'aide de Citrix ADM, vous pouvez configurer des règles pour surveiller des événements spécifiques. Les règles d'événement facilitent la surveillance d'un grand nombre d'événements générés dans votre infrastructure Citrix ADM.

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 la gravité, les instances Citrix ADC, la catégorie et les objets de défaillance. Les actions que vous pouvez attribuer aux événements sont l'envoi d'une notification par e-mail, le transfert d'interruptions SNMP depuis les instances Citrix ADC gérées vers Citrix ADM et l'envoi d'une notification par SMS.

Gestion des instances

Que se passe-t-il si une instance ADC ne peut pas se connecter à ADM après l'allocation de bande passante lorsque vous utilisez des licences de capacité groupées Citrix ADC ?

Si le rythme cardiaque entre l'instance ADC et ADM échoue, l'instance entre une période de grâce de 30 jours. Et une fois la communication rétablie, les licences de capacité groupée commencent à fonctionner. En période de grâce, les fonctions ADC ne sont pas affectées. Après 30 jours de délai de grâce, l'instance ADC lance un redémarrage à chaud et n'est pas sous licence.

Que sont les centres de données dans Citrix ADM ?

Un centre de données Citrix ADM est un regroupement logique des instances de Citrix ADC dans un emplacement géographique spécifique. Chaque serveur peut surveiller et gérer plusieurs instances Citrix ADC au sein d'un datacenter. Vous pouvez utiliser le serveur Citrix ADM pour gérer des données telles que syslog, le flux de trafic d'application et les interruptions SNMP à partir des instances gérées. Pour plus d'informations sur la configuration des centres de données, voir Procédure de configuration des centres de données pour les géomaps dans Citrix ADM.

Quels sont les différents appareils Citrix pris en charge par Citrix ADM ?

Les instances sont les appliances Citrix ou les appliances virtuelles que vous souhaitez découvrir, gérer et surveiller à partir de Citrix ADM. Vous devez ajouter ces instances au serveur Citrix ADM. Vous pouvez ajouter les appliances Citrix et les appliances virtuelles suivantes à Citrix ADM :

- Citrix MPX

- Citrix VPX
- Citrix SDX
- Citrix CPX
- Citrix Gateway
- Citrix SD-WAN WO
- Citrix SD-WAN PE

Vous pouvez ajouter des instances lors de la configuration du serveur Citrix ADM pour la première fois ou plus tard.

Qu'est-ce qu'un profil d'instance ?

Un profil d'instance est utilisé par Citrix ADM pour accéder à une instance.

Un profil d'instance contient le nom d'utilisateur et le mot de passe permettant d'accéder à une ou plusieurs instances. Un profil par défaut est disponible pour chaque type d'instance. Par exemple, le profil ns-root-profile est le profil par défaut pour les instances Citrix ADC. Il contient les informations d'identification de l'administrateur Citrix ADC par défaut. Lorsque vous modifiez les informations d'identification requises pour accéder aux instances, vous pouvez définir des profils d'instance personnalisés pour ces instances.

Pouvons-nous ajouter un nombre illimité d'instances SD-WAN dans Citrix ADM ? Citrix ADM peut-il gérer tous les compteurs scalaires et vectoriels pour le SD-WAN ?

Actuellement, il n'existe aucune limite de licence sur les instances SD-WAN pouvant être ajoutées à Citrix ADM. Citrix ADM dispose d'un ensemble de rapports intégrés qui interrogent en interne les compteurs scalaires et vectoriels.

Puis-je redécouvrir plusieurs instances Citrix VPX dans Citrix ADM ?

Oui, vous pouvez redécouvrir plusieurs instances Citrix **VPX** dans Citrix ADM pour connaître les derniers états et configurations des instances.

Accédez à **Réseaux** > **Instances** > **Citrix ADC > VPX,** sélectionnez les instances à redécouvrir, puis dans la liste **Action**, cliquez sur **Redécouvrir**. Pour plus d'informations, consultez Comment redécouvrir plusieurs instances VPX.

Citrix ADM peut-il être installé sur Citrix SDX ?

Non

Puis-je ajouter une instance Citrix ADC sur le logiciel ADM à l'aide d'une adresse IP publique ?

Oui, vous pouvez utiliser la traduction d'adresses réseau (NAT).

- Pour ajouter une instance unique : utilisez l'adresse IP NAT de l'adresse IP publique de l'instance ADC.
- Pour ajouter une paire HA ADC : ajoutez les adresses IP NAT de la paire HA au format suivant :

  <NAT **public** IP of the primary instance>#<NAT **public** IP of the secondary instance>

- Pour ajouter un cluster ADC : ajoutez toutes les adresses IP publiques NAT de toutes les instances du cluster, séparées chacune par une virgule, et ajoutez l'IP NAT de l'IP du CLUSTER entre parenthèses ou crochets. Un exemple de format : NAT1, NAT2, NAT3, (NATIP ou CLUSTERIP).

Pour plus d'informations, consultez les rubriques suivantes :

- Ajouter des instances à Citrix ADM
- Configuration de la traduction d'adresses réseau

Comment enregistrer un nœud de reprise après sinistre si les informations d'identification du nœud DR sont modifiées ?

Réinitialisez les informations d'identification du nœud de reprise après sinistre (DR) sur `nsrecover` /`nsroot` à l'aide de la commande suivante :

```
./mps/change_freebsd_password.sh <username> <password>
<!--NeedCopy-->
```

Pour enregistrer un nœud DR, suivez les étapes décrites dans Déployer et enregistrez le nœud de reprise après sinistre Citrix ADM à l'aide de la console DR.

StyleBooks

Peut-on utiliser StyleBooks pour configurer différentes instances Citrix ADC exécutées sur différentes versions du logiciel Citrix ADC ?

Oui, vous pouvez utiliser StyleBooks pour configurer différentes instances Citrix ADC exécutées sur différentes versions s'il n'y a pas d'écart entre les commandes d'une version différente.

Lorsqu'un StyleBook est utilisé pour configurer plusieurs instances Citrix ADC en même temps et que la configuration d'une instance Citrix ADC échoue, que se passe-t-il ?

Si l'application de la configuration à une instance Citrix ADC échoue, la configuration n'est pas appliquée à d'autres instances et les configurations déjà appliquées sont annulées.

Les sauvegardes Citrix ADC effectuées via Citrix ADC incluent-elles des configurations appliquées via StyleBooks ?

Oui

Gestion du système

Puis-je attribuer un nom d'hôte à mon serveur Citrix ADM ?

Oui, vous pouvez attribuer un nom d'hôte pour identifier votre serveur Citrix ADM. Pour attribuer un nom d'hôte, accédez à**Système**>**Administration système**>**Paramètres système**, puis cliquez sur**Modifier le nom d'hôte**.

Le nom d'hôte s'affiche sur la licence universelle pour Citrix ADM. Pour plus d'informations, consultez Comment attribuer un nom d'hôte à un serveur Citrix ADM.

Puis-je sauvegarder et restaurer ma configuration Citrix ADM ?

Oui, vous pouvez sauvegarder les fichiers de configuration (fichiers NTP et certificats SSL), les données système, les données d'infrastructure et d'application, ainsi que tous vos paramètres **SNMP**. Si votre Citrix ADM devient instable, vous pouvez utiliser les fichiers sauvegardés pour restaurer votre Citrix ADM à un état stable.

Pour sauvegarder et restaurer votre configuration Citrix ADM, accédez à **Système** > **Paramètres avancés** > **Fichiers de sauvegarde**, puis cliquez sur **Sauvegarder** ou **Restaurer** selon le cas. Pour plus d'informations, consultez Comment sauvegarder et restaurer la configuration sur Citrix ADM.

Citrix vous recommande d'utiliser cette fonctionnalité avant d'effectuer une mise à niveau ou pour des raisons de précaution.

Que sont les seuils et les alertes sur Citrix ADM ?

Vous pouvez définir des seuils et des alertes pour surveiller l'état d'une instance Citrix ADC et surveiller les entités sur les instances gérées.

Lorsque la valeur d'un compteur dépasse le seuil, Citrix ADM génère une alerte signalant un problème lié aux performances. Lorsque la valeur du compteur revient à la valeur d'effacement spécifiée dans le seuil, l'événement est annulé.

Puis-je générer un fichier de support technique pour Citrix ADM ?

Oui. Citrix vous recommande de générer une archive des données et des statistiques Citrix ADM avant de contacter le support technique pour déboguer un problème. L'archive est un fichier TAR que vous pouvez envoyer à l'équipe de support technique.

Vous pouvez générer un fichier de support technique contenant des journaux de débogage, la durée de collecte des journaux de débogage et des journaux distincts et divers de la base de données Citrix ADM.

Pour configurer et envoyer un fichier de support technique, accédez à**Système** >**Diagnostics** >**Support technique**, puis cliquez sur**Générer un fichier de support technique**. Pour plus d'informations, consultez Comment générer un fichier de support technique pour Citrix ADM.

Qu'est-ce que la purge de syslog ?

Syslog est un protocole standard pour la journalisation. Syslog permet d'isoler le système qui génère les informations et le système qui stocke les informations. Vous pouvez consolider les informations de journalisation et obtenir des informations à partir des données collectées. Vous pouvez également configurer syslog pour consigner différents types d'événements.

Pour limiter la quantité de données syslog stockées dans la base de données, vous pouvez spécifier l'intervalle suivant lequel vous souhaitez purger les données syslog. Vous pouvez spécifier le nombre de jours après lesquels toutes les données Syslog génériques, AppFirewall et Citrix Gateway seront supprimées de Citrix ADM.

Puis-je configurer le serveur NTP sur Citrix ADM ?

Vous pouvez configurer un serveur NTP (Network Time Protocol) dans Citrix ADM pour synchroniser l'horloge Citrix ADM avec le serveur NTP. La configuration d'un serveur NTP garantit que l'horloge Citrix ADM possède les mêmes paramètres de date et d'heure que les autres serveurs du réseau.

Pour configurer un serveur NTP, accédez à **Système** > **Serveurs NTP**, puis cliquez sur **Ajouter**. Pour plus d'informations, consultez Comment configurer le serveur NTP sur Citrix ADM.

À partir de quelle version le déploiement HA actif-passif Citrix ADM est-il pris en charge ?

Le mode de déploiement HA actif-passif de Citrix ADM est pris en charge à partir de Citrix ADM version 12.0 build 51.24.

J'avais une configuration HA active-active Citrix ADM et j'avais configuré une appliance Citrix ADC avec un serveur virtuel d'équilibrage de charge dessus pour un accès unifié à l'interface utilisateur graphique. Comment mettre à jour cette configuration ?

Après avoir mis à niveau la paire Citrix ADM HA en mode actif-passif, vous devez exécuter la commande suivante sur l'appliance Citrix ADC pour mettre à jour la configuration de l'équilibrage de charge :

add lb monitor MAS_Monitor **TCP-ECV -send "GET /mas_health HTTP/1.1\r\nAccept-Encoding: identity\r\nUser-Agent: NetScaler-Monitor\r\nConnection: close\r\n\r\n\" "-recv "{\"status-code\":0, \"is_passive\":0}"-LRTM DISABLED**

Puis-je configurer l'équilibrage de charge de la paire Citrix ADM HA sur une instance Citrix ADC à l'aide du port 443 ?

Non, vous ne pouvez pas configurer l'équilibrage de charge de la paire Citrix ADM HA sur une instance Citrix ADC à l'aide du port 443.

Lorsque vous configurez les moniteurs `http-ecv` et `https-ecv` sur Citrix ADC, il ne surveille pas correctement les nœuds Citrix ADM HA.

Un fichier de sauvegarde du serveur Citrix ADM peut-il être utilisé pour restaurer la configuration d'un autre serveur Citrix ADM ?

Oui

Une fois que Citrix ADM a sauvegardé une instance Citrix ADC, ce fichier de sauvegarde peut-il être utilisé pour restaurer la configuration d'une autre instance Citrix ADC via Citrix ADM ?

Oui. Téléchargez le fichier de sauvegarde Citrix ADM, téléchargez-le dans le référentiel de sauvegarde d'une autre instance Citrix ADC et restaurez cette instance. Assurez-vous que les informations réseau et les informations d'authentification ne sont pas en conflit. Par exemple, vérifiez les conflits d'adresse IP ou de port, ainsi que les profils de mots de passe incompatibles. Assurez-vous également que l'instance VPX restaurée possède la même adresse NSIP et la même licence Citrix ADC que celle qui a été sauvegardée.

Avant de restaurer une instance dans une paire de haute disponibilité, assurez-vous que les adresses IP et l'état (primaire ou secondaire) stockés dans le fichier de sauvegarde correspondent à ceux de la configuration HA d'origine. Vérifiez également que les nouvelles licences principales et secondaires possèdent le même type de licence Citrix ADC.

Pouvons-nous forcer Citrix ADM à utiliser une adresse SNIP pour communiquer avec les instances Citrix ADC, au lieu d'utiliser l'adresse NSIP du serveur Citrix ADM ?

Oui, vous pouvez ajouter une adresse SNIP (avec la gestion activée) dans Citrix ADM pour la communication avec les instances Citrix ADC.

Lorsque je sauvegarde des instances Citrix ADC dans Citrix ADM, le résultat est-il une sauvegarde complète ou une sauvegarde de base ?

Les sauvegardes des instances de Citrix ADC par Citrix ADM sont des sauvegardes complètes.

Existe-t-il un guide de dépannage pour Citrix ADM ?

Oui. Voir https://support.citrix.com/article/CTX224502.

Comment les instances Citrix ADC sont-elles gérées lors d'un basculement sur incident Citrix ADM HA ?

Si la vérification basée sur les pulsations et SSH échoue, le nœud principal est considéré comme inactif et le nœud secondaire prend le relais en tant que nœud principal. Toutes les instances de Citrix ADC sont mises à jour avec les derniers détails du nœud principal comme destination d'interruption SNMP par défaut.

Le nouveau nœud principal (actif) Citrix ADM vérifie si le nœud précédemment actif a été configuré en tant que collecteur AppFlow ou serveur syslog. Si tel était le cas, le nouveau serveur principal ajoute les détails du collecteur AppFlow ou du serveur syslog aux informations envoyées aux instances.

Pour syslog, il remplace les anciens détails du serveur.

Que se passe-t-il lorsque le nœud Citrix ADM HA qui est tombé en panne revient en panne ?

Après la remise en service, le nœud Citrix ADM reste passif sauf si le nœud actif bascule

Comment les instances Citrix ADC sont-elles distribuées sur les nœuds Citrix ADM HA ?

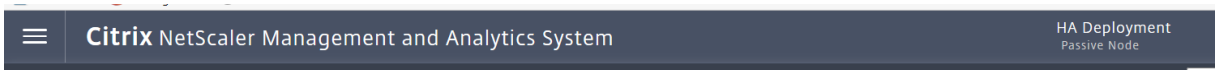
Toutes les instances Citrix ADC sont gérées par le nœud Citrix ADM principal.

Comment les licences de serveur virtuel sont-elles gérées en cas de basculement sur incident Citrix ADM HA ?

Si le nœud principal Citrix ADM sur lequel les licences de serveur virtuel sont appliquées tombe en panne, le nouveau nœud principal gère les licences de serveur virtuel pendant une période de grâce de 30 jours. Appliquez de nouveau les licences sur le nouveau système principal avant la fin de la période de grâce. Pour d'autres solutions, contactez le support Citrix.

Un équilibreur de charge est-il obligatoire pour une installation Citrix ADM HA ?

Non, mais s'il n'y a pas d'équilibrage de charge, les nœuds Citrix ADM doivent être accessibles via leurs propres adresses IP. Le nœud passif est marqué par la balise « Passif », et Citrix recommande de ne pas créer de configuration sur le nœud passif.



Citrix ADM prend-il en charge une base de données externe ?

Non

Une instance Citrix ADC gérée par Citrix ADM peut-elle être utilisée comme équilibreur de charge pour Citrix ADM HA ?

Oui

Quelles données sont synchronisées entre les nœuds Citrix ADM HA ?

La base de données Citrix ADM complète est synchronisée et les dossiers suivants sont synchronisés :

- /var/mps/tenants/root/
- /var/mps/ns_images/
- /var/mps/sdx_images/
- /var/mps/xen_nsvpx_images/
- /var/mps/cbwanopt_images/

- /var/mps/sdwanvw_images/
- /var/mps/mps_images/
- /var/mps/ssl_certs/
- /var/mps/ssl_keys/
- /mpsconfig/ssl/
- /var/mps/sauvegarde/
- /var/mps/esx_nsvpx_images/
- /var/mps/locdb/