NetScaler Application Delivery Management 14.1

Machine translated content

Disclaimer

Contents

Notes de publication

February 1, 2024

Les notes de mise à jour de NetScaler Application Delivery Management (ADM) 14.1 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 14.1 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.

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

Notes de mise à jour pour la version 14.1-12.34 de NetScaler ADM

February 1, 2024

Ce document de notes de version décrit les améliorations et les modifications, ainsi que les problèmes résolus et connus qui existent pour la version 14.1-12.34 de NetScaler ADM.

Remarques

- Ce document de notes de publication n'inclut 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.
- La version 14.1-12.34 remplace la version 14.1-12.30.
- La version 14.1-12.34 inclut une nouvelle fonctionnalité NSADM-98483 et un problème connu NSADM-106497, ainsi que toutes les améliorations et corrections de bogues disponibles dans la version 14.1-12.30.

Nouveautés

Améliorations et modifications disponibles dans la version 14.1-12.34.

Licences

Licences NetScaler Flexed Le système de licences NetScaler Flexed est le nouveau cadre de licences visant à simplifier le processus de gestion des licences. Votre licence Flexed inclut des licences d'instance logicielle (VPX/CPX/BLX, SDX, MPX et VPX FIPS) et des licences de capacité de bande passante. Vous devez appliquer les licences Flexed dans le service NetScaler Console ou NetScaler ADM sur site. Vous devez également appliquer les licences MPX Z-Cap et SDX Z-Cap sur le matériel NetScaler MPX et le matériel NetScaler SDX, respectivement. Vous pouvez ensuite les répartir entre tous les formats NetScaler déployés dans le cloud ou sur site.

Pour plus d'informations, consultez la section
Licence Flexed .

Les licences Flexed sont officiellement prises en charge dans les versions 14.1 et 13.1 de NetScaler ADM sur site.
Dans les versions 14.1-12.x d'ADM on-prem et versions ultérieures, un accès groupé à un nombre illimité de VIP ADM à des fins d'analyse est disponible et vous pouvez gérer les licences Flexed via l'interface utilisateur du tableau de bord Flexed (**NetScaler Licensing > Flexed Licensing**).

Pour les versions locales d'ADM 13.1 et 14.1 antérieures à 14.1-12.x, lorsque vous appliquez des licences flexibles, ADM les traite de la même manière que des licences groupées et affiche les détails dans l'interface utilisateur du tableau de bord groupé (**Infrastructure >** Licences groupées). L'accès groupé à un nombre illimité de VIP ADM à des fins d'analyse n'est pas disponible dans ces versions.

Pour une meilleure expérience produit mettant en valeur l'interface graphique Flexed et offrant des droits groupés, nous vous recommandons de mettre à niveau votre ADM sur site vers la version 14.1-12.x ou ultérieure.

> **Remarque :**
>
> Pour vous conformer aux exigences de licence Flexed actuelles , veuillez activer le Cloud Connector ADM sur site. Cette fonctionnalité connecte votre système ADM sur site au service ADM pour la collecte de données télémétriques. Nous vous recommandons d'activer la collecte de données télémétriques lorsque vous utilisez une licence Flexed. Pour activer ADM On-Prem Cloud Connector, consultez ADM On-Prem Cloud Connector.

[NSADM-98483]

Analytics

Détection des anomalies dans les indicateurs clés des applications En tant qu'administrateur, vous devez vous assurer que vos applications sont gérées efficacement afin d'obtenir des informations permettant de mieux hiérarchiser les priorités et de résoudre les problèmes. Dans certains

scénarios, vous souhaiterez peut-être également visualiser et analyser l'écart inhabituel des performances des applications qui peut survenir pendant une durée spécifique.

Dans **App Dashboard**, lorsque vous sélectionnez une application, l'onglet **Indicateurs clés** vous permet de voir comment vos applications sont utilisées. NetScaler ADM surveille la structure du trafic et analyse si les indicateurs clés se situent dans la plage attendue. Vous pouvez désormais visualiser les anomalies pour les indicateurs clés suivants en cas d'écart par rapport à la plage attendue :

- Temps de réponse
- Débit
- Volume de données
- Demandes par seconde

Pour plus d'informations, voir Utilisation des applications et anomalies

[NSADM-97531]

Exportez des données vers Splunk et New Relic uniquement à partir d'instances sélectionnées
Lorsque vous créez un abonnement pour exporter des données vers Splunk et New Relic, vous pouvez désormais sélectionner des instances. Si vous créez un abonnement avec des instances spécifiques, les données sont exportées vers Splunk et New Relic uniquement à partir des instances sélectionnées.

Pour plus d'informations, consultez Intégration à Splunk et Intégration à New Relic.

[NSADM-94371]

Tâches réalisables et recommandations Les améliorations suivantes sont désormais ajoutées à la fonctionnalité **Tâches** :

- Un nouvel onglet **Tâches** est introduit, dans lequel vous pouvez consulter les tâches réalisables qui nécessitent votre attention immédiate. Ces tâches sont affichées en fonction de votre utilisation actuelle. En tant qu'administrateur, l'exécution de ces tâches réalisables garantit que votre déploiement NetScaler est sécurisé, conforme et efficace. Ces tâches réalisables sont basées sur la gravité des problèmes (critique et moyen).
- L'onglet **Tâches** est renommé **Recommandations**. Dans **Recommandations**, vous pouvez continuer à passer en revue les tâches existantes et cliquer sur **Guidez-moi** pour terminer la tâche.
- L'onglet **Archive** n'est plus disponible. Au lieu de cela, vous pouvez choisir de **rejeter** une recommandation de la liste.

Pour plus d'informations, voir Tâches réalisables et recommandations.

[NSADM-91870]

Infrastructure

Utiliser le magasin de certificats pour mettre à jour les certificats SSL Lorsque vous mettez à jour un certificat SSL dans **Infrastructure > Tableau de bord SSL > Mettre à jour,** vous pouvez désormais sélectionner le certificat dans le magasin de certificats. Auparavant, vous deviez télécharger le fichier de certificat et le fichier clé pour mettre à jour un certificat SSL.

Pour plus d'informations, consultez Comment mettre à jour un certificat installé.

[NSADM-101303]

Prise en charge du journal de numérisation dans l'avis de sécurité Dans **Security Advisory** , vous pouvez désormais consulter une nouvelle option appelée **Scan Log** . À l'aide du **Scan Log** , vous pouvez :

- Consultez le rapport des cinq derniers scans CVE. Le rapport inclut à la fois l'analyse du système par défaut et l'analyse à la demande initiée par l'utilisateur.
- Téléchargez le rapport de chaque scan aux formats CSV et PDF.
- Consultez l'état de l'analyse à la demande en cours.

Pour plus d'informations, consultez l'avis de sécurité.

[NSADM-101142]

Liste mise à jour des pièges SNMP La liste des pièges SNMP est désormais mise à jour avec de nouveaux pièges ainsi que certains pièges qui manquaient auparavant. Pour consulter la liste complète, accédez à **Infrastructure > Événements > Paramètres des événements > NetScaler.**

[NSADM-99798]

Gérez les certificats et chiffrements personnalisés de base de données dans un déploiement HA NetScaler ADM vous permet désormais de remplacer les certificats de base de données intégrés par défaut par vos propres certificats émis par une autorité de certification de confiance. Vous pouvez également configurer vos propres suites de chiffrement pour la base de données ADM. Pour utiliser cette fonctionnalité, accédez à **Paramètres > Déploiement HA > Certificats de base de données**.

Pour plus d'informations, voir Gérer les certificats et chiffrements personnalisés de base de données dans le cadre d'un déploiement à haute disponibilité.

[NSADM-96583]

Partage des informations de licence d'abonnement entre ADM sur site et le service ADM Le serveur local ADM envoie désormais les informations de licence d'abonnement NetScaler au service ADM via le Cloud Connector ADM On-Prem.

[NSADM-93820]

Partage d'informations de licence groupées entre ADM sur site et le service ADM Le serveur local ADM envoie désormais les informations de licence groupées NetScaler au service ADM via le Cloud Connector ADM On-Prem.

[NSADM-93812]

Security

Tableau de bord de sécurité unifié Dans NetScaler ADM, vous pouvez désormais utiliser un tableau de bord à volet unique pour configurer les protections, activer les analyses et les déployer sur vos applications. Accédez à **Sécurité > Tableau de bord de sécurité**, puis cliquez sur **Gérer l'application** pour :

- Consultez toutes les applications sécurisées et non sécurisées.
- Sélectionnez une application non sécurisée, configurez les protections à partir de différentes options de modèle, activez l'analyse des protections et déployez-les sur votre application pour sécuriser l'application.

Auparavant, vous deviez configurer toutes les protections dans les instances NetScaler et vous ne pouviez afficher que les analyses des protections configurées dans NetScaler ADM. En tant qu'administrateur, ce tableau de bord à panneau unique vous permet de configurer les protections de l'application dans un flux de travail unique.

Pour plus d'informations, consultez le tableau de bord de sécurité unifiée.

[NSADM-92678]

StyleBooks

Utiliser les certificats du magasin de certificats NetScaler ADM dans StyleBooks Vous pouvez désormais définir StyleBooks pour utiliser les certificats du magasin de certificats NetScaler ADM. Lorsque vous créez des packs de configuration, vous pouvez sélectionner des certificats déjà existants dans le magasin de certificats ou en ajouter de nouveaux dans le magasin de certificats.

Pour plus d'informations, voir Gérer les certificats SSL depuis le magasin de certificats à l'aide de StyleBooks.

[NSADM-101515]

Définir un menu déroulant dans StyleBooks NetScaler ADM vous permet désormais de définir un menu déroulant dans les « paramètres-conditions » de la définition du StyleBook.

Pour plus d'informations, consultez la section Conditions des paramètres.

[NSADM-99543]

Téléchargez les packs d'assistance pour StyleBooks et les packs de configuration Vous pouvez désormais télécharger un pack d'assistance pour résoudre les problèmes liés à tout pack de configuration ou à toute opération StyleBook. Vous pouvez partager ces offres d'assistance avec l'équipe NetScaler lorsque vous ouvrez un ticket d'assistance pour StyleBooks. Pour télécharger un pack de support, accédez à **Applications > Configuration > Config Packs > Support Bundles**.

Pour plus d'informations, voir Télécharger le pack d'assistance.

[NSADM-97838]

Modifier l'état et l'état ARP des serveurs virtuels dans StyleBooks Dans **Applications > Configuration > Config Packs > Migrer la configuration NetScaler**, vous pouvez désormais afficher et modifier l'état (activé/désactivé) et l'état ARP de tout serveur virtuel migré vers un nouveau NetScaler.

Pour plus d'informations, voir Créer un StyleBook pour migrer la configuration de l'application NetScaler.

[NSADM-97827]

Migrez des configurations sans pack de configuration NetScaler ADM offre désormais la possibilité de migrer les configurations d'applications entre NetScaler sans créer de pack de configuration dans NetScaler ADM. Par défaut, la migration crée un pack de configuration sur ADM qui est utilisé pour gérer davantage la configuration via StyleBooks. Si vous souhaitez uniquement migrer la configuration de l'application d'un NetScaler vers un autre sans la gérer via StyleBooks par la suite, décochez la case **Gérer la configuration via ADM lors de la** migration **dans Applications > Configurations > Config Packs > Migrer la configuration NetScaler**Migrer.

Pour plus d'informations, voir Migrer la configuration de l'application NetScaler à l'aide de StyleBooks Configuration Builder.

[NSADM-97802]

Problèmes résolus

Les problèmes résolus dans la version 14.1-12.34.

Analytics

- Parfois, l'agent NetScaler ADM peut se bloquer et générer des fichiers de vidage principaux après une mise à niveau.

  [NSHELP-36428]

Infrastructure

- Dans certaines conditions, les configurations régulières appliquées à certains groupes d'utilisateurs peuvent être perdues.

  [NSADM-104565]

- Dans **Infrastructure > Instance Advisory > Security Advisory**, lorsque vous sélectionnez une instance NetScaler vulnérable dotée d'un CVE et que vous **cliquez sur Procéder à la mise à niveau**du flux de travail, le message d'erreur suivant s'affiche :

  « L'instance NetScaler sélectionnée ne nécessite pas ce flux de travail de correction »

  [NSADM-103649]

- Dans **Infrastructure > Événements > Messages d'événements**, NetScaler ADM n'indique pas si les interruptions d'utilisation du processeur NetScaler concernent le processeur par paquets ou le processeur de gestion.

  [NSADM-103391]

- Lorsque NetScaler ADM est installé sur un cluster Kubernetes, certaines pages, telles **que Infrastructure**Analytics, Events, **Syslog Events et**Data**Storage Management, peuvent ne pas**apparaître**dans l'interface**graphique de NetScaler ADM.

  [NSADM-103180]

- Lorsqu'un rapport issu d'une page défilante de NetScaler ADM est exporté, le contenu du rapport exporté peut être tronqué au-delà de la hauteur de la fenêtre visible.

  [NSADM-102765]

- Un crash du sous-système mas_service est observé lors de déploiements échelonnés.

  Ce problème se produit si vous disposez d'autorisations RBAC et que vous appartenez à un groupe dont les configurations sont les suivantes dans **Paramètres > Utilisateurs et rôles > Groupe > Paramètres d'autorisation** :

  - Une instance spécifique est sélectionnée dans **Instances**
  - **Toutes les applications** sont sélectionnées dans **Applications**

  [NSADM-99873]

- Lorsque, en tant qu'administrateur root, vous connectez pour la première fois à l'interface graphique ou à l'API NetScaler ADM avec les informations d'identification par défaut, vous êtes invité à modifier le mot de passe par défaut.

  [NSADM-95328]

Gestion et surveillance

- Lorsqu'un utilisateur RBAC envoie une demande d'API NITRO à NetScaler ADM pour récupérer la liste des serveurs NetScaler, la réponse indique à tort qu'il n'y a aucun serveur disponible. Toutefois, lorsque vous accédez à l'interface graphique NetScaler ADM**(Infrastructure > Fonctions réseau > Équilibrage de charge > Serveurs), tous les serveurs**NetScaler liés à cet utilisateur sont affichés.

  [NSHELP-36645]

- L'opération de restauration de NetScaler ADM **dans Paramètres > Fichiers de sauvegarde > Restaurer par intermittence** échoue.

  [NSHELP-36527]

- NetScaler ADM ne parvient pas à compresser certains fichiers principaux, ce qui entraîne une augmentation de la consommation d'espace disque.

  [NSHELP-36434]

- Lorsqu'un administrateur crée un groupe ayant accès à toutes les applications et qu'un utilisateur appartenant à ce groupe essaie d'accéder à la page **Infrastructure > Fonctions réseau > Équilibrage de charge > Serveurs**, l'interface graphique de NetScaler ADM devient inaccessible.

  [NSHELP-36426]

- Lors de la synchronisation des fichiers entre les nœuds principal et secondaire dans la configuration NetScaler ADM HA, le sous-système d'inventaire se bloque par intermittence.

  [NSHELP-36357]

- Dans les agents intégrés NetScaler, les alertes ou les messages relatifs aux événements ne sont pas générés même lorsque l'âge de l'événement dépasse la durée définie **dans Infrastructure > Événements > Règles > Ajouter**.

  [NSHELP-35706]

- Lorsque vous provisionnez une instance VPX sur SDX dans **Infrastructure > Instances > NetScaler > SDX > Sélectionner une action > Provisionner VPX**, l'option **Gérer viale réseau** n'apparaît pas.

  [NSHELP-36328]

StyleBooks

- Les fichiers journaux NetScaler ADM StyleBook ne sont pas automatiquement compressés même après avoir dépassé la limite de taille de fichier, ce qui entraîne une augmentation de la consommation d'espace disque.

  [NSHELP-36680]

- Lorsque des packs de configuration dont les paramètres contiennent des caractères spéciaux sont mis à jour ou supprimés, NetScaler ADM affiche un message de réussite malgré des opérations de mise à jour ou de suppression incomplètes sur NetScaler. Grâce à ce correctif, NetScaler ADM affiche désormais avec précision les erreurs pour toute configuration incomplète due à des caractères spéciaux dans la définition du pack de configuration.

  [NSADM-104423]

Problèmes connus

Les problèmes qui existent dans les versions 14.1-12.34.

Analytics

- Dans **Applications > Tableau de bord**, lorsque vous cliquez sur une application hébergée sur la paire NetScaler HA, l'onglet **Performances** de la page de détails de l'application n'affiche aucune donnée sous **Tous les services**.

  Solution : actualisez la page ou passez à un autre onglet de la page de détails de l'application, puis revenez à l'onglet **Performances** pour afficher les services associés au serveur virtuel d'équilibrage de charge.

  [NSADM-105613]

Infrastructure

- Le tableau de bord des licences Flexed affiche les informations relatives à NetScaler uniquement après avoir retiré au moins un NetScaler du pool de licences de bande passante Premium.

  [NSADM-106497]

- Lorsque des licences sont supprimées de NetScaler ADM pour VMware ESXi, le nombre de licences **dans Paramètres > Configuration des licences et des analyses peut ne pas refléter immédiatement le nombre** mis à jour.

  [NSADM-105851]

- Le rapport de différence n'est pas généré pour une tâche de mise à niveau dans **Infrastructure > Tâches de mise à niveau > Rapports** de différences .

  [NSADM-106777]

- Une fois qu'un nouveau NetScaler ADM est configuré, le message d'erreur suivant peut apparaître : « Error in operationt - Metrics not found. »

  Ce problème se produit car la tâche de purge automatique des données n'a pas encore été exécutée, ce qui entraîne l'absence de données. La tâche est planifiée pour s'exécuter pendant 3 heures. Après son exécution, les données nécessaires sont générées et le message d'erreur ne s'affiche plus.

  [NSADM-103157]

- Lorsque vous essayez d'installer un certificat sur une instance NetScaler BLX, l'installation échoue et la page **Infrastructure > Tableau de bord SSL > Journaux d'audit SSL affiche le** message d'erreur suivant :

  « SCP : L'authentification par mot de passe échoue sur *ip-address*. »

  [NSADM-102202]

- L'agent NetScaler n'est pas enregistré auprès de NetScaler ADM si l'un de ses mots de passe comporte le symbole « # ».

  [NSADM-100613]

Licences

- Une fois la licence Flexed ou Pooled appliquée, la page **Configuration Analytics** (Paramètres > Configuration **Analytics)** n'est pas mise à jour avec les informations correctes.

  Solution: actualisez la page pour obtenir les informations correctes.

  [NSADM-106665]

- Le tableau de bord des licences Flexed dans **NetScaler Licensing > Flexed Licensing Dashboard** apparaît vide.

  Solution: appliquez une licence de bande passante Premium.

  [NSADM-106561]

Gestion et surveillance

- L'agent NetScaler ADM génère des interruptions SNMP « NetScalerLoginFailure ». Ce problème se produit car les informations d'identification utilisées par l'agent ADM pour se connecter à NetScaler sont tronquées en raison d'un caractère de nouvelle ligne.

[NSHELP-36804]

- Dans une paire ADM HA, l'état de la base de données a été observé comme étant inactif et ne **se** synchronisant pas même après avoir essayé plusieurs fois d'utiliser l'option **Synchroniser la base** de données dans l'interface graphique.

  [NSHELP-29626]

Notes de publication pour la version 14.1—8.50 de NetScaler ADM

February 1, 2024

Ce document de notes de publication décrit les améliorations et les modifications, ainsi que les problèmes résolus et connus qui existent pour la version 14.1—8.50 de NetScaler ADM.

Remarques

- Ce document de notes de publication n'inclut 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.

Nouveautés

Les améliorations et modifications disponibles dans les versions 14.1 à 8.50.

Gestion et surveillance

Aide à l'identification et à la remédiation des cas CVE-2023-4966 et CVE-2023-4967

> **Remarque :**
>
> Vous pouvez consulter les détails des CVE-2023-4966 et CVE-2023-4967 uniquement si vous avez activé l'avis de sécurité via ADM On-Prem Cloud Connector. Pour plus d'informations, consultez ADM On-Prem Cloud Connector

L'avis de sécurité NetScaler ADM prend désormais en charge l'identification et la résolution des incidents CVE-2023-4966 et CVE-2023-4967.

- L'identification nécessite une combinaison de scan de version et de configuration.
- La correction nécessite une mise à niveau des instances vulnérables de NetScaler vers une version recommandée contenant le correctif.

> **Remarque :**
>
> L'avis de sécurité ne prend pas en charge les versions de NetScaler qui ont atteint la fin de vie (EOL). Nous vous recommandons de passer aux versions ou versions prises en charge par NetScaler.

Pour plus d'informations sur l'utilisation de NetScaler ADM pour mettre à niveau des instances NetScaler, consultez la section Utiliser des tâches pour mettre à niveau des instances NetScaler.

Pour plus d'informations, consultez le Bulletin de sécurité.

[NSADM-101092]

Analytics

Support pour configurer l'exportation de métriques de NetScaler vers Prometheus via StyleBook Pour exporter des métriques de NetScaler vers Prometheus, vous devez créer un profil d'analyse dans NetScaler et spécifier le fichier de schéma. Pour plus d'informations, consultez la section Surveillance de NetScaler, des applications et de la sécurité des applications à l'aide de Prometheus.

Dans **Applications > Configuration > Stylebooks > Stylebook par défaut, vous pouvez désormais utiliser le StyleBook**de configuration **Prometheus TimeSeries Analytics et exécuter la configuration** sur toutes les instances gérées.

Pour plus d'informations, consultez StyleBook d'analyse Prometheus.

[NSADM-97698]

Découvrez la cause première de la latence des applications La lenteur des applications est une préoccupation majeure pour toute organisation, car elle entraîne un impact commercial ou une productivité. Dans **Applications > Web Insight**, vous pouvez désormais consulter une nouvelle métrique intitulée **Applications présentant des anomalies du temps de réponse**. À l'aide de cette métrique, en tant qu'administrateur, vous pouvez déterminer si la latence de l'application est due aux causes suivantes :

- Latence du réseau client
- Latence réseau du serveur
- Délai de traitement du serveur

Pour plus d'informations, voir Afficher la cause première de la latence des applications.

[NSADM-97530]

Job de configuration : aide à la création d'une tâche pour configurer l'exportation de métriques de NetScaler vers Prometheus Pour exporter des métriques de NetScaler vers Prometheus, vous devez créer un profil d'analyse dans NetScaler et spécifier le fichier de schéma. Pour plus d'informations, consultez la section Surveillance de NetScaler, des applications et de la sécurité des applications à l'aide de Prometheus.

Dans **Configuration Job**, vous pouvez désormais créer une tâche à l'aide du modèle **NSConfigurePrometheusAnalyticsProfile** à partir du **modèle intégré**, spécifier les paramètres requis et exécuter la tâche sur toutes les instances gérées.

Pour plus d'informations, voir Planifier les tâches créées à l'aide de modèles intégrés.

[NSADM-97251]

Attribuer un profil réseau au NetScaler géré à partir de NetScaler ADM Lorsque vous activez l'analyse pour les serveurs virtuels dans NetScaler ADM, les données AppFlow de NetScaler sont exportées vers NetScaler ADM via l'adresse IP du sous-réseau (SNIP) NetScaler. Dans certains scénarios, le SNIP peut être bloqué en raison du pare-feu du réseau. Dans de tels scénarios, vous devrez peut-être utiliser une adresse IP différente de celle du SNIP. Pour plus d'informations sur le profil réseau, voir Utiliser une adresse IP source spécifiée pour les communications dorsales.

Vous pouvez désormais attribuer des profils réseau à une instance NetScaler via NetScaler ADM. Accédez à **Infrastructure > Instances > NetScaler**ADC, sélectionnez l'instance, puis dans la liste Sélectionner une action, **cliquez sur Configurer**les**profils réseau pour attribuer un profil réseau** à l'instance.

> **Remarque :**
>
> Assurez-vous d'avoir désactivé l'analyse sur tous les serveurs virtuels avant d'attribuer un profil réseau à l'instance.

Grâce à cette amélioration, vous pouvez attribuer un profil réseau pour l'exportation de données AppFlow de NetScaler vers NetScaler ADM.

[NSADM-91836]

Infrastructure

Améliorations du scénario d'échec de mise à niveau Lorsqu'une tâche de mise à niveau (**Infrastructure > Tâches de mise**à niveau) échoue, elle entraîne des problèmes d'espace disque en raison de la présence des fichiers de compilation et d'autres fichiers extraits. Par conséquent, la prochaine tâche de mise à niveau échoue également.

Le scénario d'échec de la tâche de mise à niveau est désormais amélioré. Si une tâche de mise à niveau échoue, NetScaler ADM supprime l'ancien fichier de compilation de l'instance NetScaler.

[NSADM-97383]

Changements liés au rebranding NetScaler ADM est désormais renommé NetScaler ADM. Pour s'aligner sur la nouvelle image de marque, l'interface graphique d'ADM est également mise à jour.

[NSADM-97365]

Stratégie d'accès pour les agents sur site Lorsque vous créez une **stratégie d'accès** avec **Modifier** l'accès pour l'agent ADM dans **Paramètres > Utilisateurs et rôles > Stratégies d'accès**, les utilisateurs associés à cette stratégie peuvent désormais enregistrer l'agent avec leurs informations d'identification.

[NSADM-97337]

Tableau de bord de gestion du stockage des données disponible dans l'interface graphique NetScaler ADM Dans **Paramètres > Gestion du stockage des données**, vous pouvez désormais afficher et gérer les informations de stockage des données à travers les différentes fonctionnalités de votre déploiement actuel. Le tableau de bord de gestion du stockage des données vous permet de visualiser la façon dont le stockage est consommé dans l'ensemble des fonctionnalités et de contrôler si la consommation de stockage se situe dans les limites du seuil spécifié.

Le tableau de bord propose les fonctionnalités suivantes :

- Vignettes **Ingestion des données, consommation de stockage**et **Actions** : les vignettes vous fournissent les informations suivantes :
  - État de l'activité d'ingestion de données
  - Informations sur vos données consommées et l'espace disque total disponible
  - Options permettant de revoir la stratégie de conservation des données, d'effectuer un nettoyage des données et de consulter les notifications de votre système
- **Tendance en matière de consommation de stockage** : vous aide à visualiser la manière dont les données sont stockées dans les différentes fonctionnalités sur une période donnée
- **Consommation de stockage par fonctionnalités** :
  - Affiche la répartition du stockage des données par différentes fonctionnalités
  - Vous permet d'effectuer des pruneaux de données, de consulter l'historique des pruneaux de données et de visualiser les fonctionnalités supprimées dans chaque pruneau de données

Pour plus d'informations, voir Utiliser le tableau de bord de stockage des données.

[NSADM-97320]

Support pour le stockage de certificats SSL dans NetScaler ADM Vous pouvez désormais gérer vos certificats SSL dans **Infrastructure > Tableau de bord SSL > Magasin de certificats**.

Utilisez le **magasin de certificats** pour :

- Ajouter, mettre à jour et supprimer des certificats
- Installation de certificats sur des instances NetScaler
- Importer des certificats depuis des instances NetScaler

Pour plus d'informations, consultez Comment utiliser le magasin de certificats.

[NSADM-97257]

La limite de sessions utilisateur est passée à 40 Dans **Paramètres > Utilisateurs et rôles > Groupes**, vous pouvez configurer jusqu'à 40 sessions utilisateur. Par défaut, 20 sessions utilisateur vous sont attribuées. Toutefois, si vous appartenez aux groupes d'administrateurs et d'utilisateurs en lecture seule, 40 sessions utilisateur vous sont attribuées par défaut et cette valeur ne peut pas être modifiée.

[NSADM-95314]

Réessayer les tâches de mise à niveau qui ont échoué Dans **Infrastructure > Tâches de mise à niveau**, vous pouvez désormais sélectionner la tâche de mise à niveau qui a échoué et effectuer l'une des actions suivantes :

- Cliquez sur **Réessayer à côté de** la tâche de mise à niveau qui a échoué
- Accédez à **Sélectionner une action > Réessayer la tâche de mise à niveau**

Pour plus d'informations, voir Réessayer les tâches de mise à niveau ayant échoué.

[NSADM-93439]

Cloud Connector ADM sur site Vous pouvez utiliser la fonctionnalité Cloud Connector pour établir une connexion entre ADM On-Prem et le service ADM. Cette connectivité vous permet de tirer parti de la fonctionnalité d'avis de sécurité d'ADM On-Prem. L'avis de sécurité vous permet de suivre les nouvelles vulnérabilités et expositions courantes (CVE), d'évaluer l'impact des CVE, de comprendre les mesures correctives et de résoudre les vulnérabilités. En tant qu'administrateur, vous pouvez surveiller les instances NetScaler pour détecter tout nouveau CVE par le biais d'une analyse périodique ou manuelle, et prendre les mesures nécessaires pour la correction.

Pour plus d'informations, consultez ADM On-Prem Cloud Connector.

[NSADM-92204]

Avis de sécurité concernant NetScaler ADM Vous pouvez configurer ADM On-Prem Cloud Connector et activer Security Advisory pour utiliser la version complète de la fonctionnalité Security Advisory dans ADM on-prem. Auparavant, l'avis de sécurité n'était disponible que dans la version préliminaire.

Pour plus d'informations, consultez l'avis de sécurité.

> **Remarque :**
>
> Si vous n'avez pas configuré ou si vous avez désactivé le Cloud Connector ADM On-Prem, vous ne pouvez utiliser l'avis de sécurité qu'en version préliminaire.

Pour plus d'informations sur ADM On-Prem Cloud Connector, consultez la section ADM On-PremCloud Connector.

[NSADM-91726]

Gestion et surveillance

Authentification requise pour que les opérations StyleBook puissent accéder aux instances NetScaler En tant qu'administrateur, vous pouvez désormais demander aux utilisateurs de fournir des informations d'identification pour toutes les opérations de StyleBook et de pack de configuration effectuées sur des instances NetScaler. Pour activer cette fonctionnalité, procédez comme suit :

- Accédez à **Paramètres > Administration > Système, fuseau horaire, URL autorisées et paramètres de l'agent > Paramètres de base**
- Sélectionnez les **informations d'identification rapides pour la connexion à l'instance**
- Sélectionnez des **informations d'identification rapides pour les opérations Stylebook**

Sinon, si vous sélectionnez **Prompt Credentials pour Instance Login** et désactivez **Prompt Credentials for Stylebook Operations**, les opérations StyleBook et le pack de configuration effectuées sur les instances NetScaler ne sont pas invitées à saisir un nom d'utilisateur et un mot de passe.

Pour plus d'informations, consultez Comment activer l'accès au shell pour les utilisateurs autres que ceux par défaut.

[NSHELP-35432]

Accès en lecture seule aux fichiers de sauvegarde et aux sessions utilisateur NetScaler ADM Les utilisateurs disposant d'un accès en lecture seule peuvent désormais consulter les pages suivantes : **Paramètres > Utilisateurs et rôles > Sessions***
**Paramètres **Fichiers de sauvegarde

[NSHELP-35431]

Configurer le seuil d'ingestion de données Vous pouvez désormais configurer un seuil d'ingestion de données dans **Paramètres > Gestion du stockage des données > Stratégie de conservation des données > Système > Paramètre d'ingestion de données**. Avec ce paramètre, vous pouvez configurer le processus au niveau du système pour qu'il s'arrête lorsque le stockage des données atteint la valeur seuil. Les valeurs seuils acceptées sont comprises entre 50 % et 80 %.

Pour plus d'informations, consultez la section Stratégie de conservation des données.

[NSHELP-35237]

Version ADM et adresse IP disponibles dans le fichier de support technique La version et l'adresse IP d'ADM sont désormais disponibles dans le fichier de support technique depuis **Paramètres > Diagnostics > Générer un fichier de support technique**.

[NSHELP-33551]

StyleBooks

Les fonctionnalités suivantes sont désormais disponibles dans StyleBooks :

- Sources de données : utilisez des instances NetScaler ADC comme sources de données ou créez des sources de données personnalisées.
- GitHub Enterprise : importez et synchronisez des StyleBooks et des packs de configuration depuis votre serveur GitHub Enterprise.
- Fonctions intégrées : les fonctions intégrées suivantes sont ajoutées :
  - `match()`
  - `contains()`
  - `select()`
  - `hash_sha256()`
  - `relate()`
  - `splat()`
- Définitions StyleBook : mettez à jour les définitions StyleBook personnalisées directement depuis l'interface graphique de NetScaler ADM.
- Packs de configuration depuis le référentiel GitHub : importez et synchronisez les packs de configuration depuis un référentiel GitHub. Auparavant, seuls les StyleBooks étaient autorisés.
- `botinsight` attribut : configurez le `botinsight` type dans la `insights` section de StyleBooks.

[NSADM-97841]

Prise en charge d'attributs supplémentaires dans StyleBooks Analytics La section d'analyse de StyleBooks est désormais améliorée pour :
- Accepter les paramètres pour configurer le mode transport (`transport-mode`)
- Configurer HDX Insight pour différents types de trafic (`enable-hdxinsight-for`)
- Activer l'option HTTP X-Forwarded-For () - Activer les mesures côté client (`http-x-forwarded-for`)
`client-side-measurements`

Pour plus d'informations, consultez la section Grammaire de StyleBooks.

[NSADM-97839]

Problèmes résolus

Les problèmes résolus dans les versions 14.1 à 8.50.

Analytics

- Le nettoyage périodique des données du tableau de bord de l'application n'a pas fonctionné comme prévu. NetScaler ADM a donc consommé davantage d'espace disque.

  [NSHELP-36184]

- Lorsque NetScaler ADM perd les licences de serveur virtuel, l'état d'analyse des serveurs virtuels utilisant ces licences devrait être désactivé. Ce scénario ne fonctionnait pas comme prévu pour les serveurs virtuels VPN.

  [NSHELP-36183]

Infrastructure

- Dans **Gateway > HDX** Insight **et Gateway > Gateway**Insight, l'axe X des graphiques affiche les dates plutôt que l'heure.

  [NSHELP-36043]

- La paire NetScaler ADM HA ne parvient pas à se remettre du scénario à cerveau divisé en raison d'un échec de synchronisation lors de la communication par battement de cœur.

  [NSHELP-35934]

- La fonctionnalité Customer User Experience Improvement Program (CUXIP) est activée pour les utilisateurs et leurs données d'utilisation sont collectées même après que l'administrateur a désactivé CUXIP dans **Paramètres > Administration > Paramètres**CUXIP.

  [NSADM-101771]

- Lorsque, en tant qu'administrateur root, vous vous connectez à l'interface graphique ou à l'API NetScaler ADM avec les informations d'identification par défaut pour la première fois, vous n'avez pas été invité à modifier le mot de passe par défaut. Avec ce correctif, vous êtes obligé de modifier le mot de passe par défaut.

  [NSADM-95328]

- Lorsque plusieurs utilisateurs SNMP sont créés simultanément à l'aide d'un script, les demandes SNMP adressées à ADM échouent.

  [NSADM-83924]

Gestion et surveillance

- Les dossiers créés dans le répertoire de sauvegarde NetScaler ADM ne sont pas supprimés lors de l'opération de suppression de sauvegarde planifiée toutes les 2 heures.

  [NSHELP-35911]

- L'authentification avec le protocole LDAP externe échoue par intermittence dans NetScaler ADM et n'est résolue qu'en redémarrant NetScaler ADM.

  [NSHELP-35733]

- **Le sous-système ADM mas_perf se bloque et un message d'événement s'affiche dans Paramètres > Événements du système ADM.**

  [NSHELP-35711]

- Les utilisateurs ne peuvent pas consulter leurs applications autorisées dans **Applications > Tableau de bord des applications**. Ce problème se produit lorsque les utilisateurs appartiennent à de nombreux groupes et que chaque groupe possède de nombreuses applications.

  [NSHELP-35165]

- Un Qualys Scan effectué sur NetScaler ADM a révélé une faible vulnérabilité active liée à l'échange de clés SSL/TLS sur les ports PostgreSQL.

  [NSHELP-34487]

- Si NetScaler se déconnecte du serveur de licences et se reconnecte dans les 10 minutes, la licence extraite par NetScaler peut apparaître deux fois sur le serveur de licences. Redémarrez le serveur de licences pour libérer cette entrée périmée.

  [NSHELP-35420]

Provisioning

- Lorsque vous provisionnez NetScaler VPX on Cloud (**Infrastructure > Instances > NetScaler > VPX > Provision) à l'aide d'ESXi ou de VMware vCenter**, la configuration de licence est ignorée.

  [NSHELP-35984]

- La mise à disposition NetScaler VPX sur VMware vCenter**(Infrastructure > Instance > NetScaler > VPX > Provision) échoue en raison du même nom que celui utilisé dans l'instance VPX**précédemment supprimée.

  [NSHELP-35983]

StyleBooks

- Si vous créez un pack de configuration à partir d'une définition de StyleBook qui possède un serveur virtuel d'authentification et des liaisons de stratégie de cache intégrées, puis que vous supprimez le pack de configuration, la suppression est réussie. Cependant, si vous essayez de créer à nouveau le pack de configuration avec les mêmes paramètres, le message d'erreur suivant s'affiche :
  `Resource already exists`.

  [NSHELP-35646]

- Lorsque vous essayez de migrer une configuration ADC d'une instance ADC source vers une instance cible dans **Applications > Configuration > Config Packs > Migrer ADC > Get Started > Spécifier la configuration, et que vous**cliquez sur **Suivant**, le message d'erreur suivant s'affiche par intermittence :

  `No Job found`.

  [NSADM-97948]

Problèmes connus

Les problèmes qui existent dans les versions 14.1 à 8.50.

Infrastructure

- Dans **Infrastructure > Instance Advisory > Security Advisory**, lorsque vous sélectionnez une instance NetScaler vulnérable dotée d'un CVE et que vous **cliquez sur Procéder à la mise à niveau**du flux de travail, le message d'erreur suivant s'affiche :

« L'instance NetScaler sélectionnée ne nécessite pas ce flux de travail de correction »

Solution : mettez à niveau manuellement l'instance NetScaler depuis Infrastructure > Tâches **de**mise à niveau.

[NSADM-103649]

- Après la configuration d'un nouveau NetScaler ADM, le message d'erreur suivant peut s'afficher : `Error in operation - Metrics not found.`

  Ce problème se produit car la tâche de purge automatique des données n'a pas encore été exécutée, ce qui entraîne l'absence de données. La tâche est planifiée pour s'exécuter pendant 3 heures. Après son exécution, les données nécessaires sont générées et le message d'erreur ne s'affiche plus.

  [NSADM-103157]

- Lorsqu'un rapport issu d'une page défilante de NetScaler ADM est exporté, le contenu du rapport exporté peut être tronqué au-delà de la hauteur de la fenêtre visible.

  [NSADM-102765]

- Lorsque vous essayez d'installer un certificat sur une instance NetScaler BLX, l'installation échoue et la page **Infrastructure > Tableau de bord SSL > Journaux d'audit SSL affiche le** message d'erreur suivant :

  `SCP: Authentication by password fails on _<ip-address>_.`

  [NSADM-102202]

- L'agent NetScaler n'est pas enregistré auprès de NetScaler ADM si l'un de ses mots de passe comporte le symbole %23.

  [NSADM-100613]

Gestion et surveillance

- Dans une paire ADM HA, l'état de la base de données a été observé comme étant inactif et ne **se** synchronisant pas même après avoir essayé plusieurs fois d'utiliser l'option **Synchroniser la base** de données dans l'interface graphique.

  [NSHELP-29626]

Notes de mise à jour relatives à la version 14.1-4.42 de NetScaler ADM

February 1, 2024

Ce document de notes de mise à jour décrit les améliorations et les modifications, ainsi que les problèmes résolus et connus qui existent dans la version Build 14.1-4.42 de NetScaler ADM.

Remarques

- Ce document de notes de publication n'inclut 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.

Nouveautés

Les améliorations et modifications disponibles dans les versions 14.1-4.42.

Analytics

Web Insight - Support permettant de visualiser la distribution en pourcentage en fonction des demandes Dans **Web Insight**, vous pouvez désormais afficher **la répartition en pourcentage par demandes** selon les indicateurs suivants :

- Clientèle
- Serveurs
- Emplacements géographiques
- URL

En tant qu'administrateur, cette amélioration vous permet de comprendre la répartition en pourcentage des demandes reçues en fonction du nombre total de demandes pour la durée sélectionnée. Par exemple, vous pouvez comparer la façon dont les serveurs reçoivent les demandes pendant la durée sélectionnée.

Pour plus d'informations, consultez Web Insight.

[NSADM-96158]

Support pour exporter depuis chaque widget dans Web Insight Dans **Web Insight**, l'option d'exportation est désormais intégrée à tous les widgets et permet d'exporter des données sous forme de tableau. Grâce à cette amélioration, vous pouvez :

- Exportez les données requises individuellement à partir de n'importe quel widget.
- Explorez n'importe quelle métrique et exportez également les données requises à partir de n'importe quel widget.

Auparavant, les données d'exportation ne fournissaient que le rapport consolidé.

> **Remarque :**
>
> Vous pouvez également continuer à utiliser l'option d'exportation existante pour générer le rapport consolidé.

[NSADM-94140]

Un tableau de bord unifié pour afficher les détails des indicateurs clés des instances En tant qu'administrateur, vous pouvez désormais visualiser un tableau de bord qui fournit une vue d'ensemble des principaux détails des indicateurs en fonction des éléments suivants :

- Applications
- Infrastructure ADC
- Sécurité des applications
- Gateway

Ce tableau de bord à panneau unique vous permet d'afficher les détails pour une meilleure expérience de surveillance de l'utilisation et des performances de l'instance.

Pour plus d'informations, voir Tableau de bord unifié

[NSADM-94137]

Exportez les événements et les données de statistiques ADM vers Splunk et New Relic Lorsque vous créez un nouvel abonnement dans **Paramètres > Intégration à l'écosystème** pour l'intégration de NetScaler ADM à Splunk et New Relic, vous pouvez désormais sélectionner l'option ADM **Events** et **ADM Metrics**. Après avoir configuré l'abonnement avec l'une de ces options ou les deux, vous pouvez afficher les données correspondantes dans le tableau de bord Splunk et New Relic.

Pour plus d'informations, consultez Intégration à Splunk et Intégration à New Relic.

[NSADM-93765]

Afficher le classement SSL d'une application Dans **Applications > Tableau de bord**, vous pouvez désormais consulter le classement SSL d'une application. Vous pouvez passer en revue les problèmes de SSL et mettre à niveau l'application pour obtenir la note A+ . Toutefois, si vous constatez une baisse du trafic en raison de cette mise à niveau, vous pouvez restaurer le profil frontal sécurisé configuré sur votre application. Cette action rétablit la note A+ par rapport à la note précédente.

Pour plus d'informations, consultez l'analyse du classement SSL A+.

[NSADM-92025]

Web Insight - Support pour afficher les valeurs nulles dans les graphiques Dans **Web Insight** , lorsque vous explorez une métrique vers le bas sous **Applications** , Clients, URL ou Instances, la vue analytique fournit désormais la visibilité des valeurs nulles (par exemple, 0 ms et 0 demande) dans le graphique pour la durée sélectionnée.

Auparavant, si aucun trafic ou transaction n'était reçu pendant la durée sélectionnée, Web Insight affichait les graphiques en omettant ces valeurs nulles. En tant qu'administrateur, vous pouvez désormais afficher le graphique complet avec ces valeurs nulles.

[NSADM-88686]

Infrastructure

Prise en charge des mots de passe des nœuds RPC pour le déploiement à haute disponibilité de NetScaler Vous pouvez désormais définir le mot de passe du nœud RPC lors de la création des nœuds principal et secondaire dans un déploiement HA. Accédez à **Infrastructure > Tâches de mise à niveau > Créer une tâche > Configurer une paire HA d'instances NetScaler** pour saisir les mots de passe des nœuds RPC pour les nœuds à haute disponibilité.

Pour plus d'informations, consultez la section Planifier la configuration d'une paire HA d'instances NetScaler.

[NSADM-93912]

L'agent NetScaler ADM met en cache les images NetScaler Le temps nécessaire à la mise à niveau de NetScaler est désormais considérablement réduit car les images NetScaler sont mises en cache dans l'agent NetScaler ADM après leur téléchargement. Il n'est donc pas nécessaire de télécharger les images pour les tâches de mise à niveau suivantes.

> **Remarque :**
>
> Cela s'applique uniquement aux ADC ajoutés à l'aide de l'agent NetScaler ADM.

Pour plus d'informations, consultez la section Création d'une tâche de mise à niveau ADC.

[NSADM-76343]

Afficher la chaîne complète de certificats Vous pouvez désormais afficher la chaîne complète de liens d'un certificat, y compris les certificats intermédiaires jusqu'au certificat de l'autorité de certification racine.

Pour afficher la chaîne de certificats, accédez à **Infrastructure > Tableau de bord SSL**, choisissez un certificat SSL et cliquez sur **Détails**.

Pour plus d'informations, consultez Afficher la chaîne de certificats SSL.

[NSADM-52467]

StyleBooks

Prise en charge de types d'arguments supplémentaires dans la fonction replace () La fonction intégrée « replace () » peut également accepter une liste des types intégrés suivants :

- `string`
- `ipaddress`
- `tcp-port`
- `number`
- **`boolean`**

Pour plus d'informations, voir Fonctions intégrées.

[NSADM-96802]

Prise en charge de la fonction multiple () Les fonctions intégrées de StyleBooks prennent désormais en charge la fonction multiple (). La fonction multiple (argument1, argument2) prend deux arguments et renvoie une liste contenant de nombreuses copies de l'argument 1. Le nombre de copies est égal au nombre passé à l'argument 2.

Pour plus d'informations, voir Fonctions intégrées.

[NSADM-95973]

Prise en charge des sections facultatives dans les packs de configuration StyleBook Les `targets`sections et `stylebook`sont désormais facultatives dans la charge utile du pack de configuration. Si vous ne spécifiez pas ces sections pour mettre à jour un pack de configuration, les dernières sections utilisées `targets`sont `stylebook`extraites de la base de données NetScaler ADM et le pack de configuration est mis à jour.

[NSADM-92377]

Spécifier l'accès des groupes d'utilisateurs aux packs de configuration En tant qu'administrateur, vous pouvez désormais empêcher les groupes d'utilisateurs d'accéder aux packs de configuration créés par d'autres groupes d'utilisateurs. Pour sélectionner cette option, accédez à **Paramètres > Utilisateurs et rôles > Groupes > Paramètres d'autorisation > Packs de configuration > Toutes les configurations créées par le groupe d'utilisateurs** .

Pour plus d'informations, consultez la section **Packs de configuration** dans Créer un groupe d'utilisateurs .

[NSADM-92374]

Problèmes résolus

Les problèmes résolus dans la version 14.1-4.42.

Analytics

- La paire NetScaler ADM HA peut entraîner un scénario de split-brain par intermittence.

  [NSHELP-35430]

- Les transactions Web HTTP dont l'URL ne contient pas de valeur de paramètre de requête ne sont pas affichées dans le tableau de bord NetScaler ADM Web Insight (**Applications > Web Insight**).

  Par exemple, si l'URL `https://www.google.com/search?q=abstract%20api` ne possède pas la valeur du paramètre de requête et qu'elle est disponible en tant que `https://www.google.com/search?q=`, les transactions HTTP sont supprimées et ne sont pas disponibles sur le tableau de bord.

  [NSADM-99448]

- Dans **Web Insight**, lorsque vous explorez une métrique vers le bas pour afficher les détails, puis que vous explorez davantage une métrique, le graphique reste dans la vue précédente, mais tous les autres détails apparaissent comme prévu.

  Par conséquent, cela crée l'hypothèse que l'analyse plus approfondie ne fonctionne pas comme prévu.

  [NSADM-98995]

Infrastructure

- Les instances MPX sont absentes de la page **Infrastructure > Inventaire NetScaler > NetScaler (MPX/VPX/CPX/BLX**).

  [NSHELP-35593]

- Lorsque vous vous connectez à l'interface graphique de NetScaler ADM avec l'authentification utilisateur LDAP et que vous utilisez « domaine\nom d'utilisateur », les préférences utilisateur ne sont pas enregistrées.

[NSADM-100995]

- Lorsque vous exécutez des commandes sur une partition pour n'importe quelle tâche de configuration, le message d'erreur suivant s'affiche : « Commande bloquée pour le périphérique de partition d'administration ».

  Ce problème est rencontré sur NetScaler 13.1-42.47 et les versions ultérieures.

  [NSADM-100416]

- Après avoir effectué un basculement pour une paire ADM HA dans **Paramètres > Déploiement > Forcer le basculement**, vous ne voyez pas les détails du nœud secondaire sur la page **Paramètres** Déploiement.

  [NSADM-98674]

- Lorsque vous essayez d'ajouter un profil Slack dans **Réglages > Notifications > Slack > Ajouter**, le profil n'est pas ajouté et le message d'erreur suivant s'affiche :

  `Please check internet connectivity`.

  [NSADM-98633]

- Lorsque, en tant qu'administrateur root, vous vous connectez à l'interface graphique ou à l'API NetScaler ADM avec les informations d'identification par défaut pour la première fois, vous n'avez pas été invité à modifier le mot de passe par défaut. Avec ce correctif, vous êtes obligé de modifier le mot de passe par défaut.

  [NSADM-95328]

Gestion et surveillance

- Lorsque vous sauvegardez ou restaurez une instance de NetScaler, le répertoire /var/metrics_conf n'est pas sauvegardé.

  [NSHELP-35724]

- Lorsque vous exportez les rapports d'expiration SSL hebdomadaires, 30 ou 90 jours depuis **Infrastructure > Tableau de bord SSL > Certificats SSL > Exporter les rapports** et que vous sélectionnez **Tabulaire**, le rapport obtenu affiche une colonne Domaine vide.

  [NSHELP-35592]

- Dans **Infrastructure > Tableau de bord SSL > Certificats SSL**, la paire de haute disponibilité NetScaler n'affiche pas l'exposant « P » et « S » pour les appareils principaux et secondaires.

  [NSHELP-35523]

- **L'état de NetScaler ADM est affiché comme étant inactif par intermittence, même lorsque tous les processus sont en cours d'exécution.**

[NSHELP-35408]

- Pour plusieurs adresses IP de cluster (CLIP) dans un cluster, lorsque vous ajoutez un CLIP entre crochets dans **Infrastructure > Instances > NetScaler**Ajouter, la configuration échoue et le CLIP n'est pas ajouté à NetScaler ADM.

  [NSHELP-35323]

- Dans **Infrastructure > Configuration > Tâches de configuration > Créer une tâche > Sélectionner une configuration**, lorsque vous entrez une variable de mot de passe (`$password$`) et que vous conservez le champ **Type** en tant que **champ de texte** au lieu de **champ de mot de passe**, puis que vous cliquez sur **Suivant**, la page ne se charge pas.

  [NSHELP-35266]

- Le processus d'inventaire NetScaler ADM se bloque par intermittence lorsque des demandes sont envoyées à d'autres processus ADM.

  [NSHELP-35048]

- NetScaler ADM ne répond pas en raison de plusieurs pannes de sous-système.

  [NSHELP-34633]

- Le site principal (paire NetScaler ADM HA) essaie sans cesse de synchroniser les données avec le nœud de reprise après sinistre NetScaler ADM et échoue.
  Ce problème se produit lorsque le site principal contient des données volumineuses (>1 Go).

  [NSHELP-32750]

Provisioning

- La mise à disposition de NetScaler VPX sur SDX (Infrastructure**> Instances > NetScaler ADC > VPX) échoue dans NetScaler ADM**.

  [NSHELP-35347]

StyleBooks

- Le déploiement des packs de configuration peut échouer lorsque la définition de StyleBook inclut la section `operations`.

  [NSHELP-35588]

- Lorsque vous ajoutez certaines versions d'Infoblox en tant que fournisseur IPAM dans **Paramètres > IPAM > Ajouter**, le message d'erreur suivant s'affiche :


```
Invalid provider information: Invalid attributes for registering
provider.
```

[NSHELP-35302]

Problèmes connus

Les problèmes qui existent dans les versions 14.1-4.42.

Infrastructure

- L'agent NetScaler n'est pas enregistré auprès de NetScaler ADM si l'un de ses mots de passe comporte un symbole. #

  [NSADM-100613]

- Dans **Paramètres > Administration > Installer les certificats SSL**, si le nom du fichier de certificat que vous téléchargez est entre parenthèses, l'installation du certificat SSL sur NetScaler échoue. Le message d'erreur suivant s'affiche :

  « Requête POST non valide, la charge utile doit commencer par object= ».

  [NSADM-99531]

Gestion et surveillance

- Dans une paire ADM HA, l'état de la base de données a été observé comme étant inactif et ne **se** synchronisant pas même après avoir essayé plusieurs fois d'utiliser l'option **Synchroniser la base** de données dans l'interface graphique.

  [NSHELP-29626]

Migrer NetScaler ADM sur site vers Citrix Cloud

February 1, 2024

Vous pouvez migrer **NetScaler ADM 13.0 64.35 ou une** version ultérieure sur site 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 .

> **Remarque :**
>
> Le service NetScaler ADM est désormais renommé en service NetScaler Console. L'interface utilisateur et la documentation de nos produits font actuellement l'objet de mises à jour pour refléter ces modifications. Pendant cette période, vous pouvez rencontrer les noms les plus anciens et les plus récents référencés de manière interchangeable. Nous vous remercions de votre compréhension durant cette transition.

Le service NetScaler Console 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 ne sont actuellement prises en charge que dans le service NetScaler Console, telles que l'analyse des périodes de pointe et de pointe, l'analyse basée sur l'apprentissage automatique pour la sécurité des applications et les 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
- Configuration de l'agent NetScaler
- Obtenir le client et le fichier CSV secret à partir de Citrix Cloud
- Valider la licence de la console NetScaler
- Migrer à l'aide d'un script

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

Configuration de l'agent NetScaler

Pour activer les communications entre les instances NetScaler et NetScaler ADM, vous devez configurer un agent. Les agents NetScaler 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 aucun agent local n'est configuré pour votre ADM local existant (autonome ou paire HA), vous devez configurer au moins un agent pour le service NetScaler Console.

- Si votre ADM local existant (autonome ou paire HA) est configuré avec des agents locaux pour les déploiements multisites, vous devez configurer le même nombre d'agents pour le service NetScaler Console.

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.

Validez les licences de service NetScaler Console

Vous devez obtenir des licences pour le service NetScaler.

- Les licences VIP du service NetScaler Console doivent être supérieures ou égales aux licences VIP locales.

  > **Remarque**
  >
  > Si les licences VIP sont inférieures, les serveurs virtuels sont sélectionnés de manière aléatoire et la configuration de niveau VIP pour le service NetScaler Console échoue.

- Si vous utilisez le déploiement local d'ADM en tant que serveur de licences, réattribuez vos licences au service NetScaler Console 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 groupées dans ADM local, vous devez obtenir les licences groupées pour le service NetScaler Console, puis attribuer 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 :
  - NetScaler SDX : 13.0 74.11 ou versions ultérieures.
  - NetScaler VPX et MPX : versions 13.0 47.24 ou 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.

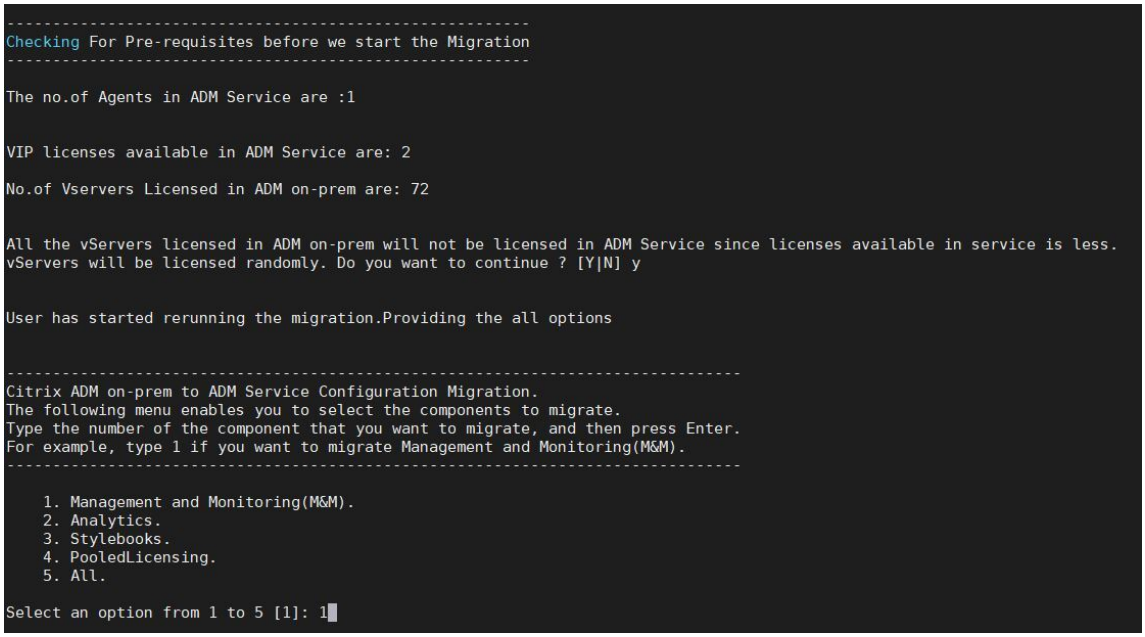
4. Pour la **version ADM 13.0 82.xx**, exécutez les commandes suivantes pour terminer la migration :

   a) `cd /mps/scripts`

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

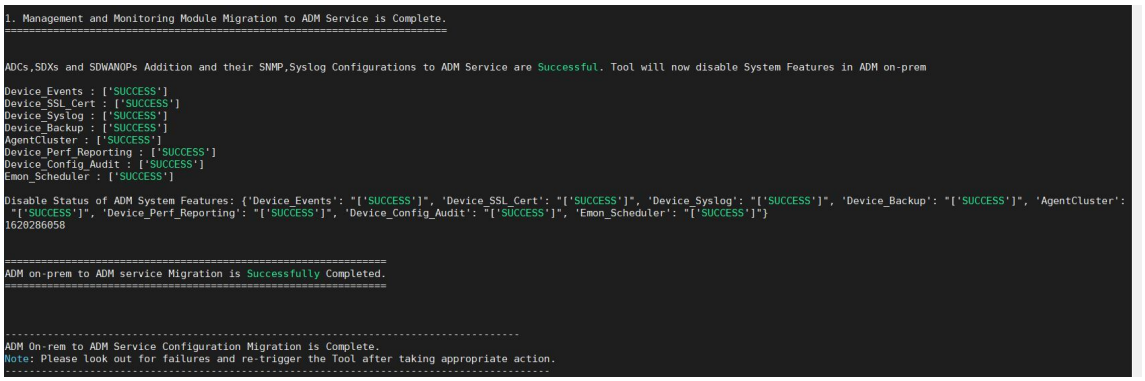
   Par exemple, `python servicemigrationtool.py /var/secureclient.csv`

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



En fonction du choix que vous offrez, seule cette fonctionnalité est migrée vers le service NetScaler Console.

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** .
> - Lorsque vous migrez des licences groupées, tous les types de licences sont migrés, y compris les serveurs virtuels.

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 NetScaler 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

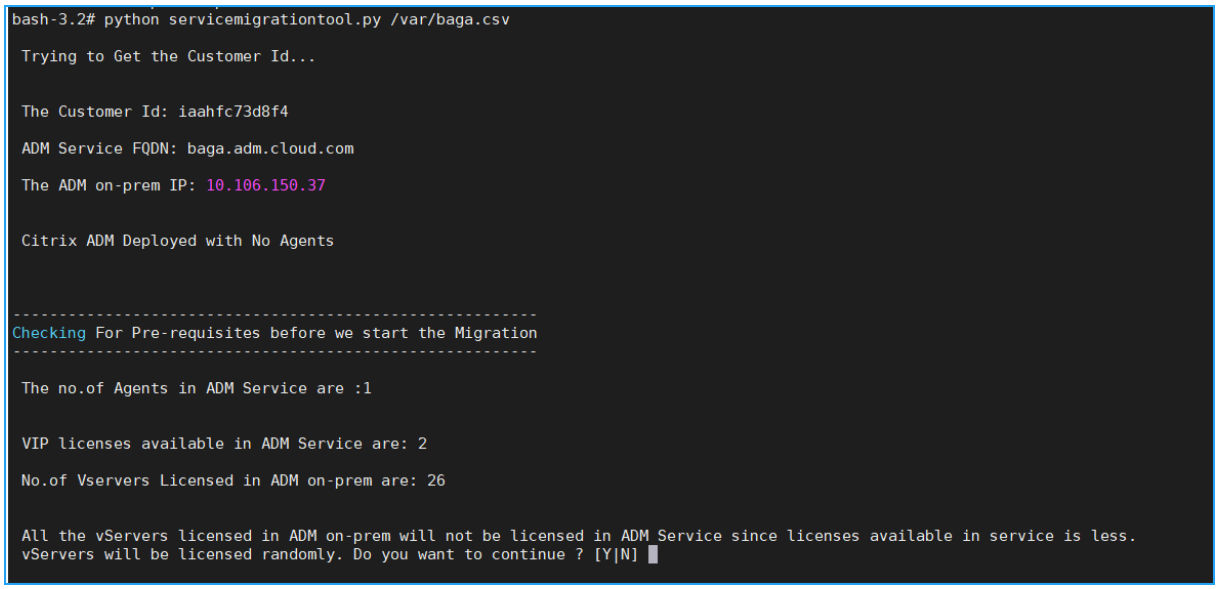
   c) Exécutez les commandes suivantes pour migrer :

      i. `cd /var`

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

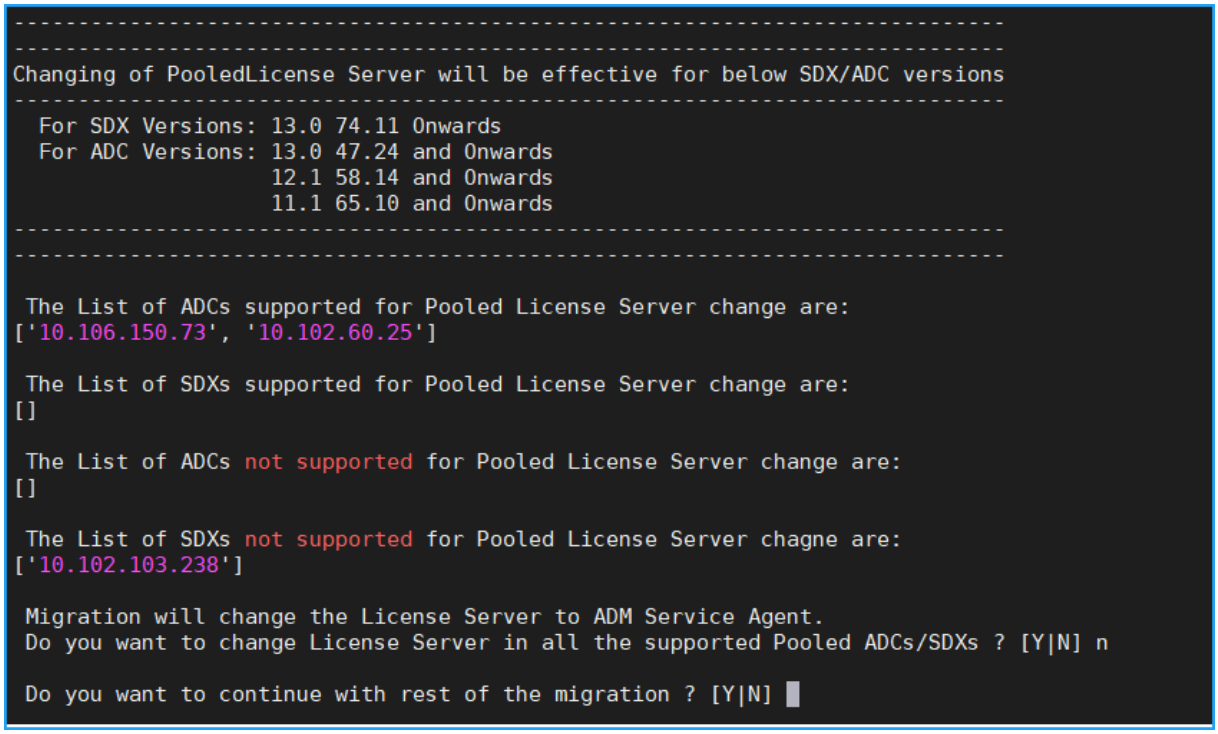
Par exemple, `python servicemigrationtool_27.py /var/secureclient.csv`

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 votre licence de service NetScaler Console est inférieure à la licence locale.



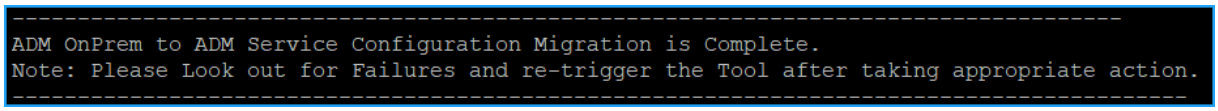
Si vous sélectionnez **Y**, la migration se poursuit en accordant une licence au VIP de manière aléatoire. Si vous sélectionnez **N**, le script arrête la migration.

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 est réussie une fois que toutes les instances ADC et leurs configurations respectives sont correctement déplacées vers le service NetScaler Console. Une fois la migration réussie, NetScaler 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 NetScaler Console) 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.

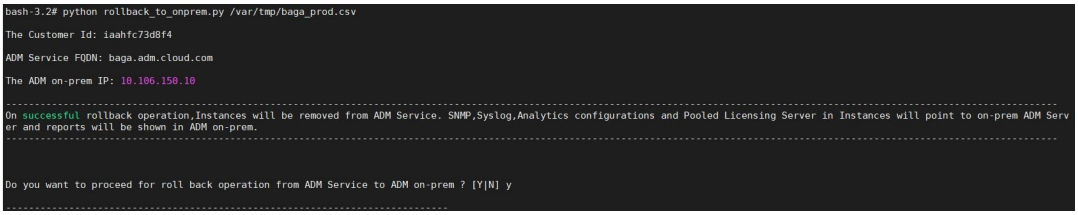
1. À l'aide d'un client SSH, connectez-vous à l'ADM local.
2. Tapez shell et appuyez sur Entrée pour passer en mode bash.
3. Pour la version **82.xx d'ADM 13.0**, exécutez les commandes suivantes pour terminer l'annulation :

    a) cd /mps/scripts

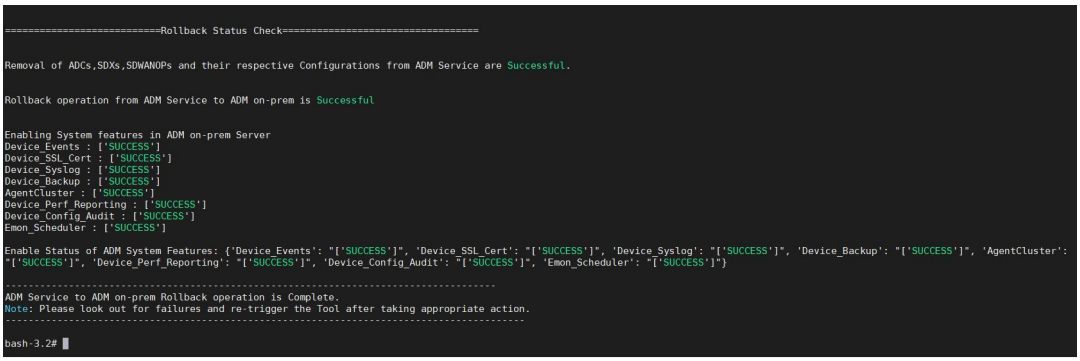
    b) rollback_to_onprem.py de python <`path of ClientID/Secret File in ADM on-prem VM`>

    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, comme l'agent NetScaler 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 une intégration plus facile et un coût de propriété inférieur à celui de NetScaler ADM sur site.
- 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 NetScaler ADM pour découvrir les dernières fonctionnalités et solutions des produits. Inscrivez-vous au webinaire en utilisant le lien suivant :

`https://www.citrix.com/events/2022/whats-new-with-citrix-application-delivery-management.html`

Que se passe-t-il après la migration si NetScaler ADM sur site 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 depuis NetScaler ADM sur site ?

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 certificats/clés SSL chargés vers NetScaler ADM sur site ne seront pas migrés vers le service ADM.

NetScaler 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 celles de NetScaler ADM VIP sur site, les serveurs virtuels reçoivent automatiquement des licences. 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 NetScaler MPX, VPX et SDX prises en charge.

Que se passe-t-il si la configuration du script de migration concernant les instances ADC échoue ?

Les instances ADC continuent de fonctionner sur la configuration 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 ADC 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 possède moins de licences que le service NetScaler 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 NetScaler ADM local est migré vers le service ADM Express Account ?

Le compte Express du service ADM ne dispose que de deux licences de serveur virtuel, de deux packs de configuration StyleBook et de deux tâches de configuration. Si votre ADM local possède plus 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']"}
```

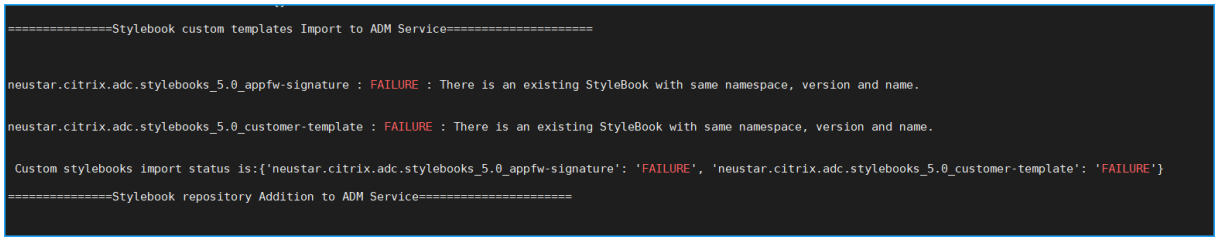
Solution : si vous avez créé des profils d'administrateur dans le service NetScaler ADM avant d'exécuter le script de migration, veillez à supprimer ces profils et à réexécuter le script de migration.

Appareil NetScaler 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']
```

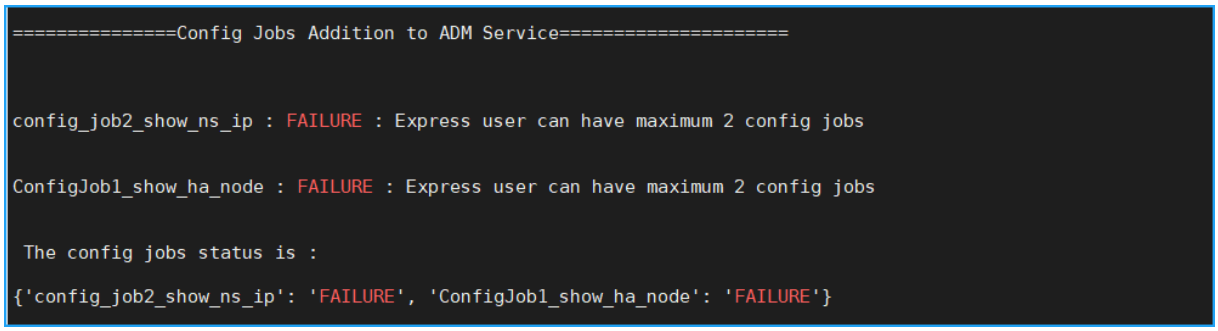
Solution : Dans ADM local, vérifiez l'état de l'instance et vérifiez si vous pouvez accéder à l'instance sans problème. Si un problème persiste, corrigez le problème et réexécutez le script de migration.

Importation de modèles personnalisés StyleBook vers le service ADM



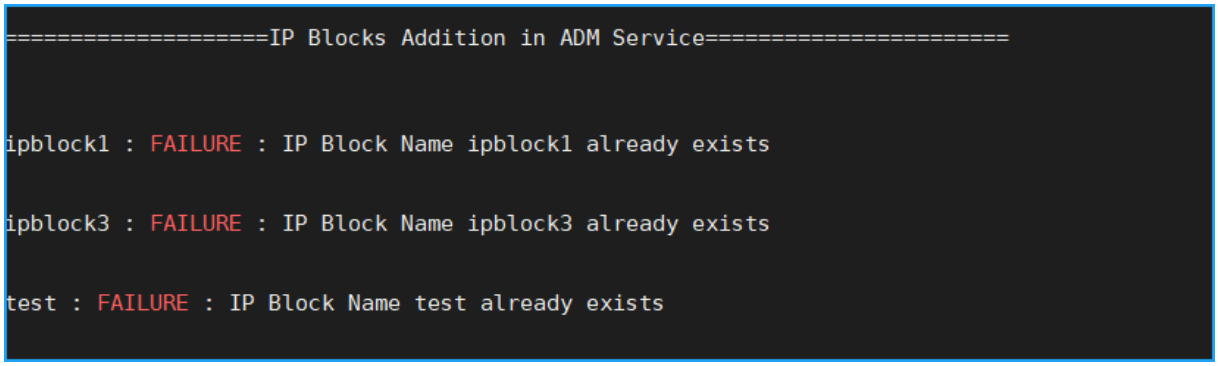
Solution : ce message d'erreur est un exemple pour le StyleBook déjà migré. Cette erreur peut également s'afficher si vous avez créé manuellement un StyleBook avec le même nom, la même version et le même espace de noms dans le service NetScaler ADM avant d'exécuter le script de migration.

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

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 NetScaler ADM
	Gestion de la configuration	Authentification	Analytics	Fonctions réseau

Gestion des instances

Comment surveiller les sites distribués à l'échelle mondiale

Comment gérer les partitions d'administration des instances NetScaler

Comment ajouter des instances à NetScaler ADM

Comment créer des groupes d'instances sur NetScaler ADM

Comment configurer des sites pour Geomaps dans NetScaler ADM

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

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

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

Comment utiliser le tableau de bord NetScaler 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 depuis NetScaler ADM

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

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

Comment redécouvrir plusieurs instances NetScaler VPX

Comment interroger des instances et des entités NetScaler dans NetScaler ADM

Comment annuler la gestion d'une instance sur NetScaler ADM

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

Gestion de la configuration

Comment créer une tâche de configuration sur NetScaler ADM

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

Comment mettre à niveau des instances NetScaler SDX à l'aide de NetScaler ADM

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

Comment replanifier des tâches configurées à l'aide de modèles intégrés dans NetScaler ADM

Comment réutiliser les tâches de configuration exécutées

Comment mettre à niveau des instances NetScaler à l'aide de NetScaler ADM

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

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

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

Comment répliquer des commandes de configuration en cours d'exécution et enregistrées d'une instance NetScaler vers une autre sur NetScaler 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 utiliser le modèle de configuration principal sur NetScaler ADM

Comment interroger l'audit de configuration des instances NetScaler

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 NetScaler ADM

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

Comment mettre à jour un certificat installé depuis NetScaler ADM

Comment associer et dissocier des certificats SSL à l'aide de NetScaler ADM

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

Comment configurer les notifications d'expiration du certificat SSL depuis NetScaler ADM

Comment utiliser le tableau de bord SSL sur NetScaler ADM

Comment interroger les certificats SSL à partir d'instances NetScaler

StyleBooks

Comment afficher différents groupes de StyleBooks

Comment créer vos propres StyleBooks

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

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

Comment créer un StyleBook pour télécharger un certificat SSL et des fichiers de clé de certificat vers NetScaler 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 NetScaler ADM

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

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

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

Comment supprimer des événements à l'aide de NetScaler ADM

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

Comment créer des règles d'événement sur NetScaler ADM

Comment modifier la gravité signalée des événements qui se produisent sur les instances NetScaler

Comment afficher le résumé des événements dans NetScaler ADM

Comment afficher la gravité des événements et l'inclinaison des interruptions SNMP sur NetScaler ADM

Comment exporter des messages Syslog à l'aide de NetScaler ADM

Comment supprimer les messages Syslog dans NetScaler 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 NetScaler ADM

Comment activer l'authentification locale de secours

Système NetScaler ADM

Comment mettre à niveau NetScaler ADM

Comment réinitialiser le mot de passe pour NetScaler ADM

Comment générer un fichier de support technique pour NetScaler ADM

Comment sauvegarder et restaurer votre serveur NetScaler ADM dans le cadre d'un déploiement sur un seul serveur

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

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

Comment configurer un serveur NTP sur NetScaler ADM

Comment configurer les paramètres SSL pour NetScaler ADM

Comment configurer l'intervalle de purge du syslog pour NetScaler ADM

Comment consulter les informations d'audit de NetScaler ADM

Comment configurer les paramètres de notification système de NetScaler ADM

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

Comment configurer un groupe de chiffrement pour NetScaler ADM

Comment créer des interruptions, des gestionnaires et des utilisateurs SNMP sur NetScaler ADM

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

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

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

Comment configurer et afficher les alarmes système sur NetScaler 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

NetScaler 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 NetScaler tels que NetScaler MPX, NetScaler VPX, NetScaler SDX, NetScaler CPX et NetScaler Gateway. 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

NetScaler 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

Vous permet de gérer les instances de NetScaler et de NetScaler Gateway.

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

NetScaler ADM rationalise 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

NetScaler 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 proposées par NetScaler 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 du trafic ICA passant par NetScaler. 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 proposées par NetScaler en fournissant une surveillance intégrée, 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 métriques des techniques d'optimisation vidéo utilisées par les instances NetScaler 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 NetScaler à l'orchestration du cloud OpenStack. NetScaler ADM et OpenStack implémentent leurs API respectives, ce qui permet d'intégrer la fonctionnalité d'équilibrage de charge (LBaaS) de l'instance NetScaler à l'orchestration du cloud OpenStack.

Orchestration

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

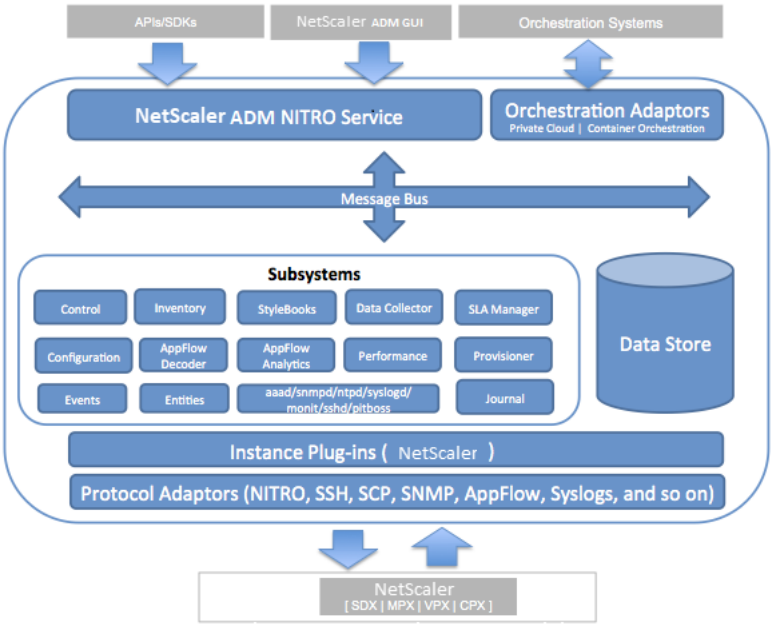
Architecture

February 1, 2024

La base de données NetScaler Application Delivery Management (ADM) est intégrée au serveur, qui 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 NetScaler ADM découvre les instances

February 1, 2024

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

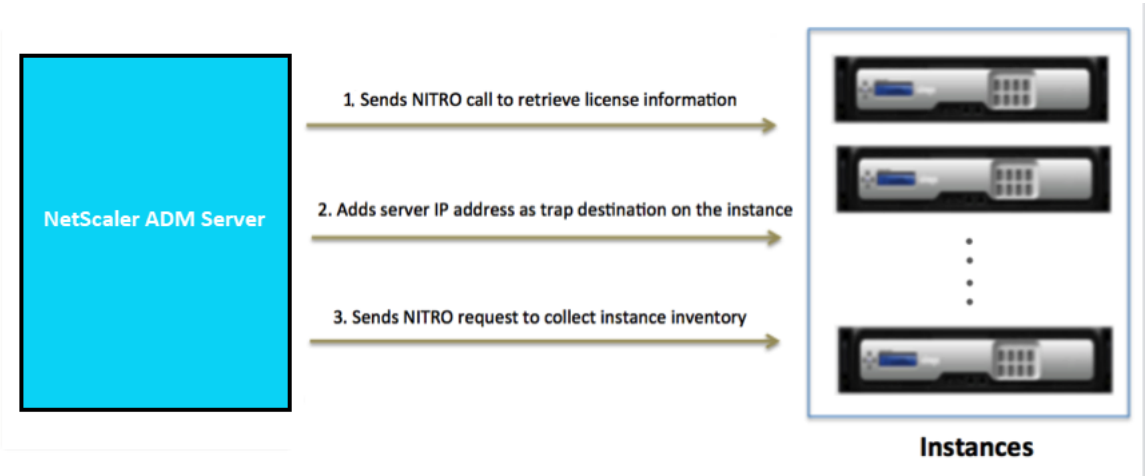
- Instances NetScaler
  - NetScaler MPX
  - NetScaler VPX
  - NetScaler SDX
  - NetScaler CPX
  - NetScaler BLX
- Instances de NetScaler Gateway

Vous pouvez ajouter des instances lors de la première configuration du serveur NetScaler ADM ou ultérieurement.

> **Remarque**
>
> NetScaler ADM utilise l'adresse IP NetScaler (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 (Independent Network Configuration) sur la paire ADC HA. Pour plus d'informations sur l'ajout d'instances, consultez la section Ajouter des instances.

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 le montre le schéma, les étapes suivantes sont exécutées implicitement par NetScaler ADM.

1. NetScaler ADM utilise les détails du profil d'instance pour se connecter à 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, NetScaler MPX, NetScaler VPX, NetScaler SDX, NetScaler BLX ou NetScaler Gateway). Lors de la détection réussie de l'instance, elle est ajoutée à la base de données d'ADM.

   Cette étape peut échouer si le profil d'instance n'inclut pas les informations d'identification correctes. Pour les instances NetScaler MPX, NetScaler VPX, NetScaler SDX, NetScaler BLX et NetScaler 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.

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

Le sondage est un processus au cours duquel NetScaler Application Delivery Management (ADM) collecte certaines informations à partir des instances NetScaler. Vous avez peut-être configuré plusieurs instances NetScaler pour votre organisation, à travers le monde. Pour surveiller vos instances via NetScaler ADM, NetScaler 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 licences, 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

NetScaler ADM utilise des protocoles tels que l'appel NITRO, Secure Shell (SSH) et Secure Copy (SCP) pour interroger les informations provenant des instances NetScaler.

Comment NetScaler ADM interroge les instances et entités gérées

NetScaler ADM interroge automatiquement à intervalles réguliers par défaut. NetScaler ADM vous permet également de configurer des intervalles d'interrogation pour certains types de sondages et vous permet d'effectuer des interrogations 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
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 **Infrastructure > Instances > NetScaler**. Sélectionnez l'instance et dans la liste **Sélectionner une action**, cliquez sur **Sauvegarde/Restaurer** .

Type de sondage	Intervalle d'interrogation	Informations sondées	Protocole utilisé	Configuration des intervalles d'interrogation
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 **Infrastructure > 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 les audits de configuration manuellement et ajouter immédiatement tous les audits de configuration des instances à NetScaler ADM. Pour ce faire, accédez à **Infrastructure > 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 NetScaler.	Appels NITRO et SCP	Oui. Accédez à **Infrastructure > 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 les certificats SSL manuellement et ajouter immédiatement tous les certificats des instances à NetScaler ADM. Pour ce faire, accédez à **Infrastructure > Tableau de bord SSL** et cliquez sur **Sonder 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 **Infrastructure > 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 NetScaler ADM. Pour ce faire, accédez à **Infrastructure > Fonctions réseau** et cliquez sur **Sonder maintenant**. La page **Sondage maintenant** vous permet d'interroger toutes les instances ou les instances sélectionnées du réseau

Remarque

Outre les sondages, les événements générés par les instances ADC gérées sont reçus par NetScaler 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 vers NetScaler 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 NetScaler gérées sont stockées en interne dans la base de données.

Différentes manières de sonder les instances

Les différentes méthodes d'interrogation utilisées par NetScaler ADM sur les instances gérées sont les suivantes :

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

Sondage mondial des instances

NetScaler 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 définir l'intervalle en fonction de vos besoins en accédant à **Infrastructure > Fonctions réseau** > **Paramètres**.

Interrogation manuelle des instances

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

Dans NetScaler ADM, il existe un intervalle d'interrogation minimum pendant lequel aucun sondage automatique n'a lieu. Si vous ajoutez une nouvelle instance NetScaler ou si une entité est mise à jour, NetScaler ADM ne reconnaît pas la nouvelle instance ni les mises à jour apportées à une entité avant le prochain sondage. 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 NetScaler, ce qui crée une lourde charge sur le réseau. Au lieu d'interroger l'ensemble du réseau, NetScaler ADM vous permet désormais d'interroger uniquement les instances et entités sélectionnées à un moment donné.

NetScaler ADM interroge automatiquement les instances gérées afin de collecter des informations à des heures précises de la journée. Le sondage sélectionné réduit le temps d'actualisation requis par NetScaler ADM pour afficher l'état le plus récent des entités liées à ces instances sélectionnées.

Pour interroger des instances spécifiques dans NetScaler ADM :

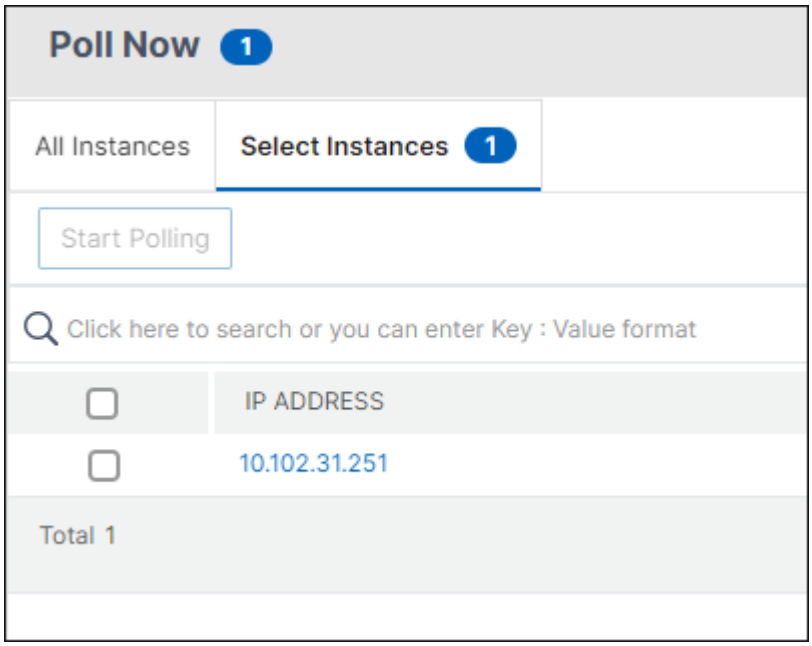
1. Dans NetScaler ADM, accédez à **Infrastructure > Fonctions**réseau.
2. Sur la page **Fonctions réseau**, en haut à droite, cliquez sur **Sondage maintenant** .

3. La page contextuelle **Poll Now** vous permet d'interroger toutes les instances NetScaler du réseau ou d'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**.



NetScaler ADM lance un sondage manuel et ajoute toutes les entités.

Interrogation manuelle des entités

NetScaler ADM vous permet également de n'interroger que 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 interrogez une entité, NetScaler ADM interroge uniquement cette entité et met à jour l'état dans l'interface graphique de NetScaler 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 NetScaler 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 NetScaler ADM, accédez à**Infrastructure > Fonctions réseau > Équilibrage de charge > Serveurs virtuels**.
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

ADM On-Prem Cloud Connector permet à Citrix Cloud de collecter des données de licence, de configuration et d'utilisation à des fins de conformité des licences, et de gérer, mesurer et améliorer le service. À partir de la version 14.1 8.x ou ultérieure, vous pouvez configurer Cloud Connector pour activer une connexion entre le service ADM et ADM On-Prem. En activant le Cloud Connector ADM On-Prem :

- Les données de licence et d'utilisation obligatoires pour la conformité aux licences Flexed sont collectées.
- Vous pouvez obtenir la fonction d'**avis de sécurité** dans ADM On-Prem. Pour plus d'informations, consultez la section Cloud Connector sur site d'ADM.

Après avoir activé Cloud Connector, la collecte des métriques de données est activée.

Catégories de données

Les tableaux suivants fournissent les détails des paramètres collectés après l'activation de Cloud Connector :

Catégories	Description	Utilisation
Déploiement et utilisation des fonctionnalités de NetScaler	Informations sur le déploiement et l'utilisation de NetScaler, telles que le nom du client, l'identifiant du client, le nombre total d'appareils gérés et le nombre total d'appareils gérés actifs.	Pour gérer, mesurer et améliorer le service.
Déploiement de NetScaler ADM	Informations sur NetScaler	Pour gérer, mesurer et améliorer le service.
Licences, droits et utilisation de NetScaler et NetScaler ADM	Droits, licences	Conformité des licences et gestion, mesure et amélioration du service.

NetScaler et NetScaler ADM - Paramètres de déploiement et d'utilisation des fonctionnalités

Paramètres	Description
onprem_ip	L'adresse IP de l'ADM
t_dix	Le nombre total de locataires connectés à ADM
déployer	Vérifie si le type de déploiement ADM est autonome ou en paire HA
is_dr	Vérifie si le nœud de reprise après sinistre est configuré ou non
is_agt	Vérifie si l'agent ADM sur site est configuré ou non
is_cloud	Vérifie si le déploiement ADM est un service ADM ou ADM sur site
is_cntr	Vérifie si le déploiement d'ADM se fait dans le cluster Kubernetes
plateforme	La plateforme sur laquelle l'ADM est hébergé. Par exemple, Citrix Hypervisor
total_users	Le nombre total d'utilisateurs locaux d'ADM
total_gui_requests	Nombre total d'utilisateurs connectés à l'interface graphique ADM au cours des dernières 24 heures

Paramètres	Description
total_api_requests	Le nombre total de demandes via l'API adressées à ADM au cours des dernières 24 heures. Cela inclut également les utilisateurs de proxy distants (demandes de l'agent).
total_api_external_requests	Le nombre total de demandes via l'API adressées à ADM qui excluent les demandes de l'agent
total_custom_apps	Le nombre total d'applications personnalisées dans ADM
total_managed_apps	Nombre total d'applications gérées dans ADM
total_apps	Le nombre total de demandes dans ADM
total_custom_sites	Nombre total de sites personnalisés configurés dans ADM
total_managed_devices	Nombre total d'instances NetScaler gérées dans ADM
total_active_managed_devices	Nombre total d'instances NetScaler à l'état UP
total_ns_device	Nombre total d'instances MPX gérées dans ADM
total_ngvpx_device	Le nombre total d'instances Gateway VPX gérées dans ADM
total_nswg_device	Nombre total d'instances de passerelle Web gérées dans ADM
total_nswgvpx_device	Nombre total d'instances VPX de passerelle Web gérées dans ADM
total_nsvpx_device	Le nombre total d'instances VPX gérées dans ADM
total_cpx_device	Le nombre total d'instances CPX gérées dans ADM
total_nsap_device	Nombre total d'instances de partition d'administration dans ADM
total_nssdx_device	Le nombre total d'instances SDX gérées dans ADM
total_agents	Nombre total d'agents ADM sur site configurés
total_active_agents	Le nombre total d'agents ADM sur site qui sont à l'état UP
total_custom_event_rules	Le total des règles d'événement personnalisées créées dans ADM
regles_total_event_rules	Le total des règles d'événement créées dans ADM

Paramètres	Description
total_stylebook_config_store_count	Le nombre total de packs de configuration créés dans ADM
total_user_sb_stylebook_count	Le nombre total de packs de configuration personnalisés créés dans ADM
total_waf_devices	Nombre total d'instances NetScaler activées en cas de violations du WAF
total_gw_devices	Nombre total d'instances NetScaler activées avec le VPN SSL
total_icaproxy_devices	Nombre total d'instances NetScaler activées avec HDX Insight dans ADM
total_bot_devices	Nombre total d'instances NetScaler activées en cas de violations de bots
total_pooled_devices	Nombre total d'instances NetScaler (gérées et non gérées) avec licences groupées
total_config_audit	Le modèle d'audit de configuration total configuré dans ADM
total_config_job	Le nombre total de tâches de configuration créées dans ADM
total_ssl_certs	Le nombre total de certifications SSL créées/modifiées/supprimées d'ADM
total_network_report	Le rapport réseau total créé dans ADM
total_k8s	Le NetScaler ADM hébergé sur le cluster Kubernetes. Le nombre total de clusters Kubernetes.
total_ipam	Le nombre total de fournisseurs IPAM ajoutés dans ADM
total_rbac_groups	Le nombre total de groupes RBAC configurés dans ADM
total_ingress_deployed	Le nombre total de contrôleurs d'entrée dans Kubernetes.
total_ipam_configured	Le nombre total de réseaux IPAM ajoutés dans ADM
total_web_transaction_analytics	Nombre total d'instances NetScaler activées avec l'analyse des transactions Web
total_pager_duty_profile	Le nombre total de profils PagerDuty ajoutés dans ADM
total_slack_profile	Le nombre total de profils Slack ajoutés dans ADM

Paramètres	Description
total_api_discovery	Nombre total d'instances NetScaler recevant des demandes d'API
total_lb_devices	Nombre total d'instances NetScaler configurées avec des serveurs virtuels d'équilibrage de charge
total_lb_devices_http	Nombre total d'instances NetScaler configurées avec des serveurs virtuels HTTP d'équilibrage de charge
total_lb_devices_ssl	Nombre total d'instances NetScaler configurées avec des serveurs virtuels SSL d'équilibrage de charge
total_cs_devices	Nombre total d'instances NetScaler configurées avec des serveurs virtuels de commutation de contenu
total_gslb_devices	Nombre total d'instances NetScaler configurées avec des serveurs virtuels d'équilibrage de charge de serveur global
total_aaa_devices	Nombre total d'instances NetScaler configurées avec des serveurs virtuels AAA
t_radius_svr	Nombre total de serveurs d'authentification RADIUS configurés dans ADM
t_ldap_svr	Nombre total de serveurs d'authentification LDAP configurés dans ADM
t_tacacs_svr	Nombre total de serveurs d'authentification TACACS configurés dans ADM
agent_id	L'identifiant unique de l'agent déployé
plateforme	Plateforme sur laquelle l'agent est hébergé. Par exemple, Citrix Hypervisor
version	Version de l'agent ADM
ville	Ville où l'agent ADM est déployé
pays	Pays dans lequel l'agent ADM est déployé
region	Région dans laquelle l'agent ADM est déployé
device_id	L'ID unique de l'instance VPX
version	La version de compilation de l'instance VPX
état	L'état actuel (UP ou Down) de l'instance VPX

Paramètres	Description
device_platform	La plate-forme sur laquelle l'instance VPX est hébergée
racine	Détails de l'utilisation du disque ADM dans les répertoires /var, /root, /flash, /var/mps
total	L'espace disque ADM total (unité : octets)
utilisé	L'espace disque ADM total utilisé
gratuit	L'espace disque ADM total disponible
Adm_analt_dx - Feature	Type d'analyse (Bot, WAF, Web Insight, Service Graph, etc.) pour lequel les problèmes sont identifiés.
Adm_analt_dx - issue_type	Catégorie de problème à laquelle appartient le problème identifié. Par exemple, licences, configuration
Adm_analt_dx - sub_issue_type	Catégorie de sous-problème correspondant au problème identifié. Le sous-problème peut être NO_VIPS_LICENSED, BOT_INSIGHT_IN_ACTION_DISABLED, NS_FEATURE_DISABLED, VSERVER_WITHOUT_BOT_POLICY_BINDING, NO_INSIGHT_IN_ACTION_DISABLED, VSERVER_WITHOUT_APPFIREWALL_POLICY_BINDING, SECURITY_INSIGHT_IN_ACTION_DISABLED, NO_CPX_VIPS_PS_BINDING PRESENT, COLLECTOR_UNBOUND_IN_VSERVER, VSERVER_WITHOUT_APPFLOW_POLICY_BINDING
feature	La fonctionnalité d'analyse activée sur les serveurs virtuels d'équilibrage de charge/de commutation de contenu
total_lbvserver_ft_enabled	Nombre total de serveurs virtuels d'équilibrage de charge sur lesquels au moins une fonctionnalité d'analyse est activée
total_csvserver_ft_enabled	Nombre total de serveurs virtuels de commutation de contenu sur lesquels au moins une fonctionnalité d'analyse est activée
feature_enabled_on_vpn	La fonctionnalité d'analyse activée sur les serveurs virtuels VPN

Paramètres	Description
total_vpnvserver_ft_enabled	Nombre total de serveurs virtuels VPN sur lesquels au moins une fonctionnalité d'analyse est activée

Éléments de données relatifs aux licences, aux droits et à l'utilisation de NetScaler et NetScaler ADM

Paramètres	Description
pool_instances_entitled	Le nombre total d'instances de pool intitulées
pool_instances_used	Nombre total d'instances groupées utilisées
pool_fips_instances_entitled	Le nombre total d'instances FIPS du pool appelées
pool_fips_instances_used	Nombre total d'instances FIPS du pool utilisées
pool_entvcpu_entitled	Le pool total de vCPU d'entreprise intitulé
pool_entvcpu_used	Le nombre total de processeurs virtuels d'entreprise utilisés
pool_entbw_entitled	La bande passante d'entreprise totale du pool intitulée [Mo/s]
pool_entbw_used	La bande passante totale utilisée par l'entreprise dans le pool [Mo/s]
pool_pltbw_entitled	La bande passante Platinum totale du pool intitulée [Mo/s]
pool_pltbw_used	La bande passante Platinum totale utilisée dans le pool [Mo/s]
pool_pltvcpu_entitled	Le pool total de vCPU Platinum intitulé
pool_pltvcpu_used	Le pool total de vCPU Platinum utilisés
pool_stdbw_entitled	La bande passante standard totale du pool intitulée
pool_stdbw_used	La bande passante standard totale du pool utilisée
pool_stdvcpu_entitled	Le pool total de vCPU standard intitulé
pool_stdvcpu_used	Le pool total de vCPU standard utilisés
pool_cpxvcpu_entitled	Le pool total de vCPU CPX intitulé

Paramètres	Description
pool_cpxvcpu_used	Le pool total de vCPU CPX utilisés
pool_perc_instances_used	Le % d'instances utilisées
pool_perc_vcpu_used	Le % de vCPU utilisés
pool_perc_bw_used	Le % de bande passante utilisée
total_entitled_vservers	Le nombre total de serveurs virtuels autorisés
total_used_vservers	Nombre total de serveurs virtuels utilisés
total_discovered_vservers	Nombre total de serveurs virtuels découverts
perc_used_vservers	Le pourcentage de serveurs virtuels utilisés/autorisés
perc_discovered_vservers	Le pourcentage de serveurs virtuels découverts ou autorisés
is_local_license	Vérifie si la licence est hébergée dans NetScaler ADM
license_edition	Type de licence (Platinum/Standard/Enterprise)
is_pooled_license	Vérifie si la licence est une licence groupée
model_id	L'ID du modèle de l'instance
plt_license_allocation	L'attribution des licences Platinum
ent_license_allocation	L'allocation des licences d'entreprise
std_license_allocation	L'allocation de licence standard
license_end_date	Nombre total de jours avant l'expiration de la licence
plateforme	Le type d'appareil
instance_id	L'identifiant unique de l'instance
instance_mode	Vérifie si l'instance est une instance autonome ou une paire HA
instance_state	État de l'instance (haut/bas)
flex_vpx_inst_entitled	Le nombre total d'instances VPX autorisées
flex_vpx_inst_allocated	Le nombre total d'instances VPX allouées
flex_sdx_inst_entitled	Le nombre total d'instances SDX autorisées
flex_sdx_inst_allocated	Le nombre total d'instances SDX allouées
flex_mpx_inst_entitled	Le nombre total d'instances MPX autorisées

Paramètres	Description
flex_mpx_inst_allocated	Le nombre total d'instances MPX allouées
flex_plt_bw_entitled	La bande passante Platinum intitulée
flex_plt_bw_allocated	La bande passante Platinum allouée
flex_ent_bw_entitled	La bande passante d'entreprise autorisée
flex_ent_bw_allocated	La bande passante d'entreprise allouée
flex_std_bw_entitled	La bande passante standard intitulée
flex_std_bw_allocated	La bande passante standard allouée
flex_vpx_fips_inst_entitled	Le nombre total d'instances FIPS autorisées
flex_vpx_fips_inst_allocated	Le nombre total d'instances FIPS allouées

Si votre NetScaler ADM est une version 14.1 4.x ou inférieure, vous pouvez créer une identité client sur Citrix Cloud pour envoyer des statistiques importantes sur l'état et l'état d'ADM, ainsi que d'autres mesures issues du déploiement d'ADM On-Prem vers un compte Citrix Cloud. Citrix collecte des statistiques pour comprendre l'utilisation de NetScaler ADM. Pour plus d'informations, consultez la section Gouvernance des données pour l'identité du client.

Licences

February 1, 2024

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

NetScaler ADM prend en charge les éditions de licence suivantes. Contactez votre représentant commercial ou partenaire NetScaler pour acheter une licence ADM.

Édition Express : vous pouvez gérer et surveiller un nombre illimité d'instances avec la licence de l'édition Express. Par défaut, la licence de l'édition Express est appliquée.

Édition avancée - Elle permet de gérer les applications découvertes et de visualiser les analyses pour les serveurs virtuels achetés ainsi que pour les serveurs virtuels gratuits.

Points à noter:

- Pour les versions **13.1-9.x ou antérieures**, vous pouvez gérer jusqu'à 30 applications découvertes ou serveurs virtuels et afficher des analyses. Au-delà des 30 applications découvertes ou

des 30 serveurs virtuels, vous devez acheter et appliquer une licence Advanced. Par exemple, si vous achetez 100 licences de serveur virtuel, vous êtes autorisé à utiliser jusqu'à 130 licences de serveur virtuel.

- Pour les versions **13.1-12.x ou ultérieures**, vous pouvez gérer jusqu'à deux applications découvertes ou serveurs virtuels et afficher des analyses. Au-delà des deux applications découvertes ou des deux serveurs virtuels, vous devez acheter et appliquer une licence Advanced. Par exemple, si vous achetez 100 licences de serveur virtuel, vous êtes autorisé à utiliser jusqu'à 102 licences de serveur virtuel.

Après la mise à niveau vers la version 13.1-12.x :

- Tous les serveurs virtuels gratuits par défaut d'Express restent fonctionnels pendant 30 jours. Vous pouvez sélectionner les 2 serveurs virtuels et appliquer les 2 licences par défaut dans le délai de grâce de 30 jours. Si aucune action de l'utilisateur n'est entreprise 30 jours après la mise à niveau, ADM applique aléatoirement la licence à 2 serveurs virtuels et annule les licences des serveurs virtuels restants. Vous devez acheter et appliquer de nouvelles licences Advanced pour activer ces serveurs virtuels.
- Après la mise à niveau, voici les modifications apportées au comportement d'ADM :
  - ADM applique un délai de grâce de 30 jours.
  - Au cours de la période de grâce de 30 jours, l'allocation de nouveaux serveurs virtuels pour les 30 serveurs virtuels gratuits express est bloquée.
    * Par exemple, si le nombre de licences de serveur virtuel disponibles avant la mise à niveau vers la version 12.x était de 30 et que seuls 20 serveurs virtuels sous licence étaient utilisés, vous n'êtes autorisé à utiliser que les 20 serveurs virtuels et vous n'êtes pas autorisé à acheter des licences pour les 10 serveurs virtuels restants pendant la période de grâce de 30 jours.
  - Toutefois, pendant la période de grâce de 30 jours, en tant qu'administrateur, vous pouvez toujours appliquer des licences Advanced ADM et allouer de nouveaux serveurs virtuels.

Fonctionnalités	Options	Édition Express	Édition Advance	Licence NetScaler
Applications	Tableau de bord des applications	Jusqu'à deux serveurs virtuels.	Autorisé pour toutes les licences de serveur virtuel achetées et deux serveurs virtuels supplémentaires.	Les informations relatives à NetScaler Web App Firewall sur App Dashboard nécessitent une licence Premium (ou) Advanced avec App Firewall.
		Web Insight	Jusqu'à deux serveurs virtuels.	Autorisé pour toutes les licences de serveur virtuel achetées et deux serveurs virtuels supplémentaires.
		Graphique de service	Jusqu'à deux serveurs virtuels.	Autorisé pour toutes les licences de serveur virtuel achetées et deux serveurs virtuels supplémentaires.
		Configuration > StyleBooks	Illimité	Illimité
Security	Tableau de bord sécurité	Jusqu'à deux serveurs virtuels.	Autorisé pour toutes les licences de serveur virtuel achetées et deux serveurs virtuels supplémentaires.	Les informations relatives à NetScaler Web App Firewall sur Security Dashboard nécessitent une licence Premium (ou) Advanced avec App Firewall.

Fonctionnalités	Options	Édition Express	Édition Advance	Licence NetScaler
		Infractions de sécurité	Jusqu'à deux serveurs virtuels.	Autorisé pour toutes les licences de serveur virtuel achetées et deux serveurs virtuels supplémentaires.
		Utilisateurs et points de terminaison	Jusqu'à deux serveurs virtuels.	Autorisé pour toutes les licences de serveur virtuel achetées et deux serveurs virtuels supplémentaires.
Gateway	HDX Insight	Jusqu'à deux serveurs virtuels.	Autorisé pour toutes les licences de serveur virtuel achetées et deux serveurs virtuels supplémentaires.	Avancé (reporting < 1 heure) Premium (reporting = illimité)
		Gateway Insight	Jusqu'à deux serveurs virtuels.	Autorisé pour toutes les licences de serveur virtuel achetées et deux serveurs virtuels supplémentaires.
Infrastructure	Analyse de l' infrastructure	Illimité	Illimité	SO
		Instances	Illimité	Illimité
		Tableau de bord SSL	Illimité	Illimité
		Événements	Illimité	Illimité
		Fonctions réseau	Illimité	Illimité
		Rapports sur le réseau	Illimité	Illimité

Fonctionnalités	Options	Édition Express	Édition Advance	Licence NetScaler
		Licences groupées	Illimité	Illimité
		Configuration > Travaux de configuration, modèles de configuration et conseils de configuration	Illimité	Illimité
		Mettre à niveau les tâches	Illimité	Illimité
		Orchestration	Illimité	Illimité
		WAN Insight	Illimité	Illimité
Paramètres	Authentification RBAC et externe (niveau d'instance)	Illimité	Illimité	SO
		RBAC et authentification externe	Illimité	Illimité

*Pour l'intégration de Citrix Director au support NetScaler 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 NetScaler ADM via l'interface graphique de NetScaler ADM.

Haute disponibilité

Le serveur NetScaler ADM peut contenir des licences VIP, CICO et des licences 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.

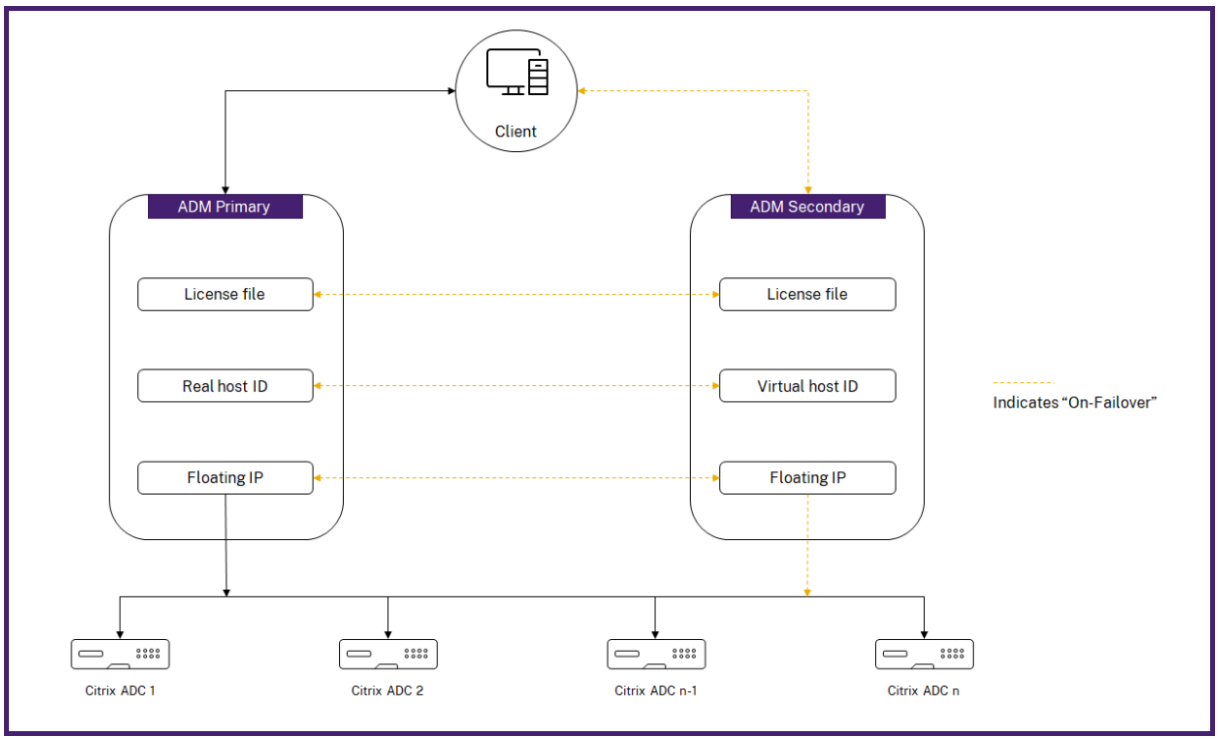
Si vous configurez une paire ADM haute disponibilité en tant que serveur de licences, les serveurs principal et secondaire doivent avoir les mêmes fichiers de licence. Par conséquent, dans le déploiement haute disponibilité d'ADM, NetScaler ADM vous permet d'attribuer les mêmes fichiers de licence aux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

> **Remarque**
>
> - Si vous avez installé NetScaler ADM 12.1.49.x ou des versions antérieures, vous bénéficiez d'un délai de grâce de 30 jours pour conserver la licence 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 NetScaler 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 licences 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 NetScaler extraient les licences du Node-1 à l'aide de l'adresse IP flottante.

Les licences sont verrouillées sur les instances ADC. Pour récupérer des licences auprès d'un NetScaler ADM HA, les instances ont besoin de l'adresse IP de l'appliance spécifique. Lorsque vous appliquez des licences sur un serveur principal, celui-ci sera chargé des licences, et il appliquera 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.

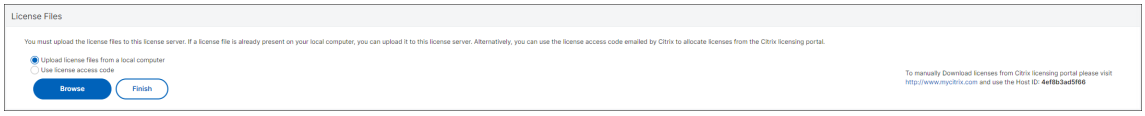
Mettre à niveau les licences de serveur virtuel

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

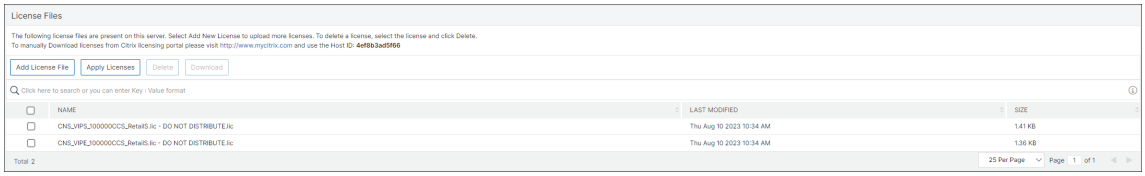
Pour mettre à niveau les licences de votre appliance :

1. Connectez-vous à NetScaler ADM à l'aide des informations d'identification de l'administrateur.
2. Accédez à**Infrastructure > Licences groupées**.
3. Accédez à **Fichiers de licences**, 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 attribuer 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, NetScaler 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 NetScaler ADM en accédant à **Paramètres > Configuration des licences**et des analyses.

Gérer les serveurs virtuels

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

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

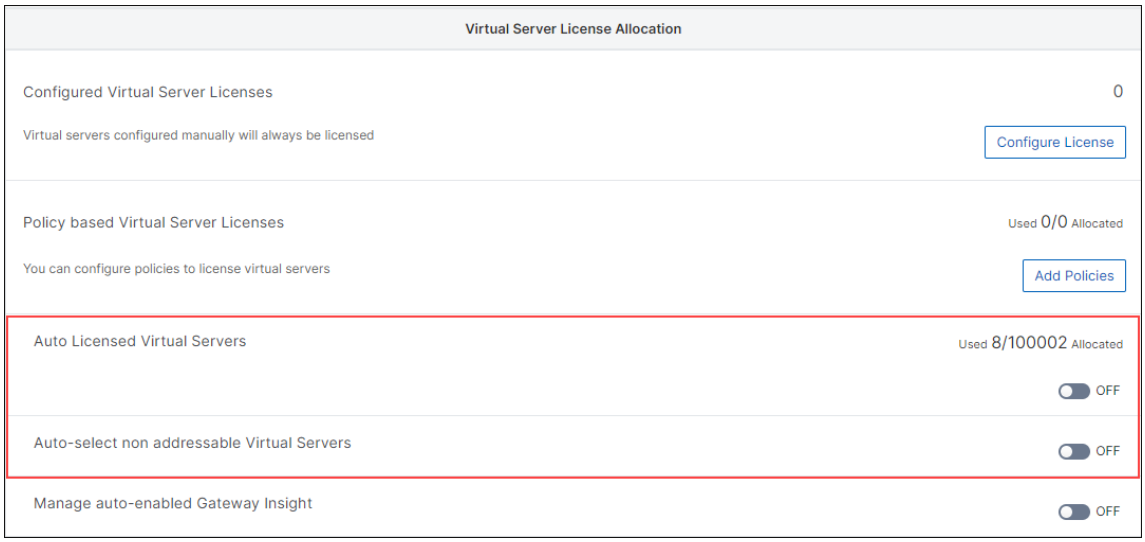
Pour sélectionner manuellement les serveurs virtuels ou pour limiter les licences aux serveurs virtuels limités, vous devez d'abord désactiver la licence automatique des serveurs virtuels, puis sélectionner les serveurs virtuels que vous souhaitez gérer.

Désactiver les serveurs virtuels sous licence automatique

1. Accédez à **Paramètres > Configuration des licences et des 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**.

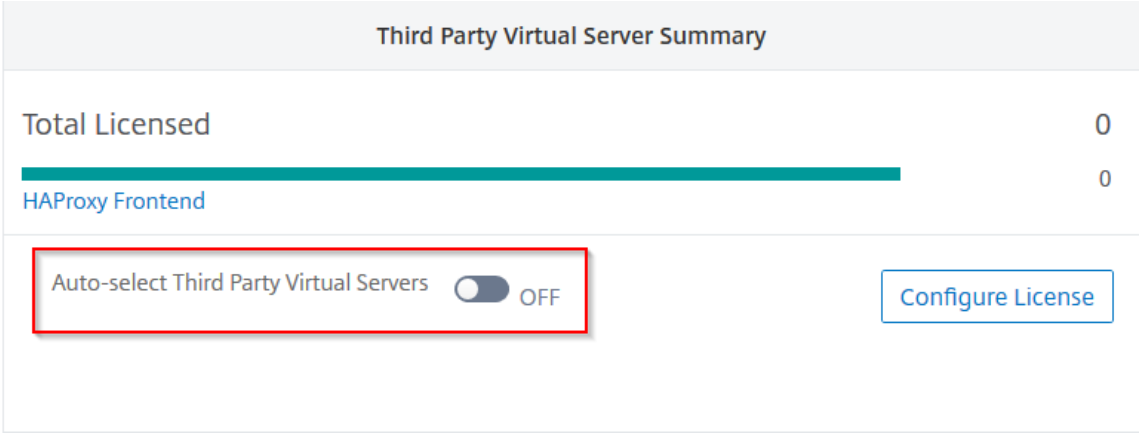


Sélection de serveurs virtuels tiers pour les licences

1. Accédez à **Paramètres > Configuration des licences et des 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

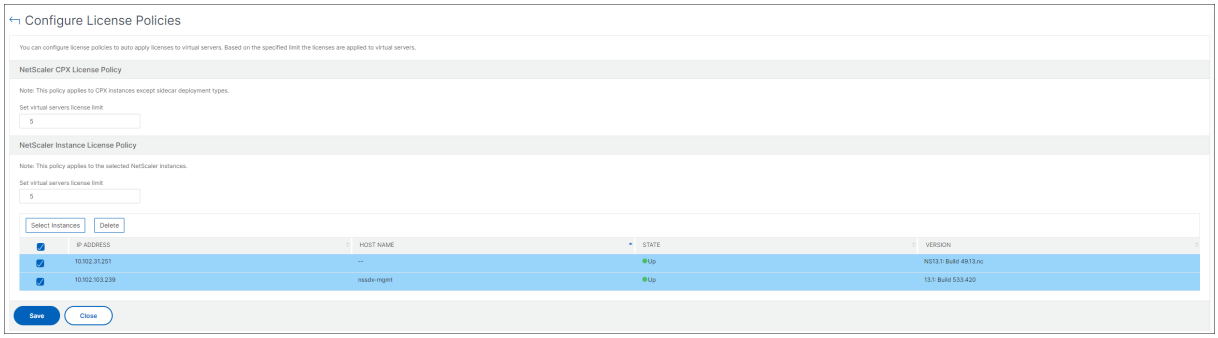
Vous pouvez configurer une stratégie pour appliquer une licence aux serveurs virtuels. Cette stratégie contrôle le nombre de serveurs virtuels pour lesquels vous souhaitez octroyer une licence automatique. Il applique également les licences aux serveurs virtuels des instances sélectionnées uniquement.

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 afficher les serveurs virtuels sous licence ou les serveurs virtuels tiers.

1. Accédez à **Paramètres > Configuration des licences et des 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, NetScaler ADM n'applique pas automatiquement de 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.

NetScaler ADM fournit une option dans NetScaler ADM sous Allocation de licences de serveur virtuel. Si vous activez l'option **Sélection automatique des serveurs virtuels non adressables**, appliquez automatiquement les licences des serveurs virtuels non adressables.

> **Remarque**
>
> - Par défaut, NetScaler 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 consulter l'état de l'expiration de la licence du serveur virtuel et définir des alertes en cas d'expiration dans NetScaler ADM.

Pour afficher l'état des licences :

1. Accédez à **Infrastructure > Licences groupées > 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 **Infrastructure > Licences groupées > 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 NetScaler ADM, vous devez comprendre la configuration logicielle requise, la configuration requise pour le navigateur, les informations de port, les informations de licence et les limites.

Exigences relatives à NetScaler ADM

Composant	Exigences
RAM	32 GB
CPU virtuel	8 processeurs **Remarque :**nous vous recommandons d'utiliser la technologie SSD pour les déploiements NetScaler ADM.
Espace de stockage	L'espace de stockage par défaut requis est de 120 Go. Les besoins de stockage réels dépendent de l'estimation du dimensionnement de NetScaler ADM. Utilisez le calculateur de dimensionnement pour calculer les estimations de stockage. Contactez votre représentant NetScaler pour accéder au calculateur de dimensionnement.

Composant	Exigences
	Si vos besoins de stockage NetScaler ADM dépassent 120 Go, vous devez connecter un disque supplémentaire. Vous ne pouvez ajouter qu'un seul disque supplémentaire. Nous vous recommandons d'estimer l'espace de stockage et de connecter des disques supplémentaires au moment du déploiement initial. Pour plus d'informations, consultez Comment attacher un disque supplémentaire à NetScaler ADM.
Interfaces réseau virtuelles	1
Débit	1 Gbit/s ou 100 Mbit/s

Exigences relatives à l'agent NetScaler ADM sur site

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

> **Remarque**
>
> Le processeur AMD est pris en charge dans :
>
> - **NetScaler ADM 13.1 build**4.43 ou version ultérieure.
> - **Agent NetScaler ADM 13.1 build**17.42 ou version ultérieure.

Version minimale de NetScaler requise pour les fonctionnalités de NetScaler ADM

> **Important**
>
> La version et la compilation de NetScaler ADM doivent être **égales ou supérieures à** vos versions et build NetScaler. Par exemple, si vous avez installé NetScaler ADM 12.1 Build 50.39, assurez-vous d'avoir installé NetScaler 12.1 Build 50.28/50.31 ou une version antérieure.

Fonctionnalité NetScaler ADM	Version du logiciel NetScaler
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 NetScaler, 10.1 et versions ultérieures Pour NetScaler 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
Violations de sécurité WAF	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 NetScaler ADM avec les instances NetScaler exécutant la version 11.0 build 66.x.

Exigences relatives aux analyses NetScaler ADM

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

Fonctionnalité NetScaler ADM	Version Citrix Virtual Apps and Desktops
HDX Insight	Citrix Virtual Apps and Desktops 7.0 et versions ultérieures

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

NetScaler ADM peut générer des rapports pour les applications publiées sur Citrix Virtual Apps ou Citrix Virtual Desktops et accessibles via Citrix Workspace. Toutefois, cette fonctionnalité dépend du système d'exploitation sur lequel Workspace est installé. Actuellement, NetScaler n'analyse pas le trafic ICA pour les applications ou les postes de travail accessibles via Citrix Workspace 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 Dell Wyse basés sur 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 NetScaler requise pour HDX Insight

Les données collectées par NetScaler ADM pour HDX Insight dépendent de la version et des licences des instances NetScaler surveillées. Les rapports HDX Insight s'affichent uniquement pour les appliances NetScaler Premium et Advanced exécutant la version 10.5 et les versions ultérieures.

Licence/durée de licence NetScaler	5 minutes	1 heure	1 jour	1 semaine	1 mois
Standard	Non	Non	Non	Non	Non
Advanced	Oui	Oui	Non	Non	Non

Licence/durée de licence NetScaler	5 minutes	1 heure	1 jour	1 semaine	1 mois
Premium	Oui	Oui	Oui	Oui	Oui

Hyperviseurs pris en charge

Le tableau suivant répertorie les hyperviseurs pris en charge par NetScaler 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, RHEL 8.0, Ubuntu 16.04 et Ubuntu 18.04

Systèmes d'exploitation et versions de Workspace pris en charge

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

Système d'exploitation	Version Workspace
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

Navigateurs pris en charge

Le tableau suivant répertorie les navigateurs Web pris en charge par NetScaler 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

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

> **Remarque**
>
> Si vous avez configuré NetScalers en mode haute disponibilité, NetScaler ADM utilise NSIP pour communiquer avec NetScaler et les ports requis restent les mêmes.

Schéma des ports réseau pour un déploiement sans agent :

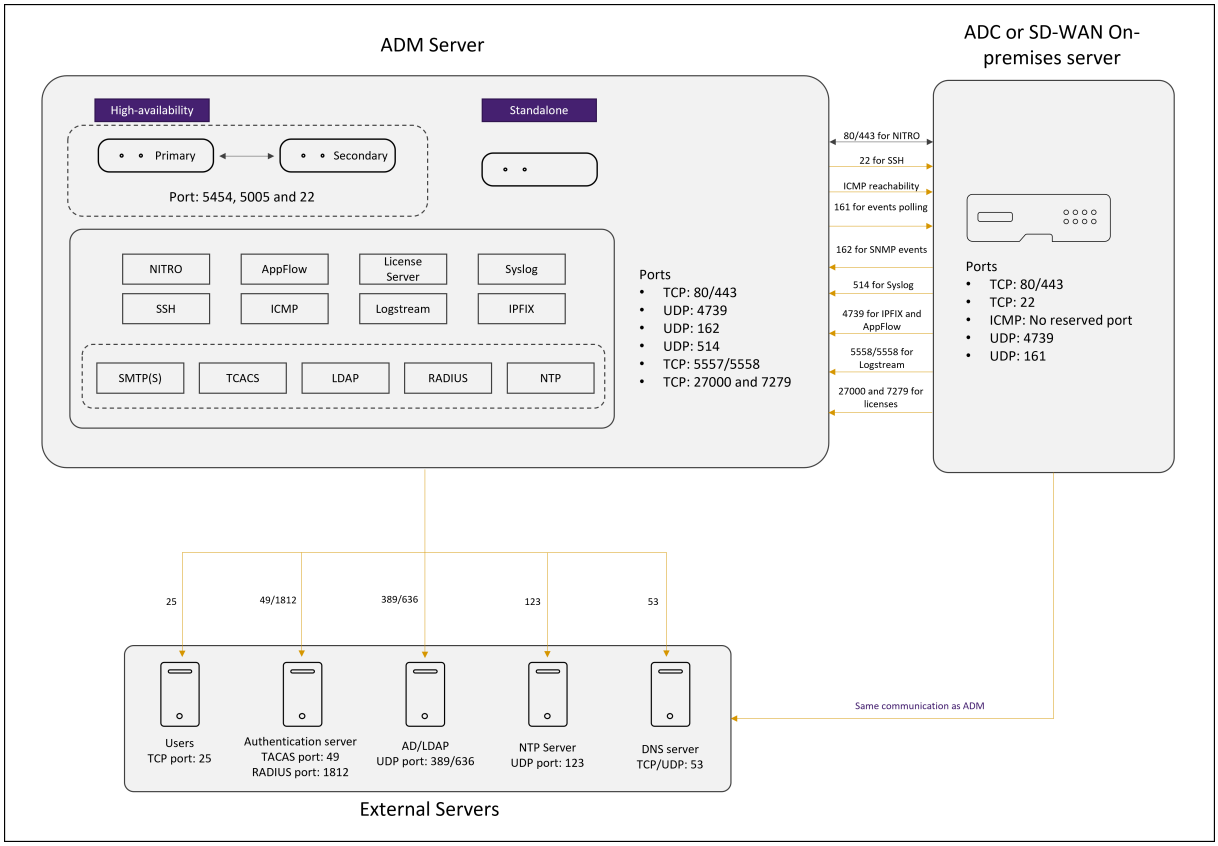


Diagramme des ports réseau pour le déploiement qui inclut l'agent ADM :

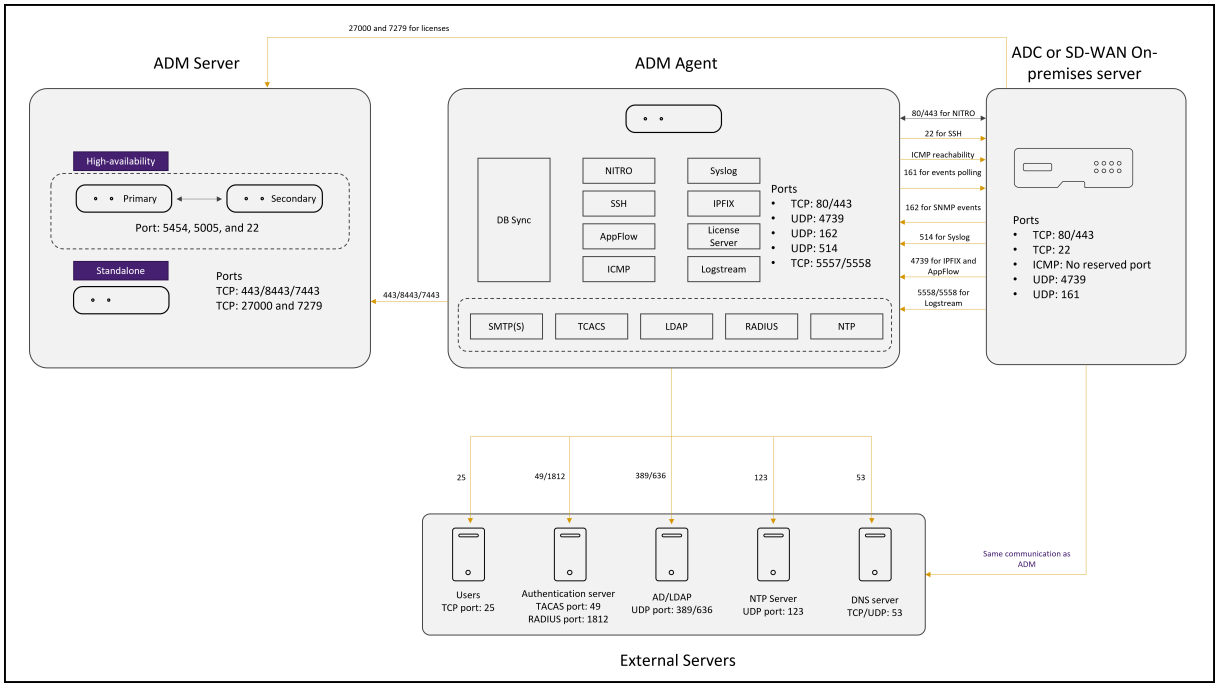


Schéma des ports réseau pour le déploiement NetScaler ADM High Availability :

Si deux serveurs NetScaler ADM sont configurés en mode haute disponibilité , lors de l'ajout d'une instance :

- NetScaler ADM communique avec NetScaler via l'adresse IP principale.
- NetScaler établit la connectivité avec NetScaler ADM via l'adresse IP flottante ADM. Cela implique que NetScaler dirige tout le trafic SNMP, Syslog et Analytics vers l'adresse IP flottante ADM.

Les sections suivantes expliquent les ports requis et leur but :

- Serveur ADM
- Agent ADM
- Instance ADC
- Serveurs externes

Ports pour le serveur ADM

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

Port	Type	Détails	Direction de la communication
80/443/5454/22	TCP	Port par défaut pour la communication et la synchronisation des bases de données entre les nœuds NetScaler ADM en mode haute disponibilité.	Nœud principal NetScaler ADM vers nœud secondaire NetScaler ADM
443/8443/7443	TCP	Port de communication entre l'agent NetScaler ADM et NetScaler ADM.	L'agent NetScaler ADM initie la communication avec NetScaler ADM. NetScaler ADM et l'agent interagissent ensuite l'un avec l'autre.
27000 et 7279	TCP	Ports de licence pour la communication entre le serveur de licences NetScaler ADM et l'instance ADC. Ces ports sont également utilisés pour les licences groupées ADC.	NetScaler vers NetScaler ADM
5005	UDP	Port pour échanger les pulsations entre les nœuds HA.	Nœud principal vers nœud secondaire de NetScaler ADM. Nœud secondaire à nœud principal de NetScaler ADM.

Si les instances NetScaler ADM et NetScaler n'utilisent aucun agent pour communiquer, ouvrez les ports suivants sur le serveur NetScaler ADM :

Port	Type	Détails	Direction de la communication
80/443	TCP	Pour les communications NITRO entre NetScaler ADM et l'instance NetScaler.	Agent NetScaler ADM vers NetScaler et NetScaler vers agent NetScaler ADM
4739	UDP	Pour la communication AppFlow entre l' instance NetScaler et NetScaler ADM.	Agent NetScaler vers NetScaler ADM
162	UDP	Pour recevoir des événements SNMP de l'instance NetScaler vers NetScaler ADM.	Agent NetScaler vers NetScaler ADM
514	UDP	Pour recevoir des messages syslog d'une instance NetScaler à destination de NetScaler ADM.	Agent NetScaler vers NetScaler ADM
5557/5558	TCP	Pour les communications logstream (pour les violations de sécurité WAF, Web Insight et HDX Insight) entre NetScaler et NetScaler ADM.	NetScaler vers NetScaler ADM
5563	TCP	Pour recevoir des métriques ADC (compteurs), des événements système et des messages du journal d'audit de l' instance NetScaler vers NetScaler ADM	NetScaler vers NetScaler ADM

Ports pour l'agent ADM

Le tableau suivant 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 NetScaler ADM et l'instance NetScaler.	Agent NetScaler ADM vers NetScaler et NetScaler vers agent NetScaler ADM
4739	UDP	Pour la communication AppFlow entre l' instance NetScaler et NetScaler ADM.	Agent NetScaler vers NetScaler ADM
162	UDP	Pour recevoir des événements SNMP de l'instance NetScaler vers NetScaler ADM.	Agent NetScaler vers NetScaler ADM
514	UDP	Pour recevoir des messages syslog d'une instance NetScaler à destination de NetScaler ADM.	Agent NetScaler vers NetScaler ADM
5557/5558	TCP	Pour les communications logstream (pour les violations de sécurité WAF, Web Insight et HDX Insight) entre NetScaler et NetScaler ADM.	NetScaler vers NetScaler ADM

Ports pour les instances ADC

Le tableau suivant explique les ports requis qui doivent être ouverts sur les instances NetScaler.

Port	Type	Détails	Direction de la communication
80/443	TCP	Pour les communications NITRO entre NetScaler ADM et l'instance NetScaler. Pour les communications NITRO entre les serveurs NetScaler ADM en mode haute disponibilité.	NetScaler ADM vers NetScaler et NetScaler vers NetScaler ADM
22	TCP	Pour les communications SSH entre NetScaler ADM et l'instance NetScaler. Pour la synchronisation entre les serveurs NetScaler ADM déployés en mode haute disponibilité. Ce port est également requis pour la communication SSH entre l'agent ADM et NetScaler.	NetScaler ADM vers NetScaler. Ou, agent NetScaler ADM pour NetScaler.
Aucun port réservé	ICMP	Pour détecter l'accessibilité du réseau entre les instances NetScaler ADM et NetScaler, ou le serveur NetScaler ADM secondaire déployé en mode haute disponibilité.	NetScaler ADM vers NetScaler

161	UDP	Pour interroger les événements à partir d'instances ADC.	NetScaler ADM vers NetScaler

Ports pour l'agent intégré ADC

Le tableau suivant décrit les ports requis qui doivent être ouverts pour un agent intégré NetScaler.

Port	Type	Détails	Direction de la communication
443	TCP	Pour toutes les communications entre NetScaler ADM et l'agent intégré de NetScaler	NetScaler ADM vers l'agent intégré NetScaler et agent intégré NetScaler vers NetScaler ADM

> **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

Le tableau suivant 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 NetScaler ADM aux utilisateurs.	NetScaler ADM pour les utilisateurs.
389/636	TCP	Port par défaut pour le protocole d'authentification. Pour la communication entre NetScaler ADM et le serveur d'authentification externe LDAP.	Serveur d'authentification externe NetScaler ADM vers LDAP

Port	Type	Détails	Direction de la communication
123	UDP	Port du serveur NTP par défaut pour la synchronisation avec plusieurs sources temporelles.	NetScaler ADM vers serveur NTP
1812	RADIUS	Port par défaut pour le protocole d'authentification. Pour la communication entre NetScaler ADM et le serveur d'authentification externe RADIUS.	Serveur d'authentification externe NetScaler ADM vers RADIUS
49	TACACS	Port par défaut pour le protocole d'authentification. Pour la communication entre NetScaler ADM et le serveur d'authentification externe TACACS.	Serveur d'authentification externe NetScaler ADM vers TACACS

Limitations

À partir de NetScaler 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 NetScaler ADM
2. Accès à la gestion pour NetScaler
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 provenant de NetScaler

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 explique comment commencer à déployer et à configurer NetScaler Application Delivery Management (ADM) pour la première fois. Ce document est destiné aux administrateurs réseau et d'applications qui gèrent les appareils réseau Citrix (NetScaler et NetScaler Gateway). Suivez les étapes décrites dans ce document quel que soit le type d'appareil que vous souhaitez gérer à l'aide de NetScaler ADM.

Si vous utilisez déjà NetScaler ADM, il est recommandé de consulter les notesde mise à jour, laconfiguration système requiseet les détails de licence avant de mettre à niveau votre serveur vers la dernière version de NetScaler ADM.

Étape 1 - Examiner les exigences du système

Avant de commencer à déployer NetScaler ADM dans votre centre de données, passez en revue la configuration logicielle requise, la configuration requise du navigateur, les informations sur les ports, les informations de licence et les limites.

- **Informations sur la licence**. Vous pouvez ajouter un nombre illimité d'instances et d'entités sans licence. Toutefois, vous ne pouvez consulter les informations analytiques que pour deux serveurs virtuels sans demander de licence. Pour consulter les analyses de plus de deux serveurs virtuels, vous devez acheter les 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 de NetScaler 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 NetScaler ADM puisse communiquer avec les instances de NetScaler. En savoir plus.
- Exigences relatives aux**instances NetScaler**. Les différentes fonctionnalités de NetScaler ADM sont prises en charge sur différentes versions du logiciel NetScaler. Consultez ces informations pour vous assurer que vous avez mis à niveau vos instances NetScaler vers la bonne version. En savoir plus.

Étape 2 - Déploiement de NetScaler ADM

Pour gérer et surveiller les applications et l'infrastructure réseau, vous devez d'abord installer NetScaler ADM sur l'un des hyperviseurs. Vous pouvez déployer NetScaler ADM en tant que serveur unique ou en mode haute disponibilité. Si vous utilisez NetScaler Insight Center, vous pouvez migrer vers NetScaler 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 le cadre d'un déploiement sur un seul serveur NetScaler ADM, la base de données est intégrée au serveur et un serveur unique traite l'ensemble du trafic. Vous pouvez déployer NetScaler ADM avec Citrix Hypervisor, VMware ESXi, Microsoft Hyper-V et Linux KVM. Voir :
  - NetScaler ADM avec Citrix Hypervisor
  - NetScaler ADM avec Microsoft Hyper-V
  - NetScaler ADM avec VMware ESXi
  - NetScaler ADM avec serveur KVM Linux
- **Déploiement haute disponibilité.** Un déploiement à haute disponibilité (HA) de deux serveurs NetScaler ADM garantit des opérations ininterrompues. Dans une configuration à haute disponibilité, les deux nœuds NetScaler ADM doivent être déployés en mode actif-passif, sur le même sous-réseau à l'aide de la même version logicielle et de la même construction, et doivent avoir les mêmes configurations. Avec le déploiement HA, la possibilité de configurer l'adresse IP flottante sur le nœud principal de NetScaler ADM élimine le besoin d'un équilibreur de charge NetScaler distinct. Pour en savoir plus, consultez la section Configurer dans un déploiement haute disponibilité.

Étape 3 - Ajouter des instances à NetScaler ADM

Dans NetScaler ADM, vous pouvez découvrir, gérer et surveiller toutes les instances NetScaler déployées sur site ou dans le cloud. Vous devez ajouter des instances au serveur NetScaler ADM si vous souhaitez gérer et surveiller ces instances. Vous pouvez ajouter les instances suivantes à NetScaler ADM :

- NetScaler
  - NetScaler MPX
  - NetScaler VPX
  - NetScaler SDX
  - NetScaler CPX
  - NetScaler BLX
  - NetScaler Gateway

Lorsque vous ajoutez une instance au serveur NetScaler 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 - Configuration du serveur NTP sur NetScaler ADM

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

En savoir plus

Étape 6 - Configuration des paramètres système pour des performances optimales de NetScaler ADM

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

optimales de votre serveur NetScaler 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 NetScaler ADM, et vous pouvez configurer des serveurs de passerelles de messagerie et de messagerie courte (SMS) pour envoyer des notifications par e-mail et par SMS 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 reporting stockées dans la base de données de votre serveur NetScaler ADM, vous pouvez spécifier l'intervalle pendant lequel vous souhaitez que NetScaler 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).
- **Configurez les paramètres de sauvegarde du système**. NetScaler ADM sauvegarde automatiquement le système tous les jours à 00h30. 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 NetScaler, vous pouvez utiliser les fichiers de sauvegarde pour rétablir 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'événements stockées dans la base de données de votre serveur NetScaler ADM, vous pouvez spécifier l'intervalle pendant lequel vous souhaitez que NetScaler ADM conserve les données de reporting réseau, les événements, les journaux d'audit et les journaux de 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 lesquels les données syslog suivantes seront supprimées de NetScaler ADM :
  - Données Syslog génériques
  - Données AppFirewall
  - Données NetScaler Gateway.

    En savoir plus

Prochaine étape

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

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

Déployer

February 1, 2024

Avant d'utiliser NetScaler 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 NetScaler 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 NetScaler 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 NetScaler ADM avec Citrix Hypervisor, VMware ESXi, Microsoft Hyper-V et Linux KVM. Voir :
  - NetScaler ADM sur Citrix Hypervisor
  - NetScaler ADM sur Microsoft Hyper-V
  - NetScaler ADM sur VMware ESXi
  - NetScaler ADM sur un serveur KVM Linux
  - NetScaler ADM sur un cluster Kubernetes
- Déploiement**haute disponibilité (HA) : un déploiement**en haute disponibilité de deux serveurs NetScaler ADM garantit des opérations ininterrompues. Dans une configuration HA, les deux nœuds NetScaler ADM doivent être déployés en mode actif-passif, sur le même sous-réseau à l'aide de la même version logicielle et de la même version, et doivent avoir les mêmes configurations. Avec le déploiement HA, la possibilité de configurer l'adresse IP flottante sur le nœud principal de NetScaler ADM élimine le besoin d'un équilibreur de charge NetScaler 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 NetScaler ADM** : Vous pouvez migrer votre déploiement de NetScaler Insight Center vers NetScaler ADM sans perdre la configuration, les paramètres ou les données existants. Avec NetScaler ADM, vous pouvez non seulement consulter les différentes analyses générées par NetScaler, mais également gérer, surveiller et dépanner l'ensemble de l'infrastructure mondiale de diffusion d'applications à partir d'une console unique et unifiée. Voir :Migration de NetScaler Insight Center vers NetScaler ADM
- **Intégrez NetScaler ADM à Director : Director**s'intègre à NetScaler ADM pour l'analyse du réseau et la gestion des performances. Voir : Intégrer NetScaler ADMà Director

Conditions préalables à l'installation de NetScaler ADM

February 1, 2024

Vous pouvez télécharger et installer NetScaler Application Delivery Management (ADM) pour les plateformes 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 limites de toutes ces plateformes.

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

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

Exigences générales pour NetScaler ADM

Composant	Exigences
RAM	32 GB

Composant	Exigences
CPU virtuel	8 processeurs
Espace de stockage	Citrix recommande d'utiliser la technologie Solid State Drive (SSD) pour les déploiements NetScaler ADM. L'espace de stockage par défaut requis est de 120 Go. Les besoins de stockage réels dépendent de l'estimation de la taille de NetScaler ADM. Utilisez le calculateur de dimensionnement mentionné dans la section **Limites maximales** (page 7) du Guide de déploiement de NetScaler 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 vos besoins de stockage NetScaler ADM dépassent 120 Go, vous devez connecter 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 NetScaler ADM.
Interfaces réseau virtuelles	1
Débit	1 Gbit/s

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

NetScaler ADM sur Citrix Hypervisor

February 1, 2024

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

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

Conditions préalables

Avant d'installer NetScaler ADM, vérifiez que les conditions suivantes sont remplies :

- 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 NetScaler ADM sur Citrix Hypervisor.
- Vous avez téléchargé le fichier image NetScaler ADM .XVA.

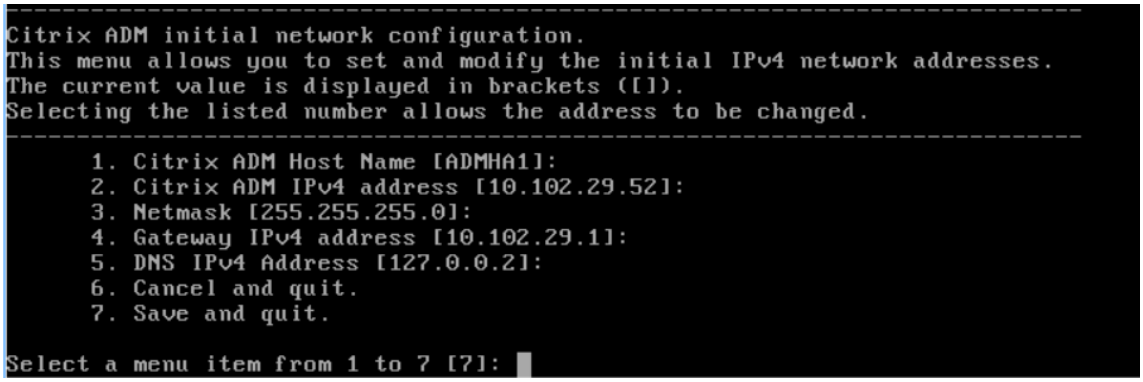
Configuration système requise pour XenCenter

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.

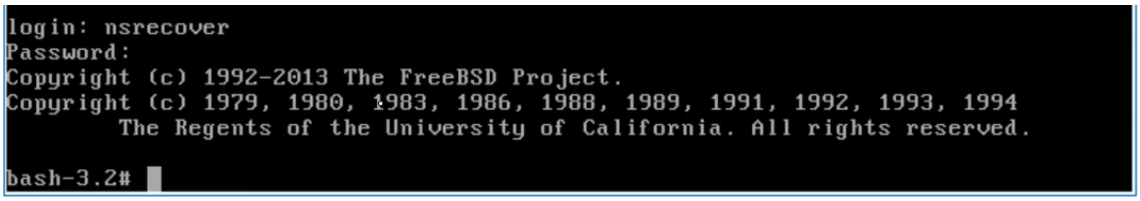
Composant	Exigences
Système d'exploitation	Windows 7, Windows Server 2003 ou Windows 10
.NET framework	Version 2.0 ou ultérieure
UC	750 MHz (MHz), recommandé : 1 gigahertz (GHz) ou plus rapide
RAM	1 Go, Recommandé : 2 Go
Carte d'interface réseau	Carte réseau 100 mégabits par seconde (Mbps) ou plus rapide

Installation de NetScaler 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.

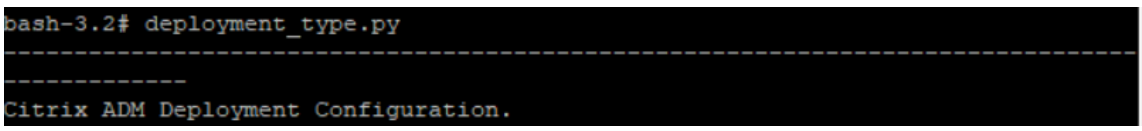


2. Après avoir spécifié les adresses IP requises, enregistrez les paramètres de configuration.
3. Lorsque vous y êtes invité, ouvrez une session à l'aide des informations d'identification nsrecover/nsroot.

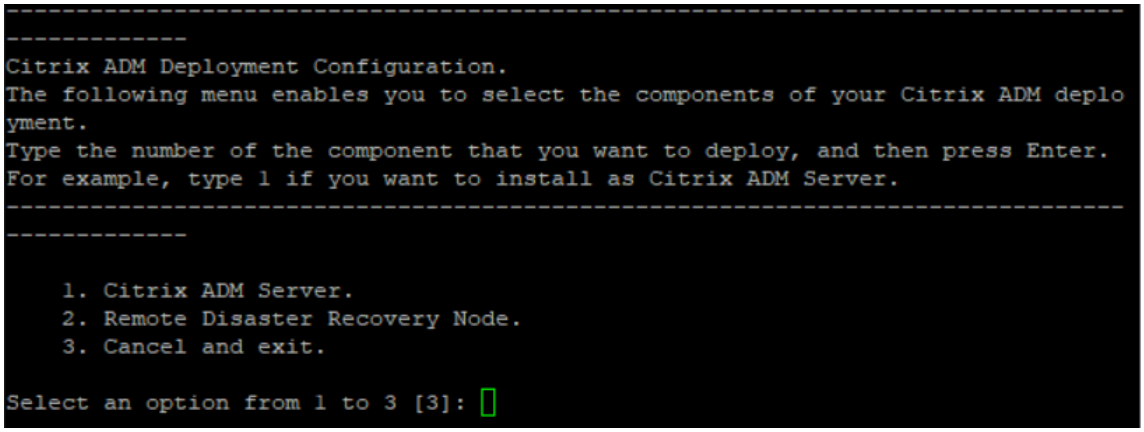


> **Remarque**
>
> Une fois que vous ouvrez une session, si vous souhaitez mettre à jour la configuration réseau initiale, tapez `networkconfig`, mettez à jour la configuration et enregistrez la configuration.

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 **NetScaler ADM Server.** Si vous ne sélectionnez aucune option, par défaut, elle est déployée en tant que serveur.



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

> **Remarque**
>
> Après avoir installé NetScaler 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 saisissant l'adresse IP du serveur NetScaler 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 NetScaler ADM.

NetScaler ADM sur Microsoft Hyper-V

February 1, 2024

Pour installer NetScaler ADM sur Microsoft Hyper-V, vous devez d'abord télécharger le fichier image NetScaler 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 NetScaler ADM, vérifiez que les conditions suivantes sont 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 NetScaler ADM.

Configuration système requise pour Microsoft Hyper-V

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

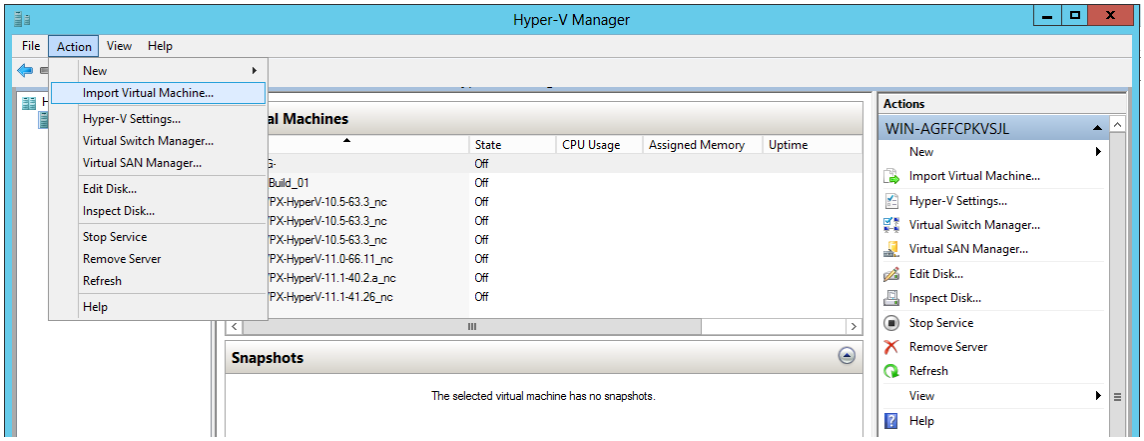
Composant	Exigences
Système d'exploitation	Windows Server 2012 R2
.NET framework	Version 2.0 ou ultérieure
UC	750 MHz (MHz), recommandé : 1 gigahertz (GHz) ou plus rapide
RAM	1 Go, Recommandé : 2 Go
Carte d'interface réseau	Carte réseau 100 mégabits par seconde (Mbps) ou plus rapide

Installation de NetScaler Application Delivery Management

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

Pour installer NetScaler 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 :

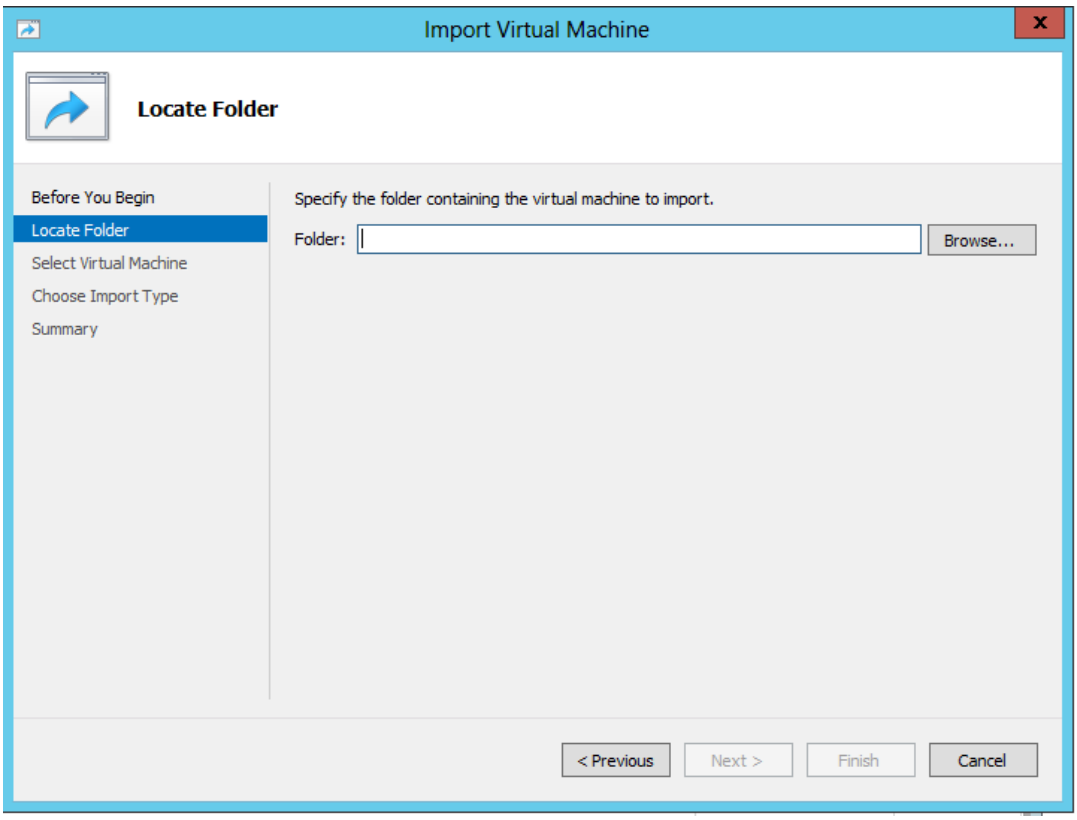
   a) Dans la boîte de dialogue Importer une machine virtuelle, dans la section **Localiser le dossier**, accédez au dossier dans lequel vous avez enregistré l'image NetScaler ADM Hyper-V, sélectionnez le dossier et cliquez sur **Suivant**.

   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.

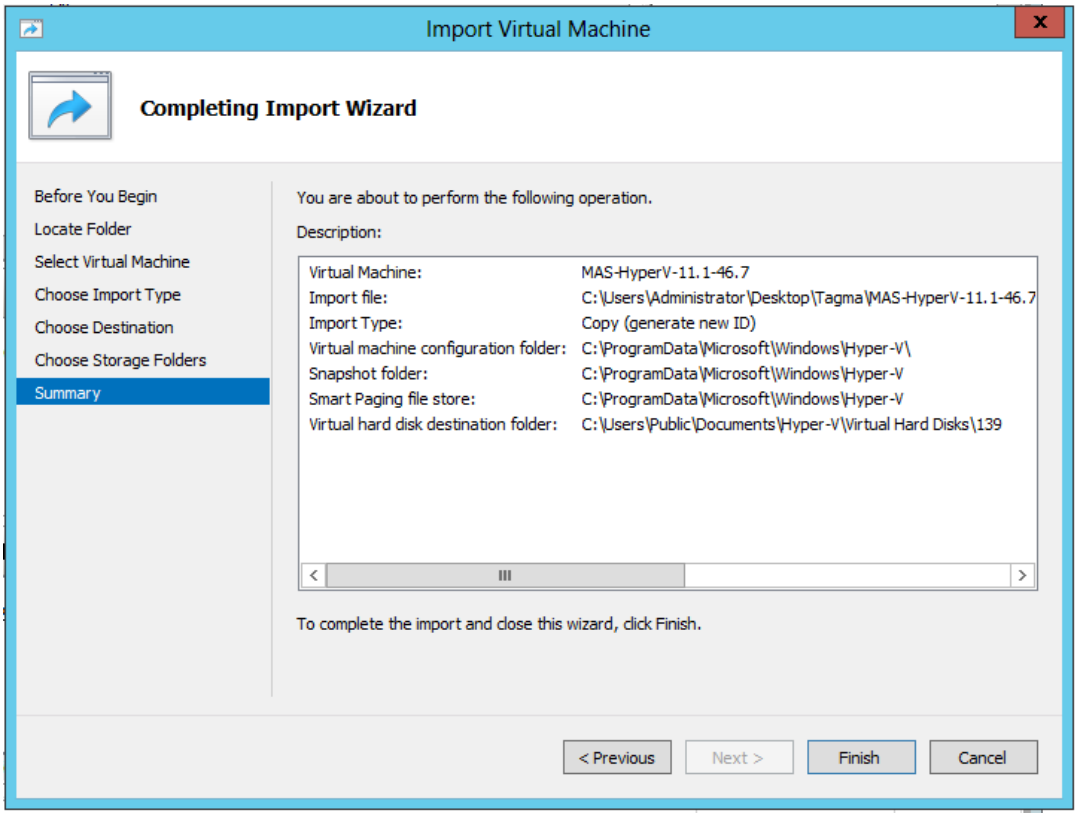
   d) Dans la section **Choisir une destination**, vous pouvez spécifier les dossiers dans lesquels stocker les fichiers de la machine virtuelle.

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



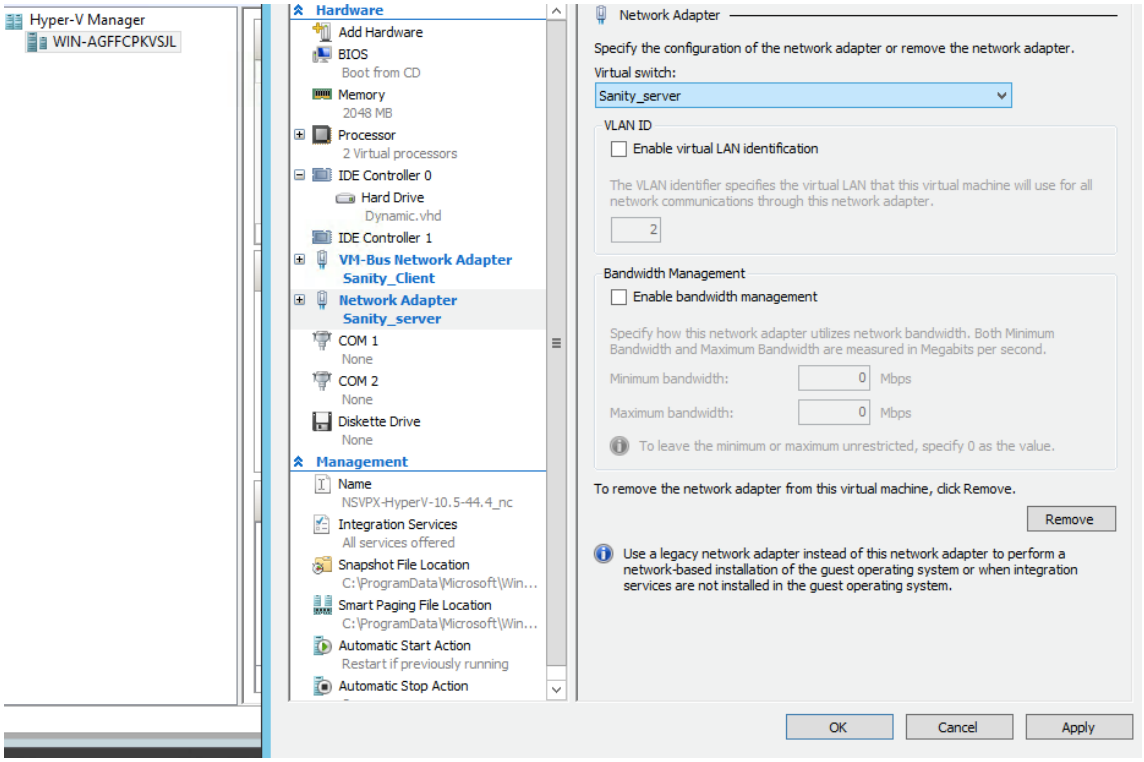
e) Dans la section **Choisir les dossiers de stockage**, vous pouvez sélectionner l'emplacement dans lequel vous souhaitez stocker les disques durs virtuels, puis cliquer sur **Suivant**.

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

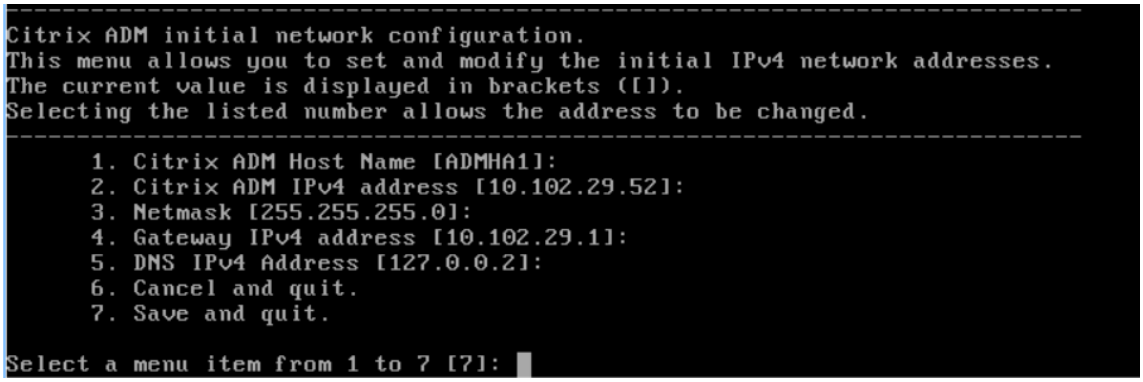


L'image de NetScaler ADM Hyper-V s'affiche dans le volet droit.

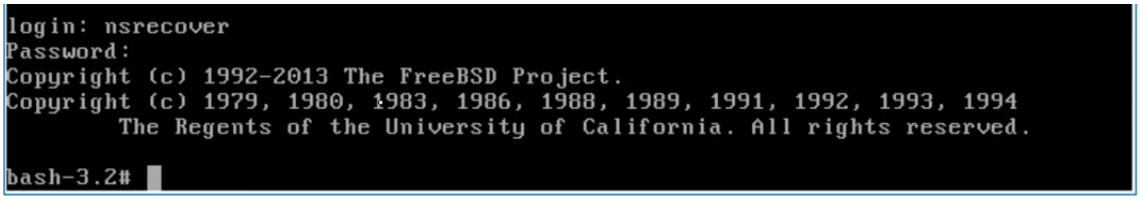
4. **Cliquez avec le bouton droit sur l'image NetScaler ADM Hyper-V, puis cliquez sur Paramètres.**
5. Dans le volet gauche de la boîte de dialogue qui s'affiche, accédez à **Matériel** > **VM_Bus Network Adaptor**et, dans le volet droit, sélectionnez le réseau approprié dans la liste Réseau.



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



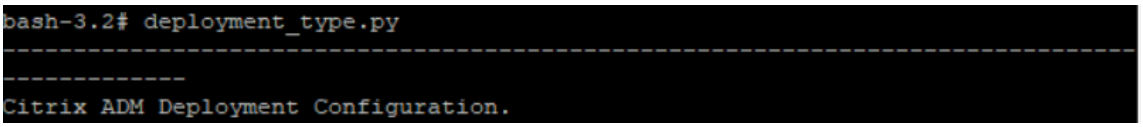
10. Après avoir spécifié les adresses IP requises, enregistrez les paramètres de configuration.
11. Lorsque vous y êtes invité, ouvrez une session à l'aide des informations d'identification nsrecover/nsroot.



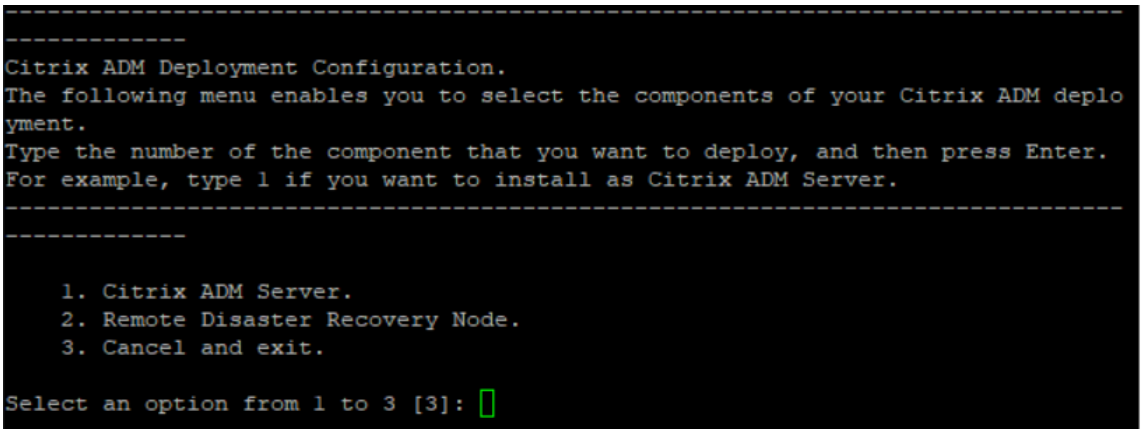
> **Remarque**
>
> Une fois que vous ouvrez une session, si vous souhaitez mettre à jour la configuration réseau initiale, tapez `networkconfig`, mettez à jour la configuration et enregistrez la configuration.

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 **NetScaler ADM Server.** Si vous ne sélectionnez aucune option, par défaut, elle est déployée en tant que serveur.



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

> **Remarque**
>
> Après avoir installé NetScaler 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 saisissant l'adresse IP du serveur NetScaler 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 NetScaler ADM.

NetScaler ADM sur VMware ESXi

February 1, 2024

Ce document explique comment installer les dispositifs virtuels NetScaler ADM sur VMware ESXi à l'aide du 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 de configuration de NetScaler ADM.

> Remarque
>
> - VMotion est uniquement pris en charge à partir de **NetScaler 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.
> - Les outils VMware pour NetScaler ADM sont fournis dans le cadre de la version logicielle et ne peuvent pas être mis à niveau ou modifiés séparément.

Pour installer NetScaler ADM

Suivez ces étapes pour installer un dispositif virtuel ADM sur VMware ESXi.

> **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. **La version 7.0.1c de VMware ESXi, version 17325551, avec adaptateur VMXNET3, est prise en charge dans NetScaler ADM 13.0 71.40 ou version ultérieure.** Reportez-vous à la documentation VMware pour connaître les étapes spécifiques à la version.

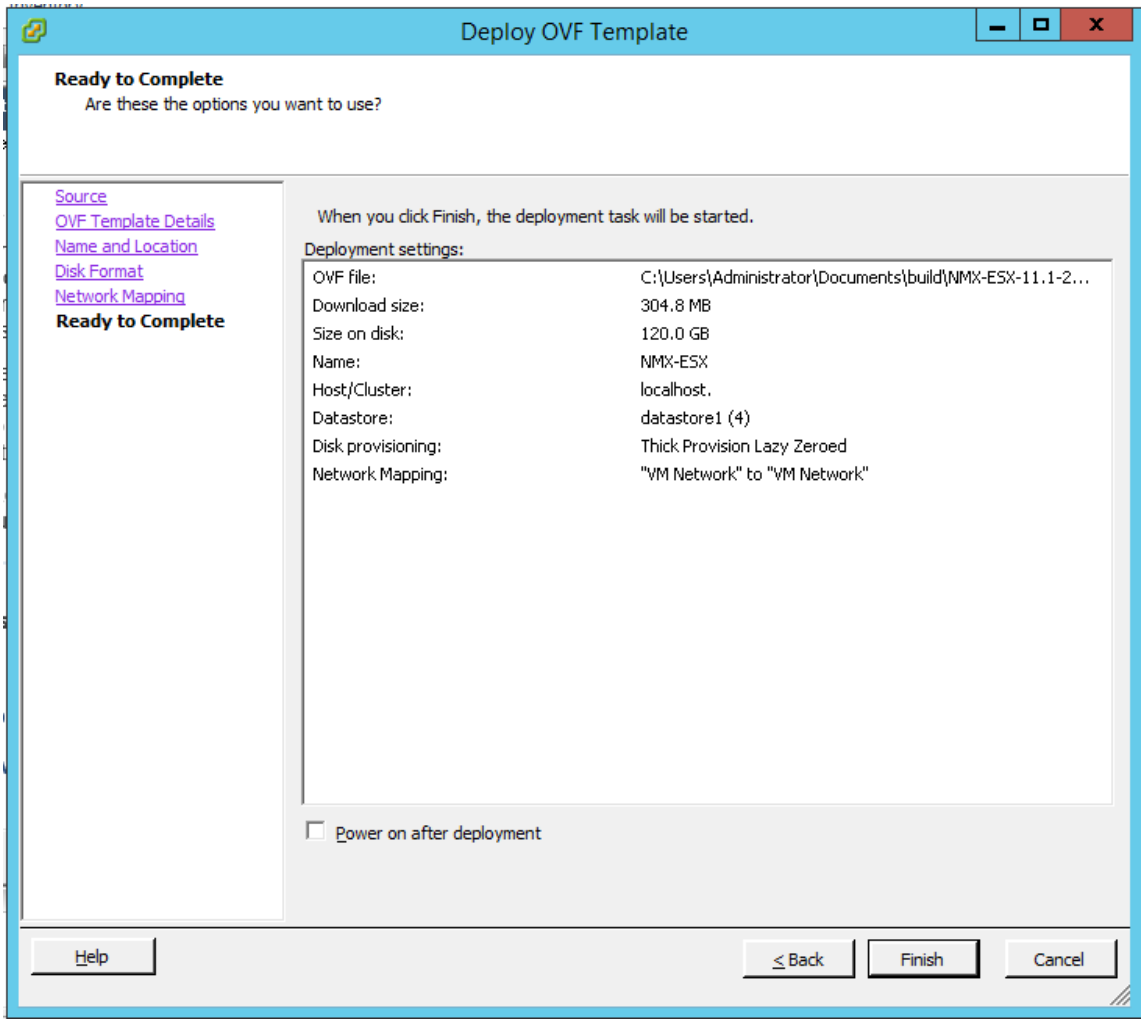
1. Démarrez le client VMware vSphere sur votre station de travail.
2. Dans la zone de texte **Adresse IP/Nom**, tapez l'adresse IP du serveur VMware ESXi auquel vous souhaitez vous connecter.
3. Dans les zones de texte **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification 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'identifiant 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**.

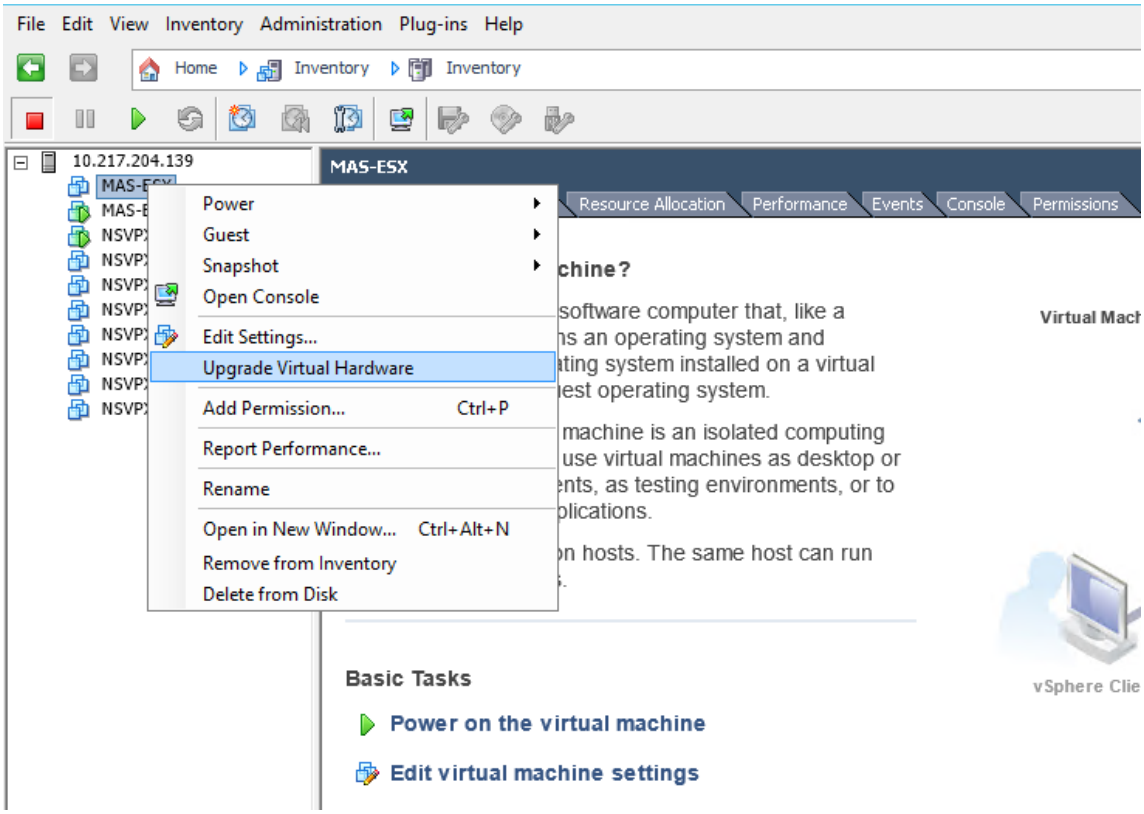
6. Sur la page **Détails du modèle OVF**, cliquez sur **Suivant**.
7. **Tapez le nom de l'appliance virtuelle NetScaler ADM, puis cliquez sur Suivant.**
8. Spécifiez le format de disque en sélectionnant le format provisionné fin ou le format provisionné épais.

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

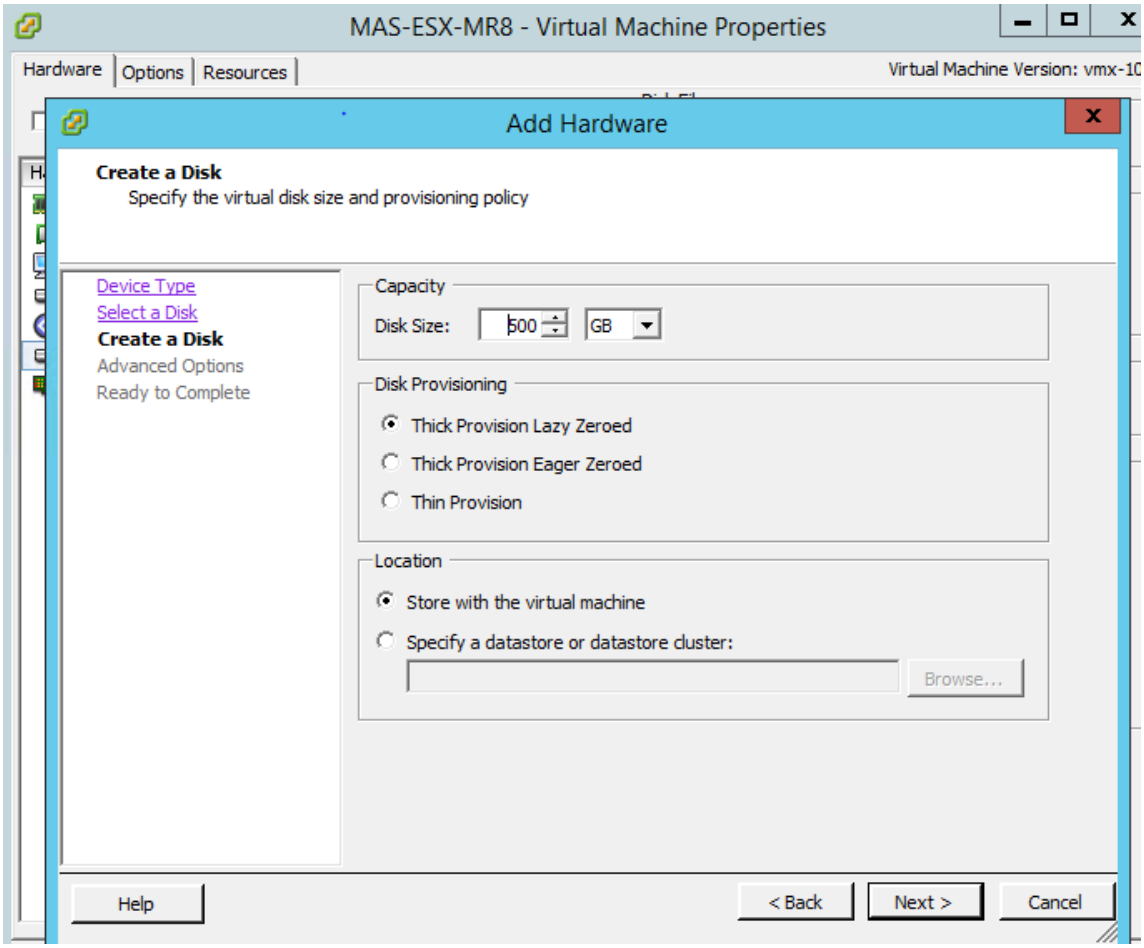
9. Cliquez sur **Terminer** pour démarrer le processus d'installation.



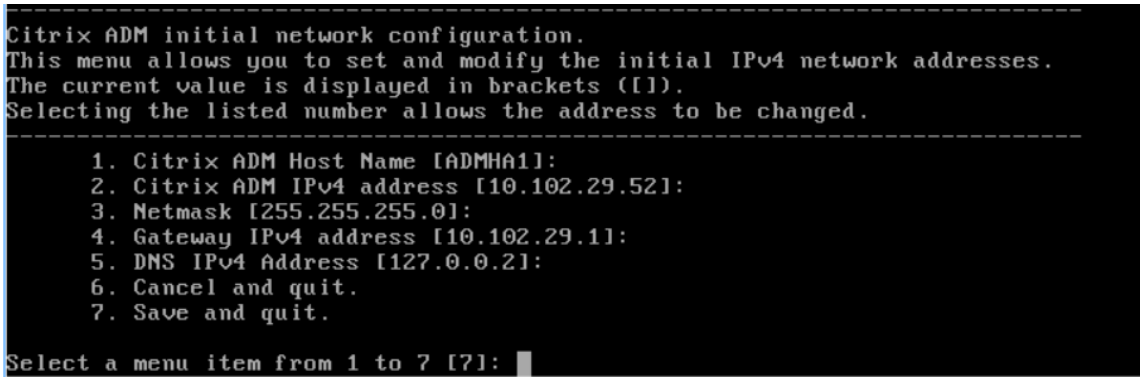
10. Vous êtes maintenant prêt à démarrer l'appliance virtuelle NetScaler ADM.
11. Dans le volet de navigation, sélectionnez l'appliance virtuelle que vous avez installée. Dans le menu **Inventaire**, cliquez avec le bouton droit sur la **machine virtuelle**, puis cliquez sur **Mettre à niveau le matériel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



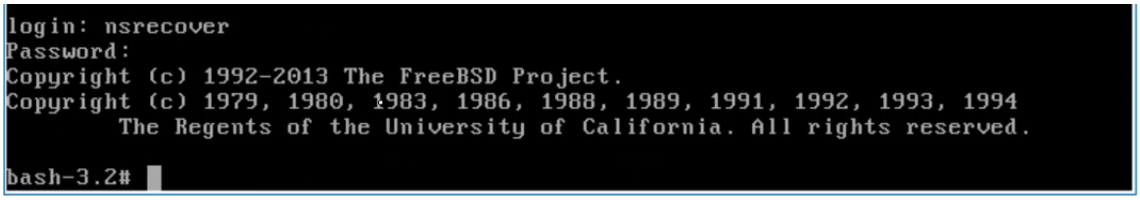
12. Dans le menu **Inventaire**, cliquez sur **Machine virtuelle**, puis sur **Modifier les paramètres**.
13. Dans la boîte de dialogue **Propriétés de la machine virtuelle**, sous l'onglet **Matériel**, cliquez sur **Mémoire**, puis dans le volet droit, spécifiez la **taille de la mémoire** sur 32 Go.
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 NetScaler ADM.



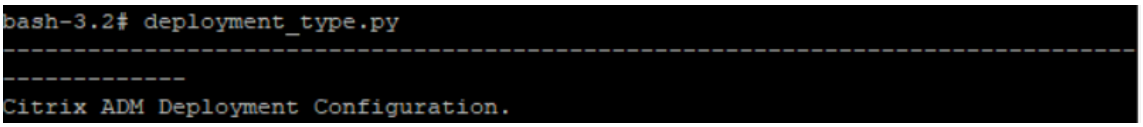
18. Après avoir spécifié les adresses IP requises, enregistrez les paramètres de configuration.
19. Lorsque vous y êtes invité, ouvrez une session à l'aide des informations d'identification nsrecover/nsroot.



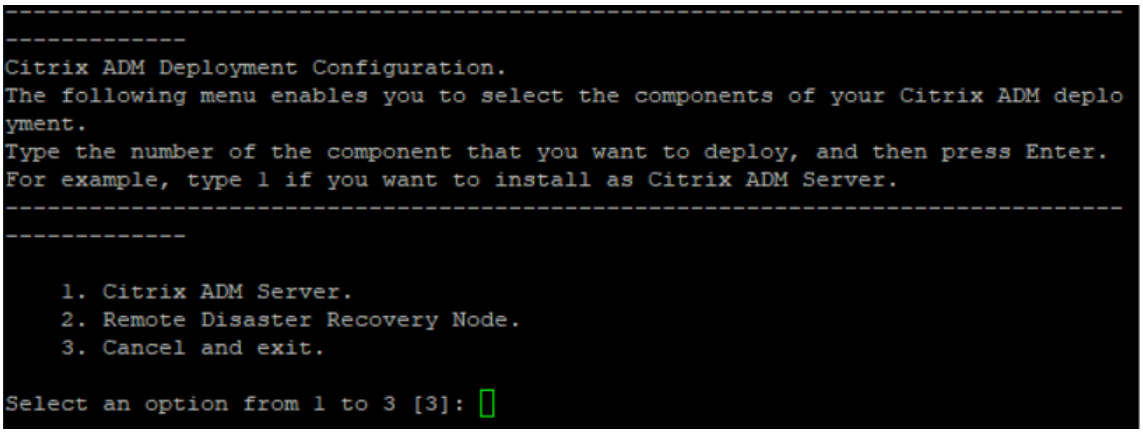
> **Remarque**
>
> Une fois que vous ouvrez une session, si vous souhaitez mettre à jour la configuration réseau initiale, tapez `networkconfig`, mettez à jour la configuration et enregistrez la configuration.

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 **NetScaler ADM Server.** Si vous ne sélectionnez aucune option, par défaut, elle est déployée en tant que serveur.



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

> **Remarque**
>
> Après avoir installé NetScaler 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 saisissant l'adresse IP du serveur NetScaler 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 NetScaler ADM.

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

Automatisez le déploiement de l'agent NetScaler ADM sur VMware ESXi

February 1, 2024

NetScaler ADM vous permet d'automatiser le déploiement des agents NetScaler ADM sur VMware ESXi.

En tant qu'administrateur, vous pouvez automatiser les actions suivantes :

- Configuration de l'agent NetScaler ADM
- Enregistrez l'agent NetScaler ADM et modifiez le mot de passe par défaut de l'agent.

Configuration de l'agent NetScaler ADM

Pour automatiser la configuration de l'agent, ajoutez les valeurs des paramètres suivants dans le fichier .ovf :

1. Adresse IP
2. Masque réseau
3. Gateway
4. Serveur de noms
5. Nom d'hôte

> **Remarque**
>
> Le fichier .ovf est disponible dans le fichier image de l'agent. Pour télécharger le fichier de l'agent NetScaler ADM, accédez à https://www.citrix.com/downloads/citrix-application-manage

> ment/. Le modèle de dénomination du fichier image de l'agent est le suivant : **MASAGENT-ESX-releasenumber-buildnumber.zip**

Enregistrez l'agent NetScaler ADM et modifiez le mot de passe par défaut

> **Remarque**
>
> Avant d'enregistrer et de modifier le mot de passe par défaut, assurez-vous d'avoir ajouté les paramètres spécifiés dans Configurer l'agent NetScaler ADM.

Pour automatiser l'enregistrement de l'agent NetScaler ADM et la modification du mot de passe par défaut, ajoutez les valeurs des paramètres suivants dans le même fichier .ovf :

1. IP du serveur ADM
2. Nom d'utilisateur ADM
3. Mot de passe ADM
4. Nouveau mot de passe de l'agent

Conditions préalables

Avant de commencer à installer un dispositif virtuel, assurez-vous de :

- Installez VMware vSphere 8.x sur une station de travail de gestion répondant à la configuration système minimale requise.
- Téléchargez les fichiers de configuration de NetScaler ADM.

Comment configurer et enregistrer un agent NetScaler ADM

1. Téléchargez et modifiez le fichier .OVF
2. Installation de l'appliance virtuelle NetScaler ADM sur VMware ESXi
3. Vérifier

Téléchargez et modifiez le fichier .OVF

1. Extrayez les fichiers du fichier MASAGENT-ESX-releasenumber-buildnumber.zip à l'emplacement souhaité. Les fichiers suivants sont disponibles :
    - fichier .ovf
    - fichier .vmdk
    - fichier .ova
    - fichier .mf

2. Ouvrez le fichier .ovf dans n'importe quel éditeur et ajoutez l'exemple de code suivant <ProductSection>..</ProductSection> après la balise </VirtualHardwareSection>

```
<ProductSection>
    <Info>Information about the installed software</Info>
    <Product>Application Delivery management</Product>
    <Vendor>Citrix</Vendor>

    <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
       string"
    ovf:key="eth0.ip">
    <Label>IPAddress</Label>
    </Property>

    <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
       string"
    ovf:key="eth0.netmask">
    <Label>Netmask</Label>
    </Property>

    <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
       string"
    ovf:key="eth0.gateway">
    <Label>Gateway</Label>
    </Property>

    <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
       string"
    ovf:key="eth0.nameserver">
    <Label>Nameserver</Label>
    </Property>

    <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
       string"
    ovf:key="eth0.hostname">
    <Label>Hostname</Label>
    </Property>

    <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
       string"
    ovf:key="eth0.ServerIP">
    <Label>ADM Server IP</Label>
    </Property>

    <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
       string"
    ovf:key="eth0.ServerUname">
    <Label>ADM Username</Label>
    </Property>

    <Property ovf:userConfigurable="true" ovf:password="true" ovf:value
       ="VALUE"
```

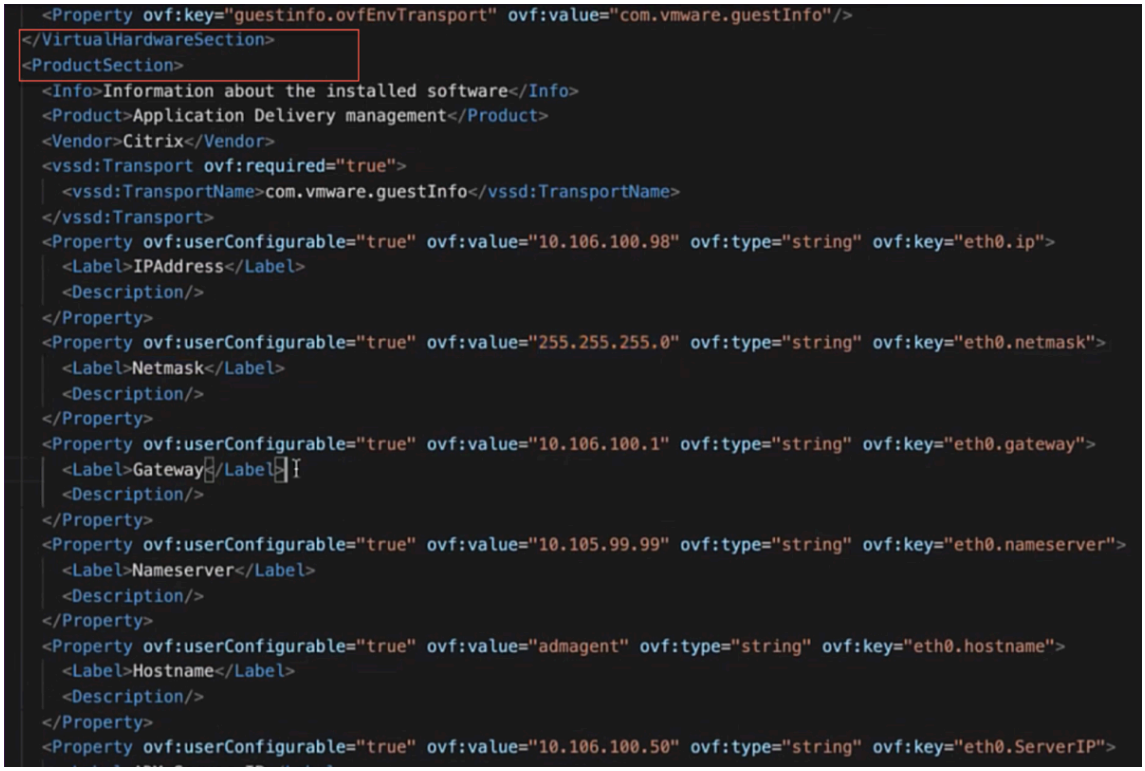


```
42      ovf:type="string" ovf:key="eth0.ServerPassword">
43      <Label>ADM Password</Label>
44      </Property>
45
46      <Property ovf:userConfigurable="true" ovf:password="true" ovf:value
           ="VALUE"
47      ovf:type="string" ovf:key="eth0.NewPassword">
48      <Label>Agent New Password</Label>
49      </Property>
50
51  </ProductSection>
52  <!--NeedCopy-->
```

1. Pour les paramètres que vous souhaitez configurer, ajoutez leurs valeurs correspondantes dans OVF:value=”value”

   - Pour configurer l’agent NetScaler ADM, ajoutez les valeurs aux paramètres suivants :
     - Adresse IP
     - Masque réseau
     - Gateway
     - Serveur de noms
     - Nom d’hôte
   - Pour enregistrer et modifier le mot de passe par défaut de l’agent NetScaler ADM, ajoutez les valeurs aux paramètres suivants :
     - IP du serveur ADM
     - Nom d’utilisateur ADM
     - Mot de passe ADM
     - Nouveau mot de passe de l’agent

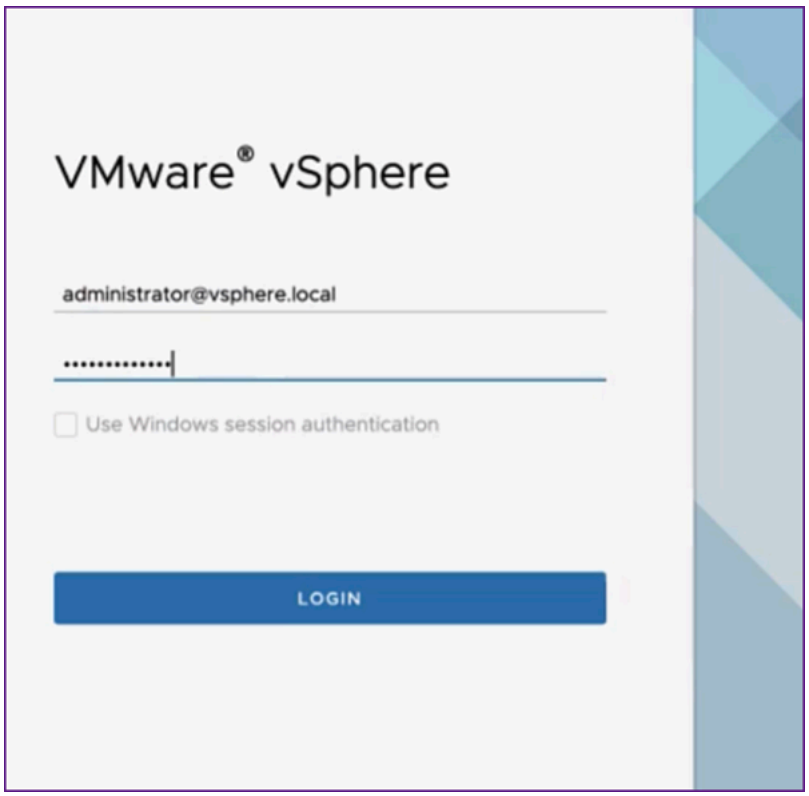
   > **Remarque**
   >
   > - Vous devez configurer l’agent NetScaler ADM avant de l’enregistrer et de modifier le mot de passe par défaut de l’agent.
   > - Si vous ne vous enregistrez pas et ne modifiez pas le mot de passe par défaut dans le fichier .ovf, vous devez effectuer ces actions manuellement après le déploiement de la machine virtuelle.



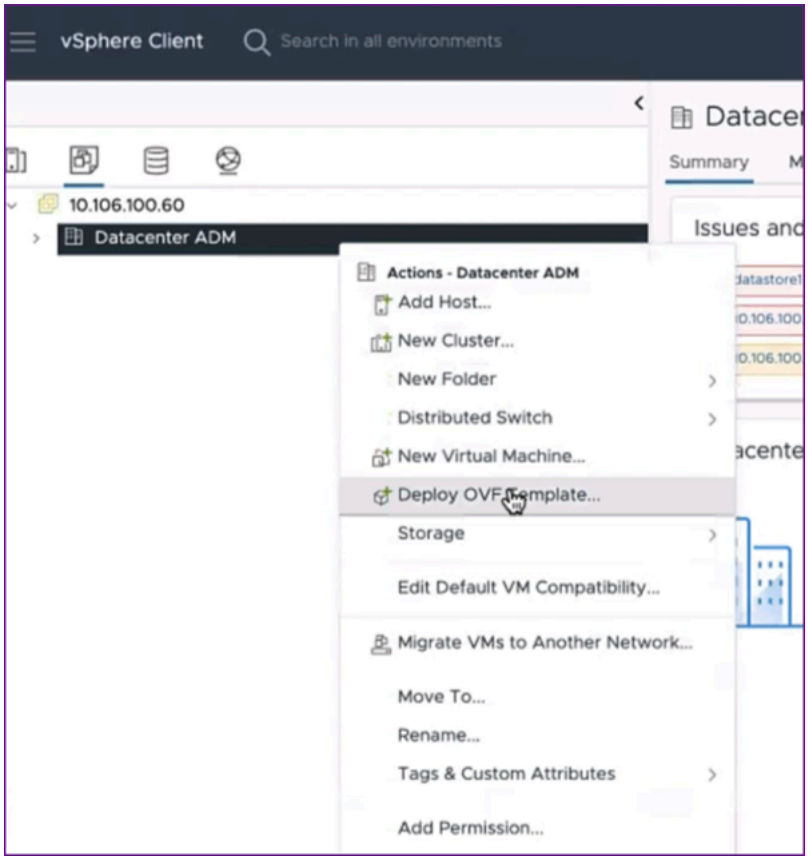
2. Après avoir ajouté les paramètres et leurs valeurs, enregistrez le fichier .ovf.

Installation de l'appliance virtuelle NetScaler ADM sur VMware ESXi

1. Connectez-vous au **client VMware vSphere** et saisissez les informations d'identification de l'administrateur. Cliquez sur **Connexion**.

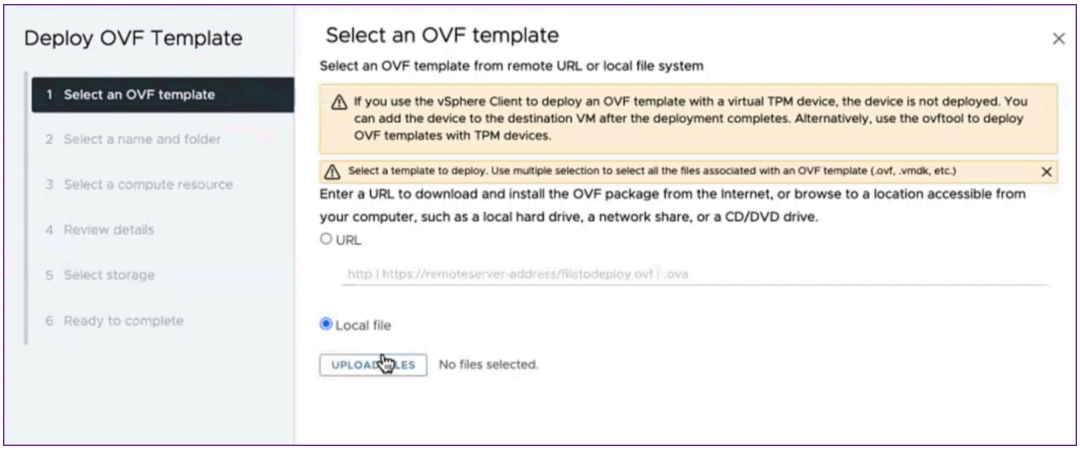


2. Sélectionnez votre serveur ESXi, puis cliquez avec le bouton droit pour sélectionner **Déployer le modèle OVF**.

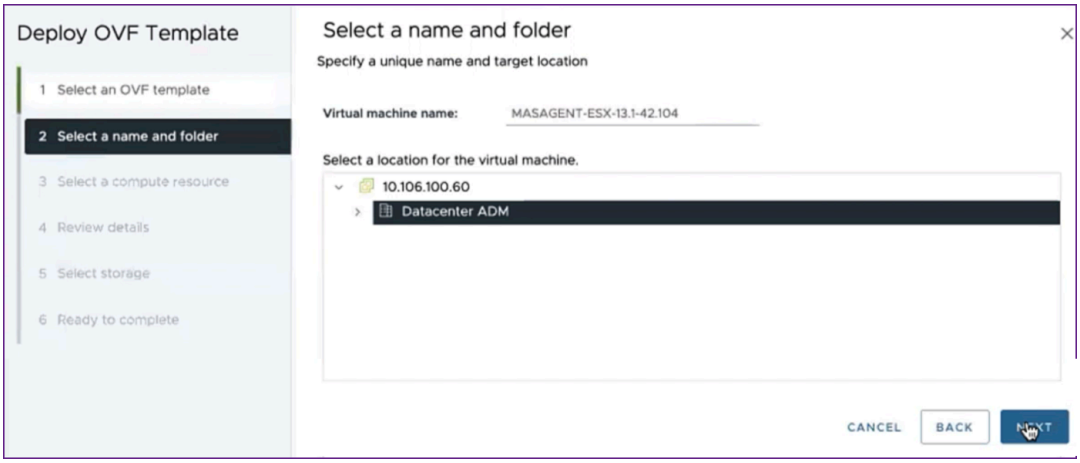


3. Sur la page **Déployer le modèle OVF** :

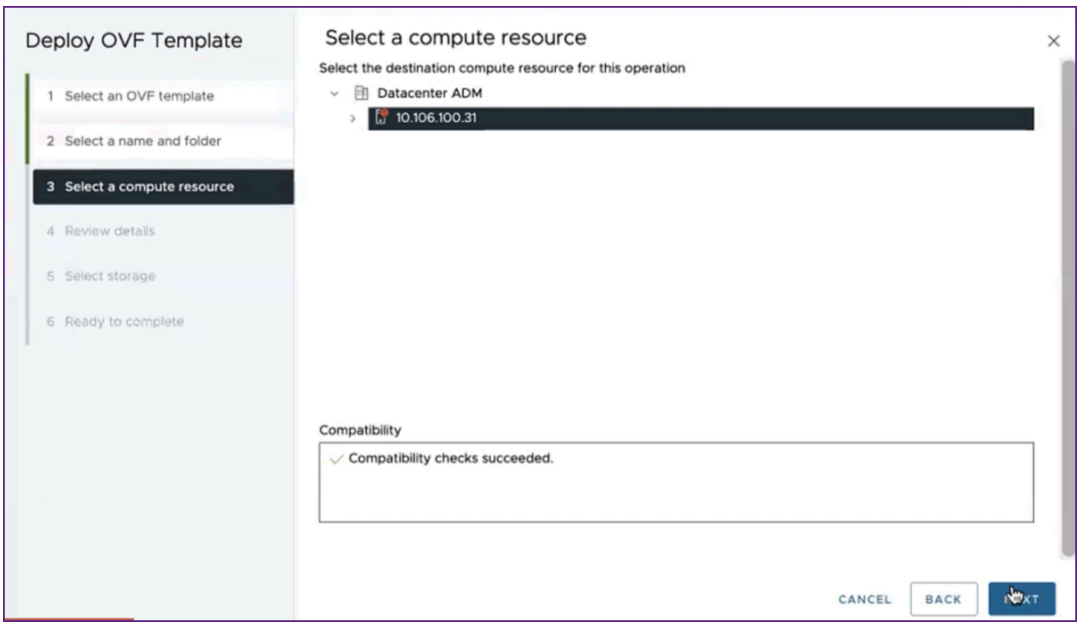
   a) **Sélectionnez un modèle OVF** : sélectionnez **Fichier local** et accédez à l'emplacement où vous avez enregistré le fichier .ovf modifié et le fichier .vmdk. Sélectionnez les fichiers et cliquez sur **Ouvrir** pour les charger. Cliquez sur **Suivant**.



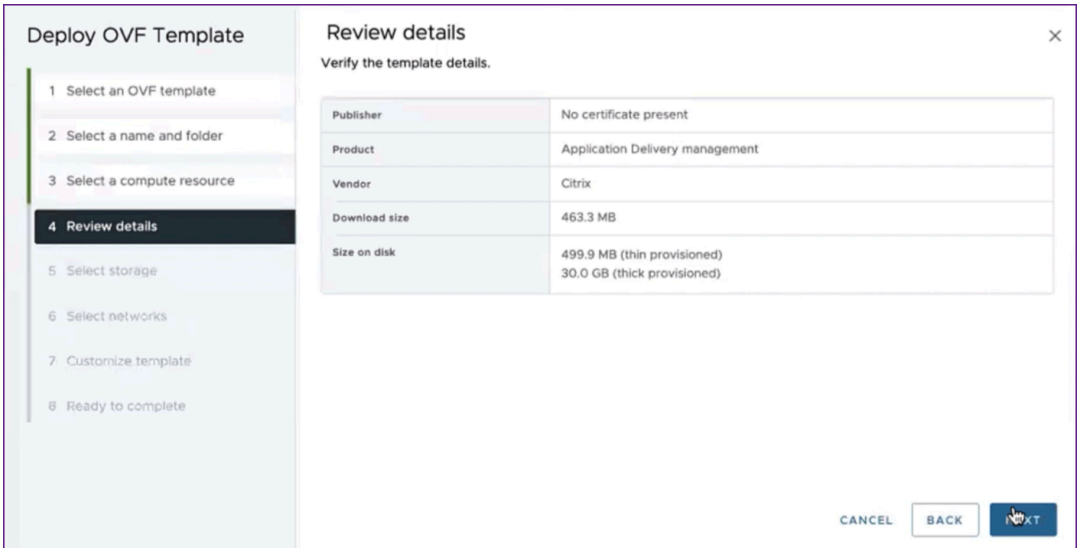
   b) **Sélectionnez un nom et un dossier** : ajoutez un nom pour le dispositif virtuel et sélectionnez l'emplacement sur l'ESXi où vous souhaitez déployer la machine virtuelle. Cliquez sur **Suivant**.



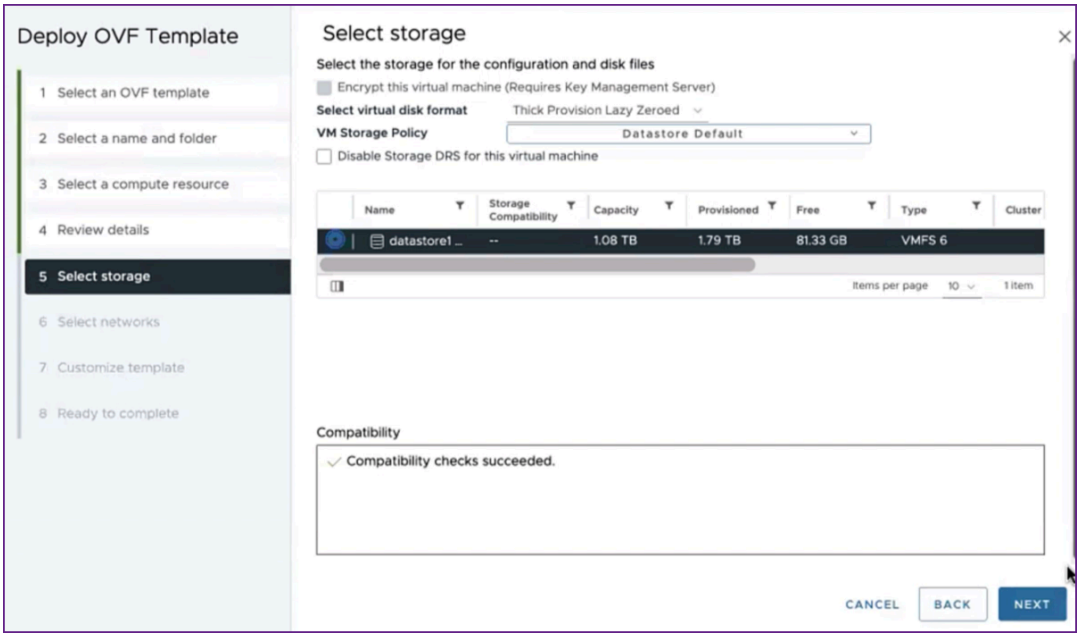
c) **Sélectionnez une ressource de calcul** : sélectionnez une ressource sur laquelle exécuter le modèle après son déploiement. Cliquez sur **Suivant**.



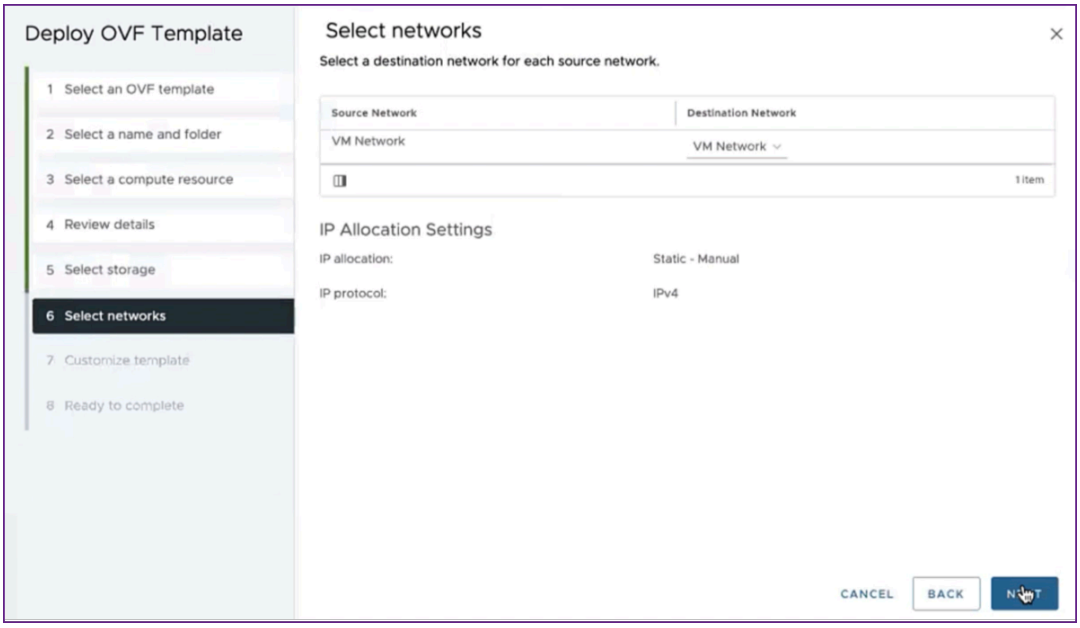
d) **Vérifiez les détails** : vérifiez les détails du modèle OVF. Cliquez sur **Suivant**.



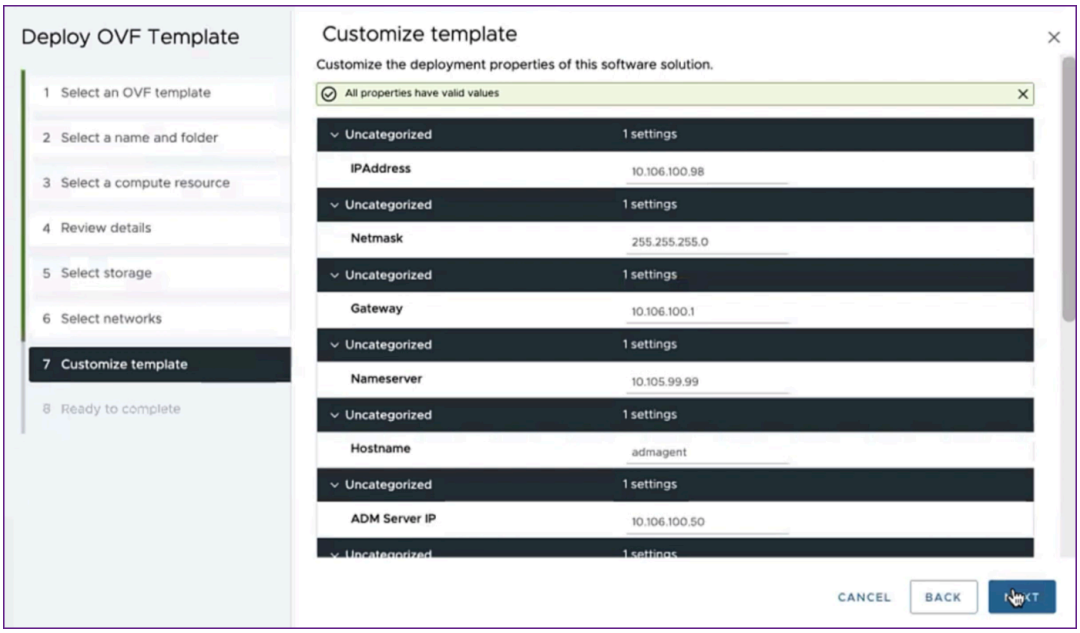
e) **Sélectionnez le stockage** : sélectionnez une banque de données pour stocker le modèle OVF. Cliquez sur **Suivant**.



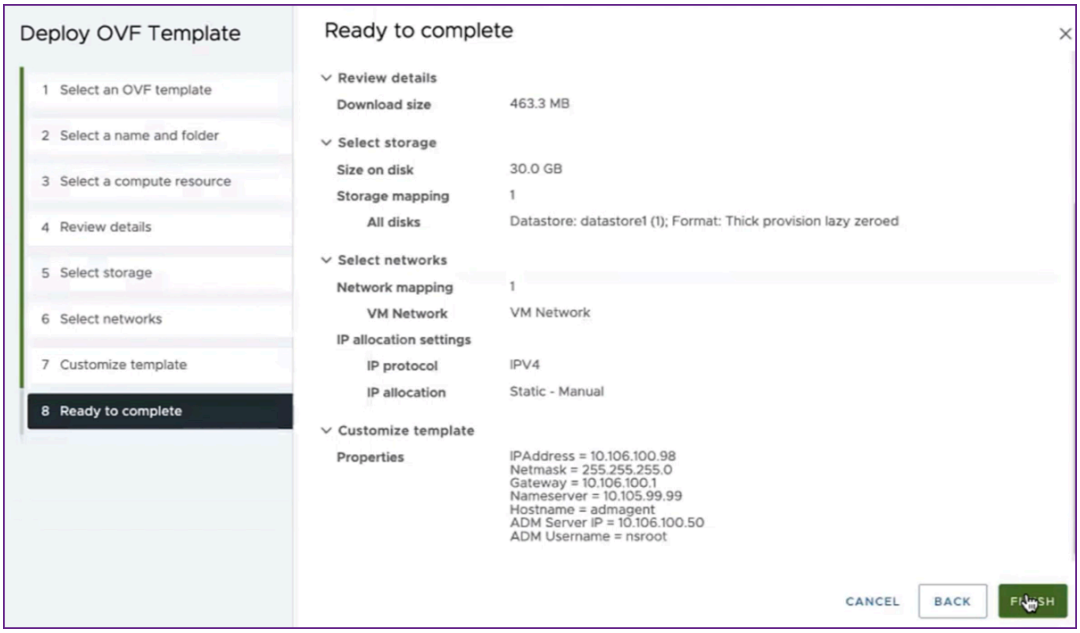
f) **Sélectionnez les réseaux** : conservez les paramètres par défaut. Cliquez sur **Suivant**.



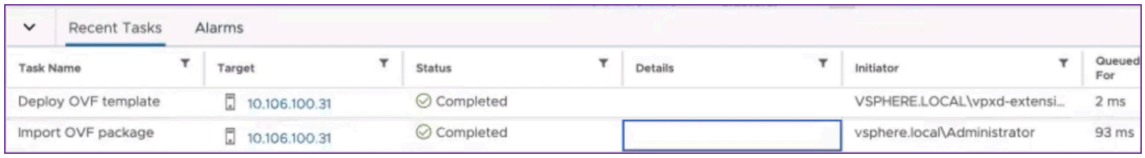
g) **Personnaliser le modèle** : passez en revue toutes les propriétés du modèle OVF. Tous les paramètres et valeurs que vous avez ajoutés au fichier .ovf dans la section Télécharger et modifier le fichier .OVF s'affichent.



h) **Prêt à terminer** : pour enregistrer les paramètres et démarrer le processus de déploiement, cliquez sur **Terminer**.

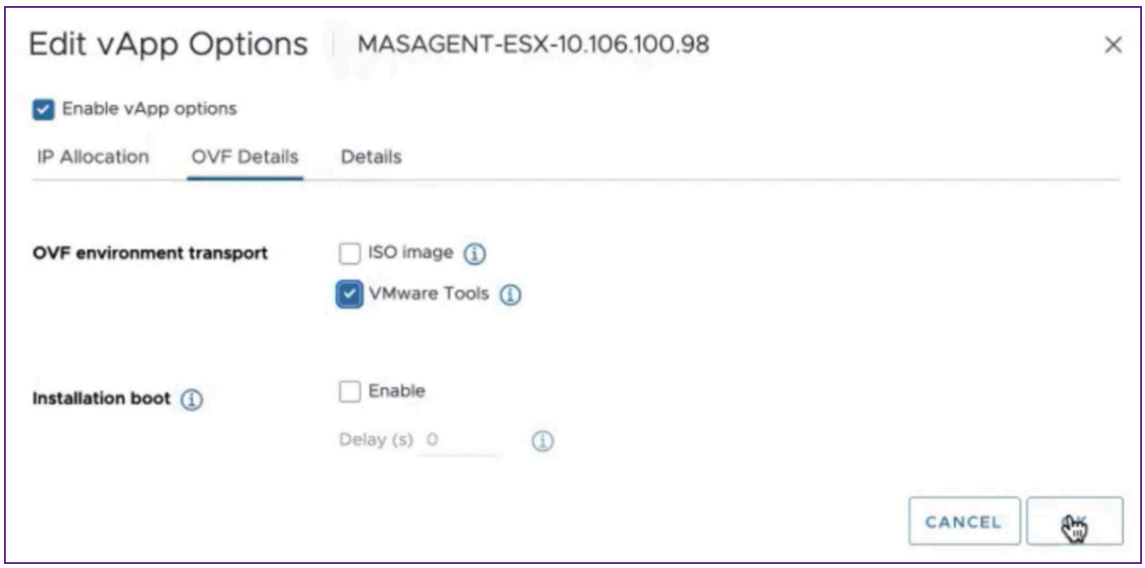


Attendez que le déploiement soit terminé. Lorsque l'état de l'opération de **déploiement du modèle OVF** est terminé à 100 %, votre agent est déployé.

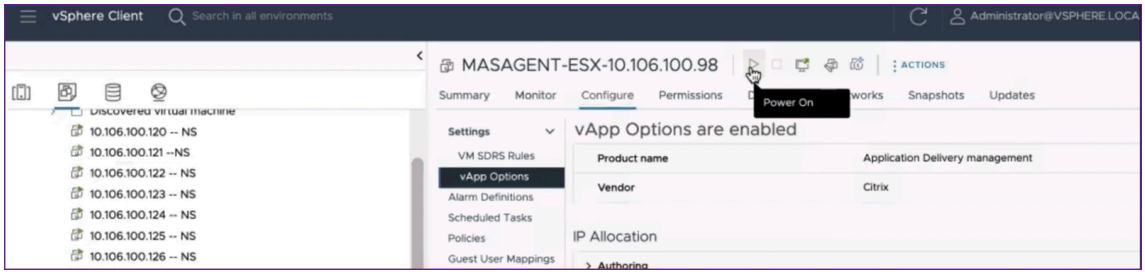


> **Important**
>
> N'allumez pas l'appliance virtuelle avant d'avoir modifié les paramètres.

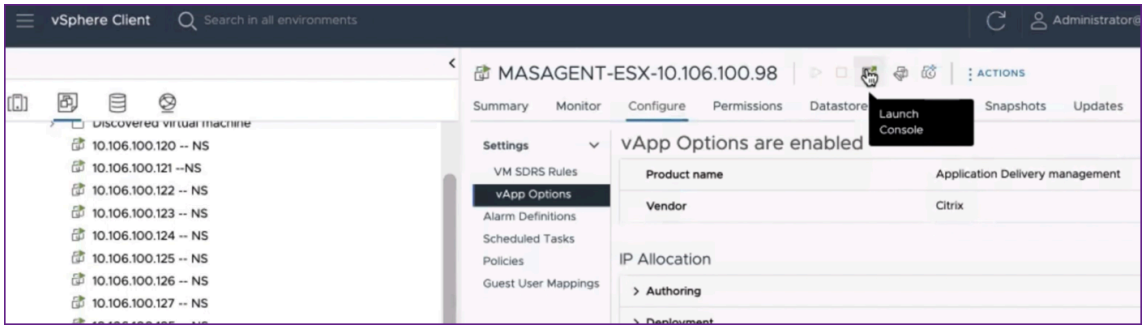
4. Cliquez sur le nouveau dispositif virtuel que vous avez installé et accédez à **Configurer > Paramètres > Options vApp > Modifier**.
5. Dans la fenêtre **Modifier les options du vApp**, accédez à **In OVF Details > Transport de l'environnement OVF**, puis sélectionnez **VMware Tools**. Cliquez sur **OK**.

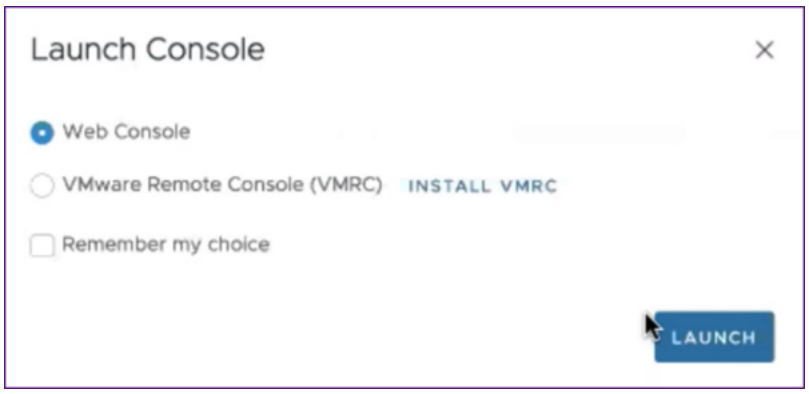


6. Cliquez avec le bouton droit sur la machine virtuelle et cliquez **sur Power On**. Vous pouvez également sélectionner l'onglet **Résumé** de la machine virtuelle et cliquer sur **Power On**.

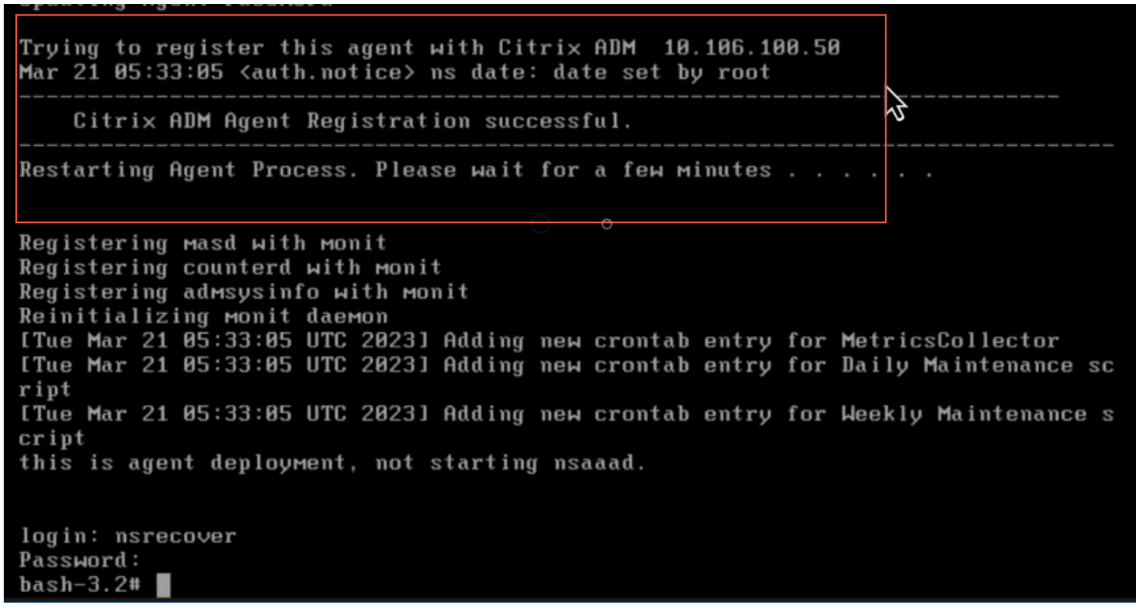


7. Dans l'onglet **Résumé**, sélectionnez **Lancer la console Web**.
   Dans la fenêtre **Launch Console**, sélectionnez **Web Console**. Cliquez sur **Launch**.





8. Dans la console, un message d'enregistrement réussi s'affiche une fois que l'agent NetScaler ADM est enregistré sur le serveur NetScaler ADM. Pour vérifier que l'agent NetScaler ADM a été déployé et que le mot de passe par défaut a été modifié, connectez-vous avec le nom d' utilisateur de l'agent NetScaler ADM et le nouveau mot de passe.



Vérifier

Pour vérifier que l'agent NetScaler ADM est déployé :

1. Une fois l'agent NetScaler ADM déployé, accédez à l'interface graphique de NetScaler ADM en saisissant l'
   adresse IP du serveur NetScaler ADM dans le navigateur.
2. Connectez-vous au serveur à l'aide de vos informations d'identification.
3. Accédez à **Infrastructure > Instances > Agents**.
   L'agent récemment déployé s'affiche dans la plateforme ESX.

NetScaler ADM sur un cluster Kubernetes

February 1, 2024

Avant d'installer les appliances virtuelles NetScaler ADM sur un cluster Kubernetes, lisez la section relative aux prérequis.

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 v1.20
  - Version client v1.20

  Tapez la commande `kubectl version` pour vérifier la version.
- L'application Helm installée sur le cluster doit avoir la version client v3.4.0 ou supérieure.

  Utilisez la commande `helm version` pour vérifier la version.
- Kubernetes cluster CNI (Container Network Interface) doit être Calico version v3.21.1 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 NetScaler

L'appliance NetScaler est requise en tant que périphérique d'entrée. ADC met à disposition les services applicatifs requis en dehors du
cluster Kubernetes. L'appliance NetScaler doit se trouver 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 NetScaler et téléchargez le fichier du NetScaler ADM Helm Chart 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 NetScaler afin que les services soient exposés au monde extérieur :

- `ingressIP`: une adresse IP virtuelle configurée dans NetScaler pour accéder à l'application.
- `applicationID`: un identifiant unique permettant de distinguer la configuration d'entrée du reste de la configuration sur l'appliance NetScaler.
- `ingressADCIP`: adresse IP NetScaler (NSIP), qui est utilisée comme entrée pour l'application ADM.
- `ingressADCUsername`: un nom d'utilisateur pour accéder à l'appliance NetScaler. 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.

NetScaler ADM sur un serveur KVM Linux

February 1, 2024

Les plateformes de virtualisation sur lesquelles NetScaler Application Delivery Management (ADM) peut être provisionné incluent Linux-KVM.

Avant d'installer NetScaler ADM sur Linux-KVM, assurez-vous que votre système dispose des extensions de virtualisation matérielle et 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 de configuration de NetScaler ADM et les télécharger sur votre ordinateur. Installez ensuite NetScaler ADM sur votre plate-forme Linux-KVM et configurez-le pour votre réseau.

Conditions préalables

Avant d'installer l'appliance virtuelle NetScaler ADM, vérifiez que Linux-KVM version 3.6.11-4 et versions ultérieures sont installés 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'existe aucune recommandation spécifique concernant la vitesse du processeur, mais plus la vitesse est élevée, meilleures sont les performances du NetScaler ADM.
Mémoire (RAM)	Minimum 4 Go pour le noyau Linux hôte. Ajoutez de la mémoire supplémentaire selon les besoins des machines virtuelles.
Disque dur	Calculez l'espace requis pour le noyau Host Linux et les machines virtuelles. Une seule machine virtuelle NetScaler ADM nécessite 120 Go d'espace disque.

> **Remarque**
>
> Les exigences en matière de mémoire et de disque dur spécifiées concernent le déploiement de NetScaler 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 NetScaler ADM ne prend en charge qu'une seule interface réseau para-virtualisée VirtIO. Assurez-vous de connecter cette interface au réseau de gestion de l'hôte Linux-KVM, afin que NetScaler ADM et Linux-KVM puissent communiquer.

Télécharger les fichiers de configuration de NetScaler ADM

Pour télécharger les fichiers de configuration de NetScaler ADM depuis : `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 des **téléchargements**, sélectionnez **NetScaler Application Delivery Management**.
5. Sur la page **NetScaler 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.

Installation de NetScaler 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.

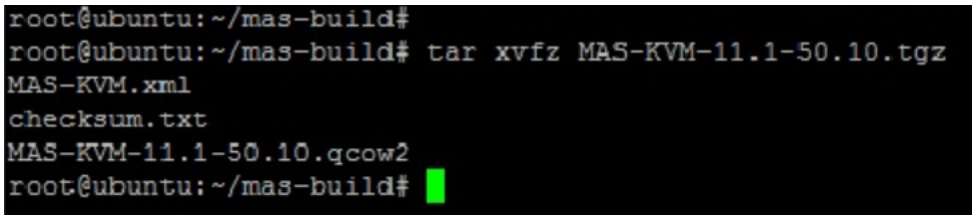
   b) Utilisez la commande tar pour décompresser le fichier image NetScaler Application Delivery Management. Le paquet décompressé contient les composants suivants :

i. Un fichier XML de domaine qui spécifie les attributs NetScaler 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.

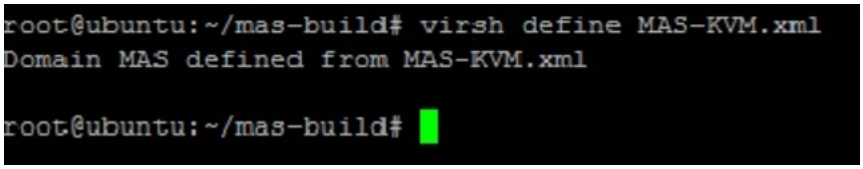
```
<name> MAS1-KVM</name>
<mac address='52:54:00:29:74:b3'/>
<source file='/var/ MAS-KVM.qcow2'/>
<source dev='eth0' mode='bridge'/>
<model type='virtio'/>
<!--NeedCopy-->
```

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
```

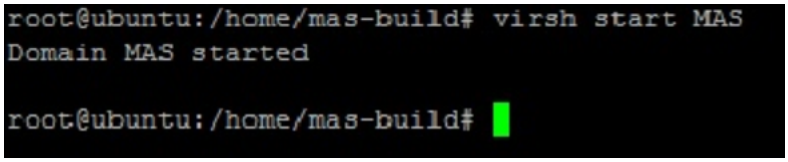


```
<!--NeedCopy-->
```



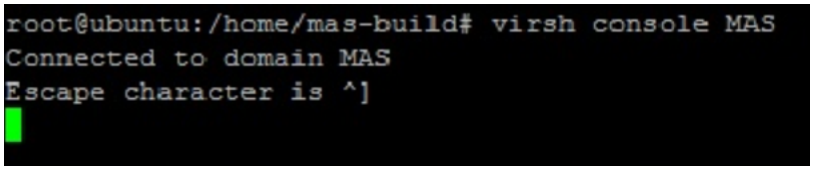
vii. Démarrez NetScaler ADM en saisissant la commande suivante : `virsh start \[\<DomainName\> | \<DomainUUID\>\]`

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



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

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



Configuration de la gestion de la mise à disposition des applications NetScaler

> **Remarque**
>
> Sur certains hôtes KVM Linux, les invités FreeBSD ne parviennent pas à redémarrer correctement s'ils ont plusieurs CPU. Lorsque l'appliance virtuelle NetScaler ADM est redémarrée, la CLI et l'interface graphique de NetScaler ADM ne répondent plus. Pour plus de détails, voir https://bugs.launchpad.net/qemu/+bug/1329956
>
> Pour éviter que la CLI et l'interface graphique de NetScaler ADM ne répondent plus lorsque l'appliance virtuelle NetScaler ADM est redémarré, arrêtez toutes les machines virtuelles de 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.

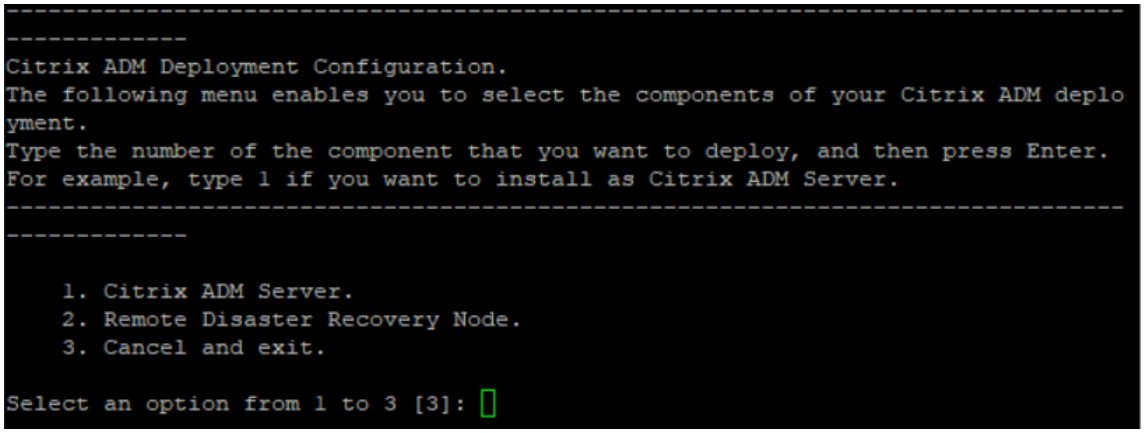
Après avoir installé NetScaler ADM, attendez environ 10 minutes pour que les services soient disponibles, puis connectez-vous à NetScaler ADM.

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 depuis l'interface utilisateur de NetScaler ADM. Sur la page d'accueil de NetScaler ADM, accédez à **Paramètres > 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 accéder au menu de configuration réseau initiale de NetScaler ADM. Configurez l'adresse IP de gestion.
4. Pour terminer la configuration réseau initiale de NetScaler ADM, suivez les instructions. La console affiche les options de configuration réseau initiale de NetScaler ADM pour définir les paramètres suivants pour NetScaler ADM. Le nom d'hôte est renseigné par défaut.
   a) Entrez **2** pour mettre à jour l'adresse IPv4 de NetScaler ADM : adresse IP de gestion à partir de laquelle vous accédez à un NetScaler 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 la passerelle : adresse IP de passerelle par défaut pour le sous-réseau de l'adresse IP de gestion de NetScaler 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 comme serveur **NetScaler ADM.**



7. Tapez **Oui** pour déployer NetScaler ADM en tant que déploiement autonome.
8. Tapez **Oui** pour redémarrer le serveur NetScaler ADM.
9. Après le redémarrage du serveur NetScaler ADM, ouvrez une session sur NetScaler ADM en utilisant les informations d'identification d'administrateur par défaut (nsroot/nsroot) via la ligne de commande ou l'interface graphique.

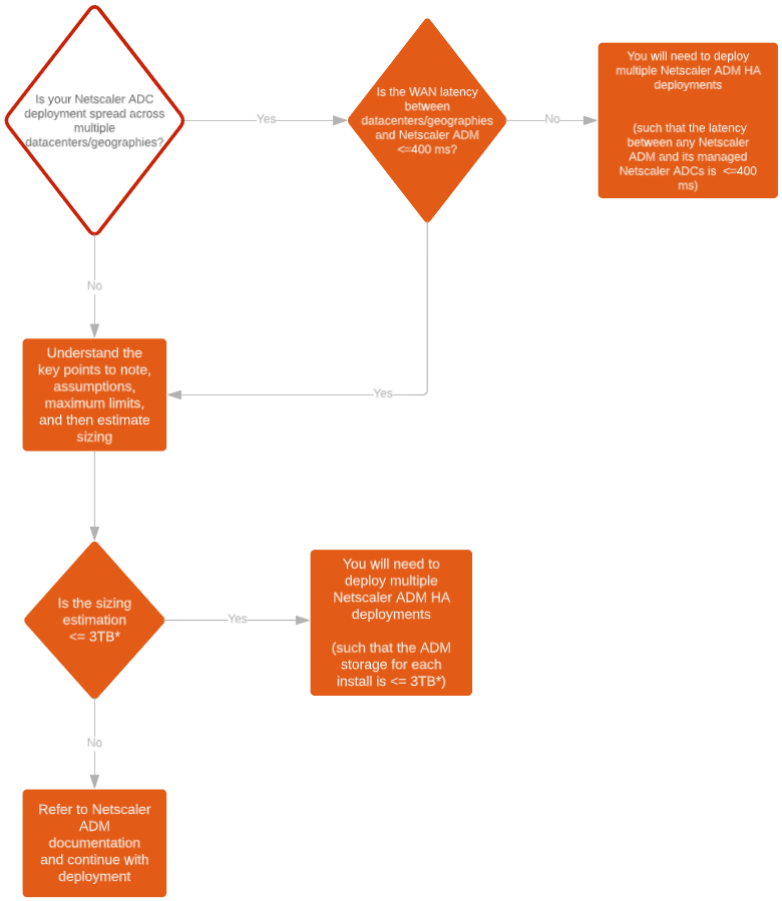
   Vous pouvez accéder ultérieurement à NetScaler ADM en saisissant l'adresse IP du serveur NetScaler ADM dans la barre d'adresse de votre navigateur. Les informations d'identification d'administrateur par défaut pour se connecter au serveur sont *nsroot/nsroot* .

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 à haute disponibilité de deux nœuds NetScaler 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 NetScaler ADM HA est de 3 To. Pour plus d'informations, consultez le guide de déploiement.
>
> **Important**
>
> **Pour accéder à NetScaler ADM 12.1 build 48.18 ou versions ultérieures via HTTPS :**
>
> Si vous avez configuré une instance NetScaler pour équilibrer la charge de NetScaler ADM en mode haute disponibilité, supprimez d'abord l'instance NetScaler. Configurez ensuite une adresse IP flottante pour accéder à NetScaler ADM en mode haute disponibilité.

Les avantages du déploiement de la haute disponibilité dans NetScaler 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 NetScaler distinct.
- Permet d'accéder facilement à l'interface utilisateur de NetScaler ADM à l'aide de l'adresse IP flottante.
- L'interface utilisateur NetScaler 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.

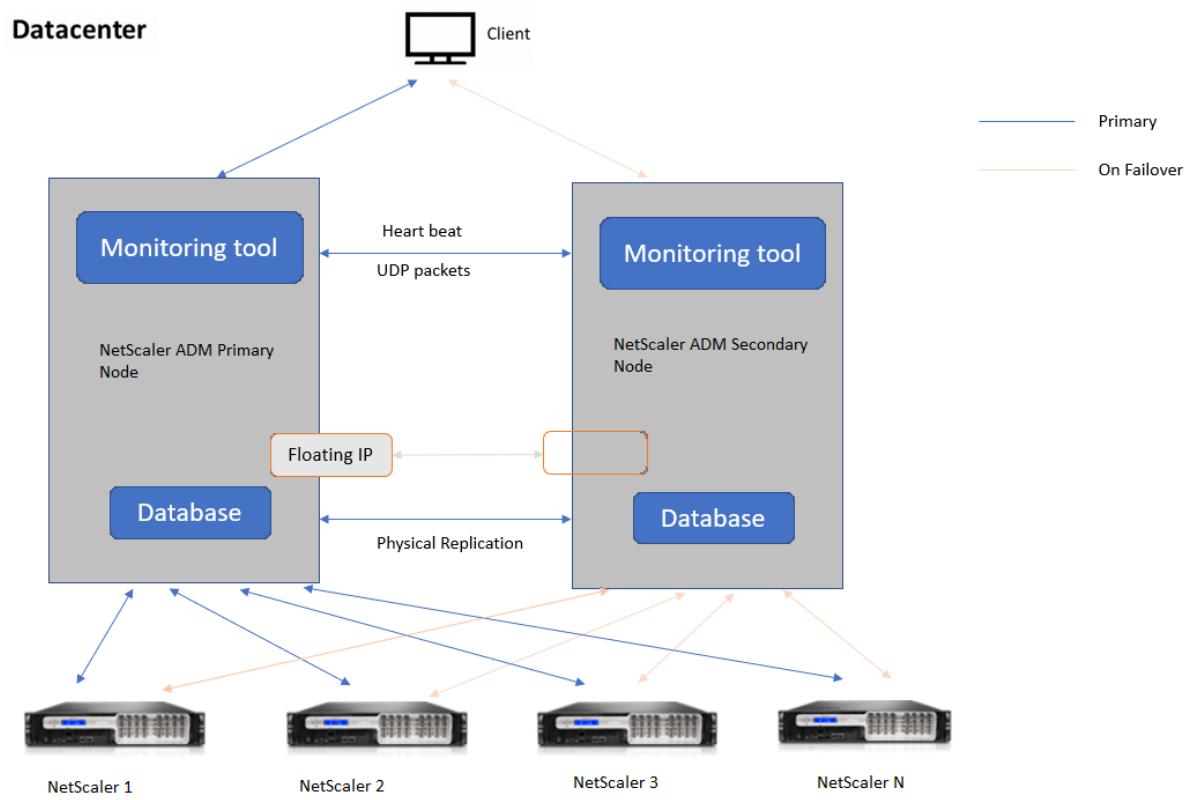
Termes	Description
Nœud principal	Premier nœud enregistré dans le déploiement de haute disponibilité.
Nœud secondaire	Deuxième nœud enregistré dans le déploiement de haute disponibilité.
Battement de cœur	Mécanisme utilisé pour échanger des messages entre le nœud principal et le nœud secondaire dans la configuration de haute disponibilité. Les messages déterminent l'état et l'état de santé de l'application sur chaque nœud individuel.

Termes	Description
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 montre l'architecture de deux nœuds NetScaler ADM déployés en mode haute disponibilité.



Dans le cadre d'un déploiement à haute disponibilité, un nœud NetScaler 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 de NetScaler 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 de NetScaler 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 NetScaler ADM et de la base de données pour échanger des informations sur l'état du nœud, son intégrité, 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 NetScaler 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 à haute disponibilité, les deux nœuds NetScaler 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.

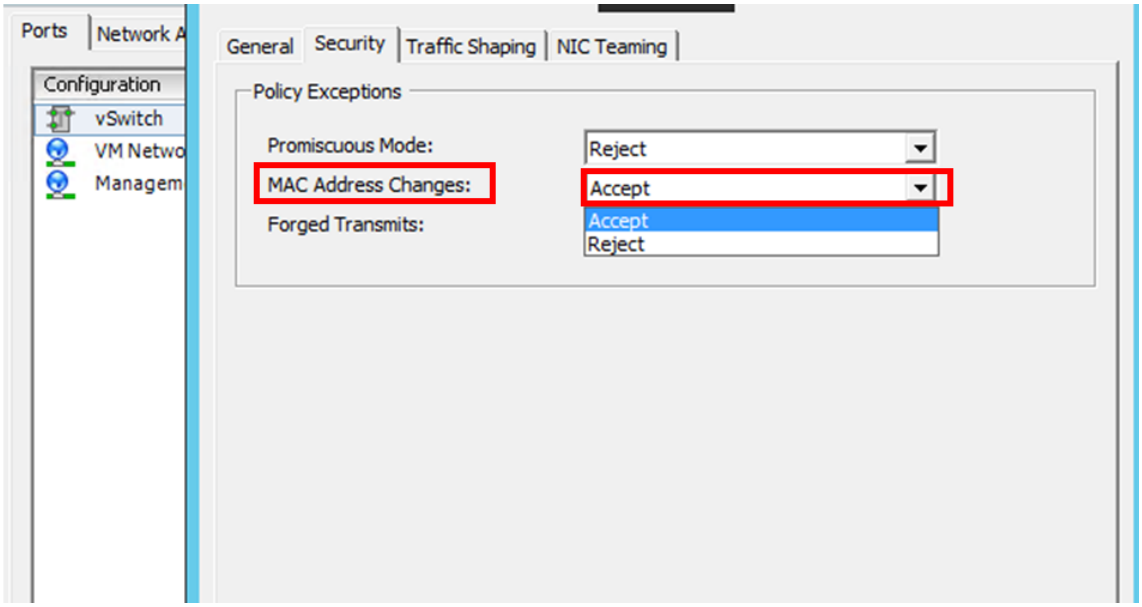
    > **Remarque**
    >
    > Citrix vous recommande d'utiliser l'adresse IP flottante pour accéder à l'interface utilisateur.

- 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 NetScaler ADM :
  - Les processus internes mettent implicitement à niveau NetScaler ADM par rapport aux versions antérieures.

    > **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 NetScaler ADM en haute disponibilité sur VMware ESXi, assurez-vous d'accepter les modifications apportées à l'adresse MAC. ESXi autorise désormais les requêtes à modifier l'adresse MAC active en autre que l'adresse MAC initiale.

> **Remarque**
>
> Pour NetScaler 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 NetScaler ADM est déployé sur la version d'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 NetScaler ADM, tenez compte des conditions préalables suivantes :

- Le déploiement haute disponibilité de NetScaler ADM est pris en charge à partir de NetScaler ADM version 12.0 build 51.24.
- Téléchargez le fichier image de NetScaler Application Delivery Management (.xva) depuis le site NetScaler : 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 de NetScaler ADM. La valeur par défaut est 120 Go. Les besoins de stockage réels dépendent de l'estimation de la taille de NetScaler ADM. Si votre besoin de stockage NetScaler ADM dépasse 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, consultezComment associer un disque supplémentaire à NetScaler 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 NetScaler 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.

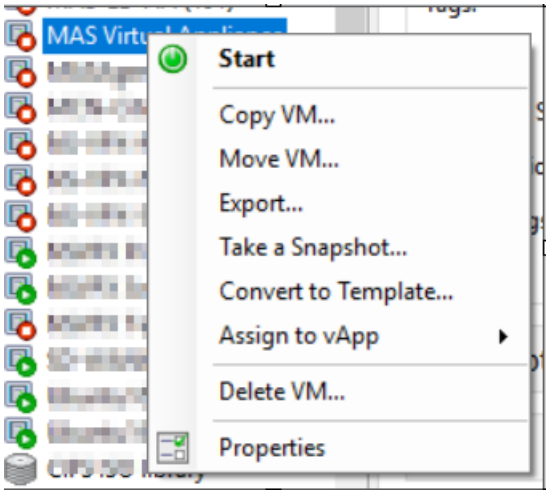
Enregistrer et déployer le premier serveur (nœud principal)

Pour enregistrer le premier nœud :

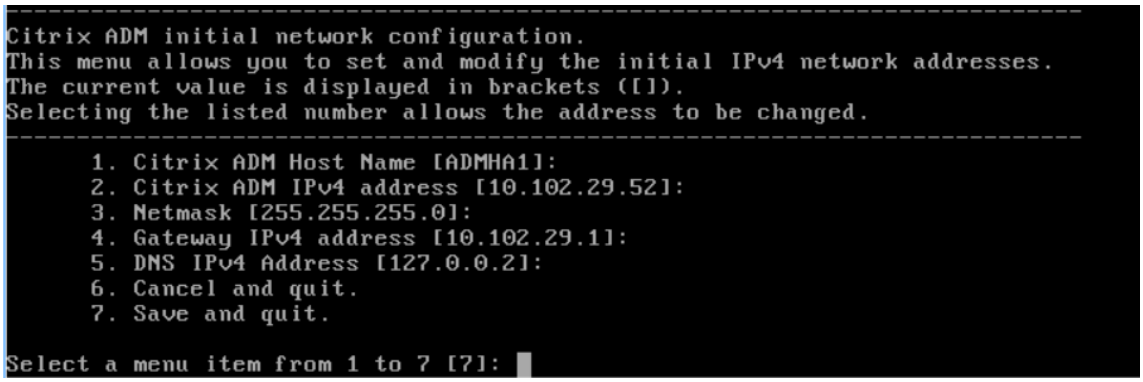
1. Utilisez le fichier image .xva téléchargé depuis le site NetScaler et importez-le dans votre hyperviseur.

   > **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 NetScaler ADM avec les configurations réseau initiales.

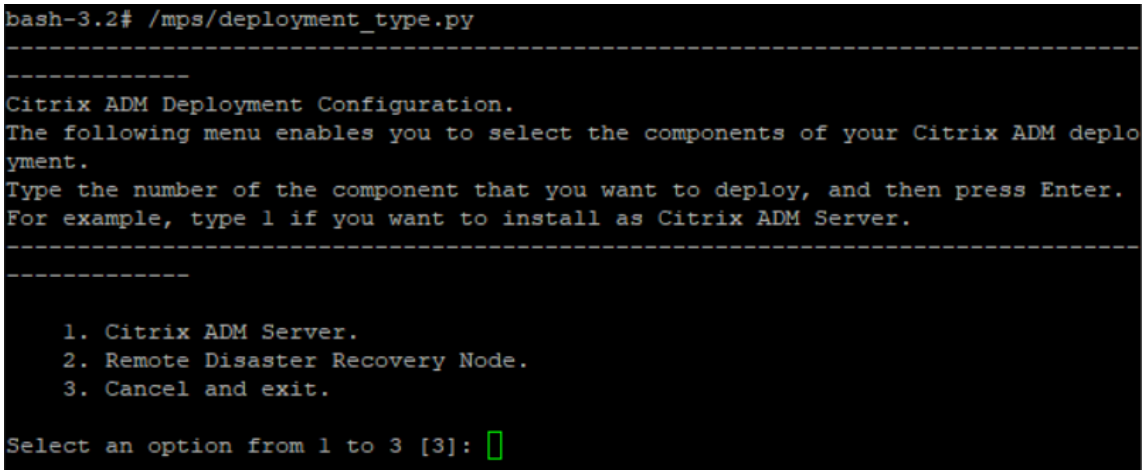
   

4. Une fois la configuration réseau initiale terminée, le système demande une connexion. Ouvrez une session à l'aide des informations d'identification suivantes : *nsrecover/nsroot*.

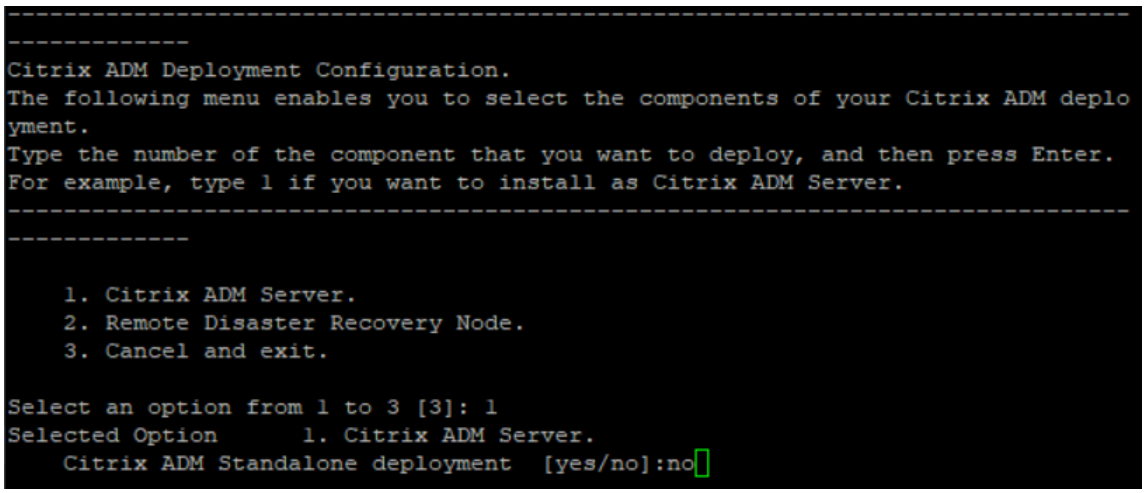
   > **Remarque**
   >
   > Une fois que vous ouvrez une session, si vous souhaitez mettre à jour la configuration réseau initiale, tapez `networkconfig`, mettez à jour la configuration et enregistrez la configuration.

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

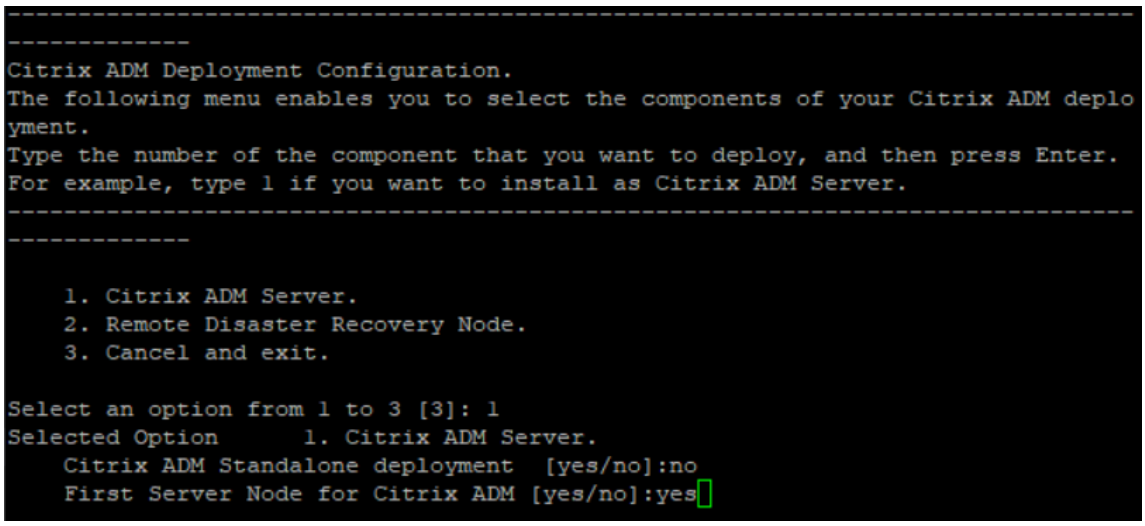
6. Sélectionnez **1** pour enregistrer le serveur NetScaler ADM en tant que nœud principal.



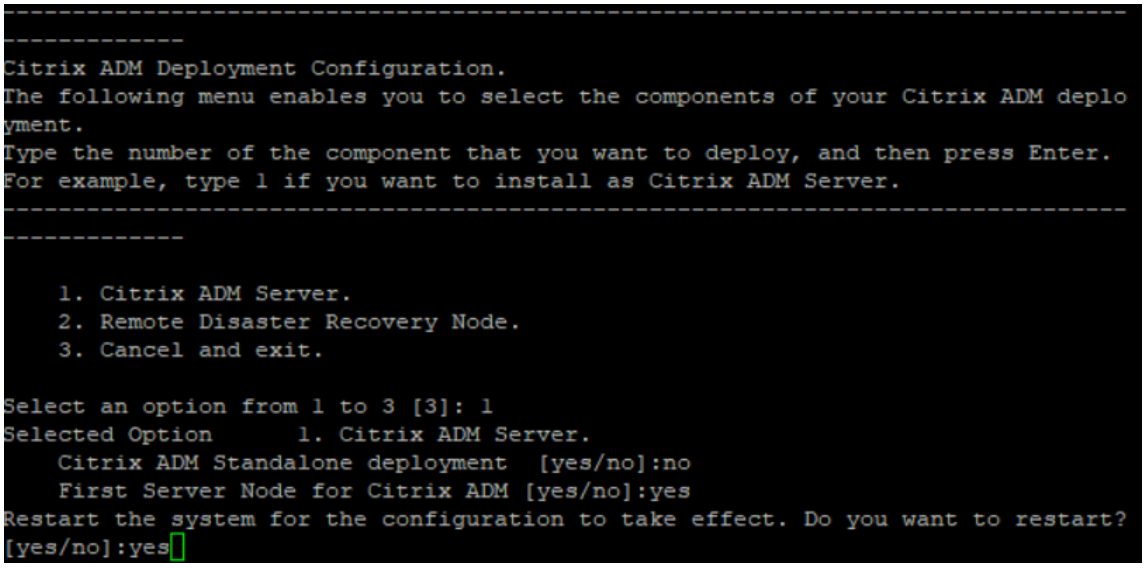
7. La console vous invite à sélectionner le déploiement autonome de NetScaler ADM. Saisissez **Non** pour confirmer le déploiement comme haute disponibilité.



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 de NetScaler ADM.

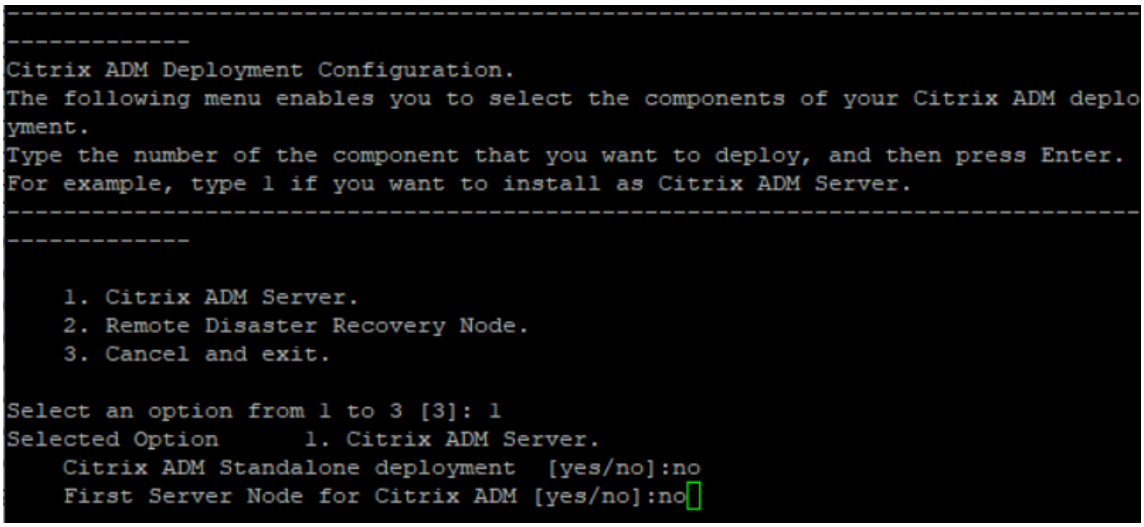
Inscrire et déployer le deuxième serveur (nœud secondaire)

1. Utilisez le fichier image **.xva** téléchargé depuis le site NetScaler et importez-le dans votre hyperviseur.
2. Dans l'onglet **Console**, configurez NetScaler ADM avec les configurations réseau initiales, comme indiqué dans l'image suivante.

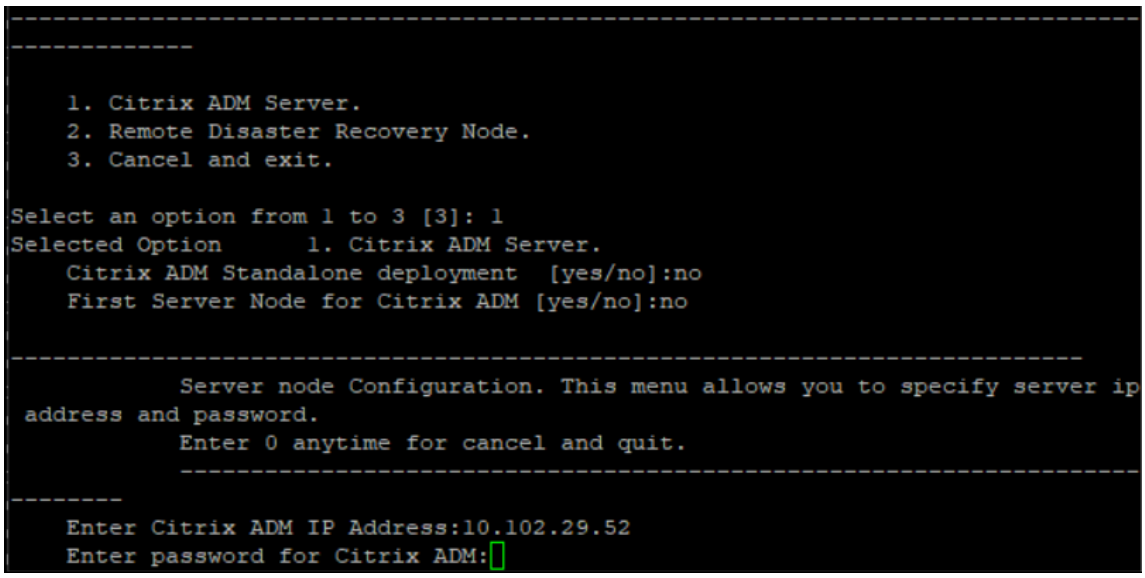
3. Une fois la configuration réseau initiale terminée, le système demande une connexion. Ouvrez une session à l'aide des informations d'identification suivantes : *nsrecover/nsroot*.

   > **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.

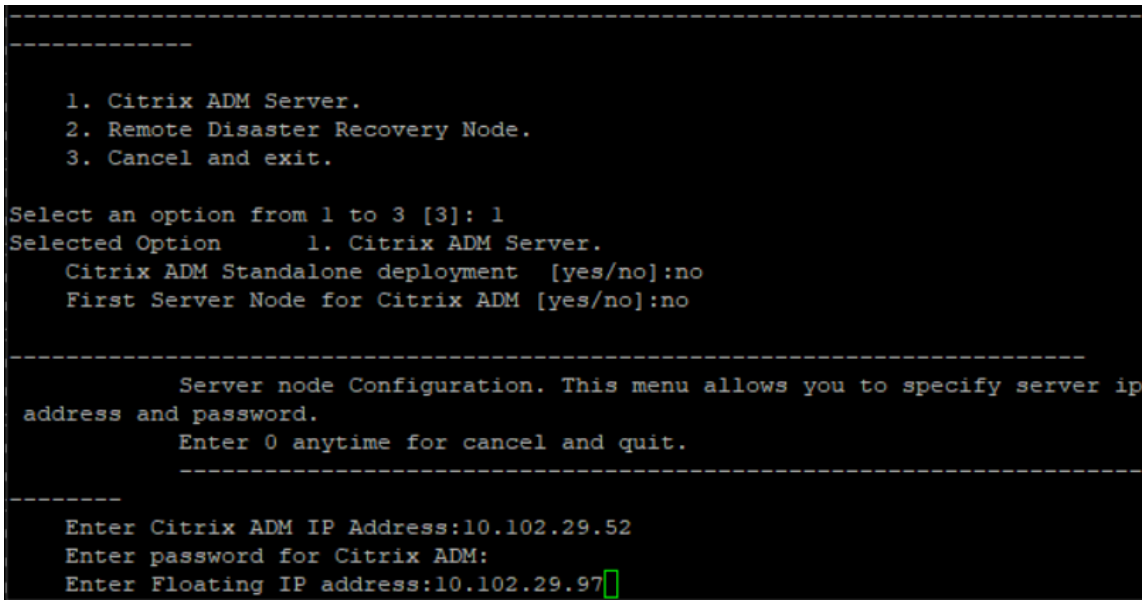
4. Pour déployer le nœud secondaire, saisissez **/mps/deployment_type.py**. Le menu de configuration du déploiement de NetScaler ADM s'affiche.
5. Sélectionnez **1** pour enregistrer le serveur NetScaler ADM en tant que nœud secondaire.
6. La console vous invite à sélectionner NetScaler ADM en tant que 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 principaux et secondaires sont affichés sur l'interface utilisateur de NetScaler 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 de NetScaler 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 NetScaler 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**.

   NetScaler ADM redémarre et la configuration prend environ 10 minutes pour prendre effet.

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

7. Connectez-vous à NetScaler ADM à l'aide des informations d'identification de l'administrateur, cliquez sur **Commencer** sur la page d'accueil et, le cas échéant, procédez comme suit :

   a) Ajouter des instances NetScaler

   b) Configurer l'identité du client

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

8. Accédez à **Paramètres > 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 NetScaler ADM et convertir les nœuds en serveurs NetScaler 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 NetScaler 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

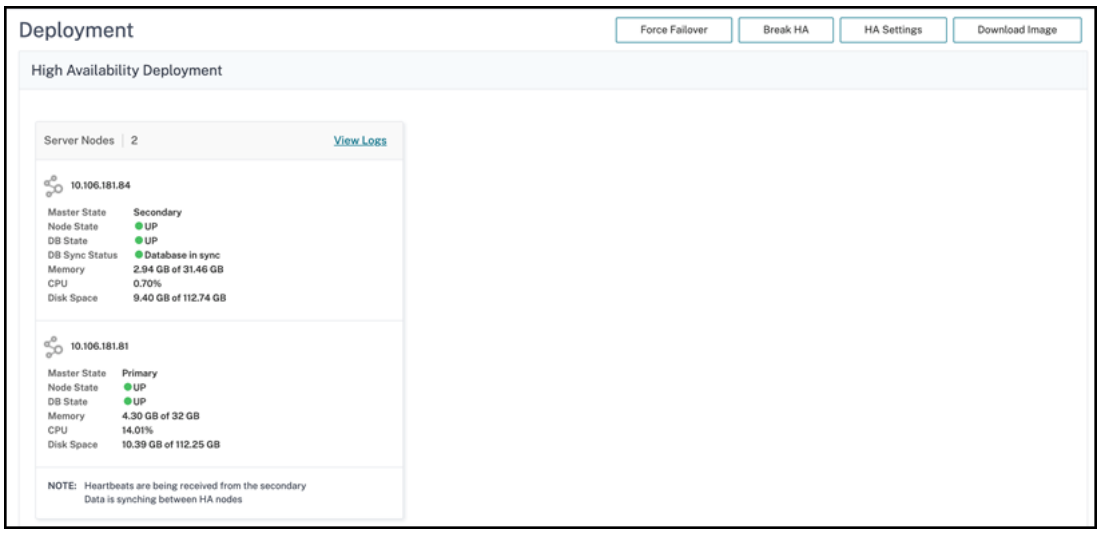
Un basculement se produit si l'une des conditions suivantes est remplie :

- **Échec du nœud** : le nœud principal s'éteint, aucun rythme cardiaque n'est détecté à partir du nœud principal pendant 180 secondes.
- **Défaillance de l'application** : le nœud principal est opérationnel mais l'un des processus NetScaler ADM est en panne.

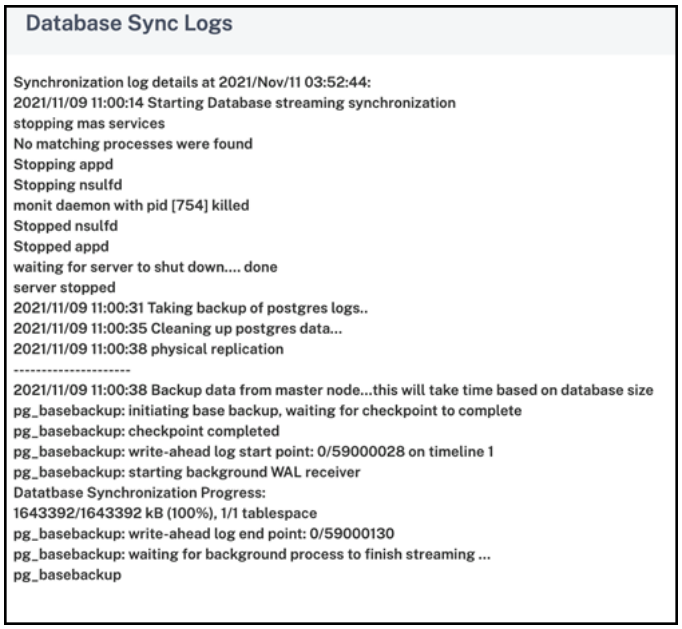
Afficher les messages du journal de synchronisation de

Dans la paire NetScaler ADM HA, les fichiers de configuration sont automatiquement synchronisés du nœud principal vers le nœud secondaire et la réplication physique en continu de la base de données a lieu.

Toutefois, en cas d'erreur de réplication en continu, le bouton **Synchroniser la base de données** apparaît. Vous pouvez cliquer sur le bouton **Sync Database** pour démarrer le processus de synchronisation de la base de données.



Pour afficher la progression de la synchronisation de la base de données, cliquez sur **Afficher les journaux**. Le message **Journaux de synchronisation de la base** de données s'affiche et vous pouvez afficher les détails de la progression de la synchronisation en temps réel.



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 NetScaler ADM ont été déployés en tant que nœud principal et nœud secondaire. En raison d'une possible interruption de la liaison réseau, la communication entre les deux nœuds NetScaler 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 NetScaler ADM 12.1 ou version ultérieure, cette situation de division du 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 réinitialisées 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) de NetScaler ADM fournit des fonctionnalités complètes de sauvegarde et de restauration du système pour NetScaler ADM déployé 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 NetScaler ADM.

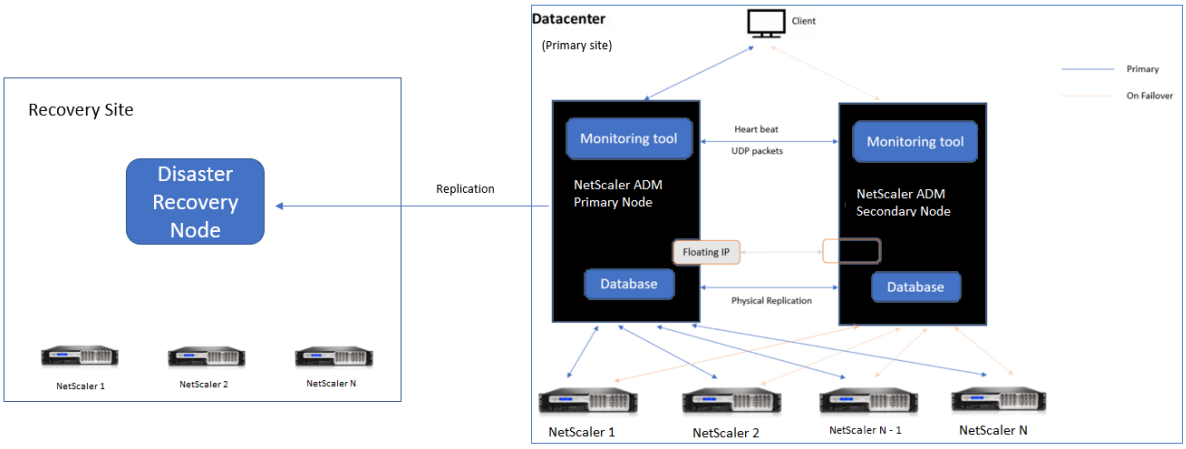
Termes	Description
Site principal (datacenter A)	Les nœuds NetScaler ADM du site principal sont déployés en mode haute disponibilité.
Site de récupération (centre de données B)	Le site de récupération dispose d'un nœud de reprise après sinistre déployé en mode autonome. Ce nœud est en mode lecture seule 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 DR 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 NetScaler ADM du site principal sont déployés en mode haute disponibilité. Pour en savoir plus, consultez Déploiement haute disponibilité

Le site de reprise dispose d'un nœud de reprise après sinistre NetScaler 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 NetScaler présentes sur le site de restauration 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, le site principal doit disposer de nœuds NetScaler ADM configurés en mode haute disponibilité.
- Le déploiement autonome de NetScaler ADM sur le site principal ne prend pas en charge la fonctionnalité de reprise après sinistre.
- La paire NetScaler 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

Composant	Exigences
Espace de stockage	Citrix recommande d'utiliser la technologie SSD (Solid-State Drive) pour les déploiements NetScaler ADM. La valeur par défaut est 120 Go. Les besoins de stockage réels dépendent de l'estimation de la taille de NetScaler ADM. Si votre besoin de stockage NetScaler ADM dépasse 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 NetScaler 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 NetScaler ADM en mode haute disponibilité
- Déployer et enregistrer le nœud de reprise après sinistre NetScaler ADM
- Activer et désactiver les paramètres de reprise après sinistre à partir de l'interface utilisateur

Déployer NetScaler ADM en mode haute disponibilité

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

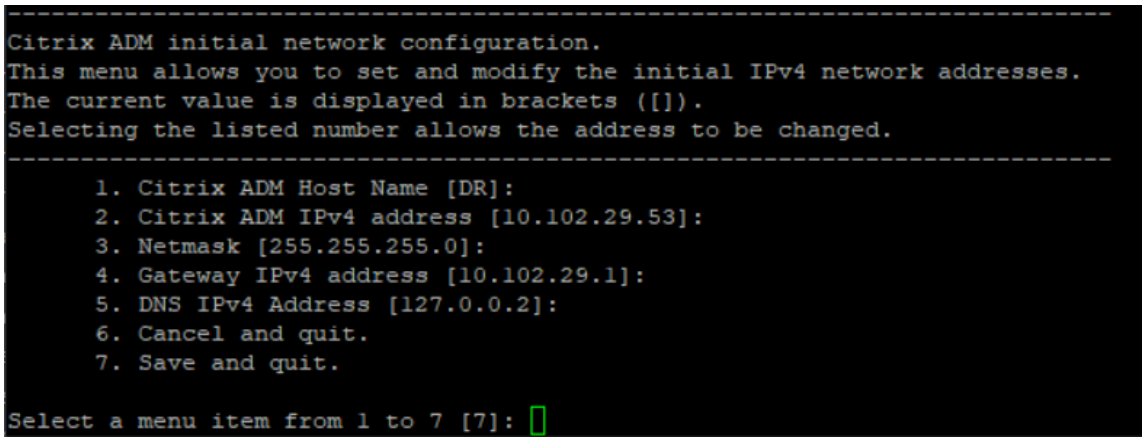
> **Remarque**
>
> - NetScaler ADM déployé en mode haute disponibilité doit être mis à niveau vers la version 13.1 de NetScaler ADM.
> - **L'adresse IP flottante est obligatoire** pour enregistrer le nœud de reprise après sinistre auprès du nœud principal.

Déployer et enregistrer le nœud de reprise après sinistre NetScaler ADM à l'aide de la console DR

Pour enregistrer le nœud de reprise après sinistre NetScaler ADM :

1. Téléchargez le fichier image `.xva` depuis le site NetScaler et importez-le dans votre hyperviseur.
2. Dans l'onglet **Console**, configurez NetScaler 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 de NetScaler ADM s'affiche.


```
bash-3.2# /mps/deployment_type.py
------------------------------------------------------------------------------
------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------
------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]:
```

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

```
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 2
Selected Option      2. Remote Disaster Recovery Node.
```

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.

```
------------------------------------------------------------------------------
    Backup node Configuration.

    Specify the IP address and the password of the Citrix ADM server.
    Type 0 anytime to cancel and quit.
    ------------------------------------------------------------------------
    Enter Citrix ADM Floating IP Address:10.102.29.97
    Enter password for Citrix ADM:
```

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

```
Stopping appd
Stopping nsulfd
Stopped nsulfd
Stopped appd
waiting for server to shut down.... done
server stopped
------------------------------------------------------------------------
    Backup node Registration successful.
    ------------------------------------------------------------------------
```


> **Remarque**
>
> - Le nœud de reprise après sinistre ne possède pas d'interface graphique.
> - Une fois l'enregistrement réussi, les informations d'identification de l'administrateur par défaut pour se connecter au serveur sont `nsroot`/`nsroot`.

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

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

Exemple :

```
/mps/change_freebsd_password.sh nsroot new_password
<!--NeedCopy-->
```

Déployer le nœud de reprise après sinistre à l'aide de l'interface graphique NetScaler 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 NetScaler ADM. Cette étape active les paramètres de reprise après sinistre à partir du site principal de NetScaler 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 NetScaler 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 DR en suivant la procédure disponible sur Déployer et enregistrer le nœud de reprise après sinistre NetScaler ADM à l'aide de la console DR.
3. Déployez le nœud de reprise après sinistre à l'aide de l'interface graphique NetScaler 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 :

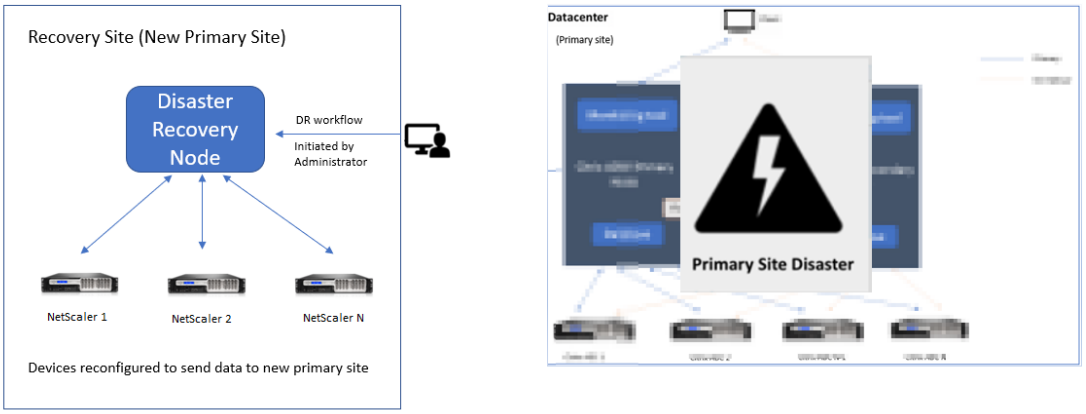
     ```
     /mps/scripts/pgsql/pgsql_restore_remote_backup.sh

     <!--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 NetScaler sont automatiquement reconfigurées pour envoyer les données au nœud de reprise après sinistre qui est désormais 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.

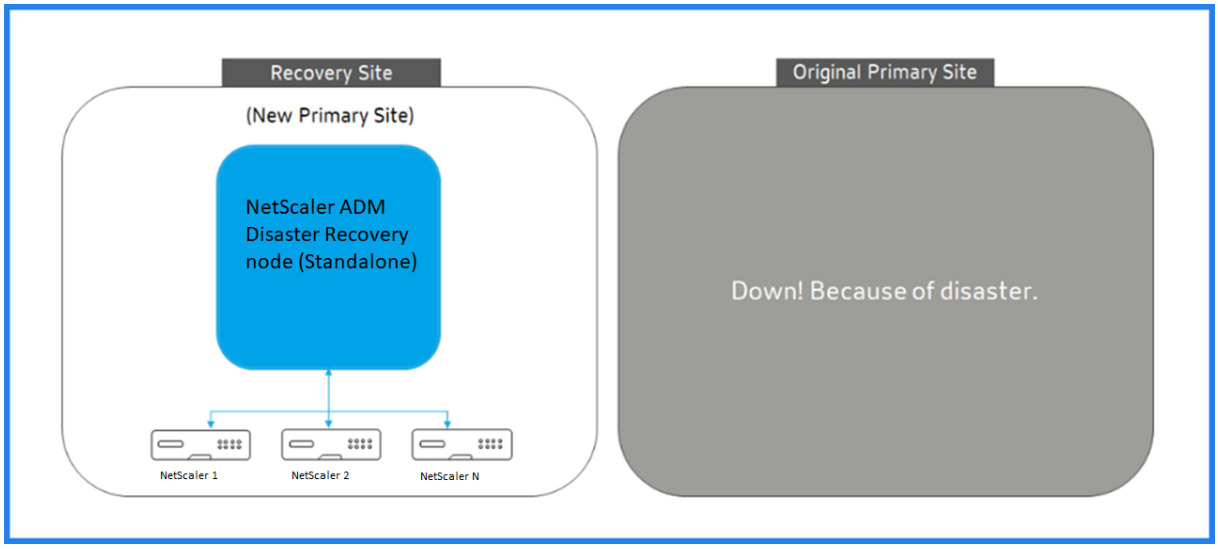
Si vous souhaitez rétablir les configurations sur le site d'origine ultérieurement, reportez-vous à la section Rétablir les configurations sur le site principal d'origine.

Important

- Si vous avez installé NetScaler ADM 12.1.49.x ou des versions antérieures, vous bénéficiez d'un délai de grâce de 30 jours pour contacter Citrix afin de réhéberger la licence d'origine sur NetScaler ADM (sur le site DR).
- Pour les versions 12.1.50.x ou ultérieures, la licence NetScaler ADM est automatiquement synchronisée avec le site DR (il n'est pas nécessaire de contacter Citrix pour obtenir la licence).
- Si vous avez appliqué des licences groupées pour les instances, les versions NetScaler **11.1 65.x ou ultérieure**, **12.1 58.x ou version ultérieure**, **13.0 47.x ou version ultérieure** et NetScaler SDX **13.0 76.x ou version ultérieure** peuvent prendre en charge la mise à jour automatique du serveur de licences sur le site DR. Pour toutes les autres versions, vous devez reconfigurer manuellement les instances sur le site DR.

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-->
```

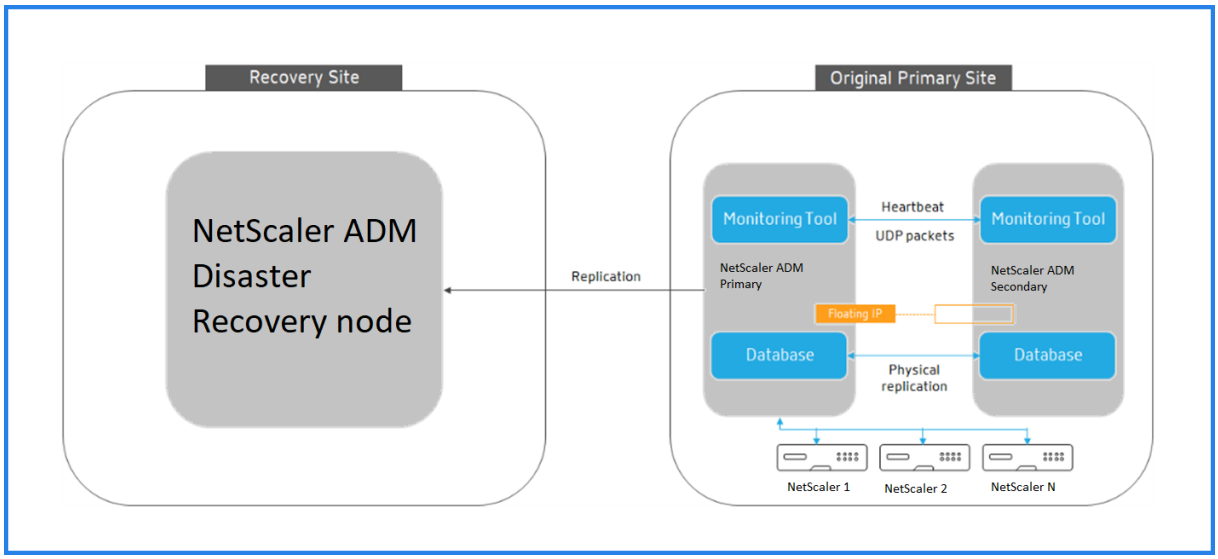
   Cette commande configure uniquement Syslog, SNMP et Analytics sur le site principal.

   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 réussi à rétablir les configurations du site DR vers le site principal d'origine, le trafic client passe par le nœud principal de NetScaler ADM.

Configurer les agents sur site pour un déploiement multisite

February 1, 2024

Dans les versions précédentes de NetScaler ADM, les instances NetScaler déployées dans des centres de données distants pouvaient être gérées et surveillées à partir de NetScaler ADM exécuté dans un centre de données principal. Les instances NetScaler ont envoyé des données directement au NetScaler ADM principal, ce qui a entraîné une consommation de bande passante WAN. De plus, le traitement des données d'analyse utilise les ressources du processeur et de la mémoire du NetScaler ADM principal.

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.
- Pour limiter le nombre d'instances qui envoient directement du trafic à NetScaler 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 ajouter directement des instances NetScaler à NetScaler 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.
> - L'agent local NetScaler ADM ne prend pas en charge les licences groupées.

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

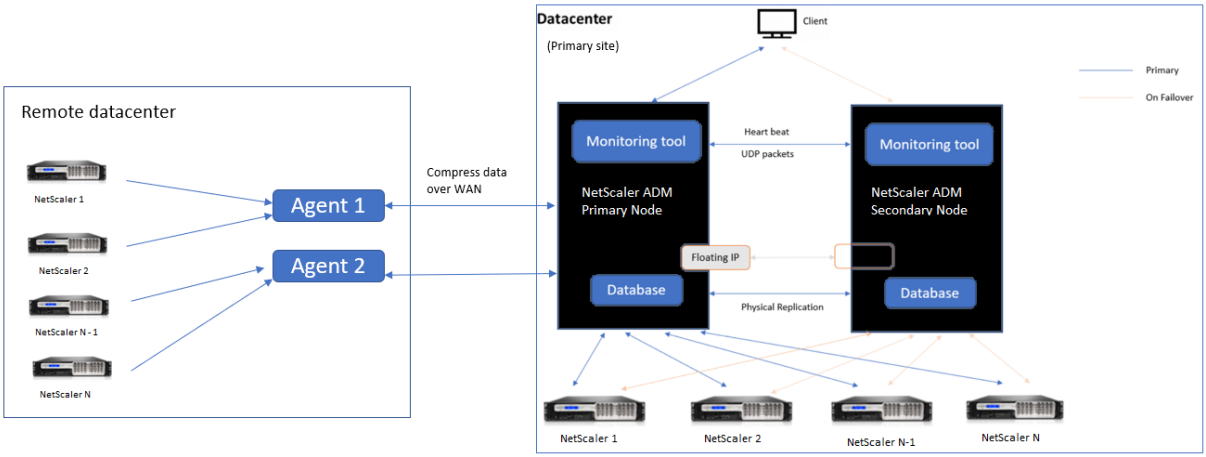
Les agents font office d'intermédiaire entre le NetScaler ADM principal et les instances découvertes dans différents centres de données. Les avantages de l'installation d'agents sont les suivants :

- Les instances sont configurées pour les agents afin que les données non traitées soient envoyées directement aux agents plutôt qu'au NetScaler ADM principal. Les agents effectuent le premier niveau de traitement des données et envoient les données traitées au format compressé au NetScaler 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 de redistribuer les instances NetScaler lors du basculement des agents. Lorsqu'un agent d'un site tombe en panne, le trafic provenant des instances NetScaler 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 montre les instances NetScaler dans deux centres de données et le déploiement de haute disponibilité de NetScaler ADM à l'aide d'une architecture basée sur des agents multisites.



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

Sur le site secondaire, les agents sont déployés et enregistrés auprès du serveur NetScaler ADM du site principal. Ces agents travaillent dans un cluster pour gérer un flux de trafic continu en cas de basculement d'agent. Les instances NetScaler du site secondaire sont enregistrées auprès du serveur NetScaler ADM principal via des agents situés sur ce site. Les instances envoient des données directement aux agents plutôt qu'au NetScaler ADM principal. Les agents traitent les données reçues des instances et les envoient au NetScaler ADM principal dans un format compressé. Les agents communiquent avec le serveur NetScaler ADM via un canal sécurisé et les données envoyées via ce canal sont compressées pour optimiser 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 NetScaler
  - 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 permettre la communication entre le NetScaler ADM principal et les instances NetScaler 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 de NetScaler 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 local NetScaler ADM.

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

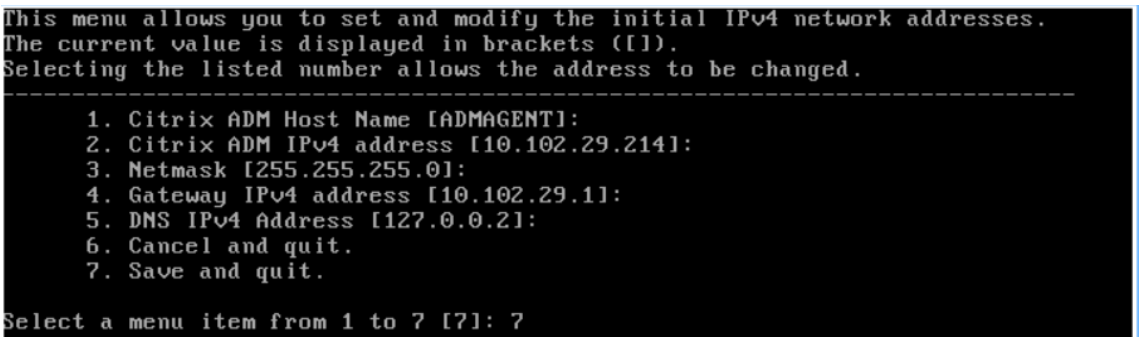
Les ports suivants doivent être ouverts entre l'agent et les instances NetScaler.

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

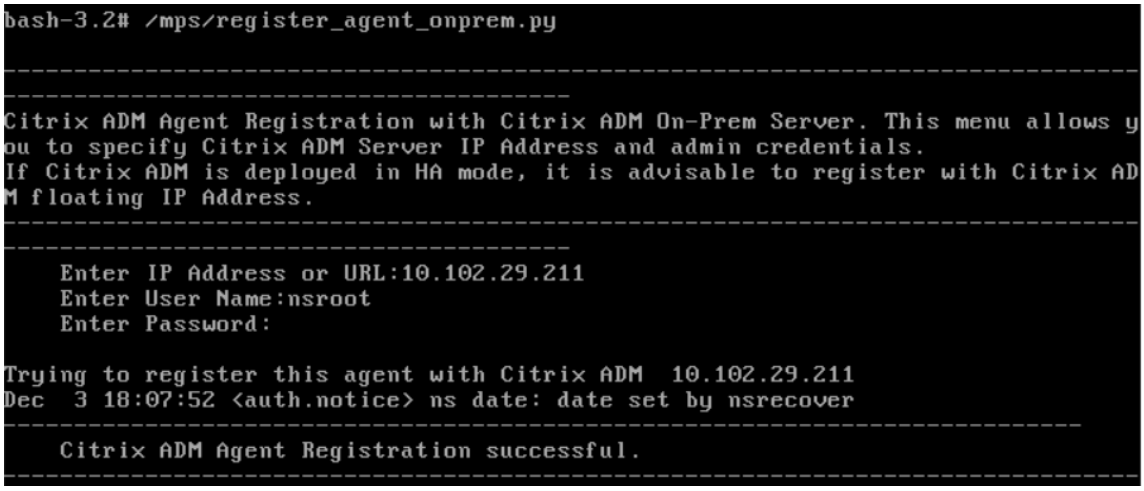
Type	Port	Détails	Direction de la communication
TCP	5557	Pour la communication Logstream entre l'agent et les instances NetScaler.	NetScaler vers NetScaler ADM

Enregistrer l'agent

1. Utilisez le fichier image de l'agent téléchargé depuis le site NetScaler et importez-le dans votre hyperviseur. 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 NetScaler ADM avec les configurations réseau initiales.
3. Entrez le nom d'hôte NetScaler 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 *nsrecover/nsroot* comme informations d'identification.
5. Pour enregistrer l'agent, entrez **/mps/register_agent_onprem.py**. Les informations d'identification de l'agent NetScaler ADM s'affichent comme indiqué dans l'image suivante.
6. Entrez l'adresse IP flottante NetScaler ADM et les informations d'identification de l'utilisateur.



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

Une fois l'agent redémarré, accédez à l'interface graphique NetScaler ADM. Dans le menu principal, accédez à la page **Infrastructure > Instances > Agents** pour vérifier l'état de l'agent. L'agent récemment ajouté est affiché à l'état **Actif** .

> **Remarque**
>
> NetScaler ADM affiche la version de l'agent et vérifie également si l'agent utilise 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 NetScaler ADM.

Attacher un agent à un site

1. Sélectionnez l'agent et cliquez sur **Joindre le site.**
2. Sur la page **Attacher un site**, sélectionnez un site dans la liste ou créez-en un 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 NetScaler qui lui sont attribuées sont automatiquement transférées vers d'autres agents opérationnels sur le même site.

Actions d'agent

Vous pouvez appliquer différentes actions à un agent sous **Infrastructure > 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 NetScaler ADM sélectionné. Vous pouvez télécharger ce fichier et l'envoyer au support technique Citrix pour enquête et dépannage.

Ajouter des instances NetScaler

Les instances sont des appliances NetScaler ADC ou des appliances virtuelles que vous souhaitez découvrir, gérer et surveiller à partir de NetScaler ADM via des agents. Vous pouvez ajouter les appliances NetScaler ADC et les appliances virtuelles suivantes à NetScaler ADM ou à ses agents :

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler Gateway
- Proxy de transfert SSL Citrix

Pour plus d'informations, consultez la section Ajouter des instances à NetScalerADM.

Joindre une instance existante à l'agent

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

1. Accédez à **Infrastructure > Instances** et sélectionnez le type d'instance. Par exemple, NetScaler.
2. Cliquez sur **Modifier** pour modifier une instance existante.
3. Cliquez sur pour sélectionner l'agent.

4. Sur 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 NetScaler ADM, accédez à **Infrastructure > Instances**. Sous **Instances**, sélectionnez le type d'instance auquel vous souhaitez accéder (par exemple, NetScaler 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 NetScaler 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 de l'agent NetScaler 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, NetScaler 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 des agents, sélectionnez les agents NetScaler ADM un par un et associez-les au même site.

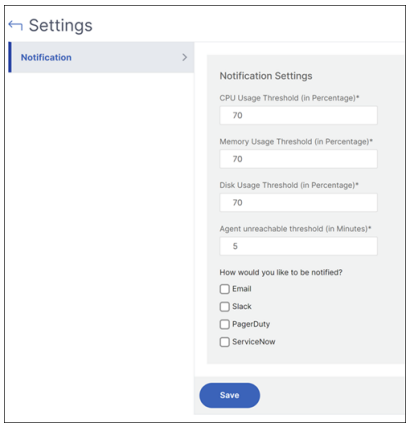
Par exemple, deux agents 10.106.1xx.2x et 10.106.1xx.3x sont rattachés et opérationnels sur le site de Bangalore. Si un agent devient inactif, NetScaler ADM le détecte et affiche son état comme étant inactif.

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

NetScaler ADM déclenche la redistribution des instances toutes les 30 minutes afin d'équilibrer la charge entre les agents actifs du site.

Configurer le seuil d'inaccessibilité de l'agent et la notification

Si un agent est en panne ou n'est pas joignable pendant un certain temps, vous pouvez recevoir une notification sur son statut par e-mail, Slack, PagerDuty et ServiceNow. Dans **Infrastructure > Instances > Agents**, cliquez sur **Paramètres**, spécifiez la durée comprise entre 5 minutes et 60 minutes, puis sélectionnez la méthode de notification dont vous souhaitez être averti.



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

February 1, 2024

Le déploiement d'un agent NetScaler ADM en tant que microservice est utile pour gérer votre NetScaler CPX. Les procédures disponibles dans ce document s'appliquent uniquement si le cluster NetScaler 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 NetScaler ADM, accédez à **Infrastructure > Instances > 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**.

Installation de l'agent NetScaler ADM dans un cluster Kubernetes

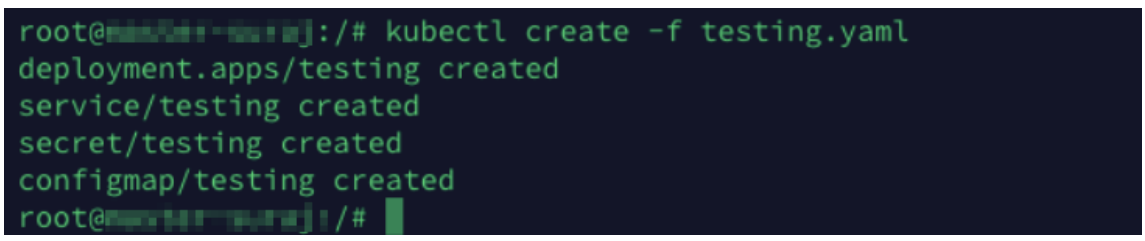
Dans le nœud principal de Kubernetes :

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 NetScaler ADM, accédez à **Infrastructure > Instances > Agents pour voir l'état** de l'agent.

Après avoir configuré l'agent, vous pouvez ajouter les instances NetScaler CPX et afficher les analyses dans Service Graph. Pour plus d'informations, consultez :

- Ajout d'instances NetScaler CPX àNetScaler ADM.
- Configuration d'un graphique de service.

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

February 1, 2024

Vous pouvez mettre à niveau votre serveur unique NetScaler ADM vers un déploiement haute disponibilité de deux serveurs NetScaler ADM. Une paire de serveurs NetScaler 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 NetScaler 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 NetScaler ADM vers une paire haute disponibilité, vous devez provisionner un nouveau nœud de serveur NetScaler ADM, le configurer en tant que deuxième serveur unique NetScaler ADM et déployer les deux serveurs NetScaler ADM en tant que paire haute disponibilité.

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

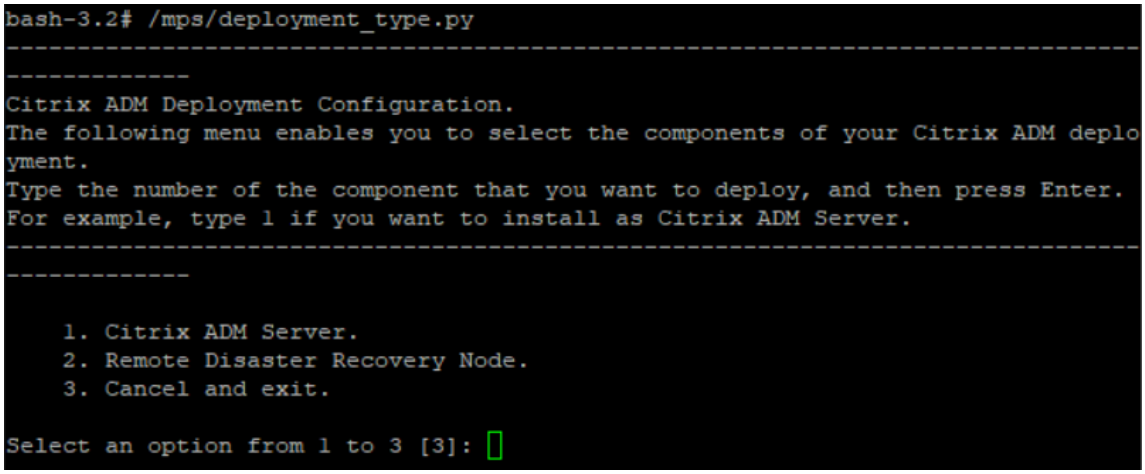
1. Modification du nœud de serveur existant
2. Provisioning du deuxième nœud de serveur
3. Déploiement des deux nœuds en mode HA
4. Configuration de la paire haute disponibilité

Modifier le nœud de serveur NetScaler ADM existant

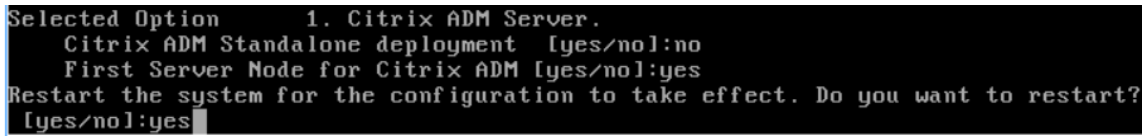
Pour migrer NetScaler ADM d'un serveur unique vers le mode haute disponibilité, vous devez modifier le type de déploiement initial du nœud de serveur en mode haute disponibilité.

1. Sur un poste de travail ou un ordinateur portable, ouvrez la console du nœud de serveur NetScaler ADM existant. Par exemple, considérez que vous avez déployé un NetScaler ADM avec l'adresse IP 10.106.171.17 en tant que serveur autonome.

2. Connectez-vous à NetScaler 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 comme serveur NetScaler 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 NetScaler.

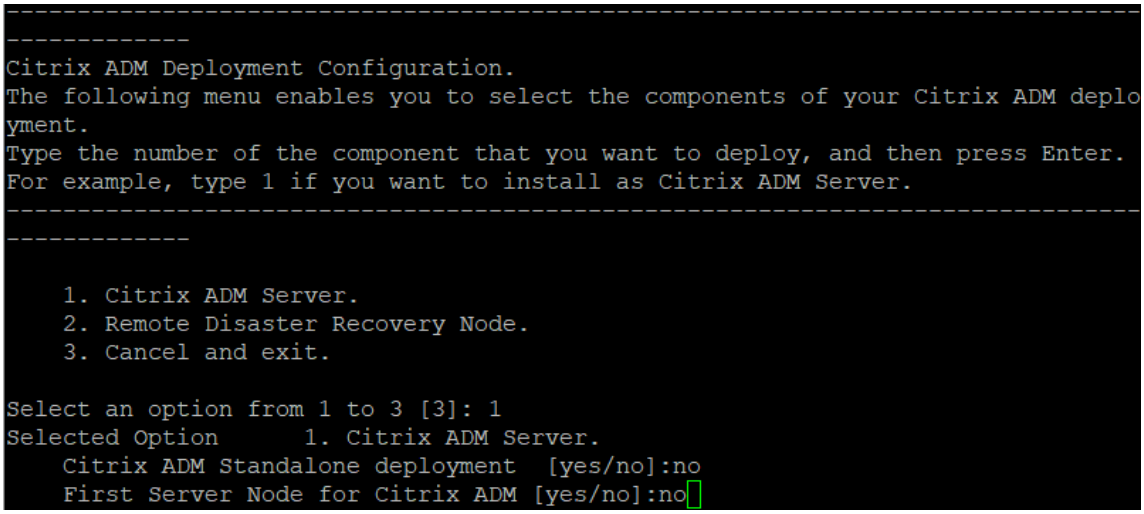
1. Importez le fichier image dans votre Hypervisor, puis, à partir de l'onglet Console, configurez les options de configuration réseau initiales comme expliqué sur l'écran suivant :


```
--------------------------------------------------------------------------------
Citrix ADM initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
--------------------------------------------------------------------------------
      1. Citrix ADM Host Name [CitrixADM]:
      2. Citrix ADM IPv4 address [10.102.29.211]:
      3. Netmask [255.255.255.0]:
      4. Gateway IPv4 address [10.102.29.1]:
      5. DNS IPv4 Address [127.0.0.2]:
      6. Cancel and quit.
      7. Save and quit.

Select a menu item from 1 to 7 [7]:
```

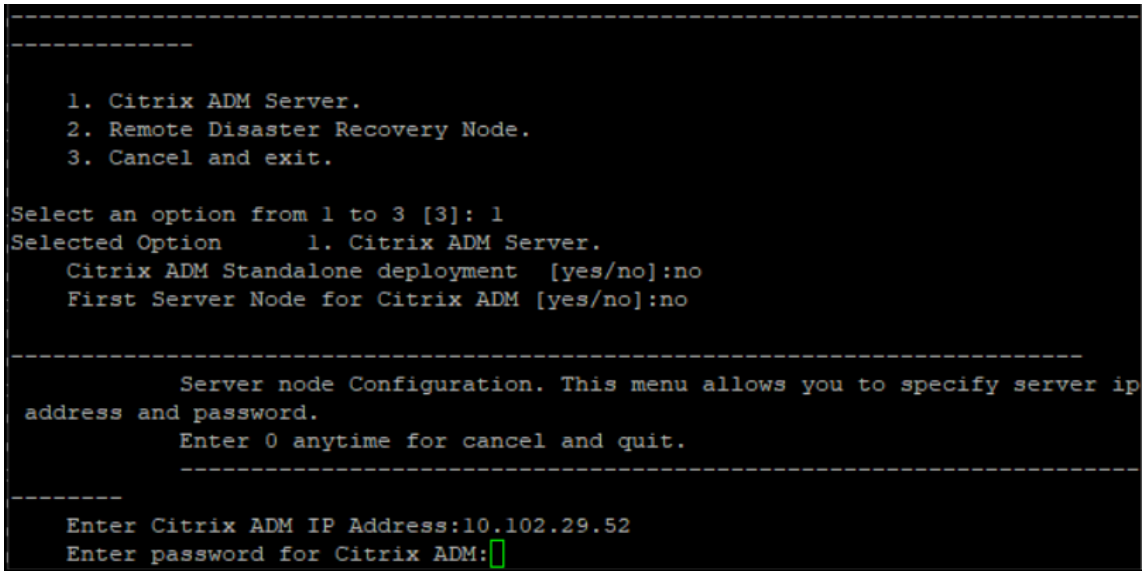
2. Après avoir spécifié les adresses IP requises, dans l'invite du shell, tapez /mps/deployment_type.py et appuyez sur Entrée.
3. Sélectionnez le type de déploiement comme serveur **NetScaler ADM.**
4. La console de déploiement vous invite à sélectionner le déploiement du serveur (en tant que serveur autonome). Tapez **Non** pour confirmer le déploiement comme paire haute disponibilité.

```
bash-3.2# /mps/deployment_type.py
--------------------------------------------------------------------------------
------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
--------------------------------------------------------------------------------
------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
    Citrix ADM Standalone deployment  [yes/no]:no
```

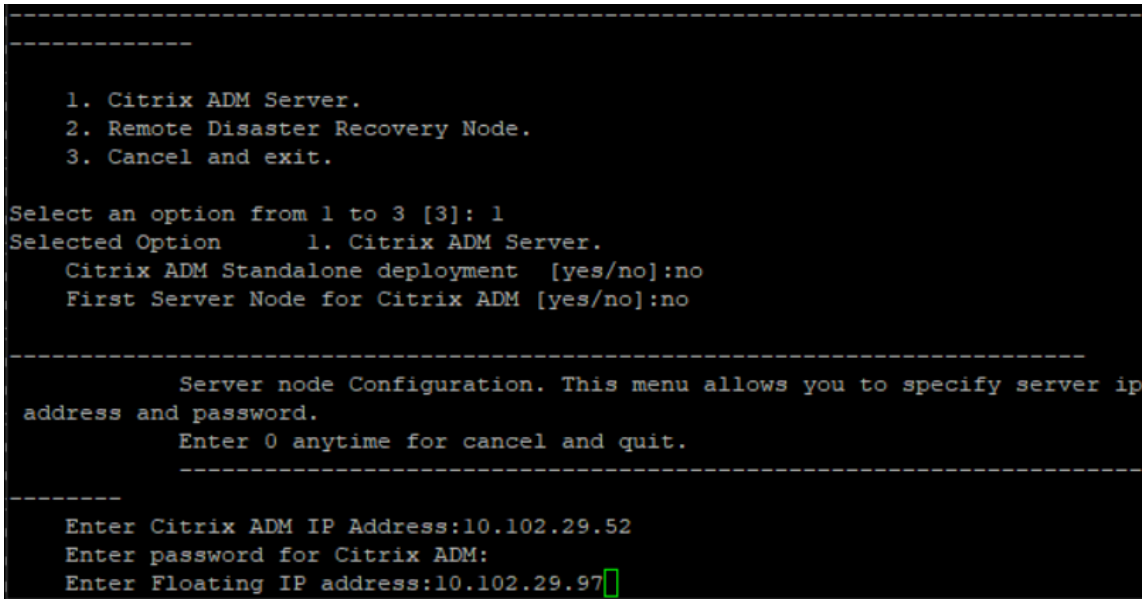
5. La console vous invite ensuite à sélectionner le (premier nœud de serveur). Tapez **Non** pour confirmer que le nœud est le deuxième nœud du serveur.



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 de haute disponibilité, vous devez déployer ces nœuds à partir de l'interface graphique du nœud de serveur NetScaler 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, saisissez l'adresse IP du nœud de serveur NetScaler 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 NetScaler 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 NetScaler ADM

February 1, 2024

Vous pouvez désormais migrer votre déploiement de NetScaler Insight Center vers NetScaler ADM sans perdre la configuration, les paramètres ou les données existants. Avec NetScaler ADM, vous pouvez non seulement consulter les différentes analyses générées par les instances NetScaler associées à une application, mais également gérer, surveiller et dépanner l'ensemble de l'infrastructure mondiale de diffusion d'applications à partir d'une console unique et unifiée.

> **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 NetScaler ADM, vérifiez que les conditions suivantes sont remplies :

- NetScaler Insight Center 11.1 Build 47.14 ou version ultérieure est installé.
- Vous avez téléchargé le fichier image NetScaler ADM 12.0 build 57.24 .tgz.

  > **Remarque**
  >
  > Vous devez installer NetScaler ADM 12.0 build 57.24, puis effectuer la mise à niveau vers la dernière version de NetScaler ADM 13.1. Pour plus d'informations, consultez la section Mettre à niveau.

- Vous avez téléchargé le fichier image .tgz de la dernière version de NetScaler ADM 13.1.

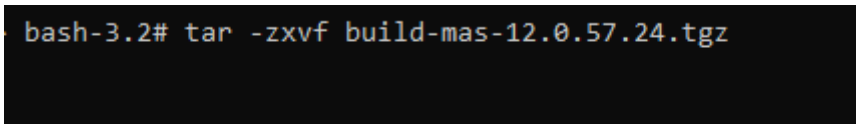
Exigences matérielles

Composant	Exigences
RAM	32 GB
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 pour les déploiements NetScaler 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 NetScaler ADM :

1. Connectez-vous à l'invite shell de NetScaler Insight Center.
2. Téléchargez le NetScaler ADM 12.0 build 57.24 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**.



4. Installez NetScaler ADM à l'aide de la commande **./installmas**.

5. Après avoir installé NetScaler ADM 12.0 build 57.24, vous devez effectuer une mise à niveau vers la dernière version de NetScaler ADM 13.1 en suivant les étapes ci-dessus.

Après la migration, toutes les instances NetScaler découvertes dans l'inventaire de NetScaler Insight Center apparaissent dans la section **Infrastructure > Instances de NetScaler** ADM. Toutefois, pour la première fois, vous devez interroger manuellement les serveurs virtuels hébergés dans les appliances découvertes.

> **Remarque**
>
> Dans NetScaler ADM, par défaut, la gestion et la surveillance de deux serveurs virtuels créés au sein des instances NetScaler découvertes sont gratuites. Pour surveiller et gérer plus de deux serveurs virtuels, installez les licences NetScaler ADM requises. Pour plus de détails, consultez la section LicencesNetScaler ADM.

Intégrez NetScaler ADM à Citrix Director

February 1, 2024

Director s'intègre à NetScaler ADM pour l'analyse du réseau et la gestion des performances.

- L'analyse du réseau permet d'obtenir des rapports HDX Insight auprès de NetScaler ADM et fournit une vue du réseau sur les applications et les ordinateurs de bureau. 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.

Après avoir intégré NetScaler 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 NetScaler 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 NetScaler ADM.
Interfaces réseau virtuelles	1
Débit	1 Gbit/s ou 100 Mbit/s

Exigences minimales

Avant de configurer l'intégration réseau, assurez-vous de créer un utilisateur RBAC avec accès à HDX Insights.

Configuration logicielle requise

Avant de migrer vers l'appliance virtuelle NetScaler ADM, vérifiez que les conditions suivantes sont remplies :

- La version 1811 de Director est installée
- NetScaler HDX Insight version 10.1 ou ultérieure est installé
- HDX Insight et NetScaler ADM prennent en charge les versions 7.0 et ultérieures de Citrix VDA
- Citrix Workspace est pris en charge sur Citrix Virtual Apps and Desktops version 7.0 et ultérieure
- Assurez-vous que MAC Citrix Workspace pour Mac version 11.8 et versions ultérieures, et Windows Citrix Workspace pour Windows 14.0 et versions ultérieures sont disponibles pour afficher des métriques ICA RTT précises.
- Les versions 11.0 et ultérieures de NetScaler ADM sont installées. Pour plus d'informations sur l'installation de NetScaler ADM, voir DéployerNetScaler ADM.

Limitations

- La disponibilité de cette fonctionnalité dépend de la licence de votre organisation et vos permissions d'administrateur.

- La session ICA Round Trip Time (RTT) affiche correctement les données pour Citrix Workspace pour Windows 3.4 ou version ultérieure et pour Citrix Workspace pour Mac 11.8 ou version ultérieure. Pour les versions précédentes de ces espaces de travail, 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 connaître les étapes permettant d'intégrer NetScaler ADM à Director, consultez https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/director/install-and-configure/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.

Connecter un disque supplémentaire à NetScaler ADM

February 1, 2024

Les besoins de stockage de NetScaler Application Delivery Management (ADM) sont déterminés en fonction de l'estimation de la taille de NetScaler ADM. Par défaut, NetScaler 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.
> - Pour un déploiement NetScaler ADM sur un seul serveur, vous ne pouvez associer qu'un seul disque au serveur en plus du disque par défaut.
> - Pour un déploiement haute disponibilité de NetScaler ADM, vous devez associer un disque supplémentaire à chaque nœud. La taille des deux disques doit être identique.
> - S'il existe un disque externe de capacité inférieure, vous devez le retirer avant d'en connecter un nouveau.
> - Nous recommandons d'utiliser la technologie SSD (Solid-State Drive) pour les dé-

> ploiements NetScaler 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. Connecter un disque supplémentaire dans un NetScaler ADM autonome
2. Lancez l'outil de partition de disque
3. Créez des partitions sur le nouveau disque supplémentaire
4. Redimensionner les partitions du disque supplémentaire existant
5. Supprimez les partitions du disque supplémentaire

Connecter un disque supplémentaire dans un NetScaler ADM autonome

1. Arrêtez la machine virtuelle NetScaler ADM.
2. Dans l'hyperviseur, connectez un disque supplémentaire de la taille requise à la machine virtuelle NetScaler ADM.

   Le disque plus grand qui vient d'être connecté stocke les données de la base de données et les fichiers journaux NetScaler ADM. Le disque par défaut existant de 120 Go est désormais utilisé pour stocker les fichiers principaux, les fichiers journaux du système d'exploitation, etc.
3. Démarrez la machine virtuelle NetScaler ADM.

Lancez l'outil de partition de disque

NetScaler ADM fournit désormais l'outil de **partition de disque NetScaler ADM, un nouvel outil**de ligne de commande.

1. À l'aide de l'outil, vous pouvez créer des partitions dans le disque supplémentaire nouvellement ajouté.
2. Vous pouvez également redimensionner les disques supplémentaires existants à l'aide de l'outil. Mais le disque externe existant ne doit pas dépasser 2 téraoctets.

   > **Remarque :**
   >
   > - Le redimensionnement des disques existants au-delà de 2 téraoctets peut entraîner une perte 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 NetScaler ADM. Vous ne pouvez pas créer de partitions sur le disque principal (par défaut) à l'aide de cet outil.

Pour lancer l'outil de partition de disque :

1. Ouvrez une connexion SSH à NetScaler ADM à l'aide d'un client SSH, tel que PuTTY.
2. Connectez-vous à NetScaler ADM à l'aide des informations d'identification. `nsrecover`/`nsroot`
3. Passez à l'invite shell et tapez :

```
/mps/DiskPartitionTool.py
<!--NeedCopy-->
```

```
bash-3.2# /mps/DiskPartitionTool.py

-------------------------------------
MAS/SVM Disk Partition Tool (DPT) 1.0
-------------------------------------
Welcome to MAS/SVM DPT! Type 'help' or '?' to view a list of commands.

(dpt):
```

> **Remarque :**
>
> Pour NetScaler ADM dans le cadre d'un déploiement à haute disponibilité, vous devez lancer l'outil sur les deux nœuds et créer ou redimensionner des partitions après avoir associé 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 ».

```
(dpt): ?create
Creates a new partition on the attached disk. A swap partition of size 32GB is also created automatically.

The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```


> **Remarque :**
>
> Il n'y a aucune limite de taille de 2 téraoctets lors de la création de partitions à l'aide de 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 l'interrompre.

```
(dpt): create

The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to continue (Y/N): y
```

```
Creating GPT partition scheme...
da1 created

Creating partition 1 using (456287933) blocks. Leaving aside 32G for swap...
da1p1 added

Creating partition 2 for swap using remaining 32G...
da1p2 added

Formatting the new partition. This may take some time (~20 seconds). Please be patient and don't interrup the process...
```

Une fois la commande create terminée, la machine virtuelle est automatiquement redémarrée pour que la nouvelle partition soit montée.

```
Create Done.
VM has to be rebooted for the new partition to be used.
Rebooting VM now...

*** FINAL System shutdown message from nsroot@ns-mgmt-system ***

System going down IMMEDIATELY
```

Après le redémarrage, la nouvelle partition est montée sur /var/mps.


```
bash-3.2# df -k
Filesystem  1024-blocks     Used     Avail Capacity  Mounted on
/dev/md0         456046   374346     72580    84%    /
devfs                 1        1         0   100%    /dev
procfs                4        4         0   100%    /proc
fdescfs               1        1         0   100%    /dev/fd
/dev/da0s1a     1623950   284466   1209568    19%    /flash
/dev/da0s1e   116073918 2812298 103975708     3%    /var
/dev/da1p1    495168802   43854 455511444     0%    /var/mps
```

La partition swap ajoutée apparaît sous forme d'espace swap dans la sortie de la commande « create ».

```
CPU:  0.0% user,  0.0% nice,  0.0% system,  0.7% interrupt, 99.3% idle
Mem: 89M Active, 21M Inact, 123M Wired, 16M Cache, 74M Buf, 6965M Free
Swap: 37G Total, 37G Free
```

> **Remarque :**
>
> L'outil redémarre la machine virtuelle une fois la partition créée.

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.

> **Remarque :**
>
> - La commande `resize` est conçue pour fonctionner sans perte de données existantes. Nous vous recommandons toutefois de sauvegarder les données critiques de ce disque sur un stockage externe avant de le redimensionner. 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 lors du redimensionnement des partitions. Une augmentation progressive de ce type garantit que vous n'aurez pas à redimensionner plus fréquemment.


```
(dpt): ?resize
Resizes existing partition on attached disk to utilize all space available. Pre-conditions are:
1. Secondary disk exists and capcity of disk < 2TB
2. A single partition exists on secondary disk and there is atleast 100GB to gain by resizing

********************
***  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.
```

La commande `resize` vérifie toutes les conditions préalables et poursuit si toutes les conditions préalables sont remplies et après que vous ayez donné votre accord pour le redimensionnement. Il arrête les processus accédant au disque, notamment les sous-systèmes NetScaler ADM, les processus de base de données PostgreSQL et le processus de surveillance NetScaler 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. Veillez à ne pas interrompre le processus pendant qu'il est en cours. L'outil redémarre la machine virtuelle après avoir redimensionné la partition.

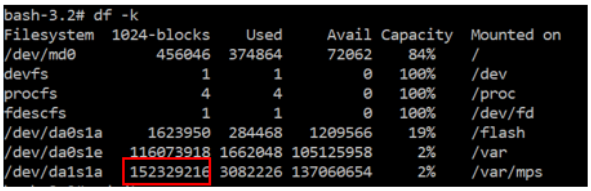
```
(dpt): resize

********************
***  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...
```

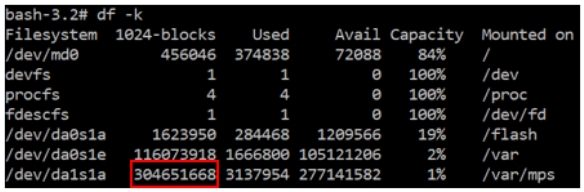
Toutes les étapes intermédiaires du processus de redimensionnement (arrêt des applications, redimensionnement du disque, croissance du système de fichiers) sont affichées sur la console. Une fois le processus terminé, le message suivant s'affiche.


```
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 lorsque vous augmentez 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. Ce problème 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.

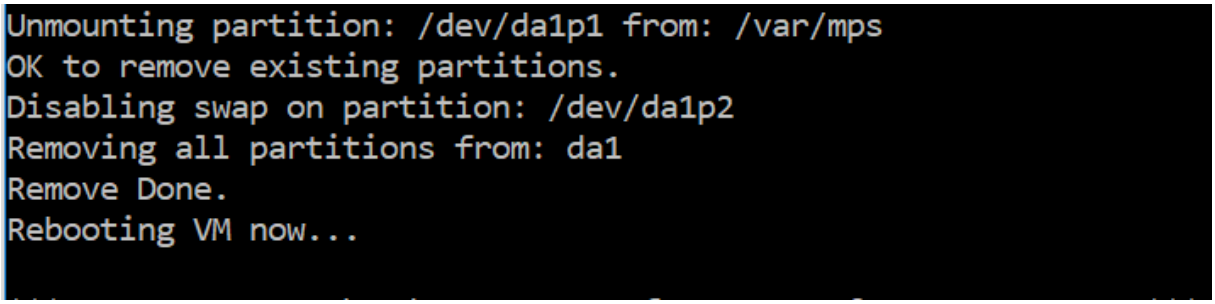
> **Remarque :**
>
> la suppression de la partition existante supprime toutes les données existantes. Par conséquent, toutes les données critiques doivent être sauvegardées sur un stockage externe avant d'utiliser cette commande.

```
(dpt): ?remove
Removes existing partition from attached disk.

********************
***  WARNING !!  ***
********************
All data on the partition/disk will be PERMANENTLY ERASED as a result of this operation.
Backup the data before proceeding with this operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

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 les moniteurs ADM) utilisant le disque secondaire. Si une partition de swap existe et que le swap est activé sur la partition, le swap est désactivé.


```
(dpt): remove

********************
***  WARNING !!  ***
********************
All data on the partition/disk will be PERMANENTLY ERASED as a result of this operation.
Backup the data before proceeding with this operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to continue (Y/N): y
```

Lorsque vous tapez « y », la commande démonte le disque et supprime toutes les partitions du disque.



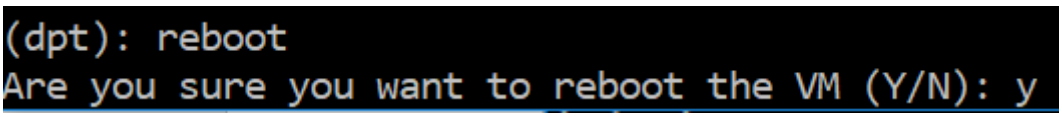
> **Remarque :**
>
> L'outil redémarre la machine virtuelle une fois que vous avez supprimé la partition.

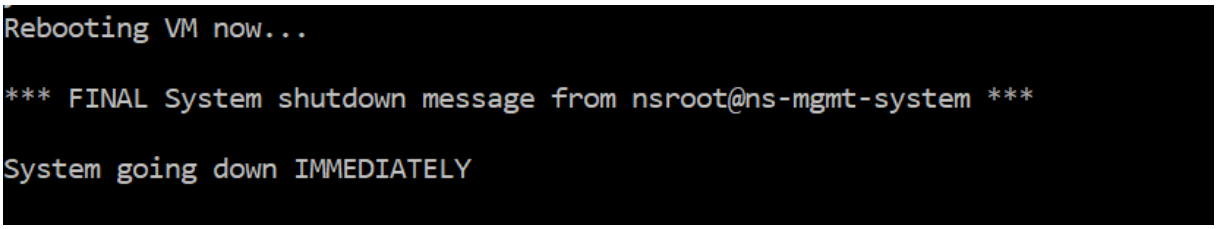
Redémarrez la machine virtuelle

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 après confirmation, tous les processus (tels que les sous-systèmes ADM, les processus PostgreSQL et les moniteurs ADM) sont arrêtés. La machine virtuelle est ensuite redémarrée.





Créer un fichier de sauvegarde des données du disque

> **Remarque :**
>
> la création d'un fichier de sauvegarde nécessite de l'espace disque. Assurez-vous que l'espace disque est suffisant (50 % ou plus) avant d'exécuter les commandes de sauvegarde.

Pour sauvegarder les données NetScaler ADM avant de redimensionner ou de supprimer les partitions :

1. Arrêtez ADM.

```
/mps/masd stop
<!--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. Générez un checksum.

```
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.

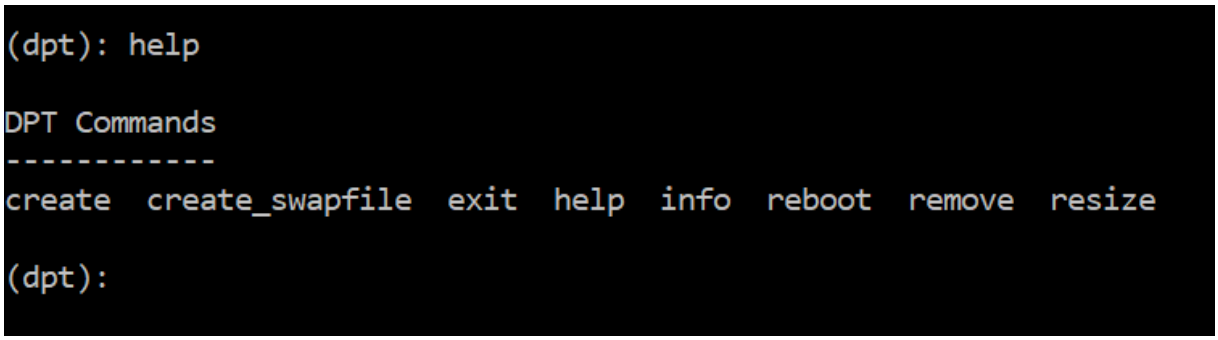
```
cd /var/mps/
rm mps_backup.tgz  mps_backup_checksum
<!--NeedCopy-->
```


Commandes supplémentaires

Outre les commandes répertoriées précédemment, vous pouvez également utiliser les commandes suivantes dans l'outil :

Commande d'aide :

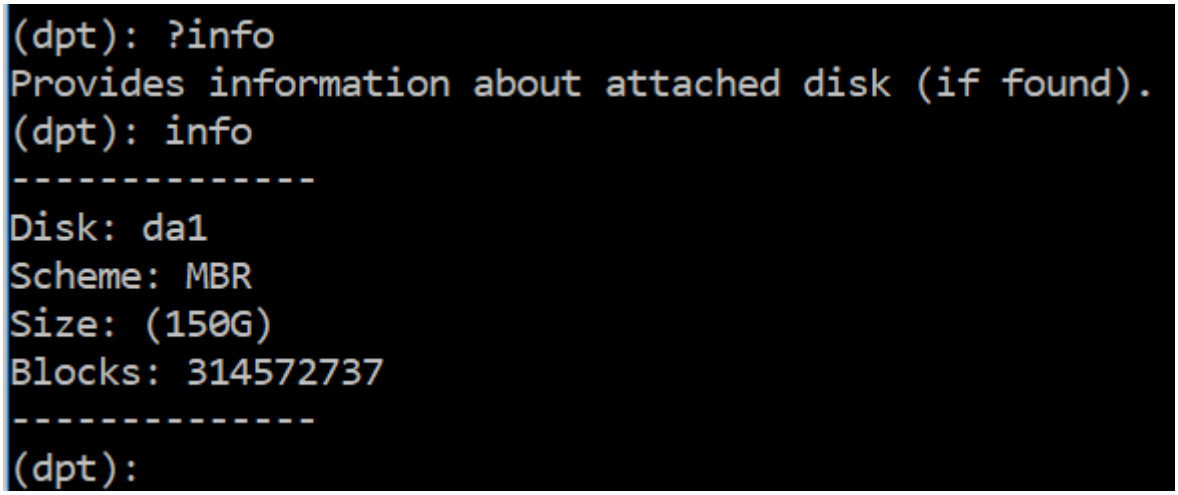
Pour répertorier les commandes prises en charge, tapez **help** ou **?** et appuyez sur Entrée. Pour obtenir de l'aide supplémentaire sur chacune des commandes, appuyez sur **Aide** ou **?** suivi du nom de la commande et appuyez sur la touche **Entrée** .



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 NetScaler 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 NetScaler ADM 12.1 ou version ultérieure.

> **Remarque :**
>
> Une partition GPT peut avoir une taille supérieure à 2 téraoctets, sauf 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. Ce problème est une limitation connue de la plateforme.



Commande Create_SWAPFile :

La partition de swap par défaut sur le disque principal de NetScaler ADM est de 4 Go. L'espace d'échange par défaut est donc de 4 Go. Pour la configuration de mémoire par défaut de NetScaler ADM qui est de 2 Go, cet espace de swap est suffisant. Toutefois, lorsque vous exécutez NetScaler ADM avec une configuration de mémoire plus élevée, vous devez disposer d'un espace de swap plus important sur le disque.

> **Remarque :**
>
> La partition d'échange est généralement une partition dédiée créée sur un disque dur (HDD) lors de l'installation du système d'exploitation. Une telle partition est également appelée espace de permutation. Une partition d'échange est utilisée pour la mémoire virtuelle qui simule la mémoire principale supplémentaire.

Les disques secondaires ajoutés dans les versions précédentes de NetScaler ADM ne comportent pas de partition de swap créée par défaut. La commande « create_swapfile » est destinée aux disques secondaires créés à l'aide d'anciennes versions de NetScaler ADM qui ne possèdent pas de partition de swap. 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

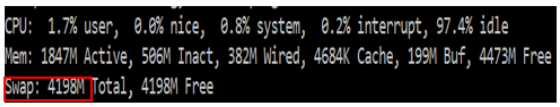
La commande `create_swapfile` n'est utile que lorsque la mémoire est supérieure ou égale à 16 Go et non lorsque la mémoire est faible. Ainsi, cette commande vérifie également la mémoire avant de procéder à la création du fichier d'échange.

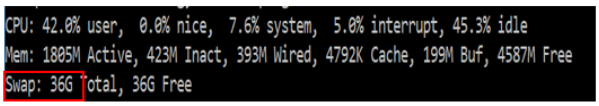

```
(dpt): ?create_swapfile
Creates a 32GB swap file on the secondary disk. Pre-conditions are:
1. Secondary disk exists
2. Secondary disk is partitioned and mounted
3. Capacity of disk >= 500GB
4. Swap file is not already found
5. RAM size >= 16GB

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 accepte de 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**.

```
(dpt): exit
bash-3.2#
```

Connectez des disques supplémentaires à NetScaler ADM déployé en haute disponibilité

Supposons que vous ayez configuré deux serveurs NetScaler ADM dans une configuration haute disponibilité sans aucun disque secondaire. Supposez également que vous avez ajouté 2 instances NetScaler 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. Arrêtez le nœud secondaire.
2. Ajoutez un disque via l'hyperviseur.

   > **Remarque :**
   >
   > Veillez à ne pas étendre le disque principal du nœud secondaire.

3. Démarrez le nœud secondaire.
4. Exécutez l'outil de partition sur le nœud secondaire.
5. Une fois le disque ajouté, le nœud secondaire redémarre.
6. Arrêtez le nœud secondaire après son redémarrage.
7. Arrêtez le nœud principal.
8. Ajoutez un disque via l'hyperviseur.

   > **Remarque :**
   >
   > Veillez à ne pas étendre le disque principal du nœud principal.

9. Démarrez le nœud principal.
10. Exécutez l'outil de partition sur le nœud principal.
11. Une fois le disque ajouté, le nœud principal redémarre.
12. Une fois que le nœud principal est opérationnel, démarrez le nœud secondaire.
13. Assurez-vous que le nœud secondaire est opérationnel et que les bases de données sont synchronisées.
14. 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 de l'ADM_Primary, vérifiez s'il s'agit du nœud principal.
5. Démarrez le nœud ADM_Secondary. Après son redémarrage, assurez-vous qu'il est apparu comme secondaire et que la synchronisation de la base de données fonctionne.

6. Confirmez 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.

Cloud Connector ADM sur site

February 1, 2024

Vous pouvez utiliser la fonctionnalité ADM On-Prem Cloud Connector pour établir une connexion entre ADM On-Prem et le service NetScaler Console.

> **Remarque :**
>
> Le service NetScaler ADM est désormais renommé en service NetScaler Console. L'interface utilisateur et la documentation de nos produits font actuellement l'objet de mises à jour pour refléter ces modifications. Pendant cette période, vous pouvez rencontrer les noms les plus anciens et les plus récents référencés de manière interchangeable. Nous vous remercions de votre compréhension durant cette transition.

Cette connectivité vous permet de sélectionner la fonctionnalité suivante à utiliser dans ADM On-Prem :

Avis de sécurité —L'avis de sécurité prend en charge l'identification automatique des NetScaler vulnérables et fournit les avantages du flux de travail de correction. L'avis de sécurité vous permet de suivre les nouvelles vulnérabilités et expositions courantes (CVE), d'évaluer l'impact des CVE, de comprendre les mesures correctives et de résoudre les vulnérabilités. En tant qu'administrateur, vous pouvez surveiller les instances NetScaler pour détecter tout nouveau CVE par le biais d'une analyse périodique ou manuelle, et prendre les mesures nécessaires pour la correction. Pour plus d'informations, consultez l'avis de sécurité.

Collectetélémétrique automatisée —Si vous utilisez une licence Flexed, nous vous recommandons d'activer Cloud Connector, qui est le mode automatique de collecte des données de télémétrie. Pour plus d'informations, consultez la section Licence de capacité flexible .

> **Remarques :**
>
> - Il n'est pas nécessaire d'ajouter ou de migrer les instances NetScaler vers le service

> NetScaler Console.
>
> - ADM On-Prem Cloud Connector nécessite que vous vous connectiez au service NetScaler Console en configurant un compte de service NetScaler Console (s'il n'est pas déjà créé).
> - À partir de la version 14.1 8.x, ADM On-Prem Cloud Connector remplace la fonctionnalité Customer Identity.
> - Une fois que vous avez configuré ADM On-Prem Cloud Connector, Citrix Cloud peut collecter les données de licence, de configuration et d'utilisation à des fins de conformité des licences et de gérer, mesurer et améliorer le service. Pour plus d'informations, consultez la section Gouvernance des données.

Conditions préalables

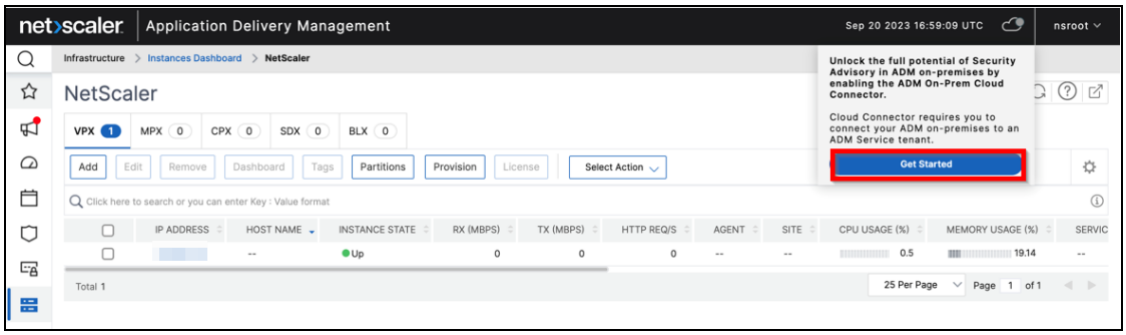
Avant de configurer ADM On-Prem Cloud Connector, assurez-vous de remplir les conditions préalables suivantes :

- Assurez-vous de disposer d'une connexion Internet ou d'un serveur proxy configuré dans ADM sur site pour l'accessibilité de Citrix Cloud.
- Assurez-vous que l'accès aux URL des points de terminaison suivants est autorisé :
  - Service de téléchargement : `https://download.citrixnetworkapi.net`
  - Service de confiance : `*.citrixnetworkapi.net`
  - URL des services
    - `*.agent.adm.cloud.com`
    - `*.adm.cloud.com`
    - `adm.cloud.com`
  - Connectivité Citrix Cloud :
    - `Citrix.cloud.com`
    - `Accounts.cloud.com`
- Assurez-vous d'avoir désactivé le bloqueur de fenêtres contextuelles dans le navigateur à partir duquel vous accédez à l'interface graphique ADM sur site.

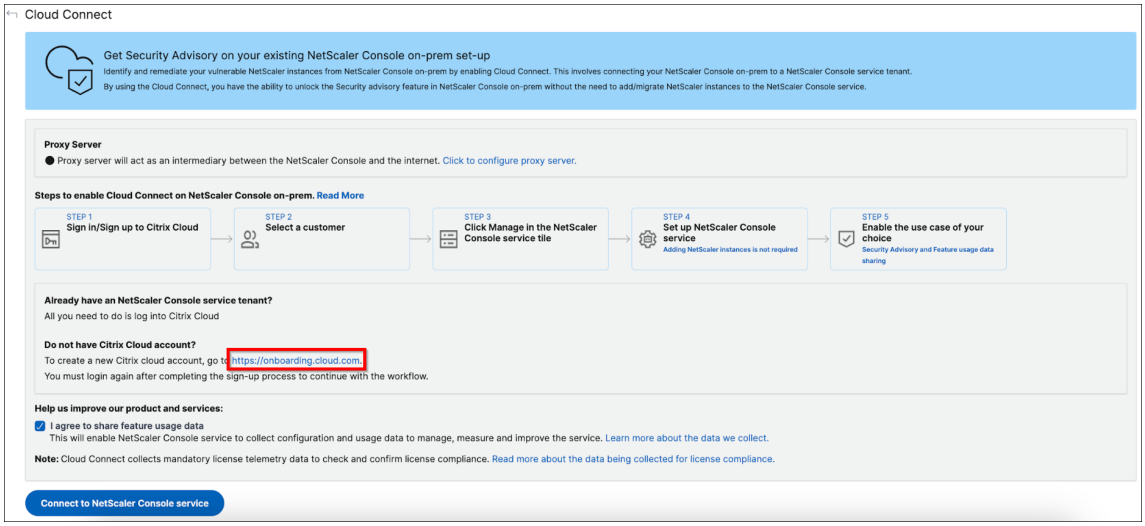
Configuration du Cloud Connector ADM On-Prem

Workflow 1 : si vous êtes un nouvel utilisateur sans compte Citrix Cloud ni locataire du service NetScaler Console

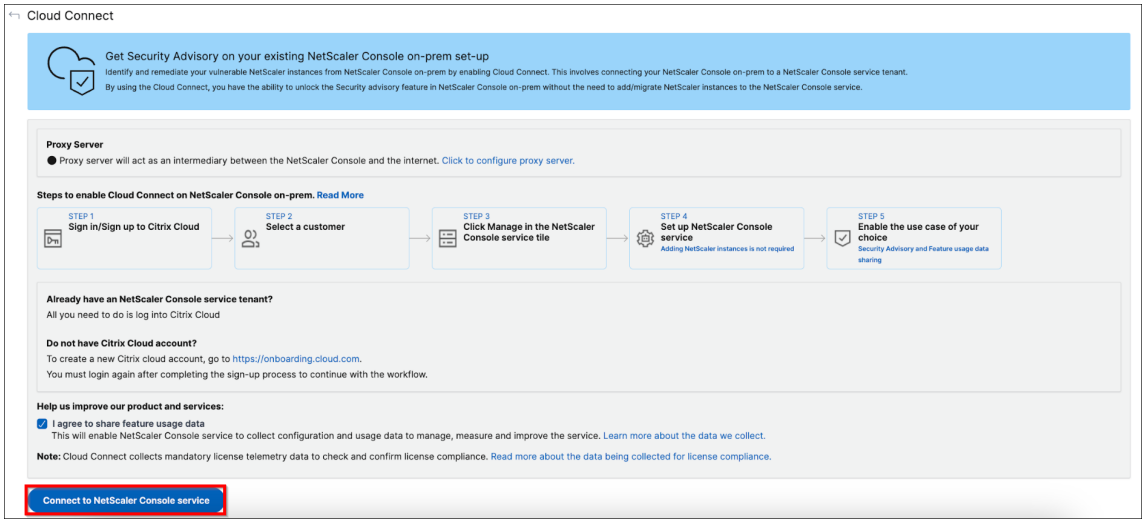
1. **Dans NetScaler ADM, cliquez sur l'icône Cloud >**Commencer**.**



2. Sur la page de configuration d'ADM On-Prem Cloud Connector, cliquez sur le lien. `https://onboarding.cloud.com`



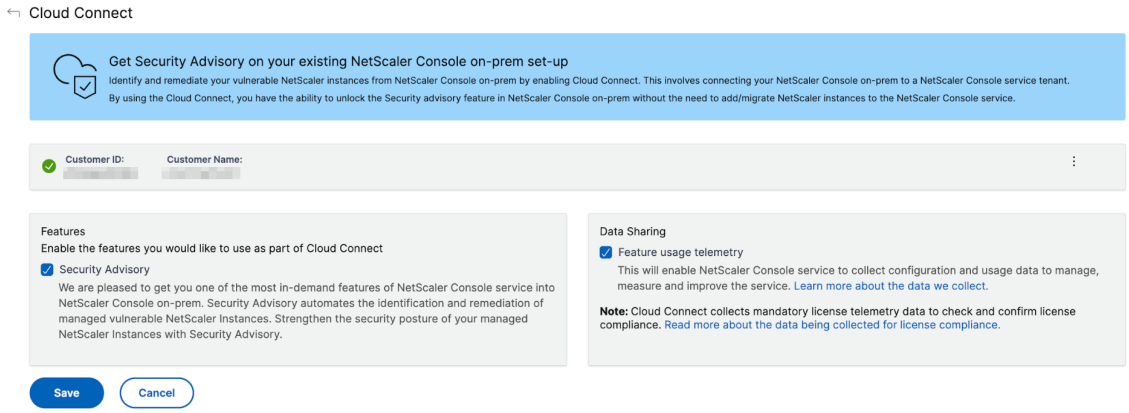
3. Suivez la procédure décrite dans ce document pour créer un compte Citrix Cloud.
4. Après avoir créé un compte Citrix Cloud, vous devez vous reconnecter en cliquant sur **Se connecter au service NetScaler Console** dans NetScaler ADM . Une fois la connexion établie, la page est redirigée vers les étapes de création du locataire du service NetScaler Console.



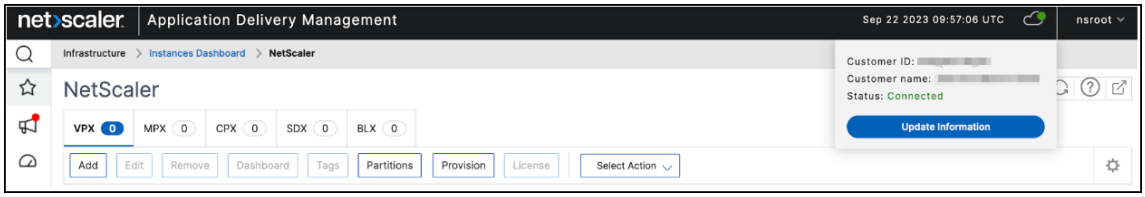
5. Sélectionnez la région qui répond aux besoins de votre entreprise et cliquez sur **OK** .
6. Sélectionnez un rôle et terminez la configuration.

   La fin de la configuration peut prendre quelques minutes. Dans ADM, vous pouvez voir que l'écran d'**activation du connecteur ADM On-Prem Cloud** est en cours. Vous pouvez soit cliquer sur **Actualiser** et attendre de voir apparaître la page de configuration mise à jour, soit cliquer sur **Annuler** pour ignorer cet écran et vérifier ultérieurement la présence de la page de configuration mise à jour.

7. La configuration du Cloud Connector ADM On-Prem est terminée. Vous pouvez continuer pour activer l'avis de sécurité sur la page de configuration d'ADM On-Prem Cloud Connector.
8. Sélectionnez l'**avis de sécurité** et cliquez sur **Enregistrer**.

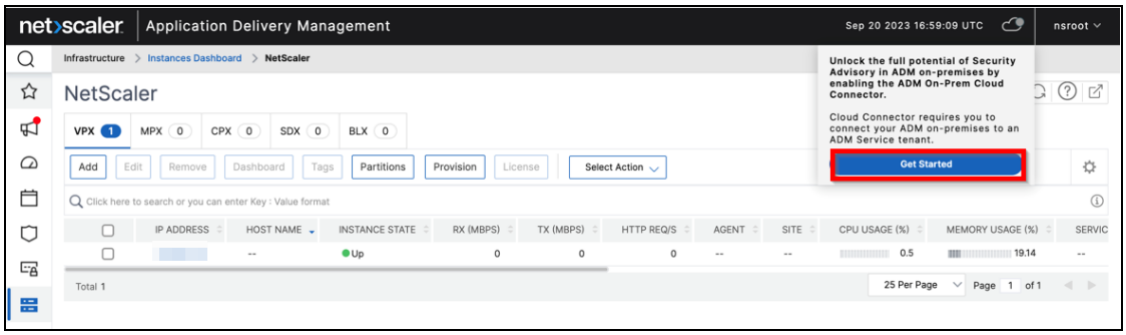


Vous pouvez voir l'état comme étant connecté.

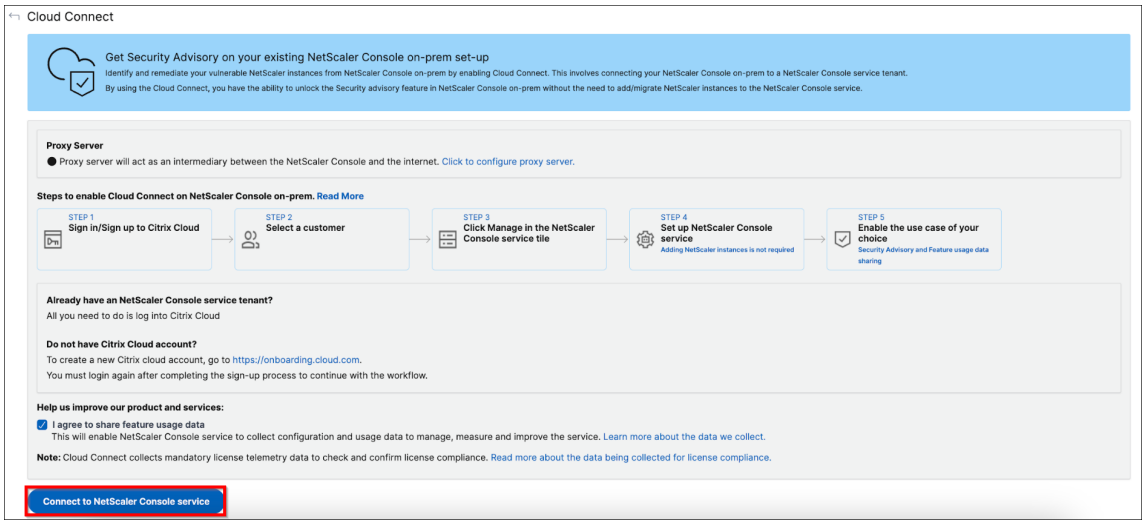


Workflow 2 : si vous possédez un compte Citrix Cloud mais que vous ne possédez pas de locataire de service NetScaler Console

1. **Dans NetScaler ADM, cliquez sur l'icône Cloud >**Commencer**.**



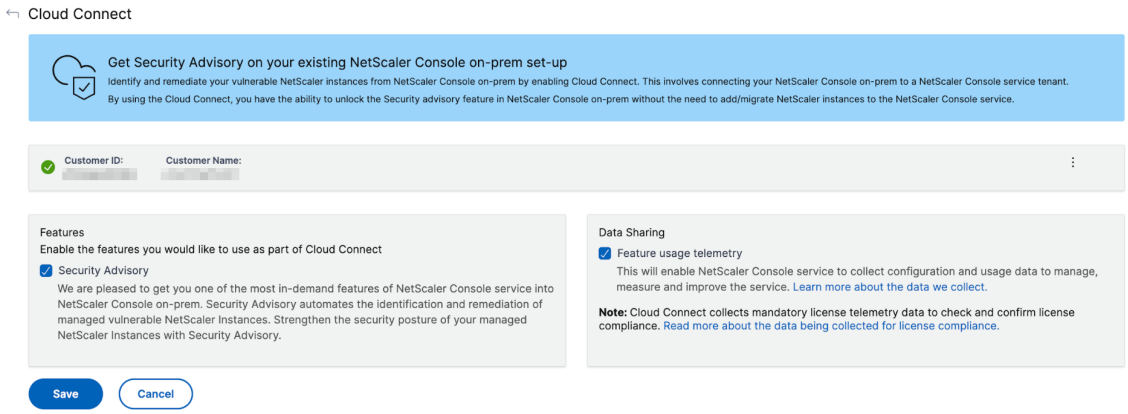
2. Cliquez sur **Se connecter au service NetScaler Console** .



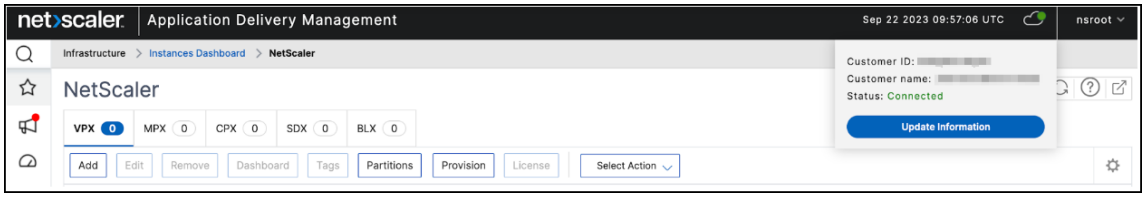
3. Vous allez être redirigé vers un nouvel onglet. Connectez-vous à Citrix Cloud.
4. Une fois que vous avez reçu le message de connexion réussie, la page est redirigée vers les étapes d'intégration d'ADM.
5. Sélectionnez une région qui répond aux besoins de votre entreprise et cliquez sur OK.
6. Sélectionnez un rôle et terminez la configuration.

La fin de la configuration peut prendre quelques minutes. Dans ADM, vous pouvez voir que l'écran d'**activation du connecteur ADM On-Prem Cloud** est en cours. Vous pouvez soit cliquer sur **Actualiser** et attendre de voir apparaître la page de configuration mise à jour, soit cliquer sur **Annuler** pour ignorer cet écran et vérifier ultérieurement la présence de la page de configuration mise à jour.

7. La configuration du Cloud Connector ADM On-Prem est terminée. Vous pouvez continuer pour activer l'avis de sécurité sur la page de configuration d'ADM On-Prem Cloud Connector.
8. Sélectionnez l'**avis de sécurité** et cliquez sur **Enregistrer**.

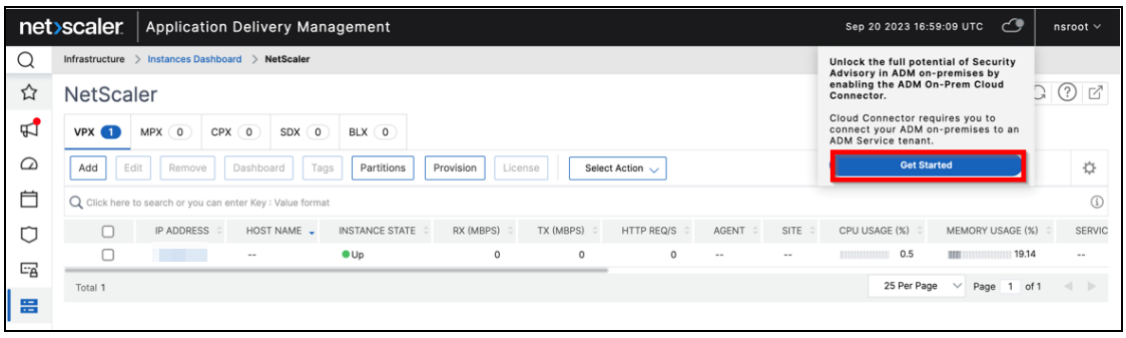


Vous pouvez voir l'état comme étant connecté.

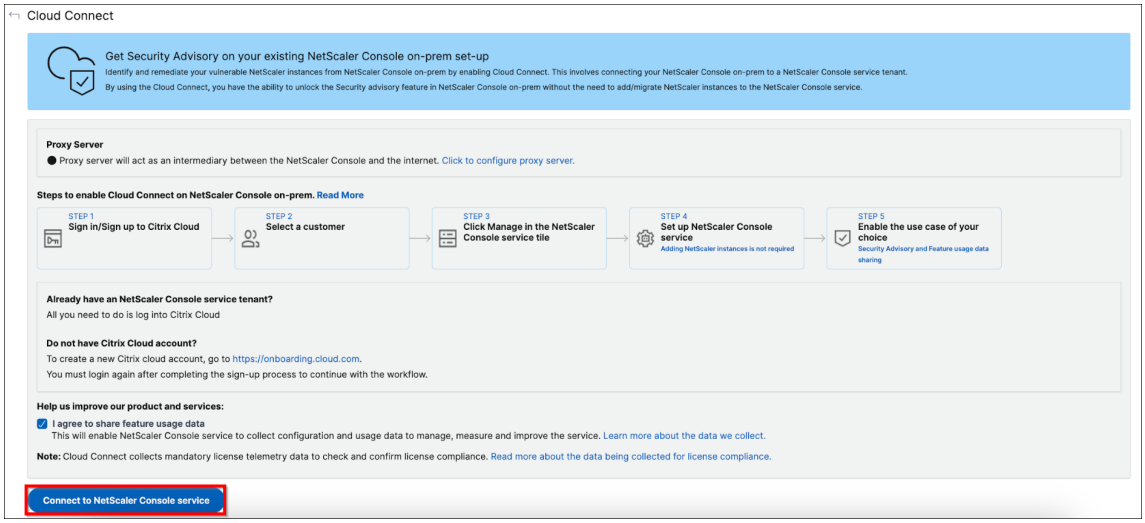


Workflow 3 : si vous êtes déjà un utilisateur disposant à la fois d'un compte Citrix Cloud et d'un locataire du service NetScaler Console

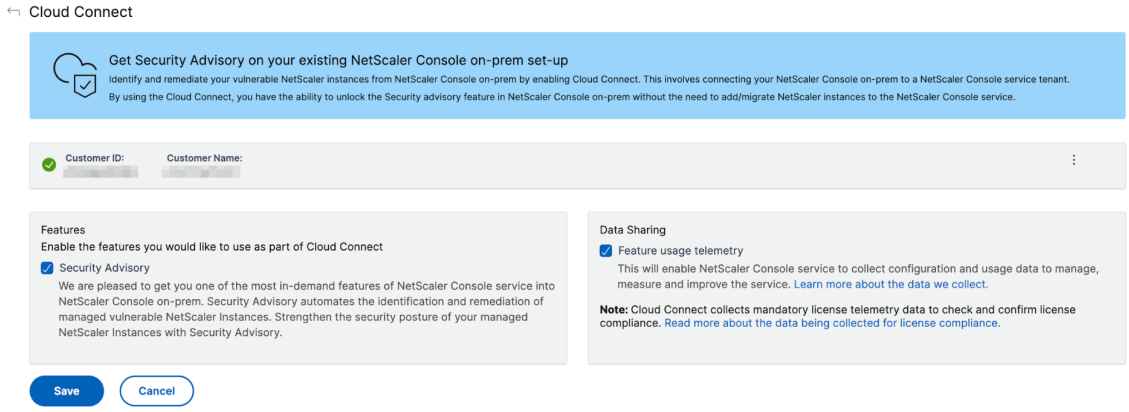
1. **Dans NetScaler ADM, cliquez sur l'icône Cloud >**Commencer**.**



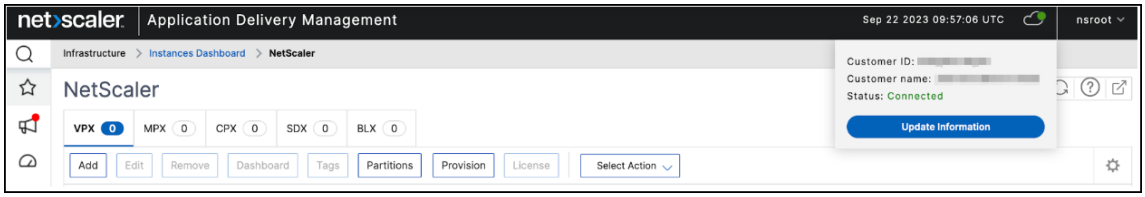
2. Cliquez sur **Se connecter au service NetScaler Console** .



3. Vous allez être redirigé vers un nouvel onglet. Connectez-vous à Citrix Cloud et sélectionnez un locataire. Après avoir sélectionné le locataire, vous recevez un message de connexion réussie.
4. La configuration du Cloud Connector ADM On-Prem est terminée. Vous pouvez continuer pour activer l'avis de sécurité sur la page de configuration d'ADM On-Prem Cloud Connector.
5. Sélectionnez l'**avis de sécurité** et cliquez sur **Enregistrer**.



Vous pouvez voir l'état comme étant connecté.



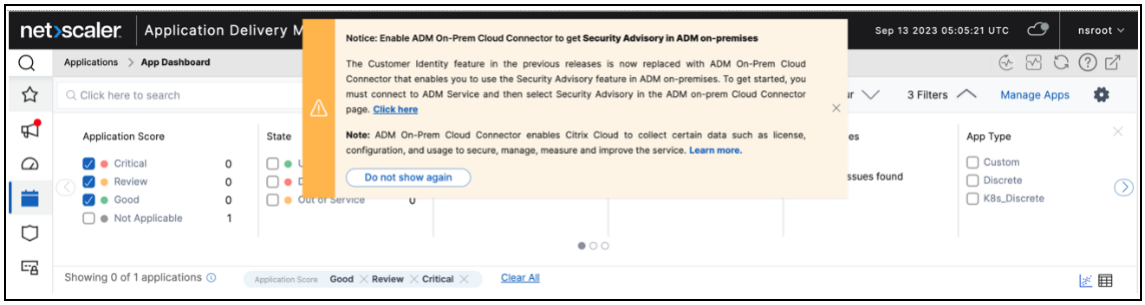
Que se passe-t-il si l'identité du client est déjà activée ?

Si vous utilisez déjà une version antérieure avec Customer Identity activée, que vous avez sélectionné le partage de données et que vous avez effectué la mise à niveau vers la dernière version (14.1 8.x), les

scénarios suivants sont applicables :

- Si vous disposez d'un locataire du service NetScaler Console, ADM On-Prem Cloud Connector est automatiquement activé dans votre ADM sur site. Il permettra à Citrix Cloud de collecter des données de licence, de configuration et d'utilisation pour gérer, mesurer et améliorer le service. Pour plus d'informations, consultez la section Gouvernance des données. Sur la page de configuration du Cloud Connector, vous pouvez sélectionner **Security Advisory** pour utiliser cette fonctionnalité.

  La notification suivante apparaît si ADM On-Prem Cloud Connector est automatiquement configuré dans votre NetScaler ADM.

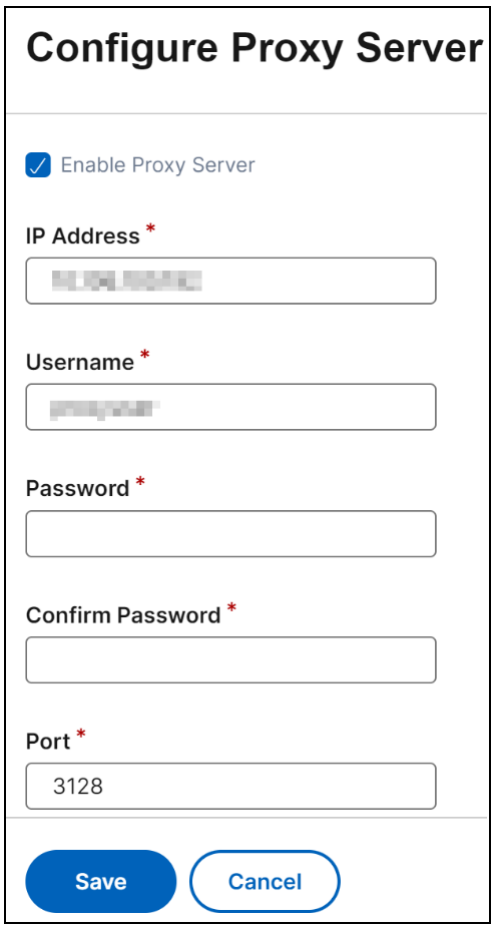


- Si vous ne disposez pas d'un locataire de service NetScaler Console ou si le partage de données n'est pas activé dans le cadre de l'identité client, l'ADM On-Prem Cloud Connector n'est pas automatiquement activé et vous devez configurer manuellement le Cloud Connector. Une fois la configuration terminée, Citrix Cloud pourra collecter des données de licence, de configuration et d'utilisation afin de gérer, de mesurer et d'améliorer le service. En savoir plus sur la collecte de données.

Autres options

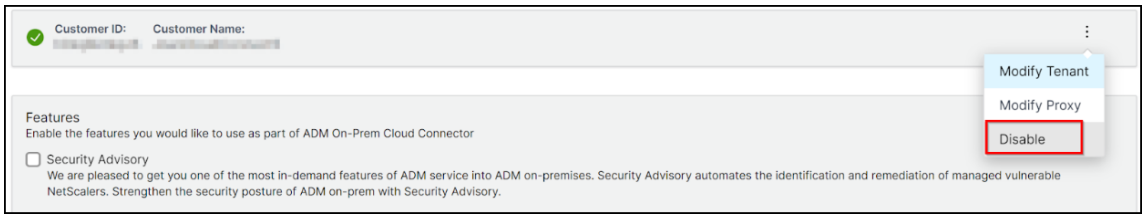
Après avoir activé ADM On-Prem Cloud Connector, vous pouvez utiliser les options suivantes :

- **Modifier le locataire** : vous permet de modifier le locataire existant. Lorsque vous cliquez sur **Modifier le locataire**, vous êtes redirigé vers un nouvel onglet et vous devez vous connecter à Citrix Cloud. Une fois la connexion établie, vous pouvez sélectionner un autre locataire.
- **Modifier le proxy** : vous permet de configurer les paramètres du proxy dans ADM on-prem. Cela est nécessaire lorsque NetScaler ADM ne dispose pas d'un accès direct à Internet via le réseau de gestion. Cliquez sur **Modifier le proxy** dans la liste, mettez à jour les détails, puis cliquez sur **Enregistrer**.



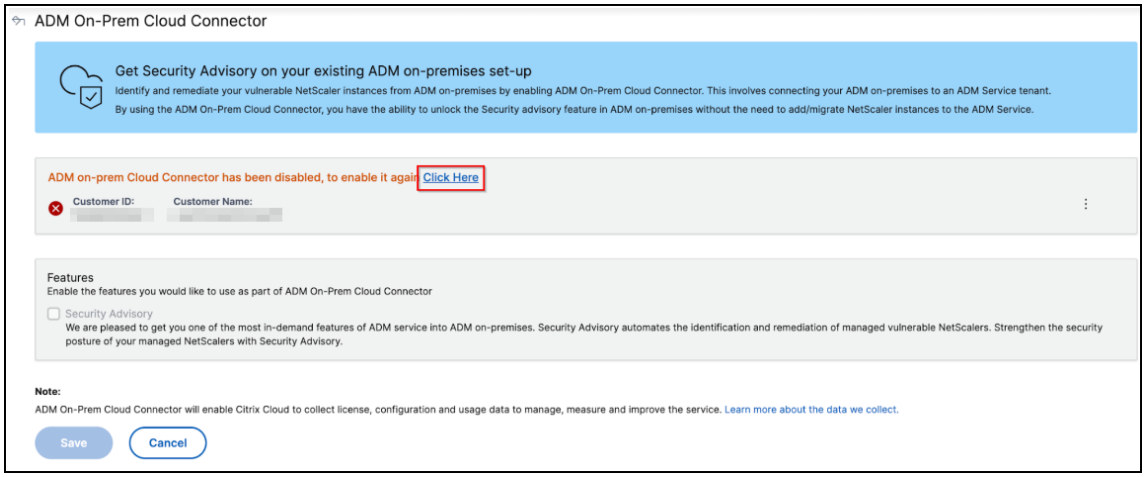
- **Désactiver** : désactive la fonctionnalité ADM On-Prem Cloud Connector. Si vous choisissez de le désactiver, la collecte des statistiques de données est désactivée et vous ne pouvez pas utiliser la version complète de l'avis de sécurité.

  Pour le désactiver, cliquez sur **Désactiver** dans la liste.



  Un message de confirmation s'affiche. Cliquez sur **Oui** pour désactiver.

  Vous pouvez réactiver ADM On-Prem Cloud Connector ultérieurement sans aucune étape supplémentaire.



Désactiver l'avis de sécurité

Sur la page de configuration d'ADM On-Prem Cloud Connector, vous pouvez également décocher la case **Avis de sécurité** pour désactiver la fonctionnalité d'avis de sécurité. Les métriques de données sont toujours collectées.

Configurer

February 1, 2024

Vous pouvez accéder à un serveur NetScaler ADM uniquement 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, consulter des analyses et configurer le serveur NetScaler 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 NetScaler ADM :

Connectez-vous à NetScaler ADM à l'aide des informations d'identification de l'administrateur.

Une fois connecté à NetScaler ADM, vous devez procéder comme suit pour commencer :

- Ajoutez des instances à NetScalerADM. Vous devez ajouter des instances au serveur NetScaler 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 NetScaler ADM. Vous devez configurer un serveur NTP (Network Time Protocol) dans NetScaler ADM pour synchroniser son horloge avec le serveur NTP.
- Configurez les paramètres système pour optimiser les performances de NetScaler ADM. Avant de commencer à utiliser NetScaler 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 NetScaler ADM.

Ajouter des instances à NetScaler ADM

February 1, 2024

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

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler BLX
- NetScaler Gateway

Vous pouvez ajouter des instances lors de la première configuration du serveur NetScaler ADM ou ultérieurement. Vous devez ensuite spécifier un profil d'instance que NetScaler ADM peut utiliser pour accéder à l'instance.

> **Remarque :**
>
> - NetScaler ADM utilise l'adresse IP NetScaler (NSIP) des instances NetScaler pour la communication. Pour plus d'informations sur les ports qui doivent être ouverts entre les instances NetScaler et NetScaler ADM, consultez la section Ports.
> - Pour savoir comment NetScaler ADM découvre les instances, consultez la section Découvrir les instances.

Comment créer un profil NetScaler

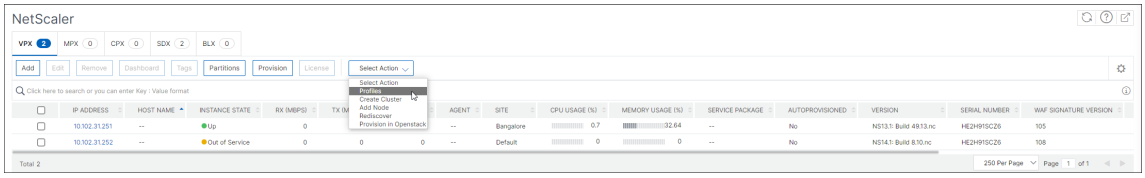
Le profil NetScaler inclut les informations d'identification, les ports et les types d'authentification pour ajouter des instances à NetScaler ADM. Pour chaque type d'instance, un profil par défaut est disponible. Par exemple, `nsroot` est le profil par défaut pour les instances NetScaler. Le profil par défaut est défini à l'aide des informations d'identification d'administrateur NetScaler 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 NetScaler à partir de la page **Instance** ou lors de l'ajout ou de la modification d'une instance.

> **Remarque :**
>
> veillez à utiliser le compte super administrateur pour créer un profil d'instance.

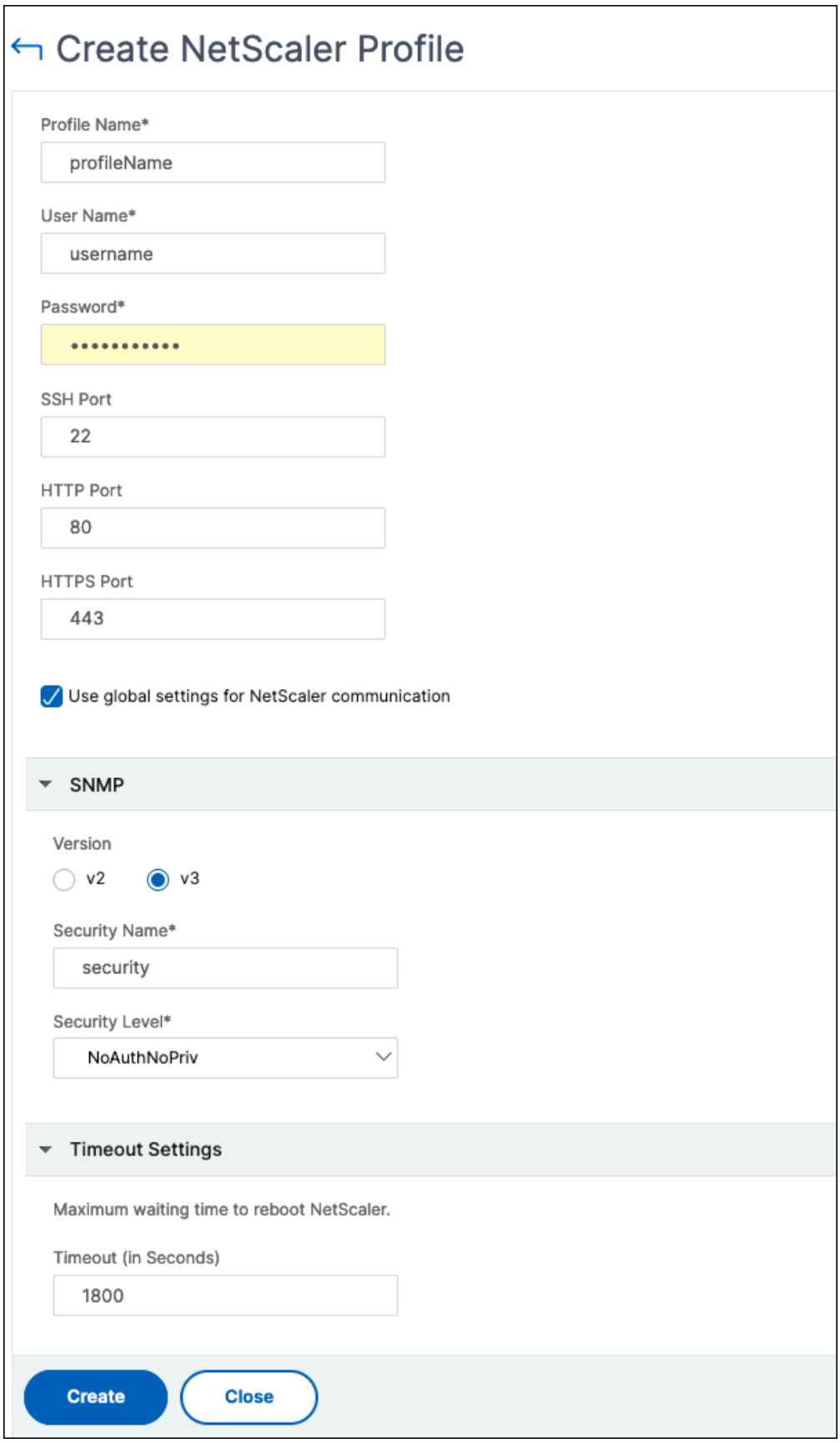
Pour créer un profil NetScaler depuis la page Instance :

1. Accédez à **Infrastructure > Instances**.
2. Sélectionnez une instance. Par exemple, NetScaler.
3. Sur la page NetScaler, sous **Sélectionner une action**, sélectionnez **Profils**.



4. Sur la page **Profils d'administration**, sélectionnez **Ajouter**.

5. Sur la page **Créer un profil NetScaler**, procédez comme suit :



a) **Nom du profil** : Spécifiez un nom de profil pour l'instance NetScaler.

b) **Nom d'utilisateur** : Spécifiez un nom d'utilisateur pour vous connecter à l'instance NetScaler.

c) **Mot de passe** : Spécifiez un mot de passe pour vous connecter à l'instance NetScaler.

d) **Port SSH** : Spécifiez le port pour la communication SSH entre NetScaler ADM et l'instance NetScaler.

e) **Port HTTP** : Spécifiez le port pour la communication HTTP entre NetScaler ADM et l'instance NetScaler.

> **Remarque :**
>
> Le port HTTP par défaut est 80. Vous pouvez également spécifier le port HTTP personnalisé ou différent du port par défaut que vous avez peut-être configuré dans votre instance NetScaler CPX. Le port HTTP personnalisé ne peut être utilisé que pour la communication entre NetScaler ADM et NetScaler CPX.

f) **Port HTTPS** : Spécifiez le port pour la communication HTTPS entre NetScaler ADM et l'instance NetScaler.

> **Remarque :**
>
> Le port HTTPS par défaut est 443. Vous pouvez également spécifier le port HTTPS personnalisé ou différent du port par défaut que vous avez peut-être configuré dans votre instance NetScaler CPX. Le port HTTPS personnalisé ne peut être utilisé que pour la communication entre NetScaler ADM et NetScaler CPX.

g) **Utiliser les paramètres globaux pour les communications NetScaler** : sélectionnez cette option si vous souhaitez utiliser les paramètres système pour la communication entre NetScaler ADM et l'instance NetScaler. 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 NetScaler SDX, seul le protocole **SNMPv2** est pris en charge.

i) **Paramètres de délai d'expiration** : Spécifiez le temps que NetScaler ADM doit attendre avant d'envoyer une demande de connexion à l'instance NetScaler après un redémarrage.

j) Sélectionnez **Créer**.

Ajouter des instances ADC à NetScaler ADM

Vous pouvez ajouter des instances lors de la première configuration du serveur NetScaler ADM ou ultérieurement.

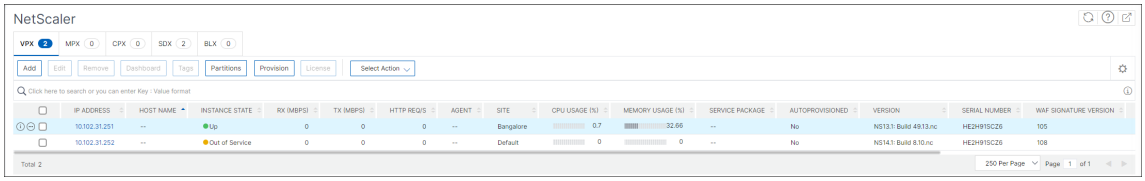
Pour ajouter des instances, vous devez spécifier le nom d'hôte ou l'adresse IP de chaque instance NetScaler, ou une plage d'adresses IP.

> **Remarque :**
>
> - Pour ajouter des instances NetScaler 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 NetScaler ADM, le cluster est uniquement représenté par l'adresse IP du cluster.
> - Pour les instances NetScaler configurées en tant que paire HA, lorsque vous ajoutez une instance, l'autre instance de la paire est automatiquement ajoutée.

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 NetScaler ADM :

1. Connectez-vous à NetScaler ADM à l'aide des informations d'identification de l'administrateur.
2. Accédez à **Infrastructure > Instances > NetScaler**. Sélectionnez le type d'instance que vous souhaitez ajouter (par exemple, NetScaler VPX) et cliquez sur **Ajouter**.



3. Sélectionnez l'une des options suivantes :

   - **Entrez l'adresse IP de l'appareil** : pour les instances NetScaler, 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`

- **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.

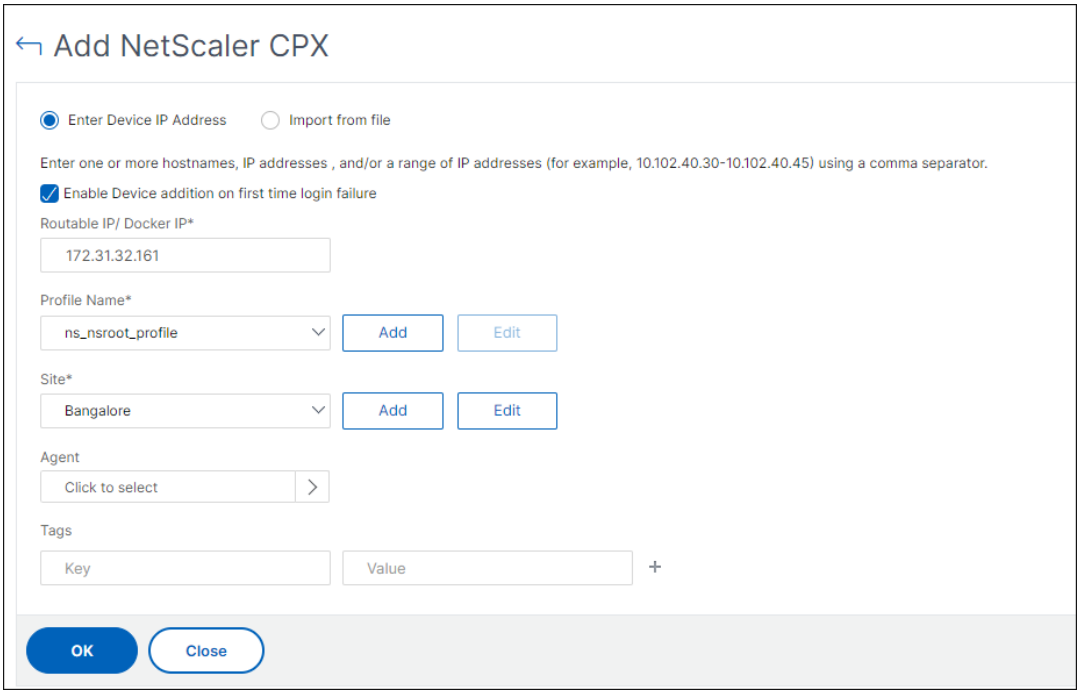
4. Dans **Nom du profil** , sélectionnez le profil d'instance approprié ou créez un profil en cliquant sur l'icône + .
5. Dans **Site** , sélectionnez l'emplacement où vous souhaitez ajouter l'instance, ou créez-en un en cliquant sur l'icône **+** .
6. Cliquez sur **OK** pour démarrer le processus d'ajout d'instances à NetScaler ADM.

> **Remarque :**
>
> Si vous souhaitez redécouvrir une instance, accédez à **Infrastructure > Instances > NetScaler**. 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 NetScaler CPX à NetScaler ADM

NetScaler ADM a été amélioré afin de prendre en charge les améliorations apportées aux fonctionnalités CPX. L'instance NetScaler CPX est désormais ajoutée à NetScaler ADM en fournissant une adresse IP pour le CPX ainsi qu'un profil d'appareil. 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, NetScaler ADM découvre et enregistre automatiquement l'instance CPX. Une instance CPX n'est plus découverte via l'hôte Docker.

1. Accédez à **Infrastructure > Instances > NetScaler** et cliquez sur **CPX**.
2. Cliquez sur **Ajouter** pour ajouter de nouvelles instances CPX dans Citrix ADM.
3. La page **Ajouter NetScaler 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 facilement l'instance ultérieurement.



> **Remarque :**
>
> Pour les instances NetScaler CPX, 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 NetScaler BLX autonome dans NetScaler ADM

Une instance NetScaler BLX autonome est une instance unique qui s'exécute sur le serveur Linux hôte dédié.

1. Accédez à **Infrastructure > Instances > NetScaler**.
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.

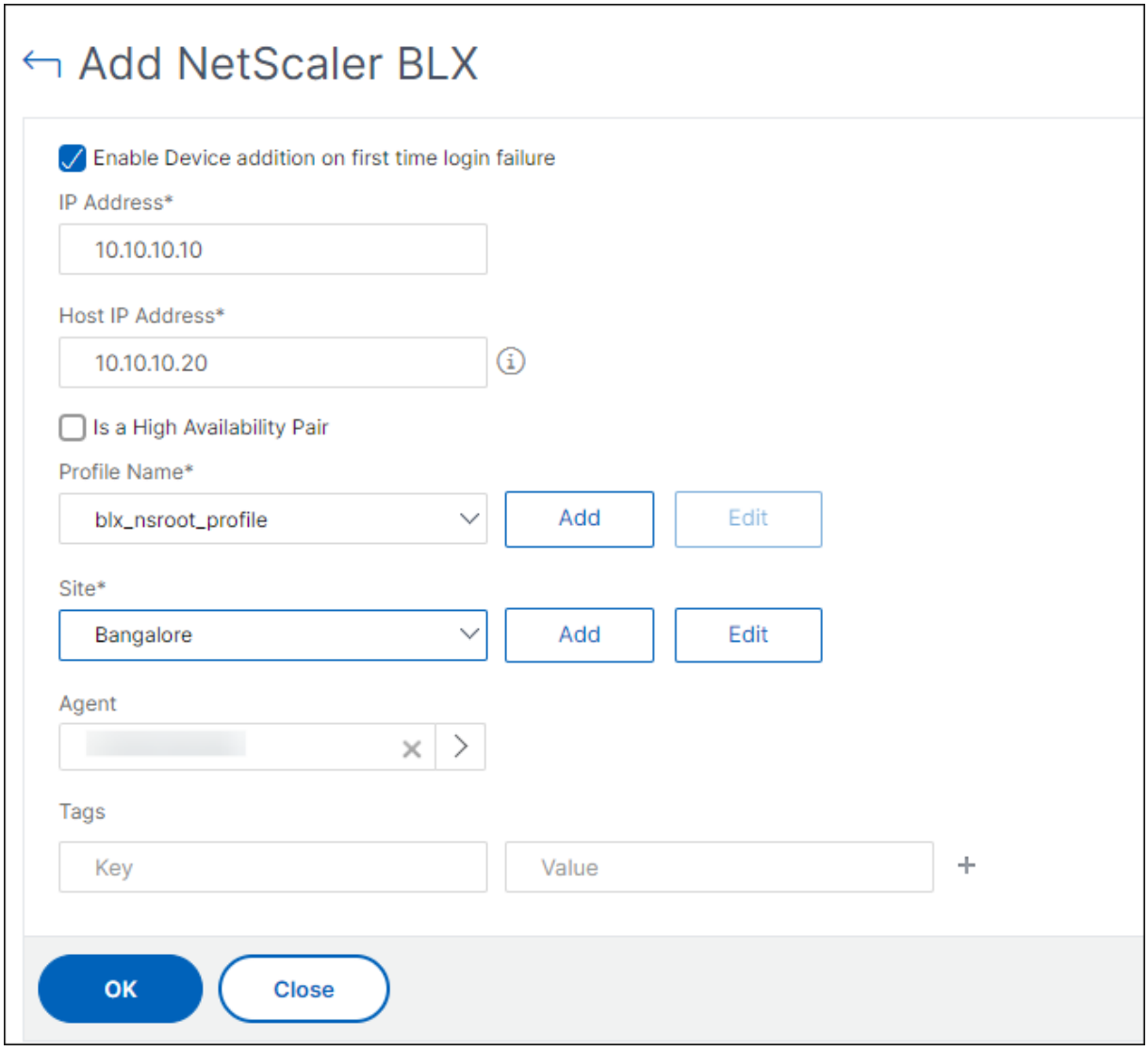
7. Dans la liste des **sites**, sélectionnez le site auquel vous souhaitez ajouter une instance.

   Si vous souhaitez ajouter un site, cliquez sur **Ajouter**.

8. Dans la liste des **agents, sélectionnez l'agent** NetScaler ADM auquel vous souhaitez associer l'instance.

   Si un seul agent est configuré sur votre NetScaler ADM, cet agent est sélectionné par défaut.

9. Cliquez sur **OK**.



Ajouter des instances NetScaler BLX à haute disponibilité dans NetScaler ADM

Les instances NetScaler BLX à 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.

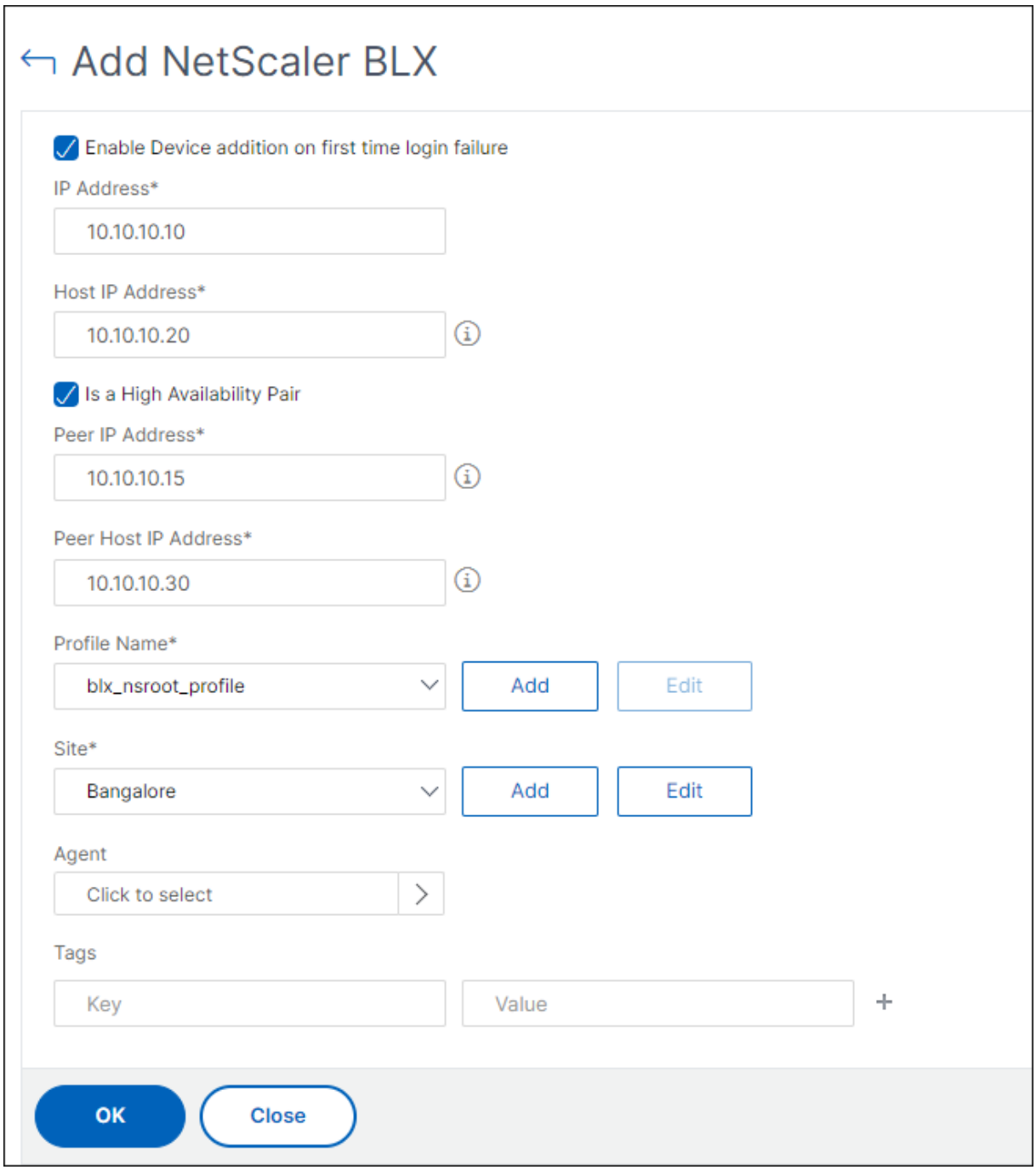
   Pour créer un profil, cliquez sur **Ajouter**.

   > **Important :**
   >
   > Assurez-vous de spécifier 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.

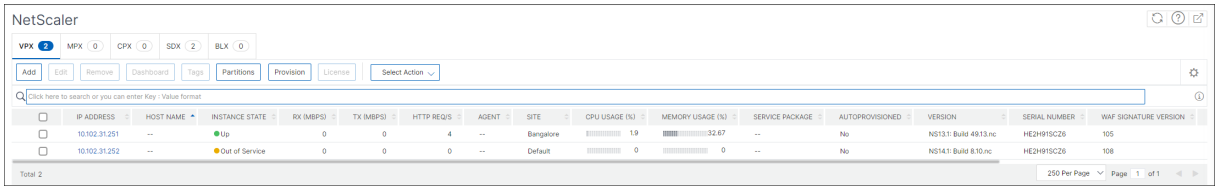
   Si vous souhaitez ajouter un site, cliquez sur **Ajouter**.
9. Dans la liste des **agents, sélectionnez l'agent** NetScaler ADM auquel vous souhaitez associer l'instance.

   Si un seul agent est configuré sur votre NetScaler ADM, cet agent est sélectionné par défaut.
10. Cliquez sur **OK**.



Accédez à l'interface graphique d'une instance depuis NetScaler ADM

1. Accédez à **Infrastructure > InstancesNetScaler**.
2. Sélectionnez le type d'instance auquel vous souhaitez accéder (par exemple, VPX, MPX, CPX, SDX ou BLX).
3. Cliquez sur l'adresse IP ou le nom d'hôte NetScaler requis.



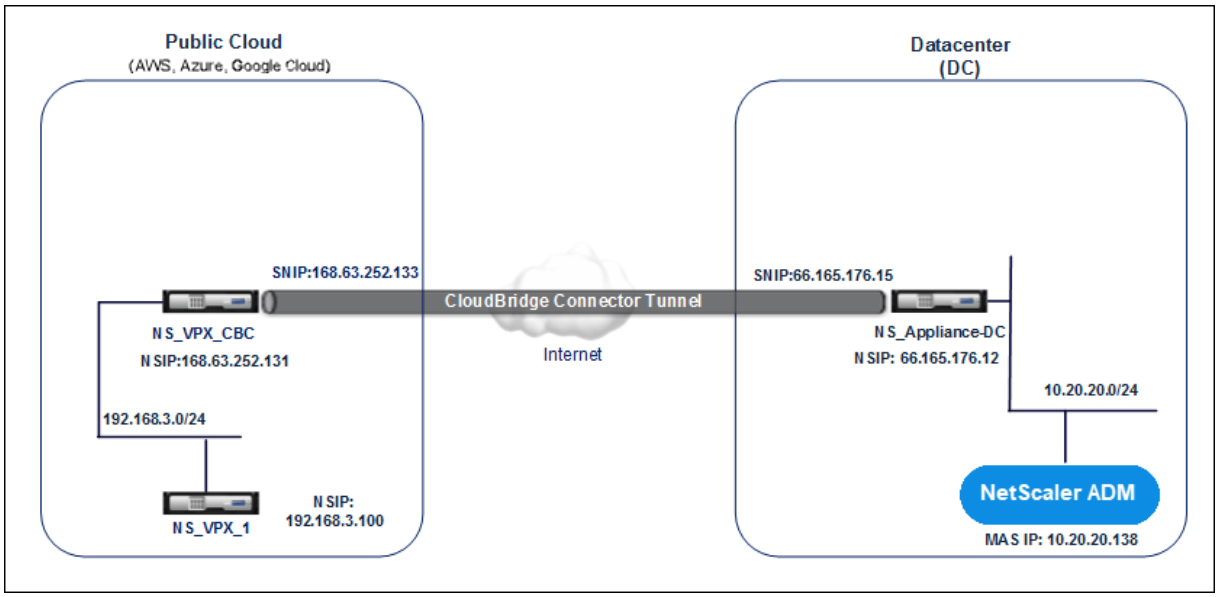
L'interface graphique de l'instance sélectionnée apparaît dans une fenêtre contextuelle.

Ajouter des instances NetScaler VPX déployées dans le cloud à NetScaler ADM

February 1, 2024

Vous pouvez utiliser NetScaler ADM pour gérer et surveiller les instances NetScaler VPX déployées sur un cloud public tel qu'Amazon Web Services (AWS), Microsoft Azure ou Google Cloud. Vous devez établir une connectivité de couche 3 entre NetScaler ADM et les instances NetScaler VPX déployées sur le cloud public. Pour établir la connectivité de couche 3, vous pouvez utiliser des solutions telles que Direct Connect to AWS, un VPN dans Azure ou des connecteurs tiers tels qu'Equinix, etc.

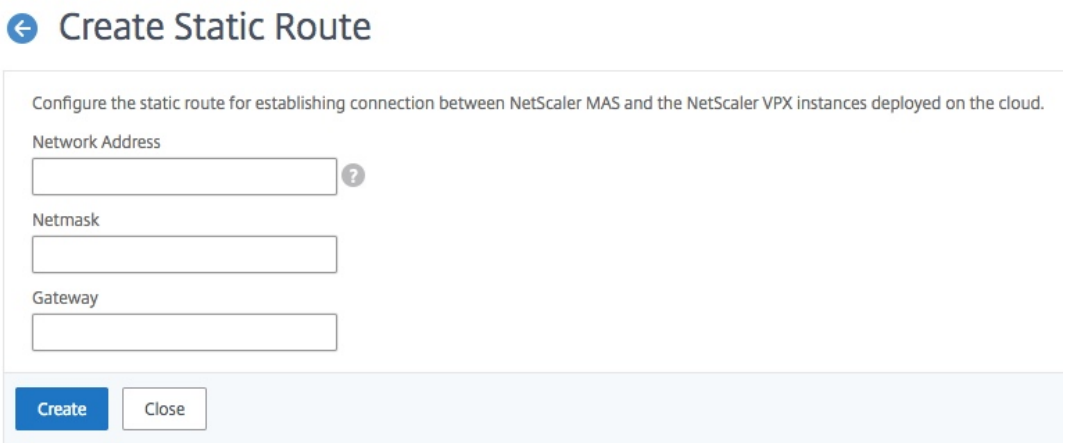
L'exemple de topologie suivant utilise Citrix CloudBridge Connector pour la connectivité de couche 3 entre NetScaler ADM et les instances NetScaler VPX déployées dans le cloud.



Un tunnel Citrix CloudBridge Connector est configuré entre l'appliance NetScaler NS_Appliance-DC, dans un centre de données DC, et l'appliance virtuelle NetScaler (VPX) NS_VPX_CBC dans le cloud public. NS_Appliance-DC et NS_VPX_CBC permettent la communication entre NetScaler ADM et l'instance NetScaler VPX, NS_VPX_1, déployée dans le cloud public. Une fois la communication établie, vous pouvez découvrir NS_VPX_1 dans NetScaler ADM.

Pour configurer cette topologie :

1. Installez, configurez et démarrez une instance NetScaler VPX dans le cloud public.
   - Pour obtenir des instructions, consultezInstaller NetScaler VPXsur AWS.
   - Pour obtenir des instructions, consultez la section Installer NetScaler VPX sur Microsoft Azure.
   - Pour obtenir des instructions, consultez Installer NetScaler VPX sur Google Cloud.
2. Déployez et configurez une appliance physique NetScaler, ou provisionnez et configurez une appliance virtuelle NetScaler (VPX) sur une plate-forme de virtualisation dans le centre de données.
   - Pour obtenir des instructions, consultez la section Installer une instance NetScaler VPX surCitrix Hypervisor.
   - Pour obtenir des instructions, reportez-vous à la section Installer des dispositifs virtuels Citrix sur VMware ESXi.
   - Pour obtenir des instructions, voir Installer des dispositifs virtuels NetScaler sur MicrosoftHyper-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 NetScaler ADM et les instances NetScaler VPX déployées sur le cloud, comme suit :
   a) Connectez-vous à NetScaler ADM.
   b) Accédez à **Système > Routes statiques**, puis cliquez sur **Ajouter**.



c) Dans le champ **Adresse réseau**, entrez l'adresse du réseau pour lequel vous souhaitez établir un itinéraire statique depuis NetScaler 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 cloud NetScaler VPX à NetScaler ADM en spécifiant la plage d'adresses IP des instances NetScaler VPX dans le cloud public. Pour obtenir des instructions détaillées, consultez la section Ajouter des instances à NetScalerADM.

Gérer les licences et activer les analyses sur les serveurs virtuels

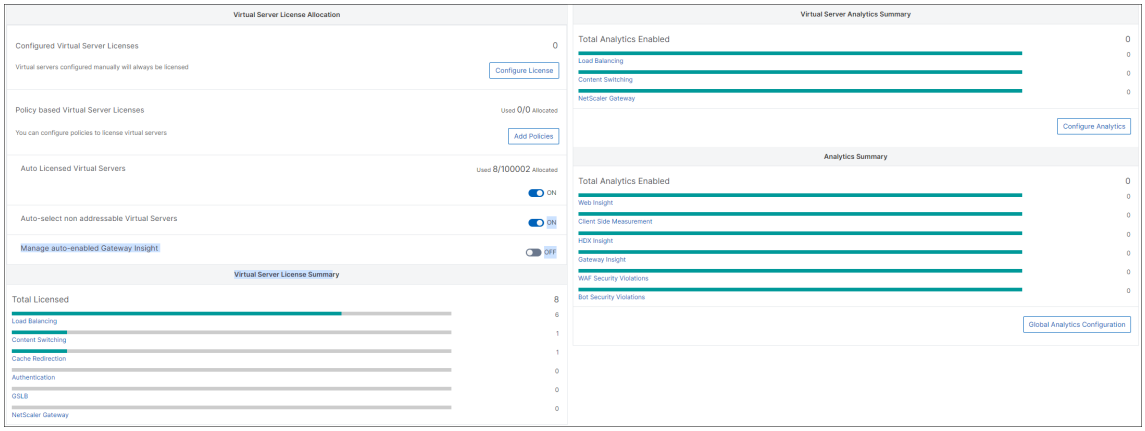
February 1, 2024

> **Remarque**
>
> - 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 **Paramètres > Configuration des licences et analyses** et désactivez l'option **Serveurs virtuels sous licence automatique** sous **Allocation de licence de serveur virtuel**.

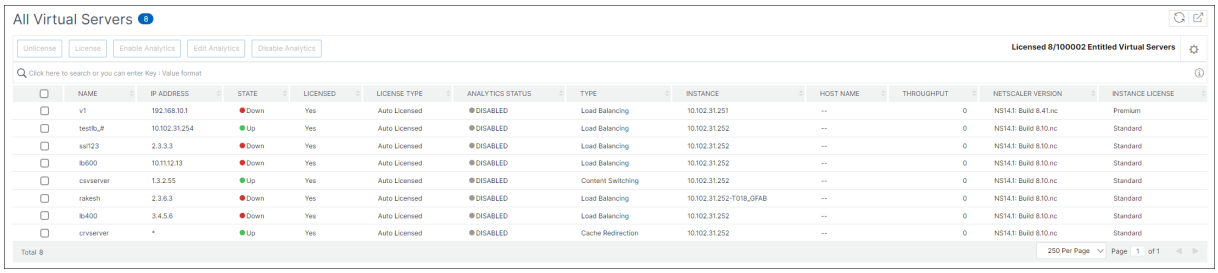
Le processus d'activation de l'analyse est simplifié. Vous pouvez obtenir une licence pour le serveur virtuel et activer les analyses dans un seul flux de travail.

Accédez à **Paramètres > Configuration des 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 :

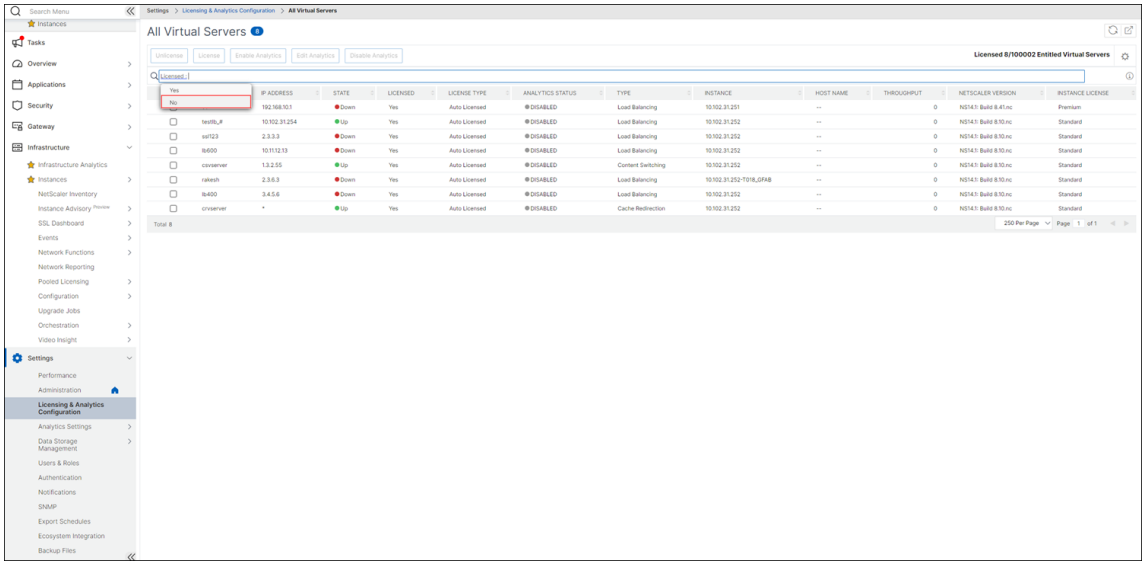
- Appliquer une licence pour les serveurs virtuels sans licence
- Supprimer la licence pour les serveurs virtuels sous licence
- Activez les analyses sur des serveurs virtuels sous licence
- Modifier les analyses
- Désactiver l'analyse

> **Remarque**
>
> Les serveurs virtuels pris en charge pour permettre l'analyse sont l'équilibrage de charge, la commutation de contenu et NetScaler Gateway.

Gestion des licences sur les serveurs virtuels

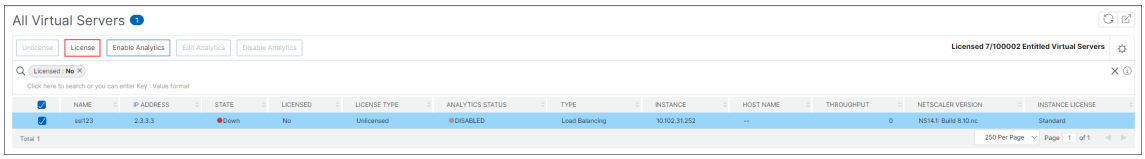
Pour obtenir une licence pour les serveurs virtuels, depuis la page **Tous les serveurs virtuels** :

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**.

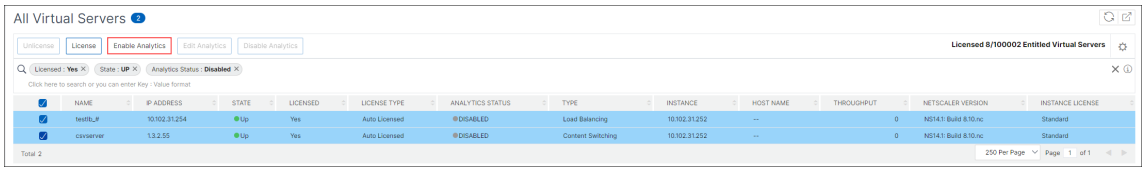
Activer l'analyse

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 **Infrastructure > Instances > NetScaler**, 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 (Violations de sécurité Web Insight ou WAF)

   b) Sélectionnez **Logstream** comme mode de transport

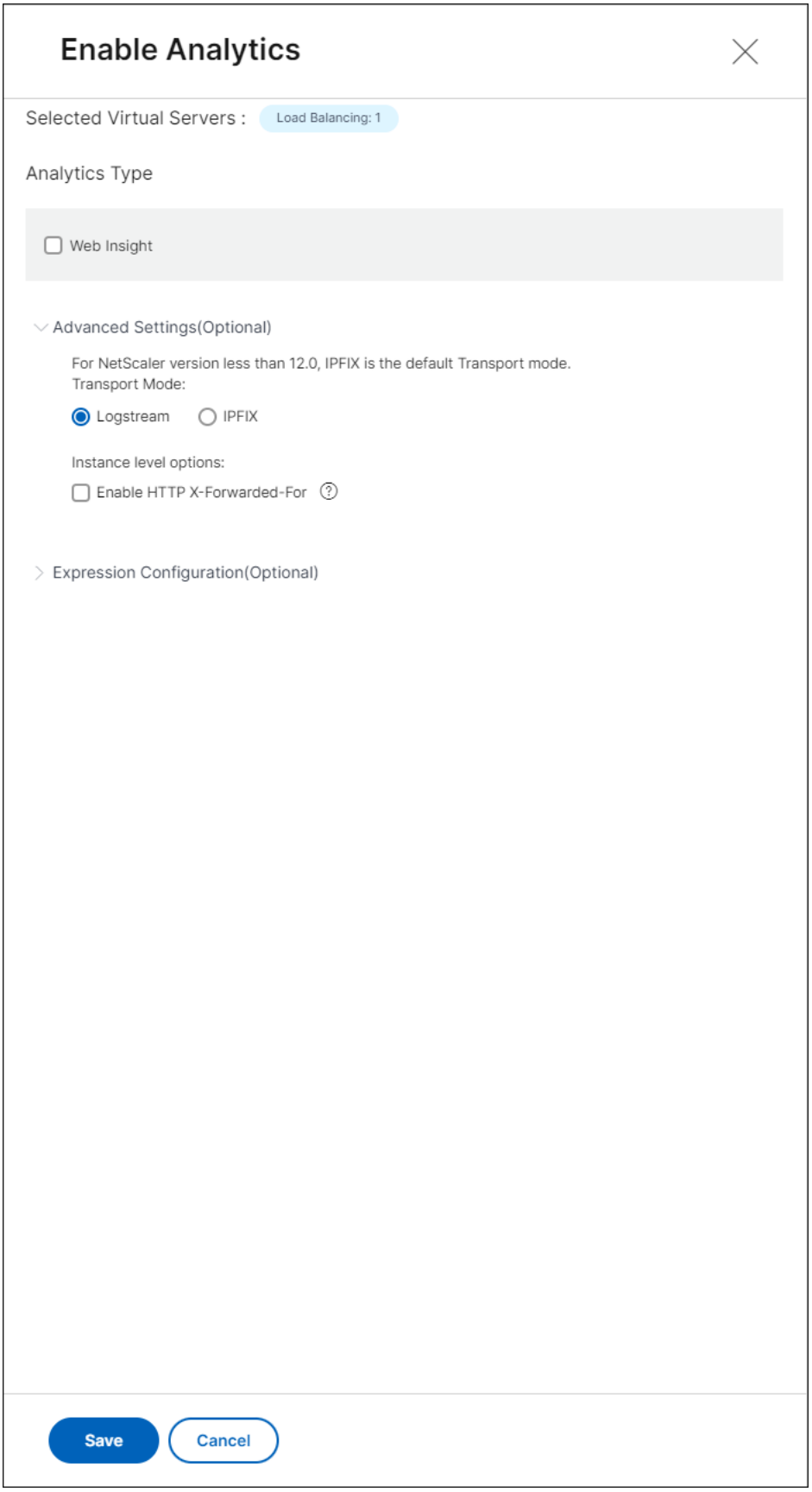
   > **Remarque**
   >
   > Pour NetScaler 12.0 ou version antérieure, **IPFIX** est l'option par défaut pour le mode transport. Pour NetScaler 12.0 ou version ultérieure, vous pouvez sélectionner **Logstream** ou **IPFIX** comme mode de transport.
   >
   > Pour plus d'informations sur IPFIX et Logstream, 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.
   - **NetScaler Gateway** : sélectionnez cette option pour afficher les analyses de NetScaler Gateway.

   d) L'expression est true par défaut

   e) Cliquez sur **OK**.



> **Remarque**
>
> - Si vous sélectionnez des serveurs virtuels sans licence, NetScaler ADM octroie d'abord une licence 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.

Une fois que vous avez **cliqué sur OK**, NetScaler ADM procède pour activer les analyses sur les serveurs virtuels sélectionnés.

> **Remarque**
>
> NetScaler ADM utilise NetScaler SNIP pour Logstream et NSIP pour IPFIX. Si un pare-feu est activé entre l'agent NetScaler ADM et l'instance NetScaler, assurez-vous d'ouvrir le port suivant pour permettre à NetScaler 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 **Infrastructure > Instances > NetScaler**, 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**

NetScaler ADM désactive les analyses sur les serveurs virtuels sélectionnés

Le tableau suivant décrit les fonctionnalités de NetScaler ADM qui prend en charge IPFIX et Logstream comme mode de transport :

Fonctionnalité	IPFIX	Logstream
Web Insight	•	•
Violations de sécurité WAF	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	Non pris en charge	•
CR Insight	•	•
Réputation IP	•	•
AppFirewall	•	•
Mesure côté client	•	•
Syslog/Auditlog	•	•

Un processus unifié pour permettre l'analyse sur les serveurs virtuels

February 1, 2024

Outre le processus existant pour activer les analyses, vous pouvez également utiliser un flux de travail à volet unique pour configurer les analyses sur :

- Tous les serveurs virtuels sous licence existants
- Les serveurs virtuels sous licence suivants

Après la configuration, cette fonctionnalité élimine la nécessité d'activer manuellement les analyses sur les serveurs virtuels existants et suivants.

Points à noter:

Avant de configurer les analyses, vous devez comprendre les comportements suivants de NetScaler ADM :

- Lorsque vous configurez cette fonctionnalité pour la première fois, vous devez vous assurer que les conditions préalables mentionnées dans ce document sont remplies.
- Modifiez les paramètres d'analyse ultérieurement.

  Supposons que vous avez configuré les paramètres d'analyse pour la première fois en sélectionnant Web Insight, HDX Insight et Gateway Insight. Si vous souhaitez modifier les paramètres d'analyse ultérieurement et désélectionner Gateway Insight, les modifications n'ont aucun impact sur les serveurs virtuels déjà activés avec les analyses.
- Les serveurs virtuels qui sont déjà activés avec les analyses.

  Supposons que vous disposez de 10 serveurs virtuels sous licence et que deux d'entre eux sont déjà activés avec Analytics. Dans ce scénario, cette fonctionnalité active les analyses uniquement pour les huit serveurs virtuels restants.
- Les serveurs virtuels qui sont désactivés manuellement à l'aide d'analyses.

  Supposons que vous disposez de 10 serveurs virtuels sous licence et que vous avez désactivé manuellement les analyses pour deux serveurs virtuels. Dans ce scénario, cette fonctionnalité active les analyses uniquement pour les huit serveurs virtuels restants et ignore les serveurs virtuels qui sont désactivés manuellement avec l'analyse.
- Les options **Violations de sécurité des bots** et **Violations de sécurité WAF** sont prises en charge uniquement sur les serveurs virtuels sous licence premium. Si les serveurs virtuels ne possèdent pas de licence Premium, les **violations de sécurité des bots** et les **violations de sécurité WAF** ne sont pas activées.

Conditions préalables

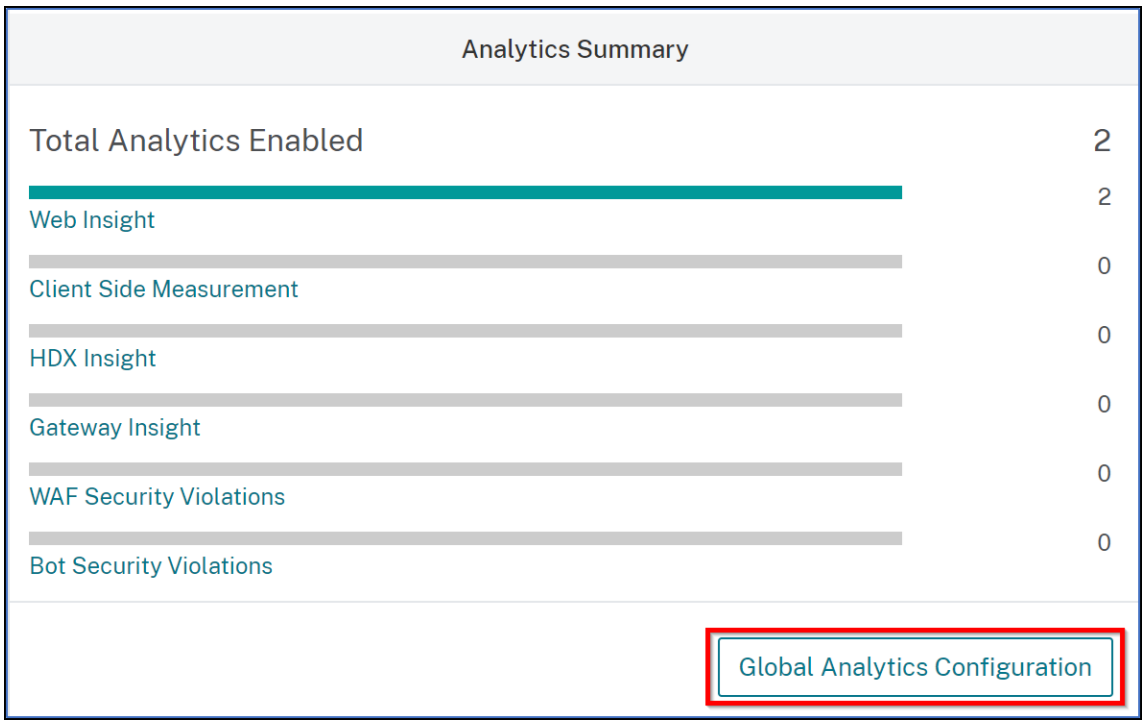
Assurez-vous que :

- Tous les serveurs virtuels existants sont sous licence.
- L'option de licence automatique est activée pour octroyer une licence à tous les serveurs virtuels suivants. Accédez à **Paramètres > Configuration des licences et des analyses** et sous **Allocation de licence de serveur virtuel**, activez l'option **Serveurs virtuels sous licence automatique** .

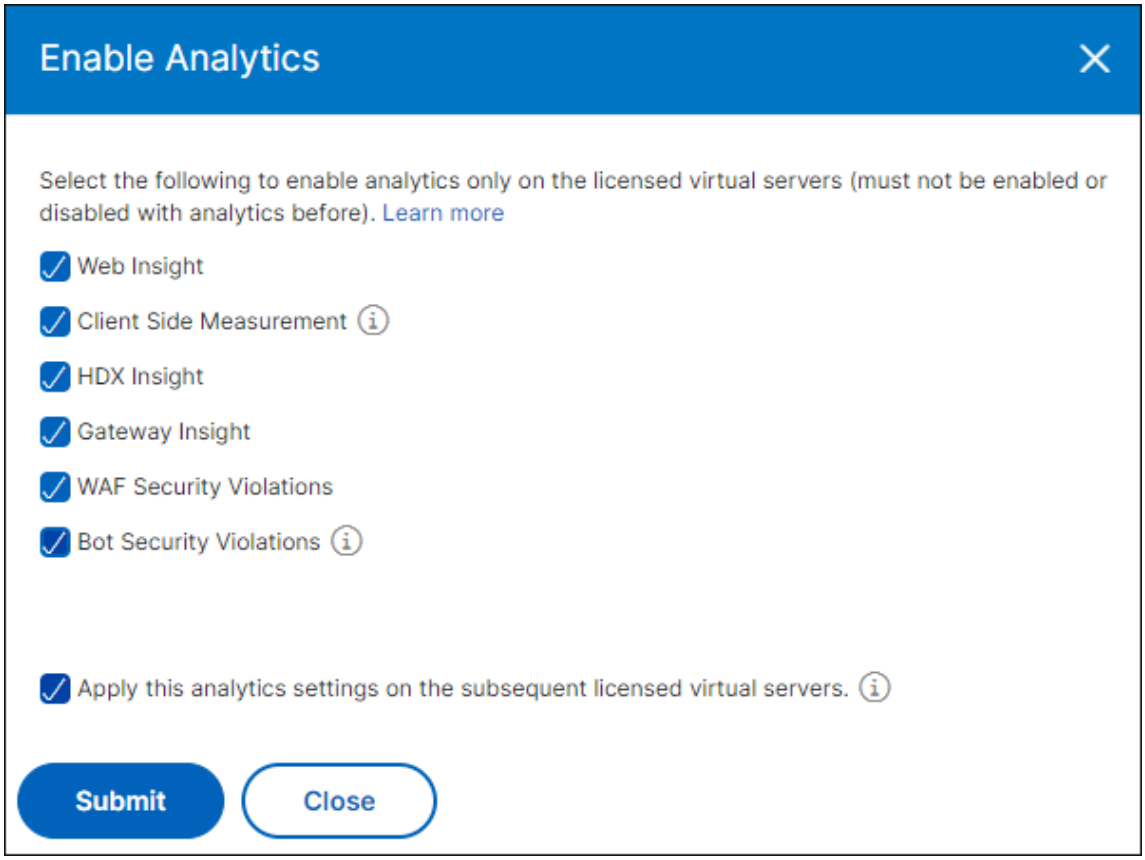
Activer l'analyse

1. Accédez à **Paramètres > Configuration des licences et des analyses**.

2. Sous **Résumé des analyses**, cliquez sur **Configuration globale des analyses**.



3. Sélectionnez les fonctionnalités d'analyse pour lesquelles vous souhaitez activer l'analyse sur les serveurs virtuels.
4. Pour activer les analyses sur les serveurs virtuels suivants, cochez la case **Appliquer ces paramètres d'analyse sur les serveurs virtuels sous licence suivants** .
5. Cliquez sur **Envoyer**.



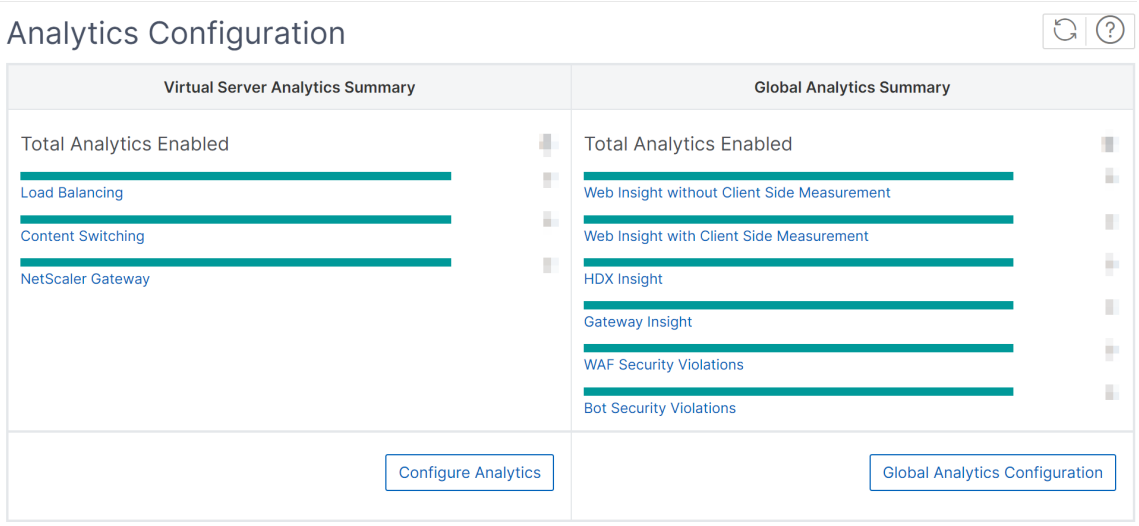
Configurer les analyses sur des serveurs virtuels sous licence flexible

February 1, 2024

La condition préalable pour activer les analyses est que les serveurs virtuels doivent disposer d'une licence. Si vous utilisez une licence flexible, tous les serveurs virtuels existants et les serveurs virtuels suivants reçoivent automatiquement une licence. Vous pouvez procéder à la configuration des analyses.

Vous pouvez configurer les analyses de deux manières. Accédez à **Paramètres > Configuration des analyses** pour afficher :

- **Résumé**des analyses des serveurs virtuels : vous permet de configurer les analyses sur les serveurs virtuels existants.
- **Résumé**global des analyses : vous permet de configurer les analyses sur les serveurs virtuels existants et ultérieurs.



Configurer les analyses sur les serveurs virtuels existants

> **Remarque :**
>
> Assurez-vous que les serveurs virtuels sur lesquels vous souhaitez activer les analyses sont en état **UP** .

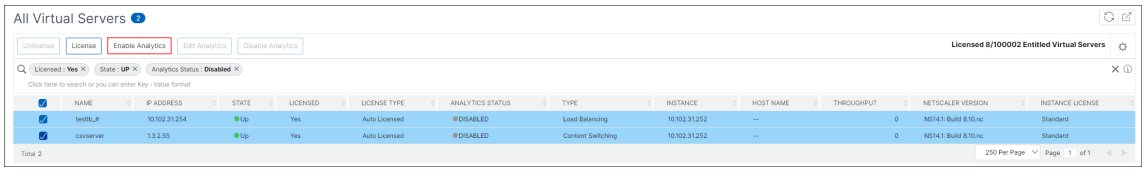
1. Sous **Résumé des analyses du serveur virtuel**, cliquez sur **Configurer les analyses**.

   La page **Tous les serveurs virtuels** s'affiche. Vous pouvez :

   - Activer l'analyse
   - 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 NetScaler Gateway.

2. Sélectionnez les serveurs virtuels, puis cliquez sur **Activer Analytics**.



> **Remarque**
>
> Vous pouvez également activer les analyses pour une instance :

```
1. Accédez à **Infrastructure > Instances > NetScaler**, puis
```



```
        sélectionnez le type d'instance. Par exemple, VPX.
2
3   1.  Sélectionnez l'instance et, dans la liste **Sélectionner
        une action** , sélectionnez **Configurer Analytics**
4
5   1.  Sur la page Configurer Analytics sur des serveurs virtuels
        , sélectionnez le serveur virtuel et cliquez sur **Activer
        Analytics**.
```

3. Dans la fenêtre **Activer Analytics** :

   a) Sélectionnez les types d'informations.

   b) Sélectionnez **Logstream** comme mode de transport.

   > **Remarque :**
   >
   > Pour NetScaler 12.0 ou version antérieure, **IPFIX** est l'option par défaut pour le mode transport. Pour NetScaler 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.
   - **NetScaler Gateway** : sélectionnez cette option pour afficher les analyses de NetScaler Gateway.

   d) L'expression est vraie par défaut.

   e) Cliquez sur **OK**.

   > **Remarque :**
   >
   > - 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.

Une fois que vous avez **cliqué sur OK**, NetScaler ADM procède pour activer les analyses sur les serveurs virtuels sélectionnés.

> **Remarque**
>
> NetScaler ADM utilise NetScaler SNIP pour Logstream et NSIP pour IPFIX. Si un pare-feu est activé entre l'agent NetScaler ADM et l'instance NetScaler, assurez-vous d'ouvrir le port suivant pour permettre à NetScaler 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. Sélectionnez les serveurs virtuels.

   > **Remarque :**
   >
   > Vous pouvez également modifier les analyses d'une instance :
   >
   > ```
   > 1.  Accédez à **Infrastructure > Instances > NetScaler**, 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. Sélectionnez les serveurs virtuels.
2. Cliquez sur **Désactiver Analytics** .

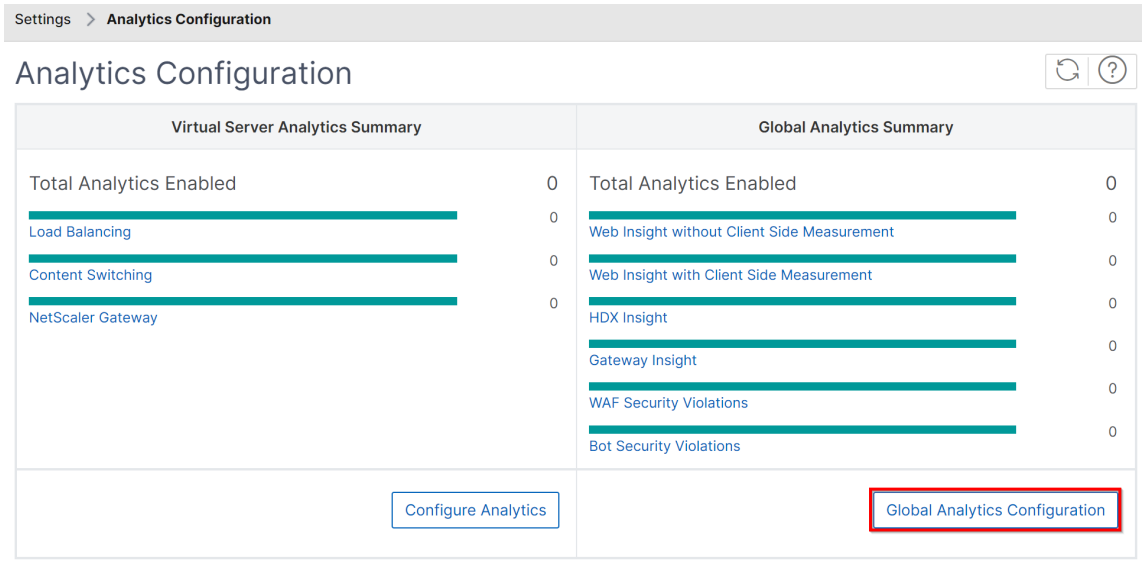
NetScaler ADM désactive les analyses sur les serveurs virtuels sélectionnés.

Le tableau suivant décrit les fonctionnalités de NetScaler ADM qui prend en charge IPFIX et Logstream comme mode de transport :

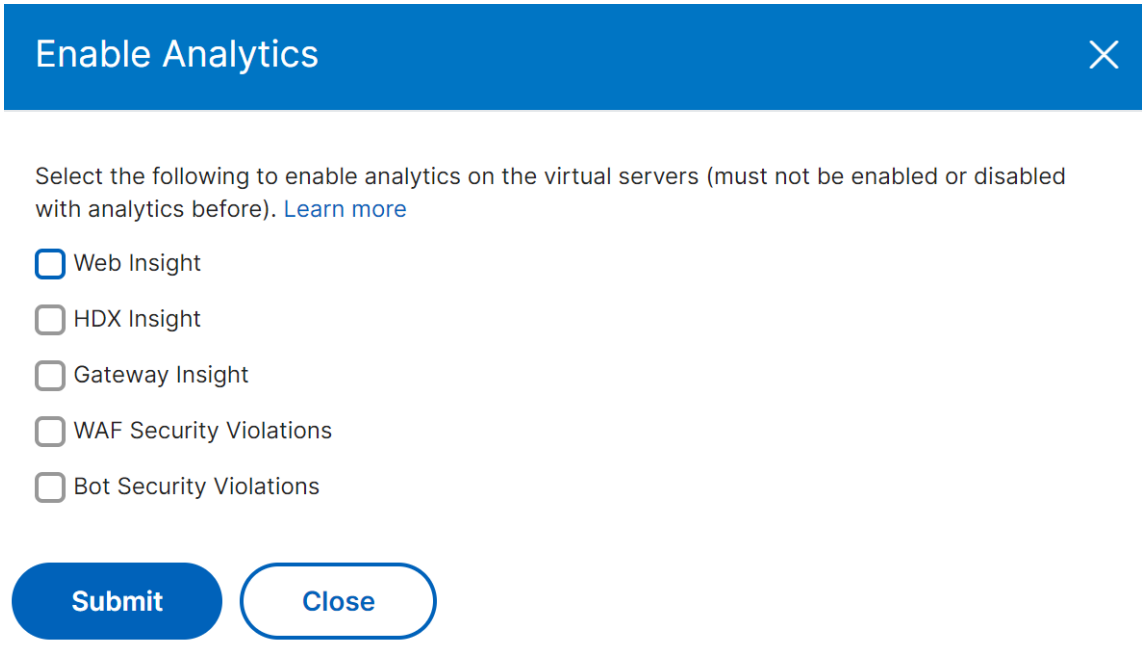
Fonctionnalité	IPFIX	Logstream
Web Insight	•	•
Violations de sécurité WAF	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	Non pris en charge	•
CR Insight	•	•
Réputation IP	•	•
AppFirewall	•	•
Mesure côté client	•	•
Syslog/Auditlog	•	•

Configurer les analyses à l'échelle mondiale

1. Sous **Résumé des analyses globales** , cliquez sur **Configuration des analyses globales** .



2. Sélectionnez les fonctionnalités d'analyse pour lesquelles vous souhaitez activer l'analyse sur les serveurs virtuels.
3. Cliquez sur Envoyer.



Après la configuration, les analyses sont activées sur les serveurs virtuels existants et suivants.

Points à noter

- Supposons que vous avez configuré la configuration d'analyse globale pour la première fois en sélectionnant Web Insight , HDX Insight et Gateway Insight. Si vous modifiez à nouveau les paramètres d'analyse ultérieurement et que vous désélectionnez Gateway Insight , les modifications n'auront aucune incidence sur les serveurs virtuels déjà activés avec Analytics.
- Supposons que vous disposez de 10 serveurs virtuels sous licence et que deux d'entre eux sont déjà activés avec les analyses à l'aide de l'option **Configurer les analyses** . Dans ce scénario, lorsque vous configurez la configuration d'analyse globale, les analyses sont appliquées uniquement aux huit serveurs virtuels restants.
- Supposons que vous disposez de 10 serveurs virtuels sous licence et que vous avez désactivé manuellement les analyses pour deux serveurs virtuels. Dans ce scénario, lorsque vous configurez la configuration d'analyse globale, les analyses sont appliquées uniquement aux huit serveurs virtuels restants et les serveurs virtuels qui sont désactivés manuellement par Analytics sont ignorés.

Attribuer un profil réseau à l'instance NetScaler gérée

February 1, 2024

Lorsque vous activez l'analyse pour les serveurs virtuels dans NetScaler ADM, les données AppFlow de NetScaler sont exportées vers NetScaler ADM via l'adresse IP du sous-réseau (SNIP) NetScaler. Dans certains scénarios, le SNIP peut être bloqué en raison du pare-feu du réseau. Dans de tels scénarios, vous devrez peut-être utiliser une adresse IP différente de celle du SNIP. Pour plus d'informations sur le profil réseau, voir Utiliser une adresse IP source spécifiée pour les communications dorsales.

Vous pouvez attribuer un profil réseau à une instance NetScaler via NetScaler ADM pour exporter des données AppFlow de NetScaler vers NetScaler ADM.

Conditions préalables

Assurez-vous que :

- La version de l'instance NetScaler **est**13.0-48.4 ou ultérieure.
- Le profil réseau est configuré dans les instances NetScaler.

Pour attribuer un profil réseau dans NetScaler ADM, procédez comme suit :

1. Accédez à **Infrastructure > Instances > NetScaler**.
2. Sélectionnez l'instance et, dans la liste **Sélectionner une action**, cliquez sur **Configurer les profils réseau** pour attribuer un profil réseau à l'instance.
3. Sélectionnez un profil réseau dans la liste et cliquez sur **Appliquer**.

> **Remarque :**
>
> Assurez-vous de désactiver l'analyse pour tous les serveurs virtuels avant d'attribuer un profil réseau à l'instance.

Configurer le serveur NTP

February 1, 2024

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

Pour configurer un serveur NTP sur NetScalerADM, procédez comme suit :

1. Dans l'interface graphique d'ADM, accédez à **Paramètres > 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 NetScaler 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 NetScaler 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 NetScaler ADM.

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 **Paramètres > 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 dépassé le seuil ou pour lesquelles un événement s'est produit, accédez à **Paramètres > 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 NetScaler ADM, et vous pouvez configurer des serveurs de passerelles de messagerie et de messagerie courte (SMS) pour envoyer des notifications par e-mail et par SMS 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 **Paramètres > Administration**. Dans la page **Administration système**, sous **Notifications d'événements**, cliquez sur **Configurer la notification et le résumé des événements > Notification d'événements**.
2. Sur la page **Configurer les paramètres de notification du système**, sélectionnez la catégorie ou la catégorie d'événements générés par NetScaler 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 reporting stockées dans la base de données de votre serveur NetScaler ADM, vous pouvez spécifier l'intervalle pendant lequel vous souhaitez que NetScaler 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).

Pour configurer le paramètre de nettoyage du système :

1. Accédez à **Paramètres > 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 Syslog génériques sont supprimées de NetScaler ADM.

Pour configurer les paramètres de purge de syslog d'instance :

1. Accédez à **Paramètres > Administration > Élagage 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'événements stockées dans la base de données de votre serveur NetScaler ADM, vous pouvez spécifier l'intervalle pendant lequel vous souhaitez que NetScaler ADM conserve les données de reporting réseau, les événements, les journaux d'audit et les journaux de 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 **Paramètres > 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, pendant lequel vous souhaitez conserver les données sur le serveur NetScaler ADM et cliquez sur Enregistrer.**

Configurer les paramètres de sauvegarde du système

NetScaler ADM sauvegarde automatiquement le système tous les jours à 00h30. 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 **Paramètres > 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 NetScaler, vous pouvez utiliser les fichiers de sauvegarde pour rétablir 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 **Paramètres > 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 **Paramètres > 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 NetScaler 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, NetScaler ADM interroge automatiquement les entités fonctionnelles 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 NetScaler et utilisez ultérieurement les fichiers sauvegardés pour restaurer l'instance ADC au même état. Pour plus d'informations, consultez la section Sauvegarder et restaurer des instances NetScaler.
- **Audit de la configuration des instances** : surveillez les modifications de configuration sur les instances NetScaler gérées, résolvez les erreurs de configuration et restaurez 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 NetScaler gérée. Les événements reçus dans NetScaler ADM sont affichés sur la page **Résumé des événements** (**Infrastructure > Événements**) et tous les événements actifs sont affichés sur la page Messages d'événements (**Infrastructure > 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** : NetScaler ADM fournit une vue centralisée des certificats SSL installés sur toutes les instances NetScaler gérées. Pour plus d'informations, consultez Tableau de bord SSL.
- **Instance Syslog** : vous pouvez surveiller les événements syslog générés sur vos instances NetScaler si vous avez configuré votre appareil pour rediriger tous les messages syslog vers NetScaler ADM.

Pour activer une fonctionnalité, effectuez les opérations suivantes :

1. Sélectionnez la fonctionnalité que vous souhaitez activer dans la liste.
2. Cliquez sur **Activer**.

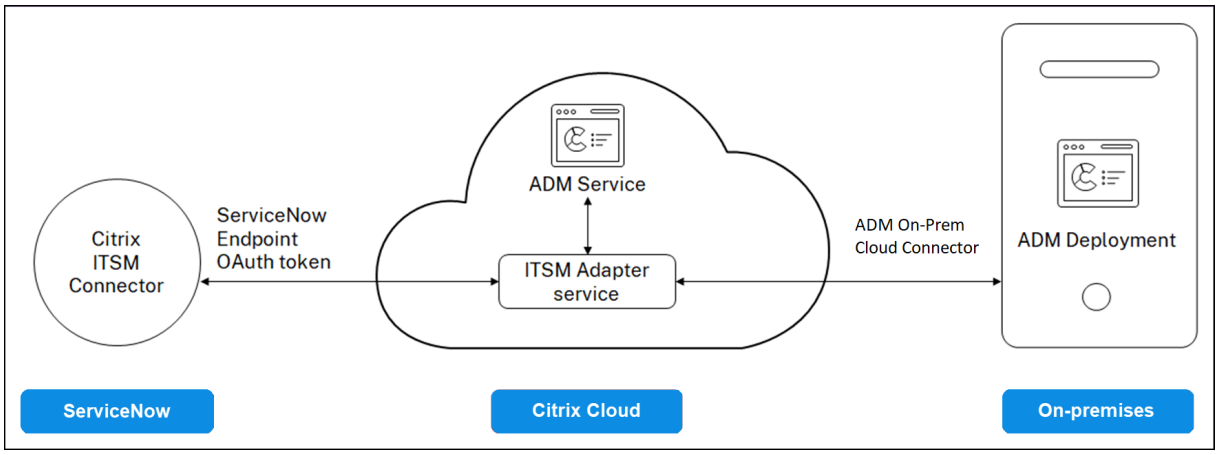
> **Important**
>
> Si une fonction est désactivée, l'utilisateur ne peut pas effectuer les opérations associées à cette fonctionnalité.

Intégrer NetScaler ADM à l'instance ServiceNow

February 1, 2024

Lorsque vous souhaitez activer les notifications ServiceNow pour les événements NetScaler et ADM, intégrez NetScaler ADM à l'instance ServiceNow. Cette intégration utilise le connecteur Citrix ITSM pour communiquer entre NetScaler 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 d'avoir configuré le Cloud Connector ADM On-Prem. Pour plus d'informations, consultez ADM On-Prem Cloud Connector.

Pour l'intégration de ServiceNow à ADM version 14.1 4.x ou antérieure, veillez à configurer l'identité du client. Pour plus d'informations, consultez Configurer l'identité du client.

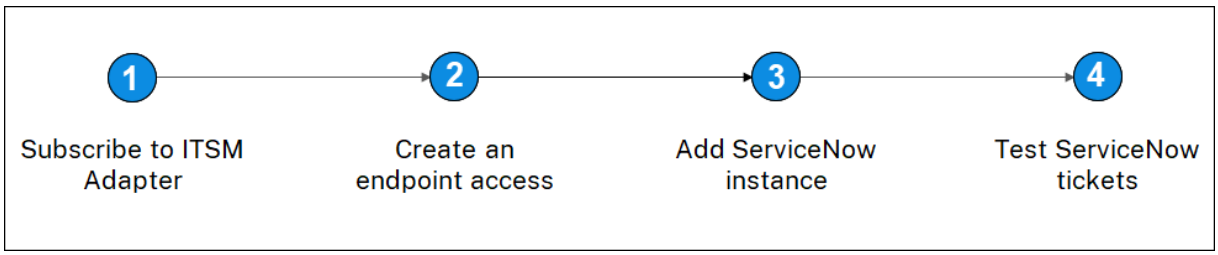
Conditions préalables

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 ?

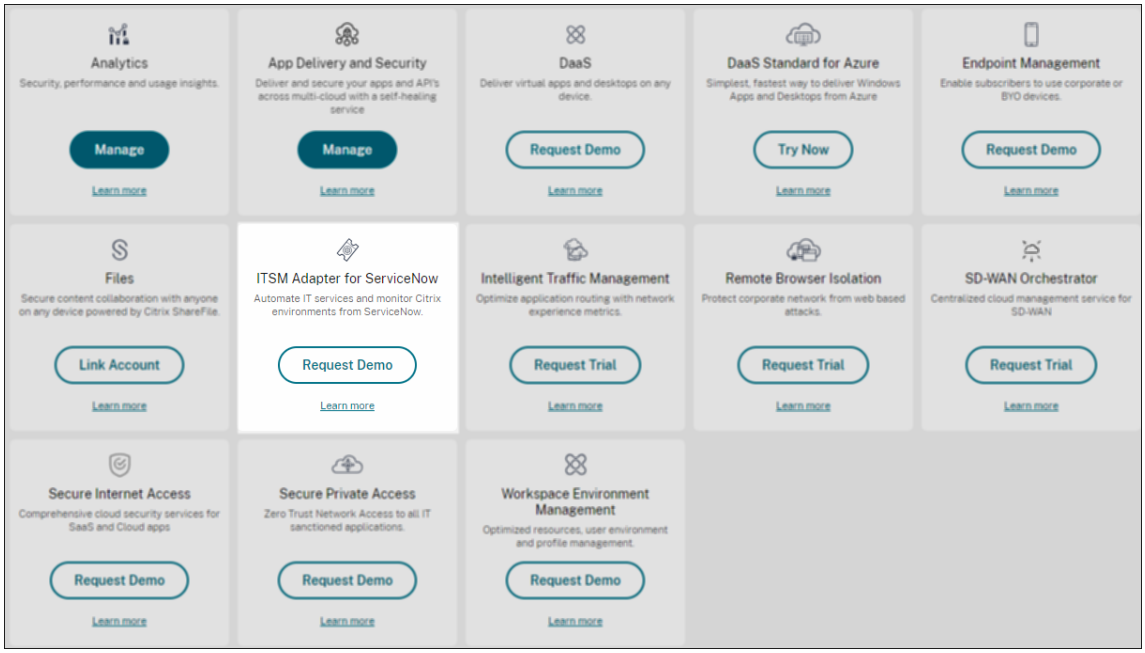
Procédez comme suit pour intégrer NetScaler ADM à ServiceNow à l'aide du connecteur ITSM :



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** .

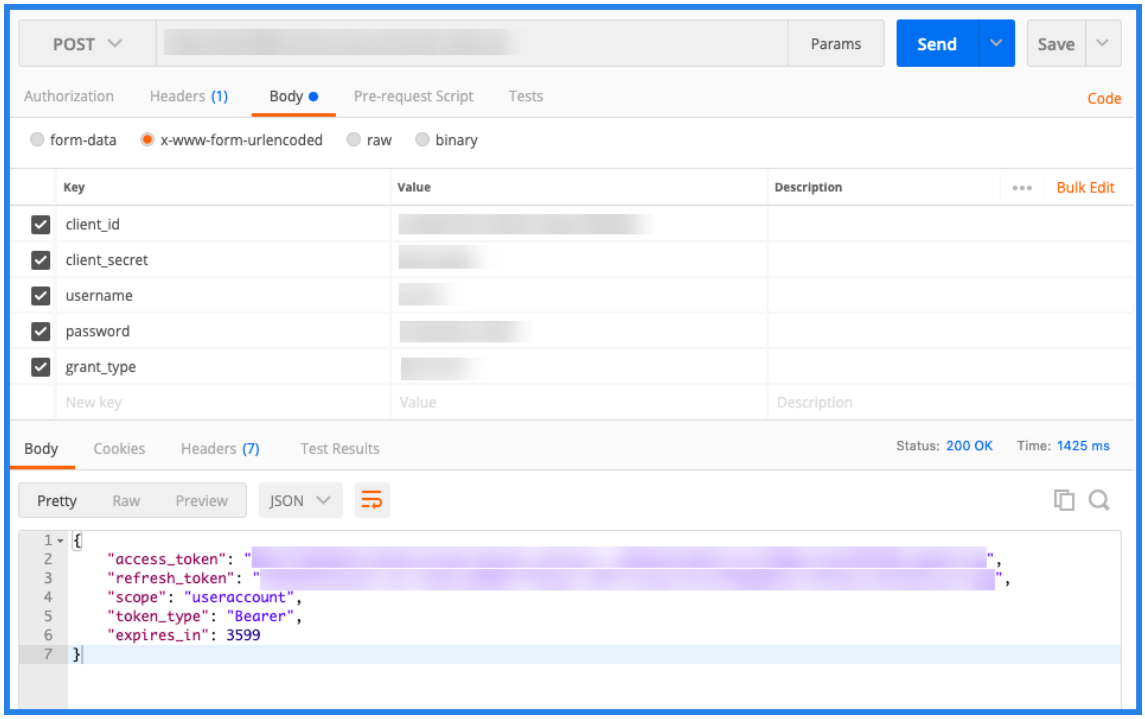


2. Accédez à **Identity Access and Management** > **API Access** et notez les informations **Client ID** et **Client Secret** .

Étape 2 - Créer un accès au point de terminaison dans l'instance ServiceNow

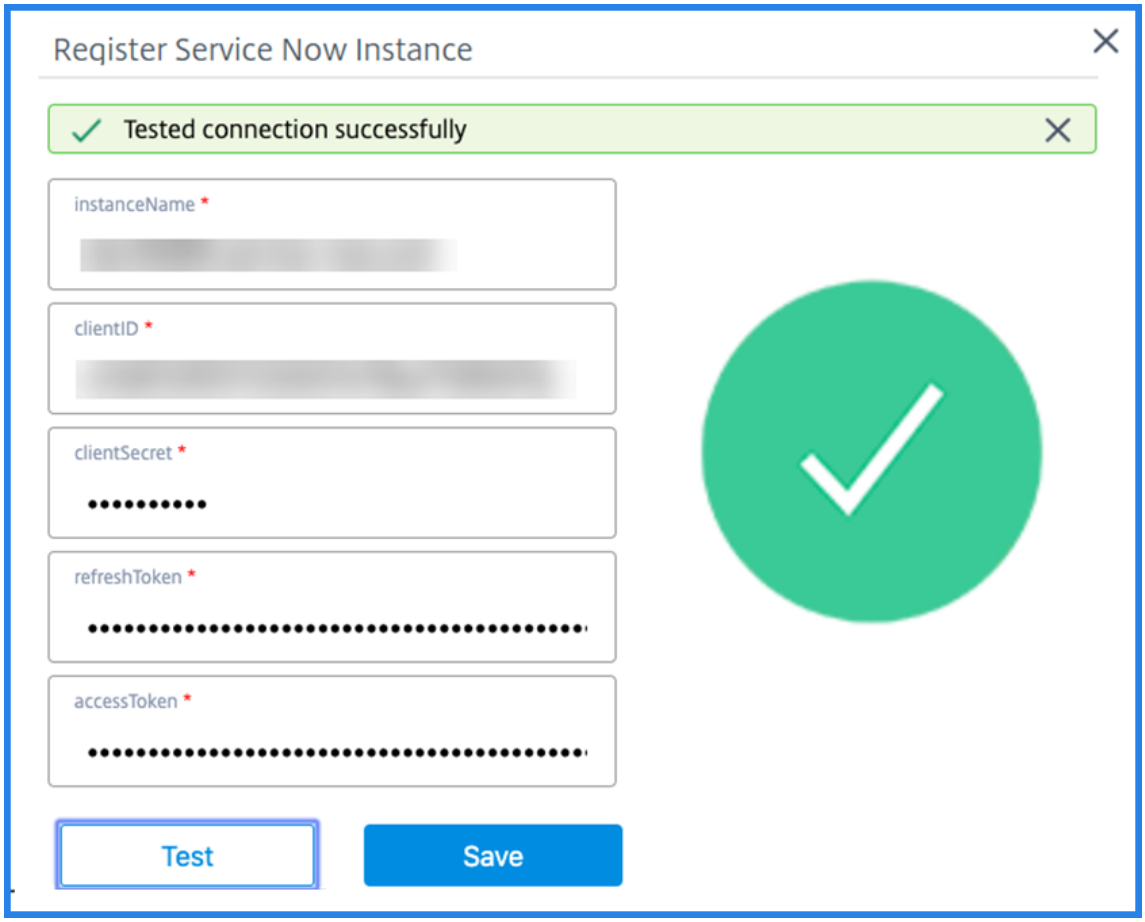
1. Connectez-vous à votre instance ServiceNow avec des informations d'identification d'administrateur.
2. Accédez au magasin ServiceNow. Téléchargez et installez le **connecteur Citrix ITSM**.

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 NetScaler 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 consulter les tickets ServiceNow dans l'interface graphique de NetScaler 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 NetScaler ADM :

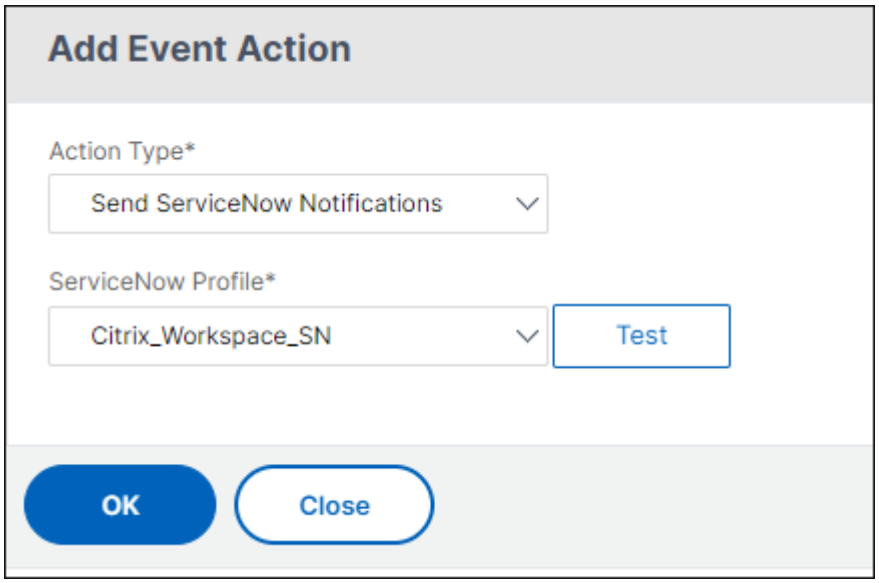
> **Important**
>
> Cette fonctionnalité est prise en charge sur ServiceNow Cloud.

- **Événements NetScaler** : NetScaler ADM peut générer les incidents ServiceNow pour l'ensemble sélectionné d'événements NetScaler à partir d'instances NetScaler gérées sélectionnées.

  Pour envoyer des notifications ServiceNow pour les événements NetScaler à partir des instances gérées, vous devez configurer une règle d'événement et attribuer à l'action de la règle l'action de la règle sous la forme Envoyer des notifications ServiceNow.

  Créez une règle d'événement sur l'ADM en accédant à **Infrastructure > Événements > Règles**. Pour plus d'informations, consultez la section Envoyer des notifications ServiceNow.

- **Analyse des applications** : NetScaler 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.

- **Les événements liés au certificat SSL et à la licence ADM** : NetScaler ADM peut générer les incidents ServiceNow relatifs à l'expiration du certificat SSL et aux événements d'expiration des licences 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, consultez L'expiration de la licence NetScalerADM.

Exporter ou planifier des rapports d'exportation

February 1, 2024

Dans NetScaler ADM, vous pouvez exporter un rapport complet pour la fonctionnalité NetScaler ADM sélectionnée. Ce rapport fournit une vue d'ensemble du mappage entre les instances, les partitions et les détails correspondants.

NetScaler ADM affiche des rapports d'exportation programmés spécifiques aux fonctionnalités sous les fonctionnalités individuelles d'ADM, que vous pouvez consulter, modifier ou supprimer. Par exemple, pour afficher les rapports d'exportation des instances NetScaler, accédez à **Réseau > Instances > NetScaler** et cliquez sur l'icône d'exportation. Vous pouvez exporter ces rapports au format PDF, JPEG, PNG et CSV.

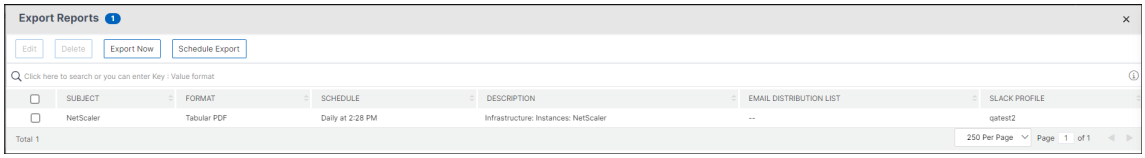
Dans **Exporter des rapports**, vous pouvez effectuer les actions suivantes :

- 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. NetScaler ADM envoie le rapport exporté à l'adresse e-mail ou au profil Slack configuré.

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 NetScaler ADM propose des fonctionnalités nouvelles et mises à jour avec des fonctionnalités améliorées. Citrix vous recommande de mettre à niveau NetScaler 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 obtenir des informations sur les licences NetScaler ADM, consultez la section Licences.

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 depuis la page de téléchargement de NetScaler ADM et suivez les instructions de cet article pour mettre à niveau votre système vers la dernière version 14.1. 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 préservée, mais NetScaler ADM ne traite aucune donnée tant que la mise à niveau n'est pas terminée.

> **Important**
>
> La version et le build de NetScaler ADM doivent être **égaux ou supérieurs à votre version et à** votre build de NetScaler. Par exemple, si vous avez installé NetScaler ADM 12.1 Build 50.39, assurez-vous d'avoir installé NetScaler 12.1 Build 50.28/50.31 ou une version antérieure.

Points à noter avant la mise à niveau vers la version 14.1 :

- 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. Mettez à niveau vers la version 13.1.
    4. Mise à niveau vers la version 14.1.
- Si vous effectuez une mise à niveau depuis la version 12.0 57.24 et les versions ultérieures, procédez d'abord à la mise à niveau vers la version 12.1, puis vers la version 14.1.
- Si vous effectuez une mise à niveau depuis la version 12.1, vous devez d'abord effectuer une mise à niveau vers la version 13.0 64.xx, puis directement vers la version 14.1
- Si vous effectuez une mise à niveau à partir de versions antérieures à 13.0 64.xx, pour une meilleure expérience utilisateur, effectuez d'abord une mise à niveau vers la version 13.0 64.xx, puis vers la version 14.1.
- Une fois la mise à niveau réussie vers la version 14.1 et après vous être connecté à l'interface graphique, il vous recommande de modifier le mot de passe si vous utilisez le mot de passe par défaut.

Points importants à prendre en compte avant de passer à la version 14.1 xx.xx et versions ultérieures

Lorsque vous mettez à niveau le logiciel ADM vers la version 14.1 xx.xx, 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 NetScaler ADM pour chaque mise à niveau, si vous effectuez une mise à niveau vers la version 14.1 xx.xx ou version ultérieure.
- Sauvegardez le serveur NetScaler ADM avant de procéder à la mise à niveau.
- Après la mise à niveau, vous devrez peut-être rétablir les connexions entre le serveur NetScaler ADM et les instances gérées. Une invite de confirmation vous avertit que les connexions peuvent échouer si vous continuez.

- Si vous effectuez une mise à niveau vers une version comprise entre 13.1.9.x et 13.1.30.x, NetScaler ADM rétablit le pack de configuration StyleBooks existant vers sa version antérieure.

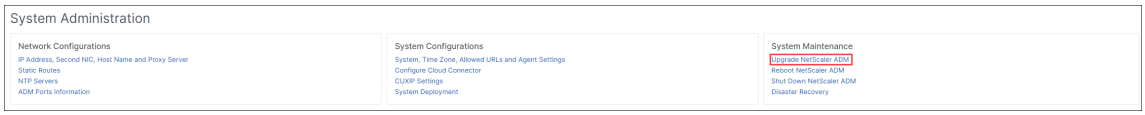
  Pour éviter ce problème, passez à la version 13.1.33.50.

- Pour les serveurs NetScaler ADM en 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.

Mettre à niveau un seul serveur NetScaler ADM vers la version 14.1 4.x

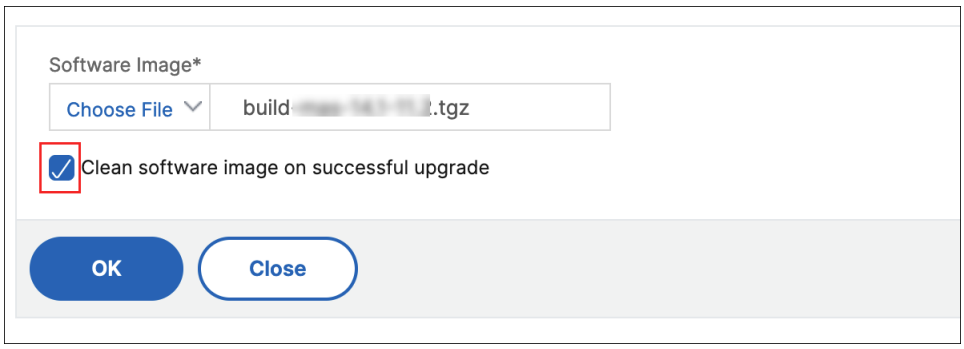
1. Connectez-vous à NetScaler ADM à l'aide des informations d'identification de l'administrateur.
2. Accédez à **Paramètres** > **Administration** . Sous **Maintenance du système**, cliquez sur **Mettre à niveau NetScaler ADM**.



3. Sur la page **Mettre à niveau NetScaler** ADM, cochez la case **Nettoyer l'image logicielle en cas de mise à niveau réussie pour supprimer les fichiers image** après la mise à niveau. La sélection de cette option supprime automatiquement les fichiers image NetScaler ADM lors de la mise à niveau.

> **Remarque**
>
> Cette option est sélectionnée par défaut. Si vous ne cochez pas cette case avant de lancer 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 génération doit être présent sur l'appliance virtuelle NetScaler 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**

Mettre à niveau une paire haute disponibilité vers la version 14.1

Pour les serveurs NetScaler ADM en mode haute disponibilité, vous pouvez effectuer la mise à niveau en accédant au nœud actif ou à l'adresse IP flottante. Les deux serveurs NetScaler ADM sont automatiquement mis à niveau vers la dernière version une fois que vous lancez le processus de mise à niveau sur l'un des serveurs.

Mettre à niveau le déploiement de reprise après sinistre de NetScaler ADM

> **Remarque :**
>
> Assurez-vous que le mot de passe est le même pour la paire HA et le nœud de reprise après sinistre.

La mise à niveau du déploiement de reprise après sinistre de NetScaler ADM s'effectue en deux étapes :

- Mettez à niveau les nœuds NetScaler 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 NetScaler 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 NetScaler ADM

1. Téléchargez le fichier image de mise à niveau de NetScaler ADM depuis le site NetScaler.

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 NetScaler ADM est un processus 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 NetScaler ADM déployés en haute disponibilité.
2. Mettez à niveau le nœud de reprise après sinistre NetScaler ADM.

   Pour plus d'informations, consultez la section Mettre à niveau le déploiement de reprise après sinistre de NetScaler ADM.

Mettre à niveau l'agent sur site

1. Téléchargez le fichier image de mise à niveau de l'agent NetScaler ADM depuis le site NetScaler.
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.
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 NetScaler ADM

Si vos besoins de stockage NetScaler ADM dépassent l'espace disque par défaut (120 Go), vous pouvez connecter un disque supplémentaire. Vous pouvez attacher plus de disque dans les déploiements mono-serveur et haute disponibilité.

Lorsque vous mettez à niveau NetScaler ADM à partir des versions 12.1-13.10, les partitions que vous aviez créées sur le disque supplémentaire dans la version précédente restent les mêmes. Les partitions ne sont ni supprimées ni redimensionnées.

La procédure pour connecter un disque supplémentaire reste la même dans la version mise à niveau. Vous pouvez désormais utiliser le nouvel outil de partitionnement de disque de NetScaler ADM pour créer des partitions sur le disque récemment ajouté. Vous pouvez également utiliser l'outil pour redimensionner les partitions dans le disque supplémentaire existant. Pour plus d'informations sur l'attachement de disques supplémentaires et sur l'utilisation du nouvel outil de partitionnement de disque, consultez Comment associer un disque supplémentaire à NetScaler ADM.

Authentification

February 1, 2024

Les utilisateurs peuvent être authentifiés soit en interne par NetScaler ADM, soit en externe par un serveur d'authentification, soit les deux. Si l'authentification locale est utilisée, l'utilisateur doit figurer dans la base de données de sécurité NetScaler 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.

NetScaler 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. NetScaler 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 NetScaler 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 NetScaler ADM.

Serveurs d'authentification externes

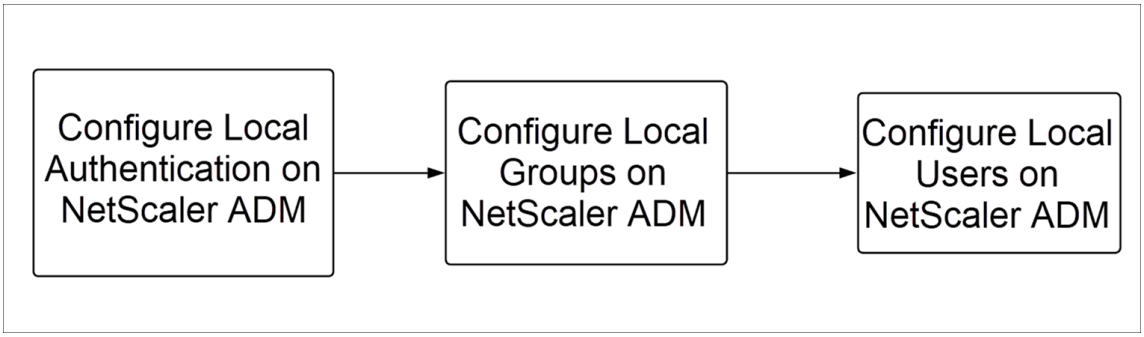
NetScaler ADM envoie toutes les demandes de service d'authentification, d'autorisation et d'audit au serveur RADIUS, LDAP ou TACACS distant. Le serveur d'authentification, d'autorisation et d'audit à distance reçoit la demande, la valide et envoie une réponse à NetScaler ADM. Lorsqu'il est configuré pour utiliser un serveur RADIUS, TACACS ou LDAP distant pour l'authentification, NetScaler 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.

Vous pouvez également utiliser la base de données interne de NetScaler 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.

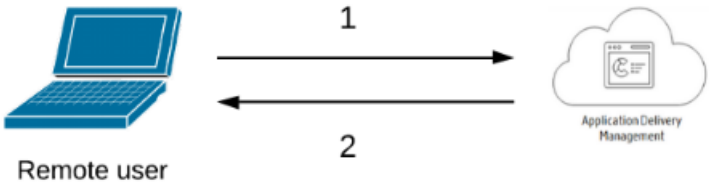
Authentifier les utilisateurs dans NetScaler ADM

Vous pouvez authentifier vos utilisateurs dans NetScaler ADM de deux manières :

- Utilisateurs locaux configurés dans NetScaler ADM



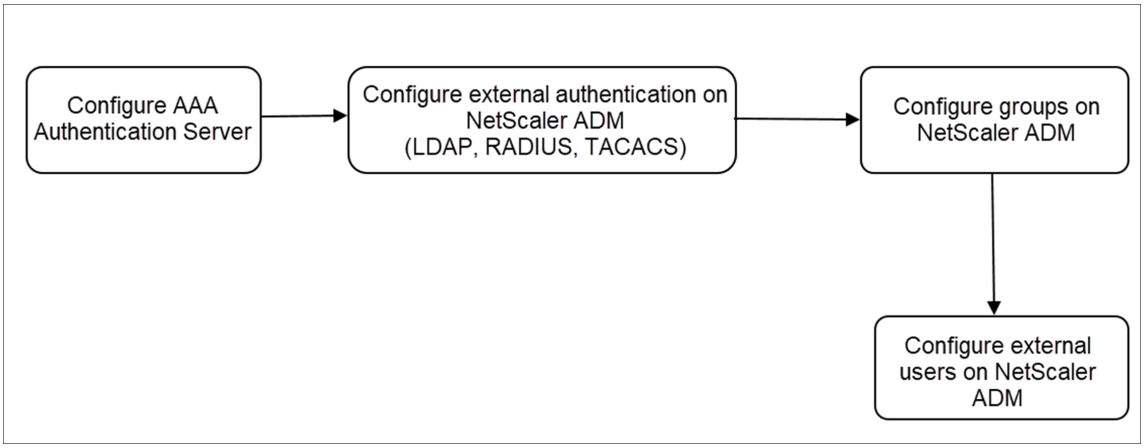
Après la configuration, ce qui suit est le flux de travail pour l'authentification de l'utilisateur sur le serveur local.



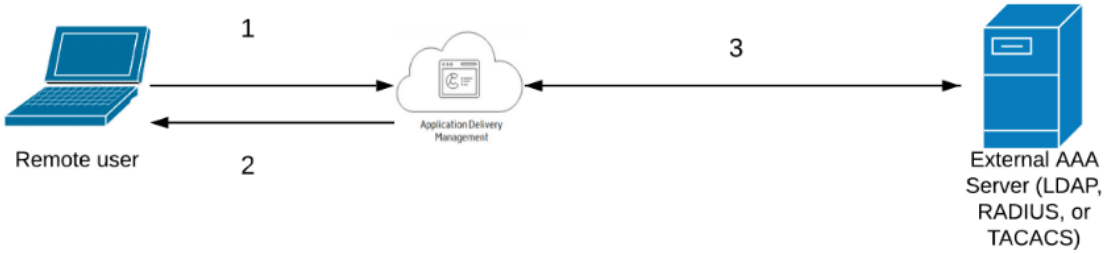
1 —L'utilisateur se connecte à NetScaler ADM

2 —NetScaler ADM invite les utilisateurs à entrer des 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 NetScaler ADM

2 —NetScaler ADM invite l'utilisateur à entrer ses informations d'identification

3 —NetScaler ADM valide les informations d'identification de l'utilisateur à l'aide du 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 NetScaler ADM

February 1, 2024

Après avoir configuré le serveur LDAP, RADIUS ou TACACS, vous pouvez ajouter ces serveurs dans NetScaler 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 **Paramètres > 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

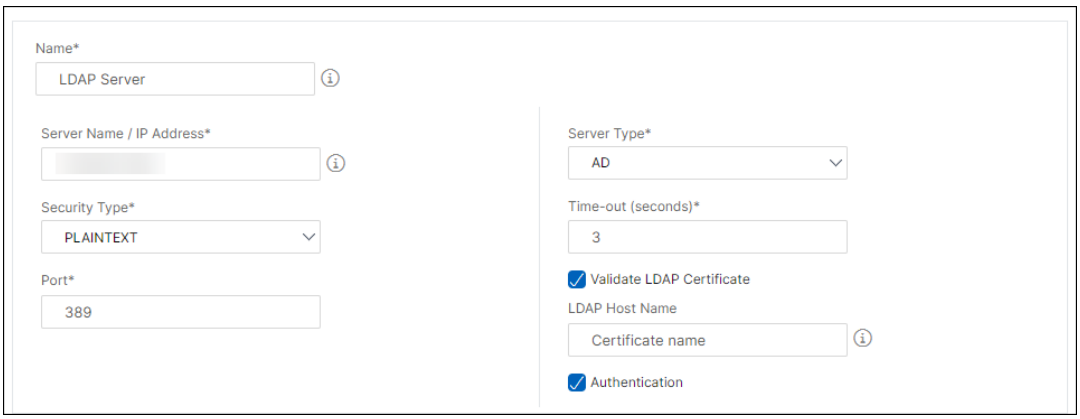
d) **Port** —Par défaut, le port 389 est utilisé pour PLAINTEXT. Vous pouvez également spécifier le port 636 pour SSL/TLS

e) **Type de serveur** : sélectionnez Active Directory (AD) ou Novell Directory Service (NDS) comme type de serveur LDAP

f) **Délai d'attente (secondes)** : délai en secondes pendant lequel le système NetScaler 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.



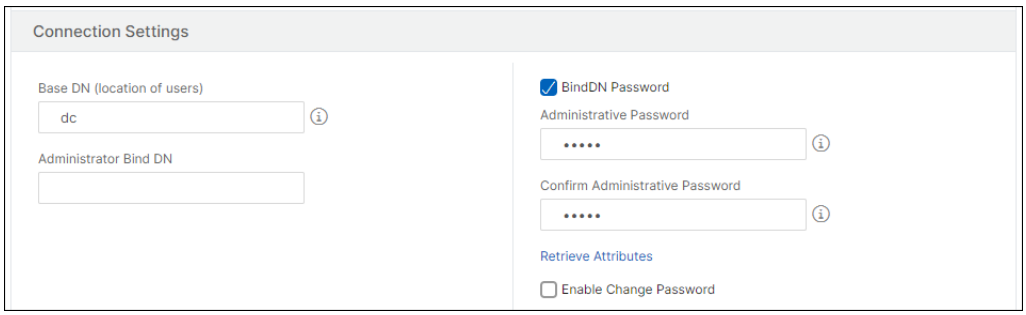
Sous Paramètres de connexion, spécifiez les paramètres suivants :

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.

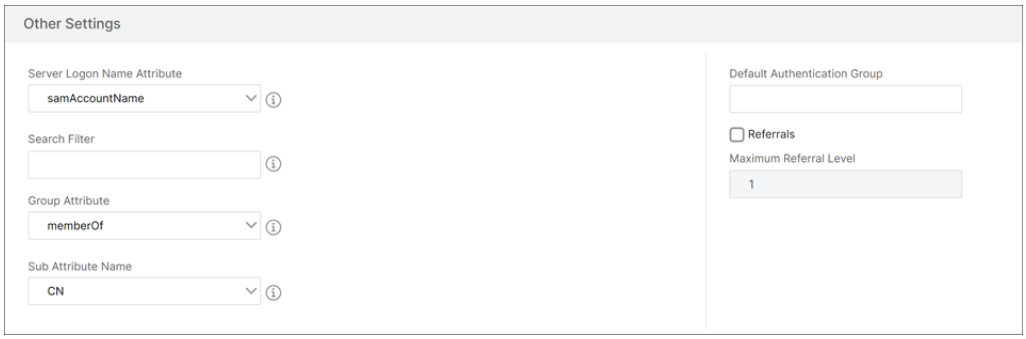
ii. **Filtre de recherche** : configurez les utilisateurs externes pour l'authentification à deux facteurs en fonction du filtre de recherche configuré dans le serveur LDAP. Par exemple, vpnallowed=true avec ldaploginame `samaccount` et le nom d'utilisateur bob fourni par l'utilisateur donnerait une 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 membres du groupe Active Directory, le nom du groupe et celui des utilisateurs sur NetScaler ADM doivent porter le même nom que celui des membres du groupe Active Directory.

5. Activez les serveurs d'authentification externes.

   Pour plus d'informations sur l'activation des serveurs d'authentification externes, voir Activer les serveurs d'authentification externes et les options de secours.

Ajouter un serveur d'authentification RADIUS

February 1, 2024

1. Accédez à **Paramètres > 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

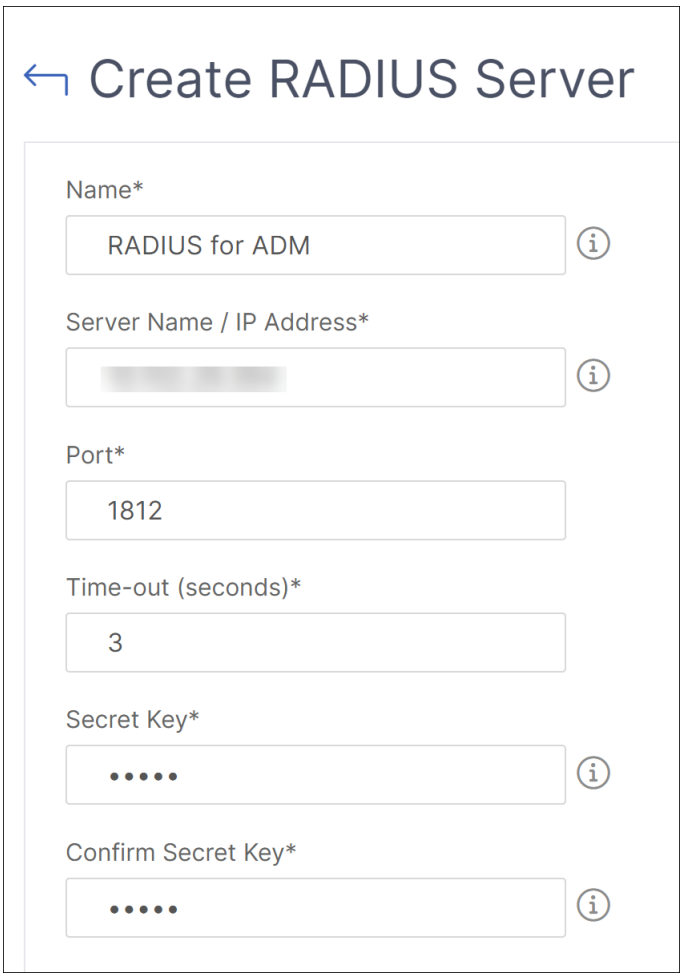
   b) **Nom du serveur/adresse IP** —Spécifiez l'adresse IP du serveur RADIUS

   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)** : délai en secondes pendant lequel le système NetScaler 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 four-

nisseur 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.

4. Activez les serveurs d'authentification externes.

   Pour plus d'informations sur l'activation des serveurs d'authentification externes, voir Activer les serveurs d'authentification externes et les options de secours.

Ajouter un serveur d'authentification TACACS

February 1, 2024

1. Accédez à **Paramètres > 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)** : délai en secondes pendant lequel le système NetScaler ADM attend une réponse du serveur LDAP

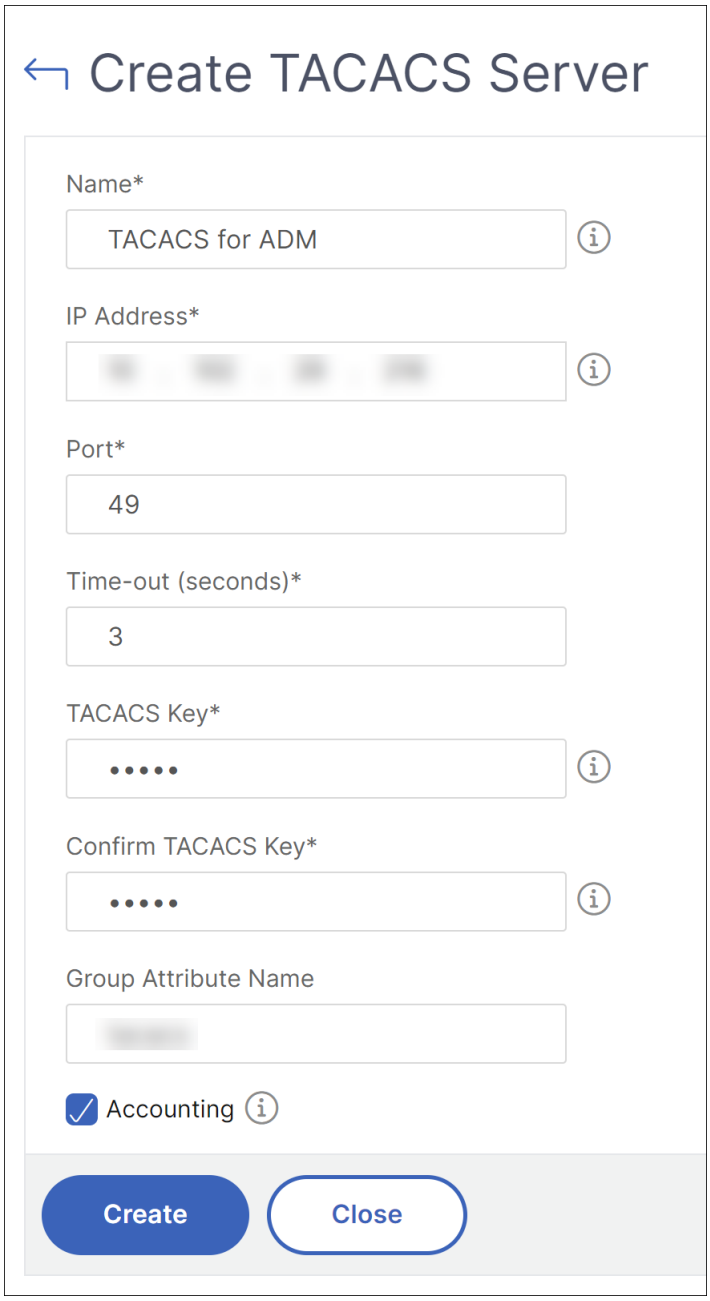
   e) Clé**TACACS** —Spécifiez la clé TACACS pour l'authentification

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**.



5. Activez les serveurs d'authentification externes.

Pour plus d'informations sur l'activation des serveurs d'authentification externes, voir Activer les serveurs d'authentification externes et les options de secours.

Utilisateurs de NetScaler ADM

February 1, 2024

Vous pouvez créer des comptes utilisateurs localement sur NetScaler 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 utilisent Active Directory, assurez-vous que le nom du groupe dans NetScaler ADM est identique à celui du groupe Active Directory sur le serveur externe.

Groupes d'utilisateurs dans NetScaler ADM

NetScaler 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 NetScaler 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 NetScaler ADM et utiliser l'authentification locale pour les utilisateurs des groupes. Si vous utilisez des serveurs externes pour l'authentification, configurez les groupes sur NetScaler 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 le nom d'un groupe correspond à celui d'un groupe sur un serveur d'authentification, l'utilisateur hérite des paramètres du groupe sur NetScaler ADM.
Si vous utilisez l'authentification locale, créez des utilisateurs et ajoutez-les aux groupes configurés sur NetScaler 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 sur le serveur TACACS est prise en charge à partir de **NetScaler ADM 13.0**.

NetScaler 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:

- Il n'est pas nécessaire de créer des utilisateurs dans NetScaler ADM, car ils sont gérés sur le serveur externe.
- NetScaler ADM autorise les utilisateurs en attribuant des autorisations de groupe pour accéder à des serveurs virtuels d'équilibrage de charge spécifiques et à des applications spécifiques du système.

Activer les serveurs d'authentification externes et les options de secours

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 NetScaler ADM et sur un serveur d'authentification externe peut se connecter à NetScaler ADM, même si les serveurs d'authentification externes configurés sont hors service ou inaccessibles. Pour garantir le fonctionnement de l'authentification de secours :

- Les utilisateurs non-NSroot doivent pouvoir accéder à NetScaler ADM si le serveur externe est en panne ou inaccessible
- Vous devez ajouter au moins un serveur externe

NetScaler 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.

NetScaler ADM peut authentifier les utilisateurs quels que soient les protocoles utilisés pour communiquer 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, NetScaler 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 NetScaler 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. NetScaler ADM tente de s'authentifier auprès des serveurs externes, en fonction des configurations. Dans cet exemple de scénario, NetScaler 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.

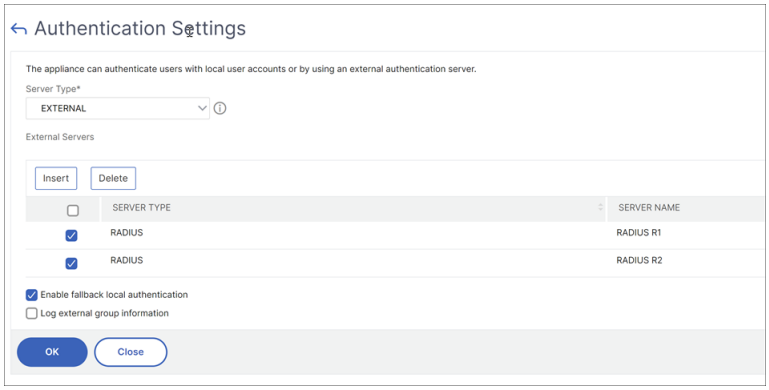
> Remarque
>
> Vous pouvez configurer jusqu'à 32 serveurs d'authentification externes dans NetScaler ADM.

Configurer des serveurs externes de secours et en cascade

1. Accédez à **Paramètres > 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. NetScaler Application Delivery Management (ADM) fournit une méthode d'authentification des utilisateurs locaux et externes. Alors que les utilisateurs locaux sont authentifiés en interne, NetScaler ADM prend en charge l'authentification externe avec les protocoles RADIUS, LDAP et TACACS. Lorsqu'un utilisateur tente d'accéder à NetScaler 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 authentification. Une fois authentifié, le protocole requis est utilisé pour identifier l'utilisateur sur NetScaler 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. NetScaler ADM permet un contrôle d'accès précis basé sur les rôles (RBAC) grâce auquel les administrateurs peuvent fournir des autorisations d'accès aux utilisateurs en fonction des rôles de chaque utilisateur au sein d'une entreprise. Le RBAC dans NetScaler ADM est obtenu en créant des stratégies d'accès, des rôles, des groupes et des utilisateurs.

Contrôle d'accès sur rôle

February 1, 2024

NetScaler ADM fournit un contrôle d'accès détaillé basé sur les rôles (RBAC), grâce auquel 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 NetScaler ADM, la création de rôles et de stratégies est spécifique à la fonctionnalité RBAC de NetScaler. 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 du groupe ADC, est le super administrateur de NetScaler ADM au sein de 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.

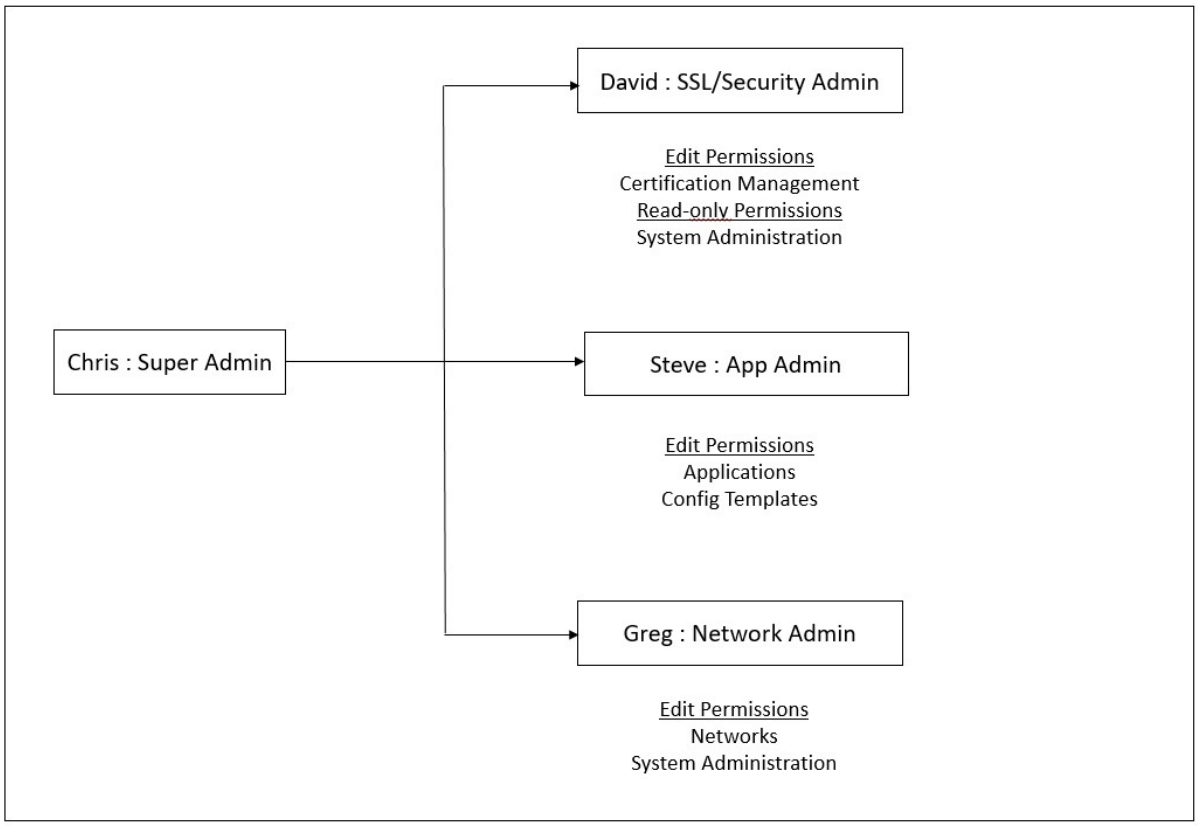
Steve, administrateur d'applications, a besoin d'accéder uniquement à des applications spécifiques et uniquement à des modèles de configuration spécifiques.

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 de NetScaler ADM peuvent être authentifiés localement ou 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

Le RBAC n'est pas entièrement pris en charge pour les fonctionnalités suivantes de NetScaler ADM :

- **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 WAF Security Violations. 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 NetScaler ADM, les StyleBooks et les packs de configuration sont considérés comme des ressources distinctes. Les autorisations d'accès, que ce soit pour afficher, modifier ou les deux, peuvent être fournies pour StyleBook et les packs de configuration séparément ou simultanément. Une autorisation d'affichage ou de modification sur les packs de configuration permet implicitement à l'utilisateur de visualiser les StyleBooks, ce qui est essentiel pour obtenir les détails du pack de configuration et créer les packs de configuration.
  - L'autorisation d'accès pour un StyleBook ou des 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 NetScaler 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. NetScaler Application Delivery Management (ADM) fournit quatre stratégies d'accès prédéfinies :

1. **adminpolicy**. Autorise l'accès à toutes les fonctionnalités de NetScaler ADM. L'utilisateur dispose à la fois d'autorisations d'affichage et de modification, peut consulter tout le contenu de NetScaler 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 consulter tout le contenu sur NetScaler ADM, mais il n'est pas autorisé à effectuer des opérations.
3. **appAdminPolicy**. Accorde des autorisations administratives pour accéder aux fonctionnalités de l'application dans NetScaler 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 NetScaler ADM, accédez à **Paramètres > Utilisateurs et rôles > 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 de NetScaler ADM, avec des options permettant de spécifier l'accès en lecture seule, d'activer/désactiver ou de modifier.
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 NetScaler ADM.
   - **Activer-Désactiver :** cette option est disponible uniquement pour les fonctionnalités des **fonctions réseau** qui permettent d'activer ou de désactiver une action sur NetScaler 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.

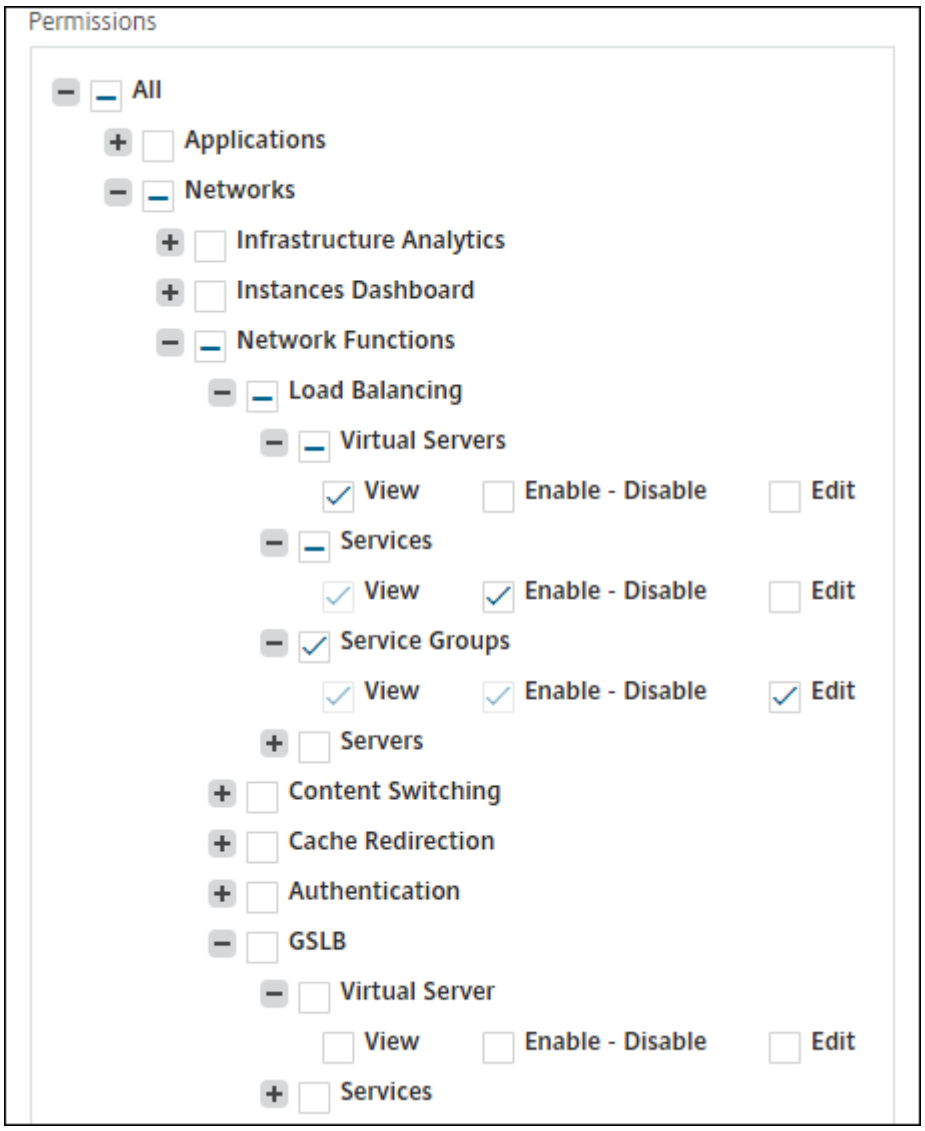
- **Modifier :** Cette option accorde l'accès complet à l'utilisateur. L'utilisateur peut modifier la fonction et ses fonctions.

  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 davantage d'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 consulter les serveurs virtuels d'équilibrage de charge dans NetScaler ADM. Pour afficher les serveurs virtuels, accédez à **Infrastructure > 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 **Infrastructure > Fonctions réseau > Équilibrage de charge** et sélectionnez l'onglet **Services** .

> **Remarque :**

> Si un utilisateur dispose de l'autorisation **Activer-Désactiver**, l'action d'activation ou de désactivation sur un service est limitée dans la page suivante :
>
> a) Accédez à **Infrastructure > Fonctions 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**.

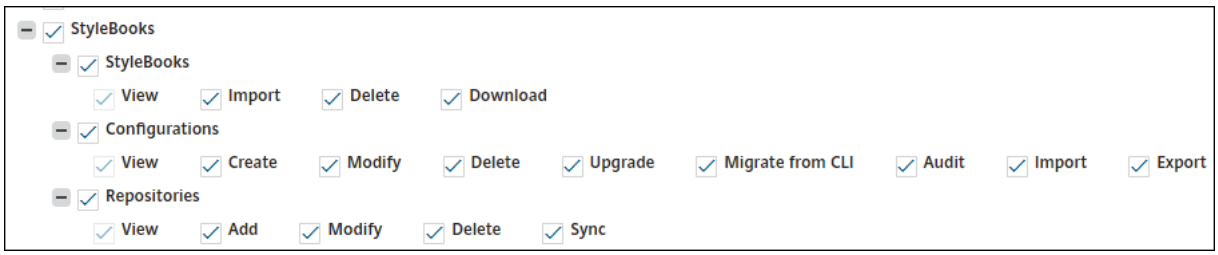
L'autorisation de **modification** est accordée à un utilisateur pour la fonctionnalité **Groupes de services** . Cette autorisation accorde l'accès complet lorsque les autorisations **Afficher** et **Activer/Désactiver** sont accordées. L'utilisateur peut modifier les groupes de services liés à un serveur virtuel d'équilibrage de charge. Pour modifier des groupes de services, accédez à **Infrastructure > 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 NetScaler ADM, un groupe peut disposer d'un accès au niveau des fonctionnalités et au niveau des ressources. Par exemple, un groupe d'utilisateurs peut avoir accès uniquement à certaines instances NetScaler, un autre groupe ne disposant que de quelques applications sélectionnées, etc.

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. Tous les utilisateurs de ce groupe se voient attribuer les mêmes droits d'accès dans NetScaler ADM.

Vous pouvez gérer l'accès d'un utilisateur dans NetScaler ADM au niveau individuel des entités fonctionnelles du réseau. Vous pouvez attribuer dynamiquement des autorisations spécifiques à l'utilisateur ou au groupe au niveau de l'entité.

NetScaler ADM traite les serveurs virtuels, les services, les groupes de services et les serveurs comme des entités fonctionnelles du réseau.

- **Serveur virtuel (applications)** : équilibrage de charge (lb), GSLB, commutation de contexte (CS), redirection du cache (CR), authentification (`Auth`) et NetScaler 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 NetScaler ADM, accédez à **Paramètres > Utilisateurs et rôles**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. La longueur maximale autorisée est de 64 caractères.
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**.

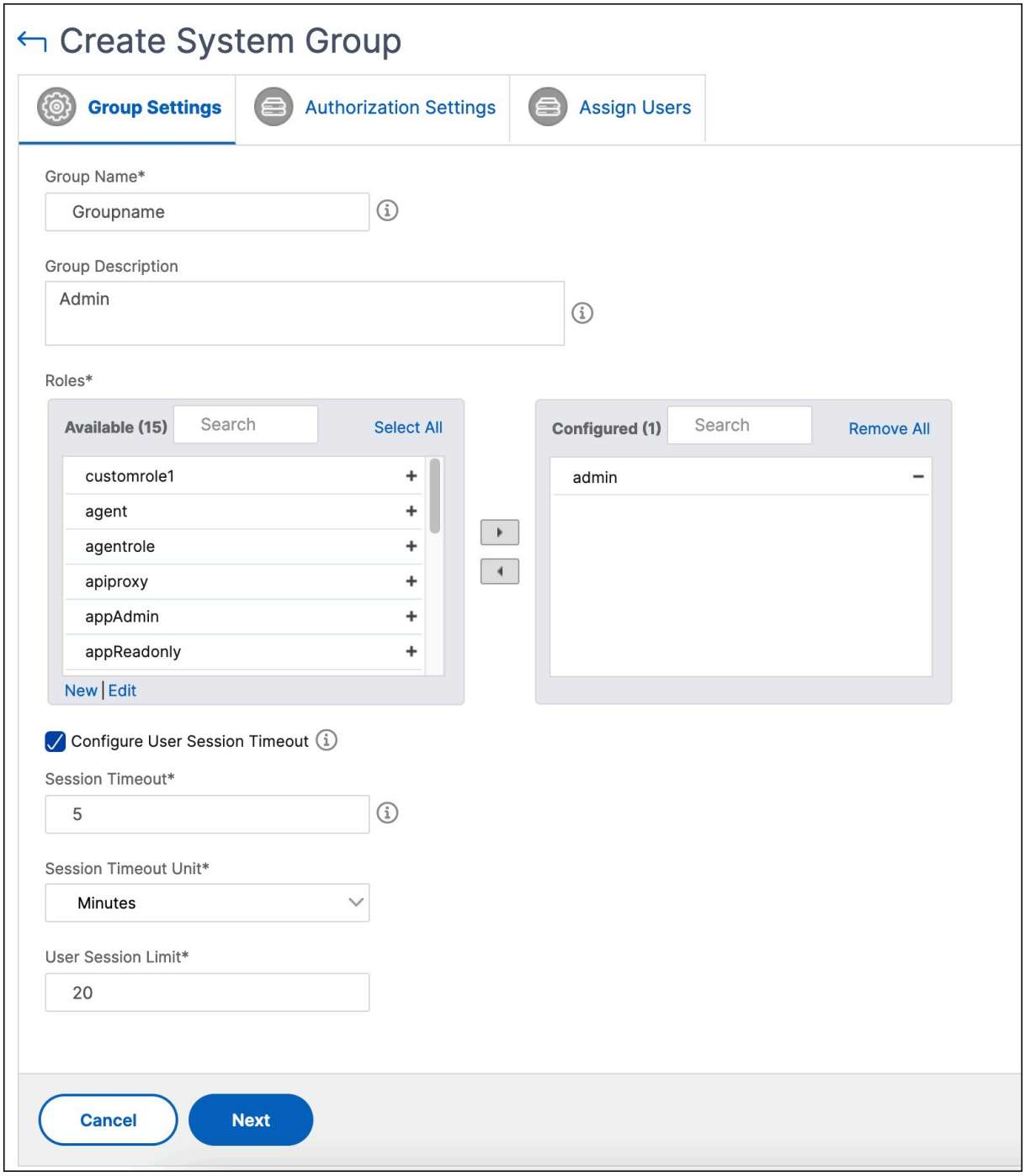
   > **Remarque :**
   >
   > Dans la liste **Disponible**, vous pouvez cliquer sur **Nouveau** ou **Modifier** et créer ou modifier des rôles. Vous pouvez également accéder à **Paramètres > Utilisateurs et rôles > Utilisateurs** et créer ou modifier des utilisateurs.
6. Sélectionnez **Configurer le délai d'expiration de la session utilisateur** pour configurer la période pendant laquelle un utilisateur doit rester actif.

   Lorsque cette option est activée, spécifiez les paramètres suivants :

- **Délai d'expiration de la session** : entrez la durée pendant laquelle une session utilisateur doit rester active. La valeur par défaut est 15.
- **Unité de délai d'expiration de session** : sélectionnez l'unité de délai d'expiration dans la liste, en minutes ou en heures. La valeur par défaut est en minutes.

7. Dans le champ **Limite de session utilisateur**, entrez le nombre maximum de sessions autorisées par utilisateur.

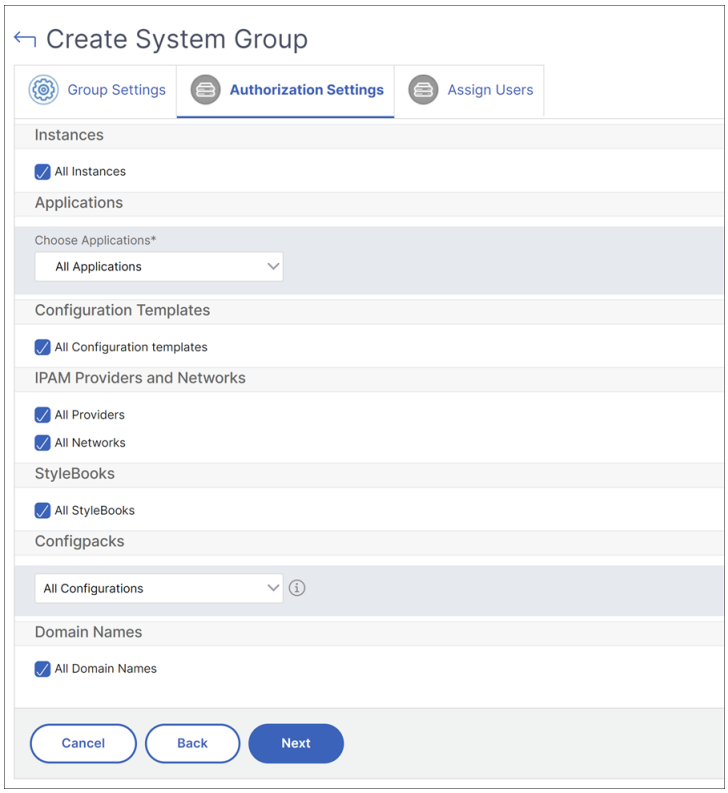
> **Remarque :**
>
> Vous pouvez configurer jusqu'à 40 sessions utilisateur. Par défaut, 20 sessions utilisateur vous sont attribuées. Toutefois, si vous appartenez aux groupes d'administrateurs et d'utilisateurs en lecture seule, 40 sessions utilisateur vous sont attribuées par défaut et cette valeur ne peut pas être modifiée.



1. 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
- Packs de configuration
- 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) Décochez la case **Tous les groupes AutoScale** et cliquez sur **Ajouter des groupes AutoScale**.

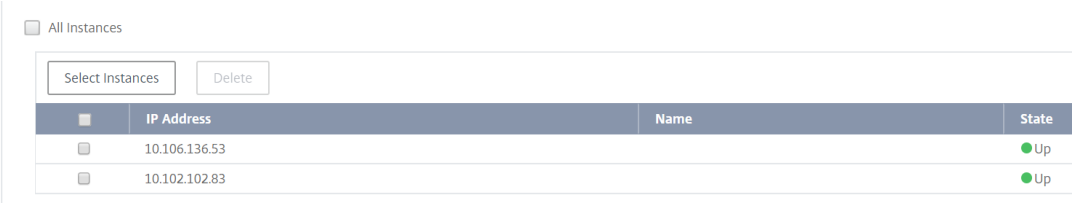
b) Sélectionnez les groupes Autoscale requis dans la liste et cliquez sur **OK**.

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. 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.

Les options suivantes sont disponibles :

- **Toutes les applications :** cette option est sélectionnée par défaut. Il ajoute toutes les applications présentes dans NetScaler 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 **Appliquer également aux entités liées**, NetScaler ADM autorise toutes les entités liées à l'application sélectionnée.

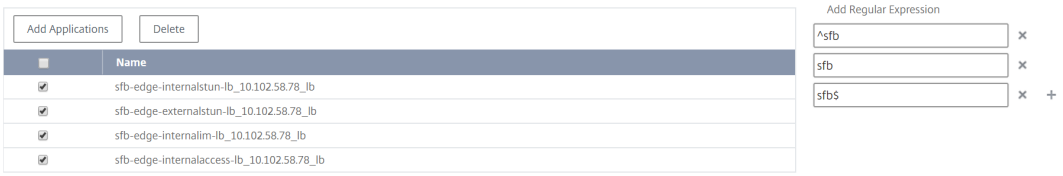
  > **Remarque :**
  >
  > Pour autoriser les entités liées, sélectionnez un seul type d'entité.

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 NetScaler ADM. Pour ajouter une expression régulière, procédez comme suit :

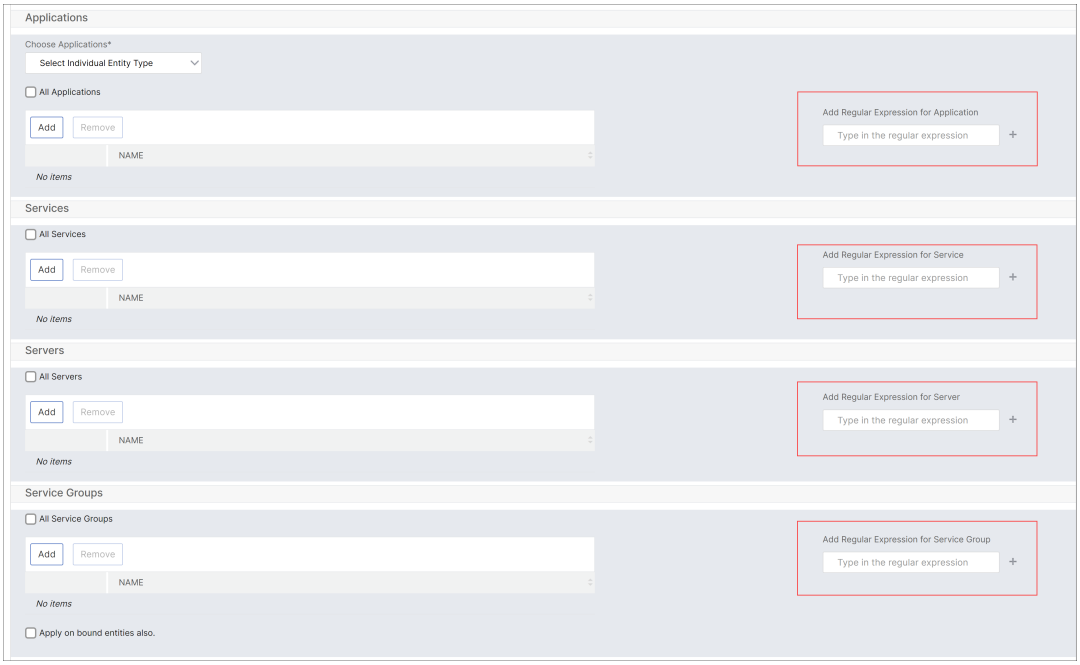
a) Cliquez sur **Ajouter une expression régulière**.

b) Spécifiez l'expression régulière dans la zone de texte.

L'image suivante explique comment utiliser une 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, NetScaler 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) Décochez la case **Tous les StyleBooks** et cliquez sur **Ajouter 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`.

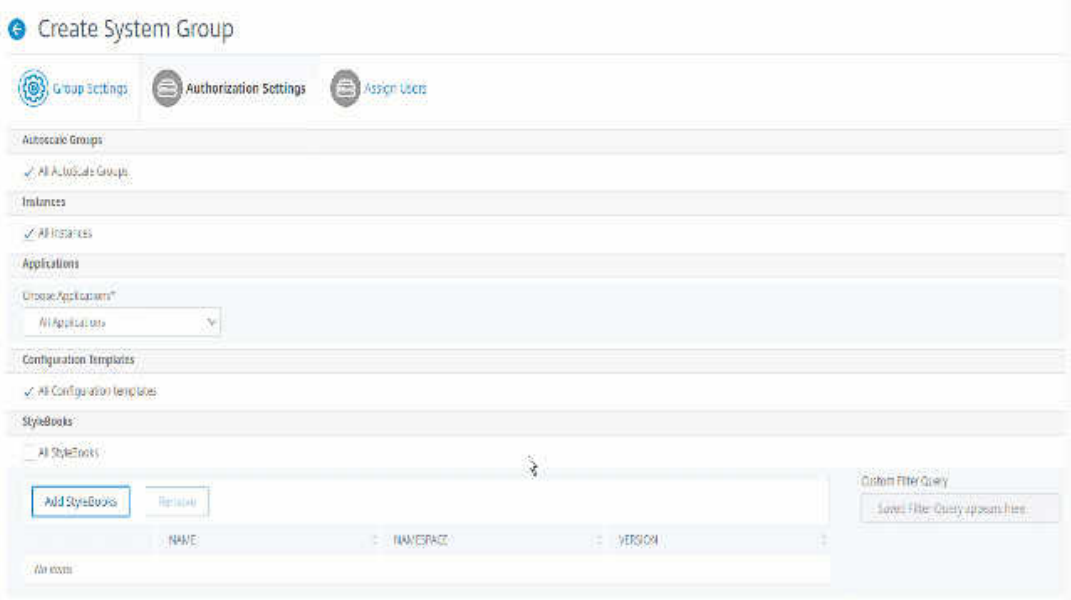
Utilisez un opérateur `Or` entre des expressions de valeur définie à l'expression clé.

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.

Packs de configuration :

Dans les **packs de configuration** , sélectionnez l'une des options suivantes :

- **Toutes les configurations** : cette option est sélectionnée par défaut. Il permet aux utilisateurs de gérer toutes les configurations présentes 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 des configurations spécifiques à n'importe quel StyleBook.
- **Toutes les configurations créées par le groupe d'utilisateurs** : cette option permet aux utilisateurs d'accéder uniquement aux configurations créées par les utilisateurs du même groupe.

Vous pouvez sélectionner les packs de configuration applicables lorsque vous créez des groupes et que vous attribuez des utilisateurs à ce groupe.

Noms de domaine :

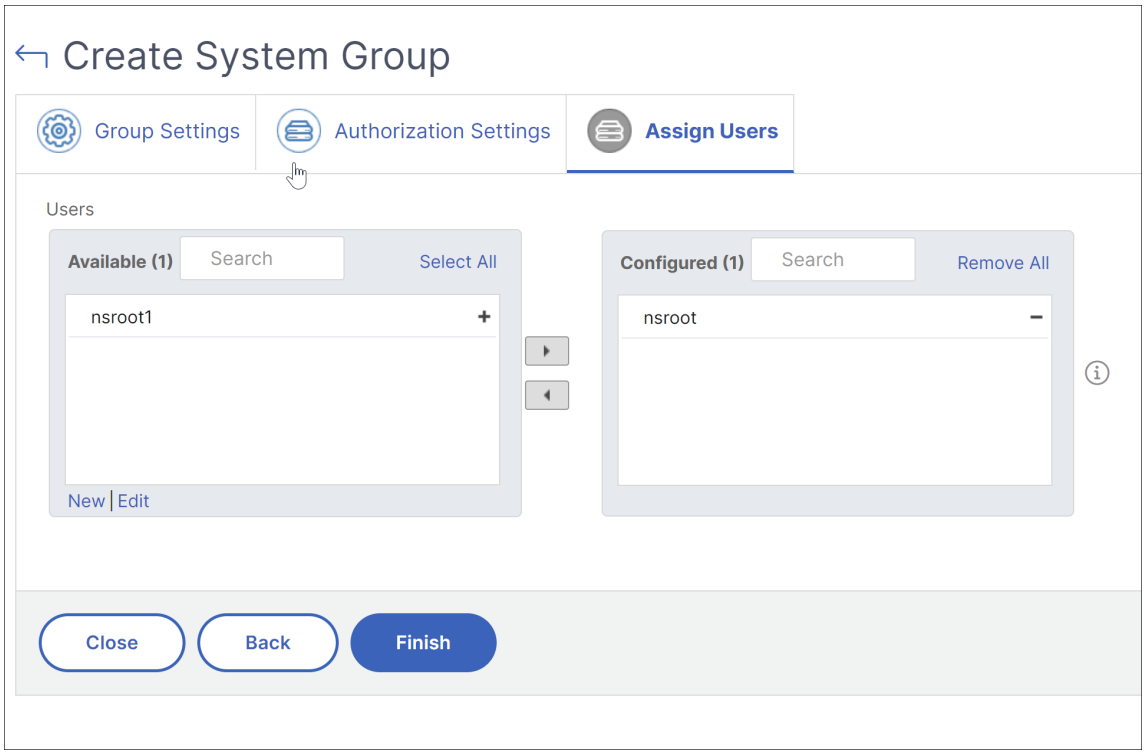
Si vous souhaitez sélectionner le nom de domaine spécifique qu'un utilisateur peut consulter ou gérer, procédez comme suit :

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**.

2. Cliquez sur **Créer un groupe**.
3. 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**.



4. 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 fonctionnelles du réseau dans NetScaler 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. Reportez-vous à la section Configurer des groupes sur NetScaler 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**
>
> NetScaler ADM traite les serveurs virtuels, les services, les groupes de services et les serveurs comme des entités fonctionnelles du 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 également aux entités liées** est désactivée. Dans le cas contraire, NetScaler ADM autorise 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 de nouvelles entités correspondent à l'expression régulière de leur type d'entité, NetScaler ADM peut accorder de manière dynamique aux utilisateurs l'accès aux 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.

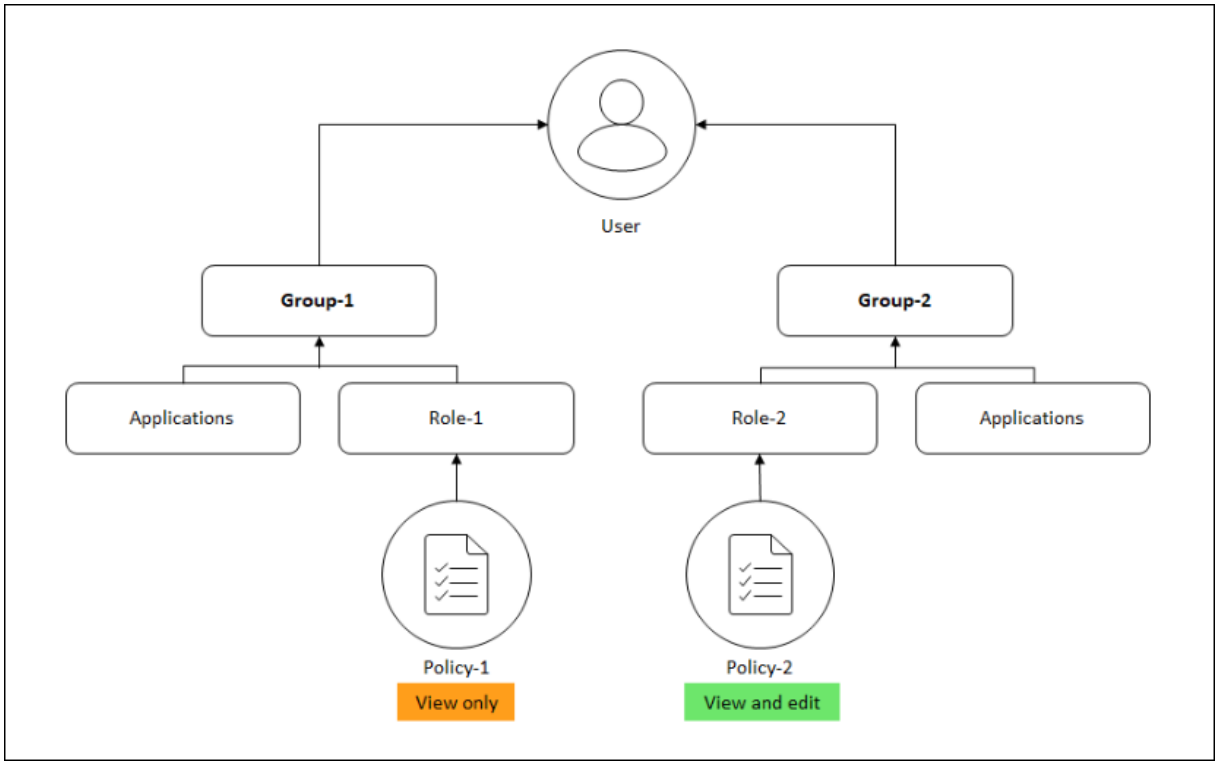
Comment l'accès utilisateur change en fonction de la portée d'autorisation

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 du RBAC lors de la mise à niveau de NetScaler ADM de la version 12.0 vers les versions ultérieures

Lorsque vous effectuez la mise à niveau de NetScaler ADM de la version 12.0 vers la version 13.1, les options permettant de fournir des autorisations de « lecture-écriture » ou de « lecture » ne s'affichent pas lors de la création de groupes. Ces autorisations sont remplacées par des « 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 la version 13.1 :

12.0	Autoriser les applications uniquement	13.1
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 NetScaler 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 accorder l'autorisation d'ajouter des instances NetScaler dans NetScaler ADM, tandis que l'autre stratégie peut accorder l'autorisation de créer et de déployer des StyleBooks et de configurer des instances NetScaler.

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.

NetScaler ADM propose quatre rôles prédéfinis :

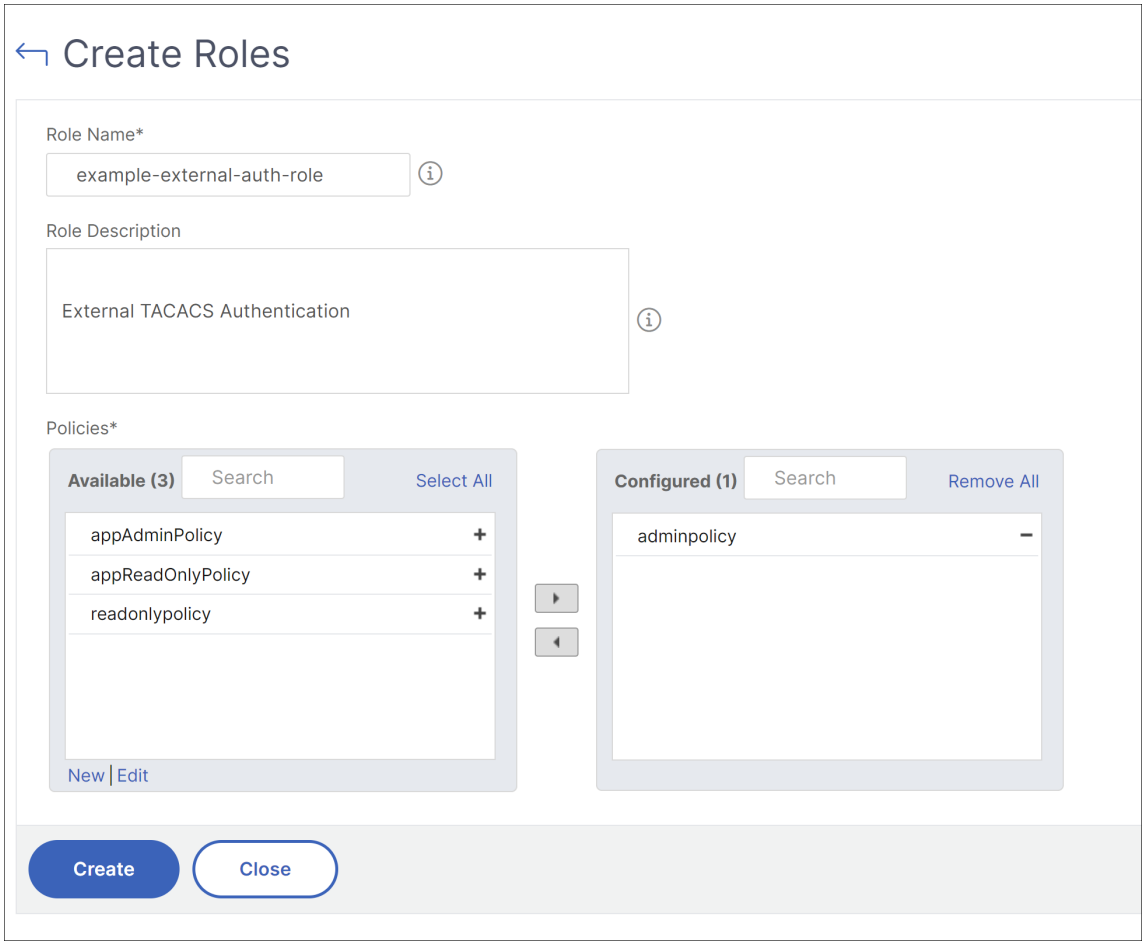
- **admin**. A accès à toutes les fonctionnalités de NetScaler ADM. (Ce rôle est lié à adminpolicy.)
- **readonly**. Accès en lecture seule. (Ce rôle est lié à la stratégie de lecture uniquement.)
- **appAdmin**. Dispose d'un accès administratif uniquement aux fonctionnalités de l'application dans NetScaler 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 NetScaler ADM, accédez à **Paramètres > Utilisateurs et 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, NetScaler Application Delivery Management (ADM) compte un utilisateur :

nsroot : l'utilisateur root (nsroot) dispose de privilèges d'administration complets sur l'appliance. L'utilisateur nsroot est le super administrateur de NetScaler ADM.

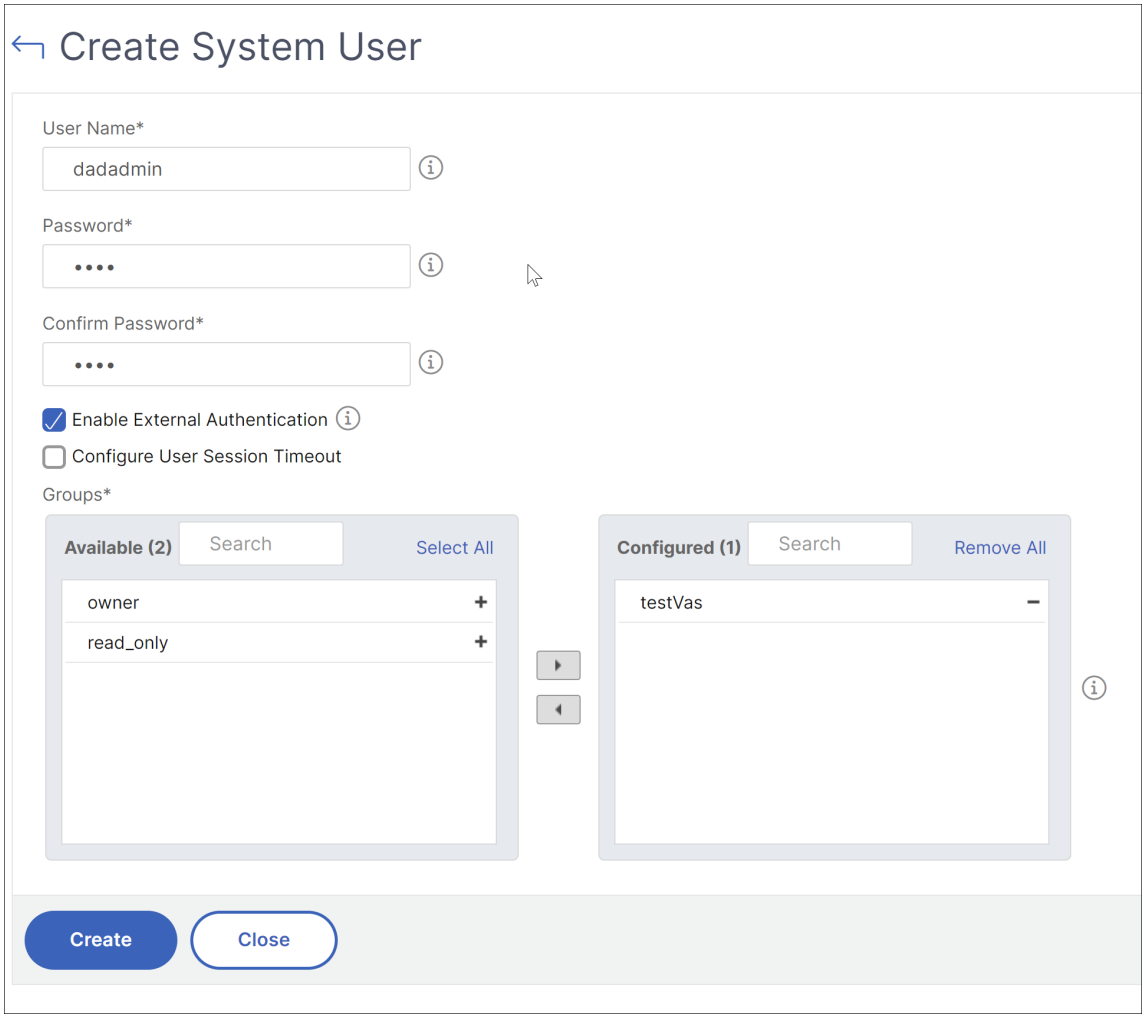
Vous pouvez créer des utilisateurs supplémentaires en configurant des comptes pour eux. Lorsque vous ajoutez de nouveaux utilisateurs à NetScaler ADM, vous pouvez définir leurs autorisations en leur attribuant les groupes, les rôles et les stratégies appropriés.

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 les utilisateurs dans NetScaler ADM :

1. Dans NetScaler ADM, accédez à **Paramètres > Utilisateurs et rôles**.
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 NetScaler 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**.

Tâches réalisables et recommandations

February 1, 2024

> **Remarque :**
>
> - L'onglet **Tâches** est renommé **Recommandations**. Dans **Recommandations**, vous pouvez continuer à passer en revue les tâches existantes et cliquer sur **Guidez-moi** pour terminer la tâche.
> - L'onglet **Archive** n'est plus disponible. Au lieu de cela, vous pouvez choisir de **rejeter** une recommandation de la liste.

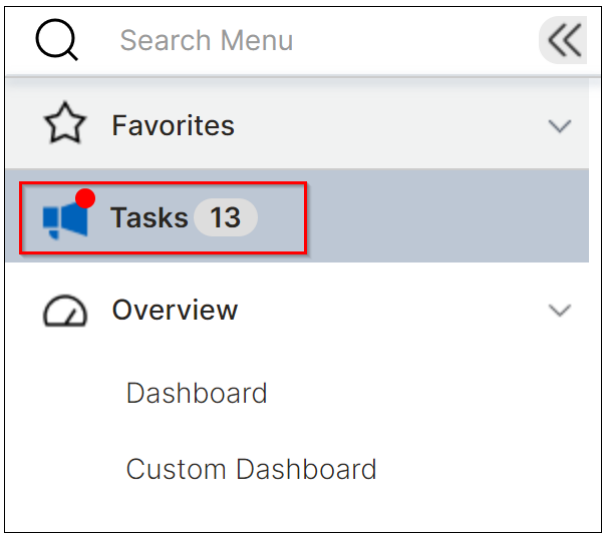
Vous avez peut-être découvert des centaines d'instances NetScaler et configuré plusieurs serveurs virtuels (applications) à partir de chaque instance. En tant qu'administrateur, vous devez vous assurer que toutes les instances NetScaler et vos applications sont gérées efficacement afin d'obtenir des informations permettant de mieux hiérarchiser les priorités et de résoudre les problèmes.

Au fur et à mesure que vous étendez votre infrastructure, vous devrez peut-être également vous concentrer sur les problèmes critiques qui ont un impact sur vos instances et applications et qui nécessitent votre attention immédiate. Vous devez également vous assurer que votre déploiement NetScaler ADM est efficace, sécurisé et conforme. En fonction de votre utilisation actuelle et de votre abonnement, la fonctionnalité **Tâches** de NetScaler ADM vous permet de visualiser à la fois les tâches **réalisables nécessitant** une action immédiate **et** les recommandations pour garantir un déploiement efficace.

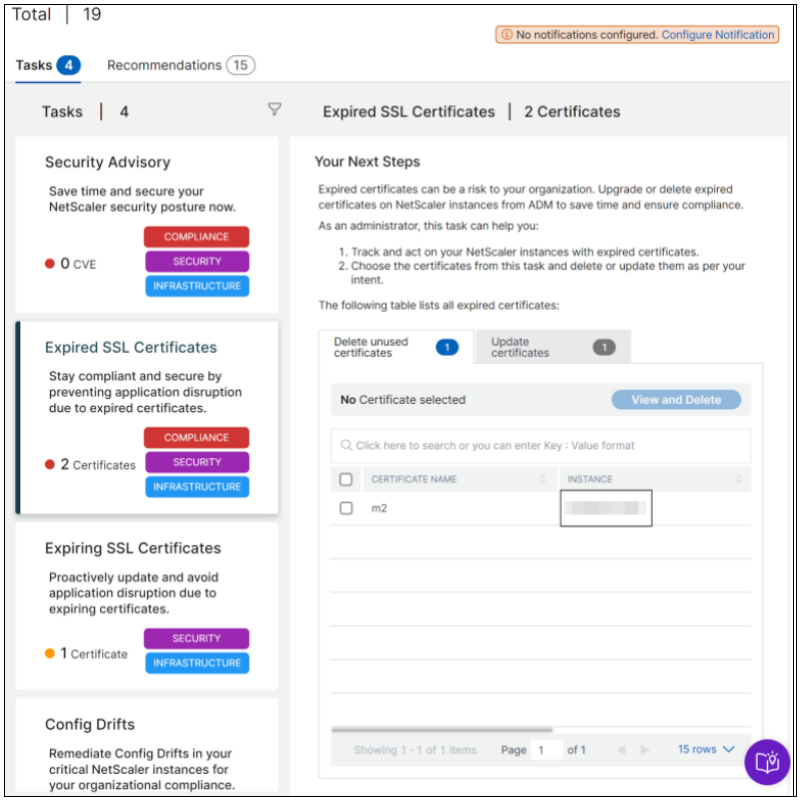
En tant qu'administrateur, en utilisant ces **tâches** et **recommandations**exploitables, vous pouvez :

- Bénéficiez d'une visibilité instantanée sur les observations ou les problèmes qui nécessitent une action immédiate de votre part.
- Configurez les notifications pour recevoir des notifications chaque fois que NetScaler ADM détecte des tâches et prend des mesures proactives.
- Réalisez un déploiement efficace des instances NetScaler ADM et NetScaler.
- Réduisez le temps et les efforts nécessaires à l'identification des problèmes critiques.
- Assurez-vous d'utiliser toutes les fonctionnalités de NetScaler ADM, de permettre la découverte du produit et les fonctionnalités recommandées par le produit pour une administration efficace du déploiement.

Dans l'interface graphique de NetScaler ADM, cliquez sur **Tâches** pour afficher à la fois les **tâches** et les **recommandations**.

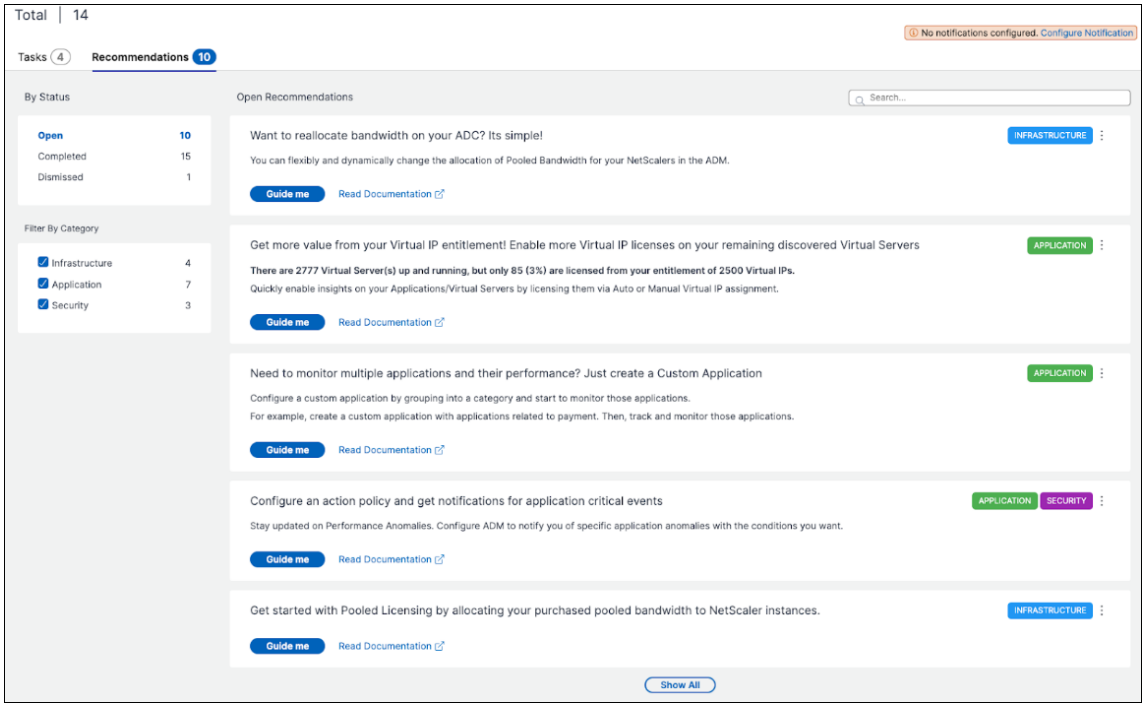


- **Tâches** : vous permet de consulter la liste des tâches qui nécessitent votre attention et votre action immédiates. Au fur et à mesure que vous étendez votre infrastructure, certains problèmes critiques peuvent passer inaperçus et entraîner une faille de sécurité. Par exemple, les instances NetScaler dotées de CVE nécessitent une attention immédiate et vous devez prendre des mesures immédiates pour vous assurer que les instances s'exécutent dans le build et la version recommandés. Dans **Tâches**, vous pouvez obtenir ces informations immédiatement. Sur la base de votre utilisation actuelle, vous pouvez afficher un total de 4 tâches. Les tâches sont affichées en fonction de leur gravité (critique et moyenne).



- **Recommandations** : fournit certaines recommandations basées sur votre utilisation actuelle afin d'améliorer votre déploiement de NetScaler ADM. Vous pouvez utiliser l'option **Guidez-moi** pour compléter n'importe quelle recommandation. Toute recommandation que vous complétez à l'aide de l'option **Guidez-moi** est déplacée vers Terminée. Vous pouvez également rejeter toutes les recommandations et celles-ci seront placées dans la catégorie **Rejetées** . Pour consulter vos recommandations rejetées, utilisez le filtre **Par statut** et sélectionnez **Rejeté** pour voir ces recommandations rejetées.

  Vous pouvez également utiliser le **filtre par catégorie** pour filtrer des recommandations spécifiques en fonction des catégories (infrastructure, application et sécurité). Vous pouvez également utiliser la barre **de recherche** et saisir les premiers caractères pour accéder à la tâche.



Tâches

Sous **Tâches**, vous pouvez consulter les 4 tâches suivantes en fonction de votre déploiement ADM actuel.

- **Certificats SSL expirés** : fournit des informations sur les certificats SSL expirés installés dans votre NetScaler ADM. Sélectionnez cette tâche pour afficher les onglets suivants :
  - **Supprimer les certificats non utilisés** : affiche les certificats qui ne sont utilisés dans aucune instance NetScaler. Pour terminer la tâche, passez en revue les certificats non utilisés, sélectionnez le certificat, cliquez sur **Afficher et supprimer**.

    Action recommandée : Vous êtes redirigé vers **Infrastructure > Tableau de bord SSL > Certificats SSL expirés**. Pour supprimer un certificat, cliquez sur **Supprimer**. Si vous souhaitez mettre à jour le certificat, sélectionnez-le et cliquez sur **Mettre à jour**. Pour plus d'informations, consultez Comment mettre à jour un certificat installé.
  - **Mettre à jour les certificats** : affiche les certificats déjà expirés. Pour terminer la tâche, passez en revue les certificats, sélectionnez-le et cliquez sur **Afficher et mettre à jour**.

    Action recommandée : Vous êtes redirigé vers **Infrastructure > Tableau de bord SSL > Certificats SSL expirés**. Sélectionnez le certificat et cliquez sur **Mettre à jour** ou **Supprimer**. Pour plus d'informations, consultez Comment mettre à jour un certificat installé.
- **Certificats SSL arrivant à expiration** —Fournit des informations sur les certificats SSL qui sont sur le point d'expirer.

Action recommandée : Sélectionnez cette tâche pour afficher les onglets en fonction du nombre total de jours avant la date d'expiration. Pour terminer la tâche, sélectionnez le certificat dans l'onglet, puis cliquez sur **Afficher et mettre à jour**. Vous êtes redirigé vers la page correspondante dans **Infrastructure > Tableau de bord SSL**. Sélectionnez le certificat et cliquez sur **Mettre à jour**. Pour plus d'informations, consultez Comment mettre à jour un certificat installé.

- **Config Drifts** : fournit des informations sur les écarts de configuration (enregistrement par rapport au diff en cours d'exécution et modèle par rapport au diff en cours d'exécution) dans les instances NetScaler. Sélectionnez cette tâche pour afficher les onglets suivants :

  - **Instances dont la configuration n'est pas enregistrée** : vous pouvez afficher les instances dont la configuration n'est pas enregistrée. Pour terminer la tâche, sélectionnez l'instance, cliquez sur **Afficher et enregistrer la configuration**.

    Action recommandée : Vous êtes redirigé vers **Infrastructure > Configuration > Audit de configuration > Rapports d'audit** et vous pouvez consulter les instances dont les configurations ne sont pas enregistrées. Cliquez sur **Enregistrer la configuration** pour terminer cette tâche. Pour plus d'informations, consultez la documentation.

  - **Instances présentant des déviations par rapport au modèle** : vous pouvez afficher les instances présentant des écarts par rapport au modèle. Pour terminer la tâche, sélectionnez l'instance, cliquez sur **Afficher et exécuter les commandes appropriées**.

    Action recommandée : Vous êtes redirigé vers **Infrastructure > Configuration > Audit de configuration > Rapports d'audit** et vous pouvez consulter les instances présentant des écarts de modèle. Suivez la documentation pour terminer la tâche.

- **Avis de sécurité** : fournit des informations sur les CVE qui ont un impact sur vos instances NetScaler. Sélectionnez cette tâche pour afficher les onglets suivants :

  - **CVE détectés** : affiche les CVE détectés et les instances NetScaler ayant un impact sur les CVE. Pour terminer cette tâche, sélectionnez un CVE, cliquez sur **Afficher et corriger**.

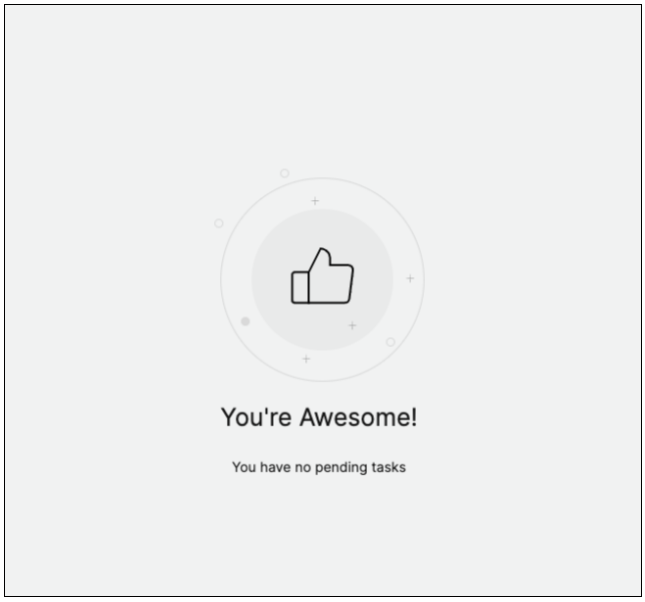
    Action recommandée : Vous êtes redirigé vers la page des **conseils de sécurité** dans **Infrastructure > Avis d'instance > Avis de sécurité**. Suivez la documentation pour terminer la tâche.

  - **Instances concernées : affiche les instances**NetScaler affectées par les CVE. Pour terminer la tâche, sélectionnez l'instance, cliquez sur **Afficher et corriger.**

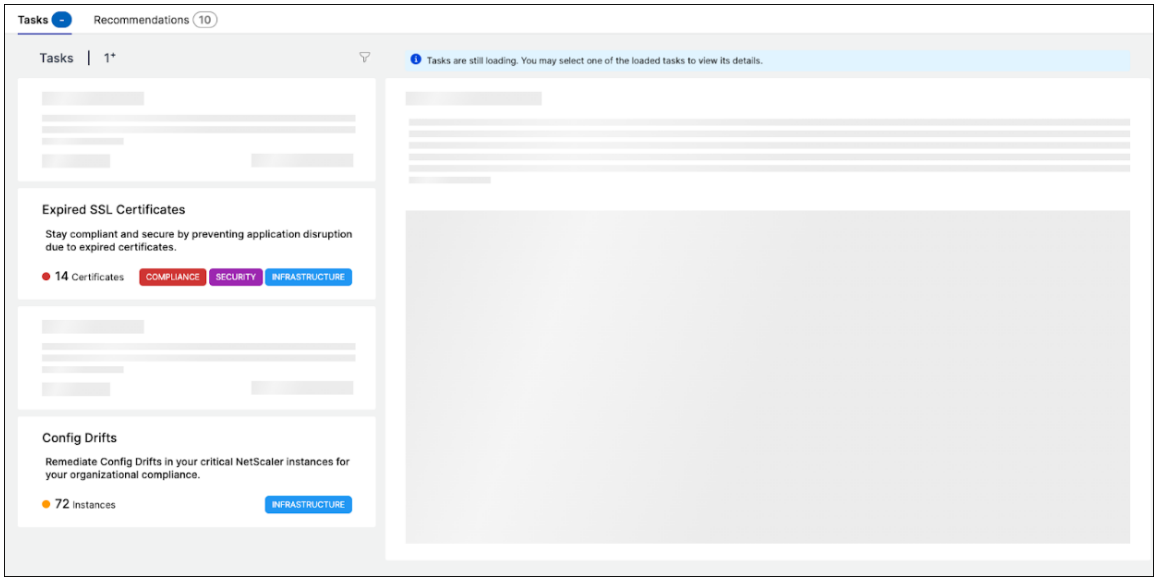
    Action recommandée : Vous êtes redirigé vers la page des **conseils de sécurité** dans **Infrastructure > Avis d'instance > Avis de sécurité**. Suivez la documentation pour terminer la tâche.

Remarque :

- Vous pouvez consulter la page suivante si aucune tâche n'est en attente sur votre NetScaler ADM :



- Dans certains scénarios, les vérifications sont effectuées dans toutes les instances et le chargement de toutes les tâches peut prendre plus de temps.



Recommandations

Le tableau suivant décrit les recommandations que vous pouvez consulter dans l'interface graphique de NetScaler ADM :

> **Remarque**
>
> Pour les licences groupées, vous recevez des recommandations basées sur vos droits de licence groupés existants.

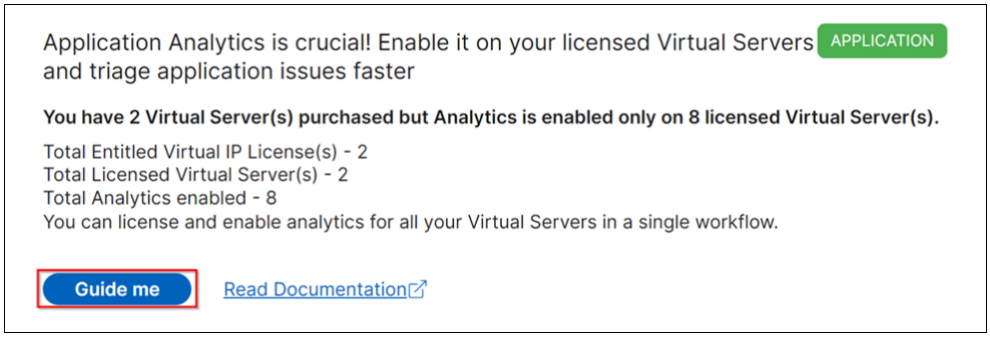
Nom de la recommandation	Quand la tâche est-elle visible dans l'interface graphique ?
Ajouter un ADC	Après avoir intégré NetScaler ADM et si aucune instance ADC n'est découverte.
Ajoutez un agent ADM externe pour utiliser le maximum de fonctionnalités de NetScaler ADM	Si aucun agent externe n'est configuré. Vous pouvez démarrer avec un agent intégré. Toutefois, un agent externe est requis pour utiliser toutes les fonctionnalités telles que les analyses, les licences groupées, etc.
Enregistrer un ADC depuis un agent intégré vers un agent externe	Une fois que vous avez intégré NetScaler ADM à l'aide du flux de travail Service Connect, les instances ADC sont intégrées à l'aide de l'agent intégré. Vous pouvez enregistrer ces instances ADC auprès d'un agent externe pour utiliser toutes les fonctionnalités telles que les analyses, les licences groupées, etc.
L'analyse des applications est cruciale ! Activez-le sur vos serveurs virtuels sous licence et triez les problèmes liés aux applications plus rapidement.	Si vous disposez de plusieurs serveurs virtuels sous licence mais que les fonctionnalités d'analyse ne sont pas activées.
Vous souhaitez réallouer de la bande passante sur votre ADC ? C'est simple !	Si les licences groupées sont allouées dans l'interface graphique de l'ADC et que ces instances ADC sont découvertes dans NetScaler ADM, vous pouvez effectuer la réallocation à l'aide de NetScaler ADM.
Tirez le meilleur parti de vos droits de propriété intellectuelle virtuelle ! Activez davantage de licences IP virtuelles sur vos serveurs virtuels découverts restants	Si vous possédez les licences requises, mais que vous ne possédez pas de licence pour tous les serveurs virtuels.
Activez l'accès granulaire basé sur les rôles pour les principaux utilisateurs de votre entreprise	Si le contrôle d'accès basé sur les rôles (RBAC) n'est pas encore configuré dans NetScaler ADM.
Configurez des règles et ne manquez aucun événement critique sur vos instances ADC	Si aucune règle d'événement personnalisée n'est encore configurée.

Nom de la recommandation	Quand la tâche est-elle visible dans l'interface graphique ?
Vous avez besoin de surveiller plusieurs applications et leurs performances ? Il suffit de créer une application personnalisée	Si l'application personnalisée n'est pas encore configurée.
Notifiez et ne manquez jamais les événements critiques dans vos applications	Si aucune stratégie d'action n'est configurée pour l'écart de score de l'application, le temps de traitement du serveur, la latence du réseau client, la latence du réseau du serveur ou le temps de réponse.
Évitez les pannes d'applications et ne manquez jamais l'expiration des certificats SSL d'une application	Si aucune alerte ou notification n'est configurée pour les certificats SSL expirant.
Avis de sécurité : maintenez vos ADC à jour avec les CVE et les mesures d'atténuation	Si les instances ADC ont un impact CVE.
Configurez une stratégied'entreprise et surveillez tout écart	Si les paramètres SSL d'entreprise ne sont pas modifiés ou sont toujours par défaut.
Vous répétez les tâches manuellement ? Créez des tâches de configuration et appliquez-les à plusieurs ADC	Si la tâche **Config Job** n'est pas encore configurée.
Gérez et surveillez le score de votre instance en sélectionnant les indicateurs personnalisés de votre choix.	Si les paramètres et les seuils par défaut dans les **paramètres du score d'instance** ne sont pas modifiés.
Suivez le score de votre application en sélectionnant les indicateurs personnalisés de votre choix.	Si les composants App Score du tableau de bord de l'application sont utilisés par défaut et qu'aucune personnalisation n'est effectuée.
Ajoutez des blocs d'adresses IP privées pour visualiser les demandes des clients dans la carte géographique	Si les blocs d'adresses IP ne sont pas configurés. Vous pouvez créer des blocs IP pour cartographier et visualiser les demandes des clients sur une carte géographique en fonction de leurs adresses IP/plage privées.
Abonnez-vous et exportez vos violations AppSec vers Splunk en temps réel	Si l'intégration de Splunk dans NetScaler ADM n'est pas encore configurée.
Personnalisez le seuil par défaut ou créez un nouveau seuil pour vos services Kubernetes	Si seuls des seuils par défaut sont utilisés dans le graphe des services et qu'aucun seuil simple ou double n'est appliqué aux services.
Configurez de manière proactive des profils de notification et recevez des notifications dans vos destinations de communication	Si aucun profil de notification n'est encore configuré.

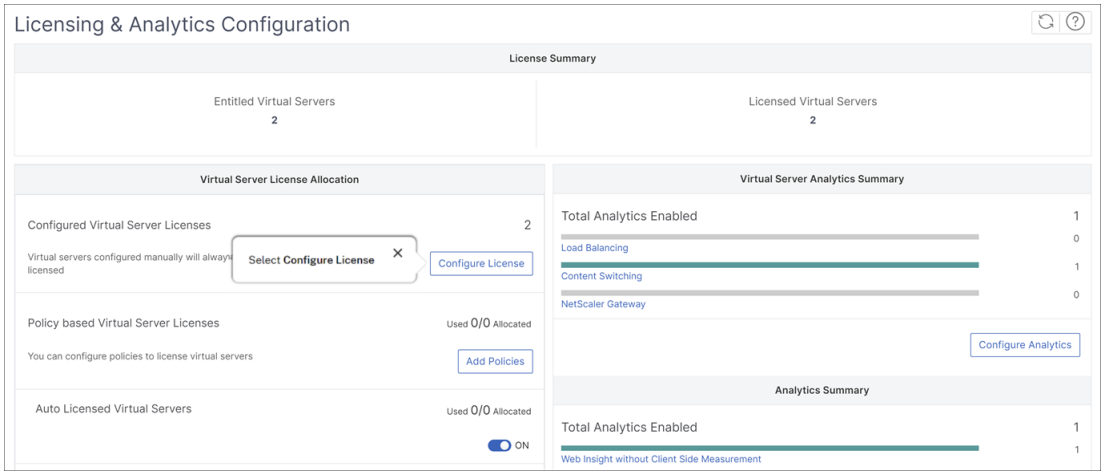
Nom de la recommandation	Quand la tâche est-elle visible dans l'interface graphique ?
Planifiez des exportations récurrentes et recevez des notifications sur les détails de l'infrastructure	Si aucun calendrier d'exportation n'est encore configuré dans **Infrastructure > Instances**.
Vous possédez ServiceNow et souhaitez l'intégrer à ADM ?	Si l'intégration de ServiceNow dans NetScaler ADM n'est pas encore configurée.
Automatisez la gestion des certificats SSL à l'aide de Venafi et ADM	Si le serveur Venafi n'est pas encore configuré dans NetScaler ADM.
Renouvelez votre licence Pooled avant son expiration.	Si votre licence actuelle est sur le point d'expirer dans 30 jours.
Commencez à utiliser les licences groupées en allouant la bande passante groupée que vous avez achetée aux instances NetScaler.	Si vous n'avez pas encore commencé à attribuer vos droits de licence groupés.
Envisagez d'acheter davantage de capacité de bande passante groupée.	Si vous avez utilisé 90 % ou plus de votre bande passante groupée autorisée.
Votre autorisation de bande passante groupée actuelle est sous-utilisée. Révisez et envisagez d'allouer davantage	Si le taux d'utilisation de votre allocation de licences groupée est inférieur à 70 %.

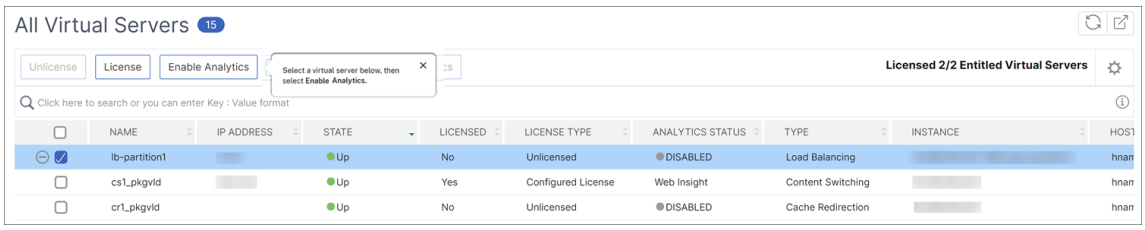
Comment utiliser le flux de travail Guideme et compléter la recommandation ?

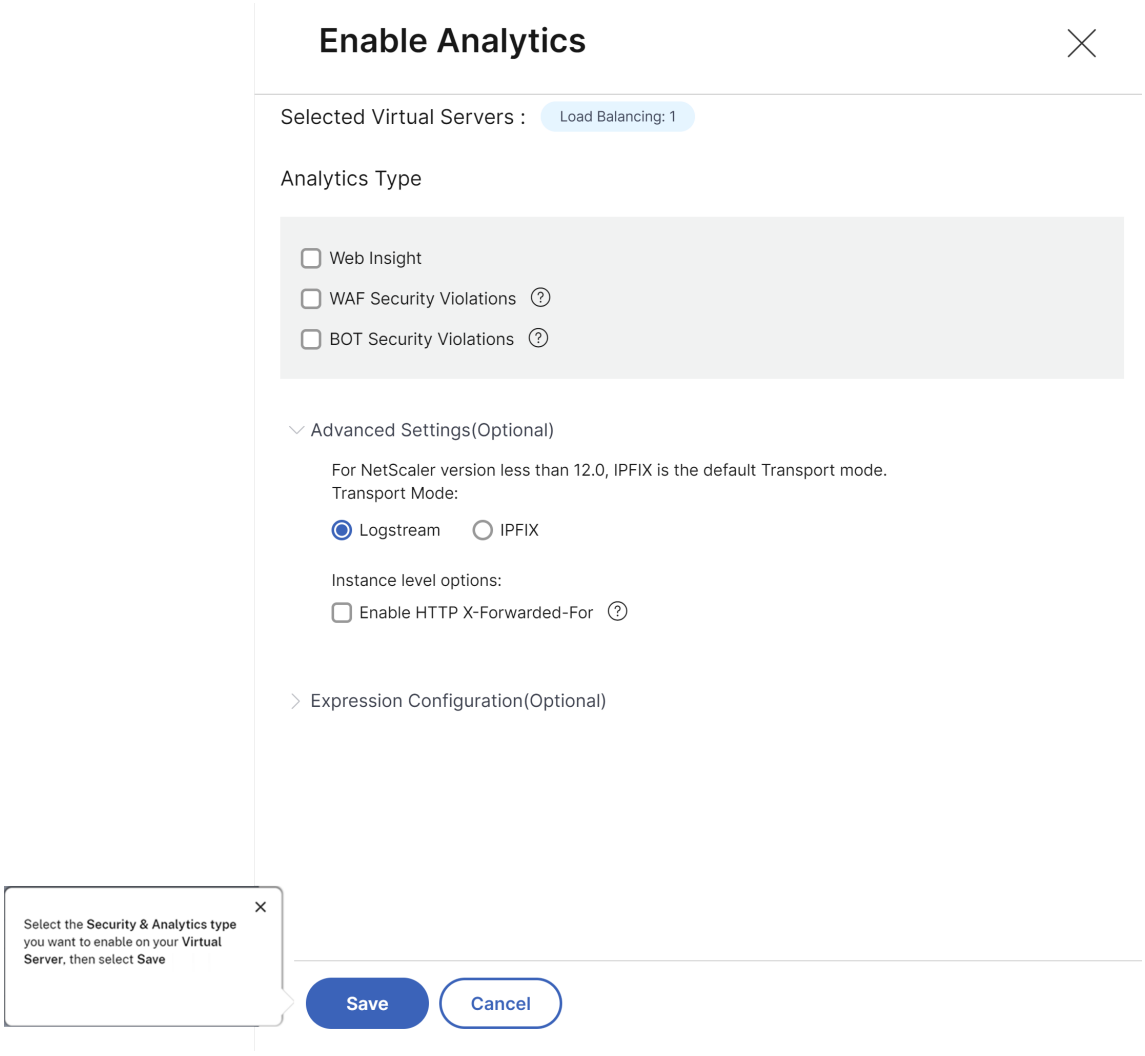
Supposons que vous souhaitez activer les analyses pour tous les serveurs virtuels sous licence. Cliquez sur **Guidez-moi** pour effectuer la tâche suivante :



Le flux de travail fournit les suggestions requises pour terminer la tâche. Dans cet exemple, après avoir cliqué sur **Guide**, suivez les suggestions d'info-bulles fournies :

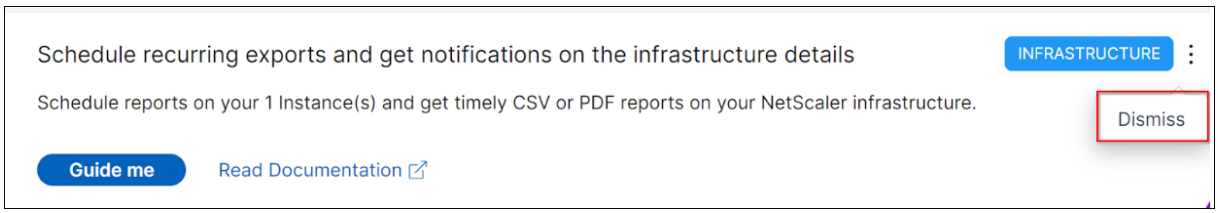
1. 

2. 

3. 

Une fois que vous avez sélectionné le type d'analyse et cliqué sur **Enregistrer les analyses**, la recommandation est terminée et elle est déplacée vers Terminé.

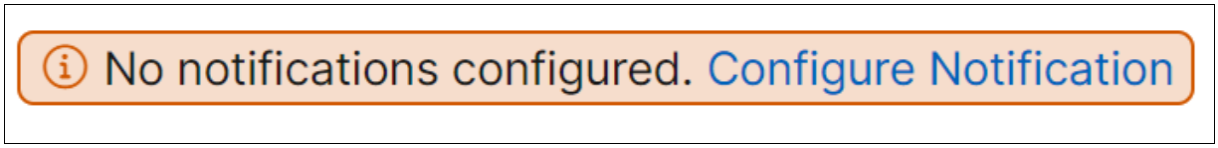
De même, si vous souhaitez terminer une recommandation ultérieurement, vous pouvez sélectionner **Rejeter dans** la liste et elle sera déplacée vers **Rejeté**.



Configurer les notifications

Vous pouvez configurer et recevoir des notifications chaque fois que NetScaler ADM identifie des tâches en cours nécessitant une action immédiate de votre part. Si vous n'avez pas configuré de

notifications, vous pouvez cliquer sur **Configurer la notification** dans le coin supérieur droit.



Sur la page **Notifications**, vous pouvez configurer des profils pour **Email** et **Slack**, puis cliquer sur **Enregistrer** pour recevoir des notifications. Pour chaque type de notification, l'interface graphique NetScaler ADM affiche la liste de distribution ou le profil configuré. NetScaler ADM envoie des notifications à la liste de distribution ou au profil sélectionné.

FAQ

1. Pourquoi le type de recommandations est-il présent pour les administrateurs ?

   Actuellement, les recommandations sont spécifiques aux déploiements et aident les administrateurs à mieux définir les configurations et les tâches de configuration afin de rendre le déploiement efficace. Cela permet également de mieux découvrir les produits et les administrateurs peuvent savoir à quoi sert une tâche et comment elle peut être utile sans aucune connaissance préalable ni savoir si la fonctionnalité existe ou non dans ADM.

2. Que se passe-t-il si je rejette une recommandation ?

   Les recommandations que vous rejetez sont déplacées vers **Rejetées**. Vous pourrez compléter ces recommandations ultérieurement.

3. Est-ce que la recommandation passe à **Terminé** si je commence un guide et que je le laisse au milieu ?

   Non, la recommandation n'est pas terminée tant que l'action n'est pas enregistrée ou terminée.

4. Puis-je effectuer une recherche ou un filtrage ?

   Oui ! Vous pouvez utiliser la barre de recherche ou sélectionner des tâches spécifiques en sélectionnant la catégorie dans la liste.

5. Est-ce que je recevrai des tâches pour effectuer des actions sur des événements dynamiques ?

   Oui ! Actuellement, vous pouvez consulter un total de 4 tâches réalisables. Pour plus d'informations, consultez la section Tâches.

6. Toutes les tâches réalisables et plus de 20 recommandations s'afficheront-elles même si je n'ai pas ajouté d'instances NetScaler dans NetScaler ADM ?

   Non L'instance NetScaler et les serveurs virtuels doivent être disponibles dans NetScaler ADM pour afficher toutes les tâches et recommandations.

7. À quelle fréquence les tâches seront-elles actualisées ?

   Lorsque vous cliquez sur **Tâches** dans le volet de navigation de gauche, elles sont actualisées et disponibles au dernier état. Les informations sont récupérées et mises à jour.

Un tableau de bord unifié pour afficher les détails des indicateurs clés des instances

February 1, 2024

Dans NetScaler ADM, vous pouvez consulter diverses informations sur l'utilisation et les performances des applications, l'infrastructure ADC, les violations de sécurité (Bot et WAF), etc. En tant qu'administrateur, vous devrez peut-être accéder aux différentes options de l'interface graphique d'ADM pour afficher plusieurs informations. Par exemple, pour vérifier les informations sur les serveurs virtuels (applications) et les instances ADC :

- Vous devez d'abord accéder à **Applications > Tableau de bord** pour afficher des informations sur les applications.
- Vous devez ensuite accéder à **Infrastructure > Analyse de l'infrastructure** pour obtenir des informations sur les instances ADC.

Pour une meilleure expérience de surveillance, vous devez disposer d'un privilège contenant une vue d'ensemble de toutes les informations requises. Accédez à **Présentation > Tableau de bord** pour visualiser un tableau de bord à volet unique avec une vue d'ensemble des détails des indicateurs clés en fonction des catégories suivantes :

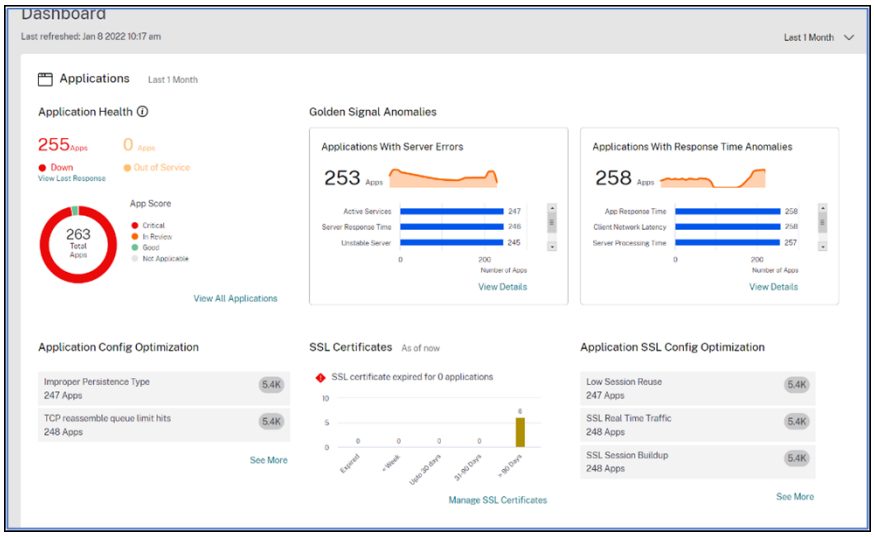
- Applications
- Infrastructure ADC
- Sécurité des applications
- Gateway

Applications

Sous **Applications**, vous pouvez consulter :

- **État des applications** : fournit une vue d'ensemble des applications en **panneou hors service**, en fonction de leur statut (**Critique**,**En cours de révision**,**Bon état**et**Non applicable**). Cliquez sur**Afficher toutes les applications** pour afficher les détails dans le tableau de bord des applications

- **Golden Signal Anomalies** —Fournit une vue d'ensemble des applications présentant des erreurs de serveur et des anomalies de temps de réponse. Cliquez sur **Afficher les détails** pour plus d'informations.
- **Optimisation de la configuration des applications** : fournit une vue d'ensemble de toutes les applications présentant des problèmes de performances. Cliquez sur **Voir plus** pour afficher les détails du problème dans le tableau de bord de l'application.
- **Certificats SSL** —Fournit une vue d'ensemble des certificats SSL ainsi que de leur validité. Cliquez sur **Gérer les certificats SSL** pour afficher plus d'informations dans le tableau de bord SSL.
- **Optimisation de la configuration SSL des applications** : fournit une vue d'ensemble de l'ensemble des applications présentant des problèmes liés au SSL. Cliquez sur **Voir plus** pour voir les détails du problème.



Infrastructure ADC

Dans **l'infrastructure ADC**, vous pouvez consulter les indicateurs clés relatifs aux instances ADC suivants :

- État de**santé de l'instance ADC** : fournit une vue d'ensemble du nombre total d'instances ADC en fonction du score de l'instance.
- **Instances ADC affectées par les CVE** : fournit une vue d'ensemble du nombre total d'instances ADC touchées par des vulnérabilités et des expositions communes (CVE).
- **Problèmes liés aux instances ADC** : fournit une vue d'ensemble des problèmes liés aux instances ADC en fonction de leur catégorie. Pour plus d'informations, consultez Infrastructure Analytics.

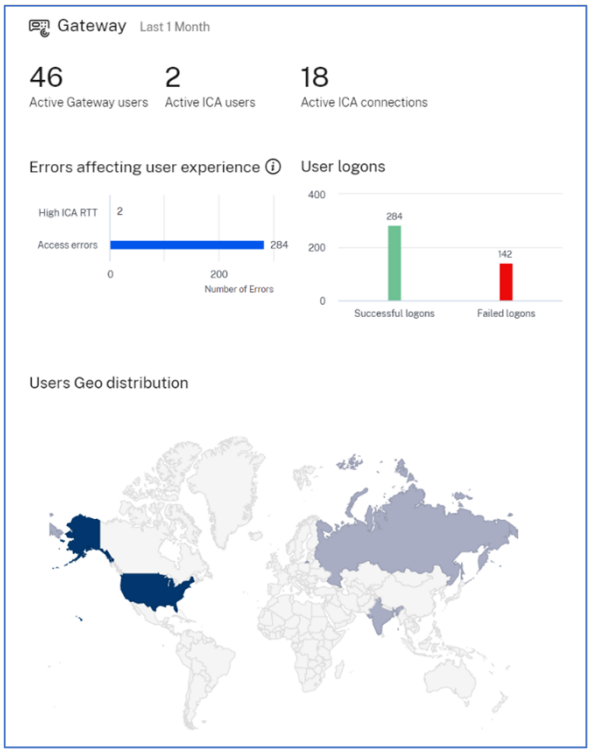
- **Résumé de la mise à niveau des instances ADC** : fournit une vue d'ensemble du nombre total d'instances ADC qui ne sont pas sur la dernière version. Cliquez sur Afficher le tableau de bord des instances ADC pour plus d'informations.

Sécurité des applications

Fournit une vue d'ensemble du nombre total d'applications concernées et du nombre total de violations (Bot et WAF) signalées pendant la durée sélectionnée. Cliquez sur **Afficher le tableau de bord** de sécurité pour afficher les informations relatives à la sécurité et aux violations

Gateway

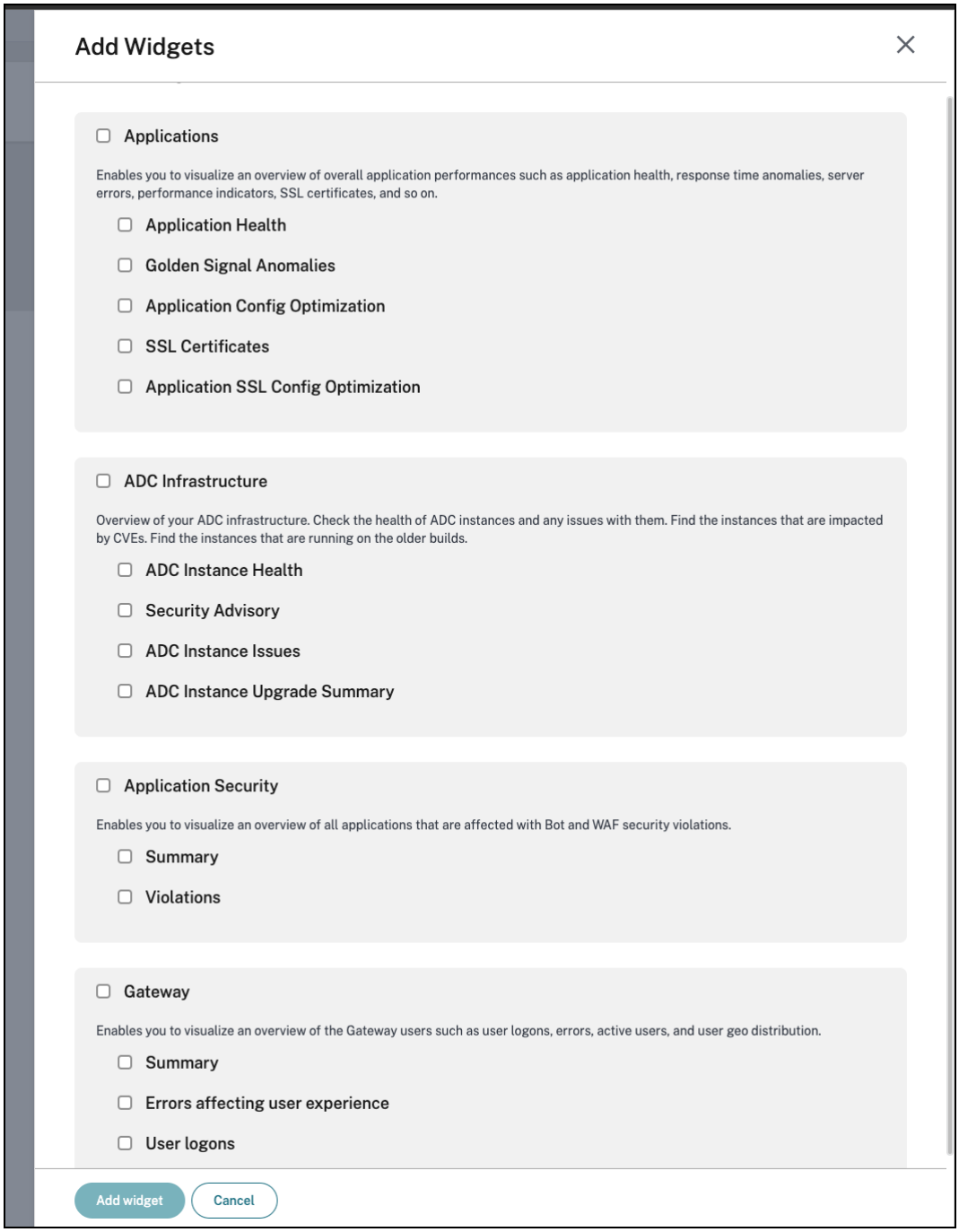
Fournit un aperçu du nombre total d'utilisateurs actifs de la passerelle, du nombre total d'utilisateurs ICA actifs et du total des connexions ICA actives. Vous pouvez également afficher les erreurs, les détails de connexion des utilisateurs et une carte géographique fournissant des détails sur la localisation des utilisateurs.



Personnalisez le tableau

Vous pouvez utiliser l'option **Modifier le tableau de bord** et personnaliser l'affichage du tableau de bord en fonction de votre choix. L'option **Modifier le tableau de bord** vous permet de :

- Faites glisser les widgets
- Supprimez l'ensemble du widget (applications, infrastructure ADC, passerelle ou sécurité des applications).
- Supprimez les petits widgets présents sous chaque widget.
- Cliquez sur **Ajouter un widget** et sélectionnez les indicateurs clés requis que vous souhaitez afficher sous chaque widget.



- Rétablir les valeurs par défaut
- Réinitialiser jusqu'à la dernière sauvegarde

Après avoir apporté des modifications, cliquez sur **Enregistrer**.

> **Remarque**
>
> - Par défaut, tous les widgets sont affichés. Si vous personnalisez le tableau de bord, enreg-

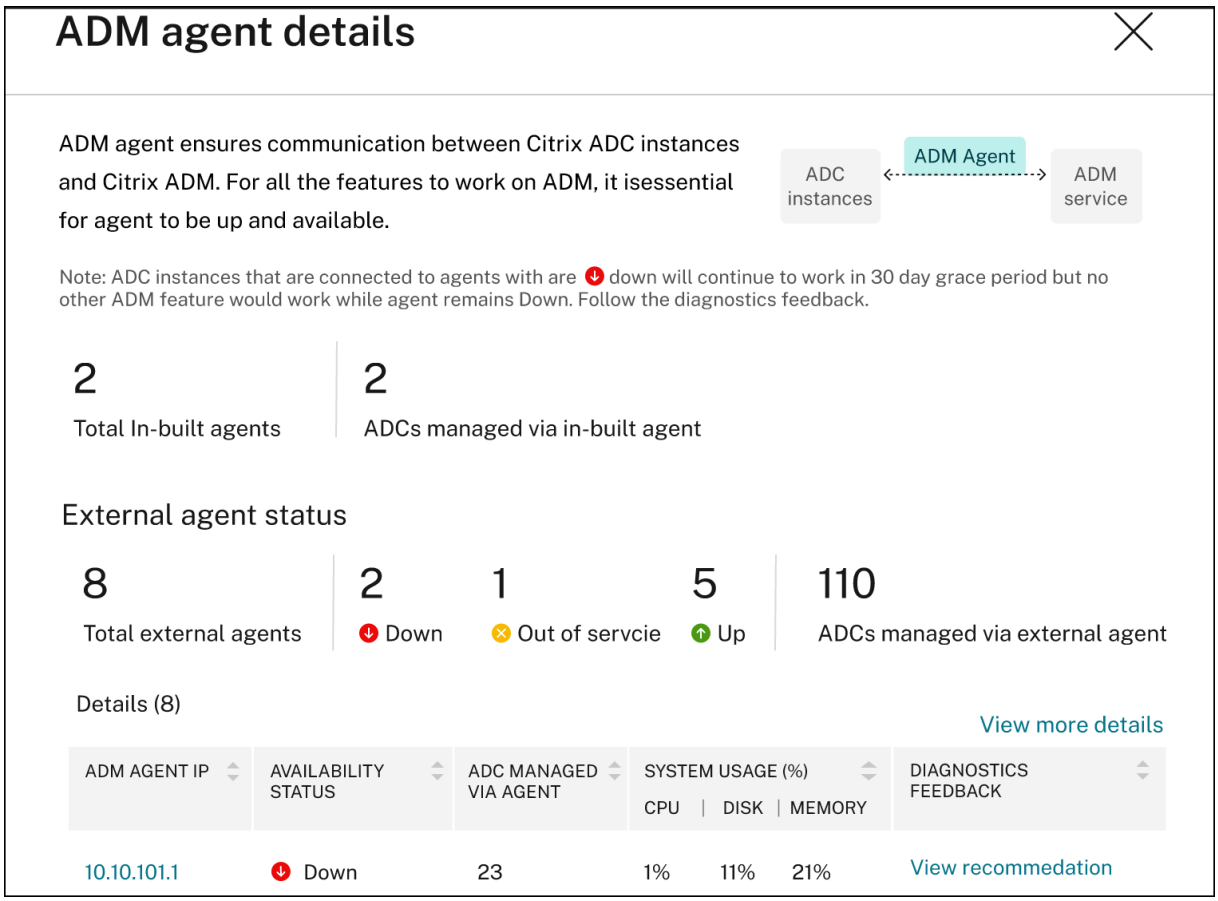
> istrez les modifications et utilisez à nouveau l'option **Rétablir les paramètres par défaut**, tous les widgets sont ajoutés au tableau de bord.
>
> - L'option **Réinitialiser à la dernière sauvegarde** charge la configuration précédemment enregistrée.

Afficher les détails des agents

Dans le tableau de bord unifié, vous pouvez visualiser une vue d'ensemble des détails sur les agents ADM. Dans **Vue d'ensemble > Tableau de bord**, à côté du **statut de l'agent ADM**, vous pouvez consulter l'état suivant qui vous permet d'analyser la disponibilité globale de l'agent :

- **Tout est disponible**. Indique que tous les agents sont opérationnels.
- **Tout n'est pas disponible** Indique que tous les agents sont hors service et ne sont pas accessibles.
- **[nombre d'agents] non disponible**. Indique que certains agents sont hors service et ne sont pas accessibles.
- **Tout est hors service**. Indique que tous les agents sont hors service.
- **[nombre d'agents] hors service**. Indique que quelques agents sont hors service.
- **Agent externe introuvable**. Indique qu'aucun agent (via un hyperviseur) n'est configuré.

Cliquez sur **Afficher les détails** pour visualiser une vue d'ensemble des détails de l'agent ADM, tels que le nombre total d'agents intégrés, le nombre total d'agents externes, l'adresse IP de l'agent, l'état, l'utilisation du système, les contrôles de diagnostic, etc.



Création et application de filtres

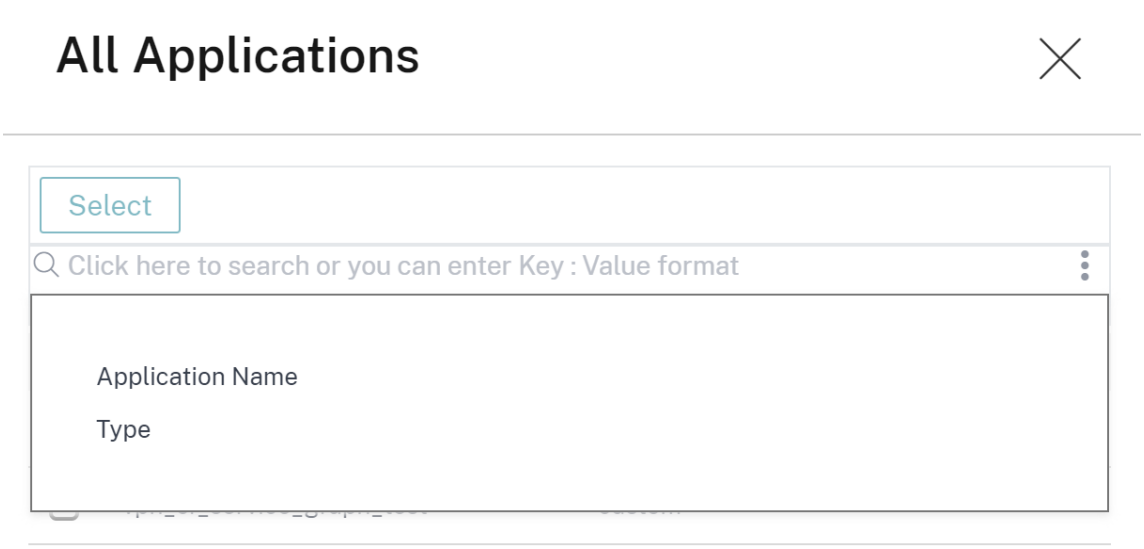
Vous pouvez appliquer des filtres et afficher des informations uniquement pour les instances ou applications sélectionnées dans les cas suivants :

- Applications
- Infrastructure ADC
- Sécurité des applications

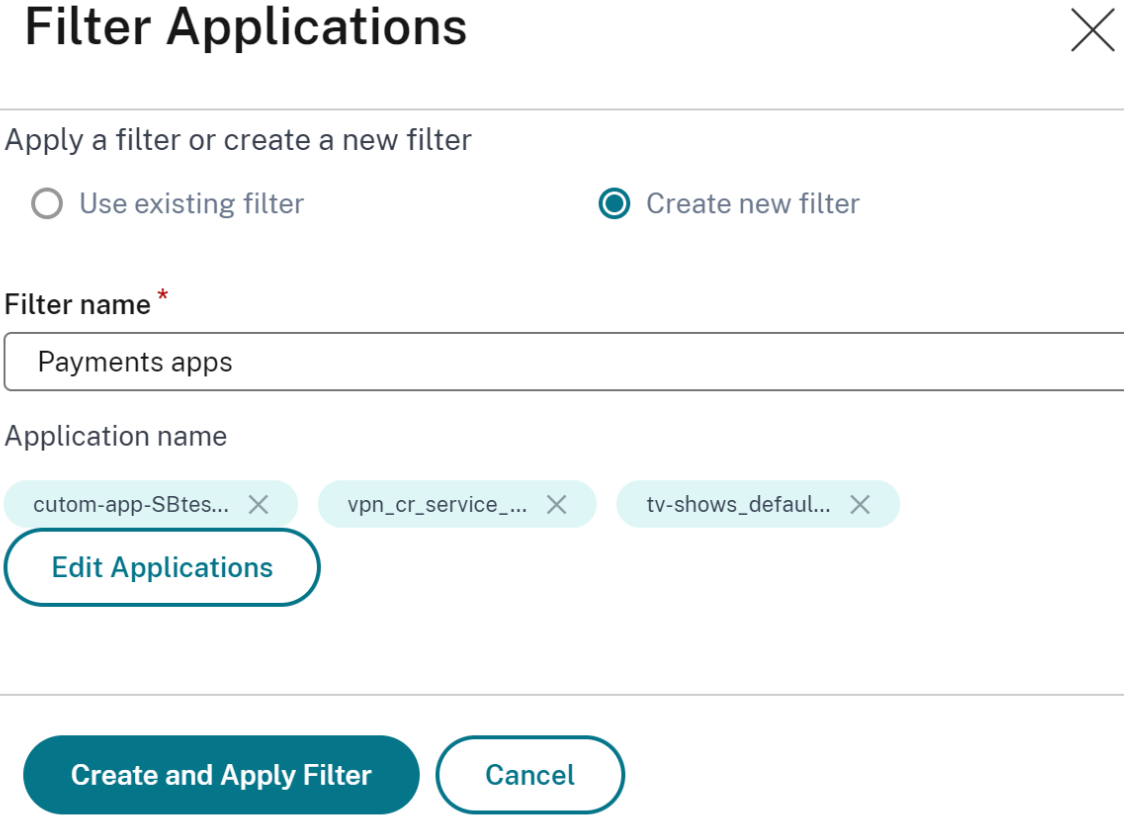
Par défaut, toutes les applications sont sélectionnées. Vous pouvez créer un filtre personnalisé à partir du tableau de bord en cliquant sur l'icône des filtres disponible dans la vignette.

Dans la fenêtre **Filtrer les applications** :

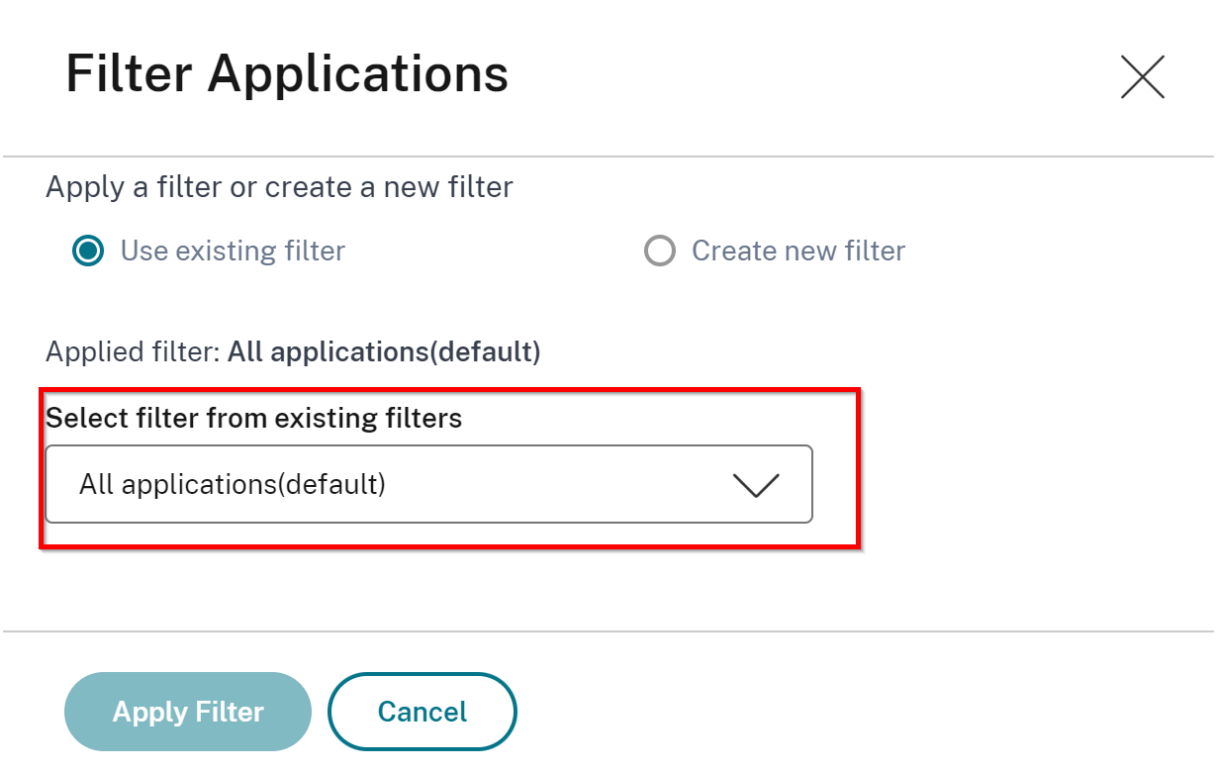
1. Sélectionnez **Créer un nouveau filtre**.
2. Fournissez un nom de filtre en fonction de votre choix.
3. Cliquez sur **Sélectionner les applications** et ajoutez toutes les applications requises pour le filtre. Lorsque vous sélectionnez des applications, vous pouvez également utiliser les filtres (**nom et**type**de l'application**), puis sélectionner des applications.



4. Cliquez sur **Créer et appliquer un filtre**.

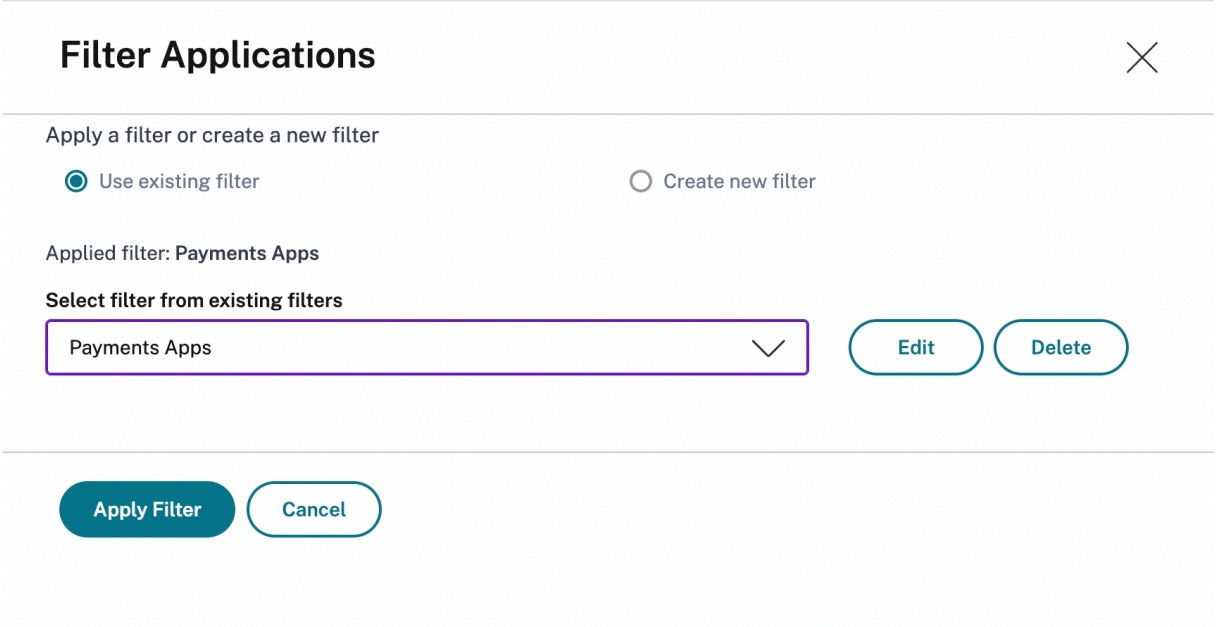


Le filtre est maintenant créé et appliqué. Vous pouvez créer d'autres filtres en suivant la même procédure. Après avoir créé des filtres, vous pouvez sélectionner et appliquer des filtres via la liste **Sélectionner un filtre parmi les filtres existants** .



Modifier les filtres

Vous pouvez modifier un filtre en le sélectionnant dans la liste et en cliquant sur **Modifier**. L'option d'édition vous permet d'ajouter ou de supprimer des applications, puis de mettre à jour le filtre.



Pour supprimer un filtre, sélectionnez-le dans la liste et cliquez sur **Supprimer**.

> **Remarque**
>
> Lorsque vous créez un filtre avec des applications et si l'une des applications est supprimée du tableau de bord de l'application, les détails de l'application sont immédiatement supprimés du tableau de bord unifié.

Applications

February 1, 2024

La fonctionnalité d'analyse et de gestion des applications de NetScaler 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 (NetScaler).

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 NetScaler dans NetScaler ADM
- Assurez-vous de disposer d'une licence valide pour vos instances NetScaler. 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, NetScaler ADM vous permet d'ajouter des licences pour deux applications au maximum. Selon votre licence, vous pouvez sélectionner et appliquer des licences pour les applications que vous souhaitez surveiller.

Applications de microservices

Dans un cluster Kubernetes, NetScaler fournit un contrôleur d'entrée pour NetScaler MPX (matériel), NetScaler VPX (virtualisé) et NetScaler CPX (conteneurisé). Pour plus d'informations, consultez NetScaler IngressController.

Les applications discrètes configurées à l'aide des instances NetScaler CPX sont appelées applications de microservices.

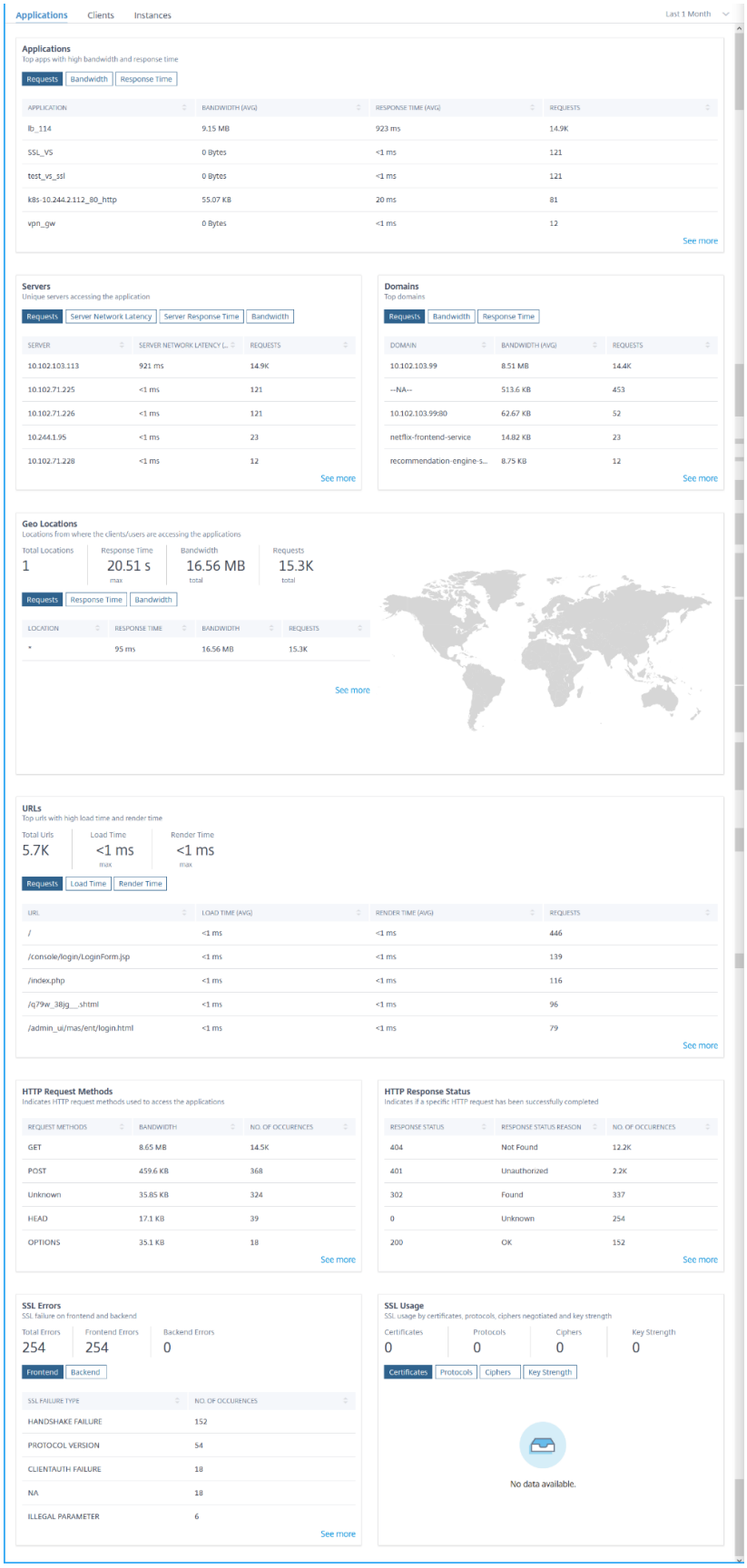
Tableau de bord Web Insight

February 1, 2024

La fonctionnalité Web Insight améliorée est augmentée et fournit une visibilité sur des mesures détaillées pour les applications Web, les clients et les instances NetScaler. 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
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

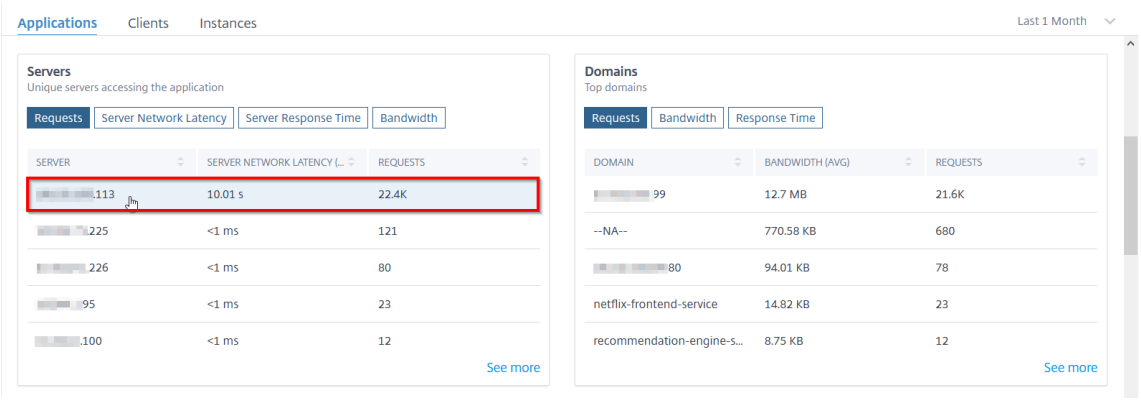


Dans chaque mesure, vous pouvez voir les 5 meilleurs résultats. Vous pouvez cliquer pour approfondir l'exploration vers le bas pour analyser le problème et prendre des mesures de dépannage plus rapidement.

> **Remarque :**
>
> - À partir de la version **14.1-4.x**, lorsque vous explorez une métrique, la vue analytique du graphique des séries chronologiques affiche des valeurs nulles (par exemple, 0 ms et 0 demande) pour la durée sélectionnée. Auparavant, si aucun trafic ou transaction n'était reçu pendant la durée sélectionnée, la vue analytique affichait les graphiques en ignorant ces valeurs nulles.
> - Dans certains scénarios, NetScaler peut ne pas être en mesure de calculer les valeurs RTT pour certaines transactions. Pour de telles transactions, NetScaler ADM affiche les valeurs RTT sous la forme
>
> - **NA** : indique lorsque l'instance ADC ne peut pas calculer le RTT.
> - **< 1 ms** —Indique quand l'instance ADC calcule le RTT en décimales entre 0 ms et 1 ms. Par exemple, 0,22 ms.

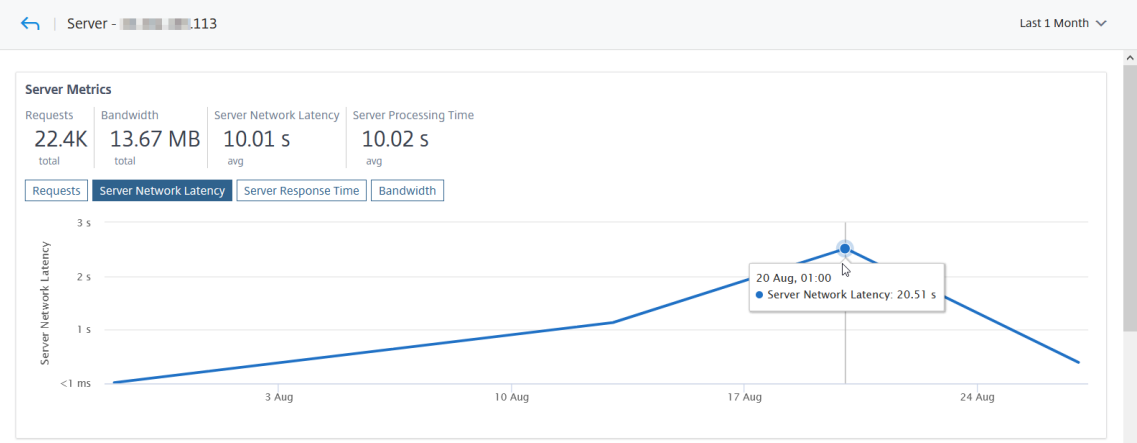
Par exemple, considérez que vous souhaitez analyser la latence du réseau du serveur pour une durée d'un mois et prendre la décision d'augmenter ou de réduire l'environnement de production. Pour analyser ceci :

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.

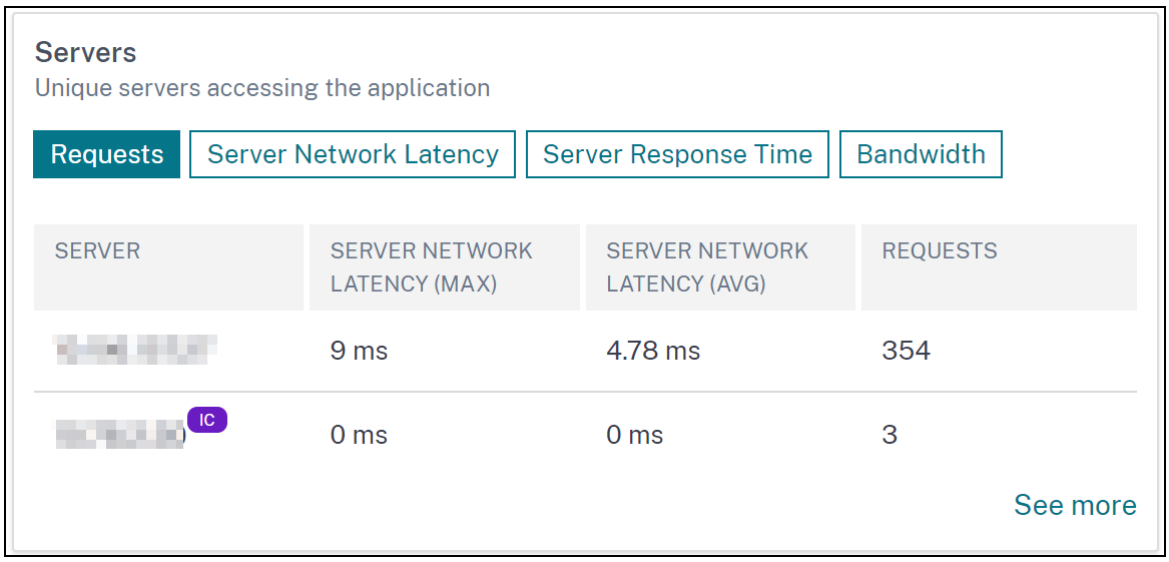


La latence moyenne indique 10,01 s et à partir du graphique, vous pouvez analyser que la latence réseau serveur pour le dernier mois semble être élevée. En tant qu'administrateur, vous pouvez prendre la décision d'étendre l'environnement de production.

Demandes de cache intégrées

Le cache intégré fournit un stockage en mémoire sur l'appliance NetScaler et diffuse du contenu Web aux utilisateurs sans qu'il soit nécessaire d'aller et retour vers un serveur d'origine.

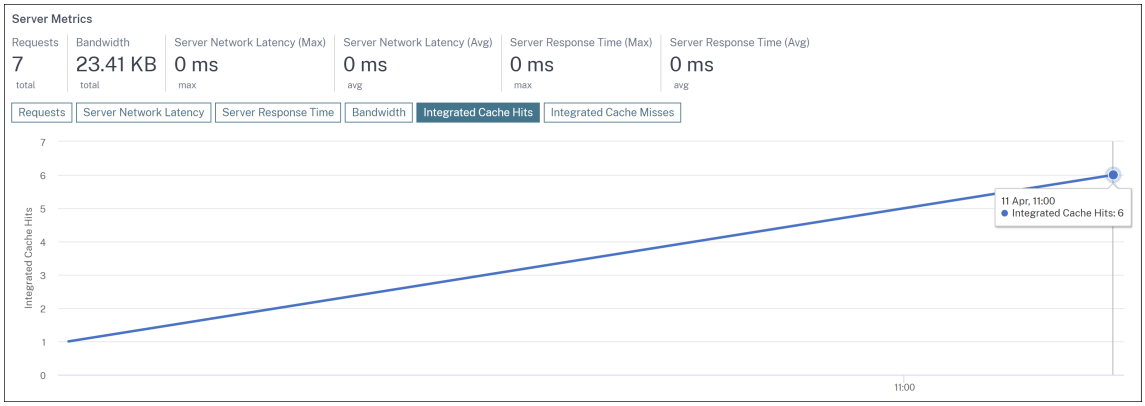
Les demandes de cache d'intégration sont actuellement visibles sous **Serveurs** avec une notification IC à côté de l'adresse IP du serveur virtuel ADC. Toutes les autres demandes sont visibles avec l'adresse IP du serveur d'origine.



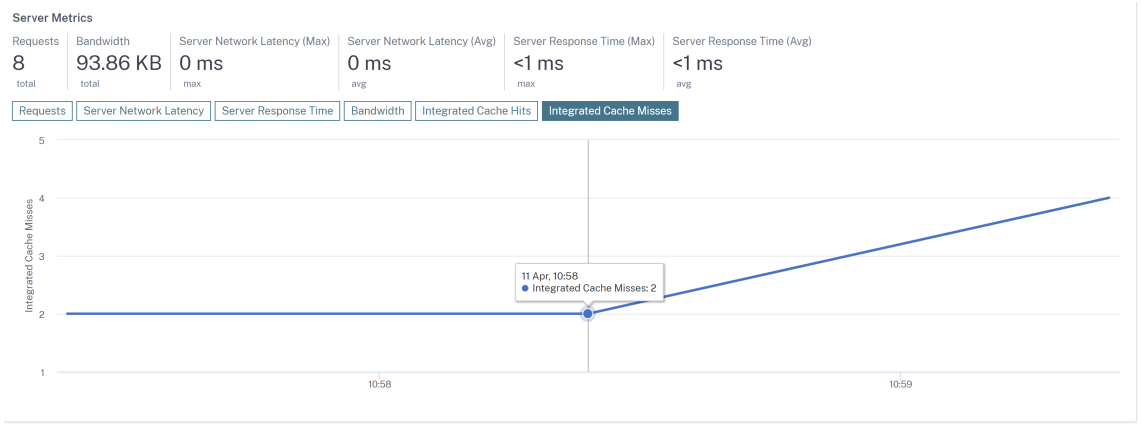
Lorsque vous explorez un serveur pour obtenir plus de détails, les **indicateurs du serveur affichent des** onglets intégrés indiquant les accès et les erreurs de cache.

La vue graphique est affichée dans :

- L'onglet **Integrated Cache Hits** vous permet de visualiser le total des réponses que l'appliance NetScaler fournit à partir du cache.



- L'onglet **Integrated Cache Misses** vous permet de visualiser le nombre total de réponses que l'appliance NetScaler reçoit depuis le serveur d'origine.



Résoudre les problèmes liés à Web Insight

Pour plus de détails, consultez le document de dépannage Résoudre les problèmes liés à Web Insight.

Découvrez la cause première de la latence des applications

February 1, 2024

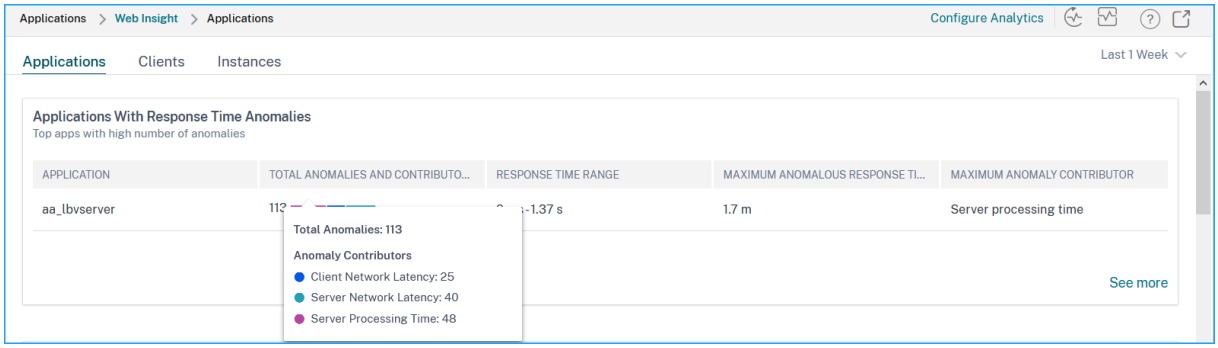
La lenteur des applications est une préoccupation majeure pour toute organisation, car elle entraîne un impact commercial ou une productivité. Dans **Applications > Web Insight**, vous pouvez désormais consulter une nouvelle métrique intitulée **Applications présentant des anomalies du temps**

de réponse. À l'aide de cette métrique, en tant qu'administrateur, vous pouvez déterminer si la latence de l'application est due aux causes suivantes :

- Latence du réseau client
- Latence réseau du serveur
- Délai de traitement du serveur

NetScaler ADM effectue des contrôles d'anomalies toutes les heures et signale les anomalies relatives au trafic de la dernière heure, en fonction de certaines conditions préalables. Par exemple, pour éviter des résultats faux positifs, si le temps de réponse est inférieur à 1 ms, les vérifications d'anomalie pour ces résultats sont ignorées.

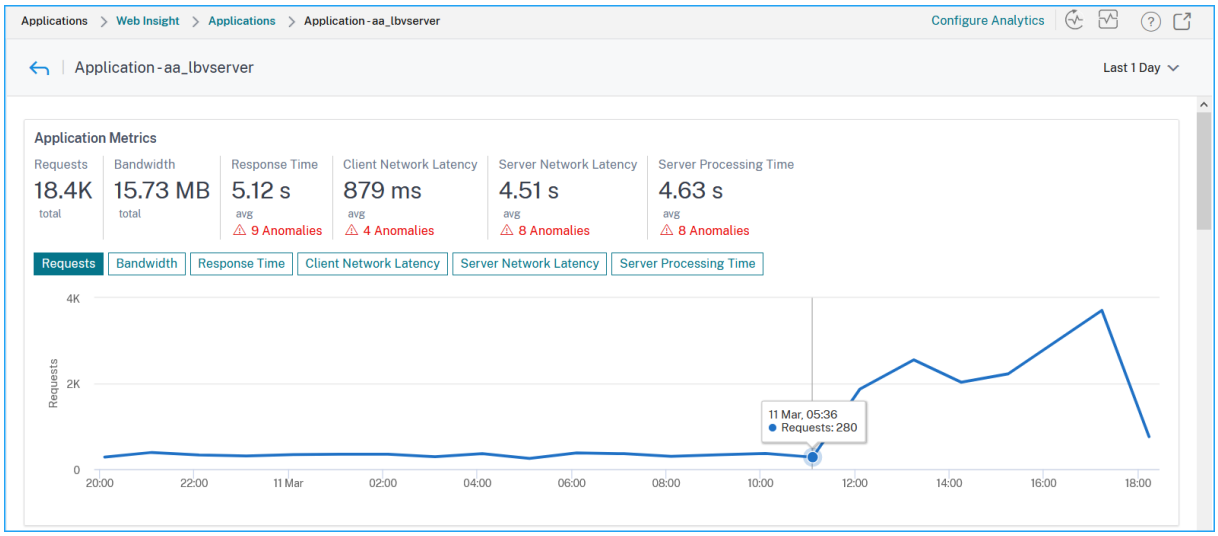
La page **Applications > Web Insight** vous permet d'afficher les applications présentant des anomalies de temps de réponse pour la durée sélectionnée. La mesure **Applications avec anomalies de temps de réponse** affiche les cinq premières applications en fonction du total des anomalies. Cliquez sur **Voir plus** pour afficher toutes les applications.



- **Application** —Indique le nom de l'application.
- **Total des anomalies et des contributeurs** —Indique le total des anomalies de l'application. Lorsque vous placez le pointeur de la souris, vous pouvez afficher le total des anomalies provenant respectivement de la latence réseau client, de la latence réseau du serveur et du temps de traitement du serveur.
- **Plage de temps de réponse** : indique la plage de temps de réponse attendue de l'application.
- **Temps de réponse anormal maximal** : indique le temps de réponse le plus élevé de l'application.
- **Contributeur d'anomalie maximale** : indique si le nombre maximal d'anomalies pour l'application provient de la latence du réseau client, de la latence réseau du serveur ou du temps de traitement du serveur.

exploration vers le bas de l'application

Cliquez sur une application pour afficher les détails des **mesures d'application** pour la durée sélectionnée.



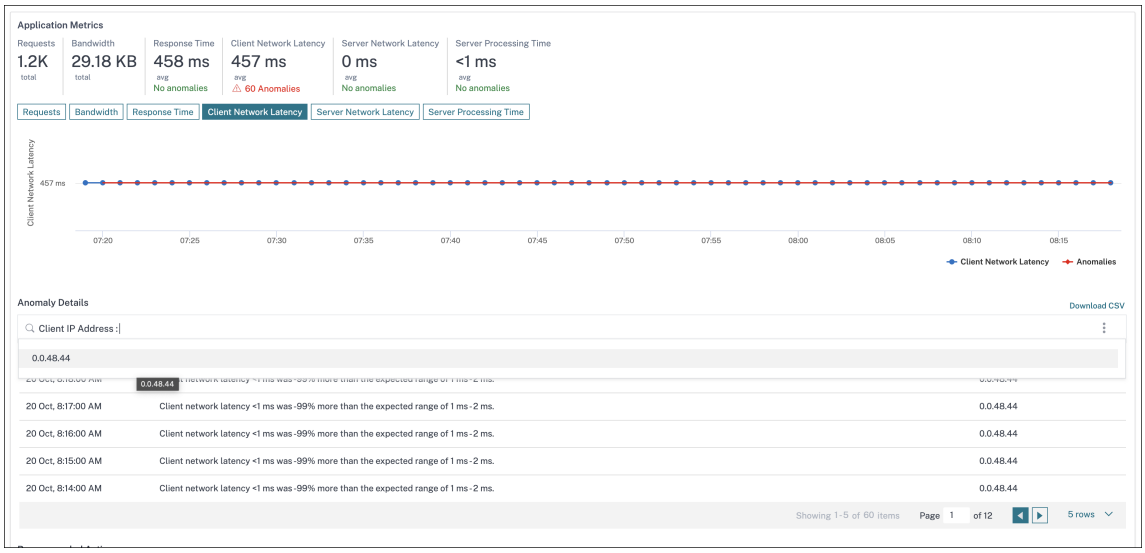
Les **mesures d'application** vous permettent d'afficher les éléments suivants :

- **Résumé** —Vue d'ensemble permettant de visualiser les performances de l'application, telles que le temps de réponse, les demandes et la bande passante.
- **Demandes** : le nombre total de demandes reçues par l'application. Vous pouvez également consulter les demandes des 5 principaux clients en fonction du nombre total de demandes.
- **Bande passante** : bande passante totale traitée par l'application. Vous pouvez également consulter la consommation de bande passante des 5 principaux serveurs en fonction de la consommation totale de bande passante.
- **Temps de réponse** —Vue d'ensemble permettant de visualiser la latence du réseau client, la latence du réseau du serveur et le temps de traitement du serveur sur le même graphique.
- **Latence du réseau client : latence** moyenne du réseau client (du client à l'ADC).
- Latence**du réseau du serveur : latence** moyenne du réseau du serveur (de l'ADC au serveur).
- **Temps de traitement du serveur : temps** de traitement moyen du serveur (du serveur à l'ADC).

Si l'application présente des anomalies, vous pouvez voir si les anomalies proviennent de la latence du réseau client, de la latence du réseau du serveur ou du temps de traitement du serveur. Cliquez sur chaque onglet pour afficher les détails.

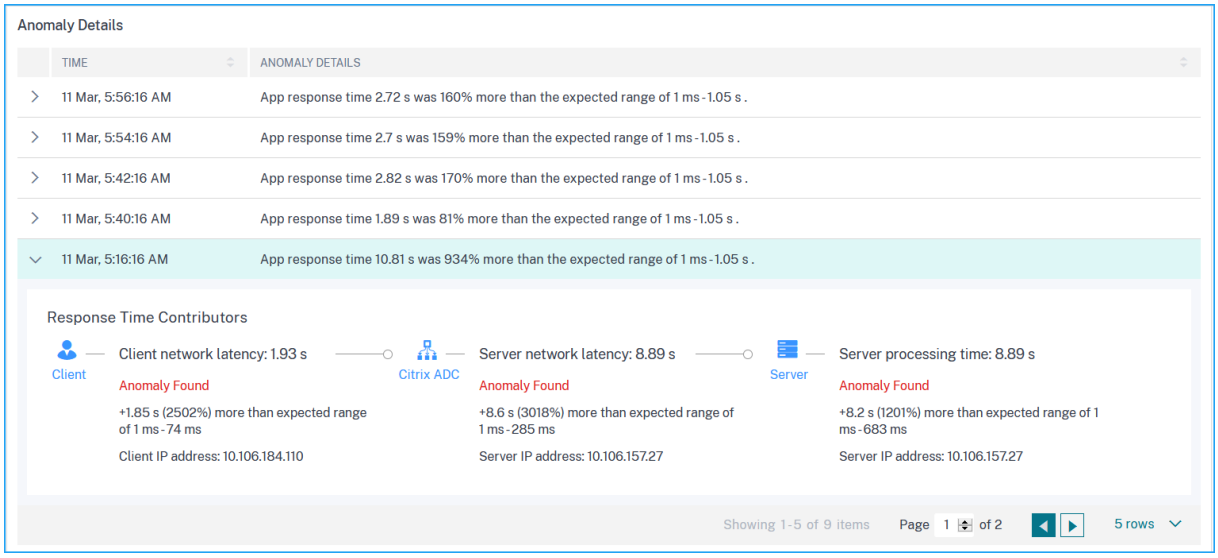
Dans les onglets **Latence du réseau client** et **Latence du réseau du serveur**, vous pouvez consulter :

- **Une barre de recherche** : cliquez sur la barre de recherche pour afficher l'adresse IP de tous les clients (dans Latence du réseau client) et des serveurs (dans Latence du réseau du serveur). Vous pouvez sélectionner l'adresse IP pour filtrer les résultats.
- **Une option d'exportation** : cliquez sur **Télécharger le fichier CSV** pour exporter les informations au format CSV.

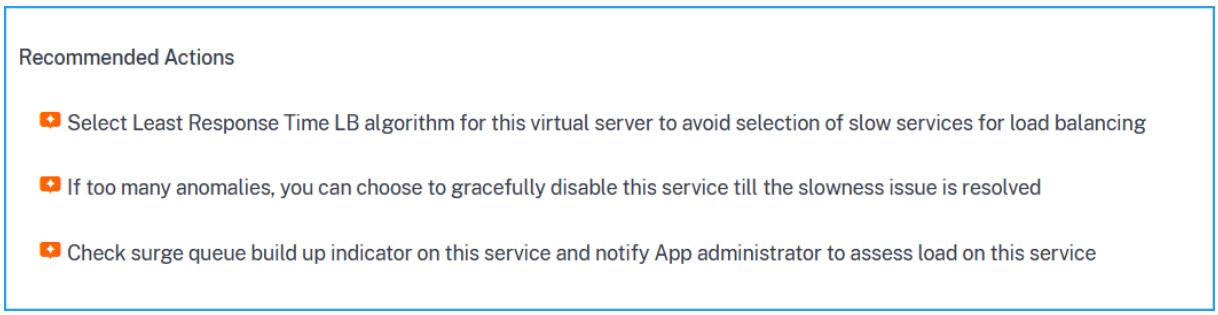


Temps de réponse

Sous **Détails des anomalies**, cliquez sur pour afficher les détails des contributeurs de temps de réponse (du client au serveur). L'exemple suivant présente une anomalie concernant la latence du réseau client, la latence réseau du serveur et le temps de traitement du serveur. Vous pouvez également afficher les plages attendues et la brèche qui s'est produite au-delà de la plage prévue.



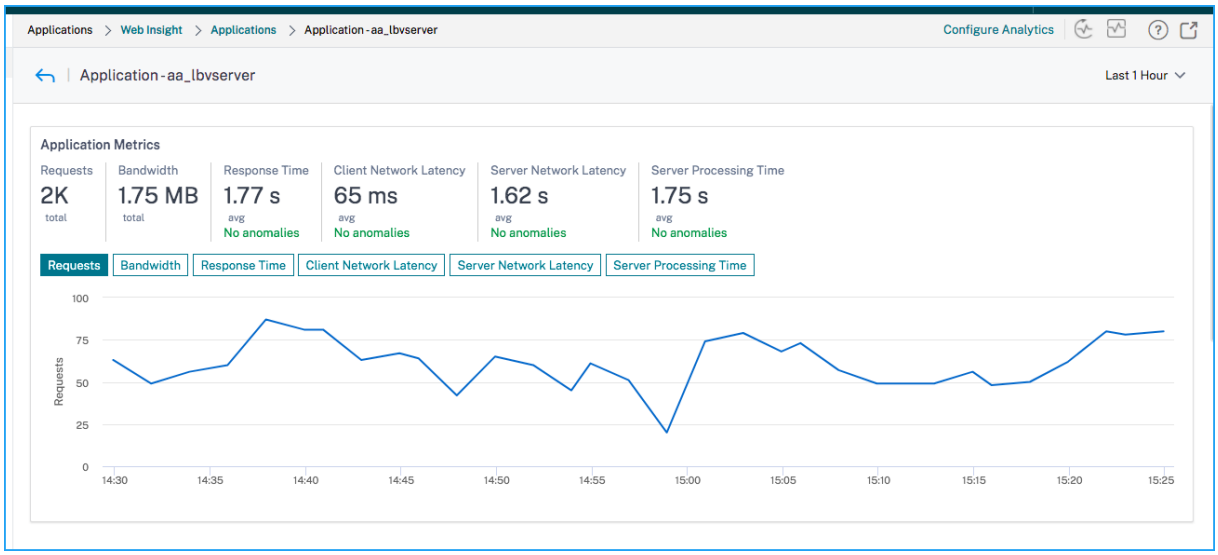
Les **actions recommandées** vous suggèrent les résolutions possibles pour les anomalies.



De même, vous pouvez cliquer sur les onglets **Latence réseau client, Latence**réseau**serveur et Temps de traitement** du serveur pour afficher :

- Anomalie qui a franchi la plage prévue.
- Actions recommandées qui vous suggèrent les résolutions possibles.

Si l'application fonctionne bien, vous pouvez afficher les mesures d'application comme aucune anomalie.



Graphique de service

February 1, 2024

La fonctionnalité graphique des services de NetScaler 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 NetScaler

- Applications Kubernetes
- Applications Web à 3 niveaux

Graphe de service pour les applications de toutes les instances NetScaler

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)
- Visualisez la vue de l'infrastructure (instance NetScaler) selon laquelle 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 NetScaler 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 métriques NetScaler
- Toutes les instances NetScaler dotées d'applications discrètes, d'applications personnalisées et d'applications de microservice discrètes
- 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 NetScaler 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 dans lequel les demandes des clients sont traitées et les métriques NetScaler 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**. NetScaler 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**. NetScaler 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**. NetScaler 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.

StyleBooks

February 1, 2024

StyleBooks simplifie la gestion des configurations NetScaler complexes pour vos applications. Un StyleBook est un modèle que vous pouvez utiliser pour créer et gérer des configurations NetScaler. Vous pouvez créer un StyleBook pour configurer une fonctionnalité spécifique de NetScaler, 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 détaillées expliquant comment y parvenir sur une instance NetScaler particulière. NetScaler Application Delivery Management (ADM) calcule la différence entre l'état existant sur un NetScaler et l'état souhaité que vous avez spécifié, et apporte les modifications nécessaires à l'infrastructure. Comme StyleBooks utilise une syntaxe déclarative, écrite en YAML, les composants d'un StyleBook peuvent être spécifiés dans n'importe quel ordre, et NetScaler 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.

- **Axé sur les applications** : StyleBooks peut être utilisé pour définir la configuration NetScaler 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 renseigner quelques paramètres pour créer ce qui peut être une configuration NetScaler complexe. Les configurations créées à partir de StyleBooks ne sont pas liées à l'infrastructure. Une configuration unique peut ainsi être déployée sur un ou plusieurs NetScalers, et peut également être déplacée entre les instances.
- **Interface utilisateur générée automatiquement** : NetScaler ADM génère automatiquement des formulaires d'interface utilisateur utilisés pour renseigner les paramètres du StyleBook lorsque la configuration est effectuée à l'aide de l'interface graphique NetScaler 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
- **Pilotée par API** : toutes les opérations de configuration sont prises en charge à l'aide de l'interface graphique NetScaler 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 NetScaler. 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 NetScaler ou sur une autre instance. Un nouveau pack de configuration est créé pour cette configuration. Un pack de configuration est enregistré à la fois sur NetScaler ADM et sur l'instance NetScaler sur laquelle la configuration est exécutée.

Vous pouvez soit utiliser les StyleBooks par défaut, fournis avec NetScaler ADM, pour créer des configurations pour votre déploiement, soit concevoir vos propres StyleBooks et les importer dans NetScaler ADM. Vous pouvez utiliser les StyleBooks pour créer des configurations à l'aide de l'interface graphique NetScaler 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

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 **Sécurité** > **Tableau de bord de sécurité**.
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.

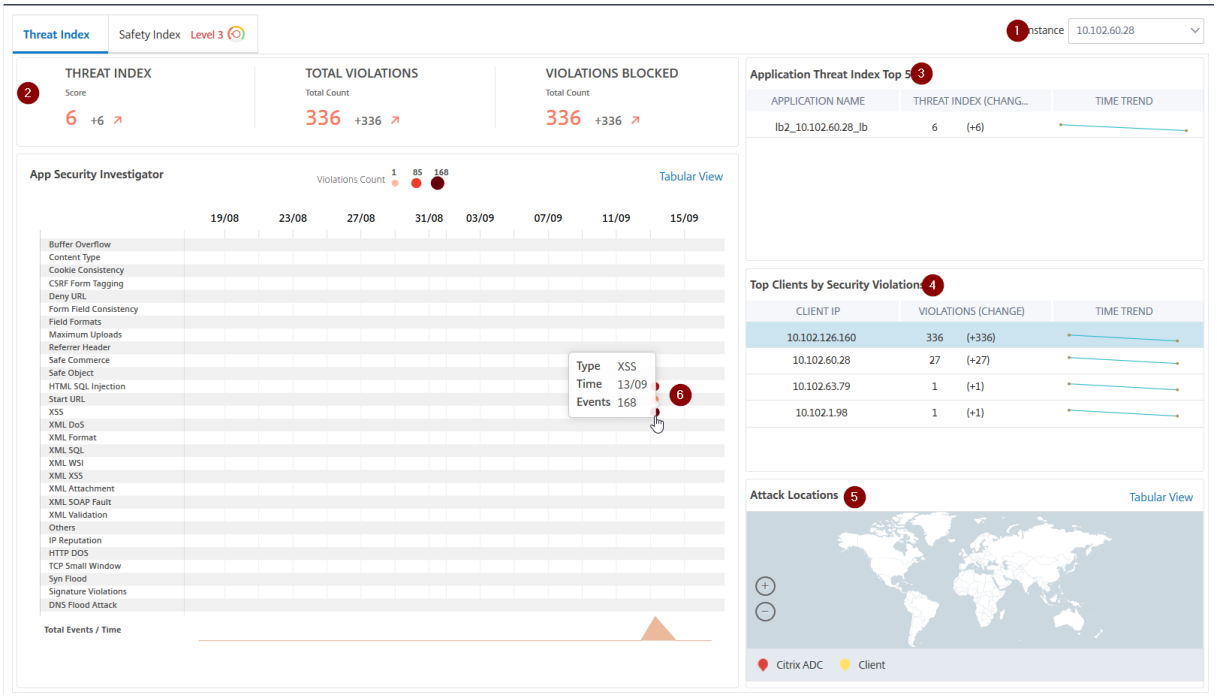
     L'indice des menaces est basé sur les informations d'attaque. Les informations relatives à l'attaque, telles que le type de violation, la catégorie d'attaque, l'emplacement et les détails du client, donnent un aperçu des attaques visant l'application. Les informations de violation sont envoyées à NetScaler 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**. Un système d'évaluation à un chiffre qui indique le niveau de sécurité avec lequel vous avez configuré les instances NetScaler 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'indice de sécurité prend en compte à la fois la configuration du pare-feu de l'application et la configuration de sécurité du système NetScaler. 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 NetScaler, telles qu'un mot de passe sécurisé pour l'utilisateur `nsroot`, ne sont pas fournies, 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 NetScaler pour laquelle vous pouvez consulter 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.

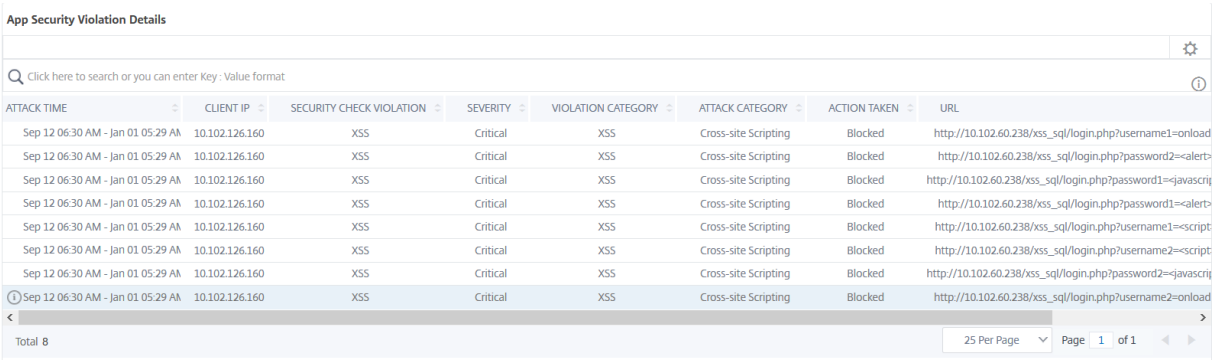
4 - Affiche les violations de sécurité en fonction des clients. Le graphique App Security Investigator s'affiche pour chaque client. Vous pouvez cliquer sur chaque adresse IP client pour afficher les résultats.

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.

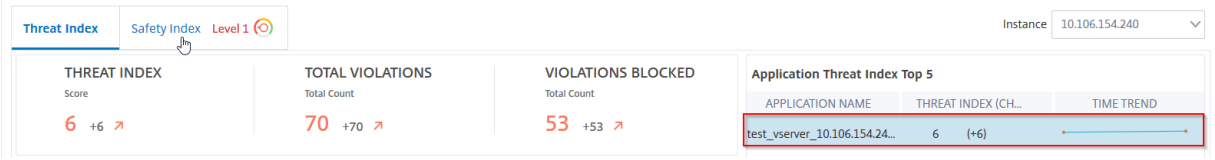
Détails de l'indice de sécurité

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.

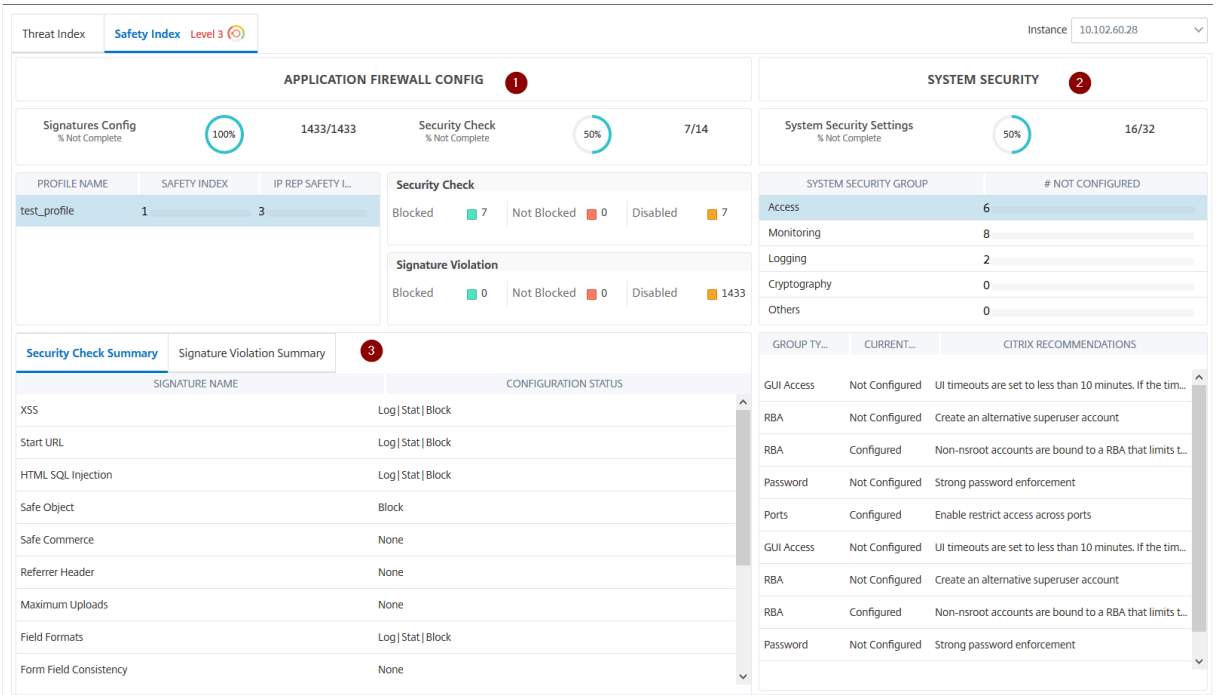
Le résumé de l'indice de sécurité fournit des informations sur l'efficacité des configurations de sécurité suivantes :

- **Configuration du pare-feu d'application**. Indique le nombre d'entités de signature et de sécurité qui ne sont pas configurées.
- **Sécurité du système NetScaler ADM**. 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 de menace en activant les **violations de sécurité WAF** pour les serveurs virtuels, puis en accédant à **Sécurité** > **Violations de sécurité**.

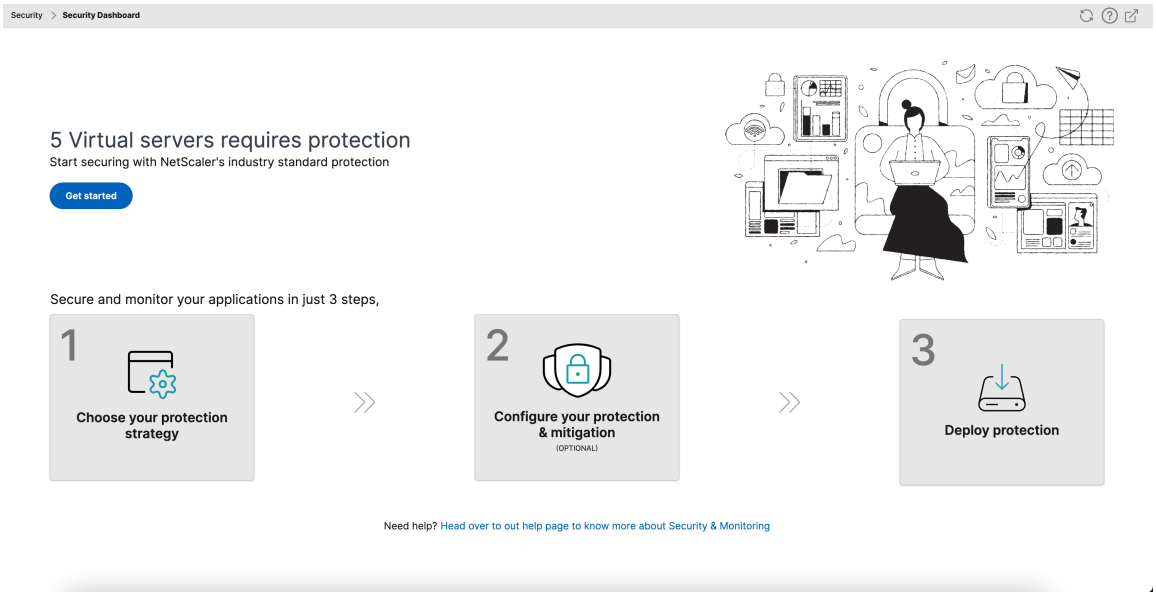
Tableau de bord de sécurité unifié

February 1, 2024

Le tableau **de bord Unified Security** est un tableau de bord à panneau unique dans lequel vous pouvez configurer les protections, activer les analyses et déployer les protections sur votre application. Dans ce tableau de bord, vous pouvez choisir parmi différentes options de modèle et effectuer l'ensemble du processus de configuration dans un flux de travail unique. Pour commencer, accédez à **Sécurité > Tableau de bord de sécurité**, puis cliquez sur **Gérer l'application**. Sur la page **Gérer l'application**, vous pouvez consulter les détails de vos applications sécurisées et non sécurisées.

> **Remarque :**
>
> - Si vous êtes un nouvel utilisateur ou si vous n'avez configuré aucune protection via Style-

Books ou directement sur les instances NetScaler, la page suivante apparaît lorsque vous **cliquez**sur Sécurité > Tableau de bord de sécurité.

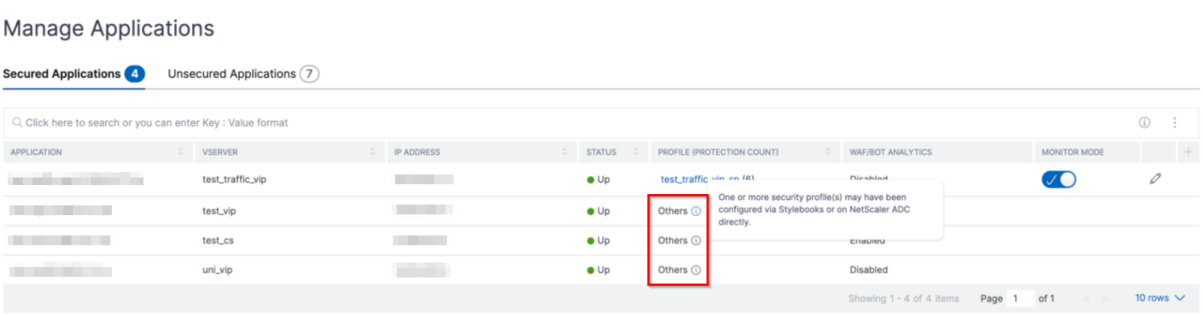


- Vous pouvez consulter le nombre total de serveurs virtuels nécessitant une protection. Cliquez sur **Commencer** pour afficher les détails de la section **Applications non sécurisées.**
- Les types de serveurs virtuels éligibles pour configurer les protections sont l'équilibrage de charge et la commutation de contenu.

Applications sécurisées

Vous pouvez consulter les détails après avoir configuré les protections à l'aide du tableau de bord de sécurité unifié. Pour plus d'informations, voir Configuration des protections pour les applications non sécurisées.

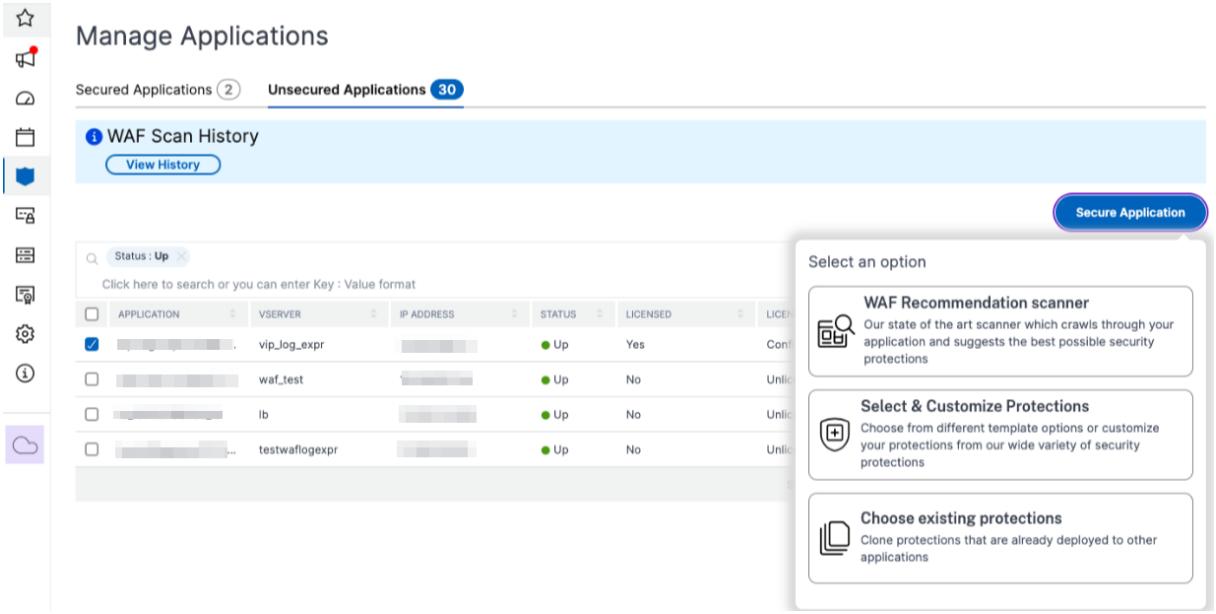
Si vous avez déjà configuré les protections directement sur les instances NetScaler ou via StyleBooks, vous pouvez consulter les applications dans l'onglet **Applications sécurisées** marqué comme **Autres** sous **Profil**.



Configurer les protections pour les applications non sécurisées

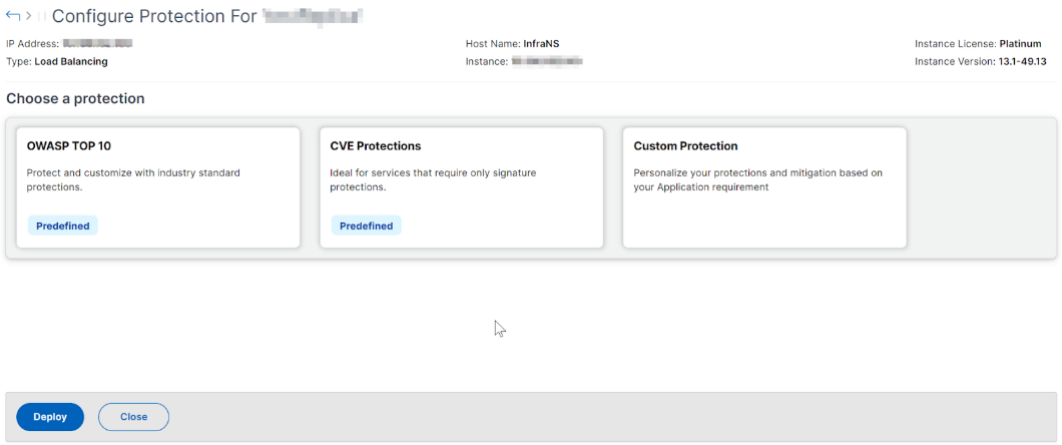
> **Remarque :**
>
> Le nombre maximum d'entités de configuration (règles) prises en charge dans la liste de blocage est de 32.

Dans l'onglet **Applications non sécurisées**, sélectionnez une application, puis cliquez sur **Application sécurisée**.



Vous pouvez sélectionner l'une des options suivantes pour protéger votre application :

- **Scanner de recommandations WAF** : cette option vous permet d'exécuter un scan sur votre application. Sur la base de certains paramètres de l'analyse, le résultat vous suggère les protections pour votre application. Vous pourriez envisager d'appliquer ces recommandations.
- **Sélectionnez et personnalisez les protections** : cette option vous permet de choisir parmi différentes options de modèle ou de personnaliser vos protections et de les déployer.



- **Top 10 de l'OWASP** - Un modèle prédéfini qui possède les protections standard de l'industrie contre les 10 principaux risques de sécurité de l'OWASP. Pour plus d'informations, consultez `https://owasp.org/www-project-top-ten/`.
- **Protections CVE** : vous pouvez créer le jeu de signatures à partir de la liste des règles de signature préconfigurées classées dans les catégories de vulnérabilités connues. Vous pouvez sélectionner des signatures pour configurer l'action de journalisation ou de blocage lorsqu'un modèle de signature correspond au trafic entrant. Le message du journal contient les détails de la vulnérabilité.
- **Protections personnalisées** : sélectionnez les protections et déployez-les en fonction de vos besoins.

- **Choisissez les protections existantes** : cette option clone les protections déployées dans une application existante. Si vous souhaitez déployer ces mêmes protections sur une autre application, vous pouvez sélectionner cette option et la déployer telle quelle sur une autre application. Vous pouvez également sélectionner cette option comme modèle, modifier les protections, puis déployer.

Scanner de recommandations WAF

> **Remarque :**
>
> - Vous ne pouvez exécuter qu'une seule analyse à la fois pour une application. Pour lancer une nouvelle analyse pour la même application ou une autre application, vous devez attendre que l'analyse précédente soit terminée.
> - Vous pouvez cliquer sur **Afficher l'historique** pour consulter l'historique et l'état des analyses précédentes. Vous pouvez également cliquer sur **Afficher le rapport**, puis appliquer les recommandations ultérieurement.

Pré-requis :

- L'instance NetScaler doit être 13.0 41.28 ou version ultérieure (pour les contrôles de sécurité) et 13.0 ou version ultérieure (pour les signatures).
- Doit avoir la licence premium.
- Doit être le serveur virtuel d'équilibrage de charge.

Pour commencer à utiliser l'analyse des recommandations WAF, vous devez fournir les informations suivantes :

1. Sous **Paramètres de numérisation** :
   - **Nom de domaine** —Spécifiez une adresse IP accessible valide ou le nom de domaine accessible au public qui est associé à l'application. Par exemple : `www.example.com`.

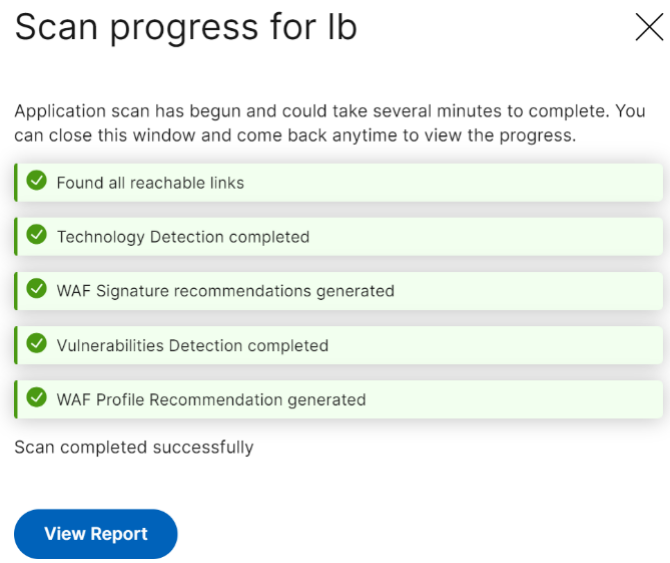
- **Protocole HTTP/HTTPS** —Sélectionnez le protocole de l'application.
- **Délai d'expiration du trafic** : temps d'attente (en secondes) pour une seule demande pendant l'analyse. La valeur doit être supérieure à 0.
- **URL à partir de laquelle lancer le scan** : page d'accueil de l'application à partir de laquelle lancer le scan. Par exemple, `https://www.example.com/home`. L'URL doit être une adresse IPv4 valide. Si les adresses IP sont privées, vous devez vous assurer qu'elles sont accessibles depuis l'adresse IP de gestion NetScaler ADM.
- **URL de connexion** : URL à laquelle les données de connexion sont envoyées à des fins d'authentification. En HTML, cette URL est communément appelée URL d'action.
- **Méthode d'authentification** : sélectionnez la méthode d'authentification prise en charge (par formulaire ou par en-tête) pour votre application.
  - L'authentification par formulaire nécessite l'envoi d'un formulaire à l'URL de connexion avec les informations de connexion. Ces informations d'identification doivent se présenter sous la forme de champs de formulaire et de leurs valeurs. L'application partage ensuite le cookie de session qui est utilisé pour maintenir les sessions pendant l'analyse.
  - L'authentification basée sur l'en-tête nécessite l'en-tête d'authentification et sa valeur dans la section des en-têtes. L'en-tête d'authentification doit avoir une valeur valide et est utilisé pour maintenir les sessions pendant l'analyse. Les champs du formulaire doivent rester vides pour les champs basés sur l'en-tête.
- **Méthode de demande** —Sélectionnez la méthode HTTP utilisée lors de l'envoi des données du formulaire à l'URL de connexion. Les méthodes de requête autorisées sont **POST**, **GET**et **PUT**.
- **Champs de formulaire** —Spécifiez les données du formulaire à envoyer à l'URL de connexion. Les champs de formulaire ne sont obligatoires que si vous sélectionnez l'authentification par formulaire. Vous devez spécifier dans les paires clé-valeur, où **le nom du champ** est la clé et la valeur du **champ est la valeur** . Assurez-vous que tous les champs de formulaire nécessaires au fonctionnement de la connexion sont correctement ajoutés, y compris les mots de passe. Les valeurs sont cryptées avant d'être stockées dans la base de données. Vous pouvez cliquer sur **Ajouter** pour ajouter plusieurs champs de formulaire. Par exemple, **Nom du champ** —nom d'utilisateur et **Valeur du champ** —admin.
- **URL de déconnexion** —Spécifiez l'URL qui met fin à la session après l'accès. Par exemple : `https://www.example.com/customer/logout`.

2. Sous **Configurations de numérisation** :
   - **Vulnérabilités à vérifier** : sélectionnez les vulnérabilités que le scanner doit détecter. Actuellement, cela est fait pour les violations de scripts intersites et d'injection SQL. Par dé-

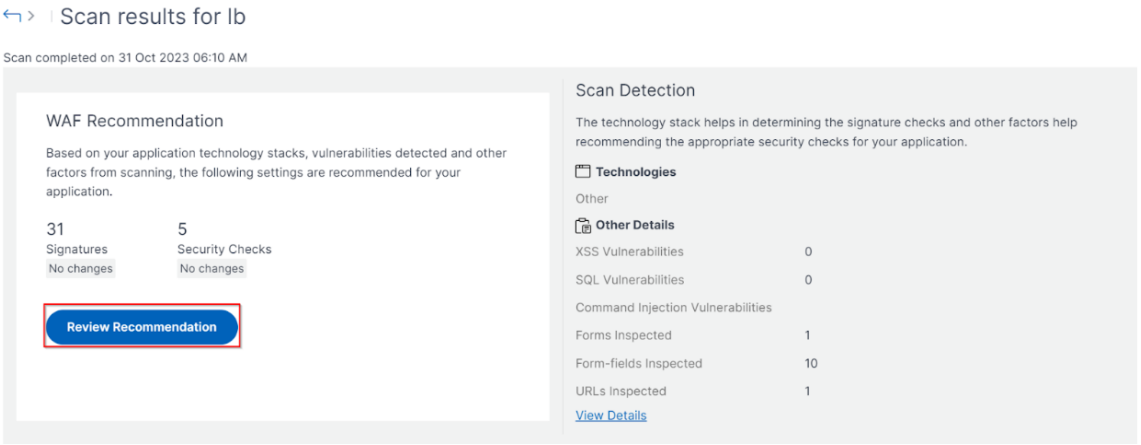
faut, toutes les violations sont sélectionnées. Après avoir sélectionné les vulnérabilités, il simule ces attaques sur l'application pour signaler la vulnérabilité potentielle. Il est recommandé d'activer cette détection qui ne se trouve pas dans l'environnement de production. Toutes les autres vulnérabilités sont également signalées, sans simuler ces attaques sur l'application.

- **Limite de taille de réponse** : limite maximale de la taille de réponse. Toutes les réponses dépassant la valeur mentionnée ne sont pas scannées. La limite recommandée est de 10 Mo (1 000 000 octets).
- **Simultanéité** des demandes : nombre total de demandes envoyées à l'application Web en parallèle.

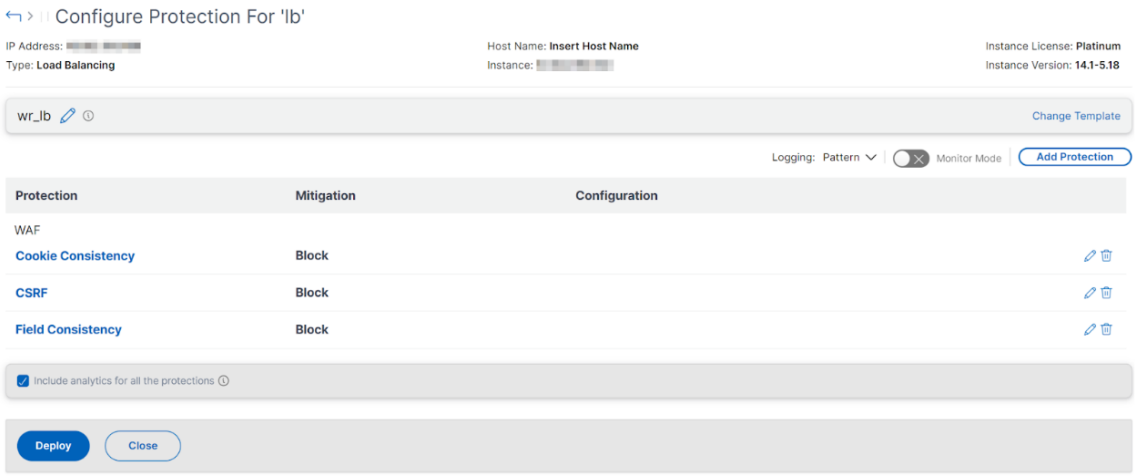
3. La configuration des paramètres de numérisation WAF est terminée. Vous pouvez cliquer sur **Démarrer le scan** pour lancer le processus de numérisation et attendre la fin de la progression. Une fois l'analyse terminée, cliquez sur **Afficher le rapport**.



4. Sur la page des résultats de l'analyse, cliquez sur **Réviser la recommandation**.



5. Passez en revue les protections ou modifiez/ajoutez d'autres protections, puis cliquez sur **Déployer**.

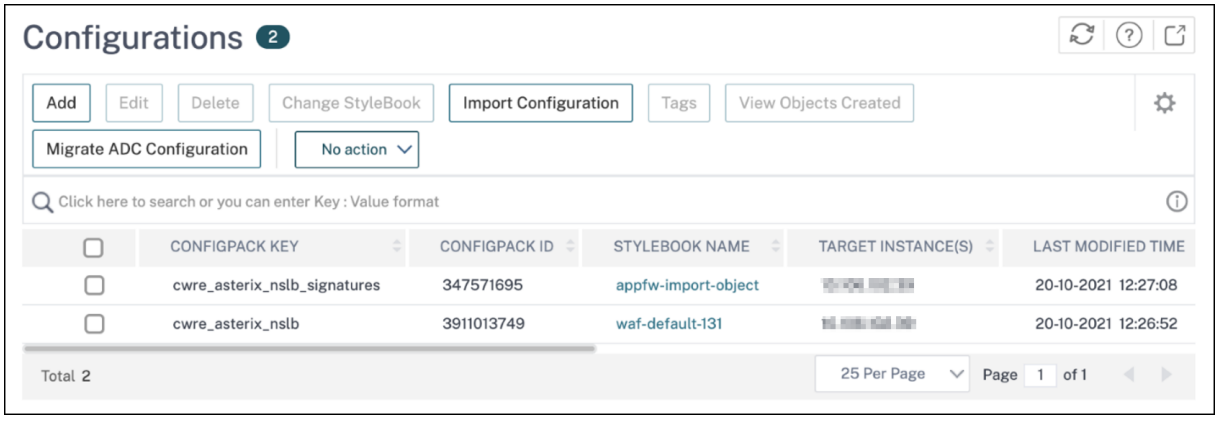


Lorsque vous appliquez les contrôles de sécurité avec succès :

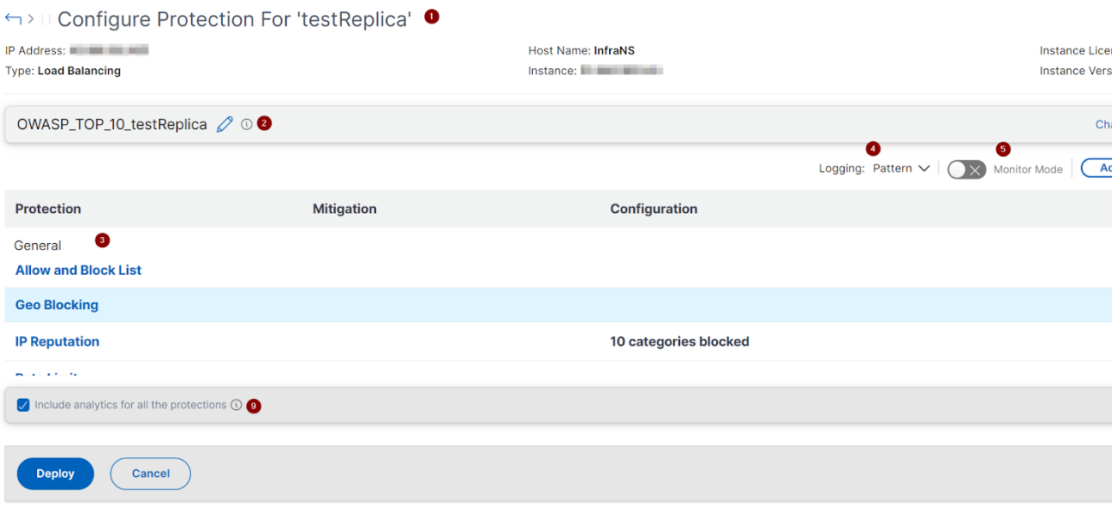
- La configuration est appliquée à l'instance NetScaler via StyleBooks, en fonction de la version.
  - Pour NetScaler 13.0, le StyleBook `unified-appsec-protection-130` est utilisé.
  - Pour NetScaler 13.1, le StyleBook `unified-appsec-protection-131` est utilisé.
  - Pour NetScaler 14.1, le StyleBook `unified-appsec-protection-141` est utilisé.
- Le profil `Appfw` est créé sur votre NetScaler et lié à l'application à l'aide de `policylabel`.
- Les signatures sont liées au profil appfw, si les signatures recommandées sont déjà appliquées.

> **Remarque**
>
> Les contrôles de sécurité sont pris en charge dans NetScaler 13.0 41.28 ou version ultérieure.

Vous pouvez vérifier que les profils et les signatures WAF sont appliqués via les StyleBooks par défaut en accédant à **Applications > Configuration > Packs de configuration**.



Sélectionnez et personnalisez les protections



Top 10 de OWASP

1 - Fournit des informations sur l'application, telles que l'adresse IP, le type de serveur virtuel, le type de licence, l'instance à partir de laquelle l'application est configurée, etc.

2 - Affiche le modèle sélectionné. Vous pouvez le renommer selon votre choix.

3 - Affiche les protections. Certaines protections nécessitent des informations supplémentaires.

4 - Affiche le type de journal détaillé. Vous pouvez sélectionner les options suivantes :

- **Modèle**. Consigne uniquement le modèle de violation.
- **Charge utile du modèle**. Modèle de violation des journaux et 150 octets de charge utile JSON supplémentaire.
- **Modèle, charge utile, en-tête**. Enregistre le schéma de violation, 150 octets de charge utile JSON supplémentaire et les informations d'en-tête HTTP.

5 - Permet d'activer le mode Moniteur. Si vous activez le mode Moniteur, le trafic est uniquement enregistré et les mesures d'atténuation ne sont pas activées.

6 - Permet d'ajouter des protections supplémentaires. Cliquez sur **Ajouter des protections** et consultez-les pour les ajouter.

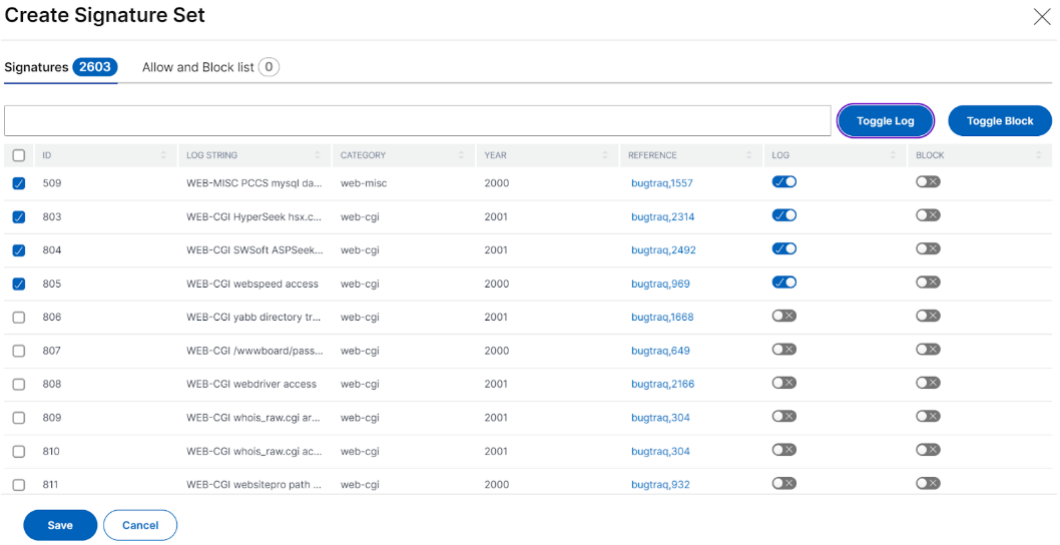
7 - Vous permet de choisir un nouveau modèle à l'aide de l'option Modifier le modèle.

8 - Permet de modifier ou de supprimer la protection.

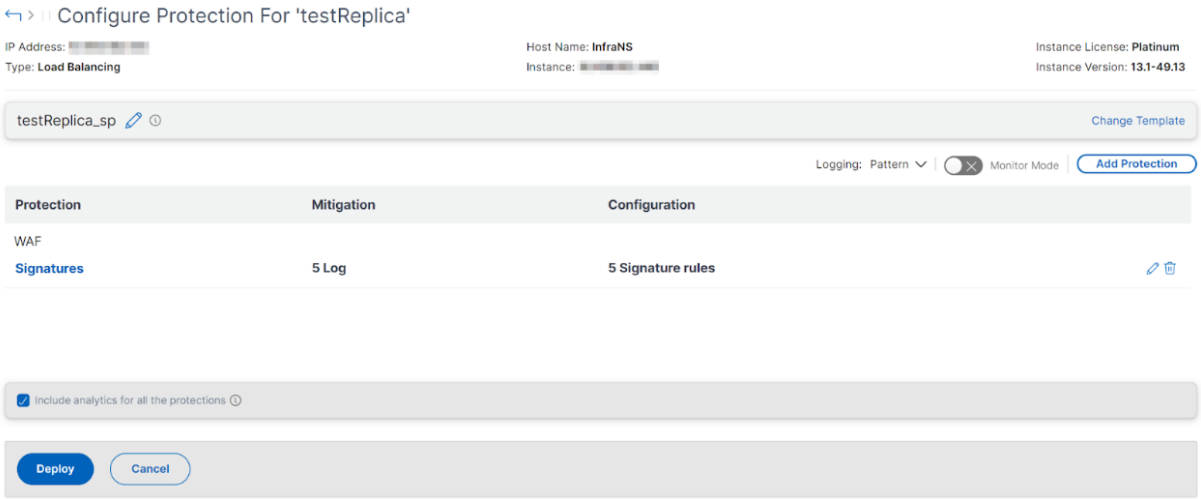
9 - Active l'analyse des protections que vous sélectionnez. Cette option est sélectionnée par défaut. Vous pouvez consulter les analyses relatives aux protections configurées dans **Sécurité > Violations de sécurité**.

Après avoir configuré les protections, cliquez sur **Déployer**.

Protections contre les CVE Pour déployer les protections CVE, cliquez sur **Créer une protection CVE.** Sur la page **Créer un ensemble de signatures**, sélectionnez les signatures dans la liste pour configurer le journal ou bloquer l'action, puis cliquez sur **Enregistrer**.

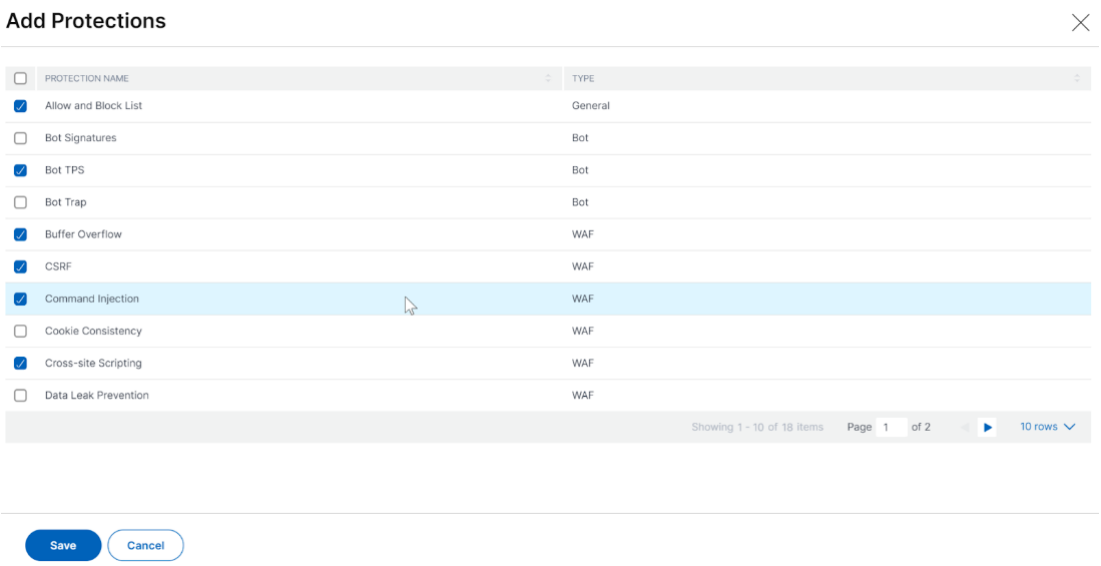


Après avoir cliqué sur **Enregistrer**, vous pouvez consulter les signatures ajoutées à la page de configuration.



Vous pouvez également cliquer sur **Ajouter une protection** pour ajouter des protections supplémentaires à l'application. Après avoir configuré toutes les protections, cliquez sur **Déployer**.

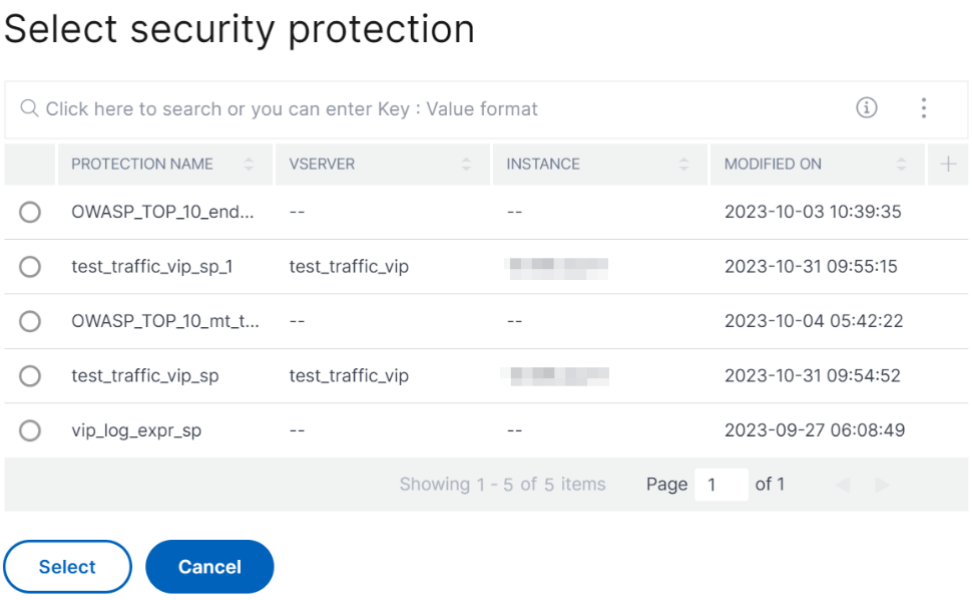
Protection personnalisée Pour déployer avec des protections adaptées à vos besoins, cliquez sur **Créer une nouvelle protection**. Sur la page **Ajouter des protections**, sélectionnez les protections que vous souhaitez déployer et cliquez sur **Enregistrer**.



Après avoir cliqué sur **Enregistrer**, passez en revue les protections sélectionnées sur la page de configuration, puis cliquez sur **Déployer**.

Choisissez les protections existantes

Pour déployer les protections existantes d'une application vers une autre, sélectionnez une protection existante dans la liste.



Une fois que vous avez sélectionné une protection, les protections existantes sont clonées et affichées sur la page de configuration. Vous pouvez modifier en fonction de vos besoins, puis cliquer sur **Déployer**.

Afficher les détails des violations de sécurité des applications

February 1, 2024

Les applications Web exposées à Internet sont devenues très vulnérables aux attaques. NetScaler ADM vous permet de visualiser les détails des violations exploitables afin de protéger les applications contre les attaques. Accédez à **Sécurité** > **Violations de sécurité** pour obtenir une solution à volet unique permettant de :

- Visualisez les applications avec une visibilité complète sur les détails des menaces associées à la fois aux violations de sécurité WAF et aux violations de sécurité des bots
- 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 NetScaler. Pour plus d'informations, consultez Configurer l'analyse intelligente des applications.

Intégration à Splunk

February 1, 2024

Vous pouvez désormais intégrer NetScaler ADM à Splunk pour consulter les analyses relatives à :

- Violations du WAF
- Violations liées aux robots
- Informations sur les certificats SSL

- Événements et indicateurs

Le module complémentaire Splunk vous permet de :

- Combinez toutes les autres sources de données externes.
- Offrez une meilleure visibilité des analyses dans un endroit centralisé.

NetScaler ADM collecte les événements Bot, WAF et SSL et les envoie régulièrement à Splunk. Le module complémentaire Splunk Common Information Model (CIM) convertit les événements en données compatibles CIM. En tant qu'administrateur, à l'aide des données compatibles CIM, vous pouvez consulter les événements dans le tableau de bord Splunk.

Pour une intégration réussie, vous devez :

- Configurer Splunk pour recevoir des données de NetScaler ADM
- Configurer NetScaler ADM pour exporter des données vers Splunk
- Afficher les tableaux de bord dans Splunk

Configurer Splunk pour recevoir des données de NetScaler ADM

Dans Splunk, vous devez :

1. Configurez le point de terminaison du collecteur d'événements HTTP Splunk et générez un jeton
2. Installez le module complémentaire Splunk Common Information Model (CIM)
3. Installez le normalisateur CIM (applicable uniquement pour WAF et les informations sur les robots)
4. Préparer un exemple de tableau de bord dans Splunk

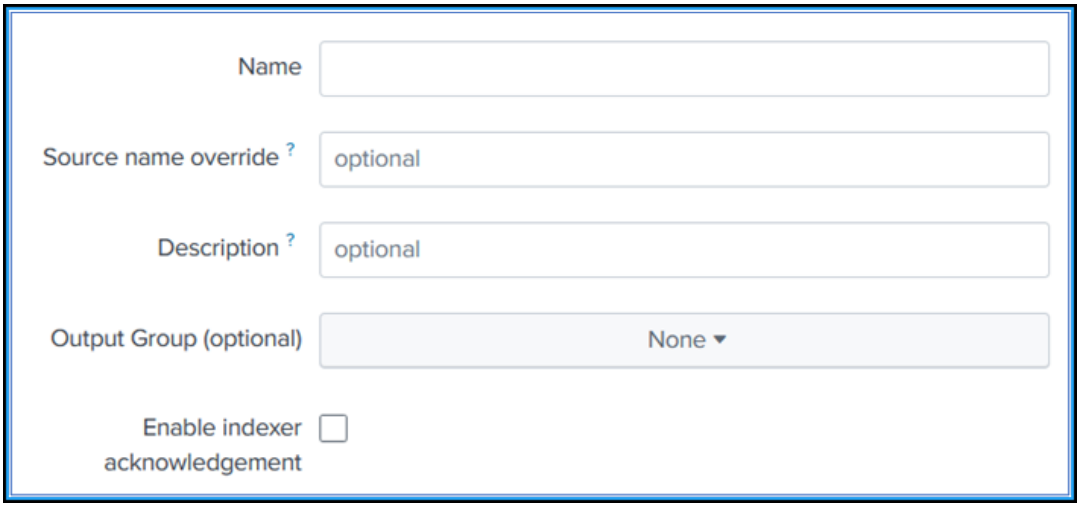
Configurez le point de terminaison du collecteur d'événements HTTP Splunk et générez un jeton

Vous devez d'abord configurer le collecteur d'événements HTTP dans Splunk. Cette configuration permet l'intégration entre l'ADM et Splunk pour envoyer les données. Ensuite, vous devez générer un jeton dans Splunk pour :

- Activez l'authentification entre ADM et Splunk.
- Recevez des données via le point de terminaison du collecteur d'événements.

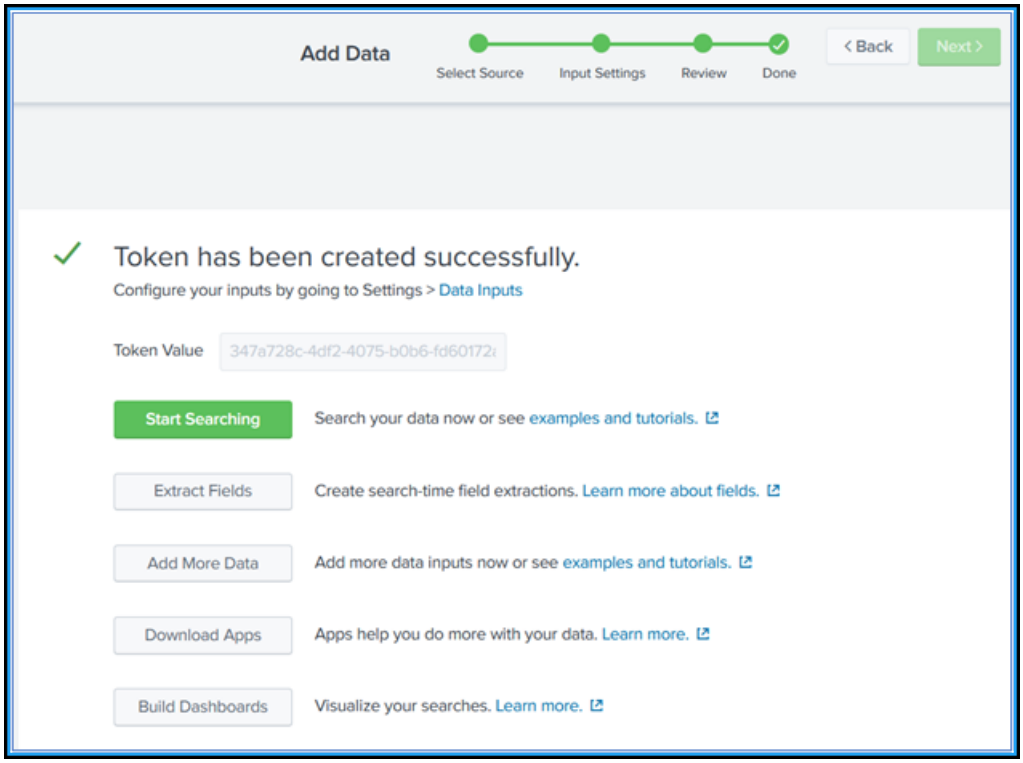
1. Connectez-vous à Splunk.

2. Accédez à **Paramètres > Entrées de données > Collecteur d'événements HTTP** et cliquez sur **Ajouter nouveau**.
3. Spécifiez les paramètres suivants :
   a) **Nom** : Spécifiez le nom de votre choix.
   b) **Remplacement du nom de la source (facultatif)** : si vous définissez une valeur, elle remplace la valeur source du collecteur d'événements HTTP.
   c) **Description (facultatif)** : Spécifiez une description.
   d) **Groupe de sortie (facultatif)** : Par défaut, cette option est sélectionnée sur Aucun.
   e) **Activer l'accusé de réception de l'indexeur** : par défaut, cette option n'est pas sélectionnée.



4. Cliquez sur **Suivant**.
5. Vous pouvez éventuellement définir des paramètres d'entrée supplémentaires sur la page **Paramètres d'entrée** .
6. Cliquez sur **Vérifier** pour vérifier les entrées, puis cliquez sur **Soumettre**.

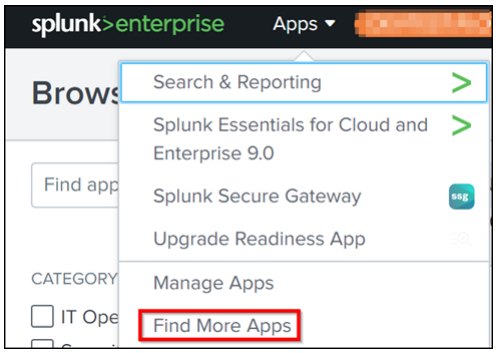
   Un jeton est généré. Vous devez utiliser ce jeton lorsque vous ajoutez des détails dans NetScaler ADM.



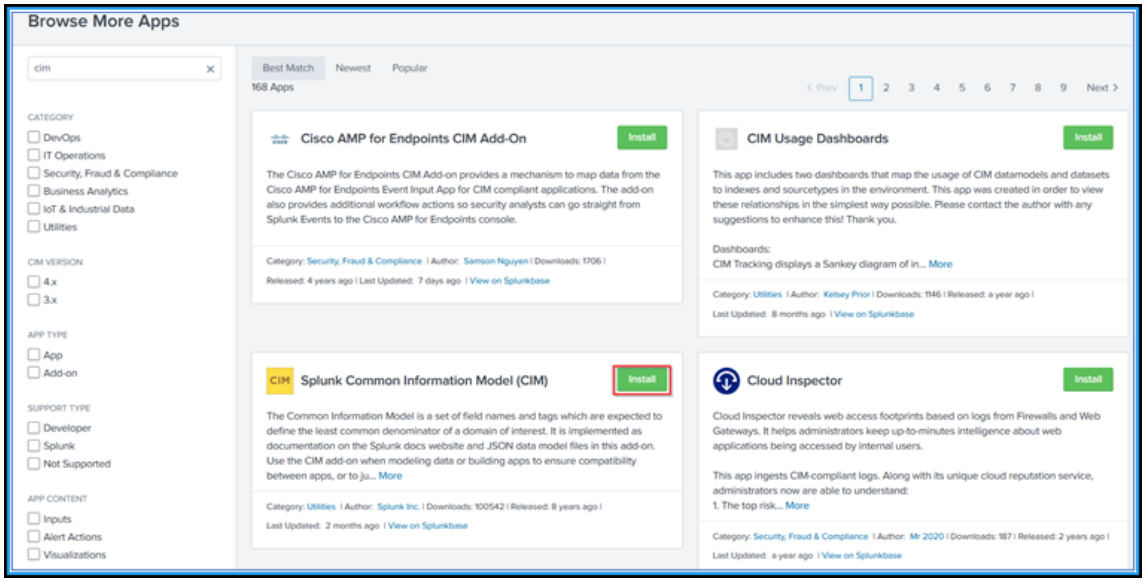
Installation du modèle d'information commun de Splunk

Dans Splunk, vous devez installer le module complémentaire Splunk CIM. Ce module complémentaire garantit que les données reçues de NetScaler ADM normalisent les données ingérées et correspondent à une norme commune en utilisant les mêmes noms de champs et balises d'événement pour des événements équivalents.

1. Connectez-vous à Splunk.
2. Accédez à **Applications > Rechercher d'autres applications**.



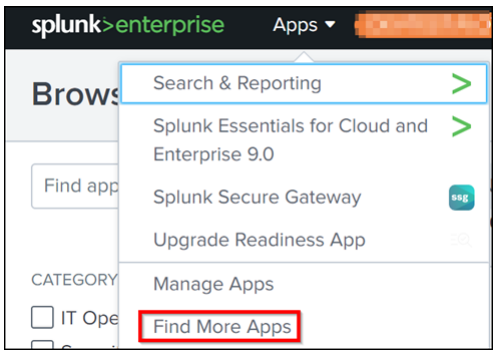
3. Tapez **CIM** dans la barre de recherche et appuyez sur **Entrée** pour obtenir le module complémentaire **Splunk Common Information Model (CIM)**, puis cliquez sur **Installer**.



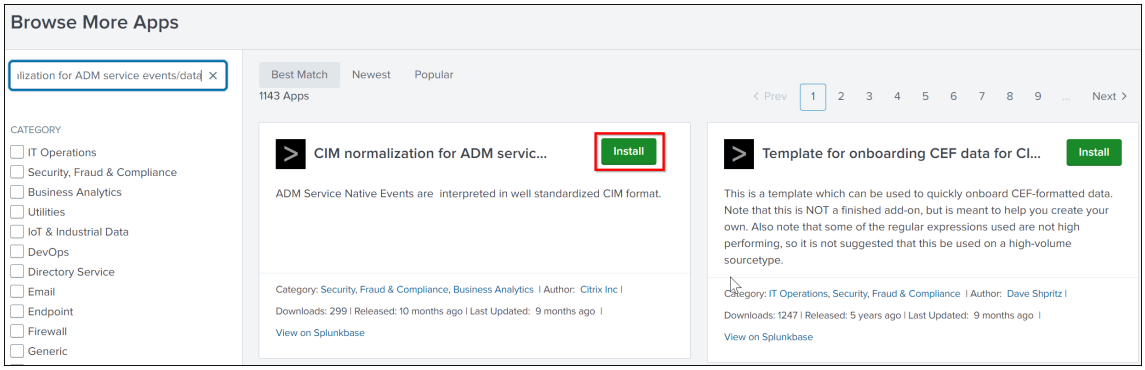
Installez le normalisateur CIM

Le normalisateur CIM est un plug-in supplémentaire que vous devez installer pour afficher les informations sur les WAF et les robots dans Splunk.

1. Sur le portail Splunk, accédez à **Applications > Rechercher d'autres**applications.



2. Tapez la **normalisation CIM pour les événements/données du service ADM** dans la barre de recherche, appuyez sur **Entrée** pour obtenir le module complémentaire, puis cliquez sur **Installer**.



Préparer un exemple de tableau de bord dans Splunk

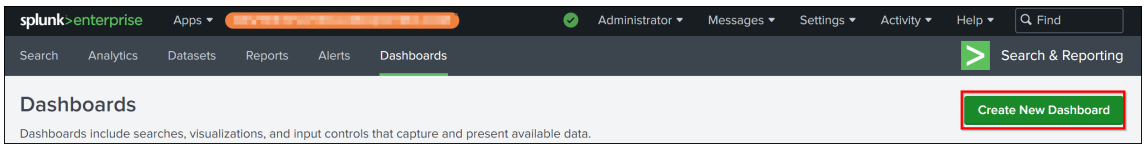
Après avoir installé Splunk CIM, vous devez préparer un exemple de tableau de bord à l'aide d'un modèle pour WAF et Bot, d'informations sur les certificats SSL, ainsi que d'événements et de statistiques. Vous pouvez télécharger le fichier modèle de tableau de bord (`.tgz`), utiliser n'importe quel éditeur (par exemple, le bloc-notes) pour copier son contenu et créer un tableau de bord en collant les données dans Splunk.

> **Remarque :**
>
> La procédure suivante pour créer un exemple de tableau de bord s'applique à tous les cas d'utilisation. Vous devez utiliser le `json` fichier requis.

1. Connectez-vous à la page de téléchargement de Citrix et téléchargez l'exemple de tableau de bord disponible sous Exemples de tableaux de bord pour terminaux tiers.
2. Extrayez le fichier, `json` ouvrez-le à l'aide de n'importe quel éditeur et copiez les données du fichier.

   Après avoir extrait, vous obtenez trois fichiers `json`. Utilisez le :

   - `adm_splunk_security_violations.json` fichier pour créer un exemple de tableau de bord WAF et Bot.
   - `adm_splunk_ssl_certificate.json` fichier pour créer un exemple de tableau de bord sur les certificats SSL.
   - `adm_splunk_events_and_metrics_history.json` fichier pour créer un tableau de bord des événements et des statistiques ADM.
3. Sur le portail Splunk, accédez à **Recherche et rapports > Tableaux** de bord, puis cliquez sur **Créer un nouveau**tableau de bord.



4. Sur la page **Créer un nouveau tableau de bord**, spécifiez les paramètres suivants :

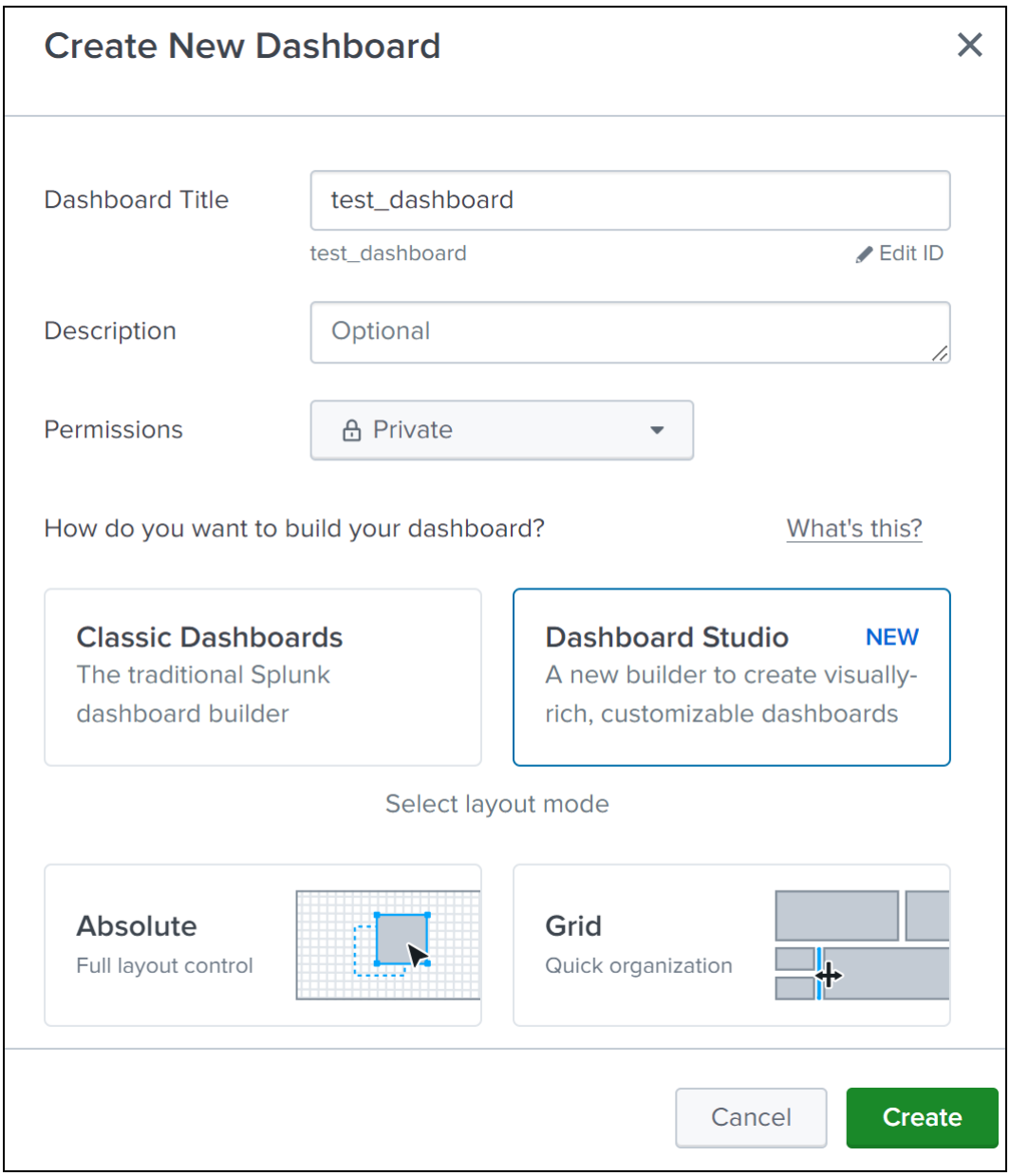
   a) **Titre du tableau** de bord : indiquez le titre de votre choix.

   b) **Description** : vous pouvez éventuellement fournir une description à titre de référence.

   c) **Autorisation** : sélectionnez **Privé** ou **Partagé dans l'application en** fonction de vos besoins.

   d) Sélectionnez **Dashboard Studio**.

   e) Sélectionnez une disposition (**Absolue** ou **Grille**), puis cliquez sur **Créer**.

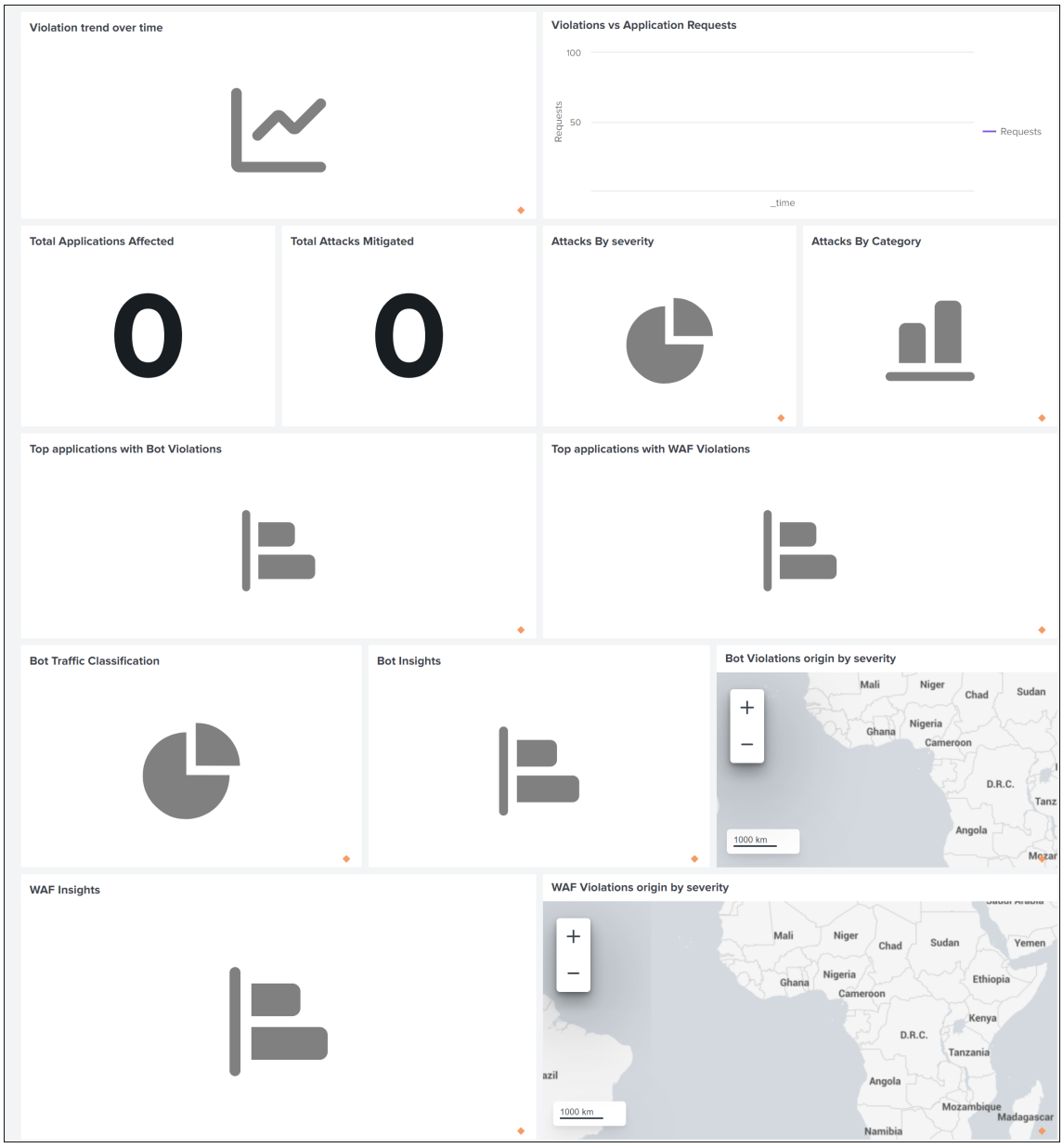


Après avoir cliqué sur **Créer**, sélectionnez l'icône **Source** dans la mise en page.

5. Supprimez les données existantes, collez les données que vous avez copiées à l'étape 2, puis cliquez sur **Retour**.
6. Cliquez sur **Enregistrer**.

   Vous pouvez consulter l'exemple de tableau de bord.

   Voici un exemple de tableau de bord pour WAF et bot.



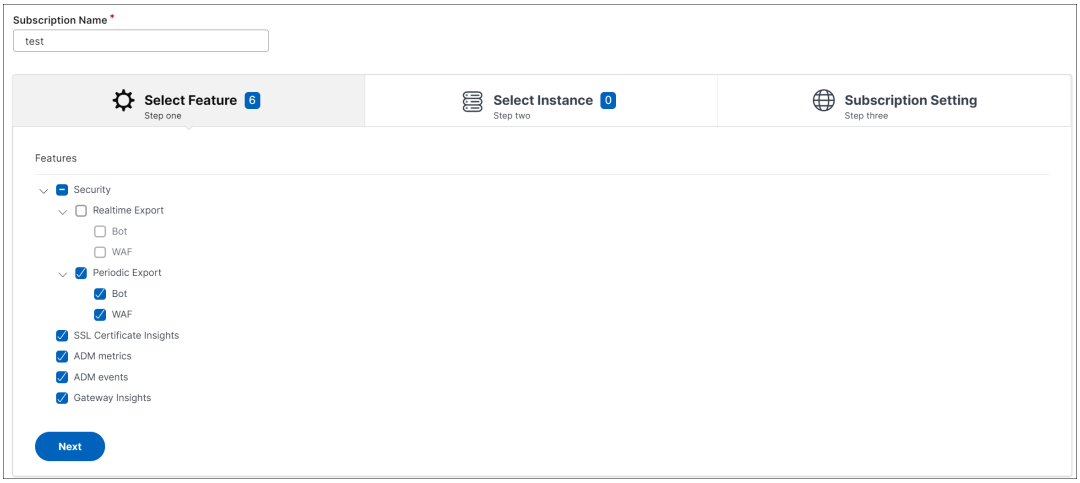
Configurer NetScaler ADM pour exporter des données vers Splunk

Tout est désormais prêt dans Splunk. La dernière étape consiste à configurer NetScaler ADM en créant un abonnement et en ajoutant le jeton.

À la fin de la procédure suivante, vous pouvez consulter le tableau de bord mis à jour dans Splunk qui est actuellement disponible dans votre NetScaler ADM :

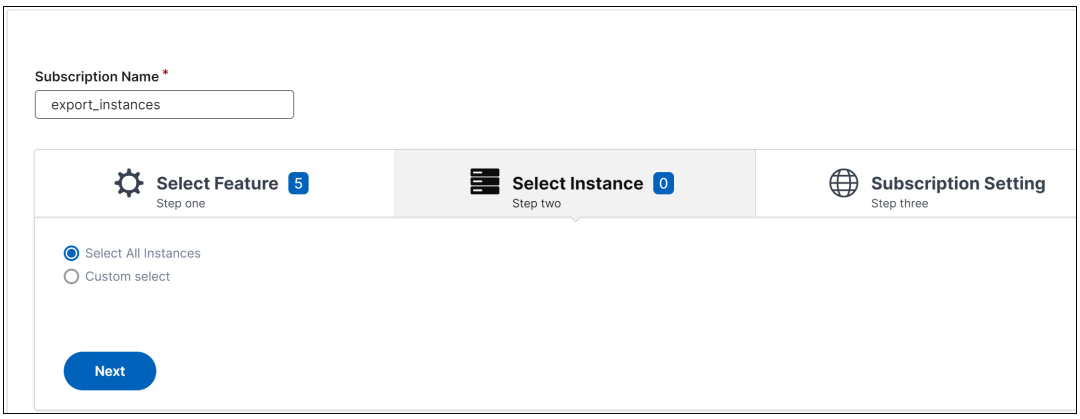
1. Connectez-vous à NetScaler ADM.
2. Accédez à **Paramètres > Intégration de l'écosystème**.
3. Sur la page **Abonnements**, cliquez sur **Ajouter**.
4. Indiquez le nom de votre choix dans le champ **Nom de l'abonnement** .
5. Dans l'onglet **Sélectionner une fonctionnalité**, vous pouvez sélectionner les fonctionnalités que vous souhaitez exporter et cliquer sur **Suivant**.

    - **Exportation en temps réel** : les violations sélectionnées sont immédiatement exportées vers Splunk.
    - **Exportation périodique** : les violations sélectionnées sont exportées vers Splunk en fonction de la durée que vous sélectionnez.



6. Dans l'onglet **Sélectionner une instance**, vous pouvez choisir **Sélectionner toutes les instances** ou **Sélection personnalisée**, puis cliquer sur **Suivant**.

    - **Sélectionnez toutes les instances** : exporte les données de toutes les instances NetScaler vers Splunk.
    - **Sélection personnalisée** : vous permet de sélectionner les instances NetScaler dans la liste. Si vous sélectionnez des instances spécifiques dans la liste, les données sont exportées vers Splunk uniquement à partir des instances NetScaler sélectionnées.



7. Dans l'onglet **Paramètres d'abonnement** :

   a) **Type de point final** : sélectionnez **Splunk**.

   b) **URL du point de terminaison** : spécifiez les détails du point de terminaison Splunk. Le point final doit être au format https://SPLUNK_PUBLIC_IP:SPLUNK_HEC_PORT/services/collector/event.

   > **Remarque**
   >
   > Il est recommandé d'utiliser le protocole HTTPS pour des raisons de sécurité.

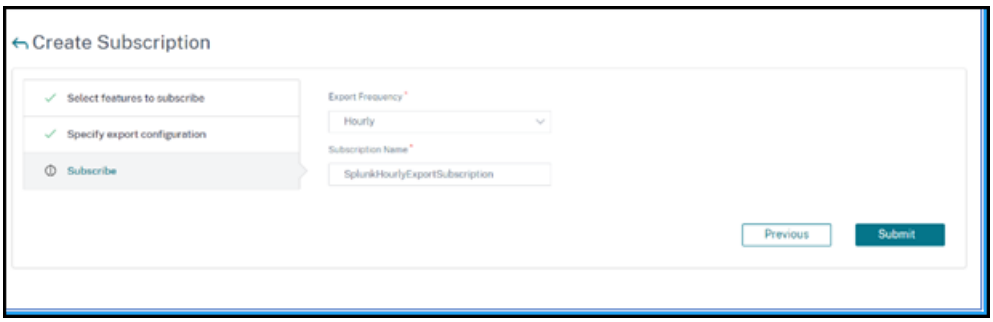
   - **SPLUNK_PUBLIC_IP** —Adresse IP valide configurée pour Splunk.
   - **SPLUNK_HEC_PORT** —Indique le numéro de port que vous avez spécifié lors de la configuration du point de terminaison de l'événement HTTP. Le numéro de port par défaut est 8088.
   - **Services/Collector/Event** —Indique le chemin de l'application HEC.

   c) **Jeton d'authentification** —Copiez et collez le jeton d'authentification depuis la page Splunk.

   d) **Sélectionnez la fréquence** : sélectionnez **Quotidien** ou **Horaire** dans la liste. En fonction de la sélection, NetScaler ADM exporte les détails vers Splunk.

   > **Remarque**
   >
   > Applicable uniquement si vous avez sélectionné des violations dans **l'exportation périodique**.

   e) Cliquez sur **Envoyer**.



Remarque

- Lorsque vous configurez avec **l'option d'exportation périodique** pour la première fois, les données des fonctionnalités sélectionnées sont immédiatement transférées vers Splunk. La fréquence d'exportation suivante se produit en fonction de votre sélection (quotidienne ou horaire).
- Lorsque vous configurez pour la première **fois avec l'option d'exportation en temps réel**, les données des fonctionnalités sélectionnées sont transmises à Splunk immédiatement dès que les violations sont détectées dans NetScaler ADM.

Afficher les tableaux de bord dans Splunk

Une fois que vous avez terminé la configuration dans NetScaler ADM, les données sont exportées depuis NetScaler ADM et les événements apparaissent dans Splunk.

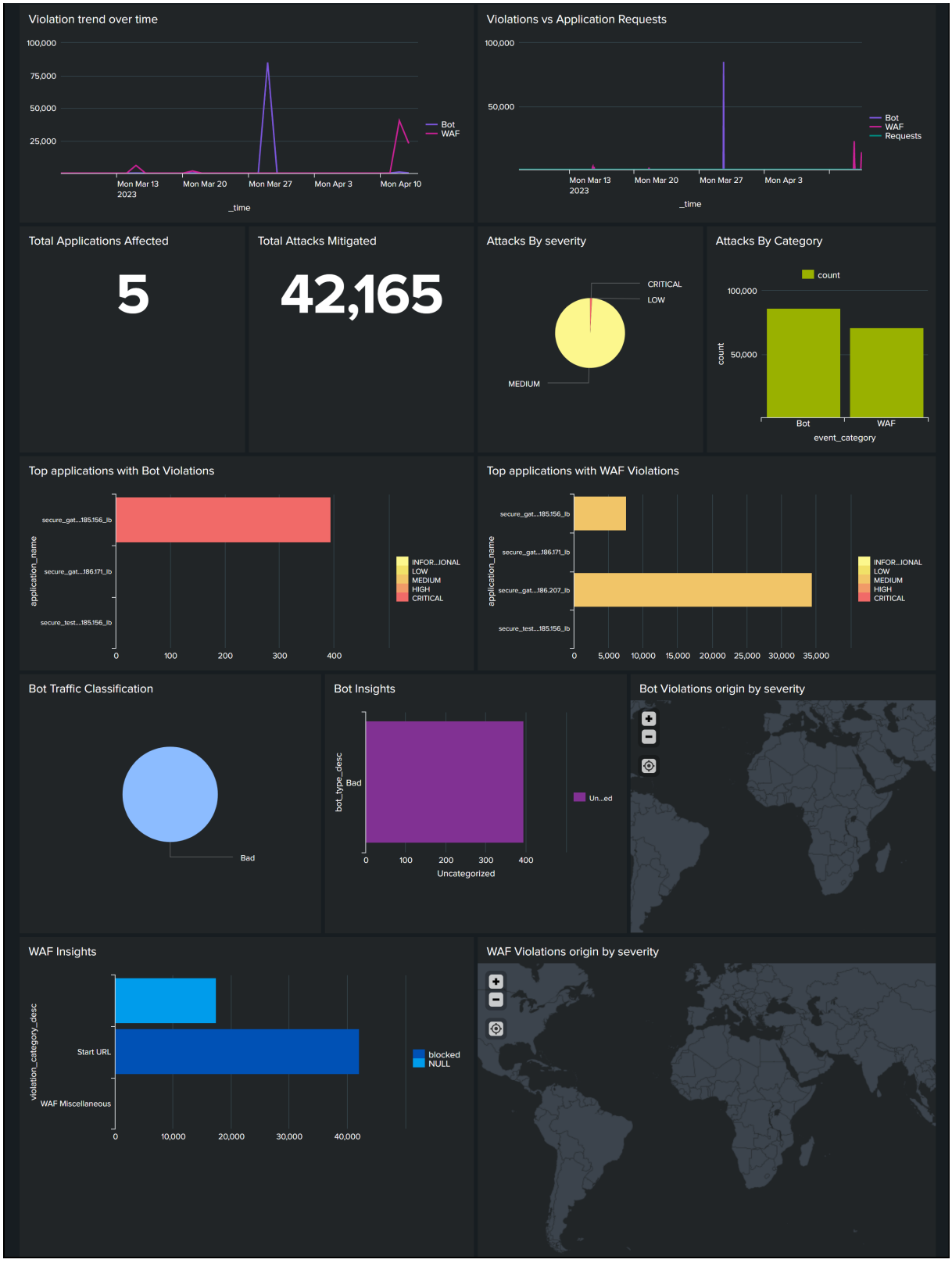
Remarque :

Pour consulter immédiatement les données actualisées relatives aux certificats SSL dans Splunk, cliquez sur **Poll now** dans le tableau de bord SSL de NetScaler ADM (**Infrastructure > Tableau de bord SSL**).

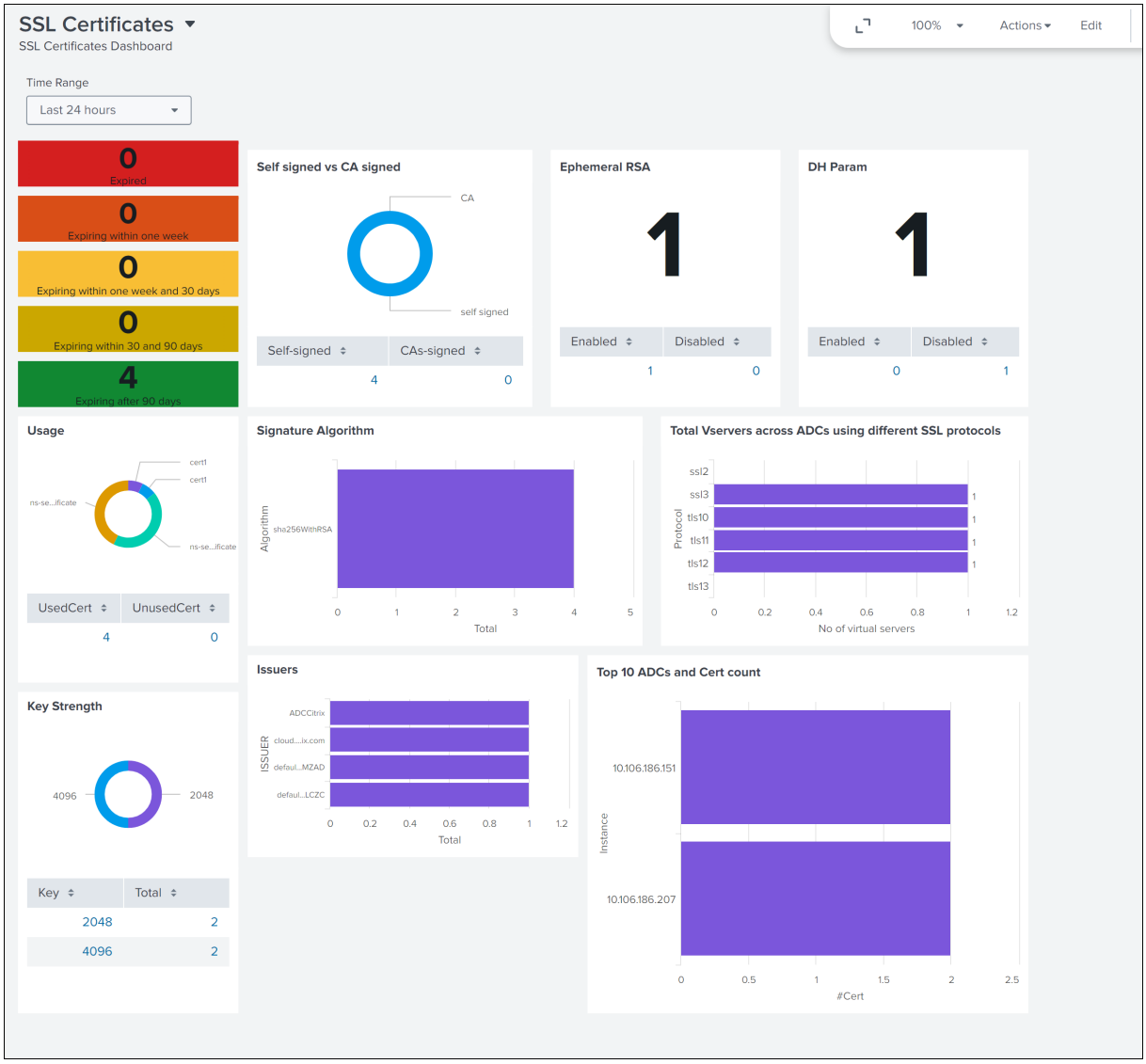
Vous êtes prêt à consulter le tableau de bord mis à jour dans Splunk sans aucune étape supplémentaire.

Accédez à Splunk et cliquez sur le tableau de bord que vous avez créé pour afficher le tableau de bord mis à jour.

Voici un exemple de tableau de bord WAF et Bot mis à jour :

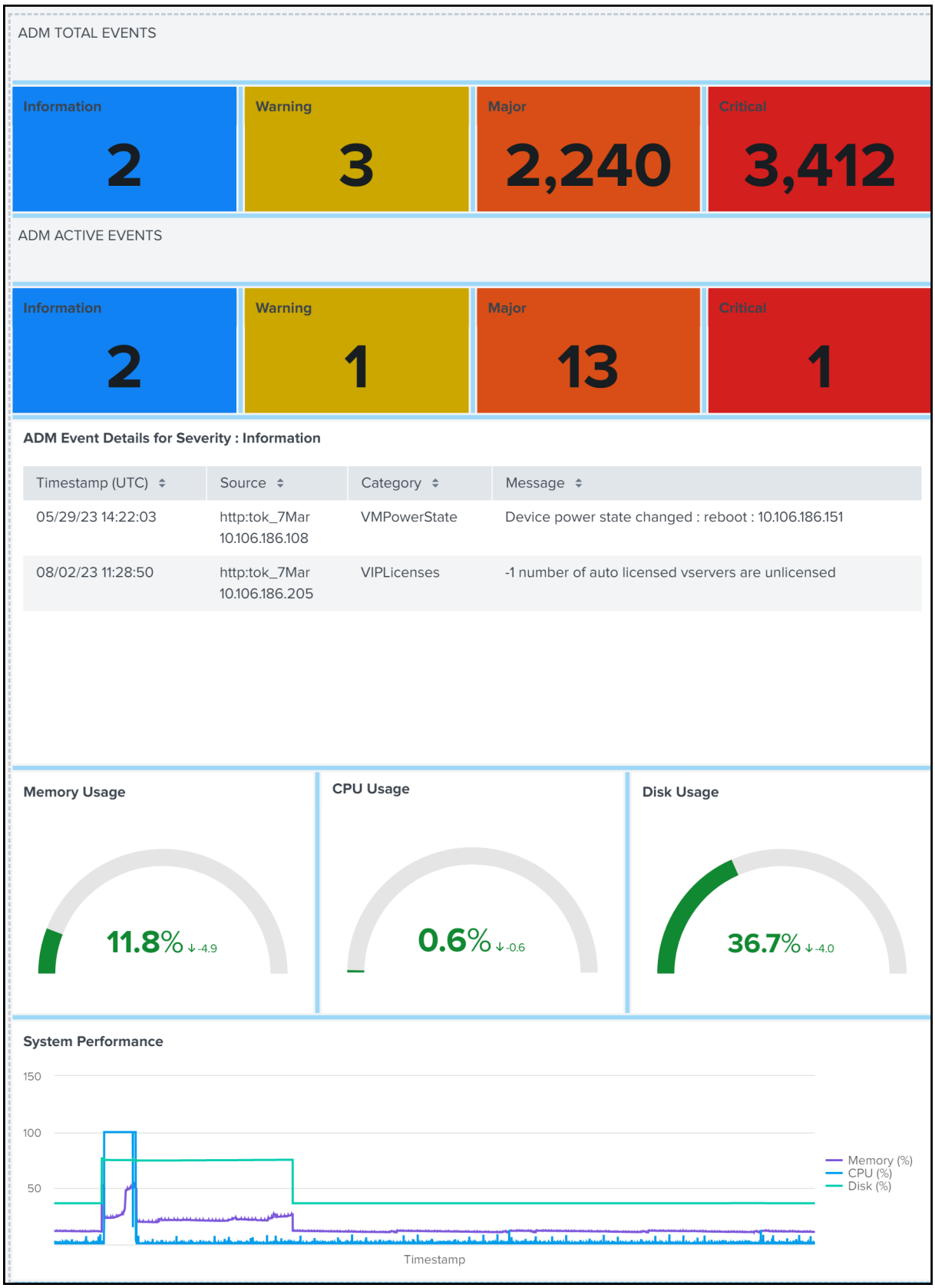


Le tableau de bord suivant est un exemple du tableau de bord actualisé d'informations sur les certificats SSL.



Le tableau de bord suivant est un exemple de tableau de bord des événements et des statistiques mis à jour.

> **Remarque :**
>
> Les données d'utilisation de la mémoire, du processeur et du disque indiquent la valeur actuelle de NetScaler ADM. La tendance à la hausse et à la baisse de ces valeurs est indiquée sur la base de la comparaison de la valeur précédente toutes les 5 minutes.



Outre le tableau de bord, vous pouvez également consulter les données dans Splunk après avoir créé l'abonnement.

1. Dans Splunk, cliquez sur **Search & Reporting**.
2. Dans la barre de recherche :
    - Tapez `sourcetype="metrics"` et sélectionnez la durée dans la liste pour afficher les données des métriques ADM.
    - Tapez `sourcetype="event"` et sélectionnez la durée dans la liste pour afficher les données des événements ADM.
    - Tapez `sourcetype="bot"` ou `sourcetype="waf"` et sélectionnez la durée dans la liste pour afficher les données BOT/WAF.
    - Tapez `sourcetype="ssl"` et sélectionnez la durée dans la liste pour afficher les données relatives aux certificats SSL.

Intégration avec New Relic

February 1, 2024

Vous pouvez désormais intégrer NetScaler ADM à New Relic pour consulter les analyses relatives aux violations du WAF et des bots dans votre tableau de bord New Relic. Grâce à cette intégration, vous pouvez :

- Combinez toutes les autres sources de données externes dans votre tableau de bord New Relic.
- Bénéficiez d'une visibilité des analyses dans un endroit centralisé.

NetScaler ADM collecte les événements Bot et WAF et les envoie à New Relic en temps réel ou périodiquement selon votre choix. En tant qu'administrateur, vous pouvez également consulter les événements Bot et WAF dans votre tableau de bord New Relic.

Conditions préalables

Pour une intégration réussie, vous devez :

- Obtenez un point de terminaison d'événement New Relic au format suivant :

  ```
  https://insights-collector.newrelic.com/v1/accounts/<account_id>/events
  ```


Pour plus d'informations sur la configuration d'un point de terminaison d'événement, consultez la documentation New Relic.

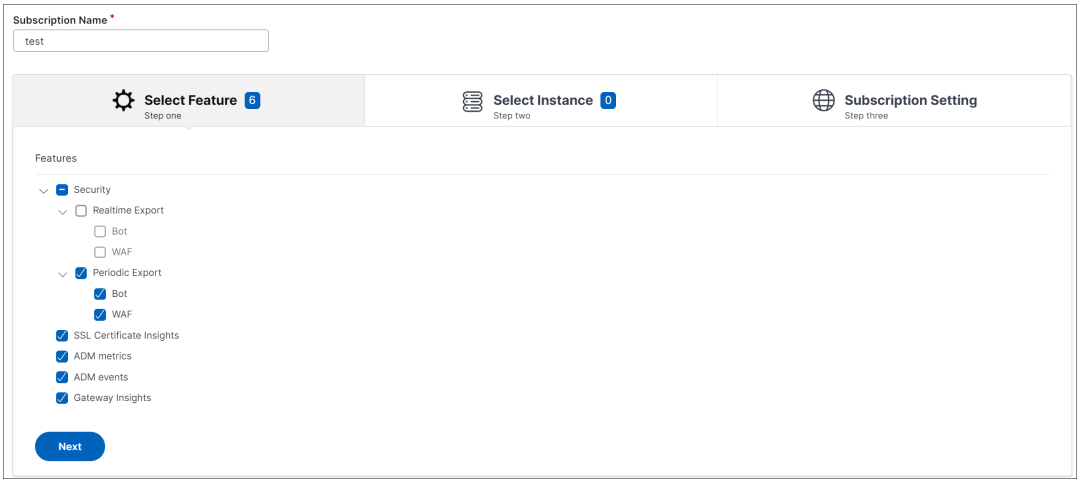
Pour plus d'informations sur l'obtention d'un identifiant de compte, consultez la documentation New Relic.

- Obtenez une clé New Relic. Pour plus d'informations, consultez la documentation de New Relic.
- Ajoutez les détails clés dans NetScaler ADM

Ajoutez les détails clés dans NetScaler ADM

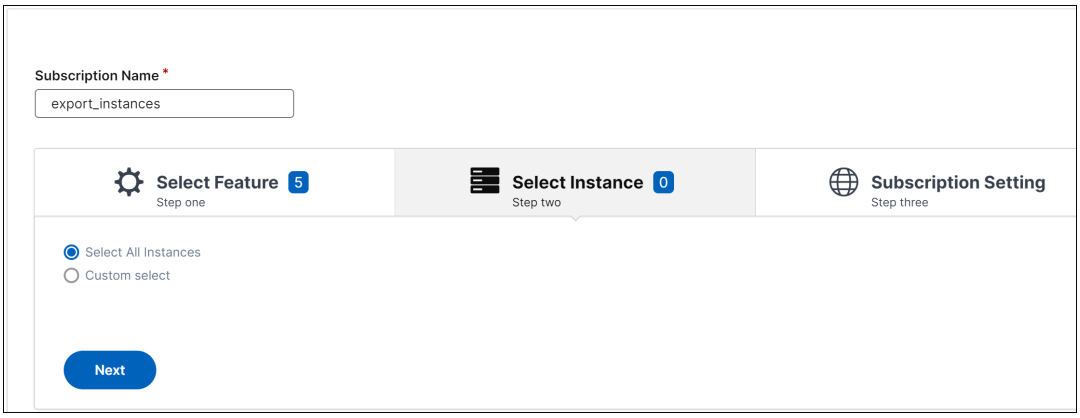
Après avoir généré un jeton, vous devez ajouter des détails dans NetScaler ADM pour l'intégrer à New Relic.

1. Connectez-vous à NetScaler ADM.
2. Accédez à **Paramètres > Intégration de l'écosystème**.
3. Sur la page **Abonnements**, cliquez sur **Ajouter**.
4. Dans l'onglet **Sélectionner une fonctionnalité**, sélectionnez les fonctionnalités que vous souhaitez exporter et cliquez sur **Suivant**.
    - **Export en temps réel** : les violations sélectionnées sont immédiatement exportées vers New Relic.
    - **Exportation périodique** : les violations sélectionnées sont exportées vers New Relic en fonction de la durée sélectionnée.



5. Dans l'onglet **Sélectionner une instance**, vous pouvez choisir **Sélectionner toutes les instances** ou **Sélection personnalisée**, puis cliquer sur **Suivant**.
    - **Sélectionnez toutes les instances** : exporte les données vers New Relic depuis toutes les instances NetScaler.

- **Sélection personnalisée** : vous permet de sélectionner les instances NetScaler dans la liste. Si vous sélectionnez des instances spécifiques dans la liste, les données sont exportées vers New Relic uniquement à partir des instances NetScaler sélectionnées.



6. Dans l'onglet **Paramètres d'abonnement** :

   a) **Type de point final** : sélectionnez **New Relic**.

   b) **URL du point de terminaison** : spécifiez les détails du point de terminaison New Relic. Le point final doit être au format `https://insights-collector.newrelic.com/v1/accounts/<account_id>/events`.

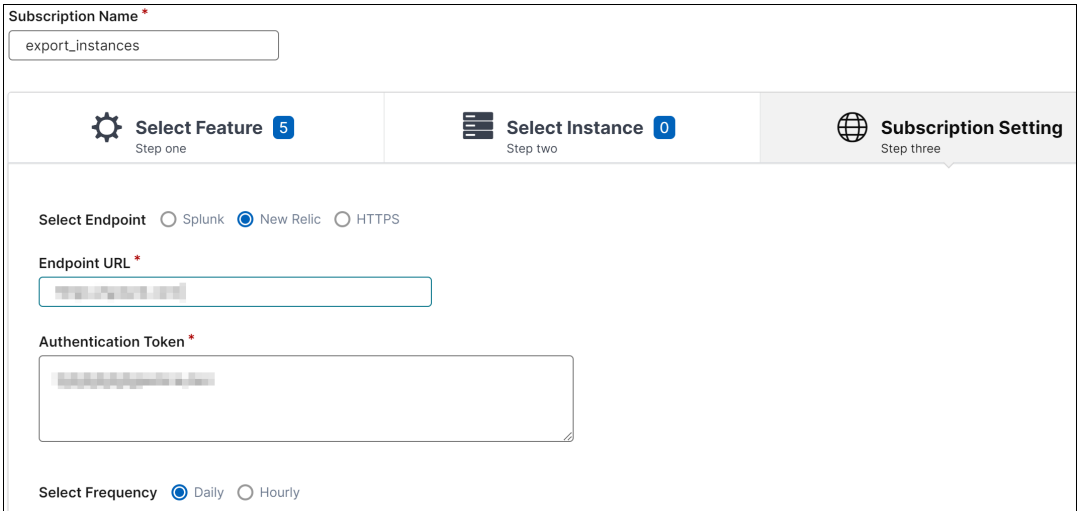
   > **Remarque**
   >
   > Il est recommandé d'utiliser le protocole HTTPS pour des raisons de sécurité.

   c) **Jeton d'authentification** : copiez et collez le jeton d'authentification depuis la page New Relic.

   d) **Sélectionnez la fréquence** : sélectionnez **Quotidien** ou **Horaire** dans la liste. En fonction de la sélection, NetScaler ADM exporte les détails vers New Relic.

   > **Remarque**
   >
   > Applicable uniquement si vous avez sélectionné des violations dans **l'exportation périodique**.

   e) Cliquez sur **Envoyer**.



Remarque

- Lorsque vous configurez avec **l'option d'exportation périodique** pour la première fois, les données des fonctionnalités sélectionnées sont immédiatement transmises à New Relic. La fréquence d'exportation suivante se produit en fonction de votre sélection (quotidienne ou horaire).
- Lorsque vous configurez pour la première **fois avec l'option d'exportation en temps réel**, les données des fonctionnalités sélectionnées sont transmises à New Relic immédiatement dès que les violations sont détectées dans NetScaler ADM.

La configuration est terminée. Vous pouvez consulter les détails sur la page **Abonnements** .

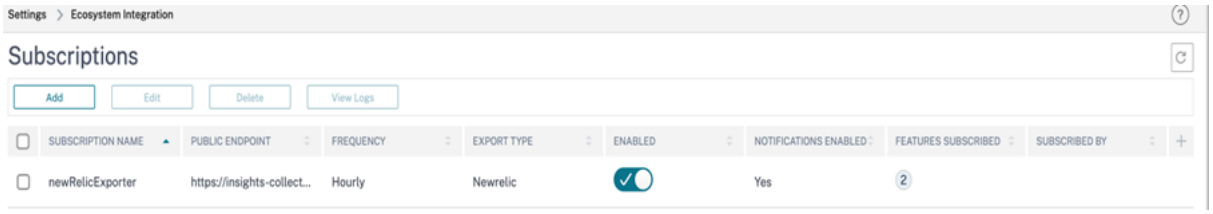
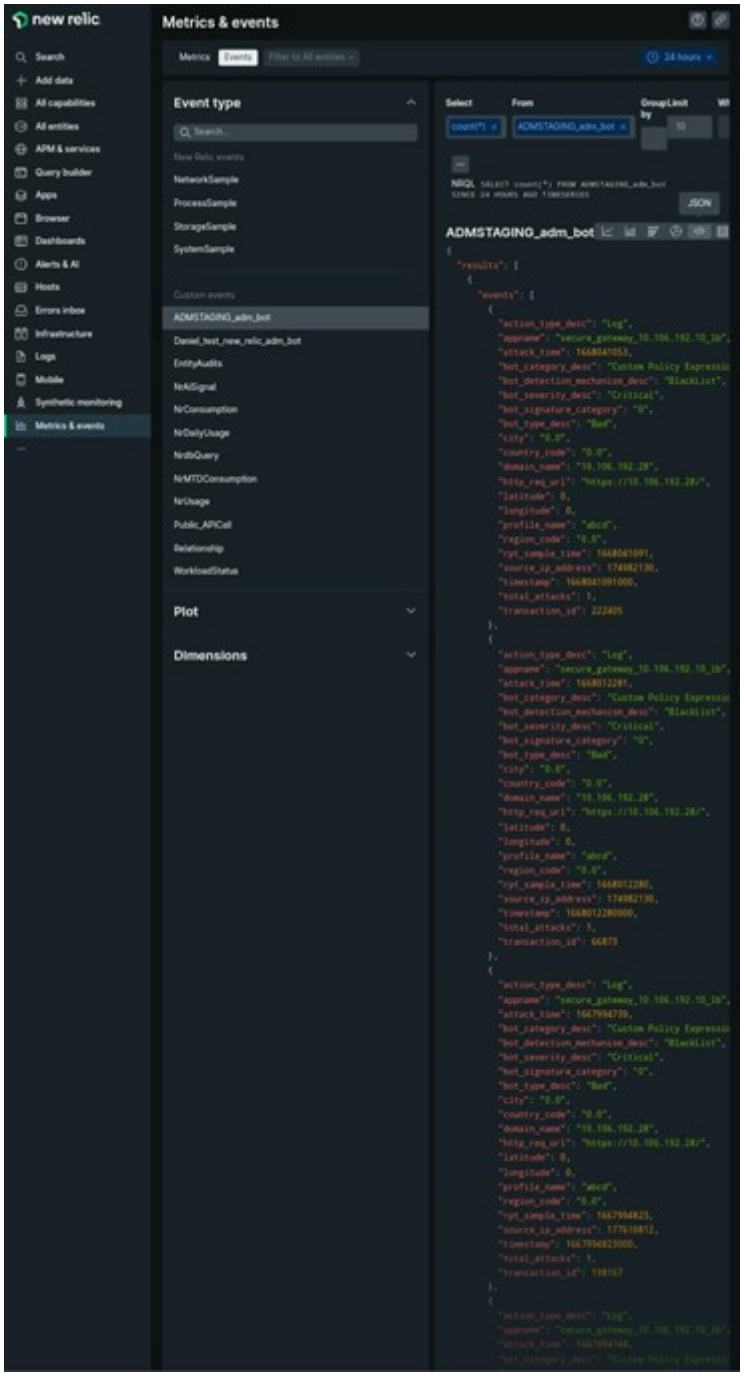


Tableau de bord New Relic

Lorsque les événements sont exportés dans New Relic, vous pouvez consulter les détails de l'événement sous **Métriques et événements** au format JSON suivant :

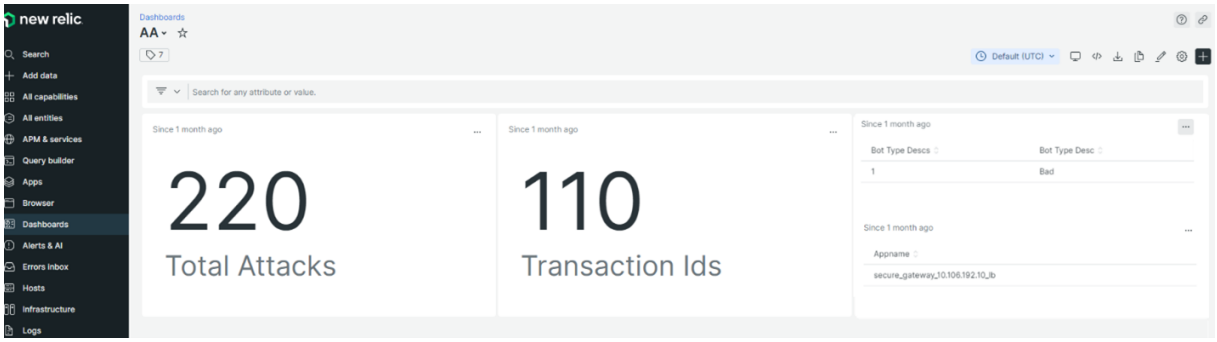
`<subsription_name>_adm_<event name>` où le nom de l'événement peut être Bot, WAF, etc.

Dans l'exemple suivant, ADMSTAGING est `<subscription_name>` et bot est `<event_name>`.



Une fois que vous avez intégré les données JSON dans votre tableau de bord New Relic, en tant qu'administrateur, vous pouvez utiliser le NRQL (New Relic Query Language) et créer un tableau de bord personnalisé avec des facettes et des widgets en fonction de votre choix en créant des requêtes autour des données ingérées. Pour plus d'informations, consultez https://docs.newrelic.com/docs/query-your-data/nrql-new-relic-query-language/get-started/introduction-nrql-new-relics-query-language/

Voici un exemple de tableau de bord créé à l'aide du NRQL :



Pour créer ce tableau de bord, les requêtes suivantes sont requises :

- Widget 1 : Tableau du nombre total d'attaques uniques dans le tableau des événements

  ```
  SELECT count(total_attacks)from <event_name> since 30 days ago
  ```

- Widget 2 : ID de transaction uniques dans le tableau des événements

  ```
  SELECT uniqueCount(transaction_id)from <event_name> since 30 days
   ago
  ```

- Widget 3 : Nombre total de types de robots uniques et leur nombre

  ```
  SELECT uniqueCount(bot_type_desc), uniques(bot_type_desc)from <
  event_name> since 30 days ago
  ```

- Widget 4 : Nombre total de noms d'applications uniques signalant des violations par des robots

  ```
  SELECT uniques(appname)from <event_name> since 30 days ago
  ```

Gateway Insight

February 1, 2024

Dans un déploiement NetScalerGateway, la visibilité des détails d'accès d'un utilisateur est essentielle pour résoudre les problèmes de défaillance d'accès. En tant qu'administrateur réseau, vous souhaitez savoir quand un utilisateur n'est pas en mesure de se connecter à NetScaler Gateway, 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 fournit une visibilité sur les défaillances rencontrées par tous les utilisateurs, quel que soit le mode d'accès, au moment de la connexion à NetScaler 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 utilisée par toutes les passerelles associées à une appliance NetScaler 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 NetScaler ADM, ce qui vous permet de 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 NetScaler ADM doivent être identiques ou ultérieures à celles de l'appliance NetScaler Gateway.
- Une heure de rapports Gateway Insight peut être consultée pour les instances NetScaler dotées d'une licence Advanced. Une licence Premium est un must afficher les rapports Gateway Insight au-delà d'une heure.

Limitations

- NetScaler Gateway ne prend pas en charge Gateway Insight lorsque la méthode d'authentification est configurée en tant qu'authentification basée sur des certificats.
- Pour les rapports Gateway Insight, les informations de géolocalisation ne sont pas fournies par l'appliance NetScaler.

- 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 de l'appliance NetScaler 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
  - Connexion OAuth-OpenID

    Pour l'authentification OAuth-OpenID Connect, NetScaler peut agir en tant que partie dépendante (RP) d'OAuth-OpenID Connect ou en tant que fournisseur d'identité de connexion (IdP) OAuth-OpenID. Lorsque l'authentification réussit, le nom d'utilisateur est indiqué sous l'onglet Utilisateurs du rapport Gateway Insight. Toutefois, vous ne pouvez pas déterminer si la session a été créée au niveau de l'IdP ou du RP.

    Remarque : L'authentification OAuth-OpenID Connect est prise en charge à partir de NetScaler ADM version 13.1 build 4.xx et versions ultérieures.

Activer Gateway Insight

Pour activer Gateway Insight pour votre appliance NetScaler Gateway, vous devez d'abord ajouter l'appliance NetScaler Gateway à NetScaler ADM. Vous devez ensuite activer AppFlow pour le serveur virtuel représentant l'application VPN. Pour plus d'informations sur l'ajout d'appareils à NetScaler ADM, consultez la section Ajouter des appareils.

> **Remarque**
>
> Pour visualiser les défaillances de l'analyse des points de terminaison (EPA) dans NetScaler ADM,

> vous devez activer l'authentification AppFlow, l'autorisation et l'audit de la journalisation des noms d'utilisateur sur l'appliance NetScaler Gateway.

La procédure suivante pour activer Gateway Insight s'applique si votre NetScaler ADM est la version **13.0**build 36.27 :

1. Accédez à **Infrastructure > Instances**, puis sélectionnez l'instance pour laquelle vous souhaitez activer AppFlow.
2. Dans la liste **Sélectionner une action**, sélectionnez **Configurer Analytics**.
3. Sur la page **Configure Insight**, sous **Configurer Analytics**, sélectionnez **NetScaler 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 NetScaler ADM version 13.0Build 41.x ou ultérieure

1. Accédez à **Infrastructure > 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 **NetScaler Gateway**
5. Cliquez sur **OK**.

Activez l'authentification AppFlow, l'autorisation et l'audit de la journalisation des noms d'utilisateur sur une appliance NetScaler 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.**

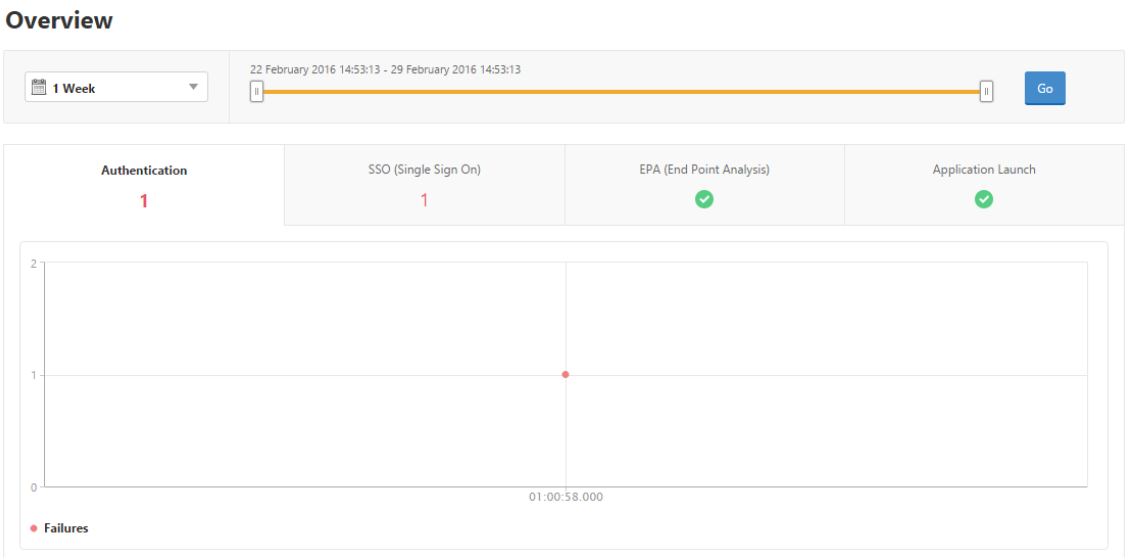
Affichage des rapports Gateway Insight

Dans NetScaler ADM, vous pouvez consulter les rapports de tous les utilisateurs, applications et passerelles associés aux appliances NetScaler Gateway, et vous pouvez consulter 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. NetScaler 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.

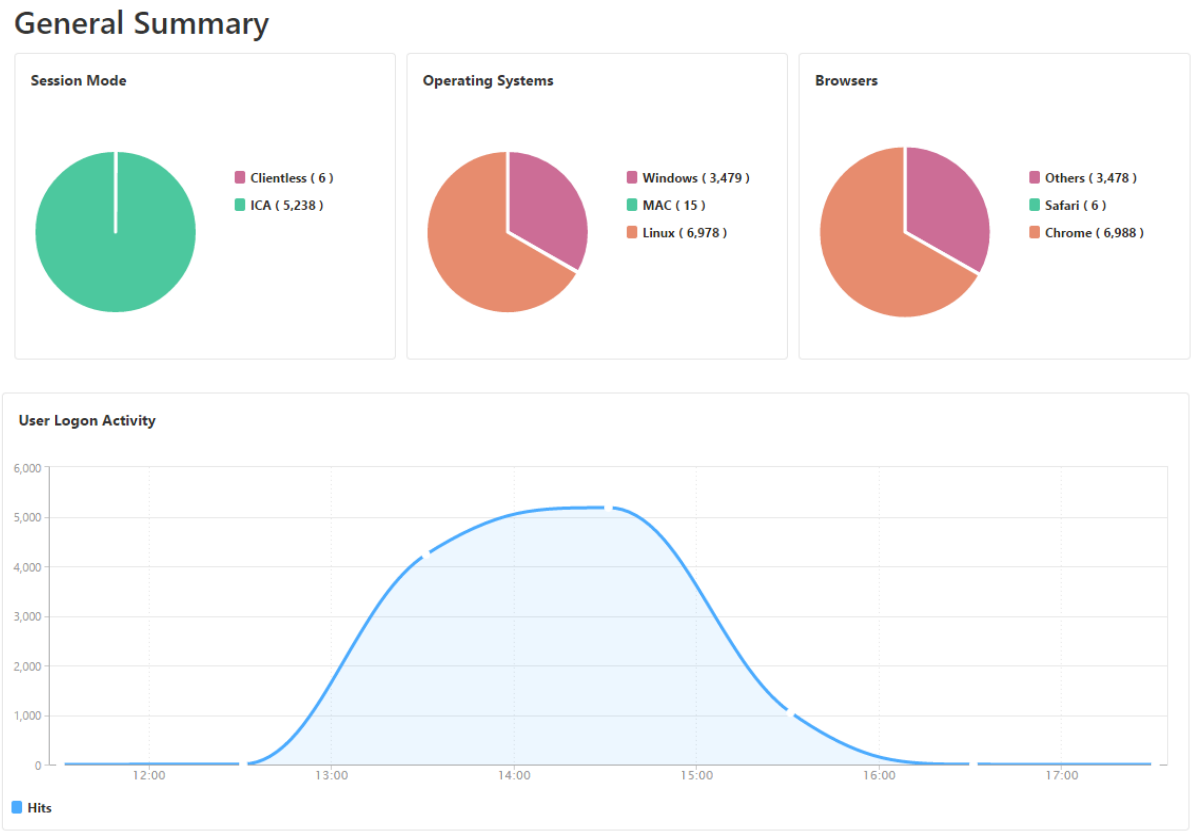
Pour afficher les échecs d'EPA, d'authentification unique, d'authentification, d'autorisation et de lancement d'application

1. Dans NetScaler ADM, accédez à **Gateway > 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 NetScaler ADM, accédez à **Gateway > Gateway Insight**, puis faites défiler la page vers le bas pour afficher les rapports.



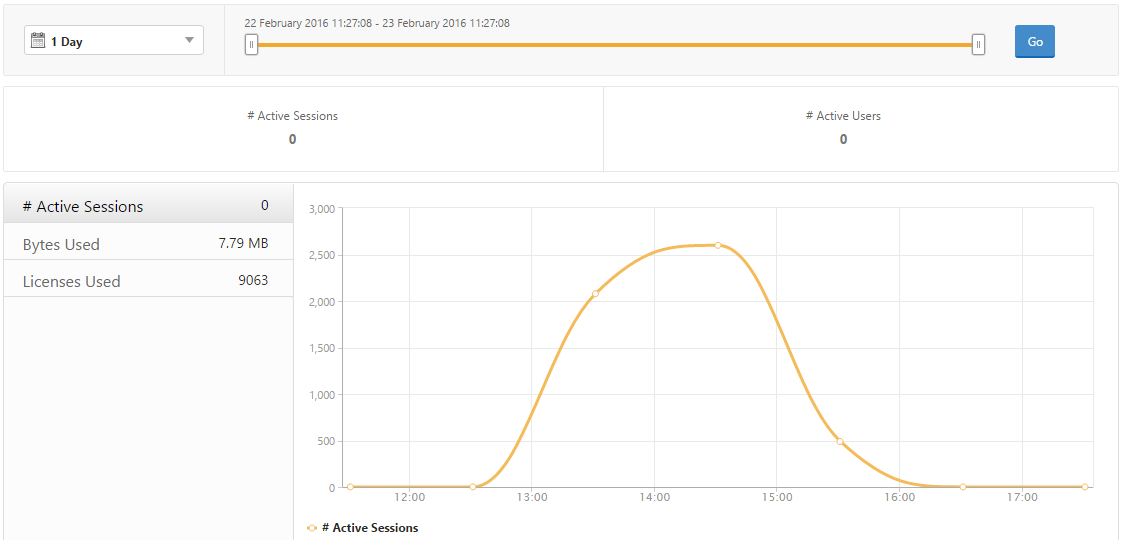
Affichage des rapports Gateway Insight pour les utilisateurs

Vous pouvez consulter les rapports relatifs aux éléments suivants :

- Tous les utilisateurs associés aux appliances NetScaler 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 NetScaler ADM, accédez à **Gateway > Gateway Insight > Users**.
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.

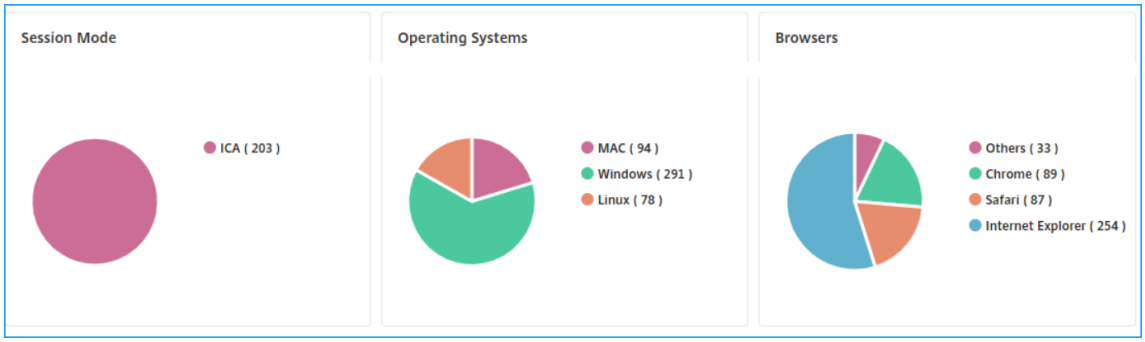


Faites défiler vers le bas pour afficher la liste des utilisateurs disponibles et des utilisateurs actifs.

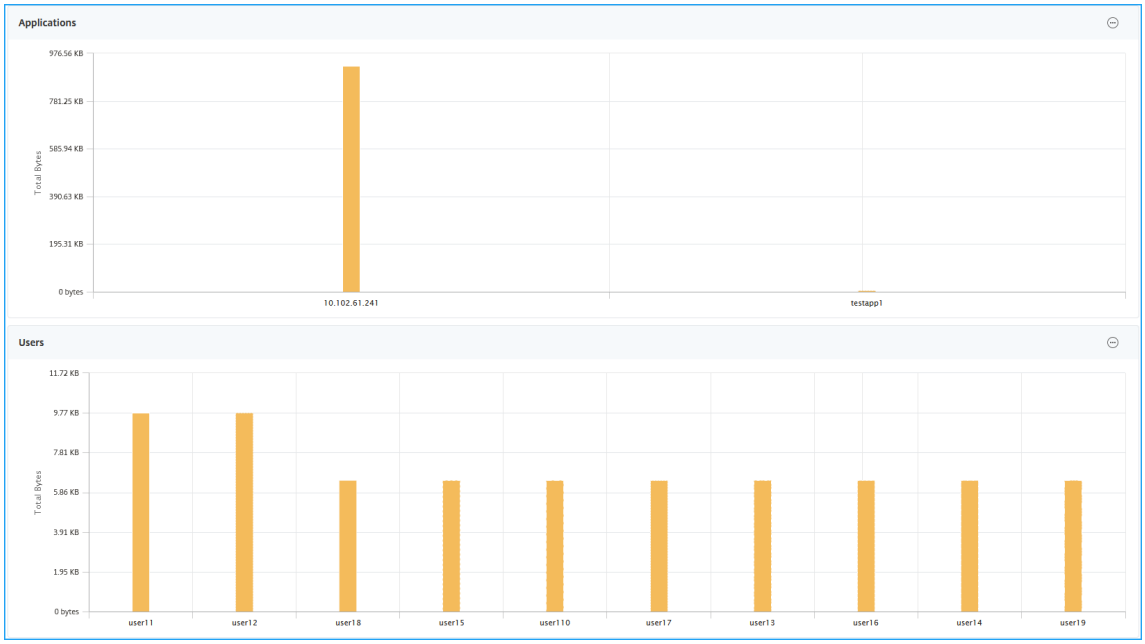
User Name	Total Bytes	# Sessions Used
user1	191.94 KB	11
user10	0	4
user100	2.81 KB	4
user1000	42.66 KB	5
user1001	2.11 KB	4
user1002	4.22 KB	4
user1003	4.22 KB	4

Sous l'onglet **Utilisateurs** ou **Utilisateurs actifs**, cliquez sur un utilisateur pour afficher les détails de l'utilisateur suivants :

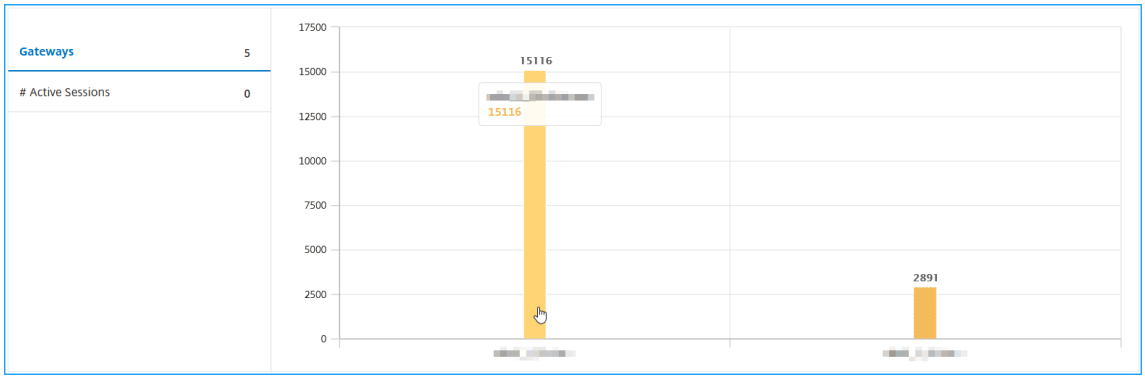
- **Détails de l'utilisateur** - Vous pouvez afficher des informations pour chaque utilisateur associé aux appliances de passerelle ADC. Accédez à **Gateway > GatewayInsight**>**Utilisateurs** et cliquez sur un utilisateur pour afficher les informations relatives à l'utilisateur sélectionné, telles que le mode session, le système d'exploitation et les navigateurs.



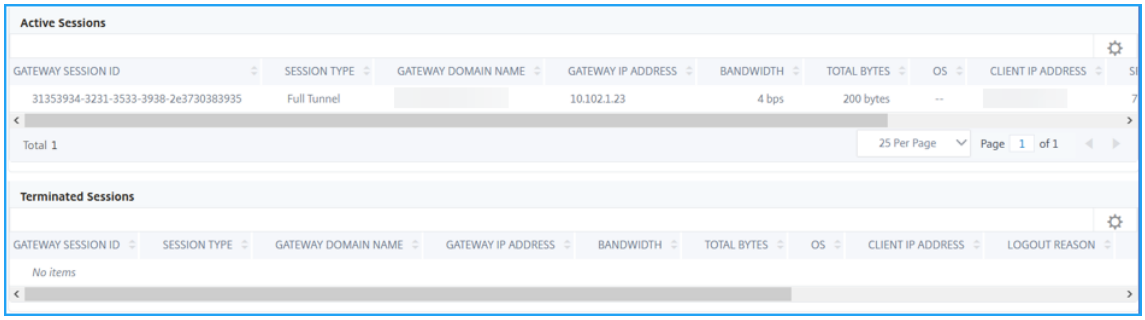
- **Utilisateurs et applications pour la passerelle sélectionnée** : accédez à **Passerelle** > **Gateway Insight** > **Gateway** et cliquez sur un nom de domaine de passerelle pour afficher les 10 applications et les 10 principaux utilisateurs associés à la passerelle sélectionnée.



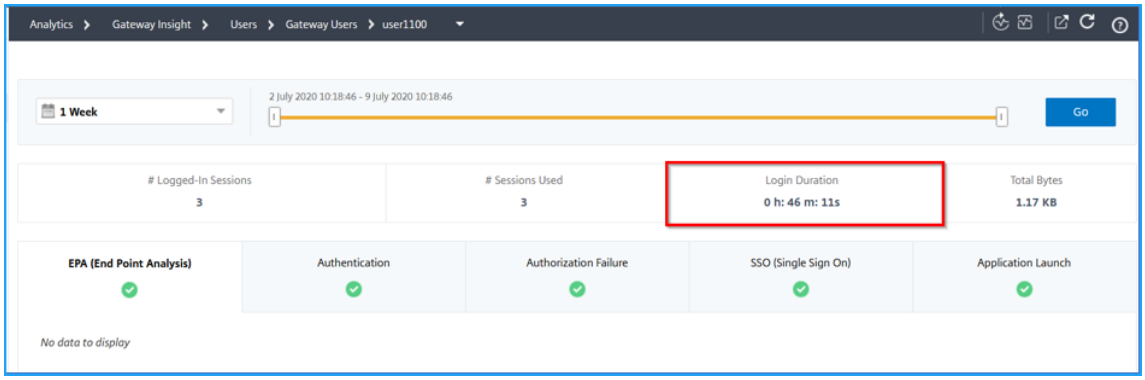
- **Afficher plus d'option pour les applications et les utilisateurs** : pour plus de 10 applications et utilisateurs, vous pouvez cliquer sur l'icône Plus dans Applications et utilisateurs pour afficher tous les détails des utilisateurs et applications associés à la passerelle sélectionnée.
- **Afficher 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 **Passerelle > Gateway Insight > Gateway** et cliquez sur le graphique à barres de la 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

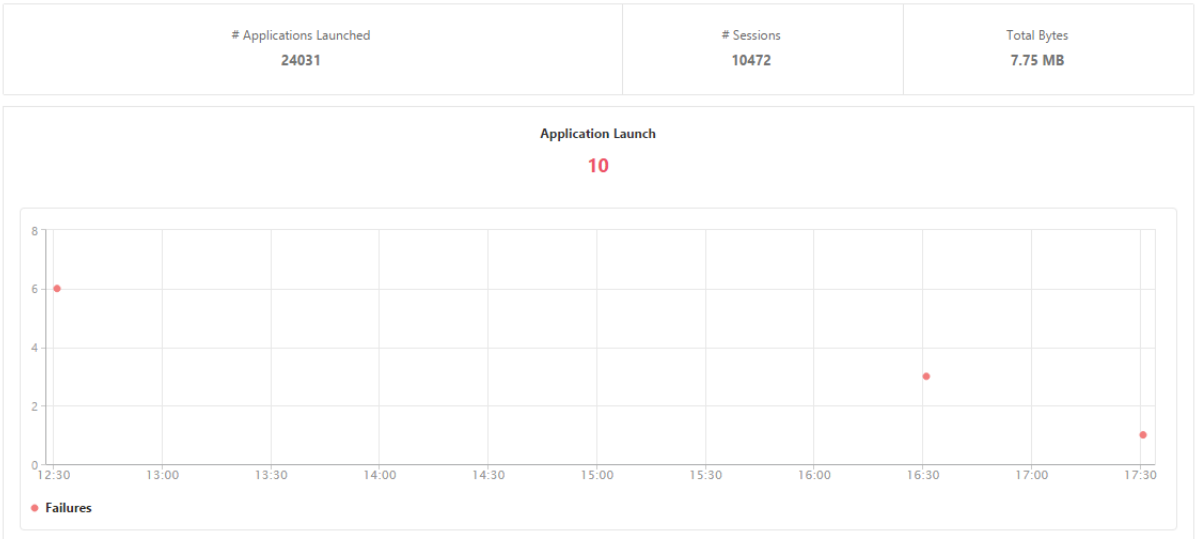
Vous pouvez afficher le nombre d'applications lancées, le nombre de sessions totales et actives, le nombre total d'octets et la bande passante consommés par les applications. Vous pouvez afficher les détails des utilisateurs, des sessions, de la bande passante et des erreurs de lancement d'une application.

Pour afficher les détails de l'application

1. Dans NetScaler ADM, accédez à **Gateway > 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.

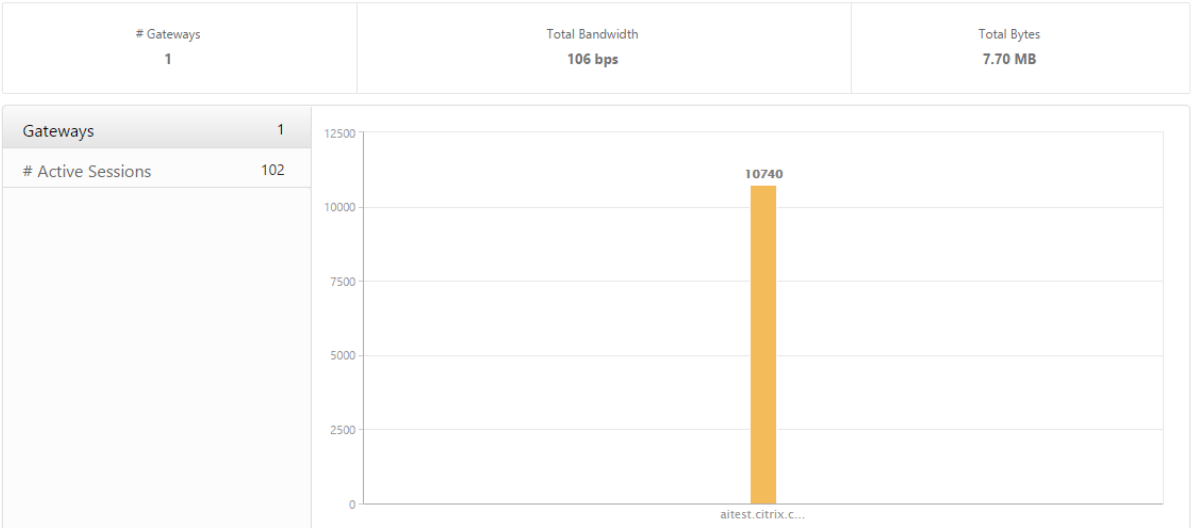
Affichage des rapports Gateway Insight pour les passerelles

Vous pouvez consulter le nombre de passerelles, le nombre de sessions actives, le nombre total d'octets et la bande passante utilisée par toutes les passerelles associées à une appliance NetScaler 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.

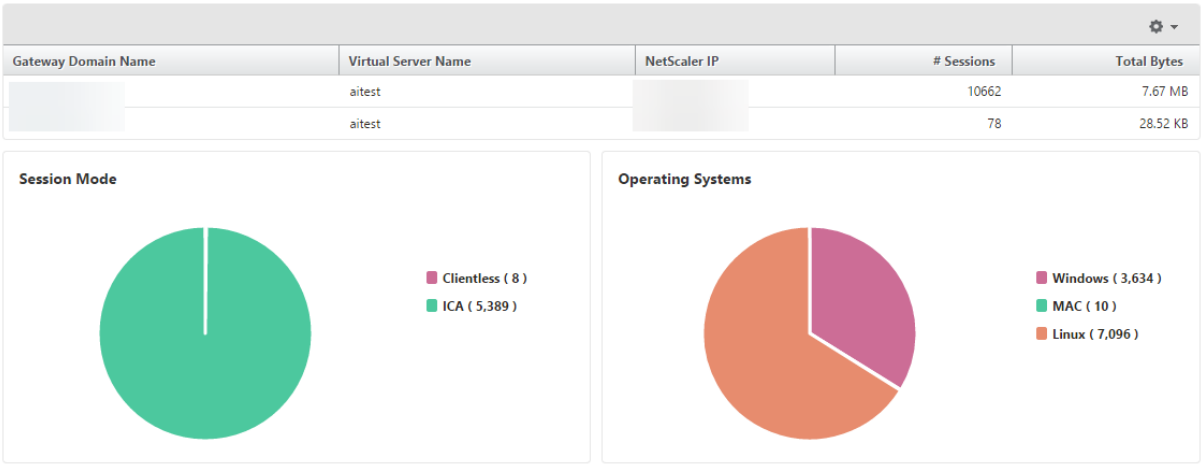
Pour afficher les détails de la Gateway

1. Dans **NetScaler ADM**, accédez à **Gateway > Gateway Insight > Gateways**.
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 consulter le nombre de passerelles, le nombre de sessions actives, le nombre total d'octets et la bande passante utilisée par toutes les passerelles associées à une appliance NetScaler Gateway à tout moment.



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 geomapping ne sont exportés que si NetScaler 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 **Paramètres > 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 vous pouvez utiliser Gateway Insight pour obtenir une visibilité sur les détails d'accès des utilisateurs, les applications et les passerelles sur les appliances NetScaler Gateway.

Un utilisateur ne peut pas se connecter à l'appliance NetScaler Gateway ou aux serveurs Web internes

En tant qu'administrateur de NetScaler Gateway, vous surveillez les appliances NetScaler Gateway via NetScaler 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.

NetScaler ADM vous permet de consulter 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 NetScaler ADM, vous pouvez rechercher un utilisateur en particulier, puis afficher tous les détails le concernant.

Pour rechercher un utilisateur :

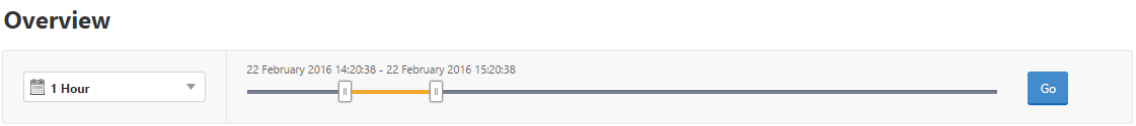
Dans NetScaler ADM, accédez à **Gateway > Gateway Insight** et, dans **la zone de texte Rechercher** des utilisateurs, spécifiez l'utilisateur que vous souhaitez rechercher.

Échec de l'authentification

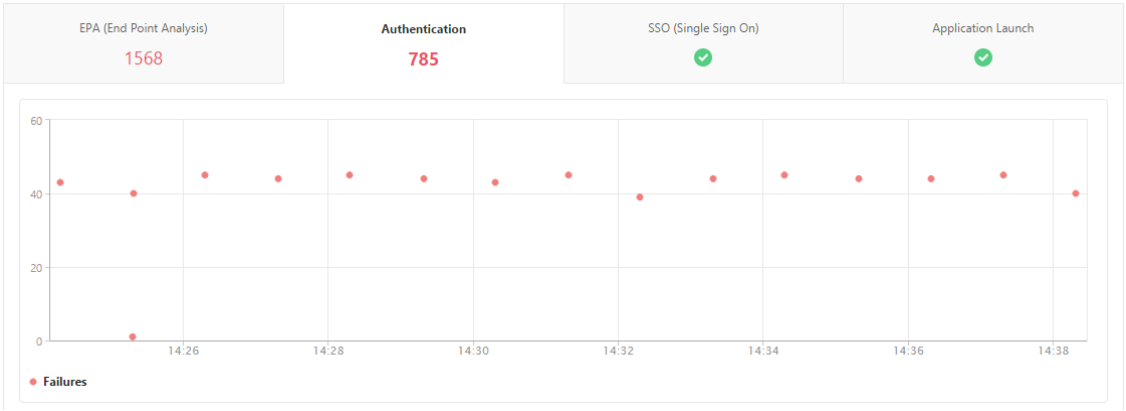
Vous pouvez afficher les erreurs d'authentification telles que les informations d'identification incorrectes ou l'absence de réponse du serveur d'authentification. Vous pouvez également voir le facteur à l'origine de l'échec de l'authentification.

Pour afficher les détails de l'échec d'authentification :

1. Dans NetScaler ADM, accédez à **Gateway > 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.

> **Important :**
>
> Si l'authentification OAuth-OpenID Connect échoue, le nom d'utilisateur est affiché en tant que **NA** dans le rapport Gateway Insight pour certains des échecs, par exemple « échec de vérification du jeton ». Dans cet échec, les noms d'utilisateur ne sont pas disponibles pour l'échec de l'au-

> thentification en raison d'un « échec de vérification du jeton » au niveau de la partie de confiance de connexion OAuth-OpenID.

USERNAME	CITRIX ADC IP ADDRESS	CLIENT IP ADDRESS	GATEWAY IP ADDRESS	VPN	CS VIRTUAL SERVER	ERROR DESCRIPTION
-NA-				gitest.citrix.com		Relying party: Token verification failed
-NA-				gitest.citrix.com		Relying party: Incoming URL query parameter from user agent is NULL in /nf/auth/doOAuth requ
-NA-				gitest.citrix.com		Relying party: Action query parameter isn't present in the URL from user agent in /nf/auth/doOA
-NA-				gitest.citrix.com		Relying party: Action query parameter isn't present in the URL from user agent in /nf/auth/doOA
-NA-				vpnvserver		Relying party: Token verification failed
-NA-				vpnvserver		Relying party: Token verification failed
-NA-				vpnvserver		Relying party: Token verification failed
-NA-				vpnvserver		Relying party: Token decryption failure

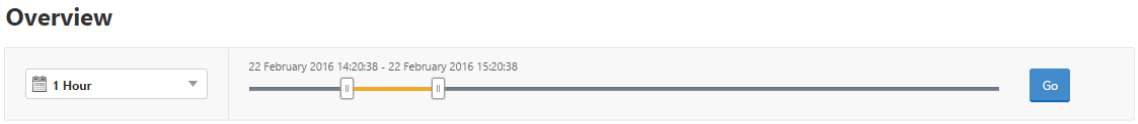
Échec de l'EPA

Vous pouvez afficher les échecs de l'EPA au stade de la pré-authentification ou de la post-authentification.

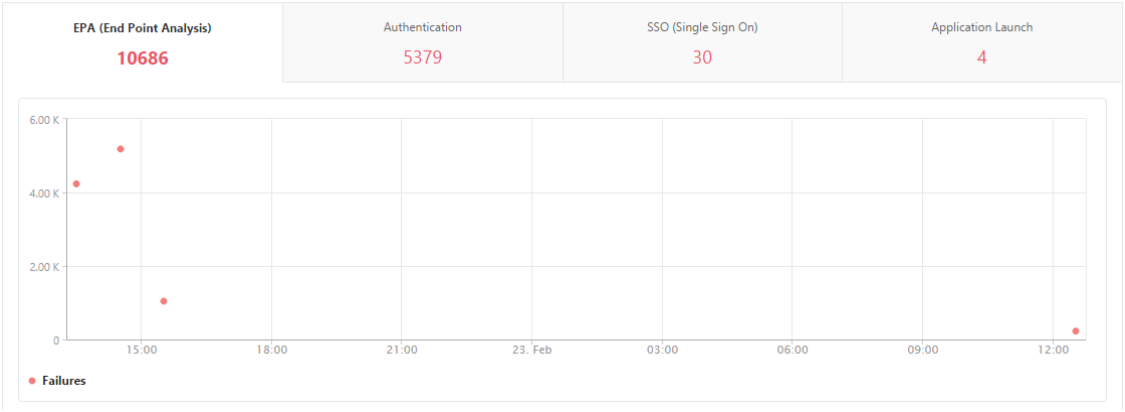
> **Important :**
>
> NetScaler Gateway signale les défaillances EPA à NetScaler ADM pour les expressions classiques et avancées. Pour les expressions avancées, les noms des stratégies ne sont pas affichés dans le tableau de bord Gateway Insight. Les échecs sont signalés si l'EPA est configuré comme l'un des facteurs du flux d'authentification nFactor.

Pour afficher les détails des échecs EPA :

1. Dans NetScaler ADM, accédez à **Gateway > 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 indique la raison de la défaillance de l'EPA. Par exemple, le message d'erreur « Echecs de pré-authentification EPA » apparaît lorsqu'un contrôle EPA échoue en raison de défaillances de nFactor EPA.

La colonne **Nom de la stratégie** affiche la stratégie à l'origine de 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. L'identifiant de dossier est affiché sur les entrées auxquelles aucun nom d'utilisateur n'est attribué si l'EPA est utilisé comme facteur dans le flux d'authentification nFactor.

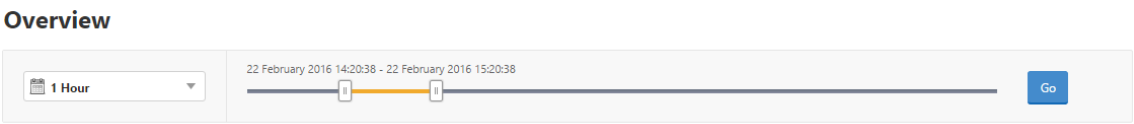
> **Remarque**
>
> NetScaler Gateway ne signale pas les défaillances de l'EPA lorsque l'expression « ClientSecurity » est configurée en tant que règle de stratégie de session VPN.

Défaillances SSO

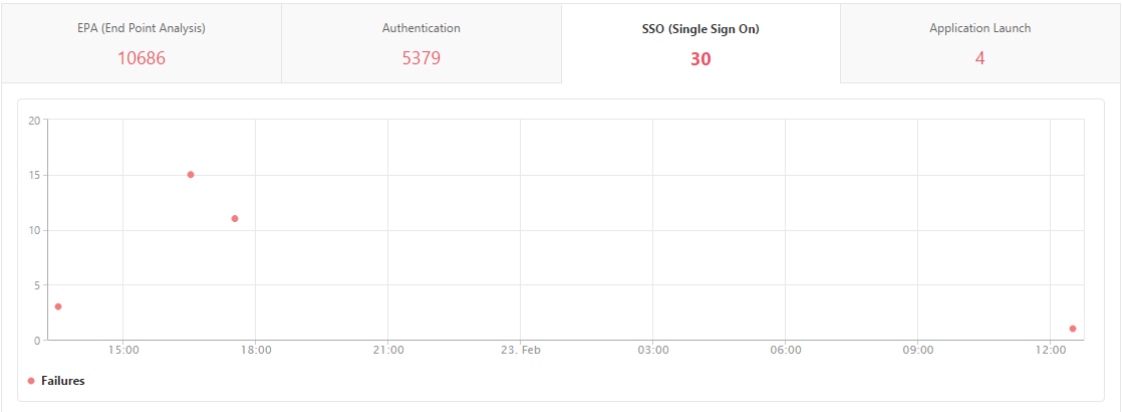
Vous pouvez consulter tous les échecs SSO survenus à tout moment pour un utilisateur accédant à n'importe quelle application via l'appliance NetScaler Gateway.

Pour afficher les détails des défaillances SSO :

1. Dans NetScaler ADM, accédez à **Gateway > 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

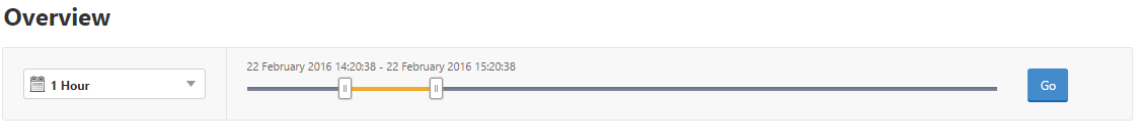
supprimer des colonnes à l'aide de la flèche vers le bas.

Une fois connecté à NetScaler Gateway, un utilisateur ne peut lancer aucune application virtuelle

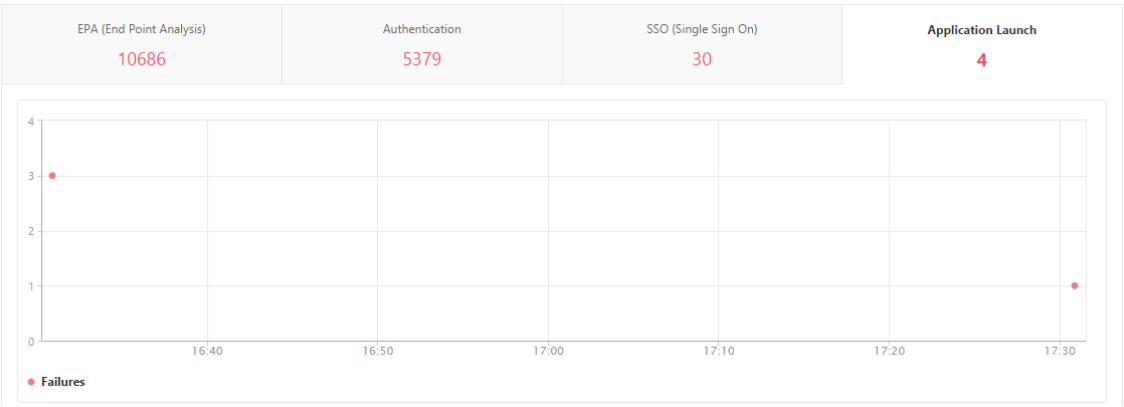
En cas d'échec de lancement de l'application, vous pouvez obtenir une visibilité sur les raisons, telles que le serveur STA (Secure Ticket Authority) inaccessible ou le serveur Citrix Virtual App, ou le ticket STA non valide. Vous pouvez afficher l'heure à laquelle l'erreur s'est produite, les détails 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 NetScaler ADM, accédez à **Gateway > 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 NetScaler ADM, vous pouvez voir le nombre total d'octets et de bande passante consommés par cette application.

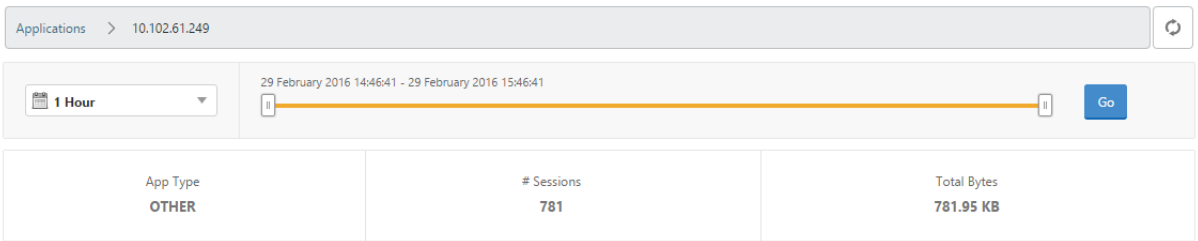
Pour afficher le nombre total d'octets et de bande passante consommés par une application :

Dans NetScaler ADM, accédez à **Gateway > Gateway Insight > Applications**, faites défiler la page vers le bas et, dans l'onglet **Autres applications**, cliquez sur l'application dont vous souhaitez afficher les détails.

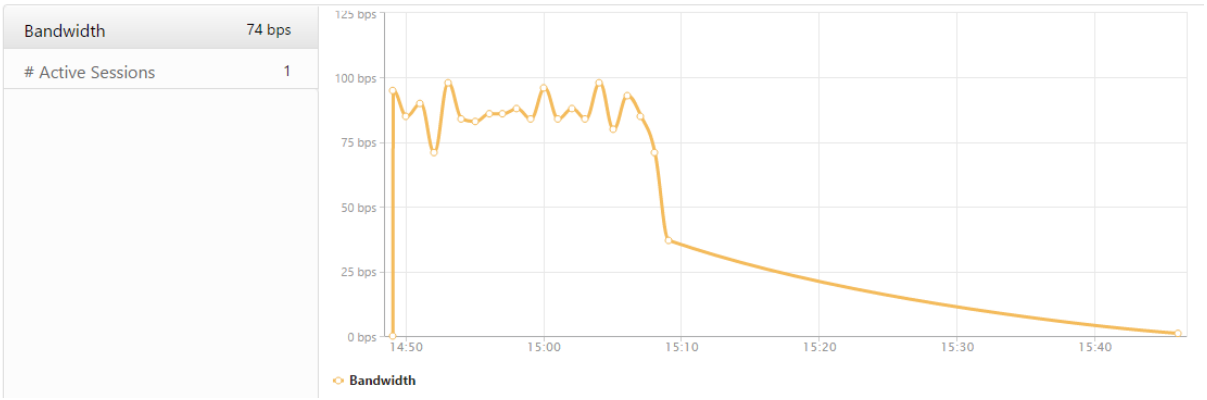
ICA Applications | Other Applications

Name	# Sessions	Bandwidth	Total Bytes
10.102.61.134	1	0 bps	12.19 KB
10.102.61.249	4	0 bps	82.32 KB
alt1-safebrowsing.google.com	1	0 bps	1.04 KB
bcwhwkevnw	1	0 bps	1.98 KB
bcwhwkevnw.citrite.net	1	0 bps	1.01 KB

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.

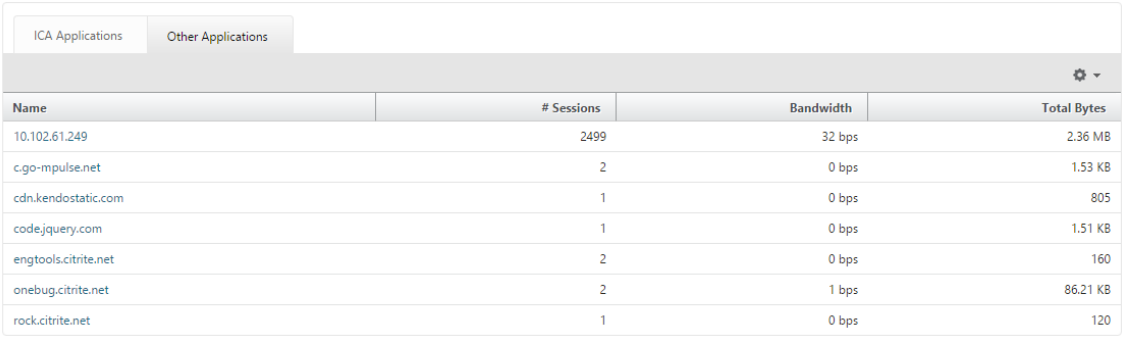


Un utilisateur s'est connecté à NetScaler Gateway avec succès, mais ne peut pas accéder à certaines ressources réseau du réseau interne

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 NetScaler ADM **, accédez à Gateway > 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.

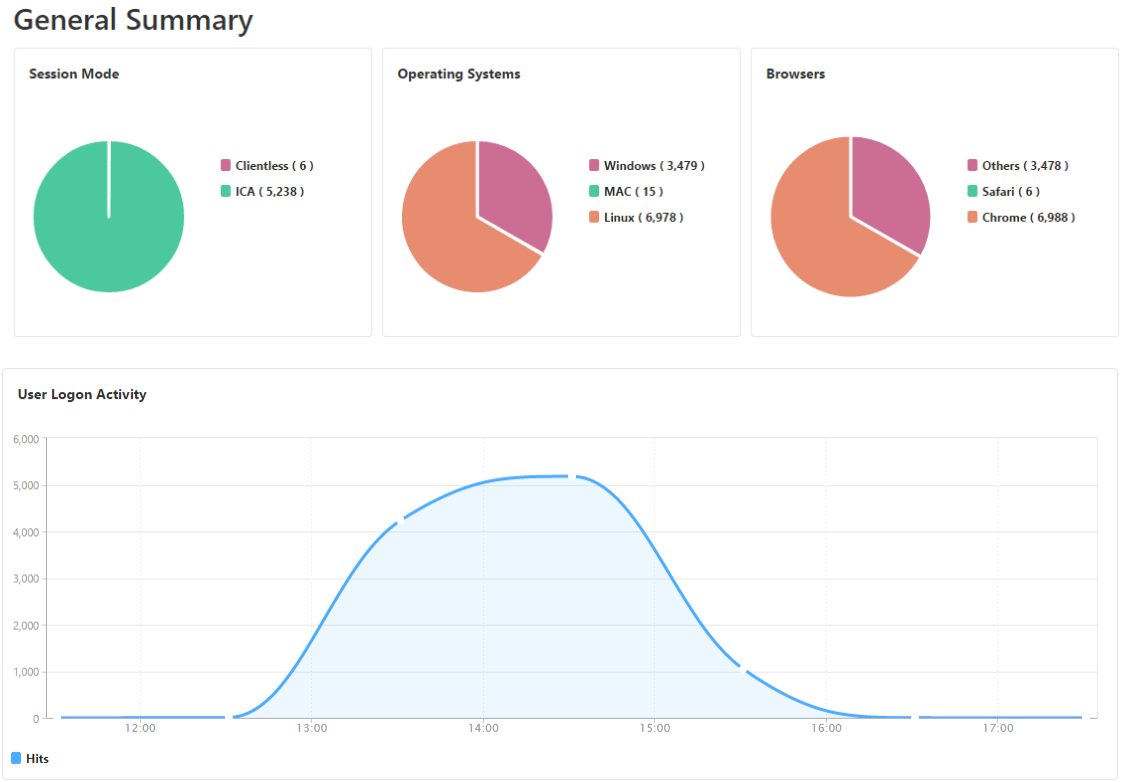
Différents utilisateurs peuvent utiliser différents déploiements de NetScaler Gateway ou se connecter à NetScaler Gateway via différents modes d'accès. L'administrateur doit être en mesure d'afficher les détails sur les types de déploiement et les modes d'accès

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 NetScaler 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 NetScaler ADM, accédez à **Gateway > 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 NetScaler et NetScaler ADM.
- Génération d'enregistrements dans NetScaler.
- Validations dans NetScaler ADM.

Liste de contrôle de la configuration Gateway Insight

- Assurez-vous que la fonctionnalité AppFlow est activée dans l'appliance NetScaler. Pour plus de détails, consultez Activation d'AppFlow.
- Vérifiez la configuration de Gateway Insight dans la configuration en cours d'exécution de NetScaler.

  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 ;

  ```
  1  bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
  2  <!--NeedCopy-->
  ```

  Le type de liaison OTHERTCP_REQUEST est également requis pour Gateway Insight.

  ```
  1  bind vpn vserver afsanity -policy afp -priority 100 -type
        OTHERTCP_REQUEST
  2  <!--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 NetScaler Gateway/VPN. Pour plus de détails, consultez Activation d'AppFlow pour les serveurs virtuels.

Liste de contrôle de la connectivité entre NetScaler et NetScaler ADM

- Vérifiez l'état du collecteur AppFlow dans NetScaler. Pour plus de détails, consultez Comment vérifier l'état de la connectivité entre NetScaler et AppFlowCollector.
- 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 **Paramètres > AppFlow > Stratégies dans l'** interface graphique pour vérifier les résultats de la stratégie AppFlow.

- Validez tout pare-feu bloquant les ports AppFlow 4739 ou 5557.

Liste de contrôle de la génération d'enregistrements dans NetScaler

- Exécutez la commande `nsconmsg -d stats -g ai_tot` et vérifiez les incréments de statistiques dans NetScaler.
- Capturez `nstrace logs` et vérifiez les paquets CFLOW pour confirmer que NetScaler exporte les 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 NetScaler ADM

- Exécutez la commande `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: vpn_"` pour consulter les journaux afin de confirmer que NetScaler ADM reçoit des enregistrements AppFlow.
- Assurez-vous que l'instance NetScaler est ajoutée à NetScaler ADM.
- Assurez-vous que le serveur virtuel NetScaler Gateway/VPN est sous licence NetScaler ADM.

Validation des journaux Logstream dans NetScaler ADM

La validation des données Logstream reçues par NetScaler ADM peut être effectuée à l'aide des méthodes suivantes :

- **Activation de la journalisation des enregistrements de données dans NetScaler 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 NetScaler

À partir de la version 13.0 build 71.x, vous pouvez consulter les journaux NetScaler pour confirmer 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

```
1 <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="
2 <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"
3 <local0.err> … GMT 0-PPE-0 : default SSLVPN Message 148 0 : "GwInsight
    : Func=update_session_appflow_collector pcb or session is NULL"
4 <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 NetScaler et NetScaler ADM.

- Offre groupée de support technique pour NetScaler et NetScaler ADM.
- `nstrace` lors du problème.

Problèmes connus

Reportez-vous aux notes de mise à jour d'ADC pour connaître les problèmes connus sur Gateway Insight.

HDX Insight

February 1, 2024

HDX Insight fournit une visibilité de bout en bout du trafic HDX vers Citrix Virtual Apps and Desktop via NetScaler. 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 de données de visibilité en temps réel et historiques permet à NetScaler Application Delivery Management (ADM) de prendre en charge un large éventail de cas d'utilisation.

Pour que les données apparaissent, vous devez activer AppFlow sur vos serveurs virtuels NetScaler 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. NetScaler ADM Analyt-

> ics 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 **Passerelle > HDX Insight > Applications** et cliquer sur **Durée du lancement**pour afficher le temps nécessaire au lancement de l'application. Vous pouvez également afficher l'agent utilisateur de tous les utilisateurs connectés en accédant à**Passerelle > HDX Insight > Utilisateurs.**

> **Remarque**HDX Insight prend en charge les partitions d'administration configurées dans les instances NetScaler exécutées sur la version logicielle 12.0.

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.

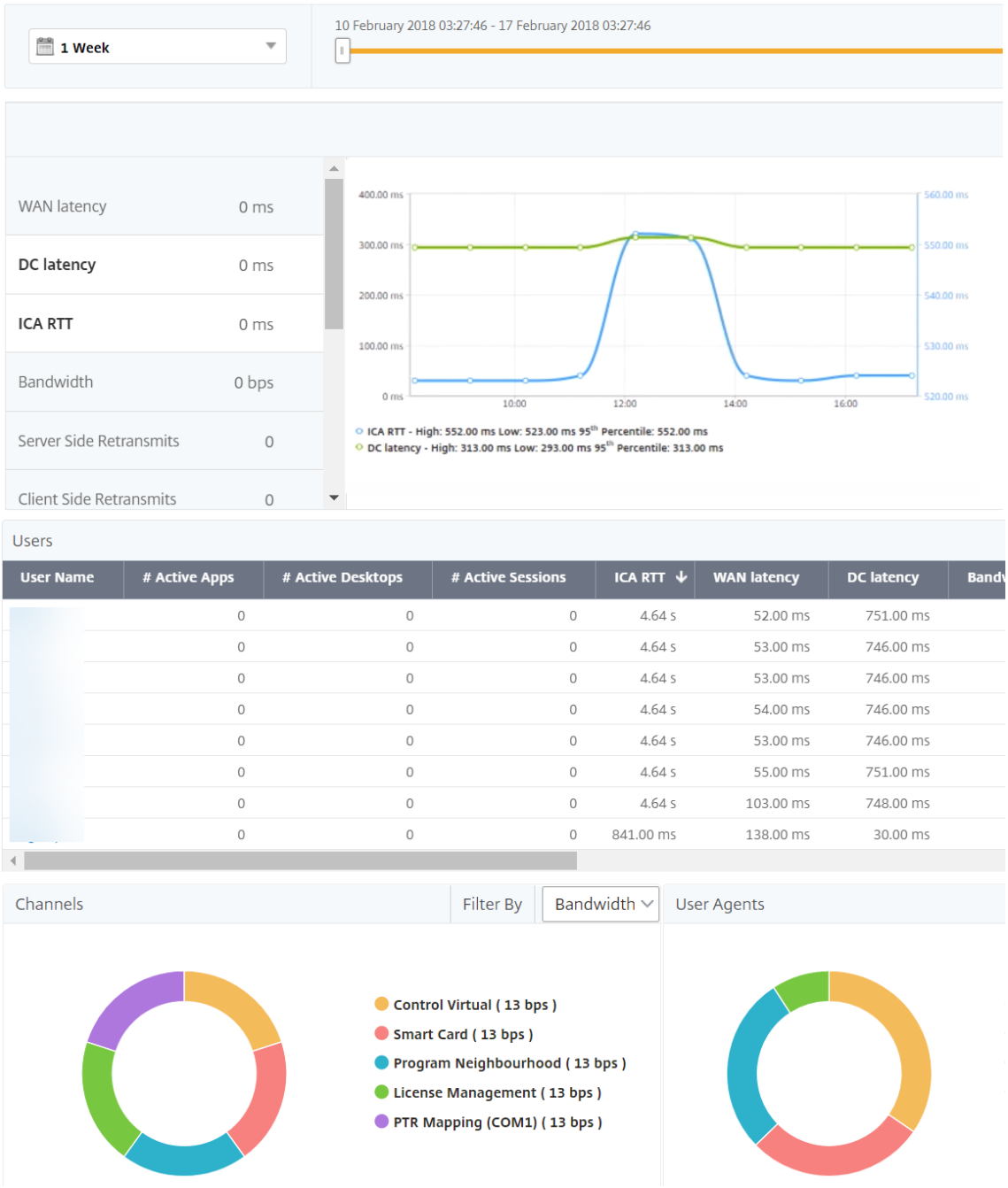
Pour identifier la cause première du problème, analysez les indicateurs suivants :

- Latence WAN
- Latence DC
- Délai d'hôte

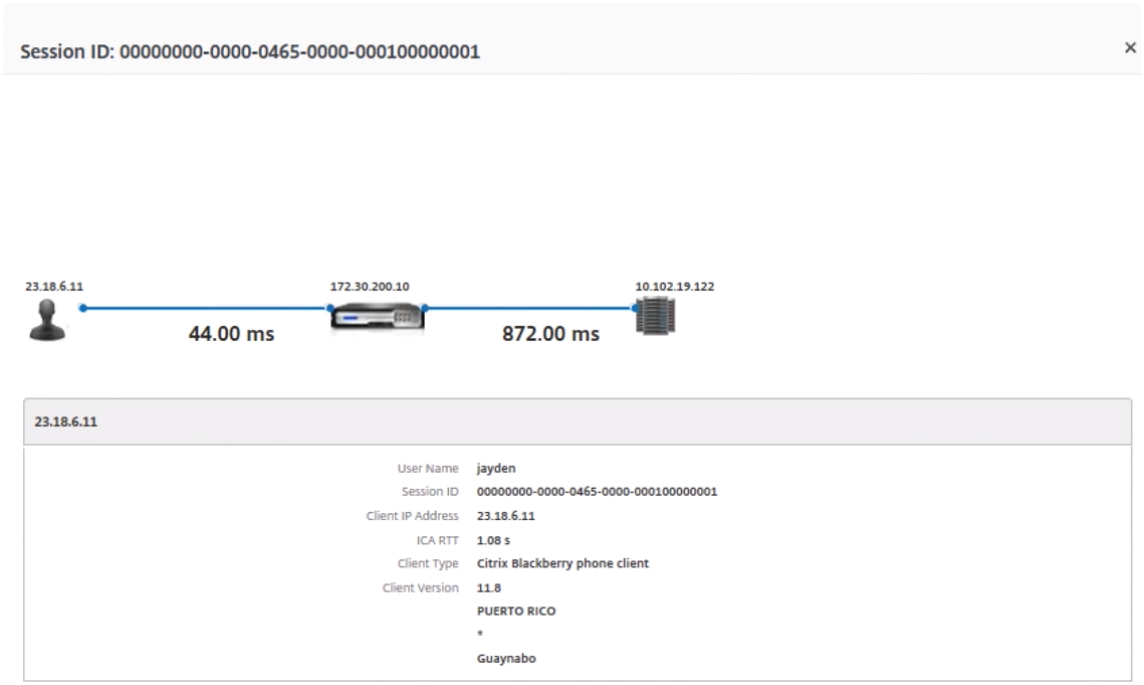
Pour afficher les mesures client :

1. Accédez à **Passerelle > 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.

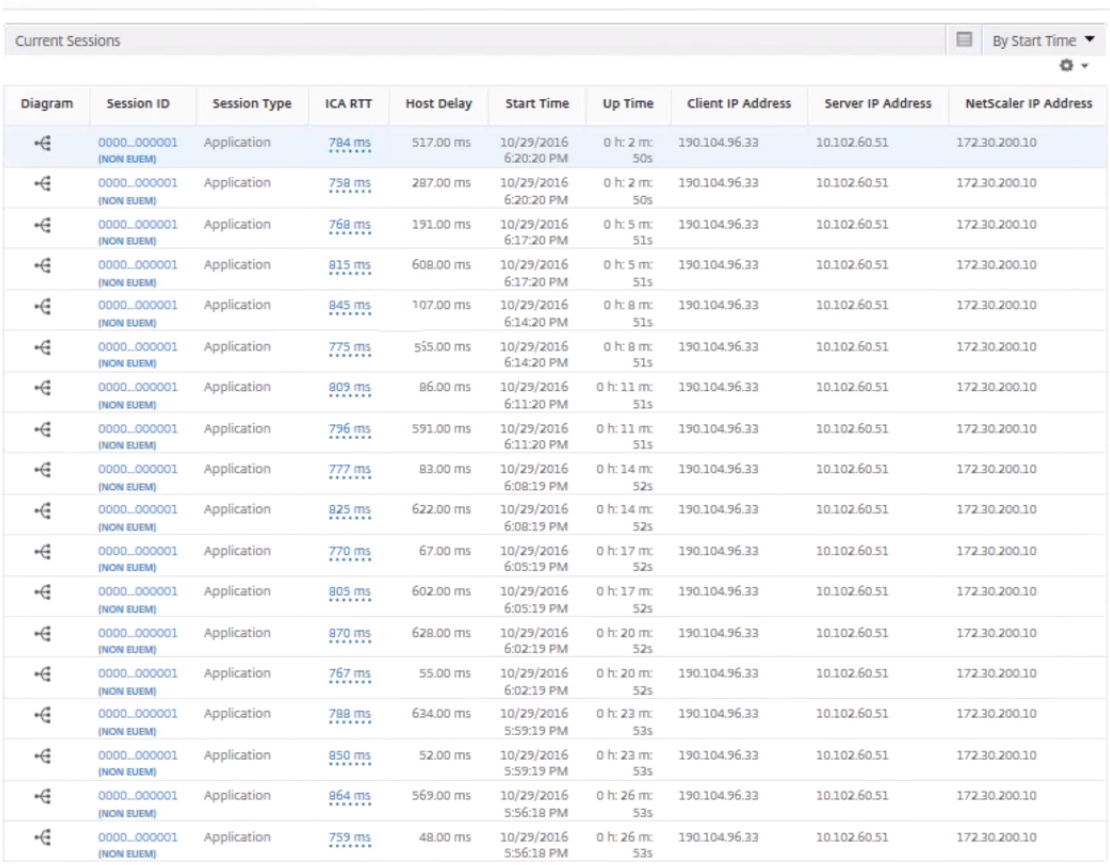
Pour identifier la cause première du problème, analysez les indicateurs suivants :

- Latence WAN
- Latence DC
- Retard de l'hôte

Pour afficher les mesures utilisateur :

1. Accédez à **Gateway > HDX Insight > Utilisateurs**.
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 d'autres indicateurs utilisateur, tels que l'instabilité du WAN et les retransmissions côté serveur si vous utilisez NetScaler ADM exécutant le logiciel 11.1 build 51.21 ou version ultérieure. Pour consulter ces mesures, accédez à **Gateway > 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 de géomaps de NetScaler ADM 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 NetScaler ADM pour afficher les géomaps d'un emplacement géographique ou d'un réseau local particulier en spécifiant la plage d'adresses IP privée (adresses IP de début et de fin) pour l'emplacement.

Vous pouvez également afficher les détails historiques et actifs des utilisateurs à partir des cartes géographiques dans HDX Insight. Accédez à **Passerelle > 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 :

Accédez à **Paramètres > Paramètres analytiques > Blocs d'adresses IP** pour configurer des géomaps pour un emplacement particulier.

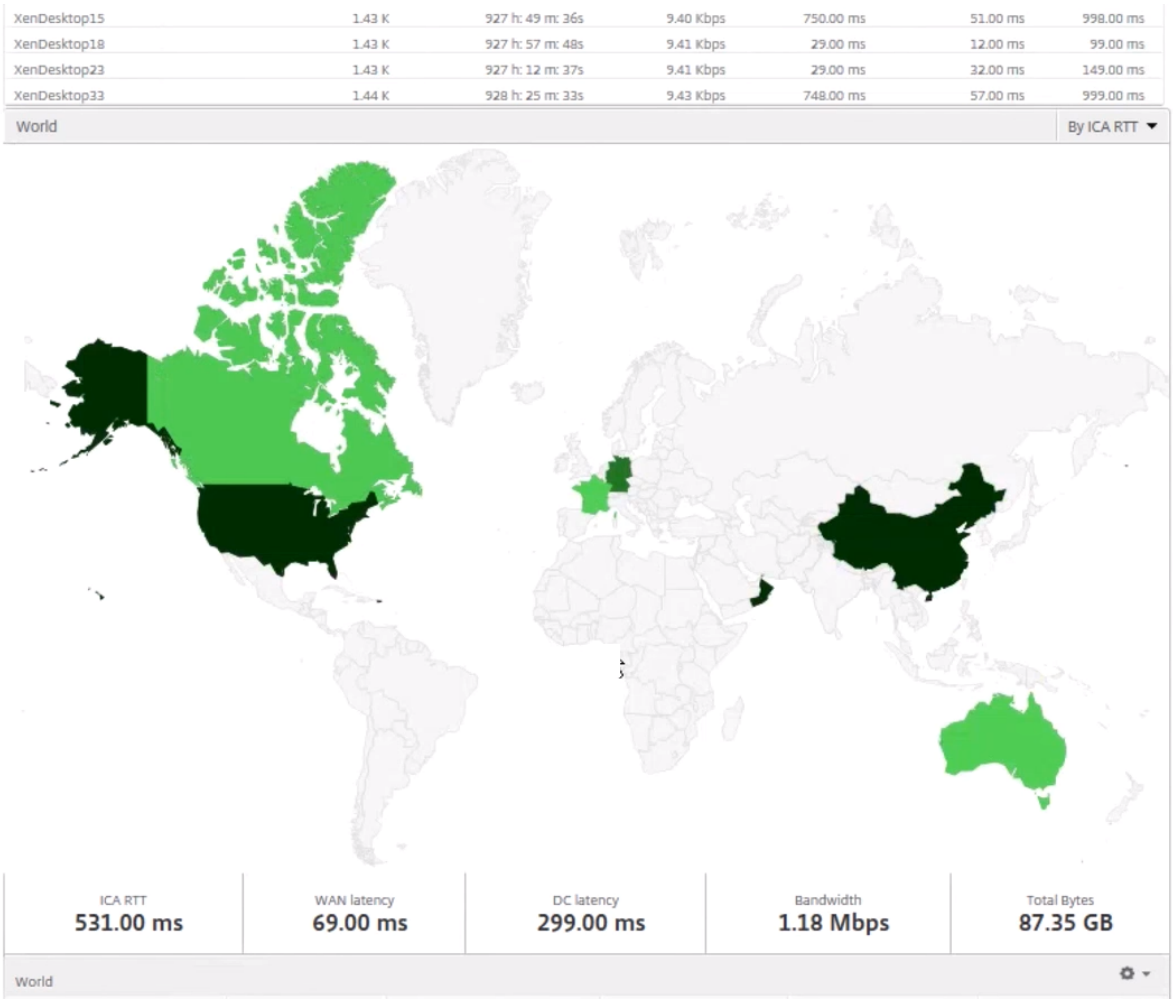
Cas d'utilisation

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 NetScaler Gateway sur Sclara.x.com pour accéder au trafic VPN. Les utilisateurs indiens utilisent l'appliance NetScaler 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 NetScaler Gateway, ce qui retarde la connexion au VPN. Certains utilisateurs se connectent donc à India.x.com au lieu de Sclara.x.com.

Un administrateur NetScaler analysant le trafic peut utiliser la fonctionnalité de carte géographique pour afficher le trafic dans les bureaux de Santa Clara. La carte montre que le temps de réponse du bureau de Santa Clara est élevé, car le bureau de Santa Clara ne dispose que d'une seule appliance NetScaler Gateway via laquelle les utilisateurs peuvent accéder au trafic VPN. L'administrateur peut donc décider d'installer un autre NetScaler Gateway, afin que les utilisateurs disposent de deux appliances NetScaler Gateway locales via lesquelles accéder au VPN.



Limitations

Si les instances NetScaler disposent d'une licence Advanced, les seuils définis sur NetScaler ADM pour HDX Insight ne seront pas déclenchés car les données analytiques ne sont collectées que pendant une heure.

Activation de la collecte de données HDX Insight

February 1, 2024

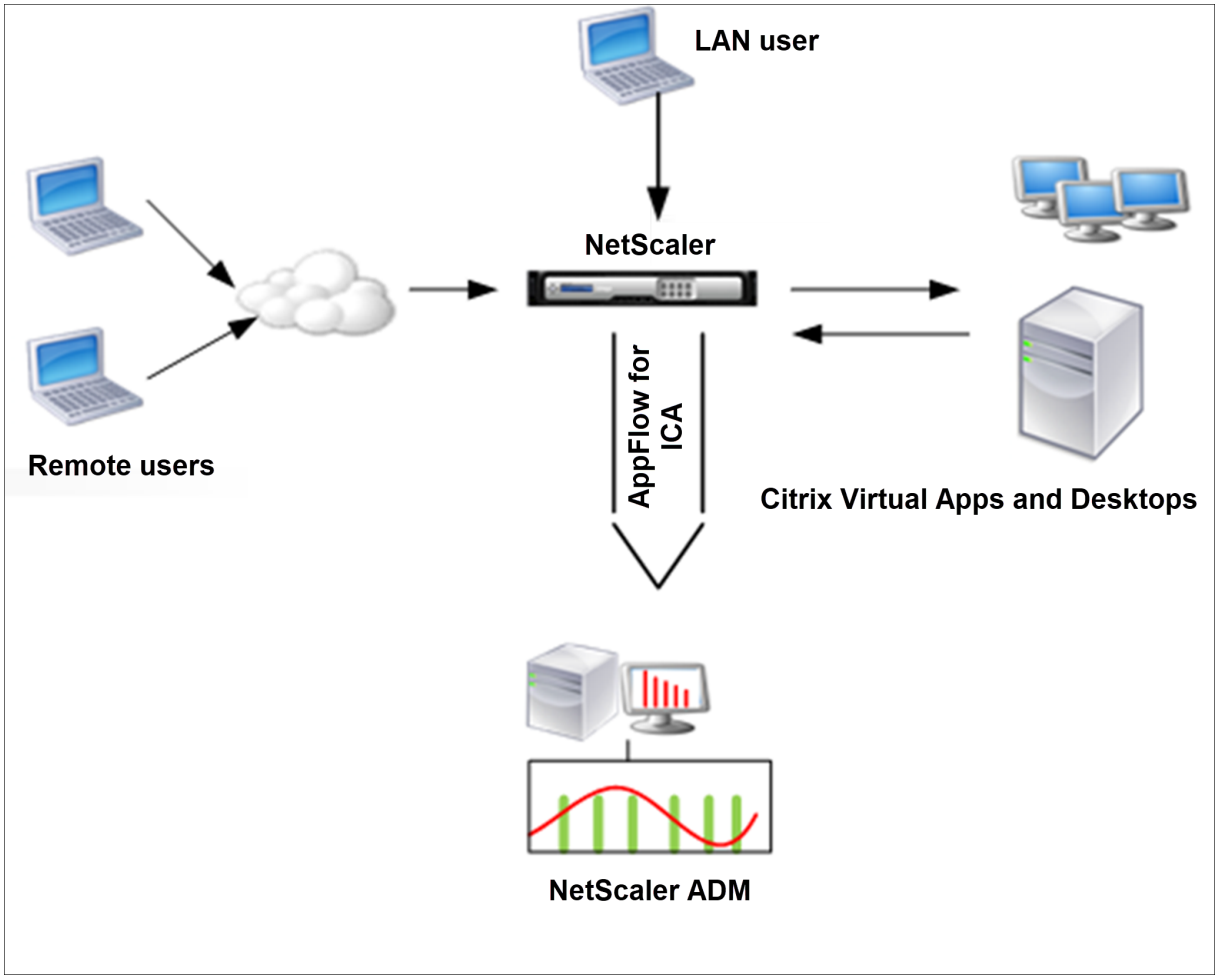
HDX Insight permet au service informatique d'offrir une expérience utilisateur exceptionnelle en fournissant une visibilité de bout en bout sans précédent sur le trafic ICA qui transite par les instances NetScaler et qui fait partie intégrante de NetScaler Application Delivery Management (ADM) Analytics. 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 pour activer la collecte de données dans NetScaler diffère selon la position de l'appliance dans la topologie de déploiement.

Activation de la collecte de données pour la surveillance des NetScalers déployés en mode utilisateur LAN

Les utilisateurs externes qui accèdent aux applications Citrix Virtual App and Desktop doivent s'authentifier sur NetScaler Gateway. Les utilisateurs internes peuvent toutefois ne pas avoir besoin d'être redirigés vers NetScaler Gateway. De plus, dans un déploiement en mode transparent, l'administrateur doit appliquer manuellement les stratégies de routage afin que les demandes soient redirigées vers l'appliance NetScaler.

Pour surmonter ces difficultés et permettre aux utilisateurs du réseau local de se connecter directement aux applications Citrix Virtual App and Desktop, vous pouvez déployer l'appliance NetScaler en mode utilisateur du réseau local en configurant un serveur virtuel de redirection du cache, qui fait office de proxy SOCKS sur l'appliance NetScaler Gateway.



> **Remarque** Les appliances NetScaler ADM et NetScaler Gateway résident dans le même sous-réseau.

Pour surveiller les appliances NetScaler déployées dans ce mode, ajoutez d'abord l'appliance NetScaler à l'inventaire NetScaler Insight, activez AppFlow, puis affichez les rapports sur le tableau de bord.

Après avoir ajouté l'appliance NetScaler à l'inventaire NetScaler ADM, vous devez activer AppFlow pour la collecte de données.

> **Remarque**
>
> - Sur une instance ADC, vous pouvez accéder à **Paramètres > AppFlow > Collectors**pour vérifier si le collecteur (c'est-à-dire NetScaler ADM) est actif ou non. L'instance NetScaler envoie des enregistrements AppFlow à NetScaler ADM à l'aide de NSIP. Mais l'instance utilise son SNIP pour vérifier la connectivité avec NetScaler ADM. Assurez-vous donc que le SNIP est configuré sur l'instance.
> - Vous ne pouvez pas activer la collecte de données sur un NetScaler déployé en mode util-

> isateur LAN à l'aide de l'utilitaire de configuration NetScaler 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, consultez la section Politiques et expressions.

Pour configurer la collecte de données sur une appliance NetScaler 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'un dispositif NetScaler Gateway, ajoutez une action à appliquer par 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 NetScaler ADM en tant que collecteur AppFlow sur l'appliance NetScaler.

```
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 NetScaler Gateway déployées en mode saut unique

Lorsque vous déployez NetScaler Gateway en mode 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 NetScaler via un réseau privé virtuel (VPN).

Pour commencer à collecter les rapports, vous devez ajouter l'appliance NetScaler Gateway à l'inventaire NetScaler Application Delivery Management (ADM) et activer AppFlow sur ADM.

Pour activer la fonctionnalité AppFlow depuis NetScaler ADM :

1. Dans un navigateur Web, saisissez l'adresse IP de NetScaler 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 **Infrastructure > Instances**, puis sélectionnez l'instance NetScaler pour laquelle vous souhaitez activer les analyses.
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**.

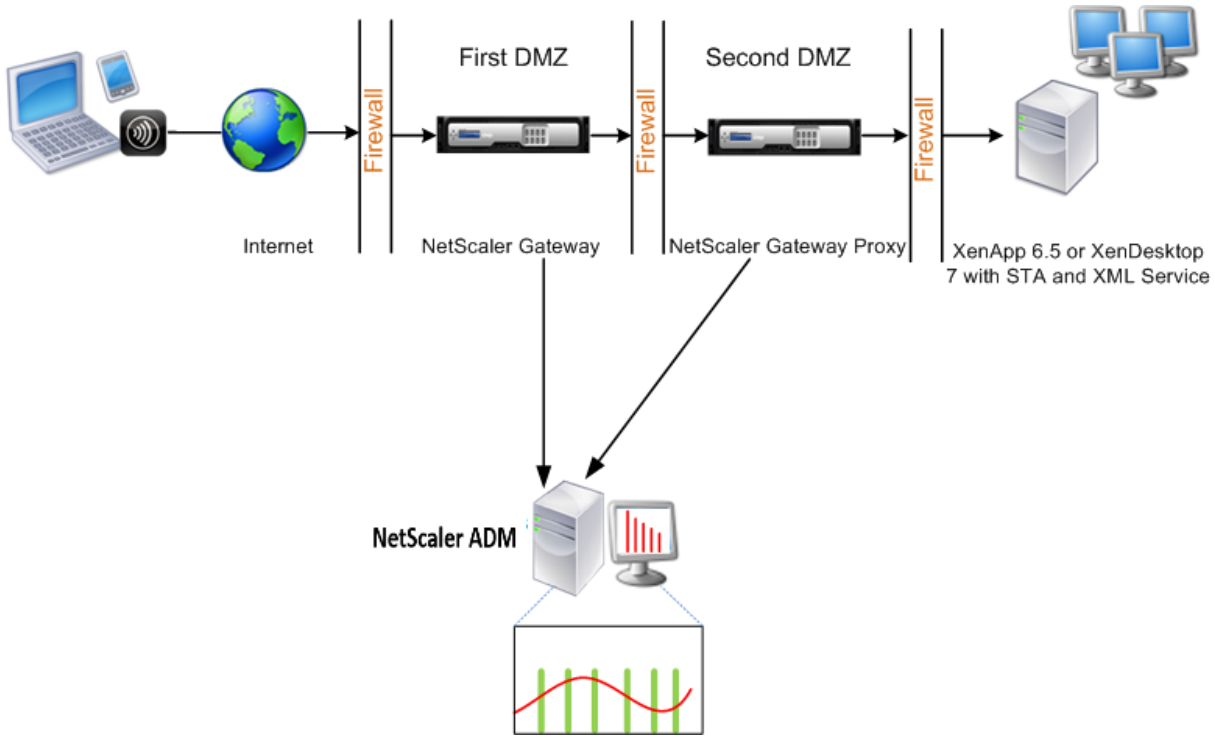
> **Remarque**
>
> lorsque vous activez AppFlow en mode saut unique, les commandes suivantes s'exécutent en arrière-plan. Ces commandes sont explicitement spécifiées ici à des fins de dépannage.

```
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 du canal virtuel EUEM font partie des données HDX Insight que NetScaler ADM reçoit des instances 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 NetScaler ADM.

Activation de la collecte de données pour les appliances NetScaler Gateway déployées en mode double saut

Le mode double saut de NetScaler Gateway fournit une protection supplémentaire au réseau interne d'une entreprise, 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 NetScaler Gateway) par lesquels passent les connexions ICA, ainsi que les détails concernant la latence de chaque connexion TCP et sa comparaison avec la latence ICA totale perçue par le client, vous devez installer NetScaler ADM afin que les appliances NetScaler Gateway publient ces statistiques vitales.



Le NetScaler Gateway de la première zone démilitarisée gère les connexions des utilisateurs et exécute les fonctions de sécurité d'un VPN SSL. Ce NetScaler Gateway chiffre les connexions utilisateur, détermine la manière dont les utilisateurs sont authentifiés et contrôle l'accès aux serveurs du réseau interne.

Le NetScaler Gateway situé dans la deuxième zone démilitarisée sert de périphérique proxy NetScaler Gateway. Ce NetScaler Gateway permet au trafic ICA de traverser la deuxième zone démilitarisée pour terminer les connexions des utilisateurs au parc de serveurs.

Le NetScaler ADM peut être déployé soit dans le sous-réseau appartenant à l'appliance NetScaler Gateway dans la première DMZ, soit dans le sous-réseau appartenant à la seconde DMZ de l'appliance NetScaler Gateway. Dans l'image ci-dessus, NetScaler ADM et NetScaler Gateway de la première zone démilitarisée sont déployés dans le même sous-réseau.

En mode double saut, NetScaler ADM collecte les enregistrements TCP d'une appliance et les enregistrements ICA de l'autre appliance. Une fois que vous avez ajouté les appliances NetScaler Gateway à l'inventaire NetScaler ADM et activé la collecte de données, chacune des appliances exporte les rapports en effectuant le suivi du nombre de sauts et de l'ID de la chaîne de connexion.

Pour que NetScaler ADM puisse identifier 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 NetScaler 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.

NetScaler ADM utilise le nombre de sauts et l'ID de la chaîne de connexion pour corréler les données provenant des deux appliances NetScaler Gateway et générer les rapports.

Pour surveiller les appliances NetScaler Gateway déployées dans ce mode, vous devez d'abord ajouter NetScaler Gateway à l'inventaire NetScaler ADM, activer AppFlow sur NetScaler ADM, puis consulter les rapports sur le tableau de bord NetScaler 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 **Infrastructure > Instances**, puis sélectionnez l'instance NetScaler pour laquelle vous souhaitez activer les analyses.
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 NetScaler ADM

Si vous autorisez NetScaler ADM à 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'un des premiers dispositifs NetScaler Gateway, puis activer AppFlow pour TCP 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 depuis NetScaler ADM :

1. Dans un navigateur Web, saisissez l'adresse IP de NetScaler 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 **Infrastructure > Instances**, puis sélectionnez l'instance NetScaler pour laquelle vous souhaitez activer les analyses.
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 NetScaler, le tableau de bord NetScaler ADM n'affiche pas les enregistrements, même si la colonne Insight indique Activé.

7. Cliquez sur **OK**.

Configuration des appliances NetScaler Gateway pour exporter des données

Après avoir installé les appliances NetScaler Gateway, vous devez configurer les paramètres suivants sur les appliances NetScaler Gateway pour exporter les rapports vers NetScaler ADM :

- Configurez les serveurs virtuels des appliances NetScaler Gateway dans la première et la deuxième zone démilitarisée pour communiquer entre eux.
- Liez le serveur virtuel NetScaler Gateway situé dans la deuxième zone démilitarisée au serveur virtuel NetScaler Gateway situé dans la première zone démilitarisée.
- Activez le double saut sur NetScaler Gateway Gateway dans la deuxième zone démilitarisée.
- Désactivez l'authentification sur le serveur virtuel NetScaler Gateway dans la deuxième zone démilitarisée.
- Activer l'une des appliances NetScaler Gateway pour exporter des enregistrements ICA

- Activez l'autre appliance NetScaler Gateway pour exporter les enregistrements TCP :
- Activez le chaînage des connexions sur les deux appliances NetScaler Gateway.

Configurez NetScaler Gateway à l'aide de l'interface de ligne de commande :

1. Configurez le serveur virtuel NetScaler Gateway dans la première DMZ pour communiquer avec le serveur virtuel NetScaler Gateway dans la seconde 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 NetScaler Gateway situé dans la deuxième zone démilitarisée au serveur virtuel NetScaler Gateway situé dans la première zone démilitarisée. Exécutez la commande suivante sur NetScaler Gateway dans la première zone démilitarisée :

```
bind vpn vserver <name> -nextHopServer <name>

bind vpn vserver vs1 -nextHopServer nh1
```

3. Activez le double saut et AppFlow sur NetScaler Gateway dans la deuxième zone démilitarisée.

```
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 NetScaler Gateway dans la deuxième zone démilitarisée.

```
set vpn vserver <name> [-authentication (ON or OFF)]

set vpn vserver vs -authentication OFF
```

5. Activez l'une des appliances NetScaler 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 NetScaler Gateway pour exporter les 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 NetScaler Gateway :

```
set appFlow param [-connectionChaining (ENABLED or DISABLED)]

set appflow param -connectionChaining ENABLED
```

Configurer NetScaler Gateway à l'aide de l'utilitaire de configuration :

1. Configurez le NetScaler Gateway dans la première DMZ pour communiquer avec le NetScaler Gateway dans la seconde DMZ et liez le Citrix NetScaler dans la seconde DMZ au NetScaler Gateway dans la première DMZ.

   a) Dans l'onglet **Configuration**, développez **NetScaler Gateway** et cliquez sur **Virtual Servers**.

   b) Dans le volet droit, double-cliquez sur le serveur virtuel et, dans le groupe Avancé, développez**Applications publiées**.

   c) Cliquez sur**Next Hop Server** et liez un serveur Next Hop à la deuxième appliance NetScaler Gateway.

2. Activez le double saut sur NetScaler Gateway Gateway dans la deuxième zone démilitarisée.

   a) Dans l'onglet **Configuration**, développez **NetScaler 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, sélectionnez **Double saut** et cliquez sur **OK**.

3. Désactivez l'authentification sur le serveur virtuel sur NetScaler Gateway dans la deuxième zone démilitarisée.

   a) Dans l'onglet **Configuration** , développez **NetScaler 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 NetScaler Gateway pour exporter des enregistrements TCP.

   a) Dans l'onglet **Configuration** , développez **NetScaler 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 NetScaler Gateway pour exporter les enregistrements ICA :

a) Dans l'onglet **Configuration** , développez **NetScaler 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 NetScaler 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 le NetScaler Gateway dans la première DMZ pour communiquer avec le NetScaler Gateway dans la seconde DMZ et liez le Citrix NetScaler dans la seconde DMZ au NetScaler Gateway dans la première DMZ.

a) Dans l'onglet Configuration , développez **NetScaler Gateway** et cliquez sur **Virtual Servers**.

b) Dans le volet droit, double-cliquez sur le serveur virtuel, puis dans le**groupe Avancé** , développez**Applications publiées**.

c) Cliquez sur**Next Hop Server** et liez un serveur Next Hop à la deuxième appliance NetScaler Gateway.

8. Activez le double saut sur NetScaler Gateway Gateway dans la deuxième zone démilitarisée.

a) Dans l'onglet Configuration , développez **NetScaler 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, sélectionnez **Double saut**, puis cliquez sur **OK**.

9. Désactivez l'authentification sur le serveur virtuel sur NetScaler Gateway dans la deuxième zone démilitarisée.

   a) Dans l'onglet Configuration , développez NetScaler 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 NetScaler Gateway pour exporter des enregistrements TCP.

    a) Dans l'onglet Configuration , développez **NetScaler Gateway** et cliquez sur **Virtual Servers**.

    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 NetScaler Gateway pour exporter des enregistrements ICA.

    a) Dans l'onglet Configuration , développez **NetScaler 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**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 NetScaler Gateway.

Activer la collecte de données pour surveiller les NetScalers déployés en mode transparent

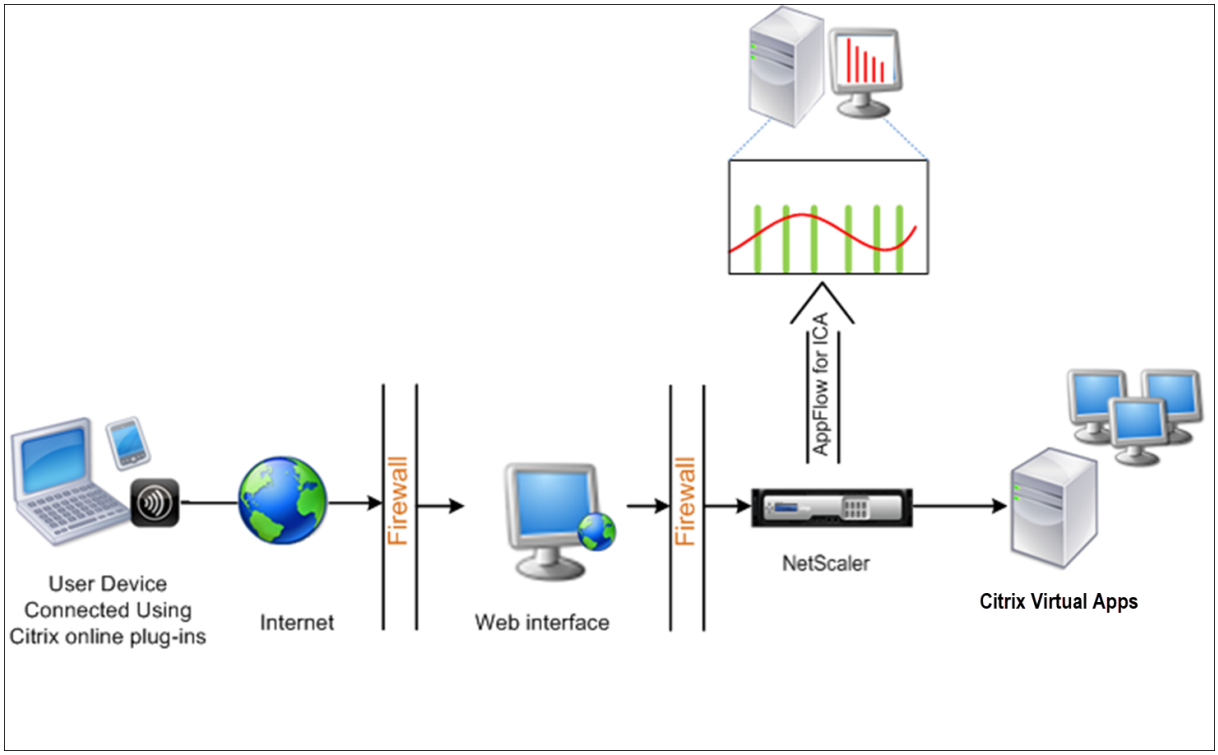
Lorsqu'un NetScaler est déployé en mode transparent, les clients peuvent accéder directement aux serveurs, sans aucun serveur virtuel intermédiaire. Si une appliance NetScaler est déployée en mode

transparent dans un environnement Citrix Virtual Apps and Desktop, le trafic ICA n'est pas transmis via un VPN.

Après avoir ajouté NetScaler à l'inventaire NetScaler 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 NetScaler ADM en tant que collecteur AppFlow sur chaque appliance NetScaler, et vous devez configurer une stratégie AppFlow pour collecter tout ou partie du trafic ICA qui passe par l'appliance.

> **Remarque**
>
> - Vous ne pouvez pas activer la collecte de données sur un NetScaler déployé en mode transparent à l'aide de l'utilitaire de configuration NetScaler 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 montre le déploiement réseau d'un NetScaler ADM lorsqu'un NetScaler est déployé en mode transparent :



Pour configurer la collecte de données sur une appliance NetScaler 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 NetScaler 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 NetScaler.

```
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 NetScaler, 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
```

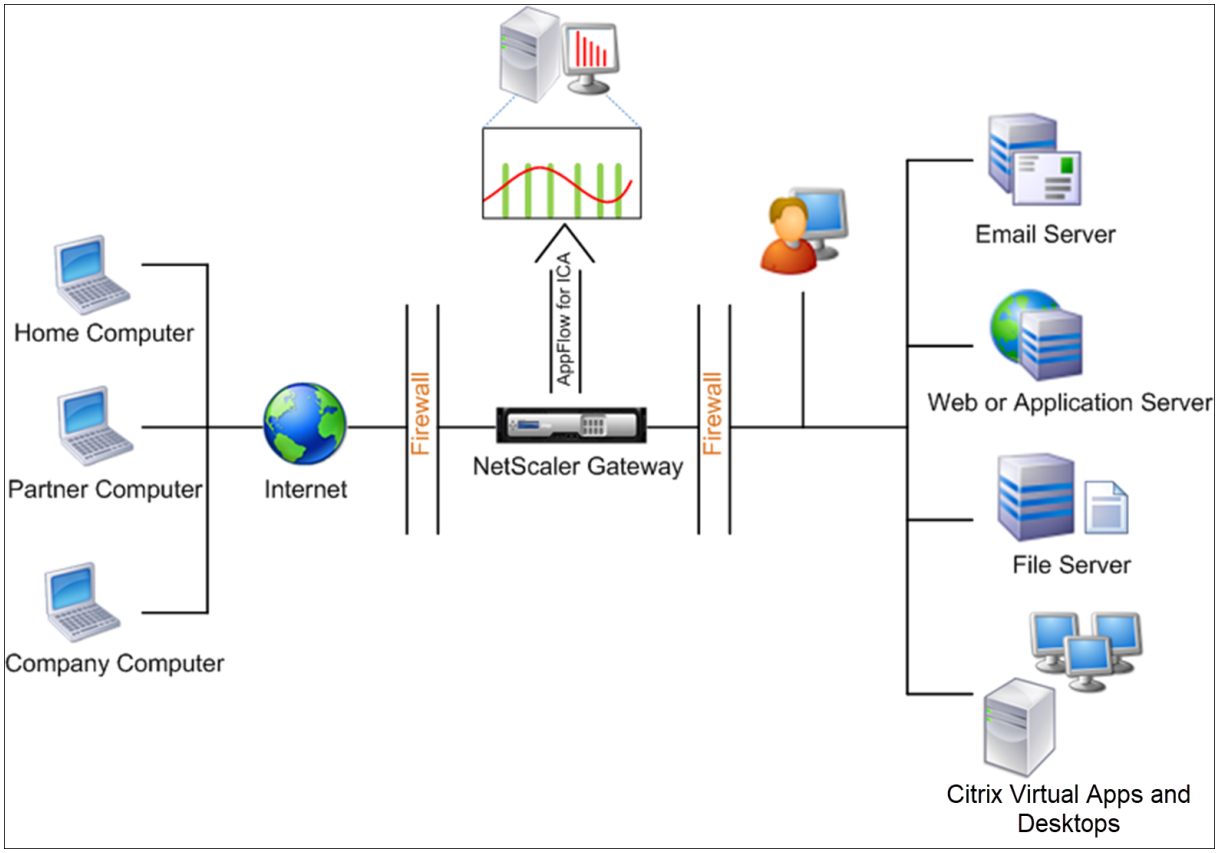
8. Enregistrez la configuration. Type : `save ns config`
"'

Activer la collecte de données pour les appliances NetScaler Gateway déployées en mode saut unique

February 1, 2024

Lorsque vous déployez NetScaler Gateway en mode 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 NetScaler via un réseau privé virtuel (VPN).

Pour commencer à collecter les rapports, vous devez ajouter l'appliance NetScaler Gateway à l'inventaire NetScaler 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 NetScaler 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**.
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 du canal virtuel EUEM font partie des données HDX Insight que NetScaler ADM reçoit des instances 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 NetScaler ADM.

Activez la collecte de données pour surveiller les NetScalers déployés en mode transparent

February 1, 2024

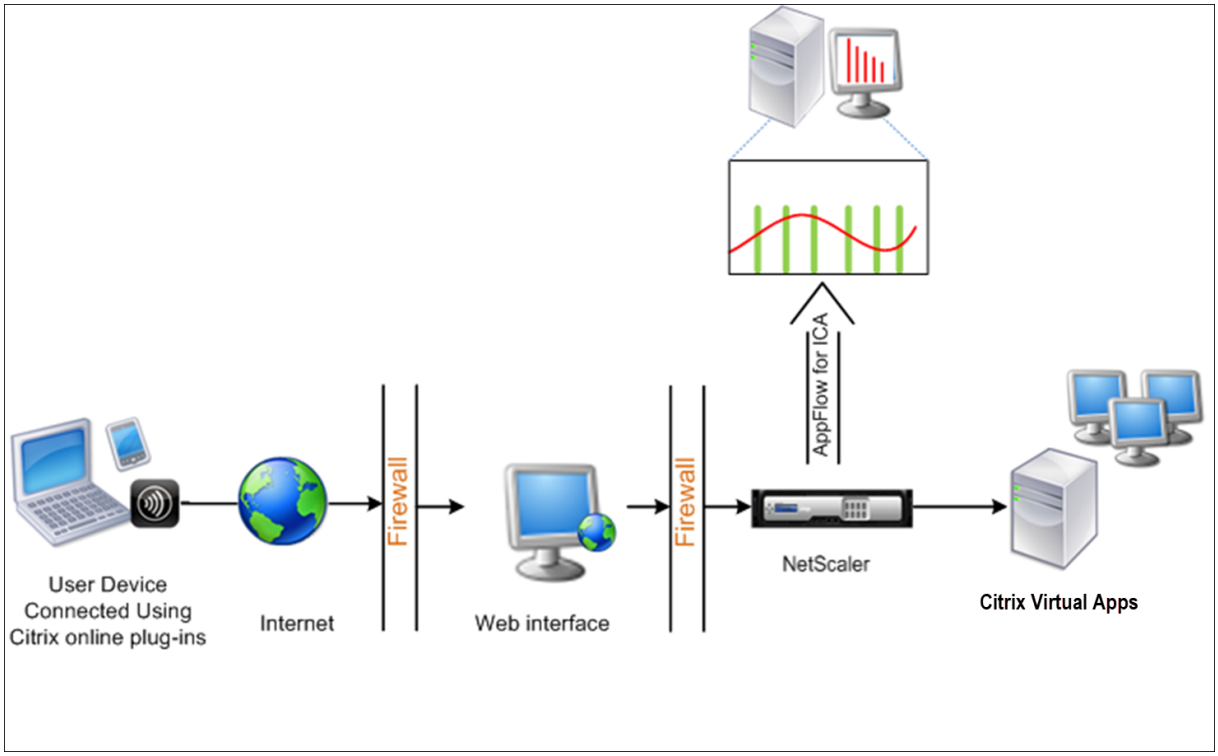
Lorsqu'un NetScaler est déployé en mode transparent, les clients peuvent accéder directement aux serveurs, sans aucun serveur virtuel intermédiaire. Si un NetScaler est déployé en mode transparent dans un environnement Citrix Virtual Apps and Desktops, le trafic ICA n'est pas transmis via un VPN.

Après avoir ajouté NetScaler à l'inventaire NetScaler 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 NetScaler ADM en tant que collecteur AppFlow sur chaque instance de NetScaler, et vous devez configurer une stratégie AppFlow pour collecter tout ou partie du trafic ICA qui circule via l'appliance.

Remarque

- Vous ne pouvez pas activer la collecte de données sur un NetScaler déployé en mode transparent à l'aide de l'utilitaire de configuration NetScaler 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 montre le déploiement réseau d'un NetScaler ADM lorsqu'un NetScaler est déployé en mode transparent :



Pour configurer la collecte de données sur une appliance NetScaler 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 NetScaler 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 NetScaler.

```
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 NetScaler, 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
```



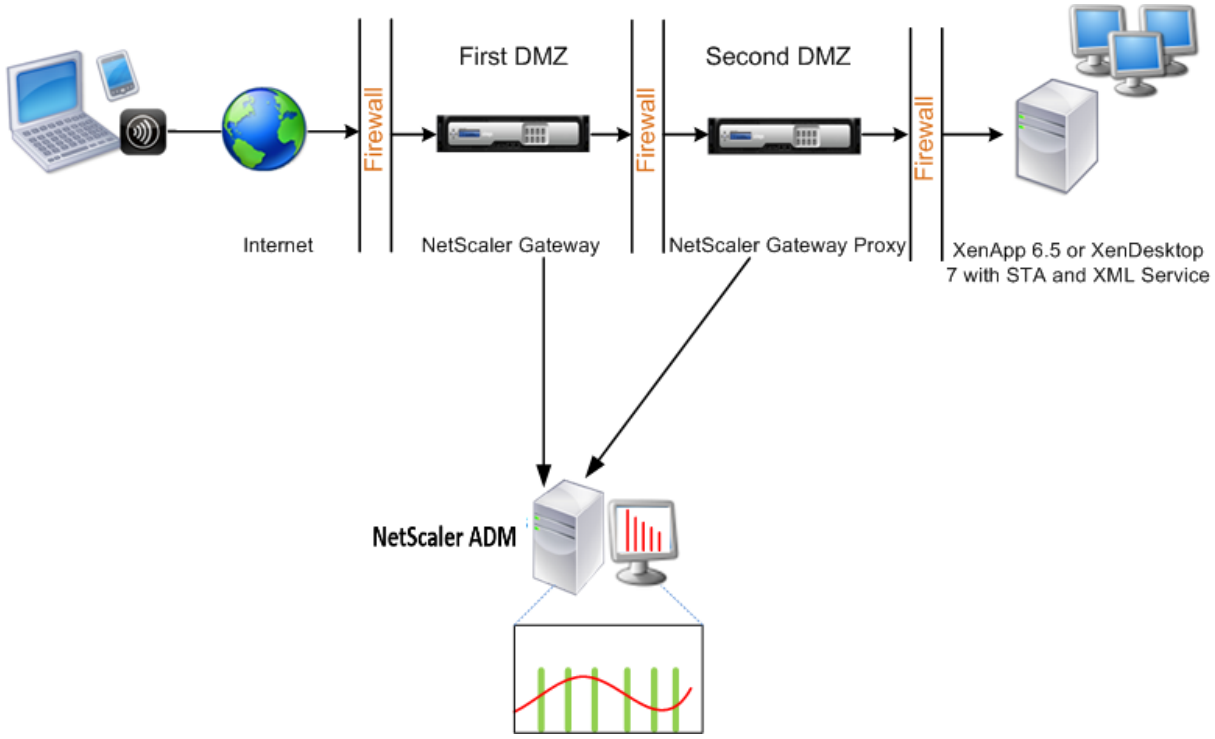
```
<!--NeedCopy-->
```

Activer la collecte de données pour les appliances NetScaler Gateway déployées en mode double saut

February 1, 2024

Le mode double saut de NetScaler Gateway fournit une protection supplémentaire au réseau interne d'une entreprise, 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 NetScaler Gateway) par lesquels passent les connexions ICA, ainsi que les détails concernant la latence de chaque connexion TCP et sa comparaison avec la latence ICA totale perçue par le client, vous devez installer NetScaler ADM, afin que les appliances NetScaler Gateway publient ces statistiques vitales.

Figure 3. NetScaler ADM déployé en mode double saut



Le NetScaler Gateway de la première zone démilitarisée gère les connexions des utilisateurs et exécute les fonctions de sécurité d'un VPN SSL. Ce NetScaler Gateway chiffre les connexions utilisateur, détermine la manière dont les utilisateurs sont authentifiés et contrôle l'accès aux serveurs du réseau interne.

Le NetScaler Gateway situé dans la deuxième zone démilitarisée sert de périphérique proxy NetScaler Gateway. Ce NetScaler Gateway permet au trafic ICA de traverser la deuxième zone démilitarisée pour terminer les connexions des utilisateurs au parc de serveurs.

Le NetScaler ADM peut être déployé soit dans le sous-réseau appartenant à l'appliance NetScaler Gateway dans la première DMZ, soit dans le sous-réseau appartenant à la seconde DMZ de l'appliance NetScaler Gateway. Dans l'image ci-dessus, NetScaler ADM et NetScaler Gateway de la première zone démilitarisée sont déployés dans le même sous-réseau.

En mode double saut, NetScaler ADM collecte les enregistrements TCP d'une appliance et les enregistrements ICA de l'autre appliance. Une fois que vous avez ajouté les appliances NetScaler Gateway à l'inventaire NetScaler ADM et activé la collecte de données, chaque appliance exporte les rapports en effectuant le suivi du nombre de sauts et de l'ID de la chaîne de connexion.

Pour que NetScaler ADM puisse identifier 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 NetScaler 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.

NetScaler ADM utilise le nombre de sauts et l'ID de la chaîne de connexion pour corréler les données provenant des deux appliances NetScaler Gateway et générer les rapports.

Pour surveiller les appliances NetScaler Gateway déployées dans ce mode, vous devez d'abord ajouter NetScaler Gateway à l'inventaire NetScaler ADM, activer AppFlow sur NetScaler ADM, puis consulter les rapports sur le tableau de bord NetScaler ADM.

Activer la collecte de données sur NetScaler ADM

Si vous autorisez NetScaler ADM à 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'une des premières appliances NetScaler 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 depuis NetScaler ADM :

1. Accédez à **Infrastructure > Instances**, puis sélectionnez l'instance NetScaler 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 les groupes de services de l'appliance NetScaler, le tableau de bord NetScaler ADM n'affiche pas les enregistrements, même si la colonne Insight indique Activé.

5. Cliquez sur **OK**.

Configurer les appliances NetScaler Gateway pour exporter des données

Après avoir installé les appliances NetScaler Gateway, vous devez configurer les paramètres suivants sur les appliances NetScaler Gateway pour exporter les rapports vers NetScaler ADM :

- Configurez les serveurs virtuels des appliances NetScaler Gateway dans la première et la deuxième zone démilitarisée pour communiquer entre eux.
- Liez le serveur virtuel NetScaler Gateway situé dans la deuxième zone démilitarisée au serveur virtuel NetScaler Gateway situé dans la première zone démilitarisée.
- Activez le double saut sur NetScaler Gateway Gateway dans la deuxième zone démilitarisée.
- Désactivez l'authentification sur le serveur virtuel NetScaler Gateway dans la deuxième zone démilitarisée.
- Activer l'une des appliances NetScaler Gateway pour exporter des enregistrements ICA
- Activez l'autre appliance NetScaler Gateway pour exporter les enregistrements TCP :
- Activez le chaînage des connexions sur les deux appliances NetScaler Gateway.

Configurez NetScaler Gateway à l'aide de l'interface de ligne de commande :

1. Configurez le serveur virtuel NetScaler Gateway dans la première DMZ pour communiquer avec le serveur virtuel NetScaler Gateway dans la seconde DMZ.

---

add vpn nextHopServer [**-secure**(ON OFF)] [**-imgGifToPng**] …

```
1 add vpn nextHopServer nh1 10.102.2.33 8443 –secure ON
2 <!--NeedCopy-->
```

2. Liez le serveur virtuel NetScaler Gateway situé dans la deuxième zone démilitarisée au serveur virtuel NetScaler Gateway situé dans la première zone démilitarisée. Exécutez la commande suivante sur NetScaler Gateway dans la première zone démilitarisée :

bind vpn vserver <name> **-nextHopServer** <name>

```
bind vpn vserver vs1 -nextHopServer nh1
<!--NeedCopy-->
```

3. Activez le double saut et AppFlow sur NetScaler Gateway dans la deuxième zone démilitarisée.

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 NetScaler Gateway dans la deuxième zone démilitarisée.

set vpn vserver [**-authentication** (ON	OFF)]

```
set vpn vserver vs -authentication OFF
<!--NeedCopy-->
```

5. Activez l'une des appliances NetScaler 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 NetScaler Gateway pour exporter les 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 NetScaler Gateway :

set appFlow param [**-connectionChaining** (ENABLED	DISABLED)]

```
set appflow param -connectionChaining ENABLED
<!--NeedCopy-->
```


Configuration de NetScaler Gateway à l'aide de l'utilitaire de configuration :

1. Configurez le NetScaler Gateway dans la première DMZ pour communiquer avec le NetScaler Gateway dans la seconde DMZ et liez le Citrix NetScaler dans la seconde DMZ au NetScaler Gateway dans la première DMZ.

    a) Dans l'onglet **Configuration**, développez **NetScaler Gateway** et cliquez sur **Virtual Servers**.

    b) Dans le volet droit, double-cliquez sur le serveur virtuel et, dans le groupe Avancé, développez**Applications publiées**.

    c) Cliquez sur**Next Hop Server** et liez un serveur Next Hop à la deuxième appliance NetScaler Gateway.

2. Activez le double saut sur NetScaler Gateway Gateway dans la deuxième zone démilitarisée.

    a) Dans l'onglet **Configuration**, développez **NetScaler 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**, sélectionnez**Double saut**et cliquez sur**OK**.

3. Désactivez l'authentification sur le serveur virtuel sur NetScaler Gateway dans la deuxième zone démilitarisée.

    a) Dans l'onglet **Configuration** , développez **NetScaler 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 NetScaler Gateway pour exporter des enregistrements TCP.

    a) Dans l'onglet **Configuration** , développez **NetScaler 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 NetScaler Gateway pour exporter les enregistrements ICA :
    a) Dans l'onglet **Configuration** , développez **NetScaler 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 NetScaler Gateway.
    a) Dans l'onglet**Configuration**, accédez à**Paramètres > 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**.

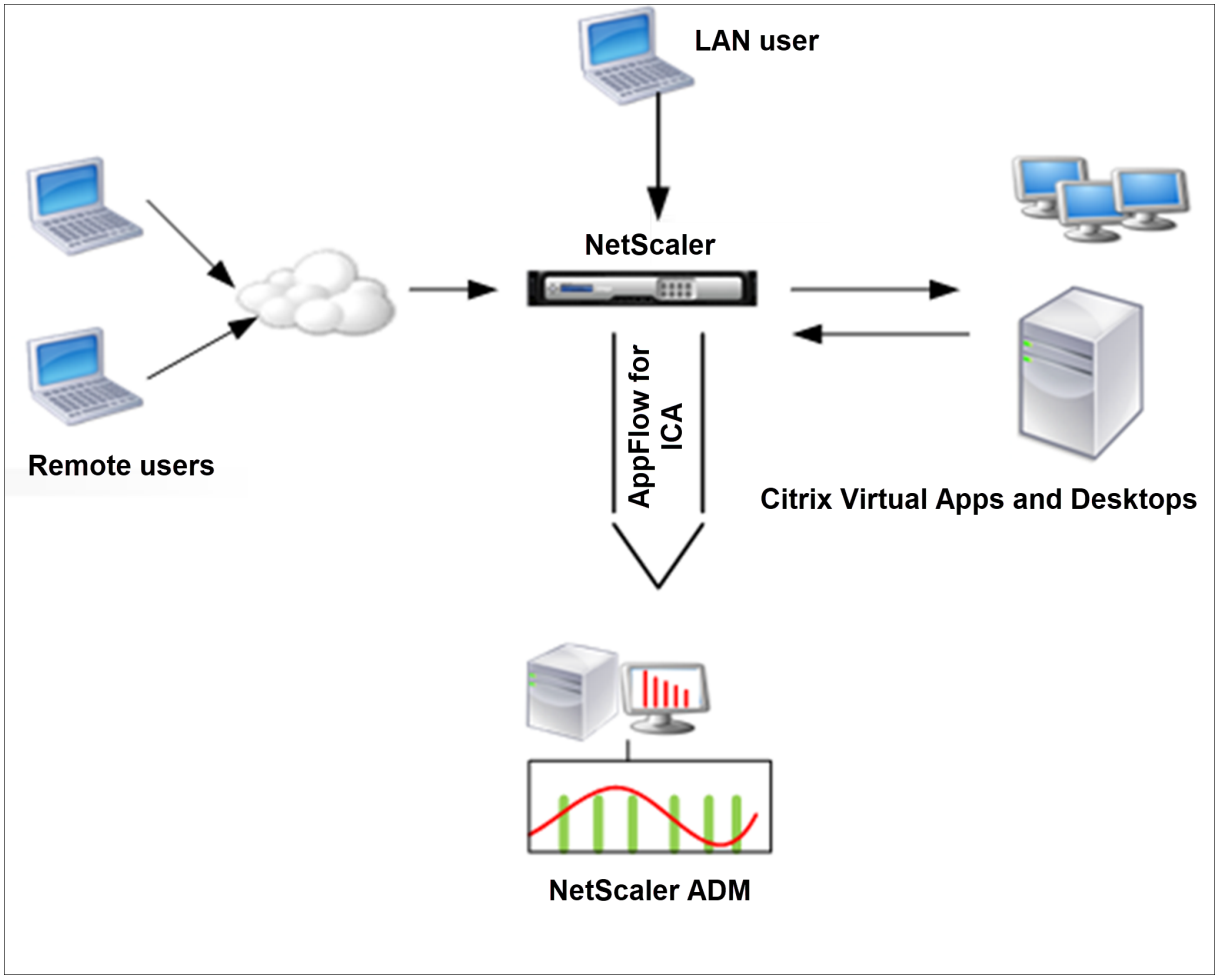
Activer la collecte de données pour surveiller les NetScalers déployés en mode utilisateur LAN

February 1, 2024

Les utilisateurs externes qui accèdent aux applications Citrix Virtual App ou Desktop doivent s'authentifier sur NetScaler Gateway. Les utilisateurs internes peuvent toutefois ne pas avoir besoin d'être redirigés vers NetScaler Gateway. De plus, dans un déploiement en mode transparent, l'administrateur doit appliquer manuellement les stratégies de routage afin que les demandes soient redirigées vers l'appliance NetScaler.

Pour surmonter ces difficultés et permettre aux utilisateurs du réseau local de se connecter directement aux applications Citrix Virtual Apps and Desktops, vous pouvez déployer l'appliance NetScaler en mode utilisateur du réseau local en configurant un serveur virtuel de redirection du cache, qui fait office de proxy SOCKS sur l'appliance NetScaler Gateway.

Figure 4. NetScaler ADM déployé en mode utilisateur LAN



Remarque Les appliances NetScaler ADM et NetScaler Gateway résident dans le même sous-réseau.

Pour surveiller les appliances NetScaler déployées dans ce mode, ajoutez d'abord l'appliance NetScaler à l'inventaire NetScaler Insight, activez AppFlow, puis affichez les rapports sur le tableau de bord.

Après avoir ajouté l'appliance NetScaler à l'inventaire NetScaler ADM, vous devez activer AppFlow pour la collecte de données.

> **Remarque**
>
> - Vous ne pouvez pas activer la collecte de données sur un NetScaler déployé en mode utilisateur LAN à l'aide de l'utilitaire de configuration NetScaler 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 une appliance NetScaler 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 local à l'aide d'une appliance NetScaler Gateway, ajoutez une action à appliquer par une stratégie qui correspond 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 NetScaler ADM en tant que collecteur AppFlow sur l'appliance NetScaler.

```
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 NetScaler Application Delivery Management (ADM) vous permet de surveiller le trafic HDX passant par les instances NetScaler. NetScaler 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 NetScaler 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 NetScaler 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 NetScaler ADM uniquement si toutes les règles du groupe de seuils configuré ne sont pas respectées. 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, NetScaler ADM génère un événement indiquant 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 NetScaler ADM et/ou la recevoir sous forme d'e-mail ou de SMS sur votre appareil mobile. Pour les deux dernières actions, vous devez configurer le serveur de messagerie ou le serveur SMS sur NetScaler 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 NetScaler 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 NetScaler ADM :

1. Dans NetScaler ADM, accédez à **Paramètres > Paramètres d'analyse > 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 :

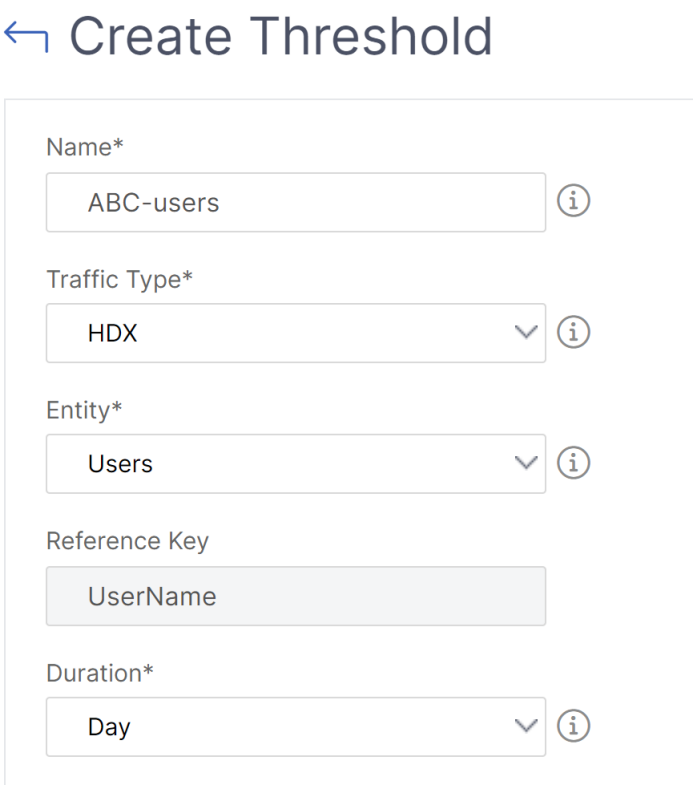
a) **Nom**. Entrez un nom pour créer un événement pour lequel NetScaler ADM génère une alerte.

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.

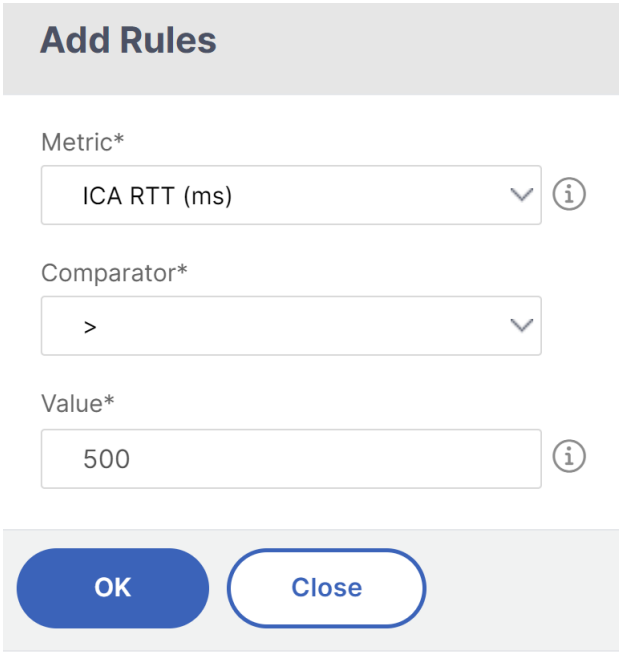
d) **Clé de référence**. Une clé de référence est automatiquement générée en fonction du type de trafic et de l'entité que vous avez sélectionnés.

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.

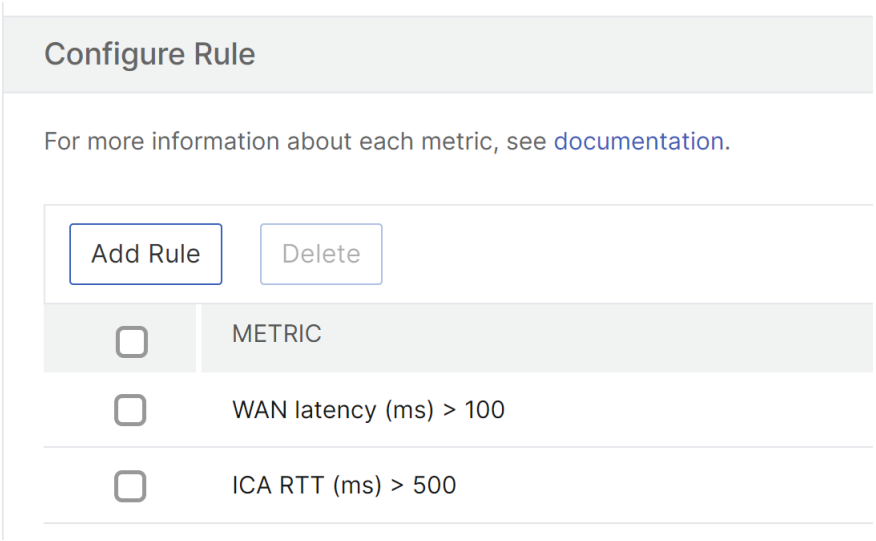


3. Création d'un groupe de règles de seuil pour toutes les entités :

   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.

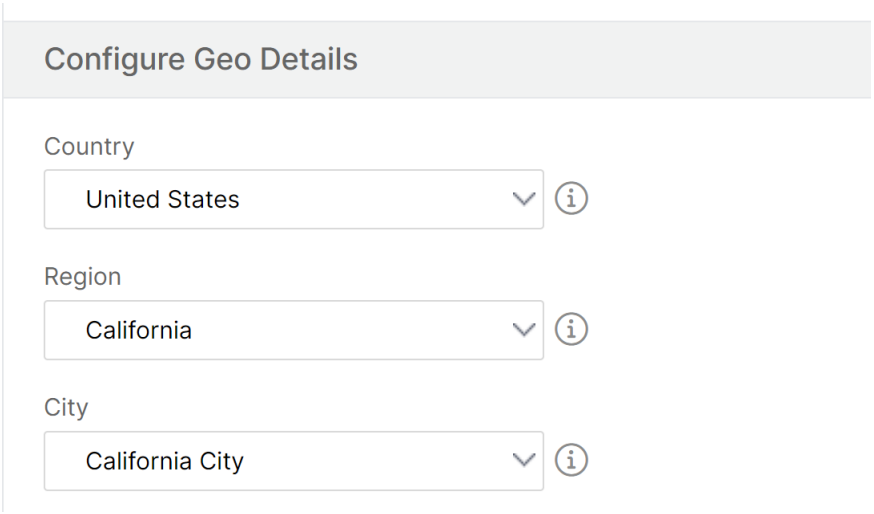


Vous pouvez créer plusieurs règles pour surveiller chaque entité. La création de plusieurs règles dans un seul groupe vous permet de surveiller les entités sous la forme d'un groupe de règles de seuil au lieu de règles individuelles. Cliquez sur **OK** pour fermer la fenêtre.



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 NetScaler 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 Insight fournit une visibilité complète des rapports et des mesures relatifs au trafic HDX sur vos instances NetScaler.

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 sur le nombre total d'applications et toutes les informations pertinentes connexes, telles que le nombre total de fois où les applications ont été lancées au cours de l'intervalle de temps spécifié.
- **Instances** : affiche les rapports sur les instances NetScaler qui font office de passerelles pour le trafic entrant.
- **Bureaux** : affiche les rapports des bureaux utilisés dans la période sélectionnée.

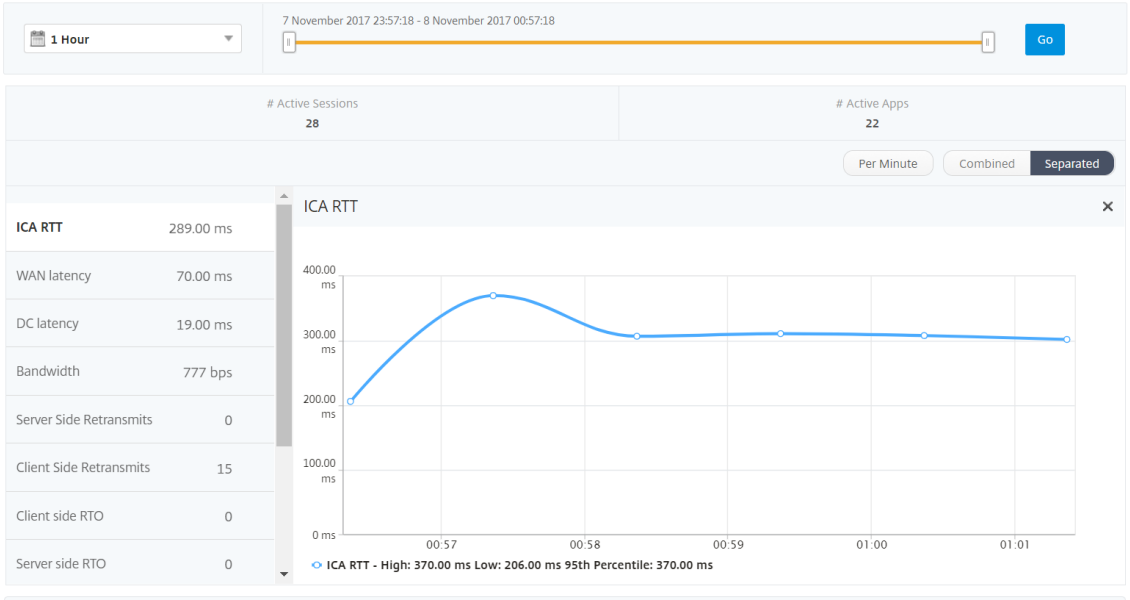
- **Licences** : affiche les rapports pour le nombre total de licences VPN SSL utilisées dans le créneau horaire spécifié.

Rapports et mesures d'affichage des utilisateurs

Les rapports et les mesures de cette vue sont affichés par utilisateur de Citrix Virtual Apps and Desktops.

Pour accéder à la vue des utilisateurs :

1. Accédez à **Gateway > 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

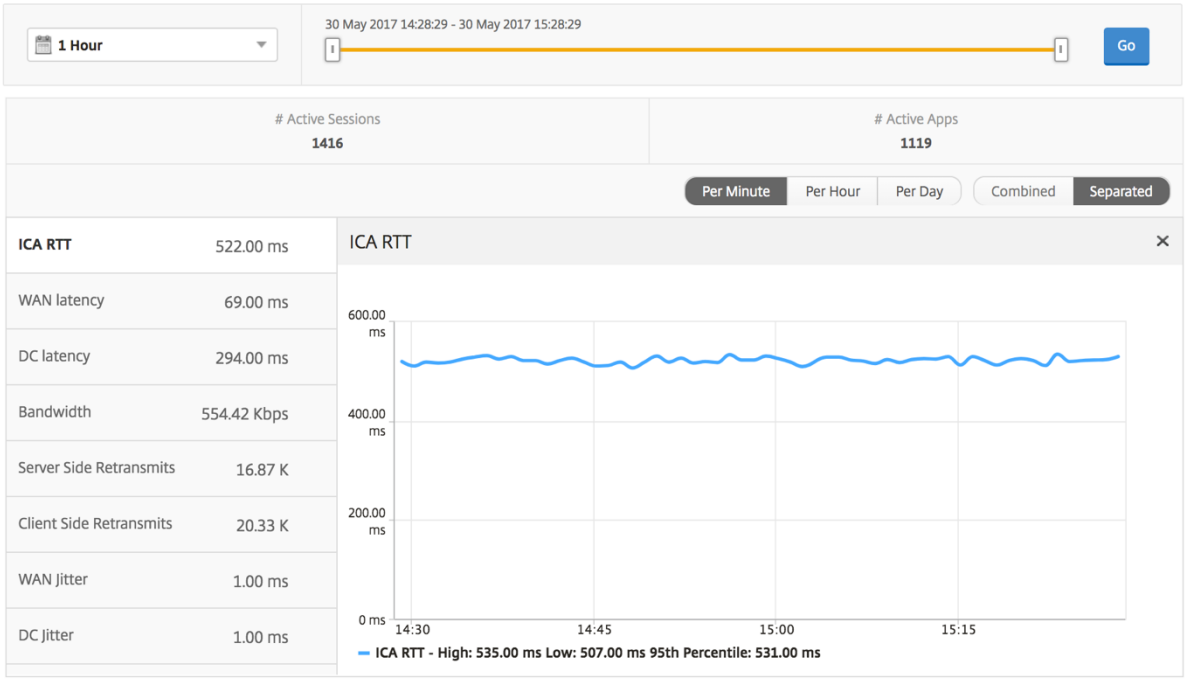
La vue récapitulative affiche les rapports de tous les utilisateurs qui se sont connectés au cours de la chronologie sélectionnée. Toutes les métriques/rapports de cette vue affichent les valeurs qui leur correspondent pour la période sélectionnée, sauf indication contraire.

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 NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre NetScaler Gateway et les serveurs VDI OU 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 lors de la connexion entre NetScaler et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre NetScaler 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 NetScaler et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre NetScaler 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 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 NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre NetScaler 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.

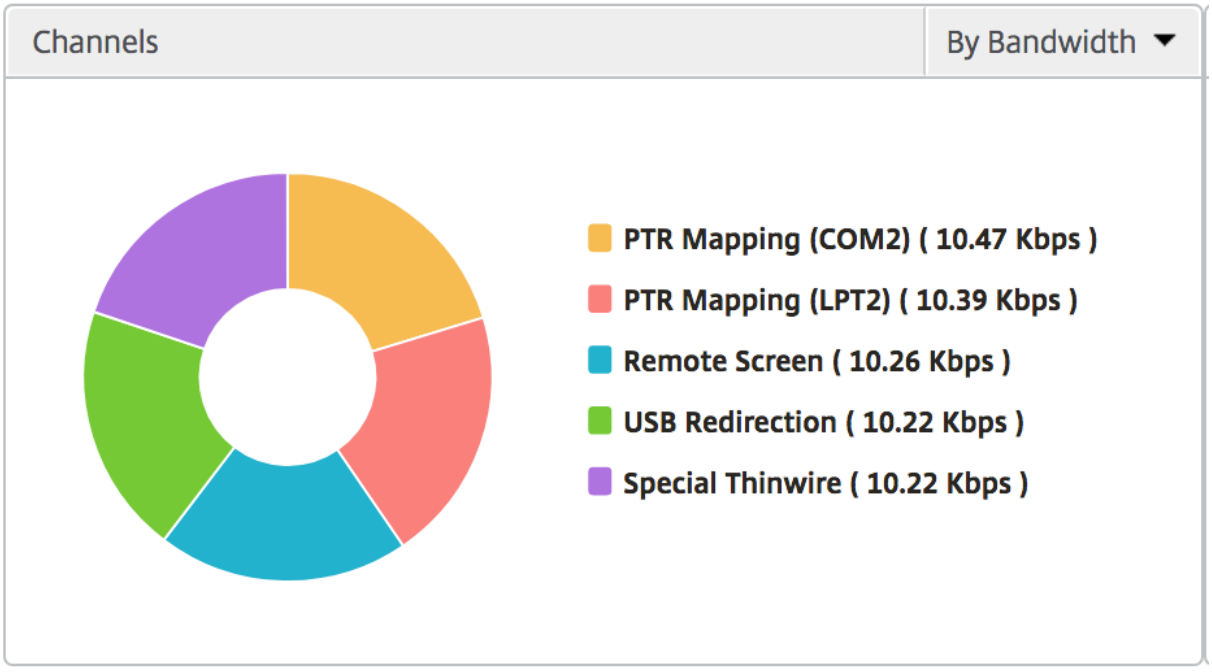
Mesures	Description
Retransmissions côté serveur	Nombre de paquets retransmis lors de la connexion entre NetScaler et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre NetScaler et l'utilisateur final. Une valeur élevée de cette mesure ne signifie 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 NetScaler et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre NetScaler 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

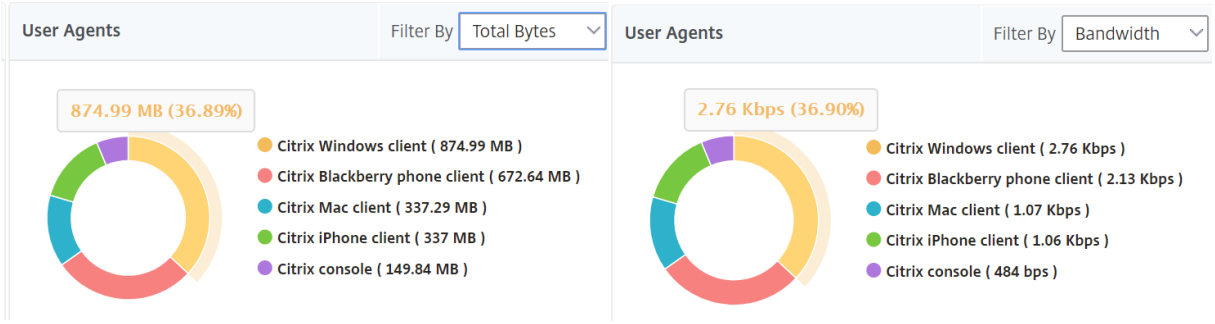
Search

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	

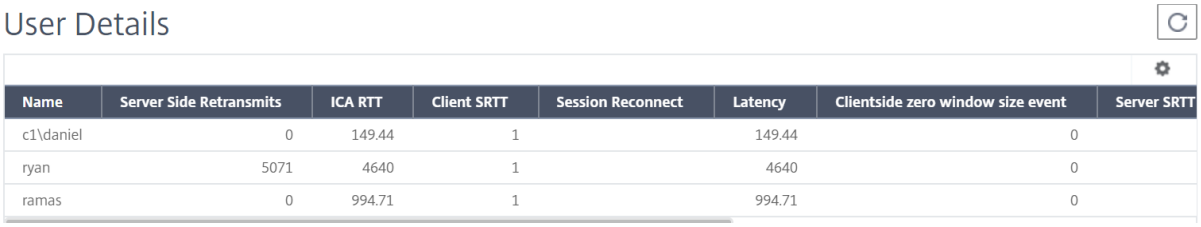
Canaux Les canaux représentent la bande passante globale ou le nombre total d'octets consommés par chaque canal virtuel ICA sous la forme d'un graphique en anneau. Vous pouvez également trier les mesures par bande passante ou Nombre total d'octets.



Agents utilisateurs Les agents utilisateurs représentent la bande passante globale/le nombre total d'octets consommés par chaque client d'espace de travail sous la forme d'un graphique en anneau. Chaque segment coloré du graphique représente un client d'espace de travail. La longueur du segment dépend du nombre d'utilisateurs qui lancent leurs applications sur ce client d'espace de travail. 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 d'espace de travail.



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	

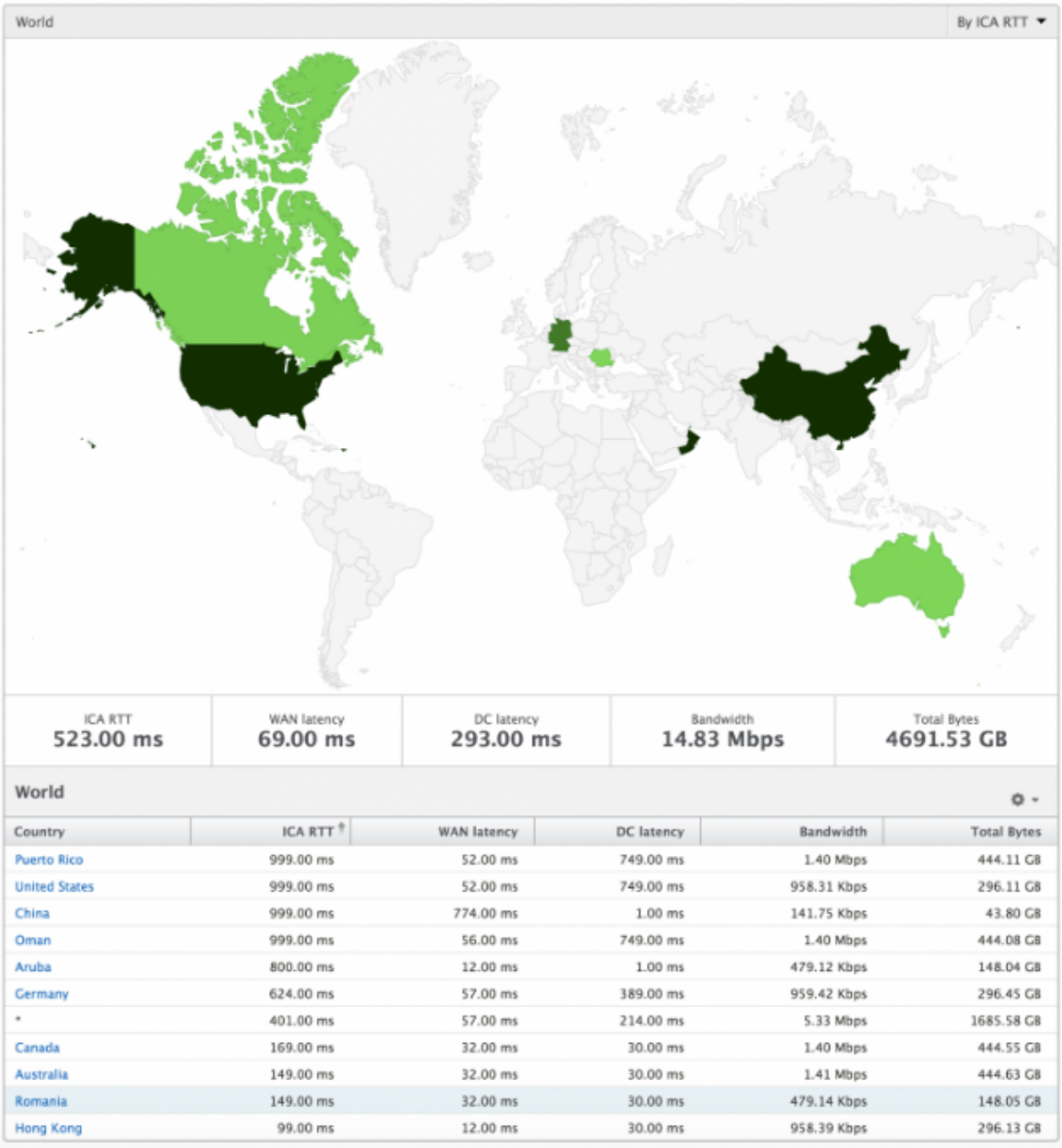
Nombre de violations des seuils Les mesures de nombre de violations des seuils représentent le nombre de seuils violés au cours de la période sélectionnée.

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 des versions 12.0 et ultérieures de NetScaler ADM, vous pouvez accéder aux 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 NetScaler ADM à l'aide d'un navigateur Web compatible.
2. Accédez à **Gateway > 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	Retard moyen du trafic ICA passant par les NetScalers dû au 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 d'espace de travail : client Windows Citrix, etc.
Version du client	Version Workspace.
MSI	Boolean (Oui/Non). Indique si la session est multiflux ICA.
Reconnexions de session	Nombre de fois où la session s'est reconnectée.

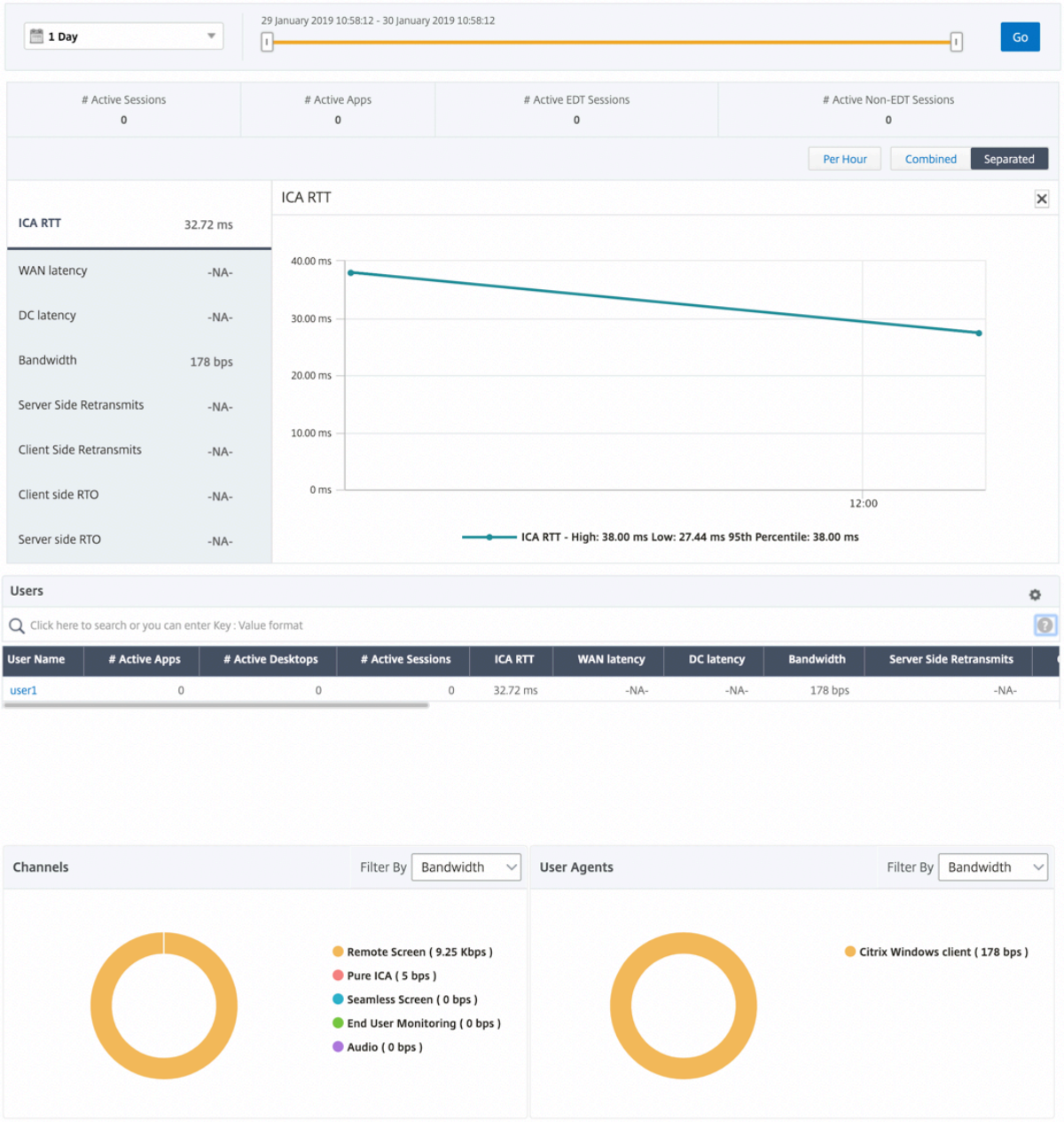
Mesures	Description
Nb d'ACR	Nombre total de fois où un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, le mode utilisateur/transparent de NetScaler Gateway.
Pays	Pays à partir duquel la session 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 NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre NetScaler 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 lors de la connexion entre NetScaler et le serveur principal.

Mesures	Description
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre NetScaler 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 NetScaler 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 lors de la connexion entre NetScaler et le serveur principal.

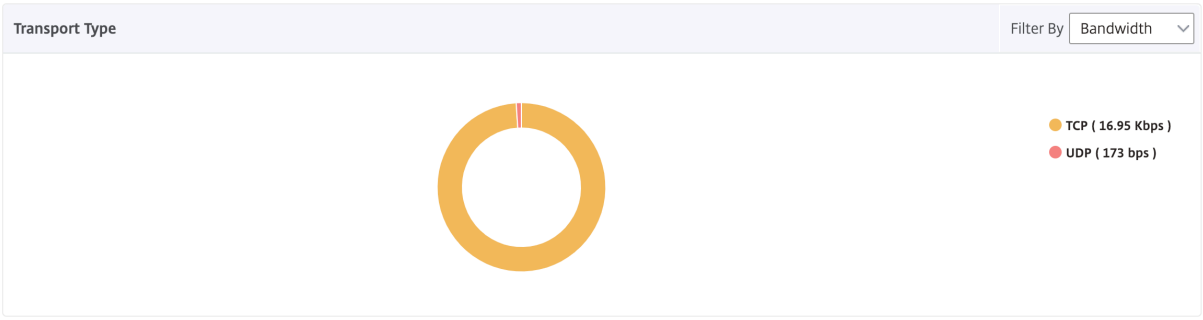
Prise en charge de l'EDT dans HDX insights

NetScaler Application Delivery Management (ADM) prend désormais en charge le transport éclairé de données (EDT) pour afficher des analyses pour HDX Insight. En d'autres termes, ADM prend désormais en charge les protocoles UDP et TCP. La prise en charge de NetScaler Gateway par EDT garantit aux utilisateurs exécutant Citrix Workspace une expérience utilisateur haute définition en cours de session sur des bureaux virtuels.

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 ».



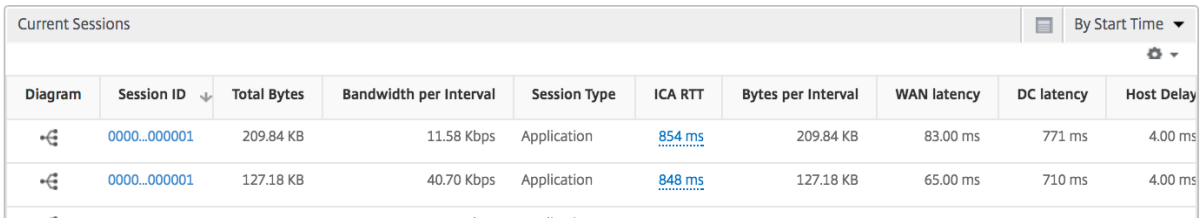
Un nouveau graphique en anneau a été introduit pour vous permettre de voir la bande passante consommée par l'utilisateur ainsi que le nombre total d'octets en fonction du type de protocole utilisé par les utilisateurs.

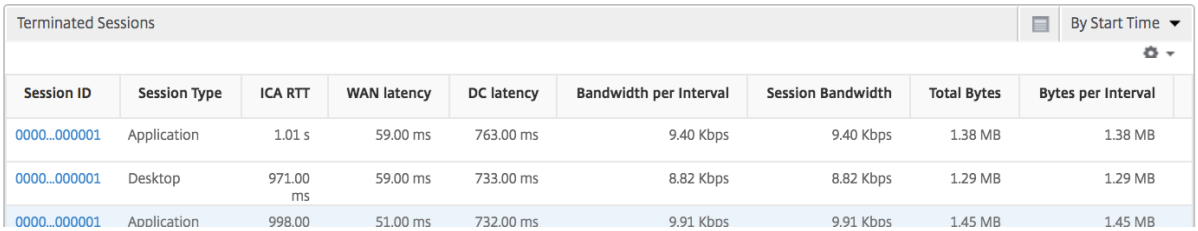


> **Remarque**
>
> L'EDT dans HDX Insight est pris en charge sur NetScaler ADM à partir de la version 12.1 build 50.28 et est disponible sur les instances ADC à partir de la version 12.1 build 49.23.

Métriques HDX Insight disponibles à partir de NetScaler ADM 12.0 et versions ultérieures :

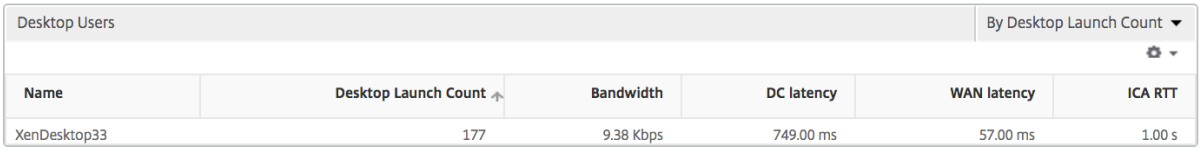
Latence côté client L7	Latence L7 moyenne observée entre le client ICA et l'instance NetScaler. Cette mesure est utile dans le cas de périphériques non Citrix présents dans le chemin de remise.
Latence côté serveur L7	Latence L7 moyenne observée entre l'appareil NetScaler et l'application virtuelle Citrix. 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.



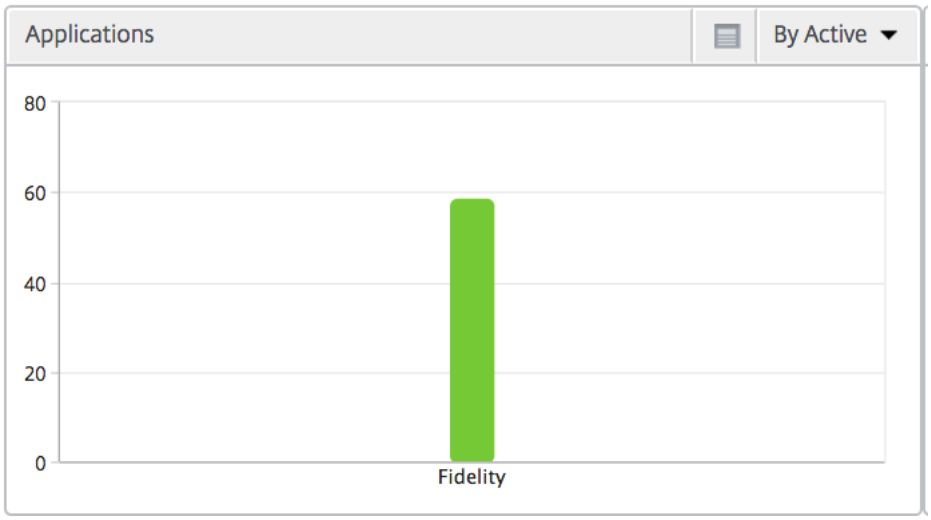


Utilisateurs de bureau Ce tableau donne un aperçu des sessions Citrix Virtual Desktop pour un utilisateur particulier. Ces mesures peuvent être triées par nombre de lancements de postes de travail et bande passante.

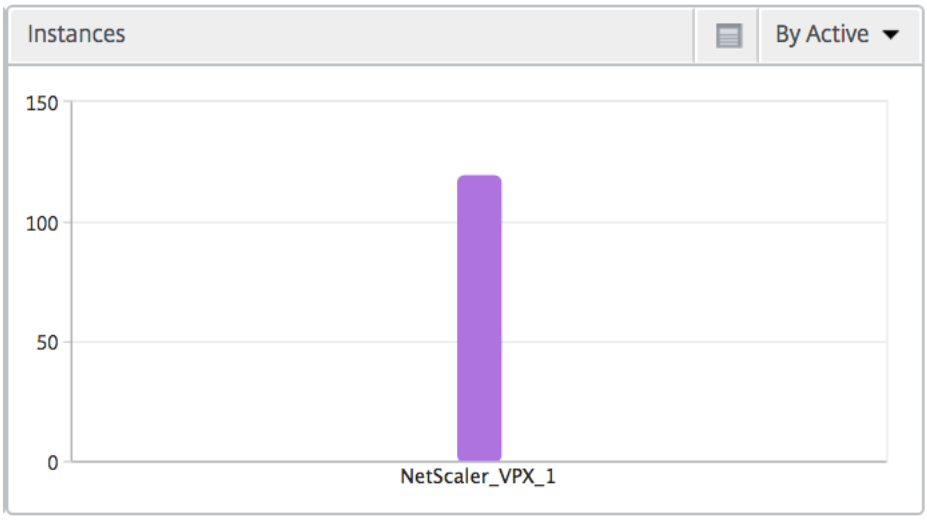
Mesures	Description
Nom	Nom du bureau virtuel Citrix.
Nombre de lancements de bureaux	Nombre de fois que l'ordinateur de bureau a été lancé.
Bande passante	Nombre total d'octets par seconde pris pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Latence DC	Latence provoquée par le côté serveur du réseau. Entre NetScaler Gateway et les serveurs VDI, CVAD ou StoreFront.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de NetScaler 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.



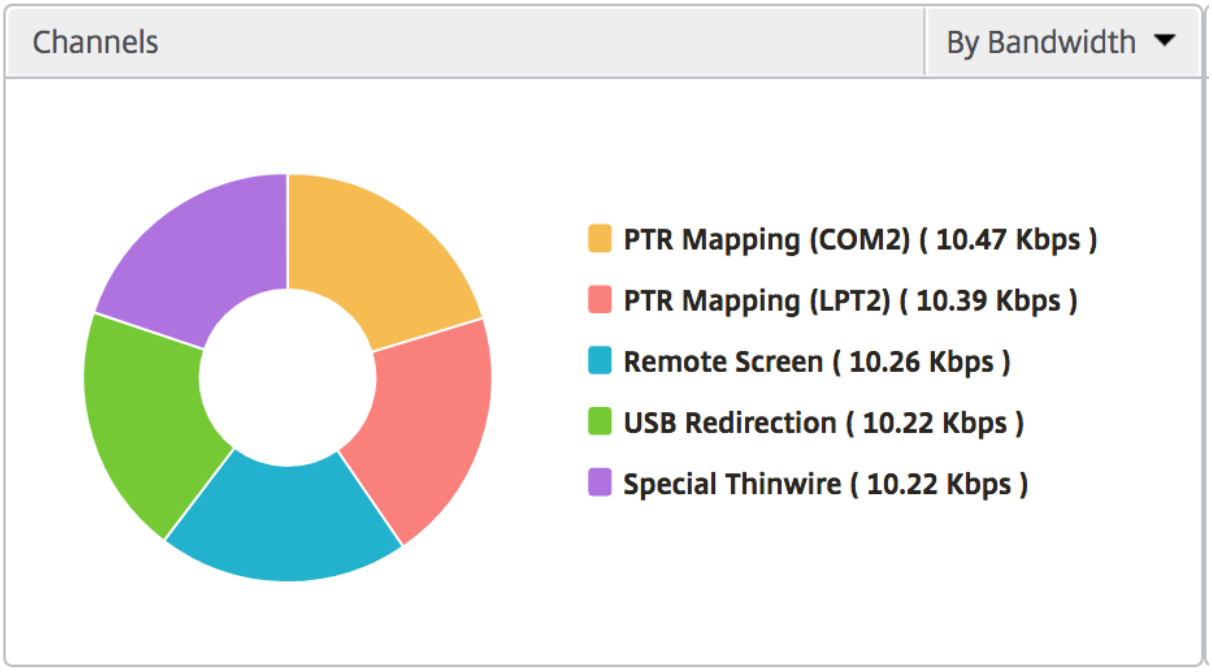
Applications Graphique à barres représentant les applications triées par Active, nombre total de lancements de session, nombre total de lancements d'applications et durée de lancement.



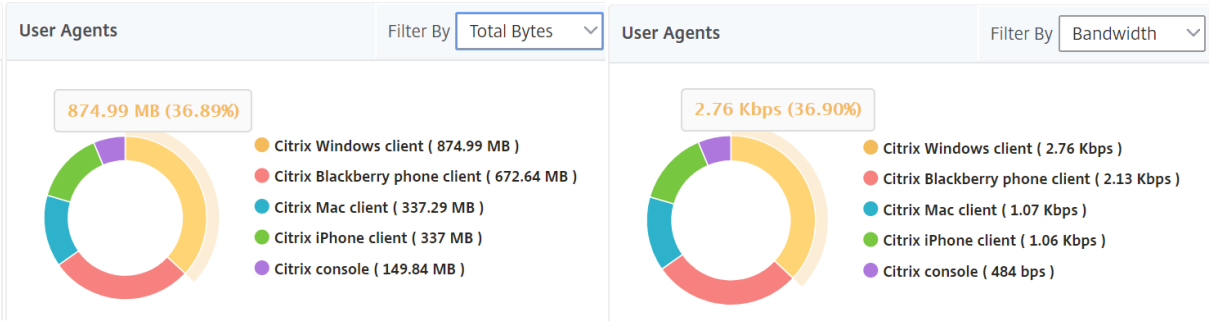
Instances Un graphique à barres représentant les instances NetScaler triées par applications actives et par nombre total d'applications



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.



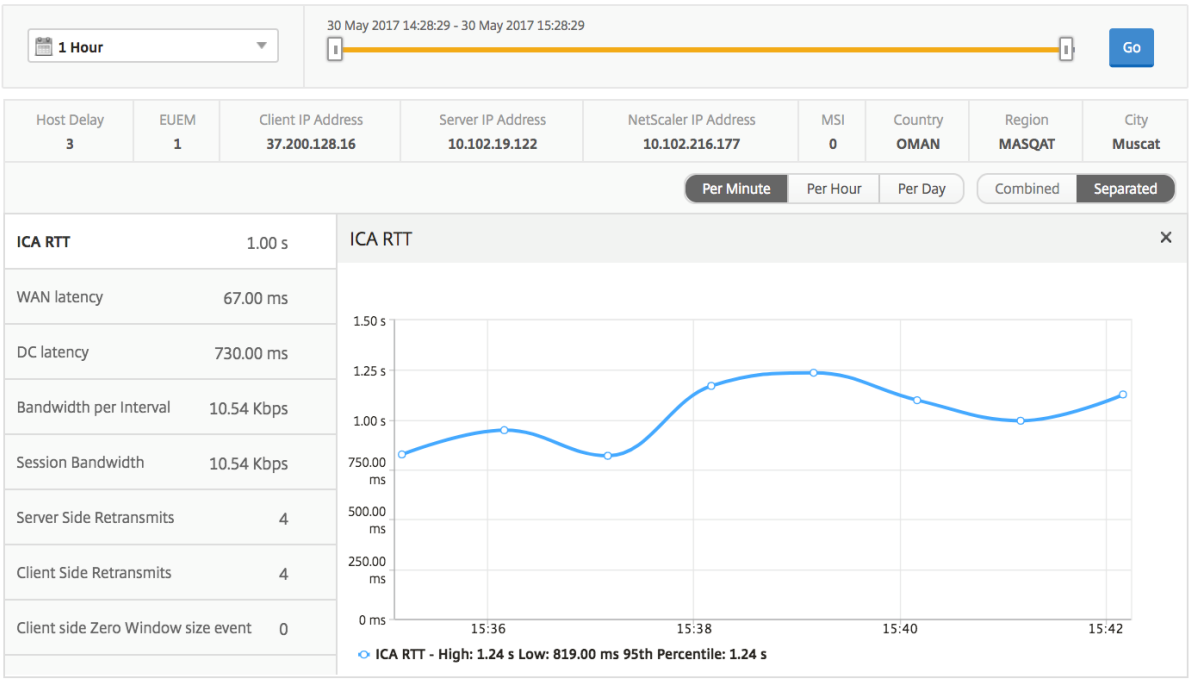
Par vue de session utilisateur La vue par session utilisateur fournit des rapports pour la session d'un utilisateur sélectionné particulier.

Pour afficher les mesures de la session d'un utilisateur sélectionné :

1. Accédez à **Gateway > 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** .

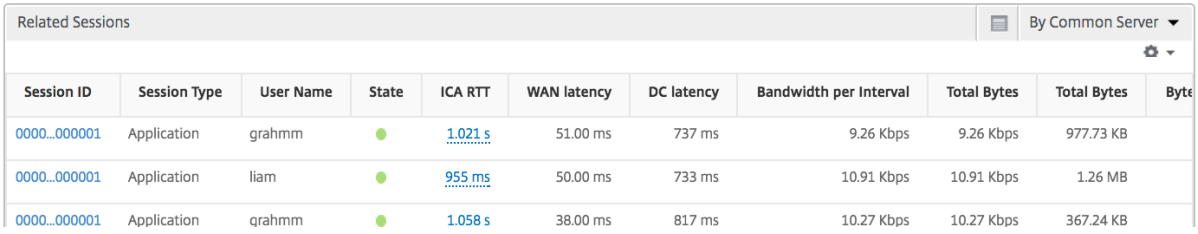
Graphique chronologique

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 NetScaler à l'utilisateur final.
Latence DC	Latence provoquée par le côté serveur du réseau. Entre NetScaler 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 lors de la connexion entre NetScaler et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre NetScaler 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 NetScaler et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre NetScaler 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.
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 en tant que serveurs communs ou NetScaler 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 **Gateway > HDX Insight > Applications** .

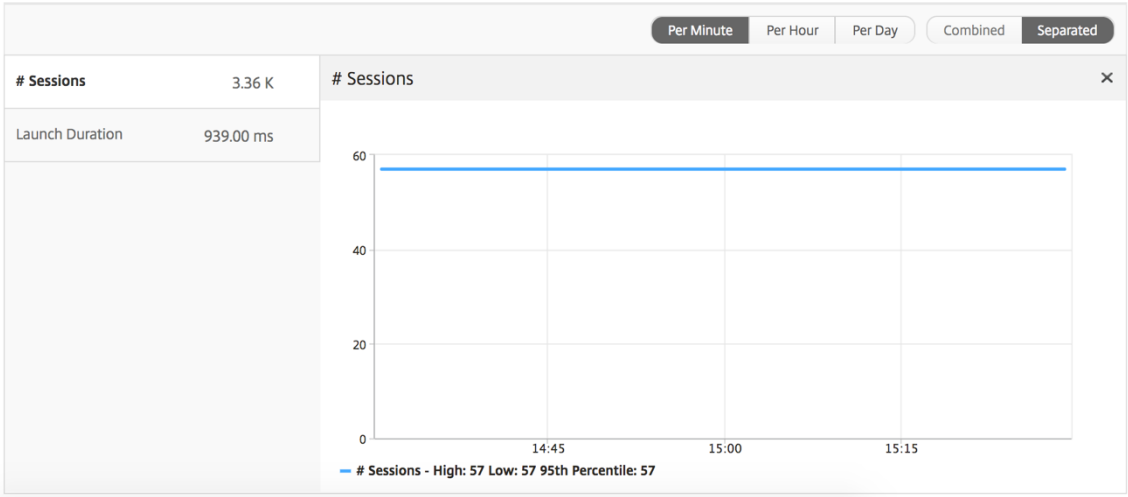
Vue récapitulative

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

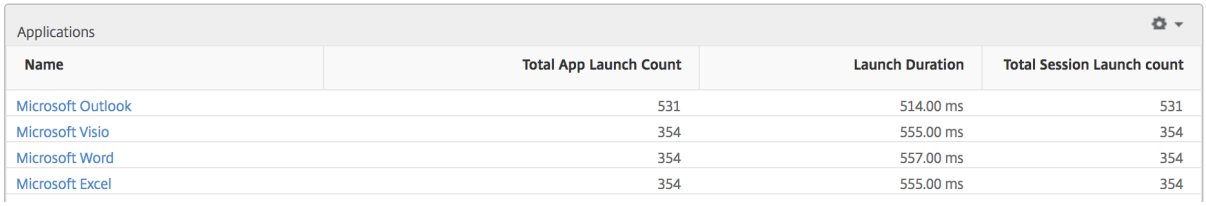
Métriques	Description
Nombre de sessions	Nombre total de séances pendant un intervalle de temps donné.
Durée du lancement	Temps moyen requis pour lancer une application.



Rapport récapitulatif des applications

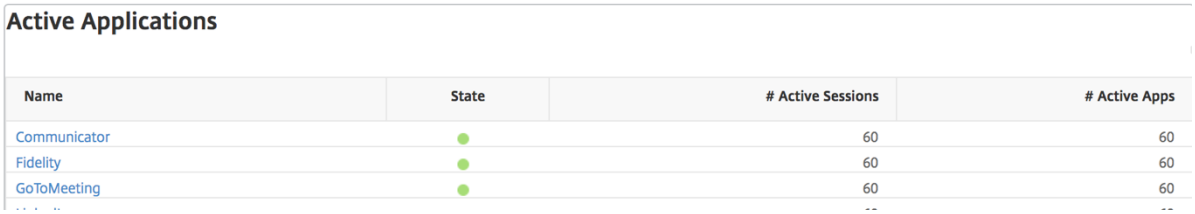
Métriques	Description
Nom	Nom de l'application virtuelle Citrix.
Nb total de sessions lancées	Nombre total de sessions Citrix Virtual App actives au cours de l'intervalle de temps donné.

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

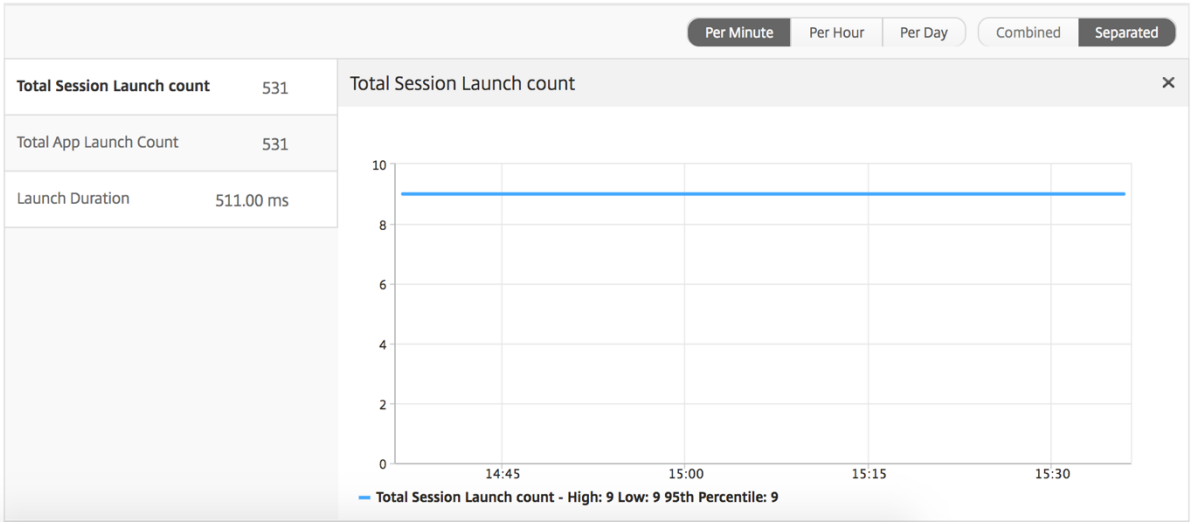
Métriques	Description
Nom	Nom de l'application virtuelle Citrix.
État	Affiche l'état de l'application : Vert-Actif, Rouge-Inactif
Nombre de sessions actives	Nombre de sessions utilisateur actives utilisant cette application pendant un intervalle de temps donné.
Nombre d'applications actives	Nombre de 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.



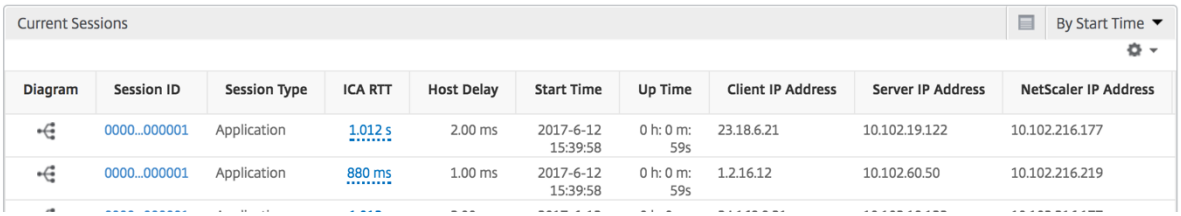
Rapport des sessions en cours

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	Retard moyen du trafic ICA passant par les NetScalers dû au 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.

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 d'espace de travail : client Windows Citrix, etc.
Version du client	Version Workspace.
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 NetScaler 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 NetScaler à l'utilisateur final.

Métriques	Description
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre NetScaler 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 lors de la connexion entre NetScaler et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre NetScaler 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 NetScaler 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 lors de la connexion entre NetScaler et le serveur principal.
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 ».

Métriques	Description
Nombre de franchissements de seuil L7	Nombre de fois qu'une violation du seuil L7 s'est produite.
Latence côté client L7	Latence L7 moyenne observée entre le client ICA et l'instance NetScaler. Cette mesure est utile dans le cas de périphériques non Citrix présents dans le chemin de remise.
Latence côté serveur L7	Latence L7 moyenne observée entre l'appareil NetScaler 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.

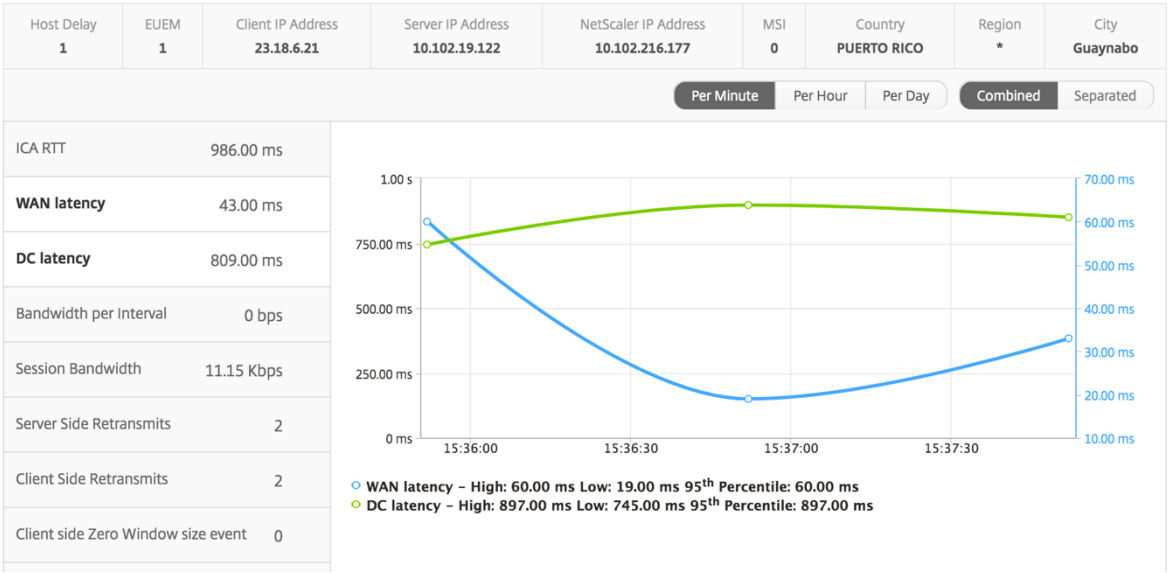
Pour afficher les rapports de session :

1. Connectez-vous à votre NetScaler ADM à l'aide d'un navigateur Web compatible.
2. Accédez à **Gateway > 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.

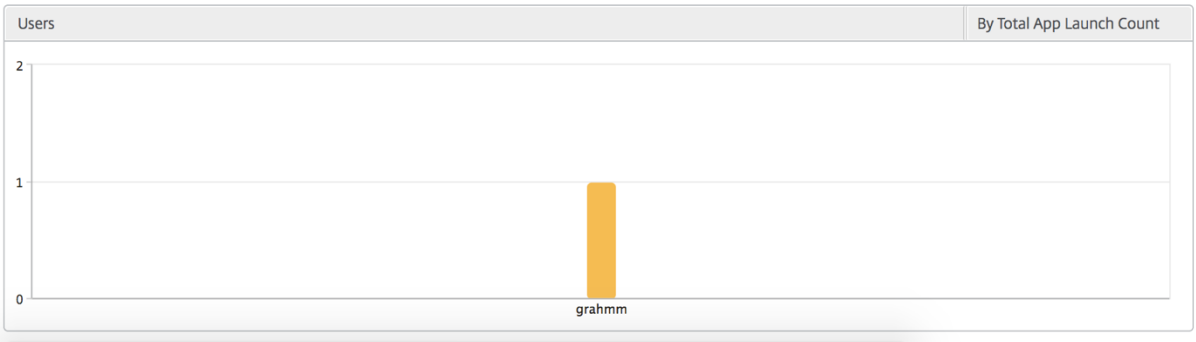
Graphique linéaire

Métriques	Description
Reconnexions de session	Nombre de fois où la session s'est reconnectée.

Métriques	Description
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 NetScaler 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 NetScaler aux serveurs principaux.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Retransmissions côté serveur	Nombre de paquets retransmis lors de la connexion entre NetScaler et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre NetScaler 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 NetScaler et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre NetScaler 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.



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 NetScaler ADM à l'aide d'un navigateur Web compatible.
2. Accédez à **Gateway > HDX Insight > Desktop** .

Vue récapitulative

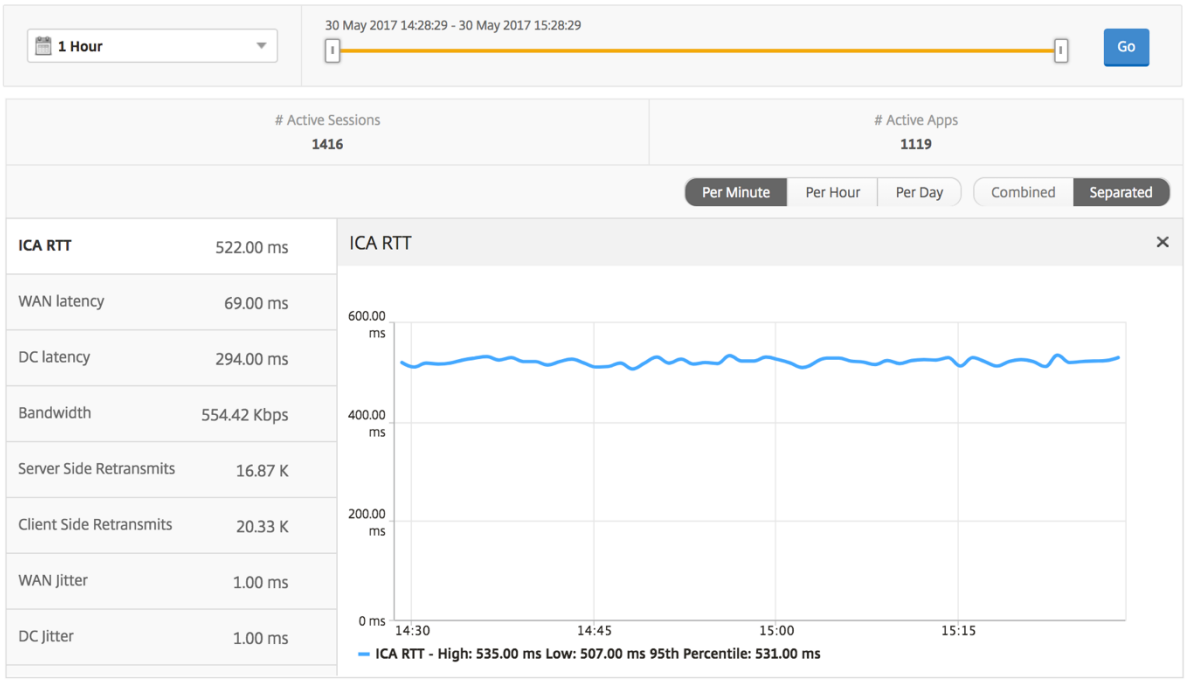
La vue récapitulative affiche les rapports de tous les Citrix Virtual Desktops qui sont connectés au cours de la chronologie sélectionnée.

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 NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre NetScaler 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 lors de la connexion entre NetScaler et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre NetScaler 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 NetScaler et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre NetScaler et le serveur principal.

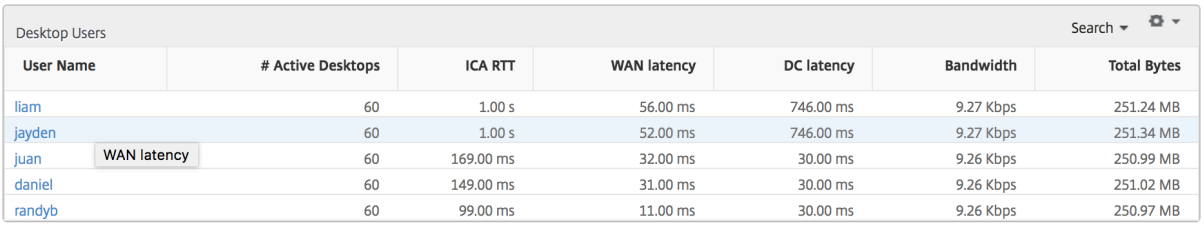
Métriques	Description
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.



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 NetScaler à l'utilisateur final.

Métriques	Description
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre NetScaler 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.
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

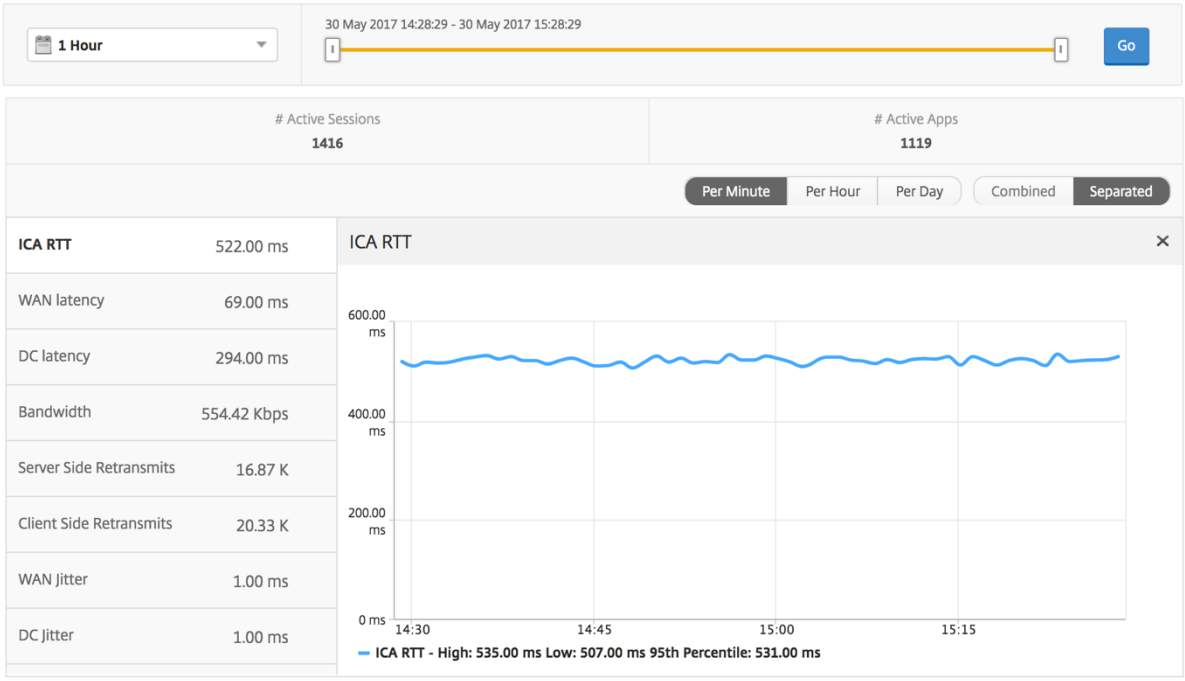
La vue par poste de travail fournit des rapports détaillés sur l'expérience utilisateur pour un Citrix Virtual Desktop sélectionné.

Pour accéder à la vue Bureau spécifique :

1. Connectez-vous à votre NetScaler ADM à l'aide d'un navigateur Web compatible.
2. Accédez à **Analytics > HDX Insight > Bureau**.
3. Sélectionnez un **poste de travail** particulier dans le **rapport récapitulatif des ordinateurs de bureau**.

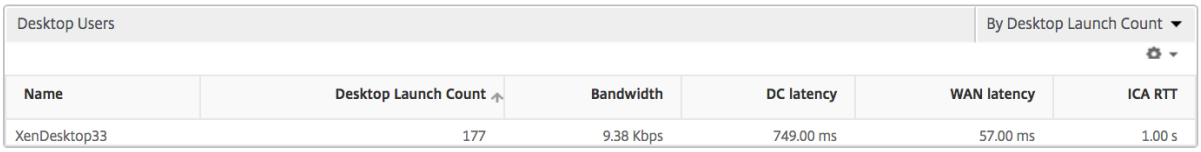
Graphique linéaire

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.
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 NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre NetScaler 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 lors de la connexion entre NetScaler et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre NetScaler 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 NetScaler et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre NetScaler 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 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 NetScaler Gateway et les serveurs VDI, CVAD ou StoreFront.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de NetScaler 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.

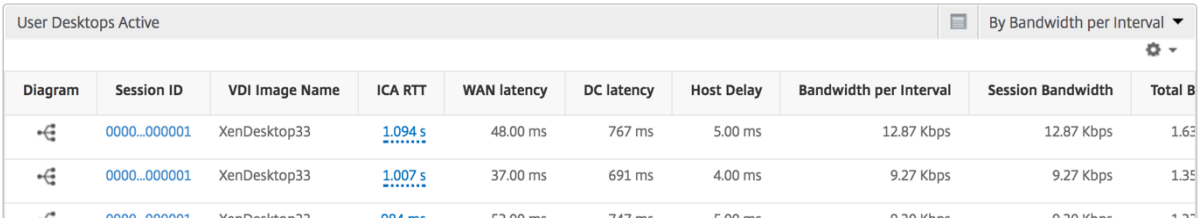


Rapport Actif/Inactif des postes de travail utilisateur Les mesures suivantes peuvent être triées en fonction de la bande passante par intervalle, des reconnexions de session et du nombre d'ACR.

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	Retard moyen du trafic ICA passant par les NetScalers dû au 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 d'espace de travail : client Windows Citrix, etc.
Version du client	Version Workspace.
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 NetScaler 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 NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre NetScaler 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 lors de la connexion entre NetScaler et le serveur principal.

Mesures	Description
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre NetScaler 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 NetScaler 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 lors de la connexion entre NetScaler et le serveur principal.
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 NetScaler ADM à l'aide d'un navigateur Web compatible.
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.

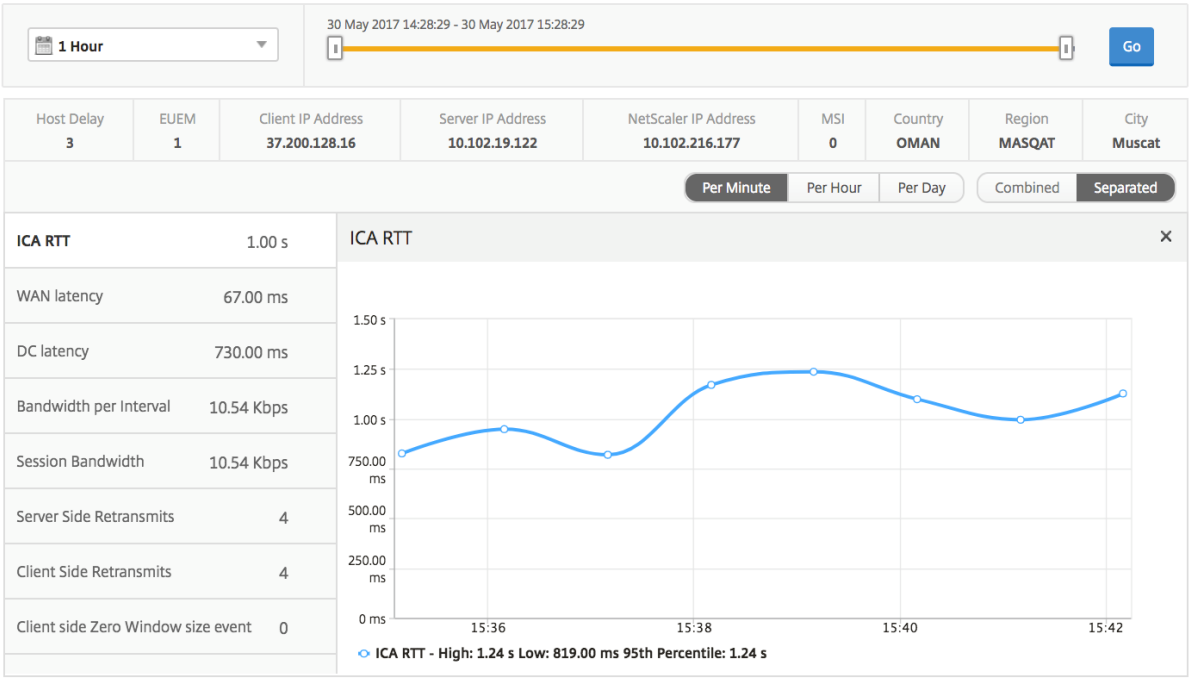
Graphique chronologique La vue par session utilisateur fournit des rapports pour la session d'un utilisateur sélectionné particulier.

Pour afficher les mesures de la session d'un utilisateur sélectionné :

1. Connectez-vous à votre NetScaler ADM à l'aide d'un navigateur Web compatible.
2. Accédez à **Gateway > 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 NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre NetScaler 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 lors de la connexion entre NetScaler et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre NetScaler 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 NetScaler et l'utilisateur final.

Mesures	Description
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre NetScaler 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.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.

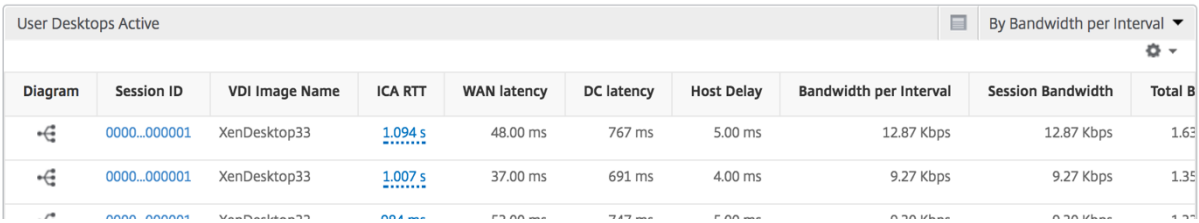


Rapport sur les sessions de bureau associées Les mesures suivantes peuvent être triées en fonction de la bande passante par intervalle, des reconnexions de session et du nombre d'ACR.

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.

Mesures	Description
Délai d'hôte	Retard moyen du trafic ICA passant par les NetScalers dû au 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 d'espace de travail : client Windows Citrix, etc.
Version du client	Version Workspace.
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 NetScaler 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.

Mesures	Description
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 NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre NetScaler 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 lors de la connexion entre NetScaler et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre NetScaler 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 NetScaler 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 lors de la connexion entre NetScaler et le serveur principal.



Rapports et mesures de vue d'instance

Les rapports et les métriques de la vue des instances se concentrent sur les instances NetScaler.

Pour accéder à la vue Instance :

1. Connectez-vous à votre NetScaler ADM à l'aide d'un navigateur Web compatible.
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

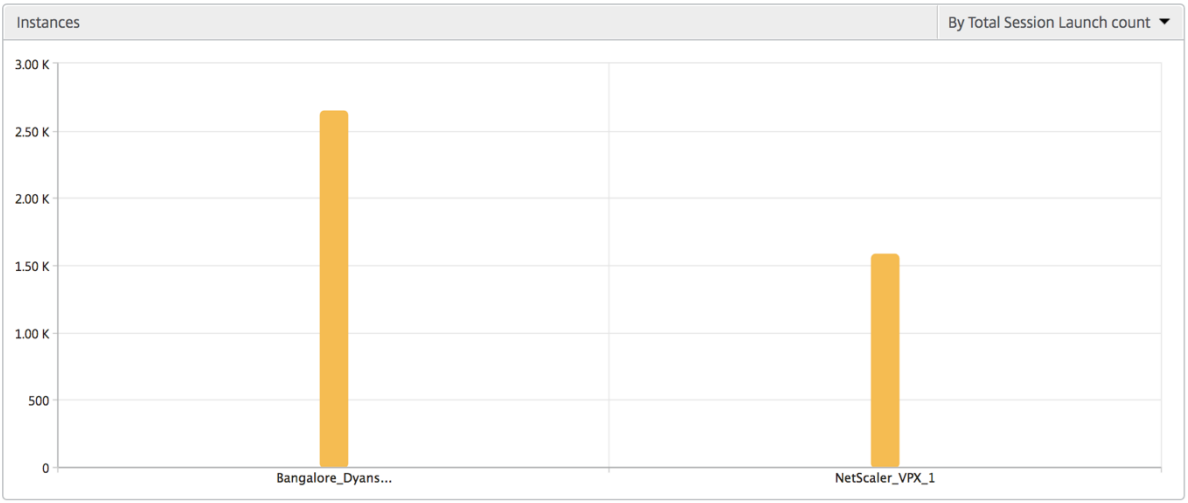
Vue récapitulative de l'instance

Cette vue est appelée vue récapitulative car elle affiche les rapports de toutes les instances NetScaler ajoutées à NetScaler ADM.

Toutes les métriques/rapports ci-dessous, sauf mention explicite, auront les valeurs qui leur correspondent pour la période sélectionnée.

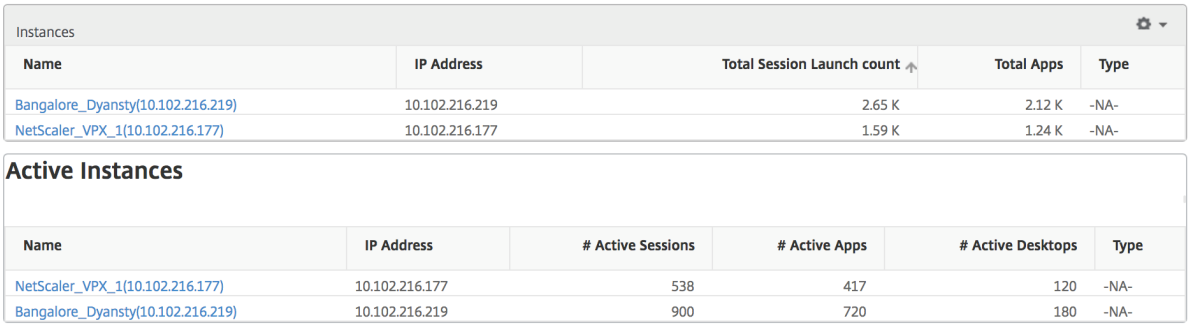
Graphique à barres d'instance

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 NetScaler.
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.

Flux ignorés Un flux ignoré est un enregistrement qui a ignoré l'analyse de la connexion ICA. Cela peut être dû à 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 d'un espace de travail ou d'un type d'espace de travail, etc. Ce tableau indique l'adresse IP et le nombre de flux ignorés. Ces espaces de travail ne font peut-être pas partie des espaces de travail sur liste blanche. Par conséquent, ces sessions sont ignorées de la surveillance.

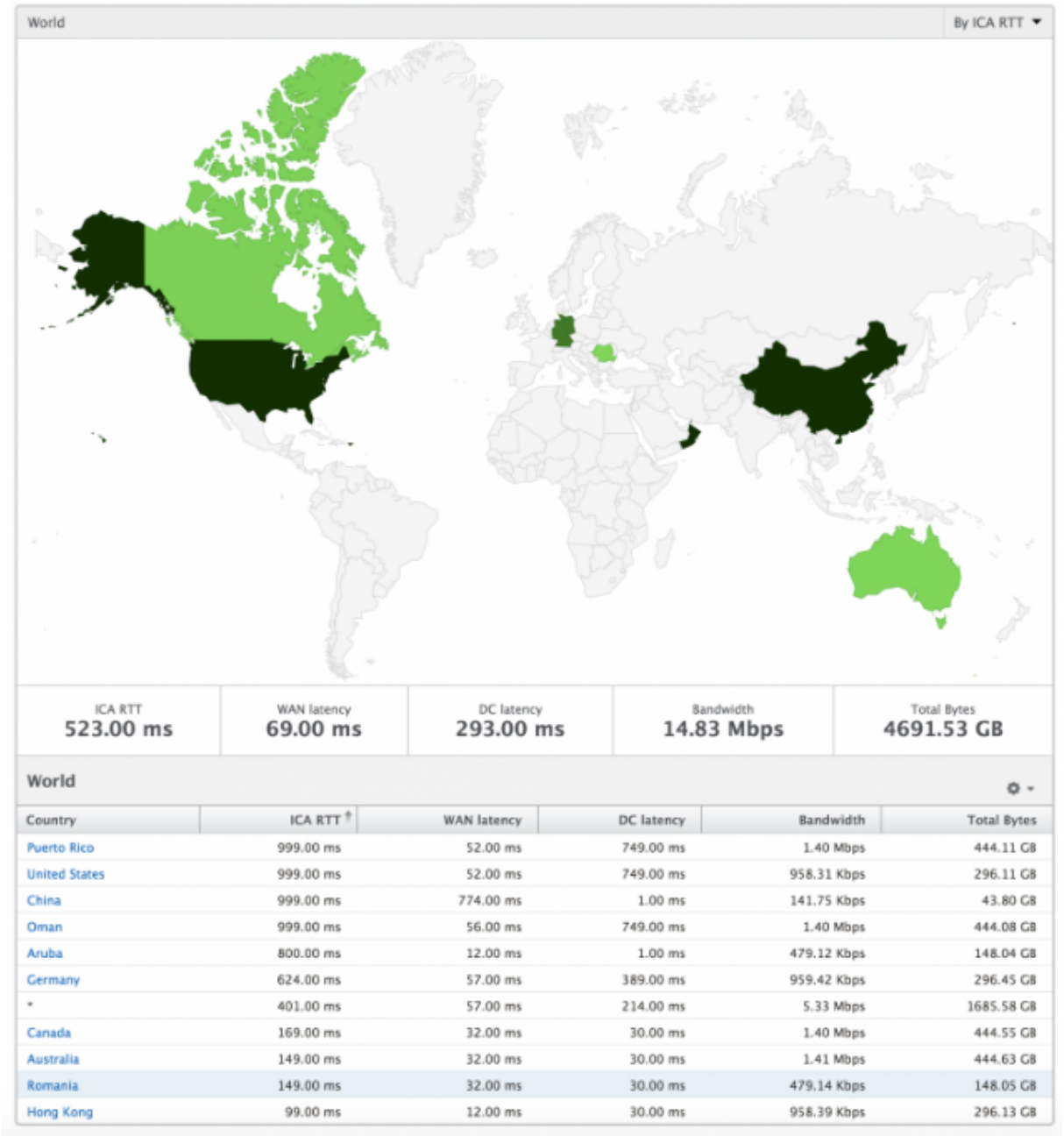

Skipped Flows

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 simplement sur la région. Les administrateurs peuvent approfondir l'exploration vers le bas pour afficher les informations par ville et par État. À partir des versions 12.0 et ultérieures de NetScaler ADM, vous pouvez accéder aux 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 de l'utilisateur final pour une instance NetScaler sélectionnée en particulier.

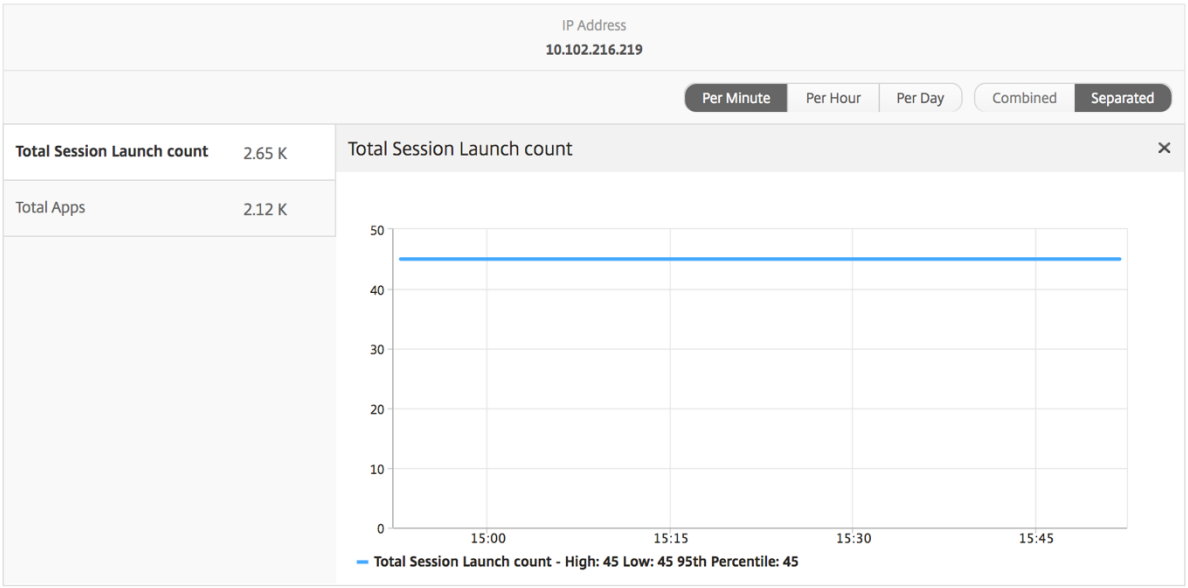
Pour accéder à la vue d'instance :

1. Connectez-vous à votre NetScaler ADM à l'aide d'un navigateur Web compatible.
2. Accédez à **Analytics > HDX Insight > Instances**.

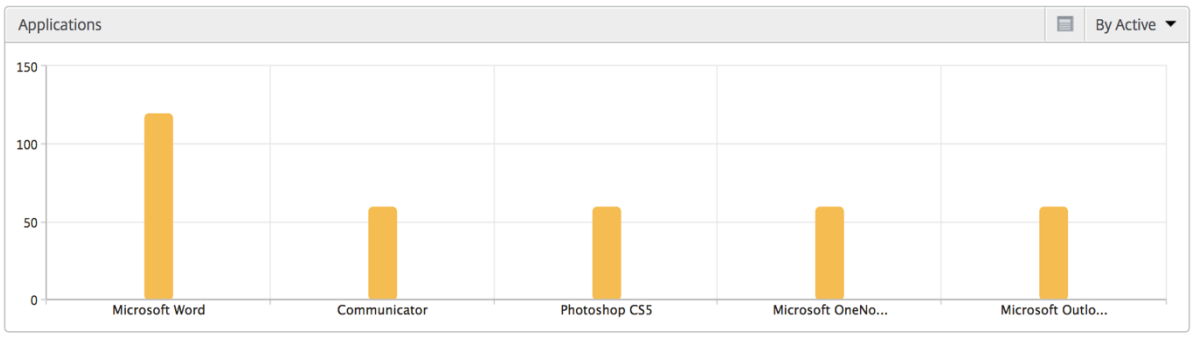
3. Sélectionnez une instance particulière dans le **rapport de synthèse des instances**.

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.

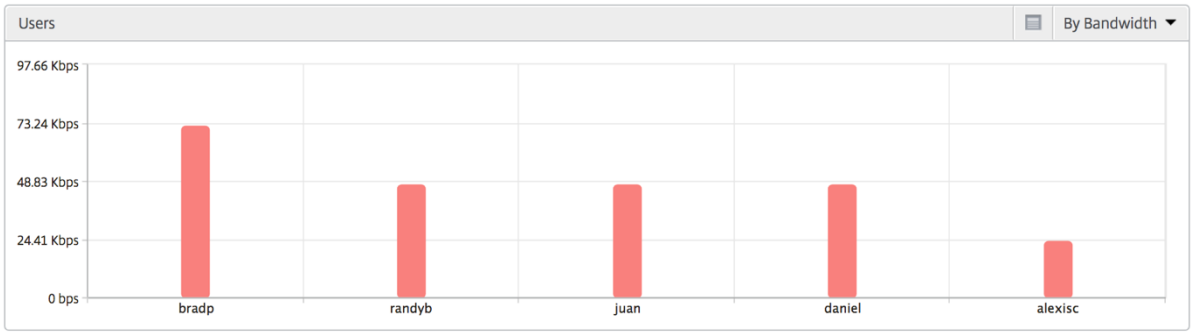


Graphique à barres des applications Affiche les 5 premières applications en fonction des critères suivants : applications actives, nombre total de lancements de session, nombre total de lancements d'applications ou durée de lancement.



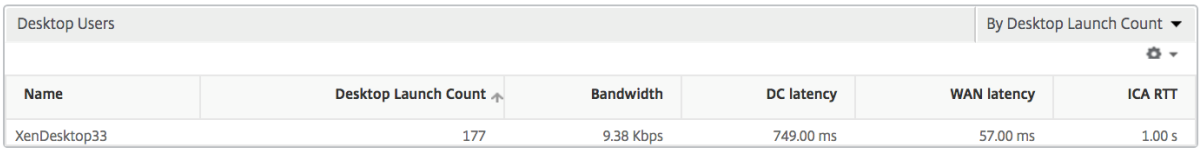
Graphique à barres des utilisateurs Le graphique à barres Utilisateurs affiche les 5 premiers utilisateurs selon les critères suivants

- 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.

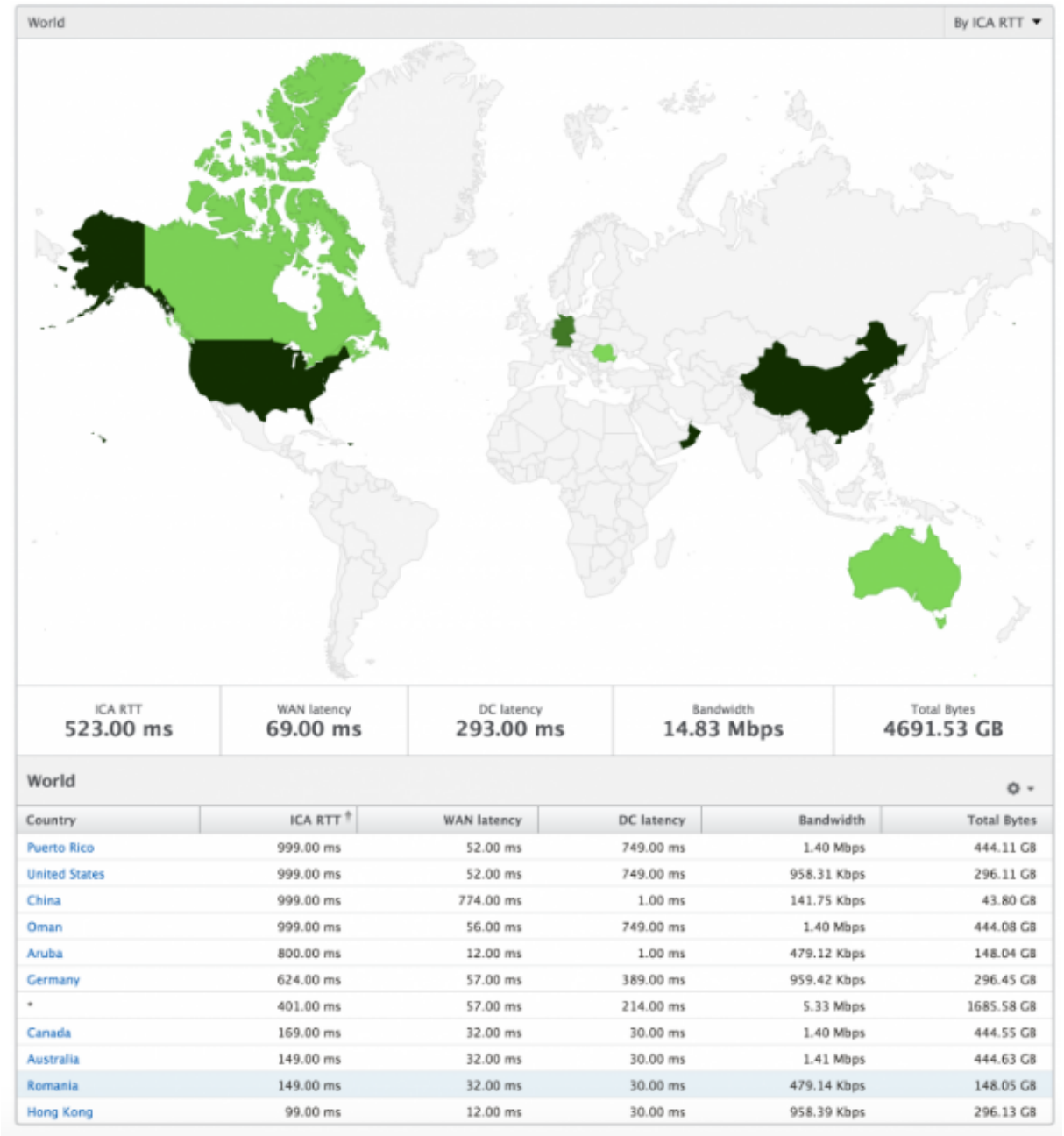
Mesures	Description
Nom	Nom du bureau virtuel Citrix.
Nombre de lancements de bureaux	Nombre de fois que l'ordinateur de bureau a été lancé.
Bande passante	Nombre total d'octets par seconde pris pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre NetScaler Gateway et les serveurs VDI, CVAD ou StoreFront.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de NetScaler 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 des versions 12.0 et ultérieures de NetScaler ADM, vous pouvez accéder aux utilisateurs connectés depuis 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

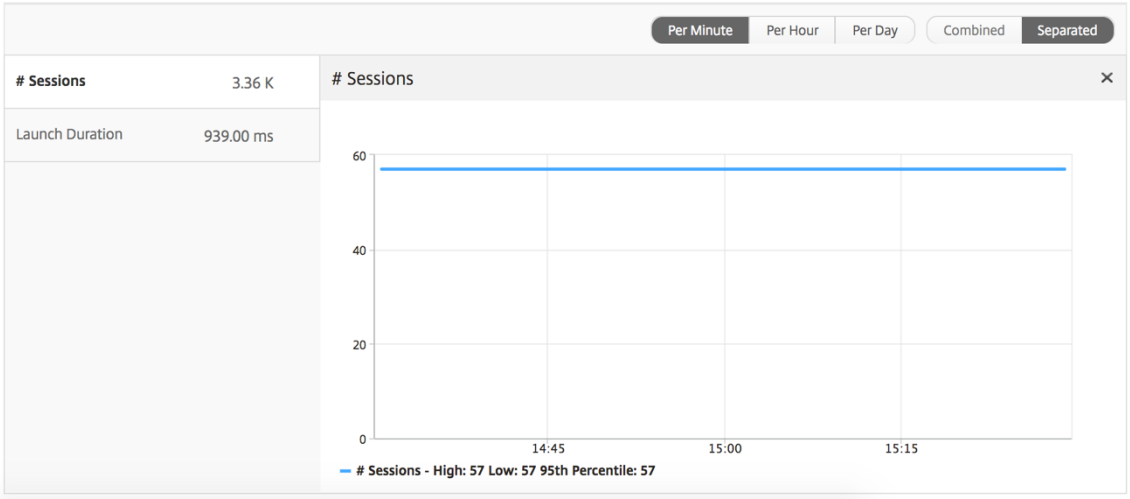
La vue des licences fournit des détails sur les informations de licence NetScaler Gateway.

Pour accéder à la vue Licence :

1. Connectez-vous à votre NetScaler ADM à l'aide d'un navigateur Web compatible.
2. Accédez à **Analytics > HDX Insight > Licences**.

Graphique linéaire

Métriques	Description
Licences utilisées	Les licences CCU NetScaler 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 NetScaler Gateway CCU que le client peut utiliser.



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 **Gateway > HDX Insight > Applications** .

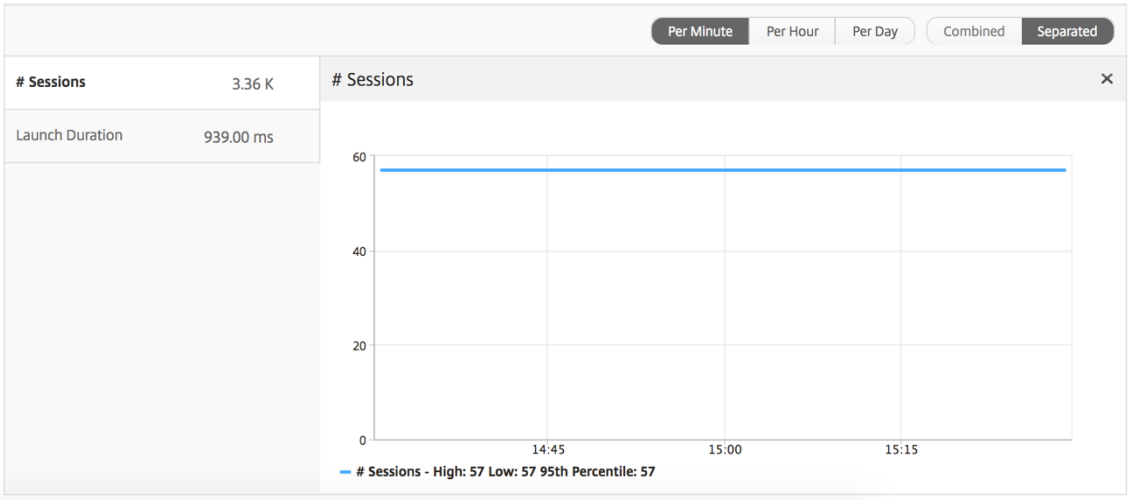
Vue récapitulative

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

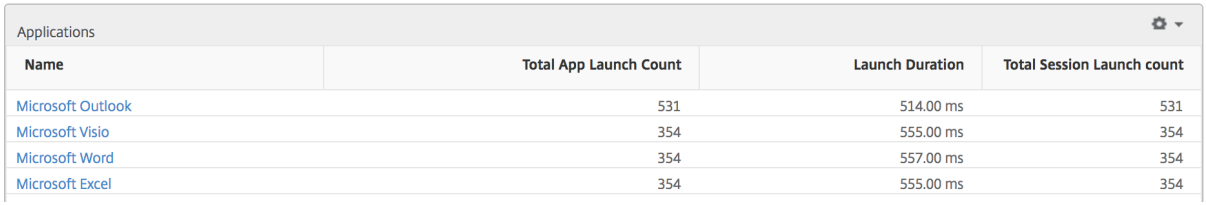
Métriques	Description
Nombre de sessions	Nombre total de séances pendant un intervalle de temps donné.
Durée du lancement	Temps moyen requis pour lancer une application.



Rapport récapitulatif des applications

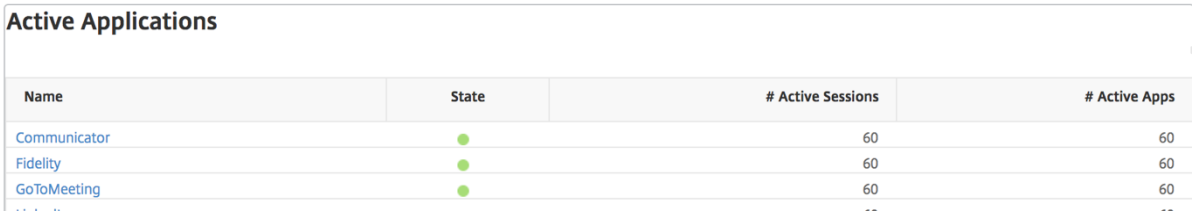
Métriques	Description
Nom	Nom de l'application virtuelle Citrix.
Nb total de sessions lancées	Nombre total de sessions Citrix Virtual App actives au cours de l'intervalle de temps donné.
Nb total d'applications lancées	Nombre total d'applications Citrix Virtual App lancées au cours de l'intervalle de 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.

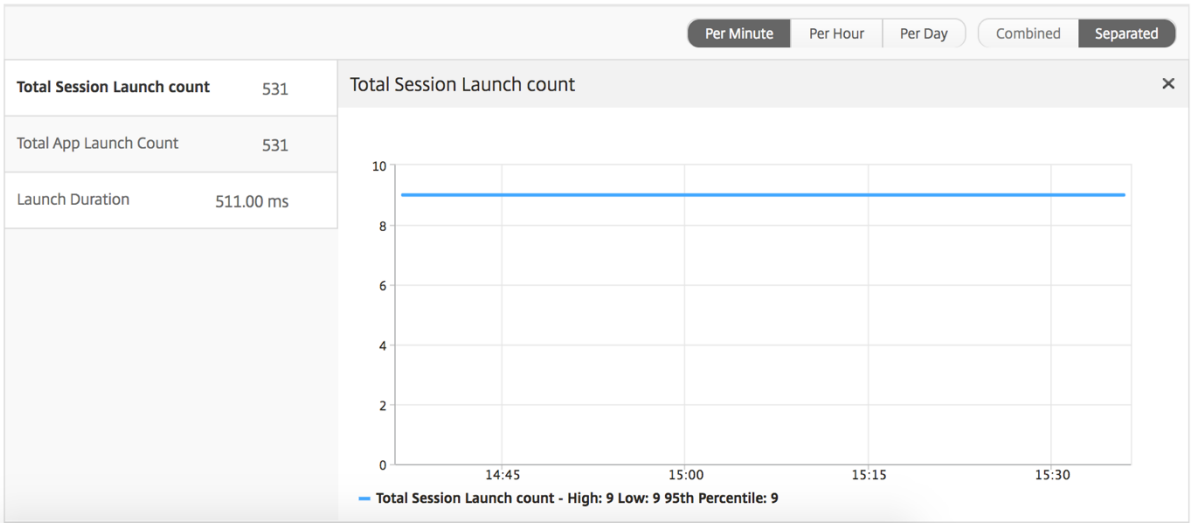


Rapport sur les seuils

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.



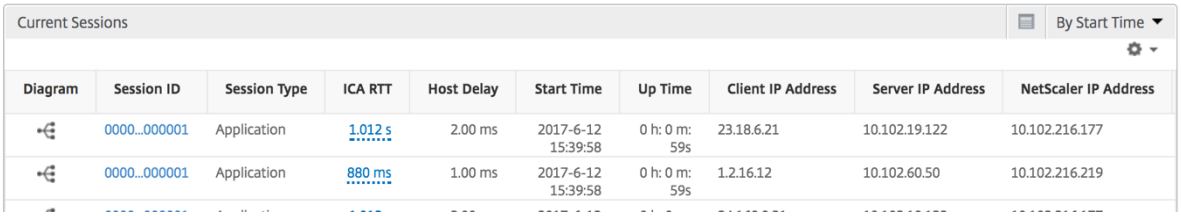
Rapport des sessions en cours

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	Retard moyen du trafic ICA passant par les NetScalers dû au 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.

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 d'espace de travail : client Windows Citrix, etc.
Version du client	Version Workspace.
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 NetScaler 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 NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire de NetScaler 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 lors de la connexion entre NetScaler et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre NetScaler 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 NetScaler 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 lors de la connexion entre NetScaler et le serveur principal.
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	Latence L7 moyenne observée entre le client ICA et l'instance NetScaler. Cette mesure est utile pour les périphériques non Citrix présents dans le chemin de remise.
Latence côté serveur L7	Latence L7 moyenne observée entre l'appareil NetScaler 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

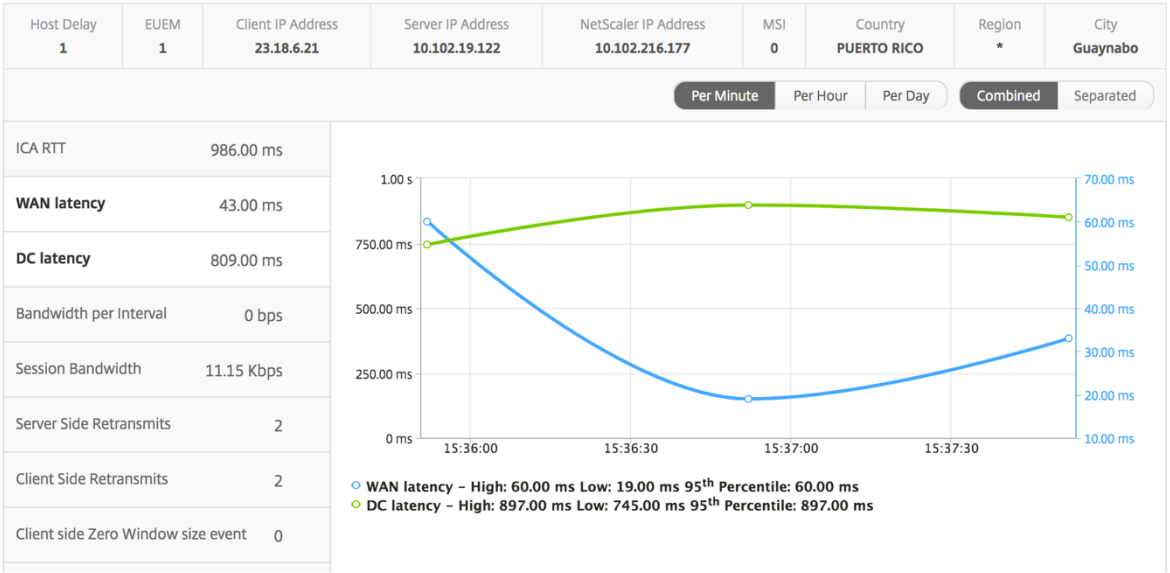
L'affichage par session d'application affiche les rapports pour une session d'application sélectionnée particulière.

Pour afficher les rapports de session :

1. Accédez à **Gateway > 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.

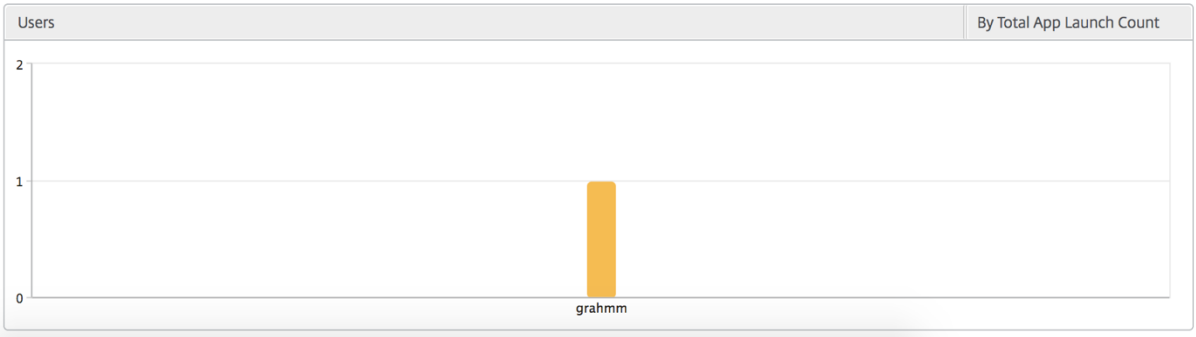
Graphique linéaire

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 NetScaler 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 NetScaler aux serveurs principaux.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Retransmissions côté serveur	Nombre de paquets retransmis lors de la connexion entre NetScaler et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre NetScaler 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 NetScaler et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre NetScaler 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.



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 **Gateway > HDX Insight > Desktop** .

Vue récapitulative

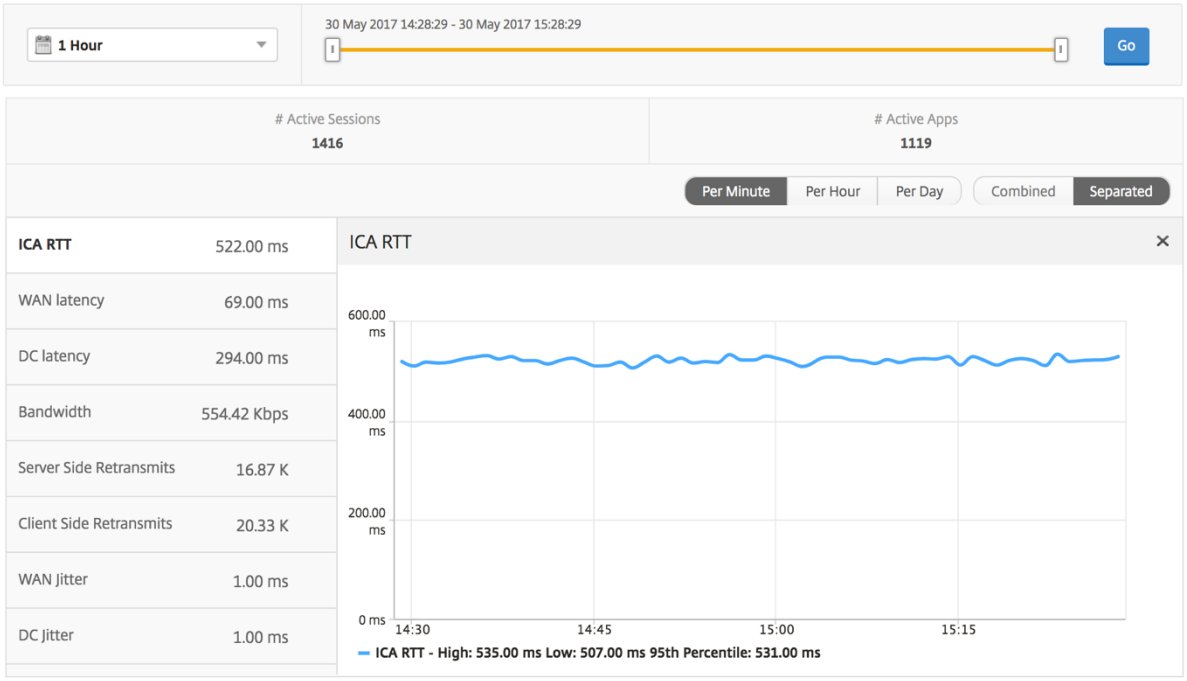
La vue récapitulative affiche les rapports de tous les Citrix Virtual Desktops qui sont connectés au cours de la chronologie sélectionnée.

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 NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire de NetScaler 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 lors de la connexion entre NetScaler et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre NetScaler 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 NetScaler et l'utilisateur final.

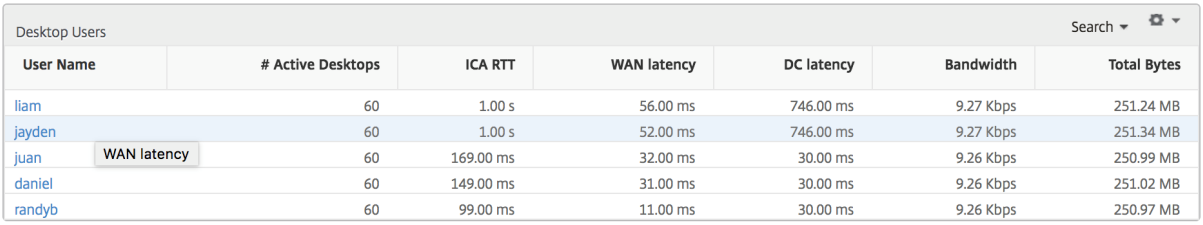
Métriques	Description
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre NetScaler et le serveur principal.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.
Événement 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 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 NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire de NetScaler 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.
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

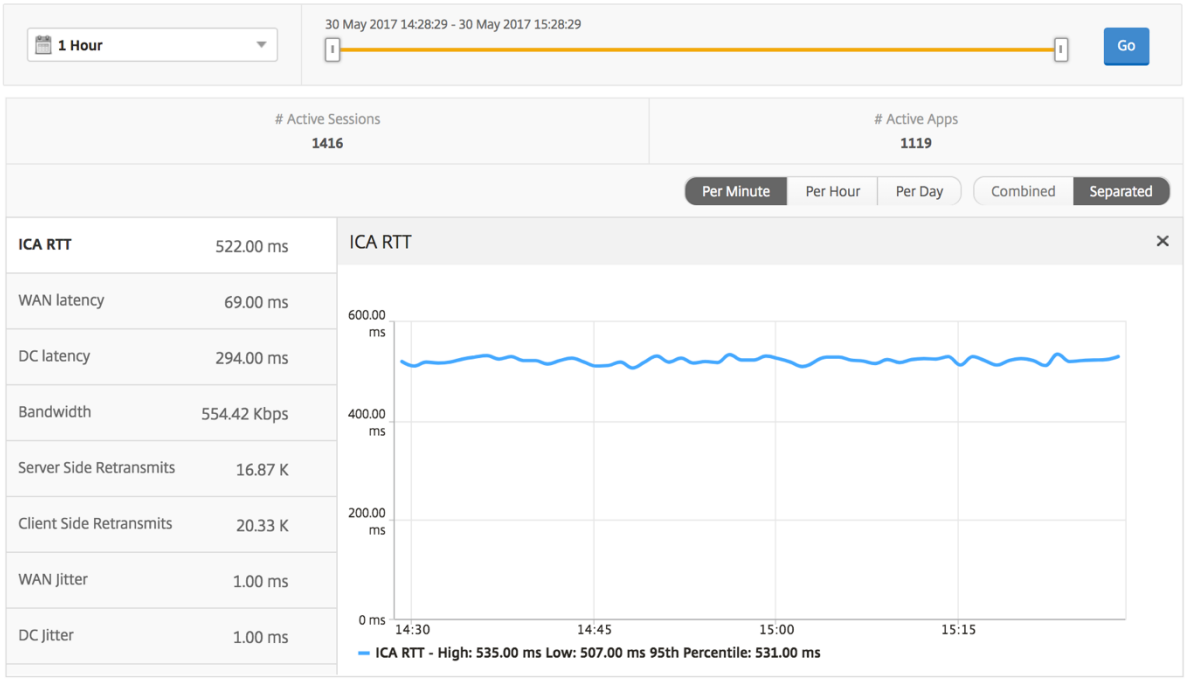
La vue par poste de travail fournit des rapports détaillés sur l'expérience utilisateur pour un Citrix Virtual Desktop sélectionné.

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

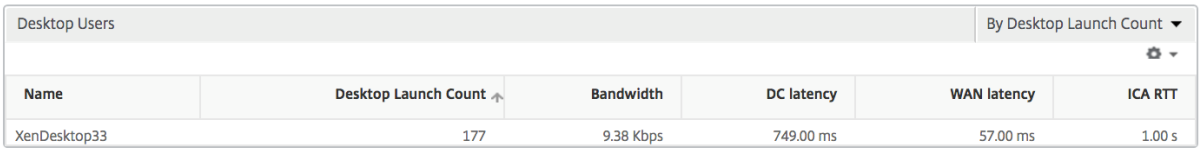
Métriques	Description
Nombre de sessions actives	Ce nombre indique le nombre de sessions Citrix Virtual Apps and Desktops actives.
Nbre d'applications actives	Ce nombre indique le nombre de sessions actives de Citrix Virtual App.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors 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 NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire de NetScaler 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 lors de la connexion entre NetScaler et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre NetScaler 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 NetScaler et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre NetScaler 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 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 NetScaler aux serveurs principaux.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de NetScaler 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.



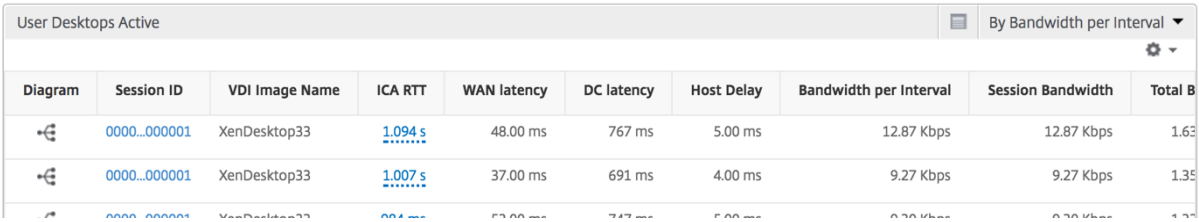
Rapport actif/inactif sur les postes de travail utilisateur

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	Retard moyen du trafic ICA passant par les NetScaler ADC dû au 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 d'espace de travail : client Windows Citrix, etc.
Version du client	Version Workspace.
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 NetScaler 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 NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire de NetScaler 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 lors de la connexion entre NetScaler et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre NetScaler 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 NetScaler 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 lors de la connexion entre NetScaler et le serveur principal.
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 **Gateway > HDX Insight > Desktop** .
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

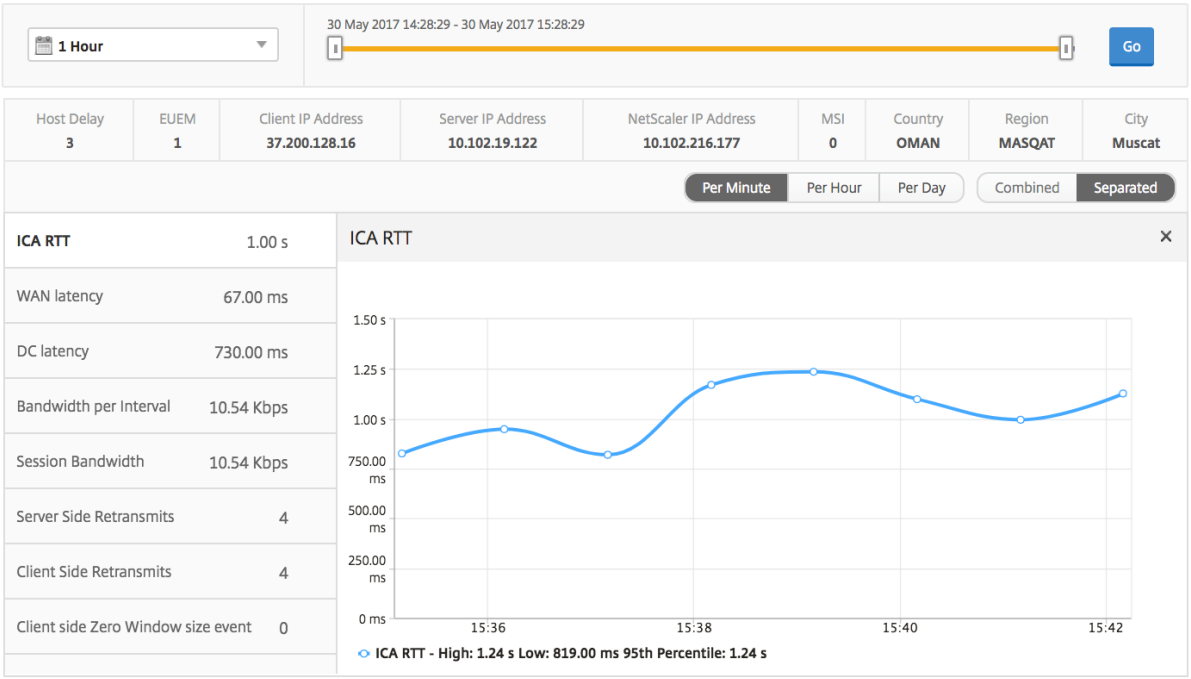
La vue par session utilisateur fournit des rapports pour la session d'un utilisateur sélectionné particulier.

Pour afficher les mesures de la session d'un utilisateur sélectionné :

1. Accédez à **Gateway > 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 NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire de NetScaler 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 lors de la connexion entre NetScaler et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre NetScaler 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 NetScaler et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre NetScaler et le serveur principal.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.

Mesures	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.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.



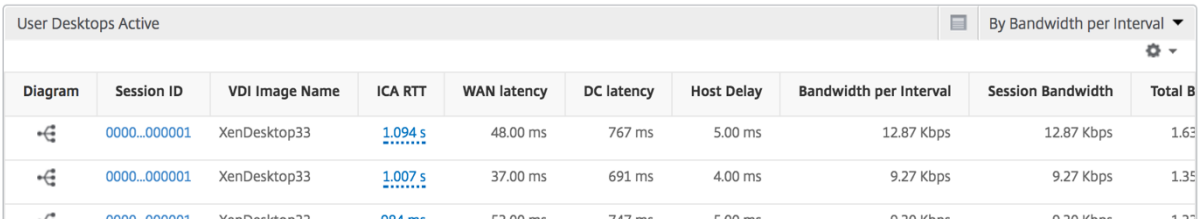
Rapport sur les sessions de bureau associées

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	Retard moyen du trafic ICA passant par les NetScalers dû au réseau de serveurs.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.

Mesures	Description
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.
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, le mode utilisateur/transparent de NetScaler 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.

Mesures	Description
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 NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire de NetScaler 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 lors de la connexion entre NetScaler et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre NetScaler 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 NetScaler 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 lors de la connexion entre NetScaler et le serveur principal.
Nom de l'image VDI	Nom du Citrix Virtual Desktops auquel l'utilisateur est connecté



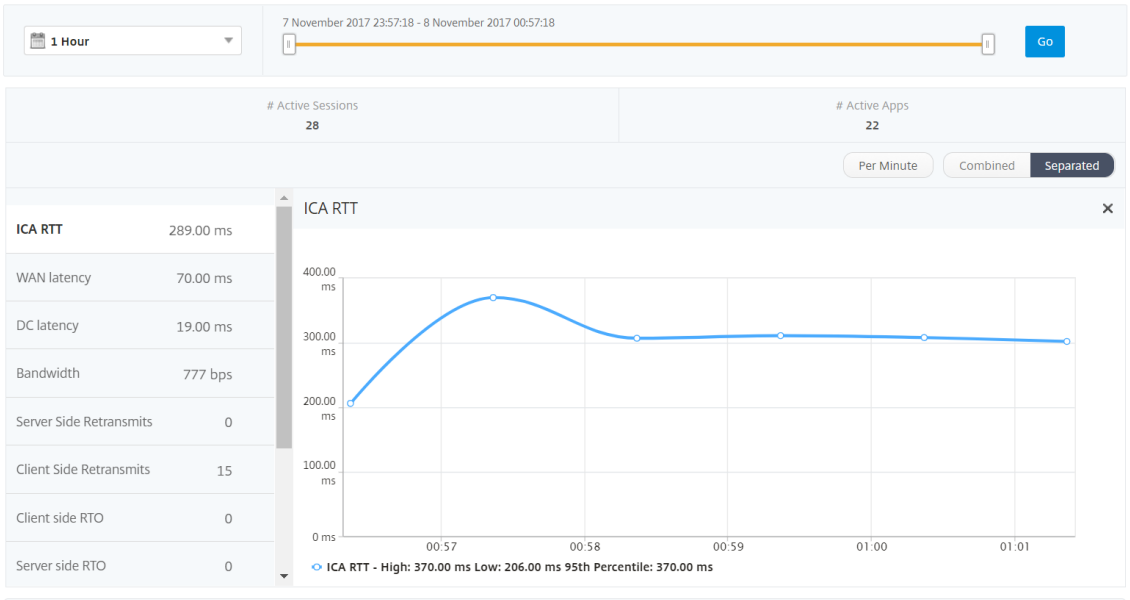
Afficher les rapports et les mesures de l'utilisateur

February 1, 2024

Les rapports et les mesures de cette vue sont affichés par les utilisateurs Citrix Virtual Apps et Desktop.

Pour accéder à la vue Utilisateurs :

1. Accédez à **Gateway > 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 :

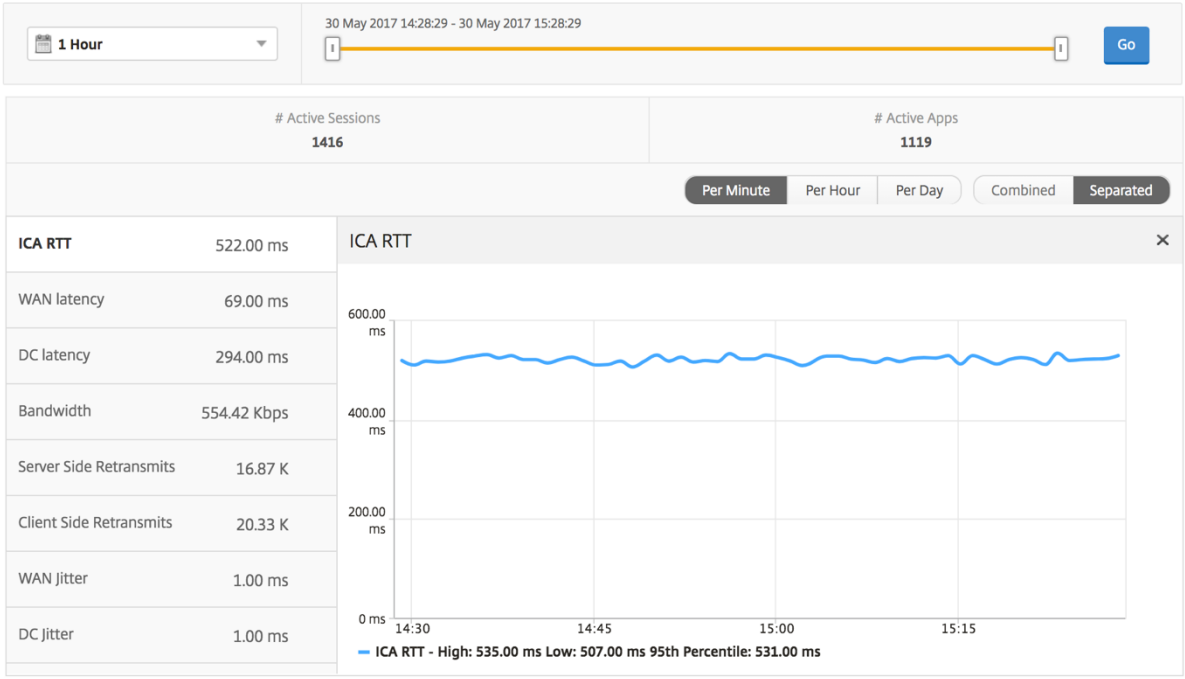
1. Utilisez la liste de périodes ou le curseur temporel pour définir l'intervalle de temps souhaité.

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 NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire de NetScaler 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 lors de la connexion entre NetScaler et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre NetScaler 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 NetScaler et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre NetScaler 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.

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 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 NetScaler à l'utilisateur final.

Mesures	Description
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire de NetScaler 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 lors de la connexion entre NetScaler et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre NetScaler 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 NetScaler et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre NetScaler 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.

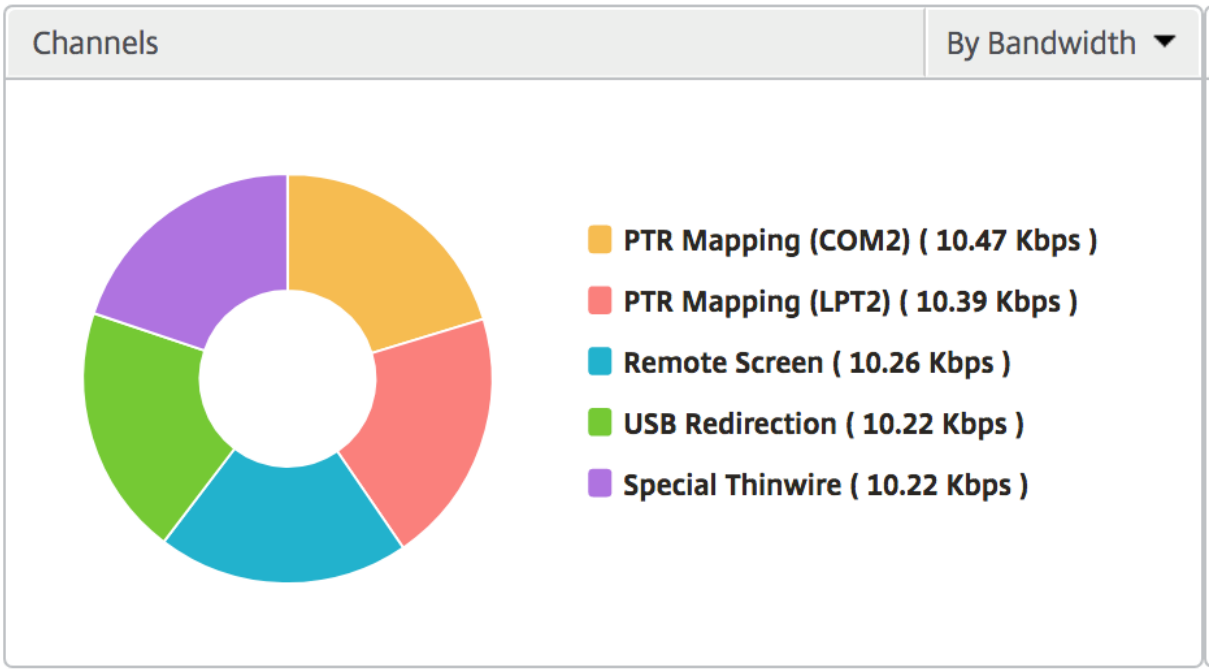
Users

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	

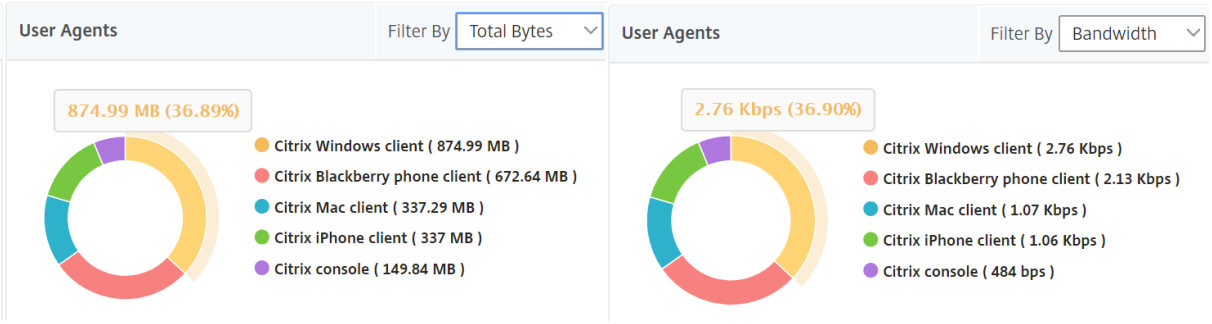
Canaux

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

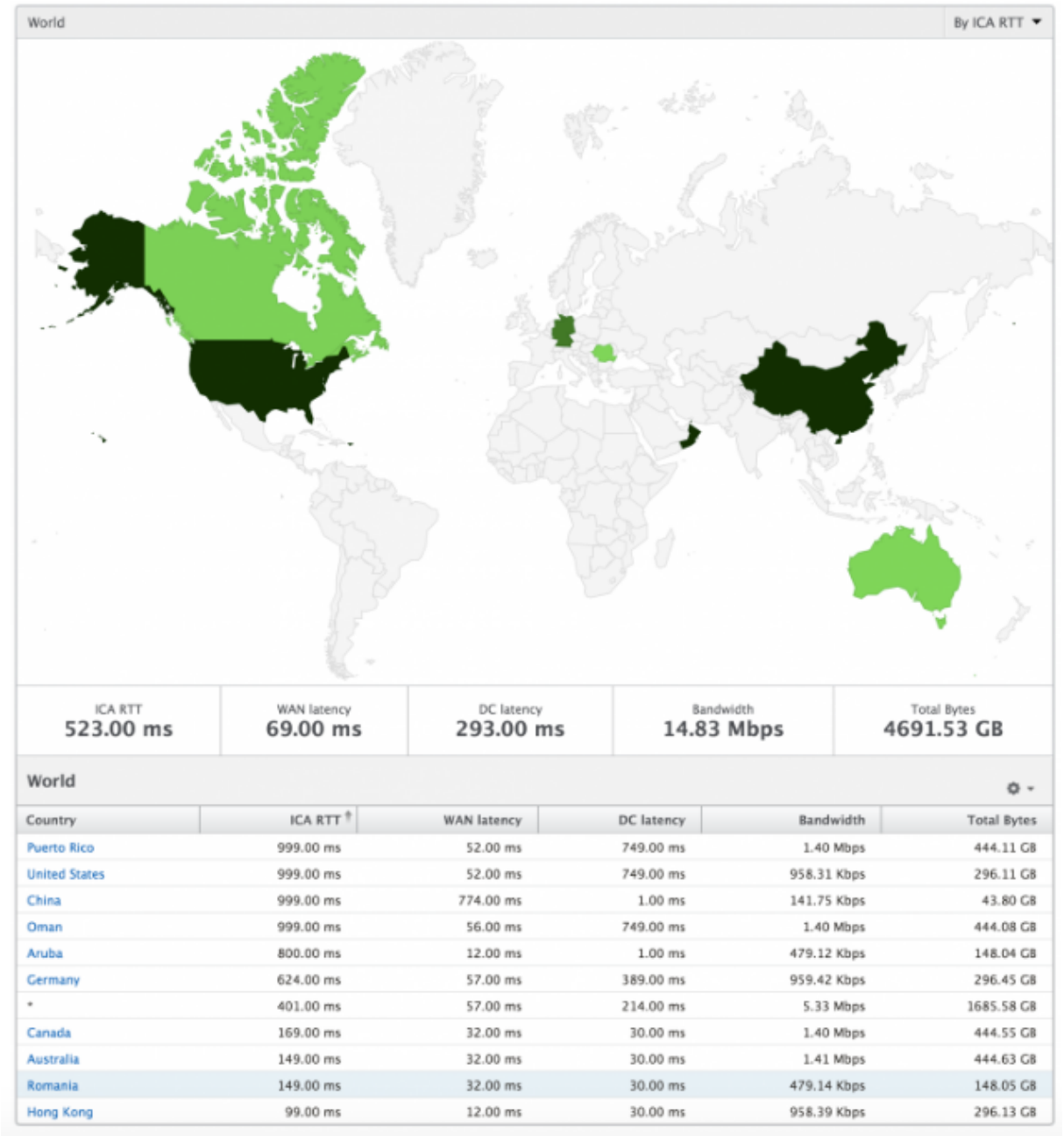
Les mesures de nombre de violations des seuils représentent le nombre de seuils violés au cours de la période sélectionnée. Pour plus d'informations, découvrez comment créer des seuils et des alertes.

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 des versions 12.0 et ultérieures de NetScaler ADM, vous pouvez accéder aux utilisateurs connectés depuis 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

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 **Gateway > 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	Retard moyen du trafic ICA passant par les NetScaler ADC dû au 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 d'espace de travail : client Windows Citrix, etc.
Version du client	Version Workspace.
MSI	Boolean (Oui/Non). Indique si la session est multiflux ICA.
Reconnexions de session	Nombre de fois où la session s'est reconnectée.

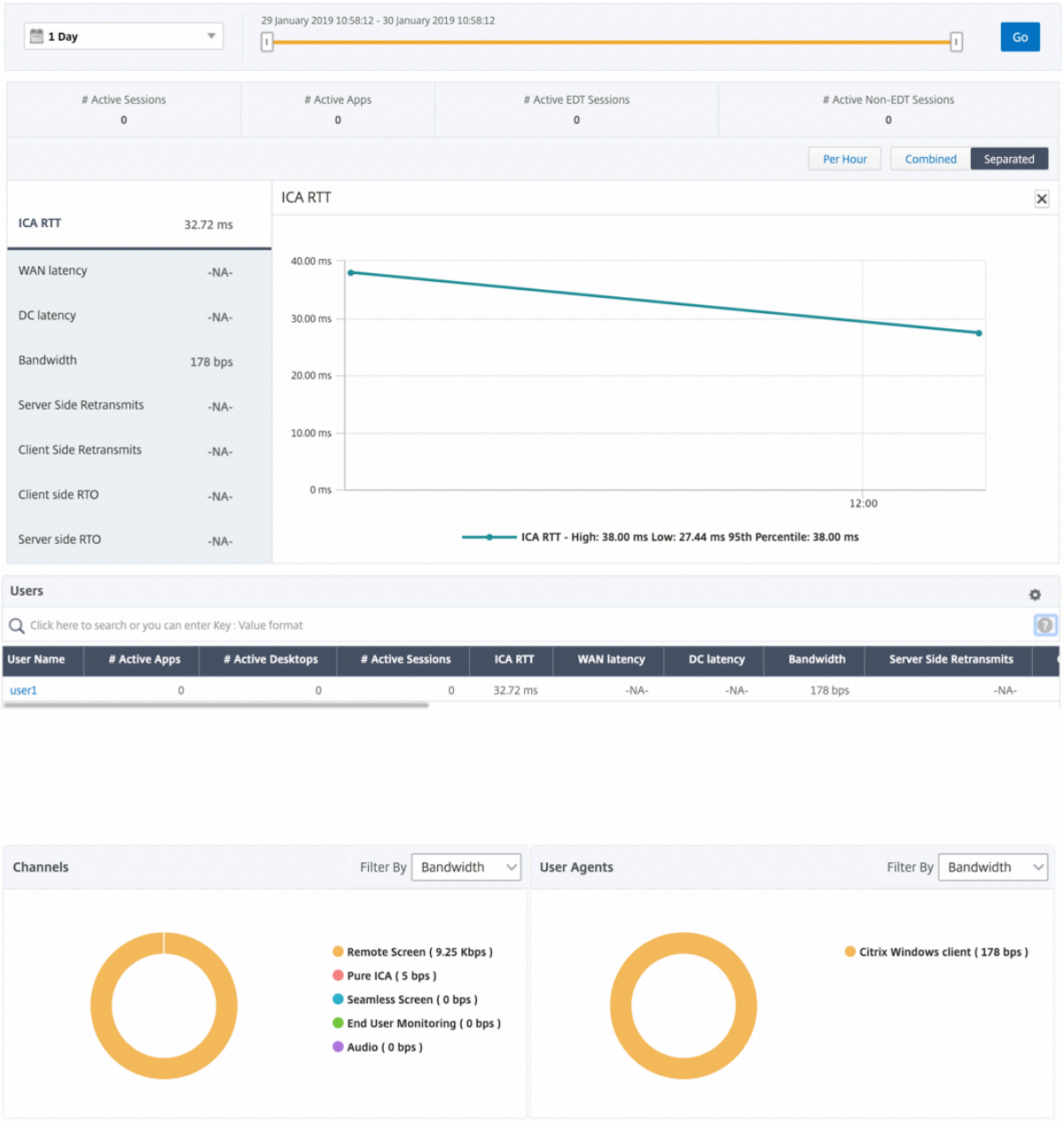
Mesures	Description
Nb d'ACR	Nombre total de fois où un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, le mode utilisateur/transparent de NetScaler Gateway.
Pays	Pays à partir duquel la session 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 NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire de NetScaler 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 lors de la connexion entre NetScaler et le serveur principal.

Mesures	Description
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre NetScaler 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 NetScaler 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 lors de la connexion entre NetScaler et le serveur principal.

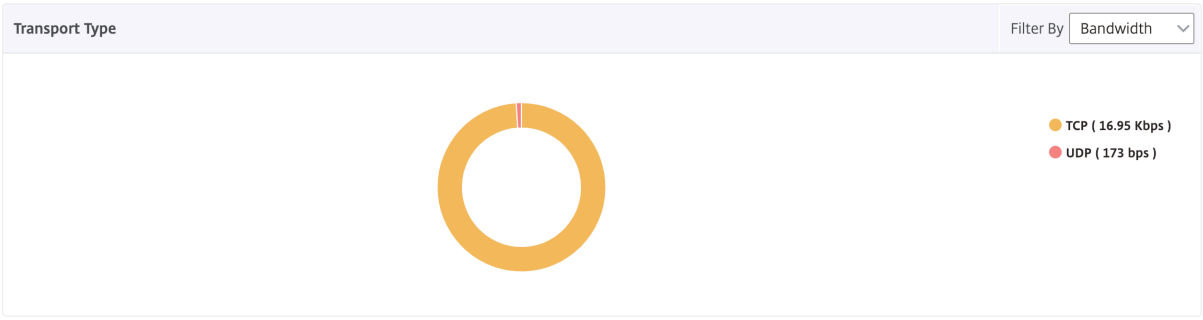
Prise en charge de l'EDT dans HDX insights

NetScaler Application Delivery Management (ADM) prend désormais en charge le transport éclairé de données (EDT) pour afficher des analyses pour HDX Insight. En d'autres termes, ADM prend désormais en charge les protocoles UDP et TCP. La prise en charge de NetScaler Gateway par EDT garantit aux utilisateurs exécutant Citrix Workspace une expérience utilisateur haute définition en cours de session sur des bureaux virtuels.

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 ».

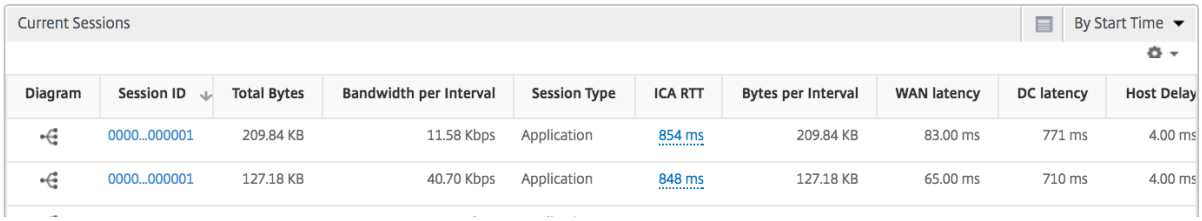


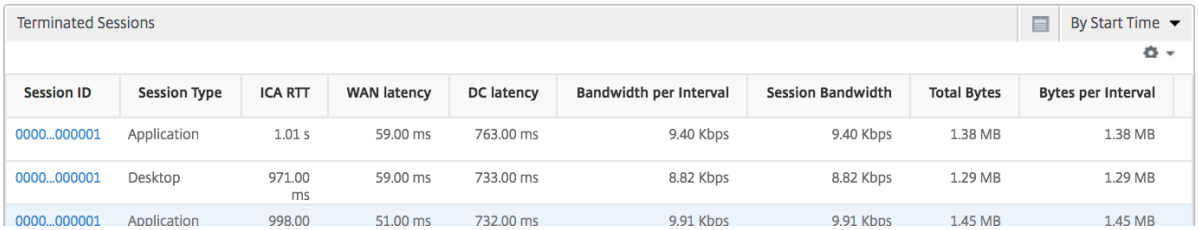
Un nouveau graphique en anneau a été introduit pour vous permettre de voir la bande passante consommée par l'utilisateur ainsi que le nombre total d'octets en fonction du type de protocole utilisé par les utilisateurs.



Métriques HDX Insight disponibles à partir de NetScaler ADM 12.0 et versions ultérieures :

Latence côté client L7	Latence L7 moyenne observée entre le client ICA et l'instance NetScaler. Cette mesure est utile dans le cas de périphériques non Citrix présents dans le chemin de remise.
Latence côté serveur L7	Latence L7 moyenne observée entre l'appareil NetScaler 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.

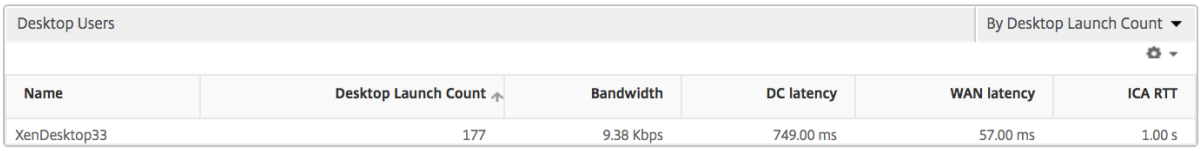




Utilisateurs de bureau

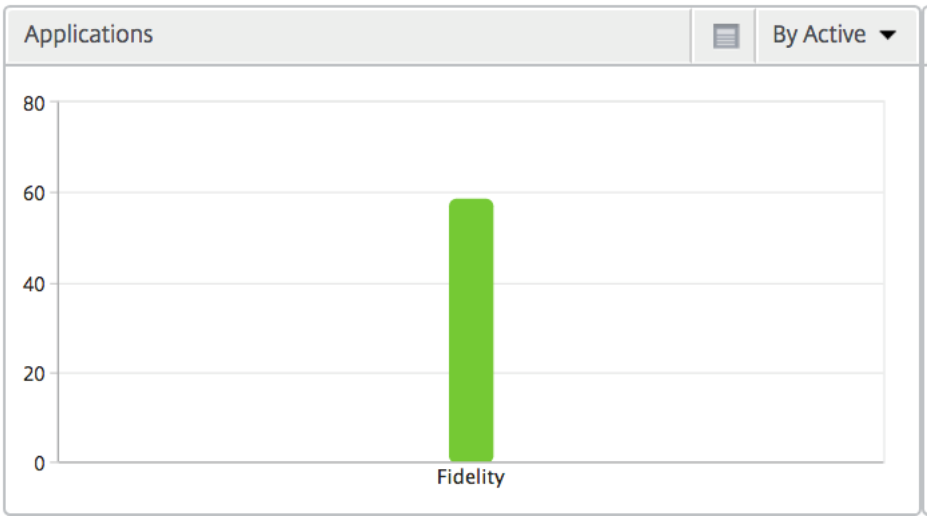
Ce tableau donne un aperçu des sessions Citrix Virtual Desktop pour un utilisateur particulier. Ces mesures peuvent être triées par nombre de lancements de postes de travail et bande passante.

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 NetScaler aux serveurs principaux.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de NetScaler 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.



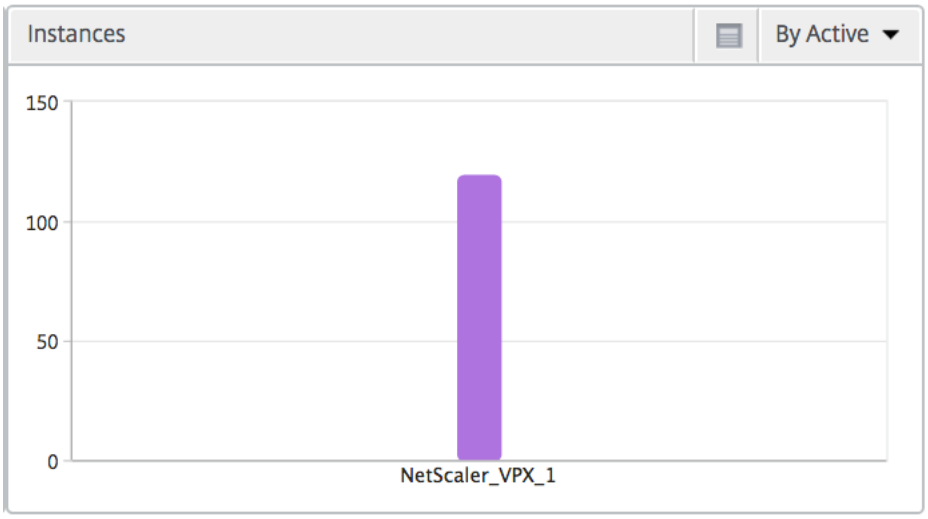
Applications

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.



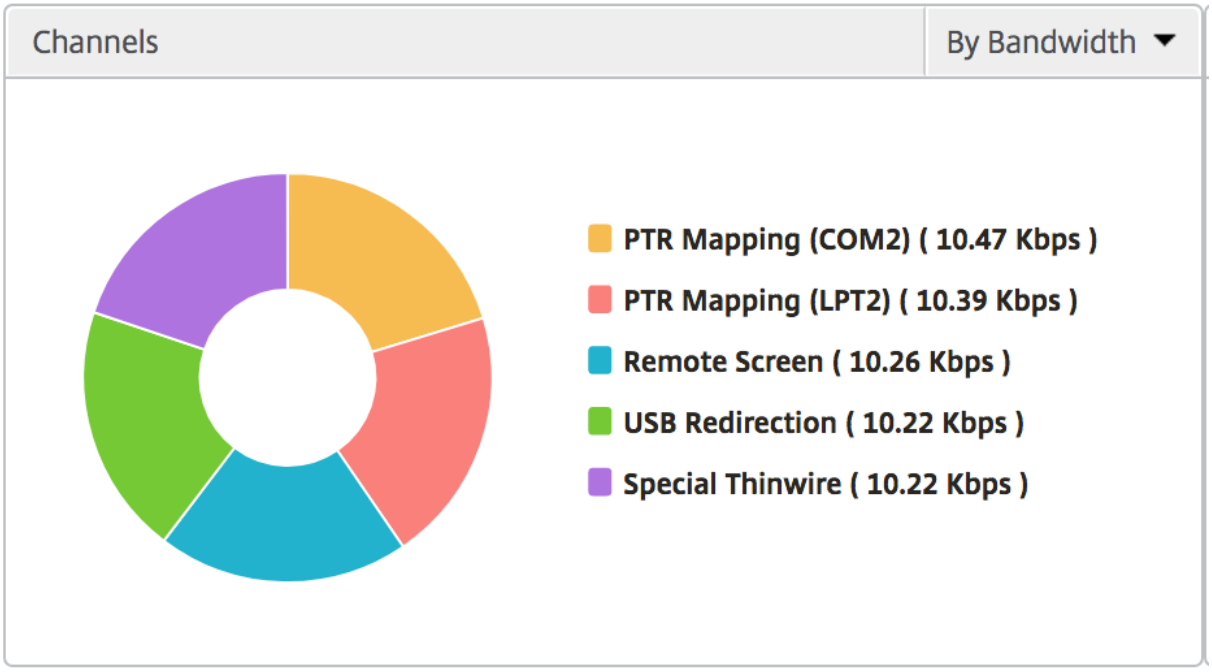
Instances

Un graphique à barres représentant les instances NetScaler triées par applications actives et par nombre total d'applications



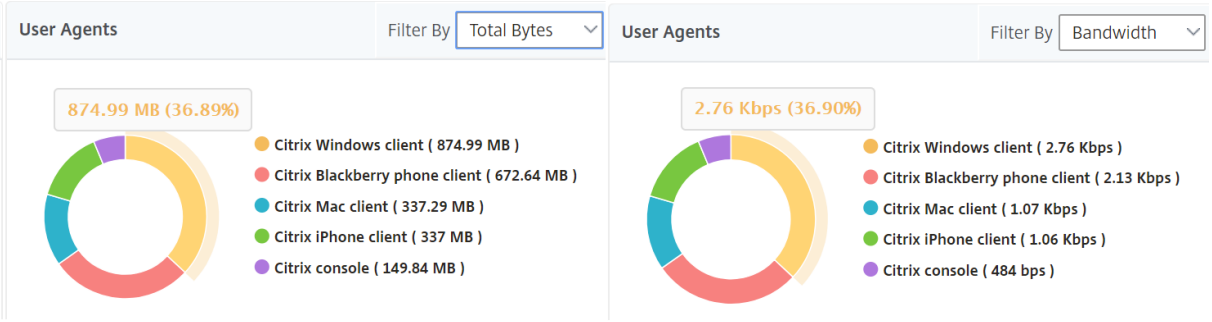
Canaux

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 :

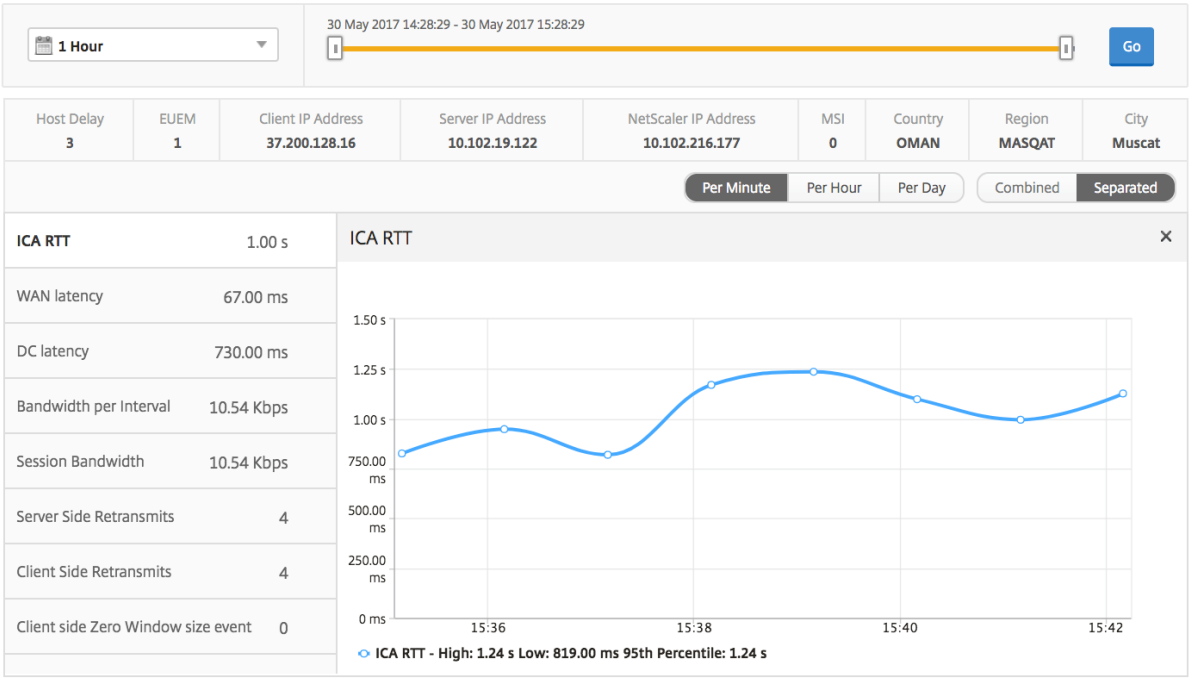
1. Accédez à **Gateway > HDX Insight > Utilisateurs** .
2. Select un utilisateur particulier dans la section **Rapport récapitulatif de l'utilisateur**.

3. Sélectionnez une session dans la colonne **Sessions en cours** ou **Sessions terminées** .

Graphique chronologique

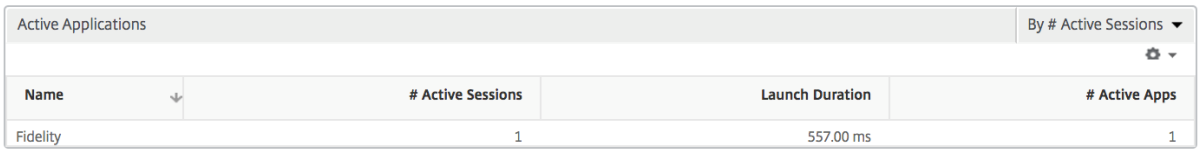
Mesures	Description
Reconnexions de session	Ce nombre indique le nombre de sessions Citrix Virtual App and Desktop actives.
Nb d'ACR	Ce nombre indique le nombre de sessions actives de Citrix Virtual App.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une 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 NetScaler à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire de NetScaler 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 lors de la connexion entre NetScaler et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre NetScaler 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 NetScaler et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre NetScaler 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.



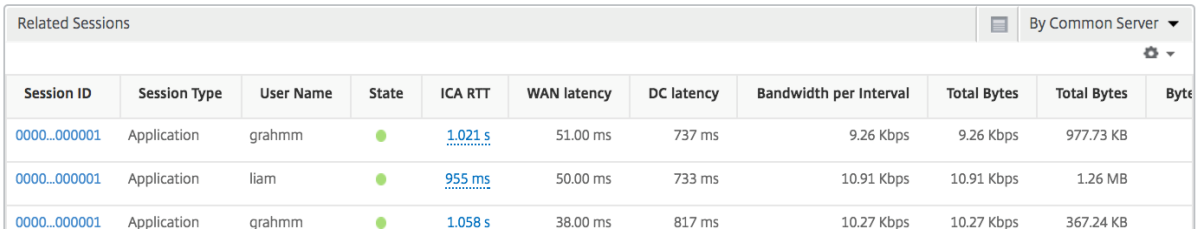
Application active

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 en tant que serveurs communs ou NetScaler commun.



Rapports et mesures d'affichage d'instance

February 1, 2024

Les rapports et les métriques de la vue des instances se concentrent sur les instances NetScaler.

Pour accéder à la vue d'instance :

1. Accédez à **Gateway > HDX Insight > Instances** .

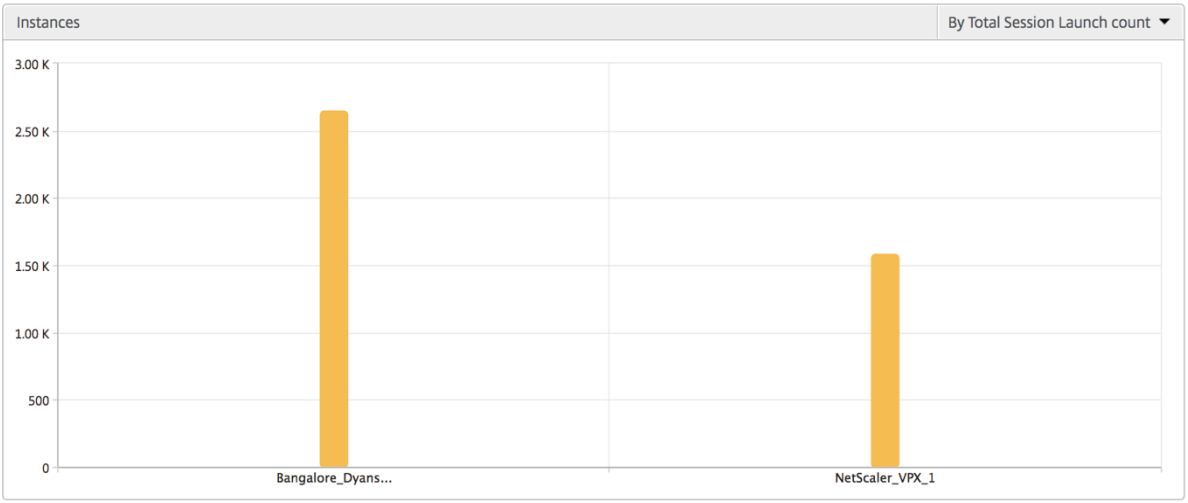
Vue récapitulative de l'instance

Cette vue est appelée vue récapitulative car elle affiche les rapports de toutes les instances NetScaler ajoutées à NetScaler ADM.

Toutes les métriques/rapports, sauf mention explicite, auront les valeurs qui leur correspondent pour la période sélectionnée.

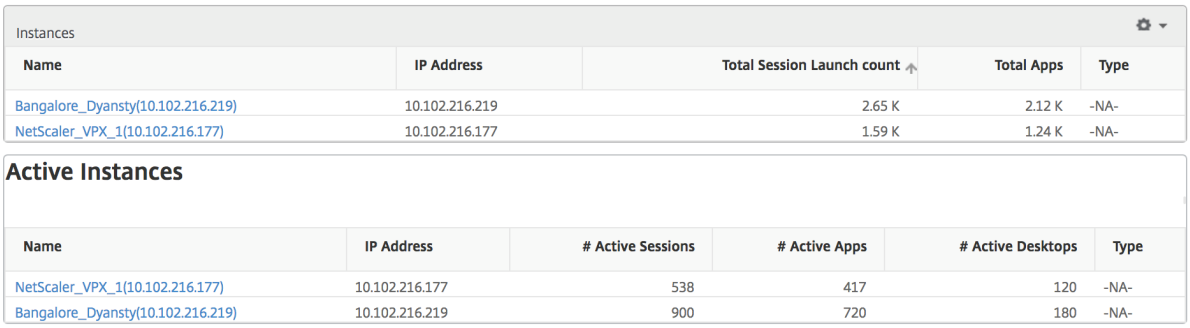
Graphique à barres d'instance

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 NetScaler.
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

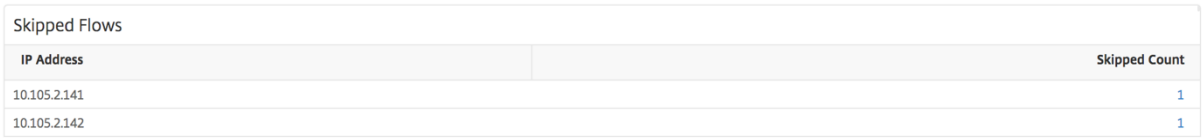
L'état des seuils représente le nombre de seuils dépassés lorsque l'*entité* est sélectionnée en tant qu'instance dans la période sélectionnée. Pour plus d'informations, consultez comment créer des

seuils et des alertes .

Flux ignorés

Un flux ignoré est un enregistrement qui a ignoré l'analyse de la connexion ICA. Cela peut être dû à 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 d'un espace de travail ou d'un type d'espace de travail, etc. Ce tableau indique l'adresse IP et le nombre de flux ignorés. Ces espaces de travail ne font peut-être pas partie des espaces de travail sur 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

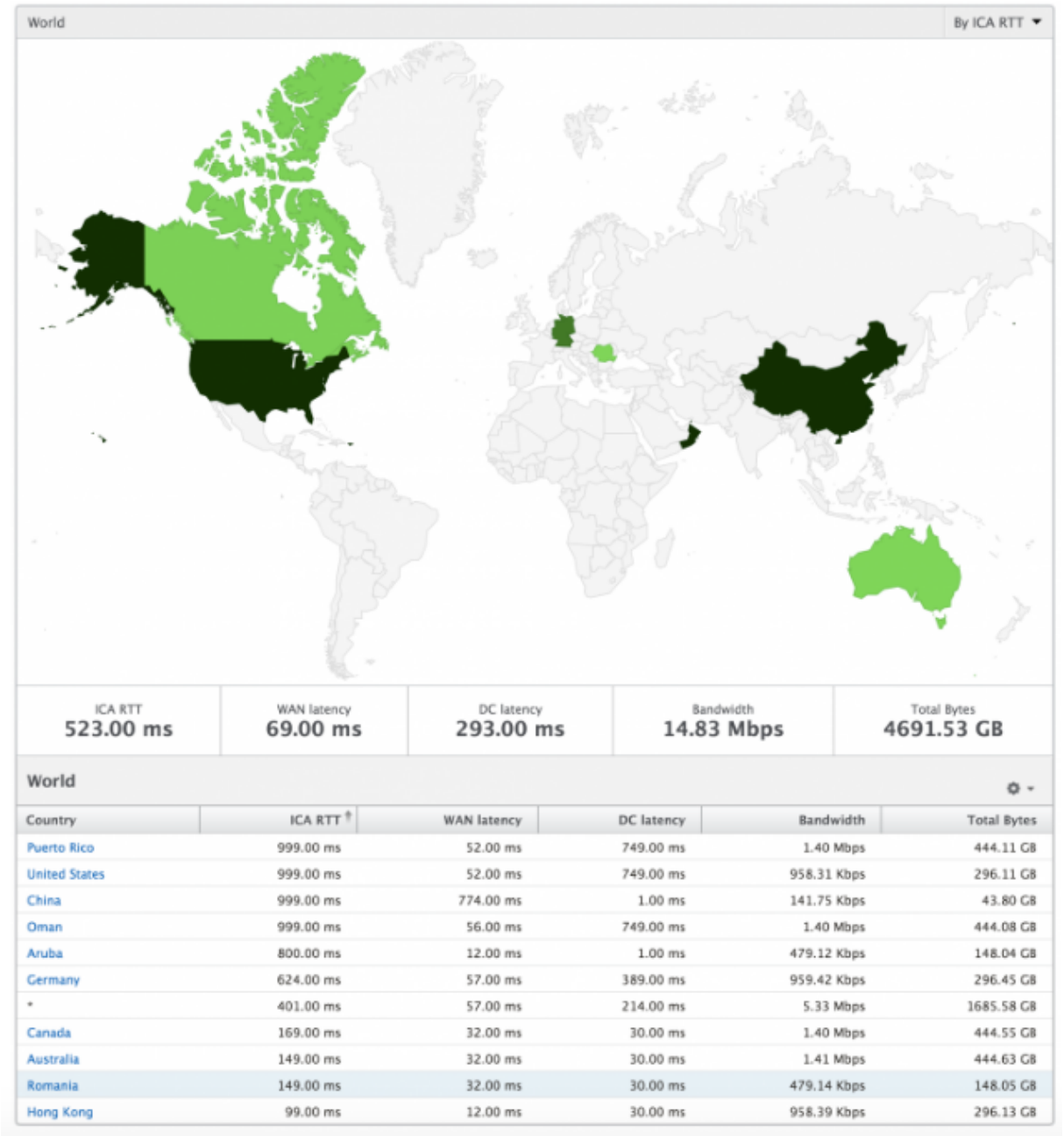
IP Address	Skipped Count
10.105.2.141	1
10.105.2.142	1

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 des versions 12.0 et ultérieures de NetScaler, vous pouvez accéder aux 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

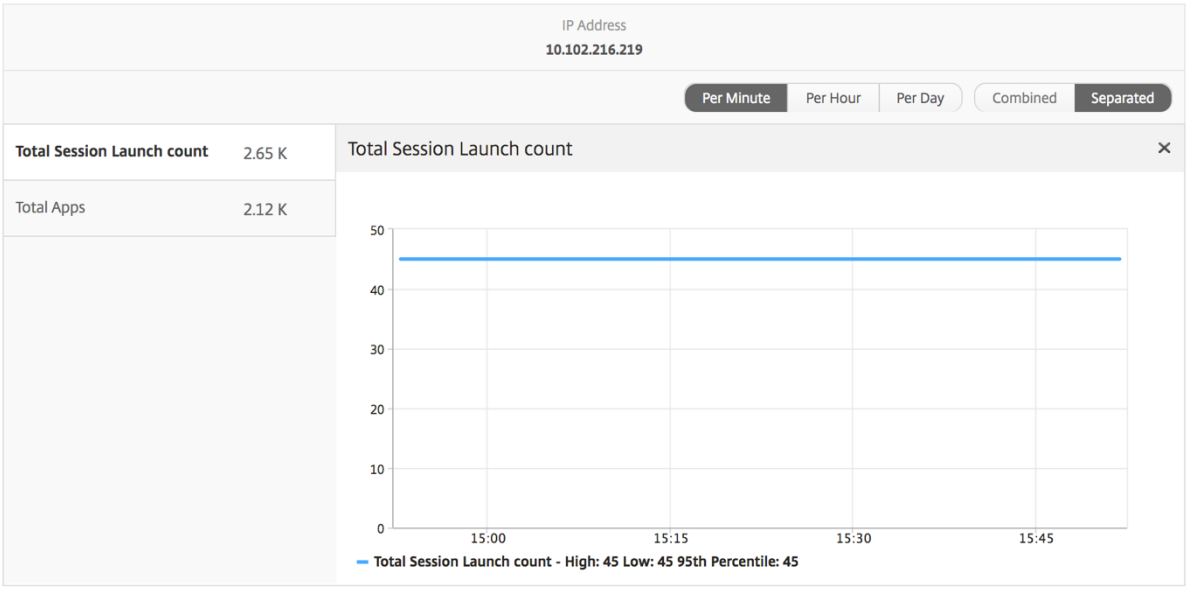
La vue par instance fournit des rapports détaillés sur l'expérience de l'utilisateur final pour une instance NetScaler sélectionnée en particulier.

Pour accéder à la vue d'instance :

1. Accédez à **Gateway > HDX Insight > Instances** .
2. Sélectionnez une instance particulière dans le **rapport de synthèse des instances**.

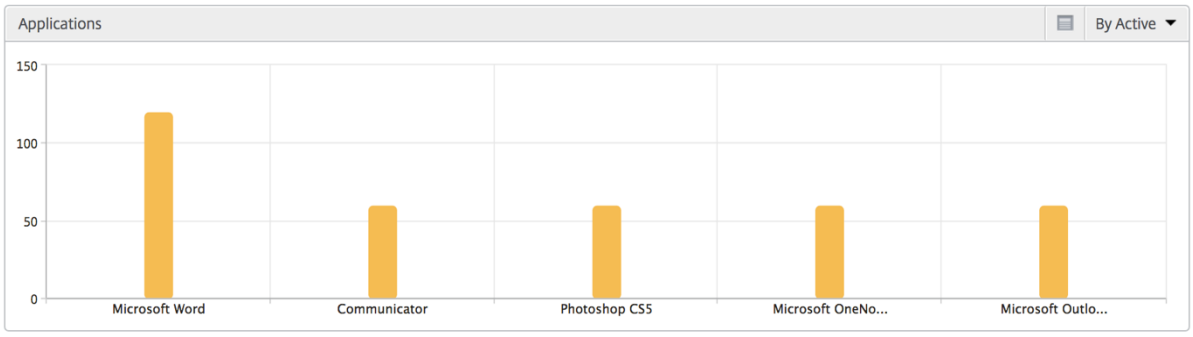
Graphique linéaire

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

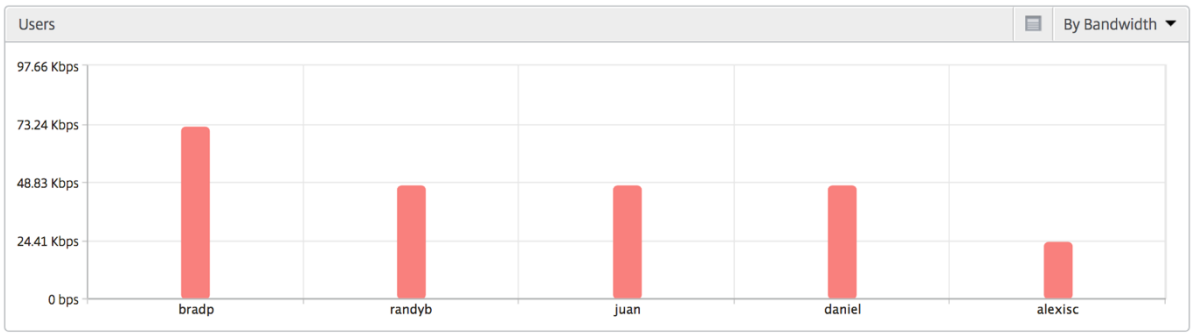
Affiche les 5 premières applications en fonction des critères suivants : applications actives, nombre total de lancements de session, nombre total de lancements d'applications ou durée de lancement.



Graphique à barres des utilisateurs

Le graphique à barres Utilisateurs affiche les 5 premiers utilisateurs selon les critères suivants

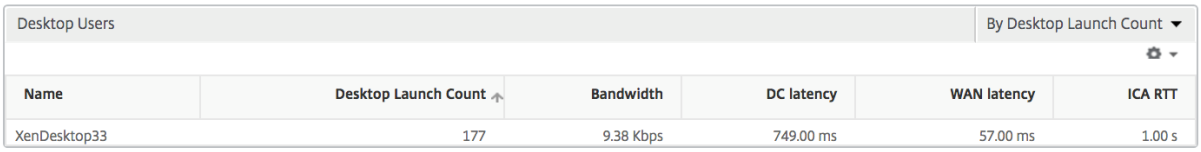
- Bande passante
- Latence WAN
- Latence DC
- RTT ICA



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 NetScaler aux serveurs principaux.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de NetScaler 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.

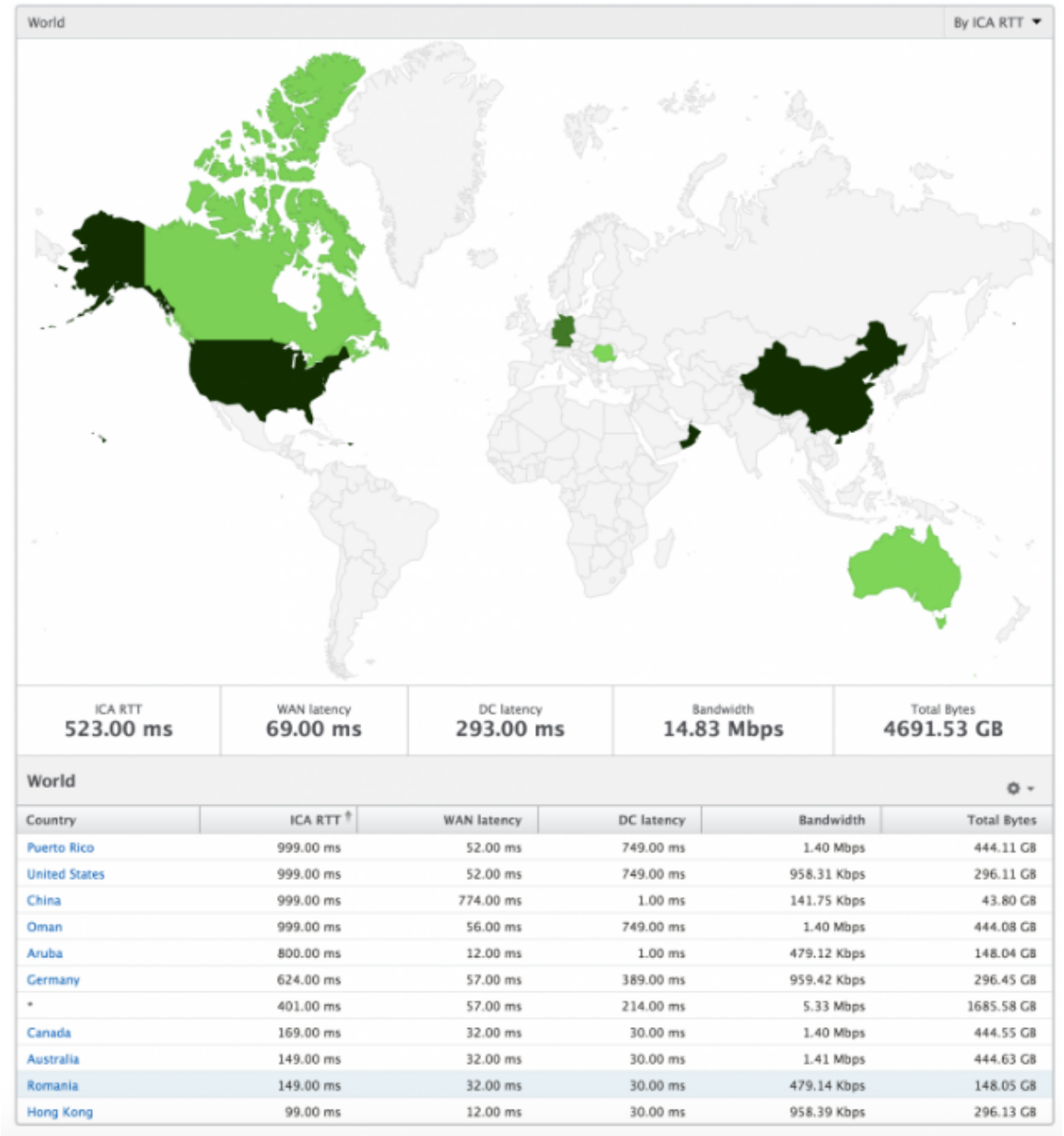


Vue du monde

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 des versions 12.0 et ultérieures de NetScaler ADM, vous pouvez accéder aux 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

Rapports et mesures d'affichage des licences

February 1, 2024

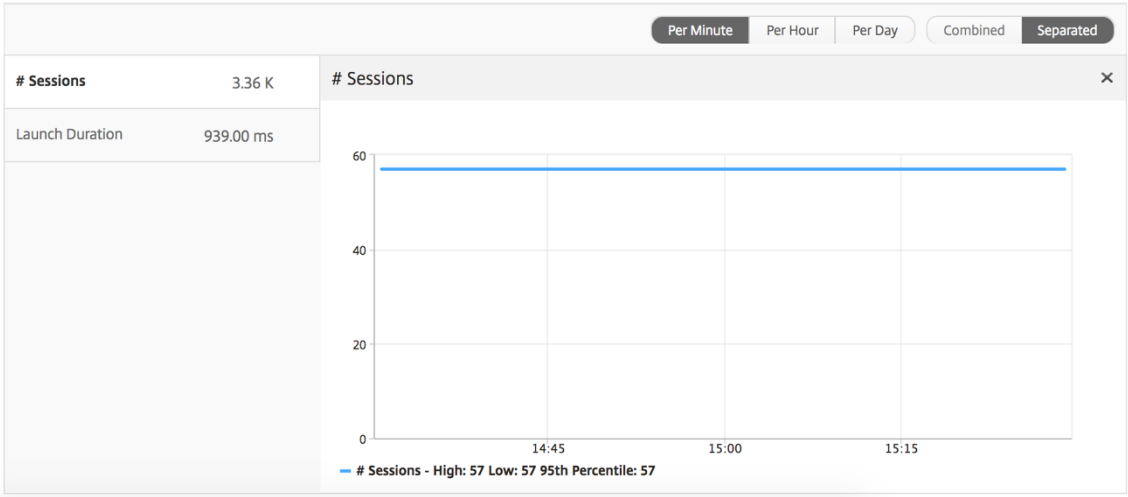
La vue des licences fournit des détails sur les informations de licence NetScaler Gateway.

Pour accéder à la vue des licences :

1. Accédez à **Gateway > HDX Insight > Licences** .

Graphique linéaire

Métriques	Description
Licences utilisées	Les licences CCU NetScaler 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 NetScaler Gateway CCU que le client peut utiliser.



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 NetScaler et NetScaler ADM.
- Génération d'enregistrements pour le trafic HDX/ICA dans NetScaler.
- Population d'enregistrements dans NetScaler ADM.

Liste de contrôle de configuration HDX Insight

- Assurez-vous que la fonctionnalité AppFlow est activée dans NetScaler. Pour plus de détails, consultez Activation d'AppFlow.
- Vérifiez la configuration de HDX Insight dans la configuration en cours d'exécution de NetScaler.

  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 ICA_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.
- `appflowlog` Le paramètre de vérification de NetScaler Gateway ou du serveur virtuel VPN est activé pour Access Gateway ou un déploiement à double saut. Pour plus de détails, consultez Activation d'AppFlow pour les serveurs virtuels.
- Vérifiez que le « chaînage des connexions » est activé dans NetScaler à double saut. Pour plus de détails, voir Configuration des appliances NetScaler Gateway pour exporter desdonnées.
- 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 des sessions sur la paire NetScaler High Availability.

Liste de contrôle de la connectivité entre NetScaler et NetScaler ADM

- Vérifiez l'état du collecteur AppFlow dans NetScaler. Pour plus de détails, consultez Comment vérifier l'état de la connectivité entre NetScaler et AppFlowCollector.
- 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 **Paramètres > AppFlow > Stratégies dans l'** interface graphique pour vérifier les résultats de la stratégie AppFlow.
- Validez tout pare-feu bloquant les ports AppFlow 4739 ou 5557.

Liste de contrôle de la génération d'enregistrements pour le trafic HDX/ICA dans NetScaler

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'omission 0 indique que l'enregistrement a été correctement exporté depuis NetScaler.

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_CID	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 espaces de travail 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_RECLIENT_VERSION	L'analyse RSA pour cet espace de travail (client) a été ignorée car il ne figure pas dans la liste des autorisations
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 l'espace de travail non valide reçue du client
147	NS_ICA_ERR_UNKNOWN_CLIENT_PRODUCT_ID	ID produit 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 VDA ne prend pas en charge Reducer version 3
167	NS_ICA_ERR_CLIENT_NOT_REDUCER_V3	Workspace ne prend pas en charge la version 3 de Reducer
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 sur 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 sur 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 du réseau local	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
hdx_dbg_reconnected_session	Nombre total de demandes de reconnexion provenant du client sans erreur NetScaler	Statistiques/Diagnostics
hdx_dbg_host_rejected_ns_reconnect	Nombre total d'hôtes rejetés par demande 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. Un canal de surveillance de l'expérience utilisateur final est requis 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
hdx_err_skip_no_msi	La fonctionnalité MSI du serveur XA/XD est absente. Cela indique une ancienne version de serveur et HDX Insight ignore cette connexion.	Erreur

Nom du compteur HDX	Motif	Catégorie (Statistiques/Erreur/-Diagnostics)
hdx_err_skip_old_server	Ancienne version de serveur non prise en charge	Erreur
hdx_err_clnt_not_whitelist	L'espace de travail du client ne figure pas dans la liste autorisée, 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
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

Nom du compteur HDX	Motif	Catégorie (Statistiques/Erreur/-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
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 NetScaler.

Population des enregistrements dans la liste de contrôle NetScaler ADM

- Exécutez la commande `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: ica_"` et consultez les journaux pour confirmer que NetScaler ADM reçoit les enregistrements AppFlow.
- Vérifiez que l'instance NetScaler est ajoutée à NetScaler ADM.
- Vérifiez que le serveur virtuel NetScaler Gateway/VPN est sous licence dans NetScaler ADM.
- Assurez-vous que le réglage des paramètres multi-sauts est activé pour le double saut.
- Assurez-vous que NetScaler Gateway est autorisé pour le deuxième saut dans le cadre d'un 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 NetScaler et NetScaler ADM.
- Versions du serveur Citrix Virtual Apps and Desktops.
- Versions de l'espace de travail client.
- 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 NetScaler.
- Bundle de support technique capturé pour NetScaler ADM.
- Traces de paquets capturées sur tous les appareils NetScaler.
  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 mise à jour d'ADC pour connaître les problèmes connus sur HDX Insight.

Analyse d'infrastructure

February 1, 2024

L'un des principaux objectifs des administrateurs réseau est de surveiller les instances NetScaler. 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 NetScaler Application Delivery Management (ADM) rassemble toutes les données collectées à partir des instances NetScaler et les quantifie dans un **score d'instance** qui définit l'état de santé 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

  Les problèmes de ressources système critiques qui peuvent survenir sur les instances NetScaler et surveillés par NetScaler ADM sont les suivants.

  - Utilisation**élevée du processeur**. L'utilisation du processeur a dépassé la valeur seuil la plus élevée dans l'instance NetScaler.
  - **Utilisation élevée de la mémoire**. L'utilisation de la mémoire a dépassé la valeur seuil la plus élevée dans l'instance NetScaler.
  - **Utilisation élevée du disque**. L'utilisation du disque a dépassé la valeur seuil la plus élevée dans l'instance NetScaler.
  - **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 ont été détectées sur l'instance NetScaler.

- **Rejets NIC**. Les paquets supprimés par la carte NIC ont dépassé la valeur seuil la plus élevée dans l'instance NetScaler.

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 manière de modifier les niveaux de gravité, voir Modifier la gravité signalée des événements qui se produisent sur les instances NetScaler.

  Pour plus d'informations sur les événements dans NetScaler 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 NetScaler
  - **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 NetScaler.

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 **Infrastructure > 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.

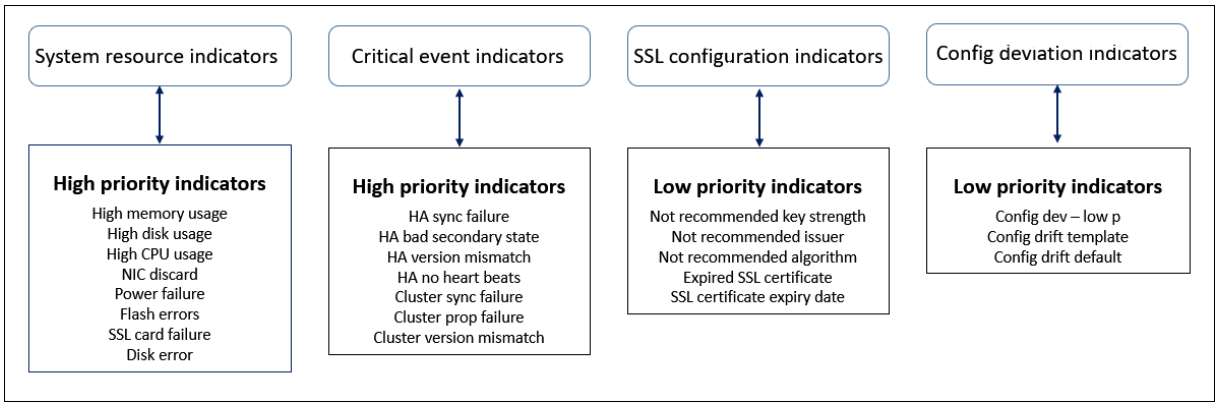
- Seuil bas —Incrément de compteur de perte ou de limite de débit de 1 paquet
- Seuil élevé : 10000 paquets baisse ou incrément du compteur de limite de taux

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.

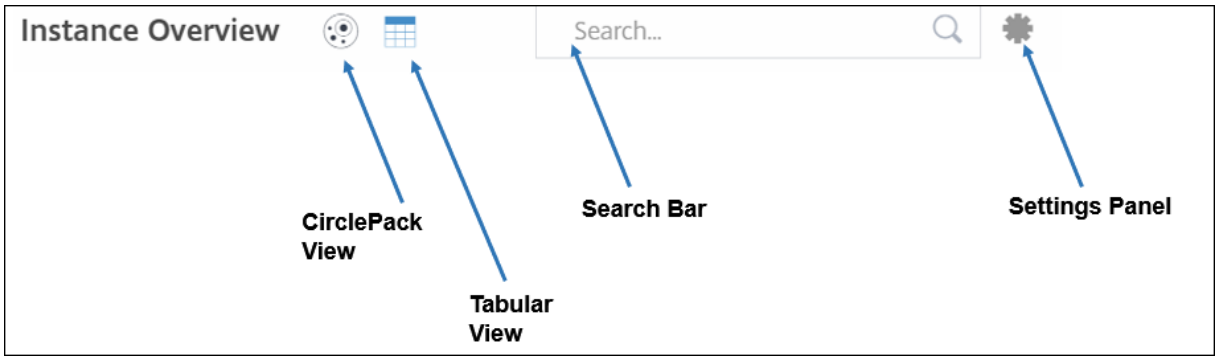
2. **Sur la base de la violation de la valeur seuil**. Par exemple, un indicateur de ressources système est déclenché lorsque la carte NIC rejette des paquets et que le seuil est dépassé.
3. **Sur la base de la violation du seuil bas et du seuil supérieur**. Ici, un indicateur peut être déclenché de 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 **Infrastructure > Analyse de l'infrastructure**.

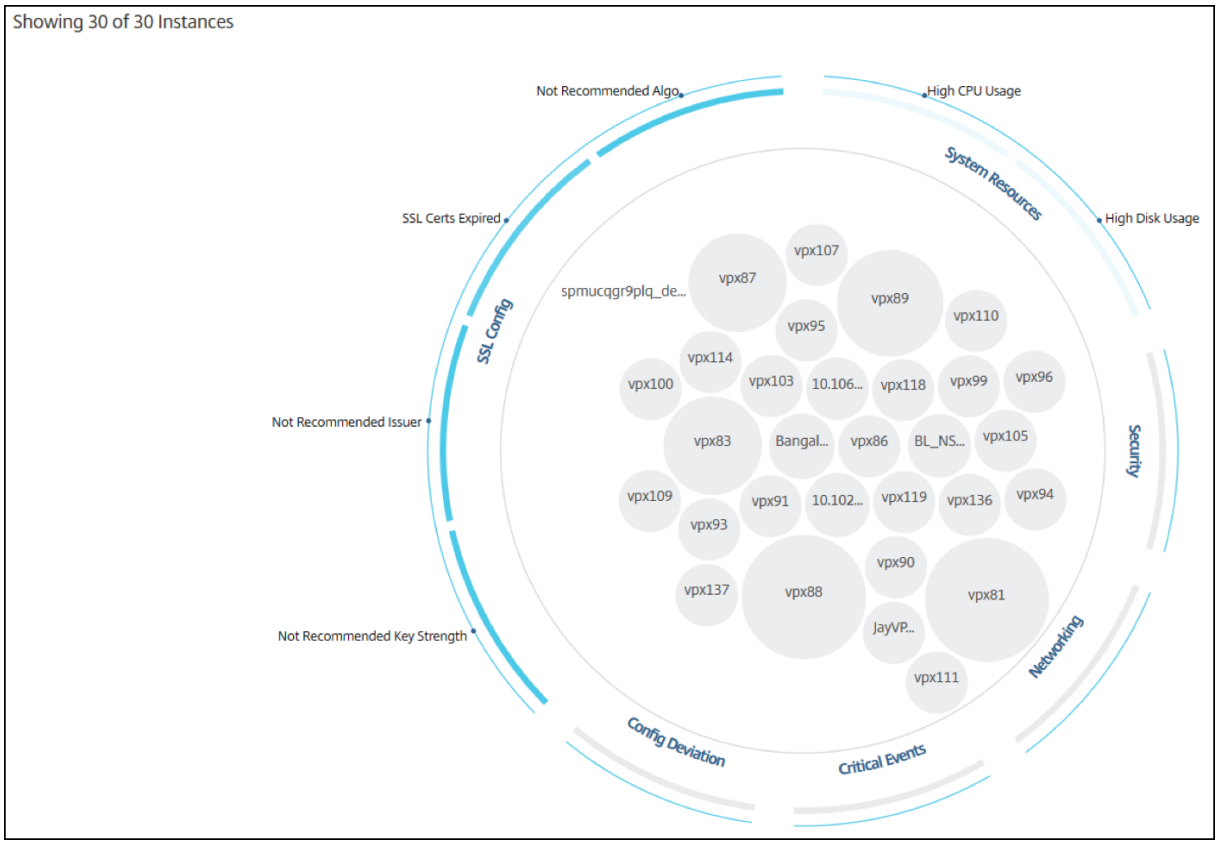
L'analyse de l'infrastructure peut être affichée au format **Circle Pack** ou **Tabulaire** . Vous pouvez basculer entre les deux formats.



- 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.



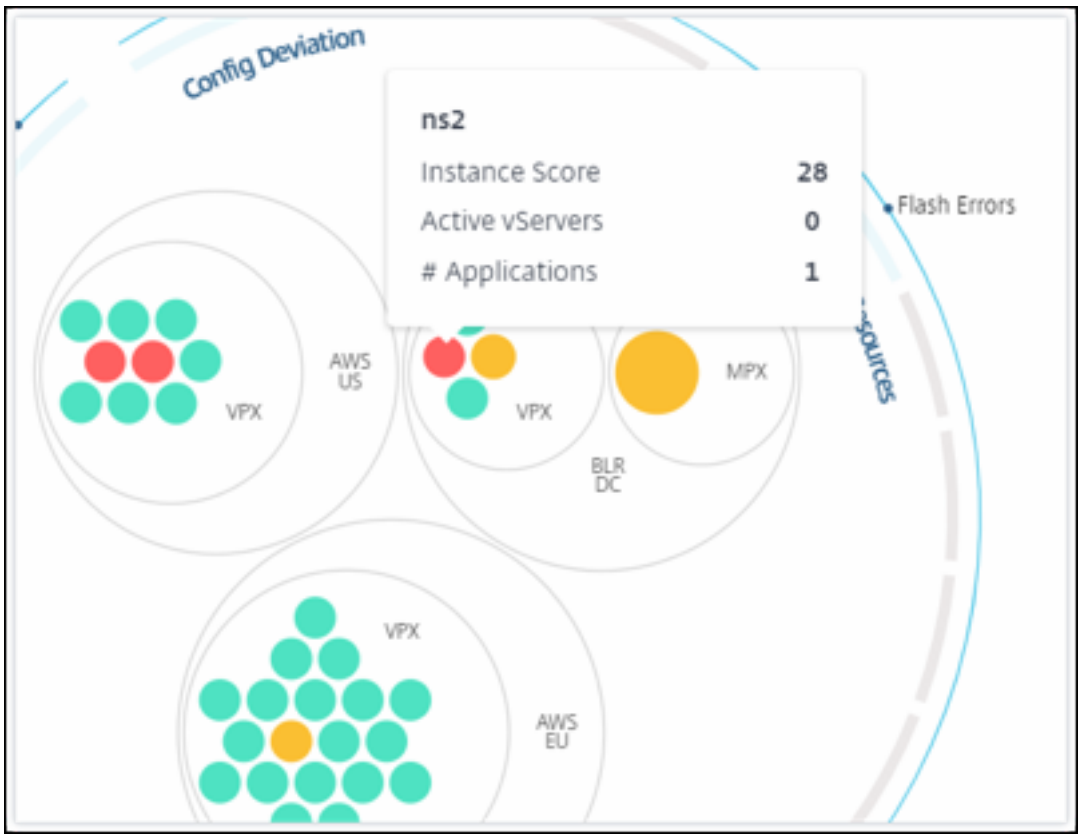
Cercles d'instance

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.

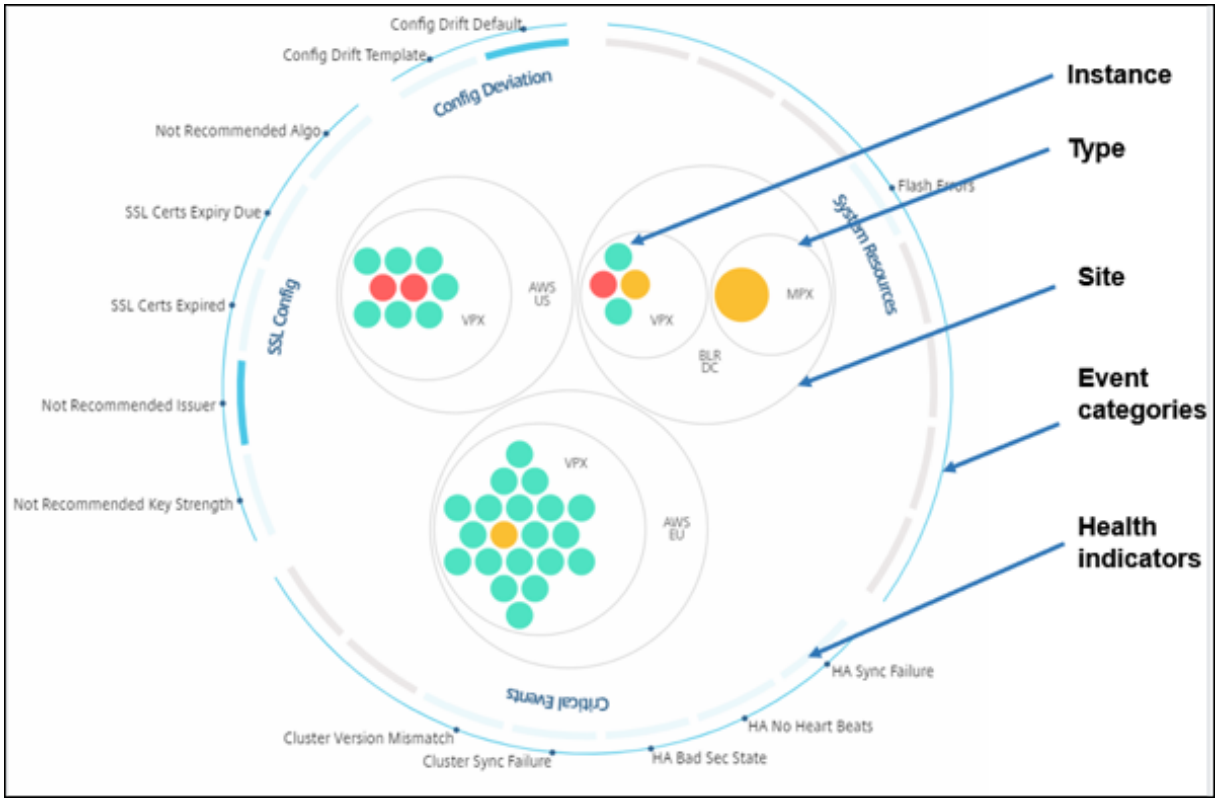


Cercles d'instance groupés

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.

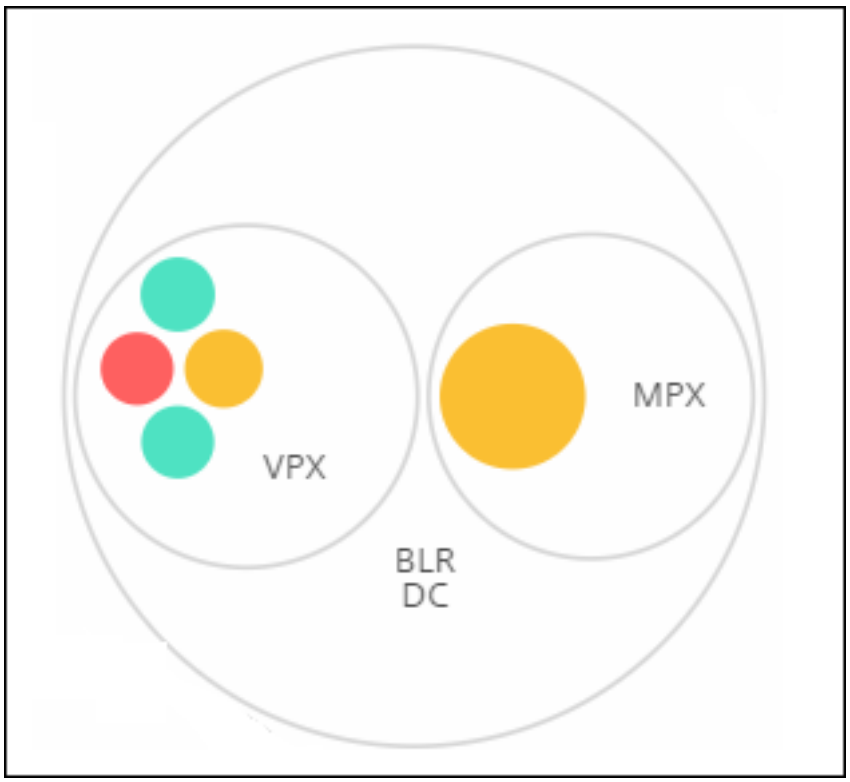


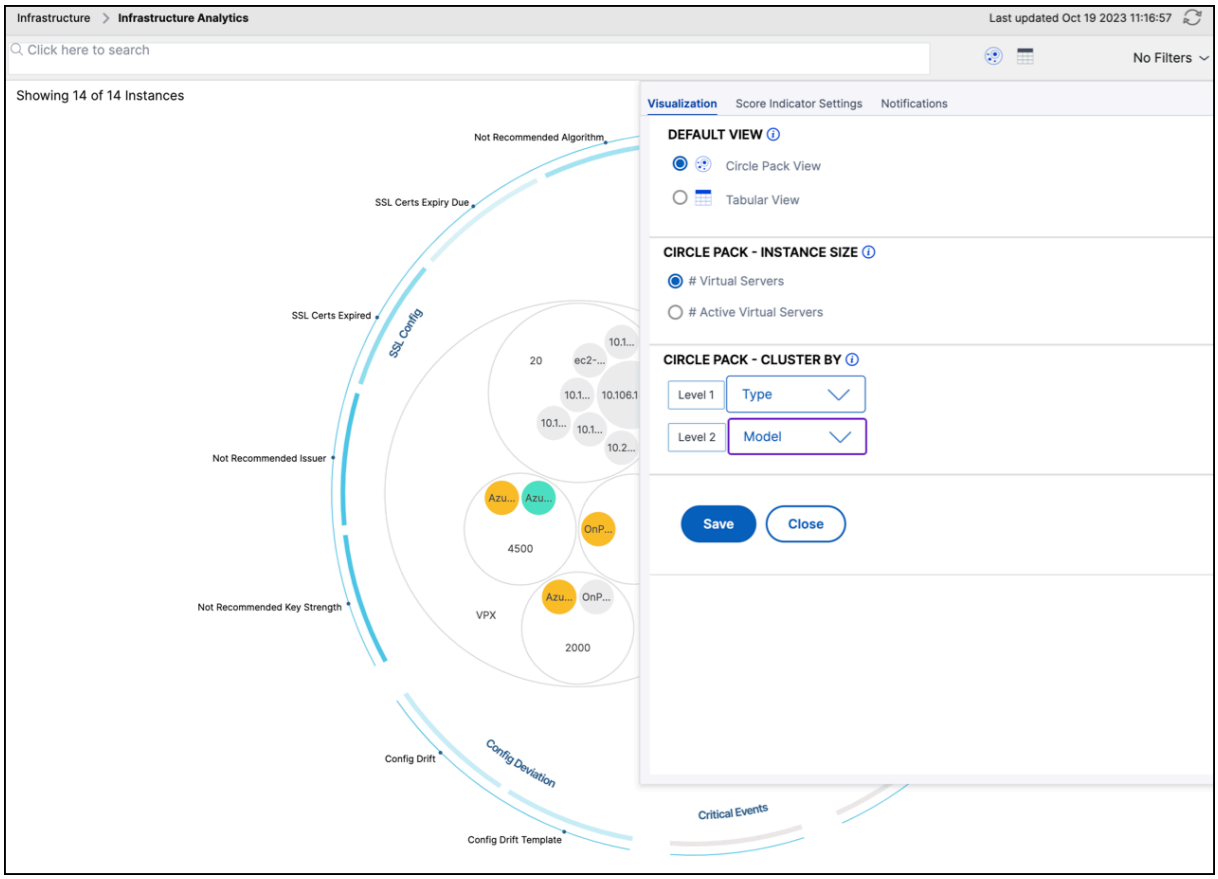
Tous ces cercles imbriqués sont délimités par deux cercles extérieurs. Les deux cercles extérieurs représentent les quatre catégories d'événements surveillés par NetScaler ADM (ressources système, événements critiques, configuration SSL et écart de configuration) et les indicateurs de santé qui y contribuent.

Cercles d'instance en cluster

NetScaler 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.

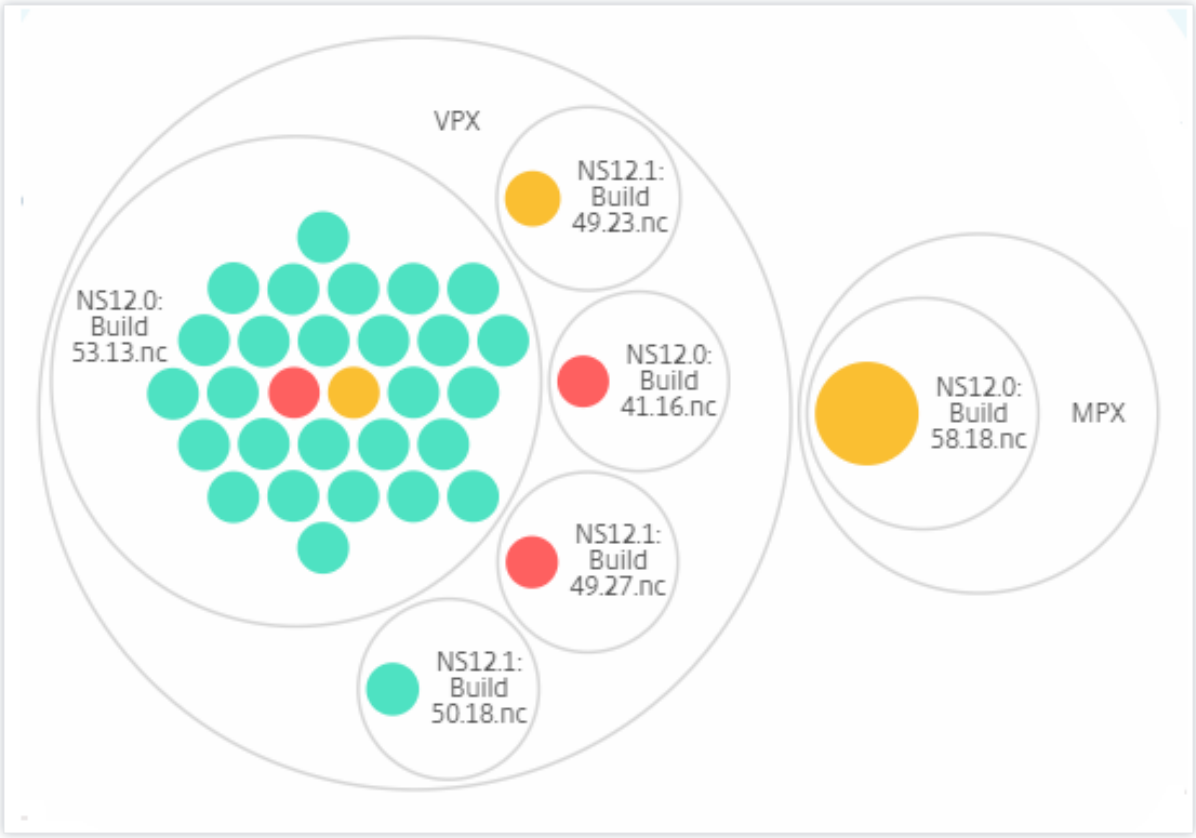




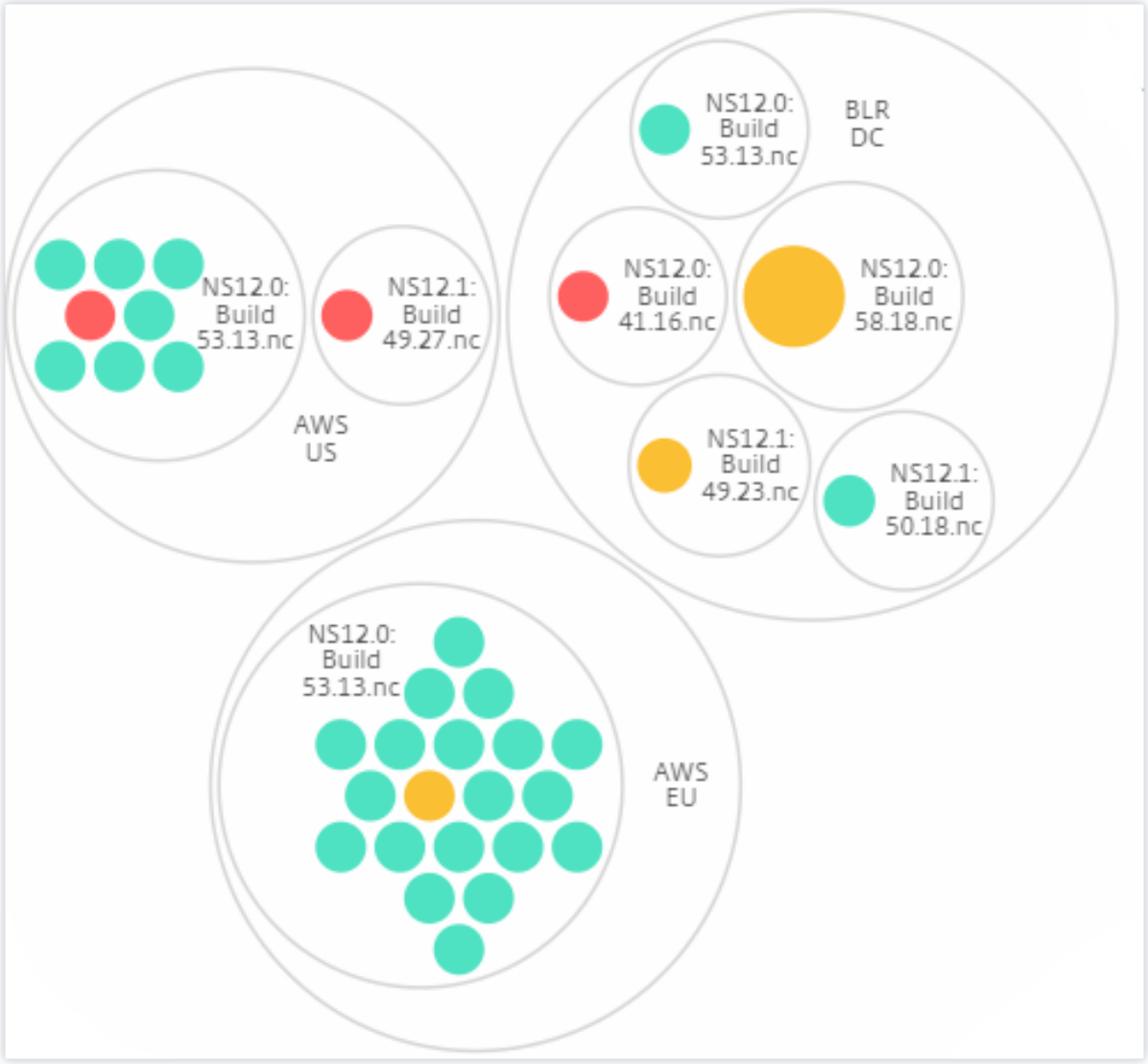
Quelques autres exemples de regroupement à deux niveaux sont les suivants :

Site et modèle :

Type et version :

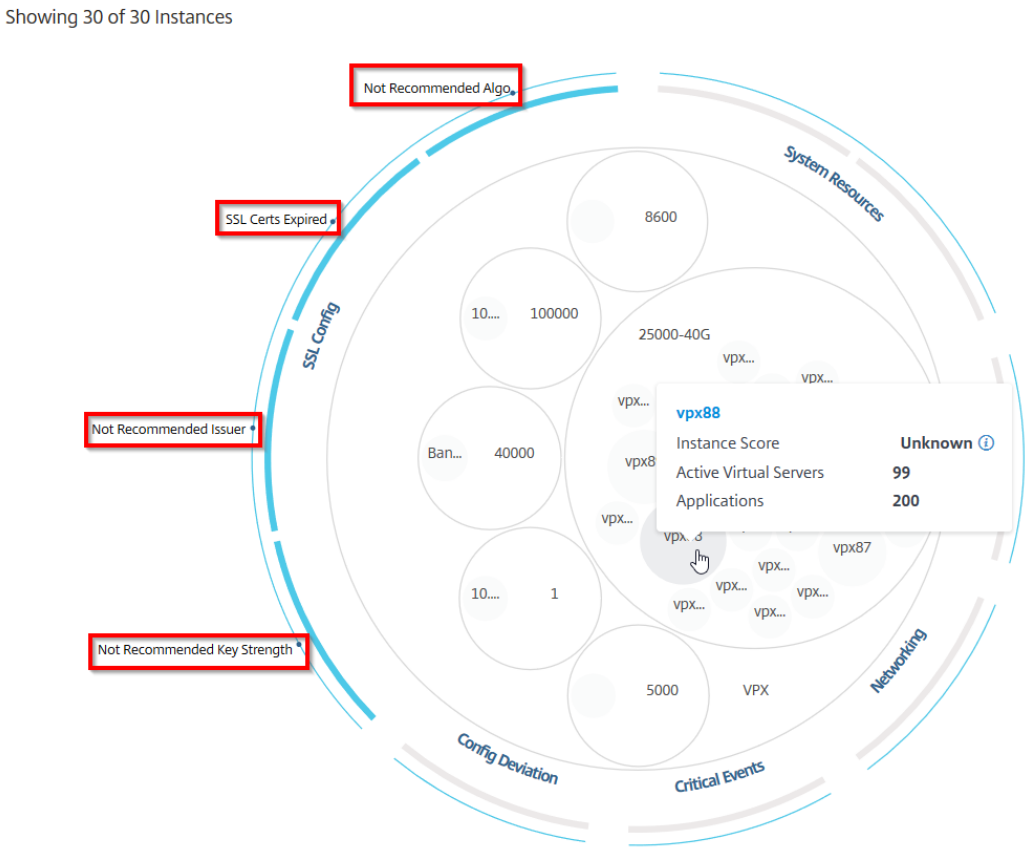


Site et version :

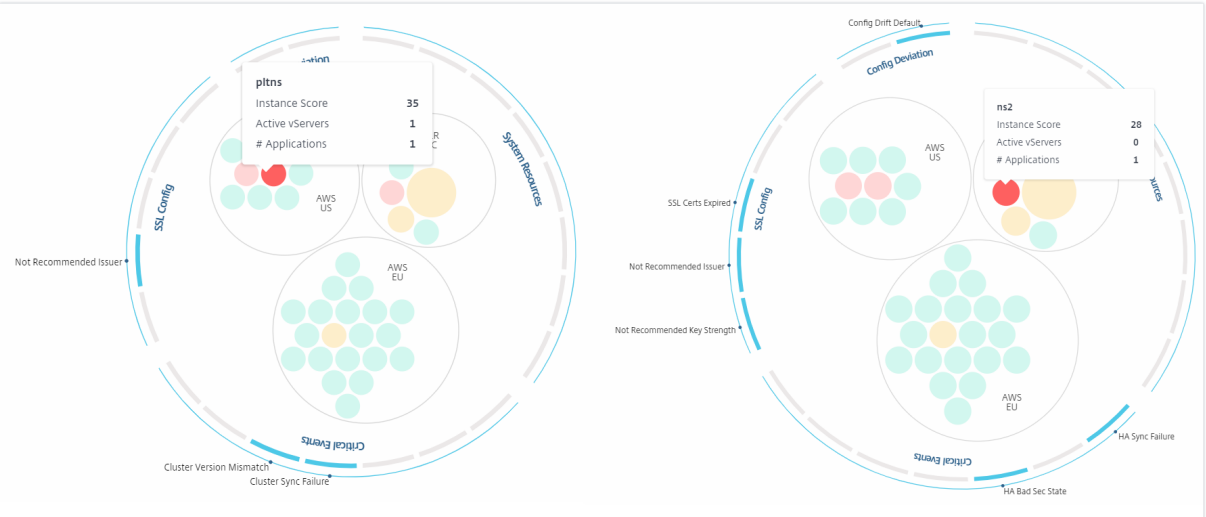


Comment utiliser Circle Pack

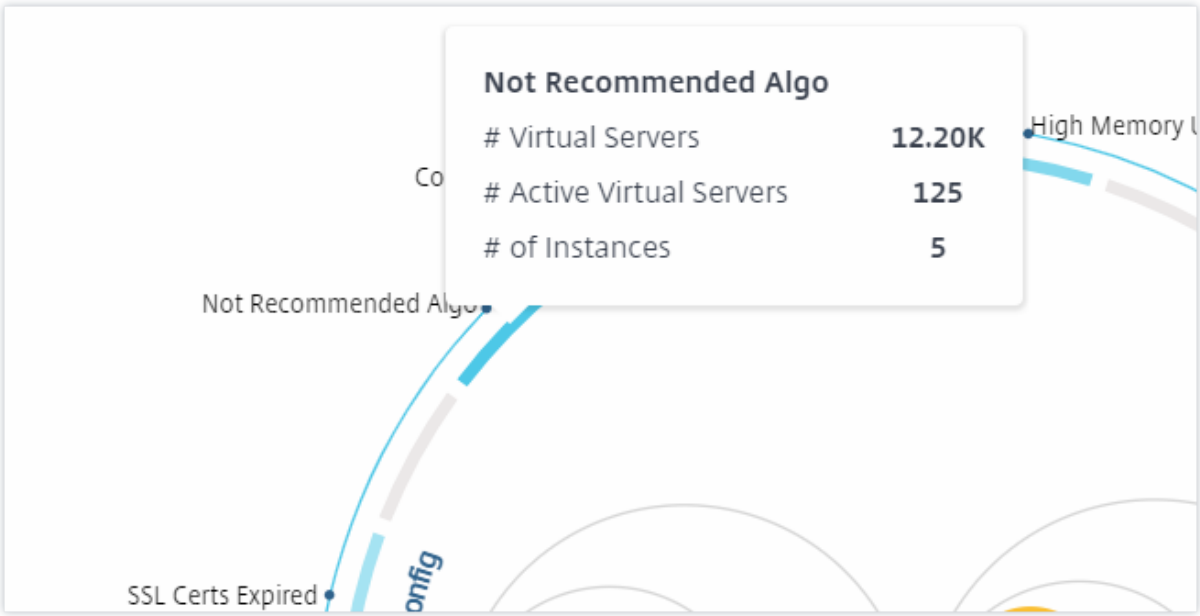
Cliquez sur chacun des cercles colorés pour mettre en surbrillance cette instance.



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.

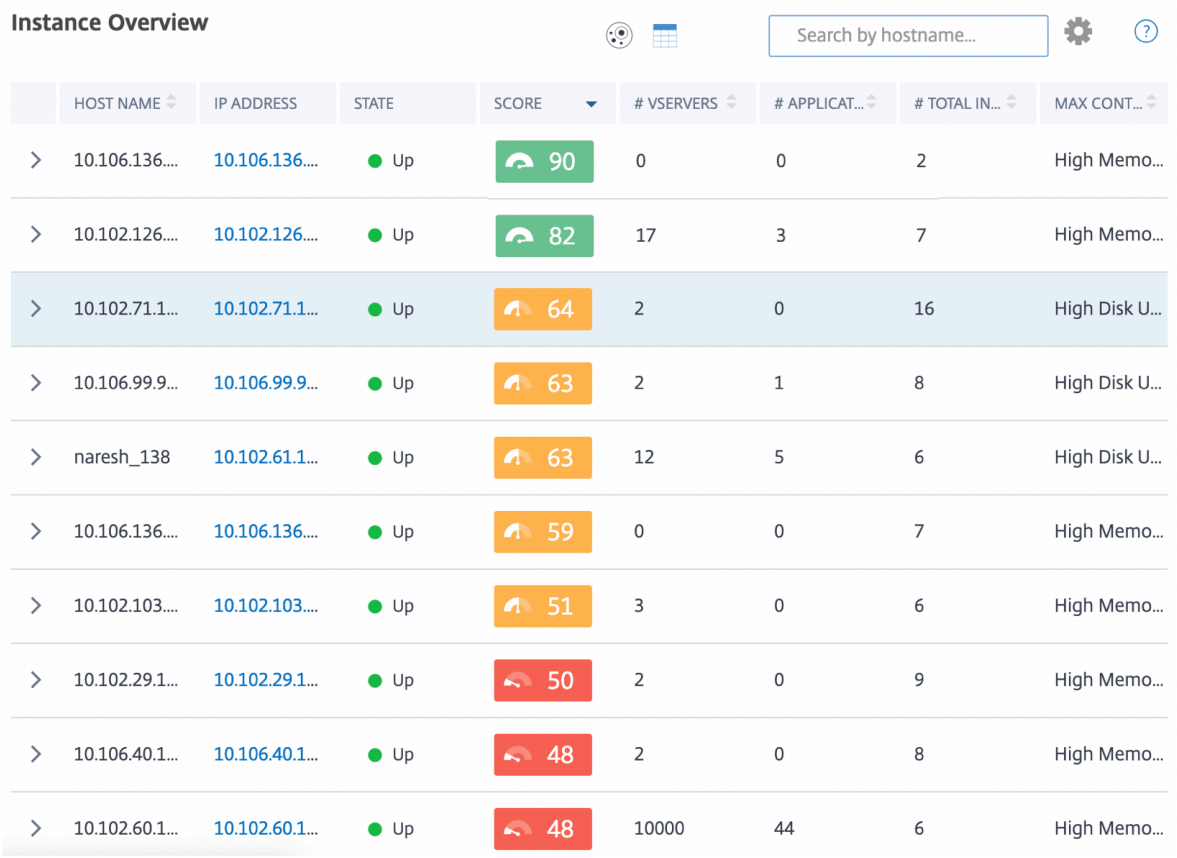


Vue tabulaire

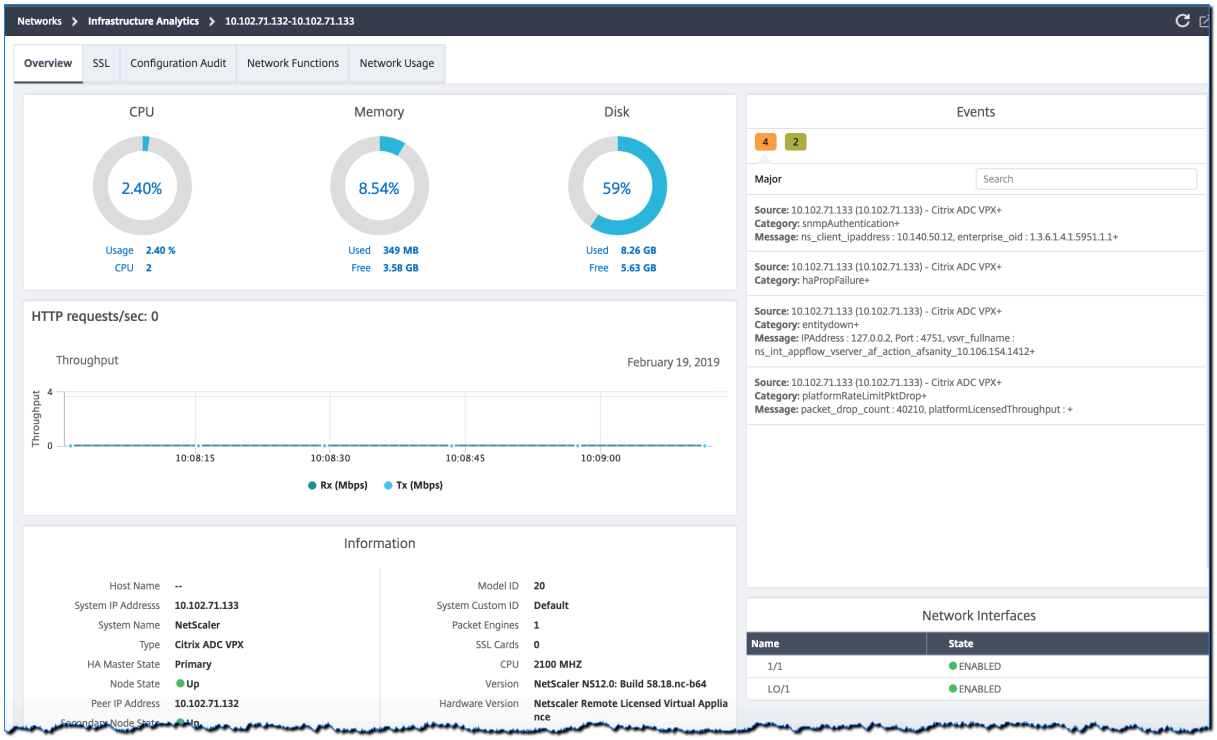
La vue tabulaire affiche les instances et les détails de ces instances dans un format tabulaire. Les détails qui s'affichent sont les suivants :

- 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

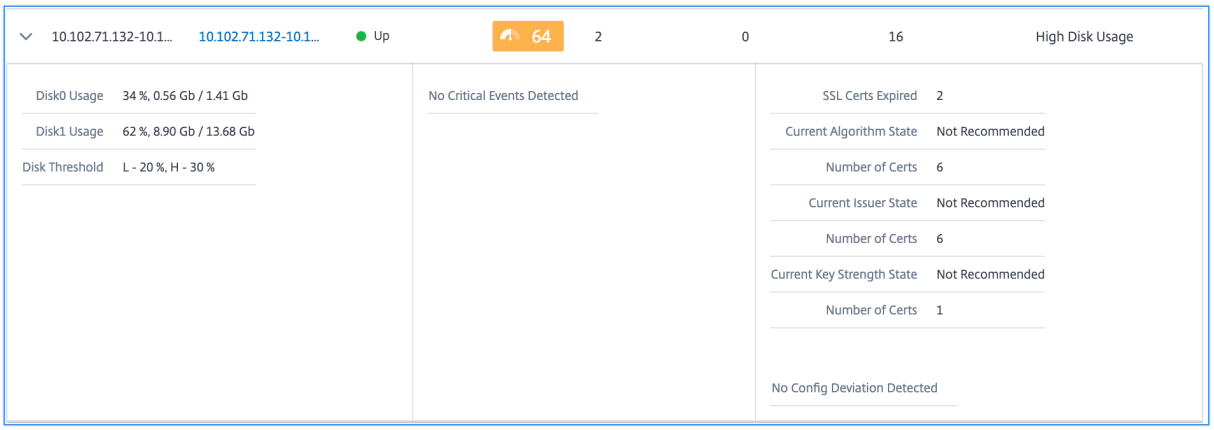
Les instances qui se trouvent dans un état critique figurent en haut du tableau, suivies par les instances qui doivent être examinées, puis par les instances les plus saines.



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.

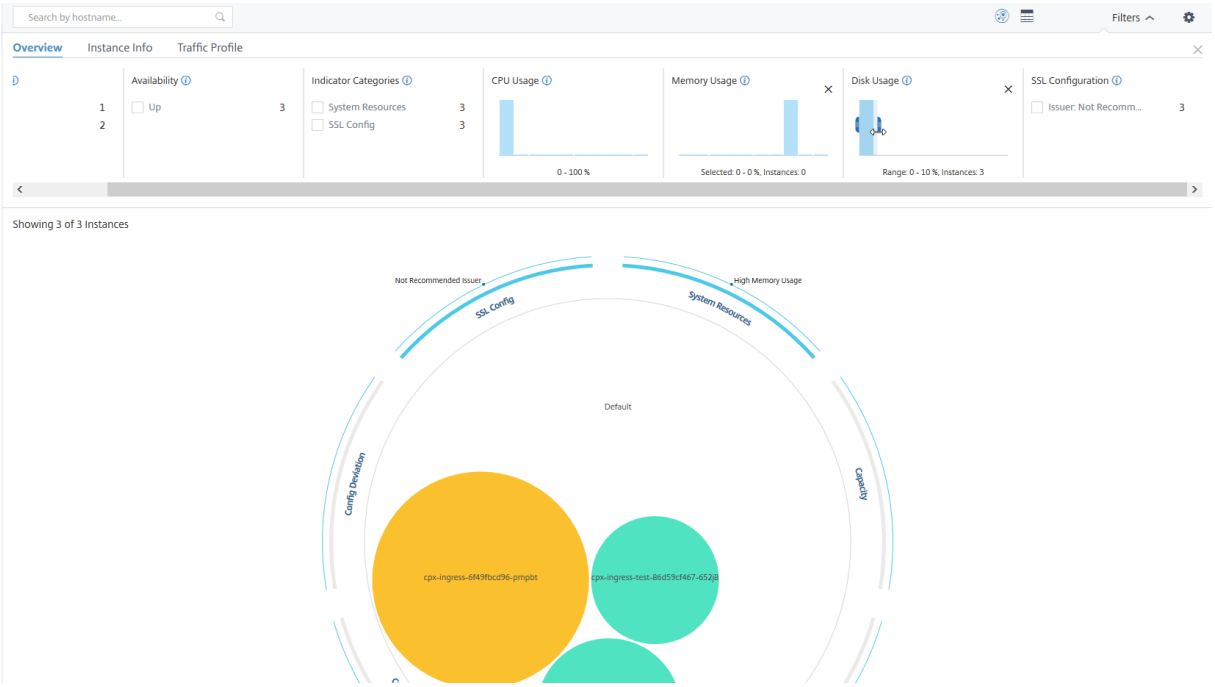
Exemple 2 : Afficher les instances qui consomment entre 10 % et 20 % de la mémoire allouée :

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 :

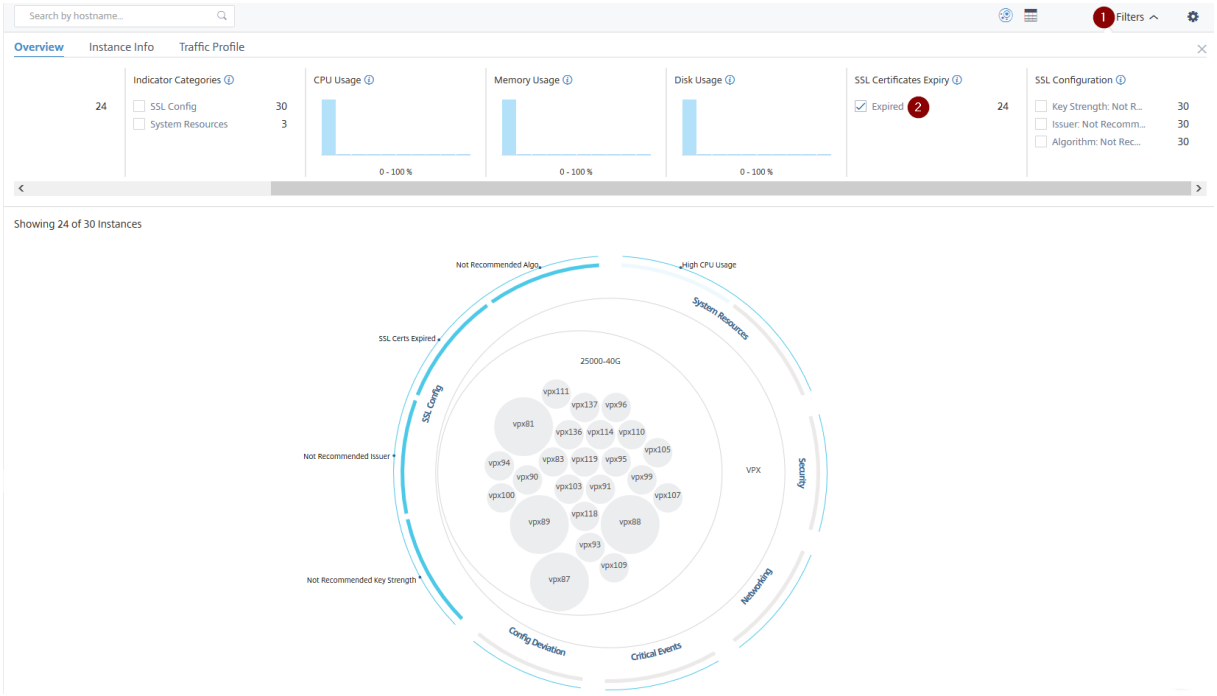
Pour afficher les instances qui ont consommé de l'espace disque entre 0 et 10 %, faites glisser le pointeur de la souris sur les deux plages.



> **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**.

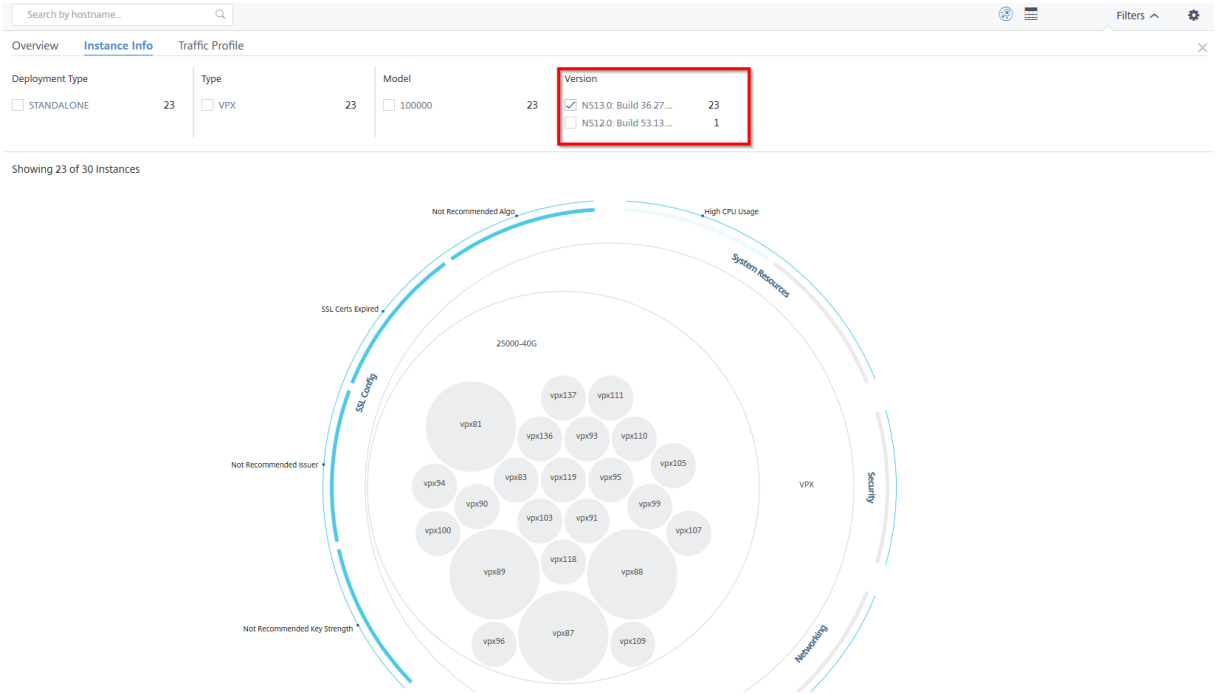
2 - Dans la section **Expiration des certificats SSL**, cochez la case **Expiré** pour afficher les instances.

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 NetScaler VPX avec un numéro de build spécifique :

Sélectionnez la version à afficher.

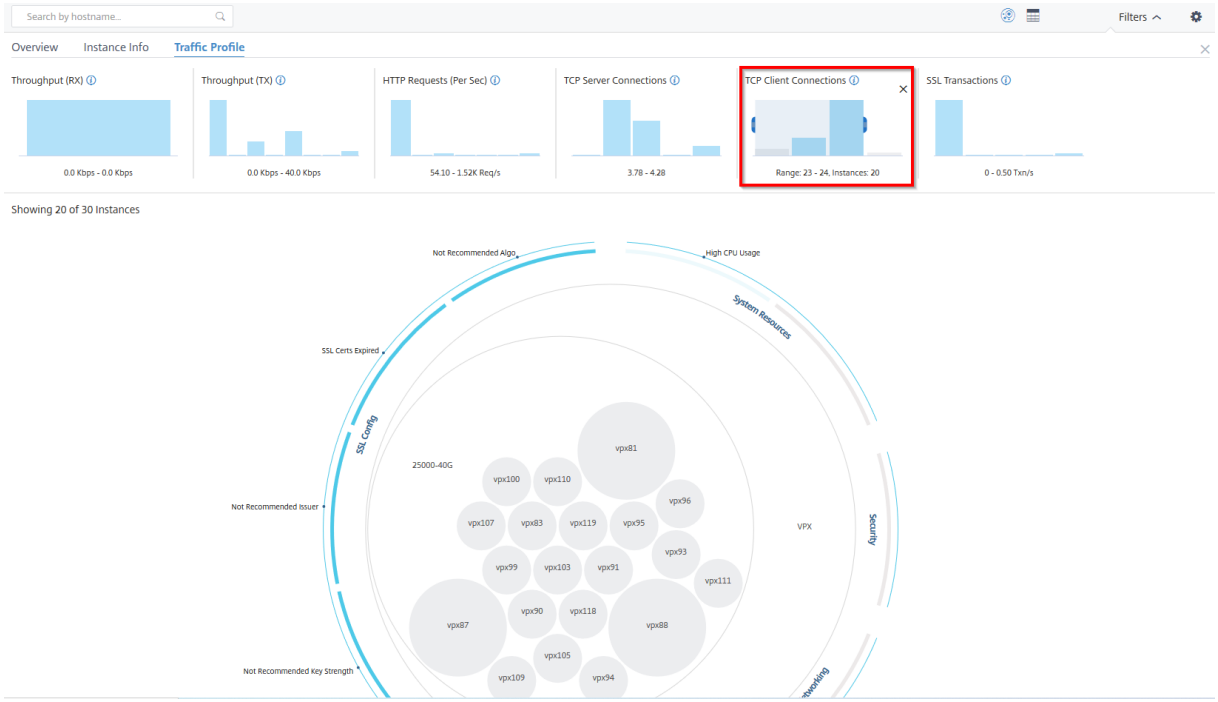


Profil de trafic

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.

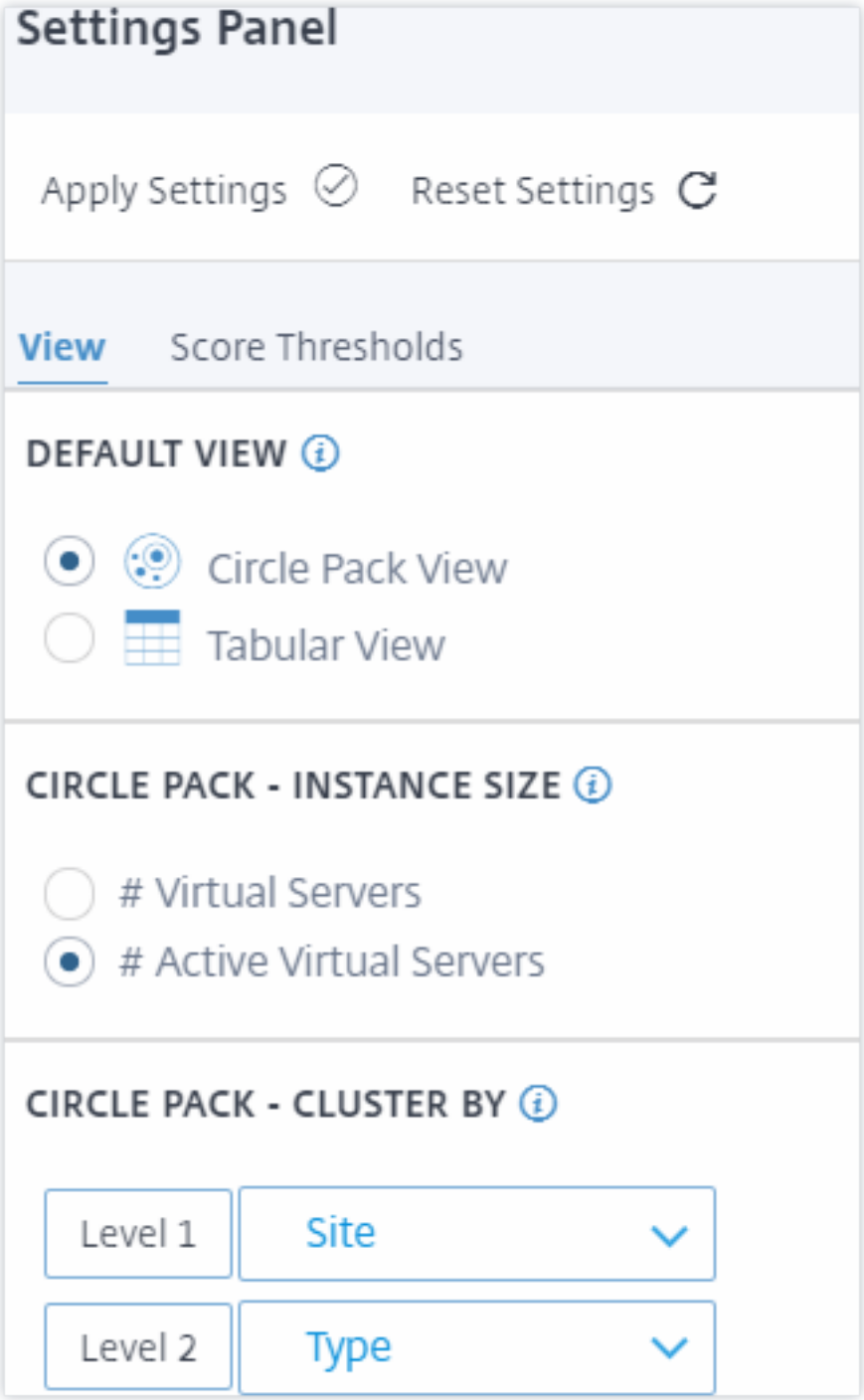


Comment utiliser le panneau des paramètres

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.

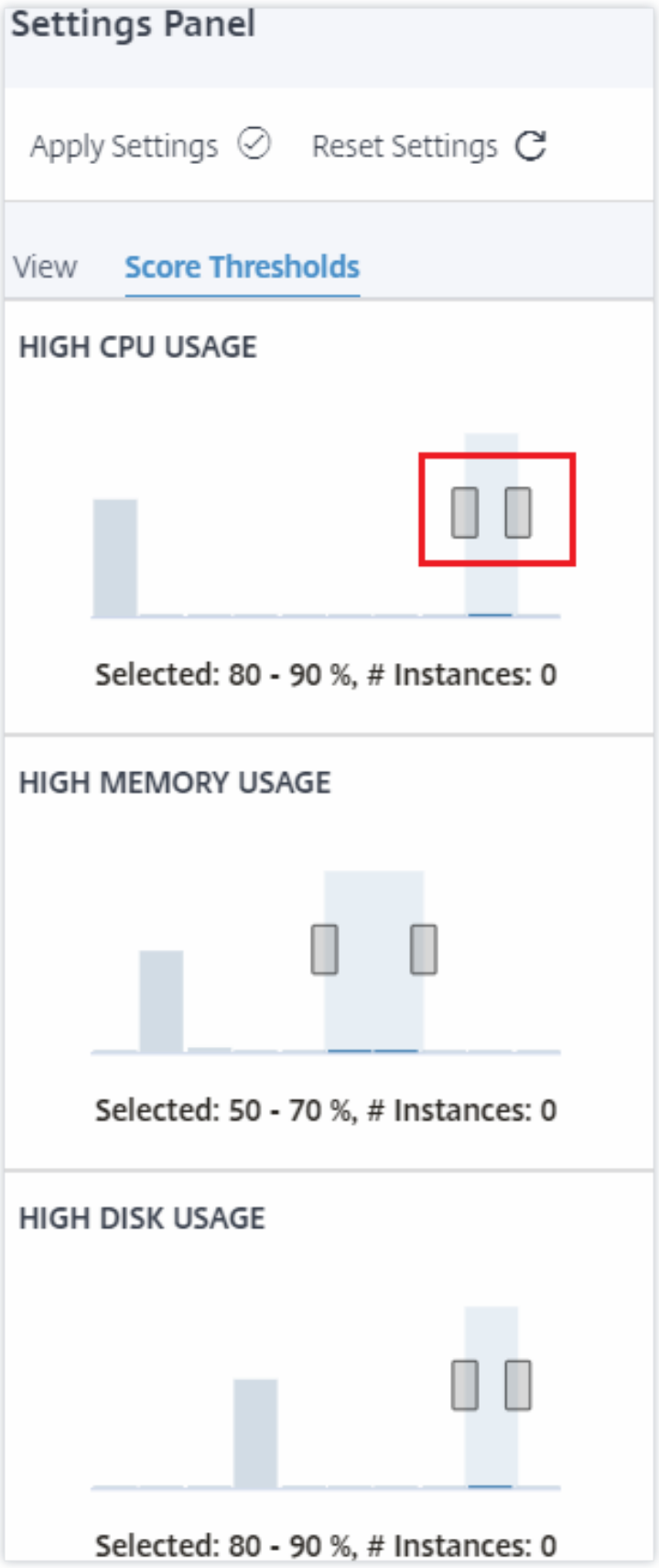
View

- **Vue par défaut**. Sélectionnez **Circle Pack** ou le format tabulaire comme affichage par défaut sur la page d'analyse. Le format que vous sélectionnez correspond à ce que vous voyez chaque fois que vous accédez à la page dans NetScaler 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 NetScaler au sein de 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.

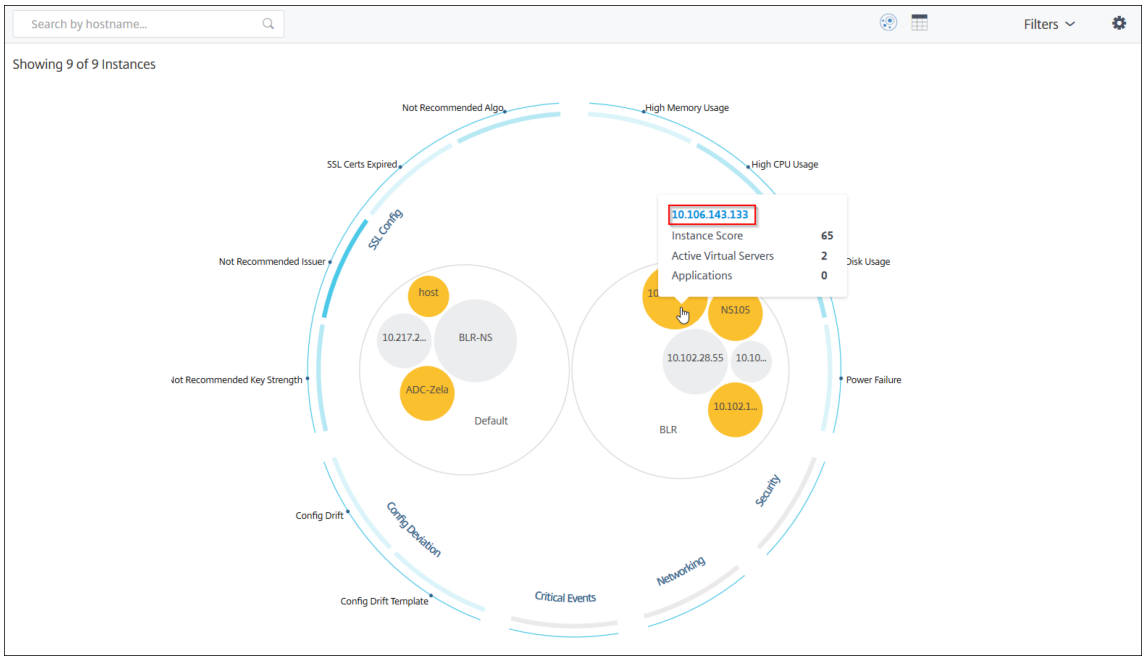
Exemple 2 - Pour surveiller les modifications de configuration :

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.

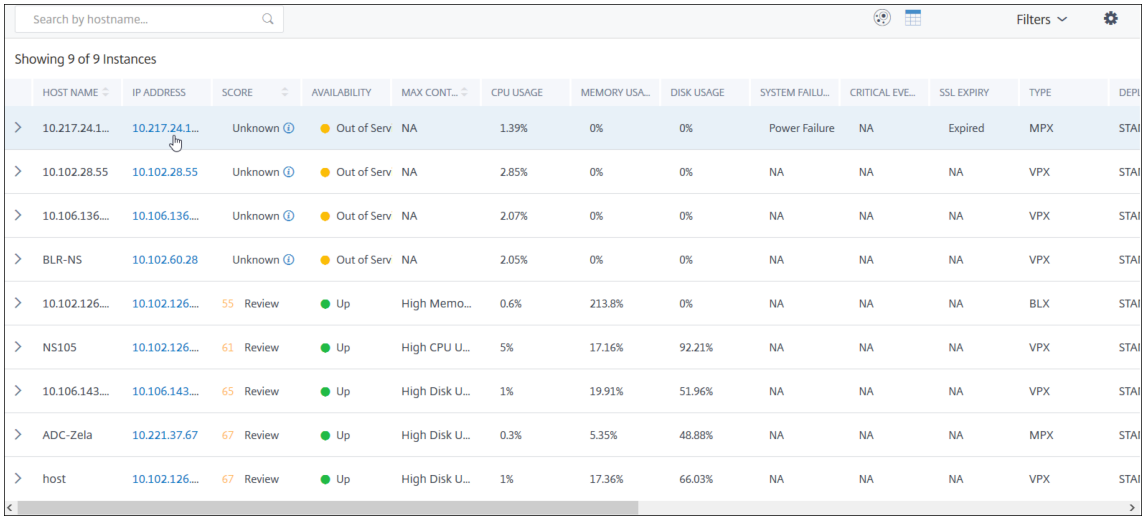
Afficher les détails de l'instance dans Infrastructure Analytics

February 1, 2024

1. Accédez à **Infrastructure > 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

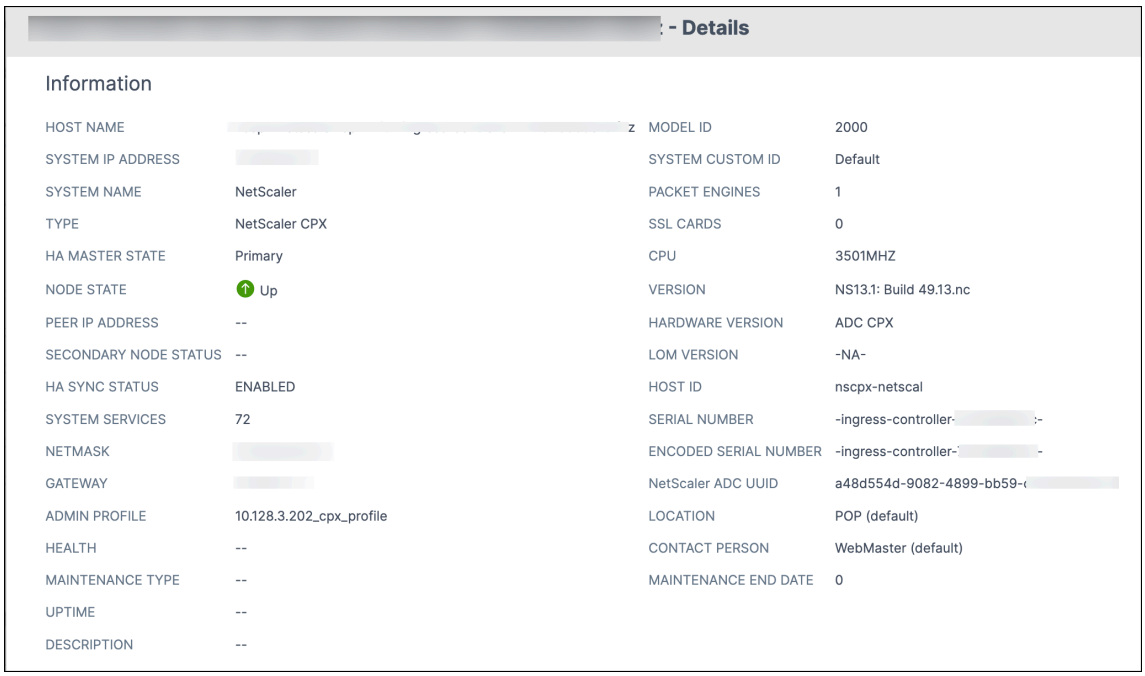
- **Score** —Indique le score de l'instance ADC et le statut (Critical, Good et Fair)
- **Disponibilité** : indique l'état de l'instance ADC, tel que **Up**, **Down**ou **Hors service**.
- **Contribution maximale** : indique la catégorie de problème pour laquelle l'instance ADC a le nombre maximal d'erreurs.
- **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
- **Événements critiques** : indique la catégorie d'événements dans laquelle l'instance NetScaler contient le plus grand nombre 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.

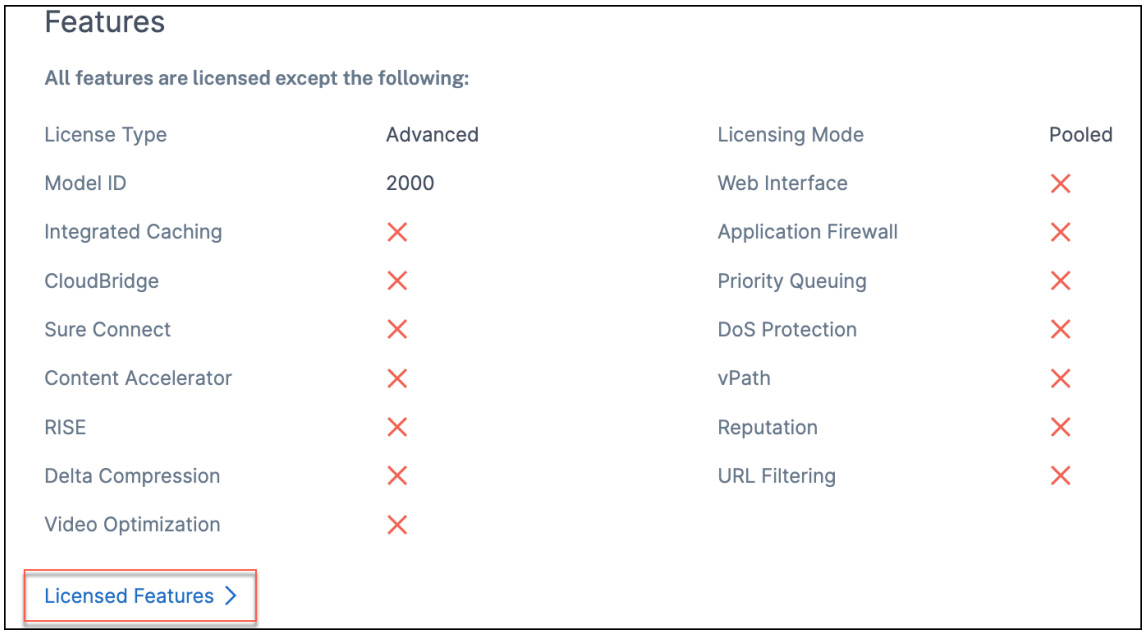
Cliquez sur **Détails de l'instance** pour afficher les détails.

Les détails suivants s'affichent :

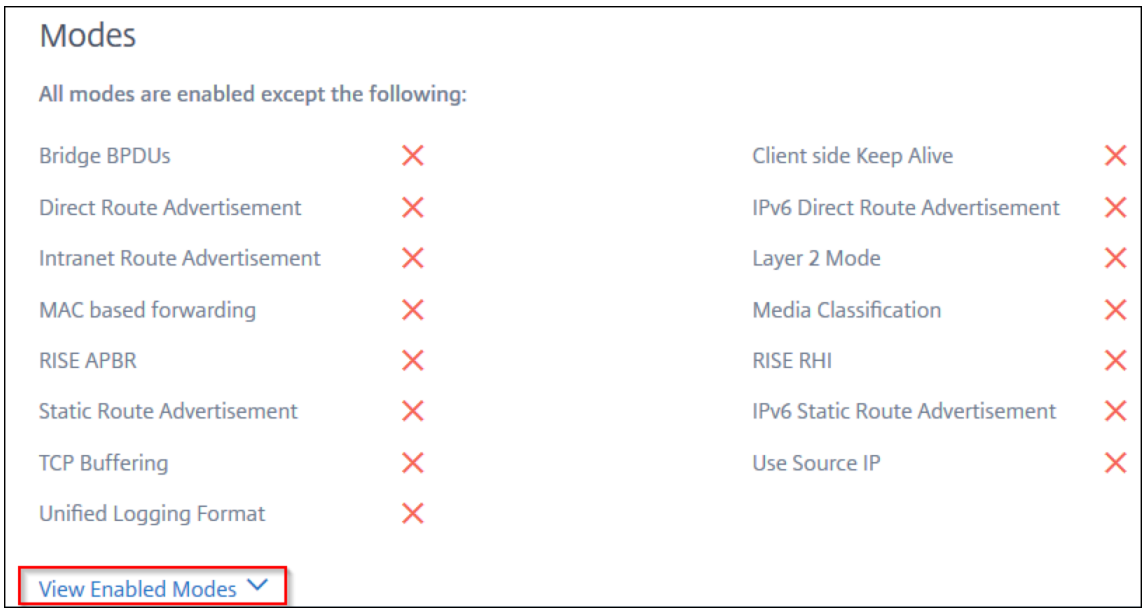
- **Informations** : détails de l'instance tels que le type d'instance, le type de déploiement, la version et le modèle.



- **Fonctionnalités** : par défaut, les fonctionnalités qui ne sont pas sous licence sont affichées. Cliquez sur **Fonctionnalités sous licence** pour afficher les fonctionnalités sous licence.

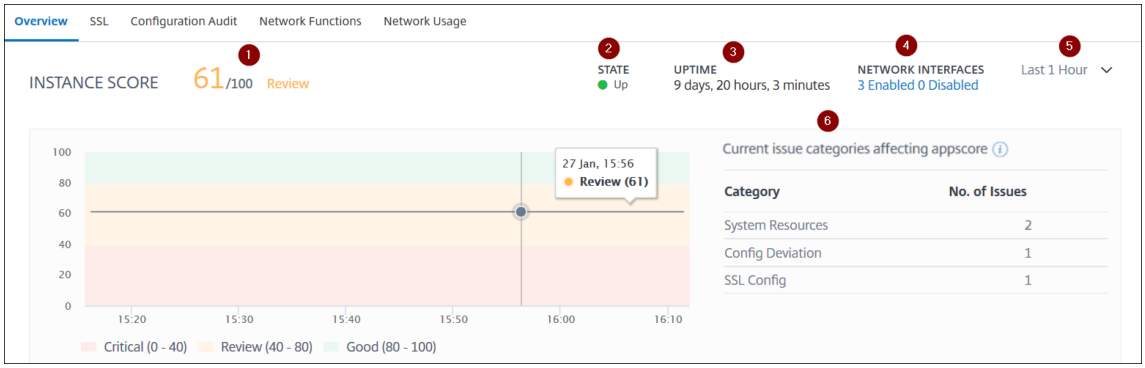


- **Modes** : par défaut, tous les modes désactivés sur l'instance sont affichés. Cliquez sur **Afficher les modes activés** pour afficher les modes activés sur l'instance.



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 NetScaler 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 NetScaler, tel **que**Up **,**Down **et**Out of Service.

3 —Indique la durée pendant laquelle l'instance NetScaler est opérationnelle.

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).

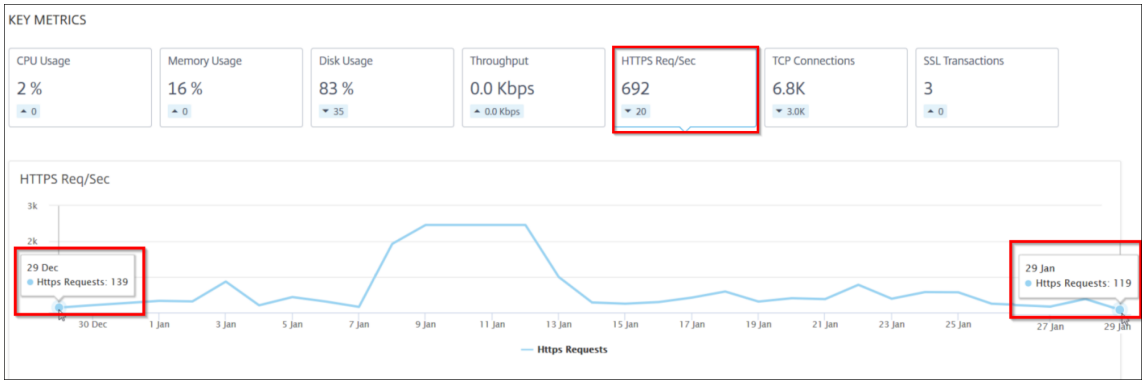
5 —Sélectionnez la durée dans la liste pour afficher les détails de l'instance.

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.

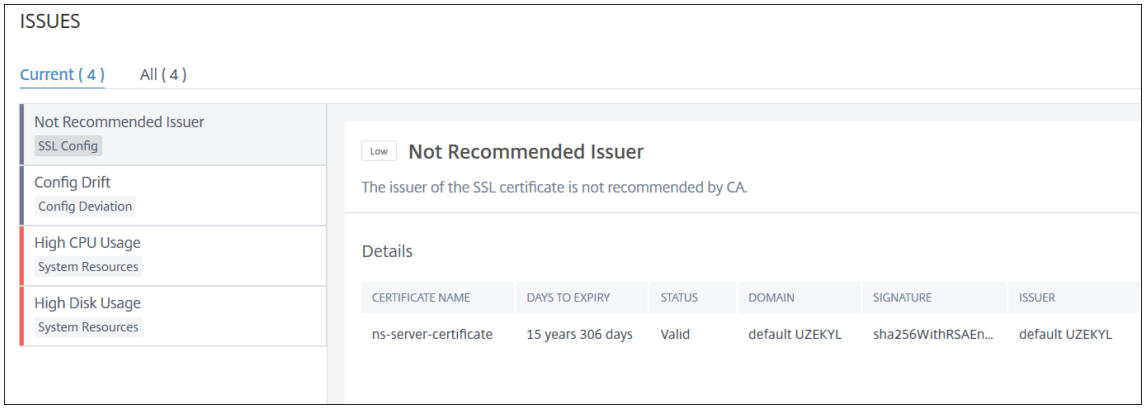
- **Problèmes**

Vous pouvez consulter les problèmes suivants qui se produisent dans l'instance NetScaler :

Catégorie de problème	Description	Problèmes
Ressources système	Affiche tous les problèmes liés aux ressources du système NetScaler tels que le processeur, la mémoire et l'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 NetScaler.	– 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 NetScaler.	– Dérive de configuration – Running vs Template
Événements critiques	Affiche tous les événements critiques liés aux instances NetScaler configurées en paire HA et en cluster.	– Défaillance de l'hélice du cluster – Échec de la synchronisation du cluster

Catégorie de problème	Description	Problèmes
		– Incompatibilité des versions du cluster – HA : mauvais état secondaire – HA Pas de battements de chaleur – Échec de synchronisation HA – Incompatibilité de version HA
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 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 per-

formances 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 **Infrastructure > 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 :

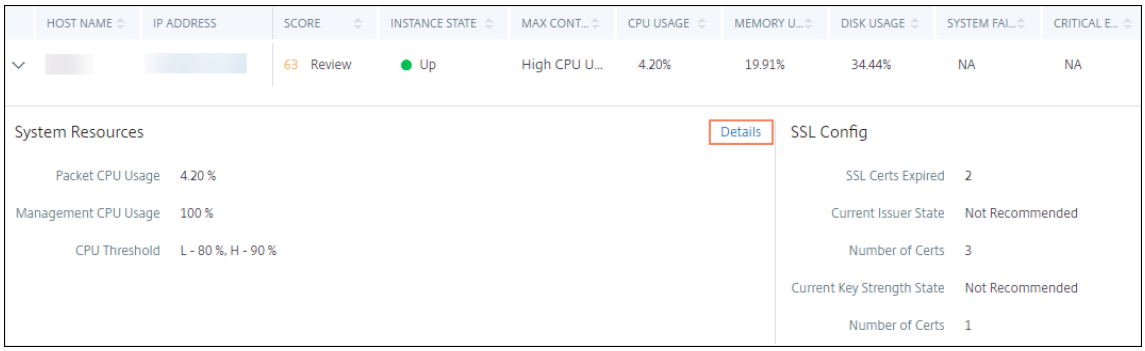
- **Limite de débit atteinte** : nombre de paquets abandonnés dans l'instance une fois la limite de débit atteinte.
- **Limite de processeur PE atteinte** : nombre de paquets déposés sur toutes les cartes réseau une fois que la limite du processeur PE est atteinte.

- **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.

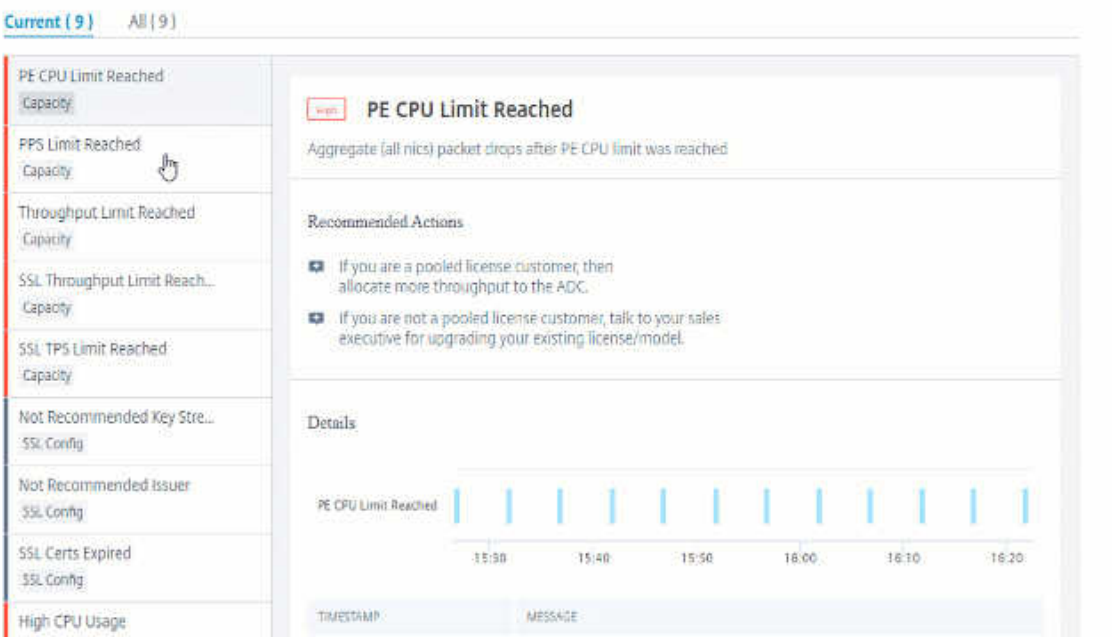
Afficher les actions recommandées pour résoudre les problèmes de capacité

L'ADM recommande des actions susceptibles de résoudre les problèmes de capacité. Pour afficher les actions recommandées, effectuez les opérations suivantes :

1. Dans **Infrastructure > 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 NetScaler ADM Infrastructure Analytics, vous pouvez :

- Découvrez un nouvel ensemble de problèmes opérationnels qui surviennent dans les instances NetScaler.
- Consultez les messages d'erreur et consultez les recommandations pour résoudre les problèmes.

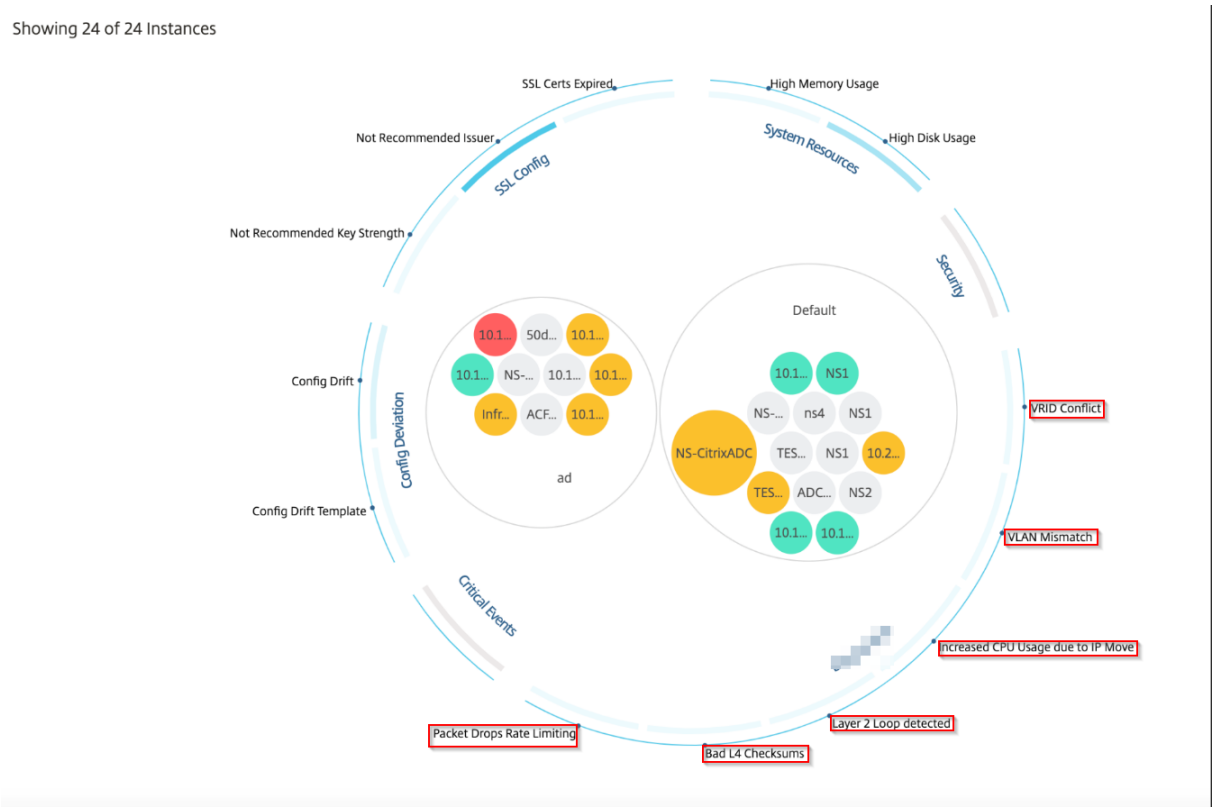
En tant qu'administrateur, vous pouvez rapidement identifier la cause première des problèmes et analyser les problèmes.

> **Remarque**
>
> Les indicateurs de règles ne sont pas supportés pour :
>
> - Instances NetScaler configurées en mode cluster.
> - Instances NetScaler configurées avec des partitions d'administration.

Dans NetScaler ADM, accédez à **Infrastructure > Analyse de l'infrastructure pour afficher des** indicateurs pour :

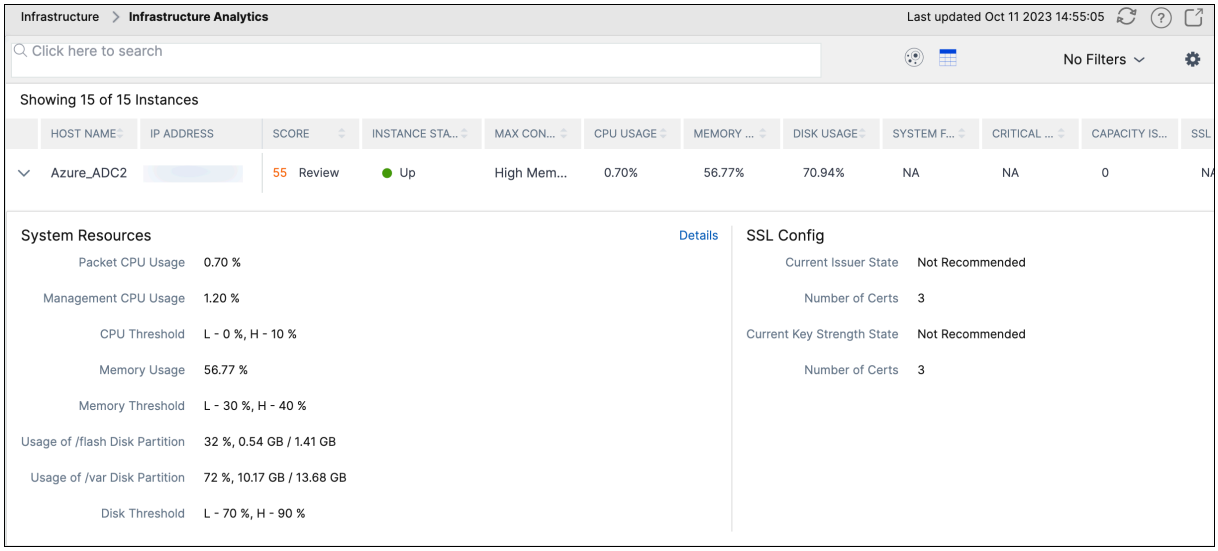
Nom de l'indicateur dans Infrastructure Analytics	Description
Échec de l'allocation de port	Détecte lorsque NetScaler utilise le SNIP pour communiquer avec une nouvelle connexion au serveur et que le nombre total de ports disponibles sur ce SNIP est épuisé. L'action recommandée consiste à ajouter un 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 le nombre maximum d'accès est imposé à la mémoire NetScaler.
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.



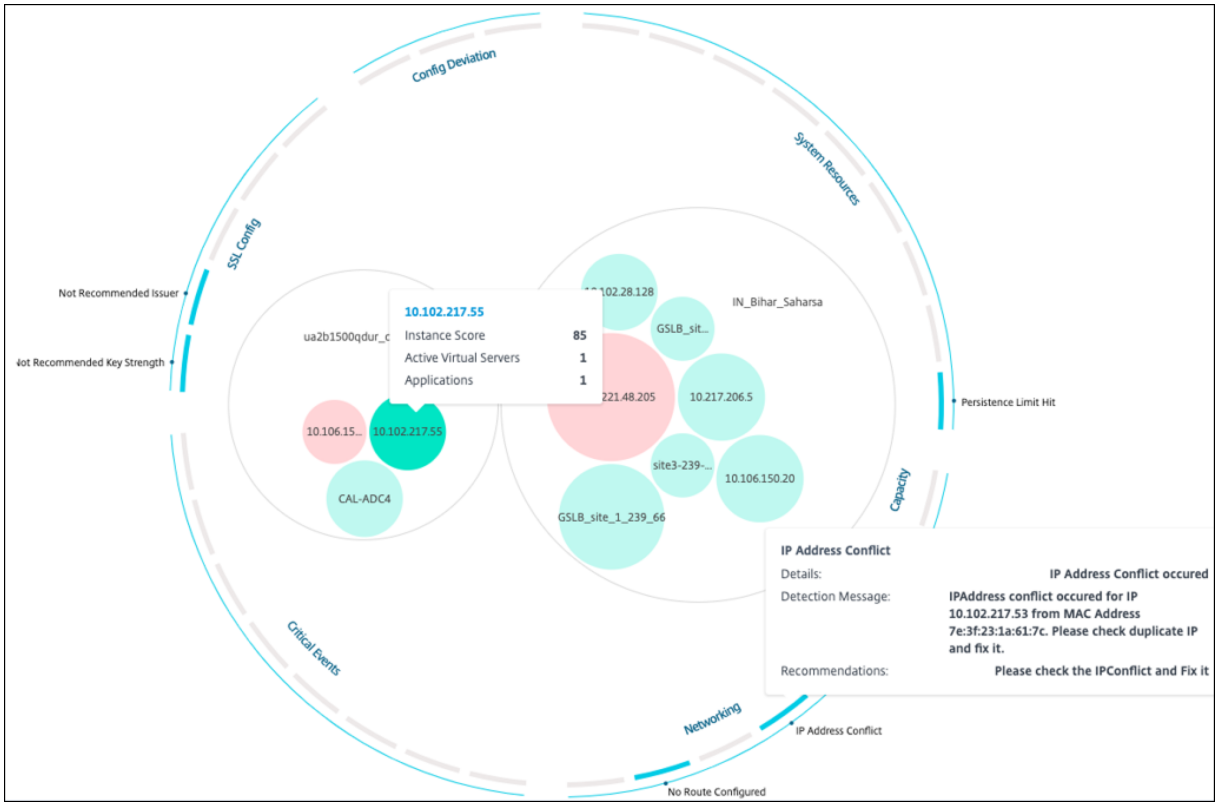
Vue tabulaire

Vous pouvez également afficher les anomalies à l'aide de l'option Vue tabulaire dans **Infrastructure Analytics**. Accédez à **Infrastructure > 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

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 NetScaler Application Delivery Management (ADM). Vous devez ajouter des instances à NetScaler ADM pour les surveiller. Les instances peuvent être ajoutées lorsque vous configurez NetScaler ADM ou version ultérieure. Une fois que vous avez ajouté des instances à NetScaler ADM, elles sont continuellement interrogées afin de collecter des informations qui peuvent ensuite être utilisées pour résoudre des problèmes ou sous forme de 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 première configuration du serveur NetScaler ADM ou ultérieurement. Pour ajouter des instances, vous devez spécifier le nom d'hôte ou l'adresse IP de chaque instance NetScaler, ou une plage d'adresses IP.

Pour savoir comment ajouter une instance à NetScaler ADM, consultez Ajouter des instances àNetScaler ADM.

Lorsque vous ajoutez une instance au serveur NetScaler ADM, le serveur s'ajoute implicitement en tant que destination piège pour l'instance et collecte l'inventaire de l'instance. Pour en savoir plus, consultez la section [Comment NetScaler ADM découvre]les instances.(/en-us/netscaler-application-delivery-management-software/current-release/overview/how-mas-discovers-instances.html)

Après avoir ajouté une instance, vous pouvez la supprimer en accédant à **Infrastructure > Instances** et en cliquant sur **Toutes les instances**. Sur la page Instances, sélectionnez l'instance à supprimer et cliquez sur **Supprimer**.

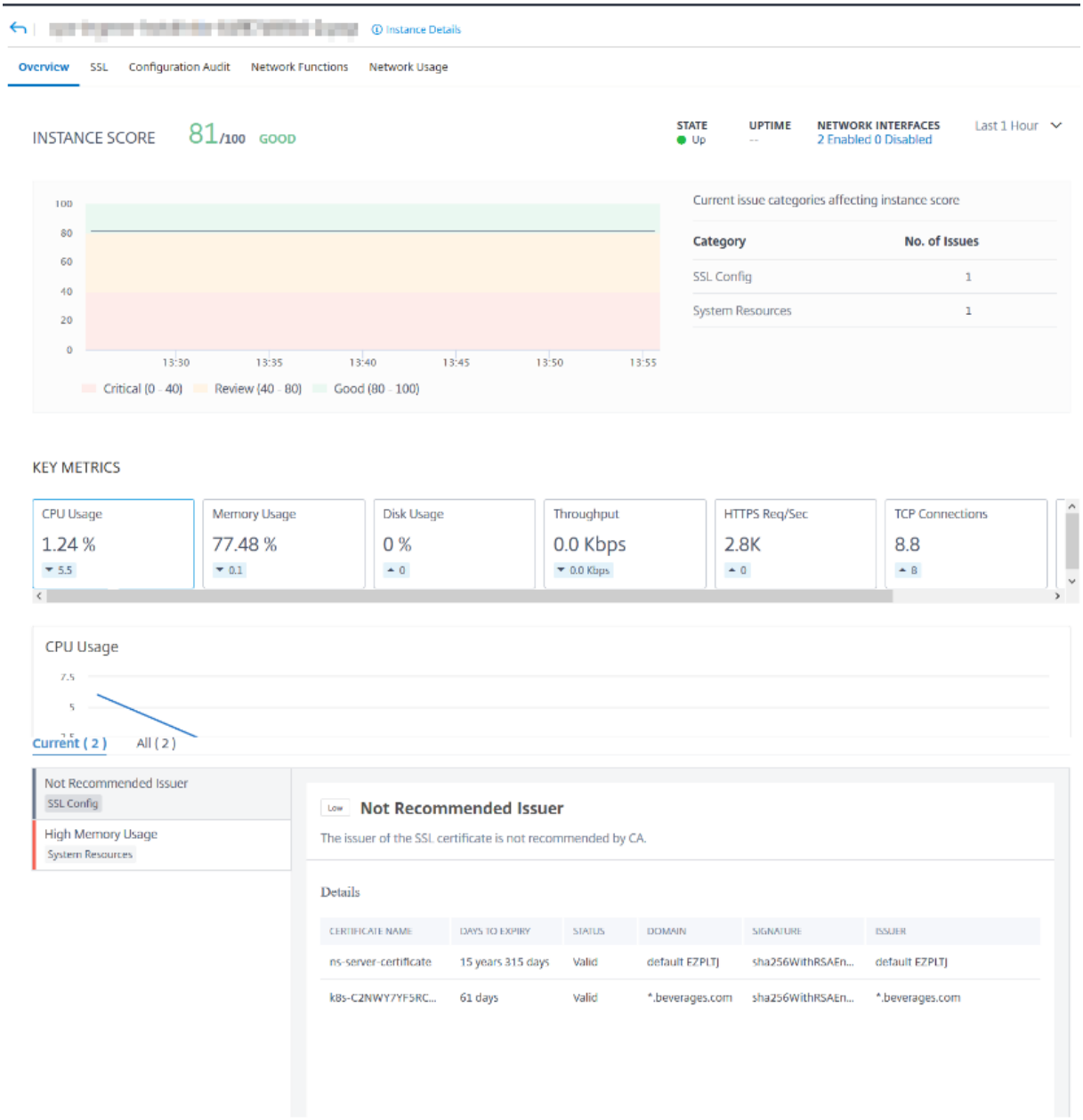
Comment utiliser le tableau de bord de l'instance

Le tableau de bord par instance de NetScaler 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 **Infrastructure > 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 NetScaler que vous avez 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.

Geomaps dans NetScaler Application Delivery Management (ADM) vous fournit une représentation graphique de vos sites et répartit votre expérience de surveillance réseau par zone géographique. Avec les géomaps, vous pouvez visualiser la distribution de votre instance réseau par emplacement et surveiller les problèmes réseau.

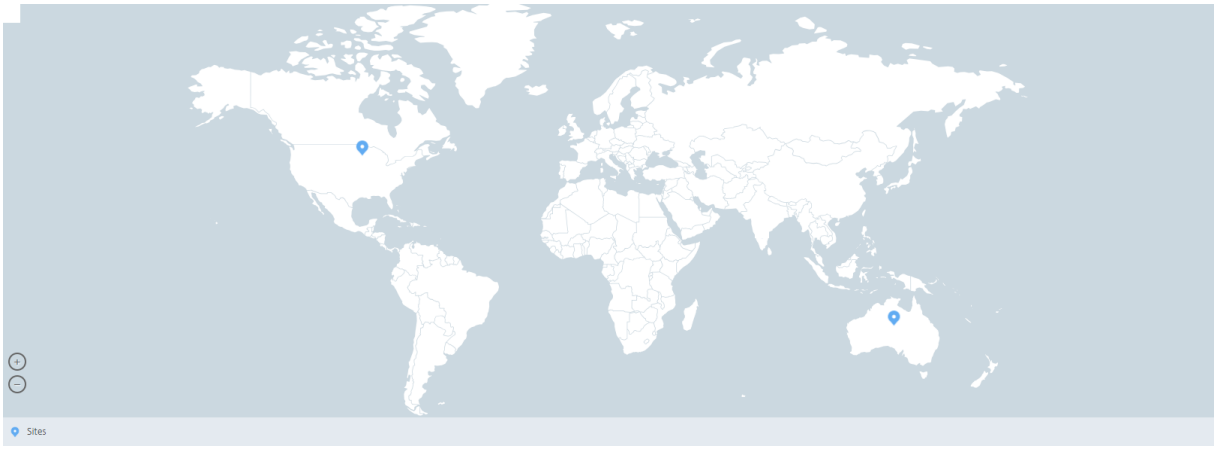
La section suivante explique comment surveiller les centres de données dans NetScaler ADM.

Le site NetScaler ADM est un regroupement logique d'instances Citrix Application Delivery Controller (ADC) situées 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. NetScaler ADM gère et surveille toutes les instances NetScaler connectées à tous les sites. Vous pouvez utiliser NetScaler ADM pour surveiller et collecter le syslog, AppFlow, le SNMP et toutes les données de ce type provenant des instances gérées.

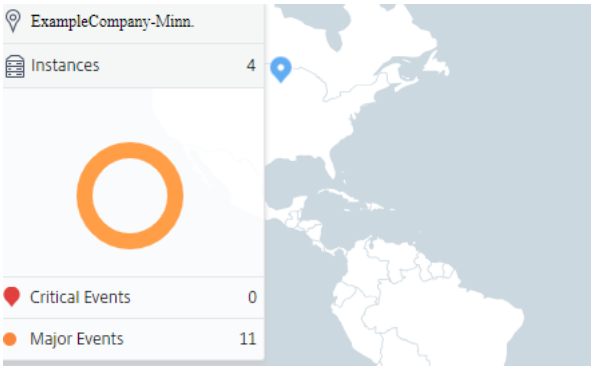
Les géomaps de NetScaler ADM vous fournissent une représentation graphique de vos sites. Geomaps décompose également votre expérience de surveillance réseau par zone géographique. Avec les géomaps, vous pouvez visualiser la distribution de votre instance réseau par emplacement et surveiller tous les problèmes réseau. Vous pouvez accéder à la page **Infrastructure > Instances** 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.

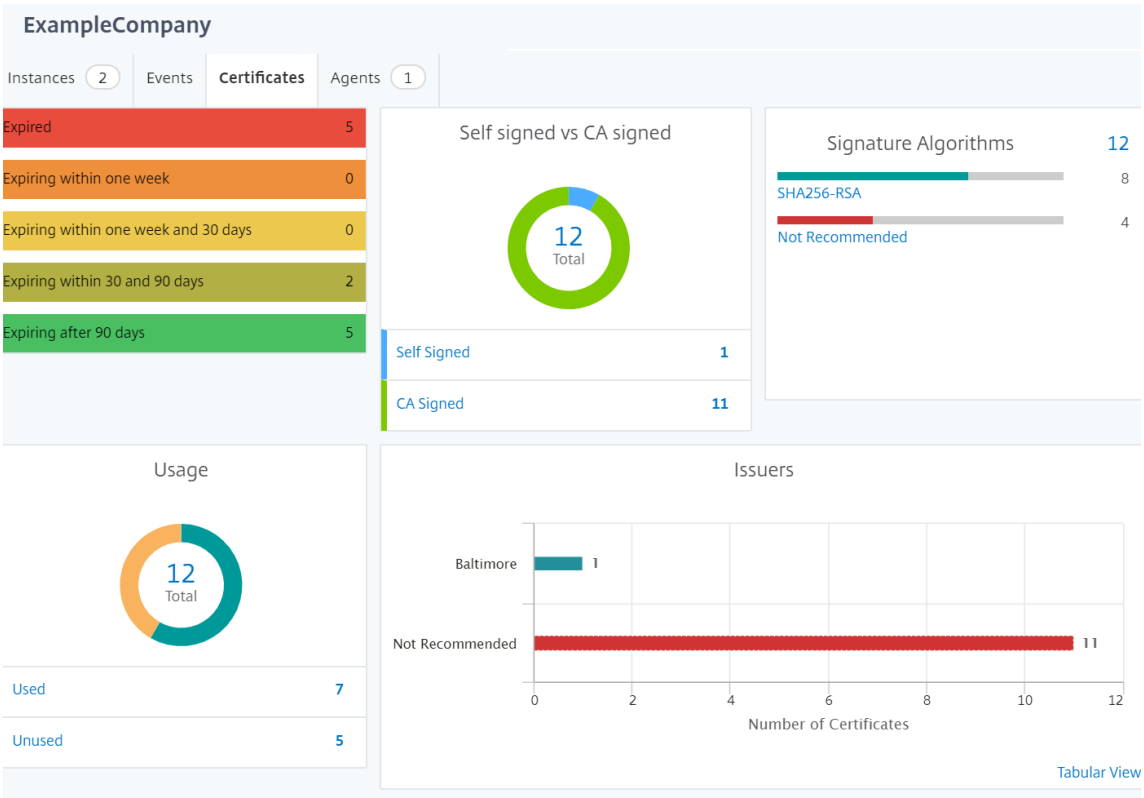


Cliquez sur les onglets pour afficher plus d'informations :

- 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 déclenchés sur une instance NetScaler.

- 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 NetScaler dans NetScaler ADM. Vous devez également ajouter l'instance au site, ajouter un agent et lier l'agent au site. NetScaler ADM reconnaît ensuite le site auquel appartiennent l'instance NetScaler et l'agent.

Pour plus d'informations sur l'ajout d'instances NetScaler, consultez la section Ajout d'instances.

Pour créer des sites :

Créez des sites avant d'ajouter des instances dans NetScaler ADM. Fournir des informations de localisation vous permet de localiser le site avec précision.

Accédez à**Infrastructure > Instances > Sites**, puis cliquez sur**Ajouter**.

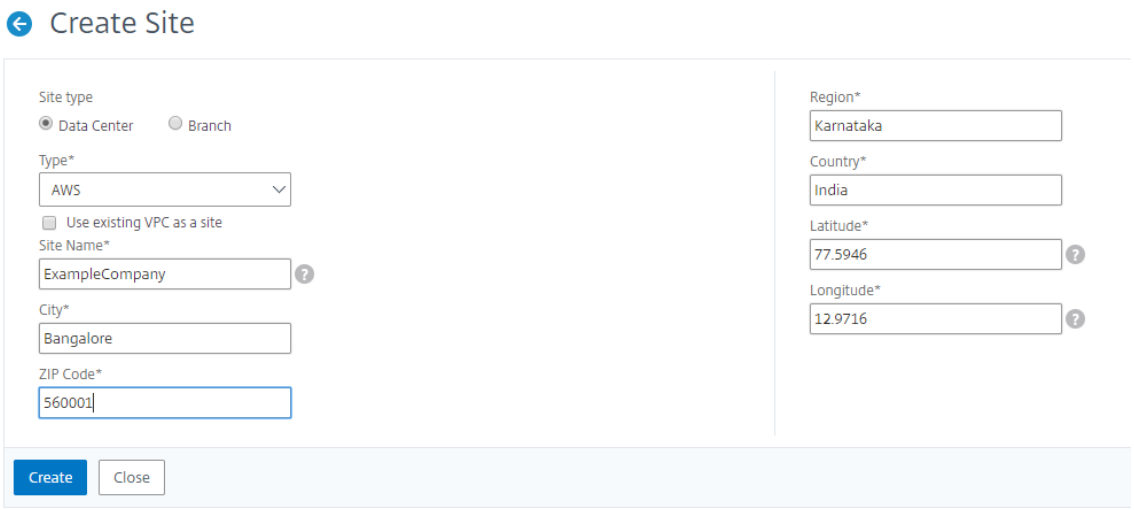
1. Dans la page**Créer un site**, spécifiez les informations suivantes :
    a) **Type de site** : Sélectionnez un **centre de données**.

    > **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**.

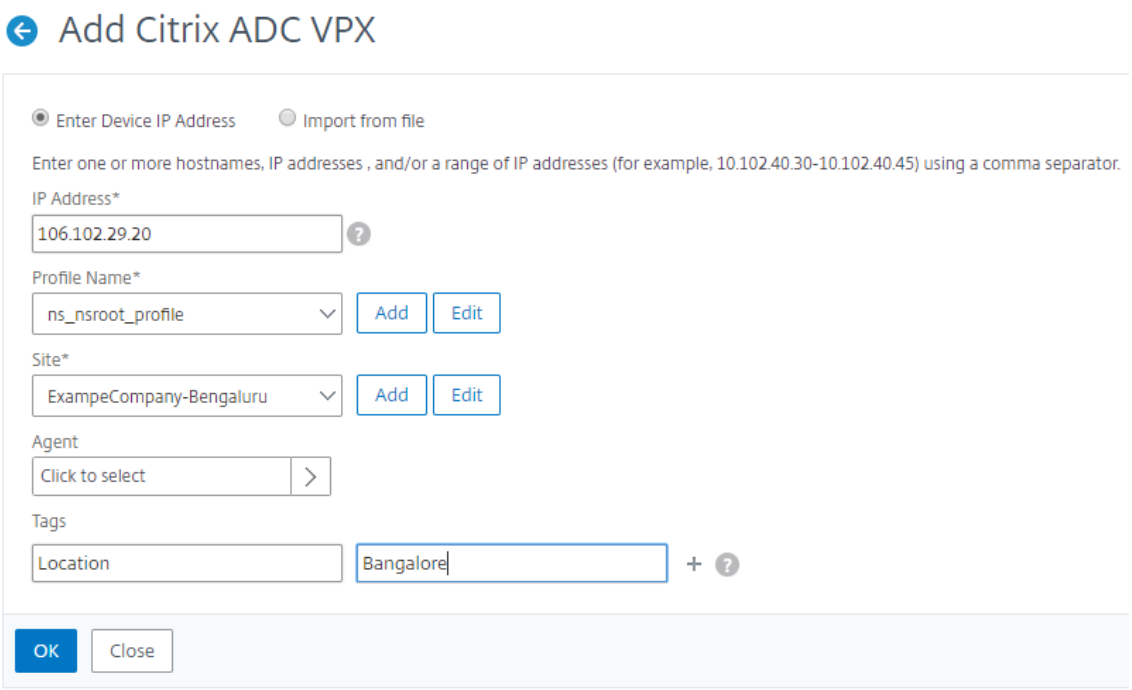


Pour ajouter des instances et sélectionner des sites :

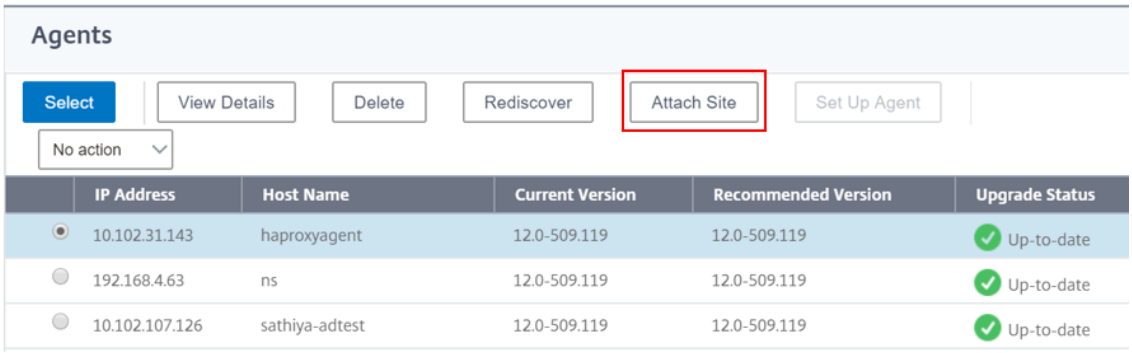
Après avoir créé des sites, vous devez ajouter des instances dans NetScaler ADM. Vous pouvez sélectionner le site précédemment créé, ou vous pouvez également créer un site et associer l'instance.

Après avoir créé des sites, vous devez ajouter des instances dans NetScaler ADM. Vous pouvez sélectionner le site précédemment créé, ou vous pouvez également créer un site et associer l'instance.

1. Dans NetScaler ADM, accédez à **Infrastructure > Instances**.
2. Sélectionnez le type d'instance à créer, puis cliquez sur **Ajouter**.
3. Sur la page **Ajouter NetScaler VPX**, saisissez 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**.

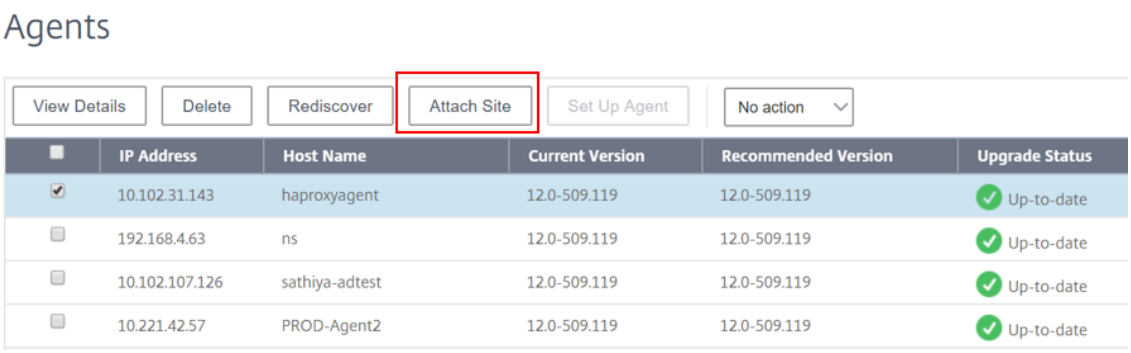


1. Sélectionnez le site dans la liste et cliquez sur **Enregistrer**.
1. Cliquez sur **OK**.

Vous pouvez également attacher un agent à un site en accédant à **Infrastructure > Instances > Agents**.

Pour associer un agent NetScaler ADM au site :

1. Dans NetScaler ADM, accédez à **Infrastructure > Instances > Agents**.
2. Sélectionnez l'agent, puis cliquez sur **Joindre le site**.



1. Vous pouvez associer le site et cliquer sur **Enregistrer**.

NetScaler ADM commence à surveiller les instances NetScaler ajoutées sur le site de Bangalore ainsi que les instances des deux autres sites.

Comment créer des balises et affecter des instances

February 1, 2024

NetScaler 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.

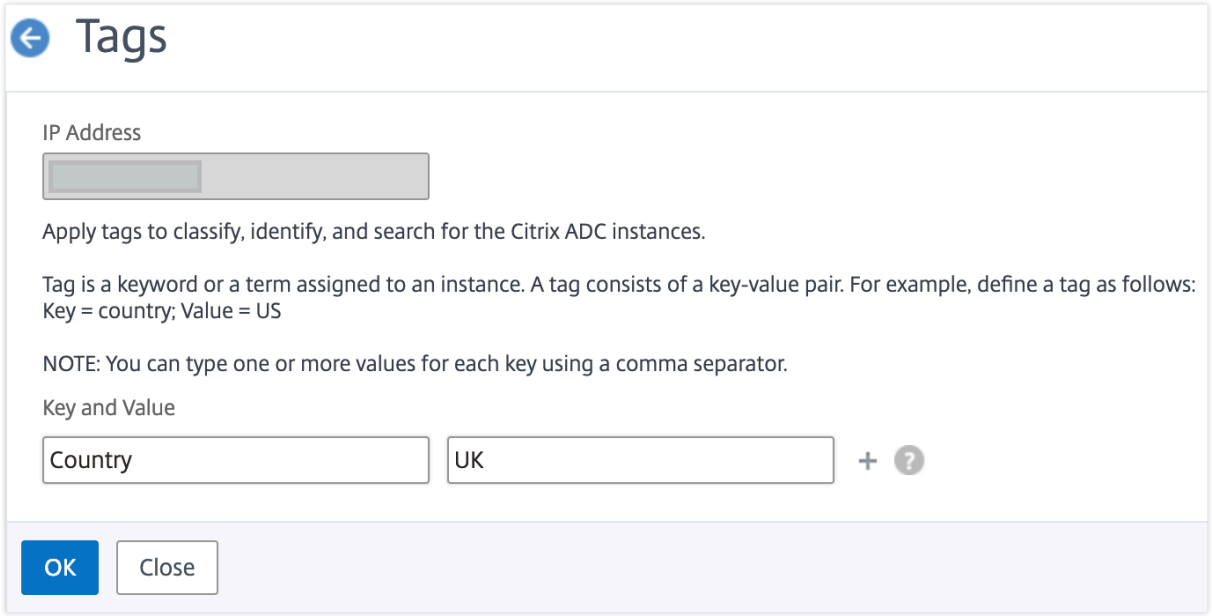
- **Cas d'utilisation 1** : Vous pouvez créer une balise pour identifier toutes les instances au Royaume-Uni. Ici, vous pouvez créer une balise avec la clé « Pays » et la valeur « UK ». Cette balise vous aide à rechercher et à surveiller toutes ces instances au Royaume-Uni.
- **Cas d'utilisation 2** : 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** : imaginez une situation dans laquelle vous souhaitez connaître la liste des instances NetScaler situées dans la région de « Swindon » au Royaume-Uni et détenues par vous, David T. Vous pouvez créer des balises pour toutes ces exigences et les attribuer à toutes les instances qui répondent à ces conditions.

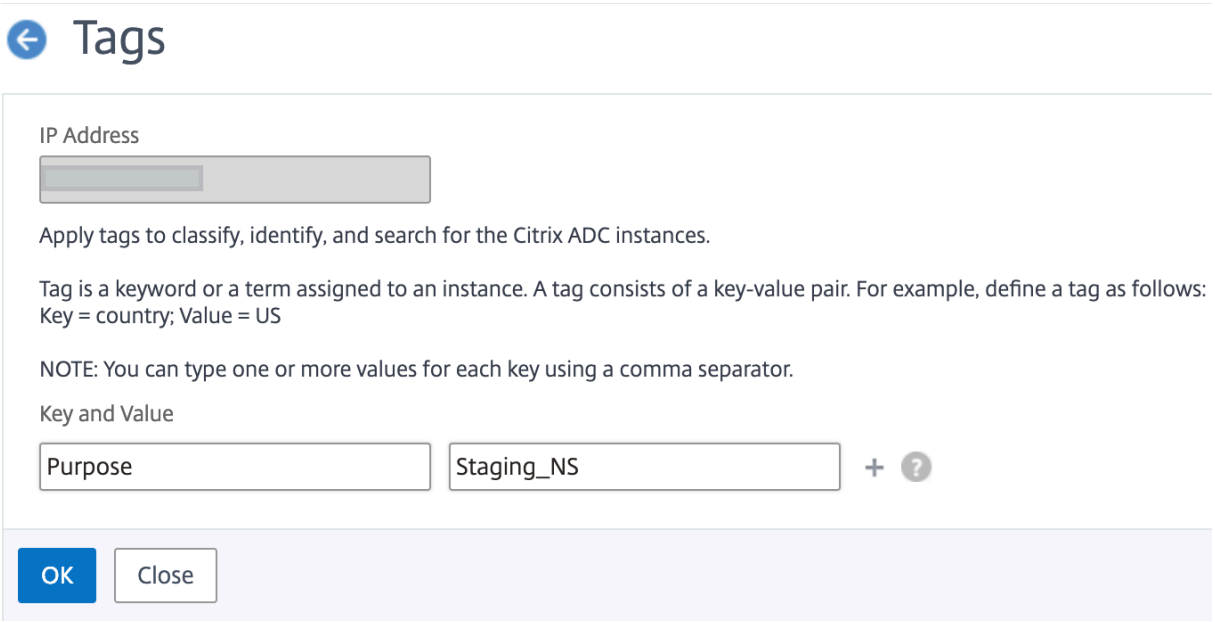
Pour attribuer des balises à une instance NetScaler VPX :

1. Dans NetScaler ADM, accédez à **Infrastructure > Instances**NetScaler.
2. Sélectionnez l'onglet **NetScaler VPX** .
3. Sélectionnez le NetScaler VPX requis.
4. Cliquez sur **Balises**.
5. Créez des balises et cliquez sur **OK**.

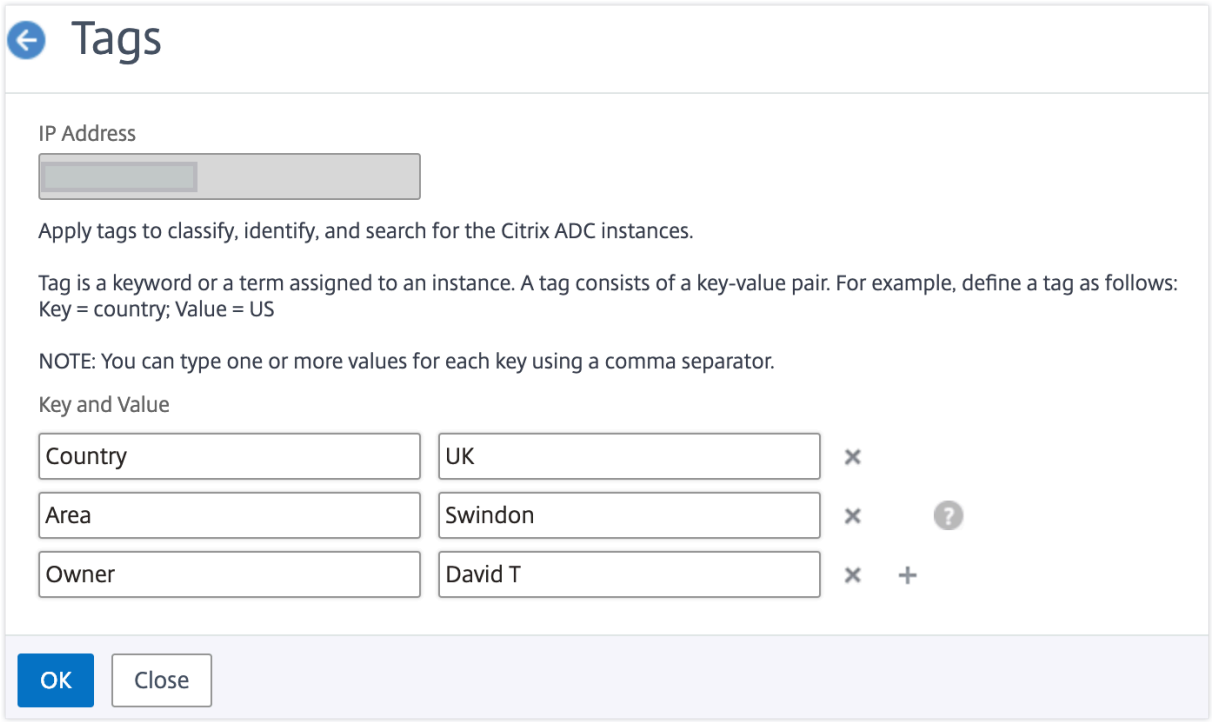
La fenêtre **Balises** qui s'affiche vous permet de créer vos propres paires « clé-valeur » en affectant des valeurs à chaque mot clé que vous créez.

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.



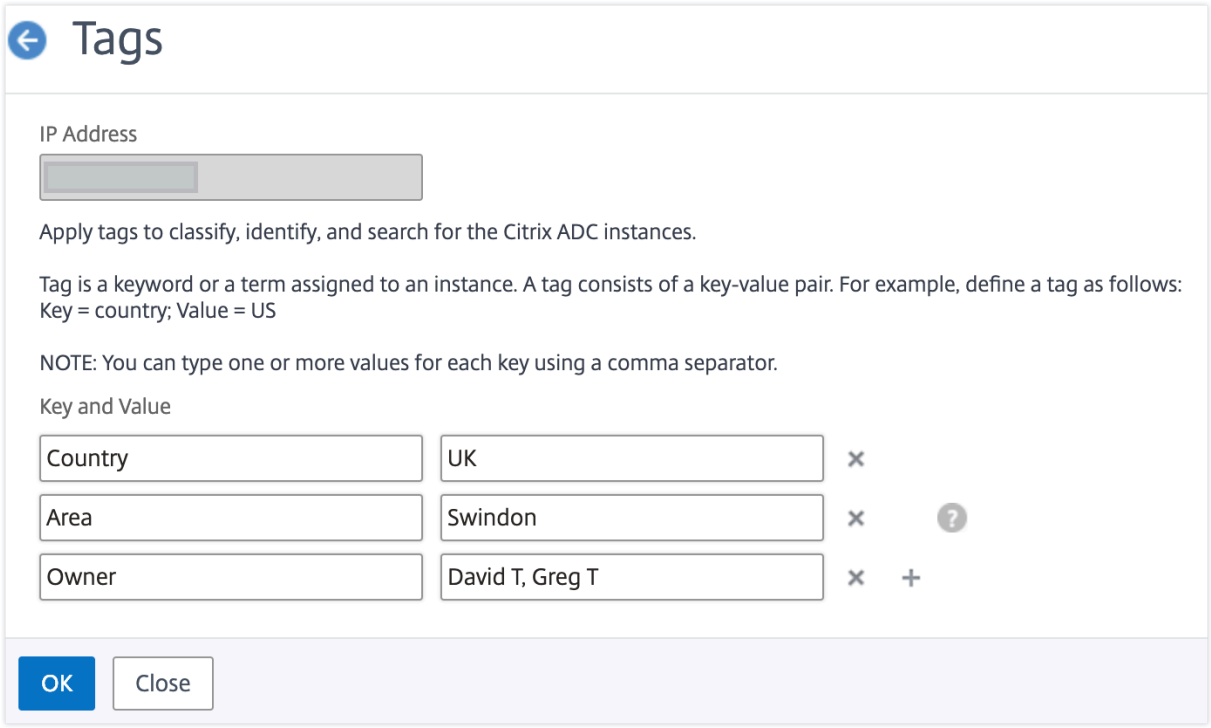


Vous pouvez également ajouter plusieurs balises en cliquant sur « +. » L'ajout de balises multiples et significatives vous permet de rechercher efficacement les instances.



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. NetScaler 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

Il se peut que NetScaler Application Delivery Management (ADM) gère de nombreuses instances NetScaler. En tant qu'administrateur, vous pouvez avoir la possibilité de rechercher dans l'inventaire des instances en fonction de certains paramètres. NetScaler ADM offre désormais une fonctionnalité de recherche améliorée permettant de rechercher un sous-ensemble d'instances NetScaler 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 NetScaler pour ajouter une description supplémentaire à propos de l'instance NetScaler.

Vous pouvez désormais associer vos instances NetScaler à des balises. Ces balises peuvent être utilisées pour mieux identifier les instances NetScaler et effectuer des recherches sur celles-ci.

- **Propriétés**. Chaque instance NetScaler ajoutée dans NetScaler ADM possède 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 NetScaler qui sont sur la version 12.0 et qui sont à 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.

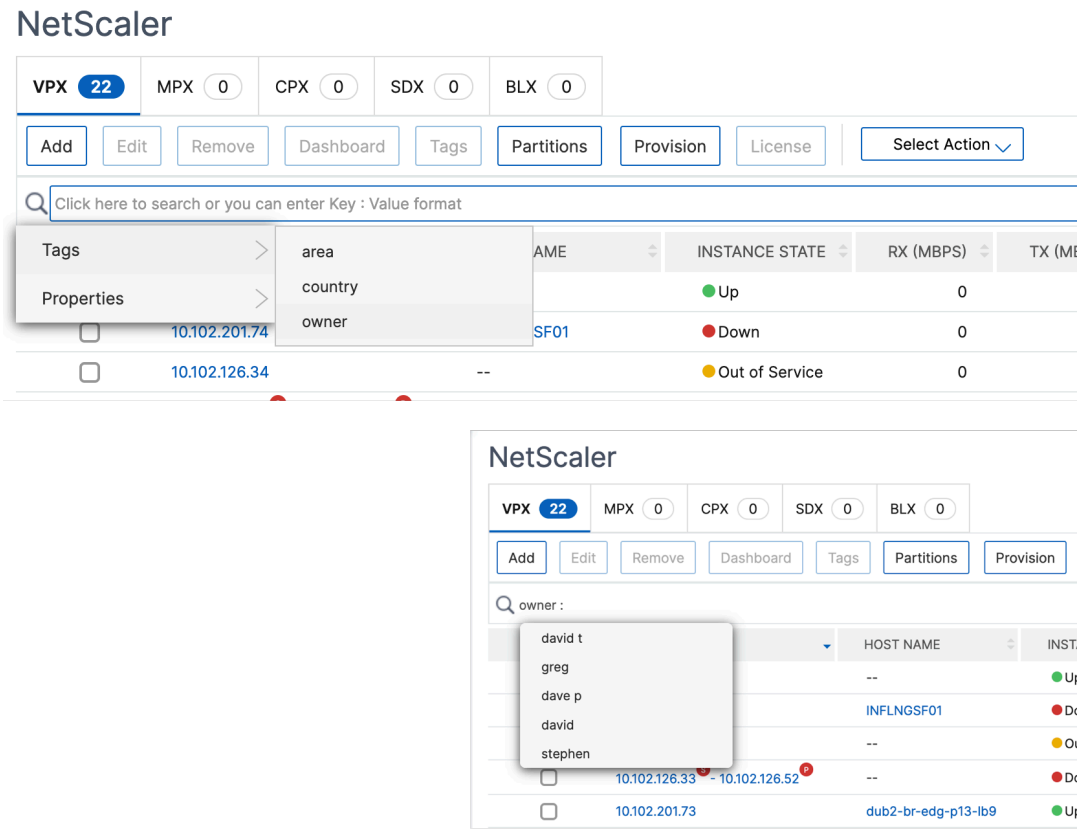
Vous pouvez utiliser une combinaison de balises et de propriétés pour créer vos propres critères de recherche.

Pour rechercher des instances NetScaler VPX

1. Dans NetScaler ADM, accédez à **Infrastructure > Instances > NetScaler** > onglet **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.

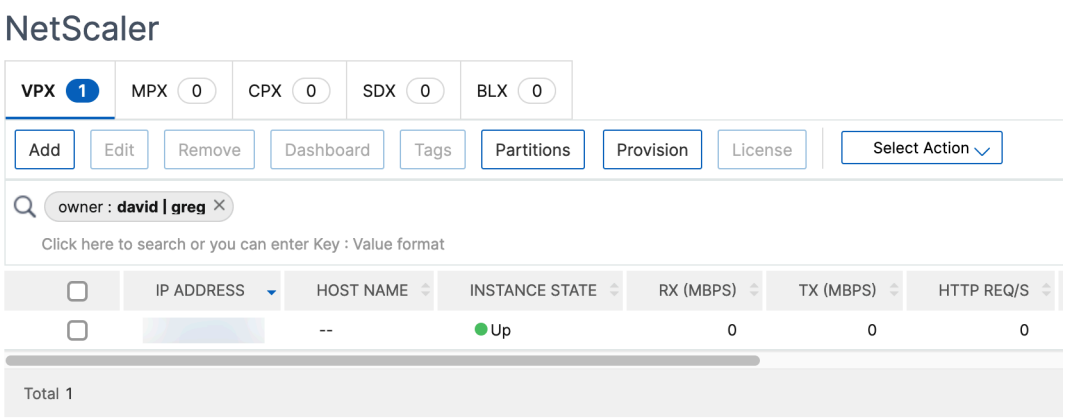
   Les exemples suivants montrent comment utiliser efficacement l'expression de recherche pour rechercher l'instance.

   a) Sélectionnez l'option **Balises** et sélectionnez **Propriétaire**. Sélectionnez « David T. »

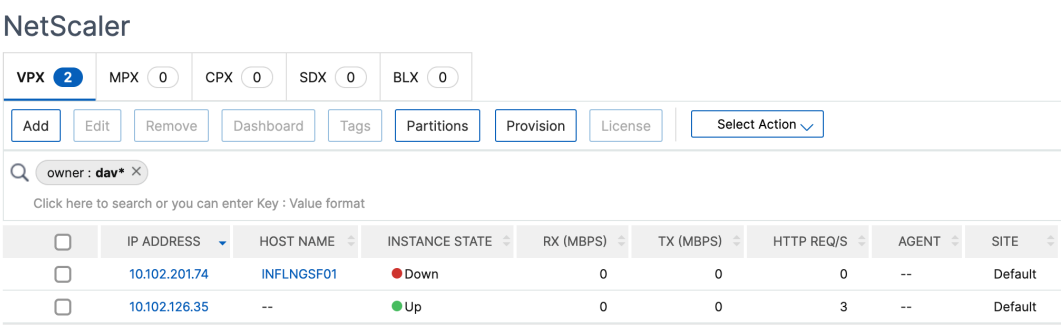


NetScaler ADM prend en charge les expressions régulières et les caractères génériques dans les expressions de recherche.

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.

Gestion des partitions d'administration des instances NetScaler

February 1, 2024

Vous pouvez configurer des partitions d'administration sur vos instances Citrix Application Delivery Controller (ADC) afin que différents groupes de votre organisation se voient attribuer des partitions différentes sur la même instance NetScaler. Un administrateur réseau peut être chargé de gérer plusieurs partitions sur plusieurs instances NetScaler.

NetScaler Application Delivery Management (ADM) permet de gérer facilement toutes les partitions détenues par 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 NetScaler ADM. Lorsque vous découvrez une instance NetScaler, les partitions d'administration configurées sur cette instance NetScaler sont automatiquement ajoutées au système.

Supposons que vous disposez de deux instances NetScaler VPX avec deux partitions configurées sur chaque instance. Par exemple, l'instance NetScaler 10.102.216.49 possède Partition_1, Partition_2 et Partition_3, et l'instance NetScaler 10.102.29.120 possède p1 et p2, comme illustré dans l'image suivante.

Pour afficher les partitions, accédez à **Infrastructure > Instances > NetScaler > 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.

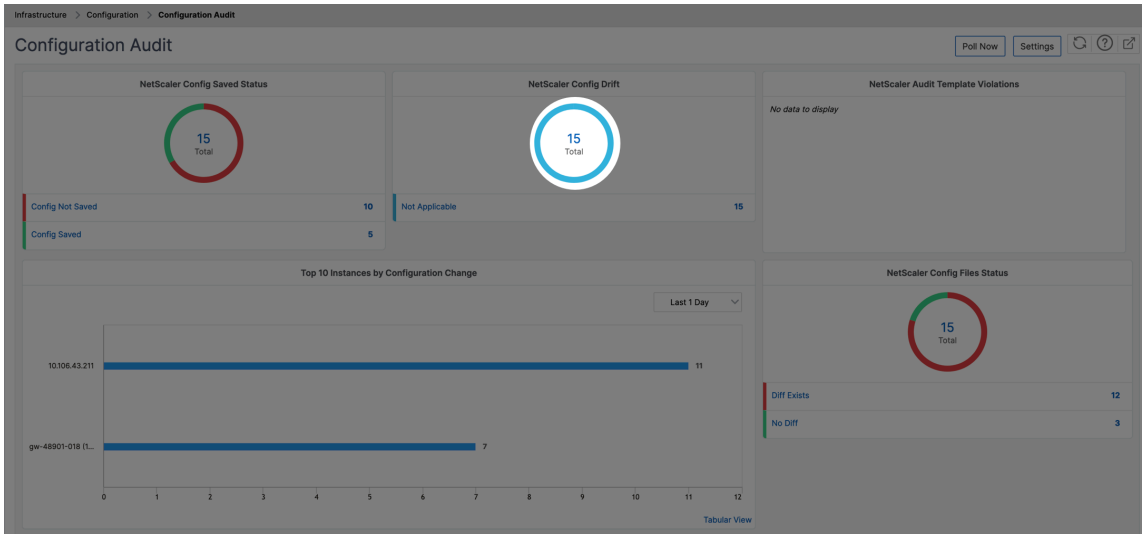
Tout d'abord, vous devez créer deux groupes avec les autorisations appropriées (par exemple : permissions admin) et inclure les instances de partition admin requises dans chaque groupe. Par exemple, créez le groupe de systèmes partition1-admin et ajoutez les partitions d'administration NetScaler 10.102.29.120-p1 et 10.102.216.49-Partition_1 à ce groupe. Créez également le groupe système partition2-admin et ajoutez les partitions d'administration NetScaler 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

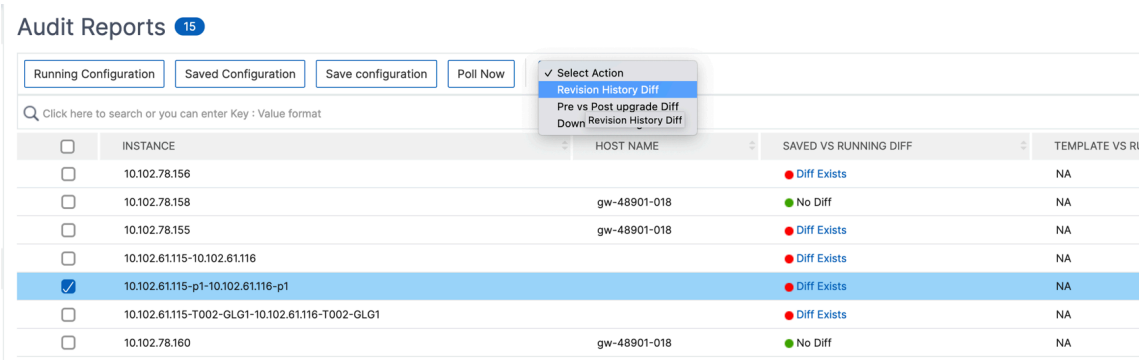
La différence entre l'historique des révisions pour la partition d'administration vous permet de visualiser la différence entre les cinq derniers fichiers de configuration d'une instance NetScaler partitionnée. Vous pouvez comparer les fichiers de configuration les uns aux autres (exemple Révision de 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 :

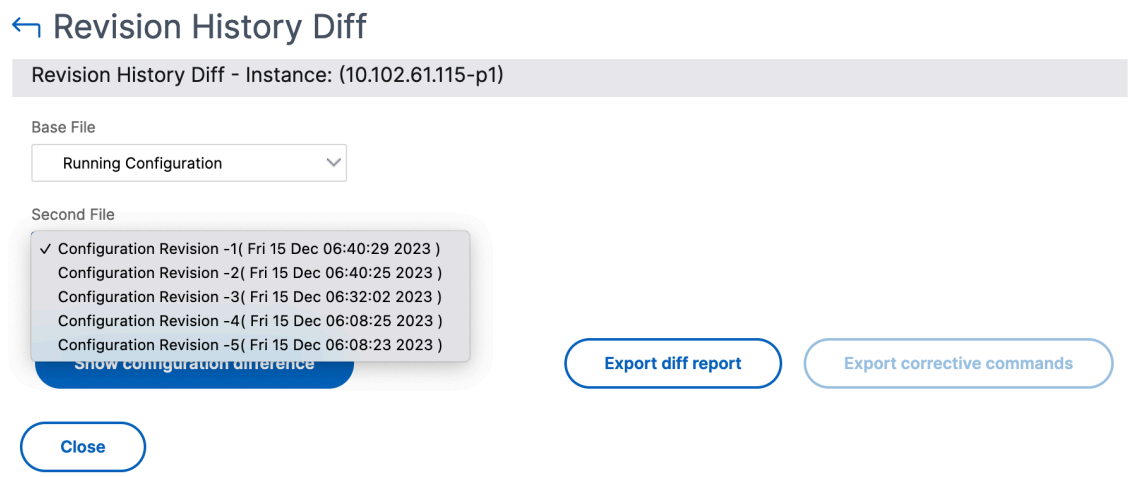
1. Accédez à **Infrastructure > Audit de configuration.** Cliquez à l'intérieur du graphique en donut qui représente l'état de configuration de l'instance. Dans la page **Rapports d'audit** qui s'ouvre, cliquez sur l'instance NetScaler partitionnée.



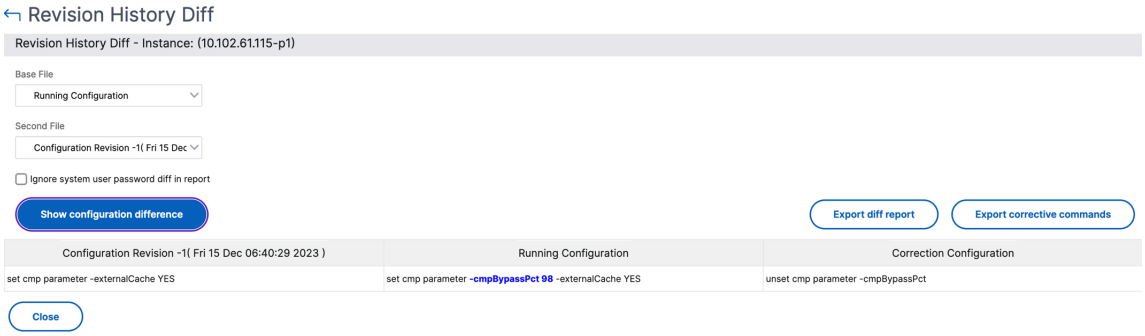
2. Dans le menu **Action**, cliquez sur **Diff Historique des révisions.**



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**.



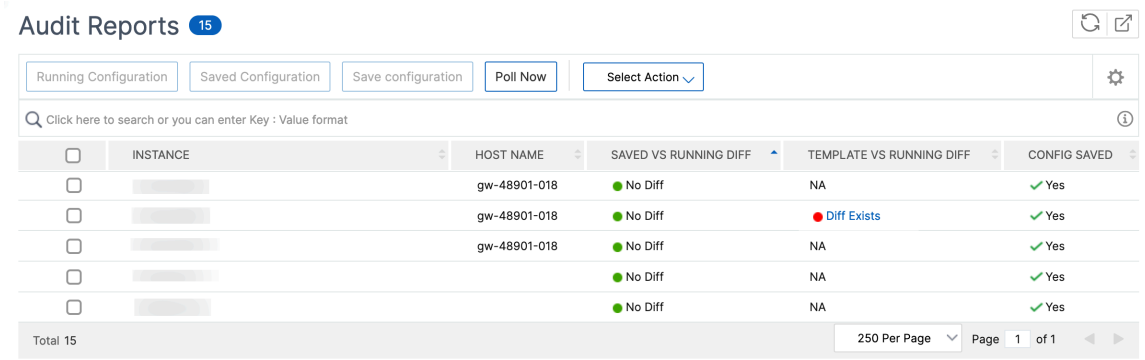
4. Vous pouvez ensuite voir la différence entre les cinq derniers fichiers de configuration pour l'instance NetScaler partitionnée sélectionnée, comme indiqué ci-dessous. Vous pouvez également afficher les commandes de configuration corrective et exporter ces commandes correctives dans votre dossier 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. Sur la page **Rapports d'audit**, cliquez sur l'instance NetScaler partitionnée.



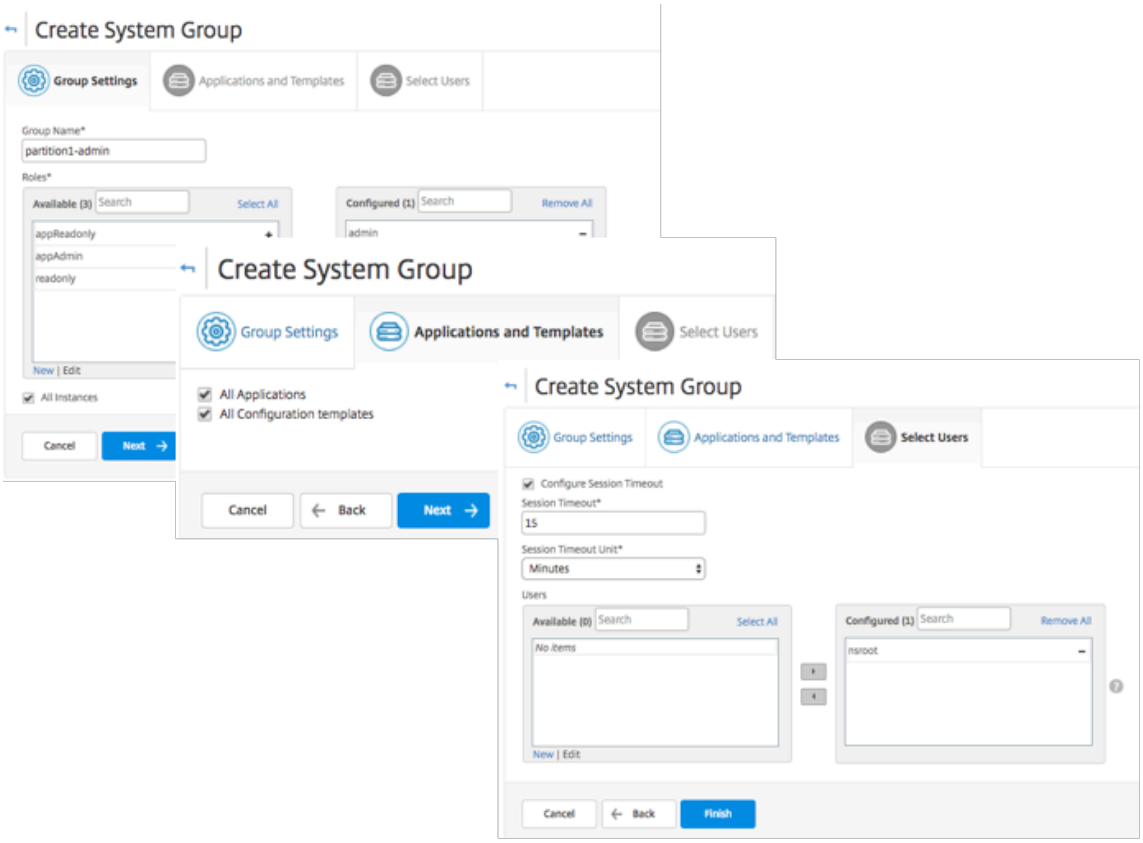
2. S'il y a une différence entre le modèle d'audit et la différence en cours d'exécution, la différence est affichée sous la forme d'un lien hypertexte. Cliquez sur le lien hypertexte pour afficher les différences s'il y en a. Avec les différences de configuration, les configurations de correction sont 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 **Paramètres > 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**Paramètres > 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.

Création d'une paire NetScaler à haute disponibilité

February 1, 2024

Une paire NetScaler High Availability (HA) peut assurer un fonctionnement ininterrompu en cas d'indisponibilité ou de panne réseau. Vous pouvez créer une paire d'instances ADC HA à l'aide de NetScaler ADM. Pour plus d'informations, consultez NetScalerHigh-availability.

Procédez comme suit pour créer une paire d'instances ADC HA dans NetScaler ADM :

1. Accédez à **Infrastructure > Instances > NetScaler**.
2. Sélectionnez une instance ADC dans la liste avec laquelle vous souhaitez créer une paire HA.

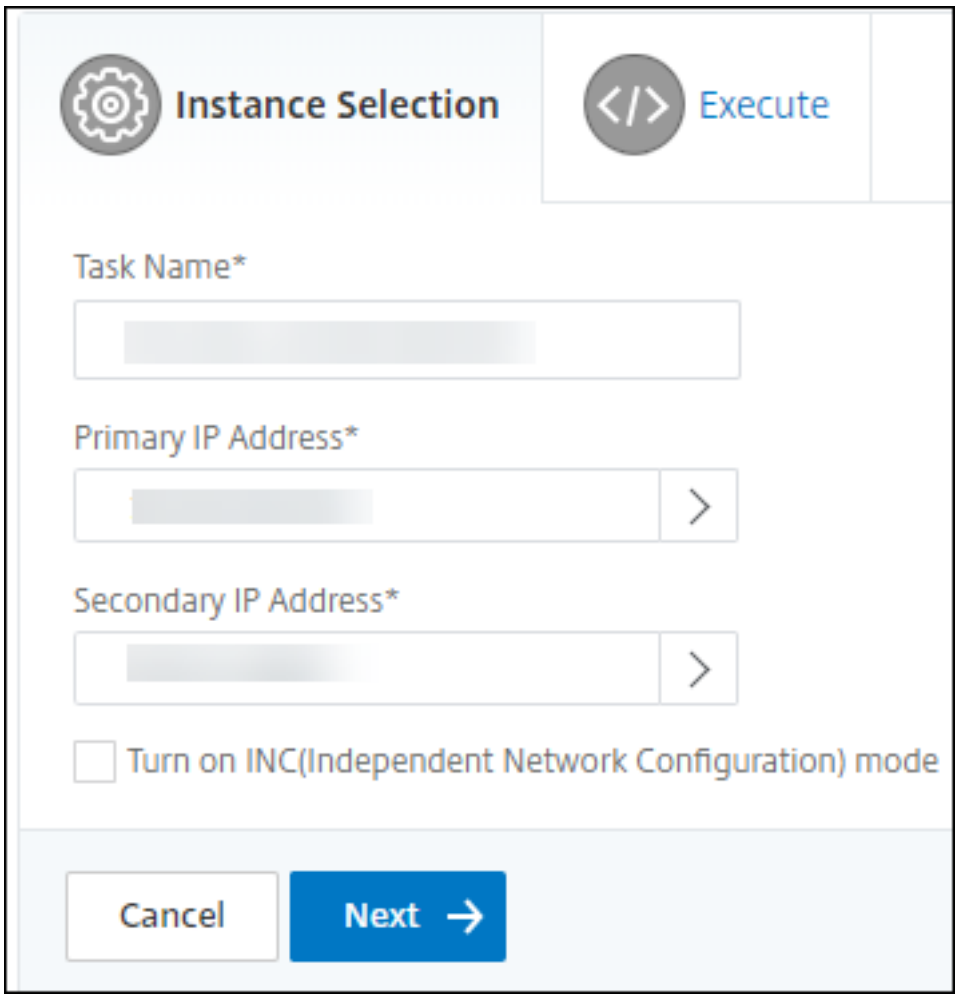
   L'instance sélectionnée devient une instance principale de la paire HA.
3. Cliquez sur Sélectionner **une action > Créer une paire HA**.
4. Dans **Sélection d'instance**, effectuez les opérations suivantes :

   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**.



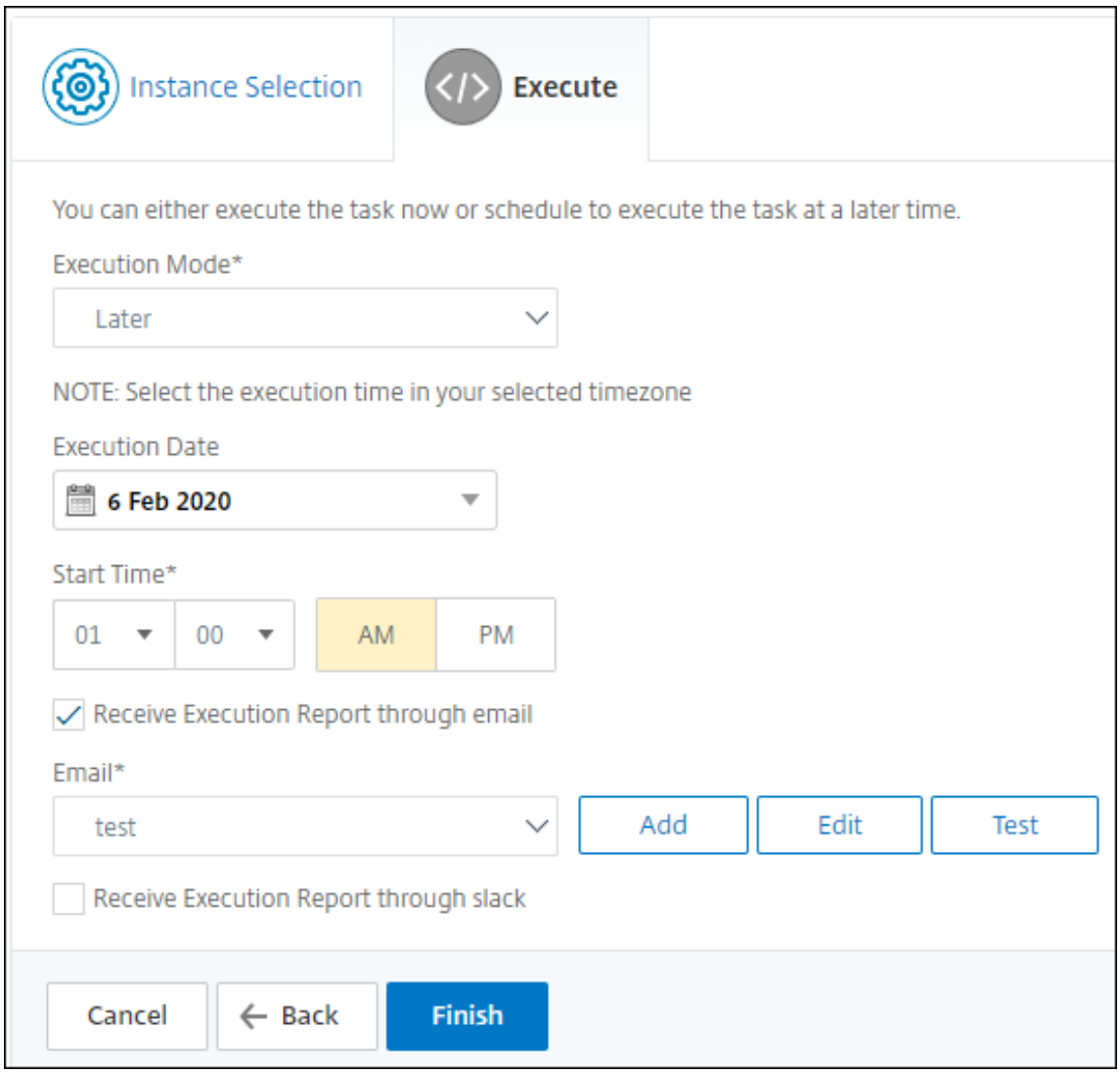
5. Dans **Execute**, vous pouvez décider de créer une paire HA maintenant ou ultérieurement.

   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.

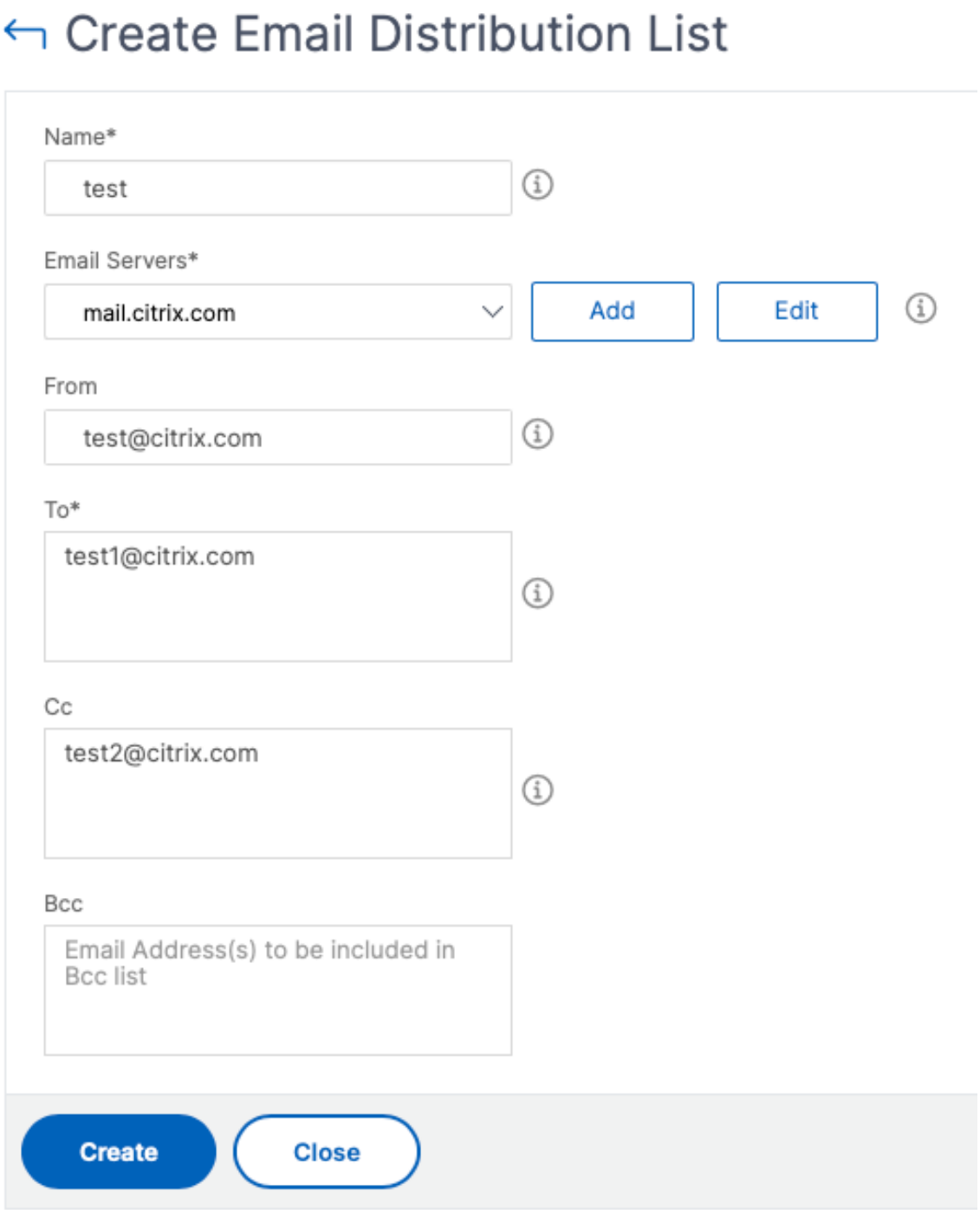
      > **Remarque**
      >
      > L'heure d'exécution est affichée dans le fuseau horaire défini dans NetScaler ADM.



Vous pouvez recevoir un rapport d'exécution de cette tâche via les éléments suivants :

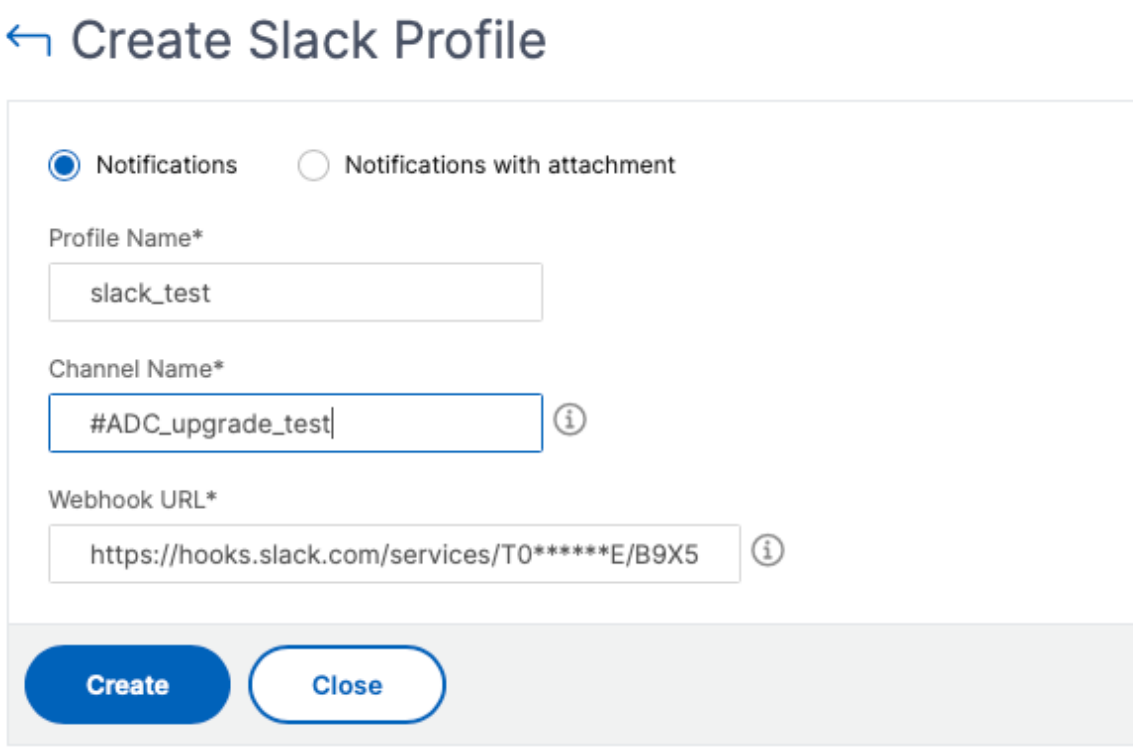
- **Courrier électronique** : sélectionnez la distribution d'e-mails dans la liste.

  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**.



Sauvegarde et restauration des instances NetScaler

February 1, 2024

Vous pouvez sauvegarder l'état actuel d'une instance NetScaler 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 méthodes pour effectuer des sauvegardes et des restaurations sur une instance NetScaler. Vous pouvez sauvegarder et restaurer manuellement les configurations NetScaler à l'aide de l'interface graphique et de l'interface de ligne de commande. Vous pouvez également utiliser NetScaler ADM pour effectuer des sauvegardes automatiques et des restaurations manuelles.

NetScaler ADM sauvegarde l'état actuel de vos instances NetScaler gérées à l'aide d'appels NITRO et des protocoles Secure Shell (SSH) et Secure Copy (SCP).

NetScaler ADM crée une sauvegarde complète et restaure les types d'instances NetScaler suivants :

- NetScaler SDX
- NetScaler VPX

- NetScaler MPX
- NetScaler BLX

> **Remarque :**
>
> - Assurez-vous que le profil NetScaler ADM dispose de l'accès administrateur pour sauvegarder et restaurer les instances ADC.
> - À partir de NetScaler ADM, vous ne pouvez pas effectuer l'opération de sauvegarde et de restauration sur un cluster NetScaler.
> - 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 NetScaler, vous devez d'abord configurer les paramètres de sauvegarde sur NetScaler ADM. Après avoir configuré les paramètres, vous pouvez sélectionner une ou plusieurs instances NetScaler et créer une sauvegarde des fichiers de configuration de ces instances. Si nécessaire, vous pouvez également restaurer les instances NetScaler 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 de NetScaler ADM pour sauvegarder une ou plusieurs instances NetScaler sélectionnée :

1. Dans NetScaler ADM, accédez à **Paramètres** > **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, NetScaler ADM est activé pour effectuer des sauvegardes des instances NetScaler. Désactivez cette option si vous ne souhaitez pas créer de fichiers de sauvegarde pour les instances.
    - **Fichier protégé par mot**de passe : (facultatif) Sélectionnez l'option de protection par mot de passe pour crypter 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 crypté sur votre ordinateur local, mais vous ne pouvez pas ouvrir le fichier à l'aide de l'interface graphique NetScaler ADM ni à l'aide d'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.

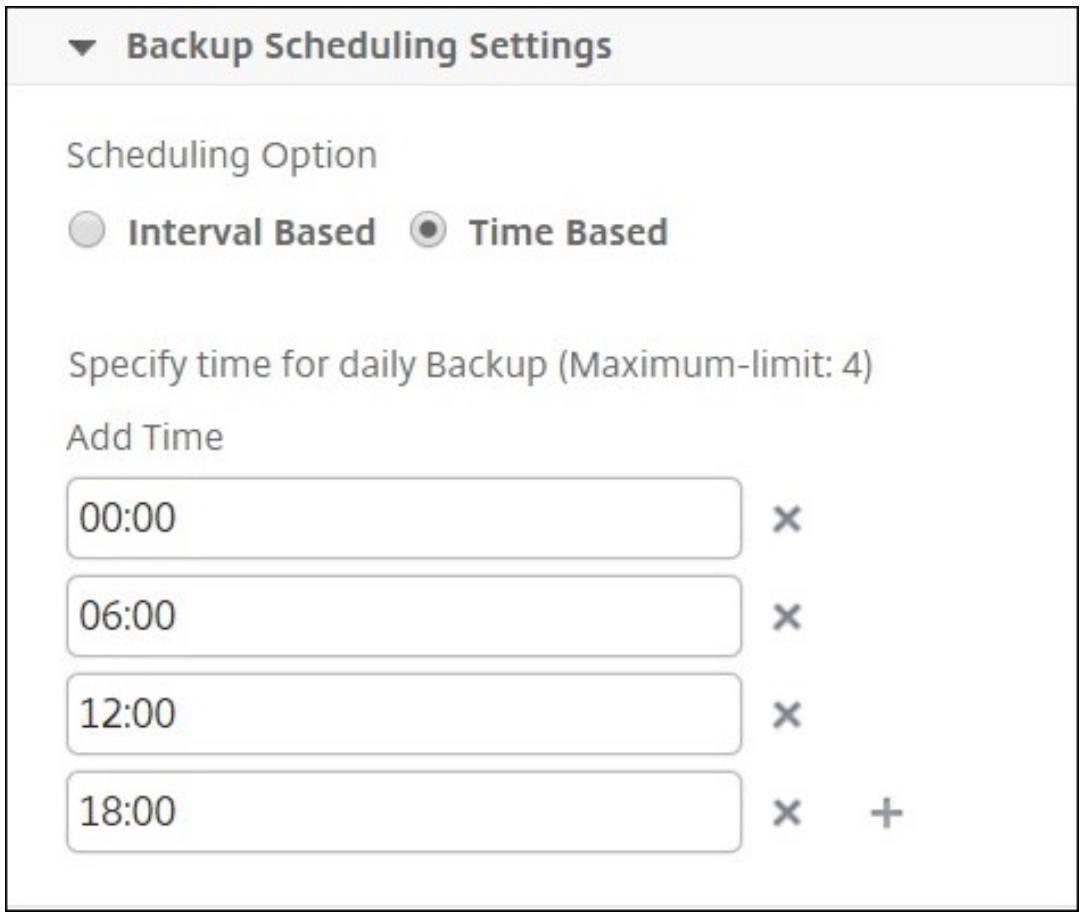
- **Nombre de fichiers de sauvegarde à conserver** : Spécifiez le nombre de fichiers de sauvegarde à conserver dans NetScaler ADM. Vous pouvez conserver jusqu'à 50 fichiers de sauvegarde par instance ADC. La valeur par défaut est trois fichiers de sauvegarde.

  > **Remarque :**
  >
  > Chaque fichier de sauvegarde tient compte de certaines exigences en matière de stockage. Nous vous recommandons de stocker un nombre optimal de fichiers de sauvegarde NetScaler sur NetScaler 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 NetScaler ADM une fois l'intervalle spécifié écoulé. 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. NetScaler ADM autorise un maximum de quatre sauvegardes quotidiennes sur les instances.



- **Paramètres NetScaler** : (facultatif) Par défaut, NetScaler ADM ne crée pas de fichier de sauvegarde lorsqu'il reçoit le piège « NetscalerConfigSave ». Vous pouvez toutefois activer l'option permettant de créer un fichier de sauvegarde chaque fois qu'une instance NetScaler envoie un piège « NetScalerConfigSave » à NetScaler ADM. Une instance NetScaler envoie « NetScalerConfigSave » chaque fois que la configuration de l'instance est enregistrée.
- **Fichiers de géodatabase** : (facultatif) Par défaut, NetScaler ADM ne sauvegarde pas les fichiers de géodatabase. Vous pouvez également activer l'option pour créer une sauvegarde de ces fichiers.

- **Transfert externe :**(facultatif) NetScaler ADM vous permet de transférer les fichiers de sauvegarde de l'instance NetScaler vers un emplacement externe :

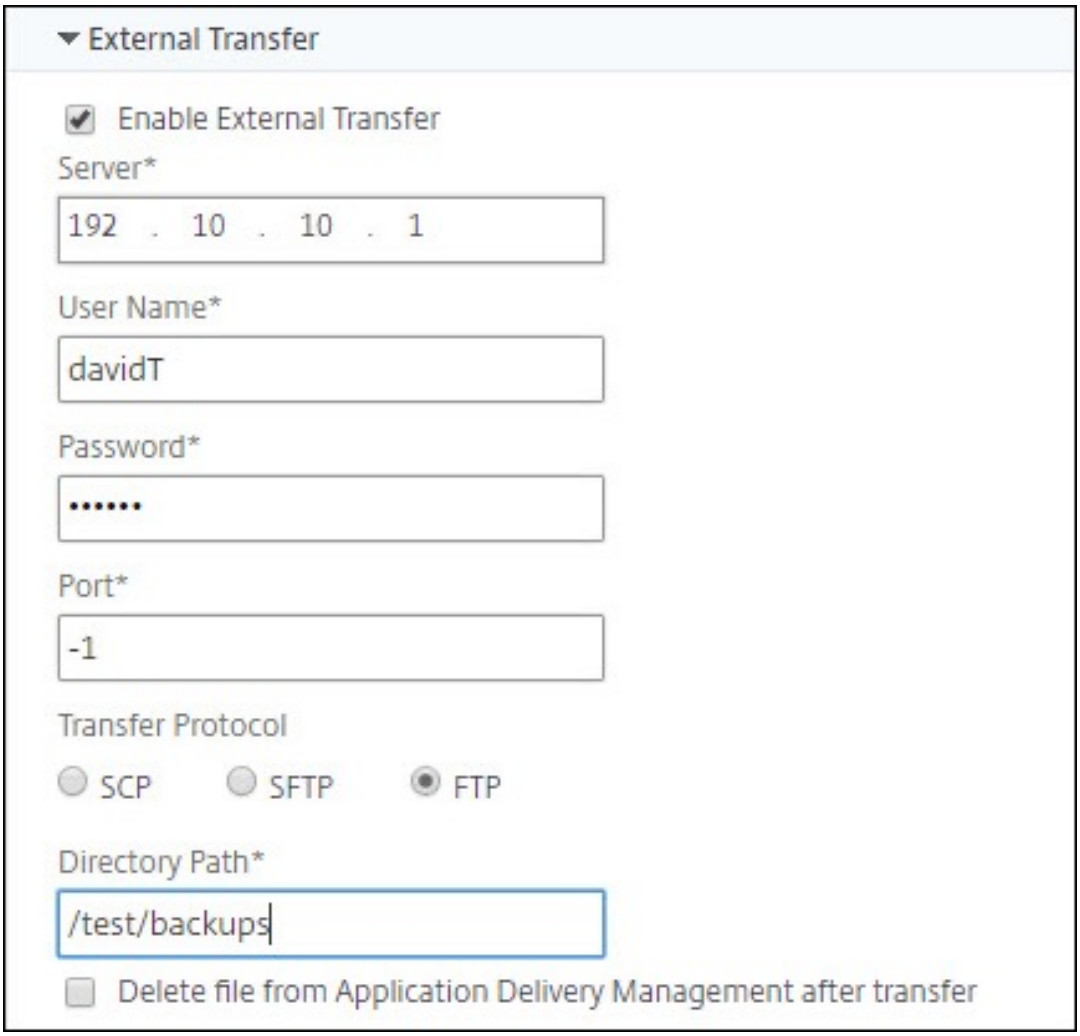
a) Spécifiez l'adresse IP de l'emplacement.

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 NetScaler ADM après l'avoir transféré vers le serveur externe.



Remarque :

NetScaler ADM s'envoie un piège SNMP ou une notification Syslog en cas d'échec de sauvegarde pour l'une des instances NetScaler sélectionnées.

Créez une sauvegarde pour une instance NetScaler sélectionnée à l'aide de NetScaler ADM

Effectuez cette tâche si vous souhaitez sauvegarder une ou plusieurs instances NetScaler sélectionnées :

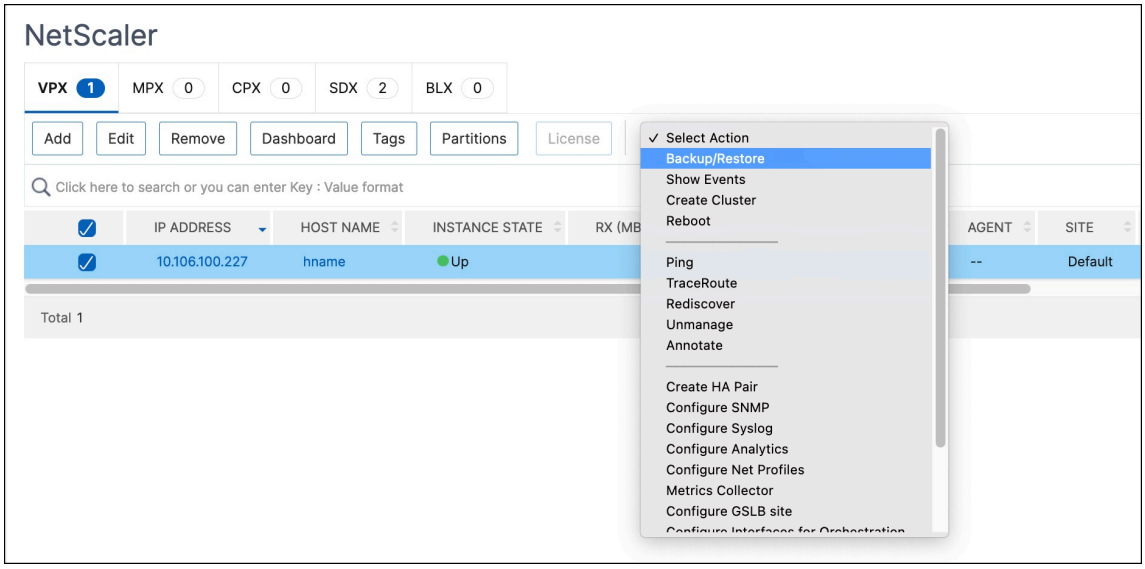
1. Dans NetScaler ADM, accédez à **Infrastructure > Instances.** Sous**Instances**, sélectionnez le type d'instance (par exemple, NetScaler VPX) à afficher à l'écran.
2. Sélectionnez l'instance à sauvegarder.
    - Pour les instances MPX, VPX et BLX, sélectionnez **Sauvegarder/Restaurer** dans la liste **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**.

Restaurez une instance NetScaler à l'aide de NetScaler ADM

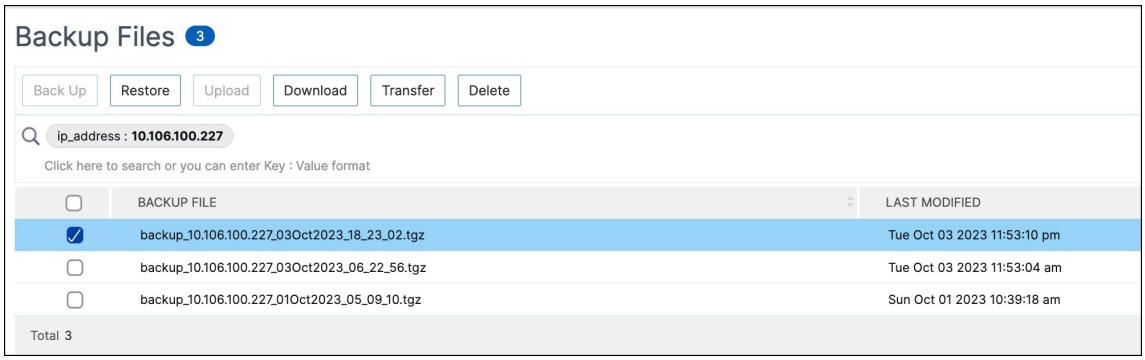
> **Remarque :**
>
> Si vous avez des instances NetScaler dans une paire HA, vous devez prendre note des points suivants :
>
> - Restaurez la même instance à partir de laquelle le fichier de sauvegarde a été créé. Par exemple, considérons un scénario selon lequel une sauvegarde a été effectuée à partir 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 une interruption de service de l'instance principale jusqu'à ce que le processus de restauration soit terminé.

Effectuez cette tâche pour restaurer une instance NetScaler à l'aide du fichier de sauvegarde que vous avez créé précédemment :

1. Accédez à **Infrastructure > Instances**, sélectionnez l'instance que vous souhaitez restaurer, puis cliquez sur**Sélectionner une action > Sauvegarde/Restauration**.



2. Dans la page**Fichiers de sauvegarde**, sélectionnez le fichier de sauvegarde contenant les paramètres à restaurer, puis cliquez sur**Restaurer**.



Restaurez une appliance NetScaler SDX à l'aide de NetScaler ADM

Dans NetScaler ADM, la sauvegarde de l'appliance NetScaler SDX inclut les éléments suivants :

- Instances NetScaler 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 NetScaler des appareils présents sur SDX
- NetScaler crée des images

- Images NetScaler 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 NetScaler SDX selon 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 NetScaler SDX à l'aide d'une sauvegarde d'une autre appliance NetScaler SDX, assurez-vous d'ajouter les licences et de configurer les paramètres réseau du service de gestion de la nouvelle appliance pour qu'ils correspondent aux paramètres du fichier de sauvegarde avant de démarrer le processus de restauration. En d'autres termes, la nouvelle appliance doit disposer d'une licence et répondre aux exigences de licence minimales du fichier de sauvegarde. Par exemple, si la sauvegarde comportait cinq instances VPX d'un total de 5 Go, la nouvelle appliance doit également être en mesure de prendre en charge ces exigences. Ou si l'appliance de sauvegarde disposait d'une licence Platinum, la nouvelle appliance doit disposer de la même licence ou d'une licence supérieure. Les paramètres réseau, tels que l'adresse IP, le masque réseau, la passerelle, l'adresse IP XenServer et le serveur DNS doivent être correctement configurés sur la nouvelle appliance.

Avant de restaurer l'appliance SDX, assurez-vous que la variante de plate-forme de l'appliance SDX sauvegardée est identique à 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 graphique de NetScaler ADM, accédez **à Infrastructure > Instances > NetScaler > SDX**. Sélectionnez une instance.
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 vers l'instance NetScaler secondaire

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 :

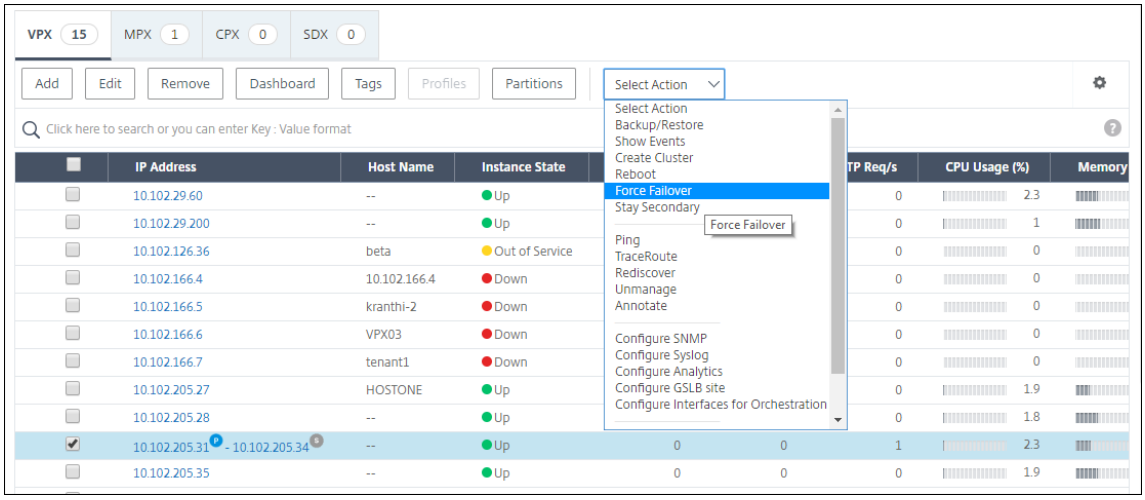
- Vous forcez le basculement sur un système autonome.
- L'instance secondaire est désactivée ou inactive. Si l'instance secondaire est inactive, vous devez attendre que son état soit activé pour forcer un basculement.
- L'instance secondaire est configurée pour rester secondaire.

L'instance NetScaler 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 vers l'instance secondaire de NetScaler à l'aide de NetScaler ADM :

1. Dans NetScaler Application Delivery Management (ADM), accédez à l'onglet **Infrastructure > Instances > NetScaler > 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 NetScaler 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.

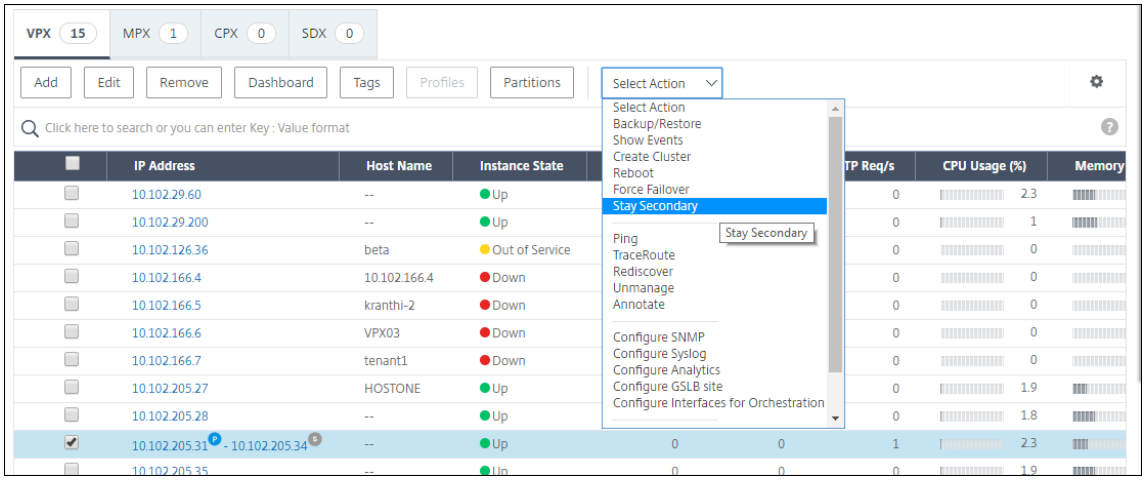
Lorsque vous forcez le nœud secondaire à rester secondaire, il reste secondaire même si le nœud principal tombe en panne. En outre, lorsque vous forcez l'état d'un nœud dans une paire HA à rester secondaire, il ne participe pas aux transitions de machines d'état HA. L'état du nœud est affiché en tant 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 NetScaler secondaire afin qu'elle reste secondaire à l'aide de NetScaler ADM :

1. Dans NetScaler Application Delivery Management (ADM), accédez à l'onglet **Infrastructure > Instances ****NetScaler**>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

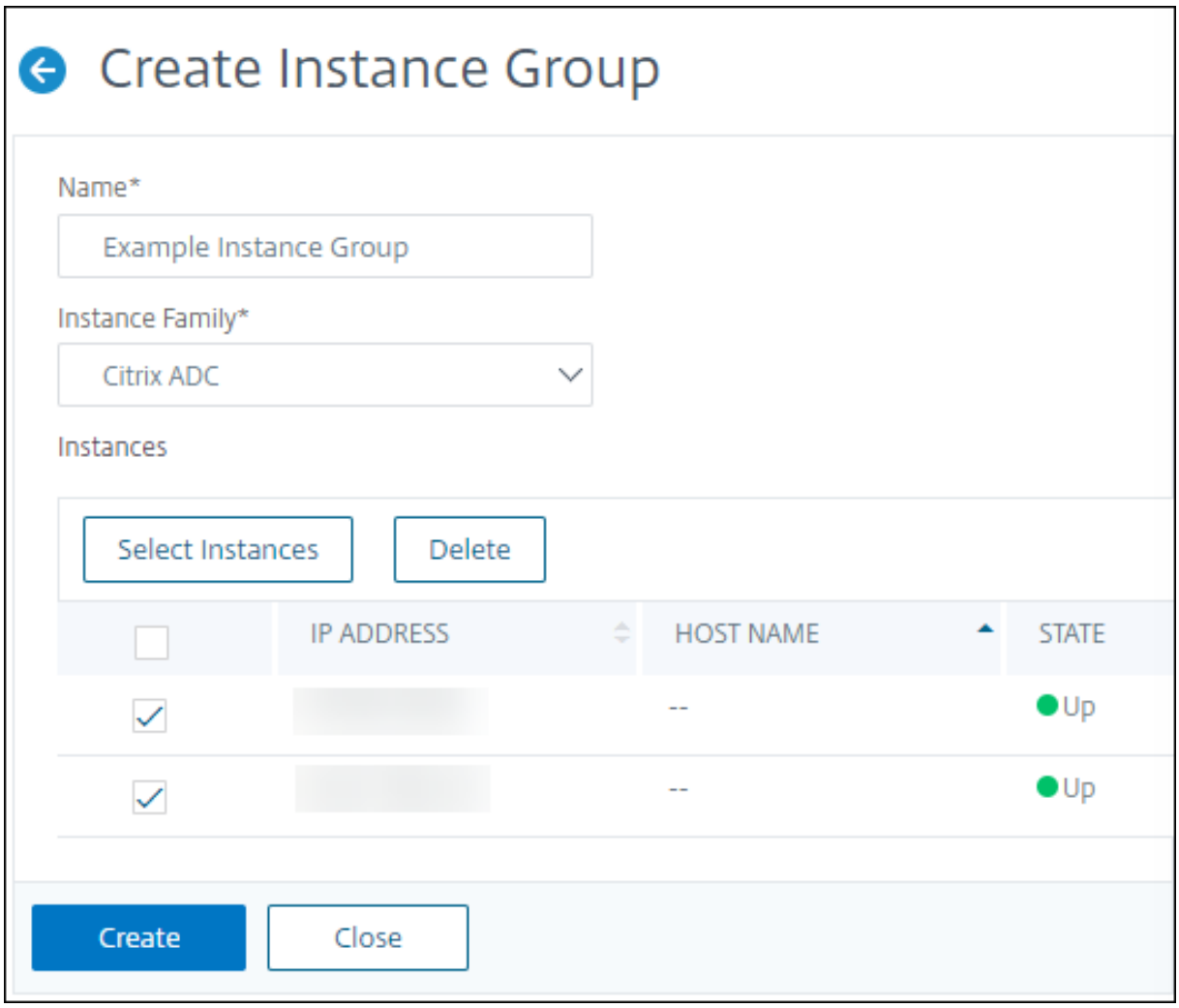
February 1, 2024

Pour créer un groupe d'instances, vous devez d'abord ajouter toutes vos instances NetScaler à NetScaler 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 NetScaler ADM

1. Dans NetScaler ADM, accédez à **Infrastructure > Groupes d'instances**, puis cliquez sur **Ajouter**.
2. Spécifiez un nom à votre groupe d'instances et sélectionnez **NetScaler** 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 NetScaler VPX sur SDX à l'aide d'ADM

February 1, 2024

Vous pouvez provisionner une ou plusieurs instances NetScaler VPX sur l'appliance SDX à l'aide de NetScaler 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 interdit de provisionner davantage d'instances NetScaler.

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 **Infrastructure > Instances > NetScaler**.

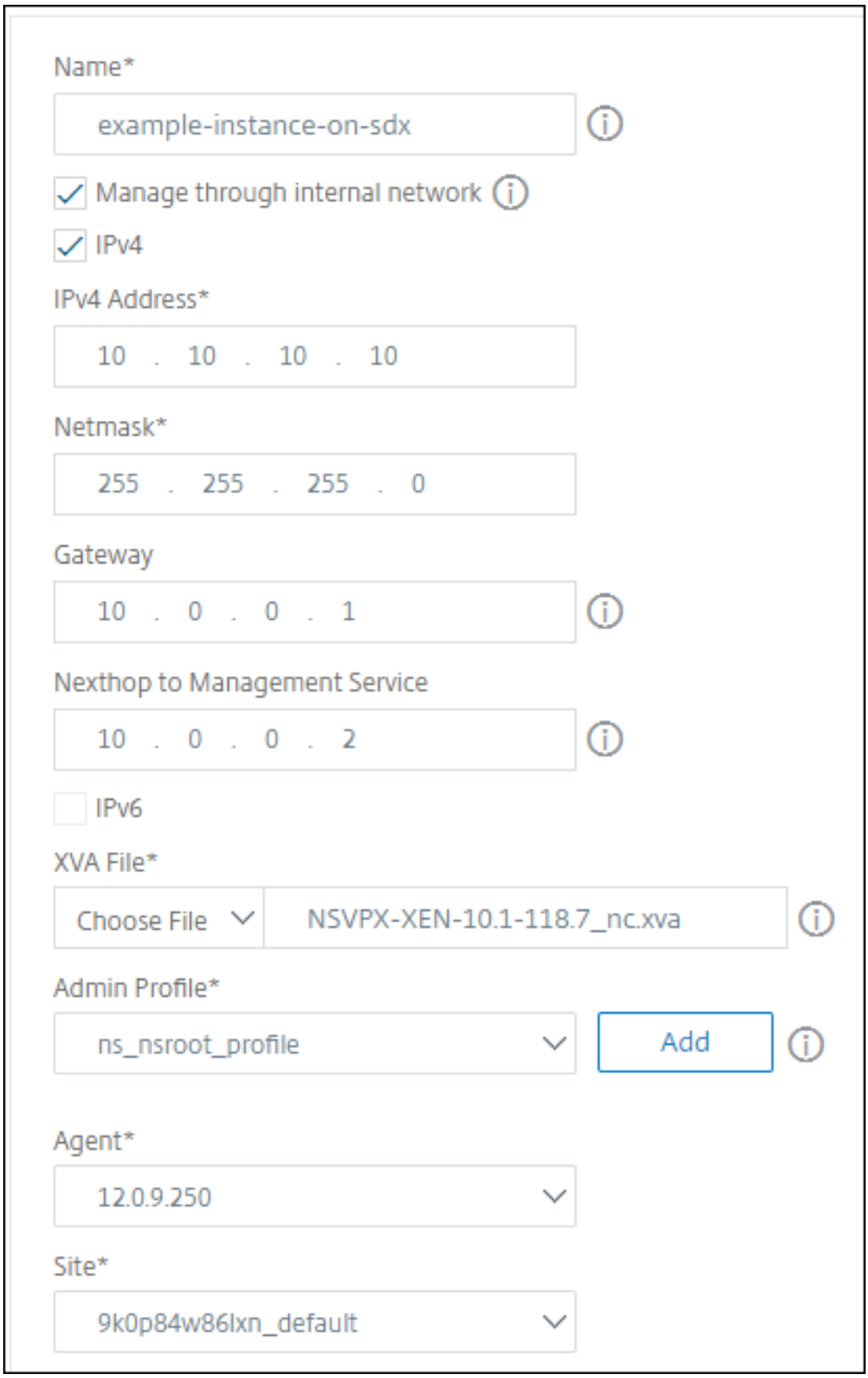
2. Dans l'onglet **SDX**, sélectionnez une instance SDX dans laquelle vous souhaitez provisionner une instance VPX.
3. Dans **Sélectionner une action**, sélectionnez **Provisionner VPX**.

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 NetScaler VPX. Une instance VPX ne peut avoir qu'une seule adresse IP de gestion (également appelée IP NetScaler). Vous ne pouvez pas supprimer l'adresse IP de NetScaler.

    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

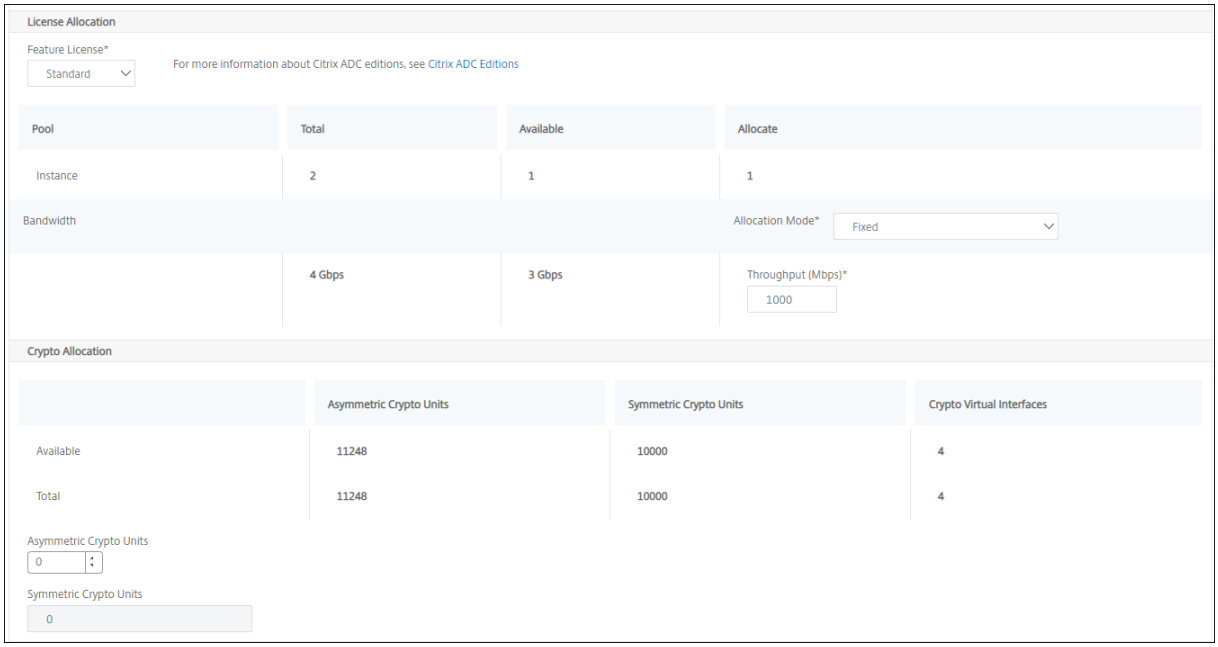
Dans la section **Allocation de licences**, spécifiez la licence VPX. Vous pouvez utiliser des licences Standard, Advanced et Premium.

- **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.

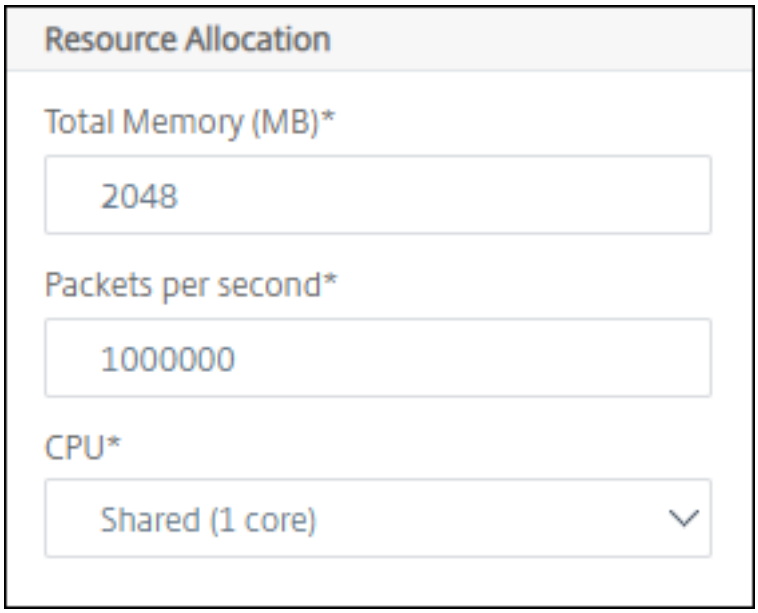
- **Mémoire totale (Mo)** - Affectez la mémoire totale à une instance. La valeur minimale est 2048 Mo.
- **Paquets par seconde** - Spécifiez le nombre de paquets à transmettre par seconde.
- **CPU** - Spécifiez le nombre de cœurs de CPU à une instance. Vous pouvez utiliser des cœurs CPU partagés ou dédiés.

  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
SDX 16000	64	30	16
SDX 9100	20	9	9

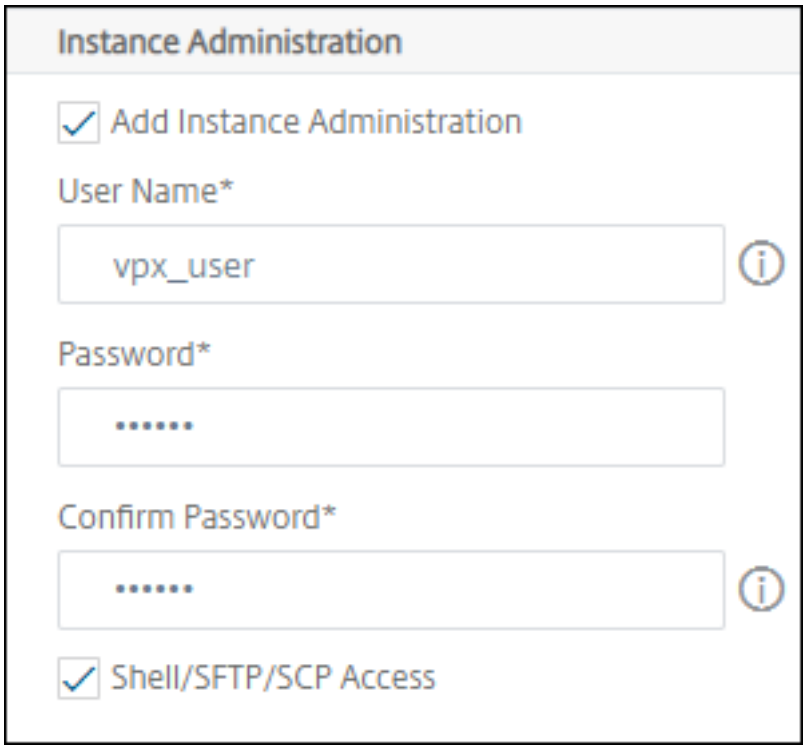
> **Remarque**
>
> Sur la plate-forme SDX 26xxx, un maximum de 26 cœurs de CPU peuvent être affectés à une instance VPX. Si des unités crypto sont affectées à l'instance, le nombre maximal de cœurs dépend du nombre d'unités de crypto et d'interfaces de données.
>
> Par exemple, si vous affectez 24000 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 NetScaler. 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 NetScaler**. Cette option est sélectionnée par défaut.



Étape 5 - Spécifier les paramètres réseau

Sélectionnez les paramètres réseau requis pour une instance :

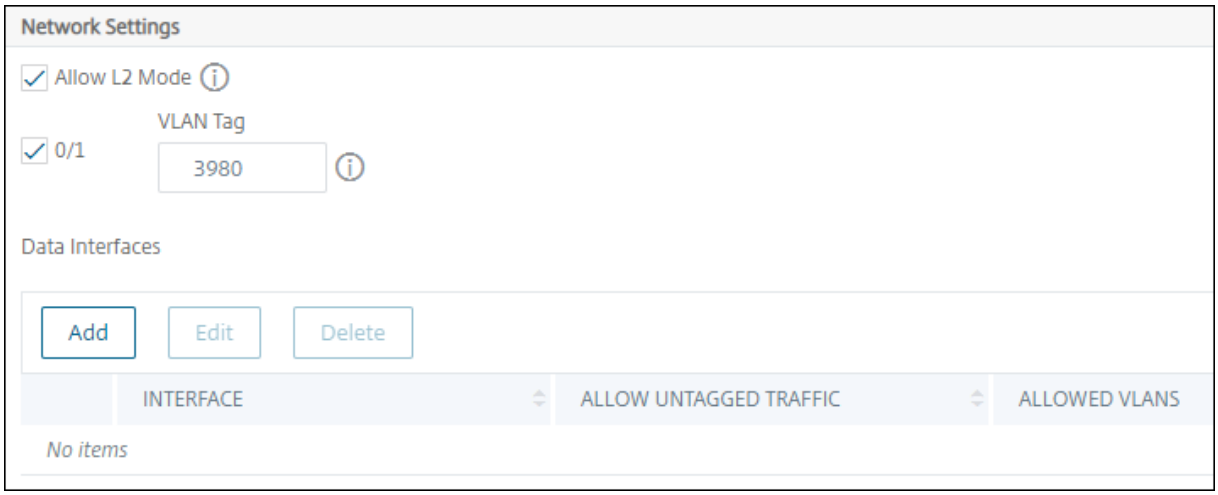
- **Autoriser le mode L2 dans les paramètres réseau** : vous pouvez autoriser le mode L2 sur l'instance NetScaler. Sélectionnez Autoriser le mode L2 sous Paramètres réseau. Avant de vous connecter à l'instance et d'activer le mode L2. Pour plus d'informations, consultez Autorisation du mode L2 sur une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

  > **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. Dans le cas contraire, tous les autres modes NetScaler risquent d'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.



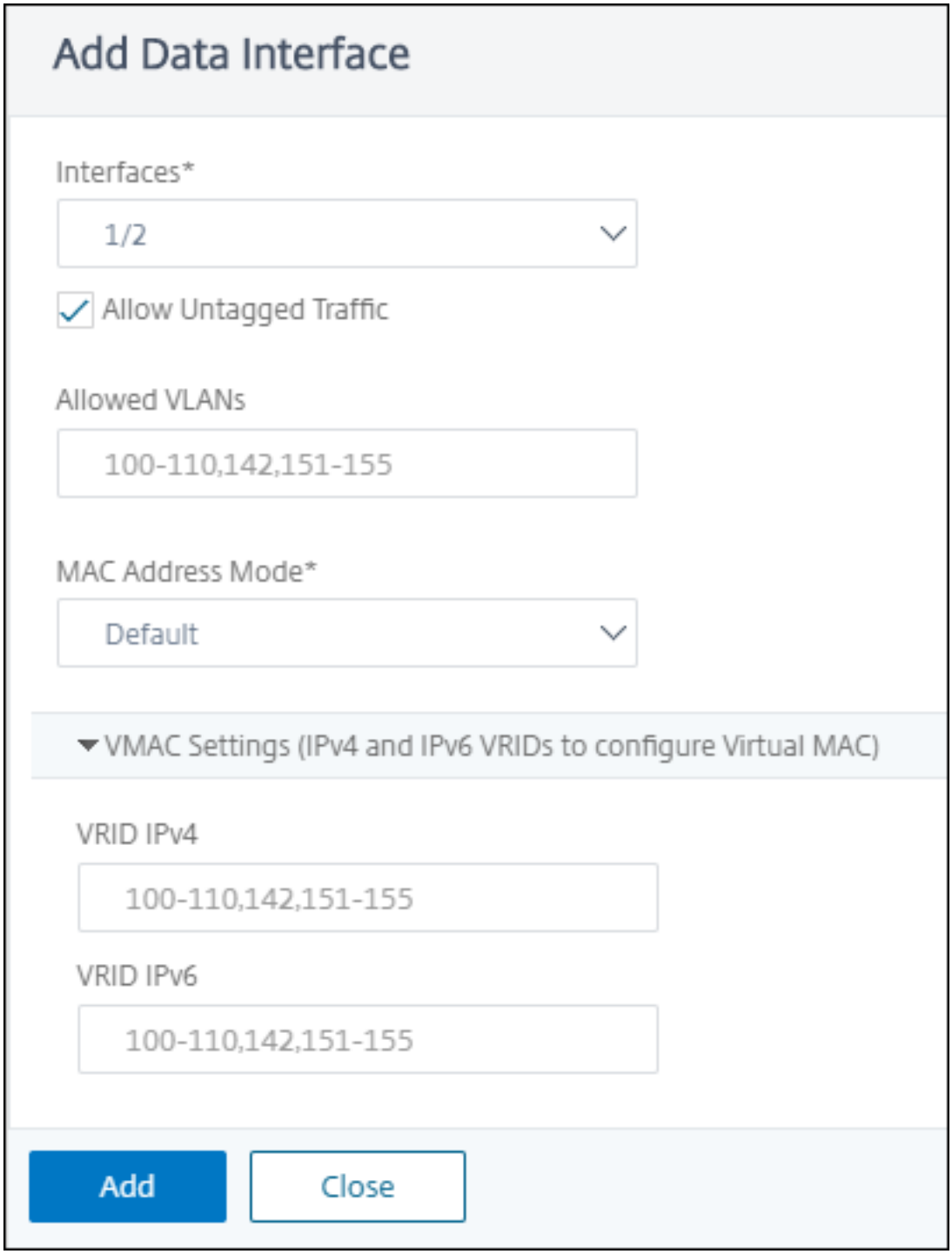
Dans **Interfaces de données**, cliquez sur **Ajouter** pour ajouter des interfaces de données et spécifiez les éléments suivants :

- **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 de VLAN pouvant être associés à une instance NetScaler.
- **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

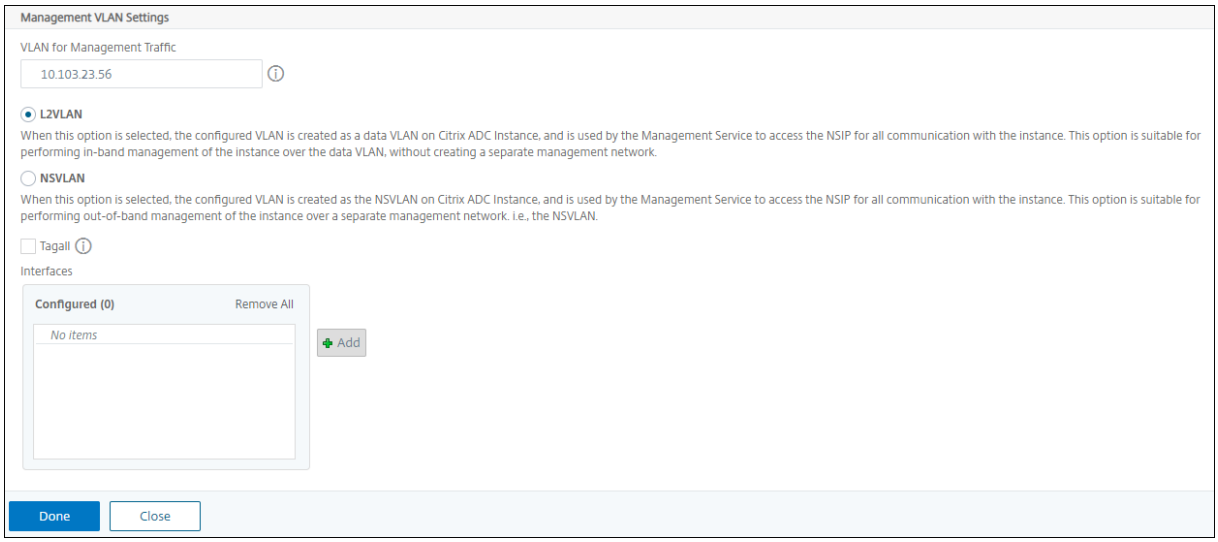
Le service de gestion et l'adresse de gestion (NSIP) de l'instance VPX se trouvent dans le même sous-réseau, et la communication se fait via une interface de gestion.

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.

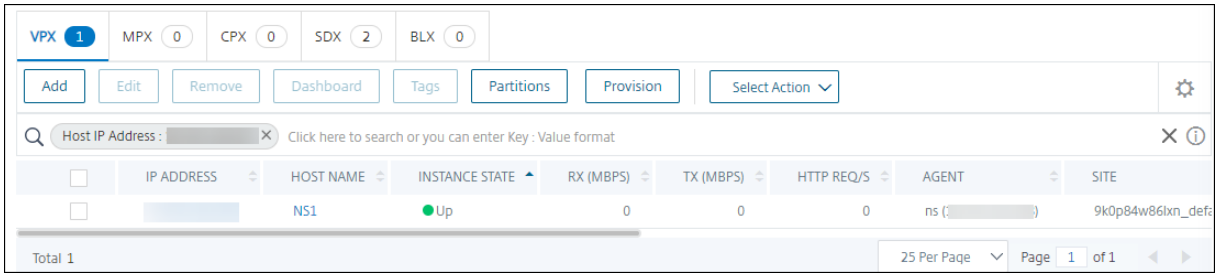


Cliquez sur **Terminé** pour provisionner une instance VPX.

Afficher l'instance VPX provisionnée

Pour afficher l'instance nouvellement provisionnée, procédez comme suit :

1. Accédez à **Infrastructure > Instances > NetScaler**.
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.



Redécouvrez plusieurs instances NetScaler VPX

February 1, 2024

Vous pouvez redécouvrir plusieurs instances NetScaler VPX dans votre configuration NetScaler Application Delivery Management (ADM). Vous pouvez également redécouvrir plusieurs instances NetScaler VPX lorsque vous souhaitez consulter les derniers états et configurations de ces instances. Le serveur NetScaler ADM redécouvre toutes les instances NetScaler VPX et vérifie si les instances Citrix Application Delivery Controller (ADC) sont accessibles.

Pour redécouvrir plusieurs instances NetScaler VPX :

1. Dans un navigateur Web, tapez l'adresse IP du serveur NetScaler 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 **l'onglet Infrastructure > Instances > NetScaler** > **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 indique la progression de la redécouverte de chacune des instances NetScaler VPX.

Annuler l'administration d'une instance

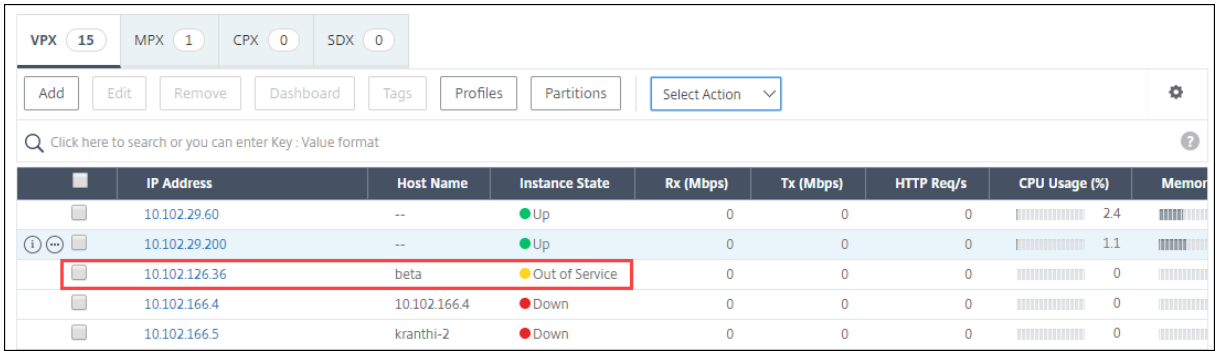
February 1, 2024

Si vous souhaitez arrêter l'échange d'informations entre NetScaler 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 **Infrastructure > Instances > NetScaler** > 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 NetScaler ADM et n'échange plus de données avec NetScaler ADM.

Tracer la route jusqu'à une instance

February 1, 2024

En traçant l'itinéraire d'un paquet entre NetScaler Application Delivery Management (ADM) et 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.

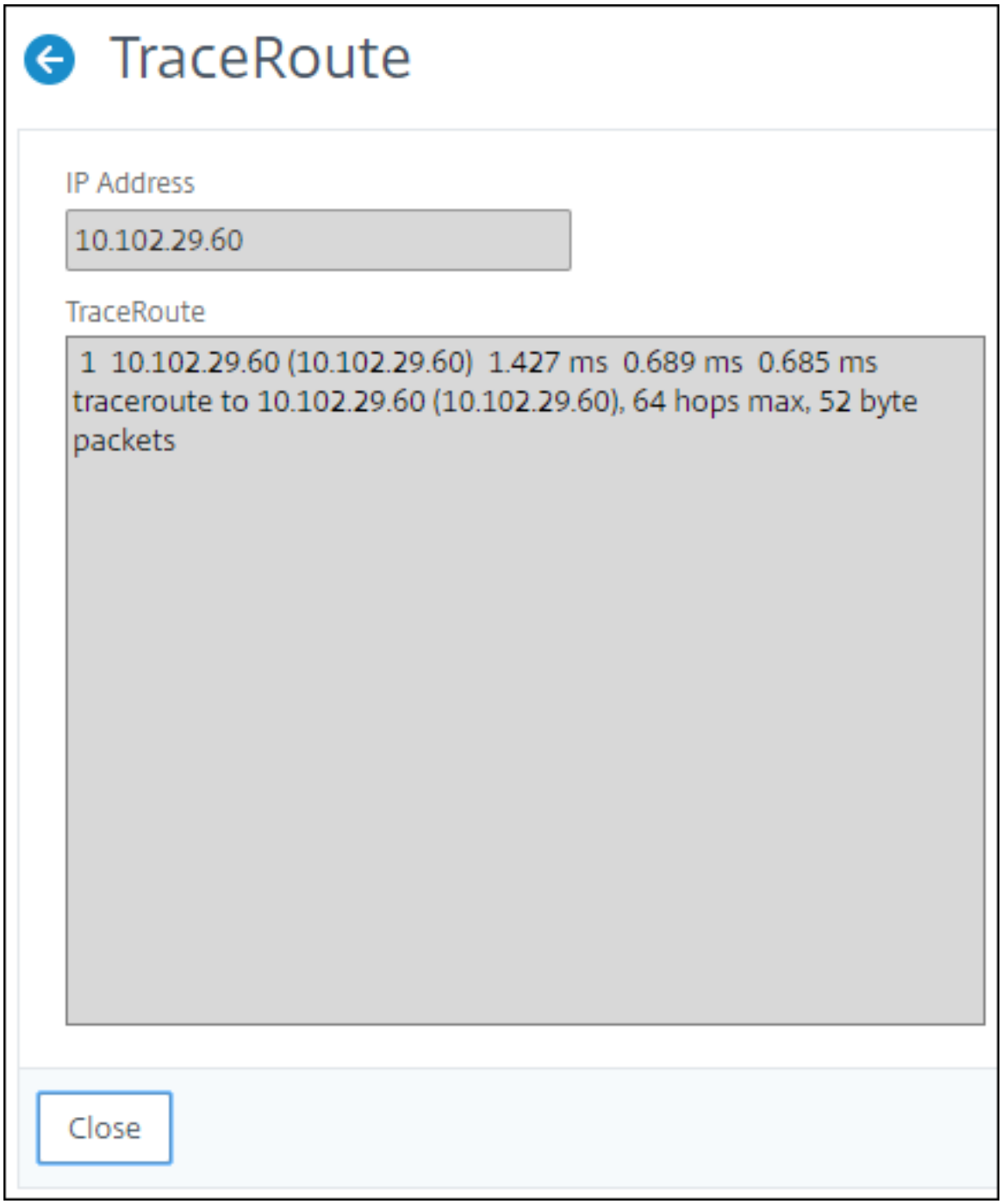
Traceroute enregistre également le temps qu'un paquet prend pour voyager d'un saut à l'autre. En cas d'interruption du transfert de paquets, traceroute indique où se situe le problème.

Pour tracer la route d'une instance :

1. Dans NetScaler ADM, accédez à **Infrastructure > Instances > NetScaler** > onglet **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.



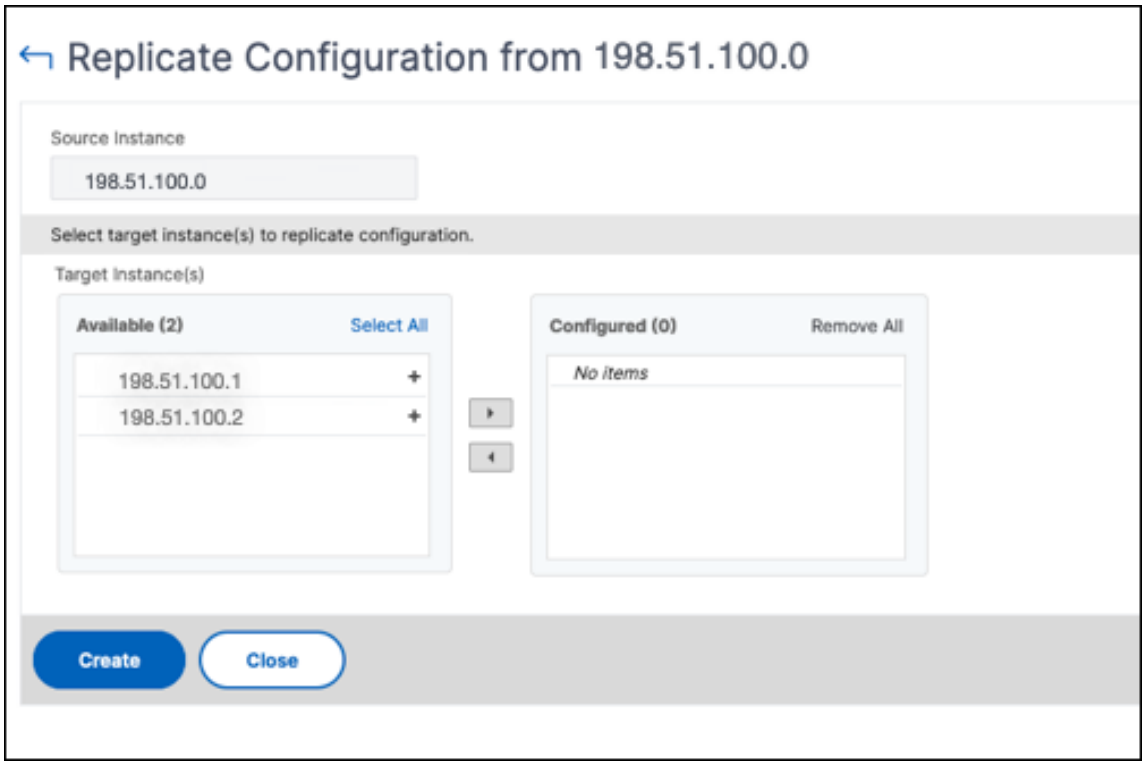
Répliquer les configurations d'une instance NetScaler à une autre

February 1, 2024

Vous pouvez utiliser la fonctionnalité de réplication de la configuration de NetScaler ADM pour copier des configurations à partir d'une instance NetScaler et les répliquer sur une ou plusieurs instances.

Pour répliquer les configurations d'une instance vers d'autres instances NetScaler

1. Accédez à **Infrastructure > Instances > NetScaler**. Sélectionnez l'instance source dont vous souhaitez répliquer les configurations sur d'autres instances et, dans la liste **Sélectionner une action**, cliquez sur **Répliquer la configuration**.
2. Dans **Configuration de réplication**, sélectionnez l'instance cible sur laquelle vous souhaitez appliquer les configurations à partir de l'instance source. Vous pouvez répliquer les configurations d'une instance source unique vers une seule instance ou plusieurs instances cibles.



3. Cliquez sur **Créer**.

Les configurations répliquées sont ajoutées à la liste des instances de NetScaler. Pour afficher l'état des instances répliquées, cliquez sur l'icône d'actualisation.

> **Remarque :**
>
> Au cours de la réplication, toutes les adresses IP réseau de l'instance source sont répliquées sur l'instance cible. Si l'instance cible se trouve sur un réseau différent de celui de l'instance source, les adresses IP de l'instance cible risquent de ne pas être accessibles. Lorsque les adresses IP ne sont pas accessibles, le statut des entités de l'instance cible est affiché comme étant en panne.
>
> Pour afficher l'état des entités configurées sur votre instance NetScaler gérée, accédez **à Infrastructure**> Fonctions réseau.

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).

NetScaler 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. NetScaler ADM rationalise 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 :

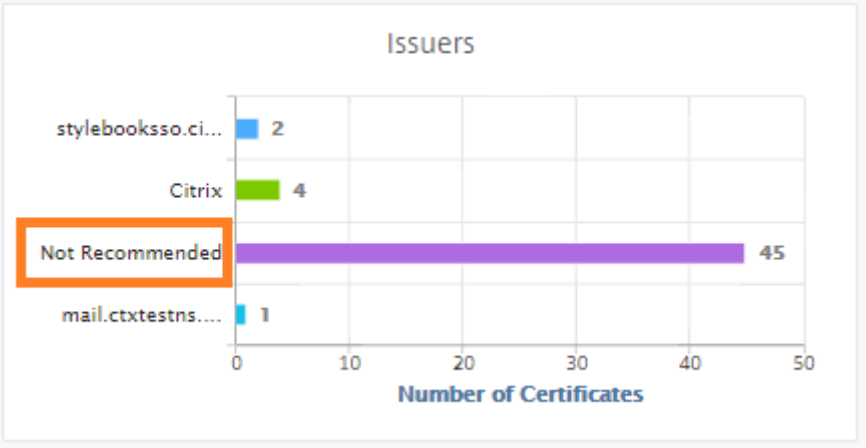
- À partir d'une autorité de certification (CA) autorisée, telle que Verisign
- En générant un nouveau certificat SSL et une nouvelle clé sur l'appliance NetScaler

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, NetScaler ADM vous aide à configurer les paramètres de stratégie SSL de l'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.



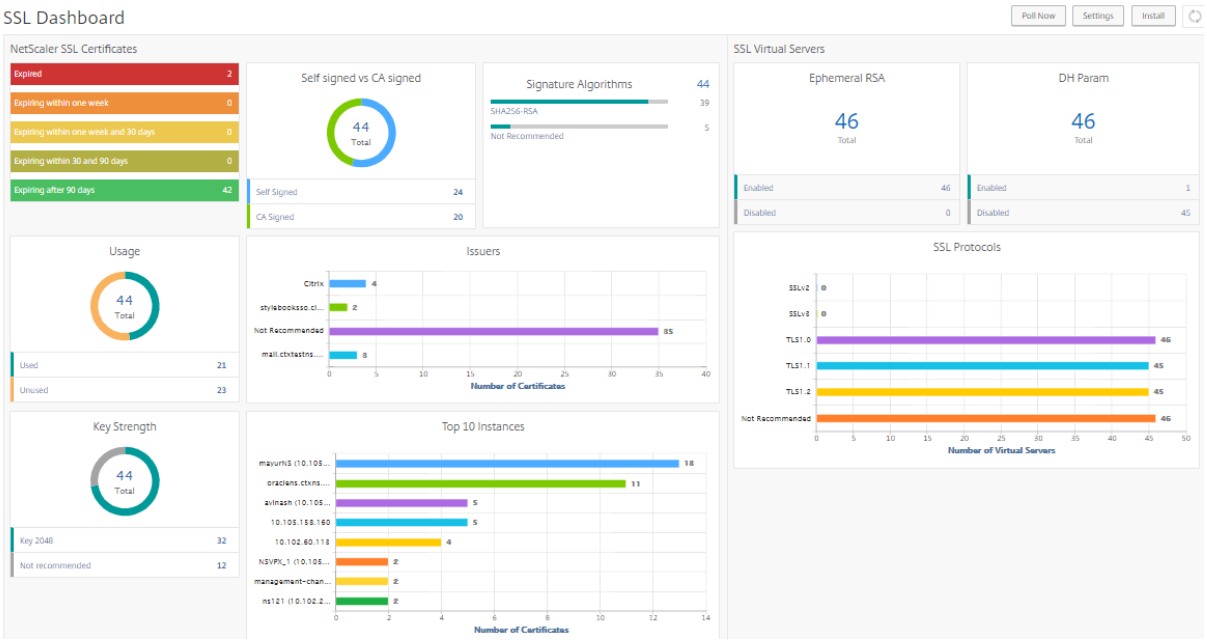
> **Remarque**
>
> Les certificats « Non recommandés » sont classés en fonction de différents paramètres, et vous pouvez les afficher dans les composants pertinents.

Fonctionnement du certificat NetScaler ADM

Le tableau de bord SSL vous fournit une présentation visuelle de tous les certificats SSL installés sur différentes instances de NetScaler. Le tableau de bord SSL inclut les informations suivantes pour chaque certificat installé sur les instances NetScaler. 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 NetScaler en fonction du nombre de certificats SSL installés.



Cas d'utilisation de la gestion des certificats SSL

Les cas d'utilisation suivants décrivent comment vous pouvez utiliser le certificat SSL pour gérer et surveiller les certificats sur plusieurs instances NetScaler.

Installer les certificats SSL

Imaginez que vous disposez d'un parc d'instances NetScaler sur lequel vous devez déployer les certificats SSL requis. NetScaler ADM vous fournit une console unifiée pour déployer les certificats SSL sur plusieurs instances NetScaler en une seule tentative.

Par exemple, vous souhaiterez peut-être installer des certificats SSL sur une ou plusieurs instances NetScaler. Cette approche vous permet de minimiser l'intervention manuelle liée à l'installation du certificat SSL sur chaque instance NetScaler. Vous pouvez effectuer une installation groupée de certificats SSL sur une ou plusieurs instances NetScaler.

Pour obtenir un résumé des certificats SSL, connectez-vous à **NetScaler ADM**, puis accédez à **Infrastructure**Tableau de bord SSL.

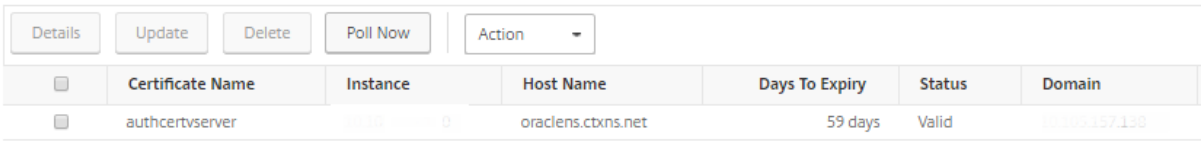
Paramètres de notification pour l'expiration du certificat

Dans ce cas d'utilisation, vous pouvez disposer de nombreux certificats répartis sur plusieurs instances NetScaler et le suivi de l'expiration de chaque certificat devient une charge supplémentaire. 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 NetScaler ADM pour qu'il envoie les notifications ou les alertes aux profils de messagerie, de téléavertisseur, de Slack ou de 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 désormais renouveler les certificats depuis NetScaler ADM. Vous pouvez renouveler les certificats existants ou créer les certificats basés sur les éléments suivants :

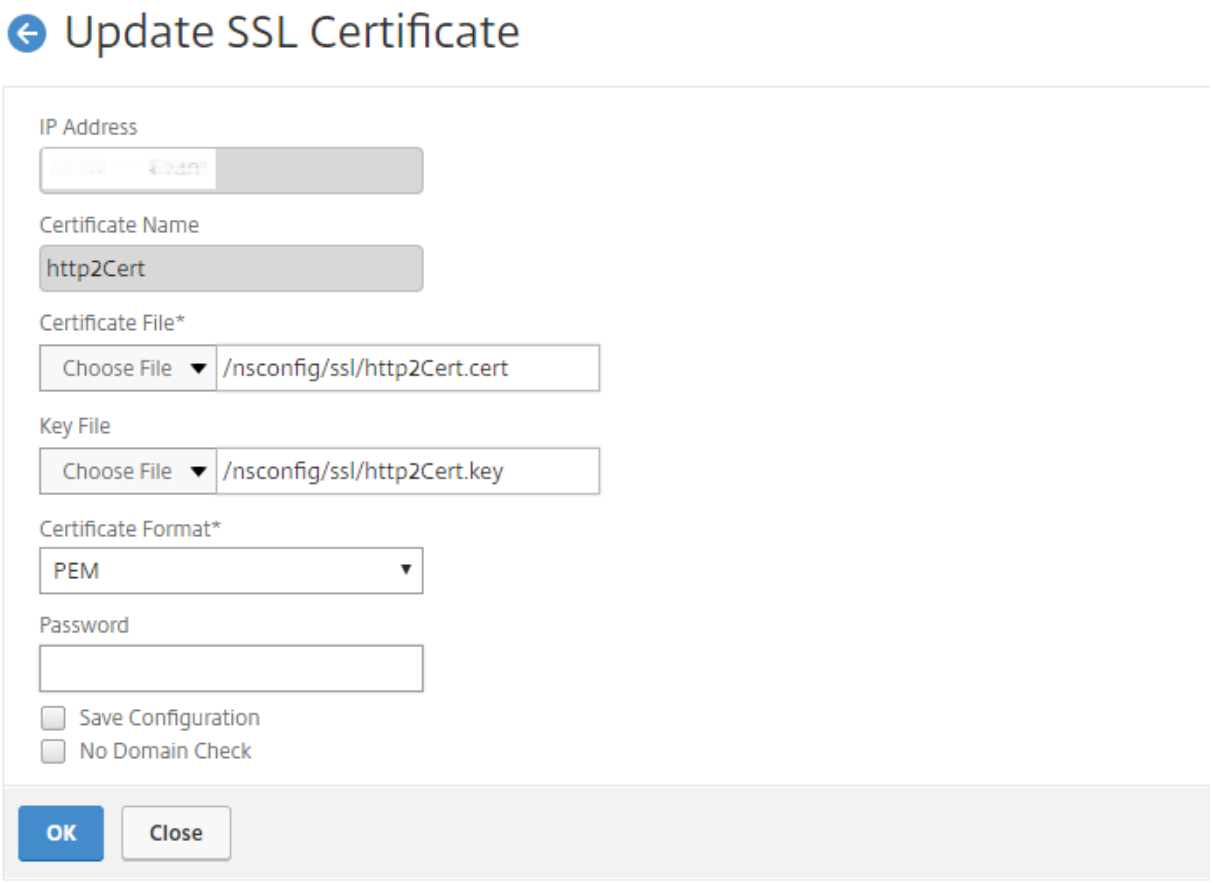
Mettre à jour le certificat existant Dans ce cas d'utilisation, vous devez mettre à jour un certificat existant une fois que vous recevez un certificat renouvelé de l'autorité de certification (CA). Vous pouvez désormais mettre à jour les certificats existants depuis NetScaler ADM sans vous connecter aux instances NetScaler.

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 NetScaler, vous pouvez désormais mettre à jour le certificat SSL depuis NetScaler ADM.

Pour mettre à jour un certificat, connectez-vous à NetScaler ADM, puis accédez à **Infrastructure**Tableau de bord SSL.

Sélectionnez le certificat que vous souhaitez mettre à jour, puis cliquez sur **Mettre à jour**.

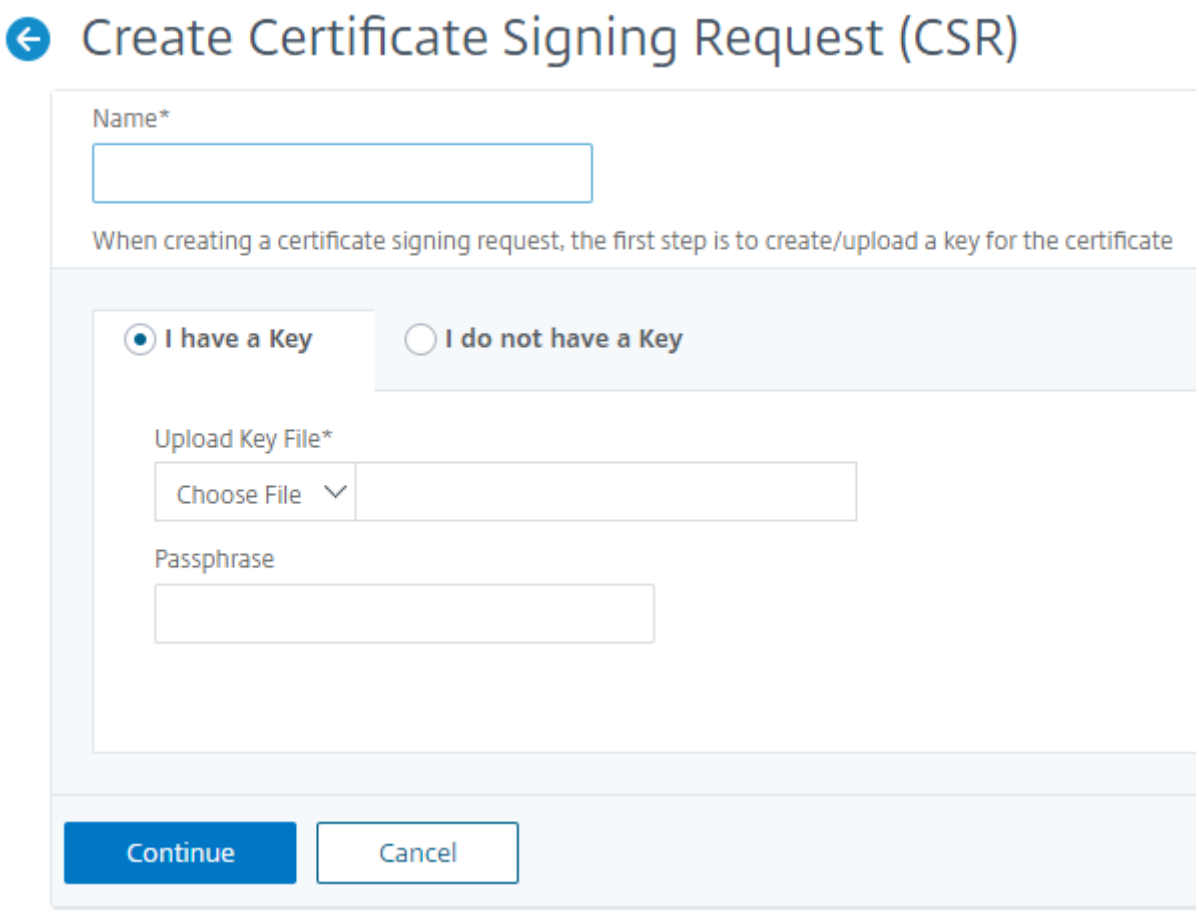
Vous avez la possibilité de mettre à jour les champs pertinents du certificat sélectionné à partir de NetScaler ADM.



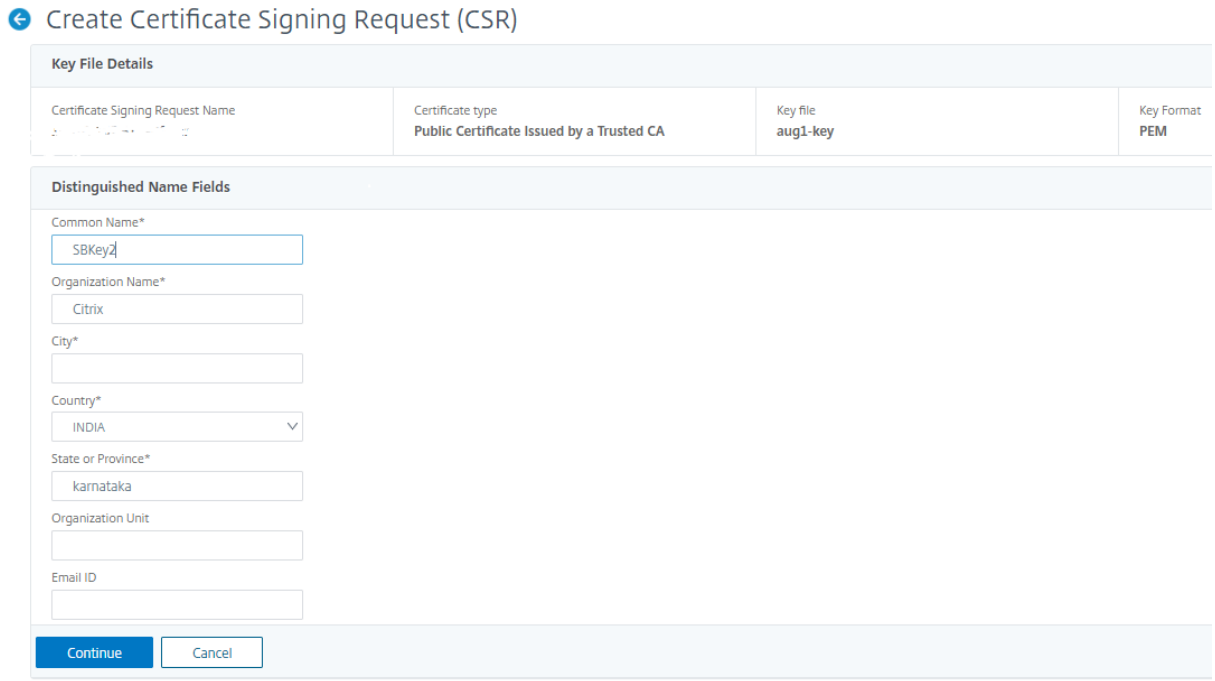
Créer une demande de signature de certificat Imaginez un cas d'utilisation où l'un des certificats SSL ne respecte pas les stratégies de l'organisation. Vous souhaitez obtenir un nouveau certificat auprès de l'autorité de certification. Vous pouvez désormais générer une demande de signature de certificat (CSR) depuis NetScaler 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.

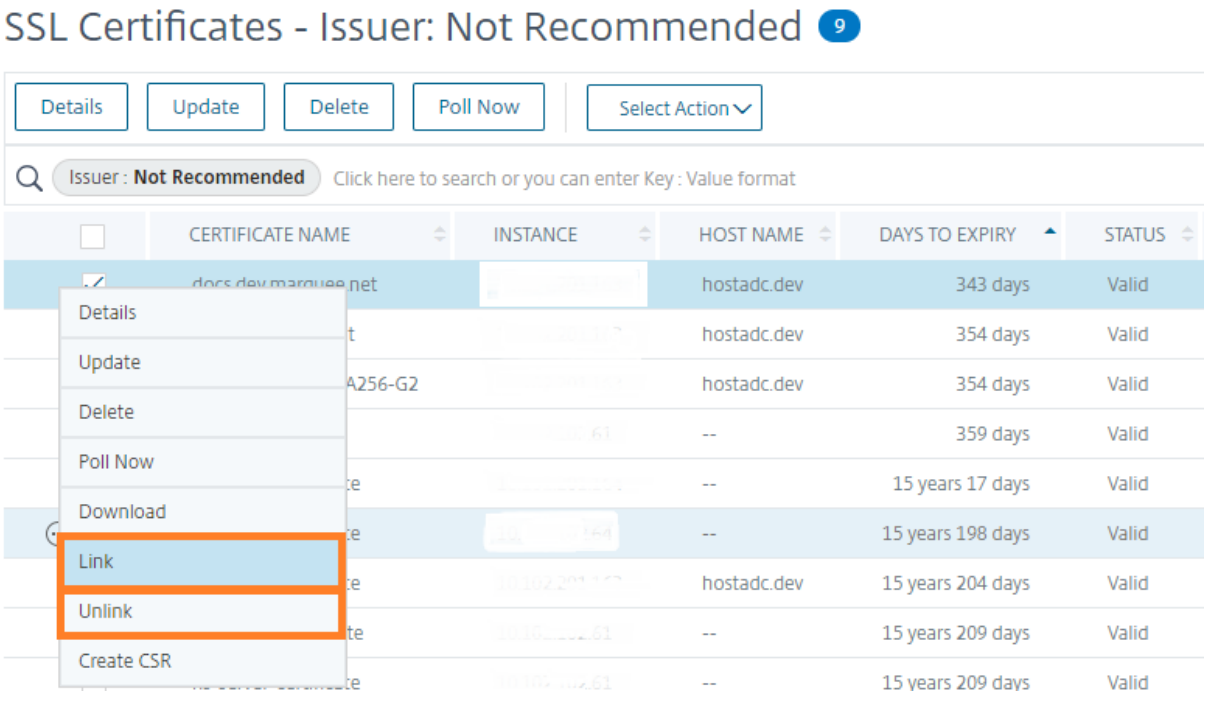


Pour donner plus de détails sur la clé sélectionnée, comme Nom commun, Nom de l'organisation, Ville, Pays, État, Unité Org et Email ID pour créer la CSR.



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.

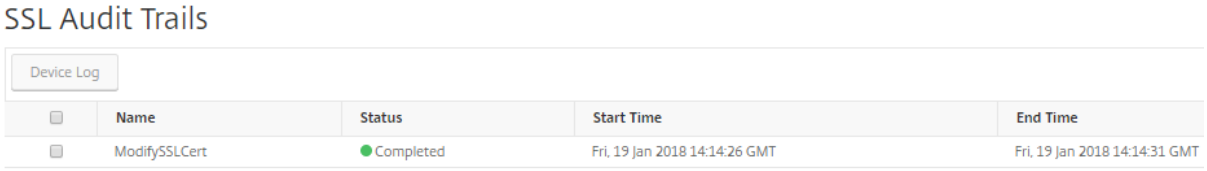


Journaux d'audit

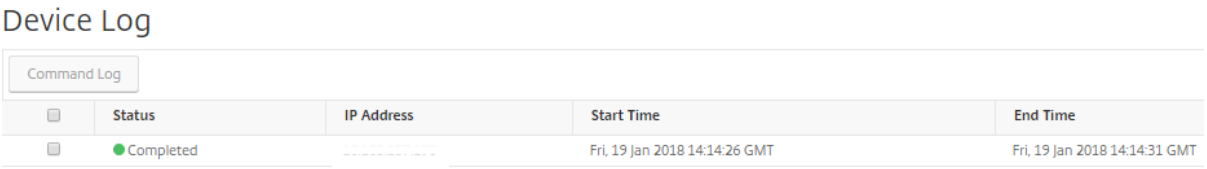
Les journaux d'audit sont un ensemble de fichiers journaux texte générés par NetScaler ADM. Il affiche l'historique des certificats SSL ajoutés, modifiés et modifiés à l'aide de NetScaler ADM sur l'appliance NetScaler spécifique. Les journaux d'audit indiquent également l'adresse IP de l'appliance NetScaler, l'état, l'heure de début et l'heure de fin de l'opération en question.

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.

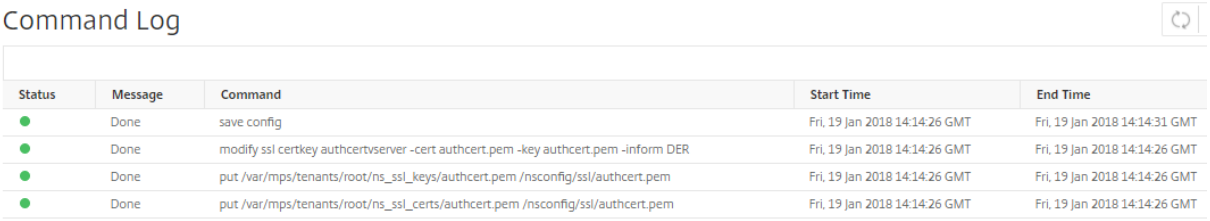
Pour déterminer les informations des certificats SSL, dans le tableau de **bord SSL**, cliquez sur **Journal d'audit**. Le récapitulatif de l'application inclut l'état des certificats SSL avec Heure de début et Heure de fin.



Pour déterminer les informations de l'appliance NetScaler relatives à un certificat SSL particulier, cochez la case de certificat correspondante 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 dans NetScaler Application Delivery Management (ADM) pour afficher des graphiques qui vous aident à suivre les émetteurs de certificats, leurs

principaux points forts et les algorithmes de signature. Le tableau de bord des certificats SSL affiche également des graphiques indiquant les éléments suivants :

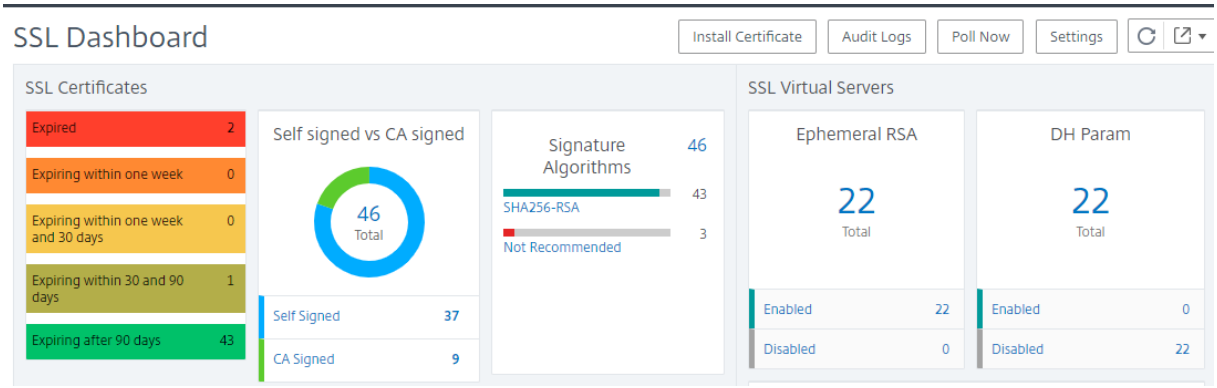
- Nombre de jours après lesquels les certificats expirent
- Nombre de certificats utilisés et non utilisés
- Nombre de certificats autosignés et signés par une autorité de certification
- Nombre d'émetteurs
- Des algorithmes de signature
- Protocoles SSL
- 10 instances les plus importantes par nombre de certificats utilisés

Pour surveiller les certificats SSL

Vous pouvez utiliser le tableau de bord SSL de NetScaler ADM pour surveiller vos certificats si votre entreprise dispose d'une stratégie SSL dans laquelle vous avez défini certaines exigences en matière de certificats SSL, par exemple, tous les certificats doivent avoir une force de clé minimale de 2 048 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 NetScaler ADM, accédez**à** Infrastructure > SSL Dashboard.



NetScaler ADM vous permet d'interroger les certificats SSL et d'ajouter immédiatement tous les certificats SSL des instances à NetScaler ADM. Pour ce faire,

1. Accédez à **Infrastructure > Tableau de bord SSL**.

2. Cliquez sur **Interroger maintenant**.

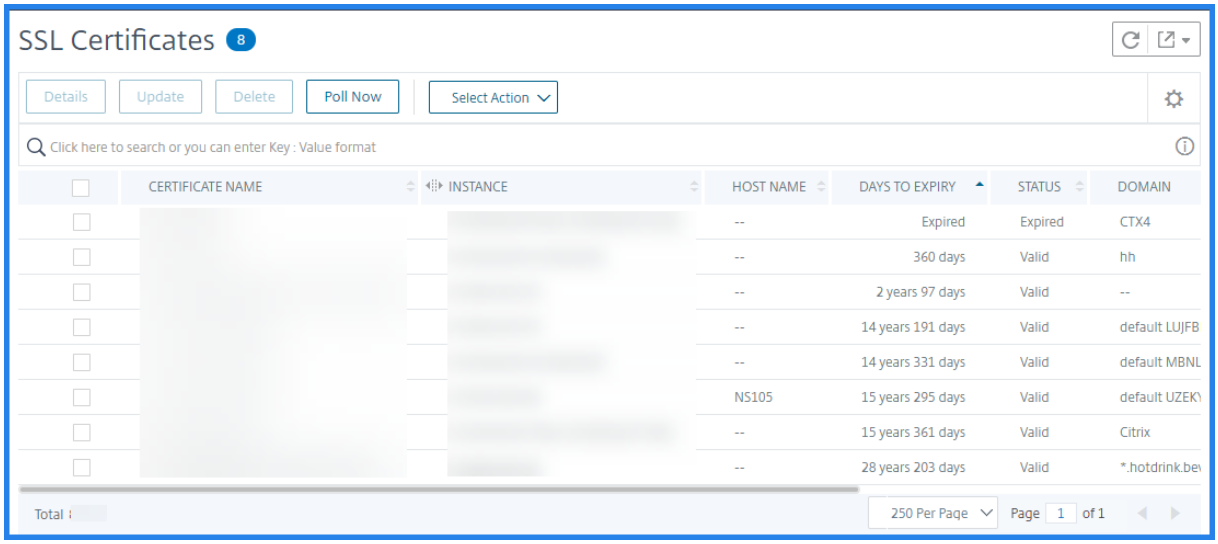
   Sur la page **Poll Now**, vous pouvez interroger toutes les instances ADC gérées ou sélectionner des instances spécifiques.

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 situé sous **Self signed vs CA signed** sur le tableau de bord, l'interface graphique ADM affiche tous les certificats SSL des instances NetScaler.



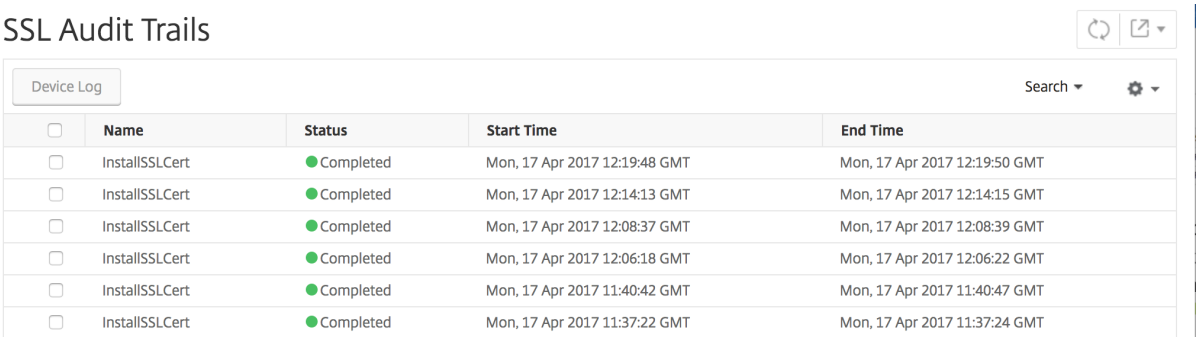
Le tableau de bord SSL NetScaler ADM montre également la distribution des protocoles SSL qui s'exécutent sur vos serveurs virtuels. En tant qu'administrateur, vous pouvez spécifier les protocoles que vous souhaitez surveiller via la stratégie SSL. Pour plus d'informations, reportez-vous à la section 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.

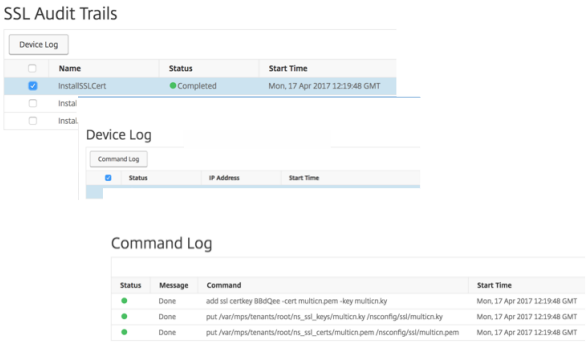
Pour afficher les pistes d'audit des certificats SSL

Vous pouvez désormais consulter les détails du journal des certificats SSL sur NetScaler ADM. Les détails du journal affichent les opérations effectuées à l'aide de certificats SSL sur NetScaler ADM, telles que : l'installation de certificats SSL, l'association et la dissociation de certificats SSL, la mise à jour des certificats SSL et la 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 NetScaler ADM à l'aide de certificats SSL, accédez à **Infrastructure > 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.

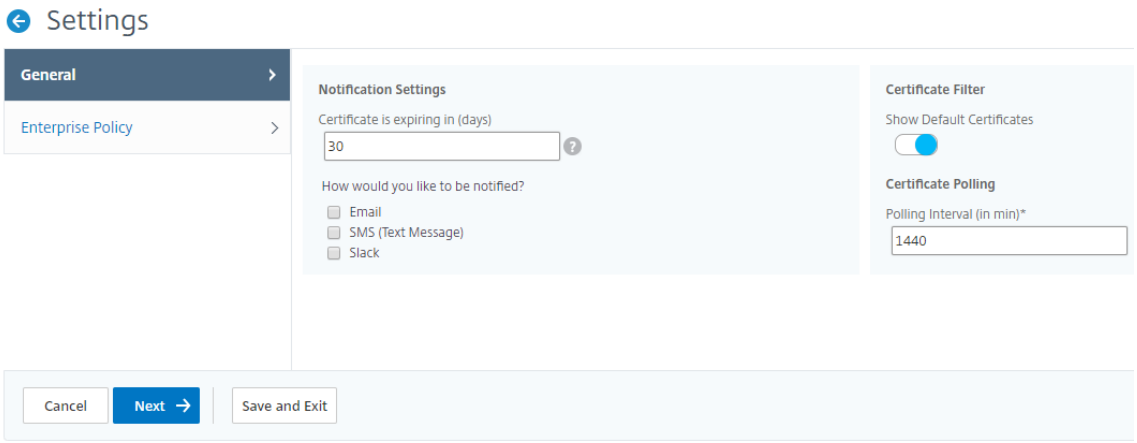


Pour exclure les certificats NetScaler par défaut du tableau de bord SSL

NetScaler ADM vous permet d'afficher ou de masquer les certificats NetScaler par défaut qui apparaissent sur les graphiques du tableau de bord SSL 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 **Infrastructure > Tableau de bord SSL** dans l'interface graphique de NetScaler 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 certificats**, décochez la case **Afficher les certificats par défaut** et cliquez sur **Enregistrer et quitter**.



Afficher, télécharger et télécharger des fichiers SSL

Pour afficher les fichiers SSL sur NetScaler ADM, accédez à **Infrastructure > Tableau de bord SSL > Fichiers SSL sur**NetScaler ADM.

Vous pouvez afficher, charger et télécharger les fichiers suivants sur NetScaler ADM :

- Certificats SSL
- Clés SSL
- CSR SSL

Pour afficher et télécharger des fichiers SSL sur une instance NetScaler, accédez à **Infrastructure > Tableau de bord SSL > Fichiers SSL sur**NetScaler.

Vous ne pouvez accéder aux fichiers SSL qu'une fois les instances NetScaler sauvegardées, soit manuellement, soit par le biais d'un processus de sauvegarde planifié.

> **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 fonc-

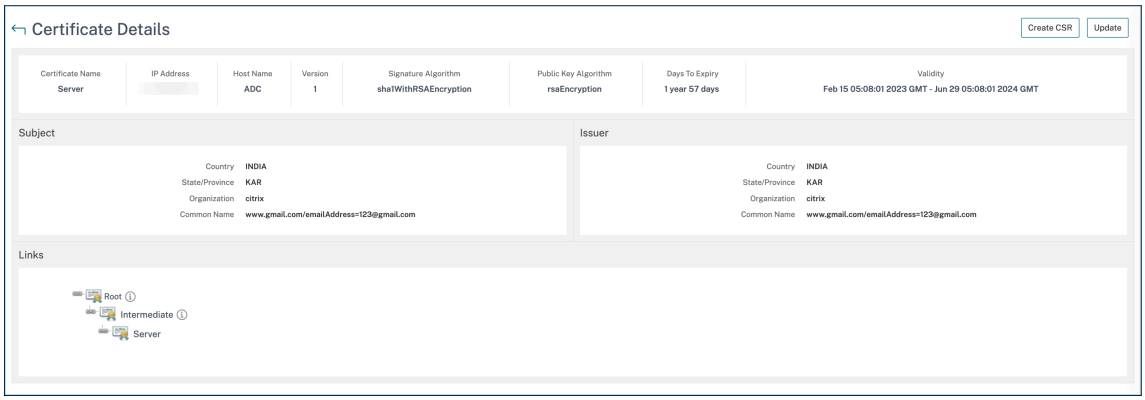
> tionnalités ADM.

Afficher la chaîne de certificats SSL

Vous pouvez consulter la chaîne de certificats complète, depuis les certificats intermédiaires jusqu'au certificat de l'autorité de certification racine.

Pour consulter une chaîne de certificats :

1. Accédez à **Infrastructure > Tableau de bord SSL** et cliquez sur les certificats SSL dans n'importe quelle vignette.
2. Sur la page **Certificats SSL**, sélectionnez un certificat et cliquez sur **Détails**. La chaîne de certificats s'affiche sous **Liens**.



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.

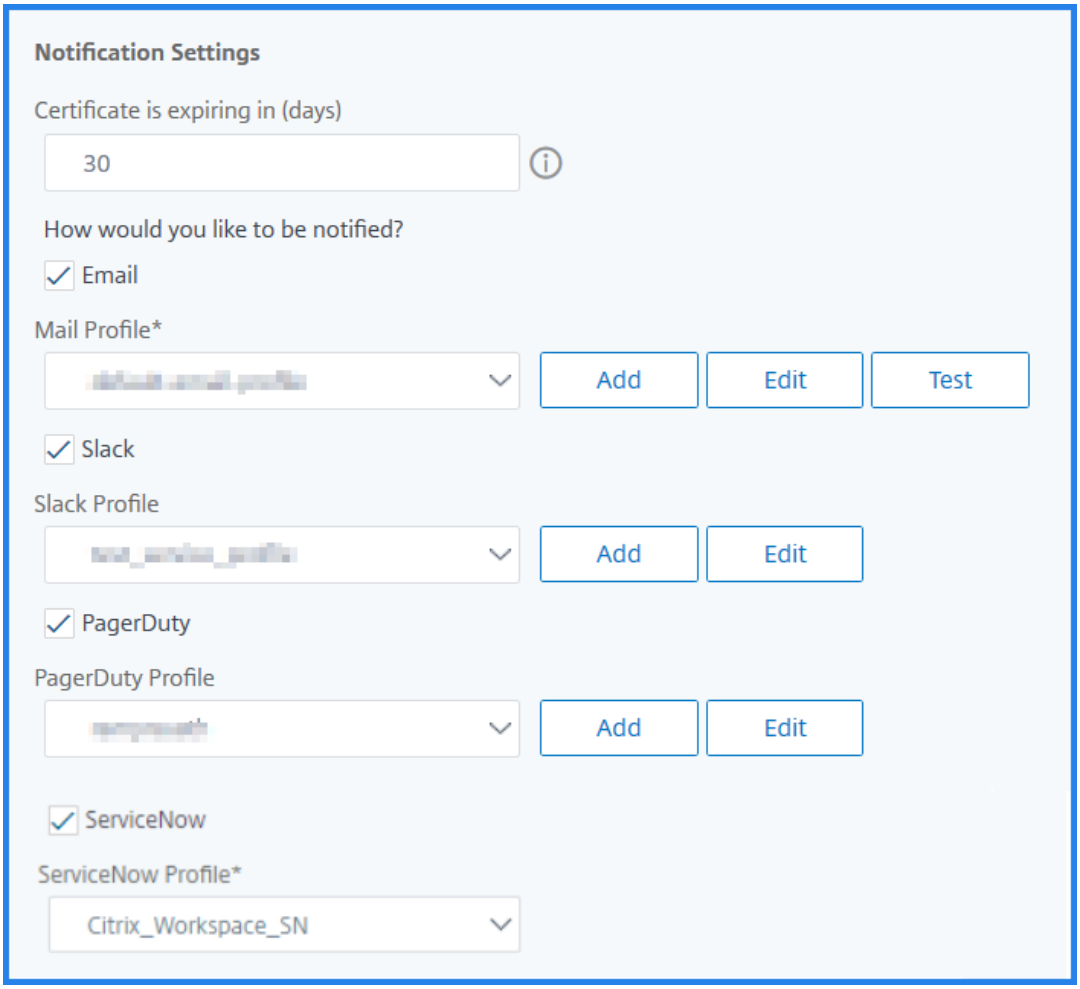
Pour configurer les notifications depuis NetScaler ADM :

1. Dans NetScaler Application Delivery Management (ADM), accédez à **Infrastructure > 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 Citrix Cloud ITSM est configuré pour ServiceNow et intégré à NetScaler ADM. Pour plus d'informations, voir Intégrer NetScaler ADMà l'instance ServiceNow.



6. Cliquez sur **Enregistrer et quitter**.

NetScaler ADM envoie désormais le piège d'expiration des certificats SSL au serveur de destination externe lorsque vos certificats SSL arrivent à expiration. NetScaler ADM envoie un piège 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 de déroutement en accédant à **Paramètres > SNMP > Destinations des déroutements**. 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.

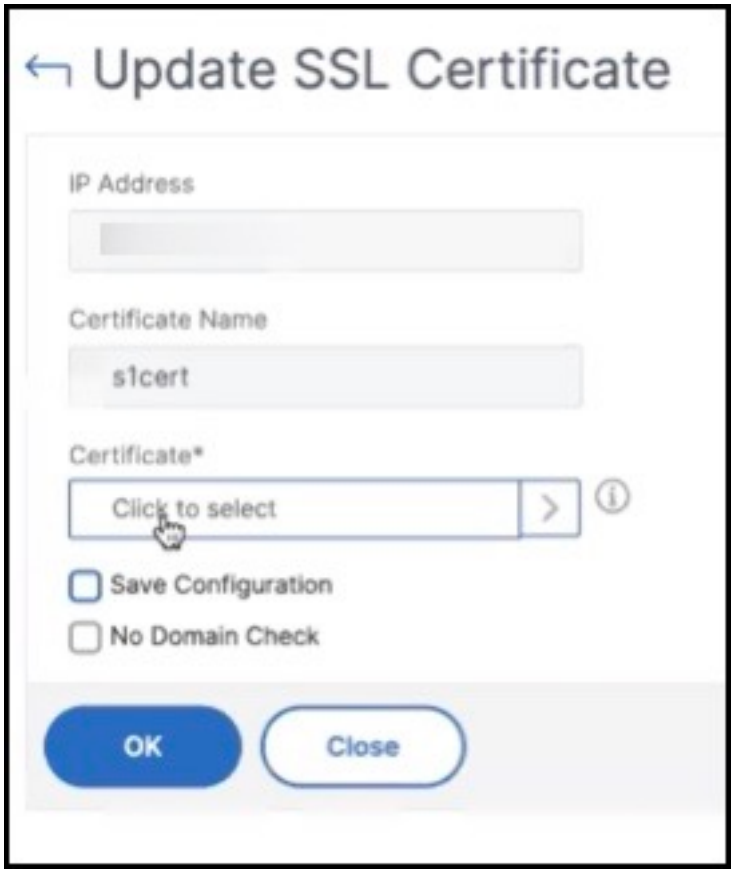
Mettre à jour un certificat installé

February 1, 2024

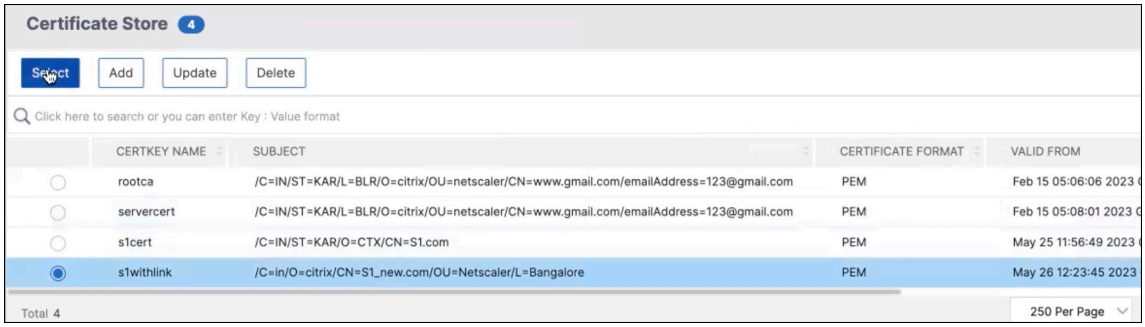
Une fois que vous avez reçu un certificat renouvelé de la part de l'autorité de certification (CA), vous n'avez pas besoin de vous connecter à des instances NetScaler individuelles pour mettre à jour les certificats. Vous pouvez mettre à jour les certificats existants dans NetScaler ADM avec les certificats du magasin de certificats.

Pour mettre à jour un certificat SSL depuis NetScaler ADM, procédez comme suit :

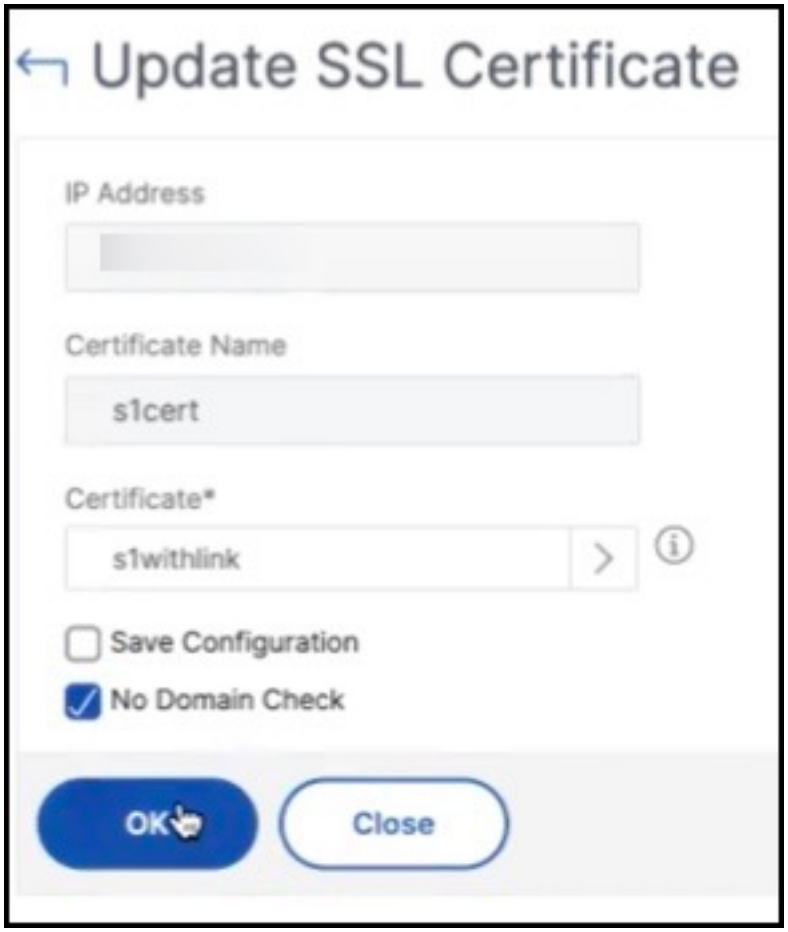
1. Dans NetScaler ADM, accédez à **Infrastructure > Tableau de bord SSL**.
2. Cliquez sur l'un des graphiques pour afficher la liste des certificats SSL.
3. Sur la page **Certificats SSL**, sélectionnez un certificat et cliquez sur **Mettre à jour**. Vous pouvez également cliquer sur le certificat SSL 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**, sélectionnez **Certificat** pour afficher la page du **magasin de certificats** .



5. Sur la page **Certificate Store**, sélectionnez le fichier de certificat que vous souhaitez ajouter. Cliquez sur **Sélectionner**.



6. Si le nom de domaine du nouveau certificat ne correspond pas à l'ancien certificat, sélectionnez **Aucune vérification de domaine** si vous souhaitez que le serveur héberge le nouveau domaine.



Cliquez sur **OK**. Tous les serveurs virtuels SSL auxquels ce certificat est lié sont automatiquement mis à jour.

> **Remarque :**
>
> Lorsque vous mettez à jour un certificat SSL existant avec une chaîne de certificats

> provenant du magasin de certificats, le certificat existant est mis à jour avec les certificats liés. Sélectionnez le certificat et cliquez sur **Détails** pour afficher la chaîne de certificats.

Installation de certificats SSL sur une instance NetScaler

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 NetScaler :

Vous pouvez également importer un certificat à partir d'une instance NetScaler choisie et l'appliquer à d'autres instances NetScaler ciblées à partir de l'interface graphique NetScaler Application Delivery Management (ADM).

1. Accédez à **Infrastructure > Tableau de bord SSL**.
2. Dans l'angle supérieur droit du tableau de bord SSL, cliquez sur **Installer**.
3. Sur la page **Installer le certificat SSL sur les instances NetScaler** , spécifiez les paramètres suivants :

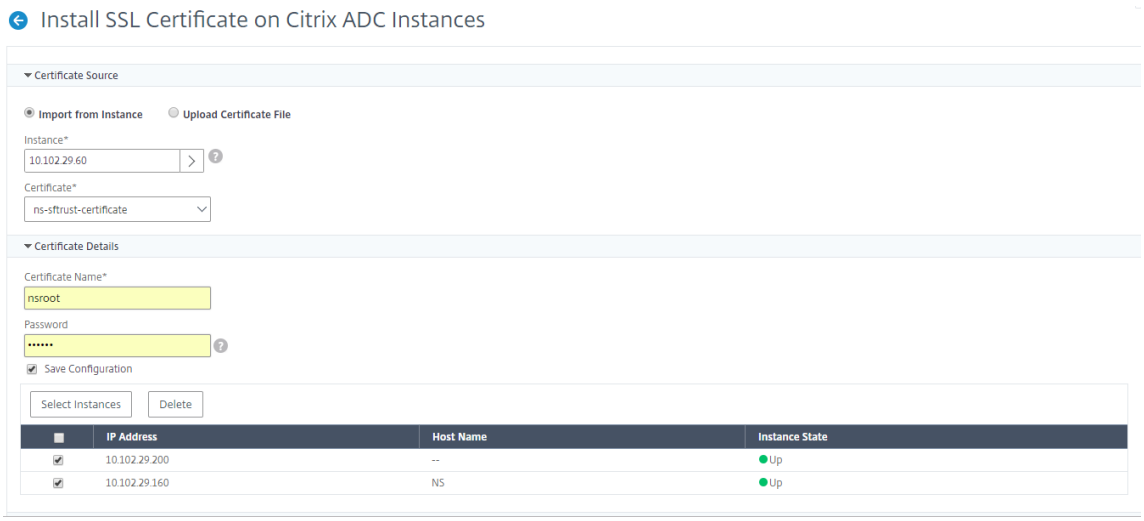
    a) Source du certificat
    Sélectionnez l'option **Importer à partir d'une instance**.

    - 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

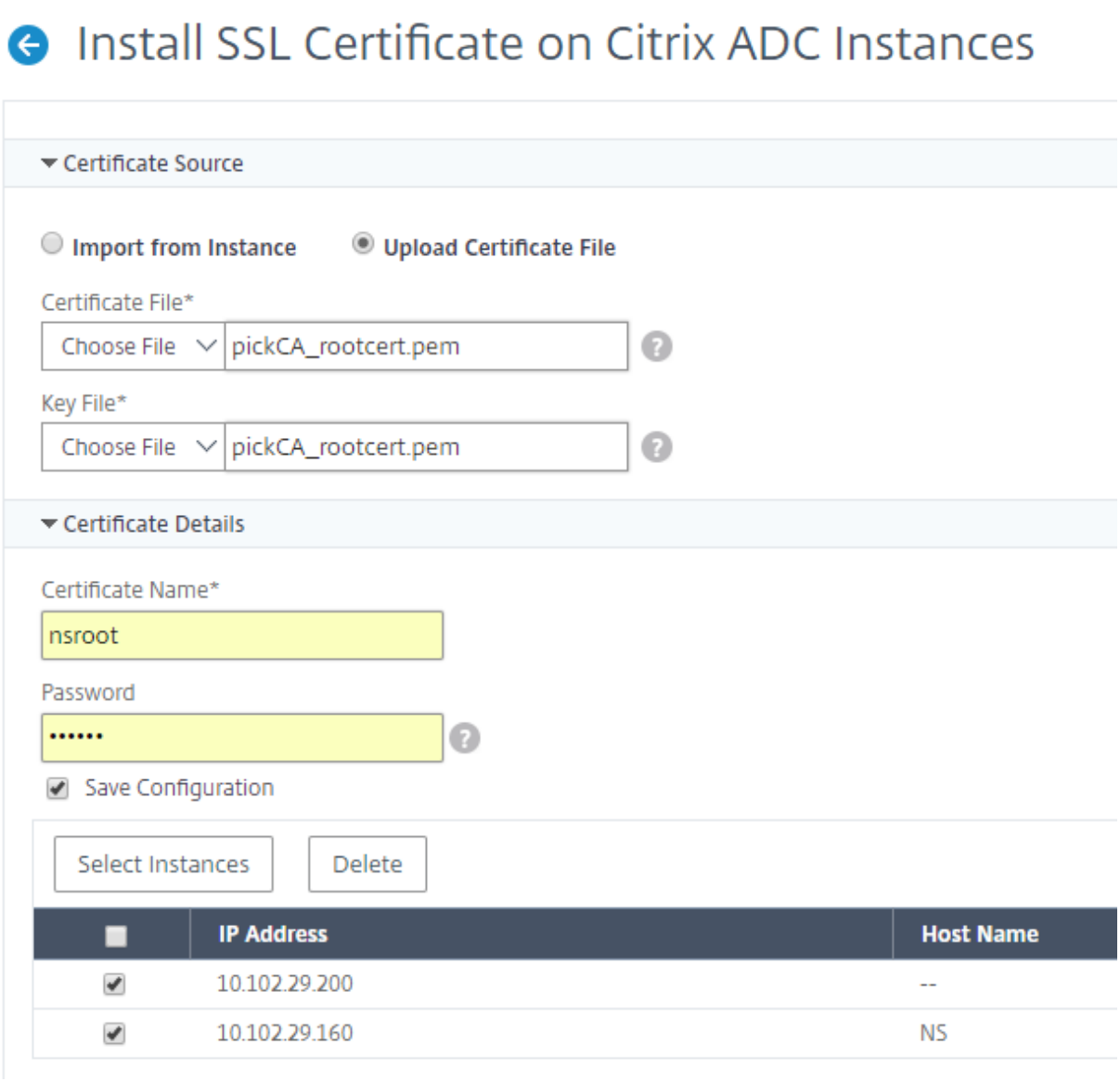
    - **Nom du certificat**. Spécifiez le nom de la clé de certificat.
    - **Mot de passe**. Mot de passe pour crypter la clé privée. Vous pouvez utiliser cette option pour télécharger des clés privées chiffrées.

4. Cliquez sur **Sélectionner les instances** pour sélectionner les instances NetScaler sur lesquelles vous souhaitez installer vos certificats.
5. Cliquez sur **OK**.



Pour installer un certificat SSL depuis NetScaler ADM :

1. Dans NetScaler ADM, accédez à **Infrastructure > Tableau de bord SSL**.
2. Dans l'angle supérieur droit du tableau de bord, cliquez sur **Installer**.
3. Sur la page **Installer un certificat SSL sur une instance NetScaler**, **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 NetScaler 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.
   - **Sélectionnez les instances** : sélectionnez les instances NetScaler 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 NetScaler ADM :

1. Dans NetScaler Application Delivery Management (ADM), accédez à **Infrastructure > 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 charger votre fichier clé, sélectionnez **Local** (votre machine locale) ou **Appliance** (le fichier clé doit être présent sur l'instance virtuelle NetScaler 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.

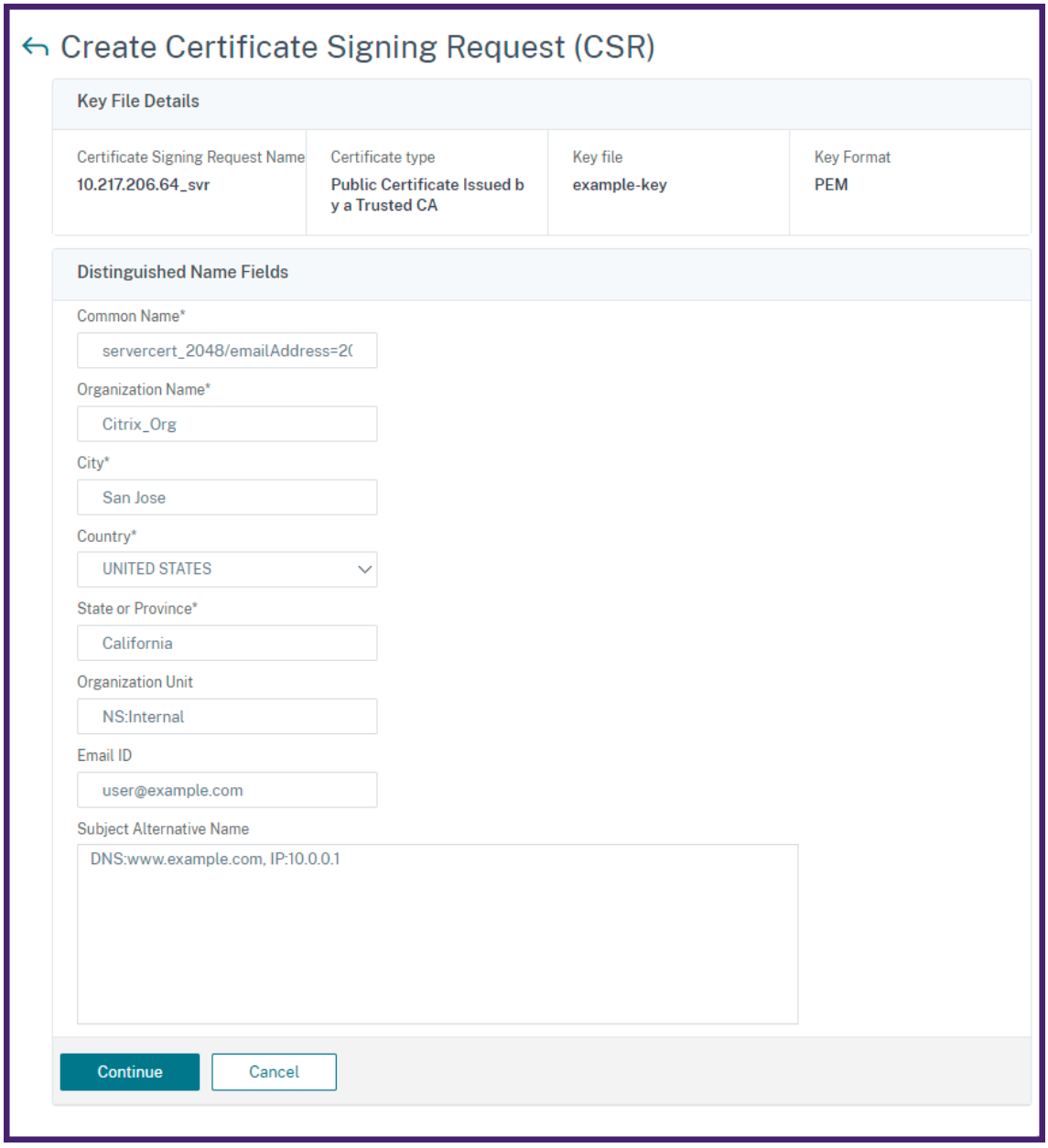
5. Cliquez sur **Continue**.
6. Sur la page suivante, fournissez plus de détails.

   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 NetScaler ADM :

1. Dans NetScaler Application Delivery Management (ADM), accédez à **Infrastructure > 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 NetScaler ADM :

1. Dans NetScaler ADM, accédez à **Infrastructure > 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 fiables, des algorithmes de signature sécurisés et sélectionner le niveau de clé recommandé pour vos clés de certificat dans NetScaler 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 NetScaler ADM, procédez comme suit :

1. Dans NetScaler 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.

   > **Remarque**
   >
   > Le tableau de bord SSL affiche uniquement les **algorithmes de signature** sélectionnés via l'option **Paramètres** et les autres sont affichés comme **Non recommandés**.

Interroger les certificats SSL provenant d'instances NetScaler

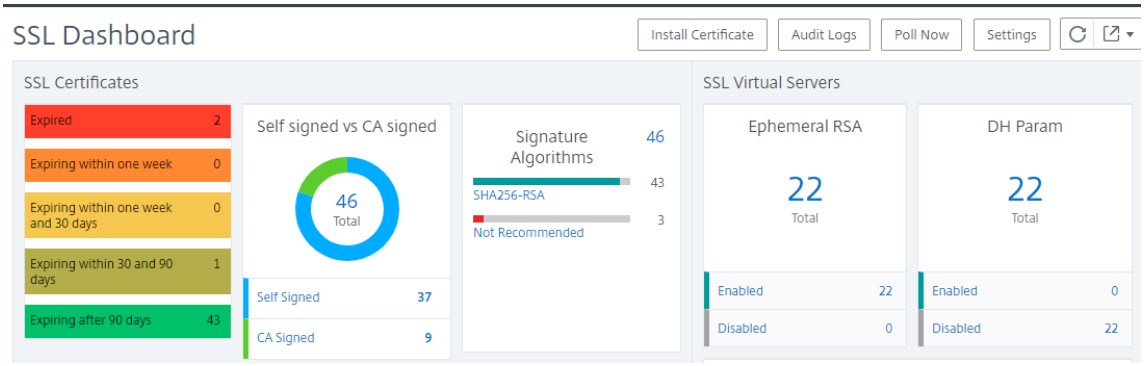
February 1, 2024

NetScaler Application Delivery Management (ADM) interroge automatiquement les certificats SSL toutes les 24 heures à l'aide des 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 des certificats SSL de toutes les instances NetScaler fait peser une lourde charge sur le réseau.

Au lieu d'interroger tous les certificats SSL des instances NetScaler, vous pouvez interroger manuellement uniquement les certificats SSL d'une ou plusieurs instances sélectionnées.

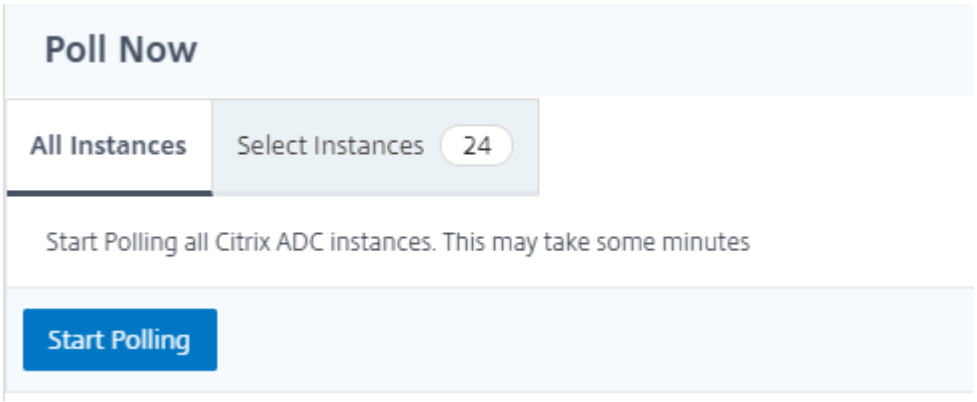
Pour interroger les certificats SSL sur les instances NetScaler :

1. Dans NetScaler ADM, accédez à **Infrastructure > Tableau de bord SSL**.
2. Dans la page **Tableau de bord SSL**, dans le coin supérieur droit, cliquez sur **Sondage maintenant** .

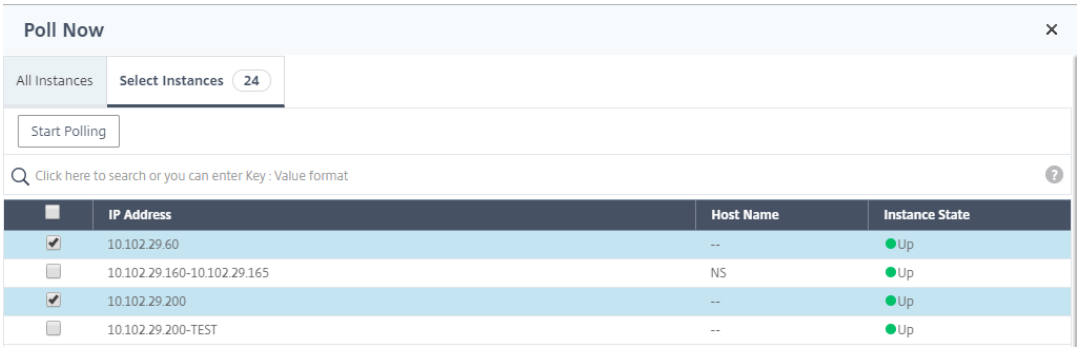


3. La page **Poll Now** s'affiche et vous permet d'interroger toutes les instances NetScaler du réseau ou d'interroger les instances sélectionnées.

   a) Pour interroger les certificats SSL de toutes les instances NetScaler, 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**.



Utiliser le magasin de certificats NetScaler ADM pour gérer les certificats SSL

February 1, 2024

Le magasin de certificats NetScaler ADM vous permet de stocker et de gérer vos certificats SSL en un seul endroit. Vous pourrez ensuite utiliser les certificats enregistrés pour configurer les paramètres NetScaler.

Le magasin de certificats vous permet d'ajouter, de mettre à jour et de supprimer des certificats SSL. Vous pouvez également utiliser le magasin de certificats pour importer un certificat depuis une instance NetScaler et l'appliquer à d'autres instances NetScaler ciblées.

Ajouter des certificats SSL au magasin de certificats

1. Accédez à **Infrastructure > Tableau de bord SSL > Magasin de certificats**. Cliquez sur **Ajouter**.
2. Sur la page **Ajouter un certificat**, entrez les informations suivantes :
    - **Nom de la clé de certification** : entrez le nom du certificat. Le nom ne doit comporter que des caractères alphanumériques ASCII, des traits de soulignement et des tirets et doit comporter moins de 30 caractères. Vous ne pouvez pas modifier le nom une fois le certificat créé.
    - **Fichier de certificat** : accédez à votre disque local et téléchargez le fichier de certificat.
    - **Fichier clé** : téléchargez le fichier clé depuis votre ordinateur local.
    - **Mot de passe** : si vous avez une clé privée chiffrée au format PEM, saisissez le mot de passe utilisé pour chiffrer la clé privée.
    - **Ajouter une chaîne de certificats** : sélectionnez cette option pour ajouter le certificat dans une chaîne de certificats.

- **Chaîne de certificats** : accédez à votre disque local et téléchargez le fichier de certificat.
- Cliquez sur **Créer**.

Mettre à jour les certificats SSL dans le magasin de certificats

1. Accédez à **Infrastructure > Tableau de bord SSL > Magasin de certificats**. Sélectionnez le certificat que vous souhaitez mettre à jour et cliquez sur **Mettre à jour**.
2. Sur la page **Mettre à jour le certificat**, entrez les informations suivantes :
   - **Nom de la clé de certification** : affiche le nom du certificat que vous avez sélectionné pour la mise à jour.
   - **Fichier de certificat** : pour mettre à jour le fichier de certificat, téléchargez-le.
   - **Fichier clé** - Pour mettre à jour le fichier clé, téléchargez un fichier clé depuis votre ordinateur local.
   - **Mot de passe** : si vous avez une clé privée chiffrée au format PEM, saisissez le mot de passe utilisé pour chiffrer la clé privée.
   - **Ajouter une chaîne de certificats** : sélectionnez cette option pour ajouter le certificat dans une chaîne de certificats.
   - **Chaîne de certificats** : accédez à votre disque local et téléchargez le fichier de certificat.
   - Cliquez sur **OK**.

Supprimer les certificats SSL du magasin de certificats

1. Accédez à **Infrastructure > Tableau de bord SSL > Magasin de certificats**. Cliquez sur **Ajouter**.
2. Lorsque vous y êtes invité, cliquez sur **Oui** pour supprimer le certificat.

Installation de certificats SSL sur les instances NetScaler

1. Accédez à **Infrastructure > Tableau de bord SSL > Magasin de certificats**. Sélectionnez le certificat que vous souhaitez installer sur une instance NetScaler.
2. Sur la page **Installer le certificat SSL sur les instances NetScaler**, entrez les informations suivantes :

   a. **Source du certificat**

   - **Certificat** : affiche le nom du certificat que vous avez sélectionné.

b. **Détails du certificat**

- **Nom du certificat** : affiche le nom du certificat.
- **Enregistrer la configuration** : sélectionnez cette option pour enregistrer la configuration NetScaler. La configuration NetScaler est enregistrée après l'installation du certificat.

3. Cliquez sur **Sélectionner les instances** pour sélectionner les instances NetScaler sur lesquelles vous souhaitez installer vos certificats.

Cliquez sur **OK**.

Importer des certificats depuis des instances NetScaler

1. Accédez à **Infrastructure > Tableau de bord SSL > Magasin de certificats**. Cliquez sur **Importer des certificats ADC**.
2. Sur la page **Importer des certificats ADC**, vous pouvez sélectionner l'un des onglets suivants :

   - **Importer des certificats ADC** : cliquez sur **Démarrer le sondage** pour interroger tous les certificats SSL sur toutes les instances NetScaler.
   - **Sélectionnez des instances** : sélectionnez une instance NetScaler et **cliquez sur Importer des certificats ADC** pour interroger les certificats SSL uniquement sur l'instance NetScaler sélectionnée.

   Après le sondage, les certificats SSL et les fichiers clés sont téléchargés et ajoutés au magasin de certificats.

   > **Remarque :**
   >
   > L'opération d'importation échoue pour les certificats si des noms de certificats identiques existent dans le magasin. Cependant, l'opération d'importation continue à interroger les certificats restants et ajoute les certificats NetScaler, s'ils sont disponibles, au magasin.

Gérez les certificats et chiffrements personnalisés de base de données dans le cadre d'un déploiement à haute disponibilité

February 1, 2024

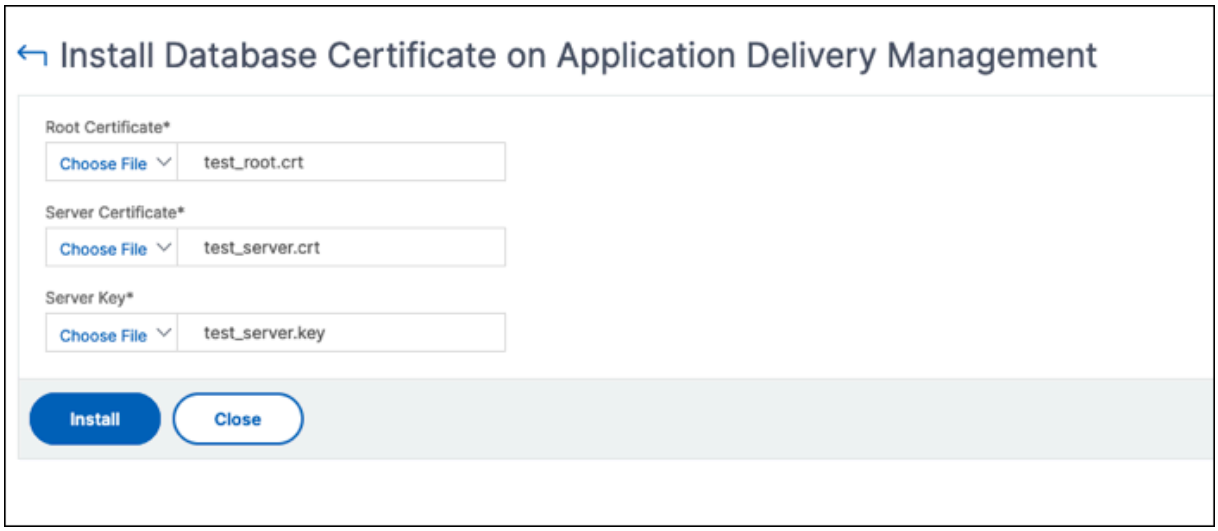
NetScaler ADM vous permet de remplacer les certificats de base de données intégrés par défaut par vos propres certificats émis par une autorité de certification de confiance. Vous pouvez également

configurer vos propres suites de chiffrement dans la base de données NetScaler ADM. Cette fonctionnalité offre une flexibilité et une sécurité accrues pour répondre à vos besoins en matière de gestion des certificats, et sécurise toutes les communications entre vos nœuds HA grâce à des certificats SSL fiables.

Installez vos certificats de base de données sur NetScaler ADM

Pour installer vos certificats dans une configuration HA :

1. Accédez à **Paramètres > Déploiement HA** et cliquez sur **Certificats de base de données**.
2. Cliquez sur l'onglet **Certificat installé**, puis sur **Installer un nouveau certificat**.
3. Sur la page **Installer le certificat de base de données sur la gestion de la mise à disposition des applications**, chargez un certificat racine, un certificat de serveur et une clé de serveur. Vous pouvez effectuer l'une des opérations suivantes :
    - **Choisissez Fichier > Local** pour télécharger un certificat ou un fichier clé depuis votre ordinateur local.
    - **Choisissez Fichier > Appliance** pour télécharger un certificat ou un fichier clé présent sur NetScaler ADM.
4. Cliquez sur **Installer**.



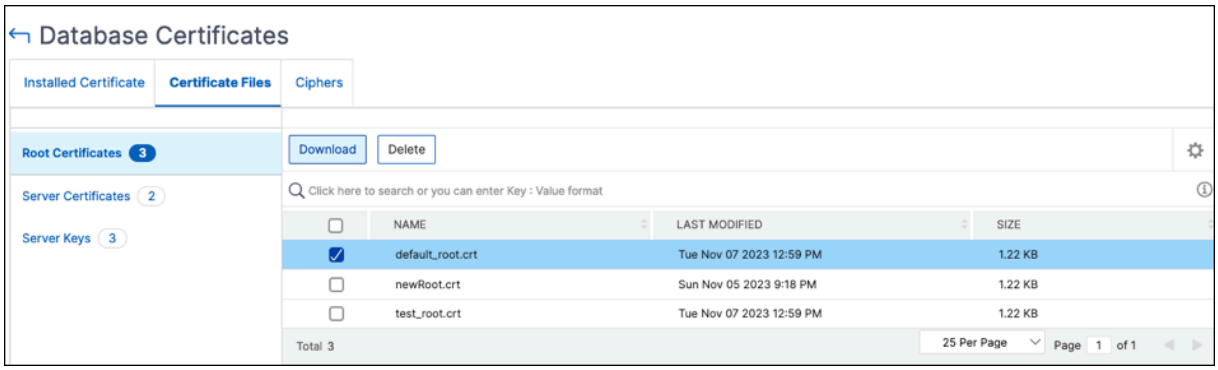
> **Remarque :**
>
> S'il existe plusieurs certificats de chaîne, vous devez les combiner dans un seul fichier. Assurez-vous que l'ordre de concaténation est correct, en commençant par les certificats intermédiaires, suivis du certificat racine. Cet ordre est essentiel pour que la chaîne de certificats soit reconnue correctement.
>
> Par exemple, la commande suivante ajoute le contenu de chaque fichier de certificat (intermedi-

> ate_certificate1.crt, intermediate_certificate2.crt et root_certificate.crt) au fichier nommé combined_certs.crt :
>
> ```
> cat intermediate_certificate1.crt >> combined_certs.crt
> cat intermediate_certificate2.crt >> combined_certs.crt
> cat root_certificate.crt >> combined_certs.crt
> ```

Gérez vos certificats de base de données installés

Pour consulter, télécharger et supprimer les certificats que vous avez installés :

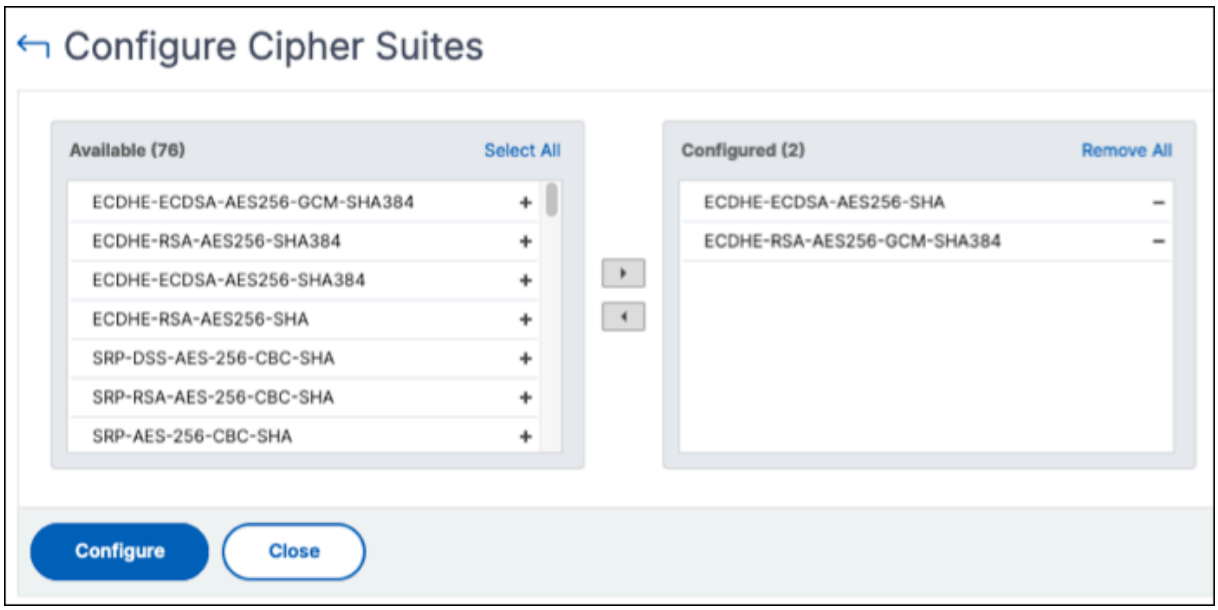
1. Accédez à **Paramètres > Déploiement HA** et cliquez sur **Certificats de base de données**.
2. Cliquez sur l'onglet **Fichiers de certificats** et sélectionnez **Certificats racine, Certificats**de **serveur ou Clés** de serveur pour voir les fichiers correspondants.
3. Pour télécharger un fichier sur votre ordinateur local, cliquez sur **Télécharger**.
4. Pour supprimer un fichier de certificat, sélectionnez-le et cliquez sur **Supprimer**. Dans la boîte de dialogue de confirmation qui s'affiche, cliquez sur **OK**.



Configurer les suites de chiffrement de base de données

Pour configurer des suites de chiffrement pour un déploiement HA :

1. Accédez à **Paramètres > Déploiement HA** et cliquez sur **Certificats de base de données**.
2. Cliquez sur l'onglet **Chiffrements**, puis sur **Configurer**le chiffrement.
3. Sur la page **Configurer les suites de chiffrement**, sélectionnez un ou plusieurs chiffrements dans la liste des chiffrements disponibles.
4. Cliquez sur **Configurer**. Dans la boîte de dialogue de confirmation qui apparaît, cliquez sur **Oui** pour modifier les paramètres de chiffrement.



> **Remarque :**
>
> La modification des paramètres de chiffrement redémarre les nœuds secondaire et de reprise après sinistre NetScaler ADM.

Événements

February 1, 2024

Lorsque l'adresse IP d'une instance Citrix Application Delivery Controller (ADC) est ajoutée à NetScaler Application Delivery Management (ADM), NetScaler ADM envoie un appel NITRO et s'ajoute implicitement en tant que 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 NetScaler gérée. Par exemple, en cas de défaillance du système ou de modification de la configuration, un événement est généré et enregistré sur le serveur NetScaler ADM. Les événements reçus dans NetScaler ADM sont affichés sur la page Résumé des événements (**Infrastructure Événements)**, et tous les événements actifs sont affichés sur la page Messages d'événements (**Infrastructure > Événements > Messages** d'événements).

NetScaler ADM vérifie également les événements générés sur les instances pour générer 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 votre infrastructure NetScaler.

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

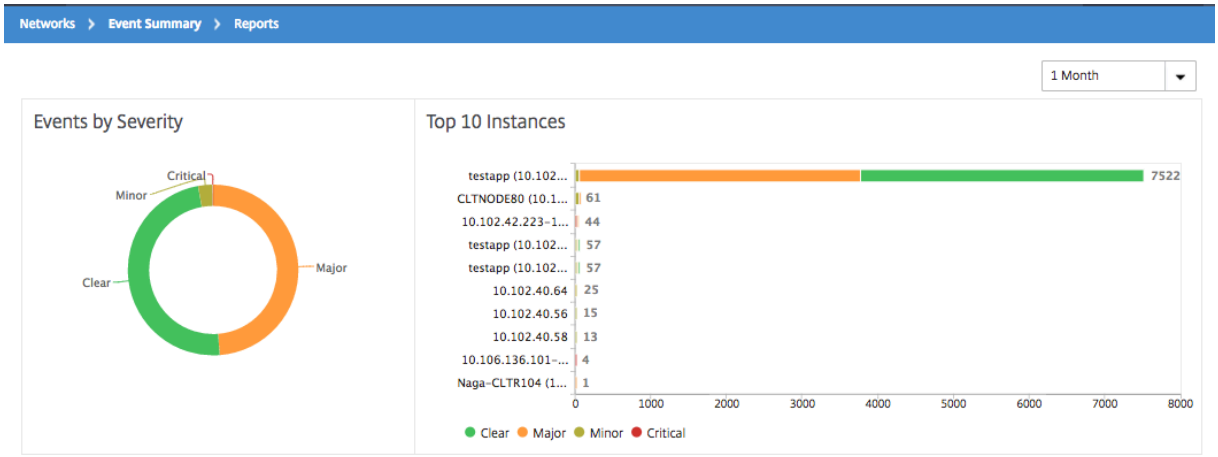
February 1, 2024

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 NetScaler Application Delivery Management (ADM) pour consulter les rapports générés contenant des informations détaillées sur la gravité des événements critiques sur toutes vos instances NetScaler.

Pour afficher les détails sur le tableau de bord des événements :

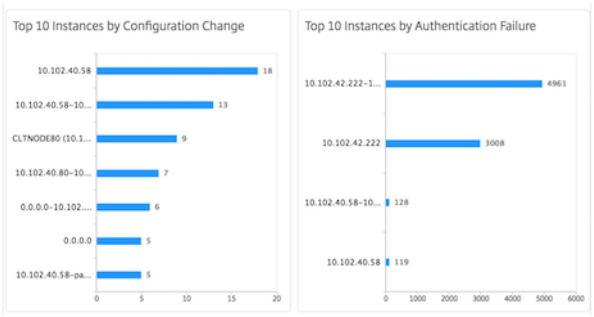
Accédez à **Infrastructure > Événements > Rapports**.

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.

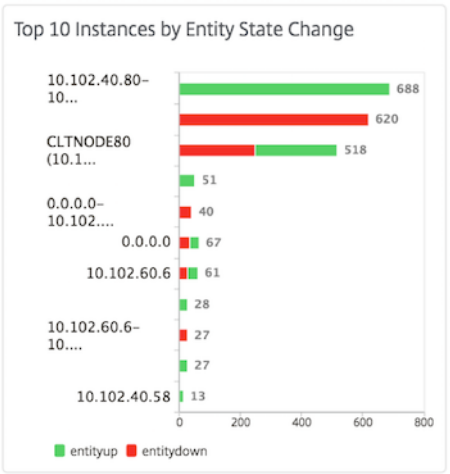


Vous pouvez afficher plus de détails en accédant au type d'instance NetScaler (**Infrastructure > Événements > Rapports ****NetScaler/ NetScaler**SDX) pour afficher les informations suivantes :

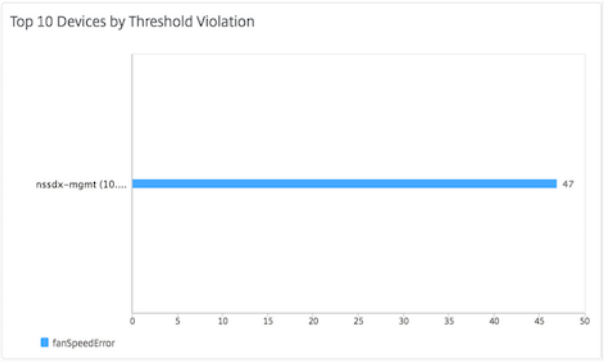
- Top 10 des périphériques par défaillance matérielle
- Les 10 principaux appareils par changement de configuration
- Top 10 des appareils par échec d'authentification



- 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

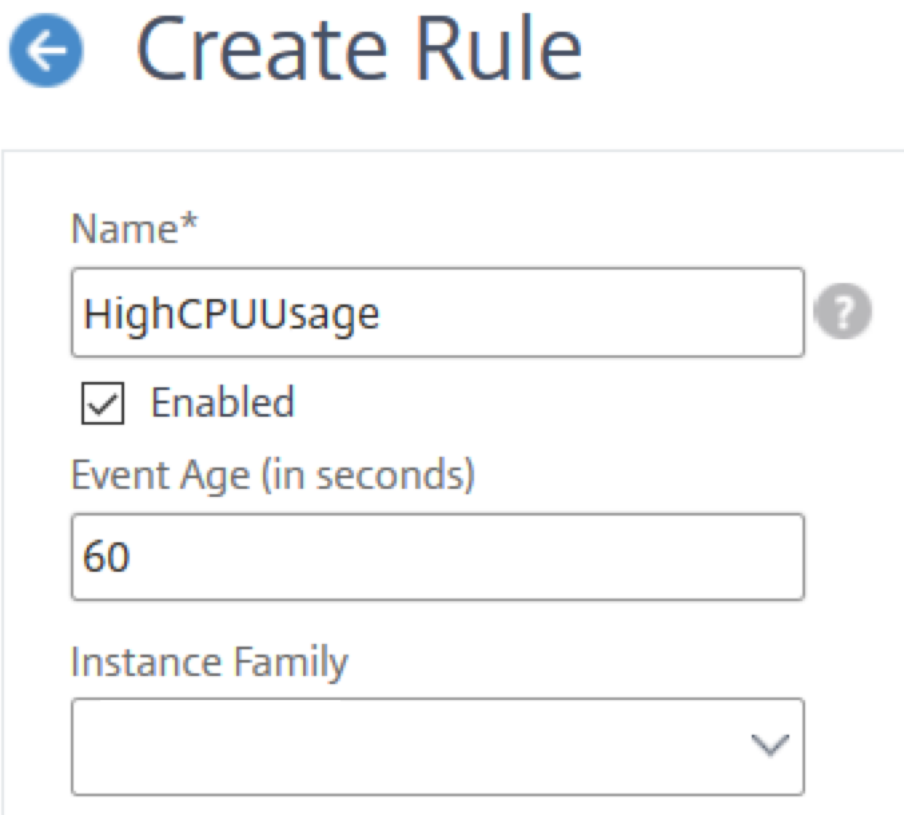
Vous pouvez définir l'option d'âge de l'événement pour spécifier l'intervalle de temps (en secondes). NetScaler ADM surveille les appliances jusqu'à la durée définie et génère un événement uniquement si l'âge de l'événement dépasse la durée définie.

> 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 NetScaler ADM :

1. Dans NetScaler ADM, accédez à **Infrastructure > 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

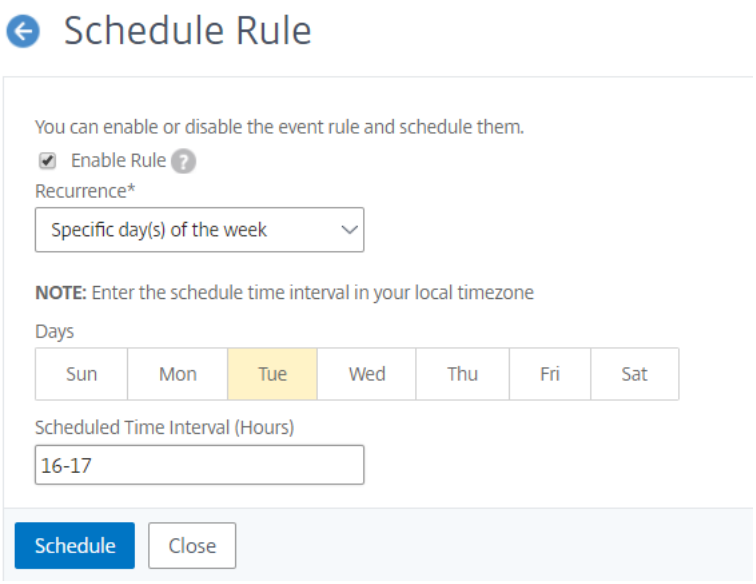
Après avoir créé un filtre pour votre règle, si vous ne souhaitez pas que le serveur NetScaler Application Delivery Management (ADM) envoie une notification chaque fois que l'événement généré répond aux critères du filtre, vous pouvez programmer le filtre pour qu'il se déclenche uniquement à des intervalles de temps spécifiques tels que tous les jours, toutes les semaines ou tous les mois.

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 NetScaler ADM reçoit ces pièges. 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 NetScaler ADM :

1. Dans NetScaler ADM, accédez **à Infrastructure**> 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

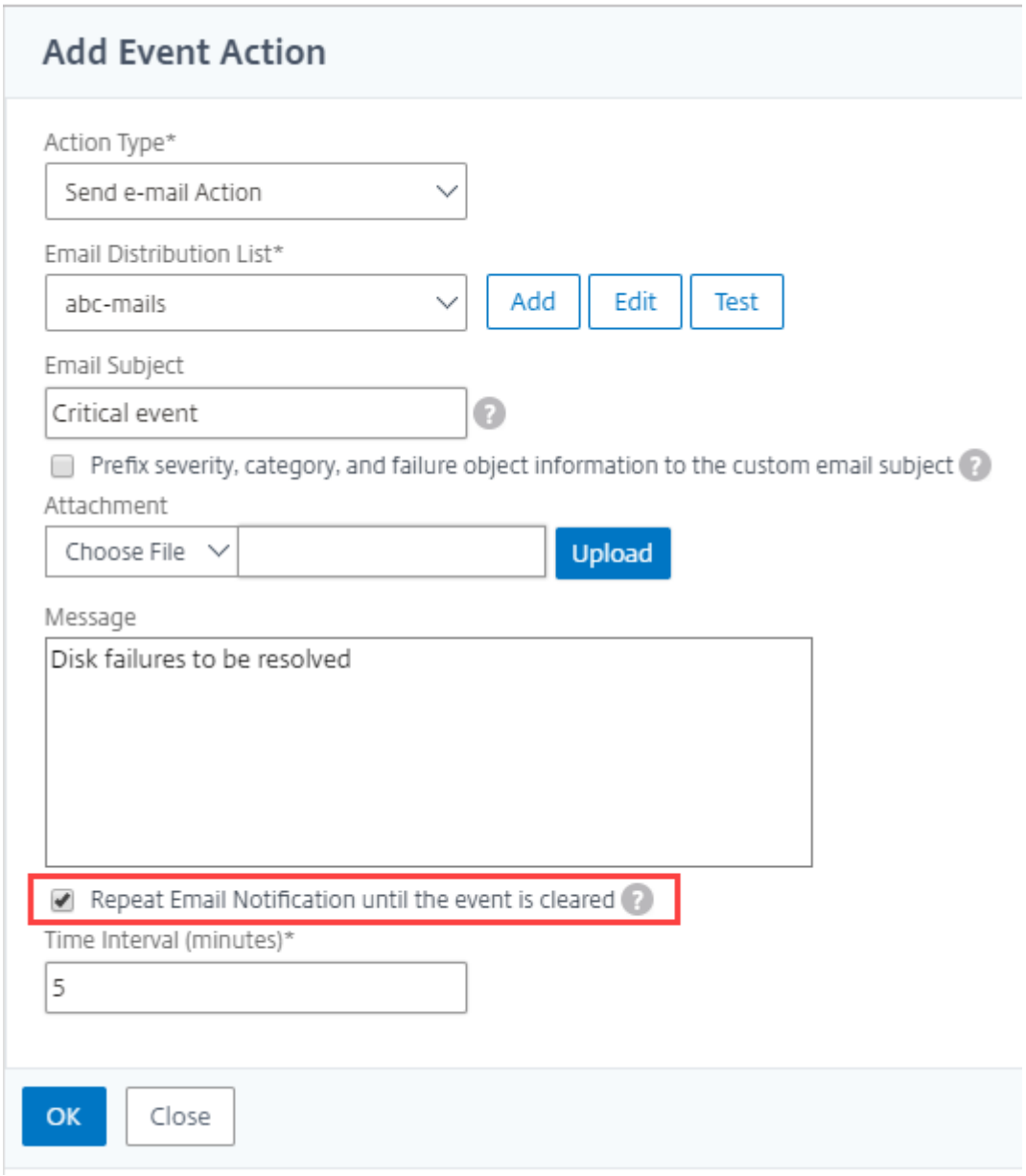
Pour vous assurer que tous les événements critiques sont traités et qu'aucune notification par e-mail importante n'est manquée, vous pouvez choisir d'envoyer des notifications par e-mail répétées pour les règles d'événements qui répondent aux critères que vous avez sélectionnés. Par exemple, si vous 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 **Infrastructure > Événements > Résumé des événements**, choisissez une **catégorie**, sélectionnez un événement dans la catégorie, puis cliquez sur **Effacer**.
> - Vous pouvez également accéder à **Infrastructure > Événements > Messages d'événement**. 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 depuis NetScaler ADM :

1. Dans NetScaler Application Delivery Management (ADM), accédez à **Infrastructure > 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

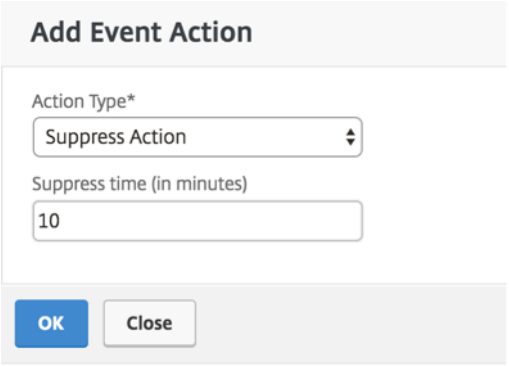
February 1, 2024

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, NetScaler ADM considère que le délai de suppression est nul et il n'expire jamais.

Pour supprimer des événements à l'aide de NetScaler ADM :

1. Dans NetScaler Application Delivery Management (ADM), accédez à **Infrastructure > 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.

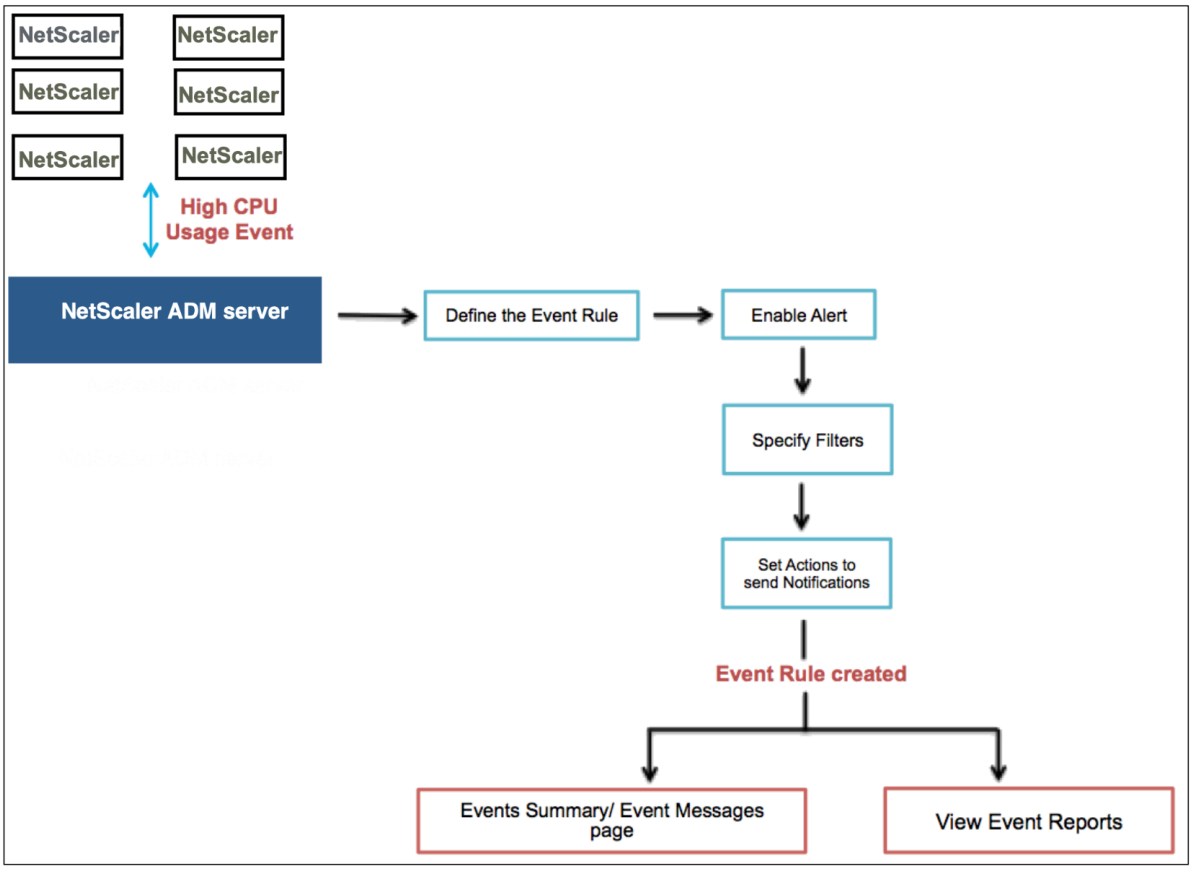
Vous pouvez filtrer un ensemble d'événements en configurant des règles avec des conditions spécifiques et en affectant des actions aux règles. Lorsque les événements générés répondent aux critères de filtre de la règle, l'action associée à la règle est exécutée. Les conditions pour lesquelles vous pouvez créer des filtres sont les suivantes : gravité, instances de Citrix Application Delivery Controller (NetScaler), 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 souhaiterez peut-être surveiller les événements « d'utilisation élevée du processeur » pour des instances NetScaler spécifiques si ces événements peuvent entraîner une panne de vos instances NetScaler. 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. Spécifiez les instances NetScaler 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

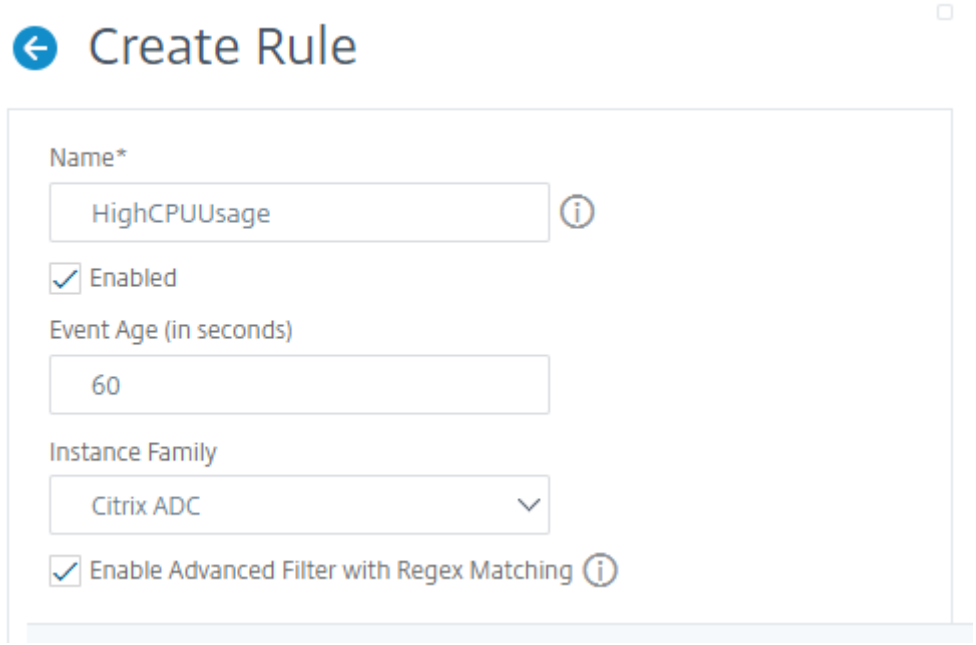
Étape 1 - Définir une règle d'événement

Accédez à **Infrastructure > 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 NetScaler ADM actualise une règle d'événement.

> 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.

Sur la base de l'exemple ci-dessus, vous souhaiterez peut-être être averti par e-mail chaque fois que votre instance NetScaler enregistre 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 NetScaler enregistre un événement « utilisation élevée du processeur » pendant 60 secondes ou plus, vous receviez une notification par e-mail contenant les détails de l'événement.



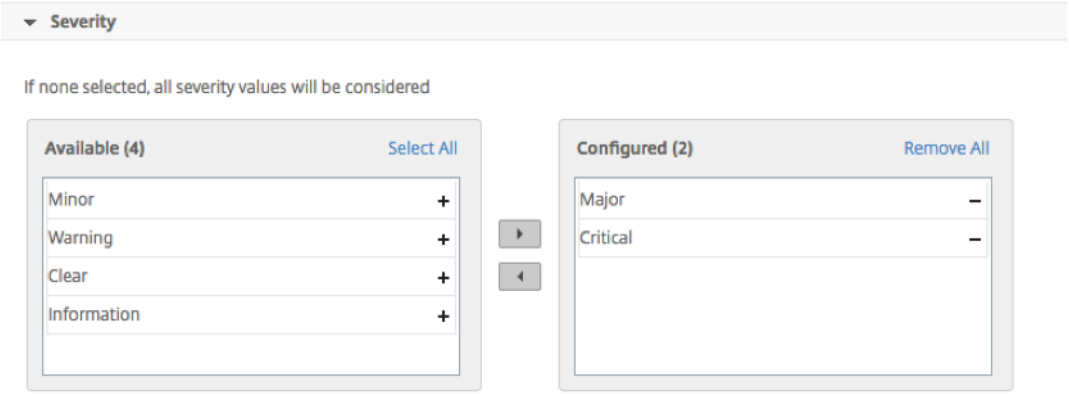
Vous pouvez également filtrer les règles d'événements par **famille d'instances pour suivre l'instance** NetScaler à partir de laquelle NetScaler ADM reçoit un événement.

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.

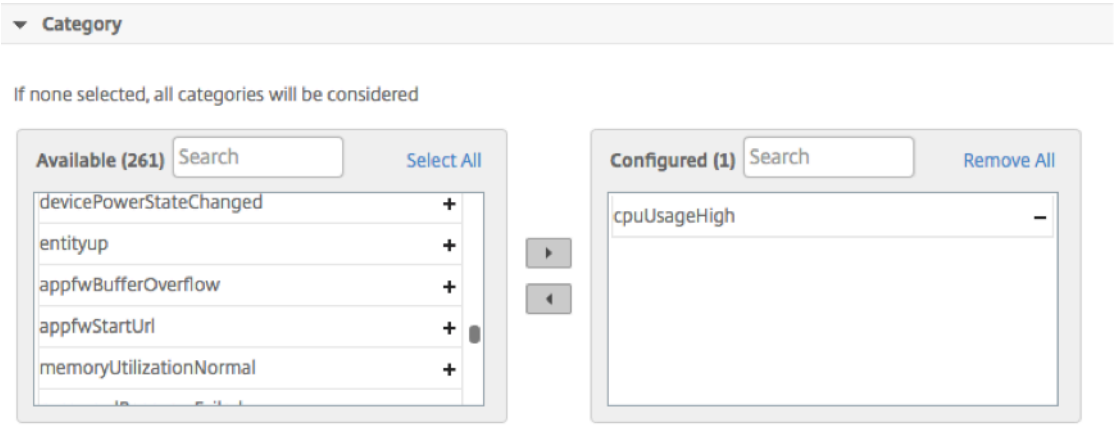


> **Remarque**
>
> Vous pouvez configurer la gravité des événements génériques et spécifiques à Advanced. Pour modifier la gravité des événements pour les instances NetScaler gérées sur NetScaler ADM, accédez à **Infrastructure > Événements > Paramètres des événements**. Choisissez la **catégorie** pour 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

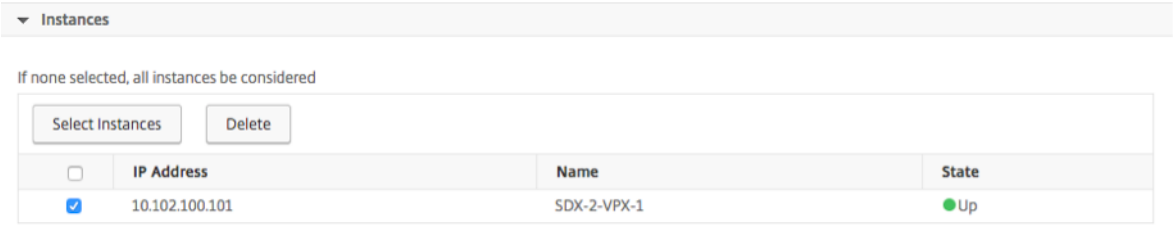
Vous pouvez spécifier la ou les catégories des événements générés par vos instances NetScaler. Toutes les catégories sont créées sur des instances NetScaler. Ces catégories sont ensuite mappées avec NetScaler ADM qui peut être utilisé pour définir des règles d'événements. Sélectionnez la catégorie à prendre en compte et déplacez-la de la table **Disponible** vers la table **configurée**.

Dans l'exemple ci-dessus, vous devez choisir « cpuUsageHigh » comme catégorie d'événement dans le tableau affiché.



Étape 4 - Spécifier les instances NetScaler

Sélectionnez les adresses IP des instances NetScaler 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

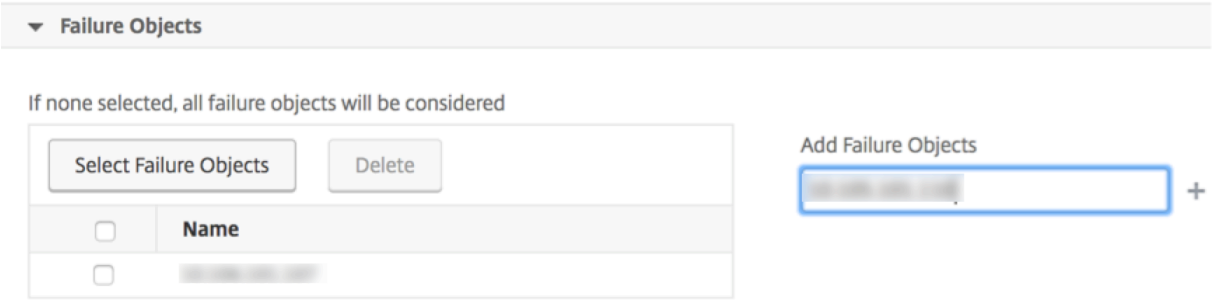
Vous pouvez sélectionner un objet de défaillance dans la liste fournie ou ajouter un objet de défaillance pour lequel un événement a été généré. Vous pouvez également spécifier une expression régulière pour ajouter des objets de défaillance. En fonction de l'expression régulière spécifiée, les objets 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 défaillant affecte la façon dont un événement est traité et garantit 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.

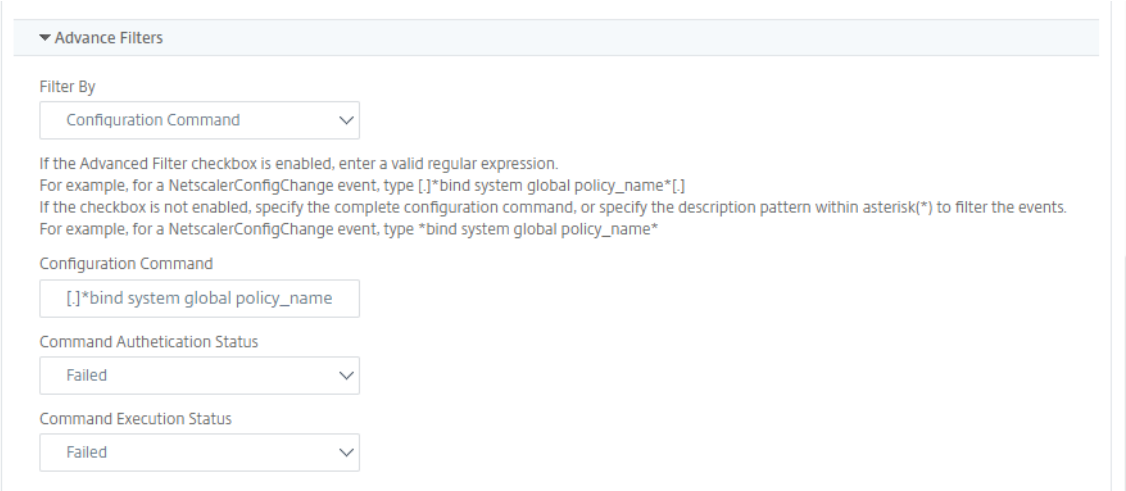


Étape 6 - Spécifier les filtres avancés

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.

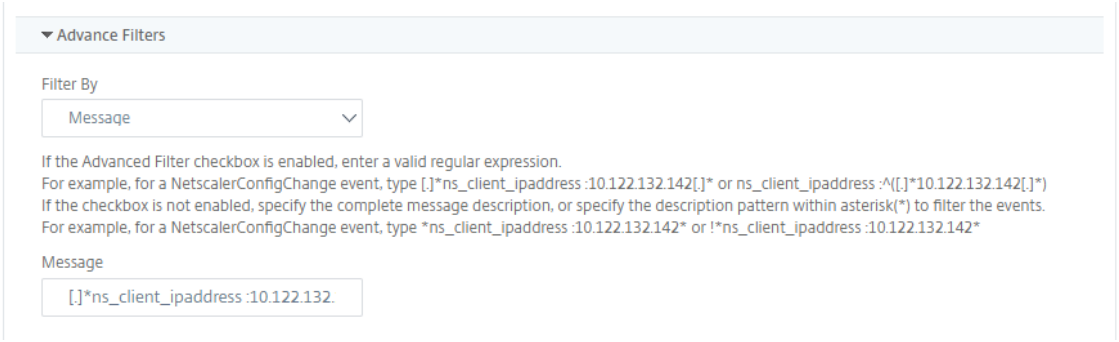
  Vous pouvez également filtrer la règle d'événement en fonction de l'état d'authentification de la commande et/ou de son état d'exécution. Par exemple, pour un `NetscalerConfigChange event`, tapez `[.]*bind system global policy_name[.]*`.

- **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 devez 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 déjà créée.

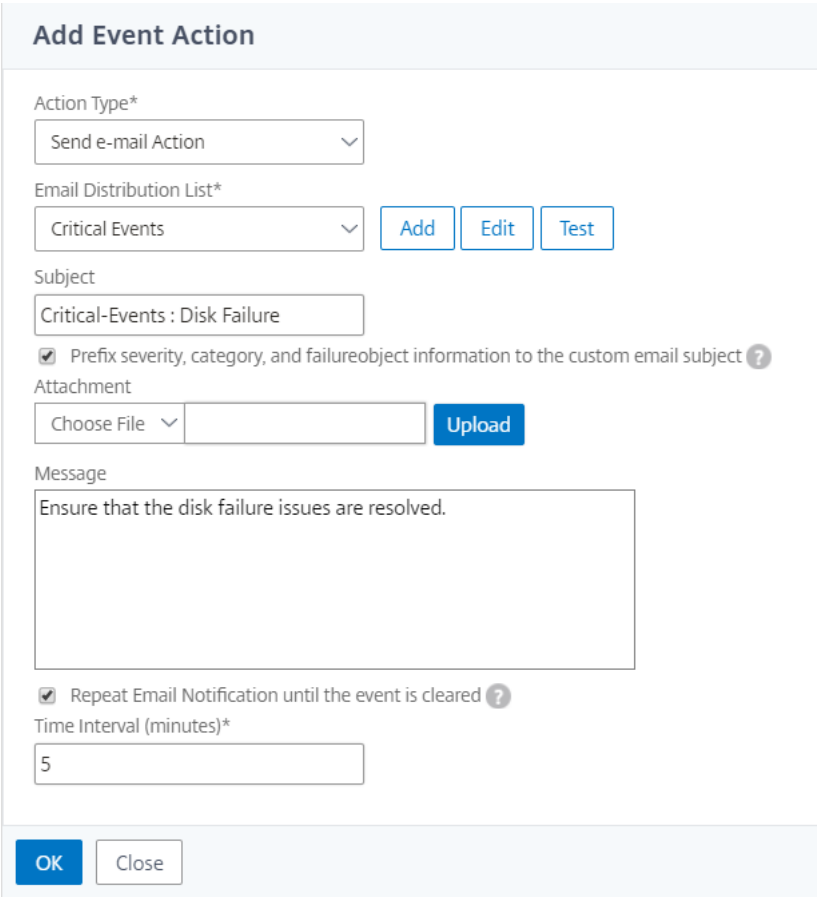
En raison du nombre élevé de serveurs virtuels configurés dans NetScaler ADM, vous pouvez recevoir un grand nombre d'e-mails chaque jour. Les e-mails ont une ligne d'objet par défaut qui fournit des informations sur la gravité de l'événement, la catégorie de l'événement et l'objet de la défaillance. Mais la ligne d'objet ne contient aucune information sur le nom du serveur virtuel d'où proviennent

ces événements. Vous avez désormais la possibilité d'inclure des informations supplémentaires telles que le nom de l'entité affectée, 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 d'événement **Exécuter une action de commande**, vous pouvez créer une commande ou un script qui peut être exécuté sur NetScaler 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 de défaillance affecte la façon dont un événement est traité et garantit que l'objet de défaillance reflète exactement le problème 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 NetScaler 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 NetScaler ADM. Par exemple, `/var`.
- Indiquez l'emplacement du fichier .sh dans NetScaler ADM à exécuter lorsque les critères de la 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

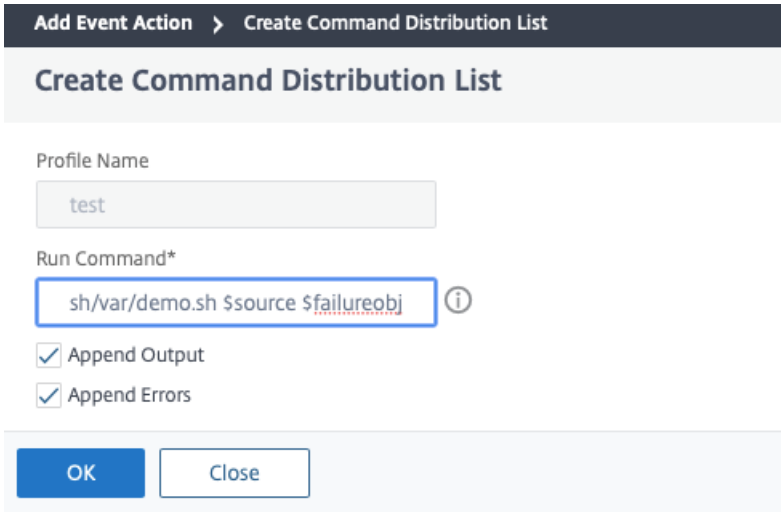
   b) Dans **Exécuter la commande**, spécifiez l'emplacement de l'agent NetScaler ADM où le script doit être exécuté. Par exemple : `/sh/var/demo.sh $source $failureobj` .

   c) Sélectionnez **Ajouter la sortie** et **Ajouter les erreurs**

   > **Remarque**
   >
   > Vous pouvez activer les options **Ajouter la sortie** et **Ajouter les 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 NetScaler ADM. Si vous n'activez pas ces options, NetScaler ADM ignore 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** .

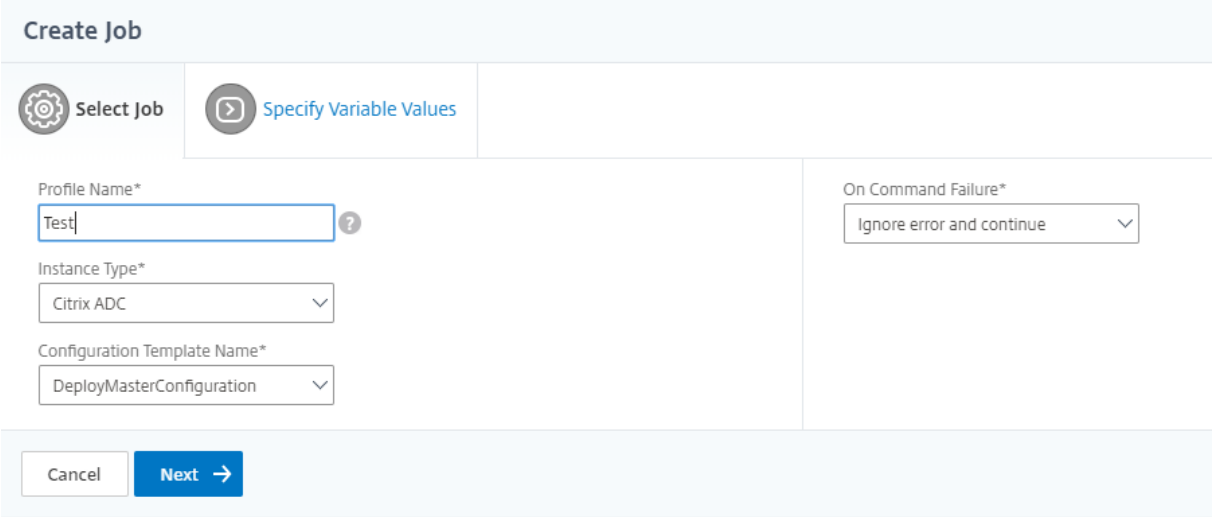


> **Remarque**
>
> Vous pouvez activer les options **Ajouter la sortie** et **Ajouter les erreurs** si vous souhaitez stocker la sortie et les erreurs générées (le cas échéant) lorsque vous exécutez un script de commande dans les fichiers journaux du serveur NetScaler ADM. Si vous n'activez pas ces options, NetScaler ADM ignore toutes les sorties et erreurs générées lors de l'exécution du script de commande.

Pour définir l'action de Execute travail

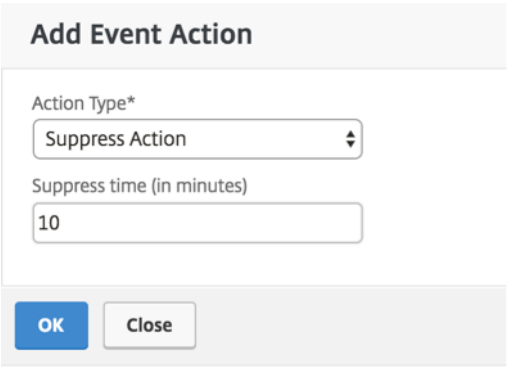
En créant un profil avec des tâches de configuration, une tâche est exécutée en tant que tâche intégrée ou en tant que tâche personnalisée pour les instances NetScaler et NetScaler SDX, pour les événements et les alarmes qui correspondent aux critères de filtre que vous avez spécifiés.

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 que vous souhaitez 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 les notifications Slack depuis NetScaler ADM

Configurez le canal Slack requis en fournissant le nom du profil et l'URL du webhook dans l'interface graphique de NetScaler ADM. Les notifications d'événement sont ensuite envoyées à ce canal. Vous pouvez configurer plusieurs canaux Slack pour recevoir ces notifications

1. Dans NetScaler ADM, accédez à**Infrastructure > 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**. Tapez le nom de la liste de profils à configurer sur NetScaler 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. Un exemple de webhook est le suivant : 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 depuis NetScaler ADM

Vous pouvez ajouter un profil PagerDuty en option dans NetScaler 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 NetScaler ADM, assurez-vous d'avoir effectué 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 NetScaler.
- **Licences** : liste des licences actuellement actives, sur le point d'expirer, etc.
- **Certificats SSL** : liste des certificats SSL ajoutés aux instances NetScaler.

Pour ajouter un profil PagerDuty dans ADM :

1. Connectez-vous à NetScaler ADM à l'aide des informations d'identification de l'administrateur.
2. Accédez à **Paramètres > 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.
- souhaitez recevoir des alertes téléphoniques concernant les événements NetScaler.

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 NetScaler, vous recevez 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 NetScaler ADM

Vous pouvez générer automatiquement des incidents ServiceNow pour les événements NetScaler ADM en sélectionnant le profil ServiceNow sur l'interface graphique de NetScaler ADM. Vous devez choisir le profil ServiceNow dans NetScaler ADM pour configurer une règle d'événement.

Avant de configurer une règle d'événement pour générer automatiquement des incidents ServiceNow, intégrez NetScaler 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 ServiceNow**.

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 NetScaler

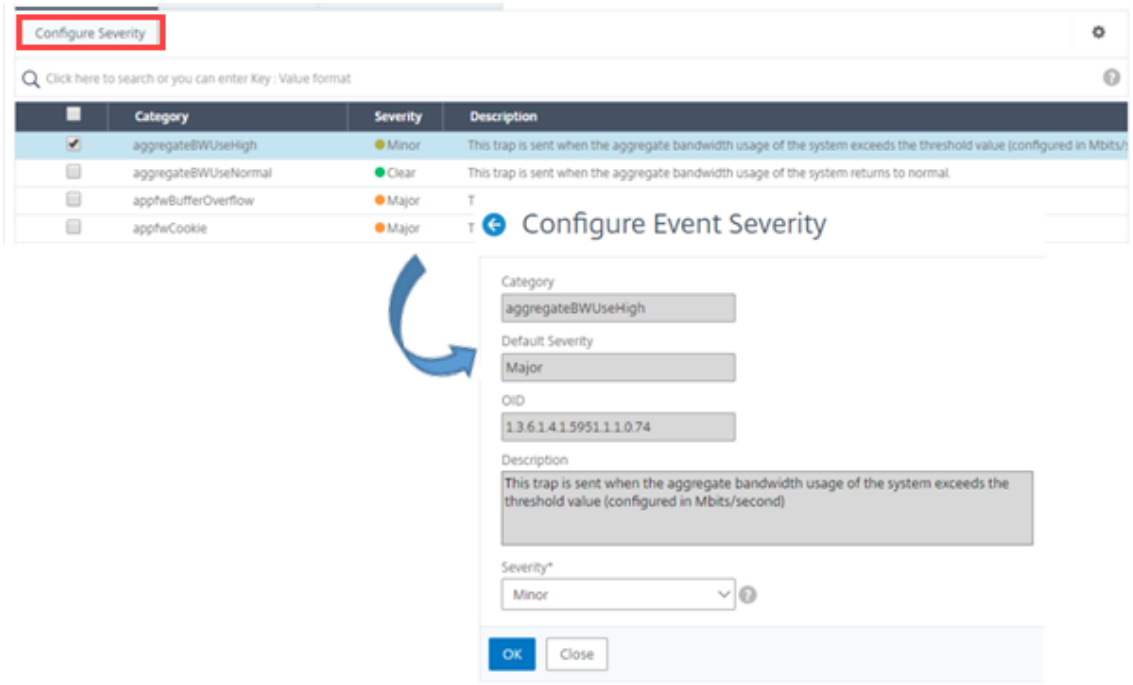
February 1, 2024

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 **Infrastructure > 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**.

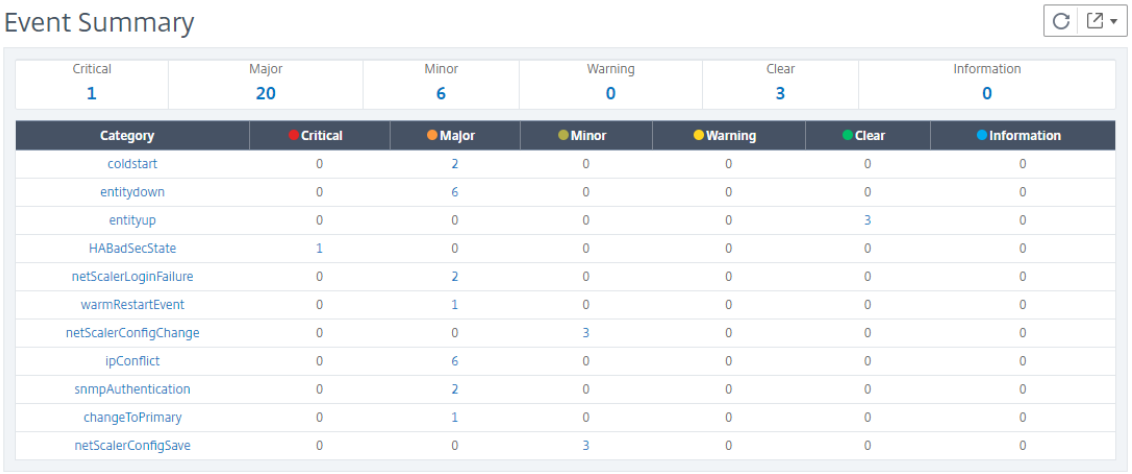


Afficher le résumé des événements

February 1, 2024

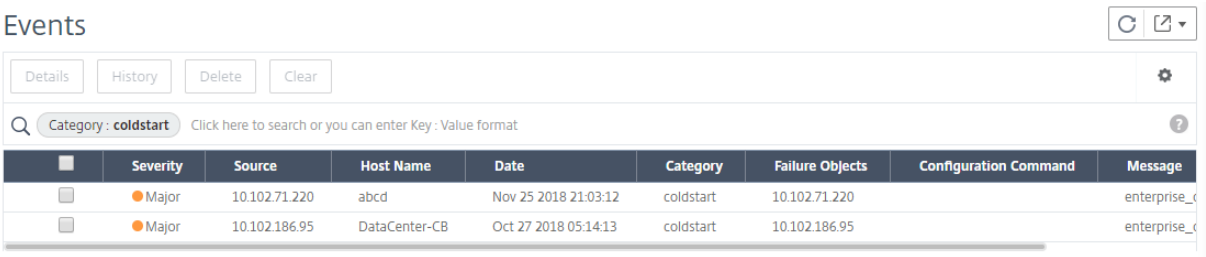
Vous pouvez désormais consulter une page récapitulative des événements pour surveiller les événements et les interruptions reçus sur votre serveur NetScaler Application Delivery Management (ADM). Accédez à **Infrastructure > Événements**. La page Récapitulatif des événements affiche les informations suivantes sous forme de tableau :

- **Récapitulatif de tous les événements reçus par NetScaler 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 produirait lorsqu'une instance de Citrix Application Delivery Controller (ADC) tombe en panne et cesse d'envoyer des informations au serveur NetScaler 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, une gravité est attribuée à chaque piège envoyé par les instances NetScaler à NetScaler ADM, mais en tant qu'administrateur réseau, vous pouvez spécifier sa gravité dans l'interface graphique de NetScaler 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 des informations supplémentaires sur l'événement, telles que l'adresse IP et le nom d'hôte de l'instance NetScaler, la date à laquelle le piège a été reçu, la catégorie, les objets défaillants, l'exécution de la commande de configuration et la notification du message.



Afficher les sévérité des événements et les détails des interruptions SNMP

February 1, 2024

Lorsque vous créez un événement et ses paramètres dans NetScaler Application Delivery Management (ADM), vous pouvez l'afficher immédiatement sur la page Résumé des événements. De même, vous pouvez consulter et surveiller l'état, le temps de disponibilité, les modèles et les versions de toutes les instances Citrix Application Delivery Controller (ADC) ajoutées à votre serveur NetScaler

ADM dans les moindres détails sur le tableau de bord de l'infrastructure.

Sur le tableau de bord de l'infrastructure, vous pouvez désormais masquer les valeurs non pertinentes afin de pouvoir visualiser et surveiller plus facilement des informations telles que la gravité des événements, leur état, leur durée de disponibilité, les modèles et la version des instances NetScaler dans les moindres détails.

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.

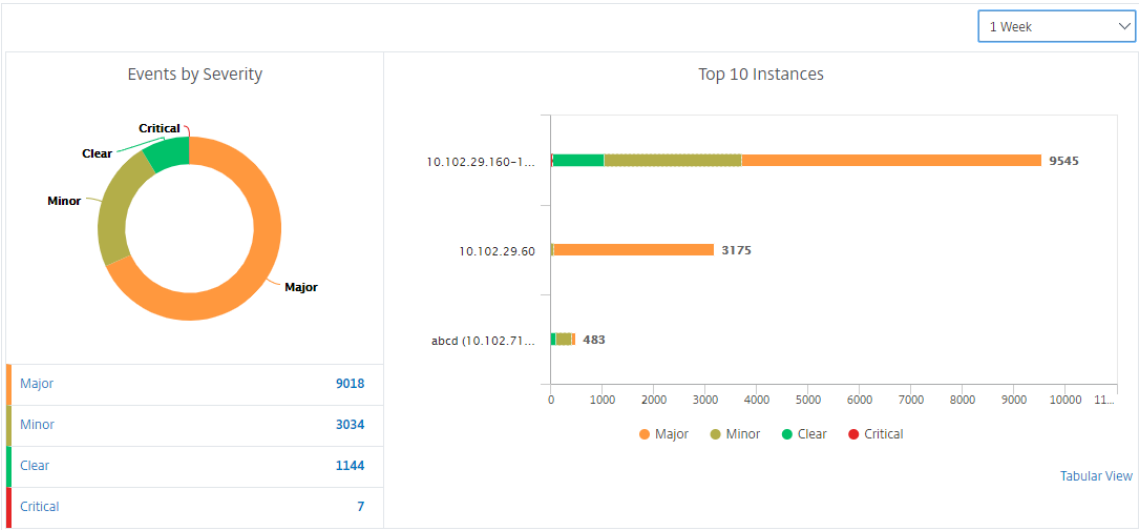
De même, vous pouvez consulter l'état de santé d'une instance NetScaler VPX sur le tableau de bord. Vous pouvez masquer le temps pendant lequel l'instance était en cours d'exécution et afficher uniquement les heures où elle était hors service. En cliquant sur le graphique, vous accédez à la page de cette 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 NetScaler ADM :

1. Connectez-vous à NetScaler ADM à l'aide de vos informations d'identification d'administrateur.
2. Accédez à **Infrastructure > Tableau de bord**.

   Ou

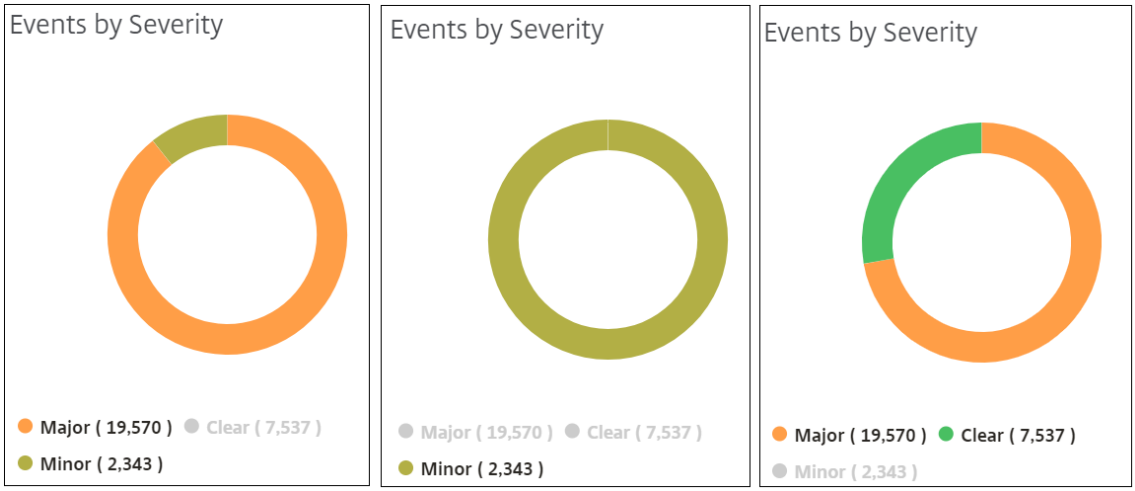
   Accédez à **Infrastructure > Événements > Rapports**.
3. Dans le menu situé dans le coin supérieur droit de la page, sélectionnez la durée pour laquelle vous souhaitez afficher les événements par gravité.



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 NetScaler
    - 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 consulter les détails des interruptions SNMP de NetScaler sur NetScaler ADM :

Vous pouvez désormais consulter les détails de chaque interruption SNMP reçue de ses instances NetScaler gérées sur le serveur NetScaler ADM sur la page Paramètres des événements. Accédez à **Infrastructure > 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 de NetScaler

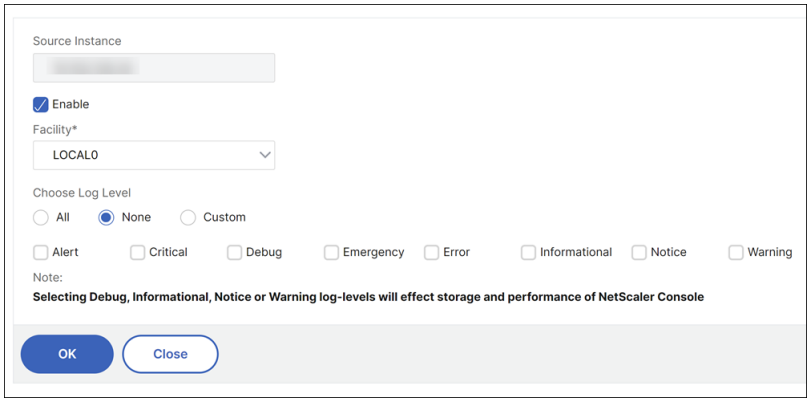
February 1, 2024

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 NetScaler. 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. Dans l'interface graphique d'ADM, accédez à **Infrastructure > Instances**.
2. Sélectionnez l'instance NetScaler à partir de laquelle vous souhaitez que les messages syslog soient collectés et affichés dans NetScaler 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**.

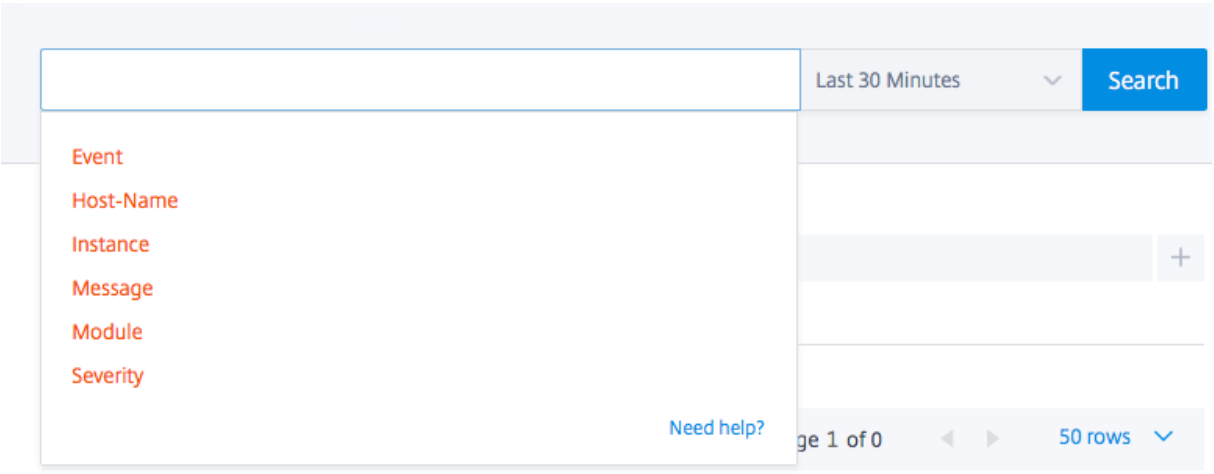


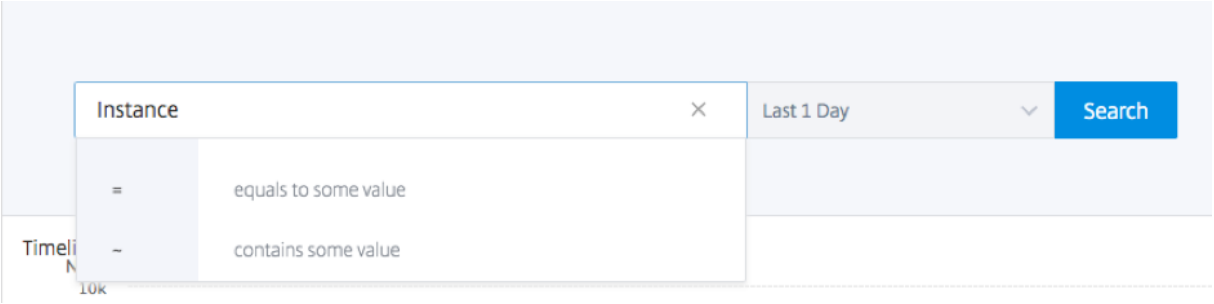
Ces étapes configurent toutes les commandes syslog dans l'instance NetScaler, et NetScaler ADM commence à recevoir les messages syslog.

Afficher et rechercher des messages syslog

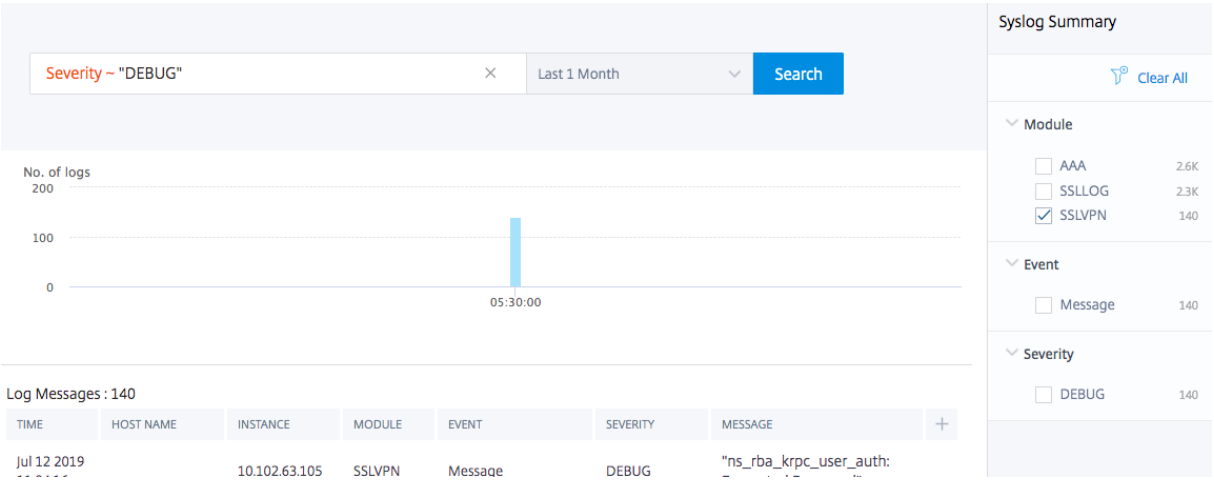
Vous pouvez consulter tous vos messages syslog générés sur vos instances NetScaler gérées. Les messages Syslog sont stockés dans la base de données de manière centralisée et sont disponibles sous **Infrastructure > Événements > Messages Syslog à des** fins d'audit. Vous pouvez combiner ces informations 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**.

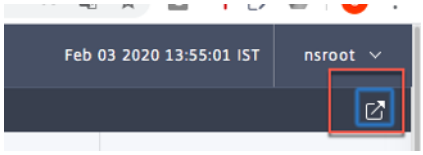


Exporter et planifier les messages syslog

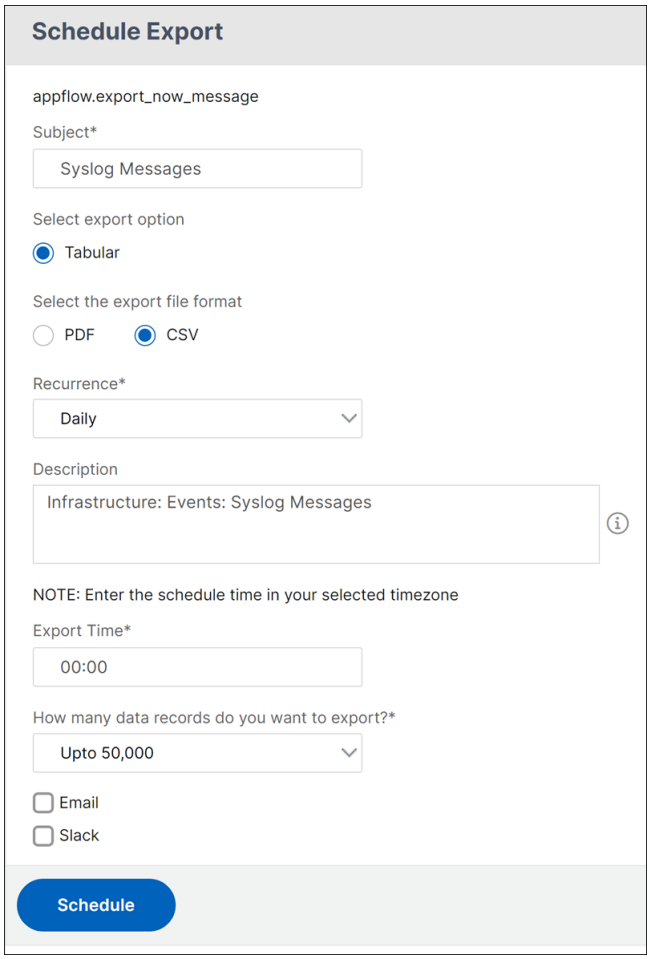
Vous pouvez afficher les messages syslog sans vous connecter à ADM, en planifiant une exportation de tous les messages syslog reçus sur le serveur. Vous pouvez exporter les messages syslog générés

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, NetScaler Application Delivery Management (ADM) reçoit tous les messages syslog qui lui sont envoyés par les instances 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 NetScaler ADM en configurant certains filtres. NetScaler ADM supprime tous les messages correspondant aux critères. Ces messages supprimés n'apparaissent pas sur l'interface graphique de NetScaler ADM et ne sont pas non plus stockés dans la base de données NetScaler ADM du client.

Vous pouvez supprimer certains messages Syslog enregistrés dans NetScaler 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 NetScaler particulière ou de plusieurs instances. Vous pouvez également fournir un modèle de texte permettant à NetScaler ADM de rechercher et de supprimer des messages. NetScaler ADM supprime tous les messages correspondant aux critères. Ces messages supprimés n'apparaissent pas sur l'interface graphique de NetScaler ADM et ne sont pas non plus stockés dans la base de données clients. 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

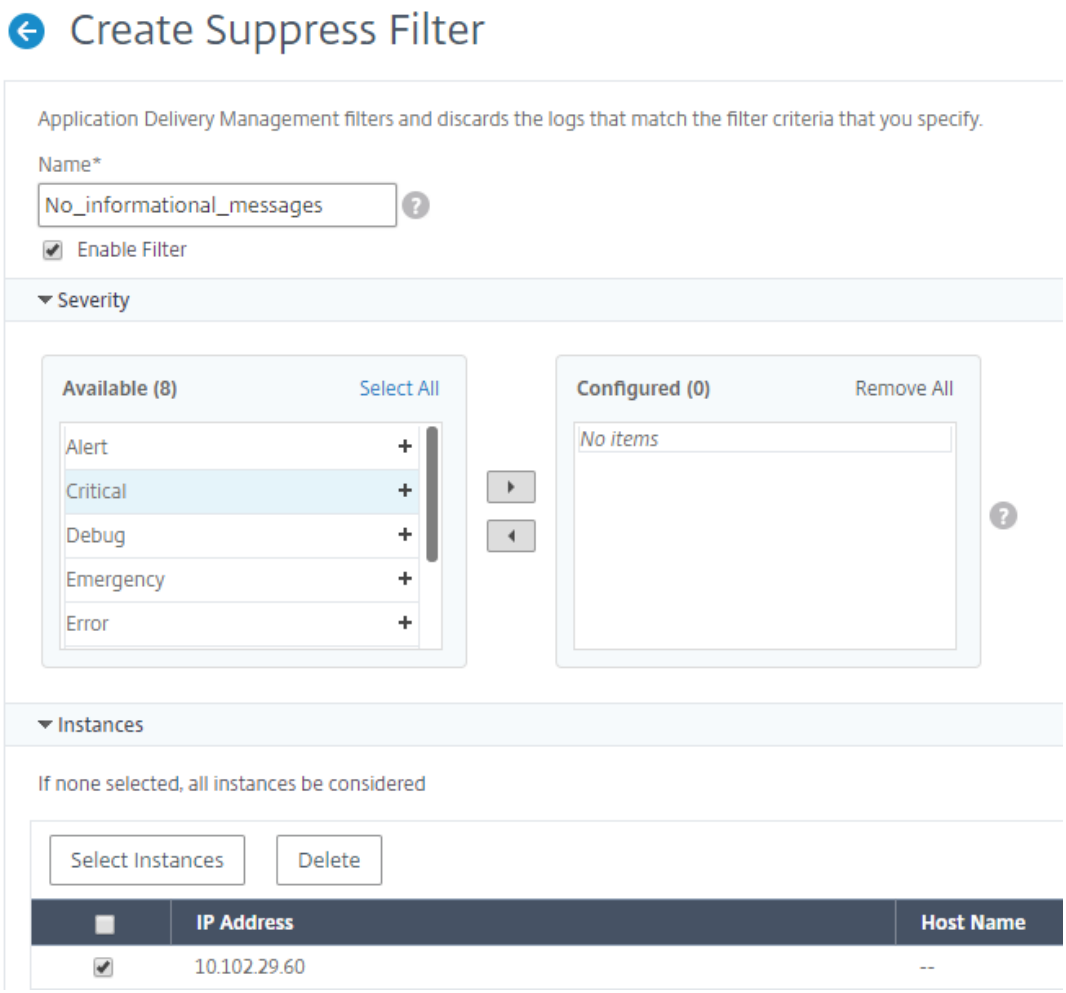
1. Dans NetScaler ADM, accédez à **Infrastructure > Événements > Messages Syslog** > **Supprimer le filtre**.
2. Sur la page **Créer un filtre de suppression**, mettez à jour les informations suivantes :
   a) **Nom** : entrez le nom du filtre.

   > **Remarque**
   >
   > Si différents utilisateurs ont un accès différent à plusieurs instances NetScaler, des

> filtres différents doivent être créés pour différentes instances, car les utilisateurs ne peuvent voir que les filtres dans lesquels ils ont accès à toutes les instances.

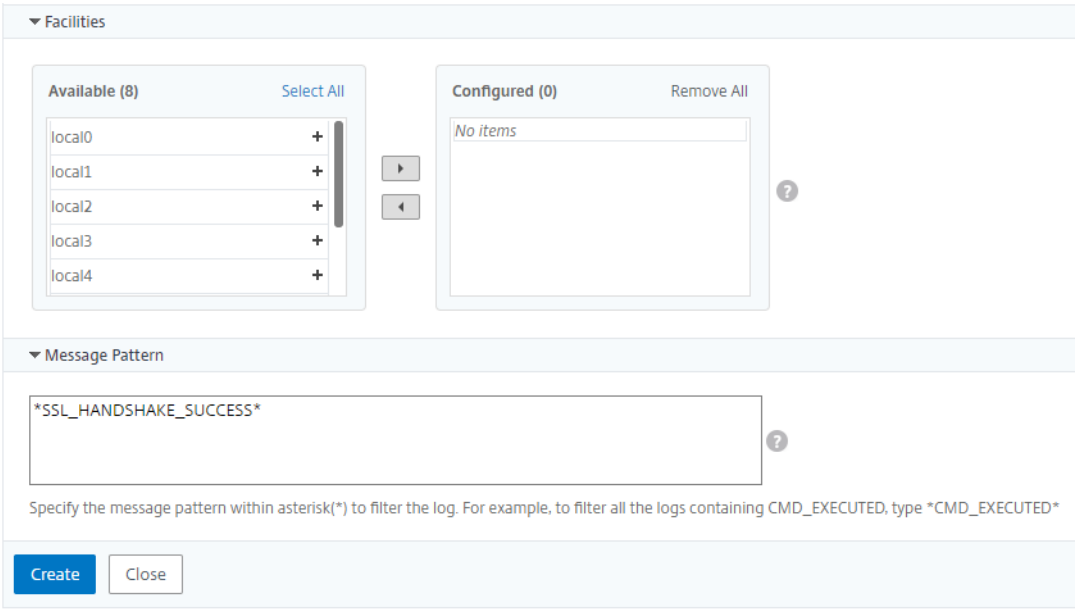
b) **Gravité** : sélectionnez et ajoutez les niveaux de journalisation pour lesquels vous devez supprimer les messages. Par exemple, si vous ne souhaitez pas voir les messages d'information qui arrivent, vous pouvez sélectionner Informationnel pour supprimer ces messages.

c) **Instances : sélectionnez les instances** NetScaler 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 NetScaler ADM, vous devez désactiver le filtre.

1. Accédez à **Infrastructure > 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

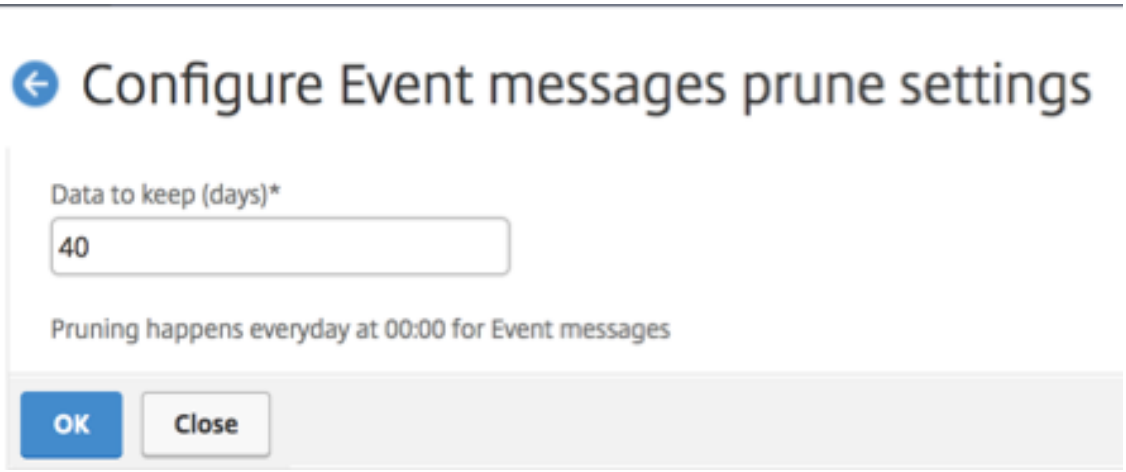
February 1, 2024

Les instances Citrix Application Delivery Controller (ADC) gérées par votre serveur NetScaler Application Delivery Management (ADM) envoient des données de messages d'événements en continu à stocker sur NetScaler ADM. Vous pouvez spécifier l'intervalle pendant lequel vous souhaitez que NetScaler ADM conserve les données de reporting 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).

> **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, pendant lequel vous souhaitez conserver les données sur le serveur NetScaler ADM et cliquez sur OK.**



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

NetScaler Application Delivery Management (ADM) vous permet de consulter les rapports des entités d'instance Citrix Application Delivery Controller (ADC) à tous les niveaux. Vous pouvez télécharger deux types de rapports dans NetScaler ADM > Fonctions réseau : 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 NetScaler.

Ce rapport vous permet d'avoir une vue d'ensemble du mappage entre les instances NetScaler, 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.

NetScaler IP Address	NetScaler HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
[illegible]	[illegible]		Load Balancing				
[illegible]	[illegible]		Load Balancing				
[illegible]	[illegible]		Load Balancing				
[illegible]	[illegible]		Load Balancing				
[illegible]	[illegible]		Load Balancing	lb11-lb#11.1.2.2:80			lb11-svcgrp#3.4.4.4-3.4.4.4:
[illegible]	[illegible]		Load Balancing	ADM-Test-LB3#10.1.1.3:80			
[illegible]	[illegible]		Load Balancing	334-lb#1.33.2.2:80			
[illegible]	[illegible]	[illegible]	Load Balancing				
[illegible]	[illegible]	[illegible]	Load Balancing				
[illegible]	[illegible]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-7bfbca74-07fb-45b6-b1a9-26ca3			33f97d16-0413-4e6e-9f3d-8
[illegible]	[illegible]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-cea2ec6b-4b0c-496b-8404-b5b6			33f97d16-0413-4e6e-9f3d-8
[illegible]	[illegible]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-fa454aa1-6cb3-4eb0-99e1-6703			33f97d16-0413-4e6e-9f3d-8
[illegible]	[illegible]		Load Balancing	kjbj-lb#1.2.3.4:80			kjbj-svcgrp
[illegible]	[illegible]	[illegible]	Load Balancing				
[illegible]	[illegible]		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 NetScaler 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 NetScaler.

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.

NetScaler 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 NetScaler ADM, accédez à **Infrastructure > 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 NetScaler ADM, accédez à **Infrastructure > 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 de NetScaler 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 du cache, l'équilibrage global de la charge des serveurs (GSLB), l'authentification et NetScaler Gateway dans NetScaler Application Delivery Management (ADM). Ce rapport vous permet d'avoir une vue d'ensemble du mappage entre les instances NetScaler, les partitions et les entités liées correspondantes (serveurs virtuels, groupes de services et services) présentes sur 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.

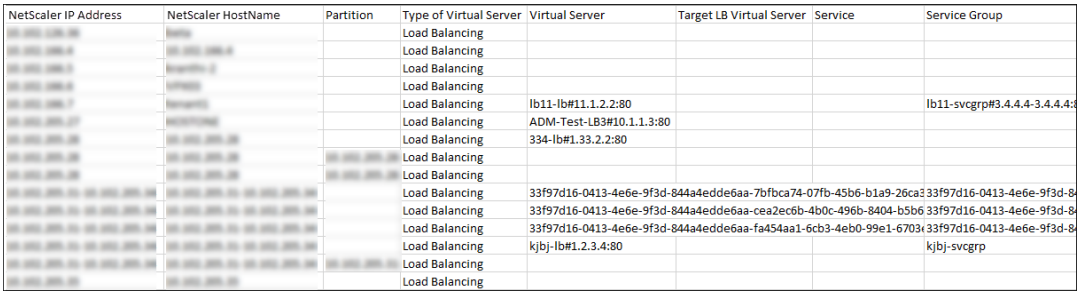
> **Remarque**
>
> - Pour les serveurs virtuels GSLB, le rapport des fonctions réseau affiche uniquement les serveurs virtuels GSLB et les services associés.
> - Pour les serveurs virtuels de commutation de contenu et de redirection de cache, le rapport affiche uniquement les liaisons vers les serveurs LB associés.
> - Les serveurs virtuels SSL ne sont pas répertoriés dans ce rapport car une liste distincte de serveurs virtuels SSL n'est pas conservée sur NetScaler 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 **Infrastructure > 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 IP Address	NetScaler HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing	lb11-lb#11.1.2.2:80			lb11-svcgrp#3.4.4.4-3.4.4.4:
[redacted]	[redacted]		Load Balancing	ADM-Test-LB3#10.1.1.3:80			
[redacted]	[redacted]		Load Balancing	334-lb#1.33.2.2:80			
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-7bfbca74-07fb-45b6-b1a9-26ca3			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-cea2ec6b-4b0c-496b-8404-b5b6			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-fa454aa1-6cb3-4eb0-99e1-6703			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	kjbj-lb#1.2.3.4:80			kjbj-svcgrp
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]		Load Balancing				

   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 NetScaler Application Delivery Management (NetScaler 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 (NetScaler) 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.

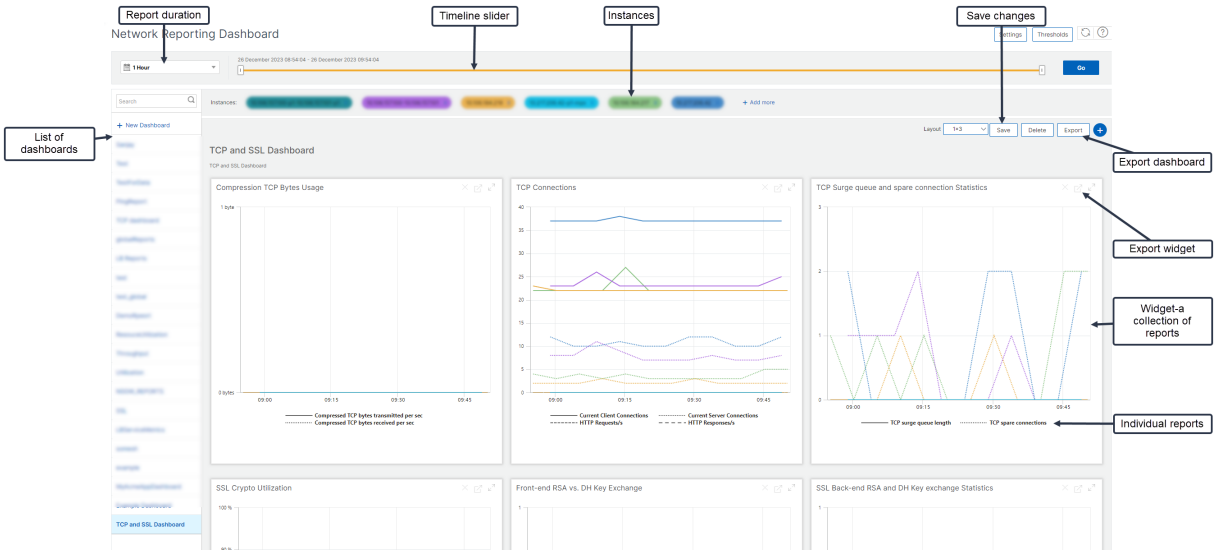
NetScaler ADM vous permet désormais de générer des rapports non seulement pour les instances au niveau mondial, mais également pour des entités telles que les serveurs virtuels et les interfaces réseau. La famille d'instances comprend des instances NetScaler. Les serveurs virtuels pour lesquels vous 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
- NetScaler Gateway

Le tableau de bord des rapports réseau de NetScaler 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 :



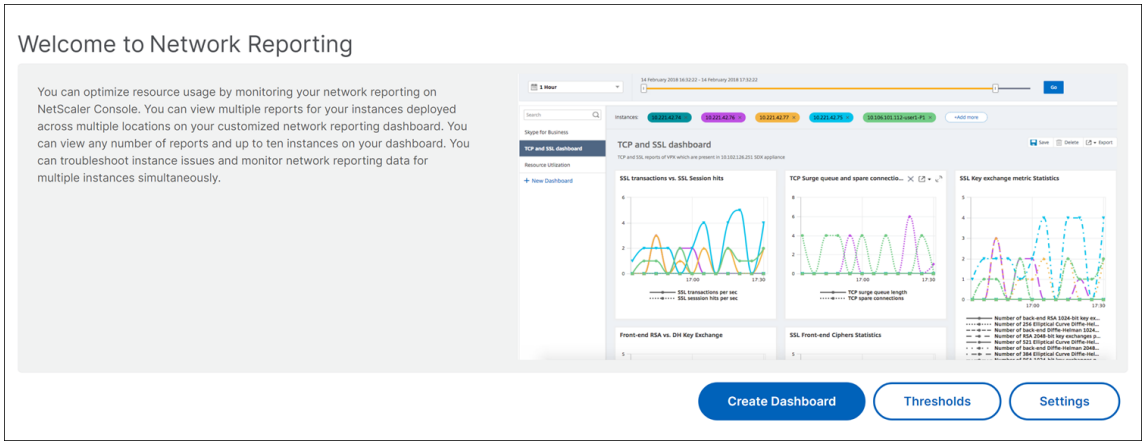
- Le panneau de gauche répertorie tous les tableaux de bord personnalisés créés dans NetScaler ADM. Vous pouvez cliquer sur l'un d'eux pour afficher les différents rapports que le tableau de bord est composé. Par exemple, un tableau de bord TCP et SSL contient divers rapports liés aux protocoles TCP 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 chronologique pour personnaliser la durée des rapports générés sur NetScaler 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, NetScaler ADM vous permet actuellement de consulter 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.

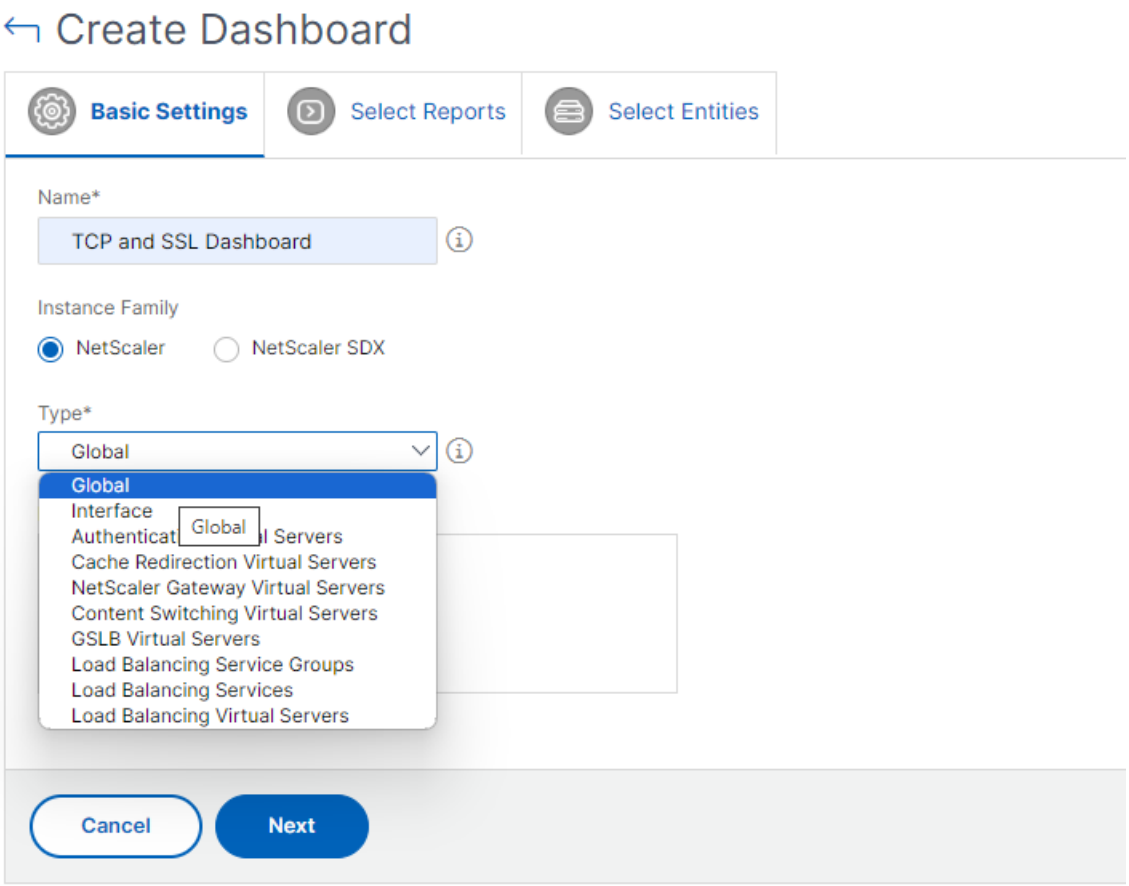
Pour afficher ou créer un tableau de bord :

1. Dans NetScaler ADM, accédez à **Infrastructure > Rapports**réseau.



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.

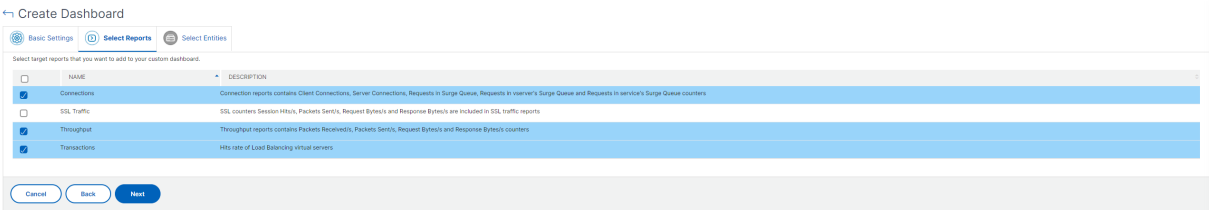
   b) **Famille d'instances**. Sélectionnez le type d'instance : NetScaler ou NetScaler SDX.

   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.

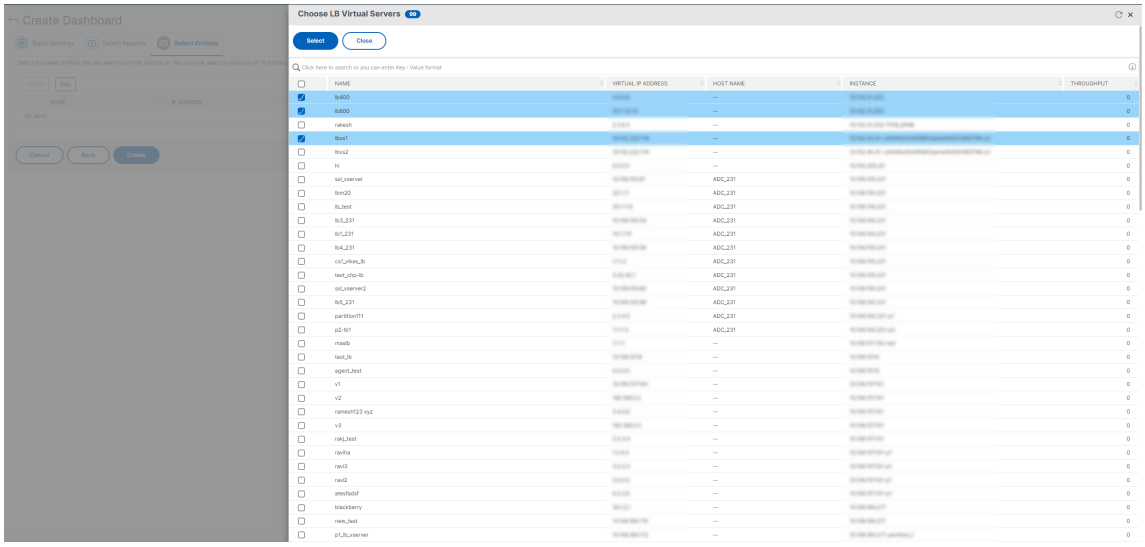
6. Dans l'onglet **Sélectionner des rapports**, sélectionnez les rapports requis. Dans cet exemple, vous pouvez sélectionner les transactions, les connexions et le débit. Cliquez sur **Suivant**.



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 NetScaler ADM si vous disposez d'autorisations en lecture seule. Vous devez disposer d'une autorisation de modification pour créer un fichier

> dans NetScaler ADM et pour pouvoir l'exporter.

Pour exporter des rapports de tableau de bord :

1. Accédez à **Infrastructure > Rapports sur le 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.

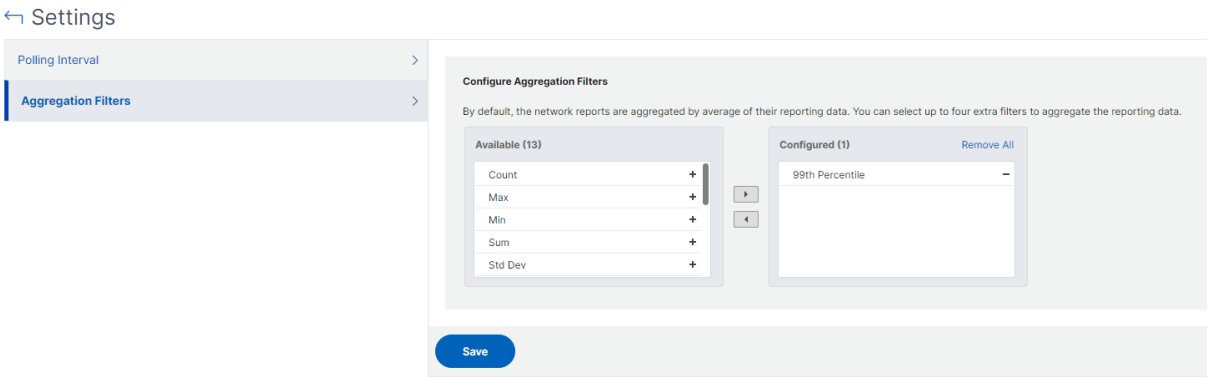
> **Remarque**
>
> Actuellement, cette option n'est disponible que lorsque vous planifiez l'exportation de rapports.

> 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 :

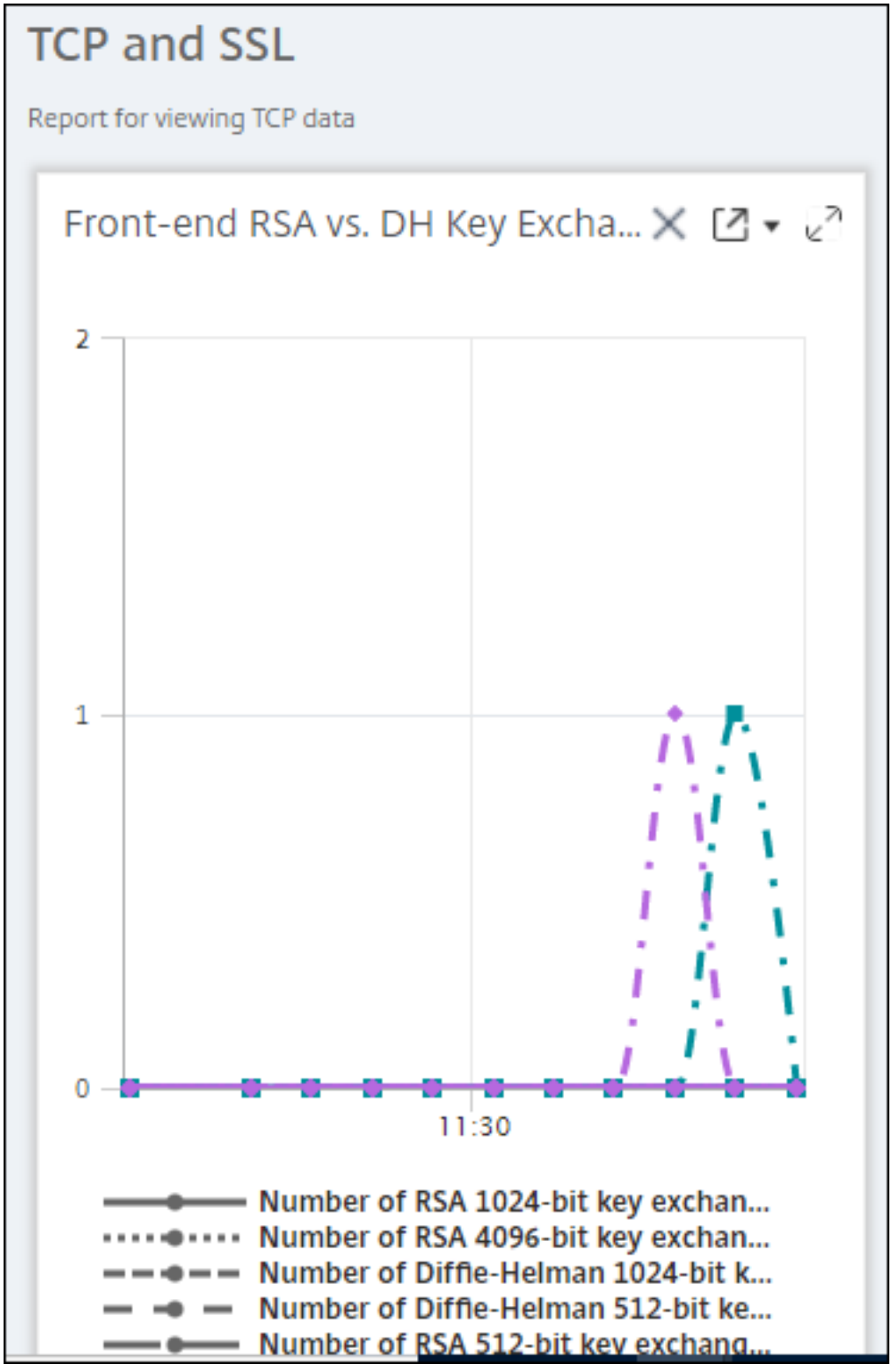
- Nombre
- Max
- Min
- Somme
- Dev Std
- Variance
- Mode
- Médiane
- 25e centile
- 75e centile

- 95e centile
- 99e centile
- Premier
- Dernier

Vous pouvez ajouter jusqu'à 4 options d'agrégation au tableau de bord. Une fois que vous avez ajouté les options d'agrégation, NetScaler ADM met environ 1 heure à générer des rapports pour les options d'agrégation sélectionnées.

Pour exporter des rapports de widget :

1. Accédez à **Infrastructure > Rapports sur le 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 gérer les seuils pour les rapports réseau sur NetScaler ADM

Pour surveiller l'état d'une instance NetScaler, vous pouvez définir des seuils sur les compteurs et recevoir des notifications lorsqu'un seuil est dépassé. Sur NetScaler 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. Ces événements peuvent être consultés en accédant à **Infrastructure > 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 NetScaler ADM, accédez à **Infrastructure > 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 NetScaler.
   - **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 **Infrastructure > Événements > Rapports**. Sur la page Rapports, vous pouvez cliquer sur le donut **Événements par gravité** pour afficher les événements par gravité.

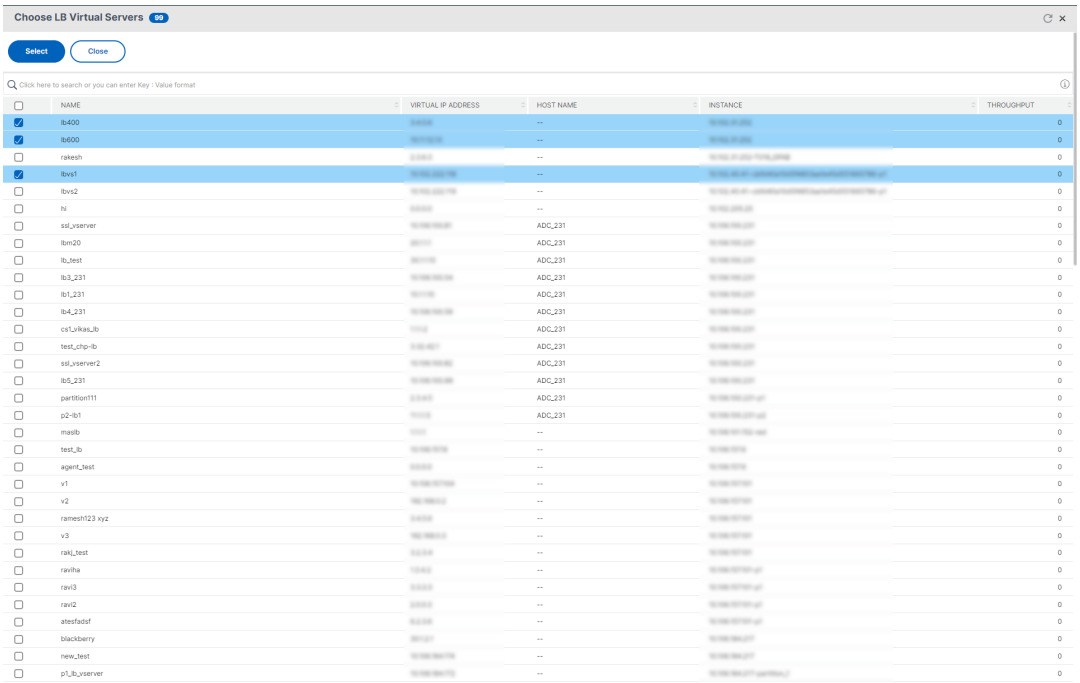
- **Valeur claire**. Entrez la valeur qui indique à quel moment effacer la valeur. Par exemple, vous pouvez supprimer le seuil des connexions client actuelles lorsque la valeur surveillée atteint 50 %. Dans ce cas, saisissez 50 comme valeur claire.
- **Gravité de l'événement** Sélectionnez le niveau de sécurité que vous souhaitez définir pour la valeur de seuil.

4. Vous pouvez choisir les instances et les entités à définir avec la valeur de seuil. Dans la section **Instances**, choisissez l'une des options suivantes :

   - **Toutes les instances**. Le seuil est défini pour toutes les instances.
   - **Instances spécifiques**. Le seuil est défini pour des instances spécifiques. Utilisez la flèche droite pour déplacer les instances de la liste **Disponible** vers la liste des instances **configurées** . Le seuil est défini pour les instances figurant dans la liste des instances **configurées** .
   - **Entités spécifiques**. Le seuil est défini pour des entités spécifiques.

     Cliquez sur **Ajouter** pour sélectionner les entités.

     Une fenêtre apparaît avec la liste des entités en fonction du type de rapport sélectionné dans le champ **Nom du rapport** . Dans cet exemple, la fenêtre **Choisir des serveurs virtuels LB** apparaît.

     Sélectionnez les entités pour lesquelles vous souhaitez définir un seuil. Cliquez sur **Sélectionner**. Les entités sélectionnées apparaissent dans la section **Instances** .

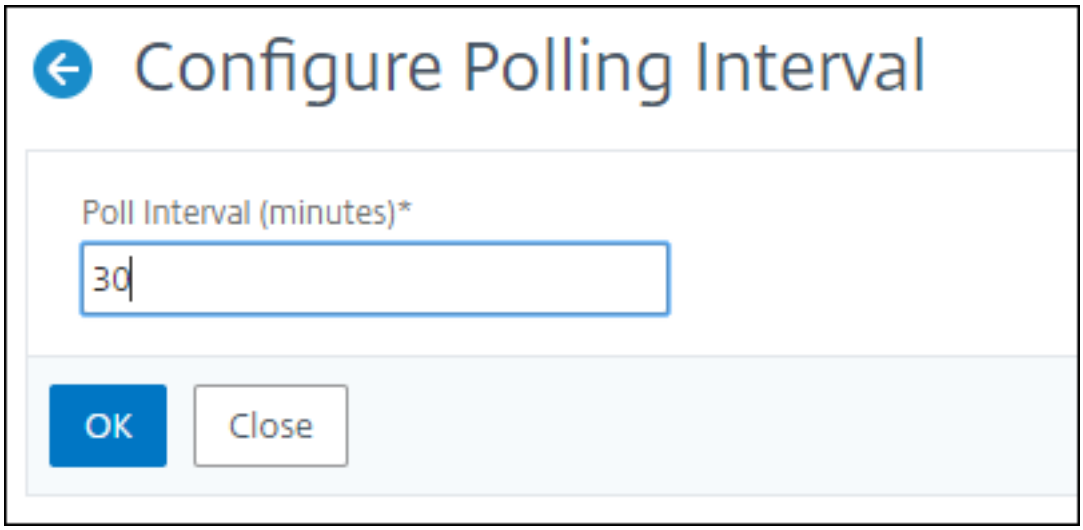
> **Remarque**
>
> L'option **Entités spécifiques** apparaît uniquement si vous sélectionnez des rapports basés sur vserver dans **Nom du rapport**. Par exemple, si vous sélectionnez **LB Service Statistics**

5. Vous pouvez également ajouter un **message d'événement**. Tapez un message que vous souhaitez afficher lorsque le seuil est atteint. NetScaler 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 **Infrastructure > Rapports réseau** et 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 reporting réseau dans NetScaler ADM. Ce paramètre limite la quantité de données de reporting réseau stockées dans la base de données du serveur NetScaler 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 doit pas dépasser 30 jours ni être inférieure à 1 jour.

Tâches de configuration

February 1, 2024

Le processus de gestion de la configuration de NetScaler Application Delivery Management (NetScaler ADM) garantit la réplication correcte des modifications de configuration, des mises à niveau du système et d'autres activités de maintenance sur plusieurs instances de Citrix Application Delivery Controller (ADC) du réseau.

NetScaler ADM vous permet de créer des tâches de configuration qui vous permettent d'effectuer facilement toutes ces activités 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 NetScaler 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 NetScaler 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 NetScaler SDX exécutant NetScaler version 11.0 et versions ultérieures. Pour effectuer une mise à niveau d'un seul bundle, vous utilisez une tâche intégrée dans NetScaler ADM. Vous pouvez également mettre à niveau une instance NetScaler en extrayant la configuration en cours ou une configuration enregistrée et en exécutant les commandes sur une autre instance NetScaler 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 soit entrer vos propres commandes CLI, soit utiliser le bouton d'enregistrement et de lecture pour obtenir des commandes à partir d'une session NetScaler. Lorsque vous exécutez la tâche, les modifications apportées au fichier ns.conf de l'instance sélectionnée sont enregistrées et copiées dans NetScaler 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 utiliser le modèle de configuration principal sur NetScaler 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 à la configuration entre les instances, répliquer les configurations sur plusieurs instances de votre réseau et enregistrer et exécuter des tâches de configuration à l'aide de l' interface graphique NetScaler Application Delivery Management (ADM) et la convertir en commandes CLI.

Vous pouvez utiliser la fonctionnalité Tâches de configuration de NetScaler ADM pour créer une tâche de configuration, envoyer des notifications par e-mail et consulter les journaux d'exécution des tâches créées.

Pour créer une tâche de configuration sur NetScaler ADM :

1. Accédez à **Infrastructure > Travaux de configuration**.

2. Cliquez sur **Créer une tâche**.
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 NetScaler à haute disponibilité, vous pouvez exécuter une tâche de configuration locale 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 chargez le fichier sur le serveur NetScaler 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.

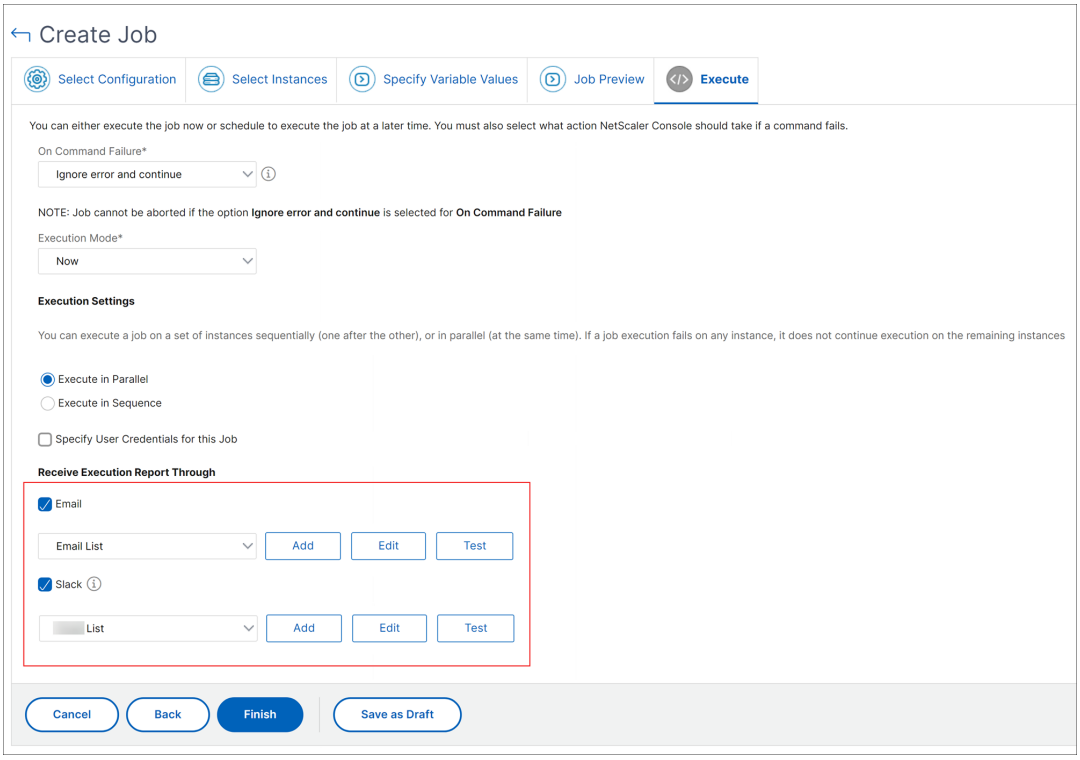
1. Accédez à **Infrastructure > Travaux de configuration**.
2. Sélectionnez le travail que vous souhaitez activer la notification par e-mail et Slack, puis cliquez sur **Modifier**.
3. Dans l'onglet **Exécuter**, accédez au volet **Recevoir le rapport d'exécution via** :

    - 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 **Infrastructure > 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.

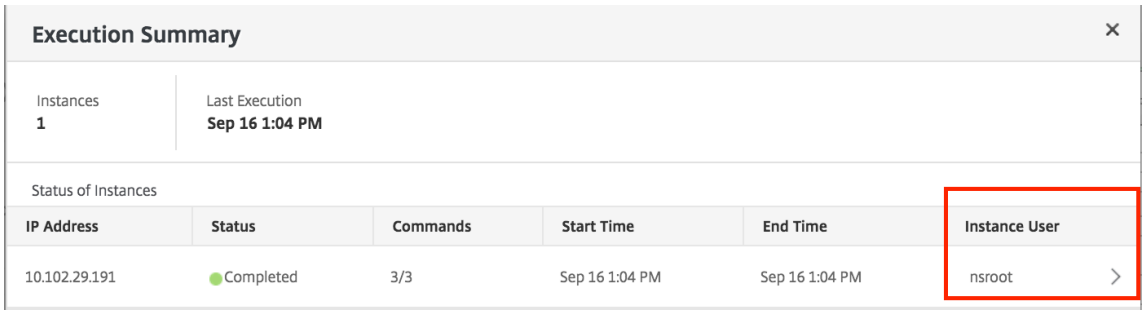
  Si vous souhaitez ajouter un profil Slack, cliquez sur **Ajouter** et spécifiez le **nom du profil**, le **nom du canal** et le **jeton** du canal Slack requis.

4. Cliquez sur **Terminer**.

Pour afficher les détails du récapitulatif d'exécution :

1. Accédez à **Infrastructure > 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



Afficher les rapports d'audit

February 1, 2024

(NetScaler ADM) vous permet de consulter et de télécharger le rapport d'audit de configuration diff dans la section audit de configuration. La section d'audit de configuration vous permet d'exporter les éléments suivants :

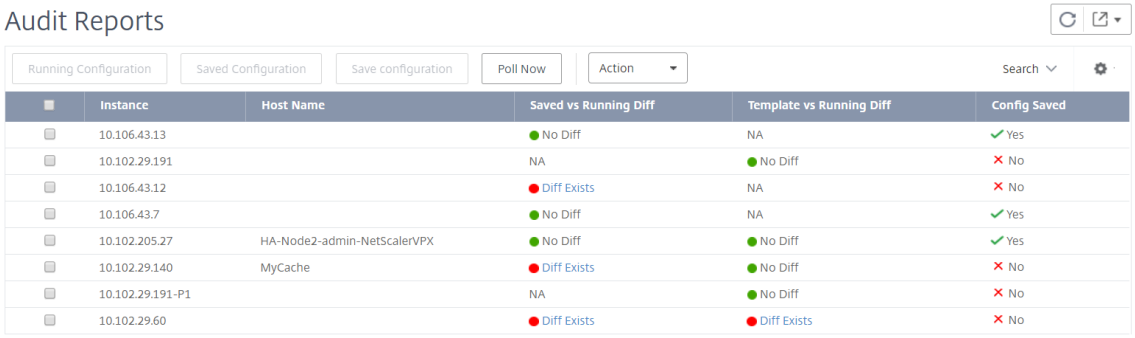
- Rapport récapitulatif sur toutes les instances par instance
- Rapport différentiel granulaire (diff) pour chaque paire instance-modèle

Les modèles **d'audit contenus dans Modèles** d'audit s'exécutent à l'heure planifiée par rapport aux 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 **NetScaler Config Drift**, la page des **rapports d'audit** qui s'affiche affiche une liste d'instances indiquant à la fois « Diff Exists » et No Diff. « Vous pouvez télécharger les rapports de comparaison affichés par NetScaler ADM.

NetScaler ADM propose également une option permettant de planifier l'exportation automatique d'un rapport de différences sous forme de pièce jointe à un e-mail. 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 NetScaler ADM, accédez à **Infrastructure > Configuration > 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.

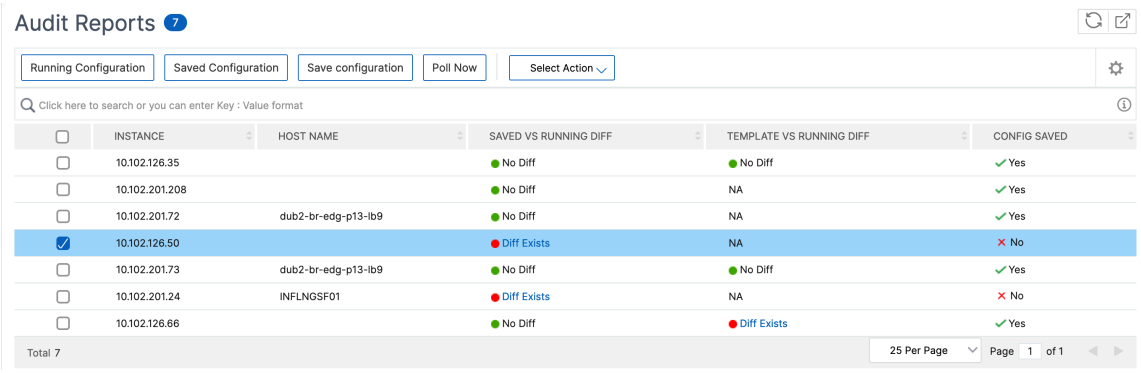


Dans l'image, vous pouvez voir que pour certains cas, un diff est présent uniquement dans **Sauvegardé vs Running Diff** et pour certains cas, un diff est présent uniquement dans **Template vs Running Diff**. Dans certains cas, des différences existent à la fois entre **Saved et Running Diff** et entre **Template et Running Diff .**

Sauvegardé vs Exécution Diff

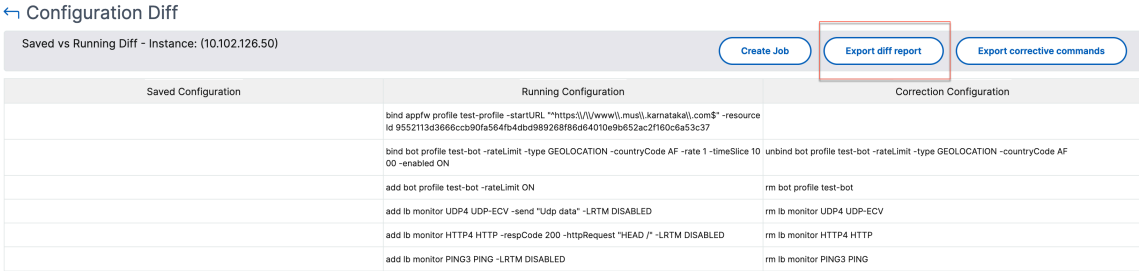
Vous pouvez consulter un rapport sur la différence entre la configuration enregistrée sur l'instance et la configuration en cours d'exécution sur l'instance.

1. Cliquez sur **Diff Exists** pour une instance sous **Saved Vs Running Diff .**



Vous pouvez consulter le rapport de configuration enregistrée par rapport à l'exécution de configuration diff pour cette instance.

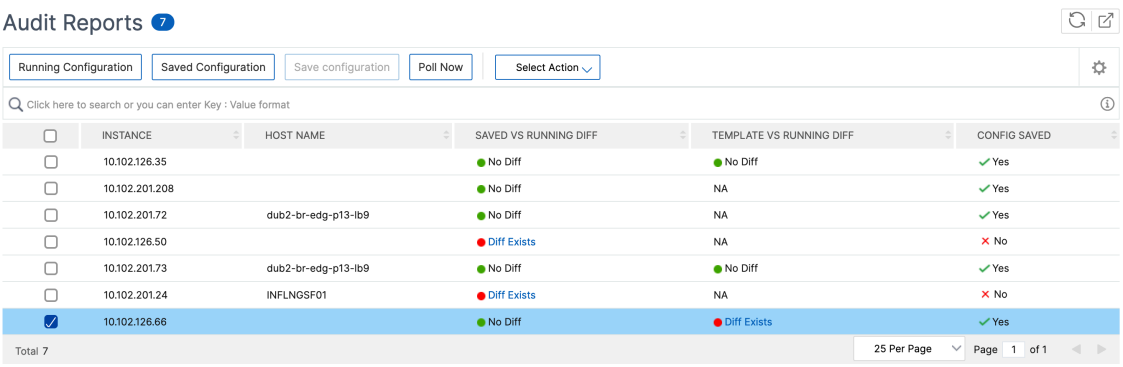
2. Cliquez sur **Exporter le rapport diff** pour télécharger un fichier .csv du rapport diff. Vous pouvez également cliquer sur **Exporter les commandes correctives** pour exporter les commandes dans un fichier .txt. Vous pouvez ensuite exécuter les commandes sur l'instance NetScaler ADM associée à partir de Configuration Jobs pour corriger la configuration de cette instance.



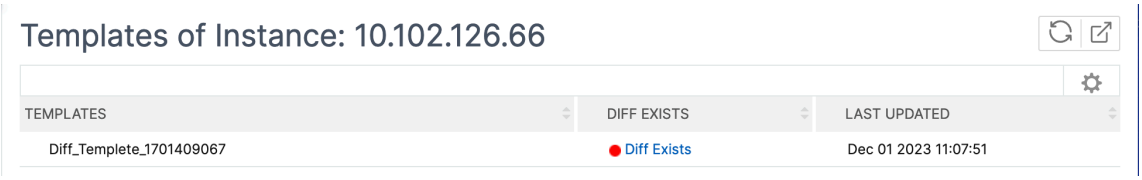
Modèle vs Courir Diff

Le **modèle vs Running Diff** inclut tous les modèles autres que **Sauvegardé vs Running Diff**, qui est le modèle par défaut. Vous pouvez voir la différence entre le modèle et la configuration en cours d'exécution.

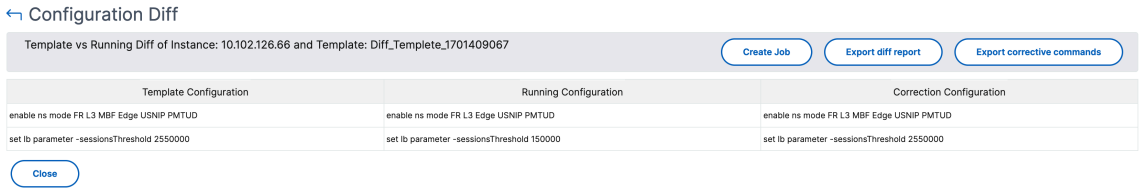
1. Cliquez sur **Diff Exists** pour l'une des instances situées sous **Template vs Running Diff .**



2. Les modèles révèlent les différences lorsque l'instance NetScaler ADM s'écarte de la configuration spécifiée par le modèle.



3. Cliquez à nouveau sur**Diff Exists**. L'image suivante montre la configuration recherchée par le modèle, les configurations en cours d'exécution et les configurations de correction ou les commandes à exécuter pour corriger la configuration. Si le champ **Configuration** en cours d'exécution est vide, cela signifie que les commandes ne sont pas configurées ou qu'elles sont supprimées.



4. 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 de l'instance.

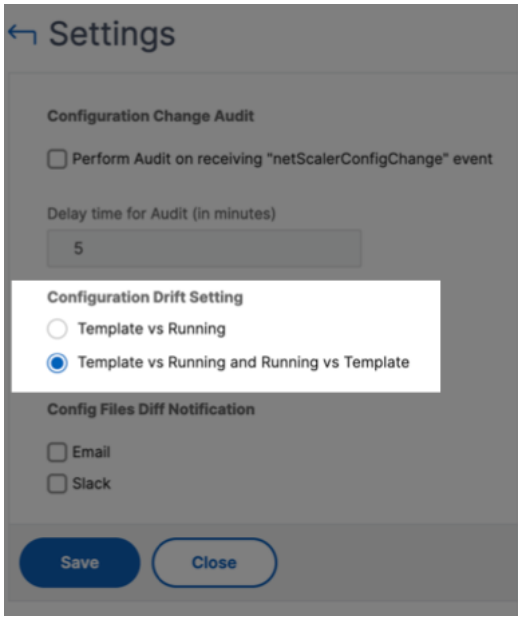
Template_vs_Running_Diff_of_Instance _10.102.126.66_and_Template _Diff_Templete_1701409067

Template Configuration	Running Configuration	Correction Configuration	
enable ns mode FR L3 MBF Edge USNIP PMTUD	enable ns mode FR L3 Edge USNIP PMTUD	enable ns mode FR L3 MBF Edge USNIP PMTUD	
set lb parameter -sessionsThreshold 2550000	set lb parameter -sessionsThreshold 150000	set lb parameter -sessionsThreshold 2550000	

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 Template vs. Le réglage Running Drift est sélectionné. Pour modifier le paramètre de dérive, sélectionnez **Paramètres** sur la page **Audit de configuration** .



Afficher les rapports d'audit de l'état des fichiers

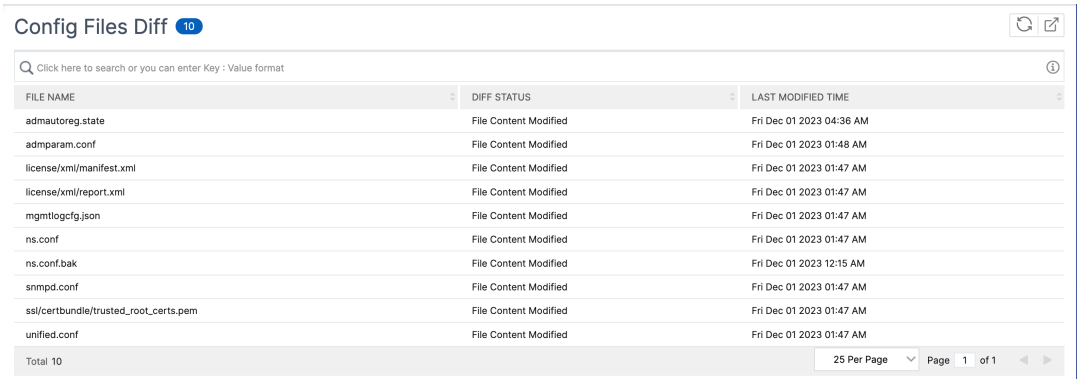
Utilisez le graphique **d'état des fichiers NetScaler** pour vérifier si des fichiers sont ajoutés, modifiés ou supprimés du `nsconfig`dossier. Par exemple, si le fichier de licence est mis à jour sur une instance NetScaler, vous pouvez vérifier quand ce fichier a été mis à jour pour la dernière fois et prendre les mesures nécessaires.

1. Accédez à **Infrastructure > Configuration > Audit de configuration**.
2. Sur la page **Audit de configuration** , cliquez sur le graphique d'état du **fichier de configuration NetScaler**.

   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 été modifiés dans le `nsconfig`dossier d'une instance depuis la **dernière heure interrogée** . 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. Cet état apparaît lorsque NetScaler ADM n'interroge pas l'instance. Par exemple, lorsqu'une instance est ajoutée récemment ou que son état est inactif, l'interrogation de l'instance n'a pas lieu.

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 NetScaler gérées, résoudre les erreurs de configuration et récupérer les configurations non enregistrées après un arrêt soudain du système.

Vous pouvez créer des modèles d'audit avec des configurations spécifiques pour auditer certaines instances. NetScaler ADM compare ces instances avec le modèle d'audit et signale toute incompatibilité dans la configuration. Le rapport sur les différences de configuration vous permet de dépanner 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 NetScaler 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.

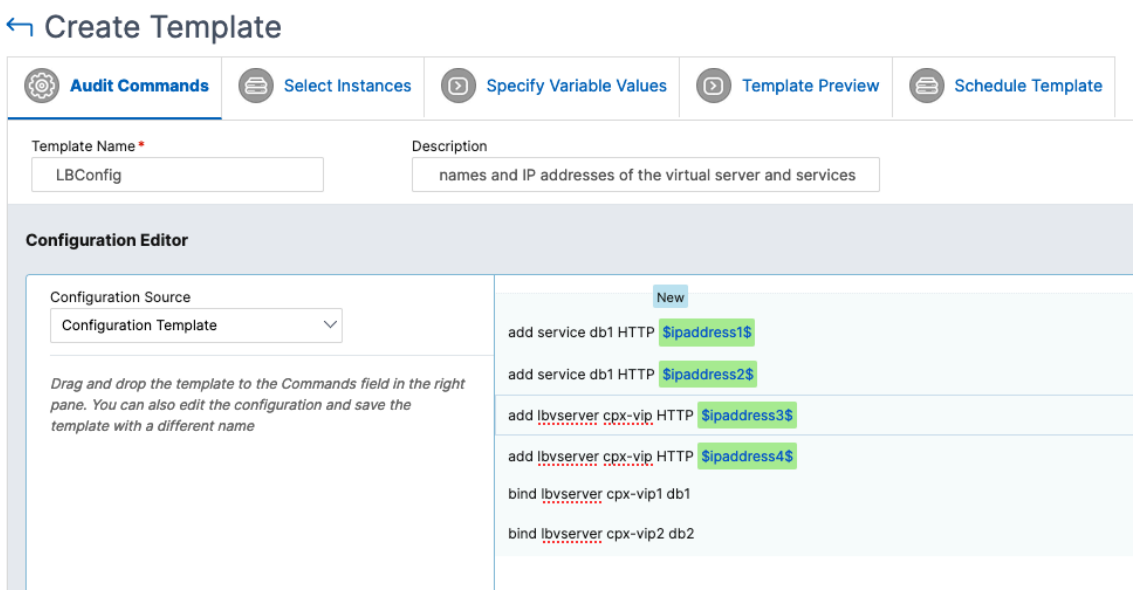
Vous avez également la possibilité d'envoyer le rapport de différences généré par NetScaler ADM aux adresses e-mail spécifiées que vous pouvez configurer. Avec cette option, les utilisateurs peuvent

recevoir le rapport sous forme de pièce jointe à un e-mail ou de notification Slack. Ils n'ont pas besoin de se connecter à NetScaler ADM pour exporter les rapports manuellement.

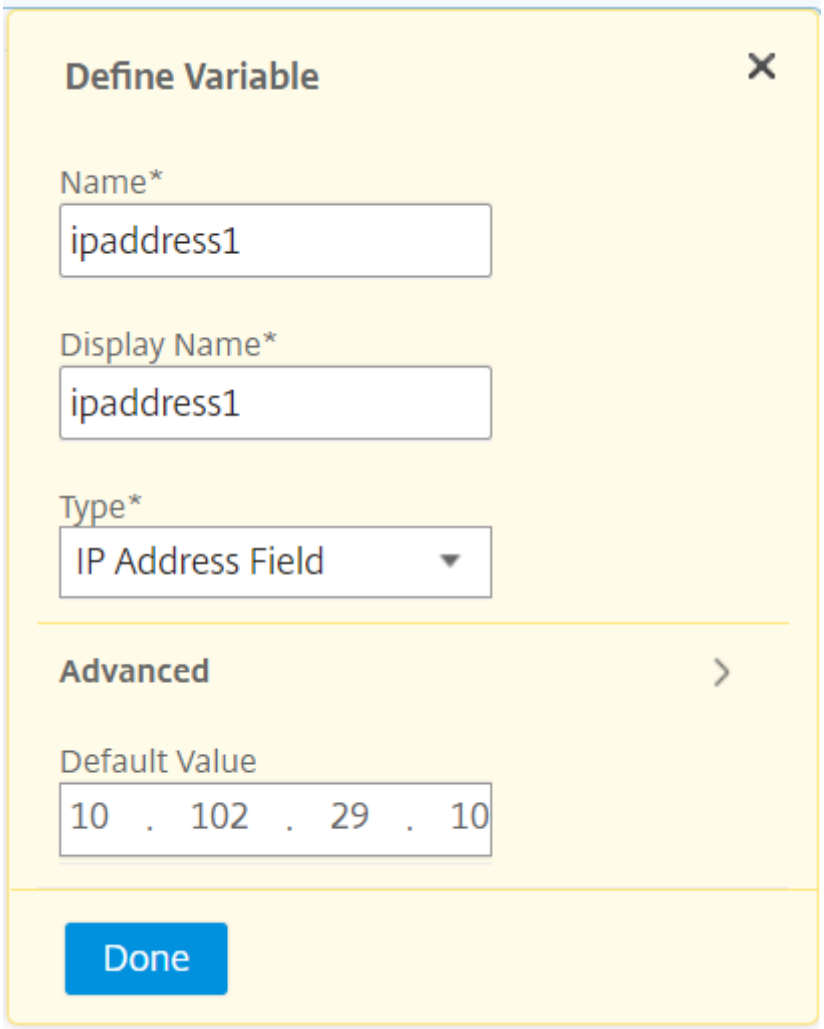
> **Remarque :**
>
> L'option **Renommer** est désactivée pour les modèles de configuration par défaut. Vous pouvez toutefois renommer les modèles de configuration personnalisés.

Pour créer des modèles d'audit :

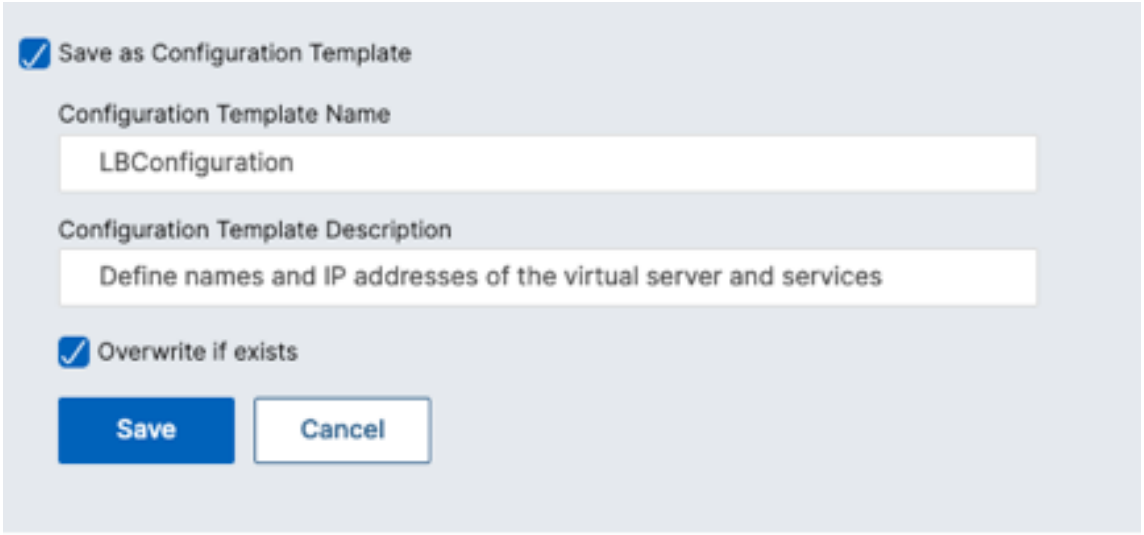
1. Accédez à **Infrastructure > Configuration > Audit de configuration > Modèles** d'audit , puis cliquez sur **Ajouter** .
2. Sur la page **Créer** un modèle et dans l'onglet **Commandes d'audit** , spécifiez le nom du modèle et sa description.
3. Sur la page **Éditeur de configuration**, saisissez 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 « $ ».



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.

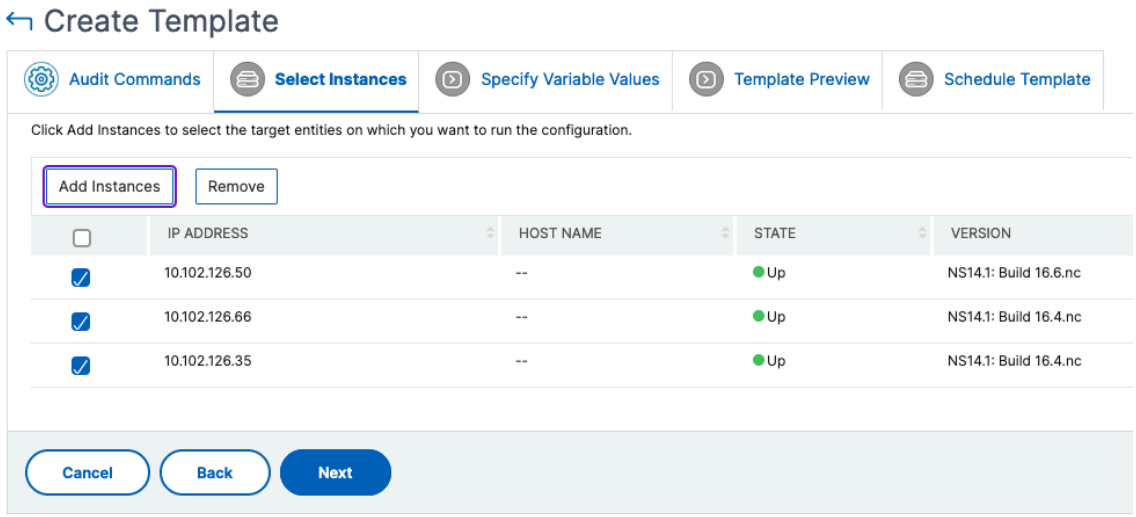


Vous pouvez également enregistrer les commandes en tant que modèle de configuration.



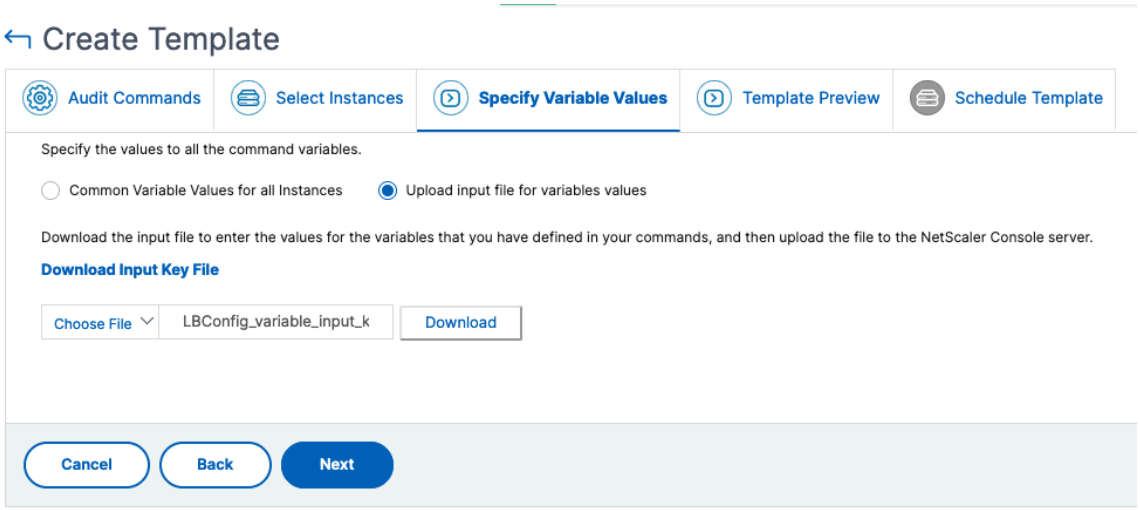
5. Cliquez sur **Enregistrer**, puis sur **Suivant**.

6. Dans l'onglet **Sélectionner les instances**, sélectionnez les instances sur lesquelles vous souhaitez exécuter l'audit de configuration et cliquez sur **Suivant**.

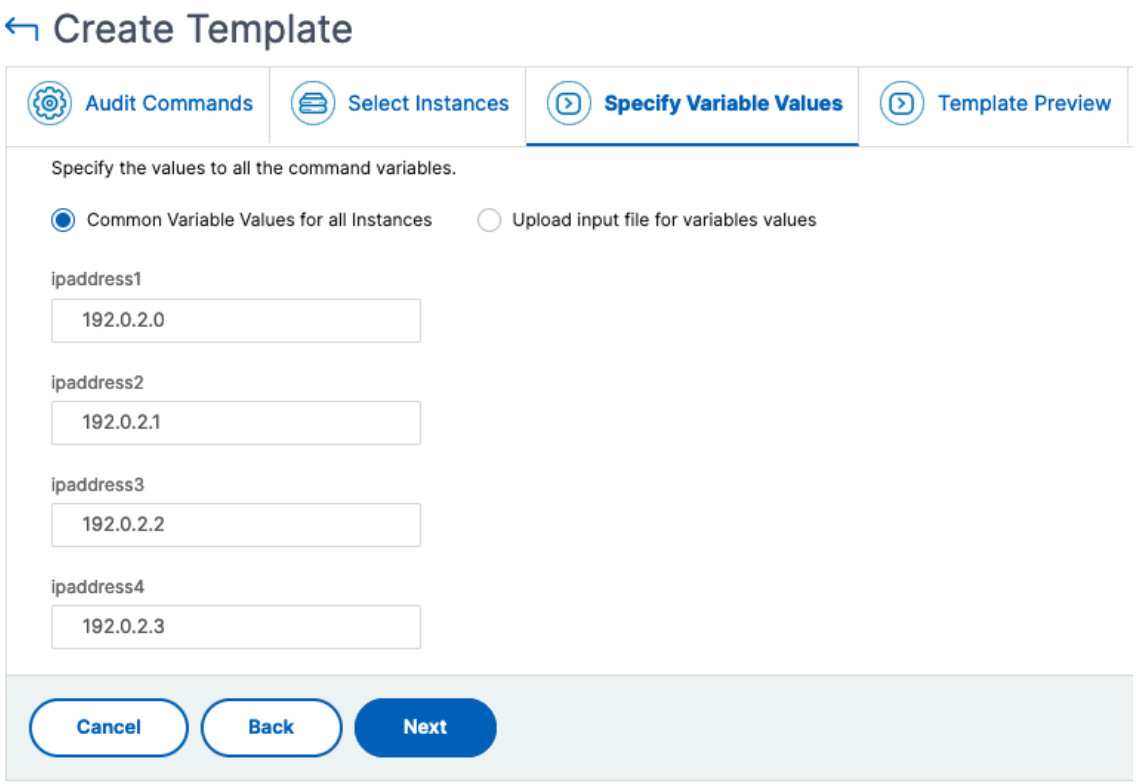


7. Dans l'onglet **Spécifier les valeurs variables**, vous disposez de deux options :

   a) Téléchargez le fichier d'entrée pour saisir les valeurs des variables que vous avez définies dans vos commandes. Après avoir saisi les variables, téléchargez le fichier sur le serveur NetScaler ADM.

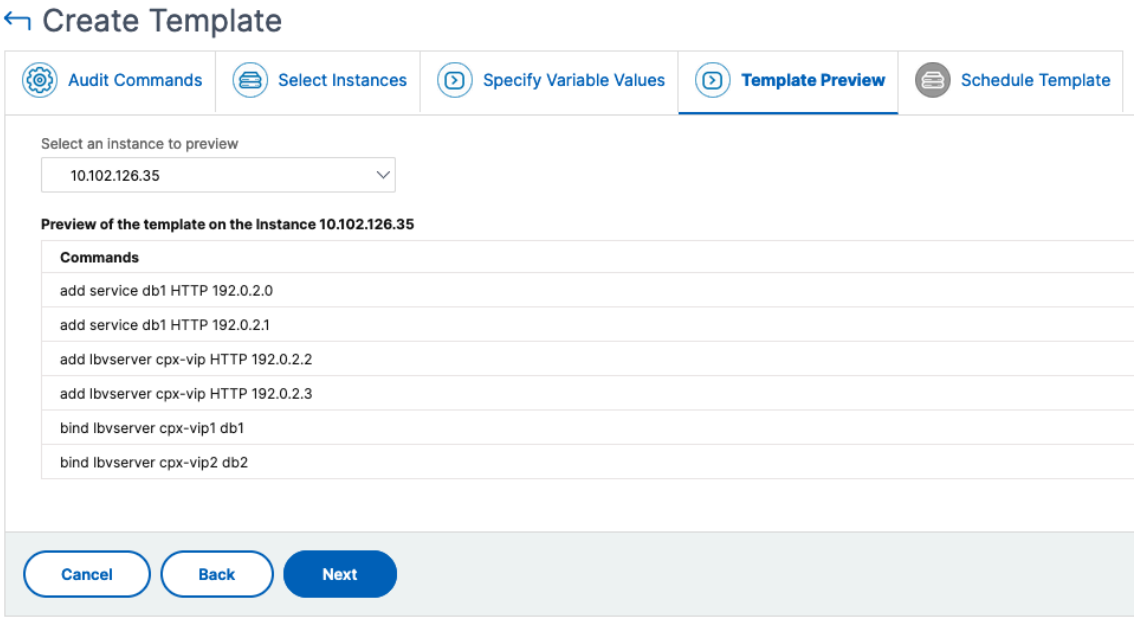


   a) Entrez des valeurs communes pour les variables que vous avez définies pour toutes les instances.



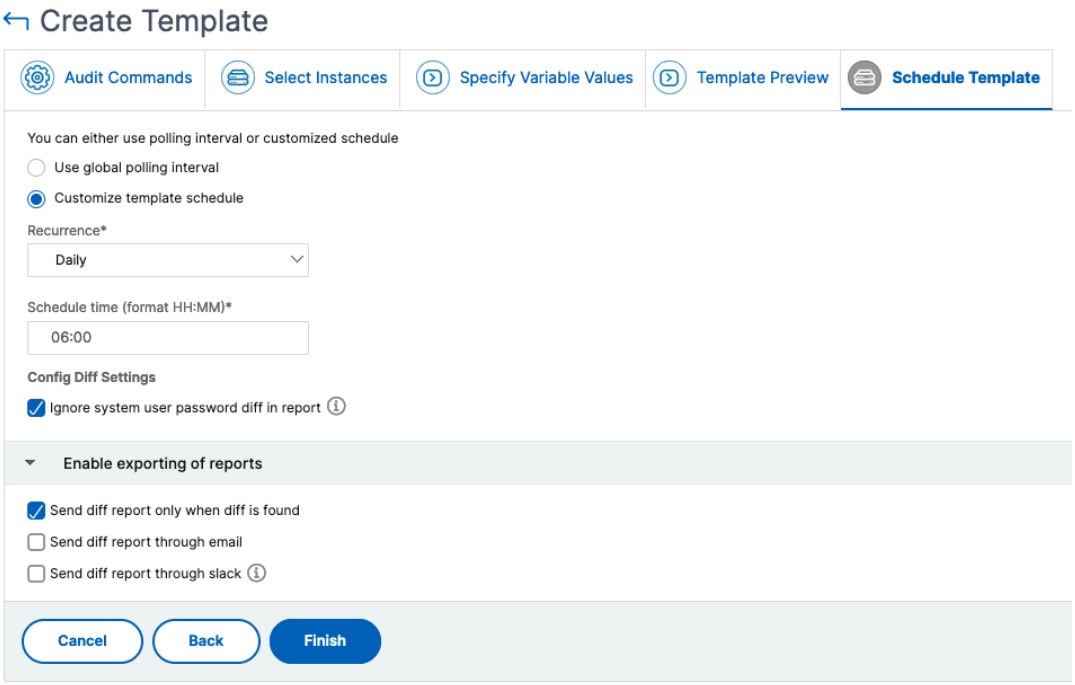
> **Remarque :**
>
> Si vous souhaitez auditer chaque instance avec des valeurs différentes, vous devez créer des variables distinctes dans le fichier d'entrée pour chaque instance.

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 NetScaler ADM.
    - **Personnaliser la planification du modèle**. Utilisez cette option pour configurer l'heure et la fréquence auxquelles les modèles doivent être exécutés.
        - Spécifiez la fréquence et le calendrier d'exécution des modèles d'audit.
    - **Activez l'exportation des rapports**. Utilisez cette option pour :
        - **Envoyer un rapport de différences, seul le diff est trouvé**
        - **Envoyer un rapport de différence par e-mail**. Configurez le profil de messagerie auquel le rapport diff doit être envoyé en tant que pièce jointe.
        - **Envoyez un rapport de différence via Slack**. Configurez la chaîne Slack à laquelle le rapport de différences doit être envoyé sous forme de notification.



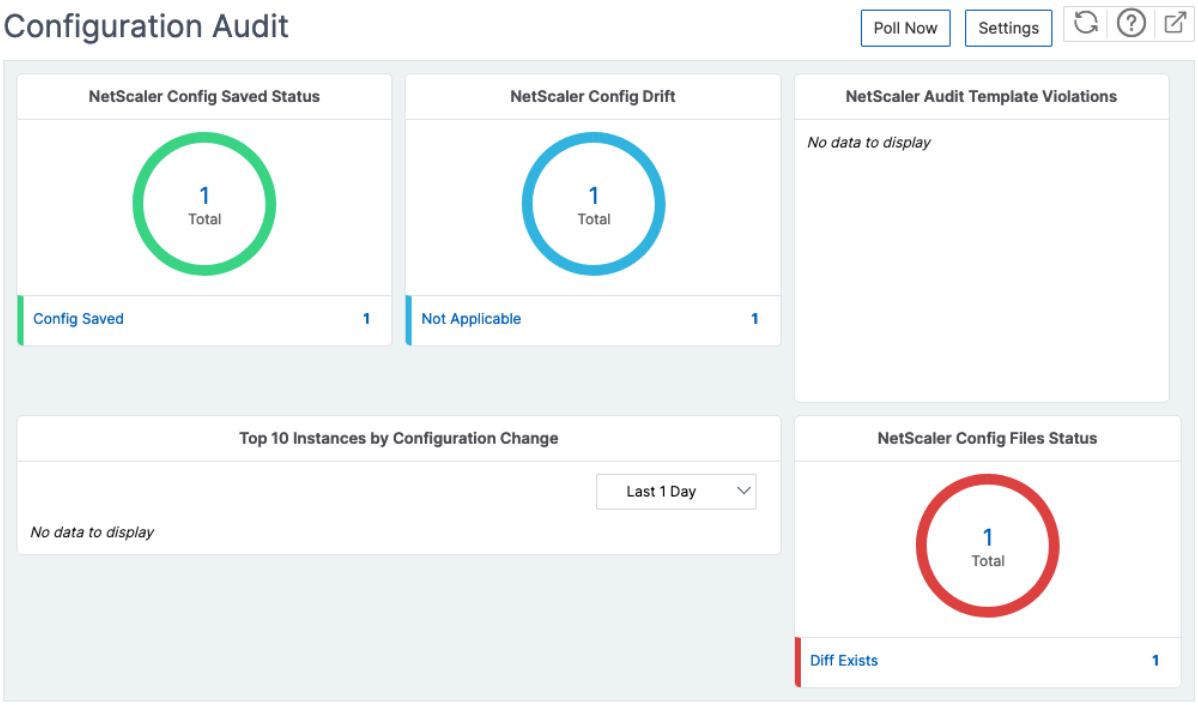
11. Cliquez sur **Terminer**.

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 modifications de configuration

Vous pouvez également utiliser le tableau de bord de l'**audit de configuration** pour afficher des informations détaillées sur les modifications de configuration, telles que :

- Les 10 premières instances par changement de configuration
- Nombre de configurations enregistrées et non enregistrées
- Le fichier ajouté, supprimé ou modifié dans le `nsconfig` dossier

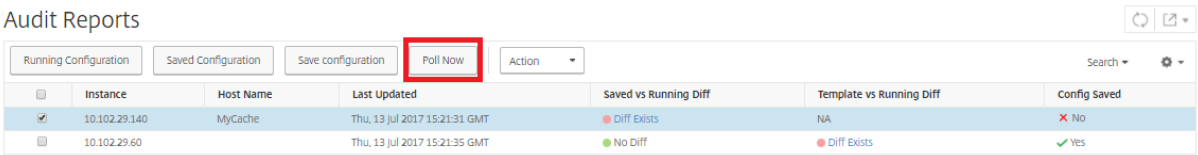


NetScaler ADM vous permet également d'interroger manuellement les audits de configuration et ajoute immédiatement tous les audits de configuration des instances à NetScaler ADM. Pour ce faire, accédez à **Infrastructure > Configuration > Audit de configuration**, cliquez sur **Interroger maintenant**. La page contextuelle **Poll Now** vous permet d'interroger toutes les instances NetScaler 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 NetScaler**
- **Dérive de configuration de NetScaler**

Sur la page **Rapports d'audit**, sélectionnez l'instance et, dans la liste **Action**, sélectionnez **Interroger maintenant** .



Le tableau d'**état du fichier de configuration NetScaler** indique l'état des fichiers NetScaler présents dans le dossier. `nsconfig` NetScaler ADM enregistre et compare les modifications apportées aux fichiers du `nsconfig` dossier 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 **Infrastructure > Configuration > Audit de configuration**.
2. Sur 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** . 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 NetScaler 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 vos applications, NetScaler ADM analyse la configuration de l'instance NetScaler et vous fournit des recommandations. Vous pouvez appliquer les configurations recommandées depuis NetScaler ADM.

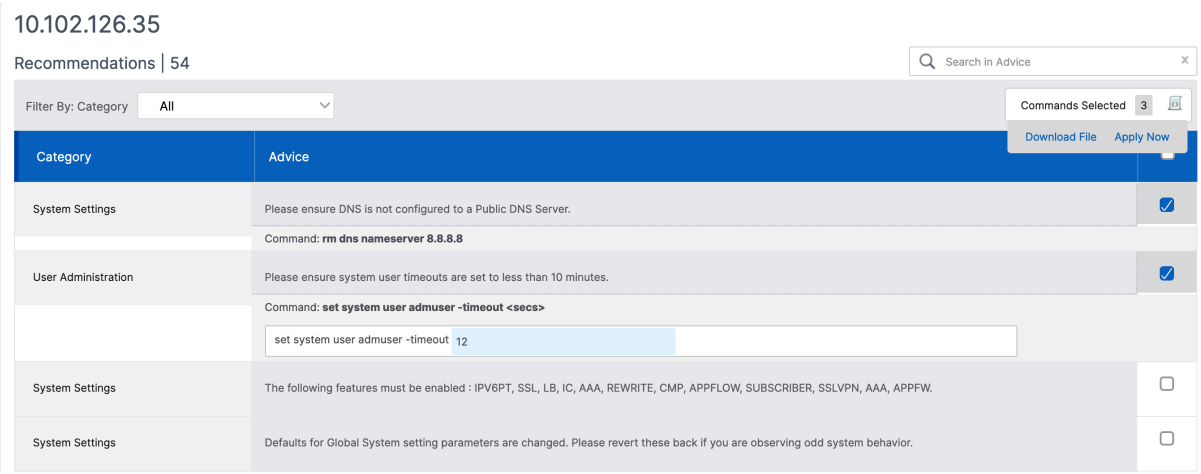
Pour analyser l'instance NetScaler :

1. Accédez à **Infrastructure > Configuration > Audit de configuration > Conseils 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 appareil** et sélectionnez l'instance NetScaler que vous souhaitez analyser.

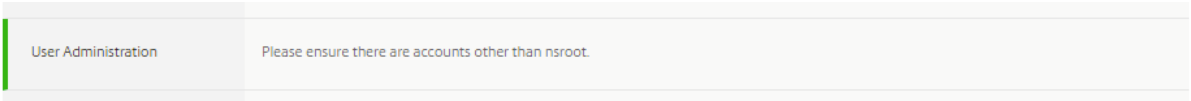
NetScaler ADM analyse la configuration de votre instance et fournit une liste de recommandations de configuration, comme indiqué dans l'image suivante. Cliquez sur la case à cocher à côté d'un conseil de configuration pour afficher les commandes correctives.



Si vous souhaitez mettre à jour votre configuration, spécifiez les valeurs des variables dans les commandes correctives et cliquez sur **Appliquer maintenant** .

> **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 à côté des conseils disparaît.



Pour afficher les détails des commandes exécutées sur votre instance réseau, accédez à **Infrastructure > Instances >**<`Instance\\_Type`**\>** , sélectionnez l'adresse IP de l'instance, puis cliquez sur Afficher les **événements** dans la liste déroulante **Actions** .

Sur la page **Événements** , consultez les détails de la modification de configuration.

Audit de configuration des sondages sur les instances NetScaler

February 1, 2024

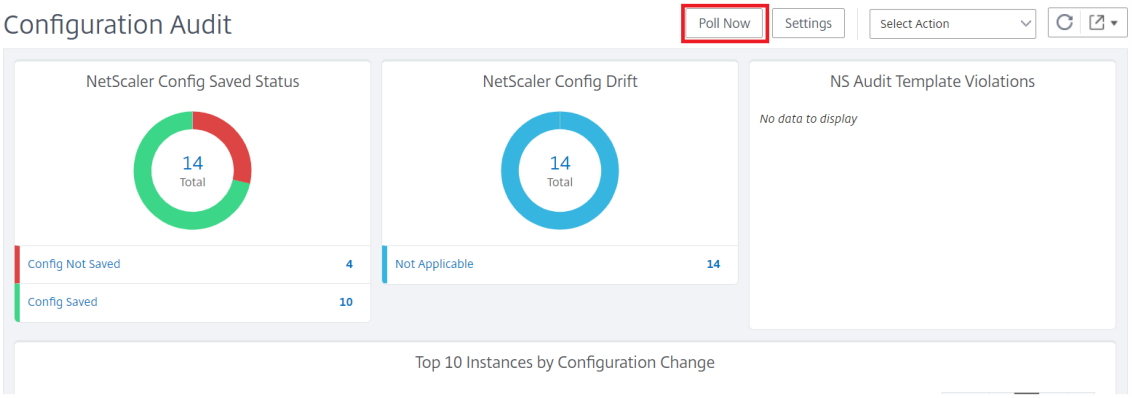
NetScaler ADM interroge automatiquement les audits de configuration toutes les 10 heures afin de détecter les modifications de configuration qui se produisent sur les instances NetScaler. Vous pouvez également interroger manuellement les audits de configuration pour découvrir les modifications ré-

centes, mais l'interrogation de la configuration de toutes les instances NetScaler fait peser une lourde charge sur le réseau.

Au lieu d'interroger l'intégralité de l'audit de configuration de l'instance NetScaler, vous pouvez interroger manuellement uniquement les audits de configuration d'une ou plusieurs instances sélectionnées.

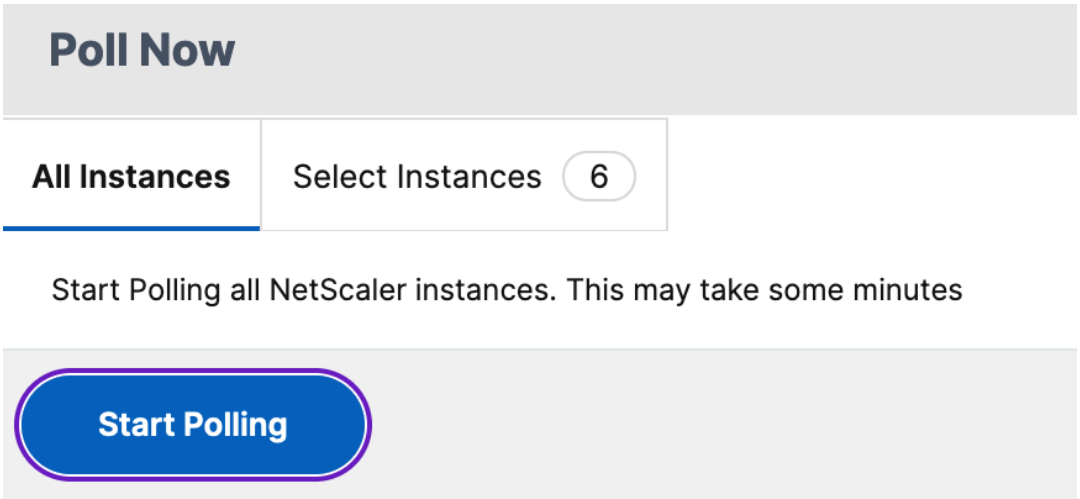
Pour interroger les audits de configuration des instances NetScaler :

1. Dans NetScaler ADM, accédez à **Infrastructure > Configuration > Audit de configuration**.
2. Dans **Configuration Audit** , cliquez sur Sonder **maintenant** .

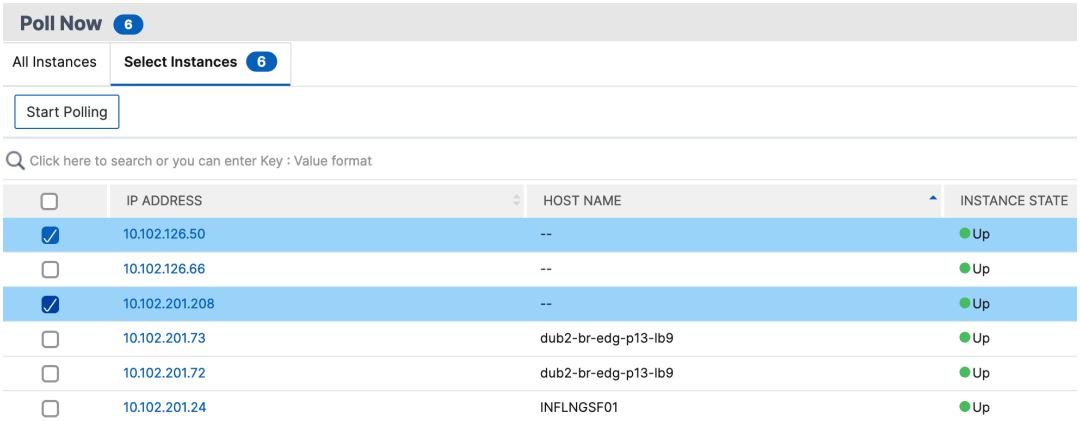


3. La page **Poll Now** s'affiche et vous permet d'interroger toutes les instances NetScaler du réseau ou d'interroger les instances sélectionnées.

   a) Pour interroger toutes les instances NetScaler, 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**.



Générer un diff d'audit de configuration pour les interruptions SNMP ConfigChange

February 1, 2024

Chaque fois qu'une modification de configuration est apportée à une instance NetScaler du réseau, le fichier de configuration est mis à jour. L'instance envoie un piège SNMP ConfigChange à NetScaler ADM. Vous pouvez activer NetScaler ADM pour effectuer un audit de configuration sur cette instance lorsque celle-ci envoie un trap 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 Diff Exists apparaît sur la page **Rapport d'audit** . Cliquez sur le lien **Diff Exists** pour accéder à la page **Configuration Diff** , où vous pouvez consulter la commande corrective. Vous pouvez utiliser ces commandes correctives pour créer une tâche de configuration et l'exécuter sur des instances NetScaler spécifiques. Lorsque vous exécutez le travail de configuration, les instances sont ramenées à la configuration souhaitée.

Pour plus d'informations sur la création de tâches de configuration à partir de commandes correctives, consultez Comment créer des tâches de configuration à partir de commandes correctives sur NetScaler ADM .

Pour exécuter des modèles d'audit de configuration lors de la réception de l'interruption SNMP ConfigChange :

NetScaler ADM vous permet d'activer l'option permettant d'exécuter le modèle d'audit de configuration dans NetScaler ADM.

1. Dans NetScaler ADM, accédez à **Infrastructure > Configuration > Audit de configuration**.
2. Cliquez sur**Paramètres** dans la page **Vérification de la configuration**.

3. Sélectionnez **Effectuer un audit lors de la réception de l'événement « NetScalerConfigChange »**.

> **Remarque :**
>
> NetScaler ADM effectue un audit de configuration pour chaque instance qui recevra les interruptions SNMP NetScalerConfigChange à l'avenir.

1. Dans le champ **Délai d'exécution du modèle d'audit** (en minutes), saisissez les minutes. NetScaler ADM exécute le modèle d'audit de configuration sur l'instance NetScaler après ce délai lorsqu'il reçoit le piège SNMP ConfigChange par cette instance.

Audit de configuration

February 1, 2024

Ce document inclut des rubriques sur la manière de :

- Afficher les rapports d'audit
- Modifications de configuration d'audit entre les instances
- Obtenir des conseils de configuration sur la configuration du réseau
- Audit de configuration des sondages sur les instances NetScaler
- Générer un diff d'audit de configuration pour les pièges SNMP ConfigChange

Tâches de mise à niveau

February 1, 2024

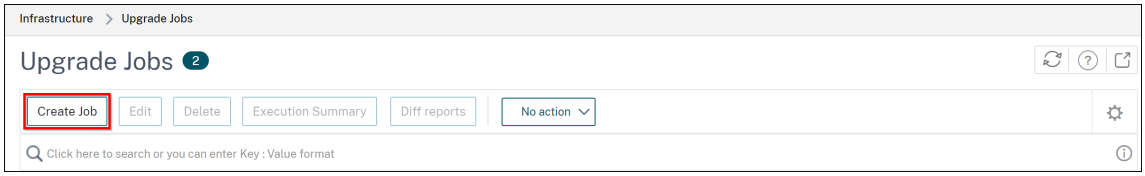
Vous pouvez créer les tâches de maintenance suivantes à l'aide de NetScaler ADM. Vous pouvez ensuite planifier les tâches de maintenance à une date et une heure spécifiques.

- Mettre à niveau les instances NetScaler
- Mettre à niveau les instances NetScaler SDX
- Mettre à niveau les instances NetScaler BLX
- Mettre à niveau les instances NetScaler dans le groupe Autoscale
- Configurer une paire d'instances NetScaler HA
- Convertir une paire d'instances HA en cluster

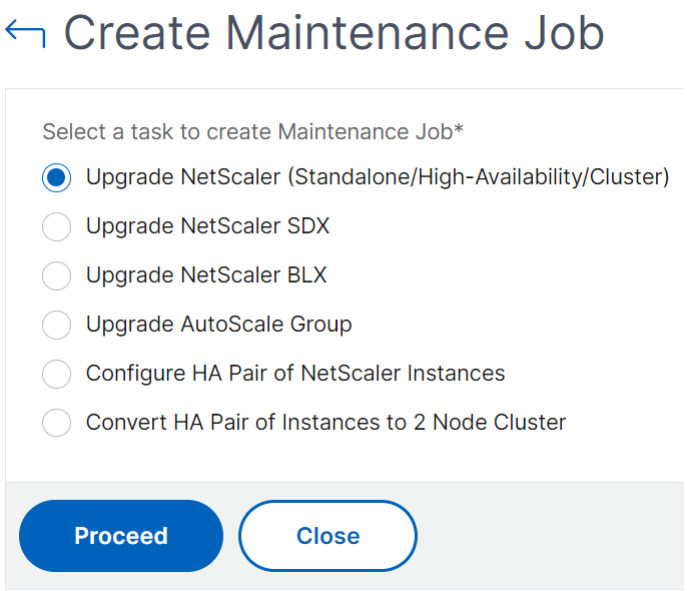
> **Remarque :**
>
> Si une tâche de mise à niveau échoue, NetScaler ADM supprime les fichiers de compilation et les autres fichiers extraits afin de garantir que les instances NetScaler disposent de suffisamment d'espace disque pour la prochaine tentative de mise à niveau.

Planifier la mise à niveau des instances NetScaler

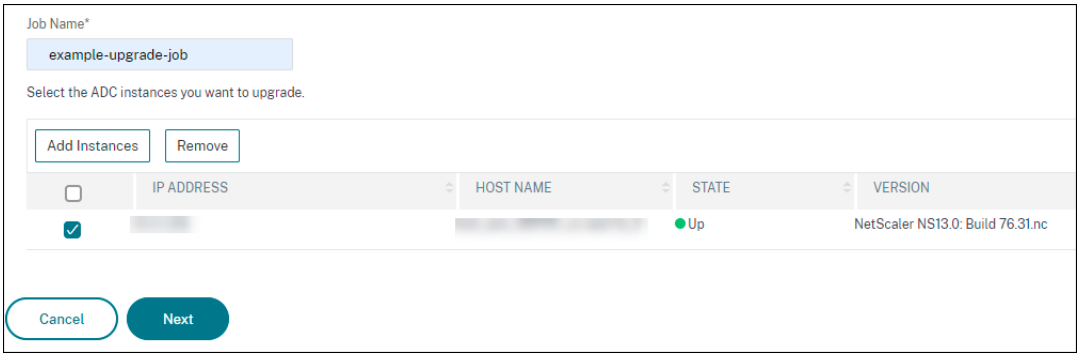
1. Accédez à **Infrastructure > Travaux de mise à niveau**. Cliquez sur **Créer une tâche**.



2. Dans **Créer des tâches de maintenance**, sélectionnez **Mettre à niveau NetScaler (standalone/High-Availability/Cluster)** et cliquez sur **Continuer**.



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. 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 sélectionner l'image. 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 le navigateur de fichiers NetScaler ADM. L'interface graphique NetScaler ADM affiche les fichiers d'instance présents sur. `/var/mps/mps_images`
     - **Ignorez le téléchargement de l'image vers ADC si l'image sélectionnée est déjà disponible** - Sélectionnez cette option si l'image est déjà présente dans l'instance NetScaler.
     - **Nettoyer l'image logicielle de NetScaler en cas de réussite de la mise à niveau** - Sélectionnez cette option pour effacer l'image téléchargée dans l'instance ADC après la mise à niveau de l'instance.

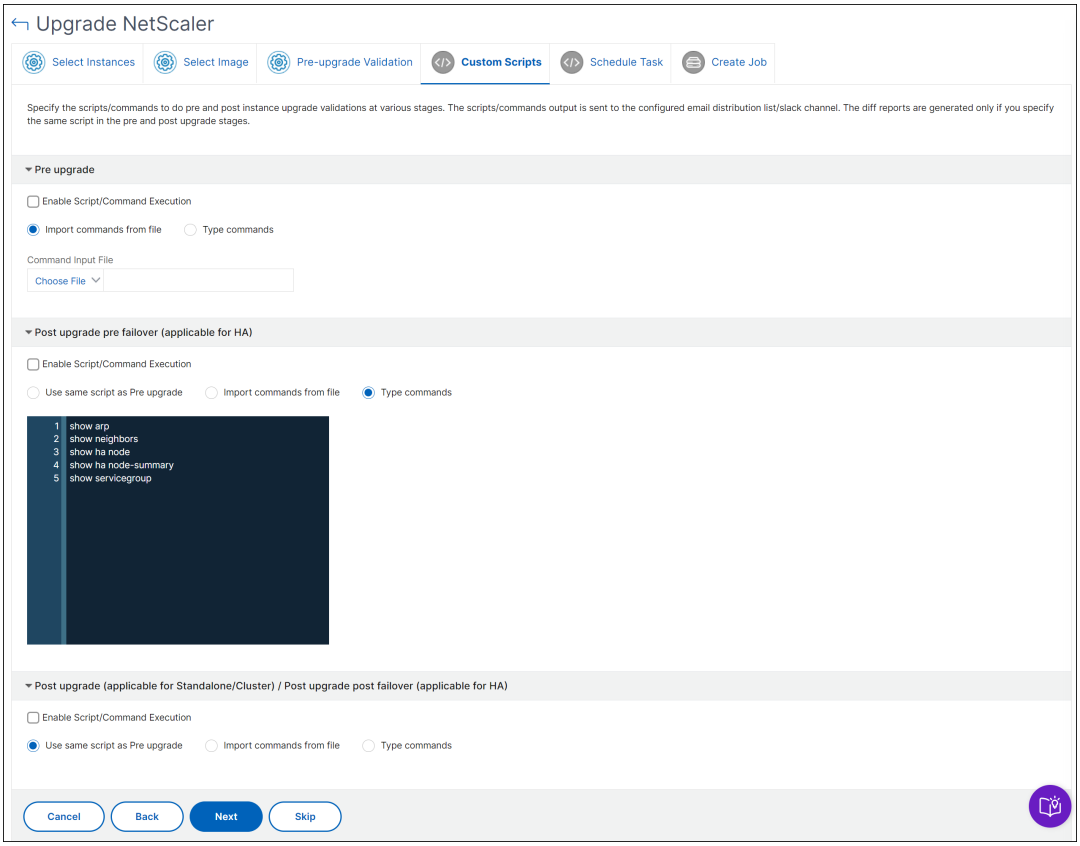
6. Cliquez sur **Suivant** pour lancer la validation préalable à la mise à niveau sur les instances sélectionnées.

   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, NetScaler ADM effectue la validation préalable à la mise à niveau uniquement sur l'instance spécifiée et non sur les autres nœuds du cluster.

7. 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 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.

8. Cliquez sur **Suivant**. 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**.

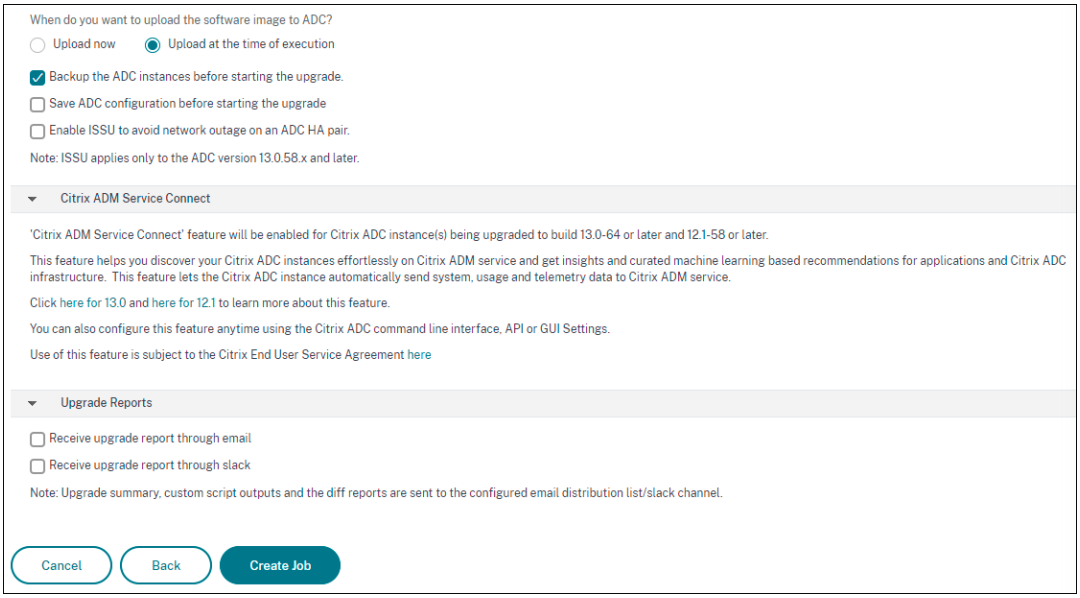
     Spécifiez la **date d'exécution** et l'**heure de début** lorsque vous souhaitez mettre à niveau une autre instance de la paire HA.

9. Cliquez sur **Suivant**. Dans **Créer une tâche**, spécifiez les détails suivants :

    a) 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.
    - **Sauvegardez les instances ADC avant de commencer la mise à niveau.** - Crée une sauvegarde des instances ADC sélectionnées.
    - **Enregistre la configuration ADC avant de démarrer la mise à niveau** : enregistre les tâches de configuration configurées sur l'instance avant la mise à niveau.
    - **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.

- **NetScaler ADM Service** Connect : si vous effectuez une mise à niveau vers les versions **13.0-64 ou ultérieure et 12.1-58 ou versionultérieure**, NetScaler ADM Service Connect est automatiquement activé. Pour plus d'informations, consultez la section Intégration simplifiée des instances NetScaler à l'aide de NetScaler ADM Service Connect.
- **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.



10. Cliquez sur **Créer une tâche**.

Planifier la mise à niveau des instances NetScaler SDX

1. Accédez à **Infrastructure > Travaux de mise à niveau**. Cliquez sur **Créer une tâche**.
2. Sélectionnez **Mettre à niveau NetScaler SDX** et cliquez sur **Continuer**.
3. Sur la page **Mettre à niveau NetScaler SDX**, dans l'onglet **Sélection d'instance** :
   a) Ajoutez un **nom de tâche**.
   b) Dans la liste des **images logicielles**, sélectionnez **Local** (votre machine locale) ou **Appliance (le fichier de génération doit être présent sur l'appliance** virtuelle NetScaler ADM).

      Le processus de chargement commence.
   c) Ajoutez les instances NetScaler SDX sur lesquelles vous souhaitez exécuter le processus de mise à niveau.
   d) Cliquez sur **Suivant**.
4. Dans l'onglet **Planifier la tâche**, sélectionnez **Maintenant** dans la liste **Mode d'exécution** pour mettre à niveau une instance NetScaler SDX maintenant, puis cliquez sur **Terminer**.
5. Pour mettre à niveau une instance NetScaler 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 NetScaler, puis cliquer sur Terminer**

6. Vous pouvez également activer les notifications par e-mail et Slack pour recevoir le rapport d'exécution de la mise à niveau de l'instance NetScaler SDX. Cliquez sur la case à cocher **Recevoir le rapport d'exécution par e-mail** et sur la case à cocher **Recevoir le rapport d'exécution via Slack** pour activer les notifications.

   Pour plus d'informations sur la configuration de la liste de distribution des e-mails et du canal Slack, reportez-vous à l'**étape 8** de la section Planification de la mise à niveau des instances de NetScaler

Planifier la mise à niveau des instances NetScaler BLX

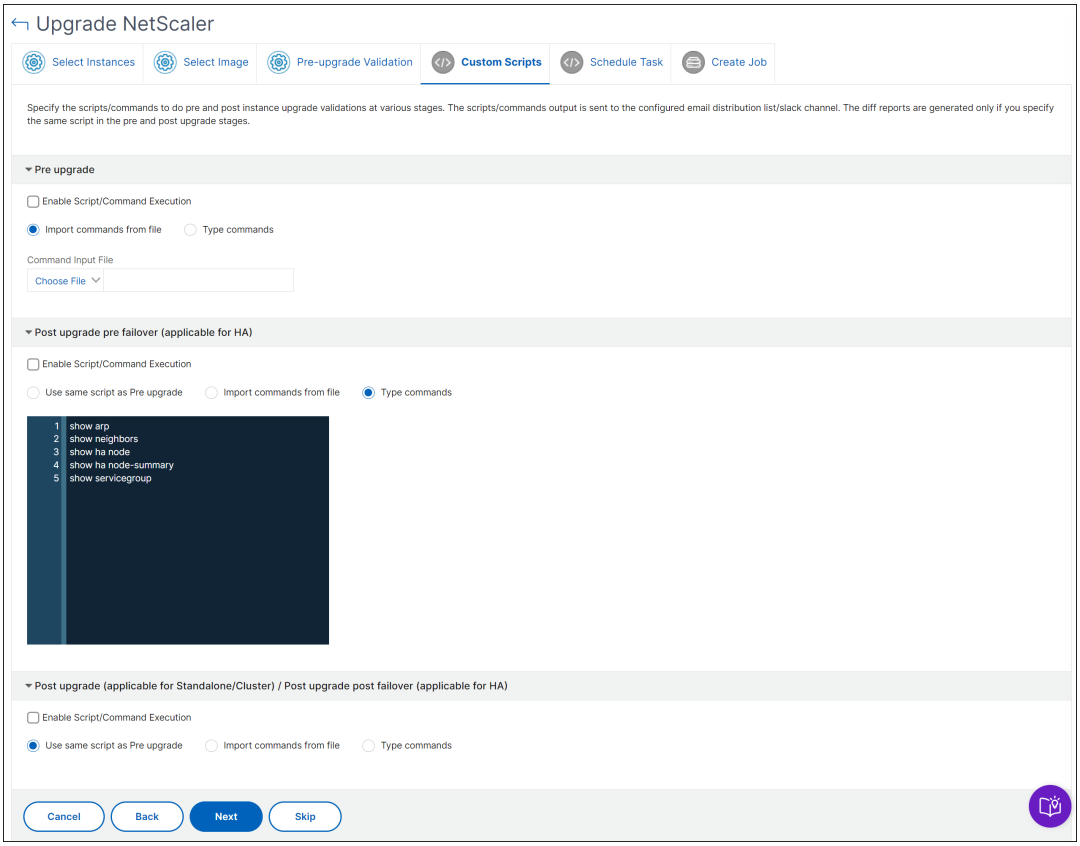
1. Accédez à **Infrastructure > Travaux de mise à niveau**. Cliquez sur **Créer une tâche**.
2. Dans **Create Maintenance Jobs**, sélectionnez **Mettre à niveau NetScaler BLX** et cliquez sur **Proceed**.
3. Dans **Sélectionner une instance**, tapez le nom de votre choix pour **Nom de la tâche**.
4. Cliquez sur **Ajouter des instances** pour ajouter les instances BLX que vous souhaitez mettre à niveau.
   - Pour mettre à niveau une paire HA, spécifiez l'adresse IP d'un 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 sélectionner l'image. Sélectionnez l'une des options suivantes dans la liste **Image logicielle** :
   - **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 le navigateur de fichiers NetScaler ADM. L'interface graphique NetScaler ADM affiche les fichiers d'instance présents sur. `/var/mps/mps_images`
     - **Ignorez le téléchargement de l'image vers ADC si l'image sélectionnée est déjà disponible** - Sélectionnez cette option si l'image est déjà présente dans l'instance NetScaler.
     - **Nettoyer l'image logicielle de NetScaler en cas de réussite de la mise à niveau** - Sélectionnez cette option pour effacer l'image téléchargée dans l'instance ADC après la mise à niveau de l'instance.
6. 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, NetScaler ADM effectue la validation préalable à la mise à niveau uniquement sur l'instance spécifiée et non sur les autres nœuds du cluster.

7. 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 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.

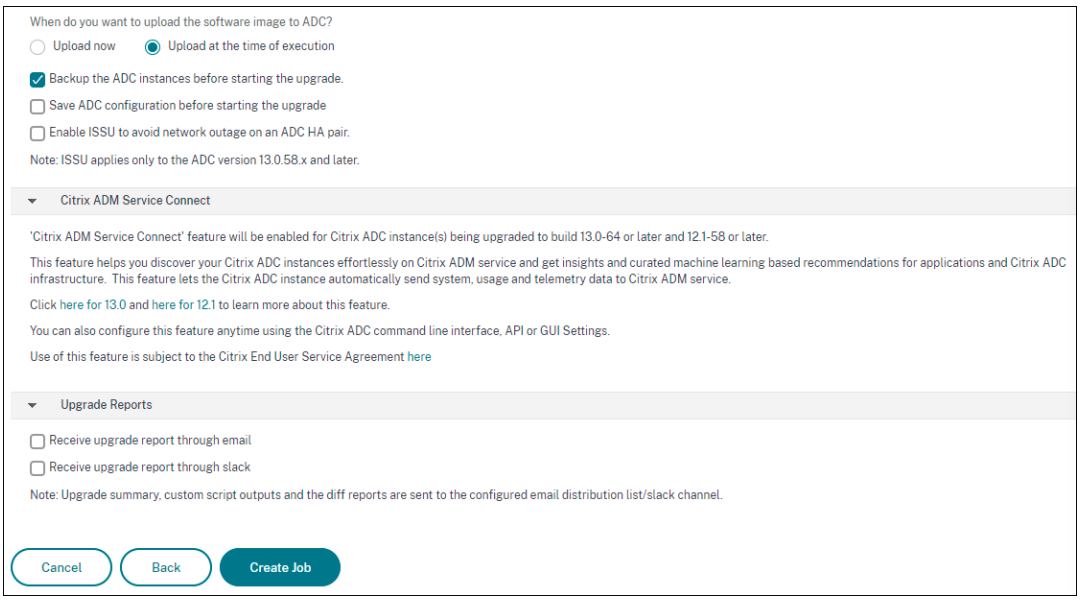
- Les routes dynamiques.

8. Cliquez sur **Suivant**. 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 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.
9. Cliquez sur **Suivant**. Dans **Créer une tâche**, spécifiez les détails suivants :
   a) 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.
      - **Sauvegarder les instances ADC avant de démarrer la mise à niveau** : crée une sauvegarde des instances ADC sélectionnées.
      - **Enregistre la configuration ADC avant de démarrer la mise à niveau** : enregistre les tâches de configuration configurées sur l'instance avant la mise à niveau.
      - **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.

   - **NetScaler ADM Service** Connect : si vous effectuez une mise à niveau vers les versions **13.0-64 ou ultérieure et 12.1-58 ou versionultérieure**, NetScaler ADM Service Connect est automatiquement activé. Pour plus d'informations, consultez la section Intégration simplifiée des instances NetScaler à l'aide de NetScaler ADM Service Connect.
   - **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.



10. Cliquez sur **Créer une tâche**.

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. Accédez à **Infrastructure > Travaux de mise à niveau**. Cliquez sur **Créer une tâche**.
2. Sélectionnez **Mettre à niveau le groupe Autoscale** et 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 NetScaler. Cette image est la version existante des instances NetScaler du groupe Autoscale.
   c) Dans **NetScaler Image**, parcourez le fichier de version de NetScaler 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 les instances NetScaler, procédez immédiatement à la mise à niveau.

- **Plus tard :** pour démarrer la mise à niveau des instances NetScaler 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 les notifications de marge pour recevoir le rapport d'exécution du groupe Mise à niveau Autoscale. Cliquez sur la case à cocher **Recevoir le rapport d'exécution par e-mail** et sur la case à cocher **Recevoir le rapport d'exécution via Slack** pour activer les notifications.

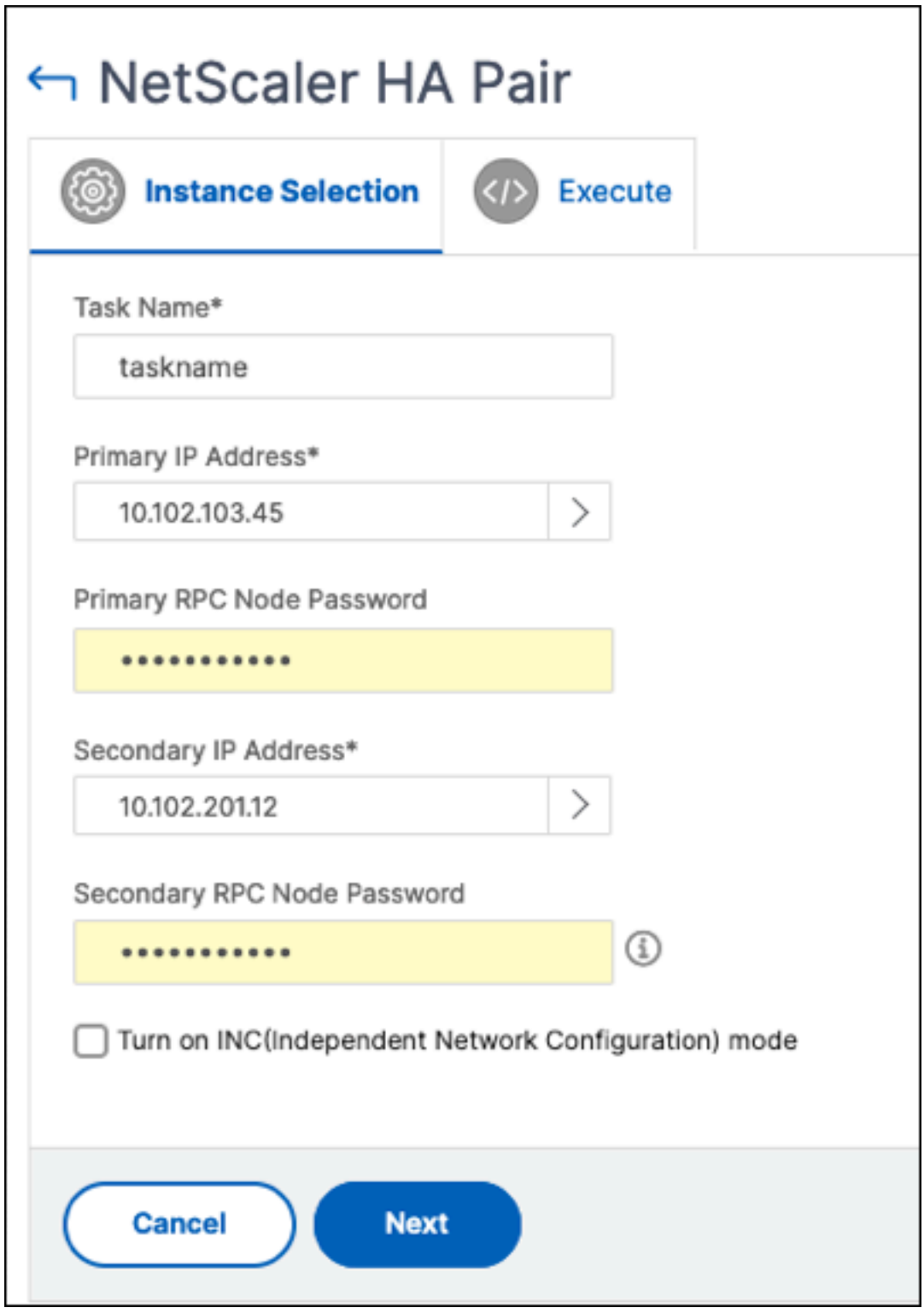
5. Cliquez sur **Terminer**.

Planifier la configuration d'une paire d'instances NetScaler HA

1. Accédez à **Infrastructure > Travaux de mise à niveau**. Cliquez sur **Créer une tâche**.
2. Sélectionnez **Configurer la paire HA d'instances NetScaler** et cliquez sur **Continuer**.
3. Sur la page **NetScaler HA Pair**, dans l'onglet **Sélection d'instances** :
   a) Ajoutez un **nom de tâche**.
   b) Sélectionnez l'adresse IP principale. Cliquez sur **OK**.
   c) Entrez le mot de passe du nœud RPC principal.
   d) Sélectionnez l'adresse IP secondaire. Cliquez sur **OK**.

> **Remarque :**
>
> Les champs de mot de passe du nœud RPC sont disponibles dans NetScaler version 14.1 et versions ultérieures.

   e) Entrez le mot de passe du nœud RPC secondaire.
   f) Cliquez pour **activer le mode INC (Independent Network Configuration)** si vous avez les instances de paires HA dans deux sous-réseaux.
   g) Cliquez sur **Suivant**.



4. Dans l'onglet **Planifier la tâche**, sélectionnez **Maintenant** dans la liste **Mode d'exécution** pour mettre à niveau une instance NetScaler maintenant, puis cliquez sur **Terminer**.
5. Pour mettre à niveau une paire NetScaler HA ultérieurement, **sélectionnez** Plus tard dans **la**

liste des modes d'exécution. **Vous pouvez ensuite choisir la date d'exécution et l'heure de début de la mise à niveau de l'instance NetScaler, puis cliquer sur Terminer.**

6. Vous pouvez également activer les notifications par e-mail et les notifications de marge pour recevoir le rapport d'exécution de la création de la paire ADC HA. Cliquez sur la case à cocher **Recevoir le rapport d'exécution par e-mail** et sur la case à cocher **Recevoir le rapport d'exécution via Slack** pour activer les notifications.

   Pour plus d'informations sur la configuration de la liste de distribution des e-mails et du canal Slack, reportez-vous à l'**étape 8** de la section Planification de la mise à niveau des instances de NetScaler

Planifier la conversion d'une paire d'instances HA en cluster

1. Accédez à **Infrastructure > Travaux de mise à niveau**. Cliquez sur **Créer une tâche**.
2. Sélectionnez **Convertir la paire d'instances HA en cluster à 2 nœuds** et cliquez sur **Continuer**.
3. Dans la page **Migrer NetScaler HA vers le cluster**, dans l'onglet **Sélection d'instance**, ajoutez un **nom de tâche** . Spécifiez l'adresse IP principale, l'adresse IP secondaire, l'ID du nœud principal, l'ID du nœud secondaire, l'adresse IP du cluster, l'ID du cluster et le fond de panier, puis cliquez sur **Suivant**.
4. Dans l'onglet **Planifier la tâche**, sélectionnez **Maintenant** dans la liste **Mode d'exécution** pour mettre à niveau une instance NetScaler maintenant, puis cliquez sur **Terminer**.
5. Pour effectuer une mise à niveau ultérieure, 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 NetScaler, puis cliquer sur **Terminer**.
6. Vous pouvez également activer les notifications par e-mail et Slack pour recevoir le rapport d'exécution de la mise à niveau d'une instance NetScaler SDX. Cliquez sur la case à cocher **Recevoir le rapport d'exécution par e-mail** et sur la case à cocher **Recevoir le rapport d'exécution via Slack** pour activer les notifications.

   Pour plus d'informations sur la configuration de la liste de distribution des e-mails et du canal Slack, reportez-vous à l'**étape 8** de la section Planifier la mise à niveau des instances NetScaler.

Utiliser des tâches pour mettre à niveau les instances NetScaler

February 1, 2024

Vous pouvez utiliser NetScaler Application Delivery Management (ADM) pour mettre à niveau une ou plusieurs instances NetScaler. 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 NetScaler en créant une tâche de maintenance, effectuez le contrôle 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 NetScaler 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 NetScaler 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.

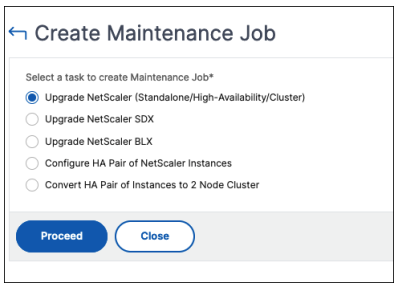
Lorsque vous mettez à niveau un cluster NetScaler, l'ADM effectue une validation préalable à la mise à niveau sur l'instance spécifiée uniquement. Avant de procéder à la mise à niveau, vérifiez et résolvez les problèmes de personnalisation, d'utilisation du disque et de matériel sur les nœuds du cluster.

Créez une tâche de maintenance des mises à niveau pour mettre à niveau les instances NetScaler

> **Remarque**
>
> La mise à niveau de NetScaler d'une version supérieure vers une version inférieure n'est pas prise en charge. Par exemple, si votre instance NetScaler est 13.0 82.x, vous ne pouvez pas rétrograder l'instance NetScaler vers la version 13.0 79.x ou toute autre version antérieure.

1. Dans NetScaler ADM, accédez à **Infrastructure > Tâches de mise à niveau**. Cliquez sur le bouton **Créer un travail**.

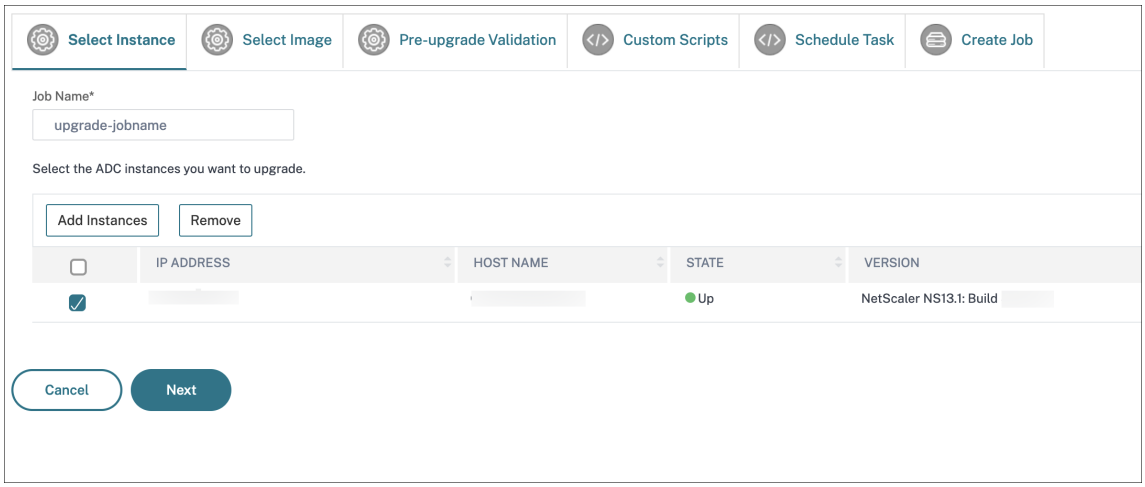
2. Dans **Créer des tâches de maintenance**, sélectionnez **Mettre à niveau NetScaler (standalone/High-Availability/Cluster)** et cliquez sur **Continuer**.



3. Dans **Sélectionner une instance**, tapez le nom de votre choix pour **Nom de la tâche**.
4. Cliquez sur **Ajouter des instances pour ajouter les instances** de NetScaler que vous souhaitez mettre à niveau.

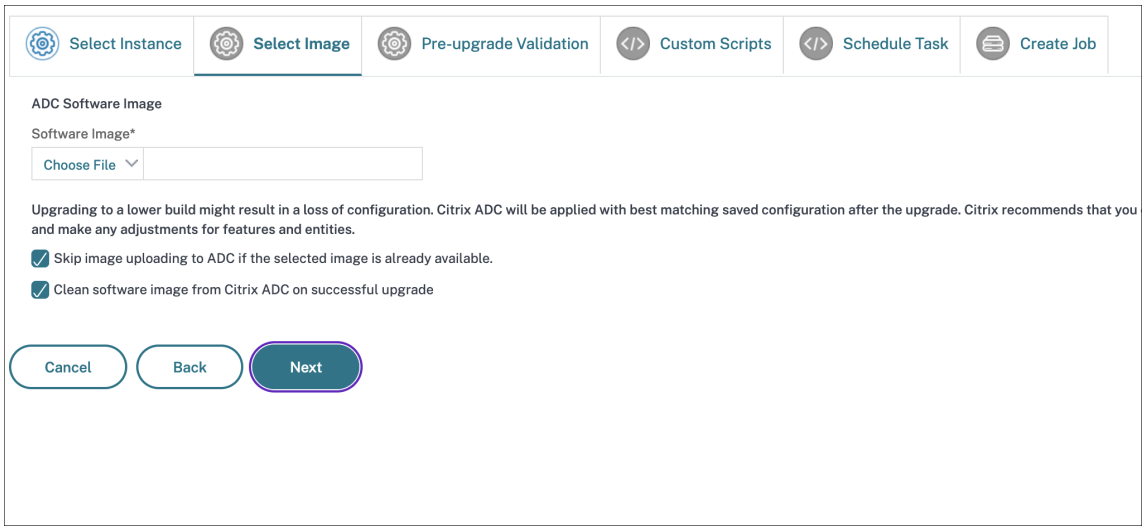
    - Pour mettre à niveau une paire haute disponibilité NetScaler, sélectionnez les adresses IP de la paire haute disponibilité (indiquées par l'exposant « S » et « P »).

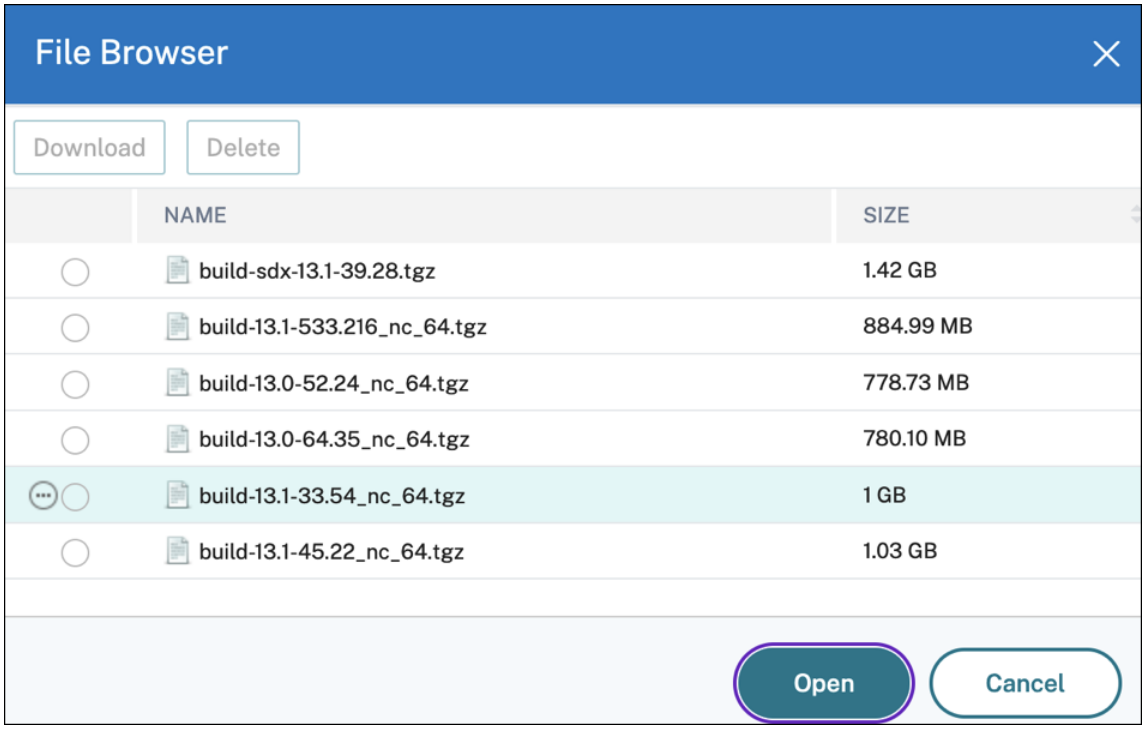
- Pour mettre à niveau un cluster, sélectionnez l'adresse IP du cluster (indiquée par l'exposant « C »).



5. Dans l'onglet **Select Image**, sélectionnez une image NetScaler depuis votre disque local ou parmi les images de génération.

   - **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 NetScaler ADM. L'interface graphique NetScaler ADM affiche les fichiers d'instance présents sur. `/var/mps/ns_images`





- **Ignorer le téléchargement de l'image vers NetScaler si l'image sélectionnée est déjà** disponible - Cette option vérifie si l'image sélectionnée est disponible dans NetScaler. La tâche de mise à niveau ignore le téléchargement d'une nouvelle image et utilise l'image disponible dans NetScaler.
- **Nettoyer l'image logicielle de NetScaler en cas de mise à niveau réussie** : cette option efface l'image téléchargée dans l'instance NetScaler après la mise à niveau de l'instance.

Cliquez sur **Suivant** pour lancer la validation préalable à la mise à niveau sur les instances sélectionnées.

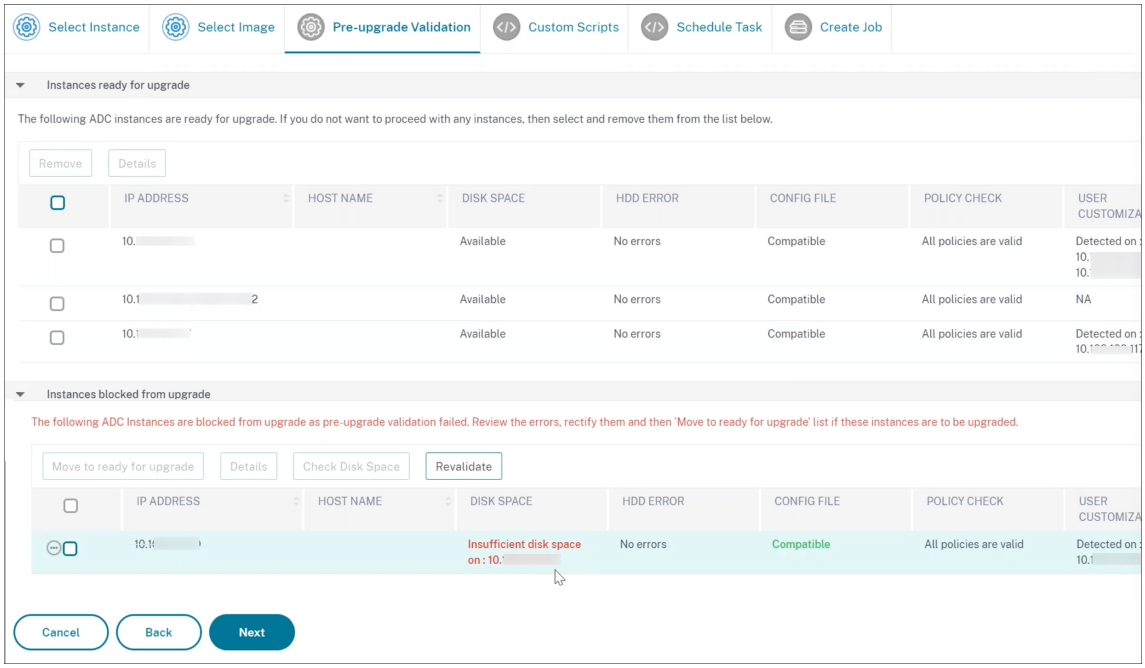
> **Remarque :**
>
> - Les images NetScaler téléchargées sont stockées dans l'agent NetScaler ADM et sont présentes dans `/var/mps/adcimages`. Ces images mises en cache peuvent être utilisées pour plusieurs mises à niveau de NetScaler, éliminant ainsi le besoin de télécharger une image à chaque mise à niveau.
> - NetScaler ADM efface les images NetScaler mises en cache tous les trois jours en fonction de l'heure de dernière modification des images. Seuls les deux derniers fichiers image sont mis en cache dans l'agent NetScaler ADM à la fois.

6. L'onglet **Validation préalable à la mise à niveau** contient les sections suivantes :

   - **Instances prêtes à être mises à niveau**. Vous pouvez poursuivre la mise à niveau de ces instances.

- **Instances bloquées lors de la mise à niveau**. La mise à niveau de ces instances NetScaler est bloquée en raison d'erreurs de validation avant la mise à niveau.

  Vous pouvez vérifier et corriger les erreurs, puis cliquer sur **Déplacer pour être prêt pour la mise à niveau pour** les mettre à niveau. 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 de NetScaler.



- **Vérification des stratégies** : si NetScaler ADM détecte des stratégies classiques non prises en charge, vous pouvez supprimer ces stratégies pour créer une tâche de mise à niveau.

> **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.

7. 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 la mise à niveau d'une instance NetScaler. 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 :

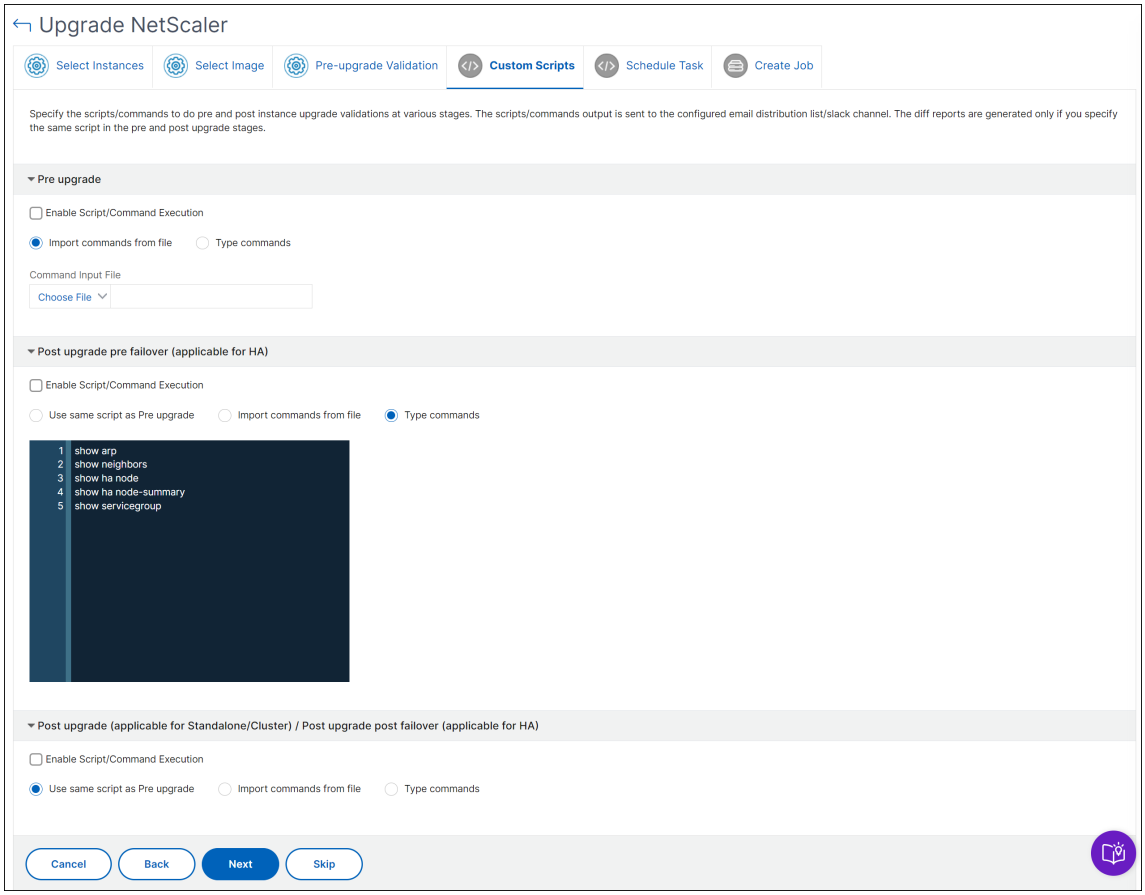
- **Avant mise à niveau** : le script spécifié s'exécute avant la mise à niveau d'une instance.
- **Après mise à niveau avant basculement (applicable pour HA)** : Cette étape s'applique uniquement au déploiement haute disponibilité. Le script spécifié s'exécute après la mise à niveau des nœuds, mais 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.
- **Tapez les commandes** : entrez les commandes directement dans 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.



8. 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 NetScaler HA en deux étapes, **sélectionnez Effectuer une mise à niveau en deux étapes pour les**nœuds en HA.

     Spécifiez la **date d'exécution** et l'**heure de début** lorsque vous souhaitez mettre à niveau une autre instance de la paire HA.

9. Dans **Créer une tâche**, spécifiez les détails suivants :

   a) Sélectionnez l'une des options suivantes dans la liste des **images logicielles** :

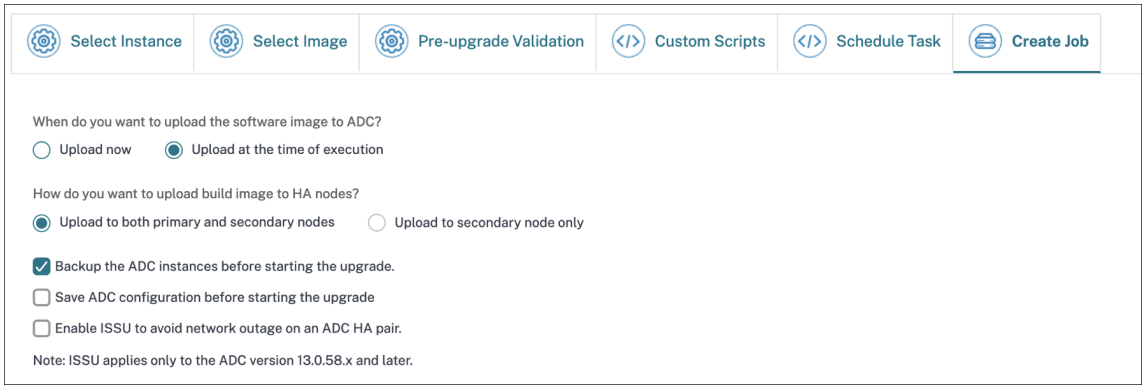
      - **Local** : sélectionnez le fichier de mise à niveau de l'instance sur votre machine locale.
      - **Appliance** : sélectionnez le fichier de mise à niveau de l'instance dans un navigateur de fichiers ADM. L'interface graphique ADM affiche les fichiers d'instance présents sur `/var/mps/mps_images`.

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.

Pour une paire à haute disponibilité, vous pouvez spécifier les nœuds sur lesquels vous souhaitez télécharger l'image :

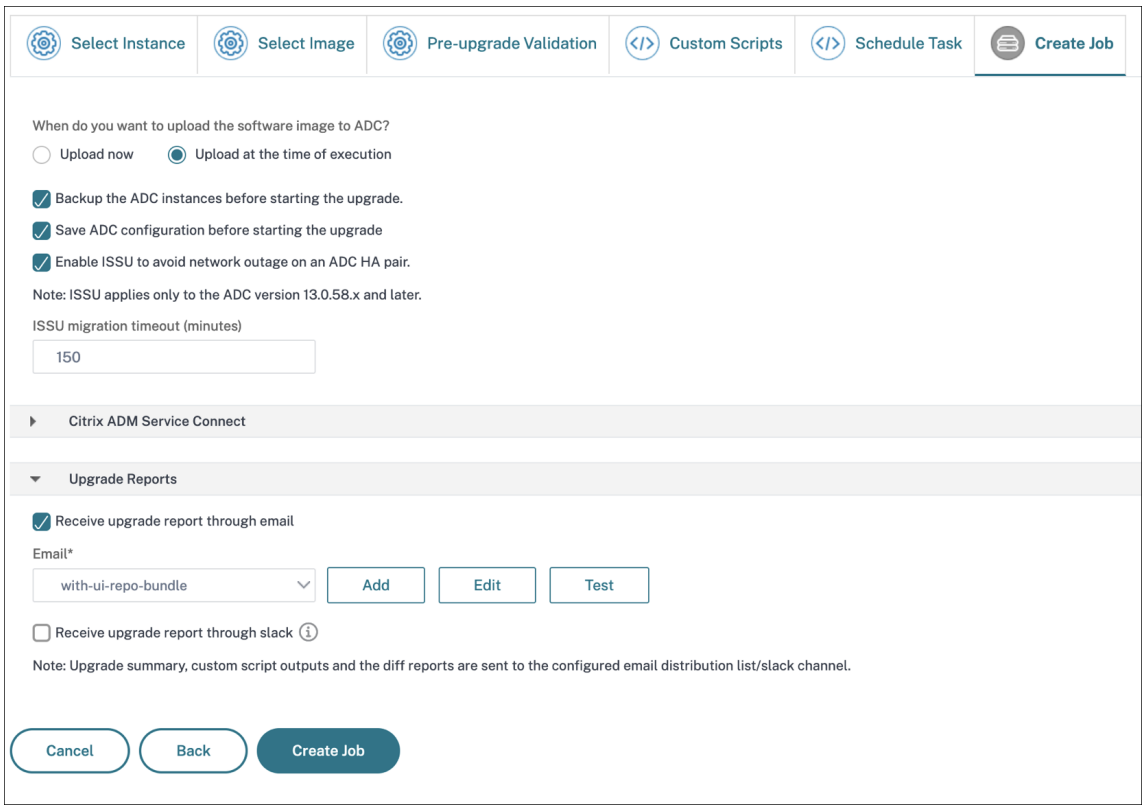
- **Charger vers les nœuds principal et secondaire** : chargez le fichier image de génération vers les nœuds principal et secondaire.
- **Charger uniquement vers le nœud secondaire** : chargez le fichier image de génération uniquement vers le nœud secondaire. Une fois le nœud secondaire mis à niveau, un basculement se produit et le fichier image de génération est chargé vers le nouveau nœud secondaire qui était auparavant le nœud principal.



Pour plus d'informations sur les scénarios de planification disponibles pour une paire haute disponibilité, consultez la section Planification de tâches de mise à niveau pour une paire haute disponibilité.

- **Nettoyer l'image logicielle de NetScaler en cas de mise à niveau réussie** : sélectionnez cette option pour effacer l'image téléchargée dans l'instance NetScaler après la mise à niveau de l'instance.
- **Sauvegardez les instances de NetScaler avant de commencer la mise à niveau.** - Crée une sauvegarde des instances NetScaler sélectionnées.
- **Conserver l'état principal et secondaire des nœuds HA après la mise à niveau** : sélectionnez cette option si vous souhaitez que la tâche de mise à niveau démarre 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 NetScaler avant de commencer la mise à niveau : enregistre la configuration** NetScaler en cours d'exécution avant de mettre à niveau les instances NetScaler.
- **Activez ISSU pour éviter les pannes réseau sur la paire NetScaler HA** : ISSU garantit la mise à niveau sans interruption de service d'une paire NetScaler haute disponibilité. Cette option fournit une fonctionnalité de migration qui respecte les connexions existantes lors de la mise à niveau. Vous pouvez donc mettre à niveau une paire NetScaler HA sans interruption de service. 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.

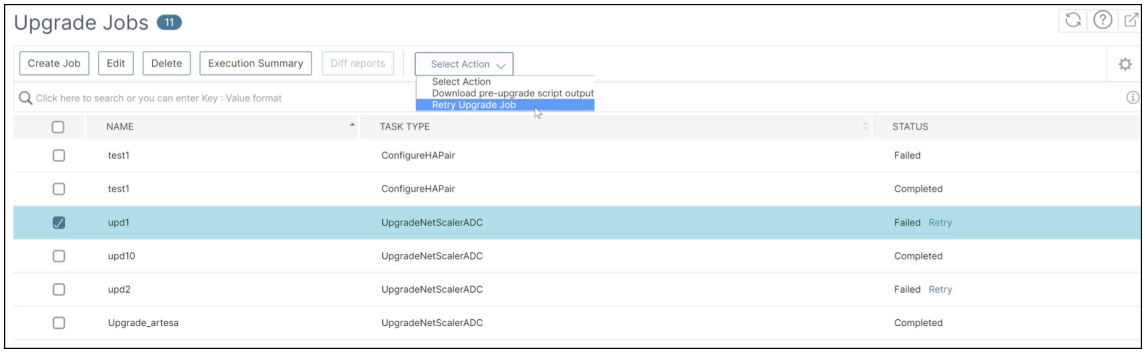


10. Cliquez sur **Créer une tâche**.

La tâche de mise à niveau apparaît dans **Infrastructure > Tâches de mise à niveau**. 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**.

Réessayer les tâches de mise à niveau qui ont échoué

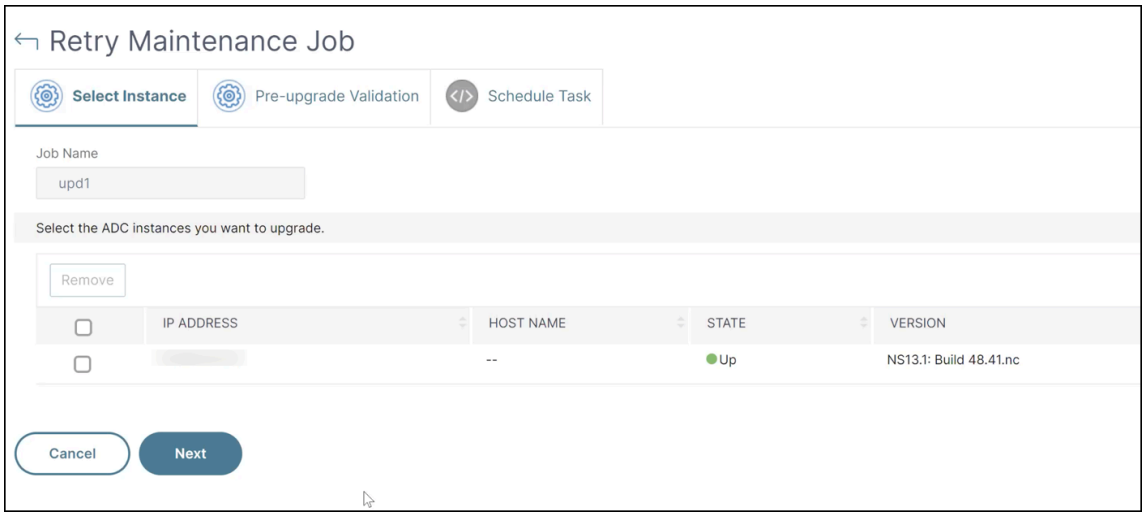
1. Dans **Infrastructure > Tâches de mise à niveau**, sélectionnez la tâche de mise à niveau qui a échoué et cliquez sur **Réessayer**. Vous pouvez également accéder à **Sélectionner une action > Réessayer la tâche de mise à niveau pour réessayer une tâche** qui a échoué.



2. Dans **Select Instance**, spécifiez les détails suivants :

   - **Nom de la tâche** : entrez un nom pour la mise à niveau.
   - Sélectionnez les instances NetScaler que vous souhaitez mettre à niveau dans la liste. Pour supprimer des instances, cliquez sur **Supprimer**.

   Cliquez sur **Suivant** pour commencer le processus de validation.

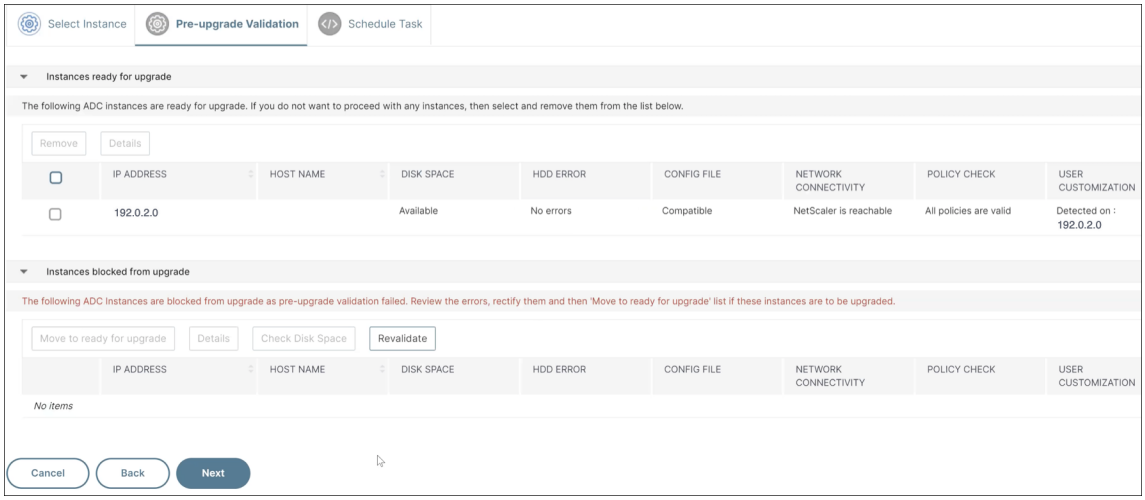


3. L'onglet **Validation préalable à la mise à niveau** contient les sections suivantes :

   - **Instances prêtes à être mises à niveau**. Vous pouvez poursuivre la mise à niveau de ces instances.
   - **Instances bloquées lors de la mise à niveau**. La mise à niveau de ces instances NetScaler est bloquée en raison d'erreurs de validation avant la mise à niveau.

Vous pouvez vérifier et corriger les erreurs, puis cliquer sur **Déplacer pour être prêt pour la mise à niveau pour** les mettre à niveau. Si l'espace disque est insuffisant sur une instance, vous pouvez vérifier et nettoyer l'espace disque. Consultez Nettoyer l'espace disque NetScaler.

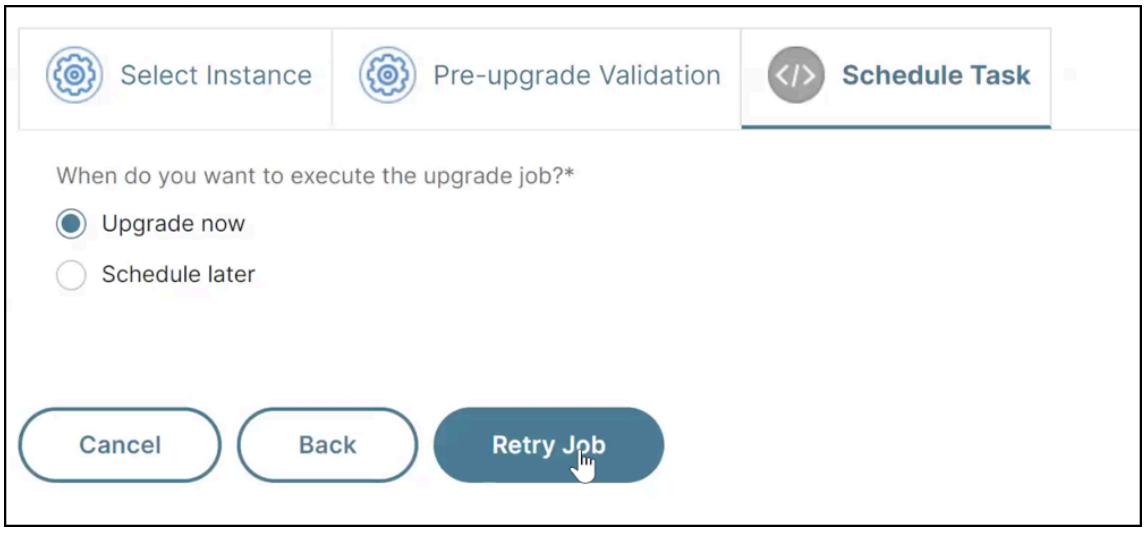
- **Vérification des stratégies** : si NetScaler ADM détecte des stratégies classiques non prises en charge, vous pouvez supprimer ces stratégies pour créer une tâche de mise à niveau.



Cliquez sur **Suivant**.

4. 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.



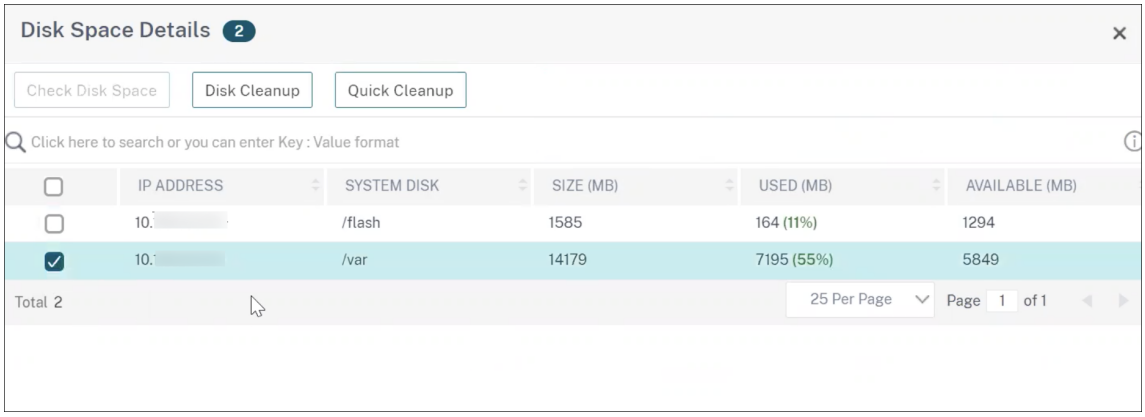
Cliquez sur **Réessayer**.

Nettoyez l'espace disque de NetScaler

Si vous rencontrez un problème d'espace disque insuffisant lors de la mise à niveau d'une instance NetScaler, nettoyez l'espace disque à partir de l'interface graphique NetScaler ADM elle-même.

1. Dans l'onglet **Validation préalable à la mise à niveau**, la section **Instances bloquées lors de la mise à niveau** affiche les instances dont la mise à niveau a échoué en raison d'un espace disque insuffisant. Sélectionnez l'instance qui présente le problème d'espace disque.
2. Cliquez sur **Vérifier l'espace disque**.

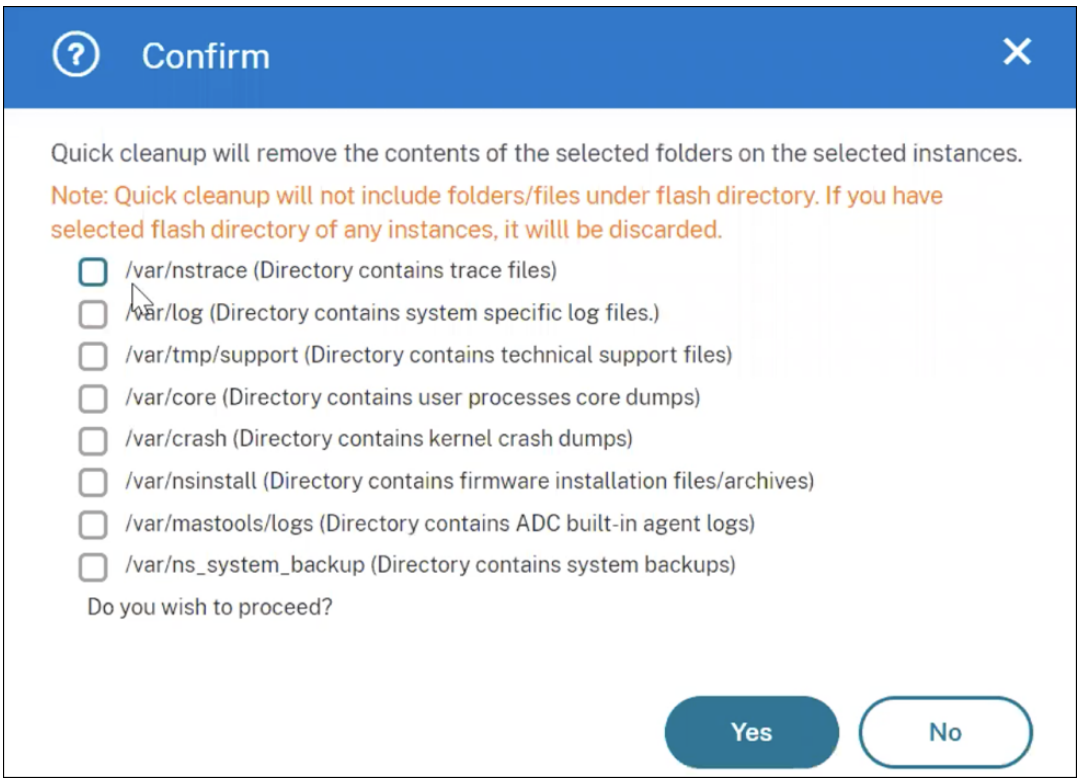
   Un volet **Détails de l'espace disque** apparaît. Ce volet affiche les instances, la mémoire utilisée et la mémoire disponible.



3. Dans le volet **Détails de l'espace disque**, sélectionnez l'instance qui doit être nettoyée et effectuez l'une des opérations suivantes :

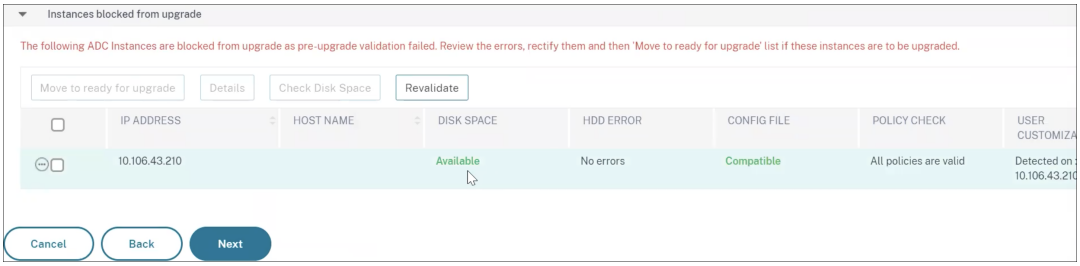
   a) **Nettoyage de disque** : accédez aux dossiers ou répertoires requis et supprimez-les pour libérer de l'espace disque.

   b) **Nettoyage rapide** - Libérez rapidement de l'espace disque en supprimant plusieurs dossiers. Dans le volet **Confirmer** qui s'affiche, sélectionnez les dossiers que vous souhaitez supprimer, puis cliquez sur **Oui**.



c) Après avoir libéré de l'espace disque, vous pouvez vérifier si suffisamment d'espace disque est désormais disponible pour mettre à niveau l'instance. Dans la section **Instances bloquées pour la mise à niveau**, cliquez sur **Revalider**.

Dans l'exemple suivant, de l'espace disque est disponible. Vous pouvez maintenant cliquer sur **Déplacer vers Prêt pour la mise** à niveau pour mettre à niveau l'instance ou sur **Suivant** pour passer à l'étape suivante.



Planification de tâches de mise à niveau pour une paire NetScaler à haute disponibilité

Le tableau suivant répertorie les différents scénarios de planification de la page **Planifier une tâche** et les options de mise à niveau correspondantes disponibles sur la page **Créer une tâche** :

Quand souhaitez-vous exécuter la tâche de mise à niveau ?	Quand souhaitez-vous télécharger l'image logicielle sur NetScaler ?	Comment souhaitez-vous télécharger l'image de construction sur les nœuds HA ?
Passez à la version supérieure	Non applicable	**Charger vers les nœuds principal et secondaire** (option par défaut)
Programmez plus tard	**Charger au moment de l'exécution** (option par défaut)	**Charger vers les nœuds principal et secondaire** (option par défaut)
Planifier ultérieurement (lorsque l'option **Effectuer une mise à niveau en deux étapes pour les nœuds dans HA** est sélectionnée)	**Charger au moment de l'exécution** (option par défaut)	**Charger maintenant** **Charger vers le nœud secondaire uniquement** (option par défaut et unique) **Charger maintenant**

Télécharger un rapport différentiel combiné d'une tâche de mise à niveau de NetScaler

Vous pouvez télécharger un rapport différentiel d'une tâche de mise à niveau de NetScaler 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. Ce rapport vous permet de déterminer les modifications apportées à l'instance NetScaler après la 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.

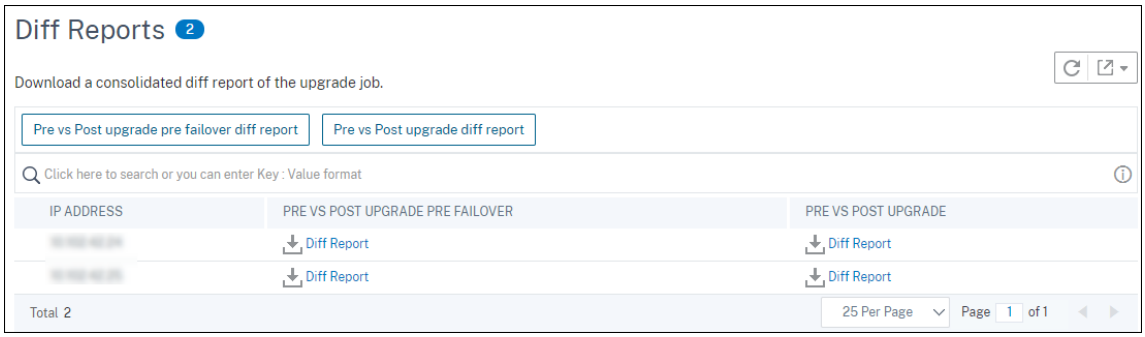
Pour télécharger un rapport diff d'une tâche de mise à niveau, procédez comme suit :

1. Accédez à **Infrastructure > 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**



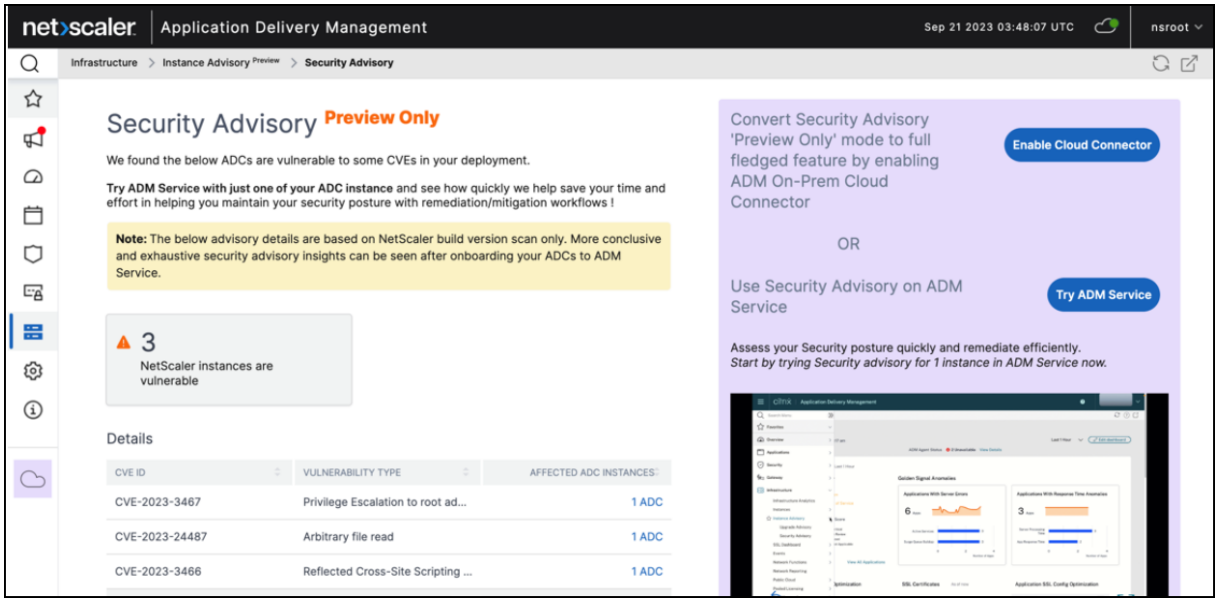
Avis de sécurité

February 1, 2024

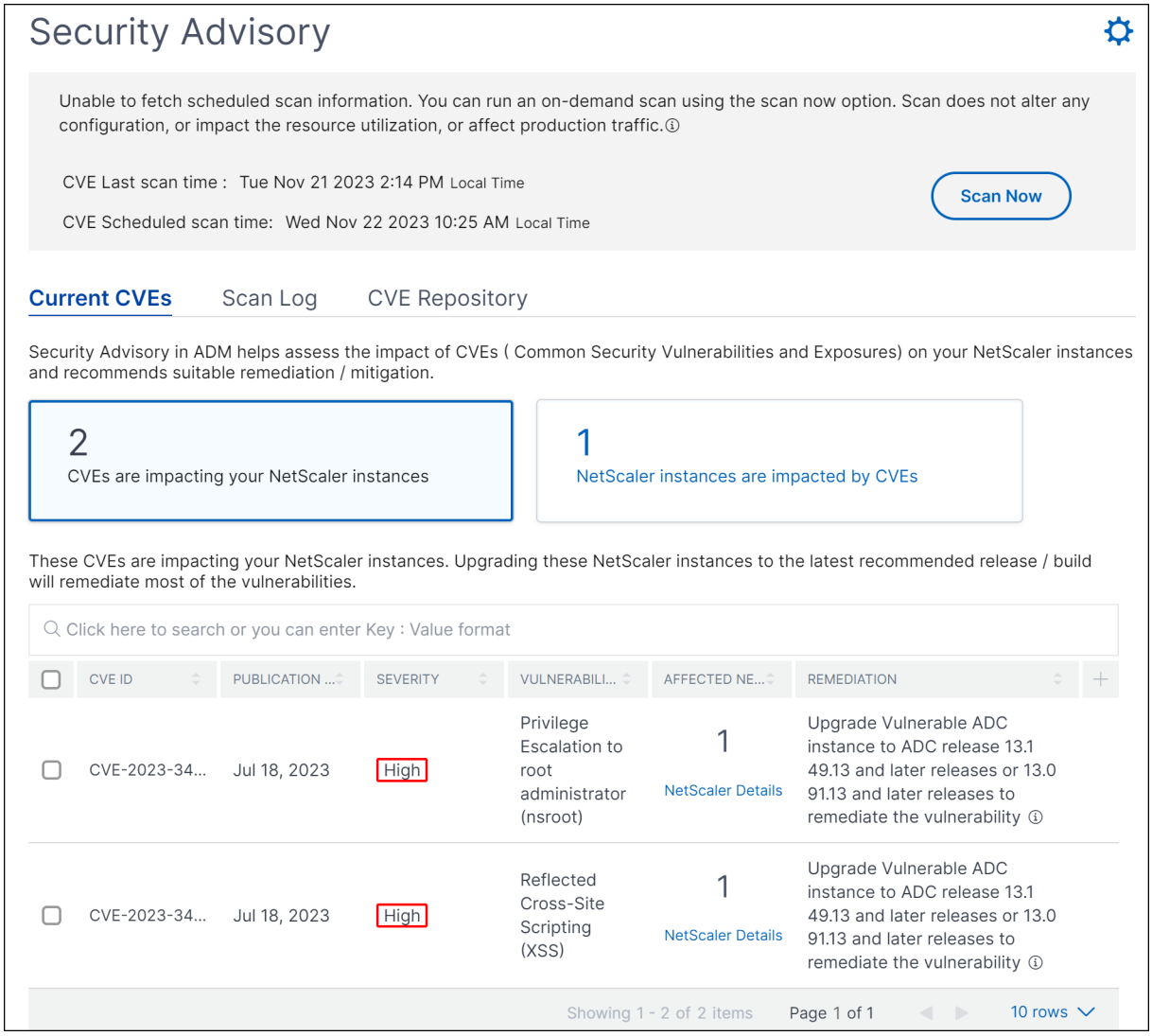
Une infrastructure sûre, sécurisée et résiliente est la ligne de vie de toute organisation. Les entreprises doivent suivre les nouvelles vulnérabilités et expositions courantes (CVE) et évaluer l'impact des CVE sur leur infrastructure. Ils doivent également comprendre et planifier les mesures correctives pour résoudre les vulnérabilités. La fonction d'avis de sécurité de NetScaler ADM vous permet d'identifier les CVE qui mettent en danger vos instances NetScaler et de recommander des mesures correctives.

À partir de la version 14.1 8.x, vous pouvez utiliser la version complète de l'avis de sécurité en configurant **ADM On-Prem Cloud Connector** et en activant **l'avis de sécurité**.

Si vous n'avez pas configuré ADM On-Prem Cloud Connector, vous pouvez uniquement consulter la version préliminaire de Security Advisory. Vous pouvez cliquer sur **Activer le Cloud Connector** et terminer la configuration pour utiliser la version complète de l'avis de sécurité. Pour plus d'informations, consultez ADM On-Prem Cloud Connector.



Après avoir configuré ADM On-Prem Cloud Connector et activé l'avis de sécurité, vous pouvez consulter la page d'avis de sécurité mise à jour.



En tant qu'administrateur, vous devez vous assurer de suivre toutes les nouvelles vulnérabilités et expositions courantes (CVE), d'évaluer l'impact des CVE, de comprendre les mesures correctives et de résoudre les vulnérabilités.

Fonctions d'avis de sécurité

Les fonctionnalités de conseil de sécurité suivantes vous aident à protéger votre infrastructure :

Fonctionnalités	Description
Analyse du système	Analyse toutes les instances gérées par défaut une fois par semaine. NetScaler ADM décide de la date et de l'heure des analyses du système et vous ne pouvez pas les modifier.

Fonctionnalités	Description
Scan à la demande	Vous pouvez scanner manuellement les instances si nécessaire. Si le temps écoulé depuis la dernière analyse du système est important, vous pouvez exécuter une analyse à la demande pour évaluer le niveau de sécurité actuel. Ou scannez après l'application d'une correction, pour évaluer la posture révisée.
Analyse d'impact CVE	Affiche les résultats de tous les CVE ayant un impact sur votre infrastructure et de toutes les instances NetScaler touchées et suggère des mesures correctives. Utilisez ces informations pour appliquer des mesures correctives afin de corriger les risques de sécurité.
Journal d'analyse	Stocke les copies des cinq derniers scans. Vous pouvez télécharger ces rapports aux formats CSV et PDF et les analyser.
Référentiel CVE	Fournit une vue détaillée de tous les CVE liés à NetScaler annoncés par Citrix depuis décembre 2019 et susceptibles d'avoir un impact sur votre infrastructure NetScaler. Vous pouvez utiliser cette vue pour comprendre les CVE dans le cadre des avis de sécurité et pour en savoir plus sur les CVE. Pour plus d'informations sur les CVE non pris en charge, consultez la section CVE non pris en charge dans l'avis de sécurité.

Points à noter

- L'avis de sécurité ne prend pas en charge les versions de NetScaler qui ont atteint la fin de vie (EOL). Nous vous recommandons de passer aux versions ou versions prises en charge par NetScaler.
- Instances prises en charge pour la détection CVE : toutes les instances NetScaler (SDX, MPX, VPX) et Gateway.
- CVE pris en charge : tous les CVE après décembre 2019.

> **Remarque :**
>
> La détection et la correction des vulnérabilités affectant le plug-in NetScaler Gateway pour Windows ne sont pas prises en charge par l'avis de sécurité de NetScaler ADM. Pour plus d'informations sur les CVE non pris en charge, consultez la section CVE non pris en charge dans l'avis de sécurité.

- L'avis de sécurité de NetScaler ADM ne tient compte d'aucun type de mauvaise configuration des fonctionnalités lors de l'identification de la vulnérabilité.
- L'avis de sécurité de NetScaler ADM prend uniquement en charge l'identification et la correction des CVE. Il ne prend pas en charge l'identification et la résolution des problèmes de sécurité mis en évidence dans l'article sur la sécurité.
- Portée de NetScaler, versions Gateway : cette fonctionnalité est limitée aux versions principales. L'avis de sécurité n'inclut aucune construction spéciale dans son champ d'application.
  - Les conseils de sécurité ne sont pas pris en charge dans la partition Admin.
- Les types de scan suivants sont disponibles pour les CVE :
  - **Analyse de version** : cette analyse nécessite que NetScaler ADM compare la version d'une instance NetScaler aux versions et aux versions sur lesquelles le correctif est disponible. Cette comparaison de versions aide l'avis de sécurité de NetScaler ADM à identifier si NetScaler est vulnérable au CVE. Par exemple, si un CVE est corrigé sur une version et une version xx.yy de NetScaler, l'avis de sécurité considère que toutes les instances de NetScaler situées sur des versions inférieures à xx.yy sont vulnérables. L'analyse de version est prise en charge aujourd'hui dans un avis de sécurité
  - **Analyse de configuration** : cette analyse nécessite que NetScaler ADM fasse correspondre un modèle spécifique à l'analyse CVE avec le fichier de configuration NetScaler (nsconf). Si le modèle de configuration spécifique est présent dans le fichier NetScaler ns.conf, l'instance est considérée comme vulnérable à ce CVE. Ce scan est généralement utilisé avec le scan de version.
    L'analyse de configuration est prise en charge aujourd'hui dans un avis de sécurité
  - **Analyse personnalisée** : cette analyse nécessite que NetScaler ADM se connecte à l'instance NetScaler gérée, lui envoie un script et l'exécute. La sortie du script aide NetScaler ADM à identifier si NetScaler est vulnérable au CVE. Les exemples incluent une sortie de commande shell spécifique, une sortie de commande CLI spécifique, certains journaux et l'existence ou le contenu de certains répertoires ou fichiers. Security Advisory utilise également des scans personnalisés pour détecter les correspondances entre plusieurs modèles de configuration, si le scan de configuration ne peut pas résoudre le problème. Pour les CVE qui nécessitent des analyses personnalisées, le script s'exécute à chaque fois que

votre analyse planifiée ou à la demande est exécutée. Pour en savoir plus sur les données collectées et les options pour des scans personnalisés spécifiques, consultez la documentation des conseils de sécurité relatifs à ce CVE.

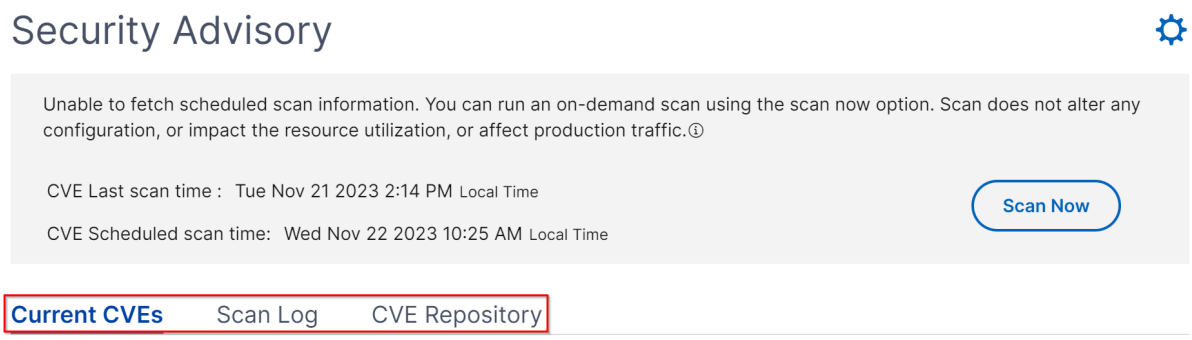
- Les scans n'ont aucune incidence sur le trafic de production sur NetScaler et ne modifient aucune configuration NetScaler sur NetScaler.
- L'avis de sécurité de NetScaler ADM ne prend pas en charge l'atténuation des CVE. Si vous avez appliqué une atténuation (solution temporaire) à l'instance NetScaler, ADM continuera à identifier NetScaler comme étant un NetScaler vulnérable jusqu'à ce que vous ayez terminé la correction.
- Pour les instances FIPS, le scan CVE n'est pas pris en charge.

Comment utiliser le tableau de bord des conseils de sécurité

Pour accéder au tableau de bord des **avis de sécurité**, à partir de l'interface graphique de NetScaler ADM, accédez à **Infrastructure > Instance Advisory > Security Advisory**.

Le tableau de bord comprend trois onglets :

- CVE actuels
- Journal d'analyse
- Référentiel CVE



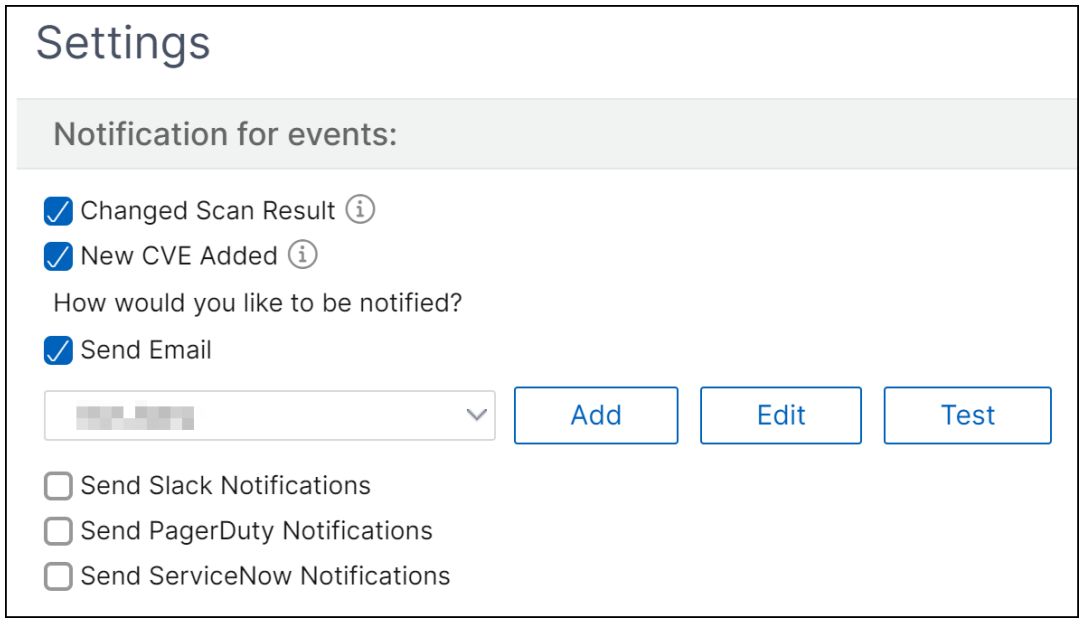
> **Important :**
>
> Dans l'interface graphique ou le rapport **Security Advisory**, tous les CVE peuvent ne pas apparaître, et vous ne voyez peut-être qu'un seul CVE. Pour contourner le problème, cliquez sur **Analyser maintenant** pour exécuter une analyse à la demande. Une fois l'analyse terminée, tous les CVE dans la portée (environ 15) apparaissent dans l'interface utilisateur ou le rapport.

Dans le coin supérieur droit du tableau de bord se trouve l'icône des paramètres, qui vous permet de :

- Activez et désactivez les notifications.

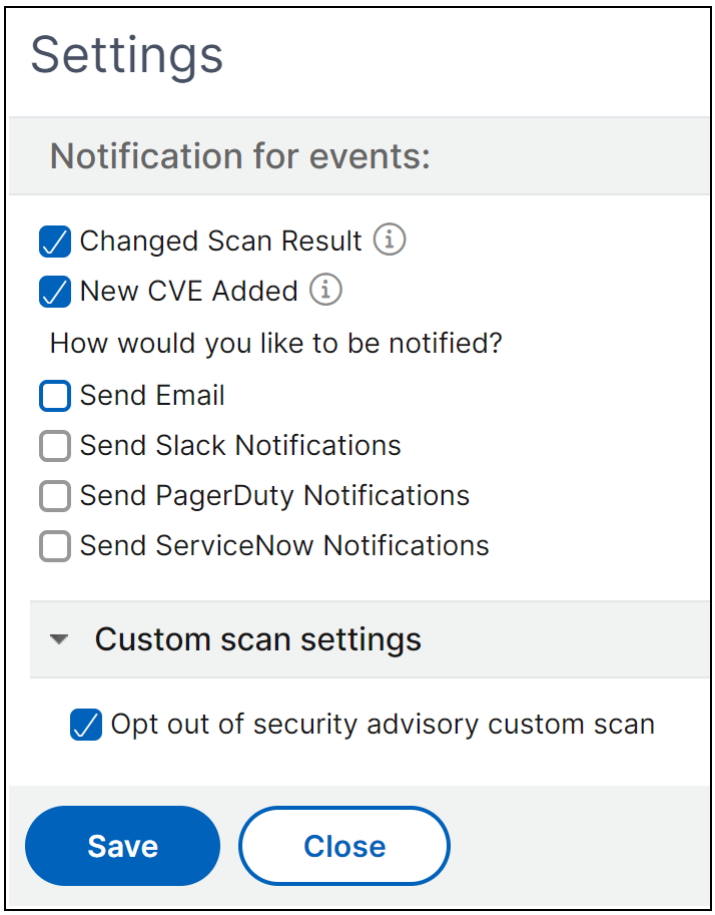
  Vous pouvez recevoir les notifications suivantes concernant l'impact du CV.

  - Notifications par e-mail, Slack, PagerDuty et ServiceNow concernant les modifications apportées aux résultats de l'analyse CVE et les nouveaux CVE ajoutés au référentiel CVE.
  - Notification dans le cloud pour les modifications apportées aux résultats de l'analyse d'impact CVE.



- Configuration des paramètres de numérisation personnalisés

  Vous pouvez cliquer sur la liste des **paramètres de numérisation personnalisés** pour afficher la case à cocher des paramètres supplémentaires. Vous avez la possibilité de cocher la case et de vous désinscrire de ces scans CVE Custom. L'impact des CVE nécessitant une analyse personnalisée ne sera pas évalué pour vos instances NetScaler dans l'avis de sécurité.



CVE actuels

Cet onglet indique le nombre de CVE ayant un impact sur vos instances ainsi que les instances affectées par les CVE. Les onglets ne sont pas séquentiels, et en tant qu'administrateur, vous pouvez basculer entre ces onglets en fonction de votre cas d'utilisation.

Le tableau indiquant le nombre de CVE ayant un impact sur les instances de NetScaler contient les informations suivantes.

ID CVE : ID du CVE impactant les instances.

Date de publication : date à laquelle le bulletin de sécurité a été publié pour ce CVE.

Scorede gravité : type de gravité (élevé/moyen/critique) et score. Pour voir le score, passez la souris sur le type de gravité.

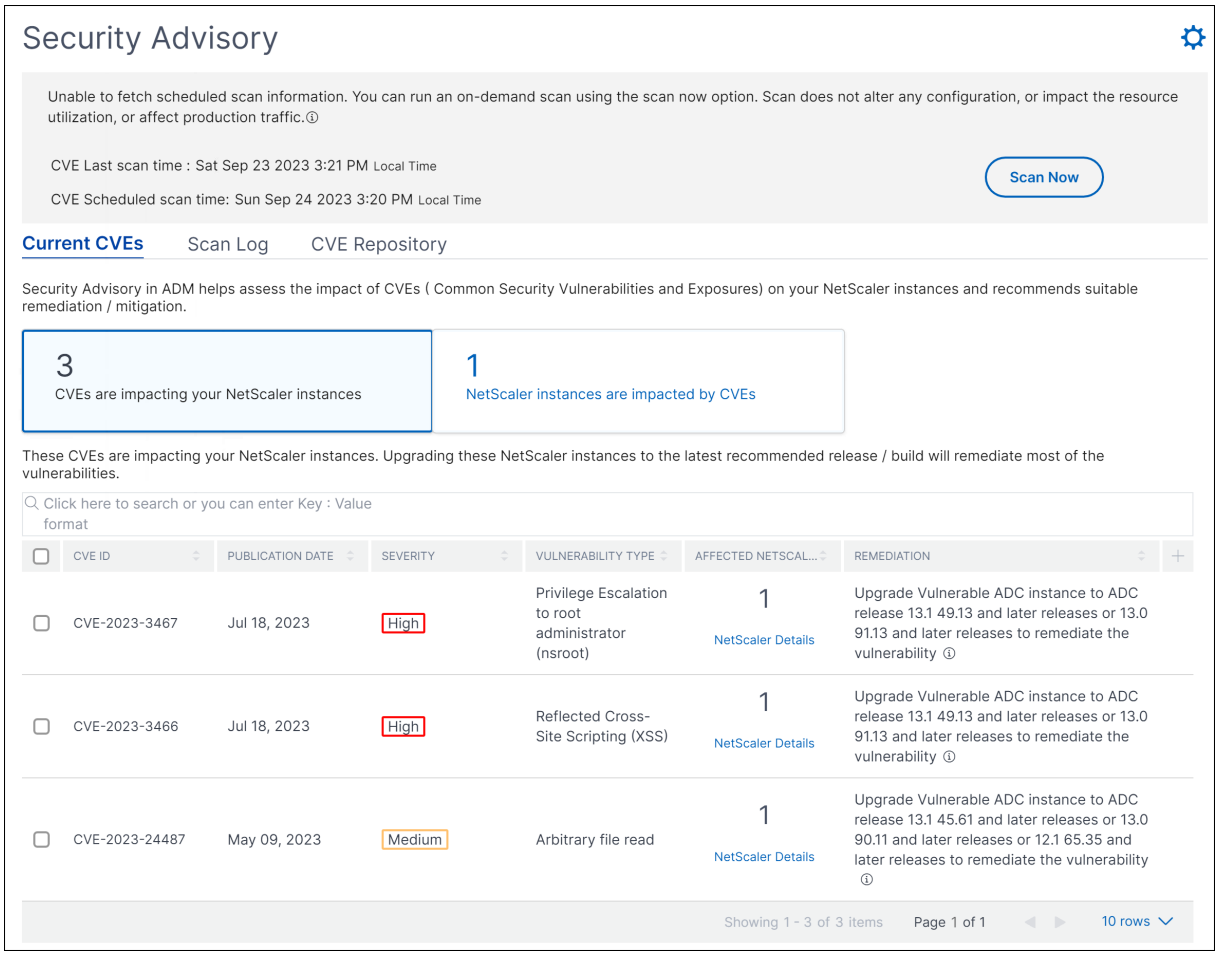
Type de vulnérabilité : type de vulnérabilité pour ce CVE.

Instances**NetScaler concernées** : nombre d'instances sur lesquelles l'ID CVE a un impact. Lorsque vous survolez, la liste des instances de NetScaler s'affiche.

Remédiation: les correctifs disponibles, qui consistent à mettre à niveau l'instance (généralement) ou à appliquer des packs de configuration.

La même instance peut être affectée par plusieurs CVE. Ce tableau vous aide à voir combien d'instances un CVE particulier ou plusieurs CVE sélectionnés ont un impact. **Pour vérifier l'adresse IP de l'instance concernée, passez le curseur sur NetScaler Details sous Instances NetScaler concernées.** Pour vérifier les détails de l'instance affectée, cliquez sur **Afficher les instances affectées** en bas du tableau.
Vous pouvez également ajouter ou supprimer des colonnes dans le tableau en cliquant sur le signe plus.

Dans cet écran, le nombre de CVE impactant vos instances est de 3 CVE et les instances concernées par ces CVE sont une.

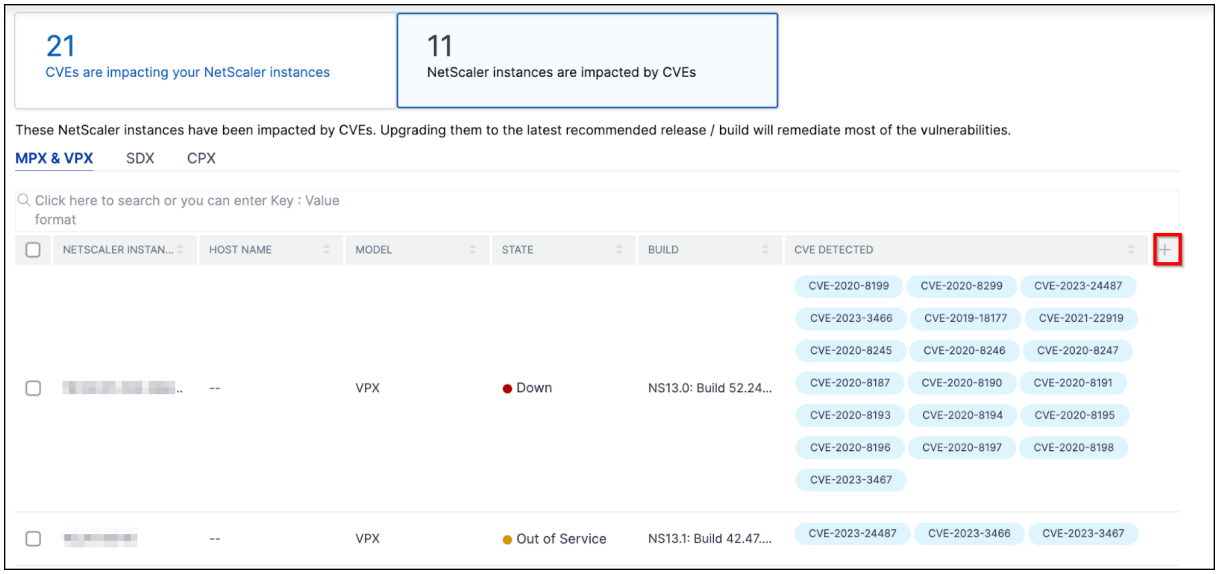


L'onglet « Les instances **<number of> NetScaler affectées par les CVE** » **affiche toutes les instances** NetScaler ADM NetScaler concernées. Le tableau présente les informations suivantes :

- Adresse IP NetScaler
- Nom d'hôte
- Numéro de modèle NetScaler

- État du NetScaler
- Version et build du logiciel
- Liste des CVE ayant un impact sur NetScaler.

Vous pouvez ajouter ou supprimer n'importe laquelle de ces colonnes selon vos besoins, en cliquant sur le signe +.



Pour résoudre le problème de vulnérabilité, sélectionnez l'instance NetScaler et appliquez la correction recommandée. La plupart des CVE ont besoin d'une mise à niveau en tant que mesure corrective, tandis que d'autres nécessitent une mise à niveau et une étape supplémentaire.

- Pour la correction du CVE-2020-8300, voir Corriger les vulnérabilités relatives à CVE-2020-8300.
- Pour CVE-2021-22927 et CVE-2021-22920, voir Corriger les vulnérabilités pour CVE-2021-22927 et CVE-2021-22920.
- Pour CVE CVE-2021-22956, voir Identification et correction des vulnérabilités relatives à CVE-2021-22956
- Pour CVE CVE-2022-27509, voir Corriger les vulnérabilités pour CVE-2022-27509

> **Remarque**
>
> Si vos instances NetScaler sont personnalisées, consultez la section Considérations relatives à la mise à niveau pour les configurations NetScaler personnalisées avant de planifier la mise à niveau de NetScaler .

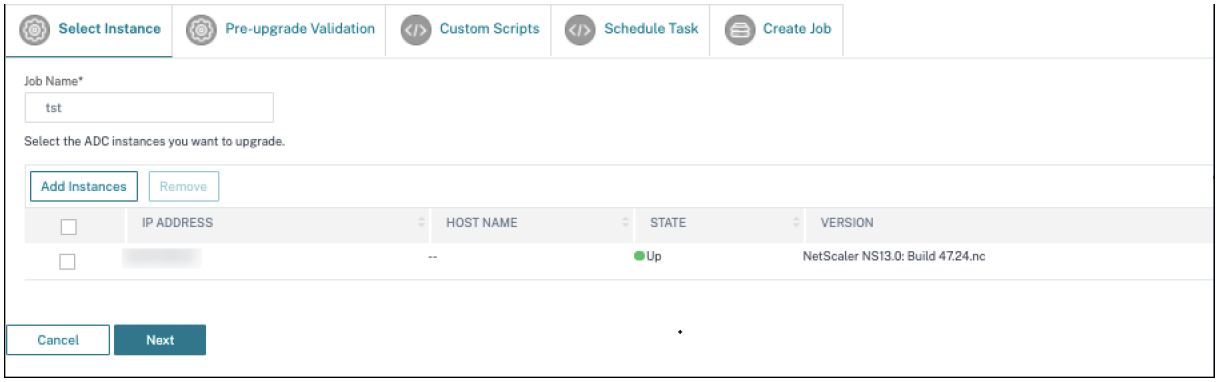
Mise à niveau : vous pouvez mettre à niveau les instances vulnérables de NetScaler vers une version et une version contenant le correctif. Ce détail peut être vu dans la colonne Correction. Pour mettre à niveau, sélectionnez l'instance, puis cliquez sur **Continuer à mettre à niveau le flux de travail**.

Dans le processus de mise à niveau, le NetScaler vulnérable est automatiquement renseigné en tant que NetScaler cible.

> **Remarque**
>
> Les versions 12.0, 11,0, 10.5 et inférieures sont déjà en fin de vie (EOL). Si vos instances NetScaler s'exécutent sur l'une de ces versions, effectuez une mise à niveau vers une version prise en charge.

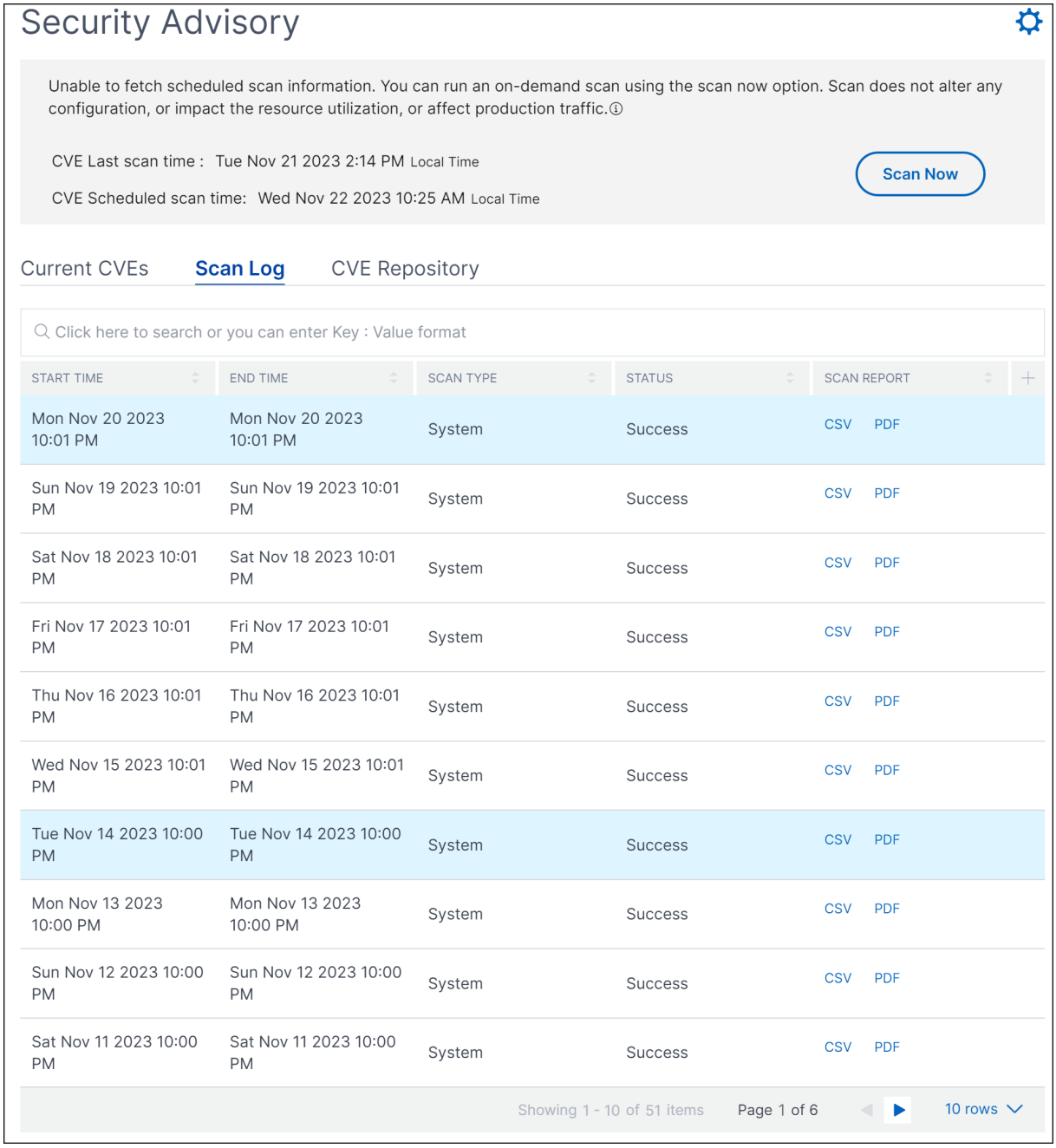
Le workflow de mise à niveau démarre. Pour plus d'informations sur l'utilisation de NetScaler ADM pour mettre à niveau des instances NetScaler, consultez la section Utiliser des tâches pour mettre à niveau des instances NetScaler.

> **Remarque**
>
> La version et la version vers laquelle vous souhaitez mettre à niveau sont à votre discrétion. Consultez les conseils figurant dans la colonne « Corrections » pour savoir quelles versions et quelles versions contiennent le correctif de sécurité. Et en conséquence, sélectionnez une version et une version prises en charge, qui n'ont pas encore atteint la fin de vie.



Journal d'analyse

L'onglet affiche les rapports des cinq dernières analyses CVE, qui incluent à la fois les analyses du système par défaut et les analyses à la demande initiées par l'utilisateur. Vous pouvez télécharger le rapport de chaque numérisation aux formats CSV et PDF. Si une analyse à la demande est en cours, vous pouvez également voir l'état d'achèvement.

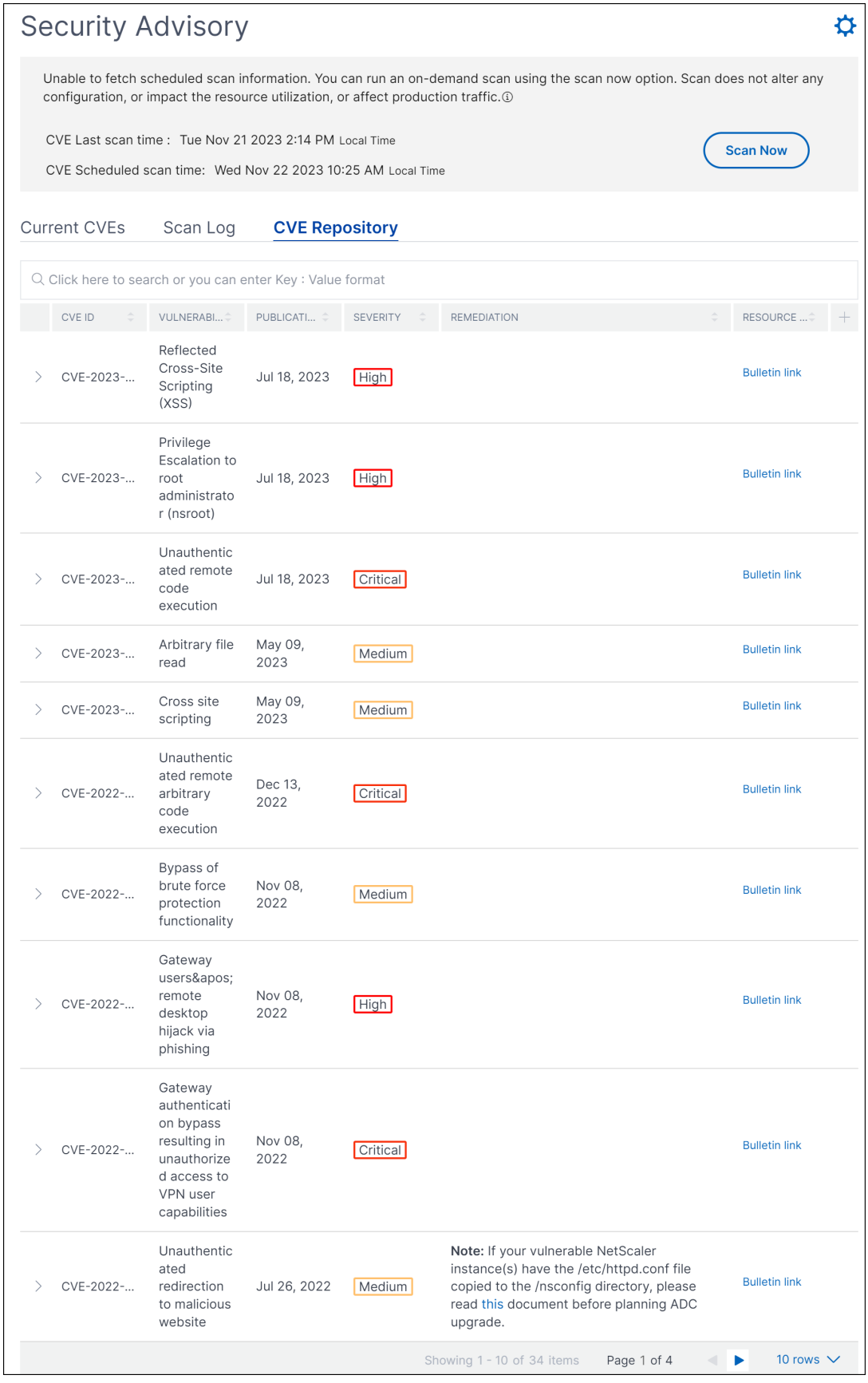


Référentiel CVE

Cet onglet inclut les dernières informations sur tous les CVE de décembre 2019, ainsi que les informations suivantes :

- Identifiants CVE
- Type de vulnérabilité
- Date de publication

- Niveau de gravité
- Correction
- Liens vers les bulletins de sécurité



Security Advisory

Unable to fetch scheduled scan information. You can run an on-demand scan using the scan now option. Scan does not alter any configuration, or impact the resource utilization, or affect production traffic.

CVE Last scan time : Tue Nov 21 2023 2:14 PM Local Time

CVE Scheduled scan time: Wed Nov 22 2023 10:25 AM Local Time

Scan Now

Current CVEs | Scan Log | CVE Repository

Click here to search or you can enter Key : Value format

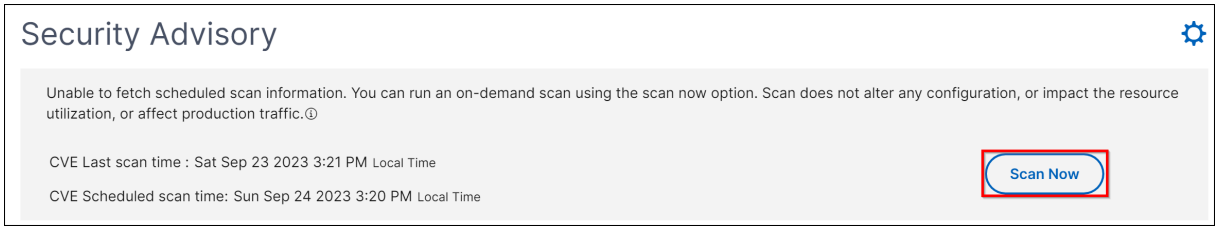
CVE ID	VULNERABI...	PUBLICATI...	SEVERITY	REMEDIATION	RESOURCE ...
CVE-2023-...	Reflected Cross-Site Scripting (XSS)	Jul 18, 2023	High		Bulletin link
CVE-2023-...	Privilege Escalation to root administrator (nsroot)	Jul 18, 2023	High		Bulletin link
CVE-2023-...	Unauthenticated remote code execution	Jul 18, 2023	Critical		Bulletin link
CVE-2023-...	Arbitrary file read	May 09, 2023	Medium		Bulletin link
CVE-2023-...	Cross site scripting	May 09, 2023	Medium		Bulletin link
CVE-2022-...	Unauthenticated remote arbitrary code execution	Dec 13, 2022	Critical		Bulletin link
CVE-2022-...	Bypass of brute force protection functionality	Nov 08, 2022	Medium		Bulletin link
CVE-2022-...	Gateway users' remote desktop hijack via phishing	Nov 08, 2022	High		Bulletin link
CVE-2022-...	Gateway authentication bypass resulting in unauthorized access to VPN user capabilities	Nov 08, 2022	Critical		Bulletin link
CVE-2022-...	Unauthenticated redirection to malicious website	Jul 26, 2022	Medium	**Note:** If your vulnerable NetScaler instance(s) have the /etc/httpd.conf file copied to the /nsconfig directory, please read this document before planning ADC upgrade.	Bulletin link

Showing 1 - 10 of 34 items Page 1 of 4 10 rows

Scanner maintenant

Vous pouvez scanner les instances à tout moment, selon vos besoins.

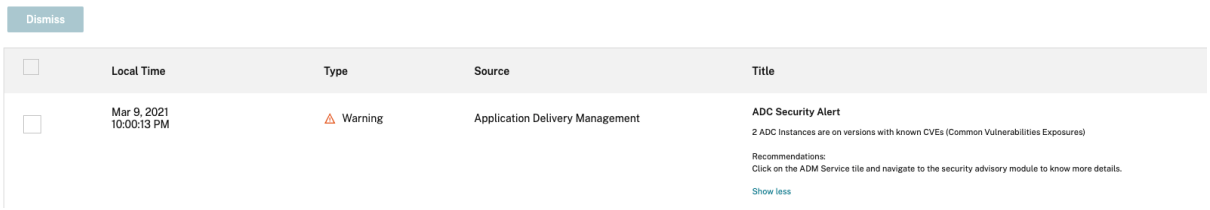
Cliquez sur **Analyser maintenant** pour rechercher les CVE qui ont un impact sur vos instances NetScaler. Une fois l'analyse terminée, les informations de sécurité révisées apparaissent dans l'interface graphique de l'avis de sécurité.



NetScaler ADM met quelques minutes à terminer l'analyse.

Notification

En tant qu'administrateur, vous recevez des notifications Citrix Cloud, qui indiquent le nombre d'instances NetScaler vulnérables aux CVE. Pour voir les notifications, cliquez sur l'icône en forme de cloche dans le coin supérieur droit de l'interface graphique de NetScaler ADM.



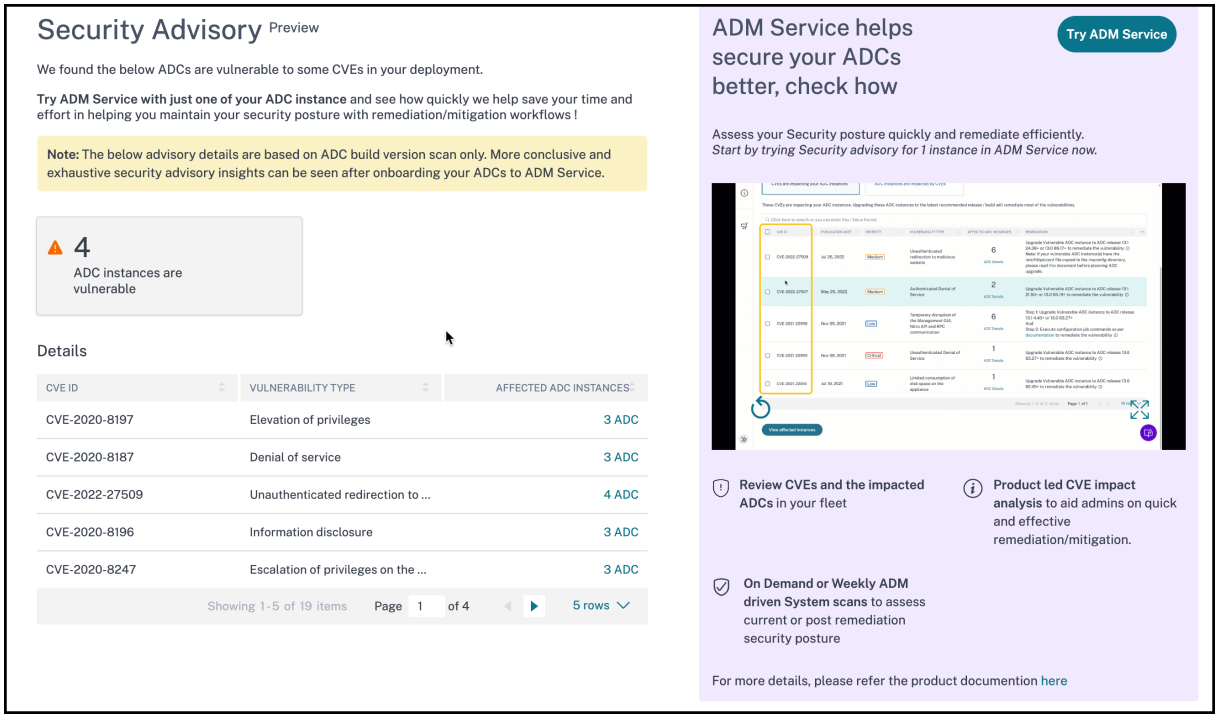
Avis de sécurité dans les versions 14.1 4.x ou antérieures

Si vous utilisez les versions précédentes, vous ne pouvez utiliser que la version préliminaire de la fonctionnalité d'avis de sécurité. La version préliminaire met uniquement en évidence les CVE NetScaler et les instances ADC intégrées au service ADM qui sont à risque. Si vous souhaitez utiliser la version complète de la fonctionnalité d'avis de sécurité, vous devez activer ADM On-Prem Cloud Connector.

> **IMPORTANT**
>
> **Pour une analyse détaillée de l'impact de la CVE, des informations concluantes sur les scans personnalisés/les scans du système, les workflows de correction et d'atténuation, essayez NetScaler ADM Service.**

Afficher l'avis de sécurité

Pour accéder à **Security Advisory**, accédez à **Infrastructure > Instance Advisory > Security Advisory**. Vous pouvez consulter l'état de vulnérabilité de toutes les instances ADC que vous gérez via NetScaler ADM.



L'avis de sécurité local de NetScaler ADM effectue uniquement une analyse de la version ADC pour vérifier la présence de CVE et les informations suivantes s'affichent.

- **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.

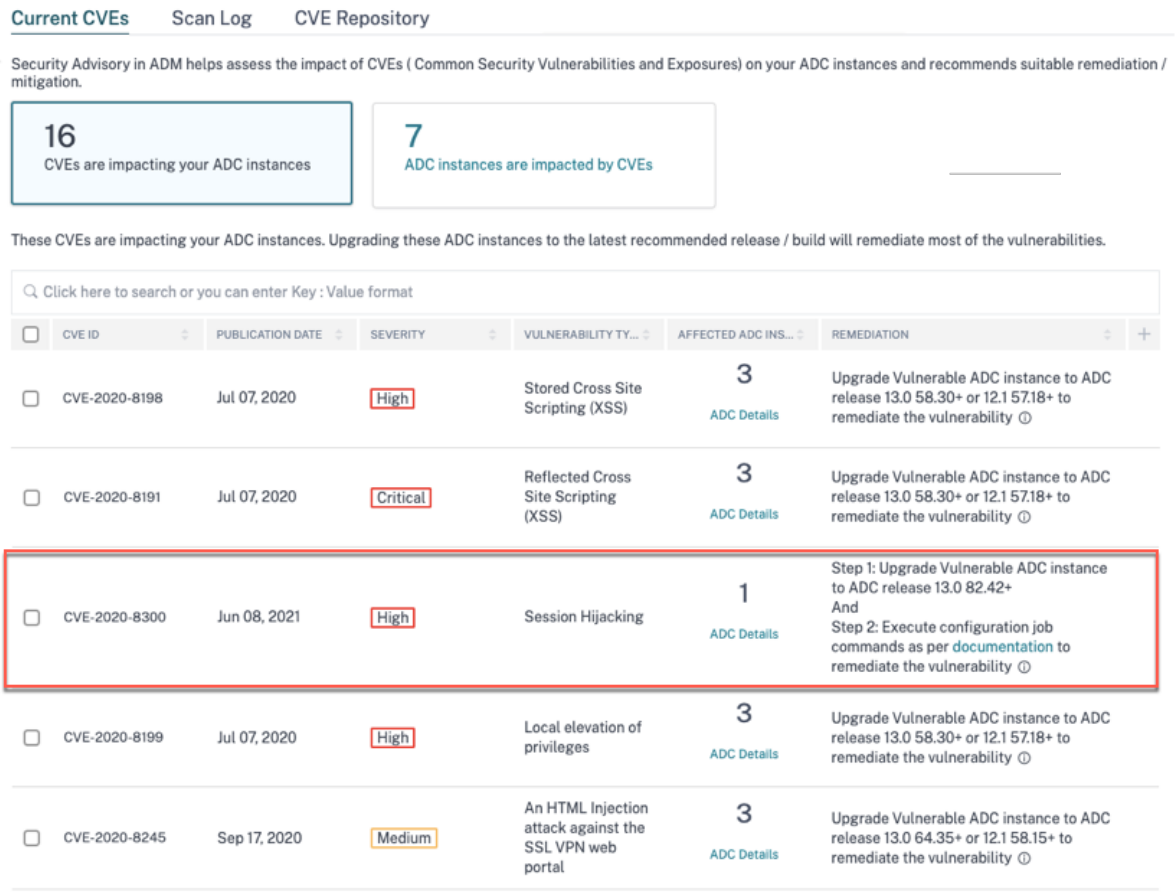
L'avis de sécurité local de NetScaler ADM vous permet également de sélectionner l'une des instances ADC et d'intégrer l'instance ADC au service ADM. Cliquez sur **Try ADM Service** et intégrez l'instance ADC au service ADM. ADM Service Security Advisory vous permet de vérifier le type de vulnérabilité d'un CVE en particulier et d'obtenir des informations sur les mesures d'atténuation et de correction nécessaires pour résoudre la vulnérabilité.

Pour plus d'informations sur l'avis de sécurité du service ADM, visionnez l'animation GIF sur la page **Avis de sécurité** .

Corriger les vulnérabilités de CVE-2020-8300

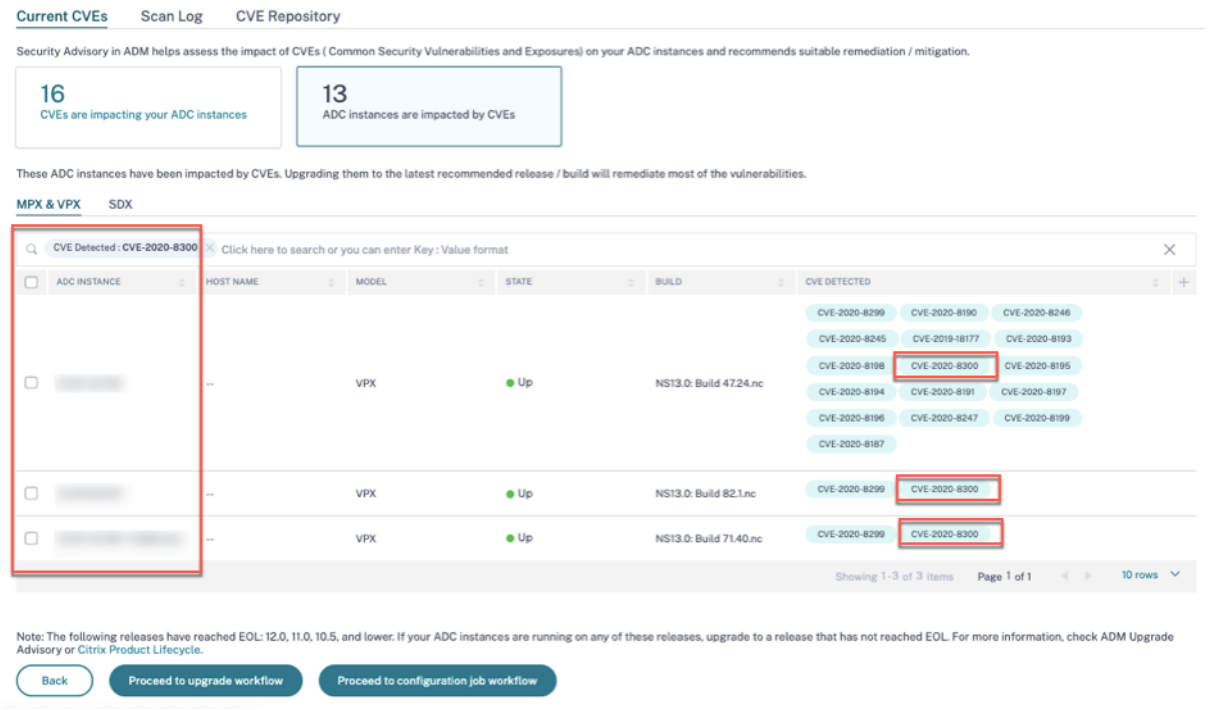
February 1, 2024

Dans le tableau de bord des conseils de sécurité de NetScaler ADM, sous **Current CVE > Les instances <number of> ADC sont affectées par les CVE**, vous pouvez voir toutes les instances vulnérables en raison de cette CVE spécifique. Pour vérifier les détails des instances concernées par CVE-2020-8300, sélectionnez **CVE-2020-8300** et cliquez sur **Afficher les instances affectées**.



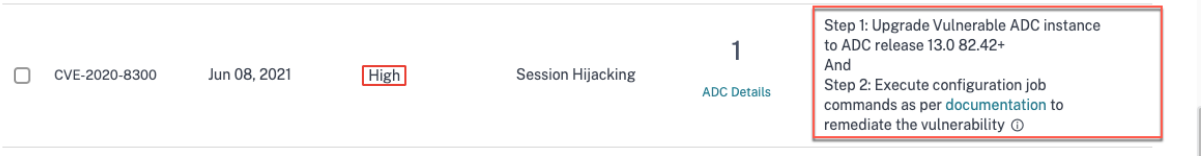
> **Remarque**
>
> Pour plus d'informations sur le tableau de bord des avis de sécurité, voir Avis de sécurité.

La fenêtre **<number of> Instances ADC impactées par les CVE** s'affiche. Vous trouverez ici le nombre et les détails des instances ADC impactées par la CVE-2020-8300.



Corriger CVE-2020-8300

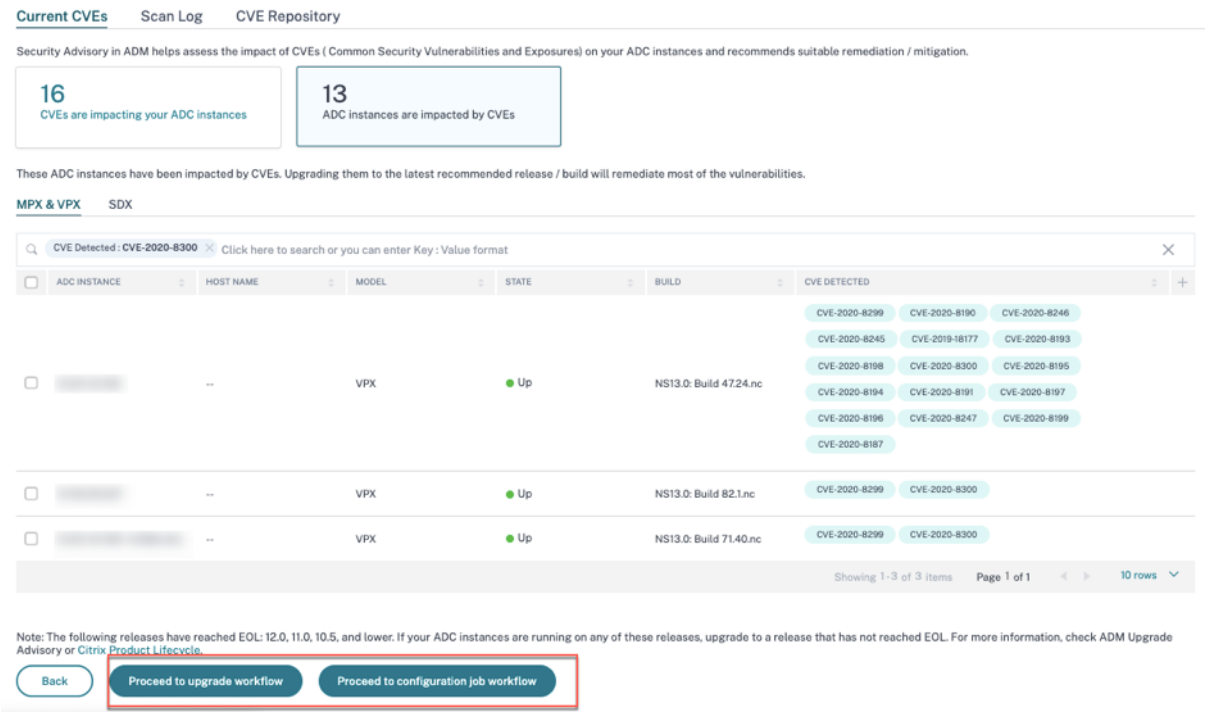
Pour les instances ADC impactées par CVE-2020-8300, la correction se fait en deux étapes. Dans l'interface graphique, sous CVE **actuels > Les instances ADC sont affectées par** les CVE , vous pouvez voir les étapes 1 et 2.



Les deux étapes sont les suivantes :

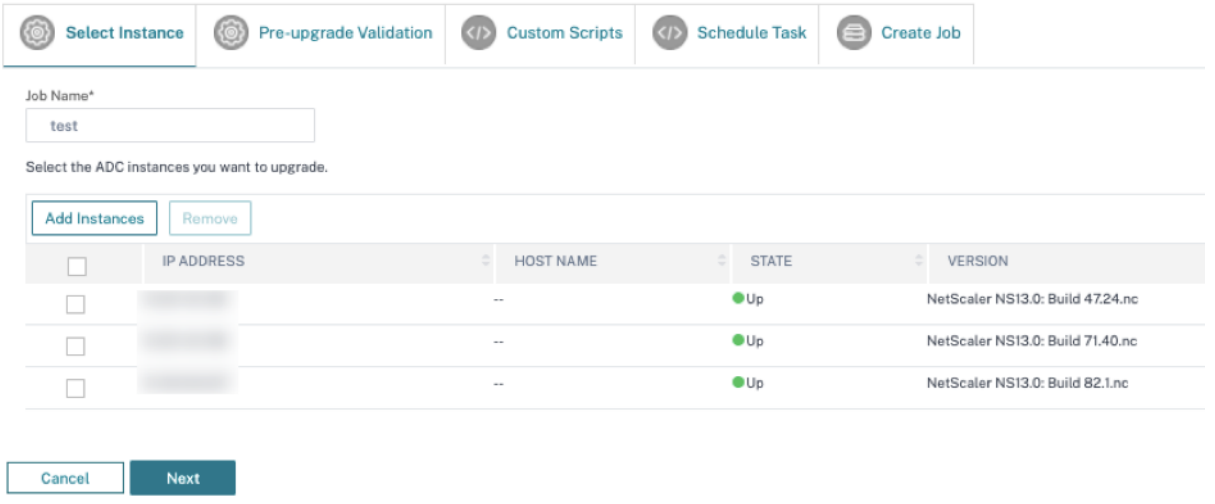
1. Mise à niveau des instances ADC vulnérables vers une version et une version contenant le correctif.
2. Appliquer les commandes de configuration requises à l'aide du modèle de configuration intégré personnalisable dans les tâches de configuration. Suivez cette étape pour chaque ADC vulnérable un par un et incluez toutes les actions SAML et les profils SAML pour cet ADC.

SousCVE actuels > Instances ADC affectées par les CVE**, vous pouvez voir deux flux de travail distincts pour ce processus de correction en deux étapes : Procéder à la mise à niveau du flux de**travail et Passer au flux**de travail de configuration.**



Étape 1 : Mettre à niveau les instances ADC vulnérables

Pour mettre à niveau les instances vulnérables, sélectionnez les instances et cliquez sur **Procéder au flux de travail de mise à niveau**. Le flux de travail de mise à niveau s'ouvre avec les instances ADC vulnérables déjà renseignées.



Pour plus d'informations sur l'utilisation de NetScaler ADM pour mettre à niveau des instances ADC, consultez Créer unetâche de mise à niveau ADC.

> **Remarque**
>
> Cette étape peut être effectuée en une seule fois pour toutes les instances ADC vulnérables.

Étape 2 : Appliquer les commandes de configuration

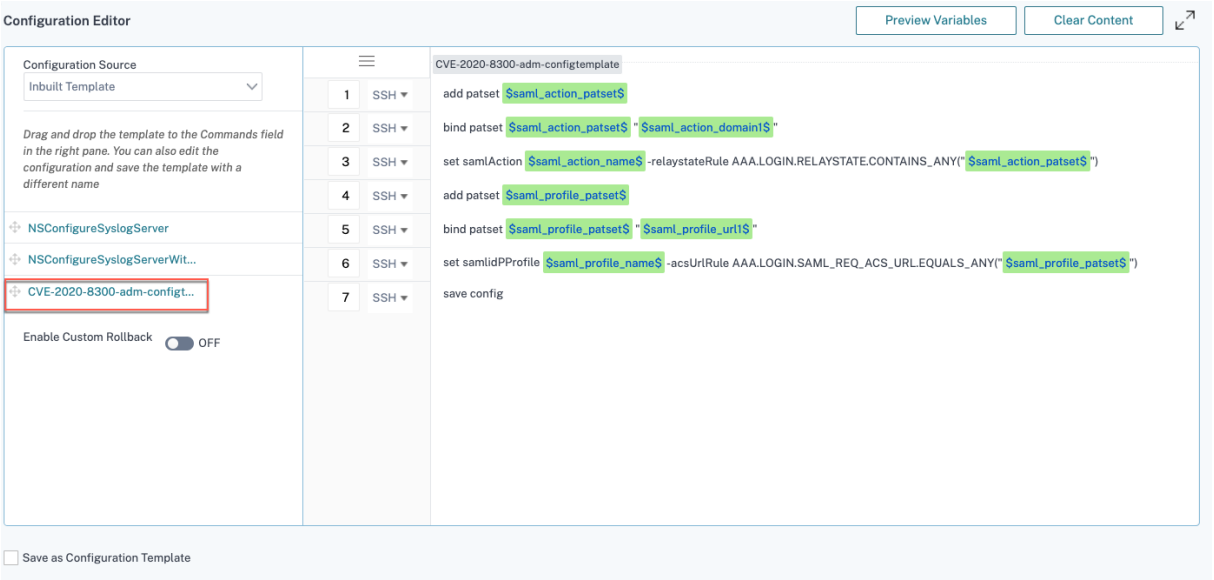
Après avoir mis à niveau les instances concernées, dans la fenêtre **<number of> Instances ADC affectées par les CVE**, sélectionnez une instance affectée par CVE-2020-8300 et cliquez sur **Procéder au flux de travail de configuration**. Le flux de travail inclut les étapes suivantes.

1. Personnalisation de la configuration.
2. Examen des instances impactées renseignées automatiquement.
3. Spécification des entrées pour les variables de la tâche.
4. Révision de la configuration finale avec les entrées variables renseignées.
5. Exécuter le travail.

Gardez les points suivants à l'esprit avant de sélectionner une instance et de cliquer sur **Procéder au flux de travail de configuration** :

- Pour une instance ADC affectée par plusieurs CVE (tels que CVE-2020-8300, CVE-2021-22927, CVE-2021-22920 et CVE-2021-22956) : lorsque vous sélectionnez l'instance et que vous cliquez sur **Procéder au flux de travail de la tâche de configuration**, le modèle de configuration intégré ne se remplit pas automatiquement sous Sélectionner la configuration. Glissez et déposez manuellement le modèle de tâche de configuration approprié sous **Modèle d'avis de sécurité** dans le volet des tâches de configuration sur le côté droit.
- Pour plusieurs instances ADC impactées par CVE-2021-22956 uniquement : vous pouvez exécuter des tâches de configuration sur toutes les instances en même temps. Par exemple, vous avez l'ADC 1, l'ADC 2 et l'ADC 3, et tous sont affectés uniquement par CVE-2021-22956. Sélectionnez toutes ces instances et cliquez sur **Procéder au flux de travail de configuration**. Le modèle de configuration intégré s'affiche automatiquement sous **Sélectionner la configuration**.
- Pour plusieurs instances ADC impactées par CVE-2021-22956 et un ou plusieurs autres CVE (telles que CVE-2020-8300, CVE-2021-22927 et CVE-2021-22920), qui nécessitent une correction à appliquer à chaque ADC à la fois : lorsque vous sélectionnez ces instances et que vous cliquez sur **Procéder au flux de travail de tâche de configuration**, une erreur se produit Un message apparaît vous demandant d'exécuter la tâche de configuration sur chaque ADC à la fois.

Étape 1 : Sélection de la configuration Dans le flux de travail de la tâche de configuration, le modèle de configuration intégré est automatiquement renseigné sous **Sélectionner la configuration**.



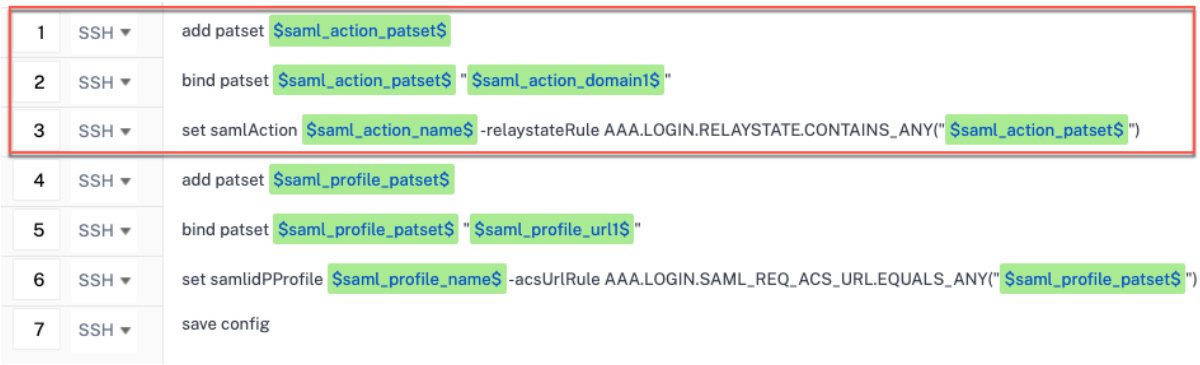
Exécutez une tâche de configuration distincte pour chaque instance ADC affectée, une par une, et incluez toutes les actions SAML et les profils SAML pour cet ADC. Par exemple, si vous avez deux instances ADC vulnérables ayant chacune deux actions SAML et deux profils SAML, vous devez exécuter cette tâche de configuration deux fois. Une fois par ADC couvrant toutes ses actions SAML et tous ses profils SAML.

ADC 1	ADC2
Tâche 1 : deux actions SAML+deux profils SAML	Tâche 2 : deux actions SAML+deux profils SAML

Donnez un nom à la tâche et personnalisez le modèle selon les spécifications suivantes. Le modèle de configuration intégré n'est qu'un modèle de plan ou de base. Personnalisez le modèle en fonction de votre déploiement pour répondre aux exigences suivantes :

a. **Actions SAML et domaines associés**

En fonction du nombre d'actions SAML que vous avez dans votre déploiement, vous devez répliquer les lignes 1 à 3 et personnaliser les domaines pour chaque action SAML.

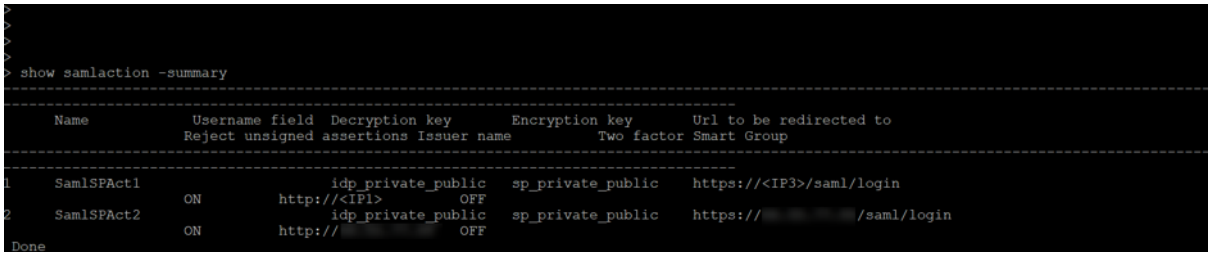


Par exemple, si vous avez deux actions SAML, répétez les lignes 1 à 3 deux fois et personnalisez en conséquence les définitions de variables pour chaque action SAML.

Et si vous avez N domaines pour une action SAML, vous devez saisir manuellement la ligne `bind patset $saml_action_patset$ "$saml_action_domain1$"` plusieurs fois pour vous assurer que la ligne apparaît N fois pour cette action SAML. Et modifiez les noms des définitions de variables suivants :

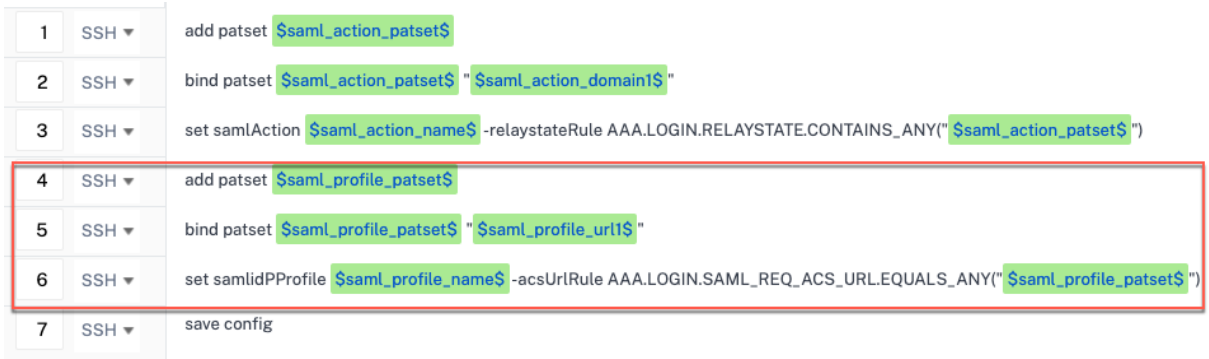
- `saml_action_patset`: est la variable du modèle de configuration et représente la valeur du nom du jeu de modèles (patset) pour l'action SAML. Vous pouvez spécifier la valeur réelle à l'étape 3 du flux de travail de configuration. Consultez la section Étape 3 : Spécifier les valeurs des variables dans ce document.
- `saml_action_domain1`: est la variable du modèle de configuration, qui représente le nom de domaine pour cette action SAML spécifique. Vous pouvez spécifier la valeur réelle à l'étape 3 du flux de travail de configuration. Consultez la section Étape 3 : Spécifier les valeurs des variables dans ce document.

Pour rechercher toutes les actions SAML d'un appareil, exécutez la commande `show samlaction` .



b. **Les profils SAML et leurs URL associées**

En fonction du nombre de profils SAML que vous avez dans votre déploiement, répliquez les lignes 4 à 6. Personnalisez les URL de chaque profil SAML.



Par exemple, si vous avez deux profils SAML, entrez manuellement les lignes 4 à 6 deux fois et personnalisez en conséquence les définitions de variables pour chaque action SAML.

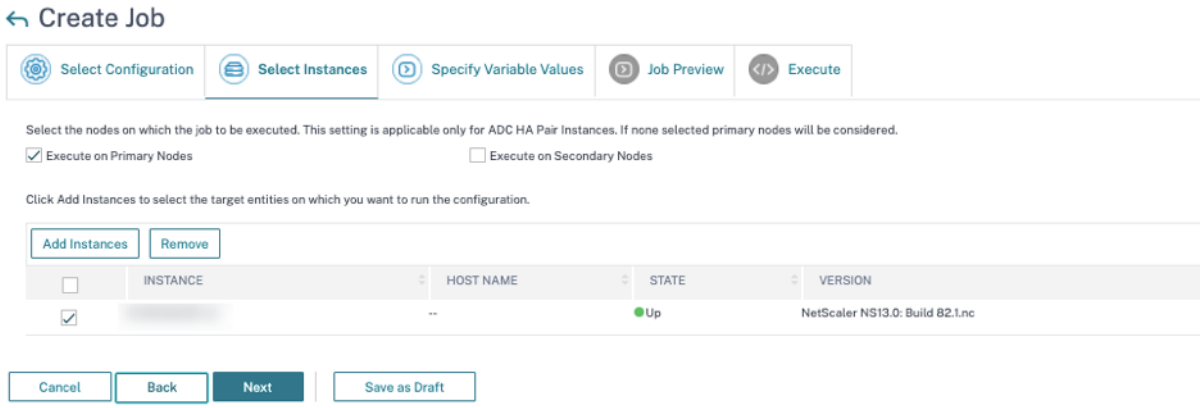
Et si vous avez N domaines pour une action SAML, vous devez saisir manuellement la ligne `bind patset $saml_profile_patset$ "$saml_profile_url1$"` plusieurs fois pour vous assurer que la ligne apparaît N fois pour ce profil SAML. Et modifiez les noms des définitions de variables suivants :

- `saml_profile_patset`: est la variable du modèle de configuration, et elle représente la valeur du nom du jeu de modèles (patset) pour le profil SAML. Vous pouvez spécifier la valeur réelle à l'étape 3 du flux de travail de configuration. Voir la section Étape 3 : Spécifier les valeurs des variables dans ce document.
- `saml_profile_url1`: est la variable du modèle de configuration, qui représente le nom de domaine pour ce profil SAML spécifique. Vous pouvez spécifier la valeur réelle à l'étape 3 du flux de travail de configuration. Voir la section Étape 3 : Spécifier les valeurs des variables dans ce document.

Pour rechercher tous les profils SAM d'un appareil, exécutez la commande `show samlidpProfile` .

Étape 2 : Sélectionnez l'instance

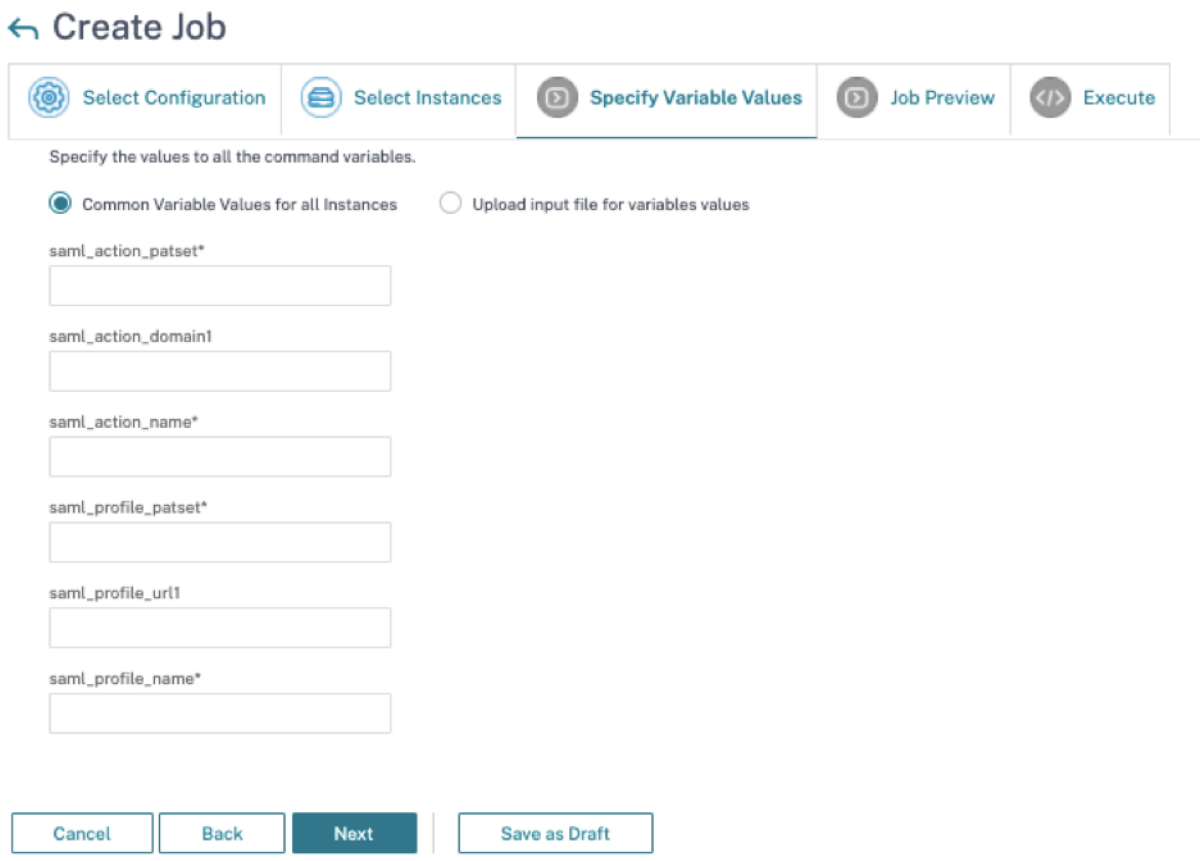
L'instance affectée est automatiquement renseignée sous **Select Instances**. Sélectionnez l'instance et cliquez sur **Suivant**.



Étape 3 : Spécifier les valeurs des variables Entrez les valeurs des variables.

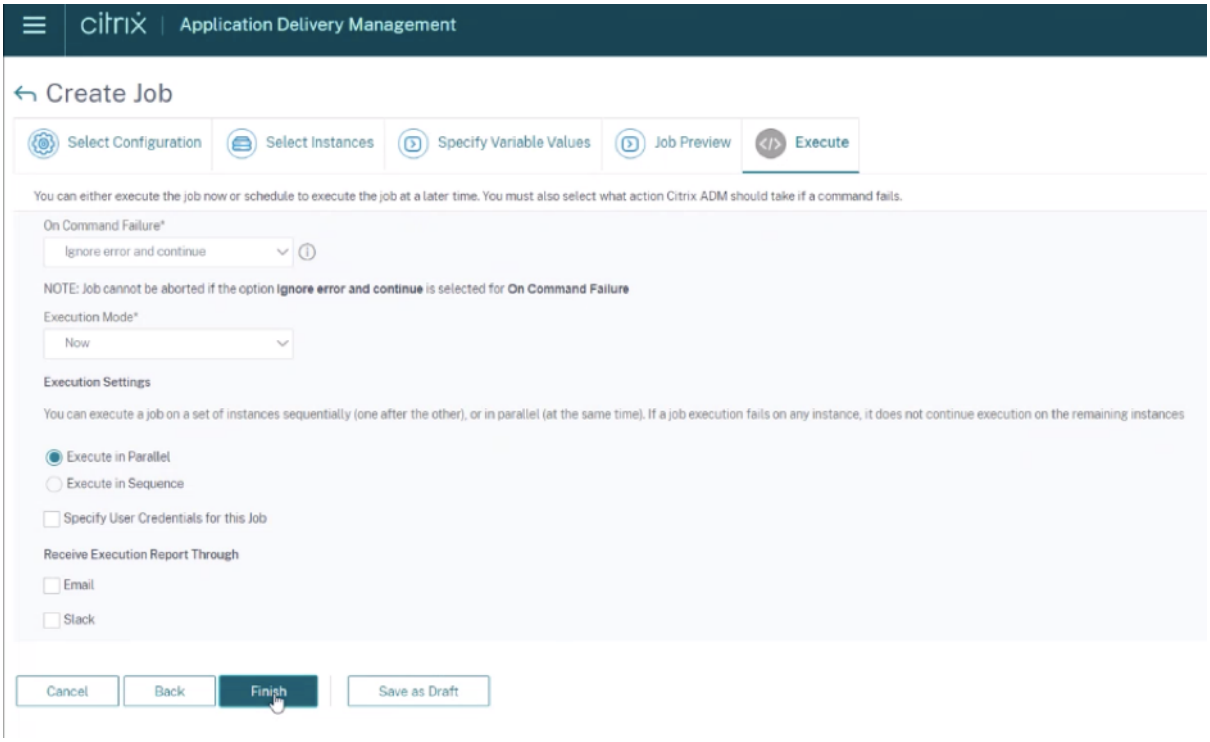
- `saml_action_patset`: ajoute un nom pour l'action SAML
- `saml_action_domain1`: entrez un domaine au format `https://<example1.com>/`
- `saml_action_name`: entrez la même action SAML pour laquelle vous configurez la tâche
- `saml_profile_patset`: ajouter un nom pour le profil SAML
- `saml_profile_url1`: entrez l'URL dans ce format `https://<example2.com>/cgi/samlauth`
- `saml_profile_name`: entrez le même profil SAML pour lequel vous configurez la tâche

> **Remarque**
>
> Pour les URL, l'extension n'est pas toujours `cgi/samlauth`. Cela dépend de l'autorisation tierce dont vous disposez et, en conséquence, vous devez mettre l'extension.



Étape 4 : Prévisualiser la configuration Prévisualise les valeurs des variables qui ont été insérées dans la configuration et cliquez sur **Suivant**.

Étape 5 : Exécuter la tâche Cliquez sur **Terminer** pour exécuter la tâche de configuration.



Une fois la tâche exécutée, elle apparaît sous **Infrastructure > Configuration > Tâches de configuration**.

Après avoir effectué les deux étapes de correction pour tous les ADC vulnérables, vous pouvez exécuter une analyse à la demande pour voir la nouvelle posture de sécurité.

Points à noter concernant le compte NetScaler ADM Express

Le compte NetScaler ADM Express possède des fonctionnalités limitées, notamment la limitation de deux tâches de configuration uniquement.

Pour la correction du CVE-2020-8300, vous devez exécuter autant de tâches de configuration que le nombre de vos instances ADC vulnérables. Par conséquent, si vous avez un compte Express et que vous devez exécuter plus de deux tâches de configuration, suivez cette solution de contournement.

Solution : exécutez deux tâches de configuration pour deux instances ADC vulnérables, puis supprimez les deux tâches pour continuer à exécuter les deux tâches suivantes pour les deux instances ADC vulnérables suivantes. Continuez ainsi jusqu'à ce que vous ayez couvert toutes les instances vulnérables. Avant de supprimer les tâches, vous pouvez télécharger le rapport pour référence ultérieure. Pour télécharger le rapport, sous **Réseau > Tâches**, sélectionnez les tâches et cliquez sur **Télécharger** sous **Actions**.

Exemple : Si vous avez six instances ADC vulnérables, exécutez deux tâches de configuration sur deux instances vulnérables respectivement, puis supprimez les deux tâches de configuration. Répétez cette

étape deux fois de plus. À la fin, vous auriez exécuté six tâches de configuration pour six instances ADC respectivement. Dans l'interface utilisateur de NetScaler ADM, sous **Infrastructure > Tâches, vous ne voyez que les deux dernières tâches**de configuration.

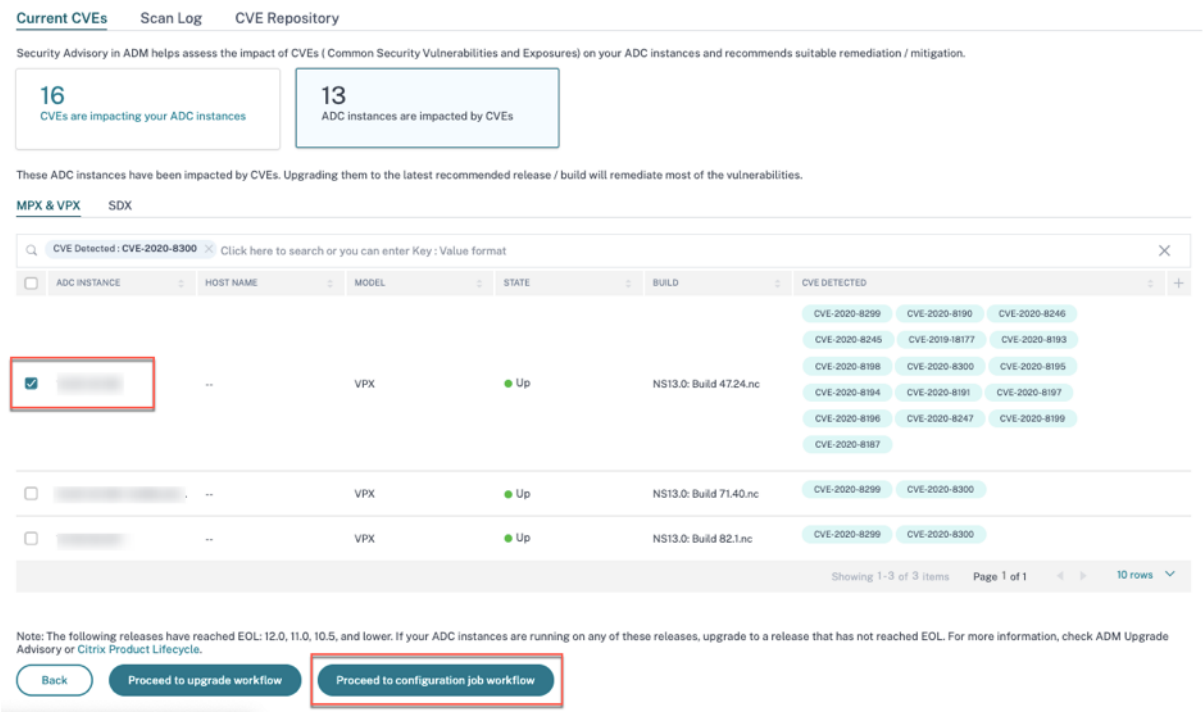
Scénario

Dans ce scénario, trois instances ADC sont vulnérables au CVE-2020-8300 et vous devez corriger toutes les instances. Procédez comme suit :

1. Mettez à niveau les trois instances ADC en suivant les étapes indiquées dans la section **Mettre à niveau une instance** de ce document.
2. Appliquez le correctif de configuration à un ADC à la fois, en utilisant le flux de travail de configuration. Consultez les étapes indiquées dans la section **Appliquer les commandes de configuration** de ce document.

L'ADC 1 vulnérable possède la configuration suivante :

Deux actions SAML	Deux profils SAML
L'action SAML 1 possède un domaine et l'action SAML 2 possède deux domaines	Le profil SAML 1 possède une URL et le profil SAML 2 possède deux URL



Sélectionnez ADC 1 et cliquez sur **Procéder au flux de travail de configuration**. Le modèle intégré se remplit automatiquement. Ensuite, donnez un nom de tâche et personnalisez le modèle en fonction de la configuration donnée.

Les tableaux suivants répertorient les définitions de variables pour les paramètres personnalisés.

Tableau 1 Définitions de variables pour l'action SAML

Configuration de l'ADC	Définition de variable pour patset	Définition de variable pour le nom de l'action SAML	Définition de variable pour le domaine
L'action SAML 1 possède un domaine	saml_action_patset1	saml_action_name1	saml_action_domain1
L'action SAML 2 comporte deux domaines	saml_action_patset2	saml_action_name2	saml_action_domain2, saml_action_domain3

Tableau 2. Définitions de variables pour le profil SAML

Configuration de l'ADC	Définition de variable pour patset	Définition de variable pour le nom de profil SAML	Définition de variable pour l'URL
Le profil SAML 1 possède une URL	saml_profile_patset1	saml_profile_nom1	saml_profile_url1
Le profil SAML 2 possède deux URL	saml_profile_patset2	saml_profile_nom2	saml_profile_url2, saml_profile_url3

Sous **Select Instances**, sélectionnez ADC 1 et cliquez sur **Next**. La fenêtre **Spécifier les valeurs des variables** s'affiche. Au cours de cette étape, vous devez fournir des valeurs pour toutes les variables définies à l'étape précédente.

Ensuite, passez en revue les variables.

Cliquez sur **Suivant**, puis sur **Terminer** pour exécuter la tâche.

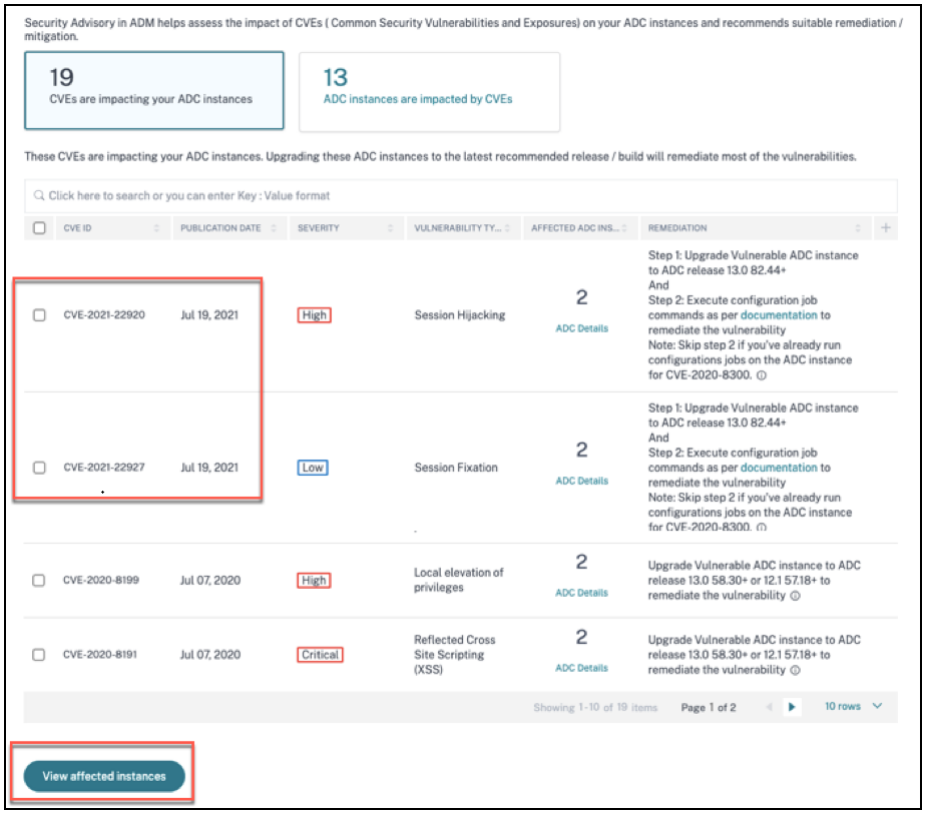
Une fois la tâche exécutée, elle apparaît sous **Infrastructure > Configuration > Tâches de configuration**.

Après avoir terminé les deux étapes de correction pour l'ADC1, suivez les mêmes étapes pour corriger l'ADC 2 et l'ADC 3. Une fois la correction terminée, vous pouvez exécuter une analyse à la demande pour voir la nouvelle posture de sécurité.

Corrigez les vulnérabilités des systèmes CVE-2021-22927 et CVE-2021-22920

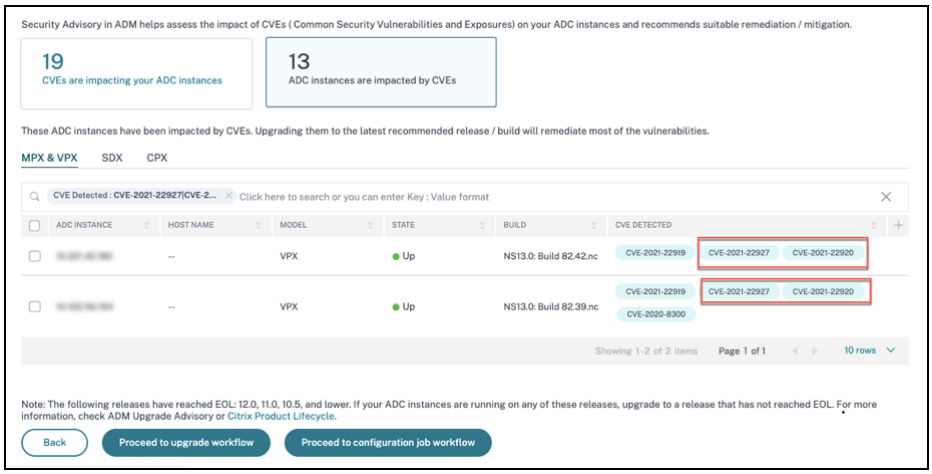
February 1, 2024

Dans le tableau de bord des avis de sécurité de NetScaler ADM, sous **CVE actuels > Les instances < `number of`> ADC sont affectées par les CVE, vous pouvez voir toutes les instances**vulnérables en raison des CVE-2021-22927 et CVE-2021-22920. Pour vérifier les détails des instances impactées par ces deux CVE, sélectionnez un ou plusieurs CVE et cliquez sur **Afficher les instances affectées**.



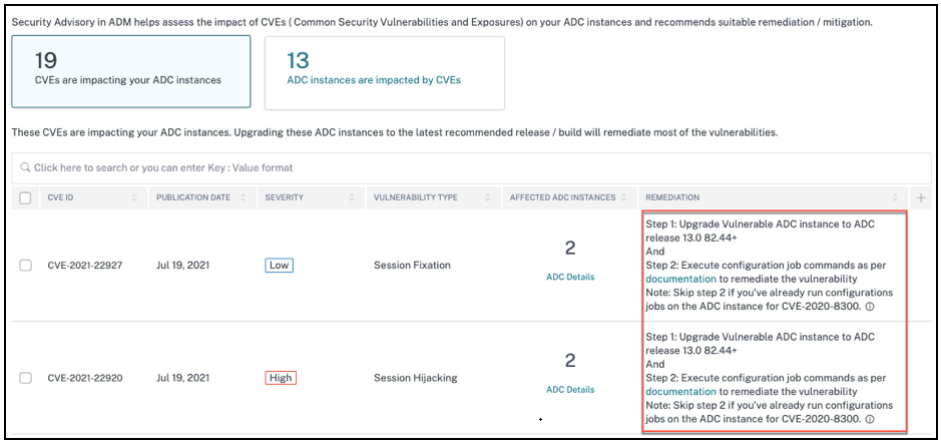
> **Remarque**
>
> L'analyse du système d'avis de sécurité peut prendre quelques heures pour se terminer et refléter l'impact des CVE-2021-22927 et CVE-2021-22920 sur le module d'avis de sécurité. Pour voir l'impact plus rapidement, lancez une analyse à la demande en cliquant sur **Scanner maintenant**.
>
> Pour plus d'informations sur le tableau de bord des avis de sécurité, voir Avis de sécurité.

La fenêtre **<number of> Instances ADC impactées par les CVE** s'affiche. Dans la capture d'écran suivante, vous pouvez voir le nombre et les détails des instances ADC affectées par CVE-2021-22927 et CVE-2021-22920.



Corrigez CVE-2021-22927 et CVE-2021-22920

Pour les instances ADC affectées par CVE-2021-22927 et CVE-2021-22920, la correction se fait en deux étapes. Dans l'interface graphique, sous CVE **actuels > Les instances ADC sont affectées par** les CVE , vous pouvez voir les étapes 1 et 2.

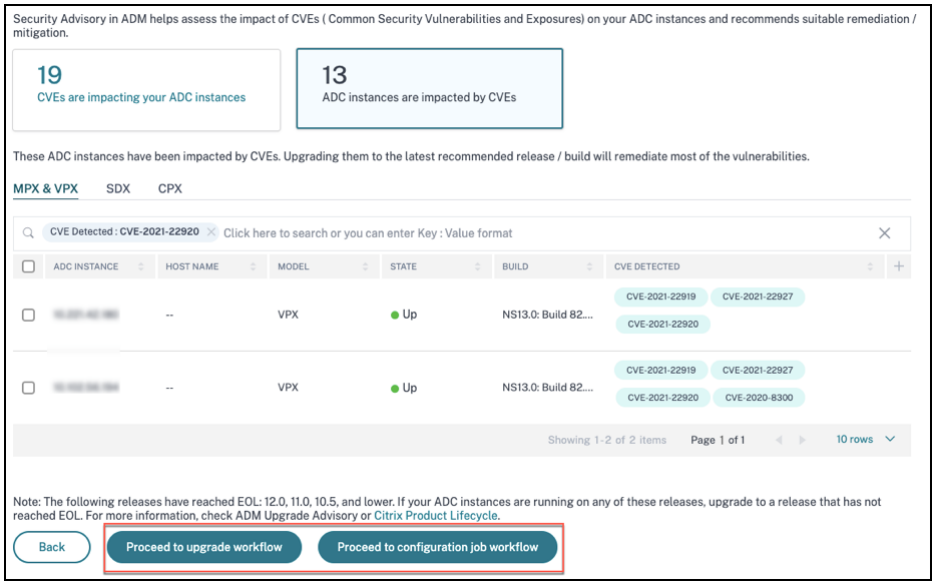


Les deux étapes sont les suivantes :

1. Mise à niveau des instances ADC vulnérables vers une version et une version contenant le correctif.
2. Appliquer les commandes de configuration requises à l'aide du modèle de configuration intégré personnalisable dans les tâches de configuration. Suivez cette étape pour chaque ADC vulnérable un par un et incluez toutes les actions SAML pour cet ADC.

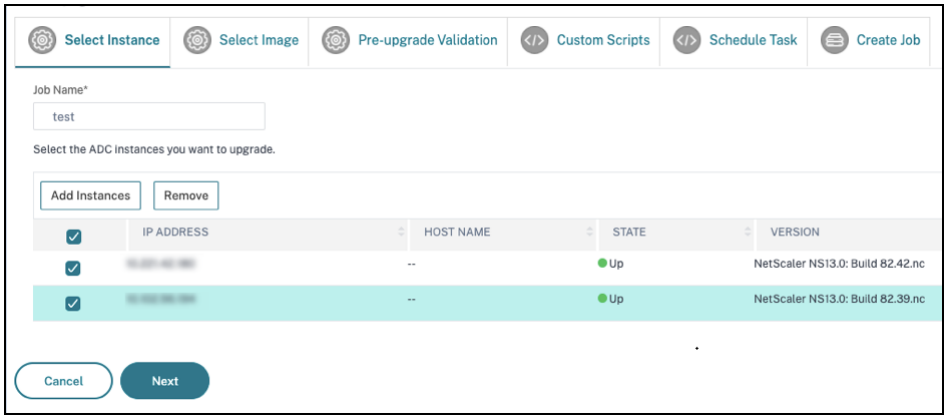
> **Remarque**
>
> Ignorez l'étape 2 si vous avez déjà exécuté des tâches de configuration sur l'instance ADC pour CVE-2020-8300.

SousCVE actuels > Instances ADC affectées par les CVE**, vous pouvez voir deux flux de travail distincts pour ce processus de correction en deux étapes : Procéder à la mise à niveau du flux de**travail et Passer au flux**de travail de configuration.**



Étape 1 : Mettre à niveau les instances ADC vulnérables

Pour mettre à niveau les instances vulnérables, sélectionnez les instances et cliquez sur **Procéder au flux de travail de mise à niveau**. Le flux de travail de mise à niveau s'ouvre avec les instances ADC vulnérables déjà renseignées.



Pour plus d'informations sur l'utilisation de NetScaler ADM pour mettre à niveau des instances ADC, consultez Créer unetâche de mise à niveau ADC.

> **Remarque**
>
> Cette étape peut être effectuée en une seule fois pour toutes les instances ADC vulnérables.
>
> **Remarque**
>
> Après avoir terminé l'étape 1 pour toutes les instances ADC vulnérables aux CVE-2021-22920 et CVE-2021-22927, effectuez une analyse à la demande. La posture de sécurité mise à jour sous **Current CVE** vous permet de déterminer si les instances ADC sont toujours vulnérables à l'un de ces CVE. À partir de la nouvelle posture, vous pouvez également vérifier si vous devez exécuter des tâches de configuration.
> Si vous avez déjà appliqué les tâches de configuration appropriées à l'instance ADC pour CVE-2020-8300 et que vous avez maintenant mis à niveau l'instance ADC, après avoir effectué l'analyse à la demande, l'instance ne s'affiche plus comme vulnérable pour CVE-2020-8300, CVE-2021-22920 et CVE-2021-22927.

Étape 2 : Appliquer les commandes de configuration

Après avoir mis à niveau les instances concernées, dans la fenêtre **<number of> Instances ADC affectées par les CVE**, sélectionnez une instance affectée par CVE-2021-22927 et CVE-2021-22920 et cliquez sur **Procéder au flux de travail de configuration**. Le flux de travail inclut les étapes suivantes.

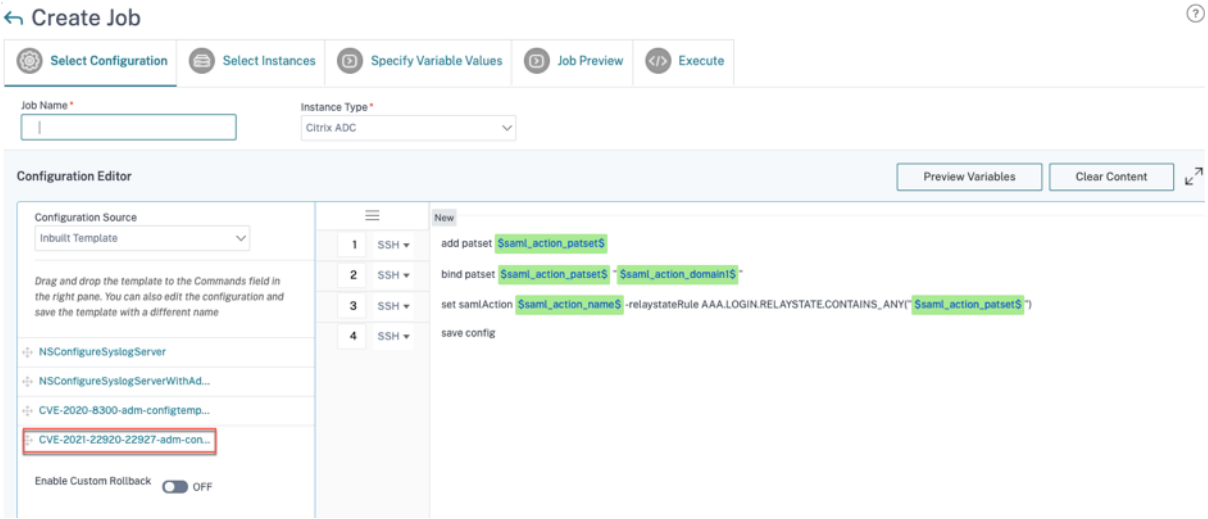
1. Personnalisation de la configuration.
2. Examen des instances impactées renseignées automatiquement.
3. Spécification des entrées pour les variables de la tâche.
4. Révision de la configuration finale avec les entrées variables renseignées.
5. Exécuter le travail.

Gardez les points suivants à l'esprit avant de sélectionner une instance et de cliquer sur **Procéder au**

flux de travail de configuration :

- Pour une instance ADC affectée par plusieurs CVE (tels que CVE-2020-8300, CVE-2021-22927, CVE-2021-22920 et CVE-2021-22956) : lorsque vous sélectionnez l'instance et que vous cliquez sur **Procéder au flux de travail de la tâche de configuration**, le modèle de configuration intégré ne se remplit pas automatiquement sous Sélectionner la configuration. Glissez et déposez manuellement le modèle de tâche de configuration approprié sous **Modèle d'avis de sécurité** dans le volet des tâches de configuration sur le côté droit.
- Pour plusieurs instances ADC impactées par CVE-2021-22956 uniquement : vous pouvez exécuter des tâches de configuration sur toutes les instances en même temps. Par exemple, vous avez l'ADC 1, l'ADC 2 et l'ADC 3, et tous sont affectés uniquement par CVE-2021-22956. Sélectionnez toutes ces instances et cliquez sur **Procéder au flux de travail de configuration**. Le modèle de configuration intégré s'affiche automatiquement sous **Sélectionner la configuration**.
- Pour plusieurs instances ADC impactées par CVE-2021-22956 et un ou plusieurs autres CVE (telles que CVE-2020-8300, CVE-2021-22927 et CVE-2021-22920), qui nécessitent une correction à appliquer à chaque ADC à la fois : lorsque vous sélectionnez ces instances et que vous cliquez sur **Procéder au flux de travail de tâche de configuration**, une erreur se produit Un message apparaît vous demandant d'exécuter la tâche de configuration sur chaque ADC à la fois.

Étape 1 : Sélection de la configuration Dans le flux de travail de configuration, le modèle de base de configuration intégré est automatiquement renseigné sous **Sélectionner la configuration**.



> **Remarque**
>
> Si l'instance ADC sélectionnée à l'étape 2 pour appliquer des commandes de configuration est vulnérable à CVE-2021-22927, CVE-2021-22920, ainsi qu'à CVE-2020-8300, le modèle de base

> pour CVE-2020-8300 est automatiquement renseigné. Le modèle CVE-2020-8300 est un super ensemble de commandes de configuration requises pour les trois CVE. Personnalisez ce modèle de base en fonction du déploiement et des besoins de votre instance ADC.

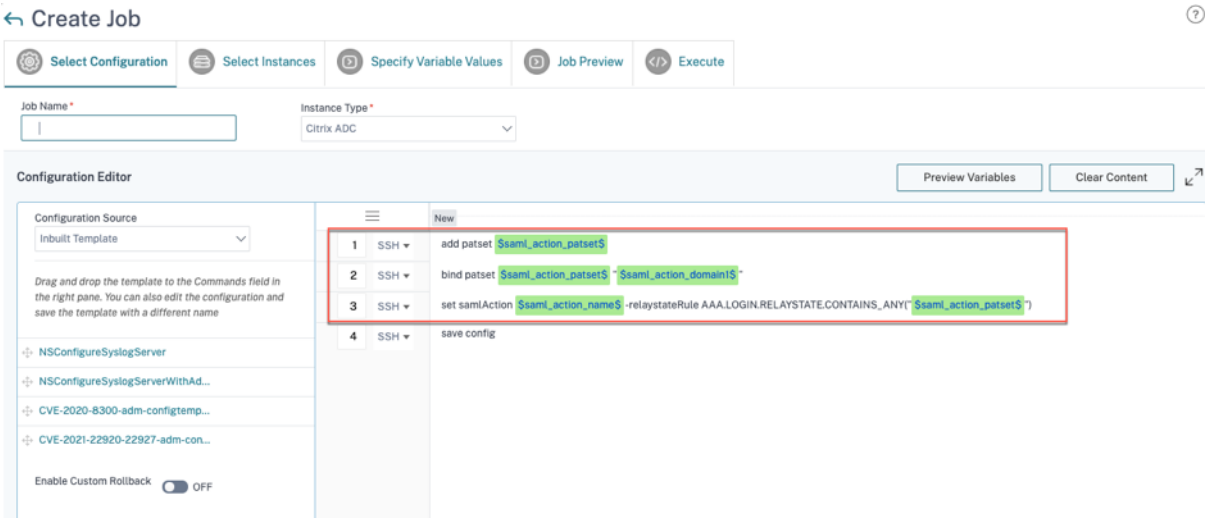
Vous devez exécuter une tâche de configuration distincte pour chaque instance ADC affectée, une par une, et inclure toutes les actions SAML pour cet ADC. Par exemple, si vous avez deux instances ADC vulnérables ayant chacune deux actions SAML, vous devez exécuter cette tâche de configuration deux fois. Une fois par ADC couvrant toutes ses actions SAML.

ADC 1	ADC2
Tâche 1 : deux actions SAML	Tâche 2 : deux actions SAML

Donnez un nom à la tâche et personnalisez le modèle selon les spécifications suivantes. Le modèle de configuration intégré n'est qu'un modèle de plan ou de base. Personnalisez le modèle en fonction de votre déploiement pour répondre aux exigences suivantes :

a. **Actions SAML et domaines associés**

En fonction du nombre d'actions SAML que vous avez dans votre déploiement, vous devez répliquer les lignes 1 à 3 et personnaliser les domaines pour chaque action SAML.



Par exemple, si vous avez deux actions SAML, répétez les lignes 1 à 3 deux fois et personnalisez en conséquence les définitions de variables pour chaque action SAML.

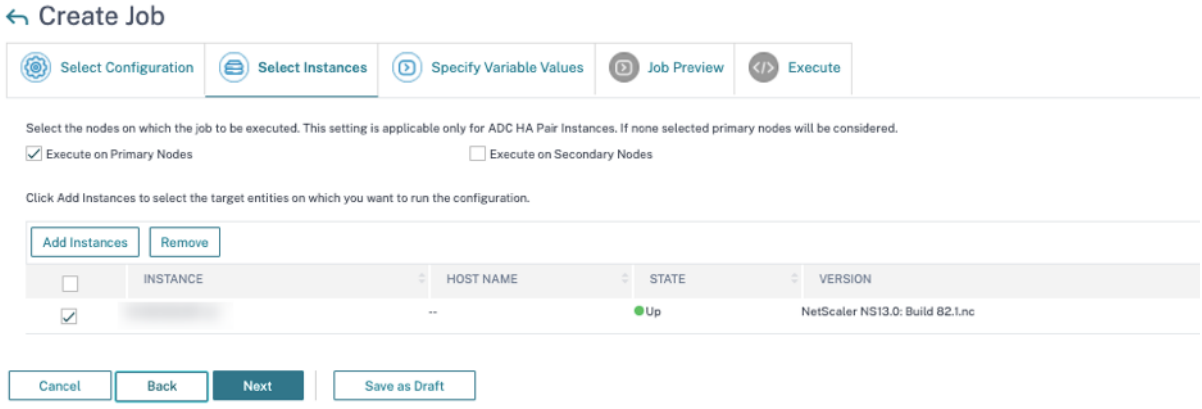
Et si vous avez N domaines pour une action SAML, vous devez saisir manuellement la ligne `bind patset $saml_action_patset$ "$saml_action_domain1$"` plusieurs fois pour vous assurer que la ligne apparaît N fois pour cette action SAML. Et modifiez les noms des définitions de variables suivants :

- `saml_action_patset`: est la variable du modèle de configuration et représente la valeur du nom du jeu de modèles (patset) pour l'action SAML. Vous pouvez spécifier la valeur réelle à l'étape 3 du flux de travail de configuration. Consultez la section Étape 3 : Spécifier les valeurs des variables dans ce document.
- `saml_action_domain1`: est la variable du modèle de configuration, qui représente le nom de domaine pour cette action SAML spécifique. Vous pouvez spécifier la valeur réelle à l'étape 3 du flux de travail de configuration. Consultez la section Étape 3 : Spécifier les valeurs des variables dans ce document.

Pour rechercher toutes les actions SAML d'un appareil, exécutez la commande `show samlaction` .

Étape 2 : Sélectionnez l'instance

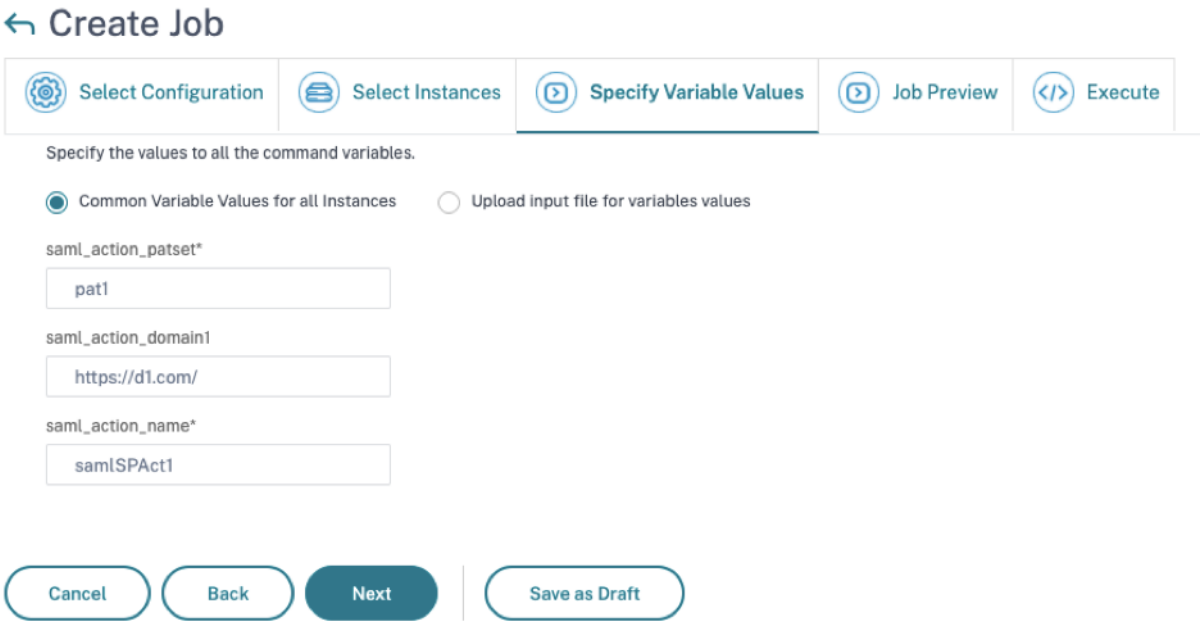
L'instance affectée est automatiquement renseignée sous **Select Instances**. Sélectionnez l'instance et cliquez sur **Suivant**.



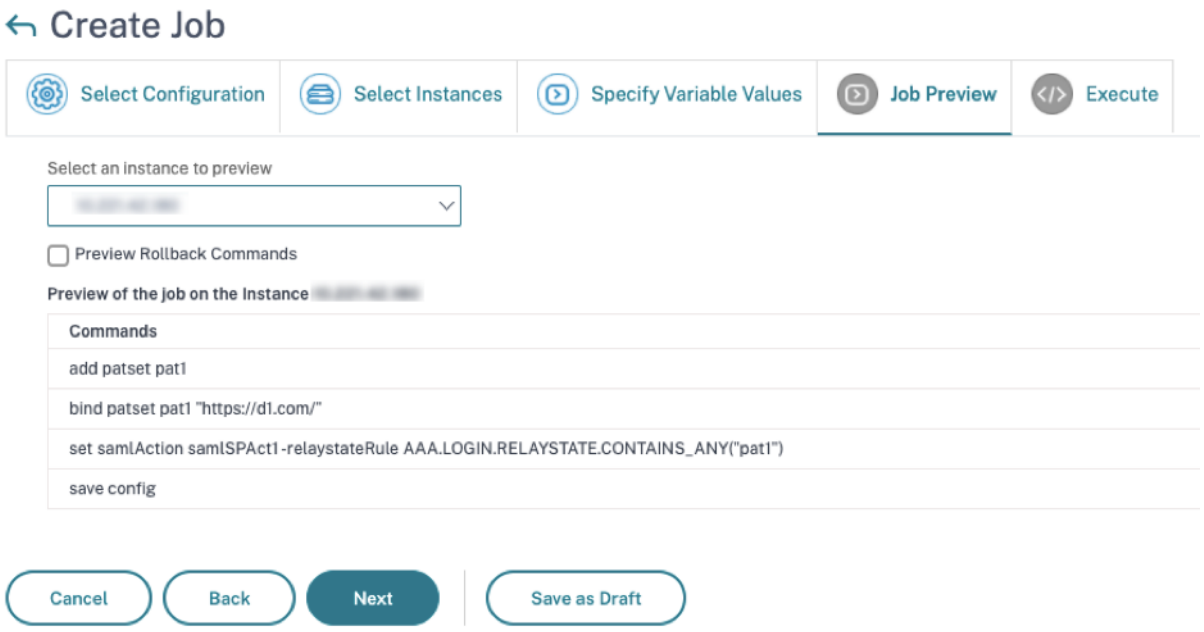
Étape 3 : Spécifier les valeurs des variables Entrez les valeurs des variables.

- `saml_action_patset`: ajoute un nom pour l'action SAML
- `saml_action_domain1`: entrez un domaine au format `https://<example1.com>/`

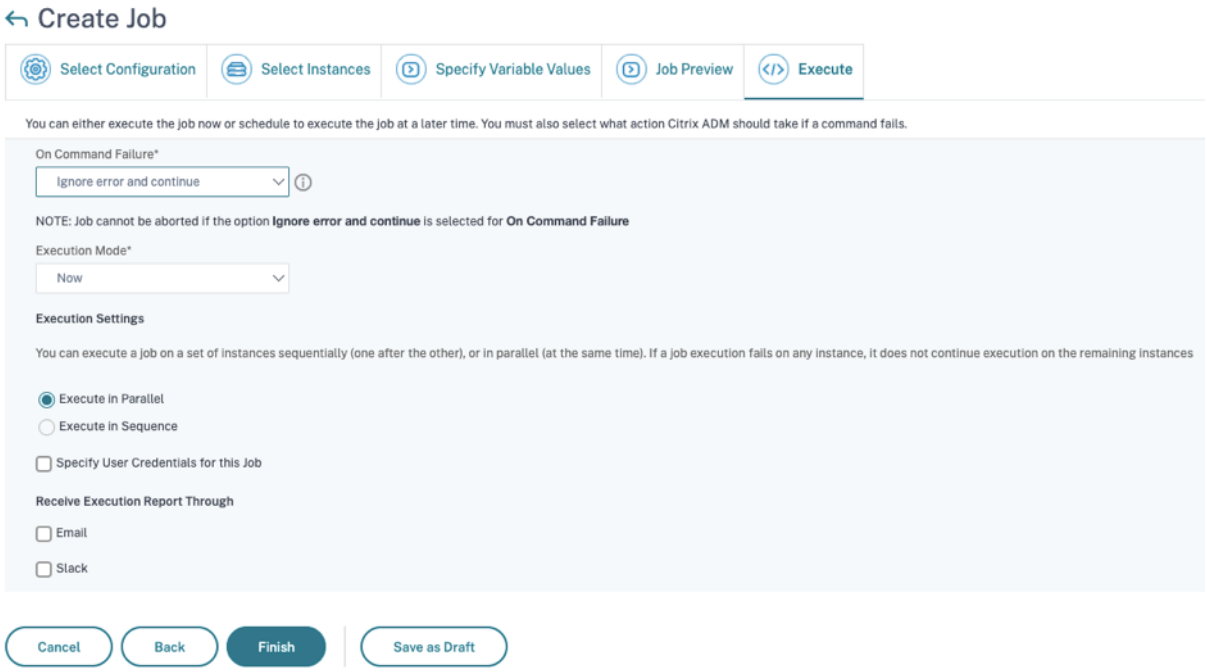
- `saml_action_name`: entrez la même action SAML pour laquelle vous configurez la tâche



Étape 4 : Prévisualiser la configuration Prévisualise les valeurs des variables qui ont été insérées dans la configuration et cliquez sur **Suivant**.



Étape 5 : Exécuter la tâche Cliquez sur **Terminer** pour exécuter la tâche de configuration.



Une fois la tâche exécutée, elle apparaît sous **Infrastructure > Configuration > Tâches de configuration**.

Après avoir effectué les deux étapes de correction pour tous les ADC vulnérables, vous pouvez exécuter une analyse à la demande pour voir la nouvelle posture de sécurité.

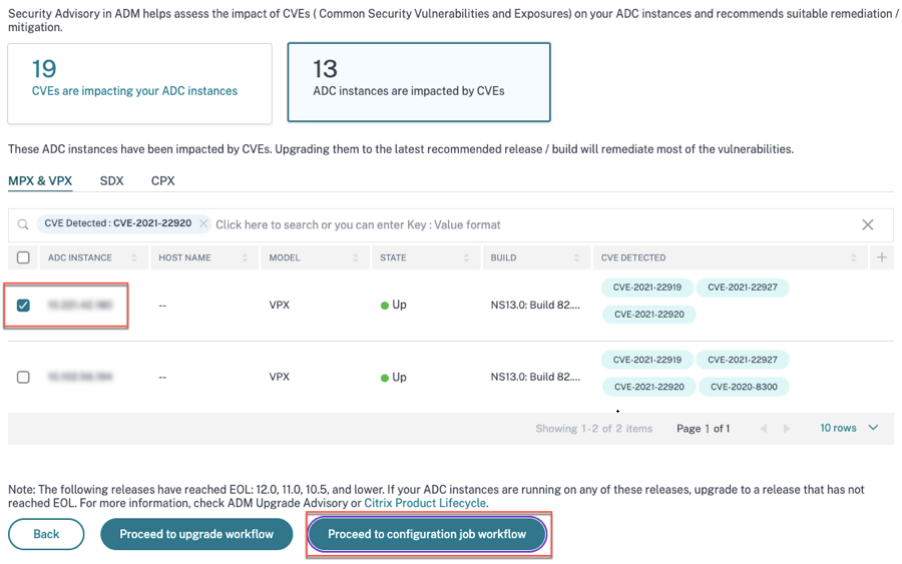
Scénario

Dans ce scénario, deux instances ADC sont vulnérables au CVE-2021-22920, et vous devez corriger toutes les instances. Procédez comme suit :

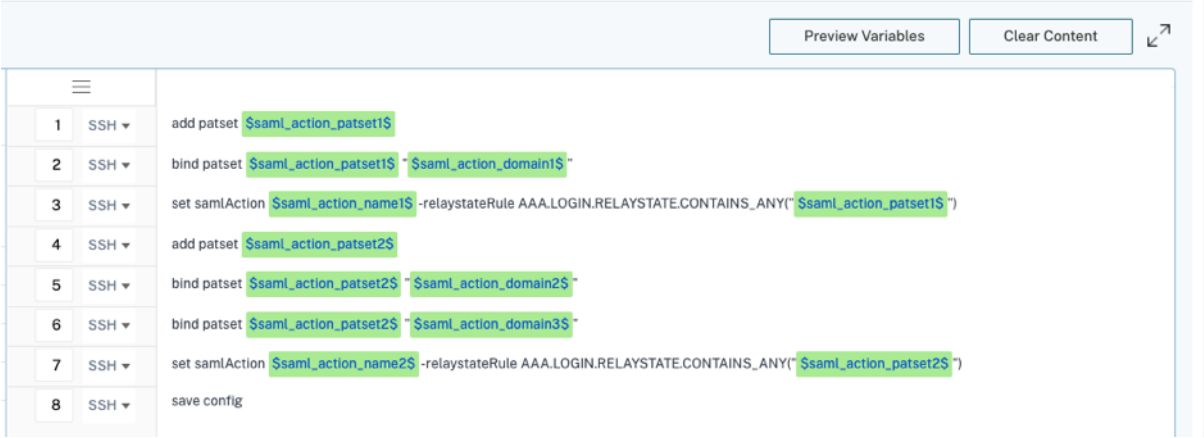
1. Mettez à niveau les trois instances ADC en suivant les étapes indiquées dans la section « Mettre à niveau une instance » de ce document.
2. Appliquez le correctif de configuration à un ADC à la fois, en utilisant le flux de travail de configuration. Consultez les étapes indiquées dans la section « Appliquer les commandes de configuration » de ce document.

L'ADC 1 vulnérable possède deux actions SAML :

- L'action SAML 1 possède un domaine
- L'action SAML 2 comporte deux domaines



Sélectionnez ADC 1 et cliquez sur **Procéder au flux de travail de configuration**. Le modèle de base intégré se remplit automatiquement. Ensuite, donnez un nom de tâche et personnalisez le modèle en fonction de la configuration donnée.

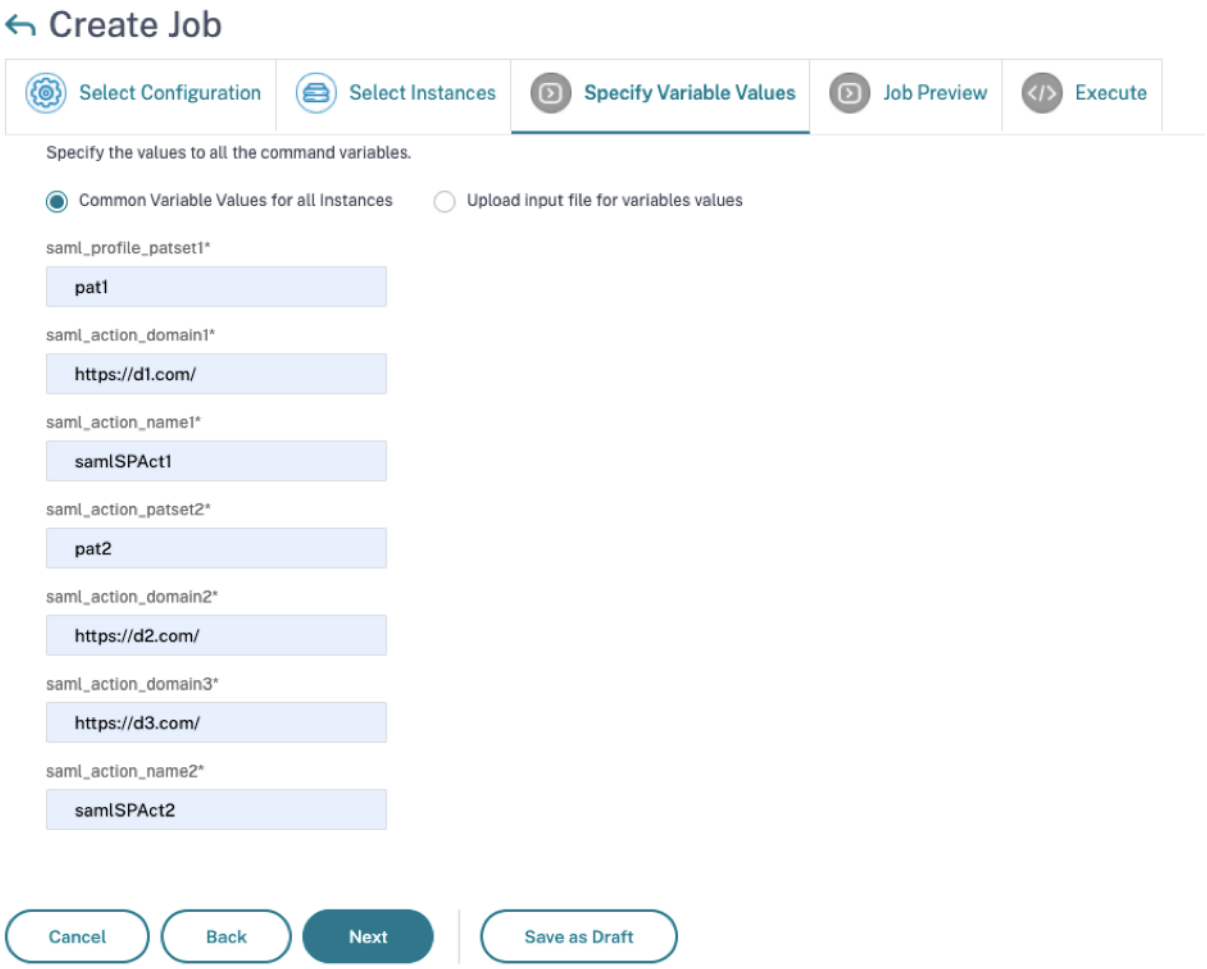


Le tableau suivant répertorie les définitions de variables pour les paramètres personnalisés.

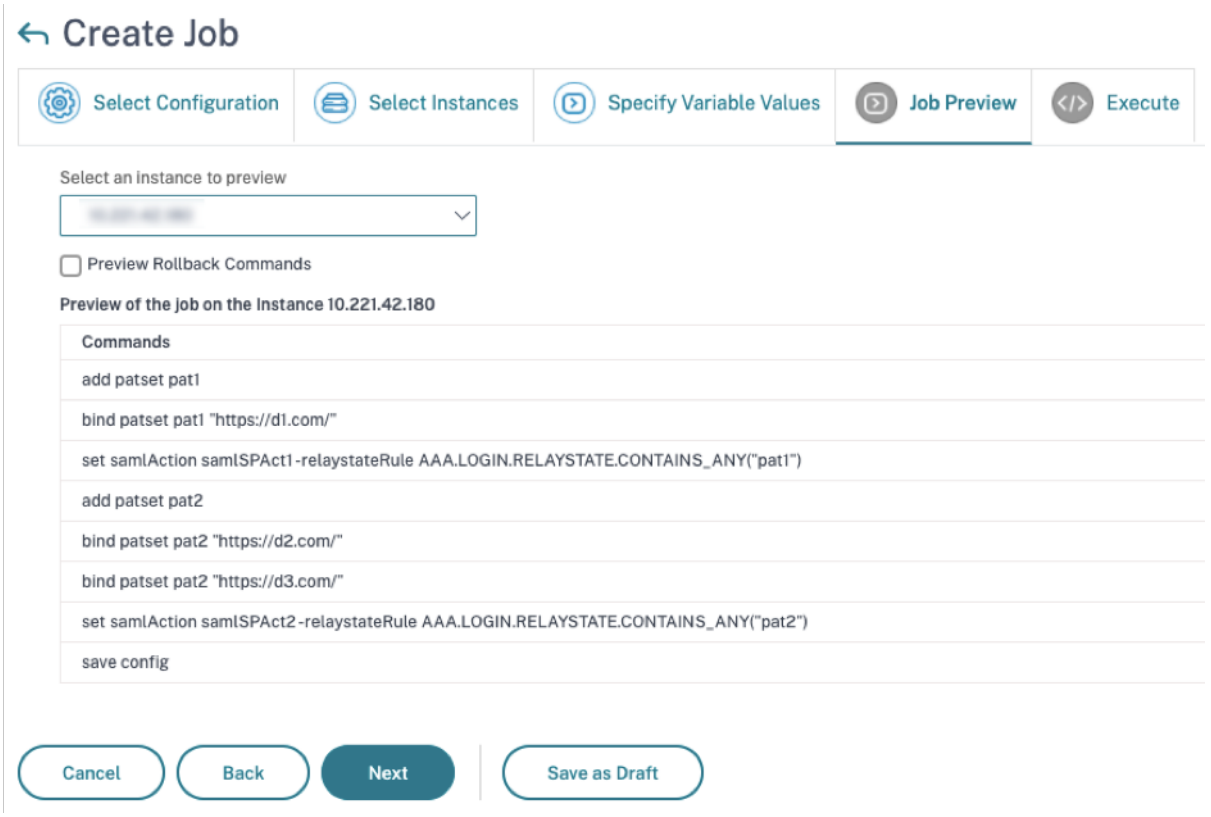
Tableau. Définitions de variables pour l'action SAML

Configuration de l'ADC	Définition de variable pour patset	Définition de variable pour le nom de l'action SAML	Définition de variable pour le domaine
L'action SAML 1 possède un domaine	saml_action_patset1	saml_action_name1	saml_action_domain1
L'action SAML 2 comporte deux domaines	saml_action_patset2	saml_action_name2	saml_action_domain2, saml_action_domain3

Sous **Select Instances**, sélectionnez ADC 1 et cliquez sur **Next**. La fenêtre **Spécifier les valeurs des variables** s'affiche. Au cours de cette étape, vous devez fournir des valeurs pour toutes les variables définies à l'étape précédente.



Ensuite, passez en revue les variables.



Cliquez sur **Suivant**, puis sur **Terminer** pour exécuter la tâche.

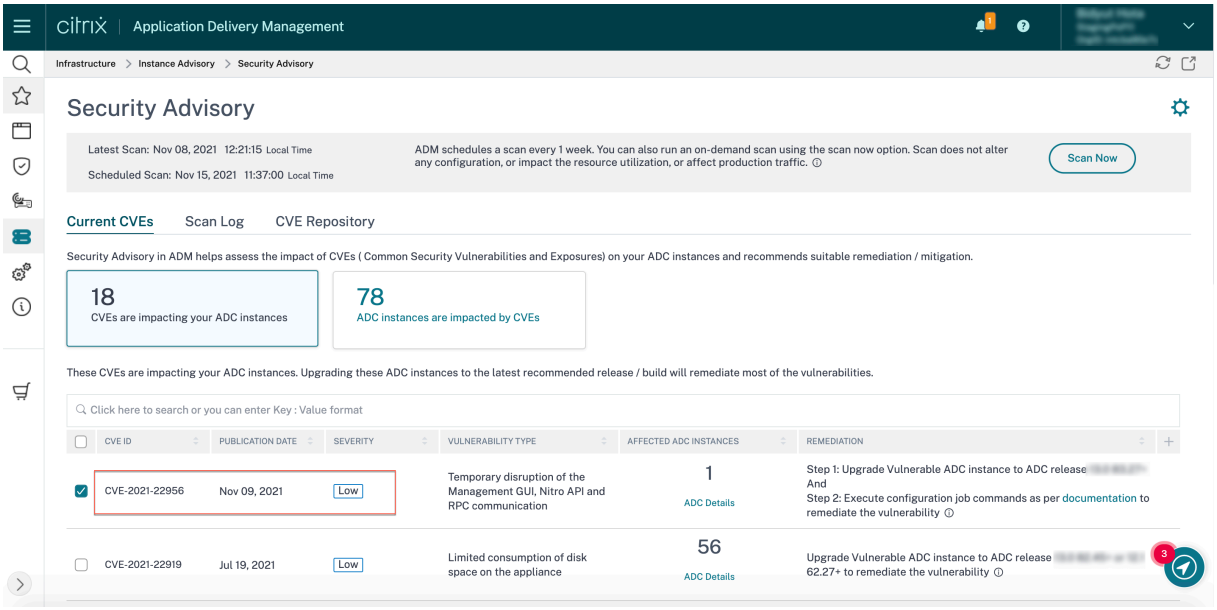
Une fois la tâche exécutée, elle apparaît sous **Infrastructure > Configuration > Tâches de configuration**.

Après avoir terminé les deux étapes de correction pour l'ADC1, suivez les mêmes étapes pour corriger l'ADC 2 et l'ADC 3. Une fois la correction terminée, vous pouvez exécuter une analyse à la demande pour voir la nouvelle posture de sécurité.

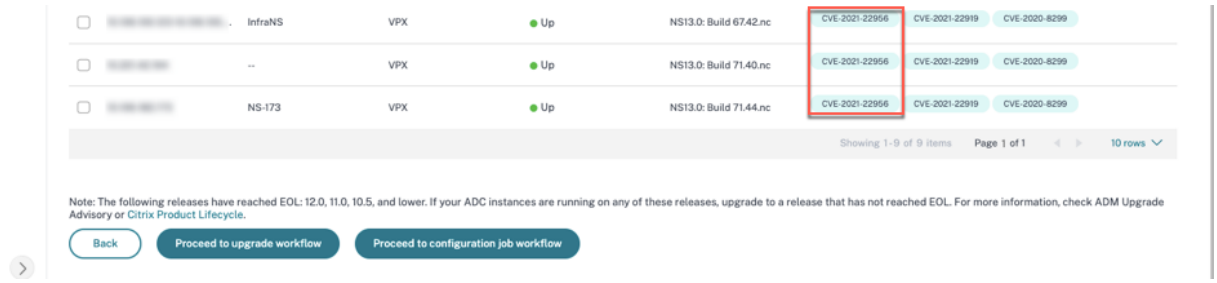
Identifier et corriger les vulnérabilités du CVE-2021-22956

February 1, 2024

Dans le tableau de bord des avis de sécurité de NetScaler ADM, sous CVE**actuels > Les instances< number of>**ADC sont affectées par des vulnérabilités et des expositions courantes (CVE), vous pouvez voir toutes les instances vulnérables en raison de cette CVE spécifique. Pour vérifier les détails des instances concernées par CVE-2021-22956, sélectionnez CVE-2021-22956 et cliquez sur **Afficher les instances affectées**.



La fenêtre Instances<number of>ADC impactées par les CVE s'affiche. Vous trouverez ici le nombre et les détails des instances ADC impactées par le CVE-2021-22956.



Pour plus d'informations sur le tableau de bord des avis de sécurité, voir Avis de sécurité.

> **Remarque**
>
> L'analyse du système d'avis de sécurité peut prendre un certain temps avant de se terminer et de refléter l'impact du CVE-2021-22956 dans le module d'avis de sécurité. Pour constater l'impact plus rapidement, lancez une analyse à la demande en cliquant sur **Analyser maintenant**.

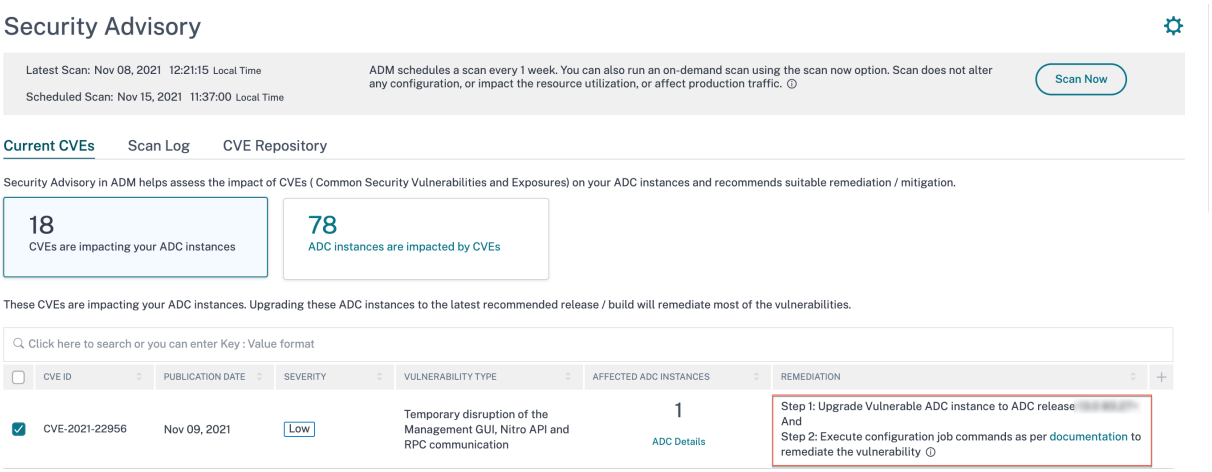
Identifiez les instances touchées par le CVE-2021-22956

Le CVE-2021-22956 nécessite un scan personnalisé, au cours duquel le service ADM se connecte à l'instance ADC gérée et envoie un script vers l'instance. Le script s'exécute sur l'instance ADC et vérifie les paramètres du fichier de configuration Apache (`httpd.conf file`) et du nombre maximum de connexions client (`maxclient`) pour déterminer si une instance est vulnérable ou non. Les informations que le script partage avec le service ADM sont l'état de vulnérabilité en booléen (vrai ou faux). Le script renvoie également au service ADM une liste des nombres de max_clients pour différentes interfaces réseau, par exemple l'hôte local, le NSIP et le SNIP avec accès de gestion.

Ce script s'exécute à chaque exécution de vos analyses à la demande planifiées. Une fois l'analyse terminée, le script est supprimé de l'instance ADC.

Corriger CVE-2021-22956

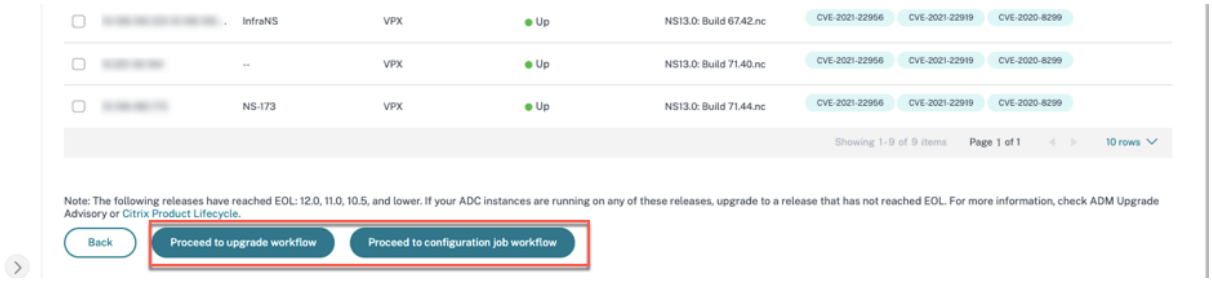
Pour les instances ADC impactées par CVE-2021-22956, la correction se fait en deux étapes. Dans l'interface graphique, sous**Current CVE > Les instances ADC sont impactées par les CVE**, vous pouvez voir les étapes 1 et 2.



Les deux étapes sont les suivantes :

1. Mise à niveau des instances ADC vulnérables vers une version et une version contenant le correctif.
2. Appliquer les commandes de configuration requises à l'aide du modèle de configuration intégré personnalisable dans les tâches de configuration.

Sous Current CVE> Instances ADC impactées par les CVE, vous pouvez voir deux workflows distincts pour ce processus de correction en deux étapes : Procéder à la mise à niveau du flux de travail et Procéder au flux de travail de configuration.



Étape 1 : Mettre à niveau les instances ADC vulnérables

Pour mettre à niveau les instances vulnérables, sélectionnez les instances et cliquez sur **Procéder au flux de travail de mise à niveau**. Le flux de travail de mise à niveau s'ouvre avec les instances ADC vulnérables déjà renseignées.

Pour plus d'informations sur l'utilisation de NetScaler ADM pour mettre à niveau des instances ADC, consultez Créer unetâche de mise à niveau ADC.

> **Remarque**
>
> Cette étape peut être effectuée en une seule fois pour toutes les instances ADC vulnérables.

Étape 2 : Appliquer les commandes de configuration

Après avoir mis à niveau les instances concernées, dans la fenêtre **<number of> Instances ADC affectées par les CVE**, sélectionnez l'instance affectée par CVE-2021-2295 et cliquez sur **Procéder au flux de travail de configuration**. Le flux de travail inclut les étapes suivantes.

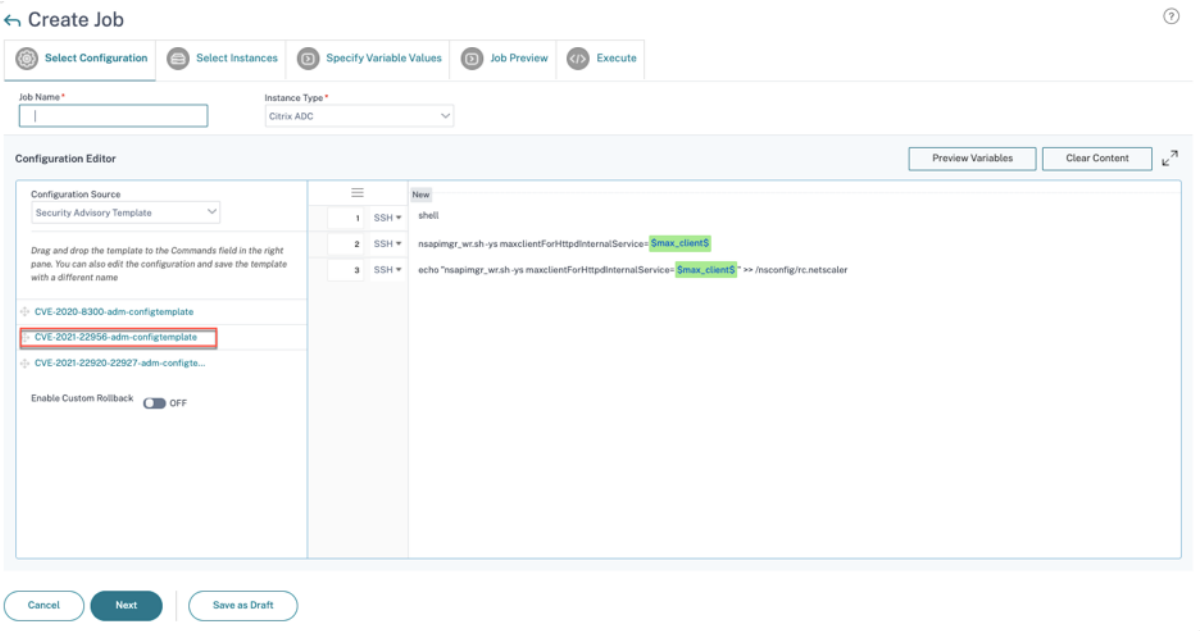
1. Personnalisation de la configuration.
2. Examen des instances impactées renseignées automatiquement.
3. Spécification des entrées pour les variables de la tâche.
4. Révision de la configuration finale avec les entrées variables renseignées.
5. Exécuter le travail.

Gardez les points suivants à l'esprit avant de sélectionner une instance et de cliquer sur **Procéder au flux de travail de configuration** :

- Pour une instance ADC affectée par plusieurs CVE (tels que CVE-2020-8300, CVE-2021-22927, CVE-2021-22920 et CVE-2021-22956) : lorsque vous sélectionnez l'instance et que vous cliquez sur **Procéder au flux de travail de la tâche de configuration**, le modèle de configuration intégré ne se remplit pas automatiquement sous Sélectionner la configuration. Glissez et déposez manuellement le modèle de tâche de configuration approprié sous **Modèle d'avis de sécurité** dans le volet des tâches de configuration sur le côté droit.
- Pour plusieurs instances ADC impactées par CVE-2021-22956 uniquement : vous pouvez exécuter des tâches de configuration sur toutes les instances en même temps. Par exemple, vous avez l'ADC 1, l'ADC 2 et l'ADC 3, et tous sont affectés uniquement par CVE-2021-22956. Sélectionnez toutes ces instances et cliquez sur **Procéder au flux de travail de configuration**. Le modèle de configuration intégré s'affiche automatiquement sous **Sélectionner la configuration**. Reportez-vous au problème connu NSADM-80913 dans les notes de publication.
- Pour plusieurs instances ADC impactées par CVE-2021-22956 et un ou plusieurs autres CVE (telles que CVE-2020-8300, CVE-2021-22927 et CVE-2021-22920), qui nécessitent une correction

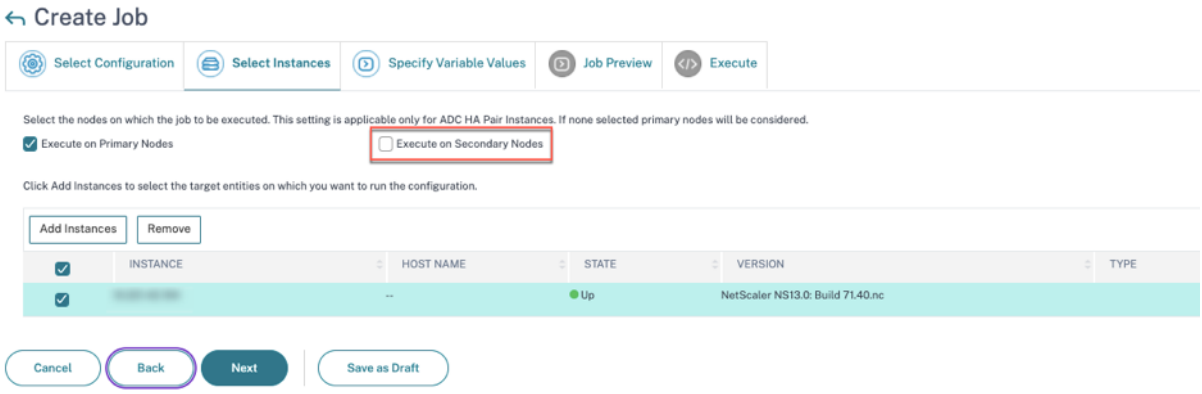
à appliquer à chaque ADC à la fois : lorsque vous sélectionnez ces instances et que vous cliquez sur **Procéder au flux de travail de tâche de configuration**, une erreur se produit Un message apparaît vous demandant d'exécuter la tâche de configuration sur chaque ADC à la fois.

Étape 1 : Sélection de la configuration Dans le flux de travail de configuration, le modèle de base de configuration intégré est automatiquement renseigné sous **Sélectionner la configuration**.



Étape 2 : Sélectionnez l'instance

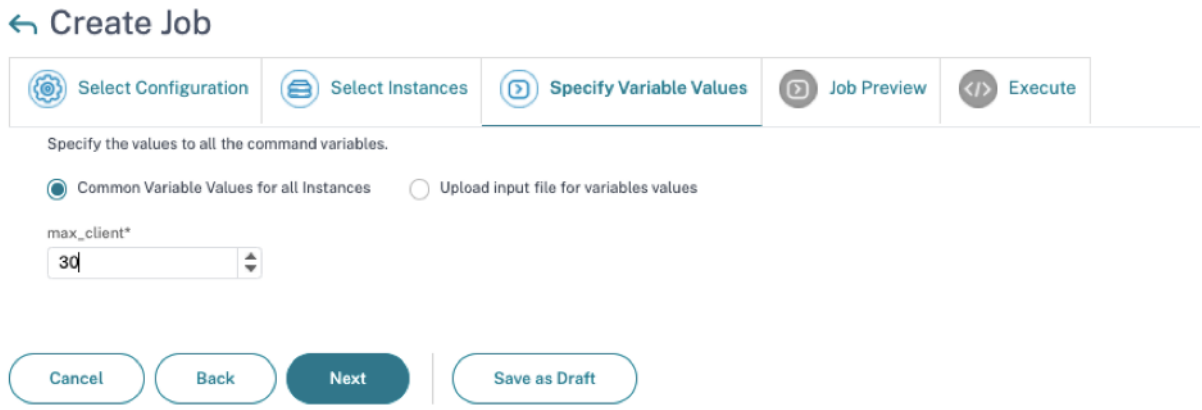
L'instance affectée est automatiquement renseignée sous **Select Instances**. Sélectionnez l'instance. Si cette instance fait partie d'une paire HA, sélectionnez **Exécuter sur des nœuds secondaires**. Cliquez sur **Suivant** .



> **Remarque**
>
> Pour les instances ADC en mode cluster, à l'aide de l'avis de sécurité ADM, ADM prend en charge l'exécution de la tâche de configuration uniquement sur le nœud CCO (Cluster Configuration Coordinator). Exécutez les commandes séparément sur les nœuds non-CCO.

`rc.netscaler` est synchronisé sur tous les nœuds HA et de cluster, ce qui rend la correction persistante après chaque redémarrage.

Étape 3 : Spécifier les valeurs des variables Entrez les valeurs des variables.



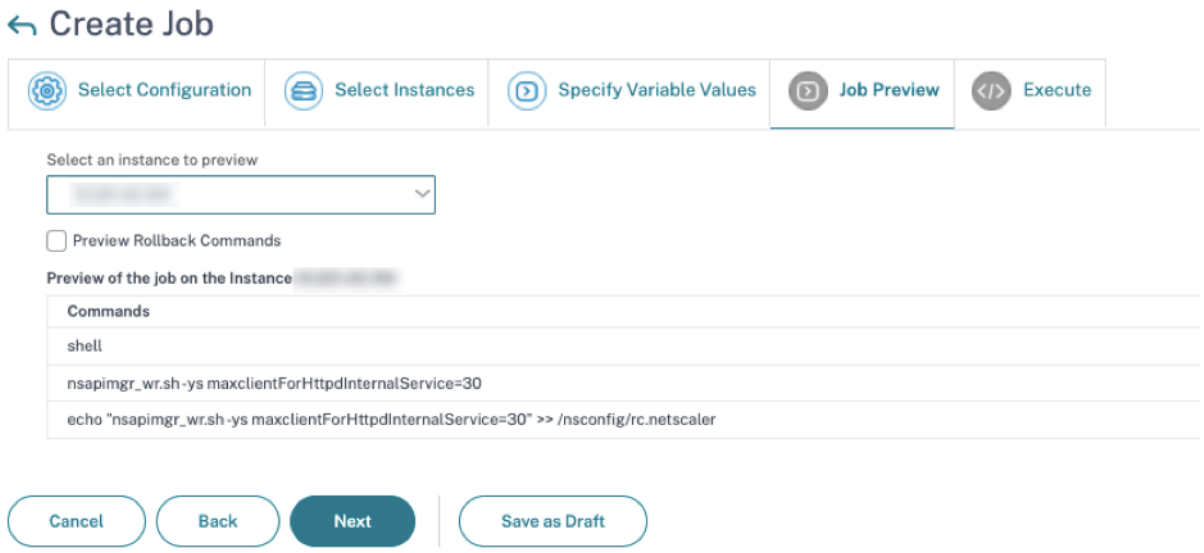
Sélectionnez l'une des options suivantes pour spécifier des variables pour vos instances :

Valeurs de variables communes pour toutes les instances : Entrez une valeur commune pour la variable `max_client`.

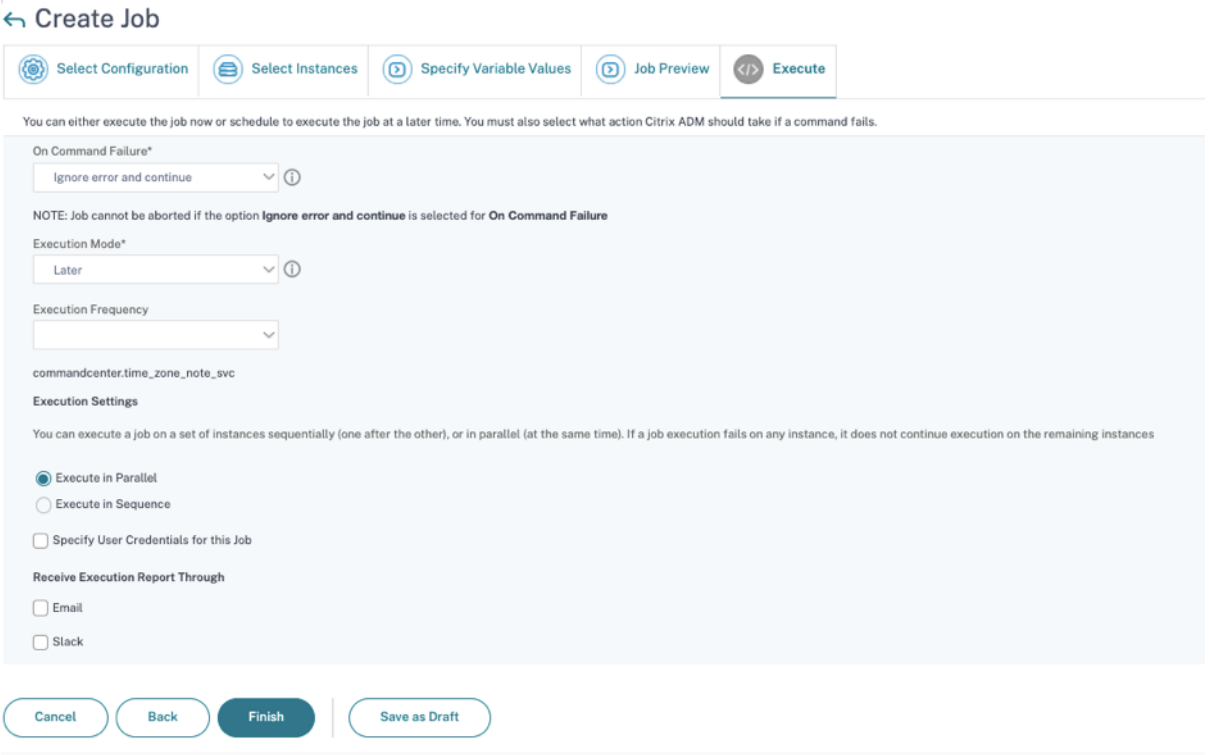
Téléchargez le fichier d'entrée pour les valeursdes variables : cliquez sur **Télécharger le fichier clé** d'entrée pour télécharger un fichier d'entrée. Dans le fichier d'entrée, entrez les valeurs de la variable, `max_client` puis téléchargez le fichier sur le serveur ADM. Reportez-vous au problème connu NSADM-80913 dans les notes de mise à jour concernant un problème lié à cette option.

> **Remarque**
>
> Pour les deux options mentionnées ci-dessus, la `max_client` valeur recommandée est 30. Vous pouvez définir la valeur en fonction de votre valeur actuelle. Toutefois, elle ne doit pas être nulle et doit être inférieure ou égale à la valeur max_client définie dans le `/etc/httpd.conf` fichier. Vous pouvez vérifier la valeur actuelle définie dans le fichier de configuration du serveur HTTP Apache `/etc/httpd.conf` en recherchant la chaîne `MaxClients`, dans l'instance ADC

Étape 4 : Prévisualiser la configuration Prévisualise les valeurs des variables qui ont été insérées dans la configuration et cliquez sur **Suivant**.



Étape 5 : Exécuter la tâche Cliquez sur **Terminer** pour exécuter la tâche de configuration.



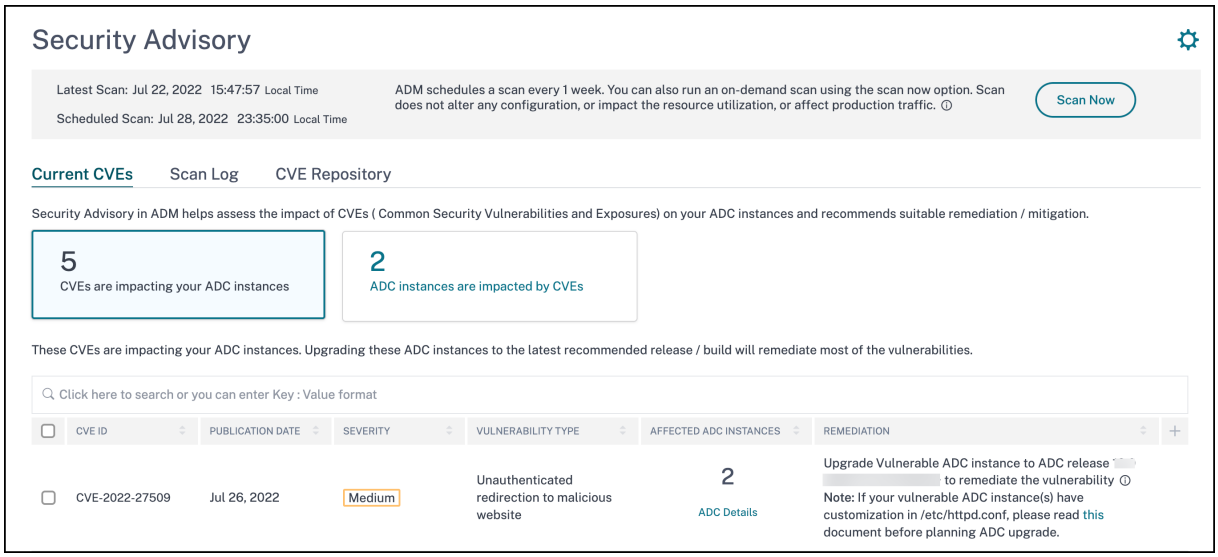
Une fois la tâche exécutée, elle apparaît sous **Infrastructure > Configuration > Tâches de configuration**.

Après avoir effectué les deux étapes de correction pour tous les ADC vulnérables, vous pouvez exécuter une analyse à la demande pour voir la nouvelle posture de sécurité.

Identifier et corriger les vulnérabilités du CVE-2022-27509

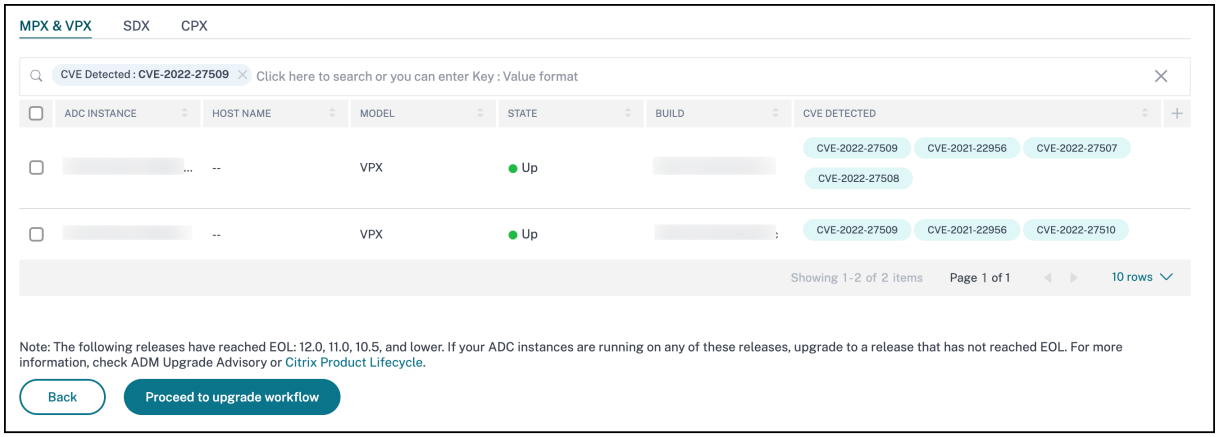
February 1, 2024

Dans le tableau de bord des avis de sécurité de NetScaler ADM, sous **CVE actuels, les instances < number of> ADC sont affectées par des CVE, vous pouvez voir toutes les instances**vulnérables en raison de la vulnérabilité CVE-2022-27509. Pour vérifier les détails des instances impactées par les CVE, sélectionnez CVE-2022-27509 et cliquez sur **Afficher les instances affectées**.



> **Remarque**
>
> Pour comprendre la raison de la vulnérabilité de l'ADC, téléchargez le rapport CSV dans l'onglet Journaux de numérisation de l'Avis de sécurité.

La fenêtre **<number of> Instances ADC impactées par les CVE** s'affiche. Dans la capture d'écran suivante, vous pouvez voir le nombre et les détails des instances ADC affectées par le CVE-2022-27509.



Pour plus d'informations sur le tableau de bord des avis de sécurité, voir Avis de sécurité.

> **Remarque**
>
> L'analyse du système d'avis de sécurité peut prendre quelques heures pour se terminer et refléter l'impact du CVE-2022-27509 sur le module d'avis de sécurité. Pour voir l'impact plus rapidement, lancez une analyse à la demande en cliquant sur **Scanner maintenant**.

Identifiez les instances touchées par le CVE-2022-27509

Le CVE-2022-27509 nécessite une combinaison de numérisation personnalisée et de numérisation de version. Dans le cadre de l'analyse personnalisée, le service ADM se connecte à l'instance ADC gérée et envoie un script à l'instance. Le script s'exécute sur l'instance ADC et détermine si l'instance est vulnérable. Ce script s'exécute à chaque fois que votre analyse planifiée ou à la demande est exécutée.

Une fois l'analyse terminée, le script est supprimé de l'instance ADC.

Vous pouvez également désactiver ces avis de sécurité (scans personnalisés). Pour plus d'informations sur les paramètres de scan personnalisés et la désactivation des scans personnalisés, consultez la section **Configurer les paramètres de scan personnalisés** sur la page **Avis de sécurité** .

Corriger le CVE-2022-27509

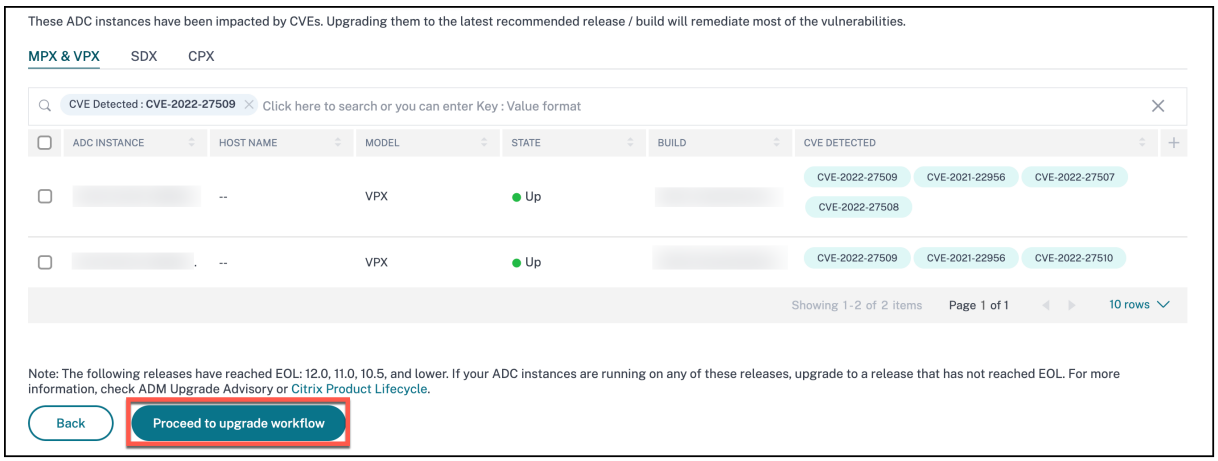
Pour les instances ADC affectées par CVE-2022-27509, la correction est un processus en une seule étape et vous devez mettre à niveau les instances ADC vulnérables vers une version et une version contenant le correctif. Dans l'interface graphique, sous **Current CVE > Les instances ADC sont impactées par les CVE**, vous pouvez voir l'étape à suivre pour y remédier.

Sous **Current CVE> Instances ADC impactées par les CVE**, vous pouvez voir le flux de travail suivant pour ce processus de correction en une seule étape, à savoir **Procéder à la mise à niveau**.

Pour mettre à niveau les instances vulnérables, sélectionnez les instances et cliquez sur **Procéder au flux de travail de mise à niveau**. Le flux de travail de mise à niveau s'ouvre avec les instances ADC vulnérables déjà renseignées.

> **IMPORTANT**
>
> Si le fichier /etc/httpd.conf de vos instances ADC vulnérables est copié dans le répertoire /nsconfig, consultez la section Considérations relatives à la mise à niveau pour les configurations ADC personnalisées avant de planifier la mise à niveau de l'ADC.

Pour plus d'informations sur l'utilisation de NetScaler ADM pour mettre à niveau des instances ADC, consultez Créer unetâche de mise à niveau ADC.



CVE non pris en charge dans l'avis de sécurité

February 1, 2024

L'avis de sécurité de NetScaler ADM suit toutes les nouvelles vulnérabilités et expositions courantes (CVE) et évalue l'impact des CVE sur l'infrastructure. Vous pouvez consulter les recommandations et prendre les mesures appropriées. Toutefois, certains CVE ne sont pas pris en charge et la détection et la correction de ces vulnérabilités ne relèvent pas du champ d'application de l'avis de sécurité de NetScaler ADM.

- **CVE-2022-21827** :

  CVE-2022-21827 a un impact sur le plug-in NetScaler Gateway pour les versions prises en charge par Windows antérieures à la version 21.9.1.2.

  La détection et la correction des vulnérabilités affectant le plug-in NetScaler Gateway pour Windows ne sont pas prises en charge par NetScaler ADM. De plus, les vulnérabilités du plug-in NetScaler Gateway ne peuvent pas être évaluées en effectuant des vérifications côté ADC, en vérifiant la version de l'ADC ou en vérifiant la configuration de l'ADC. La détection et la correction de ce CVE ne peuvent être évaluées qu'en fonction de la version du plug-in NetScaler Gateway pour Windows déployée sur le client.

  Par conséquent, la détection et la correction de cette vulnérabilité ne relèvent pas du champ d'application de NetScaler ADM Security Advisory.

Avis de mise à niveau (version préliminaire)

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 NetScaleret identifier les instances ADC qui atteignent ou ont atteint la fin de vie (EOL) ou la fin de maintenance (EOM). Ensuite, planifiez leur mise à niveau.

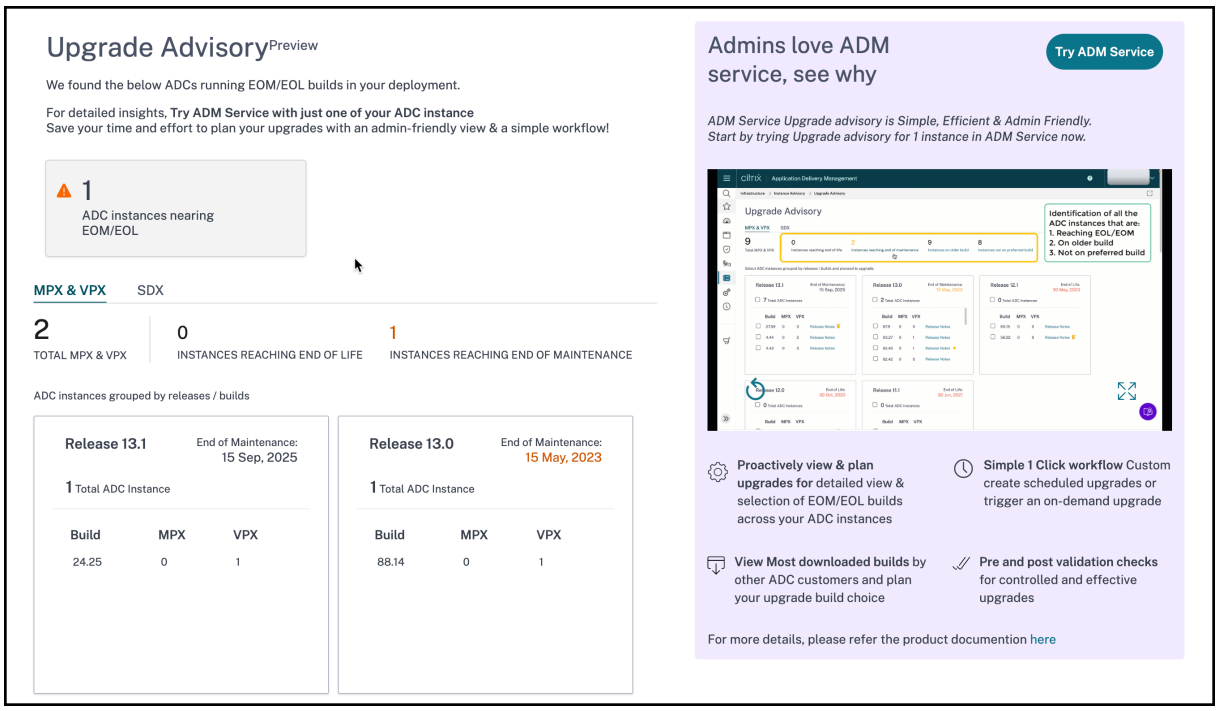
Le service de conseil de mise à niveau local de NetScaler ADM effectue une analyse de version sur les ADC et fournit une vue des versions EOM/EOL de vos instances ADC.

> **IMPORTANT**
>
> Pour obtenir des informations détaillées et connaître le flux de travail permettant de mettre à niveau les instances ADC, **essayez NetScaler**ADM Service.

Consulter l'avis de mise

Accédez à **Infrastructure > Conseil d'instance > Avis de mise à niveau** et consultez 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.

Le conseil de mise à niveau local de NetScaler ADM vous permet également de sélectionner l'une des instances ADC et d'intégrer l'instance ADC au service ADM. Cliquez sur **Try ADM Service** et intégrez l'instance ADC au service ADM. ADM Service Upgrade Advisory vous fournit le flux de travail nécessaire pour effectuer la mise à niveau par instance ADC sélectionnée.

Pour plus d'informations sur l'avis de mise à niveau du service ADM, consultez l'animation GIF sur la page d'**avis de mise à niveau** .

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

NetScaler Application Delivery Management (ADM) prend en charge le SDN dans le réseau des entreprises en s'intégrant aux contrôleurs SDN de différents fournisseurs. NetScaler ADM prend en charge à la fois VMware NSX Manager et le contrôleur d'infrastructure des stratégies d'application Cisco (APIC).

VMware NSX Manager

NetScaler ADM s'intègre à la plateforme de virtualisation réseau VMware pour automatiser le déploiement, la configuration et la gestion des services NetScaler. Cette intégration élimine les complexités traditionnelles associées à la topologie physique du réseau, ce qui permet aux administrateurs de vSphere/vCenter de déployer les services NetScaler plus rapidement par programmation.

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 NetScaler ADM permet l'intégration des produits NetScaler à VMware NSX et fournit 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 les fonctionnalités avancées de NetScaler telles que SSL et CS ainsi que l'équilibrage de charge de base via des modèles d'applications 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 NetScaler depuis 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 simplifiée avec les API NetScaler ADM, qui permettent de prendre en charge des utilisations futures imprévues.

Pour plus d'informations sur la configuration de VMware NSX Manager sur NetScaler ADM, consultez la section Intégration des appliances NetScalerà 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 automatiser le réseau via l'Application Policy Infrastructure Controller (APIC), tout en déléguant la configuration L4-L7 à NetScaler ADM, qui fait office de gestionnaire de périphériques dans l'APIC.

La solution NetScaler Hybrid Mode est prise en charge par un package de périphériques en mode hybride et NetScaler ADM. Vous devez télécharger le package de périphérique en mode hybride dans l'APIC. Pour plus d'informations, consultezNetScaler Automation à l'aide de NetScaler ADM en mode hybride de Cisco ACI.

OpenStack : intégration d'instances NetScaler

February 1, 2024

La fonctionnalité Cloud Orchestration de NetScaler Application Delivery Management (ADM) permet l'intégration des produits NetScaler à la plateforme OpenStack. En utilisant cette fonctionnalité avec la plate-forme OpenStack, les utilisateurs d'OpenStack peuvent bénéficier de la fonctionnalité d'équilibrage de charge (LBaaS) de NetScaler. Ensuite, les utilisateurs d'OpenStack peuvent déployer leurs configurations d'équilibreur de charge depuis OpenStack dans une instance NetScaler.

Les sections suivantes fournissent une brève description des fonctionnalités du flux de travail d'intégration de NetScaler ADM et OpenStack.

Pilote NetScaler pour OpenStack Neutron LBaaS

Le plug-in OpenStack Neutron LBaaS inclut un pilote NetScaler qui permet à OpenStack de communiquer avec NetScaler ADM. OpenStack utilise ce pilote pour transmettre toute configuration d'équilibrage de charge effectuée via les API LBaaS à NetScaler ADM, qui crée la configuration de l'équilibreur de charge sur les instances NetScaler souhaitées. OpenStack utilise également le pilote pour appeler NetScaler 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 NetScalers. Le logiciel pilote NetScaler pour la plate-forme OpenStack est fourni avec NetScaler ADM. Pour télécharger et installer les pilotes, vous devez d'abord installer NetScaler ADM et lancer l'application.

Enregistrement mutuel de NetScaler ADM et d'OpenStack

Vous devez d'abord enregistrer les informations OpenStack sur NetScaler ADM. Spécifiez l'adresse IP du contrôleur OpenStack et les informations d'identification utilisateur administratives du cloud, ainsi que les informations d'identification utilisateur du pilote OpenStack NetScaler. Vous pouvez ensuite spécifier les mêmes informations de connexion dans la section NetScaler_Driver du fichier de configuration Neutron (neutron.conf) afin que le pilote NetScaler d'OpenStack puisse se connecter à NetScaler ADM lors des configurations LB.

Une fois qu'OpenStack et NetScaler ADM sont enregistrés l'un avec l'autre, les deux peuvent communiquer entre eux. Les utilisateurs d'OpenStack peuvent également utiliser leurs informations d'identification existantes dans OpenStack pour se connecter à l'interface utilisateur de NetScaler ADM afin de vérifier les performances de leurs configurations LB dans NetScalers.

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 choisir l'instance NetScaler à utiliser dans chaque configuration d'équilibreur de charge créée par les utilisateurs. NetScaler ADM propose également une option permettant d'attribuer une instance NetScaler 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 package de service configuré pour le provisionnement automatique, les instances virtuelles NetScaler 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 NetScaler ADM à OpenStack Workflow
- Prerequisites

- Tâches de préconfiguration dans NetScaler 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
- Provisioning manuel de l'instance NetScaler VPX sur OpenStack
- Intégration de NetScaler ADM à OpenStack Heat Services
- Surveillance des applications OpenStack dans NetScaler ADM

Scénario de cas d'utilisation

Le scénario d'utilisation suivant explique le processus d'intégration de NetScaler ADM à la plateforme 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, a besoin de deux serveurs S1 et S1, et Tom a également besoin d'un appareil NetScaler dédié pour équilibrer la charge du trafic entre les serveurs S1 et S2 sur la plateforme OpenStack.

Pour répondre à cette exigence, Steve doit installer et configurer à la fois OpenStack et NetScaler ADM, et les préparer pour qu'ils soient compatibles entre eux. 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 d'OpenStack auprès de NetScaler ADM et configurer le pilote NetScaler LBaaS dans le composant réseau OpenStack, Neutron. Une fois l'enregistrement terminé, NetScaler ADM affiche les détails de tous les locataires d'OpenStack. Steve peut sélectionner Example-SportsOnline dans la liste qui souhaite bénéficier des fonctionnalités LBaaS de NetScaler et configurer Tom pour qu'un NetScaler dédié soit affecté à ses configurations d'équilibreur de charge dans NetScaler ADM.

Pour cela, Steve peut soit provisionner une instance NetScaler VPX sur la couche informatique (Nova) d'OpenStack à l'aide de l'interface utilisateur NetScaler ADM, soit permettre à MAS de provisionner automatiquement une instance NetScaler VPX à la demande, lorsque Tom effectue sa configuration LB dans OpenStack. Dans les deux cas, NetScaler ADM gère l'instance VPX. Pour ce faire, Steve crée un package de service dans NetScaler 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

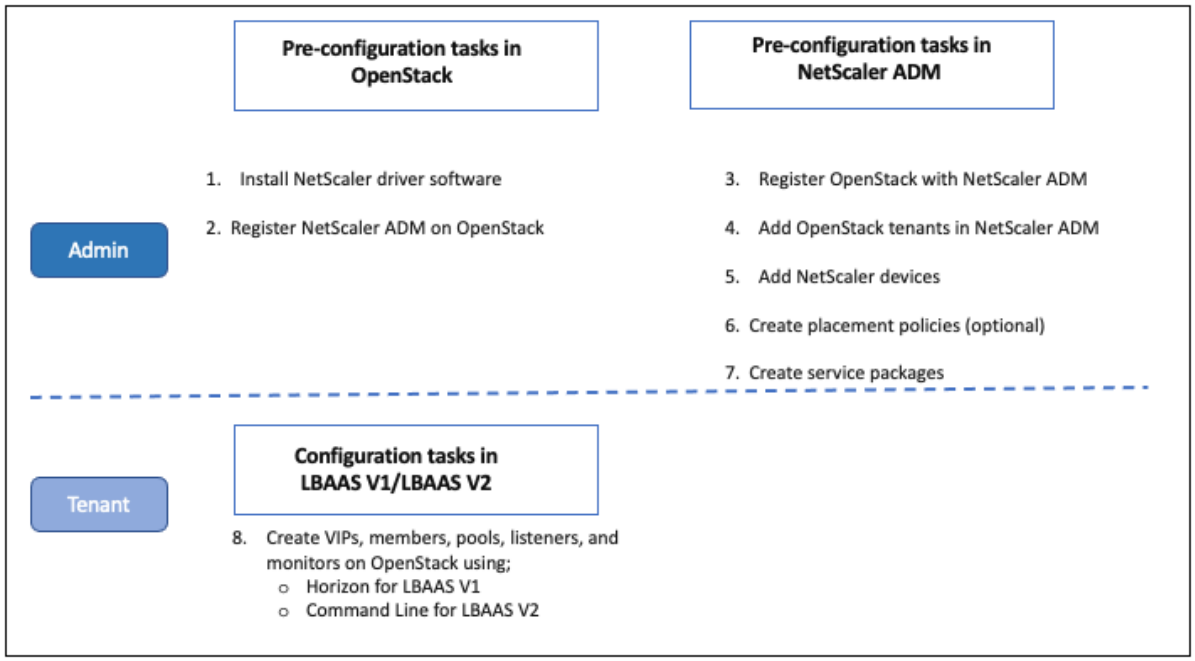
à Tom. Autrement dit, Steve sélectionne une instance non partagée pour Tom dans le package de services. Il attribue ensuite de nombreuses instances NetScaler VPX au package de services et associe Example-SportsOnline, ainsi qu'à d'autres locataires, qui ont besoin d'un NetScaler dédié au package de services. Par conséquent, lorsque Tom effectue sa première configuration d'équilibreur de charge, NetScaler ADM attribue l'une des instances NetScaler VPX du package de service à Example-SportsOnline et déploie également sa configuration dans ce NetScaler.

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 d'OpenStack sont déployés sous forme de groupes de services et de serveurs virtuels sur l'instance NetScaler. Tom peut également créer des moniteurs de santé pour surveiller les serveurs et envoyer le trafic des applications uniquement aux serveurs qui sont opérationnels à tout moment et accessibles depuis NetScaler.

La configuration d'équilibrage de charge créée dans OpenStack est désormais implémentée sur l'instance NetScaler. Une fois entièrement configurée, l'instance NetScaler VPX prend alors en charge la fonctionnalité d'équilibrage de charge et commence à accepter le trafic des applications et à équilibrer le trafic entre les serveurs S1 et S2 créés par Tom.

Intégration de NetScaler ADM à OpenStack Workflow

L'organigramme suivant illustre le flux de travail que vous devez suivre lorsque vous configurez LBaaS V1 et LBaaS V2.



NSX Manager : provisionnement manuel des instances NetScaler

February 1, 2024

NetScaler Application Delivery Management (ADM) s'intègre à la plateforme de virtualisation réseau VMware pour automatiser le déploiement, la configuration et la gestion des services NetScaler. Cette intégration élimine les complexités traditionnelles associées à la topologie physique du réseau, ce qui permet aux administrateurs de vSphere/vCenter de déployer les services NetScaler plus rapidement par programmation.

Cet article fournit une liste des tâches que vous devez effectuer à la fois sur VMware NSX Manager et sur NetScaler 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 NetScaler ADM sur l'un des hyperviseurs pris en charge.

  Pour les tâches relatives à l'installation de NetScaler ADM build 13.1 sur l'un des hyperviseurs pris en charge, consultez la section Déploiement de NetScaler 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 un dispositif virtuel NetScaler 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 NetScaler 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.

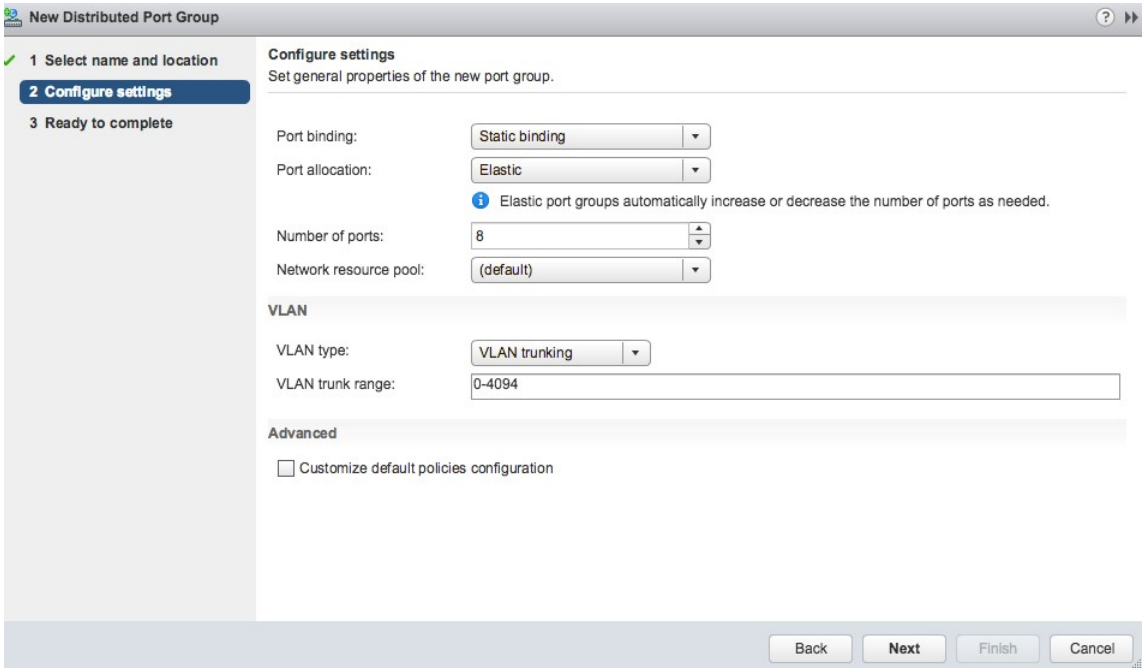
Configuration de VMware NSX

- Créez un pool d'instances NetScaler VPX de différentes capacités, qui sont ajoutées aux différents packages de services.

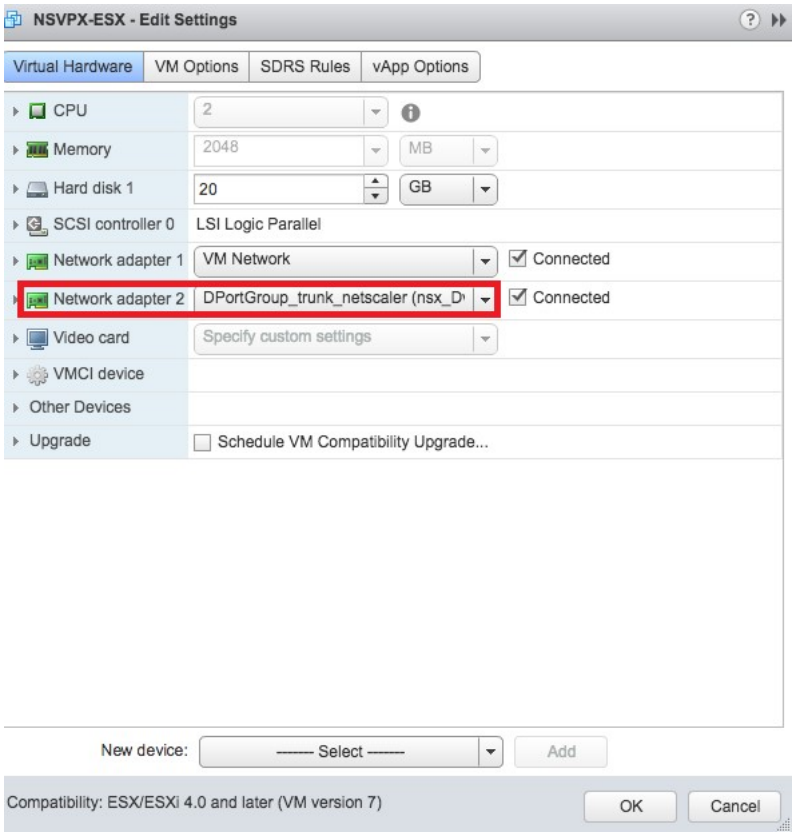
Par exemple :

- Créez cinq instances NetScaler VPX de VPX1000 (1 Gbit/s). Ces instances sont ajoutées au package de service Gold.
- Créez cinq instances NetScaler 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).

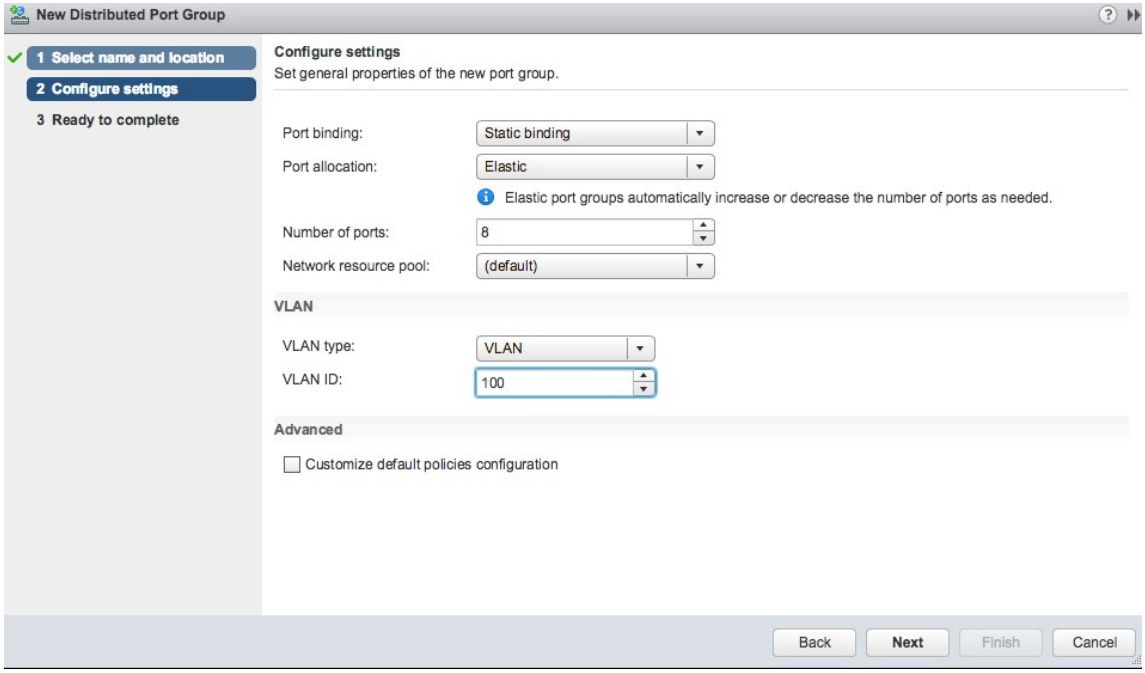


2. Créez une nouvelle interface pour chaque instance NetScaler VPX et attachez-la au groupe de ports de jonction de la plage VLAN créé ci-dessus.



3. Dans vSphere Client, accédez à **Mise en réseau**et créez un groupe de ports de type VLAN.

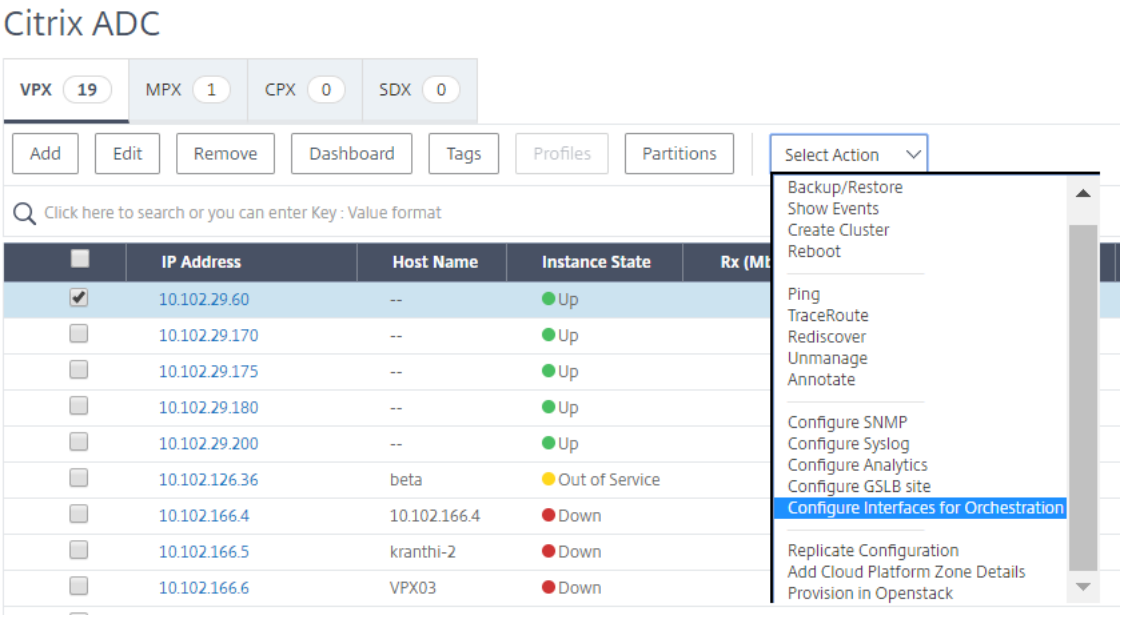
Par exemple, si le groupe de ports tronqués initial a été créé avec la plage 101 à 105, créez cinq groupes de ports VLAN un par VLAN, c'est-à-dire un groupe de ports avec VLAN 101, un autre avec VLAN102, etc., jusqu'à VLAN 105.



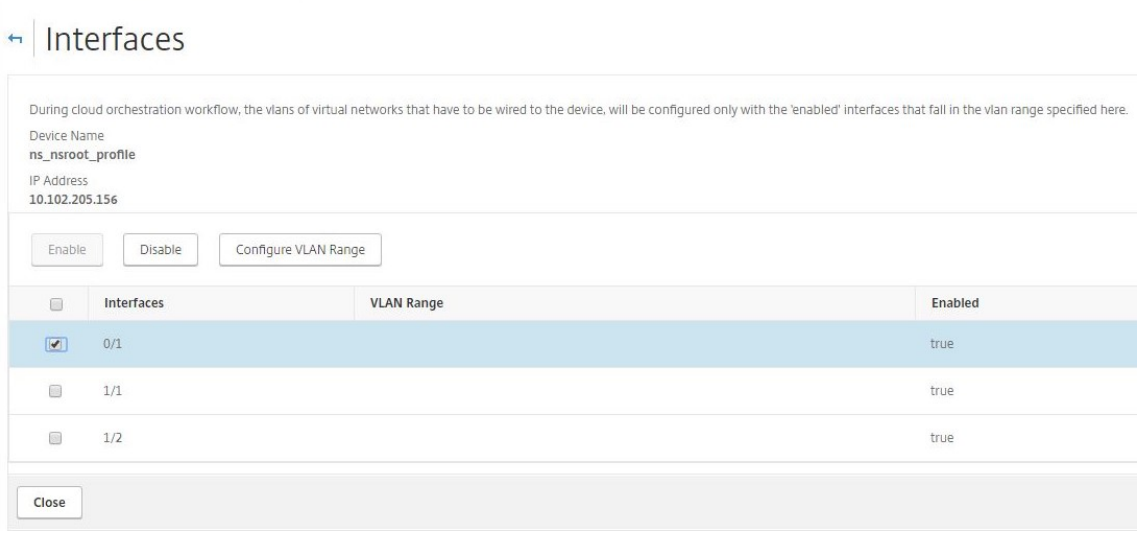
Ajouter une instance NetScaler VPX dans NetScaler ADM

Ajoutez des instances NetScaler VPX dans NetScaler ADM et spécifiez la plage de VLAN du groupe agrégé pour chaque appareil.

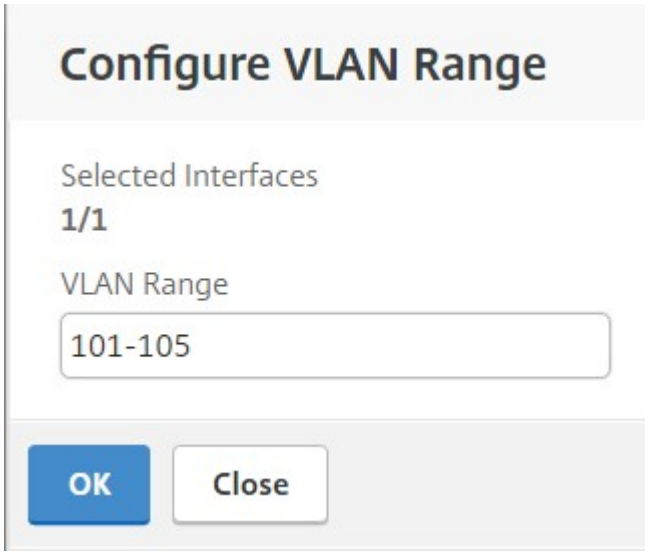
1. Dans NetScaler ADM, accédez à **Infrastructure** > **Instances NetScaler VPX**, puis cliquez sur **Ajouter**.
2. Sur la page **Ajouter un NetScaler VPX**, spécifiez les noms d'hôte des instances, l'adresse IP de chaque instance ou une plage d'adresses IP, puis sélectionnez un profil d'instance dans 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 NetScaler VPX récemment ajoutée dans la liste de la page **NetScaler VPX**, puis cliquez sur la 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.



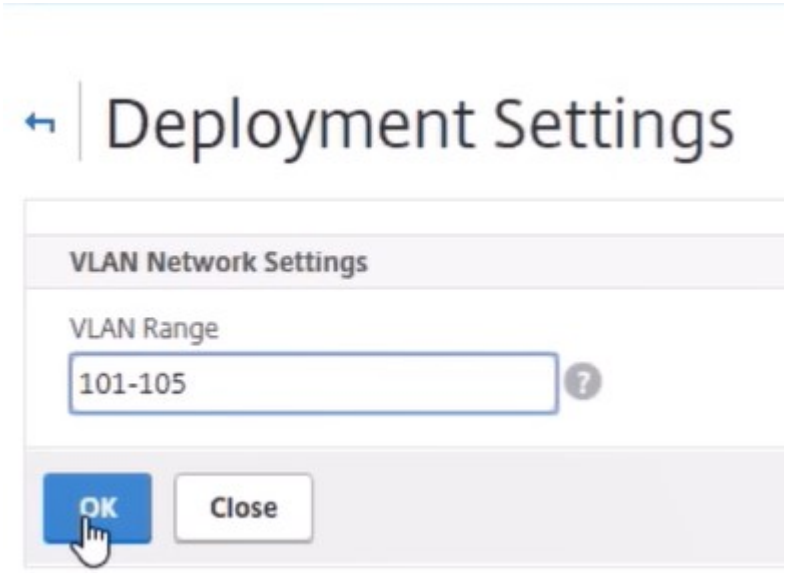
6. Sur la page **Interfaces**, sélectionnez l'interface requise, puis cliquez sur **Configurer VLAN Range**.
7. Entrez la plage de VLAN configurée dans NSX Manager, cliquez sur **OK**, puis cliquez sur **Fermer**.



Enregistrement de VMware NSX Manager auprès de NetScaler ADM

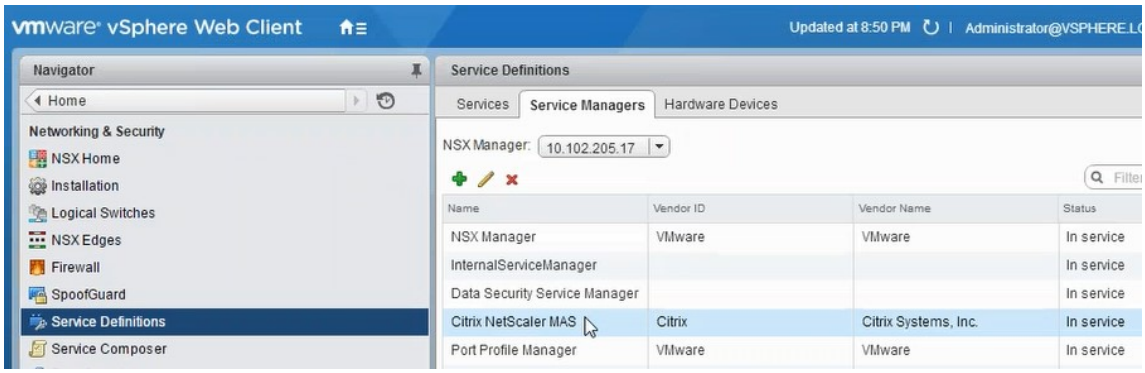
Enregistrez VMware NSX Manager auprès de NetScaler ADM pour créer un canal de communication entre eux.

1. Dans NetScaler 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 la section **Compte NetScaler ADM utilisé par NSX** Manager, définissez le nom d'utilisateur et le mot de passe du pilote NetScaler pour NSX Manager. NetScaler ADM authentifie les demandes de configuration de l'équilibreur de charge provenant de NSX Manager à l'aide de ces informations d'identification de connexion.
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 considérer Citrix NetScaler ADM comme l'un des gestionnaires de services. Cela indique que l'enregistrement est réussi et qu'un canal de communication est établi entre NSX Manager et NetScaler ADM.

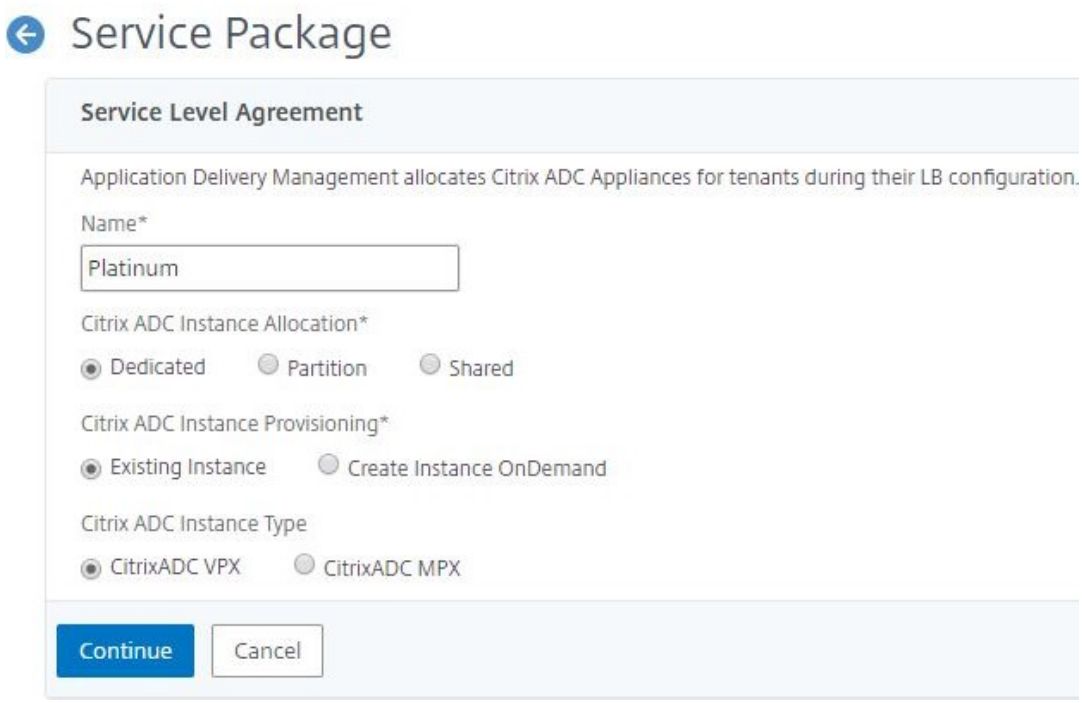


Création d'un package de services dans NetScaler ADM

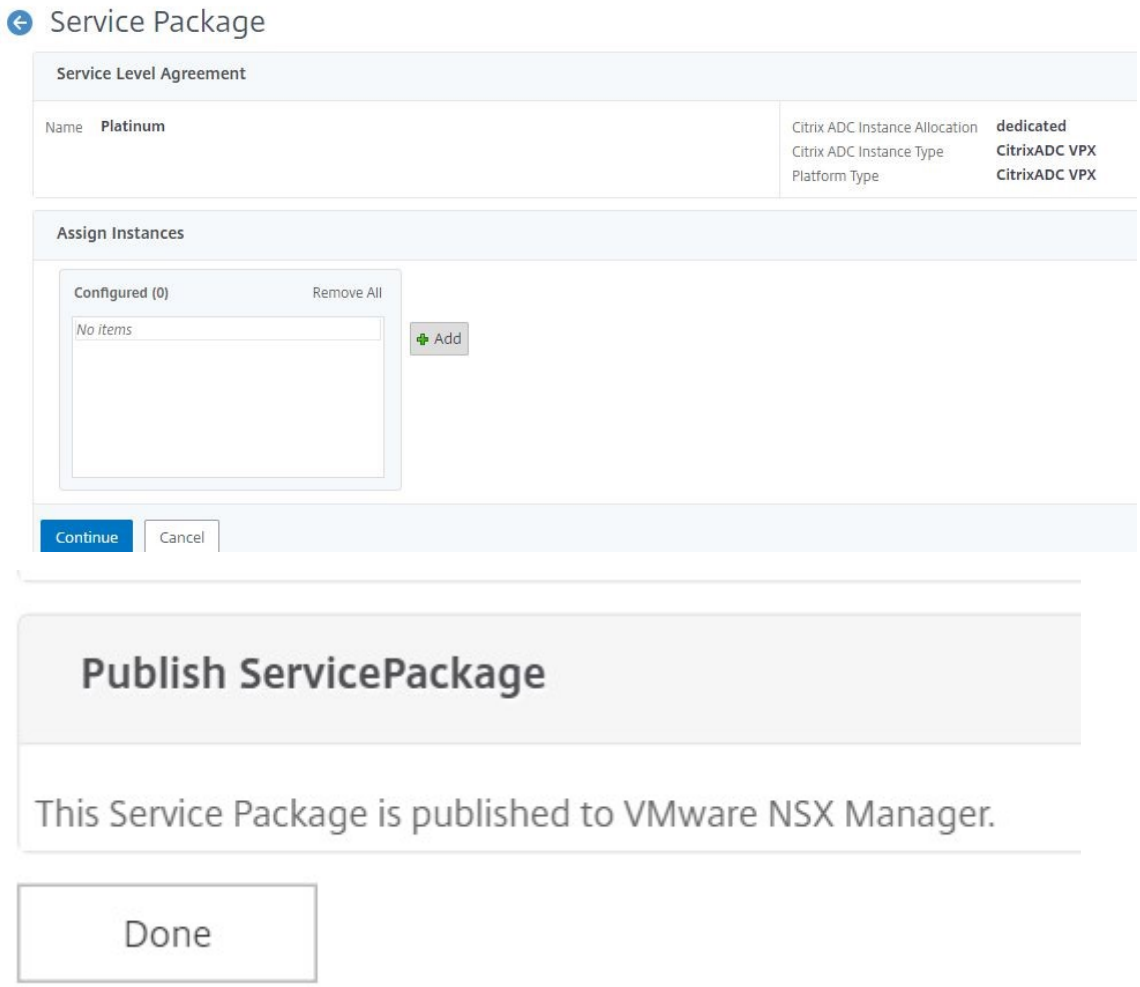
1. Dans NetScaler ADM, accédez à **Orchestration** > **SDN Orchestration**> **VMware NSXManager** > **Service Packages**, puis cliquez sur **Ajouter** pour ajouter un nouveau service package.
2. Dans la page **Service Package**, dans la section **Paramètres de base**, définissez les paramètres suivants :
   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 d'appareil : par défaut, le type d'appareil est défini sur NetScaler 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 appareils peuvent être ajoutés à un service et plusieurs périphériques peuvent utiliser le même package de service pour décharger l'instance NetScaler VPX vers NetScaler ADM.

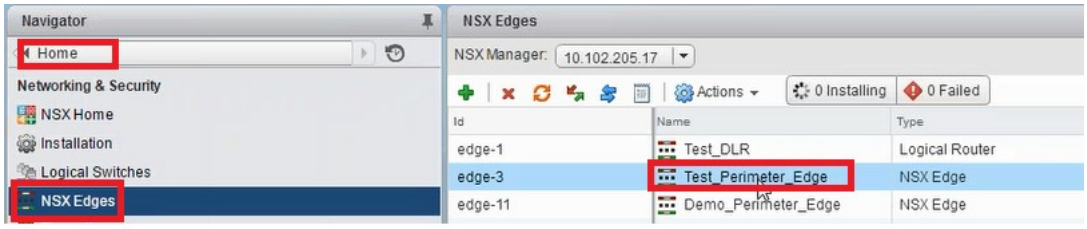
5. Ouvrez une session sur NSX Manager sur vSphere Web Client et accédez à **Définitions de service** > **Services**.

   Vous pouvez voir que le package de service NetScaler ADM est enregistré.

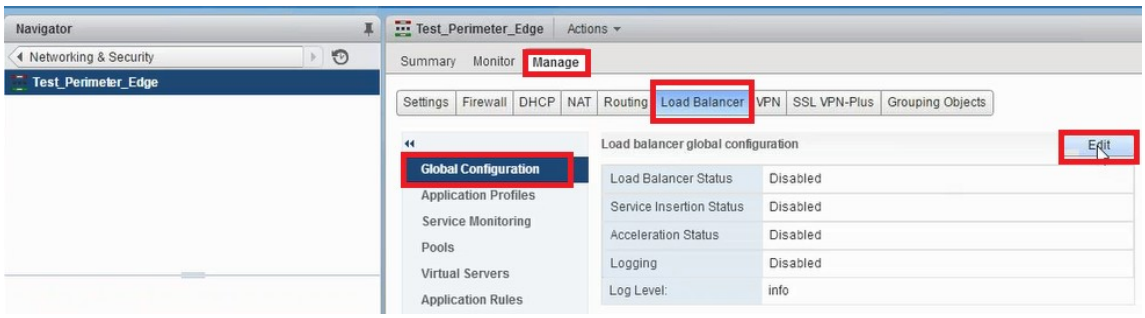
Exécution de l'insertion du service d'équilibrage de charge pour Edge

Procédez à l'insertion du service d'équilibrage de charge sur la passerelle NSX Edge créée précédemment (déchargez la fonction d'équilibrage de charge de NSX LB vers NetScaler).

1. Dans NSX Manager, accédez à **Accueil** > **NSX Edge**, puis sélectionnez la Gateway périphérique que vous avez configurée.

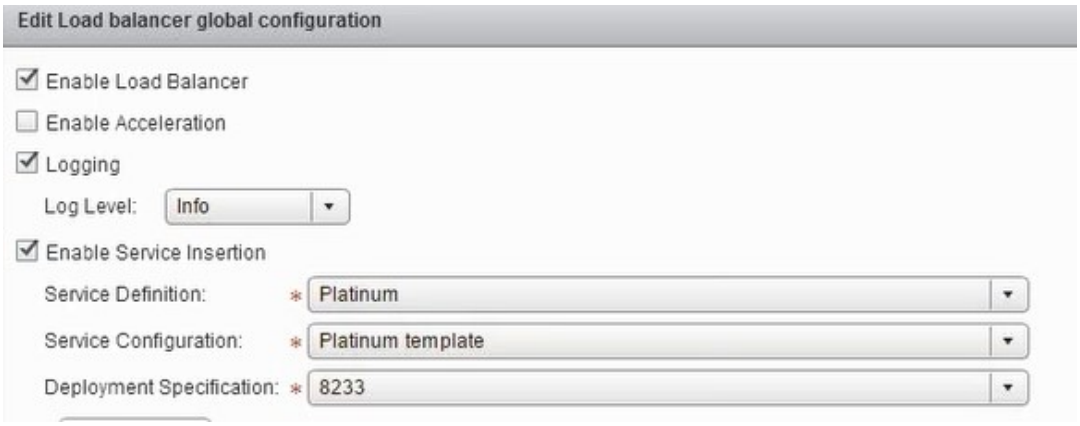


2. Cliquez sur **Gérer**, puis sur l'onglet **Équilibreur** de charge, sélectionnez **Configuration globale**, puis cliquez sur **Modifier**.

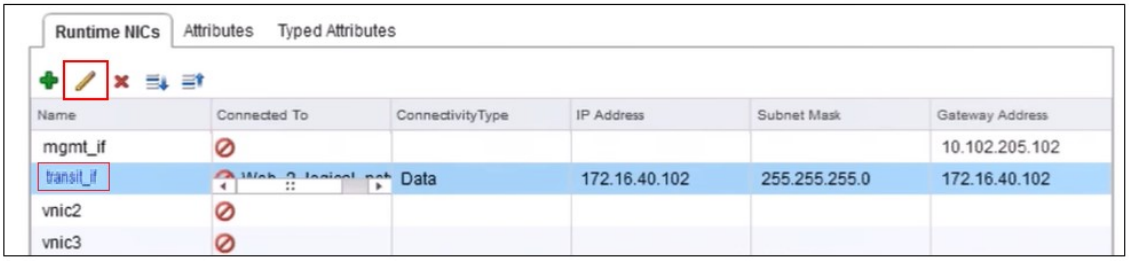


3. Sélectionnez **Activer l'équilibreur**de charge, **Journalisation**, **Activer l'insertion de service** pour les activer.

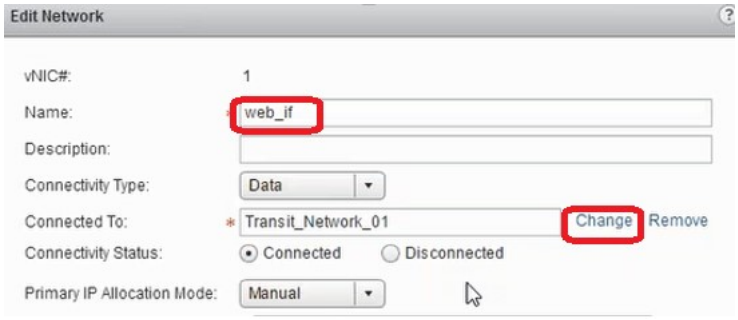
   a) Dans **Définition du service,** sélectionnez le package de service qui a été créé dans NetScaler ADM et publié sur NSX Manager.



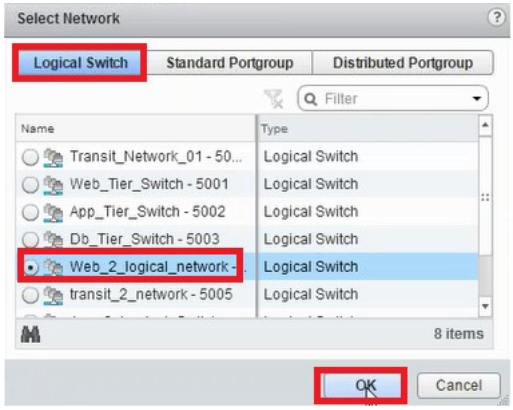
4. Sélectionnez les cartes réseau d'exécution existantes et cliquez sur l'icône Modifier pour modifier les cartes réseau d'exécution qui doivent être connectées lorsque NetScaler VPX est alloué.



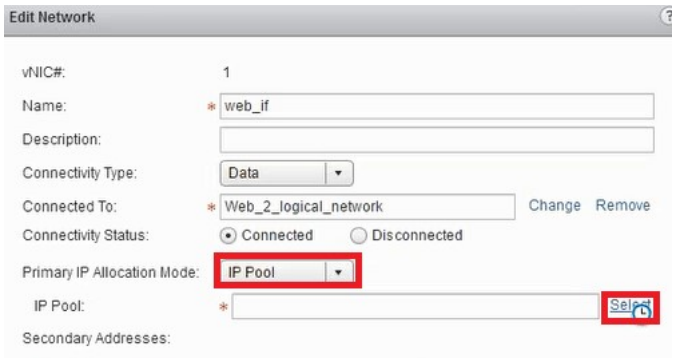
5. Modifiez le nom de la carte réseau, spécifiez le type de connectivité en tant que **données**, puis cliquez sur **Modifier**.



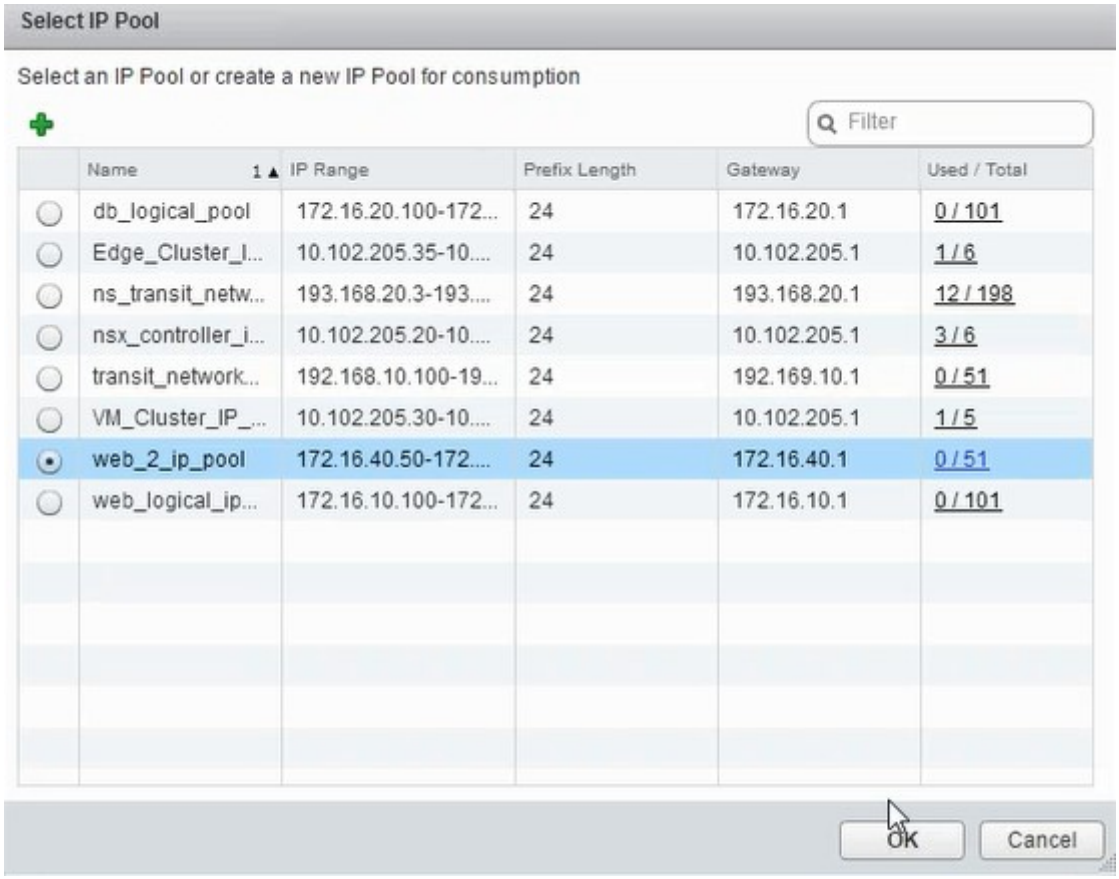
6. Sélectionnez le commutateur logique Web approprié.



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.



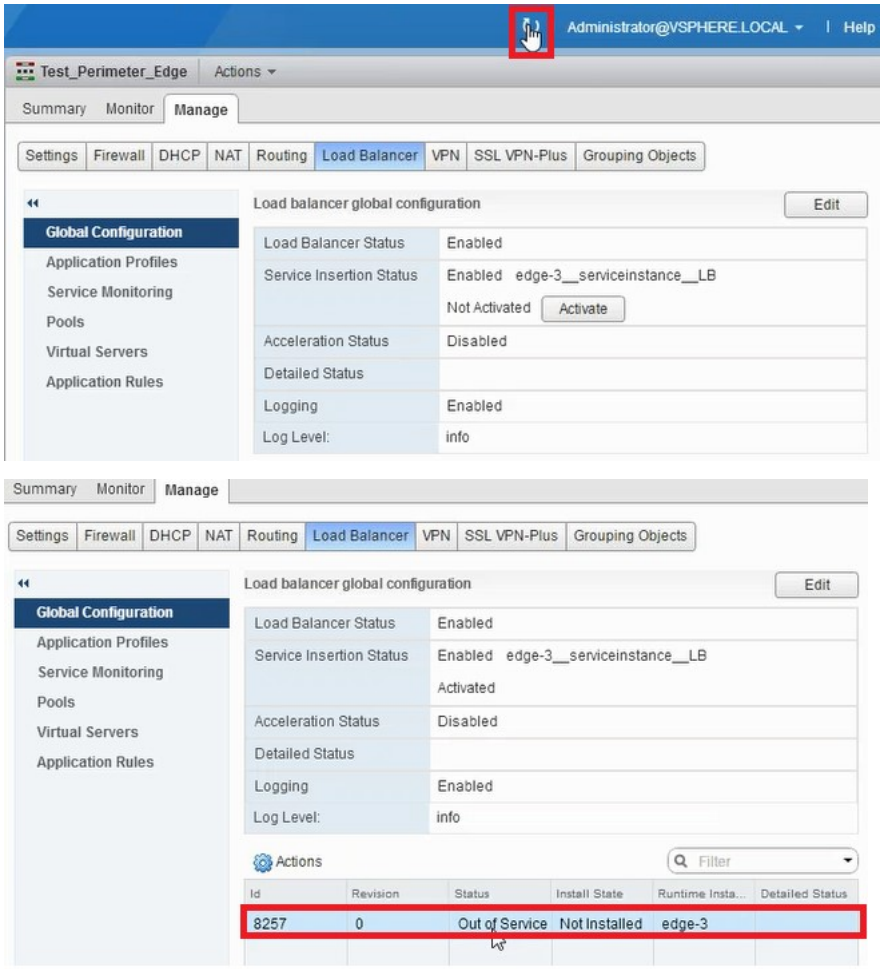
8. Dans la fenêtre **Sélectionner un pool d'adresses IP**, sélectionnez le pool d'adresses IP approprié, puis cliquez sur **OK**.



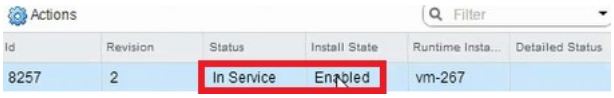
L'adresse IP est acquise et définie comme adresse IP réseau source dans l'appliance NetScaler VPX. Une Gateway L2 est créée dans NSX Manager pour mapper le VXLAN au VLAN.

> **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.



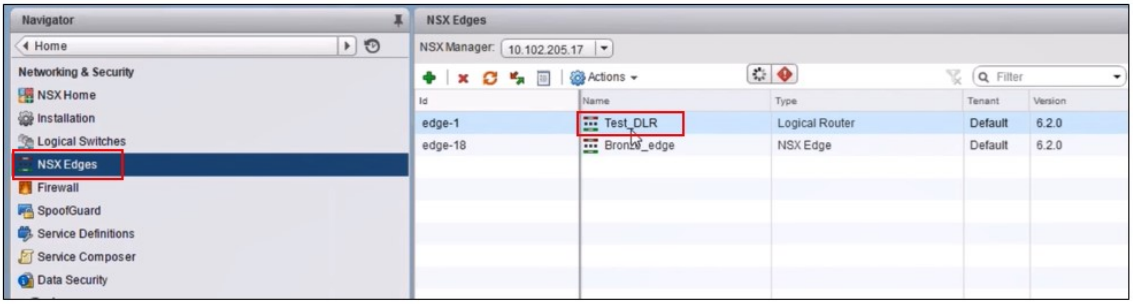
10. Une fois la machine virtuelle démarrée, la valeur de l'état passe à **En service** et celle de l'état d'installation passe à **Activé**.



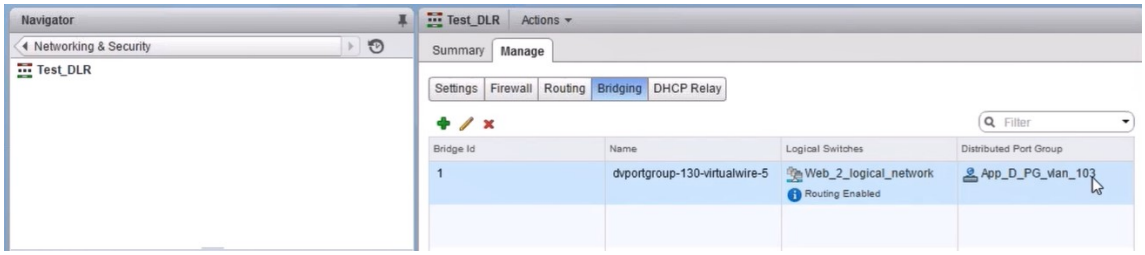
> **Remarque**
>
> Dans NetScaler ADM, accédez à **Orchestration** > **Requêtes** pour voir les détails de la progression de l'insertion du service LB.

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.



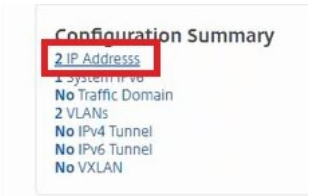
2. Dans la page DLR, accédez à **Gérer** > **Bridging**. Vous pouvez voir la Gateway L2 affichée dans la liste.



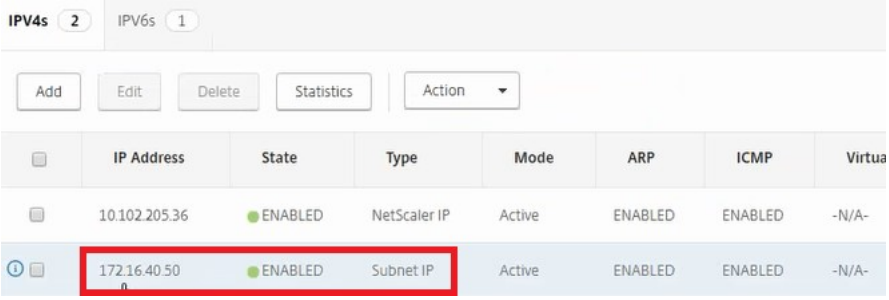
> **Remarque**
>
> Une Gateway L2 est créée pour chaque interface de données.

Affichage du NetScaler alloué

1. Connectez-vous à l'instance NetScaler VPX à l'aide de l'adresse IP affichée dans NetScaler 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 NetScaler VPX à l'aide de StyleBook

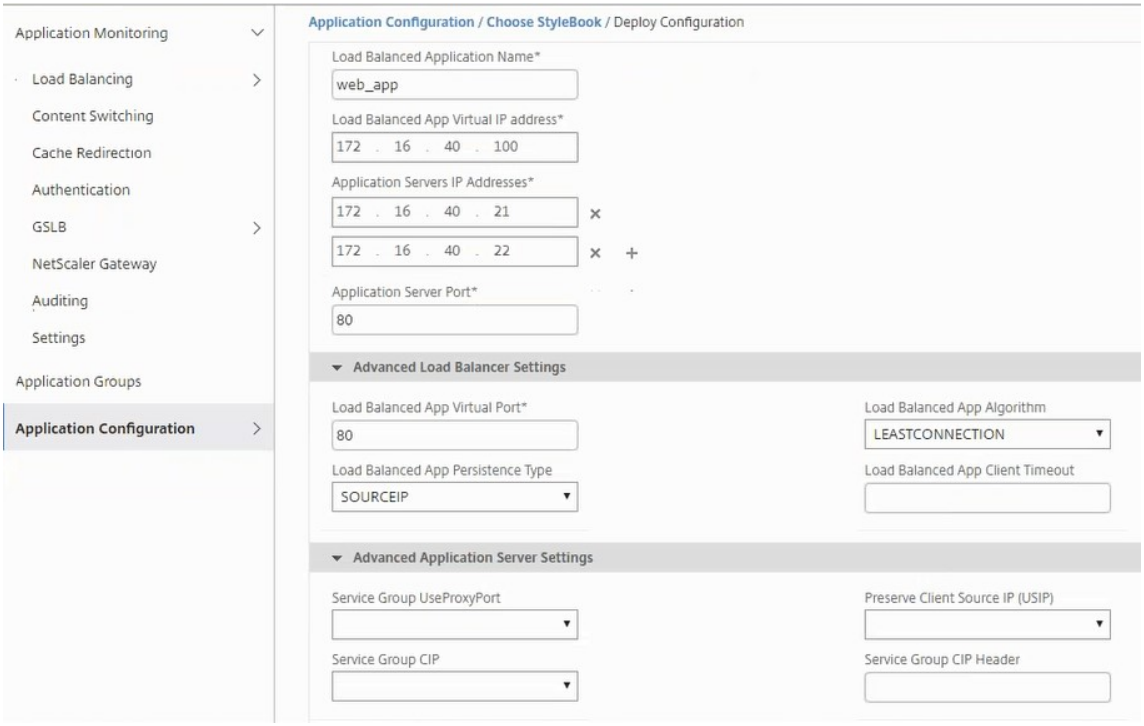
1. Dans NetScaler ADM, accédez à **Orchestration** > **SDN Orchestration** > **Configurer NSX Manager** > **Edge Gateways**.

   Notez l'adresse IP de l'instance NetScaler qui est allouée à la passerelle Edge correspondante sur laquelle la configuration d'équilibrage de charge via StyleBooks doit être appliquée.

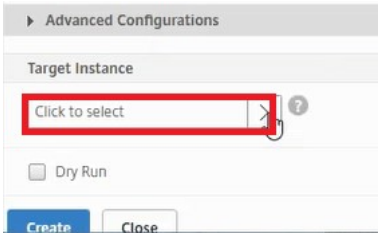
2. Créez un nouveau StyleBook. Accédez à **Applications** > **Configuration**, importez le StyleBook et sélectionnez le StyleBook dans la liste.

   Pour créer un nouveau StyleBook, voir Créer votre propre StyleBook.

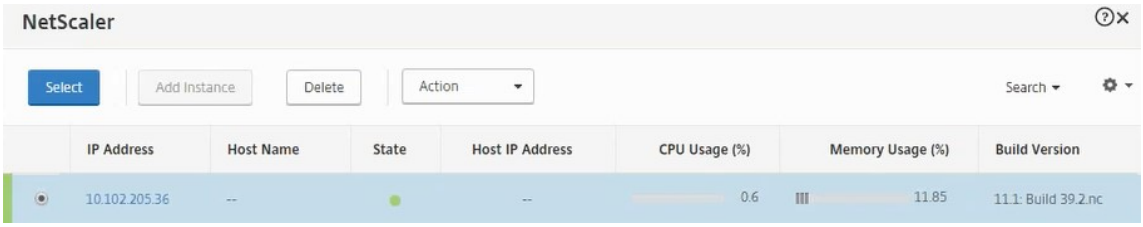
3. Spécifiez des valeurs pour tous les paramètres requis.



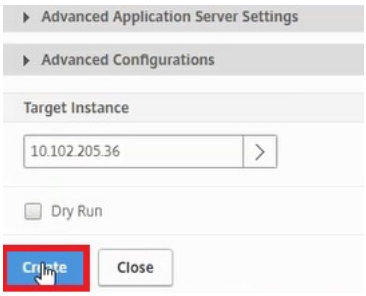
4. Spécifiez l'instance NetScaler VPX sur laquelle vous souhaitez exécuter ces paramètres de configuration.



5. Sélectionnez l'instance IP mentionnée précédemment, puis cliquez sur **Sélectionner**.

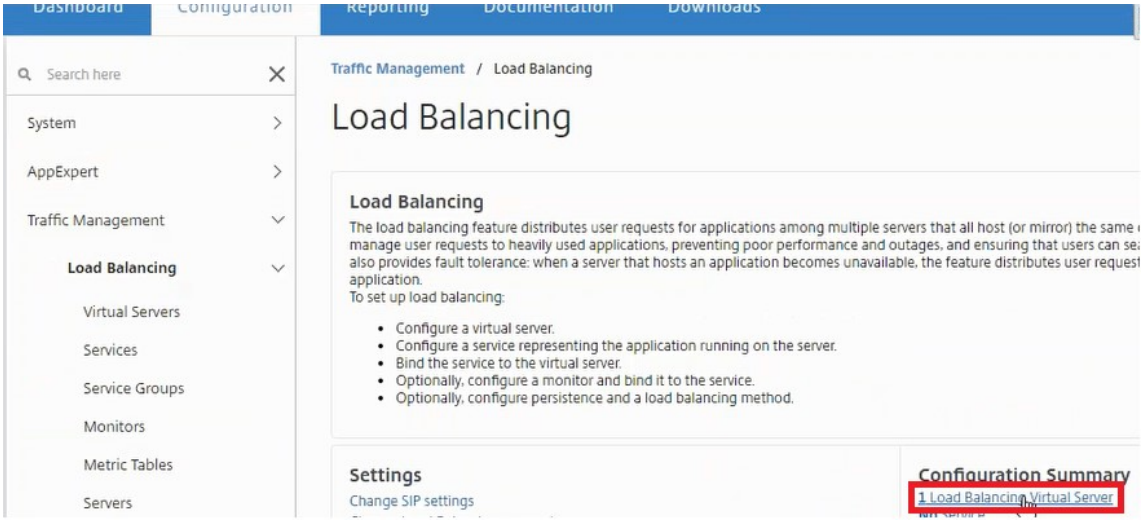


6. Cliquez sur **Créer** pour appliquer la configuration sur le périphérique sélectionné.

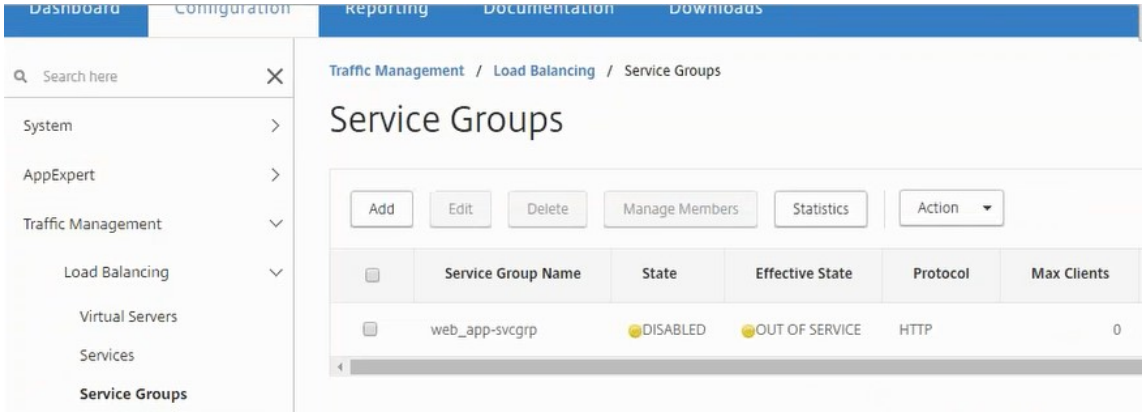


Affichage de la configuration de l'équilibreur de charge

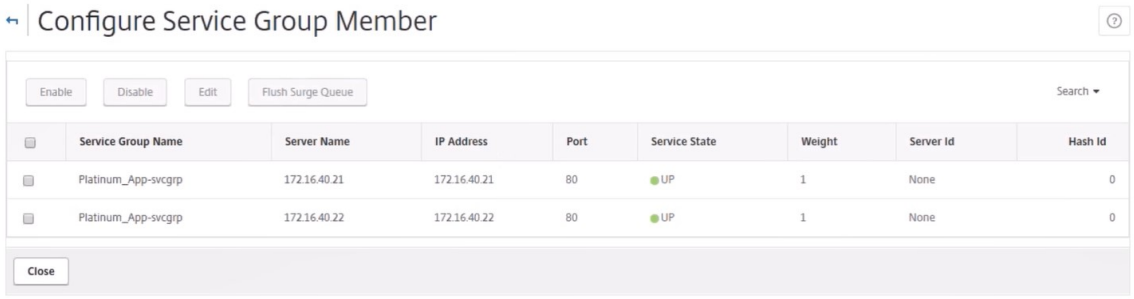
1. Connectez-vous à l'instance NetScaler VPX, accédez à **Configuration** > **Gestion du trafic** > **Équilibrage de charge** pour afficher le serveur virtuel d'équilibrage de charge créé.



Vous pouvez également afficher les groupes de services créés.



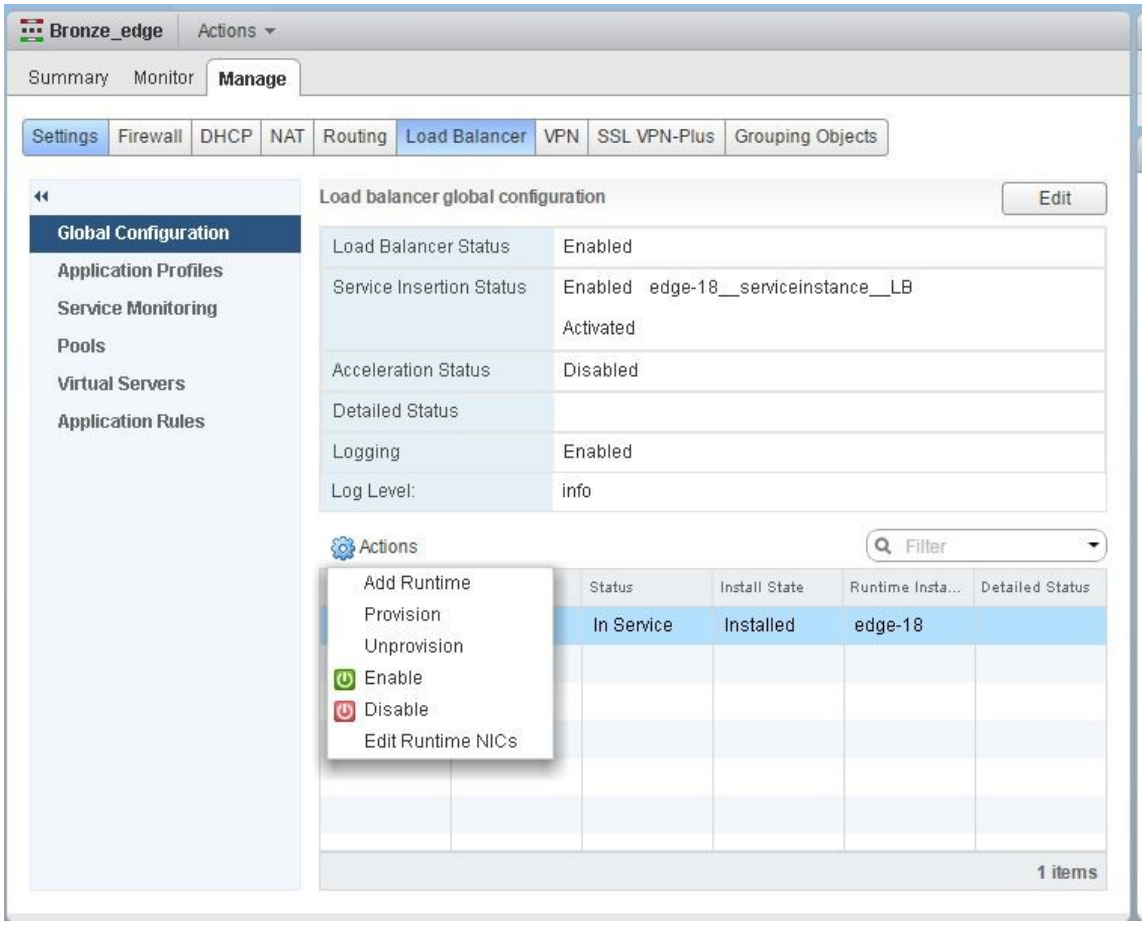
2. Sélectionnez le groupe de services, puis cliquez sur **Gérer les membres**. La page **Configurer un membre de groupe de services** affiche les membres associés au groupe de services.



Suppression du service d'équilibrage de charge

1. Dans NetScaler 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 passerelle Edge à laquelle l'instance NetScaler 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**
>
> Les passerelles Edge dans NetScaler ADM correspondent aux entrées d'exécution de NSX Manager.



L'instance NetScaler VPX est mise hors service.

4. Dans NetScaler 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 : provisionnement automatique des instances NetScaler

February 1, 2024

Vue d'ensemble

NetScaler Application Delivery Management (ADM) s'intègre à la plateforme de virtualisation réseau VMware pour automatiser le déploiement, la configuration et la gestion des services NetScaler. Cette intégration élimine les complexités traditionnelles associées à la topologie physique du réseau, ce qui

permet aux administrateurs de vSphere/vCenter de déployer les services NetScaler plus rapidement par programmation.

Lors de l'insertion et de la suppression du service d'équilibrage de charge sur VMware NSX Manager, NetScaler ADM provisionne et détruit dynamiquement les instances NetScaler. Ce provisionnement dynamique nécessite que les attributions de licences NetScaler VPX soient automatisées dans NetScaler ADM. Lorsque les licences NetScaler sont téléchargées sur NetScaler ADM, NetScaler 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**.

- NetScaler ADM, version 13.0 configuré en haute disponibilité et installé sur ESX.
- NetScaler VPX, version 13.0
- Licences NetScaler VPX pour les instances NetScaler 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 à haute disponibilité des instances NetScaler ADM et NetScaler

Pour configurer la configuration NetScaler ADM HA, installez le fichier image NetScaler ADM que vous avez téléchargé depuis le site NetScaler. Pour plus d'informations sur le provisionnement de la configuration de NetScaler ADM HA, consultez la section Déploiement de NetScalerADM en haute disponibilité.

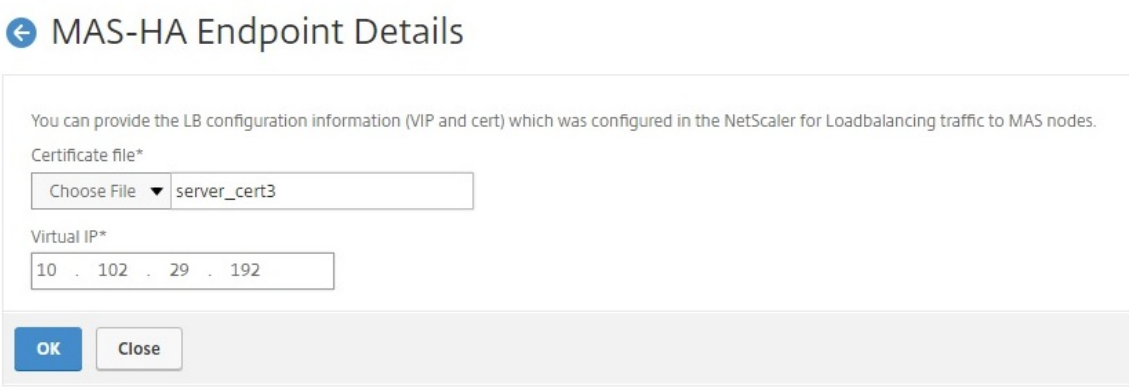
Détails de configuration du point de terminaison NetScaler ADM HA

Pour intégrer VMware NSX Manager à NetScaler ADM déployé en mode HA, vous devez d'abord saisir l'adresse IP virtuelle de l'instance d'équilibrage de charge NetScaler. Vous devez également télécharger le fichier de certificat présent sur le serveur virtuel d'équilibrage de charge NetScaler vers le système de fichiers NetScaler ADM.

Pour fournir des informations de configuration d'équilibrage de charge dans NetScaler ADM, procédez comme suit :

1. Dans le nœud NetScaler 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 **MAS-HA Endpoint Details**, téléchargez le même certificat qui est déjà présent sur l'instance NetScaler d'équilibrage de charge.
4. **Entrez l'adresse IP virtuelle de l'instance d'équilibrage de charge NetScaler et cliquez sur OK.**



Enregistrement de VMware NSX Manager auprès de NetScaler ADM

Lorsque vous configurez deux serveurs NetScaler ADM en haute disponibilité, les deux nœuds du serveur sont en mode actif-passif. Connectez-vous au nœud de serveur NetScaler ADM principal pour enregistrer VMware NSX Manager auprès de NetScaler ADM en HA, afin de créer un canal de communication entre eux.

Pour enregistrer VMware NSX Manager auprès de NetScaler ADM en mode HA :

1. Dans le nœud principal du serveur NetScaler ADM, 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 NetScaler ADM utilisé par NSX Manager, définissez le mot de passe du pilote NetScaler pour NSX Manager.
5. Cliquez sur **OK**.

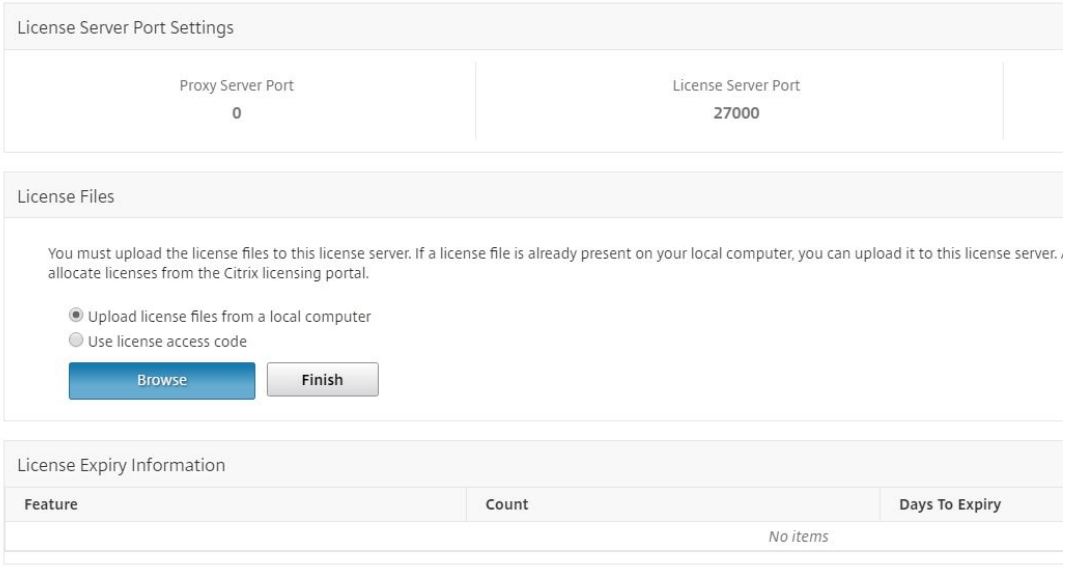
Chargement de licences dans NetScaler ADM

Téléchargez les licences NetScaler VPX vers NetScaler ADM, afin que NetScaler ADM puisse attribuer automatiquement des licences aux instances lors de l'orchestration avec NSX.

Pour installer les fichiers de licence sur NetScaler ADM :

1. Dans NetScaler ADM, accédez à **Infrastructure**Licences groupées.
2. Dans la section **Fichiers de licence**, sélectionnez l'une des options suivantes :
    a) **Charger des fichiers de licence depuis un ordinateur local** : si un fichier de licence est déjà présent sur votre ordinateur local, vous pouvez le télécharger sur NetScaler 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 NetScaler ADM à partir des paramètres de licence.



Chargement d'images NetScaler VPX dans NetScaler ADM

Ajoutez les images NetScaler à NetScaler ADM, afin que NetScaler ADM utilise ces images comme défini dans le package de service.

Pour charger des images NetScaler VPX dans NetScaler ADM :

1. Dans NetScaler ADM, accédez à **Orchestration** > **SDN Orchestration** > **VMware NSX Manager** > **Images ESX NSVPX**.
2. Cliquez sur **Charger**, puis sélectionnez le package zip NetScaler VPX dans le dossier de stockage local.

Création de packages de service dans NetScaler ADM

Créez des packages de service dans NetScaler ADM pour définir l'ensemble des SLA, qui indiquent comment les ressources NetScaler sont allouées.

Pour créer des packages de service dans NetScaler ADM :

1. Dans NetScaler ADM, accédez à **Orchestration** > **SDN Orchestration**> **VMware NSXManager** > **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**

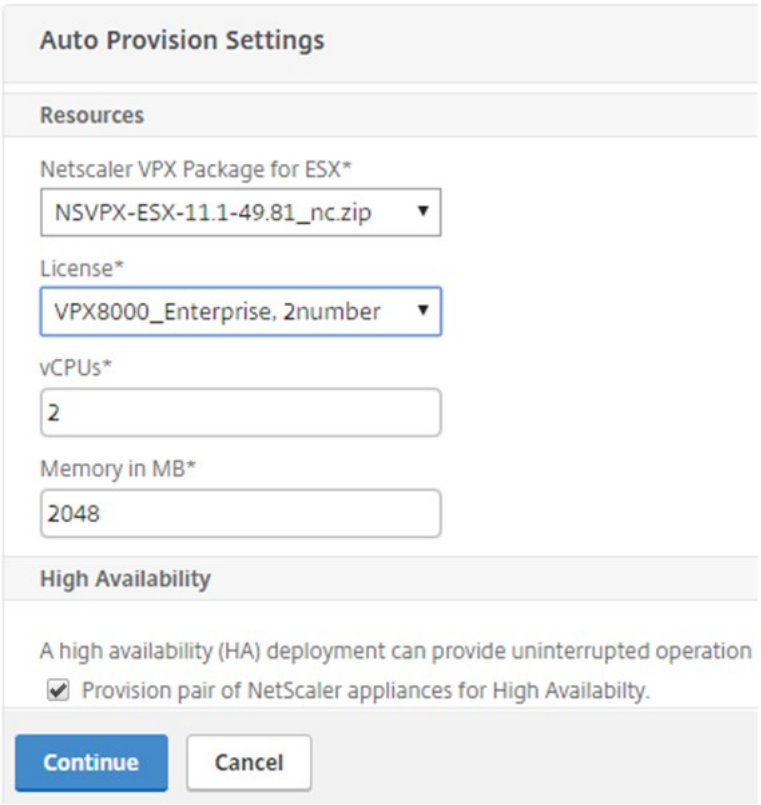
c) **Provisioning d'instances NetScaler : sélectionnez Créer une instance à la demande**

d) Plateforme d'approvisionnement automatique : sélectionnez **Citrix**NetScaler SDX

e) Cliquez sur **Continue**.

3. Dans la section **Paramètres de provisionnement automatique**, sélectionnez le package zip NetScaler VPX récemment téléchargé pour le déployer sur la plateforme NSX, sélectionnez la licence correspondante et cliquez sur **Continuer**.

> **Remarque**
>
> Dans **la section Haute disponibilité**, cochez la case pour provisionner des instances NetScaler 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 permet de déployer des instances NetScaler VPX
> - 8000 - la bande passante consommable est de 8 Go
> - Avancé : NetScaler propose trois types de licences : Standard, Advanced et Premium

> - Numéro 2 : deux instances NetScaler 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 considérer NetScaler ADM comme l'un des gestionnaires de services. Cela indique que l'enregistrement est réussi et qu'une communication bidirectionnelle est établie entre le gestionnaire NSX et NetScaler ADM.

> **Remarque**
>
> Pour NetScaler ADM dans le cadre d'un déploiement à haute disponibilité, les licences sont téléchargées uniquement sur le nœud du serveur de licences NetScaler ADM. Les nœuds NetScaler ADM sont en mode actif-passif.

Exécution de l'insertion du service d'équilibrage de charge pour Edge

Procédez à l'insertion du service d'équilibrage de charge sur la passerelle NSX Edge Gateway existante, c'est-à-dire déchargez la fonction d'équilibrage de charge de l'équilibreur de charge NSX vers NetScaler.

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. NetScaler ADM ne prend pas en charge l'allocation manuelle ou DHCP d'adresses IP.

6. Cliquez sur l'icône d'actualisation pour voir la création de l'heure d'exécution.

   > **Remarque**
   >
   > Comme vous déployez deux instances NetScaler VPX dans le cadre d'un déploiement HA, deux temps d'exécution sont créés dans NSX Manager.
   >
   > 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 NetScaler ADM, accédez à **Orchestration** > **Requêtes** pour voir les détails de la progression de l'insertion du service. Vous pouvez constater qu'une demande de création et de mise à jour de l'heure d'exécution a été envoyée à NetScaler ADM. Lorsque l'heure d'exécution a été mise à jour, sélectionnez la demande et cliquez sur le bouton **Tâches** pour voir que NetScaler ADM a été ajouté dans NSX Manager.

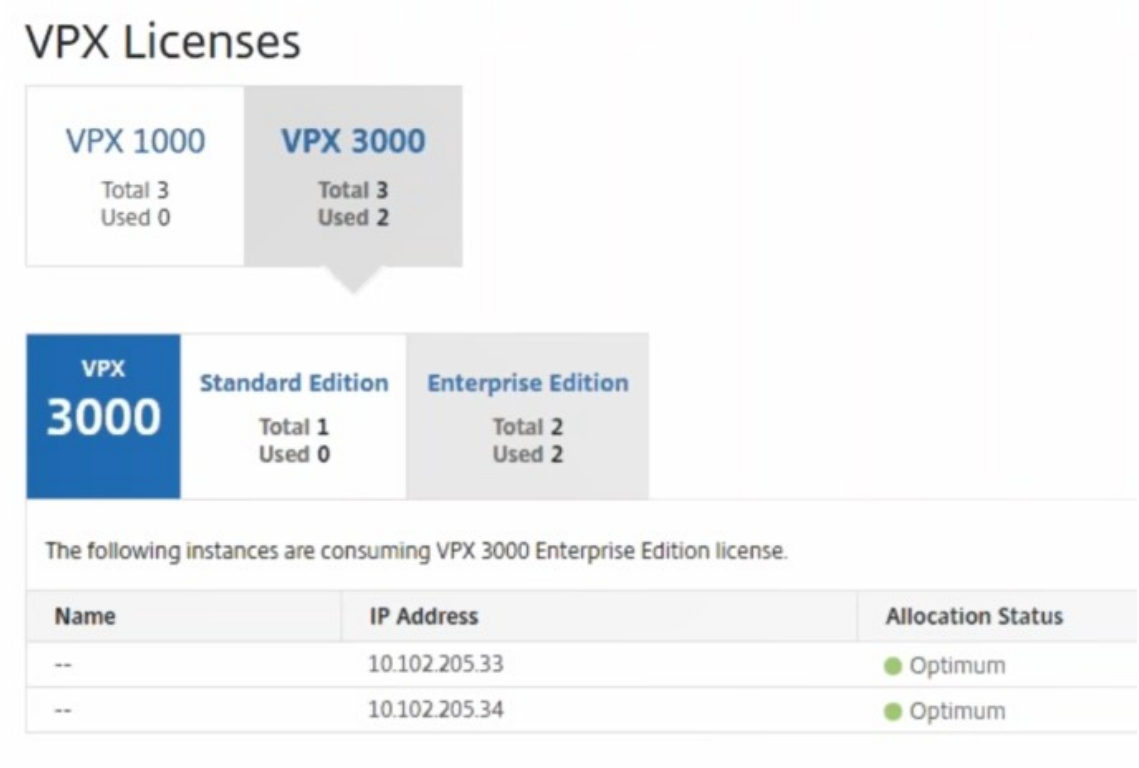
   Pour HA, il y aura deux demandes pour créer et mettre à jour deux temps d'exécution dans NetScaler ADM. Lorsque les deux temps d'exécution ont été mis à jour, sélectionnez les deux demandes et cliquez sur le bouton **Tâches** pour voir que deux nœuds NetScaler ADM HA ont été ajoutés dans NSX Manager.

10. Dans NetScaler ADM, accédez à **Orchestration** > **SDN Orchestration** > **VMware NSX Manager** > **Edge Gateways**. Dans le panneau de droite, vous pouvez voir que le NetScaler VPX a été ajouté à NSX Edge Gateway.

    Pour HA, vous pouvez voir que deux instances NetScaler VPX en mode HA ont été ajoutées à NSX Edge Gateway.

11. Dans NetScaler ADM, accédez à **Infrastructure > Licences groupées > Licences VPX.** Sélectionnez la licence NetScaler VPX et l'édition que vous avez installée.

    Les instances NetScaler VPX qui sont en mode HA consomment deux licences et l'état s'affiche sur votre écran comme ci-dessous.



Une fois l'insertion du service terminée, vous pouvez utiliser StyleBooks pour configurer les instances NetScaler selon l'une des deux méthodes suivantes :

- Configuration des services d'équilibrage de charge sur NetScaler VPX dans l'interface graphique de VMware NSX Manager
- Configuration des services d'équilibrage de charge sur NetScaler VPX dans l'interface graphique NetScaler ADM

Configuration des services d'équilibrage de charge sur NetScaler VPX dans l'interface graphique de 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 :

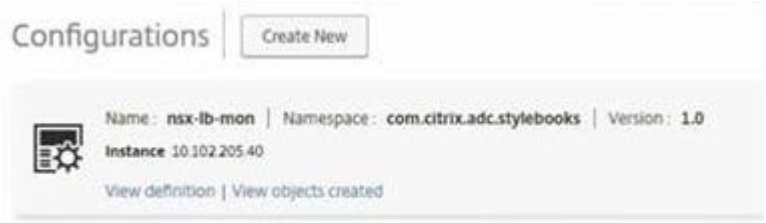
    a) Profil d'application : par défaut, le profil de service que vous avez créé dans NetScaler ADM s'affiche.

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 NetScaler ADM, accédez à **Orchestration** > **Requêtes** pour voir les détails de l'avancement de la création du service sur une ou plusieurs instances NetScaler sélectionnées.
4. Dans NetScaler 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 NetScaler VPX dans l'interface graphique NetScaler ADM

Déployez des configurations d'équilibreur de charge sur l'instance NetScaler à l'aide de NetScaler ADM StyleBooks. Pour HA, la configuration est déployée sur les deux instances NetScaler qui sont en HA.

Pour créer des packs de configuration via StyleBooks :

1. Dans NetScaler ADM, accédez à **Applications** > **Configuration** > **Créer un nouveau**, puis sélectionnez le StyleBook d'**équilibrage de charge HTTP/SSL (avec moniteurs**) 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 NetScaler 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 NetScaler VPX

Vous pouvez voir que les groupes de services et les serveurs virtuels sont créés en vous connectant à l'instance NetScaler VPX.

Pour afficher les groupes de services et les serveurs virtuels :

1. Connectez-vous à l'instance NetScaler VPX. Pour le déploiement en haute disponibilité, vous devez vous connecter aux deux instances NetScaler qui sont en haute disponibilité.
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 nécessaires sur les instances NetScaler VPX déployées sur NSX Manager, vous pouvez supprimer les insertions de services effectuées précédemment.

Pour supprimer la configuration et l'insertion de service :

1. Dans NetScaler ADM, accédez à **Applications** > **Configuration, sélectionnez la configuration**de l'application créée, puis supprimez-la en cliquant sur l'icône « X ».
2. Dans NSX Manager, accédez à la passerelle Edge à laquelle l'instance NetScaler 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 NetScaler 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

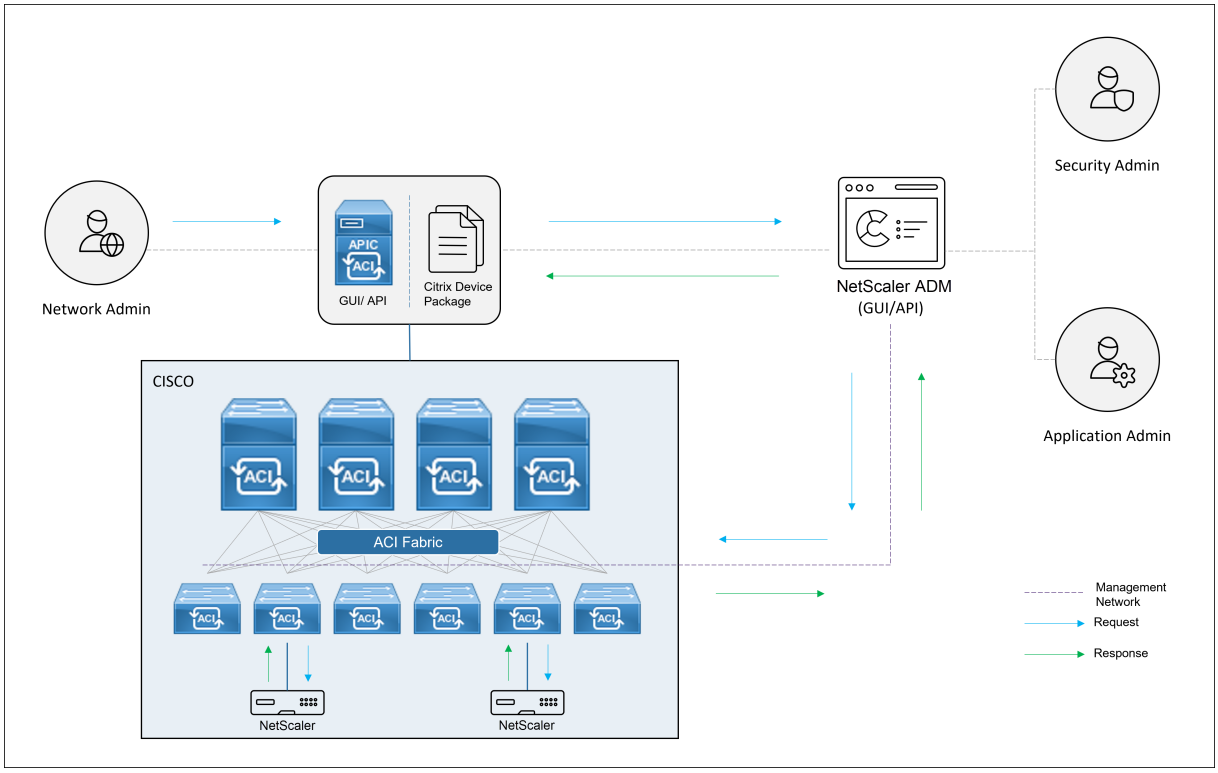
Automatisation de NetScaler à l'aide de NetScaler ADM en mode hybride Cisco ACI

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 NetScaler Application Delivery Management (ADM), qui fait office de gestionnaire de périphériques dans l'APIC.

La solution NetScaler Hybrid Mode est prise en charge par un package de périphériques en mode hybride et NetScaler ADM. Vous devez télécharger le package de périphérique en mode hybride dans l'APIC. Ce package fournit toutes les entités configurables du réseau L2-L3 à partir de NetScaler. La parité des applications est mappée par StyleBook entre NetScaler ADM et 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 NetScaler.

L'illustration suivante fournit une vue d'ensemble de NetScaler dans une solution en mode hybride :

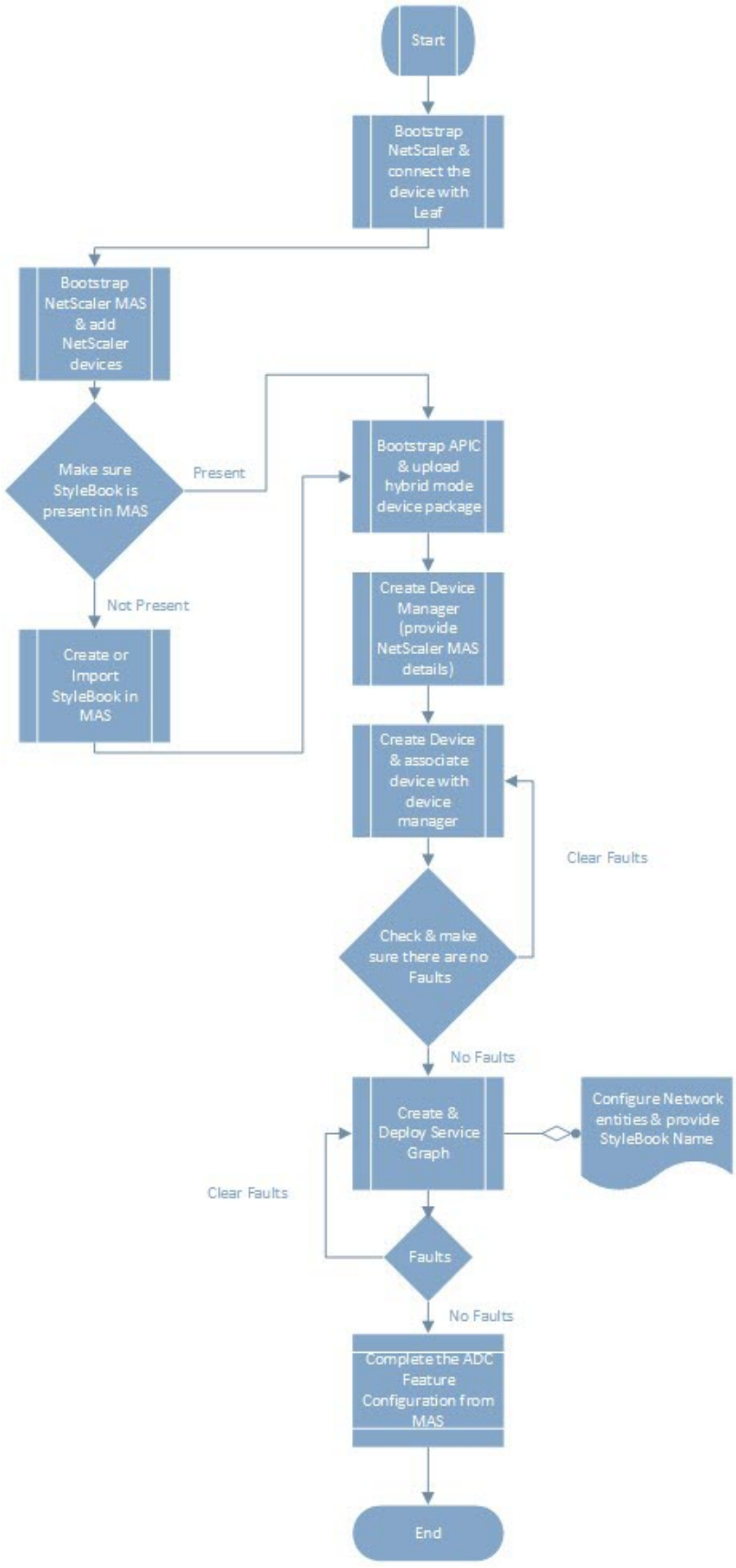


En mode hybride, la configuration de NetScaler s'effectue selon les deux phases suivantes :

1. L'assemblage du réseau est effectué à partir du Cisco APIC
2. La configuration est effectuée à partir de NetScaler 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 NetScaler ADM via le package de l'appareil, et NetScaler ADM les traite en interne et configure le NetScaler. Un administrateur d'application crée la configuration associée à l'ADC de l'application à l'aide de StyleBook dans NetScaler ADM, et ces configurations sont ensuite transférées de NetScaler ADM vers NetScaler. Le Cisco APIC et NetScaler ADM communiquent avec l'ADC via le réseau de gestion.

Le schéma suivant montre un flux de travail NetScaler dans la solution hybride :



Package d'appareils NetScaler en mode orchestrateur cloud de Cisco ACI

February 1, 2024

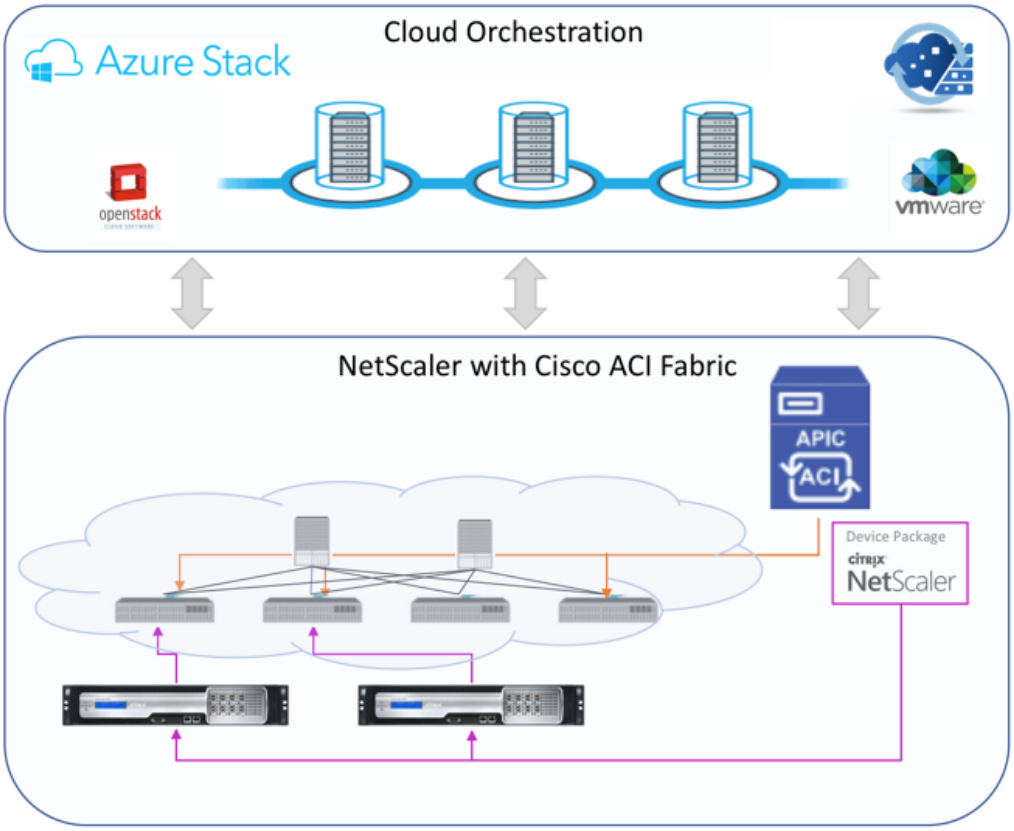
Avec la version 3.1 du contrôleur d'infrastructure des stratégies d'application (APIC), Citrix NetScaler et Cisco ACI élargissent leur portefeuille d'intégration conjoint afin de fournir une nouvelle solution répondant aux besoins des clients. Le nouveau mode d'intégration, le mode ACI Cloud Orchestrator*, 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 cloud Cisco ACI utilisant la solution NetScaler 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 NetScaler dans une solution d'orchestration dans le cloud :

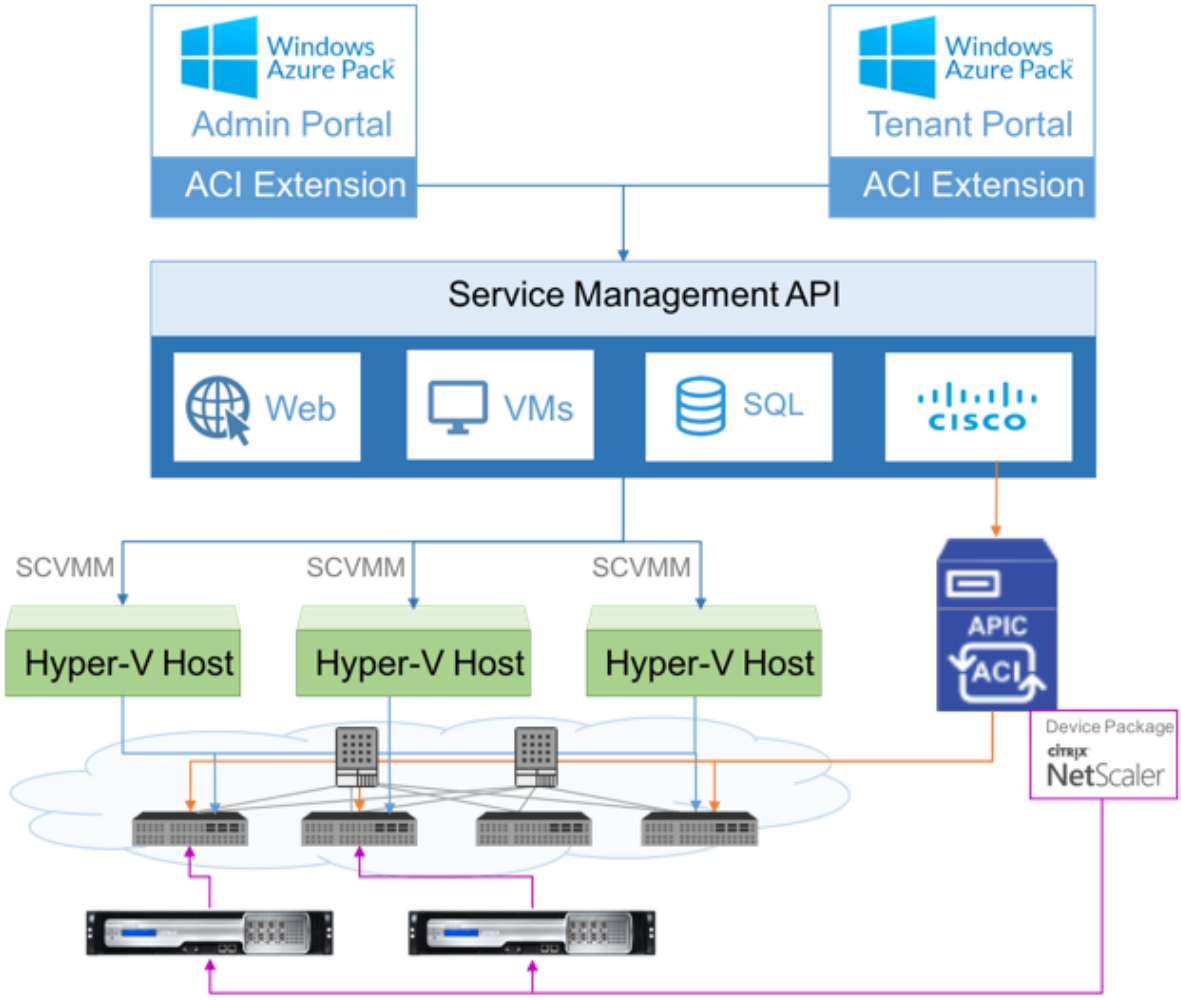


La solution en mode orchestrateur cloud utilisant Microsoft Azure Pack implique de nombreux points d'intégration, tels qu'Azure Pack vers Cisco APIC, Cisco APIC vers System Central Virtual Machine Manager (SCVMM) et Cisco APIC vers NetScaler. En tant que locataire dans le cloud privé, vous pouvez activer 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 de l'ACI, la gamme VIP, l'association d'appareils NetScaler à un cloud de machines virtuelles et la création d'un compte utilisateur locataire.
- En tant que locataire, vous pouvez effectuer des tâches telles que vous connecter au portail des locataires Azure Pack et configurer le réseau, les domaines de pont et le routage et le transfert virtuels (VRF), et utiliser les fonctionnalités d'équilibrage de charge et de RNAT de NetScaler.

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 NetScaler de la même manière 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 NetScaler prend uniquement en charge le déploiement à contexte unique. Chaque locataire dispose d'une instance NetScaler dédiée.
- Le protocole WAP (Wireless Application Protocol) prend en charge les appliances NetScaler MPX et NetScaler VPX (y compris les instances NetScaler VPX déployées sur la plateforme NetScaler 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 fonctions couvrent un ensemble complet de fonctionnalités et le mode de déploiement de NetScaler. De même, le package de périphériques en mode gestionnaire de services prend en charge la configuration à un bras et à deux bras et le déploiement de NetScaler à l'aide d'APIC. NetScaler Application Delivery Management (ADM) fait office de gestionnaire de services pour APIC et vous pouvez utiliser NetScaler ADM pour configurer les paramètres NetScaler L4-L7.

> **Remarque**
>
> En mode gestionnaire de services (mode hybride), vous ne pouvez pas réutiliser ou réattribuer la même adresse IP de serveur, qui est déjà présente dans l'appliance NetScaler.

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 cloud fournit les valeurs des paramètres ADC (VIP, lors du provisionnement du NetScaler 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 l'appareil qui configure NetScaler 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

NetScaler prend en charge les profils de fonctions 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 Citrix Cloud Mode prend en charge NetScaler 12.0 et le mode gestionnaire de services utilise également NetScaler 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 approvisionner NetScaler via un orchestrateur 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 NetScaler 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**
>
> - NetScaler ADM prend en charge la fonctionnalité Ingress sur les clusters équipés des versions 1.14-1.21 de Kubernetes.
> - NetScaler ADM prend en charge les appliances NetScaler VPX et MPX en tant que périphériques d'entrée.
> - Dans l'environnement Kubernetes, l'instance NetScaler équilibre uniquement la charge du 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 NetScaler 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 NetScaler 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.

NetScaler ADM mappe automatiquement les configurations d'entrée aux instances ADC à l'aide de stratégies d'entrée.

Pour chaque configuration d'entrée réussie, NetScaler 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 NetScaler comme appareils d'entrée sur des clusters Kubernetes, assurez-vous de disposer des éléments suivants :

- Cluster Kubernetes en place.
- Cluster Kubernetes enregistré dans NetScaler ADM.

Configurer NetScaler ADM avec un jeton secret pour gérer un cluster Kubernetes

Pour que NetScaler ADM puisse recevoir des événements de Kubernetes, vous devez créer un compte de service dans Kubernetes pour NetScaler ADM. Et, configurez le compte de service avec les autorisations RBAC nécessaires dans le cluster.

1. Créez un compte de service pour NetScaler 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 `cluster-admin` rôle pour lier le compte de service NetScaler 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 NetScaler ADM au `cluster-admin` rôle, le compte de service dispose d'un accès à l'ensemble 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 :

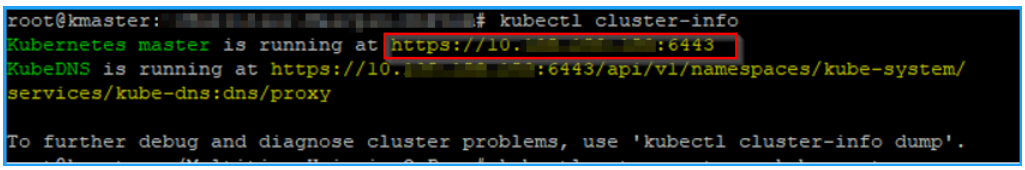
```
kubectl describe secret <token-name>
<!--NeedCopy-->
```

Ajouter le cluster Kubernetes dans NetScaler ADM

Après avoir configuré un agent NetScaler ADM et configuré des itinéraires statiques, vous devez enregistrer le cluster Kubernetes dans NetScaler ADM.

Pour enregistrer le cluster Kubernetes :

1. Connectez-vous à NetScaler ADM à l'aide des 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 de jeton d'authentification obtenue lors de la configuration de NetScaler ADM pour gérer uncluster Kubernetes. Le jeton d'authentification est requis pour valider l'accès aux communications entre le cluster Kubernetes et NetScaler ADM. Pour générer un jeton d'authentification :

i. Sur le nœud principal Kubernetes, exécutez les commandes suivantes :

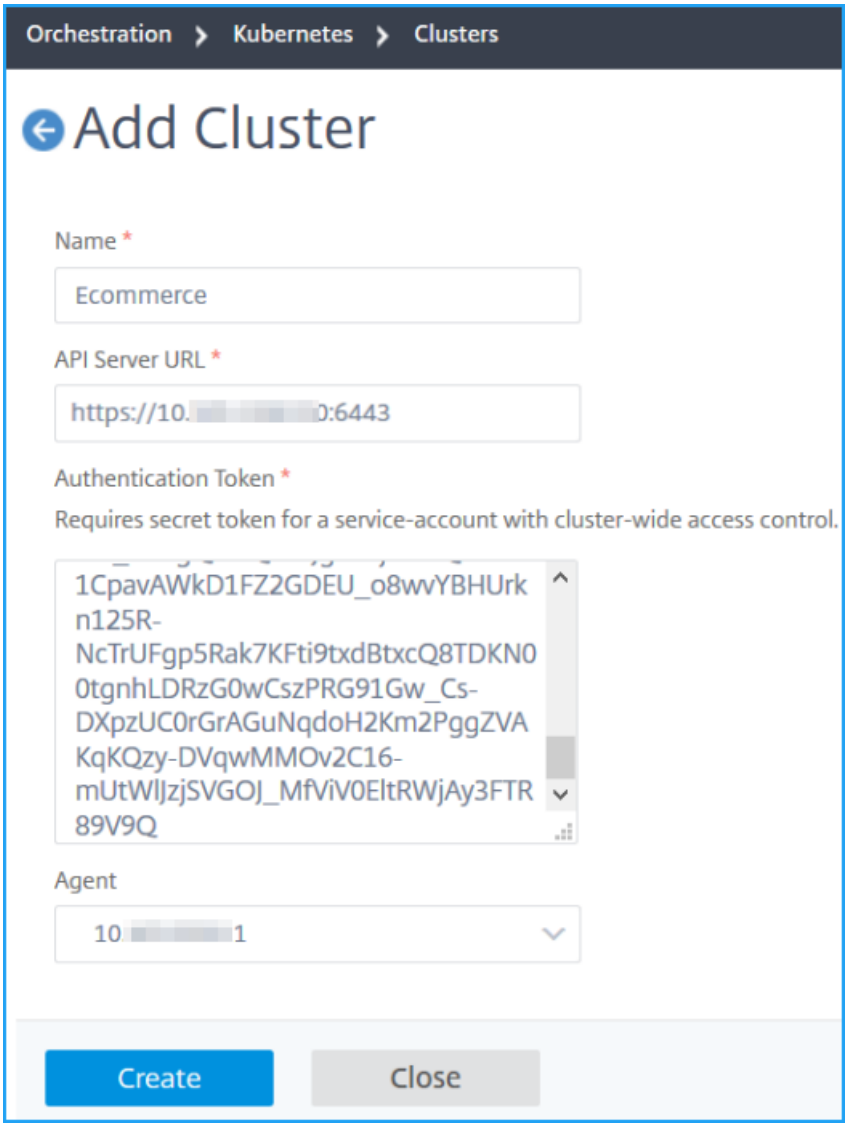
```
kubectl describe secret <token-name>
<!--NeedCopy-->
```

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 détermine quel NetScaler est utilisé pour déployer une configuration d'entrée, en fonction du cluster d'entrée ou de l'espace de nommage.

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 instances associés à l'agent NetScaler 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 **Infrastructure > 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 NetScaler 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 :

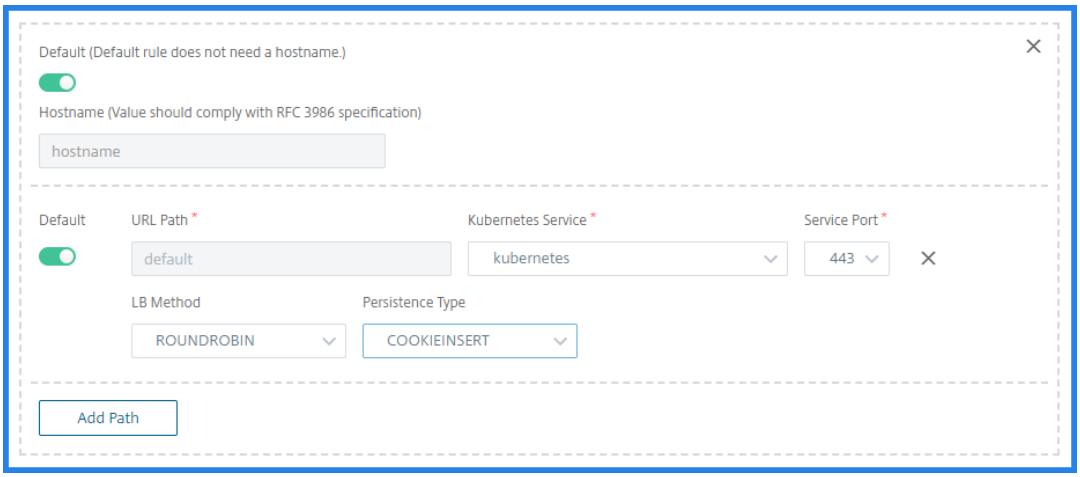
```
"lbmethod":"ROUNDROBIN"
<!--NeedCopy-->
```

- **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 :

```
"persistenceType":"COOKIEINSERT"
<!--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 **Paramètres > Configuration des licences et des analyses**.
> 2. Sous **Récapitulatif des licences du serveur virtuel**, activez la **sélection automatique des serveurs virtuels**.

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 NetScaler afin d'améliorer l'expérience client et l'efficacité opérationnelle, en 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.

Lors de l'optimisation du trafic vidéo, l'appliance NetScaler 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 de NetScaler, consultez la section Optimisation vidéo. Lorsque vous intégrez

l'appliance NetScaler à NetScaler Application Delivery Management (ADM), elle collecte des informations clés à partir des données vidéo qui transitent par l'appliance NetScaler. 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 NetScaler ADM correspondent aux sessions que vous avez sélectionnées à partir d'un échantillonnage aléatoire dans l'appliance NetScaler. Pour plus d'informations sur l'échantillonnage aléatoire, voir Optimisation vidéo.

Video Insight dans NetScaler 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 NetScaler dotées d'une licence NetScaler Premium. La licence NetScaler Premium est prise en charge pour les plateformes NetScaler Telco (VPX T1000 et VPX-T).

Pour configurer Video Insight sur une instance NetScaler, activez d'abord la fonctionnalité AppFlow, configurez un collecteur, une action et une stratégie AppFlow, puis liez la stratégie de manière globale. Lorsque vous configurez le collecteur, vous devez spécifier l'adresse IP du serveur NetScaler ADM sur lequel vous souhaitez surveiller les rapports.

Pour configurer l'aperçu vidéo sur une instance NetScaler, exécutez les commandes suivantes pour configurer un profil et une stratégie AppFlow et lier la stratégie AppFlow de manière globale.

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

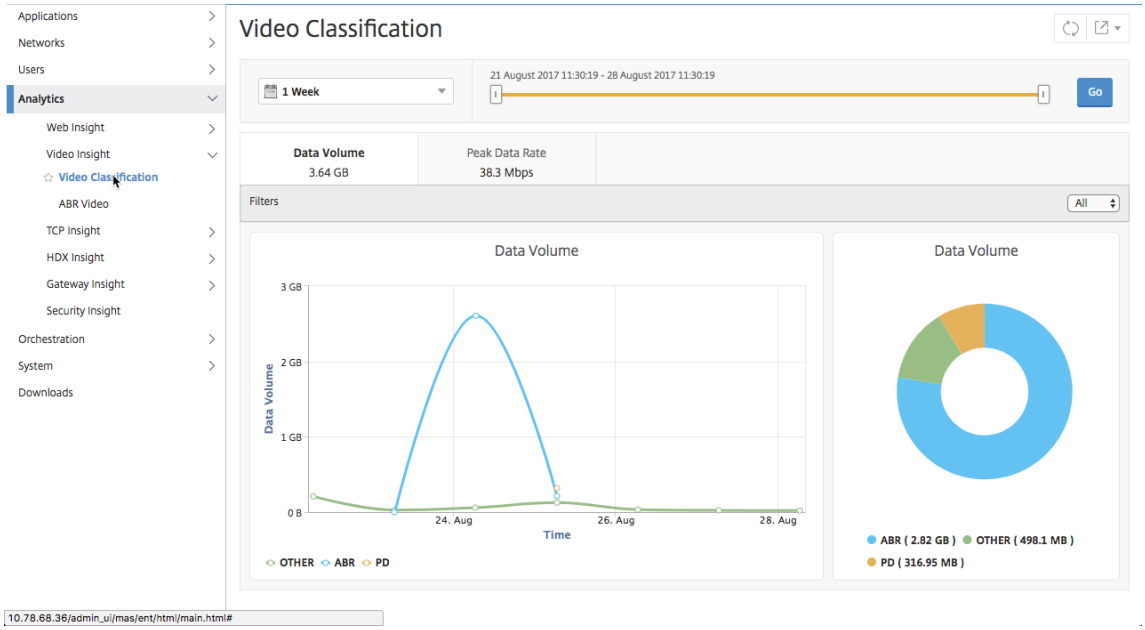
```
add appflow collector col1 -IPAddress 10.106.76.15 -port 5557 -
   Transport logstream
set appflow param -videoInsight ENABLED
add appflow action act1 -collectors col1 -videoAnalytics ENABLED
add appflow policy appol true act1
bind appflow global appol 1
enable ns mode ulfd
enable feature appflow
<!--NeedCopy-->
```

Affichage des métriques Video Insight dans NetScaler ADM

Après avoir activé Video Insight dans NetScaler ADM, vous pouvez consulter les mesures d'optimisation vidéo, telles que la classification des vidéos, 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 consulter les métriques Video Insight dans NetScaler ADM :

1. Dans un navigateur Web, tapez l'adresse IP de l'appliance virtuelle NetScaler 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

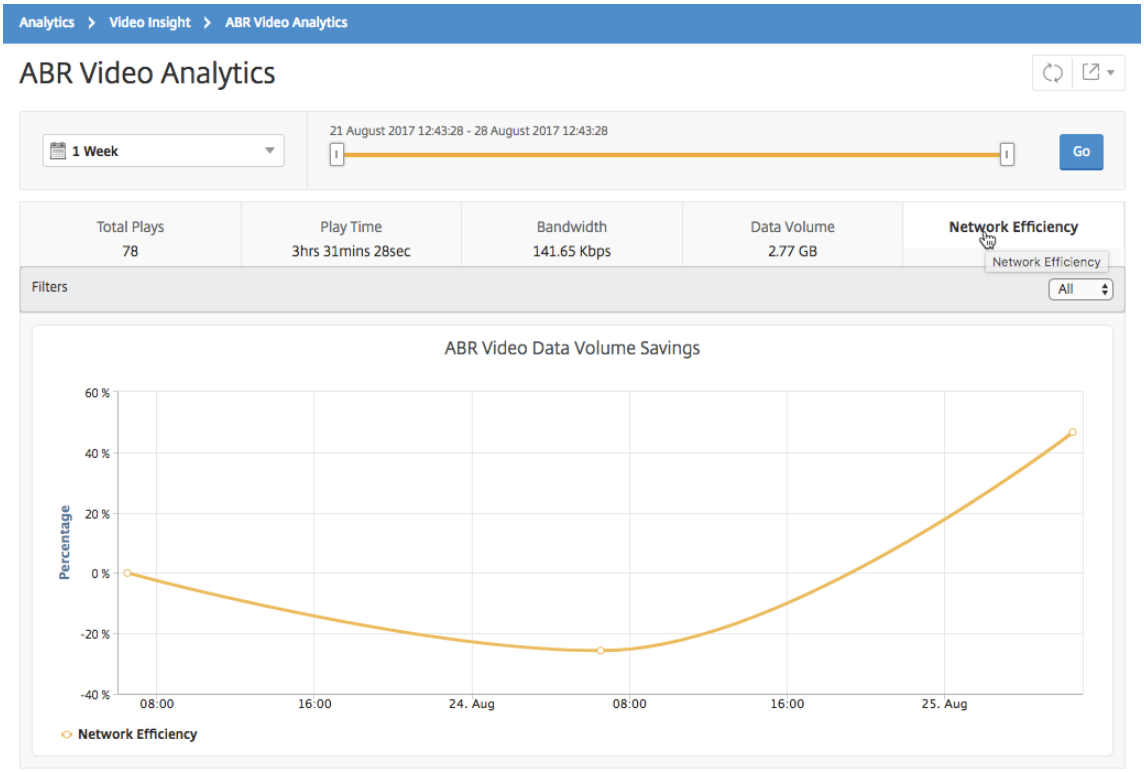
Pour une période donnée, NetScaler Application Delivery Management (ADM) fournit un graphique qui montre le ratio entre les sessions vidéo optimisées et non optimisées au cours de la période. Il affiche également le pourcentage de bande passante économisé grâce à l'optimisation. Le pourcentage de bande 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

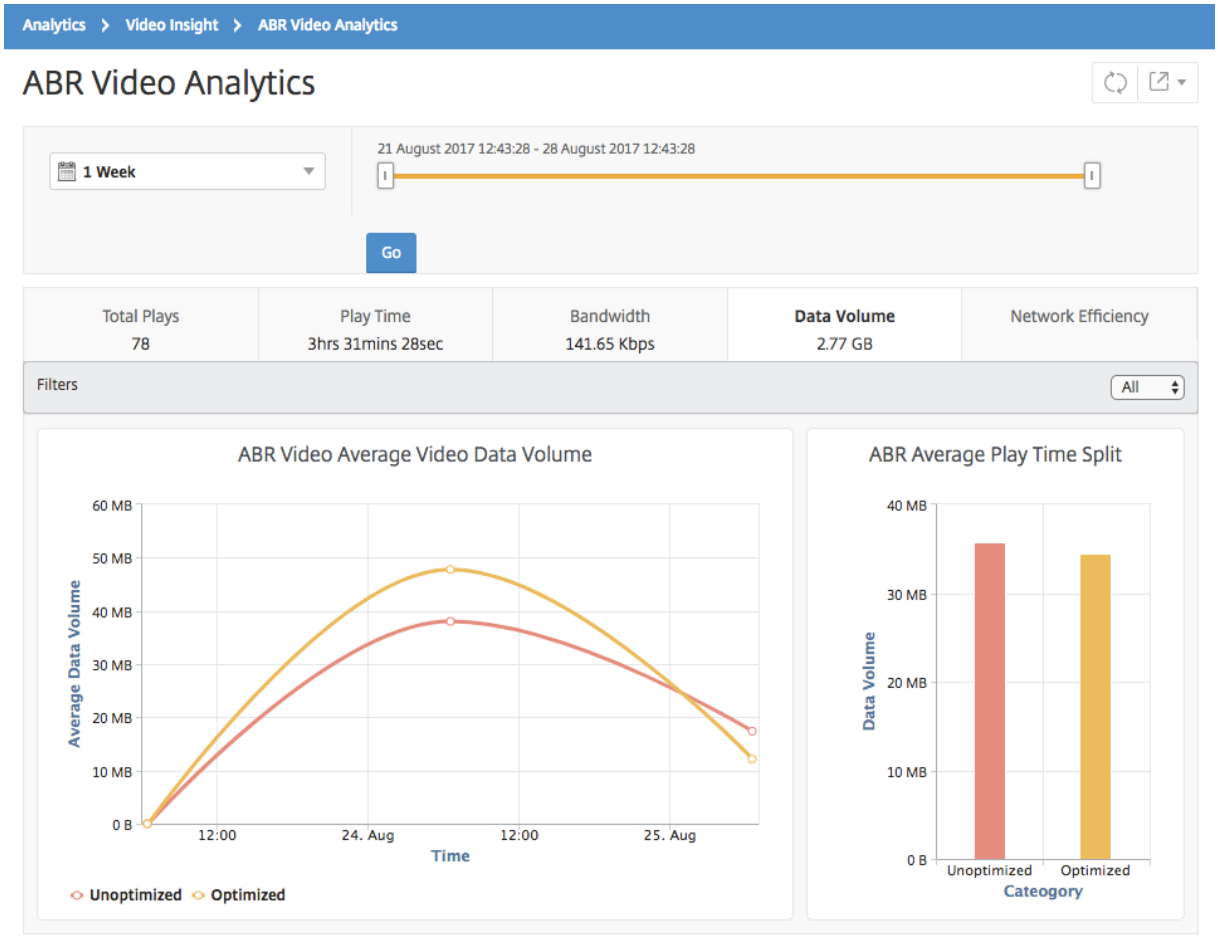
February 1, 2024

Pour une période donnée, NetScaler Application Delivery Management (ADM) affiche le volume de données utilisé par les vidéos ABR optimisées et non optimisées, afin que vous puissiez comparer les deux volumes.

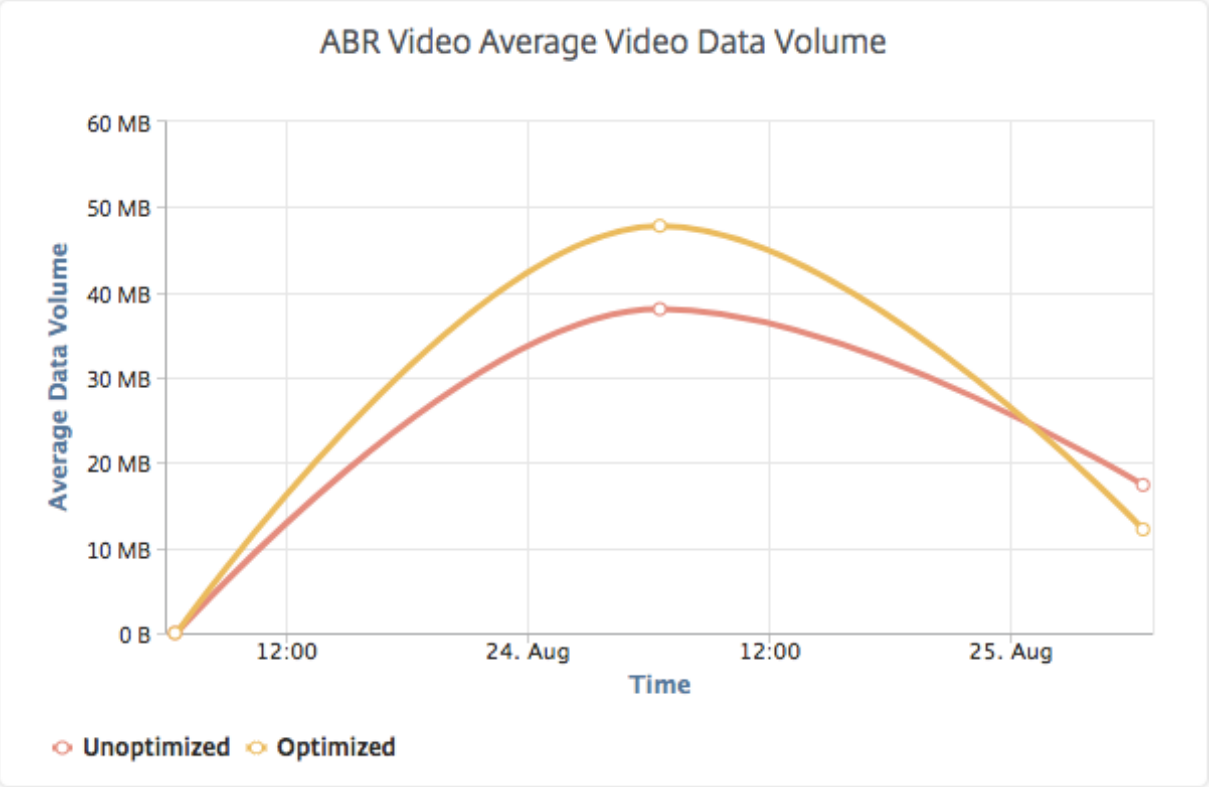
Pour voir le volume de données utilisé par les vidéos ABR :

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

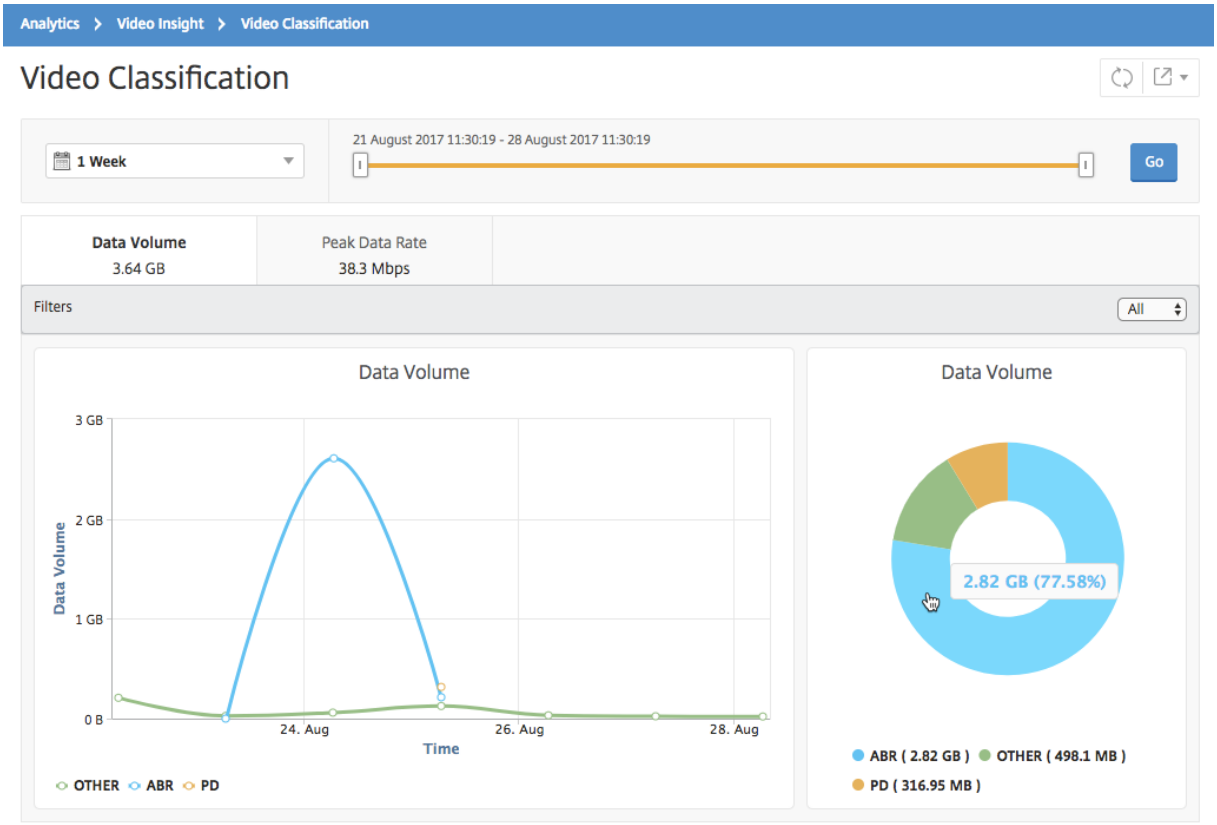
February 1, 2024

L'appliance NetScaler détecte le trafic vidéo crypté ou non crypté sur votre réseau et le type de streaming vidéo (DP ou ABR). NetScaler Application Delivery Management (ADM) affiche ces mesures ainsi que le volume de données consommé par le trafic vidéo pendant une période définie.

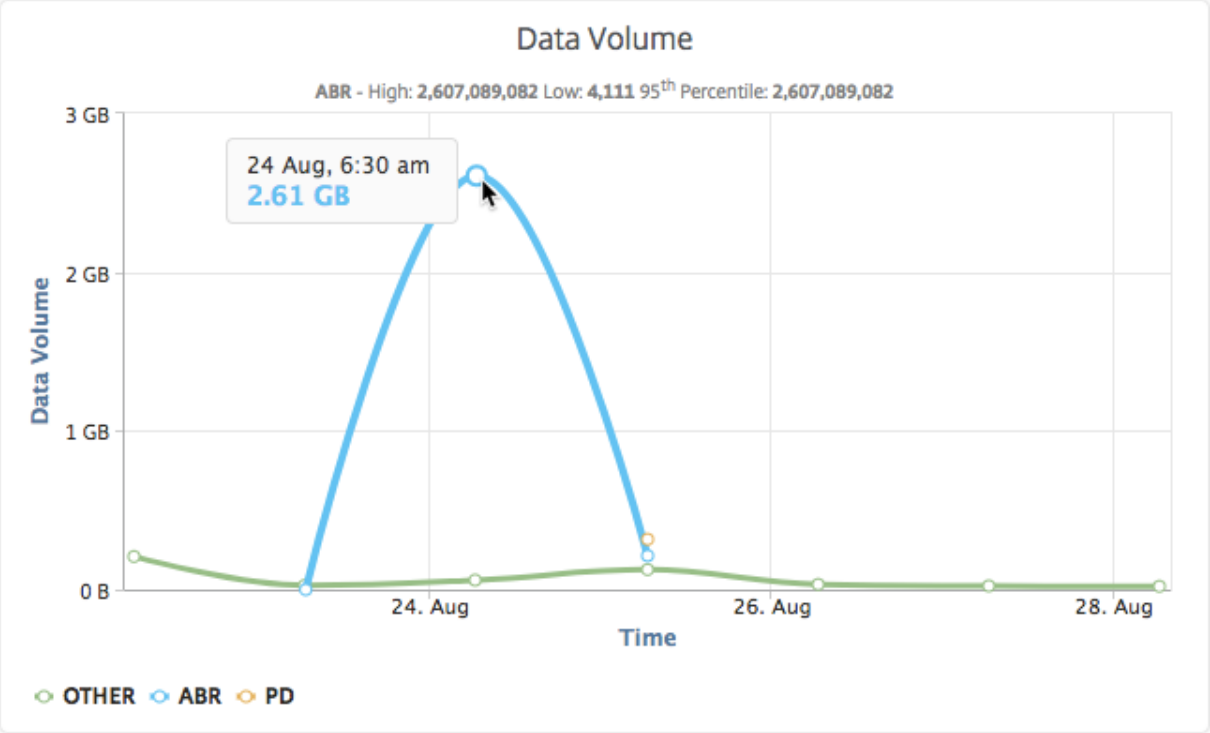
Pour voir les types de vidéos et le volume de données consommé :

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**.

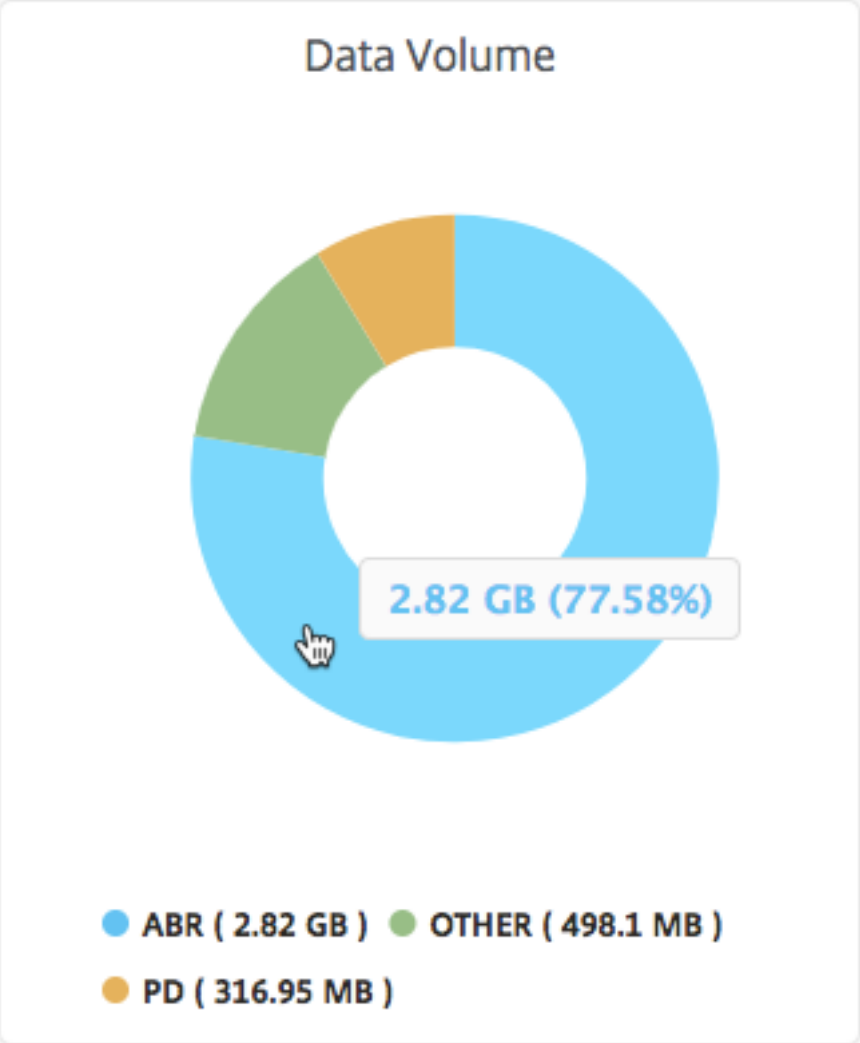
Vous pouvez utiliser la liste **Filtres** pour sélectionner le trafic HTTP, HTTPS ou QUIC.



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

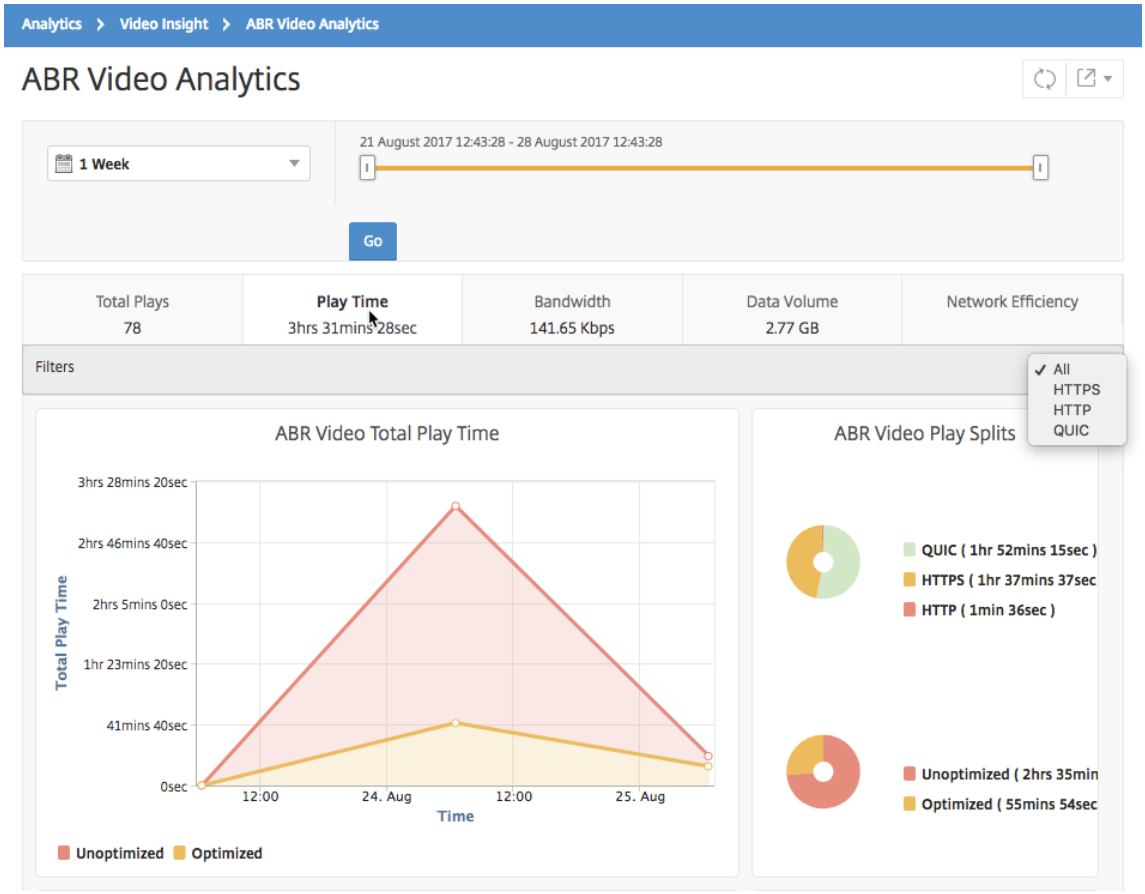
Pour une période donnée, NetScaler Application Delivery Management (ADM) fournit la durée de lecture des vidéos ABR et vous permet également de comparer la durée de lecture des vidéos ABR optimisées et non optimisées sur votre réseau.

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.

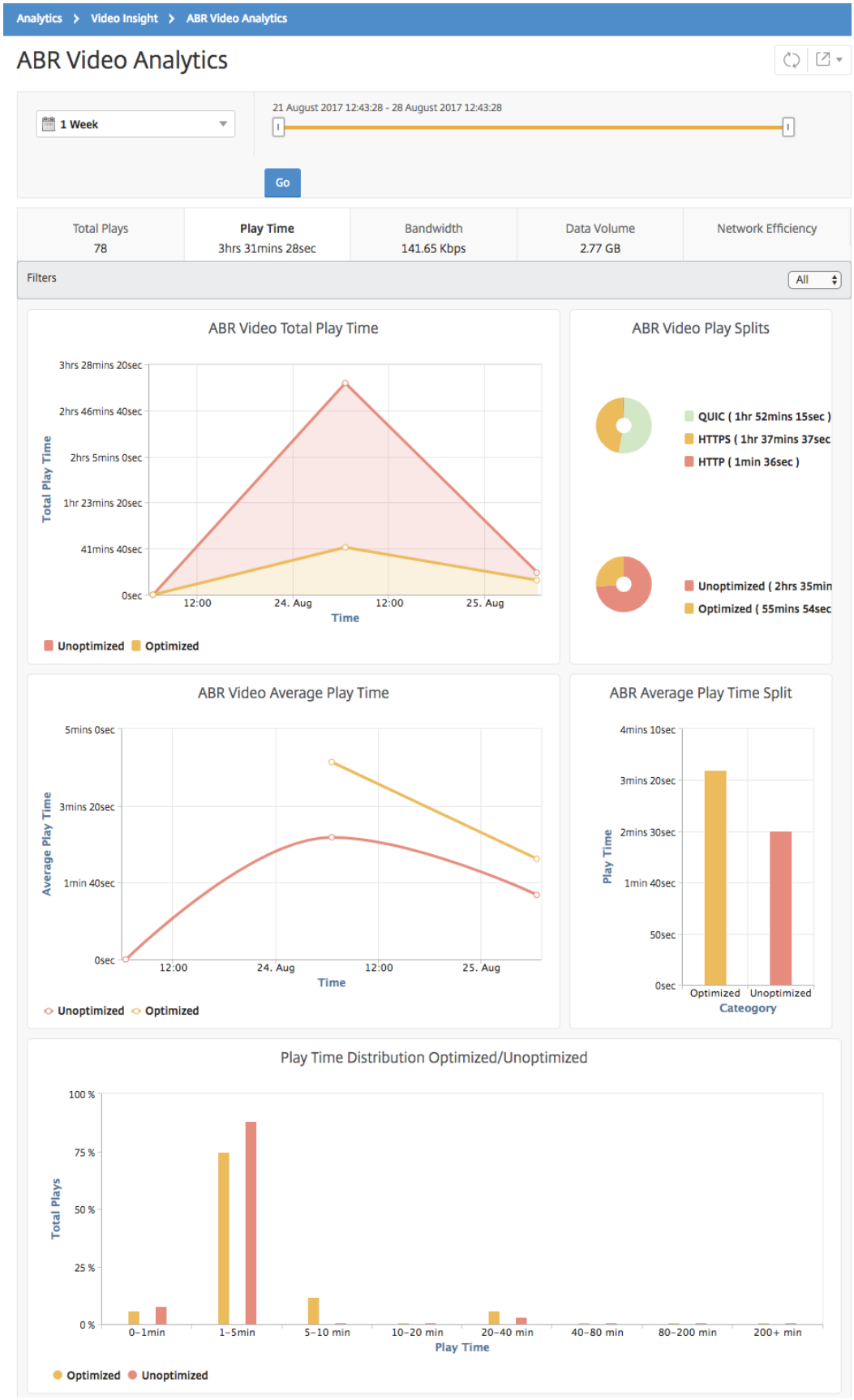
3. Cliquez sur **Aller** et sélectionnez l'onglet **Temps de lecture**.

   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

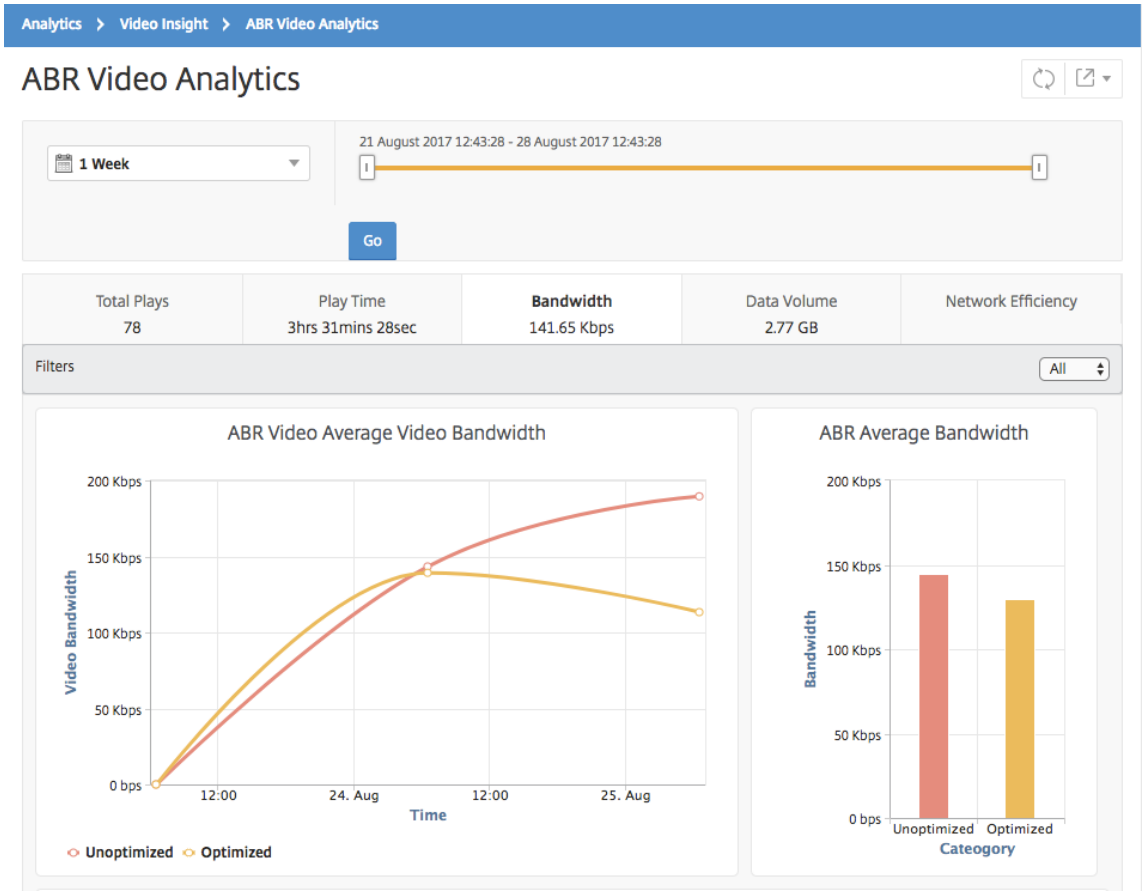
Pour une période donnée, NetScaler Application Delivery Management (ADM) fournit la bande passante consommée par les vidéos ABR optimisées et non optimisées et vous permet également de comparer la bande passante consommée par les vidéos ABR optimisées et non optimisées de votre réseau en fonction des critères suivants :

- Temps de jeu
- Volume de données

Pour consulter la consommation de bande passante :

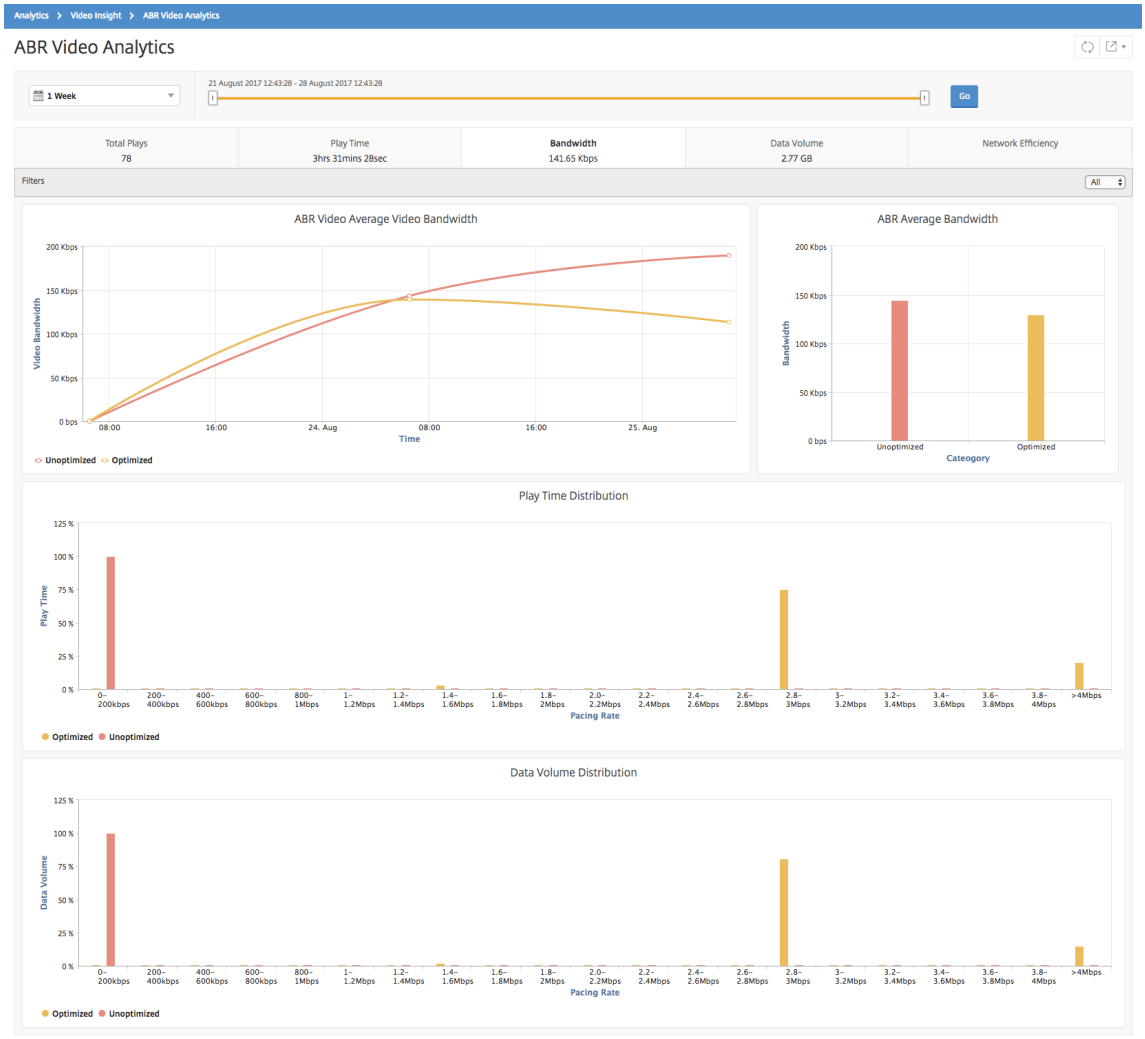
1. Accédez à **Analytics > Video Insight** et cliquez sur **ABR Video Analytics**.
2. Dans le volet droit, sélectionnez une période dans la liste. Vous pouvez personnaliser davantage la période en utilisant le curseur temporel.
3. Cliquez sur **Aller** et sélectionnez l'onglet **Bande passante**.

   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

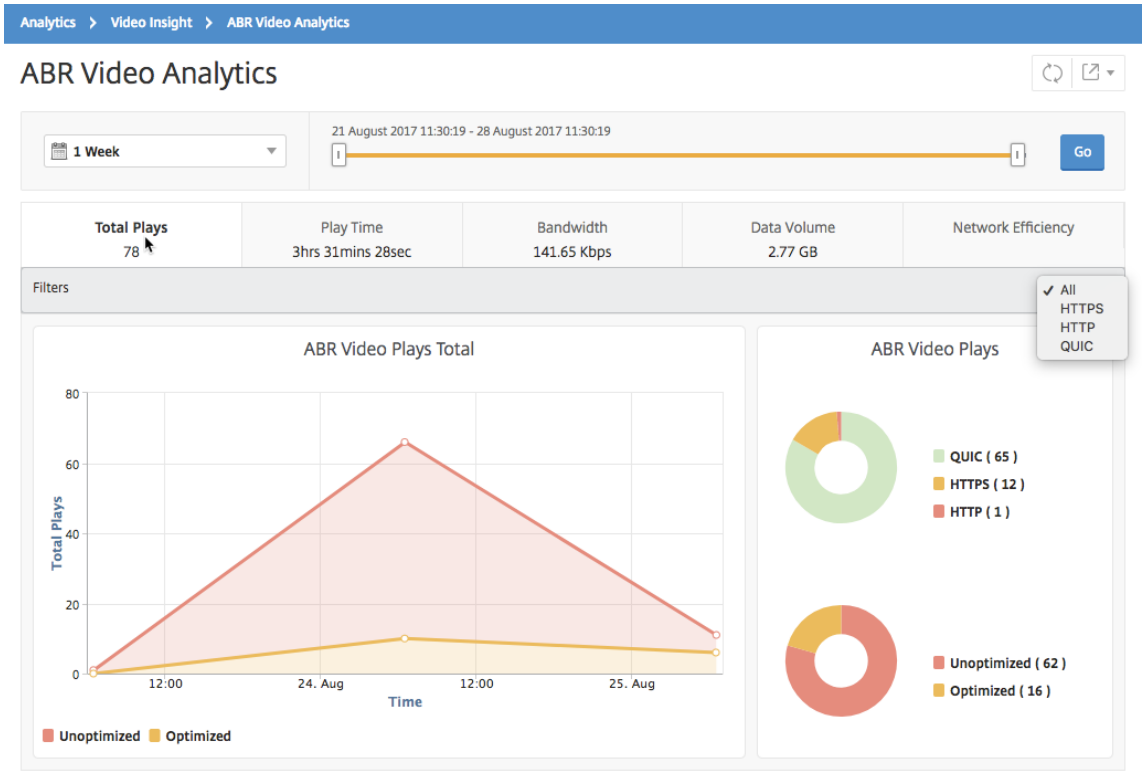
Pour une période donnée, NetScaler Application Delivery Management (ADM) affiche le nombre de lectures de vidéos ABR et vous permet de comparer le nombre de lectures optimisées et non optimisées sur votre réseau.

Pour voir le nombre de parties :

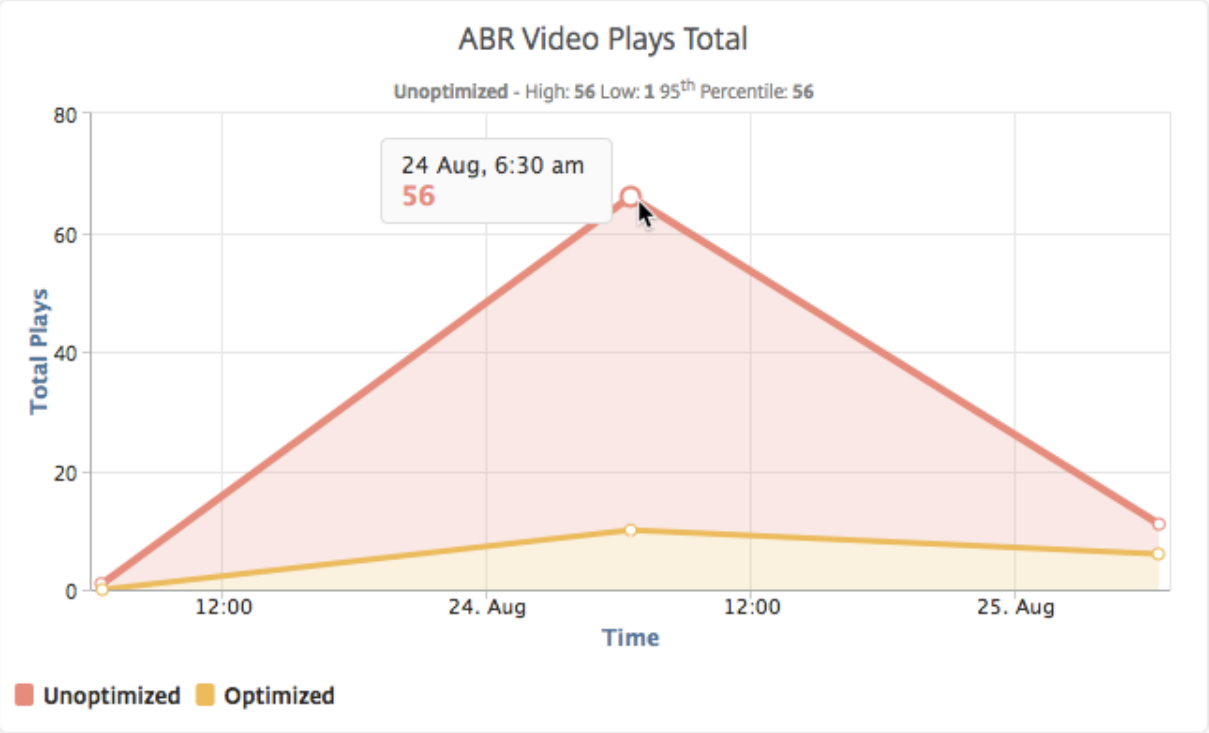
1. Accédez à **Analytics > Video Insight**, puis cliquez sur **ABR Video Analytics**.
2. Dans le volet droit, sélectionnez une période dans la liste. Vous pouvez personnaliser davantage la période en utilisant le curseur temporel.

3. Cliquez sur **Aller** et sélectionnez l'onglet **Nombre de Lecture**.

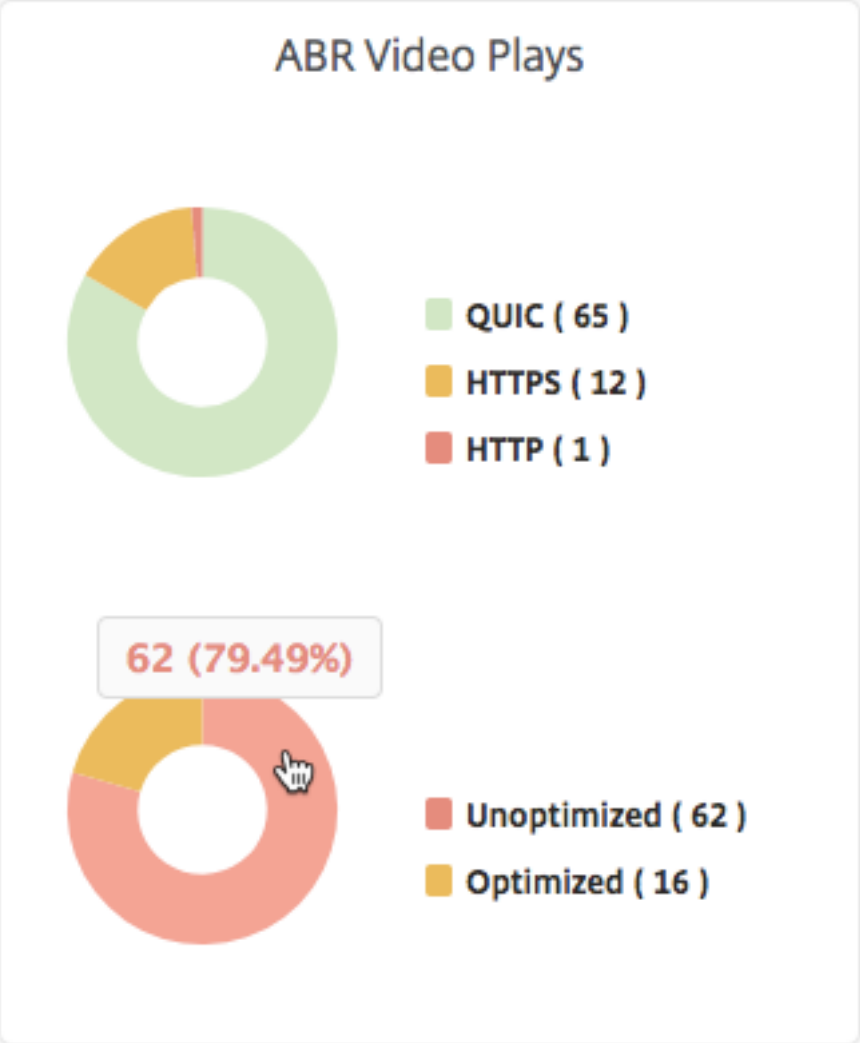
   Vous pouvez utiliser la liste **Filtres** pour sélectionner les vidéos HTTP, HTTPS ou QUIC ABR.



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

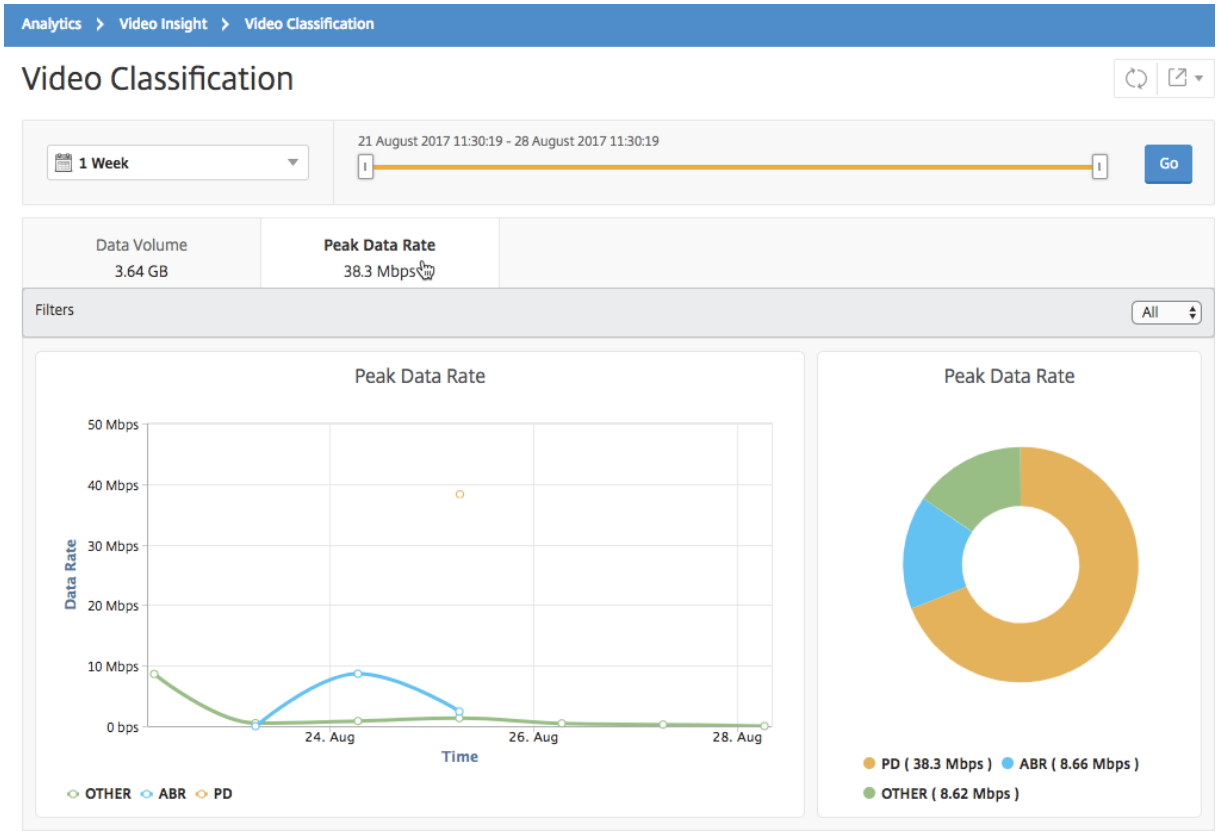
February 1, 2024

NetScaler Application Delivery Management (ADM) vous indique le débit maximal ou le débit de données du trafic vidéo sur votre réseau.

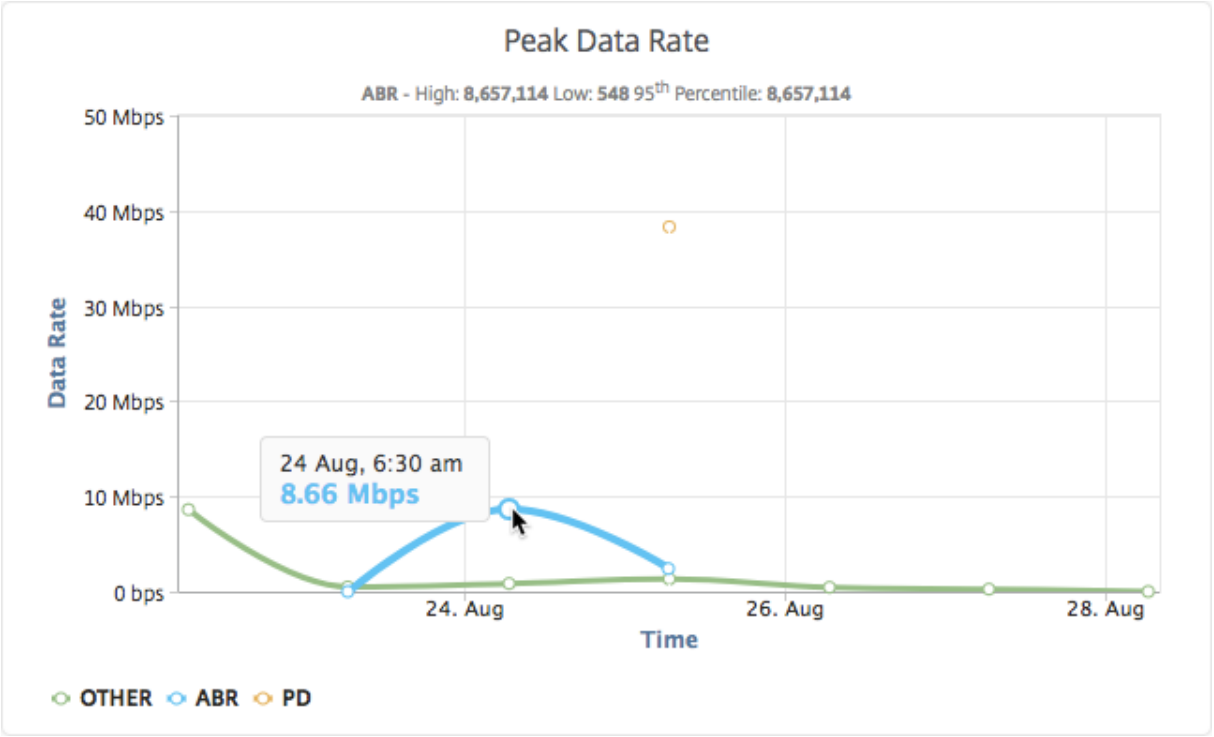
Pour voir le débit de données maximal du trafic vidéo :

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**.

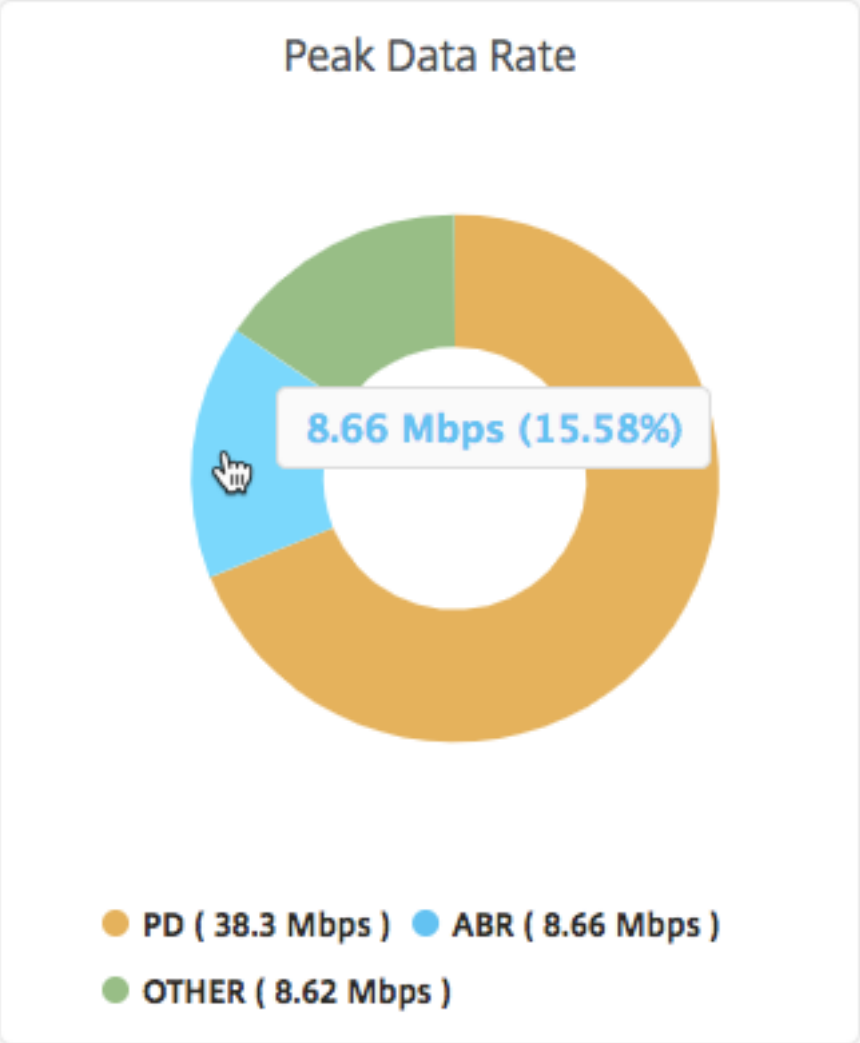
Vous pouvez utiliser la liste **Filtres** pour sélectionner le trafic HTTP, HTTPS ou QUIC.



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.



Configurer la gestion des adresses IP (IPAM)

February 1, 2024

NetScaler ADM IPAM vous permet d'attribuer et de libérer automatiquement des adresses IP dans les configurations gérées par NetScaler 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 NetScaler ADM.
- Solution IPAM Infoblox.

Vous pouvez utiliser NetScaler ADM IPAM dans :

- **StyleBooks** : attribuez automatiquement des adresses IP aux serveurs virtuels lorsque vous créez des configurations.

- **Passerelle API** : allouer automatiquement une adresse IP au proxy de l'API.

Vous pouvez également suivre les adresses IP de chaque réseau ou la plage d'adresses IP gérée par NetScaler ADM.

Ajouter un fournisseur d'adresses IP externe

NetScaler ADM dispose d'un fournisseur IPAM intégré pour gérer les adresses IP et les plages d'adresses IP. Vous pouvez également utiliser un fournisseur d'adresses IP externe pour NetScaler ADM.

> **Important :**
>
> Avant de commencer, assurez-vous que les autorisations suivantes sont activées dans le fournisseur d'adresses IP externe :
>
> - Possibilité d'interroger les réseaux présents dans le fournisseur.
> - Réserver une adresse IP dans le réseau.
> - Libérez une adresse IP du réseau.
> - Récupérer les adresses IP utilisées à partir d'un réseau.
> - Récupérer les adresses IP disponibles à partir d'un réseau.

Procédez comme suit pour ajouter une solution de fournisseur IPAM externe dans NetScaler ADM :

1. Accédez à **Paramètres > IPAM**.
2. Dans **Fournisseurs**, cliquez sur **Ajouter**.
3. Spécifiez les informations suivantes pour ajouter un fournisseur IPAM :
   - **Nom** : spécifiez le nom du fournisseur IP à utiliser dans NetScaler ADM.
   - **Fournisseur** - Sélectionnez un fournisseur IPAM dans la liste.
   - **URL** : spécifiez l'URL de la solution IPAM qui attribue des adresses IP dans un environnement NetScaler ADM. Veillez à spécifier l'URL dans le format suivant :

     ```
     https://<host name>
     <!--NeedCopy-->
     ```

     Exemple : `https://myinfoblox.example.com`
   - **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**.

Infoblox DDI en tant que fournisseur externe

NetScaler ADM prend actuellement en charge Infoblox DDI en tant que fournisseur externe.

Vous pouvez utiliser NetScaler ADM IPAM avec le fournisseur Infoblox pour effectuer les actions suivantes :

- Répertorier les réseaux IPAM
- Création, mise à jour et suppression de réseaux IPAM
- Réservez et libérez une adresse IP depuis les réseaux IPAM

Création d'un réseau IPAM Pour créer un réseau NetScaler ADM IPAM à l'aide du fournisseur Infoblox, un réseau avec la même plage d'adresses IP CIDR doit exister sur Infoblox.

Lorsque vous créez un réseau IPAM dans NetScaler ADM, vous enregistrez uniquement l'utilisation du réseau Infoblox dans NetScaler ADM. ADM travaille ensuite avec Infoblox pour gérer les adresses IP attribuées depuis le réseau. Le réseau InfoBlox peut continuer à être utilisé en dehors de NetScaler ADM.

De même, si vous supprimez le réseau NetScaler ADM IPAM, NetScaler ADM désenregistre le réseau Infoblox. Cela signifie que NetScaler ADM n'interagit plus avec Infoblox pour la gestion des adresses IP sur ce réseau.

API DDI Infoblox NetScaler ADM IPAM utilise les API Infoblox suivantes pour effectuer les actions respectives :

- (/network) - Liste tous les réseaux Infoblox disponibles
- (/réseau ? network= {id}) - Récupère les détails d'un réseau Infoblox spécifique
- (/ipv4address) - Liste toutes les adresses IP d'un réseau Infoblox
- (/record:host) - Récupère les détails d'une adresse IP spécifique
- (/{IP}) - Réserve et libère des adresses IP sur un réseau Infoblox

Pour plus d'informations sur les API Infoblox, consultez le guide de référence des API Infoblox REST disponible sur Infoblox DDI.

Ajouter un réseau

Ajoutez un réseau pour utiliser IPAM avec les configurations gérées par NetScaler ADM.

1. Accédez à **Paramètres > IPAM**.
2. Sous **Réseaux**, cliquez sur **Ajouter**.
3. Spécifiez les détails suivants :

- **Nom du réseau** : spécifiez le nom du réseau pour identifier le réseau dans NetScaler ADM.
- **Fournisseur** : sélectionnez le fournisseur dans la liste.

  Cette liste affiche les fournisseurs ajoutés dans NetScaler 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 :**
  >
  > NetScaler ADM IPAM ne prend en charge que 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 **Paramètres > IPAM**.
2. Sous 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 NetScaler ADM qui a réservé l'adresse IP. Par exemple, si StyleBooks a réservé l'adresse IP, 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. Ainsi, il affiche Configurations sous cette colonne.
- **ID de ressource** : affiche l'ID de ressource exact avec un lien. Cliquez sur ce lien pour accéder à la ressource qui utilise l'adresse IP. Pour le type de ressource de configuration, il affiche l'ID du pack de configuration comme ID de ressource.

> **Remarque :**
>
> Si vous souhaitez libérer l'adresse IP, sélectionnez l'adresse IP que vous souhaitez libérer et cliquez sur **Libérer les adresses IP allouées**.

Utiliser les journaux d'audit ADM pour gérer et surveiller votre infrastructure

February 1, 2024

Vous pouvez utiliser le service NetScaler 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

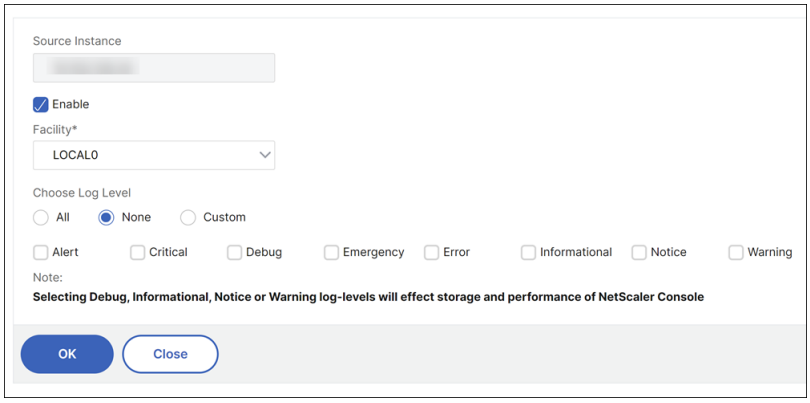
Avant de pouvoir consulter les messages syslog relatifs à l'instance ADC depuis ADM, configurez le service NetScaler ADM en tant que serveur syslog pour votre instance NetScaler. Une fois la configuration

terminée, tous les messages syslog sont redirigés de l'instance vers ADM.

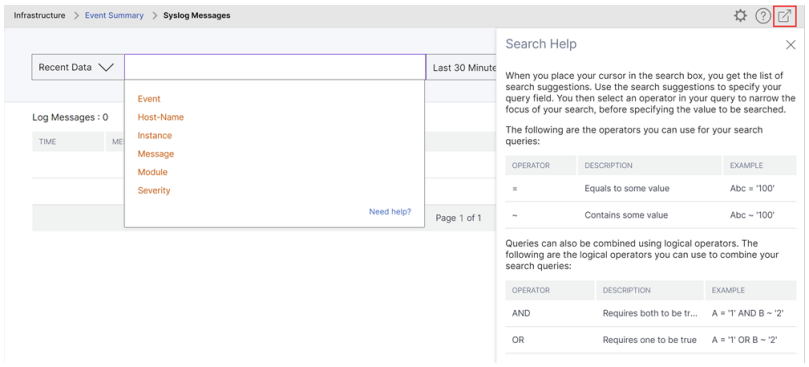
Configurer le service ADM en tant que serveur Syslog

Procédez comme suit pour configurer ADM en tant que serveur syslog :

1. Dans l'interface graphique d'ADM, accédez à **Infrastructure > Instances**.
2. Sélectionnez l'instance NetScaler à partir de laquelle vous souhaitez que les messages syslog soient collectés et affichés dans NetScaler 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 NetScaler, et NetScaler ADM commence à recevoir les messages syslog. Vous pouvez afficher les messages en accédant à **Infrastructure > 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 **Paramètres > Messages du journal d'audit ADM**.

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 **Infrastructure > Fonctions réseau > Audit**.
- Pour afficher les messages du journal d'audit pour une application spécifique dans ADM, accédez à **Applications > Tableau de bord**, cliquez sur un serveur virtuel et sélectionnez **Journal d'audit**.

Gestion des licences NetScaler pour les licences flexibles et groupées

February 1, 2024

> **Remarque :**
>
> Pour plus d'informations sur les différents types de licences NetScaler, consultez la section Présentation des licences.

Tous les détails relatifs à vos licences, tels que les paramètres de port, les fichiers de licence, les informations d'expiration et les paramètres de notification sont répertoriés sur cette page. Vous pouvez appliquer des licences, configurer des contrôles d'expiration des licences et définir des notifications relatives à l'utilisation des licences et aux jours d'expiration.

Paramètres des ports du serveur de licences

Les ports sont utilisés par les instances NetScaler pour communiquer avec le serveur de licences. Cliquez sur **l'icône Modifier et spécifiez les valeurs des paramètres suivants :

- **Port**du serveur de licences : port du serveur proxy utilisé par les instances NetScaler pour accéder au portail de licences Citrix à des fins d'attribution de licences. Valeur par défaut : 27000.
- **Port**du démon fournisseur : port du serveur de licences utilisé par les instances NetScaler pour communiquer avec le serveur de licences. Valeur par défaut : 7279.
- **Port**du serveur proxy : NetScaler ADM peut être utilisé comme proxy HTTP direct pour permettre aux instances NetScaler d'accéder au portail MyCitrix afin de récupérer automatiquement les licences. Pour activer cette fonctionnalité, spécifiez un port TCP sur lequel le proxy écoute.

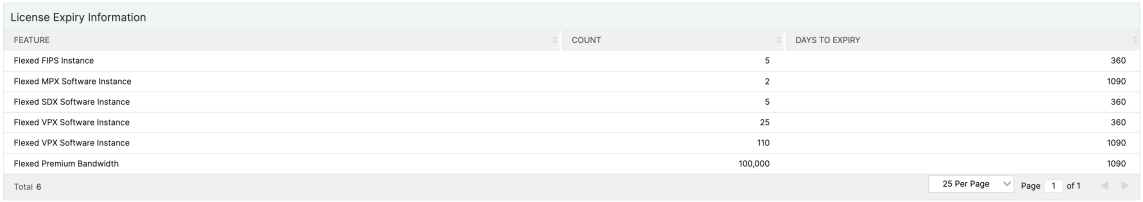
Fichiers de licences

Les fichiers de licence présents sur votre NetScaler sont répertoriés dans cette section. Vous pouvez ajouter, supprimer et télécharger des licences. Vous devez demander des licences avant de pouvoir les utiliser.

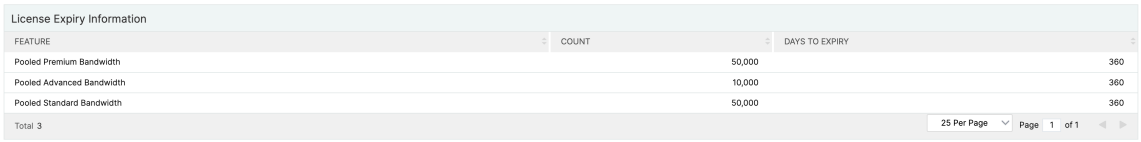
Appliquer un fichier de licence

1. Accédez à **NetScaler Licensing > License Management** .
2. Dans la section **Fichiers de licence** , cliquez sur **Ajouter un fichier de licence** et sélectionnez l'une des options suivantes :
   - **Télécharger des fichiers de licence depuis un ordinateur**local : si un fichier de licence est déjà présent sur votre ordinateur local, vous pouvez le télécharger sur NetScaler ADM.
   - **Utiliser le code**d'accès à la licence : spécifiez le code d'accès à la licence que vous avez achetée auprès de Citrix. Cliquez sur **Obtenir des licences** , puis sur **Terminer** .
3. Cliquez sur **Terminer**.
   Les fichiers de licence sont ajoutés à NetScaler ADM.
   La section **Informations sur l'expiration** des licences répertorie les licences présentes dans NetScaler ADM, leur nombre et les jours restants avant expiration.

   La capture d'écran suivante montre le nombre de licences d'instance logicielle Flexed NetScaler VPX, NetScaler MPX, NetScaler SDX et NetScaler VPX FIPS, la capacité de bande passante premium Flexed présente et les jours jusqu'à expiration.



La capture d'écran suivante montre la bande passante standard, avancée et premium groupée disponible et les jours d'expiration.



4. Sélectionnez un fichier de licence et cliquez sur **Appliquer les licences** .

Supprimer un fichier de licence

Pour supprimer un fichier de licence, sélectionnez un ou plusieurs fichiers et cliquez sur **Supprimer** . Lorsque vous supprimez une licence, vous devez d'abord l'ajouter et c'est seulement à ce moment-là que vous pourrez l'appliquer.

Télécharger un fichier de licence

Pour télécharger un fichier de licence, sélectionnez-le et cliquez sur **Télécharger** . Vous pouvez enregistrer le fichier de licence hors ligne en tant que sauvegarde.

Informations sur l'expiration de la licence

Vous pouvez désormais configurer le seuil d'expiration des licences pour les licences à capacité flexible ou groupée. Lorsque le seuil est défini, NetScaler ADM envoie des notifications par e-mail ou par SMS lorsqu'une licence arrive à expiration. Un piège SNMP et une notification sont également envoyés lorsque la licence a expiré sur NetScaler ADM.

Un événement est généré lorsqu'une notification d'expiration de licence est envoyée et cet événement peut être consulté sur NetScaler ADM depuis **Infrastructure > Événements**.

Afficher l'expiration de la licence

1. Accédez à **NetScaler Licensing > License Management** .
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 sur le point d'expirer.
- **Nombre**: nombre de serveurs virtuels ou d'instances concernés.
- **Jours avant expiration**: nombre de jours avant l'expiration de la licence.

> **Remarque :**
>
> Lorsque vous ajoutez de nouvelles licences au pool, les instances NetScaler utilisent les nouvelles licences à l'expiration de leurs licences existantes.

Paramètres de notification

Spécifiez les paramètres en fonction des notifications qui seront envoyées concernant l'utilisation de la licence et les jours d'expiration.

1. Dans la section **Paramètres de notification** , cliquez sur l'icône **Modifier** et sélectionnez **M' avertir de l'utilisation de la licence** . Définissez le seuil d'alerte, qui correspond à un pourcentage de la capacité de licence flexible ou groupée à utiliser pour envoyer une notification.
2. Choisissez le type de notification que vous souhaitez envoyer lorsque les licences atteignent le seuil ou vont expirer en cochant la case appropriée. Les types de notifications sont les suivants. Sélectionnez un type de notification et cliquez sur **Ajouter** pour ajouter des informations. Vous pouvez également vérifier que chaque notification est envoyée avant d'enregistrer vos paramètres.
   - **E-mail**: profil de messagerie ou liste de distribution pour l'envoi de notifications. Pour plus d'informations, voir Création d'une liste de distribution d'e-mails.
   - **SMS**: profil SMS ou liste de distribution pour l'envoi de notifications.
   - **Slack**: informations du profil Slack pour l'envoi de notifications.
   - **PagerDuty**: profil PagerDuty pour l'envoi de notifications.
   - **ServiceNow**: le profil Citrix ServiceNow est spécifié par défaut et est la seule option disponible actuellement.
     Pour plus d'informations sur la création de ces profils, voir Configurer les notifications
3. Spécifiez les jours d'expiration, c'est-à-dire le nombre de jours avant lesquels vous souhaitez être informé de l'expiration de la licence.
4. Cliquez sur **Enregistrer**.

Création d'une liste de distribution par e-mail

Pour créer une liste de distribution d'e-mails, procédez comme suit :

1. Sélectionnez E-**mail** et cliquez sur **Ajouter** .
2. 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 une notification par e-mail. Pour ajouter un serveur de messagerie, cliquez sur Ajouter. Spécifiez le nom du serveur/l'adresse IP et le port. Sélectionnez Authentification pour autoriser l'authentification à accéder au serveur de messagerie. Sélectionnez Sécurisé si le serveur de messagerie prend en charge l'authentification SSL. Cliquez sur Créer.
- **De : spécifiez l'adresse e**-mail à partir de laquelle NetScaler ADM envoie le message.
- **À**: spécifiez les adresses e-mail auxquelles NetScaler ADM envoie le message.
- **Cc**: spécifiez les adresses e-mail vers lesquelles NetScaler ADM copie le message.
- **Bcc**- Spécifiez les adresses e-mail vers lesquelles le NetScaler ADM copie le message à l'aveugle (sans afficher l'adresse e-mail).

3. Cliquez sur **Créer**.

Création d'une liste de distribution de SMS

Pour configurer les paramètres de notification SMS, procédez comme suit :

1. Dans **SMS**, cliquez sur **Ajouter**.
2. 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. Pour ajouter un serveur SMS, cliquez sur **Ajouter** . Spécifiez les détails du serveur et cliquez sur **Créer** .
   - **À**: spécifiez le numéro de téléphone auquel NetScaler ADM envoie le message.

3. Cliquez sur **Créer**.

Créer un profil Slack

Pour créer un profil Slack, procédez comme suit :

1. Dans **Slack**, cliquez sur **Ajouter**.
2. 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 NetScaler ADM envoie la notification.
   - **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. Toutes les notifications d'événements envoyées à cette URL sont publiées sur la chaîne Slack désignée. Voici un exemple de webhook : https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK.

Création d'un profil PagerDuty

PagerDuty vous permet de configurer les notifications par e-mail, SMS, notifications push et appels téléphoniques sur un numéro enregistré. Avant d'ajouter un profil PagerDuty dans NetScaler Application Delivery and Management, assurez-vous d'avoir effectué les configurations requises dans PagerDuty. Pour commencer à utiliser PagerDuty, consultez la documentation PagerDuty.

Pour créer un profil PagerDuty, procédez comme suit :

1. Dans **PagerDuty**, cliquez sur **Ajouter**.
2. Dans **Créer un profil PagerDuty**, spécifiez les informations suivantes :
   - **Nom**du profil - Spécifiez un nom de profil. Ce nom est utilisé par différents modules, tels que les règles relatives aux événements et les notifications SSL pour envoyer des alertes PagerDuty.
   - **Clé d'intégration** : spécifiez la clé d'intégration. Vous pouvez obtenir cette clé sur votre portail PagerDuty.
3. Cliquez sur **Créer**.

Pour plus d'informations, consultez Services et intégrations dans la documentation PagerDuty.

Afficher le profil ServiceNow

Pour activer les notifications ServiceNow pour les événements NetScaler et les événements NetScaler ADM, vous devez intégrer NetScaler Application Delivery and Management à ServiceNow à l'aide du connecteur ITSM. Pour plus d'informations, voir Intégrer NetScaler ADM à l'instance ServiceNow.

Pour afficher et vérifier le profil ServiceNow, procédez comme suit :

1. Dans **ServiceNow** , le profil **Citrix_Workspace_SN** est sélectionné par défaut.
2. Cliquez sur **Tester** pour générer automatiquement un ticket ServiceNow et vérifier la configuration.

Licence à capacité flexible

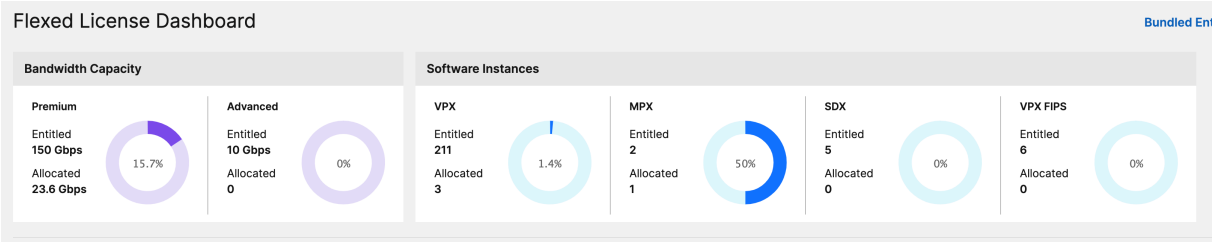
February 1, 2024

Le système de licences NetScaler Flexed est le nouveau cadre de licences visant à simplifier le processus de gestion des licences. Votre licence Flexed inclut des licences d'instance logicielle (VPX/CPX/BLX, SDX, MPX et VPX FIPS) et des licences de capacité de bande passante. Vous devez appliquer la licence Flexed sur le service NetScaler Console ou NetScaler ADM sur site. Vous devez également appliquer les licences MPX Z-Cap et SDX Z-Cap sur le matériel NetScaler MPX et NetScaler SDX respectivement. Vous pouvez ensuite les répartir entre tous les formats NetScaler déployés dans le cloud ou sur site.

Une licence Flexed propose également des analyses pour un nombre illimité de serveurs virtuels.

Si vous possédez une licence groupée et que vous avez acheté une licence Flexed, vous pouvez consulter les détails de votre licence dans le tableau de bord des licences Flexed. La bande passante et les instances combinées apparaissent dans le tableau de bord des licences Flexed.

La licence de bande passante inclut généralement uniquement l'édition Premium, sauf si vous disposiez d'une licence Pooled Standard ou Advanced auparavant, auquel cas les éditions Standard, Advanced et Premium apparaissent dans le tableau de bord des licences Flexed.



Pour plus de détails, consultez le tableau de bord des licences Flexed .

Vous pouvez utiliser les licences Flexed 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.

Collecte de données télémétriques dans le cadre d'une licence Flexed

Pour vous conformer aux exigences de licence Flexed actuelles, veuillez activer ADM On-Prem Cloud Connector. Cette fonctionnalité connecte votre système ADM sur site au service ADM (désormais renommé service NetScaler Console) pour la collecte de données télémétriques. Nous vous recommandons d'activer la collecte de données télémétriques lorsque vous utilisez une licence Flexed. Pour activer ADM On-Prem Cloud Connector, consultez Cloud Connector.

ADM On-Prem Cloud Connector permettra à Citrix Cloud de collecter des données de licence, de configuration et d'utilisation à des fins de conformité des licences, et de gérer, mesurer et améliorer le service. En savoir plussur les données que nous collectons.

> **Remarque :**
>
> Outre ce mode automatisé de collecte de données, un mode manuel permettant d'activer et de partager les données de télémétrie sera disponible dans une prochaine version. Vous pouvez partager les données de télémétrie en mode automatique ou manuel. Une fois que ces deux modes sont disponibles, il est obligatoire de partager les données de télémétrie, faute de quoi le support et la maintenance seront suspendus au bout de 90 jours.

Matériel à capacité nulle

Lorsqu'elles sont gérées par le biais de licences NetScaler Flexed, les instances MPX et SDX sont qualifiées de « matériel à capacité nulle » car elles ne peuvent pas fonctionner tant qu'elles n'ont pas extrait les ressources du pool de bande passante. Ainsi, ces plates-formes sont également appelées appliances MPX-Z et SDX-Z.

Le matériel à capacité nulle nécessite une licence Z-cap pour extraire la bande passante du pool commun.

> **Remarque :**
>
> - L'installation d'une licence à capacité nulle fonctionne de la même manière que les autres licences locales NetScaler. Pour plus d'informations sur l'obtention et l'installation d'une licence à capacité nulle, consultez le guide des licences pour NetScaler.

Gestion et installation des licences Z-cap

Vous devez installer une licence Z-cap manuellement, à l'aide du numéro de série du matériel ou du code d'accès à la licence. Une fois qu'une licence Z-cap est installée, elle est verrouillée sur le matériel et ne peut pas être partagée entre les instances matérielles NetScaler à la demande. Cependant, vous pouvez déplacer manuellement la licence Z-cap vers une autre instance matérielle NetScaler.

Les instances NetScaler MPX exécutant la version 11.1 du logiciel NetScaler version 54.14 ou ultérieure et les instances NetScaler SDX exécutant la version 11.1 build 58.13 ou ultérieure prennent en charge les licences NetScaler Flexed. Pour en savoir plus, voir le **tableau 1. Licences flexibles prises en charge pour les instances**MPX et SDX.

Instances NetScaler VPX autonomes

Les instances NetScaler VPX exécutant le logiciel NetScaler version 11.1 Build 54.14 et versions ultérieures et les hyperviseurs suivants prennent en charge les licences Flexed :

- VMware ESX 6.0

- Citrix Hypervisor
- Linux KVM

Les instances NetScaler VPX exécutant le logiciel NetScaler version 12.0 Build 51.24 et versions ultérieures sur les hyperviseurs et les plateformes cloud suivants prennent en charge les licences Flexed :

- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

Les instances NetScaler VPX exécutant les versions 13.0 et 13.1 du logiciel NetScaler (toutes les versions) sur les hyperviseurs et les plateformes cloud suivants prennent en charge les licences Flexed :

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM
- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

> **Remarque :**
>
> Pour activer la communication entre NetScaler ADM et Microsoft Azure ou AWS, un tunnel IPSEC doit être configuré. Pour plus d'informations, consultez Ajouter des instances NetScaler VPX déployées dans le cloud à NetScaler ADM. Contrairement au matériel à capacité nulle, NetScaler VPX ne nécessite pas de licence à capacité nulle. Pour traiter le trafic, il doit extraire la bande passante et une licence d'instance du pool.

Instances NetScaler CPX autonomes

Les instances NetScaler CPX déployées sur un hôte Docker prennent en charge les licences Flexed. Contrairement au matériel à capacité nulle, NetScaler CPX ne nécessite pas de licence Z-cap. Une seule instance NetScaler CPX consommant un débit allant jusqu'à 1 Gbit/s élimine une seule instance et aucune bande passante du pool de licences. Par exemple, supposons que vous disposez de 20 instances NetScaler CPX avec un pool de bande passante de 20 Gbit/s. Si l'une des instances NetScaler

CPX consomme un débit de 500 Mbit/s, le pool de bande passante reste de 20 Gbit/s pour les 19 instances NetScaler CPX restantes.

Si la même instance NetScaler CPX commence à consommer 1 500 Mbit/s de débit, le pool de bande passante dispose de 19,5 Gbit/s pour les 19 instances NetScaler CPX restantes.

Pour les licences Flexed, vous ne pouvez ajouter de bande passante que par multiples de 10 Mbit/s.

Instances NetScaler BLX autonomes

Les instances NetScaler BLX prennent en charge les licences Flexed. Une instance NetScaler BLX ne nécessite pas de licence Z-cap. Pour traiter le trafic, une instance NetScaler BLX doit extraire de la bande passante et une licence d'instance dans le pool.

Pool de bande passante

Le pool de bande passante est la bande passante totale qui peut être partagée par les instances NetScaler, à la fois physiques et virtuelles. Le pool de bande passante comprend un pool pour l'édition logicielle Premium. Si vous passez d'une licence groupée à une licence flexible, vous pourriez trouver une combinaison d'éditions logicielles Standard, Advanced et Premium. La bande passante d'une instance NetScaler MPX/VPX/CPX/BLX donnée ne peut pas être extraite simultanément de différents pools. 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

Il existe trois types de pools d'instances logicielles :

- Instance logicielle VPX/CPX/BLX
- Instance logicielle MPX (le même pool s'applique à MPX FIPS)
- Instance logicielle SDX (le même pool s'applique à SDX FIPS)
- Instance logicielle VPX FIPS

Une fois extraite du pool, une licence déverrouille les ressources de l'instance logicielle, notamment les CPU/PE, les cœurs SSL, les paquets par seconde et la bande passante.

Serveur de licences NetScaler ADM

Les licences NetScaler Flexed utilisent le NetScaler ADM configuré en tant que serveur de licences pour gérer les licences Flexed : licences de pool de bande passante et licences de pool d'instances.

Lors de l'extraction de licences à partir de la bande passante et du pool d'instances, le facteur de forme NetScaler et le numéro de modèle matériel d'un matériel à capacité nulle déterminent

- La bande passante minimale et le nombre d'instances qu'une instance NetScaler doit récupérer avant d'être fonctionnelle.
- La bande passante maximale et le nombre d'instances qu'un NetScaler peut récupérer.
- 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 NetScaler 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 NetScaler est de 1 Gbit/s, 1 000 Mbit/s peuvent être extraits, mais pas 200 Mbit/s ni 150,5 Gbit/s. L'unité de bande passante minimale est différente de la largeur de bande minimale requise. Une instance NetScaler 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/les instances maximales, la bande passante/les instances minimales et l'unité de bande passante minimale pour toutes les instances NetScaler prises en charge. Le tableau 5 récapitule les exigences de licence pour différents formats pour toutes les instances NetScaler prises en charge. Les tableaux suivants font référence à la configuration requise.

> **Remarque :**
>
> L'unité de débit de bande passante minimale pour NetScaler CPX/BLX/VPX est de 10 Mbit/s. L'unité de débit de bande passante minimale pour NetScaler MPX/SDX est de 1 Gbit/s.

Tableau 1A. Capacité flexible prise en charge pour MPX

Ligne de produits	Bande passante minimale (Gbps)	Bande passante maximale (Gbit/s)	Unité de bande passante minimale
MPX 5900Z	1	10	1 Gbit/s
MPX 8900Z	5	30	1 Gbit/s
MPX 8900Z FIPS	5	20	1 Gbit/s
MPX 9100Z	10	95	1 Gbit/s
MPX 9100Z FIPS	10	95	1 Gbit/s
MPX 14000Z	20	100	1 Gbit/s
MPX 14000Z-40G	20	100	1 Gbit/s

Ligne de produits	Bande passante minimale (Gbps)	Bande passante maximale (Gbit/s)	Unité de bande passante minimale
MPX 14000Z-40S	40	100	1 Gbit/s
MPX 14000Z FIPS	30	80	1 Gbit/s
MPX 15000 Hz	20	120	1 Gbit/s
MPX 15000Z-50G	20	120	1 Gbit/s
MPX 15000Z FIPS	30	120	1 Gbit/s
MPX 16 000 Hz	30	250	1 Gbit/s
MPX 22000Z	40	120	1 Gbit/s
MPX 24000Z	100	150	1 Gbit/s
MPX 25000Z	100	160	1 Gbit/s
MPX 25000Z-40G	100	200	1 Gbit/s
MPX 26000Z	100	200	1 Gbit/s
MPX 26000Z-50S	100	200	1 Gbit/s
MPX 26000Z-100 G	100	200	1 Gbit/s

Tableau 1A. Capacité flexible prise en charge pour la version NetScaler SDX antérieure à la version 13.0-47.x

Ligne de produits	Bande passante minimale (Gbps)	Bande passante maximale (Gbit/s)	Instances minimales	Nombre maximum d’ instances	Unité de bande passante minimale
SDX 8900Z	10	30	2	7	1 Gbit/s
SDX 14000Z	20	100	5	25	1 Gbit/s
SDX 14000Z-40G	40	100	20	25	1 Gbit/s
SDX 15000Z	20	120	5	55	1 Gbit/s
SDX 15000Z-50G	20	120	5	55	1 Gbit/s
SDX 22000Z	40	120	80	80	1 Gbit/s

Ligne de produits	Bande passante minimale (Gbps)	Bande passante maximale (Gbit/s)	Instances minimales	Nombre maximum d' instances	Unité de bande passante minimale
SDX 24000Z	100	150	80	80	1 Gbit/s
SDX 25000Z	100	200	20	115	1 Gbit/s
SDX 25000Z-40G	100	200	20	115	1 Gbit/s
SDX 26000Z	100	200	20	115	1 Gbit/s
SDX 26000Z-50S	100	200	20	115	1 Gbit/s
SDX 26000Z-100G	100	200	20	115	1 Gbit/s

Tableau 1B. Capacité flexible prise en charge pour NetScaler SDX version 13 (version 13.0-47.x et versions ultérieures), version 13.1 (version antérieure à 51.x) et version 14.1 (version antérieure à 12.x)

Ligne de produits	Bande passante minimale (Gbps)	Bande passante maximale (Gbit/s)	Instances minimales	Nombre maximum d' instances	Unité de bande passante minimale
SDX 8900Z	5	30	1	7	1 Gbit/s
SDX 9100Z	10	95	2	7	1 Gbit/s
SDX 14000Z	10	100	2	25	1 Gbit/s
SDX 14000Z-40G	20	100	10	25	1 Gbit/s
SDX 15000Z	10	120	2	55	1 Gbit/s
SDX 15000Z-50G	10	120	2	55	1 Gbit/s
SDX 16000Z	15	250	10	55	1 Gbit/s
SDX 22000Z	20	120	40	80	1 Gbit/s
SDX 24000Z	50	150	40	80	1 Gbit/s

Ligne de produits	Bande passante minimale (Gbps)	Bande passante maximale (Gbit/s)	Instances minimales	Nombre maximum d' instances	Unité de bande passante minimale
SDX 25000Z	50	200	10	115	1 Gbit/s
SDX 25000Z-40G	50	200	10	115	1 Gbit/s
SDX 26000Z	50	200	10	115	1 Gbit/s
SDX 26000Z-50S	50	200	10	115	1 Gbit/s
SDX 26000Z-100G	50	200	10	115	1 Gbit/s

Tableau 1C. Capacité flexible prise en charge pour NetScaler SDX version 13.1 (build 51.x et versions ultérieures) et version 14.1 (build 12.x et versions ultérieures)

Ligne de produits	Bande passante minimale (Gbps)	Bande passante maximale (Gbit/s)	Instances minimales	Nombre maximum d' instances	Unité de bande passante minimale
SDX 8900Z	5	30	1	7	1 Gbit/s
SDX 9100Z	10	95	1	7	1 Gbit/s
SDX 14000Z	10	100	1	25	1 Gbit/s
SDX 14000Z-40G	20	100	1	25	1 Gbit/s
SDX 15000Z	10	120	1	55	1 Gbit/s
SDX 15000Z-50G	10	120	1	55	1 Gbit/s
SDX 16000Z	15	250	1	55	1 Gbit/s
SDX 22000Z	20	120	1	80	1 Gbit/s
SDX 24000Z	50	150	1	80	1 Gbit/s
SDX 25000Z	50	200	1	115	1 Gbit/s

Ligne de produits	Bande passante minimale (Gbps)	Bande passante maximale (Gbit/s)	Instances minimales	Nombre maximum d'instances	Unité de bande passante minimale
SDX 25000Z-40G	50	200	1	115	1 Gbit/s
SDX 26000Z	50	200	1	115	1 Gbit/s
SDX 26000Z-50S	50	200	1	115	1 Gbit/s
SDX 26000Z-100G	50	200	1	115	1 Gbit/s

Remarques :

- La quantité minimale d'achat peut être différente de la configuration minimale requise.
- Sur NetScaler SDX exécutant les versions 14.1-12.x et ultérieures, avec une licence Flexed, la restriction visant à extraire un nombre minimum de licences d'instance est supprimée. En d'autres termes, vous pouvez consulter au moins une licence d'instance.

Tableau 2. Bande passante minimale/maximale et instances minimales/maximales prises en charge pour les instances NetScaler 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. Bande passante minimale/maximale et instances minimale/maximale prises en charge pour les instances NetScaler 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. Bande passante minimale/maximale et instances minimales/maximales prises en charge pour les instances NetScaler 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. Licence de capacité nulle pour différents formats

Ligne de produits	Matériel à capacité nulle
MPX	Licence requise
SDX	Licence requise
VPX	-

Ligne de produits	Matériel à capacité nulle
CPX	-
BLX	-

Configuration des licences flexibles

February 1, 2024

> **Remarque :**
>
> Si vous avez des licences groupées et que vous avez maintenant acheté et appliqué des licences Flexed, les droits combinés apparaissent dans le tableau de bord des licences Flexed.

Les licences NetScaler Flexed vous permettent de partager des licences de bande passante ou d'instance entre différents formats NetScaler. Utilisez cette capacité flexible pour les instances situées dans le centre de données ou dans 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 sur d'autres instances NetScaler nécessitant des ressources.

Vous pouvez utiliser les licences Flexed 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.

Vous pouvez effectuer les tâches suivantes dans NetScaler ADM :

1. Téléchargez les fichiers de licence Flexed (pool de bande passante ou pool d'instances logicielles) sur le serveur de licences.

   > **Remarque :**
   >
   > Le serveur de licences est le serveur NetScaler ADM sur site.

2. Téléchargez les licences SDX ou MPX à capacité nulle sur le matériel SDX ou MPX, et attribuez des licences du pool de licences aux instances NetScaler à la demande.

   - Consultez les licences des instances NetScaler en fonction de la capacité minimale et maximale de l'instance.

Vous pouvez télécharger des licences Flexed, notamment des licences de bande passante, d'instance et Z-cap sur citrix.com. Pour plus d'informations, consultez le guide de licence pour NetScaler.

États de licence NetScaler Flexed

Les états de licence Flexed indiquent la licence requise sur une instance NetScaler. Les instances NetScaler configurées avec les licences Flexed présentent l'un des états suivants :

- **Alloué**: l'instance fonctionne avec une capacité de licence appropriée.
- **Grace** : l'instance est exécutée sur une licence de grâce.
- **Connexion perdue**: la communication entre NetScaler ADM et l'instance ne fonctionne pas.

Avant de commencer

Assurez-vous que les conditions préalables suivantes sont remplies avant de configurer les licences Flexed :

- Les `27000`ports et `7279`sont accessibles depuis NetScaler vers NetScaler ADM, pour vérifier les licences. Voir la section Configuration requise.

Étape 1 - Appliquer des licences dans NetScaler ADM

1. Accédez à **NetScaler Licensing > License Management** .
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 NetScaler 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 NetScaler ADM à partir des **paramètres de licence**.

3. Cliquez sur **Terminer**.

   Les fichiers de licence sont ajoutés à NetScaler ADM. La section **Informations sur l'expiration** des licences répertorie les licences présentes dans NetScaler ADM et les jours restants avant 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 NetScaler d'utiliser la licence sélectionnée en tant que licence Flexed.

Étape 2 - Enregistrer NetScaler ADM en tant que serveur de licences et attribuer des licences

Vous pouvez enregistrer NetScaler ADM en tant que serveur de licences pour une instance NetScaler.

Enregistrer un serveur NetScaler ADM à l'aide de l'interface graphique

Dans l'interface graphique de NetScaler ADM, enregistrez le serveur NetScaler ADM associé à une instance NetScaler.

1. Connectez-vous à l'interface graphique de NetScaler.
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 NetScaler ADM associé qui est enregistré auprès de NetScaler ADM.
6. Sélectionnez **S'inscrire auprès de NetScaler ADM.**
7. Entrez les informations d'identification de votre serveur NetScaler ADM pour enregistrer une instance auprès de NetScaler ADM et cliquez sur **Continuer**. Dans NetScaler ADM, l'un des serveurs est le serveur de licences.
8. Dans **Allouer des licences**, sélectionnez l'édition de la licence et spécifiez la bande passante requise.

   Pour la première fois, attribuez des licences dans NetScaler. Vous pouvez ultérieurement modifier ou libérer l'allocation de licences à partir de l'interface graphique NetScaler 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.

Ajouter un serveur NetScaler ADM à l'aide de l'interface de ligne de commande

Si une instance NetScaler ne possède pas d'interface graphique, utilisez les commandes CLI suivantes pour ajouter un serveur NetScaler ADM associé à une instance :

1. Connectez-vous à la console NetScaler.
2. Ajoutez l'adresse IP du serveur NetScaler ADM associé qui est enregistré auprès de NetScaler ADM. Le port de licence par défaut est 27000.

```
1 > add ns licenseserver <adm-server-IP-address> -port <adm-server-
     license-port-number>
2 <!--NeedCopy-->
```

3. Affichez la bande passante de licence disponible sur le serveur de licences :

```
1 > sh ns licenseserverpool
2 <!--NeedCopy-->
```

4. Allouez la bande passante de licence à partir de l'édition de licence requise :

```
1 > set ns capacity -unit gbps -bandwidth <specify-license-bandwidth
     > edition <specify-license-edition>
2 <!--NeedCopy-->
```

> **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 - Modifier la bande passante flexible pour les instances NetScaler

1. Accédez à **NetScaler Licensing > Flexed Licensing > Dashboard** .
2. Dans la section **NetScalers sous licence** , sélectionnez une instance et cliquez sur **Modifier la bande passante**.
3. Sur la page **Modifier la bande passante** , entrez un nombre dans la colonne **Allouer** .
4. Cliquez sur **Envoyer**.

NetScaler MPX-Z

MPX-Z est l'appliance NetScaler MPX à capacité flexible. MPX-Z prend en charge le pool de bande passante pour les licences Premium uniquement.

MPX-Z nécessite une licence pour pouvoir se connecter au serveur de licences. Vous pouvez installer la licence 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 MPX-Z, MPX perd sa licence. Les licences sont transmises au 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 Flexed requises pour sa capacité configurée.

NetScaler SDX-Z

SDX-Z est l'appliance NetScaler SDX à capacité flexible. SDX-Z prend en charge la bande passante et le pool d'instances pour les licences de l'édition Premium.

SDX-Z nécessite une licence pour pouvoir se connecter au serveur de licences. Vous pouvez installer la licence SDX-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 SDX-Z, SDX perd sa licence. Les licences sont transmises au serveur de licences.

Vous pouvez modifier dynamiquement la bande passante d'une instance SDX-Z sans redémarrer.

> **Remarque :**
>
> Lorsque vous redémarrez l'instance, elle extrait automatiquement les licences Flexed requises pour sa capacité configurée.

Paire de haute disponibilité NetScaler

Avant de commencer, assurez-vous que le serveur NetScaler ADM est configuré en tant que serveur de licences. Pour plus d'informations, voir Configurer NetScaler ADM en tant que serveur de licences

Lorsque vous allouez la bande passante à une paire NetScaler HA, NetScaler ADM extrait la bande passante allouée à l'instance principale. Vous devez répéter le processus pour l'instance secondaire.

Pour attribuer des licences de pool à une paire NetScaler HA, voir Allouer des licences flexibles aux instances NetScaler

La page **Flexed Capacity** affiche les instances et leur capacité allouée séparément.

Tableau de bord flexible des licences

February 1, 2024

Le tableau de bord des licences Flexed vous donne une vue complète de la capacité de bande passante et des instances que vous avez achetées.

La capacité de bande passante entre les éditions et les détails des instances pour différents formats, tels que MPX, VPX et SDX, sont affichés sur cette page. NetScaler MPX et NetScaler MPX FIPS ont le même fichier de licence. De même, NetScaler SDX et NetScaler SDX FIPS ont le même fichier de licence. Cependant, NetScaler VPX FIPS possède un fichier différent de NetScaler VPX et s'affiche séparément. En outre, NetScaler BLX et NetScaler CPX nécessitent des licences NetScaler VPX et font partie de l'autorisation et de l'allocation de VPX. Une licence Flexed ne prend en charge que l'édition premium. Toutefois, si vous avez acheté des licences Flexed et que vous disposiez auparavant d'une capacité de bande passante standard ou avancée groupée, les informations relatives à la capacité de bande passante (Standard ou Advanced) sont également répertoriées dans le tableau de bord des licences Flexed.

Les informations relatives à vos instances NetScaler sous licence sont disponibles dans la section **Licensed** NetScaler. Vous pouvez sélectionner une instance et modifier la bande passante ou libérer la licence pour cette instance.

Vous pouvez filtrer les résultats en fonction des paramètres suivants :

- Filtrer par bande passante
  - Premium
  - Advanced
  - Standard
- Facteur de forme
  - NetScaler MPX
  - NetScaler VPX
  - NetScaler SDX

- État de la licence
  - Connexion perdue
  - Grace
  - Attribué

Modifier la bande passante allouée sur une instance NetScaler

1. Accédez à **NetScaler Licensing > Flexed Licensing > Dashboard** .
2. Dans la section **NetScalers sous licence** , sélectionnez une instance et cliquez sur **Modifier la bande passante**.
3. Sur la page **Modifier la bande passante** , entrez un nombre dans la colonne **Allouer** .
4. Cliquez sur **Envoyer**.

Délivrez des licences sur une instance NetScaler

Pour transférer des licences vers une autre instance, vous devez libérer la licence sur l'instance actuelle, puis appliquer la licence à la nouvelle instance. La sélection de **Release License** permet d' effectuer les opérations suivantes :

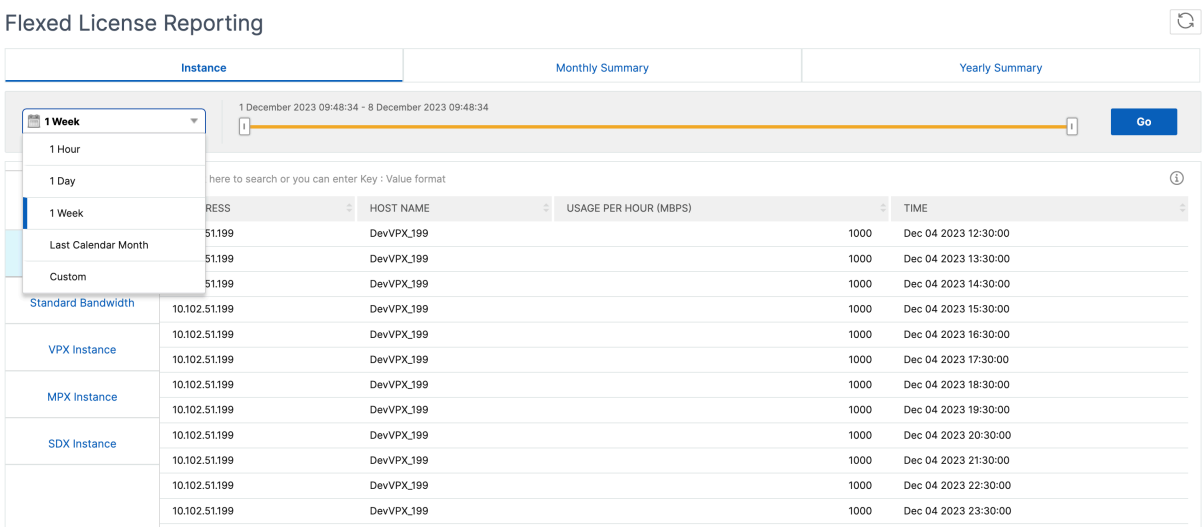
- Libère toutes les licences, qui sont extraites sur cette instance, vers le serveur de licences.
- Supprime la configuration du serveur de licences sur cette instance.

Si vous sélectionnez **Oui** , votre instance NetScaler perd sa licence et ne peut traiter aucun trafic.

Rapports flexibles sur les licences

February 1, 2024

Vous pouvez consulter les détails relatifs à votre instance logicielle et à l'attribution de licences de bande passante et à vos droits pour connaître la quantité allouée sur ce droit. Vous pouvez consulter les détails de l'instance, tels que l'instance qui consomme la quantité de bande passante (utilisation par heure) et l'heure à laquelle elle le fait. Vous pouvez spécifier une période allant d'une heure à une période personnalisée.



Les vues graphiques sont disponibles dans les onglets **Résumé mensuel** et **Résumé annuel** . Les graphiques suivants présentent quelques exemples de droits et d'allocations d'instances logicielles.

Capacité groupée de NetScaler

February 1, 2024

La capacité NetScaler Pooled vous permet de partager la bande passante ou les licences d'instance entre différents formats NetScaler. 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 situées dans le centre de données ou dans 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 NetScaler nécessitant des 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 provisionnement des instances.

Fonctionnement des licences de capacité NetScaler Pooled

La capacité groupée de NetScaler comprend les éléments suivants :

- Les instances NetScaler, qui peuvent être classées dans les catégories suivantes :
  - Matériel à capacité nulle
  - Instances NetScaler VPX autonomes ou instances NetScaler CPX ou instances NetScaler BLX
- Pool de bande passante
- Pool d'instances
- NetScaler ADM configuré en tant que serveur de licences

Matériel à capacité nulle

Lorsqu'elles sont gérées via la capacité groupée NetScaler, les instances MPX et SDX sont qualifiées de « matériel à capacité nulle » car elles 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. Consultez le tableau 1 de cette page pour connaître les capacités groupées prises en charge pour les instances MPX et SDX. Consultez le tableau 5 pour les exigences de licence pour les différents formats MPX et SDX.
> - L'installation d'une licence à capacité nulle fonctionne de la même manière que les autres licences locales NetScaler. Pour plus d'informations sur l'obtention et l'installation d'une licence à capacité nulle, consultez le guide des licences pour NetScaler.

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 NetScaler à la demande. Toutefois, vous pouvez déplacer manuellement la licence de plate-forme vers une autre instance matérielle NetScaler.

Les instances NetScaler MPX exécutant la version 11.1 du logiciel NetScaler version 54.14 ou ultérieure et les instances NetScaler SDX exécutant la version 11.1 build 58.13 ou ultérieure prennent en charge la capacité NetScaler Pooled. Pour en savoir plus, voir le **tableau 1. Capacité groupée prise en charge pour les instances**MPX et SDX.

Instances NetScaler VPX autonomes

Les instances NetScaler VPX exécutant le logiciel NetScaler version 11.1 Build 54.14 et versions ultérieures et les hyperviseurs suivants prennent en charge la capacité groupée :

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM

Les instances NetScaler VPX exécutant le logiciel NetScaler version 12.0 Build 51.24 et versions ultérieures sur les hyperviseurs et les plateformes cloud suivants prennent en charge la capacité groupée :

- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

Les instances NetScaler VPX exécutant les versions 13.0 et 13.1 du logiciel NetScaler (toutes les versions) sur les hyperviseurs et les plateformes cloud suivants prennent en charge la capacité groupée :

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM
- Microsoft Hyper-V

- AWS
- Microsoft Azure
- Google Cloud

> **Remarque**
>
> Pour permettre la communication entre NetScaler ADM et Microsoft Azure ou AWS, un tunnel IPSEC doit être configuré. Pour plus d'informations, voir Ajouter des instances NetScaler VPX déployées dans le cloud àNetScaler ADM.
> Contrairement au matériel à capacité nulle, NetScaler 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 NetScaler CPX autonomes

Les instances NetScaler CPX déployées sur un hôte Docker prennent en charge la capacité groupée. Contrairement au matériel à capacité nulle, NetScaler CPX ne nécessite pas de licence de plateforme. Une seule instance NetScaler CPX consommant un débit allant jusqu'à 1 Gbit/s élimine une seule instance et aucune bande passante du pool de licences. Par exemple, supposons que vous disposez de 20 instances NetScaler CPX avec un pool de bande passante de 20 Gbit/s. Si l'une des instances NetScaler CPX consomme un débit de 500 Mbit/s, le pool de bande passante reste de 20 Gbit/s pour les 19 instances NetScaler CPX restantes.

Si la même instance NetScaler CPX commence à consommer 1 500 Mbit/s de débit, le pool de bande passante dispose de 19,5 Gbit/s pour les 19 instances NetScaler CPX restantes.

Pour les licences de pool, vous pouvez ajouter plus de bande passante uniquement en multiples de 10 Mbps.

Instances NetScaler BLX autonomes

Les instances NetScaler BLX prennent en charge les licences de capacité groupée. Une instance NetScaler BLX ne nécessite pas de licence de plate-forme. Pour traiter le trafic, une instance NetScaler BLX doit extraire de la bande passante et une licence d'instance dans le pool.

Pool de bande passante

Le pool de bande passante est la bande passante totale qui peut être partagée par les instances NetScaler, à la fois physiques et virtuelles. Le pool de bande passante comprend des pools distincts pour chaque édition logicielle (Standard, Advanced et Premium). La bande passante de différents pools ne peut pas être extraite simultanément pour une instance NetScaler donnée. 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 NetScaler VPX ou d'instances NetScaler CPX ou d'instances NetScaler BLX qui peuvent être gérées via la capacité NetScaler Pooled ou le nombre d'instances NetScaler VPX dans une instance SDX-Z.

Une fois retirée du pool, une licence déverrouille les ressources de l'instance MPX-Z, SDX-Z, VPX, NetScaler CPX et NetScaler BLX, notamment 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 NetScaler ADM

La capacité groupée de NetScaler utilise le NetScaler ADM configuré en tant que serveur de licences pour gérer les licences de capacité groupée : licences de pool de bande passante et licences de pool d'instances. Vous pouvez utiliser le logiciel NetScaler ADM pour gérer les licences de capacité groupée sans licence NetScaler ADM.

Lors de l'extraction de licences à partir de la bande passante et du pool d'instances, le facteur de forme NetScaler et le numéro de modèle matériel d'un matériel à capacité nulle déterminent

- La bande passante minimale et le nombre d'instances qu'une instance NetScaler doit récupérer avant d'être fonctionnelle.
- La bande passante maximale et le nombre d'instances qu'un NetScaler peut récupérer.
- 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 NetScaler 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 NetScaler est de 1 Gbit/s, 1 000 Mbit/s peuvent être extraits, mais pas 200 Mbit/s ni 150,5 Gbit/s. L'unité de bande passante minimale est différente de la largeur de bande minimale requise. Une instance NetScaler 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/les instances maximales, la bande passante/les instances minimales et l'unité de bande passante minimale pour toutes les instances NetScaler prises

en charge. Le tableau 5 résume les exigences de licence pour différents formats pour toutes les instances NetScaler 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 8900Z	30	5	SO	SO	1 Gbit/s
MPX 9100Z	30	10	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
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 16000Z series	200	30	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

Ligne de produits	Bande passante maximale (Gbit/s)	Bande passante minimale (Gbps)	Instances minimales	Nombre maximum d' instances	Unité de bande passante minimale
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 8900Z	30	10	1	7	1 Gbit/s
SDX 9100Z	95	20	1	7	1 Gbit/s
SDX 14000Z series	100	10	1	25	1 Gbit/s
SDX 14000Z 40G series	100	1	2	25	1 Gbit/s
SDX 14000Z 40S series	100	20	1	25	1 Gbit/s
SDX 14000Z FIPS series	100	10	1	25	1 Gbit/s
SDX 15000Z 50G	120	10	1	55	1 Gbit/s
SDX 15000Z	120	10	1	55	1 Gbit/s
SDX 16000Z series	200	15	1	55	1 Gbit/s
SDX 22000Z series	120	20	1	80	1 Gbit/s
SDX 25000Z 40G	200	50	1	115	1 Gbit/s
SDX 25000ZA	200	50	1	115	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 26000Z 100G	200	50	1	115	1 Gbit/s
SDX 26000Z	200	50	1	115	1 Gbit/s
SDX 26000Z 50S	200	50	1	115	1 Gbit/s
Série SDX 24000Z	150	50	1	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 NetScaler 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 NetScaler 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 NetScaler 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 à la bande passante et aux éditions	Abonnement aux instances
MPX	Licence requise	Licence requise	-
SDX	Licence requise	Licence requise	Licence requise

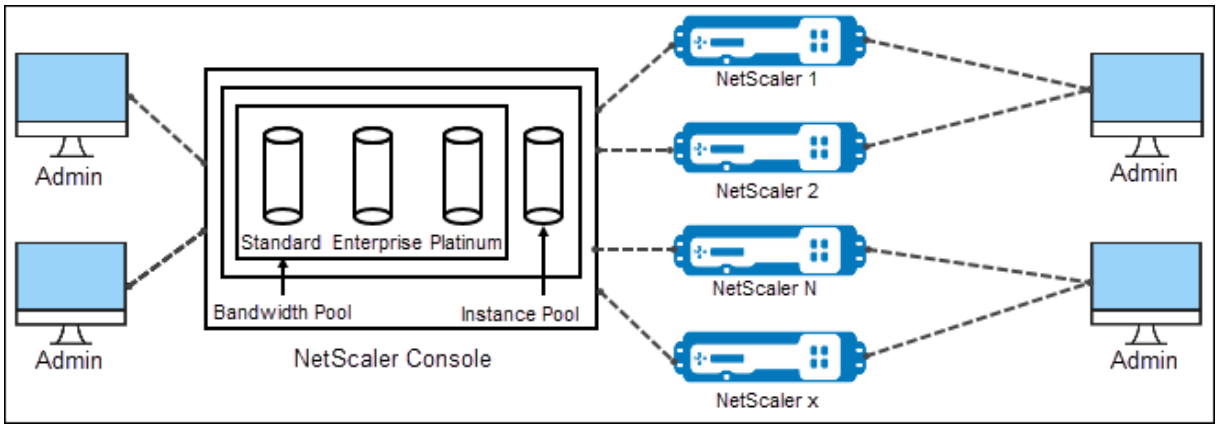
Ligne de produits	Achat de matériel à capacité nulle	Abonnement à la bande passante et aux éditions	Abonnement aux instances
VPX	-	Licence requise	Licence requise
CPX	-	-	Licence requise
BLX	-	Licence requise	Licence requise

Configurer la capacité groupée de NetScaler

February 1, 2024

Pour utiliser la capacité NetScaler Pooled, configurez NetScaler ADM en tant que serveur de licences pour les instances NetScaler requises. Les instances NetScaler enregistrent et retirent des licences auprès de NetScaler ADM. Vous pouvez effectuer les tâches suivantes dans l'interface graphique de distribution et de gestion des applications NetScaler :

- Téléchargez les fichiers de licence de capacité groupée (bande passante et pool d'instances) sur le serveur de licences.
- Allouez des licences du pool de licences aux instances NetScaler à la demande.
- Consultez les licences des instances NetScaler (MPX-Z /SDX-Z/VPX/CPX/BLX) en fonction de la capacité minimale et maximale de l'instance.
- Configurez la capacité groupée pour que les instances NetScaler FIPS puissent enregistrer ou retirer des licences.



Versions matérielles et logicielles prises en charge

Pour connaître les versions matérielles et logicielles prises en charge pour la capacité groupée, consultez la section NetScaler Pooled capacity.

États des capacités groupées de NetScaler

Les états de capacité groupée indiquent la licence requise pour une instance NetScaler. Les instances NetScaler configurées avec une capacité groupée présentent 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 de NetScaler ADM pour la gestion, ou la communication NITRO entre NetScaler ADM et les instances ne fonctionne pas.
- **Non alloué** : la licence n'est pas allouée dans l'instance.

Étape 1 - Appliquer des licences dans NetScaler ADM

1. Dans NetScaler ADM, accédez à **NetScaler Licensing > Pooled Licensing** .
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 NetScaler 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 NetScaler ADM à partir des **paramètres de licence**.

3. Cliquez sur **Terminer**.

   Les fichiers de licence sont ajoutés à NetScaler ADM. L'onglet **Informations d'expiration** des licences répertorie les licences présentes dans NetScaler ADM et les jours restants avant 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 NetScaler d'utiliser la licence sélectionnée en tant que capacité groupée.

Pour plus d'informations sur la façon d'appliquer des licences groupées à NetScaler Application Delivery and Management, consultez la vidéo correspondante :

Il s'agit d'une vidéo intégrée. Cliquez sur le lien pour visionner la vidéo

Étape 2 - Enregistrer NetScaler ADM en tant que serveur de licences

Pour enregistrer NetScaler ADM en tant que serveur de licences pour une instance NetScaler, suivez l'une des procédures suivantes :

- Utiliser l'interface graphique
- Utiliser l'interface de ligne de commande

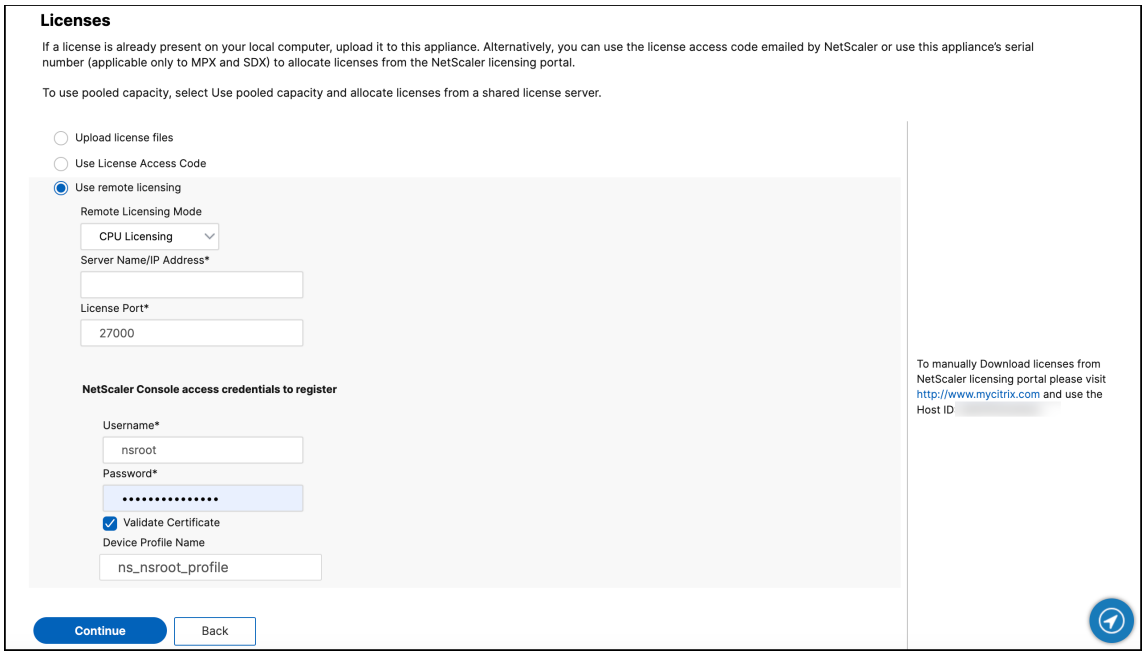
Utiliser l'interface graphique pour enregistrer NetScaler ADM en tant que serveur de licences

Dans l'interface graphique de NetScaler, enregistrez le serveur NetScaler ADM en tant que serveur de licences.

1. Connectez-vous à l'interface graphique de NetScaler.
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 NetScaler ADM.

   > Pour un déploiement HA, utilisez une adresse IP flottante. Pour plus d'informations sur la configuration, voir Configurer le déploiement à haute disponibilité.
   >
   > Pour un déploiement utilisant un NetScaler ADM autonome ou un agent, consultez la section Présentation des licences

6. Sélectionnez **S'inscrire auprès de NetScaler ADM.**
7. Entrez vos informations d'identification NetScaler ADM pour enregistrer une instance auprès de NetScaler 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, attribuez des licences dans NetScaler. Vous pouvez ultérieurement modifier ou libérer l'allocation de licences à partir de l'interface graphique NetScaler ADM.

   a) 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 l'interface de ligne de commande pour ajouter NetScaler ADM en tant que serveur de licences

Si une instance NetScaler ne possède pas d'interface graphique, utilisez les commandes CLI suivantes pour ajouter le serveur NetScaler ADM en tant que serveur de licences :

1. Connectez-vous à la console NetScaler.
2. Ajoutez l'adresse IP du serveur NetScaler ADM :


```
> add ns licenseserver <adm-server-IP-address> -port <adm-server-port-number> -licensemode <license-mode>
<!--NeedCopy-->
```

Pour plus d'informations, consultez la section Présentation des licences.

3. Afficher la bande passante de licence disponible sur le serveur de licences.

```
> sh ns licenseserverpool
<!--NeedCopy-->
```

Cette commande répertorie les licences en fonction du mode de licence spécifié lors de l'ajout du serveur de licences.

Exemple1 :

Si le mode de licence spécifié est `CICO`, la sortie ne contient que des licences CICO.

```
> add licenseserver [redacted] -licensemode CICO
 Done
> sh licenseserverpool
        VPX8000P Total                  : 1
        VPX8000P Available              : 1
```

Exemple-2 :

Si le mode de licence spécifié est `Pooled`, la sortie contient uniquement des licences de capacité groupée.

```
> add licenseserver [redacted] -licensemode Pooled
 Done
> sh licenseserverpool
        Instance Total                  : 40
        Instance Available              : 38
        Standard Bandwidth Total        : 210.00 Gbps
        Standard Bandwidth Available    : 210.00 Gbps
        Enterprise Bandwidth Total      : 50.00 Gbps
        Enterprise Bandwidth Available  : 50.00 Gbps
        Platinum Bandwidth Total        : 210.00 Gbps
        Platinum Bandwidth Available    : 205.00 Gbps
```

Exemple3 :

Si le mode de licence spécifié est `vCPU`, la sortie contient uniquement des licences d'UC virtuelles.

```
> add licenseserver [redacted] -licensemode vCPU
 Done
> sh licenseserverpool
        Standard CPU Total              : 100
        Standard CPU Available          : 100
        Enterprise CPU Total            : 100
        Enterprise CPU Available        : 100
        Platinum CPU Total              : 25
        Platinum CPU Available          : 20
```


Pour afficher toutes les licences ensemble, exécutez la commande suivante :

```
> sh ns licenseserverpool -getallLicenses
<!--NeedCopy-->
```

Exemple de sortie :

```
> sh licenseserverpool -getallLicenses
        Instance Total                      : 40
        Instance Available                  : 33
        Standard Bandwidth Total            : 210.00 Gbps
        Standard Bandwidth Available        : 210.00 Gbps
        Enterprise Bandwidth Total          : 50.00 Gbps
        Enterprise Bandwidth Available      : 50.00 Gbps
        Platinum Bandwidth Total            : 210.00 Gbps
        Platinum Bandwidth Available        : 205.00 Gbps
        VPX8000P Total                      : 1
        VPX8000P Available                  : 1
        Standard CPU Total                  : 100
        Standard CPU Available              : 100
        Enterprise CPU Total                : 100
        Enterprise CPU Available            : 100
        Platinum CPU Total                  : 25
        Platinum CPU Available              : 20
```

4. Allouez la bande passante de licence à partir de l'édition de licence requise :

```
> set ns capacity -unit <specify-mbps-or-gbps> -bandwidth <specify
    -amount-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 - Allouer des licences groupées aux instances NetScaler

Pour attribuer des licences de capacité groupée à partir de l'interface graphique NetScaler ADM, procédez comme suit :

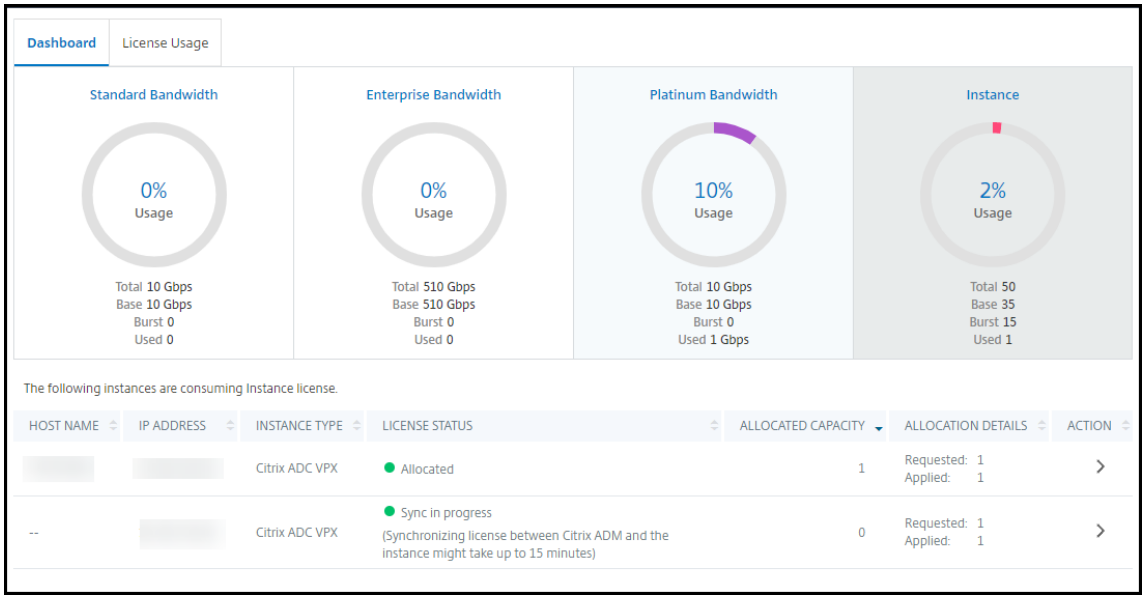
1. Connectez-vous à NetScaler ADM.
2. Accédez à **Infrastructure > Licences > Licences de bande passante > Capacité groupée**.

   La capacité de l'instance FIPS apparaît uniquement si vous chargez des licences d'instance FIPS vers NetScaler 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 NetScaler.
>
> 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 NetScaler dans la liste des instances disponibles en cliquant sur le bouton **>**.

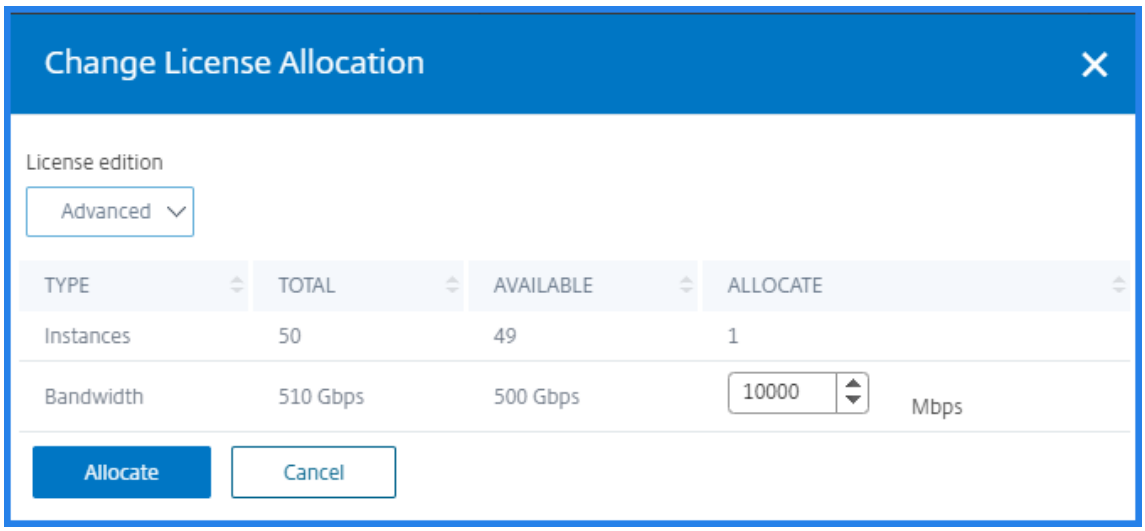


La colonne **STATUT DE LA LICENCE** affiche les messages d'état d'allocation de licence correspondants.

> **Remarque :**
>
> L'onglet **Instances non gérées** affiche les instances découvertes mais non gérées dans NetScaler 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 la liste d'**allocation** . 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 une instance si vous modifiez l'édition de la licence.

Pour plus d'informations sur la façon de modifier l'allocation de bande passante, voir la vidéo correspondante :

Il s'agit d'une vidéo intégrée. Cliquez sur le lien pour visionner la vidéo

Configurer la capacité groupée sur les instances NetScaler

Vous pouvez configurer des licences de capacité groupée sur les instances NetScaler suivantes :

- Instances NetScaler
- Instances NetScaler VPX
- Paire de haute disponibilité NetScaler

Instances NetScaler MPX

MPX-Z est l'appliance NetScaler MPX dotée de capacités groupées. 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 la plateforme 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 NetScaler VPX

Une instance NetScaler VPX dotée de capacités groupées peut extraire des licences d'un pool de bande passante (éditions Advanced/Standard). Vous pouvez utiliser l'interface graphique de NetScaler pour extraire les licences 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 groupée configurées sont automatiquement extraites du serveur NetScaler ADM.

Paire de haute disponibilité NetScaler

Avant de commencer, assurez-vous que le serveur NetScaler ADM est configuré en tant que serveur de licences. Pour plus d'informations, voir Configurer NetScaler ADM en tant que serveurde licences.

Pour les instances NetScaler 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 attribuer une licence de pool à chaque nœud de la paire, suivez les étapes indiquées dans Allouer des licences groupées aux instances NetScaler. Attribuez d'abord la licence au premier nœud, puis répétez les mêmes étapes pour attribuer la licence au second nœud.

Mettre à niveau une licence perpétuelle de NetScaler VPX vers la capacité NetScaler Pooled

February 1, 2024

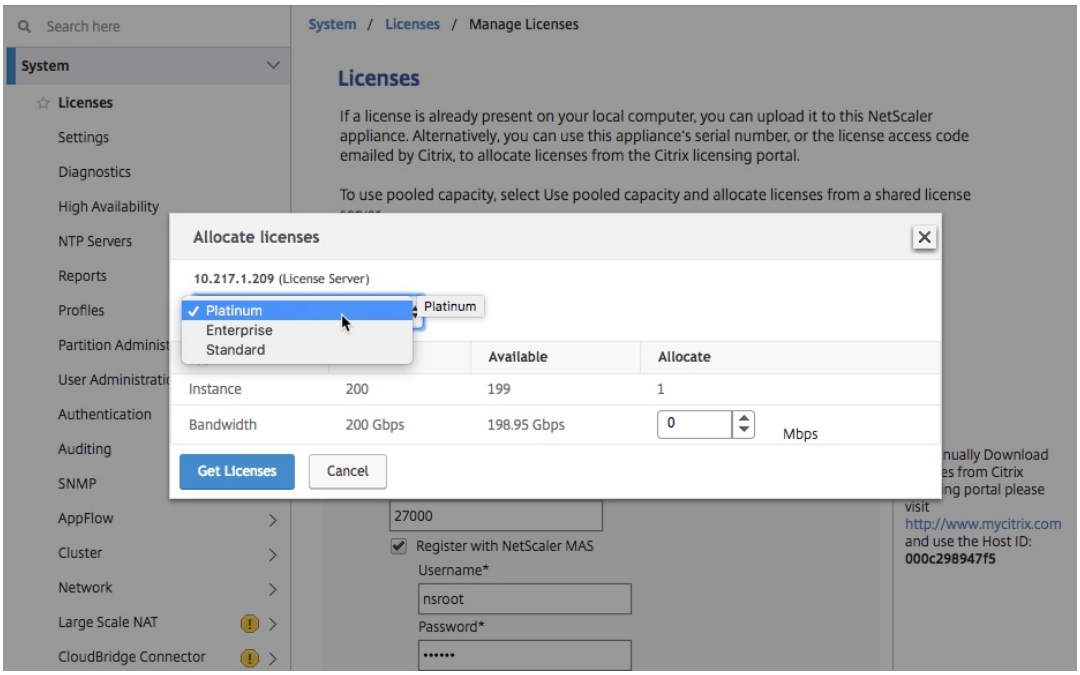
Les instances NetScaler VPX dotées d'une licence perpétuelle peuvent être mises à niveau vers une licence ADC Pooled Capacity. La mise à niveau vers une licence de capacité groupée vous permet d'attribuer des licences du pool de licences aux instances VPX à la demande. Vous pouvez également configurer une licence de capacité groupée pour les instances ADC configurées en mode haute disponibilité. Pour configurer une licence de capacité groupée pour les instances VPX en mode haute disponibilité, consultez Mise à niveau de la licence perpétuelle de NetScaler VPX High Availability Pair vers NetScaler Pooled Capacity .

Conditions préalables

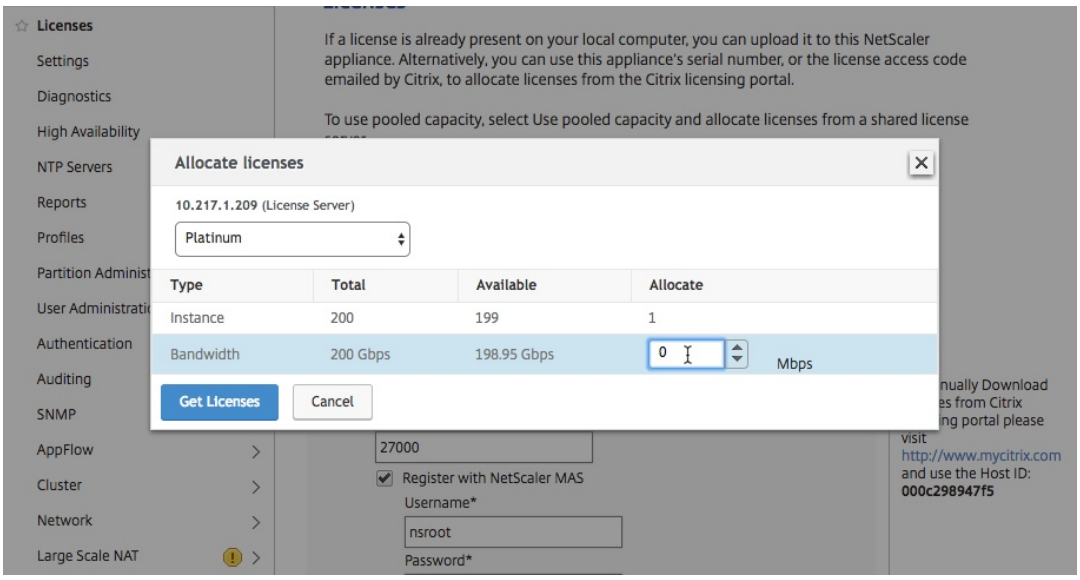
Pour passer à la capacité NetScaler Pooled, procédez comme suit :

1. Dans un navigateur Web, saisissez l'adresse IP de l'instance VPX, par exemple http://192.168.100.1.
2. Dans **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 **S'inscrire auprès de NetScaler ADM** est cochée et entrez les informations d'identification NetScaler ADM si vous souhaitez gérer les licences de pool de votre instance via NetScaler ADM.
    d) Cliquez sur **Continuer**.
7. Dans **Allouer des licences**, procédez comme suit :

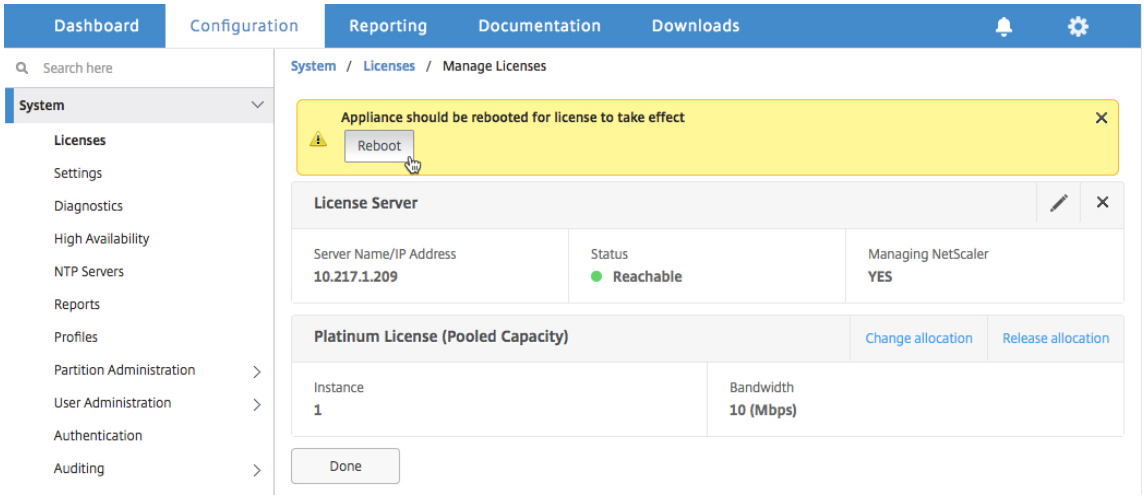
a) Sélectionnez l'édition de licence dans la liste déroulante.



b) Allouez la bande passante à l'appliance NetScaler depuis le menu **Allocation** 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 sous licence sur l'appliance NetScaler 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.

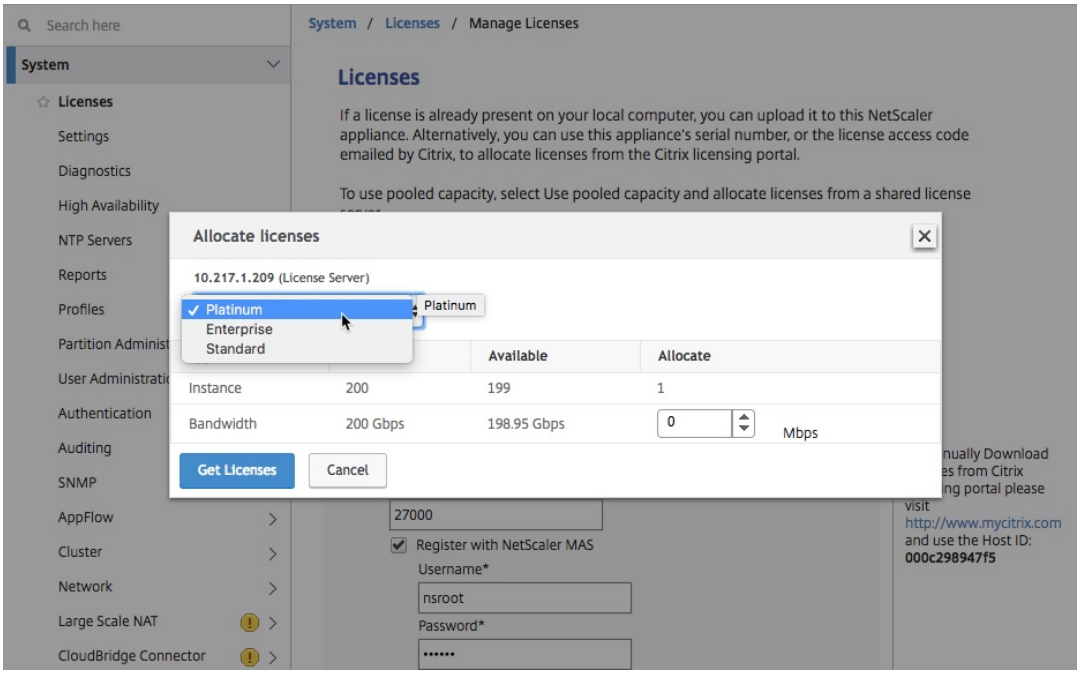
Mettez à niveau la licence perpétuelle de la paire de haute disponibilité NetScaler VPX vers la capacité NetScaler Pooled

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.

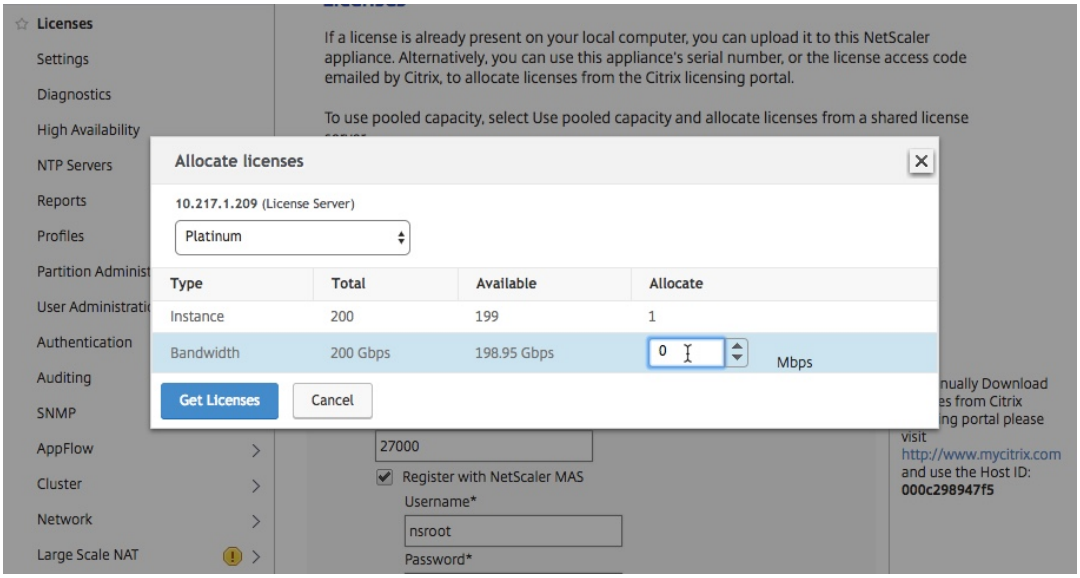
Pour mettre à niveau une configuration NetScaler VPX HA existante vers NetScaler Pooled Capacity :

1. Ouvrez une session sur l'instance VPX secondaire (nœud 2). Dans un navigateur Web, tapez l' adresse IP de l'appliance NetScaler, par exemple. `http://192.168.100.1`
2. Dans **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification de l'administrateur.

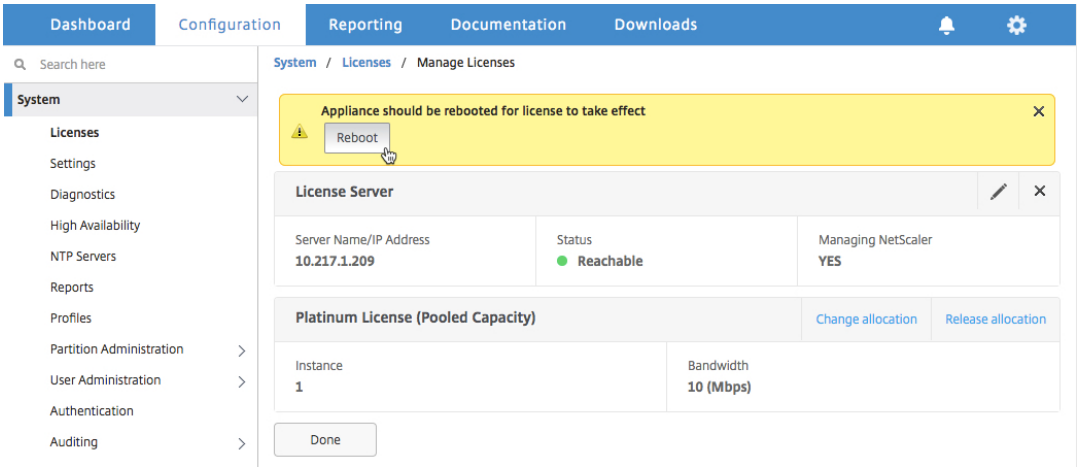
3. Sur la page **Bienvenue**, cliquez sur **Continuer**.
4. Sous l'onglet Configuration, accédez à **Système > Licences**, puis cliquez sur **Gérer les licences**.
5. Sur la page **Licences**, cliquez sur **Ajouter une nouvelle licence**.
6. Choisissez **Utiliser les licences à distance** et procédez 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 **S'inscrire auprès de NetScaler ADM** est cochée et entrez les informations d'identification NetScaler ADM si vous souhaitez gérer les licences de pool de votre instance via NetScaler ADM.
    d) Cliquez sur **Continuer**.
7. Dans **Allouer des licences**, procédez comme suit :
    a) Sélectionnez l'édition de licence dans la liste déroulante.



    b) Allouez la bande passante à l'appliance NetScaler depuis le menu **Allocation** 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. Après le basculement, connectez-vous à la nouvelle instance VPX secondaire (nœud 1) et répétez le même processus pour ajouter la nouvelle instance secondaire au pool.

   Si vous souhaitez modifier les instances principale et secondaire de la paire HA en fonction de 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-->
```


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 de NetScaler MPX vers la capacité NetScaler Pooled

February 1, 2024

NetScaler MPX avec licence perpétuelle peut être mis à niveau vers la licence NetScaler Pooled Capacity. La mise à niveau vers la licence NetScaler Pooled Capacity vous permet d'allouer des licences du pool de licences aux appliances NetScaler à la demande. Vous pouvez également configurer une licence de capacité NetScaler Pooled pour les instances NetScaler configurées en mode haute disponibilité. Pour configurer une licence NetScaler Pooled Capacity pour les instances NetScaler MPX en mode haute disponibilité, consultez Mise à niveau de la licence perpétuelle de la paire NetScaler MPX High Availability vers NetScaler Pooled capacity.

> **Remarque**
>
> La conversion d'une licence perpétuelle à une licence à capacité groupée est un processus à sens unique pour l'attribution des droits de licence. Vous ne pouvez pas rétablir la licence de capacité groupée à perpétuelle.
>
> **Important**
>
> Pour mettre à niveau NetScaler MPX vers une licence de capacité NetScaler Pooled, vous devez télécharger la licence MPX-Z sur l'appliance.

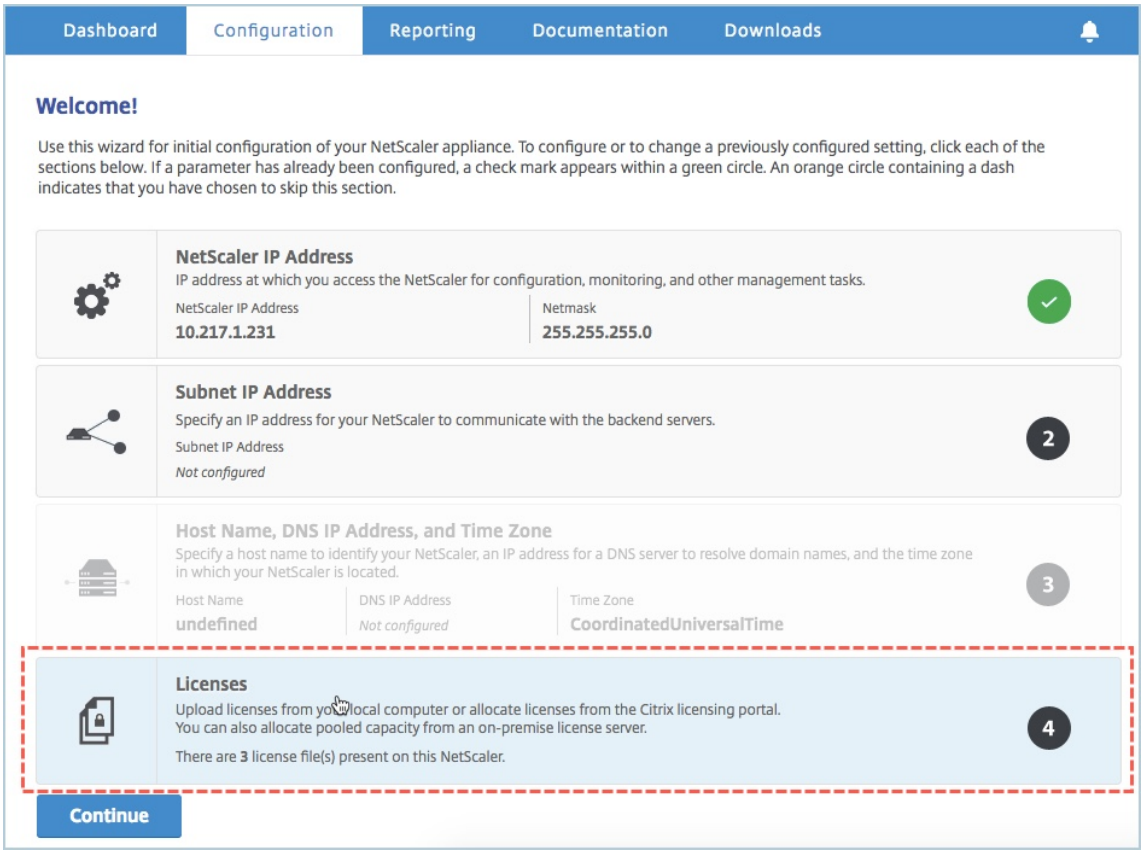
Pour passer à la capacité NetScaler Pooled, procédez comme suit :

1. Dans un navigateur Web, saisissez l'adresse IP du NetScaler, par exemplehttp://192.168.100.1.
2. Dans **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification de l'administrateur.
3. Sur la page **Bienvenue**, cliquez sur **Continuer**.

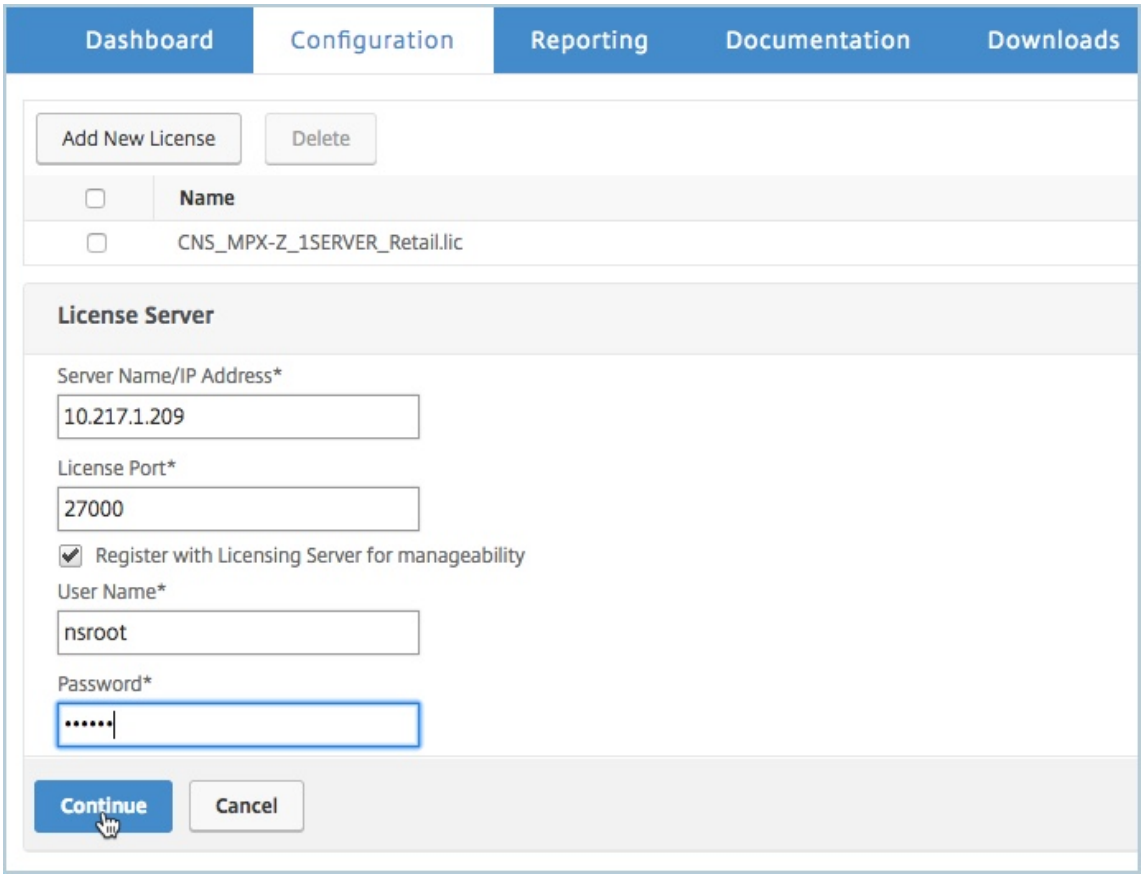
4. Téléchargez la licence à capacité nulle (licence MPX-Z). Sous l'onglet Configuration, accédez à **Système** > **Licences**.
5. Dans le volet d'informations, cliquez sur **Gérer les licences** , puis sur Ajouter une **nouvelle licence** .
6. Sur la page **Licences** , sélectionnez Charger les **fichiers de licence** et cliquez **sur**Parcourir pour sélectionner la licence à capacité nulle sur 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 NetScaler ADM, en utilisant le protocole 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.

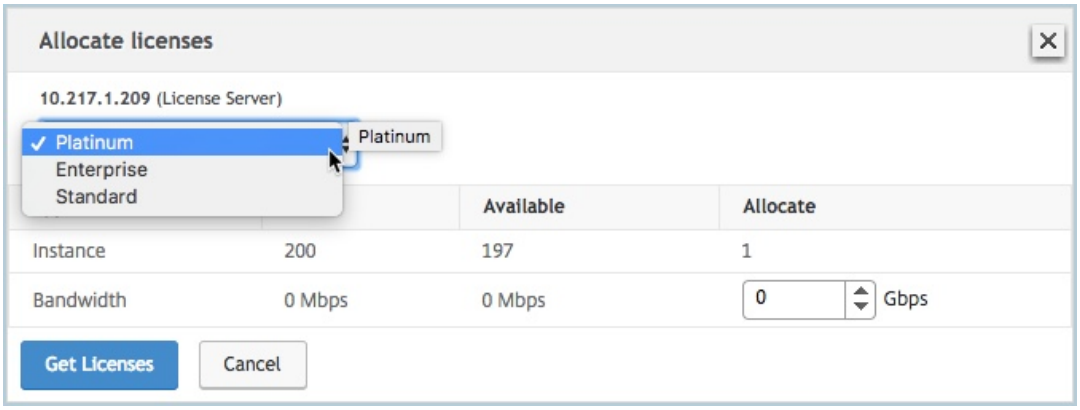
b) Dans le champ **Port de licence**, entrez le port du serveur de licences. Valeur par défaut : 27000.

c) Si vous souhaitez gérer les licences de pool de votre instance via NetScaler ADM, cochez la case **S'inscrire auprès du serveur de licences pour la gérabilité** et entrez les informations d'identification NetScaler ADM.

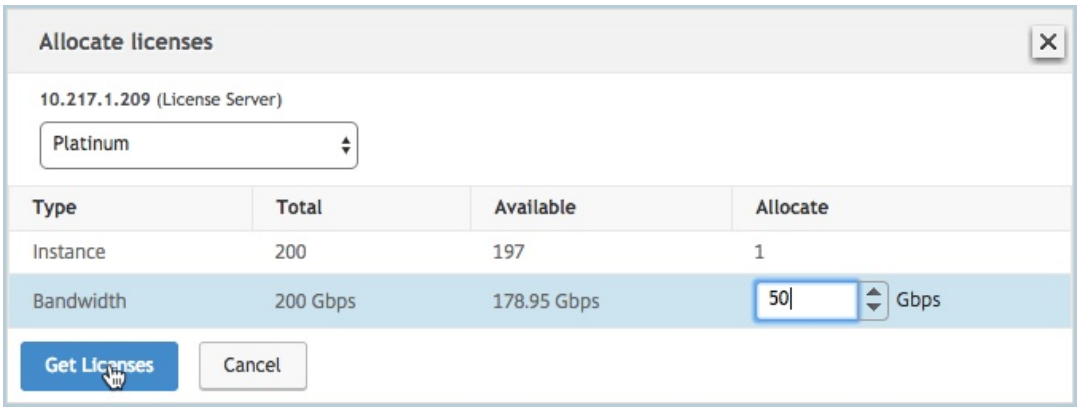
d) Cliquez sur **Continuer**.

12. Dans **Allouer des licences**, procédez comme suit :

a) Sélectionnez l'édition de licence dans la liste déroulante.



b) Allouez la bande passante à NetScaler depuis le menu **Allouer**, puis cliquez sur **Obtenir des licences**.



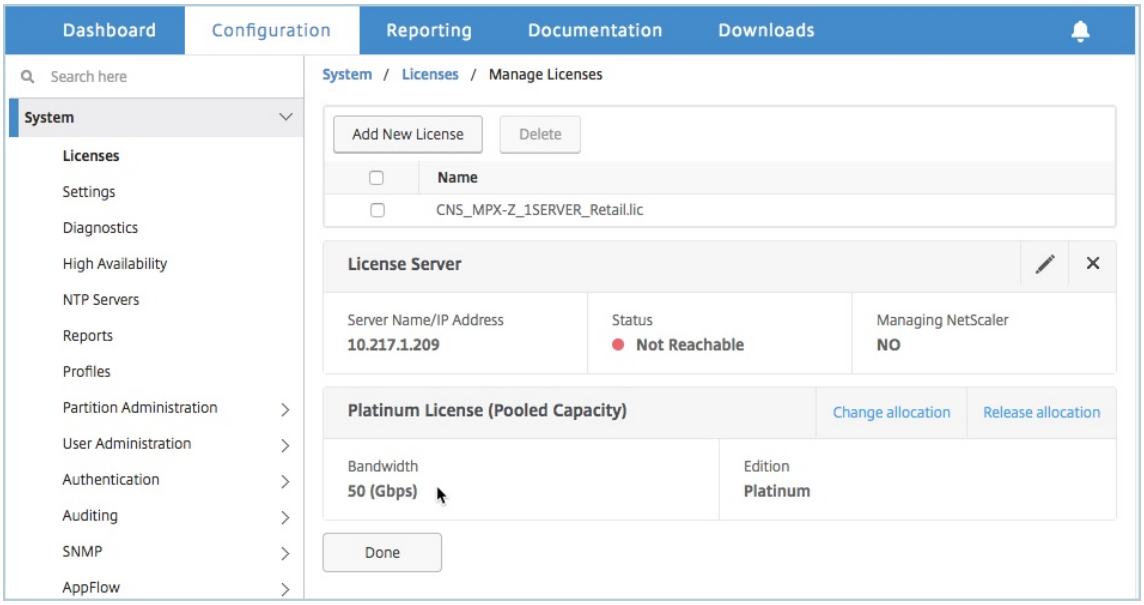
c) Lorsque vous y êtes invité, cliquez sur **Redémarrer** pour redémarrer l'appliance.

13. Une fois NetScaler MPX redémarré, connectez-vous à NetScaler 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 de la paire haute disponibilité NetScaler MPX vers la capacité NetScaler Pooled

Pour les appliances MPX configurées en mode haute disponibilité, vous devez configurer la capacité groupée sur les instances NetScaler principale et secondaire de la paire HA. Allouez des licences de même capacité aux instances NetScaler principale et secondaire 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 à chacune des instances NetScaler principale et secondaire de la paire HA.

> **Important**
>
> Pour mettre à niveau NetScaler MPX afin d'utiliser la licence de capacité NetScaler Pooled, 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 vers les instances NetScaler MPX de la paire HA :

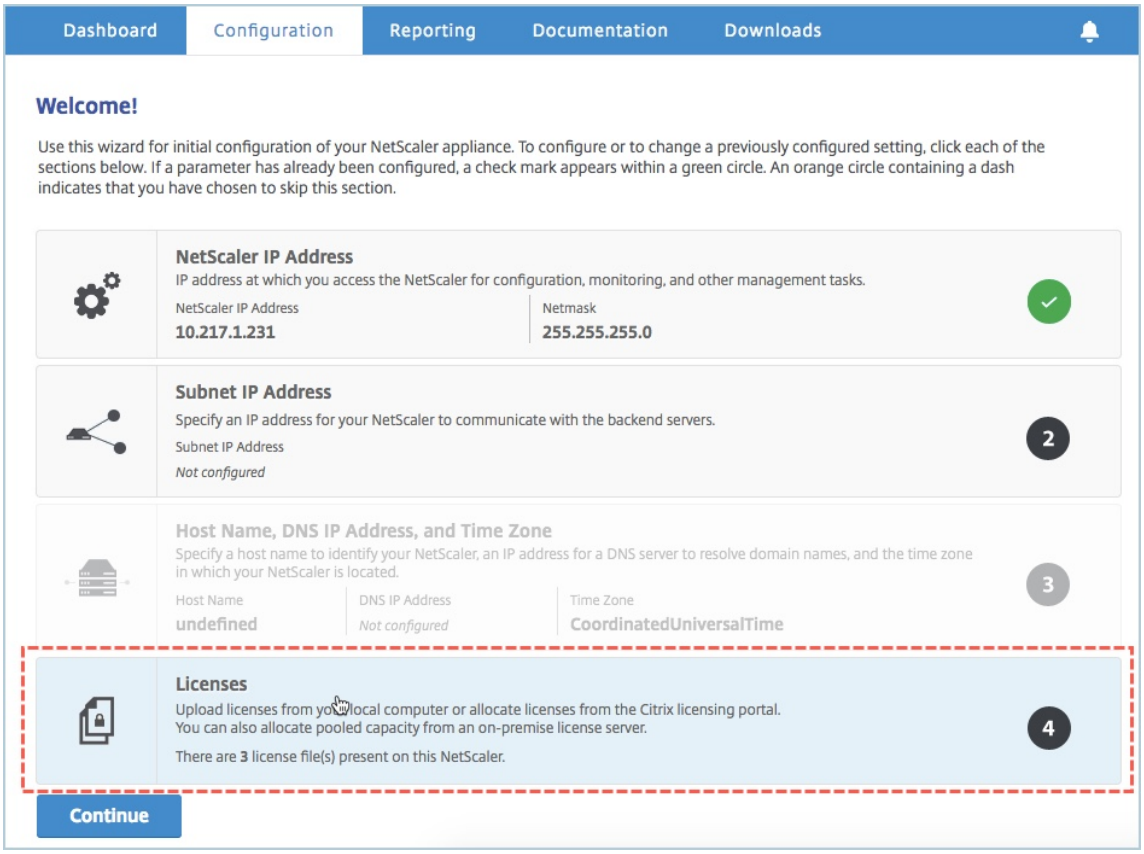
1. Dans un navigateur Web, saisissez l'adresse IP de l'appliance, telle que http://192.168.100.1.
2. Dans **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification de l'administrateur.
3. Sur la page **Bienvenue**, cliquez sur **Continuer**.

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. Sur la page **Licences** , sélectionnez Charger les **fichiers de licence** et cliquez **sur**Parcourir pour sélectionner la licence à capacité nulle sur votre machine locale.

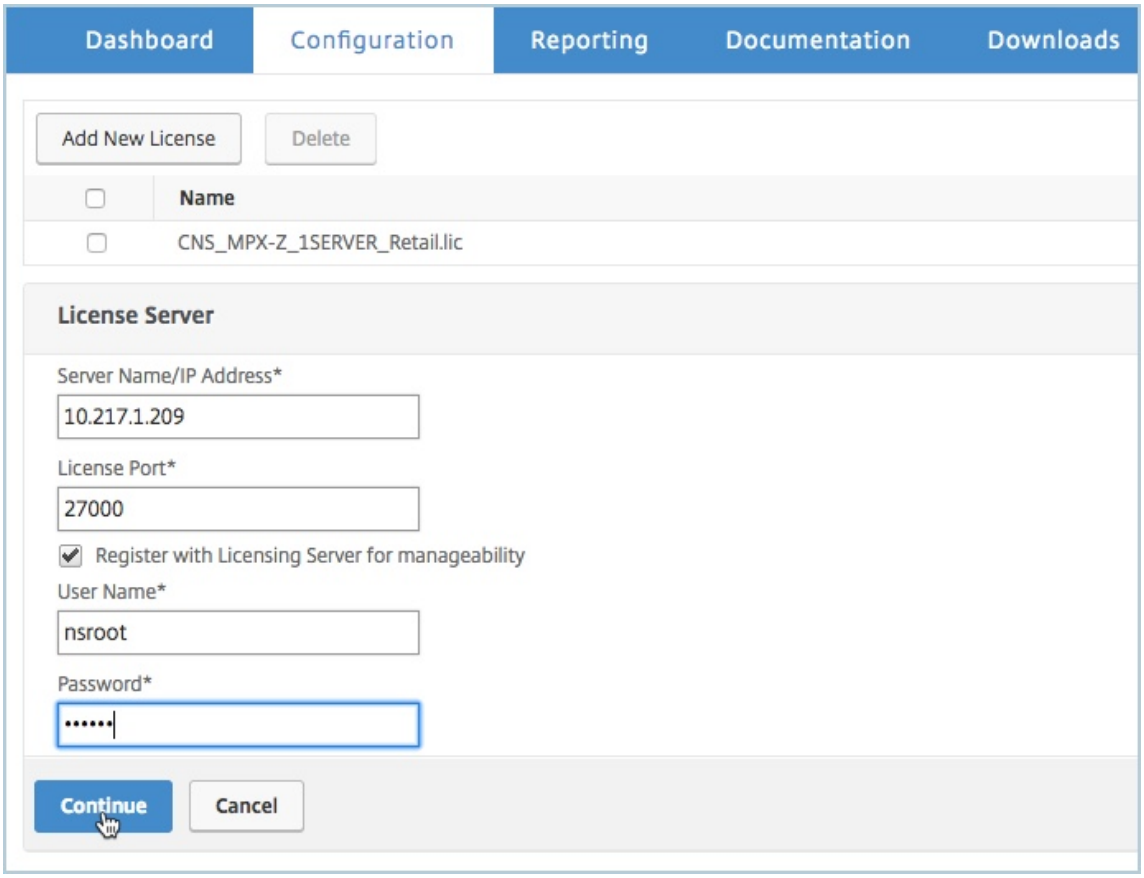
   Une fois la licence téléchargée, vous êtes invité à redémarrer l'appliance.
7. Cliquez sur **Redémarrer** pour redémarrer l'appliance.
8. Sur la page **Confirmer**, cliquez sur **Oui**.

Pour mettre à niveau une configuration HA existante vers NetScaler Pooled Capacity :

1. Connectez-vous à l'instance NetScaler MPX secondaire. Dans un navigateur Web, saisissez l'adresse IP de NetScaler, par exemplehttp://192.168.100.1.
2. Dans **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.

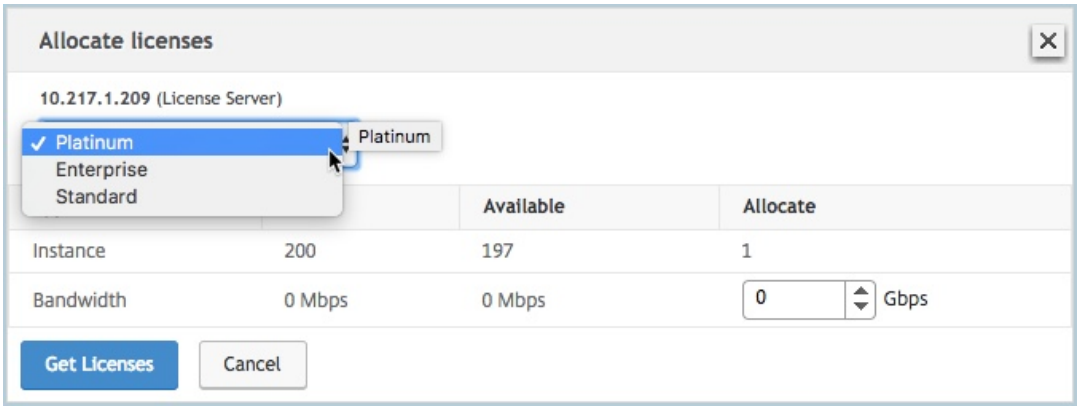
b) Dans le champ **Port de licence**, entrez le port du serveur de licences. Valeur par défaut : 27000.

c) Si vous souhaitez gérer les licences de pool de votre instance via NetScaler ADM, cochez la case **S'inscrire auprès du serveur de licences pour la gérabilité** et entrez les informations d'identification NetScaler ADM.

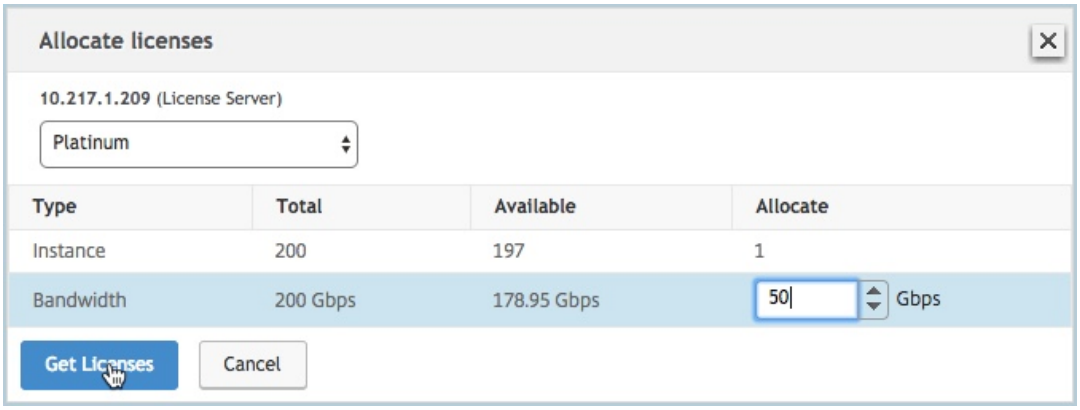
d) Cliquez sur **Continuer**.

5. Dans **Allouer des licences**, procédez comme suit :

a) Sélectionnez l'édition de licence dans la liste déroulante.



b) Allouez la bande passante à NetScaler depuis le menu **Allouer**, puis 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. Ouvrez une session sur le NetScaler MPX principal existant et redémarrez l'appliance. Procédez comme suit :

   a) Dans un navigateur Web, saisissez l'adresse IP du NetScaler, par exemplehttp://192.168.100.1.

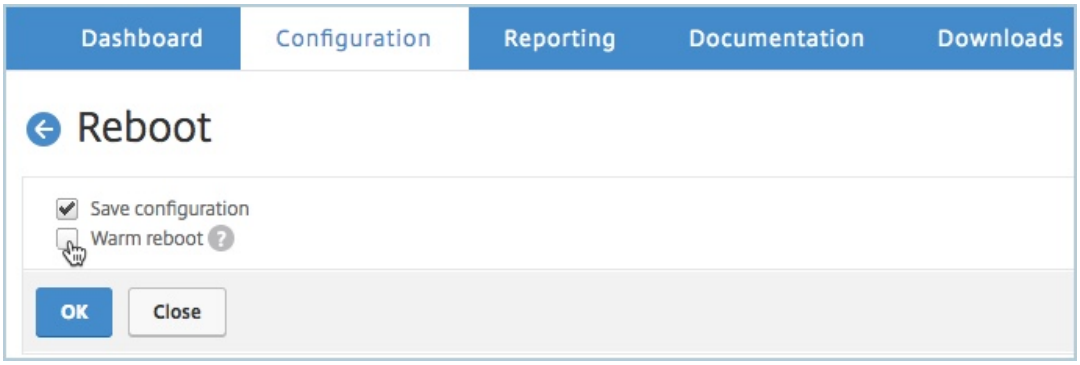
   b) Dans **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification de l'administrateur.

   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 NetScaler MPX principal, il devient le NetScaler MPX secondaire de la paire HA. Si vous souhaitez modifier les instances principale et secondaire de la paire HA en fonction de 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
<!--NeedCopy-->
```

Mettre à niveau une licence perpétuelle d'un NetScaler SDX vers une capacité NetScaler Pooled

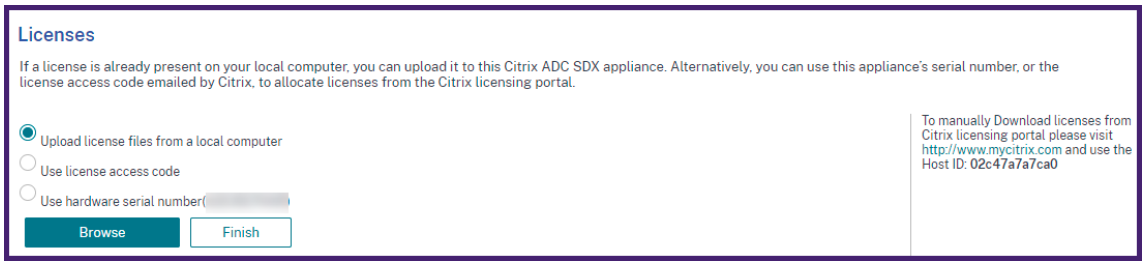
February 1, 2024

NetScaler SDX avec licence perpétuelle peut être mis à niveau vers une licence de capacité NetScaler Pooled. La mise à niveau vers la licence NetScaler Pooled Capacity vous permet d'attribuer des licences du pool de licences à NetScaler à la demande. Vous pouvez également configurer une licence de capacité NetScaler Pooled pour les instances NetScaler configurées en mode haute disponibilité.

> **Important**
>
> La conversion d'une licence perpétuelle à une licence à capacité groupée est un processus d'attribution de licence unidirectionnel. Vous ne pouvez pas rétablir la licence de capacité groupée à perpétuelle.
>
> - Pour mettre à niveau NetScaler SDX vers la licence NetScaler Pooled Capacity, vous devez télécharger la licence SDX-Z sur l'appliance.
> - Assurez-vous que vous êtes autorisé à ajouter des instances NetScaler dans NetScaler ADM.
> - Pour garantir l'absence d'impact sur les licences actuelles, le client doit allouer le même nombre d'instances et de bande passante que celui disponible dans le cadre de la licence perpétuelle.

Pour passer à la capacité NetScaler Pooled, procédez comme suit :

1. Dans un navigateur Web, saisissez l'adresse IP de NetScaler SDX, par exemplehttp://192.168.100.1.
2. Dans **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. Sur la page **Licences** , sélectionnez **Charger les fichiers de licence depuis un ordinateur local** et cliquez **sur**Parcourir pour sélectionner la licence à capacité nulle depuis votre ordinateur local. Puis, cliquez sur **Terminer**.



Une fois la licence à capacité nulle appliquée avec succès, la section **Licences** groupées apparaît sur la page **Licences** .

> **Remarque**
>
> Pour supprimer l'ancien fichier de licence, il n'est pas nécessaire de redémarrer votre NetScaler SDX afin d'éviter toute interruption de service. Pour obtenir de l'aide supplémentaire, contactez le support de NetScaler .

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.

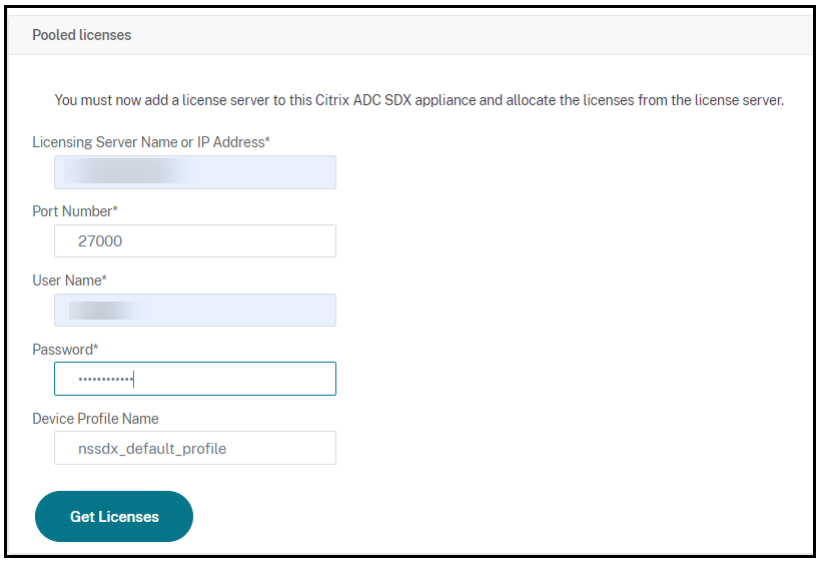
      - Si vous souhaitez configurer le serveur NetScaler ADM en tant que serveur de licences, spécifiez l'adresse IP du serveur NetScaler ADM.
      - Si vous utilisez un agent pour communiquer avec le serveur NetScaler ADM, spécifiez l'adresse IP de l'agent NetScaler ADM.

   b) Dans le champ **Numéro de port**, entrez le port du serveur de licences. Valeur par défaut : 27000.

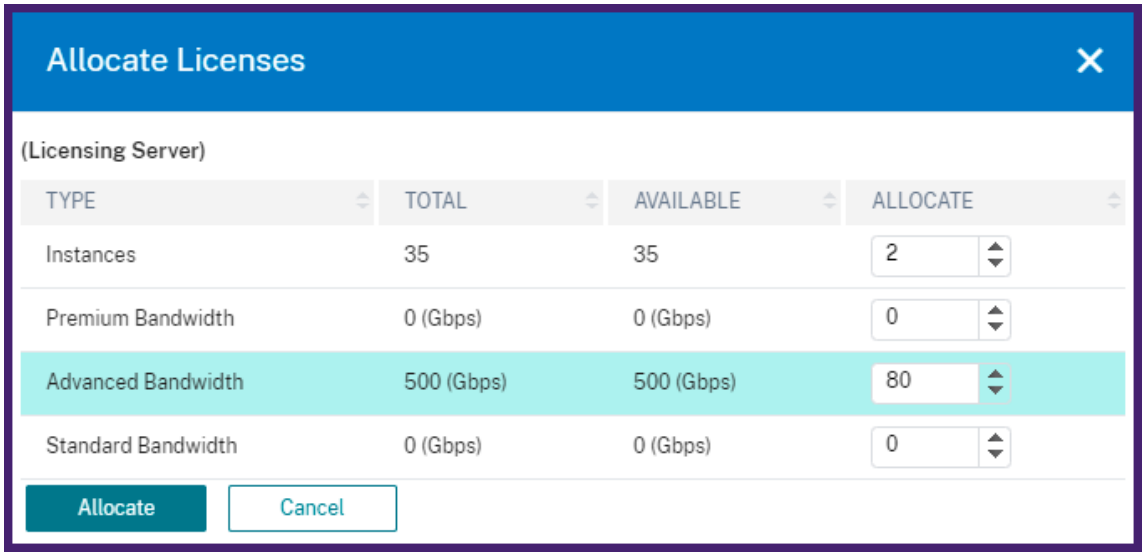
c) Spécifiez **le nom d'utilisateur** et le **mot de passe** du serveur de licences.

- Pour le serveur NetScaler ADM, entrez les informations d'identification de l'administrateur.
- Pour l'agent NetScaler ADM, entrez les informations d'identification de l'agent.

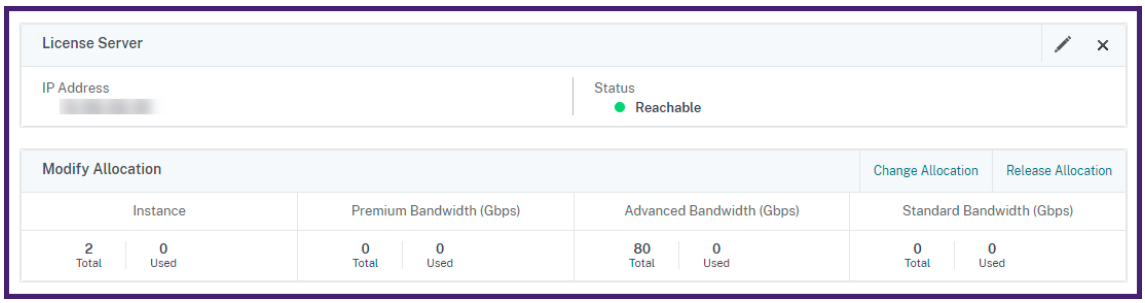
d) Cliquez sur **Obtenir licences**.



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.

NetScaler : capacité groupée sur les instances NetScaler en mode cluster

February 1, 2024

Vous pouvez configurer la capacité NetScaler Pooled sur les instances NetScaler configurées en tant que cluster. Les conditions préalables à la configuration de la capacité groupée sur les instances NetScaler en mode cluster sont les suivantes :

- Les instances s'exécutent individuellement dans un mode de licence de capacité groupée pour former le cluster.
- Toutes les instances doivent fonctionner avec la même bande passante.
- Toutes les instances ont vérifié la capacité mise en commun à partir de la même solution NetScaler Application Delivery and Management.
- De nouvelles instances ne peuvent pas être ajoutées à un cluster NetScaler existant à moins que leur capacité et leurs configurations NetScaler ADM ne soient identiques à celles des instances existantes du cluster.

Toute extraction de capacité depuis le cluster NetScaler attribue la même capacité à tous les nœuds du cluster et lors de la sortie, bande passante = bande passante fournie * nombre de nœuds.

Par exemple, si vous extrayez 50 Mbit/s de bande passante du cluster NetScaler 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

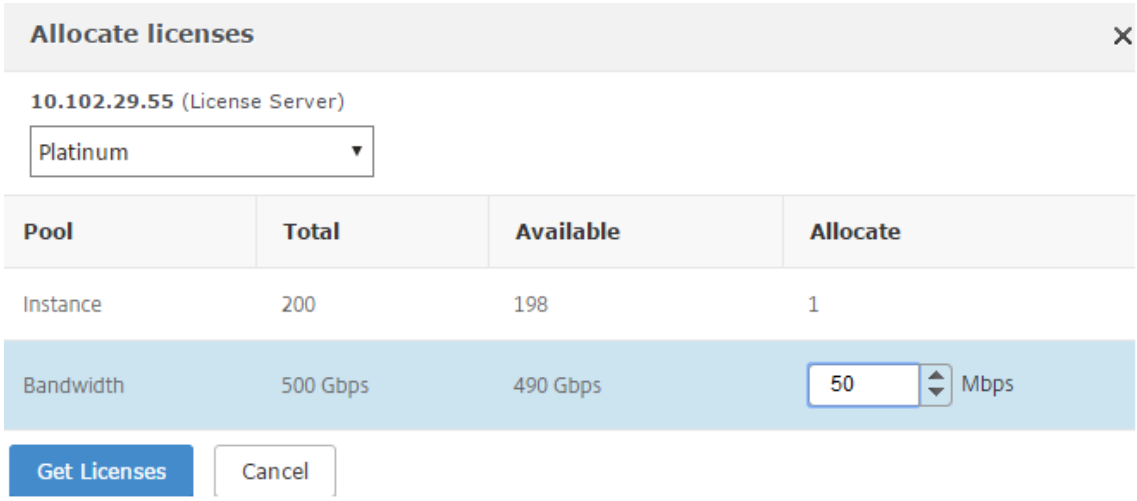
> avec la capacité des instances restantes.

Allouer une capacité groupée ADC à un cluster ADC

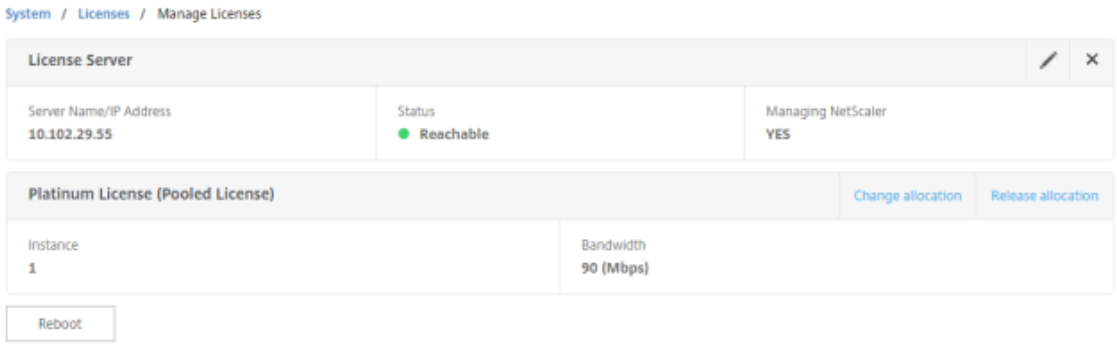
Attribuez des licences à chaque nœud de cluster séparément. Parce que les commandes de propagation et de synchronisation des licences entre les nœuds du cluster sont désactivées.

Répétez la procédure suivante sur chaque nœud de cluster :

1. Dans un navigateur Web, saisissez l'adresse IP NetScaler (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,** puis 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 NetScaler ADM, cochez la case **S'inscrire auprès de NetScaler ADM pour la gérabilité** et entrez les informations d'identification NetScaler ADM .
6. Sélectionnez l'édition de la licence et la bande passante requise, puis cliquez sur **Obtenir des licences**.

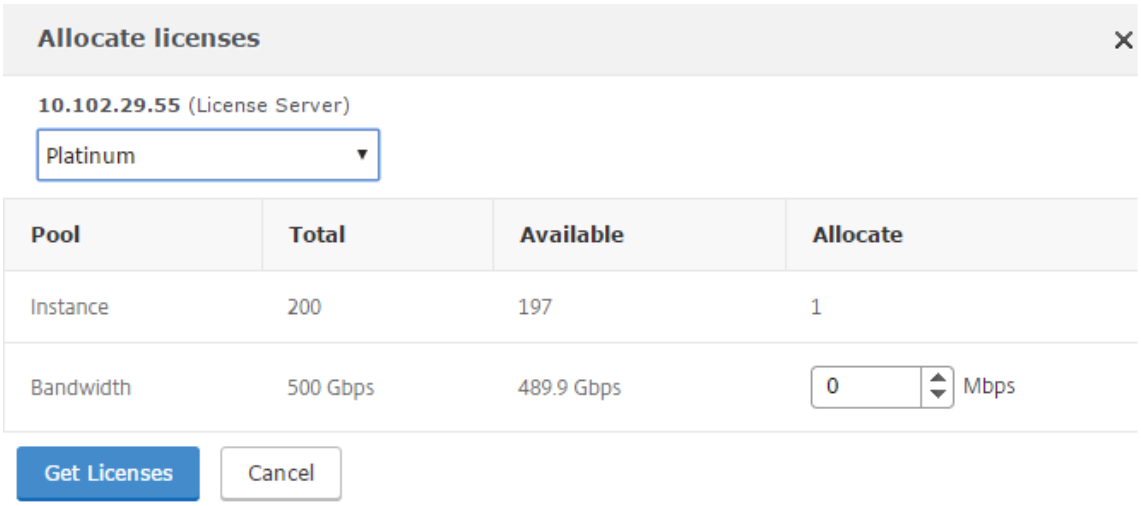


7. Vous pouvez modifier ou libérer l'allocation de licence en sélectionnant **Modifier l'allocation** ou **Libérer l'allocation** .



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 NetScaler à partir de la liste déroulante **Allocation** . 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 NetScaler (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 :

```
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 NetScaler 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
```


Comportements attendus lorsque des problèmes surviennent

February 1, 2024

Voici les comportements attendus des serveurs de licences et des instances NetScaler lorsqu'ils rencontrent les problèmes décrits :

Le serveur de licences cesse de répondre

> **Avertissement**
>
> Le serveur de licences ne répond pas. NetScaler continue de fonctionner avec la capacité actuelle pendant 30 jours. Au bout de 30 jours, si la connectivité au serveur de licences n'est pas rétablie, NetScaler perd sa capacité actuelle et arrête de traiter le trafic.

Si le serveur de licences cesse de répondre, l'instance NetScaler entre dans la période de grâce jusqu'à ce que la connectivité soit rétablie.

L'instance NetScaler Pooled cesse de répondre

Si l'instance NetScaler Pooled cesse de répondre et que le serveur de licences est en bon état, le serveur de licences enregistre toutes les licences de l'instance NetScaler au bout de 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 NetScaler Pooled cessent de répondre

Si le serveur de licences et l'instance NetScaler Pooled redémarrent et rétablissent la connexion, le serveur de licences enregistre toutes ses licences au bout de 10 minutes et les instances NetScaler Pooled retirent automatiquement les licences une fois le redémarrage terminé.

L'instance NetScaler Pooled s'arrête correctement

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 que les licences de l'instance NetScaler Pooled ne sont plus 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 le paiement échoue en raison de l'absence de capacité disponible dans le pool, NetScaler vérifie l'inventaire des licences du pool de distribution et de gestion des applications NetScaler et vérifie toute capacité disponible. Une alarme SNMP est déclenchée pour informer l'utilisateur de cette condition si NetScaler ne fonctionne pas à pleine capacité conformément à la configuration. Si aucune capacité n'est disponible dans le pool de bande passante, l'instance du pool perd sa 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 NetScaler Pooled sont en bon état mais que la connectivité réseau est perdue, les instances continuent de 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 a rétabli la connectivité avec les instances NetScaler, les instances vérifient à nouveau les licences.

Période de grâce

Lorsqu'une instance NetScaler Pooled est en bon état et que le serveur de licences cesse de répondre, l'instance continue de fonctionner avec sa 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.

Scénarios relatifs à l'expiration des licences flexibles ou groupées et au comportement des problèmes de connectivité

February 1, 2024

Ce document présente différents scénarios d'expiration de licence et de comportement de problèmes de connectivité dans NetScaler MPX, NetScaler SDX et NetScaler VPX/NetScaler BLX/NetScaler CPX.

Types de licences flexibles

- Instance logicielle (VPX/BLX/CPX, SDX, MPX, VPX FIPS)

- Capacité de bande passante

MPX FIPS utilise une licence du pool de logiciels MPX. SDX FIPS utilise une licence du pool de logiciels SDX. VPX FIPS utilise une licence du pool de logiciels VPX FIPS.

Scénario : facteur de forme MPX

Vous utilisez des licences Flexed/Pooled et les licences vont bientôt expirer. Les scénarios suivants expliquent le comportement lorsqu'une nouvelle licence est chargée sur NetScaler Application Delivery and Management avant et après l'expiration de la durée, ou lorsqu'aucun fichier de licence n'est présent.

Avant l'expiration du mandat

Si la nouvelle licence est chargée avant l'expiration de la période et que l'ancienne licence est toujours valide, deux pools de capacité différents (ancienne et nouvelle) sont disponibles.

- Si NetScaler est opérationnel, il passe facilement à la nouvelle licence Flexed/Pooled après l'expiration de l'ancienne licence.
- Le redémarrage n'est pas nécessaire.
- NetScaler ne nécessite pas de reconfiguration manuelle de la capacité.

Après l'expiration du mandat

Dans ce cas, le pool de capacité existant a expiré.

- NetScaler continue de fonctionner sous licence jusqu'à ce qu'il soit redémarré.
- Si NetScaler redémarre et qu'aucun fichier de licence valide n'est présent, il perd sa licence.
- Si NetScaler continue de récupérer la nouvelle licence, celle-ci doit être reconfigurée manuellement (réaffectation de capacité).

Scénario : facteur de forme SDX

Vous utilisez des licences Flexed/Pooled et les licences vont bientôt expirer. Les scénarios suivants expliquent le comportement lorsqu'une nouvelle licence est chargée sur NetScaler Application Delivery and Management avant et après l'expiration de la durée, ou lorsqu'aucun fichier de licence n'est présent.

Avant l'expiration du mandat

Si la nouvelle licence est chargée avant l'expiration de la période et que l'ancienne licence est toujours valide, deux pools de capacité différents (ancienne et nouvelle) sont disponibles.

- Si NetScaler est opérationnel, il passe facilement à la nouvelle licence Flexed/Pooled après l'expiration de l'ancienne licence.
- Le redémarrage n'est pas nécessaire.
- NetScaler ne nécessite pas de reconfiguration manuelle de la capacité.

Après l'expiration du mandat

Dans ce cas, le pool de capacité existant a expiré.

- NetScaler continue de fonctionner sous licence jusqu'à ce qu'il soit redémarré.
- Si le service de gestion redémarre et qu'aucun fichier de licence valide n'est présent, le débit de tous les VPX est réduit à 1 Mbit/s.
- Si le service de gestion reste actif pour récupérer la nouvelle licence, celle-ci doit être reconfigurée manuellement (réaffectation de capacité).

Scénario : facteur de forme VPX/BLX/CPX

Vous utilisez des licences Flexed/Pooled et les licences vont bientôt expirer. Les scénarios suivants expliquent le comportement lorsqu'une nouvelle licence est chargée sur NetScaler Application Delivery and Management avant et après l'expiration de la durée, ou lorsqu'aucun fichier de licence n'est présent.

Avant l'expiration du mandat

Si la nouvelle licence est chargée avant l'expiration de la période et que l'ancienne licence est toujours valide, deux pools de capacité différents (ancienne et nouvelle) sont disponibles.

- Si NetScaler est opérationnel, il passe facilement à la nouvelle licence Flexed/Pooled après l'expiration de l'ancienne licence.
- Le redémarrage n'est pas nécessaire.
- NetScaler ne nécessite pas de reconfiguration manuelle de la capacité.

Après l'expiration du mandat

Dans ce cas, le pool de capacité existant a expiré.

- NetScaler continue de fonctionner sous licence jusqu'à ce qu'il soit redémarré.
- Si NetScaler redémarre et qu'aucun fichier de licence valide n'est présent, VPX et BLX perdent leur licence et CPX devient CPX Express.
- Si NetScaler continue de récupérer la nouvelle licence, celle-ci doit être reconfigurée manuellement (réaffectation de capacité).

Résumé

Le tableau suivant récapitule le comportement de tous les formats NetScaler si aucune nouvelle licence n'est appliquée à NetScaler Application Delivery and Management :

Facteur de forme	Après l'expiration de la licence	Après le redémarrage de NetScaler
VPX/BLX	Continue de fonctionner jusqu'au redémarrage	VPX/BLX perd sa licence
CPX	Continue de fonctionner jusqu'au redémarrage	CPX devient CPX Express
MPX	Continue de fonctionner jusqu'au redémarrage	MPX devient sans licence
SDX	Continue de fonctionner jusqu'au redémarrage	Le débit de tous les VPX est réduit à 1 Mbps (les rendant inutilisables)

Scénarios relatifs au comportement des problèmes de connectivité

En cas de rupture de connectivité entre NetScaler et le serveur NetScaler Application Delivery and Management sur site, le comportement est le suivant :

- NetScaler est en cours de mise en service pendant 30 jours.
- Pendant cette période de grâce, la fonctionnalité de licence continue de fonctionner jusqu'au trentième jour.
- Le trente et unième jour,
  - NetScaler VPX/NetScaler CPX/NetScaler BLX et NetScaler MPX subissent un redémarrage forcé et perdent leur licence.
  - Le débit de tous les VPX de NetScaler SDX est réduit à 1 Mbit/s.

Configurer le serveur de mise à disposition et de gestion des applications NetScaler en tant que serveur de licences flexible ou groupé

February 1, 2024

En tant qu'administrateur, vous pouvez configurer le serveur NetScaler Application Delivery and Management uniquement en tant que serveur de licences Flexed ou Pooled. Avec cette configuration, le serveur NetScaler ADM reçoit uniquement les données de licence des instances NetScaler.

Parfois, vous pouvez être soumis à une obligation réglementaire qui impose d'empêcher les données des instances NetScaler de quitter la zone de réglementation. Dans de telles situations, vous pouvez déployer une instance locale du serveur ADM sur site dans votre zone de réglementation afin d'utiliser les fonctionnalités de gestion, de surveillance et d'analyse. Lorsque vous suivez la même approche pour utiliser la fonctionnalité de licences flexibles ou groupées, vous devez répartir les licences flexibles ou groupées sur différents serveurs de licences NetScaler ADM. Cette approche ne vous offre pas la flexibilité nécessaire pour attribuer des licences flexibles ou groupées à vos instances NetScaler déployées dans le monde entier.

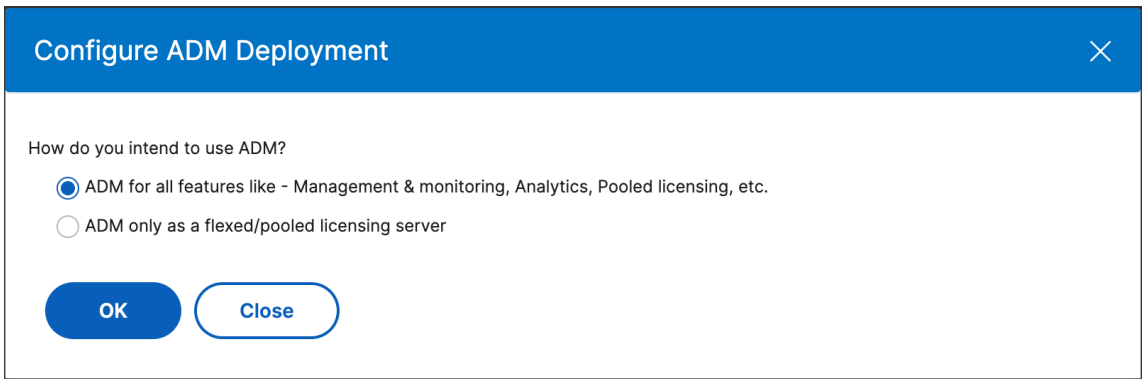
Par conséquent, configurez le serveur NetScaler ADM uniquement en tant que serveur de licences Flexed ou Pooled. Le serveur NetScaler ADM reçoit uniquement les données de licence de toutes les instances NetScaler. Vous pouvez donc respecter le mandat réglementaire et attribuer de manière dynamique des licences de capacité flexible ou groupée entre les instances NetScaler déployées dans le monde entier.

Comment configurer le serveur NetScaler ADM uniquement en tant que serveur de licences flexible ou groupé

Avant de commencer, assurez-vous qu'aucune instance NetScaler n'est ajoutée au serveur NetScaler ADM. Ajoutez des instances NetScaler uniquement après avoir terminé l'étape 4.

Pour configurer le serveur NetScaler ADM uniquement pour le serveur de licences Flexed ou Pooled, procédez comme suit :

1. Accédez à **Paramètres > Administration**.
2. Dans la section **Configurations système**, sélectionnez **Déploiement du système**.
3. Dans **ADM Deployment** , sélectionnez **ADM uniquement en tant que serveur de licences flexible/**groupé .



4. Cliquez sur **OK**.

   Cette action conserve uniquement la fonctionnalité de licence flexible ou groupée et désactive les fonctionnalités suivantes de NetScaler ADM :

   - Sauvegarde NetScaler ADM
   - Gestion d'événements
   - Gestion des certificats SSL
   - Rapports sur le réseau
   - Fonctions réseau
   - Audit de configuration

   > **Remarque**
   >
   > Par défaut, la fonctionnalité d'analyse de NetScaler 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 NetScaler ADM affiche désormais uniquement la fonctionnalité de licence flexible ou groupée. Et, les entités restantes n'apparaissent pas.

5. Après avoir configuré NetScaler ADM uniquement pour la fonctionnalité de licence, ajoutez des instances NetScaler sur la page **Infrastructure > Instances**.

> **Remarque**
>
> - Vous pouvez ajouter une instance NetScaler dans un ou plusieurs serveurs NetScaler ADM. Lorsque vous modifiez le mot de passe de telles instances NetScaler, veillez à le mettre à jour sur tous les serveurs NetScaler ADM sur lesquels l'instance est découverte.
> - Un utilisateur peut toujours effectuer certaines opérations sur les fonctionnalités désactivées dans l'interface graphique NetScaler ADM. Par exemple, le sondage d'événements et la sauvegarde NetScaler. En tant que super administrateur, si vous souhaitez restreindre ces opérations, désactivez l'accès des utilisateurs pour les autres administrateurs à l'

> aide d'une stratégie d'accès appropriée. Pour plus d'informations, consultez la section Configurer les stratégies d'accès sur NetScaler ADM.

Enregistrez-vous et découvrez les licences NetScaler VPX et NetScaler BLX

February 1, 2024

Vous pouvez attribuer des licences NetScaler VPX et NetScaler BLX à des instances NetScaler à la demande auprès de NetScaler Application Delivery and Management. Le logiciel NetScaler ADM stocke et gère les licences, qui disposent d'un cadre de licences qui permet un provisionnement de licences évolutif et automatisé. Une instance peut récupérer la licence auprès de NetScaler ADM lors de son provisionnement. Lorsqu'une instance est supprimée ou détruite, elle vérifie sa licence auprès du logiciel NetScaler ADM.

Conditions préalables

Assurez-vous que les conditions préalables suivantes sont remplies :

- Vous utilisez une image NetScaler VPX exécutant la version logicielle 12.0.
  Par exemple : NSVPX-ESX-12.0-xx.xx_NC.zip
- Vous avez installé NetScaler ADM avec la version 12.0.
  Par exemple : MAS-ESX-12.0-xx.xx.zip

> **Remarque**
>
> Pour gérer les licences NetScaler VPX existantes par NetScaler ADM, vous devez réhéberger les licences sur NetScaler ADM.

Installation de licences dans NetScaler ADM

> **Remarque**
>
> Avant d'installer les licences, redémarrez l'appliance virtuelle NetScaler ADM si vous avez modifié l'édition logicielle ou la bande passante.

Pour installer les fichiers de licence sur NetScaler ADM :

1. Dans un navigateur Web, saisissez l'adresse IP de NetScaler 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**Infrastructure > Licences groupées**.
4. Dans la section **Fichiers de licence**, sélectionnez l'une des options suivantes :

    - **Charger des fichiers de licence depuis un ordinateur local** : si un fichier de licence est déjà présent sur votre ordinateur local, vous pouvez le télécharger sur NetScaler 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.

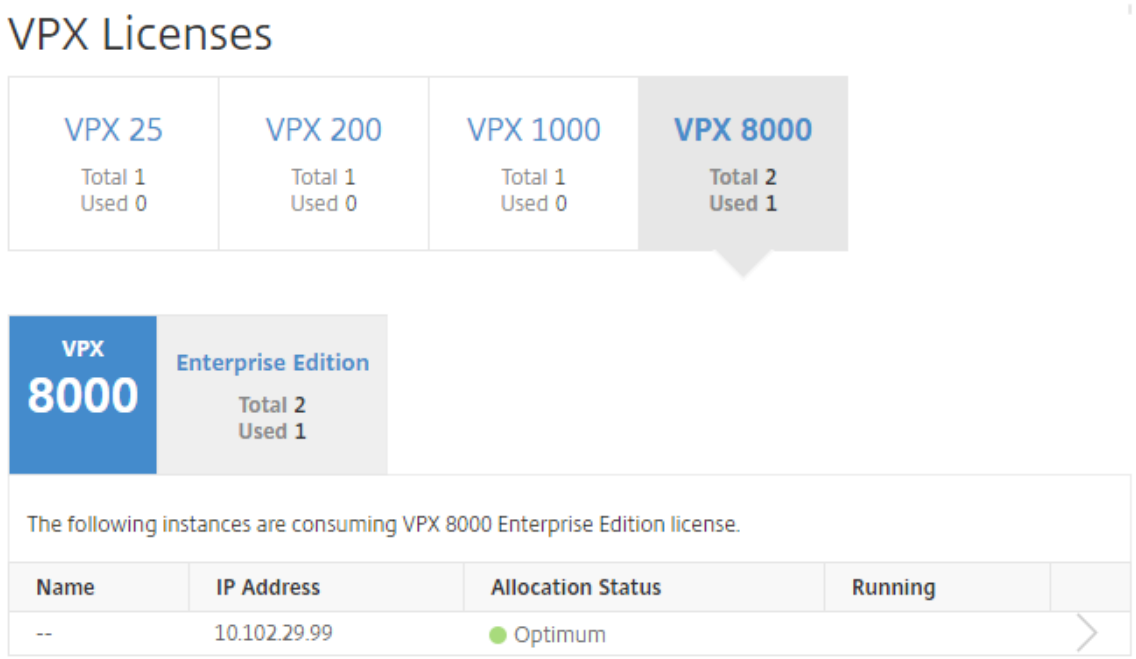
    À tout moment, vous pouvez ajouter d'autres licences à NetScaler ADM à partir de la page Paramètres de **licence** .

Vérification

Vous pouvez consulter les licences disponibles et allouées dans l'interface graphique NetScaler ADM.

Pour afficher les licences :

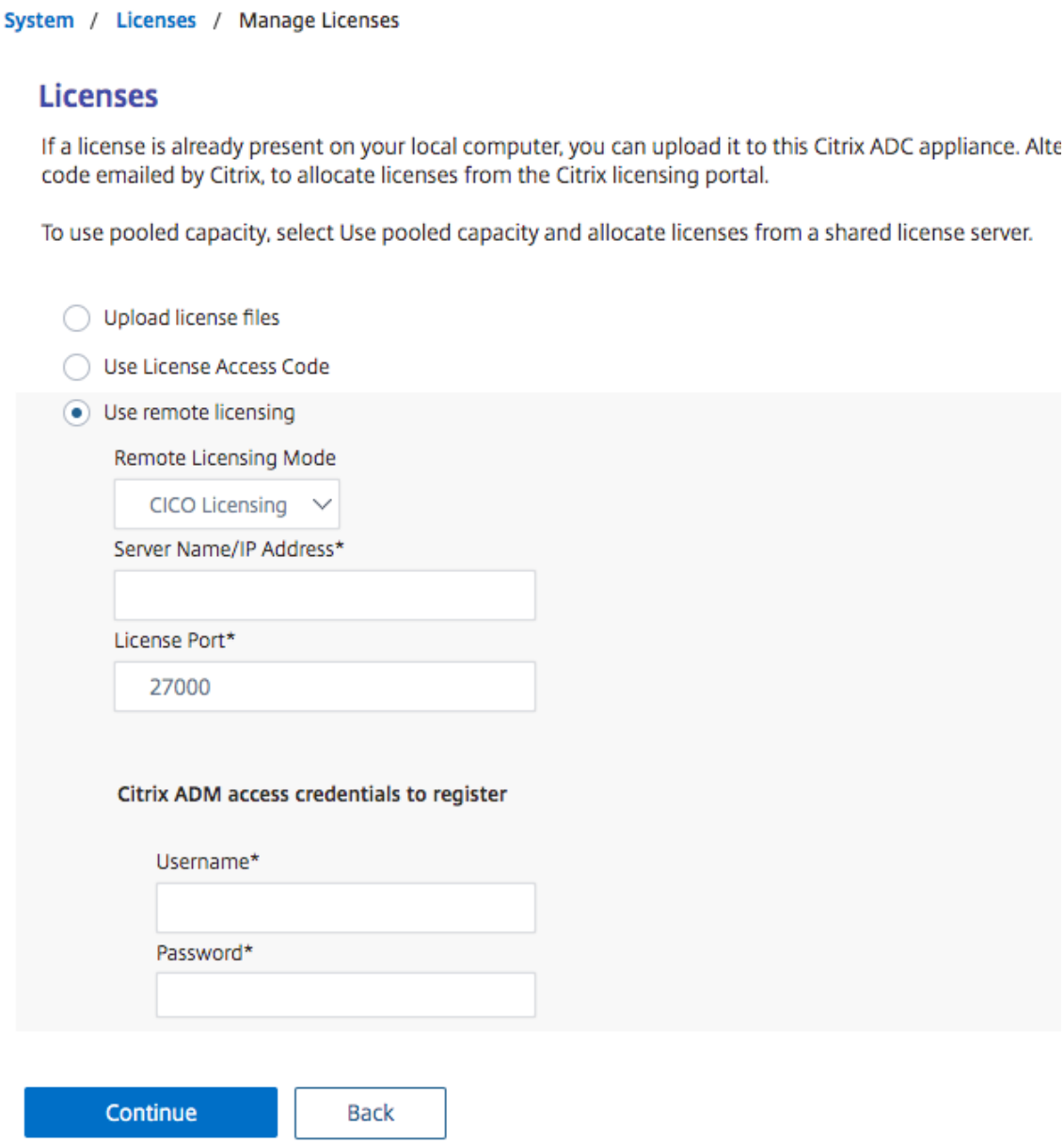
1. Dans un navigateur Web, saisissez l'adresse IP de NetScaler ADM (par exemple, http://192.168.100.1).
2. Dans **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Dans l'onglet Configuration, accédez à **Infrastructure > Licences groupées > Licences VPX**.



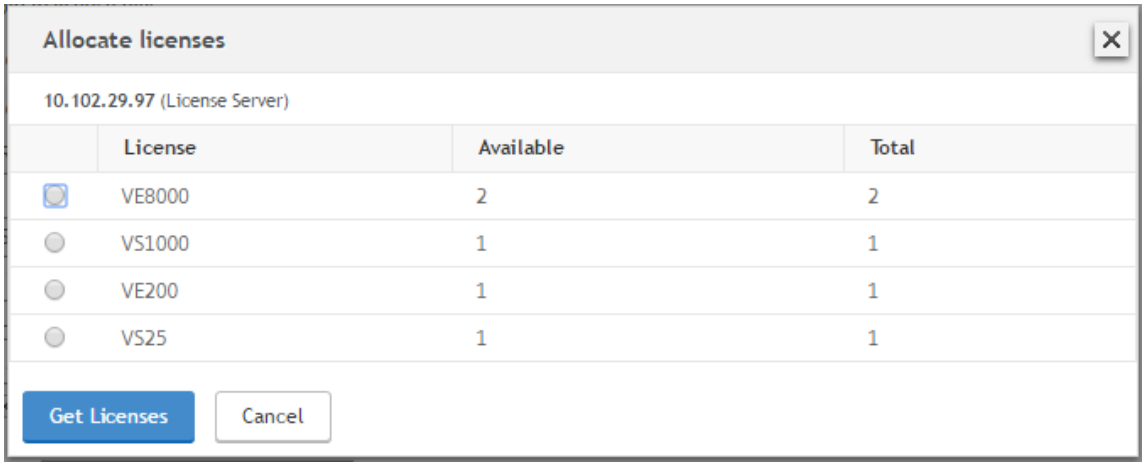
4. Vous pouvez afficher les licences allouées dans le tableau sous la section Licences disponibles.

Allouez des licences NetScaler VPX et NetScaler BLX à une instance NetScaler à l'aide de l'interface graphique NetScaler

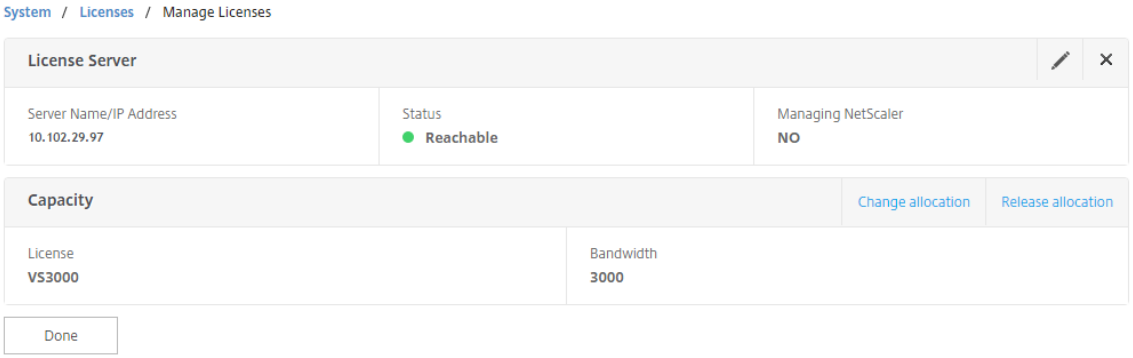
1. Dans un navigateur Web, saisissez l'adresse IP de l'instance NetScaler (par exemple, http://192.168.100.1).
2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Dans l'onglet Configuration, accédez à **Paramètres > Licences > 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 Nom **d'utilisateur** et **mot** de passe , entrez les informations d'identification NetScaler 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 NetScaler redémarre.
8. Vous pouvez modifier ou libérer l'allocation de licences en accédant à **Système > Licences > Gérer les licences** , puis en sélectionnant **Modifier l'allocation** ou Libérer l'**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**.

Allouez des licences NetScaler VPX et NetScaler BLX à une instance NetScaler à l'aide de la CLI NetScaler

1. Dans un client SSH, entrez l'adresse IP de l'instance NetScaler 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 NetScaler, 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
```

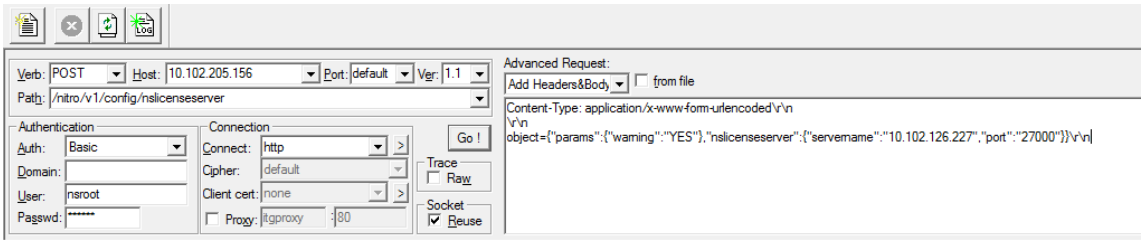
Allouez des licences NetScaler VPX et NetScaler BLX à une instance NetScaler à l'aide de l'API

Dans un navigateur Web ou un client API, connectez-vous à l'instance NetScaler 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 " : " <NetScaler ADM IP> " , " port " : " 27000 "  }
  }
 \r\n
<!--NeedCopy-->
```

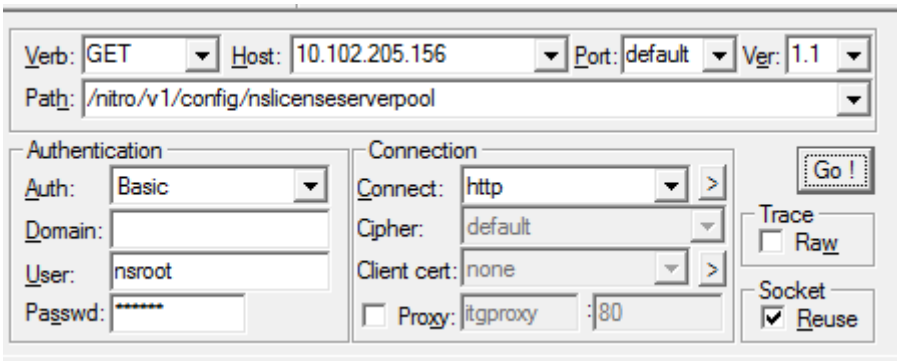


NetScaler ADM répond à la demande. L'exemple de réponse suivant montre un succès.

```
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



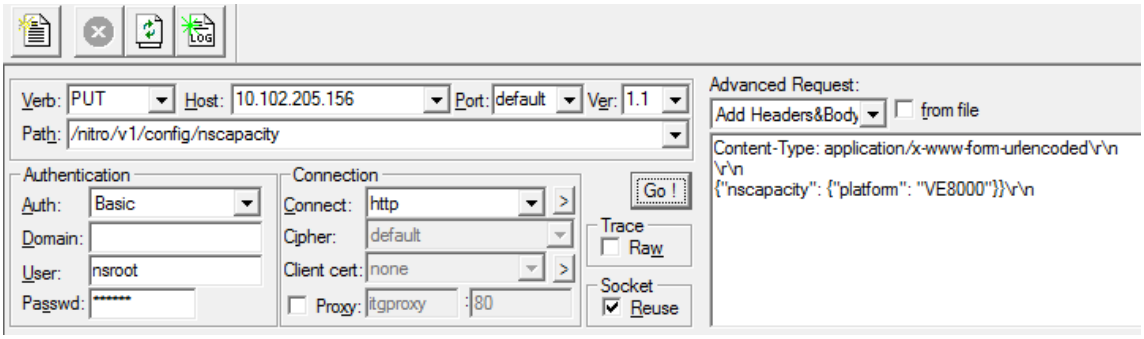
NetScaler ADM répond à la demande. L'exemple de réponse suivant montre le succès et la liste des licences disponibles sur le serveur de licences.

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 NetScaler :

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-->
```

NetScaler 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 NetScaler VPX et NetScaler BLX, sans aucun impact sur la bande passante de licence allouée à l'instance et sans 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 permet de se connecter au nouveau serveur et de libérer les ressources associées à l'ancien serveur de licences.

Mise à jour à l'aide de l'interfacegraphique : 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, voir Allouer des licences NetScaler VPX et NetScaler BLX à une instance NetScaler à l'aide de l'interface graphique NetScaler .

Configurer les contrôles d'expiration pour les licences d'enregistrement et de sortie NetScaler VPX et NetScaler BLX

Vous pouvez désormais configurer le seuil d'expiration des licences NetScaler VPX et NetScaler BLX. En définissant des seuils, NetScaler ADM envoie des notifications par e-mail ou SMS lorsqu'une licence arrive à expiration. Un piège SNMP et une notification sont également envoyés lorsque la licence a expiré sur NetScaler ADM.

Un événement est généré lorsqu'une notification d'expiration de licence est envoyée et cet événement peut être consulté sur NetScaler ADM.

Pour configurer les contrôles d'expiration de licence :

1. Accédez à**Infrastructure > Licences groupées**.
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 licence groupée à utiliser pour informer 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. Spécifiez ensuite la date à laquelle vous souhaitez envoyer la notification en termes de nombre de jours avant l'expiration de la licence.
6. Cliquez sur **Enregistrer**.

Licence de processeur virtuel NetScaler

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.

Licence de processeur virtuel pour NetScaler VPX

Auparavant, les licences NetScaler VPX étaient attribuées en fonction de la consommation de bande passante des instances. Un NetScaler VPX est limité à l'utilisation d'une bande passante spécifique et à d'autres mesures de performances 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 TPS et le débit de compression. La mise à niveau de la licence NetScaler 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. NetScaler ADM prend désormais en charge l'attribution de licences à l'instance NetScaler en fonction des exigences du processeur virtuel.

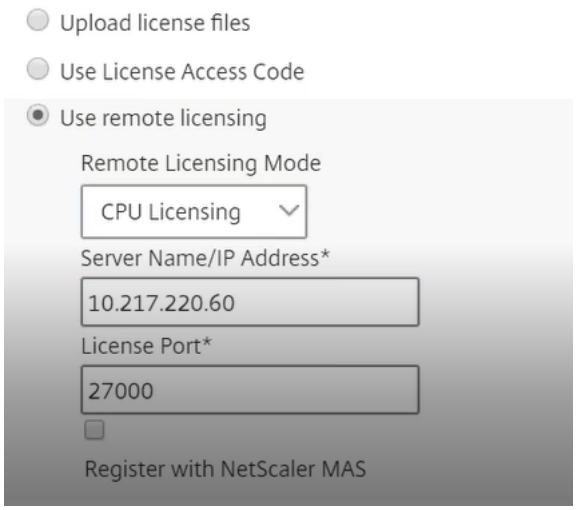
Dans la fonctionnalité de licence basée sur l'utilisation du processeur virtuel, la licence spécifie le nombre de processeurs auxquels un NetScaler VPX particulier a droit. Ainsi, le NetScaler VPX peut récupérer des licences uniquement pour le nombre de processeurs virtuels exécutés sur celui-ci à partir du serveur de licences. NetScaler VPX vérifie les licences en fonction du nombre de processeurs en cours d'exécution sur le système. NetScaler VPX ne prend pas en compte les processeurs inactifs lors de la vérification des licences.

Semblable à la capacité de licence groupée et aux fonctionnalités de licence CICO, le serveur de licences NetScaler ADM gère un ensemble distinct de licences de processeurs virtuels. 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 NetScaler VPX après avoir vérifié les licences.

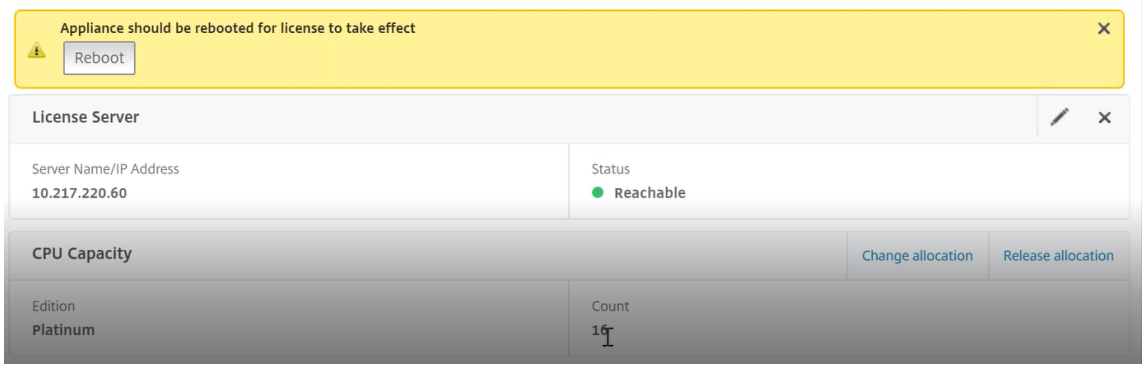
Pour configurer le serveur de licences dans NetScaler VPX à l'aide de l'interface graphique :

1. Dans NetScaler 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 NetScaler VPX auprès de NetScaler ADM. Si ce n'est pas déjà fait, activez **Enregistrer auprès de NetScaler ADM** et saisissez les informations de connexion NetScaler 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 la licence.



> **Remarque**
>
> Vous pouvez également libérer la licence actuelle et vérifier à partir d'une autre édition. Par exemple, vous utilisez déjà une licence Standard Edition sur votre instance. Vous pouvez libérer cette licence, puis vérifier à partir de Advanced Edition.

Configuration d'un serveur de licences dans une licence NetScaler VPX à l'aide de l'interface de ligne de commande

Dans la console NetScaler VPX, tapez les commandes suivantes pour les deux tâches suivantes :

1. Pour ajouter le serveur de licences à NetScaler 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 NetScaler 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 NetScaler VPX :

```
add licenseserver <licensing server IP address> -forceUpdateIP
```

Cette commande permet de se connecter au nouveau serveur et de libérer les ressources associées à l'ancien serveur de licences.

Gestion des licences de processeur virtuel sur NetScaler ADM

1. Dans NetScaler ADM, accédez à **Infrastructure > Licences groupées > Processeur virtuel groupé.**
2. La page affiche les licences allouées pour chaque type d'édition de licence.

3. Cliquez sur le chiffre figurant dans chaque beignet pour afficher les instances NetScaler qui utilisent cette licence.

Licence de processeur virtuel pour NetScaler CPX

Lors du provisionnement de l'instance NetScaler CPX, vous pouvez configurer l'instance NetScaler CPX pour récupérer les licences auprès du serveur de licences en fonction de l'utilisation du processeur sur l'instance.

NetScaler CPX s'appuie sur le serveur de licences, qui s'exécute sur NetScaler ADM, pour gérer les licences. NetScaler CPX extrait les licences du serveur de licences lors de son démarrage. Les licences sont réenregistrées sur le serveur de licences lorsque NetScaler CPX s'arrête.

Vous pouvez télécharger l'image NetScaler CPX depuis le registre de conteneurs Quay à l' aide de la commande « docker pull » et la déployer sur votre environnement.

Trois types de licences sont disponibles pour les licences NetScaler CPX :

1. Licences d'abonnement au processeur virtuel prises en charge pour NetScaler CPX et VPX
2. Licences de capacité groupée
3. Licences CP1000 prenant en charge un ou plusieurs vCPU pour NetScaler CPX uniquement

Pour configurer les licences d'abonnement vCPU lors du provisionnement de l'instance NetScaler CPX, procédez comme suit :

Spécifiez le nombre de licences vCPU utilisées par l'instance NetScaler CPX.

- Cette valeur est entrée en tant que variable d'environnement via Docker, Kubernetes ou Mesos/-Marathon.
- La variable cible est « CPX_CORES ». Le NetScaler CPX peut prendre en charge de 1 à 16 cœurs.

Pour spécifier 2 cœurs, vous pouvez exécuter la commande docker run comme suit :


```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
    -e EULA=yes -e CPX_CORES=2
<!--NeedCopy-->
```

Lors du provisionnement d'une instance NetScaler CPX, définissez le serveur de licences NetScaler 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 NetScaler.
- *<LS_PORT>* est le port du serveur de licences NetScaler. Par défaut, le port est 27000.

> **Remarque**
>
> Par défaut, l'instance NetScaler CPX extrait la licence du pool d'abonnements vCPU. L'instance NetScaler CPX extrait un nombre « n » de licences si elle est exécutée avec « n » processeurs.

Pour configurer la capacité NetScaler Pooled ou les licences CP1000 lors du provisionnement de l'instance NetScaler CPX :

Si vous souhaitez récupérer la licence de l'instance NetScaler CPX à l'aide de la licence groupée (basée sur la bande passante) ou du pool privé NetScaler CPX (CP1000 ou basé sur un pool privé), vous devez fournir les variables d'environnement en conséquence.

Par exemple,

```
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 le retrait depuis le pool CP1000 (pool privé NetScaler CPX). L'instance NetScaler CPX extrait ensuite « n » le nombre d'instances pour « n » le nombre de cœurs spécifié 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 de NetScaler CPX multicœur incluent « n » vCPU (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 du pool de bande passante Premium tout en permettant à NetScaler CPX de fonctionner jusqu'à 2 000 Mbit/s. Dans le cas des licences groupées, les 1 000 premiers Mbit/s 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 paramètres système

February 1, 2024

Le tableau suivant décrit la liste des options disponibles sous **Paramètres** > **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 de NetScaler ADM qui sont utilisés pour déployer NetScaler ADM

Configurations réseau	Options	Description
	Deuxième carte réseau	Vous permet de configurer une deuxième carte réseau pour isoler l'accès à la gestion de NetScaler ADM. Pour plus d'informations, voir Configurer une double carte réseau pour accéder à NetScaler ADM
	Nom d'hôte	Vous permet d'attribuer un nom d'hôte à NetScaler ADM. Pour plus d'informations, voir Attribuer un nom d'hôte à un serveur NetScaler ADM
	Serveur proxy	Permet de configurer ADM en tant que serveur proxy. Pour plus d'informations, consultez NetScaler ADM en tant que serveur proxy d'API
Itinéraires statiques		Vous permet de configurer des routes statiques pour établir une connexion entre les instances NetScaler ADM et NetScaler VPX
Serveurs NTP		Garantit que l'horloge NetScaler 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		Vous permet de comprendre quel port doit être ouvert pour la communication entre les instances ADM et ADC. 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 NetScaler 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 NetScaler ADM. Vous pouvez utiliser cette fonctionnalité pour définir des messages de rappel pour vous-même ou pour l'utilisateur qui se connecte à NetScaler 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 unique de NetScaler 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 NetScaler ADM	Vous permet de mettre à niveau NetScaler ADM via l'interface graphique. Pour plus d'informations, consultez Mettre à niveau
Redémarrez NetScaler ADM	Vous permet de redémarrer NetScaler ADM
Arrêter NetScaler ADM	Vous permet d'arrêter NetScaler 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	Vous permet de limiter la quantité de données de reporting stockées dans la base de données du serveur NetScaler ADM. Pour plus d'informations, voir Configurer les paramètres d'nettoyer du système
	Événements d'instance	Vous permet de limiter les messages d'événements signalant les données stockées dans NetScaler 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 NetScaler 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	Vous permet de configurer les paramètres de NetScaler ADM pour sauvegarder une ou plusieurs instances NetScaler 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 NetScaler Application Delivery Management (ADM) pour qu'il vous envoie 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

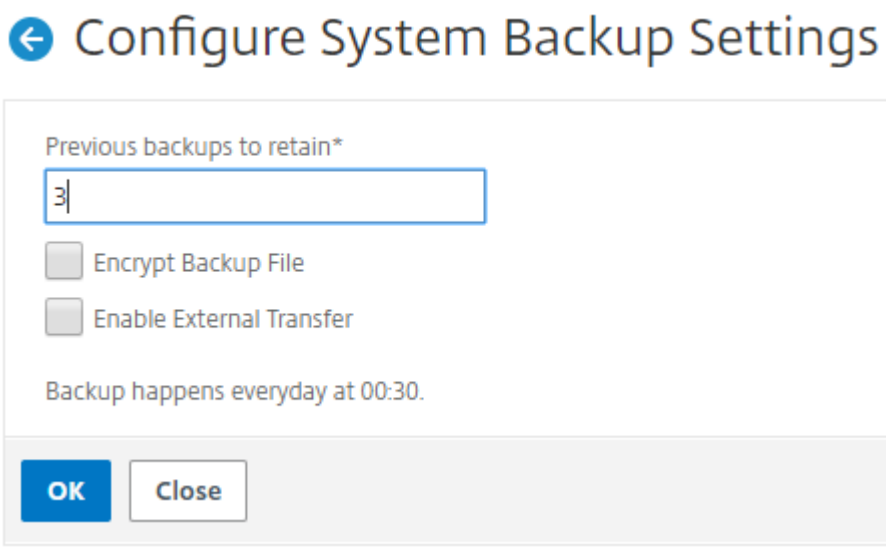
Configurer les fonctionnalités	Description
Désactiver ou activer des fonctionnalités	Vous pouvez activer ou désactiver des fonctionnalités dans NetScaler ADM. Pour plus d'informations, voir Activer ou désactiver les fonctionnalités ADM

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 NetScaler Application Delivery Management (ADM).

1. Accédez à **Paramètres > Administration** . Sous **Sauvegarde** , cliquez sur **Configurer la sauvegarde du système et de l'instance** .
2. Sur la page **Sauvegarde > Système**, spécifiez les informations suivantes :
   - Sauvegardes précédentes à conserver. Vous ne pouvez conserver qu'un maximum de 10 sauvegardes.
   - Sélectionnez **Chiffrer le fichier de sauvegarde** pour crypter les fichiers de sauvegarde.
   - Sélectionnez **Activer le transfert externe** pour transférer une copie de votre fichier de sauvegarde vers un autre système. Lorsque vous souhaitez restaurer la configuration, vous devez d'abord télécharger le fichier sur le serveur NetScaler 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, voir Transférer un fichier de sauvegarde NetScaler ADM vers un système externe.
3. Cliquez sur **OK**.



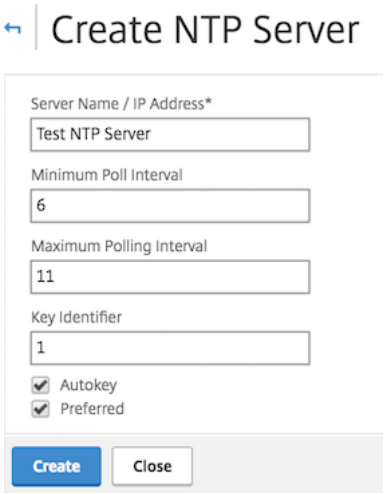
Configurer un serveur NTP

February 1, 2024

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

Pour configurer un serveur NTP sur NetScaler ADM :

1. Accédez à **Paramètres > 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 NetScaler ADM :

1. Accédez à **Paramètres > 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.

Mise à niveau de NetScaler Application Delivery Management (ADM)

February 1, 2024

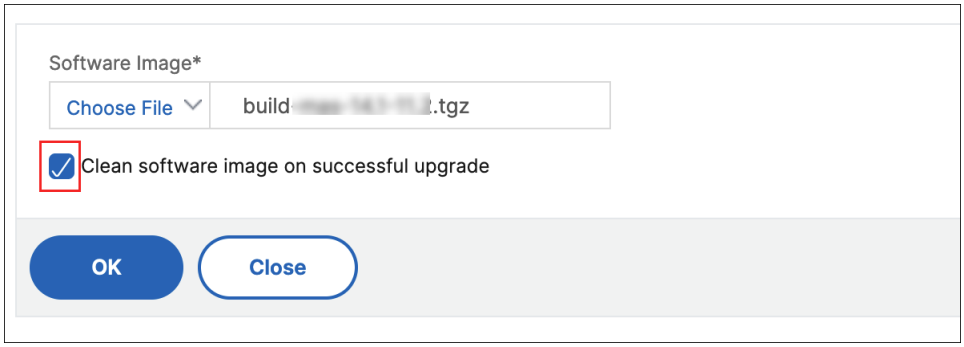
Chaque version de NetScaler ADM propose des fonctionnalités nouvelles et mises à jour avec des fonctionnalités améliorées. Une liste complète des améliorations est répertoriée dans les notes de mise à jour accompagnant l'annonce de publication. Prenez le temps de lire les notes de mise à jour avant de 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 NetScaler ADM :

1. Accédez à **Paramètres > Administration**. Sous **Maintenance du système**, cliquez sur **Mettre à niveau NetScaler ADM**.
2. **Sur la page Mettre à niveau NetScaler ADM, téléchargez 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**.



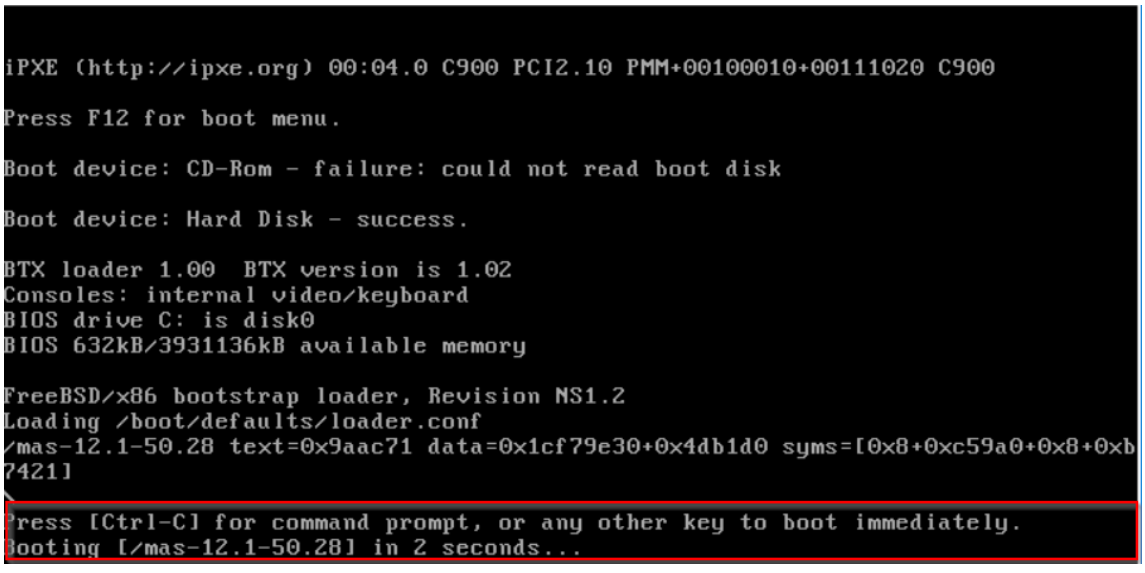
Comment réinitialiser le mot de passe pour NetScaler ADM

February 1, 2024

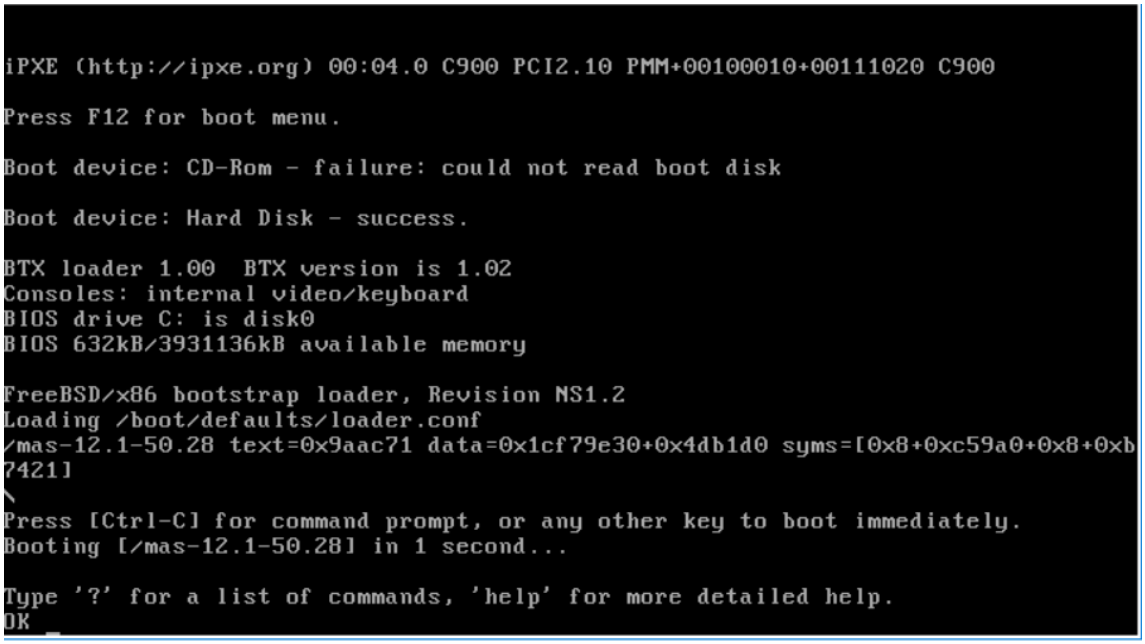
La procédure de réinitialisation du mot de passe de NetScaler ADM peut différer selon les hyperviseurs sur lesquels il est hébergé. Si vous avez modifié votre mot de passe par défaut et souhaitez le rétablir, vous pouvez le réinitialiser en redémarrant le nœud NetScaler ADM.

Citrix Hypervisor utilisant XenCenter :

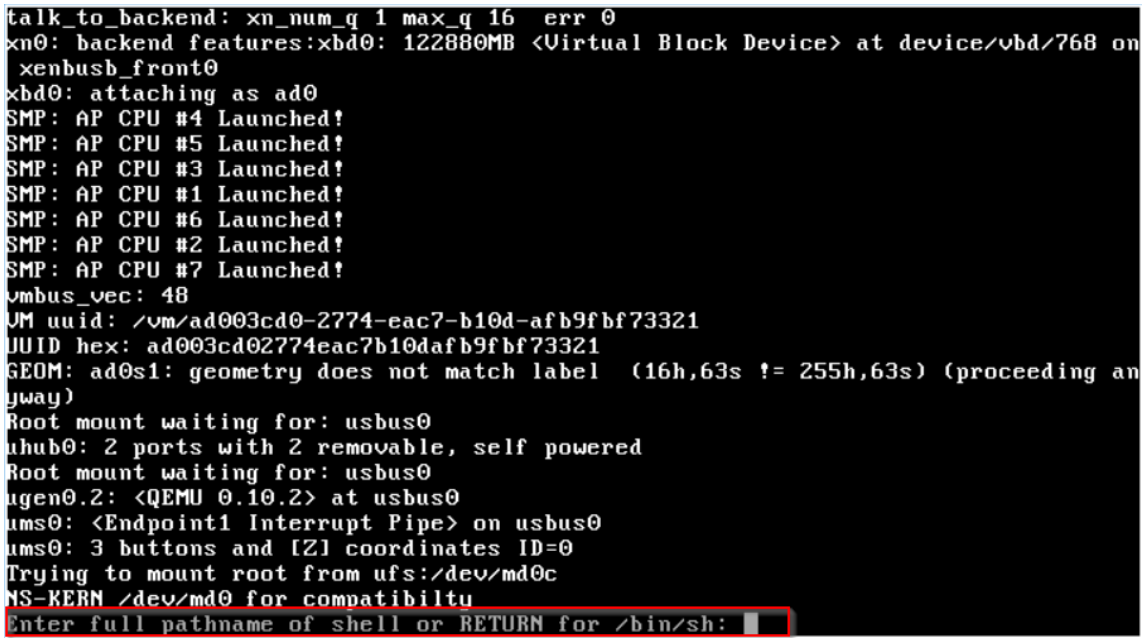
1. Connectez-vous à Citrix Hypervisor à l'aide de XenCenter.
2. **Sélectionnez le nœud NetScaler ADM, cliquez avec le bouton droit de la souris et sélectionnez Redémarrer.**
3. Sous l'onglet **Console**, appuyez sur **CTL +C** pour interrompre la séquence de démarrage.



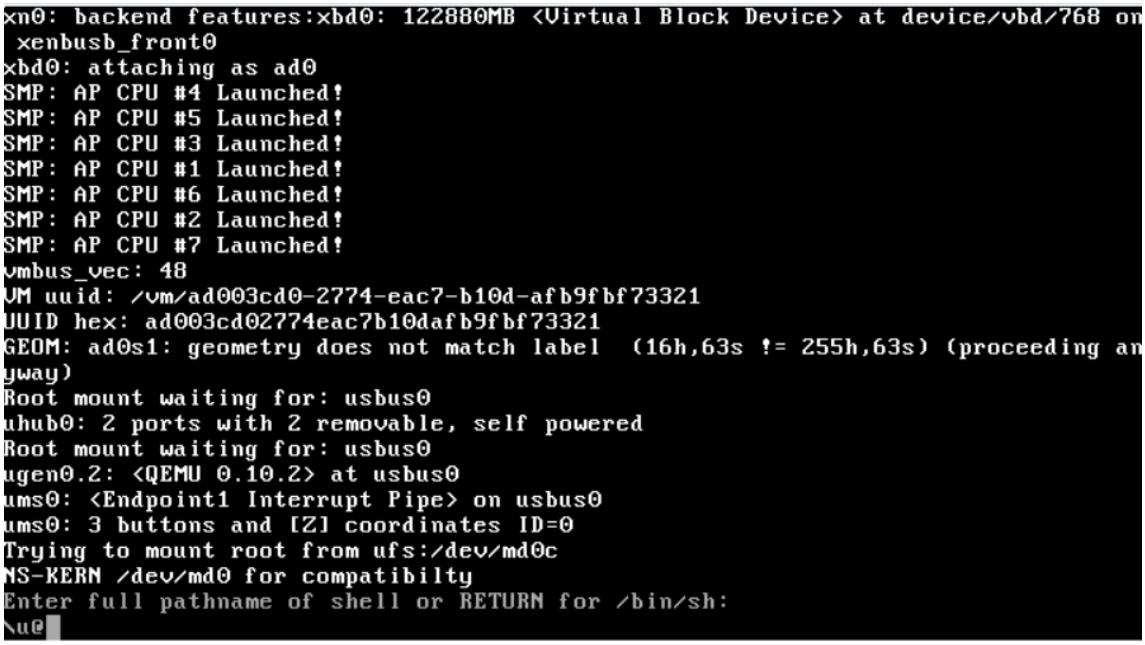
4. Exécutez la commande **boot -s** à l'invite OK.



NetScaler ADM redémarre et affiche le message suivant :

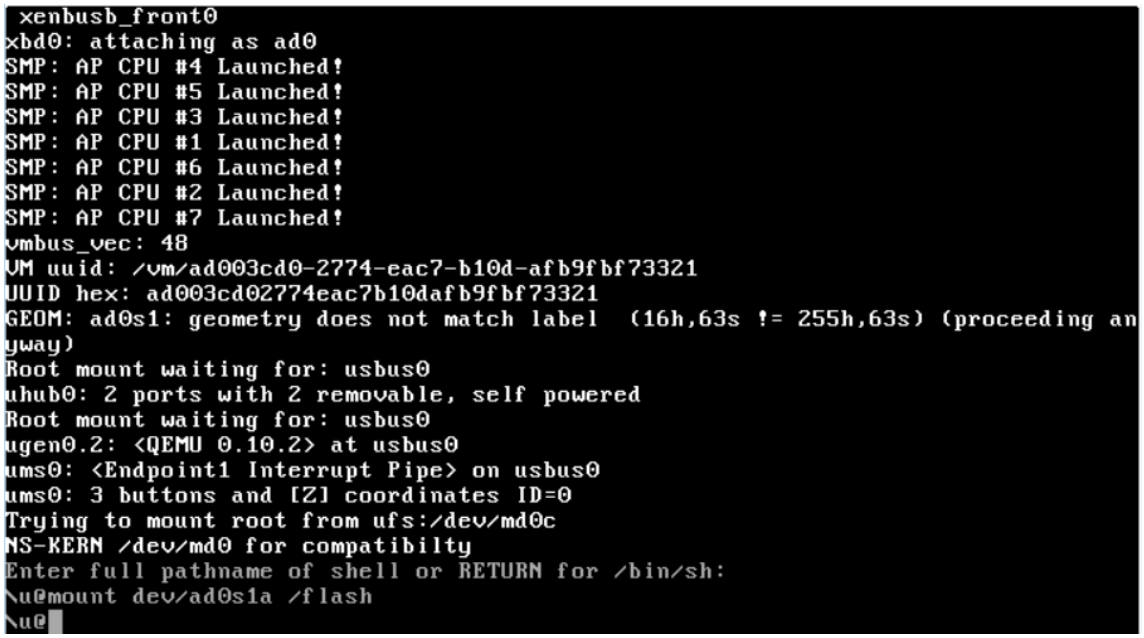


5. Appuyez sur **Entrée** pour obtenir l'invite /u@.



6. Montez la partition flash à l'aide de la commande suivante :

   ```
   mount /dev/da0s1a /flash
   ```



7. Créez un fichier à l'aide de la commande suivante :

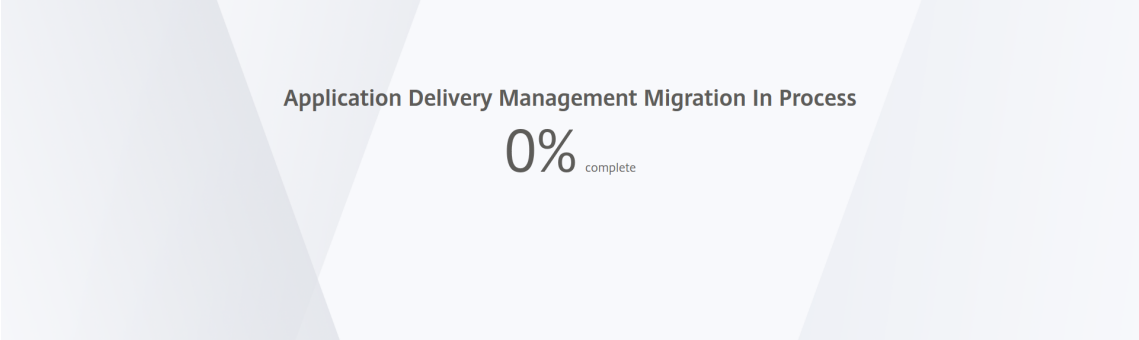
   ```
   touch /flash/mpsconfig/.recover
   ```

   Le mot de passe est maintenant réinitialisé au mot de passe par défaut.

8. Exécutez la commande **Reboot** pour redémarrer NetScaler 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 NetScaler ADM et attendez que le redémarrage soit terminé.



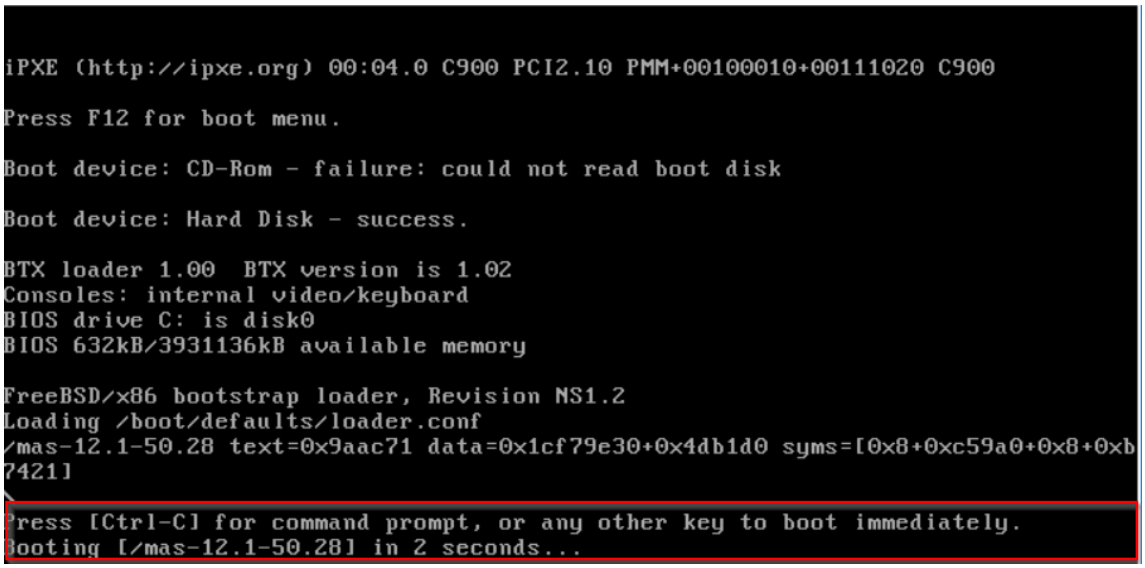
Vous pouvez maintenant utiliser les informations d'identification *nsroot/nsroot* pour ouvrir une session à partir de l'interface graphique et *nsrecover/nsroot* pour ouvrir une session à partir de l'Hypervisor.

> 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 NetScaler 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 NetScaler ADM, cliquez avec le bouton droit de la souris, puis sélectionnez Redémarrer.**
3. Sous l'onglet **Console**, appuyez sur **CTL +C** pour interrompre la séquence de démarrage.



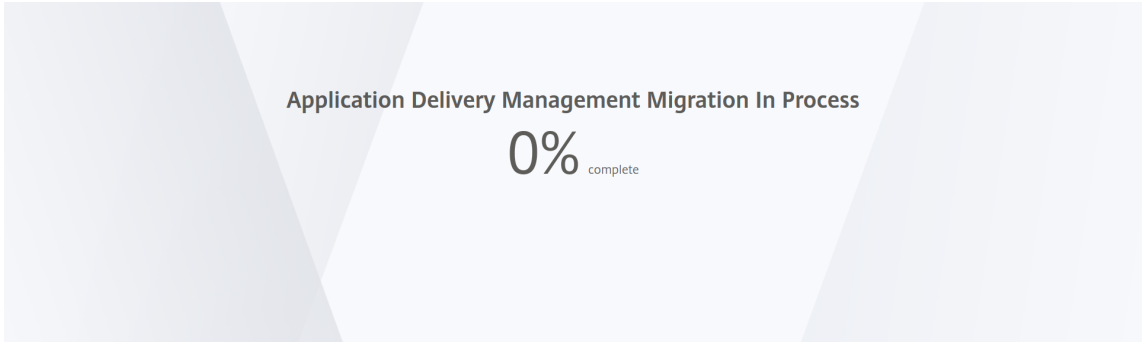
4. Exécutez la commande **boot -s** dans l'invite OK.

   NetScaler 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 NetScaler ADM.
9. Accédez à l'interface graphique NetScaler ADM et attendez que le redémarrage soit terminé.

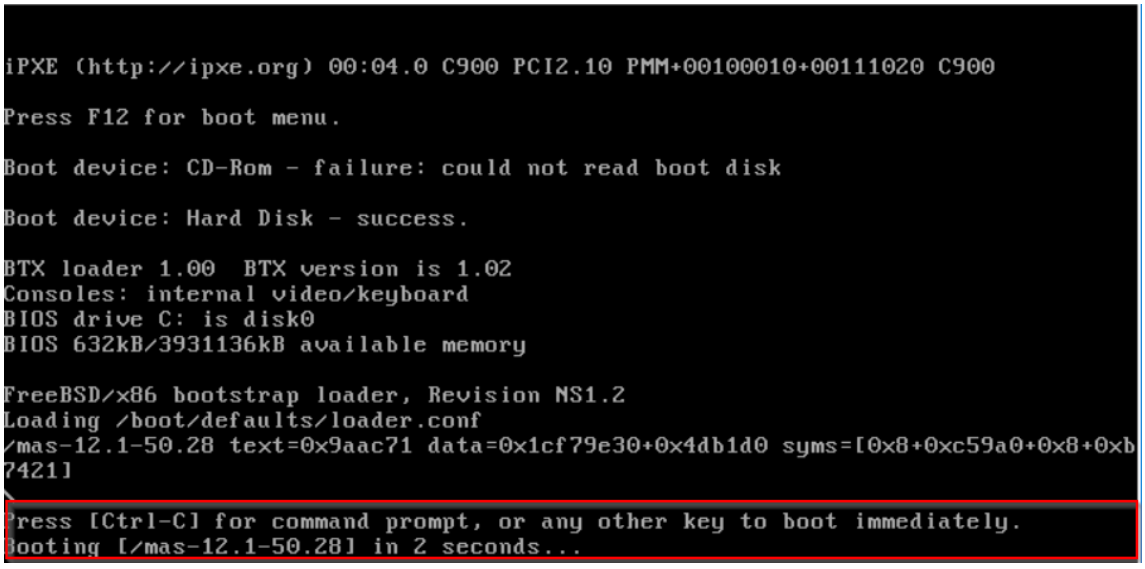


Vous pouvez désormais utiliser les informations d'identification *nsroot/nsroot* pour ouvrir une session à partir de l'interface graphique et *nsrecover/nsroot* pour ouvrir une session à partir du serveur ESX.

> 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 NetScaler 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 NetScaler ADM, cliquez avec le bouton droit de la souris, 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.

   NetScaler ADM redémarre.

5. Appuyez sur **Entrée** pour obtenir l'invite /u@.
6. Montez la partition flash à l'aide de la commande suivante :

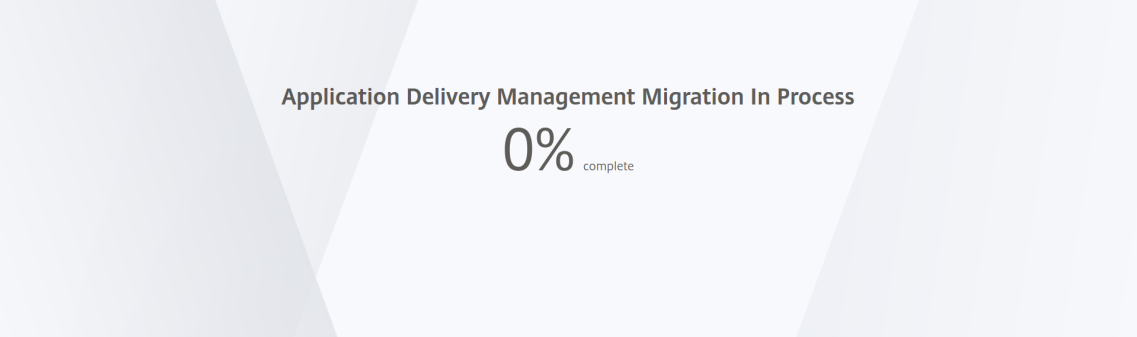
   ```
   mount dev/ad0s1a /flash
   ```

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 NetScaler ADM.
9. Accédez à l'interface graphique NetScaler 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 NetScaler 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 NetScaler ADM à l'aide d'un client SSH sur le serveur KVM.
2. Redémarrez NetScaler 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 NetScaler 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
   ```

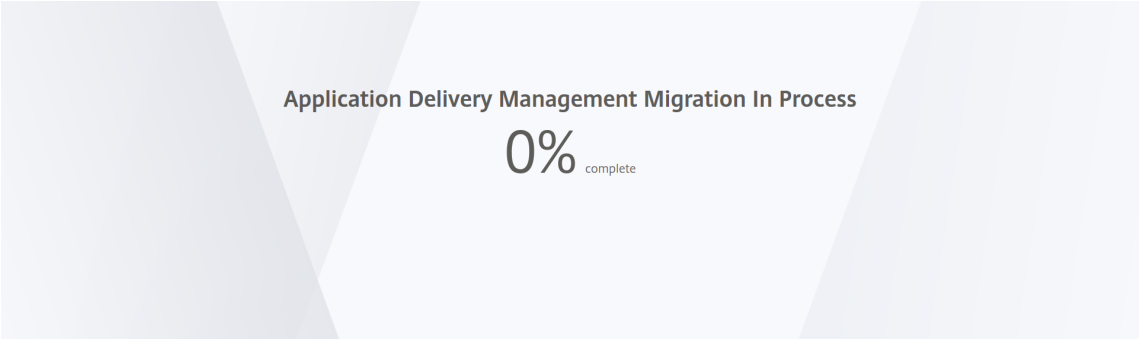

8. Créez un fichier à l'aide de la commande suivante :

   ```
   touch /flash/mpsconfig/.recover
   ```

   Le mot de passe est maintenant réinitialisé au mot de passe par défaut.

9. Exécutez la commande **Reboot** pour redémarrer NetScaler ADM.

10. Accédez à l'interface graphique NetScaler 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 NetScaler ADM :
>
> - `rm /flash/mpsconfig/master.passwd`
> - `rm –rf /etc/passwd`

Configurer une carte réseau secondaire pour accéder à NetScaler ADM

February 1, 2024

Vous pouvez configurer une deuxième carte réseau pour isoler l'accès de gestion à NetScaler 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 NetScaler ADM.

Envisagez un scénario dans lequel vous souhaitez isoler le trafic pour :

- Réunir toutes les communications entre NetScaler ADM et ses instances NetScaler gérées sur un seul réseau.

- Disposer d'un accès de gestion à NetScaler ADM sur un autre réseau.

Dans ce scénario, en tant qu'administrateur, vous pouvez :

- Configurez une adresse IP pour le trafic entre NetScaler ADM et ses instances NetScaler gérées.
- Configurez une autre adresse IP pour gérer le logiciel NetScaler ADM afin d'effectuer toutes les tâches administratives du logiciel.

> **Remarque**
>
> Si NetScaler ADM est configuré en tant que paire HA, l'adresse IP de gestion configurée sur la seconde carte réseau est associée au nœud principal.

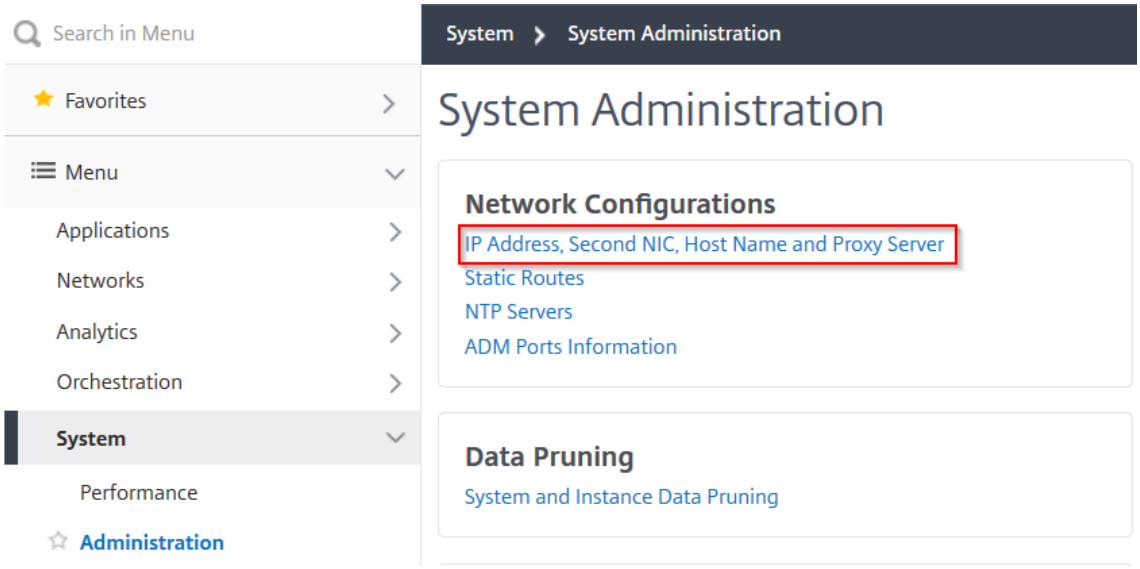
Conditions préalables

- Assurez-vous d'avoir déployé et configuré **NetScaler 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).

Pour attribuer une adresse IP à une carte réseau sur un Citrix Hypervisor et créer une interface secondaire, voir Attribuer une adresse IP à une carte réseau.

Configurer une deuxième carte réseau dans NetScaler ADM

1. Connectez-vous à l'interface graphique d'ADM.
2. Accédez à **Paramètres > 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.

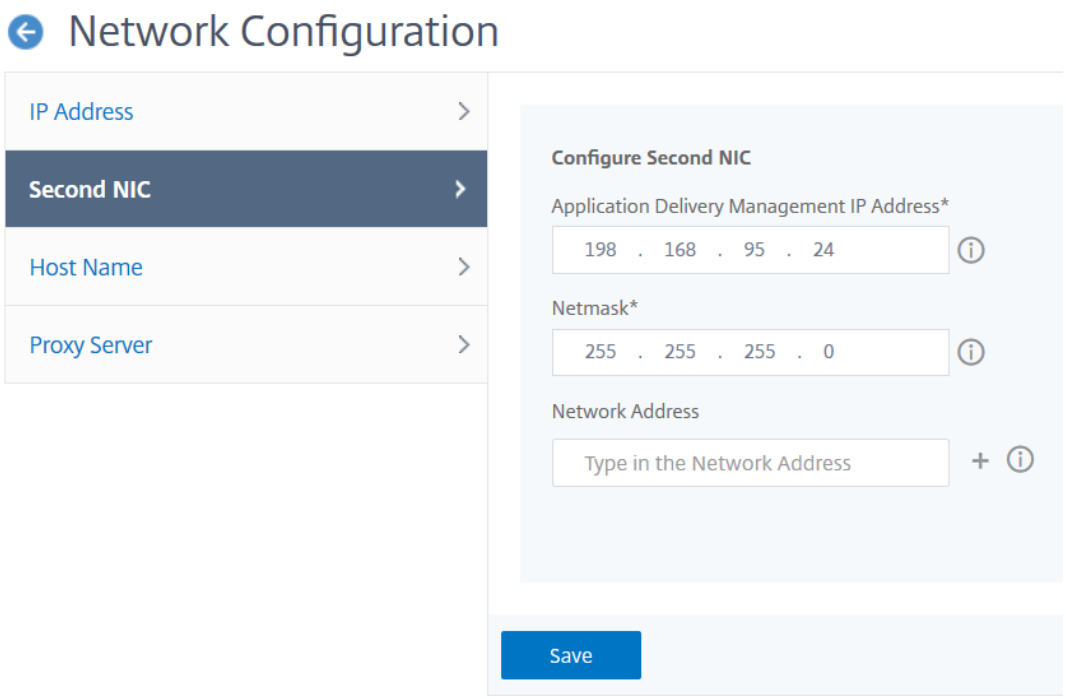
4. Cliquez sur l'onglet Deuxième carte réseau et configurez les paramètres suivants :

   a) **Adresse IP de gestion de la mise à disposition des applications** : entrez une adresse IP valide pour accéder à NetScaler ADM. Vous pouvez utiliser cette adresse IP pour accéder à NetScaler 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 NetScaler ADM. Cliquez sur **+** pour ajouter d'autres adresses IP. Ce champ est facultatif.

   d) Cliquez sur **Enregistrer**.



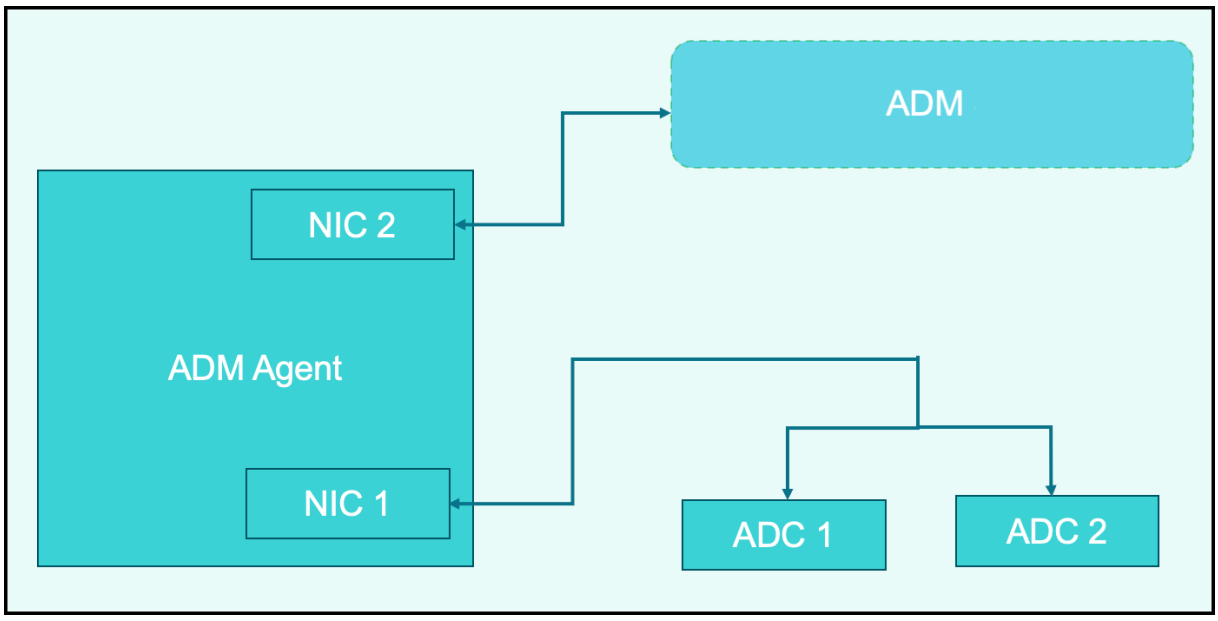
Configuration d'une carte réseau secondaire pour accéder à l'agent ADM

February 1, 2024

Vous pouvez configurer deux cartes réseau sur un agent ADM. À l'aide de l'architecture à double carte réseau, l'agent ADM sera capable de :

- Établissez la communication entre l'agent ADM et les instances ADC : vous pouvez utiliser la première carte réseau pour isoler le trafic reçu et envoyé via NetScaler ADM et également pour communiquer entre NetScaler ADM et ses instances NetScaler gérées sur un autre réseau.
- Établir la communication entre l'agent ADM et NetScaler ADM : vous pouvez utiliser la deuxième carte réseau pour gérer le NetScaler ADM qui se trouve sur un réseau et effectuer des tâches administratives

> **Remarque**
>
> Vous ne pouvez pas échanger les fonctionnalités et la configuration des deux cartes réseau.



Dans ce scénario, en tant qu'administrateur, vous pouvez :

- Configurez l'adresse IP pour le trafic entre NetScaler ADM et ses instances NetScaler gérées.
- Configurez l'adresse IP pour gérer le logiciel NetScaler ADM afin d'effectuer toutes les tâches administratives du logiciel.

> **Remarque**
>
> Il n'est pas obligatoire de configurer deux cartes réseau pour un agent ADM. Il est facultatif et n'est requis que lorsque le trafic entre l'agent ADM, NetScaler ADM et les ADC doit être séparé.

Modifiez les adresses réseau IPV4 NIC à l'aide de l'interface de ligne de commande

1. Ouvrez une connexion SSH à la console de l'agent NetScaler ADM à l'aide d'un client SSH, tel que PuTTY.
2. Connectez-vous à l'aide des informations d'identification **nsrecover/nsroot** et passez à l'invite du shell.
3. Exécutez la commande **ifconfig**. Vous pouvez voir les détails des deux cartes réseau que vous avez configurées -
    - NIC 1 —Pour la communication entre l'agent ADM et la communication ADC
    - NIC 2 : pour la communication entre l'agent ADM et NetScaler ADM


```
bash-3.2# ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 1500
        options=680003<RXCSUM,TXCSUM,LINKSTATE,RXCSUM_IPV6,TXCSUM_IPV6>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        groups: lo
pflog0: flags=0<> metric 0 mtu 33152
        groups: pflog
1/1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether a2:56:cd:d2:f8:8c
        hwaddr a2:56:cd:d2:f8:8c
        inet6 fe80::a056:cdff:fed2:f88c%1/1 prefixlen 64 scopeid 0x3
        inet 10.102.103.247 netmask 0xffffff00 broadcast 10.102.103.255
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet manual
        status: active
1/2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 32:89:fe:8c:8f:45
        hwaddr 32:89:fe:8c:8f:45
        inet6 fe80::3089:feff:fe8c:8f45%1/2 prefixlen 64 scopeid 0x4
        inet 10.102.103.250 netmask 0xffffff00 broadcast 10.102.103.255
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet manual
        status: active
```

4. Exécutez la commande **networkconfig**. Un menu apparaît qui vous permet de définir ou de modifier les adresses réseau IPV4.

```
bash-3.2# /mps/networkconfig

------------------------------------------------------------------------------
Citrix ADM Agent initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
------------------------------------------------------------------------------
     1. Citrix ADM Agent Host Name [ns]:
     2. Citrix ADM Agent IPv4 address [10.102.103.247]:
     3. Netmask [255.255.255.0]:
     4. Gateway IPv4 address [10.102.103.1]:
     5. DNS IPv4 Address [10.102.166.70]:
     6. Second NIC IPv4 address [10.102.103.250]:
     7. Second NIC Netmask [255.255.255.0]:
     8. Second NIC Network address [10.102.103.251,10.102.103.252,10.102.103.252]:
     9. Second NIC Gateway IPv4 address [10.102.103.2]:
    10. Cancel and quit.
    11. Save and quit.
```

> **Remarque**
>
> L'adresse réseau de la deuxième carte réseau peut prendre plusieurs valeurs IP.

5. Sélectionnez un élément de menu à modifier. Enregistrez et quittez les paramètres.

Configurer l'intervalle de purge de syslog

February 1, 2024

Syslog est un protocole standard de journalisation. Il comporte 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 (OS) FreeBSD sous-jacent de l'instance NetScaler, 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.

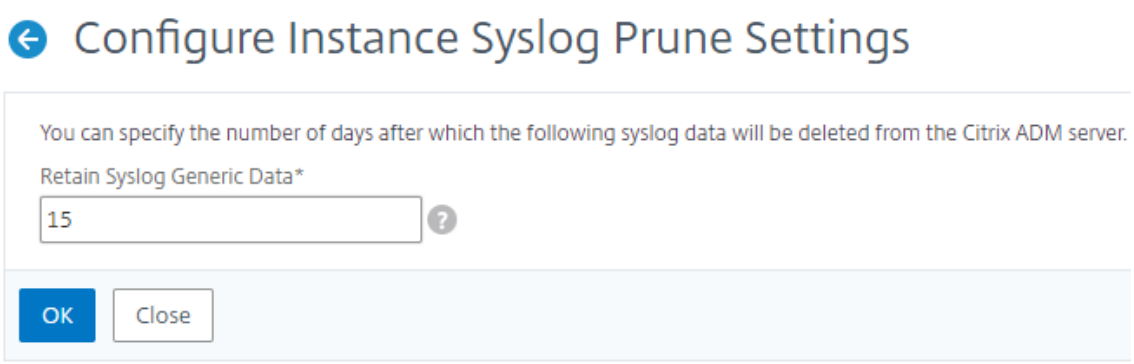
Pour limiter la quantité de données syslog stockées dans la base de données, vous pouvez spécifier l'intervalle auquel vous souhaitez nettoyer les données syslog. Vous pouvez spécifier le nombre de jours après lesquels les données syslog suivantes seront supprimées de NetScaler Application Delivery Management (ADM) :

- Données Syslog génériques
- Données AppFirewall
- Données NetScaler Gateway

Vous pouvez également configurer l'intervalle d'nettoyer de NetScaler Gateway par type de syslog. Cet intervalle d'nettoyer est prioritaire par rapport à l'intervalle runique configuré pour conserver les données NetScaler Gateway.

Pour configurer les paramètres d'intervalle d'nettoyer de Syslog pour NetScaler ADM :

1. Accédez à **Paramètres > 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)**. Entrez le nombre de jours pendant lesquels NetScaler ADM conserve les messages Syslog génériques.



Configurer les paramètres de nettoyer système et d'un nettoyer d'événement

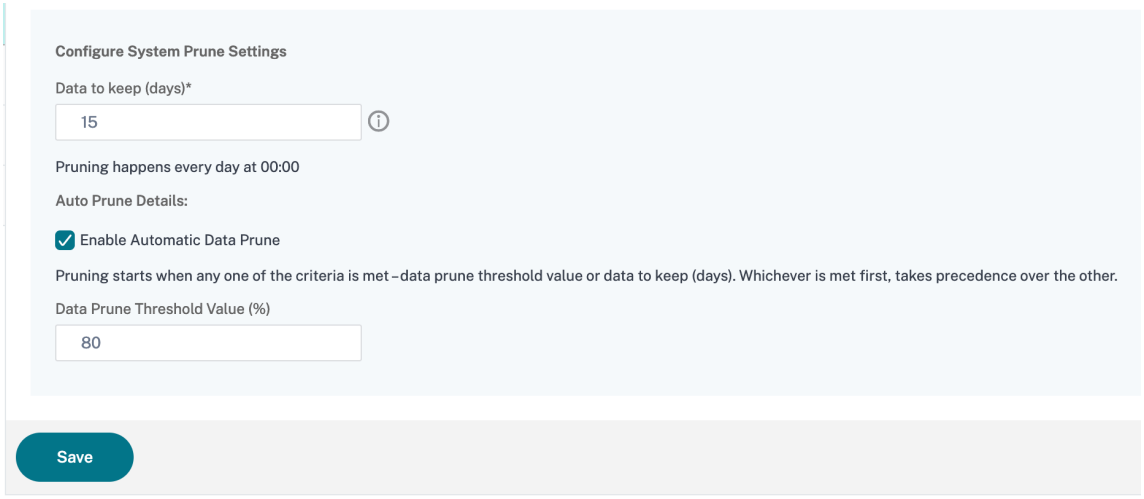
February 1, 2024

Pour limiter la quantité de données de reporting stockées dans la base de données du logiciel NetScaler Application Delivery Management (ADM), vous pouvez nettoyer supprimer. Vous pouvez spécifier l'intervalle pendant lequel vous souhaitez que NetScaler ADM conserve les données de reporting 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).

> **Remarque**
>
> La valeur que vous spécifiez ne peut pas dépasser 30 jours ni être inférieure à 15 jours.

Pour configurer les paramètres d'nettoyer du système pour les rapports de performance :

1. Accédez à **Paramètres** > **Administration** . Sous **Nettoyage des données**, cliquez sur **Nettoyage des données du système et de l'instance**.
2. Sur la page **Configurer les paramètres de nettoyage du système**, spécifiez les éléments suivants :
   - Nombre de jours pendant lesquels les données doivent être conservées
   - Pourcentage d'espace disque (seuil de nettoyage)
3. Cliquez sur **OK**.



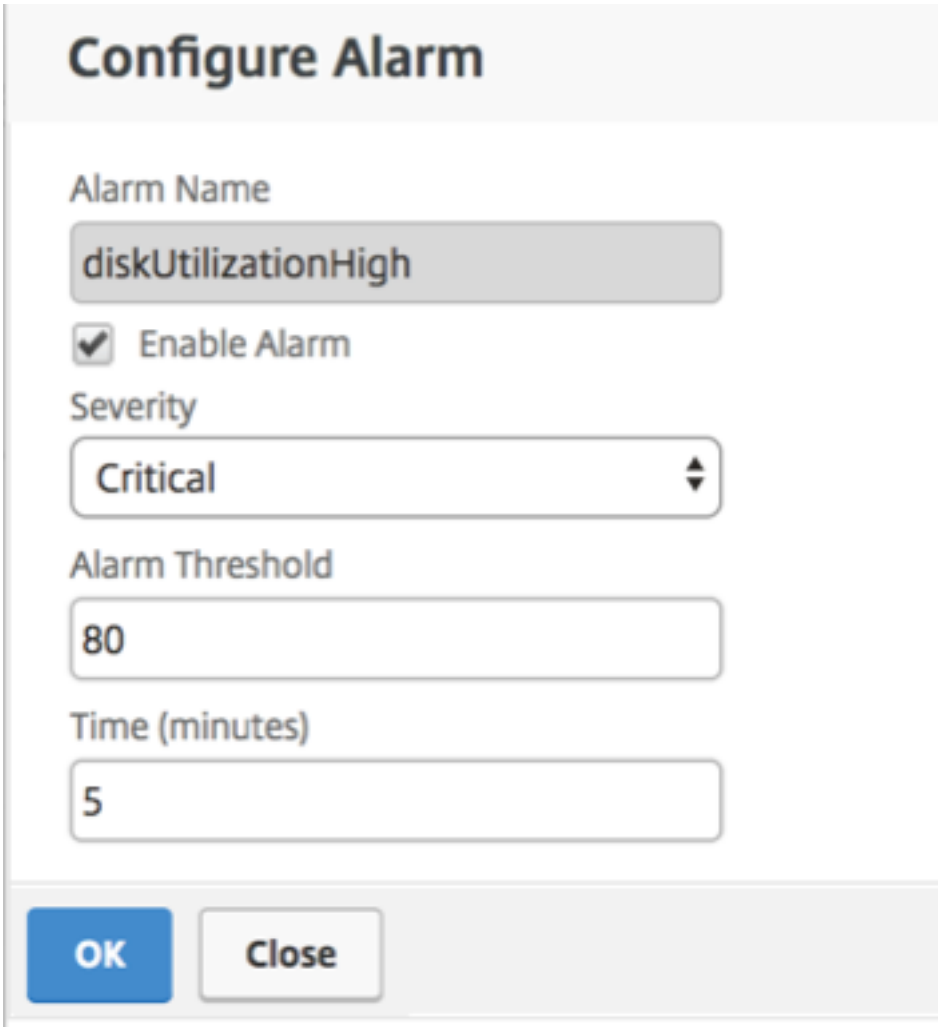
Vous pouvez activer le nettoyage automatique en cochant la case **Activer le nettoyage automatique des données**. Une alarme est déclenchée et un e-mail est envoyé lorsque l'utilisation du disque dépasse la **valeur seuil de nettoyage des données**configurée.

> **Remarque**
>
> Le nettoyage commence lorsque l'un des critères est rempli : valeur du seuil de nettoyage des données ou données à conserver (jours). Celui qui est atteint en premier a la priorité sur l'autre.

Pour configurer et activer les paramètres d'alarme :

1. Accédez à **Paramètres** > **SNMP**. Cliquez sur **Alarmes** dans le coin supérieur droit.
2. Sélectionnez l'alarme que vous souhaitez configurer (par exemple, DiskUtilizationHigh) et cliquez sur **Modifier**.
3. Sur la page **Configurer l'alarme**, spécifiez les éléments suivants :

- **Gravité** : sélectionnez le niveau de gravité.
- **Seuil d'alarme** : entrez la valeur pour laquelle la gravité de l'événement est calculée.
- **Heure** : saisissez l'heure (en minutes) au bout de laquelle vous souhaitez déclencher l'alarme.



Configurer les paramètres Events Prune à l'aide de NetScaler ADM

Pour limiter la quantité de données de messages d'événements stockées dans votre base de données NetScaler ADM, vous pouvez spécifier l'intervalle pendant lequel vous souhaitez que NetScaler 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).

1. Accédez à **Paramètres > Administration > Élagage des données**, puis cliquez sur **Élagage des données système et instance**. Cliquez sur **Événements d'instance**.
2. **Entrez l'intervalle de temps, en jours, pendant lequel vous souhaitez conserver les données sur le serveur NetScaler ADM et cliquez sur Enregistrer.**

Activer l'accès shell pour les utilisateurs non par défaut

February 1, 2024

Vous pouvez activer l'accès au shell pour les utilisateurs autres que ceux par défaut dans NetScaler 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 au shell pour les utilisateurs autres que ceux par défaut dans NetScaler ADM :

1. Dans NetScaler ADM, accédez à **Paramètres > Administration**.
2. Dans **Configurations du système**, cliquez sur **Système, Fuseau horaire, URL autorisées et paramètres de l'agent.**
3. Sur la page **Configurations du système**, configurez les paramètres suivants :

    - **Communication avec les instances** : sélectionnez le protocole de communication.
    - **Accès sécurisé** : activez un accès sécurisé pour NetScaler 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 des certificats** : vous permet de télécharger des certificats depuis le NetScaler ajouté.
    - **Activer l'accès au shell pour les utilisateurs autres que nsroot** : activez l'accès au shell pour les utilisateurs autres que ceux par défaut dans NetScaler ADM.
    - **Demander les informations d'identification des utilisateurs pour la connexion à l'instance** : autorisez les utilisateurs à saisir leurs informations d'identification lorsqu'ils se connectent aux instances depuis NetScaler ADM.
        - **Informations d'identification rapides pour les opérations Stylebooks** : autorisez les utilisateurs à saisir leurs informations d'identification lorsqu'ils utilisent StyleBook et les opérations du pack de configuration sur les instances NetScaler.

            > **Remarque :**
            > Si l'option **Prompt Credentials for Instance Login** est sélectionnée et que **les informations d'identification rapides pour les opérations Stylebook** sont désactivées, les utilisateurs ne sont pas invités à fournir des informations d'

> identification pour StyleBook et les opérations du pack de configuration sur les instances NetScaler.

4. Cliquez sur **OK**.

Restaurez les serveurs NetScaler ADM inaccessibles

February 1, 2024

NetScaler Application Delivery Management (ADM) fournit désormais un outil de maintenance de base de données permettant de nettoyer la base de données système. Vous pouvez désormais lancer l'utilitaire NetScaler ADM pour vous connecter au système de fichiers, supprimer quelques composants et rendre la base de données accessible. Le script de restauration NetScaler ADM est un outil qui permet de récupérer de l'espace dans le système de fichiers en supprimant les tables et les 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.

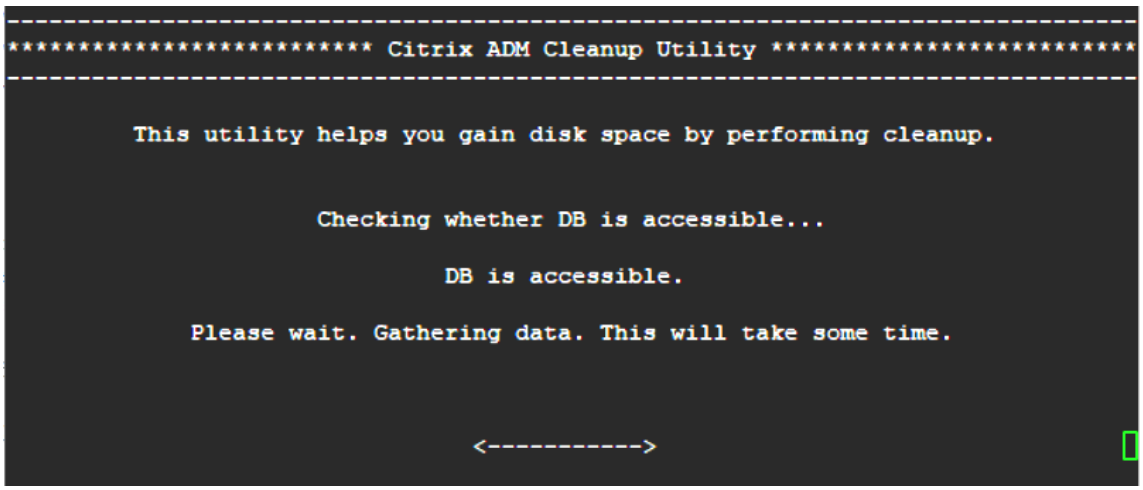
Comment utiliser le script de restauration de base de données NetScaler ADM pour un déploiement autonome de NetScaler ADM

Utilisez la procédure suivante dans un déploiement NetScaler ADM sur un seul serveur pour vous connecter au système de fichiers, supprimer quelques composants, rendre la base de données accessible, puis effectuer les opérations de restauration.

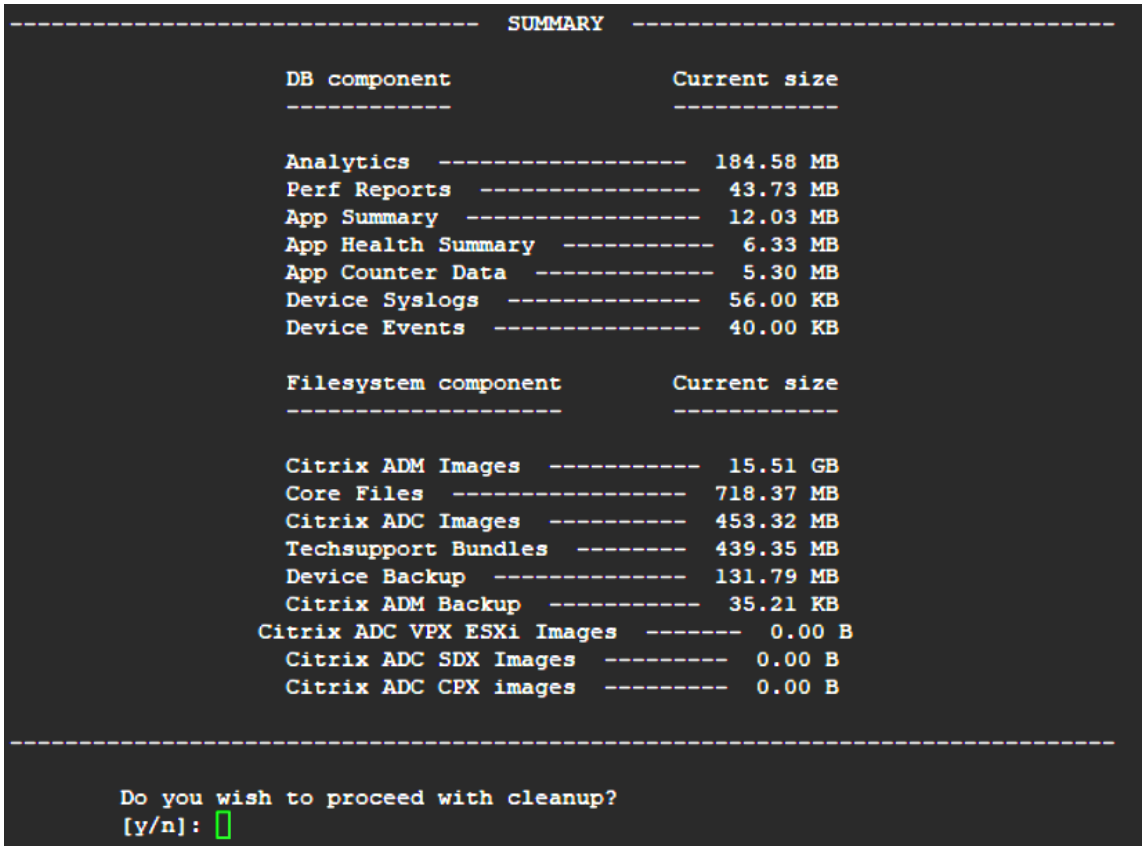
1.
```
Last login: Fri Nov 30 09:51:19 2018 from 10.252.241.100
Have a nice daybash-3.2# /mps/mas_recovery/mas_recovery.py
```

2. **Lorsque l'écran affiche un message d'avertissement concernant l'arrêt de certains processus NetScaler 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.



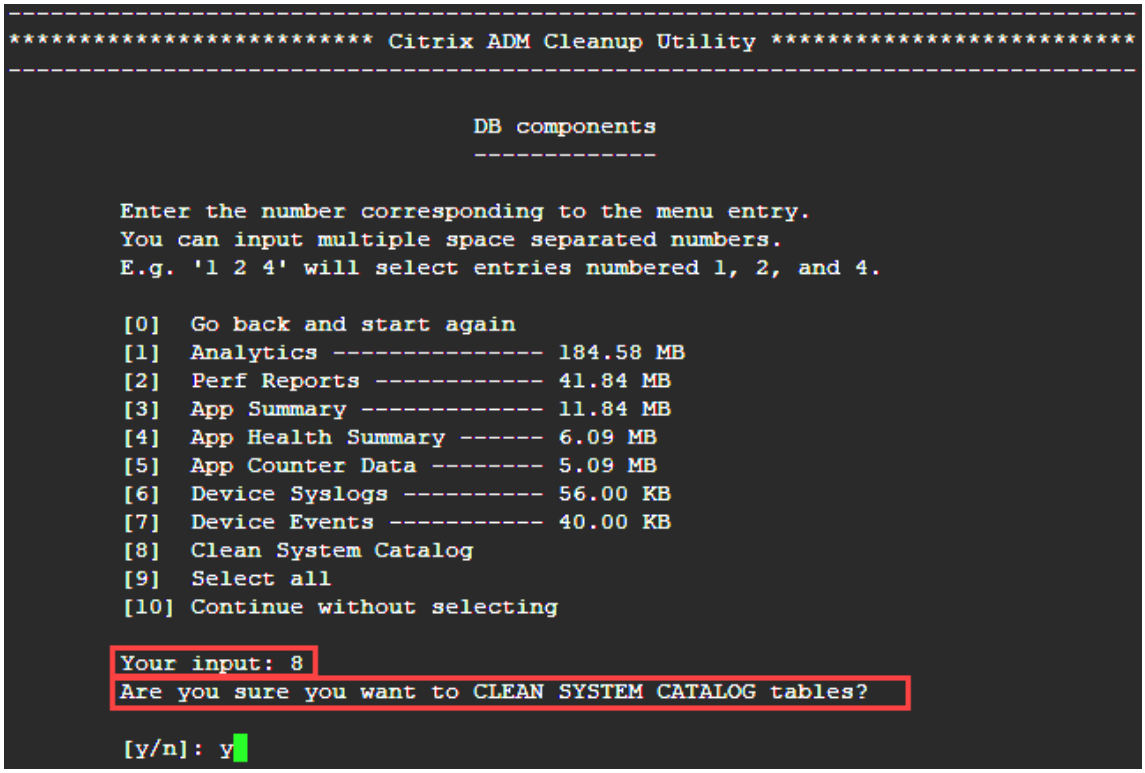
3. L'écran affiche la liste des fichiers de la base de données. Tapez « y » et appuyez sur la touche Entrée pour commencer le processus de nettoyage.



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.

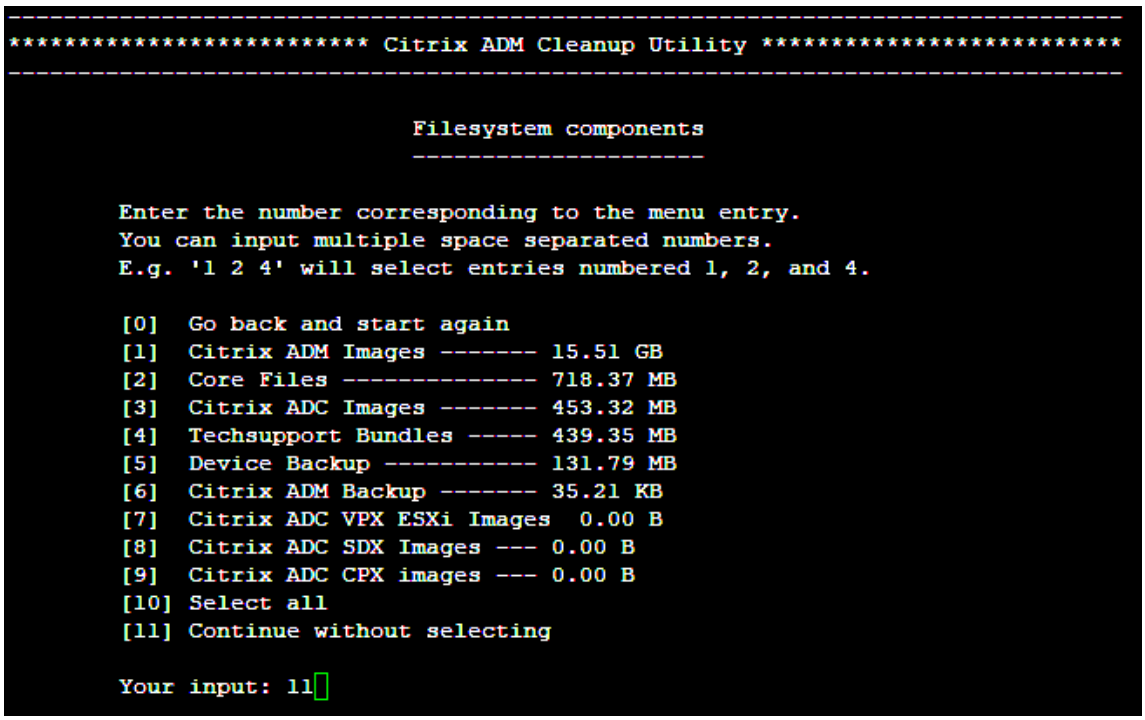
> **Remarque**
>
> NetScaler ADM inclut des tables utilisateur appelées catalogue système. Le catalogue système est un emplacement de la base de données NetScaler ADM où un système de gestion de base de données relationnelle stocke les métadonnées du schéma, telles que les informations relatives aux tables et aux colonnes et aux 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. Cette activité permet non seulement de libérer de l'espace disque, mais également d'améliorer les performances globales de la base de données et donc de NetScaler ADM.



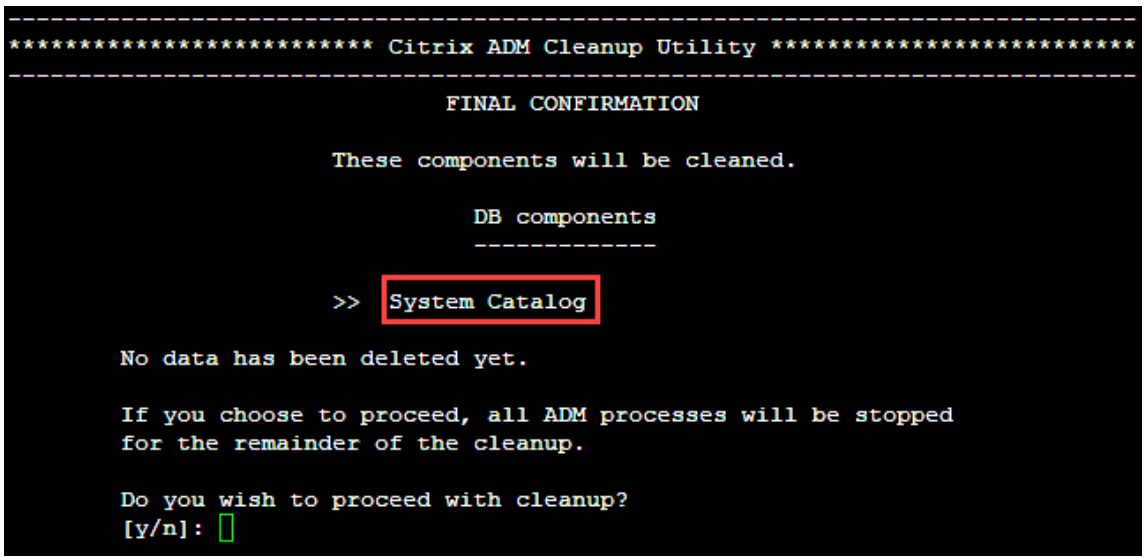
L'utilitaire de nettoyage vous permet de nettoyer les composants de base de données et les composants de fichiers. Vous pouvez sélectionner n'importe quel composant de fichier en saisissant un chiffre compris entre « 1 » et « 9 », ou en tapant « 11 » et en appuyant sur la touche Entrée pour nettoyer 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

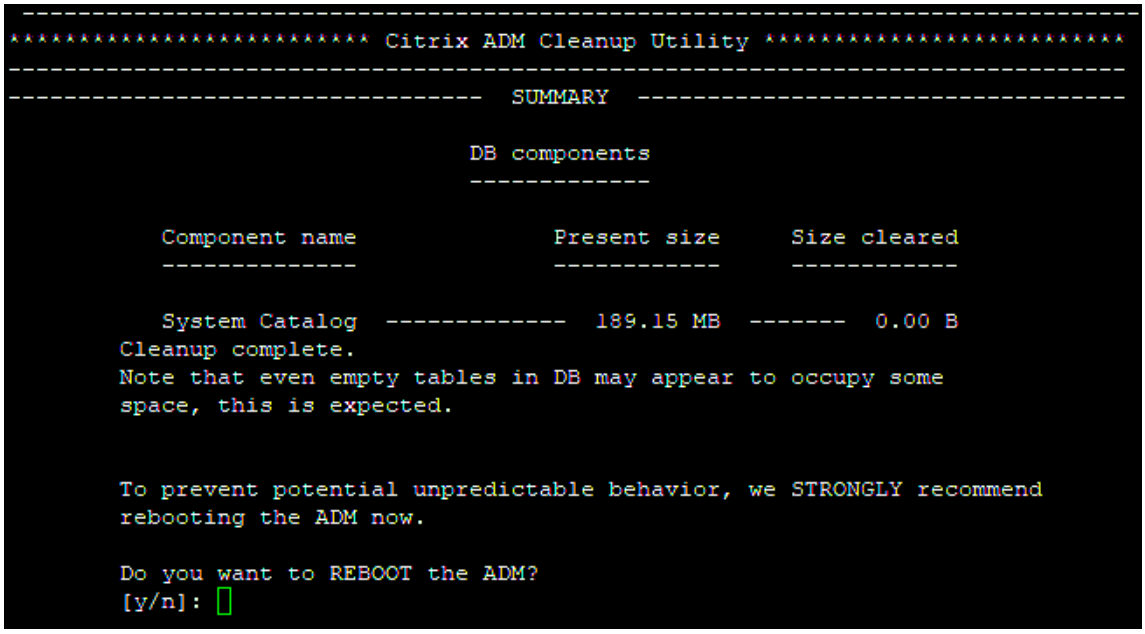
> sélectionné. Dans cet exemple, il s'agit du « catalogue système ».



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 NetScaler ADM.

   Assurez-vous de redémarrer NetScaler 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 NetScaler ADM. Vous devriez alors pouvoir vous connecter à la base de données NetScaler ADM. Si ce n'est pas le cas, exécutez à nouveau le script de récupération pour libérer plus d'espace. Lorsque NetScaler 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 utiliser le script de restauration de base de données NetScaler ADM pour un déploiement de haute disponibilité de NetScaler ADM

Le système de base de données pour les serveurs NetScaler ADM dans un déploiement à haute disponibilité est en mode de synchronisation continue. Lorsque vous utilisez le nouvel outil de restauration de base de données, il n'est pas nécessaire de répliquer la procédure sur les deux serveurs NetScaler 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 restauration du déploiement autonome NetScaler ADM

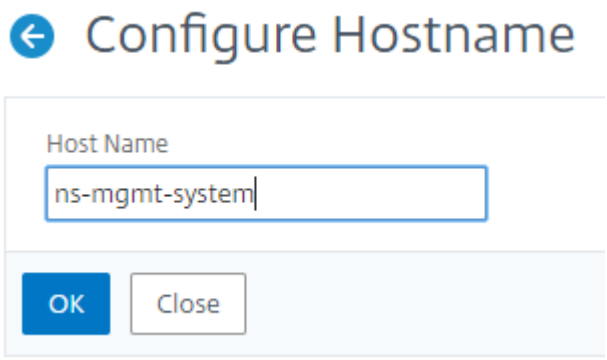
Attribuer un nom d'hôte à un serveur NetScaler ADM

February 1, 2024

Pour identifier un serveur NetScaler Application Delivery Management (ADM), vous pouvez lui attribuer un nom d'hôte. Le nom d'hôte est affiché sur la licence universelle pour NetScaler ADM.

Pour attribuer un nom d'hôte à un serveur NetScaler ADM :

1. Dans NetScaler 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**.



> **Remarque**
>
> Vous pouvez également utiliser la commande `networkconfig` de votre hyperviseur et modifier le nom d'hôte.

Sauvegardez et restaurez votre serveur NetScaler ADM

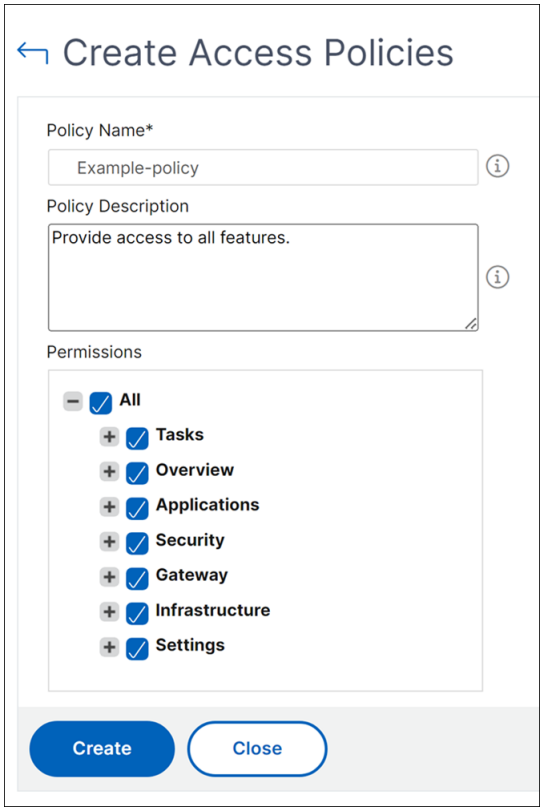
February 1, 2024

Vous pouvez effectuer des sauvegardes périodiques de votre serveur NetScaler 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 **Paramètres > Fichiers de sauvegarde** s'affiche uniquement pour les utilisateurs qui ont accès à toutes les fonctionnalités d'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 NetScaler ADM :
  - SNMP
  - Fichiers de configuration du serveur Syslog
  - Fichiers NTP

  - Certificats SSL
  - Fichiers du Centre de contrôle
- Sauvegardes des instances NetScaler gérées par le serveur NetScaler 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 NetScaler 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 de NetScaler ADM

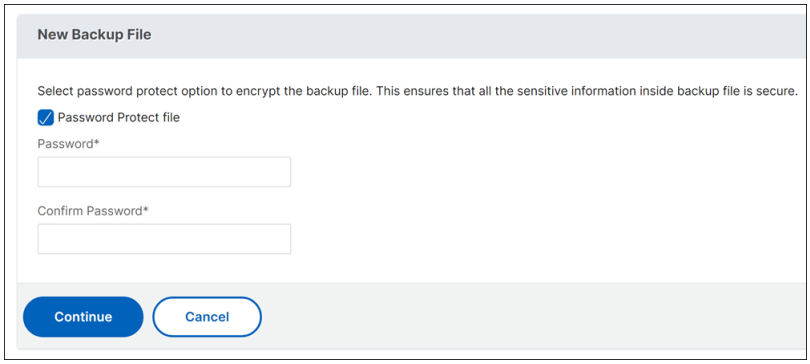
Par défaut, le serveur NetScaler ADM sauvegarde la configuration toutes les 24 heures (à 00h30). Vous pouvez également planifier et sélectionner l'heure de la sauvegarde. Vous pouvez également déplacer une copie du fichier sauvegardé vers un autre système.

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 insuffisant, vous pouvez stocker jusqu'à 10 fichiers de sauvegarde sur votre serveur NetScaler 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 NetScaler ADM :

1. Accédez à **Paramètres > 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.

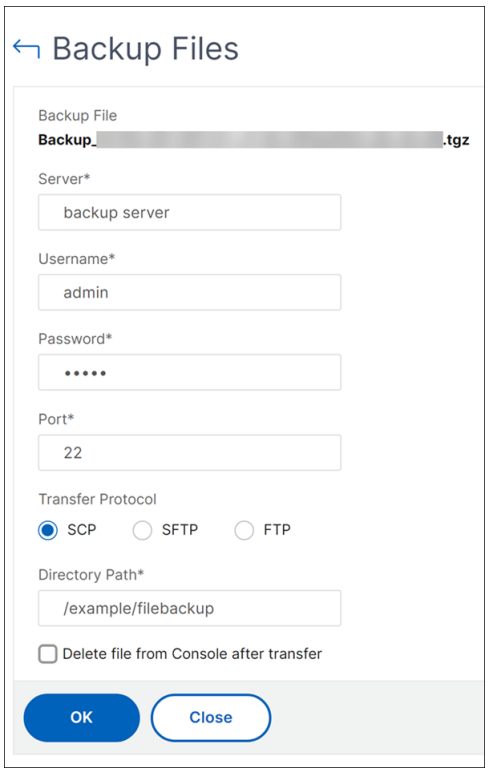


Transférer un fichier de sauvegarde NetScaler ADM vers un système externe

Vous pouvez transférer une copie du fichier de sauvegarde vers un autre système par mesure de précaution. Lorsque vous souhaitez restaurer la configuration, commencez par charger le fichier sur le serveur NetScaler ADM, puis effectuez l'opération de restauration.

Pour transférer un fichier de sauvegarde NetScaler ADM :

1. Accédez à**Paramètres > 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 NetScaler 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 **Paramètres > Fichiers de sauvegarde**, sélectionnez le fichier à copier, puis cliquez sur **Télécharger**.

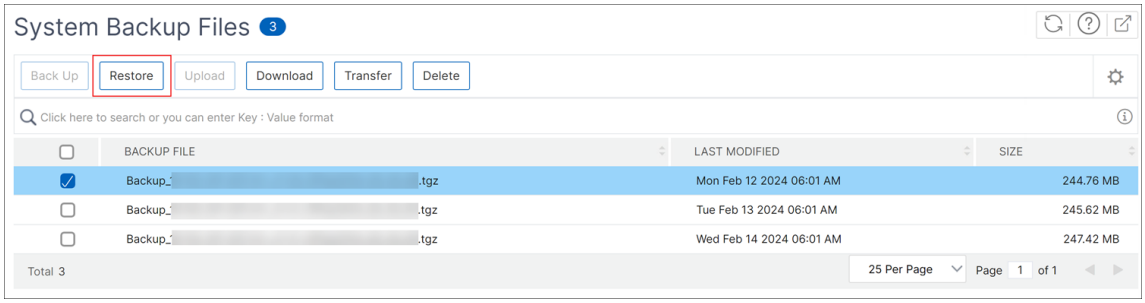
Restaurez la configuration de NetScaler ADM à partir d'un fichier de sauvegarde

Lorsque vous restaurez la configuration de NetScaler ADM à partir d'un fichier précédemment sauvegardé, l'opération de restauration détaille 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 NetScaler ADM à partir d'un fichier de sauvegarde :

1. Accédez à**Paramètres > 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 **Paramètres > Fichiers de sauvegarde**, puis cliquez sur **Télécharger**.

Instantanés de machines virtuelles de NetScaler ADM dans le cadre d'un déploiement à haute disponibilité

February 1, 2024

Vous pouvez prendre des instantanés des serveurs NetScaler ADM dans le déploiement HA avant de commencer votre mise à niveau. Les instantanés capturent l'état complet de la machine virtuelle au moment où vous les prenez.

Prenez un instantané des serveurs NetScaler ADM

Utilisez la séquence suivante pour prendre des instantanés des serveurs NetScaler ADM :

1. Serveur secondaire NetScaler ADM
2. Serveur principal NetScaler ADM

Pour prendre un instantané des serveurs NetScaler ADM :

1. Sur votre hyperviseur, sélectionnez le serveur secondaire NetScaler ADM dans la liste des machines virtuelles.
2. Prenez un instantané de machine virtuelle.

> **Remarque :**
>
> Nous vous recommandons de sélectionner **Prendre la mémoire de la machine virtuelle** lors de la prise du snapshot.

3. Donnez un nom significatif à l'instantané et entrez une description, si nécessaire.

   Le snapshot est stocké dans le répertoire de la machine virtuelle par défaut.

4. Répétez les mêmes étapes pour le serveur principal.

> **Remarque :**
>
> Il n'est pas nécessaire de mettre la machine virtuelle hors tension lorsque vous prenez un instantané.

Restaurer un instantané des serveurs NetScaler ADM

Lorsque vous restaurez un instantané, vous rétablissez la mémoire, les paramètres et l'état des disques de la machine virtuelle dans l'état dans lequel ils se trouvaient au moment où vous avez pris le snapshot.

Utilisez la séquence suivante pour restaurer les instantanés des serveurs NetScaler ADM :

1. Serveur principal NetScaler ADM
2. Serveur secondaire NetScaler ADM

Pour restaurer le snapshot des serveurs NetScaler ADM :

1. Sur votre hyperviseur, sélectionnez le serveur principal NetScaler ADM dans la liste des machines virtuelles.
2. Cliquez avec le bouton droit sur la machine virtuelle et rétablissez le snapshot.

   La machine virtuelle revient au snapshot le plus récent.

3. Répétez les mêmes étapes pour le serveur secondaire NetScaler ADM.

Afficher les informations d'audit

February 1, 2024

Syslog est un protocole standard de journalisation. Il comporte 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 (OS) FreeBSD sous-jacent de l'instance

NetScaler, 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 appareil NetScaler si vous configurez l'appareil pour rediriger les messages syslog vers NetScaler 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 NetScaler 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 NetScaler 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 NetScaler ADM :

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**.

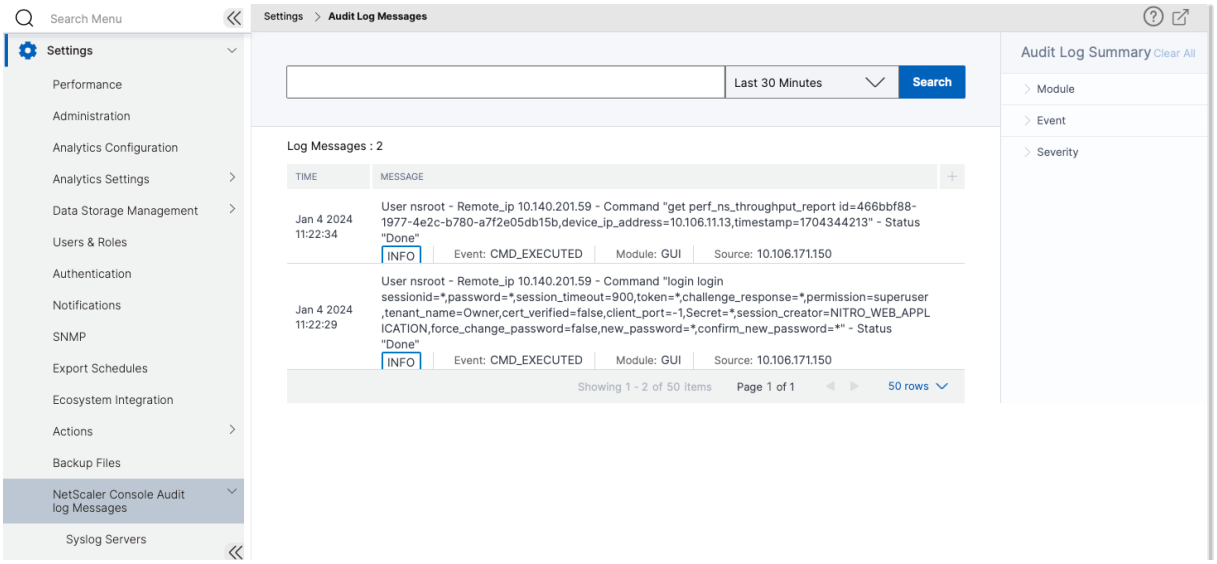
Pour afficher les messages Syslog sur NetScaler ADM :

Vous pouvez désormais consulter tous vos messages syslog générés sur vos instances NetScaler gérées si vous avez configuré votre instance pour rediriger les messages syslog vers le serveur NetScaler ADM. Les messages syslog sont stockés dans la base de données du serveur NetScaler ADM de manière centralisée 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 NetScaler Application Delivery Management (ADM) et spécifier le type de clients qui se connectent au système.

Pour configurer les paramètres SSL pour NetScaler 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**.

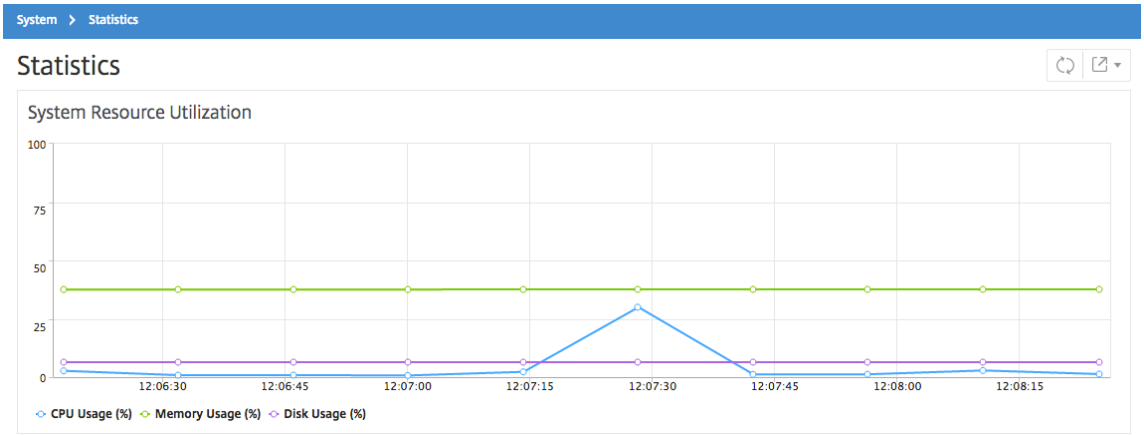
Surveiller l'utilisation du processeur, de la mémoire et du disque

February 1, 2024

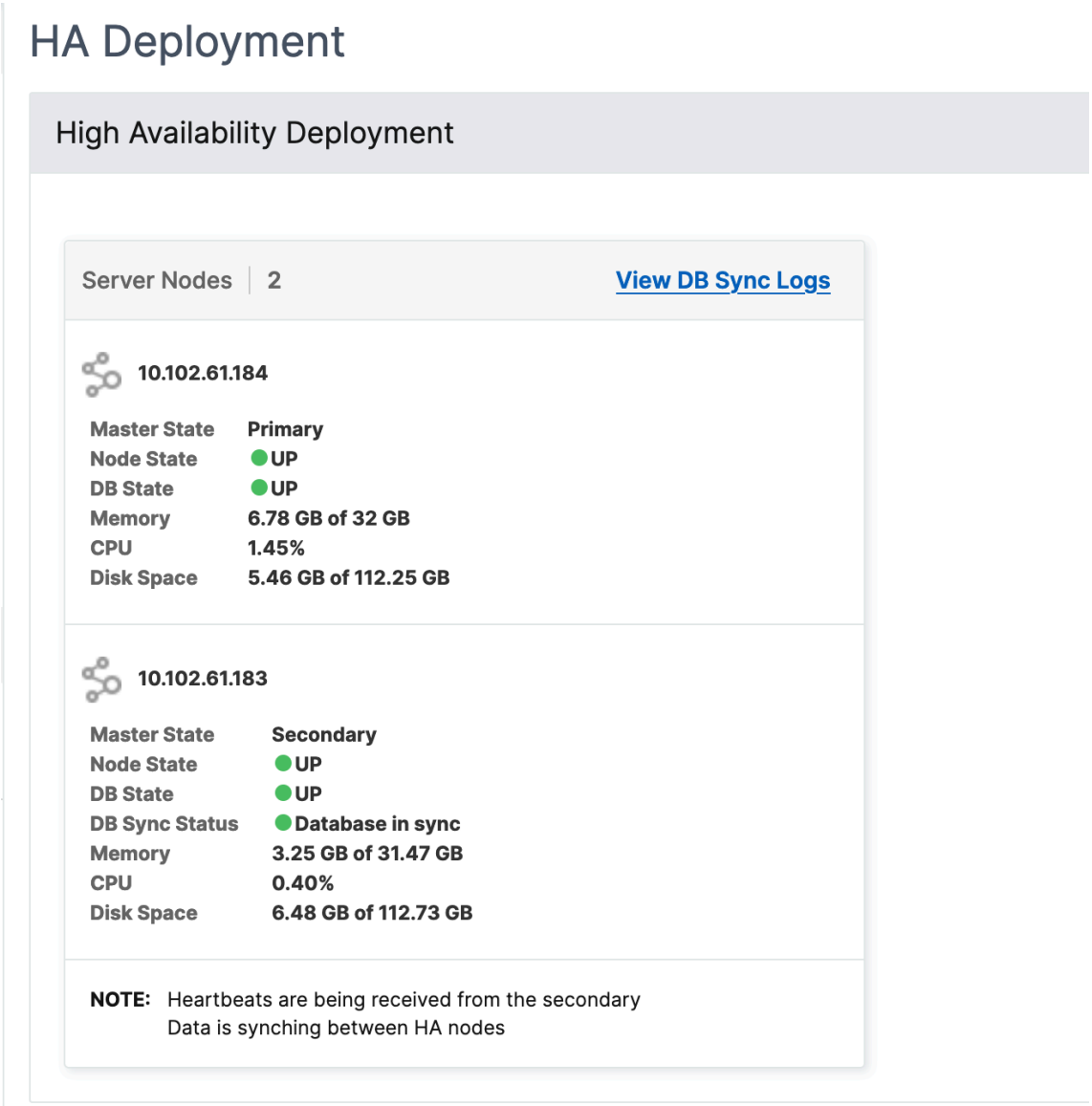
Vous pouvez utiliser les informations conservées dans les journaux et les statistiques. Ces informations sont également affichées dans des rapports qui vous aident à configurer et à gérer NetScaler Application Delivery Management (ADM).

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 **Paramètres > 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

February 1, 2024

Vous pouvez sélectionner un type de notification pour recevoir des notifications pour les fonctionnalités suivantes :

- **Événements** : liste des événements générés pour les instances NetScaler. 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 Expiration de la licence NetScaler ADM.

- **Certificats SSL** : liste des certificats SSL ajoutés aux instances NetScaler. 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

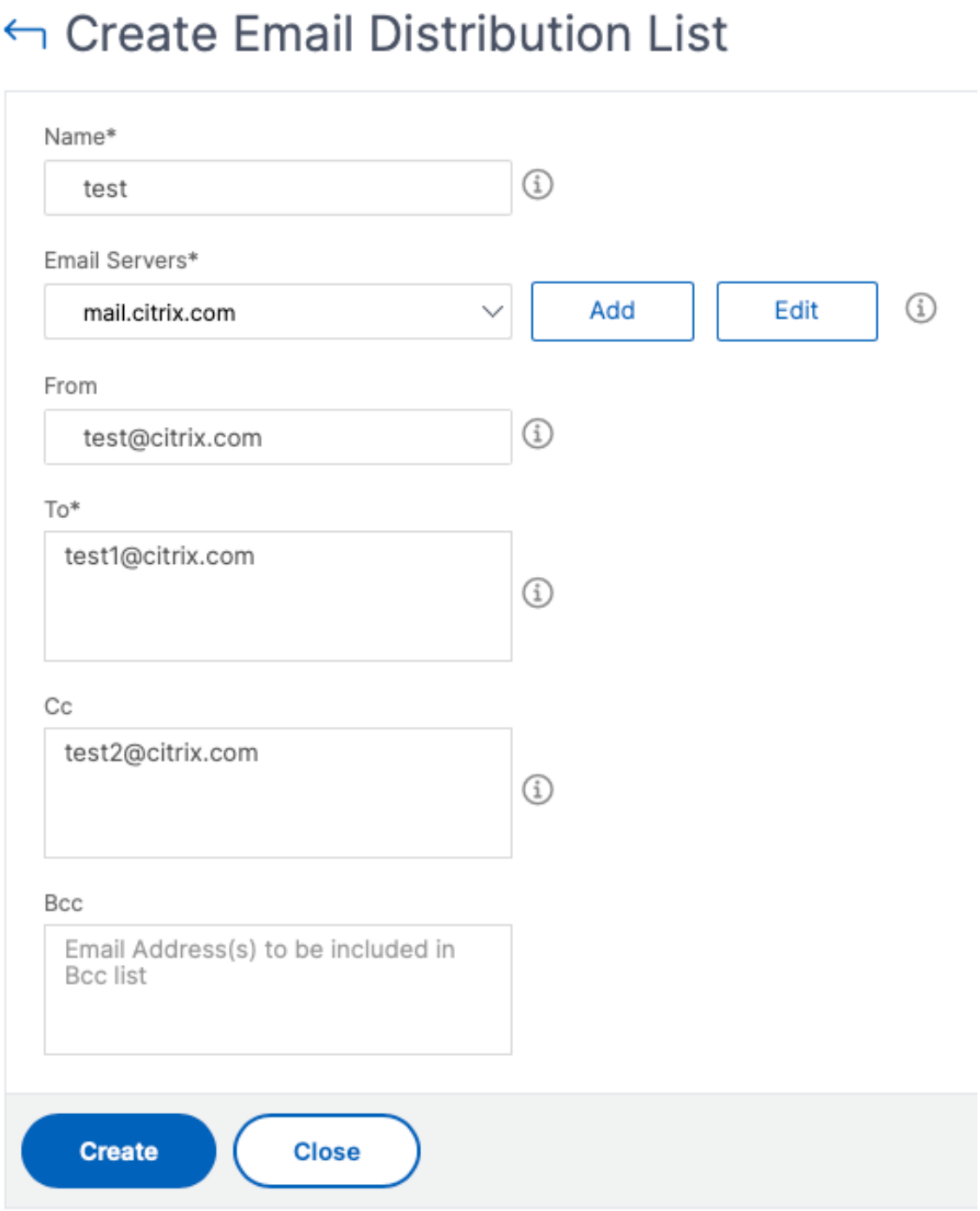
Pour chaque type de notification, l'interface graphique ADM affiche la liste ou le profil de distribution configuré. L'ADM envoie des notifications à la liste de distribution ou au profil sélectionné.

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 **Paramètres > 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 **Paramètres > 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**.

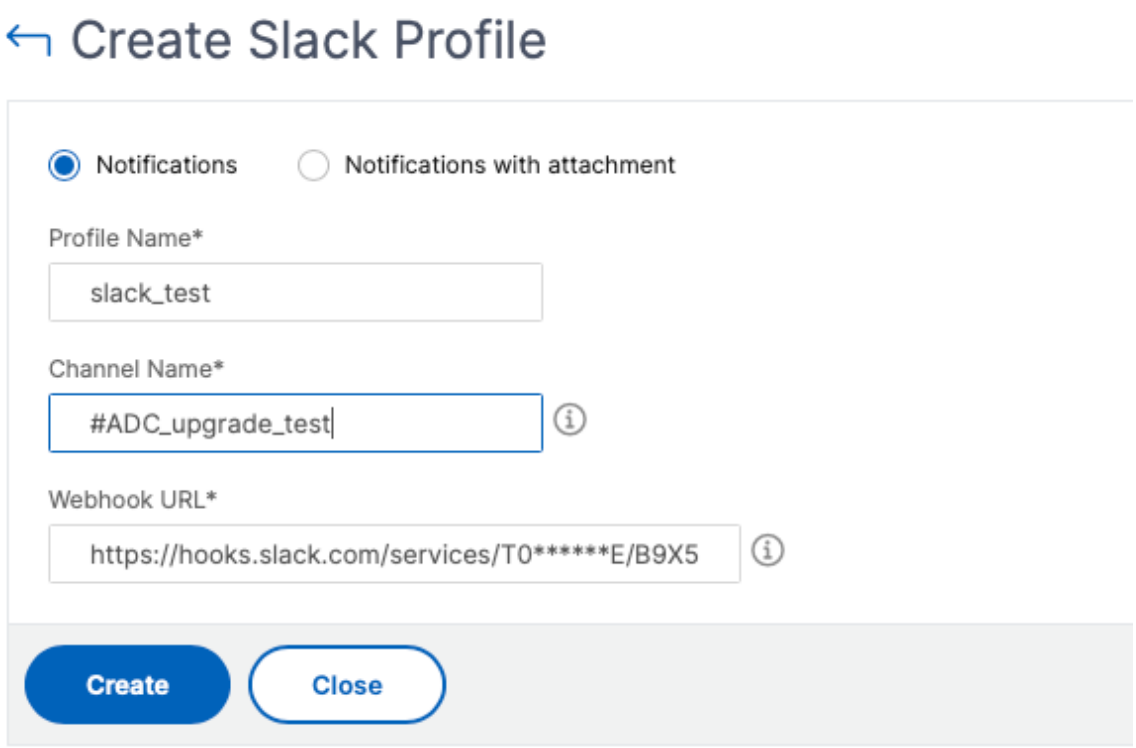
Répétez cette procédure pour créer plusieurs listes de distribution de SMS. L'onglet **SMS** affiche toutes les listes de distribution de SMS présentes dans ADM.

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 **Paramètres > 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 NetScaler ADM, assurez-vous d'avoir effectué 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 **Paramètres > 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 NetScaler et les événements ADM, vous devez intégrer NetScaler ADM à ServiceNow à l'aide du connecteur ITSM. Pour plus d'informations, voir Intégrer NetScaler ADM à l'instance ServiceNow.

Pour afficher et vérifier le profil ServiceNow, procédez comme suit :

1. Accédez à **Paramètres > 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 consulter les tickets ServiceNow dans l'interface graphique de NetScaler 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 NetScaler 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 NetScaler ADM en mode haute disponibilité, vous pouvez générer un fichier de support technique à partir de l'un ou l'autre 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 NetScaler 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 ADM sur votre stockage local, puis utiliser un navigateur Web pour le télécharger vers Citrix Insight Services (CIS).

   b) Vous pouvez également télécharger les fichiers de support technique sur le site Web du 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 directement vers CIS à l'aide d'un proxy depuis 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.

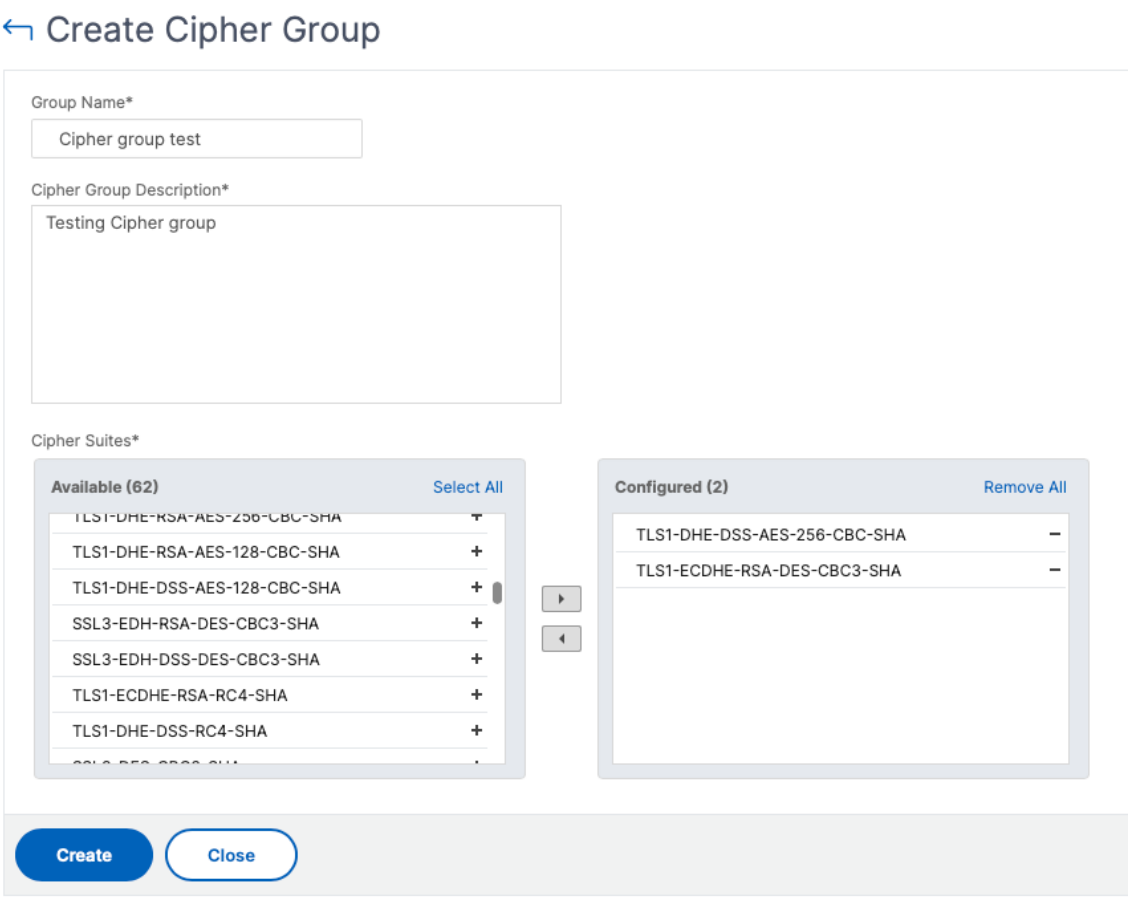
Configurer un groupe de chiffrement

February 1, 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 NetScaler ADM :

1. Accédez à **Paramètres > 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 survient sur NetScaler ADM, un piège SNMP est généré. Les interruptions sont ensuite envoyées à un périphérique distant appelé serveur de destination d'interruptions ou *destination d'interruptions SNMP*. Ici, NetScaler ADM est configuré comme destination du piège. 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 NetScaler 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'état de santé de vos serveurs NetScaler 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.

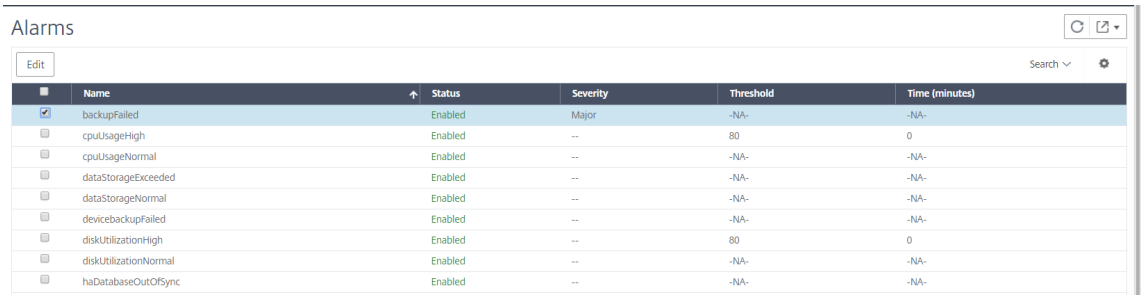
Vous pouvez attribuer ou modifier la gravité d'une alarme. Les niveaux de gravité que vous pouvez attribuer sont Critique, Majeur, Mineur, Avertissement et Informatif.

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 NetScaler ADM tente de sauvegarder les fichiers système et que la tentative échoue, une alarme se déclenche. Vous pouvez consulter le message sur NetScaler 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 NetScaler ADM :

1. Accédez à **Paramètres > SNMP** . Cliquez sur **Alarmes** dans le coin supérieur droit.



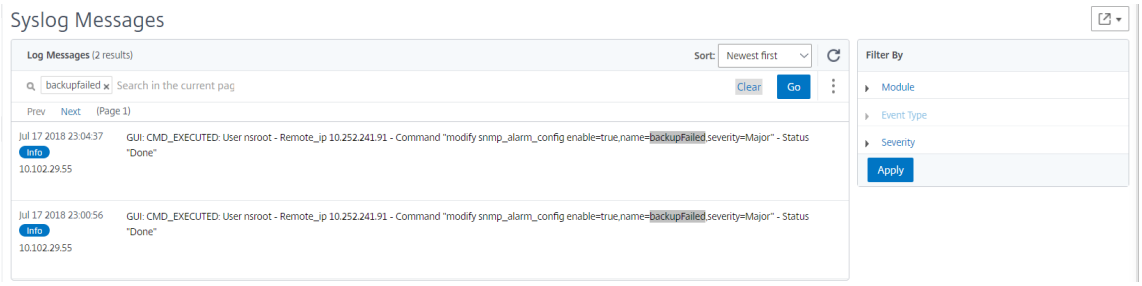
2. Sélectionnez l'alarme à configurer (par exemple, BackupFailed) et cliquez sur **Modifier** pour modifier ses paramètres.

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 NetScaler 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 configuration des notifications système, consultez Comment configurer les paramètres de notification système de NetScaler ADM.

Création de gestionnaires et d'utilisateurs SNMP pour l'agent NetScaler ADM

February 1, 2024

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.

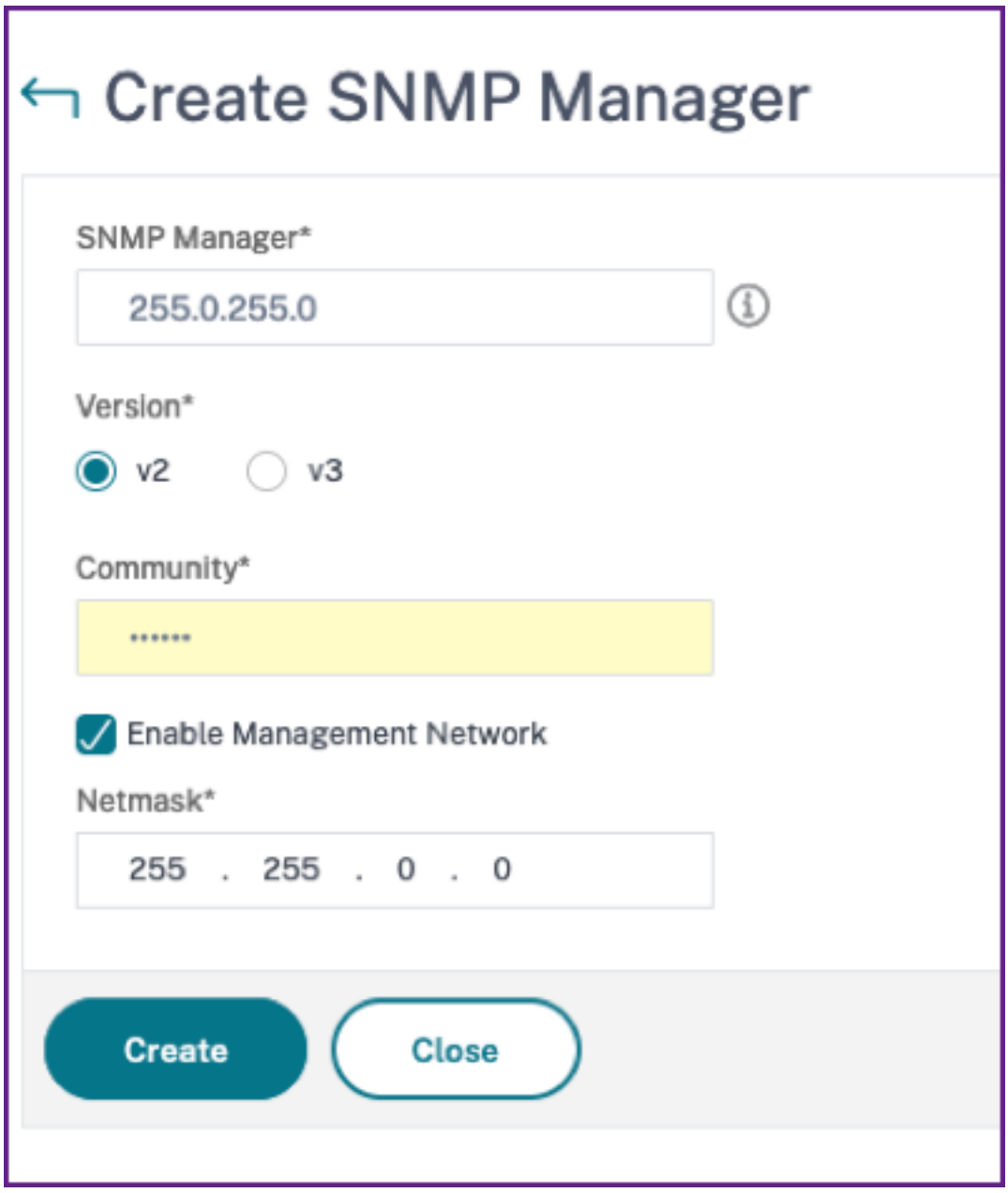
Vous pouvez ajouter un gestionnaire SNMP pour interroger un agent NetScaler ADM. Le gestionnaire est conforme aux normes SNMP V2 et V3. Si vous spécifiez un ou plusieurs gestionnaires SNMP, l'agent

NetScaler ADM n'accepte les requêtes SNMP provenant d'aucun hôte, à l'exception des gestionnaires SNMP spécifiés.

Ajouter un gestionnaire SNMP v2

Pour ajouter un gestionnaire SNMP v2 pour l'agent NetScaler ADM :

1. Accédez à **Infrastructure > Agents**, sélectionnez un agent NetScaler ADM, puis cliquez sur **Sélectionner une action**> Gérer le SNMP.
2. Dans l'onglet **SNMP> SNMP Manager**, cliquez sur **Ajouter**.
3. Sur la page **Créer un gestionnaire SNMP**, spécifiez les détails suivants :
    - **Gestionnaire SNMP**. Entrez le nom ou l'adresse IP du gestionnaire SNMP.
    - **Version**. Sélectionnez v2.
    - **Communauté**. Entrez le nom d'une communauté. Une configuration de communauté SNMP authentifie les requêtes SNMP provenant des gestionnaires SNMP.
    - **Activer le réseau de gestion** : cochez cette case pour spécifier le masque réseau du réseau du gestionnaire SNMP.
    - **Masque réseau** : entrez le masque de sous-réseau associé à une adresse IP.
4. Cliquez sur **Créer**.



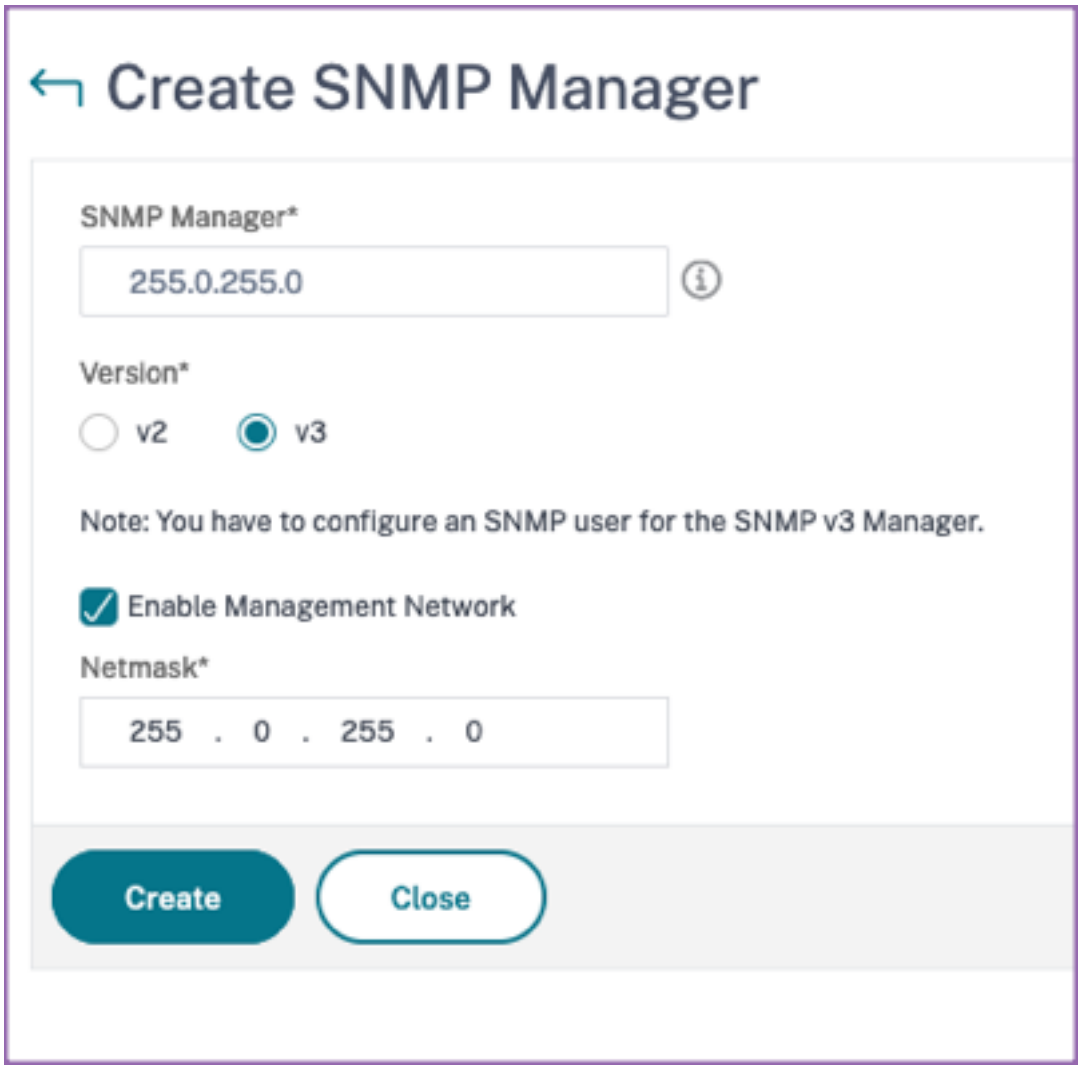
Ajouter un gestionnaire SNMP v3

Pour ajouter un gestionnaire SNMP v3 pour l'agent NetScaler ADM :

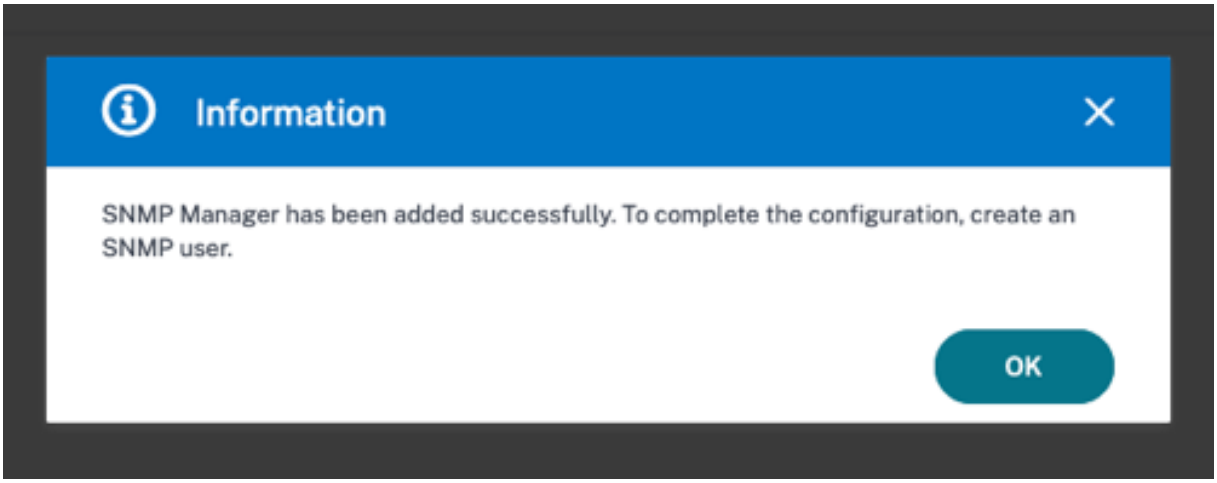
1. Accédez à **Infrastructure > Agents**, sélectionnez un agent NetScaler ADM, puis cliquez sur **Sélectionner une action**> Gérer le SNMP.
2. Dans l'onglet **SNMP> SNMP Manager**, cliquez sur **Ajouter**.
3. Sur la page **Créer un gestionnaire SNMP**, spécifiez les détails suivants :

- **Gestionnaire SNMP**. Entrez le nom ou l'adresse IP du gestionnaire SNMP.
- **Version**. Sélectionnez v3.
- **Activer le réseau de gestion** : cochez cette case pour spécifier le masque réseau du réseau du gestionnaire SNMP.
- **Masque réseau** : entrez le masque de sous-réseau associé à une adresse IP.

4. Cliquez sur **Créer**.



Une boîte de dialogue s'affiche pour confirmer qu'un gestionnaire SNMP est créé et vous invite à configurer un utilisateur SNMP.



> **Remarque**
>
> Vous devez configurer un utilisateur SNMP pour un gestionnaire SNMP v3. Pour configurer l'utilisateur SNMP, accédez à **SNMP > Utilisateur SNMP**.

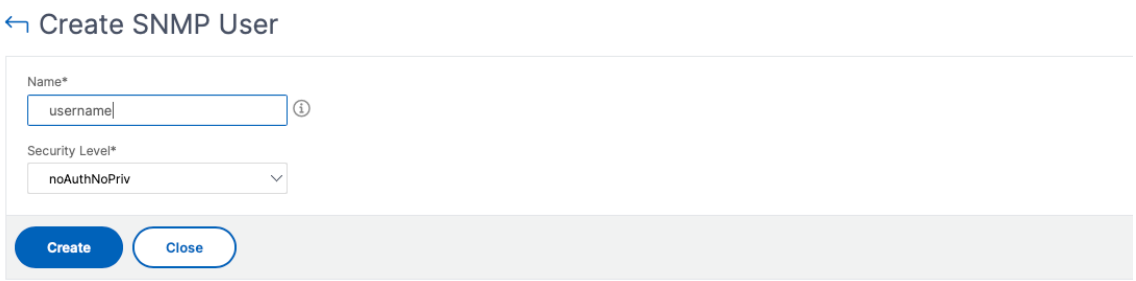
Ajouter un utilisateur SNMP

Ajoutez un utilisateur SNMP pour répondre aux requêtes SNMP v3 à partir d'un gestionnaire SNMP.

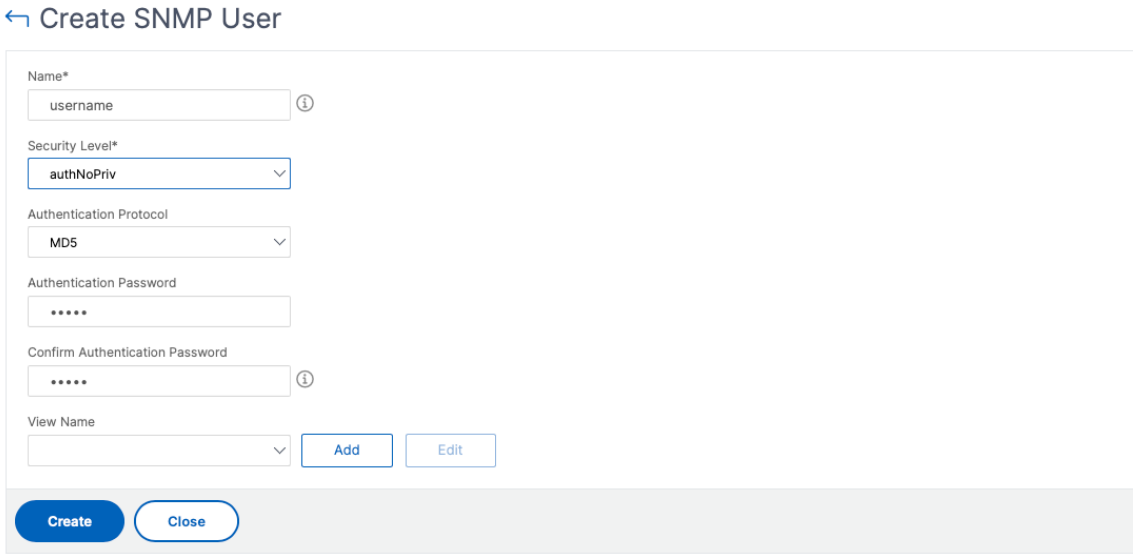
Pour ajouter un utilisateur SNMP pour l'agent NetScaler ADM :

1. Accédez à **Infrastructure > Agents**, sélectionnez un agent NetScaler ADM, puis cliquez sur **Sélectionner une action**> Gérer le SNMP.
2. Dans l'onglet **SNMP> Utilisateur SNMP**, cliquez sur **Ajouter**.
3. Sur la page **Créer un utilisateur SNMP**, ajoutez les informations suivantes :
   - **Nom**. Entrez le nom d'utilisateur.
   - **Niveau de sécurité**. Niveau de sécurité requis pour la communication entre l'agent NetScaler ADM et le gestionnaire SNMP.

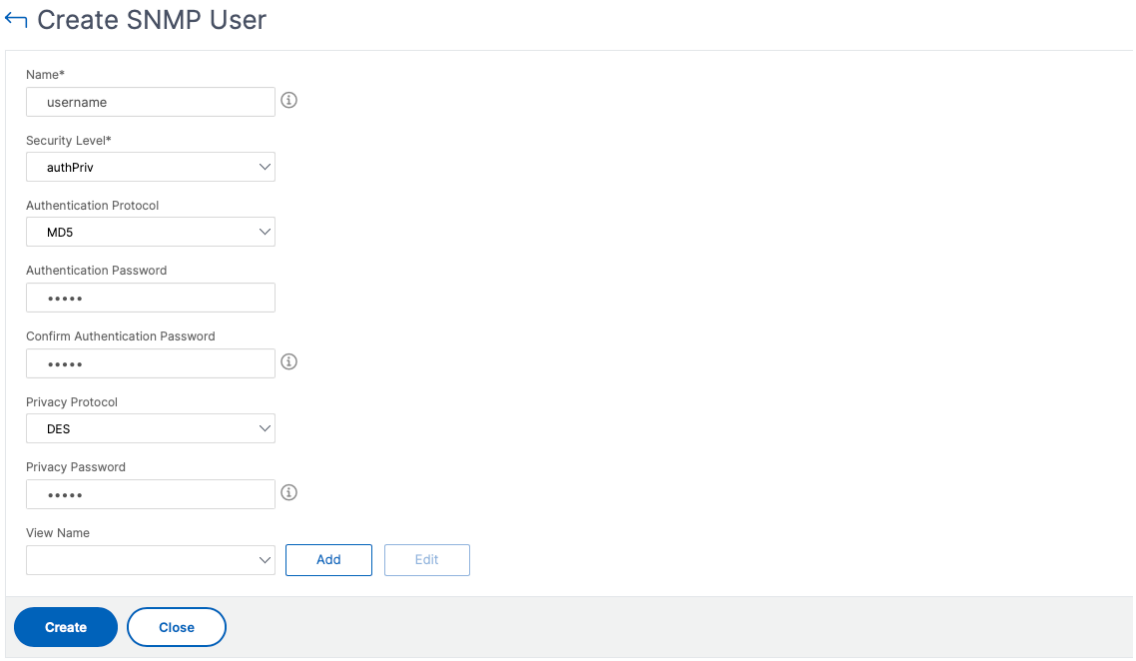
     Sélectionnez l'un des niveaux de sécurité suivants :
   - **noAuthNoPriv**. N'exigent ni authentification ni chiffrement.



- **authNoPriv**. Nécessite une authentification mais pas de chiffrement.



- **authPriv**. Exigez l'authentification et le chiffrement.



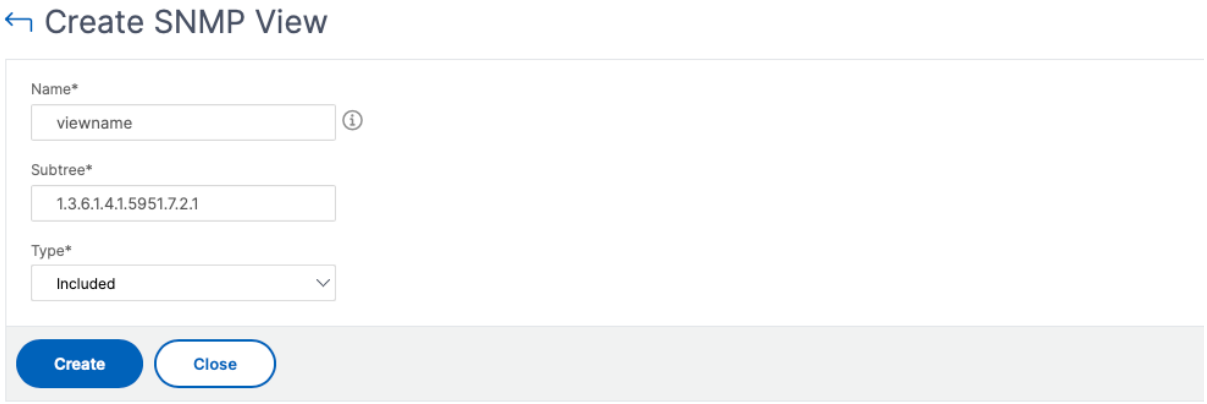
En fonction du niveau de sécurité que vous avez attribué à l'utilisateur, fournissez des protocoles d'authentification supplémentaires, tels que des protocoles d'authentification, des mots de passe de confidentialité et attribuez des vues SNMP.

Gestion des vues SNMP

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

Pour autoriser ou restreindre un OID SNMP pour l'agent NetScaler ADM :

1. Accédez à **Infrastructure > Agents > Gérer le SNMP** et dans l'onglet **Affichage SNMP**, cliquez sur **Ajouter**.
2. Dans la fenêtre **Créer une vue SNMP**, entrez les informations suivantes :
   - **Nom de la vue** : nom de la vue SNMP. Une instance peut avoir de nombreuses vues SNMP portant le même nom, différenciées par les paramètres de la sous-arborescence.
   - **Sous-arbre** : branche particulière (sous-arbre) de l'arborescence MIB que vous souhaitez associer à cette vue SNMP. Vous devez spécifier la sous-arborescence en tant qu'OID SNMP.
   - **Type** : Ce champ vous permet d'inclure ou d'exclure des sous-arbres d'une vue.
3. Cliquez sur **Créer**.



Configurer les paramètres de l'agent

February 1, 2024

Vous pouvez modifier l'intervalle de conservation et les exigences de modification du mot de passe de l'agent NetScaler ADM.

Définir l'intervalle de garder en vie de l'agent

Le serveur et l'agent NetScaler ADM conservent la même connexion TCP pendant l'intervalle de maintien en activité spécifié. Un agent utilise cette connexion pour envoyer les données des instances

gérées au serveur NetScaler ADM.

1. Accédez à **Paramètres > Administration**.
2. Sélectionnez **Système, fuseau horaire, URL autorisées et Paramètres de l'agent** sous **Configurations système**.
3. Dans **Paramètres de base > Paramètres de l'agent**, spécifiez l'intervalle de maintien en activité compris entre 30 et 120 secondes.
4. Cliquez sur **Enregistrer**.

Changer le mot de passe de l'agent sans le mot de passe actuel

Vous pouvez autoriser la modification des mots de passe des agents sans leur mot de passe actuel.

1. Accédez à **Paramètres > Administration**.
2. Sélectionnez **Système, fuseau horaire, URL autorisées et Paramètres de l'agent** sous **Configurations système**.
3. Dans la case à cocher **Paramètres de base > Paramètres de l'agent > Supprimer le mot de passe actuel requis pour la modification du mot de passe de l'agent**, vous pouvez effectuer les opérations suivantes :
   - Cochez la case pour supprimer le champ **Mot de passe actuel** sur la page Mot de **passe de l'agent de modification** .
   - Décochez la case pour conserver le champ **Mot de passe actuel** sur la page **Changer le mot de passe de l'agent** .
4. Cliquez sur **Enregistrer**.

> **Remarque**
>
> Pour afficher la page **Modifier le mot de passe de l'agent**, accédez à **Infrastructure > Instances > Agents**, sélectionnez un agent, puis cliquez sur **Sélectionner une action > Modifier le mot de passe**.

Utiliser le tableau de bord de gestion du stockage des données

February 1, 2024

Il est important de connaître les fonctionnalités utilisées dans NetScaler ADM et l'utilisation des données de chacune de ces fonctionnalités. Le tableau de bord **de gestion du stockage des données**

répond à cet objectif et fonctionne comme votre outil de visualisation, vous permettant de comprendre l'ensemble des données stockées dans la base de données NetScaler ADM à travers différentes fonctionnalités. Le tableau de bord indique également si le stockage consommé se situe dans les limites spécifiées ou s'il est supérieur au stockage autorisé.

En tant qu'administrateur, vous pouvez effectuer les tâches suivantes dans le tableau de bord **de gestion du stockage des données** :

- Afficher la consommation de stockage des données au cours des 30 derniers jours - Les tendances en matière de stockage des données sont stockées dans la base de données NetScaler ADM au cours des 30 derniers jours. Ces tendances sont disponibles sous forme graphique ou tabulaire. Ces tendances indiquent la quantité de données entrée et la quantité de données stockées après les cycles de nettoyage planifiés dans NetScaler ADM.
- Afficher l'état d'ingestion des données - L'activité d'ingestion de données se produit tant que le stockage consommé se situe dans les limites du stockage autorisé. Lorsque le stockage consommé est supérieur au stockage autorisé, l'activité des données est suspendue.
- Envoyer des notifications - Vous pouvez configurer l'envoi de notifications lorsque le stockage consommé atteint 75 % ou 100 % de l'espace de stockage autorisé, ce qui permet aux utilisateurs de gérer leur stockage.
- Flexibilité de gestion de l'espace de stockage des données - Vous pouvez créer plus d'espace dans les données stockées en effectuant un nettoyage des données que vous jugez appropriées pour être supprimées ou réduites.

Accédez à **Paramètres > Gestion du stockage des données** pour afficher votre tableau de bord de stockage des données.

Les sections suivantes expliquent comment utiliser le tableau de bord de **gestion du stockage des données** pour une gestion efficace du stockage des données :

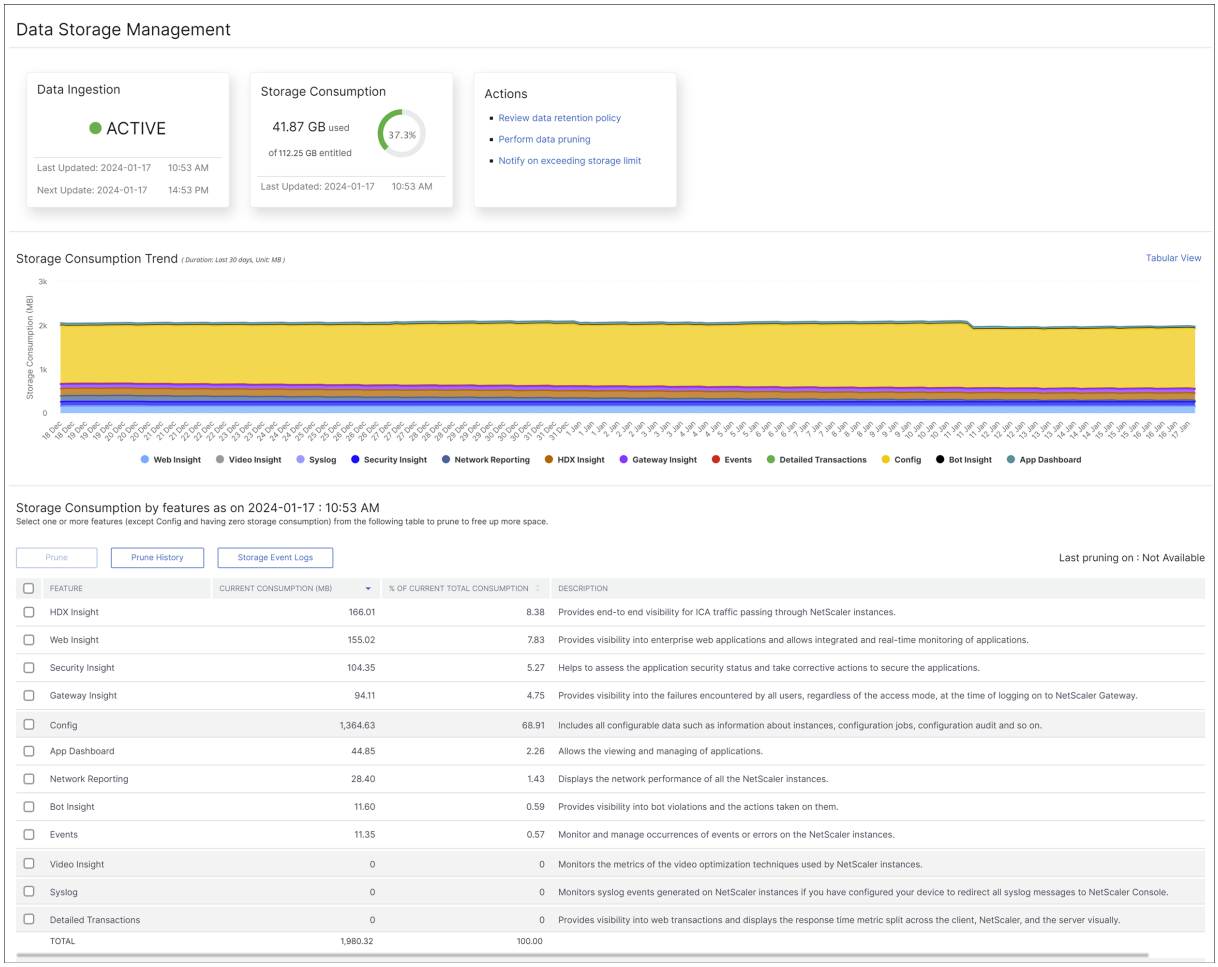
- Comprenez votre stockage de données - Cette section vous aide à comprendre comment utiliser le tableau de bord pour consulter les informations relatives à votre stockage de données.
- Gérez votre stockage de données - Cette section fournit des informations sur les actions que vous pouvez effectuer dans le tableau de bord pour gérer votre stockage de données.

Comprenez votre stockage de données

February 1, 2024

Vous pouvez utiliser le tableau de bord **de gestion du stockage des données** de NetScaler ADM pour consulter les données et les graphiques qui vous aident à suivre votre utilisation du stockage de données.

Pour surveiller votre consommation de stockage de données, accédez à **Paramètres > Gestion du stockage des données**.



Le tableau de bord de gestion du stockage des données indique les informations suivantes :

- État de votre activité d'ingestion de données
- Consommation totale de stockage
- Tendances de consommation de stockage
- Consommation de stockage par fonctionnalités

État de votre activité d'ingestion de données

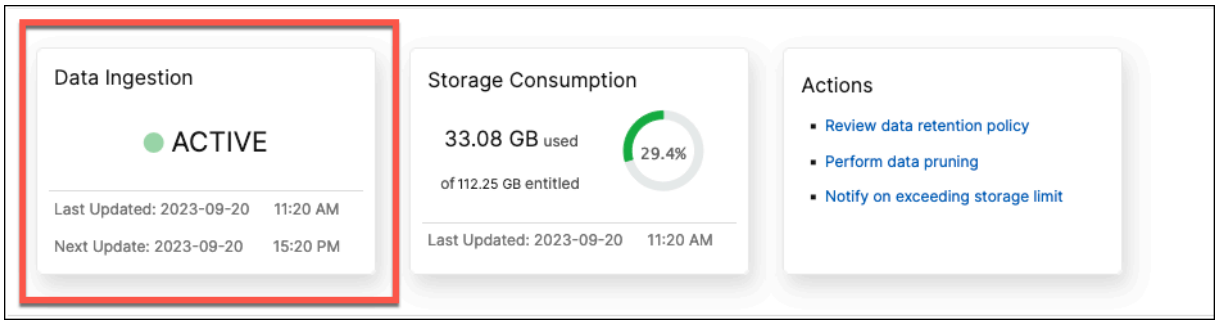
L'ingestion de données fait référence au processus d'importation de données volumineuses et variées depuis toutes les instances NetScaler gérées via diverses fonctionnalités telles que les événements, les Syslogs, les rapports réseau, etc. dans le stockage NetScaler ADM.

L'état d'ingestion des données indique si NetScaler ADM collecte des statistiques à partir d'instances NetScaler. L'activité d'ingestion de données se poursuit tant que le stockage consommé se trouve

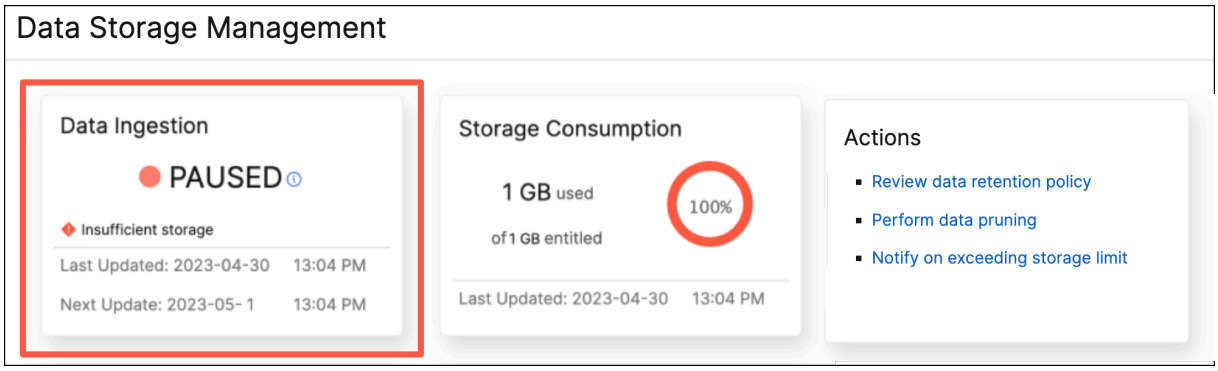
dans le stockage autorisé. Lorsque la consommation est supérieure au stockage autorisé, l'ingestion des données est suspendue.

Consultez la vignette **Ingestion des données** pour comprendre l'état actuel de l'ingestion des données. Cette vignette affiche l'un des deux états suivants :

- **Actif** : l'activité d'ingestion de données est en cours.



- **Suspendu** - L'activité d'ingestion de données est suspendue car le stockage consommé dépasse le stockage autorisé.

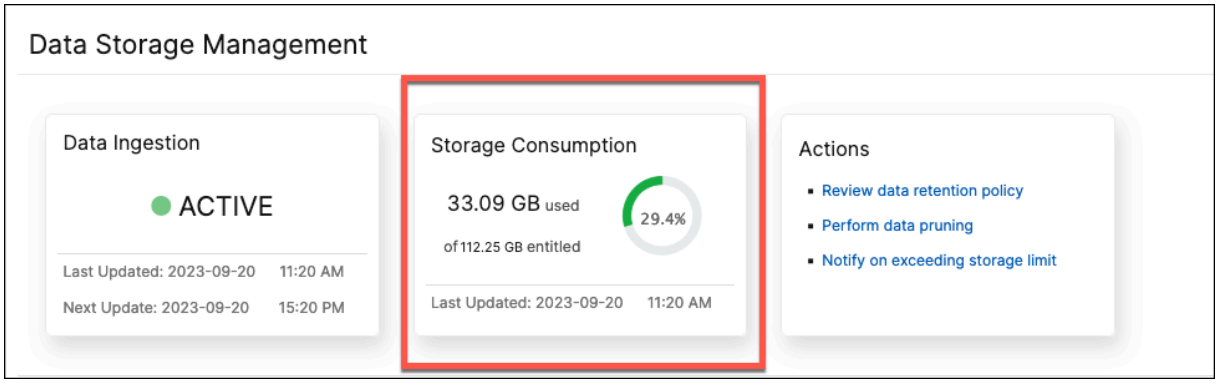


Comment reprendre votre ingestion de données interrompue

Pour reprendre votre activité d'ingestion de données, vous pouvez effectuer un nettoyage des données. Pour plus d'informations, consultez la section Effectuer un nettoyage des données.

Consommation totale de stockage

Pour un aperçu rapide de votre stockage de données, consultez la vignette **Consommation de stockage** .



La vignette **Consommation de stockage** affiche le stockage total utilisé par toutes les fonctionnalités du déploiement.

Passez la souris sur le graphique en forme de beignet pour voir ce qui suit :

Intitulé Storage

Le stockage autorisé est le stockage total que vous pouvez utiliser conformément à votre licence. Si vous possédez une licence Express, vous bénéficiez de 500 Mo de stockage autorisé. Si vous possédez une licence Advanced, vous bénéficiez de 500 Mo de stockage par VIP acheté et de tout stockage supplémentaire acheté directement sans acheter de VIP.

Envisagez les scénarios suivants :

- Tu as acheté 20 VIP. Vous bénéficiez de 500 Mo de stockage gratuit pour chaque VIP. Votre espace de stockage autorisé est de 20*500 = 10 Go.
- Vous avez acheté 20 VIP et un espace de stockage supplémentaire de 5 Go. Vous bénéficiez de 500 Mo de stockage gratuit pour chaque VIP. Votre espace de stockage autorisé est de 20*500 + 5 = 15 Go.

Stockage consommé

Le stockage consommé est le stockage total utilisé par toutes les fonctionnalités du déploiement. Les critères de code couleur suivants indiquent la quantité de stockage utilisée par les fonctionnalités :

- **Vert** - L'espace de stockage consommé est inférieur à 75 % du stockage autorisé.
- **Ambre** - Le stockage consommé représente entre 75 % et 99 % du stockage autorisé.
- **Rouge** - La limite de stockage consommée a atteint ou est supérieure au stockage autorisé actuel.

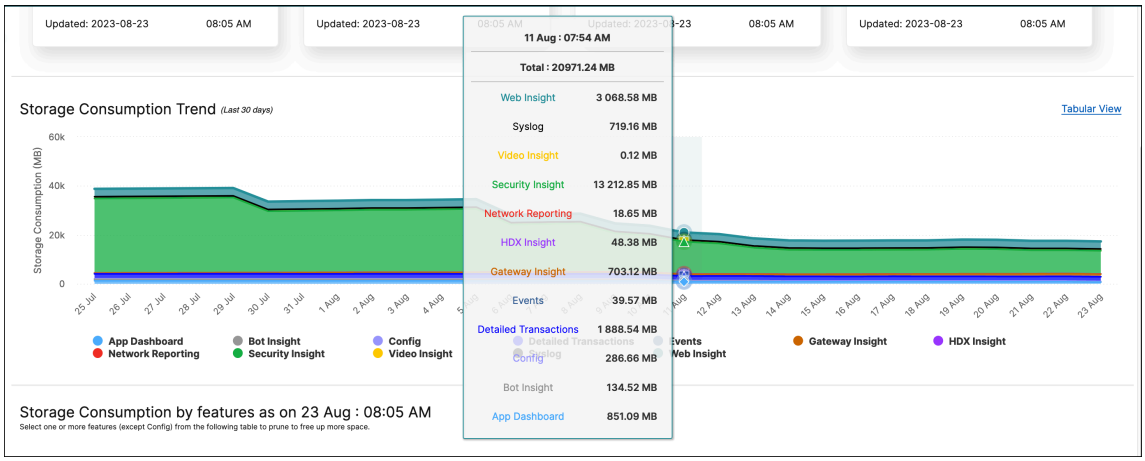
Tendances de consommation de stockage

Pour savoir comment les données ont été consommées au cours des 30 derniers jours, consultez la section **Tendance en matière de consommation de stockage** .

Storage Consumption Trend fournit des informations sur les fonctionnalités qui utilisent le plus ou le moins de stockage sur une période donnée et vous aide à gérer efficacement votre consommation de stockage de données.

Vous pouvez consulter les tendances relatives aux données de stockage sous l'une des formes suivantes :

- **Vue graphique** : affiche la manière dont le stockage des données est réparti entre les différentes fonctionnalités de NetScaler ADM. Passez votre souris sur la chronologie pour afficher les informations de stockage des données pour n'importe quel jour du mois.



> **Remarque :**
>
> La **vue graphique** est la vue par défaut.

- **Vue tabulaire** : cliquez sur Vue **tabulaire pour afficher** les informations de stockage des données sous forme de tableau.

Storage Consumption Trend *(Last 30 days)* Graphical View

FEATURE	25 JUL	26 JUL	27 JUL	28 JUL	29 JUL	30 JUL	31 JUL	1 AUG	2 AUG	3 AUG	4 AUG
Security Insight	30415.05	30478.90	30535.21	30596.05	30648.76	25069.69	25222.26	25380.30	25552.37	25551.91	2570
Web Insight	3193.42	3200.39	3207.48	3213.02	3219.95	3226.22	3231.98	3238.30	3246.83	3252.87	3258
Detailed Transactions	2007.07	1998.34	1985.43	2046.68	2031.71	2014.52	1995.44	1985.16	2039.65	2025.91	2014
Gateway Insight	248.15	279.05	310.27	342.74	373.78	403.89	434.83	466.64	499.50	499.01	529.
Syslog	775.05	775.54	776.50	686.32	697.56	708.37	719.57	720.30	721.24	721.61	721.5
App Dashboard	1240.54	1237.85	1238.79	1238.08	1238.98	1238.13	1238.94	1238.66	1239.17	1239.24	1238
Config	269.76	270.68	272.41	273.02	274.16	275.49	275.18	272.52	271.13	271.70	271.8
HDX Insight	52.95	52.72	52.49	52.53	52.45	52.64	52.75	52.83	52.80	53.23	52.9
Events	45.06	45.27	44.85	44.49	43.96	43.63	43.24	43.08	43.16	42.95	42.5
Network Reporting	21.80	21.78	21.77	21.77	21.77	21.77	21.77	21.77	21.75	22.07	22.2
Bot Insight	544.23	543.98	544.09	544.32	544.10	544.01	544.10	544.05	544.10	544.10	544.
Video Insight	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25
TOTAL	38813.31	38904.75	38989.54	39059.27	39147.42	33598.61	33780.30	33963.85	34231.95	34224.85	3439

Showing 1 - 12 of 12 items Page 1 of 1

> **Remarque :**
>
> La vue tabulaire vous permet de filtrer les données à l'aide du champ de recherche.

Le tableau suivant décrit les champs affichés dans la section **Tendance de consommation de stockage** :

FONCTIONNALITÉ	DESCRIPTION
Config	Inclut toutes les données configurables telles que les informations sur les instances, les tâches de configuration, l'audit de configuration, etc.
HDX Insight	Fournit une visibilité de bout en bout du trafic ICA passant par NetScaler.
Rapports sur le réseau	Affiche les performances réseau de toutes les instances NetScaler.
Web Insight	Fournit une visibilité sur les applications Web d'entreprise et permet une surveillance intégrée et en temps réel des applications.
Security Insight	Aide à évaluer l'état de sécurité des applications et à prendre des mesures correctives pour sécuriser les applications.
Gateway Insight	Fournit une visibilité sur les défaillances rencontrées par tous les utilisateurs, quel que soit le mode d'accès, au moment de la connexion à NetScaler Gateway.

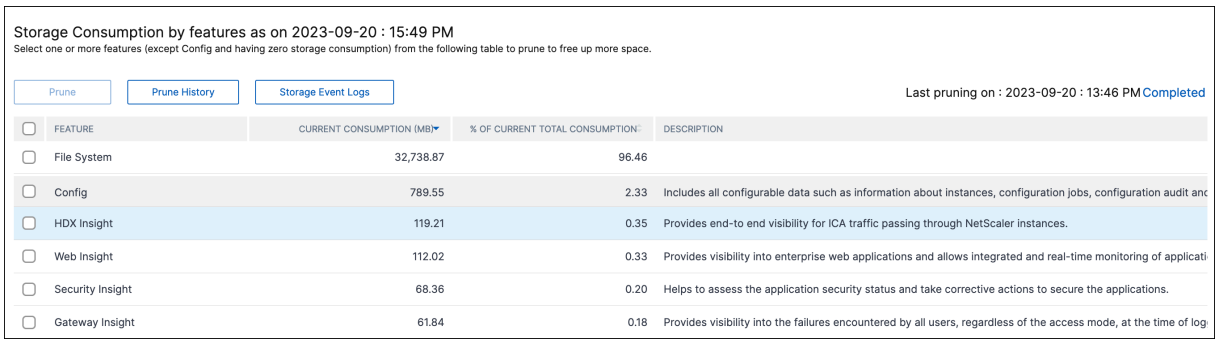
FONCTIONNALITÉ	DESCRIPTION
Événements	Surveillez et gérez les occurrences d'événements ou d'erreurs sur les instances NetScaler.
Tableau de bord des applications	Permet de visualiser et de gérer les applications.
Bot Insight	Fournit une visibilité sur les violations commises par les robots et les mesures prises à leur sujet.
Syslog	Surveille les événements Syslog générés sur les instances NetScaler si vous avez configuré votre appareil pour rediriger tous les messages Syslog vers NetScaler ADM.
Video Insight	Surveille les indicateurs des techniques d'optimisation vidéo utilisées par les instances NetScaler.
Transactions détaillées	Fournit une visibilité sur les transactions Web et affiche visuellement les mesures du temps de réponse réparties entre le client, NetScaler et le serveur.

Consommation de stockage par fonctionnalités

Pour en savoir plus sur la façon dont le stockage des données est réparti entre les différentes fonctionnalités, consultez la section « Consommation **de stockage par fonctionnalités », comme indiqué dans la section *dd mmm***.

La consommation de stockage par fonctionnalités, comme sur *ddmmm*, vous permet de comprendre :

- L'espace de stockage utilisé par les différentes fonctionnalités de NetScaler ADM
- Pourcentage d'espace utilisé par les fonctionnalités un jour donné



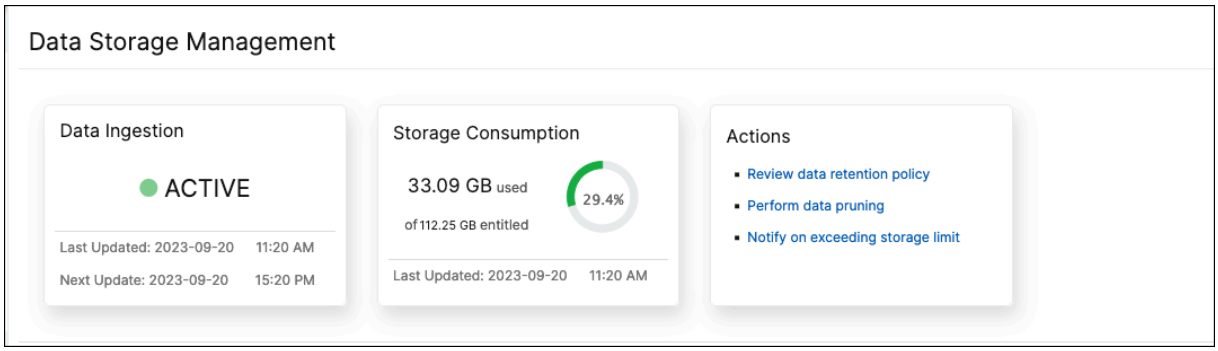
Si vous souhaitez trier les entrées du tableau, les en-têtes du tableau. NetScaler ADM trie le tableau de manière alphanumérique de haut en bas en fonction des données de la colonne choisie. Pour trier le tableau dans l'ordre inverse, cliquez à nouveau sur l'en-tête de colonne.

Pour plus d'informations sur le nettoyage de vos données, le nettoyage de l'historique et les journaux des événements de stockage, consultez la section Gérer votre stockage de données

Gérez votre espace de stockage

February 1, 2024

Vous pouvez utiliser le tableau de bord **de gestion du stockage des** données pour observer votre utilisation du stockage de données et prendre les mesures nécessaires pour libérer de l'espace ou augmenter l'espace de stockage lorsque votre stockage de données dépasse la limite autorisée.



La vignette **Actions** affiche la liste des étapes recommandées que vous pouvez suivre pour gérer votre capacité de stockage :

- Réviser la stratégie de conservation des données
- Effectuer le nettoyage des données
- Notifier en cas de dépassement de la limite de stockage

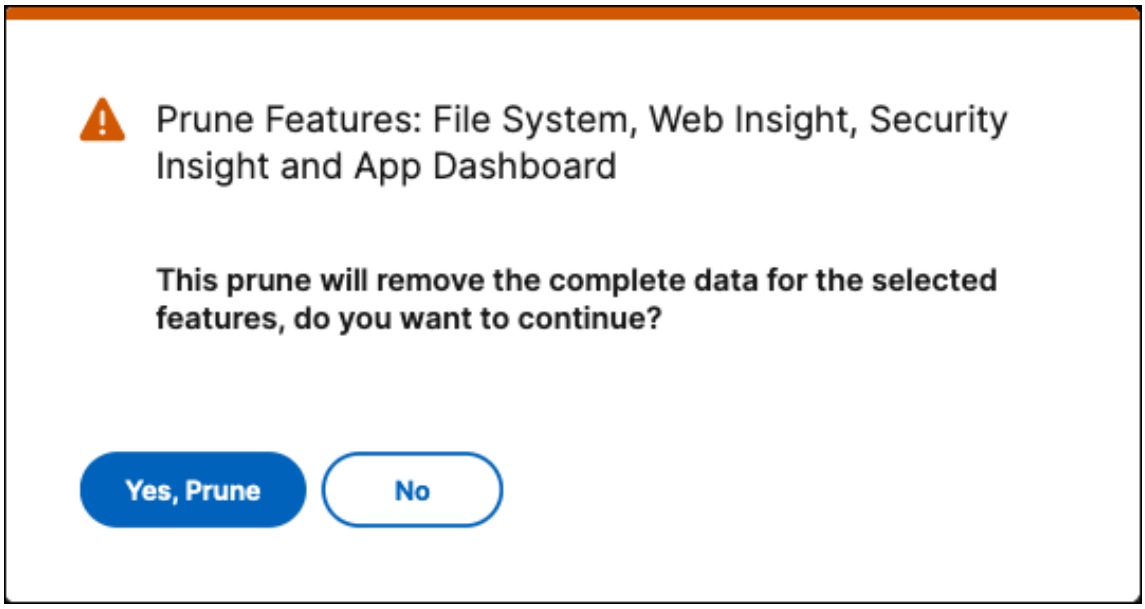
Effectuer le nettoyage des données

Élaguez vos données pour optimiser les ressources de stockage et obtenir plus d'espace de stockage. En plus de libérer de l'espace, le nettoyage des données améliore la qualité des données et accélère les temps de traitement. Nous vous recommandons de consulter et de purger les données inutiles à intervalles réguliers. Ce processus garantit que vos ressources sont utilisées judicieusement et que NetScaler ADM est agile et réactif.

Pour nettoyer vos données :

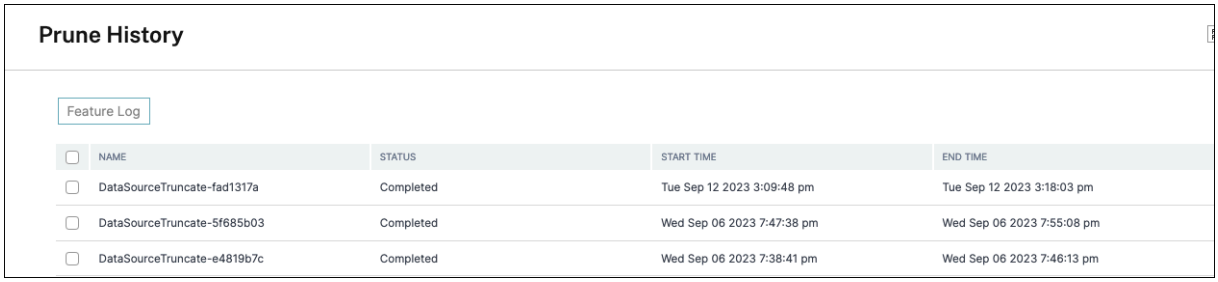
1. Sur la page **Gestion du stockage des données**, faites défiler la page vers le bas jusqu'à la section ***Consommation de stockage par fonctionnalités, comme sur yyyy-mm-dd*** .
2. Sélectionnez une ou plusieurs fonctionnalités et cliquez sur **Tailler**. Vous ne pouvez pas sélectionner **Config** car il inclut toutes les configurations du système.

   Une fenêtre contextuelle vous invite à confirmer si vous souhaitez supprimer toutes les données relatives aux fonctionnalités sélectionnées. Cliquez sur **Oui, Prune**.



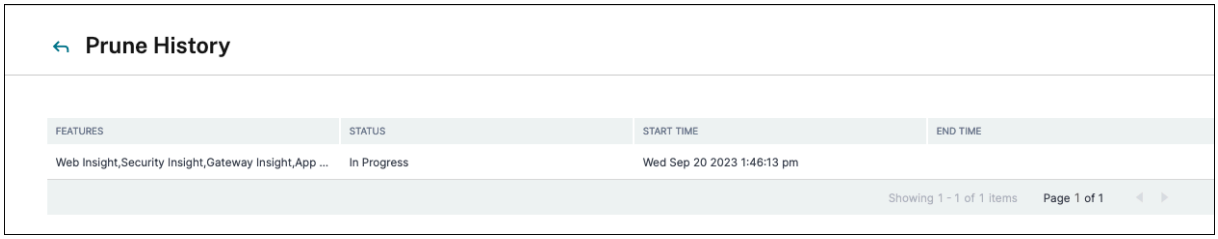
Afficher l'historique des pruneaux

Cliquez sur **Afficher l'historique des pruneaux** pour obtenir des détails sur toutes les activités de nettoyage que vous avez effectuées dans NetScaler ADM.



La page **Prune Logs : Task Logs** affiche la liste de toutes les tâches de nettoyage, y compris leur statut, leur heure de début et leur heure de fin respectifs.

Pour savoir quelles fonctionnalités ont été supprimées lors de chacune des opérations de nettoyage, sélectionnez une tâche et cliquez sur **Feature Log**.



Afficher les journaux des événements de stockage

Cliquez sur **Storage Event Logs** pour obtenir un aperçu de toutes les fois où vos données ont dépassé ou atteint 75 % de votre limite de licence.

Réviser la stratégie de conservation des données

La stratégie de conservation des données fait référence à un ensemble de règles et de configurations qui déterminent la manière dont NetScaler ADM gère et conserve les données historiques au fil du temps. Cette stratégie décrit la durée de conservation des données avant leur suppression automatique.

Si vous souhaitez réduire l'espace de stockage utilisé par les différentes fonctionnalités, vous pouvez modifier la durée de conservation des données dans NetScaler ADM.

Utilisez la page **Stratégie de conservation des données** pour modifier les paramètres de stockage des données pour :

- Messages d'événements
- Messages Syslog
- Données de reporting sur le réseau

Pour plus d'informations sur les paramètres de stockage des données, consultez la section Stratégie de conservation des données.

Signaler le dépassement de la limite de stockage

Vous pouvez configurer des notifications pour que NetScaler ADM vous envoie des alertes lorsque votre capacité de stockage de données dépasse les limites spécifiées.

Pour consulter et configurer les notifications de votre système :

1. Dans la vignette **Actions**, cliquez **sur Avertir en cas de dépassement de la limite de stockage**.
2. Sur la page **Configurer les notifications système**, sous la catégorie d'**événements système, assurez-vous que la catégorieDataStorageExceeded** est sélectionnée pour recevoir les notifications.

Vous pouvez définir différents paramètres relatifs à la manière et au moment où les notifications sont envoyées à vous ou à d'autres utilisateurs. Sélectionnez le mode de communication préféré (par exemple, e-mail, notifications Slack, PagerDuty et ServiceNow) et définissez les destinataires des notifications.

Pour plus d'informations sur la façon de configurer les profils et d'envoyer des notifications, voir Configurer les notifications.

Stratégie de rétention des données

February 1, 2024

Pour limiter la quantité de données de reporting stockées dans la base de données de votre serveur NetScaler ADM, vous pouvez spécifier l'intervalle pendant lequel vous souhaitez que NetScaler 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).

Pour configurer le paramètre de nettoyage du système :

1. Accédez à **Paramètres > Gestion du stockage des données > Stratégie de conservation des données**.
2. Sur la page **Data Pruning**, cliquez sur **Système.**
3. Sur la page **Système**, entrez les informations suivantes :
    - **Données à conserver (jours)** - Entrez le nombre de jours pendant lesquels les données doivent être conservées. Vous devez spécifier une valeur comprise entre 1 et 30.

- **Valeur seuil d'élagage des données (%)** - Entrez une limite de seuil (en pourcentage) à définir comme condition pour les processus d'élagage ou de nettoyage des données. Lorsque les données de la base de données atteignent ce pourcentage de capacité de stockage spécifié, des procédures de nettoyage des données sont déclenchées pour supprimer les données et libérer de l'espace.
- **Détails du découpage automatique** - Sélectionnez **Activer le découpage automatique des** données si vous souhaitez que le nettoyage des données commence lorsque l'un des critères suivants est satisfait :
  - La valeur de seuil de données spécifiée dans **Data Prune Threshold Value (%)** est atteinte.
  - Le nombre de jours spécifié dans la valeur **Données à conserver (jours)** est atteint.
- **Paramètre d'ingestion de données** - Entrez une limite de seuil (en pourcentage) à définir comme condition d'ingestion de données. Lorsque les données de la base de données atteignent ce pourcentage spécifié, l'activité d'ingestion de données est suspendue. Vous devez spécifier une limite comprise entre 50 % et 80 %.

4. Cliquez sur **Enregistrer** pour enregistrer les paramètres.

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 Syslog génériques sont supprimées de NetScaler ADM.

Pour configurer les paramètres de purge de syslog d'instance :

1. Accédez à **Paramètres > Gestion du stockage des données > Stratégie de conservation des données**.
2. Dans la page **Nettoyage des données**, cliquez sur **Événements d'instance**.
3. Dans le champ **Conserver les données génériques de Syslog**, spécifiez le nombre de jours compris entre 1 et 180.
4. Cliquez sur **Enregistrer**.

Configurer les paramètres de nettoyage d'événement d'instance

Pour limiter la quantité de données de messages d'événements stockées dans la base de données de votre serveur NetScaler ADM, vous pouvez spécifier l'intervalle pendant lequel vous souhaitez que NetScaler ADM conserve les données de reporting réseau, les événements, les journaux d'audit et les journaux de 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 **Paramètres > Gestion du stockage des données > Stratégie de conservation des données**.
2. Dans la page **Nettoyage des données**, cliquez sur **Événements d'instance**.
3. **Dans le champ**Données à conserver (jours)**, entrez l'intervalle de temps, en jours, pendant lequel vous souhaitez conserver les données sur le serveur NetScaler ADM et cliquez sur Enregistrer.**

Configurer les paramètres de nettoyage des rapports réseau

Pour limiter les données de reporting réseau stockées dans NetScaler ADM, vous pouvez spécifier l'intervalle pendant lequel vous souhaitez conserver les données historiques des rapports réseau.

Pour configurer les paramètres de nettoyage d'événement d'instance :

1. Accédez à **Paramètres > Gestion du stockage des données > Stratégie de conservation des données**.
2. Sur la page d'**élagage des données**, cliquez sur **Network Reporting**.
3. Dans le champ **Données à conserver (jours)**, spécifiez le nombre de jours compris entre 1 et 30.
4. Cliquez sur **Enregistrer**.

NetScaler ADM en tant que serveur proxy d'API

February 1, 2024

En plus de pouvoir recevoir des demandes d'API REST NITRO pour ses propres fonctionnalités de gestion et d'analyse, NetScaler Application Delivery Management (NetScaler ADM) peut fonctionner comme un serveur proxy d'API REST pour ses instances gérées. Au lieu d'envoyer des demandes d'API directement aux instances gérées, les clients de l'API REST peuvent envoyer les demandes d'API à NetScaler ADM. NetScaler ADM peut faire la différence entre les demandes d'API auxquelles il doit répondre et les demandes d'API qu'il doit transmettre sans modification à une instance gérée.

En tant que serveur proxy d'API, NetScaler ADM vous offre les avantages suivants :

- **Validation des demandes d'API**. NetScaler ADM valide toutes les demandes d'API par rapport aux stratégies de sécurité et de contrôle d'accès basées sur les rôles (RBAC) configurées.

NetScaler ADM tient également compte des locataires et garantit que l'activité des API ne dépasse pas les limites des locataires.

- **Audit centralisé**. NetScaler ADM tient à jour un journal d'audit de toutes les activités d'API liées à ses instances gérées.
- **Gestion de session**. NetScaler ADM évite aux clients d'API de devoir gérer des sessions avec des instances gérées.

Comment fonctionne NetScaler ADM en tant que serveur proxy d'API

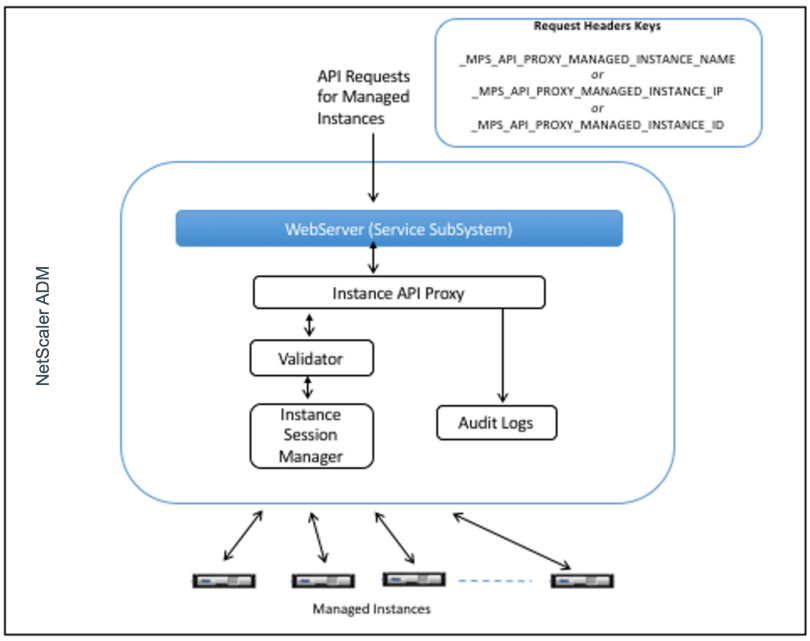
Lorsque vous souhaitez que NetScaler ADM transfère une demande à une instance gérée, vous configurez le client d'API pour inclure l'un des en-têtes HTTP suivants dans la demande d'API :

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 **Paramètres > 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 aide NetScaler ADM à identifier une demande d'API comme devant être transmise à une instance gérée. La valeur de l'en-tête aide NetScaler ADM à identifier l'instance gérée à laquelle il doit transmettre la demande.

Ce flux est représenté dans la figure suivante :



Comme le montre la figure ci-dessus, lorsque l'un de ces en-têtes HTTP apparaît dans une demande, NetScaler ADM traite la demande comme suit :

1. Sans modifier la demande, NetScaler ADM transmet la demande au moteur proxy de l'API de l'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, NetScaler ADM identifie une session gérée par le gestionnaire de session de l'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 **Paramètres > Administration**.
> 2. Dans **Configurations système**, sélectionnez **Système, Fuseau horaire, URL autorisées et Message du jour**.

Comment utiliser NetScaler ADM comme serveur proxy d'API

Les exemples suivants montrent les requêtes d'API REST qu'un client d'API envoie à un serveur NetScaler ADM dont l'adresse IP est 192.0.2.5. NetScaler ADM doit transmettre les demandes, sans modification, à une instance gérée dont l'adresse IP est 192.0.2.10. Tous les exemples utilisent l'en-tête _MPS_API_PROXY_MANAGED_INSTANCE_IP.

Avant d'envoyer les demandes d'API à NetScaler ADM, le client d'API doit :

- Connectez-vous à NetScaler 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-->
```

NetScaler ADM répond à la demande d'ouverture de session par 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 NetScaler ADM une demande d'API sous la forme suivante :

```
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 NetScaler ADM une demande d'API sous la forme suivante :

```
    POST /nitro/v1/config/lbvserver/sample_lbvserver
    Content-type: application/json
    Accept-type: application/json
    _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
    SESSID: ##
       D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D

    {

         "lbvserver":{

             "name":"sample_lbvserver",
             "servicetype":"HTTP",
             "ipv46":"10.102.1.11",
             "port":"80"
          }

     }

<!--NeedCopy-->
```

Exemple 3 : Modifier un serveur virtuel d'équilibrage de charge

Le client doit envoyer à NetScaler ADM une demande d'API sous la forme suivante :

```
    PUT /nitro/v1/config/lbvserver
    Content-type: application/json
    Accept-type: application/json
    _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
    SESSID: ##
       D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D

    {

       "lbvserver":{

            "name":"sample_lbvserver",
            "appflowlog":"DISABLED"
         }

     }

<!--NeedCopy-->
```


Exemple 4 : Suppression d'un serveur virtuel d'équilibrage de charge

Le client doit envoyer à NetScaler ADM une demande d'API sous la forme suivante :

```
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 NetScaler ADM une demande d'API sous la forme suivante :

```
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-->
```

FAQ

February 1, 2024

Cette section fournit la FAQ sur les fonctionnalités suivantes de NetScaler Application Delivery Management (NetScaler 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 NetScaler Gateway déployées en mode saut unique ?

Les données du canal virtuel EUEM font partie des données HDX Insight que NetScaler ADM reçoit des instances 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 NetScaler 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 puis-je permettre à NetScaler ADM de surveiller le trafic des applications Web et des postes de travail virtuels ?

1. Accédez à **Infrastructure** > **Instances** > **NetScaler** , puis sélectionnez l'instance NetScaler sur laquelle vous souhaitez activer les analyses.
2. Dans la liste **Sélectionner une action**, sélectionnez **Configurer Analytics**.
3. Sur la page **Configurer Analytics**, 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 NetScaler de la version 11.0, de la version 65.30 et des versions ultérieures, NetScaler ADM ne propose aucune option permettant d'activer Security Insight de manière explicite. Assurez-vous de configurer les paramètres AppFlow sur les instances NetScaler, afin que NetScaler ADM commence à recevoir le trafic Security Insight en même temps que le trafic Web Insight. Pour plus d'informations sur la façon de définir les paramètres AppFlow sur les instances NetScaler, voir Pour définir les paramètres AppFlow à l'aide de l'utilitaire deconfiguration.

Après avoir ajouté les instances NetScaler, NetScaler ADM commence-t-il automatiquement à collecter des informations analytiques ?

Non. Activez les analyses sur les serveurs virtuels hébergés dans les instances NetScaler gérées par NetScaler ADM. Pour plus de détails, consultez Comment activer Analytics sur les instances.

Est-il nécessaire d'accéder à l'appliance NetScaler individuelle pour activer les analyses ?

Non. Toutes les configurations sont effectuées à partir de l'interface utilisateur NetScaler ADM, qui répertorie les serveurs virtuels hébergés sur l'instance NetScaler spécifique. Pour plus de détails, consultez Comment activer Analytics sur les instances.

Quels sont les types de serveurs virtuels qui peuvent être répertoriés sur une instance NetScaler pour permettre l'analyse ?

Actuellement, l'interface utilisateur de NetScaler 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 connecter un disque supplémentaire à NetScaler ADM ?

Pour connecter un disque supplémentaire à NetScaler ADM :

1. Arrêtez la machine virtuelle NetScaler ADM.
2. Dans l'hyperviseur, connectez un disque supplémentaire de la taille requise à la machine virtuelle NetScaler ADM.

   Supposons, par exemple, que vous souhaitiez augmenter l'espace disque à 200 Go, dans une machine virtuelle NetScaler 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 connectés seront utilisés pour stocker les données de base de données et les fichiers journaux NetScaler 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 NetScaler ADM.

Qu'entendez-vous par « les collecteurs ne sont pas configurés sur les instances NetScaler » ?

Un collecteur reçoit les enregistrements AppFlow générés par l'appliance NetScaler.

NetScaler ADM reçoit le trafic Security Insight et Web Insight des instances NetScaler lorsque la fonctionnalité AppFlow est activée. Lorsque vous activez la fonctionnalité AppFlow sur une instance NetScaler, vous devez spécifier au moins un collecteur auquel les enregistrements AppFlow sont

envoyés. Si les collecteurs ne sont pas configurés sur les instances NetScaler, NetScaler ADM ne reçoit pas le trafic provenant des instances.

Par exemple, cinq instances NetScaler sont ajoutées à NetScaler ADM. Si aucun collecteur n'est spécifié pour deux instances, aucun trafic ne circule vers NetScaler 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 NetScaler ADM d'équilibrer la charge des demandes d'authentification qui sont dirigées vers les serveurs d'authentification externes. 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 NetScaler 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, consultezAuthentification 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, NetScaler ADM accède à la base de données utilisateur locale pour authentifier vos utilisateurs.

Dans NetScaler ADM, accédez à **Paramètres > 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 NetScaler 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 NetScaler ADM.

Pourquoi devons-nous attribuer des autorisations de groupe ?

Lorsque vous utilisez la fonctionnalité d'équilibrage de charge de NetScaler, vous pouvez intégrer NetScaler ADM à des serveurs d'authentification externes et importer des informations sur les groupes d'utilisateurs à partir des serveurs d'authentification. Connectez-vous à NetScaler ADM, créez manuellement les mêmes informations de groupe dans NetScaler ADM et attribuez des autorisations à ces groupes. Les autorisations des utilisateurs et des groupes d'utilisateurs sont gérées dans NetScaler ADM et non sur 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 NetScaler 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 que vous pouvez généralement

attribuer sont les autorisations permettant de gérer les instances NetScaler, les instances NetScaler SDX, les serveurs virtuels, etc., afin que les utilisateurs de ce groupe puissent gérer uniquement ces instances ou ces 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 fonctionnent toujours sur NetScaler ADM.

Gestion de la configuration

Puis-je effectuer une configuration sur plusieurs instances NetScaler simultanément à l'aide de NetScaler ADM ?

Oui, vous pouvez utiliser des tâches de configuration pour effectuer la configuration sur plusieurs instances NetScaler.

Que sont les tâches de configuration sur NetScaler 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 à la configuration entre les instances, répliquer les configurations sur plusieurs instances de votre réseau et enregistrer et exécuter des tâches de configuration à l'aide de l'interface graphique NetScaler ADM. Vous pouvez également convertir les tâches enregistrées en commandes CLI.

Vous pouvez utiliser la fonctionnalité Tâches de configuration de NetScaler ADM pour créer une tâche de configuration, envoyer des notifications par e-mail et consulter les journaux d'exécution des tâches créées.

Puis-je planifier des tâches à l'aide de modèles intégrés dans NetScaler 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 de certificats SSL de NetScaler ADM entraîne-t-elle la suppression de certificats d'instances NetScaler ?

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 NetScaler ADM depuis l'hyperviseur ou 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 NetScaler ADM, accédez à **Paramètres > Administration des utilisateurs > Utilisateurs**.

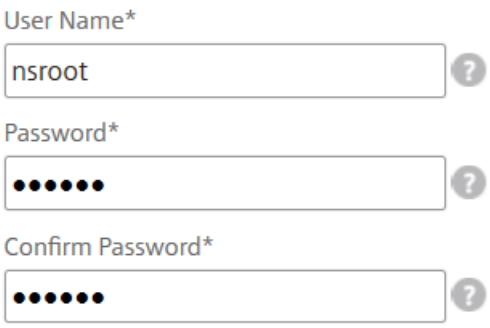
   La **page Utilisateurs** s'affiche.

2. Sélectionnez le nom d'utilisateur **nsroot** et cliquez sur **Modifier**.

   La page **Configurer l'utilisateur du 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 désormais utiliser le nouveau mot de passe pour vous connecter à partir de l'interface graphique, de l'hyperviseur 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 NetScaler ADM standalone et NetScaler ADM HA ?

NetScaler ADM standalone et NetScaler ADM HA prennent tous deux 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 NetScaler 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 **Paramètres > 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 NetScaler 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.

NetScaler ADM prend-il en charge le stockage SAN ?

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

NetScaler ADM prend-il en charge un disque supplémentaire ?

Oui. Une nouvelle installation de la paire NetScaler 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 **Paramètres > 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 **Paramètres > 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 ?

Le processeur AMD est pris en charge dans :

- **NetScaler ADM 13.1 build**4.43 ou version ultérieure.
- **Agent NetScaler ADM 13.1 build**17.42 ou version ultérieure.

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 NetScaler gérées à l'aide de NetScaler ADM ?

En tant qu'administrateur réseau, vous pouvez consulter des détails tels que les modifications de configuration, les conditions de connexion, les pannes matérielles, les violations des seuils et les modifications de l'état des entités sur vos instances NetScaler, ainsi que les événements et leur gravité sur des instances spécifiques. Vous pouvez utiliser le tableau de bord des événements NetScaler ADM pour consulter les rapports générés pour obtenir des informations détaillées sur la gravité des événements critiques sur toutes vos instances NetScaler.

Quelles sont les règles de l'événement ?

À l'aide de NetScaler ADM, vous pouvez configurer des règles pour surveiller des événements spécifiques. Les règles d'événements facilitent la surveillance de nombreux événements générés dans votre infrastructure NetScaler 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 NetScaler, 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 des interruptions SNMP depuis les instances NetScaler gérées vers NetScaler 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 une licence de capacité groupée NetScaler ?

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 groupées 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 NetScaler ADM ?

Un centre de données NetScaler ADM est un regroupement logique des instances NetScaler dans un emplacement géographique spécifique. Chaque serveur peut surveiller et gérer plusieurs instances NetScaler au sein d'un centre de données. Vous pouvez utiliser le serveur NetScaler ADM pour gérer des données telles que le syslog, le flux de trafic des applications et les interruptions SNMP provenant des instances gérées. Pour plus de détails sur la configuration des centres de données, consultez Comment configurer les centres de données pour les géomaps dans NetScaler ADM.

Quelles sont les différentes appliances NetScaler ADC prises en charge par NetScaler ADM ?

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

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler Gateway

Vous pouvez ajouter des instances lors de la première configuration du serveur NetScaler ADM ou ultérieurement.

Qu'est-ce qu'un profil d'instance ?

Un profil d'instance est utilisé par NetScaler 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 est le profil par défaut pour les instances NetScaler. Il contient les informations d'identification d'administrateur NetScaler 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.

Puis-je redécouvrir plusieurs instances NetScaler VPX dans NetScaler ADM ?

Oui, vous pouvez redécouvrir plusieurs instances Citrix **VPX** dans NetScaler ADM pour connaître les derniers états et configurations des instances.

****Accédez à **Infrastructure > Instances > NetScaler **VPX, sélectionnez les instances que vous souhaitez redécouvrir et, dans la liste des actions, cliquez sur Redécouvrir.**** Pour plus d'informations, consultez Comment redécouvrir plusieurs instances VPX.

NetScaler ADM peut-il être installé sur NetScaler SDX ?

Non

Puis-je ajouter une instance NetScaler 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 NetScaler 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 DR NetScaler ADM à l'aide de la console DR.

StyleBooks

Les StyleBooks peuvent-ils être utilisés pour configurer différentes instances NetScaler exécutées sur différentes versions du logiciel NetScaler ?

Oui, vous pouvez utiliser StyleBooks pour configurer différentes instances NetScaler s'exécutant sur différentes versions s'il n'y a aucune différence entre les commandes des différentes versions.

Lorsqu'un StyleBook est utilisé pour configurer plusieurs instances NetScaler en même temps et que la configuration d'une instance NetScaler échoue, que se passe-t-il ?

Si l'application de la configuration à une instance NetScaler échoue, la configuration n'est plus appliquée à d'autres instances et les configurations déjà appliquées sont annulées.

Les sauvegardes NetScaler effectuées via NetScaler incluent-elles des configurations appliquées via StyleBooks ?

Oui

Gestion du système

Puis-je attribuer un nom d'hôte à mon serveur NetScaler ADM ?

Oui, vous pouvez attribuer un nom d'hôte pour identifier votre serveur NetScaler ADM. Pour attribuer un nom d'hôte, accédez à **Système**> **Administration du système** > **Paramètres système**, puis cliquez sur **Modifier le nom d'hôte**.

Le nom d'hôte est affiché sur la licence universelle pour NetScaler ADM. Pour plus d'informations, consultez Comment attribuer un nom d'hôte à un serveur NetScaler ADM.

Puis-je sauvegarder et restaurer ma configuration NetScaler 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 NetScaler ADM devient instable, vous pouvez utiliser les fichiers sauvegardés pour restaurer votre NetScaler ADM à un état stable.

Pour sauvegarder et restaurer votre configuration NetScaler 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 NetScalerADM.

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 NetScaler ADM ?

Vous pouvez définir des seuils et des alertes pour surveiller l'état d'une instance NetScaler et surveiller les entités sur les instances gérées.

Lorsque la valeur d'un compteur dépasse le seuil, NetScaler 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 NetScaler ADM ?

Oui. Citrix vous recommande de générer une archive des données et des statistiques de NetScaler 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.

Vous pouvez générer un fichier de support technique contenant les journaux de débogage, la durée pendant laquelle les journaux de débogage ont été collectés et des journaux distincts et divers à partir de la base de données NetScaler 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 NetScalerADM.

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, les données AppFirewall et les données NetScaler Gateway seront supprimées de NetScaler ADM.

Puis-je configurer le serveur NTP sur NetScaler ADM ?

Vous pouvez configurer un serveur NTP (Network Time Protocol) dans NetScaler ADM pour synchroniser l'horloge de NetScaler ADM avec le serveur NTP. La configuration d'un serveur NTP garantit que l'horloge NetScaler 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 un serveur NTP sur NetScalerADM.

À partir de quelle version le déploiement HA actif-passif de NetScaler ADM est-il pris en charge ?

Le mode de déploiement HA actif-passif de NetScaler ADM est pris en charge à partir de NetScaler ADM version 12.0 build 51.24.

J'avais une configuration HA active-active NetScaler ADM et j'avais configuré une appliance NetScaler avec un serveur virtuel d'équilibrage de charge pour un accès unifié à l'interface graphique. Comment mettre à jour cette configuration ?

Après avoir mis à niveau la paire NetScaler ADM HA vers le mode actif-passif, vous devez exécuter la commande suivante sur l'appliance NetScaler pour mettre à jour la configuration d'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 NetScaler ADM HA sur une instance NetScaler à l'aide du port 443 ?

Non, vous ne pouvez pas configurer l'équilibrage de charge de la paire NetScaler ADM HA sur une instance NetScaler à l'aide du port 443.

Lorsque vous configurez les moniteurs `http-ecv` et `https-ecv` sur NetScaler, celui-ci ne surveille pas correctement les nœuds NetScaler ADM HA.

Un fichier de sauvegarde du serveur NetScaler ADM peut-il être utilisé pour restaurer la configuration d'un autre serveur NetScaler ADM ?

Oui

Une fois que NetScaler ADM a sauvegardé une instance NetScaler, ce fichier de sauvegarde peut-il être utilisé pour restaurer la configuration d'une autre instance NetScaler via NetScaler ADM ?

Oui. Téléchargez le fichier de sauvegarde NetScaler ADM, chargez-le dans le référentiel de sauvegarde d'une autre instance NetScaler 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 NetScaler que celles qui ont été sauvegardées.

Avant de restaurer une instance dans une paire haute disponibilité, assurez-vous que les adresses IP et l'état (principal ou secondaire) stockés dans le fichier de sauvegarde correspondent à ceux de la configuration HA d'origine. Vérifiez également que le nouveau principal et le nouveau secondaire possèdent le même type de licence NetScaler.

Pouvons-nous forcer NetScaler ADM à utiliser une adresse SNIP pour communiquer avec les instances NetScaler, au lieu d'utiliser l'adresse NSIP du serveur NetScaler ADM ?

Oui, vous pouvez ajouter une adresse SNIP (avec la gestion activée) dans NetScaler ADM pour communiquer avec les instances NetScaler.

Lorsque je sauvegarde des instances NetScaler dans NetScaler ADM, le résultat est-il une sauvegarde complète ou une sauvegarde de base ?

Les sauvegardes des instances NetScaler effectuées par NetScaler ADM sont des sauvegardes complètes.

Existe-t-il un guide de dépannage pour NetScaler ADM ?

Oui. Voir https://support.citrix.com/article/CTX224502.

Comment les instances NetScaler sont-elles gérées en cas de basculement de NetScaler 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 NetScaler sont mises à jour avec les derniers détails du nœud principal en tant que destination des interruptions SNMP par défaut.

Le nouveau nœud NetScaler ADM principal (actif) vérifie si le nœud précédemment actif a été configuré en tant que collecteur AppFlow ou serveur syslog. Si c'était le cas, le nouveau nœud 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 NetScaler ADM HA qui est tombé en panne revient ?

Après la remise en service, le nœud NetScaler ADM reste passif à moins que le nœud actif ne bascule

Comment les instances NetScaler sont-elles réparties entre les nœuds NetScaler ADM HA ?

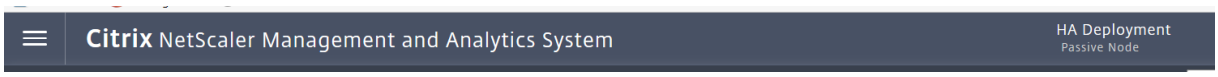
Toutes les instances NetScaler sont gérées par le nœud NetScaler ADM principal.

Comment les licences de serveur virtuel sont-elles gérées en cas de basculement de NetScaler ADM HA ?

Si le nœud principal NetScaler 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 NetScaler.

Un équilibreur de charge est-il obligatoire pour une configuration NetScaler ADM HA ?

Non, mais s'il n'y a pas d'équilibreur de charge, les nœuds NetScaler ADM doivent être accessibles via leurs propres adresses IP. Le nœud passif est marqué par la balise « Passif » et Citrix recommande de ne créer aucune configuration sur le nœud passif.



NetScaler ADM prend-il en charge une base de données externe ?

Non

Une instance NetScaler gérée par NetScaler ADM peut-elle être utilisée comme équilibreur de charge pour NetScaler ADM HA ?

Oui

Quelles données sont synchronisées entre les nœuds NetScaler ADM HA ?

La base de données NetScaler 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/