



# NetScaler Application Delivery Management 12.1

Machine translated content

## Disclaimer

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

## Contents

<b>Notes de publication</b>	<b>14</b>
<b>Mise en route</b>	<b>16</b>
<b>Liste des articles pratiques</b>	<b>20</b>
<b>Vue d'ensemble</b>	<b>25</b>
<b>Caractéristiques et solutions</b>	<b>26</b>
<b>Architecture</b>	<b>29</b>
<b>Comment Citrix ADM découvre des instances</b>	<b>30</b>
<b>Vue d'ensemble de l'interrogation</b>	<b>32</b>
<b>Gouvernance des données</b>	<b>42</b>
<b>Licences</b>	<b>44</b>
<b>Configuration système requise</b>	<b>55</b>
<b>Déployer</b>	<b>63</b>
<b>Conditions préalables à l'installation de Citrix ADM</b>	<b>64</b>
<b>Citrix ADM avec Citrix Hypervisor</b>	<b>65</b>
<b>Citrix ADM avec Microsoft Hyper-V</b>	<b>68</b>
<b>Citrix ADM avec VMware ESXi</b>	<b>74</b>
<b>Citrix ADM avec serveur KVM Linux</b>	<b>79</b>
<b>Configurer le déploiement haute disponibilité</b>	<b>85</b>
<b>Configurer la reprise après sinistre pour une haute disponibilité</b>	<b>101</b>
<b>Configurer les agents sur site pour un déploiement multisite</b>	<b>109</b>
<b>Migrer le déploiement d'un serveur unique Citrix ADM vers un déploiement haute disponibilité</b>	<b>119</b>
<b>Migrer de NetScaler Insight Center vers Citrix ADM</b>	<b>124</b>



<b>Migrer les configurations du Command Center vers Citrix ADM</b>	<b>126</b>
<b>Intégrer Citrix ADM avec Citrix Director</b>	<b>134</b>
<b>Joindre un disque supplémentaire à Citrix ADM</b>	<b>136</b>
<b>Configurer</b>	<b>149</b>
<b>Ajouter des instances à Citrix ADM</b>	<b>150</b>
<b>Ajouter des instances Citrix ADC VPX déployées dans le cloud à Citrix ADM</b>	<b>157</b>
<b>Activer les analyses sur les serveurs virtuels</b>	<b>159</b>
<b>Configurer le serveur NTP</b>	<b>163</b>
<b>Configurer les paramètres système</b>	<b>164</b>
<b>Mettre à niveau</b>	<b>167</b>
<b>Authentification</b>	<b>180</b>
<b>Comment extraire un groupe de serveurs d'authentification</b>	<b>189</b>
<b>Ajouter un serveur d'authentification LDAP</b>	<b>193</b>
<b>Comment activer l'authentification locale de secours</b>	<b>195</b>
<b>Comment ajouter des serveurs d'authentification RADIUS</b>	<b>197</b>
<b>Comment ajouter des serveurs d'authentification TACACS</b>	<b>200</b>
<b>Comment monter en cascade des serveurs d'authentification externes</b>	<b>201</b>
<b>Contrôle d'accès</b>	<b>203</b>
<b>Contrôle d'accès sur rôle</b>	<b>203</b>
<b>Configurer les stratégies d'accès</b>	<b>206</b>
<b>Configurer les groupes</b>	<b>210</b>
<b>Configurer les rôles</b>	<b>214</b>
<b>Configurer les utilisateurs</b>	<b>216</b>
<b>Multilocation : offrez un environnement de gestion exclusif à vos locataires</b>	<b>218</b>

<b>Applications</b>	<b>227</b>
<b>Analyse des performances des applications</b>	<b>239</b>
<b>Analyse de la sécurité des applications</b>	<b>242</b>
<b>Créer une définition d'application</b>	<b>242</b>
<b>Créer un seuil et une alerte pour l'analyse des applications</b>	<b>249</b>
<b>StyleBooks</b>	<b>250</b>
<b>Groupes StyleBook</b>	<b>253</b>
<b>Importation et synchronisation de StyleBooks à partir d'un référentiel GitHub</b>	<b>259</b>
<b>Utiliser les StyleBooks par défaut</b>	<b>261</b>
<b>Masquer tous les StyleBooks par défaut</b>	<b>264</b>
<b>StyleBook Google Apps SSO</b>	<b>266</b>
<b>SSO Office 365 StyleBook</b>	<b>270</b>
<b>StyleBook Microsoft Skype for Business</b>	<b>279</b>
<b>StyleBook Microsoft Exchange</b>	<b>288</b>
<b>Microsoft SharePoint StyleBook</b>	<b>291</b>
<b>StyleBook proxy Microsoft ADFS</b>	<b>301</b>
<b>StyleBook Oracle e-business</b>	<b>319</b>
<b>Créer et utiliser des StyleBooks personnalisés</b>	<b>321</b>
<b>StyleBook pour créer un serveur virtuel d'équilibrage de charge</b>	<b>324</b>
<b>StyleBook pour créer une configuration d'équilibrage de charge de base</b>	<b>331</b>
<b>Créer un StyleBook composite</b>	<b>338</b>
<b>Utiliser les attributs de l'interface graphique dans un StyleBook personnalisé</b>	<b>341</b>
<b>Utiliser des StyleBooks personnalisés</b>	<b>342</b>
<b>Créer un StyleBook pour charger des fichiers vers Citrix ADM</b>	<b>347</b>

<b>Créer un StyleBook pour charger des fichiers de certificat SSL et de clé de certificat vers Citrix ADM</b>	<b>350</b>
<b>Activer l'analyse et configurer les alarmes sur un serveur virtuel défini dans un StyleBook</b>	<b>356</b>
<b>Rôles d'instance</b>	<b>358</b>
<b>Créer un StyleBook pour effectuer des opérations non CRUD</b>	<b>366</b>
<b>Utiliser l'API pour créer des configurations à partir de StyleBooks</b>	<b>367</b>
<b>Utiliser l'API pour créer des configurations pour charger des fichiers de certificat et de clé</b>	<b>375</b>
<b>Utiliser l'API pour créer des configurations pour télécharger n'importe quel type de fichier</b>	<b>377</b>
<b>Utiliser l'API pour importer des StyleBooks personnalisés</b>	<b>378</b>
<b>Utiliser l'API pour télécharger des StyleBooks personnalisés</b>	<b>380</b>
<b>Utiliser l'API pour supprimer des StyleBooks personnalisés</b>	<b>381</b>
<b>Grammaire de StyleBooks</b>	<b>383</b>
<b>En-tête</b>	<b>385</b>
<b>Importer des StyleBooks</b>	<b>386</b>
<b>Paramètres</b>	<b>387</b>
<b>Parameters-default-sources construct</b>	<b>398</b>
<b>Substitutions</b>	<b>400</b>
<b>Composants</b>	<b>406</b>
<b>Composants d'assistance</b>	<b>407</b>
<b>Propriétés facultatives</b>	<b>409</b>
<b>Properties-Default-Sources, construction</b>	<b>410</b>
<b>Composants imbriqués</b>	<b>412</b>
<b>Conditionner la construction</b>	<b>414</b>
<b>Construction repeat</b>	<b>415</b>

<b>Construction repeat-condition</b>	<b>417</b>
<b>Répétitions imbriquées</b>	<b>418</b>
<b>Sorties</b>	<b>419</b>
<b>Référence des paramètres</b>	<b>420</b>
<b>Référence parent</b>	<b>421</b>
<b>Référence des composants</b>	<b>422</b>
<b>Référence des substitutions</b>	<b>423</b>
<b>Référence de variable</b>	<b>424</b>
<b>Opérations</b>	<b>425</b>
<b>Analytics</b>	<b>427</b>
<b>Alarmes</b>	<b>429</b>
<b>Expressions</b>	<b>432</b>
<b>Interpolations sur place</b>	<b>436</b>
<b>Fonctions intégrées</b>	<b>440</b>
<b>Détection des dépendances</b>	<b>450</b>
<b>Gestion des instances</b>	<b>452</b>
<b>Surveiller les sites distribués à l'échelle mondiale</b>	<b>454</b>
<b>Comment créer des balises et affecter des instances</b>	<b>460</b>
<b>Procédure de recherche d'instances à l'aide de valeurs de balises et de propriétés</b>	<b>463</b>
<b>Gérer les partitions d'administration des instances Citrix ADC</b>	<b>466</b>
<b>Sauvegarder et restaurer des instances Citrix ADC</b>	<b>471</b>
<b>Forcer un basculement sur incident à l'instance secondaire Citrix ADC</b>	<b>478</b>
<b>Forcer une instance Citrix ADC secondaire à rester secondaire</b>	<b>479</b>
<b>Créer des groupes d'instances</b>	<b>480</b>

<b>Redécouvrir plusieurs instances Citrix VPX</b>	<b>481</b>
<b>Annuler l'administration d'une instance</b>	<b>482</b>
<b>Tracer la route jusqu'à une instance</b>	<b>482</b>
<b>Événements</b>	<b>484</b>
<b>Utiliser le tableau de bord des événements</b>	<b>484</b>
<b>Définir l'âge de l'événement pour les événements</b>	<b>486</b>
<b>Planifier un filtre d'événement</b>	<b>487</b>
<b>Définir des notifications par e-mail répétées pour les événements</b>	<b>489</b>
<b>Suppression d'événements</b>	<b>491</b>
<b>Créer des règles d'événement</b>	<b>492</b>
<b>Modifier la gravité signalée des événements qui se produisent sur les instances Citrix ADC</b>	<b>504</b>
<b>Afficher le résumé des événements</b>	<b>505</b>
<b>Afficher les sévérité des événements et les détails des interruptions SNMP</b>	<b>506</b>
<b>Exporter les messages syslog</b>	<b>509</b>
<b>Supprimer les messages Syslog</b>	<b>512</b>
<b>Configurer les paramètres de nettoyage pour les événements d'instance</b>	<b>514</b>
<b>Tableau de bord SSL</b>	<b>515</b>
<b>Utiliser le tableau de bord SSL</b>	<b>516</b>
<b>Configurer les notifications pour l'expiration du certificat SSL</b>	<b>520</b>
<b>Mettre à jour un certificat installé</b>	<b>521</b>
<b>Installer des certificats SSL sur une instance Citrix ADC</b>	<b>522</b>
<b>Créer une demande de signature de certificat (CSR)</b>	<b>524</b>
<b>Lier et dissocier les certificats SSL</b>	<b>526</b>
<b>Configurer une stratégie d'entreprise</b>	<b>527</b>

<b>Interroger les certificats SSL à partir d'instances Citrix ADC</b>	<b>527</b>
<b>Tâches de configuration</b>	<b>529</b>
<b>Créer une tâche de configuration</b>	<b>531</b>
<b>Utiliser l'enregistrement et la lecture pour créer des tâches de configuration</b>	<b>533</b>
<b>Utiliser les tâches de configuration pour répliquer la configuration d'une instance vers plusieurs instances</b>	<b>538</b>
<b>Utiliser des variables dans les tâches de configuration</b>	<b>542</b>
<b>Créer des tâches de configuration à partir de commandes correctives</b>	<b>548</b>
<b>Répliquez la configuration en cours et enregistrée d'une instance NetScaler vers une autre</b>	<b>550</b>
<b>Réutiliser les tâches de configuration exécutées</b>	<b>552</b>
<b>Planifier les tâches créées à l'aide de modèles intégrés</b>	<b>553</b>
<b>Utiliser les tâches de maintenance pour mettre à niveau les instances NetScaler SDX</b>	<b>556</b>
<b>Création de tâches de configuration pour les instances Citrix SD-WAN WANOP</b>	<b>557</b>
<b>Utiliser le modèle de configuration maître</b>	<b>563</b>
<b>Utiliser les tâches pour mettre à niveau les instances de Citrix ADC</b>	<b>570</b>
<b>Utiliser des modèles de configuration pour créer des modèles d'audit</b>	<b>575</b>
<b>Utiliser la commande SCP (put) dans les tâches de configuration</b>	<b>578</b>
<b>Replanifier les tâches configurées à l'aide de modèles intégrés</b>	<b>582</b>
<b>Réutiliser les modèles d'audit de configuration dans les tâches de configuration</b>	<b>582</b>
<b>Importer et exporter des modèles de configuration</b>	<b>586</b>
<b>Tâches de maintenance</b>	<b>588</b>
<b>Audit de configuration</b>	<b>600</b>
<b>Créer des modèles d'audit</b>	<b>600</b>
<b>Afficher les rapports d'audit</b>	<b>605</b>

<b>Modifications de configuration d'audit entre les instances</b>	<b>608</b>
<b>Obtenir des conseils de configuration sur la configuration du réseau</b>	<b>613</b>
<b>Audit de configuration d'interrogation des instances Citrix ADC</b>	<b>615</b>
<b>Générer un diff d'audit de configuration pour les interruptions SNMP ConfigChange</b>	<b>617</b>
<b>Fonctions réseau</b>	<b>618</b>
<b>Générer des rapports pour les entités d'équilibrage de charge</b>	<b>618</b>
<b>Exporter ou planifier l'exportation des rapports sur les fonctions réseau</b>	<b>622</b>
<b>Rapports sur le réseau</b>	<b>625</b>
<b>Analytics</b>	<b>636</b>
<b>Exigences en matière de licence</b>	<b>638</b>
<b>Vue d'ensemble de Logstream</b>	<b>639</b>
<b>Désactiver la collecte de données d'URL</b>	<b>643</b>
<b>Créer des seuils et des alertes</b>	<b>644</b>
<b>Configurer des seuils adaptatifs</b>	<b>645</b>
<b>Configurer la persistance de la base de données</b>	<b>645</b>
<b>Diagnostics en libre-service pour Analytics</b>	<b>647</b>
<b>Web Insight</b>	<b>650</b>
<b>HDX Insight</b>	<b>677</b>
<b>Activation de la collecte de données HDX Insight</b>	<b>684</b>
<b>Activer la collecte de données pour les appliances Citrix Gateway déployées en mode à saut unique</b>	<b>698</b>
<b>Activez la collecte de données pour surveiller les ADC NetScaler déployés en mode transparent</b>	<b>699</b>
<b>Activer la collecte de données pour les appliances Citrix Gateway déployées en mode double saut</b>	<b>702</b>

<b>Activez la collecte de données pour surveiller les ADC NetScaler déployés en mode utilisateur LAN</b>	<b>707</b>
<b>Créer des seuils et configurer des alertes pour HDX Insight</b>	<b>711</b>
<b>Affichage des rapports et des mesures HDX Insight</b>	<b>715</b>
<b>Rapports et mesures d’affichage des applications</b>	<b>761</b>
<b>Rapports et mesures d’affichage du Bureau</b>	<b>769</b>
<b>Afficher les rapports et les mesures de l’utilisateur</b>	<b>782</b>
<b>Rapports et mesures d’affichage d’instance</b>	<b>799</b>
<b>Rapports et mesures d’affichage des licences</b>	<b>806</b>
<b>Résoudre les problèmes HDX Insight</b>	<b>807</b>
<b>Gateway Insight</b>	<b>821</b>
<b>Résoudre les problèmes liés à Gateway Insight</b>	<b>839</b>
<b>Security Insight</b>	<b>842</b>
<b>SSL Insight</b>	<b>862</b>
<b>TCP Insight</b>	<b>872</b>
<b>WAN Insight</b>	<b>877</b>
<b>Video Insight</b>	<b>881</b>
<b>Afficher l’efficacité du réseau</b>	<b>884</b>
<b>Comparer le volume de données utilisé par les vidéos ABR optimisées et non optimisées</b>	<b>885</b>
<b>Afficher le type de vidéos diffusées en continu et le volume de données consommé à partir de votre réseau</b>	<b>887</b>
<b>Comparer le temps de lecture optimisé et non optimisé des vidéos ABR</b>	<b>890</b>
<b>Comparer la consommation de bande passante des vidéos ABR optimisées et non optimisées</b>	<b>893</b>
<b>Comparer le nombre optimisé et non optimisé de lectures de vidéos ABR</b>	<b>895</b>
<b>Afficher le débit de données de pointe pour une période spécifique</b>	<b>898</b>



<b>Analyse de Secure Web Gateway</b>	<b>901</b>
<b>Tableaux de bord</b>	<b>902</b>
<b>Cas d'utilisation</b>	<b>908</b>
<b>Orchestration</b>	<b>920</b>
<b>OpenStack : intégrer des instances Citrix ADC</b>	<b>922</b>
<b>Conditions préalables</b>	<b>926</b>
<b>Tâches de pré-configuration dans Citrix ADM et OpenStack</b>	<b>927</b>
<b>Configurer LBaaS V1 à l'aide d'Horizon</b>	<b>938</b>
<b>Configurer LBaaS V2 à l'aide de la ligne de commande</b>	<b>939</b>
<b>Configurer la commutation de contenu de couche 7</b>	<b>944</b>
<b>Provisioning manuel de l'instance Citrix ADC VPX sur OpenStack</b>	<b>952</b>
<b>Provisionnement de l'instance Citrix ADC VPX sur OpenStack à l'aide de StyleBook</b>	<b>954</b>
<b>Prise en charge des licences d'enregistrement et de récupération VPX et des licences groupées pour l'environnement OpenStack</b>	<b>956</b>
<b>Prise en charge du VLAN partagé pour les partitions d'administration</b>	<b>959</b>
<b>Flux de travail de licence d'essai</b>	<b>962</b>
<b>Intégration avec les services OpenStack Heat</b>	<b>963</b>
<b>Stratégies d'isolement des packages de services</b>	<b>969</b>
<b>Attribution de périphériques flexible basée sur des règles</b>	<b>972</b>
<b>NSX Manager : Provisioning manuel des instances Citrix ADC</b>	<b>977</b>
<b>NSX Manager : Provisioning automatique des instances Citrix ADC</b>	<b>994</b>
<b>Automatisation Citrix ADC à l'aide de Citrix ADM en mode hybride ACI Cisco</b>	<b>1006</b>
<b>Conditions préalables</b>	<b>1009</b>
<b>Configurer Citrix ADC en mode hybride à l'aide de Cisco APIC et Citrix ADM</b>	<b>1010</b>

<b>Créer un StyleBook pour une application à l'aide de Citrix ADM</b>	<b>1010</b>
<b>Importer le package de périphériques en mode hybride Citrix ADC dans Cisco APIC</b>	<b>1011</b>
<b>Ajouter Citrix ADM en tant que gestionnaire de périphériques dans Cisco APIC</b>	<b>1013</b>
<b>Ajouter Citrix ADC en tant que périphérique dans Cisco ACI à l'aide d'APIC</b>	<b>1017</b>
<b>Créer et déployer un graphique de service</b>	<b>1021</b>
<b>Configurer les paramètres L4-L7 à partir de Citrix ADM à l'aide de StyleBook</b>	<b>1031</b>
<b>Attacher et détacher les événements de point de terminaison d'APIC</b>	<b>1036</b>
<b>Rapports d'erreurs APIC</b>	<b>1037</b>
<b>Journaux générés par Citrix ADM</b>	<b>1037</b>
<b>Journaux générés par le package de périphériques en mode hybride</b>	<b>1042</b>
<b>Package de périphériques Citrix ADC en mode Cloud Orchestrator de Cisco ACI</b>	<b>1046</b>
<b>Capacité du pool de Citrix ADC</b>	<b>1051</b>
<b>Configurer la capacité du pool de Citrix ADC</b>	<b>1057</b>
<b>Mettre à niveau une licence perpétuelle dans Citrix ADC MPX vers Citrix ADC Pooled Capacity</b>	<b>1068</b>
<b>Mettre à niveau une licence perpétuelle dans un SDX Citrix ADC vers une capacité groupée Citrix ADC</b>	<b>1077</b>
<b>Capacité mise en commun Citrix ADC sur les instances Citrix ADC en mode cluster</b>	<b>1079</b>
<b>Contrôle de l'intégrité</b>	<b>1082</b>
<b>Comportements attendus lorsque des problèmes surviennent</b>	<b>1084</b>
<b>Configurer les contrôles d'expiration pour les licences de capacité du pool</b>	<b>1085</b>
<b>Licence d'enregistrement et de départ Citrix ADC VPX</b>	<b>1086</b>
<b>Licences de processeur virtuel Citrix ADC</b>	<b>1095</b>
<b>Gérer les instances Citrix SD-WAN</b>	<b>1100</b>
<b>Ajouter des instances Citrix SD-WAN</b>	<b>1104</b>

<b>Afficher les données d'analyse Citrix SD-WAN pour un déploiement multi-sauts</b>	<b>1109</b>
<b>Voir les rapports d'événements des instances de Citrix SD-WAN WANOP</b>	<b>1112</b>
<b>Afficher les rapports réseau des instances de Citrix SD-WAN WANOP</b>	<b>1113</b>
<b>Sauvegarder les instances de Citrix SD-WAN WANOP</b>	<b>1115</b>
<b>Gérer les instances HaProxy</b>	<b>1123</b>
<b>Ajouter des instances HAProxy à Citrix ADM</b>	<b>1123</b>
<b>Tableau de bord de l'application HaProxy</b>	<b>1127</b>
<b>Licences tierces</b>	<b>1132</b>
<b>Contrôle d'accès basé sur les rôles pour les instances HaProxy</b>	<b>1135</b>
<b>Surveiller les instances HaProxy</b>	<b>1136</b>
<b>Afficher les détails des frontends configurés sur les instances HaProxy</b>	<b>1136</b>
<b>Afficher les détails des backends configurés sur les instances HaProxy</b>	<b>1137</b>
<b>Afficher les détails des serveurs configurés sur les instances HaProxy</b>	<b>1138</b>
<b>Afficher les instances HaProxy avec le plus grand nombre de frontends ou de serveurs</b>	<b>1139</b>
<b>Redémarrer une instance HAProxy</b>	<b>1140</b>
<b>Sauvegarder et restaurer une instance HaProxy</b>	<b>1141</b>
<b>Modifier le fichier de configuration HaProxy</b>	<b>1142</b>
<b>Gérer les paramètres système</b>	<b>1144</b>
<b>Configurer les paramètres de sauvegarde du système</b>	<b>1151</b>
<b>Configurer un serveur NTP</b>	<b>1152</b>
<b>Mettre à niveau Citrix ADM</b>	<b>1154</b>
<b>Comment réinitialiser le mot de passe pour Citrix ADM</b>	<b>1155</b>
<b>Configurer l'intervalle de purge de syslog</b>	<b>1162</b>
<b>Configurer les paramètres de nettoyage du système</b>	<b>1163</b>

<b>Activer l'accès shell pour les utilisateurs non par défaut</b>	<b>1165</b>
<b>Récupérer des serveurs Citrix ADM inaccessibles</b>	<b>1166</b>
<b>Attribuer un nom d'hôte à un serveur Citrix ADM</b>	<b>1172</b>
<b>Sauvegarder et restaurer votre serveur Citrix ADM</b>	<b>1172</b>
<b>Afficher les informations d'audit</b>	<b>1176</b>
<b>Configurer les paramètres SSL</b>	<b>1178</b>
<b>Surveiller l'utilisation du processeur, de la mémoire et du disque</b>	<b>1179</b>
<b>Configurer les paramètres de notification système</b>	<b>1180</b>
<b>Générer un fichier de support technique</b>	<b>1183</b>
<b>Configurer un groupe de chiffrement</b>	<b>1185</b>
<b>Créer une destination d'interruptions SNMP, une communauté de gestionnaires et des utilisateurs</b>	<b>1186</b>
<b>Configurer et afficher les alarmes système</b>	<b>1187</b>
<b>Citrix ADM en tant que serveur proxy API</b>	<b>1189</b>
<b>FAQ</b>	<b>1194</b>

## Notes de publication

February 1, 2024

Les notes de mise à jour de Citrix Application Delivery Management (ADM) 12.1 décrivent les nouvelles fonctionnalités, les améliorations apportées aux fonctionnalités existantes et les problèmes connus d'une version. La section des notes de version de la version 12.1 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.

Pour afficher le document complet des notes de publication, cliquez sur le lien suivant.

---

Notes de publication	Date de publication	Version
<a href="#">Notes de version pour la version 62.21 de Citrix ADM 12.1 Release</a>	Date de publication : 13 mai 2021	Version de la note de publication : 1.0
<a href="#">Notes de version pour la version 61.18 de la version 12.1 de Citrix ADM</a>	Publié le 4 février 2021	Version de la note de publication : 1.0
<a href="#">Notes de publication pour la version 60.16 de la version 12.1 de Citrix ADM</a>	Publié le : 6 novembre 2020	Version de la note de publication : 1.0
<a href="#">Notes de publication pour la version 59.16 de Citrix ADM 12.1</a>	Publié le : 28 septembre 2020	Version de la note de publication : 1.0
<a href="#">Notes de publication pour la version 58.14 de la version 12.1 de Citrix ADM</a>	Publié le : 20 août 2020	Version de la note de publication : 1.0
<a href="#">Notes de publication pour la version 57.18 de la version 12.1 de Citrix ADM</a>	Publié le : 11 juin 2020	Version de la note de publication : 1.0
<a href="#">Notes de publication pour la version 56.22 de la version 12.1 de Citrix ADM</a>	Date de publication : 30 mars 2020	Version de la note de publication : 1.0

Notes de publication	Date de publication	Version
<a href="#">Notes de publication pour la version 55.13 de Citrix ADM 12.1</a>	Publié le : 7 novembre 2019	Version de la note de publication : 1.0
<a href="#">Notes de publication pour la version 54.13 de Citrix ADM 12.1</a>	Publié : 20 septembre 2019 ; mis à jour le 26 septembre	Version de note de version : 2.0
<a href="#">Notes de publication pour la version 53.12 de Citrix ADM 12.1 Release</a>	Publié le : 28 août 2019	Version de note de version : 3.0
<a href="#">Notes de publication pour la version 52.15 de Citrix ADM 12.1 Release</a>	Publié le : 10 juin 2019	Version de la note de publication : 1.0
<a href="#">Notes de publication pour la version 50.43 de la version 12.1 de Citrix ADM</a>	Publié le : 17 mai 2019	Version de note de version : 2.0
<a href="#">Notes de publication pour la version 50.39 de Citrix ADM 12.1 Release</a>	Publié le : 17 mai 2019	Version de note de version : 2.0
<a href="#">Notes de publication pour la version 50.33 de Citrix ADM 12.1 Release</a>	Publié le : 16 avril 2019	Version de la note de publication : 1.0
<a href="#">Notes de publication pour la version 50.30 de la version 12.1 de Citrix ADM</a>	Publié le : 14 janvier 2019	Version de la note de publication : 1.0
<a href="#">Notes de publication pour la version 50.28 de Citrix ADM 12.1 Release</a>	Publié le : 1er décembre 2018	Version de la note de publication : 1.0
<a href="#">Notes de publication pour la version 49.23 de Citrix ADM 12.1 Release</a>	Publié le : 29 août 2018	Version de la note de publication : 1.0
<a href="#">Notes de publication pour la version 48.18 de Citrix ADM 12.1 Release</a>	Publié le : 18 juin 2018	Version de note de version : 2.0

### Remarque

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

## Mise en route

February 1, 2024

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

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

### Étape 1 - Examiner les exigences du système

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

- **Informations sur la licence.** Vous pouvez gérer et surveiller n'importe quel nombre d'instances et d'entités sans licence. Toutefois, vous ne pouvez gérer que 30 applications découvertes et afficher les informations d'analyse pour seulement 30 serveurs virtuels sans appliquer de licence. Pour gérer plus de 30 applications ou afficher des analyses pour plus de 30 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.](#)
- **Configuration requise pour le navigateur.** Pour accéder à l'interface graphique Citrix ADM, vous devez vous assurer que vous disposez du navigateur requis et de la version correcte. [En savoir plus.](#)
- **Ports.** Assurez-vous que les ports requis sont ouverts pour que Citrix ADM puisse communiquer avec les instances Citrix ADC ou SD-WAN ou les instances Citrix ADC et SD-WAN. [En savoir plus.](#)

- **Configuration requise pour l'instance de Citrix ADC.** Différentes fonctionnalités de Citrix ADM sont prises en charge sur différentes versions du logiciel Citrix ADC. Vérifiez ces informations pour vous assurer que vous avez mis à niveau vos instances Citrix ADC vers la version correcte. [En savoir plus.](#)
- **Configuration requise pour l'instance Citrix SD-WAN.** Vérifiez ces informations pour vous assurer que vous avez mis à niveau vos instances Citrix SD-WAN vers la version correcte et que vous disposez des éditions de plate-forme correctes. [En savoir plus.](#)

## Étape 2 - Déployer Citrix ADM

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

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

## Étape 3 - Ajouter des instances à Citrix ADM

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



- Citrix ADC
  - Citrix ADC MPX
  - Citrix ADC VPX
  - Citrix ADC SDX
  - Citrix ADC CPX
  - Citrix Gateway
  - Citrix SD-WAN
- HaProxy

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

[En savoir plus](#)

#### **Étape 4 - Activer les analyses sur les serveurs virtuels**

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

[En savoir plus](#)

#### **Étape 5 - Configurer le serveur NTP sur Citrix ADM**

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

[En savoir plus](#)

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

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

- **Configurez les alarmes système.** 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.

- **Configurez les notifications système.** Vous pouvez envoyer des notifications à certains groupes d'utilisateurs pour diverses fonctions liées au système. Vous pouvez configurer un serveur de notifications dans Citrix ADM et configurer des serveurs de Gateway de messagerie et SMS (Short Message Service) pour envoyer des notifications par courrier électronique et texte aux utilisateurs. Cela garantit que vous êtes informé de toutes les activités au niveau du système, telles que la connexion utilisateur ou le redémarrage du système.
- **Configurez les paramètres de nettoyage du système.** Pour limiter la quantité de données de rapport stockées dans la base de données de votre serveur Citrix ADM, vous pouvez spécifier l'intervalle pendant lequel vous souhaitez que Citrix ADM conserve les données de rapport réseau, les événements, les journaux d'audit et les journaux des tâches. Par défaut, ces données sont nettoyées toutes les 24 heures (à 00.00 heures).
- **Configurez les paramètres de sauvegarde du système.** Citrix ADM sauvegarde automatiquement le système tous les jours à 00 h 30. Par défaut, il enregistre trois fichiers de sauvegarde. Vous souhaitez peut-être conserver un plus grand nombre de sauvegardes du système.
- **Configurez les paramètres de sauvegarde d'instance.** Si vous sauvegardez l'état actuel d'une instance Citrix ADC, vous pouvez utiliser les fichiers de sauvegarde pour restaurer la stabilité au cas où l'instance deviendrait instable. Cela est particulièrement important avant d'effectuer une mise à niveau. Par défaut, une sauvegarde est effectuée toutes les 12 heures et trois fichiers de sauvegarde sont conservés dans le système.
- **Configurez les paramètres de nettoyage d'événement d'instance.** Pour limiter la quantité de données de messages d'événement stockées dans la base de données de votre serveur Citrix ADM, vous pouvez spécifier l'intervalle pendant lequel vous souhaitez que Citrix ADM conserve les données de rapport réseau, les événements, les journaux d'audit et les journaux des tâches. Par défaut, ces données sont effacées toutes les 24 heures (à 00:00 heures).
- **Configurez les paramètres de purge Syslog de l'instance.** Pour limiter la quantité de données syslog stockées dans la base de données, vous pouvez spécifier l'intervalle auquel vous souhaitez purger les données syslog. Vous pouvez spécifier le nombre de jours après lesquels les données Syslog suivantes sont supprimées de Citrix ADM :
  - Données Syslog génériques
  - Données AppFirewall
  - Données Citrix Gateway.

[En savoir plus](#)

## Prochaine étape

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

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

**Gestion des instances SD-WAN Citrix ADC.** Toutes les fonctionnalités de Citrix ADM ne sont pas prises en charge sur les instances WO SD-WAN. Par exemple, la gestion des certificats ou l'audit de configuration ne sont pas pris en charge. Pour savoir quelles fonctionnalités sont prises en charge et comment les utiliser, consultez la section [Gestion de Citrix SD-WAN WO à l'aide de Citrix ADM](#).

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

## Liste des articles pratiques

February 1, 2024

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

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

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

### Gestion des instances

[Comment surveiller les sites distribués à l'échelle mondiale](#)

[Comment gérer les partitions d'administration des instances Citrix ADC](#)

[Comment ajouter des instances à Citrix ADM](#)

[Comment créer des groupes d'instances sur Citrix ADM](#)

[Comment faire pour configurer des sites pour Geomaps dans Citrix ADM](#)

[Comment forcer un basculement vers l'instance secondaire de Citrix ADC à l'aide de Citrix ADM](#)

[Comment forcer une instance secondaire de Citrix ADC à rester secondaire à l'aide de Citrix ADM](#)

[Comment sauvegarder et restaurer une instance à l'aide de Citrix ADM](#)

[Comment utiliser le tableau de bord Citrix ADM pour surveiller une instance HAProxy](#)

[Comment afficher les détails des frontends configurés sur les instances HAProxy](#)

[Comment afficher les détails des backends configurés sur les instances HAProxy](#)

[Comment afficher les détails des serveurs configurés sur les instances HAProxy](#)

[Comment redémarrer une instance HAProxy à partir de Citrix ADM](#)

[Comment sauvegarder et restaurer une instance HAProxy à l'aide de Citrix ADM](#)

[Comment modifier le fichier de configuration HAProxy à l'aide de Citrix ADM](#)

[Comment redécouvrir plusieurs instances Citrix ADC VPX](#)

[Comment interroger les instances et entités Citrix ADC dans Citrix ADM](#)

[Comment annuler la gestion d'une instance sur Citrix ADM](#)

[Comment tracer l'itinéraire vers une instance à partir de Citrix ADM](#)

## **Gestion de la configuration**

[Comment créer une tâche de configuration sur Citrix ADM](#)

[Comment utiliser la commande SCP \(put\) dans les tâches de configuration](#)

[Comment faire pour mettre à niveau des instances Citrix ADC SDX à l'aide de Citrix ADM](#)

[Comment planifier des tâches créées à l'aide de modèles intégrés dans Citrix ADM](#)

[Comment replanifier des travaux configurés à l'aide de modèles intégrés dans Citrix ADM](#)

[Comment réutiliser les tâches de configuration exécutées](#)

[Comment faire pour mettre à niveau des instances Citrix ADC à l'aide de Citrix ADM](#)

[Comment utiliser des variables dans des tâches de configuration sur Citrix ADM](#)

[Comment utiliser des modèles de configuration pour créer des modèles d'audit sur Citrix ADM](#)

[Comment créer des tâches de configuration à partir de commandes correctives sur Citrix ADM](#)

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

[Comment faire pour créer des tâches de configuration pour les instances WO Citrix SD-WAN dans Citrix ADM](#)

[Comment utiliser Record-and-Play pour créer des tâches de configuration](#)

[Comment faire pour utiliser les tâches de configuration pour répliquer la configuration d'une instance vers plusieurs instances](#)

[Comment faire pour utiliser le modèle de configuration maître sur Citrix ADM](#)

[Comment interroger l'audit de configuration des instances Citrix ADC](#)

[Comment réutiliser les modèles d'audit de configuration dans les tâches de configuration](#)

[Comment importer et exporter des modèles de configuration](#)

[Comment générer un diff d'audit de configuration pour les pièges SNMP ConfigChange](#)

## **Gestion des certificats**

[Comment configurer une stratégie d'entreprise sur Citrix ADM](#)

[Comment installer des certificats SSL sur une instance Citrix ADC à partir de Citrix ADM](#)

[Comment mettre à jour un certificat installé depuis Citrix ADM](#)

[Comment lier et dissocier des certificats SSL à l'aide de Citrix ADM](#)

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

[Comment configurer les notifications pour l'expiration du certificat SSL à partir de Citrix ADM](#)

[Comment faire pour utiliser le tableau de bord SSL sur Citrix ADM](#)

[Comment interroger les certificats SSL à partir d'instances Citrix ADC](#)

## **Gestion des applications**

[Comment créer une définition d'application dans Citrix ADM](#)

## **StyleBooks**

[Comment afficher différents groupes de StyleBooks](#)

[Comment utiliser les StyleBooks fournis avec Citrix ADM](#)

[Comment créer vos propres StyleBooks](#)

[Comment utiliser des StyleBooks définis par l'utilisateur dans Citrix ADM](#)

[Comment utiliser l'API pour créer des configurations à partir de StyleBooks](#)

[Comment activer les analyses et configurer les alarmes sur un serveur virtuel défini dans un Style-Book](#)

[Comment créer un StyleBook pour télécharger des fichiers vers Citrix ADM](#)

[Comment utiliser l'API pour créer des configurations permettant de télécharger n'importe quel type de fichier](#)

[Comment faire pour créer un StyleBook pour charger des fichiers de certificat SSL et de clé de certificat vers Citrix ADM](#)

[Comment utiliser l'API pour créer des configurations afin de télécharger des fichiers de certificats et de clés](#)

[Comment faire pour utiliser Microsoft Skype for Business StyleBook dans les entreprises](#)

[Comment utiliser Microsoft Exchange StyleBook dans les entreprises](#)

[Comment faire pour utiliser Microsoft SharePoint StyleBook dans les entreprises](#)

## **Analytics**

[Comment activer les analyses sur les instances](#)

[Comment configurer des seuils adaptatifs](#)

[Comment configurer la gestion des SLA](#)

[Comment configurer la synthèse des bases de données à des fins d'analyse](#)

[Comment créer des seuils et des alertes à l'aide de Citrix ADM](#)

[Comment désactiver la collecte de données URL à des fins d'analyse à partir de Citrix ADM](#)

[Comment afficher le type de vidéos diffusées en continu et le volume de données consommé à partir de votre réseau](#)

[Comment afficher le débit de données de pointe pour une période donnée](#)

[Comment comparer le nombre de lectures optimisé et non optimisé de vidéos ABR](#)

[Comment comparer le temps de lecture optimisé et non optimisé des vidéos ABR](#)

[Comment comparer la consommation de bande passante des vidéos ABR optimisées et non optimisées](#)

[Comment comparer le volume de données utilisé par les vidéos ABR optimisées et non optimisées](#)

[Comment afficher l'efficacité du réseau](#)

## **Gestion d'événements**

[Comment définir l'âge des événements sur Citrix ADM](#)

[Comment planifier un filtre d'événements à l'aide de Citrix ADM](#)

[Comment configurer des notifications par e-mail répétées pour les événements provenant de Citrix ADM](#)

[Comment supprimer des événements à l'aide de Citrix ADM](#)

[Comment utiliser le tableau de bord des événements pour surveiller les événements](#)

[Comment créer des règles d'événement sur Citrix ADM](#)

[Comment faire pour modifier la gravité signalée des événements qui se produisent sur les instances de Citrix ADC](#)

[Comment afficher le résumé des événements dans Citrix ADM](#)

[Comment afficher la sévérité des événements et les asymétries des pièges SNMP sur Citrix ADM](#)

[Comment exporter des messages syslog à l'aide de Citrix ADM](#)

[Comment supprimer les messages Syslog dans Citrix ADM](#)

[Comment configurer les paramètres de paramétrage pour les événements d'instance](#)

## **Authentification**

[Comment monter en cascade des serveurs d'authentification externes](#)

[Comment ajouter des serveurs d'authentification RADIUS](#)

[Comment ajouter des serveurs d'authentification LDAP](#)

[Comment ajouter des serveurs d'authentification TACACS](#)

[Comment extraire un groupe de serveurs d'authentification dans Citrix ADM](#)

[Comment activer l'authentification locale de secours](#)

## **Système Citrix ADM**

[Comment mettre à niveau Citrix ADM](#)

[Comment réinitialiser le mot de passe pour Citrix ADM](#)

[Comment générer un fichier de support technique pour Citrix ADM](#)

[Comment sauvegarder et restaurer votre serveur Citrix ADM dans le cadre d'un déploiement de serveur unique](#)

- [Comment sauvegarder et restaurer une configuration Citrix ADM dans une paire HA](#)
- [Comment activer l'accès au shell pour les utilisateurs autres que ceux par défaut dans Citrix ADM](#)
- [Comment configurer le serveur NTP sur Citrix ADM](#)
- [Comment configurer les paramètres SSL pour Citrix ADM](#)
- [Comment configurer l'intervalle de purge Syslog pour Citrix ADM](#)
- [Comment afficher les informations d'audit de Citrix ADM](#)
- [Comment configurer les paramètres de notification système de Citrix ADM](#)
- [Comment surveiller l'utilisation du processeur, de la mémoire et du disque de Citrix ADM](#)
- [Comment configurer un groupe de chiffrement pour Citrix ADM](#)
- [Comment créer des pièges, des gestionnaires et des utilisateurs SNMP sur Citrix ADM](#)
- [Comment attribuer un nom d'hôte à un serveur Citrix ADM](#)
- [Comment configurer les paramètres d'nettoyage du système pour Citrix ADM](#)
- [Comment configurer les paramètres de sauvegarde du système à l'aide de Citrix ADM](#)
- [Comment configurer et afficher les alarmes système sur Citrix ADM](#)
- [Procédure de diagnostic et de dépannage des instances Citrix ADC](#)

## **Fonctions réseau**

- [Comment générer des rapports pour les entités d'équilibrage de charge](#)
- [Comment exporter ou planifier l'exportation de rapports sur les fonctions réseau](#)

## **Vue d'ensemble**

February 1, 2024

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



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

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

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

## Caractéristiques et solutions

February 1, 2024

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

### Analyse et gestion des applications

#### [Analyse des performances des applications](#)

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

#### [Analyses de sécurité des applications](#)

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

### Réseaux

#### [Instances](#)

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

#### [Groupes d'instances](#)

Vous permet de regrouper vos instances comme suit :

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

### Gestion d'événements

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

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

### Gestion des certificats

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

### Gestion de la configuration

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

### Audit de configuration

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

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

### Rapports sur le réseau

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

## **Analytics**

### Web Insight

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

### HDX Insight

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

### Gateway Insight

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

### Security Insight

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

### SSL Insight

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

### TCP Insight

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

### Video Insight

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

### WAN Insight

L'analyse WAN Insight permet aux administrateurs de surveiller facilement le trafic WAN accéléré et non accéléré qui circule entre le centre de données et les appliances d'optimisation WAN des succur-

sales. WAN Insight offre également une visibilité sur les clients, les applications et les succursales du réseau, afin de vous aider à résoudre efficacement les problèmes réseau.

## Orchestration

### Orchestration dans le cloud

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

### Orchestration

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

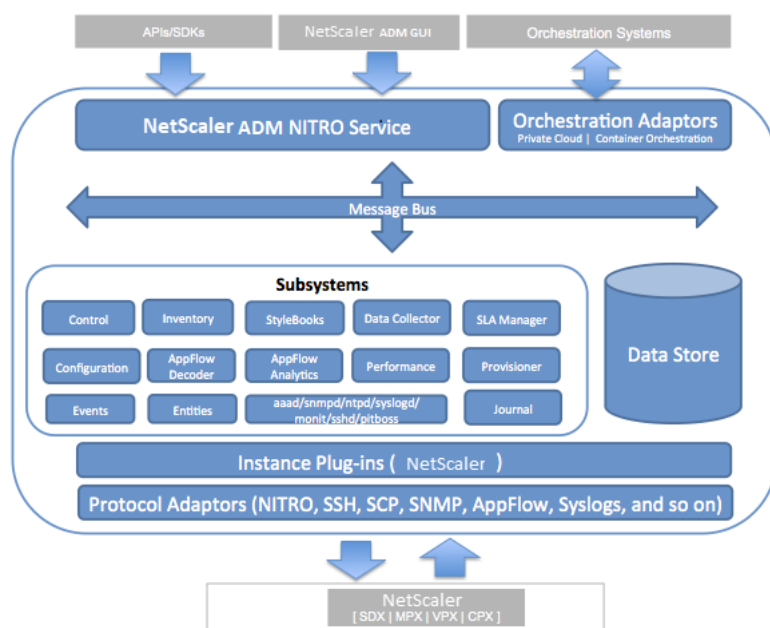
## Architecture

February 1, 2024

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

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

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



Le sous-système Service dans ADM agit comme un serveur Web qui gère les requêtes HTTP et les réponses envoyées aux sous-systèmes dans 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, Stylebooks, Data Collector, Configuration, AppFlow Decoder, AppFlow Analytics, Performance, Events, Entités, SLA Manager, Provisioner et Journal) a un rôle spécifique.

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

## Comment Citrix ADM découvre des instances

February 1, 2024

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

- Instances ADC Citrix

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

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

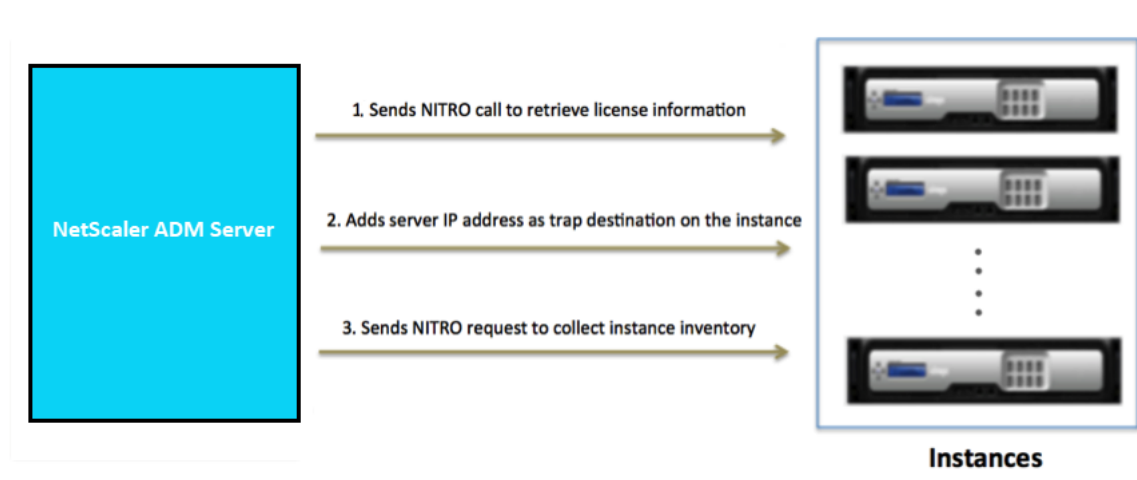
**Remarque**

Citrix ADM utilise l'adresse IP NetScaler (NSIP) des instances Citrix ADC pour la communication. ADM peut également découvrir des instances ADC avec une adresse IP de sous-réseau (SNIP) dont l'accès à la gestion est activé. Pour plus d'informations sur les ports qui doivent être ouverts entre les instances ADC et ADM, consultez [Ports](#).

Pour Citrix SD-WAN WO, ADM utilise l'adresse IP de gestion des instances pour la communication. Vous ne pouvez pas ajouter d'instances Citrix SD-WAN SE/PE dans ADM. Vous pouvez configurer ADM en tant que collecteur AppFlow sur les appliances Citrix SD-WAN SE/PE.

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

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



Comme le montre le diagramme, les étapes suivantes sont effectuées implicitement par Citrix ADM.

1. Citrix ADM utilise les détails du profil d'instance pour ouvrir une session sur l'instance. À l'aide d'un appel NITRO ADC, ADM récupère les informations de licence de l'instance. Sur la base des

informations de licence, il détermine si l'instance est une instance ADC et le type de plate-forme ADC (par exemple, Citrix ADC MPX, ADC VPX, ADC SDX ou Citrix Gateway). Lors de la détection réussie de l'instance, elle est ajoutée à la base de données d'ADM.

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

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

#### Remarque

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

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

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

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

3. ADM collecte l'inventaire de l'instance en envoyant une demande NITRO. Il collecte les détails de l'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, etc.

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

Pour savoir comment ajouter des instances à ADM, consultez la section [Ajouter des instances](#).

## Vue d'ensemble de l'interrogation

February 1, 2024

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

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

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

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

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

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

Type de sondage	Intervalle d'interrogation	Informations sondées	Protocole utilisé	Configuration des intervalles d'interrogation
<b>Sondage d'instance</b>	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



Type de sondage	Intervalle d'interrogation	Informations sondées	Protocole utilisé	Configuration des intervalles d'interrogation
<b>Interprétation d'inventaire</b>	Toutes les 30 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
<b>Collecte de données de performance</b>	Toutes les 5 minutes (par défaut)	Informations de reporting du réseau	Appel NITRO	Non
<b>Sondage de sauvegarde d'instance</b>	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 <b>Réseaux &gt; Instances &gt; Citrix ADC.</b> Sélectionnez l'instance et dans la liste <b>Sélectionner une action,</b> cliquez sur <b>Sauvegarde/Restaurer .</b>

Type de sondage	Intervalle d'interrogation	Informations sondées	Protocole utilisé	Configuration des intervalles d'interrogation
<b>Sondage d'audit de configuration</b>	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	<p>Oui. Accédez à <b>Réseaux &gt; Audit de configuration</b>.</p> <p>Dans la page Audit de configuration, cliquez sur <b>Paramètres</b> et configurez l'intervalle d'interrogation pour l'interrogation d'audit de configuration.</p>

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

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

Type de sondage	Intervalle d'interrogation	Informations sondées	Protocole utilisé	Configuration des intervalles d'interrogation
<b>Sondage des entités</b>	Toutes les 30 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.	NITRO appelle.	Oui, mais ne peut pas être réglé sur moins de 10 minutes. Pour configurer, accédez à <b>Réseaux &gt; Fonctions réseau</b> . Dans la page Fonction réseaux, cliquez sur <b>Paramètres</b> pour configurer l'intervalle d'interrogation.

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

**Remarque**

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

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

## Différentes manières de sonder les instances

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

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

### Sondage mondial des instances

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

### Interrogation manuelle des instances

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

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

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

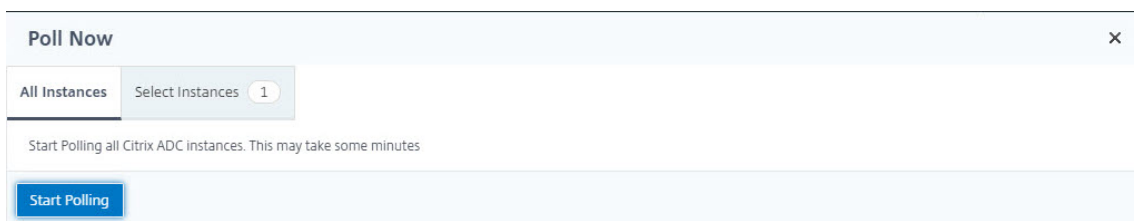
### Pour interroger des instances spécifiques dans Citrix ADM :

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

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

- a) Onglet **Toutes les instances** : cliquez sur **Commencer le sondage** pour interroger toutes les instances.
- b) Onglet **Sélectionner les instances** - sélectionnez les instances dans la liste

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



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

## Interrogation manuelle des entités

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

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



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

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

### Remarque

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

### Pour interroger des entités spécifiques dans Citrix ADM :

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

1. Dans Citrix ADM, accédez à **Réseaux > Fonctions réseau > Équilibrage de charge > 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.

Instance	Host Name	Name	Protocol	State	Effective State	Last State Chang	
<input checked="" type="checkbox"/>	10.102.29.60	-NA-	asd234	HTTP	Down	DOWN	22 days, 02h : 53m
<input type="checkbox"/>	10.102.29.60	-NA-	asd229	HTTP	Up	Up	22 days, 02h : 53m
<input type="checkbox"/>	10.102.29.60	-NA-	asd11	HTTP	Up	Up	22 days, 02h : 53m
<input type="checkbox"/>	10.102.29.60	-NA-	asd165	HTTP	Up	Up	22 days, 02h : 53m
<input type="checkbox"/>	10.102.29.60	-NA-	asd158	HTTP	Up	Up	22 days, 02h : 53m
<input type="checkbox"/>	10.102.29.60	-NA-	sharepoint-application-test-audio-management-lb	HTTP	Up	Up	22 days, 02h : 53m
<input type="checkbox"/>	10.106.43.12	-NA-	lbv_test_entity_144.122.201.24	HTTP	Up	Up	03h : 04m : 31s
<input type="checkbox"/>	10.102.29.60	-NA-	asd178	HTTP	Up	Up	22 days, 02h : 53m
<input type="checkbox"/>	10.106.43.12	-NA-	lbv_test_entity_144.122.200.19	HTTP	Down	DOWN	03h : 04m : 31s
<input type="checkbox"/>	10.102.29.60	-NA-	asd82	HTTP	Down	DOWN	22 days, 02h : 53m

## Gouvernance des données

February 1, 2024

L'authentification des clients est d'une importance vitale pour une organisation car elle lui permet de protéger ses ressources réseau en autorisant uniquement les clients ou utilisateurs authentifiés à accéder à son réseau. En tant qu'administrateur, il est important que vous identifiiez vos utilisateurs avant de les autoriser à se connecter aux ressources du réseau Citrix.

À partir de la version 12.1 version 50.x, Citrix Application Delivery Management (ADM) exige que vous vous authentifiiez sur l'interface graphique ADM avant de commencer à accéder aux informations. Vous devez vous enregistrer sur les services cloud Citrix avant de vous authentifier sur ADM. Vous devez fournir les informations d'identification de l'utilisateur Citrix Cloud sur l'interface graphique ADM. Pour plus d'informations, consultez la section [S'inscrire à Citrix Cloud](#).

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

### **Workflow si vous êtes un nouvel utilisateur**

1. Terminez l'installation de Citrix ADM sur l'Hypervisor sélectionné.
2. Configurez les différentes adresses IP requises.
3. Dans un navigateur Web, tapez l'adresse IP de Citrix ADM.
4. Dans les champs Nom d'utilisateur et Mot de passe, entrez les informations d'identification de l'administrateur.
5. La page Configurer l'identité du client s'ouvre et vous devez vous identifier à l'aide de vos informations d'identification Citrix Cloud.  
  
Si vous n'avez pas créé de compte sur Citrix Cloud, cliquez sur [Citrix Cloud](#) pour vous inscrire.
6. Cliquez sur Authentifier et indiquez l'adresse e-mail que vous avez utilisée pour vous inscrire sur le cloud Citrix.
7. Activez la case à cocher à côté de « J'accepte de partager des données pour la télémétrie » et cliquez sur Soumettre.

### **Workflow si vous êtes un utilisateur existant effectuant une mise à niveau vers la dernière version 12.1**

1. Après la mise à niveau de Citrix ADM vers la dernière version de la version 12.1, dans un navigateur Web, saisissez l'adresse IP du Citrix ADM.
2. Dans les champs Nom d'utilisateur et Mot de passe, entrez les informations d'identification de l'administrateur.
3. La page Configurer l'identité du client s'ouvre et vous devez vous identifier à l'aide de vos informations d'identification Citrix Cloud.  
  
Si vous n'avez pas créé de compte sur Citrix Cloud, cliquez sur [Citrix Cloud](#) pour vous inscrire.
4. Cliquez sur Authentifier et indiquez l'adresse e-mail que vous avez utilisée pour vous inscrire sur le cloud Citrix.

5. Activez la case à cocher à côté de « J'accepte de partager des données pour la télémétrie » et cliquez sur Soumettre.

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

- en accédant à **Système** > Administration du système , puis en cliquant sur Authentification.
- en cliquant sur le symbole du nuage en haut à droite de l'interface graphique ADM. Une fois l'authentification réussie, le « X » devient une coche verte.

#### Remarque

Assurez-vous que les domaines suivants sont en liste blanche :

- \*.citrixnetworkapi.net
- \*.blob.core.windows.net

En téléchargeant vos données sur Citrix ADM et en utilisant les fonctionnalités de Citrix ADM, vous acceptez et consentez à ce que Citrix collecte, stocke, transmet, gère, traite et utilise des informations techniques, utilisateur ou connexes concernant vos produits et services Citrix.

À tout moment, les informations reçues par Citrix seront traitées conformément à la [Stratégie de confidentialité de Citrix.com](#) .

## Licences

February 1, 2024

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

Vous pouvez gérer et surveiller n'importe quel nombre d'instances et d'entités sans licence. Toutefois, vous ne pouvez gérer que 30 applications découvertes sur l'App Dashboard et consulter les données d'analyse de 30 serveurs virtuels uniquement sans appliquer de licence. Pour gérer plus de 30 applications découvertes ou pour consulter les analyses de plus de 30 serveurs virtuels, vous devez acheter et appliquer des licences.

	Fonctionnalités de Citrix ADM	[ <b>GRATUIT</b> ] La licence Citrix ADM n'est pas requise quel que soit le nombre de serveurs virtuels	La licence Citrix ADM est requise pour plus de 30 serveurs virtuels	Exigence de licence Citrix ADC
Analytics	Web Insight	Non	Oui	Sans objet
	HDX Insight*	Non	Oui	Enterprise (création de rapports < 1 heure) Premium (création de rapports = illimitée)
	Security Insight	Non	Oui	Licence Premium (ou) Enterprise avec App Firewall
	SSL Insight	Non	Oui	Sans objet
	Gateway Insight	Non	Oui	Enterprise (création de rapports < 1 heure) Premium (création de rapports = illimitée)
	TCP Insight	Non	Oui	Sans objet
	Video Insight	Non	Oui	Premium (série Citrix-T 1000, VPX-T)
	WAN Insight	Non	Sans objet	L'instance Citrix SD-WAN doit être Optimization Edition (WANOP)
Applications				

	Fonctionnalités de Citrix ADM	[ <b>GRATUIT</b> ] La licence Citrix ADM n'est pas requise quel que soit le nombre de serveurs virtuels	La licence Citrix ADM est requise pour plus de 30 serveurs virtuels	Exigence de licence Citrix ADC
	Statistiques des applications (Tableau de bord de l'application, Tableau de bord de la sécurité de l'application)	Non	Oui	Les informations relatives au Citrix ADC Web App Firewall sur le tableau de bord des applications et le tableau de bord de sécurité des applications nécessitent une licence Premium (ou) Enterprise avec App Firewall.
	Stylebooks	Oui	Non	Sans objet
Réseaux	Serveur de licences	Oui	Non	Sans objet
	Gestion de l'inventaire : tableau de bord de l'infrastructure, groupes d'instances, tableau de bord des instances et sites	Oui	Non	Sans objet
	Gestion des événements et Syslog	Oui	Non	Sans objet

Fonctionnalités de Citrix ADM	[ <b>GRATUIT</b> ] La licence Citrix ADM n'est pas requise quel que soit le nombre de serveurs virtuels	La licence Citrix ADM est requise pour plus de 30 serveurs virtuels	Exigence de licence Citrix ADC
Tâches de configuration, audit de configuration et conseils de configuration	Oui	Non	Sans objet
Rapports réseau (au niveau de l'instance)	Oui	Non	Sans objet
Rapports réseau (au niveau du serveur virtuel)	Oui	Non	Sans objet
Fonctions réseau (visibilité et gestion des serveurs virtuels, des services, des groupes de services, des serveurs)	Oui	Non	Sans objet
Gestion, surveillance et tableau de bord des certificats SSL (au niveau de l'instance)	Oui	Non	Sans objet
Tableau de bord des certificats SSL (au niveau du serveur virtuel)	Oui	Non	Sans objet

System

	Fonctionnalités de Citrix ADM	[ <b>GRATUIT</b> ] La licence Citrix ADM n'est pas requise quel que soit le nombre de serveurs virtuels	La licence Citrix ADM est requise pour plus de 30 serveurs virtuels	Exigence de licence Citrix ADC
Orchestration	Authentification RBAC et externe (niveau d'instance)	Oui	Non	Sans objet
	RBAC et authentification externe	Oui	Non	Sans objet
	Intégration à OpenStack	Oui	Non	Sans objet
	Intégration à VMware NSX	Oui	Non	Sans objet
	Intégration Cisco APIC	Oui	Non	Sans objet
Équilibreurs de charge tiers	Intégration de conteneurs	Oui	Non	Sans objet
	HAProxy : visibilité sur l'hôte/l'instance/le backend/les serveurs/le frontend, la configuration du téléchargement ou du téléchargement et le redémarrage de l'appliance.	Oui	Non	Sans objet

Tableau de bord des applications	Non	Oui (nécessite une licence distincte)	Sans objet
----------------------------------	-----	---------------------------------------	------------

---

\*Pour l'intégration de Citrix Director au support Citrix ADM, Citrix Director doit disposer d'une licence Premium.

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

## Haute disponibilité

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

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

### Remarque

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

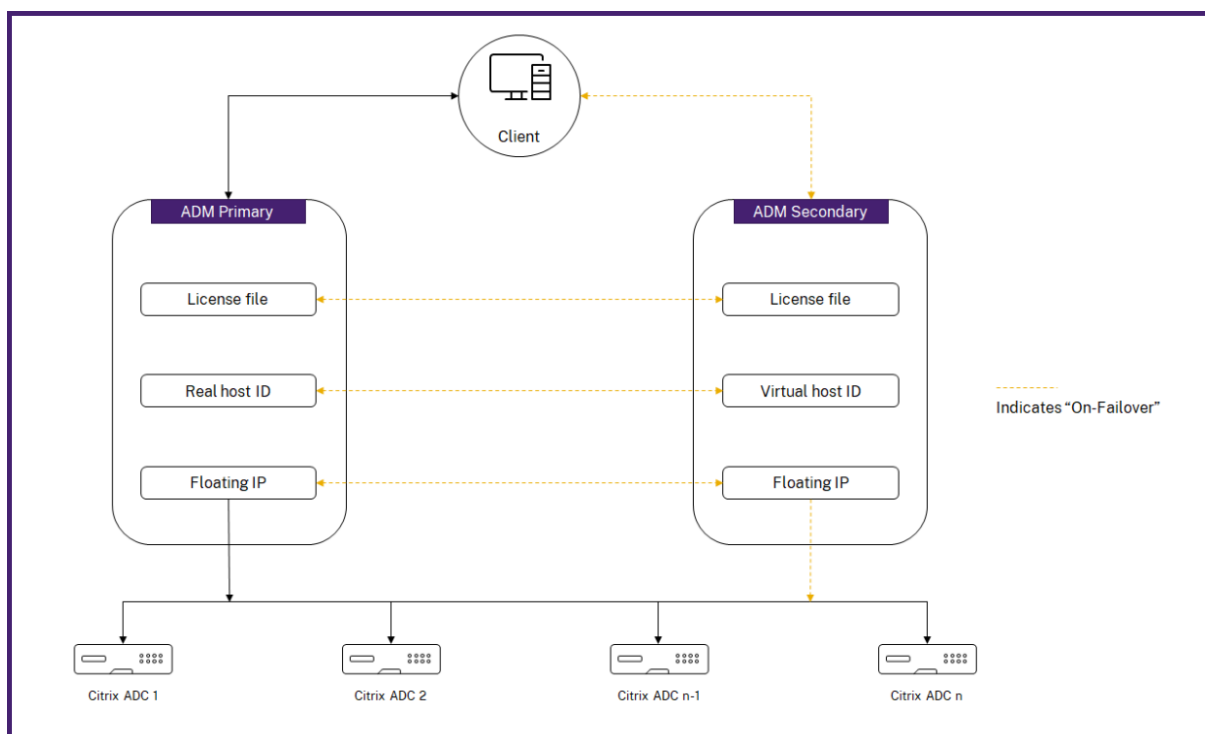
## Comment les licences sont-elles synchronisées entre les nœuds haute disponibilité ADM ?

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

- **ID d'hôte réel** - Cet ID est généré à partir d'une adresse MAC du serveur ADM. Chaque déploiement autonome ADM possède un ID d'hôte unique.



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



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

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

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

## Orchestration

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

## Mettre à niveau les licences de serveur virtuel

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

### Pour mettre à niveau les licences de votre appliance :

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

#### Remarque

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

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

<input type="checkbox"/>	Name	Last Modified	Size
<input type="checkbox"/>	CNS_VIPE_100CCS_RetailS_LaterSA.lic	2016-06-27 14:09:44	1.06 KB
<input type="checkbox"/>	CNS_VIPE_500CCS_RetailS.lic	2016-06-27 14:09:44	1.06 KB

## Vérification

Vous pouvez vérifier les licences installées sur votre Citrix ADM en accédant à **Réseaux > Licences > Licences système**.

Licenses / System Licenses

System Licenses	
Allowed Virtual Servers 530	Total Managed Virtual Servers 169

### Licenciez les serveurs virtuels

Vous pouvez sélectionner les serveurs virtuels à gérer et à surveiller via Citrix ADM. Si le nombre total de serveurs virtuels hébergés par les instances Citrix ADC découvertes est inférieur au nombre de licences de serveur virtuel installées, Citrix ADM octroie des licences à tous les serveurs virtuels.

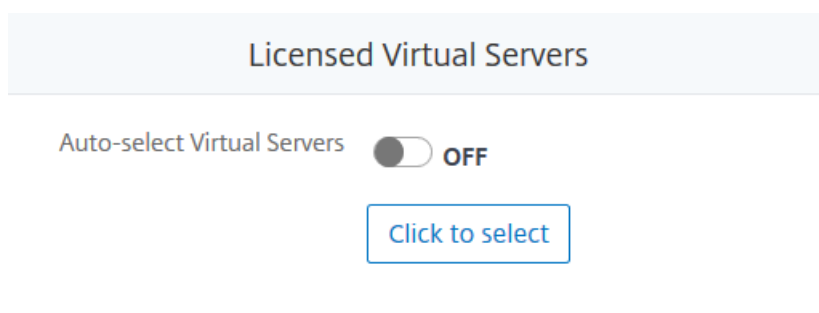
Vous pouvez sélectionner les serveurs virtuels que vous souhaitez gérer et surveiller via Citrix ADM.

#### Points à noter :

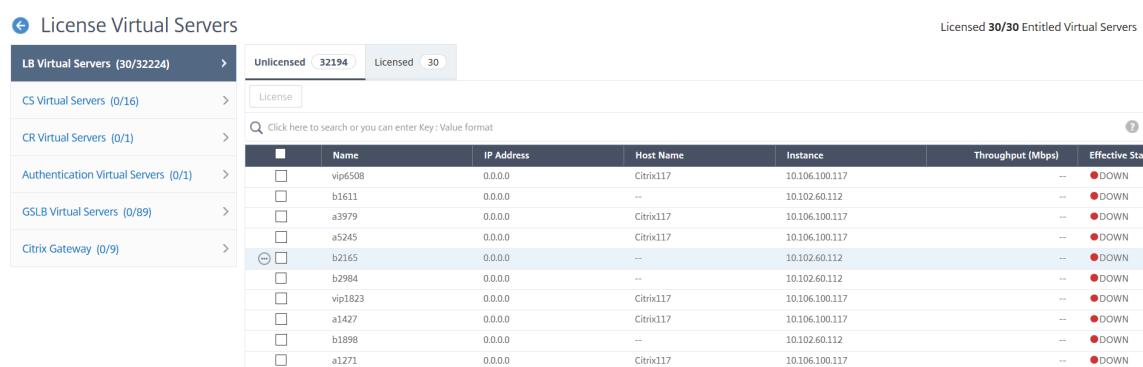
- Par défaut, Citrix ADM octroie automatiquement des licences aux serveurs virtuels de manière aléatoire après chaque cycle d'interrogation du serveur virtuel.
- Si le nombre total de serveurs virtuels découverts dans votre Citrix ADM est inférieur au nombre de licences de serveur virtuel installées, Citrix ADM, par défaut, octroie des licences à tous les serveurs virtuels.
- Pour sélectionner manuellement les serveurs virtuels ou pour limiter les licences aux serveurs virtuels limités, vous devez d'abord désactiver la licence automatique des serveurs virtuels, puis sélectionner les serveurs virtuels que vous souhaitez gérer.
- Citrix ADM n'octroie pas de licence aux serveurs virtuels non adressables. Pour les gérer, vous devez les licencier manuellement.

#### Pour gérer les serveurs virtuels sous licence :

1. Ouvrez une session sur Citrix ADM à l'aide des informations d'identification de l'administrateur.
2. Accédez à **Réseaux > Licences > Licences système**.  
Le tableau de bord des licences système s'affiche.
3. Sous **Serveurs virtuels sous licence**, désactivez la **sélection automatique des serveurs virtuels** et cliquez sur l'option **Cliquez pour sélectionner**.



4. Dans l'écran **License Virtual Server**, sélectionnez le type de serveurs virtuels en cliquant sur l'onglet correspondant.



5. Dans l'onglet **Sans licence**, sélectionnez les serveurs virtuels pour lesquels vous souhaitez octroyer une licence et cliquez sur **Licence**. Dans l'onglet **Licence**, sélectionnez les serveurs virtuels dont vous souhaitez annuler la licence et cliquez sur **Annuler la licence**.
6. Cliquez sur **Suivant** pour accéder à l'onglet des autres serveurs virtuels, ou cliquez sur **Enregistrer et quitter pour attribuer** une licence aux serveurs virtuels sélectionnés.

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

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

Citrix ADM propose une nouvelle option sous **Réseaux > Licences > Licences système**. Autrement dit, la nouvelle option **Sélection automatique des serveurs virtuels non adressables**. L'activation de cette option vous permet désormais de spécifier explicitement que la licence doit inclure également des serveurs virtuels non adressables.

### Remarque

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

## Contrôles d'expiration pour les licences de serveurs virtuels

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

### Pour afficher l'état des licences :

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

### Pour configurer les paramètres de notification des licences :

1. Accédez à **Réseaux > Licences > Paramètres**.
2. Dans la section **Paramètres de notification**, cliquez sur l'icône en forme de crayon et modifiez les paramètres.
  - **Profil d'e-mail** : profil d'e-mail ou liste de distribution pour l'envoi de notifications lorsque les licences atteignent le seuil ou expirent.
  - **Profil SMS** : profil SMS ou liste de distribution permettant d'envoyer des notifications lorsque les licences atteignent le seuil ou arrivent à expiration.
  - **Seuil d'alerte** : 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.
  - **Jours d'expiration** : nombre de jours restants avant l'expiration.

## Configuration système requise

February 1, 2024

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

### Configuration requise pour Citrix ADM

Composant	Exigences
RAM	32 GB
CPU virtuel	8 processeurs <b>Remarque:</b> Citrix recommande d'utiliser la technologie SSD pour les déploiements Citrix ADM.
Espace de stockage	<p>La valeur par défaut est 120 Go. Les besoins réels de stockage dépendent de l'estimation de la taille de Citrix ADM. Utilisez le calculateur de dimensionnement mentionné dans la section <b>Limites maximales</b> (page 7) du Guide de déploiement Citrix ADM HA. Ce guide est disponible sur notre <a href="#">site de téléchargement</a>, sous <b>NetScaler MAS Release 12.1 &gt; Versions antérieures</b>. <b>Remarque :</b> vous avez besoin d'un compte Citrix pour accéder au guide de déploiement et à la calculatrice de dimensionnement.</p> <p>Si votre besoin de stockage Citrix ADM dépasse 120 Go, vous devez connecter un disque supplémentaire. Vous ne pouvez ajouter qu'un seul disque supplémentaire.</p> <p>Citrix vous recommande d'estimer le stockage et d'attacher un disque supplémentaire au moment du déploiement initial.</p>

Composant	Exigences
	Pour plus d'informations, consultez <a href="#">Comment attacher un disque supplémentaire à Citrix ADM</a> .
Interfaces réseau virtuelles	1
Débit	1 Gbit/s ou 100 Mbit/s

Remarque

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

### Configuration requise pour l'agent sur site Citrix ADM

Composant	Exigences
RAM	8 GB  <b>Remarque</b> : La valeur par défaut est 8 Go. Citrix vous recommande d'augmenter la valeur par défaut à 32 Go pour de meilleures performances.
CPU virtuel	2 processeurs  <b>Remarque</b> : La valeur par défaut est de 2 processeurs. Citrix vous recommande d'augmenter la valeur par défaut à 8 processeurs pour de meilleures performances.
Espace de stockage	30 GB
Interfaces réseau virtuelles	1
Débit	1 Gbit/s

Remarque

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

### Version minimale de Citrix ADC requise pour les fonctionnalités Citrix ADM

**Important**

La version et la version de Citrix ADM doivent être **égales ou supérieures** à celles de votre version

et build de Citrix ADC. Par exemple, si vous avez installé Citrix ADM 12.1 Build 50.39, assurez-vous d'avoir installé Citrix ADC 12.1 Build 50.28/50.31 ou une version antérieure.

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

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

### **Configuration requise pour la gestion des instances Citrix SD-WAN**

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



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

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

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

- Client léger Dell Wyse WTOS modèle R10L Rx0L
- NComputing N400
- Dell Wyse WTOS modèle CX0 C00X Xenith
- Dell Wyse WTOS modèle TX0 T00X Xenith2
- Modèle CX0 C10LE WTOS de Dell Wyse
- Client léger HDX Dell Wyse WTOS modèle R00LX Rx0L
- Dell Wyse Enhanced SUSE Linux Enterprise, modèle Dx0D, D50D
- Client léger Dell Wyse ZX0 Z90D7 (WEST7)

### Configuration requise pour les analyses Citrix ADM

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

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

**Remarque**

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

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

**Clients légers pris en charge pour des informations HDX**

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

**Licence d'instance Citrix ADC requise pour HDX Insight**

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

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

Entreprise	Oui	Oui	Non	Non	Non
Platine	Oui	Oui	Oui	Oui	Oui

### Hyperviseurs pris en charge

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

Hyperviseur	Versions
Citrix Hypervisor	7.1 et 7.4
VMware ESX	6.0, 6.5 et 6.7
Microsoft Hyper-V	2012 R2 et 2016
KVM générique	RHEL 7.4 et Ubuntu 16.04

### Systèmes d'exploitation et versions de Receiver prises en charge

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

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

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

### Navigateurs pris en charge

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

Navigateur Web	Version
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

## Ports supportés

Citrix ADM utilise l'adresse IP Citrix ADC (connue sous le nom NSIP) pour communiquer avec Citrix ADC. Pour les communications entre les instances Citrix ADC et Citrix ADM, ou les instances Citrix SD-WAN et Citrix ADM, les ports suivants doivent être ouverts dans Citrix ADM :

### Remarque

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

Type	Port	Détails	Direction de la communication
TCP	80/443	Pour la communication NITRO depuis Citrix ADM vers Citrix ADC ou Citrix SD-WAN instance.443. Pour la communication NITRO entre les serveurs Citrix ADM en mode haute disponibilité.	Citrix ADM vers Citrix ADC et Citrix ADC vers Citrix ADM
TCP	22	Pour la communication SSH depuis Citrix ADM vers Citrix ADC ou Citrix SD-WAN instance. Pour la synchronisation entre les serveurs Citrix ADM déployés en mode haute disponibilité. Et, ce port est requis pour la communication SSH entre l'agent ADM et Citrix ADC.	Citrix ADM vers Citrix ADC et agent Citrix ADM vers Citrix ADC
UDP	4739	Pour la communication AppFlow à partir d'une instance Citrix ADC ou Citrix SD-WAN vers Citrix ADM.	Citrix ADC ou Citrix SD-WAN vers Citrix ADM
ICMP	Aucun port réservé	Pour détecter l'accessibilité réseau entre les instances Citrix ADM et Citrix ADC, les instances SD WAN ou le serveur Citrix ADM secondaire déployé en mode haute disponibilité.	
UDP	161, 162	Pour recevoir des événements SNMP de l'instance Citrix ADC vers Citrix ADM.	**Port 161**: Citrix ADM vers Citrix ADC
		**Port 162** - Citrix ADC vers Citrix ADM	
UDP	514	Pour recevoir des messages syslog à partir d'une instance Citrix ADC ou Citrix SD-WAN vers Citrix ADM.	Citrix ADC ou Citrix SD-WAN vers Citrix ADM
TCP	25	Pour envoyer des notifications SMTP depuis Citrix ADM aux utilisateurs.	
TCP	389/636	Port par défaut pour le protocole d'authentification. Pour la communication entre Cit-	

rix ADM et le serveur d'authentification externe LDAP. | Serveur d'authentification externe Citrix ADM vers LDAP |

| UDP | 123 | Port du serveur NTP par défaut pour, synchronisation avec plusieurs sources temporelles. |

| RADIUS | 1812 | Port par défaut pour le protocole d'authentification. Pour la communication entre Citrix ADM et le serveur d'authentification externe RADIUS. | Serveur d'authentification externe Citrix ADM vers RADIUS |

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

| TCP | 5563 | Pour recevoir des mesures ADC (compteurs), des événements système et des messages du journal d'audit de l'instance Citrix ADC vers Citrix ADM. | Citrix ADC vers Citrix ADM |

| TCP | 5557/5558 | Pour la communication **\*\*logstream\*\*** (pour Security Insight, Web Insight et HDX Insight) entre Citrix ADC et Citrix ADM. | Citrix ADC vers Citrix ADM |

| TCP | 5454 | Port par défaut pour la communication et la synchronisation de base de données entre les nœuds Citrix ADM en mode haute disponibilité. | Nœud principal Citrix ADM vers le nœud secondaire Citrix ADM |

| TCP | 27000 | Port de licence pour la communication entre le serveur de licences Citrix ADM et l'instance CPX. | Citrix ADC vers Citrix ADM |

| TCP | 7279 | Port du démon fournisseur Citrix. | Citrix ADC vers Citrix ADM |

| TCP | 443/8443/7443 | Port de communication entre l'agent Citrix ADM et Citrix ADM. L'agent ADM initie la communication avec Citrix ADM. | Agent Citrix ADM vers Citrix ADM |

## Limitations

Dans la version 12.1 de Citrix ADM, les fonctionnalités suivantes prennent en charge le format IPv6 des adresses IP :

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

10. Sauvegarde et restauration des instances ADC
11. Événements SNMP des Citrix ADC

Les fonctionnalités suivantes ne prennent pas en charge IPv6 :

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

## Déployer

February 1, 2024

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

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

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

## Conditions préalables à l'installation de Citrix ADM

February 1, 2024

Vous pouvez télécharger et installer Citrix 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 limitations de toutes ces plates-formes.

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

- [Citrix ADM avec Citrix Hypervisor](#)
- [Citrix ADM avec Microsoft HyperV](#)
- [Citrix ADM avec VMware ESXi](#)
- [Citrix ADM avec serveur KVM Linux](#)

### Configuration générale requise pour Citrix ADM version 12.1

---

Composant	Exigences
RAM	32 GB
CPU virtuel	8 processeurs
Espace de stockage	Citrix recommande d'utiliser la technologie SSD (Solid State Drive) pour les déploiements Citrix ADM.

Composant	Exigences
Interfaces réseau virtuelles	<p>L'espace de stockage par défaut requis est de 120 Go. Les besoins réels de stockage dépendent de l'estimation de la taille de Citrix ADM. Utilisez le calculateur de dimensionnement mentionné dans la section <b>Limites maximales</b> (page 7) du Guide de déploiement Citrix ADM HA. Ce guide est disponible sur notre <a href="#">site de téléchargement</a>, sous <b>NetScaler MAS Release 12.1 &gt; Versions antérieures</b>. <b>Remarque</b> : vous avez besoin d'un compte Citrix pour accéder au guide de déploiement et à la calculatrice de dimensionnement</p> <p>Si votre besoin de stockage Citrix ADM dépasse 120 Go, vous devez connecter un disque supplémentaire.</p> <p>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.</p> <p>Pour plus d'informations, consultez <a href="#">Comment attacher un disque supplémentaire à Citrix ADM</a>.</p>
Débit	1
	1 Gbit/s

Remarque :

Citrix vous recommande d'héberger le disque dur virtuel Citrix ADM sur un stockage local. Lorsqu'il est hébergé sur des périphériques de stockage dans un SAN, Citrix ADM peut ne pas fonctionner comme prévu.

## Citrix ADM avec Citrix Hypervisor

February 1, 2024

Pour installer Citrix ADM sur Citrix Hypervisor (anciennement XenServer), vous devez d'abord



télécharger le fichier image .vxa Citrix ADM sur votre ordinateur local. Vous devez utiliser Citrix XenCenter pour effectuer l'installation de Citrix ADM.

**Remarque :**

Citrix ADM ne prend pas en charge XenMotion.

## Conditions préalables

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

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

## Configuration système requise pour XenCenter

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

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

## Installation de Citrix Application Delivery Management

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

```

-----
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 [ADMHA1]:
    2. Citrix ADM IPv4 address [10.102.29.52]:
    3. Netmask [255.255.255.0]:
    4. Gateway IPv4 address [10.102.29.11]:
    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, enregistrez les paramètres de configuration.
3. Lorsque vous y êtes invité, ouvrez une session à l'aide des informations d'identification nsrecover/nsroot.

```

login: nsrecover
Password:
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
    The Regents of the University of California. All rights reserved.

bash-3.2# █

```

#### Remarque

Une fois connecté, si vous souhaitez mettre à jour la configuration réseau initiale, tapez `networkconfig`, mettez à jour la configuration et enregistrez-la.

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

```

bash-3.2# deployment_type.py
-----
Citrix ADM Deployment Configuration.

```

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

```

-----
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deployment.
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]: █

```

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

#### Remarque

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

## Vérification

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

Le navigateur affiche l'utilitaire de configuration Citrix ADM.

## Citrix ADM avec Microsoft Hyper-V

February 1, 2024

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

### Conditions préalables

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

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

## Configuration système requise pour Microsoft Hyper-V

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

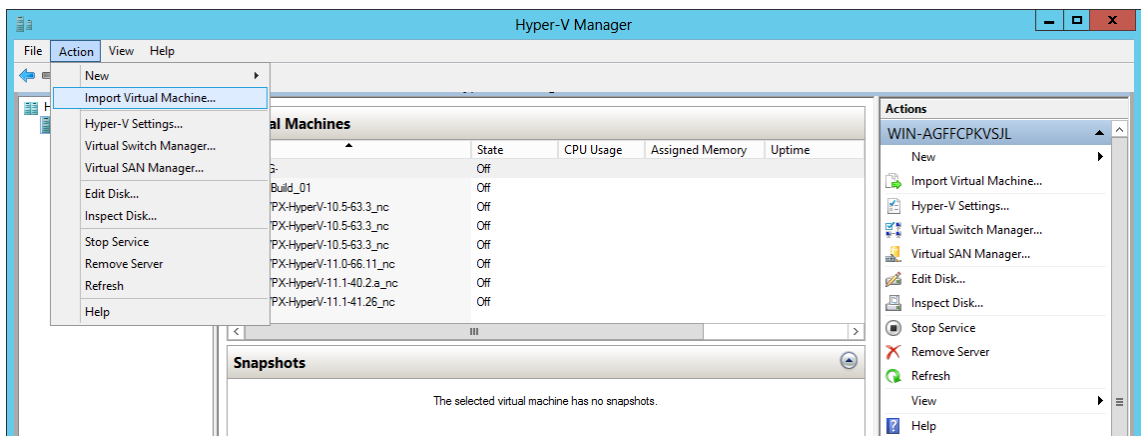
Composant	Exigences
Système d'exploitation	Windows Server 2012 R2
.NET framework	Version 2.0 ou ultérieure
UC	750 mégahertz (MHz), recommandé : 1 gigahertz (GHz) ou plus rapide
RAM	1 Go, Recommandé : 2 Go
Carte d'interface réseau	Carte réseau 100 mégabits par seconde (Mbps) ou plus rapide

## Installation de Citrix Application Delivery Management

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

### Pour installer Citrix ADM :

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

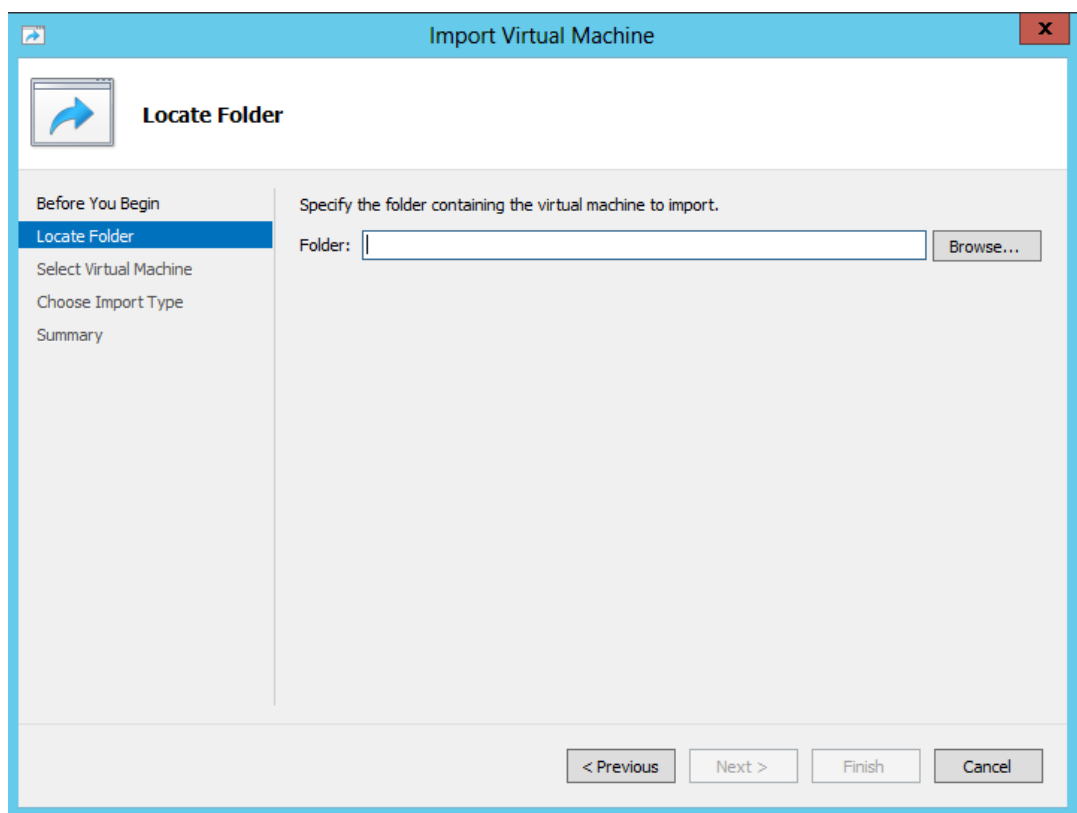


3. Importez l'image Hyper-V et procédez comme suit :
  - a) Dans la boîte de dialogue Importer une machine virtuelle, dans la section **Localiser** un dossier, accédez au dossier dans lequel vous avez enregistré l'image Citrix ADM Hyper-V, sélectionnez le dossier et cliquez sur **Suivant**.

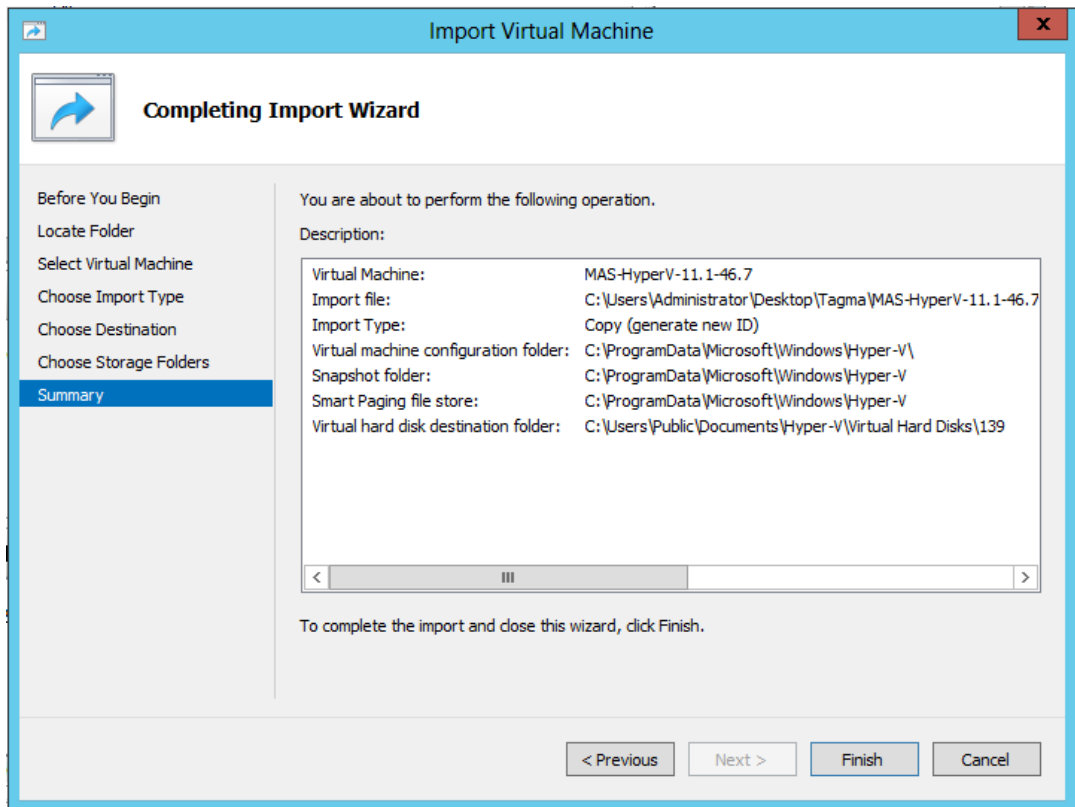
- b) Dans la section Sélectionner une machine virtuelle, sélectionnez le nom de la machine virtuelle appropriée.
- c) Dans la section **Choisir le type d'importation**, sélectionnez l'option Copier la machine virtuelle (créer un nouvel identifiant unique) et cliquez sur Suivant.
- d) Dans la section **Choisir une destination**, vous pouvez spécifier les dossiers dans lesquels stocker les fichiers de la machine virtuelle.

**Remarque**

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

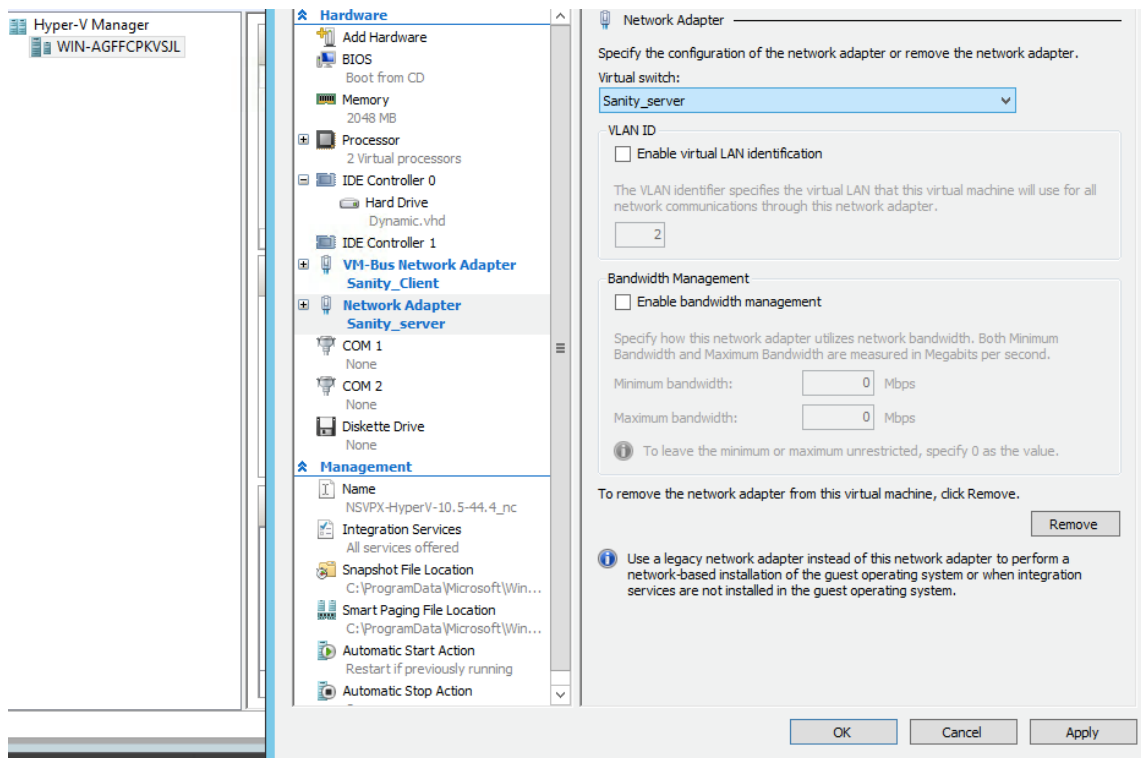


- e) Dans la section **Choisir les dossiers de stockage**, vous pouvez sélectionner l'emplacement dans lequel vous souhaitez stocker les disques durs virtuels, puis cliquer sur **Suivant**.
- f) Vous pouvez vérifier les détails de la machine virtuelle dans le volet récapitulatif, cliquez sur **Terminer**.



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

4. Cliquez avec le bouton droit sur l'image Citrix ADM Hyper-V, puis cliquez sur **Paramètres**.
5. Dans le volet gauche de la boîte de dialogue qui apparaît, accédez à **Matériel > Adaptateur réseau VM\_Bus**, puis dans le volet droit, dans la liste déroulante Réseau, sélectionnez le réseau approprié.



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

```

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 [ADMHA1]:
 2. Citrix ADM IPv4 address [10.102.29.52]:
 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]:
    
```

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 nsre-cover/nsroot.

```
login: nsrecover
Password:
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.

bash-3.2#
```

### Remarque

Une fois connecté, si vous souhaitez mettre à jour la configuration réseau initiale, tapez `networkconfig`, mettez à jour la configuration et enregistrez-la.

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

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

```
bash-3.2# deployment_type.py
-----
Citrix ADM Deployment Configuration.
```

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

```
-----
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deployment.
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]:
```

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

15. Tapez **Oui** pour redémarrer le serveur Citrix ADM.

### Remarque

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

## Vérification

Une fois le serveur installé, vous pouvez accéder à l'interface utilisateur graphique en tapant l'adresse IP du serveur Citrix ADM dans la barre d'adresse de votre navigateur. Les informations d'identification



d'administrateur par défaut pour se connecter au serveur sont nsroot/nsroot.

Le navigateur affiche l'utilitaire de configuration Citrix ADM.

## Citrix ADM avec VMware ESXi

February 1, 2024

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

### Conditions préalables

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

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

#### Remarque

VMotion n'est pas pris en charge sur Citrix ADM.

### Pour installer Citrix ADM

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

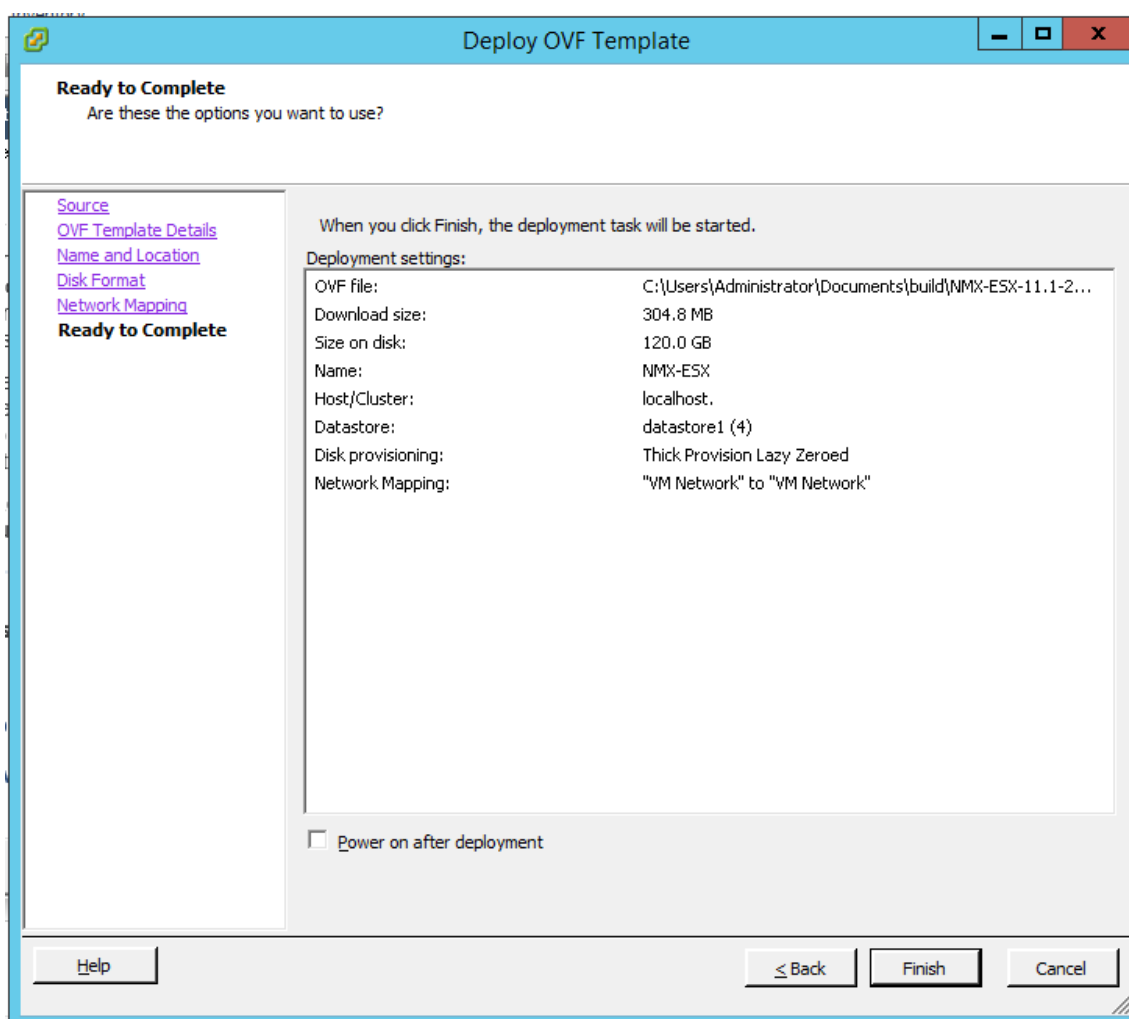
prend en charge le système d'exploitation FreeBSD. Cliquez sur **Oui**.

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

**Remarque**

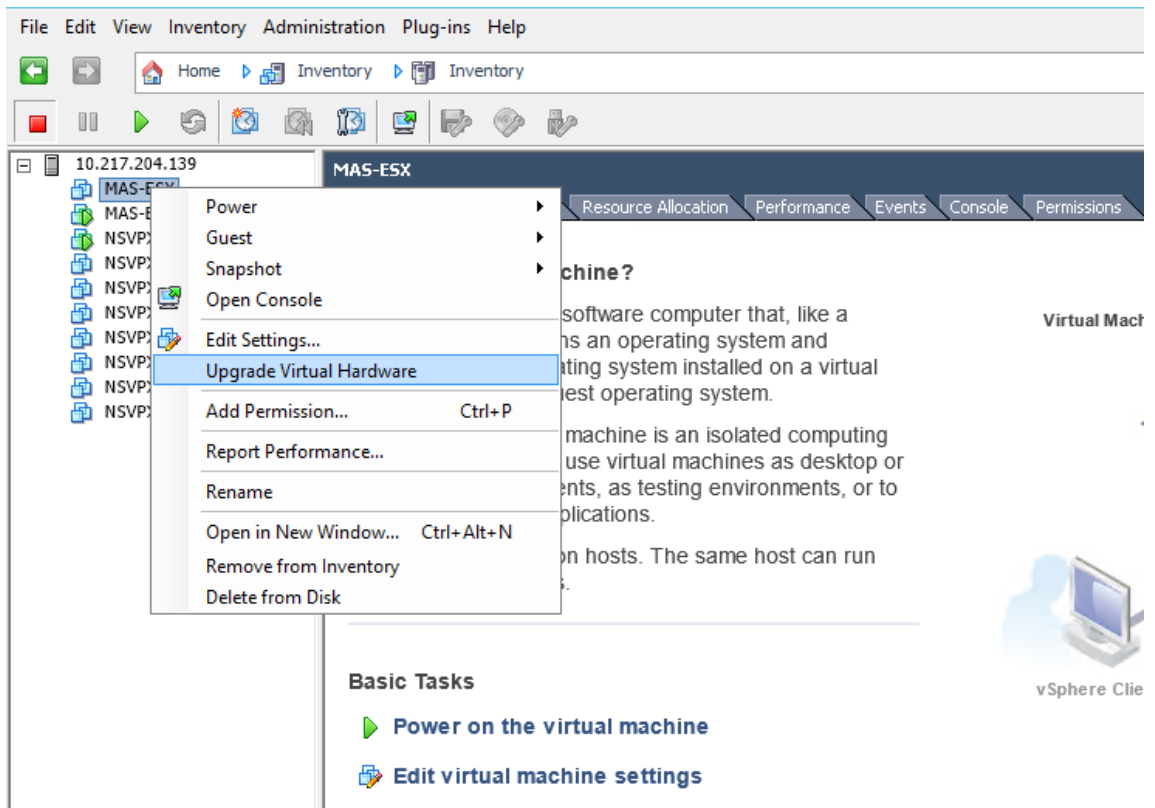
Citrix vous recommande de sélectionner le **format provisionné Thick**.

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

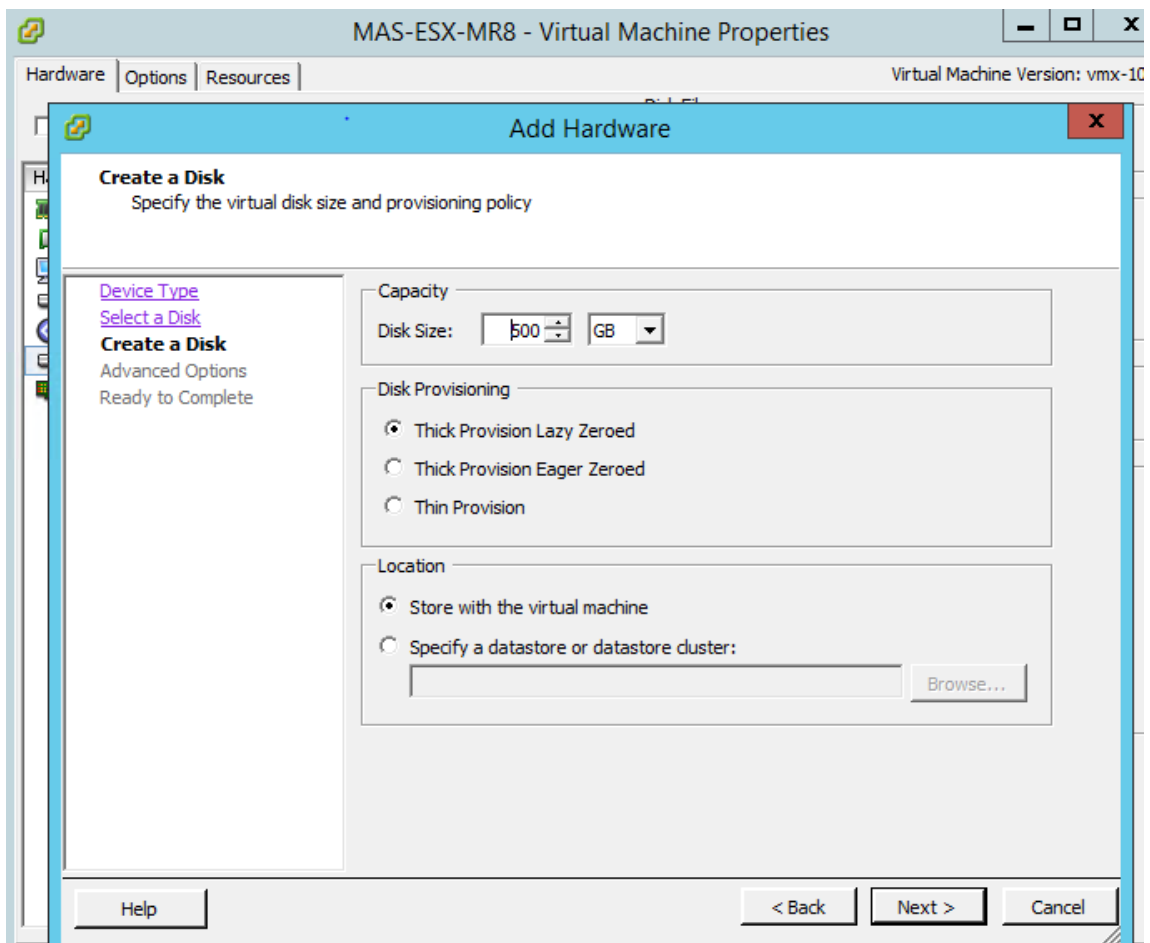


10. Vous êtes maintenant prêt à démarrer l'appliance virtuelle Citrix ADM.
11. Dans le volet de navigation, sélectionnez l'appliance virtuelle que vous avez installée. Dans le menu **Inventaire**, cliquez avec le bouton droit sur la **machine virtuelle**, puis cliquez sur **Met-**

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

```

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 [ADMHA1]:
2. Citrix ADM IPv4 address [10.102.29.52]:
3. Netmask [255.255.255.0]:
4. Gateway IPv4 address [10.102.29.11]:
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]:
    
```

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 nsre-cover/nsroot.

```
login: nsrecover
Password:
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
The Regents of the University of California. All rights reserved.

bash-3.2#
```

### Remarque

Une fois connecté, si vous souhaitez mettre à jour la configuration réseau initiale, tapez `networkconfig`, mettez à jour la configuration et enregistrez-la.

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

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

```
bash-3.2# deployment_type.py
-----
Citrix ADM Deployment Configuration.
```

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

```
-----
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deployment.
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]:
```

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

23. Tapez **Oui** pour redémarrer le serveur Citrix ADM.

### Remarque

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

## Vérification

Une fois le serveur installé, vous pouvez accéder à l'interface utilisateur graphique en saisissant l'adresse IP du serveur Citrix ADM dans le navigateur. Les informations d'identification d'administra-

teur par défaut pour se connecter au serveur sont nsroot/nsroot.

Le navigateur affiche l'utilitaire de configuration Citrix ADM.

#### **Remarque**

Lors d'un déploiement sur VMware ESXi, la mise en place de Citrix ADM peut prendre jusqu'à 30 minutes ou plus.

## **Citrix ADM avec serveur KVM Linux**

February 1, 2024

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

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

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

### **Conditions préalables**

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

### **Configuration matérielle requise**

Composant	Exigences
UC	<p>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.</p> <p><b>Remarque</b> Pour vérifier si votre CPU prend en charge l'hôte Linux, entrez la commande suivante à l'invite du shell Linux hôte :</p> <pre>*. egrep'^flags.* ( vmx   svm )' /proc/cpuinfo*</pre> <p>Si les paramètres du BIOS de l'extension sont désactivés, vous devez les activer dans le BIOS. Il n'y a pas de recommandation spécifique pour la vitesse du processeur, mais plus la vitesse, meilleures sont les performances du Citrix ADM.</p>
Mémoire (RAM)	<p>Minimum 4 Go pour le noyau Linux hôte. Ajoutez de la mémoire supplémentaire selon les besoins des machines virtuelles.</p>
Disque dur	<p>Calculez l'espace requis pour le noyau Host Linux et les machines virtuelles. Une seule machine virtuelle Citrix ADM nécessite 120 Go d'espace disque.</p>

#### Remarque

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

#### Configuration logicielle requise

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

**Configuration réseau requise** Citrix ADM prend en charge une seule interface réseau paravirtualisée VirtIO. Cette interface doit être connectée au réseau de gestion de l'hôte Linux-KVM, afin que Citrix ADM et Linux-KVM puissent communiquer.

## Télécharger les fichiers d'installation de Citrix ADM

Pour télécharger les fichiers d'installation de Citrix ADM à partir de :

1. Ouvrez un navigateur Web et saisissez [www.citrix.com](http://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 déroulante **Téléchargements**, sélectionnez **Citrix Application Delivery Management**.
5. Sur la page **Citrix Application Delivery Management**, sélectionnez la version. Par exemple, sélectionnez la **version 12.1**.
6. Cliquez sur **Logiciel produit** pour le développer, puis cliquez sur la dernière version. Par exemple, sélectionnez **Citrix ADM Release (Feature Phase) 12.1 Build 49.23/49.37**.  
La page de construction sélectionnée s'affiche.
7. Dans la liste déroulante **Aller au téléchargement**, sélectionnez l'**image Citrix ADM pour KVM, 12.1 Build xx.xx**.
8. Cliquez sur **Télécharger le fichier**, acceptez le contrat de licence de l'utilisateur final et téléchargez le fichier image compressé dans n'importe quel dossier de votre ordinateur local.

## Installer Citrix Application Delivery Management sur Linux-KVM

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



```

1 tar -xvfz MAS-KVM.tgz
2 MAS-KVM.xml
3 MAS-KVM.qcow2
4 checksum.txt
5 <!--NeedCopy-->

```

```

root@ubuntu:~/mas-build#
root@ubuntu:~/mas-build# tar xvfz MAS-KVM-11.1-50.10.tgz
MAS-KVM.xml
checksum.txt
MAS-KVM-11.1-50.10.qcow2
root@ubuntu:~/mas-build# █

```

- 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 - Spécifiez le nom.
  - B. mac - Spécifiez l'adresse MAC.
  - C. fichier source : spécifiez le chemin 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 : spécifiez le mode.
- E. type de modèle - Définit sur VirtIO.
- F. source dev - Spécifiez l'interface.

```

1 <name> MAS1-KVM</name>
2 <mac address='52:54:00:29:74:b3' />
3 <source file='/var/ MAS-KVM.qcow2' />
4 <source dev='eth0' mode='bridge' />
5 <model type='virtio' />
6 <!--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*

```

1 virsh define MAS-KVM.xml
2 Domain MAS defined from MAS-KVM.xml
3 <!--NeedCopy-->

```

```
root@ubuntu:~/mas-build# virsh define MAS-KVM.xml
Domain MAS defined from MAS-KVM.xml

root@ubuntu:~/mas-build#
```

Démarrez Citrix ADM en saisissant la commande `virsh start <DomainName>` suivante :

```
vii
1 virsh start MAS
2 Domain MAS started
3 <!--NeedCopy-->
```

```
root@ubuntu:/home/mas-build# virsh start MAS
Domain MAS started

root@ubuntu:/home/mas-build#
```

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

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

```
root@ubuntu:/home/mas-build# virsh console MAS
Connected to domain MAS
Escape character is ^]

```

## Configurer Citrix Application Delivery Management

### Remarque

Sur certains hôtes KVM Linux, les invités FreeBSD ne parviennent pas à redémarrer correctement s'ils ont plusieurs CPU. Lorsque le dispositif virtuel Citrix ADM est redémarré, l'interface de ligne de commande et l'interface graphique Citrix ADM ne répondent plus. Pour plus de détails, voir <https://bugs.launchpad.net/qemu/+bug/1329956>

Pour éviter que l'interface de ligne de commande et l'interface graphique Citrix ADM ne répondent plus lorsque le dispositif virtuel Citrix ADM est redémarré, arrêtez toutes les machines virtuelles sur l'hôte KVM et effectuez les opérations suivantes sur l'hôte KVM :

1. Supprimez le module `kvm_intel` à l'aide de la commande suivante :

```
rmmod kvm_intel
```

2. Désactivez ApiCV et rechargez le module `kvm_intel` à l'aide de la commande suivante :  

```
modprobe kvm_intel enable_apicv=n
```
3. Démarrez les machines virtuelles sur l'hôte KVM.

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

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

#### Remarque

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

2. À l'invite, tapez : `shell`
3. Tapez **networkconfig** pour entrer dans le menu de configuration réseau initiale Citrix ADM. Configurez l'adresse IP de gestion.
4. Pour terminer la configuration réseau initiale de Citrix ADM, suivez les instructions. La console affiche les options de configuration réseau initiale Citrix ADM permettant de définir les paramètres suivants pour Citrix ADM. Le nom d'hôte est renseigné par défaut.
  - a) Entrez **2** pour mettre à jour Citrix ADM IPv4 adresse - adresse IP de gestion à laquelle vous accédez à un Citrix ADM
  - b) Entrez **3** pour mettre à jour le masque de sous-réseau associé à l'adresse IP de gestion
  - c) Entrez **4** pour mettre à jour l'adresse IPv4 de Gateway - adresse IP de passerelle par défaut pour le sous-réseau de l'adresse IP de gestion de l'Citrix ADM
  - d) Entrez **7** pour enregistrer et quitter - enregistre vos modifications de configuration et quitte le système.

```
-----
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 [ADMHA1]:
 2. Citrix ADM IPv4 address [10.102.29.52]:
 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]:
```

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

```
-----
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deployment.
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]:
```

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

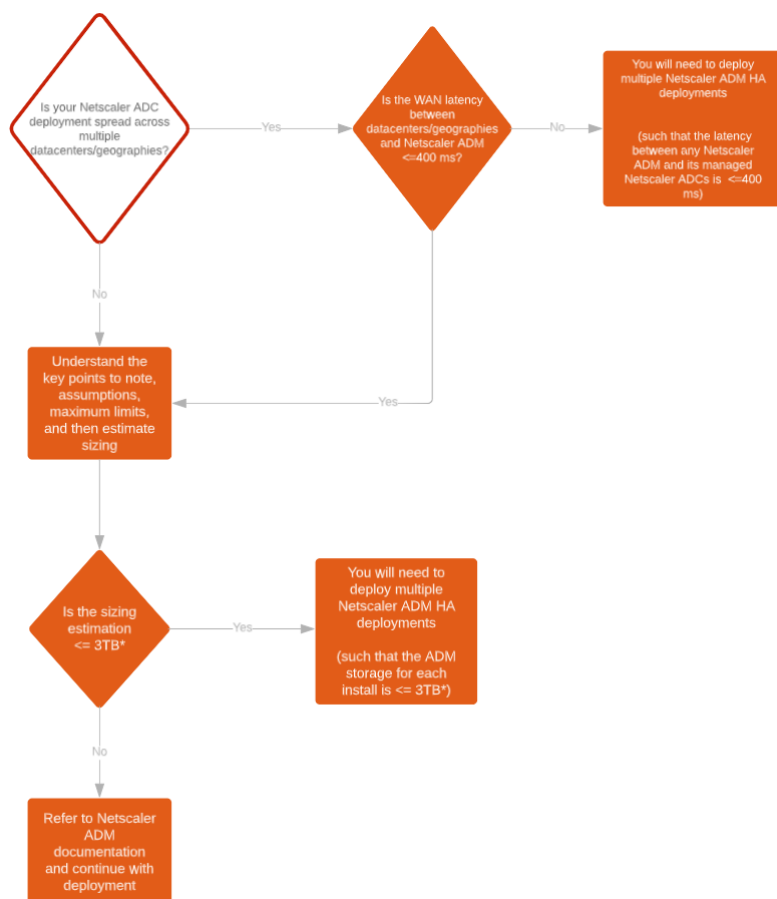
Vous pouvez accéder ultérieurement à Citrix ADM en tapant l'adresse IP du serveur Citrix ADM dans la barre d'adresse de votre navigateur. Les informations d'identification d'administrateur par défaut pour se connecter au serveur sont `nsroot/nsroot`.

## Configurer le déploiement haute disponibilité

February 1, 2024

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

## Scénario de déploiement



### Remarque

La limite de stockage maximale validée pour un seul déploiement Citrix ADM HA est de 3 To. Pour plus d'informations, consultez le [guide de déploiement](#).

### Important

**Pour accéder à Citrix ADM 12.1 build 48.18 ou à des versions ultérieures à l'aide du protocole HTTPS :**

Si vous avez configuré une instance Citrix ADC pour équilibrer la charge de Citrix ADM en mode haute disponibilité, supprimez d'abord l'instance Citrix ADC. Configurez ensuite une adresse IP

flottante pour accéder à Citrix ADM en mode haute disponibilité.

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

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

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

---

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

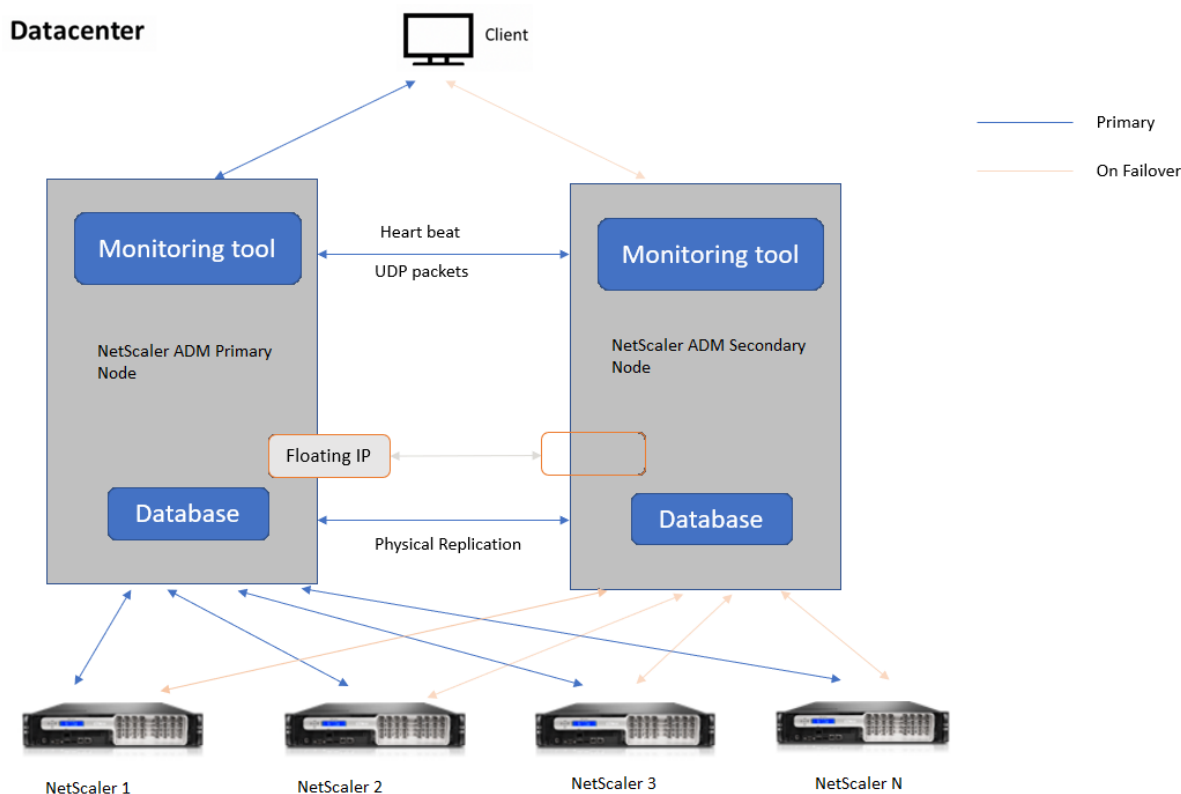
Termes	Description
Adresse IP flottante	Une adresse IP flottante est une adresse IP qui peut être déplacée instantanément d'un nœud à un autre dans le même sous-réseau. En interne, il est configuré en tant qu'alias sur l'interface réseau du nœud principal. En cas de basculement, l'adresse IP flottante 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 illustre l'architecture de deux nœuds Citrix ADM déployés en mode haute disponibilité.



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

### Outil de surveillance

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

### Nœud principal

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



## Nœud secondaire

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

## Réplication physique en continu

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

## Messages sur les battements cardiaques

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

## Adresse IP flottante

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

## Points clés à noter

- Dans une configuration haute disponibilité, les deux nœuds Citrix ADM sont déployés en mode actif-passif. Ils doivent être sur les mêmes sous-réseaux utilisant la même version du logiciel et la même génération, et avoir les mêmes configurations.

- Adresse IP flottante :
  - L'adresse IP flottante est configurée sur le nœud principal.
  - Les instances n'ont pas besoin d'être reconfigurées en cas de basculement.
  - Vous pouvez accéder à un nœud haute disponibilité depuis l'interface utilisateur, soit en utilisant l'adresse IP du nœud principal, soit en utilisant l'adresse IP flottante.

**Remarque**

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

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

**Remarque**

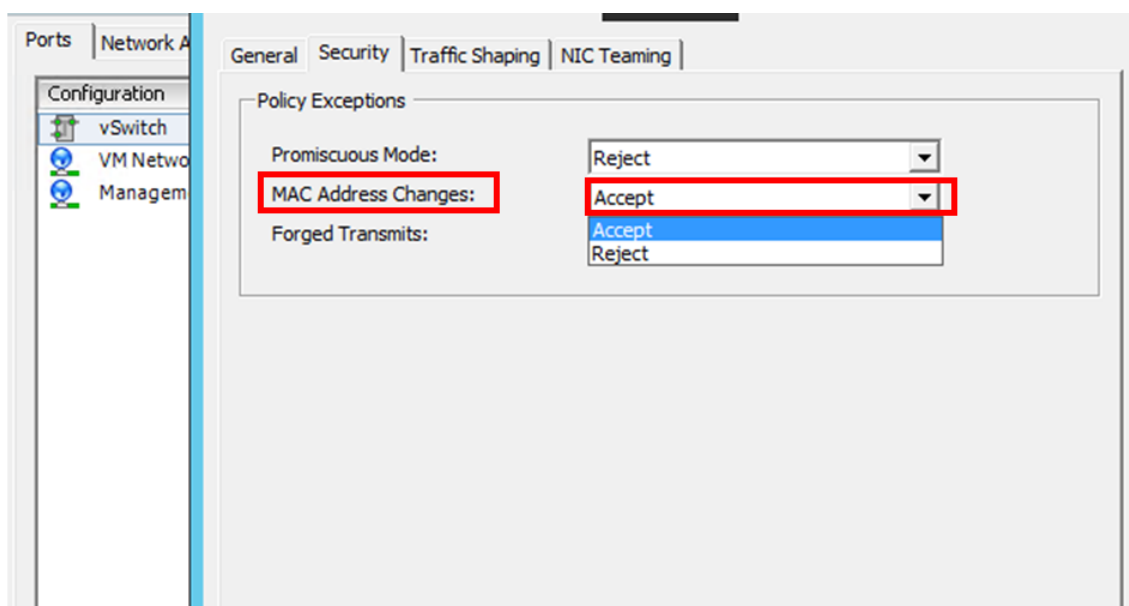
Une fois la mise à niveau réussie, vous devez configurer l'adresse IP flottante.

- Le port UDP par défaut 5005 est disponible sur les deux nœuds pour l'envoi de pulsations et pour la réception de messages.

- Adresse MAC

Le paramètre de l'option « Changements d'adresse MAC » dans un hyperviseur affecte le trafic reçu par une machine virtuelle. Autoriser l'activation des modifications d'adresse MAC sur le commutateur virtuel afin que l'adresse IP flottante se déplace en toute transparence vers le nouveau nœud principal après le basculement.

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



## Conditions préalables

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

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

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

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

Composant	Exigences
RAM	<b>32 GB</b>
CPU virtuel	<b>8 processeurs</b>

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

### Pour configurer Citrix ADM en mode haute disponibilité

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

### Enregistrer et déployer le premier serveur (nœud principal)

Pour enregistrer le premier nœud :

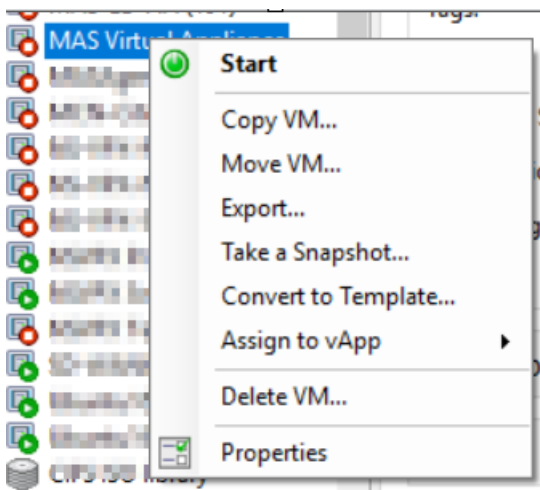
1. Utilisez le fichier image .xva téléchargé depuis le site de téléchargement de Citrix et importez-le dans votre hyperviseur.

**Remarque**

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

Preparing to Import VM

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



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

```

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 [ADMHA1]:
2. Citrix ADM IPv4 address [10.102.29.52]:
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 [?]:
    
```

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 connecté, si vous souhaitez mettre à jour la configuration réseau initiale, tapez `networkconfig`, mettez à jour la configuration et enregistrez-la.

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

```
-----
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deployment.
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]: █
```

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

```
bash-3.2# /mps/deployment_type.py
-----
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deployment.
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]: █
```

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

```
-----
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deployment.
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█
```

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

```

-----
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deployment.
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
First Server Node for Citrix ADM [yes/no]:yes

```

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

```

-----
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deployment.
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
First Server Node for Citrix ADM [yes/no]:yes
Restart the system for the configuration to take effect. Do you want to restart?
[yes/no]:yes

```

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

### Inscrire et déployer le deuxième serveur (nœud secondaire)

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

### Remarque

Une fois connecté, si vous souhaitez mettre à jour la configuration réseau initiale, tapez `networkconfig`, mettez à jour la configuration et enregistrez-la.

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

```

-----
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deployment.
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
First Server Node for Citrix ADM [yes/no]:no

```

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

```

-----

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
First Server Node for Citrix ADM [yes/no]:no

-----

Server node Configuration. This menu allows you to specify server ip address and password.
Enter 0 anytime for cancel and quit.
-----

Enter Citrix ADM IP Address:10.102.29.52
Enter password for Citrix ADM:

```



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

```
-----
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
First Server Node for Citrix ADM [yes/no]:no

-----
Server node Configuration. This menu allows you to specify server ip
address and password.
Enter 0 anytime for cancel and quit.
-----

Enter Citrix ADM IP Address:10.102.29.52
Enter password for Citrix ADM:
Enter Floating IP address:10.102.29.97
```

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

#### Remarque

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

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

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

#### Remarque

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

### Pour déployer des nœuds en tant que paire haute disponibilité :

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

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

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

Remarque :

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

7. Connectez-vous à Citrix ADM à l'aide des informations d'identification de l'administrateur, cliquez sur **Get Started** sur la page d'accueil et, si vous le souhaitez, effectuez les opérations suivantes :
  - a) Ajouter des instances de Citrix ADC
  - b) Configurer l'identité du client

Remarque :

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

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

Pour plus d'informations, consultez la [Foire aux questions](#).

## Désactiver la haute disponibilité

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

**Remarque**

Désactivez la haute disponibilité depuis le nœud principal.

### Pour désactiver la haute disponibilité :

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

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

## Redéployez la haute disponibilité

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

## Scénarios de basculement à haute disponibilité

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

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

## Scénario de cerveau divisé

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

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

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

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

### Remarque

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

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

## Configurer la reprise après sinistre pour une haute disponibilité

February 1, 2024

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

La fonctionnalité de reprise après sinistre (DR) de Citrix ADM 12.1 fournit des fonctionnalités complètes de sauvegarde et de restauration du système pour Citrix 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 Citrix ADM.

---

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

---

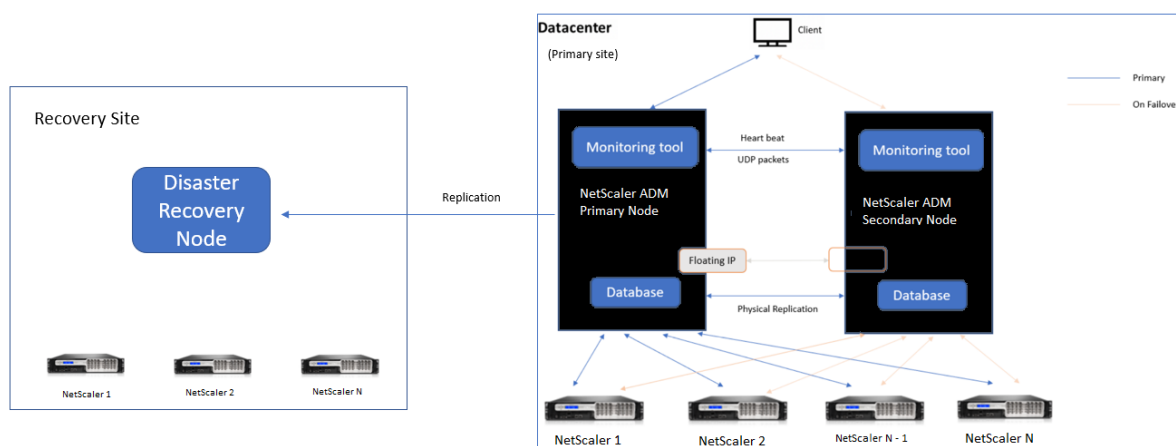
Remarque : Le site principal et le site de reprise après sinistre communiquent entre eux via les ports 5454 et 22, et ces ports sont activés par défaut.

Pour plus d'informations sur les ports et les protocoles, reportez-vous à la section [Ports](#).

## Workflow de reprise après sinistre

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

### Configuration initiale avant sinistre



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

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

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

### Conditions préalables

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

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

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

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

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

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

## Première configuration de la reprise après sinistre

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

### Déployer Citrix ADM en mode haute disponibilité

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

#### Remarque

- Citrix ADM déployé en mode haute disponibilité doit être mis à niveau vers la version 12.1 de Citrix 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 Citrix ADM

Pour enregistrer le nœud de reprise après sinistre Citrix ADM :

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

#### Remarque

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

```
-----
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 [DR]:
 2. Citrix ADM IPv4 address [10.102.29.53]:
 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]: █
```

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

```
bash-3.2# /mps/deployment_type.py
-----
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deployment.
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 deployment.
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.
```

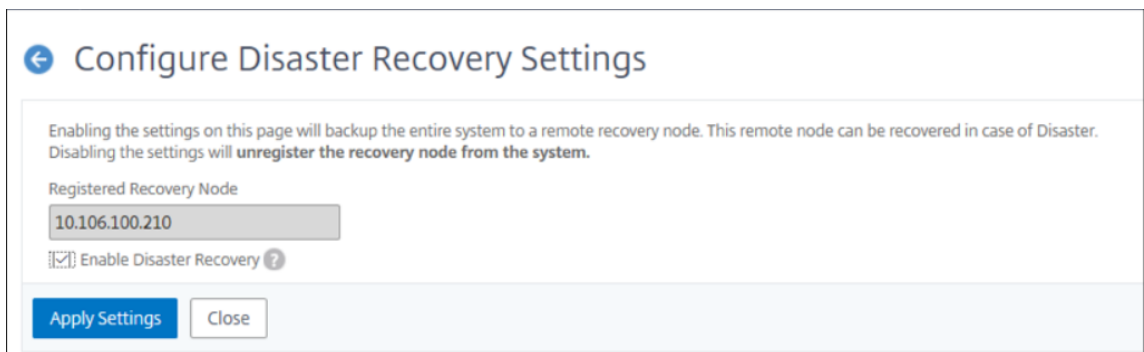
**Remarque**

Le nœud de reprise après sinistre n’a pas d’interface graphique.

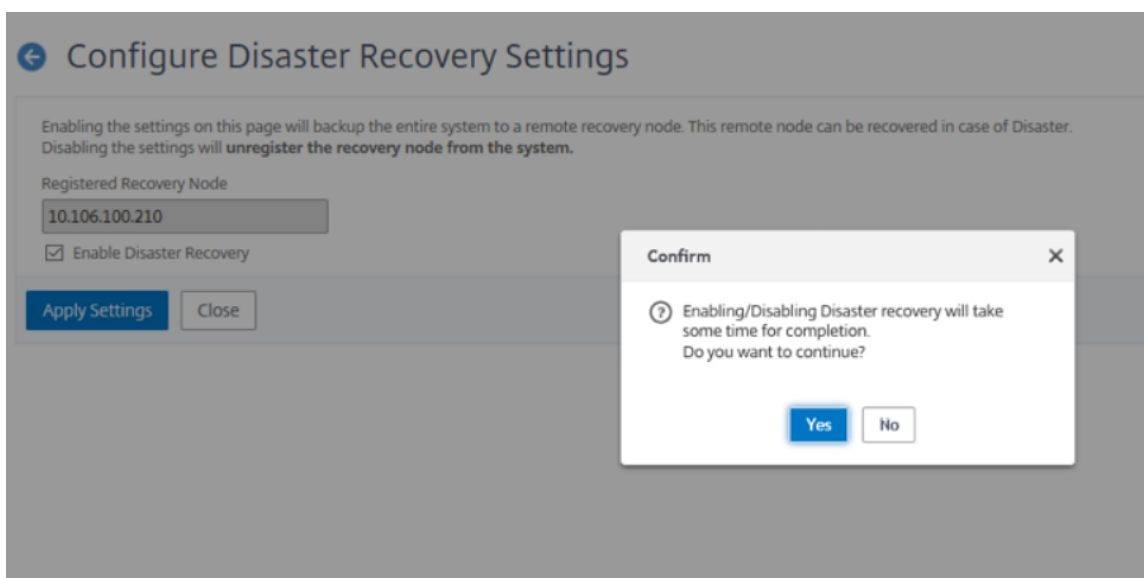
**Activer les paramètres de reprise après sinistre à partir de l’interface graphique Citrix ADM**

Une fois le nœud de reprise après sinistre enregistré avec succès, vous pouvez activer les paramètres de reprise après sinistre depuis l’interface utilisateur du site principal de Citrix ADM.

1. Accédez à **Système > Administration système > Paramètres de reprise après sinistre**.
2. Dans la page **Configurer les paramètres de reprise après sinistre**, activez la case à cocher **Activer la reprise après sinistre**, puis cliquez sur **Appliquer les paramètres**.



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 la liaison WAN (Wide Area Network).

Pour désactiver les paramètres de reprise après sinistre, **désactivez la case à cocher Activer la reprise après sinistre** et cliquez sur **Appliquer les paramètres**.

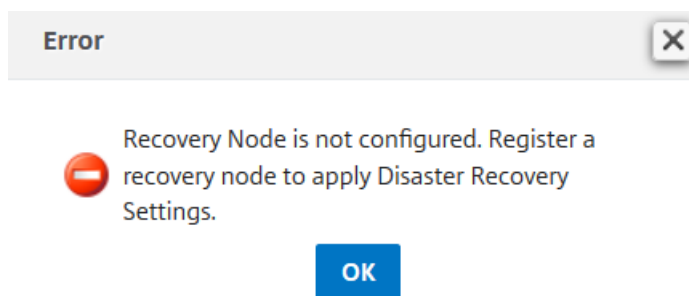
Une boîte de dialogue de confirmation s'affiche. Cliquez sur **Oui** pour continuer.

### Important

- Il incombe à l'administrateur de détecter qu'un sinistre s'est produit sur le site principal.
- Le flux de travail de reprise après sinistre n'est pas automatisé et l'administrateur doit le lancer manuellement après la panne du site principal.
- 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 sur le site principal, vous devez mettre à niveau manuellement le nœud autonome sur le site DR.

Si vous désactivez l'option **Activer la reprise après sinistre** et que vous cliquez sur **Appliquer les paramètres**, Citrix ADM ne vous permet pas de sélectionner à nouveau l'option **Activer la reprise après sinistre**.

Le message d'erreur suivant s'affiche lorsque vous cliquez sur **Paramètres de reprise après sinistre** :



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

- a) Connectez-vous au nœud DR à l'aide d'un Hypervisor ou d'une console SSH.
- b) Configurez le nœud DR en suivant la procédure disponible sur Déployer et enregistrez le nœud de reprise après sinistre Citrix ADM.
- c) Activez l'option de reprise après sinistre.

Pour plus d'informations, consultez la [Foire aux questions](#).

## Flux de travail après le désastre

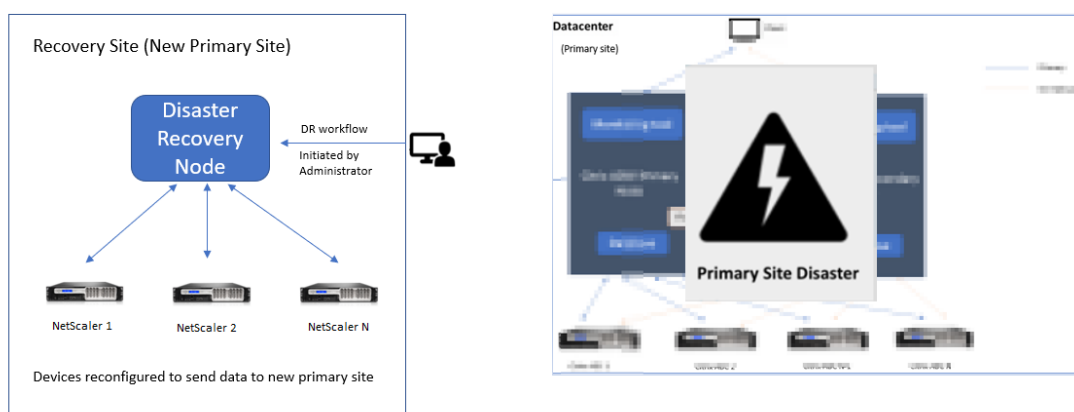
Lorsque le site principal tombe en panne après un sinistre, le flux de travail de reprise après sinistre doit être lancé comme suit :

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 le script de restauration suivant sur le nœud de reprise après sinistre (sur le site de reprise) : `/mps/scripts/pgsql/pgsql_restore_remote_backup.sh`

```
bash-3.2# sh /mps/scripts/pgsql/pgsql_restore_remote_backup.sh
```

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

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



Remarque :

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

## Reprise après sinistre

Une fois que le sinistre s'est produit et que l'administrateur a lancé le script de restauration, le site DR devient le nouveau site principal.

### Important

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

## Configurer les agents sur site pour un déploiement multisite

February 1, 2024

Dans les versions précédentes de Citrix ADM, les instances Citrix ADC déployées dans des centres de données distants pouvaient être gérées et surveillées à partir de Citrix ADM s'exécutant dans un centre de données principal. Les instances de Citrix ADC ont envoyé des données directement à l'NetScaler ADM principal, ce qui a entraîné une consommation de bande passante WAN (Wide Area Network). En outre, le traitement des données analytiques utilise les ressources du processeur et de la mémoire du Citrix ADM principal.

Les clients ont leurs centres de données situés dans le monde entier. Les agents jouent un rôle essentiel dans les scénarios suivants où les clients peuvent choisir :

- pour installer des agents dans des centres de données distants afin de réduire la consommation de bande passante du WAN.
- pour limiter le nombre d'instances qui envoient directement du trafic au Citrix ADM principal à des fins de 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 Citrix ADC au Citrix ADM principal.

- Si vous avez installé des agents pour le ou les centres de données distants, la communication entre les agents et le site principal s'effectue via une adresse IP flottante. Pour plus d'informations, reportez-vous à la section [port](#).
- Vous pouvez installer des agents et appliquer des licences groupées aux instances du ou des centres de données distants. Dans ce scénario, la communication entre le site principal et le ou les centres de données distants s'effectue via l'adresse IP flottante.

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

### Remarque

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

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

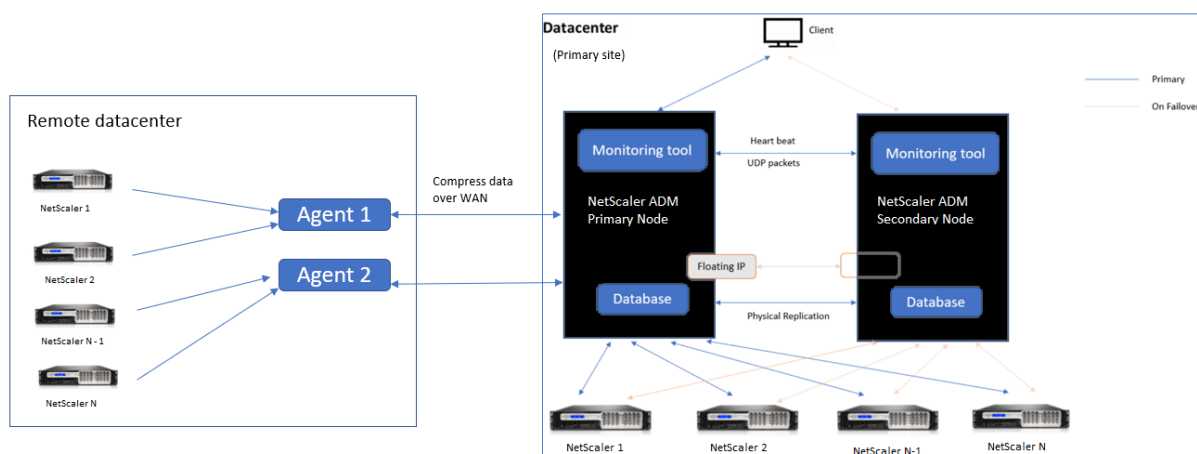
- Les instances sont configurées pour les agents de sorte que les données non traitées soient envoyées directement aux agents au lieu de Citrix ADM principal. Les agents effectuent le premier niveau de traitement des données et envoient les données traitées au format compressé au Citrix ADM principal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

### Remarque

Le nombre d'agents à installer par site dépend du trafic traité. Citrix a actuellement validé deux agents par site pour le scénario de basculement des agents. Citrix recommande d'installer au moins deux agents par site afin que le trafic soit acheminé vers un autre agent en cas de basculement d'un agent.

## Architecture

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



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

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

### Mise en route

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

### Installation de l'agent dans un centre de données

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

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

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

#### Remarque

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

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

---

Composant	Exigences
RAM	8 GB <b>Remarque</b> : Citrix vous recommande d'augmenter la valeur par défaut à 32 Go pour de meilleures performances.
CPU virtuel	2 processeurs <b>Remarque</b> : Citrix vous recommande d'augmenter la valeur par défaut à 8 processeurs pour de meilleures performances.
Espace de stockage	30 GB
Interfaces réseau virtuelles	1
Débit	1 Gbit/s

---

#### Ports

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

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

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

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



## Enregistrer l'agent

1. Utilisez le fichier image de l'agent téléchargé à partir du site de téléchargement Citrix et importez-le dans votre Hypervisor. Le modèle de dénomination du fichier image de l'agent est le suivant, **MASAGENT-<HYPERVISOR>-<Version.no>**. Par exemple : **Masagent-XEN-12.1-XY.XVA**
2. Dans l'onglet **Console**, configurez Citrix ADM avec les configurations réseau initiales.
3. Entrez le nom d'hôte Citrix ADM, l'adresse IPv4 et l'adresse IPv4 de la passerelle. Sélectionnez l'option 7 pour enregistrer et quitter la configuration.

```

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 [ADMAGENT]:
2. Citrix ADM IPv4 address [10.102.29.214]:
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

```

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 d'enregistrement de l'agent Citrix ADM sont affichées comme indiqué dans l'image suivante.
6. Entrez l'adresse IP flottante Citrix ADM et les informations d'identification de l'utilisateur.

```

bash-3.2# /mps/register_agent_onprem.py
-----
Citrix ADM Agent Registration with Citrix ADM On-Prem Server. This menu allows you
to specify Citrix ADM Server IP Address and admin credentials.
If Citrix ADM is deployed in HA mode, it is advisable to register with Citrix AD
M floating IP Address.
-----
Enter IP Address or URL:10.102.29.211
Enter User Name:nsroot
Enter Password:

Trying to register this agent with Citrix ADM 10.102.29.211
Dec  3 18:07:52 <auth.notice> ns date: date set by nsrecover
-----
Citrix ADM Agent Registration successful.

```

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

Une fois l'agent redémarré, accédez à l'interface graphique Citrix ADM. Dans le menu principal, accédez à **la page Réseaux** Agents pour vérifier l'état de l'agent. L'agent nouvellement ajouté est affiché

à l'état **Up**.

#### Remarque

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

### Ajouter un agent au site

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

#### Remarque

- Par défaut, tous les agents nouvellement enregistrés sont ajoutés au centre de données par défaut.
- Il est important d'associer l'agent au bon site. En cas de défaillance d'un agent, les instances Citrix ADC qui lui sont affectées sont automatiquement commutées vers d'autres agents fonctionnels sur le même site.

### Ajouter des instances de Citrix ADC

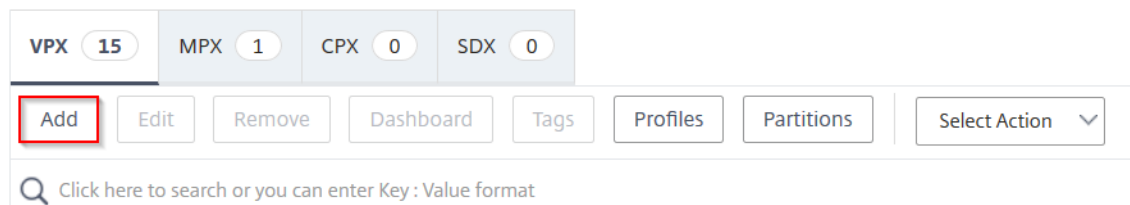
Les instances sont des appliances Citrix ou des appliances virtuelles que vous souhaitez découvrir, gérer et surveiller depuis Citrix ADM via des agents. Vous pouvez ajouter les appliances Citrix et les appliances virtuelles suivantes à Citrix ADM ou aux agents :

- Citrix ADC MPX
- Citrix ADC VPX
- Citrix ADC SDX
- Citrix ADC CPX
- Citrix Gateway
- Citrix Secure Web Gateway
- Citrix SD-WAN WO

## Ajouter une nouvelle instance

1. Accédez à **Réseaux > Instances** et sélectionnez le type d'instance. Par exemple, Citrix ADC.
2. Cliquez sur **Ajouter** pour ajouter une nouvelle instance.

### Citrix ADC



3. Cochez la case **Entrer l'adresse IP de l'appareil** et entrez l'adresse IP.
4. Dans Nom du **profil**, sélectionnez le profil d'instance approprié ou créez un nouveau profil en cliquant sur l'icône+.

#### Remarque

Pour chaque type d'instance, un profil par défaut est disponible. Par exemple, le profil ns-root-profile est le profil par défaut pour les instances Citrix ADC.

5. Sélectionnez le **site** auquel vous souhaitez associer l'instance.

#### Remarque

En fonction du site sélectionné, la liste des agents associés à ce site s'affiche. Assurez-vous de sélectionner le **site** auquel vous souhaitez associer l'instance.

## ← Add Citrix ADC VPX

Enter Device IP Address     Import from file

Enter one or more hostnames, IP addresses , and/or a range of IP addresses (for example, 10.102.40.30-10.102.40.45) using a comma separator.

IP Address\*

 ?

Profile Name\*

Site\*

Agent

 >

Tags

  +

6. Cliquez sur **pour sélectionner l'agent**. Sur la page **Agent**, sélectionnez l'agent auquel vous souhaitez associer l'instance, puis cliquez sur **Sélectionner**.

Agents								
<input checked="" type="button" value="Select"/> <input type="button" value="View Details"/> <input type="button" value="Delete"/> <input type="button" value="Rediscover"/> <input type="button" value="Attach Site"/>								
<input type="text" value="Click here to search or you can enter Key : Value format"/>								
	IP Address	Host Name	Version	State	Platform	Country	Region	City
<input checked="" type="radio"/>		AGENT	12.1-50.28	● Up	XenServer	--	--	--

7. Sur la page Ajouter Citrix VPX, cliquez sur **OK**.

## ← Add Citrix ADC VPX

Enter Device IP Address     Import from file

Enter one or more hostnames, IP addresses , and/or a range of IP addresses (for example, 10.102.40.30-10.102.40.45) using a comma separator.

IP Address\*

10.102.29.70 ?

Profile Name\*

ns\_nsroot\_profile Add Edit

Site\*

Default Add Edit

Agent

10.102.29.214 >

Tags

Key Value +

OK Close

### Mettre à jour une instance existante pour l'associer à un agent

Si une instance est déjà ajoutée au Citrix ADM principal, vous pouvez l'associer à un agent en modifiant le flux de travail d'ajout d'instances et en sélectionnant un agent.

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

#### Remarque

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

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

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

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

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

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

#### **Important**

L'ajout d'un agent pour les instances Citrix ADC dans les centres de données distants est recommandé mais pas obligatoire.

Si vous souhaitez ajouter l'instance directement au MAS principal, ne sélectionnez pas **d'agent** lors de l'ajout d'instances.

### **Regroupez l'agent**

Le terme **cluster d'agents** fait référence à un mécanisme dans lequel les agents attachés à un site sont regroupés de manière logique, de sorte qu'en cas de défaillance de l'un des agents, les instances Citrix ADC qui lui envoient du trafic sont automatiquement reconfigurées pour commencer à envoyer du trafic aux autres agents sains de ce groupe ou site.

L'avantage d'avoir des agents regroupés sur un site distant est que si un agent échoue, celui-ci est détecté par Citrix ADM et implicitement, toutes les instances sont redistribuées aux autres agents disponibles dans ce cluster.

Par exemple, nous avons deux agents 10.106.1xx.2x et 10.106.1xx.7x qui sont attachés et opérationnels sur le site de Bangalore, comme indiqué ci-dessous.

#### **Si un agent tombe en panne, Citrix ADM le détecte et affiche l'état comme étant inactif.**

Les instances attachées à cet agent sont automatiquement reconfigurées pour utiliser l'autre agent du même cluster comme destination du trap, serveur Syslog, etc.

#### **Remarque**

Il y aura un certain retard lors de la reconfiguration des instances.

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

February 1, 2024

Vous pouvez mettre à niveau votre serveur unique Citrix ADM vers un déploiement haute disponibilité de deux serveurs Citrix ADM. Une paire de serveurs Citrix ADM à haute disponibilité est en mode actif-passif, et les deux serveurs ont la même configuration. Dans ce type de déploiement actif-passif, un

serveur Citrix ADM est configuré en tant que nœud principal et l'autre en tant que nœud secondaire. Si, pour une raison quelconque, le nœud principal tombe en panne, le nœud secondaire prend le relais.

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

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

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

### Modifier le nœud de serveur Citrix ADM existant

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

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

```
bash-3.2# /mps/deployment_type.py
-----
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deployment.
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. 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.

```
Selected Option      1. Citrix ADM Server.
Citrix ADM Standalone deployment [yes/no]:no
First Server Node for Citrix ADM [yes/no]:yes
Restart the system for the configuration to take effect. Do you want to restart?
[yes/no]:yes
```

## Provisionner le deuxième nœud de serveur

Vous devez provisionner le second serveur sur votre Hypervisor. Utilisez le même fichier image que celui que vous avez utilisé pour installer le premier serveur ou procurez-vous un fichier image de la même version sur le site de téléchargement de Citrix.

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

```
-----
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 en tant que **serveur Citrix ADM**.
4. La console de déploiement vous invite à sélectionner le déploiement du serveur (en tant que serveur autonome). Tapez **Non** pour confirmer le déploiement comme paire haute disponibilité.



```

bash-3.2# /mps/deployment_type.py
-----
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deployment.
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.

```

-----
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deployment.
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
First Server Node for Citrix ADM [yes/no]:no

```

6. Entrez l'adresse IP et le mot de passe du premier serveur.

```

-----
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
First Server Node for Citrix ADM [yes/no]:no

-----
Server node Configuration. This menu allows you to specify server ip
address and password.
Enter 0 anytime for cancel and quit.
-----

Enter Citrix ADM IP Address:10.102.29.52
Enter password for Citrix ADM:

```

7. Entrez l'adresse IP flottante du premier nœud.

```

-----
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
First Server Node for Citrix ADM [yes/no]:no

-----
Server node Configuration. This menu allows you to specify server ip
address and password.
Enter 0 anytime for cancel and quit.
-----

Enter Citrix ADM IP Address:10.102.29.52
Enter password for Citrix ADM:
Enter Floating IP address:10.102.29.97

```

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

## Déployer les deux serveurs en mode haute disponibilité

Pour terminer le processus d'installation des deux nœuds de serveur en tant que paire haute disponibilité, vous devez déployer ces nœuds à partir de l'interface graphique du nœud de serveur Citrix ADM existant précédemment. La communication interne entre les deux serveurs démarre lorsque vous déployez les deux nœuds de serveur.

1. Dans un navigateur Web, tapez l'adresse IP du nœud serveur Citrix ADM existant précédemment.

2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Sous l'onglet **Système**, accédez à **Déploiement** et cliquez sur **Déployer**.
4. Un message de confirmation s'affiche. Cliquez sur **Oui**.

#### Remarque

Après avoir déployé Citrix ADM en haute disponibilité, vous pouvez accéder au nœud principal à l'aide de l'adresse IP flottante. Vous ne pouvez pas accéder au nœud secondaire à partir de la version 12.1.

5. Bien que vous ayez saisi l'adresse IP flottante lors de la configuration du deuxième nœud de serveur, vous avez la possibilité de mettre à jour le FIP sur la page **Systèmes**. Cliquez sur **Paramètres HA > Configurer l'adresse IP flottante pour le mode haute disponibilité**. Vous pouvez afficher l'adresse IP flottante que vous avez configurée précédemment. Vous pouvez entrer une nouvelle adresse IP et cliquer sur **OK**.

## Migrer de NetScaler Insight Center vers Citrix ADM

February 1, 2024

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

#### Remarque

La migration n'est actuellement prise en charge que sur les instances NetScaler Insight Center Standalone.

### Conditions préalables

Avant de migrer l'apppliance virtuelle NetScaler Insight Center vers Citrix ADM, vérifiez que les conditions suivantes ont été remplies :

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

### Remarque

Vous devez installer Citrix ADM 12.0 build 57.24, puis effectuer une mise à niveau vers la dernière version de Citrix ADM 12.1. Pour plus d'informations, consultez la section [Mettre à niveau](#).

- Vous avez téléchargé le dernier fichier d'image .tgz de génération Citrix ADM 12.1.

## Configuration matérielle requise

Composant	Exigences
RAM	32 GB
CPU virtuel	8 processeurs
Espace de stockage	120 GB
	<b>Remarque</b> Citrix vous recommande d'utiliser <b>500 Go</b> pour de meilleures performances. Citrix recommande également d'utiliser la technologie SSD (Solid State Drive) pour les déploiements Citrix ADM.
Interfaces réseau virtuelles	1
Débit	1 Gbit/s ou 100 Mbit/s
Exigences relatives à l'hyperviseur	
Citrix Hypervisor	6.2, 6.5
VMware ESX	5.5, 6.0
Microsoft Hyper-V	2012 R2
Linux - KVM	Ubuntu, Fedora

## Procédure d'installation

### Pour migrer NetScaler Insight Center vers Citrix ADM :

1. Connectez-vous à l'invite shell de NetScaler Insight Center.
2. Téléchargez la version 57.24 de Citrix ADM 12.0 dans le dossier `/var/mps/mps_images`.
3. Décompressez le fichier TGZ à l'aide de la commande **tar -zxvf build-mas-12.0-57.24.tgz**.

```
bash-3.2# tar -zxvf build-mas-12.0.57.24.tgz
```

4. Installez Citrix ADM à l'aide de `./installmas`.

```
bash-3.2# ./installmas
```

5. Après avoir installé Citrix ADM 12.0 build 57.24, vous devez effectuer la mise à niveau vers la dernière version de Citrix ADM 12.1 en suivant les étapes ci-dessus.

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

#### Remarque

Dans Citrix ADM, par défaut, la gestion et la surveillance de 30 serveurs virtuels créés dans les instances NetScaler découvertes sont gratuites. Pour surveiller et gérer plus de 30 serveurs virtuels, installez les licences MAS requises. Pour plus de détails, consultez la section [Système de licences Citrix ADM](#).

## Migrer les configurations du Command Center vers Citrix ADM

February 1, 2024

Vous pouvez désormais migrer les configurations de votre Command Center vers Citrix Application Delivery Management (ADM) sans perdre la configuration, les paramètres ou les données existants de votre déploiement Command Center et de votre déploiement Citrix ADM. Vous pouvez consulter les configurations du Command Center migrées dans Citrix ADM une fois le processus de migration terminé.

### Points à noter

- La migration des configurations du Command Center vers Citrix ADM est prise en charge dans les déploiements suivants :

- Déploiement autonome du Command Center vers Citrix ADM autonome ou déploiement haute disponibilité de Citrix ADM.
- De la haute disponibilité du Command Center au déploiement autonome de Citrix ADM ou au déploiement de haute disponibilité de Citrix ADM.

#### Remarque

Vous devez utiliser uniquement l'adresse IP du nœud principal du déploiement à haute disponibilité Command Center et Citrix ADM lors de la migration du déploiement autonome ou haute disponibilité de Command Center vers un déploiement à haute disponibilité ou autonome Citrix ADM.

- Vous pouvez exécuter l'outil Command Center plusieurs fois sur des déploiements Citrix ADM identiques ou différents :
  - Chaque fois que vous exécutez l'outil Command Center au-delà de la première fois pour le même Citrix ADM, les journaux apparaissent comme ayant échoué pour les configurations qui ont déjà été migrées et qui existent dans Citrix ADM.
  - Si une nouvelle configuration a été ajoutée dans le Centre de commandes depuis l'exécution de l'outil antérieur jusqu'à maintenant pour le même Citrix ADM, toutes ces configurations, à l'exception des nouvelles tâches personnalisées, seront migrées vers Citrix ADM.
- La migration des configurations de Command Center vers Citrix ADM est prise en charge pour les périphériques Citrix ADC, Citrix ADC SDX et Citrix SD-WAN WO.
- Toutes les communications entre Command Center et Citrix ADM se font via une connexion HTTPS.
- Il est vivement recommandé de sauvegarder les données existantes de Citrix ADM avant de migrer les configurations du Command Center.
- Une fois la migration du Command Center terminée, les partitions d'administration de Citrix ADC sont détectées automatiquement dans Citrix ADM.

## Limitations

Les configurations de Command Center suivantes ne sont pas migrées de l'appliance Command Center vers Citrix ADM :

- Fichiers de configuration de sauvegarde de périphérique
- Détails du délai d'expiration dans les profils d'appareils SD-WAN WO

- Les détails suivants sous les déclencheurs d'événement et d'alarme ne sont pas migrés :
  - Détails relatifs à l'annulation de l'exécution de la commande
  - Exécuter les détails de la tâche
  - Les déclencheurs dont tous les paramètres sont vides (gravité/catégorie/instances/objets de défaillance) ne sont pas migrés
  - Les déclencheurs dont les instances ont l'état cluster HA, principal et secondaire ne sont pas migrés si les trois états des instances sont sélectionnés
- Les tâches personnalisées sans description ne sont pas migrées
- Paramètres de gravité des événements
- Détails du calendrier des événements
- Filtres de suppression Syslog
- Détails des tâches de configuration
- Modèles d'audit
- Stratégies d'audit sans appareils
- Détails du calendrier de la stratégie d'audit
- Paramètres d'étendue autorisés par le RBAC des groupes
- Paramètres de surveillance et de gestion de la base de données
- Rapports personnalisés sur les performances
- Seuils de performance
- Vues personnalisées de Fault/Syslog/Reports/Entity Monitoring
- Rapports sur AppFirewall et NS Gateway et détails de leur calendrier
- Détails de configuration automatique SD-WAN WO
- Paramètres de haute disponibilité
- Paramètres de sauvegarde système programmés
- Paramètres de nouvelle tentative de base de données
- Heure programmée pour la purge de Syslog
- Toutes les données statistiques telles que le syslog, les événements et les journaux d'audit de tous les modules.

## Conditions préalables

Avant de migrer les configurations du Command Center vers Citrix ADM, assurez-vous que les conditions préalables suivantes sont remplies :

- Vous exécutez Command Center version 5.2 build 48.2 ou ultérieure.
- Vous avez installé et configuré Citrix ADM version 12.0 build 51.24 ou version ultérieure.
- Seul l'utilisateur administrateur exécutera la migration de configuration du Command Center.
- Pour une migration réussie des tâches personnalisées, le champ de description est obligatoire dans le Command Center.
- La communication entre le Command Center et Citrix ADM est basée sur NITRO. Vous devez configurer et ouvrir les paramètres de protocole SSL (Secure Socket Layer) et TLS (Transport Layer Security) nécessaires sur Command Center et Citrix ADM pour les communications NITRO.

### Remarque

Si vous utilisez une version de Command Center antérieure à 5.2 build 48.2, vous devez mettre à niveau la version de Command Center vers 5.2 build 48.2, puis migrer les configurations de Command Center vers Citrix ADM. Pour plus d'informations sur la mise à niveau du dispositif Command Center, reportez-vous à [la section Mise à niveau Command Center](#)

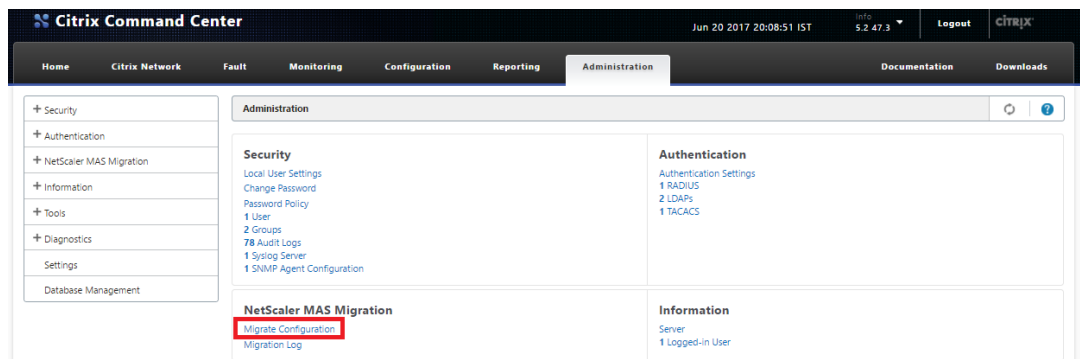
## Migrer les configurations

Pour migrer une configuration du Command Center vers Citrix ADM, vous avez besoin de l'adresse IP de l'appliance Command Center et des informations d'identification de l'administrateur.

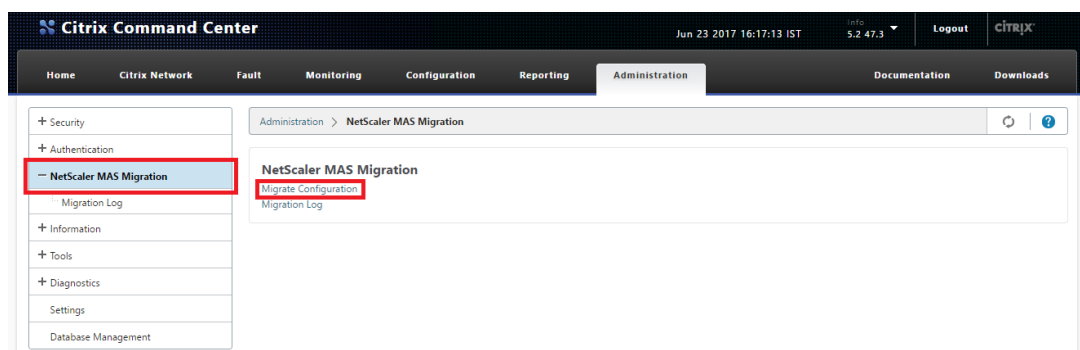
### Pour migrer les configurations du Command Center vers Citrix ADM, procédez comme suit :

1. Dans un navigateur Web, saisissez l'adresse IP de l'appliance Command Center.
2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification de l'administrateur et connectez-vous.
3. Après une connexion réussie, dans l'écran qui apparaît, sélectionnez l'onglet **Administration** et effectuez l'une des opérations suivantes :
  - Dans le volet droit, sous **Citrix ADM Migration** , sélectionnez **Migrer la configuration** , comme indiqué dans la figure suivante.





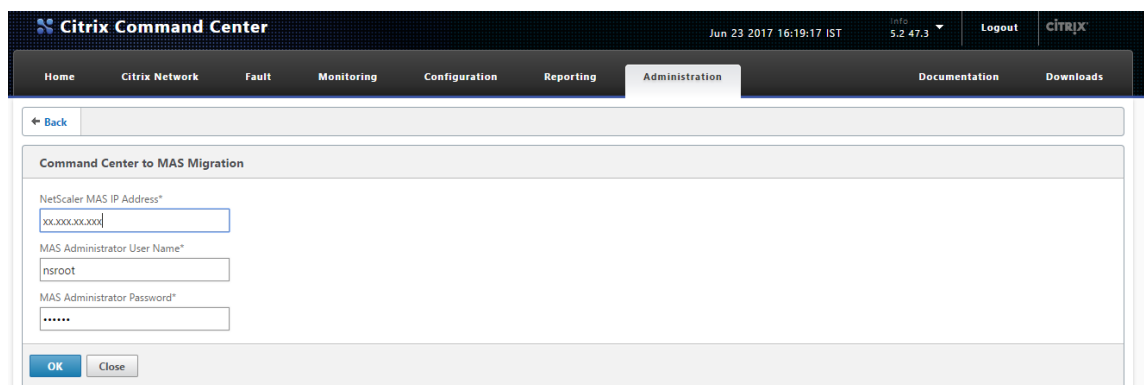
- Dans le volet gauche, sélectionnez **Citrix ADM Migration** , puis cliquez sur **Migrer la configuration** , comme illustré dans la figure suivante.



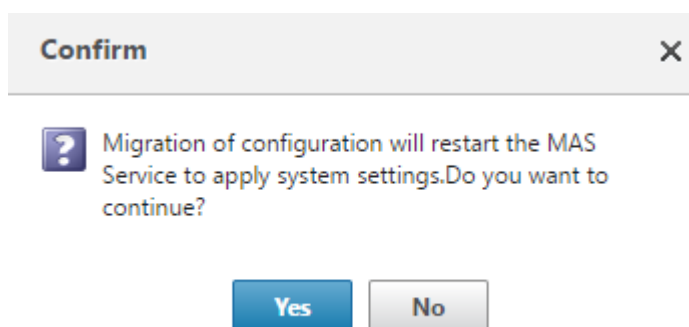
4. Dans la boîte de dialogue **de migration du Command Center vers MAS** , entrez l'adresse IP du serveur Citrix ADM et les informations d'identification de l'administrateur, puis cliquez sur **OK**.

### Remarque

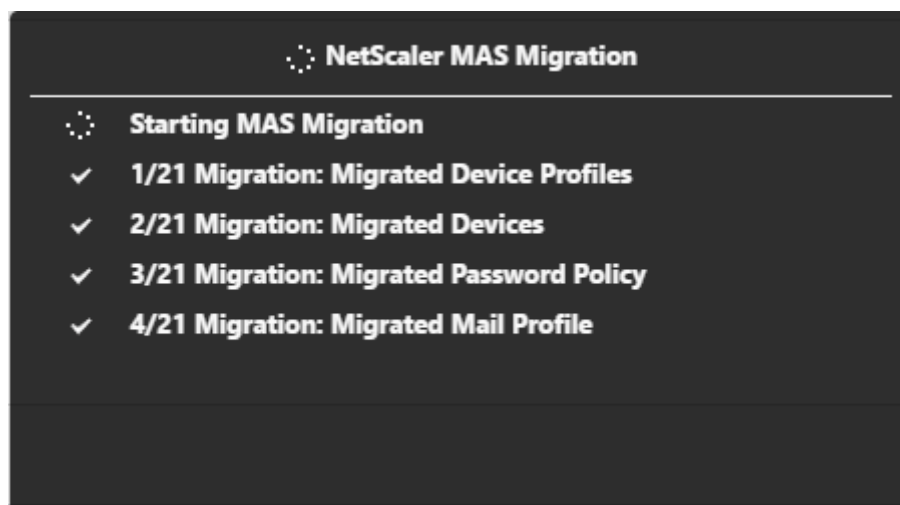
Dans le cas d'un déploiement haute disponibilité Citrix ADM, entrez l'adresse IP du nœud principal.



5. À l'invite de confirmation, cliquez sur **Oui**.



L'écran affiche la progression des tâches de migration.

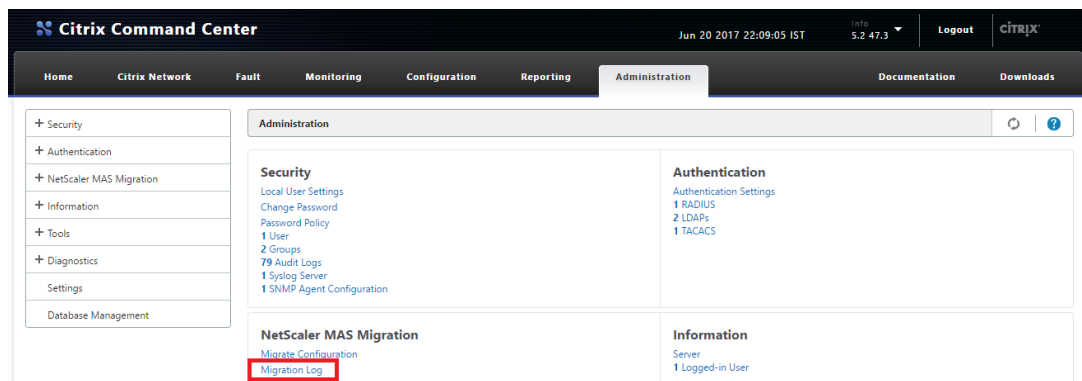


L'opération **Migration de la configuration** prend en entrée les détails du déploiement Citrix ADM et ses informations d'identification d'administrateur. L'opération **Migrate Configuration migre** ensuite la configuration du déploiement du Command Center vers le déploiement de Citrix ADM.

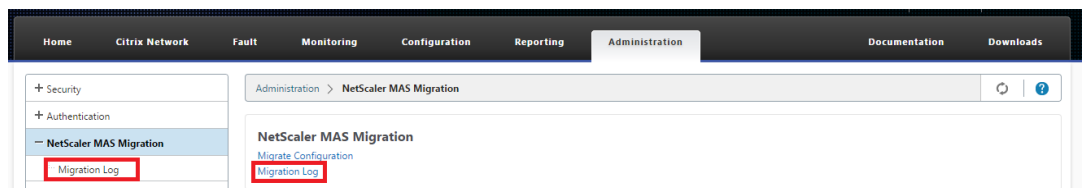
Lorsque les tâches sont terminées, vous pouvez vérifier la configuration du Command Center migrée à partir des journaux de migration du Command Center et des données Citrix ADM.

### **Pour utiliser les journaux de migration du Command Center pour vérifier la migration**

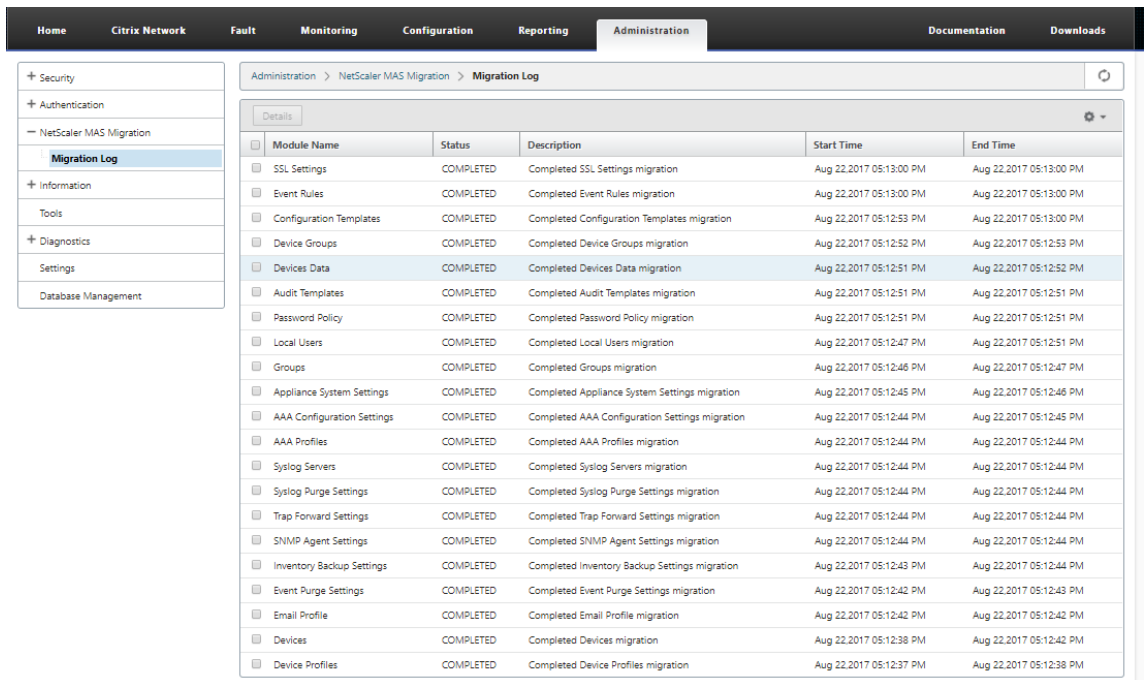
1. Dans l'interface graphique Command Center, sous l'onglet **Administration**, effectuez l'une des opérations suivantes :
  - Dans le volet droit, sous **Citrix ADM Migration**, cliquez sur **Journal** de migration.



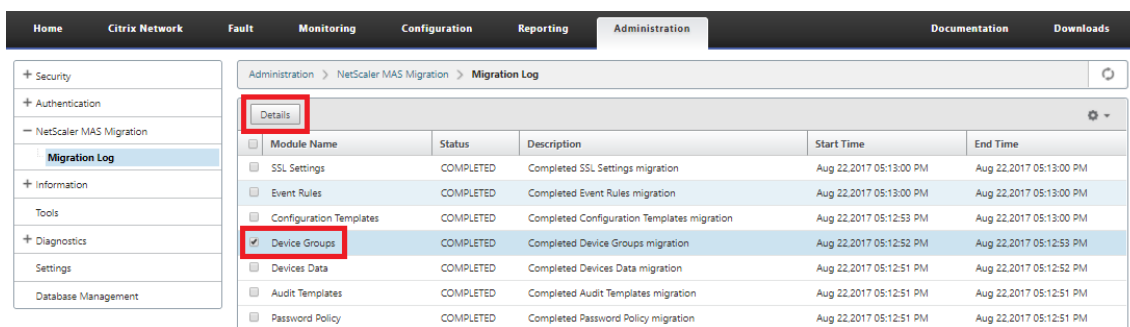
- Dans le volet de gauche, sélectionnez **Citrix ADM Migration** , puis cliquez sur **Journal de migration** .



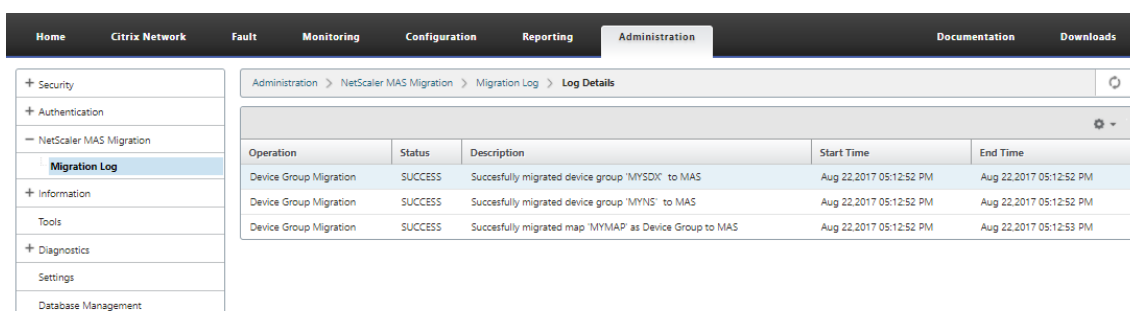
2. Consultez la liste des journaux de migration.



- 3. Pour afficher plus de détails, sélectionnez **Nom du module** ou pour afficher les détails d'un module particulier, sélectionnez ce module, puis cliquez sur **Détails**.



4. L'exemple suivant montre les détails du journal d'un module sélectionné.



## Pour utiliser Citrix ADM pour vérifier la migration

Au cours du processus de migration, les configurations du Command Center sont migrées vers Citrix ADM et sont affichées sous forme de configurations Citrix ADM dans l'interface graphique de Citrix ADM.

Une fois le processus de migration terminé, le serveur Citrix ADM redémarre et il se peut qu'il y ait un arrêt momentané. Lorsque le serveur Citrix ADM est opérationnel, accédez à l'interface graphique Citrix ADM en saisissant l'adresse IP du serveur Citrix ADM dans la barre d'adresse de votre navigateur.

Le tableau suivant montre comment la terminologie Citrix ADM pour les configurations migrées correspond à la terminologie utilisée dans Command Center.

### Terminologie du Command Center

### Terminologie Citrix ADM

Profils d'appareils

Profils d'instance

Les appareils et leur état (gérés/non gérés, par exemple)

Les instances et leur état (gérées/non gérées, par exemple)

Annotations sur les appareils

Annotations d'instance

Groupes d'appareils

Groupes d'instances

Cartes

Groupes d'instances

Terminologie du Command Center	Terminologie Citrix ADM
Déclencheurs d'événement et d'alarme	Règles de l'événement
Commandes de tâches intégrées et personnalisées	Modèles de configuration sous l'éditeur de création de tâches
Stratégies d'audit planifiées	Modèles d'audit
Stratégie de mot de passe	Stratégie de mot de passe
Utilisateurs (utilisateurs locaux uniquement)	Utilisateurs du système
Groupes*	Groupes de systèmes
Profils d'authentification et paramètres d'authentification	Profils d'authentification et configuration de l'authentification
Paramètres de messagerie	Serveur de messagerie/liste de distribution d'e-mails
Serveur Syslog	Serveur Syslog
Paramètres SSL	Paramètres SSL
Configuration de l'agent SNMP	gestionnaire SNMP
Paramètres Trap Forward	Réglages du trap
Paramètres de purge des événements	Paramètres de nettoyage des paramètres
Paramètres d'inventaire	Paramètres de sauvegarde de l'instance
Paramètres de purge Syslog	Paramètres de paramétrage de Syslog
Paramètres réseau de l'appliance tels que DNS, NTP et fuseau horaire	Paramètres réseau Citrix ADM tels que DNS, NTP et fuseau horaire

\*Les groupes disposant de toutes les autorisations dans le Command Center sont migrés en tant que groupes dotés d'un rôle « administrateur » dans Citrix ADM. Tous les autres groupes du Command Center sont migrés en tant que groupes dotés d'un rôle « en lecture seule » dans Citrix ADM.

## Intégrer Citrix ADM avec Citrix Director

February 1, 2024

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

- L'analyse du réseau permet d'obtenir des rapports HDX Insight auprès de Citrix ADM et fournit une vue d'application et de bureau du réseau. Grâce à cette fonctionnalité, Director fournit une

vue analytique avancée du trafic ICA dans votre déploiement.

- La gestion des performances fournit un archivage des données d'historique ainsi que des rapports de tendance. Avec la conservation de l'historique des données par rapport à l'évaluation en temps réel, vous pouvez créer des rapports de tendance, y compris des tendances de capacité et d'intégrité.

Une fois que vous avez intégré Citrix ADM à Director, les rapports HDX Insight vous fournissent les informations suivantes dans Director :

- L'onglet Réseau de la page Tendances indique les effets de latence et de bande passante pour les applications, les postes de travail et les utilisateurs tout au long de votre déploiement.
- La page Détails de l'utilisateur affiche des informations spécifiques à la latence et à la bande passante pour une session utilisateur particulière.

## Conditions préalables

### Configuration matérielle requise pour la migration HDX Insight vers Citrix ADM

---

Composant	Exigences
RAM	32 GB
CPU virtuel	8
Espace de stockage	500 GB. Citrix recommande d'utiliser la technologie SSD (Solid State Drive) pour les déploiements Citrix ADM.
Interfaces réseau virtuelles	1
Débit	1 Gbit/s ou 100 Mbit/s

---

### Exigences en matière de logiciels

Avant de migrer vers l'appliance virtuelle Citrix ADM, vérifiez que les conditions suivantes ont été remplies :

- La version 1811 de Director est installée
- NetScaler HDX Insight version 10.1 ou ultérieure est installé
- HDX Insight et Citrix ADM prennent en charge Citrix VDA version 7.0 et versions ultérieures
- Citrix Workspace est pris en charge sur Citrix Virtual Apps and Desktops version 7.0 et ultérieure

- Assurez-vous que MAC, Citrix Receiver pour Mac version 11.8 et versions ultérieures, et Windows Citrix Receiver pour Windows 14.0 et versions ultérieures sont disponibles pour afficher des métriques ICA RTT précises.
- Citrix ADM version 11.0 et ultérieure est installé. Pour plus d'informations sur la façon d'installer Citrix ADM, consultez [Déployer Citrix ADM](#).

## Limitations

- La disponibilité de cette fonctionnalité dépend de la licence de votre organisation et vos permissions d'administrateur.
- La session Round Trip Time (RTT) de l'ICA affiche correctement les données pour Citrix Receiver pour Windows 3.4 ou version ultérieure et pour Citrix Receiver pour Mac 11.8 ou version ultérieure. Pour les versions antérieures de ces Receiver, les données ne s'affichent pas correctement.
- Dans la vue Tendances, les données d'ouverture de session de connexion HDX ne sont pas collectées pour les VDA antérieurs à la version 7. Pour les VDA antérieurs, les données du graphique sont affichées en tant que 0.
- Pour les déploiements qui possèdent déjà un disque dur externe dont l'espace de stockage est inférieur à 500 Go, vous ne pouvez pas ajouter un autre disque dur.

### Remarque

- Pour plus d'informations sur Director et pour les étapes à suivre pour intégrer Citrix ADM à Director, reportez-vous à la section <http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-11/director.html>.
- Pour plus d'informations sur HDX Insight, reportez-vous à la section <http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-11/director/hdx-insight.html>.

## Joindre un disque supplémentaire à Citrix ADM

February 1, 2024

Les besoins en stockage de Citrix Application Delivery Management (ADM) sont déterminés en fonction de votre estimation de dimensionnement Citrix ADM. Par défaut, Citrix ADM vous fournit une capacité de stockage de 120 Go. Si vous avez besoin de plus de 120 Go pour stocker vos données, vous pouvez joindre un disque supplémentaire.

### Remarque

- Estimez les besoins en stockage et connectez un disque supplémentaire au serveur au moment du déploiement initial de Citrix ADM.
- Pour un déploiement Citrix ADM mono-serveur, vous ne pouvez attacher qu'un seul disque au serveur en plus du disque par défaut.
- Pour un déploiement haute disponibilité Citrix ADM, vous devez attacher un disque supplémentaire à chaque nœud. La taille des deux disques doit être identique.
- Si vous avez déjà rattaché un disque externe de capacité inférieure, vous devez le retirer avant de joindre un nouveau disque.
- Vous pouvez attacher un disque supplémentaire d'une capacité supérieure à 2 téraoctets. Si nécessaire, la taille du disque peut également être inférieure à 2 téraoctets.
- Citrix recommande d'utiliser la technologie SSD (Solid State Drive) pour les déploiements Citrix ADM.

Ce document explique les scénarios suivants concernant la connexion d'un nouveau disque supplémentaire, la création de partitions et le redimensionnement des disques supplémentaires :

1. Joindre un nouveau disque supplémentaire
2. Lancez l'outil de partitionnement de disque
3. Créez des partitions sur le nouveau disque supplémentaire
4. Redimensionner le disque supplémentaire existant
5. Supprimer les partitions sur le disque supplémentaire

### Joindre un disque supplémentaire dans un Citrix ADM autonome

Pour attacher un disque à la machine virtuelle, procédez comme suit :

1. Arrêtez la machine virtuelle Citrix ADM.
2. Dans l'Hypervisor, attachez un disque supplémentaire de la taille de disque requise à la machine virtuelle Citrix ADM.

Le disque nouvellement connecté stocke les données de base de données et les fichiers journaux Citrix ADM. Le disque par défaut existant de 120 gigaoctets est désormais utilisé pour stocker les fichiers principaux, les fichiers journaux du système d'exploitation, etc.

3. Démarrez la machine virtuelle Citrix ADM.



## Outil de partition de disque Citrix ADM

Citrix ADM fournit désormais l'**outil de partition de disque Citrix ADM**, un nouvel outil de ligne de commande. Les fonctionnalités de cet outil sont décrites en détail comme suit :

1. À l'aide de l'outil, vous pouvez créer des partitions dans le disque supplémentaire nouvellement ajouté.
2. Vous pouvez également redimensionner un disque supplémentaire existant à l'aide de cet outil. Mais le disque externe existant ne doit pas être supérieur à 2 téraoctets.

### Remarque

- Il n'est pas possible de redimensionner des disques existants au-delà de 2 téraoctets sans perdre de données. Cela est dû à une limitation connue de la plateforme.
- Pour créer une capacité de stockage supérieure à 2 téraoctets, vous devez supprimer les partitions existantes et créer des partitions à l'aide de ce nouvel outil.

3. À l'aide de ce nouvel outil, vous pouvez effectuer n'importe quelle action de partition sur le disque de manière explicite. L'outil vous offre une visibilité et un contrôle clairs sur le disque et les données associées.

### Remarque

Vous ne pouvez utiliser cet outil que sur le disque supplémentaire que vous avez connecté au serveur Citrix ADM. Vous ne pouvez pas créer de partitions sur le disque principal (par défaut) de 120 gigaoctets à l'aide de cet outil.

## Lancez l'outil de partition de disque

1. Ouvrez une connexion SSH à Citrix ADM à l'aide d'un client SSH, tel que PuTTY.
2. Ouvrez une session sur Citrix ADM à l'aide des informations d'identification de l'administrateur.
3. Passez à l'invite shell et tapez :

```
1 /mps/DiskPartitionTool.py
2 <!--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 Citrix ADM dans le cadre d'un déploiement haute disponibilité, vous devez lancer l'outil sur les deux nœuds et créer ou redimensionner des partitions après avoir attaché des disques aux machines virtuelles respectives.

**Créez des partitions sur le nouveau disque supplémentaire**

La commande **create** est utilisée pour créer des partitions chaque fois qu'un nouveau disque secondaire est ajouté. Vous pouvez également utiliser cette commande pour créer des partitions sur un disque secondaire existant après la suppression des partitions existantes à l'aide de la commande « remove ».

```
(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 pas de limitation de taille de 2 téraoctets lors de la création de partitions avec l'outil de partition de disque. L'outil peut créer des partitions de plus de 2 téraoctets. Lorsque vous partitionnez le disque, une partition d'échange d'une taille de 32 Go est automatiquement ajoutée. La partition principale utilise alors tout l'espace restant sur le disque.

Une fois la commande exécutée, un schéma de partition de table de partition GUID (GPT) est créé. Une partition de swap de 32 Go et une partition de données sont également créées pour utiliser le reste de l'espace. Un nouveau système de fichiers est ensuite créé sur la partition principale.

**Remarque**

Ce processus peut prendre quelques secondes et vous ne devez pas interrompre le processus.

```
(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 interrupt 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 que vous avez créé la partition.

## Redimensionner les partitions du disque supplémentaire existant

Vous pouvez utiliser la commande **resize** pour redimensionner le disque attaché (secondaire). Vous pouvez redimensionner un disque doté d'un enregistrement de démarrage principal (MBR) ou d'un schéma GPT. La taille du disque doit être inférieure à 2 téraoctets jusqu'à un maximum de 2 téraoctets.

#### Remarque

- La commande « redimensionner » est conçue pour fonctionner sans perdre de données existantes. Citrix recommande toutefois de sauvegarder les données critiques de ce disque sur un stockage externe avant de tenter le redimensionnement. La sauvegarde des don-

nées est utile dans les cas où les données du disque peuvent être corrompues pendant l'opération de redimensionnement.

- Assurez-vous d'augmenter l'espace disque par incréments de 100 Go d'espace lors du redimensionnement des partitions. Une telle augmentation incrémentielle garantit que vous n'auriez pas à redimensionner plus fréquemment.

```
(dpt): ?resize
Resizes existing partition on attached disk to utilize all space available. Pre-conditions are:
1. Secondary disk exists and capacity 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 « redimensionner » vérifie toutes les conditions préalables et procède si toutes les conditions préalables sont remplies et après avoir donné votre consentement au redimensionnement. Il arrête les processus accédant au disque, notamment les sous-systèmes Citrix ADM, les processus de base de données PostgreSQL et le processus de surveillance Citrix ADM. Une fois les processus arrêtés, le disque est démonté pour le préparer au redimensionnement. Le redimensionnement se fait en étendant la partition pour occuper tout l'espace disponible, puis en développant le système de fichiers. Si une partition d'échange existe sur le disque, elle est supprimée et recrée à la fin du disque après le redimensionnement. La partition d'échange est abordée dans la section **Créer** une commande du document.

### Remarque

Le processus de « croissance du système de fichiers » peut prendre un certain temps et veiller à ne pas interrompre le processus pendant qu'il est en cours. L'outil redémarre la machine virtuelle après avoir redimensionné la partition.

```
(dpt): resize
*****
*** WARNING !! ***
*****
Resizing the partition/disk works without affecting the existing data.
However we strongly recommend you to manually backup your data before proceeding with the operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
Are you sure you want to resize (Y/N): y

Unmounting partition: /dev/da1p1 from: /var/mps
OK to resize existing partition.
Disabling swap on partition: /dev/da1p2
Deleting swap partition: da1p2
Resizing partition da1p1..
da1p1 resized

Adding a swap partition da1p2..
da1p2 added

Formatting the newly added portions of the partition. This may take some time (~10 seconds). Please be patient and don't
interrupt the process...
```

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

```

Resize Done.
VM has to be rebooted for the resized partition to be used.
Rebooting VM now...

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

System going down IMMEDIATELY
    
```

Après le redémarrage, l’augmentation de taille peut être observée à l’aide de la commande « df ». Voici les détails avant et après avoir augmenté la taille :

<pre> 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             </pre>	<pre> 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             </pre>
--	--

## Supprimez les partitions du disque supplémentaire

Une partition existante sur le disque secondaire peut être redimensionnée jusqu’à 2 téraoctets. Ceci est dû à une limitation connue de la partition. Si vous voulez un disque de plus de 2 téraoctets, connectez un nouveau disque et partitionnez-le à l’aide de l’outil de partition de disque. Vous pouvez également supprimer la partition existante à l’aide de la commande **remove**, puis créer une partition.

### Remarque

La suppression de la partition existante supprime toutes les données existantes. Par conséquent, toutes les données critiques doivent être sauvegardées sur un stockage externe avant d’utiliser cette commande.

```

(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 le moniteur

ADM) à l'aide du disque secondaire. Si une partition de swap existe et que le swap est activé sur la partition, le swap est désactivé.

```
(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.

```
Unmounting partition: /dev/da1p1 from: /var/mps
OK to remove existing partitions.
Disabling swap on partition: /dev/da1p2
Removing all partitions from: da1
Remove Done.
Rebooting VM now...
```

#### 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 created.
The VM is rebooted automatically after these operations. If the automatic reboot does not happen, then this command can be used to reboot the VM.
```

Vous êtes invité à confirmer et une fois confirmé, il arrête tous les processus (tels que les sous-systèmes ADM, les processus PostgreSQL et le moniteur ADM). La machine virtuelle est ensuite redémarrée.

```
(dpt): reboot
Are you sure you want to reboot the VM (Y/N): y
```

```
Rebooting VM now...  
  
*** FINAL System shutdown message from nsroot@ns-mgmt-system ***  
  
System going down IMMEDIATELY
```

## Créer un fichier de sauvegarde des données du disque

Voici les étapes à suivre pour sauvegarder les données Citrix ADM avant de redimensionner ou de supprimer les partitions.

### Remarque

La création d'un fichier de sauvegarde nécessite de l'espace disque. Citrix vous recommande de vous assurer qu'il y a suffisamment d'espace disque disponible (50 % ou plus) avant l'exécution des commandes de sauvegarde.

#### 1. Arrêtez ADM.

```
1 /mps/masd stop  
2 <!--NeedCopy-->
```

#### 2. Arrêtez PostgreSQL.

```
1 su -l mpspostgres /mps/scripts/pgsql/stoppgsql_smart.sh  
2 <!--NeedCopy-->
```

#### 3. Arrêter le moniteur ADM.

```
1 /mps/scripts/stop_mas_monit.sh  
2 <!--NeedCopy-->
```

#### 4. Créer une archive tarball.

```
1 cd /var  
2 tar cvfz /var/mps/mps_backup.tgz mps  
3 <!--NeedCopy-->
```

### Remarque

L'opération prend du temps en fonction de la taille des données à sauvegarder.

#### 5. Générer une somme de contrôle.

```
1 md5 mps_backup.tgz > mps_backup_checksum  
2 <!--NeedCopy-->
```

#### 6. Copiez à distance l'archive et la somme de contrôle.

```
1 scp
2 <!--NeedCopy-->
```

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.

```
1 rm mps_backup.tgz mps_backup_checksum
2 <!--NeedCopy-->
```

## Commandes supplémentaires

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

### Commande d'aide :

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

```
(dpt): help
DPT Commands
-----
create  create_swapfile  exit  help  info  reboot  remove  resize
(dpt):
```

### Commande Info :

La commande **info** fournit des informations sur le disque secondaire connecté s'il existe. La commande fournit le nom du périphérique, le schéma de partition, la taille sous forme lisible par l'homme et le nombre de blocs de disque. Le schéma peut être MBR ou GPT. Un schéma MBR signifie que le disque a été partitionné à l'aide d'une version antérieure de la version Citrix ADM. La partition basée sur MBR/GPT peut être redimensionnée mais pas au-delà de 2 téraoctets. Le schéma de partition GPT signifie que le disque a été partitionné à l'aide de Citrix ADM 12.1 ou version ultérieure.

#### Remarque

Une partition GPT peut être supérieure à 2 téraoctets, mais lors de sa création. Toutefois, vous ne pouvez pas redimensionner le disque à une taille supérieure à 2 téraoctets après avoir créé un disque de taille inférieure. Il s'agit d'une limitation connue de la plate-forme.



```
(dpt): ?info
Provides information about attached disk (if found).
(dpt): info
-----
Disk: da1
Scheme: MBR
Size: (150G)
Blocks: 314572737
-----
(dpt):
```

**Commande Create\_SWAPFile :**

La partition d'échange par défaut sur le disque principal de Citrix ADM est de 4 Go et, par conséquent, l'espace d'échange par défaut est de 4 Go. Pour la configuration de mémoire par défaut de Citrix ADM, qui est de 2 Go, cet espace d'échange est suffisant. Toutefois, lorsque vous exécutez Citrix ADM avec une configuration de mémoire plus élevée, vous devez disposer de plus d'espace d'échange alloué sur le disque.

**Remarque**

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

Les disques secondaires ajoutés dans les versions antérieures de Citrix ADM n'ont pas de partition d'échange créée par défaut. La commande « create\_swapfile » est destinée aux disques secondaires créés à l'aide d'anciennes versions de Citrix ADM qui n'ont pas de partition d'échange. La commande vérifie les éléments suivants :

- Présence d'un disque secondaire
- Disque en cours de montage
- Taille du disque (au moins 500 Go)
- L'existence du fichier d'échange

La commande « create\_swapfile » n'est utile que lorsque la mémoire est supérieure ou égale à 16 Go et non lorsque la mémoire est faible. Par conséquent, cette commande vérifie également la mémoire avant de procéder à la création du fichier d'échange.

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

Creating swapfile is a time consuming operation and can take ~5 minutes to complete. Once started the operation should not be interrupted.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

Si toutes les conditions sont remplies et que l'utilisateur consent à continuer, un fichier d'échange de 32 Go est créé sur le disque secondaire. Le processus de création du fichier d'échange prend quelques minutes et veillez à ne pas interrompre le processus en cours. Une fois terminé, un redémarrage est effectué pour que le fichier d'échange prenne effet.

```
Creating swapfile. This may take some time (~5 mins). Please be patient and don't interrupt the process...
32768+0 records in
32768+0 records out
34359738368 bytes transferred in 724.061475 secs (47454173 bytes/sec)

Changing permissions for created swapfile...

Create (swapfile) Done.
VM has to be rebooted for the newly created swapfile to take effect.
```

Après le redémarrage, l'augmentation du swap peut être observée à l'aide de la commande supérieure.

<pre>CPU: 1.7% user, 0.0% nice, 0.8% system, 0.2% interrupt, 97.4% idle Mem: 1847M Active, 506M Inact, 382M Wired, 4684K Cache, 199M Buf, 4473M Free Swap: 4198M Total, 4198M Free</pre>	<pre>CPU: 42.0% user, 0.0% nice, 7.6% system, 5.0% interrupt, 45.3% idle Mem: 1805M Active, 423M Inact, 393M Wired, 4792K Cache, 199M Buf, 4587M Free Swap: 36G Total, 36G Free</pre>
--	---

### Commande de sortie :

Pour quitter l'outil, tapez exit et appuyez sur la touche **Entrée**.

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

## Attacher des disques supplémentaires à Citrix ADM déployés en haute disponibilité

Considérons un scénario dans lequel vous avez configuré une paire de serveurs Citrix ADM dans une configuration haute disponibilité sans disque secondaire. Supposons également que vous avez ajouté au moins deux instances Citrix ADC, vérifié et vérifié que tous les processus sont en cours d'exécution. Dans cette configuration, vous pouvez ajouter des disques secondaires aux machines virtuelles. Dans une configuration haute disponibilité, vous devez ajouter des disques supplémentaires aux deux nœuds, comme indiqué dans cette tâche :

1. Supposons que les noms de nœud Citrix ADM soient « ADM\_Primary » et « ADM\_Secondary ».

2. Commencez par exécuter l'outil de partition sur ADM\_Secondary, puis ajoutez un disque secondaire. La machine virtuelle redémarre après l'ajout du disque.
3. Arrêtez ADM\_Secondary après son redémarrage.
4. Exécutez maintenant l'outil de partition sur ADM\_Primary et ajoutez un disque secondaire. La machine virtuelle redémarre après l'ajout du disque.

Assurez-vous d'ajouter des disques de capacité similaire aux deux nœuds. Par exemple, si vous ajoutez un disque d'une capacité de 500 Go au nœud principal, ajoutez également un disque d'une capacité de 500 Go au nœud secondaire.

5. Après le redémarrage d'ADM\_Primary, vérifiez qu'il s'agit bien du nœud principal.
6. Démarrez maintenant le nœud ADM\_Secondary. Assurez-vous qu'il est apparu en tant que nœud secondaire et que les bases de données ont été synchronisées.
7. Confirmez que toutes les données existent toujours.

**Effectuez les étapes suivantes pour augmenter la capacité de la RAM sur les deux nœuds :**

1. Arrêtez ADM\_Secondary et augmentez la taille de la RAM si nécessaire. Ne redémarrez pas le nœud.
2. Arrêtez ADM\_Primary et augmentez la taille de la RAM si nécessaire.  

Assurez-vous d'augmenter la taille de la RAM de manière égale sur les deux nœuds. Par exemple, si vous augmentez la taille de la RAM sur le nœud principal à 16 Go, procédez de même sur le nœud secondaire.
3. Redémarrez ADM\_Primary.
4. Après le redémarrage d'ADM\_Primary, vérifiez qu'il s'agit bien du nœud principal.
5. Démarrez maintenant le nœud ADM\_Secondary. Après le redémarrage, assurez-vous qu'il est devenu secondaire et que la synchronisation de la base de données fonctionne.
6. Confirmez maintenant que toutes les données existent toujours.

**Remarque**

Une fois que vous avez ajouté le disque secondaire, le nœud principal met un certain temps à apparaître. En outre, l'ensemble du processus d'ajout de disques secondaires aux deux nœuds et d'augmentation de la capacité de la RAM nécessite que les deux nœuds soient inactifs pendant un certain temps. Prenez en compte ce temps d'arrêt lorsque vous planifiez cette activité de maintenance.

## Configurer

February 1, 2024

Vous pouvez accéder à un serveur Citrix ADM uniquement à l'aide de l'interface utilisateur graphique (GUI). Vous devez accéder à l'interface graphique pour ajouter des instances, gérer et surveiller vos instances et applications, afficher des analyses et configurer le serveur Citrix ADM.

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

Les navigateurs suivants sont pris en charge.

---

Navigateur Web	Version
Internet Explorer	11.0 et versions ultérieures
Google Chrome	Chrome 19 et versions ultérieures
Safari	Safari 5.1.1 et versions ultérieures
Mozilla Firefox	Firefox 3.6.25 et versions ultérieures

---

### Pour accéder à l'interface graphique Citrix ADM :

1. Dans un navigateur Web, tapez l'adresse IP de Citrix ADM (par exemple, <http://192.168.100.1>). Il s'agit de la même adresse IP que celle que vous avez spécifiée lors de l'installation du serveur.
2. Dans les champs **Nom d'utilisateur** et Mot de **passé** , entrez les informations d'identification de l'administrateur. Les informations d'identification de l'administrateur par défaut sont ns-root/nsroot.

Après avoir ouvert une session sur Citrix ADM, vous devez effectuer les opérations suivantes pour démarrer :

- [Ajoutez des instances à Citrix ADM](#). Vous devez ajouter des instances au serveur Citrix ADM si vous souhaitez gérer et surveiller ces instances.
- [Activez les analyses sur les serveurs virtuels](#). Pour afficher les données d'analyse pour le flux de trafic de votre application, vous devez activer la fonctionnalité Analytics sur les serveurs virtuels qui reçoivent le trafic pour les applications spécifiques.
- [Configurez le serveur NTP sur Citrix ADM](#). Vous devez configurer un serveur NTP (Network Time Protocol) dans Citrix ADM pour synchroniser son horloge avec le serveur NTP.
- [Configurez les paramètres système pour optimiser les performances Citrix ADM](#). Avant de commencer à utiliser Citrix ADM pour gérer et surveiller vos instances et applications, il

est recommandé de configurer quelques paramètres système qui garantiront des performances optimales de votre serveur Citrix ADM.

## Ajouter des instances à Citrix ADM

February 1, 2024

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

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

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

### Remarque

- Citrix ADM utilise l'adresse IP NetScaler (NSIP) des instances Citrix ADC pour la communication. Pour plus d'informations sur les ports qui doivent être ouverts entre les instances Citrix ADC et Citrix ADM, consultez [Ports](#).
- Pour les instances Citrix SD-WAN WO et Citrix SD-WAN EE, Citrix ADM utilise l'adresse IP de gestion des instances pour la communication.
- Pour savoir comment Citrix ADM découvre des instances, consultez la section [Découvrir des instances](#).

## Comment créer un profil Citrix ADC

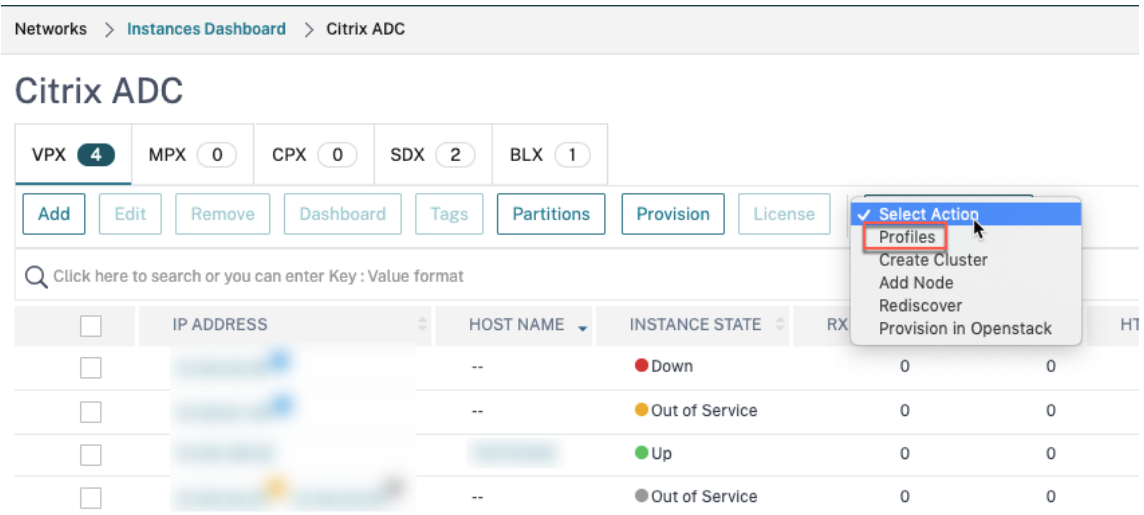
Le profil Citrix ADC contient le nom d'utilisateur, le mot de passe, les ports de communication et les types d'authentification des instances que vous souhaitez ajouter à Citrix ADM. Pour chaque type d'

instance, un profil par défaut est disponible. Par exemple, nsroot est le profil par défaut pour les instances de Citrix ADC. Le profil par défaut est défini à l'aide des informations d'identification d'administrateur Citrix ADC par défaut. Si vous avez modifié les informations d'identification d'administrateur par défaut de vos instances, vous pouvez définir des profils d'instance personnalisés pour ces instances. Si vous modifiez les informations d'identification d'une instance après sa découverte, vous devez modifier le profil d'instance ou créer un profil, puis redécouvrir l'instance.

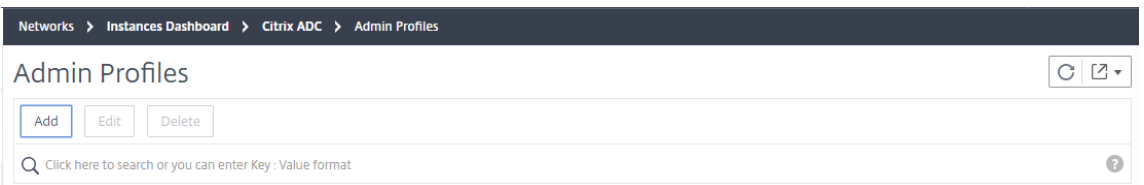
Vous pouvez créer un profil Citrix ADC à partir de la page **Instance** ou lors de l'ajout ou de la modification d'une instance.

**Pour créer un profil Citrix ADC à partir de la page Instance :**

1. Accédez à **Réseaux > Instances**.
2. Sélectionnez une instance. Par exemple, Citrix ADC.
3. Sur la page Citrix ADC, sélectionnez **Profils**.



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



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

## ← Create Citrix ADC Profile

Profile Name\*  ✘ Please enter value

User Name\*

Password\*

SSH Port

Note: HTTP port and HTTPS port are configurable for CPX only.

HTTP Port

HTTPS Port

Use global settings for Citrix ADC communication

▼ SNMP

Version  
 v2  v3

Community\*

▼ Timeout Settings

Waiting Time for sending the request from Application Delivery Management to Citrix ADC after successful reboot.

Timeout (in Seconds)

- a) **Nom du profil** : spécifiez un nom de profil pour l'instance Citrix ADC.
- b) **Nom d'utilisateur** : spécifiez un nom d'utilisateur pour vous connecter à l'instance Citrix ADC.
- c) **Mot de passe** : spécifiez un mot de passe pour vous connecter à l'instance Citrix ADC.
- d) **Port SSH** : Spécifiez le port de communication SSH entre Citrix ADM et l'instance Citrix ADC.
- e) **Port HTTP** : Spécifiez le port de communication HTTP entre Citrix ADM et l'instance Citrix ADC.

**Remarque**

Le port HTTP par défaut est 80. Vous pouvez également spécifier le port HTTP personnalisé ou autre que celui par défaut que vous avez peut-être configuré dans votre instance CPX Citrix ADC. Le port HTTP personnalisé peut être utilisé pour la communication uniquement entre Citrix ADM et Citrix ADC CPX.

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

**Remarque**

Le port HTTPS par défaut est 443. Vous pouvez également spécifier le port HTTPS personnalisé ou autre que celui par défaut que vous avez peut-être configuré dans votre instance CPX Citrix ADC. Le port HTTPS personnalisé peut être utilisé pour la communication uniquement entre Citrix ADM et Citrix ADC CPX.

- g) **Utiliser les paramètres globaux pour les communications Citrix ADC** : sélectionnez cette option si vous souhaitez utiliser les paramètres système pour la communication entre Citrix ADM et l'instance Citrix ADC, sinon sélectionnez http ou https.
- h) **Version SNMP** : sélectionnez **SNMPv2** ou **SNMPv3** et procédez comme suit :
- i. Si vous sélectionnez SNMPv2, spécifiez le nom de la **communauté** pour l'authentification.
  - ii. **Si vous sélectionnez SNMPv3, spécifiez le nom de sécurité et le niveau de sécurité.** En fonction du niveau de sécurité, sélectionnez le **type d'authentification** et le **type de confidentialité**.



▼ SNMP

Version

v2  v3

Security Name\*

Security Level\*

AuthPriv

Authentication Type\*

MD5

Authentication Password\*

Privacy Type\*

DES

Privacy Password\*

**Remarque**

Pour Citrix ADC SDX, seul le protocole **SNMPv2** est pris en charge.

- i) **Paramètres de délai d'attente** : Spécifiez le temps pendant lequel Citrix ADM doit attendre avant d'envoyer une demande de connexion à l'instance Citrix ADC après un redémarrage.
- j) Sélectionnez **Créer**.

**Ajouter des instances ADC à Citrix ADM**

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

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

Pour les instances SD-WAN, spécifiez l'adresse IP de chaque instance ou une plage d'adresses IP. Notez que Citrix ADM prend uniquement en charge les éditions Citrix SD-WAN WO et Citrix SD-WAN PE.

**Remarque**

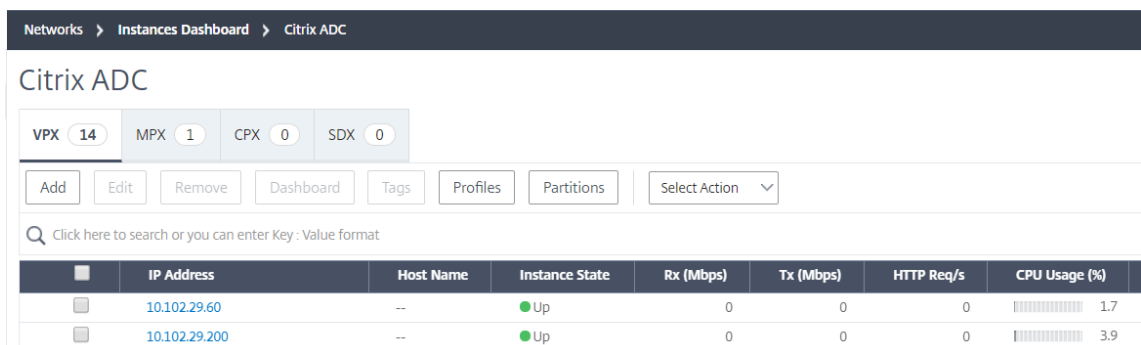
- Pour ajouter des instances Citrix ADC configurées dans un cluster, vous devez spécifier l'adresse IP du cluster ou l'un des nœuds individuels de la configuration du cluster. Toutefois, sur Citrix ADM, le cluster est représenté uniquement par son adresse IP.
- Pour les instances Citrix ADC configurées en tant que paire HA, lorsque vous ajoutez une instance, l'autre instance de la paire est automatiquement ajoutée.

Si deux serveurs Citrix ADM sont configurés en **mode haute disponibilité**, lorsqu'une instance est ajoutée, la source de trafic passe par l'adresse IP flottante ADM.

Lorsque vous ajoutez une instance à partir d'une donnée distante configurée avec un agent sur site, la source de trafic passe par l'agent ADM.

**Pour ajouter une instance à Citrix ADM :**

1. Ouvrez une session sur Citrix ADM à l'aide des informations d'identification de l'administrateur.
2. Accédez à **Réseaux > Instances > Citrix ADC**. Sélectionnez le type d'instance à ajouter (par exemple, Citrix ADC VPX) et cliquez sur **Ajouter**.



The screenshot shows the Citrix ADC Instances Dashboard. At the top, there are navigation links: Networks > Instances Dashboard > Citrix ADC. Below this, the title 'Citrix ADC' is displayed. There are four tabs for instance types: VPX (14), MPX (1), CPX (0), and SDX (0). Below the tabs are several action buttons: Add, Edit, Remove, Dashboard, Tags, Profiles, Partitions, and a Select Action dropdown menu. A search bar is present with the text 'Click here to search or you can enter Key: Value format'. Below the search bar is a table with the following columns: IP Address, Host Name, Instance State, Rx (Mbps), Tx (Mbps), HTTP Req/s, and CPU Usage (%). The table contains two rows of data:

IP Address	Host Name	Instance State	Rx (Mbps)	Tx (Mbps)	HTTP Req/s	CPU Usage (%)
10.102.29.60	--	Up	0	0	0	1.7
10.102.29.200	--	Up	0	0	0	3.9

3. Sélectionnez l'une des options suivantes :
  - **Entrez l'adresse IP du périphérique**- Pour les instances Citrix ADC, spécifiez le nom d'hôte ou l'adresse IP de chaque instance, ou une plage d'adresses IP. Pour les instances SD-WAN, spécifiez l'adresse IP de chaque instance ou une plage d'adresses IP.
  - **Importer à partir d'un fichier**- À partir de votre système local, téléchargez un fichier texte contenant les adresses IP de toutes les instances que vous souhaitez ajouter.
4. Dans **Nom du profil**, sélectionnez le profil d'instance approprié ou créez un nouveau profil en cliquant sur l'icône +.
5. Dans **Site**, sélectionnez l'emplacement auquel vous souhaitez ajouter l'instance, ou créez un nouvel emplacement en cliquant sur l'icône +.
6. Cliquez sur **OK** pour lancer le processus d'ajout d'instances à Citrix ADM.

### Remarque

Si vous souhaitez redécouvrir une instance, accédez à **Réseaux > Instances > Citrix ADC**. Sélectionnez l'instance que vous souhaitez redécouvrir, puis dans la liste **Sélectionner une action**, cliquez sur **Redécouvrir**.

## Ajouter des instances CPX ADC à Citrix ADM

Citrix ADM a été amélioré pour prendre en charge les améliorations apportées aux fonctionnalités CPX. L'instance CPX Citrix ADC est désormais ajoutée à Citrix ADM en fournissant une adresse IP pour le CPX ainsi qu'un profil de périphérique. Le processus d'ajout d'une instance CPX est maintenant similaire à la façon dont d'autres types d'ADC tels que VPX ou MPX sont ajoutés dans ADM. De plus, l'enregistrement de CPX dans ADM a été amélioré. Lorsqu'un CPX démarre, Citrix ADM détecte et enregistre automatiquement l'instance CPX. Une instance CPX n'est plus découverte via l'hôte Docker.

1. Accédez à **Réseaux > Instances > Citrix ADC**, puis cliquez sur l'onglet **CPX**.
2. Cliquez sur **Ajouter**.
3. La page **Ajouter Citrix ADC CPX** s'ouvre. Entrez les valeurs pour les paramètres suivants :
  - a) Vous pouvez ajouter des instances CPX en fournissant l'adresse IP accessible de l'instance CPX ou l'adresse IP du conteneur Docker où l'instance CPX est hébergée.
  - b) Sélectionnez le profil de l'instance CPX.
  - c) Sélectionnez le site sur lequel les instances doivent être déployées.
  - d) Sélectionnez l'agent.
  - e) En option, vous pouvez entrer la paire clé-valeur de l'instance. L'ajout d'une paire clé-valeur vous permet de rechercher plus tard l'instance.

## ← Add Citrix ADC CPX

Enter Device IP Address     Import from file

Enter one or more hostnames, IP addresses , and/or a range of IP addresses (for example, 10.102.40.30-10.102.40.45) using a comma separator.

Routable IP/ Docker IP\*

?

Profile Name\*

Site\*

Agent

>

Tags

+

### Remarque

Pour les instances CPX Citrix ADC, vous devez spécifier les détails des ports **HTTP**, **HTTPS**, **SSH** et **SNMP** de l'hôte lors de la création du profil d'instance CPX. Vous pouvez également spécifier la plage de ports publiés par l'hôte dans les champs **Port de départ** et **nombre de ports**.

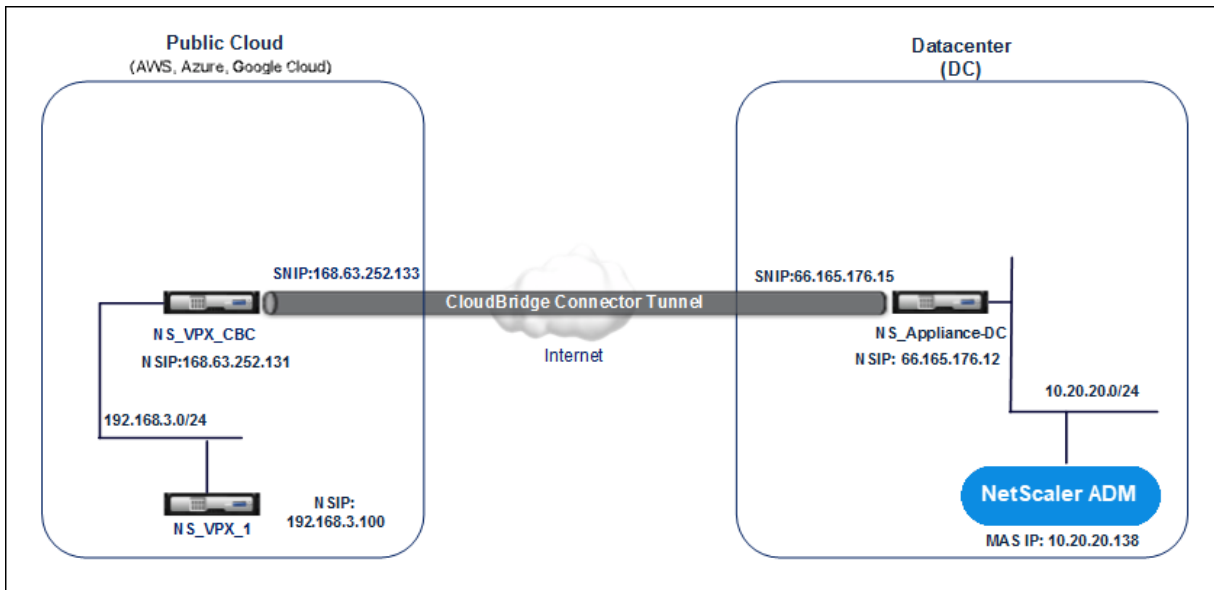
4. Cliquez sur **OK**.

## Ajouter des instances Citrix ADC VPX déployées dans le cloud à Citrix ADM

February 1, 2024

Vous pouvez utiliser Citrix ADM pour gérer et surveiller les instances Citrix ADC VPX déployées sur un cloud public tel qu'Amazon Web Services (AWS) ou Microsoft Azure. Vous devez établir une connectivité de couche 3 entre Citrix ADM et les instances Citrix ADC VPX déployées sur le cloud public. Pour établir la connectivité de couche 3, vous pouvez utiliser des solutions telles que NetScaler Cloud-Bridge Connector, Citrix SD-WAN, Direct Connect to AWS, VPN dans Azure ou des connecteurs tiers tels qu'Equinix, etc.

L'exemple de topologie suivant utilise NetScaler CloudBridge Connector pour la connectivité de couche 3 entre Citrix ADM et les instances Citrix ADC VPX déployées dans le cloud.



Un tunnel CloudBridge Connector est configuré entre l’appliance Citrix ADC NS\_Appliance-DC, dans le centre de données DC, et l’appliance virtuelle Citrix ADC (VPX) NS\_VPX\_CBC dans le cloud public. NS\_Appliance-DC et NS\_VPX\_CBC permettent la communication entre Citrix ADM et l’instance Citrix ADC VPX, NS\_VPX\_1, déployée dans le cloud public. Une fois la communication établie, vous pouvez découvrir NS\_VPX\_1 dans Citrix ADM.

**Pour configurer cette topologie :**

1. Installez, configurez et démarrez une instance Citrix ADC VPX dans le cloud public.
  - Pour obtenir des instructions, consultez la section [Installation de Citrix ADC VPX sur AWS](#).
  - Pour obtenir des instructions, consultez la section [Installation de Citrix ADC VPX sur Microsoft Azure](#).
2. Déployez et configurez une appliance physique Citrix ADC, ou provisionnez et configurez une appliance virtuelle Citrix ADC (VPX) sur une plate-forme de virtualisation dans le centre de données.
  - Pour obtenir des instructions, consultez la section [Installation des appliances virtuelles Citrix ADC sur Citrix Hypervisor](#).
  - Pour obtenir des instructions, consultez la section [Installation d’appliances virtuelles Citrix sur VMware ESXi](#).
  - Pour obtenir des instructions, consultez la section [Installation d’appareils virtuels Citrix ADC sur Microsoft Hyper-V](#).
3. Configurez le connecteur CloudBridge entre le centre de données et le cloud public. Pour obtenir des instructions, consultez la section [Configuration de CloudBridge Connector](#).

4. Configurez la route statique pour établir la connexion entre Citrix ADM et les instances Citrix ADC VPX déployées sur le cloud, comme suit :

- a) Connectez-vous à Citrix ADM.
- b) Accédez à **Système > Routes statiques**, puis cliquez sur **Ajouter**.

### ← Create Static Route

Configure the static route for establishing connection between NetScaler MAS and the NetScaler VPX instances deployed on the cloud.

Network Address

Netmask

Gateway

- c) Dans le champ **Adresse réseau** , entrez l'adresse du réseau sur lequel vous souhaitez établir un itinéraire statique à partir de Citrix ADM via le connecteur.
  - d) Dans le champ **Masque réseau**, entrez le masque réseau du réseau.
  - e) Dans le champ **Passerelle**, entrez l'adresse de la Gateway.
5. Ajoutez les instances de cloud Citrix ADC VPX à Citrix ADM en spécifiant la plage d'adresses IP des instances Citrix ADC VPX dans le cloud public. Pour obtenir des instructions détaillées, [cliquez sur Ajouter des instances à Citrix ADM](#).

## Activer les analyses sur les serveurs virtuels

February 1, 2024

Vous pouvez activer les analyses pour un serveur virtuel spécifique sur l'instance sélectionnée, représentant un serveur d'applications, et surveiller le trafic de ce serveur d'applications. Les analyses fournissent des statistiques pour le serveur virtuel.

### Remarque

Pour les instances Citrix ADC de version 11.0, version 65.30 et versions ultérieures, il n'existe aucune option sur Citrix ADM pour activer Security Insight explicitement. Assurez-vous de configurer les paramètres AppFlow sur les instances Citrix ADC. Une fois la configuration des

paramètres AppFlow terminée, Citrix 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 Citrix ADC, consultez [Pour définir les paramètres AppFlow à l'aide de l'utilitaire de configuration](#).

**Pour activer Analytics sur chaque instance sur Citrix ADM, procédez comme suit :**

1. Accédez à **Réseaux > Instances** et sélectionnez l'instance Citrix ADC pour laquelle vous souhaitez activer les analyses. Par exemple, Citrix ADC.
2. Dans la liste des instances, sélectionnez une instance.
3. Dans la liste **Sélectionner une action**, sélectionnez **Configurer Analytics**.
4. Dans la liste des applications, sélectionnez les serveurs virtuels et cliquez sur **Activer AppFlow**.
5. Dans le champ **Activer AppFlow**, saisissez **true** et, en fonction des analyses que vous souhaitez activer, sélectionnez **Security Insight** ou **Web Insight**, ou les deux.

### Enable AppFlow

**Select Expression**

Load Balancing

▼

true

**Transport Mode**    IPFIX    Logstream

Web Insight

Client Side Measurement

Security Insight

If there is a firewall between Citrix ADM and the Citrix ADC instance, please make sure the TCP port 5557 is open. This is to allow ADM to collect AppFlow traffic.

OK

Cancel

**Remarque**

Citrix ADM utilise Citrix ADC SNIP pour Logstream et NSIP pour IPFIX. Si un pare-feu est activé entre Citrix ADM et Citrix ADC instance, assurez-vous d'ouvrir le port suivant pour

permettre à Citrix ADM de collecter le trafic AppFlow :

Mode de transport	IP source	Type	Port
IPFIX	NSIP	UDP	4739
Logstream	SNIP	TCP	5557

- Pour **HDX Insight** et **Gateway Insight**, lorsque vous cliquez sur **Activer AppFlow**, vous devez sélectionner le **serveur virtuel VPN** configuré sur votre instance Citrix ADC et cocher les cases **ICA** ou **HTTP** en conséquence.

### Enable AppFlow

Select Expression \*

VPN

Transport Mode  IPFIX  Logstream  ICA

TCP

HTTP

If the AppFlow for a virtual server is enabled on more than one NetScaler Management and Analytics System appliance, then the appliance on which the AppFlow is enabled most recently has the highest priority for collecting the information.

OK

Cancel

- Pour **TCP Insight**, accédez à **Système > Paramètres d'analyse** Configurer les fonctionnalités, puis sélectionnez **Activer TCP Insight**.
- Pour **Video Insight**, vous devez apporter les modifications de configuration sur l'appliance Citrix ADC. Pour plus d'informations sur la façon d'activer les analyses pour Video Insight, consultez [Video Insight](#).
- Pour **WAN Insight**,
  - a) Accédez à **Infrastructure > Instances > NetScaler SD-WAN WO** et sélectionnez l'appliance d'optimisation WAN du centre de données.
  - b) Dans la liste déroulante **Action**, sélectionnez **Activer Insight**.



c) Sélectionnez les paramètres suivants selon les besoins :

- Collecte de données géographiques pour HDX Insight : partage l'adresse IP du client avec l'API Google Geo.
- AppFlow : commence à collecter des données à partir des instances d'optimisation WAN.
  - \* TCP et WanOpt : fournit des rapports TCP et WanOpt Insight .
  - \* HDX : fournit des rapports HDX Insight.
  - \* TCP uniquement pour HDX : fournit TCP uniquement pour les rapports HDX Insight.

Vous pouvez sélectionner le **mode de transport AppFlow** vers IPFIX ou Logstream tout en activant AppFlow sur les instances Citrix ADC découvertes dans Citrix ADM. Pour plus d'informations sur IPFIX et Logstream, consultez la section [Présentation de Logstream](#) .

Le tableau suivant décrit les fonctionnalités de Citrix ADM qui prennent en charge IPFIX et Logstream en tant que mode de transport :

Fonctionnalité	IPFIX	Logstream
Web Insight	•	•
Security Insight	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	Non pris en charge	•
CR Insight	•	•
Réputation IP	•	•
AppFirewall	•	•
Mesure côté client	•	•
Syslog/Auditlog	•	•

Vous pouvez également activer ou désactiver le traitement du trafic Web Insight à l'aide de l'option **Enable Web Insight** dans Citrix ADM. Si vous ne souhaitez pas surveiller le trafic Web Insight, vous pouvez désactiver cette option. Pour plus d'informations, consultez la section [Traitement du trafic Web Insight par Citrix ADM](#) .

## Configurer le serveur NTP

February 1, 2024

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

### Pour configurer un serveur NTP sur Citrix ADM:

1. Accédez à **Système** > **Serveurs NTP**, puis cliquez sur **Ajouter**.
2. Dans la page **Créer un serveur NTP**, entrez les détails suivants :
  - **Nom du serveur/adresse IP** —Entrez le nom de domaine ou l'adresse IP du serveur NTP. Le nom ou l'adresse IP ne peuvent pas être modifiés après avoir ajouté le serveur NTP.
  - Intervalle **minimum d'interrogation** : spécifiez la valeur minimale de l'intervalle entre les messages NTP transmis, en secondes sous la forme d'une puissance de 2. Par exemple, si vous souhaitez que l'intervalle minimal 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.
  - **Préférez** —Sélectionnez cette option si vous souhaitez spécifier ce serveur NTP comme serveur préféré pour la synchronisation des horloges. Cela ne s'applique que si plusieurs serveurs sont configurés.

3. Cliquez sur **Créer**.

### Pour activer la synchronisation NTP sur Citrix ADM :

1. Accédez à **Système** > **Serveurs NTP**.
2. Cliquez sur **Synchronisation NTP** et **activez la case à cocher Activer la synchronisation NTP**.
3. Cliquez sur **OK**.

## Configurer les paramètres système

February 1, 2024

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

### Configurer les alarmes système

Vous devez configurer les alarmes système pour vous assurer que vous êtes conscient 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 correspondant à cette catégorie d'alarme se produit (par exemple, LoginFailure), un message est enregistré dans le système et vous pouvez le visualiser sous forme de message Syslog.

#### Pour configurer les alarmes système :

1. Accédez à **Système > Alarmes** , sélectionnez l'alarme que vous souhaitez configurer, puis cliquez sur **Modifier** .
2. Sur la page **Configurer l'alarme**, sélectionnez la gravité de l'alarme et définissez le seuil.
3. Pour afficher les alarmes qui ont enfreint le seuil ou pour lesquelles un événement s'est produit, accédez à **Système > Audit** et cliquez sur **Messages Syslog**.

### Configurer les notifications système

Vous pouvez envoyer des notifications à certains groupes d'utilisateurs pour un certain nombre de fonctions liées au système. Vous pouvez configurer un serveur de notifications dans Citrix ADM et configurer des serveurs de Gateway de messagerie et SMS (Short Message Service) pour envoyer des notifications par courrier électronique et texte aux utilisateurs. Cela garantit que vous êtes informé de toutes les activités au niveau du système, telles que la connexion utilisateur ou le redémarrage du système.

#### Pour configurer les notifications système :

1. Accédez à **Système > Notifications**. Sous **Paramètres**, cliquez sur **Modifier les paramètres de notification**.
2. Dans la page **Configurer les paramètres de notification système**, sélectionnez la catégorie ou la catégorie d'événements générés par Citrix ADM.
3. Ensuite, configurez le serveur de messagerie ou le serveur SMS pour recevoir une notification par e-mail ou SMS, ou les deux.

### Configurer les paramètres de nettoyage du système

Pour limiter la quantité de données de reporting stockées dans la base de données de votre serveur Citrix ADM, vous pouvez spécifier l'intervalle pour lequel Citrix ADM conserve les données de reporting réseau, les événements, les journaux d'audit et les journaux de tâches. Par défaut, ces données sont élaguées toutes les 24 heures (à 00.00 heures).

#### Pour configurer le paramètre de nettoyage du système :

1. Accédez à **Système > Administration du système**. Sous **Paramètres d'élagage**, cliquez sur **Paramètres d'élagage du système**.
2. Sur la page **Configurer les paramètres de System Prune**, spécifiez le nombre de jours pendant lesquels vous souhaitez conserver les données, puis cliquez sur **OK**.

### Configurer les paramètres de sauvegarde du système

Citrix ADM sauvegarde automatiquement le système tous les jours à 00h30. Par défaut, il enregistre trois fichiers de sauvegarde. Vous souhaitez peut-être conserver un plus grand nombre de sauvegardes du système. Vous pouvez également chiffrer le fichier de sauvegarde. Vous pouvez également choisir d'enregistrer la sauvegarde sur un serveur externe.

#### Pour configurer les paramètres de sauvegarde du système :

1. Accédez à **Système > Administration du système**.
2. Sous **Paramètres de sauvegarde**, cliquez sur **Paramètres de sauvegarde système**.
3. Sur la page **Configurer les paramètres de sauvegarde du système**, spécifiez les valeurs requises.

### Configurer les paramètres de sauvegarde d'instance

Si vous sauvegardez l'état actuel d'une instance Citrix ADC, vous pouvez utiliser les fichiers de sauvegarde pour rétablir la stabilité en cas d'instabilité de l'instance. Cela est particulièrement important

avant d'effectuer une mise à niveau. Par défaut, une sauvegarde est effectuée toutes les 12 heures et trois fichiers de sauvegarde sont conservés dans le système.

**Pour configurer les paramètres de sauvegarde d'instance :**

1. Accédez à **Système > Administration du système** .
2. Sous **Paramètres de sauvegarde** , sélectionnez **Paramètres de sauvegarde de l'instance** et spécifiez les valeurs requises.

**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 Citrix ADM, vous pouvez spécifier l'intervalle pendant lequel Citrix ADM conserve les données de rapport 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 **Système > Administration du système** .
2. Sous **Paramètres d'élagage** , cliquez sur **Instance Events Prune Settings** .
3. Entrez l'intervalle de temps, en jours, pendant lequel vous souhaitez conserver les données sur le serveur Citrix ADM et cliquez sur **OK**.

**Configurer 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 suivant lequel vous souhaitez purger les données syslog. Vous pouvez spécifier le nombre de jours après lesquels les données Syslog générique seront supprimées de Citrix ADM.

**Pour configurer les paramètres de purge de syslog d'instance :**

1. Accédez à **Système > Administration système**. Sous Paramètres d'élagage, cliquez sur Paramètres de **purge du Syslog de l'instance** .
2. Dans la page Configurer les paramètres de purge Syslog de l'instance, spécifiez le nombre de jours compris entre 1 et 180 dans le champ **Conserver les données génériques Syslog** .
3. Cliquez sur **OK**.

## Mettre à niveau

February 1, 2024

Chaque version de Citrix ADM offre des fonctionnalités nouvelles et mises à jour avec des fonctionnalités améliorées. Citrix vous recommande de mettre à niveau Citrix ADM vers la dernière version pour bénéficier des nouvelles fonctionnalités et des corrections de bogues. Une liste complète des améliorations, des problèmes connus et des corrections de bogues est incluse dans les notes de mise à jour accompagnant chaque annonce de publication. Il est également important de comprendre le cadre de licences et les types de licences qui peuvent être utilisés avant de commencer la mise à niveau. [Pour plus d'informations sur les licences Citrix ADM, reportez-vous à la section Gestion](#)

Les informations relatives au chemin de mise à niveau sont également disponibles dans le [Guide de mise à niveau Citrix](#)

### Avant de procéder à la mise à niveau

Téléchargez le package de mise à niveau depuis la page de téléchargements de Citrix ADM et suivez les instructions de cet article pour mettre à niveau votre système vers la dernière version 12.1. Une fois l'opération de mise à niveau démarrée, Citrix ADM redémarre et les connexions existantes sont interrompues et reconnectées lorsque la mise à niveau est terminée avec succès. La configuration existante est conservée, mais Citrix ADM ne traite aucune donnée tant que la mise à niveau n'est pas terminée.

#### Important

La version et la version de Citrix ADM doivent être **égales ou supérieures à** celles de votre version et build de Citrix ADC. Par exemple, si vous avez installé Citrix ADM 12.1 Build 50.39, assurez-vous d'avoir installé Citrix ADC 12.1 Build 50.28/50.31 ou une version antérieure.

### Points à noter avant la mise à niveau vers la version 12.1 :

- Si vous effectuez une mise à niveau vers la version Citrix ADM 12.1 build 48.18 à partir de la version 11.1 ou de la version 12.0 antérieure à 56.x, effectuez les étapes suivantes.
  - Mise à niveau de la version existante vers la version 12.0 57.24.
  - Ensuite, passez à la dernière version de la version 12.1.

Vous devez suivre ce processus en deux étapes car certaines procédures de nettoyage sont requises pour réussir la mise à niveau vers la version 12.1. Ces procédures ne sont disponibles qu'à partir de 12.0 build 56.x.

- Avec la version 12.1, le déploiement de haute disponibilité permet de configurer une adresse IP flottante sur le nœud principal et d'éliminer le besoin d'un équilibreur de charge Citrix ADC distinct. En raison de cette amélioration, le déploiement haute disponibilité doit se trouver sur le même sous-réseau. Si votre déploiement actuel concerne différents sous-réseaux, vous devez consulter cet article pour en savoir plus sur le processus de mise à niveau.
- Avec la version 12.1, la prise en charge de la sauvegarde avancée a été supprimée. La fonctionnalité de sauvegarde avancée n'est plus disponible après la mise à niveau vers Citrix ADM 12.1. Consultez cet article pour plus de détails.

#### Remarque

Vous ne pouvez pas rétrograder Citrix ADM d'une version 12.1 vers une version antérieure.

#### Précautions recommandées :

- Sauvegardez le serveur Citrix ADM avant de procéder à la mise à niveau.
- Après la mise à niveau, vous devrez peut-être rétablir les connexions entre le serveur Citrix ADM et les instances gérées. Une invite de confirmation vous avertit que les connexions peuvent échouer si vous continuez.
- Pour les serveurs Citrix ADM dans une configuration haute disponibilité, lors de la mise à niveau, n'apportez aucune modification de configuration sur aucun des nœuds.

#### Avertissement

N'actualisez pas le navigateur tant que le processus de mise à niveau n'est pas terminé. Le processus de mise à niveau peut prendre quelques minutes.

- Après la mise à niveau, le nœud actif peut changer dans une paire de haute disponibilité.

### Mettre à niveau un seul serveur Citrix ADM

#### Pour mettre à niveau un serveur Citrix ADM unique :

1. Dans un navigateur Web, saisissez l'adresse IP du serveur Citrix ADM.

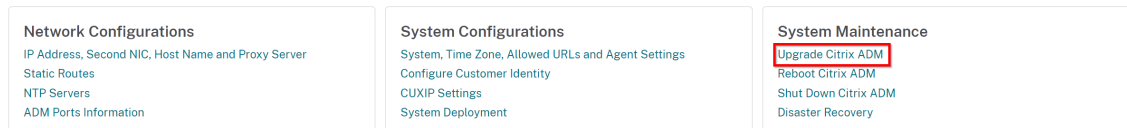
#### Remarque

Pour les serveurs Citrix ADM en mode haute disponibilité, saisissez l'adresse IP de l'un des serveurs Citrix ADM de la paire HA ou du serveur virtuel d'équilibrage de charge.

2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.

3. Accédez à **Système > Administrations du système** . Sous le sous-titre **Administration du système**, cliquez sur **Mettre à niveau Citrix ADM**.

System Administration

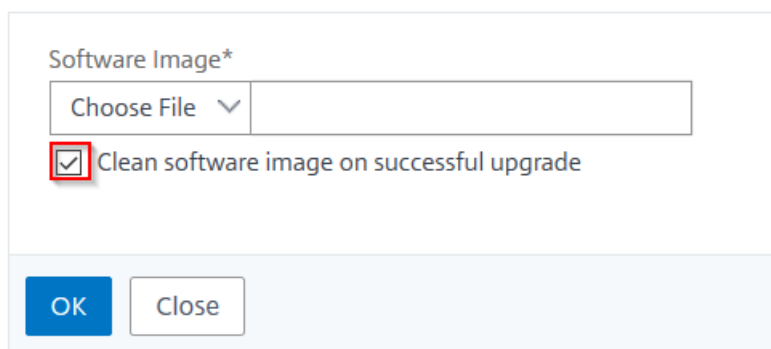


4. Sur la page **Mettre à niveau Citrix ADM**, activez la case à cocher **Nettoyer l'image logicielle lors de la mise à niveau réussie** pour supprimer les fichiers image après la mise à niveau. La sélection de cette option supprime automatiquement les fichiers image Citrix ADM lors de la mise à niveau.

**Remarque**

Cette option est sélectionnée par défaut. Si vous ne cochez pas cette case avant de commencer le processus de mise à niveau, vous devez supprimer manuellement les images.

## ← Upgrade Citrix ADM



5. Vous pouvez ensuite télécharger un nouveau fichier image en sélectionnant **Local** (votre machine locale) ou **Appliance**. Le fichier de construction doit être présent sur l'appliance virtuelle Citrix ADM.



## ← Upgrade Citrix ADM

Software Image\*

Choose File ▾
build-mas-██████████.tgz
?

Clean software image on successful upgrade

OK
Close

La boîte de dialogue Confirmer s'affiche. Cliquez sur **OK**.

6. Cliquez sur **OK**.

Le processus de mise à niveau démarre.

### Mise à niveau d'une paire à haute disponibilité provenant de versions antérieures vers la version 12.1

Pour les serveurs Citrix ADM en mode haute disponibilité, vous pouvez effectuer la mise à niveau en accédant au nœud actif ou à l'adresse IP du serveur virtuel d'équilibrage de charge. Les deux serveurs Citrix ADM sont automatiquement mis à niveau vers la dernière version une fois que vous lancez le processus de mise à niveau dans l'un ou l'autre des serveurs.

#### Important

##### Points à noter lors de la mise à niveau de Citrix ADM en mode haute disponibilité

Lors de la mise à niveau de Citrix ADM en mode haute disponibilité vers la version 12.1 à partir d'une version antérieure, la connexion haute disponibilité est établie en interne par le script « join HA » qui s'exécute sur le nœud secondaire. La durée du processus de mise à niveau dépend de l'infrastructure réseau, des données présentes dans la base de données et de la vitesse de la liaison. Le rétablissement de la connexion entre les deux nœuds peut prendre quelques heures. Pendant cette période, le nœud principal ne reçoit aucun battement cardiaque du nœud secondaire. Une notification s'affiche en cas de battement de cœur manquant sur l'interface utilisateur principale jusqu'à ce que le processus de mise à niveau soit terminé. Une fois le processus de mise à niveau terminé, le nœud secondaire redémarre et le déploiement de haute disponibilité est terminé.

### Remarque

Pour connaître l'état de la mise à niveau, connectez-vous à chaque nœud via SSH, exécutez les commandes suivantes et vérifiez la sortie :

```
installations de pgrep -lf
```

```
maintenance de pgrep -lf
```

```
pgrep -lf join_streaming_replication
```

```
pgrep -lf pg_basebackup
```

Si l'une de ces commandes indique un processus en cours d'exécution sur l'un des nœuds, la mise à niveau est en cours et ne doit pas être interrompue. Ne redémarrez pas Citrix ADM pendant cette période et n'essayez pas de forcer le basculement sur le nœud secondaire.

Une fois le processus de mise à niveau terminé, il se peut que vous ne puissiez pas vous connecter avec nsroot/nsroot ou vos informations d'identification utilisateur. Cela est dû au fait que le sous-système Citrix ADM n'a pas complètement redémarré ou que la migration est peut-être toujours en cours. Ne redémarrez pas Citrix ADM et ne tentez pas de récupérer le mot de passe. Cela peut avoir un effet indésirable et le système peut se comporter de manière incohérente. Si nécessaire, vous pouvez essayer de vous connecter à l'aide des `<your_password_for_the_nsroot_user>` informations d'identification nsrecover/.

Après la mise à niveau et avant de commencer les opérations, assurez-vous que les nœuds principal et secondaire sont mis à niveau et que le redémarrage est terminé.

### Remarque

Vous ne pouvez pas mettre à niveau Citrix ADM en mode haute disponibilité à l'aide de l'interface de ligne de commande.

### Licences groupées sur des serveurs Citrix ADM en haute disponibilité :

Lorsque les serveurs Citrix ADM sont déployés en mode haute disponibilité, le fichier de licence est joint au nœud principal et configuré (nœud verrouillé) avec l'ID d'hôte ou l'adresse MAC du serveur principal. La fonctionnalité de licences groupées est désormais prise en charge par Citrix ADM en haute disponibilité à partir de la version 12.1. Pour configurer la fonctionnalité de licences groupées sur les deux nœuds, vous devez disposer de fichiers de licence identiques sur les deux nœuds. Pour installer une licence identique sur le nœud secondaire, vous devez réhéberger la licence sur l'HostID (adresse MAC) du nœud secondaire.

Envisagez un scénario dans lequel Citrix ADM dispose de deux nœuds de serveur S1 et S2 en mode haute disponibilité. Le fichier de licence d'origine, L1, est installé sur le serveur S1. Le fichier de licence L2 réhébergé doit maintenant être attribué à S2.

Suivez les étapes pour mettre à niveau Citrix ADM en mode haute disponibilité de 12.0 vers 12.1 et

configurer la fonctionnalité de licences groupées :

1. Connectez-vous au nœud principal des serveurs Citrix ADM en mode haute disponibilité et effectuez le processus de mise à niveau.
2. Installez le fichier de licence L2 réhébergé sur le nœud de serveur secondaire S2.

À l'heure actuelle :

- Si S2 est le nœud principal, vous pouvez installer la licence L2 en accédant à l'interface graphique de cette instance.
  - Si S2 est le nœud secondaire, vous devez effectuer manuellement un basculement afin que S2 devienne désormais le nœud principal. Installez la licence L2 sur le nouveau nœud principal à l'aide de l'interface graphique.  
Cela est dû au fait que vous ne pouvez accéder qu'au serveur principal en haute disponibilité via l'interface graphique.
3. Configurez l'adresse IP flottante sur le nouveau nœud principal.
  4. Supprimez les adresses IP du serveur de licences sur les instances Citrix ADC et reconfigurez-les pour utiliser l'adresse IP flottante. Effectuez cette opération sur toutes les instances de Citrix ADC.

Citrix vous recommande d'effectuer la mise à niveau des licences groupées à haute disponibilité Citrix ADM en créant une fenêtre de maintenance sur les instances Citrix ADC. En effet, la suppression du serveur de licences et l'ajout d'une adresse IP flottante entraînent le retour temporaire des instances Citrix ADC à la bande passante minimale prise en charge.

### **Scénarios de mise à niveau de haute disponibilité**

Il peut y avoir deux scénarios dans lesquels les serveurs Citrix ADM sont déployés en mode haute disponibilité.

- Les serveurs principal et secondaire sont déployés sur le même sous-réseau.
- Les serveurs principal et secondaire sont déployés dans différents sous-réseaux.

Ce document de mise à niveau vous aide à mettre à niveau Citrix ADM dans ces deux scénarios.

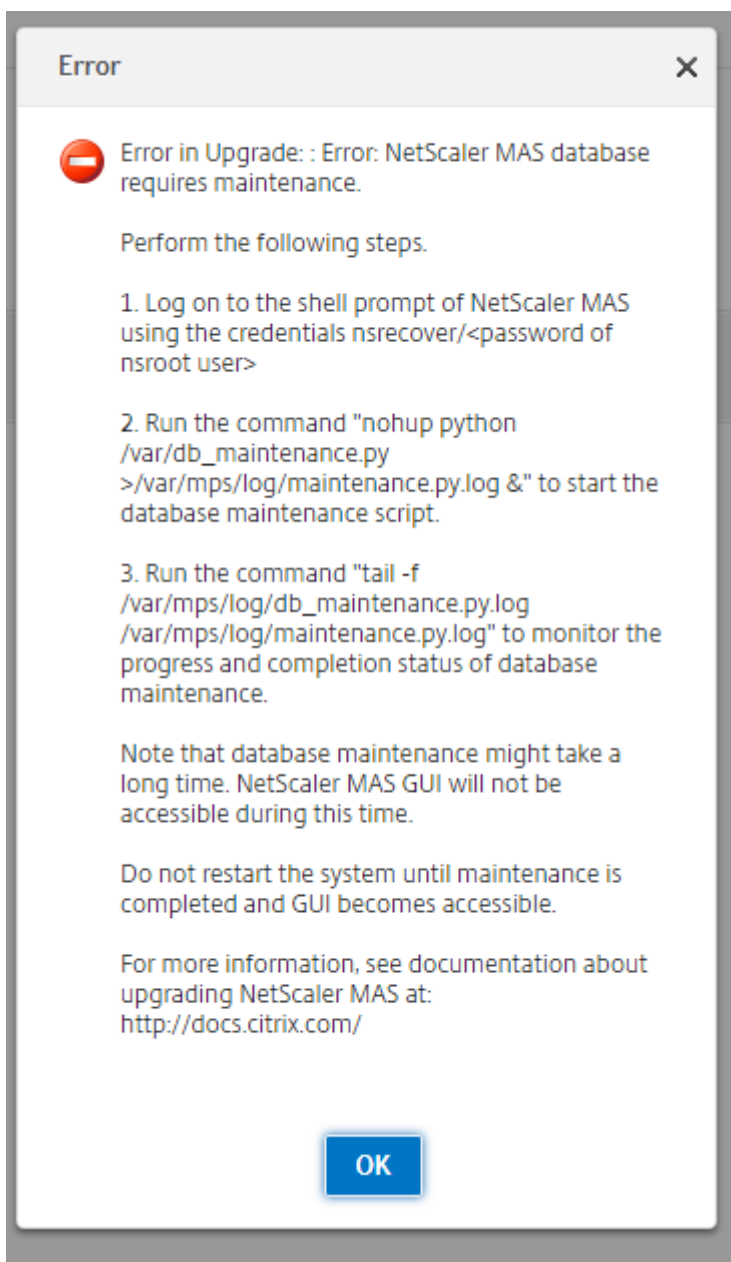
- Mise à niveau d'une configuration haute disponibilité sur le même sous-réseau
- Mise à niveau d'une configuration de haute disponibilité dans différents sous-réseaux

### **Mettre à niveau une configuration à haute disponibilité sur le même sous-réseau**

La mise à niveau des serveurs Citrix ADM déployés en mode haute disponibilité sur le même sous-réseau est gérée automatiquement par Citrix ADM 12.1.

**Pour mettre à niveau Citrix ADM déployé en mode haute disponibilité sur le même sous-réseau :**

1. Connectez-vous au nœud principal et accédez à **Système > Administrations système**.
2. Sous **Administration du système**, cliquez sur **Mettre à niveau Citrix ADM**.
3. En cas d'erreur lors de la mise à niveau, le message d'erreur suivant s'affiche. Suivez les instructions indiquées dans le message sur le serveur principal.

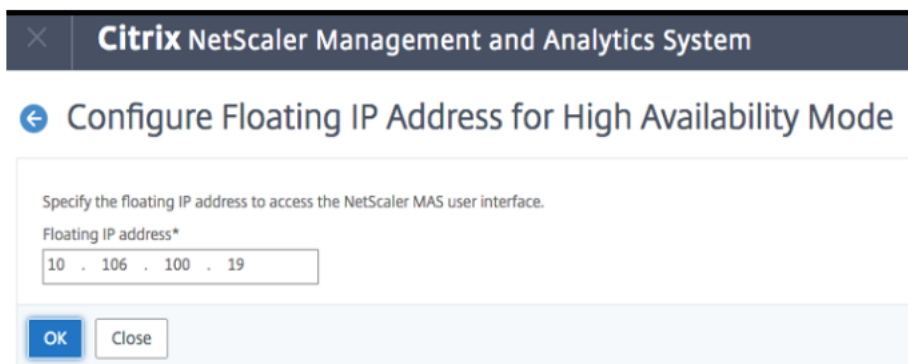


4. Dans le cadre du processus de mise à niveau, vous devez effectuer une procédure de nettoyage via la CLI. Pendant le processus de nettoyage, le nœud secondaire devient le nœud principal. L'ancien nœud principal n'est pas accessible via son interface graphique. Ne redémarrez pas l'ancien nœud principal ainsi que le nouveau nœud principal pendant que le processus de nettoyage est en cours. Une fois le processus de nettoyage terminé, poursuivez la procédure de mise à niveau via le nouveau nœud principal.
5. Une fois le processus de mise à niveau terminé, les deux nœuds doivent synchroniser leurs bases de données. Le temps nécessaire à la synchronisation complète et à l'apparition du nouveau nœud secondaire dépend des données présentes dans les bases de données.

**Remarque**

Une fois la mise à niveau réussie, vous devez configurer l'adresse IP flottante à l'aide de l'interface utilisateur Citrix ADM.

6. Pour configurer une adresse IP flottante, accédez à **Système > Déploiement > Configurer une adresse IP flottante pour le mode haute disponibilité**.
7. Spécifiez l'adresse IP flottante comme indiqué dans l'image suivante et cliquez sur **OK**.



The screenshot shows a web browser window titled "Citrix NetScaler Management and Analytics System". The page content includes a back arrow icon and the heading "Configure Floating IP Address for High Availability Mode". Below this, there is a text prompt: "Specify the floating IP address to access the NetScaler MAS user interface." A text input field labeled "Floating IP address\*" contains the IP address "10 . 106 . 100 . 19". At the bottom of the form, there are two buttons: "OK" and "Close".

**Mettre à niveau une configuration de haute disponibilité dans différents sous-réseaux**

La mise à niveau des serveurs Citrix ADM déployés en mode haute disponibilité sur différents sous-réseaux doit être gérée par un administrateur.

Dans ce scénario, le nœud Citrix ADM HA 1 (principal) se trouve dans le sous-réseau 1 et le nœud Citrix ADM HA 2 (secondaire) se trouve dans le sous-réseau 2.

**Pour mettre à niveau Citrix ADM déployé en mode haute disponibilité sur différents sous-réseaux :**

1. Interrompez manuellement la configuration de haute disponibilité. Pour plus d'informations, consultez la section [Désactivation de la haute disponibilité](#).
2. Mettez à niveau le nœud autonome Citrix ADM 1. Pour plus d'informations sur la mise à niveau de Citrix ADM, consultez la section [Mettre à niveau un seul serveur Citrix ADM](#).
3. Configurez et enregistrez un nouveau nœud autonome Citrix ADM 3 dans le sous-réseau 1.
4. Après avoir enregistré le nœud 1 et le nœud 3, déployez ces deux nœuds en mode haute disponibilité. Pour plus de détails, voir [Déploiement du nœud principal et du nœud secondaire en tant que paire à haute disponibilité](#).

**Remarque**

La configuration de l'adresse IP flottante est obligatoire.

5. Supprimez le nœud Citrix ADM 2.

## **Mettre à niveau une paire à haute disponibilité des versions 12.1 précédentes vers la dernière version**

Vous pouvez mettre à niveau les serveurs Citrix ADM déployés en haute disponibilité depuis une version 12.1 antérieure vers une version 12.1 ultérieure.

Pour mettre à niveau Citrix ADM déployé en mode haute disponibilité :

1. Téléchargez le fichier image Citrix ADM 12.1 build 49.37 depuis la page de téléchargement de Citrix.com.
2. Connectez-vous au nœud principal et accédez à **Système > Administrations système**.
3. Sous Administration du système, cliquez sur **Mettre à niveau Citrix ADM**.
4. Accédez au dossier dans lequel se trouve l'image.

Lors de la mise à niveau, n'apportez aucune modification de configuration à l'un ou l'autre des nœuds.

### **Avertissement**

- N'actualisez pas le navigateur tant que le processus de mise à niveau n'est pas terminé. Le processus de mise à niveau peut prendre quelques minutes.

Après la mise à niveau, le nœud actif peut changer dans une paire de haute disponibilité.

## **Mettre à niveau le déploiement de reprise après sinistre Citrix ADM**

La mise à niveau du déploiement de reprise après sinistre Citrix ADM se fait en deux étapes :

Vous devez d'abord mettre à niveau les nœuds Citrix ADM configurés en mode haute disponibilité sur le site principal. Plus tard, vous devez mettre à niveau le nœud de reprise après sinistre.

Assurez-vous d'avoir mis à niveau les serveurs Citrix ADM déployés en haute disponibilité avant de mettre à niveau le nœud de reprise après sinistre.

- Si vous mettez à niveau les serveurs Citrix ADM en mode haute disponibilité à partir d'anciennes versions vers la version 12.1, consultez la section [Mettre à niveau une paire haute disponibilité des versions antérieures vers la version 12.1](#) dans ce document.
- Si vous effectuez une mise à niveau d'une version 12.1 antérieure vers une version 12.1 ultérieure sur la paire haute disponibilité, voir [Mettre à niveau une paire haute disponibilité des versions 12.1 précédentes vers la dernière version](#) de ce document.

## Mettre à niveau le nœud de reprise après sinistre Citrix ADM

1. Téléchargez le fichier image de mise à niveau Citrix ADM à partir du site de téléchargement Citrix.
2. Téléchargez ce fichier sur 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 ».

```
login as: nsrecover
Using keyboard-interactive authentication.
Password:
Last login: Fri Aug 31 05:41:16 2018 from 10.252.241.37
bash-3.2# cd /var/mps/mps_images/
bash-3.2# tar zxvf build-mas-12.1-500.113.tgz
```

4. Accédez au dossier dans lequel vous avez placé le fichier image et décompressez le fichier.
5. Exécutez le script suivant :

```
./installmas
```

```
bash-3.2# ./installmas
```

## Mettre à niveau les agents sur site pour un déploiement multisite

La mise à niveau du déploiement de l'agent Citrix ADM s'effectue en trois étapes.

Assurez-vous d'avoir effectué les tâches suivantes avant de mettre à niveau les agents sur site :

1. Mettez à niveau les serveurs Citrix ADM déployés en haute disponibilité.
  - Si vous mettez à niveau les serveurs Citrix ADM en mode haute disponibilité à partir d'anciennes versions vers la version 12.1, consultez la section [Mettre à niveau une paire haute disponibilité des versions antérieures vers la version 12.1](#) dans ce document.
  - Si vous effectuez une mise à niveau d'une version 12.1 antérieure vers une version 12.1 ultérieure sur la paire haute disponibilité, voir [Mettre à niveau une paire haute disponibilité des versions 12.1 précédentes vers la dernière version](#)
2. Mettez à niveau le nœud de reprise après sinistre Citrix ADM.

Pour plus d'informations, consultez [Mettre à niveau le déploiement de récupération d'urgence Citrix ADM](#).



## Mettre à niveau l'agent sur site

1. Télécharger le fichier image de mise à niveau de l'agent Citrix ADM à partir du site de téléchargement Citrix.
2. Téléchargez ce fichier sur le nœud Agent à l'aide des informations d'identification « nsrecover ».
3. Assurez-vous que vous téléchargez l'image de mise à niveau de l'agent correcte. Le nom du fichier image est au format suivant :  
build-masagent-12.1-48.18.tgz
4. Connectez-vous à l'agent local à l'aide des informations d'identification « nsrecover ».
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 :

```
./install masagent
```

```
bash-3.2# ./installmasagent
```

## Supprimer la prise en charge de la fonctionnalité de sauvegarde et de restauration avancées de Citrix ADM

Au lieu d'utiliser la fonctionnalité de sauvegarde avancée pour effectuer une sauvegarde complète de votre serveur Citrix ADM, vous pouvez désormais utiliser la nouvelle fonctionnalité de **reprise** d'activité disponible dans Citrix ADM version 12.1 pour effectuer une sauvegarde complète de votre configuration de haute disponibilité Citrix ADM et vous aider à résoudre les cas d'utilisation liés à la continuité des activités.

### Important

1. La fonctionnalité de sauvegarde avancée n'est plus disponible après la mise à niveau vers Citrix ADM 12.1. Pour supprimer la fonctionnalité de sauvegarde avancée et continuer à sauvegarder à l'aide de la fonctionnalité de reprise après sinistre, voir [Sauvegarder votre Citrix ADM après la mise à niveau vers Citrix ADM 12.1](#). La reprise après sinistre est prise en charge uniquement avec Citrix ADM HA.
2. Pour continuer à effectuer une sauvegarde partielle du serveur Citrix ADM incluant les

fichiers de configuration, les détails de l'instance, les données système, etc., puis pour restaurer votre serveur Citrix ADM dans le cadre d'un déploiement autonome (sauvegarde partielle), consultez [Comment sauvegarder et restaurer votre serveur Citrix ADM dans un déploiement à serveur unique](#).

En cas de sinistre sur le serveur principal, utilisez la fonction de reprise après sinistre pour démarrer et configurer Citrix ADM sur le même serveur principal sans perdre de données. La fonctionnalité n'est disponible que sur les serveurs Citrix ADM déployés dans une configuration haute disponibilité à partir de la version 12.1 de Citrix ADM.

### **Sauvegardez votre serveur Citrix ADM après la mise à niveau vers Citrix ADM 12.1**

Pour continuer à sauvegarder votre serveur Citrix ADM, Citrix recommande ce qui suit :

1. Supprimez vos paramètres de sauvegarde à distance sur Citrix ADM en procédant comme suit :
  - a) Accédez à **Système > Administration du système > Paramètres avancés de sauvegarde du système**.
  - b) Sur la page Configurer les paramètres de sauvegarde avancés, sélectionnez **Non** pour désactiver les sauvegardes à distance.
  - c) Cliquez sur **Appliquer les paramètres**. Attendez que votre serveur Citrix ADM redémarre et appliquez les paramètres modifiés.
  - d) Supprimez votre nœud de sauvegarde à distance.
2. Déployez et configurez un nouveau serveur Citrix ADM, créez une configuration haute disponibilité avec le serveur Citrix ADM existant qui a été redémarré à l'étape ci-dessus.
  - Pour en savoir plus sur le déploiement autonome de Citrix ADM, voir [Déployer Citrix ADM](#).
  - Pour en savoir plus sur le déploiement de Citrix ADM HA, consultez la section [Déploiement à haute disponibilité](#).
3. Configurez la reprise après sinistre pour continuer à sauvegarder et à restaurer les données. Pour plus d'informations sur la reprise après sinistre, voir [Configurer la reprise après sinistre pour une haute disponibilité](#).

### **Ajouter un disque supplémentaire au serveur Citrix ADM**

Si vos besoins en stockage Citrix ADM dépassent l'espace disque par défaut (120 gigaoctets), vous pouvez joindre un disque supplémentaire. Vous pouvez associer des disques supplémentaires à la fois dans le cadre de déploiements à serveur unique et à haute disponibilité.

Lorsque vous effectuez la mise à niveau de Citrix ADM de la version 12.0 vers la version 12.1, les partitions que vous aviez créées sur le disque supplémentaire dans la version précédente restent les mêmes. Les partitions ne sont pas supprimées et ne sont pas redimensionnées.

La procédure d'attachement d'un disque supplémentaire reste la même dans la version mise à niveau. Vous pouvez maintenant utiliser le nouvel outil de partitionnement de disque dans Citrix ADM pour créer des partitions dans le disque nouvellement ajouté. Vous pouvez également utiliser l'outil pour redimensionner les partitions du disque supplémentaire existant. Pour plus d'informations sur la façon d'attacher des disques supplémentaires et d'utiliser le nouvel outil de partitionnement de disque, consultez [Comment attacher un disque supplémentaire à Citrix ADM](#).

## Provisionner des instances Citrix ADC dans OpenStack à l'aide de StyleBooks

À partir de Citrix ADM 12.1 build 49.23, l'architecture du flux de travail d'orchestration OpenStack a été mise à jour. Le workflow utilise désormais Citrix ADM StyleBooks pour configurer les instances Citrix ADC. Si vous effectuez une mise à niveau vers Citrix ADM 12.1 build 49.23 à partir de la version 12.0 ou de la version 12.1 build 48.18, vous devez exécuter le script de migration suivant :

```
1 /mps/scripts/migration_scripts/migrate_configurations.py
2 <!--NeedCopy-->
```

Pour plus d'informations sur le StyleBook « os-cs-lb-mon » et le script de migration, consultez [Provisionnement d'une instance Citrix ADC VPX sur OpenStack à l'aide de StyleBook](#)

## Authentification

February 1, 2024

24 mai 2018

Les utilisateurs peuvent être authentifiés soit en interne par Citrix Application Delivery Management (ADM), soit en externe par un serveur d'authentification, soit les deux. Si l'authentification locale est utilisée, l'utilisateur doit se trouver dans la base de données de sécurité Citrix ADM. Si l'utilisateur est authentifié en externe, son « nom externe » doit correspondre à l'identité d'utilisateur externe enregistrée auprès du serveur d'authentification, en fonction du protocole d'authentification sélectionné.

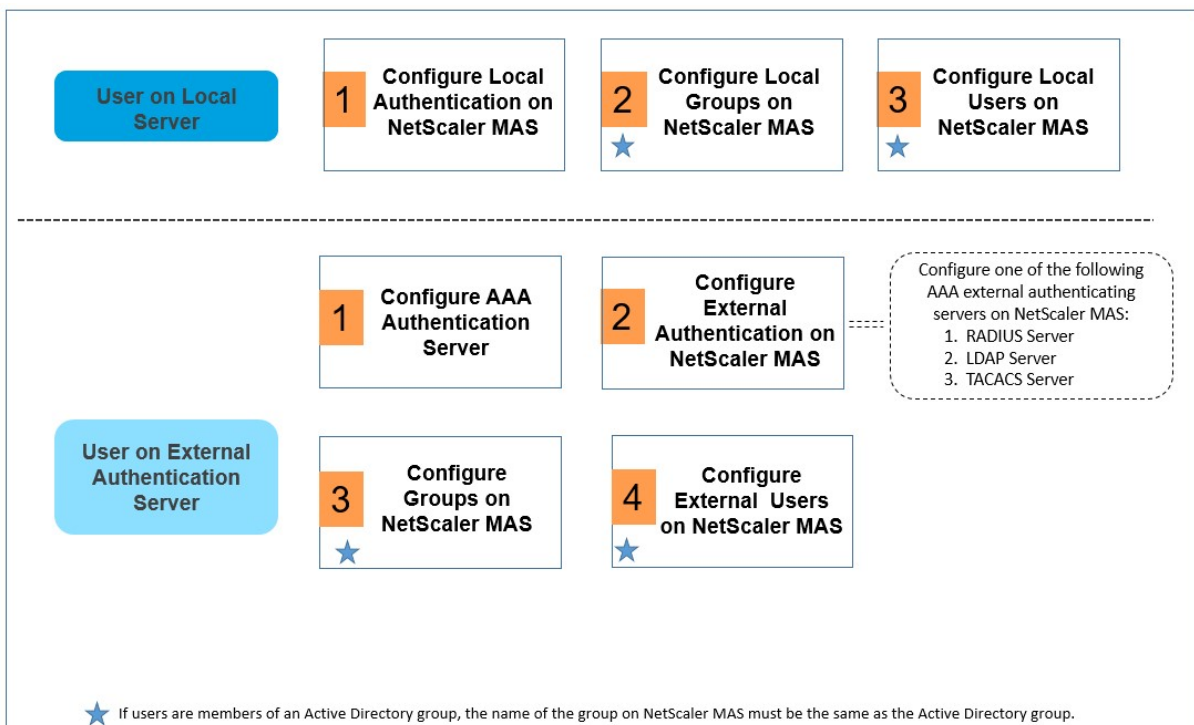
Citrix ADM prend en charge l'authentification externe au moyen des protocoles RADIUS, LDAP et TACACS. Ce support unifié fournit une interface commune pour authentifier et autoriser tous les utilisateurs de serveurs d'authentification, d'autorisation et de comptabilité (AAA) locaux et externes qui accèdent au système. Citrix ADM peut authentifier les utilisateurs quels que soient

les protocoles qu'ils utilisent pour communiquer avec le système. Lorsqu'un utilisateur tente d'accéder à une implémentation Citrix ADM configurée pour l'authentification externe, le serveur d'applications demandé envoie le nom d'utilisateur et le mot de passe au serveur RADIUS, LDAP ou TACACS pour authentification. Si l'authentification est réussie, le protocole correspondant est utilisé pour identifier l'utilisateur dans Citrix ADM.

Vous pouvez authentifier vos utilisateurs dans Citrix ADM de deux manières :

- À l'aide de serveurs locaux Citrix ADM
- En utilisant des serveurs d'authentification externes

L'organigramme suivant montre le flux de travail à suivre lorsque vous authentifiez des utilisateurs locaux ou externes :



## Configuration de serveurs d'authentification externes

Citrix ADM prend en charge divers protocoles pour fournir des services externes d'authentification, d'autorisation et de comptabilité (AAA).

Citrix ADM envoie toutes les demandes de service d'authentification, d'autorisation et de comptabilité (AAA) au serveur RADIUS, LDAP ou TACACS+ distant. Le serveur AAA distant reçoit la demande, la valide et renvoie une réponse à Citrix ADM. Lorsqu'il est configuré pour utiliser un serveur RADIUS, TACACS+ ou LDAP distant pour l'authentification, Citrix ADM devient un client RADIUS, TACACS+ ou LDAP. Dans l'une de ces configurations, les enregistrements d'authentification sont stockés dans la

base de données du serveur hôte distant. Le nom du compte de connexion et de déconnexion, les autorisations attribuées et les enregistrements de comptabilisation du temps sont également stockés sur le serveur AAA pour chaque utilisateur.

En outre, vous pouvez utiliser la base de données interne de Citrix ADM pour authentifier les utilisateurs localement. Vous créez des entrées dans la base de données pour les utilisateurs, leurs mots de passe et leurs rôles par défaut. Vous pouvez également créer des groupes de serveurs 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 des serveurs de différents types dans un groupe et vous pouvez également inclure la base de données interne en tant que sauvegarde d'authentification de secours dans la liste configurée de serveurs AAA.

### **Configuration d'un serveur d'authentification RADIUS**

Vous pouvez configurer Citrix ADM pour authentifier l'accès des utilisateurs auprès d'un ou de plusieurs serveurs RADIUS. Votre configuration peut nécessiter l'utilisation d'une adresse IP de serveur d'accès réseau (IP NAS) ou d'un identifiant de serveur d'accès réseau (ID NAS). Lorsque vous configurez Citrix ADM pour utiliser un serveur d'authentification RADIUS, suivez les instructions suivantes : Si vous activez l'utilisation de l'adresse IP du NAS, l'appliance envoie son adresse IP configurée au serveur RADIUS, au lieu d'envoyer l'adresse IP source utilisée pour établir la connexion RADIUS.

- Si vous configurez l'ID NAS, l'appliance envoie l'identificateur au serveur RADIUS. Si vous ne configurez pas l'ID NAS, l'appliance envoie son nom d'hôte au serveur RADIUS.
- Si vous activez l'adresse IP du NAS, l'appliance ignore tout identifiant NAS configuré et utilise l'adresse IP du NAS pour communiquer avec le serveur RADIUS.

#### **Pour configurer un serveur d'authentification RADIUS :**

1. Dans Citrix ADM, accédez à **Système > Authentification > RADIUS** .
2. Sur la page **RADIUS** , cliquez sur **Ajouter** .
3. Sur la page **Créer un serveur RADIUS** , définissez les paramètres et cliquez sur **Créer** pour ajouter le serveur à la liste des serveurs d'authentification RADIUS. Les paramètres suivants sont obligatoires :
  - a) **Nom**. Nom du serveur RADIUS.
  - b) **Nom du serveur/adresse IP** . Nom du serveur ou adresse IP du serveur RADIUS.
  - c) **Port**. Par défaut, le port 1812 est utilisé pour l'authentification RADIUS. Vous pouvez spécifier un autre numéro de port si nécessaire.

- d) **Délai d'attente (secondes)**. Durée, en secondes, pendant laquelle le système Citrix ADM attend une réponse du serveur RADIUS.
  - e) **Clé secrète**. Toute expression alphanumérique. Il s'agit de la clé partagée entre Citrix ADM et le serveur RADIUS pour permettre la communication.
4. Cliquez sur **Détails** pour développer la section et définir les paramètres supplémentaires, puis cliquez sur **Créer**.

Pour plus de détails sur l'ajout de serveurs RADIUS, consultez [Comment ajouter des serveurs d'authentification RADIUS.] (</en-us/netscaler-application-delivery-management-software/12-1/authentication/authentication-how-to-articles/add-radius-authentication-server.html>)

### Configuration d'un serveur d'authentification LDAP

Vous pouvez configurer Citrix ADM pour authentifier l'accès des utilisateurs auprès d'un ou de plusieurs serveurs LDAP. L'autorisation LDAP nécessite des noms de groupe identiques dans Active Directory, sur le serveur LDAP et sur Citrix ADM. Les caractères et la casse doivent également correspondre.

#### Pour configurer un serveur d'authentification LDAP :

1. Dans Citrix ADM, accédez à **Système > Authentification > LDAP** .
2. Sur la page **LDAP**, cliquez sur **Ajouter**.
3. Sur la page **Créer un serveur LDAP**, définissez les paramètres et cliquez sur **Créer** pour ajouter le serveur à la liste des serveurs d'authentification LDAP. Les paramètres suivants sont obligatoires :
  - a) **Nom**. Nom du serveur LDAP.
  - b) **Nom du serveur/adresseIP**. Nom du serveur ou adresse IP du serveur LDAP.
  - c) **Type de sécurité**. Type de communication requis entre le système et le serveur LDAP. Sélectionnez dans la liste déroulante. 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 l'authentification LDAP. Vous pouvez spécifier un autre numéro de port si nécessaire.
  - e) **Type de serveur**. Sélectionnez **Active Directory (AD)** ou **Novell Directory Service (NDS)** comme type de serveur LDAP.
  - f) **Délai d'expiration (secondes)**. Durée, en secondes, pendant laquelle le système Citrix ADM attend une réponse du serveur LDAP.

Vous pouvez fournir des informations supplémentaires. Vous pouvez également valider le certificat LDAP en cochant la case **Valider le certificat LDAP** et en spécifiant le nom d'hôte à saisir sur le certificat. Parmi les paramètres supplémentaires que vous pouvez ajouter, citons les détails du serveur de noms de domaine (DN) pour les requêtes concernant un service d'annuaire, le groupe d'authentification par défaut, les attributs de groupe et d'autres attributs.

Le DN de base est généralement dérivé du DN de liaison en supprimant le nom d'utilisateur et en spécifiant le groupe auquel appartiennent les utilisateurs. Dans la zone de texte Administrator Bind DN, tapez le DN de liaison administrateur pour les requêtes adressées à l'annuaire LDAP.

Voici des exemples de syntaxe pour le DN de base :

- ou=utilisateurs, dc=ace, dc=com
- CN=Utilisateurs, dc=ace, dc=com

Voici des exemples de syntaxe pour bind DN :

- nom de domaine/utilisateur
- ou=administrateur, dc=ace, dc=com
- user@domain.name (pour Active Directory)
- CN=Administrateur, CN=Utilisateurs, dc=ace, dc=com

Le nom du groupe et le nom des utilisateurs que vous définissez dans Citrix ADM doivent être similaires à ceux configurés sur le serveur LDAP.

#### Remarque

Lors de la configuration d'un serveur RADIUS ou LDAP, dans la section **Détails**, vous pouvez saisir le nom d'un **groupe d'authentification par défaut**. Ce groupe par défaut est choisi pour autoriser l'utilisateur lorsque l'authentification réussit, que l'utilisateur soit lié à un groupe ou non. L'utilisateur reçoit ensuite une combinaison d'autorisations configurées sur ce groupe par défaut et sur les autres groupes, qu'il soit affecté au groupe ou non.

Pour plus de détails sur l'ajout de serveurs LDAP, consultez [Comment ajouter des serveurs d'authentification LDAP](#).

Pour plus de détails sur la mise en cascade de serveurs d'authentification externes, consultez [Comment mettre en cascade des serveurs d'authentification externes](#).

### Configuration d'un serveur d'authentification TACACS

TACACS, comme RADIUS et LDAP, gère les services d'authentification à distance pour l'accès au réseau.

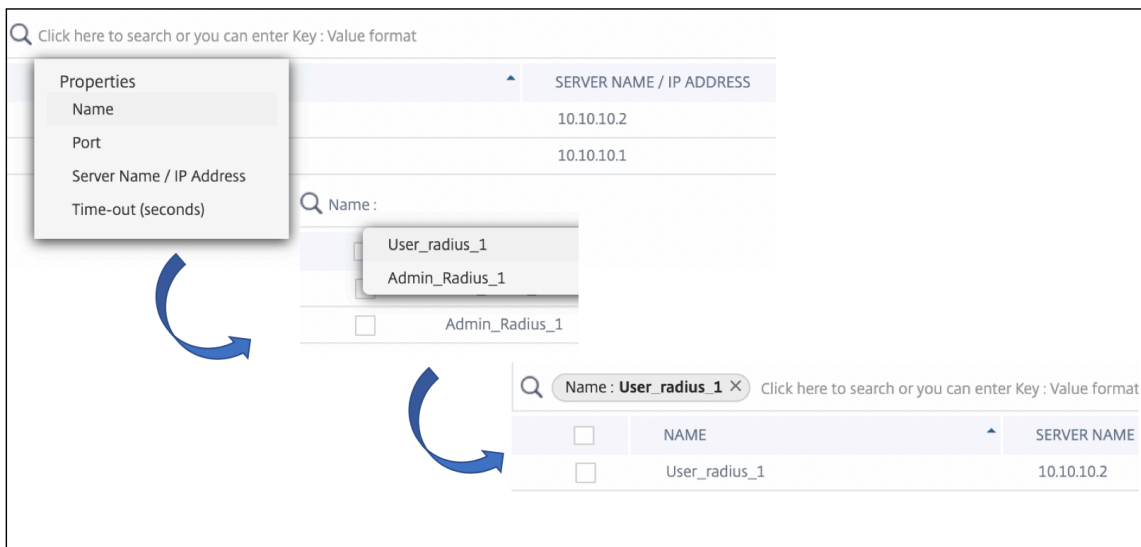
### Configurez un serveur d'authentification TACACS :

1. Dans **Citrix ADM** , accédez à **Système > Authentification > TACACS** .
2. Sur la page **TACACS** , cliquez sur **Ajouter** .
3. Sur la page **Créer un serveur TACACS** , entrez les informations suivantes :
  - a) Nom du serveur TACACS
  - b) Adresse IP du serveur TACACS
  - c) Port et délai d'expiration (en secondes)
  - d) Clé partagée par le système et le serveur TACACS pour la communication.
  - e) Sélectionnez Comptabilité si vous souhaitez que l'apppliance enregistre les informations d'audit avec le serveur TACACS.
4. Cliquez sur **Créer**.

Pour plus de détails sur l'ajout de serveurs TACACS, consultez [Comment ajouter des serveurs d'authentification TACACS](#) .

#### Remarque

Pour rechercher les serveurs d'authentification ajoutés dans Citrix ADM, cliquez dans la barre de recherche et sélectionnez les critères de recherche requis.



### Configurer une authentification locale des utilisateurs dans Citrix ADM

Si vous utilisez l'authentification locale, créez des utilisateurs, puis ajoutez-les aux groupes que vous créez sur Citrix ADM. Après avoir configuré les utilisateurs et les groupes, vous pouvez appliquer des



stratégies d'autorisation et de session, créer des signets, spécifier des applications et spécifier l'adresse IP des partages de fichiers et des serveurs auxquels les utilisateurs ont accès.

#### **Pour configurer une authentification locale dans Citrix ADM :**

1. Dans Citrix ADM, accédez à **Système > Authentification**, puis cliquez sur **Configuration de l'authentification**.
2. Sur la page **Configuration de l'authentification**, sélectionnez **LOCAL** dans la liste déroulante **Type de serveur**, puis cliquez sur **OK**.

#### **Configurer une authentification externe dans Citrix ADM**

Lorsque vous configurez des serveurs d'authentification externes dans Citrix ADM, les groupes d'utilisateurs authentifiés sur ces serveurs externes sont importés dans Citrix ADM. Il n'est pas nécessaire de créer des utilisateurs sur Citrix ADM. Les utilisateurs sont gérés sur les serveurs externes depuis Citrix ADM. Vous devez toutefois vous assurer que les niveaux d'autorisation des groupes d'utilisateurs sur les serveurs d'authentification externes sont conservés dans Citrix ADM. Citrix ADM autorise les utilisateurs en attribuant des autorisations de groupe pour l'accès à des serveurs virtuels d'équilibrage de charge spécifiques et à des applications spécifiques du système. Si un serveur d'authentification est ultérieurement supprimé du système, les groupes et les utilisateurs seront automatiquement supprimés du système.

#### **Pour configurer une authentification externe dans Citrix ADM, procédez comme suit :**

1. Dans Citrix ADM, accédez à **Système > Authentification**, puis cliquez sur **Configuration de l'authentification**.
2. Sur la page **Configuration de l'authentification**, sélectionnez **EXTERNE** dans la liste déroulante **Type de serveur**.
3. Cliquez sur **Insérer**.
4. Sur la page **Serveurs externes**, sélectionnez un serveur d'authentification. Vous pouvez éventuellement sélectionner plusieurs serveurs d'authentification à mettre en cascade.

##### **Remarque**

Seuls les serveurs externes peuvent être mis en cascade.

5. Sélectionnez **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. Cliquez sur **OK** pour fermer la page.

Les serveurs sélectionnés sont affichés sur la page **Serveurs d'authentification**.

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.

## Configurer des groupes dans Citrix ADM

Citrix ADM vous permet d'authentifier et d'autoriser vos utilisateurs en créant des groupes et en ajoutant les utilisateurs aux groupes. Un groupe peut avoir des autorisations « administrateur » ou « lecture seule » et tous les utilisateurs de ce groupe recevront les mêmes autorisations.

Dans Citrix ADM, un groupe est défini comme un ensemble d'utilisateurs disposant d'autorisations similaires. Un groupe peut avoir un ou plusieurs rôles. Un utilisateur est défini comme une entité qui peut avoir accès en fonction des autorisations attribuées. Un utilisateur peut appartenir à un ou plusieurs groupes.

Vous pouvez créer des groupes locaux dans Citrix ADM et utiliser l'authentification locale pour les utilisateurs des groupes. Si vous utilisez des serveurs externes pour l'authentification, configurez les groupes sur Citrix ADM pour qu'ils correspondent aux groupes configurés sur les serveurs d'authentification du réseau interne. Lorsqu'un utilisateur ouvre une session et est authentifié, si un nom de groupe correspond à un groupe sur un serveur d'authentification, l'utilisateur hérite des paramètres du groupe sur Citrix ADM.

Après avoir configuré les groupes, vous pouvez appliquer des stratégies d'autorisation et de session, créer des signets, spécifier des applications et spécifier les adresses IP des partages de fichiers et des serveurs auxquels l'utilisateur a accès.

Si vous utilisez l'authentification locale, créez des utilisateurs et ajoutez-les à des groupes configurés sur Citrix ADM. Les utilisateurs héritent ensuite des paramètres de ces groupes.

### Remarque

Si les utilisateurs sont membres d'un groupe Active Directory, le nom du groupe et les noms des utilisateurs sur Citrix ADM doivent être identiques à ceux du groupe Active Directory.

### Pour configurer des groupes d'utilisateurs dans Citrix ADM, procédez comme suit :

1. Dans Citrix ADM, accédez à **Système > Administration des utilisateurs > Groupes**.
2. Sur la page **Groupes**, cliquez sur **Ajouter** pour créer un groupe. Par défaut, deux groupes sont créés dans Citrix ADM, avec des autorisations définies sur admin et en lecture seule. Vous pouvez ajouter vos utilisateurs à ces groupes ou créer d'autres groupes pour vos utilisateurs.
3. Dans l'onglet **Paramètres du groupe** de la page **Créer un groupe de systèmes**, saisissez le nom du groupe et définissez les **rôles** en tant qu'administrateur ou en lecture seule. Vous pouvez sélectionner **Configurer le délai d'expiration de la session** utilisateur pour définir une limite de délai pour les sessions utilisateur connectées pour ce groupe.

### Remarque

Assurez-vous que le nom du groupe d'utilisateurs créé sur Citrix ADM est le même que sur les serveurs d'authentification externes. Dans le cas contraire, le système ne reconnaîtra pas le groupe et les membres du groupe ne seront pas extraits dans le système.

4. Dans l'onglet **Paramètres d'autorisation**, sélectionnez les groupes requis. Cliquez sur **Créer un groupe**.
5. Dans l'onglet **Attribuer des utilisateurs**, sélectionnez les utilisateurs que vous souhaitez ajouter au groupe. Les utilisateurs sont ajoutés à ce tableau lorsque vous configurez les utilisateurs dans [Configurer les utilisateurs dans Citrix ADM](#).
6. Cliquez sur **Terminer**.

Lorsque vous avez fini de créer un groupe dans le système, tous les utilisateurs du serveur d'authentification externe sont extraits dans le système. Si le nom du groupe correspond au nom du groupe sur le serveur d'authentification externe, l'utilisateur hérite de toutes les définitions d'autorisation lorsqu'il est connecté au système.

## Configurer les utilisateurs dans Citrix ADM

Vous pouvez créer des comptes d'utilisateurs localement sur Citrix ADM pour compléter les utilisateurs sur les serveurs d'authentification. Par exemple, vous pouvez créer des comptes d'utilisateurs locaux pour des utilisateurs temporaires, tels que des consultants ou des visiteurs, sans créer d'entrée pour ces utilisateurs sur le serveur d'authentification. Si vous authentifiez localement des utilisateurs présents sur des serveurs d'authentification externes, assurez-vous que les mêmes utilisateurs sont présents à la fois sur les serveurs d'authentification et sur Citrix ADM.

### Pour configurer des utilisateurs dans Citrix ADM :

1. Dans Citrix ADM, accédez à **Système > Administration des utilisateurs > Utilisateurs**.
2. Sur la page **Utilisateurs**, cliquez sur **Ajouter** pour ajouter des utilisateurs à Citrix ADM.
3. Sur la page **Créer un utilisateur système**, définissez les paramètres suivants :
  - a) **Nom d'utilisateur**. Nom de l'utilisateur
  - b) **Mot de passe**. Mot de passe que l'utilisateur utilisera pour se connecter à Citrix ADM
  - c) **Activez l'authentification externe**. Si cette option n'est pas activée, l'utilisateur sera authentifié en tant qu'utilisateur local.
  - d) **Configurez le délai d'expiration de la session utilisateur**. Durée pendant laquelle un utilisateur peut rester actif. Cette période peut être définie en minutes ou en heures.

4. Dans le tableau **Groupes** , sélectionnez le groupe auquel vous souhaitez ajouter l'utilisateur. Les membres du groupe sont ajoutés à ce tableau lorsque vous configurez des groupes dans Configuration des groupes d'utilisateurs dans Citrix ADM .
5. Cliquez sur **Créer**.

#### Remarque

Si les utilisateurs sont sur Active Directory, assurez-vous que le nom du groupe dans Citrix ADM est identique à celui du groupe Active Directory sur le serveur externe.

## Comment extraire un groupe de serveurs d'authentification

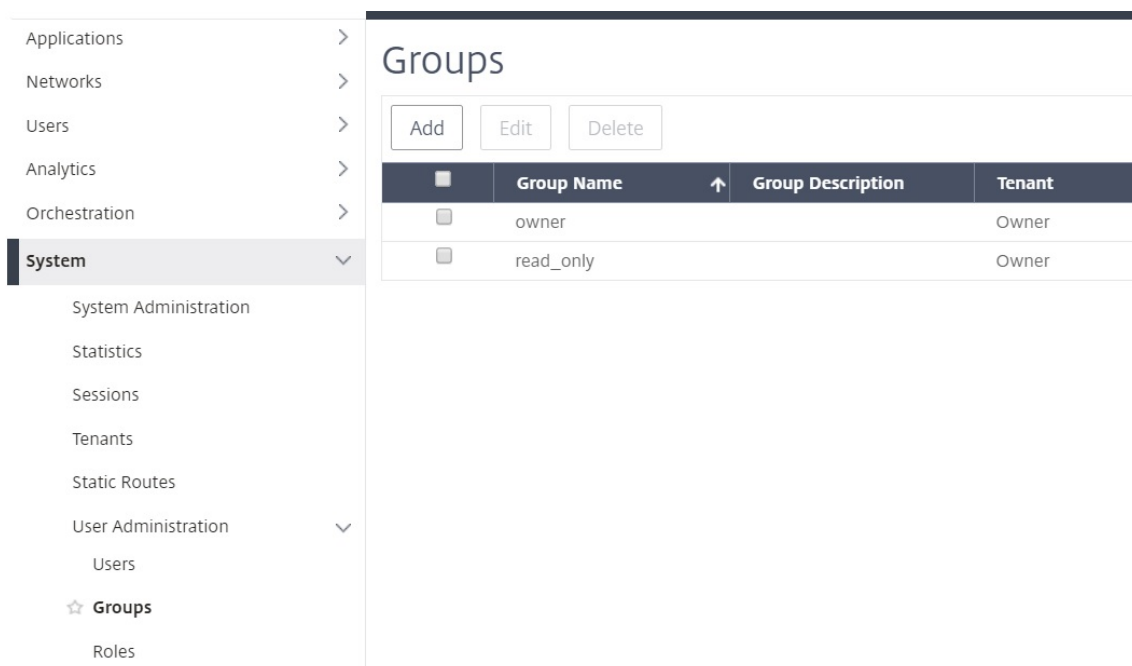
February 1, 2024

Citrix Application Delivery Management (ADM) vous permet d'extraire le groupe d'utilisateurs existant sur le serveur d'authentification externe et de leur attribuer des autorisations en fonction de leurs rôles et conformément aux définitions de Citrix ADC. Cela présente deux avantages :

1. Il n'est pas nécessaire de créer des utilisateurs sur Citrix ADM. Bien que les groupes soient extraits vers le serveur Citrix ADM, ils sont gérés sur les serveurs externes à partir du serveur Citrix ADM plutôt que de les ajouter au système.
2. Citrix ADM effectue l'autorisation des utilisateurs en attribuant des autorisations de groupe pour accéder à des serveurs virtuels d'équilibrage de charge spécifiques et à des applications spécifiques sur le système. À l'avenir, lorsque le serveur d'authentification en question sera supprimé du système, les groupes et les utilisateurs seront automatiquement supprimés du système.

### Configuration des groupes et attribution des autorisations aux groupes

1. Dans Citrix ADM, accédez à **Système > Administration des utilisateurs > Groupes**.
2. Cliquez sur **Ajouter** pour créer un groupe.



The screenshot shows the NetScaler ADM interface. On the left, a navigation sidebar is visible with the following items: Applications, Networks, Users, Analytics, Orchestration, System (selected), System Administration, Statistics, Sessions, Tenants, Static Routes, User Administration (expanded to show Users), Groups (highlighted with a star), and Roles. The main content area is titled 'Groups' and contains three buttons: 'Add', 'Edit', and 'Delete'. Below these buttons is a table with the following data:

<input type="checkbox"/>	Group Name	↑	Group Description	Tenant
<input type="checkbox"/>	owner			Owner
<input type="checkbox"/>	read_only			Owner

3. Dans l'onglet **Paramètres du groupe**, tapez le nom du groupe, définissez les autorisations comme admin, readonly, AppReadOnly ou AppAdmin. Les autres options que vous pouvez configurer sont le délai d'expiration de session, dans lequel vous pouvez définir une limite de délai d'expiration pour les sessions connectées aux utilisateurs de ce groupe, et vous pouvez également définir les instances de machine virtuelle auxquelles les membres du groupe peuvent accéder.

#### Remarque

Assurez-vous que le nom du groupe d'utilisateurs créé sur Citrix ADM est exactement le même que celui créé sur les serveurs d'authentification externes. Sinon, le système ne reconnaîtra pas le groupe et les membres du groupe ne seront pas extraits dans le système.

## ← Create System Group

Group Settings
 Authorization Settings
 Assign Users

Group Name\*  
 ?

Group Description  
 ?

Roles\*

Available (3)  Select All

appReadOnly	+
appAdmin	+
readonly	+

New | Edit

Configured (1)  Remove All

admin	-
-------	---

Configure User Session Timeout

4. Dans l'onglet **Paramètres d'autorisation**, vous pouvez fournir des paramètres d'autorisation pour les quatre groupes suivants :

- Instances
- Applications
- Modèles de configuration
- StyleBooks

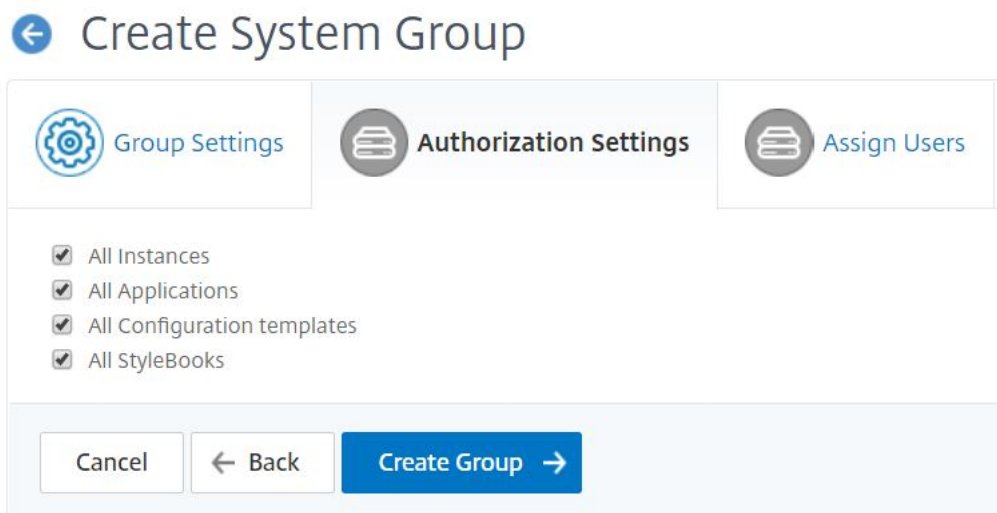
Par défaut, votre utilisateur peut accéder à tous les groupes ci-dessus. Vous pouvez désactiver les cases à cocher et fournir un accès sélectif à chacun de ces groupes.

Par exemple :

- Vous pouvez **décocher** la case Instances et sélectionner uniquement les instances requises auxquelles vous souhaitez donner accès à vos utilisateurs.
- Désactivez la case à cocher **Toutes les applications** et sélectionnez uniquement les applications et les modèles requis. Lorsque vous ajoutez des applications à un groupe dans Citrix ADM, vous pouvez utiliser une expression régulière pour rechercher et ajouter les applications

qui répondent aux critères d'expression régulière pour les groupes. Les utilisateurs liés à ces groupes ne peuvent accéder qu'à ces applications spécifiques. L'expression regex spécifiée est conservée dans Citrix ADM. C'est-à-dire que Citrix ADM autorise le stockage de l'expression régulière fournie dans la zone de texte **Ajouter une expression régulière** dans le système et met à jour dynamiquement la portée d'autorisation chaque fois que de nouvelles applications répondent à cette expression régulière. Lorsque de nouvelles applications sont ajoutées au système, Citrix ADM applique les critères de recherche aux nouvelles applications, et l'application qui répond aux critères est ajoutée dynamiquement au groupe. Il n'est pas nécessaire d'ajouter manuellement les nouvelles applications au groupe. Les applications sont mises à jour dynamiquement dans le système, et les utilisateurs du groupe concerné peuvent voir les applications sous les modules appropriés dans Citrix ADM.

- Décochez la case **Tous les modèles de configuration** pour autoriser l'accès uniquement aux modèles requis.
- Décochez la case **Tous les StyleBooks** et sélectionnez les StyleBooks requis auxquels votre utilisateur peut accéder.
- 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. Les packs de configuration de ce StyleBook sont également inclus dans ce que l'utilisateur a accès.



Lorsque vous avez fini de créer un groupe dans le système, tous les utilisateurs du serveur d'authentification externe sont extraits dans le système. Vous pouvez le vérifier en sélectionnant le groupe et en cliquant sur **Modifier**. Le tableau Utilisateurs de Create System Group affiche la liste des utilisateurs connectés au groupe. Vous pouvez également attribuer des utilisateurs au groupe dans l'onglet **Attribuer des utilisateurs**.

Si le nom du groupe correspond au nom du groupe sur le serveur d'authentification externe, l'utilisateur hérite de toutes les définitions d'autorisation lorsqu'il est connecté au système.

## Ajouter un serveur d'authentification LDAP

February 1, 2024

Lorsque vous intégrez le protocole LDAP aux serveurs d'authentification RADIUS et TACAS, vous pouvez utiliser Citrix ADM pour rechercher et authentifier les informations d'identification des utilisateurs à partir d'annuaires distribués.

1. Accédez à **Système > Authentification**.
2. Sélectionnez l'onglet **LDAP**, puis cliquez sur **Ajouter**.
3. Sur la page **Créer un serveur LDAP**, spécifiez les paramètres suivants :
  - a) **Nom** : spécifiez le nom du serveur LDAP
  - b) **Nom du serveur/adresse IP** — **Spécifiez l'adresse IP** LDAP ou le nom du serveur
  - c) **Type de sécurité** : type de communication requis entre le système et le serveur LDAP. Sélectionnez dans la liste. Si la communication en texte brut est inadéquate, vous pouvez choisir une communication cryptée en sélectionnant Transport Layer Security (TLS) ou SSL
  - d) **Port** — Par défaut, le port 389 est utilisé pour PLAINTEXT. Vous pouvez également spécifier le port 636 pour SSL/TSL
  - e) **Type de serveur** : sélectionnez Active Directory (AD) ou Novell Directory Service (NDS) comme type de serveur LDAP
  - f) **Délai d'attente (secondes)** : durée en secondes pendant laquelle le système Citrix ADM attend une réponse du serveur LDAP
  - g) **Nom d'hôte LDAP** — Activez la case à cocher Valider le certificat LDAP et spécifiez le nom d'hôte à saisir sur le certificat

Désactivez l'option **Authentification** et spécifiez la clé publique SSH. Avec l'authentification par clé, vous pouvez récupérer la liste des clés publiques stockées sur l'objet utilisateur. Ces clés publiques sont stockées sur le serveur LDAP via SSH.



The screenshot shows a configuration form for LDAP connection parameters. The fields are as follows:

- Name\***: Citrix LDAP
- Server Name / IP Address\***: 10.203.71.38
- Security Type\***: PLAINTEXT
- Port\***: 389
- Server Type\***: AD
- Time-out (seconds)\***: 10
- Validate LDAP Certificate**
- LDAP Host Name**: Certificate name
- Authentication**
- SSH Public key\***: (empty field)

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

The screenshot shows the 'Connection Settings' section of the configuration form. The fields are as follows:

- Base DN (location of users)**: dc
- Administrator Bind DN**: (empty field)
- BindDN Password**
- Administrative Password**: (masked with dots)
- Confirm Administrative Password**: (masked with dots)
- [Retrieve Attributes](#)
- Enable Change Password**

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 produirait une chaîne de recherche LDAP de `:. &(vpnallowed=true)(samaccount=bob)`
- iii. **Attribut de groupe** : sélectionnez MemberOf dans la liste.
- iv. **Nom du sous-attribut** : nom du sous-attribut pour l'extraction de groupes depuis le serveur LDAP.

- v. **Groupe d'authentification** par défaut : groupe par défaut à choisir lorsque l'authentification aboutit, en plus des groupes extraits.

#### 4. Cliquez sur **Créer**.

Le serveur LDAP est maintenant configuré.

##### Remarque

Si les utilisateurs sont des membres du groupe Active Directory, le groupe et les noms des utilisateurs sur Citrix ADM doivent avoir les mêmes noms que les membres du groupe Active Directory.

## Comment activer l'authentification locale de secours

February 1, 2024

La fonction d'authentification locale de secours permet à l'authentification locale de prendre le relais en cas d'échec de l'authentification externe. Un utilisateur configuré à la fois sur Citrix Application Delivery Management (ADM) et sur un serveur d'authentification externe peut se connecter à Citrix ADM, même si le serveur d'authentification externe configuré est en panne ou inaccessible. Pour que l'authentification locale de secours fonctionne, assurez-vous de prendre en compte les trois facteurs suivants :

- Vous devriez pouvoir accéder à Citrix ADM même après la panne du serveur d'authentification externe.
- Vous devez être configuré à la fois sur Citrix ADM et sur le serveur d'authentification externe.
- Vous devez ajouter au moins un serveur externe.

**Pour activer l'authentification locale de secours, procédez comme suit :**

1. Dans Citrix ADM, accédez à **Système > Authentification** , puis cliquez sur **Configuration de l'authentification** .
2. Sélectionnez **EXTERNE** dans la liste Type de serveur.

**Remarque** Si vous sélectionnez **LOCAL** dans la liste, l'authentification des utilisateurs s'effectue sur le serveur d'authentification local par défaut.

3. Cliquez sur **Insérer**, sélectionnez un serveur externe dans la liste des serveurs externes affichée, puis cliquez sur **OK** pour ajouter le serveur externe.

**Remarque** Vous devez déjà avoir ajouté les serveurs externes avant cette étape pour les faire apparaître dans la liste. Pour plus d'informations sur l'ajout de serveurs externes, consultez les articles suivants :

- [Comment ajouter des serveurs Radius](#)
- [Comment ajouter des serveurs LDAP](#)
- [Comment ajouter des serveurs TACACS](#)

4. Sélectionnez l'option **Activer l'authentification locale** de secours .

## ← Authentication Configuration

The appliance can authenticate users with local user accounts or by using an external authentication server.

Server Type\*

EXTERNAL

External Servers

<input type="checkbox"/>	Server Type	Server Name
<input checked="" type="checkbox"/>	RADIUS	RADIUS R1
<input checked="" type="checkbox"/>	RADIUS	RADIUS R2

Enable fallback local authentication

## Comment ajouter des serveurs d'authentification RADIUS

February 1, 2024

Un serveur d'authentification RADIUS fonctionne à l'aide du protocole UDP (User Datagram Protocol). Le serveur RADIUS reçoit la demande de connexion d'un utilisateur et l'authentifie. Le serveur renvoie ensuite les informations de configuration au système qui fournit les services à l'utilisateur. Le serveur RADIUS est connecté à un serveur d'accès réseau (NAS). Lorsque le NAS envoie une demande d'accès, le serveur RADIUS recherche le nom d'utilisateur et d'autres informations dans sa base de données. Si le nom d'utilisateur n'existe pas dans la base de données, le serveur RADIUS envoie immédiatement un message de rejet d'accès ou peut charger un profil par défaut sur Citrix ADM. Dans RADIUS, l'authentification et l'autorisation sont couplées. Si les informations de l'utilisateur sont authentifiées, le serveur RADIUS renvoie une réponse Access-Accept. Il envoie également une liste de paires attribut-valeur qui décrivent les paramètres à utiliser pour cette session particulière.

### Configuration d'un serveur d'authentification RADIUS

1. Dans Citrix ADM, accédez à **Système > Authentification > RADIUS**.
2. Sur la page **RADIUS**, cliquez sur **Ajouter**.
3. Sur la page **Créer un serveur RADIUS**, définissez les paramètres, puis cliquez sur **Créer** pour ajouter le serveur à la liste des serveurs d'authentification RADIUS.
4. Les paramètres suivants sont obligatoires pour créer le serveur RADIUS :
  - **Nom**: entrez le nom du serveur RADIUS
  - **Nom du serveur/Adresse IP** : saisissez le nom du serveur ou l'adresse IP du serveur RADIUS
  - **Port**: par défaut, le port 1812 est utilisé pour les messages d'authentification RADIUS. Vous pouvez spécifier un autre numéro de port, si nécessaire.
  - **Délai d'attente (secondes)**: saisissez le nombre de secondes. Durée pendant laquelle le système Citrix ADM attend une réponse du serveur RADIUS.
  - **Clé secrète** : saisissez n'importe quelle expression alphanumérique. Clé partagée entre Citrix ADM et le serveur RADIUS pour la communication.
5. Cliquez sur **Détails** pour développer la section et définir les paramètres supplémentaires.

## ← Create RADIUS Server

Name*	<input type="text" value="Admin_radius_1"/>	?
Server Name / IP Address*	<input type="text" value="10.10.10.0"/>	?
Port*	<input type="text" value="1812"/>	
Time-out (seconds)*	<input type="text" value="3"/>	
Secret Key*	<input type="password" value="....."/>	?
Confirm Secret Key*	<input type="password" value="....."/>	?

▶ Details

Vous pouvez fournir d'autres informations facultatives lors de l'ajout d'un serveur RADIUS. Certains des paramètres supplémentaires que vous pouvez saisir sont les détails du NAS, les informations sur le fournisseur, les informations sur les attributs et le type d'authentification par mot de passe.

### Remarque

Pour que l'authentification RADIUS fonctionne, assurez-vous que le groupe configuré sur Citrix ADM et le groupe extrait via l'utilisateur RADIUS sont identiques. L'utilisateur est autorisé en fonction des autorisations attribuées au groupe.

Par exemple, considérez un scénario dans le serveur FreeRADIUS, où

- Mot de passe en texte clair = « 1.citrix »
- Group-Names = « radiusgroup1, group1 »

Dans ce cas, l'utilisateur appartient à deux groupes : radiusgroup1 et group1. Dans ce cas, le séparateur de groupes est «

, » Si vous vous connectez à Citrix ADM en tant qu'utilisateur RADIUS « RadiusUser1 » appartenant au groupe « radiusgroup1 », assurez-vous que le même nom de groupe « radiusgroup1 » est également configuré sur Citrix ADM.

localisée Fournissez les détails concernant l'identifiant du fournisseur, le type d'attribut, le séparateur de groupes (le cas échéant) pour que l'extraction du groupe se fasse comme indiqué dans l'image suivante.

```
#
# Created for Citrix Use
# currently only using attribute 6 in this setup.

VENDOR Citrix 66

BEGIN-VENDOR Citrix
ATTRIBUTE Group-Names 6 string
END-VENDOR Citrix
```

## Comment ajouter des serveurs d'authentification TACACS

February 1, 2024

TACACS, avec RADIUS et LDAP, gère les services d'authentification à distance pour l'accès au réseau.

### Configuration d'un serveur d'authentification TACACS

1. Dans **Citrix ADM**, accédez à **Système > Authentification > TACACS**.
2. Sur la page **TACACS**, cliquez sur **Ajouter**.
3. Sur la page **Créer un serveur TACACS**, entrez les informations suivantes :
  - a) Nom du serveur TACACS
  - b) Adresse IP du serveur TACACS
  - c) Port et délai d'expiration en secondes
  - d) Tapez la clé partagée par le système et le serveur TACACS pour la communication.
4. Sélectionnez **Comptabilité** si vous souhaitez que l'appliance enregistre les informations d'audit sur le serveur TACACS.
5. Cliquez sur **Créer**.

## ← Create TACACS Server

Name\*  
 ?

IP Address\*  
 ?

Port\*

Time-out (seconds)\*

TACACS Key\*  
 ?

Confirm TACACS Key\*  
 ?

Accounting ?

## Comment monter en cascade des serveurs d'authentification externes

February 1, 2024

Un Citrix Application Delivery Management (ADM) prend en charge un système unifié de protocoles d'authentification, d'autorisation et de comptabilité (AAA), notamment RADIUS, LDAP et TACACS, en plus de prendre en charge les serveurs locaux pour authentifier les utilisateurs et les groupes locaux. Le support unifié fournit une interface commune pour authentifier et autoriser tous les clients AAA locaux et externes qui accèdent au système. Citrix ADM peut authentifier les utilisateurs quels que soient les protocoles qu'ils communiquent avec le système.

La mise en cascade des serveurs d'authentification externes fournit un processus continu sans échec pour l'authentification et l'autorisation des utilisateurs externes. Si l'authentification échoue sur le



premier serveur d'authentification, Citrix ADM tente d'authentifier l'utilisateur à l'aide du second serveur d'authentification externe, etc. Pour activer l'authentification en cascade, vous devez ajouter les serveurs d'authentification externes à Citrix ADM. Vous pouvez ajouter n'importe quel type de serveurs d'authentification externes pris en charge (RADIUS, LDAP et TACACS). Par exemple, si vous souhaitez ajouter quatre serveurs d'authentification externes pour l'authentification en cascade, vous pouvez ajouter deux serveurs RADIUS, un serveur LDAP et un serveur TACACS, ou tous les serveurs peuvent être de type RADIUS. Vous pouvez configurer jusqu'à 32 serveurs d'authentification externes dans Citrix ADM.

## Configuration de serveurs d'authentification externes en cascade

1. Dans Citrix ADM, accédez à **Systeme > Authentification**.
2. Sur la page **Authentification**, cliquez sur **Configuration de l'authentification**.
3. Sur la page **Configuration de l'authentification**, sélectionnez **EXTERNE** dans la liste déroulante **Type de serveur** (seuls les serveurs externes peuvent être mis en cascade).
4. Cliquez sur **Insérer**, puis sur la page **Serveurs externes**, sélectionnez un ou plusieurs serveurs d'authentification que vous souhaitez mettre en cascade.
5. Sélectionnez **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. Cliquez sur **OK** pour fermer la page.

Les serveurs sélectionnés sont affichés sous Serveurs externes, comme indiqué dans la figure ci-dessous.

Vous pouvez également spécifier l'ordre d'authentification en utilisant l'icône à côté des noms des serveurs pour déplacer les serveurs vers le haut ou vers le bas de la liste.

### ← Authentication Configuration

The appliance can authenticate users with local user accounts or by using an external authentication server.

Server Type\*

External Servers

<input type="checkbox"/>	Server Type	Server Name
<input checked="" type="checkbox"/>	RADIUS	RADIUS R1
<input checked="" type="checkbox"/>	RADIUS	RADIUS R2

Enable fallback local authentication  
 Log external group information

## 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 toute première authentification. Citrix Application Delivery Management (ADM) fournit une méthode d'authentification à la fois des utilisateurs locaux et des utilisateurs externes. Alors que les utilisateurs locaux sont authentifiés en interne, Citrix ADM prend en charge l'authentification externe au moyen des protocoles RADIUS, LDAP et TACACS. Lorsqu'un utilisateur tente d'accéder à Citrix ADM configuré pour l'authentification externe, le serveur d'applications demandé envoie le nom d'utilisateur et le mot de passe au serveur RADIUS, LDAP ou TACACS pour l'authentification. Une fois authentifié, le protocole requis est utilisé pour identifier l'utilisateur sur Citrix ADM.

Le contrôle d'accès est le processus d'application de la sécurité requise pour une ressource particulière. Il s'agit d'une technique de sécurité qui peut être utilisée pour réglementer qui peut consulter ou utiliser des ressources dans un environnement informatique. Le but du contrôle d'accès est de limiter les actions ou les opérations qu'un utilisateur légitime d'un système informatique peut effectuer. Le contrôle d'accès limite ce qu'un utilisateur peut faire directement, ainsi que les programmes qui s'exécutent pour le compte de l'utilisateur. Le contrôle d'accès vise ainsi à empêcher les activités susceptibles d'entraîner une violation de la sécurité. Le contrôle d'accès suppose que l'authentification de l'utilisateur a été vérifiée avec succès avant l'application du contrôle d'accès via un moniteur de référence. Citrix ADM permet un contrôle d'accès basé sur les rôles (RBAC), qui permet aux administrateurs de fournir des autorisations d'accès aux utilisateurs en fonction des rôles des utilisateurs individuels au sein d'une entreprise. Le RBAC dans Citrix ADM est réalisé en créant des stratégies d'accès, des rôles, des groupes et des utilisateurs.

## Contrôle d'accès sur rôle

February 1, 2024

Citrix Application Delivery Management (ADM) fournit un contrôle d'accès basé sur les rôles (RBAC) précis 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 attribuée à des utilisateurs ou à des groupes sur la base de conditions spécifiques. Dans Citrix ADM, la création de rôles et de stratégies est spécifique à la fonctionnalité RBAC de Citrix ADC. Les rôles et les stratégies peuvent être facilement créés, modifiés ou supprimés au fur et à mesure que les besoins de l'entreprise évoluent, sans avoir à mettre à jour individuellement les privilèges de chaque utilisateur.

Les rôles peuvent être basés sur des fonctionnalités ou des ressources. Par exemple, pensez à un administrateur SSL/sécurité et à un administrateur d'application. Un administrateur SSL/Security doit disposer d'un accès complet aux fonctionnalités de gestion et de surveillance des certificats SSL, mais doit disposer d'un accès en lecture seule pour les opérations d'administration du système. Un administrateur d'applications doit être en mesure d'accéder uniquement aux ressources relevant de son domaine de compétence.

### **Exemple :**

Chris, le chef de groupe ADC, est le super administrateur de Citrix ADM dans son organisation. Il crée trois rôles d'administrateur : administrateur de sécurité, administrateur d'application et administrateur réseau.

David, l'administrateur de la sécurité, doit avoir un accès complet pour la gestion et la surveillance des certificats SSL, mais doit avoir un accès en lecture seule pour les opérations d'administration du système.

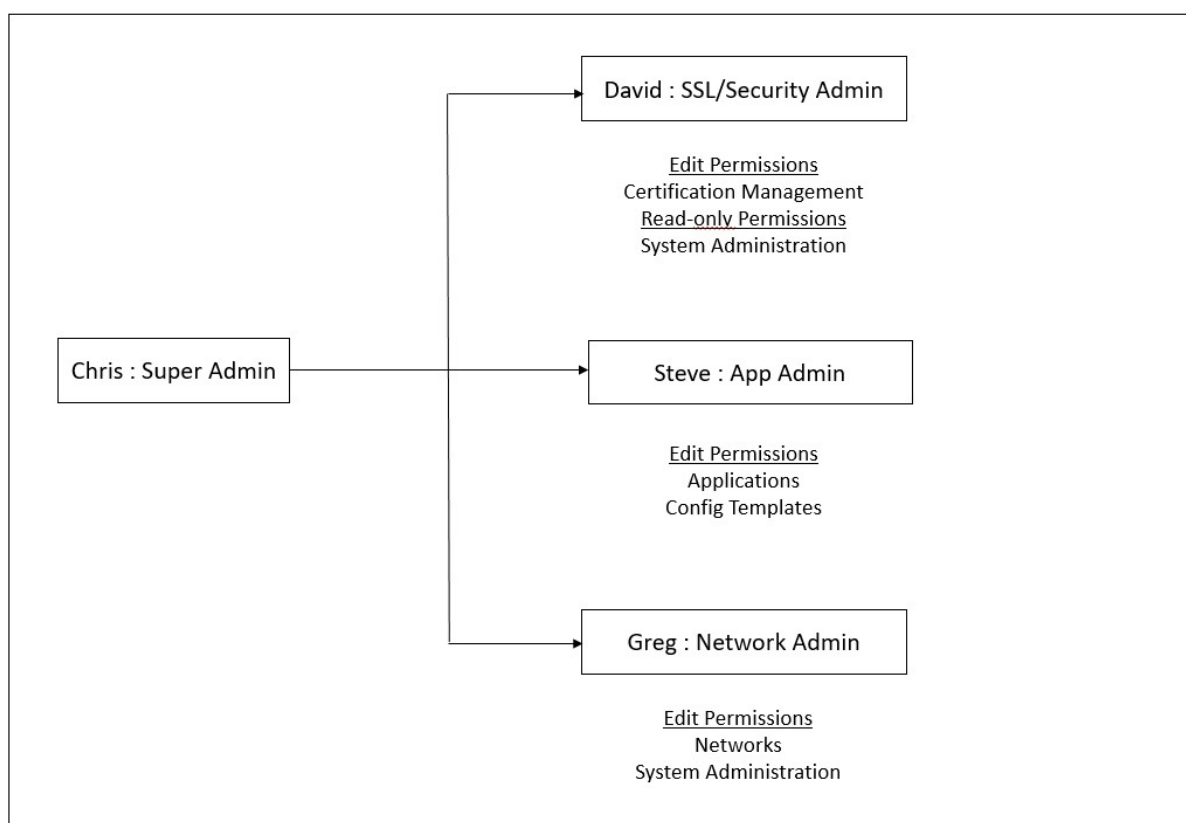
Steve, administrateur d'applications, a besoin d'accéder uniquement à des applications spécifiques et uniquement à des modèles de configuration spécifiques.

Greg, administrateur réseau, a besoin d'un accès à l'administration du système et du réseau.

Chris doit également fournir le RBAC à tous les utilisateurs, qu'ils soient locaux, externes ou multi-locataires.

Les utilisateurs Citrix ADM peuvent être authentifiés localement ou via un serveur externe (RADIUS/L-DAP/TACACS). Les paramètres RBAC doivent être applicables à tous les utilisateurs, quelle que soit la méthode d'authentification adoptée.

L'image suivante montre les autorisations dont disposent les administrateurs et les autres utilisateurs et leurs rôles dans l'organisation.



## Limitations

RBAC n'est pas entièrement pris en charge pour les fonctionnalités Citrix ADM suivantes :

- **Analytics** - RBAC n'est pas entièrement pris en charge dans les modules d'analyse. La prise en charge du RBAC est limitée au niveau de l'instance et ne s'applique pas au niveau de l'application dans les modules d'analyse Web Insight, SSL Insight, Gateway Insight, HDX Insight et Security Insight. Par exemple :

### Exemple 1 : RBAC basé sur une instance (pris en charge)

Un administrateur auquel quelques instances ont été attribuées ne peut voir que ces instances sous **Web Insight > Instances**, et uniquement les serveurs virtuels correspondants sous **Web Insight > Applications**, car le RBAC est pris en charge au niveau de l'instance.

### Exemple 2 : RBAC basé sur l'application (non pris en charge)

Un administrateur auquel quelques applications ont été attribuées peut voir tous les serveurs virtuels sous **Web Insight > Applications**, mais ne peut pas y accéder, car le RBAC n'est pas pris en charge au niveau des applications.

- **StyleBooks** : le RBAC n'est pas entièrement pris en charge pour StyleBooks.

- Dans Citrix ADM, les Stylebooks et les packs de configuration sont considérés comme des ressources distinctes. Des autorisations d'accès, que ce soit pour afficher, modifier ou les deux, peuvent être fournies séparément ou simultanément pour Stylebook et les packs de configuration. Une autorisation d'affichage ou de modification sur les packs de configuration permet implicitement à l'utilisateur d'afficher les StyleBooks, ce qui est essentiel pour obtenir les détails du configpack et créer de nouveaux packs de configuration.
  - L'autorisation d'accès pour Stylebook ou packs de configuration spécifiques n'est pas prise en charge  
Exemple : s'il existe déjà un configpack sur l'instance, les utilisateurs peuvent modifier la configuration sur une instance Citrix ADC cible même s'ils n'ont pas accès à cette instance.
- **Orchestration** - RBAC n'est pas pris en charge pour Orchestration.

## Configurer les stratégies d'accès

February 1, 2024

Les stratégies d'accès définissent les autorisations. Une stratégie peut être appliquée à un seul utilisateur ou groupe, ou à plusieurs utilisateurs et plusieurs groupes. Citrix Application Delivery Management (ADM) fournit quatre stratégies d'accès prédéfinies :

1. **adminpolicy**. Autorise l'accès à toutes les fonctionnalités de Citrix ADM. L'utilisateur dispose d'autorisations d'affichage et de modification, peut afficher tout le contenu Citrix ADM et peut effectuer toutes les opérations de modification. Autrement dit, l'utilisateur peut effectuer des opérations d'ajout, de modification et de suppression sur les ressources.
2. **readonlypolicy**. Octroie des autorisations en lecture seule. L'utilisateur peut afficher tout le contenu sur Citrix ADM, mais n'est autorisé à effectuer aucune opération.
3. **appAdminPolicy**. Octroie des autorisations d'administration pour accéder aux fonctionnalités de l'application dans Citrix ADM. Un utilisateur lié à cette stratégie peut ajouter, modifier et supprimer des applications personnalisées et activer ou désactiver les services, les groupes de services et les différents serveurs virtuels, tels que la commutation de contenu, la redirection de cache et les serveurs virtuels HAProxy.
4. **appReadOnlyPolicy**. Octroie une autorisation en lecture seule pour les fonctionnalités de l'application. Un utilisateur lié à cette stratégie peut afficher les applications, mais ne peut pas effectuer d'opérations d'ajout, de modification, de suppression, d'activation ou de désactivation.

**Remarque** Les stratégies prédéfinies ne peuvent pas être modifiées.

Vous pouvez également créer vos propres stratégies (définies par l'utilisateur).

**Pour créer des stratégies d'accès définies par l'utilisateur :**

1. Dans Citrix ADM, accédez à **Système > Administration des utilisateurs > Stratégies d'accès**.
2. Cliquez sur **Ajouter**.
3. Dans le champ **Nom de la stratégie**, entrez le nom de la stratégie et entrez la description dans le champ **Description de la stratégie**.
4. La section **Autorisations** répertorie toutes les fonctionnalités de Citrix ADM, avec des options permettant de spécifier un accès en lecture seule ou en modification. Cliquez sur l'icône (+) pour développer chaque groupe d'entités en plusieurs entités. Vous devez cocher la case à côté du nom de la fonctionnalité pour accorder aux utilisateurs les autorisations d'affichage ou de modification. L'option Modifier inclut l'autorisation d'affichage. Sélectionnez **Afficher** pour la lecture seule ou **Modifier** pour un accès complet.

**Remarque** Développez Load Balancing et GSLB pour afficher davantage d'options de configuration.

Permissions

All Toggle all "View" selection

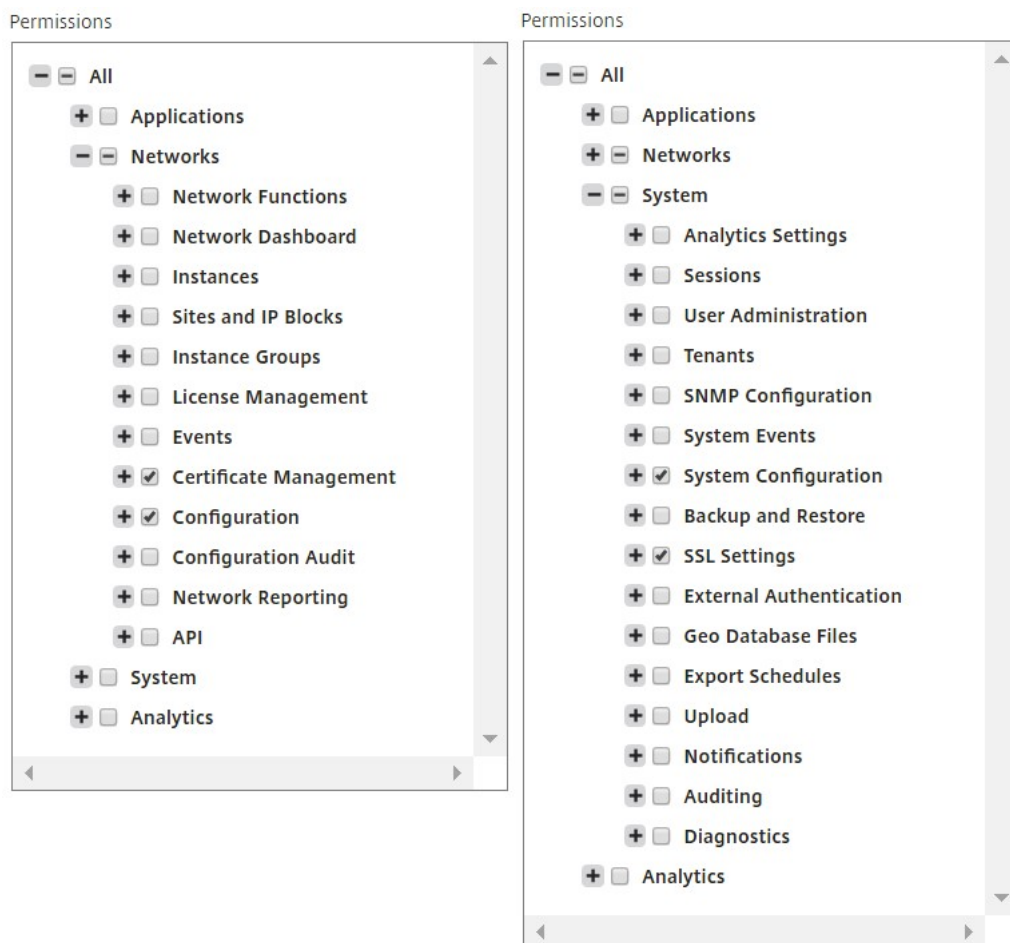
- Applications
- Networks
  - Instance Groups
  - Certificate Management
  - Domain Names
  - Instances Dashboard
  - Events
  - Instances
  - API
  - Sites and IP Blocks
  - Network Reporting
  - Configuration
  - Configuration Audit
  - Agents
  - Autoscale Groups
  - License Management
  - Network Functions
    - GSLB
      - Virtual Server
        - View  Edit
      - Services
      - Domains
    - Auditing
    - Authentication
    - Load Balancing
      - Services
      - Virtual Servers
        - Edit  View
      - Service Groups
      - Servers
    - Cache Redirection
    - HAProxy
    - Content Switching
    - Citrix Gateway
    - Settings
  - Analytics
  - Orchestration
  - System

**Remarque** La sélection de **Modifier** peut affecter en interne des autorisations dépendantes qui ne sont pas affichées comme étant activées dans la section **Autorisations** . Par exemple, lorsque vous activez les autorisations de modification pour la gestion des erreurs, Citrix ADM fournit en interne l'autorisation de configurer un profil de messagerie ou de créer des configurations de serveur SMTP, afin que l'utilisateur puisse envoyer le rapport sous la forme d'un courrier électronique.

**Exemple :**

David est l'administrateur chargé de la gestion et de la sécurité des certificats SSL dans Citrix ADM. Dans la stratégie attribuée à David, l'administrateur coche les cases suivantes dans la section **Autorisations** :

- **Réseaux > Configuration > Modifier**
- **Réseaux > Gestion des certificats > Modifier**
- **Système > Paramètres SSL > Modifier**
- **Système > Configuration du système > Modifier**





5. Cliquez sur **Créer**.

## Configurer les groupes

February 1, 2024


Dans Citrix Application Delivery Management (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 Citrix ADC ; un autre groupe peut n'avoir accès qu'à 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 Citrix ADM.


**Pour créer des groupes d'utilisateurs et attribuer des rôles aux groupes d'utilisateurs, procédez comme suit :**


1. Dans Citrix ADM, accédez à **Système > Administration des utilisateurs > Groupes**.
2. Cliquez sur **Ajouter**.
3. Dans le champ **Nom du groupe**, entrez le nom du groupe.
4. Dans le champ **Description du groupe**, saisissez une description de votre groupe. Fournir une bonne description du groupe vous aide à mieux comprendre le rôle et la fonction du groupe ultérieurement.
5. Dans la section **Rôles**, ajoutez ou déplacez un ou plusieurs rôles dans la liste **Configuré**.

**Remarque** Dans la liste **Disponible**, vous pouvez cliquer sur **Nouveau** ou **Modifier** et créer ou modifier des rôles. Vous pouvez également accéder à **Système > Administration des utilisateurs > Utilisateurs** et créer ou modifier des utilisateurs.

## ← Create System Group

 **Group Settings**

 Authorization Settings

 Assign Users

Group Name\*  
 ?

Group Description  
 ?

Roles\*

**Available (3)**  Select All

appReadOnly	+
appAdmin	+
readonly	+

New | Edit

**Configured (1)**  Remove All

admin	-
-------	---

Configure User Session Timeout

### Remarque

Vous pouvez créer un nouveau rôle en cliquant sur **Nouveau**, ou vous pouvez accéder à **Système > Administration des utilisateurs > Utilisateurs** et créer de nouveaux utilisateurs à partir de cet écran.

6. Cliquez sur **Suivant**. Dans l'onglet **Paramètres d'autorisation**, vous pouvez fournir des paramètres d'autorisation pour les quatre groupes suivants :

- Instances
- Applications
- Modèles de configuration
- StyleBooks

Par défaut, votre utilisateur peut accéder à tous les groupes ci-dessus. Vous pouvez désactiver les cases à cocher et fournir un accès sélectif à chacun de ces groupes.

Par exemple :

- Vous pouvez **décocher** la case Instances et sélectionner uniquement les instances requises auxquelles vous souhaitez donner accès à vos utilisateurs.
- Désactivez la case à cocher **Toutes les applications** et sélectionnez uniquement les applications et les modèles requis. Lorsque vous ajoutez des applications à un groupe dans Citrix ADM, vous pouvez utiliser une expression régulière pour rechercher et ajouter les applications qui répondent aux critères d'expression régulière pour les groupes. Les utilisateurs liés à ces groupes ne peuvent accéder qu'à ces applications spécifiques. L'expression regex spécifiée est conservée dans Citrix ADM. C'est-à-dire que Citrix ADM autorise le stockage de l'expression régulière fournie dans la zone de texte **Ajouter une expression régulière** dans le système et met à jour dynamiquement la portée d'autorisation chaque fois que de nouvelles applications répondent à cette expression régulière. Lorsque de nouvelles applications sont ajoutées au système, Citrix ADM applique les critères de recherche aux nouvelles applications, et l'application qui répond aux critères est ajoutée dynamiquement au groupe. Il n'est pas nécessaire d'ajouter manuellement les nouvelles applications au groupe. Les applications sont mises à jour dynamiquement dans le système, et les utilisateurs du groupe concerné peuvent voir les applications sous les modules appropriés dans Citrix ADM.
- Décochez la case **Tous les modèles de configuration** pour autoriser l'accès uniquement aux modèles requis.
- Décochez la case **Tous les StyleBooks** et sélectionnez les StyleBooks requis auxquels votre utilisateur peut accéder.

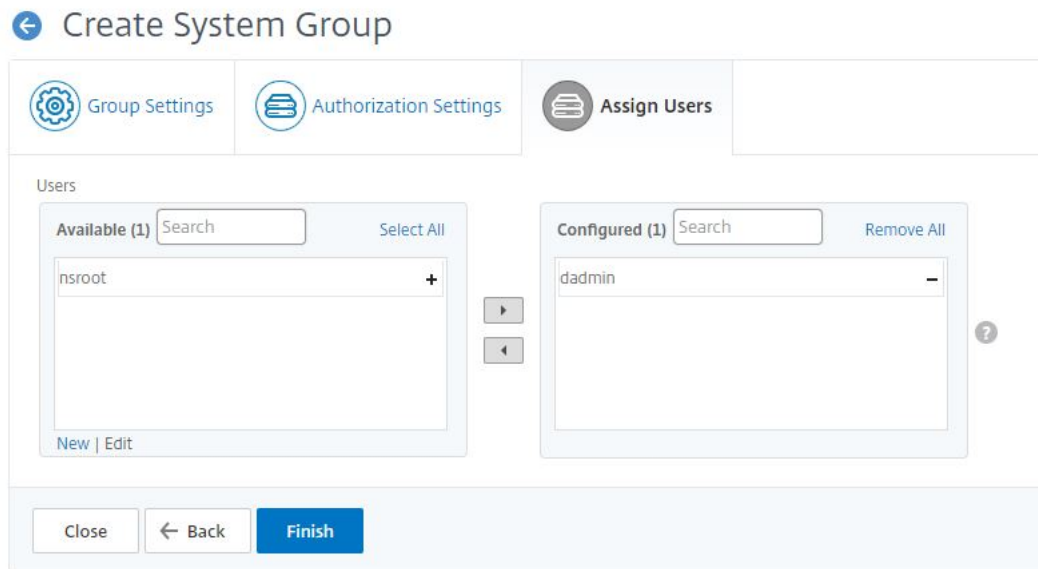
Vous pouvez sélectionner les StyleBooks requis lorsque vous créez des groupes et ajoutez des utilisateurs à ce groupe. Lorsque votre utilisateur sélectionne le StyleBook autorisé, tous les StyleBooks dépendants sont également sélectionnés. Les packs de configuration de ce StyleBook sont également inclus dans ce que l'utilisateur a accès.

← Create System Group

	Name	Namespace	Version
<input checked="" type="checkbox"/>	microsoft-sharepoint-2016	com.citrix.adc.enterprise.stylebooks	1.2
<input checked="" type="checkbox"/>	microsoft-office365-sso	com.citrix.adc.enterprise.stylebooks	1.0
<input checked="" type="checkbox"/>	microsoft-exchange-2016	com.citrix.adc.enterprise.stylebooks	1.2
<input checked="" type="checkbox"/>	microsoft-adfsproxy	com.citrix.adc.enterprise.stylebooks	1.0

- Décochez la case **Tous les noms de domaine DNS** et ajoutez les noms de domaine de la liste auxquels vous souhaitez que vos utilisateurs accèdent.

7. Cliquez sur **Créer un groupe**.
8. Dans l'onglet **Attribuer des utilisateurs**, sélectionnez l'utilisateur dans la liste **Disponible** et ajoutez-le à la liste **Configuré**. Par exemple, « dadmin ».



**Remarque** Vous pouvez également ajouter de nouveaux utilisateurs en cliquant sur **Nouveau**.

9. Cliquez sur **Terminer**.

#### Remarque

En tant qu'administrateur Citrix ADM, vous pouvez accorder à vos utilisateurs une autorisation « en lecture seule » ou une autorisation « affichage et modification » pour les interfaces utilisateur individuelles des modules ADM en fonction des paramètres de stratégie d'accès du RBAC. Si l'utilisateur est affecté à deux groupes ou plus, c'est-à-dire s'il est mappé en interne à plusieurs zones d'autorisation et à plusieurs stratégies d'accès, ADM réunit les autorisations de tous ces groupes et autorise l'utilisateur en conséquence.

Par exemple, considérez que l'utilisateur1 est affecté à un groupe doté de deux stratégies d'accès, P1 et P2. Chaque stratégie comporte un type d'autorisation différent. P1 dispose de l'autorisation « lecture seule », tandis que P2 dispose de l'autorisation « afficher et modifier ». Vous souhaitez que votre utilisateur visualise un ensemble d'applications dans le cadre de la stratégie P1 et modifie un autre ensemble d'applications dans le cadre de la stratégie P2. Mais par défaut, Citrix ADM combine les deux types d'autorisation et attribue l'autorisation « Afficher et modifier » à l'utilisateur. Ainsi, votre utilisateur pourra désormais consulter et modifier toutes les applications.

ADM ne prend pas en charge les cas d'utilisation dans lesquels vous pouvez attribuer différents types d'autorisations au même utilisateur. Vous ne pouvez attribuer qu'un seul type d'autorisation à vos utilisateurs. ADM peut soit autoriser l'utilisateur1 à afficher toutes les applications ou un ensemble d'applications sélectionné, soit autoriser l'utilisateur1 à afficher et à modifier toutes les applications ou l'ensemble d'applications sélectionné.

## Cartographie du RBAC lors de la mise à niveau de Citrix ADM de la version 12.0 à la version 12.1

Lorsque vous mettez à niveau Citrix ADM de la version 12.0 à la version 12.1, les options permettant de fournir des autorisations de « lecture-écriture » ou de « lecture » lors de la création de groupes ne s'affichent pas. Ces autorisations ont été remplacées par « rôles et stratégies d'accès », ce qui vous donne plus de flexibilité pour fournir des autorisations basées sur les rôles aux utilisateurs. Le tableau suivant montre comment les autorisations de la version 12.0 sont mappées à celles de la version 12.1 :

12.0	Autoriser les applications uniquement	12.1
admin read-write	False	administrateur
admin read-write	True	appAdmin
admin read-only	False	readonly
admin read-only	True	appReadOnly

## Configurer les rôles

February 1, 2024

Dans Citrix Application Delivery Management (ADM), chaque rôle est lié à une ou plusieurs stratégies d'accès. Vous pouvez définir des relations un-à-un, un-à-plusieurs et plusieurs vers plusieurs entre les stratégies et les rôles. Vous pouvez lier un rôle à plusieurs stratégies, et vous pouvez lier plusieurs rôles à une seule stratégie.

Par exemple, un rôle peut être lié à deux stratégies, l'une définissant les autorisations d'accès pour une entité et l'autre définissant les autorisations d'accès pour une autre entité. Une stratégie peut autoriser l'ajout d'instances Citrix ADC dans Citrix ADM, tandis que l'autre stratégie peut autoriser la création et le déploiement de StyleBooks et la configuration d'instances Citrix ADC.

Lorsque plusieurs stratégies définissent des autorisations de mise à jour et de lecture seule pour une seule entité, les autorisations de mise à jour ont la priorité.

Citrix ADM fournit quatre rôles prédéfinis :

- **admin**. A accès à toutes les fonctionnalités Citrix ADM. (Ce rôle est lié à adminpolicy.)
- **readonly**. Accès en lecture seule. (Ce rôle est lié à la stratégie de lecture uniquement.)
- **appAdmin**. Accès administratif uniquement aux fonctionnalités de l'application dans Citrix ADM. (Ce rôle est lié à appAdminPolicy).
- **appReadOnly**. Dispose d'un accès en lecture seule aux fonctionnalités de l'application. (Ce rôle est lié à appReadOnlyPolicy.)

**Remarque** Les rôles prédéfinis ne peuvent pas être modifiés.

Vous pouvez également créer vos propres rôles (définis par l'utilisateur).

**Pour créer des rôles et leur attribuer des stratégies :**

1. **Dans Citrix ADM, accédez à** Système>Administration des utilisateurs > Rôles.
2. Cliquez sur **Ajouter**.
3. Dans le champ **Nom du rôle**, entrez le nom du rôle et fournissez la description dans le champ **Description du rôle** (facultatif).
4. Dans la section **Stratégies**, ajoutez ou déplacez une ou plusieurs stratégies vers la liste **configurée**.

## ← Create Roles

Role Name\*  
example-external-auth-role ?

Role Description  
External TACACS Authentication ?

Policies\*

Available (3) Search Select All

appAdminPolicy	+
readonlypolicy	+
appReadOnlyPolicy	+

New | Edit

Configured (1) Search Remove All

adminpolicy	-
-------------	---

Create Close

5. Cliquez sur **Créer**.

## Configurer les utilisateurs

February 1, 2024

Par défaut, Citrix Application Delivery Management (ADM) possède un utilisateur :

nsroot : l'utilisateur root (nsroot) dispose de privilèges d'administration complets sur l'apppliance. L'utilisateur nsroot est le super administrateur de Citrix ADM.

Vous pouvez créer des utilisateurs supplémentaires en configurant des comptes pour eux. Lorsque vous ajoutez de nouveaux utilisateurs à Citrix ADM, vous pouvez définir leurs autorisations en attribuant les groupes, les rôles et les stratégies appropriés.

Vous pouvez affecter un utilisateur à un groupe et lier le groupe à des rôles. Vous pouvez définir des relations un-à-un, un-à-plusieurs ou plusieurs à plusieurs entre les utilisateurs, les groupes, les rôles et les stratégies d'accès. Un utilisateur peut être affecté à plusieurs groupes. Un groupe peut avoir plusieurs rôles et plusieurs groupes peuvent avoir des rôles identiques.

**Pour configurer des utilisateurs dans Citrix ADM :**

1. Dans Citrix ADM, accédez à **Système > Administration des utilisateurs > Utilisateurs**.
2. Cliquez sur **Ajouter**.
3. Entrez les informations suivantes :
  - a) **Nom d'utilisateur**. Nom de l'utilisateur
  - b) **Mot de passe**. Mot de passe avec lequel l'utilisateur se connecte à Citrix ADM
4. Vous pouvez également sélectionner **Activer l'authentification externe** afin que l'utilisateur puisse être authentifié via un serveur d'authentification externe.
5. Si vous avez créé des groupes et souhaitez affecter l'utilisateur à un groupe, dans la section **Groupes**, déplacez un ou plusieurs groupes de la liste **Disponible** vers la liste **configurée**.

← Create System User

User Name\*  
dadmin ?

Password\*  
.... ?

Confirm Password\*  
.... ?

Enable External Authentication ?  
 Configure User Session Timeout ?

Groups\*

Available (3)	Select All
NSMASUser1	+
read_only	+
owner	+

▶

Configured (1)	Remove All
NSMASUser11	-

?

Create Close

6. Cliquez sur **Créer**.



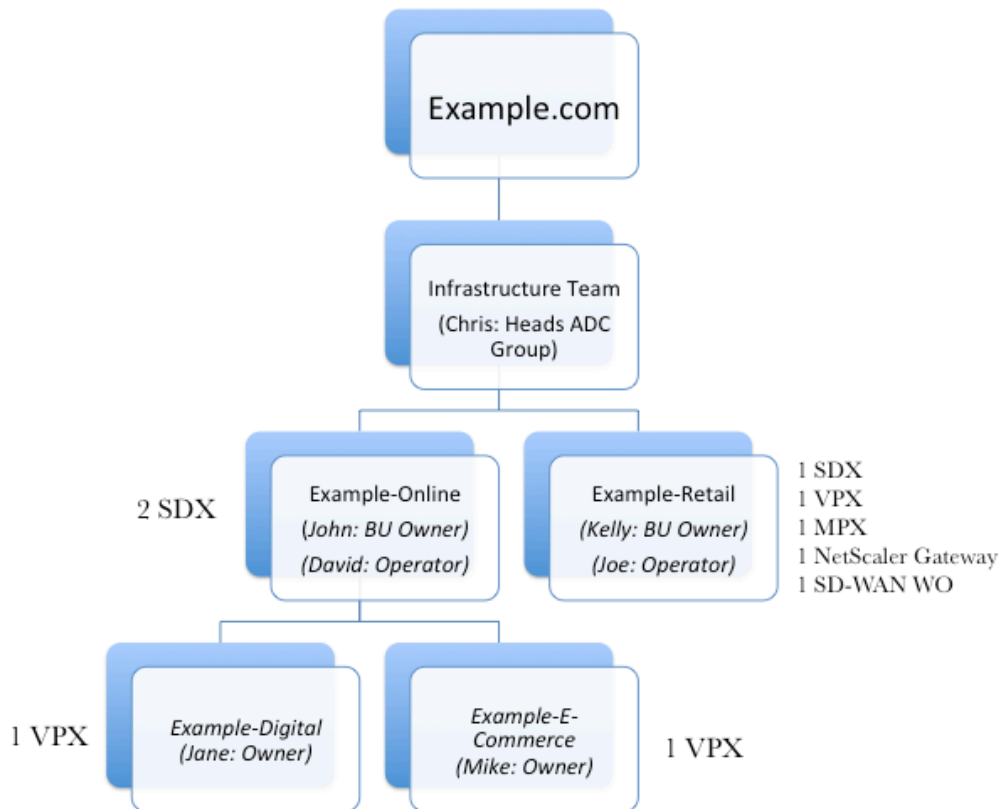
## **Multilocation : offrez un environnement de gestion exclusif à vos locataires**

February 1, 2024

Citrix Application Delivery Management (ADM) fournit une fonctionnalité multi-tenant qui vous permet de configurer le système pour plusieurs locataires. Chaque locataire peut ajouter ses instances réseau, gérer et surveiller ces instances et applications, et créer ses propres utilisateurs et groupes. Aucun locataire n'a de visibilité sur les instances et les applications des autres locataires. Seul l'administrateur système a une visibilité sur toutes les instances, applications et rapports de tous les locataires. Toutefois, l'administrateur système ne peut pas créer d'utilisateurs pour les locataires. Toutes les tâches au niveau du système ne peuvent être effectuées que par l'administrateur système.

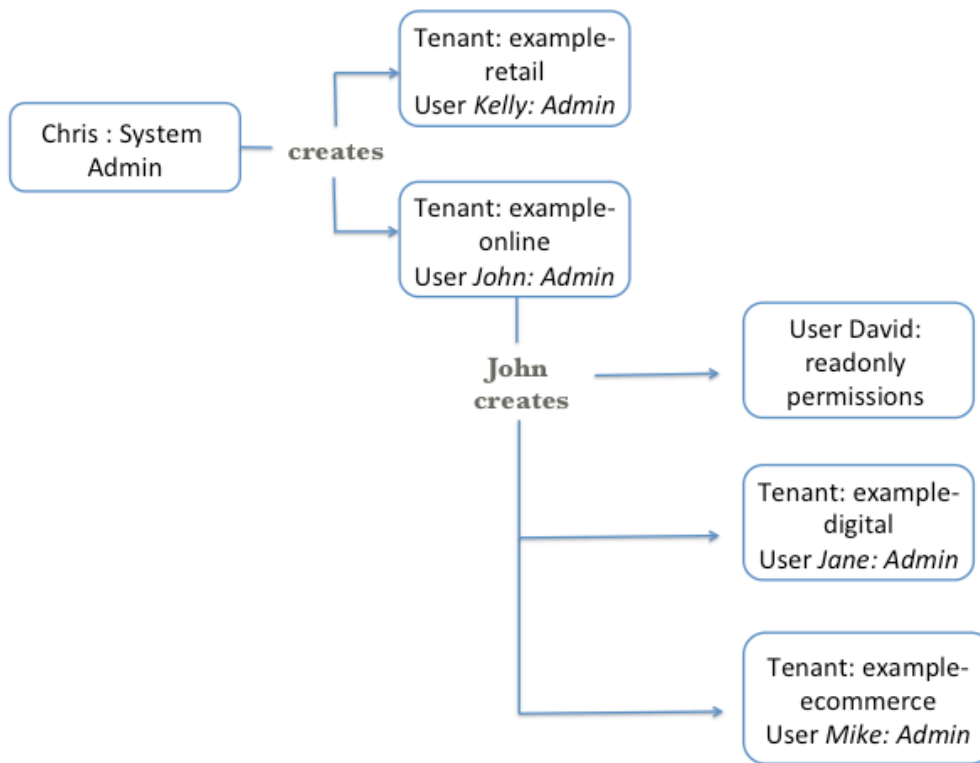
Imaginons un scénario dans lequel une organisation telle que `exemple.com` possède un groupe d'infrastructure et plusieurs unités commerciales au sein de celui-ci. Ils souhaitent gérer de manière centralisée toutes les instances de leur réseau. Cependant, ils souhaitent offrir un environnement exclusif à chaque unité commerciale.

L'image suivante montre comment le groupe d'infrastructure d'organisation `exemple.com` est structuré. Ils souhaitent que chacune des quatre unités commerciales dispose d'environnements de gestion exclusifs. Cette image montre également le nombre d'instances que chaque unité commerciale souhaite gérer.



Chris, le chef de groupe ADC, est l'administrateur système de Citrix ADM. Chris crée deux locataires pour les deux unités commerciales, Example-Online et Example-Retail, et attribue deux utilisateurs en tant qu'administrateurs de ces locataires. Chaque administrateur de locataires peut désormais ajouter d'autres utilisateurs, ajouter des instances qu'il souhaite gérer et créer des sous-locataires dans son environnement de locataire.

L'image suivante montre les locataires et les utilisateurs créés dans Citrix ADM pour cet exemple.



## Ajouter des locataires

Dans cet exemple, Chris, l'administrateur système crée deux locataires : exemple-online et exemple-retail. Lors de la création des locataires, Chris crée également un utilisateur administrateur par défaut pour chaque locataire.

### Pour ajouter des locataires

1. Accédez à **Système > Locataires**, puis cliquez sur **Ajouter**.
2. Sur la page **Créer un locataire**, spécifiez le nom du locataire et le nom d'utilisateur du locataire que vous souhaitez attribuer en tant qu'administrateur à ce locataire. Indiquez également le mot de passe.
3. Cliquez sur **Créer**.

## ← Create Tenant

Tenant Name\*  
 ?

**Tenant User**

Tenant User Name\*  
 ?

Password\*  
 ?

Confirm Password\*  
 ?

▶ Additional Information

Sur la page **Locataires**, vous pouvez afficher la liste des locataires créés.

### Tenants

<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <span style="float: right;">Search ▾</span>	
<input type="checkbox"/>	Name
<input type="checkbox"/>	example-online
<input type="checkbox"/>	example-retail

Vous pouvez également afficher la liste des utilisateurs admin pour chaque locataire sur la page **Système > Administration des utilisateurs > Utilisateurs**.

## Users

<input type="checkbox"/>	User Name	Admin Domain Name
<input type="checkbox"/>	John	example-online
<input type="checkbox"/>	Kelly	example-retail
<input type="checkbox"/>	nsroot	Owner

Lorsque vous créez un locataire, trois groupes système par défaut sont créés : groupe admin, AdminExceptSystem\_Group et groupe en lecture seule.

Exemple :

Le locataire example-online possède les groupes par défaut suivants :

- example-online\_admin\_group
- example-online\_adminExceptSystem\_group
- example-online\_readonly\_group

<input type="checkbox"/>	Group Name	Group Description	Tenant
<input type="checkbox"/>	example-online_admin_group		example-online
<input type="checkbox"/>	example-online_adminExceptSystem_group		example-online
<input type="checkbox"/>	example-online_readonly_group		example-online

### Connectez-vous à Citrix ADM en tant qu'utilisateur locataire

Une fois les locataires créés, un utilisateur locataire peut se connecter à Citrix ADM à l'aide des informations d'identification de l'utilisateur locataire. Pour ce faire, un locataire doit fournir à la fois le nom de domaine et le nom d'utilisateur, par exemple, exemple-online \ John.

A login form with a dark grey background. It contains two input fields: 'User Name' with the text 'example-online\John' and 'Password' with six asterisks. Below the fields is a large blue button labeled 'Log On'.

### Ajouter des instances en tant qu'utilisateur locataire

Une fois qu'un client ouvre une session, Citrix ADM lui demande d'ajouter des instances. Cliquez sur **+ Nouveau** pour ajouter les instances que vous souhaitez gérer. Vous pouvez également cliquer sur Faire plus tard et ajouter les instances ultérieurement à partir de l'onglet Infrastructure. Pour plus d'informations, voir *Ajout d'une instance à Citrix ADM*.

A screenshot of the 'Add New Instances' dialog box. It shows a header with a hamburger menu icon and the text 'Add New Instances'. Below is a section titled 'Instances | 0' with a '+ New' button. A subtitle reads: 'The instances in your network that you want to manage, monitor, and get real-time visibility into.' The main area contains the text 'No instances found.' At the bottom, there are three buttons: 'Back', 'Finish', and 'Do it Later'.

Dans cet exemple, John ajoute deux instances Citrix ADC SDX.

Spécifiez le type d'instance, les adresses IP (séparées par des virgules) et le nom de profil que Citrix ADM peut utiliser pour accéder aux instances, puis cliquez sur **OK**.

A screenshot of the 'Add Instance' dialog box. It has a title bar with 'Add Instance' and a close button. The form contains:
 

- 'Instance Type\*' dropdown menu with 'Citrix ADC SDX' selected.
- Instruction: 'Enter one or more hostnames, IP addresses, and/or a range of IP addresses (for example, 10.102.40.30-10.102.40.45) using a comma separator.'
- 'IP Address\*' input field with the text '10.102.126.247,10.102.126.251'.
- 'Profile Name\*' dropdown menu with 'nssdx\_default\_profile' selected, followed by '+' and edit icons.

 At the bottom are 'OK' and 'Close' buttons.

## Créer un utilisateur

John, l'administrateur du locataire, souhaite maintenant créer un utilisateur pour David afin que David puisse surveiller toutes les instances et applications de ce locataire. Cependant, Chris ne souhaite pas que David effectue une tâche de configuration sur les instances ou modifie les paramètres système du locataire. Ainsi, Chris crée un utilisateur david avec des autorisations en lecture seule.

### Pour créer un utilisateur :

1. Accédez à **Système > Administration des utilisateurs > Utilisateurs**, puis cliquez sur **Ajouter**.
2. Dans la page **Créer un utilisateur système**, spécifiez le nom d'utilisateur et le mot de passe de l'utilisateur que vous souhaitez créer.
3. Sous **Groupes**, sélectionnez le groupe que vous souhaitez affecter à cet utilisateur. Dans cet exemple, `example-online_readonly_group` est affecté à l'utilisateur david.

### ← Create System User

User Name\*  
david ?

Password\*  
..... ?

Confirm Password\*  
..... ?

Enable External Authentication  
 Configure User Session Timeout

Groups\*

Available (4)	Select All
NSMASUser11	+
NSMASUser1	+
read_only	+
owner	+

Configured (1)	Remove All
example-online_readonly_group	-

▶ ◀ ?

Create Close

## Créer des locataires au sein des locataires

Un administrateur de locataires peut créer des sous-locataires s'il souhaite partitionner davantage son locataire. Cependant, il ne peut créer qu'un seul niveau de sous-locataires. Dans cet exemple, John crée deux sous-locataires, `exemple-digital` et `exemple-ecommerce`. Lors de la création de ces deux sous-locataires, Chris désigne Jane et Mike en tant qu'utilisateur administrateur respectivement.

Pour créer un locataire au sein d'un locataire, suivez les étapes décrites dans la section [Ajouter des locataires](#).

Vous pouvez afficher les locataires créés sur la page **Locataires**.



Tenants			
<input type="button" value="Add"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="text" value="Search"/>
<input type="checkbox"/>	Name		
<input type="checkbox"/>	exemple-digital		
<input type="checkbox"/>	exemple-ecommerce		

Vous pouvez également afficher les autorisations attribuées aux utilisateurs. Accédez à **Système > Administration des utilisateurs > Utilisateurs**, sélectionnez un utilisateur, puis cliquez sur **Modifier**.

Sur la page **Configurer l'utilisateur du système**, sous **Groupes**, vous pouvez consulter les groupes attribués à cet utilisateur. Dans cet exemple, vous pouvez voir que `exemple-digital_admin_group` est affecté à Jane.



## ← Configure System User

User Name

Change Password  
 Enable External Authentication  
 Configure User Session Timeout

Groups\*

**Available (5)** Select All

NSMASUser11	+
NSMASUser1	+
read_only	+
owner	+
example-online_readonly_group	+

**Configured (1)** Remove All

example-digital_admin_group	-
-----------------------------	---

En tant qu'administrateur locataire, si vous avez déjà ajouté des instances à Citrix ADM, vous pouvez attribuer les instances aux utilisateurs de votre locataire ou de vos sous-locataires à des fins de gestion et de surveillance. Par exemple, John peut affecter une instance VPX à Jane à des fins de gestion.

1. Accédez à **Système > Administration des utilisateurs > Groupe**.
2. Sélectionnez le groupe auquel l'utilisateur est affecté et cliquez sur **Modifier**.

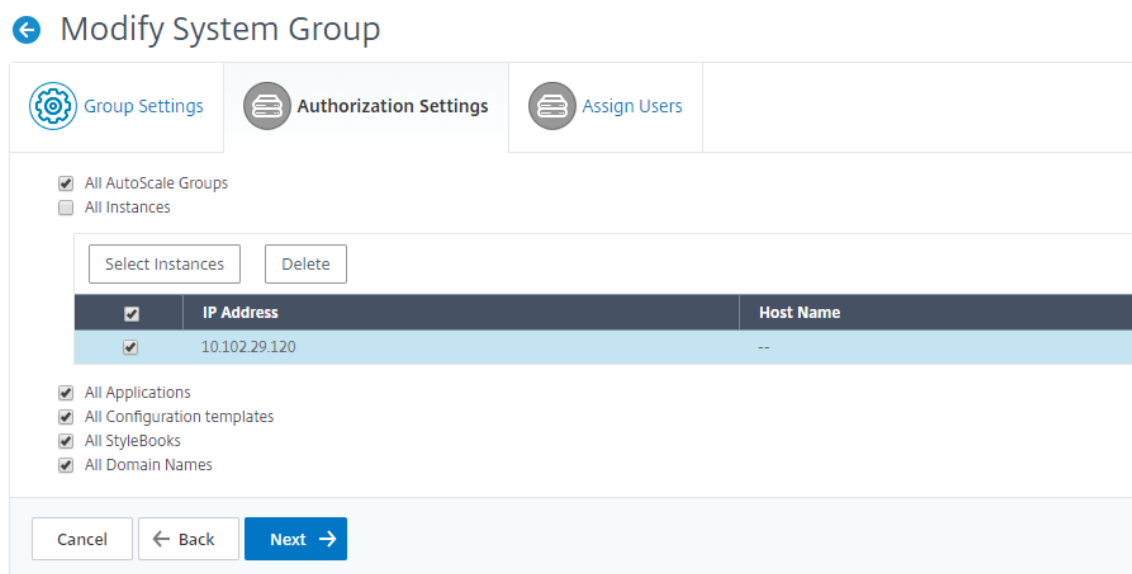
Groups 🔄 ↗

⚙️

🔍 Click here to search or you can enter Key : Value format ?

	Group Name	Group Description	Tenant
<input checked="" type="checkbox"/>	example-digital_admin_group	admin	Owner
<input type="checkbox"/>	example-online_readonly_group		Owner
<input type="checkbox"/>	NSMASUser1	Admin	Owner
<input type="checkbox"/>	NSMASUser11		Owner
<input type="checkbox"/>	owner		Owner
<input type="checkbox"/>	read_only		Owner

3. Dans la page **Modifier le groupe système**, sous l'onglet **Paramètres d'autorisation**, désactivez la case à cocher **Toutes les instances**.



4. Sélectionnez les instances que l'utilisateur doit gérer, puis cliquez sur **Sélectionner les instances**.
5. Cliquez sur **Suivant**, puis cliquez sur **Terminer**.

## Applications

February 1, 2024

La fonctionnalité d'analyse et de gestion des applications de Citrix ADM renforce l'approche centrée sur les applications afin de vous aider à relever divers défis de mise à disposition d'applications. Cette approche vous donne une visibilité sur le score de santé des applications, vous aide à déterminer les risques de sécurité, à détecter les anomalies dans les flux de trafic des applications et à prendre des mesures correctives.

L'illustration suivante donne un aperçu des différentes tâches que vous pouvez effectuer pour la gestion et l'analyse des applications :

Les applications peuvent être des applications découvertes, des applications HAProxy ou des applications personnalisées.

### Applications découvertes

Applications créées automatiquement pour chaque serveur virtuel géré. Les applications découvertes disposeront toujours d'un serveur virtuel et ces applications ne peuvent pas être modifiées ou supprimées directement.

## Applications personnalisées

Applications créées par les utilisateurs à partir d'applications découvertes. Citrix ADM vous permet d'ajouter, de modifier et de supprimer ces applications. Les applications personnalisées sont créées par :

- Un ou plusieurs serveurs virtuels
- Un ou plusieurs frontends HAProxy.

Lorsque vous créez une application personnalisée, toutes les applications découvertes ajoutées à l'application personnalisée sont supprimées du tableau de bord de l'application.

### Points à noter

- Vous ne pouvez pas ajouter une application découverte parmi plusieurs applications personnalisées.
- Vous ne pouvez pas créer d'application personnalisée si toutes les applications découvertes sont déjà attribuées à une autre application personnalisée. Vous devez supprimer une application personnalisée existante pour libérer les applications découvertes afin de pouvoir en reconstituer de nouvelles.
- Vous ne pouvez pas créer d'application personnalisée contenant des serveurs virtuels et des interfaces HAProxy.

## Applications HAProxy

Les applications discrètes HAProxy sont créées automatiquement pour chaque interface HAProxy gérée. Vous pouvez également regrouper ces applications pour former des applications personnalisées similaires aux applications Citrix ADC. Pour plus d'informations, consultez [Gestion et surveillance des instances HAProxy avec Citrix ADM](#).

### Points à noter

Les fonctionnalités ou mesures suivantes du tableau de bord des applications ne sont pas prises en charge pour les applications HAProxy :

- Enquêteur d'activité de l'application
- Score de l'application
- Indice des menaces

- Tendence d'utilisation maximale
- Débit
- Connexions au serveur
- Transactions

## Création d'une application personnalisée

Vous pouvez créer des applications personnalisées en ajoutant une ou plusieurs applications découvertes lors de la définition d'une application.

### Pour créer une application personnalisée :

1. Accédez à **Applications > Tableau de bord**, puis cliquez sur **Définir une application personnalisée**.
2. Sur l'écran de définition de l'application, définissez les paramètres suivants :

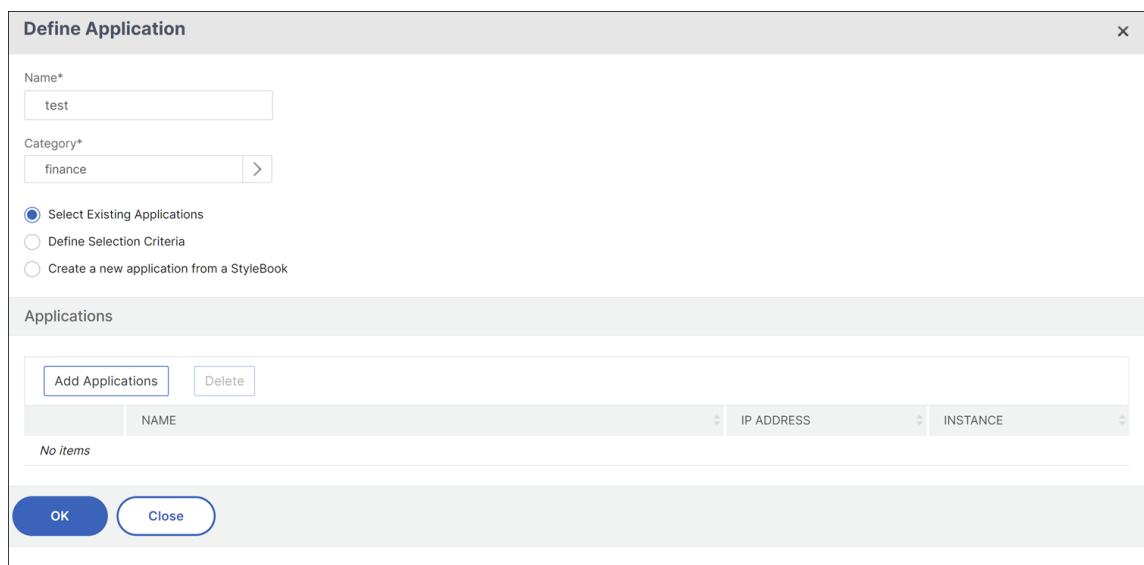
Champ	Description
Nom	Nom de l'application personnalisée
Catégorie	Nom de la catégorie pour laquelle toutes les applications liées à cette catégorie seront regroupées sur le tableau de bord des applications.
Sélectionner des applications existantes	Option permettant d'ajouter des serveurs virtuels si les critères de définition sont basés sur les serveurs virtuels sous licence surveillés par Citrix ADM.
Définir les critères de sélection	Option permettant de définir l'application par plage de serveurs virtuels ou par plage d'adresses IP de serveur/service d'origine. <ul style="list-style-type: none"> <li>• <b>Serveur.</b> Vous spécifiez l'adresse IP du serveur ou du service, le nom du serveur ou le port du serveur principal sur lequel les applications s'exécutent. Vous pouvez entrer une adresse IP, une plage d'adresses IP ou une combinaison des deux séparées par des virgules. Par exemple, vous pouvez entrer 10.102.29.20, 10.102.43.10-60, 10.216.43.45.</li> </ul>

Champ	Description
	<ul style="list-style-type: none"> <li>• <b>Serveurs virtuels.</b> Vous pouvez spécifier l'une des options suivantes : l'adresse IP du serveur virtuel, le nom du serveur virtuel ou le port du serveur principal sur lequel les applications s'exécutent. Vous pouvez entrer une adresse IP ou une plage d'adresses IP ou une combinaison des deux séparées par des virgules. Par exemple, vous pouvez entrer 10.102.29.20, 10.102.43.10-60, 10.216.43.45.</li> </ul>

3. Cliquez sur OK.

**Remarque**

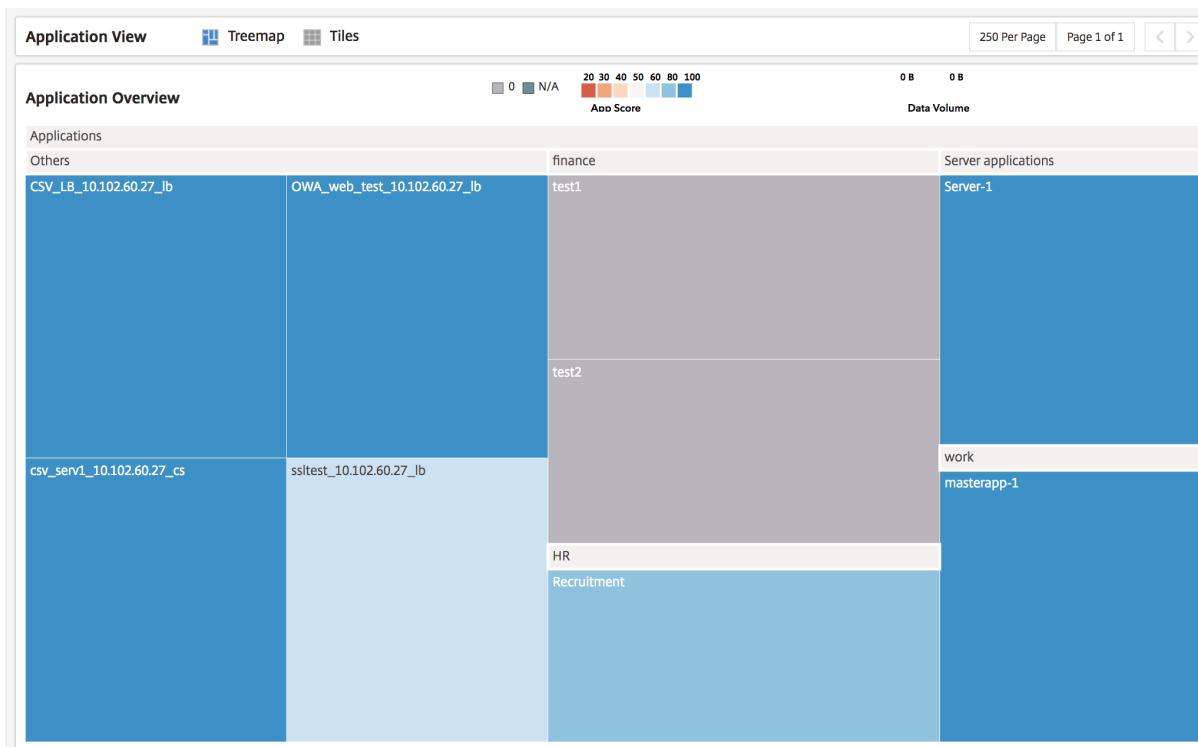
Actuellement, Application Dashboard prend uniquement en charge l'équilibrage de charge et le changement de contenu des serveurs virtuels.



**Regrouper vos applications**

Le regroupement de vos applications vous permet de les gérer et de les surveiller facilement. Vous pouvez regrouper vos applications en sélectionnant ou en créant une catégorie lors de la définition d'une application. Pour créer ou sélectionner la catégorie, lors de la définition de l'application, cliquez sur le bouton à côté du champ Catégorie.

Les applications qui ne sont ajoutées à aucune catégorie sont affichées dans la catégorie **Autres** .



## Tableau de bord de l’application

Le tableau de bord des applications fournit une vue globale de toutes les applications surveillées par Citrix ADM et fournit des informations clés relatives à toutes les applications. Par exemple, le tableau de bord affiche les mesures de performance et de sécurité, les compteurs et l’état de santé des applications. Pour afficher les informations relatives à une application particulière, sélectionnez l’application. Et dans le panneau Résumé, des graphiques à barres présentent des indicateurs tels que le score des applications et les indices de menace, pour toutes les applications surveillées.

## Afficher vos applications

Le tableau de bord des applications affiche les applications sous forme de nœuds sur une arborescence, dont la taille est fonction du volume de données de l’application. La couleur d’une vignette indique le score de l’application, le rouge indiquant une santé minimale et le bleu une bonne santé.

Vous pouvez basculer l’affichage du tableau de bord de votre application en arborescence ou en vignettes en sélectionnant l’une des options sur l’écran du tableau de bord de l’application, dans lequel vous pouvez voir les détails des applications sous forme de cartes. Par défaut, 250 applications sont affichées sur le tableau de bord des applications. Pour afficher plus d’applications, cliquez sur l’option de la page suivante.

Les applications sont regroupées selon les catégories qui ont été sélectionnées lors de leur définition. Les applications peuvent être triées ou rendues visibles en sélectionnant les mesures de l'application dans le panneau de résumé de l'application. Par exemple, si vous souhaitez afficher les applications dont le score est compris entre 20 et 40, sélectionnez le graphique à barres approprié dans la section App Score du panneau de résumé des applications. De même, vous pouvez sélectionner d'autres indicateurs dans le panneau récapitulatif de l'application.

### **Panneau récapitulatif de l'application**

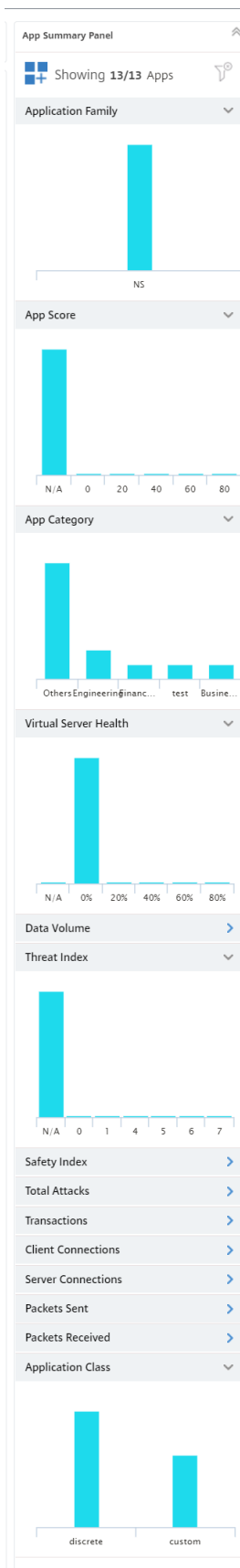
Le panneau récapitulatif des applications affiche toutes les statistiques des applications qui sont visibles sur le tableau de bord des applications. Ce panneau vous permet de trier et d'afficher les applications sur le tableau de bord en sélectionnant ou désélectionnant les mesures relatives aux applications. Le panneau récapitulatif de l'application affiche les statistiques suivantes :

---

Métriques	Description
Famille d'applications	Graphique à barres qui regroupe le nombre d'applications en fonction du type d'instances Citrix ADC sur lesquelles elles sont configurées.
Score de l'application	Un système de notation qui définit les performances d'une application
Catégorie d'application	Un graphique à barres qui affiche un histogramme pour toutes les catégories définies dans Citrix ADM. Toutes les applications discrètes apparaissent désormais dans la catégorie « Autres », et les applications personnalisées apparaissent sous leur nom de catégorie respectif.
Santé du serveur virtuel	Un graphique à barres qui affiche le nombre de demandes dans chaque catégorie. Les applications sont classées selon une valeur de score de santé de 0 %, 20 %, 40 %, 60 %, 80 % et 100 %.
Volume de données	Système de notation qui regroupe le nombre d'applications en fonction du volume de données de l'application. Le volume de données est calculé en fonction du nombre total d'octets demandés par les applications et du nombre d'octets reçus en réponse des applications.

Métriques	Description
Indice des menaces	Système d'évaluation à un chiffre qui indique la criticité des attaques contre l'application, que celle-ci soit protégée ou non par une appliance Citrix ADC.
Indice de sécurité	Système de notation à un chiffre indiquant la manière dont vous avez configuré en toute sécurité les instances Citrix ADC pour protéger les applications contre les menaces et les vulnérabilités externes.
Nombre total d'attaques	Le nombre total d'attaques contre les applications
Transactions	L'éventail des transactions effectuées par les applications.
Connexions client	Le nombre de connexions client établies par les applications.
Connexions au serveur	Le nombre de connexions au serveur établies par les applications.
Paquets envoyés	Le nombre de paquets envoyés par les applications.
Paquets reçus	Le nombre de paquets reçus par les applications.
Classe d'application	Un graphique à barres qui regroupe le nombre d'applications selon qu'il s'agit d'applications discrètes ou personnalisées.



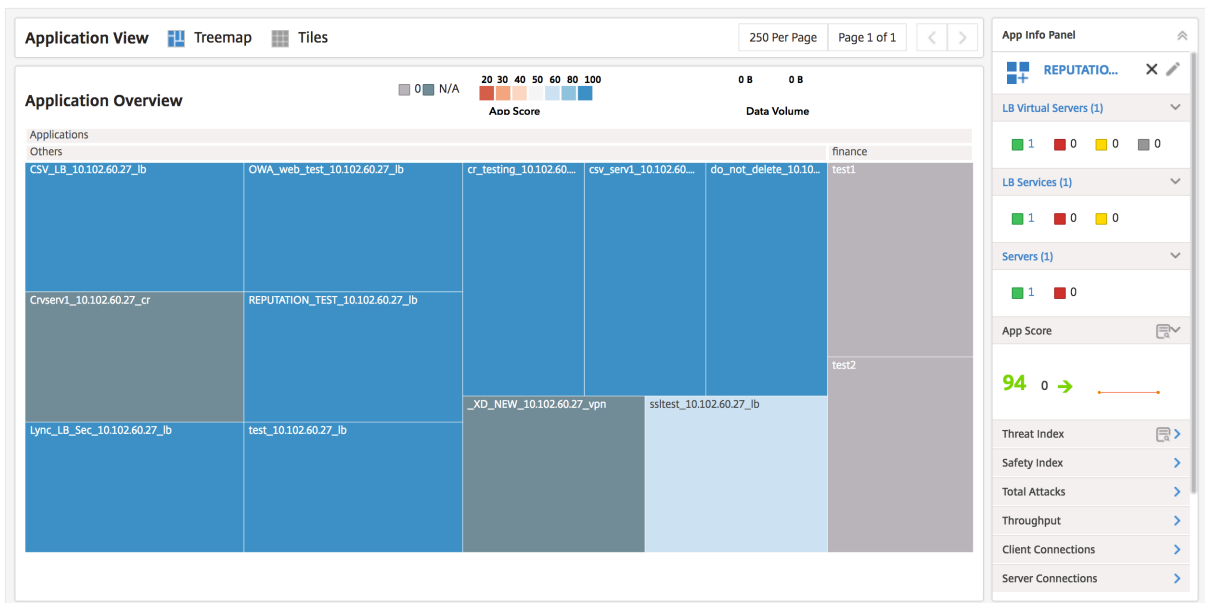


Par exemple, dans le panneau récapitulatif de l'application, faites défiler l'écran vers le bas pour trouver le graphique à barres « Virtual Server Health ». Dans le graphique de la barre d'intégrité du serveur virtuel, Citrix ADM classe les applications en fonction du pourcentage d'intégrité du serveur virtuel. Le graphique à barres affiche le nombre d'applications dont la valeur de santé des serveurs virtuels est comprise entre 0 % et 100 %.

L'état de santé des serveurs virtuels représente l'état des serveurs virtuels regroupés dans des applications distinctes. Mais s'il existe des applications personnalisées qui comprennent deux serveurs virtuels ou plus, le moins d'intégrité du serveur virtuel est pris en compte dans le groupe.

Vous pouvez désormais appliquer un filtre et voir uniquement les applications dans le tableau de bord de l'application qui correspondent aux critères de sélection. Cliquez sur la barre indiquant 0 %. Cette barre affiche le nombre d'applications dont l'état de santé du serveur virtuel est compris entre 0 % et 20 %. Vous pouvez désormais séparer les applications dont l'état de santé des serveurs virtuels est faible et prendre des mesures correctives

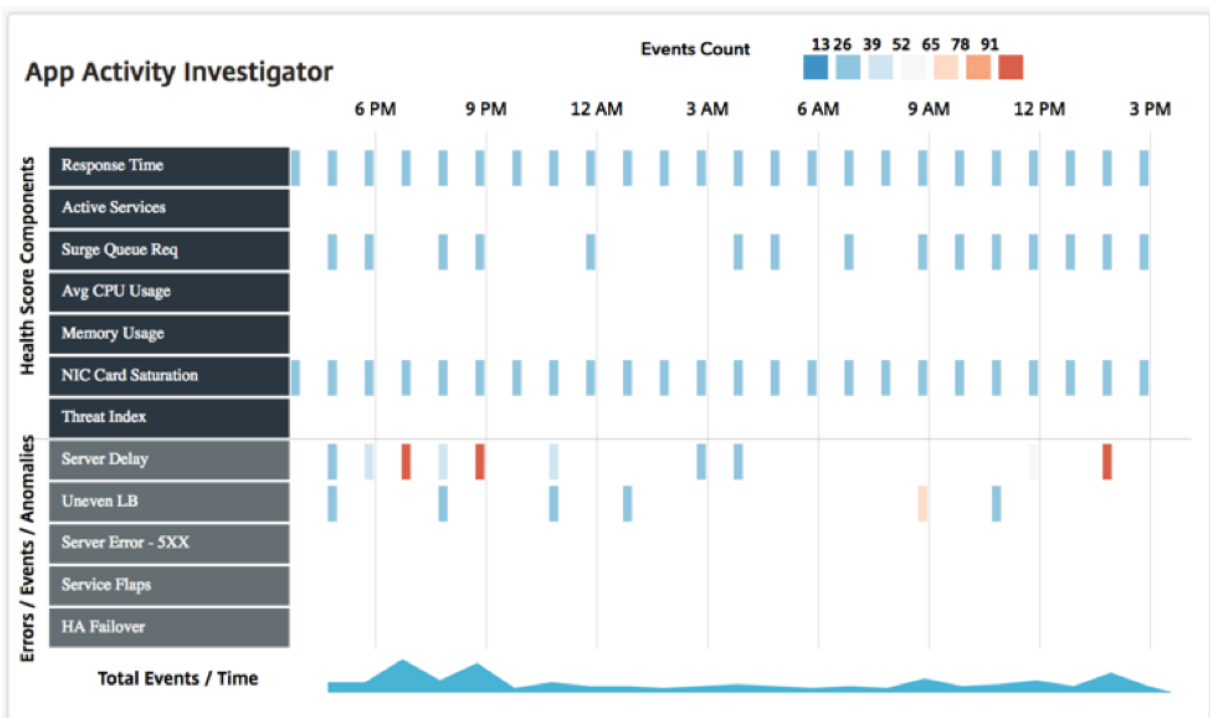
**Panneau d'informations sur l'application** Le panneau Informations sur l'application se trouve au premier niveau lorsque vous explorez une application vers le bas. Il affiche les métriques et les composants clés de l'application, ainsi que son état. Par exemple, pour toute application sélectionnée, le panneau Informations sur l'application affiche le nombre total de serveurs virtuels, le nombre total de services, le score de l'application et d'autres informations. Pour afficher le panneau d'informations de l'application, cliquez sur n'importe quelle vignette de l'application sur le tableau de bord de l'application. Le panneau Informations sur l'application remplace ensuite le panneau Résumé de l'application .



**Investigateur d'activités liées à** L'App Activity Investigator est l'un des deuxièmes niveaux lorsque vous effectuez une exploration vers le bas depuis une application. Vous pouvez accéder à App Activity Investigator en sélectionnant l'icône de recherche dans le panneau Informations sur l'application ou en double-cliquant sur la vignette de l'application dans le tableau de bord de l'application.

L'App Activity Investigator affiche des informations clés telles que les composants App Score, les erreurs, les événements et les anomalies.

Chacune des légendes est agrégée à une minute d'intervalle si la durée sélectionnée est d'une heure, et à une heure d'intervalle si la durée sélectionnée est d'un jour.



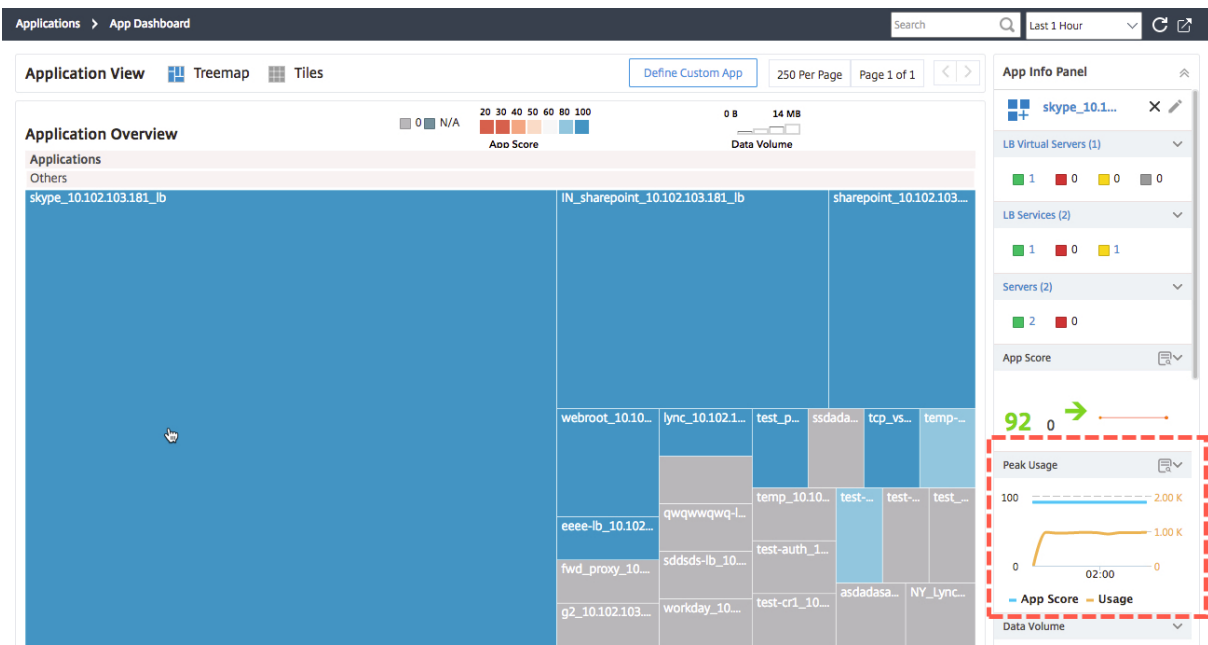
Ces écarts sont affichés sous forme de légendes rectangulaires sur le graphique. Ces légendes sont agrégées et sont codées par couleur en fonction du nombre d'événements qui se sont produits. Le bleu indique le plus petit nombre d'événements et le rouge le maximum. Vous pouvez placer le pointeur de la souris sur une légende pour afficher des détails tels que le type d'erreur, l'heure et le nombre d'événements agrégés pour la légende sélectionnée. Vous pouvez personnaliser la période du graphique en la sélectionnant dans la liste déroulante.

**Tendance d'utilisation des applications** Dans la plupart des cas, en tant que propriétaire d'entreprise, vous prenez des décisions concernant l'efficacité de vos applications et les tendances d'utilisation sur la base de statistiques et de données. Pour comprendre la tendance d'utilisation des applications, vous devez collecter des informations provenant de plusieurs entités de votre déploiement, telles que l'infrastructure principale, les proxys, les réseaux CDN, etc. Ensuite, corrélisez les informations collectées pour obtenir des analyses appropriées, cela prend beaucoup de temps.

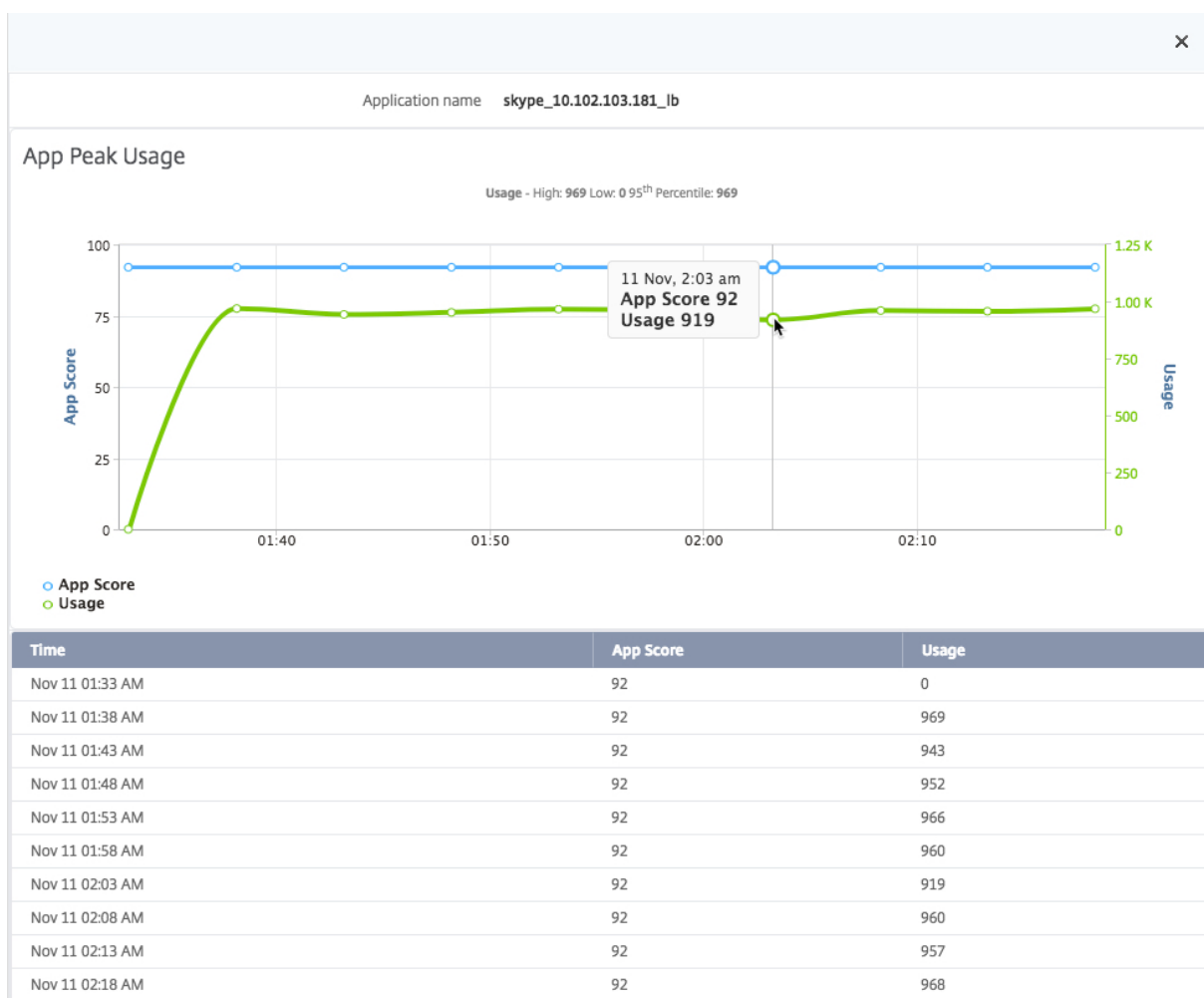
Au lieu de cela, l'apppliance Citrix ADC déployée en tant qu'ADC dans votre déploiement contient toutes les informations relatives à l'application et les statistiques d'utilisation de celle-ci. Vous pouvez transmettre ces informations à Citrix ADM. Citrix ADM collecte ces informations et fournit des informations détaillées sur l'utilisation et les performances de l'application. Vous pouvez utiliser ces informations pour prendre des décisions efficaces en fonction de l'utilisation et des performances de l'application.

Le panneau d'informations sur les applications du tableau de bord des applications indique la tendance d'utilisation maximale d'une application. Vous pouvez utiliser la tendance d'utilisation maximale pour évaluer les performances de l'application et prendre les mesures appropriées pour améliorer les performances de l'application.

Pour afficher la tendance d'utilisation maximale d'une application, accédez à **Applications > Tableau de bord** des applications. Sélectionnez l'application et la tendance d'utilisation maximale de l'application s'affiche dans la section Utilisation **maximale** du panneau d'informations de l'application.



Vous pouvez également cliquer sur la section **Utilisation maximale** pour afficher le score de l'application et l'utilisation de l'application. À l'aide de ces informations, vous pouvez identifier le pic d'utilisation de l'application et l'associer au score d'application correspondant afin d'évaluer l'impact sur les performances de l'application pendant la durée d'utilisation maximale.



## Exporter les rapports du tableau de bord de l'application et du tableau de bord de

Citrix ADM vous permet de prendre un instantané des pages actuelles du Tableau de bord de l'application et du Tableau de bord de la sécurité des applications et de les exporter en tant que rapports. À intervalles réguliers, les administrateurs de l'application peuvent avoir besoin d'utiliser ces rapports pour mettre à jour l'utilisation de l'application et les pénalités de performance.

Grâce à cette fonctionnalité, les administrateurs peuvent extraire ces données sous forme de rapports .png ou .pdf.

### Remarque

Contrairement aux autres options d'exportation de rapports dans Citrix ADM, vous ne pouvez exporter les rapports App Dashboard et Security Dashboard que sous forme de fichiers .pdf ou .png. D'autres options telles que .jpg et .csv ne sont pas prises en charge actuellement.

1. Sur la page Tableau de **bord des applications** ou Tableau de **bord de la sécurité** des applications, cliquez sur l'icône d'exportation en haut à droite de la page.

2. Choisissez l'option d'exportation en tant que fichier .pdf ou .png.
3. Cliquez sur **OK**.

Le rapport se télécharge sur votre système. À partir des pages App Dashboard et App Security Dashboard, vous pouvez également accéder à des pages de deuxième niveau et les exporter sous forme de rapports. Actuellement, vous pouvez télécharger des rapports d'une seule application à la fois.

## Analyse des performances des applications

February 1, 2024

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 et si tous les systèmes sont opérationnels. Le score de l'application s'affiche au niveau de l'application. Le calcul de la note est basé sur les trois éléments clés suivants :

- **Score de performance de l'application (score APDEX de l'application)**. Dérivé de la variation du temps de réponse du serveur de l'application.
- **Ressource système Citrix ADC**. Dérivé sur la base de trois autres composantes :
  - Utilisation du processeur
  - Utilisation de la mémoire
  - Saturation de la carte NIC
- **Ressource du serveur d'applications**. Dérivé de deux autres composants :
  - Pourcentage de services actifs
  - Demandes de file d'attente de surtension

Le score App est calculé à partir de ces scores, où le score de ressources système Citrix ADC et le score de ressources App Server sont soustraits du score Performance App. App Score est disponible pour toutes les applications définies avec des serveurs virtuels d'équilibrage de charge et de commutation de contenu détectés, ainsi que pour les applications personnalisées que vous définissez dans le tableau de bord de l'application.

### Pour configurer le score d'application dans Citrix ADM :

1. Dans Citrix ADM, accédez à **Analytics > Paramètres**.
2. Dans la page **Paramètres**, cliquez sur **Configurer le score de l'application**.
3. Sur la page **Configurer le score d'application**, entrez les valeurs des paramètres suivants :

- a) **Seuil de file d'attente de surtension inférieur.** Valeur de seuil inférieure du rapport entre le nombre total de connexions en attente de soumission pour le serveur virtuel et les connexions établies.
- b) **Seuil de file d'attente de surtension plus élevé.** Valeur de seuil supérieure du rapport entre le nombre total de connexions en attente de soumission pour le serveur virtuel et les connexions établies.
- c) **Seuil CPU faible ( %).** Valeur de seuil inférieure de l'utilisation totale de l'UC dans l'instance de Citrix ADC.
- d) **Seuil CPU élevé ( %).** Valeur de seuil plus élevée de l'utilisation totale de l'UC dans l'instance de Citrix ADC.
- e) **Seuil de mémoire faible ( %).** Valeur de seuil inférieure de l'utilisation totale de la mémoire dans l'instance de Citrix ADC.
- f) **Seuil de mémoire élevé ( %).** Valeur de seuil plus élevée de l'utilisation totale de la mémoire dans l'instance de Citrix ADC.
- g) **Rejets de carte réseau.** La valeur seuil inférieure des paquets rejetés par les interfaces.
- h) **Rejets de cartes réseau élevés.** La valeur seuil la plus élevée des paquets rejetés par les interfaces.
- i) **Temps de réponse.** Intervalle de temps entre l'envoi d'un paquet de requête et la réception du premier paquet de réponse à partir du service configuré sur le serveur virtuel. La valeur par défaut configurée dans Citrix ADM est 500 ms.
- j) **Seuil des services actifs.** Valeur de seuil du pourcentage de services qui doivent être actifs et qui sont liés au serveur virtuel.

## ← Configure App Score

Configure the below settings to calculate the App Score values

Lower Surge Queue Threshold

 ?

Higher Surge Queue Threshold

Low CPU Threshold (%)

High CPU Threshold (%)

Low Memory Threshold (%)

High Memory Threshold (%)

Low NIC Discards

High NIC Discards

Server Response Time (ms)

Active Services Threshold (%)

OK

Close

4. Cliquez sur **OK**.



## Analyse de la sécurité des applications

February 1, 2024

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 de synchronisation, les attaques par petites fenêtres et les attaques par inondation DNS pour les instances Citrix ADC découvertes.

### Remarque

Pour afficher les mesures du tableau de bord de sécurité des applications, les informations AppFlow for Security doivent être activées sur les instances Citrix ADC que vous souhaitez surveiller.

### Pour afficher les mesures de sécurité d'une instance de Citrix ADC sur le tableau de bord de sécurité de l'application :

1. Dans un navigateur Web, tapez l'adresse IP de Citrix Application Delivery Management (par exemple, <http://192.168.100.1>).
2. Dans **Nom d'utilisateur** et mot de **passé** , entrez les informations d'identification de l'administrateur.
3. Accédez à **Applications** > Tableau de **bord de sécurité** des applications , puis sélectionnez l'adresse IP de l'instance dans la liste déroulante **Appareils** .

Vous pouvez approfondir l'exploration des écarts signalés dans App Security Investigator en cliquant sur les bulles tracées sur le graphique.

## Créer une définition d'application

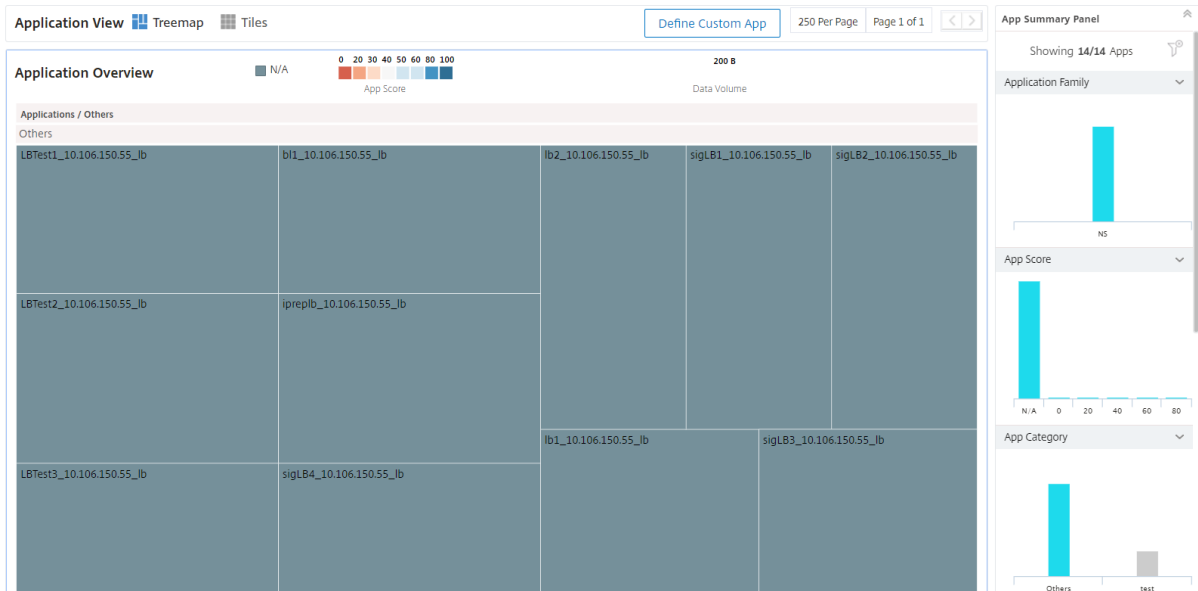
February 1, 2024

Vous pouvez définir une application personnalisée en fonction d'un ensemble d'applications découvertes dans Citrix ADM.

Dans Citrix ADM, lorsque vous accédez au Tableau de **bord des applications**, la page **Présentation des applications** affiche les applications par défaut. Ces applications par défaut ou « applications discrètes » sont les 30 applications pour lesquelles vous disposez des licences par défaut. Vous découvrez ces applications lorsque vous installez Citrix ADM dans votre environnement d'entreprise.

Lorsque vous créez des « applications personnalisées », les applications personnalisées remplacent les applications discrètes. Les applications personnalisées sont disposées sur le tableau de bord en fonction de la catégorie que vous avez choisie lors de leur création.

Vous pouvez afficher ces applications, découvertes et personnalisées, de deux manières : treemap et tuiles.



Vous pouvez créer une application personnalisée via une configuration statique ou dynamique.

1. **Définition statique des applications** - Dans une définition statique, vous pouvez définir une application. Cette définition n'est pas mise à jour lorsque de nouveaux serveurs virtuels sont configurés sur votre instance de Citrix ADC. Vous devez mettre à jour manuellement cette liste pour inclure d'autres serveurs virtuels.
2. **Définition dynamique des applications** - Dans une définition dynamique, vous pouvez utiliser l'un des trois critères ci-dessous pour définir une application :
  - a) **Serveurs.** Spécifiez l'adresse IP du serveur ou du service, le nom du serveur ou le port du serveur principal sur lequel les applications s'exécutent. Vous pouvez entrer une adresse IP, une plage d'adresses IP ou une combinaison des deux séparées par des virgules. Par exemple, vous pouvez entrer 10.102.29.20, 10.102.43.10-60, 10.216.43.45.
  - b) **Serveurs virtuels.** Vous pouvez spécifier l'une des options suivantes :
    - i. Adresse IP du serveur virtuel
    - ii. Nom du serveur virtuel, ou
    - iii. Port du serveur principal sur lequel les applications sont en cours d'exécution.

Vous pouvez entrer une adresse IP ou une plage d'adresses IP ou une combinaison des deux

séparées par des virgules. Par exemple, vous pouvez entrer 10.102.29.20, 10.102.43.10-60, 10.216.43.45.

3. **StyleBooks.** Vous pouvez créer des applications personnalisées à l'aide d'un StyleBook par défaut ou personnalisé déjà présent dans Citrix ADM. StyleBooks simplifie la gestion des configurations Citrix ADC complexes pour vos applications. Sélectionnez un StyleBook présent dans Citrix ADM et tapez les valeurs de paramètre StyleBook Citrix ADM crée la configuration (configpack) sur les instances Citrix ADC cibles en fonction du StyleBook sélectionné. Citrix ADM crée également une application personnalisée qui inclut tous les serveurs virtuels définis dans le configpack.

#### Remarque

Une application personnalisée et un pack de configuration sont créés si suffisamment de licences Citrix ADC sont disponibles.

Lorsque vous créez une application qui répond aux conditions définies ci-dessus dans l'un des trois critères, l'application est mise à jour automatiquement dans le Tableau de bord des applications lorsque Citrix ADM interroge les entités. Pour lancer un sondage manuellement, cliquez sur **Sondage maintenant** situé dans l'onglet **Applications**.

### Pour créer une application

1. Dans Citrix ADM, accédez à **Applications > tableau de bord** et cliquez sur **Définir une application personnalisée** pour créer une application personnalisée.
2. Dans la fenêtre **Définir une application**, tapez le nom de l'application dans le champ **Nom**.
3. Sélectionnez la catégorie d'application dans la section **Catégorie**. Citrix ADM vous permet de définir des catégories pour regrouper les applications définies par l'utilisateur. Vous pouvez également ajouter d'autres catégories si nécessaire.
4. Vous pouvez créer une application personnalisée selon l'une des trois méthodes suivantes :
  - a) **Sélectionnez Applications existantes.** Pour sélectionner des applications existantes, assurez-vous que l'**option Sélectionner des applications existantes** est activée. Choisissez l'application dans la liste de la section **Applications**. Cliquez sur **Ajouter des applications** pour ajouter de nouvelles applications à la liste.
  - b) **Définir les critères de sélection.** Vous pouvez également définir un critère de sélection pour ajouter des applications dans Citrix ADM. Vous pouvez ajouter des applications selon l'une des trois méthodes suivantes :
    - i. Spécification de l'adresse IP du serveur virtuel. Vous pouvez entrer une adresse IP ou une plage d'adresses IP ou une combinaison des deux séparées par des virgules.

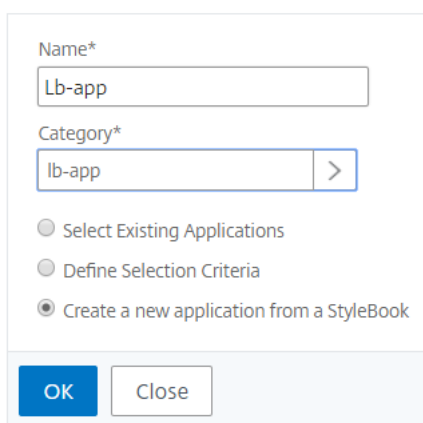
- ii. Spécifier le nom du serveur sur lequel les applications ou services sont en cours d'exécution.

**Remarque**

Vous pouvez également rechercher des noms de serveur à l'aide d'extensions génériques. Par exemple, `ssl*` ajoutera tous les serveurs virtuels `ssl` à l'application.

- iii. Spécification du numéro de port auquel l'application écoute sur le serveur sélectionné.
- c) **Créez une nouvelle application à partir de StyleBook.** Sélectionnez le StyleBook requis dans Citrix ADM pour créer des packs de configuration sur les instances de Citrix ADC et associer les serveurs virtuels à une application personnalisée.

## ← Define Application



Name\*

Lb-app

Category\*

lb-app

Select Existing Applications

Define Selection Criteria


Create a new application from a StyleBook

OK Close

5. Cliquez sur **OK**. Si vous avez choisi de créer des applications à partir de StyleBooks, la page **Choisir StyleBook** s'ouvre. Cette page contient la liste de tous les StyleBooks présents dans Citrix ADM.

## Choose StyleBook


**HTTP/SSL LoadBalancing (with Monitors) StyleBook**

 This stylebook defines a typical Load Balanced Application configuration with monitors.

DEFAULT Name : **lb-mon** | Namespace : **com.citrix.adc.stylebooks** | Version : **1.0**

[View Definition](#)


**Microsoft Exchange 2016**

 This StyleBook defines NetScaler configuration for Microsoft Exchange 2016

DEFAULT Name : **microsoft-exchange-2016** | Namespace : **com.citrix.adc.enterprise.stylebooks** | Version : **1.2**

[View Definition](#)


**HTTP/SSL Content Switched Application with Monitors**

 This StyleBook defines a typical HTTP or SSL Content Switched Application configuration with monitors.

DEFAULT Name : **cs-lb-mon** | Namespace : **com.citrix.adc.stylebooks** | Version : **1.0**

[View Definition](#)

**GSLB StyleBook**

 This StyleBook is used to configure one or a number of NetScalers in different sites into a GSLB setup. It is assumed that the SNIP IP on each NetScaler to be used by this StyleBook as the Site IP is already configured on the appliance.

DEFAULT Name : **gslb** | Namespace : **com.citrix.adc.stylebooks** | Version : **1.0**

[View Definition](#)

6. Sélectionnez le StyleBook. Le StyleBook s'ouvre en tant que formulaire d'interface utilisateur. Entrez les valeurs de tous les paramètres dans le StyleBook. Vous pouvez également cliquer sur Afficher la **définition** pour afficher la structure du StyleBook avant de l'utiliser. Pour plus d'informations sur l'utilisation de StyleBooks personnalisés ou par défaut, voir [Utiliser des StyleBooks par défaut](#).
7. Une application personnalisée et le pack de configuration sont maintenant créés sur les instances de Citrix ADC que vous avez sélectionnées dans la section cible du StyleBook

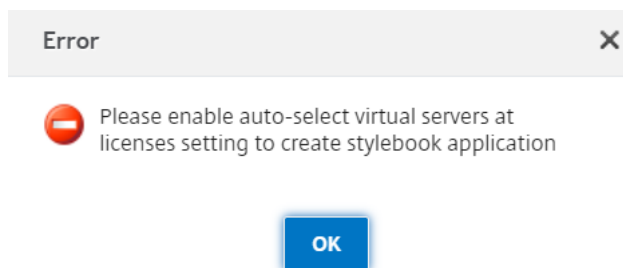
### Remarque

Une application personnalisée et un pack de configuration sont créés si suffisamment de licences Citrix ADM sont disponibles.

## Pour sélectionner automatiquement des serveurs virtuels pour l'octroi de licences

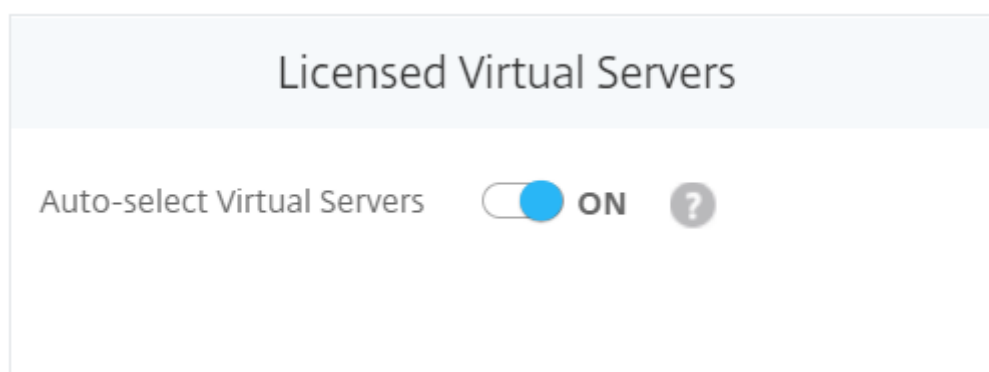
Vous devez autoriser Citrix ADM à sélectionner automatiquement les serveurs virtuels pour l'octroi de licences lorsque vous utilisez l'option StyleBook pour créer des configurations. Si vous n'avez pas

activé la sélection automatique, vous pouvez recevoir un message d'erreur comme indiqué dans l'image ci-dessous :



**Pour activer la sélection automatique des serveurs virtuels :**

1. Dans Citrix ADM, accédez à **Réseaux > Licences > Licences système** .
2. Cliquez sur **Sélectionner automatiquement les serveurs virtuels** pour activer l'option dans la section **Serveurs virtuels sous licence**.



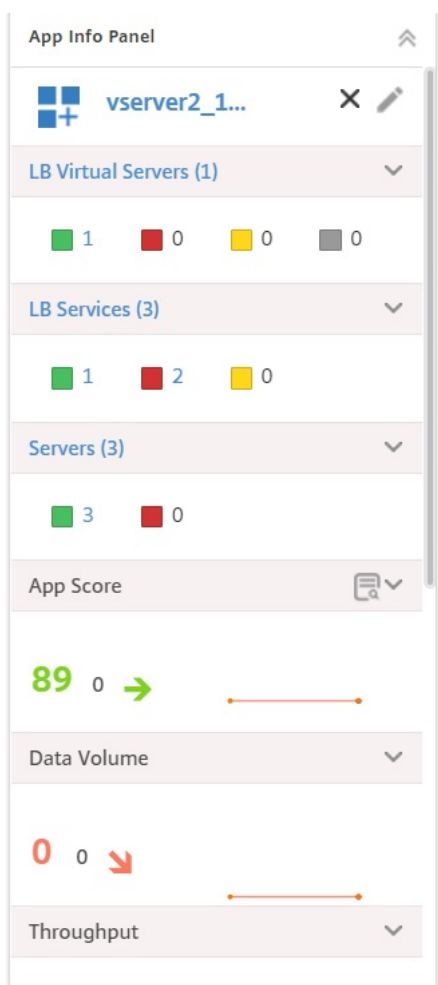
Lorsque cette option est activée, Citrix ADM sélectionne automatiquement les serveurs virtuels à octroyer une licence. Et lorsqu'il n'est pas activé, vous devez explicitement sélectionner les serveurs virtuels.

**Pour afficher les détails de l'application dans Citrix ADM**

Citrix ADM affiche tous les détails d'une application dans un volet distinct à droite, appelé **Panneau d'informations sur l'application**.

**Pour afficher le panneau d'informations sur l'application :**

1. Dans Citrix ADM, accédez à **Application > Tableau de bord**.
2. Dans la section **Présentation de l'application**, cliquez sur l'application pour laquelle vous souhaitez afficher les détails.



Les entités liées à l'application que vous avez sélectionnée sont disposées verticalement dans le **volet d'informations sur l'application**. Les boîtes disposées verticalement dans le volet affichent les éléments suivants :

- nom de chaque entité
- le nombre d'entités actives
- entités inactives
- entités hors service

Les entités affichées ici sont les serveurs virtuels, les services, les groupes de services et les serveurs d'applications. Le volet affiche également d'autres données telles que le score d'application, le volume de données, le débit, les connexions serveur et client et les transactions qui se produisent dans chaque application.

Vous pouvez afficher le nombre de serveurs virtuels, de services et de groupes de services qui se trouvent dans des états différents pour chaque application. Vous pouvez cliquer sur le nom de l'entité ou

sur le nombre affiché pour activer ou désactiver directement les entités. Vous pouvez également activer ou désactiver d'autres entités liées telles que des serveurs virtuels, des services et des groupes de services.

Pour plus d'informations sur la configuration des serveurs d'équilibrage de charge, voir [Create Load Balancing Support via Application Dashboard](#).

## Créer un seuil et une alerte pour l'analyse des applications

February 1, 2024

L'analyse des applications sur Citrix ADM vous permet de surveiller les différents types de trafic transitant par les instances Citrix. Citrix ADM vous permet de définir des seuils sur différents compteurs utilisés pour surveiller le trafic d'informations. Vous pouvez également configurer des règles et créer des alertes dans Citrix ADM.

1. Dans Citrix ADM, accédez à **Analytics > Paramètres > Seuils**. Sur la page **Seuils**, cliquez sur **Ajouter**.
2. Sur la page **Créer un seuil**, indiquez les informations suivantes :
  - a) **Nom**. Entrez un nom pour créer un événement pour lequel Citrix ADM génère une alerte.
  - b) **Type** de trafic \*\*. Dans la zone de liste, sélectionnez APPANALYTICS.
  - c) **Entité**. Dans la zone de liste, sélectionnez la catégorie ou le type de ressource. Par défaut, « applications » est sélectionné comme entité.
  - d) **Clé** de référence \*\*. Une clé de référence est 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.



## ← Create Threshold

Name\*  
 ?

Traffic Type\*  
 ?

Entity\*  
 ?

Reference Key

Duration\*

3. Dans la section **Configurer la règle**, créez une règle en choisissant la métrique **App Score**, un comparateur obligatoire, et indiquez une valeur de seuil.

**Configure Rule**

Metric\*  
 ?

Comparator\*  
 ?

Value\*  
 ?

4. Cliquez sur **Activer le seuil** pour permettre à Citrix ADM de commencer à surveiller les entités.
5. Vous pouvez également configurer des actions telles que les notifications par e-mail et les notifications par SMS. Cliquez sur **Créer**.

**Notification Settings**

Enable Threshold ?

Notify through Email ?

Email Distribution List\*  
 +  ?

Notify through SMS

## StyleBooks

February 1, 2024

StyleBooks simplifie la gestion des configurations Citrix ADC complexes pour vos applications. Un StyleBook est un modèle que vous pouvez utiliser pour créer et gérer des configurations Citrix ADC. Vous pouvez créer un StyleBook pour configurer une fonctionnalité spécifique de Citrix ADC, ou vous pouvez concevoir un StyleBook pour créer des configurations pour le déploiement d'une application d'entreprise telle que Microsoft Exchange ou Lync.

Les StyleBooks s'intègrent parfaitement aux principes de l'infrastructure en tant que code appliqués par les équipes DevOps, où les configurations sont déclaratives et contrôlées par version. Les configurations sont également répétées et déployées dans leur ensemble. Les StyleBooks offrent les avantages suivants :

- **Déclaratif** : StyleBooks sont écrits dans une syntaxe déclarative plutôt que impérative. Les stylebooks vous permettent de vous concentrer sur la description du résultat ou de l'« état souhaité » de la configuration plutôt que sur les instructions étape par étape sur la façon de l'atteindre sur une instance Citrix ADC particulière. Citrix Application Delivery Management (ADM) calcule la différence entre l'état existant sur un Citrix ADC et l'état souhaité que vous avez spécifié, et apporte les modifications nécessaires à l'infrastructure. Étant donné que StyleBooks utilise une syntaxe déclarative, écrite en YAML, les composants d'un StyleBook peuvent être spécifiés dans n'importe quel ordre, et Citrix ADM détermine l'ordre correct en fonction de leurs dépendances calculées.
- **Atomic** : lorsque vous utilisez StyleBooks pour déployer des configurations, la configuration complète est déployée ou aucune d'entre elles n'est déployée, ce qui garantit que l'infrastructure reste toujours dans un état cohérent.
- **Versionné** : un StyleBook possède un nom, un espace de noms et un numéro de version qui le distinguent de manière unique de tous les autres StyleBook du système. Toute modification apportée à un StyleBook nécessite la mise à jour de son numéro de version (ou de son nom ou de son espace de noms) afin de conserver ce caractère unique. La mise à jour de version vous permet également de conserver plusieurs versions du même StyleBook.
- **Composable** : une fois qu'un StyleBook est défini, le StyleBook peut être utilisé comme une unité pour créer d'autres StyleBooks. Vous pouvez éviter de répéter les modèles de configuration courants. Cela vous permet également d'établir des éléments de base standard au sein de votre organisation. Comme les StyleBooks sont versionnés, les modifications apportées aux StyleBooks existants génèrent de nouveaux StyleBooks, garantissant ainsi que les StyleBooks dépendants ne sont jamais cassés involontairement.
- **Centré sur les applications** : les StyleBooks peuvent être utilisés pour définir la configuration Citrix ADC d'une application complète. La configuration de l'application peut être abstraite à l'aide de paramètres. Par conséquent, les utilisateurs qui créent des configurations à partir d'un StyleBook peuvent interagir avec une interface simple consistant à remplir quelques paramètres pour créer ce qui peut être une configuration Citrix ADC complexe. Les configura-

tions créées à partir de StyleBooks ne sont pas liées à l'infrastructure. Une configuration unique peut donc être déployée sur un ou plusieurs Citrix ADC et peut également être déplacée d'une instance à l'autre.

- **UI générée automatiquement** : Citrix ADM génère automatiquement des formulaires d'interface utilisateur utilisés pour remplir les paramètres du StyleBook lorsque la configuration est effectuée à l'aide de l'interface graphique Citrix ADM. Les auteurs de StyleBook n'ont pas besoin d'apprendre un nouveau langage d'interface utilisateur ni de créer des pages et des formulaires d'interface utilisateur séparément
- **Piloté par API** : toutes les opérations de configuration sont prises en charge à l'aide de l'interface graphique Citrix ADM ou via des API REST. Les API peuvent être utilisées en mode synchrone ou asynchrone. Outre les tâches de configuration, les API StyleBooks vous permettent également de découvrir le schéma (description des paramètres) de n'importe quel StyleBook lors de l'exécution.

Vous pouvez utiliser un StyleBook pour créer plusieurs configurations. Chaque configuration est enregistrée en tant que pack de configuration. Par exemple, considérez que vous disposez d'un StyleBook qui définit une configuration d'application d'équilibrage de charge HTTP typique. Vous pouvez créer une configuration avec des valeurs pour les entités d'équilibrage de charge et l'exécuter sur une instance de Citrix ADC. Cette configuration est enregistrée en tant que pack de configuration. Vous pouvez utiliser le même StyleBook pour créer une autre configuration avec des valeurs différentes et l'exécuter sur la même instance Citrix ADC ou une autre. Un nouveau pack de configuration est créé pour cette configuration. Un pack de configuration est enregistré à la fois sur Citrix ADM et sur l'instance Citrix ADC sur laquelle la configuration est exécutée.

Vous pouvez utiliser les StyleBooks par défaut, livrés avec Citrix ADM, pour créer des configurations pour votre déploiement, ou concevoir vos propres StyleBooks et les importer dans Citrix ADM. Vous pouvez utiliser les StyleBooks pour créer des configurations à l'aide de l'interface graphique Citrix ADM ou à l'aide d'API.

Ce document contient les informations suivantes :

- [Comment consulter des StyleBooks](#)
- [StyleBooks par défaut](#)
- [Stylebooks développés pour les applications professionnelles](#)
- [StyleBooks personnalisés](#)
- [API dans StyleBooks](#)
- [Grammaire de StyleBooks](#)

## Groupes StyleBook

February 1, 2024

Les StyleBooks dans Citrix Application Delivery Management (ADM) peuvent être regroupés de deux manières. Ils peuvent être regroupés en tant que StyleBooks par défaut ou StyleBooks personnalisés. Ils peuvent également être regroupés en tant que StyleBooks publics ou privés. Dans Citrix ADM, vous pouvez afficher tous les StyleBooks présents dans le système. Citrix ADM vous permet également de trier et d'afficher les StyleBooks. Vous pouvez également afficher un affichage graphique de la manière dont StyleBooks sont connectés les uns aux autres.

Ce document vous indique également comment télécharger et supprimer des StyleBooks personnalisés. Vous pouvez télécharger un StyleBook personnalisé pour apporter des modifications ou pour créer un nouveau StyleBook basé sur le précédent. Vous pouvez également supprimer un StyleBook personnalisé.

### StyleBooks personnalisés et par défaut

- Les StyleBooks par défaut sont les StyleBooks présents dans le système de fichiers Citrix ADM et ils vous permettent de créer des configurations que vous pouvez déployer sur vos instances Citrix ADC.
- Les StyleBooks personnalisés sont vos propres StyleBooks que vous pouvez écrire et importer dans Citrix ADM, et créer des objets de configuration.

Les StyleBooks par défaut et personnalisés peuvent être publics ou privés.

### StyleBooks publics et privés

Les StyleBooks à partir desquels vous pouvez créer des packs de configuration à déployer sur les instances Citrix ADC peuvent être classés dans la catégorie des StyleBooks « publics ». C'est-à-dire qu'ils sont tous disponibles pour votre utilisation directe pour créer des configurations.

Mais certains StyleBooks sont utilisés comme blocs de construction pour d'autres StyleBooks. Ces blocs de construction sont les StyleBooks intégrés qui composent les StyleBooks par défaut. Ces StyleBooks sont appelés StyleBooks « privés ». Bien qu'ils ne soient pas directement utilisés pour créer des packs de configuration sur les instances, vous souhaitez peut-être afficher ces StyleBooks sur Citrix ADM. Pour marquer un StyleBook comme privé, vous pouvez utiliser l'attribut `private` pour empêcher qu'un StyleBook ne soit répertorié sur Citrix ADM.

```
1 name: basic-lb-config
```

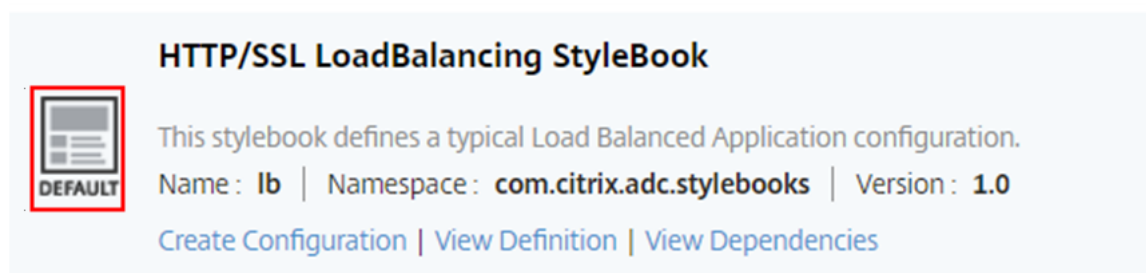
```
2 description: This StyleBook defines a simple load balancing
   configuration and is a building block to build other load balancing
   configurations.
3 display-name: Load Balancing Configuration
4 namespace: com.example.stylebooks
5 private: true
6 schema-version: "1.0"
7 version: "0.1"
8 <!--NeedCopy-->
```

## Affichage de StyleBooks

Le nombre de StyleBooks, qu'ils soient par défaut ou privés, augmente dans Citrix ADM. Vous souhaitez peut-être rechercher le StyleBook auquel vous souhaitez accéder. Vous souhaitez peut-être également afficher les deux types de StyleBooks séparément.

Dans Citrix ADM, lorsque vous accédez à **Applications > StyleBooks**, vous pouvez afficher la liste des StyleBooks présents dans le système.

Un StyleBook public par défaut comporte l'icône suivante dans son panneau :



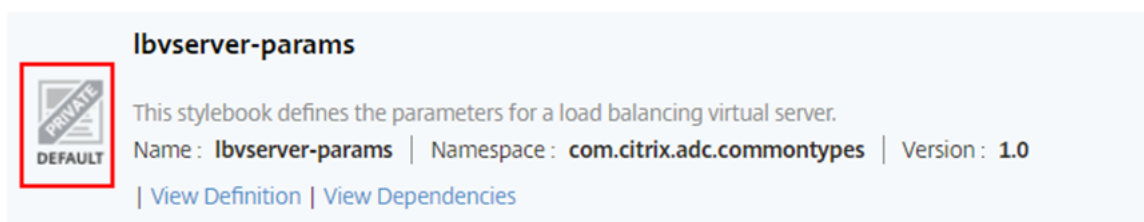
**HTTP/SSL LoadBalancing StyleBook**

This stylebook defines a typical Load Balanced Application configuration.

Name: **lb** | Namespace: **com.citrix.adc.stylebooks** | Version: **1.0**

[Create Configuration](#) | [View Definition](#) | [View Dependencies](#)

Alors qu'un StyleBook privé par défaut possède une icône qui le déclare en tant que StyleBook privé :



**lbserver-params**

This stylebook defines the parameters for a load balancing virtual server.


Name: **lbserver-params** | Namespace: **com.citrix.adc.commonotypes** | Version: **1.0**

[View Definition](#) | [View Dependencies](#)

Bien que vous puissiez afficher la définition et les dépendances d'un StyleBook privé, vous ne pouvez pas créer un pack de configuration à partir d'un StyleBook privé. Vous pouvez toujours utiliser un StyleBook privé dans votre propre StyleBook.

Un StyleBook public personnalisé a une icône différente comme le montre l'image suivante :

**Enable Netscaler features** | Citrix ADC Versions Supported : **10.5, 11.0, 11.1, 12.0 and 12.1**




This shows how to enable Netscaler features  
Name : **EnableFeatures** | Namespace : **com.example.stylebooks** | Version : **0.1**

[Create Configuration](#) | [View Definition](#) | [View Dependencies](#) | [Download](#) | [Delete](#)

Alors que, un StyleBook privé personnalisé apparaît avec cette icône :

**certificate**



This stylebook defines a typical ssl certificate type.  
Name : **certificate** | Namespace : **com.citrix.adc.commontypes** | Version : **1.1**

[View Definition](#) | [View Dependencies](#) | [Download](#) | [Delete](#)


En haut à droite de la page, vous pouvez voir une option permettant de trier les StyleBooks. Il y a trois options - toutes, publiques ou privées StyleBooks. Cliquez sur l'une des options.

StyleBooks

Public

Q Click here to search or you can enter Key : Value format


**Enable Netscaler features** | Citrix ADC Versions Supported : **10.5, 11.0, 11.1, 12.0 and 12.1**



This shows how to enable Netscaler features  
Name : **EnableFeatures** | Namespace : **com.example.stylebooks** | Version : **0.1**

[Create Configuration](#) | [View Definition](#) | [View Dependencies](#) | [Download](#) | [Delete](#)


**HTTP/SSL LoadBalancing StyleBook** | Citrix ADC Versions Supported : **10.5, 11.0, 11.1, 12.0 and 12.1**



This stylebook defines a typical Load Balanced Application configuration.  
Name : **lb** | Namespace : **com.citrix.adc.stylebooks** | Version : **1.1**

[Create Configuration](#) | [View Definition](#) | [View Dependencies](#)

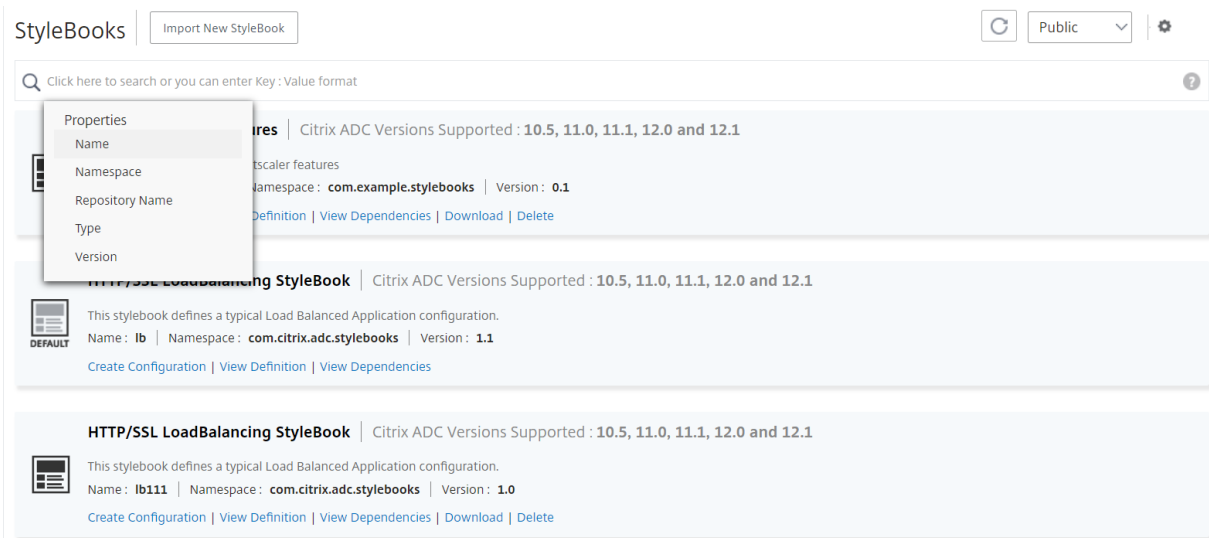
**HTTP/SSL LoadBalancing StyleBook** | Citrix ADC Versions Supported : **10.5, 11.0, 11.1, 12.0 and 12.1**



This stylebook defines a typical Load Balanced Application configuration.  
Name : **lb111** | Namespace : **com.citrix.adc.stylebooks** | Version : **1.0**

[Create Configuration](#) | [View Definition](#) | [View Dependencies](#) | [Download](#) | [Delete](#)

Vous pouvez également rechercher un StyleBook particulier en cliquant sur l'icône de recherche. Les trois options de recherche disponibles sont le nom, l'espace de noms et la version. L'opération de recherche n'est pas sensible à la casse.



### Affichage des dépendances de StyleBook

Citrix ADM vous permet d'afficher un affichage graphique de la manière dont StyleBooks sont connectés les uns aux autres.

Dans Citrix ADM, vous pouvez utiliser les StyleBooks par défaut pour créer des configurations pour votre déploiement. Vous pouvez également concevoir vos propres StyleBooks et les importer dans Citrix ADM.

Une caractéristique importante et puissante de StyleBooks est qu'ils peuvent être utilisés comme blocs de construction pour d'autres StyleBooks. Vous pouvez importer un StyleBook dans un autre StyleBook. Un Stylebook importé est déclaré en tant que type et est utilisé par les composants ou les paramètres du second StyleBook.

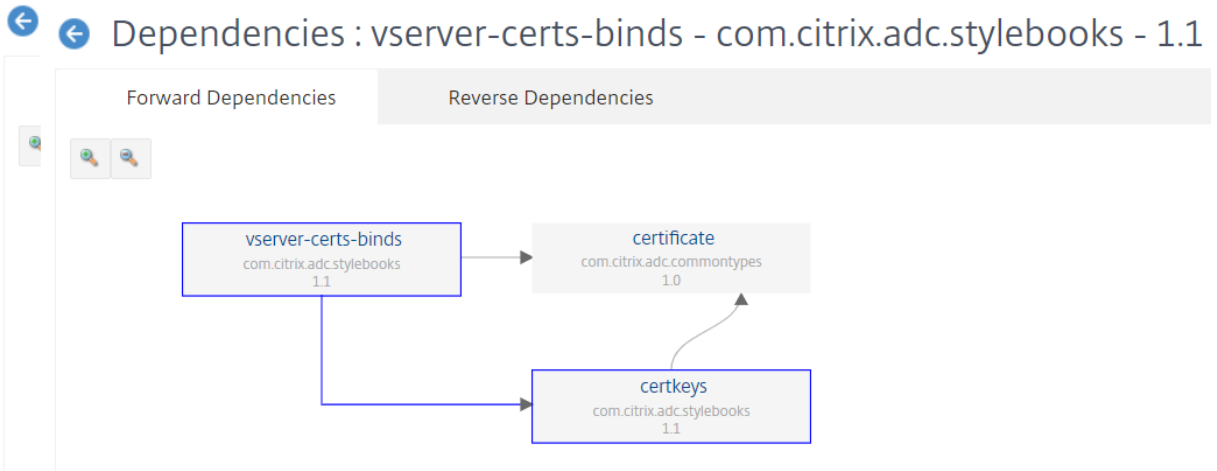
Un StyleBook utilisé par d'autres StyleBooks ne peut pas être supprimé du système. Cependant, un affichage graphique de StyleBooks vous permet de savoir quels StyleBooks empêchent la suppression d'un StyleBook. En regardant le graphique, il est possible de voir les relations entre plusieurs StyleBooks.

### Pour afficher les dépendances de StyleBook

Dans Citrix ADM, accédez à **Applications > StyleBooks**. La page StyleBooks affiche tous les StyleBooks disponibles pour votre utilisation dans Citrix ADM. Faites défiler l'écran vers le bas et trouvez votre StyleBook. Le panneau StyleBook affiche des liens permettant de créer une configuration, d'afficher la définition de StyleBook et d'afficher les dépendances de StyleBook. Cliquez sur **Afficher les dépendances**.

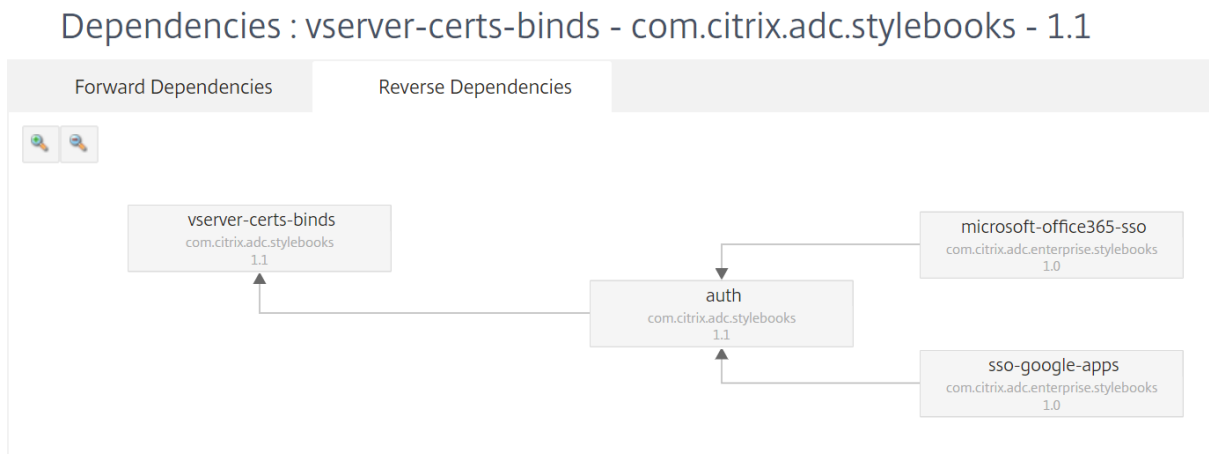
## Dépendances de transfert

L'onglet Forward Dependencies vous permet de visualiser les différents StyleBooks par défaut que votre StyleBook utilise. Suivez les flèches pour trouver le StyleBook utilisé par un StyleBook. Lorsque vous pointez votre souris sur l'une des flèches, la flèche et les StyleBooks connectés les uns aux autres sont surlignés. Vous pouvez également cliquer sur les noms du StyleBook pour afficher la définition de ce StyleBook.



## Inverser les dépendances

L'onglet Dépendances inversées vous permet d'afficher graphiquement les StyleBooks qui utilisent votre StyleBook. Si vous suivez les flèches, vous pouvez voir que tous les StyleBooks affichés pointent vers votre StyleBook. Certains StyleBooks utilisent directement le StyleBook et certains StyleBook peuvent l'utiliser via un autre StyleBook.





## Téléchargement de StyleBooks personnalisés

Pour télécharger des Stylebooks personnalisés depuis Citrix ADM, accédez à **Applications > Style-Books > Configurations**. Dans la liste des StyleBooks affichés sur le panneau de droite, les Style-Books personnalisés peuvent les télécharger. Cliquez sur **Download (Télécharger)**. Si le StyleBook possède des StyleBooks personnalisés dépendants, même ces StyleBooks sont téléchargés sur votre système.

### Remarque

Vous ne pouvez pas télécharger les StyleBooks par défaut ou personnalisés qui sont marqués comme publics ou privés.

The screenshot shows the 'StyleBooks' management interface. At the top, there is a search bar and a filter dropdown menu currently set to 'Public'. Below the search bar, three StyleBook entries are listed:

- Enable Netscaler features**: Citrix ADC Versions Supported : 10.5, 11.0, 11.1, 12.0 and 12.1. Name: EnableFeatures | Namespace: com.example.stylebooks | Version: 0.1. The 'Download' button is highlighted with a red box.
- HTTP/SSL LoadBalancing StyleBook**: Citrix ADC Versions Supported : 10.5, 11.0, 11.1, 12.0 and 12.1. Name: lb | Namespace: com.citrix.adc.stylebooks | Version: 1.1. Marked as 'DEFAULT'.
- HTTP/SSL LoadBalancing StyleBook**: Citrix ADC Versions Supported : 10.5, 11.0, 11.1, 12.0 and 12.1. Name: lb111 | Namespace: com.citrix.adc.stylebooks | Version: 1.0.

### Remarque

Vous ne pouvez pas télécharger les StyleBooks par défaut de Citrix ADM. Vous pouvez toutefois afficher leurs définitions et leurs dépendances en cliquant sur les liens **Afficher la définition** et **Afficher les dépendances** dans le panneau StyleBook.

## Supprimer des StyleBooks personnalisés

Vous pouvez également supprimer des StyleBooks personnalisés en cliquant sur l'icône « X » sur le côté droit du panneau StyleBook. Une fenêtre contextuelle vous invite à confirmer si vous souhaitez supprimer le StyleBook de Citrix ADM. Si le StyleBook utilise d'autres StyleBooks personnalisés (qui ne sont pas utilisés par d'autres StyleBooks), vous pouvez également choisir de les supprimer en cochant la case.

StyleBooks

Public Public Private All

Click here to search or you can enter Key : Value format

**Enable Netscaler features** | Citrix ADC Versions Supported : 10.5, 11.0, 11.1, 12.0 and 12.1

This shows how to enable Netscaler features  
Name : **EnableFeatures** | Namespace : **com.example.stylebooks** | Version : 0.1  
[Create Configuration](#) | [View Definition](#) | [View Dependencies](#) | [Download](#) | [Delete](#)

**HTTP/SSL LoadBalancing StyleBook** | Citrix ADC Versions Supported : 10.5, 11.0, 11.1, 12.0 and 12.1

This stylebook defines a typical Load Balanced Application configuration.  
Name : **lb** | Namespace : **com.citrix.adc.stylebooks** | Version : 1.1  
[Create Configuration](#) | [View Definition](#) | [View Dependencies](#)

**HTTP/SSL LoadBalancing StyleBook** | Citrix ADC Versions Supported : 10.5, 11.0, 11.1, 12.0 and 12.1

This stylebook defines a typical Load Balanced Application configuration.  
Name : **lb111** | Namespace : **com.citrix.adc.stylebooks** | Version : 1.0  
[Create Configuration](#) | [View Definition](#) | [View Dependencies](#) | [Download](#) | [Delete](#)

### Remarque

Vous ne pouvez pas supprimer un StyleBook personnalisé qui possède d'autres StyleBooks dans Citrix ADM qui en dépendent.

## Importation et synchronisation de StyleBooks à partir d'un référentiel GitHub

February 1, 2024

Supposons que vous utilisez des processus CI/CD pour votre développement ou que vous gérez tous les objets de déploiement dans GitHub. Vous avez peut-être créé plusieurs StyleBooks pour déployer vos configurations Citrix ADC et vous gérez les StyleBooks dans les référentiels GitHub. Vous pouvez désormais importer directement ces StyleBooks dans Citrix Applications and Delivery Management (ADM). Il n'est pas nécessaire de les copier manuellement depuis GitHub et de les charger dans Citrix ADM.

Vous pouvez désormais définir un référentiel dans Citrix ADM qui représente un référentiel GitHub en fournissant l'URL du référentiel GitHub. Vous devez fournir votre nom d'utilisateur et votre mot de passe (ou jeton d'API) créés dans GitHub. Cela signifie que seuls les utilisateurs autorisés possédant un compte valide sur GitHub peuvent importer et synchroniser StyleBooks.

Après avoir créé le référentiel, vous pouvez synchroniser Citrix ADM avec votre référentiel GitHub. Citrix ADM importe les StyleBooks trouvés dans ce référentiel, puis les valide et les ajoute à la liste des StyleBooks dans Citrix ADM. Les styleBooks ne sont pas ajoutés à Citrix ADM s'ils échouent la validation. Vous devez corriger les erreurs et valider les versions mises à jour dans votre référentiel GitHub. Plus tard, vous pouvez essayer de les importer ou de les synchroniser à nouveau dans Citrix ADM.

### Remarque

- Actuellement, vous ne pouvez importer et synchroniser que des StyleBooks auxquels aucun StyleBooks dépendant n'est associé. C'est-à-dire que le StyleBook doit avoir toutes les configurations dont il a besoin pour être défini dans un seul fichier.
- La synchronisation à partir d'un référentiel GitHub doit être lancée manuellement à partir de l'interface graphique ou de l'API Citrix ADM. C'est-à-dire qu'actuellement, l'importation de StyleBooks ne se fait pas automatiquement en fonction de l'activité de validation de GitHub.

Vous pouvez actuellement importer des fichiers StyleBooks à partir de la branche master uniquement.

### Conditions préalables

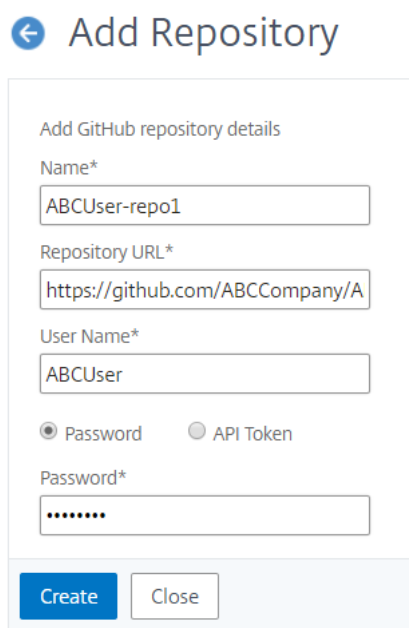
- Vous devez avoir un compte valide dans GitHub.
- Les fichiers StyleBook doivent exister dans le dossier racine de la branche principale du référentiel GitHub.

### Ajout d'un référentiel et importation de StyleBooks à partir de GitHub

1. Dans Citrix ADM, accédez à **Applications > Configurations > Référentiels**.
2. Cliquez sur **Ajouter**. Dans la fenêtre **Ajouter un référentiel**, entrez les paramètres suivants :
  - **Nom**. Entrez le nom du référentiel. Ce nom peut être le même que le nom du référentiel dans GitHub ou un autre.
  - **URL du référentiel**. Tapez l'URL du référentiel GitHub.
  - **Nom d'utilisateur et mot de passe**. Saisissez le nom d'utilisateur et le mot de passe avec lequel vous accédez au compte GitHub.

**Remarque** Vous pouvez également fournir le jeton d'API à la place d'un mot de passe. Les jetons API peuvent être utilisés à la place d'un mot de passe pour GitHub sur HTTPS. Vous pouvez également les utiliser pour vous authentifier auprès de l'API via l'authentification de base.

3. Cliquez sur **Créer**.



← Add Repository

Add GitHub repository details

Name\*

ABCUser-repo1

Repository URL\*

https://github.com/ABCCompany/A

User Name\*

ABCUser

Password  API Token

Password\*

.....

Create Close

Le référentiel est créé dans Citrix ADM.

4. Pour importer ou synchroniser StyleBooks, sélectionnez le référentiel dans la page **Référentiels**, puis cliquez sur **Synchroniser**.

Les autres actions que vous pouvez utiliser ici sont les suivantes :

- **Modifier.** Vous pouvez modifier l'URL, le nom d'utilisateur et le mot de passe (ou le jeton API) du référentiel.
- **Supprimer.** Vous pouvez supprimer le référentiel ainsi que tous les StyleBooks présents dans Citrix ADM qui ont été importés précédemment à partir de ce référentiel GitHub.

#### Remarque

Vous ne pouvez pas supprimer un référentiel de Citrix ADM s'il a des StyleBooks auxquels ConfigPacks est associé.

- **Réinitialiser.** Vous pouvez supprimer tous les StyleBooks dans Citrix ADM synchronisés à partir de ce référentiel sans réellement supprimer l'entrée de référentiel de Citrix ADM.
- **Liste des fichiers.** Vous pouvez voir une liste de tous les StyleBooks présents dans Citrix ADM qui proviennent du référentiel GitHub.

## Utiliser les StyleBooks par défaut

February 1, 2024

Un ensemble de StyleBooks par défaut est fourni avec Citrix Application Delivery Management (ADM). Lorsque vous utilisez un StyleBook par défaut, vous devez spécifier des valeurs pour les paramètres du StyleBook et sélectionner les adresses IP des instances Citrix ADC où vous souhaitez exécuter la configuration. Après avoir soumis la configuration, Citrix ADM valide les valeurs des paramètres que vous avez spécifiées, crée un graphe de la configuration, se connecte aux instances Citrix ADC et exécute la configuration sur les instances.

## Pour créer une configuration à partir d'un StyleBook par défaut

1. Accédez à **Applications > Configurations > StyleBooks**. La page StyleBooks affiche tous les StyleBooks de Citrix ADM. Cette liste inclut les StyleBooks par défaut et personnalisés. Vous pouvez taper le nom du StyleBook dans le champ de recherche et appuyer sur la touche **Entrée**. Sinon, vous pouvez faire défiler la liste pour trouver le Stylebook.
2. Cliquez sur **Créer une configuration**. Spécifiez les valeurs requises pour les paramètres.

The screenshot shows a configuration form with the following sections and fields:

- Load Balanced Application Name\***: Input field containing "lb-app".
- Load Balanced App Virtual IP address\***: Input field containing "192 . 128 . 29 . 41".
- Load Balanced App Virtual Port**: Input field containing "80".
- Load Balanced App Protocol\***: Dropdown menu set to "HTTP".
- Advanced Load Balancer Settings** (expanded):
  - Application Servers IP Addresses**: Two input fields containing "10 . 102 . 29 . 52" and "10 . 102 . 29 . 53".
  - Application Servers FQDN names**: Input field containing "example.app.com".
  - Application Server Port\***: Input field containing "80".
  - Application Server Protocol\***: Dropdown menu set to "HTTP".
- Advanced Application Server Settings** (collapsed):
  - SSL Certificate Settings** (collapsed):
 

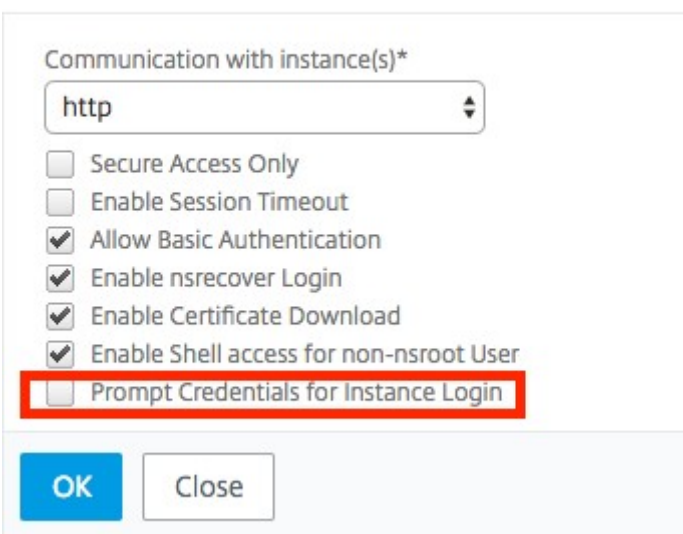
Certificate Name	CertKey Format	Certificate Key Name	Private Key Password
No Items			
  - Target Instances**: Input field with "Click to select" and a right arrow.
  - Dry Run**: Unchecked checkbox.

At the bottom of the form are two buttons: **Create** and **Close**.

3. Sous **Instances cibles**, cliquez sur et sélectionnez l'adresse IP de l'instance Citrix ADC sur laquelle vous souhaitez exécuter la configuration. Si vous souhaitez exécuter cette configuration sur plusieurs instances, cliquez sur « + » pour ajouter d'autres instances.

Si l'option **Demander des informations d'identification pour la connexion à l'instance** est activée dans **Citrix ADM > Système > Modifier les paramètres système > Modifier les paramètres système**, vous êtes invité à entrer vos informations d'identification d'instance Citrix ADC lorsque vous exécutez la commande sur les instances Citrix ADC sélectionnées. Sinon, Citrix ADM utilise les informations d'identification d'instance stockées dans le profil d'instance pour se connecter à l'instance.

## ← Modify System Settings



Communication with instance(s)\*

http

- Secure Access Only
- Enable Session Timeout
- Allow Basic Authentication
- Enable nsrecover Login
- Enable Certificate Download
- Enable Shell access for non-nsroot User
- Prompt Credentials for Instance Login

OK Close

Si vous souhaitez tester ou valider votre configuration avant de l'exécuter sur l'instance Citrix ADC, sélectionnez **Exécution à sec**, puis cliquez sur **Créer**. Si votre configuration est valide, les objets créés sur la base des valeurs que vous avez fournies sont affichés.

**Objects** ×

---

**Objects Added on Instance : 10.102.29.140**

---

**Type : server**  
 domain : example.app.com  
 name : example.app.com-server

---

**Type : service**  
 name : example.app.com-service  
 port : 80  
 servername : example.app.com-server  
 servicetype : HTTP

---

**Type : lbserver**  
 appflowlog : ENABLED  
 authentication : OFF  
 authn401 : OFF  
 downstateflush : ENABLED  
 ipv46 : 192.128.29.41  
 lbmethod : LEASTCONNECTION  
 name : lb-app-lb  
 port : 80  
 servicetype : HTTP

---

**Type : servicegroup**  
 cip : DISABLED  
 cka : NO  
 cmp : NO  
 downstateflush : DISABLED  
 servicegroupname : lb-app-svcgrp  
 servicetype : HTTP  
 sp : OFF  
 state : ENABLED  
 tcpb : NO  
 useproxyport : NO

4. Désactivez la case à cocher **Exécution à sec** et cliquez sur **Créer** pour créer la configuration et exécuter la configuration sur l'instance Citrix ADC. La configuration StyleBook que vous avez créée apparaît dans la liste des configurations, comme indiqué ci-dessous.

**Remarque**

Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter des instances Citrix ADC récemment découvertes dans Citrix ADM à la liste des instances disponibles dans cette fenêtre.

Vous pouvez désormais examiner, mettre à jour ou supprimer ce pack de configuration à l'aide de Citrix ADM.

## Masquer tous les StyleBooks par défaut

February 1, 2024

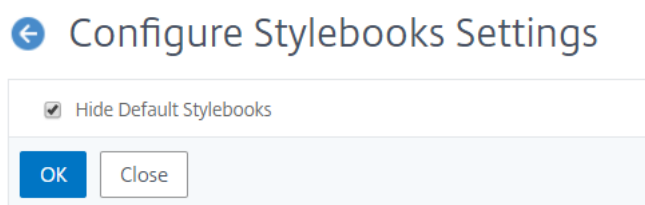
Citrix ADM répertorie tous les StyleBooks présents dans le système de dossiers Citrix ADM. La liste des StyleBooks inclut les StyleBooks par défaut et personnalisés qui peuvent être à la fois privés et publics.

En tant qu'administrateur, vous souhaitez peut-être masquer tous les StyleBooks par défaut. Vous pouvez autoriser vos utilisateurs à consulter et à accéder uniquement aux StyleBooks personnalisés créés par vous ou par les utilisateurs.

Citrix ADM vous permet d'afficher vos StyleBooks personnalisés et de masquer tous les StyleBooks par défaut fournis avec Citrix ADM. Une nouvelle option d'interface graphique permet de masquer tous les StyleBooks par défaut.

**Pour masquer tous les StyleBooks par défaut :**

1. Dans Citrix ADM, accédez à **Applications > Configurations > Paramètres**.
2. La page **Paramètres** affiche des informations indiquant si les StyleBooks par défaut sont visibles par les utilisateurs ou non.
3. Pour masquer les StyleBooks par défaut, cliquez sur l'icône d'édition en haut à droite.
4. Sur la page **Configurer les paramètres du StyleBook**, sélectionnez l'option **Masquer les StyleBooks par défaut**.
5. Cliquez sur **OK**.



La page **Configurer les paramètres StyleBook** est toujours visible pour les utilisateurs si vous n'avez pas choisi de masquer la page à l'aide de la fonction RBAC. Il se peut que les utilisateurs aient toujours la possibilité d'afficher les StyleBooks par défaut.

Pour masquer la page **Configurer les paramètres StyleBook**, vous devez créer une stratégie et attribuer cette stratégie aux utilisateurs qui ne doivent pas voir les StyleBooks par défaut.

**Pour créer une stratégie RBAC :**

1. Dans Citrix ADM, accédez à **Compte > Administration des utilisateurs > Stratégies d'accès**.
2. Cliquez sur **Add** pour créer une stratégie.
3. Entrez le nom de la stratégie.
4. Dans la section **Autorisations**, assurez-vous que l'option **Tout > Applications > Configuration > Paramètres** n'est pas sélectionnée, puis cliquez sur **OK**.



Après avoir créé des stratégies, vous devez créer des rôles, lier chaque rôle à une ou plusieurs stratégies et affecter des rôles à des groupes d'utilisateurs. Pour en savoir plus sur la façon d'associer des stratégies à des utilisateurs, consultez [Configuration du contrôle d'accès basé sur les rôles](#).

## StyleBook Google Apps SSO

February 1, 2024

Google Apps est un ensemble d'outils, de logiciels et de produits de cloud computing, de productivité et de collaboration développés par Google. L'authentification unique (SSO) permet aux utilisateurs d'accéder à toutes leurs applications cloud d'entreprise, y compris les administrateurs qui se connectent à la console d'administration, en se connectant en une seule fois pour tous les services à l'aide de leurs informations d'identification d'entreprise.

Le Citrix ADM SSO Google Apps StyleBook vous permet d'activer l'authentification unique pour Google Apps via des instances Citrix ADC. StyleBook configure l'instance Citrix ADC en tant que fournisseur d'identité SAML pour authentifier les utilisateurs pour accéder à Google Apps.

L'activation de l'authentification unique pour les applications Google dans une instance Citrix ADC à l'aide de ce StyleBook se traduit par les étapes suivantes :

1. Configuration du serveur virtuel d'authentification
2. Configuration d'une stratégie et d'un profil d'IDP SAML
3. Liaison de la stratégie et du profil au serveur virtuel d'authentification
4. Configuration d'un serveur d'authentification LDAP et d'une stratégie sur l'instance
5. Lier le serveur et la stratégie d'authentification LDAP à votre serveur virtuel d'authentification configuré sur l'instance

### Détails de configuration :

Le tableau ci-dessous répertorie les versions logicielles minimales requises pour que cette intégration fonctionne correctement. Le processus d'intégration devrait également fonctionner avec des versions supérieures de celui-ci.

---

Produit	Version minimale requise
Citrix ADC	Version 11.0, licence Enterprise/Platinum

---

Les instructions suivantes supposent que vous avez déjà créé les entrées DNS externes et/ou internes appropriées pour acheminer les demandes d'authentification vers une adresse IP surveillée par Citrix ADC.

## Déploiement des configurations Google apps StyleBook SSO :

La tâche suivante vous aide à déployer le Microsoft SSO Google Apps StyleBook sur votre réseau d'entreprise.

### Pour déployer l'application Google StyleBook SSO

1. Dans Citrix ADM, accédez à **Applications > Configurations > StyleBooks**. La page StyleBooks affiche tous les StyleBooks disponibles pour votre utilisation dans Citrix ADM. Faites défiler vers le bas et trouvez **SSO Google Apps StyleBook**. Cliquez sur **Créer une configuration**.
2. Le StyleBook s'ouvre sous la forme d'une page d'interface utilisateur sur laquelle vous pouvez entrer les valeurs de tous les paramètres définis dans ce StyleBook.
3. Entrez des valeurs pour les paramètres suivants :
  - a) **Nom de l'application**. Nom de la configuration SSO Google Apps à déployer sur votre réseau.
  - b) **Authentification Adresse IP virtuelle**. Adresse IP virtuelle utilisée par le serveur virtuel AAA auquel la stratégie d'IdP SAML de Google Apps est liée.
  - c) **Expression de règle SAML**. Par défaut, l'expression Citrix ADC Policy (PI) suivante est utilisée : HTTP.REQ.HEADER (« Referer »).CONTAINS (« google »). Mettez à jour ce champ avec une autre expression si votre besoin est différent. Cette expression de stratégie correspond au trafic auquel ces paramètres d'SSO SAML sont appliqués et s'assure que l'en-tête Referer provient d'un domaine Google.
4. La section Paramètres d'Idp SAML vous permet de configurer votre instance Citrix ADC en tant que fournisseur d'identité SAML en créant le profil et la stratégie d'IDP SAML utilisés par le serveur virtuel AAA créé à l'étape 3.
  - a) **Nom de l'émetteur SAML**. Dans ce champ, entrez le nom de domaine complet public de votre serveur virtuel d'authentification. Exemple : `https://<Citrix ADC Auth VIP>/saml/login`
  - b) **ID du fournisseur de services (SP) SAML**. (facultatif) Le fournisseur d'identité Citrix ADC accepte les demandes d'authentification SAML provenant d'un nom d'émetteur qui correspond à cet identifiant.
  - c) **URL du service client Assertion**. Entrez l'URL du fournisseur de services à laquelle le fournisseur d'identité Citrix ADC doit envoyer les assertions SAML après une authentification utilisateur réussie. L'URL du service client d'assertion peut être initiée sur le site serveur du fournisseur d'identité ou sur le site du fournisseur de services.

- d) Vous pouvez saisir d'autres champs facultatifs dans cette section. Par exemple, vous pouvez définir les options suivantes :
- i. Profil de liaison SAML (le profil par défaut est le profil « POST »).
  - ii. Algorithme de signature pour vérifier/signer les demandes/réponses SAML (par défaut est « RSA-SHA1 »).
  - iii. Méthode pour digérer le hachage pour les demandes/réponses SAML (par défaut est « SHA-1 »).
  - iv. Algorithme de chiffrement (AES256 par défaut) et autres paramètres.

**Remarque**

Citrix vous recommande de conserver les paramètres par défaut car ces paramètres ont été testés pour fonctionner avec Google Apps.

- e) Vous pouvez également activer la case à cocher Attributs utilisateur pour entrer les détails de l'utilisateur tels que :
- i. Nom de l'attribut utilisateur
  - ii. Expression Citrix ADC PI évaluée pour extraire la valeur de l'attribut
  - iii. Nom convivial de l'attribut
  - iv. Sélectionnez le format de l'attribut utilisateur.

Ces valeurs sont incluses dans l'assertion SAML émise. Vous pouvez inclure jusqu'à cinq ensembles d'attributs utilisateur dans une assertion émise par Citrix ADC à l'aide de ce StyleBook.

5. Dans la section Paramètres LDAP, entrez les informations suivantes pour authentifier les utilisateurs de Google Apps. Pour que les utilisateurs du domaine puissent se connecter à l'instance Citrix ADC à l'aide de leurs adresses e-mail professionnelles, vous devez configurer les éléments suivants :
- a) **Base LDAP (Active Directory).** Entrez le nom de domaine de base pour le domaine dans lequel les comptes d'utilisateur résident dans Active Directory (AD) pour lequel vous souhaitez autoriser l'authentification. Par exemple, dc=netScaler, dc=com
  - b) **DN de liaison LDAP (Active Directory).** Ajoutez un compte de domaine (à l'aide d'une adresse e-mail pour faciliter la configuration) qui dispose des droits de parcourir l'arborescence AD. Par exemple, CN=Manager, dc=netScaler, dc=com
  - c) **Mot de passe du nom unique de liaison LDAP (Active Directory).** Entrez le mot de passe du compte de domaine pour l'authentification.

- d) Quelques autres champs que vous devez saisir dans cette section sont les suivants :
- i. Adresse IP du serveur LDAP auquel Citrix ADC se connecte pour authentifier les utilisateurs
  - ii. Nom de domaine complet du serveur LDAP

**Remarque**

Vous devez spécifier au moins l'une des deux options ci-dessus : l'adresse IP du serveur LDAP ou le nom de domaine complet.

- iii. Port serveur LDAP auquel Citrix ADC se connecte pour authentifier les utilisateurs (la valeur par défaut est 389).
  - iv. Nom d'hôte LDAP. Ceci est utilisé pour valider le certificat LDAP si la validation est activée (par défaut, il est désactivé).
  - v. Attribut de nom de connexion LDAP. L'attribut par défaut utilisé pour extraire les noms de connexion est « sAMAccountName ».
  - vi. Autres paramètres LDAP divers facultatifs
6. Dans la section Certificat SSL SAML IdP, vous pouvez spécifier les détails du certificat SSL :
- a) **Nom du certificat.** Entrez le nom du certificat SSL.
  - b) **Fichier de certificat.** Choisissez le fichier de certificat SSL dans le répertoire de votre système local ou sur Citrix ADM.
  - c) **Format CertKey.** Sélectionnez le format du certificat et des fichiers de clé privée dans la zone de liste déroulante. Les formats pris en charge sont les extensions de fichier .pem et .der.
  - d) **Nom de la clé de certificat.** Entrez le nom de la clé privée du certificat.
  - e) **Fichier clé du certificat.** Sélectionnez le fichier contenant la clé privée du certificat depuis votre système local ou depuis Citrix ADM.
  - f) **Mot de passe de clé privée.** Si votre fichier de clé privée est protégé par un mot de passe, saisissez-le dans ce champ.
  - g) Vous pouvez également activer la case à cocher Paramètres avancés du certificat pour saisir des détails tels que la période de notification d'expiration du certificat, activer ou désactiver le moniteur d'expiration des certificats.
7. Vous pouvez éventuellement sélectionner le certificat CA SSL IdP si le certificat IDP SAML saisi ci-dessus nécessite l'installation d'un certificat public CA sur Citrix ADC. Assurez-vous de sélectionner « Est un certificat CA » dans les paramètres avancés.

8. Vous pouvez éventuellement sélectionner le certificat SSL SAML SP pour spécifier le certificat SSL Google (clé publique) utilisé pour valider les demandes d'authentification de Google Apps (SAML SP).
9. Cliquez sur **Target Instances** et sélectionnez la ou les instances Citrix ADC sur lesquelles déployer cette configuration SSO Google Apps. Cliquez sur **Créer** pour créer la configuration et déployer la configuration sur les instances Citrix ADC sélectionnées.

#### Remarque

Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter des instances Citrix ADC récemment découvertes dans Citrix ADM à la liste des instances disponibles dans cette fenêtre.

#### Également

##### Conseil

>>

Citrix recommande, avant d'exécuter la configuration proprement dite, de sélectionner **Dry Run** pour confirmer visuellement les objets de configuration créés sur les instances Citrix ADC cibles par le StyleBook.

## SSO Office 365 StyleBook

February 1, 2024

Microsoft™ Office 365 est une suite d'applications de productivité et de collaboration basées sur le cloud fournies par Microsoft sur une base d'abonnement. Il inclut les applications serveur les plus populaires de Microsoft, telles qu'Exchange, SharePoint, Office et Skype for Business. L'authentification unique (SSO) permet aux utilisateurs d'accéder à toutes leurs applications cloud d'entreprise :

- Y compris les administrateurs qui se connectent à la console d'administration
- Connexion unique à tous les services Microsoft Office 365 à l'aide de leurs informations d'identification d'entreprise.

Le StyleBook SSO Office 365 vous permet d'activer l'authentification unique pour Microsoft Office 365 via des instances Citrix ADC. Vous pouvez désormais configurer l'authentification SAML avec Citrix ADC en tant que fournisseur d'identité SAML (IdP) et Microsoft Office 365 en tant que fournisseur de services SAML.

L'activation de l'authentification unique pour Microsoft Office 365 dans une instance Citrix ADC à l'aide de ce StyleBook implique les étapes suivantes :

1. Configuration du serveur virtuel d'authentification
2. Configuration d'une stratégie et d'un profil d'IDP SAML
3. Liaison de la stratégie et du profil au serveur virtuel d'authentification
4. Configuration d'un serveur d'authentification LDAP et d'une stratégie sur l'instance
5. Liez le serveur et la stratégie d'authentification LDAP à votre serveur virtuel d'authentification configuré sur l'instance.

Le tableau répertorie les versions logicielles minimales requises pour que cette intégration fonctionne correctement. Le processus d'intégration devrait également fonctionner avec des versions supérieures de celui-ci.

Produit	Version minimale requise
Citrix ADC	11.0, licence Enterprise/Platinum

Les instructions suivantes supposent que vous avez déjà créé les entrées DNS externes et internes appropriées. Ces entrées sont essentielles pour acheminer les demandes d'authentification vers une adresse IP surveillée par Citrix ADC.

Les instructions suivantes vous aideront à implémenter le StyleBook SSO Office 365 dans votre réseau d'entreprise.

### **Pour déployer le SSO Microsoft Office 365 StyleBook**

1. Dans Citrix Application Delivery Management (ADM), accédez à **Applications > StyleBooks**. La page **StyleBooks** affiche tous les StyleBooks disponibles pour votre utilisation dans Citrix ADM. Faites défiler l'écran vers le bas et trouvez **SSO Office 365 StyleBook**. Cliquez sur **Créer une configuration**.
2. Le StyleBook s'ouvre sous la forme d'une page d'interface utilisateur sur laquelle vous pouvez entrer les valeurs de tous les paramètres définis dans ce StyleBook.
3. Entrez des valeurs pour les paramètres suivants :
  - a) **Nom de l'application**. Nom de la configuration SSO Microsoft Office 365 à déployer sur votre réseau.
  - b) **Authentification Adresse IP virtuelle**. Adresse IP virtuelle à utiliser par le serveur virtuel AAA auquel la stratégie IdP SAML de Microsoft Office 365 est liée.

SSO Office 365 Application Name\*

Office365\_app\_server ?

Authentication Virtual IP address\*

192 . 10 . 10 . 10 ?

4. Dans la section **Paramètres des certificats SSL**, entrez les noms du certificat SSL et la clé de certificat.

**Remarque**

Il ne s'agit pas du certificat de fournisseur de services Office 365. Ce certificat SSL est lié au serveur d'authentification virtuel sur l'instance Citrix ADC.

5. Sélectionnez les fichiers correspondants dans votre dossier de stockage local. Vous pouvez également saisir le mot de passe de clé privée pour charger les clés privées chiffrées au format PEM.

SSL Certificate for the Authentication Virtual IP

---

SSL Certification to be bound to authentication vserver on NetScaler (Not Office 365 Certificate)

Certificate Name\*

office365\_ssl\_test\_cert ?

Certificate File\*

Choose File ▾ test\_cert.pem ?

CertKey Format\*

PEM ▾

Certificate Key Name

office365\_ssl\_test\_cert\_key ?

Certificate Key File

Choose File ▾ test\_cert\_key.pem ?

Private Key Password

Advanced Certificate Settings

6. Vous pouvez également activer la case à cocher **Paramètres de certificat avancés**. Ici, vous pouvez entrer des détails tels que la période de notification d'expiration du certificat, activer ou désactiver le moniteur d'expiration du certificat.
7. Vous pouvez éventuellement cocher la case **Certificat de CA SSL pour l'adresse IP virtuelle d'authentification** si le certificat SSL nécessite l'installation d'un certificat public de l'autorité de certification sur Citrix ADC. Assurez-vous de choisir « Est un certificat CA » dans la section **Paramètres de certificat avancés** ci-dessus.
8. Dans la section **Paramètres LDAP pour SSO Office 365**, entrez les informations suivantes pour authentifier les utilisateurs Office 365. Pour permettre aux utilisateurs du domaine de se connecter à l'instance Citrix ADC à l'aide de leurs adresses e-mail professionnelles, configurez ce qui suit :

- **Base LDAP (Active Directory)**. Entrez le nom de domaine de base du domaine dans lequel les comptes d'utilisateur résident dans Active Directory (AD) pour autoriser l'authentification. Par exemple, dc=netScaler, dc=com
- **DN de liaison LDAP (Active Directory)**. Ajoutez un compte de domaine (à l'aide d'une adresse e-mail pour faciliter la configuration) qui dispose des droits de parcourir l'arborescence AD. Par exemple, CN=Manager, dc=netScaler, dc=com
- **Mot de passe du nom unique de liaison LDAP (Active Directory)**. Entrez le mot de passe du compte de domaine pour l'authentification.
- Quelques autres champs que vous devez saisir dans cette section sont les suivants :
  - Adresse IP du serveur LDAP auquel Citrix ADC se connecte pour authentifier les utilisateurs.
  - Nom de domaine complet du serveur LDAP.

**Remarque**

Vous devez spécifier au moins l'une des deux options ci-dessus : l'adresse IP du serveur LDAP ou le nom de domaine complet.

- Port serveur LDAP auquel Citrix ADC se connecte pour authentifier les utilisateurs (la valeur par défaut est 389). LDAPS utilise 636.
- Nom d'hôte LDAP. Le nom d'hôte est utilisé pour valider le certificat LDAP si la validation est activée (elle est désactivée par défaut).
- Attribut de nom de connexion LDAP. L'attribut par défaut utilisé pour extraire les noms de connexion est « sAMAccountName ».
- Autres paramètres LDAP divers facultatifs.



Active Directory (LDAP) Settings for SSO Office 365

LDAP Settings for SSO Office 365

LDAP (Active Directory) Base\*

 ?

LDAP (Active Directory) Bind DN\*

 ?

LDAP (Active Directory) Bind DN Password\*

 ?

LDAP Server (Active Directory) IP

 ?

LDAP Server FQDN name

 ?

LDAP Server (Active Directory) Port

LDAP Host name

 ?

Active Directory LDAP

Validate LDAP Certificate

LDAP (Active Directory) Login username

9. Dans la section **Certificat IdP SAML**, vous pouvez spécifier les détails des certificats SSL utilisés pour l'assertion SAML.

- **Nom du certificat.** Entrez le nom du certificat SSL.
- **Fichier de certificat.** Choisissez le fichier de certificat SSL dans le répertoire de votre système local.
- **Format CertKey.** Sélectionnez le format du certificat et des fichiers de clé privée dans la

zone de liste déroulante. Les formats pris en charge sont les extensions de fichier .pem et .der.

- **Nom de la clé de certificat.** Entrez le nom de la clé privée du certificat.
- **Fichier clé du certificat.** Sélectionnez le fichier contenant la clé privée du certificat à partir de votre système local.
- **Mot de passe de clé privée.** Entrez le mot de passe qui protège votre fichier de clé privée.

Vous pouvez également activer la case à cocher **Paramètres de certificat avancés**. Ici, vous pouvez entrer des détails tels que la période de notification d'expiration du certificat, activer ou désactiver le moniteur d'expiration du certificat.

### SAML IdP Certificate

SSL Certificate used by NetScaler to sign issued SAML assertions

Certificate Name\*  
 ?

Certificate File\*  
 test\_ssl\_saml\_cert.pem ?

CertKey Format\*

Certificate Key Name  
 ?

Certificate Key File  
 test\_ssl\_saml\_cert\_key.pem ?

Private Key Password

Advanced Certificate Settings

10. Le cas échéant, vous pouvez sélectionner un **certificat d'autorité de certification SAML IdP** si le certificat SAML IdP entré ci-dessus nécessite l'installation d'un certificat public d'autorité de

certification sur Citrix ADC. Assurez-vous de sélectionner **Est un certificat d'autorité de certification** dans la section **Paramètres de certificat avancés** ci-dessus.

11. Dans la section **Certificat SP SAML**, entrez les détails suivants pour le certificat public SSL Office 365. Ce certificat est utilisé par l'instance Citrix ADC pour vérifier les demandes d'authentification SAML entrantes.
  - **Nom du certificat.** Entrez le nom du certificat SSL.
  - **Fichier de certificat.** Choisissez le fichier de certificat SSL dans le répertoire de votre système local.
  - **Format CertKey.** Sélectionnez le format du certificat et des fichiers de clé privée dans la zone de liste déroulante. Les formats pris en charge sont les extensions de fichier .pem et .der.
  - Vous pouvez également activer la case à cocher **Paramètres de certificat avancés**. Ici, vous pouvez entrer des détails tels que la période de notification d'expiration du certificat, activer ou désactiver le moniteur d'expiration du certificat.

SAML SP Certificate

Office365 SSL Public Certificate used by NetScaler to verify incoming SAML authentication requests

Certificate Name\*

office365\_ssl\_saml\_sp\_test\_cert ?

Certificate File\*

Choose File test\_ssl\_saml\_sp\_cert.pem ?

CertKey Format\*

PEM

12. La section **Paramètres d'Idp SAML** vous permet de configurer votre instance Citrix ADC en tant que fournisseur d'identité SAML en créant le profil et la stratégie d'IDP SAML utilisés par le serveur virtuel AAA créé à l'étape 3.
  - **Nom de l'émetteur SAML.** Dans ce champ, saisissez le nom de domaine complet public de votre serveur virtuel d'authentification. Exemple : `https://<Citrix ADC Auth VIP>/saml/login`
  - **Expression d'identifiant de nom.** Tapez l'expression Citrix ADC qui est évaluée pour extraire le NameIdentifier SAML envoyé dans l'assertion SAML. Exemple : `"HTTP.REQ.USER.ATTRIBUTE(2).B64ENCODE"`
  - **Algorithme de signature :** sélectionnez l'algorithme pour vérifier/signer les requêtes/réponses SAML (la valeur par défaut est « RSA-SHA256 »).
  - **Méthode de digestion.** Sélectionnez la méthode de digestion du hachage pour les requêtes/réponses SAML (la valeur par défaut est « SHA256 »).

- **Nom du public.** Entrez le nom de l'entité ou l'URL qui représente le fournisseur de services (Microsoft Office 365).
- **ID du fournisseur de services (SP) SAML.** (facultatif) Le fournisseur d'identité Citrix ADC accepte les demandes d'authentification SAML provenant d'un nom d'émetteur qui correspond à cet identifiant.
- **URL du service client Assertion.** Entrez l'URL du fournisseur de services à laquelle le fournisseur d'identité Citrix ADC doit envoyer les assertions SAML après une authentification utilisateur réussie. L'URL du service client d'assertion peut être initiée sur le site serveur du fournisseur d'identité ou sur le site du fournisseur de services.
- Vous pouvez saisir d'autres champs facultatifs dans cette section. Par exemple, vous pouvez définir les options suivantes :
  - **Nom de l'attribut SAML.** Nom de l'attribut utilisateur envoyé dans l'assertion SAML.
  - **Nom convivial de l'attribut SAML.** Nom convivial de l'attribut utilisateur envoyé dans l'assertion SAML.
  - **Expression IP pour l'attribut SAML.** Par défaut, l'expression de stratégie (PI) Citrix ADC suivante est utilisée : HTTP.REQ.USER.ATTRIBUTE (1). Ce champ spécifie le premier attribut utilisateur envoyé par le serveur LDAP (mail) en tant qu'attribut d'authentification SAML.
  - Sélectionnez le format de l'attribut utilisateur.

Ces valeurs sont incluses dans l'assertion SAML émise.

#### Conseil

Citrix vous recommande de conserver les paramètres par défaut, car ces paramètres ont été testés pour fonctionner avec les applications Microsoft Office 365.

Saml issuer name

Name Identifier Expression  
 ?

Signature Algorithm  
 ?

Digest Method

Audience name or url

Option to Reject unsigned SAML Requests

SAML Attribute Name

SAML Attribute Friendly Name

PI Expression for SAML Attribute

SAML Attribute Format  
 ?

13. Cliquez sur **Instances cibles** et sélectionnez la ou les instances Citrix ADC sur lesquelles déployer cette configuration Microsoft Office 365 SSO. Cliquez sur **Créer** pour créer la configuration et déployer la configuration sur les instances Citrix ADC sélectionnées.

### Target Instances

 > + ?

#### Conseil

Citrix recommande qu'avant d'exécuter la configuration réelle, vous sélectionnez **Exécuter à sec** pour afficher les objets de configuration créés sur les instances Citrix ADC cibles par le StyleBook.

## StyleBook Microsoft Skype for Business

February 1, 2024

L'application Skype for Business 2015 s'appuie sur plusieurs composants externes pour fonctionner. Le réseau Skype for Business comprend divers systèmes, tels que les serveurs et leurs systèmes d'exploitation, les bases de données, les systèmes d'authentification et d'autorisation, les systèmes et infrastructures de réseau et les systèmes PBX téléphoniques. Skype for Business Server 2015 est disponible en deux versions, Standard Edition et Enterprise Edition. La principale différence réside dans la prise en charge des fonctionnalités de haute disponibilité qui ne sont incluses que dans l'édition Enterprise. Pour mettre en œuvre la haute disponibilité, plusieurs serveurs frontaux doivent être déployés dans un pool et les serveurs SQL doivent être mis en miroir.

Un déploiement Enterprise Edition permet de créer plusieurs serveurs avec des rôles différents.

### Composants principaux

Les principaux composants de l'application Skype for Business 2015 sont les suivants :

- Serveurs frontaux
- Serveurs Edge
- Serveurs Director
- Serveurs de base de données (SQL)

## Serveurs frontaux

Dans l'application Skype for Business, le serveur frontal est le serveur principal de votre réseau. Il fournit des liens et des services pour l'authentification des utilisateurs, l'enregistrement, la présence, le carnet d'adresses, les conférences audiovisuelles, le partage d'applications, la messagerie instantanée et les conférences Web. Si vous déployez Skype for Business 2015 édition Entreprise, la topologie consiste généralement en au moins deux serveurs frontaux équilibrés de charge dans un pool front-end avec un serveur de base de données qui héberge l'instance SQL Server contenant la base de données Skype for Business.

## Serveurs Edge

Le déploiement de serveurs Edge pour Skype for Business est nécessaire si les utilisateurs externes qui ne sont pas connectés au réseau interne de votre organisation doivent pouvoir interagir avec les utilisateurs internes. Ces utilisateurs externes peuvent être des utilisateurs distants authentifiés et anonymes, des partenaires fédérés ou d'autres clients mobiles.

Il existe quatre types de rôles dans le serveur Skype For Business Edge :

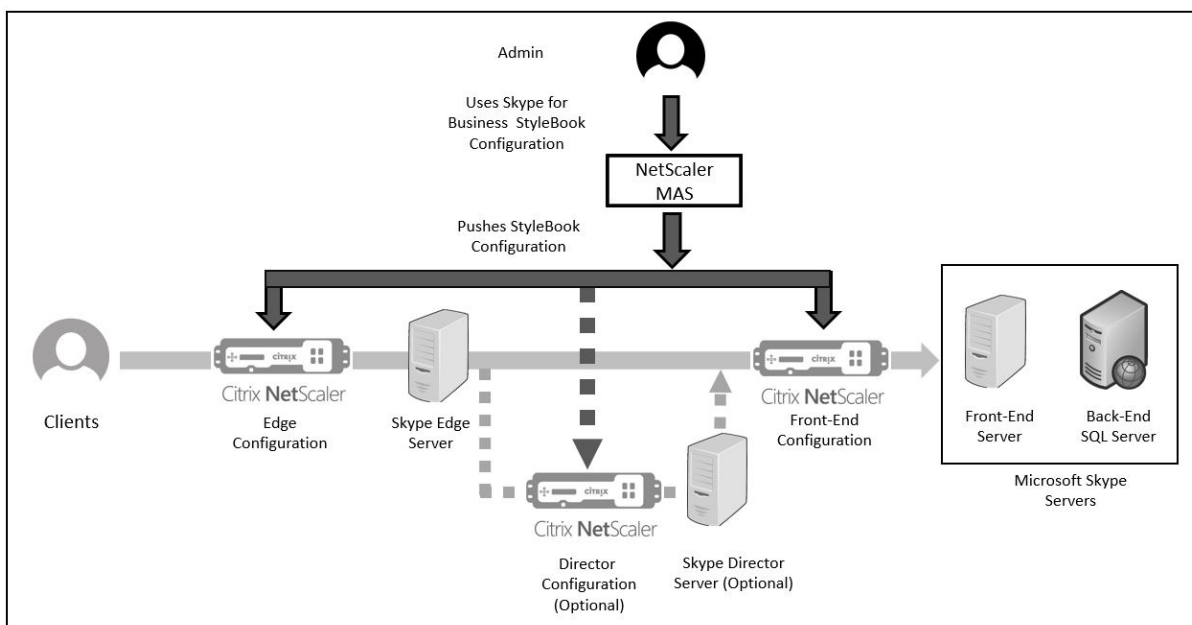
- Access Edge, qui gère le trafic SIP et authentifie les connexions externes, permet la connexion à distance et permet la connexion de fédération
- Web Conferencing, qui gère les paquets de conférence de données et permet aux utilisateurs externes d'accéder à Skype for Business
- A/V Conferencing, qui gère les paquets de conférence audio/vidéo et étend l'audio et la vidéo, le partage d'applications et le transfert de fichiers aux utilisateurs externes
- XMPP Proxy, qui gère les paquets XMPP, et permet aux serveurs ou clients basés sur XMPP de se connecter à Skype for Business.

## Serveurs Director

La fonction principale du serveur Director dans Skype for Business 2015 est d'authentifier les points de terminaison et de « diriger » les utilisateurs vers le pool qui contient leur compte. Dans Skype for Business 2015, bien que le Director soit un rôle entièrement dédié et spécifique sur un serveur autonome, il s'agit d'un serveur facultatif. Cela facilite la sécurité en facilitant le déploiement ou la suppression des configurations.

Les directeurs sont particulièrement utiles lorsqu'il existe plusieurs pools, car ils fournissent un point de contact unique pour authentifier les points de terminaison. De plus, pour les utilisateurs distants, un Director sert de saut supplémentaire entre le pool Edge et le pool Front-End, ajoutant ainsi une couche de protection supplémentaire contre les attaques.

La figure suivante représente schématiquement le déploiement des serveurs Skype dans le réseau :



### Configuration d’instances Citrix ADC dans une entreprise

Le tableau suivant répertorie les adresses IP utilisées dans l’exemple de configuration inclus dans les instructions ci-dessous :

Serveurs Skype for Business			
	Adresse IP virtuelle	Adresses IP du serveur	Instance Citrix ADC
Serveurs Edge	VIP externe -	192.20.20.21 ;	10.102.29.141
	192.20.20.20	192.20.20.22	
	VIP interne -	10.10.10.21;	
	10.10.10.20	10.10.10.22	
Serveurs frontaux	10.10.10.10	10.10.10.11 ;	10.102.29.60
		10.10.10.12	
Serveur Director	10.10.10.30	10.10.10.31;	10.102.29.93
		10.10.10.32	

#### Pour configurer des serveurs frontaux

1. Dans Citrix Application Delivery Management (ADM), accédez à **Applications > Configuration**, puis cliquez sur **Create New**. La page **Choisir un StyleBook** affiche tous les StyleBooks disponibles pour votre utilisation dans Citrix ADM. Faites défiler l’écran vers le bas et sélectionnez **Microsoft Skype for Business 2015 StyleBook**. Le StyleBook s’ouvre en tant que page d’



interface utilisateur sur laquelle vous pouvez entrer les valeurs de tous les paramètres définis dans ce StyleBook.

2. Dans la section **Serveur Edge**, entrez les adresses IP virtuelles (VIP) et les adresses IP de tous les serveurs Edge du réseau suivantes.
  - a) Adresse VIP externe et adresses IP des serveurs Edge qui seront utilisés pour Access Edge, les conférences Web Edge et A/V Edge.
  - b) Adresse VIP interne et adresses IP des serveurs Edge qui seront connectés au réseau interne.
  - c) Deux serveurs Edge externes et deux serveurs internes sur votre réseau.
3. Dans la section **Serveur frontal**, entrez l'adresse IP du serveur frontal virtuel (VIP) qui doit être créé pour les serveurs front-end Skype for Business. Entrez également les adresses IP de tous les serveurs d'interface Skype for Business du réseau.
4. Dans la section **Director Server**, entrez l'adresse IP virtuelle (VIP) des serveurs Director à créer pour l'application Skype for Business. Entrez également les adresses IP de tous les serveurs Skype for Business Director du réseau. Créez au moins deux serveurs Director pour une haute disponibilité.
5. La section **Paramètres avancés** répertorie tous les ports par défaut configurés sur les instances Citrix ADC pour les trois serveurs Skype.

Le tableau suivant fournit une liste de tous les ports et protocoles par défaut :

Label	Port	Protocole	Description
Port HTTP	80	HTTP	Utilisé pour la communication entre les serveurs frontaux et les noms de domaine complets de la ferme Web lorsque le protocole HTTPS n'est pas utilisé.
Port HTTPS	443	HTTPS	Utilisé pour la communication entre les serveurs frontaux et les noms de domaine complets de la batterie Web.

---

Label	Port	Protocole	Description
Port interne AutoDiscover	4443	HTTPS	Communications inter-pool HTTPS (à partir du proxy inverse) et HTTPS Front-end pour la connexion AutoDiscover.
Port RPC	135	DCOM et appel de procédure à distance (RPC)	Utilisé pour les opérations basées sur DCOM telles que le déplacement d'utilisateurs, la synchronisation des réplicateurs d'utilisateurs et la synchronisation du carnet d'adresses.
Port SIP	5061	TCP (TLS)	Utilisé par les serveurs frontaux pour toutes les communications SIP internes.
Port de focus SIP	444	HTTPS, TCP	Utilisé pour la communication HTTPS entre le Focus (le composant qui gère l'état de la conférence Skype) et les serveurs individuels.
Port de groupe SIP	5071	TCP	Utilisé pour les demandes SIP entrantes pour l'application du groupe de réponse.
Port de partage d'applications SIP	5065	TCP	Utilisé pour les demandes d'écoute SIP entrantes pour le partage d'applications.

---

Label	Port	Protocole	Description
Port auxiliaire SIP	5072	TCP	Utilisé pour les demandes SIP entrantes pour le préposé (c'est-à-dire pour la conférence d'accès à distance).
Port d'annonce SIP Conf	5073	TCP	Utilisé pour les demandes SIP entrantes pour le service d'annonce de conférence sur le serveur Skype for Business (c'est-à-dire pour les téléconférences).
Port SIP CallPark	5075	TCP	Utilisé pour les requêtes SIP entrantes pour l'application CallPark.
Port d'admission d'appels SIP	448	TCP	Utilisé pour le contrôle d'admission des appels par le service de stratégie de bande passante du serveur Skype for Business.
Port TURN d'admission d'appel SIP	5080	TCP	Utilisé pour le contrôle d'admission des appels par le service de stratégie de bande passante pour le trafic Audio/Video Edge TURN.
Port de test audio SIP	5076	TCP	Utilisé pour les demandes SIP entrantes pour le service de test audio.

Label	Port	Protocole	Description
Port externe HTTPS	443	HTTPS	Utilisé pour les ports externes pour la communication SIP/TLS pour l'accès utilisateur à distance, l'accès à des conférences Web internes, et les communications multimédia STUN/TCP entrantes et sortantes pour accéder aux médias internes et aux sessions A/V.
Port interne HTTPS	443	HTTPS	Utilisé pour les ports internes pour la communication SIP/TLS pour l'accès utilisateur à distance, l'accès à des conférences Web internes, et les communications multimédia STUN/TCP entrantes et sortantes pour accéder aux médias internes et aux sessions A/V.
Port d'accès distant externe SIP	5061	TCP	Utilisé pour les ports externes pour la communication SIP/MTLS pour l'accès utilisateur à distance ou la fédération.

Label	Port	Protocole	Description
Port d'accès à distance interne SIP	5061	TCP	Utilisé pour les ports internes pour la communication SIP/MTLS pour l'accès utilisateur à distance ou la fédération.
Port UDP STUN externe SIP	3478	UDP	Utilisé pour les ports externes pour les communications multimédia entrantes et sortantes STUN/UDP.
Port UDP STUN interne SIP	3478	UDP	Utilisé pour les ports internes pour les communications multimédia entrantes et sortantes STUN/UDP.
Port de messagerie instantanée interne SIP	5062		Utilisé pour les ports internes pour l'authentification SIP/MTLS des communications de messagerie instantanée sortant via le pare-feu interne.
Port HTTP	80	TCP	Utilisé pour la communication initiale entre les directeurs et les FQDN de la ferme Web.
Port HTTPS	443	HTTPS	Utilisé pour la communication entre les directeurs et les noms de domaine complets de la batterie de serveurs Web.

Label	Port	Protocole	Description
Port interne AutoDiscover	4443	HTTPS	Utilisé pour les communications entre pools HTTPS (à partir de Reverse Proxy) et HTTPS Director pour la connexion AutoDiscover.
Port interne SIP	5061	TCP	Utilisé pour les communications internes entre les serveurs et pour les connexions client.

6. Dans la section **Instances cibles**, sélectionnez les trois instances Citrix ADC différentes sur lesquelles déployer les trois serveurs Skype for Business.

**Remarque**

Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter des instances Citrix ADC récemment découvertes dans Citrix ADM à la liste des instances disponibles dans cette fenêtre.

7. Cliquez sur **Créer** pour créer la configuration sur les instances Citrix ADC sélectionnées.

**Conseil**

Citrix vous recommande de sélectionner **Dry Run** pour vérifier les objets de configuration qui doivent être créés sur l'instance cible avant d'exécuter la configuration réelle sur l'instance.

Lorsque la configuration est créée avec succès, le StyleBook crée 25 serveurs virtuels d'équilibrage de charge. En d'autres termes, pour chaque port, un serveur virtuel d'équilibrage de charge est défini avec un groupe de services, et le groupe de services est lié au serveur virtuel d'équilibrage de charge. La configuration ajoute également les serveurs frontaux en tant que membres du groupe de services et les lie au groupe de services. Le nombre de membres du groupe de services créés est égal au nombre de serveurs frontaux créés.

La figure suivante montre les objets créés sur chaque serveur :

Objects Added on Instance : 10.102.29.93   Roles : frontend   Count : 72	Objects Added on Instance : 10.102.29.140   Roles : director   Count : 22	Objects Added on Instance : 10.102.29.60   Roles : edge   Count : 35
<p><b>Type : lbvserver</b>                      appflowlog : ENABLED                      downstateflush : ENABLED                      ipv46 : 10.10.10.10                      lbmethod : LEASTCONNECTION                      name : microsoft-skype-application-sfb-fe-http-lb                      persistencytype : SOURCEIP                      port : 80                      servicetype : TCP</p>	<p><b>Type : lbvserver</b>                      appflowlog : ENABLED                      downstateflush : ENABLED                      ipv46 : 10.10.10.30                      lbmethod : LEASTCONNECTION                      name : microsoft-skype-application-sfb-dir-http-lb                      persistencytype : SOURCEIP                      port : 80                      servicetype : TCP</p>	<p><b>Type : lbvserver</b>                      ipv46 : 192.20.20.20                      name : microsoft-skype-application-sfb-edge-externalsip-lb                      port : 443                      servicetype : TCP</p>
<p><b>Type : servicegroup</b>                      servicegroupname : microsoft-skype-application-sfb-fe-http-svcgrp                      servicetype : TCP</p>	<p><b>Type : servicegroup</b>                      servicegroupname : microsoft-skype-application-sfb-dir-http-svcgrp                      servicetype : TCP</p>	<p><b>Type : servicegroup</b>                      servicegroupname : microsoft-skype-application-sfb-edge-externalsip-svcgrp                      servicetype : TCP</p>
<p><b>Type : lbvserver_servicegroup_binding</b>                      name : microsoft-skype-application-sfb-fe-http-lb                      servicegroupname : microsoft-skype-application-sfb-fe-http-svcgrp</p>	<p><b>Type : lbvserver_servicegroup_binding</b>                      name : microsoft-skype-application-sfb-dir-http-lb                      servicegroupname : microsoft-skype-application-sfb-dir-http-svcgrp</p>	<p><b>Type : lbvserver_servicegroup_binding</b>                      name : microsoft-skype-application-sfb-edge-externalsip-lb                      servicegroupname : microsoft-skype-application-sfb-edge-externalsip-svcgrp</p>
<p><b>Type : server</b>                      ipaddress : 10.10.10.11                      name : 10.10.10.11</p>	<p><b>Type : server</b>                      ipaddress : 10.10.10.31                      name : 10.10.10.31</p>	<p><b>Type : server</b>                      ipaddress : 192.20.20.21                      name : 192.20.20.21</p>
		<p><b>Type : server</b>                      ipaddress : 192.20.20.22</p>

## StyleBook Microsoft Exchange

February 1, 2024

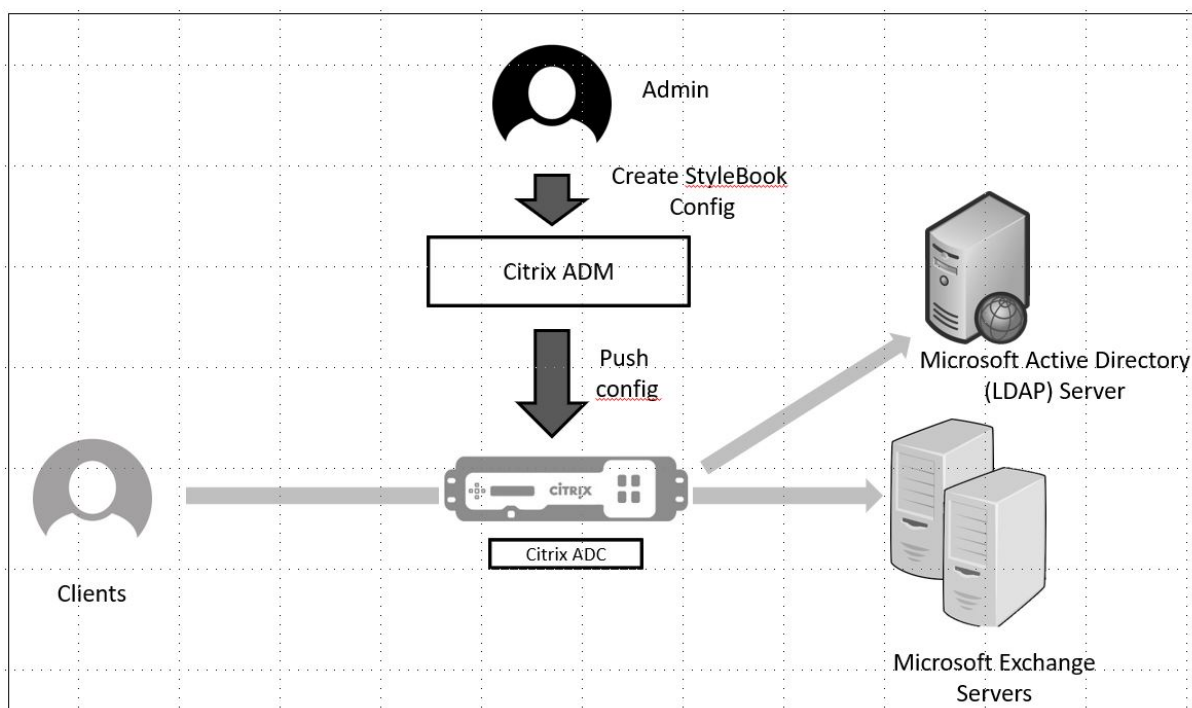
Vous pouvez utiliser le StyleBook de Microsoft Exchange 2016 pour déployer une configuration Citrix ADC qui optimise et sécurise une application d'entreprise Microsoft Exchange 2016 sur votre réseau. Microsoft Exchange 2016 est une application d'entreprise clé pour fournir des services de messagerie, de gestion des informations personnelles et de messagerie à vos employés et aux autres parties prenantes.

### Fonctionnalités de Citrix ADC configurées à l'aide de Microsoft Exchange StyleBook

Le Microsoft Exchange 2016 StyleBook active et configure les fonctionnalités Citrix ADC suivantes pour les serveurs Microsoft Exchange 2016 :

- Équilibrage de charge : équilibrage de charge de base qui permet l'équilibrage de charge de plusieurs serveurs Exchange
- Commutation de contenu : commutation de contenu qui permet un accès IP unique et la redirection des requêtes vers les serveurs virtuels d'équilibrage de charge appropriés
- Réécriture : redirige les utilisateurs vers des pages sécurisées
- Déchargement SSL : décharge le traitement SSL vers Citrix ADC, réduisant ainsi la charge sur le serveur Exchange

La figure suivante représente schématiquement le déploiement des serveurs Exchange dans le réseau :



## Conditions préalables

- Pour l'authentification basée sur des certificats, tous les hôtes adressables faisant partie de la configuration réseau doivent avoir des noms de domaine résolubles et pas uniquement des adresses IP.
- Assurez-vous que les ports SIP sont accessibles sur le serveur Microsoft Exchange 2016.

## Configuration du StyleBook de Microsoft Exchange

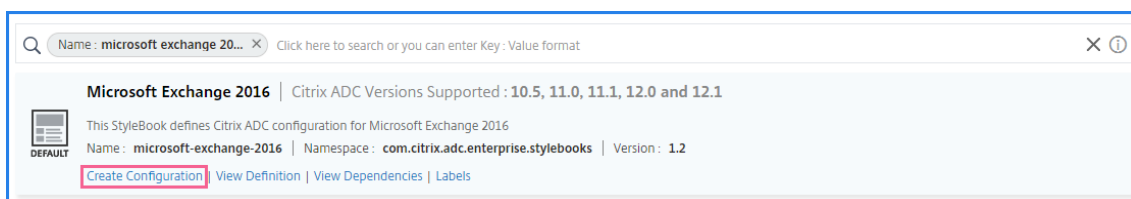
Configurez le Microsoft Exchange StyleBook dans votre entreprise pour déployer la configuration Citrix ADC.

### Pour configurer l'application Microsoft Exchange

1. Dans Citrix ADM, accédez à **Applications > StyleBooks**.
2. Recherchez **Microsoft Exchange 2016 StyleBook** et cliquez sur **Créer une configuration**.

Le StyleBook apparaît sous la forme d'un formulaire d'interface utilisateur sur lequel vous pouvez saisir les valeurs de tous les paramètres définis dans ce StyleBook.





3. Entrez les détails des paramètres suivants :

- **Nom de l'application Exchange** : nom de l'application Microsoft Exchange dans votre réseau
- **Exchange VIP** : adresse IP virtuelle sur Citrix ADC qui reçoit les demandes des clients pour l'application Microsoft Exchange
- **IP Exchange Server** : adresses IP de tous les serveurs Exchange du réseau.

Si vous souhaitez ajouter d'autres adresses IP, cliquez sur l'icône plus (+). Habituellement, deux serveurs Exchange sont configurés dans le réseau.

4. Dans la section **Certificats Exchange**, téléchargez les certificats Exchange vers Citrix ADM. Entrez les noms du certificat et des fichiers clés et téléchargez-les depuis le stockage local. Vous pouvez également fournir un mot de passe de clé privée pour crypter le fichier clé.

#### Remarque

Assurez-vous que les fichiers de certificat sont au format « .pem » ou « .der ». Citrix ADM rejette les fichiers d'autres formats.

Si vous souhaitez spécifier les détails d'expiration du certificat ou tout autre paramètre avancé, sélectionnez **Paramètres de certificat avancés**.

5. Dans la section de **configuration de l'authentification Active Directory Exchange**, configurez les paramètres AD en entrant les données.

- **Active Directory Authentication VIP** : adresse IP virtuelle utilisée pour créer et configurer le serveur virtuel AD (LDAP) sur une appliance Citrix ADC.
- **Active Directory Server IP** - Adresse IP de votre Controller de domaine Active Directory.
- **Chaîne de base Active Directory** : chaîne de base LDAP dans Active Directory. Par exemple, CN = Utilisateurs, DC=CTXNSSFB, DC=COM.
- **Nom distinctif (DN) Active Directory LDAP Bind** : le nom distinctif (DN) LDAP Bind est utilisé pour lier cet objet au serveur LDAP (AD). Par exemple « CN = Administrateur, CN = Utilisateurs, dc=acme, dc=com »
- **Mot de passe LDAP Bind Distinguished Name (DN) Active Directory** : le nom distinctif LDAP Bind (DN) est le mot de passe pour l'authentification AD

- **Attribut de nom d'utilisateur Active Directory : attribut** AD pour le nom d'utilisateur. Le Citrix ADC utilise l'attribut LDAP pour interroger les serveurs Active Directory externes. Par exemple, « SAMAccountName »
  - **Nom d'attribut du groupe Active Directory** : noms d'attributs du groupe LDAP configurés sur le serveur LDAP. Par exemple, « MemberOf » pour l'attribut de groupe dans LDAP.
  - **Nom de sous-attribut Active Directory** : noms de sous-attribut LDAP configurés sur le serveur LDAP. Par exemple, « cn » pour le sous-attribut dans LDAP.
  - **Domaine d'authentification Active Directory** : nom de domaine AD/LDAP utilisé pour l'authentification. Par exemple, ctxnssf.com.
6. Dans la section **Instances cibles**, sélectionnez l'instance Citrix ADC sur laquelle déployer cette configuration Exchange.

#### Remarque

Si vous souhaitez afficher les instances Citrix ADC récemment découvertes, cliquez sur l'icône d'actualisation.

7. Cliquez sur **Créer** pour créer le fichier de configuration et exécuter la configuration sur l'instance Citrix ADC sélectionnée.

Citrix vous recommande de sélectionner d'abord **Exécuter à sec** pour vérifier les objets de configuration créés sur l'instance cible avant d'exécuter la configuration réelle sur l'instance.

Lorsque la configuration a été créée avec succès, StyleBook a créé un serveur virtuel de commutation de contenu, cinq serveurs virtuels d'équilibrage de charge et une stratégie LDAP liée à un serveur virtuel d'authentification LDAP. En outre, les groupes de services correspondants sont créés et liés aux serveurs virtuels d'équilibrage de charge.

## Microsoft SharePoint StyleBook

February 1, 2024

Microsoft SharePoint 2016 est une application d'entreprise clé qui fournit principalement un système de gestion et de stockage de documents, hautement configurable et pris en charge par tous les principaux navigateurs.

Vous pouvez utiliser le StyleBook de Microsoft SharePoint 2016 pour déployer une configuration Citrix ADC qui optimise et sécurise l'application d'entreprise Microsoft SharePoint 2016 sur votre réseau.

## Conditions préalables

- Microsoft SharePoint 2016
- Citrix ADM, version 12.0 et versions ultérieures
- Citrix ADC, version 10.5 et ultérieure

## Fonctionnalités de Citrix ADC configurées par le StyleBook de Microsoft SharePoint 2016

Vous pouvez utiliser le StyleBook de Microsoft SharePoint 2016 pour activer et configurer les fonctionnalités Citrix ADC suivantes pour Microsoft SharePoint 2016 :

- Équilibrage de charge
- Commutation de contenu
- Répondeur
- Réécriture
- Compression
- Mise en cache intégrée

### Équilibrage de charge

L'équilibrage de charge Citrix ADC répartit uniformément les demandes vers les serveurs SharePoint principaux. La surveillance intelligente des serveurs dorsaux empêche l'envoi de demandes vers des serveurs défectueux.

Le StyleBook de SharePoint configure 12 serveurs virtuels d'équilibrage de charge, chacun dédié aux demandes d'équilibrage de charge pour un certain type de contenu, tel que des documents, des images, des fichiers audio, vidéo et d'autres types de fichiers.

Le SharePoint StyleBook prend désormais en charge le mode SSL de l'application SharePoint en configurant des serveurs virtuels LB basés sur SSL. Assurez-vous que SSL est sélectionné comme protocole frontal. Notez que le port virtuel est défini sur 443 par défaut. Vous pouvez également sélectionner SSL pour lier des groupes de services (serveurs d'applications SharePoint) aux serveurs virtuels d'équilibrage de charge cibles. Notez que le protocole principal est défini par défaut sur HTTP.

### Commutation de contenu

La fonctionnalité de commutation de contenu est utilisée pour distribuer les demandes des clients sur plusieurs serveurs virtuels d'équilibrage de charge sur la base de types spécifiques de contenu SharePoint demandé (par exemple, des documents, des images et des fichiers audio ou vidéo). Le module de commutation de contenu dirige le trafic entrant vers un serveur virtuel d'équilibrage de

charge optimal capable de traiter ce type de contenu. Vous pouvez donc appliquer différentes stratégies d'optimisation à différents types de trafic. Par exemple, vous souhaitez peut-être utiliser des stratégies de compression ou de mise en cache différentes pour les vidéos et pour les documents texte.

### **Répondeur**

La fonctionnalité de répondeur d'une instance Citrix ADC peut être utilisée pour rediriger facilement les utilisateurs du protocole HTTP vers le protocole HTTPS. Le répondeur peut également être configuré pour fournir des pages d'erreur personnalisées. La stratégie Responder détermine les demandes (trafic) sur lesquelles une action doit être entreprise et lie chaque stratégie à un serveur virtuel d'équilibrage de charge. Le SharePoint StyleBook inclut une configuration qui redirige les utilisateurs des URL HTTP vers les URL HTTPS.

### **Réécrire**

Le module de réécriture est utilisé pour modifier les en-têtes de demande/réponse, les URL ou le contenu à la volée. Ce module fonctionne en ligne avec le traitement du trafic et peut donc modifier le flux de trafic en fonction de cas d'utilisation particuliers. Par exemple, la réécriture peut donner accès au contenu demandé sans révéler de détails inutiles sur le serveur du site Web.

Dans le StyleBook de SharePoint, la fonction de réécriture est utilisée pour supprimer les en-têtes inutiles des demandes des utilisateurs.

### **Compression**

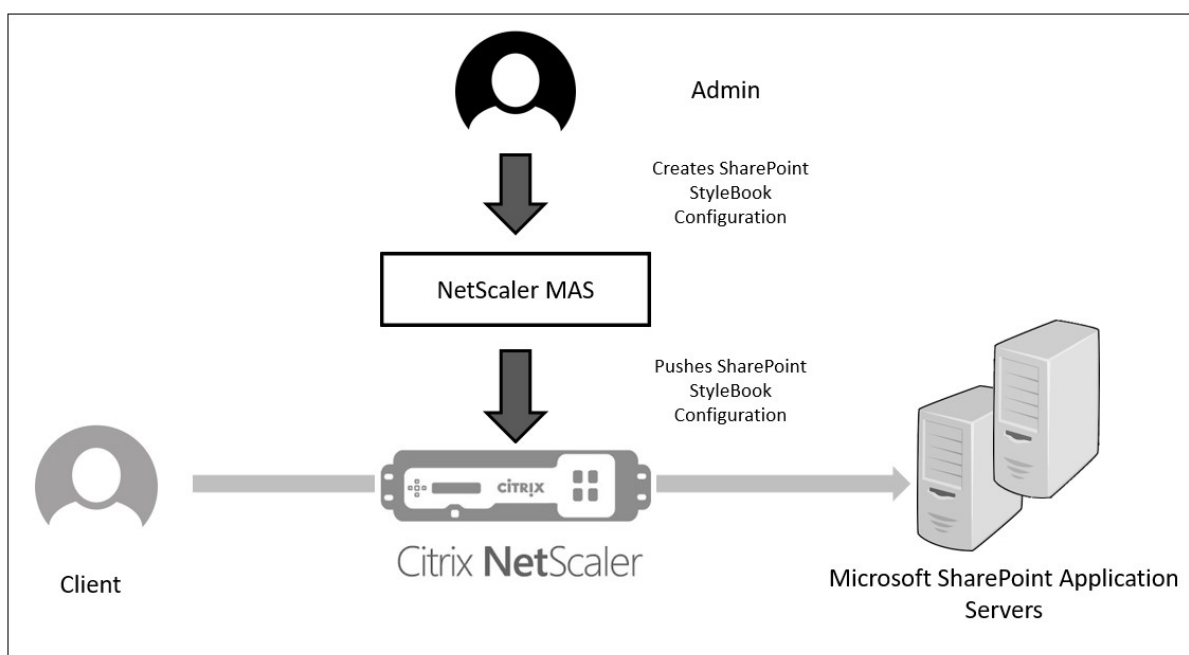
Le moteur de compression Citrix ADC identifie et compresse le contenu compressible. Ce processus améliore le temps de transmission des données et réduit les besoins en bande passante réseau des clients, tout en économisant des cycles de processeur sur les serveurs de contenu SharePoint. Une instance Citrix ADC peut compresser à la fois des données statiques et des données générées dynamiquement. Il applique l'algorithme de compression GZIP ou DEFLATE pour supprimer les informations superflues et répétitives des réponses du serveur et représenter les informations d'origine dans un format plus compact et efficace. La capacité du navigateur client à décompresser les données dépend de l'algorithme ou des algorithmes qu'il prend en charge : GZIP, DEFLATE ou les deux.

Une instance Citrix ADC est configurée pour compresser le texte dans des documents HTML, XML, texte brut, feuille de style en cascade (CSS) et Microsoft Office, mais ne compresse pas les images au format GIF ou JPG. Les principaux avantages du trafic compressé incluent la réduction des coûts de bande passante, la réduction de la latence du WAN et de meilleures performances des serveurs

## Mise en cache intégrée

Le cache en mémoire Citrix ADC peut stocker des objets SharePoint afin de fournir rapidement le contenu fréquemment demandé aux utilisateurs. Le contenu mis en cache inclut les documents téléchargés et les fichiers audio, vidéo et image.

La figure suivante représente schématiquement le déploiement de serveurs SharePoint dans un réseau frontal par une instance Citrix ADC sur laquelle Citrix ADM est utilisé pour déployer une configuration SharePoint StyleBook.



## Déploiement de configurations SharePoint StyleBook

La tâche suivante vous aidera à déployer le StyleBook Microsoft SharePoint 2016 sur votre réseau professionnel.

### Pour déployer Microsoft SharePoint 2016 StyleBook :

1. Dans Citrix ADM, accédez à **Applications > Administration > Configuration**, puis cliquez sur **Créer un nouveau**.  
La page **Choisir un StyleBook** affiche tous les StyleBooks disponibles pour votre utilisation dans Citrix ADM.
2. Faites défiler l'écran vers le bas et sélectionnez **Microsoft SharePoint 2016 StyleBook**.

### Remarque

Dans Citrix ADM, accédez à **Applications > Configurations > StyleBooks**. Faites défiler vers le bas pour trouver le **StyleBook de Microsoft SharePoint 2016**, puis cliquez sur **Créer une configuration**.

Le StyleBook s'ouvre en tant que formulaire d'interface utilisateur sur lequel vous pouvez entrer les valeurs de tous les paramètres définis dans ce StyleBook.

Entrez des valeurs pour les paramètres suivants :

- a) **Nom de l'application SharePoint.** Nom de la configuration SharePoint à déployer sur votre réseau.
- b) **Adresse IP virtuelle SharePoint.** Adresse IP virtuelle à laquelle l'instance Citrix ADC reçoit les demandes des clients pour l'application Microsoft SharePoint.
- c) **Port virtuel SharePoint.** Le port TCP à utiliser par les utilisateurs pour accéder à l'application SharePoint
- d) **Protocole frontend SharePoint.** Sélectionnez le protocole d'interface SharePoint dans la liste déroulante. Les options disponibles sont HTTP ou SSL.

### Remarque

Si vous sélectionnez SSL, assurez-vous que le paramètre de configuration de réécriture est activé dans la section Paramètres avancés de SharePoint de ce StyleBook.

- e) **Adresses IP des serveurs SharePoint.** Adresses IP de tous les serveurs SharePoint du réseau.
- f) **Port des serveurs SharePoint.** Numéro de port TCP utilisé par les serveurs SharePoint. Par défaut, il s'agit de 80. Vous pouvez modifier cette valeur si nécessaire, mais assurez-vous que ce port est accessible sur les serveurs Microsoft SharePoint 2016.

SharePoint Application Name\*  
 ?

SharePoint Virtual VIP\*  
 ?

Sharepoint Virtual Port

Sharepoint frontend Protocol  
 ▾

Sharepoint Servers IPs\*  
 ×  
 × + ?

Sharepoint Servers Port

3. Dans la section **Paramètres des certificats SSL**, cliquez sur + pour entrer le nom du certificat SSL, la clé de certificat, et sélectionnez les fichiers respectifs dans votre dossier de stockage local.

Certificate Name\*  
 ?

Certificate File\*  
 test\_cert.pem ?

CertKey Format\*  
 ▾

Certificate Key Name  
 ?

Certificate Key File  
 test\_cert\_key.pem ?

Private Key Password

**Advanced Certificate Settings**

4. Vous pouvez également cliquer sur **Paramètres de certificat avancés** pour activer ou désactiver la surveillance de l'expiration des certificats SSL. Si vous activez la surveillance de l'expiration des certificats, définissez le nombre de jours afin que Citrix ADM émette une alarme après ces nombreux jours pendant lesquels le certificat est sur le point d'expirer. Vous avez également la possibilité de vérifier l'OCSP en tant que fonctionnalité facultative ou obligatoire.

**Advanced Certificate Settings**

Advanced certificate settings

Certificate Expiry Monitor  
 ▾ ?

Certificate Expiry Notification Period  
 ?

Is a CA Certificate

Skip CA Name

OCSP Check  
 ▾ ?

SNI Certificate



5. La section **Paramètres avancés** de SharePoint vous permet d'activer les fonctionnalités de Citrix ADC qui seront configurées sur les instances de Citrix ADC. Bien que les fonctionnalités d'équilibrage de charge et de commutation de contenu soient configurées sur les instances par défaut, vous pouvez choisir les autres fonctionnalités, à savoir la configuration du répondeur, la configuration de réécriture, la configuration de compression et la configuration de mise en cache intégrée, que vous souhaitez configurer sur l'instance.
6. Cliquez sur **Target Instances** et sélectionnez l'instance Citrix ADC sur laquelle déployer cette configuration SharePoint. Cliquez sur **Créer** pour créer la configuration et déployer la configuration sur l'instance Citrix ADC sélectionnée.

**Remarque**

Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter des instances Citrix ADC récemment découvertes dans Citrix ADM à la liste des instances disponibles dans cette fenêtre.

**Sharepoint Advanced Settings**

Options to selectively enable configurations of features for Sharepoint

- Enable Responder Configuration
- Enable Rewrite Configuration
- Enable Compression Configuration
- Enable Caching Configuration

**Target Instances**

>

+

Create

Close

Dry Run

**Remarque**

Citrix recommande, avant d'exécuter la configuration proprement dite, de sélectionner **Dry Run** pour vérifier les objets de configuration qui seront créés sur l'instance cible.

Lorsque la configuration est créée et déployée avec succès, le StyleBook SharePoint crée un serveur virtuel de commutation de contenu et 12 serveurs virtuels d'équilibrage de charge. Il crée également

des stratégies et des groupes de services et les lie aux serveurs virtuels d'équilibrage de charge. Les stratégies créées dépendent des fonctionnalités sélectionnées dans le StyleBook lors de la création du pack de configuration.

### **Affichage des objets définis sur l'instance de Citrix ADC**

Une fois le pack de configuration créé sur Citrix ADM, vous pouvez afficher tous les objets créés sur l'instance Citrix ADC pour le SharePoint StyleBook. Accédez à **Applications > Administration > Configuration**, puis cliquez sur **Afficher les objets créés**. La figure suivante montre certains des objets créés, avec les adresses IP spécifiées dans l'exemple illustré dans « Deploying SharePoint StyleBook Configurations from Citrix ADM. »

<p><b>Type : lbvserver</b></p> <p>appflowlog : DISABLED          backuppersistencetimeout : 20          downstateflush : DISABLED          ipv46 : 0.0.0.0          lbmethod : LEASTCONNECTION          name : sharepoint application test frontpage services lb          persistencebackup : SOURCEIP          persistencetype : COOKIEINSERT          port : 0          servicetype : HTTP          timeout : 20</p>
<p><b>Type : servicegroup</b></p> <p>cip : DISABLED          cka : YES          cmp : NO          downstateflush : DISABLED          healthmonitor : NO          servicegroupname : sharepoint-application-test-frontpage-services-svcgrp          servicetype : HTTP          sp : ON          state : ENABLED          tcpb : NO          useproxypport : NO          usip : NO</p>
<p><b>Type : lbvserver_servicegroup_binding</b></p> <p>name : sharepoint-application-test-frontpage-services-lb          servicegroupname : sharepoint-application-test-frontpage-services-svcgrp</p>
<p><b>Type : servicegroup_servicegroupmember_binding</b></p> <p>ip : 192.10.10.11          port : 80          servicegroupname : sharepoint-application-test-frontpage-services-svcgrp</p>
<p><b>Type : servicegroup_servicegroupmember_binding</b></p> <p>ip : 192.10.10.12          port : 80          servicegroupname : sharepoint-application-test-frontpage-services-svcgrp</p>
<p><b>Type : csaction</b></p> <p>name : sharepoint-application-test-cs-frontpage-services-csaction          targetlbvserver : sharepoint-application-test-frontpage-services-lb</p>
<p><b>Type : cspolicy</b></p> <p>action : sharepoint-application-test-cs-frontpage-services-csaction          policyname : sharepoint-application-test-cs-frontpage-services-cspol          rule : HTTP.REQ.HEADER("X-Vermeer-Content-Type").EXISTS</p>
<p><b>Type : csvserver_cspolicy_binding</b></p> <p>name : sharepoint-application-test-cs          policyname : sharepoint-application-test-cs-frontpage-services-cspol          priority : 10</p>

## StyleBook proxy Microsoft ADFS

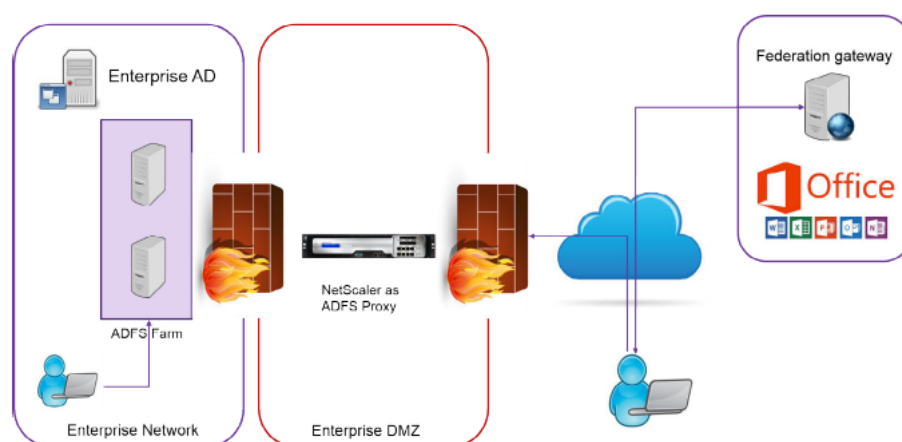
February 1, 2024

Le proxy Microsoft™ ADFS joue un rôle important en fournissant un accès par authentification unique aux ressources internes compatibles avec la fédération et aux ressources cloud. Office 365 est un exemple de ressources cloud. Le but du serveur proxy ADFS est de recevoir et de transférer des demandes vers des serveurs ADFS qui ne sont pas accessibles à partir d'Internet. Le proxy ADFS est un proxy inverse qui réside généralement dans le réseau de périmètre (DMZ) de votre organisation. Le proxy ADFS joue un rôle essentiel dans la connectivité des utilisateurs distants et l'accès aux applications.

Citrix ADC dispose de la technologie précise qui permet de sécuriser la connectivité, l'authentification et la gestion de l'identité fédérée. L'utilisation de Citrix ADC comme proxy ADFS évite de devoir déployer un composant supplémentaire dans la zone démilitarisée.

Le logiciel Microsoft ADFS Proxy StyleBook dans Citrix Application Delivery Management (ADM) vous permet de configurer un serveur proxy ADFS sur une instance Citrix ADC.

L'image suivante montre le déploiement d'une instance de Citrix ADC en tant que serveur proxy ADFS dans la zone DMZ d'entreprise.



### Avantages de l'utilisation de Citrix ADC comme proxy ADFS

1. Répond à la fois aux besoins d'équilibrage de charge et de proxy ADFS
2. Prend en charge les scénarios d'accès utilisateur internes et externes
3. Prend en charge des méthodes complètes de pré-authentification
4. Offre une expérience d'authentification unique aux utilisateurs
5. Prend en charge les protocoles actifs et passifs

- a) Voici des exemples d'applications à protocole actif : Microsoft Outlook, Microsoft Skype for Business
  - b) Voici des exemples d'applications à protocole passif : application Web Microsoft Outlook, navigateurs Web
6. Périphérique renforcé pour un déploiement basé sur DMZ
7. Ajoute de la valeur en utilisant des fonctionnalités supplémentaires de base de l'Citrix ADC ADC
- a) Commutation de contenu
  - b) Déchargement SSL
  - c) Réécriture
  - d) Sécurité (Citrix ADC AAA)

Pour les scénarios basés sur un protocole actif, vous pouvez vous connecter à Office 365 et fournir vos informations d'identification. Microsoft Federation Gateway contacte le service ADFS (via le proxy ADFS) au nom du client de protocole actif. La passerelle soumet ensuite les informations d'identification à l'aide de l'authentification de base (401). Citrix ADC gère l'authentification du client avant l'accès au service ADFS. Après l'authentification, le service ADFS fournit un jeton SAML à Federation Gateway. La Federation Gateway, à son tour, soumet le jeton à Office 365 pour fournir un accès client.

Pour les clients passifs, l'ADFS Proxy StyleBook crée un compte utilisateur Kerberos Constrained Delegation (KCD). Le compte KCD est nécessaire pour que l'authentification SSO Kerberos puisse se connecter aux serveurs ADFS. Le StyleBook génère également une stratégie LDAP et une stratégie de session. Ces stratégies sont ultérieurement liées au serveur virtuel Citrix ADC AAA qui gère l'authentification pour les clients passifs.

Le StyleBook peut également garantir que les serveurs DNS du Citrix ADC sont configurés pour ADFS.

La section de configuration ci-dessous explique comment configurer Citrix ADC pour gérer l'authentification client basée sur des protocoles actifs et passifs.

### Détails de la configuration

Le tableau ci-dessous répertorie les versions logicielles minimales requises pour que cette intégration soit déployée avec succès.

---

Produit	Version minimale requise
Citrix ADC	11.0, licence Enterprise/Platinum

---

Les instructions suivantes supposent que vous avez déjà créé les entrées DNS externes et internes appropriées.

## Déploiement de configurations StyleBook du proxy Microsoft ADFS depuis Citrix ADM

Les instructions suivantes vous aideront à implémenter le proxy Microsoft ADFS StyleBook dans votre réseau d'entreprise.

### Pour déployer le proxy Microsoft ADFS StyleBook

1. **Dans Citrix ADM, accédez à Applications > StyleBooks.** La page **StyleBooks** affiche tous les StyleBooks disponibles pour votre utilisation dans Citrix ADM.
2. Faites défiler l'écran vers le bas et trouvez le **StyleBook du proxy Microsoft ADFS**. Cliquez sur **Créer une configuration**.  
Le StyleBook s'ouvre sous la forme d'une page d'interface utilisateur sur laquelle vous pouvez saisir les valeurs de tous les paramètres définis dans ce StyleBook.
3. Entrez les valeurs des paramètres suivants :
  - a) **Nom du déploiement du proxy ADFS.** Sélectionnez un nom pour la configuration du proxy ADFS déployée sur votre réseau.
  - b) **FQDN ou IP des serveurs ADFS.** Entrez les adresses IP ou les noms de domaine complets (FQDN) de tous les serveurs ADFS du réseau.
  - c) **IP VIP publique du proxy ADFS.** Tapez l'adresse IP virtuelle publique sur l'Citrix ADC qui fonctionne en tant que serveur proxy ADFS.

ADFSProxy Deployment Name\*

 ?

ADFS Servers FQDNs and/or IPs\*

 + ?

ADFSProxy Public VIP IP\*

 ?

4. Dans la section **Certificats de proxy ADFS**, tapez les détails du certificat SSL et de la clé de certificat.

Ce certificat SSL est lié à tous les serveurs virtuels créés sur l'instance Citrix ADC.

Sélectionnez les fichiers correspondants dans votre dossier de stockage local. Vous pouvez également saisir le mot de passe de clé privée pour charger les clés privées chiffrées au format .pem.

### ADFSProxy Certificates

ADFS certificates bound to the SSL VServers created by this StyleBook

#### Certificate File path

Certificate Name\*  
 ?

Certificate File\*  
  ?

CertKey Format\*  
 ▾

Certificate Key Name  
 ?

Certificate Key File  
  ?

Private Key Password

Advanced Certificate Settings

CA Certificate File path

Vous pouvez également activer la case à cocher **Paramètres de certificat avancés**. Vous pouvez saisir ici des informations telles que la période de notification d'expiration des certificats, activer ou désactiver le moniteur d'expiration des certificats.

- Vous pouvez également activer la case à cocher **Certificat d'autorité de certification SSL** si le certificat SSL nécessite l'installation d'un certificat public d'autorité de certification sur Citrix ADC. Vérifiez que vous sélectionnez **Est un certificat d'autorité de certification** dans la section **Paramètres de certificat avancés**.
- Activer l'authentification pour les clients actifs et passifs. Entrez le nom de domaine DNS utilisé

dans Active Directory pour l'authentification des utilisateurs. Vous pouvez ensuite configurer l'authentification pour les clients actifs ou passifs, ou les deux.

7. Entrez les informations suivantes pour activer l'authentification pour les clients actifs :

**Remarque**

La configuration de la prise en charge des clients actifs est facultative.

- a) **Authentification active par proxy ADFS VIP.** Tapez l'adresse IP virtuelle du serveur d'authentification virtuel sur l'instance Citrix ADC sur laquelle les clients actifs sont redirigés pour l'authentification.
- b) Nom d'**utilisateur du compte de service** Entrez le nom d'utilisateur du compte de service utilisé par Citrix ADC pour authentifier vos utilisateurs auprès d'Active Directory.
- c) Mot de **passage du compte de service** Saisissez le mot de passe utilisé par Citrix ADC pour authentifier vos utilisateurs dans l'annuaire actif.

Enable Authentication for ADFS Passive and/or Active clients

Turn on authentication for ADFSProxy for Active and Passive Clients

ADFSProxy Authentication Domain\*

 ?

Enable Active Clients Authentication

Parameters for configuring Active Client Authentication to ADFS (AD Negotiate + SSO to ADFS)

ADFSProxy Active Authentication VIP\*

 ?

Service Account Username\*

 ?

Service Account Password\*

 ?

Kerberos Delegate Username\*

 ?

Kerberos Delegate Password\*

 ?

8. Configurez l'authentification pour les clients passifs en activant l'option correspondante et en configurant les paramètres LDAP.



### Remarque

La configuration de la prise en charge des clients passifs est facultative.

Entrez les informations suivantes pour activer l'authentification pour les clients passifs :

- a) **Base LDAP (Active Directory).** Tapez le nom de domaine de base du domaine dans lequel les comptes d'utilisateur résident dans Active Directory (AD) pour autoriser l'authentification. Par exemple, dc=netScaler, dc=com
- b) **DN de liaison LDAP (Active Directory).** Ajoutez un compte de domaine (à l'aide d'une adresse e-mail pour faciliter la configuration) qui dispose des privilèges pour parcourir l'arborescence AD. Par exemple, CN=Manager, dc=netScaler, dc=com
- c) **Mot de passe du nom unique de liaison LDAP (Active Directory).** Entrez le mot de passe du compte de domaine pour l'authentification.

Quelques autres champs que vous devez saisir dans les valeurs de cette section sont les suivants :

- d) **IP du serveur LDAP (Active Directory).** Entrez l'adresse IP du serveur Active Directory pour que l'authentification AD fonctionne correctement.
- e) **Nom de domaine complet du serveur LDAP .** Entrez le nom de domaine complet du serveur Active Directory. Le nom FQDN est facultatif. Fournissez l'adresse IP comme à l'étape 1 ou le nom de domaine complet.
- f) **Port Active Directory du serveur LDAP.** Par défaut, les ports TCP et UDP pour le protocole LDAP sont 389, tandis que le port TCP pour Secure LDAP est 636.
- g) **Nom d'utilisateur de connexion LDAP (Active Directory).** Entrez le nom d'utilisateur sous la forme « SAMAccountName ».
- h) **VIP de l'authentification passive par proxy ADFS.** Entrez l'adresse IP du serveur virtuel proxy ADFS pour les clients passifs.

### Remarque

Les champs marqués par « \* » sont obligatoires.

Enable Passive Clients Authentication

Parameters for configuring AD Auth for ADFSProxy

LDAP (Active Directory) Base\*  
 ?

LDAP (Active Directory) Bind DN\*  
 ?

LDAP (Active Directory) Bind DN Password\*  
 ?

LDAP Server (Active Directory) IP  
 ?

LDAP Server FQDN name  
 ?

LDAP Server (Active Directory) Port  
 ?

LDAP Host name  
 ?

Active Directory LDAP ?  
 Validate LDAP Certificate

LDAP (Active Directory) Login username

LDAP (Active Directory) Group Attribute Name  
 ?

LDAP (Active Directory) Group Sub-Attribute username

LDAP (Active Directory) default group

LDAP (Active Directory) SSO Attribute

Secure LDAP (Active Directory) Connection using SSL or TLS

9. Vous pouvez également configurer un VIP DNS pour vos serveurs DNS.

Configure DNS Settings

DNS settings

DNS VIP IP address\*

192 . 50 . 50 . 12 ?

IP addresses of DNS Servers\*

10 . 30 . 30 . 5 + ?

10. Cliquez sur **Instances cibles** et sélectionnez les instances Citrix ADC pour déployer cette configuration de proxy Microsoft ADFS. Cliquez sur **Créer** pour créer la configuration et déployer la configuration sur les instances Citrix ADC sélectionnées.

Target Instances

192.168.153.160 > + ?

Create Close Dry Run

#### Remarque

Citrix recommande de sélectionner **Essai** avant d'exécuter la configuration réelle. Vous pouvez d'abord afficher les objets de configuration créés sur les instances Citrix ADC cibles par le Style-Book. Vous pouvez ensuite cliquer sur **Créer** pour déployer la configuration sur les instances sélectionnées.

#### Objets créés

Plusieurs objets de configuration sont créés lorsque la configuration du proxy ADFS est déployée sur l'instance Citrix ADC. L'image suivante affiche la liste des objets créés.

# NetScaler Application Delivery Management 12.1

<p><b>Type : systemfile</b></p> <p><b>filecontent :</b> LS0L5L1CRUJgTtBDRVJUSZQDFUR30L501CK1JSURVENDQW9H20F35UJ8Z0ICQXp8Tma3Foa2HOKwQqFRi0ZB1 VFRKXKVRV8N114Q1FH2LNV8LNPJ8LUNKQJZVWqjKxW7T7W0LXKtH8R0ZjYHf9yORJQzQvY7jwEEZCV 1URXIPVEEVTVnd05Wd1HEVEISTVRF6UR9EQTFNFG3T7ZdZ23K9R0RBVQjntZCQUJ1NRDnsdmrKxTmaatF6WVcx FRaJGaGw1YnWapWwXRMkZ0YKvCafyMwMxV052Y5B0VYQXRNJK3CKYBWLURWUJFLREF3QEWLUZMNUUS CQUJFQQR0R0FN5LUC2dLQPRRURFSL1gpaVVC23TR0gopQmPKSZZ6WmWmQJ1FKZ20d3Hf9pG7T7ma3dG4o4hNp5 9KXQCCHNmeG56K2RbVjyaUHhakeEaZVPYKFSmd2N2NHaGhml3pVQVpDa3MyDkVocp6J5EiXOWKQmBwC3HTI H3VpBakZvtnMTVh5kxMwWbuzndyTicQ3V7VMyRTFDNp1WG1TznhdulzTzndFZznov5DhQIMACjPvDvhai 08554ntZLkLkFQWb0L18d0BmWwKHhBRUR5U10RFQOmWkWThreus54B3CQF8F8T0NBULV8dL4E8Cqz KOG3CjNlUzjkeE15ukUwXhN3V55XpR0ZaV1V8cMxL09PLUGR8ZNEFZWxz6UJhGLpWmZpHWZnJkdM50 zFRhNhdVYHdgaKw11M1NMcWwDGVVcN8QzXusjW1NnAqJv0D1TbU1RVVDH1ZjQzRkUzTfHkTzCZ1hW0UjVR NEVESLazE1V7C50UjKKEE5P7aR0Z2mmdrczrv058F70K50L3L1F7KqgQV0V565LUNWELU50LQp=</p> <p><b>fileencoding :</b> BASE64 <b>filelocation :</b> /nsconfig/ssl <b>filename :</b> saml-idd.pem</p>
<p><b>Type : systemfile</b></p> <p><b>filecontent :</b> LS0L5L1CRUJgTtBDRVJUSZQDFUR30L501CK1JSURVENDQW9H20F35UJ8Z0ICQXp8Tma3Foa2HOKwQqFRi0ZB1 QzWwY7YNazjFT0EaJ9CvPpR9SLQ5P8KXQjCOHnmeG4kekkb26ycmIRZpLg1T2JBUjndYTR2hoZR0DfAQZ1 8T1U1159QmH0CUNSEKEEPUJN1V9jBakQvRnN7W4CKHvZFHm53K5XNEN1J98R8MUKZv460ruZ2yAH h0bY1Y2Lb0jWaxdREFRQJBBdCCQJv51FGEVZLV8BNDoveA03T0VnKjRTK3Rj2NEH8nFVjPc1V0LQZy2h2 WUjontH8ZDvR9DfQdmyNE53hVx8QkpaZ0gleokRhZjT1oadtzc0XVY8LumovDnaah0sZ1aMEQ4J w50B8Hjy0e0LjNMDaL0rN1M1G5AM7cc1N0ThaC2pawKCS0T78kzm3dfj5c3aRfemDNWFC8A 1Rz2hTzZPF6T9gwYUNQWFWNC1QVoyeThubxpvMXNDW1dE9m8B8NApGRhZNY2wkyHqSpWYpsRWY wWdAZWw5TzVYwQ4qWdgyYkTnIITPWR0zRvFYQmNhmjmsXNDZjFQzAQZkKkFhdFT3htTQZ1zm 1PZ7W1D2mWwMwNDSjU18G1NNEWwQqF7hQWZ3NwW8w8yKfFwWwY0T8kKzGdY5Cj0N0j0p lMzqNw5tumpzTfFKZ1Qz2LdLFQ1LpVUVV0y0XpFanR8zbR7FhVUzJ3V0XCVU11DvVWg01Y1B50F4FE VCLWwQh5a0jUGVd0R53GLQmRQ2BME1B8MVAz0Kwpsa08005TDpUGNYUZZ0KJURBLQKQRtvaAxl GELB83N1E3FCWwJ4R75AKFFZ7N1U1159QmH0CUNSEKEEPUJN1V9jBakQvRnN7W4CKHvZFHm53K5XNEN1J98R8MUKZv460ruZ2yAH Ee0KJm1WwWJnr0eakJ5TE3KYU5STxpTWFYkhaF4R1L5D8yQnFYEUE0M1B4Zm9Fj9ndedCAH2azRiumpa 0150L1V0K85U0EgUjFjWfUR58LrvktLS0LQp=</p> <p><b>fileencoding :</b> BASE64 <b>filelocation :</b> /nsconfig/ssl <b>filename :</b> saml-idd.key</p>
<p><b>Type : sslcertkey</b></p> <p><b>cert :</b> saml-idd.pem <b>certkey :</b> adfs-certificate <b>inform :</b> PEM <b>key :</b> saml-idd.key</p>

**Objects Added on Instance : 192.168.153.160 | Count : 57**

**Type : nsfeature**

**Meta Properties**

action : enable

feature : cs lb ssl rewrite aaa

**Type : lbvserver**

ipv46 : 192.50.50.12

name : ns-ads-dep01-ads-dns

port : 53

servicetype : DNS

**Type : service**

ip : 10.30.30.5

name : ns-ads-dep01-dns-svc-1

port : 53

servicetype : DNS

**Type : lbvserver\_service\_binding**

name : ns-ads-dep01-ads-dns

servicename : ns-ads-dep01-dns-svc-1

**Type : authenticationnegotiateaction**

domain : ADFS.CITRIX.COM

domainuser : nsroot

domainuserpasswd : nsroot

name : ns-ads-dep01-negotiate-action

**Type : authenticationpolicy**

**action** : ns-ads-dep01-negotiate-action  
**name** : ns-ads-dep01-negotiate-policy  
**rule** : true

**Type : aaakcdaccount**

**delegateduser** : nsroot  
**kcdaccount** : ns-ads-dep01-ads-auth401-kcd-  
**kcdpassword** : nsroot  
**realmstr** : ADFS.CITRIX.COM

**Type : tmsessionaction**

**kcdaccount** : ns-ads-dep01-ads-auth401-kcd-  
**name** : ns-ads-dep01-ads-auth401-tmsession-action  
**persistentcookie** : ON  
**persistentcookievalidity** : 3  
**sso** : ON

**Type : tmsessionpolicy**

**action** : ns-ads-dep01-ads-auth401-tmsession-action  
**name** : ns-ads-dep01-ads-auth401-tmsession-policy  
**rule** : ns\_true

**Type : authenticationvserver**

**authenticationdomain** : ADFS.CITRIX.COM  
**failedlogintimeout** : 1  
**ipv46** : 192.50.50.40  
**maxloginattempts** : 255  
**name** : ns-ads-dep01-ads-auth401-auth-vserver  
**port** : 443  
**servicetype** : SSL

**Type : sslvserver\_sslcertkey\_binding**

**certkeyname** : adfs-certificate  
**vservername** : ns-adfs-dep01-adfs-auth401-auth-vserver

**Type : authenticationvserver\_authenticationpolicy\_binding**

**name** : ns-adfs-dep01-adfs-auth401-auth-vserver  
**policy** : ns-adfs-dep01-negotiate-policy  
**priority** : 10

**Type : authenticationvserver\_tmssessionpolicy\_binding**

**name** : ns-adfs-dep01-adfs-auth401-auth-vserver  
**policy** : ns-adfs-dep01-adfs-auth401-tmsession-policy  
**priority** : 10

**Type : authenticationldapaction**

**authentication** : ENABLED  
**authtimeout** : 30  
**followreferrals** : OFF  
**ldapbase** : dc=netScaler,dc=com  
**ldapbinddn** : cn=Manager,dc=netScaler,dc=com  
**ldapbinddnpassword** : nsroot  
**ldaploginname** : samAccountName  
**name** : ns-adfs-dep01-ldap-action  
**passwdchange** : DISABLED  
**sectype** : PLAINTEXT  
**serverip** : 10.30.30.3  
**serverport** : 389  
**ssonameattribute** : userPrincipalName  
**svrtype** : AD  
**validateservercert** : NO

**Type : authenticationpolicy**

**action** : ns-adfs-dep01-ldap-action  
**name** : ns-adfs-dep01-ldap-policy  
**rule** : true

**Type : aaakcdaccount**

**kcdaccount** : ns-ads-dep01-ads-ldap-kcd-acc  
**realmstr** : ADFS.CITRIX.COM

**Type : tmsessionaction**

**kcdaccount** : ns-ads-dep01-ads-ldap-kcd-acc  
**name** : ns-ads-dep01-ads-ldap-tmsession-action  
**persistentcookie** : OFF  
**sso** : ON

**Type : tmsessionpolicy**

**action** : ns-ads-dep01-ads-ldap-tmsession-action  
**name** : ns-ads-dep01-ads-ldap-tmsession-policy  
**rule** : ns\_true

**Type : authenticationvserver**

**authenticationdomain** : ADFS.CITRIX.COM  
**failedlogintimeout** : 1  
**ipv46** : 192.50.50.30  
**maxloginattempts** : 255  
**name** : ns-ads-dep01-ads-ldap-auth-vserver  
**port** : 443  
**servicetype** : SSL

**Type : sslvserver\_sslcertkey\_binding**

**certkeyname** : ads-certificate  
**vservername** : ns-ads-dep01-ads-ldap-auth-vserver

**Type : authenticationvserver\_authenticationpolicy\_binding**

**name** : ns-ads-dep01-ads-ldap-auth-vserver  
**policy** : ns-ads-dep01-ldap-policy  
**priority** : 10



**Type : authenticationvserver\_tmssessionpolicy\_binding**

**name** : ns-adfs-dep01-adfs-ldap-auth-vserver  
**policy** : ns-adfs-dep01-adfs-ldap-tmsession-policy  
**priority** : 10

**Type : csvserver**

**ipv46** : 192.50.50.50  
**name** : ns-adfs-dep01-cs  
**port** : 443  
**servicetype** : SSL

**Type : lbvserver**

**ipv46** : 192.50.50.50  
**name** : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb  
**port** : 445  
**servicetype** : SSL

**Type : servicegroup**

**servicegroupname** : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp  
**servicetype** : SSL

**Type : lbvserver\_servicegroup\_binding**

**name** : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb  
**servicegroupname** : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp

**Type : server**

**ipaddress** : 192.30.30.30  
**name** : 192.30.30.30

**Type : servicegroup\_servicegroupmember\_binding**

**ip** : 192.30.30.30  
**port** : 443  
**servicegroupname** : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp

**Type : sslserver\_sslcertkey\_binding**

**certkeyname** : adfs-certificate

**vservername** : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb

**Type : csaction**

**name** : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction

**targetlbserver** : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb

**Type : cspolicy**

**action** : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction

**policyname** : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol

**rule** : HTTP.REQ.URL.CONTAINS("/adfs/services/trust") || HTTP.REQ.URL.CONTAINS("/federa

**Type : csvserver\_cspolicy\_binding**

**name** : ns-adfs-dep01-cs

**policyname** : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol

**priority** : 9800

**Type : lbvserver**

**appflowlog** : ENABLED

**authentication** : ON

**authenticationhost** : ADFS.CITRIX.COM

**authn401** : OFF

**authnvsname** : ns-adfs-dep01-adfs-ldap-auth-vserver

**downstateflush** : ENABLED

**ipv46** : 192.50.50.50

**lbmethod** : LEASTCONNECTION

**name** : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb

**port** : 446

**servicetype** : SSL

**Type : servicegroup**

**servicegroupname** : ns-ads-dep01-ns-ads-dep01-ads-passive-svcgrp  
**servicetype** : SSL

**Type : lbvserver\_servicegroup\_binding**

**name** : ns-ads-dep01-ns-ads-dep01-ads-passive-lb  
**servicegroupname** : ns-ads-dep01-ns-ads-dep01-ads-passive-svcgrp

**Type : servicegroup\_servicegroupmember\_binding**

**ip** : 192.30.30.30  
**port** : 443  
**servicegroupname** : ns-ads-dep01-ns-ads-dep01-ads-passive-svcgrp

**Type : sslvserver\_sslcertkey\_binding**

**certkeyname** : ads-certificate  
**vservername** : ns-ads-dep01-ns-ads-dep01-ads-passive-lb

**Type : csaction**

**name** : ns-ads-dep01-cs-ns-ads-dep01-ads-passive-csaction  
**targetlbvserver** : ns-ads-dep01-ns-ads-dep01-ads-passive-lb

**Type : cspolicy**

**action** : ns-ads-dep01-cs-ns-ads-dep01-ads-passive-csaction  
**policyname** : ns-ads-dep01-cs-ns-ads-dep01-ads-passive-cspol  
**rule** : HTTP.REQ.URL.CONTAINS("/ads/lis/auth/integrated") || HTTP.REQ.URL.CONTAINS("/ads/lis/wia")

**Type : csvserver\_cspolicy\_binding**

**name** : ns-ads-dep01-cs  
**policyname** : ns-ads-dep01-cs-ns-ads-dep01-ads-passive-cspol  
**priority** : 9900

**Type : lbvserver**

**appflowlog** : ENABLED  
**authentication** : OFF  
**authn401** : ON  
**authnvsname** : ns-ads-dep01-ads-auth401-auth-vserver  
**downstateflush** : ENABLED  
**ipv46** : 192.50.50.50  
**lbmethod** : LEASTCONNECTION  
**name** : ns-ads-dep01-ns-ads-dep01-ads-active-lb  
**port** : 444  
**servicetype** : SSL

**Type : servicegroup**

**servicegroupname** : ns-ads-dep01-ns-ads-dep01-ads-active-svcgrp  
**servicetype** : SSL

**Type : lbvserver\_servicegroup\_binding**

**name** : ns-ads-dep01-ns-ads-dep01-ads-active-lb  
**servicegroupname** : ns-ads-dep01-ns-ads-dep01-ads-active-svcgrp

**Type : servicegroup\_servicegroupmember\_binding**

**ip** : 192.30.30.30  
**port** : 443  
**servicegroupname** : ns-ads-dep01-ns-ads-dep01-ads-active-svcgrp

**Type : sslvserver\_sslcertkey\_binding**

**certkeyname** : ads-certificate  
**vservername** : ns-ads-dep01-ns-ads-dep01-ads-active-lb

**Type : csaction**

**name** : ns-ads-dep01-cs-ns-ads-dep01-ads-active-csaction  
**targetlbvserver** : ns-ads-dep01-ns-ads-dep01-ads-active-lb

**Type : cspolicy**

**action** : ns-ads-dep01-cs-ns-ads-dep01-ads-active-csaction  
**policyname** : ns-ads-dep01-cs-ns-ads-dep01-ads-active-cspol  
**rule** : true

**Type : csvserver\_cspolicy\_binding**

**name** : ns-ads-dep01-cs  
**policyname** : ns-ads-dep01-cs-ns-ads-dep01-ads-active-cspol  
**priority** : 10000

**Type : sslvserver\_sslcertkey\_binding**

**certkeyname** : ads-certificate  
**vservername** : ns-ads-dep01-cs

**Type : rewritepolicylabel**

**labelname** : ns-ads-dep01-request-rewritepolicylabel  
**transform** : HTTP\_REQ

**Type : rewritepolicylabel**

**labelname** : ns-ads-dep01-response-rewritepolicylabel  
**transform** : HTTP\_RES

**Type : rewriteaction**

**name** : ns-ads-dep01-HTTP.REQUEST-rewrite-action  
**stringbuilderexpr** : "/ads/services/trust/proxymex"  
**target** : HTTP.REQUEST  
**type** : REPLACE

**Type : rewritepolicy**

**action** : ns-ads-dep01-HTTP.REQUEST-rewrite-action  
**name** : ns-ads-dep01-HTTP.REQUEST-rewrite-policy  
**rule** : HTTP.REQUEST.CONTAINS("/ads/services/trust") && (!HTTP.REQUEST.CONTAINS("/trust/proxymex"))

**Type : rewritepolicylabel\_rewritepolicy\_binding**

gotopriorityexpression : END  
labelname : ns-adfs-dep01-request-rewritepolicylabel  
policyname : ns-adfs-dep01-HTTPREQ.URL-rewrite-policy  
priority : 10

**Type : lbvserver\_rewritepolicy\_binding**

bindpoint : REQUEST  
gotopriorityexpression : END  
invoke : true  
labelname : ns-adfs-dep01-request-rewritepolicylabel  
labeltype : policylabel  
name : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb  
policyname : NOPOLICY-rewrite  
priority : 10

## StyleBook Oracle e-business

February 1, 2024

Oracle E-Business Suite est la suite la plus complète d'applications métier globales intégrées. Cette suite permet aux entreprises de prendre de meilleures décisions, de réduire les coûts et d'améliorer les performances. Elle comprend les applications suivantes.

- Planification des ressources de l'entreprise (ERP)
- Gestion de la relation client (CRM)
- Gestion de la chaîne d'approvisionnement (SCM)

Ces applications informatiques sont développées ou acquises par Oracle. Le StyleBook d'Oracle E-Business Suite 12.2 vous permet de déployer la configuration sur les instances Citrix ADC sélectionnées.

Ce StyleBook crée une configuration d'équilibrage de charge qui comprend un serveur virtuel d'équilibrage de charge, un groupe de services et une liste de services. Il lie également les services au groupe de services et lie le groupe de services au serveur virtuel. Vous pouvez choisir une communication chiffrée en sélectionnant SSL et en fournissant les fichiers SSL et les fichiers clés de votre système local.

## Pour créer une configuration pour Oracle E-Business Suite 12.2

1. Dans Citrix Application Delivery Management (ADM), accédez à **Applications > Configuration > StyleBooks**. La page **StyleBooks** affiche tous les StyleBooks disponibles dans votre Citrix ADM. Faites défiler l'écran vers le bas et sélectionnez **Oracle E-Business Suite 12.2**. Vous pouvez également utiliser l'option de recherche pour effectuer une recherche dans le StyleBook.
2. Cliquez sur **Créer une configuration** dans le panneau StyleBook.
3. Entrez le nom de l'application d'équilibrage de charge et l'adresse IP virtuelle dans la section des paramètres de l'équilibreur de charge.
4. Sélectionnez le protocole requis. Vous avez deux options ici - HTTP et HTTPS/SSL. Vous pouvez également saisir le numéro de port.
5. Entrez les adresses IP de tous les serveurs d'applications Oracle E-Business Suite du réseau qui doivent être équilibrés en termes de charge. Cliquez sur **+** pour ajouter d'autres adresses IP de serveur.
6. Dans la section **Paramètres des certificats SSL**, sélectionnez les fichiers correspondants dans votre stockage local. Vous pouvez également activer la case à cocher **Paramètres de certificat avancés**. Ici, vous pouvez configurer plus de détails tels que la période de notification d'expiration du certificat. Vous pouvez également activer ou désactiver le moniteur d'expiration des certificats.

Sélectionnez l'instance Citrix ADC cible sur laquelle la configuration doit être créée, puis cliquez sur **Créer**.

This configuration will be created from the StyleBook 'oracle-ebusiness-suite12' (namespace: 'com.citrix.adc.enterprise.stylebooks ,version: '1.0').

Application Name\*

Virtual IP (VIP)\*

Protocol

Virtual Port

Oracle E-Business Suite Server IPs\*  
 ×  
 × +

SSL Certificate settings +

Certificate Name	CertKey Format	Certificate Key Name	Private Key Password
oracle-cert-file	PEM	oracle-cert-key-file	× >

Advanced Settings

Target Instances  
 > +

### Conseil

Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter des instances Citrix ADC récemment découvertes dans Citrix ADM à la liste des instances disponibles dans cette fenêtre. L'icône d'actualisation est actuellement disponible uniquement sur Citrix ADM.

## Créer et utiliser des StyleBooks personnalisés

February 1, 2024

Vous pouvez écrire votre propre StyleBook pour votre déploiement, l'importer dans Citrix Application Delivery Management (ADM) et créer des objets de configuration. Vous pouvez également utiliser l'API pour créer des configurations à partir de vos StyleBooks.

Ce document contient les informations suivantes :

### Avant de commencer

Avant de commencer à créer des StyleBooks, assurez-vous de connaître les points suivants :

- API NITRO. Pour plus d'informations, consultez la [documentation de l'API Nitro](#)
- YAML

Les fichiers StyleBook utilisent le format YAML. Pour plus d'informations sur le format YAML, consultez [Syntaxe YAML](#).

Voici une liste des instructions YAML dont vous devez tenir compte lors de la création de StyleBooks :

- YAML fait la distinction entre majuscules et minuscules.
- YAML nécessite une indentation appropriée
- Utilisez `<spacebar>` la touche pour créer une indentation appropriée. N'utilisez pas de `<tab>` clé. L'utilisation de `<tab>` la clé crée une erreur de compilation lors de l'importation de votre StyleBook vers MA Service
- N'utilisez pas de chaînes entre guillemets. N'incluez la chaîne entre guillemets que si une chaîne contient des signes de ponctuation (tirets, deux-points, etc.) Si vous souhaitez interpréter un nombre comme une chaîne, insérez-le entre guillemets ou utilisez la fonction intégrée `str ()` de StyleBooks.



- Les littéraux tels que YES/Yes/yes/Y/y/NO/no/No/n/N, ON/On/on/OFF/Off/off et TRUE/true/truthy/-FALSE/False/false/falsely sont considérés comme des booléens et sont équivalents respectivement à true et false. Pour les interpréter comme des chaînes, incluez-les entre guillemets. Par exemple :
  - “YES”
  - “No”
  - “True”
  - “False” et ainsi de suite.

### Remarque

Avant d’importer votre fichier StyleBook dans Citrix ADM, il est recommandé de vérifier si votre fichier est conforme au format YAML. Citrix vous recommande d’utiliser le validateur YAML intégré dans StyleBooks pour valider et importer le contenu YAML.

Lors de la configuration de StyleBooks, vous ne pouvez utiliser que les ressources Nitro Configuration qui prennent en charge les opérations de **création** et de **suppression** (méthodes POST et DELETE HTTP). Pour plus d’informations, consultez la [documentation sur les API Nitro](#).

## Anatomie d’un StyleBook

Pour écrire des StyleBooks, vous devez comprendre la grammaire, la syntaxe et la structure des StyleBooks. Un StyleBook classique comporte les sections suivantes :

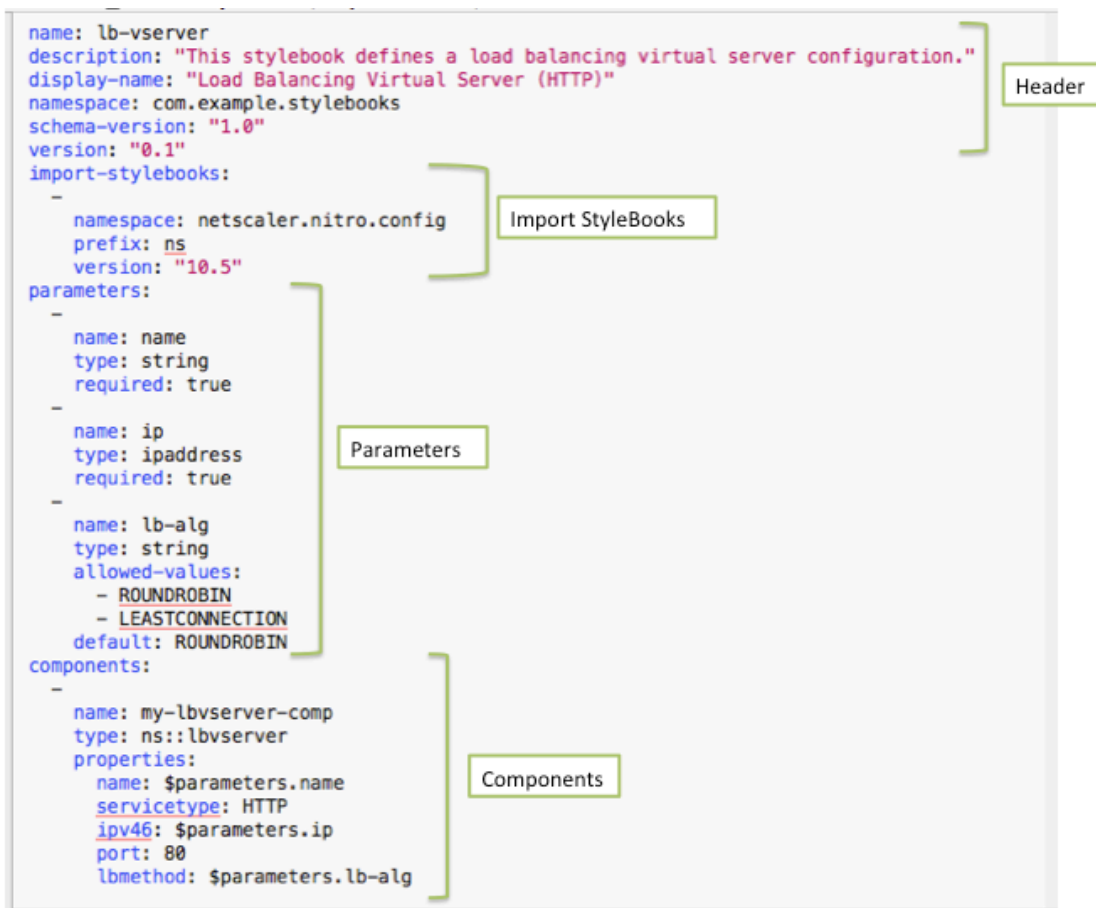
- **En-tête** : Cette section vous permet de définir l’identité d’un StyleBook et de décrire son rôle. Il s’agit d’une section obligatoire.
- **Importer des StyleBooks** : cette section vous permet de déclarer à quel autre StyleBook vous souhaitez faire référence depuis votre StyleBook actuel. L’importation de StyleBooks de configuration Citrix ADC NITRO ou d’autres StyleBooks est requise pour écrire un StyleBook. Il s’agit d’une section obligatoire.
- **Paramètres** : Cette section vous permet de définir les paramètres dont vous avez besoin dans votre StyleBook pour créer une configuration. Il décrit l’entrée que votre StyleBook prend. Il s’agit d’une section facultative.
- **Composants** : Cette section vous permet de définir les entités (objets de configuration) créées par le StyleBook pour une configuration spécifique. Cette section est considérée comme le cœur d’un StyleBook. Les composants utilisent généralement l’entrée fournie dans la section des paramètres pour adapter la configuration générée par le StyleBook. Il s’agit d’une section facultative.

Un StyleBook peut comporter une section de paramètres, une section de composants, ou les deux. Un StyleBook contenant uniquement la section des paramètres est utile pour définir une

liste de paramètres pouvant être utilisés par d'autres StyleBooks. Cela favorise la réutilisation des groupes de paramètres dans un ensemble de StyleBooks. Un StyleBook avec uniquement une section de composants peut être utilisé lorsque vous souhaitez spécifier les valeurs des attributs du StyleBook au lieu de définir des paramètres pour prendre en compte les entrées de l'utilisateur.

- **Sorties** : tandis que la section des paramètres définit les entrées du StyleBook, cette section facultative définit ses sorties. Dans cette section de sorties facultatives, vous pouvez spécifier les composants que vous souhaitez exposer aux utilisateurs qui créent une configuration à partir de ce StyleBook et aux autres StyleBooks qui importent ce StyleBook. Les utilisateurs et les StyleBooks qui importent peuvent ensuite référencer les propriétés des composants exposés.
- **Opérations** : Un StyleBook peut contenir une section facultative pour activer Analytics dans Citrix ADM sur n'importe quel serveur virtuel faisant partie du StyleBook.

La figure suivante montre un contour simple d'un StyleBook.



Les exemples suivants vous aident à connaître la grammaire et la structure d'un StyleBook et à écrire des StyleBooks avec des niveaux de complexité croissants.

- [StyleBook pour créer un serveur virtuel d'équilibrage de charge](#)

- [StyleBook pour créer une configuration d'équilibrage de charge de base](#)
- [Créer un StyleBook composite](#)
- [Personnalisez votre StyleBook en utilisant les attributs de l'interface](#)

## StyleBook pour créer un serveur virtuel d'équilibrage de charge

February 1, 2024

Dans cet exemple, vous concevez un StyleBook de base qui crée un serveur virtuel d'équilibrage de charge de type protocole HTTP et écoutant sur le port 80. Le nom du serveur virtuel, l'adresse IP et les paramètres de la méthode d'équilibrage de charge acceptent des valeurs définies par l'utilisateur, c'est-à-dire qu'il s'agit des paramètres du StyleBook.

### En-tête

Les six premières lignes d'un StyleBook constituent la section d'en-tête. Dans cet exemple, la section d'en-tête est écrite comme suit :

```
1 name: lb-vserver
2 description: This StyleBook defines a load balancing virtual server
  configuration.
3 display-name: Load Balancing Virtual Server (HTTP)
4 namespace: com.example.stylebooks
5 schema-version: "1.0"
6 version: "0.1"
7 <!--NeedCopy-->
```

La section d'en-tête inclut les informations suivantes :

- **nom** : nom pour ce StyleBook.
- **description** : Description définissant ce que fait ce StyleBook. Cette description apparaît sur Citrix ADM.
- **display-name** : nom descriptif du StyleBook qui apparaît sur Citrix ADM.
- **espace de noms** : un espace de noms fait partie d'un identificateur unique pour un StyleBook afin d'éviter les collisions de noms.
- **schema-version** : prend toujours la valeur « 1.0 » dans cette version.
- **version** : numéro de version du StyleBook. Vous pouvez modifier le numéro de version lorsque vous mettez à jour le StyleBook.

La combinaison du **nom**, de l'**espace** de noms et de la **version** identifie de manière unique un StyleBook dans le système. Vous ne pouvez pas avoir deux StyleBooks avec la même combinaison de nom, d'espace de noms et de version dans Citrix ADM. Cependant, vous pouvez avoir deux StyleBooks avec le même nom et la même version mais des espaces de noms différents, ou avec le même espace de noms et la même version mais des noms différents.

#### Remarque

Supposons que vous avez mis à jour votre StyleBook et que vous avez un numéro de version mis à jour. Maintenant, si vous faites référence (c'est-à-dire si vous importez) ce StyleBook dans d'autres StyleBooks, veillez à mettre à jour le numéro de version dans d'autres StyleBooks également, afin qu'ils utilisent la bonne version du StyleBook importé.

### Importer des StyleBooks

La section qui suit l'en-tête s'appelle « import-stylebooks ». Dans cette section, vous devez déclarer l'espace de noms et le numéro de version de tout autre StyleBook auquel vous souhaitez faire référence dans votre StyleBook actuel. Cela vous permet d'importer et de réutiliser d'autres StyleBooks au lieu de recréer la même configuration dans votre propre StyleBook.

Dans cet exemple, la section import-stylebooks est écrite comme suit :

```
1 import-stylebooks:  
2 -  
3   namespace: netscaler.nitro.config  
4   prefix: ns  
5   version: "10.5"  
6 <!--NeedCopy-->
```

Chaque StyleBook doit faire référence à l'espace de noms netscaler.nitro.config s'il utilise directement l'un des objets de configuration NITRO. Cet espace de noms contient tous les types de Citrix ADC NITRO, tels que LBVServer. Comme les versions 10.5 et ultérieures du logiciel sont prises en charge, vous pouvez utiliser votre StyleBook pour créer et exécuter des configurations sur n'importe quelle instance Citrix ADC exécutant la version 10.5 et les versions ultérieures.

Le préfixe utilisé dans la section import-stylebooks est un raccourci qui fait référence à la combinaison de l'espace de noms et de la version. Dans ce cas, ns fait référence à netscaler.nitro.config de la version 10.5. Dans les dernières sections de votre StyleBook, au lieu d'utiliser l'espace de noms et la version pour faire référence au StyleBook importé, vous pouvez utiliser la chaîne de préfixe choisie, par exemple ns, dans l'exemple ci-dessus.

La version utilisée dans les StyleBooks est la version NITRO de Citrix ADC. Un StyleBook basé sur Nitro version X peut être utilisé pour configurer n'importe quel Citrix ADC version X ou supérieure.

**Remarque**

Pour vous assurer que vos StyleBooks peuvent être utilisés pour configurer n'importe quelle instance Citrix ADC de la version 10.5 ou ultérieure, Citrix recommande que, pour une compatibilité maximale, vous importez l'espace de noms Nitro 10.5 dans vos StyleBooks qui utilisent directement les StyleBooks intégrés à Nitro (espace de noms : netscaler.nitro.config, version : 10.5).

Il est important qu'un StyleBook qui importe d'autres StyleBooks soit basé sur une version Nitro qui est à la même version ou supérieure que les StyleBooks qu'il importe. Par exemple, un StyleBook basé sur la version 10.5 de Nitro ne peut pas dépendre d'un StyleBook basé sur la version 11.1, ni l'utiliser ou l'importer. Mais un StyleBook basé sur la version 11.1 peut importer un StyleBook basé sur n'importe quelle version inférieure à 11.1.

Il est également possible qu'un StyleBook n'importe pas du tout l'espace de noms Nitro. Cela signifie qu'un StyleBook n'a pas besoin de définir directement les composants Nitro, mais peut importer (dépendre) les StyleBooks qui définissent les composants Nitro. Le StyleBook qui importe d'autres StyleBooks acquiert toujours la version Nitro la plus élevée dans la hiérarchie de ses dépendances et peut donc être utilisé pour configurer des Citrix ADC de cette version ou supérieure.

**Paramètres**

La section des paramètres vous permet de déclarer tous les paramètres dont vous avez besoin dans votre StyleBook. En tant que développeur de StyleBook, vous devez décider de l'entrée que vous souhaitez que les utilisateurs de votre StyleBook spécifient. Dans cet exemple, vous avez créé votre StyleBook de manière à ce que ses utilisateurs fournissent le nom du serveur virtuel, son adresse IP et la méthode d'équilibrage de charge.

La section des paramètres se présenterait comme suit :

```
1 parameters:
2   -
3     name: name
4     type: string
5     label: Application Name
6     description: Name of the application configuration.
7     required: true
8
9   -
10    name: ip
11    type: ipaddress
12    label: Application Virtual IP (VIP)
13    description: Application VIP that the clients access.
14    required: true
15
16  -
17    name: lb-alg
```

```
18 type: string
19 label: LoadBalancing Algorithm
20 description: Choose the load balancing algorithm (method) used for
    load balancing client request between the application servers.
21 allowed-values:
22 - ROUNDROBIN
23 - LEASTCONNECTION
24 default: ROUNDROBIN
25 <!--NeedCopy-->
```

### Remarque

Si vous ne fournissez pas l'étiquette d'un paramètre, Citrix ADM utilise l'attribut name lors de l'affichage de ce paramètre. Vous devez toujours définir une étiquette pour vos paramètres afin de pouvoir contrôler leur affichage dans Citrix ADM.

Toutefois, lors de l'utilisation des API, le paramètre est désigné par son nom.

Dans cette section, vous avez déclaré trois paramètres indiqués par leurs valeurs d'attribut **name** : **name** pour le nom du serveur virtuel, **ip** pour l'adresse IP du serveur virtuel, et **lb-alg** pour la méthode d'équilibrage de charge.

- **type.** Type de valeur que ces paramètres peuvent prendre. Par exemple, name et lb-alg peuvent prendre une valeur de chaîne et la valeur IP doit être de type adresse IP. Les paramètres d'un StyleBook peuvent être de l'un des types intégrés suivants :
- **chaîne.** Une panoplie de personnages. Si aucune longueur n'est spécifiée, la valeur de la chaîne peut prendre n'importe quel nombre de caractères. Toutefois, vous pouvez limiter la longueur d'un type de chaîne en utilisant les attributs min-length et max-length.
- **numéro.** Un nombre entier. Vous pouvez spécifier le nombre minimum et maximum que ce type peut prendre en utilisant les attributs min-value et max-value.
- **booléen.** Peut être vrai ou faux. Notez également que tous les littéraux sont considérés par YAML comme des booléens (par exemple, Oui ou Non).
- **ipaddress.** Chaîne qui représente une adresse IPv4 ou IPv6 valide.
- **port TCP.** Nombre compris entre 0 et 65535 qui représente un port TCP ou UDP.
- **password.** Une valeur de chaîne opaque/secrète. Lorsque Citrix ADM affiche une valeur pour ce paramètre, elle s'affiche sous la forme d'astérisques (\*\*\*\*\*).
- **Certfile.** Fichier de certificat.
- **fichier clé.** Fichier de clé privée du certificat.
- **fichier.** Un paramètre de ce type nécessite que l'utilisateur télécharge un fichier, par exemple un certificat ou un fichier clé.

- **objet.** Se compose de plusieurs éléments et chacun de ces éléments est un paramètre. Ce type peut être utilisé pour regrouper plusieurs paramètres associés sous un paramètre parent.
- **requis.** Indique si un paramètre est obligatoire ou facultatif. S'il est défini sur true, le paramètre est obligatoire et l'utilisateur doit fournir une valeur pour ce paramètre lors de la création de configurations à l'aide de ce StyleBook. Par défaut, tous les paramètres sont facultatifs. Dans cet exemple, le **nom** et l'**adresse IP** sont des paramètres obligatoires tandis que **lb-alg** est un paramètre facultatif dont la valeur par défaut est « ROUNDROBIN ».

Utilisez l'attribut **default** pour attribuer une valeur par défaut à un paramètre facultatif. Lors de la création d'une configuration, si un utilisateur ne spécifie aucune valeur, la valeur par défaut est utilisée. Par exemple, pour le paramètre **lb-alg**, la valeur par défaut est ROUNDROBIN.

Utilisez l'attribut **allowed-values** pour définir des valeurs spécifiques parmi lesquelles un utilisateur peut choisir lors de la création d'une configuration. Dans cet exemple, vous avez spécifié deux valeurs pour le paramètre **lb-alg** : ROUNDROBIN et LEASTCONNECTION.

Lorsque vous importez votre StyleBook et l'utilisez, Citrix ADM affiche un formulaire avec ces trois paramètres. Les champs affichés pour name et ip permettent la saisie du type de valeur de chaîne et d'adresse IP, et le champ lb-alg est affiché sous forme de liste déroulante avec ROUNDROBIN sélectionné comme valeur par défaut.

#### Remarque

Outre les types intégrés, un paramètre peut avoir un autre type StyleBook. C'est une façon de réutiliser les paramètres définis dans d'autres StyleBooks.

## Composants

La dernière section de ce StyleBook s'appelle la section Composants et est considérée comme la section la plus importante du StyleBook. Dans cette section, vous définissez les objets de configuration qui doivent être créés par le StyleBook.

Pour cet exemple, vous devez écrire la section des composants comme suit :

```
1 components:
2   -
3     name: lbserver-comp
4     type: ns::lbserver
5     properties:
6       name: $parameters.name
7       servicetype: HTTP
8       ipv46: $parameters.ip
9       port: 80
10      lbmethod: $parameters.lb-alg
11 <!--NeedCopy-->
```

Cet exemple ne contient qu'un seul composant. Les principaux attributs d'un composant sont le nom, le type et les propriétés. Le type d'un composant détermine les propriétés qu'il fournit. Les composants sont de deux types :

- **Type intégré.** Ce type est fourni par le système et vous n'avez pas à le définir. Par exemple, les types d'entités NITRO « lbvserver » ou « servicegroup ». Dans cet exemple, vous utilisez un type de composant intégré.
- **Type composite.** Ce type est le StyleBook que vous avez créé et importé dans Citrix ADM, ou le StyleBook par défaut fourni avec Citrix ADM. Vous pouvez en savoir plus sur les StyleBooks composites dans [Créer un StyleBook composite](#).

Dans cet exemple, vous avez défini un composant appelé **lbvserver-comp**. Ce composant est du type **ns : :lbvserver** (un type Nitro intégré), où « ns » est le préfixe qui fait référence à l'espace de noms netscaler.nitro.config et à la version 10.5 que vous avez spécifiés dans la section import-stylebooks, et « lbvserver » est une ressource Nitro dans cet espace de noms.

Les **propriétés** définies ici sont les attributs de la ressource « lbvserver ». Pour en savoir plus sur toutes les ressources Citrix ADC Nitro disponibles et leurs attributs, consultez la [documentation de l'API REST Citrix ADC NITRO](#).

Les propriétés de cette section incluent les attributs obligatoires de la ressource « lbvserver » et vous permettent de spécifier des valeurs pour ces attributs. Dans cet exemple, vous spécifiez des valeurs statiques pour le type de service et le port alors que les propriétés name, ipv46 et lbmethod obtiennent leurs valeurs à partir des paramètres d'entrée. Dans le reste du StyleBook, vous pouvez faire référence aux noms de paramètres définis dans la section parameters à l'aide de l'expression **\$parameters.<parameter-name>**, par exemple, **\$parameters.ip**.

#### Remarque

Par convention, le préfixe « ns » est toujours utilisé pour désigner un espace de noms Citrix ADC Nitro dans la section « import-stylebooks ». Bien que ce ne soit pas obligatoire, Citrix recommande d'utiliser la même convention dans vos propres StyleBooks pour des raisons de cohérence.

## Créez votre StyleBook

Maintenant que vous avez défini toutes les sections requises de ce StyleBook, regroupez-les toutes pour créer votre premier StyleBook. Copiez et collez le contenu du StyleBook dans un éditeur de texte, puis enregistrez le fichier sous le **nom lb-vserver.yaml**. Citrix vous recommande d'utiliser le validateur YAML intégré dans StyleBooks pour valider et importer le contenu YAML.

Le contenu complet du fichier lb-vserver.yaml est reproduit ci-dessous :

```
1 name: lb-vserver
2 namespace: com.example.stylebook
```



```
3 version: "1.0"
4 display-name: Load Balancing Virtual Server (HTTP)
5 description: "This stylebook defines a very simple load balancing HTTP
  virtual server configuration"
6 schema-version: "1.0"
7
8 import-stylebooks:
9   -
10    namespace: netscaler.nitro.config
11    version: "10.5"
12    prefix: ns
13   -
14    namespace: com.citrix.adc.stylebooks
15    version: "1.0"
16    prefix: stlb
17
18 parameters:
19   -
20    name: name
21    label: "Application Name"
22    description: "Give a name to the application configuration."
23    type: string
24    required: true
25   -
26    name: vip-ipaddress
27    label: "Load Balancer IP Address"
28    description: "The Application VIP that clients access"
29    type: ipaddress
30    required: true
31   -
32    name: lb-alg
33    label: LB Algorithm
34    description: Load Balancing Algorithm
35    type: string
36    default: ROUNDROBIN
37    allowed-values:
38     - ROUNDROBIN
39     - LEAST-CONNECTION
40
41 components:
42   -
43    name: lbserver-comp
44    description: This StyleBook component (a Builtin Nitro StyleBook)
45    builds a Citrix ADC load balancing virtual server configuration
46    object.
47    type: ns::lbserver
48    properties:
49     name: $parameters.name
50     ipv46: $parameters.vip-ipaddress
51     lbmethod: $parameters.lb-alg
52     servicetype: HTTP
53     port: 80
54 <!--NeedCopy-->
```

Pour commencer à utiliser votre StyleBook pour créer des configurations, vous devez l'importer dans Citrix ADM, puis l'utiliser. Pour plus d'informations, consultez [Comment utiliser des StyleBooks définis par l'utilisateur](#).

Vous pouvez également importer ce StyleBook dans d'autres StyleBooks (à l'aide de la construction Import-Stylebooks). Vous pouvez également modifier ce StyleBook pour inclure plus de paramètres et de composants comme décrit dans la section suivante.

## StyleBook pour créer une configuration d'équilibrage de charge de base

February 1, 2024

Dans l'exemple précédent, vous avez créé un StyleBook de base pour créer un serveur virtuel d'équilibrage de charge. Vous pouvez enregistrer ce StyleBook sous un autre nom, puis le mettre à jour pour inclure des paramètres et des composants supplémentaires pour une configuration de base d'équilibrage de charge. Enregistrez ce fichier StyleBook sous le **nom basic-lb-config.yaml**.

Dans cette section, vous allez concevoir un nouveau StyleBook qui crée une configuration d'équilibrage de charge comprenant un serveur virtuel d'équilibrage de charge, un groupe de services et une liste de services. Il lie également les services au groupe de services et lie le groupe de services au serveur virtuel.

### En-tête

Pour créer ce StyleBook, vous devez commencer par mettre à jour la section d'en-tête. Cette section est similaire à celle que vous avez créée pour le serveur virtuel d'équilibrage de charge StyleBook. Dans la section d'en-tête, remplacez la valeur du **nom** par basic-lb-config. Mettez également à jour **la description** et le **nom d'affichage** pour décrire correctement ce StyleBook. Il n'est pas nécessaire de modifier l'espace de **noms** et les valeurs de **version**. Comme vous avez modifié le nom, la combinaison du nom, de l'espace de noms et de la version crée un identifiant unique pour ce StyleBook dans le système.

```
1 name: basic-lb-config
2 description: This StyleBook defines a simple load balancing
  configuration.
3 display-name: Load Balancing Configuration
4 namespace: com.example.stylebooks
5 schema-version: "1.0"
6 version: "0.1"
7 <!--NeedCopy-->
```

## Importer des StyleBooks

La section import-stylebooks reste la même. Il fait référence à l'espace de noms netscaler.nitro.config pour utiliser les objets de configuration Nitro.

```
1 import-stylebooks:  
2 -  
3 namespace: netscaler.nitro.config  
4 prefix: ns  
5 version: "10.5"  
6 <!--NeedCopy-->
```

## Paramètres

Vous devez mettre à jour la section des paramètres pour ajouter deux paramètres supplémentaires pour définir la liste des services ou serveurs et le port sur lequel les services écoutent. Les trois premiers paramètres, name, ip et lb-alg, restent les mêmes.

```
1 parameters:  
2 -  
3 name: name  
4 type: string  
5 label: Application Name  
6 description: Name of the application configuration  
7 required: true  
8 -  
9 name: ip  
10 type: ipaddress  
11 label: Application Virtual IP (VIP)  
12 description: Application VIP that the clients access  
13 required: true  
14 -  
15 name: lb-alg  
16 type: string  
17 label: LoadBalancing Algorithm  
18 description: Choose the load balancing algorithm used for load  
19 balancing client requests between the application servers.  
20 allowed-values:  
21 - ROUNDROBIN  
22 - LEASTCONNECTION  
23 default: ROUNDROBIN  
24 -  
25 name: svc-servers  
26 type: ipaddress[]  
27 label: Application Server IPs  
28 description: The IP addresses of all the servers of this application  
29 required: true  
30 -  
31 name: svc-port  
32 type: tcp-port
```

```

32   label: Server Port
33   description: The TCP port open on the application servers to receive
      requests.
34   default: 80
35   <!--NeedCopy-->

```

Dans cet exemple, le paramètre **svc-servers** est ajouté pour accepter une liste d'adresses IP des services qui représentent les serveurs principaux de l'application. Ceci est un paramètre obligatoire comme indiqué par **requis : true**. Le deuxième paramètre, **svc-port**, indique le numéro de port sur lequel les serveurs écoutent. Le numéro de port par défaut est 80 pour le paramètre **svc-port**, s'il n'est pas spécifié par l'utilisateur.

## Composants

Vous devez également mettre à jour la section des composants pour définir des composants supplémentaires afin qu'ils utilisent les deux nouveaux paramètres et créent la configuration complète d'équilibrage de charge.

Pour cet exemple, vous devez écrire la section des composants comme suit :

```

1  components:
2  -
3    name: lbserver-comp
4    type: ns::lbserver
5    properties:
6      name: $parameters.name + "-lb"
7      servicetype: HTTP
8      ipv46: $parameters.ip
9      port: 80
10     lbmethod: $parameters.lb-alg
11
12  components:
13  -
14     name: svcg-comp
15     type: ns::servicegroup
16     properties:
17       name: $parameters.name + "-svcgrp"
18       servicetype: HTTP
19
20  components:
21  -
22     name: lbserver-svg-binding-comp
23     type: ns::lbserver_servicegroup_binding
24     properties:
25       name: $parent.parent.properties.name
26       servicegroupname: $parent.properties.name
27  -
28     name: members-svcg-comp
29     type: ns::servicegroup_servicegroupmember_binding
30     repeat: $parameters.svc-servers

```

```
31  repeat-item: srv
32  properties:
33    ip: $srv
34    port: str($parameters.svc-port)
35    servicegroupname: $parent.properties.name
36  <!--NeedCopy-->
```

Dans cet exemple, le composant d'origine **lbvserver-comp** (de l'exemple précédent) possède désormais un composant enfant appelé **svcg-comp**. De plus, le composant **svcg-comp** contient deux composants enfants. L'imbrication d'un composant dans un autre composant permet au composant imbriqué de créer des objets de configuration en se référant aux attributs du composant parent. Le composant imbriqué peut créer un ou plusieurs objets pour chaque objet créé dans le composant parent.

Le composant **svcg-comp** est utilisé pour créer un groupe de services sur l'instance Citrix ADC en utilisant les valeurs fournies pour les attributs de la ressource « servicegroup ». Dans cet exemple, vous spécifiez une valeur statique pour le type de service, tandis que name obtient sa valeur à partir du paramètre d'entrée. Vous faites référence au **nom** du paramètre défini dans la section des paramètres en utilisant la notation **\$parameters.name + "-svcgrp"**, où **-svcgrp** est ajouté (concaténé) au nom défini par l'utilisateur.

Le composant **svcg-comp** a deux composants enfants, **lbvserver-svg-binding-comp** et **members-svcg-comp**.

Le premier composant enfant, **lbvserver-svg-binding-comp**, est utilisé pour lier un objet de configuration entre le groupe de services créé par son composant parent et le serveur virtuel d'équilibrage de charge (lbvserver) créé par le composant parent du parent. La notation \$parent, également appelée référence parente, est utilisée pour faire référence aux entités dans les composants parents. Par exemple, **servicegroupname : \$parent.properties.name** fait référence au groupe de services créé par le composant parent **svcg-comp**, et **name : \$parent.parent.properties.name** fait référence au serveur virtuel créé par le composant parent **lbvserver-comp** du parent.

Le composant **members-svcg** est utilisé pour lier des objets de configuration entre la liste des services au groupe de services créé par le composant parent. La création de plusieurs objets de configuration de liaison est réalisée en utilisant la construction de **répétition** de StyleBook pour parcourir la liste des serveurs spécifiés dans le paramètre **svc-servers**. Au cours de l'itération, ce composant StyleBook crée un objet de configuration Nitro de type **servicegroup\_servicegroupmember\_binding** pour chaque service (appelé srv dans la construction **repeat-item**) du groupe de services, et il définit l'attribut **IP de chaque objet de configuration Nitro sur l'adresse IP** du serveur correspondant.

En général, vous pouvez utiliser les constructions **repeat** et **repeat-item** d'un composant pour que ce composant génère plusieurs objets de configuration du même type. Vous pouvez attribuer un nom de variable à la construction **repeat-item**, par exemple, srv, pour désigner la valeur actuelle dans l'itération. Ce nom de variable est référencé dans les propriétés du même composant ou dans les composants enfants comme **\$<varname>**, par exemple \$srv.

Dans l'exemple ci-dessus, vous avez utilisé l'imbrication de composants les uns aux autres pour construire facilement cette configuration. Dans ce cas particulier, l'imbrication des composants n'était pas le seul moyen de créer la configuration. Vous auriez pu obtenir le même résultat sans imbrication, comme indiqué ci-dessous :

```
1 components:
2 -
3   name: members-svcg-comp
4   type: ns::servicegroup_servicegroupmember_binding
5   repeat: $parameters.svc-servers
6   repeat-item: srv
7   properties:
8     ip: $srv
9     port: str($parameters.svc-port)
10    servicegroupname: $components.svcg-comp.properties.name
11 -
12  name: lbvserver-svg-binding-comp
13  type: ns::lbvserver_servicegroup_binding
14  properties:
15    name: $components.lbvserver-comp.properties.name
16    servicegroupname: $components.svcg-comp.properties.name
17 -
18  name: lbvserver-comp
19  type: ns::lbvserver
20  properties:
21    name: $parameters.name + "-lb"
22    servicetype: HTTP
23    ipv46: $parameters.ip
24    port: 80
25    lbmethod: $parameters.lb-alg
26 -
27  name: svcg-comp
28  type: ns::servicegroup
29  properties:
30    name: $parameters.name + "-svcgrp"
31    servicetype: HTTP
32 <!--NeedCopy-->
```

Ici, tous les composants sont au même niveau (c'est-à-dire qu'ils ne sont pas imbriqués) mais le résultat obtenu (la configuration Citrix ADC générée) est le même que celui des composants imbriqués utilisés précédemment. En outre, l'ordre dans lequel les composants sont déclarés dans le StyleBook n'a pas d'incidence sur l'ordre de création des objets de configuration. Dans cet exemple, les composants **svcg-comp** et **lbvserver-comp**, même s'ils ont été déclarés en dernier, doivent être construits avant de générer le deuxième composant **lbvserver-svg-binding-comp** car le second composant contient des références directes à ces composants.

#### Remarque

Par convention, les noms des StyleBooks, des paramètres, des substitutions, des composants

et des sorties sont en minuscules. Lorsqu'ils contiennent plusieurs mots, ils sont séparés par un caractère « - ». Par exemple, « lb-bindings », « app-name », « rewrite-config », etc. Une autre convention consiste à suffixer les noms des composants avec la chaîne « -comp ».

## Sorties

La dernière section que vous pouvez ajouter au nouveau StyleBook est la section des sorties dans laquelle vous spécifiez ce que ce StyleBook expose à ses utilisateurs (ou dans d'autres StyleBooks) après avoir été utilisé pour créer une configuration. Par exemple, vous pouvez spécifier dans la section des sorties d'exposer les objets de configuration lbserver et servicegroup qui seraient créés par ce StyleBook.

```
1 outputs:
2 -
3   name: lbserver-comp
4   value: $components.lbserver-comp
5   description: The component that builds the Nitro lbserver
6               configuration object
7 -
8   name: servicegroup-comp
9   value: $components.svcg-comp
10  description: The component that builds the Nitro servicegroup
11              configuration object
12 <!--NeedCopy-->
```

La section des sorties d'un StyleBook est facultative. Un StyleBook n'a pas besoin de renvoyer des sorties. Cependant, en renvoyant certains composants internes sous forme de sorties, cela donne aux StyleBooks qui importent ce StyleBook plus de flexibilité, comme vous pouvez le constater lors de la création d'un StyleBook composite.

### Remarque

Il est recommandé d'exposer un composant entier du StyleBook dans la section des sorties, plutôt qu'une seule propriété d'un composant (par exemple, exposez l'intégralité de \$components.lbserver-comp plutôt que le nom \$components.lbserver-comp.properties.name). Ajoutez également une description à la sortie expliquant ce que représente la sortie spécifique.

## Créez votre StyleBook

Maintenant que vous avez défini toutes les sections requises de ce StyleBook, regroupez-les toutes pour créer votre second StyleBook. Vous avez déjà enregistré ce fichier StyleBook en tant que **basic-lb-config.yaml**. Citrix vous recommande d'utiliser le validateur YAML intégré à la page StyleBooks pour valider et importer le contenu YAML.

Le contenu complet du fichier **basic-lb-config.yaml** est reproduit ci-dessous :

```
1 name: basic-lb-config
2 namespace: com.example.stylebooks
3 version: "0.1"
4 display-name: Load Balancing Configuration
5 description: This StyleBook defines a simple load balancing
  configuration.
6 schema-version: "1.0"
7
8 import-stylebooks:
9   -
10    namespace: netscaler.nitro.config
11    version: "10.5"
12    prefix: ns
13  parameters:
14    -
15    name: name
16    type: string
17    label: Application Name
18    description: Give a name to the application configuration.
19    required: true
20    -
21    name: ip
22    type: ipaddress
23    label: Application Virtual IP (VIP)
24    description: The Application VIP that clients access
25    required: true
26    -
27    name: lb-alg
28    type: string
29    label: LoadBalancing Algorithm
30    description: Choose the loadbalancing algorithm (method) used for
  loadbalancing client requests between the application servers.
31    allowed-values:
32      - ROUNDROBIN
33      - LEASTCONNECTION
34    default: ROUNDROBIN
35    -
36    name: svc-servers
37    type: ipaddress[]
38    label: Application Server IPs
39    description: The IP addresses of all the servers of this application
40    required: true
41
42  components:
43    -
44    name: lbserver-comp
45    type: ns::lbserver
46    properties:
47      name: $parameters.name + "-lb"
48      servicetype: HTTP
49      ipv46: $parameters.ip
50      port: 80
51      lbmethod: $parameters.lb-alg
```



```
52 -
53   name: svcg-comp
54   type: ns::servicegroup
55   properties:
56     servicegroupname: $parameters.name + "-svcgrp"
57     servicetype: HTTP
58
59 -
60   name: lbvserver-svg-binding-comp
61   type: ns::lbvserver_servicegroup_binding
62   properties:
63     name: $components.lbvserver-comp.properties.name
64     servicegroupname: $components.svcg-comp.properties.servicegroupname
65 -
66   name: members-svcg-comp
67   type: ns::servicegroup_servicegroupmember_binding
68   repeat: $parameters.svc-servers
69   repeat-item: srv
70   properties:
71     ip: $srv
72     port: 80
73     servicegroupname: $components.svcg-comp.properties.servicegroupname
74 outputs:
75 -
76   name: lbvserver-comp
77   value: $components.lbvserver-comp
78   description: The component that builds the Nitro lbvserver
79               configuration object
79 -
80   name: servicegroup-comp
81   value: $components.svcg-comp
82   description: The component that builds the Nitro servicegroup
83               configuration object
83 <!--NeedCopy-->
```

Pour commencer à utiliser votre StyleBook pour créer des configurations, vous devez l'importer dans Citrix ADM, puis l'utiliser. Pour plus d'informations, consultez [Comment utiliser des StyleBooks définis par l'utilisateur](#).

Vous pouvez également importer ce StyleBook dans d'autres StyleBooks et utiliser ses propriétés comme décrit dans la section suivante.

## Créer un StyleBook composite

February 1, 2024

Une caractéristique importante et puissante de StyleBooks est qu'ils peuvent être utilisés comme blocs de construction pour d'autres StyleBooks. Un StyleBook peut être importé dans un autre Style-

Book et il peut être considéré comme un **type** utilisé par les composants du second StyleBook, similaire à un StyleBook intégré à Nitro.

Par exemple, vous pouvez utiliser le StyleBook **basic-lb-config** que vous avez créé dans la section précédente, pour créer un autre StyleBook appelé **composite-example** . Pour utiliser le StyleBook « basic-lb-config », vous devez l'importer dans le nouveau StyleBook dans la section import-stylebooks.

## Créez votre StyleBook

Le nouveau StyleBook se présente comme suit :

```
1 name: composite-example
2 namespace: com.example.stylebooks
3 version: "0.1"
4 display-name: Load Balancing Virtual Server (HTTP/RoundRobin)
5 description: This StyleBook defines a RoundRobin load balancing
6               configuration with a monitor.
7 schema-version: "1.0"
8 import-stylebooks:
9   -
10    namespace: netscaler.nitro.config
11    version: "10.5"
12    prefix: ns
13   -
14    namespace: com.example.stylebooks
15    version: "0.1"
16    prefix: stlb
17 parameters:
18   -
19    name: name
20    type: string
21    label: Application Name
22    description: Give a name to the application configuration.
23    required: true
24   -
25    name: ip
26    type: ipaddress
27    label: Application Virtual IP (VIP)
28    description: The Application VIP that clients access
29    required: true
30   -
31    name: svc-servers
32    type: ipaddress[]
33    label: Application Server IPs
34    description: The IP addresses of all the servers of this
35    application
36    required: true
37   -
38    name: response-code
```

```

38     type: string[]
39     label: List of Response Codes
40     description: List of Response Codes - Provide a list of response
         codes in integer.
41
42     components:
43     -
44         name: basic-lb-comp
45         type: stlb::basic-lb-config
46         description: This component's type is another StyleBook that builds
         the NetScaler lbvserver, servicegroups and services
         configuration objects.
47         properties:
48             name: $parameters.name
49             ip: $parameters.ip
50             svc-servers: $parameters.svc-servers
51     -
52         name: monit-comp
53         type: ns::lbmonitor
54         description: This component is a basic Nitro type (a Builtin
         StyleBook) that builds the NetScaler monitor configuration
         object.
55         properties:
56             monitorname: $parameters.name + "-mon"
57             type: HTTP
58             respcode: $parameters.response-code
59             httprequest: "'GET /'"
60             lrtm: ENABLED
61             secure: "YES"
62
63         components:
64         -
65             name: monit-svcgrp-bind-comp
66             type: ns::servicegroup_lbmonitor_binding
67             properties:
68                 servicegroupname: $components.basic-lb-comp.outputs.
                 servicegroup-comp.properties.servicegroupname
69                 monitor_name: $parent.properties.monitorname
70 <!--NeedCopy-->

```

Dans la section `import-stylebooks`, vous importez le StyleBook `basic-lb-config` en utilisant son espace de noms et sa version, désignés par le préfixe « `stlb` ».

Dans la section `Composants`, deux composants sont définis. Le premier composant est de type **stlb :basic-lb-config**, où « `basic-lb-config` » est le nom du StyleBook que vous avez créé dans [StyleBook pour créer une configuration d'équilibrage de charge de base](#). Les propriétés définies pour ce composant correspondent aux paramètres obligatoires déclarés dans le StyleBook `basic-lb-config`. Vous pouvez toutefois utiliser n'importe quel paramètre du StyleBook (obligatoire et facultatif). Au lieu de reconstruire un serveur `lbvserver`, un groupe de services et des liaisons de service et de groupe de services, vous importez le StyleBook qui fait tout cela en tant que composant et vous l'utilisez pour créer ces objets de configuration dans le nouveau StyleBook.

StyleBook ajoute un deuxième composant, « monit-comp », qui utilise les attributs de la ressource Nitro « lbmonitor » (un StyleBook intégré) pour créer un objet de configuration de moniteur. Il possède également un sous-composant « monit-svcgrp-bind-comp » pour créer l'objet de configuration de liaison qui lie le moniteur au groupe de services créé dans le premier composant. **Étant donné que le composant servicegroup créé dans le StyleBook « basic-lb-config » est exposé en tant que sortie, ce StyleBook peut y accéder à l'aide de l'expression `$components.basic-lb-comp.outputs.servicegroup-comp`.** Ceci est un exemple de la façon dont la section des sorties peut être utilisée par les StyleBooks d'importation pour avoir accès aux composants des StyleBooks importés auxquels ils n'auraient pas pu accéder autrement.

Ensuite, copiez et collez le contenu du StyleBook dans un éditeur de texte, puis enregistrez le fichier sous le **nom composite-exemple.yaml**. Assurez-vous de valider le contenu YAML avant d'importer le fichier dans Citrix ADM. Ensuite, importez-le dans Citrix ADM et créez une ou plusieurs configurations à l'aide de ce StyleBook.

Citrix vous recommande d'utiliser le validateur YAML intégré dans StyleBooks pour valider et importer le contenu YAML.

## Utiliser les attributs de l'interface graphique dans un StyleBook personnalisé

February 1, 2024

Vous pouvez ajouter des attributs GUI dans la section Paramètres de votre StyleBook pour rendre les champs intuitifs lorsqu'ils sont affichés sur Citrix Application Delivery Management (ADM).

**Exemple.** Vous pouvez ajouter un nom descriptif au paramètre à l'aide de l'attribut `label` et ajouter une infobulle pour ce paramètre à l'aide de l'attribut `description`.

```
1 name: ip
2 label: Virtual Server IP Address
3 description: IP address of the virtual server that represents the load
   balanced application.
4 type: ipaddress
5 required: true
6 <!--NeedCopy-->
```

**Exemple.** Si vous avez un paramètre de type object, vous pouvez définir la mise en page à l'aide de l'attribut `gui`. Dans cet exemple, la mise en page est un objet pliable où les champs sont affichés en deux colonnes.

```
1 name: svcg-advanced
2 label: Advanced Application Server Settings
3 type: object
```

```

4 required: false
5 gui:
6   collapse_pane: true
7   columns: 2
8 <!--NeedCopy-->

```

**Exemple.** Vous pouvez également afficher une vue récapitulative d'un paramètre de type object [] (liste d'objets) sous forme de tableau avec les paramètres internes représentant les colonnes. Pour inclure ou exclure un paramètre interne de la vue récapitulative, vous pouvez utiliser l'attribut `summary_display` dans la section de l'interface graphique comme suit :

```

1 name: settings
2 label: Settings
3 type: object[]
4 parameters:
5   -
6     name: name
7     label: Name
8     description: Name of this setting
9     type: string
10    gui:
11      summary_display: true
12 <!--NeedCopy-->

```

**Exemple.** Certains StyleBooks sur Citrix ADM sont utilisés uniquement comme blocs de construction pour d'autres StyleBooks. Vous pouvez également ne pas vouloir que les utilisateurs créent des configurations directement à partir de ces StyleBooks. Parce que ces StyleBooks doivent être utilisés dans le cadre d'autres StyleBooks. Marquez le StyleBook comme privé pour vous assurer que le StyleBook n'est pas utilisé directement pour créer des configurations dans l'interface graphique Citrix ADM.

```

1 name: basic-lb-config
2 description: This stylebook defines a simple load balancing
   configuration.
3 display-name: Load Balancing Configuration
4 namespace: com.example.stylebooks
5 private: true
6 schema-version: "1.0"
7 version: "0.1"
8 <!--NeedCopy-->

```

## Utiliser des StyleBooks personnalisés

February 1, 2024

Après avoir créé votre StyleBook, vous devez l'importer dans Citrix ADM pour l'utiliser. Citrix ADM vous permet d'importer un seul StyleBook sous forme YAML ou plusieurs fichiers StyleBook YAML sous la

forme d'un bundle dans un formulaire .zip, .tgz ou .gz. Le système Citrix ADM valide vos StyleBooks lors de l'importation. Le Stylebook est maintenant prêt à être utilisé pour créer des configurations.

Citrix ADM dispose également d'un éditeur YAML intégré que vous pouvez utiliser pour composer le contenu de StyleBook YAML. L'éditeur YAML vous permet de valider vos constructions YAML à partir de l'interface utilisateur graphique Citrix ADM. Vous n'avez pas besoin d'utiliser un outil distinct pour ces vérifications de validation. Le contenu est validé par rapport aux normes YAML et tout écart est mis en évidence. Vous pouvez ensuite corriger le contenu et essayer d'importer le StyleBook dans Citrix ADM. L'éditeur YAML intégré offre deux avantages lors de la rédaction de votre propre StyleBook.

- **Code couleur.** L'éditeur affiche le contenu StyleBook analysé selon les directives YAML, et le code couleur vous aide à différencier facilement les clés et les valeurs définies dans le contenu YAML.
- **Validation YAML.** Le contenu est validé pour toutes les erreurs YAML lorsque vous saisissez et toute déviation est immédiatement mise en surbrillance. Cela vous permet d'écrire du texte conforme aux directives YAML avant même d'importer le StyleBook dans Citrix ADM. Actuellement, l'éditeur valide le contenu conformément aux directives YAML. Il ne valide pas l'exactitude du code et les erreurs typographiques.

## Importer votre StyleBook

1. Dans Citrix ADM, accédez à **Applications > Configuration > StyleBooks**, puis cliquez sur **Importer un nouveau StyleBook**.
2. Cliquez sur l'une des trois options disponibles pour importer le StyleBook.
  - a) **Dossier.** Sélectionnez le fichier ou l'ensemble de fichiers requis dans votre espace de stockage local.

### Remarque

Dans cet exemple, importez le StyleBook « lb-vserver.yaml » que vous avez créé dans [StyleBook pour créer un serveur virtuel d'équilibrage de charge](#).

The screenshot shows the 'Import StyleBook' dialog box. At the top, there are four radio buttons: 'File' (selected), 'Bundle', 'Raw', and 'Sync Repository'. Below them is the instruction 'Choose a YAML StyleBook file.' A file selection field contains 'lb-server.yml' and a 'Choose File' button. There is also an unchecked checkbox labeled 'Include an icon for the StyleBook'. At the bottom, there are two buttons: 'Create' and 'Close'.

- b) **Forfait.** Citrix ADM vous permet d'importer plusieurs StyleBooks au format YAML. Vous pouvez importer plusieurs fichiers YAML StyleBook compressés au format zip (.zip) ou archive (.tgz, .gz).

The screenshot shows the 'Import StyleBook' dialog box. At the top, there are four radio buttons: 'File', 'Bundle' (selected), 'Raw', and 'Sync Repository'. Below them is the instruction 'Choose zip (.zip) or tarball file (.tgz, .gz) bundle that includes multiple StyleBook YAML files.' A file selection field contains 'StyleBooks-yaml.zip' and a 'Choose File' button. There is also an unchecked checkbox labeled 'Include an icon for the StyleBook'. At the bottom, there are two buttons: 'Create' and 'Close'.

- c) **Cru.** Composez le contenu de votre StyleBook dans l'éditeur YAML.

**Remarque**

Lors de la composition de StyleBook, assurez-vous de connaître les points suivants :

- API NITRO
- YAML

Pour plus d'informations sur la façon d'écrire vos propres StyleBooks, consultez [Comment créer vos propres StyleBooks](#).

```
1 name: lb-vserver
2 namespace: com.example.stylebook
3 version: "1.0"
4 display-name: Load Balancing Virtual Server (HTTP)
5 description: "This stylebook defines a very simple load balancing HTTP virtual server configuration"
6 schema-version: "1.0"
7
8 import-stylebooks:
9 -
10   namespace: netscaler.nitro.config
11   version: "10.5"
12   prefix: ns
13 -
14   namespace: com.citrix.adc.stylebooks
15   version: "1.0"
16   prefix: stlb
17
18
```

### Remarque

Vous pouvez également copier et coller le contenu à partir d'un fichier YAML StyleBook pour valider le contenu.

### 3. Cliquez sur **Créer**.

Citrix ADM valide désormais votre StyleBook pour toutes les erreurs syntaxiques et sémantiques selon la grammaire StyleBook. Votre StyleBook n'est pas importé dans Citrix ADM s'il y a des erreurs. S'il n'y a pas d'erreur, le StyleBook est importé avec succès et est maintenant répertorié sur la page StyleBooks. Vous pouvez identifier le StyleBook par le nom complet que vous avez défini dans la section d'en-tête du StyleBook.

### Remarque

Si vous importez un ensemble de fichiers, Citrix ADM décompresse le dossier compressé et valide tous les StyleBooks.

Le bundle n'est pas importé même si un fichier StyleBook échoue le test de validation.

Pour plus d'informations sur la grammaire de StyleBook et la syntaxe des différentes constructions et attributs, consultez [StyleBook Grammar](#).

### 4. Pour créer des configurations à partir de ce StyleBook, cliquez sur le lien **Créer une configuration**. Le StyleBook s'ouvre en tant que page d'interface utilisateur sur laquelle vous pouvez



entrer les valeurs de tous les paramètres définis dans ce StyleBook.

5. Spécifiez les valeurs requises pour les paramètres. Dans l'exemple ci-dessous, vous pouvez voir que le **nom de l'application** et les champs d'**adresse IP de l'équilibreur de charge** sont affichés en tant que champs obligatoires et peuvent accepter des valeurs utilisateur. L'**algorithme LB** ne comporte que deux valeurs parmi lesquelles vous pouvez choisir et, par défaut, ROUNDROBIN est sélectionné.
6. Sous **Instances cibles**, cliquez et sélectionnez l'adresse IP de l'instance Citrix ADC sur laquelle vous souhaitez exécuter la configuration. Vous pouvez également déployer la configuration sur plusieurs Citrix ADC, en spécifiant autant d'instances cibles que nécessaire.

Si vous souhaitez consulter les objets de configuration Citrix ADC (Nitro) qui seraient créés sur votre Citrix ADC avant de créer la configuration, cliquez sur **Exécuter à sec**. Si votre configuration est valide, les objets de configuration qui seraient créés sur la base des valeurs que vous avez fournies sont affichés. Dans cet exemple, un seul objet de type lbserver est créé par cet exemple StyleBook. Ce serveur lbserver était le seul composant qui a été défini dans cet exemple de base StyleBook. Vous pouvez ensuite cliquer sur **Créer** pour créer réellement la configuration sur les instances Citrix ADC sélectionnées.

Une fois la création terminée, le nouveau ConfigPack est répertorié sur la page Configurations.

#### Remarque

Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter des instances Citrix ADC récemment découvertes dans Citrix ADM à la liste des instances disponibles dans cette fenêtre.

## Rechercher des StyleBooks personnalisés

Citrix ADM vous permet désormais de rechercher StyleBooks en fonction de leur type. Autrement dit, vous pouvez désormais rechercher des StyleBooks par défaut ou des StyleBooks personnalisés. Cette option est particulièrement utile lorsque vous devez rechercher vos StyleBooks définis par l'utilisateur parmi un grand nombre de StyleBooks par défaut.

### Pour rechercher des StyleBooks personnalisés

1. Dans Citrix ADM, accédez à **Applications > Configurations > StyleBooks**.
2. Cliquez sur l'icône de recherche en haut à droite.
3. Dans la barre de recherche qui apparaît, sélectionnez **Type** dans la première liste, puis **Personnalisé** dans la liste d'options suivante.
4. Citrix ADM affiche uniquement les StyleBooks définis par l'utilisateur.

## Créer un StyleBook pour charger des fichiers vers Citrix ADM

February 1, 2024

Citrix Application Delivery Management (Citrix ADM) StyleBooks vous permettent de créer des configurations Citrix ADC qui peuvent inclure, entre autres, lors du téléchargement de fichiers de n'importe quel type depuis votre système de fichiers local vers l'instance Citrix ADC, à l'aide de l'interface graphique Citrix ADM ou des API. Ces fichiers peuvent être des exemples de fichiers de certificats ou de fichiers de géolocalisation. Vous pouvez également spécifier le répertoire dans lequel télécharger ces fichiers.

### Configuration de StyleBook

Voici un exemple de StyleBook qui décrit comment télécharger un fichier de géolocalisation sur l'instance Citrix ADC. Les fichiers géo sont généralement utilisés dans les configurations GSLB pour définir la proximité statique en fonction de l'emplacement géographique :

### Créez votre StyleBook -1

```
1 name: upload-geolocations
2 namespace: com.citrix.adc.stylebooks.samples
3 version: "1.0"
4 display-name: GeoLocation File Upload
5 description: This StyleBook is used to upload a geolocation file to
   Citrix ADC
6 schema-version: "1.0"
7
8 import-stylebooks:
9 -
10 namespace: netscaler.nitro.config
11 version: "11.1"
12 prefix: ns
13
14 parameters:
15 -
16 name: locationfile
17 label: Location File
18 description: The system file path of the geolocation file on Citrix
   ADM
19 type: file
20 required: true
21
22 components:
23 -
24 name: upload-file-comp
```

```

25 type: ns::systemfile
26 properties:
27     filename: $parameters.locationfile.filename
28     filelocation: "/var/netscaler/inbuilt_db/"
29     filecontent: base64.encode($parameters.locationfile.contents)
30 <!--NeedCopy-->

```

### Remarque

Le paramètre utilisé dans cet exemple est un fichier de type. Vous pouvez importer ce StyleBook dans Citrix ADM et l'utiliser pour télécharger des fichiers de géolocalisation.

Ce StyleBook exige que le fichier soit déjà présent dans Citrix ADM (par exemple, vous l'auriez déjà copié dans Citrix ADM à l'aide d'un utilitaire comme scp).

Si vous souhaitez télécharger un fichier vers des Citrix ADC via Citrix ADM sans le copier au préalable dans le système de fichiers Citrix ADM, vous pouvez créer un StyleBook qui comporte deux paramètres « chaîne », l'un permet de spécifier le nom de fichier à utiliser sur le Citrix ADC et l'autre pour spécifier le contenu de l'objet et utilisez ces deux paramètres dans les composants upload-file-comp. Voici une alternative à StyleBook pour télécharger un fichier de géolocalisation :

## Créez votre StyleBook - 2

```

1 name: upload-geolocations-alt
2 namespace: com.citrix.adc.stylebooks.samples
3 version: "1.0"
4 display-name: GeoLocation File Upload
5 description: This StyleBook is used to upload a geolocation file to
6   Citrix ADC
7 schema-version: "1.0"
8 import-stylebooks:
9   -
10     namespace: netscaler.nitro.config
11     version: "11.1"
12     prefix: ns
13
14 parameters:
15   -
16     name: filename
17     label: Location Filename
18     description: The name of the location file on the Citrix ADC
19     type: string
20     required: true
21   -
22     name: filecontents
23     label: Location File Contents
24     description: The contents of the location file
25     type: string

```

```
26   required: true
27
28   components:
29     -
30       name: upload-file-comp
31       type: ns::systemfile
32       properties:
33         filename: $parameters.filename
34         filelocation: "/var/Citrix ADC/inbuilt_db/"
35         filecontent: base64.encode($parameters.filecontents)
36 <!--NeedCopy-->
```

## Création de configurations pour télécharger des fichiers

La procédure suivante crée une configuration sur une instance Citrix ADC sélectionnée qui téléchargerait un fichier de géolocalisation à l'aide du premier StyleBook décrit ci-dessus.

### Pour créer une configuration pour le téléchargement de fichiers :

1. Dans Citrix ADM, accédez à **Applications > Configuration**, puis cliquez sur **Créer un nouveau**. La page Choisir un StyleBook affiche tous les StyleBooks disponibles dans votre Citrix ADM. Faites défiler vers le bas et sélectionnez le StyleBook que vous avez importé.

Les paramètres du StyleBook apparaissent sous la forme d'une page d'interface utilisateur qui vous permet de saisir les valeurs de tous les paramètres définis dans ce StyleBook.

2. Entrez le nom de l'équilibreur de charge et l'adresse IP virtuelle dans la section des paramètres de base de l'équilibreur de charge.
3. Dans la section **Fichier de localisation**, entrez le nom ou l'emplacement du fichier.

#### Remarque

Assurez-vous que dans Citrix ADM, le fichier se trouve sous le dossier du locataire actuel uniquement. Utilisez n'importe quel protocole de transfert de fichiers pour copier le fichier dans le système de fichiers Citrix ADM.

4. Vous pouvez être invité à fournir vos informations d'identification utilisateur avant d'accéder aux instances cibles.
5. Sélectionnez l'instance Citrix ADC cible sur laquelle la configuration doit être créée, puis cliquez sur **Créer**.

#### Remarque

Citrix vous recommande de sélectionner **Exécuter à sec** pour vérifier les objets de configuration créés sur l'instance cible avant d'exécuter la configuration réelle sur l'instance.

Lorsque la création du configpack est réussie, le fichier est enregistré sur le système de fichiers d'instance Citrix ADC sous l'emplacement : `/var/netscaler/inbuilt_db/`

#### Remarque

Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter des instances Citrix ADC récemment découvertes dans Citrix ADM à la liste des instances disponibles dans cette fenêtre.

### Utilisation de l'API Citrix ADM pour créer un configpack

Vous pouvez également utiliser l'API Citrix ADM pour créer un configpack qui télécharge des fichiers vers l'instance Citrix ADC sélectionnée. Pour plus d'informations sur l'utilisation des API, voir [Comment utiliser l'API pour créer des configurations afin de charger n'importe quel type de fichier](#).

## Créer un StyleBook pour charger des fichiers de certificat SSL et de clé de certificat vers Citrix ADM

February 1, 2024

Lors de la création d'une configuration StyleBook qui utilise le protocole SSL, vous devez télécharger les fichiers de certificat SSL et les fichiers de clé de certificat conformément aux paramètres StyleBook. StyleBook vous permet de télécharger directement les fichiers SSL et les fichiers clés depuis votre système local à l'aide de l'interface graphique Citrix ADM. Vous pouvez également utiliser les API Citrix ADM pour télécharger des fichiers de certificat et des fichiers de clé qui sont déjà gérés par Citrix ADM.

### Configuration de StyleBook

Ce document vous aide à créer votre propre StyleBook - **Serveur virtuel d'équilibrage de charge (SSL)**

avec des composants pour télécharger des certificats SSL et des fichiers clés. Le StyleBook fourni ici à titre d'exemple crée une configuration de serveur virtuel d'équilibrage de charge de base sur l'instance Citrix ADC sélectionnée. La configuration utilise le protocole SSL. Pour créer une configuration à l'aide de ce StyleBook, vous devez fournir le nom et l'adresse IP du serveur virtuel, sélectionner les paramètres de la méthode d'équilibrage de charge et télécharger le fichier de certificat et le fichier de clé de certificat pour le serveur virtuel, ou utiliser un fichier de certificat et un fichier de clé de certificat qui sont déjà présent dans Citrix ADM. Ils sont spécifiés dans la section « paramètres », comme indiqué ci-dessous :

```

1 parameters:
2   -
3     name: name
4     type: string
5     required: true
6   -
7     name: ip
8     type: ipaddress
9     required: true
10  -
11    name: lb-alg
12    type: string
13    allowed-values:
14      - ROUNDROBIN
15      - LEASTCONNECTION
16    default: ROUNDROBIN
17  -
18    name: certificate
19    label: "SSL Certificate File"
20    description: "The file name of the SSL certificate file"
21    type: certfile
22  -
23    name: key
24    label: "SSL Certificate Key File"
25    description: "The file name of the server certificate's private key
26                file"
26    type: keyfile
27  <!--NeedCopy-->

```

Deux composants sont ensuite créés dans la section Composants du StyleBook, comme indiqué ci-dessous. Le composant « my-lbserver-comp » est de type ns : :lbserver, où :

- « ns » est le préfixe qui fait référence à l'espace de noms intégré netscaler.nitro.config et à la version 10.5 que vous avez spécifiés dans la section import-stylebooks.
- « lbserver » est un StyleBook intégré dans cet espace de noms. Il correspond à la ressource serveur virtuel d'équilibrage de charge Citrix ADC NITRO du même nom.

Le deuxième composant « lbserver-certificate-comp » est de type stlb vserver-certs-binds. Le préfixe « stlb » fait référence à l'espace de noms « com.citrix.adc.stylebooks » et à la version 1.0 spécifiée dans la section import-stylebooks du StyleBook. Si l'espace de noms « com.citrix.adc.stylebooks » peut être considéré comme un dossier, « vserver-certs-binds » est un autre StyleBook (ou un fichier) dans ce dossier. Les StyleBooks qui se trouvent dans l'espace de noms « com.citrix.adc.stylebooks » sont expédiés dans le cadre de Citrix ADM.

Le StyleBook « vserver-certs-binds » utilisé par les StyleBooks définis par l'utilisateur vous permet de configurer facilement les certificats en téléchargeant les fichiers de certificat et de clé sur l'instance Citrix ADC cible et en configurant la liaison des fichiers de certificat et de clé vers les serveurs virtuels appropriés. Les propriétés de ce composant sont - le nom du serveur virtuel lb et les noms des certi-

ficats SSL que vous fournissez lors de la création du configpack.

```
1 components:
2   -
3     name: my-lbvserver-comp
4     type: ns::lbvserver
5     properties:
6       name: $parameters.name
7       servicetype: SSL
8       ipv46: $parameters.ip
9       port: 443
10      lbmethod: $parameters.lb-alg
11   -
12     name: lbvserver-certificate-comp
13     type: stlb::vserver-certs-binds
14     description: Binds lbvserver with server certificate
15     properties:
16       vserver-name: $components.my-lbvserver-comp.properties.name
17     certificates:
18       -
19         cert-name: $parameters.name + "-lb-cert"
20         cert-file: $parameters.certificate
21         ssl-inform: PEM
22         key-name: $parameters.name + "-key"
23         key-file: $parameters.key
24 <!--NeedCopy-->
```

Lorsque vous utilisez l'API pour créer une configuration à partir d'un tel StyleBook, utilisez uniquement les noms de fichiers (pas le chemin complet du fichier). Ces fichiers devraient déjà être disponibles dans les dossiers de certificats et de fichiers clés sur Citrix ADM. Le fichier de certificat SSL téléchargé est stocké sur Citrix ADM dans le répertoire /var/mps/tenants/... Le répertoire /ns\_ssl\_certs et le fichier clé du certificat SSL sont stockés dans /var/mps/tenants/... Répertoire /ns\_ssl\_keys dans Citrix ADM.

## Création de configurations pour télécharger des fichiers SSL

La procédure suivante crée une configuration de serveur virtuel d'équilibrage de charge de base sur une instance Citrix ADC sélectionnée à l'aide du protocole SSL du StyleBook spécifié ci-dessus. Vous pouvez utiliser cette procédure pour télécharger les fichiers de certificat SSL et les fichiers de clés de certificat dans Citrix ADM.

### Pour créer une configuration pour le téléchargement de fichiers

1. Dans Citrix ADM, accédez à **Applications > Configuration > StyleBooks**. La page **StyleBooks** affiche tous les StyleBooks disponibles dans votre Citrix ADM.

2. Faites défiler vers le bas et sélectionnez **Serveur virtuel d'équilibrage de charge (SSL)** ou tapez **Serveur virtuel d'équilibrage de charge (SSL)** dans le champ de recherche et appuyez sur la touche **Entrée**.
3. Cliquez sur le lien **Créer une configuration** dans le panneau StyleBook.  
Les paramètres du StyleBook apparaissent sous la forme d'une page d'interface utilisateur qui vous permet de saisir les valeurs de tous les paramètres définis dans ce StyleBook.
4. Entrez le nom de l'équilibreur de charge et l'adresse IP virtuelle dans la section des paramètres de base de l'équilibreur de charge.
5. Dans la section **Paramètres des certificats SSL**, sélectionnez les fichiers correspondants dans votre dossier de stockage local. Vous pouvez également sélectionner les fichiers présents sur le Citrix ADM lui-même.
6. Sélectionnez l'instance Citrix ADC cible sur laquelle la configuration doit être créée, puis cliquez sur **Créer**.

**Remarques :**

Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter des instances Citrix ADC récemment découvertes dans Citrix ADM à la liste des instances disponibles dans cette fenêtre.

Dans Citrix ADM, les StyleBooks par défaut suivants, fournis dans le cadre de Citrix ADM, vous permettent de créer un support SSL en téléchargeant les certificats et clés SSL.

- StyleBook LoadBalancing HTTP/SSL (lb)
- Équilibrage de charge HTTP/SSL (avec moniteurs) StyleBook (lb-mon)
- Application de commutation de contenu HTTP/SSL avec moniteurs (cs-lb-mon)
- Exemple d'application StyleBook utilisant les fonctionnalités CS, LB et SSL (sample-cs-app)

Vous pouvez également créer vos propres StyleBooks qui utilisent les certificats SSL de la même manière que décrite dans le StyleBook ci-dessus

**Créez votre StyleBook**

Le contenu complet du fichier lb-vserver-ssl.yaml est illustré ci-dessous :

```
1 name: lb-vserver-ssl
2 description: "This stylebook defines a load balancing virtual server
3   configuration."
4 display-name: "Load Balancing Virtual Server (SSL)"
5 namespace: com.example.ssl.stylebooks
6 schema-version: "1.0"
7 version: "0.1"
8 import-stylebooks:
```



```
9 -
10 namespace: netScaler.nitro.config
11 prefix: ns
12 version: "10.5"
13 -
14 namespace: com.citrix.adc.stylebooks
15 prefix: stlb
16 version: "1.0"
17
18 parameters:
19 -
20 name: name
21 type: string
22 required: true
23 -
24 name: ip
25 type: ipAddress
26 required: true
27 -
28 name: lb-alg
29 type: string
30 allowed-values:
31 - ROUNDROBIN
32 - LEASTCONNECTION
33 default: ROUNDROBIN
34 -
35 name: certificate
36 label: "SSL Certificate File"
37 description: "The file name of the SSL certificate file"
38 type: certfile
39 -
40 name: key
41 label: "SSL Certificate Key File"
42 description: "The file name of the server certificate's private key
43 file"
44 type: keyfile
45
46 components:
47 -
48 name: my-lbvserver-comp
49 type: ns::lbvserver
50 properties:
51 name: $parameters.name
52 servicetype: SSL
53 ipv46: $parameters.ip
54 port: 443
55 lbmethod: $parameters.lb-alg
56 -
57 name: lbvserver-certificate-comp
58 type: stlb::vserver-certs-binds
59 description: Binds lbvserver with server certificate
60 properties:
61 vserver-name: $ components.my-lbvserver-comp.properties.name
```

```
61     certificates:
62     -
63       cert-name: $parameters.name + "-lb-cert"
64       cert-file: $parameters.certificate
65       ssl-inform: PEM
66       key-name: $parameters.name + "-key"
67       key-file: $parameters.key
68 <!--NeedCopy-->
```

### Utilisation de l'API Citrix ADM pour créer un pack de configuration

Vous pouvez également utiliser l'API Citrix ADM pour créer un configpack qui télécharge les fichiers Cert et Key vers l'instance Citrix ADC sélectionnée. Pour plus d'informations sur l'utilisation des API, consultez [Comment utiliser l'API pour créer des configurations afin de télécharger des fichiers de certificats et de clés](#).

### Affichage des objets définis sur l'instance de Citrix ADC

Une fois le pack de configuration StyleBook (configpack) créé sur Citrix ADM, cliquez sur **Afficher les objets créés** pour afficher tous les objets Citrix ADC créés sur l'instance Citrix ADC cible

Objects

Objects Added on Instance : 10.102.29.200

**Type : lbvserver**

**ipv46** : 10.10.10.1  
**lbmethod** : ROUNDROBIN  
**name** : vserver-1  
**port** : 80  
**servicetype** : SSL

**Type : systemfile**

**filecontent** :  
 L50tL51CRUdJTIBDRVJUSUJZQ0FURS0tL50tCk1JSUMzakNDQWtiZ0F3SUJBJZ0ICQURBTk1Jna3Foa2IH0XcwQkFrc0ZBREEVTVFzd0NRWURWUUVFHRkdKVI6RUWkTUFrR0EXVUVDQk1D  
 WtJFeEV6QVJcz05WQkFJVEWNUtMhbjJoWTJ4agNtRXhEakFNQmdOVk1RCV0Z3Y0d4bApNqJRFRFMU1ERXhOekEYtURZMU5Gb1HEVEUYtURFeE56QTJNRRFKXkZvd1B6RUXnQ  
 WtHQTfVRUJoTUNWVv14CkN6QUcPZ05WQkFnVEFTmHNuk13RVZFRZRUUhFd3B6Wvc1MFIXTnNZWEpoTVE0d0RBWURWUUVLXRdWaGNiQnMKWIRDQm56QU5CZ2XaGtpRzI  
 3MEJBUIVUGQUFPQmpRQXdnWWTdZ1IFQXZFa2FoNjJFRnViTmVgUKnaQk9nN0pEZAo0dVQ1ZDBIM3UycUtaMTQrdzRjVkd5U053L1Rxt2Rhk1F3T0xiaU9OdDBhLzhKRdVyc096Q3N  
 CWHRLdUsyZzRPNhuNi8wc28ZzFJKZTVKeFERnNmNst2VsYjdBpUpFTWVXZDd5WjJGbVfQZHgrZEROMJUxT25aa0pmeXN3NXdSVTKSnpuQnRza3hRcJ8Qbnj2S0tBa0NBd0VbQWFP  
 QjZUQ011akFkQmdOVkhRNEVGZ1FVam5XYVJsalF5N0pQNFozcwp0LzFIWmYVWUprZ3dad1JIEVllwakhQXdxYb0Fvam5XYVJsalF5N0pQNFozc3QvMUhaZi9ZSmtpaFE2UkjNRdH4CkN6  
 QUcPZ05WQkFzVEFSVIRNUXN3Q1FZRFZRUUIFd0pQWVRFVE1CRUdBMVVFQnhNS2MyRnVkr0ZqYkdGeVIURU8KTUF3R0EXVUVDaE1GWWvhCd2jHVONBUUF3REFZRFZSMFRQWV3  
 QXdfQ196QUcXZ05WSFE4RUjBTUNBU3RVFZSgpZSVPjQVlNFFnRUJcQVFEQWdFR01DNEdDV0Nhu0FHRYtF5UJUeUJFoRmgST1pYUJRZMkZzWlhJZ1JYnVaWEpoCmRHvmtJRUS5sY2  
 5ScFpbtGpZWFJSTUEWR0NtCudTSWizRFFQK3VUFBNEdCQU50RWY3aUFSRIRQUlo0b2pjWm0KThIFhGaTE0SGxjK0VpMUnej3R09Ddb3pibWNxemZOZXVSTdRQVISSXQ3Wkh  
 hYWt0Vg0NXLivUhdPzXFlcgpSc2xNTzBnQ1hES3BtuZtXQ3VhdFhBbvHxU2xrTEt3TfHL0pkdTbHSEfkdVhtRvKwNW52M016RWHtVW8xelhJcNfSxYXNcG9QUE14Qks0RmIBNWxs  
 QnAwTwt0tL50tLUVORCDBDRVJUSUJZQ0FURS0tL50tCg==

**fileencoding** : BASE64  
**filelocation** : /nsconfig/ssl  
**filename** : test\_cert.pem

**Type : systemfile**

**filecontent** :  
 L50tL51CRUdJTIBS0UEqUJfJKVfURSBLRvktL50tLQpNSUIDWFEJQkFB50jnUUM4U1jxSHJZUVC1cz0E0vKvKa0U2RHnrTjNpNVbM1i3ZTdhb3BUWGo3RGdovWjKSTNECjIPbzUxcjVEQTR0  
 dUk0MjNSci93a1BtdxC3TUt3RmUxNjRyYURnN0dmcI9TeWpkMUUvS2tuRKQ3chVINTZVWwHMKNNlrUxg1WjN2SmxFV1pDTJNINBnm2juVTZkbvF5L0t6RG5CRIRbk5Nnzj5VEZDdlEr  
 ZXU4b29DUUIEQVFBQgpbB0dBUUIENJZjaDBIRFJ0N5SVjMxc3FjbUZ1NHJCM0Zub25ZN21ZT05s0HZ4WHRqU0owwmdmxGRmZSTW9RMIMyCmU3Z0tjT040Rmo1YwK1N1gwN01aV1  
 dXY1o0aEhrrMm5jMjMjOENLSWSoelhnyfLQJRaMgP1TnUvNE1paVlyahIKNkFROXluV0VMRIBDTjZWwMHFQZwXGYxpVbnZJaH2pMfZGZcsyrUNBY0drVhG0Z0VUDVFEMkIVODhGaU  
 kzVfJOYwpmCvJEMHh2ZVFWMKF6ZVBEYmFnTVFFRINWZVZ3Yk11V3RJM2J0SKdwWXMkUkpleitOdGw0dVprRGVQbnNJZE5ZCjNjWjNsNUp4QWtFQxc5WDDkTDJanVpYAEVpM0Yzdj  
 YwU1U5RWwM4Z01FdvHfZihUendCczpuanjJckRIMUI0enYKR0hSU1ImUedYeHh5cjRKVmC4Q25kcz2VOHEXN0N05UxHUUpBS1Ft3UzYjVSMZByWURCS3BTQmFaaWpsM1NiMgo5Y3  
 VmdkVndVlQci9ZVtBTZVnCEg5dXdYXIHaInQBIR6OTM3UUFNk2gOK2xwZGikS3Q0sKjKNmtR5kjbTHVScIRaUHBEV2UrcWVleGM1MmjzctjZz0ZHC3Z2T3Ivams5QTKu5Qkx5STBJeH  
 FVnlyk25KcdlmeEpXWEI5b3jJZxcKRzV1dmdEWG9zdnly83eklyRUNRRDMzV1HeUw2MjJaRzZverHlXr1o1d1pCTFTv1VjVE1zSngZOW5NUjoZgpkajNwCe10Y3plOFVKvmlPaGtyd  
 WNmmb29tRlNPaUN4ZxhPQXm2MmVEZxNnQotL50tLUVORCBSU0EgUJfJKVfURSBLRvktL50tLQo=

**fileencoding** : BASE64  
**filelocation** : /nsconfig/ssl  
**filename** : test\_cert\_key.pem

**Type : sslcertkey**

**cert** : test\_cert.pem  
**certkey** : vserver-1-lb-cert  
**inform** : PEM  
**key** : test\_cert\_key.pem

**Type : sslvserver\_sslcertkey\_binding**

**certkeyname** : vserver-1-lb-cert  
**vservername** : vserver-1

## Activer l’analyse et configurer les alarmes sur un serveur virtuel défini dans un StyleBook

February 1, 2024

Vous pouvez utiliser la construction des opérations pour configurer Citrix ADM Analytics afin de collecter des enregistrements Appflow sur tout ou partie des transactions de trafic gérées par tout composant de serveur virtuel faisant partie d'un StyleBook. Vous pouvez également utiliser cette construction pour configurer des alarmes afin d'obtenir un aperçu du trafic géré par le serveur virtuel.

L'exemple suivant montre une section Opérations d'un StyleBook :

```
1 operations:
2   analytics:
3     -
4       name: lbvserver-ops
5       properties:
6         target: $components.basic-lb-comp.outputs.lbvserver
7         filter: HTTP.REQ.URL.CONTAINS("catalog")
8     -
9   alarms:
10    -
11      name: lbvserver-alarm
12      properties:
13        target: $outputs.lbvserver
14        email-profile: $parameters.emailprofile
15        sms-profile: "NetScalerSMS"
16
17    rules:
18      -
19        metric: "total_requests"
20        operator: "greaterthan"
21        value: 25
22        period-unit: $parameters.period
23      -
24        metric: "total_bytes"
25        operator: "lessthan"
26        value: 60
27        period-unit: "day"
28 <!--NeedCopy-->
```

Les attributs de la section Analytics sont utilisés pour demander à la fonctionnalité d'analyse Citrix ADM de collecter des enregistrements d'appflow sur un composant de serveur virtuel identifié par la propriété cible. Vous pouvez également spécifier une propriété de filtre qui accepte une expression de stratégie Citrix ADC pour filtrer les demandes pour lesquelles des enregistrements appflow sont collectés sur le serveur virtuel.

Lorsqu'un configpack est créé à partir de ce StyleBook, la fonctionnalité d'analyse Citrix ADM est configurée pour collecter les enregistrements appflow sur les serveurs virtuels qui ont été spécifiés lors de leur création lors de la création d'un configpack.

Les attributs de la section alarmes permettent de définir des seuils pour générer des alarmes et envoyer des notifications sur le serveur virtuel identifié par la propriété cible. Dans l'exemple ci-dessus, les propriétés email-profile et sms-profile sont utilisées pour spécifier où les notifications doivent être envoyées. La section Règles définit les seuils. Par exemple, si le nombre total de demandes traitées

par le serveur virtuel est supérieur à 25 et pour une période définie par l'utilisateur, une alarme est définie et une notification est envoyée. L'«unité de période » indique la fréquence à laquelle une alarme est déclenchée. Il peut prendre la valeur du jour, de l'heure ou de la semaine.

Vous pouvez utiliser les opérateurs suivants pour comparer la valeur de mesure à la valeur de seuil :

- “greaterthan”for “>”
- “lessthan”for “<”
- “greaterthanequal”for “>=”
- « lessthanequal » pour « <= »

Notez que StyleBooks utilise des noms d'API pour les mesures et non pas les noms affichés sur l'interface graphique d'analyse Citrix ADM.

Pour savoir comment afficher et analyser les données collectées sur des serveurs virtuels créés dans le cadre d'un configpack, consultez la documentation d'analyse Citrix ADM.

## Rôles d'instance

January 23, 2024

Dans Citrix Application Delivery Management (ADM), il peut y avoir un scénario dans lequel vous devez configurer plusieurs instances Citrix ADC pour une seule application, mais également dans lequel chaque instance ADC nécessite une configuration différente pour y être déployée. Un exemple de ce cas est le Microsoft Skype for Business StyleBook par défaut.

StyleBooks permet actuellement de créer un configpack et d'appliquer la même configuration sur plusieurs instances Citrix ADC. Un tel scénario où la configuration est identique sur toutes les instances ADC, peut être appelé configuration symétrique.

Désormais, avec la fonctionnalité « rôles d'instance » de StyleBooks, vous pouvez créer une configuration asymétrique, c'est-à-dire un pack de configuration qui peut être appliqué sur plusieurs instances ADC, mais avec des configurations différentes sur différentes instances ADC.

Lorsqu'une fonctionnalité StyleBook avec des rôles d'instance est utilisée pour créer un configpack, chaque instance ADC d'un configpack peut se voir attribuer un rôle différent. Ce rôle détermine les objets de configuration du configpack que l'instance ADC recevra.

### Points à noter :

- L'ensemble des rôles d'instance dans un StyleBook sont définis lors de la création du StyleBook.
- Les rôles sont attribués à une instance ADC spécifique lors de la création ou de la mise à jour du configpack.

## Section Rôles de cible

Une nouvelle section dans un StyleBook appelée « rôles cibles » est introduite, dans laquelle tous les rôles pris en charge par le StyleBook sont déclarés.

Cette section est généralement placée après la section « Import-StyleBooks » d'un StyleBook et avant la section des paramètres.

Dans l'exemple StyleBook suivant, deux rôles sont définis dans la section « rôles cibles » : A et B.

```
1 target-roles:
2
3   -
4     name: A
5     name: B
6     min-targets: 2
7     max-targets: 5
8 <!--NeedCopy-->
```

Vous pouvez voir que le rôle B définit également deux sous-propriétés facultatives, min-targets et max-targets.

Bien que ces deux sous-propriétés soient facultatives, min-targets spécifie le nombre minimum obligatoire d'instances ADC auxquelles ce rôle doit être attribué lors de la création d'un configpack à partir de ce StyleBook, et max-targets spécifie le nombre maximum d'instances ADC auxquelles ce rôle peut être attribué lors de la création d'un configpack à partir de ce StyleBook.

Si ces sous-propriétés ne sont pas spécifiées, le nombre d'instances ADC pouvant être configurées pour ce rôle n'est pas limité. Si min-targets = 0, la configuration associée à ce rôle est facultative et si min-targets = 1, cette configuration est obligatoire et au moins une instance ADC doit être configurée pour ce rôle.

## Rôle « par défaut »

En plus des rôles explicitement définis, il existe un rôle implicite que tous les StyleBooks ont, et ce rôle est appelé comme rôle par défaut. Ce rôle peut être utilisé comme n'importe quel autre rôle dans un StyleBook. Lors de la création d'un configpack, si aucun rôle spécifique n'est attribué à une instance ADC, l'instance est implicitement affectée au rôle « par défaut ». L'instance recevra désormais tous les objets de configuration générés par les composants ayant le rôle « par défaut ».

## Composants avec des rôles

Une fois les rôles qu'un StyleBook peut prendre en charge (y compris le rôle « par défaut ») définis, les rôles peuvent être utilisés dans la section des composants d'un StyleBook. Si vous souhaitez qu'

un composant soit déployé uniquement sur des instances ADC qui jouent un certain rôle, vous pouvez spécifier l'attribut `role` dans le cadre du composant, comme illustré dans l'exemple suivant d'un composant :

```
1  -
2    name: C1
3    type: ns::lbvserver
4    roles:
5      - A
6    properties:
7      name: lb1
8      servicetype: HTTP
9      ipv46: 1.1.1.1
10     port: 80
11 <!--NeedCopy-->
```

Dans l'exemple ci-dessus, le composant génère un « lbvserver » qui sera déployé sur les instances jouant le rôle A. Notez que l'attribut `roles` d'un composant est une liste et que plusieurs rôles peuvent être attribués à un composant. Ces rôles auraient été déclarés dans la section « rôles cibles » du StyleBook.

Remarque : Si un composant d'un StyleBook ne spécifie pas d'attribut de rôle, les objets de configuration générés par le composant sont créés sur toutes les instances Citrix ADC quel que soit leur rôle. Vous pouvez utiliser cette fonctionnalité efficacement pour créer des objets de configuration qui peuvent être appliqués à toutes les instances d'un configpack.

Supposons qu'il existe un StyleBook avec deux rôles définis - A et B, et qui contient quatre composants.

- Le composant C1 a les rôles A et B
- Le composant C2 a le rôle B
- Aucun rôle n'est défini pour le composant C3
- Le composant C4 a le rôle « par défaut »

La section Composants de ce StyleBook est reproduite ci-dessous :

```
1  components:
2    -
3      name: C1
4      type: ns::lbvserver
5      roles:
6        - A
7        - B
8      properties:
9        name: lb1
10       servicetype: HTTP
11       ipv46: 1.1.1.1
12       port: 80
13    -
14     name: C2
```

```
15     type: ns::lbserver
16     roles:
17       - B
18     properties:
19       name: lb2
20       servicetype: HTTP
21       ipv46: 12.12.12.12
22       port: 80
23   -
24     name: C3
25     type: ns::lbserver
26     properties:
27       name: lb3
28       servicetype: HTTP
29       ipv46: 13.13.13.13
30       port: 80
31   -
32     name: C4
33     type: ns::lbserver
34     roles:
35       - default
36     properties:
37       name: lb4
38       servicetype: HTTP
39       ipv46: 14.14.14.14
40       port: 80
41 <!--NeedCopy-->
```

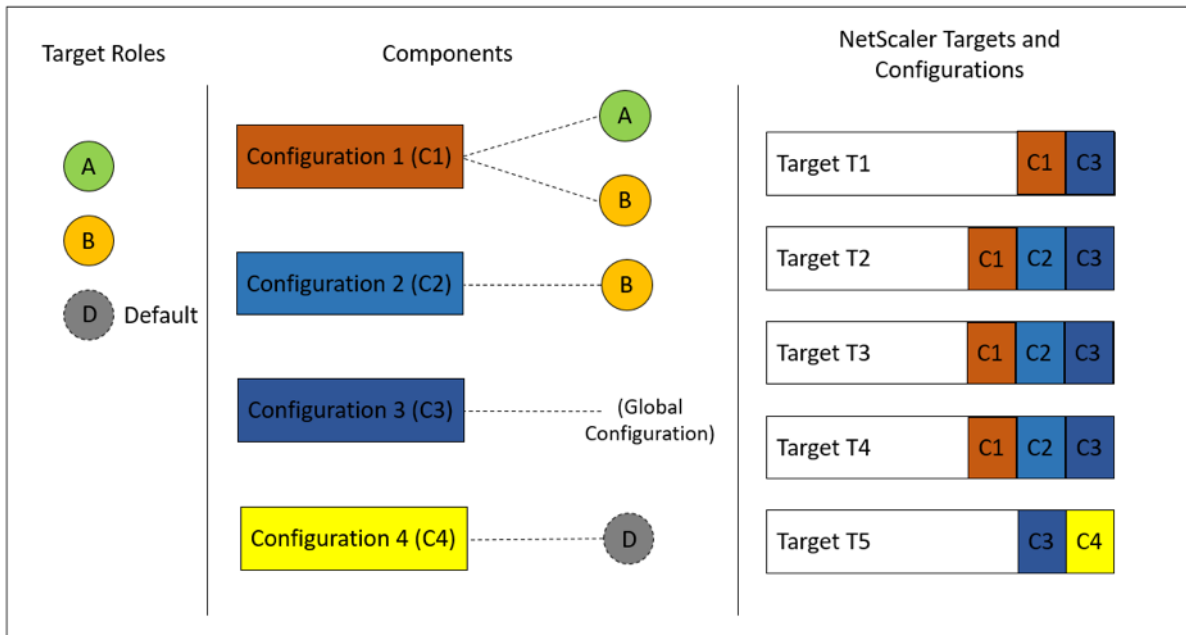
Notez que le composant C3 n'a pas de rôle défini, ce qui signifie que le composant est déployé sur toutes les instances, quel que soit leur rôle. D'autre part, le composant C4 a le rôle « default », ce qui signifie qu'il est appliqué à toute instance qui n'a pas de rôle explicite qui lui est assigné.

Maintenant, considérez que vous souhaitez créer un configpack à l'aide de ce StyleBook et le déployer sur cinq instances ADC. À ce stade, vous pouvez affecter les rôles aux instances de la manière suivante :

- Le rôle A est attribué aux instances T1, T2, T3 et T4
- Le rôle B est attribué aux instances T2, T3 et T4
- Aucun rôle n'est attribué à l'instance T5

L'image suivante résume les attributions de rôle et montre la configuration résultante que chaque instance ADC recevra :





Notez que le composant C3 est déployé sur toutes les instances quel que soit le rôle, car ce composant ne possédait aucun attribut rôle.

Vous pouvez également utiliser la fonction « Dry Run » lors de la création d'un configpack pour afficher et vérifier l'attribution correcte des rôles et les objets de configuration qui seront créés sur chaque instance ADC.

## Créez votre StyleBook

Le contenu complet du StyleBook « demo-target-roles » est fourni ci-dessous :

```

1 ---
2 name: demo-target-roles
3 namespace: com.example.stylebooks
4 version: "1.2"
5 schema-version: "1.0"
6 import-stylebooks:
7   -
8     namespace: netscaler.nitro.config
9     prefix: ns
10    version: "10.5"
11 parameters:
12   -
13     name: appname
14     type: string
15     required: true
16     key: true
17 target-roles:
18   -
19     name: A
    
```

```
20  -
21    name: B
22    min-targets: 2
23    max-targets: 5
24  components:
25    -
26      name: C1
27      type: ns::lbserver
28      roles:
29        - A
30        - B
31      properties:
32        name: lb1
33        servicetype: HTTP
34        ipv46: 1.1.1.1
35        port: 80
36    -
37      name: C2
38      type: ns::lbserver
39      roles:
40        - B
41      properties:
42        name: lb2
43        servicetype: HTTP
44        ipv46: 12.12.12.12
45        port: 80
46    -
47      name: C3
48      type: ns::lbserver
49      properties:
50        name: lb3
51        servicetype: HTTP
52        ipv46: 13.13.13.13
53        port: 80
54    -
55      name: C4
56      type: ns::lbserver
57      roles:
58        - default
59      properties:
60        name: lb4
61        servicetype: HTTP
62        ipv46: 14.14.14.14
63        port: 80
64  <!--NeedCopy-->
```

L'image suivante montre les objets créés pour un exemple de configpack :

Objects created ( 9 ) x

<b>Instance : 10.102.102.136   Roles : B   Count : 3</b>
<b>Type : lbserver</b> ipv46 : 1.1.1.1 name : lb1 port : 80 servicetype : HTTP
<b>Type : lbserver</b> ipv46 : 12.12.12.12 name : lb2 port : 80 servicetype : HTTP
<b>Type : lbserver</b> ipv46 : 13.13.13.13 name : lb3 port : 80 servicetype : HTTP
<b>Instance : 10.102.102.135   Roles : B   Count : 3</b>
<b>Type : lbserver</b> ipv46 : 1.1.1.1 name : lb1 port : 80 servicetype : HTTP
<b>Type : lbserver</b> ipv46 : 12.12.12.12 name : lb2 port : 80 servicetype : HTTP
<b>Type : lbserver</b> ipv46 : 13.13.13.13 name : lb3 port : 80 servicetype : HTTP
<b>Instance : 10.102.102.62   Roles : A, default   Count : 3</b>
<b>Type : lbserver</b> ipv46 : 1.1.1.1 name : lb1 port : 80 servicetype : HTTP
<b>Type : lbserver</b> ipv46 : 13.13.13.13 name : lb3 port : 80 servicetype : HTTP
<b>Type : lbserver</b> ipv46 : 14.14.14.14 name : lb4 port : 80 servicetype : HTTP

## Utilisation des API

Lorsque vous utilisez l'API REST, vous pouvez spécifier des rôles pour chaque instance ADC lors de la création ou de la mise à jour du configpack comme suit. Dans le bloc « cibles », spécifiez l'UUID de l'instance Citrix ADC spécifique sur laquelle vous souhaitez déployer les composants individuels.

```
1  "targets": [  
2      {  
3  
4          "id": "<ADC-UUID>",  
5          "roles": ["A"]  
6      }  
7  ,  
8  ]  
9  <!--NeedCopy-->
```

Un exemple complet d'API REST est fourni à titre de référence.

POST/<ADM-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/1.2/demo-target-roles/configpacks

```
1  {  
2  
3      "configpack": {  
4  
5          "parameters": {  
6  
7              "appname": "app1"  
8          }  
9      ,  
10     "targets": [  
11         {  
12  
13             "id": "f53c35c3-a6bc-4619-b4b4-ad7ab6a94ddb",  
14             "roles": ["A"]  
15         }  
16     ,  
17         {  
18  
19             "id": "c08caa1c-1011-48aa-b8c7-9aed1cd38ed0",  
20             "roles": ["A", "B"]  
21         }  
22     ,  
23         {  
24  
25             "id": "88ac90cb-a5cb-445b-8617-f83d0ef6174e",  
26             "roles": ["A", "B"]  
27         }  
28     ,  
29         {  
30  
31             "id": "bf7b0f74-7a83-4856-86f4-dcc951d3141e",
```

```
32     "roles": ["A", "B"]
33     }
34   ,
35     {
36     "id": "fa5d97ab-ca29-4adf-b451-06e7a234e3da",
37     "roles": ["default"]
38     }
39   ]
40 }
41 }
42 }
43 }
44 }
45 }
46 <!--NeedCopy-->
```

## Créer un StyleBook pour effectuer des opérations non CRUD

February 1, 2024

StyleBooks gère les configurations de Citrix ADC en calculant les objets de configuration nécessaires sur les instances de Citrix ADC. Ces objets sont ajoutés, mis à jour ou supprimés de l'instance chaque fois que vous créez ou mettez à jour un ConfigPack. C'est à ce moment que vous spécifiez l'« état désiré. »

Toutefois, certains objets de configuration Citrix ADC prennent en charge quelques opérations autres que la création, la mise à jour ou la suppression (opérations CRUD). Par exemple, un objet d'équilibrage de charge (lbserver) ou un objet de fonctionnalité Citrix ADC (nsfeature) peut prendre en charge l'opération « enable » ou « disable ». De même, les clés de certification Citrix ADC prennent en charge les opérations « link » et « unlink » pour lier ou dissocier un certificat à un autre certificat. Ces opérations sur les objets Citrix ADC sont appelées opérations non CRUD. Cette section décrit comment effectuer des opérations non CRUD sur des objets de configuration qui les prennent en charge à l'aide de StyleBooks.

### Remarque

La liaison entre les objets de configuration (par exemple, lier une clé de certification à un serveur lbserver) n'est pas considérée comme une opération non CRUD. En effet, les liaisons Nitro sont représentées en tant qu'objets de configuration à part entière. Ces objets sont créés et supprimés comme tout autre objet de configuration Citrix ADC.

## Soutenir les opérations non CRUD

Une nouvelle construction appelée « méta-propriétés » est ajoutée dans le composant au même niveau que la construction « propriétés ». Le seul attribut pris en charge dans cette construction est actuellement appelé « action ». Cet attribut peut prendre des valeurs telles que « enable » ou « disable » qui sont prises en charge par cet objet de configuration.

```
1 components:
2   -
3     name: my-lbvserver-comp
4     type: ns::lbvserver
5     meta-properties
6       action: enable
7     properties:
8       name: $parameters.name
9       servicetype: HTTP
10      ipv46: $parameters.ip
11      port: 80
12      lbmethod: $parameters.lb-alg
13 <!--NeedCopy-->
```

Dans l'exemple ci-dessus, le composant « my-lbvserver-comp » est du type « ns::lbvserver ». Le « ns » est le préfixe qui fait référence à l'espace de noms netScaler.nitro.config et à la version 10.5 que vous avez spécifiés dans la section import-stylebooks. Le « lbvserver » est une ressource NITRO dans cet espace de noms. En tant qu'action implicite, le serveur lbvserver est d'abord créé par le StyleBook, puis l'opération « activer » est effectuée sur celui-ci.

L'action spécifiée dans les méta-propriétés est effectuée sur l'objet de configuration uniquement lors de la création du ConfigPack. Les mises à jour du ConfigPack n'effectuent pas d'actions non CRUD.

### Remarque

La valeur de l'attribut action ne peut pas être une expression StyleBook évaluée dynamiquement.

## Utiliser l'API pour créer des configurations à partir de StyleBooks

February 1, 2024

Après avoir créé votre StyleBook, vous devez l'importer dans Citrix Application Delivery Management (ADM) pour l'utiliser soit à l'aide de Citrix ADM, soit à l'aide des API Citrix ADM. Citrix ADM valide votre StyleBook lorsque vous l'importez, et si la validation est réussie, votre StyleBook apparaît dans le catalogue Citrix ADM de StyleBooks, prêt à être utilisé pour créer des configurations.

Vous pouvez désormais utiliser les API StyleBook pour créer des configurations basées sur ce StyleBook. Vous pouvez utiliser n'importe quel outil tel que l'outil de ligne de commande curl ou l'extension de navigateur Chrome Postman pour envoyer des requêtes HTTP à Citrix ADM.

### Exemple 1

Considérez le StyleBook « lb-vserver » que vous avez créé dans [StyleBook pour créer un serveur virtuel d'équilibrage de charge](#). Utilisez l'API REST pour créer un configpack à partir de ce StyleBook comme suit :

```
1 POST
2
3 https://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/lb-vserver/configpacks
4
5 <!--NeedCopy-->
```

```
1 Content-Type: application/json
2 Accept: application/json
3 {
4
5   "configpack":
6   {
7
8     "parameters": {
9
10      "name": "lb1",
11      "ip": "10.102.117.31"
12    }
13  ,
14  "target_devices":
15  [
16    {
17
18      "id": "deecce30-f478-4446-9741-a85041903410"
19    }
20  ]
21  }
22  }
23
24  }
25
26 <!--NeedCopy-->
```

Dans cette requête HTTP, l'id (par exemple, « deecce30-f478-4446-9741-a85041903410 ») est l'ID d'instance de l'instance Citrix ADC sur laquelle le serveur virtuel d'équilibrage de charge lb1 avec l'adresse IP 10.102.117.31 est créé. L'ID d'instance de l'instance Citrix ADC est extrait de Citrix ADM.

Pour obtenir l'ID d'une instance gérée par Citrix ADM, vous pouvez utiliser les API Citrix ADM. Par ex-

emple, pour récupérer l’ID d’instance d’une instance Citrix ADC dont l’adresse IP est 192.168.153.160, vous pouvez utiliser l’API suivante :

```
1 GET https://<MAS-IP>/nitro/v1/config/ns?filter=ip_address
   :192.168.153.160
2 <!--NeedCopy-->
```

```
1 Accept: application/json
2 <!--NeedCopy-->
```

La réponse contient l’ID de la charge utile :

```
1 200
2 OK
3 Content-Type: application/json
4 {
5
6   "errorcode": 0,
7   "message": "Done",
8   "operation": "get",
9   "resourceType": "ns",
10  "username": "nsroot",
11  "tenant_name": "Owner",
12  "resourceName": "",
13  "ns":
14  [
15    {
16
17     "is_grace": "false",
18     "hostname": "",
19     "std_bw_config": "0",
20     "gateway_deployment": "false",
21     ... "id": "deec30-f478-4446-9741-a85041903410",
22     ...
23   }
24 ]
25 }
26 }
27
28 <!--NeedCopy-->
```

Si la configuration (configpack) a été créée avec succès, vous recevez la réponse HTTP suivante :

```
1 200 OK
2 Content-Type: application/json
3 {
4
5   "configpack":
6   {
7
8     "config_id": "1460806080"
9   }
10 }
```



```
11 }
12
13 <!--NeedCopy-->
```

Vous avez créé votre première configuration (configpack) qui est identifiée de manière unique à l'aide de l'ID 1460806080. Vous pouvez utiliser cet ID pour interroger, mettre à jour ou supprimer la configuration.

## Exemple 2

Vous pouvez utiliser le même StyleBook pour créer une autre configuration ou configpack et l'exécuter sur les mêmes instances de Citrix ADC ou différentes. Dans cet exemple, créez une autre configuration et fournissez un nom et une adresse IP différents pour le serveur virtuel et spécifiez LEASTCONNECTION comme méthode d'équilibrage de charge. Déployez cette configuration sur deux instances Citrix ADC.

La requête HTTP est la suivante :

```
1 POST
2
3 https://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/lb-vserver/configpacks
4 <!--NeedCopy-->
```

```
1 Content-Type: application/json
2 Accept: application/json
3 {
4
5   "configpack":
6   {
7
8     "parameters":
9     {
10
11       "name": "lb2",
12       "ip": "10.102.117.32",
13       "lb-alg": "LEASTCONNECTION"
14     }
15   ,
16   "target_devices"
17   [
18   {
19     "id": "deecce30-f478-4446-9741-a85041903410" }
20   ,
21   {
22     "id": "debecc60-d589-4557-8632-a74032802412" }
23   ]
24   ]
25 }
```

```
26
27 }
28
29 <!--NeedCopy-->
```

Dans cette requête HTTP, le serveur virtuel d'équilibrage de charge lb2 avec l'adresse IP 10.102.117.32 est créé sur les deux instances Citrix ADC représentées par les ID « deecce30-f478-4446-9741-a85041903410 » et « debecc60-d589-4557-8632-a74032802412 ».

En cas de création réussie du configpack, la réponse HTTP suivante est reçue :

```
1 200 OK
2 Content-Type: application/json
3 {
4
5   "configpack":
6   {
7
8     "config_id": "1657696292"
9   }
10 }
11 }
12
13 <!--NeedCopy-->
```

Ce nouveau configpack a un identifiant différent 165769629. Vous pouvez mettre à jour ou supprimer cette configuration à l'aide de cet ID.

### Exemple 3

Considérez le StyleBook « basic-lb-config » que vous avez créé dans [StyleBook pour créer une configuration d'équilibrage de charge de base](#). Utilisez l'API REST pour créer un configpack à partir de ce StyleBook comme suit :

```
1 POST
2
3 http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example
   .stylebooks/0.1/basic-lb-config/configpacks
4 <!--NeedCopy-->
```

```
1 Content-Type: application/json
2 Accept: application/json
3 {
4
5   "configpack":
6   {
7
8     "parameters":
9     {
10
```

```
11     "name": "myapp",
12     "ip": "10.70.122.25",
13     "svc-servers":
14     ["192.168.100.11", "192.168.100.12"],
15     "svc-port": 8080
16   }
17 ,
18   "target_devices":
19   [
20     {
21
22     "id": "deecce30-f478-4446-9741-a85041903410"
23     }
24   ,
25     {
26
27     "id": "debecc60-d589-4557-8632-a74032802412"
28     }
29   ]
30 }
31 }
32 }
33 }
34 }
35 <!--NeedCopy-->
```

Dans cette requête HTTP, la configuration d'équilibrage de charge est exécutée sur deux instances Citrix ADC. Vous pouvez ouvrir une session sur ces instances Citrix ADC pour vérifier si un serveur virtuel et un groupe de services avec deux services liés sont créés.

#### Exemple 4

Prenons l'**exemple composite StyleBook composite** que vous avez créé dans [Créer un StyleBook composite](#). Utilisez l'API REST pour créer un configpack à partir de ce StyleBook comme suit :

```
1 POST http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
  example.stylebooks/0.1/composite-example/configpacks
2 <!--NeedCopy-->
```

```
1 Content-Type: application/json
2 Accept: application/json
3 {
4
5   "configpack":
6   {
7
8     "parameters": {
9
10     "name": "myapp",
11     "ip": "2.2.2.2",
```

```
12     "svc-servers": ["10.102.29.52", "10.102.29.53"]
13     }
14   ,
15   "target_devices":
16   [
17   {
18     "id": "deecce30-f478-4446-9741-a85041903410"
19   }
20   ,
21   {
22     "id": "debecc60-d589-4557-8632-a74032802412"
23   }
24   ]
25 }
26 }
27 }
28 }
29 }
30 }
31 }
32 <!--NeedCopy-->
```

Dans cette requête HTTP, la configuration est créée sur deux instances Citrix ADC représentées par leurs ID. Si vous ouvrez une session sur les instances Citrix ADC, vous pouvez afficher les objets de configuration créés par le StyleBook « basic-lb-config » qui a été importé dans le StyleBook « composite-example ». Vous pouvez également voir un nouveau moniteur HTTP appelé « myapp-mon » qui faisait partie du StyleBook « composite-example ».

En cas de création réussie du configpack, la réponse HTTP suivante est reçue :

```
1 200 OK
2 Content-Type: application/json{
3
4   "configpack": {
5
6     "config_id": "4917276817"
7   }
8
9 }
10
11 <!--NeedCopy-->
```

### Mise à jour d'une configuration

Pour mettre à jour cette configuration, par exemple, en ajoutant un nouveau serveur backend avec l'adresse IP 10.102.29.54 au serveur virtuel d'équilibrage de charge myapp, utilisez l'API pour mettre à jour un configpack comme suit :

```
1 PUT http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/composite-example/configpacks/4917276817
```

```
2 <!--NeedCopy-->
1 Content-Type: application/json
2 Accept: application/json
3 {
4
5   "configpack": {
6
7     "parameters": {
8
9       "name": "myapp",
10      "ip": "2.2.2.2",
11      "svc-servers": ["10.102.29.52", "10.102.29.53", "10.102.29.54"]
12    }
13  },
14  "target_devices":
15  [
16    {
17
18      "id": "deecee30-f478-4446-9741-a85041903410"
19    }
20  ,
21  {
22
23      "id": "debecc60-d589-4557-8632-a74032802412"
24    }
25  ]
26 ]
27 }
28
29 }
30
31 <!--NeedCopy-->
```

En cas de mise à jour réussie du configpack, la réponse HTTP suivante est reçue :

```
1 200 OK
2 Content-Type: application/json
3 {
4
5   "configpack": {
6
7     "config-id": "4917276817"
8   }
9
10  }
11
12 <!--NeedCopy-->
```

## Suppression d'une configuration

Pour supprimer cette configuration (à partir de toutes les instances de Citrix ADC), vous pouvez utiliser l'API pour supprimer un configpack comme suit :

```
1 DELETE http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.  
example.stylebooks/0.1/composite-example/configpacks/4917276817  
2 <!--NeedCopy-->
```

```
1 Accept: application/json  
2 <!--NeedCopy-->
```

En cas de suppression réussie du configpack, la réponse HTTP suivante est reçue :

```
1 200 OK  
2 Content-Type: application/json  
3 {  
4  
5   "configpack": {  
6  
7     "config_id": "4917276817"  
8   }  
9  
10  }  
11  
12 <!--NeedCopy-->
```

Vous pouvez ouvrir une session sur l'instance de Citrix ADC et vérifier que tous les objets de configuration qui font partie de ce configpack ont été supprimés.

Si vous souhaitez supprimer la configuration d'instances Citrix ADC spécifiques au lieu de toutes, utilisez l'opération update configpack décrite ci-dessus et modifiez l'attribut « target\_devices » dans la charge utile JSON pour supprimer les ID d'instance Citrix ADC spécifiques.

## Utiliser l'API pour créer des configurations pour charger des fichiers de certificat et de clé

February 1, 2024

Utilisez les API StyleBook pour créer des configurations basées sur ce StyleBook. Vous pouvez utiliser n'importe quel outil tel que l'outil de ligne de commande curl ou l'extension du navigateur Chrome Postman pour envoyer des requêtes HTTP à Citrix Application Delivery Management (ADM).

Prenons l'exemple StyleBook que vous avez créé pour télécharger les fichiers de certificat et de clé dans [Comment créer un StyleBook pour télécharger des fichiers de certificat et de clé de certificat SSL vers Citrix ADM](#). Utilisez l'API REST pour créer un configpack à partir de ce StyleBook comme suit :

```
1 POST
2
3 https://<MAS_IP_Address>/stylebook/nitro/v1/config/stylebooks/com.
   citrix.adc.stylebooks/1.0/lb-mon/configpacks?mode=async
4 <!--NeedCopy-->
```

```
1 Content-Type: application/jsonAccept: application/json {
2
3   "configpack": {
4
5     "parameters": {
6
7       "lb-appname": "lbmon",
8       "lb-virtual-ip": "13.1.11.10",
9       "lb-virtual-port": "80",
10      "lb-service-type": "HTTP",
11      "svc-service-type": "HTTP",
12      "svc-servers": [
13        {
14
15          "ip": "14.1.1.15",
16          "port": "80"        }
17      ],
18      "certificates": [
19        {
20
21          "cert-name": "server_cert",
22          "cert-file": "server_cert.pem",
23          "ssl-inform": "PEM",
24          "key-name": "server_key",
25          "key-file": "server_key.pem",
26          "cert-password": "secret",
27          "cert-advanced": {
28
29            "is-ca-cert": false,
30            "skip-ca-name": false
31          }
32        }
33      ]
34    },
35
36    "lb-advanced": {
37
38      "flush-on-state-down": "ENABLED",
39      "auth-params": {
40
41        "authentication": "OFF",
42        "authentication-http-401": "OFF"
43      }
44    },
45
46    "appflow-log": "ENABLED",
```

```
47         "algorithm": "LEASTCONNECTION"
48     }
49     ,
50     "svcg-advanced": {
51         "svc-client-ip": "DISABLED",
52         "svc-use-source-ip": "NO",
53         "svc-use-proxy-port": "NO",
54         "svc-surge-protection": "OFF",
55         "svc-client-keepalive": "NO",
56         "svc-tcp-buffering": "NO",
57         "svc-compression": "NO",
58         "svc-state": "ENABLED",
59         "svc-downstate-flush": "DISABLED",
60         "svc-enable-health-monitor": "NO"
61     }
62 }
63 }
64 }
65 ,
66 "targets": [
67     {
68         "id": "8c158e7a-0087-423f-91b0-0ccf16de552a"
69     }
70 ]
71 }
72 ]
73 }
74 }
75 }
76 }
77 <!--NeedCopy-->
```

Ce configpack est identifié de manière unique à l'aide de l'ID 8c158e7a-0087-423f-91b0-0ccf16de552a. Vous pouvez utiliser cet ID pour interroger, mettre à jour ou supprimer la configuration. Une fois la mise à jour réussie du configpack, les fichiers de certificat et de clé sont téléchargés dans le système de fichiers Citrix ADM.

## Utiliser l'API pour créer des configurations pour télécharger n'importe quel type de fichier

February 1, 2024

Vous pouvez également utiliser l'API Citrix Application Delivery Management (ADM) pour créer un configpack qui télécharge des fichiers vers l'instance Citrix ADC sélectionnée.

Prenons l'exemple StyleBook que vous avez créé pour télécharger des fichiers de tout type dans [Comment créer un StyleBook pour télécharger des fichiers vers le service Citrix ADC MA](#). Comme



dans l'exemple dans la rubrique ci-dessus, créez un configpack et spécifiez la valeur du paramètre « locationfile » comme chemin d'accès au fichier d'emplacement sur Citrix ADM.

Utilisez l'API REST pour créer un configpack à partir de ce StyleBook comme suit :

```
1 POST
2
3 https://<mas_ip>/stylebook/nitro/v1/config/stylebooks/com.citrix.adc.
  stylebooks.samples/1.0/upload-geolocations/configpacks
4 <!--NeedCopy-->
```

```
1 Content-Type: application/json
2 Accept: application/json
3 {
4
5   "configpack":
6   {
7
8     "parameters": {
9
10      "locationfile": "/var/mps/tenants/root/files/ /
      custom_geolocations.csv"
11    }
12  ,
13    "targets": [
14      {
15
16        "id": "5e540839-cd6c-437e-ac53-7d49bc2602b5"
17      }
18    ]
19  }
20 }
21
22 }
23
24 <!--NeedCopy-->
```

## Utiliser l'API pour importer des StyleBooks personnalisés

February 1, 2024

Vous pouvez désormais utiliser les API StyleBook pour importer des StyleBooks personnalisés dans Citrix Application Delivery Management (ADM). Utilisez l'API REST pour créer un configpack à partir de ce StyleBook comme suit dans n'importe quel outil tel que l'outil de ligne de commande curl ou l'extension de navigateur Chrome Postman. Par exemple, vous pouvez importer un StyleBook nommé exemple-lb qui peut être utilisé pour créer une configuration d'équilibrage de charge sur une instance Citrix ADC.

```
1 HTTP Method: POST
2 URL: http://<mas-ip>/stylebook/nitro/v1/config/stylebooks
3 Headers:
4 Content-Type: application/json
5 Accept: application/json
6 RequestBody:
7 {
8
9     "stylebook":
10    {
11
12        "file_name": "example-lb.yaml",
13        "source": "<base64-contents>",
14        "encoding": "base64"
15    }
16 }
17 }
18
19 <!--NeedCopy-->
```

où, la valeur de l'attribut « source », est l'encodage base64 du contenu de votre fichier StyleBook. Vous pouvez coller le contenu YAML de votre fichier StyleBook dans un outil en ligne, par exemple, <https://www.browserling.com/tools/file-to-base64> pour obtenir la chaîne base64 que vous pouvez ensuite utiliser comme valeur pour l'attribut « source » ci-dessus.

À l'aide de cet appel API, vous pouvez également télécharger un fichier tarball compressé (fichier .tgz) contenant plusieurs fichiers StyleBook en une seule opération API. Pour ce faire, changez simplement l'attribut file\_name par le nom de fichier .tgz et la valeur de l'attribut source par le codage base64 du contenu de votre fichier .tgz.

Une fois l'API exécutée avec succès dans l'outil, vous obtenez la réponse suivante qui indique que le StyleBook a été importé dans Citrix ADM.

```
1 200 OK
2 <!--NeedCopy-->
```

#### Corps de réponse :

```
1 {
2
3
4     "stylebook":
5     {
6
7
8         "name": "example-lb",
9
10        "namespace": "com.example.stylebook",
11
12        "version": "1.0"
13    }
```

```
14     }
15
16
17   }
18
19 <!--NeedCopy-->
```

## Utiliser l'API pour télécharger des StyleBooks personnalisés

February 1, 2024

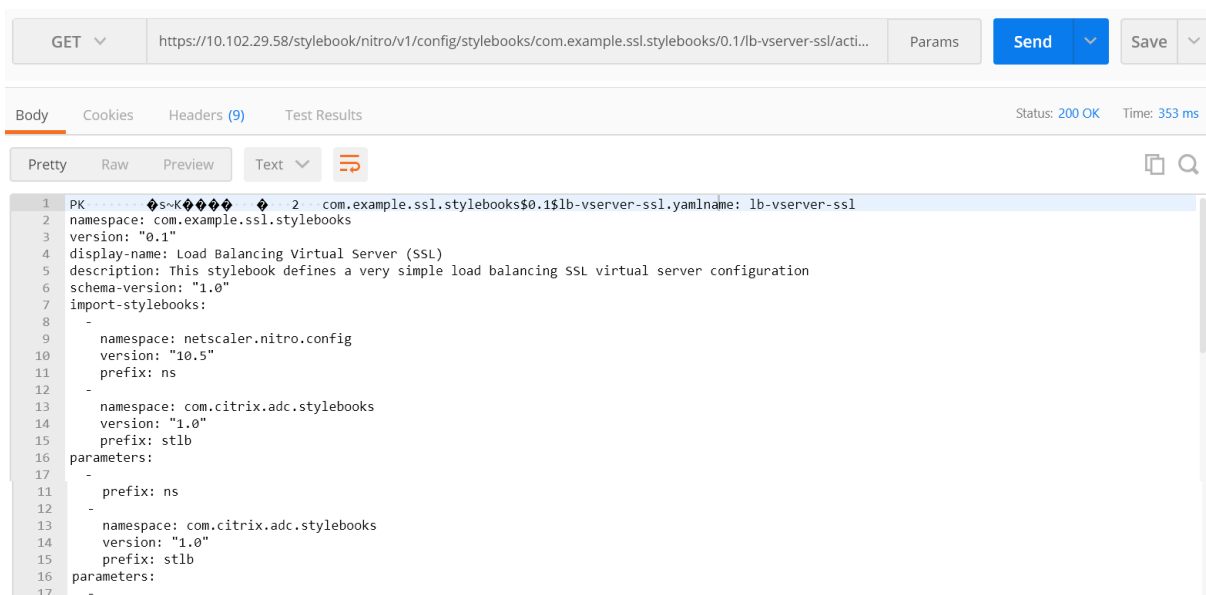
Vous pouvez télécharger un StyleBook personnalisé en fournissant l'API REST StyleBooks suivante :

```
1 GET
2
3 https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks/<NAMESPACE>/<
  VERSION>/<NAME>/actions/download
4 <!--NeedCopy-->
```

Vous pouvez exécuter l'API dans n'importe quel outil tel que l'outil de ligne de commande curl ou l'extension de navigateur Postman Chrome après avoir modifié les champs d'adresse IP, de nom, de version et d'espace de noms.

```
1 GET
2
3 https://10.102.29.58/stylebook/nitro/v1/config/stylebooks/com.example.
  ssl.stylebooks/0.1/lb-vserver-ssl/actions/download`
4 <!--NeedCopy-->
```

Le StyleBook au format .yaml est téléchargé.



## Utiliser l'API pour supprimer des StyleBooks personnalisés

February 1, 2024

Vous pouvez supprimer le StyleBook personnalisé en fournissant l'API REST StyleBooks suivante :

```

1 DELETE
2
3 https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks/<NAMESPACE>/<
4   VERSION>/<NAME>?dependencies=true
5 <!--NeedCopy-->
  
```

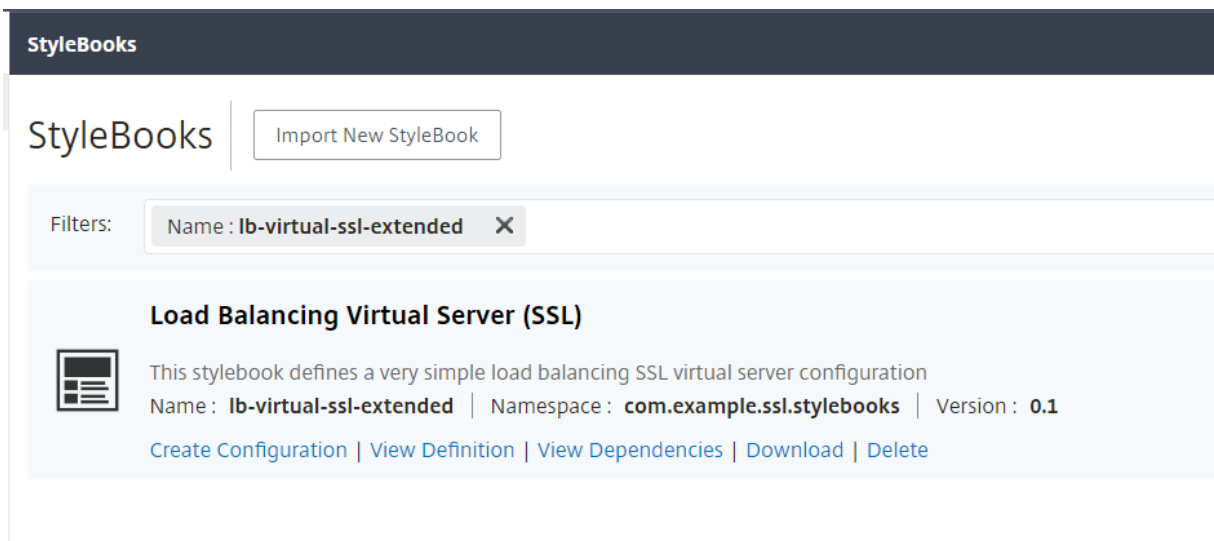
Si le paramètre de requête dépendances de l'URL n'est pas fourni ou si sa valeur est définie sur false, les dépendances StyleBook ne sont pas supprimées (seul le StyleBook lui-même est supprimé).

Lorsque vous recevez un code d'état de réponse HTTP 200, cela signifie que le StyleBook personnalisé (et ses dépendances) est correctement supprimé de Citrix ADM.

### Remarque

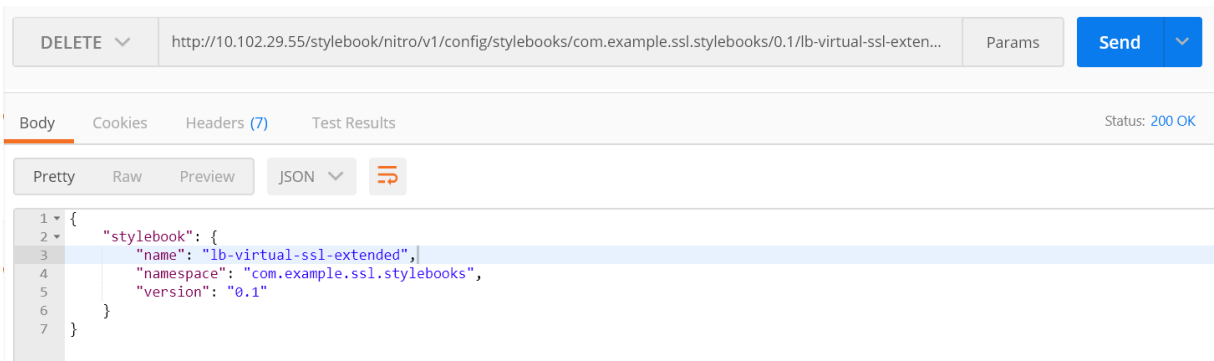
Vous ne pouvez pas supprimer un StyleBook personnalisé qui possède d'autres StyleBooks dans le service MA qui en dépendent.

Par exemple, supposons que vous avez créé un StyleBook nommé « lb-virtual-ssl-extended » dans Citrix ADM. Vous avez ensuite décidé de supprimer ce StyleBook.

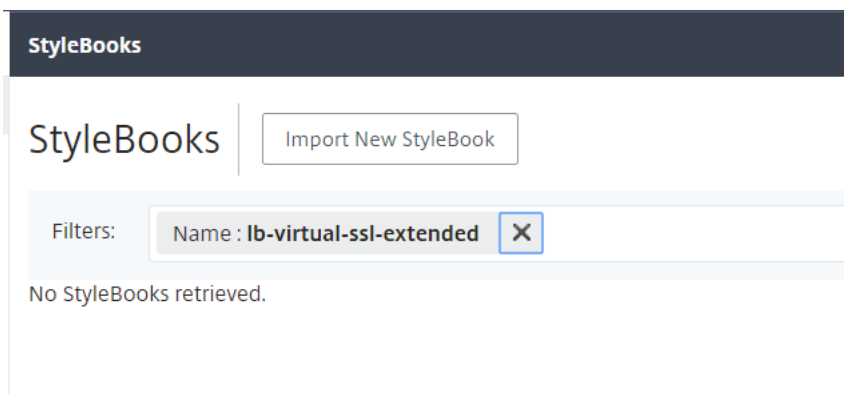


Vous pouvez exécuter l'API dans n'importe quel outil tel que l'outil de ligne de commande curl ou l'extension de navigateur Postman Chrome après avoir modifié les champs d'adresse IP, de nom, de version et d'espace de noms.

SUPPRIMER <https://10.102.29.55/stylebook/nitro/v1/config/stylebooks/com.example.ssl.stylebooks/0.1/lb-virtual-ssl-extended?dependencies=false>



Le StyleBook est supprimé de Citrix ADM.



## Grammaire de StyleBooks

February 1, 2024

Vous pouvez concevoir vos propres StyleBooks, les importer dans Citrix Application Delivery Management (ADM), puis les utiliser pour créer des configurations à l'aide de l'interface graphique Citrix ADM ou à l'aide d'API. Pour pouvoir créer vos propres StyleBooks, vous devez d'abord comprendre la grammaire et la syntaxe des différentes constructions et attributs que vous pouvez utiliser.

Ce document décrit les différentes constructions et références que vous pouvez utiliser lors de la création de StyleBooks.

Cliquez sur le nom d'une section, d'une construction ou d'une référence dans le tableau ci-dessous pour afficher les détails.

|||

|—|—|

| [Header](/fr-fr/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/header-section.html) | [Importer des StyleBooks](/fr-fr/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/import-stylebooks-section.html) |

| [Parameters](/fr-fr/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/parameters-section.html) | [Parameters-default-sources construct](/fr-fr/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/parameters-default-sources-construct.html) |

| [Substitutions](/fr-fr/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/substitutions.html) | [Components](/fr-fr/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/components.html) |

| [Propriétés facultatives](/fr-fr/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/optional-properties.html) | [Composants d'assistance](/fr-fr/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/helper-components.html) |

| [Propriétés, sources par défaut](/fr-fr/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/properties-default-sources.html) | [Composants imbriqués](/fr-fr/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/nested-components.html) |

| [Conditionner la construction](/fr-fr/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/condition-construct.html) | [Construction repeat](/fr-fr/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/repeat-construct.html) |

| [Construction repeat-condition](/fr-fr/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/repeat-condition-construct.html) | [Outputs](/fr-fr/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/outputs.html) |

[Répétitions imbriquées](/fr-fr/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/nested-repeats.html)	[Référence parent](/fr-fr/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/parent-reference.html)
[Référence des paramètres](/fr-fr/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/parameter-reference.html)	[Référence des substitutions](/fr-fr/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/substitutions-reference.html)
[Référence des composants](/fr-fr/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/components-reference.html)	[Opérations](/fr-fr/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/operations.html)
[Référence de variable](/fr-fr/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/variable-reference.html)	[Alarms](/fr-fr/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/alarms.html)
[Analytics](/fr-fr/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/analytics.html)	[Fonctions intégrées](/fr-fr/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/built-in-functions.html)
[Expressions](/fr-fr/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/expressions.html)	[Détection des dépendances](/fr-fr/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/dependency-detection.html)
[Interpolations sur place](#)	

#### Remarque

Lorsque vous définissez un élément de répétition, un indice de répétition ou des arguments de fonctions de substitution, n'utilisez pas les mots réservés suivants pour nommer une variable définie par l'utilisateur, `<var-name>`

- livre de style, paramètres, substitutions, composants, propriétés, sorties, parent, self, opérations, analyses, alarmes
- repeat-item, repeat-item-0, repeat-item-1, repeat-item-2
- indice de répétition, indice de répétition 0, indice de répétition 1, indice de répétition 2
- default
- rôles, rôle, cibles, cible
- context, parent-context, parent\_context

Pour plus d'informations et des exemples sur la façon de concevoir vos propres StyleBooks, consultez [Comment créer vos propres StyleBooks](#).

## En-tête

February 1, 2024

Les six premières lignes d'un StyleBook constituent la section d'en-tête. Cette section vous permet de définir l'identité d'un StyleBook et de décrire son rôle. Il s'agit d'une section obligatoire.

Le tableau suivant décrit les attributs de la section d'en-tête :

Attribut	Description
nom	Un nom permettant d'identifier le StyleBook. Cet attribut est obligatoire.
description	Description qui définit ce que fait un StyleBook. Cette description apparaît sur l'interface graphique Citrix ADM. Il s'agit d'un attribut facultatif.
display-name	Un nom descriptif pour le StyleBook. Ce nom apparaît sur l'interface graphique Citrix ADM. Il s'agit d'un attribut facultatif.
auteur	L'auteur, la personne ou l'organisation qui crée le StyleBook. Il s'agit d'un attribut facultatif.
espace de noms	Un espace de noms fait partie de l'identifiant unique d'un StyleBook afin d'éviter les collisions de noms. Un espace de noms peut être n'importe quelle chaîne, mais il est recommandé de l'utiliser pour nommer la société, le service ou l'unité qui a créé ou possède un ensemble de StyleBooks. Par exemple, vous pouvez utiliser le format suivant : <company> . <department> . <unit > . <a href="#">stylebooks</a> . Il s'agit d'un attribut obligatoire.
version	Numéro de version du StyleBook. Vous pouvez modifier le numéro de version lorsque vous mettez à jour un StyleBook. Les StyleBooks de différentes versions peuvent coexister ensemble. Il s'agit d'un attribut obligatoire.
version du schéma	Version du schéma StyleBooks. Il prend la valeur « 1.0 » dans la version actuelle de Citrix ADM. Il s'agit d'un attribut obligatoire.
privé	Si cet attribut est défini sur true, le StyleBook ne s'affiche pas sur l'interface graphique Citrix ADM. Il s'agit d'un paramètre utile pour les StyleBooks qui sont des éléments de base pour d'autres StyleBooks et qui ne sont pas destinés à être utilisés directement par les utilisateurs. Il s'agit d'un attribut facultatif. Sa valeur par défaut est false.

### Exemple :

```
1     name: lb
2     description: "This stylebook defines a sample load balancing
3     configuration."
4     display-name: "Load Balancing StyleBook (HTTP)"
5     author: Mike Smith (ACME Infra team)
6     namespace: com.example.stylebooks
7     schema-version: "1.0"
8     version: "0.1"
```



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

La combinaison du nom, de l'espace de noms et de la version identifie de manière unique un StyleBook dans le système. Vous ne pouvez pas avoir deux StyleBooks avec la même combinaison de nom, d'espace de noms et de version dans Citrix ADM. Cependant, vous pouvez avoir deux StyleBooks avec le même nom et la même version mais des espaces de noms différents, ou avec le même espace de noms et la même version mais des noms différents.

## Importer des StyleBooks

February 1, 2024

Il s'agit de la deuxième section de votre StyleBook et vous permet de déclarer à quel autre StyleBook vous souhaitez faire référence à partir de votre StyleBook actuel. Cela vous permet d'importer et de réutiliser d'autres StyleBooks au lieu de recréer la même configuration dans votre propre StyleBook. Il s'agit d'une section obligatoire.

Vous devez déclarer l'**espace de noms** et le numéro de **version** du ou des StyleBook auxquels vous souhaitez faire référence dans votre StyleBook actuel. Chaque StyleBook doit faire référence à l'espace de noms `netScaler.nitro.config` s'il utilise directement l'un des objets de configuration NITRO. Cet espace de noms contient tous les types NITRO Citrix ADC, tels que le service `lbvserver` ou le moniteur. StyleBooks for Citrix ADC versions 10.5 et ultérieures sont pris en charge, ce qui signifie que vous pouvez utiliser votre StyleBook pour créer et exécuter des configurations sur n'importe quelle instance Citrix ADC exécutant la version 10.5 ou ultérieure.

L'attribut **préfixe** utilisé dans la section `import-stylebooks` est un raccourci qui fait référence à la combinaison de l'espace de noms et de la version. Par exemple, le préfixe « `ns` » peut être utilisé pour faire référence à l'espace de noms `netScaler.nitro.config` avec la version 10.5. Dans les sections ultérieures de votre StyleBook, au lieu d'utiliser l'espace de noms et la version chaque fois que vous souhaitez faire référence à un StyleBook avec cet espace de noms et cette version, vous pouvez simplement utiliser la chaîne de préfixe choisie avec le nom du StyleBook pour l'identifier de manière unique.

### Exemple :

```
1     import-stylebooks:
2     -
3         namespace: netScaler.nitro.config
4         version: "10.5"
5         prefix: ns
6     -
7         namespace: com.acme.stylebooks
8         version: "0.1"
9         prefix: stlb
10 <!--NeedCopy-->
```

Dans l'exemple ci-dessus, le premier préfixe défini s'appelle `ns` et fait référence à l'espace de noms `netScaler.nitro.config` et à la version 10.5. Le deuxième préfixe défini s'appelle `stlb` et fait référence à l'espace de noms `com.acme.stylebooks` et à la version 0.1.

Après avoir défini un préfixe, chaque fois que vous souhaitez faire référence à un type ou à un StyleBook appartenant à un espace de noms et à une version spécifiques, vous pouvez utiliser la notation **<namespace-shorthand>::<type-name>**. Par exemple, **`ns : lbserver` fait référence au type `lbserver`** défini dans l'espace de noms `netScaler.nitro.config`, version 10.5.

De même, si vous voulez faire référence à un StyleBook avec la version « 0.1 » dans l'espace de noms `com.acme.stylebooks`, vous pouvez utiliser la notation **`stlb::<stylebook-name>`**.

#### Remarque

Par convention, le préfixe « `ns` » est utilisé pour faire référence à l'espace de noms NITRO de Citrix ADC.

## Paramètres

February 1, 2024

Cette section vous permet de définir tous les paramètres dont vous avez besoin dans votre StyleBook pour créer une configuration. Il décrit l'entrée que votre StyleBook prend. Bien qu'il s'agisse d'une section facultative, la plupart des StyleBooks peuvent en avoir besoin. Vous pouvez considérer la section Paramètres pour définir les questions auxquelles les utilisateurs doivent répondre lorsqu'ils utilisent le StyleBook pour créer une configuration sur une instance d'Citrix ADC.

Lorsque vous importez votre StyleBook dans Citrix ADM et que vous l'utilisez pour créer une configuration, l'interface graphique utilise cette section du StyleBook pour afficher un formulaire qui prend en entrée les valeurs des paramètres que vous avez définis.

La section suivante décrit les attributs que vous devez spécifier pour chaque paramètre de cette section :

### nom

Nom du paramètre que vous souhaitez définir. Vous pouvez spécifier un nom alphanumérique.

Le nom doit commencer par un alphabet et peut inclure des alphabets, des chiffres, un tiret (-) ou un trait de soulignement (\_) supplémentaires.

Notez que lors de l'écriture d'un StyleBook, vous pouvez utiliser cet attribut « `name` » pour faire référence au paramètre dans d'autres sections en utilisant la notation `$parameters.<name>`.

**Obligatoire ?** Oui

### étiquette

Chaîne affichée dans l'interface graphique d'ADM en tant que nom de ce paramètre.

**Obligatoire ?** Non

### description

Chaîne d'aide qui décrit à quoi sert le paramètre. L'interface graphique ADM affiche ce texte lorsque l'utilisateur clique sur l'icône d'aide associée à ce paramètre.

**Obligatoire ?** Non

### type

Type de valeur que ces paramètres peuvent prendre. Les paramètres peuvent être de l'un des types intégrés suivants :

- **string** : un tableau de caractères. Si aucune longueur n'est spécifiée, la valeur de la chaîne peut prendre n'importe quel nombre de caractères. Toutefois, vous pouvez limiter la longueur d'un type de chaîne en utilisant les attributs `min-length` et `max-length`.
- **number** : Un nombre entier. Vous pouvez spécifier le nombre minimum et maximum que ce type peut prendre en utilisant les attributs `min-value` et `max-value`.
- **boolean** : peut être vrai ou faux. Notez également que tous les littéraux sont considérés par YAML comme des booléens (par exemple, Oui ou Non).
- **ipaddress** : chaîne qui représente une adresse IPv4 ou IPv6 valide.
- **tcp-port** : nombre compris entre 0 et 65535 qui représente un port TCP ou UDP.
- **password** : Représente une valeur de chaîne opaque/secrète. Lorsque l'interface graphique Citrix ADM affiche une valeur pour ce paramètre, elle s'affiche sous la forme d'astérisques (\*\*\*\*\*).
- **certfile** : Représente un fichier de certificat. Cela vous permet de télécharger les fichiers directement à partir de votre système local lorsque vous créez une configuration StyleBook à l'aide de l'interface graphique ADM. Le fichier de certificat téléchargé est stocké dans le répertoire `/var/mps/tenants//ns_ssl_certs` dans ADM.

Le fichier de certificat sera ajouté à la liste des certificats gérés par ADM.

- **keyfile** : Représente un fichier de clé de certificat. Cela vous permet de télécharger le fichier directement à partir de votre système local lorsque vous créez une configuration StyleBook à l'aide de l'interface graphique Citrix ADM. Le fichier de certificat téléchargé est stocké dans le répertoire `/var/mps/tenants//ns_ssl_keys` dans Citrix ADM.

Le fichier de clé de certificat est ajouté à la liste des clés de certificat gérées par Citrix ADM.

- **file** : Représente un fichier.
- **objet** : Ce type est utilisé lorsque vous souhaitez regrouper plusieurs paramètres liés sous un élément parent. Vous devez spécifier le paramètre parent le type comme « objet ». Un paramètre de type « objet » peut avoir une section « paramètres » imbriquée pour décrire les paramètres qu'il contient.
- **un autre StyleBook** : lorsque vous utilisez ce type de paramètre, ce paramètre s'attend à ce que sa valeur soit sous la forme des paramètres définis dans le StyleBook indiquant son type.

Un paramètre peut également avoir un type qui est une liste de l'un des types énumérés ci-dessus, en ajoutant « [] » à la fin du type. Par exemple, si l'attribut type est string [], ce paramètre prend une liste de chaînes en entrée. Vous pouvez fournir une, deux ou plusieurs chaînes pour ce paramètre lors de la création d'une configuration à partir de ce StyleBook.

**Obligatoire ?** Oui

### clé

Spécifiez true ou false pour indiquer si ce paramètre est un paramètre clé pour le StyleBook.

Un StyleBook ne peut avoir qu'un seul paramètre défini comme paramètre « key ».

Lorsque vous créez des configurations différentes à partir du même StyleBook (sur les mêmes instances Citrix ADC ou différentes), chaque configuration a une valeur différente/unique pour ce paramètre.

La valeur par défaut est false.

**Obligatoire ?** Non

### requis

Spécifiez true ou false pour indiquer si un paramètre est obligatoire ou facultatif. S'il est défini sur true, le paramètre est obligatoire et l'utilisateur doit fournir une valeur pour ce paramètre lors de la création de configurations.

L'interface graphique Citrix ADM force l'utilisateur à fournir une valeur valide pour ce paramètre.

La valeur par défaut est false.

### **Obligatoire ?** Non

#### **Remarque**

Si un paramètre a `type: object` et `required: false`, les sous-paramètres de ce paramètre ne sont pas évalués.

Si vous voulez que la valeur par défaut des sous-paramètres prenne effet, définissez `required: true` pour le paramètre principal comme suit :

```
1   type: object
2   required: true
3   gui:
4     collapse_pane: true
5 <!--NeedCopy-->
```

L'attribut `collapse_pane` affiche l'objet et ses sous-paramètres réduits dans l'interface utilisateur, sauf si l'utilisateur développe le volet.

### **valeurs autorisées**

Utilisez cet attribut pour définir une liste de valeurs valides pour un paramètre, lorsque le type est défini sur « string. »

Lors de la création d'une configuration à partir de l'interface graphique Citrix ADM, l'utilisateur est invité à sélectionner une valeur de paramètre dans cette liste.

#### **Exemple 1 :**

nom : adresse IP

type : chaîne

allowed-values:

- SOURCEIP
- DEST IP
- NONE

#### **Exemple 2 :**

nom : Port TCP

type : tcp-port

allowed-values:

- 80

- 81
- 8080

**Exemple 3 :**

(liste des ports tcp-, où chaque élément de la liste ne peut avoir que des valeurs spécifiées dans des valeurs autorisées)

nom : tcpports

type : tcp-port []

allowed-values:

- 80
- 81
- 8080
- 8081

**Obligatoire ?** Non

**default**

Utilisez cet attribut pour affecter une valeur par défaut à un paramètre facultatif. Lors de la création d'une configuration, si un utilisateur ne spécifie pas de valeur, la valeur par défaut est utilisée.

Lors de la création de la configuration à partir de l'interface graphique Citrix ADM, si un utilisateur ne fournit pas de valeur pour un paramètre qui n'a pas de valeur par défaut, aucune valeur n'est définie pour ce paramètre.

**Exemple 1 :**

nom : délai d'expiration

type : nombre

default : 20

**Exemple 2 :**

(où, la valeur par défaut du paramètre est une liste de valeurs) :

nom : protocoles

type : chaîne []

par défaut :

- TCP

- UDP
- Adresse IP

**Exemple 3 :**

nom : délai d'expiration

type : nombre

défaut: 20

**Exemple 4:**

nom : tcpport

type : tcp-port

défaut: 20

**Obligatoire ?** Non

**modèle**

Utilisez cet attribut pour définir un motif (expression régulière) pour les valeurs valides de ce paramètre, lorsque le type du paramètre est « string. »

**Exemple :**

name : appname

type : chaîne

motif : « [a-z] + »

**Obligatoire ?** Non

**min-value**

Utilisez cet attribut pour définir la valeur minimale des paramètres de type « number » ou « tcp-port ».

**Exemple :**

nom : audio-port

type : tcp-port

min-value : 5000

La valeur min. des nombres peut être négative, mais la valeur min. pour tcp-port ne doit pas être négative.

**Obligatoire ?** Non

### **max-value**

Utilisez cet attribut pour définir la valeur maximale des paramètres de type « number » ou « tcp-port ».

La valeur maximale doit être supérieure à la valeur minimale, si elle est définie.

#### **Exemple :**

nom : audio-port

type : tcp-port

min-value : 5000

valeur max-: 15000

**Obligatoire ?** Non

### **min-length**

Utilisez cet attribut pour définir la longueur minimale des valeurs acceptées pour un paramètre de type « string. »

La longueur minimale des caractères définis en tant que valeurs doit être supérieure ou égale à zéro.

#### **Exemple :**

name : appname

type : chaîne

min-length : 3

**Obligatoire ?** Non

### **max-length**

Utilisez cet attribut pour définir la longueur maximale des valeurs acceptées pour un paramètre de type « string. »

La longueur maximale des valeurs doit être supérieure ou égale à la longueur des caractères définis en min-length.

#### **Exemple :**

name : appname

type : chaîne



max-length : 64

**Obligatoire** ? Non

### **min-items**

Utilisez cet attribut pour définir le nombre minimum d'éléments dans un paramètre qui est une liste.

Le nombre minimum d'éléments doit être supérieur ou égal à zéro.

**Exemple :**

nom : server-ips

type : ipaddress[]

min-items : 2

**Obligatoire** ? Non

### **max-items**

Utilisez cet attribut pour définir le nombre maximal d'éléments dans un paramètre qui est une liste.

Le nombre maximal d'articles doit être supérieur au nombre minimum d'articles s'il est défini.

**Exemple :**

nom : server-ips

type : ipaddress[]

min-items : 2

max-items : 250

**Obligatoire** ? Non

### **Gui**

Utilisez cet attribut pour personnaliser la mise en page du paramètre de type « object » dans l'interface graphique Citrix ADM.

**Obligatoire** ? Non

**colonnes**

Ceci est un sous-attribut de l'attribut gui. Utilisez-le pour définir le nombre de colonnes à afficher dans l'interface graphique Citrix ADM.

**Obligatoire ?** Non

**modifiable**

Ceci est un sous-attribut de l'attribut gui. Utilisez cette option pour spécifier si le paramètre peut être mis à jour après la création de la configuration.

Si la valeur est définie sur false, le champ de paramètre est grisé lorsque vous mettez à jour la configuration.

**Obligatoire ?** Non

**collapse\_pane**

Ceci est un sous-attribut de l'attribut gui. Utilisez cette option pour spécifier si le volet définissant la disposition de ce paramètre d'objet est pliable.

Si la valeur est définie sur true, l'utilisateur peut développer ou réduire les paramètres enfants sous ce paramètre parent.

**Exemple :**

```
1   gui:
2
3     collapse_pane: true
4
5     columns: 2
6
7     updatable: false
8 <!--NeedCopy-->
```

Exemple de section complète des paramètres :

```
1 parameters:
2
3   -
4
5     name: name
6
7     label: Name
8
9     description: Name of the application
10
```

```
11     type: string
12
13     required: true
14
15     -
16
17         name: ip
18
19         label: IP Address
20
21         description: The virtual IP address used for this application
22
23         type: ipaddress
24
25         required: true
26
27     -
28
29         name: svc-servers
30
31         label: Servers
32
33         type: object[]
34
35         required: true
36
37         parameters:
38
39             -
40
41                 name: svc-ip
42
43                 label: Server IP
44
45                 description: The IP address of the server
46
47                 type: ipaddress
48
49                 required: true
50
51             -
52
53                 name: svc-port
54
55                 label: Server Port
56
57                 description: The TCP port of the server
58
59                 type: tcp-port
60
61                 default: 80
62
63     -
```

```
64
65     name: lb-alg
66
67     label: LoadBalancing Algorithm
68
69     type: string
70
71     allowed-values:
72
73     - ROUNDROBIN
74
75     - LEASTCONNECTION
76
77     default: ROUNDROBIN
78
79 -
80
81     name: enable-healthcheck
82
83     label: Enable HealthCheck?
84
85     type: boolean
86
87     default: true
88 <!--NeedCopy-->
```

Voici un exemple qui définit tous les attributs d'une liste et les valeurs expliquées dans les sections précédentes :

“YAML

```
name: features-list
type: string[]**
min-length: 1
max-length: 3
min-items: 1
max-items: 3
pattern: “[A-Z]+”
allowed-values:
- SP
- LB
- CS
default:
- LB
```

## Parameters-default-sources construct

February 1, 2024

Vous pouvez utiliser cette construction pour réutiliser les définitions de paramètres d'autres StyleBooks.

Imaginons un scénario dans lequel un paramètre ou un groupe de paramètres est utilisé à plusieurs reprises dans plusieurs StyleBooks. **Pour éviter de redéfinir ces paramètres, chaque fois que vous souhaitez créer un nouveau StyleBook, vous pouvez les définir une fois, puis importer leurs définitions dans les StyleBooks qui ont besoin de ces paramètres à l'aide de la construction parameters-default-sources.**

Par exemple, si plusieurs de vos StyleBooks doivent configurer une adresse IP virtuelle, vous devrez peut-être définir les mêmes paramètres liés aux adresses IP virtuelles dans chaque nouveau StyleBook que vous créez. Au lieu de cela, vous pouvez créer un StyleBook distinct appelé, par exemple, « vip-params » dans lequel vous définissez tous les paramètres associés, comme indiqué dans l'exemple suivant :

```
1      -
2      name: vip-params
3      namespace: com.acme.commonypes
4      version: "1.0"
5      description: This StyleBook defines a typical virtual IP config.
6      private: true
7      schema-version: "1.0"
8      parameters:
9      -
10         name: lb-appname
11         label: Load Balanced Application Name
12         description: Name of the Load Balanced application
13         type: string
14         required: true
15     -
16         name: lb-virtual-ip
17         label: Load Balanced App Virtual IP address
18         description: Virtual IP address representing the Load
19         Balanced application
20         type: ipaddress
21         required: true
22     -
23         name: lb-virtual-port
24         label: Load Balanced App Virtual Port
25         description: TCP port representing the Load Balanced
26         application
27         type: tcp-port
28         default: 80
29     -
30         name: lb-service-type
```

```

29     label: Load Balanced App Protocol
30     description: Protocol used for the Load Balanced application
31     .
32     type: string
33     default: HTTP
34     required: true
35     allowed-values:
36     - HTTP
37     - SSL
38     - TCP
39 <!--NeedCopy-->

```

Ensuite, vous pouvez créer d'autres StyleBooks utilisant ces paramètres. Voici un exemple d'un tel StyleBook.

```

1     -
2     name: acme-biz-app
3     namespace: com.acme.stylebooks
4     version: "1.0"
5     description: This stylebook defines the Citrix ADC configuration
6     for Biz App
7     schema-version: "1.0"
8     import-stylebooks:
9     -
10    namespace: com.acme.commontypes
11    prefix: cmtypes
12    version: "1.0"
13    parameters-default-sources:
14    - cmtypes::vip-params
15    parameters:
16    -
17    name: monitorname
18    label: Monitor Name
19    description: Name of the monitor
20    type: string
21    required: true
22    -
23    name: type
24    label: Monitor Type
25    description: Type of the monitor
26    type: string
27    required: true
28    allowed-values:
29    - PING
30    - TCP
31    - HTTP
32    - HTTP-ECV
33    - TCP-ECV
34    - HTTP-INLINE
35 <!--NeedCopy-->

```

Dans StyleBook, acme-biz-app, tout d'abord, l'espace de noms et la version du styleBook vip-params sont importés à l'aide de la section « import-stylebooks ». Ensuite, la construction **parameters-**

**default-sources** est ajoutée et le nom StyleBook, c'est-à-dire vip-params, est spécifié. Cela a le même effet que de définir les paramètres du styleBook vip-params directement dans ce StyleBook.

Vous pouvez inclure des paramètres de plusieurs StyleBooks, car les parameters-default-sources sont une liste et chaque élément de la liste doit être un StyleBook.

En plus d'inclure des paramètres provenant d'autres StyleBooks, vous pouvez également définir vos propres paramètres en utilisant la section des paramètres. La liste complète des paramètres du Style-Book est la combinaison de paramètres inclus dans d'autres StyleBooks et de paramètres définis dans ce StyleBook. Par conséquent, l'expression **\$parameters** fait référence à cette combinaison de paramètres.

Notez que si un paramètre est défini à la fois dans un StyleBook importé et dans le StyleBook actuel, la définition du StyleBook actuel remplace la définition importée depuis un autre StyleBook. Vous pouvez l'utiliser efficacement en personnalisant certains paramètres importés si nécessaire, tout en utilisant les autres paramètres importés tels quels.

La construction parameters-default-sources peut également être utilisée dans les paramètres imbriqués comme indiqué :

```
1 parameters:
2   -
3     name: vip-details
4     label: Virtual IP details
5     description: Details of the Virtual IP
6     type: object
7     required: true
8     parameters-default-sources:
9       - cmtypes::vip-params
10 <!--NeedCopy-->
```

Cela revient à ajouter les paramètres des paramètres vip-params de StyleBook directement en tant que paramètres enfants du paramètre vip-details dans ce StyleBook.

## Substitutions

February 1, 2024

La section substitutions est utilisée pour définir des noms abrégés pour des expressions complexes qui peuvent être utilisés dans le reste du StyleBook afin de faciliter la lecture du StyleBook. Ils sont également utiles lorsque la même expression ou valeur est répétée plusieurs fois dans le StyleBook, par exemple une valeur constante. L'utilisation d'un nom de substitution pour cette valeur vous permet de mettre à jour uniquement la valeur de substitution lorsque cette valeur doit être modifiée plutôt que de la mettre à jour à chaque emplacement où elle apparaît dans le StyleBook, ce qui pourrait être sujet à des erreurs.

Les substitutions sont également utilisées pour définir des correspondances entre les valeurs, comme décrit dans des exemples plus loin dans ce document.

Chaque substitution dans la liste est composée d'une clé et d'une valeur. La valeur peut être une valeur simple, une expression, une fonction ou une carte.

Dans l'exemple suivant, deux substitutions sont définies. Le premier est « http-port » qui peut être utilisé comme abrégé pour 8181. En utilisant une substitution, vous pouvez désigner cela dans le reste du StyleBook comme **\$substitutions.http-port** au lieu de 8181.

**substitutions :**

http-port : 8181

Cela vous permet de spécifier un nom mnémorique à un numéro de port et de définir ce numéro de port en un seul endroit dans le StyleBook, quel que soit le nombre de fois qu'il est utilisé. Si vous voulez modifier le numéro de port en 8080, vous pouvez le modifier dans la section de substitution, et la modification prendra effet partout où le nom mnémorique http-port est utilisé. L'exemple suivant montre comment une substitution est utilisée dans un composant.

```
1 components:
2   -
3     name: my-lbvserver-comp
4     type: ns::lbvserver
5     properties:
6       name: $parameters.name + "-lb"
7       servicetype: HTTP
8       ipv46: $parameters.ip
9       port: \*\*$substitutions.http-port\*\*
10      lbmethod: $parameters.lb-alg
11 <!--NeedCopy-->
```

Une substitution peut également être une expression complexe. L'exemple suivant montre comment deux substitutions utilisent des expressions.

```
1 substitutions:
2   app-rule: HTTP.REQ.HEADER("X-Test-Application").EXISTS
3   app-name: str("acme-") + $parameters.name + str("-app")
4 <!--NeedCopy-->
```

Une expression de substitution peut également utiliser des expressions de substitution existantes, comme indiqué dans l'exemple suivant.

```
1 substitutions:
2   http-port: 8181
3   app-name: str("acme-") + $parameters.name + str($substitutions.http-
4     port) + str("-app")
4 <!--NeedCopy-->
```

Les cartes sont une autre fonctionnalité utile des substitutions, dans lesquelles vous pouvez associer



des clés à des valeurs. Voici un exemple de substitution de carte.

```

1 substitutions:
2   secure-port:
3     true: int("443")
4     false: int("80")
5   secure-protocol:
6     true: SSL
7     false: HTTP
8 <!--NeedCopy-->

```

L'exemple suivant montre comment utiliser les cartes secure-port et secure-protocol.

```

1 components:
2   -
3     name: my-lbserver-comp
4     type: ns::lbserver
5     properties:
6       name: $parameters.name + "-lb"
7       servicetype: \*\*$substitutions.secure-protocol[$parameters.
is-secure]\*\*
8       ipv46: $parameters.ip
9       port: \*\*$substitutions.secure-port[$parameters.is-secure
]\*\*
10      lbmethod: $parameters.lb-alg
11 <!--NeedCopy-->

```

Cela implique que si l'utilisateur de StyleBook spécifie la valeur booléenne « true » au paramètre is-secure, ou coche la case correspondant à ce paramètre dans l'interface graphique Citrix ADM, la propriété servicetype de ce composant est affectée à la valeur **SSL** et la propriété port est attribuée la valeur **443**. Toutefois, si l'utilisateur spécifie « false » pour ce paramètre ou désactive la case à cocher correspondante dans l'interface graphique de Citrix ADM, la propriété servicetype reçoit la valeur **HTTP** et le port reçoit la valeur **80**.

L'exemple suivant montre comment utiliser les substitutions en tant que fonction. Une fonction de substitution peut prendre un ou plusieurs arguments. Les arguments doivent être de type simple par exemple, string, number, ipaddress, booléen et autres types.

#### **substitutions :**

```
form-lb-name(name): $name + "-lb"
```

Dans cet exemple, nous définissons une fonction de substitution « form-lb-name » qui prend un argument de chaîne appelé « name » et l'utilise pour créer une nouvelle chaîne qui suffixe « -lb » à la chaîne dans l'argument name. Une expression utilisant cette fonction de substitution peut être écrite comme suit :

```
$substitutions.form-lb-name("my")
```

qui renvoie « my-lb »

Prenons un autre exemple :

**substitutions :**

```
cspol-priority(priority): 10100 - 100 * $priority
```

La substitution `cspol-priority` est une fonction qui prend un argument appelé `priority` et l'utilise pour calculer une valeur. Dans le reste du StyleBook, cette substitution peut être utilisée comme illustré dans l'exemple suivant :

```
1 components:
2   -
3     name: cspolicy-binding-comp
4     type: ns::csvserver_cspolicy_binding
5     condition: not $parameters.is-default
6     properties:
7       name: $parameters.csvserver-name
8       policyname: $components.cspolicy-comp.properties.policyname
9       priority: $substitutions.cspol-priority($parameters.pool.
10    priority)
11 <!--NeedCopy-->
```

La substitution peut également être composée d'une clé et d'une valeur. La valeur peut être une valeur simple, une expression, une fonction, une carte, une liste ou un dictionnaire.

Voici un exemple de substitution appelée 'slist' dont la valeur est une liste :

```
1 substitutions:
2   slist:
3     - a
4     - b
5     - c
6 <!--NeedCopy-->
```

La valeur d'une substitution peut également être un dictionnaire de paires clé-valeur comme on le voit dans l'exemple suivant d'une substitution appelée 'sdict' ci-dessous :

```
1 substitutions:
2   sdict:
3     a: 1
4     b: 2
5     c: 3
6 <!--NeedCopy-->
```

Vous pouvez créer des attributs plus complexes en combinant les listes et les dictionnaires. Par exemple, une substitution appelée « slistofdict » renvoie une liste de paires clé-valeur.

```
1 slistofdict:
2   -
3     a: $parameters.cs1.lb1.port
4     b: $parameters.cs1.lb2.port
5   -
```

```

6     a: $parameters.cs2.lb1.port
7     b: $parameters.cs2.lb2.port
8 <!--NeedCopy-->

```

Mais, dans l'exemple suivant, une substitution « sdictoflist » renvoie une paire clé-valeur, où la valeur elle-même est une autre liste.

```

1     sdictoflist:
2     a:
3         - 1
4         - 2
5     b:
6         - 3
7         - 4
8 <!--NeedCopy-->

```

Dans les composants, ces substitutions peuvent être utilisées dans les constructions de condition, de propriétés, de répétition, de condition.

L'exemple suivant d'un composant montre comment une substitution peut être utilisée lors de la spécification des propriétés :

```

1     properties:
2     a: $substitutions.slist
3     b: $substitutions.sdict
4     c: $substitutions.slistofdict
5     d: $substitutions.sdictoflist
6 <!--NeedCopy-->

```

Un cas d'utilisation pour définir une substitution dont la valeur est une liste ou un dictionnaire est lorsque vous configurez un serveur virtuel de commutation de contenu et plusieurs serveurs virtuels d'équilibrage de charge. Puisque tous les serveurs virtuels lb liés au même serveur virtuel cs peuvent avoir une configuration identique, vous pouvez utiliser la liste de substitution et le dictionnaire pour créer cette configuration afin d'éviter de répéter cette configuration pour chaque serveur virtuel lb.

L'exemple suivant montre la substitution et le composant dans les cs-lb-mon StyleBooks pour créer une configuration de serveur virtuel de commutation de contenu. Lors de la construction des propriétés de cs-lb-mon StyleBooks, la substitution complexe « lb-properties » spécifie les propriétés des serveurs virtuels lb associés au serveur virtuel cs. La substitution « lb-properties » est une fonction qui prend le nom, le type de service, l'adresse IP virtuelle, le port et les serveurs comme paramètres et génère une paire clé-valeur comme valeur. Dans le composant « cs-pools », nous assignons la valeur de cette substitution au paramètre lb-pool pour chaque pool.

```

1 substitutions:
2   cs-port[]:
3     true: int("80")
4     false: int("443")
5   lb-properties(name, servicetype, vip, port, servers):
6     lb-appname: $name

```

```

7     lb-service-type: $servicetype
8     lb-virtual-ip: $vip
9     lb-virtual-port: $port
10    svc-servers: $servers
11    svc-service-type: $servicetype
12    monitors:
13      -
14        monitorname: $name
15        type: PING
16        interval: $parameters.monitor-interval
17        interval_units: SEC
18        retries: 3
19    components:
20      -
21        name: cs-pools
22        type: stlb::cs-lb-mon
23        description: | Updates the cs-lb-mon configuration with the
24                      different pools provided. Each pool with rule result in a dummy LB
25                      vserver, cs action, cs policy, and csvserver_cspolicy_binding
26                      configuration.
27        condition: $parameters.server-pools
28        repeat: $parameters.server-pools
29        repeat-item: pool
30        repeat-condition: $pool.rule
31        repeat-index: ndx
32        properties:
33          appname: $parameters.appname + "-cs"
34          cs-virtual-ip: $parameters.vip
35          cs-virtual-port: $substitutions.cs-port($parameters.protocol == "
36          HTTP")
37          cs-service-type: $parameters.protocol
38          pools:
39            -
40              lb-pool: $substitutions.lb-properties($pool.pool-name, "HTTP"
41              , "0.0.0.0", 0, $pool.servers)
42              rule: $pool.rule
43              priority: $ndx + 1
44    <!--NeedCopy-->

```

**Carte de substitution :**

Vous pouvez créer des substitutions qui associent des clés à des valeurs. Par exemple, imaginez un scénario dans lequel vous souhaitez définir le port par défaut (valeur) à utiliser pour chaque protocole (clé). Pour cette tâche, écrivez une carte de substitution comme suit.

```

1 substitutions:
2   port:
3     HTTP: 80
4     DNS: 53
5     SSL: 443
6 <!--NeedCopy-->

```

Dans cet exemple, HTTP est mappé à 80, DNS est mappé à 53 et SSL est mappé à 443. Pour récupérer

le port d'un certain protocole donné en tant que paramètre, utilisez l'expression

`$substitutions.port[$parameters.protocol]`

L'expression renvoie une valeur basée sur le protocole spécifié par l'utilisateur.

- Si la clé est HTTP, l'expression renvoie 80
- Si la clé est DNS, l'expression renvoie 53
- Si la clé est SSL, l'expression renvoie 443
- Si la clé n'est pas présente dans la carte, l'expression ne renvoie aucune valeur

## Composants

February 1, 2024

La construction Components d'un StyleBook est considérée comme la section la plus importante du StyleBook. Dans cette section, vous définissez les objets de configuration qui doivent être créés. À l'aide de cette construction, vous pouvez créer un ou plusieurs objets de configuration du même type.

La construction des composants peut utiliser l'entrée fournie dans la section des paramètres pour adapter la configuration générée par le StyleBook. Cette section est facultative, bien que la plupart des StyleBooks aient une section sur les composants.

Le tableau suivant décrit les principaux attributs d'un composant.

Attribut	Description
nom	Le nom du composant. Vous pouvez spécifier un nom alphanumérique. Le nom doit commencer par un alphabet et peut inclure des alphabets, des chiffres, un tiret (-) ou un trait de soulignement (_) supplémentaires.
description	Description du rôle de ce composant dans le StyleBook.
type	Le type détermine les propriétés que ce composant fournit. Les composants ont deux types de types : <b>Type intégré</b> : Ce type est fourni par le système et vous n'avez pas à le définir, par exemple, les types d'entités NITRO « lbserver » ou « servicegroup ». Lorsqu'un composant dispose d'un attribut type intégré, il crée un objet de configuration de ce type sur l'Citrix ADC. Par exemple, si un composant fait référence au type intégré « lbserver », ce composant crée un serveur virtuel d'équilibrage de charge sur l'instance de Citrix ADC qui est la cible de la configuration. <b>Type composite</b> : ce type fait référence à un StyleBook existant que vous avez créé et importé dans Citrix ADM. Lorsqu'un composant possède un attribut de type composite, il crée tous les objets de configuration, qui sont spécifiés dans le StyleBook référencé, sur l'instance Citrix ADC qui est la cible de la configuration. Cela vous permet de combiner plusieurs StyleBooks où chaque StyleBook

crée une partie de la configuration finale. Pour plus d'informations sur les StyleBooks composites, voir [Créer un StyleBook composite](/fr-fr/netScaler-application-delivery-management-software/12-1/stylebooks/how-to-create-custom-stylebooks).

| propriétés|Les sous-attributs qui peuvent être utilisés pour un attribut de type de composant. Les propriétés valides pour un composant sont dictées par son type. Pour un type intégré, il s'agit des propriétés ou des attributs de l'objet Nitro correspondant. Pour un composant dont le type est un autre StyleBook, c'est-à-dire un type composite, les propriétés correspondent aux paramètres définis dans ce StyleBook.

|

#### Exemple :

```
1 components:
2   -
3     name: my-lbvserver-comp
4     type: ns::lbvserver
5     properties:
6       name: $parameters.name
7       servicetype: HTTP
8       ipv46: $parameters.ip
9       port: 80
10      lbmethod: $parameters.lb-alg
11 <!--NeedCopy-->
```

Dans cet exemple, vous avez défini un composant appelé my-lbvserver-comp. Ce composant est du type ns : :lbvserver (un type intégré), où « ns » est le préfixe qui fait référence à l'espace de noms netScaler.nitro.config et à la version 10.5 que vous avez spécifié dans la section import-stylebooks, et « lbvserver » est une ressource NITRO dans cet espace de noms.

Les propriétés de cette section incluent quatre attributs obligatoires et un attribut facultatif (lbmethod) de la ressource « lbvserver » et vous permettent de spécifier des valeurs pour ces attributs. Dans cet exemple, vous spécifiez des valeurs statiques pour le type de service et le port alors que les propriétés name, ipv46 et lbmethod obtiennent leurs valeurs à partir des paramètres d'entrée. Vous vous référez aux noms de paramètres définis dans la section des paramètres en utilisant \$parameters.<name> notation, par exemple, \$parameters.ip.

#### Remarque

Vous devez utiliser des minuscules pour les noms d'attributs des types de ressources NITRO (les propriétés de ses composants). Sinon, l'importation d'un StyleBook échouera.

## Composants d'assistance

February 1, 2024

L'utilisation principale de la section des composants dans un StyleBook est de générer des objets de configuration via des types intégrés de Nitro ou un autre StyleBook qui crée les objets de configuration réels. Les composants d'assistance ne construisent pas d'objets de configuration par eux-mêmes. Les composants auxiliaires prennent les entrées d'autres sections, telles que les objets de paramètres, les propriétés d'autres composants ou les sorties d'autres composants, et les transforment en d'autres formes. Cela peut être utilisé ultérieurement par d'autres composants pour générer les objets de configuration réels. Un composant d'assistance peut être de deux types : un type d'objet ou un autre StyleBook qui ne contient pas de section de composant.

L'exemple suivant illustre un extrait d'un StyleBook utilisé pour créer un serveur d'équilibrage de charge avec moniteur (lb-mon-comp) sur une instance de Citrix ADC.

```
1 parameters:
2   -
3     name: appname
4     type: string
5   -
6     name: ips
7     type: ipaddress[]
8   -
9     name: vip
10    type: ipaddress
11
12 components:
13   -
14     name: help-comp
15     type: cmtypes::server-ip-port-params
16     repeat:
17       repeat-list: $parameters.ips
18       repeat-item: server-ip
19     properties:
20       ip: $server-ip
21       port: 80
22   -
23     name: lb-mon-comp
24     type: stlb::lb-mon
25     properties:
26       lb-appname: $parameters.appname
27       lb-virtual-ip: $parameters.vip
28       lb-virtual-port: 80
29       lb-service-type: HTTP
30       svc-service-type: HTTP
31       svc-servers: $components.help-comp.properties
32 <!--NeedCopy-->
```

La section Paramètres vous permet d'entrer le nom de l'application et les adresses IP des serveurs d'équilibrage de charge. Dans la section du composant lb-mon-comp, le paramètre svc-servers de lb-mon StyleBook attend une liste d'objets où chaque élément possède deux sous-paramètres : ip et port.

Cependant, la section paramètres de ce StyleBook accepte uniquement les adresses IP du serveur via `$parameters.ips`. Le StyleBook suppose que tous les serveurs s'exécutent sur le port 80. Pour créer la configuration d'équilibrage de charge à l'aide de `lb-mon` StyleBook, vous devez transformer le fichier `$parameters.ips` en une liste d'objets. Ceci est réalisé à l'aide du composant d'assistance, `help-comp` dans l'exemple ci-dessus. Le composant `help-comp` est du type `server-ip-port-params` StyleBook. Ce StyleBook ne comporte aucun composant. Par conséquent, il ne crée aucun objet de configuration. Le `help-comp` crée une liste répétée sur `$parameters.ips` et construit un objet composé d'une adresse IP et d'un port (défini sur une valeur statique de 80) pour chaque élément de `$parameters.ips`. Ainsi, `help-comp` transforme une liste d'adresses IP en une liste d'objets qui peuvent être utilisés ultérieurement dans `lb-mon-comp` pour attribuer la propriété `svc-servers`. Le résultat de la commande `help-comp` est attribué à la propriété `svc-servers` de `lb-mon-comp`.

## Propriétés facultatives

February 1, 2024

Dans certains cas, la valeur d'une propriété d'un composant provient d'une expression, qui peut être une expression simple, telle qu'une référence de paramètre, ou une expression plus complexe. La définition de cette valeur de propriété est facultative dans le composant. Vous pouvez choisir de définir la valeur de la propriété uniquement si l'expression renvoie une valeur réelle, sinon vous pouvez choisir de ne pas définir cette propriété.

Par exemple, considérez que l'une des propriétés que vous souhaitez définir est la méthode `lbmethod` (algorithme d'équilibrage de charge) d'un composant dont le type est `ns::lbserver`. La valeur de la propriété `lbmethod` est extraite d'une valeur de paramètre fournie par l'utilisateur, comme indiqué ci-dessous :

```
1 components
2   -
3     name: lbserver_comp
4     type: ns::lbserver
5     properties:
6       name: $parameters.lb-appname + "-lb"
7       servicetype: $parameters.lb-service-type
8       ipv46: $parameters.lb-virtual-ip
9       port: 80
10      lbmethod: $parameters.lb-advanced.algorithm
11 <!--NeedCopy-->
```

Maintenant, considérez que le paramètre **`lb-advanced.algorithm`** est un paramètre facultatif. Et, si l'utilisateur ne fournit pas de valeur pour ce paramètre parce qu'il est facultatif, l'expression **`$parameters.lb-advanced.algorithm`** est évaluée à valeur vide. Par conséquent, une valeur non



valide est transmise pour la propriété `lbmethod`. Afin d'éviter une telle situation, vous pouvez annoter la propriété comme facultative en suffixant son nom avec « ? » comme suit :

```
1 components
2   -
3     name: lbserver_comp
4     type: ns::lbserver
5     properties:
6       name: $parameters.lb-appname + "-lb"
7       servicetype: $parameters.lb-service-type
8       ipv46: $parameters.lb-virtual-ip
9       port: 80
10      lbmethod?: $parameters.lb-advanced.algorithm
11 <!--NeedCopy-->
```

L'utilisation de « ? » omet la propriété si l'expression sur le droit n'évalue rien, ce qui équivaldrait, dans ce cas, à un composant défini comme suit :

```
1 components
2   -
3     name: lbserver_comp
4     type: ns::lbserver
5     properties:
6       name: $parameters.lb-appname + "-lb"
7       servicetype: $parameters.lb-service-type
8       ipv46: $parameters.lb-virtual-ip
9       port: 80
10 <!--NeedCopy-->
```

Comme **lbmethod** est facultatif, son omission en fait un composant valide. Notez que `lbmethod` peut prendre sa valeur par défaut si elle est définie dans son type « `ns : lbserver` ».

## Properties-Default-Sources, construction

February 1, 2024

La construction `properties-default-sources` est analogue à la construction `parameters-default-sources`. Alors que la construction `parameters-default-sources` permet la réutilisation de paramètres existants (provenant d'autres StyleBooks) dans un StyleBook, la construction `properties-default-sources` permet à l'utilisateur de spécifier les propriétés d'un composant en fonction de sources existantes.

Les propriétés d'un composant peuvent être réparties dans différentes sections du StyleBook. Par exemple, les propriétés peuvent provenir de paramètres d'objets, de substitutions renvoyant un objet, de propriétés d'autres composants ou de sorties d'autres composants. Dans ce cas, vous devez redéfinir les propriétés qui apparaissent dans d'autres sections du StyleBook dans la définition

du composant. Il est clair que cela est redondant et peut entraîner des erreurs. Pour résoudre ce problème, la construction `properties-default-sources` peut être utilisée. La construction `properties-default-sources` est une liste dans laquelle chaque élément identifie une source pour certaines propriétés du composant.

Par exemple, considérez un composant qui crée une configuration `lbserver`. Ce composant doit définir les propriétés du serveur `lbserver` comme suit.

```

1 parameters:
2   -
3     name: lb
4     type: ns::lbserver
5 components:
6   -
7     name: lb-comp
8     type: ns::lbserver
9     properties:
10      name: $parameters.lb.name
11      ipv46: $parameters.lb.ipv46
12      port: $parameters.lb.port
13      servicetype: $parameters.lb.servicetype
14      lbmethod: $parameters.lb.lbmethod
15 <!--NeedCopy-->

```

Dans l'exemple ci-dessus, observez que les valeurs de toutes les propriétés définies dans la section composants sont extraites de l'objet `$parameters.lb`. Bien qu'elles soient extraites d'une seule source, les propriétés sont à nouveau définies dans le `StyleBook`. En outre, si un nouveau sous-paramètre de l'objet `$parameters.lb` pertinent pour la configuration du `lbserver` est ajouté, vous devez mettre à jour le composant `lb-comp` pour ajouter la nouvelle propriété correspondant au nouveau sous-paramètre.

Pour éviter de redéfinir les propriétés et récupérer toutes les propriétés pertinentes d'un composant sans les énumérer explicitement dans la section propriétés, la construction `properties-default-sources` peut être utilisée. L'exemple ci-dessus peut être écrit comme suit.

```

1 parameters:
2   -
3     name: lb
4     type: ns::lbserver
5 components:
6   -
7     name: lb-comp
8     type: ns::lbserver
9     properties-default-sources:
10      - $parameters.lb
11 <!--NeedCopy-->

```

Dans l'exemple ci-dessus, l'utilisation de la construction `properties-default-sources` entraîne une réduction de la taille de la définition du composant, ce qui vous permet de définir un composant de

manière concise. De plus, chaque fois que la source des propriétés du composant change, les modifications sont reflétées automatiquement. Par exemple, lorsqu'une nouvelle propriété, par exemple « persistencetype », est ajoutée à l'objet \$parameters.lb, cette propriété est ajoutée à la configuration de lb-comp par défaut puisque persistencetype est une propriété de lbserver. Ainsi, la construction `properties-default-sources` fournit une interface dynamique pour définir les composants sans se soucier des changements qui se produisent dans les sources des propriétés du composant.

## Calcul des propriétés du composant

Cette section explique comment les propriétés sont récupérées si la construction `properties-default-sources` est utilisée dans un composant. Tout d'abord, le compilateur StyleBooks identifie la liste des propriétés d'un composant en fonction de son type (dans l'exemple ci-dessus, `lbserver`). Ensuite, le compilateur récupère ces propriétés à partir des multiples sources dans l'ordre dans lequel elles sont définies (dans la section `properties-default-sources` du composant). Si une propriété existe dans plusieurs sources, la propriété apparaissant dans la dernière source a priorité sur les autres. Enfin, une propriété récupérée à l'aide de la construction `properties-default-sources` peut être remplacée dans la section propriétés du composant. Il est important de noter que la définition d'une section de composant doit au moins comporter une section `properties-default-sources` ou une section de propriétés. Il peut avoir les deux.

## Composants imbriqués

February 1, 2024

L'imbrication d'un composant dans un autre composant permet au composant imbriqué de créer ses objets de configuration en se référant aux objets de configuration ou au contexte créé par le composant parent. Le composant imbriqué peut créer un ou plusieurs objets pour chaque objet créé dans le composant parent. L'imbrication d'un composant dans un autre composant n'indique aucune relation entre les objets de configuration créés. L'imbrication permet aux composants de créer plus facilement des objets de configuration dans un contexte existant des composants parents.

### Exemple :

```
1 components:
2   -
3     name: my-lbserver-comp
4     type: ns::lbserver
5     properties:
6       name: $parameters.name + "-lb"
7       servicetype: HTTP
8       ipv46: $parameters.ip
```

```

9     port: 80
10    lbmethod: $parameters.lb-alg
11    components:
12      -
13        name: my-svcg-comp
14        type: ns::servicegroup
15        properties:
16          name: $parameters.name + "-svcgrp"
17          servicetype: HTTP
18        components:
19          -
20            name: lbserver-svg-binding-comp
21            type: ns::lbserver_servicegroup_binding
22            properties:
23              name: $parent.parent.properties.name
24              servicegroupname: $parent.properties.name
25            -
26              name: members-svcg-comp
27              type: ns::servicegroup_servicegroupmember_binding
28              repeat:
29                repeat-list: $parameters.svc-servers
30                repeat-item: srv
31              properties:
32                ip: $srv
33                port: str($parameters.svc-port)
34                servicegroupname: $parent.properties.name
35    <!--NeedCopy-->

```

Dans cet exemple, l'imbrication à plusieurs niveaux est utilisée. Le composant my-lbserver-comp possède un composant enfant appelé my-svcg-comp. Et, le composant my-svcg-comp a deux composants enfants à l'intérieur. Le composant my-svcg-comp est utilisé pour créer un objet de configuration de groupe de services sur l'instance de Citrix ADC en fournissant des valeurs aux attributs du type de ressource NITRO intégré « servicegroup. » Le premier composant enfant du composant my-svcg, lbserver-svg-binding-comp, est utilisé pour lier le groupe de services créé par son composant parent au serveur virtuel d'équilibrage de charge (lbserver) créé par le composant parent du composant parent. La notation \$parent, également appelée référence parente, est utilisée pour faire référence aux entités dans les composants parents. Le deuxième composant enfant, members-svcg-comp, est utilisé pour lier la liste des services au groupe de services créé par le composant parent. La liaison est obtenue en utilisant la construction de répétition de StyleBook pour parcourir la liste des services spécifiés pour le paramètre svc-servers. Pour plus d'informations sur les constructions de répétition, voir [Répétition de construction](#).

Vous pouvez également créer les mêmes objets de configuration sans utiliser l'imbrication de composants. Pour plus d'informations et d'exemples, consultez [StyleBook pour créer une configuration d'équilibrage de charge de base](#).

## Conditionner la construction

February 1, 2024

Vous pouvez rendre un composant conditionnel à l'aide d'une structure de condition. La valeur d'une construction conditionnelle est une expression booléenne dont la valeur est vraie ou fausse. Si la condition est vraie, le composant est utilisé pour créer ses objets de configuration. Si la condition est fausse, le composant est ignoré et aucun objet de configuration n'est créé par son intermédiaire. L'expression booléenne est souvent basée sur des valeurs de paramètres.

### Exemple :

```
1 components:
2   -
3     name: servicegroup-comp
4     type: ns::servicegroup
5     condition: $parameters.svc-server-ips
6     properties:
7       name: $parameters.name + "-svcgrp"
8       servicetype: HTTP
9 <!--NeedCopy-->
```

Dans cet exemple, si l'utilisateur spécifie une valeur pour le paramètre facultatif `svc-server-ips`, le composant, `servicegroup-comp`, est traité par le moteur StyleBook. Si la condition est fausse, c'est-à-dire si l'utilisateur ne fournit pas de valeur à ce paramètre, une valeur nulle est affectée à ce paramètre et est évaluée à `false`, le moteur StyleBook ignore la présence de ce composant et aucun groupe de services n'est créé.

Notez que l'expression booléenne peut être basée sur n'importe quelle expression valide prise en charge dans StyleBooks (par exemple, si un autre composant est présent ou si un paramètre a une certaine valeur).

L'exemple suivant génère l'objet de configuration de type NITRO `ns::systemfile` si la condition est évaluée comme vraie.

### Exemple :

```
1     components
2       -
3         name: pem_key_files
4         type: ns::systemfile
5         condition: "$components.der-certificate-files-comp or
6 $components.pem-certificate-files-comp"
7         properties:
8           filecontent: $certificate.keyfile.contents
9           fileencoding: "BASE64"
10          filelocation: "/nsconfig/ssl"
11          filename: $certificate.keyfile.filename
```

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

Dans cet exemple, la condition est une expression « OR » complexe, dans laquelle vous souhaitez que cet objet de configuration soit créé par le StyleBook uniquement si deux autres composants du Style-Book ont été traités (non ignorés), créant ainsi une dépendance entre les composants.

## Construction repeat

February 1, 2024

Vous pouvez utiliser la construction **répétée** d'un composant pour créer plusieurs objets de configuration du même type.

Dans l'exemple suivant, le composant **members-svcg-comp** est utilisé pour lier la liste des services au groupe de services créé par le composant parent. Pour créer un objet de configuration qui lie chaque serveur au groupe de services, utilisez la construction de **répétition** pour parcourir la liste des services spécifiés pour le paramètre **svc-servers**. Au cours de l'itération, le composant crée un objet NITRO de type **servicegroup\_servicegroupmember\_binding** pour chaque service (appelé **srv** dans la construction **répét-item**) dans le groupe de services, et il définit l'attribut **ip** de chaque objet NITRO sur l'adresse IP du service correspondant.

### Exemple :

```
1 components:
2   -
3     name: my-lbvserver-comp
4     type: ns::lbvserver
5     properties:
6       name: $parameters.name + "-lb"
7       servicetype: HTTP
8       ipv46: $parameters.ip
9       port: 80
10      lbmethod: $parameters.lb-alg
11      components:
12        -
13          name: my-svcg-comp
14          type: ns::servicegroup
15          properties:
16            name: $parameters.name + "-svcgrp"
17            servicetype: HTTP
18          components:
19            -
20              name: lbvserver-svg-binding-comp
21              type: ns::lbvserver\servicegroup\binding
22              properties:
23                name: $parent.parent.properties.name
```

```

24         servicegroupname: $parent.properties.
      name
25         -
26         name: members-svcg-comp
27         type: ns::servicegroup\servicegroupmember\
      binding
28         repeat:
29           repeat-list: $parameters.svc-servers
30           repeat-item: srv
31         properties:
32           ip: $srv
33           port: $parameters.svc-port
34           servicegroupname: $parent.properties.
      name
35 <!--NeedCopy-->

```

La **répétition** est un objet en soi, et **repeat-list** et **repeat-item** sont des attributs de l'objet répété.

- **repeat-list** est un attribut obligatoire qui identifie la liste sur laquelle le composant itère.
- **repeat-item** est facultatif et est utilisé pour donner un nom convivial à l'élément actif dans l'itération.

S'il n'est pas spécifié, l'élément en cours est accessible à l'aide de l'expression **\$repeat-item**. Le dernier composant de l'exemple ci-dessus peut également être écrit comme suit :

```

1         -
2         name: members-svcg-comp
3         type: ns::servicegroup_servicegroupmember_binding
4         repeat:
5           repeat-list: $parameters.svc-servers
6         properties:
7           ip: $repeat-item
8           port: $parameters.svc-port
9           servicegroupname: $parent.properties.name
10 <!--NeedCopy-->

```

En plus de pouvoir faire référence à l'élément en cours en itérant sur une liste, il est également possible de faire référence à l'index actuel de l'élément de la liste à l'aide de **repeat-index**. Dans l'exemple suivant, **repeat-index** est utilisé pour calculer un numéro de port basé sur l'index actuel :

```

1         name: services
2         type: ns::service
3         repeat:
4           repeat-list: $parameters.app-services
5           repeat-item: srv
6         properties:
7           ip: $parameters.app-ip
8           port: $parameters.base-port + repeat-index
9           servicegroupname: $parent.properties.name
10 <!--NeedCopy-->

```

Comme pour la construction **repeat-item**, vous pouvez attribuer un nom de variable différent pour faire référence à l'index actuel de l'itération. L'exemple précédent est équivalent à l'exemple suivant :

```
1      -
2          name: services
3          type: ns::service
4          repeat:
5              repeat-list: $parameters.app-services
6              repeat-item: srv
7              repeat-index: idx
8          properties:
9              ip: $parameters.app-ip
10             port: $parameters.base-port + $idx
11             servicegroupname: $parent.properties.name
12 <!--NeedCopy-->
```

## Construction repeat-condition

February 1, 2024

La construction à conditions répétées est évaluée à chaque itération d'une construction répétée et le résultat détermine s'il faut créer l'objet de configuration au cours de cette itération ou passer à l'itération suivante. L'exemple suivant montre l'utilisation de la construction **repeat-condition** :

### Exemple :

```
1 components
2     -
3         name: der-key-files-comp
4         type: ns::systemfile
5         repeat:
6             repeat-list: $parameters.certificates
7             repeat-item: certificate
8             repeat-condition: $certificate.ssl-inform == DER
9             properties:
10                filecontent: base64($certificate.keyfile.contents)
11                fileencoding: BASE64
12                filelocation: /nsconfig/ssl
13                filename: $certificate.keyfile.file
14 <!--NeedCopy-->
```

Dans cet exemple, le composant **der-key-files-comp** effectue une itération sur tous les certificats fournis par l'utilisateur, mais il crée uniquement des objets de configuration qui correspondent à des certificats avec un codage DER. Dans chaque itération, l'expression de condition de répétition est évaluée pour tester si l'encodage de certificat est de type DER. S'il n'est pas de type DER, aucun objet de configuration n'est créé dans l'itération en cours et l'itération passe au certificat suivant de la liste.



## Répétitions imbriquées

February 1, 2024

Avec la construction répétitive imbriquée, vous pouvez avoir plusieurs constructions répétées dans chaque composant en fonction de la définition du composant. Envisagez une répétition imbriquée de deux niveaux. Pour chaque élément de la liste extérieure (première liste de répétitions), vous pouvez créer une liste de répétition pour tous les éléments de la liste intérieure (deuxième liste de répétitions). Le compilateur StyleBook prend en charge jusqu'à trois répétitions imbriquées. Chaque niveau de répétition est associé à des attributs `repeat-item` et `repeat-index`. Les attributs `repeat-item` et `repeat-index` sont tous deux facultatifs. En outre, chaque répétition peut également spécifier une condition de répétition.

### Exemple :

```
1 parameters:
2   -
3     name: vips
4     type: ipaddress[]
5   -
6     name: vip-ports
7     type: tcp-port[]
8 components:
9   -
10    name: lbvservers-comp
11    type: ns::lbserver
12    repeat:
13      repeat-list: $parameters.vips
14      repeat-item: ip
15      repeat:
16        repeat-list: $parameters.vip-ports
17        repeat-item: port
18    properties:
19      name: str("lb-") + str($ip) + '-' + str($port)
20      servicetype: HTTP
21      ipv46: $ip
22      port: $port
23 <!--NeedCopy-->
```

Dans l'exemple ci-dessus, pour chaque élément de `$parameters.vips`, nous procédons à une itération sur tous les éléments de `$parameters.vip-ports`. Ainsi, pour chaque adresse IP spécifiée dans `$parameters.vips`, nous créons des objets de configuration `lbserver` pour tous les ports spécifiés dans `$parameters.vip-ports`. La section des propriétés définit le nom de l'objet avec « lb » comme préfixe pour la combinaison de l'adresse IP et du port. Par conséquent, pour chaque itération, `$ip + $port` définit une combinaison unique d'adresse IP et de numéro de port.

Si l'attribut `repeat-item` n'est pas fourni, le compilateur génère une valeur par défaut pour celui-ci.

Les valeurs par défaut pour `repeat-item` sont : `$repeat-item`, `$repeat-item-1`, `$repeat-item-2` respectivement pour chaque niveau de répétition. De même, si l'attribut `repeat-index` n'est pas fourni, le compilateur génère une valeur par défaut pour celui-ci. Les valeurs par défaut pour `repeat-index` sont : `$repeat-index`, `$repeat-index-1` et `$repeat-index-2` respectivement pour chaque niveau de répétition.

L'exemple suivant décrit la convention de dénomination en l'absence d'attributs `repeat-item` et `repeat-index` dans un objet de répétition imbriqué.

**Exemple :**

```
1 components:
2 -
3   name: lbvservers-comp
4   type: ns::lbserver
5   repeat:
6     repeat-list: $parameters.vips
7     repeat:
8       repeat-list: $parameters.vip-ports
9   properties:
10    name: str("lb-") + str($repeat-item) + '-' + str($repeat-item
11    -1)
11    servicetype: HTTP
12    ipv46: $repeat-item
13    port: $repeat-item-1
14 <!--NeedCopy-->
```

## Sorties

February 1, 2024

Dans la section des sorties, vous spécifiez ce qu'un StyleBook expose à ses utilisateurs une fois qu'il a créé avec succès tous les objets de configuration. La section des sorties d'un StyleBook est facultative. Un StyleBook n'a pas besoin de renvoyer des sorties. Cependant, en renvoyant certains composants internes sous forme de sortie, cela donne à tous les StyleBooks qui les importent plus de flexibilité, comme vous pouvez le voir lors de la création d'un StyleBook composite.

Le tableau suivant décrit les attributs utilisés dans la section des sorties.

Attribut	Description	Mandatory
nom	Le nom de la sortie correspondant à l'objet de configuration que vous souhaitez exposer.	Oui
description	Chaîne de texte décrivant la sortie.	Non
valeur	Cet attribut indique comment extraire la valeur renvoyée par un StyleBook.	Oui

**Exemple :**

```

1 outputs:
2   -
3     name: lbvserver
4     description: LBVServer component
5     value: $components.my-lbvserver-comp
6   -
7     name: svc-grp
8     description: ServiceGroup name
9     value: $components.my-svcg.properties.name
10 <!--NeedCopy-->

```

Dans cet exemple, vous exposez le composant **lbvserver** et le **nom** du groupe de services qui seraient créés par le StyleBook. La valeur de la sortie appelée **lbvserver** est le composant **my-lbvserver-comp**. **De même, la valeur de la sortie appelée svc-grp est le nom du groupe de services créé par le composant my-svcg.**

**Référence des paramètres**

February 1, 2024

Dans la construction des composants, vous vous référez aux paramètres définis dans la section des paramètres à l'aide de la notation `$parameters.<parametername>`. Si `<parametername>` contient lui-même des paramètres (lorsque le type est objet), vous devez utiliser la notation `$parameters.<parametername>.<sub-parametername>`, etc.

**Exemple :**

```

1 parameters:
2   -

```

```
3     name: name
4     label: Name
5     type: string
6     required: true
7     -
8     name: vip
9     label: Virtual IP and Port
10    type: object
11    required: true
12    parameters:
13      -
14        name: ip
15        label: Virtual IP
16        description: The Virtual IP Address
17        type: ipaddress
18        required: true
19        -
20          name: port
21          label: The Virtual Port
22          description: The TCP port for the Virtual IP
23          type: tcp-port
24          default: 80
25  components:
26    -
27      name: my-lbvserver-comp
28      type: ns::lbvserver
29      properties:
30        name: $parameters.name
31        servicetype: HTTP
32        ipv46: $parameters.vip.ip
33        port: $parameters.vip.port
34  <!--NeedCopy-->
```

## Référence parent

February 1, 2024

Si vous utilisez des [composants imbriqués](#), vous pouvez faire référence au composant parent en utilisant la notation `$parent`. Si le composant parent construit plusieurs objets de configuration à l'aide de la construction de répétition, et dans chaque itération, les composants enfants créent d'autres objets de configuration, la notation `$parent` fait toujours référence à l'itération actuelle du composant parent. Par exemple, `$parent.properties.name` fait référence à la propriété `name` de l'objet de configuration créé dans l'itération en cours par le parent.

### Exemple :

```
1  components:
2  -
```

```

3   name: my-lbvserver-comp
4   type: ns::lbvserver
5   properties:
6     name: $parameters.name + "-lb"
7     servicetype: HTTP
8     ipv46: $parameters.ip
9     port: 80
10    lbmethod: $parameters.lb-alg
11    components:
12      -
13        name: my-svcg-comp
14        type: ns::servicegroup
15        properties:
16          name: $parameters.name + "-svcgrp"
17          servicetype: HTTP
18          components:
19            -
20              name: lbvserver-svg-binding-comp
21              type: ns::lbvserver_servicegroup_binding
22              properties:
23                name: $parent.parent.properties.name
24                servicegroupname: $parent.properties.name
25              -
26                name: members-svcg-comp
27                type: ns::servicegroup_servicegroupmember_binding
28                repeat: $parameters.svc-servers
29                repeat-item: srv
30                properties:
31                  ip: $srv
32                  port: str($parameters.svc-port)
33                  servicegroupname: $parent.properties.name
34  <!--NeedCopy-->

```

Vous pouvez également naviguer vers le haut dans la hiérarchie des composants en accédant aux propriétés des parents jusqu'aux composants de niveau supérieur. Par exemple, le nom de la propriété du composant **lbvserver-svg-binding-comp** tire sa valeur du nom de propriété du parent de son composant parent, le composant **my-lbvserver-comp**, à l'aide de la notation **\$parent.parent**.

## Référence des composants

February 1, 2024

Dans la construction des composants, vous faites référence au composant de niveau supérieur dans le StyleBook en utilisant la notation **\$components.<componentname>**. S'il y a des composants imbriqués dans un composant de niveau supérieur, la notation utilisée est **\$components.<componentname>.componentname** pour y faire référence, et ainsi de suite.

**Exemple :**

```

1 components:
2   -
3     name: my-lbvserver-comp
4     type: ns::lbvserver
5     properties:
6       name: $parameters.name + "-lb"
7       servicetype: HTTP
8       ipv46: $parameters.ip
9       port: 80
10      lbmethod: $parameters.lb-alg
11   -
12     name: my-svcg-comp
13     type: ns::servicegroup
14     properties:
15       name: $parameters.name + "-svcgrp"
16       servicetype: HTTP
17   -
18     name: members-svcg-comp
19     type: ns::servicegroup_servicegroupmember_binding
20     repeat: $parameters.svc-servers
21     repeat-item: srv
22     properties:
23       ip: $srv
24       port: str($parameters.svc-port)
25       servicegroupname: $components.my-svcg-comp.properties.name
26   -
27     name: lbvserver-svg-binding-comp
28     type: ns::lbvserver_servicegroup_binding
29     properties:
30       name: $components.my-lbvserver-comp.properties.name
31       servicegroupname: $components.my-svcg-comp.properties.name
32 <!--NeedCopy-->

```

Dans cet exemple, les composants **my-svcg-comp** et **my-lbvserver-comp** doivent être construits avant de construire le dernier composant **lbvserver-svg-binding-comp** car il y a des références à ces composants dans ce dernier composant. Ces références sont fournies en utilisant les références de composants désignées par **\$components.<componentname>**.

## Référence des substitutions

February 1, 2024

Dans la section composants ou la section opérations, vous faites référence aux substitutions définies dans la section substitutions à l'aide de la notation **\$substitutions.<substitution-name>**. Par exemple, **\$substitutions.http-port**.

Si une substitution est une carte, vous pouvez faire référence à un élément de la carte sous

la forme `$substitutions.<substitutions-name>[<map-key>]`. Par exemple, `$substitutions.protocol-map[$parameters.port]`.

## Référence de variable

February 1, 2024

Lorsque vous utilisez les constructions `repeat-item` et `repeat-item` dans des composants pour créer plusieurs objets de configuration, vous pouvez attribuer un nom de variable à la construction `repeat-item`. Cette variable peut ensuite être référencée dans les propriétés de ce composant ou dans les composants enfants à l'aide de la notation `$\<varname\>`. Notez que lorsque la construction `repeat` est utilisée sans la construction `repeat-item` dans un composant, une variable par défaut appelée `$repeat-item` peut être utilisée pour accéder aux éléments d'itération.

### Exemple :

```
1 components:
2   -
3     name: server-members-comp
4     type: ns::server
5     condition: $parameters.svc-server-domain-names
6     repeat: $parameters.svc-server-domain-names
7     repeat-item: server-name
8     properties:
9       name: $server-name + "-server"
10      domain: $server-name
11     components:
12       -
13         name: service-members-comp
14         type: ns::service
15         properties:
16           name: $server-name + "-service"
17           servername: $parent.properties.name
18           servicetype: $parameters.svc-service-type
19           port: $parameters.svc-server-port
20 <!--NeedCopy-->
```

Dans l'exemple ci-dessus, un nom de variable, `nom_serveur`, est affecté à la construction d'élément répétitif. Ce nom de variable est mentionné dans les propriétés du même composant ainsi que dans les composants enfants `$\<varname\>`.

## Opérations

February 1, 2024

Operations est une section facultative dans un StyleBook. Dans cette section, vous pouvez configurer les analyses Citrix Application Delivery Management (ADM) pour collecter des enregistrements AppFlow sur toutes ou certaines des transactions de trafic. Le serveur virtuel créé sur une instance Citrix ADC à l'aide du StyleBook gère ces transactions de trafic. Dans cette section, vous pouvez également configurer Citrix ADM pour déclencher des alarmes lorsque certaines conditions de trafic sont remplies sur un serveur virtuel.

Vous pouvez configurer Citrix ADM via StyleBooks pour collecter des statistiques de trafic à partir de divers Citrix ADM Insights répertoriés comme suit :

- Web Insight
- Security Insight
- HDX Insight
- Citrix Gateway Insight.

Les serveurs virtuels pris en charge sont l'équilibrage de charge, la commutation de contenu et les serveurs virtuels VPN.

Activez Web Insight et Security Insight ou l'un d'entre eux pour l'analyse sur un serveur virtuel d'équilibrage de charge ou de commutation de contenu. Toutefois, pour les serveurs virtuels VPN, vous devez activer HDX Insight et Citrix Gateway Insight ou l'un d'entre eux.

Tout Citrix ADM Insight activé sur les instances Citrix ADC via StyleBooks utilise le protocole IPFIX (AppFlow) pour envoyer les données des instances à Citrix ADC.

En outre, lorsque vous activez Web Insight, les « Mesures côté client » sont activées sur l'équilibrage de charge et les serveurs virtuels de commutation de contenu.

### Exemple 1 :

L'exemple suivant montre comment écrire la section des opérations dans un StyleBook pour activer HDX Insight et Citrix Gateway Insight sur un serveur virtuel VPN :

```
1 name: simple-vpn-ops
2 namespace: com.example.stylebooks
3 schema-version: "1.0"
4 version: "0.1"
5 description: Test StyleBook to enable hdxinsight and gatewayinsight on
  a VPN vserver
6 import-stylebooks:
7   -
8     namespace: netscaler.nitro.config
9     version: "10.5"
```



```

10     prefix: ns
11     components:
12         -
13             name: vpnserver-comp
14             type: ns::vpnserver
15             properties:
16                 name: str("vpn-") + str($current-target.ip)
17                 servicetype: SSL
18                 ipv46: 1.1.21.37
19                 port: 443
20     operations:
21         analytics:
22             -
23                 name: comp-ops
24                 properties:
25                     target: $components.vpnserver-comp
26                     filter: "true"
27                     insights:
28                         -
29                             type: hdxinsight**
30                         -
31                             type: gatewayinsight
32     outputs:
33         -
34             name: myvpns
35             value: $components.vpnserver-comp
36     <!--NeedCopy-->

```

**Exemple 2 :**

L'exemple suivant montre comment écrire la section Opérations dans un StyleBook pour activer Web Insight et Security Insight sur un serveur virtuel d'équilibrage de charge :

```

1 name: simple-lb-ops
2 namespace: com.example.stylebooks
3 schema-version: "1.0"
4 version: "0.1"
5 description: Test StyleBook to enable webinsight and securityinsight on
6             LB vserver
7 import-stylebooks:
8     -
9         namespace: netscaler.nitro.config
10        version: "10.5"
11        prefix: ns
12    components:
13        -
14            name: lbvserver-comp
15            type: ns::lbvserver
16            properties:
17                name: str("lb-") + str($current-target.ip)
18                servicetype: HTTP
19                ipv46: 1.1.21.37
20                port: 80

```

```

20 operations:
21   analytics:
22     -
23       name: comp-ops
24       properties:
25         target: $components.lbvserver-comp
26         filter: "true"
27         insights:
28           -
29             type: webinsight
30           -
31             type: securityinsight
32 outputs:
33   -
34     name: mylbs
35     value: $components.lbvserver-comp
36 <!--NeedCopy-->

```

## Analytics

February 1, 2024

La sous-section Analytics de la section Opérations a une structure similaire à celle de la section Composants. Chaque élément de la section d'analyse est utilisé pour configurer la fonctionnalité Citrix ADM Analytics pour un ou plusieurs serveurs virtuels créés par le StyleBook.

Un élément de la section Analytics possède les attributs suivants :

Attribut	Description	Mandatory
nom	Nom de l'élément d'analyse.	Oui
description	Chaîne de texte décrivant ce qu'est cet élément.	Non
condition	Expression booléenne. Lorsque cette condition est évaluée à faux, l'ensemble de l'élément d'analyse est ignoré.	Non
répétition	Répète sur une liste.	Non
condition de répétition	Expression booléenne. Si l'expression donne la valeur false, l'itération en cours est ignorée.	Non

Attribut	Description	Mandatory
article répété	Nom de l'élément dans l'itération en cours.	Non
indice de répétition	Nom de la valeur d'index de l'itération en cours.	Non
propriétés	La liste des propriétés des analyses.	Oui
target	L'une des propriétés de la liste. L'expression cible est le nom d'un serveur virtuel, configuré sur Citrix ADC, pour lequel les analyses seront collectées.	Oui
filtre	L'une des propriétés de la liste. La valeur de cet attribut est une expression de stratégie avancée Citrix ADC qui est utilisée pour filtrer les requêtes sur le serveur virtuel pour lesquelles les analyses seront collectées. Par défaut, les données d'analyse sont collectées sur tout le trafic passant par le serveur virtuel.	Non

**Exemple :**

```

1  operations:
2
3    analytics:
4
5      -
6
7      name: lbvserver-ops-comp
8
9      properties:
10
11     target: $components-basic-lb-comp.outputs.lbvserver-name
12
13     filter: HTTP.REQ.URL.CONTAINS("catalog")
14 <!--NeedCopy-->

```

Chaque attribut de la section Analytics est utilisé pour indiquer à la fonctionnalité Citrix ADM Analytics de configurer les instances Citrix ADC pour collecter les enregistrements Appflow sur le serveur virtuel

identifié par la propriété cible.

## Alarmes

February 1, 2024

La sous-section alarmes de la section des opérations présente une structure similaire et les mêmes attributs que dans la sous-section d'analyse. La seule différence est dans l'attribut properties. Pour obtenir la liste de tous les attributs (autres que l'attribut de propriétés), consultez [Analytics](#).

Les propriétés suivantes sont disponibles dans une sous-section alarmes :

---

Attribut	Description	Mandatory
target	Expression qui évalue le nom d'un serveur virtuel, configuré sur Citrix ADC, pour lequel les alarmes sont configurées.	Oui
profil de courrier électronique	Nom d'un profil de messagerie défini dans la fonctionnalité Citrix ADM Analytics et contenant une liste d'adresses e-mail que vous souhaitez notifier lorsque l'alarme est déclenchée.	Non (un profil e-mail ou un profil sms doit être défini)
profil sms-	Nom d'un profil SMS défini dans la fonctionnalité Citrix ADM Analytics et contenant une liste de numéros de téléphone que vous souhaitez notifier lorsque l'alarme est déclenchée.	Non (un profil e-mail ou un profil sms doit être défini)
rules	Liste de règles définissant les conditions qui déclenchaient une alarme pour le serveur virtuel défini par la propriété cible.	Oui

Attribut	Description	Mandatory
métrique	Un attribut de règle. Le nom d'une métrique que vous souhaitez suivre concernant le serveur virtuel Citrix ADC.	Oui
opérateur	Un attribut de règle. Opérateur à utiliser pour comparer la mesure à la valeur. Les opérateurs valides sont « supérieur à » et « inférieur à ».	Oui
valeur	Un attribut de règle. La valeur seuil à laquelle la métrique est comparée à l'aide de l'opérateur. Si la valeur de la métrique dépasse ce seuil, les alarmes associées sont déclenchées.	Oui
unité de période	Attribut d'une règle. Fréquence à laquelle alerter les utilisateurs si la règle d'alarme est respectée. Cela peut contenir la valeur du jour, de l'heure ou de la semaine. Cela signifie que si la règle est respectée, une alarme sera envoyée une fois par unité de période (par exemple, une fois par jour).	Oui

Le tableau suivant fournit une liste des mesures qui sont suivies concernant le serveur virtuel Citrix ADC.

Compteurs|Description|Description détaillée|Calcul de Citrix ADM

|—||—||—||—|

|Pour un serveur virtuel VPN :|

total\_requests|Nombre total de lancements de sessions VPN|Nombre total de sessions actives sur ce serveur virtuel VPN démarrées pendant un intervalle de temps spécifié par l'utilisateur.|Compteur croissant de façon monotone, incrémenté à chaque lancement de nouvelle session|

|app\_count|Nombre de lancements d'applications VPN|Nombre total d'applications VPN uniques sur

ce serveur virtuel VPN lancées pendant un intervalle de temps spécifié par l'utilisateur. |Augmenter le compteur de façon monotone à chaque lancement d'une nouvelle application|  
app\_launch\_duration	Durée de lancement de l'application VPN	Durée moyenne de lancement d'une application (en millisecondes)	Valeur moyenne calculée sur les durées de lancement de toutes les applications VPN lancées sur ce serveur virtuel VPN
Autres serveurs virtuels (CS, LB, Auth, GSLB)			
Total\_Requests	Nombre de requêtes	Nombre de requêtes client sur ce serveur virtuel depuis le dernier redémarrage de l'appliance ou depuis la création du serveur virtuel, selon la date la plus récente.	Compteur monotone croissant, incrémenté à chaque nouvelle requête vers ce serveur virtuel.
total\_bytes	bytes	Nombre total d'octets transférés du serveur virtuel vers Citrix ADM sur l'intervalle de temps spécifié.	Compteur monotone croissant pour tenir compte du nombre total d'octets servis par ce serveur virtuel.
Application\_Response\_time	Temps de réponse	Temps de réponse moyen du serveur virtuel.	Valeur moyenne des temps de réponse de toutes les demandes reçues par ce serveur virtuel depuis le dernier redémarrage de l'appliance (ou depuis la création du serveur virtuel), selon la dernière éventualité.

Exemple d'une section d'alarmes dans un StyleBook :

```

1 operations:
2   alarms:
3     -
4       name:lbvserver_alarm
5       properties:
6         target: $outputs.lbvserver
7         email-profile: $parameters.emailprofile
8         sms-profile: "NetScalerSMS"
9         rules:
10          -
11            metric: "total_requests"
12            operator: "greaterthan"
13            value: 25
14            period-unit: weekly
15          -
16            metric: "total_bytes"
17            operator: "lessthan"
18            value: 1024
19            period-unit: day
20
21 <!--NeedCopy-->

```

## Expressions

February 1, 2024

L'une des fonctionnalités les plus puissantes de StyleBook est l'utilisation d'expressions. Vous pouvez utiliser des expressions StyleBooks dans différents scénarios pour calculer des valeurs dynamiques. L'exemple ci-dessous montre une expression pour concaténer une valeur de paramètre avec une chaîne littérale.

### Exemple :

```
$parameters.appname + « -mon »
```

Cette expression récupère le paramètre nommé appname et le concatène avec la chaîne « -mon ».

Les types d'expressions suivants sont pris en charge :

### Expressions arithmétiques

- Ajout (+)
- Substraction (-)
- Multiplication (\*)
- Division (/)
- Module (%)

### Exemples :

- Ajouter deux nombres : `$parameters.a + $parameters.b`
- Multiplier deux nombres : `$parameters.a * 10`
- Trouver le reste après la division d'un nombre par un autre :

```
15% 10 Résultats dans 5
```

### Expressions de chaînes

- Concaténer deux chaînes (+)

### Exemple :

```
Concaténer deux chaînes : str (« app- ») + $parameters.appname
```

## Liste des expressions

Fusionne deux listes (+)

### Exemple :

- Concaténer deux listes : `$parameters.external-servers + $parameters.internal-servers`
- Si `$parameters.ports-1` est `[80, 81]` et `$parameters.ports-2` est `[81, 82]`, alors `$parameters.ports-1 + $parameters.ports-2` apparaissent sous forme de liste `[80, 81, 81, 82]`

## Expressions relationnelles

- `==` : Teste si deux opérandes sont égaux et renvoie true s'ils sont égaux, sinon renvoie false.
- `!=` : Teste si deux opérandes sont différents et renvoie true s'ils sont différents, sinon renvoie false.
  - `>` : Renvoie true si le premier opérande est supérieur au second opérande, else renvoie false.
  - `>=` : Renvoie true si le premier opérande est supérieur ou égal au second opérande, else renvoie false.
- `<` : Renvoie true si le premier opérande est inférieur au second opérande, else renvoie false.
- `<=` : Renvoie true si le premier opérande est inférieur ou égal au second opérande, else renvoie false.

### Exemple :

- Utilisation de l'opérateur Egalité : `$parameters.name == « abcd »`
- Utilisation de l'opérateur d'inégalité : `$parameters.name != « par défaut »`
- Exemples pour d'autres opérateurs relationnels
  - `10 > 9`
  - `10 >= 10`
  - `0 < 9`
  - `10 <= 9`
  - `10 == 10`
  - `10 != 1`

## Expressions logiques (booléennes)

- `et` : L'opérateur logique 'et'. Si les deux opérandes sont vrais, le résultat est vrai, sinon il est faux.



- ou : L'opérateur logique 'ou'. Si l'un des opérandes est vrai, le résultat est vrai, sinon il est faux.
- not : L'opérateur unaire. Si l'opérande est vrai, le résultat est faux, et vice-versa.
- in : Teste si le premier argument est une sous-chaîne du second argument
- in : Teste si un élément fait partie d'une liste

#### Remarque

Vous pouvez taper des expressions cast où les chaînes peuvent être converties en nombres et les nombres peuvent être convertis en chaînes. De même, un port tcp-peut être converti en un nombre, et une adresse IP peut être converti en une chaîne.

Vous devez utiliser un délimiteur avant et après tout opérateur. Vous pouvez utiliser les délimiteurs suivants :

- Avant un opérateur : espace, tabulation, virgule, (,), [,]
- Après un opérateur : espace, onglet, (, [,
- Par exemple :
- abc + def
- 100 % 10
- 10 > 9

### Validation du type d'expression

Le moteur StyleBook permet désormais une vérification de type plus forte pendant la compilation, c'est-à-dire que les expressions utilisées lors de l'écriture du StyleBook sont validées lors de l'importation de StyleBook lui-même plutôt que lors de la création du pack de configuration.

Toutes les références aux paramètres, substitutions, composants, propriétés des composants, sorties des composants, variables définies par l'utilisateur (élément répété, index répété, arguments des fonctions de substitution, etc.) sont toutes validées pour leur existence et leurs types.

#### Exemple de contrôles de type :

Dans l'exemple suivant, le type attendu de propriété de port de lbvserver StyleBook est tcp-port. Dans les versions antérieures de Citrix Application Delivery Management (ADM), le compilateur StyleBook a calculé la valeur sous forme de chaîne et StyleBook a été importé et exécuté. Maintenant, les validations de type se produisent au moment de la compilation (import-time). Le compilateur trouve que string et tcp-port ne sont pas des types compatibles et, par conséquent, le compilateur StyleBook génère une erreur et échoue l'importation ou la migration du StyleBook.

```

1 components:
2   -
3     name: lbvserver-comp
4     type: ns::lbvserver
5     properties:
6       name: mylb
7       ipv46: 10.102.190.15
8       port: str("80")
9       servicetype: HTTP
10
11 You should now declare this as a number for the compiler to
12     successfully compile this StyleBook.
13
14     port: 80
15 <!--NeedCopy-->

```

### Exemple de marquage d'expressions non valides :

Dans les versions antérieures, lorsqu'une expression non valide était affectée à un nom de propriété, le compilateur ne détectait pas d'expressions non valides et autorisait l'importation des StyleBooks dans Citrix ADM. Maintenant, si ce StyleBook est importé dans Citrix ADM, le compilateur identifiera ces expressions non valides et le signalera. Par conséquent, le StyleBook ne sera pas importé dans Citrix ADM.

Dans cet exemple, l'expression affectée à la propriété name dans le composant lb-sg-binding-comp est : \$components.lbvserver-comp.properties.lbservername. Cependant, il n'y a pas de propriété appelée lbservername dans le composant lbvserver-comp. Dans les versions précédentes de Citrix ADM, le compilateur aurait autorisé cette expression et l'aurait importée avec succès. L'échec réel se produirait lorsqu'un utilisateur souhaite créer un pack de configuration à l'aide de ce StyleBook. Toutefois, ce type d'erreur est identifié lors de l'importation et le StyleBook n'est pas importé dans Citrix ADM. Vous devez corriger manuellement ces erreurs et importer les StyleBooks.

```

1 components:
2   -
3     name: lbvserver-comp
4     type: ns::lbvserver
5     properties:
6       name: mylb
7       ipv46: 10.102.190.15
8       port: 80
9       servicetype: HTTP
10   -
11     name: sg-comp
12     type: ns::servicegroup
13     properties:
14       servicegroupname: msg
15       servicetype: HTTP
16   -
17     name: lb-sg-binding-comp
18     type: ns::lbvserver_servicegroup_binding

```

```

19     condition: $parameters.create-binding
20     properties:
21         name: $components.lbvserver-comp.properties.lbvservername
22         servicegroupname: $components.sg-comp.properties.servicegroupname
23 <!--NeedCopy-->

```

## Listes d'indexation

Les éléments d'une liste sont maintenant accessibles en les indexant directement :

```

|||
|-----|-----|
-|
| Expression | Description |
| $components.test-lbs[0] | Fait référence au premier élément du composant test-lbs |
| $components.test-lbs[0].properties.p1 | Fait référence à la propriété p1 du premier élément du composant test-lbs |
| $components.lbcomps[0].outputs.servicegroups[1].properties.servicegroupname | Fait référence à la propriété servicegroupname du deuxième élément du composant servicegroups, qui est une sortie du premier élément du composant lbcomps |
|

```

## Interpolations sur place

February 2, 2024

Il est désormais possible de remplacer une ou plusieurs parties d'une chaîne à l'aide d'une ou plusieurs expressions StyleBook. Lorsque ces expressions de chaîne sont évaluées par le compilateur StyleBook, la partie de la chaîne qui utilise une expression StyleBook est remplacée par la valeur de l'expression. Pour inclure des expressions StyleBook dans une chaîne, nous utilisons la notation suivante :

```
"...%{...}%..."
```

où les caractères entre "%{ "and "}" forment une expression StyleBook. Ces expressions sont appelées « interpolations sur place. »

Par exemple, la chaîne « lb-%{\$parameters.appname}%-svc » est une expression de chaîne avec interpolation sur place d'une expression StyleBook. La valeur de l'expression de chaîne dépend de la valeur de l'expression d'interpolation. Considérez que **\$parameters.appname** est affecté avec "app1." L'expression de chaîne est ensuite évaluée à **lb-app1-svc**. Cela permet aux valeurs de ne

pas être codées en dur dans des expressions de chaîne, mais d’être évaluées en fonction des valeurs définies par l’utilisateur.

Un cas d’utilisation pratique des interpolations sur place consiste à paramétrer les expressions de stratégie dans StyleBooks. Imaginons un scénario dans lequel vous souhaitez écrire une expression de stratégie qui vérifie si l’URL HTTP contient un mot spécifique, par exemple « jpeg ».

Pour cela, vous écrivez une expression de stratégie comme suit : “HTTP.REQ.URL.CONTAINS(\“jpeg\” )”.

Maintenant, si vous souhaitez paramétrer l’objet dans l’URL HTTP, vous pouvez ajouter un paramètre de chaîne dans le StyleBook, par exemple \$parameters.url-object. L’expression de stratégie doit être écrite en fonction de ce paramètre. Pour ce faire, vous utilisez la concaténation de chaînes pour obtenir le résultat. L’expression ressemblerait à :

```
str("HTTP.REQ.URL.CONTAINS(\")+ $parameters.url-object + "\")"
```

Si \$parameter.url-object est assigné « csv », l’expression ci-dessus correspond à “HTTP.REQ.URL.CONTAINS(\“csv\” )”. Cependant, cette expression n’est pas facile à lire. Pour faciliter la lecture et la compréhension de ce paramétrage, vous pouvez utiliser des interpolations sur place.

L’expression avec interpolation sur place est maintenant :

```
str("HTTP.REQ.URL.CONTAINS(%{quotewrap($parameters.url-object)}%)")
```

Dans l’expression ci-dessus, vous avez utilisé une expression d’interpolation qui ajoute les guillemets internes autour de la valeur du \$parameters.url-object. Le résultat de cette expression est identique à celui ci-dessus, mais il semble plus intuitif et plus proche du résultat réel.

## Types autorisés à l’intérieur des interpolations

Vous pouvez utiliser des expressions qui génèrent des valeurs des types suivants dans les interpolations : booléen, nombre, port TCP, adresse IP et chaîne. La valeur générée est automatiquement transformée en chaîne lorsque les interpolations sont remplacées par le résultat.

Les expressions de chaîne peuvent comporter 0, 1 ou plusieurs interpolations. Dans une interpolation séquentielle, différentes parties de l’expression de chaîne peuvent être remplacées par différentes expressions StyleBook. Par exemple, la chaîne lb-%{\$parameters.appname}%-%{\$parameters.vip}% renvoie “lb-app1-1.1.1.1”, si \$parameters.appname est “app1” et \$parameters.vip est “1.1.1.1”

Les expressions de chaîne prennent également en charge les interpolations imbriquées. Autrement dit, une expression d’interpolation peut être imbriquée dans une autre expression d’interpolation afin que la valeur d’une expression puisse devenir une entrée dans la seconde expression.

Par exemple, considérez une chaîne “%{lb-%{\$parameters.port + 1}%}%”

La chaîne interne, “**%{\$parameters.port + 1}%”**returns “**lb-81**”si **\$parameters.port**est égal à 80. Ici, cette expression est imbriquée dans une autre expression d’interpolation.

Le tableau suivant décrit les différents types d’interpolations avec des exemples et des résultats correspondants. Les valeurs des paramètres utilisés dans les exemples sont les suivantes :

- \$parameters.appname: “lb1”
- \$parameters.vip: “1.1.1.1”
- \$parameters.n1: 1
- \$parameters.n2: 3

### Interpolations simples

Expression	Résultat
lb-%{\$parameters.appname}%-def	lb-lb1-def

### Conversions automatiques de type

Expression	Résultat
lb-%{1}%	lb-1
lb-%{\$parameters.vip}%	lb-1.1.1.1
lb-%{true}%	lb-True

### Interpolations séquentielles

Expression	Résultat
%{\$parameters.appname}%- %{str(\$parameters.appname)}%	lb1-lb1
lb-%{1}%-%{2}%	lb-1-2

## Interpolations imbriquées

Expression	Résultat
<code>%{abc-%{\$parameters.n1 + 1}}%</code>	abc-2
<code>str(“%{abc-%{\$parameters.n1}}%”- %{\$parameters.n2}%)</code>	bc-1-3

## Interpolations avec quotewrap

Expression	Résultat
<code>str(“%{quotewrap(abcd)}%”)</code>	“abcd
<code>str(“%{quotewrap(https://)} %”+HTTP. REQ.HOSTNAME+HTTP.REQ.URL”)</code>	“«code class=“language-plaintext highlighter-rouge”>https://“+HTTP.REQ.HOST NAME+HTTP.REQ.URL</code>

## Caractères d’échappement dans les interpolations

Si les caractères “%{“or “}%”font partie de la chaîne, vous devez fournir “\”comme caractère d’échappement afin que le compilateur StyleBook ne les évalue pas comme des balises d’interpolation.

### Exemple :

`str(“%{\%{ + str($parameters.vip) + }\%}%)”` returns “%{1.1.1.1}%”if \$parameters.vip is 1.1.1.1

Le tableau suivant décrit quelques expressions supplémentaires et leurs résultats :

Catégorie	Expression	Résultat
Escaping interpolations	<code>str(“%{str(\$parameters.n1) + }\%}%)”)</code>	1}%
	<code>lb-%{str(\$parameters.n1) + }\%}%)</code>	lb-1}%
	<code>”%{str(\$parameters.n1) + \ }\%\\”}%)”</code>	1}%

---

Catégorie	Expression	Résultat
-----------	------------	----------

---

## Fonctions intégrées

February 1, 2024

Les expressions dans StyleBooks peuvent utiliser des fonctions intégrées.

Par exemple, vous pouvez utiliser la fonction intégrée, `str ()` pour transformer un nombre en chaîne.

`str ($parameters.order)`

Ou, vous pouvez utiliser la fonction intégrée, `int ()` pour transformer une chaîne en un entier.

`int ($parameters.priority)`

Voici la liste des fonctions intégrées prises en charge dans les expressions StyleBook avec des exemples de leur utilisation :

### **str()**

La fonction `str ()` transforme l'argument input en une valeur de chaîne.

Types d'arguments autorisés :

- string
- nombre
- Port TCP
- booléen
- Adresse IP

### **Exemples :**

- `set-+ str(10)` returns `set-10`
- `str(10)` returns `10`
- `str(1.1.1.1)` returns `1.1.1.1`
- `str(T rue)` returns `T rue`
- `str(mas)` returns `mas`

## **int()**

La fonction `int()` prend une chaîne, un nombre ou un `tcpport` comme argument et renvoie un entier.

### **Exemples :**

- `int("10")` returns 10
- `int(10)` returns 10

## **bool()**

La fonction `bool()` prend n'importe quel type comme argument. Si la valeur de l'argument est `false`, vide ou inexistante, cette fonction renvoie `false`.

Sinon, il retourne `true`.

### **Exemples :**

- `bool(true)` returns "true"
- `bool(false)` returns "false"
- `bool($parameters.a)` returns `false` if the
- `$parameters.a` is `false`, empty, or not present.

## **len()**

La fonction `len()` prend une chaîne ou une liste comme argument, et renvoie le nombre de caractères dans une chaîne ou le nombre d'éléments dans une liste.

### **Exemple 1 :**

Si vous définissez une substitution comme suit :

```
items: ["123", "abc", "xyz"]
```

```
len($substitutions.items) returns 3
```

### **Exemple 2 :**

```
len("netscaler mas") returns 13
```

### **Exemple 3 :**

```
len($parameters.vips) returns 3 if $parameters.vip is  
assigned a value ['1.1.1.1', '1.1.1.2', '1.1.1.3']
```



## **min()**

La fonction min() prend une liste ou une série de nombres ou tcp-ports comme arguments, et renvoie le plus petit élément.

### **Exemples avec une série de numéros/ports tcp :**

- min (80, 100, 1000) renvoie 80
- min (-20, 100, 400) renvoie -20
- min (-80, -20, -10) renvoie -80
- min (0, 100, -400) renvoie -400

### **Exemples avec une liste de numéros/tcp-ports :**

- Le support \$parameters.ports est une liste de ports TCP et a la valeur : [80, 81, 8080].  
min(\$parameters.ports) returns 80.

## **max()**

La fonction max () prend une liste ou une série de nombres ou tcp-ports comme arguments, et renvoie l'élément le plus grand.

### **Exemples avec une série de numéros/ports tcp :**

- max (80, 100, 1000) renvoie 1000
- max (-20, 100, 400) renvoie 400
- max (-80, -20, -10) renvoie -10
- max (0, 100, -400) renvoie 100

### **Exemples avec une liste de numéros/tcp-ports :**

- Le support \$parameters.ports est une liste de ports TCP et a la valeur : [80, 81, 8080].  
max(\$parameters.ports) returns 8080.

## **bin()**

La fonction bin() prend un nombre comme argument, et renvoie une chaîne qui représente le nombre au format binaire.

### **Exemples d'expressions :**

bin(100) returns "0b1100100"

## **oct()**

La fonction `oct()` prend un nombre comme argument, et renvoie une chaîne qui représente le nombre au format octal.

### **Exemples d'expressions :**

`oct(100)` returns “0144”

## **hex()**

La fonction `hex()` prend un nombre comme argument, et renvoie une chaîne minuscule qui représente le nombre au format hexadécimal.

### **Exemples d'expressions :**

`hex(100)` returns “0x64”

## **lower()**

La fonction `lower()` prend une chaîne comme argument et renvoie la même chaîne en minuscules.

### **Exemple :**

`lower(“MAS”)` returns “mas”

## **upper()**

La fonction `upper()` prend une chaîne comme argument et renvoie la même chaîne en majuscules.

### **Exemple :**

`upper(“netscaler_mas”)` returns “NET SCALER\_MAS”

## **sum()**

La fonction `sum()` prend une liste de nombres ou `tcpports` comme arguments et renvoie la somme des nombres dans la liste.

### **Exemple 1 :**

Si vous définissez une substitution comme suit :  
substitutions :

- liste de numéros :

- 11
- 22
- 55

sum(\$substitutions.list-of-numbers) returns 88

**Exemple 2 :**

Si \$parameters.ports est [80, 81, 82], sum (\$parameters.ports) renvoie 243

**pow()**

La fonction pow() prend deux nombres comme arguments et renvoie un nombre qui représente le premier argument soulevé à la puissance du second.

**Exemple :**

pow(3,2) returns 9

**ip()**

La fonction ip prend une chaîne ou une adresse IP comme argument renvoie l'adresse IP en fonction de la valeur d'entrée.

**Exemples :**

- ip("2.1.1.1") returns "2.1.1.1"
- ip(3.1.1.1) returns "3.1.1.1"

**base64.encode()**

La fonction base64.encode() prend un argument de chaîne et renvoie la chaîne encodée base64.

**Exemple :**

base64.encode("abcd") returns "YWJjZA=="

**base64.decode()**

La fonction base64.decode prend la chaîne encodée base64 comme argument et renvoie la chaîne décodée.

**Exemple :**

base64.decode("YWJjZA==") returns "abcd"

## **exists()**

La fonction existe prend un argument de n'importe quel type et renvoie un booléen. La valeur de retour est True si l'entrée a une valeur quelconque. La valeur renvoyée est False Si l'argument input n'a pas de valeur (c'est-à-dire aucune valeur).

Considérez que \$parameters.monitor est un paramètre facultatif. Si vous fournissez une valeur à ce paramètre lors de la création d'un configpack, exists (\$parameters.monitor) renvoie True.

Sinon, il renvoie False.

## **filter()**

La fonction filter() prend deux arguments.

Argument 1 : fonction de substitution qui prend un argument et renvoie une valeur booléenne.

Argument 2 : une liste.

La fonction renvoie un sous-ensemble de la liste d'origine où chaque élément est évalué à « True » lorsqu'il est passé à la fonction de substitution dans le premier argument.

### **Exemple :**

Supposons que nous ayons défini une fonction de substitution comme suit.

substitutions :

```
1 x(a) : $a != 81
```

Cette fonction renvoie True si la valeur d'entrée n'est pas égale à 81. Sinon, il renvoie False.

Suppose,

\$parameters.ports est [81, 80, 81, 89]

filter (\$substitutions.x, \$parameters.ports) renvoie [80, 89] en supprimant toutes les occurrences de 81 de la liste.

## **if-then-else()**

La fonction if-then-else() prend trois arguments.

Argument 1 : Expression booléenne

Argument 2 : Toute expression

Argument 3 : Toute expression (facultatif)

Si l'expression de l'argument 1 est évaluée à True, la fonction renvoie la valeur de l'expression fournie comme argument 2.

Sinon, si l'argument 3 est fourni, la fonction renvoie la valeur de l'expression dans l'argument 3.

Si l'argument 3 n'est pas fourni, la fonction ne renvoie aucune valeur.

**Exemple 1 :**

`if-then-else($parameters.servicetype == HTTP, 80, 443)` returns "80" if `$parameters.servicetype` has value "HTTP." Sinon, la fonction renvoie "443".

**Exemple 2 :**

`if-then-else($parameters.servicetype == HTTP, $parameters.hport, $parameters.sport)` returns the value of "`$parameters.hport`" if `$parameters.servicetype` has value "HTTP."

Sinon, la fonction renvoie la valeur de « `$parameters.sport`. »

**Exemple 3 :**

`if-then-else($parameters.servicetype == HTTP, 80)` returns "80" if `$parameters.servicetype` has value "HTTP."

Sinon, la fonction ne renvoie aucune valeur.

## join()

La fonction `join()` prend deux arguments :

Argument 1 : liste de nombres, tcp-ports, chaînes ou adresses IP

Argument 2 : chaîne de délimiteur (facultatif)

La fonction joint les éléments de la liste fournie comme argument 1 dans une chaîne, où chaque élément est séparé par la chaîne de délimiteur fournie comme argument deux. Si l'argument deux n'est pas fourni, les éléments de la liste sont réunis en une seule chaîne.

**Exemple :**

- `$parameters.ports` est [81, 82, 83].
  - Avec l'argument de délimiteur :  
`join($parameters.ports, '-')` returns "81-82-83"
  - Sans argument de délimiteur :  
`join($parameters.ports)` returns "818283"

## **map()**

La fonction de map prend deux arguments ;

Argument 1 : N'importe quelle fonction

Argument 2 : Une liste d'éléments.

La fonction renvoie une liste où chaque élément de la liste est le résultat de l'application de la fonction mapfunction (argument un) à l'élément correspondant dans l'argument deux.

Fonctions autorisées dans l'argument 1 :

- Fonctions intégrées qui prennent un argument :  
base64.encode, base64.decode, bin, bool, exists, hex, int, ip, len, lower, upper, oct, quotewrap, str, trim, upper, url.encode, url.decode
- Fonctions de substitution qui prennent au moins un argument.

### **Exemple :**

Supposons que \$parameters.nums soit [81, 82, 83].

- Mapper à l'aide d'une fonction intégrée, str

```
map(str, $parameters.nums) returns ["81", "82", "83"]
```

Le résultat de la fonction map est la liste des chaînes où chaque élément est une chaîne est calculée en appliquant la fonction str sur l'élément correspondant dans la liste d'entrée (\$parameters.nums).

- Carte utilisant une fonction de substitution

- Substitutions :

```
add-10(port): $port + 10
```

- Expression :

```
map($substitutions.add-10,
```

```
$parameters.nums) renvoie une liste de nombres :
```

```
[91, 92, 93]
```

Le résultat de cette fonction de carte est une liste de nombres, chaque élément est calculé en appliquant la fonction de substitution \$substitutions.add-10 sur l'élément correspondant dans la liste d'entrée (\$parameters.nums).

## **quotewrap()**

La fonction quotewrap prend une chaîne comme argument et renvoie une chaîne après avoir ajouté des guillemets doubles avant et après la valeur d'entrée.

### **Exemple :**

quotewrap("mas") renvoie ""mas""

## **replace()**

La fonction replace prend trois arguments :

Argument 1 : chaîne

Argument 2 : chaîne

Argument 3 : chaîne (facultatif)

La fonction remplace toutes les occurrences de l'argument deux par l'argument trois dans l'argument un.

Si l'argument trois n'est pas fourni, toutes les occurrences de l'argument deux sont supprimées de l'argument un (en d'autres termes, remplacées par une chaîne vide).

Remplacez une sous-chaîne par une autre sous-chaîne :

- replace('abcdef', 'def', 'xyz') renvoie "abcxyz".
  - Toutes les occurrences de « def » sont remplacées par « xyz ».
- replace('abcdefabc', 'def') renvoie "abcabc".
  - Comme il n'y a pas de troisième argument, « def » est supprimé de la chaîne résultante.

## **trim()**

La fonction trim renvoie une chaîne où les espaces de début et de fin sont supprimés de la chaîne d'entrée.

### **Exemple :**

trim(' abc ') renvoie "abc"

### **truncate()**

La fonction truncate prend deux arguments :

Argument 1 : chaîne

Argument 2 : nombre

La fonction renvoie une chaîne dans laquelle la chaîne d'entrée de l'argument 1 est tronquée à la longueur spécifiée par l'argument 2.

#### **Exemple :**

`truncate('netscaler mas', 9)` renvoie "netscaler"

### **url.encode**

La fonction url.encode renvoie une chaîne où les caractères sont transformés en utilisant le jeu de caractères ASCII selon la RFC 3986.

#### **Exemple :**

`url.encode("a/b/c")` renvoie "a%2Fb%2Fc"

### **url.decode**

La fonction url.decode renvoie une chaîne où l'argument encodé URL est décodé dans une chaîne régulière selon la RFC 3986.

#### **Exemple :**

`url.decode("a%2Fb%2Fc")` renvoie "a/b/c"

### **is-ipv4()**

La fonction is-ipv4 () prend une adresse IP comme argument et renvoie « true » si l'adresse IP est au format IPv4.

`is-ipv4 (10.10.10.10)` renvoie « True »

### **is-ipv6()**

La fonction is-ipv6 () prend une adresse IP comme argument et renvoie « true » si l'adresse IP est au format IPv6.

`is-ipv6 (2001:DB8 : :)` renvoie « True »



## Détection des dépendances

February 1, 2024

Les composants d'un StyleBook peuvent faire référence aux propriétés ou aux sections d'autres composants du même StyleBook. Les composants sont des blocs complets en eux-mêmes et ils peuvent ne pas être écrits dans le même ordre que celui dans lequel ils doivent être exécutés. Le compilateur StyleBook vérifie l'ordre dans lequel les composants sont écrits, puis les exécute dans un ordre logique.

### Exemple :

```
1 components:
2   -
3     name: lbserver-comp
4     type: ns::lbserver
5     properties:
6       name: mylb
7       ipv46: 10.102.190.15
8       port: 80
9       servicetype: HTTP
10  -
11  name: lb-sg-binding-comp
12  type: ns::lbserver_servicegroup_binding
13  condition: $parameters.create-binding
14  properties:
15    name: $components.lbserver-comp.properties.name
16    servicegroupname: $components.sg-comp.properties.servicegroupname
17  -
18  name: sg-comp
19  type: ns::servicegroup
20  properties:
21    servicegroupname: msg
22    servicetype: HTTP
23  <!--NeedCopy-->
```

Dans l'exemple ci-dessus, trois composants sont définis - **lbserver-comp**, **lb-sg-binding-comp** et **sg-comp**. Lorsque ce StyleBook est exécuté, le lbserver-comp est d'abord créé. Le lb-sg-binding-comp fait référence aux propriétés lbserver-comp, mais il ne peut pas être créé ensuite, bien qu'il s'agisse du deuxième composant défini dans le StyleBook. En effet, le lb-sg-binding-comp dépend également du sg-comp qui n'a pas encore été créé. Par conséquent, le compilateur réorganise les composants de manière à ce que les dépendances d'un composant soient résolues au moment où un composant est créé, et exécute cette liste réorganisée de composants. L'ordre d'exécution du StyleBook ci-dessus est le suivant : lbserver-comp, sg-comp et lb-sg-binding-comp.

Ainsi, l'auteur d'un StyleBook n'a pas besoin de s'inquiéter de l'ordre correct des composants. Les composants peuvent apparaître dans n'importe quel ordre. Le compilateur calcule l'ordre d'exécution.

tion correct des composants en fonction de la façon dont les composants se réfèrent. Notez que cette détection et cette réorganisation des dépendances fonctionnent également pour les sections de substitution et de sortie.

## Dépendances cycliques

Comme un composant peut faire référence à un autre composant, il est possible qu'un cycle de dépendances soit introduit dans la définition du StyleBook. Par exemple, si le composant A fait référence à une propriété définie dans le composant B, qui fait encore référence à une propriété définie dans le composant A. Ce type de dépendance est appelé dépendances cycliques. Les dépendances cycliques ne peuvent pas être résolues automatiquement. L'auteur du StyleBook doit corriger manuellement la définition du StyleBook pour éliminer ces dépendances cycliques. Le compilateur sera en mesure d'identifier les dépendances cycliques - si elles existent, et de les signaler.

L'exemple suivant montre une dépendance cyclique des composants :

```
1 components:
2   -
3     name: lbserver-comp
4     type: ns::lbserver
5     properties:
6       name: $components.lb-sg-binding-comp.properties.name
7       ipv46: 10.102.190.15
8       port: 80
9       servicetype: HTTP
10    -
11     name: lb-sg-binding-comp
12     type: ns::lbserver_servicegroup_binding
13     condition: $parameters.create-binding
14     properties:
15       name: mylb
16       servicegroupname: $components.sg-comp.properties.servicegroupname
17    -
18     name: sg-comp
19     type: ns::servicegroup
20     properties:
21       servicegroupname: msg
22       servicetype: $components.lbserver-comp.properties.servicetype
23 <!--NeedCopy-->
```

Dans l'exemple ci-dessus, il existe trois composants : **lbserver-comp**, **lb-sg-binding-comp** et **sg-comp**. **lbserver-comp** dépend de **lb-sg-binding-comp**, **lb-sg-binding-comp** dépend de **sg-comp** et **sg-comp** dépend de **lbserver-comp**. Ici, un cycle de dépendances entre ces composants est formé et cela ne peut pas être résolu automatiquement. Par conséquent, ce StyleBook ne peut pas être exécuté. Le compilateur StyleBook détecte cela et empêche l'importation de StyleBook dans Citrix ADM.

## Gestion des instances

February 1, 2024

Les instances sont des appliances Citrix Application Delivery Controller (ADC) que vous pouvez gérer, surveiller et dépanner à l'aide de Citrix Application Delivery Management (ADM). Vous devez ajouter des instances à Citrix ADM pour les surveiller. Des instances peuvent être ajoutées lorsque vous configurez Citrix ADM ou ultérieurement. Une fois que vous avez ajouté des instances à Citrix ADM, elles sont interrogées en permanence pour collecter des informations qui peuvent être utilisées ultérieurement pour résoudre des problèmes ou en tant que données de reporting.

Les instances peuvent être regroupées sous la forme d'un groupe statique ou d'un bloc IP privé. Un groupe statique d'instances peut être utile lorsque vous souhaitez exécuter des tâches spécifiques telles que des tâches de configuration, etc. Un bloc IP privé regroupe vos instances en fonction de leur emplacement géographique.

### Ajouter une instance

Vous pouvez ajouter des instances lors de la configuration du serveur Citrix ADM pour la première fois ou ultérieurement. Pour ajouter des instances, vous devez spécifier le nom d'hôte ou l'adresse IP de chaque instance Citrix ADC, ou une plage d'adresses IP.

Pour savoir comment ajouter une instance à Citrix ADM, consultez la section [Ajouter des instances à Citrix ADM](#).

Lorsque vous ajoutez une instance au serveur Citrix ADM, le serveur s'ajoute implicitement comme destination d'interruption pour l'instance et collecte l'inventaire de l'instance. Pour en savoir plus, consultez [Comment Citrix ADM découvre les instances](#).

Après avoir ajouté une instance, vous pouvez la supprimer en accédant à **Réseaux > Tableau de bord** et en cliquant sur **Toutes les instances**. Sur la page Instances, sélectionnez l'instance à supprimer et cliquez sur **Supprimer**.

### Comment utiliser le tableau de bord de l'instance

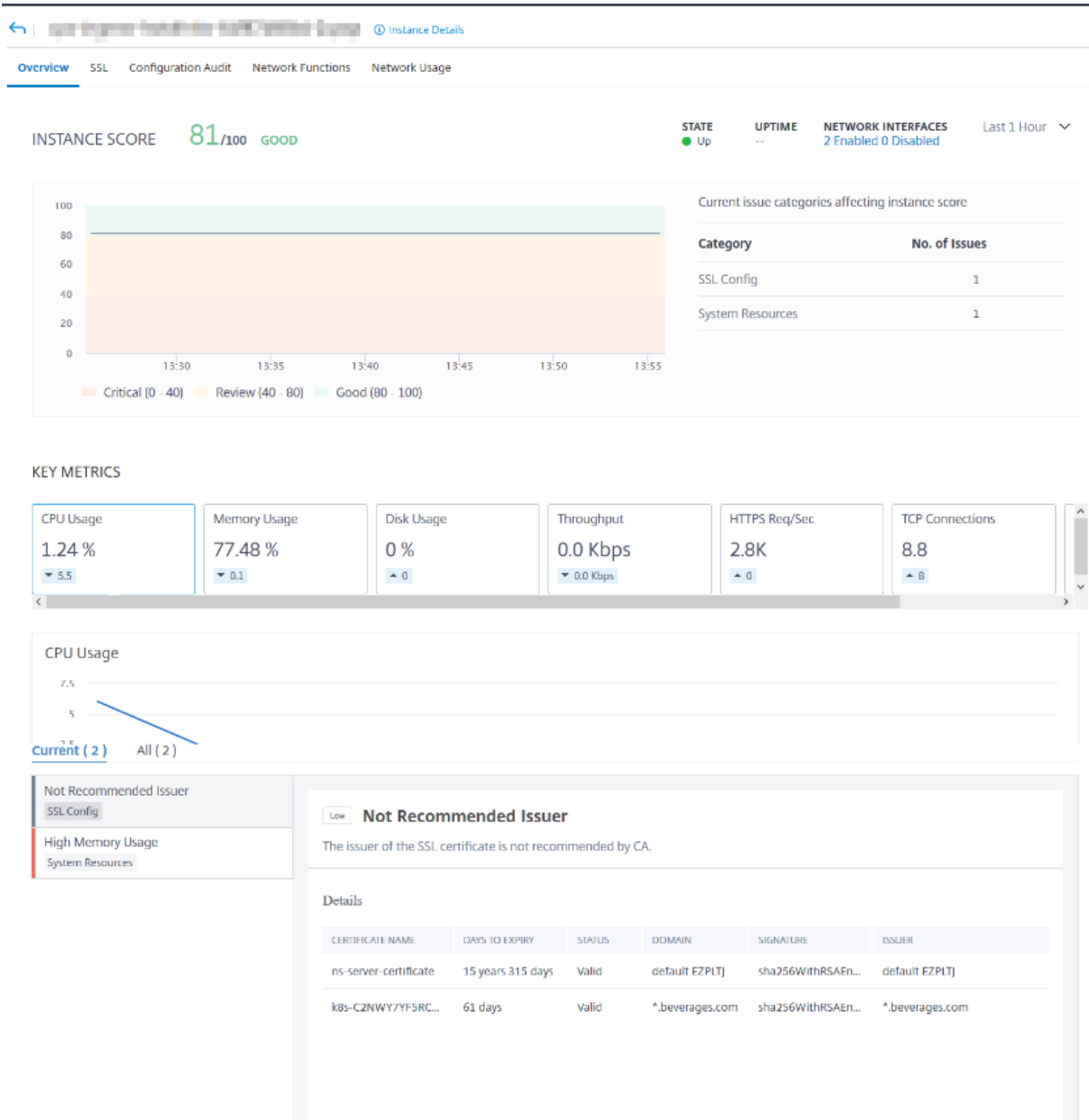
Le tableau de bord par instance de Citrix ADM affiche les données sous forme de tableau et de graphique pour l'instance sélectionnée. Les données collectées à partir de votre instance lors du processus de sondage sont affichées sur le tableau de bord.

Par défaut, chaque minute, les instances gérées sont interrogées pour la collecte de données. Les informations statistiques telles que l'état, les requêtes HTTP par seconde, l'utilisation du processeur, l'utilisation de la mémoire et le débit sont collectées en continu à l'aide des appels NITRO. En tant qu'

administrateur, vous pouvez afficher toutes ces données collectées sur une seule page, identifier les problèmes dans l'instance et prendre des mesures immédiates pour les corriger.

Pour afficher le tableau de bord d'une instance spécifique, accédez à **Réseaux > Instances**. Dans le résumé, choisissez le type d'instance, puis sélectionnez l'instance à afficher et cliquez sur **Tableau de bord**.

L'illustration suivante fournit une vue d'ensemble des différentes données affichées sur le tableau de bord par instance :



- **Vue d'ensemble.** L'onglet Vue d'ensemble affiche l'utilisation du processeur et de la mémoire de l'instance choisie. Vous pouvez également afficher les événements générés par l'instance

et les données de débit. Les informations spécifiques à l'instance, telles que l'adresse IP, son matériel et ses versions LOM, les détails du profil, le numéro de série, la personne à contacter, etc. sont également affichées ici. En faisant défiler vers le bas, les fonctionnalités sous licence disponibles sur l'instance choisie ainsi que les modes configurés sur celle-ci.

- **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 configuration NetScaler du tableau de bord affichent des informations détaillées sur les modifications de configuration enregistrées par rapport aux configurations non enregistrées.**
- **Fonctions réseau.** À l'aide du tableau de bord des fonctions réseau, vous pouvez surveiller l'état des entités configurées sur l'instance Citrix ADC sélectionnée. Vous pouvez afficher des graphiques pour vos serveurs virtuels qui affichent des données telles que les connexions client, le débit et les connexions serveur.
- **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 » en bas à droite de l'écran pour ajouter un rapport de performance supplémentaire.

## Surveiller les sites distribués à l'échelle mondiale

February 1, 2024

En tant qu'administrateur réseau, vous devrez peut-être surveiller et gérer les instances réseau déployées sur des sites géographiques. Toutefois, il n'est pas facile d'évaluer les besoins du réseau lors de la gestion des instances réseau dans des datacenters répartis géographiquement.

Les géomaps de Citrix Application Delivery Management (ADM) vous fournissent une représentation graphique de vos sites et répartit votre expérience de surveillance réseau par géographie. Avec les géomaps, vous pouvez visualiser la distribution de votre instance réseau par emplacement et surveiller les problèmes réseau.

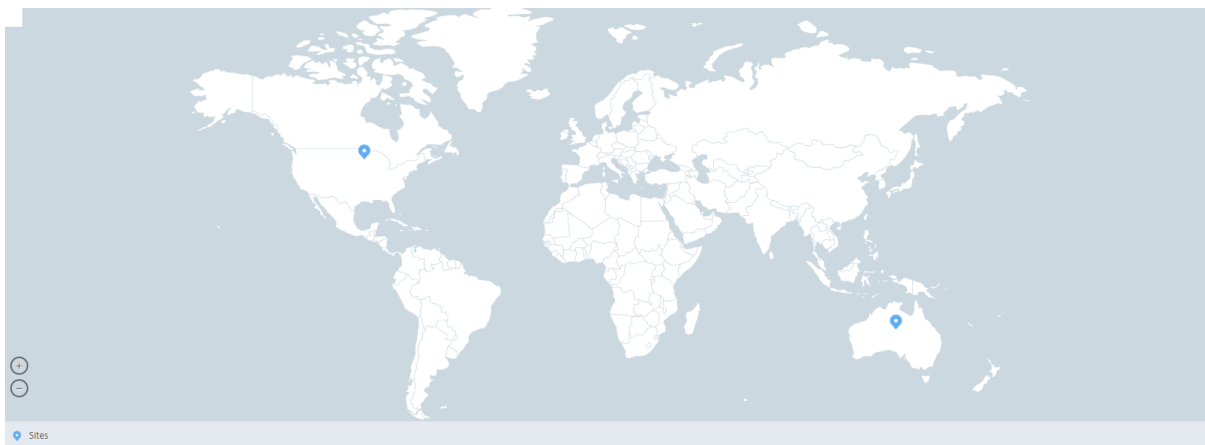
La section suivante explique comment surveiller les centres de données dans Citrix ADM.

Le site Citrix ADM est un regroupement logique d'instances de Citrix Application Delivery Controller (ADC) dans un emplacement géographique spécifique. Par exemple, lorsqu'un site est affecté à Amazon Web Services (AWS) et un autre site peut être affecté à Azure™. Un autre site est hébergé dans les locaux du locataire. Citrix ADM gère et surveille toutes les instances Citrix ADC connectées à tous les sites. Vous pouvez utiliser Citrix ADM pour surveiller et collecter des données Syslog, AppFlow, SNMP et toutes les données de ce type provenant des instances gérées.

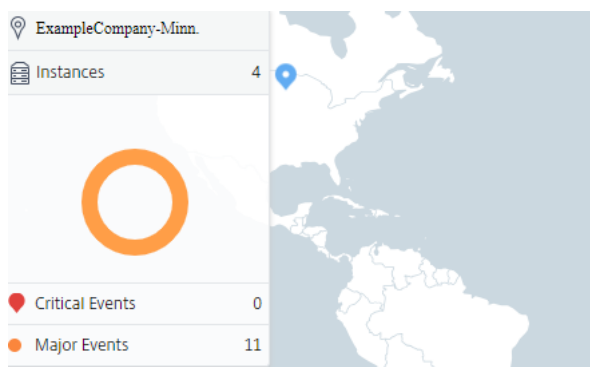
Geomaps dans Citrix ADM vous fournit une représentation graphique de vos sites. Geomaps décompose également votre expérience de surveillance réseau par zone géographique. Avec les géomaps, vous pouvez visualiser la distribution de votre instance réseau par emplacement et surveiller tous les problèmes réseau. Vous pouvez accéder à la page **Réseaux > Tableau de bord** pour obtenir une représentation visuelle des sites créés sur la carte du monde.

### Cas d'utilisation

Un opérateur de téléphonie mobile de premier plan, ExampleCompany, s'appuyait sur des fournisseurs de services privés pour héberger ses ressources et ses applications. L'entreprise possédait déjà deux sites, l'un à Minneapolis aux États-Unis et l'autre à Alice Springs en Australie. Dans cette image, vous pouvez voir que deux marqueurs représentent les deux sites existants.

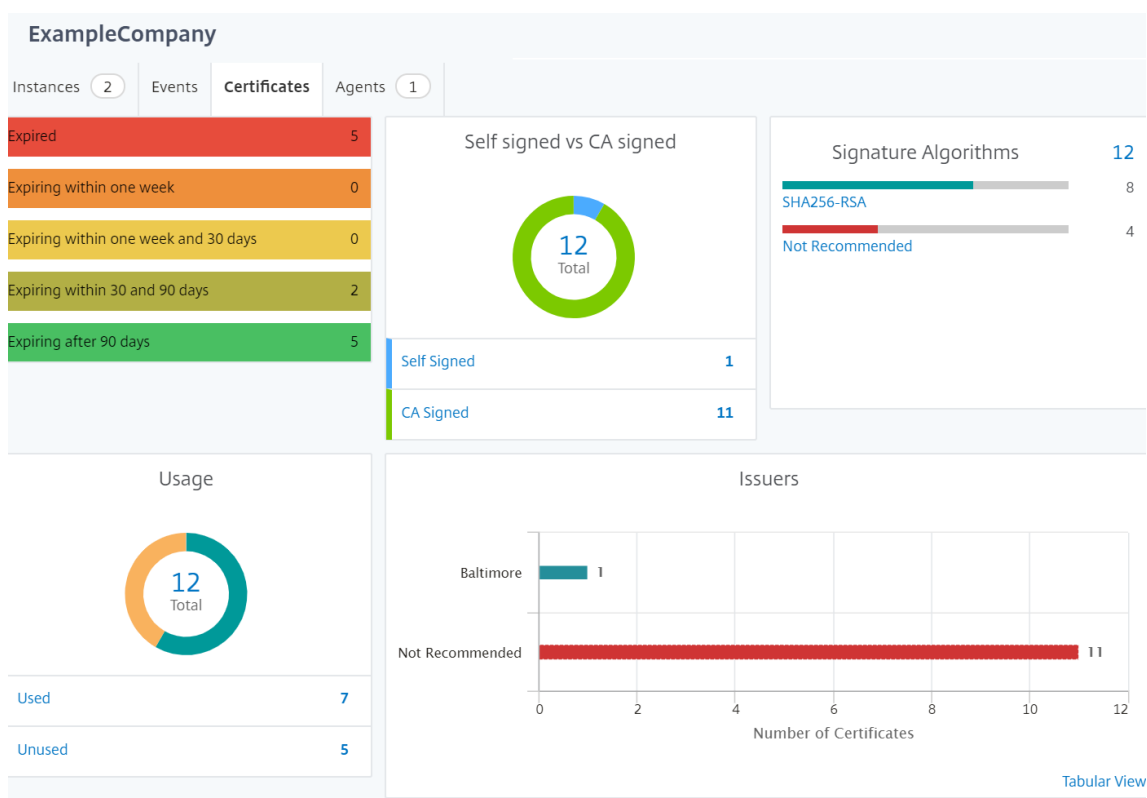


Les marqueurs affichent également un nombre, qui indique le nombre d'applications dans chaque site. Vous pouvez cliquer sur ces marqueurs pour plus d'informations sur chaque site.



Cliquez sur les onglets pour afficher plus d'informations :

- Onglet **Instances** : affichez les informations suivantes dans cet onglet :
  - Adresse IP de chaque instance réseau
  - Type d'instance
  - Nombre d'événements critiques sur eux
  - Événements significatifs et tous les événements générées sur une instance Citrix ADC.
- Onglet **Événements** : consultez la liste des événements critiques et significatifs signalés sur les instances.
- Onglet **Certificats** : affichez les informations suivantes dans cet onglet :
  - Liste des certificats de toutes les instances
  - État d'expiration
  - Informations vitales et les 10 principales instances de nombreux certificats utilisés.
- Onglet **Agents** : affichez la liste des agents auxquels les instances sont liées.



## Configuration des géomaps

ExampleCompany a décidé de créer un troisième site à Bangalore, en Inde. L'entreprise souhaitait tester le cloud en déchargeant certaines de ses applications informatiques internes les moins critiques vers le bureau de Bangalore. L'entreprise a décidé d'utiliser les services de cloud computing d'AWS.

En tant qu'administrateur, vous devez d'abord créer un site, puis ajouter les instances Citrix ADC dans Citrix ADM. Vous devez également ajouter l'instance au site, ajouter un agent et lier l'agent au site. Citrix ADM reconnaît ensuite le site auquel appartient l'instance Citrix ADC et l'agent.

Pour plus d'informations sur l'ajout d'instances Citrix ADC, consultez la section [Ajout d'instances](#).

### Pour créer des sites :

Créez des sites avant d'ajouter des instances dans Citrix ADM. Fournir des informations de localisation vous permet de localiser le site avec précision.

Accédez à **Réseaux > Sites**, puis cliquez sur **Ajouter**.

1. Dans la page **Créer un site**, spécifiez les informations suivantes :
  - a) **Type de site** : Sélectionnez un **centre de données**.



### Remarque

Le site peut fonctionner comme centre de données principal ou comme succursale. Choisissez en conséquence.

- b) **Type** : Sélectionnez AWS comme fournisseur de cloud dans la liste.

### Remarque

Cochez la case **Utiliser un VPC existant comme site** en conséquence.

- c) **Nom du site** : entrez le nom du site.
- d) **Ville** : entrez la ville.
- e) **Code postal** : entrez le code postal.
- f) **Région** : entrez la région.
- g) **Pays** : Tapez le pays
- h) **Latitude** : saisissez la latitude de l'emplacement.  
Pour la latitude sud, spécifiez des valeurs négatives. Exemple : -77.5946.
- i) **Longitude** : saisissez la longitude de l'emplacement.  
Pour la longitude ouest, spécifiez des valeurs négatives. Exemple : -12.9716.

## 2. Cliquez sur **Créer**.

### ← Create Site

Site type  
 Data Center  Branch

Type\*  
AWS

Use existing VPC as a site

Site Name\*  
ExampleCompany

City\*  
Bangalore

ZIP Code\*  
560001

Region\*  
Karnataka

Country\*  
India

Latitude\*  
77.5946

Longitude\*  
12.9716

Create Close

### Pour ajouter des instances et sélectionner des sites :

Après avoir créé des sites, vous devez ajouter des instances dans Citrix ADM. Vous pouvez sélectionner le site précédemment créé, ou vous pouvez également créer un site et associer l'instance.

Après avoir créé des sites, vous devez ajouter des instances dans Citrix ADM. Vous pouvez sélectionner le site précédemment créé, ou vous pouvez également créer un site et associer l'instance.

1. Dans Citrix ADM, accédez à **Réseaux > Instances**.
2. Sélectionnez le type d'instance à créer, puis cliquez sur **Ajouter**.
3. Sur la page **Ajouter Citrix ADC VPX**, tapez l'adresse IP et sélectionnez le profil dans la liste.
4. Sélectionnez le site dans la liste. Vous pouvez cliquer sur le signe + à côté **du champ Site** pour créer un site ou cliquer sur l'icône de modification pour modifier les détails du site par défaut.
5. Cliquez sur la flèche droite et sélectionnez l'agent dans la liste qui s'affiche.

### ← Add Citrix ADC VPX

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**.

Agents					
	IP Address	Host Name	Current Version	Recommended Version	Upgrade Status
<input checked="" type="radio"/>	10.102.31.143	haproxyagent	12.0-509.119	12.0-509.119	✓ Up-to-date
<input type="radio"/>	192.168.4.63	ns	12.0-509.119	12.0-509.119	✓ Up-to-date
<input type="radio"/>	10.102.107.126	sathiya-adtest	12.0-509.119	12.0-509.119	✓ Up-to-date

1. Sélectionnez le site dans la liste et cliquez sur **Enregistrer**.

1. Cliquez sur **OK**.

Vous pouvez également attacher un agent à un site en accédant à **Réseaux > Agents**.

**Pour associer un agent Citrix ADM au site :**

1. Dans Citrix ADM, accédez à **Réseaux > Agents**.
2. Sélectionnez l'agent, puis cliquez sur **Joindre le site**.

### Agents

	IP Address	Host Name	Current Version	Recommended Version	Upgrade Status
<input checked="" type="checkbox"/>	10.102.31.143	haproxyagent	12.0-509.119	12.0-509.119	✔ Up-to-date
<input type="checkbox"/>	192.168.4.63	ns	12.0-509.119	12.0-509.119	✔ Up-to-date
<input type="checkbox"/>	10.102.107.126	sathiya-adtest	12.0-509.119	12.0-509.119	✔ Up-to-date
<input type="checkbox"/>	10.221.42.57	PROD-Agent2	12.0-509.119	12.0-509.119	✔ Up-to-date

1. Vous pouvez associer le site et cliquer sur **Enregistrer**.

Citrix ADM commence à surveiller les instances de Citrix ADC ajoutées dans le site Bangalore ainsi que les instances des deux autres sites.

## Comment créer des balises et affecter des instances

February 1, 2024

Citrix Application Delivery Management (ADM) vous permet désormais d'associer vos instances Citrix Application Delivery Controller (ADC) à des balises. Une balise est un mot-clé ou un terme à un mot que vous pouvez affecter à une instance. Les balises ajoutent des informations supplémentaires sur l'instance. Les balises peuvent être considérées comme des métadonnées qui permettent de décrire une instance. Les balises vous permettent de classer et de rechercher des instances en fonction de ces mots-clés spécifiques. Vous pouvez également affecter plusieurs balises à une seule instance.

Les cas d'utilisation suivants vous aident à comprendre comment le balisage des instances peut vous aider à mieux les surveiller.

- **Cas d'utilisation 1** : vous pouvez créer une balise pour identifier toutes les instances situées au Royaume-Uni. Ici, vous pouvez créer une balise avec la clé comme « Pays » et la valeur comme « Royaume-Uni ». Cette balise vous aide à rechercher et à surveiller toutes les instances situées au Royaume-Uni.

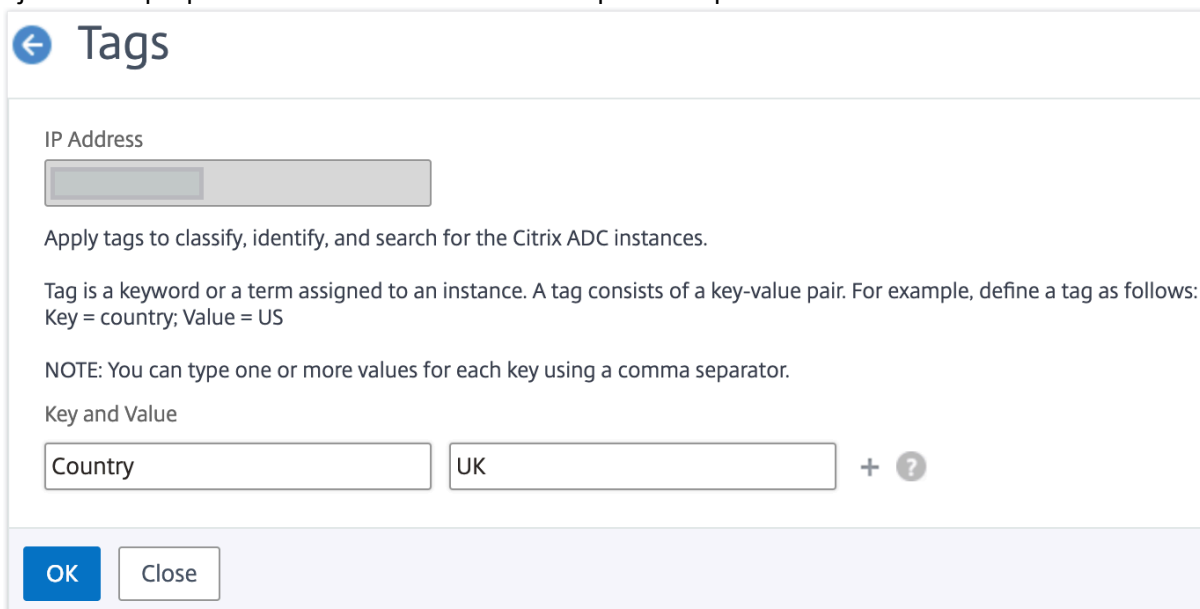
- **Cas d'utilisation 2** : vous souhaitez rechercher des instances qui se trouvent dans l'environnement intermédiaire. Ici, vous pouvez créer une balise avec la clé comme "Purpose" et la valeur comme "Staging\_NS." Cette balise vous permet de séparer toutes les instances utilisées dans l'environnement intermédiaire des instances dont les requêtes client sont exécutées à travers elles.
- **Cas d'utilisation 3** : Considérez une situation où vous souhaitez connaître la liste des instances de Citrix ADC situées dans la région de Swindon au Royaume-Uni et que vous possédez, David T. Vous pouvez créer des balises pour toutes ces exigences et l'affecter à toutes les instances qui satisfont à ces conditions.

**Pour affecter des balises à l'instance Citrix ADC VPX :**

1. Dans Citrix ADM, accédez à **Réseaux > Instances > Citrix ADC**.
2. Sélectionnez l'onglet **Citrix ADC VPX**.
3. Sélectionnez le Citrix VPX requis.
4. Cliquez sur **Balises**.
5. Créez des balises et cliquez sur **OK**.

La fenêtre **Balises** qui s'affiche vous permet de créer vos propres paires « clé-valeur » en affectant des valeurs à chaque mot clé que vous créez.

Par exemple, les images suivantes montrent quelques mots clés créés et leurs valeurs. Vous pouvez ajouter vos propres mots clés et saisir une valeur pour chaque mot clé.



## ← Tags

IP Address

Apply tags to classify, identify, and search for the Citrix ADC instances.

Tag is a keyword or a term assigned to an instance. A tag consists of a key-value pair. For example, define a tag as follows:  
Key = country; Value = US

NOTE: You can type one or more values for each key using a comma separator.

Key and Value

Purpose	Staging_NS	+	?
---------	------------	---	---

OK Close

Vous pouvez également ajouter plusieurs balises en cliquant sur « +. » L'ajout de balises multiples et significatives vous permet de rechercher très efficacement les instances.

## ← Tags

IP Address

Apply tags to classify, identify, and search for the Citrix ADC instances.

Tag is a keyword or a term assigned to an instance. A tag consists of a key-value pair. For example, define a tag as follows:  
Key = country; Value = US

NOTE: You can type one or more values for each key using a comma separator.

Key and Value

Country	UK	x	
Area	Swindon	x	?
Owner	David T	x	+

OK Close

Vous pouvez ajouter plusieurs valeurs à un mot-clé en les séparant par des virgules.

Par exemple, vous attribuez le rôle d'administrateur à un autre collègue, Greg T. Vous pouvez ajouter son nom en le séparant par une virgule. L'ajout de plusieurs noms vous aide à rechercher par l'un des noms ou par les deux noms. Citrix ADM reconnaît les valeurs séparées par des virgules en deux valeurs différentes.

## ← Tags

IP Address

Apply tags to classify, identify, and search for the Citrix ADC instances.

Tag is a keyword or a term assigned to an instance. A tag consists of a key-value pair. For example, define a tag as follows:  
Key = country; Value = US

NOTE: You can type one or more values for each key using a comma separator.

Key and Value

Country	UK	x	
Area	Swindon	x	?
Owner	David T, Greg T	x	+

Pour en savoir plus sur la recherche d'instances en fonction de balises, consultez [Comment rechercher des instances à l'aide des valeurs des balises et des 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 Citrix Application Delivery Management (ADM) gère un grand nombre d'instances de Citrix ADC. En tant qu'administrateur, vous pouvez avoir la possibilité de rechercher dans l'inventaire des instances en fonction de certains paramètres. Citrix ADM offre désormais une fonctionnalité de recherche améliorée pour rechercher un sous-ensemble d'instances Citrix ADC en fonction des paramètres que vous définissez dans le champ de recherche. Vous pouvez rechercher les instances en fonction de deux critères : les balises et les propriétés.

- **Étiquettes.** Les balises sont des termes ou des mots-clés que vous pouvez attribuer à une instance Citrix ADC pour ajouter une description supplémentaire de l'instance Citrix ADC. Vous

pouvez désormais associer vos instances Citrix ADC à des balises. Ces balises peuvent être utilisées pour mieux identifier et rechercher sur les instances Citrix ADC.

- **Propriétés.** Chaque instance Citrix ADC ajoutée dans Citrix ADM a quelques paramètres ou propriétés par défaut associés à cette instance. Par exemple, chaque instance a son propre nom d'hôte, adresse IP, version, ID d'hôte, ID de modèle matériel, etc. Vous pouvez rechercher des instances en spécifiant des valeurs pour n'importe laquelle de ces propriétés.

Par exemple, imaginez une situation dans laquelle vous souhaitez connaître la liste des instances Citrix ADC qui sont sur la version 12.0 et qui sont dans l'état UP. Ici, la version et l'état de l'instance sont définis par les propriétés par défaut.

Outre la version 12.0 et l'état UP des instances, vous pouvez également rechercher les instances qui vous appartiennent. Vous pouvez créer une balise « Propriétaire » et attribuer une valeur « David T » à cette balise. Pour plus d'informations sur la création et l'affectation de balises, voir Procédure de création de balises et d'affectation à des instances.

Vous pouvez utiliser une combinaison de balises et de propriétés pour créer vos propres critères de recherche.

### **Pour rechercher des instances Citrix ADC VPX**

1. Dans Citrix ADM, accédez à l'onglet **Réseaux > Instances > Citrix ADC > VPX**.
2. Cliquez sur le champ de recherche. Vous pouvez créer une expression de recherche en utilisant des balises ou des propriétés ou en combinant les deux.

Les exemples suivants montrent comment utiliser efficacement l'expression de recherche pour rechercher l'instance.

- a) Sélectionnez l'option **Balises** et sélectionnez **Propriétaire**. Sélectionnez « David T. »

## NetScaler

The screenshot shows the NetScaler interface with search filters: VPX (22), MPX (0), CPX (0), SDX (0), and BLX (0). Below the filters are buttons for Add, Edit, Remove, Dashboard, Tags, Partitions, Provision, License, and a Select Action dropdown. A search bar contains the text "Click here to search or you can enter Key : Value format". A dropdown menu is open over the search bar, showing "Tags" and "Properties" categories. Under "Properties", the "owner" property is selected, and a list of values is shown: "area", "country", and "owner". The main table below shows columns for IP ADDRESS, HOST NAME, INSTANCE STATE, RX (MBPS), and TX (MBPS). The first row shows IP 10.102.201.74, HOST NAME SF01, and INSTANCE STATE Up. The second row shows IP 10.102.126.34, HOST NAME --, and INSTANCE STATE Out of Service.

The screenshot shows the NetScaler interface with search filters: VPX (22), MPX (0), CPX (0), SDX (0), and BLX (0). Below the filters are buttons for Add, Edit, Remove, Dashboard, Tags, Partitions, and Provision. A search bar contains the text "owner :". A dropdown menu is open over the search bar, showing a list of names: "david t", "greg", "dave p", "david", and "stephen". The main table below shows columns for IP ADDRESS, HOST NAME, and INST. The first row shows IP 10.102.126.33 - 10.102.126.52, HOST NAME --, and INST. Up. The second row shows IP 10.102.201.73, HOST NAME dub2-br-edg-p13-lb9, and INST. Up.

Citrix ADM prend en charge les expressions régulières et les caractères génériques dans les expressions de recherche.

- b) Vous pouvez utiliser des expressions régulières pour élargir les critères de recherche. Par exemple, vous souhaitez rechercher des instances appartenant à David ou à Stephen. Dans ce cas, vous pouvez taper les valeurs en les séparant par une expression « | ».

## NetScaler

The screenshot shows the NetScaler interface with search filters: VPX (1), MPX (0), CPX (0), SDX (0), and BLX (0). Below the filters are buttons for Add, Edit, Remove, Dashboard, Tags, Partitions, Provision, License, and a Select Action dropdown. A search bar contains the text "owner : david | greg". Below the search bar is the text "Click here to search or you can enter Key : Value format". The main table below shows columns for IP ADDRESS, HOST NAME, INSTANCE STATE, RX (MBPS), TX (MBPS), and HTTP REQ/S. The first row shows IP ADDRESS --, HOST NAME --, INSTANCE STATE Up, RX (MBPS) 0, TX (MBPS) 0, and HTTP REQ/S 0. Below the table is a summary bar that says "Total 1".

- c) Vous pouvez également utiliser des caractères génériques pour remplacer ou représenter un ou plusieurs caractères. Par exemple, vous pouvez taper « Dav\* » pour rechercher toutes les instances appartenant à David T et Dave P.



NetScaler

VPX 2 MPX 0 CPX 0 SDX 0 BLX 0

Add Edit Remove Dashboard Tags Partitions Provision License Select Action

owner: dav\*

Click here to search or you can enter Key : Value format

	IP ADDRESS	HOST NAME	INSTANCE STATE	RX (MBPS)	TX (MBPS)	HTTP REQ/S	AGENT	SITE
<input type="checkbox"/>	10.102.201.74	INFLNGSF01	Down	0	0	0	--	Default
<input type="checkbox"/>	10.102.126.35	--	Up	0	0	3	--	Default

### Remarque

Pour plus d'informations sur les expressions régulières et les caractères génériques et sur leur utilisation, cliquez sur l'icône « Informations » dans la barre de recherche.

## Gérer les partitions d'administration des instances Citrix ADC

February 1, 2024

Vous pouvez configurer des partitions d'administration sur vos instances de Citrix Application Delivery Controller (ADC) de sorte que différents groupes de votre organisation se voient attribuer des partitions différentes sur la même instance de Citrix ADC. Un administrateur réseau peut être affecté pour gérer plusieurs partitions sur plusieurs instances Citrix ADC.

Citrix Application Delivery Management (ADM) offre un moyen transparent de gérer toutes les partitions appartenant à un administrateur à partir d'une console unique. Vous pouvez gérer ces partitions sans perturber d'autres configurations de partitions.

Pour permettre à plusieurs utilisateurs de gérer différentes partitions d'administration, vous devez créer des groupes, puis affecter des utilisateurs et des partitions à ces groupes. Chaque utilisateur peut afficher et gérer uniquement les partitions du groupe auquel il appartient. Chaque partition d'administration est considérée comme une instance dans Citrix ADM. Lorsque vous découvrez une instance Citrix ADC, les partitions d'administration configurées sur cette instance Citrix ADC sont automatiquement ajoutées au système.

Considérez que vous avez deux instances Citrix VPX avec deux partitions configurées sur chaque instance. Par exemple, l'instance Citrix ADC 10.102.216.49 a Partition\_1, Partition\_2 et Partition\_3, et l'instance Citrix ADC 10.102.29.120 a p1 et p2 comme illustré dans l'image suivante.

Pour afficher les partitions, accédez à **Réseaux > Instances > Citrix ADC > VPX**, puis cliquez sur **Partitions**.

Vous pouvez affecter user-p1 les partitions suivantes : 10.102.29.120-p1 et 10.102.216.49-Partition\_1.

Vous pouvez également attribuer à user-p2 la gestion des partitions 10.102.29.80-p2, 10.102.216.49-Partition\_2 et 10.102.216.49-Partition\_3.

Ensuite, vous devez créer les deux utilisateurs, user-p1 et user-p2, et vous devez affecter les utilisateurs aux groupes que vous avez créés pour eux.

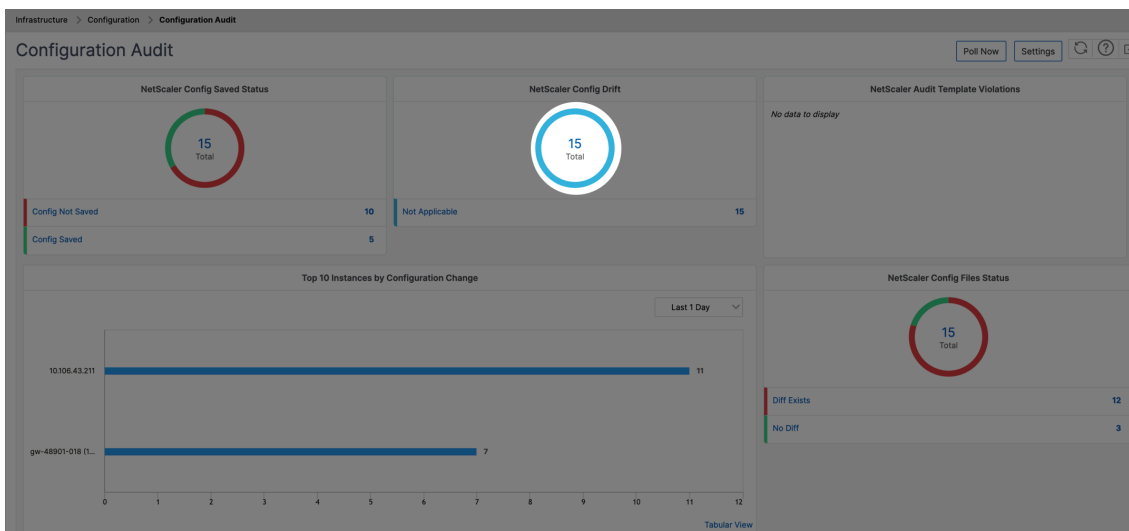
Tout d’abord, vous devez créer deux groupes avec les autorisations appropriées (par exemple : permissions admin) et inclure les instances de partition admin requises dans chaque groupe. Par exemple, créez le groupe système partition1-admin et ajoutez les partitions d’administration Citrix ADC 10.102.29.120-p1 et 10.102.216.49-Partition\_1 à ce groupe. Créez également le groupe système partition2-admin et ajoutez les partitions d’administration Citrix ADC 10.102.29.120-p2, 10.102.216.49-Partition\_2 et 10.102.216.49-Partition\_3 et à ce groupe.

Après avoir créé la partition admin, vous pouvez également utiliser la fonction de différence d’historique des révisions et le modèle d’audit pour la fonctionnalité de partition admin à des fins d’audit

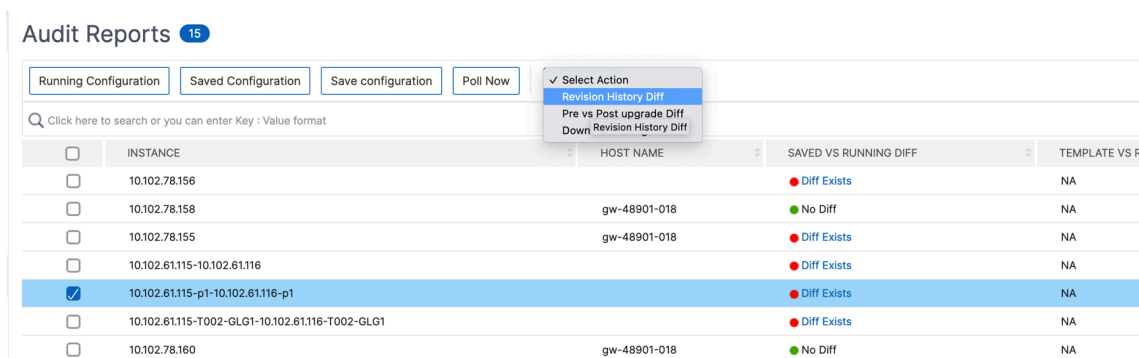
**La différence d’historique des révisions** pour la partition d’administration vous permet d’afficher la différence entre les cinq derniers fichiers de configuration pour une instance Citrix ADC partitionnée. Vous pouvez comparer les fichiers de configuration les uns aux autres (exemple Révision de configuration - 1 avec Révision de configuration -2) ou avec la configuration en cours d’exécution/enregistrée avec Révision de configuration. Avec les différences de configuration, les configurations de correction sont également affichées. Vous pouvez exporter toutes les commandes correctives dans votre dossier local et corriger les configurations.

**Pour afficher la différence dans l’historique des révisions :**

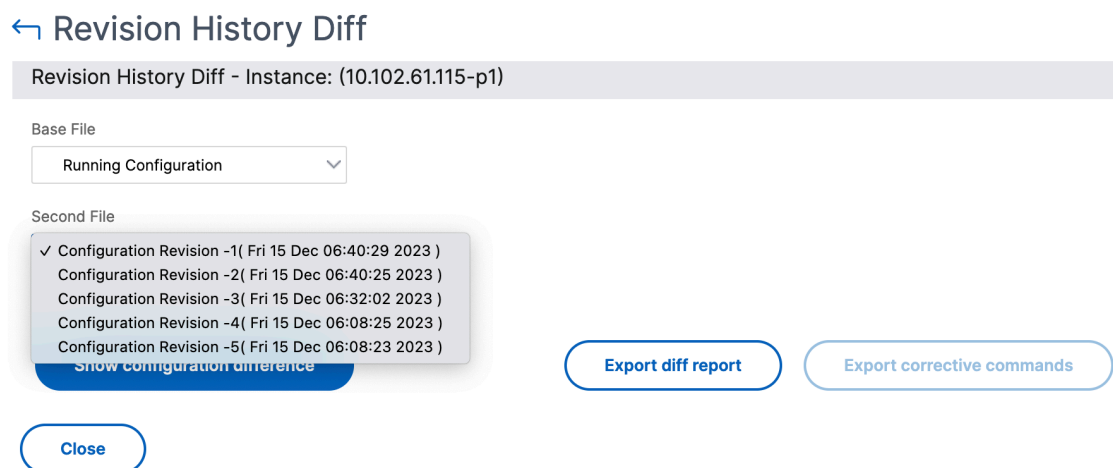
1. Accédez à **Réseaux > Audit de configuration**. Cliquez à l’intérieur du graphique en donut qui représente l’état de configuration de l’instance. Dans la page **Rapports d’audit** qui s’ouvre, cliquez sur l’instance Citrix ADC partitionnée.



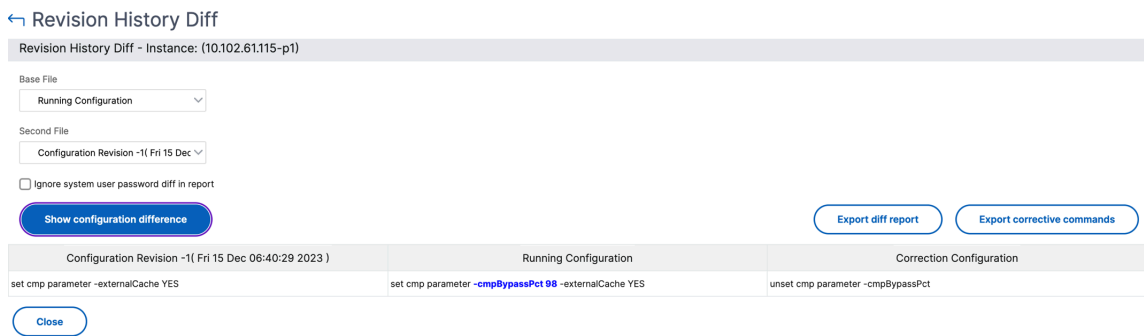
2. Dans le menu **Action**, cliquez sur **Diff Historique des révisions**.



3. Dans la page **Diff de l'historique des révisions**, sélectionnez les fichiers que vous souhaitez comparer. Par exemple, comparez la configuration enregistrée avec la révision de configuration -1, puis cliquez sur **Afficher la différence de configuration**.



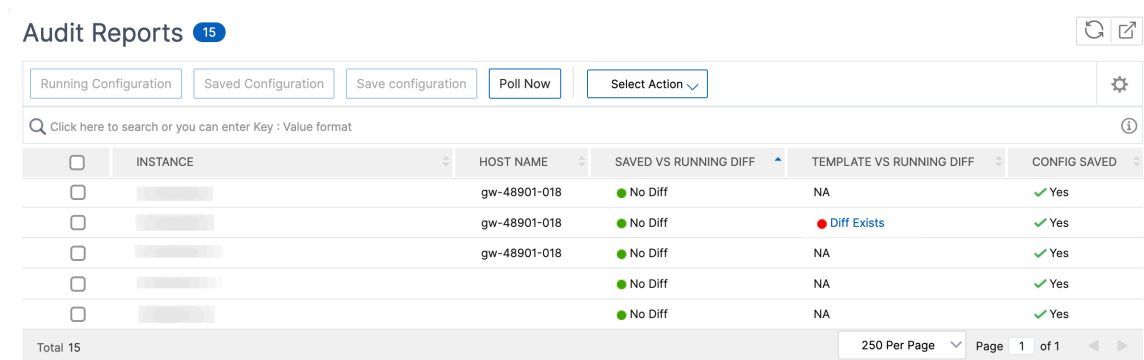
4. Vous pouvez ensuite afficher la différence entre les cinq derniers fichiers de configuration pour l'instance Citrix ADC partitionnée sélectionnée, comme indiqué ci-dessous. Vous pouvez également afficher les commandes de configuration corrective et exporter ces commandes correctives dans votre dossier local. Ces commandes correctives sont les commandes qui doivent être exécutées sur le fichier de base afin d'obtenir la configuration à l'état souhaité (fichier de configuration utilisé pour la comparaison).



**Les modèles d’audit pour la partition** vous permettent de créer un modèle de configuration personnalisé et de l’associer à une instance de partition. Toute variation de la configuration d’exécution de l’instance avec le modèle d’audit est affichée dans la colonne **Template vs Running diff** de la page **Rapports d’audit** . Outre les différences de configuration, les configurations de correction sont également affichées. Vous pouvez également exporter toutes les commandes correctives dans votre dossier local et corriger les configurations.

**Pour afficher la différence entre le modèle et l’exécution :**

1. Dans la page **Rapports d’audit**, cliquez sur l’instance Citrix ADC partitionnée.



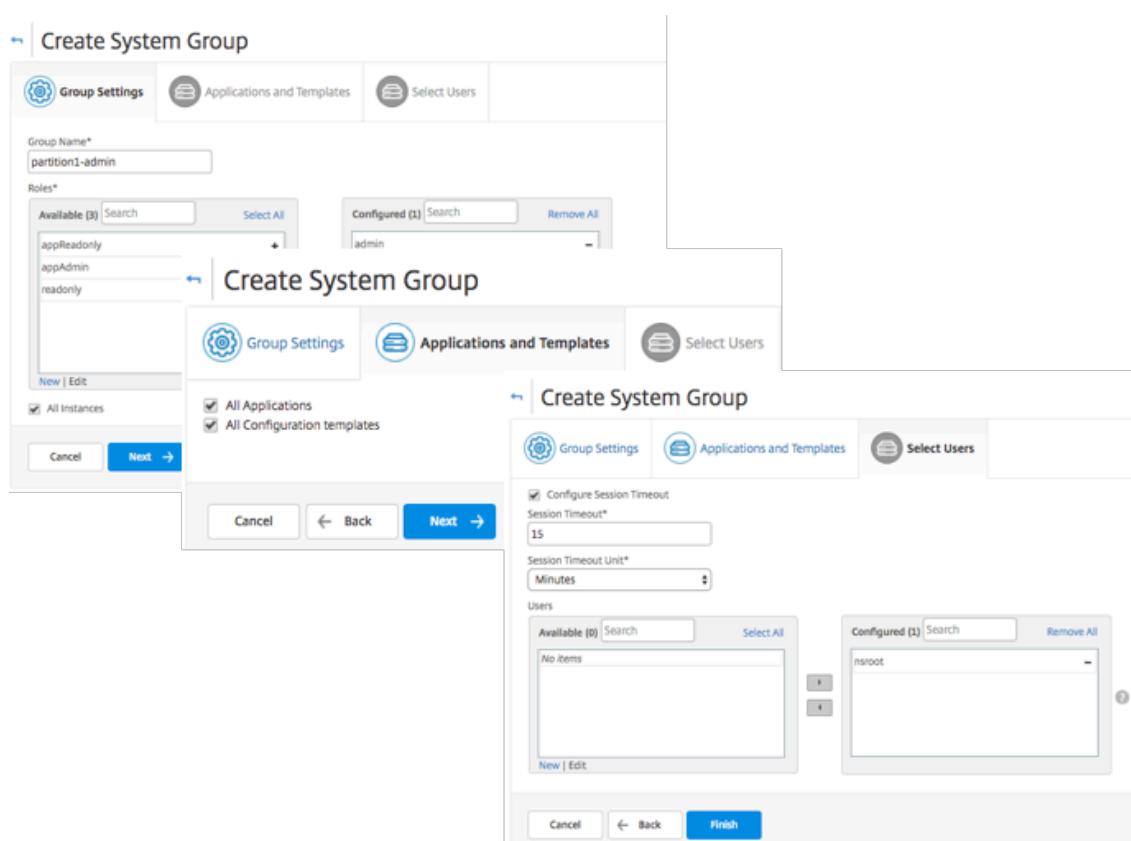
2. S’il existe une différence entre le modèle d’audit et la configuration en cours d’exécution, la différence est affichée sous forme de lien hypertexte. Cliquez sur le lien hypertexte pour afficher les différences s’il y en a. Avec les différences de configuration, les configurations de correction sont également affichées. Vous pouvez également exporter toutes les commandes correctives dans votre dossier local et corriger les configurations.

**Pour créer des groupes :**

1. Accédez à **Système > Administration des utilisateurs > Groupes**, puis cliquez sur **Ajouter**.
2. Dans la page **Créer un utilisateur système**, spécifiez les éléments suivants :
  - Onglet **Paramètres du groupe** : entrez le nom du groupe et les autorisations de rôle. Pour autoriser l’accès à des instances spécifiques, désactivez la case à cocher **Toutes les instances** , puis choisissez vos instances sur la page **Sélectionner les instances** .

- **Onglet Applications et modèles** : vous pouvez choisir d'utiliser ce groupe dans toutes les applications et tous les modèles de configuration.
- **Onglet Sélectionner les utilisateurs** : **sélectionnez les utilisateurs que vous souhaitez ajouter à ce groupe**. Vous pouvez cliquer sur le lien **Nouveau** dans le tableau **Disponible** pour créer de nouveaux utilisateurs. Vous pouvez également configurer le délai d'expiration de la session, dans lequel vous pouvez configurer la période pendant laquelle un utilisateur peut rester actif.

3. Cliquez sur **Terminer**.



**Pour créer des utilisateurs :**

1. Accédez à **Système>Administration des utilisateurs> Utilisateurs**, puis cliquez sur **Ajouter**.
2. Dans la page **Créer un utilisateur système**, spécifiez le nom d'utilisateur et le mot de passe. Vous pouvez éventuellement activer l'authentification externe et configurer le délai d'expiration de la session.
3. Attribuez l'utilisateur à un groupe en ajoutant le nom du groupe de la liste **Disponible** à la liste **configurée**.
4. Cliquez sur **Créer**.

Maintenant, déconnectez-vous et ouvrez une session avec les informations d'identification de l'utilisateur p1. Vous pouvez afficher et gérer uniquement les partitions d'administration qui vous sont attribuées pour gérer et surveiller.

## Sauvegarder et restaurer des instances Citrix ADC

February 1, 2024

Vous pouvez sauvegarder l'état actuel d'une instance Citrix ADC et utiliser ultérieurement les fichiers sauvegardés pour la restaurer dans le même état. Vous devez toujours sauvegarder une instance avant de la mettre à niveau ou pour des raisons de précaution. Une sauvegarde d'un système stable vous permet de le restaurer à un point stable s'il devient instable.

Il existe plusieurs façons d'effectuer des sauvegardes et des restaurations sur une instance Citrix ADC. Vous pouvez sauvegarder et restaurer manuellement les configurations Citrix ADC à l'aide de l'interface graphique et de l'interface de ligne de commande. Vous pouvez également utiliser Citrix ADM pour effectuer des sauvegardes automatiques et des restaurations manuelles.

Citrix ADM sauvegarde l'état actuel de vos instances Citrix ADC gérées à l'aide d'appels NITRO et des protocoles Secure Shell (SSH) et Secure Copy (SCP).

Citrix ADM crée une sauvegarde complète et restaure les types d'instance Citrix ADC suivants :

- Citrix SDX
- Citrix VPX
- Citrix MPX

Pour plus d'informations, consultez [Sauvegarder et restaurer une instance ADC].(<https://docs.citrix.com/en-us/citrix-adc/12-1/system/basic-operations/backup-restore-citrix-adc-appliance.html>)

### Remarque

- À partir de Citrix ADM, vous ne pouvez pas effectuer l'opération de sauvegarde et de restauration sur un cluster Citrix ADC.
- Vous ne pouvez pas utiliser le fichier de sauvegarde provenant d'une instance pour restaurer une autre instance.

Les fichiers sauvegardés sont stockés en tant que fichier TAR compressé dans le répertoire suivant :

```
1 /var/mps/tenants/root/device_backup/  
2 <!--NeedCopy-->
```

Pour éviter les problèmes dus à la non-disponibilité de l'espace disque, vous pouvez enregistrer un maximum de 50 fichiers de sauvegarde dans ce répertoire.

Pour sauvegarder et restaurer des instances Citrix ADC, vous devez d'abord configurer les paramètres de sauvegarde sur Citrix ADM. Après avoir configuré les paramètres, vous pouvez sélectionner une ou plusieurs instances Citrix ADC et créer une sauvegarde des fichiers de configuration dans ces instances. Si nécessaire, vous pouvez également restaurer les instances de Citrix ADC à l'aide de ces fichiers sauvegardés.

## Configurer les paramètres de sauvegarde d'instance

La page **Paramètres de sauvegarde d'instance** vous permet de configurer les paramètres sur Citrix ADM pour sauvegarder une instance Citrix ADC sélectionnée ou plusieurs instances :

Dans Citrix ADM, accédez à **Système > Administration système**. Dans le volet droit, sous Paramètres de l'**instance**, sélectionnez **Paramètres de sauvegarde de l'instance** et spécifiez ce qui suit :

1. **Activer les sauvegardes d'instance** : par défaut, Citrix ADM est activé pour effectuer des sauvegardes d'instances Citrix ADC. Désactivez cette option si vous ne souhaitez pas créer de fichiers de sauvegarde pour les instances.
2. **Fichier de protection par mot de passe** : (facultatif) Sélectionnez l'option de protection par mot de passe pour chiffrer le fichier de sauvegarde. Le chiffrement du fichier de sauvegarde garantit la sécurité de toutes les informations sensibles contenues dans le fichier de sauvegarde.

### Remarque

Vous pouvez télécharger le fichier de sauvegarde chiffré sur votre ordinateur local, mais vous ne pouvez pas ouvrir le fichier avec l'interface graphique Citrix ADM ni avec un éditeur de texte. Le fichier peut être récupéré et utilisé par Citrix ADM seul. 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.

3. **Nombre de fichiers de sauvegarde à conserver** : spécifiez le nombre de fichiers de sauvegarde à conserver dans Citrix ADM. Vous pouvez conserver jusqu'à 50 fichiers de sauvegarde de l'état actuel d'une instance Citrix ADC. La valeur par défaut est trois fichiers de sauvegarde.

### Remarque

Chaque fichier de sauvegarde tient compte de certaines exigences en matière de stockage. Citrix vous recommande de stocker un nombre optimal de fichiers de sauvegarde Citrix ADC sur Citrix ADM en fonction de vos besoins.

### ← Configure Instance Backup Settings

Enable Instance Backups

Select password protect option to encrypt the backup file. This ensures that all the sensitive information inside backup file is secure.

Password Protect file

Password\*

Confirm Password\*

Number of Backup Files to retain\*

**Note:** Encrypted backup can be downloaded to your local machine but contents cannot be visible. Only MAS can use backup file for restore purpose. Restoring encrypted backup will prompt for password.

4. **Paramètres de planification des sauvegardes** : (facultatif) Deux options sont disponibles pour créer des fichiers de sauvegarde, mais vous ne pouvez utiliser qu'une seule option à la fois :

- a) L'option de planification de sauvegarde par défaut est « basée sur l'intervalle. » Un fichier de sauvegarde est créé dans Citrix ADM après l'expiration de l'intervalle spécifié. L'intervalle de sauvegarde par défaut est de 12 heures.
- b) Vous pouvez également modifier le type de sauvegardes planifiées en fonction du temps. Dans cette option, vous spécifiez l'heure au format « heures:minutes » à laquelle la sauvegarde doit avoir lieu. Citrix ADM permet à un maximum de quatre sauvegardes quotidiennes sur les instances.



**▼ Backup Scheduling Settings**

Scheduling Option

Interval Based  Time Based

Specify time for daily Backup (Maximum-limit: 4)

Add Time

00:00	×	
06:00	×	
12:00	×	
18:00	×	+

5. **Paramètres de Citrix ADC** : (facultatif) Par défaut, Citrix ADM ne crée pas de fichier de sauvegarde lorsqu'il reçoit l'interruption « NetScalerConfigSave ». Toutefois, vous pouvez activer l'option pour créer un fichier de sauvegarde chaque fois qu'une instance Citrix ADC envoie un piège « NetScalerConfigSave » à Citrix ADM. Une instance Citrix ADC envoie « NetScalerConfigSave » chaque fois que la configuration sur l'instance est enregistrée.
6. **Fichiers de géodatabase** : (facultatif) Par défaut, Citrix ADM ne sauvegarde pas les fichiers de géodatabase. Vous pouvez également activer l'option pour créer une sauvegarde de ces fichiers.

**▼ Citrix ADC Settings**

Do instance backup when NetScalerConfigSave trap is received

Include GeoDB Files

7. **Transfert externe** :(facultatif) Citrix ADM vous permet de transférer les fichiers de sauvegarde d'instance Citrix ADC vers un emplacement externe :
  - a) Spécifiez l'adresse IP de l'emplacement.

- b) Spécifiez le nom d'utilisateur et le mot de passe du serveur externe vers lequel vous souhaitez transférer les fichiers de sauvegarde.
- c) Spécifiez le protocole de transfert et le numéro de port.
- d) Vous pouvez spécifier le chemin du répertoire dans lequel le fichier doit être stocké.
- e) Vous avez également la possibilité de supprimer le fichier de sauvegarde de Citrix ADM après l'avoir transféré vers le serveur externe.

▼ External Transfer

Enable External Transfer

Server\*

192 . 10 . 10 . 1

User Name\*

davidT

Password\*

\*\*\*\*\*

Port\*

-1

Transfer Protocol

SCP     SFTP     FTP

Directory Path\*

/test/backups

Delete file from Application Delivery Management after transfer

**Remarque**

Citrix ADM envoie un piège SNMP ou une notification Syslog à lui-même en cas d'échec de sauvegarde pour l'une des instances Citrix ADC sélectionnées.

## Créer une sauvegarde pour une instance Citrix ADC sélectionnée à l'aide de Citrix ADM

Effectuez cette tâche si vous souhaitez sauvegarder une ou plusieurs instances Citrix ADC sélectionnées :

1. Dans Citrix ADM, accédez à **Réseaux > Instances**. Sous **Instances**, sélectionnez le type d'instances (Citrix VPX, par exemple) à afficher à l'écran.
2. Sélectionnez l'instance à sauvegarder.
  - Pour les instances MPX et VPX, 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 si vous souhaitez chiffrer votre fichier de sauvegarde pour plus de sécurité. Vous pouvez entrer votre mot de passe ou utiliser le mot de passe global que vous avez précédemment spécifié sur la page Paramètres de sauvegarde d'instance.
5. Cliquez sur **Continuer**.

## Restaurer une instance Citrix ADC à l'aide de Citrix ADM

Remarque :

Si vous avez des instances Citrix ADC dans une paire HA, vous devez prendre en compte les points suivants :

- Restaurer la même instance à partir de laquelle le fichier de sauvegarde a été créé. Par exemple, considérons un scénario selon lequel une sauvegarde a été effectuée à partir de l'instance principale de la paire HA. Au cours du processus de restauration, assurez-vous de restaurer la même instance, même si elle n'est plus l'instance principale.
- Lorsque vous lancez le processus de restauration sur l'instance ADC principale, vous ne pouvez pas accéder à l'instance principale et l'instance secondaire est remplacée par **STAYSECONDARY**. Une fois le processus de restauration terminé sur l'instance principale, l'instance ADC secondaire passe du mode **STAYSECONDARY** au mode **ENABLED** et fait à nouveau partie de la paire HA. Vous pouvez vous attendre à un temps d'arrêt possible sur l'instance principale jusqu'à ce que le processus de restauration soit terminé.

Effectuez cette tâche pour restaurer une instance Citrix ADC à l'aide du fichier de sauvegarde que vous avez créé précédemment :

1. Accédez à **Réseaux > Instances**, sélectionnez l'instance à restaurer, puis cliquez sur **Afficher la sauvegarde**.

2. Dans la page **Fichiers de sauvegarde**, sélectionnez le fichier de sauvegarde contenant les paramètres à restaurer, puis cliquez sur **Restaurer**.

The screenshot illustrates the process of restoring a Citrix ADC SDX appliance. It is divided into two main sections:

**Citrix ADC Dashboard:** This section shows a list of instances. The first instance, with IP address 10.102.29.60 and state 'Up', is selected. A context menu is open over this instance, with 'Backup/Restore' highlighted. Other actions in the menu include Show Events, Create Cluster, Reboot, Ping, TraceRoute, Rediscover, Unmanage, and Annotate.

IP Address	Host Name	Instance State
10.102.29.60	--	Up
10.102.29.200	--	Up
10.102.126.36	beta	Out of Service
10.102.166.4	10.102.166.4	Down

**Backup Files Page:** This section shows a list of backup files for the selected IP address (10.102.29.60). The files are listed with their names, last modified dates, and sizes.

Backup File	Last Modified	Size
backup_10.102.29.60_27Nov2018_01_35_14.tgz	Tue Nov 27 2018 7:05:27 AM	171.12 KB
backup_10.102.29.60_27Nov2018_13_35_14.tgz	Tue Nov 27 2018 7:05:29 PM	171.12 KB
backup_10.102.29.60_28Nov2018_01_35_15.tgz	Wed Nov 28 2018 7:05:28 AM	170.91 KB

## Restaurer une appliance Citrix ADC SDX à l'aide de Citrix ADM

Dans Citrix ADM, la sauvegarde de l'appliance Citrix ADC SDX comprend les éléments suivants :

- Instances Citrix ADC hébergées sur l'appliance
- Certificats et clés SSL SVM
- Paramètres d'élagage de l'instance (au format XML)
- Paramètres de sauvegarde de l'instance (au format XML)
- Paramètres du sondage sur les certificats SSL (au format XML)
- Fichier db SVM
- Fichiers de configuration Citrix ADC des appareils présents sur SDX
- Images de génération Citrix ADC
- Images Citrix ADC XVA, ces images sont stockées à l'emplacement suivant :  
`/var/mps/sdx_images/`
- Image d'ensemble SDX unique (SVM+XS)
- Images d'instances tierces (si provisionnées)

Vous devez restaurer votre appliance Citrix ADC SDX à la configuration disponible dans le fichier de sauvegarde. Pendant la restauration de la appliance, toute la configuration actuelle est supprimée.

Si vous restaurez l'appliance Citrix ADC SDX à l'aide d'une sauvegarde d'une autre appliance Citrix ADC SDX, assurez-vous d'ajouter les licences et de configurer les paramètres réseau du Service de

gestion de l'apppliance pour qu'ils correspondent à ceux du fichier de sauvegarde avant de démarrer le processus de restauration.

Assurez-vous que la variante de plate-forme Citrix ADC SDX sauvegardée est la même que celle sur laquelle vous tentez de restaurer. 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'apppliance SDX à partir du fichier sauvegardé :

1. Dans l'interface utilisateur graphique Citrix ADM, accédez à **Réseaux > Instances > Citrix ADC**.
2. Cliquez sur **Sauvegarde/Restaurer**.
3. Sélectionnez le fichier de sauvegarde de la même instance que vous souhaitez restaurer.
4. Cliquez sur **Reconditionner la sauvegarde**.

Lorsque l'apppliance 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'apppliance SDX.

Lorsque vous reconditionnez le fichier de sauvegarde, il inclut tous les fichiers sauvegardés ensemble pour restaurer l'apppliance SDX. Le fichier de sauvegarde reconditionné garantit la restauration réussie de l'apppliance SDX.

5. Sélectionnez le fichier de sauvegarde qui est réemballé et cliquez sur **Restaurer**.

## Forcer un basculement sur incident à l'instance secondaire Citrix ADC

February 1, 2024

Vous pouvez forcer un basculement si, par exemple, vous devez remplacer ou mettre à niveau l'instance principale Citrix Application Delivery Controller (ADC). Vous pouvez forcer le basculement à partir de l'instance principale ou secondaire. Lorsque vous forcez un basculement sur l'instance principale, la principale devient la secondaire et la secondaire devient la principale. Le basculement forcé n'est possible que lorsque l'instance principale peut déterminer que l'instance secondaire est active.

Un basculement forcé n'est ni propagé ni synchronisé. Pour consulter l'état de la synchronisation après un basculement forcé, vous pouvez consulter l'état de l'instance.

Un basculement forcé échoue dans l'une des circonstances suivantes :

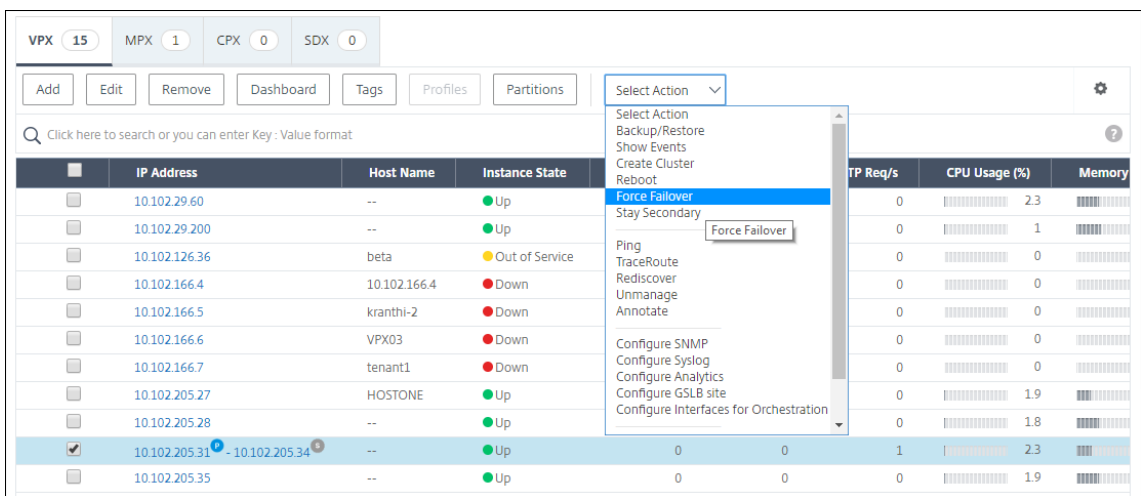
- Vous forcez le basculement sur un système autonome.
- L'instance secondaire est désactivée ou inactive. Si l'instance secondaire est inactive, vous devez attendre que son état soit activé pour forcer un basculement.
- L'instance secondaire est configurée pour rester secondaire.

L'instance Citrix ADC affiche un message d'avertissement si elle détecte un problème potentiel lorsque vous exécutez la commande force failover. Le message inclut les informations qui ont déclenché l'avertissement et demande une confirmation avant de continuer.

Vous pouvez forcer un basculement sur une instance principale ou secondaire.

**Pour forcer un basculement sur incident vers l'instance Citrix ADC secondaire à l'aide de Citrix ADM :**

1. Dans Citrix Application Delivery Management (ADM), accédez à l'onglet **Réseaux > Instances > Citrix ADC > VPX**, puis sélectionnez une instance.
2. Sélectionnez les instances d'une configuration HA à partir des instances répertoriées sous le type d'instance sélectionné.
3. Dans le menu **Action**, sélectionnez **Force Failover**.
4. Cliquez sur **Oui** pour confirmer l'action de basculement forcé.



**Forcer une instance Citrix ADC secondaire à rester secondaire**

February 1, 2024

Dans une configuration HA, le nœud secondaire peut être forcé de rester secondaire quel que soit l'état du nœud principal.

Par exemple, supposons que le nœud principal doit être mis à niveau et que le processus prend quelques secondes. Pendant la mise à niveau, le nœud principal peut s'arrêter pendant quelques secondes, mais vous ne voulez pas que le nœud secondaire prenne le relais ; vous voulez qu'il reste le nœud secondaire même s'il détecte une défaillance dans le nœud principal.

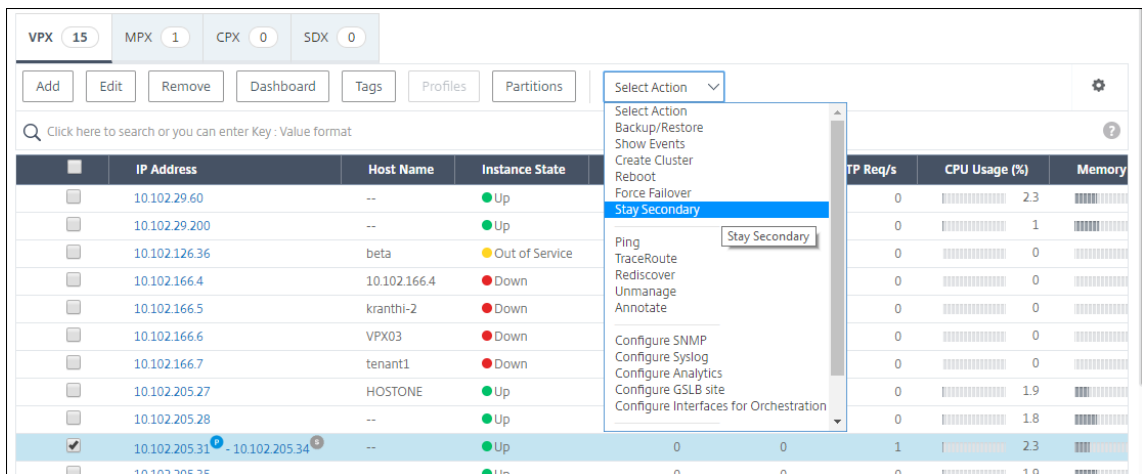
Lorsque vous forcez le nœud secondaire à rester secondaire, il le restera même si le nœud principal tombe en panne. En outre, lorsque vous forcez l'état d'un nœud dans une paire HA à rester secondaire, il ne participe pas aux transitions de machines d'état HA. L'état du nœud est affiché en tant que STAY-SECONDARY.

**Remarque**

Lorsque vous forcez un système à rester secondaire, le processus de forçage n'est ni propagé ni synchronisé. Elle affecte uniquement le nœud sur lequel vous exécutez la commande.

**Pour configurer une instance Citrix ADC secondaire pour qu'elle reste secondaire à l'aide de Citrix ADM :**

1. Dans Citrix Application Delivery Management (ADM), accédez à l'onglet **Réseaux > Instances > Citrix ADC > VPX**, puis sélectionnez une instance.
2. Sélectionnez les instances d'une configuration HA à partir des instances répertoriées sous le type d'instance sélectionné.
3. Dans le menu **Action**, sélectionnez **Rester secondaire**.
4. Cliquez sur **Oui** pour confirmer l'exécution de l'action « Rester secondaire ».



**Créer des groupes d'instances**

February 1, 2024

Pour créer un groupe d'instances, vous devez d'abord ajouter toutes vos instances Citrix Application Delivery Controller (ADC) à Citrix Application Delivery Management (ADM). Après avoir ajouté les instances avec succès, créez des groupes d'instances en fonction de leur famille d'appareils. En créant un groupe d'instances, vous pouvez effectuer simultanément des actions telles que la mise à niveau, la sauvegarde et la restauration sur toutes les instances qui ont été groupées, au lieu de les exécuter séparément sur chaque instance.

**Pour créer un groupe d'instances à l'aide de Citrix ADM :**

1. Dans Citrix ADM, accédez à **Réseaux > Groupes d'instances**, puis cliquez sur **Ajouter** .
2. Donnez un nom à votre groupe d'instances et sélectionnez la famille d'instances dans la liste.
3. Sélectionnez le type d'instance dans le menu **Famille** d'instances.
4. Cliquez sur **Sélectionner les instances** et sélectionnez les instances dans la fenêtre qui s'ouvre.
5. Cliquez sur **Créer**.

## Redécouvrir plusieurs instances Citrix VPX

February 1, 2024

Vous pouvez désormais redécouvrir plusieurs instances Citrix VPX dans votre configuration de Citrix Application Delivery Management (ADM). Auparavant, vous pouviez redécouvrir uniquement des instances Citrix VPX uniques. Vous pouvez redécouvrir plusieurs instances Citrix VPX lorsque vous souhaitez afficher les derniers états et configurations de ces instances. Le serveur Citrix ADM redécouvre toutes les instances Citrix VPX et vérifie si les instances de Citrix Application Delivery Controller (ADC) sont accessibles.

**Pour redécouvrir plusieurs instances Citrix VPX :**

1. Dans un navigateur Web, tapez l'adresse IP du serveur Citrix ADM (par exemple, <http://192.168.100.1>).
2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur. Les informations d'identification de l'administrateur par défaut sont nsroot et nsroot.
3. Accédez à **Réseaux > Instances > Citrix ADC** > onglet **VPX** et sélectionnez les instances que vous souhaitez redécouvrir.
4. Dans le menu **Sélectionner une action**, cliquez sur **Redécouvrir**.
5. Lorsque le message de confirmation de l'exécution de l'utilitaire Redécouvrir s'affiche, cliquez sur **Oui**.



L'écran signale la progression de la redécouverte de chacune des instances Citrix VPX.

## Annuler l'administration d'une instance

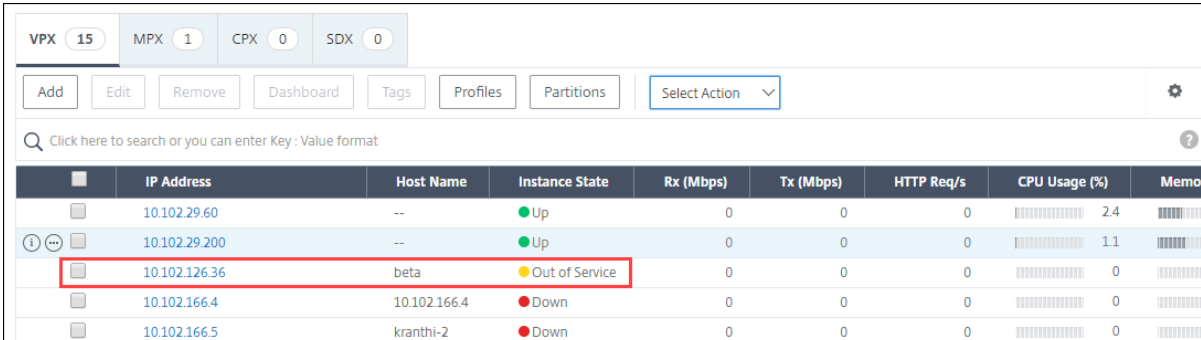
February 1, 2024

Si vous souhaitez arrêter l'échange d'informations entre Citrix Application Delivery Management (ADM) et les instances de votre réseau, vous pouvez annuler la gestion des instances.

### Pour annuler la gestion d'une instance :

Accédez à **Réseaux > Instances > Citrix ADC > onglet VPX**. Dans la liste des instances, cliquez avec le bouton droit sur une instance, puis sélectionnez **Ne pas gérer**, ou sélectionnez l'instance et, dans la liste **Sélectionner une action**, sélectionnez **Ne pas gérer**.

L'état de l'instance sélectionnée devient **Absence de service**, comme illustré dans la figure suivante.



	IP Address	Host Name	Instance State	Rx (Mbps)	Tx (Mbps)	HTTP Req/s	CPU Usage (%)	Memor
	10.102.29.60	--	Up	0	0	0	2.4	
	10.102.29.200	--	Up	0	0	0	1.1	
	10.102.126.36	beta	Out of Service	0	0	0	0	
	10.102.166.4	10.102.166.4	Down	0	0	0	0	
	10.102.166.5	kranthi-2	Down	0	0	0	0	

L'instance n'est plus gérée par Citrix ADM et n'échange plus de données avec Citrix ADM.

## Tracer la route jusqu'à une instance

February 1, 2024

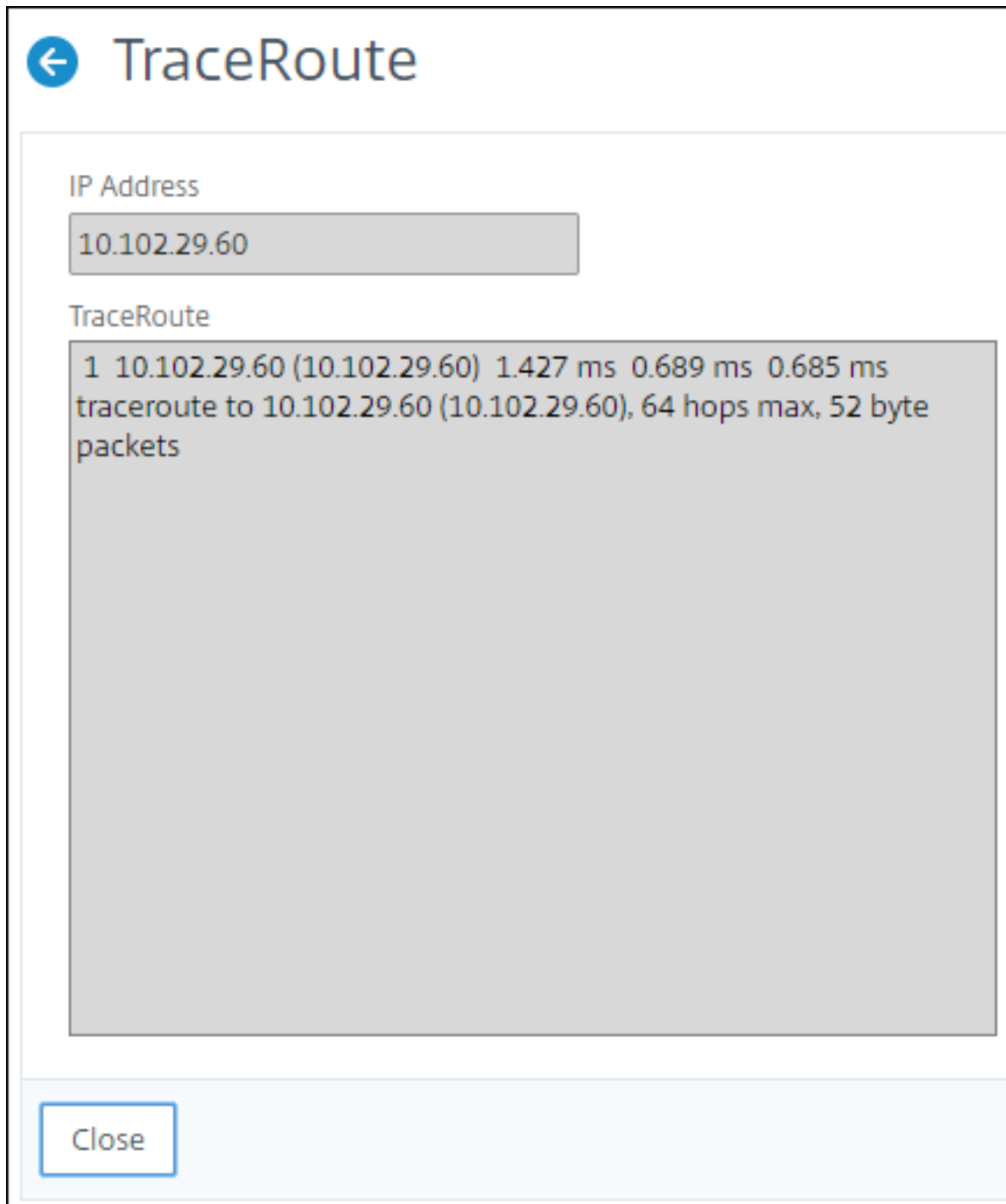
En traçant l'itinéraire d'un paquet de Citrix Application Delivery Management (ADM) à une instance, vous pouvez trouver des informations telles que le nombre de sauts nécessaires pour atteindre l'instance. Traceroute trace le chemin du paquet de la source à la destination. Il affiche la liste des sauts réseau ainsi que le nom d'hôte et l'adresse IP de chaque entité de la route.

Traceroute enregistre également le temps qu'un paquet prend pour voyager d'un saut à l'autre. En cas d'interruption du transfert de paquets, traceroute indique où se situe le problème.

### Pour tracer la route d'une instance :

1. Dans Citrix ADM, accédez à l'onglet **Réseaux > Instances > Citrix ADC > VPX**.
2. Dans la liste des instances, cliquez avec le bouton droit sur une instance, puis sélectionnez **TraceRoute** ou sélectionnez l'instance et, dans le menu **Sélectionner une action**, cliquez sur **TraceRoute**.

La boîte de message TraceRoute indique l'itinéraire vers l'instance et la durée, en millisecondes, consommée par chaque saut.



## Événements

February 1, 2024

Lorsque l'adresse IP d'une instance de Citrix Application Delivery Controller (ADC) est ajoutée à Citrix Application Delivery Management (ADM), Citrix ADM envoie un appel NITRO et s'ajoute implicitement comme destination d'interruption pour que l'instance reçoive ses interruptions ou événements.

Les événements représentent l'occurrence d'événements ou d'erreurs sur une instance Citrix ADC gérée. Par exemple, en cas de défaillance du système ou de modification de la configuration, un événement est généré et enregistré sur le serveur Citrix ADM. Les événements reçus dans Citrix ADM s'affichent sur la page Récapitulatif des événements (**Réseaux > Événements**) et tous les événements actifs sont affichés dans la page Messages d'événements (**Réseaux > Événements > Messages d'événements**).

Citrix ADM vérifie également les événements générés sur les instances pour former des alarmes de différents niveaux de gravité et les affiche sous forme de messages, dont certains peuvent nécessiter une attention immédiate. Par exemple, la défaillance du système pourrait être classée comme gravité de l'événement « critique » et devrait être corrigée immédiatement.

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 Citrix ADC.

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

Vous pouvez également vous assurer que plusieurs notifications sont déclenchées pour un intervalle de temps spécifique pour un événement jusqu'à ce que l'événement soit effacé. À titre de mesure supplémentaire, vous pouvez personnaliser votre e-mail avec une ligne d'objet spécifique, un message utilisateur et charger une pièce jointe.

## Utiliser le tableau de bord des événements

February 1, 2024

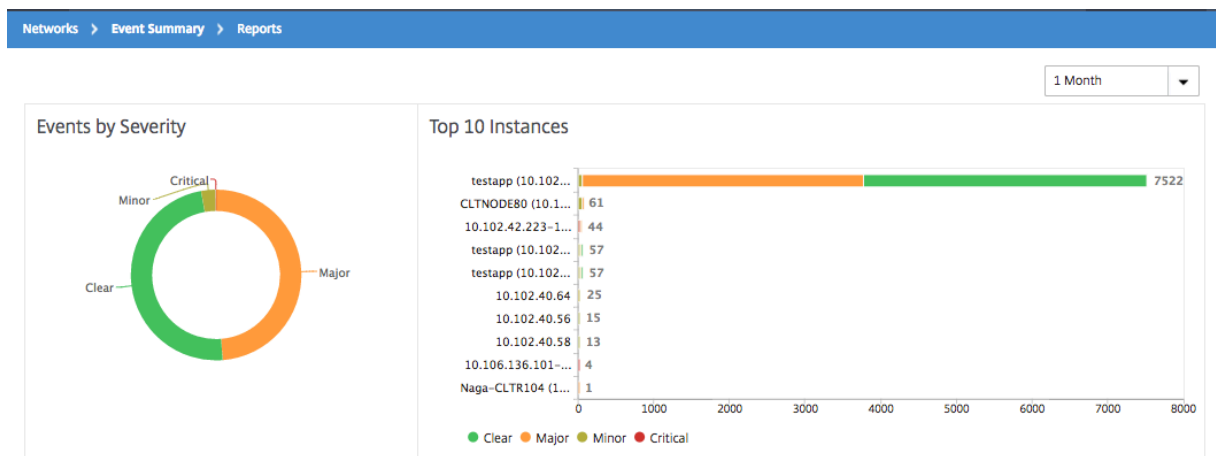
En tant qu'administrateur réseau, vous pouvez consulter des informations telles que les modifications de configuration, les conditions de connexion, les défaillances matérielles, les violations des seuils et les modifications de l'état des entités sur vos instances Citrix Application Delivery Controller (ADC),

ainsi que les événements et leur gravité sur des instances spécifiques. Vous pouvez utiliser le tableau de bord des événements de Citrix Application Delivery Management (ADM) pour consulter les rapports générés contenant des informations détaillées sur la gravité des événements critiques sur toutes vos instances Citrix ADC.

**Pour afficher les détails sur le tableau de bord des événements :**

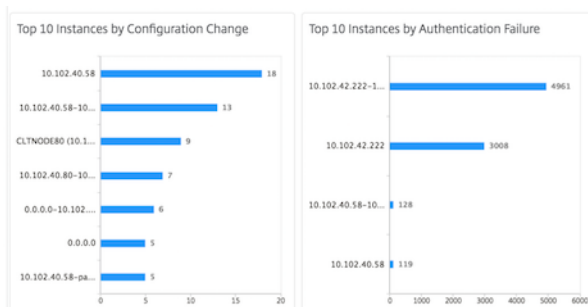
Accédez à **Réseaux > Événements > Rapports.**

Le graphique 10 principaux périphériques du tableau de bord affiche un rapport des 10 instances les plus importantes selon le nombre d'événements générés sur elles. Vous pouvez cliquer sur une instance dans le graphique pour voir plus de détails sur la gravité de l'événement.

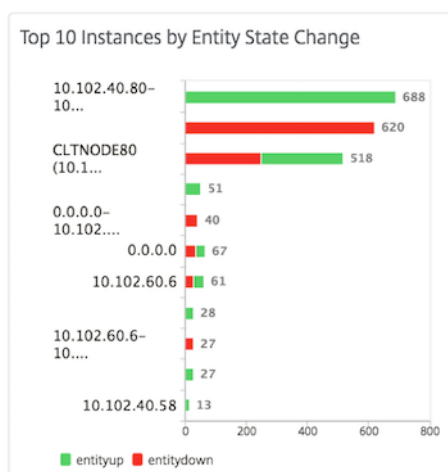


Vous pouvez afficher plus de détails en accédant au type d'instance Citrix ADC (**Réseaux > Événements > RapportsNetScaler/ NetScaler SDX/ NetScaler SD-WAN WO**) pour afficher les informations suivantes :

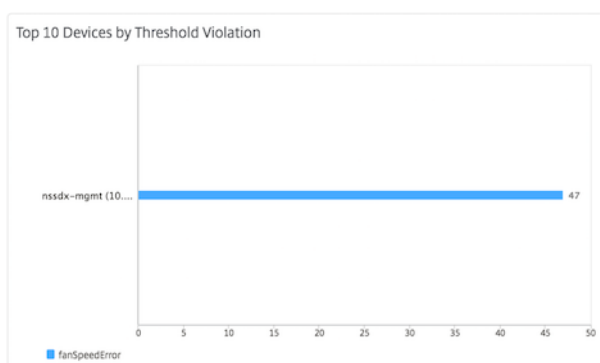
- Top 10 des périphériques par défaillance matérielle
- Les 10 principaux appareils par changement de configuration
- Top 10 des appareils par échec d'authentification



- 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). Citrix ADM surveille les appliances jusqu'à la durée définie et génère un événement uniquement si l'âge de l'événement dépasse la durée définie.

Remarque :

La valeur minimale de l'âge de l'événement est de 60 secondes. Si vous gardez le champ **Âge de l'événement** vide, la règle d'événement est appliquée immédiatement après l'événement.

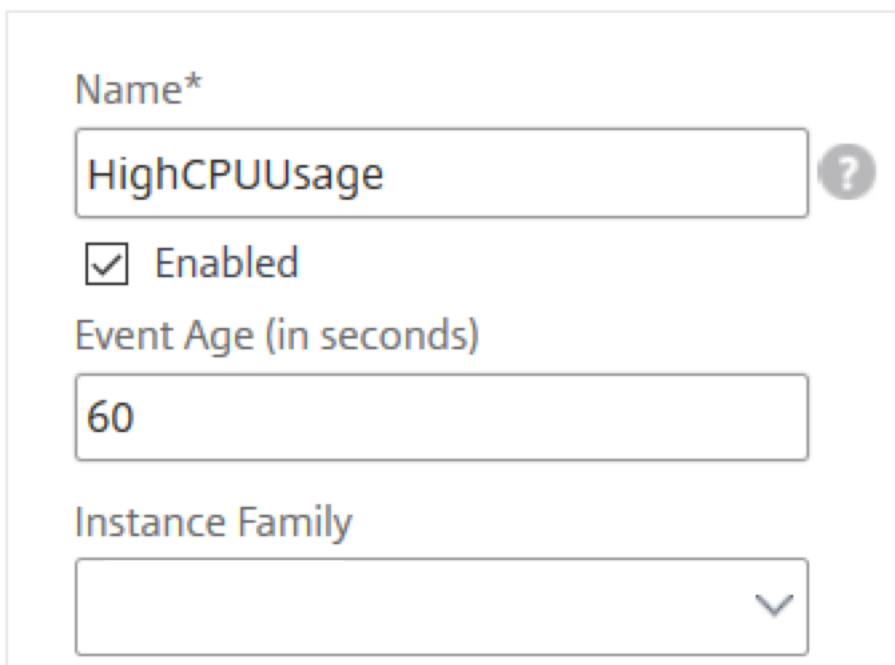
Par exemple, imaginez que vous souhaitez gérer différentes appliances ADC et recevoir une notification par e-mail lorsque l'un de vos serveurs virtuels tombe en panne pendant 60 secondes ou plus. Vous pouvez créer une règle d'événement avec les filtres nécessaires et définir l'âge d'événement de

la règle sur 60 secondes. Ensuite, chaque fois qu'un serveur virtuel reste en panne pendant 60 secondes ou plus, vous recevrez une notification par e-mail avec des détails tels que le nom de l'entité, le changement d'état et l'heure.

**Pour définir l'âge des événements dans Citrix ADM :**

1. Dans Citrix ADM, accédez à **Réseaux > Événements > Règles**, puis cliquez sur **Ajouter**.
2. Dans la page **Créer une règle**, définissez les paramètres de la règle.
3. Spécifiez l'âge de l'événement en secondes.

## Create Rule



Name\*

HighCPUUsage

Enabled

Event Age (in seconds)

60

Instance Family

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 ci-dessus, sélectionnez les interruptions entityup, entitydown et entityofs.

## Planifier un filtre d'événement

February 1, 2024

Après avoir créé un filtre pour votre règle, si vous ne souhaitez pas que le serveur ADM (Citrix Application Delivery Management) envoie une notification chaque fois que l'événement généré satisfait aux

critères de filtre, vous pouvez programmer le filtre pour qu'il se déclenche uniquement à des intervalles de temps spécifiques, tels que quotidiens, hebdomadaires ou mensuels.

Par exemple, si vous avez planifié une activité de maintenance système pour différentes applications sur vos instances à des moments différents, les instances peuvent générer plusieurs alarmes.

Si vous avez configuré un filtre pour ces alarmes et activé les notifications par e-mail pour ces filtres, le serveur envoie un grand nombre de notifications par e-mail lorsque Citrix ADM reçoit ces interruptions. Si vous souhaitez que le serveur envoie ces notifications par e-mail uniquement pendant une période spécifique, vous pouvez le faire en planifiant un filtre.

#### **Pour planifier un filtre à l'aide de Citrix ADM :**

1. Dans Citrix ADM, accédez à **Réseaux > Événements > Règles** .
2. Sélectionnez la règle pour laquelle vous souhaitez planifier un filtre, puis cliquez sur **Afficher la planification**.
3. Dans la page **Règle programmée**, cliquez sur **Planifier** et spécifiez les paramètres suivants :
  - **Activer la règle** : cochez cette case 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)** : heure (s) à laquelle planifier la règle (utilisez le format 24 heures).
4. Cliquez sur **Planifier**.

## ← Schedule Rule

You can enable or disable the event rule and schedule them.

Enable Rule [?](#)

Recurrence\*

Specific day(s) of the week ▼

**NOTE:** Enter the schedule time interval in your local timezone

Days

Sun	Mon	Tue	Wed	Thu	Fri	Sat
-----	-----	-----	-----	-----	-----	-----

Scheduled Time Interval (Hours)

16-17

[Schedule](#) [Close](#)

## Définir des notifications par e-mail répétées pour les événements

February 1, 2024

Pour vous assurer que tous les événements critiques sont traités et qu'aucune notification par e-mail importante n'est manquée, vous pouvez choisir d'envoyer des notifications par e-mail répétées pour les règles d'événements qui répondent aux critères que vous avez sélectionnés. Par exemple, si vous avez créé une règle d'événement pour les instances qui impliquent des défaillances de disque et que vous souhaitez être averti jusqu'à ce que le problème soit résolu, vous pouvez choisir de recevoir des notifications par e-mail répétées sur ces événements.

Ces notifications par e-mail sont envoyées à plusieurs reprises, à des intervalles prédéfinis, jusqu'à ce que le destinataire reconnaisse avoir vu la notification ou que la règle d'événement soit effacée.

### Remarque

Les événements ne peuvent être effacés automatiquement que si un piège « clair » équivalent est défini et envoyé depuis votre instance Citrix Application Delivery Controller (ADC).

Pour effacer manuellement un événement, vous pouvez effectuer les opérations suivantes :

- Accédez à **Réseaux > Événements > Récapitulatif** des événements, choisissez une **catégorie** et sélectionnez un événement dans la catégorie, puis cliquez sur **Effacer**.
- Vous pouvez également accéder à **Réseaux > Événements > Messages d'événements**.



Choisissez un type d'instance, puis sélectionnez un événement dans la grille ci-dessous et cliquez sur **Effacer**.

**Pour définir des notifications par e-mail répétées à partir de Citrix ADM :**

1. Dans Citrix Application Delivery Management (ADM), accédez à **Réseaux > Événements > Règles**, puis cliquez sur **Ajouter** pour créer une règle.
2. Dans la page **Créer une règle**, définissez les paramètres de la règle.
3. Sous Actions relatives aux **règles d'événement**, cliquez sur **Ajouter une action**. Sélectionnez ensuite **Envoyer une action par e-mail** dans la liste déroulante **Type d'action** et sélectionnez une liste de **distribution par e-mail**.
4. Vous pouvez également ajouter une ligne d'objet personnalisée et un message utilisateur, et télécharger une pièce jointe à votre e-mail lorsqu'un événement entrant correspond à la règle configurée.
5. Activez la case à cocher **Répéter la notification par e-mail jusqu'à ce que l'événement soit désactivée**.

### Add Event Action

Action Type\*

Email Distribution List\*  
 Add Edit Test

Email Subject  
 ?

Prefix severity, category, and failure object information to the custom email subject ?

Attachment  
 Upload

Message

Repeat Email Notification until the event is cleared ?

Time Interval (minutes)\*

OK Close

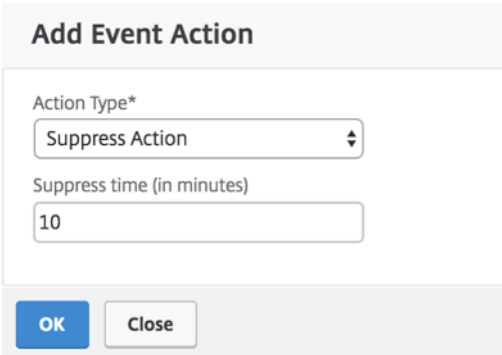
## Suppression d'événements

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.

**Pour supprimer des événements à l'aide de Citrix ADM :**

1. Dans Citrix Application Delivery Management (ADM), accédez à **Réseaux > Événements > Règles**. Cliquez sur **Ajouter**.
2. Spécifiez tous les paramètres requis pour créer une règle.
3. Sous **Actions de règle d'événement**, cliquez sur **Ajouter une action** pour affecter des actions de notification à l'événement.
4. Dans la page **Ajouter une action d'événement**, sélectionnez **Supprimer une action** dans le menu déroulant **Type d'action** et spécifiez la période, en minutes, pour laquelle un événement doit être supprimé.
5. Cliquez sur **OK**.



**Add Event Action**

Action Type\*

Suppress Action

Suppress time (in minutes)

10

OK Close

## Créer des règles d'événement

February 1, 2024

24 mai 2018

Vous pouvez configurer des règles pour surveiller des événements spécifiques. Les règles facilitent la surveillance d'un grand nombre d'événements générés sur votre infrastructure Citrix Application Delivery Controller (ADC).

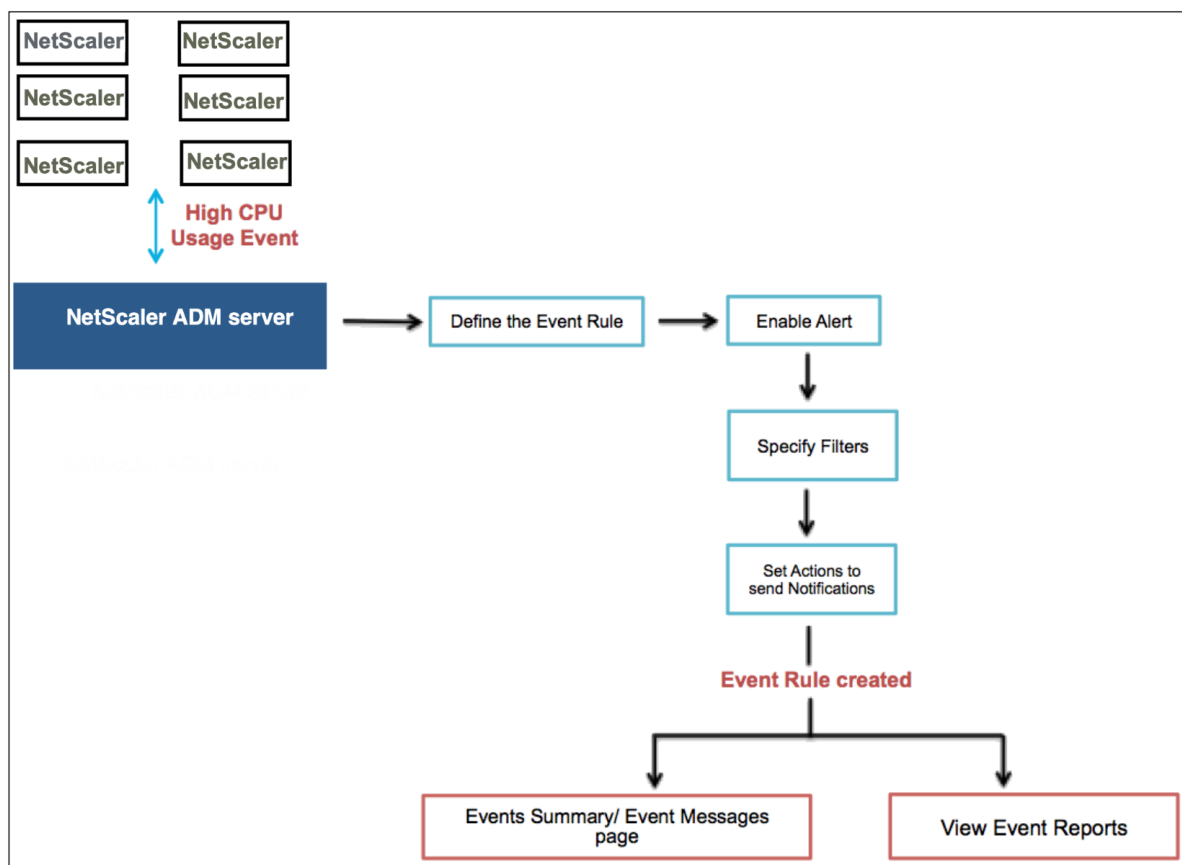
Vous pouvez filtrer un ensemble d'événements en configurant des règles avec des conditions spécifiques et en affectant des actions aux règles. Lorsque les événements générés répondent aux critères de filtre de la règle, l'action associée à la règle est exécutée. Les conditions pour lesquelles vous pouvez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

Vous pouvez 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
- **Action** d'envoi de SMS : envoyez un message SMS pour chaque événement correspondant aux critères du filtre.
- **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.

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/ou une pièce jointe.



Par exemple, en tant qu'administrateur, vous pouvez surveiller les événements « utilisation élevée de l'UC » pour des instances Citrix ADC spécifiques si ces événements peuvent entraîner une panne de vos instances Citrix ADC. Vous pouvez créer une règle pour surveiller les instances et spécifier une action qui vous enverra une notification par e-mail lorsqu'un événement de la catégorie « utilisation élevée

du processeur » se produit. Vous pouvez programmer l'exécution de la règle à une heure précise, par exemple entre 11 h et 23 h, afin de ne pas être averti chaque fois qu'un événement est généré.

La configuration d'une règle d'événement implique les tâches suivantes :

1. Définissez la règle
2. Choisissez la gravité de l'événement détecté par la règle
3. Spécifiez la catégorie de l'événement
4. Spécifier les instances Citrix ADC auxquelles la règle s'applique
5. Spécifier les objets de défaillance
6. Spécifier des filtres supplémentaires
7. Spécifier les actions à effectuer lorsque la règle détecte un événement

## Étape 1 - Définir une règle d'événement

Accédez à **Réseaux > Événements > Règles**, puis cliquez sur **Ajouter** . Si vous souhaitez activer votre règle, cochez la case **Activer la règle** .

Vous pouvez définir l'option **Event Age** pour spécifier l'intervalle de temps (en secondes) après lequel Citrix Application Delivery Management (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 souhaitez peut-être être averti par e-mail chaque fois que votre instance Citrix ADC présente un événement « utilisation élevée du processeur » pendant une période de 60 secondes ou plus. Vous pouvez définir l'âge de l'événement à 60 secondes, de sorte que chaque fois que votre instance Citrix ADC présente un événement « utilisation élevée du processeur » pendant 60 secondes ou plus, vous receviez une notification par e-mail contenant les détails de l'événement.

# ← Create Rule

Name\*

HighCPUUsage ?

Enabled

Event Age (in seconds)

60

Instance Family

▼

Vous pouvez également filtrer les règles d'événement par **famille de périphériques** pour suivre l'instance de Citrix ADC à partir de laquelle Citrix ADM reçoit un événement.

## 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.

▼ Severity

If none selected, all severity values will be considered

Available (4)		Configured (2)	
Minor	+	Major	-
Warning	+	Critical	-
Clear	+		
Information	+		

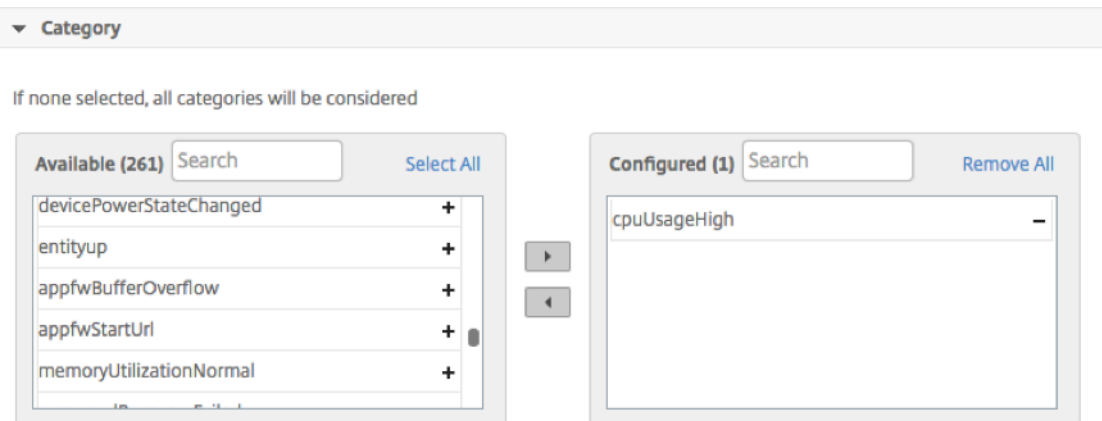
**Remarque**

Vous pouvez configurer la gravité des événements génériques et spécifiques à l'entreprise. Pour modifier la gravité des événements pour les instances Citrix ADC gérées sur Citrix ADM, accédez à **Réseaux > Événements > Paramètres des événements**. Choisissez la **catégorie** pour laquelle vous souhaitez configurer la gravité de l'événement, puis cliquez sur **Configurer la gravité**. Attribuez un nouveau niveau de gravité et cliquez sur **OK**.

**Étape 3 - Spécifier la catégorie d'événement**

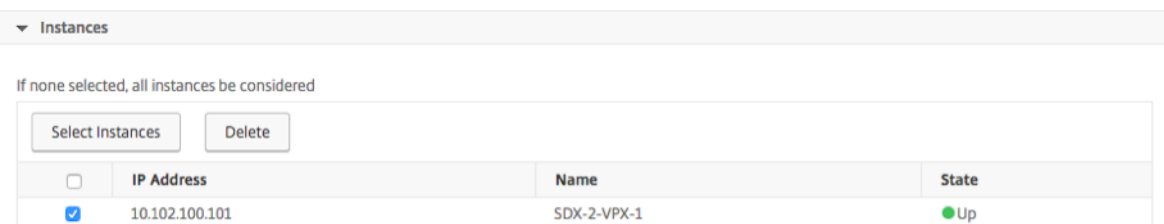
Vous pouvez spécifier la ou les catégories des événements générés par vos instances Citrix ADC. Toutes les catégories sont créées sur des instances Citrix ADC. Ces catégories sont ensuite mappées avec Citrix ADM qui peut être utilisé pour définir des règles d'événements. Sélectionnez la catégorie à prendre en compte et déplacez-la de la table **Disponible** vers la table **configurée**.

Dans l'exemple ci-dessus, vous devrez choisir « CPUUsageHigh » comme catégorie d'événement dans le tableau affiché.



**Étape 4 - Spécifier les instances de Citrix ADC**

Sélectionnez les adresses IP des instances Citrix ADC pour lesquelles vous souhaitez définir la règle d'événement. Dans la section **Instances**, cliquez sur **Sélectionner des instances**. Dans la page **Sélectionner des instances**, choisissez vos instances, puis cliquez sur **Sélectionner**.



## Étape 5 - Sélectionner les objets de défaillance

Vous pouvez sélectionner un objet d'échec dans la liste déroulante fournie ou ajouter un objet d'échec pour lequel un événement a été généré. Les objets d'échec sont des instances d'entité ou des compteurs pour lesquels un événement a été généré.

L'objet Failure affecte la façon dont un événement est traité et garantit que l'objet Failure reflète le problème exact tel qu'il a été notifié. Cela peut être utilisé pour détecter rapidement les problèmes et identifier la raison de l'échec, au lieu de simplement signaler les événements bruts. Par exemple, si un utilisateur rencontre des problèmes de connexion, l'objet de l'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.

▼ Failure Objects

If none selected, all failure objects will be considered

Select Failure Objects Delete

Add Failure Objects

	Name
<input type="checkbox"/>	[blurred]

## Étape 6 - Spécifier des filtres supplémentaires

Vous pouvez filtrer davantage une règle d'événement en :

- **Commandes de configuration** : vous pouvez spécifier la commande de configuration complète ou spécifier le modèle de description dans un astérisque (\*) pour filtrer les événements. Outre la commande, vous pouvez choisir de filtrer davantage la règle d'événement en fonction de l'état d'authentification de la commande et/ou de son statut d'exécution. Par exemple, pour un événement NetScalerConfigChange, tapez \*bind system global policy\_name\*.



▼ Advance Filters

Filter By

Specify the complete configuration command, or specify the description pattern within asterisk(\*) to filter the events. For example, for a NetscalerConfigChange event, type \*bind system global policy\_name\*.

Configuration Command

Command Authentication Status

Command Execution Status

- **Messages** - Vous pouvez spécifier la description complète du message ou spécifier le modèle de description dans un astérisque (\*) pour filtrer les événements. Par exemple, pour un événement NetScalerConfigChange, tapez \*ns\_client\_ipaddress:10.102.126.250\*.

▼ Advance Filters

Filter By

Specify the complete message description, or specify the description pattern within asterisk(\*) to filter the events. For example, for a NetscalerConfigChange event, type \*ns\_client\_ipaddress :10.102.126.250\*.

Message

## 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 une action e-mail
- Envoyer une action de piège
- Envoyer une action par SMS
- Exécuter l'action de commande
- Exécuter une action de travail
- Supprimer l'action

**Pour définir l'action relative à la règle relative aux événements de messagerie électronique :**

Lorsque vous choisissez le type d'action d'événement Envoyer une action e-mail, un message électronique est déclenché lorsque les événements répondent aux critères de filtre définis. Vous devrez soit créer une liste de distribution d'e-mails en fournissant les détails du serveur de messagerie ou du profil de messagerie, soit sélectionner une liste de distribution d'e-mails que vous avez créée précédemment.

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.

Grâce à cette option, vous pouvez également vous assurer que tous les événements critiques sont traités et qu'aucune notification importante par e-mail n'est oubliée, en cochant la case **Répéter la notification par e-mail jusqu'à ce que l'événement soit** désactivé pour envoyer des notifications par e-mail répétées pour les règles relatives aux 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.

## Add Event Action

Action Type\*

Send e-mail Action

Email Distribution List\*

Critical Event

Subject

Critical Event -Disk Failures

Repeat Email Notification until the event is cleared

Time Interval (minutes)\*

5

Attachment

Choose File

Upload

Message

Ensure that disk failure issues are resolved.

OK

Close

**Pour définir l'action de la règle Trap Event :**

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 d'interruptions (ou les détails d'une destination d'interruptions et d'un profil d'interruptions), les messages d'interruptions sont envoyés à un auditeur d'interruptions spécifiques lorsque les événements répondent aux critères de filtre définis.

**Pour définir l'action de la règle relative aux événements SMS :**

Lorsque vous choisissez le type **d'action d'événement Envoyer** une action par SMS, un message SMS (**Short Message Service**) pour chaque événement qui correspond aux critères du filtre. Vous devrez soit créer une liste de distribution de SMS en fournissant les détails du serveur SMS ou du profil SMS, soit sélectionner une liste de distribution de SMS que vous avez créée précédemment.

**Pour définir l'action Exécuter la commande :**

Lorsque vous choisissez l'**action d'événement Exécuter l'action de commande**, vous pouvez créer une commande ou un script qui peut être exécuté sur Citrix ADM pour les événements correspondant à un critère de filtre particulier. Par exemple, si un événement de gravité « critique » est déclenché lors d'un changement de configuration sur une instance gérée, vous pouvez exécuter un script de commande.

Vous pouvez également définir les paramètres suivants pour le script **Run Command Action** :

---

Paramètre	Description
\$source	Ce paramètre correspond à l'adresse IP source de l'événement reçu.
Catégorie \$	Ce paramètre correspond au type de pièges défini dans la catégorie du filtre
\$entité	Ce paramètre correspond aux instances ou aux compteurs d'entités pour lesquels un événement a été généré. Il peut inclure les noms de compteur pour tous les événements liés aux seuils, les noms d'entités pour tous les événements liés aux entités et les noms de certificats pour tous les événements liés aux certificats.
\$severity	Ce paramètre correspond à la gravité de l'événement.

\$failureobj

L'objet Failure affecte la façon dont un événement est traité et garantit que l'objet Failure reflète le problème exact tel qu'il a été notifié. Cela peut être utilisé pour détecter rapidement les problèmes et identifier la raison de l'échec, au lieu de simplement signaler les événements bruts.

#### Remarque

Pendant l'exécution de la commande, ces paramètres seront remplacés par des valeurs réelles.

#### Pour configurer l'action événementielle « Exécuter l'action de commande » sur Citrix ADM :

1. Sous **Actions relatives aux règles d'événement**, cliquez sur **Ajouter une action** et sélectionnez Exécuter une **action de commande** dans la liste déroulante **Type** d'action.
2. Sur la page **Créer une liste de distribution** de commandes, indiquez un nom de profil et la commande à exécuter. Cette commande sera exécutée lorsque les événements répondront aux critères de filtre définis.

Add Event Action > Create Command Distribution List

### Create Command Distribution List

Profile Name

Run Command\*

 ⓘ

Append Output

Append Errors

OK Close

#### Remarque

Vous pouvez activer les options **Ajout de sortie** et **Ajout d'erreurs** si vous souhaitez stocker la sortie et les erreurs générées (le cas échéant) lorsque vous exécutez un script de commande dans les fichiers journaux du serveur Citrix ADM. Si vous n'activez pas ces

options, Citrix ADM ignorera toutes les sorties et erreurs générées lors de l'exécution du script de commande.

### Pour définir l'action Exécuter la tâche, procédez comme suit :

En créant un profil avec des tâches de configuration, une tâche est exécutée en tant que tâche intégrée ou personnalisée pour les instances Citrix ADC, Citrix SDX et Citrix SD-WAN WO, pour les événements et les alarmes correspondant aux critères de filtre que vous avez spécifiés.

1. Sous **Actions relatives aux règles d'événement**, cliquez sur **Ajouter une action** et sélectionnez **Exécuter l'action de tâche** dans le menu **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.

**Create Job**

Select Job | Specify Variable Values

Profile Name\*  
Test

Instance Type\*  
Citrix ADC

Configuration Template Name\*  
DeployMasterConfiguration

On Command Failure\*  
Ignore error and continue

Cancel | Next →

### Pour définir l'action de suppression :

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.

### Add Event Action

Action Type\*

Suppress Action

Suppress time (in minutes)

10

**OK** Close

Votre règle d'événement est maintenant créée avec des filtres appropriés et des actions de règle d'événement bien définies.

## Modifier la gravité signalée des événements qui se produisent sur les instances Citrix ADC

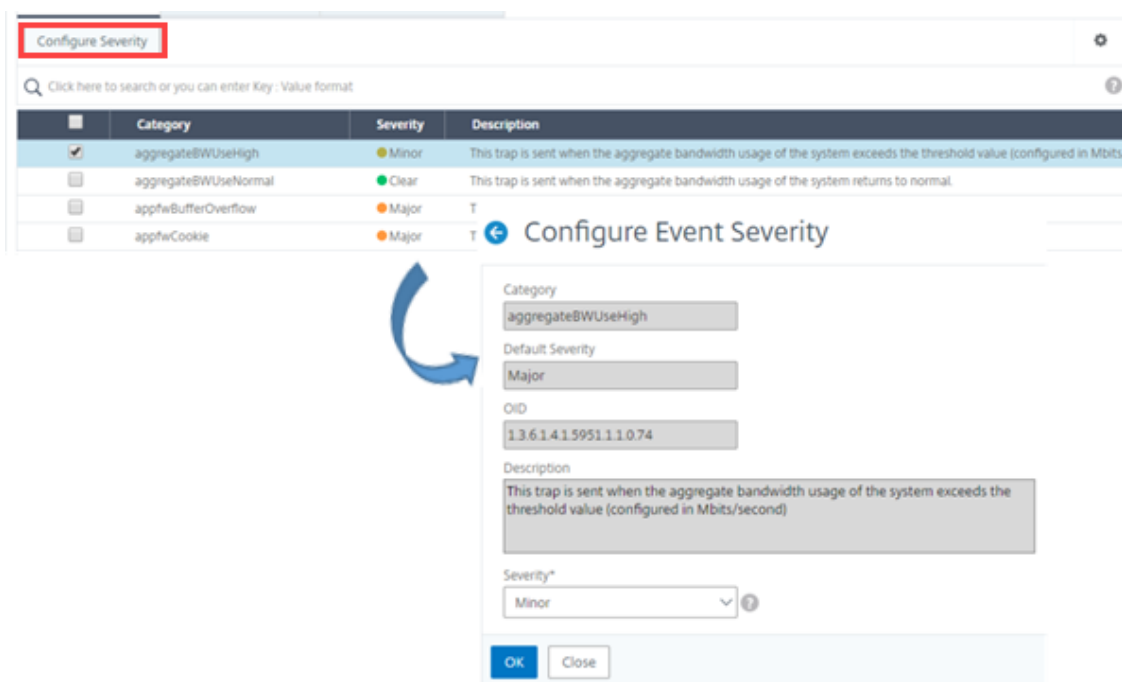
February 1, 2024

Vous pouvez gérer les rapports d'événements générés sur tous vos appareils, de sorte que vous pouvez afficher les détails d'événements concernant un événement particulier sur une instance particulière et afficher les rapports en fonction de la gravité de l'événement. Vous pouvez créer des règles d'événement qui utilisent les paramètres de gravité par défaut, et vous pouvez modifier les paramètres de gravité. Vous pouvez configurer la gravité des événements génériques et spécifiques à l'entreprise.

Vous pouvez définir les niveaux de gravité suivants : Critique, Majeur, Mineur, Avertissement et Clair.

### Pour modifier la gravité de l'événement :

1. Accédez à **Réseaux > Événements > Paramètres d'événement**.
2. Cliquez sur l'onglet correspondant au type d'instance de Citrix Application Delivery Controller (ADC) que vous souhaitez modifier. Sélectionnez ensuite la catégorie dans la liste et cliquez sur **Configurer la gravité**.
3. Dans **Configurer la gravité de l'événement**, sélectionnez le niveau de gravité dans la liste déroulante.
4. Cliquez sur **OK**.



## Afficher le résumé des événements

February 1, 2024

Vous pouvez désormais afficher une page Récapitulatif des événements pour surveiller les événements et les interruptions reçus sur votre serveur ADM (Application Delivery Management) Citrix. Accédez à **Réseaux > Événements**. La page Récapitulatif des événements affiche les informations suivantes sous forme de tableau :

- **Résumé de tous les événements reçus par Citrix ADM.** Les événements sont répertoriés par catégorie et les différentes sévérité sont affichées dans différentes colonnes : Critique, Majeur, Mineur, Avertissement, Effacer et Informations. Par exemple, un événement critique se produit lorsqu'une instance de Citrix Application Delivery Controller (ADC) s'arrête et arrête d'envoyer des informations au serveur Citrix ADM. Pendant l'événement, une notification est envoyée à un administrateur, expliquant la raison pour laquelle l'instance est en panne, le temps pendant lequel elle était en panne, 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.



Event Summary 🔄 📄

Critical	Major	Minor	Warning	Clear	Information	
1	20	6	0	3	0	
Category	Critical	Major	Minor	Warning	Clear	Information
coldstart	0	2	0	0	0	0
entitydown	0	6	0	0	0	0
entityup	0	0	0	0	3	0
HABadSecState	1	0	0	0	0	0
netScalerLoginFailure	0	2	0	0	0	0
warmRestartEvent	0	1	0	0	0	0
netScalerConfigChange	0	0	3	0	0	0
ipConflict	0	6	0	0	0	0
snmpAuthentication	0	2	0	0	0	0
changeToPrimary	0	1	0	0	0	0
netScalerConfigSave	0	0	3	0	0	0

- **Nombre de pièges reçus pour chaque catégorie.** Nombre de pièges reçus, classés par gravité. Par défaut, chaque interruption envoyée à partir d’instances Citrix ADC à Citrix ADM a une gravité attribuée, mais en tant qu’administrateur réseau, vous pouvez spécifier sa gravité dans l’interface graphique Citrix ADM.

Si vous cliquez sur un type de catégorie ou une interruption, vous accédez à la page **Événements**, sur laquelle les filtres tels que Catégorie et Gravité sont présélectionnés. Cette page affiche plus d’informations sur l’événement, telles que l’adresse IP et le nom d’hôte de l’instance Citrix ADC, la date à laquelle l’interruption a été reçue, la catégorie, les objets d’échec, l’exécution de la commande de configuration et la notification de message.

Events 🔄 📄

Details History Delete Clear ⚙️

🔍 Category: coldstart Click here to search or you can enter Key: Value format ?

	Severity	Source	Host Name	Date	Category	Failure Objects	Configuration Command	Message
<input type="checkbox"/>	Major	10.102.71.220	abcd	Nov 25 2018 21:03:12	coldstart	10.102.71.220		enterprise_...
<input type="checkbox"/>	Major	10.102.186.95	DataCenter-CB	Oct 27 2018 05:14:13	coldstart	10.102.186.95		enterprise_...

## Afficher les sévérité des événements et les détails des interruptions SNMP

February 1, 2024

Lorsque vous créez un événement et ses paramètres dans Citrix Application Delivery Management (ADM), vous pouvez afficher l’événement immédiatement sur la page Récapitulatif des événements. De même, vous pouvez afficher et surveiller l’intégrité, le temps de fonctionnement, les modèles et les versions de toutes les instances de Citrix Application Delivery Controller (ADC) ajoutées à votre

serveur Citrix ADM en détail dans le tableau de bord de l'infrastructure.

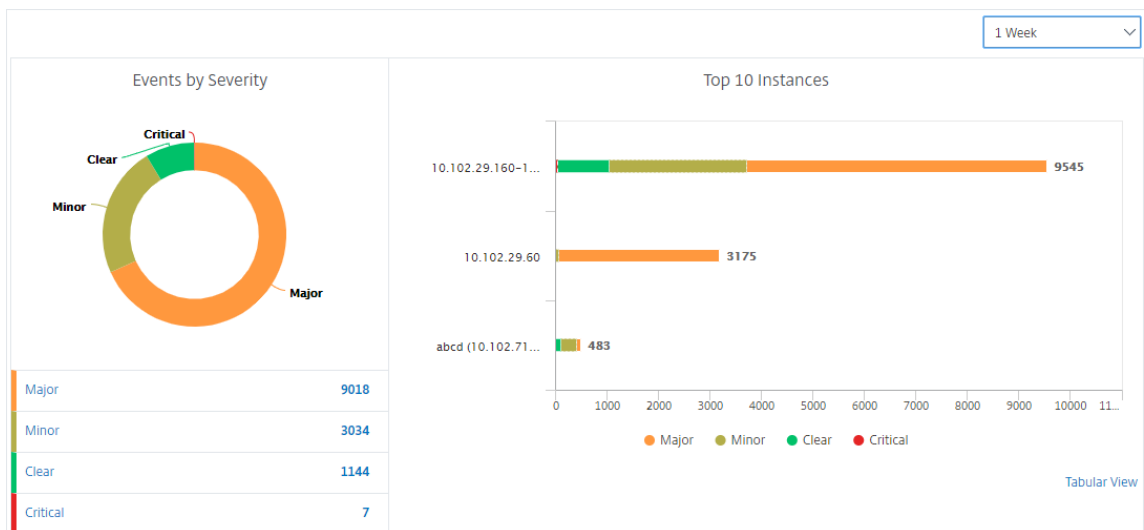
Dans le tableau de bord Infrastructure, vous pouvez désormais masquer les valeurs non pertinentes afin de pouvoir afficher et surveiller plus facilement les informations telles que les événements par gravité, intégrité, temps de fonctionnement, modèles et version des instances Citrix ADC en détail.

Par exemple, les événements présentant un niveau de gravité **critique** peuvent se produire rarement. Toutefois, lorsque ces événements critiques se produisent sur votre réseau, vous souhaitez 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 que vous avez sélectionnée : la source de l'instance, la date, la catégorie et la notification de message envoyée lorsque l'événement critique s'est produit.

De même, vous pouvez afficher l'intégrité d'une instance Citrix VPX sur le tableau de bord. Vous pouvez masquer le temps pendant lequel l'instance était en cours d'exécution et afficher uniquement les heures où elle était hors service. En cliquant sur le graphique, vous accédez à la page de cette instance, où le filtre *hors service* est déjà appliqué, et voyez des détails tels que le nom d'hôte, le nombre de requêtes HTTP reçues par seconde, l'utilisation du processeur, etc. Vous pouvez également sélectionner l'instance et voir le tableau de bord de cette instance Citrix particulière pour plus de détails

**Pour sélectionner des événements spécifiques par gravité dans Citrix ADM :**

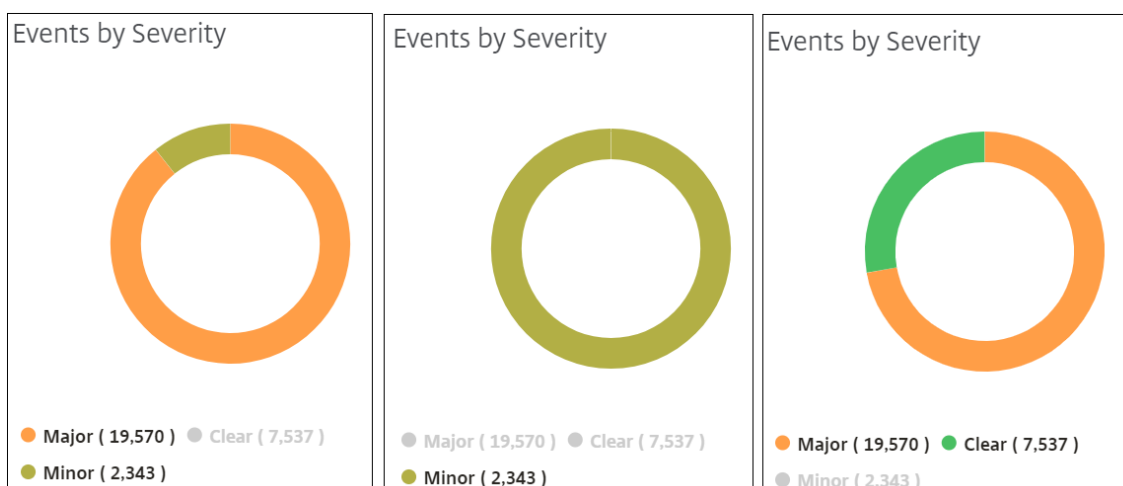
1. Connectez-vous à Citrix ADM à l'aide de vos informations d'identification d'administrateur.
2. Accédez à **Réseaux > Tableau de bord**  
Ou  
Accédez à **Réseaux > Événements > Rapports**.
3. Dans le menu situé dans le coin supérieur droit de la page, sélectionnez la durée pour laquelle vous souhaitez afficher les événements par gravité.



4. Le graphique **Événements par gravité** affiche une représentation visuelle de tous les événements par gravité. Différents types d'événements sont représentés sous forme de sections colorées différentes, et la longueur de chaque section correspond au nombre total d'événements de ce type de gravité.
5. Vous pouvez cliquer sur chaque section du graphique en anneau pour afficher la page des **événements basés sur la gravité** correspondante, qui affiche les détails suivants concernant la gravité sélectionnée pour la durée sélectionnée :
  - Source de l'instance
  - Données de l'événement
  - Catégorie d'événements générés par l'instance Citrix ADC
  - Notification de message envoyée

#### Remarque

Sous le diagramme en beignet, vous pouvez voir une liste des gravités qui sont représentées dans le graphique. Par défaut, un graphique en donut affiche tous les événements de tous les types de gravité. Par conséquent, tous les types de gravité de la liste sont mis en surbrillance. Vous pouvez basculer les types de gravité pour afficher et surveiller plus facilement la gravité de votre choix.



### Pour afficher les détails des interruptions SNMP Citrix ADC sur Citrix ADM :

Vous pouvez désormais afficher les détails de chaque interruption SNMP reçue de ses instances Citrix ADC gérées sur le serveur Citrix ADM dans la page **Paramètres d'événement**. Accédez à **Réseaux > Événements > Paramètres d'événement**. Pour une interruption spécifique reçue de votre instance, vous pouvez afficher les détails suivants sous forme de tableau :

- **Catégorie** : spécifie la catégorie de l'instance à laquelle appartient l'événement.
- **Gravité** - La gravité de l'événement est indiquée par les couleurs et son type de gravité.
- **Description** - Spécifie les messages associés à l'événement.

Par exemple, dans le cas d'un événement de la catégorie **MonRespTimeoutBelowThresh**, la description du piège s'affiche sous la forme « Ce piège est envoyé lorsque le délai de réponse d'une sonde de surveillance revient à la normale, inférieur au seuil défini ».

## Exporter les messages syslog

February 1, 2024

Vous pouvez désormais afficher les messages syslog sans vous connecter à Citrix Application Delivery Management (ADM), en planifiant une exportation de tous les messages syslog reçus sur le serveur. Vous pouvez exporter les messages syslog générés sur vos instances de Citrix Application Delivery Controller (ADC) aux formats PDF, CSV, PNG et JPEG. Vous pouvez planifier l'exportation de ces rapports vers des adresses e-mail spécifiées à différents intervalles.

### Remarque

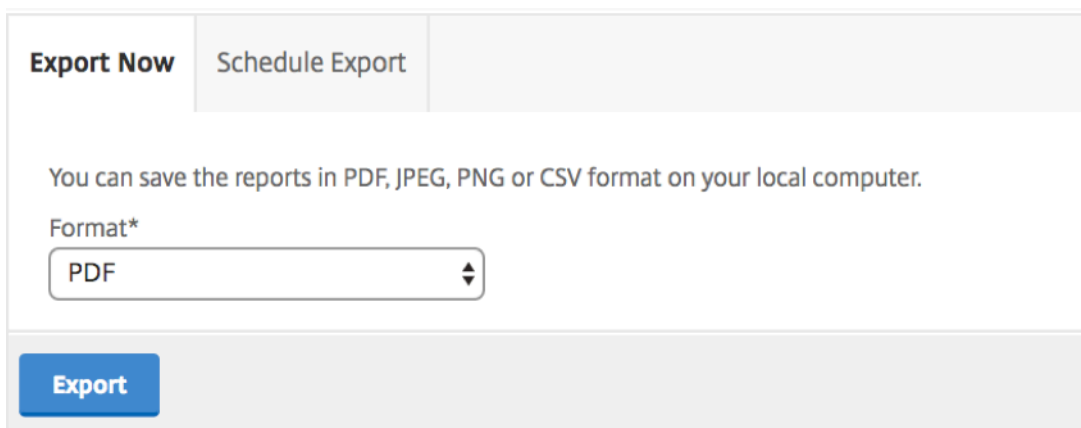
Pour plus d'informations sur la configuration d'un serveur Syslog, les données Syslog et le for-

mat d'heure, et sur la manière d'afficher les messages Syslog sur Citrix ADM, voir [Afficher les informations d'audit](#).

Pour afficher les messages syslog, accédez à **Réseaux>Événements>Messages Syslog**. Dans le volet droit, sous **Syslog Viewer**, vous pouvez filtrer les messages syslog que vous souhaitez afficher par module, type d'événement, gravité et adresse IP source. Cliquez sur **Appliquer** pour générer les messages syslog.

#### Pour exporter un rapport de messages syslog à l'aide de Citrix ADM :

1. Accédez à **Réseaux> Événements > Messages Syslog**.
2. Dans le volet droit, cliquez sur le bouton d'exportation en haut à droite de la page Syslog Messages.
3. Sous l'onglet **Exporter maintenant**, sélectionnez le format requis, puis cliquez sur **Exporter**.



**Export Now** | Schedule Export

You can save the reports in PDF, JPEG, PNG or CSV format on your local computer.

Format\*

PDF

**Export**

#### Pour planifier l'exportation du rapport des messages syslog à l'aide de Citrix ADM :

1. Accédez à **Réseaux > Événements > Messages Syslog**.
2. Sur la page **Messages Syslog**, dans le volet droit, cliquez sur **Exporter**.
3. Sous l'onglet **Planifier le rapport**, définissez les paramètres suivants :
  - **Description** : Message décrivant la raison de l'exportation du rapport.
  - **Format**: format dans lequel le rapport doit être exporté.
  - **Récurrence**: intervalle auquel le rapport doit être exporté .
  - **Heure d'exportation** : heure à laquelle l'état doit être exporté. Entrez l'heure au format 24 heures, pour votre fuseau horaire local.
  - **Liste de distribution d'e-mails** : Liste des destinataires à recevoir le rapport par courriel. Choisissez une liste de distribution d'e-mails dans la liste déroulante fournie. Un e-mail est déclenché lorsque le rapport est généré et répond aux critères d'heure planifiée. Si vous

souhaitez créer une nouvelle liste de distribution d'e-mails, cliquez sur + et fournissez les détails du serveur de messagerie et du profil de messagerie.

### Comment faire pour configurer les paramètres de nettoyage des événements à l'aide de Citrix ADM

Pour limiter la quantité de données de messages d'événements stockées dans la base de données de votre serveur Citrix ADM, vous pouvez spécifier l'intervalle pendant lequel Citrix ADM conserve les données de rapport 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).

Accédez à **Système > Administration système**. Sous Paramètres de **l'instance**, cliquez sur **Events Prune Settings**. Entrez l'intervalle de temps, en jours, pendant lequel vous souhaitez conserver les

données sur le serveur Citrix ADM et cliquez sur **OK**.

## Supprimer les messages Syslog

February 1, 2024

Lorsqu'il est configuré en tant que serveur syslog, Citrix Application Delivery Management (ADM) reçoit tous les messages syslog qui lui sont envoyés par les instances de Citrix Application Delivery Controller (ADC) configurées. Il se peut que vous ne vouliez pas voir un grand nombre de messages. Par exemple, il se peut que vous ne souhaitiez pas voir tous les messages de niveau informatif. Vous pouvez maintenant ignorer certains des messages syslog qui ne vous intéressent pas. Vous pouvez supprimer certains messages Syslog entrant dans Citrix ADM en configurant certains filtres. Citrix ADM supprime tous les messages correspondant aux critères. Ces messages supprimés n'apparaissent pas sur l'interface graphique Citrix ADM et ces messages ne sont pas non plus stockés dans la base de données Citrix ADM du client.

Vous pouvez supprimer certains messages Syslog enregistrés qui arrivent dans Citrix ADM en configurant certains filtres. Les deux filtres qui peuvent être utilisés pour supprimer les messages syslog sont la gravité et la facilité. Vous pouvez également supprimer les messages provenant d'une instance Citrix ADC particulière ou de plusieurs instances. Vous pouvez également fournir un modèle de texte pour Citrix ADM pour rechercher et supprimer des messages. Citrix ADM supprime tous les messages correspondant aux critères. Ces messages supprimés n'apparaissent pas sur l'interface graphique Citrix ADM et ne sont pas non plus stockés dans la base de données client. Par conséquent, une bonne quantité d'espace est économisée sur le serveur de stockage.

Voici quelques cas d'utilisation pour supprimer les messages Syslog :

- Si vous souhaitez ignorer tous les messages de niveau d'information, supprimez le niveau 6 (informationnel)
- Si vous souhaitez uniquement enregistrer les conditions d'erreur du pare-feu, supprimez tous les niveaux autres que le niveau 3 (erreurs)

### Suppression des messages syslog en créant des filtres

1. Dans Citrix ADM, accédez à **Réseaux > Événements > Messages Syslog > Supprimer le filtre**.
2. Sur la page **Créer un filtre de suppression**, mettez à jour les informations suivantes :
  - a) **Nom** : entrez le nom du filtre.

**Remarque**

Si différents utilisateurs ont un accès différent à plusieurs instances Citrix ADC, différents filtres doivent être créés pour différentes instances, car les utilisateurs ne 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 Citrix ADC sur lesquelles les messages syslog ont été configurés.

← Create Suppress Filter

Application Delivery Management filters and discards the logs that match the filter criteria that you specify.

Name\*  
 ?

Enable Filter

▼ Severity

Available (8) Select All

Alert	+
Critical	+
Debug	+
Emergency	+
Error	+

▶

◀

Configured (0) Remove All

No items

?

▼ Instances

If none selected, all instances be considered

	IP Address	Host Name
<input checked="" type="checkbox"/>	10.102.29.60	--

- d) **Installations** - Sélectionnez la ressource pour supprimer les messages en fonction de la source qui les génère.
- e) **Modèle de message** : vous pouvez également saisir un modèle de texte entouré d'un astérisque (\*) pour supprimer les messages. Les messages sont recherchés pour la chaîne



de modèle de texte et les messages qui contiennent ce modèle sont supprimés.

## Désactivation du filtre

Pour autoriser l’affichage des messages sur Citrix ADM, vous devez désactiver le filtre.

1. Accédez à **Réseaux > Événements > Messages Syslog > Supprimer le filtre**, puis sur la page **Supprimer le filtre**, sélectionnez le filtre et cliquez sur **Modifier**.
2. Dans la page **Configurer Supprimer le filtre**, **désactivez la case à cocher Activer le filtre** pour désactiver le filtre.

## Configurer les paramètres de nettoyage pour les événements d’instance

February 1, 2024

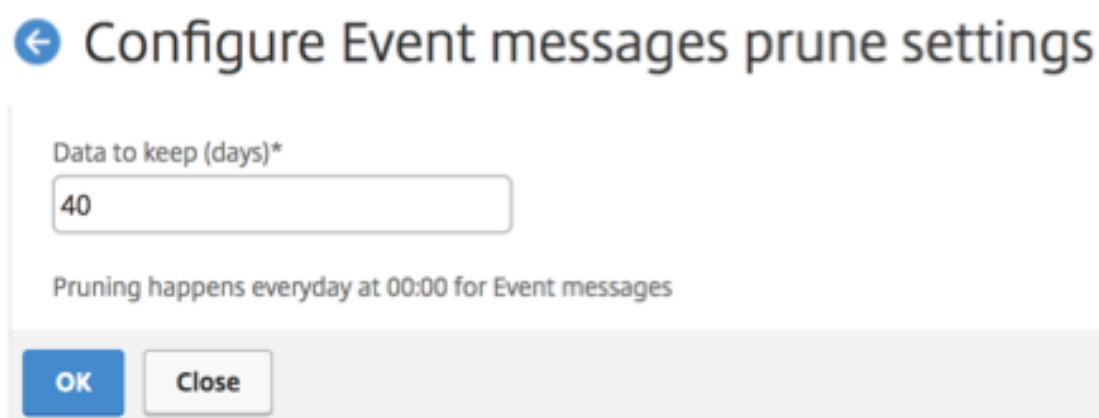
Les instances de Citrix Application Delivery Controller (ADC) gérées par votre serveur Citrix Application Delivery Management (ADM) envoient des données de messages d’événements en continu pour être stockées sur Citrix ADM. Vous pouvez spécifier l’intervalle pendant lequel Citrix ADM conserve les données de reporting réseau, les événements, les journaux d’audit et les journaux de tâches. Par défaut, ces données sont nettoyées toutes les 24 heures (à 00.00 heures).

### Remarque

La valeur que vous pouvez spécifier ne peut pas dépasser 40 jours ni être inférieure à 1 jour.

**Pour configurer les paramètres nettoyer pour les événements d'instance :**

1. Accédez à **Système > Administration système**.
  2. Sous **Paramètres de nettoyage**, cliquez sur **Paramètres de nettoyage des événements d'instance**.
  3. Entrez l'intervalle de temps, en jours, pour lequel vous souhaitez conserver les données sur le serveur Citrix ADM et cliquez sur **OK**.
- 



## Tableau de bord SSL

February 1, 2024

Citrix Application Delivery Management (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 de Citrix ADM et ses fonctionnalités, vous devez comprendre ce qu'est un certificat SSL et comment utiliser Citrix ADM pour suivre vos certificats SSL.

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).

Vous pouvez obtenir un certificat SSL et une clé de l'une des manières suivantes :

- De la part d'une autorité de certification (CA) autorisée

- En générant un nouveau certificat SSL et une nouvelle clé sur l'appliance Citrix ADC

Citrix ADM fournit une vue centralisée des certificats SSL installés sur toutes les instances Citrix ADC gérées. Sur le tableau de bord SSL, vous pouvez afficher des graphiques qui vous aident à suivre les émetteurs de certificats, les forces clés, les algorithmes de signature, les certificats expirés ou non utilisés, etc. Vous pouvez également voir la distribution des protocoles SSL qui s'exécutent sur vos serveurs virtuels et les clés qui y sont activées.

Vous pouvez également configurer des notifications pour vous informer lorsque les certificats sont sur le point d'expirer et inclure des informations sur les instances Citrix ADC qui utilisent ces certificats.

Vous pouvez lier les certificats d'une instance Citrix ADC à un certificat d'autorité de certification. Cependant, assurez-vous que les certificats que vous liez au même certificat d'autorité de certification ont la même source et le même émetteur. Après avoir lié les certificats à un certificat d'autorité de certification, vous pouvez les dissocier.

## Utiliser le tableau de bord SSL

February 1, 2024

Vous pouvez utiliser le tableau de bord des certificats SSL dans Citrix Application Delivery Management (ADM) pour afficher des graphiques qui vous aident à suivre les émetteurs de certificats, leurs principaux atouts et les algorithmes de signature. Le tableau de bord des certificats SSL affiche également des graphiques indiquant les éléments suivants :

- Nombre de jours après lesquels les certificats expirent
- Nombre de certificats utilisés et non utilisés
- Nombre de certificats autosignés et signés par une autorité de certification
- Nombre d'émetteurs
- Des algorithmes de signature
- Protocoles SSL
- 10 instances les plus importantes par nombre de certificats utilisés

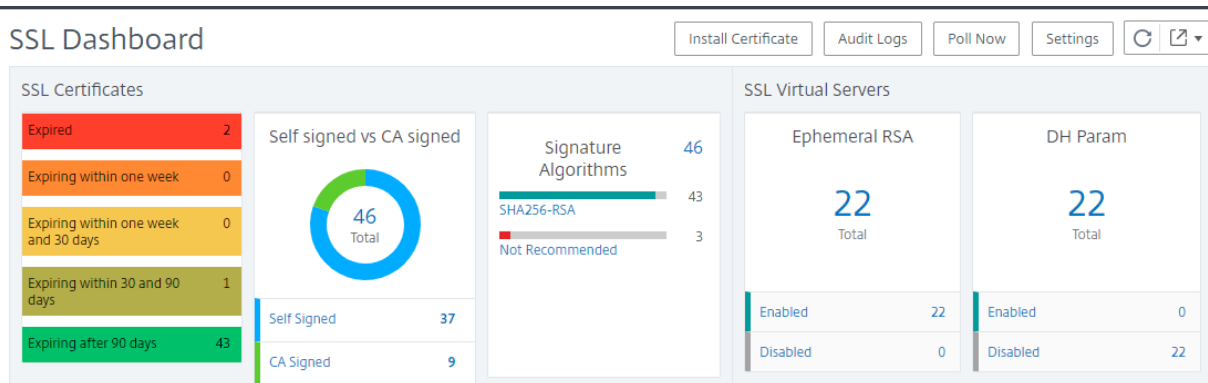
## Pour surveiller les certificats SSL

Vous pouvez utiliser le tableau de bord SSL sur Citrix ADM pour surveiller vos certificats si votre entreprise a une stratégie SSL dans laquelle vous avez défini certaines exigences de certificat SSL, telles que

tous les certificats doivent avoir des valeurs clés minimales de 2048 bits et une autorité de certification de confiance doit l'autoriser.

Dans un autre exemple, vous avez peut-être téléchargé un nouveau certificat mais oublié de le lier à un serveur virtuel. Le tableau de bord SSL met en évidence les certificats SSL utilisés ou non. Dans la section Utilisation, vous pouvez voir le nombre de certificats installés et le nombre de certificats utilisés. Vous pouvez ensuite cliquer sur le graphique pour voir le nom du certificat, l'instance sur laquelle il est utilisé, sa validité, son algorithme de signature, etc.

Pour surveiller les certificats SSL dans Citrix ADM, accédez à **Réseaux** > Tableau de **bord SSL**.



Citrix ADM vous permet d'interroger les certificats SSL et d'ajouter immédiatement tous les certificats SSL des instances à Citrix ADM. Pour ce faire, accédez à **Réseaux** > Tableau de **bord SSL** et cliquez sur Sonder **maintenant** . La page **Poll Now** apparaît, offrant la possibilité d'interroger toutes les instances Citrix Application Delivery Controller (ADC) du réseau ou d'interroger les instances sélectionnées.

Vous pouvez utiliser le tableau de bord SSL Citrix ADM pour afficher ou surveiller les détails des certificats SSL Citrix ADC, des serveurs virtuels SSL et des protocoles SSL. Les nombres « Total » sont des liens hypertexte sur lesquels vous pouvez cliquer pour afficher les détails relatifs aux certificats SSL, aux serveurs virtuels SSL ou aux protocoles SSL.

Par exemple, lorsqu'un utilisateur clique sur le nombre 52 sous « Auto-signé vs. Autorité de certification signée » dans la figure ci-dessus, une nouvelle fenêtre apparaît, montrant les détails des 52 certificats SSL sur les instances de Citrix ADC.

	CERTIFICATE NAME	INSTANCE	HOST NAME	DAYS TO EXPIRY	STATUS	DOMAIN
<input type="checkbox"/>			--	Expired	Expired	CTX4
<input type="checkbox"/>			--	360 days	Valid	hh
<input type="checkbox"/>			--	2 years 97 days	Valid	--
<input type="checkbox"/>			--	14 years 191 days	Valid	default LUJFB
<input type="checkbox"/>			--	14 years 331 days	Valid	default MBNL
<input type="checkbox"/>			NS105	15 years 295 days	Valid	default UZEK
<input type="checkbox"/>			--	15 years 361 days	Valid	Citrix
<input type="checkbox"/>			--	28 years 203 days	Valid	*.hotdrink.be

Le tableau de bord SSL Citrix ADM affiche également la distribution des protocoles SSL qui s'exécutent sur vos serveurs virtuels. En tant qu'administrateur, vous pouvez spécifier les protocoles que vous souhaitez surveiller via la stratégie SSL. Les protocoles pris en charge sont SSLv2, SSLv3, TLS1.0, TLS1.1 et TLS1.2. 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 donut apparaît après que les clés Diffie-Hellman (DH) ou Ephemeral RSA sont activées ou désactivées sur le tableau de bord SSL. Ces clés permettent une communication sécurisée avec les clients d'exportation même si le certificat serveur ne prend pas en charge les clients d'exportation, comme dans le cas d'un certificat 1024 bits. Cliquez sur le graphique approprié pour afficher la liste des serveurs virtuels sur lesquels les clés DH ou Ephemeral RSA sont activées.

### Pour afficher les pistes d'audit des certificats SSL

Vous pouvez désormais afficher les détails du journal des certificats SSL sur Citrix ADM. Les détails du journal affichent les opérations effectuées à l'aide de certificats SSL sur Citrix ADM, telles que : installation de certificats SSL, liaison et dissociation de certificats SSL, mise à jour de certificats SSL et suppression de certificats SSL. Les informations de piste d'audit sont utiles lors de la surveillance des modifications de certificat SSL effectuées sur une application avec plusieurs propriétaires.

Pour afficher un journal d'audit pour une opération particulière effectuée sur Citrix ADM à l'aide de certificats SSL, accédez à **Réseaux** > Tableau de **bord SSL** > **Pistes d'audit SSL**.

## SSL Audit Trails

<input type="checkbox"/>	Name	Status	Start Time	End Time
<input type="checkbox"/>	InstallSSLCert	Completed	Mon, 17 Apr 2017 12:19:48 GMT	Mon, 17 Apr 2017 12:19:50 GMT
<input type="checkbox"/>	InstallSSLCert	Completed	Mon, 17 Apr 2017 12:14:13 GMT	Mon, 17 Apr 2017 12:14:15 GMT
<input type="checkbox"/>	InstallSSLCert	Completed	Mon, 17 Apr 2017 12:08:37 GMT	Mon, 17 Apr 2017 12:08:39 GMT
<input type="checkbox"/>	InstallSSLCert	Completed	Mon, 17 Apr 2017 12:06:18 GMT	Mon, 17 Apr 2017 12:06:22 GMT
<input type="checkbox"/>	InstallSSLCert	Completed	Mon, 17 Apr 2017 11:40:42 GMT	Mon, 17 Apr 2017 11:40:47 GMT
<input type="checkbox"/>	InstallSSLCert	Completed	Mon, 17 Apr 2017 11:37:22 GMT	Mon, 17 Apr 2017 11:37:24 GMT

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 exécutées sur cette instance.

### SSL Audit Trails

The screenshot shows the 'SSL Audit Trails' interface. It features a 'Device Log' section with a table of entries. The first entry, 'InstallSSLCert', is selected. Below this, there are two sub-sections: 'Device Log' and 'Command Log'. The 'Device Log' section shows a table with columns for 'Status', 'IP Address', and 'Start Time'. The 'Command Log' section shows a table with columns for 'Status', 'Message', 'Command', and 'Start Time'. The 'Command Log' table contains three entries, all with a status of 'Done', representing the execution of commands to install and configure the SSL certificate.

## Pour exclure les certificats Citrix ADC par défaut sur le tableau de bord SSL

Citrix ADM vous permet d'afficher ou de masquer les certificats Citrix ADC par défaut qui s'affichent dans les graphiques SSL Dashboard en fonction de vos préférences. Par défaut, tous les certificats sont affichés sur le tableau de bord SSL, y compris les certificats par défaut.

Pour afficher ou masquer les certificats par défaut sur le tableau de bord SSL :

1. Accédez à **Réseaux > Tableau de bord SSL** dans l'interface graphique Citrix ADM.
2. Sur la page **Tableau de bord SSL**, cliquez sur **Paramètres**.
3. Dans la page **Paramètres**, sélectionnez **Général**.
4. Entrez le nombre de jours d'expiration du certificat pour recevoir une notification concernant l'expiration du certificat.
5. Sélectionnez la méthode de notification et créez les profils correspondants.
6. Dans la section **Filtre de certificat**, désactivez la case à cocher **Afficher les certificats par défaut** et cliquez sur **Enregistrer et quitter**.

The screenshot shows the 'Settings' page in NetScaler ADM. On the left, there is a navigation menu with 'General' and 'Enterprise Policy'. The main content area is divided into three sections: 'Notification Settings', 'Certificate Filter', and 'Certificate Polling'. In 'Notification Settings', the 'Certificate is expiring in (days)' field is set to 30. Below it, there are three checkboxes for notification methods: 'Email', 'SMS (Text Message)', and 'Slack'. In 'Certificate Filter', the 'Show Default Certificates' toggle is turned on. In 'Certificate Polling', the 'Polling Interval (in min)\*' field is set to 1440. At the bottom, there are three buttons: 'Cancel', 'Next →', and 'Save and Exit'.

## Configurer les notifications pour l'expiration du certificat SSL

February 1, 2024

En tant qu'administrateur de la sécurité, vous pouvez configurer des notifications pour vous informer de l'expiration prochaine des certificats et pour inclure des informations sur les instances de Citrix Application Delivery Controller (ADC) qui utilisent ces certificats. En activant les notifications, vous pouvez renouveler vos certificats SSL à temps.

Par exemple, vous pouvez définir une notification par e-mail pour envoyer une liste de distribution par e-mail 30 jours avant l'expiration de votre certificat.

### Pour configurer des notifications à partir de Citrix ADM :

1. Dans Citrix Application Delivery Management (ADM), accédez à **Réseaux > Tableau de bord SSL**.
2. Dans la page **Tableau de bord SSL**, cliquez sur **Paramètres**.
3. Sur la page **Paramètres SSL**, cliquez sur l'icône **Modifier**.
4. Dans la section **Paramètres de notification**, indiquez à quel moment vous souhaitez envoyer la notification en termes de nombre de jours avant la date d'expiration.
5. Choisissez le type de notification que vous souhaitez envoyer. Sélectionnez le type de notification et la liste de distribution dans le menu déroulant. Les types de notification sont les suivants :
  - **E-mail** : spécifiez un serveur de messagerie et les détails du profil. Un e-mail est déclenché lorsque vos certificats sont sur le point d'expirer.
  - **SMS** —Spécifiez un serveur de service de messages courts (SMS) et les détails du profil. Un message SMS est déclenché lorsque vos certificats sont sur le point d'expirer.

- **Slack** - Spécifiez les détails du profil Slack.

6. Cliquez sur **Enregistrer et quitter**.

Citrix ADM envoie désormais l'interruption d'expiration de certificat SSL au serveur de destination d'interruption externe lorsque vos certificats SSL sont expirés. Citrix ADM envoie une interruption lorsque les deux conditions suivantes sont remplies :

- Vous avez configuré le nombre de jours pour l'expiration du certificat dans la page des paramètres du tableau de bord SSL .
- Vous avez ajouté la destination du piège.

Vous pouvez définir des destinations d'interruption en accédant à **Système > SNMP > Destinations d'interruption** . Tapez l'adresse IP du serveur SNMP de destination où les interruptions sont envoyées. Entrez le numéro de port et tapez « public » (sans guillemets) comme chaîne de communauté.

## Mettre à jour un certificat installé

February 1, 2024

Après avoir reçu un certificat renouvelé de l'autorité de certification (CA), vous pouvez mettre à jour les certificats existants à partir de Citrix Application Delivery Management (ADM) sans avoir à ouvrir une session à des instances Citrix Application Delivery Controller (ADC) individuelles.

### Pour mettre à jour un certificat SSL, une clé ou les deux à partir de Citrix ADM :

1. Dans Citrix ADM, accédez à **Réseaux > Tableau de bord SSL**.
2. Cliquez sur l'un des graphiques pour afficher la liste des certificats SSL.



3. Sur la page **Certificats SSL**, sélectionnez un certificat et cliquez sur **Mettre à jour**. Vous pouvez également cliquer sur le certificat SSL pour afficher ses détails, puis cliquez sur **Mettre à jour** dans le coin supérieur droit de la page **Certificat SSL**.
4. Sur la page **Mettre à jour le certificat SSL**, apportez les modifications requises au certificat, à la clé ou aux deux, puis cliquez sur **OK**.

## Installer des certificats SSL sur une instance Citrix ADC

February 1, 2024

Avant d'installer des certificats SSL sur des instances ADC (Citrix Application Delivery Controller), assurez-vous que les certificats sont émis par des autorités de certification approuvées. Assurez-vous également que la force de clé des clés de certificat est de 2048 bits ou plus et que les clés sont signées à l'aide d'algorithmes de signature sécurisés.

### Pour installer un certificat SSL à partir d'une autre instance Citrix ADC :

Vous pouvez également importer un certificat à partir d'une instance Citrix ADC choisie et l'appliquer à d'autres instances Citrix ADC ciblées à partir de l'interface graphique de Citrix Application Delivery Management (ADM).

1. Accédez à **Réseaux > Tableau de bord SSL**.
2. Dans l'angle supérieur droit du tableau de bord SSL, cliquez sur **Installer**.
3. 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 Citrix ADC sur lesquelles vous souhaitez installer vos certificats.

5. Cliquez sur **OK**.

## Install SSL Certificate on Citrix ADC Instances

▼ Certificate Source

Import from Instance  Upload Certificate File

Instance\*  
10.102.29.60

Certificate\*  
ns-sftrust-certificate

▼ Certificate Details

Certificate Name\*  
nsroot

Password  
\*\*\*\*\*

Save Configuration

Select Instances Delete

	IP Address	Host Name	Instance State
<input checked="" type="checkbox"/>	10.102.29.200	--	● Up
<input checked="" type="checkbox"/>	10.102.29.160	NS	● Up

**Pour installer un certificat SSL à partir de Citrix ADM :**

1. Dans Citrix ADM, accédez à **Réseaux > Tableau de bord SSL**.
2. Dans l'angle supérieur droit du tableau de bord, cliquez sur **Installer**.
3. Sur la page **Installer un certificat SSL sur une instance NetScaler**, sélectionnez **Télécharger le fichier de certificats** et spécifiez les paramètres suivants :
  - **Fichier de certificat** : téléchargez un fichier de certificat SSL en sélectionnant **Local** (votre machine locale) ou **Appliance** (le fichier de certificat doit être présent sur l'instance virtuelle Citrix ADM).
  - **Fichier clé** : téléchargez le fichier clé.
  - **Nom du certificat** — Spécifiez le nom de la clé de certificat.
  - **Mot de passe** : mot de passe pour crypter la clé privée. Vous pouvez utiliser cette option pour télécharger des clés privées chiffrées.
  - **Sélectionner les instances** : sélectionnez les instances Citrix ADM sur lesquelles vous souhaitez installer vos certificats.
4. Pour enregistrer la configuration en vue d'une utilisation ultérieure, activez la case à cocher **Enregistrer la configuration**.
5. Cliquez sur **OK**.

## ← Install SSL Certificate on Citrix ADC Instances

▼ Certificate Source

Import from Instance     Upload Certificate File

Certificate File\*

Choose File
pickCA\_rootcert.pem
?

Key File\*

Choose File
pickCA\_rootcert.pem
?

▼ Certificate Details

Certificate Name\*

nsroot

Password

.....

Save Configuration

Select Instances
Delete

	IP Address	Host Name
<input checked="" type="checkbox"/>	10.102.29.200	--
<input checked="" type="checkbox"/>	10.102.29.160	NS

### Créer une demande de signature de certificat (CSR)

February 1, 2024

Une demande de signature de certificat (CSR) est un bloc de texte chiffré qui est généré sur le serveur sur lequel le certificat sera utilisé. Il contient des informations qui seront incluses dans le certificat, telles que le nom de votre organisation, le nom commun (nom de domaine), la localité et le pays.

#### Pour créer un CSR à l'aide de Citrix ADM :

1. Dans Citrix Application Delivery Management (ADM), accédez à **Réseaux > Tableau de bord SSL**.

2. Cliquez sur l'un des graphiques pour afficher la liste des certificats SSL installés, puis sélectionnez le certificat pour lequel vous souhaitez créer un CSR et sélectionnez **Créer CSR** dans la liste **Sélectionner une action**.
3. Dans la page **Créer une demande de signature de certificat (CSR)**, spécifiez un nom pour la CSR.
4. Procédez comme suit :
  - **Télécharger une clé** : sélectionnez l'option **J'ai une clé** . Pour télécharger votre fichier de clé, sélectionnez **Local** (votre machine locale) ou **Appliance** (le fichier de clé doit être présent sur l'instance virtuelle Citrix ADM).
  - **Créer une clé** - Sélectionnez l'option Je n'ai pas de clé, puis spécifiez les paramètres suivants :

---

<b>Algorithme de chiffrement</b>	Type de clé. Par exemple, RSA.
<b>Nom du fichier clé</b>	Nom du fichier dans lequel la clé RSA est stockée.
<b>Taille de la clé</b>	Taille de la clé en bits.
<b>Valeur de l'exposant public</b>	Choisissez <b>3</b> ou <b>F4</b> dans la liste déroulante fournie. Cette valeur fait partie de l'algorithme de chiffrement requis pour créer votre clé RSA.
<b>Format clé</b>	Par défaut, PEM est sélectionné. PEM est le format de clé recommandé pour votre certificat SSL.
<b>Algorithme d'encodage PEM</b>	Dans la liste déroulante, sélectionnez l'algorithme ( <b>DES</b> ou <b>DES3</b> ) à utiliser pour chiffrer la clé RSA générée. Si vous sélectionnez cet algorithme, vous devrez fournir un mot de passe PEM.
<b>Passphrase PEM</b>	Si vous avez choisi l'algorithme de codage PEM, entrez un mot de passe.
<b>Confirmer la phrase secrète PEM</b>	Confirmez votre mot de passe PEM.

---

5. Cliquez sur **Continuer**.
6. Sur la page suivante, fournissez des détails supplémentaires. Si vous souhaitez créer le CSR sans modifier les valeurs par défaut, cliquez sur **Continuer**.

### Remarque

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.

La plupart des autorités de certification acceptent les soumissions de certificats par courriel. L'AC retournera un certificat valide à l'adresse e-mail à partir de laquelle vous soumettez le CSR.

## Lier et dissocier les certificats SSL

February 1, 2024

Vous créez un ensemble de certificats en liant plusieurs certificats entre eux. Pour lier un certificat à un autre certificat, l'émetteur du premier certificat doit correspondre au domaine du second certificat. Par exemple, si vous souhaitez lier le certificat A au certificat B, l'« émetteur » du certificat A doit correspondre au « domaine » du certificat B.

### Pour lier un certificat SSL à un autre certificat à l'aide de Citrix ADM :

1. Dans Citrix Application Delivery Management (ADM), accédez à **Réseaux > Tableau de bord SSL**.
2. Cliquez sur l'un des graphiques pour afficher la liste des certificats SSL.
3. Sélectionnez le certificat que vous souhaitez lier, puis sélectionnez **Lien** dans la liste déroulante **Action**.
4. Dans la liste des certificats correspondants, sélectionnez le certificat auquel vous souhaitez lier, puis cliquez sur **OK**.

### Remarque

Si aucun certificat correspondant n'est trouvé, le message suivant s'affiche : Aucun certificat trouvé à lier.

### Pour dissocier un certificat SSL à l'aide de Citrix ADM :

1. Dans Citrix ADM, accédez à **Réseaux > Tableau de bord SSL**.
2. Cliquez sur l'un des graphiques pour afficher la liste des certificats SSL.
3. Choisissez l'un des certificats liés, puis sélectionnez **Dissocier dans** la liste déroulante **Action**.
4. Cliquez sur **OK**.

### Remarque

Si le certificat sélectionné n'est pas lié à un autre certificat, le message suivant s'affiche : Le certificat n'a pas de lien d'autorité de certification.

## Configurer une stratégie d'entreprise

February 1, 2024

Vous pouvez configurer une stratégie d'entreprise et ajouter toutes les autorités de certification approuvées, des algorithmes de signature sécurisés et sélectionner la force de clé recommandée pour vos clés de certificat dans Citrix Application Delivery Management (ADM). Si l'un des certificats installés sur votre instance de 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 valeur de clé du certificat ne correspond pas à la valeur de clé recommandée dans la stratégie de l'entreprise, le tableau de bord des certificats SSL affiche la valeur de ces clés comme non recommandée.

### Pour configurer une stratégie d'entreprise sur Citrix ADM :

1. Dans Citrix ADM, accédez à **Infrastructure** > Tableau de **bord SSL**, puis cliquez sur **Paramètres**.
2. Sur la page Paramètres SSL, cliquez sur l'icône **Modifier** pour ajouter toutes les autorités de certification de confiance, les algorithmes de signature sécurisée et sélectionner la force de clé recommandée pour vos certificats et clés.
3. Cliquez sur **Enregistrer** pour enregistrer votre stratégie d'entreprise.

## Interroger les certificats SSL à partir d'instances Citrix ADC

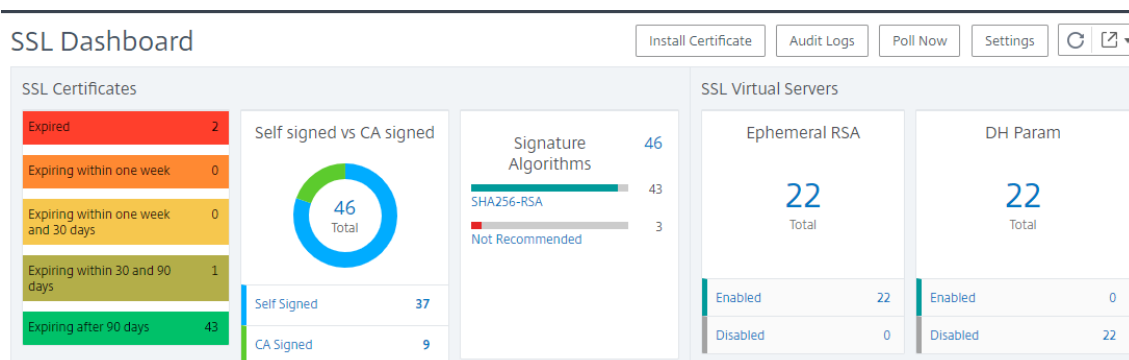
February 1, 2024

Citrix Application Delivery Management (ADM) interroge automatiquement les certificats SSL toutes les 24 heures à l'aide d'appels NITRO et du protocole Secure Copy (SCP). Vous pouvez également interroger manuellement les certificats SSL pour découvrir les certificats SSL nouvellement ajoutés sur les instances de Citrix Application Delivery Controller (ADC). L'interrogation de toutes les instances Citrix ADC certificats SSL place une lourde charge sur le réseau.

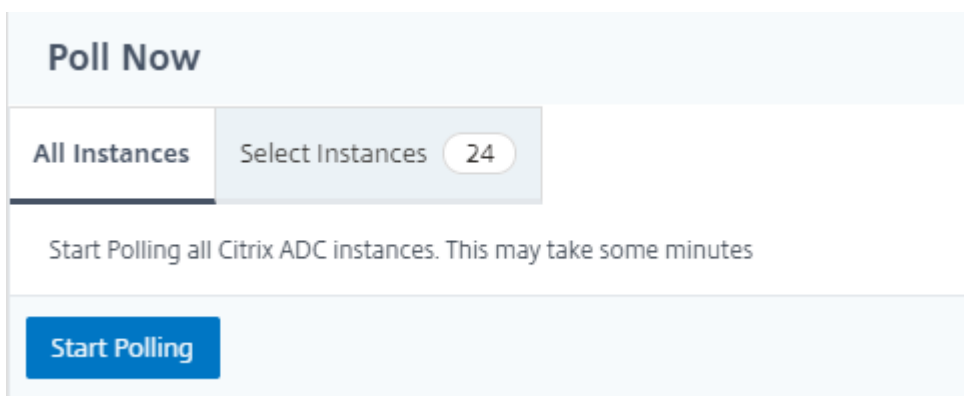
Au lieu d'interroger les certificats SSL de tous les instances Citrix ADC, vous pouvez interroger manuellement uniquement les certificats SSL d'une ou plusieurs instances sélectionnées.

**Pour interroger des certificats SSL sur des instances Citrix ADC :**

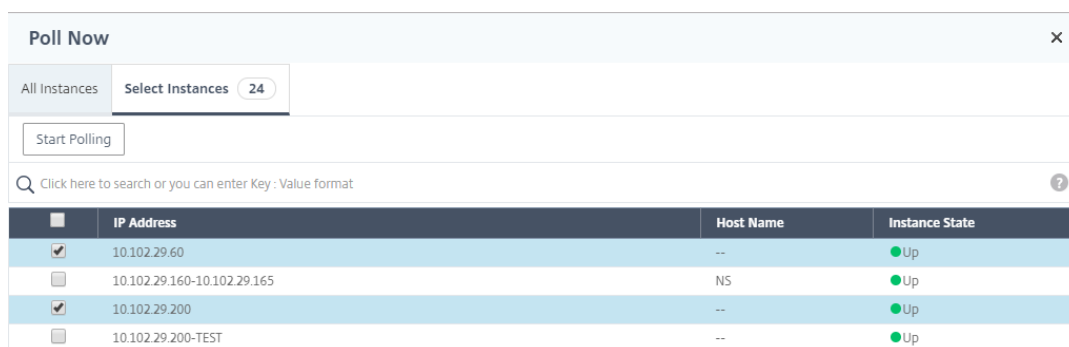
1. Dans Citrix ADM, accédez à **Réseaux > Tableau de bord SSL**.
2. Dans la page **Tableau de bord SSL**, dans le coin supérieur droit, cliquez sur **Sondage maintenant**.



3. La page **Poll Now** s'affiche et vous permet d'interroger toutes les instances Citrix ADC du réseau ou d'interroger les instances sélectionnées.
  - a) Pour interroger les certificats SSL de toutes les instances Citrix ADC, sélectionnez l'onglet **Toutes les instances** et cliquez sur **Démarrer** le sondage.



- b) Pour interroger des instances spécifiques, sélectionnez l'onglet **Sélectionner des instances**, sélectionnez les instances dans la liste, puis cliquez sur **Interroger maintenant**.



	IP Address	Host Name	Instance State
<input checked="" type="checkbox"/>	10.102.29.60	--	● Up
<input type="checkbox"/>	10.102.29.160-10.102.29.165	NS	● Up
<input checked="" type="checkbox"/>	10.102.29.200	--	● Up
<input type="checkbox"/>	10.102.29.200-TEST	--	● Up

## Tâches de configuration

February 1, 2024

Le processus de gestion de la configuration Citrix Application Delivery Management (Citrix ADM) garantit la réplication correcte des modifications de configuration, des mises à niveau du système et d'autres activités de maintenance sur plusieurs instances Citrix Application Delivery Controller (ADC) du réseau.

Citrix ADM vous permet de créer des tâches de configuration qui vous aideront à effectuer toutes ces activités facilement sur plusieurs appareils en une seule tâche. Les tâches de configuration et les modèles simplifient les tâches administratives les plus répétitives en une seule tâche sur Citrix ADM. Une tâche de configuration contient un ensemble de commandes de configuration que vous pouvez exécuter sur un ou plusieurs appareils gérés.

Les tâches de configuration peuvent soit utiliser des commandes SSH pour effectuer des commandes de configuration, soit utiliser SCP pour copier des fichiers depuis localement ou vers une autre appliance. Par exemple, nous pouvons planifier un basculement HA ou une mise à niveau HA.

Vous pouvez créer une tâche de configuration à l'aide de l'une des quatre options suivantes dans Citrix ADM. Utilisez l'une de ces options pour créer une source réutilisable de commandes et d'instructions au système pour exécuter un travail de configuration.

1. Modèle de configuration
2. Instance
3. Fichier
4. Enregistrer et lire



## Modèle de configuration

Vous pouvez créer des modèles de configuration tout en créant une nouvelle tâche 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. 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 le travail à exécuter à un stade ultérieur.

## Instance

Vous pouvez effectuer une mise à niveau groupée unique de vos instances Citrix SDX exécutant Citrix ADC version 11.0 et ultérieure. Pour effectuer une mise à niveau groupée unique, vous utilisez une tâche intégrée dans Citrix ADM. Vous pouvez également mettre à niveau une instance Citrix ADC en extrayant la configuration en cours d'exécution ou une configuration enregistrée et en exécutant les commandes sur une autre instance Citrix ADC du même type. Cela vous permet de répliquer la configuration d'une instance sur l'autre.

## Fichier

Vous pouvez télécharger un fichier de configuration à partir de votre machine locale et créer des tâches.

Avantages de l'utilisation d'un fichier

- Vous pouvez utiliser n'importe quel fichier texte pour créer une source réutilisable de commandes de configuration.
- Aucun type de formatage n'est requis.
- Le fichier peut être enregistré sur votre ordinateur local.

Vous pouvez créer et enregistrer un nouveau fichier ou importer un fichier existant et exécuter les commandes.

## Enregistrer et lire

En utilisant Create job, vous pouvez soit entrer vos propres commandes CLI, soit utiliser le bouton Record and play pour obtenir des commandes à partir d'une session Citrix ADC. Lorsque vous exécutez le travail, les modifications apportées au fichier ns.conf sur l'instance sélectionnée sont enregistrées et copiées dans Citrix ADM.

## Articles connexes

- [Comment utiliser la commande SCP \(put\) dans les tâches de configuration](#)
- [Comment utiliser des variables dans les tâches de configuration](#)
- [Comment créer des tâches de configuration à partir de commandes correctives](#)
- [Comment utiliser les modèles de configuration pour créer des modèles d'audit](#)
- [Comment utiliser l'enregistrement et la lecture pour créer des tâches de configuration](#)
- [Comment faire pour utiliser le modèle de configuration maître sur Citrix ADM](#)

## Créer une tâche de configuration

February 1, 2024

Une tâche est un ensemble de commandes de configuration que vous pouvez créer et exécuter sur une ou plusieurs instances gérées. Vous pouvez créer des tâches pour apporter des modifications de configuration entre les instances, [répliquer des configurations sur plusieurs instances](#) de votre réseau et des [tâches de configuration d'enregistrement et de lecture](#) à l'aide de l'interface graphique Citrix Application Delivery Management (ADM) et les convertir en commandes CLI.

Vous pouvez utiliser la fonctionnalité Travaux de configuration de Citrix ADM pour créer une tâche de configuration, envoyer des notifications par e-mail et vérifier les journaux d'exécution des tâches créées.

### Pour créer une tâche de configuration sur Citrix ADM :

1. Accédez à **Réseaux > Travaux de configuration**.
2. Cliquez sur **Créer 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 déroulante.
4. Dans la liste déroulante **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 déroulante Source de configuration, sélectionnez les différents modèles, puis faites-les glisser et déposez les modèles 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 de tâche de configuration principale de déploiement pour la première fois, puis que vous ajoutez un modèle de type différent, l'ensemble du modèle de tâche sera de type Configuration principale.

5. 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 ultérieurement lors de la modification de la tâche de configuration.
6. Vous pouvez définir des variables qui vous permettent d'attribuer différentes valeurs pour ces paramètres ou d'exécuter une tâche 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.
7. Dans l'onglet **Sélectionner les instances**, sélectionnez les instances sur lesquelles vous souhaitez exécuter l'audit de configuration et cliquez sur **Suivant**.
8. Dans l'onglet **Spécifier les valeurs variables**, vous disposez de deux options :
  - a) Téléchargez le fichier d'entrée pour entrer les valeurs des variables que vous avez définies dans vos commandes, puis téléchargez le fichier sur le serveur Citrix ADM.
  - b) Entrez des valeurs communes pour les variables que vous avez définies pour toutes les instances
9. Cliquez sur **Suivant**.
10. Vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance dans l'onglet **Job Preview**. Pour évaluer les commandes d'annulation, cochez la case **Aperçu des commandes d'annulation**

11. Dans l'onglet **Exécuter**, choisissez d'exécuter votre tâche maintenant ou de planifier l'exécution de la tâche ultérieurement. Vous devez également sélectionner l'action que Citrix ADM doit effectuer en cas d'échec de la commande.

**Pour envoyer une notification par e-mail pour une offre d'emploi :**

Une notification par e-mail est désormais envoyée chaque fois qu'une tâche est exécutée ou planifiée. La notification couvrira des détails tels que la réussite ou l'échec de la tâche, ainsi que les détails pertinents.

Après avoir créé une tâche, dans l'onglet Exécuter, cochez la case **E-mail** dans la section Recevoir le rapport d'exécution via. 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.

**Pour afficher les détails du récapitulatif d'exécution :**

Accédez à **Réseaux > Travaux de configuration**. Sélectionnez une tâche et cliquez sur **Détails**. Cliquez sur **Résumé de l'exécution** pour voir l'état de l'instance qui a exécuté la tâche, les commandes exécutées sur la tâche, les heures de début et de fin de la tâche et le nom de l'utilisateur de l'instance.

Execution Summary						×
Instances <b>1</b>		Last Execution <b>Sep 16 1:04 PM</b>				
Status of Instances						
IP Address	Status	Commands	Start Time	End Time	Instance User	
10.102.29.191	● Completed	3/3	Sep 16 1:04 PM	Sep 16 1:04 PM	nsroot >	

## Utiliser l'enregistrement et la lecture pour créer des tâches de configuration

February 1, 2024

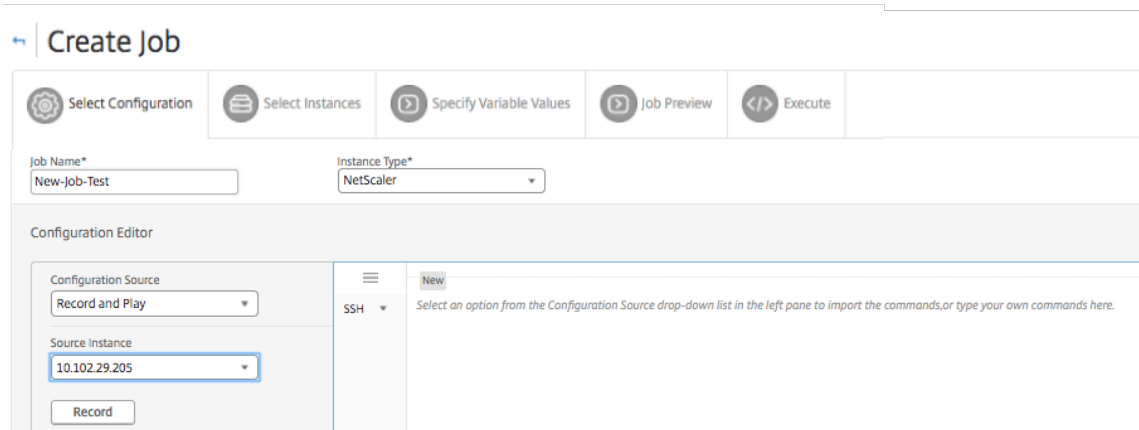
Si vous avez l'habitude d'utiliser l'interface graphique NetScaler pour configurer une instance NetScaler, vous pouvez parfois avoir du mal à vous souvenir des commandes CLI exactes pour créer une tâche de configuration et l'exécuter sur plusieurs instances NetScaler.

Citrix ADM vous permet d'enregistrer les tâches de configuration effectuées à l'aide de l'interface graphique d'une instance NetScaler et de les convertir en commandes CLI. Vous pouvez ensuite créer

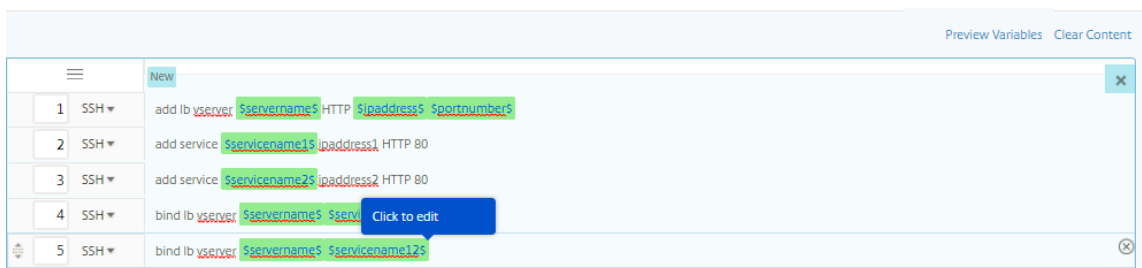
une tâche de configuration à partir de ces commandes CLI et exécuter cette tâche sur plusieurs instances.

## Pour enregistrer la configuration de l'interface graphique et la convertir en tâche de configuration

1. Accédez à **Réseaux > Tâches de configuration** , puis cliquez sur **Créer une tâche** .
2. Spécifiez le nom de la tâche et le type d'instance.
3. Dans la liste **Source de configuration**, sélectionnez **Record and Play**, puis sélectionnez l'instance source à partir de laquelle vous souhaitez enregistrer la configuration. Cliquez sur **Enregistrer**.

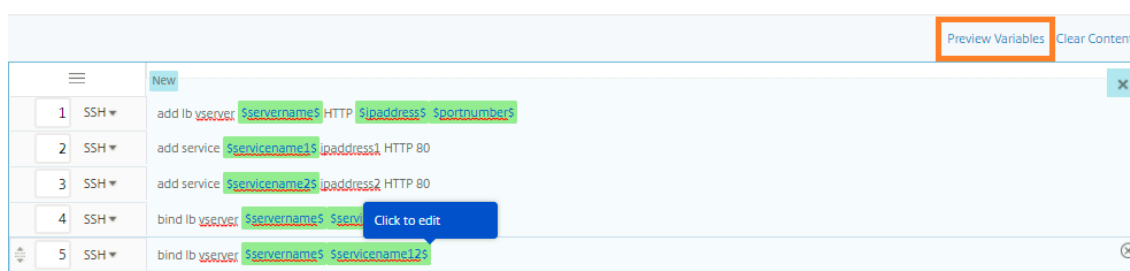


4. L'**interface graphique de NetScaler** s'ouvre. Configurez les fonctionnalités et paramètres que vous souhaitez que la tâche de configuration contienne. Fermez ensuite la fenêtre de l'interface graphique de NetScaler et cliquez sur **Arrêter** dans l'éditeur de **configuration**. Les commandes apparaissent sous la forme d'un lien dans le volet gauche. Faites glisser les commandes vers le volet droit, puis cliquez sur **Suivant**.



Vous pouvez ensuite réorganiser les commandes dans l'éditeur de configuration selon les besoins. Vous pouvez déplacer la commande d'une ligne à l'autre en faisant glisser la ligne de commande. Vous pouvez également déplacer ou réorganiser la ligne de commande d'une ligne à n'importe quelle ligne cible en changeant simplement le numéro de ligne de commande dans la zone de texte.

5. Vous pouvez consulter toutes les variables que vous avez définies lors de la création ou de la modification d'un travail de configuration dans une vue consolidée unique.
6. Pour afficher toutes les variables dans une seule vue consolidée, procédez de l'une des manières suivantes :
  - Lors de la création d'une tâche de configuration, accédez à **Réseaux > Tâches de configuration**, puis sélectionnez **Créer une tâche**. Sur la page **Créer un travail**, vous pouvez consulter toutes les variables que vous avez ajoutées lors de la création du travail de configuration.
  - Lorsque vous modifiez une tâche de configuration, accédez à **Réseau > Tâches de configuration**, sélectionnez le nom de la tâche et cliquez sur **Modifier**. Sur la page **Configurer la tâche**, vous pouvez consulter toutes les variables qui ont été ajoutées lors de la création de la tâche de configuration.
7. Vous pouvez ensuite cliquer sur l'onglet **Aperçu des variables** pour prévisualiser les variables dans une vue consolidée unique que vous avez définie lors de la création ou de la modification d'une tâche de configuration.



8. Une nouvelle fenêtre contextuelle apparaît et affiche tous les paramètres des variables telles que Nom, Nom d'affichage, Type et valeur par défaut dans un format tabulaire. Vous pouvez également modifier et modifier ces paramètres. Cliquez sur le bouton **Terminé** après avoir modifié l'un des paramètres.

Name*	Display Name*	Type*	Default Value
portnumber	portnumber	Text Field	
ipaddress	ipaddress	Text Field	
servername	servername	Text Field	
servicename1	servicename1	Text Field	
servicename2	servicename2	Text Field	
servicename12	servicename12	Text Field	

Done

9. Cliquez sur **Ajouter des instances** et sélectionnez les instances sur lesquelles vous souhaitez exécuter le travail de configuration. Cliquez sur **OK**, puis sur **Suivant**.

IP Address	Name	State
10.102.216.219		●
10.102.216.49-Partition_3	NS_AppFW2	●
10.102.126.64	AppDiscovery-DONOTDELETE-2	●
<input checked="" type="checkbox"/> 10.102.29.191		●
10.102.29.120-p1		●
<input checked="" type="checkbox"/> 10.102.29.80	NS80	●
172.17.0.30(10.102.38.136)		●
10.102.216.49-Partition_2	NS_AppFW2	●
10.102.29.120-p2		●
10.102.216.49	NS_AppFW2	●
<input checked="" type="checkbox"/> 10.102.29.70	MyCache	●
<input checked="" type="checkbox"/> 10.102.29.200	MyCache	●

10. Si vous avez spécifié des variables dans les commandes, sous l'onglet **Spécifier des valeurs variables**, sélectionnez l'une des options suivantes pour spécifier des variables pour vos instances :
  - **Télécharger le fichier d'entrée pour les valeurs des variables** : cliquez sur **Télécharger le fichier clé d'entrée** pour télécharger un fichier d'entrée. Dans le fichier d'entrée, entrez des valeurs pour les variables que vous avez définies dans vos commandes, puis téléchargez le fichier sur le serveur Citrix ADM.
  - **Valeurs de variables communes pour toutes les instances** : entrez des valeurs pour les variables. Les variables varient en fonction du modèle sélectionné.

Les fichiers d'entrée contenant les valeurs des variables sont conservés (avec le même nom de fichier) dans les tâches de configuration. Vous pouvez afficher et modifier ces fichiers d'entrée que vous avez utilisés et chargés précédemment lors de la création ou de la modification des tâches de configuration.

Pour afficher les tâches de configuration exécutées lors de la création d'une tâche de configuration, accédez à **Réseau > Tâches de configuration**, puis cliquez sur **Créer une tâche**. Dans la page **Créer une tâche**. Dans l'onglet **Spécifier les valeurs des variables**, sélectionnez l'option **Valeurs de variables communes pour toutes les instances** pour afficher les fichiers téléchargés. Pour modifier les fichiers d'entrée, téléchargez le fichier d'entrée, puis modifiez et chargez les fichiers (en conservant le même nom de fichier).

Pour afficher les tâches de configuration déjà exécutées lors de la modification d'une tâche de configuration, accédez à **Réseau > Tâches de configuration**, sélectionnez le nom de la tâche et cliquez sur **Modifier**. Dans la page **Configurer la tâche**, sous l'onglet **Spécifier les valeurs de variable**, sélectionnez l'option **Valeurs variables communes pour toutes les instances** pour afficher les fichiers chargés. Pour modifier les fichiers d'entrée, téléchargez le fichier d'entrée, puis modifiez et téléchargez les fichiers (en conservant le même nom de fichier) .10.Sous l'onglet **Aperçu des tâches**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances.

11. Sous l'onglet **Aperçu du travail**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances.
12. Sous l'onglet **Exécuter**, vous pouvez choisir d'exécuter votre travail maintenant ou de le planifier à une date ultérieure. Vous pouvez également choisir l'action que Citrix ADM doit entreprendre en cas d'échec de la commande.

Vous pouvez également choisir d'autoriser les utilisateurs autorisés à exécuter des tâches sur vos instances gérées, et vous pouvez choisir d'envoyer une notification par e-mail concernant la réussite ou l'échec de la tâche, ainsi que d'autres informations.



13. Sur la page **Tâches**, vous pouvez ensuite afficher la progression de l'exécution de votre tâche de configuration sur toutes les instances.

Jobs

Jobs

<input type="checkbox"/>	Name	Execution Summary	Instance Family	Instances	Commands	Actions
<input type="checkbox"/>	new-job-test Created on: Jan 31 5:23 PM Created by: nsroot	<div style="width: 75%; background-color: green; height: 10px; margin-bottom: 5px;"></div> 75% In progress.. Started by nsroot on Jan 31 5:23 PM	NetScaler	4	5	<input type="button" value="Abort"/>

## Utiliser les tâches de configuration pour répliquer la configuration d'une instance vers plusieurs instances

February 1, 2024

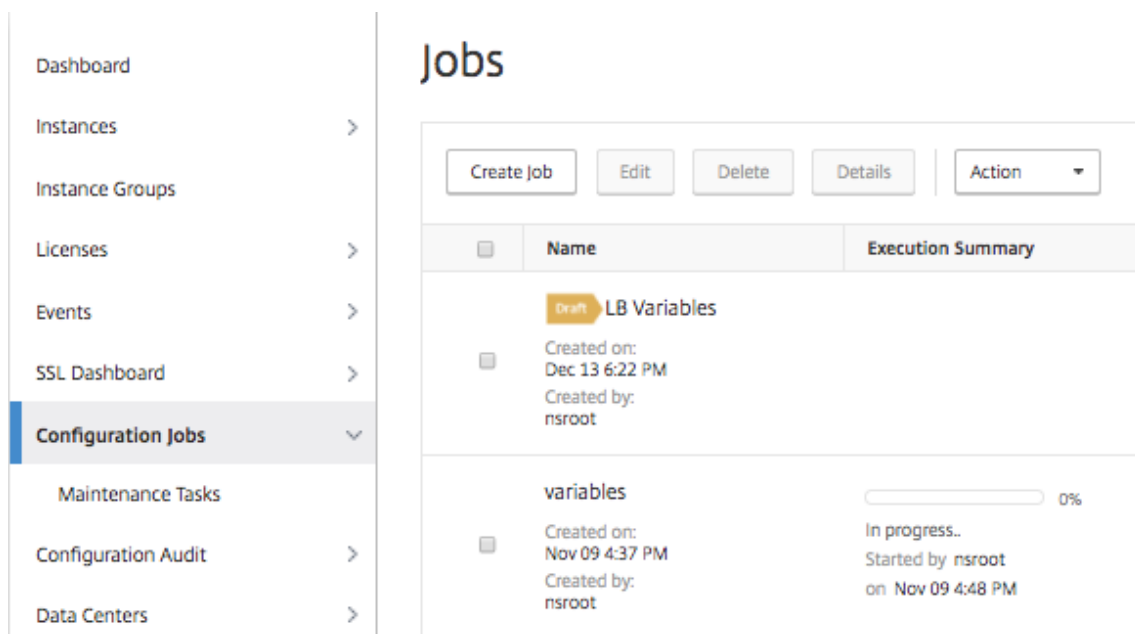
Vous pouvez utiliser la fonctionnalité Configuration Jobs de Citrix ADM pour extraire une configuration particulière d'une instance NetScaler et la répliquer sur plusieurs instances.

Par exemple, vous avez peut-être configuré à la fois l'équilibrage de charge et l'optimisation du front-

end (FEO) sur une instance NetScaler pour votre déploiement. Toutefois, vous souhaitez désormais répliquer uniquement la configuration FEO vers d'autres instances NetScaler.

**Pour récupérer et répliquer la configuration d'une instance vers d'autres instances NetScaler :**

1. Accédez à **Réseaux > Travaux de configuration**, puis cliquez sur **Créer un travail** .



2. Spécifiez le nom de la tâche et le type d'instance.
3. Sélectionnez **Instance** comme **source de configuration** et sélectionnez l'instance source dont vous souhaitez répliquer la configuration. Sélectionnez le type de configuration que vous souhaitez extraire. Si vous sélectionnez « Configuration par durée de temps », définissez la période pendant laquelle vous avez exécuté cette configuration, puis cliquez sur **Extraire**.

Le nombre de commandes exécutées sur cette instance pendant la durée que vous avez sélectionnée est affiché à l'écran, comme le montre l'image ci-dessous.

Job Name\*

replicate-job

### Configuration Editor

Configuration Source

Instance

Source Instance

10.102.29.120

Running Configuration

Saved Configuration

Configuration by time duration

Duration

Today

**Extract**

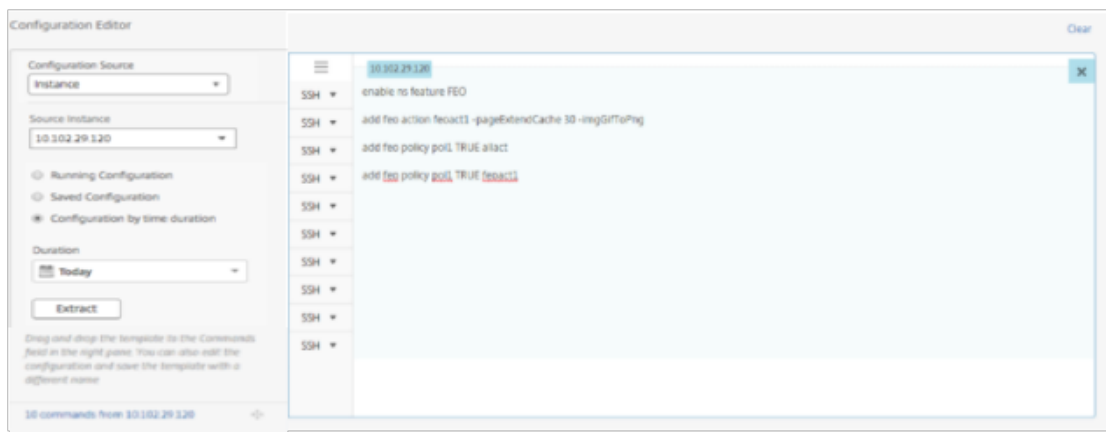
*Drag and drop the template to the Commands field in the right pane. You can also edit the configuration and save the template with a different name*

10 commands from 10.102.29.120

4. Glissez et déposez les **commandes dans le champ Commandes** du volet droit.



Conservez uniquement les commandes liées à FEO et supprimez manuellement les commandes liées à l'équilibrage de charge ou les commandes liées à toute autre configuration, puis cliquez sur **Suivant**.



5. Cliquez sur **Ajouter des instances** et ajoutez les instances sur lesquelles vous souhaitez appliquer la configuration FEO. Cliquez sur **OK**, puis sur **Suivant**.
6. Si vous avez spécifié des variables dans les commandes, dans l'onglet Spécifier les valeurs des variables, cliquez sur **Télécharger le fichier clé d'entrée**. Dans le fichier téléchargé, spécifiez les valeurs des variables, puis chargez le fichier sur Citrix ADM.
7. Sous l'onglet **Aperçu des tâches**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances.
8. Dans l'onglet **Exécuter**, cliquez sur **Terminer** pour exécuter la tâche sur les instances NetScaler sélectionnées.

## Utiliser des variables dans les tâches de configuration

February 1, 2024

Une tâche de configuration est un ensemble de commandes de configuration que vous pouvez exécuter sur une ou plusieurs instances gérées. Lorsque vous exécutez la même configuration sur plusieurs instances, vous souhaitez peut-être utiliser des valeurs différentes pour les paramètres utilisés dans votre configuration. Vous pouvez définir des variables qui vous permettent d'attribuer différentes valeurs pour ces paramètres ou d'exécuter une tâche sur plusieurs instances.

Par exemple, envisagez une configuration d'équilibrage de charge de base dans laquelle vous ajoutez un serveur virtuel d'équilibrage de charge, ajoutez deux services et liez les services au serveur virtuel. À présent, vous souhaitez peut-être avoir la même configuration sur deux instances, mais avec des valeurs différentes pour le serveur virtuel, les noms de services et les adresses IP. Vous pouvez utiliser la fonctionnalité de tâches de configuration pour y parvenir en utilisant des variables pour définir les noms et les adresses IP du serveur virtuel et des services.

Dans cet exemple, les commandes et variables suivantes sont utilisées :

ajouter le nom du serveur lb `vserver`, l'adresse **IP** HTTP et le numéro de **port**

ajouter un service **servicename1** `ipaddress1` HTTP 80

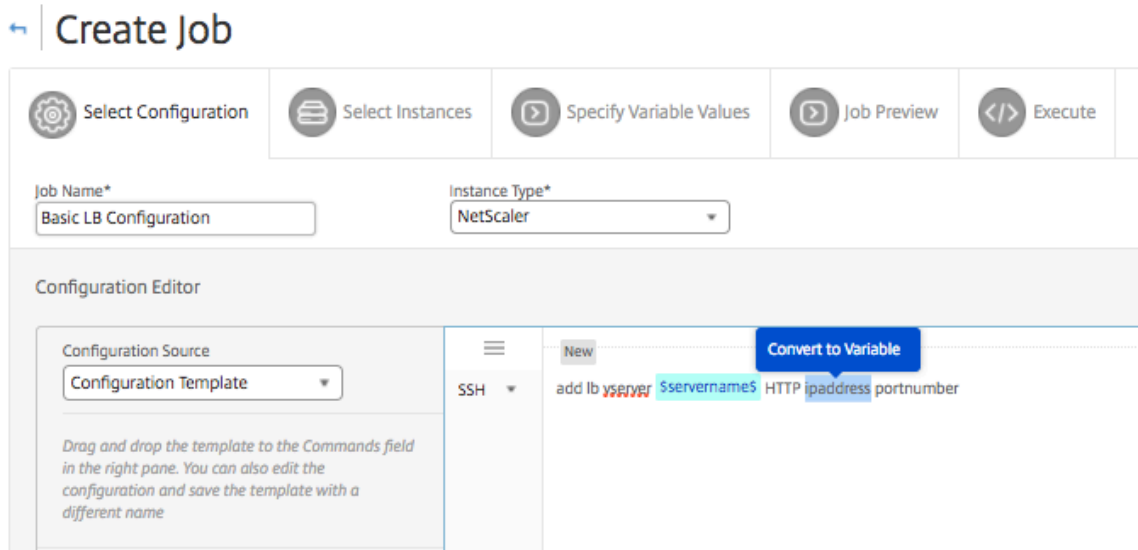
ajouter un service **servicename2** `ipaddress2` HTTP 80

bind lb `vserver` **servername** `servicename1`

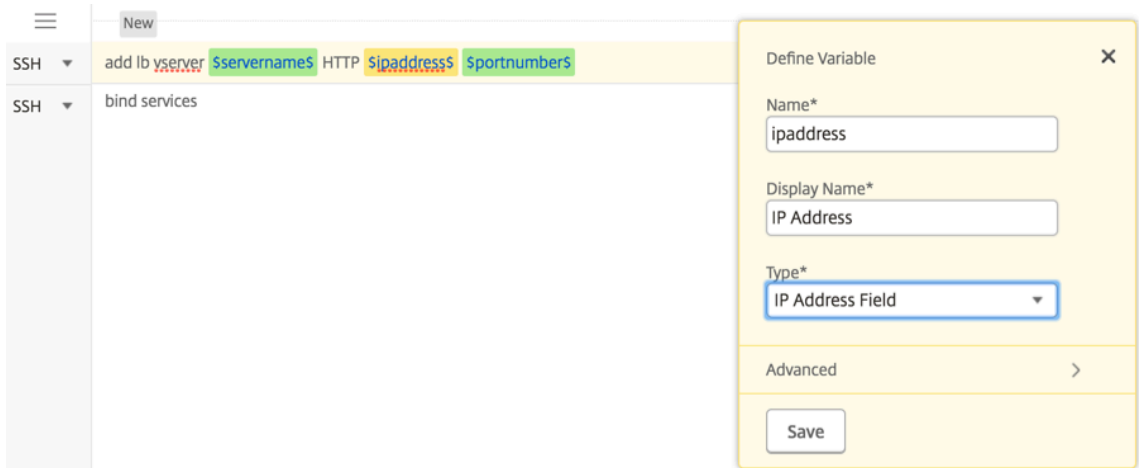
bind lb `vserver` **servername** `servicename2`

### Pour créer une tâche de configuration en définissant des variables dans Citrix ADM :

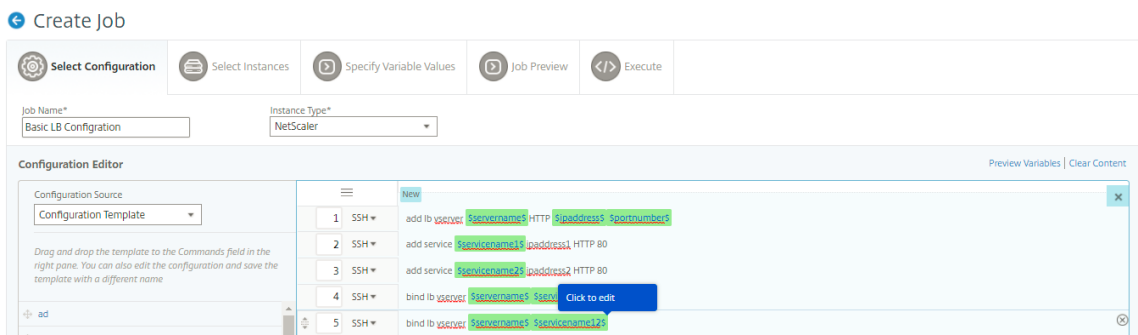
1. Accédez à **Réseaux > Travaux de configuration**.
2. Cliquez sur **Créer une tâche**.
3. Sur la page **Créer une tâche**, sélectionnez les paramètres de tâche personnalisés tels que le nom de la tâche, le type d'instance et le type de configuration.
4. Dans l'Éditeur de configuration, tapez les commandes pour ajouter un serveur virtuel d'équilibrage de charge, deux services et lier les services au serveur virtuel. Double-cliquez pour sélectionner les valeurs que vous souhaitez convertir en variable, puis cliquez sur **Convertir en variable**. Par exemple, sélectionnez l'adresse IP du serveur d'équilibrage de charge `ipaddress`, puis cliquez sur **Convertir en variable** comme indiqué dans l'image ci-dessous.



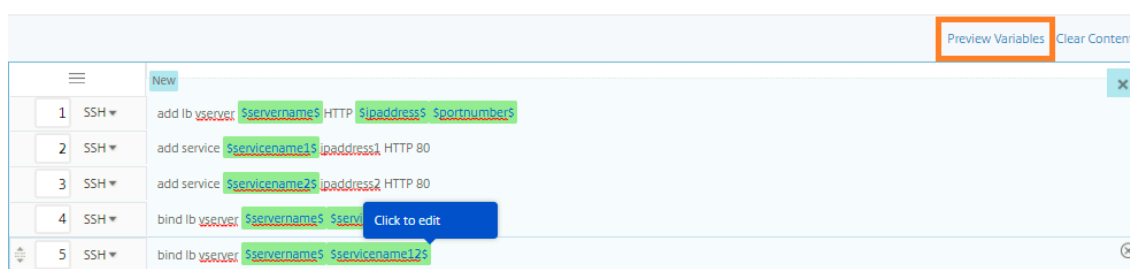
- Une fois que vous voyez des symboles en dollars encadrer la valeur de la variable, cliquez sur la variable pour préciser davantage les détails de la variable, tels que son nom, son nom d’affichage et son type. Vous pouvez également cliquer sur l’option **Avancé** si vous souhaitez spécifier une valeur par défaut pour votre variable. Cliquez sur **Enregistrer**, puis sur **Suivant**.



Tapez le reste de vos commandes et définissez toutes les variables.



6. Vous pouvez consulter toutes les variables que vous avez définies lors de la création ou de la modification d'un travail de configuration dans une vue consolidée unique.
7. Pour afficher toutes les variables dans une seule vue consolidée, procédez de l'une des manières suivantes :
  - Lors de la création d'une tâche de configuration, accédez à **Réseaux > Tâches de configuration**, puis sélectionnez **Créer une tâche**. Sur la page **Créer un travail**, vous pouvez consulter toutes les variables que vous avez ajoutées lors de la création du travail de configuration.
  - Lorsque vous modifiez une tâche de configuration, accédez à **Réseau > Tâches de configuration**, sélectionnez le nom de la tâche et cliquez sur **Modifier**. Sur la page **Configurer la tâche**, vous pouvez consulter toutes les variables qui ont été ajoutées lors de la création de la tâche de configuration.
8. Vous pouvez ensuite cliquer sur l'onglet **Aperçu des variables** pour prévisualiser les variables dans une vue consolidée unique que vous avez définie lors de la création ou de la modification d'une tâche de configuration.



9. Une nouvelle fenêtre contextuelle apparaît et affiche tous les paramètres des variables telles que Nom, Nom d'affichage, Type et valeur par défaut dans un format tabulaire. Vous pouvez également modifier et modifier ces paramètres. Cliquez sur le bouton **Terminé** après avoir modifié l'un des paramètres.

Name*	Display Name*	Type*	Default Value
portnumber	portnumber	Text Field	
ipaddress	ipaddress	Text Field	
servername	servername	Text Field	
servicename1	servicename1	Text Field	
servicename2	servicename2	Text Field	
servicename12	servicename12	Text Field	

Done

10. Vous pouvez ensuite réorganiser les commandes dans l'éditeur de configuration selon les besoins. Vous pouvez déplacer la commande d'une ligne à l'autre en faisant glisser la ligne de commande. Vous pouvez également déplacer ou réorganiser la ligne de commande d'une ligne à n'importe quelle ligne cible en changeant simplement le numéro de ligne de commande dans la zone de texte.
11. Sélectionnez les instances sur lesquelles vous souhaitez exécuter le travail de configuration.
12. Dans l'onglet **Spécifier les valeurs variables**, sélectionnez l'option **Télécharger le fichier d'entrée pour les valeurs variables**, puis cliquez sur **Télécharger le fichier clé d'entrée**. Dans notre exemple, vous devrez spécifier le nom du serveur sur chaque instance, les adresses IP du serveur et des services, les numéros de port et les noms de service. Enregistrez le fichier et téléchargez-le. Si vos valeurs ne sont pas définies avec précision, le système peut déclencher une erreur.
13. Le fichier de clé d'entrée est téléchargé sur votre système local et vous pouvez le modifier en spécifiant les valeurs des variables pour chaque instance NetScaler que vous avez sélectionnée précédemment et en **cliquant sur** Télécharger pour télécharger le fichier de clé d'entrée sur Citrix ADM. Cliquez sur **Suivant**. Le fichier clé d'entrée est téléchargé sur votre système local et vous pouvez le modifier en spécifiant les valeurs des variables pour chaque instance NetScaler que vous avez sélectionnée précédemment.

**Remarque** Dans le fichier clé en entrée, les variables sont définies à trois niveaux :

- Au niveau mondial
- Au niveau du groupe d'instances
- Niveau de l'instance

Les variables globales sont des valeurs variables appliquées à toutes les instances. Les valeurs des variables au niveau du groupe d'instances sont appliquées à toutes les instances définies



dans un groupe. Les valeurs des variables au niveau de l'instance ne sont appliquées qu'à une instance spécifique.

Citrix ADM donne la priorité aux valeurs au niveau de l'instance. Si aucune valeur n'est fournie aux variables pour les instances individuelles, Citrix ADM utilise la valeur fournie au niveau du groupe. Si aucune valeur n'est fournie au niveau du groupe, Citrix ADM utilise la valeur variable fournie au niveau global. Si vous fournissez une entrée pour une variable sur les trois niveaux, Citrix ADM utilise la valeur de niveau d'instance comme valeur par défaut.

14. Cliquez sur **Télécharger** pour télécharger le fichier clé d'entrée sur Citrix ADM. Cliquez sur **Suivant**.

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	#Basic LB	Configuration_variable_input_key_file											
2													
3	#Global	servername	ipaddress	portnumb	servicenar	ipaddress	servicenar	ipaddress2					
4	Global Val	ServerNan	10.102.29.	80	ServiceNai	10.102.29.	ServiceNai	10.102.29.3					
5	#Instance	servername	ipaddress	portnumb	servicenar	ipaddress	servicenar	ipaddress2					
6	10.102.29.	ServerNan	10.102.29.	80	ServiceNai	10.102.29.	ServiceNai	10.102.29.3					
7	10.102.20	ServerNan	10.102.29.	80	ServiceNai	10.102.29.	ServiceNai	10.102.29.3					
8	10.106.15	ServerNan	10.102.29.	80	ServiceNai	10.102.29.	ServiceNai	10.102.29.3					
9													
10													
11													
12													
13													

**Important**

Lorsque vous téléchargez un fichier CSV à partir d'un Mac, Mac stocke le fichier CSV avec des points-virgules au lieu de virgules. Cela entraînera l'échec de la configuration lorsque vous téléchargez le fichier d'entrée et exécutez le travail. Si vous utilisez un Mac, utilisez un éditeur de texte pour apporter les modifications nécessaires, puis téléchargez le fichier.

15. Vous pouvez également attribuer des valeurs de variables communes à toutes les instances et cliquer sur **Télécharger** pour télécharger le fichier clé d'entrée vers Citrix ADM.

Les fichiers d'entrée de clé contenant les valeurs des variables sont conservés (avec le même nom de fichier) dans les tâches de configuration. Vous pouvez afficher et modifier ces fichiers d'entrée que vous avez utilisés et chargés précédemment lors de la création ou de la modification des tâches de configuration.

Pour afficher les tâches de configuration exécutées lors de la création d'une tâche de configuration, accédez à **Réseau > Tâches de configuration**, puis cliquez sur **Créer une tâche**. Dans la page **Créer une tâche**. Dans l'onglet **Spécifier les valeurs des variables**, sélectionnez l'option **Valeurs de variables communes pour toutes les instances** pour afficher les fichiers

téléchargés. Pour modifier les fichiers d'entrée, téléchargez le fichier d'entrée, puis modifiez et chargez les fichiers (en conservant le même nom de fichier).

Pour afficher les tâches de configuration déjà exécutées lors de la modification d'une tâche de configuration, accédez à **Réseau > Tâches de configuration**, sélectionnez le nom de la tâche et cliquez sur **Modifier**. Dans la page **Configurer la tâche**, sous l'onglet **Spécifier les valeurs de variable**, sélectionnez l'option **Valeurs variables communes pour toutes les instances** pour afficher les fichiers chargés. Pour modifier les fichiers d'entrée, téléchargez le fichier d'entrée, puis modifiez et chargez les fichiers (en conservant le même nom de fichier).

16. Sous l'onglet **Aperçu des tâches**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances.
17. Dans l'onglet **Exécuter**, vous pouvez choisir d'exécuter votre tâche maintenant ou de planifier son exécution ultérieurement. Vous pouvez également choisir l'action que Citrix ADM doit entreprendre en cas d'échec de la commande et si vous souhaitez envoyer une notification par e-mail concernant la réussite ou l'échec de la tâche, ainsi que d'autres informations.

**Configure Job**

Select Configuration | Select Instances | Specify Variable Values | Job Preview | **Execute**

You can either execute the job now or schedule to execute the job at a later time. You must also select what action NetScaler MAS should take if a command fails.

On Command Failure\*

Execution Mode\*

**Execution Settings**  
 You can execute a job on a set of instances sequentially (one after the other), or in parallel (at the same time). If a job execution fails on any instance, it does not conti

Execute in Parallel  
 Execute in Sequence  
 Specify User Credentials for this Job

Receive Execution Report Through  
 Email

Cancel | Back | **Finish** | Save and Exit

Après avoir configuré vos tâches et les avoir exécutées, vous pouvez consulter les détails de la tâche en accédant à **Réseaux > Tâches de configuration** et en sélectionnant la tâche que vous venez de configurer. Cliquez sur **Détails** puis sur **Détails des variables** pour voir la liste des variables ajoutées à votre travail.

Jobs / Job Details

### Job Details

Configuration Parameters	Name <b>Basic LB Configuration</b>	Instance Type <b>NetScaler</b>	Commands <b>5</b>
--------------------------	---------------------------------------	-----------------------------------	----------------------

<b>Execution Summary</b>	Instances <b>2</b>	Last Execution <b>Nov 23 5:06 PM</b>	<b>100%</b> C
<b>Variable Details</b>	Variables <b>7</b>		
<b>Execution Parameters</b>	Execution Frequency <b>Once</b>	Next Execution <b>N/A</b>	Execute In Parz

**Variable Details**

Variables  
7

Variable	Display Name	Type
ipaddress	ipaddress	IP Address Field
ipaddress1	ipaddress1	IP Address Field
ipaddress2	ipaddress2	IP Address Field
servicename2	servicename2	Text Field
servername	servername	Text Field
servicename1	servicename1	Text Field

### Remarque

Les valeurs que vous avez fournies pour les variables à l'**ÉTAPE 5** sont conservées par Citrix ADM lorsque vous enregistrez la tâche et la quittez, ou lorsque vous planifiez l'exécution d'une tâche ultérieurement.

## Créer des tâches de configuration à partir de commandes correctives

February 1, 2024

Vous pouvez utiliser la fonctionnalité de modèle d'audit dans Citrix Application Delivery Management (ADM) pour surveiller les modifications de configuration des instances Citrix ADC gérées et résoudre les erreurs de configuration.

Le flux de travail typique pour l'audit des modifications de configuration à l'aide de modèles d'audit se compose des étapes suivantes :

1. Créez un modèle d'audit avec un ensemble de commandes Citrix ADC valides/attendues pour auditer les configurations d'instance.
2. Sélectionnez les instances Citrix ADC sur lesquelles vous souhaitez exécuter le modèle d'audit pour vérifier les différences entre la configuration en cours d'exécution et les configurations attendues.
3. Comprendre les commandes différentielles/correctrices et utiliser la fonctionnalité « Create Job » pour obtenir les configurations de l'instance à l'état souhaité

Imaginez un scénario dans lequel plusieurs administrateurs gèrent cinq instances Citrix ADC. Tous ces administrateurs mettent à jour la configuration de l'instance existante au fur et à mesure que des modifications sont nécessaires. Le super administrateur veut s'assurer qu'un certain ensemble de configuration importante reste intact, indépendamment des modifications apportées par d'autres administrateurs. Dans ce cas d'utilisation, le super administrateur crée un modèle de configuration censé être présent sur les instances Citrix ADC et l'exécute sur les instances. Citrix ADM compare la configuration du modèle d'audit à la configuration en cours d'exécution et signale toute incompatibilité dans le tableau de bord **Audit de configuration**.

Si vous remarquez une modification de la configuration de certaines instances, vous pouvez utiliser la fonctionnalité de commandes correctives Citrix ADM pour créer une tâche de configuration avec les commandes de configuration modifiées et corrigées pour des instances Citrix ADC spécifiques.

S'il existe une différence entre la configuration du modèle d'audit et la configuration en cours d'exécution, un message d'état **Différent existe** apparaît sur la page **Rapport d'audit**. En cliquant sur le lien **Diff Exist**, vous accédez à la page **Configuration Diff**, où vous pouvez afficher la commande corrective. Vous pouvez également utiliser ces commandes correctives pour créer une tâche de configuration et l'exécuter sur des instances Citrix ADC spécifiques afin de rétablir la configuration souhaitée.

### **Pour créer une tâche de configuration à partir de commandes correctives sur Citrix ADM**

1. Accédez à **Réseaux > Audit de configuration**.
2. Sur la page **Audit de configuration**, cliquez à l'intérieur de l'un des deux graphiques en donut pour accéder à la page **Rapports d'audit**.
3. Cliquez sur le lien **Diff Exists** (sous la colonne **Saved vs Running Diff** du tableau) pour l'instance pour laquelle vous souhaitez corriger les commandes de configuration. La page **Configuration Diff** apparaît, répertoriant les différences entre la configuration enregistrée, la configuration en cours d'exécution et la configuration de correction pour cette instance.

## Audit Reports

Running Configuration		Saved Configuration		Save configuration	Action	
Instances	Last Updated	Saved vs Running Diff	Template vs Run			
10.102.29.191	Tue, 13 Dec 2016 15:43:38 GMT	Diff Exists	NA			
10.102.29.205	Tue, 13 Dec 2016 15:43:36 GMT	Diff Exists	NA			
HA-Node2-demo-NetScalerVPX (10.102.122.92-10.102.122.93)	Tue, 13 Dec 2016 15:43:34 GMT	Diff Exists	NA			
10.102.29.80	Tue, 13 Dec 2016 15:43:35 GMT	No Diff	NA			
10.102.29.60	Tue, 13 Dec 2016 15:43:36 GMT	No Diff	NA			

4. Cliquez sur **Créer un travail** pour accéder à la page **Créer un travail**, sur laquelle les commandes correctives ont été préremplies. Pour obtenir des instructions sur la façon de créer un travail de configuration, consultez [Comment créer un travail de configuration sur Citrix ADM](#).

Configuration Diff

Saved vs Running Diff of Device: (10.102.29.191) Create Job Export all the corrective commands

Saved Configuration	Running Configuration	Correction Configuration
	bind serviceGroup servicegroup-nmas1 10.10.10.1 80	unbind serviceGroup servicegroup-nmas1 10.10.10.1 80
	bind lb vserver nmas-ha-lb service_nmas3	unbind lb vserver nmas-ha-lb service_nmas3
	add service service_nmas3 10.102.29.54 HTTP 80 -gsib NONE -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp OFF -crtTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO	rm service service_nmas3
	add server 10.102.29.54 10.102.29.54	rm server 10.102.29.54
	add server 10.10.10.1 10.10.10.1	rm server 10.10.10.1
set appflow param -templateRefresh 3600 -httpUri ENABLED -httpCookie ENABLED -httpReferer ENABLED -httpMethod ENABLED -httpHost ENABLED -httpUserAgent ENABLED -httpContentType ENABLED	set appflow param -templateRefresh 60 -httpUri ENABLED -httpCookie ENABLED -httpReferer ENABLED -httpMethod ENABLED -httpHost ENABLED -httpUserAgent ENABLED -httpContentType ENABLED	set appflow param -templateRefresh 3600 -httpUri ENABLED -httpCookie ENABLED -httpReferer ENABLED -httpMethod ENABLED -httpHost ENABLED -httpUserAgent ENABLED -httpContentType ENABLED

Close

## Répliquez la configuration en cours et enregistrée d'une instance NetScaler vers une autre

February 1, 2024

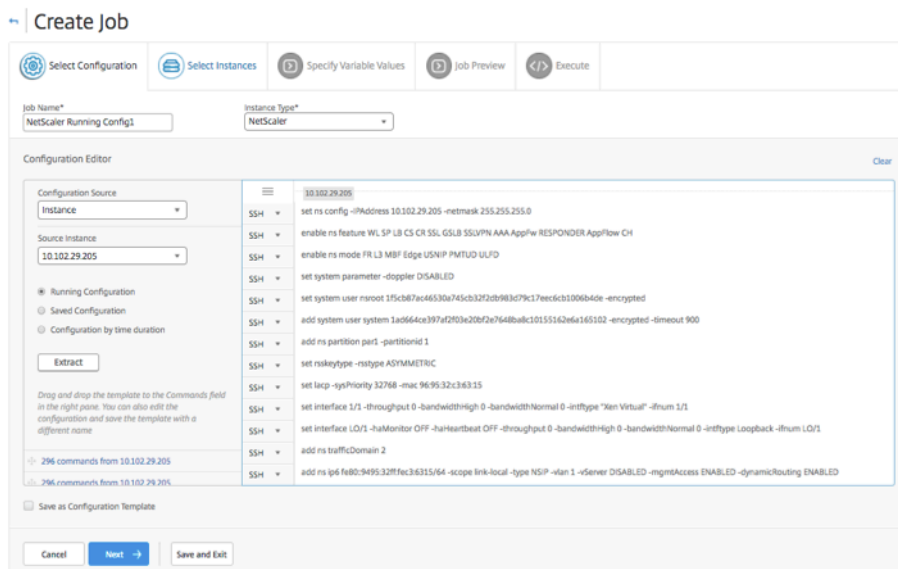
24 mai 2018

Vous pouvez désormais répliquer la configuration d'une instance NetScaler sur d'autres instances. Lorsque vous configurez une tâche dans Citrix ADM, sélectionnez une instance comme source de configuration et choisissez la configuration en cours d'exécution ou enregistrée de l'instance sélectionnée.

Par exemple, lorsque vous sélectionnez **Configuration en cours d'exécution** et que vous cliquez sur **Extraire**, Citrix ADM envoie une demande à l'instance NetScaler sélectionnée pour localiser la configuration en cours d'exécution et l'affiche sous forme de modèle. Vous pouvez glisser-déposer le modèle dans le champ **Commandes** du volet droit. Vous pouvez modifier les commandes, les paramètres et les instances.

**Pour répliquer les commandes de configuration en cours d'exécution et enregistrées d'une instance vers une autre instance sur Citrix ADM :**

1. Accédez à **Réseaux > Tâches de configuration**, puis cliquez sur **Créer une tâche**.
2. Spécifiez le nom de la tâche et le type d'instance. Par exemple, spécifiez *NetScaler RunningConfig1* comme nom de votre tâche et le type d'instance comme *NetScaler*.
3. Sélectionnez **Instance** comme **source de configuration**, sélectionnez l'instance source dont vous souhaitez répliquer la configuration sur d'autres instances.
4. Les trois options suivantes s'affichent :
  - Configuration en cours d'exécution
  - Configuration enregistrée
  - Configuration par durée
5. Choisissez **Exécution de la configuration**, puis cliquez sur **Extraire**. Le nombre de commandes de configuration en cours d'exécution exécutées sur cette instance est affiché.



6. Glissez et déposez les **commandes dans le champ Commandes** du volet droit.
7. Vous pouvez modifier les commandes dans le champ Commandes. Par exemple, si les commandes extraites visent à configurer une instance NetScaler. Cela peut inclure l'ajout de partitions,

la configuration de l'équilibrage de charge, la liaison du serveur d'équilibrage de charge aux services, etc. Vous souhaitez peut-être modifier vos commandes afin de configurer vos nouvelles instances NetScaler sans partitions. Donc, pour supprimer les partitions, supprimez manuellement les commandes liées à la création de partitions et cliquez sur **Suivant**.

8. Cliquez sur **Ajouter des instances** et ajoutez les instances sur lesquelles vous souhaitez appliquer les commandes de configuration en cours d'exécution. Cliquez sur **OK**, puis sur **Suivant**.
9. Si vous avez spécifié des variables dans les commandes, sous l'onglet **Spécifier les valeurs de variable**, cliquez sur **Télécharger le fichier de clé d'entrée**. Dans le fichier téléchargé, spécifiez les valeurs des variables, puis chargez le fichier sur Citrix ADM.
10. Sous l'onglet **Aperçu des tâches**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances.
11. Dans l'onglet **Exécuter**, vous pouvez choisir d'exécuter votre tâche maintenant ou de planifier son exécution ultérieurement. Vous pouvez également choisir l'action que Citrix ADM doit entreprendre en cas d'échec de la commande et si vous souhaitez envoyer une notification par e-mail concernant la réussite ou l'échec de la tâche, ainsi que d'autres informations.

## Réutiliser les tâches de configuration exécutées

February 1, 2024

Les tâches de configuration vous permettent de créer un ensemble de commandes de configuration que vous pouvez exécuter sur une ou plusieurs instances gérées. Vous pouvez également exécuter le même ensemble de tâches de configuration enregistrées après avoir modifié les commandes, les paramètres, la source de configuration et les instances de la tâche. Cela est utile lorsque les mêmes ensembles de commandes doivent être exécutés sur une instance différente, ou lorsque la tâche rencontre une erreur et arrête toute exécution ultérieure.

Citrix Application Delivery Management (ADM) fournit une fonction permettant de réexécuter les tâches terminées. Avec cette fonction, les tâches qui sont complètement exécutées peuvent être réexécutées sans changer le nom de la tâche.

**Remarque** Vous ne pouvez réexécuter que les tâches exécutées lorsque le mode d'exécution est « Maintenant ».

### Pour modifier les tâches terminées :

1. Sur la page d'accueil de Citrix ADM, accédez à **Réseaux > Tâches de configuration**.

2. Dans la page **Tâches**, sélectionnez un travail qui affiche le résumé de l'exécution comme terminé, puis cliquez sur **Modifier**. Vous pouvez également modifier une tâche de configuration planifiée.
3. Sur la page **Configurer la tâche**, vous pouvez voir que le nom de la tâche et le type d'instance ne sont pas modifiables. Vous pouvez modifier d'autres champs tels que la source de configuration, ajouter des instances, modifier les valeurs des variables et définir les paramètres d'exécution.
4. Cliquez sur **Terminer** pour exécuter à nouveau la tâche de configuration.

**Jobs** ↻ 📄

Search ▾

<input checked="" type="checkbox"/>	Name	Execution Summary	Instance Type	Instances	Commands	Actions
<input checked="" type="checkbox"/>	ns-config-syslog Created on: Apr 20 9:14 PM Created by: nsroot	Completed Started by nsroot on Apr 20 9:14 PM	NetScaler	1	3	<input type="button" value="Abort"/>

### Remarque

Vous pouvez également sélectionner la tâche et cliquer à nouveau sur **Exécuter** pour exécuter la tâche sans modifier la source, l'instance et les commandes. Cela est utile lorsque vous devez exécuter le même ensemble de commandes sur les mêmes instances. Parfois, le travail peut rencontrer une erreur transitoire du côté serveur, et vous devrez peut-être exécuter à nouveau la tâche.

**Jobs** ↻ 📄

Search ▾

<input checked="" type="checkbox"/>	Name	Execution Summary	Instance Type	Instances	Commands	Actions
<input checked="" type="checkbox"/>	ns-config-syslog Created on: Apr 20 9:14 PM Created by: nsroot	Completed Started by nsroot on Apr 20 9:14 PM	NetScaler	1	3	<input type="button" value="Abort"/>

## Planifier les tâches créées à l'aide de modèles intégrés

February 1, 2024

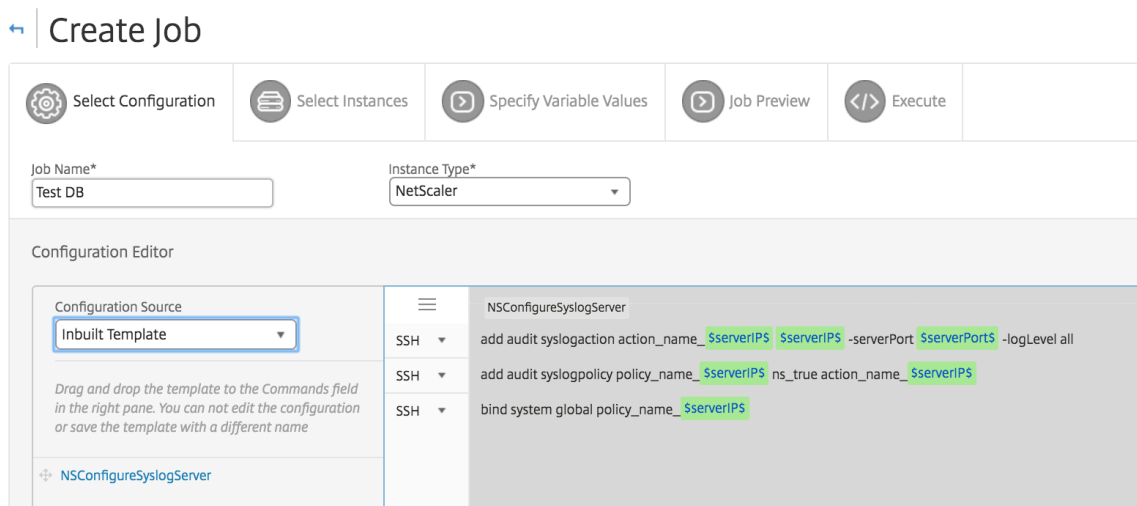
Vous pouvez planifier une tâche à l'aide de l'option de modèle intégrée. Une tâche est un ensemble de commandes de configuration que vous pouvez exécuter sur une ou plusieurs instances gérées. Par



exemple, utilisez l'option de modèle intégrée pour planifier une tâche de configuration des serveurs syslog. Vous pouvez également choisir d'exécuter la tâche immédiatement ou de planifier son exécution à un stade ultérieur.

## Pour planifier un travail à l'aide de modèles intégrés dans Citrix Application Delivery Management (ADM)

1. Dans Citrix ADM, accédez à **Réseaux** > **Tâches de configuration**, puis cliquez sur **Créer un tâche**.
2. Dans la page **Créer un travail**, sous l'onglet **Sélectionner une configuration**, spécifiez le **nom du travail** et sélectionnez le **type d'instance** dans la liste déroulante.
3. Sélectionnez **Modèle intégré** dans la liste déroulante **Source de configuration**. Faites glisser la commande **\*NSConfigureSyslogServer** vers le volet droit, puis cliquez sur **Suivant**.



4. Sous l'onglet **Sélectionner des instances**, cliquez sur **Ajouter** des instances, sélectionnez les instances sur lesquelles vous souhaitez exécuter le travail, puis cliquez sur **OK**.
5. Cliquez sur **Suivant**. Dans l'onglet **Spécifier les valeurs des variables**, sélectionnez l'une des options suivantes pour spécifier des variables pour vos instances :
  - **Valeurs de variables à partir d'un fichier d'entrée** : téléchargez un fichier d'entrée pour entrer des valeurs pour les variables que vous avez définies dans vos commandes. Chargez ensuite le fichier sur le serveur Citrix ADM.
  - **Valeurs de variables communes pour toutes les instances** —Spécifiez l'adresse IP et le port du serveur Syslog.
6. Sous l'onglet **Aperçu des tâches**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances.

7. Cliquez sur **Suivant**.
  8. Sous l'onglet **Exécuter**, définissez les conditions suivantes :
    - **En cas d'échec** de commande : si une commande échoue, vous pouvez soit ignorer les erreurs et continuer à exécuter la tâche, soit arrêter l'exécution de la tâche. Choisissez l'action que vous souhaitez exécuter dans la liste déroulante.
    - **Mode d'exécution** : vous pouvez exécuter la tâche maintenant ou planifier une exécution ultérieure. Si vous souhaitez planifier le travail ultérieurement, vous devez spécifier les paramètres de fréquence d'exécution pour ce travail. Choisissez la planification à suivre dans la liste déroulante.
  9. Vous pouvez également exécuter une tâche sur un ensemble d'instances de manière séquentielle ou en parallèle en sélectionnant la méthode requise dans **Paramètres d'exécution**. Si l'exécution d'une tâche échoue sur une instance, elle ne se poursuit pas sur les instances restantes.
- Vous pouvez choisir d'autoriser les utilisateurs autorisés à exécuter des tâches sur vos instances gérées. Une notification par e-mail peut également être envoyée concernant le succès ou l'échec du travail, ainsi que d'autres détails.
10. Cliquez sur **Terminer**.

← | Create Job

Select Configuration | Select Instances | Specify Variable Values | Job Preview | **Execute**

You can either execute the job now or schedule to execute the job at a later time. You must also select what action NetScaler MAS should take if a command fails.

On Command Failure\*

Execution Mode\*

Execution Settings  
 You can execute a job on a set of instances sequentially (one after the other), or in parallel (at the same time). If a job execution fails on any instance, it does not continue execution on the remaining instances

Execute in Parallel  
 Execute in Sequence

Specify User Credentials for this job

User Name\*

Password\*

Receive Execution Report Through  
 Email

Cancel | ← Back | **Finish** | Save and Exit

## Utiliser les tâches de maintenance pour mettre à niveau les instances NetScaler SDX

February 1, 2024

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 groupée unique, vous utilisez une tâche intégrée dans Citrix ADM. Grâce à cette tâche intégrée, vous pouvez mettre à niveau le service de gestion NetScaler SDX, Citrix Hypervisor, ainsi que les packs et correctifs supplémentaires pour Citrix Hypervisor.

### Pour mettre à niveau les instances NetScaler SDX à l'aide de Citrix ADM :

1. Accédez à **Réseaux** > Tâches de **configuration** Tâches de **maintenance**.
2. Cliquez sur **Créer une tâche**. Sur la page Créer une tâche, sélectionnez la tâche intégrée Mettre à niveau **NetScaler SDX** pour mettre à niveau vos instances NetScaler SDX. Cliquez sur **Continuer**.
3. Sur la page Mettre à niveau une ou plusieurs appliances NetScaler, dans l'onglet **Sélection** des instances, spécifiez le **nom de la tâche** et cliquez sur **Ajouter des instances**.
4. Sélectionnez les instances ou groupes d'instances cibles que vous souhaitez mettre à niveau.
5. Après avoir ajouté les instances ou les groupes d'instances NetScaler, cliquez sur **suivant** pour lancer la validation préalable à la mise à niveau sur les instances sélectionnées. L'écran indique la progression de la pré-validation de chacune des instances NetScaler.
6. Sur la page **Modifier la mise à niveau des appliances NetScaler**, sélectionnez l'onglet **Mettre à niveau**. Dans le menu **Image logicielle**, sélectionnez **Local** (votre machine locale) ou **Appliance** (le fichier de génération doit être présent sur Citrix ADM).
7. Vous pouvez également voir si des instances présentent des erreurs de mise à niveau de pré-validation. Ces erreurs sont affichées sous forme de message. Les messages indiquent les erreurs liées à l'espace disque, au disque dur et à la personnalisation de l'utilisateur. Si vous ne souhaitez pas continuer avec les instances qui ont échoué la vérification de mise à niveau de pré-validation, vous pouvez supprimer les instances. Pour supprimer les instances, sélectionnez-les et cliquez sur **Supprimer**.
8. Sous l'onglet **Planifier la tâche**, vous pouvez également définir les détails d'exécution dans lesquels vous pouvez effectuer le processus de mise à niveau maintenant ou le planifier pour une date ultérieure. Vous pouvez également choisir de sauvegarder votre instance NetScaler SDX, de recevoir un rapport d'exécution par e-mail ou d'effectuer une mise à niveau en deux étapes pour les nœuds en haute disponibilité.

La mise à niveau en deux étapes pour les nœuds dans HA vous donne la possibilité d'effectuer la mise à niveau immédiatement ou de planifier une heure pour les nœuds à mettre à jour les uns après les autres. La synchronisation et la propagation des nœuds sont désactivées jusqu'à ce que les deux nœuds soient correctement mis à niveau.

## Création de tâches de configuration pour les instances Citrix SD-WAN WANOP

February 1, 2024

Une tâche est un ensemble de commandes de configuration que vous pouvez créer et planifier sur une ou plusieurs instances gérées. Pour les instances Citrix SD-WAN WANOP, vous pouvez utiliser les options suivantes pour créer des tâches :

- **Modèle de configuration** : vous pouvez utiliser l'éditeur de configuration pour saisir des commandes CLI, enregistrer la configuration en tant que modèle et l'utiliser pour configurer des tâches.
- **Modèle intégré** : Vous pouvez choisir parmi une liste de modèles de configuration. Ces modèles fournissent les syntaxes des commandes CLI et vous permettent de spécifier des valeurs pour les variables. Les modèles intégrés sont répertoriés, avec leur description dans le tableau ci-dessous.
- **Fichier** : Vous pouvez télécharger un fichier de configuration à partir de votre machine locale et créer des tâches.

Une fois qu'une tâche est créée, vous pouvez choisir d'exécuter la tâche immédiatement ou de planifier l'exécution ultérieure. Vous pouvez également définir la fréquence d'exécution

---

Modèle intégré	Description
EnableCloudBridgeWANOpt	Active le trafic via l'appliance Citrix SD-WAN WANOP.
DisableCloudBridgeWANOpt	Désactive le trafic via l'appliance Citrix SD-WAN WANOP.
RestartCloudBridgeWANOpt	Redémarre l'appliance WANOP Citrix SD-WAN.
RestoreConfig	Restaure la configuration de l'appliance Citrix SD-WAN WANOP.

Modèle intégré	Description
AddLink	La création ou la définition de liens permettent à l'apppliance WANOP SD-WAN d'éviter la congestion et la perte des liaisons et d'effectuer la mise en forme du trafic. Vous pouvez définir la bande passante maximale envoyée ou reçue sur le lien et spécifier également qu'il s'agit du trafic côté LAN ou WAN.
ConfigureBandwidth	Définit les limites de bande passante et les autres paramètres de gestion de bande passante
AddUser	Ajoute un nouvel utilisateur auquel vous pouvez attribuer des privilèges.
AddUserAdvancedPlatform	Ajoute un nouvel utilisateur vous permet d'attribuer des privilèges non disponibles dans le modèle AddUser.
AddService-class	Crée une classe de service pour l'apppliance Citrix SD-WAN WANOP avec un ou plusieurs filtres de classe de service et l'active.
SetApplication	Définit la définition du classificateur d'applications.
AddorRemoveVideoCachingPorts	Ajoute ou supprime le numéro de port auquel la source vidéo peut envoyer ou recevoir des données. Le port par défaut est 80.
RemoveVideoCachingSource	Supprime une ou plusieurs sources de mise en cache vidéo. Spécifiez l'adresse IP de la source vidéo ou le nom de domaine.
RemoveAllVideoCaching	Supprime toutes les sources de mise en cache vidéo disponibles.
VideoCachingState	Active ou désactive la fonctionnalité de mise en cache vidéo sur les appliances Citrix SD-WAN WANOP.
ClearVideoCaching	Efface le cache vidéo ou les statistiques de mise en cache vidéo.
SetVideoCaching	Définit la taille maximale des objets mis en cache. Un objet supérieur à cette limite n'est pas mis en cache. Par défaut, la taille maximale de l'objet de mise en cache est de 100 Mo.

---

Modèle intégré	Description
AddVideoCachingSource	Ajoute l'adresse IP ou le nom de domaine de la source vidéo. Inclut des options permettant d'activer ou de désactiver la mise en cache vidéo pour cette source.
ConfigureRemotelicenseServer	Configure le serveur de licences centralisé. Spécifiez le modèle du serveur de licences, l'adresse IP et le numéro de port.
ConfigureLocalLicenseServer	Définit l'emplacement du serveur de licences comme étant local.
InstallCACert	Installe les certificats d'autorité de certification sur l'appliance WANOP Citrix SD-WAN. Spécifiez le nom du certificat, le nom du fichier et le mot de passe du keystore.
InstallCombinedCerKey	Installe un fichier de paire de clés de certificat SSL combiné.
InstallSeperateCerKey	Installe le certificat SSL et la clé sous forme de fichiers distincts.
EnableWCCP	Active le mode de déploiement WCCP.
AddWCCPServiceGroup	Ajoute une nouvelle définition de groupe de services WCCP pour l'appliance Citrix SD-WAN WANOP.
DisableWCCP	Désactive le mode de déploiement WCCP.
AddTrafficShapingPolicy	Crée une stratégie de régulation du trafic pour l'appliance Citrix SD-WAN. La stratégie contrôle la bande passante réseau.
SetTrafficShapingPolicy	Modifie la stratégie de mise en forme du trafic pour l'appliance WANOP Citrix SD-WAN. La stratégie contrôle la bande passante réseau.
AddVideoPrePopulation	Crée une entrée de pré-population vidéo, qui vous permet de télécharger et de mettre en cache une vidéo à l'avance. Vous pouvez également spécifier à quel moment mettre en cache une vidéo.
UpdateVideoPrePopulation	Modifie une entrée de préremplissage vidéo, qui indique à quel moment mettre en cache une vidéo.

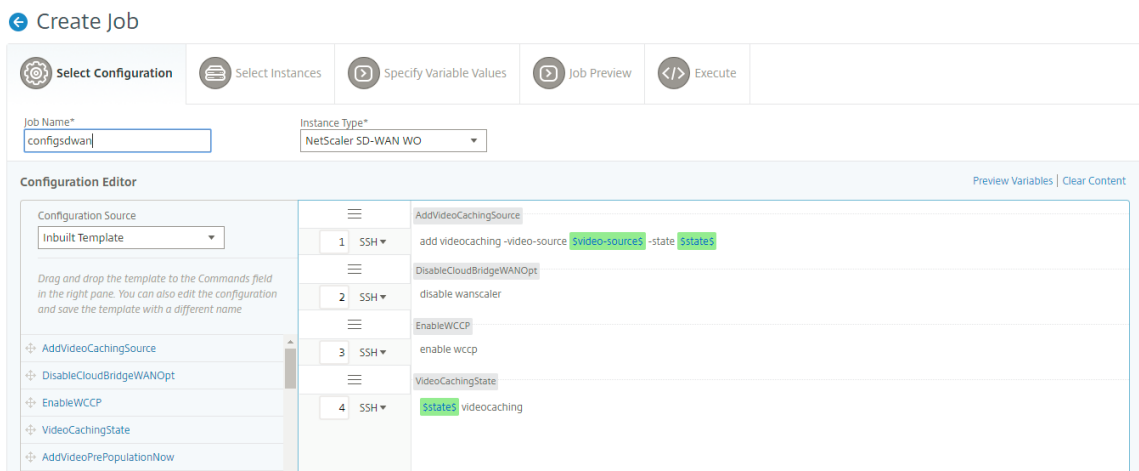
Modèle intégré	Description
AddVideoPrePopulationNow	Configure la prépopulation vidéo, ce qui vous permet de télécharger et de mettre en cache immédiatement une vidéo. Vous pouvez contrôler la façon dont vous souhaitez télécharger et mettre en cache des vidéos à partir de l'URL ou des URL.
VideoPrePopulationState	Modifie, démarre, met à jour ou supprime le pré-remplissage vidéo.
ConfigureSyslogServer	Définit l'adresse IP et le numéro de port du serveur Syslog.
ConfigureAlert	Configure le niveau d'alerte.

**Pour créer une tâche de configuration pour les instances WANOP Citrix SD-WAN :**

1. Dans Citrix ADM, accédez à **Réseaux > Tâches de configuration**, puis cliquez sur **Créer une tâche**.
2. Dans la page **Créer un travail**, sous l'onglet **Sélectionner une configuration**, spécifiez le **nom du travail**.
3. Dans le champ **Type d'instance**, sélectionnez **Citrix SD-WAN WO**.
4. Dans la liste déroulante **Source de configuration**, sélectionnez une option pour créer un travail.

**Remarque**

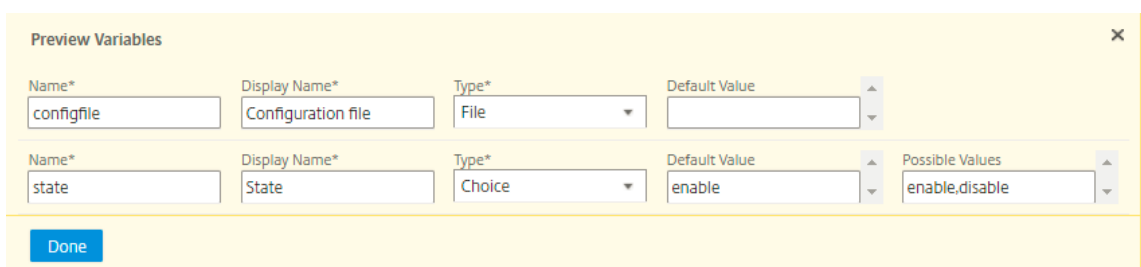
Sélectionnez **Enregistrer en tant que modèle de configuration** et spécifiez un nom pour enregistrer la configuration en tant que modèle et la réutiliser.



5. Vous pouvez consulter toutes les variables que vous avez définies lors de la création ou de la modification d'un travail de configuration dans une vue consolidée unique.
6. Pour afficher toutes les variables dans une seule vue consolidée, procédez de l'une des manières suivantes :
  - Lors de la création d'une tâche de configuration, accédez à **Réseaux > Tâches de configuration**, puis sélectionnez **Créer une tâche**. Sur la page **Créer un travail**, vous pouvez consulter toutes les variables que vous avez ajoutées lors de la création du travail de configuration.
  - Lorsque vous modifiez une tâche de configuration, accédez à **Réseau > Tâches de configuration**, sélectionnez le nom de la tâche et cliquez sur **Modifier**. Sur la page **Configurer la tâche**, vous pouvez consulter toutes les variables qui ont été ajoutées lors de la création de la tâche de configuration.
7. Vous pouvez ensuite cliquer sur l'onglet **Aperçu des variables** pour prévisualiser les variables dans une vue consolidée unique que vous avez définie lors de la création ou de la modification d'une tâche de configuration.



8. Une nouvelle fenêtre contextuelle apparaît et affiche tous les paramètres des variables telles que Nom, Nom d'affichage, Type et valeur par défaut dans un format tabulaire. Vous pouvez également modifier et modifier ces paramètres. Cliquez sur le bouton **Terminé** après avoir modifié l'un des paramètres.



9. Cliquez sur **Suivant**, puis sur l'onglet **Sélectionner des instances**, cliquez sur **Ajouter des instances**. Sélectionnez les instances sur lesquelles vous souhaitez exécuter la tâche, puis cliquez sur **OK**.
10. Cliquez sur **Suivant**, puis sur l'onglet **Spécifier les valeurs de variable**, sélectionnez l'une des options suivantes pour spécifier des variables pour vos instances :



- **Télécharger le fichier d'entrée pour les valeurs des variables** : cliquez sur **Télécharger le fichier clé d'entrée** pour télécharger un fichier d'entrée. Dans le fichier d'entrée, entrez des valeurs pour les variables que vous avez définies dans vos commandes, puis téléchargez le fichier sur le serveur Citrix ADM.
- **Valeurs de variables communes pour toutes les instances** : entrez des valeurs pour les variables. Les variables varient en fonction du modèle sélectionné.

Les fichiers d'entrée contenant les valeurs des variables sont conservés (avec le même nom de fichier) dans les tâches de configuration. Vous pouvez afficher et modifier ces fichiers d'entrée que vous avez utilisés et chargés précédemment lors de la création ou de la modification des tâches de configuration.

Pour afficher les tâches de configuration exécutées lors de la création d'une tâche de configuration, accédez à **Réseau > Tâches de configuration**, puis cliquez sur **Créer une tâche**. Dans la page **Créer une tâche**. Sous l'onglet **Spécifier les valeurs variables**, sélectionnez l'option **Valeurs variables communes pour toutes les instances** pour afficher les fichiers téléchargés. Pour modifier les fichiers d'entrée, téléchargez le fichier d'entrée, puis modifiez et chargez les fichiers (en conservant le même nom de fichier).

Pour afficher les tâches de configuration déjà exécutées lors de la modification d'une tâche de configuration, accédez à **Réseau > Tâches de configuration**, sélectionnez le nom du travail et cliquez sur **Modifier**. Dans la page **Configurer le travail**, sous l'onglet **Spécifier les valeurs de variable**, sélectionnez l'option **Valeurs variables communes pour toutes les instances** pour afficher les fichiers téléchargés. Pour modifier les fichiers d'entrée, téléchargez le fichier d'entrée, puis modifiez et téléchargez les fichiers (en conservant le même nom de fichier)

11. Cliquez sur **Suivant**, dans l'onglet **Aperçu de la tâche**, vous pouvez évaluer et vérifier les commandes à exécuter en tant que tâche.
12. Cliquez sur **Suivant**, sous l'onglet **Exécuter**, définissez les conditions suivantes :

- **En cas d'échec d'une commande** : Que faire en cas d'échec d'une commande : ignorez les erreurs et poursuivez le travail, ou arrêtez toute exécution ultérieure du travail. Choisissez une action dans la liste déroulante.
- **Mode d'exécution** : exécutez le travail immédiatement ou planifiez l'exécution pour une période ultérieure. Si vous planifiez l'exécution pour une période ultérieure, vous devez spécifier les paramètres de fréquence d'exécution pour la tâche. Choisissez la planification à suivre dans la liste déroulante **Fréquence d'exécution**.

← Create Job

Select Configuration | Select Instances | Specify Variable Values | Job Preview | Execute

You can either execute the job now or schedule to execute the job at a later time. You must also select what action NetScaler MAS should take if a command fails.

On Command Failure\*

Execution Mode\*

Execution Settings  
 You can execute a job on a set of instances sequentially (one after the other), or in parallel (at the same time). If a job execution fails on any instance, it does not continue execution on the remaining instances.

Execute in Parallel  
 Execute in Sequence

Receive Execution Report Through  
 Email

Cancel | Back | Finish | Save and Exit

13. Sous **Paramètres d'exécution**, sélectionnez cette option pour exécuter le travail de manière séquentielle (l'un après l'autre) ou en parallèle (en même temps).
14. Pour qu'un rapport d'exécution de tâche soit envoyé par e-mail à une liste de destinataires, cochez la case **E-mail** dans la section **Recevoir le rapport d'exécution via** . Dans la liste déroulante qui s'affiche, choisissez une liste de distribution de courrier électronique. Pour créer une liste de distribution d'e-mails, cliquez sur l'icône **+** et entrez les adresses e-mail des destinataires, ainsi que les détails du serveur de messagerie.
15. Cliquez sur **Terminer**.

## Utiliser le modèle de configuration maître

February 1, 2024

L'utilisation d'un modèle de configuration maître est une option flexible pour créer et déployer une configuration maître sur plusieurs instances Citrix ADC.

En tant qu'administrateur, vous pouvez modifier la configuration et enregistrer les licences, certificats et autres fichiers sur l'instance ADC. Vous pouvez enregistrer la nouvelle configuration en tant que modèle de configuration maître (fichier .conf).

Pour enregistrer votre modèle de configuration principal à partir d'une instance ADC, vous pouvez effectuer l'une des opérations suivantes :

- À l'invite de commandes, entrez **save ns config**. La configuration est enregistrée dans la mémoire FLASH de l'instance dans le fichier /nsconfig/ns.conf.
- À partir de l'interface graphique de l'instance, accédez à **Diagnostics > Afficher la configuration**. Choisissez le type de configuration que vous souhaitez enregistrer. Par exemple, si vous souhaitez enregistrer la configuration enregistrée de votre instance, sélectionnez **Configuration enregistrée**. Cliquez sur le lien **Enregistrer le texte dans un fichier** pour enregistrer le fichier 'ns.conf' sur votre machine locale.

Lorsque vous déployez le modèle de configuration principal à l'aide du modèle de configuration « DeployMasterConfiguration » lors de la création d'une nouvelle tâche, vous pouvez le personnaliser davantage pour chaque instance ADC spécifique en ajoutant des commandes supplémentaires, en modifiant les commandes existantes et en fournissant différentes valeurs de variables dans le fichier d'entrée.

Par exemple, en tant qu'administrateur, vous pouvez télécharger des clés de certificat sur vos instances ADC en plus du fichier ns.conf et déployer la configuration principale sur eux également.

#### **Important**

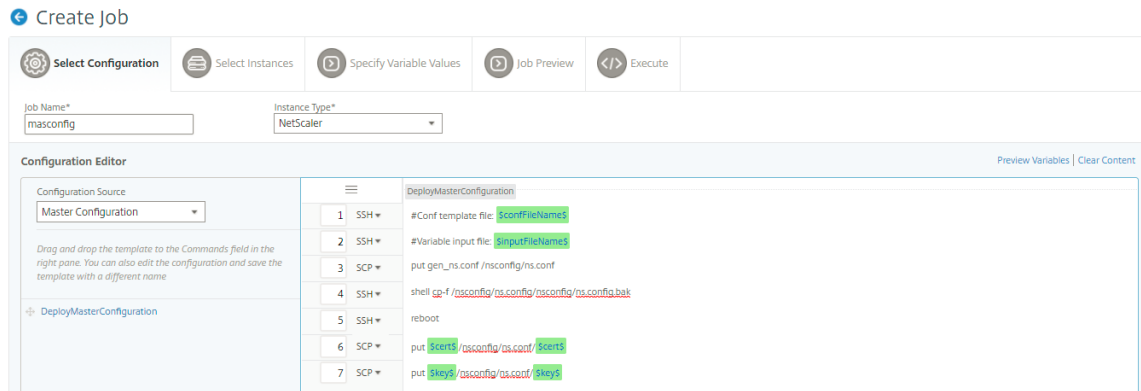
Vous ne pouvez pas exécuter de tâche de configuration à l'aide du modèle DeployMasterConfiguration sur des instances Citrix ADC CPX, des instances configurées dans un cluster ou sur des instances ADC partitionnées.

#### **Pour créer une tâche de configuration à l'aide du modèle de configuration Master Config sur Citrix ADM :**

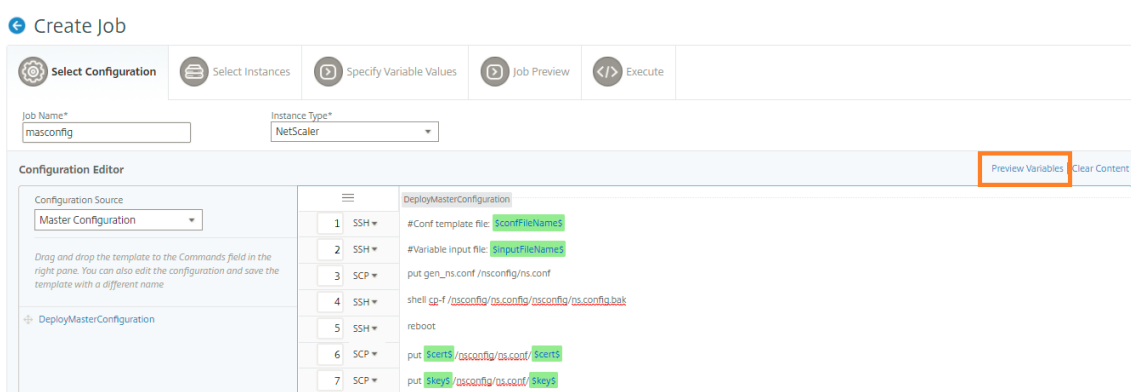
1. Dans Citrix ADM, accédez à **Réseaux > Tâches de configuration**, puis cliquez sur **Créer une tâche**.
2. Dans la page **Créer un travail**, sous l'onglet **Sélectionner une configuration**, spécifiez le **nom du travail** et sélectionnez le **type d'instance** dans la liste déroulante.
3. Sélectionnez **Configuration principale** dans la liste déroulante **Source de configuration**. Glissez et déposez les commandes du modèle DeployMasterConfiguration dans le volet droit. Vous pouvez également ajouter, modifier ou supprimer des commandes dans le volet droit. Cliquez sur **Suivant**.

### Remarque

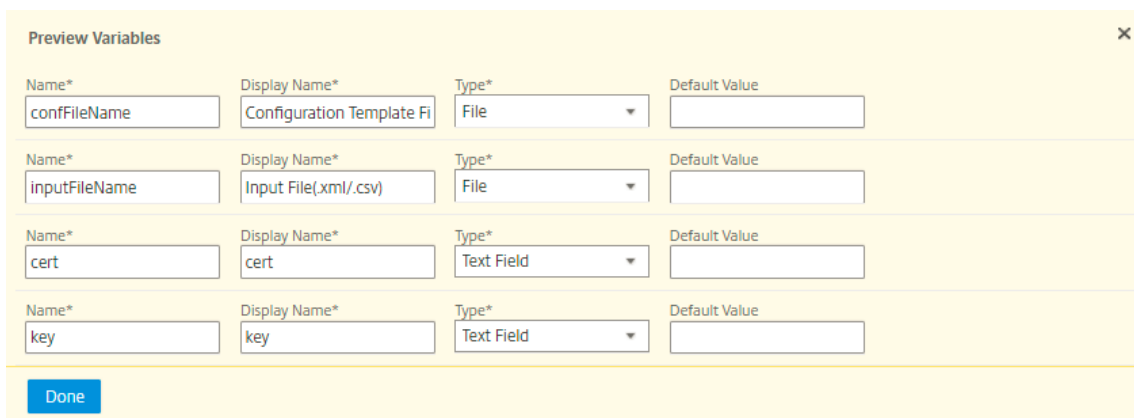
Vous pouvez ajouter des commandes **put** pour ajouter des fichiers d'entrée à votre modèle. Dans notre exemple, nous devons télécharger des fichiers de certificat et de clé en plus du fichier modèle de configuration et des fichiers d'entrée variables.



4. Vous pouvez consulter toutes les variables que vous avez définies lors de la création ou de la modification d'un travail de configuration dans une vue consolidée unique.
5. Pour afficher toutes les variables dans une seule vue consolidée, procédez de l'une des manières suivantes :
  - Lors de la création d'une tâche de configuration, accédez à **Réseaux > Tâches de configuration**, puis sélectionnez **Créer une tâche**. Sur la page **Créer un travail**, vous pouvez consulter toutes les variables que vous avez ajoutées lors de la création du travail de configuration.
  - Lorsque vous modifiez une tâche de configuration, accédez à **Réseau > Tâches de configuration**, sélectionnez le nom de la tâche et cliquez sur **Modifier**. Sur la page **Configurer la tâche**, vous pouvez consulter toutes les variables qui ont été ajoutées lors de la création de la tâche de configuration.
6. Vous pouvez ensuite cliquer sur l'onglet **Aperçu des variables** pour prévisualiser les variables dans une vue consolidée unique que vous avez définie lors de la création ou de la modification d'une tâche de configuration.



7. Une nouvelle fenêtre contextuelle apparaît et affiche tous les paramètres des variables telles que Nom, Nom d’affichage, Type et valeur par défaut dans un format tabulaire. Vous pouvez également modifier et modifier ces paramètres. Cliquez sur le bouton **Terminé** après avoir modifié l’un des paramètres.



8. Sélectionnez les instances sur lesquelles vous souhaitez exécuter le travail de configuration, puis cliquez sur **Suivant**.
9. Dans l’onglet **Spécifier les valeurs des variables**, chargez les éléments suivants :
  - **Fichier de modèle de configuration (.conf)** : téléchargez le fichier .conf que vous avez extrait d’une instance ADC.
  - **Télécharger le fichier d’entrée (.xml/csv)** - Téléchargez le fichier d’entrée avec les valeurs des variables que vous avez définies dans vos commandes.

Un exemple de fichier XML est fourni ici pour votre utilisation. Assurez-vous que les fichiers xml contiennent les détails correspondant aux instances ADC que vous utilisez.

```

1 <?xml version="1.0" encoding="UTF-8" ?>
2
3 <properties>
4
5 <!--
6

```

```
7 Provide inputs for all the parameters defined in the master config
  file.
8
9 - global. This tag contains all the common parameters and value.
10
11 - devicegroup. This tag contains all the instance group specific
  parameters and values.
12
13 If the same parameters are defined in global and instance tags,
  the instance specific parameters value will take precedence
  over the instance group. The instance group specific parameters
  value will take precedence over global parameters in the
  execution.
14
15 - name. This attribute represents the name of the instance group.
16
17 - device. This tag contains all the instance specific parameters
  and value.
18
19 If the same parameters are defined in global and instance tags,
  the instance specific parameters value will take precedence in
  the execution.
20
21 - name. This attribute represents the IP Address of the instance.
  Host name is not supported for the attribute.
22
23 HA pair should be represented as <primaryip>-<secondaryip>.
  Example 10.102.2.1-10.102.2.2
24
25 In the template file, the parameter name must be specified within
  the dollar sign, Example: $NSIP$, $CC_Trap_Dest$ and parameters
  names are case sensitive.
26 -->
27
28 <global>
29
30 </global>
31 <devicegroup name="BLR_DEVS">
32 </devicegroup>
33 <device name="10.106.101.209">
34 <param name="IP" value="10.106.101.209"/>
35 </device>
36
37 <!-- HA PAIR-->
38 <!--<device name="10.102.43.154-10.102.43.155">
39 <param name="NSIP" value="10.102.43.154"/>
40 <param name="HostName" value="NS43HA"/>
41 <param name="LBSERVER" value="haserver43http"/>
42 <param name="SNMPTrapDest" value="10.102.43.130"/>
43 </device-->
44 </properties>
45
46 <!--NeedCopy-->
```

10. Cliquez sur **Suivant**.

← Create Job

Select Configuration | Select Instances | **Specify Variable Values** | Job Preview | Execute

Configuration Template File(.conf)\*  
Choose File

Input File(.xml/.csv)\*  
Choose File

Cancel | Back | **Next** | Save and Exit

Les fichiers d'entrée contenant les valeurs des variables sont conservés (avec le même nom de fichier) dans les tâches de configuration. Vous pouvez afficher et modifier ces fichiers d'entrée que vous avez utilisés et chargés précédemment lors de la création ou de la modification des tâches de configuration.

Pour afficher les tâches de configuration exécutées lors de la création d'une tâche de configuration, accédez à **Réseau > Tâches de configuration**, puis cliquez sur **Créer une tâche**. Dans la page **Créer une tâche**, dans l'onglet **Spécifier les valeurs des variables**, sélectionnez l'option **Valeurs de variables communes pour toutes les instances** pour afficher les fichiers téléchargés. Pour modifier les fichiers d'entrée, téléchargez le fichier d'entrée, puis modifiez et chargez les fichiers (en conservant le même nom de fichier).

Pour afficher les tâches de configuration déjà exécutées lors de la modification d'une tâche de configuration, accédez à **Réseau > Tâches de configuration**, sélectionnez le nom de la tâche et cliquez sur **Modifier**. Dans la page **Configurer la tâche**, sous l'onglet **Spécifier les valeurs de variable**, sélectionnez l'option **Valeurs variables communes pour toutes les instances** pour afficher les fichiers chargés. Pour modifier les fichiers d'entrée, téléchargez le fichier d'entrée, puis modifiez et chargez les fichiers (en conservant le même nom de fichier).

1. Sous l'onglet **Aperçu des tâches**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances, puis cliquez sur **Suivant**.

← Create Job

Select Configuration    Select Instances    Specify Variable Values    **Job Preview**    Execute

Select an instance or instance group to preview  
 10.106.43.177

Preview of Job on the Instance 10.106.43.177

```
[Task ns.conf for 10.106.43.177]
set ns config -IPAddress 10.106.43.177 -netmask 255.255.255.0
enable ns mode FR L3 Edge USNIP PMTUD
set system parameter -doppler DISABLED
set system user nsroot 1d88eecb931c4166b9891fbbaf242260116f9e59ec171716 -encrypted
set rsskeytype -rsstype ASYMMETRIC
set lacp -sysPriority 32768 -mac 3a:52:5f:a6:af:70
set interface 1/1 -throughput 0 -bandwidthHigh 0 -bandwidthNormal 0 -intftype "Xen Virtual" -ifnum 1/1
set interface LO/1 -haMonitor OFF -throughput 0 -bandwidthHigh 0 -bandwidthNormal 0 -intftype Loopback -ifnum LO/1
add ns ip6 fe80::3852:5fff:fea6:af70/64 -scope link-local -type NSIP -vian 1 -vServer DISABLED -mgmtAccess ENABLED -dynamicRouting ENABLED
set ipsec parameter -lifetime 28800
set nd6RAvariables -vian 1
add snmp community public123 ALL
add snmp community kii all
add vian 233
set snmp alarm APPFW-BUFFER-OVERFLOW -timeout 1
```

2. Dans l'onglet **Exécuter**, vous pouvez choisir d'exécuter votre tâche maintenant ou de planifier son exécution ultérieurement. Vous pouvez également choisir l'action que Citrix ADM doit entreprendre en cas d'échec de la commande.

Vous pouvez également choisir d'autoriser les utilisateurs autorisés à exécuter des tâches sur vos instances gérées, et vous pouvez choisir d'envoyer une notification par e-mail concernant la réussite ou l'échec de la tâche, ainsi que d'autres informations.



Après avoir exécuté votre tâche, vous pouvez voir les détails de la tâche en accédant à **Réseaux** > Tâches de **configuration** et en sélectionnant la tâche que vous venez de configurer. Cliquez sur **Détails** puis sur **Résumé de l'exécution** pour voir les détails de votre tâche. Cliquez sur l'instance pour voir les **journaux de commandes** et voir les commandes exécutées sur la tâche.

Command Log		
Status	Command	Message
✓	put /var/mps/tenants/root/config_mgmt/MySSLCert.crt /nsconfig/ssl/MySSLCert.crt	Done
✓	put /var/mps/tenants/root/config_mgmt/MySSLCertKey.key /nsconfig/ssl/MySSLCertKey.key	Done
✓	shell cp -f /nsconfig/ns.conf /nsconfig/ns.conf.bak	Done
✓	#Conf template file: NS12_0_41_Template.conf	Done
✓	#Variable input file: NS12_0_41_AnswerKey.xml	Done
✓	put /var/mps/tenants/root/config_mgmt/ns_#7A818EB30E94FAA36144CC5F0782E06A13C3122F6BC67B32190444FC6F06.conf /nsconfig/ns.conf	Done
✓	shell	Done
✓	reboot	Done

## Utiliser les tâches pour mettre à niveau les instances de Citrix ADC

February 1, 2024

Vous pouvez utiliser Citrix Application Delivery Management (ADM) pour mettre à niveau une ou plusieurs instances Citrix ADC. Avant de mettre à niveau une instance, assurez-vous d'avoir téléchargé les fichiers de compilation et de documentation appropriés sur les instances Citrix ADC. Vous devez

connaître le cadre de licences et les types de licences avant de mettre à niveau une instance.

Lorsque vous mettez à niveau votre instance Citrix ADC en créant une tâche de maintenance, vous pouvez effectuer les opérations suivantes :

- Effectuez une vérification de pré-validation sur les instances en cours de mise à niveau. Le contrôle de pré-validation consiste en les contrôles suivants :
  1. Recherchez les personnalisations existantes sur les instances de Citrix ADC et supprimez les personnalisations. Vous pouvez réappliquer toutes les personnalisations une fois le processus de mise à niveau terminé.
  2. Vérifiez l'utilisation du disque des instances de Citrix ADC. Si l'utilisation du disque est supérieure à 80 %, nettoyez l'espace disque.
  3. Recherchez les problèmes matériels de disque des instances de Citrix ADC.
- Effectuez la mise à niveau de la paire HA Citrix ADC en deux étapes.
  1. Effectuez immédiatement la tâche de mise à niveau sur un nœud ou vous pouvez même la planifier pour plus tard.
  2. Planifiez la mise à niveau pour l'autre nœud ultérieurement. Il doit être planifié après la mise à niveau du nœud initial.

Lorsque vous mettez à niveau une paire Citrix ADC HA, notez les points suivants :

- Actuellement, le deuxième nœud de la paire HA est mis à niveau en premier, puis, la mise à niveau pour le premier nœud est planifiée pour être effectuée ultérieurement.
- La synchronisation et la propagation des nœuds sont désactivées jusqu'à ce que les deux nœuds soient correctement mis à niveau.
- Après la mise à niveau des deux nœuds, vous verrez un message d'erreur dans l'historique d'exécution (qui indique que HA Sync n'est pas activé) si vos nœuds de la paire HA sont sur des versions ou versions différentes.

### **Pour créer une tâche de maintenance afin de mettre à niveau votre instance Citrix ADC :**

#### **Remarque**

La mise à niveau ADC d'une version supérieure à une version inférieure n'est pas prise en charge. Par exemple, si votre instance Citrix ADC est 13.0 82.x, vous ne pouvez pas rétrograder l'instance ADC vers 13.0 79.x ou toute autre version antérieure.

1. Accédez à **Réseaux > Travaux de configuration > Travaux de maintenance**.
2. Dans la page Travaux de maintenance, cliquez sur **Créer un travail**.

3. Sur la page Créer un travail de maintenance, sélectionnez **Mettre à niveau Citrix ADC/Mettre à niveau Citrix ADC HA** et cliquez sur **Poursuivre**.

## Create Maintenance Job

Select a task to create Maintenance Job\*

- Upgrade Citrix ADC/Upgrade Citrix ADC HA
- Upgrade Citrix SD-WAN WO
- Upgrade Citrix ADC SDX
- Configure HA Pair of Citrix ADC Instances
- Convert HA Pair of Instances to 2 Node Cluster

Proceed

Close

4. Sur une ou plusieurs pages Mettre à niveau le ou les appareils Citrix ADC, dans l'onglet **Sélection d'instance**, spécifiez le **nom du travail** et cliquez sur **Ajouter des instances**.

← Upgrade Citrix ADC Appliance(s)

Instance Selection Upgrade Schedule Task

Job Name\*  
Upgrade task

Select the target instances to run this task.

Add Instances Remove

<input type="checkbox"/>	IP ADDRESS
<input checked="" type="checkbox"/>	

Clicking Next button will start pre-upgrade validation over the instances.

Cancel Next →

5. Sélectionnez les instances ou groupes d'instances cibles que vous souhaitez mettre à niveau.

#### Remarque

- Pour mettre à niveau les instances Citrix ADC en mode haute disponibilité, vous devez sélectionner les adresses IP des instances principales ou secondaires. Toutefois, il est recommandé de toujours utiliser le nœud principal pour la mise à niveau.
- Pour mettre à niveau les instances Citrix ADC en mode cluster, sélectionnez l'adresse IP du cluster.

6. Après avoir ajouté les instances ou les groupes d'instances Citrix ADC, cliquez sur **Suivant** pour démarrer la validation préalable à la mise à niveau sur les instances sélectionnées. L'écran indique la progression de la pré-validation de chacune des instances Citrix ADC.
7. Sur la page **Mettre à niveau le ou les appareils Citrix ADC**, sélectionnez l'onglet **Mettre à niveau**. Dans le menu **Image logicielle**, sélectionnez **Local** (votre ordinateur local) ou **Appliance** (le fichier de génération doit être présent sur Citrix ADM).
8. Vous pouvez également voir si des instances présentent des erreurs de mise à niveau de pré-

validation. Ces erreurs sont affichées sous forme de message. Les messages indiquent les erreurs liées à l'espace disque, au disque dur et à la personnalisation de l'utilisateur.

Si vous ne souhaitez pas continuer avec les instances qui ont échoué la vérification de mise à niveau de pré-validation, vous pouvez supprimer les instances. Pour supprimer les instances, sélectionnez-les et cliquez sur **Supprimer**.

1. Cliquez sur **Suivant**.

#### Remarque

Il est fortement recommandé de poursuivre le processus de mise à niveau, uniquement si la vérification de validation avant la mise à niveau réussit pour les instances de Citrix ADC.

2. Sous l'onglet **Planifier la tâche**, vous pouvez également définir les détails d'exécution dans lesquels vous pouvez effectuer le processus de mise à niveau maintenant ou le planifier pour une date ultérieure.
3. Vous pouvez activer la notification par e-mail pour recevoir le rapport d'exécution de la mise à niveau des instances Citrix ADC. Cochez la case **Recevoir le rapport d'exécution par e-mail** pour activer la notification par e-mail. Pour créer une liste de distribution d'e-mails :
  - Sélectionnez l'icône **+** pour créer la liste de distribution des e-mails.
  - Sur la page **Créer une liste de distribution d'e-mails**, spécifiez un **nom** pour la liste de distribution d'e-mails. Ajoutez le serveur de messagerie SMTP à utiliser pour envoyer des notifications par e-mail au serveur de messagerie. Dans la zone **De**, ajoutez l'adresse e-mail à partir de laquelle envoyer des messages. Dans la zone **À**, ajoutez l'adresse e-mail ou les adresses auxquelles envoyer des messages. Vous pouvez également ajouter une ou plusieurs adresses e-mail auxquelles envoyer des copies et des copies de messages sans afficher ces adresses dans les messages ou les copies. Cliquez sur **Créer**. Après avoir créé la liste de distribution d'e-mails, cliquez sur **Terminer** pour terminer le processus de configuration.
4. Dans l'onglet **Planifier la tâche**, vous pouvez également effectuer la mise à niveau en deux étapes pour les nœuds en haute disponibilité. Vous pouvez effectuer la mise à niveau immédiatement ou planifier une heure pour que les nœuds soient mis à jour les uns après les autres. La synchronisation et la propagation des nœuds sont désactivées jusqu'à ce que les deux nœuds soient correctement mis à niveau.

**Upgrade Citrix ADC Appliance(s)**

Instance Selection Upgrade Schedule Task

Perform Citrix ADC backup  
 Receive Execution Report through email

Email\*  
Example server

Receive Execution Report through slack ⓘ

▼ Execution Details

You can either execute the task now or schedule to execute the task at a later time.

Execution Mode\*  
Now

Perform two stage upgrade for nodes in HA ⓘ  
Note: HA Sync and HA Propagation will be disabled until both the nodes are upgraded successfully.

Execution Date  
28 Jan 2020

Start Time\*  
01 00 AM PM

## Utiliser des modèles de configuration pour créer des modèles d'audit

February 1, 2024

Vous pouvez désormais utiliser des commandes de configuration précédemment enregistrées en tant que modèles de configuration pour créer des modèles d'audit pouvant être appliqués à des instances NetScaler spécifiques. Lors de la création d'un modèle d'audit, vous pouvez glisser-déposer des modèles de configuration précédemment enregistrés dans le champ Commandes et modifier le modèle en fonction de vos besoins. Vous pouvez ensuite appliquer le modèle d'audit à des instances NetScaler spécifiques. Citrix ADM compare ces instances avec le modèle d'audit et signale toute incompatibilité. Ce processus vous aide à identifier les erreurs et à les corriger en temps opportun.

Vous pouvez créer des modèles de configuration tout en créant une nouvelle tâche et en enregistrant

un ensemble de commandes de configuration en tant que modèle. Lorsque vous enregistrez ces modèles sur la page **Créer des tâches**, ils s'affichent automatiquement sur la page **Créer un modèle**.

Par exemple, envisagez une configuration d'équilibrage de charge de base pour laquelle vous ajoutez un serveur virtuel d'équilibrage de charge, ajoutez deux services et liez les services au serveur virtuel.

Cet exemple utilise les commandes suivantes :

```
add lb vserver servername HTTP ipaddress portnumber
```

```
add service servicename1 ipaddress1 HTTP 80
```

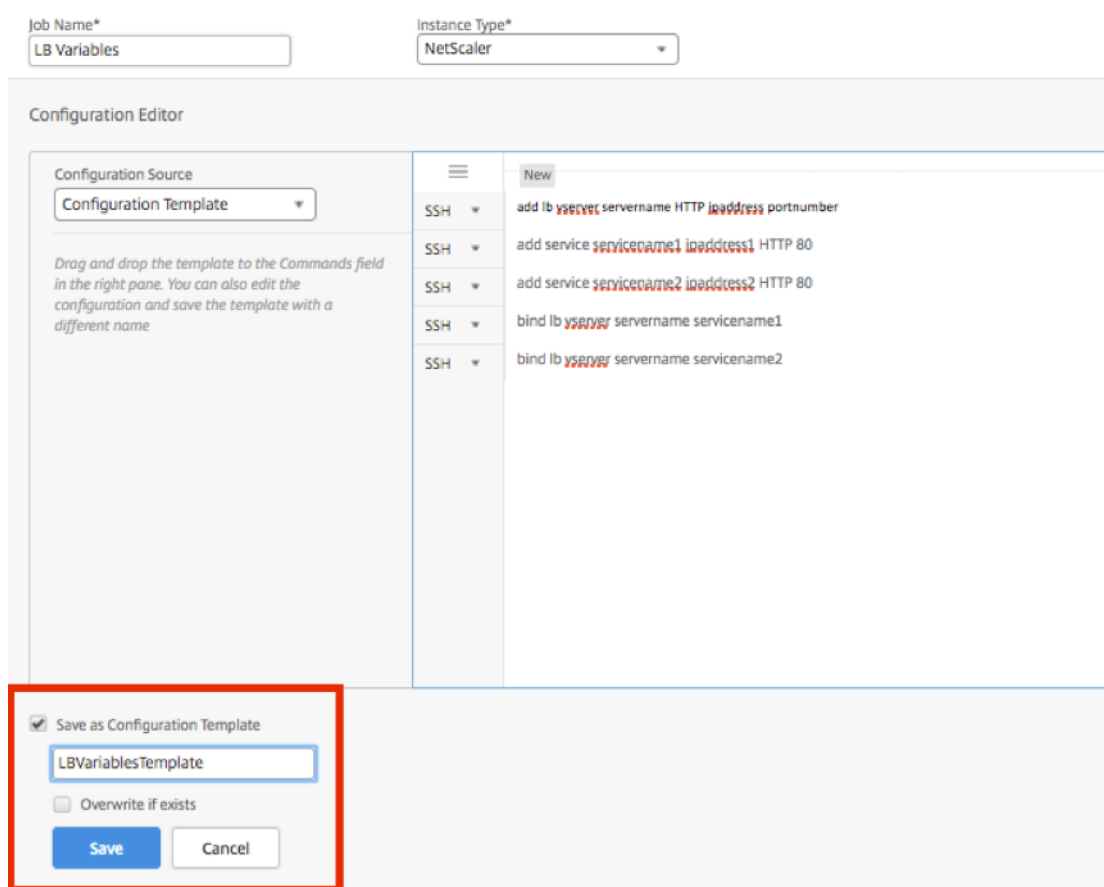
```
add service servicename2 ipaddress2 HTTP 80
```

```
bind lb vserver servername servicename1
```

```
bind lb vserver servername servicename2
```

**Pour enregistrer un modèle de configuration dans Citrix ADM :**

1. Accédez à **Réseaux > Tâches de configuration**, puis cliquez sur **Créer une tâche**.
2. Sur la page **Créer un travail**, spécifiez le nom du travail et le type d'instance.
3. Choisissez **Modèle de configuration** comme source de configuration et, dans le champ **Commandes**, saisissez des commandes telles que celles de l'exemple ci-dessus.
4. Cochez la case **Enregistrer en tant que modèle de configuration** et spécifiez un nom pour votre modèle. Vous pouvez choisir d'écraser d'autres modèles qui existent avec le même nom.
5. Cliquez sur **Enregistrer**.



**Pour utiliser un modèle de configuration pour créer un modèle d’audit dans Citrix ADM :**

1. Accédez à **Réseaux > Audit de configuration > Modèles d’audit**, puis cliquez sur **Ajouter**.
2. Dans la page **Créer un modèle**, spécifiez un nom pour le nom du modèle et entrez une description.
3. Dans la liste **Source de configuration**, sélectionnez **Modèle de configuration**, puis glissez et déposez le modèle dans le champ Commandes du volet droit. Vous pouvez également modifier la configuration et enregistrer le modèle sous un autre nom. Cliquez sur **Suivant**.
4. Dans l’onglet **Sélectionner des instances**, cliquez sur **Ajouter des instances** et ajoutez les instances sur lesquelles vous souhaitez exécuter la configuration. Cliquez sur **OK**.
5. Cliquez sur **Terminer**.



**Create Template**

Audit Commands Select Instances

Template Name\* LBVariableTemplate Description Create LB server with variables

Configuration Editor

Configuration Source Configuration Template

Drag and drop the template to the Commands field in the right pane. You can also edit the configuration and save the template with a different name

LBVariableTemplate

```
add lb vserver servername HTTP ipaddress portnumber
add service servicename1 ipaddress1 HTTP 80
add service servicename2 ipaddress2 HTTP 80
bind lb vserver servername servicename1
bind lb vserver servername servicename2
```

Cancel Next →

Le modèle d'audit apparaît dans la liste Modèles d'audit et est exécuté toutes les 12 heures par rapport aux configurations des instances spécifiées.

## Utiliser la commande SCP (put) dans les tâches de configuration

February 1, 2024

Vous pouvez utiliser la fonctionnalité Tâches de configuration de Citrix ADM pour créer des tâches de configuration, envoyer des notifications par e-mail et consulter les journaux d'exécution des tâches créées. Une tâche est un ensemble de commandes de configuration que vous pouvez créer et exécuter sur une seule instance gérée ou sur plusieurs instances gérées. Par exemple, vous pouvez utiliser des tâches de configuration pour les mises à niveau des appareils.

Les tâches de configuration dans Citrix ADM utilisent les commandes SSH (Secure Shell) pour configurer les instances, et vous pouvez configurer une tâche de configuration pour utiliser Secure Copy

(SCP) pour transférer des fichiers en toute sécurité. SCP est basé sur le protocole SSH. L'une des commandes SCP que vous pouvez inclure dans une tâche de configuration est la commande « put ». Vous pouvez utiliser la commande « put » dans les tâches de configuration pour télécharger ou transférer un ou plusieurs fichiers stockés dans un répertoire local de votre système vers Citrix ADM, puis vers un répertoire de la ou des instances NetScaler.

**Remarque** Le fichier est chargé sur Citrix ADM puis copié (placé) dans les instances NetScaler sélectionnées. Le fichier téléchargé est stocké dans Citrix ADM et est supprimé uniquement lorsque le travail est supprimé. Cela est nécessaire pour les tâches dont l'exécution est prévue ultérieurement.

La commande a la syntaxe suivante :

```
put <local_filename> <remote_path/remote_filename>
```

où

<local\_filename> est le nom du fichier local à télécharger.

<remote\_path / remote\_filename> est le chemin d'accès à un répertoire distant et le nom à attribuer au fichier lorsqu'il est copié dans ce répertoire.

Lors de la création du travail de configuration, vous pouvez convertir les paramètres de nom de fichier local et distant en variables. Cela vous permet d'attribuer différents fichiers à ces paramètres pour le même ensemble d'instances NetScaler chaque fois que vous exécutez la tâche. En outre, lorsque vous utilisez un fichier à plusieurs endroits dans une tâche et si vous souhaitez renommer le fichier, vous pouvez redéfinir la variable au lieu de changer le nom du fichier à tous les endroits.

#### **Pour utiliser la commande put pour télécharger des fichiers dans une tâche de configuration :**

1. Accédez à **Réseaux > Travaux de configuration**.
2. Sur la page **Travaux**, cliquez sur **Créer un travail**.
3. Dans la page **Créer un travail**, entrez le nom du travail dans le champ Nom du travail et, dans le volet **Éditeur de configuration**, entrez la commande « put ».

Par exemple, si vous souhaitez créer une tâche de configuration qui copie un fichier de certificat SSL enregistré sur votre système local vers plusieurs instances NetScaler, vous pouvez ajouter une commande « put » qui utilise une variable au lieu du nom d'un fichier spécifique, et définir le type de variable comme « file ».

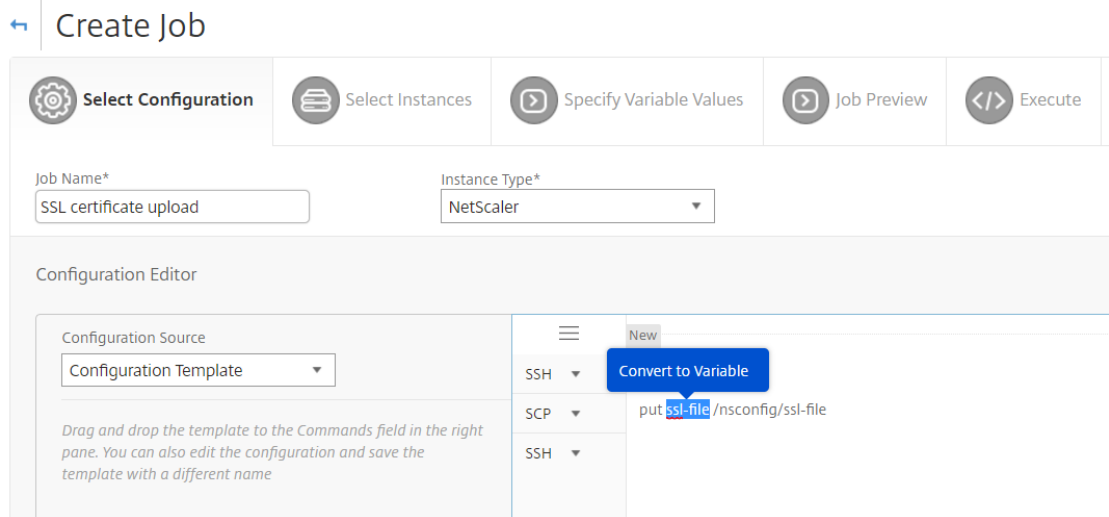
```
1 put ssl-file /nsconfig/ssl-file
2 <!--NeedCopy-->
```

Dans cet exemple,

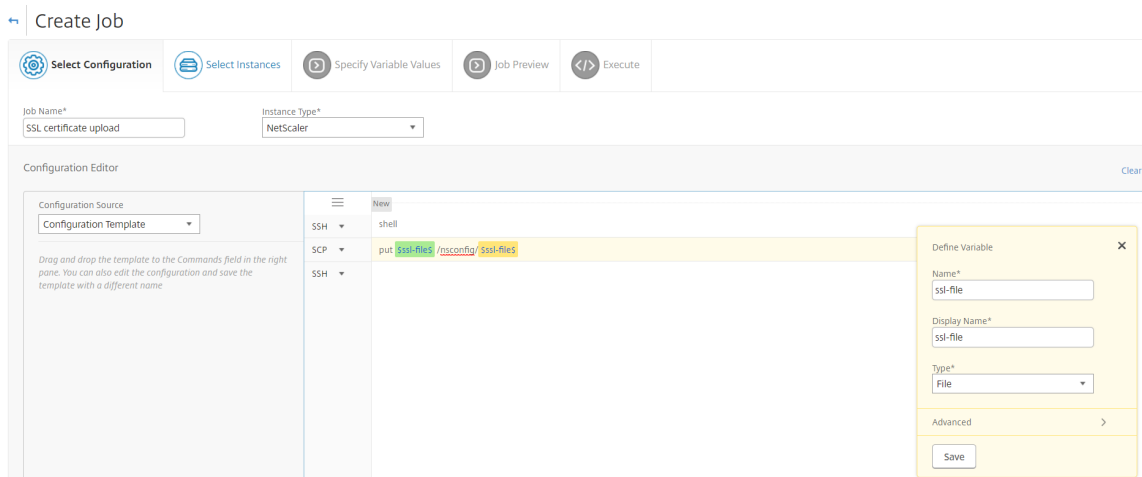
- ssl-file - Il s'agit du nom du fichier qui doit être téléchargé dans l'instance NetScaler.

- /nsconfig/ssl-file - Il s'agit du dossier de destination sur l'instance où le fichier ssl-sera placé après l'exécution de la tâche.

4. Dans la commande que vous venez de saisir, sélectionnez le nom de fichier que vous souhaitez convertir en variable, puis cliquez sur **Convertir en variable**, comme illustré dans la figure suivante.

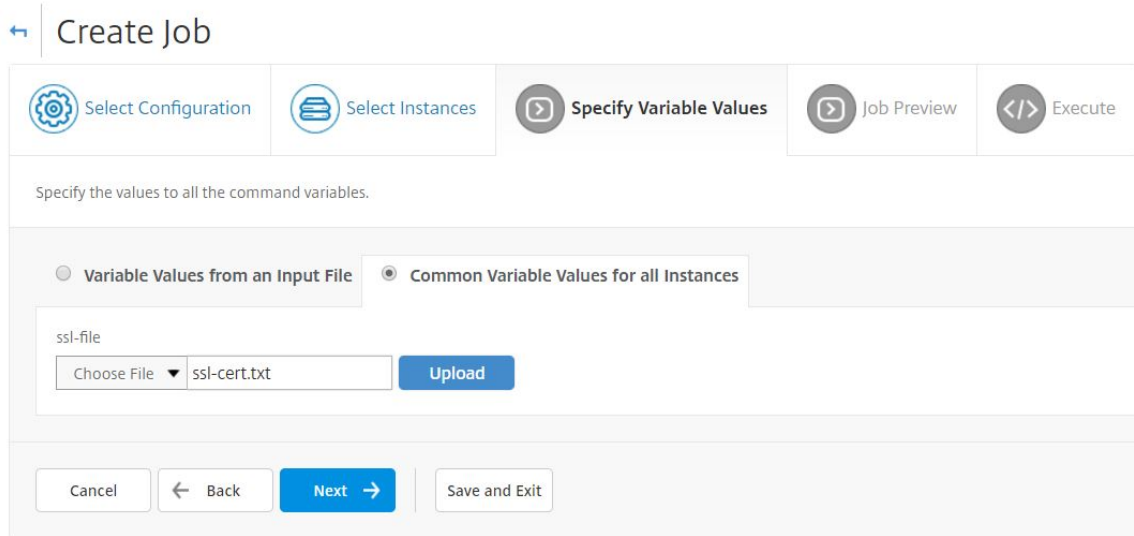


5. Vérifiez que le nom du fichier a été entouré de signes dollar (indiquant qu'il s'agit maintenant d'une variable), puis cliquez sur la variable.
6. Spécifiez les détails de la variable, tels que le nom, le nom complet et le type.
7. Dans la liste déroulante **Type**, sélectionnez **Fichier**. Cliquez sur **Enregistrer**. La déclaration de la variable en tant que type « Fichier » vous permet de télécharger des fichiers vers Citrix ADM.

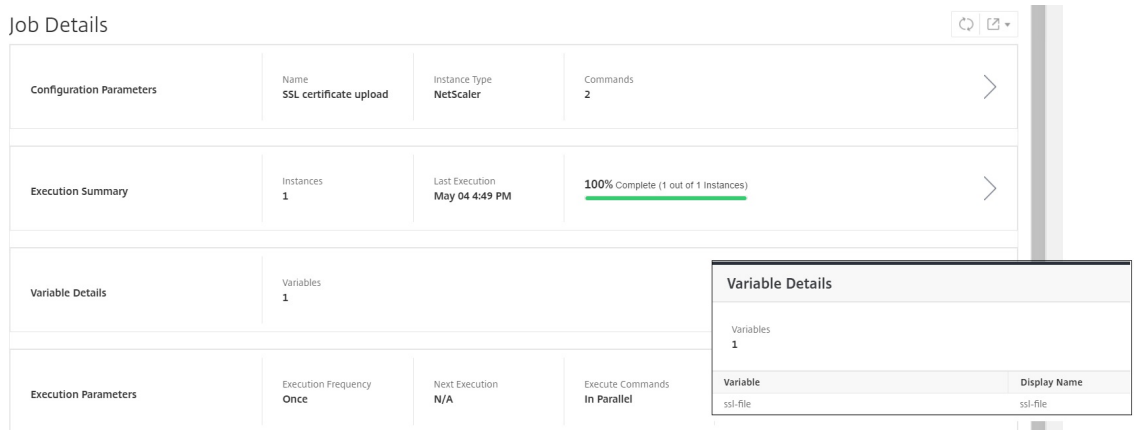


8. Cliquez sur **Suivant** et sélectionnez les instances NetScaler vers lesquelles copier les fichiers.
9. Sous l'onglet **Spécifier les valeurs de variables**, sélectionnez **Valeurs de variables communes pour toutes les instances** section, sélectionnez le fichier dans le stockage local de

votre système, cliquez sur **Télécharger** pour **télécharger** le fichier dans Citrix ADM, puis cliquez sur **Suivant**.



10. Sous l'onglet **Aperçu des tâches**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances.
11. Dans l'onglet **Exécuter**, vous pouvez exécuter la tâche maintenant ou planifier son exécution ultérieurement. Vous pouvez également choisir l'action que Citrix ADM doit entreprendre en cas d'échec de la commande. Vous pouvez également créer une notification par e-mail pour recevoir une notification sur le succès ou l'échec de la tâche, ainsi que d'autres détails. Cliquez sur **Terminer**.
12. Vous pouvez consulter les détails de la tâche en accédant à **Réseaux > Tâches de configuration** et en sélectionnant la tâche que vous venez de configurer. Cliquez sur **Détails**, puis sur **Détails des variables** pour répertorier les variables ajoutées à votre tâche.



## Replanifier les tâches configurées à l'aide de modèles intégrés

February 1, 2024

Vous pouvez replanifier une tâche que vous avez planifiée à l'aide de modèles intégrés dans Citrix Application Delivery Management (ADM). Par exemple, vous pouvez modifier l'action que Citrix ADM doit effectuer en cas d'échec d'une commande. Si vous avez précédemment choisi d'ignorer une erreur et de continuer, vous pouvez la modifier pour annuler toutes les commandes réussies en cas d'échec d'une commande.

### Pour replanifier un travail configuré à l'aide de modèles intégrés dans Citrix ADM

1. Dans Citrix ADM, accédez à **Réseaux > Travaux de configuration**.
2. Sélectionnez le travail à modifier, ajouter ou supprimer des instances, spécifiez des valeurs variables, puis modifiez les actions d'exécution et les paramètres.
3. Cliquez sur **Terminer** pour replanifier la tâche.

#### Remarque

Vous pouvez également sélectionner la tâche et cliquer sur **Exécuter à nouveau** pour exécuter la tâche sans modifier la source, l'instance et les commandes. Cela est utile lorsque vous devez exécuter le même ensemble de commandes sur les mêmes instances. Parfois, le travail peut rencontrer une erreur transitoire du côté serveur, et vous devrez peut-être l'exécuter à nouveau.

## Réutiliser les modèles d'audit de configuration dans les tâches de configuration

February 1, 2024

En tant qu'administrateur, vous pouvez désormais enregistrer les commandes de configuration sous la forme d'un ensemble de modèles de configuration réutilisables lorsque vous créez une tâche et exécutez un audit de configuration. Le modèle de configuration créé et enregistré dans Configuration Jobs est disponible dans Configuration Audit pour créer un modèle d'audit qui peut être appliqué à des instances Citrix ADC spécifiques. De même, le modèle d'audit créé dans le module Configuration Audit est disponible dans les tâches de configuration afin que vous puissiez exécuter le modèle en tant que tâche de configuration. Toute modification apportée au modèle est désormais visible dans les modules Jobs de configuration et Configuration Audit.

Auparavant, la tâche de configuration et les modèles d'audit de configuration devaient être créés séparément pour la même configuration et enregistrés dans des fichiers différents. Cela a entraîné une duplication des efforts lors de la création et de la maintenance des modèles.

Citrix Application Delivery Management (ADM) vous permet d'enregistrer ce modèle dans le système afin que le modèle d'audit soit également disponible dans les tâches de configuration. Les modèles d'audit peuvent désormais être utilisés pour créer des tâches de configuration. De cette façon, les modèles peuvent être utilisés de manière interchangeable entre les tâches de configuration et les audits de configuration.

Par exemple, envisagez une configuration d'équilibrage de charge de base pour laquelle vous ajoutez un serveur virtuel d'équilibrage de charge, ajoutez deux services et liez les services au serveur virtuel.

Cet exemple utilise les commandes suivantes :

```
1 add lb vserver servername HTTP ipaddress portnumber
2
3 add service servicename1 ipaddress1 HTTP 80
4
5 add service servicename2 ipaddress2 HTTP 80
6
7 bind lb vserver servername servicename1
8
9 bind lb vserver servername servicename2
10 <!--NeedCopy-->
```

## Création d'un modèle dans les audits de configuration et réutilisation dans les travaux de configuration

Effectuez la tâche suivante pour créer un modèle dans le module d'audit de configuration et le réutiliser dans le module de tâches de configuration.



### Pour créer un modèle d'audit :

1. Dans **Citrix ADM**, accédez à Réseaux > Audit de configuration > Modèle d'audit, puis cliquez sur **Ajouter**.
2. Dans la page **Créer un modèle**, spécifiez le nom du modèle. Vous pouvez également ajouter plus d'informations sur le modèle dans le champ **Description**.
3. Dans le volet **Commandes**, entrez les commandes de l'exemple.
4. Cochez la case **Enregistrer en tant que modèle de configuration** et spécifiez un nom pour votre modèle. Par exemple, vous pouvez nommer ce modèle comme « LBVariablesTemplate. » Vous pouvez choisir d'écraser d'autres modèles qui existent avec le même nom.

**Remarque** Le nom du modèle d’audit peut être identique au nom du modèle de configuration.

5. Cliquez sur **Enregistrer**, puis sur **Suivant**.

## ← Create Template

 Audit Commands  Select Instances

Template Name\*

Description

### Configuration Editor

Configuration Source

*Drag and drop the template to the Commands field in the right pane. You can also edit the configuration and save the template with a different name*

- config-template2
- config-template1

```
shell
add lb vserver servername HTTP ipaddress portnumber
add service servicename1 ipaddress1 HTTP 80
add service servicename2 ipaddress2 HTTP 80
bind lb vserver servername servicename1
bind lb vserver servername servicename2
```

Save as Configuration Template

Overwrite if exists

6. Cliquez sur **Suivant**.

7. Dans l'onglet **Sélectionner les instances**, sélectionnez les **instances Citrix ADC** sur lesquelles vous souhaitez exécuter ces commandes de configuration et cliquez sur **Terminer**. Le nouveau modèle est désormais visible dans la liste des modèles d'audit.

## Audit Templates

<input type="button" value="Add"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
<input type="checkbox"/>	Template Name	Description
<input type="checkbox"/>	LBVariablesTemplate	Basic load balancing configuration to add a load balancing virtual server
<input type="checkbox"/>	config-template2	abc
<input type="checkbox"/>	abc	

8. Lorsque vous souhaitez exécuter ces commandes de configuration, accédez à **Réseaux > Travaux de configuration**, puis cliquez sur **Créer un travail**. Le modèle d'audit que vous avez créé précédemment est répertorié en tant que modèle de configuration.

### Pour réutiliser le modèle d'audit dans les tâches de configuration :

1. Entrez un nom pour la tâche et sélectionnez le type d'instance, puis glissez et déposez le modèle dans le volet de commandes.

Lors de la création du travail de configuration, vous pouvez convertir les paramètres de nom de fichier local et distant en variables. Cela vous permet d'attribuer différents fichiers à ces paramètres pour le même ensemble d'instances Citrix ADC chaque fois que vous exécutez la tâche.

2. Dans la commande que vous avez saisie, sélectionnez le nom de fichier à convertir en variable, puis cliquez sur **Convertir en variable**.
3. Dans l'onglet **Sélectionner** les instances, sélectionnez les instances sur lesquelles vous souhaitez exécuter ces commandes.
4. Si vous avez spécifié des variables dans les commandes, dans l'onglet **Spécifier les valeurs de variable**, sélectionnez l'une des options suivantes pour spécifier des variables pour vos instances :

- Valeurs de variables à partir d'un fichier d'entrée : téléchargez un fichier d'entrée pour saisir les valeurs des variables que vous avez définies dans vos commandes, puis chargez le fichier sur le serveur Citrix ADM.
- Valeurs de variables communes à toutes les instances : spécifiez l'adresse IP et le port du serveur Syslog.

5. Dans l'onglet **Aperçu des tâches**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances et cliquer sur **Suivant**.



6. Dans l'onglet **Exécuter**, cliquez sur **Terminer** pour exécuter le travail de configuration. Maintenant, si vous souhaitez ajouter un autre service à ce serveur d'équilibrage de charge et lier le service au serveur, vous pouvez modifier les commandes dans la page de commande et les enregistrer.
7. Accédez à **Modèles d'audit** et cliquez sur **Ajouter**.
8. Glissez et déposez le modèle « LBVariablesTemplate » dans le volet des commandes. Vous pouvez voir que le modèle a été mis à jour avec les nouvelles commandes.

Le modèle d'audit apparaît dans la liste Modèles d'audit et est exécuté toutes les 12 heures par rapport aux configurations des instances spécifiées. Vous pouvez désormais créer des modèles et les réutiliser entre les tâches de configuration et les modules d'audit de configuration.

## Importer et exporter des modèles de configuration

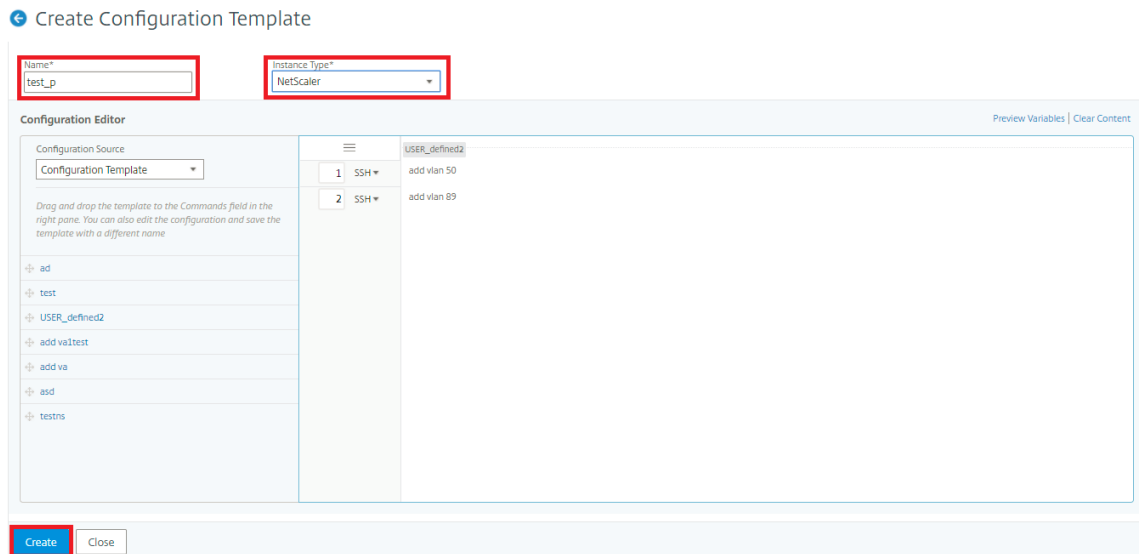
February 1, 2024

Vous pouvez exporter les modèles de configuration depuis n'importe quel Citrix Application Delivery Management (ADM). Vous pouvez également importer le fichier dans le même Citrix ADM ou dans un autre Citrix ADM à tout moment à l'avenir. Les données des modèles de configuration (telles que les commandes de configuration, les définitions de variables et les paramètres) ne sont pas perdues.

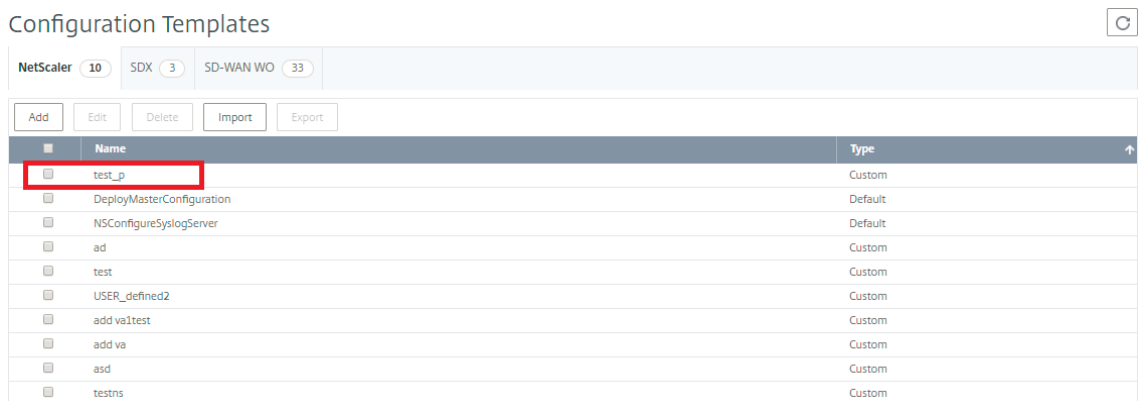
Vous pouvez exporter les modèles de configuration dans un format de fichier **.json** et les enregistrer dans le dossier local. Vous pouvez importer un modèle de configuration. fichiers **json** dans Citrix ADM. Ce fichier est peut-être nouveau ou celui que vous avez exporté depuis le même Citrix ADM ou un autre Citrix ADM.

### Pour exporter les modèles de configuration :

1. Accédez à **Réseaux > Tâches de configuration > Modèles de configuration**.
2. Cliquez sur le bouton **Ajouter** pour créer le modèle de configuration.
3. Dans la page **Créer un modèle de configuration**, spécifiez le nom du modèle de configuration et choisissez le type d'instance. Sous **Éditeur de configuration**, sélectionnez la source de configuration comme Modèle de configuration dans le menu déroulant. Vous pouvez glisser-déposer les modèles de configuration existants dans l'éditeur de configuration. Cliquez sur **Créer**.



4. Accédez à **Réseaux > Travaux de configuration > Modèles de configuration** pour afficher les modèles créés dans la liste des modèles de configuration.



5. Sélectionnez le modèle de configuration nouvellement créé et cliquez sur le bouton **Exporter**.

Le modèle de configuration correspondant est téléchargé sur votre système local au format **.json**.

**Pour importer les modèles de configuration :**

1. Accédez à **Réseaux > Travaux de configuration > Modèles de configuration** et cliquez sur le bouton **Importer** . Sélectionnez le chemin où vous avez le **.json** du modèle de configuration et téléchargez le. fichiers**.json**. Il est fortement recommandé de télécharger le. fichiers**.json** que vous avez déjà exportés.
2. Vous pouvez également importer le modèle de configuration à l'aide de l'option **Fichier** dans l'Éditeur de configuration.
3. Sélectionnez **Fichier** dans le menu déroulant de l'**éditeur de configuration**.
4. Sélectionnez **Choisir un fichier (.json)** à partir de votre système local et téléchargez le modèle de configuration. fichiers**.json**.

← Create Configuration Template

Name\*  Instance Type\*

Configuration Editor Preview Variables | Clear Content

Configuration Source

Please upload valid text, conf or json file to import the commands.

Choose File

SSH  Select an option from the Configuration Source drop-down list in the left pane to import the commands, or type your own commands here.

### Remarque

- Chaque nouveau modèle importé est enregistré avec une nouvelle chaîne d'identification.
- Vous ne pouvez importer les modèles de configuration que si le fichier est enregistré dans le format **json**. Si vous importez les modèles de configuration autres que les fichiers **.json** depuis votre système local, une erreur s'affiche et l'importation des fichiers échoue.

## Tâches de maintenance

January 23, 2024

Vous pouvez créer les tâches de maintenance suivantes à l'aide de Citrix ADM. Vous pouvez ensuite planifier les tâches de maintenance à une date et à une heure spécifiques.

- Mettre à niveau les instances de Citrix ADC
- Mettre à niveau les instances Citrix SD WAN-WO
- Mettre à niveau les instances Citrix ADC SDX
- Configurer la paire HA d'instances Citrix ADC
- Convertir une paire d'instances HA en cluster à 2 nœuds

### Planifier la mise à niveau des instances Citrix ADC

1. Accédez à **Réseaux > Travaux de configuration > Travaux de maintenance**. Cliquez sur le bouton **Créer une tâche**.
2. Sur la page Créer une tâche de maintenance, sélectionnez **Mettre à niveau Citrix ADC/Mettre à niveau Citrix ADC HA** et cliquez sur **Continuer**.

## Create Maintenance Job

Select a task to create Maintenance Job\*

- Upgrade Citrix ADC/Upgrade Citrix ADC HA
- Upgrade Citrix SD-WAN WO
- Upgrade Citrix ADC SDX
- Configure HA Pair of Citrix ADC Instances
- Convert HA Pair of Instances to 2 Node Cluster

Proceed

Close

3. Sur la page Mettre à niveau les appareils Citrix ADC, dans l'onglet **Sélection** des instances, ajoutez les instances Citrix ADC sur lesquelles vous souhaitez exécuter le processus de mise à niveau. Cliquez sur **Suivant** pour lancer la validation préalable à la mise à niveau sur les instances sélectionnées.

← Upgrade Citrix ADC Appliance(s)

Instance Selection Upgrade Schedule Task

Job Name\*  
Upgrade task

Select the target instances to run this task.

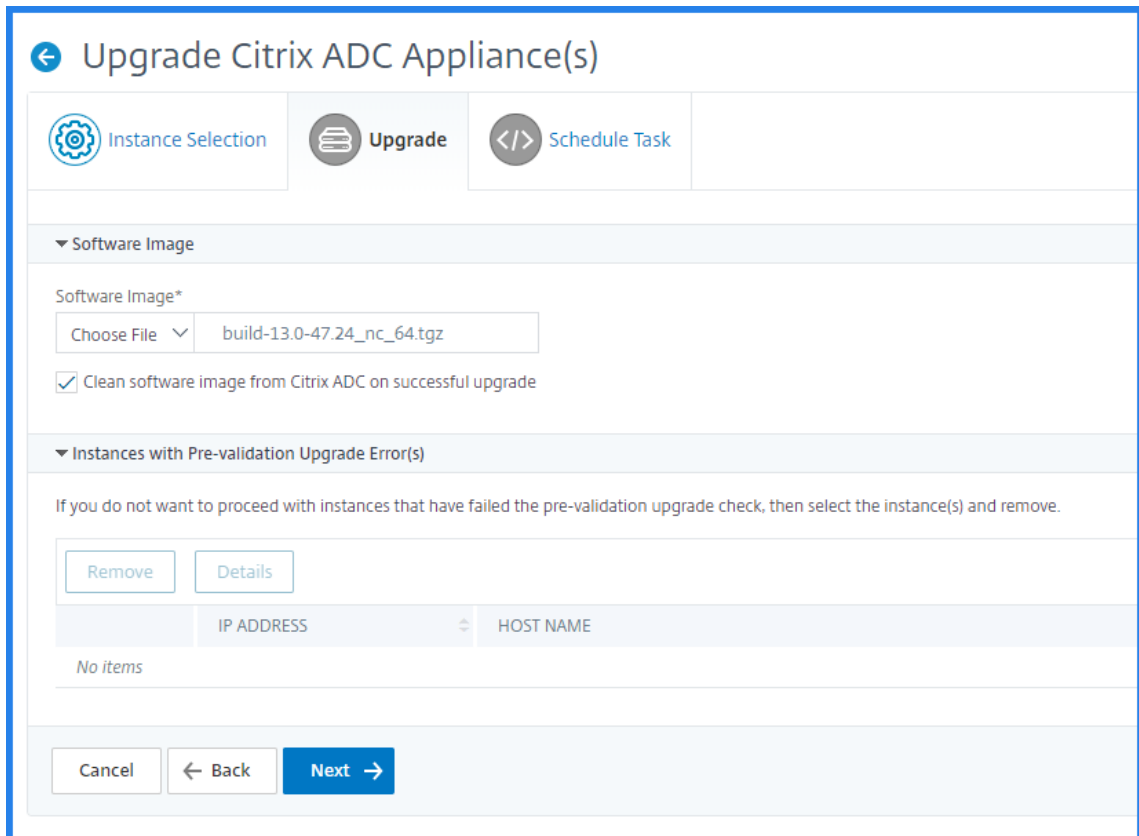
Add Instances Remove

	IP ADDRESS
<input type="checkbox"/>	
<input checked="" type="checkbox"/>	

Clicking Next button will start pre-upgrade validation over the instances.

Cancel Next →

4. Dans l'onglet **Mise à niveau**, dans la liste des images logicielles, sélectionnez Local (votre machine locale) ou Appliance (le fichier de construction doit être présent sur l'appliance virtuelle Citrix ADM).



5. Vous pouvez activer la notification par e-mail pour recevoir le rapport d'exécution de la mise à niveau des instances Citrix ADC. Cochez la case **Recevoir le rapport d'exécution par e-mail** pour activer la notification par e-mail.
6. Sélectionnez l'icône + pour créer la liste de distribution des e-mails.
7. Pour mettre à niveau l'instance Citrix ADC dès maintenant, sélectionnez **Maintenant** dans la liste des modes d'exécution.
8. Pour mettre à niveau l'instance Citrix ADC 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 des instances Citrix ADC.

The screenshot displays the 'Upgrade Citrix ADC Appliance(s)' configuration interface. At the top, there are three tabs: 'Instance Selection', 'Upgrade', and 'Schedule Task'. The 'Schedule Task' tab is active. Below the tabs, there are several configuration options:

- Perform Citrix ADC backup
- Receive Execution Report through email
- Email\* field with a dropdown menu showing 'Example server' and buttons for 'Add', 'Edit', and 'Test'.
- Receive Execution Report through slack ⓘ

Under the 'Execution Details' section, there is a note: 'You can either execute the task now or schedule to execute the task at a later time.' The 'Execution Mode\*' is set to 'Now'. There is a checkbox for 'Perform two stage upgrade for nodes in HA ⓘ' with a note: 'Note: HA Sync and HA Propagation will be disabled until both the nodes are upgraded successfully.' The 'Execution Date' is set to '28 Jan 2020'. The 'Start Time\*' is set to '01:00 AM'. At the bottom, there are 'Cancel', 'Back', and 'Finish' buttons.

9. Sur la page **Créer une liste de distribution d'e-mails**, indiquez un nom pour la liste de distribution d'e-mails. Ajoutez le serveur de messagerie SMTP à utiliser pour envoyer des notifications par e-mail au serveur de messagerie. Dans la zone **De**, ajoutez l'adresse e-mail à partir de laquelle envoyer des messages. Dans la zone **À**, ajoutez l'adresse e-mail ou les adresses auxquelles envoyer des messages. Vous pouvez également ajouter une ou plusieurs adresses e-mail auxquelles envoyer des copies et des copies de messages sans afficher ces adresses dans les messages ou les copies. Cliquez sur **Créer**. Après avoir créé la liste de distribution d'e-mails, cliquez sur **Terminer** pour terminer le processus de configuration.

### Create Email Distribution List

Name\*

Email Servers\*

From

To\*

Cc

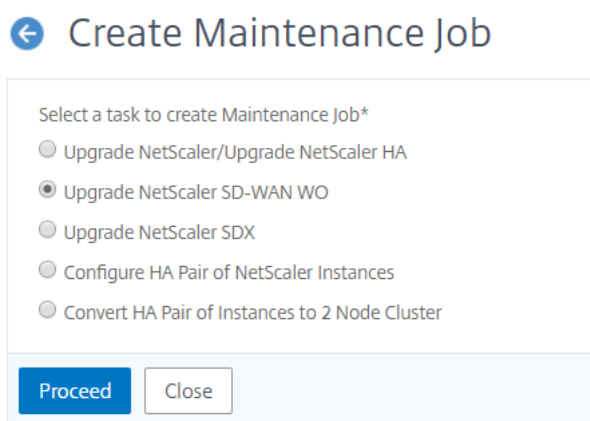
 

Bcc

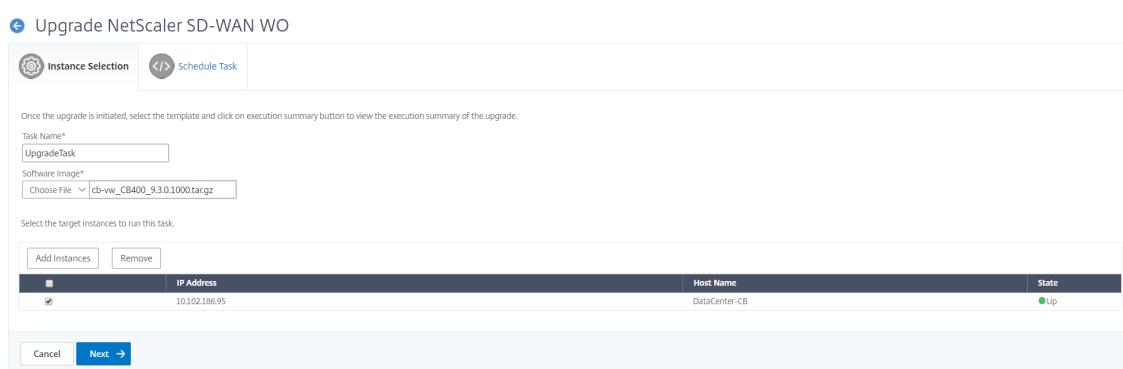


## Planifier la mise à niveau des instances WO Citrix SD-WAN

1. Dans Citrix ADM, accédez à **Réseaux** > Tâches de **configuration** > **Tâches** de **maintenance**. Cliquez sur le bouton **Créer une tâche**.
2. Sur la page **Créer un travail de maintenance**, sélectionnez **Mettre à niveau Citrix SD-WAN WO** et cliquez sur **Continuer**.



3. Dans la page **Mettre à niveau Citrix SD-WAN WO**, dans l'onglet **Sélection d'instance**, ajoutez un **nom de tâche**. Dans la liste des images logicielles, sélectionnez Local (votre machine locale) ou Appliance (le fichier de génération doit être présent sur l'appliance virtuelle Citrix MAS). Ajoutez les instances Citrix SD-WAN WO sur lesquelles vous souhaitez exécuter le processus de mise à niveau. Cliquez sur **Suivant**.



4. Pour mettre à niveau l'instance Citrix SD-WAN WO dès maintenant, sélectionnez **Maintenant** dans la liste des **modes d'exécution**. Cliquez sur **Terminer**.
5. Pour mettre à niveau l'instance Citrix SD-WAN WO 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 Citrix SD-WAN WO.
6. Vous pouvez activer la notification par e-mail pour recevoir le rapport d'exécution de la mise à niveau de l'instance Citrix SD-WAN WO. Cochez la case **Recevoir le rapport d'exécution par**

**e-mail** pour activer la notification par e-mail.

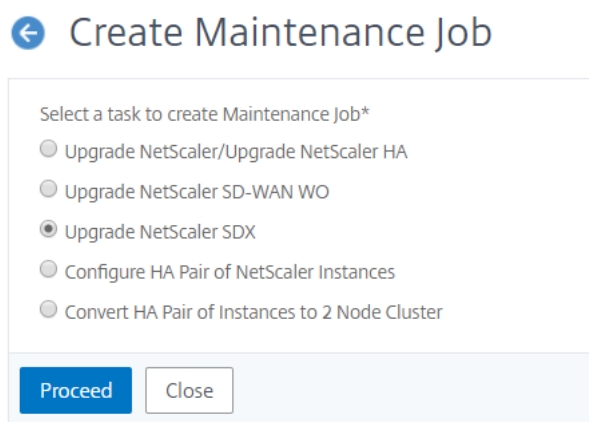
7. Sélectionnez l'icône **+** pour créer la liste de distribution d'e-mails.

8. Dans la page **Créer une liste de distribution de courrier électronique**, spécifiez un nom pour la liste de distribution de courrier électronique. Ajoutez le serveur de messagerie SMTP à utiliser pour envoyer des notifications par e-mail au serveur de messagerie. Dans la zone **De**, ajoutez l'adresse e-mail à partir de laquelle envoyer des messages. Dans la zone **À**, ajoutez l'adresse e-mail ou les adresses auxquelles vous souhaitez envoyer des messages. Vous pouvez également ajouter une ou plusieurs adresses e-mail auxquelles envoyer des copies et des copies des messages sans afficher ces adresses dans les messages ou les copies. Cliquez sur **Créer**. Après avoir créé la liste de distribution d'e-mails, cliquez sur **Terminer** pour terminer le processus de configuration.

## Planifier la mise à niveau des instances Citrix ADC SDX

1. Dans Citrix ADM, accédez à **Réseaux** > Tâches de **configuration** > Tâches de **maintenance**. Cliquez sur le bouton **Créer une tâche**.

2. Sur la page **Créer un travail de maintenance**, sélectionnez **Mettre à niveau Citrix ADC SDX**, puis cliquez sur **Continuer**.



3. Sur la page **Mettre à niveau le matériel SDX Citrix ADC**, dans l'onglet **Sélection d'instance**, ajoutez un **nom de tâche**. Dans la liste des images logicielles, sélectionnez Local (votre machine locale) ou Appliance (le fichier de génération doit être présent sur l'appliance virtuelle Citrix ADM). Ajoutez les instances Citrix ADC SDX sur lesquelles vous souhaitez exécuter le processus de mise à niveau. Cliquez sur **Suivant**.
4. Vous pouvez activer la notification par e-mail pour recevoir le rapport d'exécution de la mise à niveau de l'instance SDX Citrix ADC. Cochez la case **Recevoir le rapport d'exécution par e-mail** pour activer la notification par e-mail.
5. Sélectionnez l'icône **+** pour créer la liste de distribution d'e-mails.
6. Pour mettre à niveau l'instance Citrix ADC SDX dès maintenant, sélectionnez **Maintenant** dans la liste des **modes d'exécution**. Cliquez sur **Terminer**.
7. Pour mettre à niveau l'instance Citrix ADC SDX ultérieurement, sélectionnez **Plus tard** dans la liste 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 SDX Citrix ADC.
8. Dans la page **Créer une liste de distribution de courrier électronique**, spécifiez un nom pour la liste de distribution de courrier électronique. Ajoutez le serveur de messagerie SMTP à utiliser pour envoyer des notifications par e-mail au serveur de messagerie. Dans la zone **De**, ajoutez l'adresse e-mail à partir de laquelle envoyer des messages. Dans la zone **À**, ajoutez l'adresse e-mail ou les adresses auxquelles vous souhaitez envoyer des messages. Vous pouvez également ajouter une ou plusieurs adresses e-mail auxquelles envoyer des copies et des copies des messages sans afficher ces adresses dans les messages ou les copies. Cliquez sur **Créer**. Après avoir créé la liste de distribution d'e-mails, cliquez sur **Terminer** pour terminer le processus de configuration.

## Planifier la configuration de la paire HA d'instances Citrix ADC

1. Accédez à **Réseaux > Travaux de configuration > Travaux de maintenance** . Cliquez sur le bouton **Créer une tâche**.
2. Sur la page **Créer une tâche de maintenance**, sélectionnez **Configurer HA Pair of Citrix ADC Instances** et cliquez sur **Continuer**.

### ← Create Maintenance Job

Select a task to create Maintenance Job\*

- Upgrade NetScaler/Upgrade NetScaler HA
- Upgrade NetScaler SD-WAN WO
- Upgrade NetScaler SDX
- Configure HA Pair of NetScaler Instances
- Convert HA Pair of Instances to 2 Node Cluster

**Proceed**

3. Dans la page **Citrix ADC HA Paire**, dans l'onglet **Sélection d'instance**, ajoutez un **nom de tâche**. Entrez l'adresse IP principale et l'adresse secondaire, puis cliquez sur **Suivant**.

### ← NetScaler HA Pair

**Instance Selection** **Schedule Task**

Task Name\*

Primary IP Address\*  
 >

Secondary IP Address\*  
 >

Turn on INC(Independent Network Configuration) mode

**Next →**

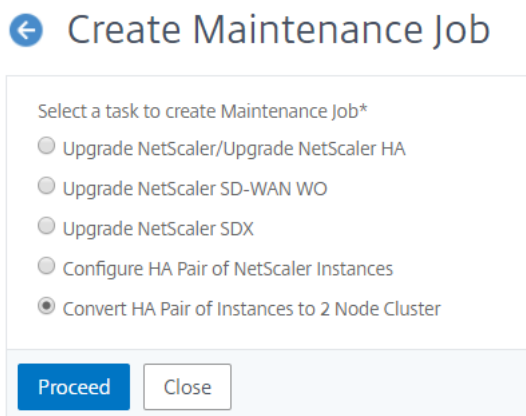
4. Sous l'onglet **Planifier la tâche**, vous pouvez choisir de configurer la paire Citrix ADC HA maintenant ou ultérieurement.
5. Pour configurer la paire Citrix ADC HA dès maintenant, sélectionnez **Maintenant** dans la liste des **modes d'exécution**. Vous pouvez activer la notification par e-mail pour recevoir le rapport

d'exécution de la paire Citrix ADC HA. Cochez la case **Recevoir le rapport d'exécution par e-mail** pour activer la notification par e-mail.

6. Pour configurer la paire Citrix ADC 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. Vous pouvez activer la notification par e-mail pour recevoir le rapport d'exécution de la paire Citrix ADC HA. Cochez la case **Recevoir le rapport d'exécution par e-mail** pour activer la notification par e-mail.
7. Sélectionnez l'icône **+** pour créer la liste de distribution d'e-mails.
8. Sur la page **Créer une liste de distribution d'e-mails**, indiquez un **nom** pour la liste de distribution d'e-mails. Ajoutez le serveur de messagerie SMTP à utiliser pour envoyer des notifications par e-mail au serveur de messagerie. Dans la zone **De**, ajoutez l'adresse e-mail à partir de laquelle vous souhaitez envoyer les messages. Dans la zone **À**, ajoutez l'adresse e-mail ou les adresses auxquelles vous souhaitez envoyer des messages. Vous pouvez également ajouter une ou plusieurs adresses e-mail auxquelles envoyer des copies et des copies des messages sans afficher ces adresses dans les messages ou les copies. Cliquez sur **Créer**. Après avoir créé la liste de distribution d'e-mails, cliquez sur **Terminer** pour terminer le processus de configuration.

## Planifier la conversion d'une paire d'instances HA en cluster

1. Accédez à **Réseaux > Travaux de configuration > Travaux de maintenance** . Cliquez sur le bouton **Créer une tâche**.
2. Sur la page **Créer un travail de maintenance**, sélectionnez **Convertir une paire d'instances HA en cluster à 2 nœuds**, puis cliquez sur **Continuer** .



3. Sur la page **Migrer Citrix ADC HA vers le cluster**, dans l'onglet **Sélection d'instance**, ajoutez un **nom de tâche**. Spécifiez l'adresse IP principale, l'adresse secondaire, l'ID du nœud principal, l'ID du nœud secondaire, l'adresse IP du cluster, l'ID du cluster et le backplane. Cliquez sur **Suivant**.

## ← Migrate NetScaler HA to Cluster

⚙️ Instance Selection </> Schedule Task

Task Name\*

Primary IP Address\*

Secondary IP Address\*

Primary Node ID\*

Secondary Node ID\*

Cluster IP Address\*

Cluster ID\*

Backplane\*

4. Sous l'onglet **Planifier la tâche**, vous pouvez choisir de migrer la HA Citrix ADC vers Cluster maintenant ou une version ultérieure.
5. Pour configurer la paire Citrix ADC 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. Vous pouvez activer la notification par e-mail pour recevoir le rapport d'exécution de la paire Citrix ADC HA. Cochez la case **Recevoir le rapport d'exécution par e-mail** pour activer la notification par e-mail.
6. Sélectionnez l'icône **+** pour créer la liste de distribution d'e-mails.
7. Dans la page **Créer une liste de distribution de courrier électronique**, spécifiez un nom pour la liste de distribution de courrier électronique. Ajoutez le serveur de messagerie SMTP à utiliser pour envoyer des notifications par e-mail au serveur de messagerie. Dans la zone **De**, ajoutez l'adresse e-mail à partir de laquelle vous souhaitez envoyer les messages. Dans la zone **À**, ajoutez l'adresse e-mail ou les adresses auxquelles vous souhaitez envoyer des messages. Vous pouvez également ajouter une ou plusieurs adresses e-mail auxquelles envoyer des copies et des

copies des messages sans afficher ces adresses dans les messages ou les copies. Cliquez sur **Créer**. Après avoir créé la liste de distribution d'e-mails, cliquez sur **Terminer** pour terminer le processus de configuration.

## Audit de configuration

February 1, 2024

Ce document comprend :

- [Création de modèles d'audit](#)
- [Affichage des rapports d'audit](#)
- [Modifications de configuration d'audit entre les instances](#)
- [Obtenir des conseils de configuration sur la configuration réseau](#)
- [Comment interroger l'audit de configuration des instances NetScaler](#)

## Créer des modèles d'audit

February 1, 2024

Vous voulez vous assurer que certaines configurations s'exécutent sur des instances spécifiques pour des performances optimales de votre réseau. Vous souhaitez également surveiller les modifications de configuration sur les instances de Citrix Application Delivery Controller (ADC) gérées, résoudre les erreurs de configuration et restaurer les configurations non enregistrées après un arrêt soudain du système. Vous pouvez créer des modèles d'audit avec des configurations spécifiques que vous souhaitez auditer sur certaines instances. Citrix Application Delivery Management (Citrix ADM) compare ces instances avec le modèle d'audit et signale s'il y a une incompatibilité dans la configuration. Chaque fois qu'il y a une incompatibilité de configuration, Citrix ADM génère un rapport de diff de configuration, qui vous permet de résoudre les problèmes et de corriger les modifications de configuration indésirables.

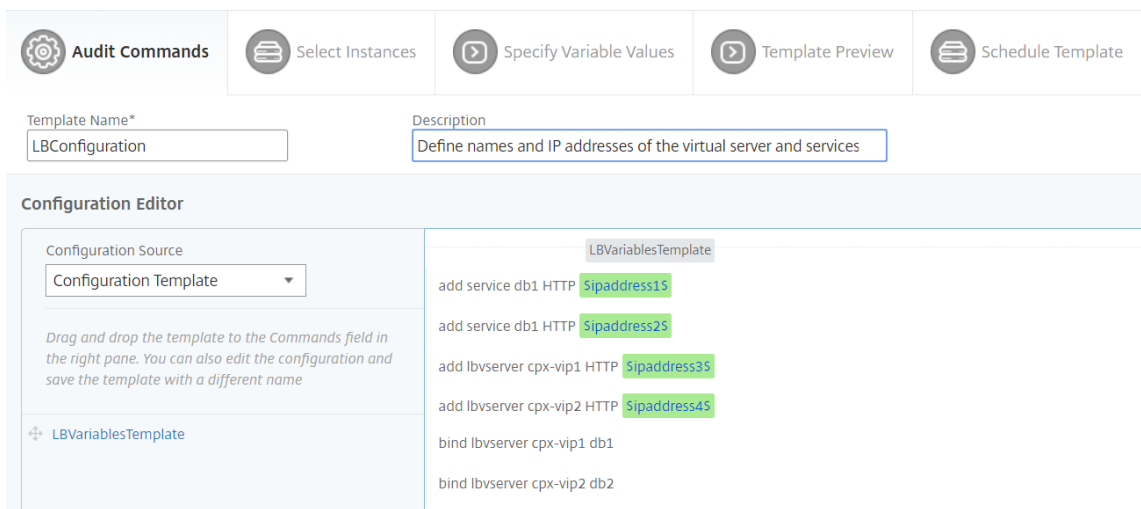
Vous pouvez automatiser l'exécution du modèle d'audit en

- Planification de l'heure à laquelle le modèle doit être exécuté
- Définition de la fréquence à laquelle Citrix ADM doit exécuter le modèle. Vous pouvez exécuter le modèle tous les jours, un jour spécifique d'une semaine ou à une date spécifique d'un mois.

Vous avez également la possibilité d'envoyer le rapport de comparaison généré par Citrix ADM à des adresses e-mail spécifiées que vous pouvez configurer. Cette option permet à votre utilisateur de recevoir le rapport sous la forme d'une pièce jointe et il n'est pas nécessaire que l'utilisateur se connecte à Citrix ADM pour exporter les rapports manuellement.

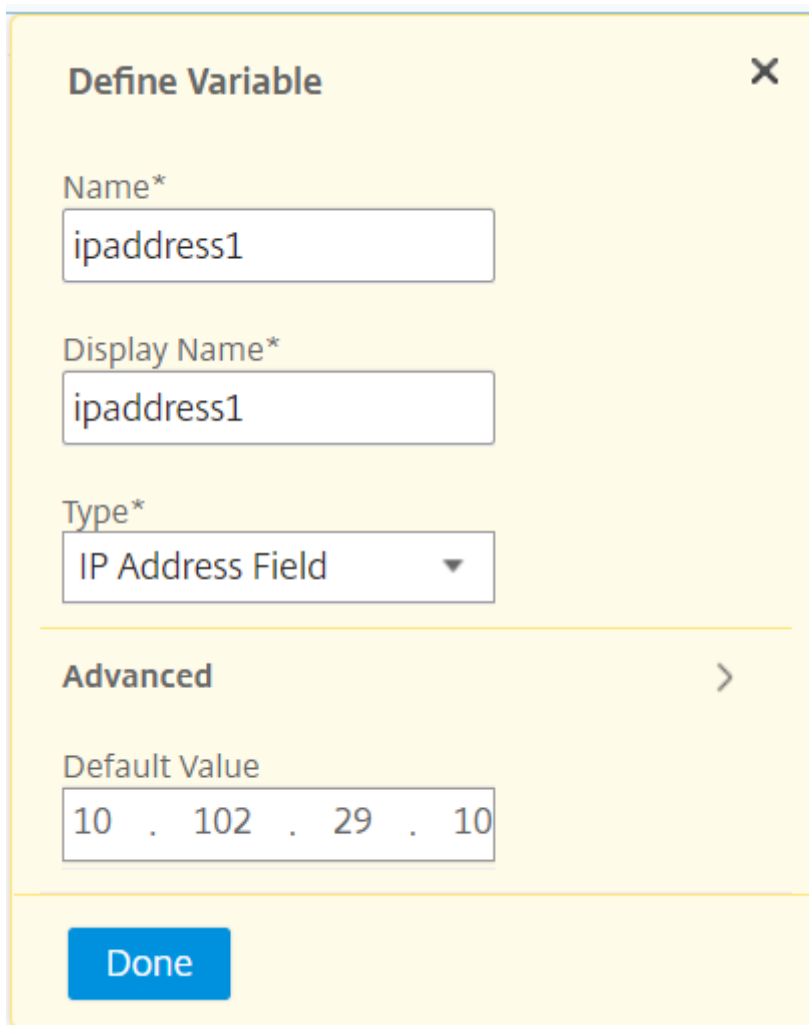
**Pour créer des modèles d'audit :**

1. Accédez à **Réseaux > Audit de configuration > Modèles d'audit**, puis cliquez sur **Ajouter**.
2. Dans la page **Créer un modèle** et dans l'onglet **Commandes d'audit**, spécifiez le nom du modèle et sa description.
3. Sur la page **Éditeur de configuration**, saisissez vos commandes et enregistrez-les en tant que modèle de configuration. Vous pouvez également faire glisser un modèle existant du volet gauche vers l'éditeur.
4. Sélectionnez les valeurs que vous souhaitez convertir en variable, puis cliquez sur **Convertir en variable**. Par exemple, sélectionnez l'adresse IP du serveur d'équilibrage de charge « ipaddress1 », puis cliquez sur **Convertir en variable**. La variable est maintenant entourée de « \$ » comme indiqué dans l'image ci-dessous.



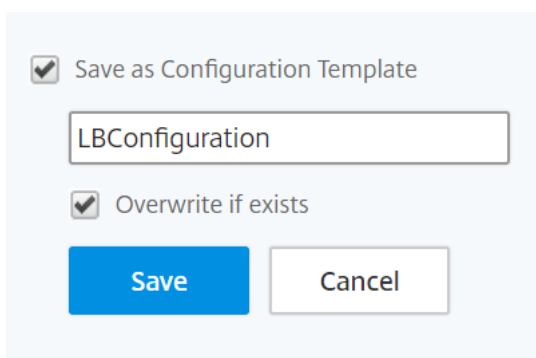
Dans la fenêtre **Définir une variable**, définissez les propriétés de cette variable - nom, nom d'affichage et type de la variable. Cliquez sur l'option **Avancé** si vous souhaitez spécifier une valeur par défaut pour votre variable.





The image shows a 'Define Variable' dialog box with a yellow background and a close button (X) in the top right corner. It contains three input fields: 'Name\*' with the value 'ipaddress1', 'Display Name\*' with the value 'ipaddress1', and 'Type\*' with a dropdown menu set to 'IP Address Field'. Below these fields is an 'Advanced' section with a right-pointing chevron. Under 'Advanced', there is a 'Default Value' field containing the IP address '10 . 102 . 29 . 10'. At the bottom of the dialog is a blue 'Done' button.

Vous pouvez également enregistrer les commandes en tant que modèle de configuration.



The image shows a 'Save as Configuration Template' dialog box with a light blue background. It features a checked checkbox for 'Save as Configuration Template' and a text input field containing 'LBConfiguration'. Below this is another checked checkbox for 'Overwrite if exists'. At the bottom are two buttons: a blue 'Save' button and a white 'Cancel' button.

5. Cliquez sur **Enregistrer**, puis sur **Suivant**.
6. Dans l'onglet **Sélectionner les instances**, sélectionnez les instances sur lesquelles vous souhaitez exécuter l'audit de configuration et cliquez sur **Suivant**.

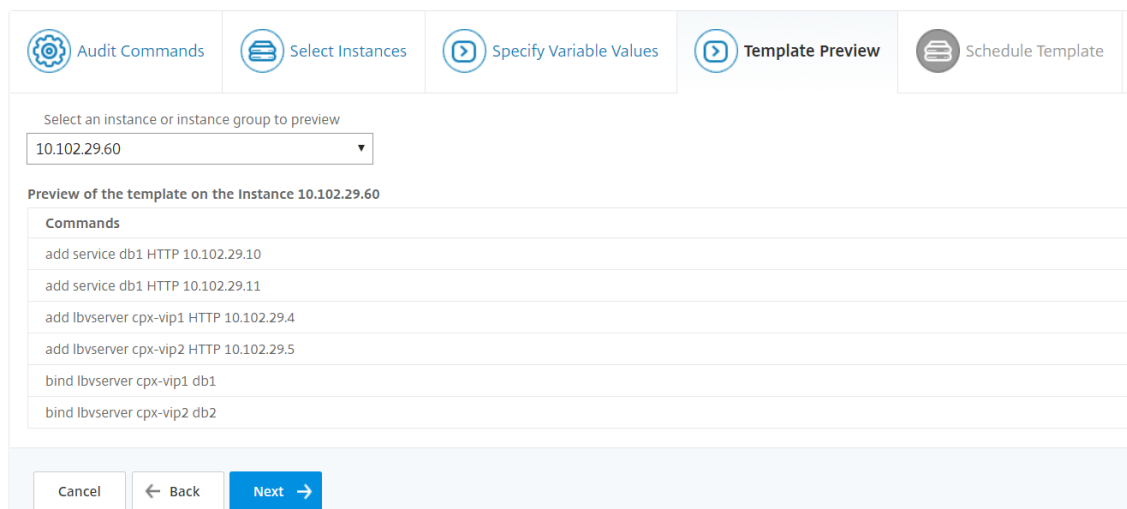
7. Dans l'onglet **Spécifier les valeurs variables**, vous disposez de deux options :

- a) Téléchargez le fichier d'entrée pour entrer les valeurs des variables que vous avez définies dans vos commandes, puis téléchargez le fichier sur le serveur Citrix ADM
- b) Entrez des valeurs communes pour les variables que vous avez définies pour toutes les instances

8. Cliquez sur **Suivant**.

← Create Template

9. Dans l'onglet **Aperçu du modèle**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances. Cliquez sur **Suivant**.



10. Dans l'onglet **Modèle de planification**, vous disposez des options suivantes pour planifier l'exécution du modèle et configurer l'adresse de messagerie pour envoyer le rapport de diff.

- **Utilisez l'intervalle d'interrogation global.** Sélectionnez cette option pour exécuter le modèle sur les instances à un moment configuré globalement sur Citrix ADM.

#### Remarque

Pour configurer l'intervalle d'interrogation global dans Citrix ADM, accédez à **Réseaux > Audit de configuration > Modèles d'audit**, puis cliquez sur **Intervalle d'interrogation globale**. Dans le champ **Intervalle d'interrogation**, entrez les minutes auxquelles Citrix ADM doit interroger globalement les instances.

- **Personnaliser la planification du modèle.** Utilisez cette option pour configurer l'heure et la fréquence auxquelles les modèles doivent être exécutés
- **Envoyer le rapport par courrier électronique.** Utilisez cette option pour configurer le profil de messagerie auquel le rapport de diff doit être envoyé en tant que pièce jointe.

11. Cliquez sur **Terminer**.

### ← Create Template

Audit Commands  Select Instances  Specify Variable Values  Template Preview  Schedule Template

You can either use polling interval or customized schedule

Use global polling interval

Customize template schedule

Recurrence\*

Daily

Schedule time (format HH:MM)\*

06:00

Send report through email

Mail Profile

abcd

Le modèle d'audit apparaît dans la liste **Modèles d'audit** et est exécuté à l'heure planifiée par rapport aux configurations dans les instances spécifiées.

## Afficher les rapports d'audit

February 1, 2024

Citrix Application Delivery Management (Citrix ADM) vous permet d'afficher et de télécharger le rapport d'audit de configuration dans la section Audit de configuration. La section Audit de configuration vous permet d'exporter le rapport de synthèse sur toutes les instances et par instance, et vous permet également d'exporter un rapport de diff granulaire pour chaque paire de modèles d'instance.

Les modèles d'audit qui apparaissent dans la liste Modèles d'audit sont exécutés à l'heure planifiée sur les configurations des instances spécifiées. Le graphique **NetScaler Config Drift** du tableau de bord de l'**audit de configuration** affiche des détails de haut niveau sur les modifications de configuration enregistrées par rapport aux configurations non enregistrées. Lorsque vous cliquez sur le graphique de **dérive de configuration NetScaler**, la page **Rapports d'audit** qui suit affiche une liste d'instances indiquant à la fois « Diff Exists » et « No Diff ». Vous pouvez télécharger les rapports diff affichés par Citrix ADM.

Citrix ADM fournit également une option pour planifier l'exportation automatique du rapport diff en tant que pièce jointe de messagerie. Pour plus d'informations sur la façon de planifier l'exportation des rapports, consultez [Création de modèles d'audit](#).

### Pour exporter des rapports d'audit de configuration :

1. Dans Citrix ADM, accédez à **Réseaux > Audit de configuration**.
2. Sur la page **Configuration Audit**, cliquez dans le graphique **NetScaler Config Drift**.
3. La page **Rapports d'audit** répertorie les instances qui présentent une différence. La page affiche également une liste d'instances qui ne présentent aucune différence dans leurs configurations en cours d'exécution.

Audit Reports

Instance	Host Name	Saved vs Running Diff	Template vs Running Diff	Config Saved
10.106.43.13		No Diff	NA	Yes
10.102.29.191		NA	No Diff	No
10.106.43.12		Diff Exists	NA	No
10.106.43.7		No Diff	NA	Yes
10.102.205.27	HA-Node2-admin-NetScalerVPX	No Diff	No Diff	Yes
10.102.29.140	MyCache	Diff Exists	No Diff	No
10.102.29.191-P1		NA	No Diff	No
10.102.29.60		Diff Exists	Diff Exists	No

Dans l'image, vous pouvez voir que pour certains cas, un diff est présent uniquement dans **Sauvegardé vs Running Diff** et pour certains cas, un diff est présent uniquement dans **Template vs Running Diff**. Dans certains cas, des différences existent à la fois entre **Saved et Running Diff** et entre **Template et Running Diff**.

### Sauvegardé vs Exécution Diff

Vous pouvez afficher un rapport de diff entre la configuration enregistrée sur l'instance et la configuration en cours d'exécution sur cette instance. Par exemple, cliquez sur **Diff Exists** pour une instance sous **Saved vs Running Diff**.

Instance	Host Name	Saved vs Running Diff	Template vs Running Diff	Config Saved
10.106.43.13		No Diff	NA	Yes
10.102.29.191		NA	No Diff	No
10.106.43.12		Diff Exists	NA	No
10.106.43.7		No Diff	NA	Yes
10.102.205.27	HA-Node2-admin-NetScalerVPX	No Diff	No Diff	Yes
10.102.29.140	MyCache	Diff Exists	No Diff	No
10.102.29.191-P1		NA	No Diff	No
10.102.29.60		Diff Exists	Diff Exists	No

Ici, vous pouvez voir un rapport pour la configuration enregistrée par rapport à l'exécution de diff de configuration pour cette instance.

Configuration Diff

Saved vs Running Diff - Instance: (10.102.29.60)

Create job Export diff report Export corrective commands

Saved Configuration	Running Configuration	Correction Configuration
set urfiltering parameter -TimeOfDayToJupdateDB 03:00 -ProxyPa ssword b63a0b9e68619fe528b62402791659d8719aee26ec0c10661aed9e78e80509 7 -encrypted -encryptmethod ENCMTD_3	set urfiltering parameter -TimeOfDayToJupdateDB 03:00 -ProxyPa ssword a3962b89cfc8a32e2e34d690e9df2142c1a744386f8adbfb22b405d31af449f -encrypted -encryptmethod ENCMTD_3	

Close

Cliquez sur **Exporter le rapport diff** pour télécharger un fichier .csv du rapport diff. Vous pouvez également cliquer sur Exporter les commandes correctives pour exporter les commandes dans un fichier .txt. Vous pouvez ensuite exécuter les commandes sur l'instance Citrix ADM associée à partir des tâches de configuration pour corriger la configuration dans cette instance.

### Modèle vs Courir Diff

Le **modèle vs Running Diff** inclut tous les modèles autres que **Sauvegardé vs Running Diff**, qui est le modèle par défaut. Vous pouvez afficher la différence qui existe entre le modèle et la configuration en cours d'exécution. Par exemple, cliquez sur **Diff Exists** pour l'une des instances sous **Modèle vs Running Diff**.

Instance	Host Name	Saved vs Running Diff	Template vs Running Diff	Config Saved
10.106.43.13		● No Diff	NA	✓ Yes
10.102.29.191		NA	● No Diff	✗ No
10.106.43.12		● Diff Exists	NA	✗ No
10.106.43.7		● No Diff	NA	✓ Yes
10.102.205.27	HA-Node2-admin-NetScalerVPX	● No Diff	● No Diff	✓ Yes
10.102.29.140	MyCache	● Diff Exists	● No Diff	✗ No
10.102.29.191-P1		NA	● No Diff	✗ No
10.102.29.60		● Diff Exists	● Diff Exists	✗ No

Maintenant, vous pouvez voir que deux modèles affichent diff et que l'instance Citrix ADM a une configuration différente de celle que le modèle recherche.

Templates of Instance: 10.102.29.60

Templates	Diff Exists	Last Updated
LBVariablesTemplate	● Diff Exists	Oct 10 2017 05:30:02
LBConfigurationAudit	● Diff Exists	Oct 27 2017 12:14:30

Cliquez à nouveau sur **Diff Exists**. L'image suivante montre la configuration recherchée par le modèle et la configuration en cours d'exécution vide, car aucune commande de ce type n'a été configurée ou n'a été supprimée. Vous pouvez également voir les configurations de correction ou les commandes à exécuter pour corriger la configuration.

Configuration Diff

Template vs Running Diff of Instance: 10.102.29.60 and Template: LBVariablesTemplate

Create job **Export diff report** Export corrective commands

Template Configuration	Running Configuration	Correction Configuration
add service lbservice2 10.102.29.11 HTTP 80		add service lbservice2 10.102.29.11 HTTP 80
add service lbservice1 10.102.29.10 HTTP 80		add service lbservice1 10.102.29.10 HTTP 80
add lb vserver lserver1 HTTP 10.102.29.1 80		add lb vserver lserver1 HTTP 10.102.29.1 80
bind lb vserver servname lbservice2		bind lb vserver servname lbservice2

Close

Cliquez sur **Exporter le rapport diff** pour télécharger un fichier .csv du rapport diff. Vous pouvez également cliquer sur **Exporter les commandes correctives** pour exporter les commandes dans un

fichier .txt. Vous pouvez ensuite exécuter les commandes dans l'interface de ligne de commande pour corriger la configuration dans cette instance.

L'image suivante montre un exemple de fichier diff .csv téléchargé sur votre système :

#Template vs Running Diff of Instance: 10.102.29.60 and Template: LBVariablesTemplate		
Template Configuration	Running Configuration	Correction Configuration
add service lbservice2 10.102.29.11 HTTP 80		add service lbservice2 10.102.29.11 HTTP 80
add service lbservice1 10.102.29.10 HTTP 80		add service lbservice1 10.102.29.10 HTTP 80
add lb vserver lserver1 HTTP 10.102.29.1 80		add lb vserver lserver1 HTTP 10.102.29.1 80
bind lb vserver servername lbservice2		bind lb vserver servername lbservice2

## Modifications de configuration d'audit entre les instances

February 1, 2024

Vous voulez vous assurer que certaines configurations s'exécutent sur des instances spécifiques pour des performances optimales de votre réseau. Vous souhaitez également surveiller les modifications de configuration sur les instances de Citrix Application Delivery Controller (ADC) gérées, résoudre les erreurs de configuration et restaurer les configurations non enregistrées après un arrêt soudain du système. Vous pouvez créer des modèles d'audit avec des configurations spécifiques que vous souhaitez exécuter sur certaines instances. Citrix Application Delivery Management (Citrix ADM) compare ces instances avec le modèle d'audit et signale en cas de non-concordance dans la configuration. Cela vous permet de dépanner et de corriger les erreurs.

Vous pouvez automatiser l'exécution du modèle d'audit en planifiant l'heure à laquelle le modèle doit être exécuté. Vous pouvez également définir la fréquence à laquelle Citrix ADM doit exécuter le modèle. Vous pouvez exécuter le modèle tous les jours, un jour spécifique d'une semaine ou à une date spécifique d'un mois. Vous avez également la possibilité d'envoyer le rapport diff généré par Citrix ADM aux adresses e-mail spécifiées que vous pouvez configurer. Par cette option, votre utilisateur reçoit le rapport en tant que pièce jointe et il n'est pas nécessaire que l'utilisateur se connecte à Citrix ADM pour vérifier manuellement les rapports.

### Pour créer des modèles d'audit :

1. Accédez à **Réseaux > Audit de configuration > Modèles d'audit**, puis cliquez sur **Ajouter**.
2. Dans la page **Créer un modèle** et dans l'onglet **Commandes d'audit**, spécifiez le nom du modèle et sa description.
3. Dans l'**Éditeur de configuration**, tapez vos commandes et enregistrez les commandes en tant que modèle de configuration. Vous pouvez également faire glisser un modèle existant à partir du volet gauche de l'éditeur.

4. Sélectionnez les valeurs que vous souhaitez convertir en variable, puis cliquez sur **Convertir en variable**. Par exemple, sélectionnez l'adresse IP du serveur d'équilibrage de charge « ipaddress » et cliquez sur **Convertir en variable** comme indiqué dans l'image ci-dessous.

← Create Template

The screenshot shows the 'Create Template' workflow in the NetScaler Configuration Editor. At the top, there are five tabs: 'Audit Commands', 'Select Instances', 'Specify Variable Values', 'Template Preview', and 'Schedule Template'. Below the tabs, there are two input fields: 'Template Name\*' with the value 'LBConfiguration' and 'Description' with the value 'Define names and IP addresses of the virtual server and services'. The main area is the 'Configuration Editor', which has a 'Configuration Source' dropdown set to 'Configuration Template'. Below this, there is a text box with instructions: 'Drag and drop the template to the Commands field in the right pane. You can also edit the configuration and save the template with a different name'. On the right side, there is a list of configuration commands with variables highlighted in green: 'add lb vserver \$servername\$ HTTP \$ipaddress\$ \$portnumbers\$', 'add service \$servicename1\$ \$ipaddress1\$ HTTP 80', 'add service \$servicename2\$ \$ipaddress2\$ HTTP 80', 'bind lb vserver \$servername\$ \$servicename1\$', and 'bind lb vserver \$servername\$ \$servicename2\$'. A '+ LBVariablesTemplate' button is visible at the bottom left of the editor area.

- 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.

The screenshot shows a dialog box titled 'Save as Configuration Template'. It has a checked checkbox 'Save as Configuration Template' and a text input field containing 'LBConfiguration'. Below this, there is another checked checkbox 'Overwrite if exists'. At the bottom, there are two buttons: 'Save' (in a blue box) and 'Cancel' (in a white box with a grey border).

5. Cliquez sur **Enregistrer**, puis sur **Suivant**.
6. Dans l'onglet **Select Instances**, sélectionnez les instances sur lesquelles vous souhaitez exécuter l'audit de configuration.
7. Dans l'onglet **Spécifier les valeurs variables**, vous disposez de deux options :
  - a) Téléchargez le fichier d'entrée pour entrer les valeurs des variables que vous avez définies dans vos commandes, puis téléchargez le fichier sur le serveur Citrix ADM
  - b) Entrez des valeurs communes pour les variables que vous avez définies pour toutes les instances
8. Cliquez sur **Suivant**.



← Create Template

Audit Commands
  Select Instances
  Specify Variable Values
  Template Preview
  Schedule Template

Specify the values to all the command variables.

Upload input file for variables values  
 Common Variable Values for all Instances

servername

ipaddress

portnumber

servicename1

ipaddress1

servicename2

ipaddress2

9. Dans l'onglet **Aperçu du modèle**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances. Cliquez sur **Suivant**.
10. Dans l'onglet **Modèle de calendrier**, vous disposez de trois options pour automatiser l'exécution du modèle et l'adresse e-mail pour envoyer le rapport de comparaison.
  - **Utilisez l'intervalle d'interrogation global.** Sélectionnez cette option pour exécuter le modèle sur les instances à un moment configuré globalement sur Citrix ADM
  - **Personnaliser la planification du modèle.** Utilisez cette option pour configurer l'heure et la fréquence auxquelles les modèles doivent être exécutés
  - **Envoyer le rapport par courrier électronique.** Utilisez cette option pour configurer le profil de messagerie auquel le rapport de diff doit être envoyé en tant que pièce jointe.
11. Cliquez sur **Terminer**.

### ← Create Template

Audit Commands  Select Instances  Specify Variable Values  Template Preview  **Schedule Template**

You can either use polling interval or customized schedule

Use global polling interval

Customize template schedule

Recurrence\*

Daily

Schedule time (format HH:MM)\*

06:00

Send report through email

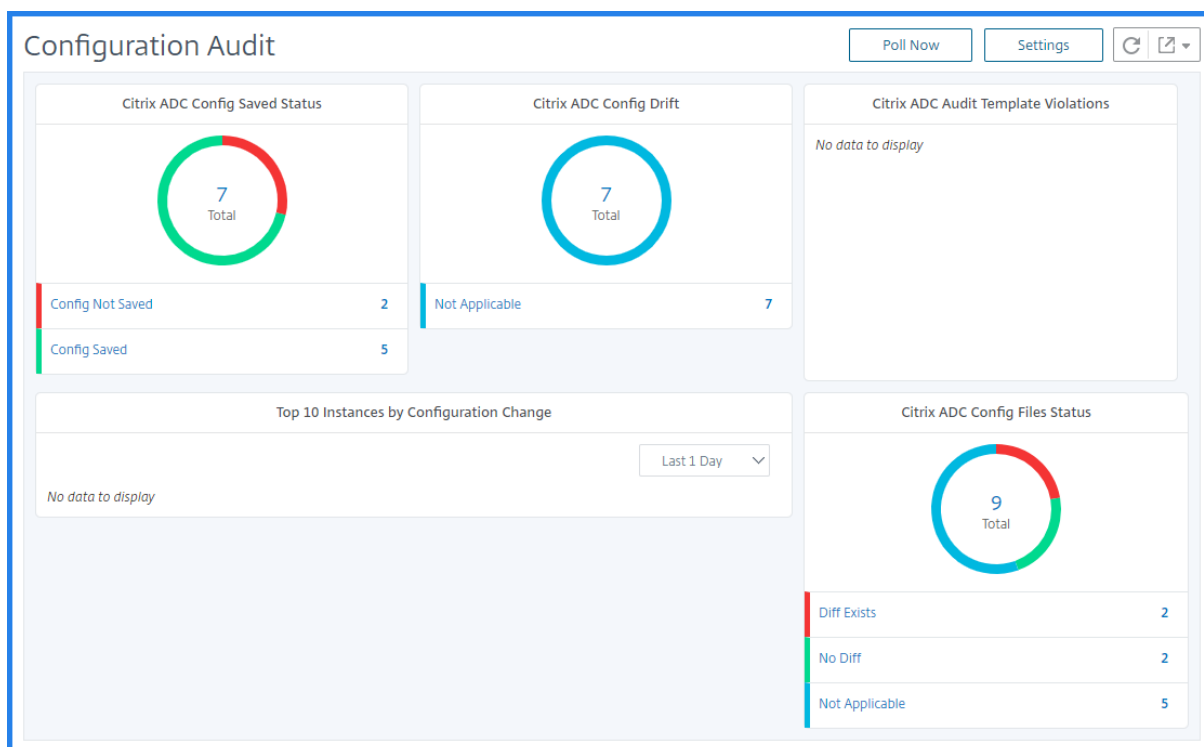
Mail Profile

abcd

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.

### Affichage des détails des modifications de configuration

Vous pouvez également utiliser le tableau de bord d’audit de configuration pour afficher des informations détaillées sur les modifications de configuration, telles que les dix principales instances par modification de configuration ou le nombre de configurations enregistrées et non enregistrées.



Citrix ADM vous permet également d’interroger manuellement les audits de configuration et ajoute immédiatement tous les audits de configuration des instances à Citrix ADM. Pour ce faire, accédez à **Réseaux > Audit de configuration**, cliquez sur **Sondage maintenant** . La page contextuelle **Sondage maintenant** vous permet d’interroger toutes les instances Citrix ADC du réseau ou d’interroger les instances sélectionnées.

Vous pouvez également forcer un audit sur une instance. Pour ce faire, cliquez sur le **graphique d’état** enregistré de NetScaler Config ou sur le graphique **NetScaler Config Drift**. Sur la page **Rapports d’audit** , sélectionnez l’instance et, dans la liste des **actions** , sélectionnez **Poll Now w**.

Audit Reports

Running Configuration   Saved Configuration   Save configuration   **Poll Now**   Action

Instance	Host Name	Last Updated	Saved vs Running Diff	Template vs Running Diff	Config Saved
<input checked="" type="checkbox"/> 10.102.29.140	MyCache	Thu, 13 Jul 2017 15:21:31 GMT	Diff Exists	NA	No
<input type="checkbox"/> 10.102.29.60		Thu, 13 Jul 2017 15:21:35 GMT	No Diff	Diff Exists	Yes

**Pour définir les notifications d’audit de configuration :**

1. Accédez à **Réseaux > Audit de configuration**.
2. Dans la page **Audit de configuration**, cliquez sur **Paramètres** .
3. Sur la page **Paramètres de notification**, cliquez sur l’icône **Modifier** pour activer les paramètres de notification.
4. Cochez la case **Activé**, puis choisissez une liste de distribution d’e-mails dans la liste déroulante. Vous pouvez également créer une liste de distribution d’e-mails en cliquant sur l’icône **+** et en

spécifiant les détails du serveur de messagerie.

## Obtenir des conseils de configuration sur la configuration du réseau

February 1, 2024

Vous configurez vos instances de Citrix Application Delivery Controller (ADC) avec des configurations optimales afin d'obtenir des performances optimales sur vos applications. Cependant, il peut arriver que certaines configurations ne soient pas des configurations standard, ce qui peut affecter les performances de vos applications.

Pour vous aider à optimiser les performances de votre application, Citrix Application Delivery Management (Citrix ADM) analyse la configuration de l'instance Citrix ADC et vous fournit des recommandations. Vous pouvez appliquer les configurations recommandées à partir de Citrix ADM.

### Pour analyser l'instance de Citrix ADC :

1. Accédez à **Réseaux > Audit de configuration > Conseil de configuration** .
2. Procédez comme suit :
  - Cliquez sur **Charger le fichier de configuration** et téléchargez le fichier de configuration de votre instance réseau.
  - Cliquez sur **Sélectionner un périphérique** et sélectionnez l'instance Citrix ADC que vous souhaitez analyser.

Citrix ADM analyse la configuration de votre instance et fournit une liste de recommandations de configuration, comme indiqué dans l'image ci-dessous. Cochez la case située en regard d'un conseil de configuration pour afficher les commandes correctives.

### 10.102.29.60

Recommendations | 52 Search in Advice x

Filter By: Category All Commands Selected 1

Category	Advice	
System Settings	DNS server is currently not configured. Please make sure this is configured.	<input type="checkbox"/>
User Administration	Please ensure there are accounts other than nsroot. Command: add system user <userName> <Password> -timeout 600 add system user <userName> <Password> -timeout 600	<input checked="" type="checkbox"/>
User Administration	Please ensure system users other than nsroot are bound to an RBA policy.	<input type="checkbox"/>
System Settings	The following features must be enabled : IPV6PT, AAA, SUBSCRIBER, AAA, APPFW.	<input type="checkbox"/>

Si vous souhaitez mettre à jour votre configuration, spécifiez les valeurs des variables dans les commandes correctives et cliquez sur **Appliquer maintenant**, comme indiqué dans l’image ci-dessous.

#### 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 devraient pas modifier les commandes.

### 10.102.29.60

Recommendations | 52 Search in Advice x

Filter By: Category All Commands Selected 1

Category	Advice		
System Settings	DNS server is currently not configured. Please make sure this is configured.	<input type="checkbox"/>	Download File Apply Now
User Administration	Please ensure there are accounts other than nsroot. Command: add system user <userName> <Password> -timeout 600 add system user new-user new-user -timeout 600	<input checked="" type="checkbox"/>	

Lorsque la commande est exécutée avec succès sur l’instance réseau, la case à cocher en regard de l’avis disparaît.

User Administration	Please ensure there are accounts other than nsroot.	
---------------------	---	--

Si vous souhaitez afficher les détails des commandes exécutées sur votre instance réseau, accédez à **Réseaux > Instances > , <Instance\_Type>** sélectionnez l'adresse IP de l'instance, puis cliquez sur **Événements** dans la liste déroulante **Actions** liste.

The screenshot shows the NetScaler VPX interface. At the top, there is a breadcrumb trail: **Networks > Instances > NetScaler VPX**. Below this, the title **NetScaler VPX** is displayed. A row of buttons includes **Add**, **Edit**, **Remove**, **Dashboard**, **View Backup**, **Profiles**, and **Partitions**. Below the buttons is a table with the following columns: **IP Address**, **Host Name**, **State**, **Rx (Mbps)**, **Tx (Mbps)**, and **HTTP requests/sec**. The table contains four rows of data. To the right of the table, an **Actions** menu is open, listing various actions such as **Select Action**, **Create Cluster**, **Reboot**, **Events** (which is highlighted in blue), **Ping**, **TraceRoute**, **Rediscover**, **Enable/Disable Insight**, **Unmanage**, and **Annotate**.

	IP Address	Host Name	State	Rx (Mbps)	Tx (Mbps)	HTTP requests/sec
<input checked="" type="checkbox"/>	10.102.29.60	10.102.29.60	● Up	0	0	0
<input type="checkbox"/>	10.102.29.140	MyCache	● Up	0	0	0
<input type="checkbox"/>	10.102.29.93	10.102.29.93	● Up	0	0	0
<input type="checkbox"/>	10.102.29.200	MyCache	● Up	0	0	0

Sur la page **Événements**, vous pouvez afficher les détails de la modification de configuration.

The screenshot shows the **Events** page in the NetScaler VPX interface. At the top, there is a breadcrumb trail: **Networks > Instances > NetScaler VPX > Events**. Below this, the title **Events** is displayed. A row of buttons includes **Details** (highlighted with a red box), **History**, **Delete**, and **Clear**. To the right of the buttons, there are search and settings icons. Below the buttons, there is a filter section with the text **Filters: Source : 10.102.29.60** and a **Remove all** link. Below the filter section is a table with the following columns: **Severity**, **Source**, **Host Name**, **Date**, **Category**, **Failure Objects**, and **Configuration Command**. The table contains three rows of data.

	Severity	Source	Host Name	Date	Category	Failure Objects	Configuration Command
<input checked="" type="checkbox"/>	● Minor	10.102.29.60	10.102.29.60	Fri, 21 Apr 2017 16:32:48 GMT	netScalerConfigChange	nsroot	add system user new-user *****
<input type="checkbox"/>	● Minor	10.102.29.60	10.102.29.60	Wed, 19 Apr 2017 01:57:54 GMT	netScalerConfigSave	nsroot	
<input type="checkbox"/>	● Major	10.102.29.60	10.102.29.60	Wed, 19 Apr 2017 01:57:41 GMT	ipConflict	10.10.10.10	

## Audit de configuration d'interrogation des instances Citrix ADC

February 1, 2024

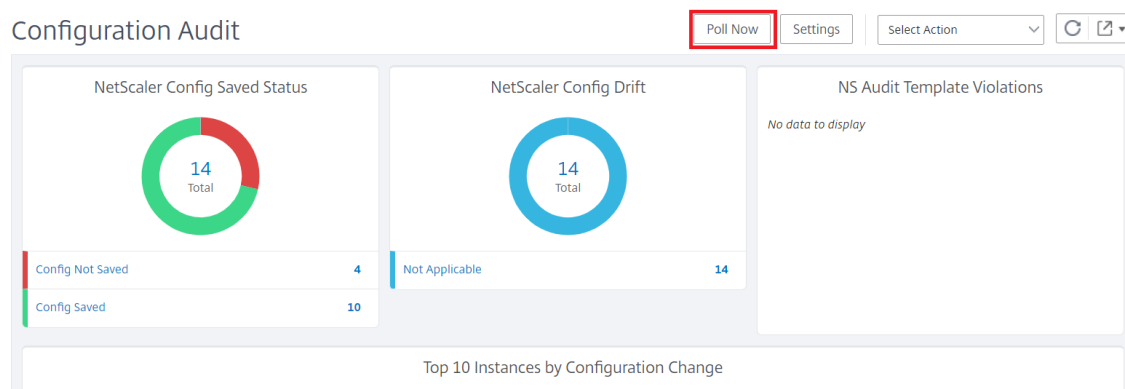
Citrix Application Delivery Management (Citrix ADM) interroge automatiquement les audits de configuration toutes les 10 heures pour rechercher les modifications de configuration qui se produisent sur les instances de Citrix Application Delivery Controller (ADC). Vous pouvez également interroger manuellement les audits de configuration pour découvrir les modifications récentes, mais l'interrogation de toutes les instances de Citrix ADC entraîne une lourde charge sur le réseau.

Au lieu d'interroger l'ensemble de l'audit de configuration des instances Citrix ADC, vous pouvez interroger manuellement uniquement les audits de configuration d'une ou plusieurs instances sélectionnées.

### Pour interroger les audits de configuration des instances Citrix ADC :

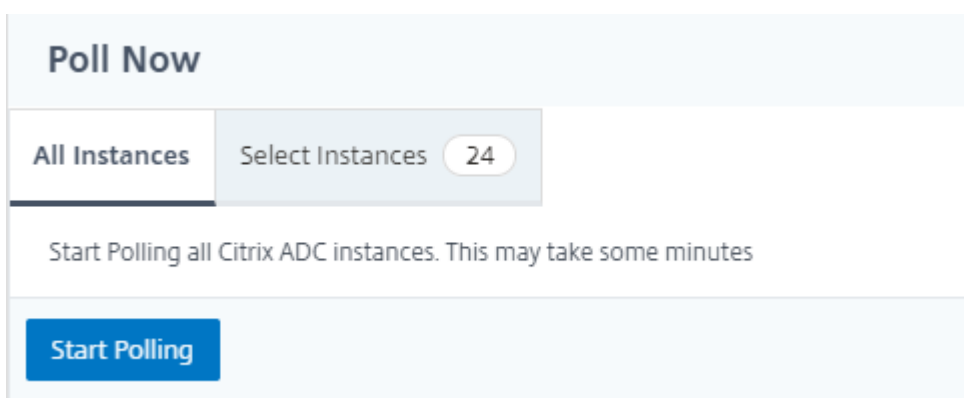
1. Dans Citrix ADM, accédez à **Réseaux > Audit de configuration**.

2. Dans la page **Audit de configuration**, dans le coin supérieur droit, cliquez sur **Sondage maintenant**.



3. La page **Interroger maintenant** apparaît, vous donnant la possibilité d’interroger toutes les instances Citrix ADC dans le réseau ou d’interroger les instances sélectionnées.

- a) Pour interroger toutes les instances Citrix ADC, sélectionnez l’onglet **Toutes les instances** et cliquez sur **Démarrer l’interrogation**.



- b) Pour interroger des instances spécifiques, sélectionnez l’onglet **Sélectionner des instances**, sélectionnez les instances dans la liste, puis cliquez sur **Interroger maintenant**.

<input type="checkbox"/>	IP Address	Host Name	Instance State
<input checked="" type="checkbox"/>	10.102.29.60	--	● Up
<input type="checkbox"/>	10.102.29.160-10.102.29.165	NS	● Up
<input checked="" type="checkbox"/>	10.102.29.200	--	● Up
<input type="checkbox"/>	10.102.29.200-TEST	--	● Up

## Générer un diff d'audit de configuration pour les interruptions SNMP ConfigChange

February 1, 2024

Chaque fois qu'il y a une modification de configuration dans une instance de Citrix Application Delivery Controller (ADC) dans le réseau, le fichier de configuration est mis à jour. L'instance envoie une interruption SNMP ConfigChange à Citrix Application Delivery Management (Citrix ADM). Vous pouvez activer Citrix ADM pour effectuer un audit de configuration sur cette instance lorsque l'instance envoie une interruption SNMP ConfigChange.

S'il existe une différence entre la configuration du modèle d'audit et la configuration en cours d'exécution, un message d'état Différent existe apparaît sur la page Rapport d'audit. En cliquant sur le lien Diff Exist, vous accédez à la page Configuration Diff, où vous pouvez afficher la commande corrective. Vous pouvez utiliser ces commandes correctives pour créer un travail de configuration et l'exécuter sur les instances d'ADC Citrix spécifiques. Lorsque vous exécutez le travail de configuration, les instances sont ramenées à la configuration souhaitée. Pour plus d'informations sur la façon de créer un travail de configuration à partir de commandes correctives, consultez [Comment créer des travaux de configuration à partir de commandes correctives sur Citrix ADM](#).

### Pour exécuter des modèles d'audit de configuration lors de la réception de l'interruption SNMP ConfigChange :

Citrix ADM vous permet d'activer l'option permettant d'exécuter le modèle d'audit de configuration dans Citrix ADM.

1. Dans Citrix ADM, accédez à **Réseaux > Audit de configuration**.
2. Cliquez sur **Paramètres** dans la page **Vérification de la configuration**.
3. Cliquez sur l'icône de modification dans la section **Paramètres d'audit des modifications de configuration**.
4. Cochez la case **Effectuer un audit de configuration lors de la réception de l'événement NetScalerConfigChange**.

#### Remarque

Il s'agit d'un paramètre global pour toutes les instances. Citrix ADM effectue un audit de configuration pour chaque instance sur laquelle il recevra les interruptions SNMP NetScalerConfigChange à l'avenir.

1. Dans le champ **Délai d'exécution du modèle d'audit** (en minutes), saisissez les minutes. Citrix ADM exécute le modèle d'audit de configuration sur l'instance de Citrix ADC après ce délai lorsqu'il reçoit l'interruption SNMP ConfigChange par cette instance.



## Fonctions réseau

February 1, 2024

À l'aide de la fonctionnalité Network Functions, vous pouvez surveiller l'état des entités configurées sur vos instances Citrix Application Delivery Controller (ADC) gérées. Vous pouvez afficher des statistiques telles que les détails de transaction, les détails de connexion et le débit d'un serveur virtuel d'équilibrage de charge. Vous pouvez également activer ou désactiver les entités lorsque vous planifiez une maintenance.

Le tableau de bord Network Functions fournit les graphiques suivants :

- Les 5 meilleurs serveurs virtuels avec le plus grand nombre de connexions client
- Les 5 meilleurs serveurs virtuels avec le plus grand nombre de connexions
- Les 5 meilleurs serveurs virtuels avec un débit maximal (Mo/sec)
- Les 5 derniers serveurs virtuels présentant le débit le plus faible (Mo/sec)
- Les 5 meilleures instances avec la plupart des serveurs virtuels
- État des serveurs virtuels
- État de santé des serveurs virtuels d'équilibrage de charge
- Protocoles

## Générer des rapports pour les entités d'équilibrage de charge

February 1, 2024

Citrix Application Delivery Management (ADM) vous permet de consulter les rapports des entités d'instance Citrix Application Delivery Controller (ADC) à tous les niveaux. Il existe deux types de rapports que vous pouvez télécharger dans Citrix ADM > Network Functions : les rapports consolidés et les rapports individuels.

**Rapports consolidés** : vous pouvez télécharger et consulter un rapport consolidé ou résumé pour toutes les entités gérées sur des instances Citrix ADC.

Ce rapport vous permet d'avoir une vue de haut niveau du mappage entre les instances Citrix ADC, les partitions et les entités d'équilibrage de charge correspondantes (serveurs virtuels, groupes de services et services) présentes sur le réseau.

L'image suivante montre un exemple de rapport récapitulatif.

Citrix ADC IP Address	Citrix ADC HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
	beta		Load Balancing				
			Load Balancing				
			Load Balancing				
			Load Balancing				
			Load Balancing	lb11-lb#11.1.2.2:80			lb11-svcgrp#3.4.4.4-3.4.4.4:80
			Load Balancing	ADM-Test-LB3#10.1.1.3:80			
			Load Balancing	334-lb#1.33.2.2:80			
			Load Balancing				
			Load Balancing				
			Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-7bfbc74-07fb-45b6-b	33f97d16-0413-4e6e-9f3d-844		
			Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-cea2ec6b-4b0c-496b-8	33f97d16-0413-4e6e-9f3d-844		
			Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-fa454aa1-6cb3-4eb0-9	33f97d16-0413-4e6e-9f3d-844		
			Load Balancing	kjbj-lb#1.2.3.4:80			kjbj-svcgrp
			Load Balancing				

Le rapport consolidé est au format CSV. Les entrées de chaque colonne sont décrites comme suit :

- **Adresse IP NetScaler : l'adresse IP** de l'instance Citrix ADC est affichée dans le rapport
- Nom d'**hôte NetScaler : le nom** d'hôte est affiché dans le rapport.
- **Partition** : l'adresse IP de la partition administrative est affichée
- **Serveur virtuel** : <name\_of\_the\_virtual\_server>#virtual\_IP\_address :port\_number
- **Services** : <name\_of\_the\_service>#service-IP\_address:port\_number
- **Groupes de services** : <name\_of\_service\_group>#membre\_serveur1\_adresse\_IP:port, adresse\_IP\_de\_serveur2\_adresse\_IP:port, membre\_serveur3\_adresse\_IP:port,..., Adresse IP du membre du serveur : port

#### Remarque

- Si aucun nom d'hôte n'est disponible, l'adresse IP correspondante s'affiche.
- Les colonnes vides indiquent que les entités respectives ne sont pas configurées pour cette instance Citrix ADC.

**Rapports individuels** : vous pouvez également télécharger et consulter des rapports indépendants de toutes les instances et entités. Par exemple, vous pouvez télécharger un rapport concernant uniquement les serveurs virtuels d'équilibrage de charge, les services d'équilibrage de charge ou les groupes de services d'équilibrage de charge.

Citrix ADM vous permet de télécharger le rapport instantanément. Vous pouvez également planifier la génération du rapport à une heure fixe une fois par jour, une fois par semaine ou une fois par mois.

### Générer un rapport d'équilibrage de charge combiné

1. Dans Citrix ADM, accédez à **Réseaux > Fonctions réseau > Équilibrage de charge**.

2. Sur la page **d'équilibrage** de charge, cliquez sur  .

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.

## Export

Subject\*

Format\*

Recurrence\*

Description

**NOTE:** Enter the schedule time in your selected timezone

Days of Week

Sun	Mon	Tue	Wed	Thu	Fri	Sat
-----	-----	-----	-----	-----	-----	-----

Export Time\*

Email

Email Distribution List\*  
 Add Edit Test

Slack

Schedule

**Remarque**

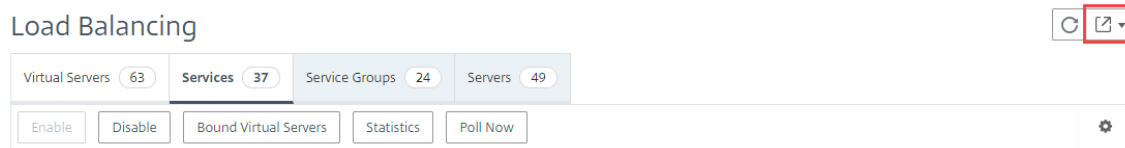
Si vous sélectionnez Récurrence **mensuelle**, assurez-vous de saisir tous les jours où vous souhaitez que le rapport soit planifié, séparés par des virgules.

## Générer un rapport d'entité d'équilibrage de charge individuel

Vous pouvez générer et exporter un rapport individuel pour un type particulier d'entité associé aux instances. Par exemple, considérez un scénario dans lequel vous souhaitez afficher une liste de tous les services d'équilibrage de charge du réseau.

1. Dans Citrix ADM, accédez à **Réseaux > Fonctions réseau > Équilibrage de charge > Services**.

2. Sur la page **Services**, cliquez sur le bouton **Exporter** en haut à droite.



- Sélectionnez **l'onglet Exporter maintenant** si vous souhaitez générer et afficher le rapport en ce moment.
- Sélectionnez **Planifier l'exportation** pour planifier la génération et l'exportation du rapport à intervalles réguliers.

#### Remarque

Vous pouvez uniquement télécharger les rapports ou les exporter sous forme de pièces jointes à un courrier électronique. Vous ne pouvez pas afficher les rapports sur l'interface graphique Citrix ADM.

## Exporter ou planifier l'exportation des rapports sur les fonctions réseau

February 1, 2024

Vous pouvez générer un rapport complet pour certaines fonctions réseau telles que l'équilibrage de charge, la commutation de contenu, la redirection de cache, l'équilibrage de charge globale du serveur (GSLB), l'authentification et Citrix Gateway dans Citrix Application Delivery Management (ADM). Ce rapport vous permet d'avoir une vue d'ensemble du mappage entre les instances Citrix ADC, 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

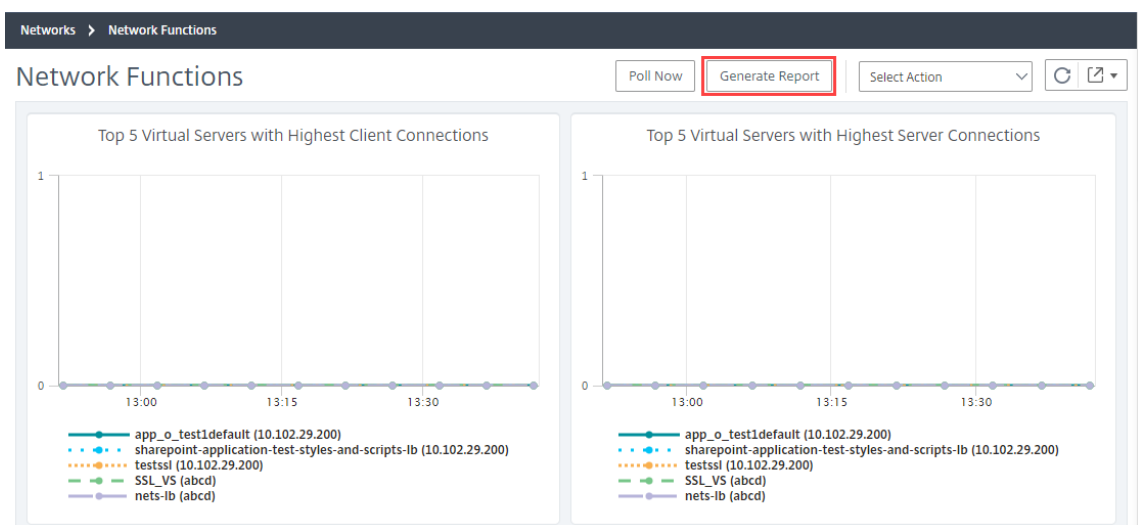
Vous pouvez planifier l'exportation de ces rapports vers des adresses e-mail spécifiées à des intervalles différents.

**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 gérée sur Citrix ADM.
- Lorsqu'un nouveau rapport est généré, les anciens rapports sont automatiquement supprimés de votre compte.
- Vous ne pouvez pas générer de rapport sur les fonctions réseau pour HAProxy.

**Pour exporter et planifier des rapports sur les fonctions réseau :**

1. Accédez à **Réseaux > Fonctions réseau**.
2. Dans la page **Fonctions réseau**, dans le volet droit, cliquez sur **Générer un rapport** dans le coin supérieur droit de la page.



3. Sur la page **Générer un rapport**, vous disposez des 2 options suivantes :

- a) Sélectionnez l'**onglet Exporter maintenant** et cliquez sur **OK**. Le rapport est téléchargé sur votre système.

## ← Generate Report

**Export Now**     **Schedule Export**

You can generate the report and download now for the following selected Network Functions

- Load Balancing
- Content Switching
- Cache Redirection
- Authentication
- Citrix Gateway
- GSLB

**OK**    **Close**

L'image suivante montre un exemple de rapport de fonctions réseau.

NetScaler ADC IP Address	NetScaler ADC HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
10.102.61.115-10.102.61.118	10.102.61.115-10.102.61.118		Load Balancing	lb_test_1#10.10.10.10:80		adm_metric_collector_svc_10.106.171.41#10.106.171.41:80	
10.102.61.115-10.102.61.118	10.102.61.115-10.102.61.118		Load Balancing	lbvs_511#51.1.1.1:80		test_1#10.102.61.105:80	
10.102.61.115-10.102.61.118	10.102.61.115-10.102.61.118		Load Balancing	lbvs_521#52.1.1.1:80		test_1#10.102.61.105:80	
10.102.61.115-10.102.61.118	10.102.61.115-10.102.61.118		Load Balancing	SG_HS_DNS_MON#1.2.22.2:80			sc1
10.102.61.115-10.102.61.118	10.102.61.115-10.102.61.118		Load Balancing	SG_HS_DNS_MON#1.3.4.5:80			
10.102.61.115-10.102.61.118	10.102.61.115-10.102.61.118		Load Balancing	atest94#1.1.1.11:80			
10.102.61.115-10.102.61.118	10.102.61.115-10.102.61.118		Load Balancing	lbvs1_101#1.10.1.1:80			
10.102.61.115-10.102.61.118	10.102.61.115-10.102.61.118		Load Balancing	lbvs1_1010#1.10.1.10:80			
10.102.61.115-10.102.61.118	10.102.61.115-10.102.61.118		Load Balancing	lbvs1_10100#1.10.1.100:80			
10.102.61.115-10.102.61.118	10.102.61.115-10.102.61.118		Load Balancing	lbvs1_10101#1.10.1.101:80			
10.102.61.115-10.102.61.118	10.102.61.115-10.102.61.118		Load Balancing	lbvs1_10102#1.10.1.102:80			
10.102.61.115-10.102.61.118	10.102.61.115-10.102.61.118		Load Balancing	lbvs1_10103#1.10.1.103:80			

- b) Sélectionnez l'**onglet Planifier le rapport** pour planifier la génération et l'exportation du rapport à intervalles réguliers. Spécifiez les paramètres de récurrence de génération de rapport et créez un profil de messagerie vers lequel le rapport est exporté.
  - i. **Récurrence** : sélectionnez **Quotidien**, **Hebdomadaire** ou **Mensuel** dans la zone de liste déroulante.
  - ii. **Heure de récurrence**- Entrez l'heure en tant que Heure : Minute au format 24 heures.
  - iii. **Profil de messagerie** : sélectionnez un profil dans la liste déroulante ou cliquez sur **+** pour créer un profil de messagerie.

Cliquez sur **Activer la planification pour planifier** votre rapport, puis cliquez sur **OK**. En cochant la case **Activer la planification**, vous pouvez générer les rapports sélectionnés.

## ← Generate Report

Export Now
 Schedule Export

You can schedule the export of the reports to specified email addresses at various intervals for the following selected Network Functions

- Load Balancing
- Content Switching
- Cache Redirection
- Authentication
- Citrix Gateway
- GSLB

**Schedule Details**

Recurrence\*

**NOTE:** Enter the schedule time in your selected timezone

Export time\*

Email

Email Profile\*  
 Add Edit Test

Slack

Enable Schedule

## Rapports sur le réseau

February 1, 2024

Vous pouvez optimiser l'utilisation des ressources en surveillant les rapports de votre réseau sur Citrix Application Delivery Management (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 (ADC) pour équilibrer la charge, changer de contenu ou compresser le trafic. Les performances réseau peuvent avoir un impact sur les performances de l'application. Pour continuer à maintenir les performances de vos applications, vous devez surveiller régulièrement les performances de votre réseau et vous assurer que toutes les ressources sont utilisées de manière optimale.

Citrix ADM vous permet désormais de générer des rapports non seulement pour des instances au niveau global, mais aussi pour des entités telles que les serveurs virtuels et les interfaces réseau. La



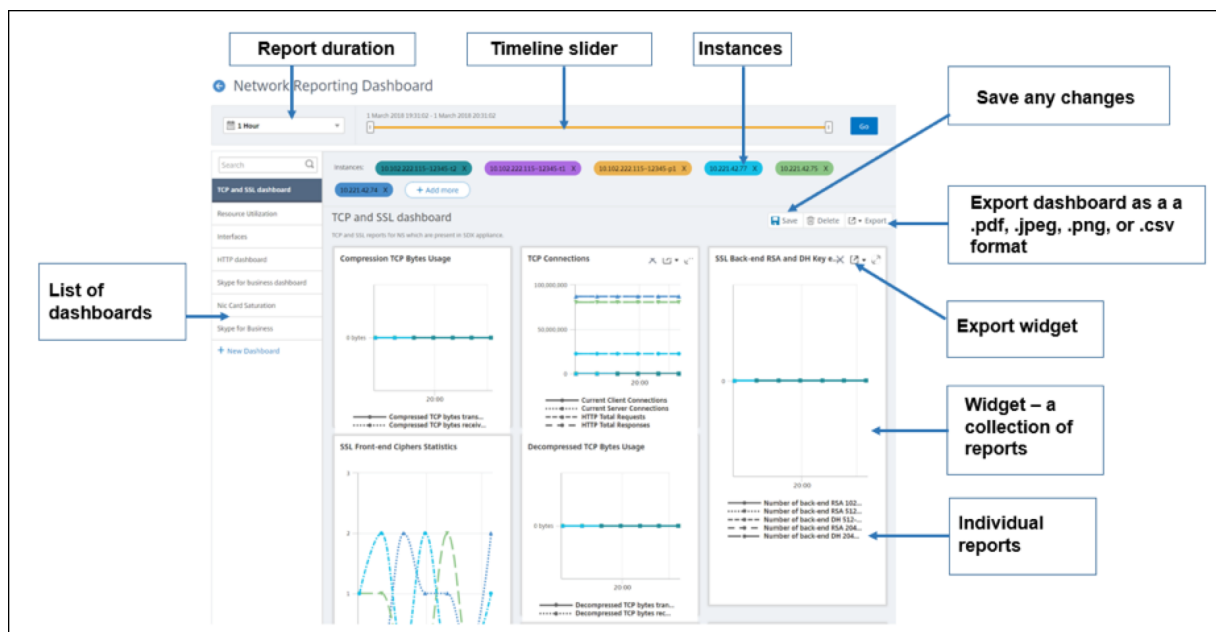
famille d’instances comprend les instances Citrix ADC et SD-WAN. Les serveurs virtuels pour lesquels vous pouvez générer des rapports sont les suivants :

- Serveurs d’équilibrage de charge
- Serveurs de commutation de contenu
- Redirection du cache
- Équilibrage global de la charge de service (GSLB)
- Authentification
- Citrix Gateway

Le tableau de bord des rapports réseau de Citrix ADM est hautement personnalisable. Vous pouvez désormais créer plusieurs tableaux de bord pour différentes instances, serveurs virtuels et autres entités.

### Tableau de bord de rapports réseau

L’image suivante appelle les différentes fonctionnalités du tableau de bord :



- Le panneau de gauche répertorie tous les tableaux de bord personnalisés créés dans Citrix ADM. Vous pouvez cliquer sur l’un d’eux pour afficher les différents rapports dont 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 une variété de rapports. Un widget représente un rapport sur le tableau de bord, c’est-à-dire une

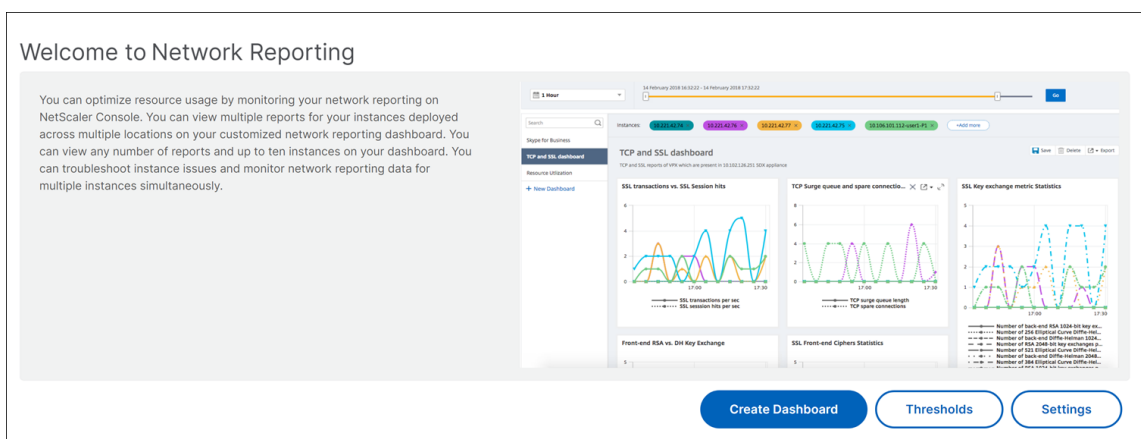
collection de rapports plus associés. Par exemple, un rapport d'utilisation des octets TCP compressés contient des rapports sur les octets TCP compressés transférés et reçus par seconde.

- Vous pouvez afficher les rapports pendant une heure, un jour, une semaine ou un mois. En outre, vous pouvez désormais utiliser l'option du curseur de chronologie pour personnaliser la durée des rapports générés sur Citrix ADM.
- Vous pouvez supprimer un rapport en cliquant sur « X ». Vous pouvez également exporter le rapport au format .pdf, .jpeg, .png ou .csv vers votre système. Vous pouvez également planifier l'heure et la récurrence de la génération du rapport. Vous pouvez également configurer une liste de distribution par e-mail 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, actuellement Citrix ADM vous permet d'afficher des rapports pour dix instances.
- Vous pouvez également exporter l'intégralité du tableau de bord au format .pdf, .jpeg, .png ou .csv vers votre système. Toutes les modifications apportées au tableau de bord doivent être enregistrées. Cliquez sur Enregistrer pour enregistrer vos modifications.

La section suivante explique en détail les tâches de création d'un tableau de bord, de génération de rapports et d'exportation de rapports.

## Pour afficher ou créer un tableau de bord

1. Dans Citrix ADM, accédez à **Réseaux > Network Reporting**.



## ← Create Dashboard

Basic Settings Select Reports Select Entities

Name\*  
 ?

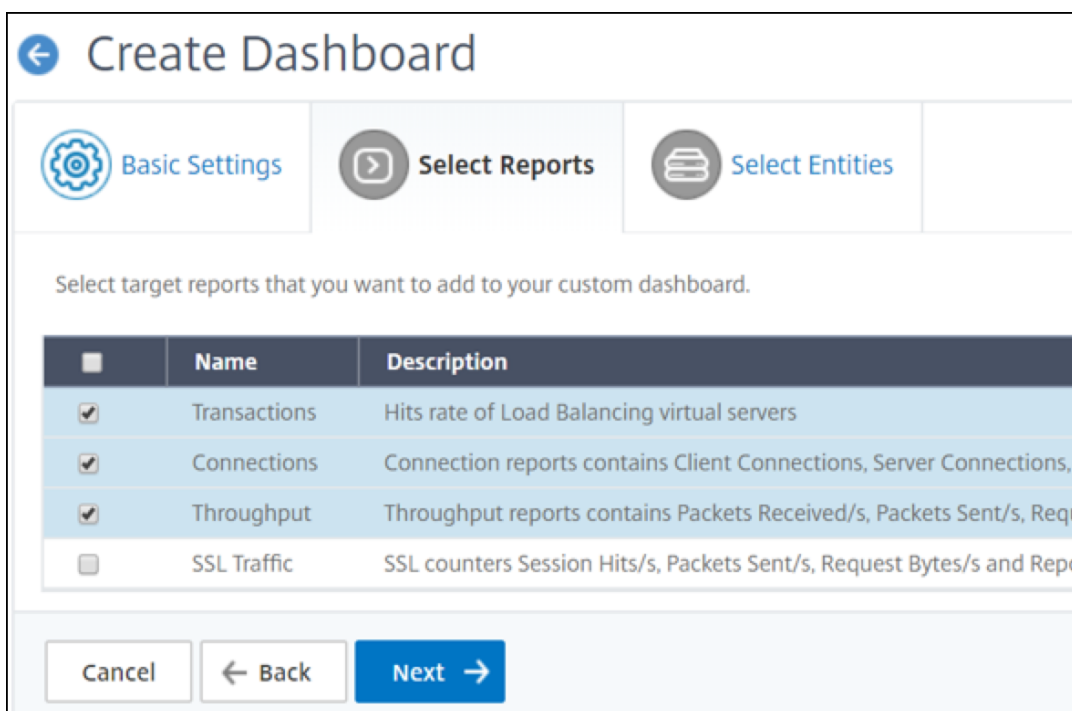
Instance Family  
 Citrix ADC  Citrix SD-WAN

Type\*  
 ?

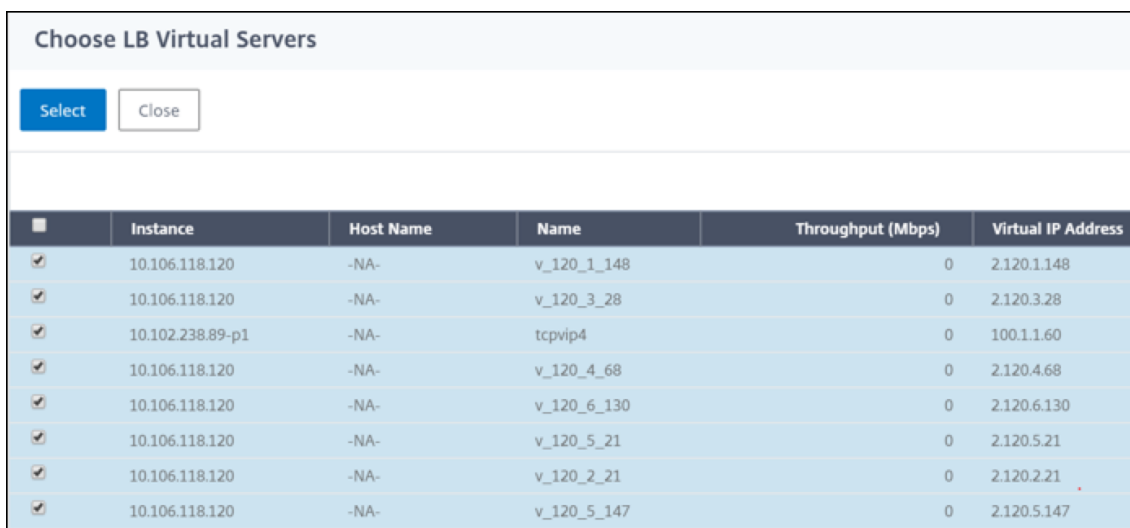
Description\*  
 ?

2. 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**.
3. 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.
4. Pour créer un tableau de bord, cliquez sur **Créer un tableau de bord**
5. La page **Créer un tableau** de bord s'ouvre.
6. Dans l'onglet **Paramètres de base**, entrez les informations suivantes :
  - a) **Nom**. Entrez le nom du tableau de bord.
  - b) **Famille d'instances**. Sélectionnez le type d'instance : Citrix ADC ou Citrix SD-WAN
  - 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.
- e) Cliquez sur **Suivant**.



- 7. Dans l'onglet **Sélectionner les entités**, cliquez sur **Ajouter**.
- 8. Dans la fenêtre **Choose LB Virtual Servers** qui s'ouvre, sélectionnez le nombre de serveurs virtuels que vous souhaitez surveiller.



**Remarque**

Selon le type d'entité que vous avez sélectionné dans l'onglet Paramètres de base, l'onglet Entités est renseigné avec les entités correspondantes. Par exemple, si vous sélectionnez

global, vous pouvez ajouter des instances.

9. Cliquez sur **Créer**.

Le tableau de bord **TCP et SSL** est créé et affiche tous les rapports que vous avez sélectionnés.

#### Remarque

Actuellement, les modifications que vous apportez aux légendes ou aux filtres ne peuvent pas être enregistrées.

### Exportation de rapports réseau

Bien que vous puissiez exporter des rapports de widgets aux formats .pdf, .png, .jpeg ou .csv, vous pouvez exporter l'intégralité des tableaux de bord uniquement aux formats .pdf, .jpeg ou .png.

#### Remarque

Vous ne pouvez pas exporter de rapports dans Citrix ADM si vous disposez d'autorisations en lecture seule. Vous avez besoin d'une autorisation de modification pour pouvoir créer un fichier dans Citrix ADM et pour pouvoir exporter le fichier.

#### Pour exporter des rapports de tableau de bord :

1. Accédez à **Réseaux > Rapports réseau**
2. Cliquez sur **Afficher les tableaux de bord** pour afficher tous les tableaux de bord que vous avez créés.
3. Dans le volet gauche, cliquez sur un tableau de bord. Dans cet exemple, cliquez sur **Tableau de bord 1**.
4. Cliquez sur le bouton d'exportation en haut à droite de la page.
5. Sous l'onglet **Exporter maintenant**, sélectionnez le format requis, puis cliquez sur **Exporter**.

Lors de la planification des rapports réseau, vous pouvez personnaliser l'en-tête du rapport en saisissant une chaîne de texte dans le champ Objet. Le rapport créé à l'heure planifiée aura 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

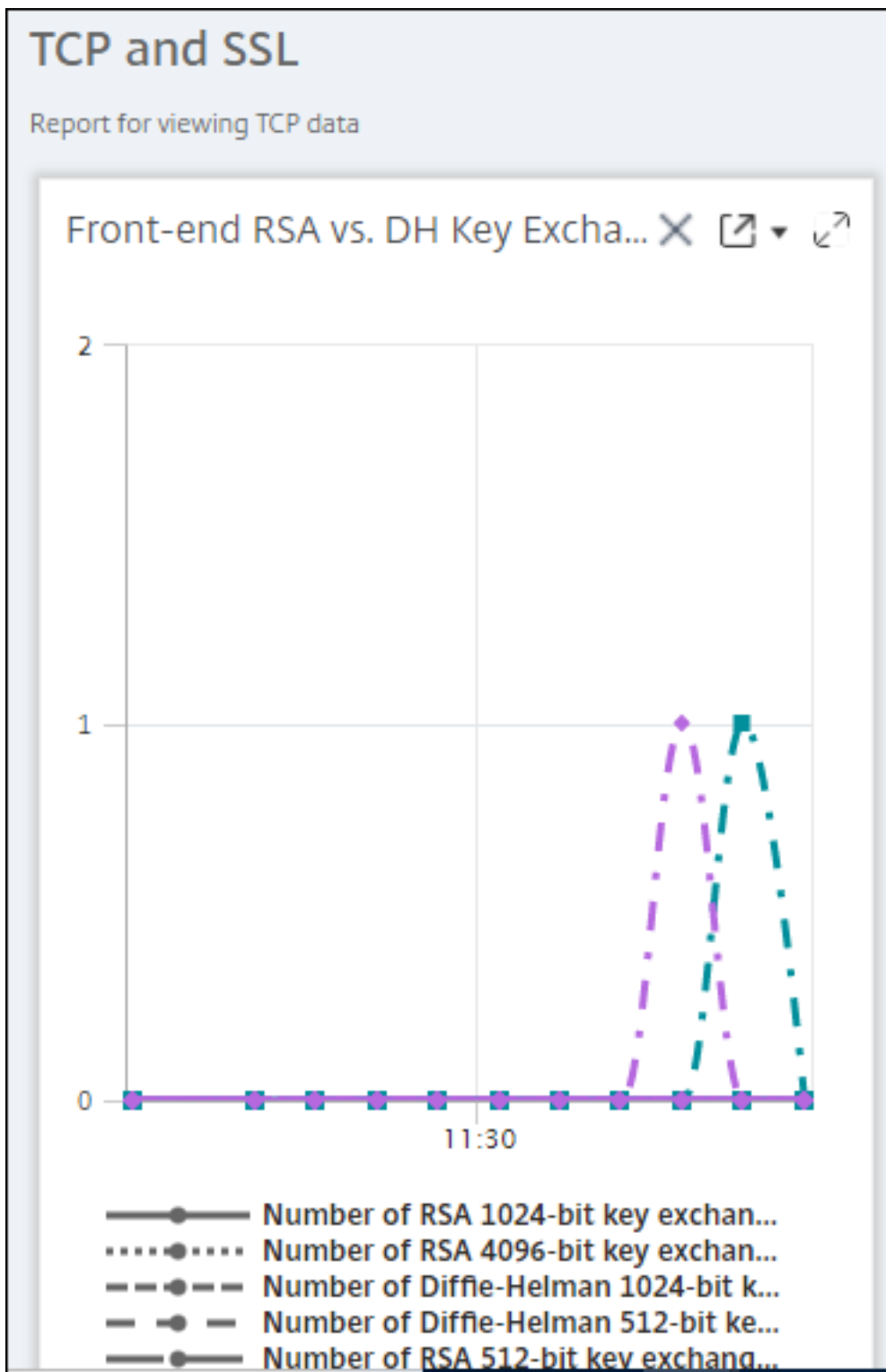
Actuellement, cette option n'est disponible que lorsque vous planifiez l'exportation de rapports. Vous ne pouvez pas ajouter un en-tête au rapport lorsque vous les exportez instantanément.

#### Pour exporter des rapports de tableau de bord :

1. Accédez à **Réseaux > Rapports réseau**
2. Cliquez sur **Afficher les tableaux de bord** pour afficher tous les tableaux de bord que vous avez créés.
3. Dans le volet gauche, cliquez sur un tableau de bord. Dans cet exemple, cliquez sur **Tableau de bord 1**.
4. Cliquez sur le bouton d'exportation en haut à droite de la page.
5. Sous l'onglet **Exporter maintenant**, sélectionnez le format requis, puis cliquez sur **Exporter**. \*\*

**Pour exporter des rapports de widget :**

1. Accédez à **Réseaux > Rapports réseau**.
2. Cliquez sur **Afficher les tableaux de bord** pour afficher tous les tableaux de bord que vous avez créés.
3. Dans le volet gauche, cliquez sur un tableau de bord. Dans cet exemple, cliquez également sur **TCP et SSL**.
4. Sélectionnez un widget. Par exemple, sélectionnez **Front-end RSA vs. Échange** de clés DH.
5. Cliquez sur le bouton Exporter dans le coin supérieur droit de la page
6. Sous l'onglet **Exporter maintenant**, sélectionnez le format requis, puis cliquez sur **Exporter**.



## Comment faire pour gérer les seuils pour les rapports réseau sur Citrix ADM

Pour surveiller l'état d'une instance Citrix ADC, vous pouvez définir des seuils sur les compteurs et recevoir des notifications lorsqu'un seuil est dépassé. Sur Citrix ADM, vous pouvez configurer des seuils et les afficher, les modifier et les supprimer.

Par exemple, vous pouvez recevoir une notification par e-mail lorsque le compteur de connexions d'un serveur virtuel de commutation de contenu atteint une valeur spécifiée. Vous pouvez définir un seuil pour un type d'instance spécifique. Vous pouvez également choisir les rapports que vous souhaitez générer pour des mesures de compteur spécifiques à partir de l'instance choisie.

Lorsque la valeur d'un compteur dépasse ou tombe en dessous (comme spécifié par la règle) de la valeur seuil, un événement de la gravité spécifiée est généré pour signaler un problème lié aux performances. Lorsque la valeur du compteur revient à une valeur que vous considérez normale, l'événement est effacé. Pour afficher ces événements, accédez à **Réseaux > Événements > Rapports**. Sur la page Rapports, vous pouvez cliquer sur le donut **Événements par gravité** pour afficher les événements par gravité.

Vous pouvez également associer une action à un seuil tel que l'envoi d'un e-mail ou d'un message SMS en cas de violation du seuil.

### Pour créer un seuil

1. Dans Citrix ADM, accédez à **Réseaux > Rapports réseau > Seuils**. Sous **Seuils**, cliquez sur **Ajouter**.

1. Sur la page **Créer un seuil**, indiquez les informations suivantes :

- **Nom du seuil**. Nom du seuil.
- **Type d'instance**. Choisissez Citrix ADC ou Citrix SD-WAN WO.
- **Nom du rapport**. Nom du rapport de performance qui fournit des informations sur ce seuil.

2. 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 souhaitez peut-être générer un événement présentant une gravité critique



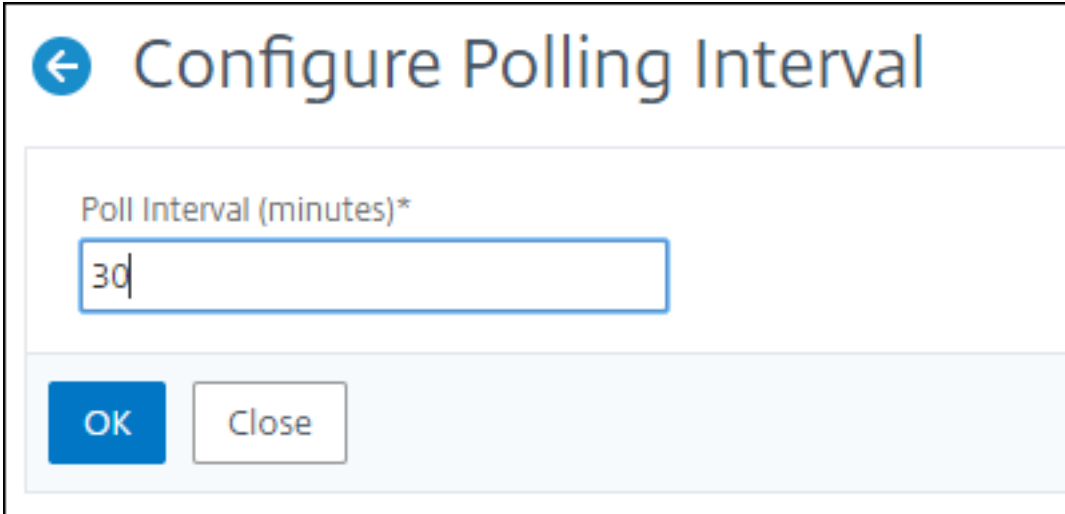
si la valeur surveillée pour les connexions client actuelles atteint 80 %. Dans ce cas, tapez 80 comme valeur de seuil. Vous pouvez afficher les événements de « gravité critique » en accédant à **Réseaux > Événements > Rapports**. Sur la page Rapports, vous pouvez cliquer sur le donut **Événements par gravité** pour afficher les événements par gravité.

- **Valeur claire.** Entrez la valeur qui indique à quel moment effacer la valeur. Par exemple, vous pouvez supprimer le seuil des connexions client actuelles lorsque la valeur surveillée atteint 50 %. Dans ce cas, saisissez 50 comme valeur claire.
  - **Gravité de l'événement** Sélectionnez le niveau de sécurité que vous souhaitez définir pour la valeur de seuil.
3. Choisissez l'adresse IP de la ou des instances pour lesquelles vous souhaitez définir le seuil.
  4. Vous pouvez également ajouter un **message d'événement**. Tapez un message que vous souhaitez afficher lorsque le seuil est atteint. Citrix ADM ajoute la valeur surveillée et la valeur de seuil à ce message.
  5. Sélectionnez **Activer** pour activer le seuil pour générer des alarmes.
  6. Vous pouvez éventuellement configurer des **actions** telles que des notifications par e-mail et/ou par SMS.
  7. 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. Cela récupère les statistiques d'instance telles que les informations de compteur et les agrèges sur la base de la minute, de l'heure, du jour ou de la semaine. Vous pouvez afficher ces données agrégées dans des rapports prédéfinis.

Pour définir l'intervalle d'interrogation des performances, accédez à **Réseaux > Rapport réseau**, puis cliquez sur **Configurer l'intervalle d'interrogation**. Votre intervalle de scrutin ne peut pas être inférieur à 5 minutes ou supérieur à 60 minutes.



← Configure Polling Interval

Poll Interval (minutes)\*

30

OK Close

### Configuration des paramètres de nettoyage des rapports réseau

Vous pouvez configurer l'intervalle de purge des données de rapport réseau dans Citrix ADM. Cela limite la quantité de données de reporting réseau stockées dans la base de données du serveur Citrix ADM. Par défaut, le nettoyage se produit toutes les 24 heures (à 01.00 heures) pour le réseau qui rapporte des données historiques.

#### Remarque

La valeur que vous pouvez spécifier ne peut pas dépasser 90 jours ni être inférieure à 1 jour.

### Pour configurer les paramètres de nettoyage des rapports réseau :

1. Accédez à **Système > Administration du système** . Sous **Paramètres d'élagage** , cliquez sur Paramètres **d'élagage de Network Reporting** .

## System Administration

<p><b>Set Up Citrix ADM</b></p> <ul style="list-style-type: none"><li>Setup Wizard Settings</li><li>Network Configuration</li><li>Install SSL Certificate</li><li>View SSL Certificate</li></ul> <p><b>System Settings</b></p> <ul style="list-style-type: none"><li>Configure Customer Identity</li><li>Change System Time Zone</li><li>Change Hostname</li><li>Change System Settings</li><li>Change Display Time Zone</li><li>Configure SSL Settings</li><li>Configure User Experience Improvement Settings</li><li>Configure Allowed URLs List</li><li>Configure message of the day</li></ul> <p><b>Prune Settings</b></p> <ul style="list-style-type: none"><li>System Prune Settings</li><li>Instance Events Prune Settings</li><li>Instance Syslog Prune Settings</li><li><b>Network Reporting Prune Settings</b></li></ul>	<p><b>System Administration</b></p> <ul style="list-style-type: none"><li>Upgrade Citrix ADM</li><li>Reboot Citrix ADM</li><li>Shut Down Citrix ADM</li></ul> <p><b>Backup Settings</b></p> <ul style="list-style-type: none"><li>System Backup Settings</li><li>Instance Backup Settings</li></ul>
--	---

2. Sur la page **Configurer les paramètres de Network Reporting Prune**, spécifiez le nombre de jours pendant lesquels vous souhaitez conserver les données, puis cliquez sur **OK**.

### ← Configure Network Reporting prune settings

Data to keep (days)\*

 ?

Pruning happens everyday at 01:00 for Network Reporting historical data

OK

Close

Toutes les données de performance des rapports réseau sont conservées dans la base de données Citrix ADM pendant le nombre de jours sélectionnés.

## Analytics

February 1, 2024

La fonctionnalité Citrix ADM Analytics fournit un moyen simple et évolutif d'examiner diverses informations Citrix ADC afin d'analyser et d'améliorer les performances des applications. Vous pouvez utiliser une ou plusieurs fonctionnalités d'analyse simultanément sur Citrix ADM.

Le tableau suivant décrit diverses fonctionnalités d'analyse prises en charge sur Citrix ADM :

Fonctionnalité d'analyse	Description
Web Insight	Web Insight offre une visibilité sur les applications Web d'entreprise et vous permet de surveiller toutes les applications Web dans Citrix ADC. En tant qu'administrateur, vous pouvez voir la surveillance intégrée et en temps réel des applications.
HDX Insight	HDX Insight offre une visibilité de bout en bout pour le trafic ICA passant par Citrix ADC. HDX Insight vous permet d'afficher en temps réel les mesures de latence du client et du réseau, les rapports historiques, les données de performance de bout en bout et de résoudre les problèmes de performances.
Gateway Insight	Gateway Insight offre une visibilité sur les défaillances rencontrées par tous les utilisateurs, quel que soit le mode d'accès, au moment de la connexion à Citrix Gateway.
Security Insight	Security Insight fournit une solution sur un seul écran pour vous aider à évaluer l'état de sécurité de votre application et à prendre des mesures correctives pour sécuriser vos applications.
SSL Insight	SSL Insight offre une visibilité sur les transactions Web sécurisées (HTTPS) et vous permet de surveiller toutes les applications Web sécurisées dans Citrix ADC. En tant qu'administrateur, vous pouvez voir la surveillance intégrée, en temps réel et historique des transactions Web sécurisées.

Fonctionnalité d'analyse	Description
TCP Insight	TCP Insight fournit une solution simple et évolutive pour surveiller les mesures des techniques d'optimisation et des stratégies (ou algorithmes) de contrôle de la congestion utilisées dans les instances de Citrix ADC afin d'éviter la congestion du réseau lors de la transmission de données.
Video Insight	La fonctionnalité Video Insight fournit une solution simple et évolutive pour surveiller les mesures des techniques d'optimisation vidéo utilisées par les appliances Citrix ADC afin d'améliorer l'expérience client et l'efficacité opérationnelle.
WAN Insight	L'analyse WAN Insight permet aux administrateurs de surveiller facilement le trafic WAN accéléré et non accéléré qui circule entre le centre de données et les appliances d'optimisation WAN des succursales. WAN Insight offre également une visibilité sur les clients, les applications et les succursales du réseau afin de résoudre efficacement les problèmes réseau.

## Exigences en matière de licence

February 1, 2024

Le tableau suivant décrit les exigences en matière de licences sur les instances Citrix ADC pour consulter les différents rapports d'analyse sur Citrix ADM :

Fonctionnalités Citrix ADM Analytics	Exigence de licence Citrix ADC
Web Insight	Le rapport Web Insight sur Citrix ADM est pris en charge sur toutes les éditions de licence Citrix ADC (Standard/Enterprise/Platinum).

Fonctionnalités Citrix ADM Analytics	Exigence de licence Citrix ADC
HDX Insight	Le rapport HDX Insight sur Citrix ADM est pris en charge sur l'une des licences Citrix ADC suivantes : Enterprise Edition (pour les rapports inférieurs à 1 heure) ou Platinum Edition (pour des rapports illimités). <b>Remarque</b> l'édition de licence standard n'est pas prise en charge.
Security Insight	Le rapport Security Insight sur Citrix ADM est pris en charge sur les éditions Platinum ou Enterprise avec une licence App Firewall. <b>Remarque</b> l'édition de licence standard et la licence de pare-feu d'application autonome ne sont pas prises en charge.
SSL Insight	Le rapport SSL Insight sur Citrix ADM est pris en charge sur toutes les éditions de licence Citrix ADC (Standard/Enterprise/Platinum).
Gateway Insight	Le rapport Gateway Insight sur Citrix ADM est pris en charge sur l'une des licences Citrix ADC suivantes : Enterprise Edition (pour les rapports inférieurs à 1 heure) ou Platinum Edition (pour des rapports illimités). <b>Remarque</b> l'édition de licence standard n'est pas prise en charge.
TCP Insight	Le rapport TCP Insight est pris en charge sur toutes les éditions de licence Citrix ADC (Standard/Enterprise/Platinum).
Video Insight	Le rapport Video Insight sur Citrix ADM est pris en charge sur l'édition Citrix ADC Premium (série VPX-T 1000, VPX-T).
WAN Insight	Le rapport WAN Insight sur Citrix ADM est pris en charge sur Citrix SD-WAN WO Edition (WAN Optimization Edition).

## Vue d'ensemble de Logstream

February 1, 2024

Les instances Citrix ADC génèrent des enregistrements AppFlow et constituent un point de contrôle central pour tout le trafic d'applications dans le centre de données. IPFIX et Logstream sont les protocoles qui transportent ces enregistrements AppFlow des instances de Citrix ADC vers Citrix ADM. Pour plus d'informations, voir [AppFlow](#).

- IPFIX est un standard ouvert Internet Engineering Task Force (IETF) défini dans la RFC 5101. IPFIX utilise le protocole UDP qui est un protocole de transport peu fiable utilisé pour le flux de données dans une direction. Comme IPFIX utilise le protocole UDP, le respect de la norme IPFIX permet de traiter davantage de ressources dans Citrix ADM.
- Logstream est un protocole appartenant à Citrix qui est utilisé comme l'un des modes de transport pour transférer efficacement les données du journal d'analyse des instances de Citrix ADC vers Citrix ADM. Logstream utilise un protocole TCP fiable et nécessite moins de ressources pour traiter les données.

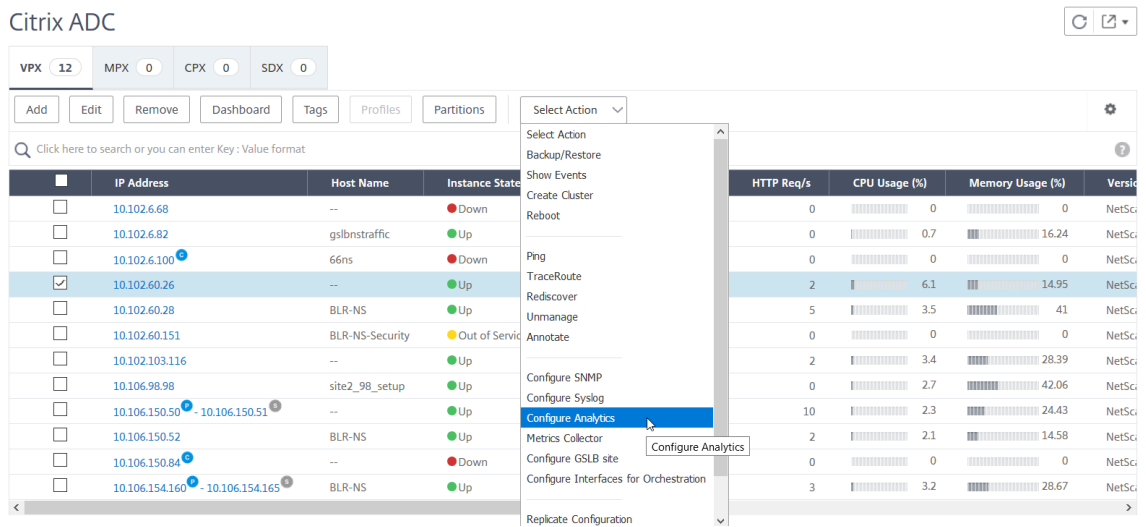
Pour Citrix ADC compris entre **11.1 Build 47.14 et 11.1 Build 62.8**, Logstream est le mode de transport par défaut pour activer Web Insight (HTTP) et IPFIX est le seul mode de transport permettant d'activer d'autres informations. Pour les versions de Citrix ADC allant de la version **12.0 à la dernière version**, vous pouvez sélectionner Logstream ou IPFIX comme mode de transport.

### Remarque

La version et la version de Citrix ADM doivent être égales ou supérieures à la version et à la version de Citrix ADC. Par exemple, si vous avez installé Citrix ADC 12.1 Build 50.28/50.31 ou une version antérieure, assurez-vous d'avoir installé Citrix ADM 12.1 Build 50.39.

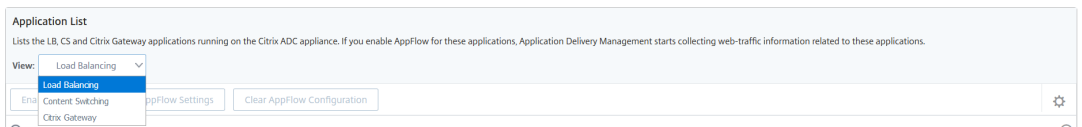
**Pour utiliser Logstream comme mode de communication tout en activant les analyses sur Citrix ADM, procédez comme suit :**

1. Accédez à **Réseaux > Instances > Citrix ADC**, puis sélectionnez l'instance Citrix ADC sur laquelle vous souhaitez activer l'analyse.
2. Dans la liste **Sélectionner une action**, sélectionnez **Configurer Analytics**.

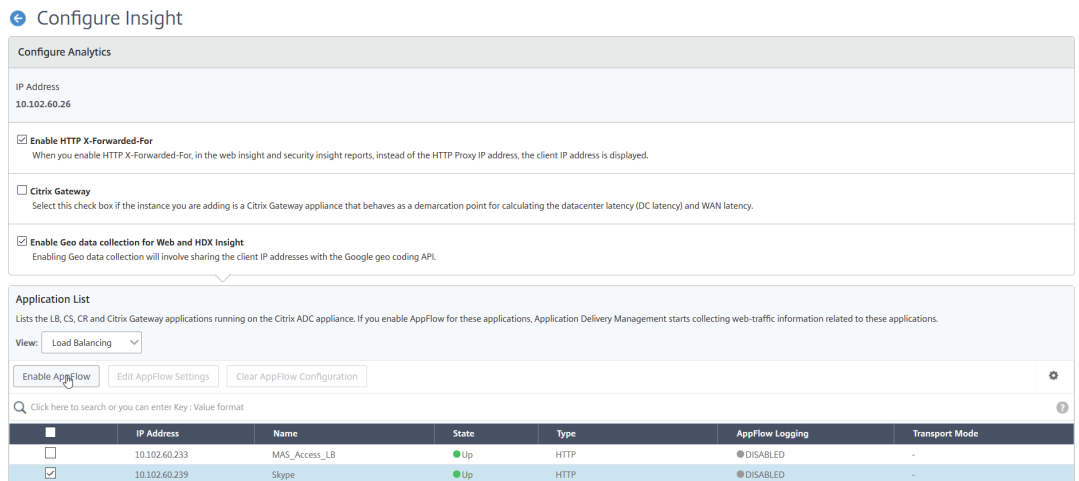


3. Sur la page **Configurer Insight** :

- a) Sélectionnez la **liste des applications** pour l'équilibrage de charge ou la commutation de contenu.



- b) Sélectionnez le serveur virtuel et cliquez sur **Activer AppFlow**.



4. Dans la boîte de dialogue Activer AppFlow :

- Entrez **true** dans la zone de texte
- Sélectionnez **Logstream** comme mode de transport



**Remarque**

Citrix vous recommande de sélectionner Logstream comme mode de transport.

- Sélectionnez le type d'aperçu et cliquez sur **OK**.

Le tableau suivant décrit les fonctionnalités de Citrix ADM qui prend en charge Logstream en tant que mode de transport :

Fonctionnalité	IPFIX	Logstream
Web Insight	•	•
Security Insight	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	Non pris en charge	•
CR Insight	•	•
Réputation IP	•	•
AppFirewall	•	•

Fonctionnalité	IPFIX	Logstream
Mesure côté client	•	•
Syslog/Auditlog	•	•

## Désactiver la collecte de données d'URL

February 1, 2024

Vous pouvez désactiver la collecte de données d'URL si vous ne souhaitez pas que les rapports d'URL s'affichent sur le nœud Web Insight du tableau de bord dans Citrix Application Delivery Management (ADM).

### Pour désactiver la collecte de données d'URL à partir de Citrix ADM

1. Dans Citrix ADM, accédez à **Analytics > Paramètres**, puis cliquez sur **Configurer les journaux des enregistrements de données Analytics**.
2. Dans la section **Paramètres de collecte de données URL Web Insight**, si l'option **Activer la collecte de données URL** est cochée, désactivez la case à cocher.
3. Cliquez sur **OK**.

#### ← Configure Analytics Data Record Logs

**Data Record Log Settings**

Data record logs provide detailed information about appflow records that Application Delivery Management collects from the Citrix ADCs.

- Enable HDX Insight Logs ?
- Enable Web Insight Logs
- Enable CB WAN Insight Logs
- Enable Security Insight Logs
- Enable Video Insight Logs
- Enable TCP Insight Logs

**Web Insight Report Settings**

Select the Web Insight entities for which you want to view reports on the dashboard.

- Show HTTP Request Method Report
- Show HTTP Response Status Report
- Show User Agent Report
- Show Operating System Report
- Show Domain Report

**Web Insight URL Data Collection Settings**

If you do not want the URL reports to be displayed on the Web Insight node of the dashboard, disable the URL data collection settings.

- Enable URL Data Collection ?

## Créer des seuils et des alertes

February 1, 2024

Vous pouvez définir des seuils et des alertes pour surveiller l'état d'une instance Citrix ADC. Vous pouvez définir des seuils sur les compteurs et surveiller les instances et les entités sur les instances gérées.

Lorsque la valeur d'un compteur dépasse le seuil, Citrix Application Delivery Management (ADM) génère un événement pour signifier un problème lié aux performances. Lorsque la valeur du compteur correspond à la valeur d'effacement spécifiée dans le seuil, l'événement est effacé, ce qui signifie que le seuil particulier est revenu à son état normal.

Vous pouvez également associer une action au seuil. Les actions incluent l'envoi d'une alerte, d'un e-mail ou d'une notification par SMS. Lorsque le seuil est atteint, Citrix ADM effectue l'action que vous définissez automatiquement, comme l'activation d'une alerte et l'envoi d'une notification par e-mail ou SMS.

### Pour créer un seuil et une alerte à l'aide de Citrix ADM

1. Dans Citrix ADM, accédez à **Analytics > Paramètres > Seuils**. Sous **Seuils**, cliquez sur **Ajouter**.
2. Sur la page **Créer des seuils**, spécifiez les informations suivantes :
  - **Nom** : nom pour configurer le seuil.
  - **Type de trafic** : type de trafic pour lequel vous souhaitez configurer le seuil.
  - **Entité** : catégorie ou type de ressource pour lequel vous souhaitez configurer le seuil.
  - **Clé de référence** : valeur générée automatiquement en fonction du type de trafic et de l'entité sélectionnés.
  - **Durée** : intervalle pour lequel vous souhaitez configurer le seuil.
  - **Configurer la règle** : règle de la mesure pour laquelle vous souhaitez configurer le seuil.
  - **Paramètres de notification** - Activez le seuil et recevez des notifications via différents canaux tels que e-mail, mou ou sms lorsque le seuil dépasse.
3. Cliquez sur **Créer**.

Pour l'aperçu HDX, vous pouvez également définir plusieurs seuils pour lesquels une alerte est générée uniquement si toutes les entités du seuil configuré sont violées.

## Configurer des seuils adaptatifs

February 1, 2024

La fonctionnalité de seuil adaptative définit la valeur de seuil pour le nombre maximal de visites sur chaque URL. Si le nombre maximal de visites sur une URL est supérieur à la valeur seuil définie pour l'URL, un message Syslog est envoyé à un serveur Syslog externe. L'intervalle entre les valeurs de seuil peut être exprimé en jours ou en semaines.

La valeur seuil est calculée comme suit :

**Valeur seuil = Nombre maximum de visites \* Multiplicateur de seuil**

Où :

- Le nombre maximal de visites est le nombre maximum de visites sur une URL.
- Le multiplicateur de seuil est une valeur entière que vous définissez (par défaut : 2).

### Pour créer un seuil adaptatif à l'aide de Citrix ADM

1. Dans Citrix ADM, accédez à **Analytics > Paramètres > Seuils adaptatifs**, puis cliquez sur **Ajouter**.
2. Dans la page **Seuils adaptatifs**, spécifiez les paramètres suivants :
  - **Nom** : nom du seuil
  - **Entité** - URL
  - **Durée** - Durée du seuil (jour ou semaine)
  - **Multiplicateur de seuil** : entier défini par l'utilisateur qui est multiplié par le nombre maximal de visites de l'URL spécifiée afin d'obtenir le seuil adaptatif pour l'URL.

## Configurer la persistance de la base de données

February 1, 2024

Configurer la persistance de la base de données dans Citrix Application Delivery Management (ADM) vous permet de personnaliser la durée de stockage des données historiques de vos données d'analyse Citrix ADC. Vous pouvez choisir les types de persistance de base de données suivants pour les données historiques de vos analyses :

- Des heures pour conserver les données minutieusement
- Jours pendant lesquels les données horaires doivent être conservées
- Jours pendant lesquels conserver les données quotidiennes

### Pour configurer la persistance de la base de données

1. Accédez à > **Analytics** > **Paramètres** > **Persistance de la base de données**.
2. Cliquez sur le type Insight dont vous souhaitez configurer la persistance de la base de données.

Data Persistence

You can customize the duration for which you want to store the historical data of your Citrix ADC analytics data.

Insight Name	Hours to persist minutely data	Days to persist hourly data	Days to persist daily data
Gateway Insight	4 Hours	1 Days	31 Days
HDX Insight	4 Hours	1 Days	31 Days
Secure Web Gateway	2 Hours	1 Days	31 Days
Security Insight	4 Hours	1 Days	31 Days
TCP Insight	2 Hours	1 Days	31 Days
Video Insight	2 Hours	1 Days	31 Days
Wan Opt	2 Hours	1 Days	31 Days
Web Insight	4 Hours	1 Days	31 Days

3. Spécifiez la durée pendant laquelle vous souhaitez conserver les données Insight sur Citrix ADM. Par exemple, pour Gateway Insight, vous pouvez stocker les données historiques de vos analyses pendant 2 heures, ou les données horaires pendant 1 jour.

### ← Gateway Insight

Configure the duration you want to persist the Gateway Insight data for on per summarization level

Hours to persist minutely data

Days to persist hourly data

Days to persist daily data

OK Close

## Diagnostiques en libre-service pour Analytics

February 1, 2024

Citrix Application Delivery Management (ADM) effectue des diagnostics en libre-service pour identifier les problèmes de licence et de configuration sur les instances gérées pour les fonctionnalités d'analyse suivantes :

- Web Insight
- HDX Insight
- Gateway Insight
- Security Insight
- Analyse de Secure Web Gateway

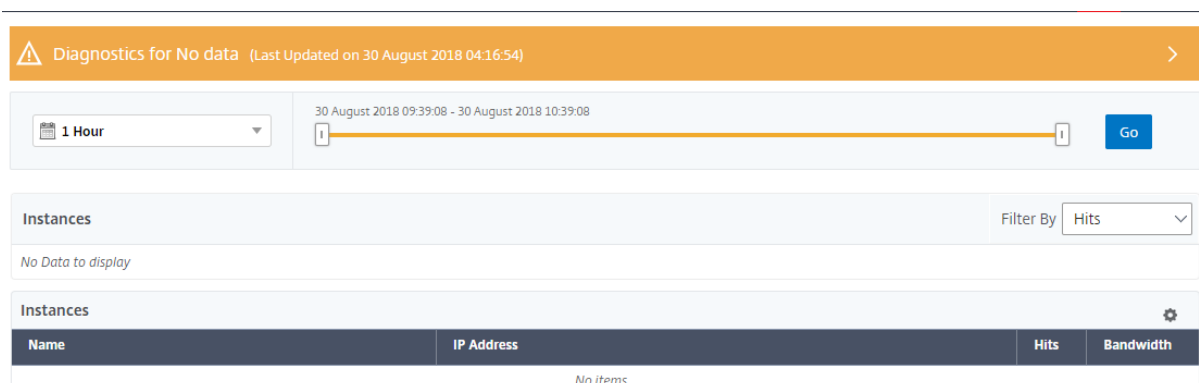
Les diagnostics en libre-service s'exécutent toutes les 12 heures et génèrent un rapport de diagnostic si des problèmes sont détectés pour chacune des fonctionnalités d'analyse spécifiées. Le rapport de diagnostic fournit les sources des problèmes, les types de problèmes et les actions correctives pour les résoudre. Les diagnostics en libre-service vous aident à identifier et à résoudre les problèmes plus rapidement.

Par exemple, si la stratégie AppFlow n'est pas liée à un serveur virtuel ou qu'un serveur virtuel n'est pas sous licence, Citrix ADM n'obtient pas les données souhaitées pour la surveillance Web Insight. Le diagnostic en libre-service identifie les problèmes et génère un rapport de diagnostic. Vous pouvez consulter le rapport de diagnostic pour vérifier les problèmes et effectuer les actions correctives.

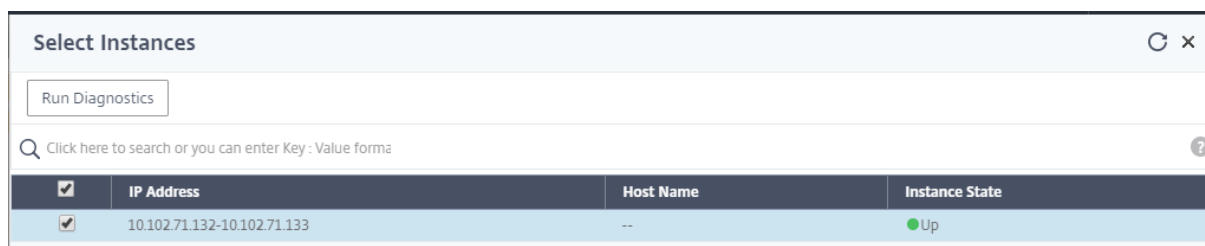
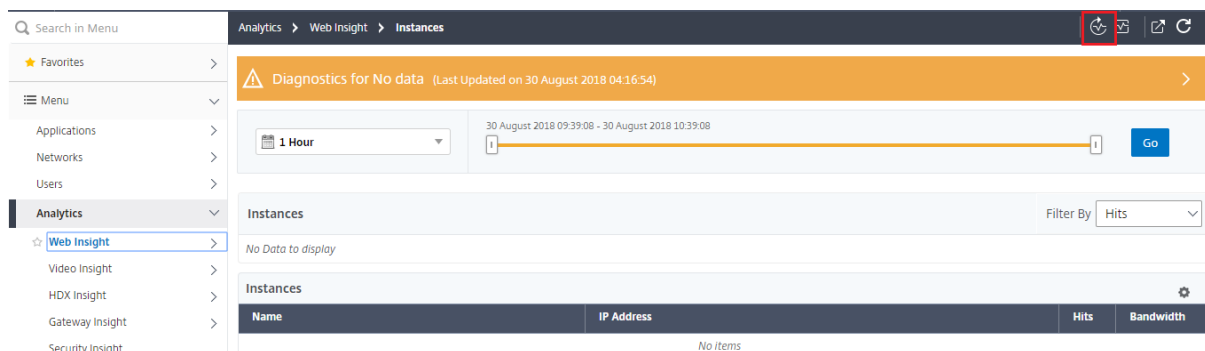
### Voir le rapport de diagnostic

Pour afficher les rapports de diagnostic pour les fonctionnalités d'analyse spécifiées, vous devez accéder au nœud d'analyse respectif dans le tableau de bord de Citrix ADM.

Par exemple, pour afficher le rapport de diagnostic pour Web Insight, accédez à **Analytics > Web Insight**. Sur la page Web Insight, sélectionnez l'icône **Afficher les diagnostics**.



Vous pouvez également exécuter un diagnostic instantané si vous souhaitez vérifier les problèmes. Cliquez sur **Exécuter les diagnostics**. Choisissez les instances et sélectionnez **Exécuter les diagnostics**.



## Analyser le rapport de diagnostic

Les diagnostics en libre-service affichent le rapport de diagnostic sur fond orange ou bleu en fonction de l'importance des problèmes.

Le rapport de diagnostic sur fond orange indique une criticité plus élevée que sur fond bleu.

Par exemple, cinq serveurs virtuels sont configurés sur votre instance Citrix ADC. Si vous n'avez activé les paramètres AppFlow sur aucun serveur virtuel, Citrix ADM ne reçoit pas le trafic Web Insight et Security Insight à des fins d'analyse. Les diagnostics en libre-service identifient les problèmes de configuration comme critiques. Les rapports de diagnostic s'affichent en arrière-plan orange dans les fonctionnalités Web Insight et Security Insight.

The screenshot shows a diagnostic report with an orange header. The title is "Diagnostics for No data" with a warning icon and a timestamp "(Last Updated on 13 August 2018 15:30:06)". Below the header, under the "Configuration" section, there are two numbered items:

1. Some of the AppFlow params are disabled on 1 instance.
2. ADM/agent (collector) is not bound to any action on 1 instance.

A "See More" link is visible in the bottom right corner.

Si vous avez activé AppFlow sur l'un des serveurs virtuels, Citrix ADM reçoit des données à des fins d'analyse. Vous voyez le rapport de diagnostic en arrière-plan bleu car au moins un serveur virtuel envoie du trafic pour analyse.

The screenshot shows a diagnostic report with a blue header. The title is "Diagnostics for Partial data" with an information icon and a timestamp "(Last Updated on 13 August 2018 15:30:06)". Below the header, under the "Configuration" section, there are five numbered items:

1. There is no AppFlow policy bound to 216 virtual servers.
2. ADM/agent (collector) is not bound to any action of the Virtual Server on 19 instances.
3. ADM/agent (collector) does not have the highest priority in policy binding on 5 instances.
4. Web Insight is not enabled on the AppFlow action of 1 instance.
5. ADM/agent (collector) is not bound to any action on 1 instance.

A "See More" link is visible in the bottom right corner.

**IMPORTANT** : Les diagnostics en libre-service ne vérifient pas le flux de trafic. Il vérifie uniquement les problèmes de licence ou de configuration associés aux fonctionnalités d'analyse spécifiées sur les instances gérées. Parfois, vous ne voyez aucune donnée d'analyse car aucun trafic actif ne passe par des serveurs virtuels.

Le rapport de diagnostic comporte une page de résumé et une page d'informations détaillées.

La page de résumé fournit une vue d'ensemble des types de problèmes (licence ou configuration). La page peut contenir des liens hypertexte qui vous dirigent vers les pages de configuration pertinentes.

Par exemple, s'il n'y a pas de serveurs virtuels d'équilibrage de charge sous licence sur votre Citrix ADM, la page de résumé fournit un lien hypertexte qui vous dirige vers la page **Licences système**.

The screenshot shows a diagnostic report with an orange header. The title is "Diagnostics for No data" with a warning icon and a timestamp "(Last Updated on 23 August 2018 16:08:03)". Below the header, there are two sections:

- License**
  1. There are no Load Balancing virtual servers licensed on this ADM. [Click here to go to configure License page.](#)
- Configuration**
  1. Collectors are not configured on 2 instances.

A "See More" link is visible in the bottom right corner.

Pour afficher les informations détaillées sur les problèmes, cliquez sur **Voir plus** sur la page récapitulative.

La page d'informations détaillées fournit des informations complètes sur les problèmes et recommande les actions que vous devez effectuer. Vous pouvez cliquer sur le lien hypertexte correspondant à chaque problème pour configurer l'instance gérée ou le serveur virtuel.



Diagnostics Details					
IP Address	Host Name	Virtual Server Name	Issue Type	Message	Action
10.102.71.150	NS150	-NA-	Configuration	This Citrix ADM or Agent is not bound to any action on the instance	Please add this Citrix ADM or Agent as collector in an action to receive data
10.102.71.150	NS150	test pooja	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.102.71.150	NS150	test pooja check with	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppSecTest5	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppSecTest77	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppTest132	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppTest194	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppSecTest95	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppSecTest30	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppSecTest29	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppSecTest35	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppTest131	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppSecTest71	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy

Vous pouvez également rechercher les problèmes en fonction de l'action, du nom d'hôte, de l'adresse IP et du type de problème, etc.

Diagnostics Details					
IP	Properties	Issue Type	Message	Action	
10.102.71.150	Host Name	Configuration	This Citrix ADM or Agent is not bound to any action on the instance	Please add this Citrix ADM or Agent as collector in an action to receive data	
10.102.71.150	IP Address	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy	
10.102.71.150	Issue Type	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy	
10.102.71.150	Message	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy	
10.106.150.55	Virtual Server Name	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy	
10.106.150.55	-NA-	AppSecTest77	Configuration	Please bind the virtual server with an AppFlow Policy	
10.106.150.55	-NA-	AppTest132	Configuration	Please bind the virtual server with an AppFlow Policy	
10.106.150.55	-NA-	AppTest194	Configuration	Please bind the virtual server with an AppFlow Policy	
10.106.150.55	-NA-	AppSecTest95	Configuration	Please bind the virtual server with an AppFlow Policy	
10.106.150.55	-NA-	AppSecTest30	Configuration	Please bind the virtual server with an AppFlow Policy	
10.106.150.55	-NA-	AppSecTest29	Configuration	Please bind the virtual server with an AppFlow Policy	
10.106.150.55	-NA-	AppSecTest35	Configuration	Please bind the virtual server with an AppFlow Policy	
10.106.150.55	-NA-	AppTest131	Configuration	Please bind the virtual server with an AppFlow Policy	

Après avoir résolu les problèmes, vous devez exécuter un diagnostic instantané pour générer le dernier rapport de diagnostic.

## Web Insight

February 1, 2024

Web Insight permet aux administrateurs de surveiller toutes les applications Web desservies par les instances de Citrix ADC. En tant qu'administrateur, vous pouvez obtenir une surveillance intégrée et en temps réel des applications à partir d'instances de Citrix ADC. Web Insight fournit des informations critiques telles que la latence du réseau client et le temps de réponse du serveur, garantissant

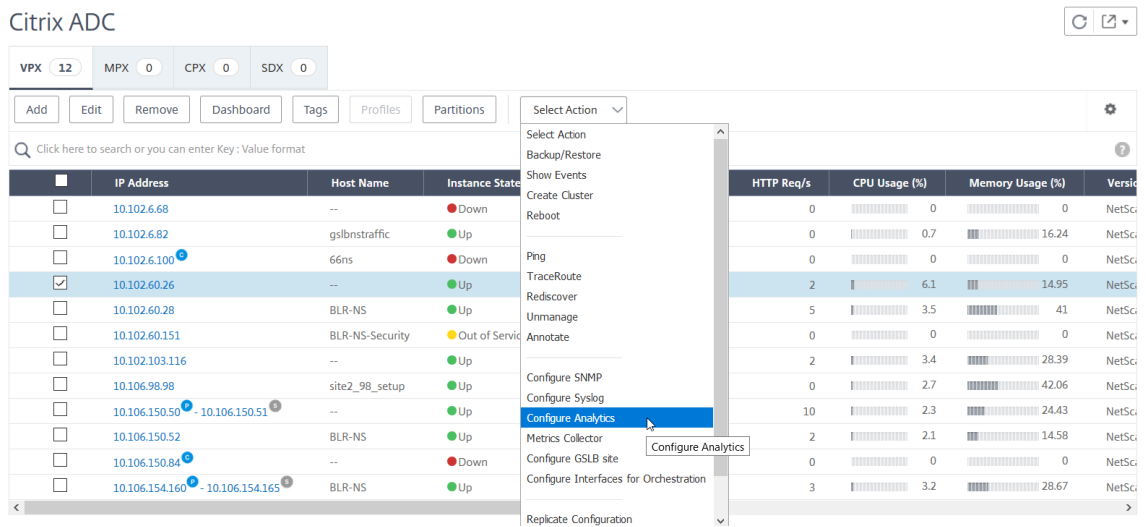
ainsi la surveillance et l'amélioration des performances des applications. Les données utilisées pour l'analyse sont capturées à partir de chaque transaction HTTP, HTTPS traitée par l'instance de Citrix ADC. Les données d'analyse vous permettent d'analyser les performances des instances Citrix ADC, de l'application, de l'URL, du client et du serveur dans votre environnement.

Voici quelques-uns des cas d'utilisation que vous pouvez afficher les données à l'aide de Web Insight :

- La liste des clients qui connaissent une latence élevée lors de l'accès à une application telle que SharePoint
- La meilleure application qui a eu le plus de succès en une heure
- La liste des applications et des URL accessibles depuis les clients
- Le système d'exploitation et le navigateur utilisés par un client particulier
- Applications ou serveurs qui envoient le plus de réponses liées aux erreurs
- Problèmes d'accessibilité avec un client particulier
- Problèmes d'accessibilité pour une partie ou l'ensemble des applications d'un client particulier
- Peu de pages d'une application sont lentes à partir d'un client particulier et du serveur principal
- L'application est lente lorsqu'elle est accédée à partir d'un client particulier et d'un serveur principal

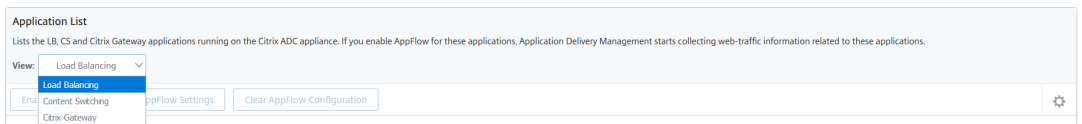
Vous pouvez activer Web Insight pour un serveur virtuel spécifique sur une instance sélectionnée afin de surveiller le trafic sur votre application Web. La fonctionnalité Web Insight fournit ensuite des statistiques pour le serveur virtuel dans Citrix ADM. Pour activer le Web Insight :

1. Ouvrez une session sur Citrix ADM avec les informations d'identification de l'administrateur.
2. Accédez à **Réseaux > Instances > Citrix ADC**, puis sélectionnez l'instance Citrix ADC sur laquelle vous souhaitez activer l'analyse.
3. Dans la liste **Sélectionner une action**, sélectionnez **Configurer Analytics**.

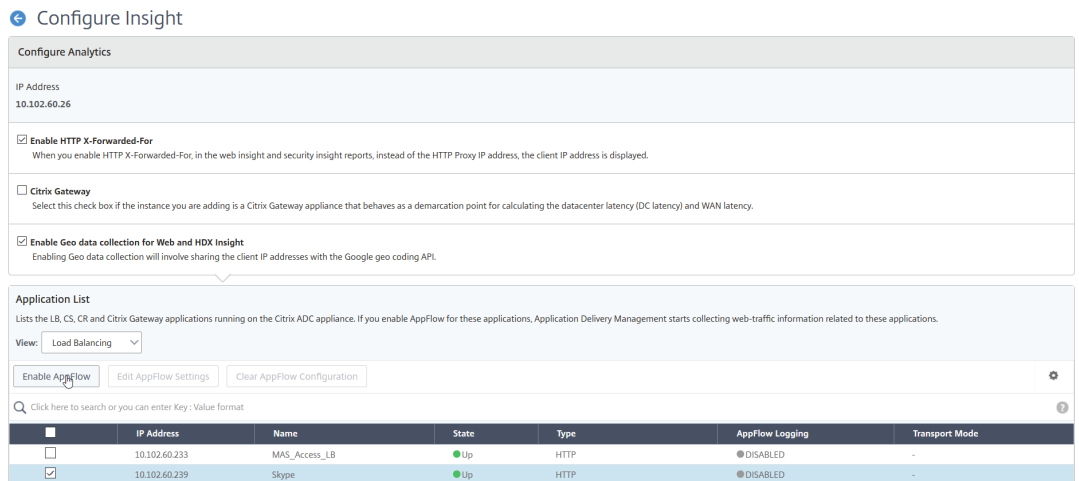


4. Sur la page **Configurer Insight** :

- a) Sélectionnez la **liste des applications** pour l'équilibrage de charge ou la commutation de contenu.



- b) Sélectionnez le serveur virtuel et cliquez sur **Activer AppFlow**.



5. Dans la boîte de dialogue Activer AppFlow :

- Entrez **true** dans la zone de texte
- Sélectionnez **Logstream** comme mode de transport

Remarque : Citrix vous recommande de sélectionner Logstream comme mode de transport.

- Sélectionnez **Web Insight** et cliquez sur **OK**.

**Enable AppFlow**

**Select Expression**

Load Balancing ▼

▼

true

**Transport Mode**    IPFIX    Logstream

Web Insight

Client Side Measurement

Security Insight

If there is a firewall between Citrix ADM and the Citrix ADC instance, please make sure the TCP port 5557 is open. This is to allow ADM to collect AppFlow traffic.

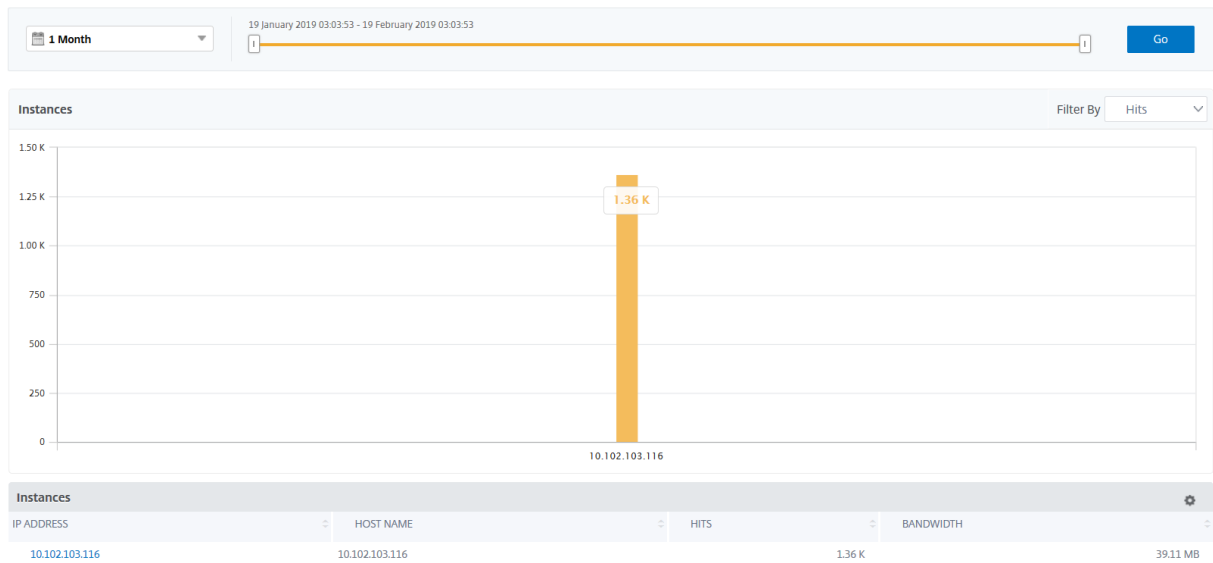
OK

Cancel

## Analyser les problèmes liés aux applications Web

L'un des problèmes courants qu'un administrateur doit identifier est les problèmes de latence. En tant qu'administrateur, vous devez déterminer si le problème de latence provient du réseau serveur, du réseau client ou du temps de réponse du serveur. À l'aide de Citrix ADM, vous pouvez identifier ces informations en accédant à **Analytics > Web Insight**.

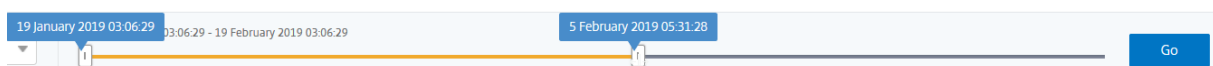
Lorsque vous accédez à **Analytics > Web Insight**, il affiche les instances Citrix ADC activées avec Web Insight. Vous pouvez afficher les informations détaillées pour les instances telles que l'adresse IP, le nom d'hôte, le nombre total d'accès et la bande passante.



À l'aide de la liste, vous pouvez sélectionner la durée pour afficher les informations relatives aux instances.

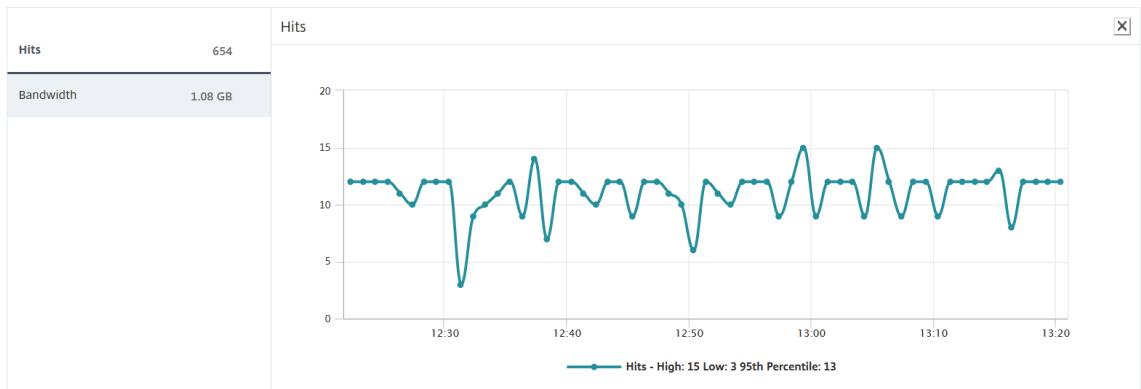


Vous pouvez également utiliser le curseur pour personnaliser la durée du temps et cliquer sur **Aller** pour afficher les résultats.

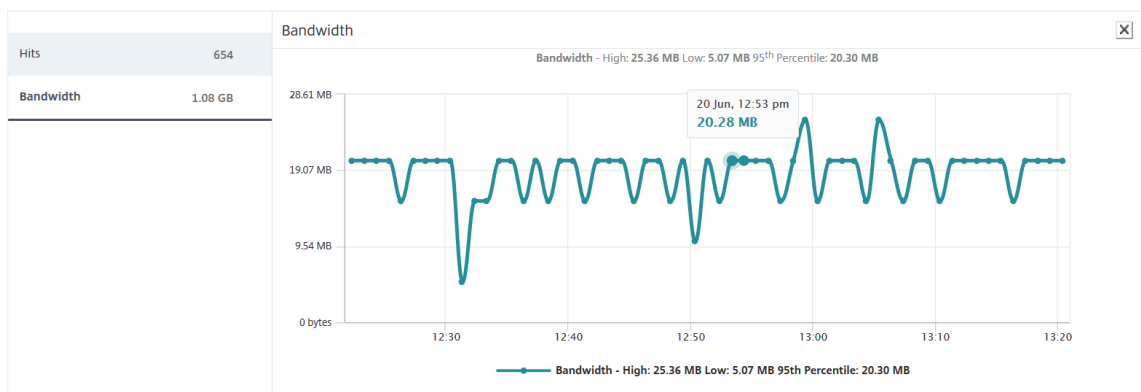


Lorsque vous cliquez sur le graphique ou l'adresse IP de l'instance, les informations détaillées sur l'instance s'affichent. Vous pouvez afficher des informations sur les éléments suivants :

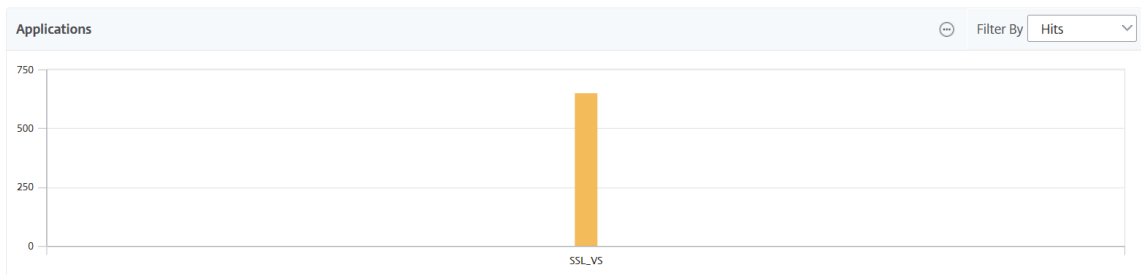
• **Nombre total de visites**



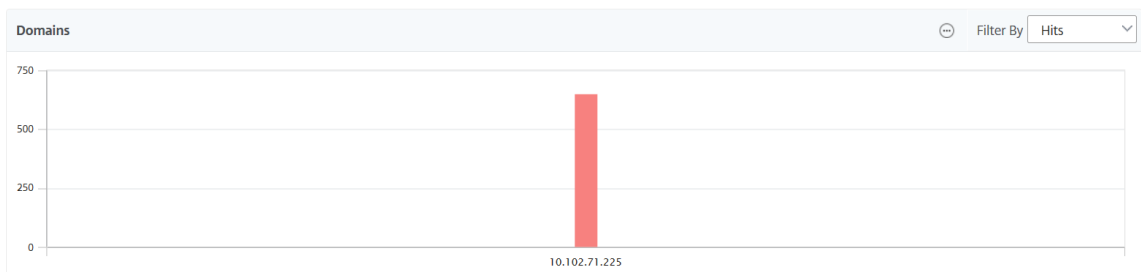
• **Bande passante**



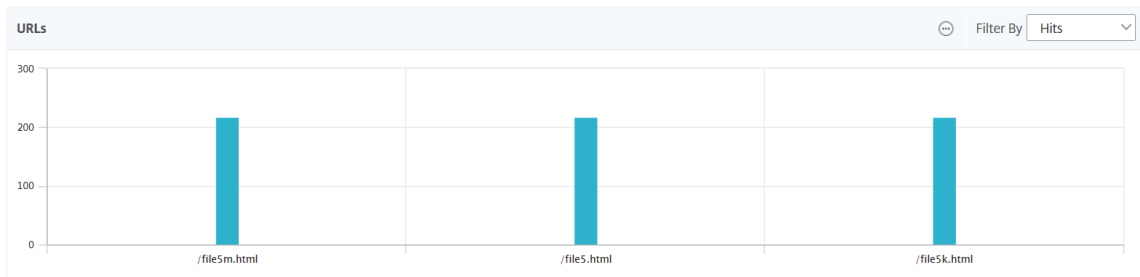
• **Applications**



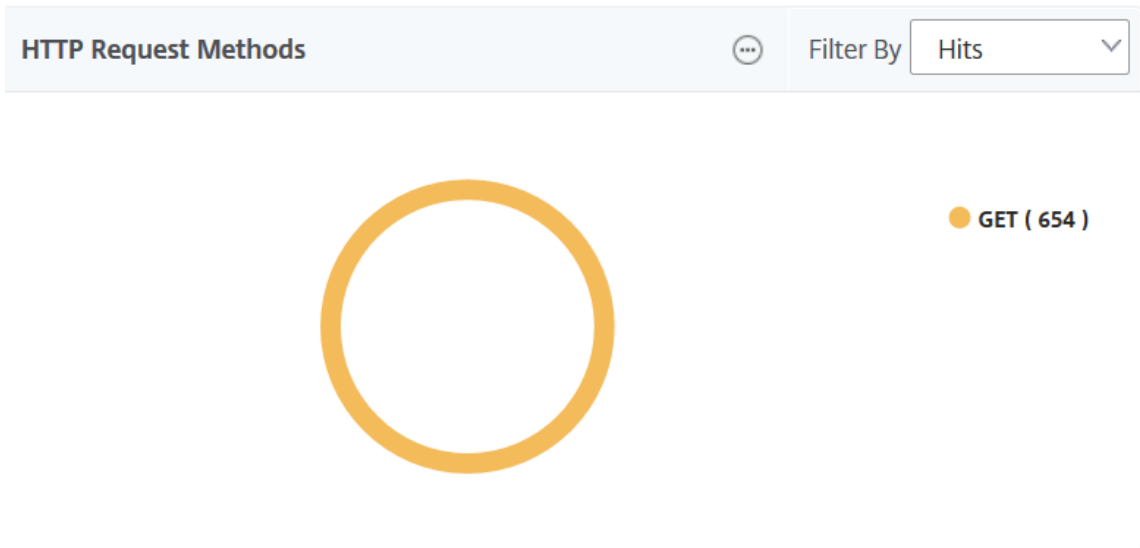
• **Domaines**



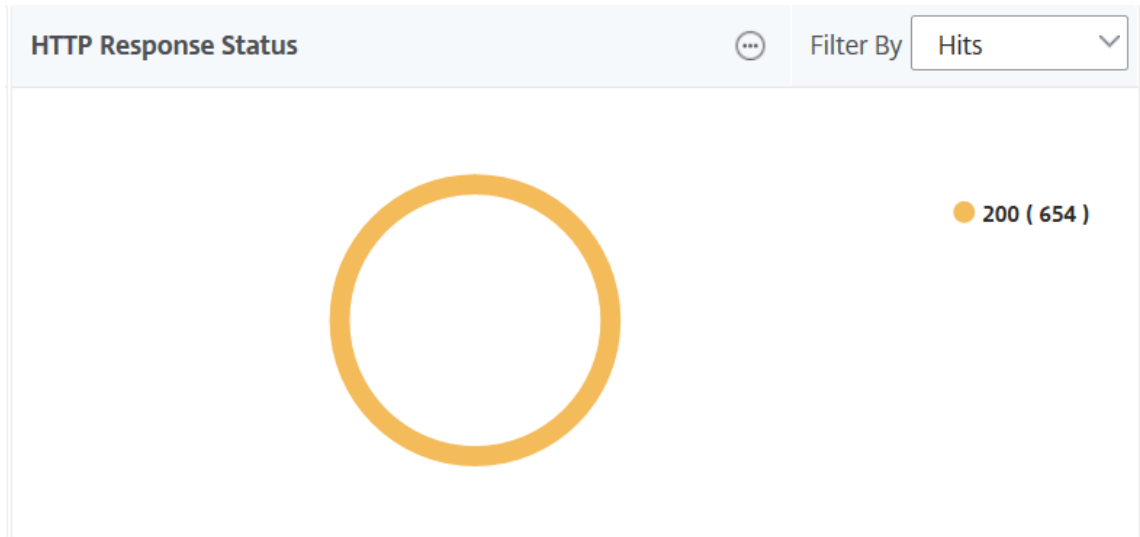
• **URL**



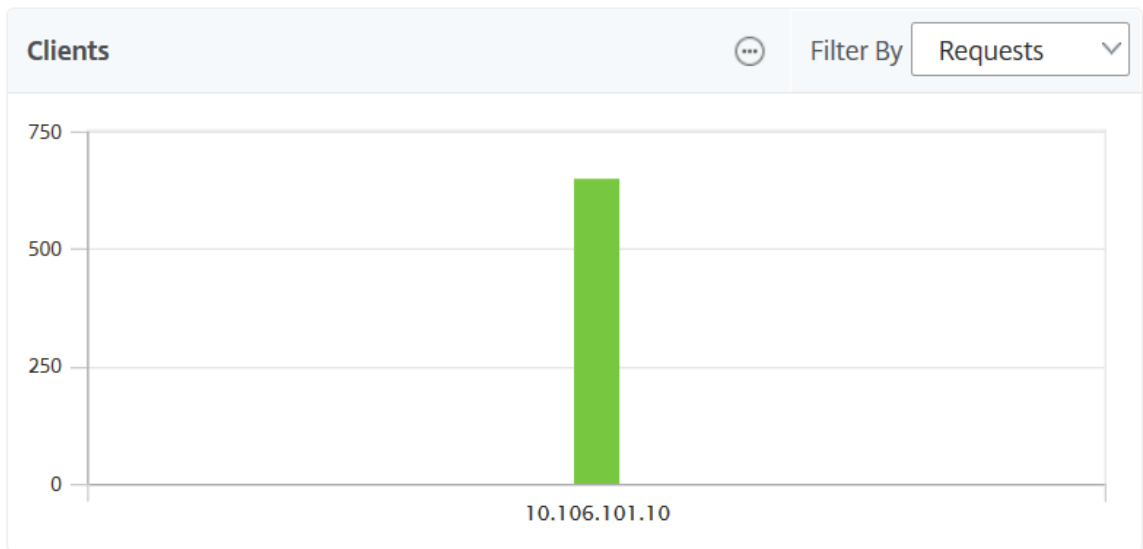
- **Méthodes de requête HTTP**



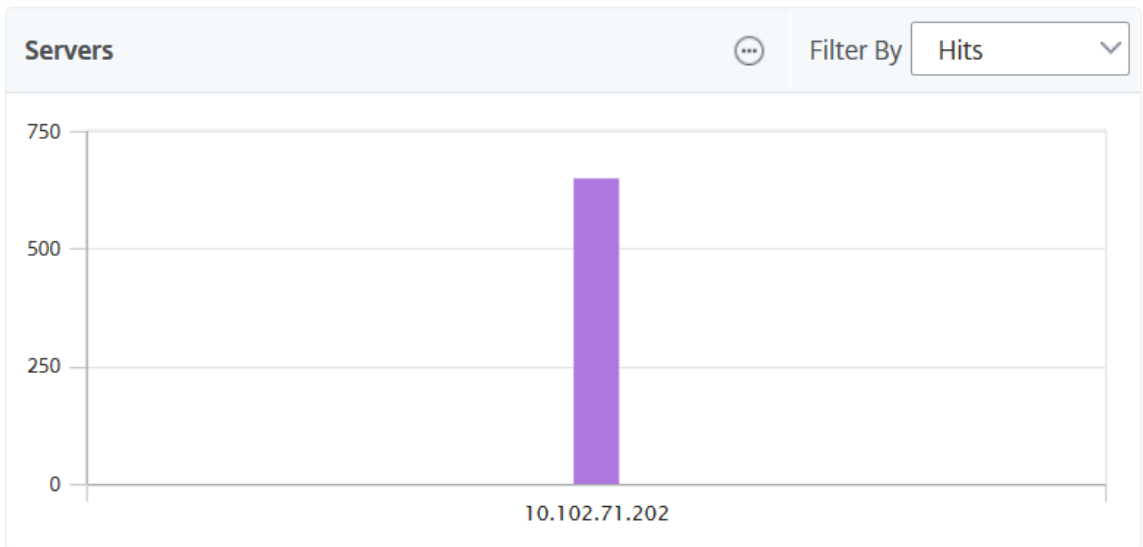
- **État de la réponse HTTP**



- **Clientèle**

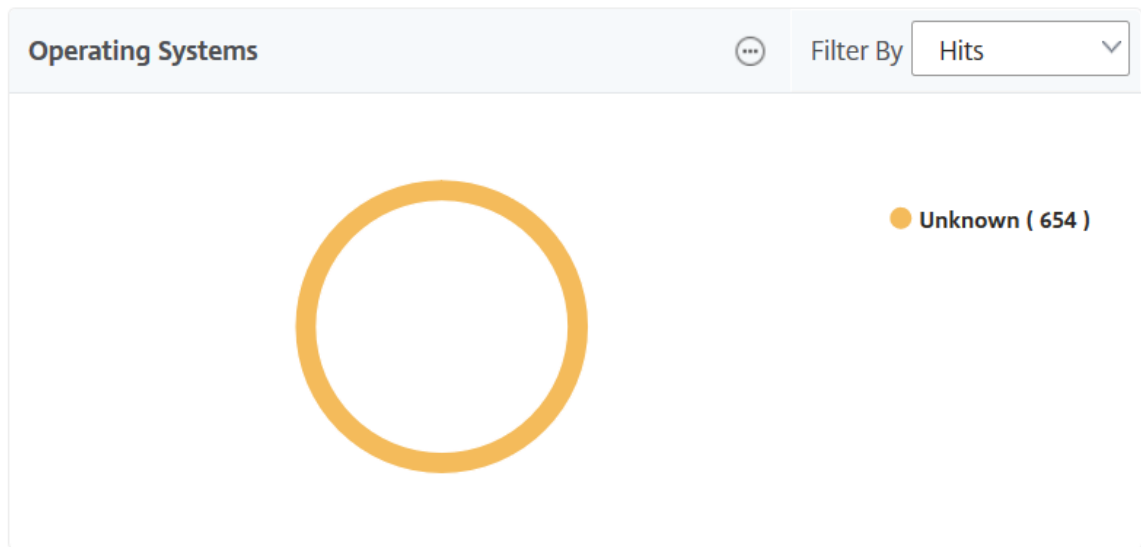


- **Serveurs**

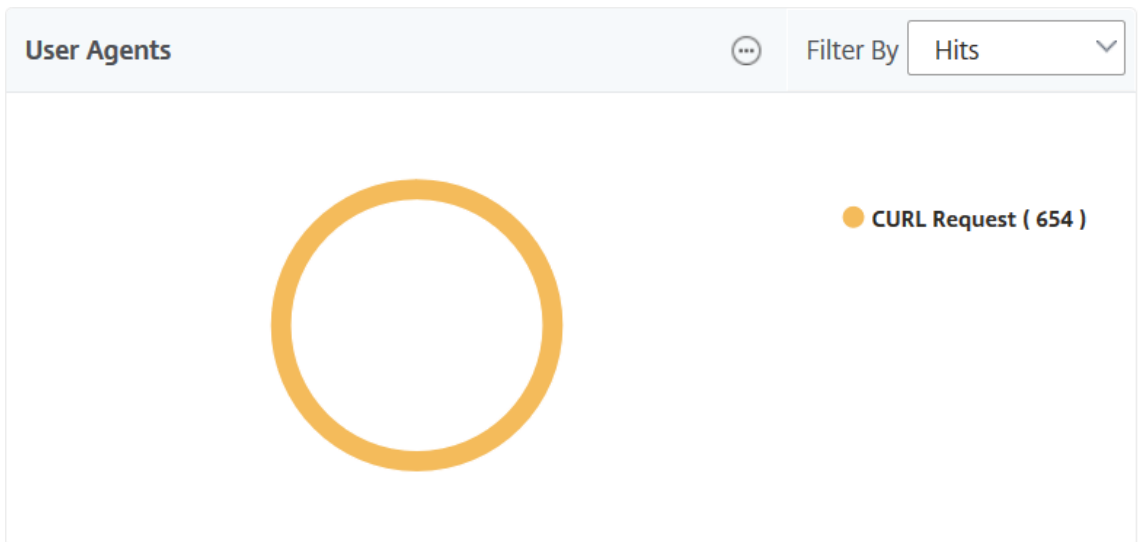


- **Systemes d'exploitation**



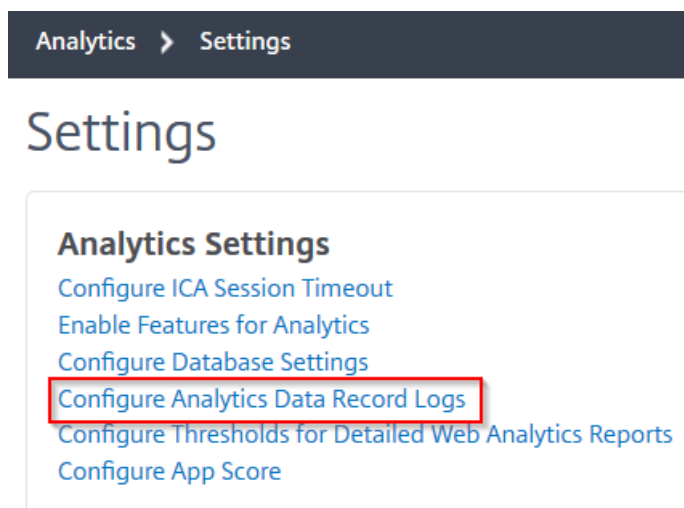


• **Agents utilisateur**

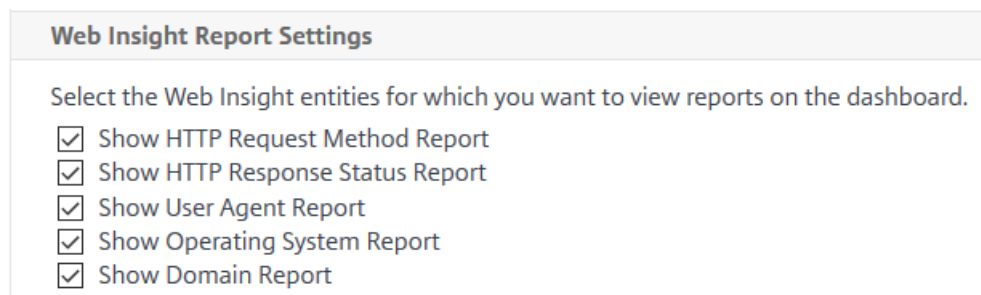


Vous pouvez également sélectionner **des entités Web Insight** pour lesquelles vous souhaitez afficher des rapports sur l'interface graphique.

1. Accédez à **Analytics > Web Insight > Paramètres** .
2. Cliquez sur **Configurer les journaux des enregistrements de données Analytics**.



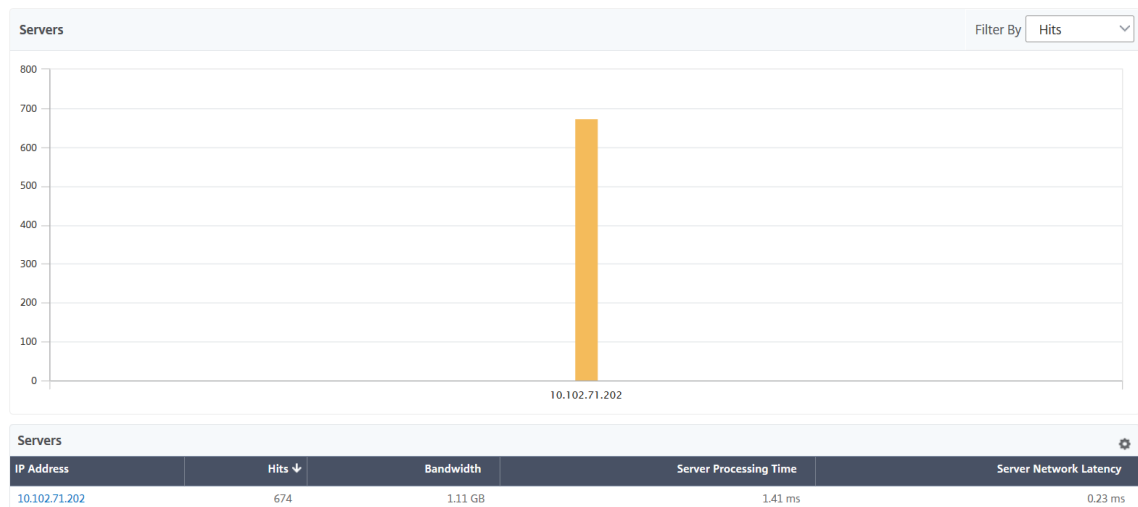
3. Sous **Paramètres de rapport Web Insight**, sélectionnez les entités que vous souhaitez afficher des rapports sur l'interface graphique.



4. Cliquez sur **OK**.

Pour effectuer une analyse plus approfondie, vous pouvez cliquer sur chaque catégorie d'aperçu sous Web Insight dans l'interface graphique. Par exemple, si vous souhaitez vérifier les problèmes pour les serveurs configurés :

1. Accédez à **Analytics > Web Insight > Serveurs**.
2. La page Serveurs s'affiche avec tous les serveurs configurés.
3. Cliquez sur l'adresse IP du graphique. Vous pouvez également cliquer sur l'adresse IP dans le tableau.



La vue d’aperçu détaillée du serveur sélectionné s’affiche. Dans cette vue, vous pouvez rechercher plusieurs informations telles que :

- Nombre total de visites reçues par le serveur
- Bande passante
- Délai de traitement du serveur
- Latence réseau du serveur
- Serveurs virtuels configurés pour le serveur
- Nombre total de clients accédant au serveur
- Nombre total de codes de réponse fournis par le serveur

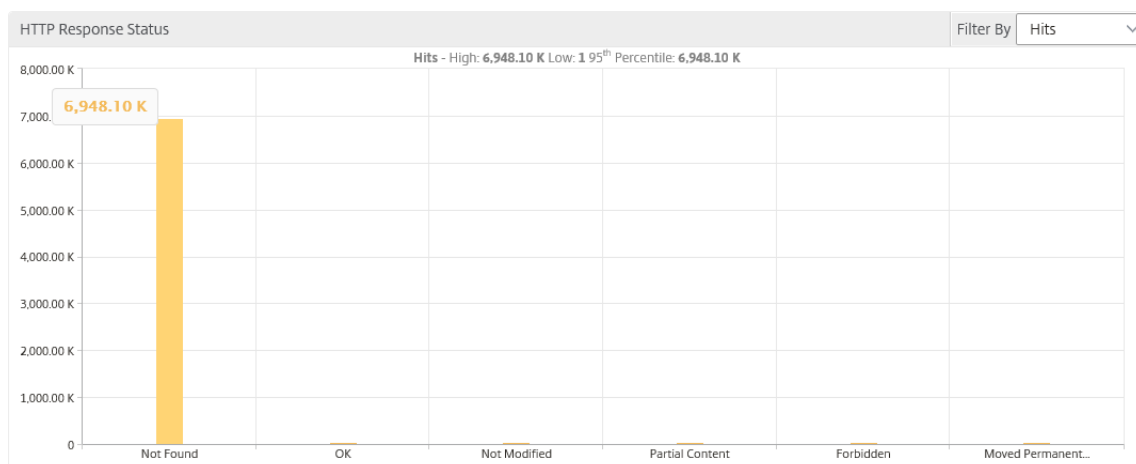
### Cas d’utilisation 1 - Erreur interne du serveur

Considérez un scénario selon lequel vos utilisateurs rencontrent une erreur d’inaccessibilité 500 pour votre application Web. L’erreur 500 (introuvable) est une erreur d’état de réponse HTTP qui indique un problème sur le serveur Web, mais le serveur n’indique pas le problème explicitement. Pour identifier et analyser le problème réel :

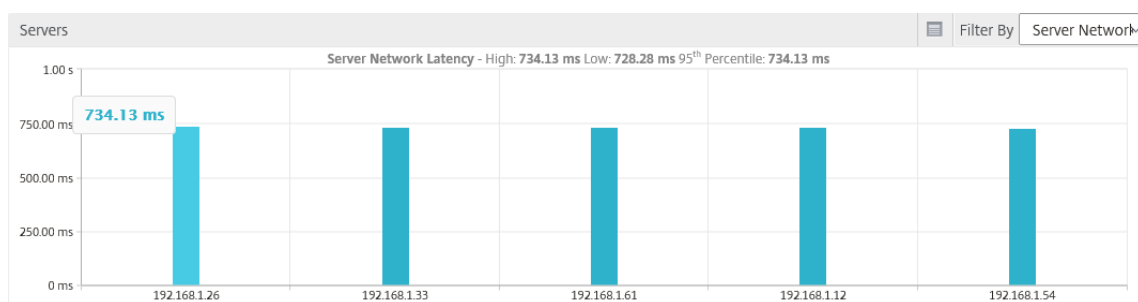
1. Accédez à **Analytics > Web Insight > État des réponses**.

La page du tableau de bord s’affiche. Le tableau de bord fournit les mesures que vous pouvez utiliser pour analyser le succès et l’échec des transactions HTTP traitées.

2. Cliquez sur **Non trouvé** dans le graphique.



3. Faites défiler vers le bas pour afficher le **graphique Serveurset**, dans la liste **Filtrer par**, sélectionnez **Latence réseau du serveur**.



Le graphique indique que chaque serveur d’applications a rencontré un problème lors de la récupération de l’application Web et donc le temps de réponse pour le serveur Web est augmenté. Le problème peut être lié au fait que le serveur Web ne répond à aucune demande d’un serveur.

## Cas d’utilisation 2 - L’utilisateur connaît une lenteur dans l’accès à l’application Web

Considérez un scénario selon lequel votre application Web est hébergée par 10 serveurs Web différents. Lorsque plusieurs utilisateurs accèdent à l’application en même temps, un ou plusieurs utilisateurs peuvent rencontrer une lenteur de l’application. En tant qu’administrateur, vous devez analyser les scénarios suivants pour comprendre la cause première du problème :

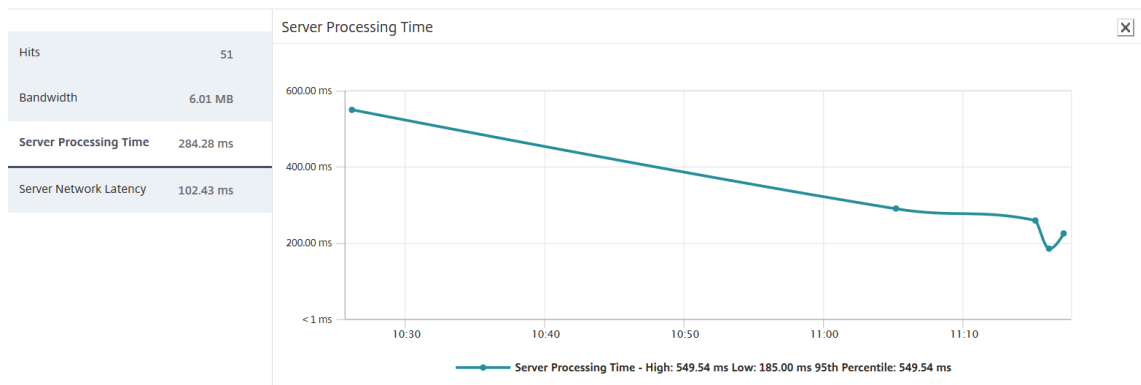
### Scénario 1 - Temps de traitement du serveur :

Lorsque plusieurs requêtes touchent les 10 serveurs Web en même temps, le temps nécessaire pour charger la requête diffère en fonction de :

- Nombre de demandes dans la file d’attente.
- Bande passante consommée par chaque requête pour traiter la transaction HTTP.

Le graphique du serveur peut vous aider à comprendre le temps de traitement de chaque serveur pour la demande traitée par les serveurs. De même, le graphique de l'application affiche les accès, le temps de réponse et la bande passante consommée par chaque transaction HTTP.

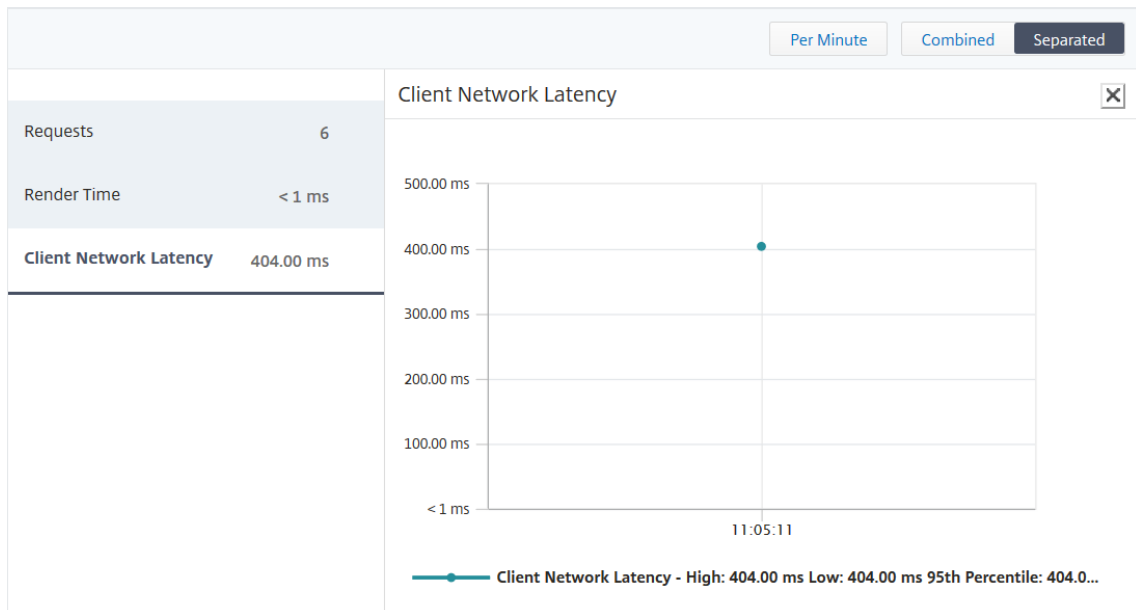
1. Accédez à **Analytics > Web Insight > Serveurs**.
2. Sélectionnez le serveur dans le graphique.
3. Cliquez sur **Temps de traitement du serveur** pour analyser le temps de traitement du serveur.



### Scénario 2 - Latence du client :

Le temps de réponse et le nombre total d'accès pour l'application peuvent être la raison de la lenteur de l'accès à l'application. Vous pouvez vérifier la latence du réseau client et analyser les mesures de latence du réseau client. Pour analyser la cause première :

1. Accédez à **Analytics > Web Insight > Clients**.
2. Sélectionnez le client dans le graphique.
3. Cliquez sur **Latence réseau client** pour analyser la latence élevée.



Dans cet exemple, en tant qu'administrateur, vous pouvez voir que la cause principale du problème provient du réseau client car la latence du réseau client indique un niveau élevé.

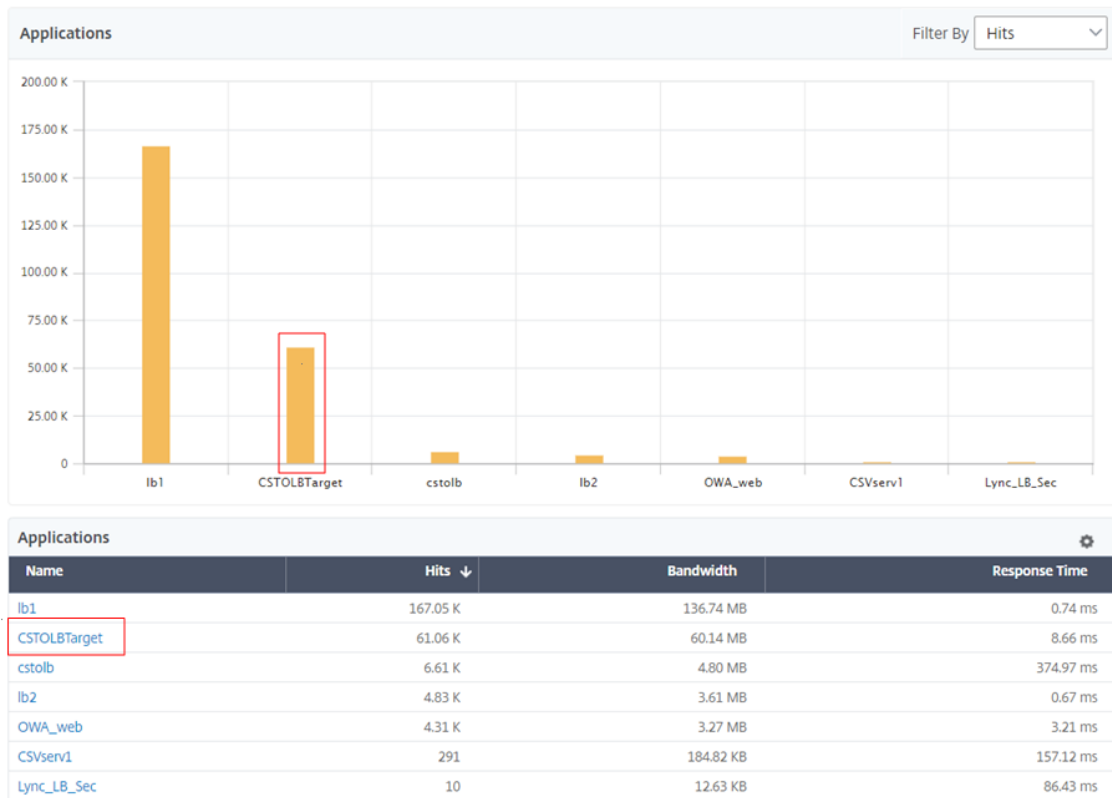
### Cas d'utilisation 3 - Lenteur dans l'accès à l'application Web

Considérez un scénario selon lequel vous disposez de serveurs Web pour les utilisateurs Windows et de serveurs Web pour les utilisateurs Mac, et vos utilisateurs signalent une lenteur dans l'accès à l'application Web. En tant qu'administrateur, vous savez que vous avez :

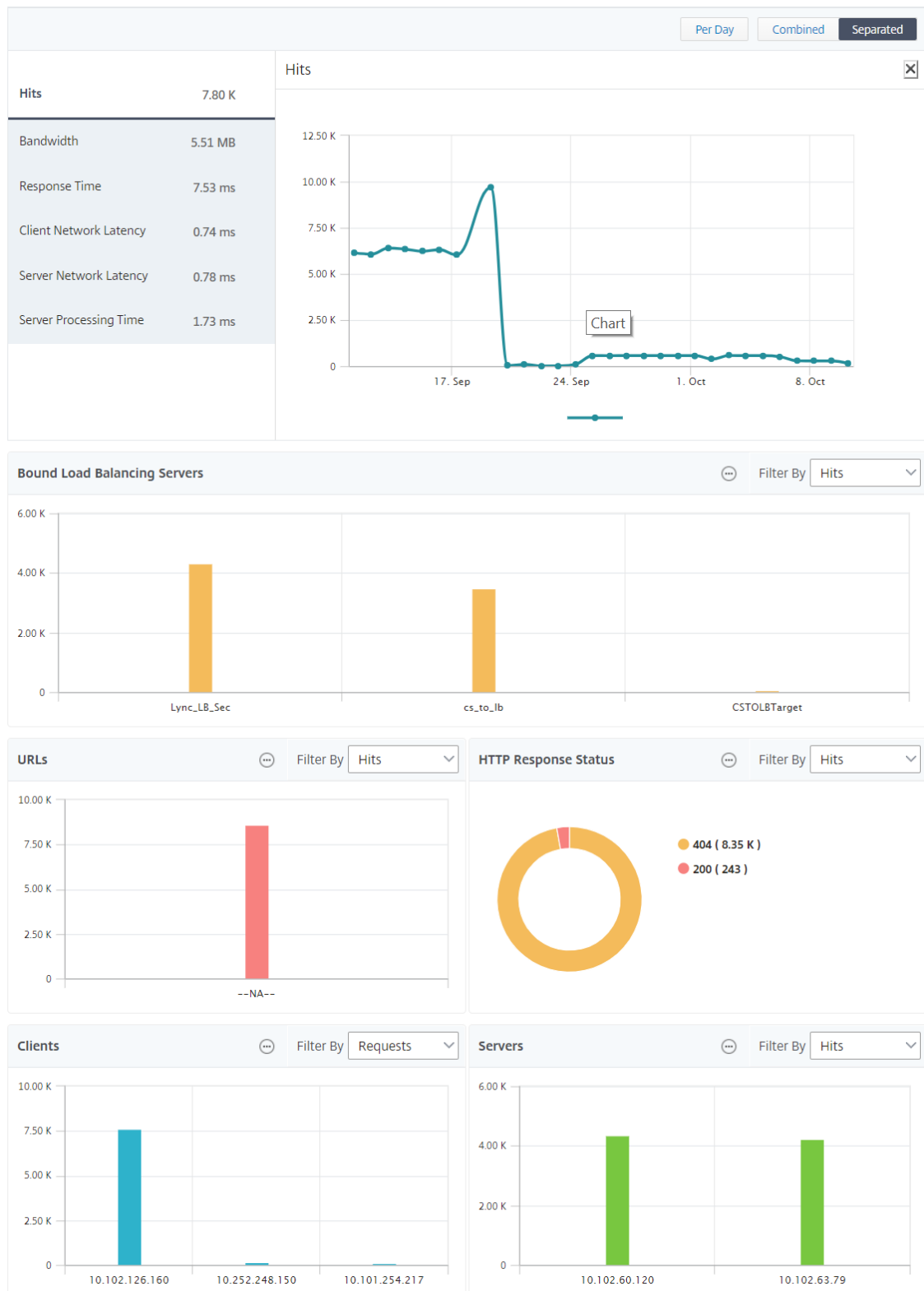
- Configuration d'un serveur virtuel de commutation de contenu pour les utilisateurs Windows.
- Configuration d'un serveur virtuel de commutation de contenu pour les utilisateurs Mac.
- Configuration des services associés liés aux serveurs virtuels pour rediriger les demandes basées sur les utilisateurs Windows et Mac.

Pour analyser la cause première du problème de lenteur de l'application Web :

1. Accédez à **Analytics > Web Insight > Applications**
2. Sélectionnez le serveur virtuel de commutation de contenu.  
Par exemple, l'application « CStolbTarget » dans l'image est un serveur virtuel de commutation de contenu lié à d'autres serveurs virtuels d'équilibrage de charge



3. Cliquez sur le serveur virtuel de commutation de contenu pour afficher l'autre serveur virtuel d'équilibrage de charge. Vous pouvez également cliquer sur le nom de l'application dans le tableau.



Vous pouvez également cliquer sur les serveurs d'équilibrage de charge liés pour afficher les détails Web Insight de ces applications.

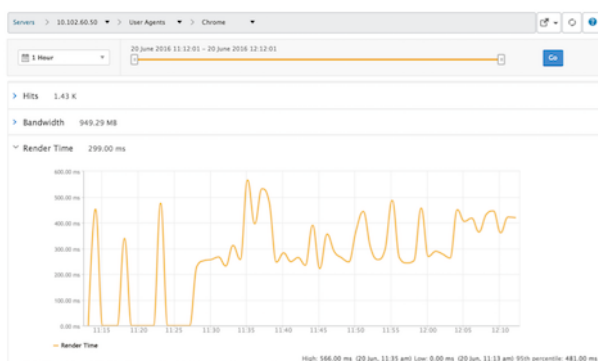


## Analyser des informations pour les navigateurs et les systèmes d'exploitation

Vous pouvez utiliser Web Insight pour vous aider à séparer les problèmes de latence L7 et à comprendre l'utilisation des appareils mobiles. En tant qu'administrateur, les informations peuvent vous aider à comprendre les différentes prises de système d'exploitation au sein de votre base d'utilisateurs.

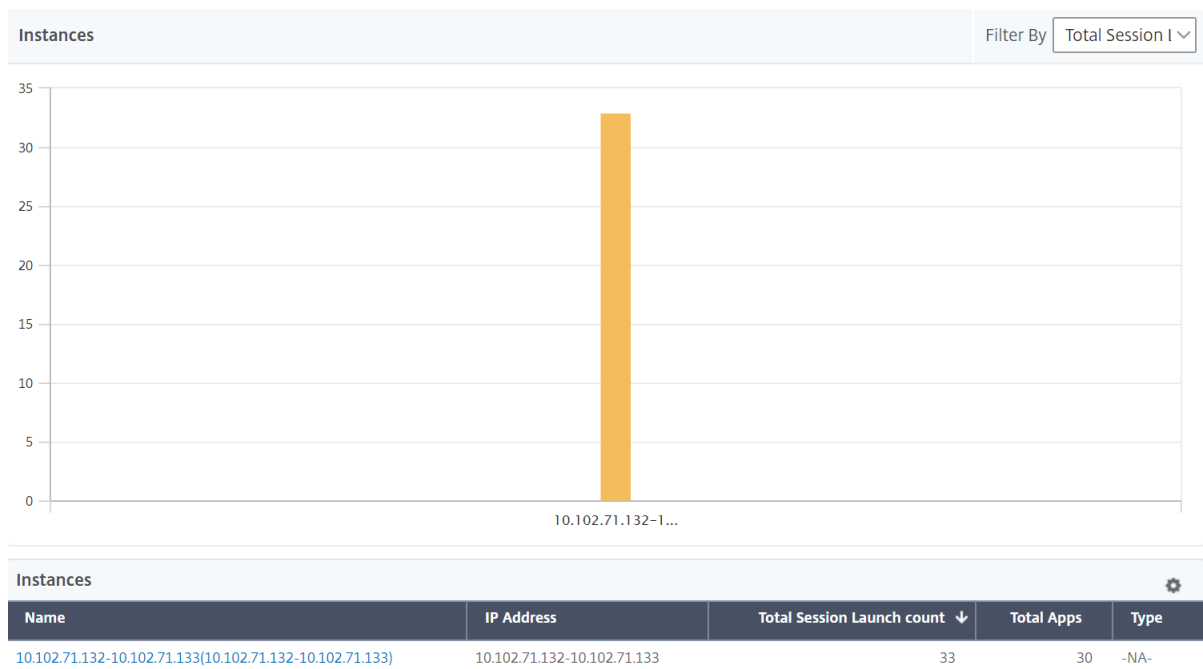
Accédez à **Analytics > Web Insight > Système d'exploitation** pour voir pourquoi l'accès des utilisateurs est lent et si cela est dû à une incompatibilité entre certains navigateurs. Vous pouvez également voir quels systèmes d'exploitation sont utilisés sur certains clients et quels navigateurs sont accessibles. Vous pouvez comparer le temps de rendu entre les différents navigateurs et explorer plus loin vers un navigateur particulier pour identifier les pages d'application associées au temps de rendu le plus élevé pour ce navigateur.

Par exemple, vous pouvez sélectionner Google Chrome et voir les temps de rendu correspondants pour les différentes pages URL d'une application particulière.



## Instances Citrix ADC déployées en mode haute disponibilité

Citrix ADM fournit des rapports pour les instances ADC déployées en mode haute disponibilité. Les rapports agrégés pour les instances en mode haute disponibilité sont pris en charge dans toutes les analyses.



Vous pouvez cliquer sur le nom des instances en haute disponibilité pour afficher plus de détails.

1 Week

1

19 September 2018 08:29:00 - 26 September 2018 08:29:00

1

Go

IP Address  
10.102.71.132-10.102.71.133

Per Day

Combined

Separated

**Total Session Launch count** 33

---

Total Apps 30

**Total Session Launch count** ✕

**Applications** Filter By Launch Durati

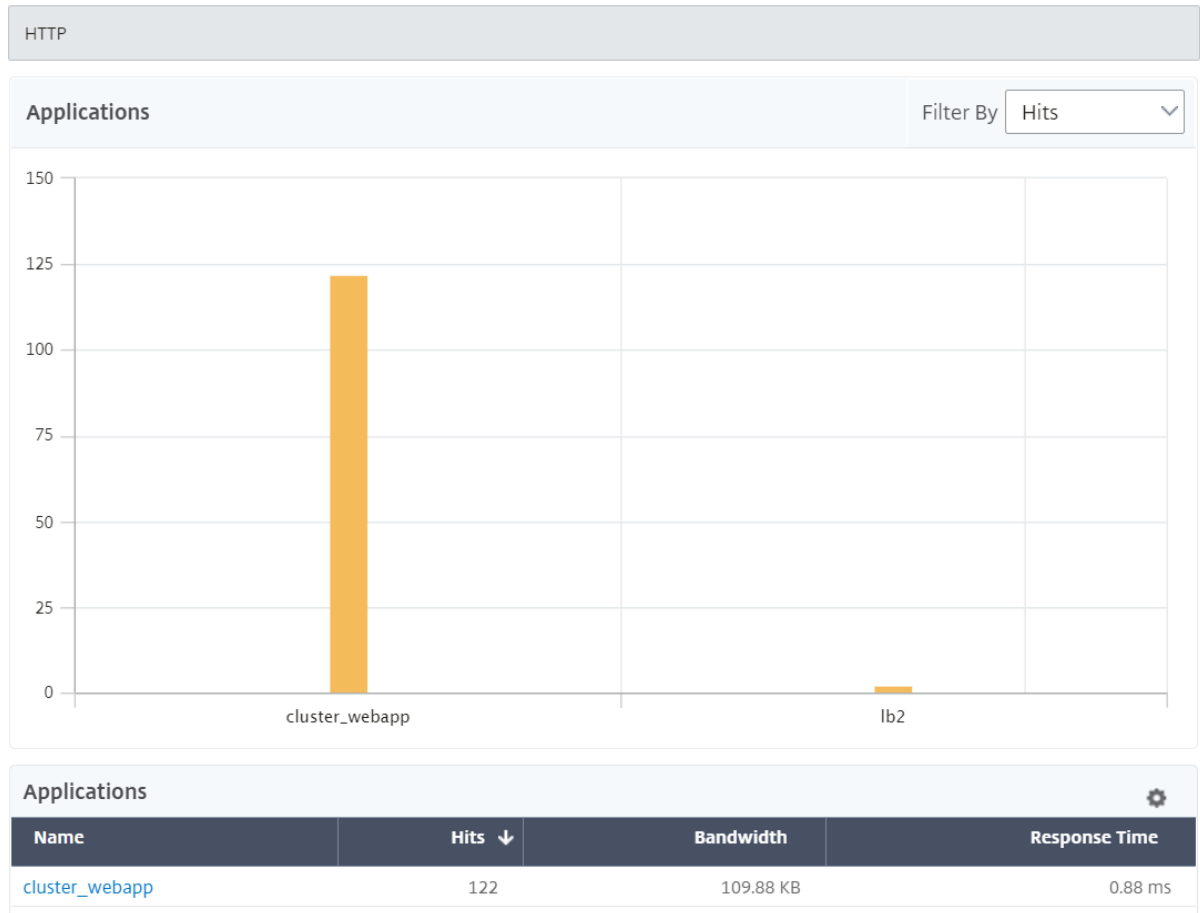
**Users** Filter By Bandwidth

**Desktop Users** Filter By Desktop Laun

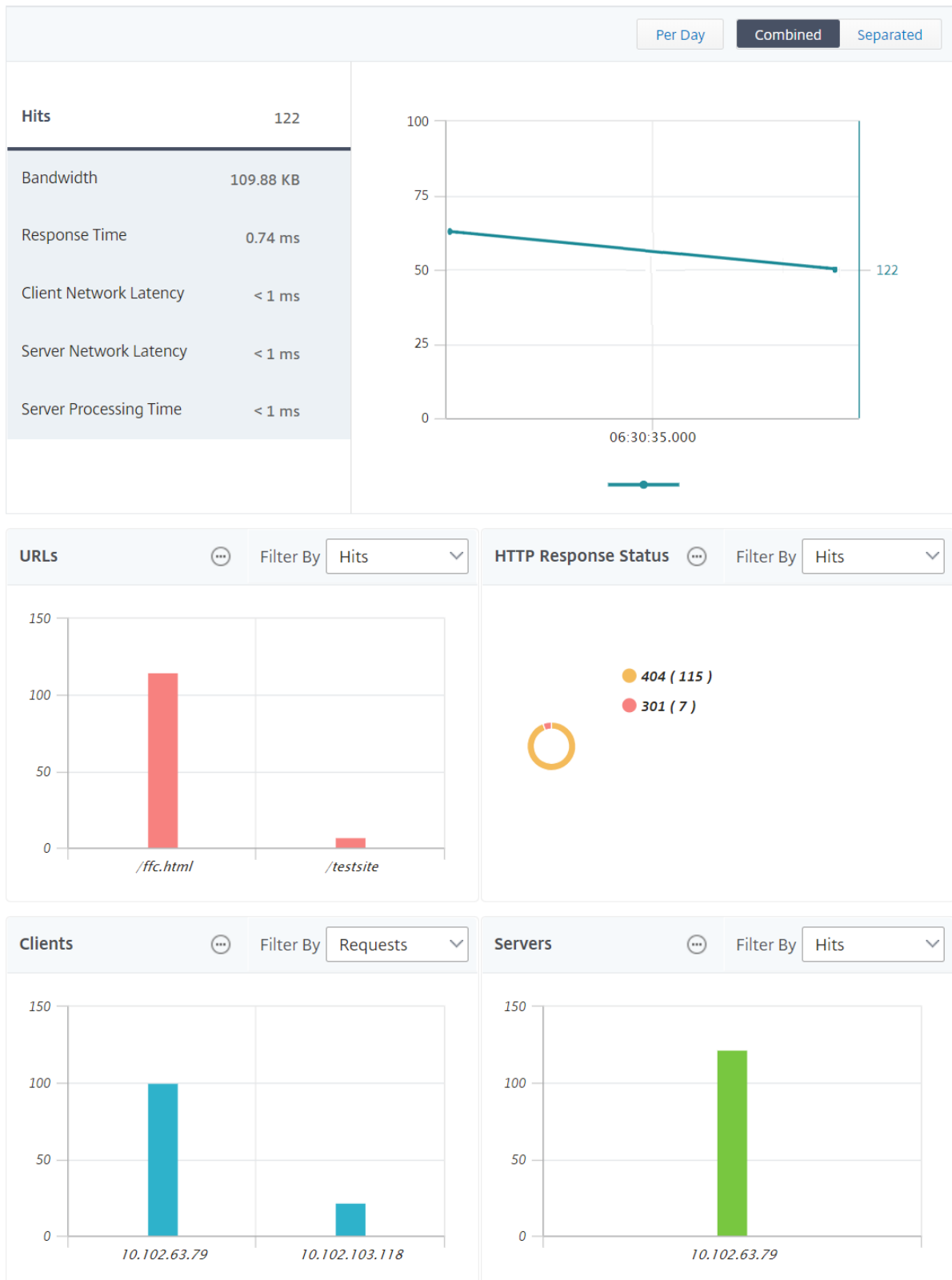
Name	Desktop Launch Count ↓	Session Duration	Bandwidth	DC latency	WAN latency	ICA RTT
XENAPP	2	0 h: 49 m: 0s	1.25 bps	16.00 ms	14.00 ms	20.00 ms
XA65	1	0 h: 7 m: 33s	18.35 Kbps	0 ms	5.00 ms	23.67 ms
XENAPP	1	0 h: 49 m: 0s	0.63 bps	16.00 ms	14.00 ms	20.00 ms
XENAPP	1	0 h: 49 m: 0s	1.25 bps	16.00 ms	14.00 ms	20.00 ms

## Instances Citrix ADC déployées en mode cluster

Citrix ADM fournit des rapports pour les instances ADC déployées en mode cluster. Les rapports agrégés pour les instances en mode cluster sont pris en charge dans toutes les analyses.



Vous pouvez également cliquer sur le nom d'hôte CLIP pour afficher tous les détails sur les instances ADC déployées en mode cluster.



### Remarque

- Toutes les données précédemment collectées avant la mise à niveau vers Citrix ADM 12.1 build 503.x continuent d'être affichées en tant que rapports indépendants pour la période jusqu'à ce que les données persistent.
- Pour les instances ADC déployées en mode cluster, l'ID de domaine d'observation/les noms de domaine d'observation sont remplacés par le nom d'hôte CLIP et CLIP. Toutes les données précédemment collectées continuent de déclarer l'ID de domaine d'observation/nom de domaine d'observation.

## Configuration de la géomap Web Insight

La fonctionnalité Geomaps de Citrix ADM affiche l'utilisation des applications Web sur différents emplacements géographiques sur une carte. Les administrateurs peuvent utiliser ces informations pour comprendre les tendances de l'utilisation des applications et pour la planification des capacités.

Geomap fournit des informations sur les mesures suivantes propres à un pays, un état et une ville :

- Nombre total de visites : nombre total d'accès à une application.
- Bande passante : bande passante totale consommée lors du traitement des demandes des clients
- Temps de réponse : Temps moyen nécessaire pour envoyer des réponses aux demandes des clients.

Les géomaps fournissent des informations qui peuvent être utilisées pour traiter plusieurs cas d'utilisation tels que les suivants :

- Région ayant le nombre maximal de clients accédant à une application
- Région ayant le temps de réponse le plus élevé
- Région qui consomme le plus de bande passante

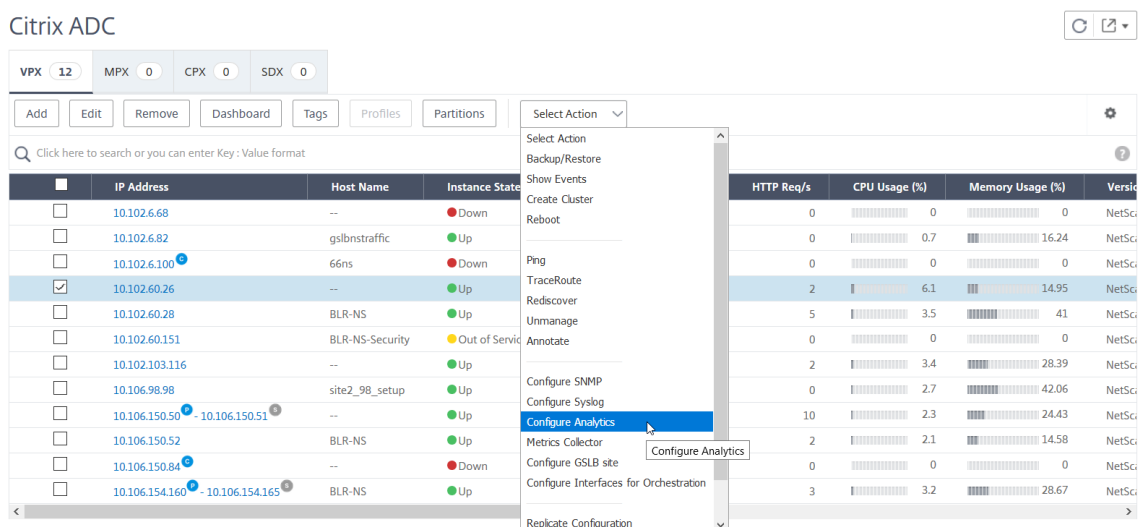
Citrix ADM vous offre une option pour configurer des géomaps pour les adresses IP privées ou les adresses IP publiques.

### Configurer les géomaps pour les adresses IP privées

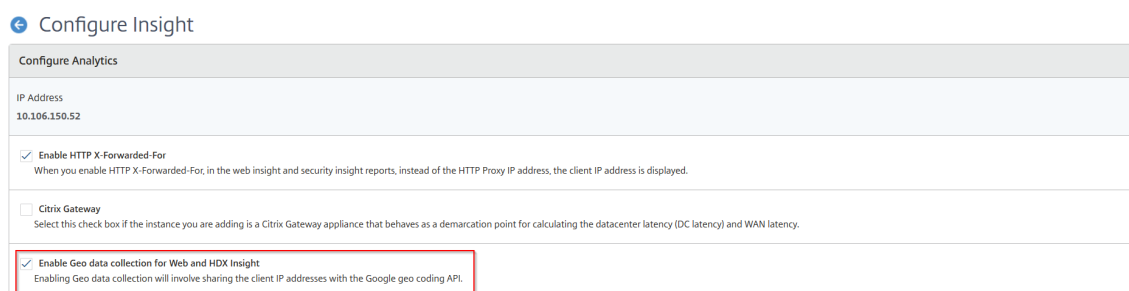
Pour afficher le trafic d'application Web provenant d'adresses IP privées sur la géomap, vous devez d'abord créer des blocs d'adresses IP privées, puis activer la collecte de données géographiques.

Pour activer la collecte de données géographiques :

1. Accédez à **Réseaux > Instances > Citrix ADC**, puis sélectionnez l'instance de Citrix ADC.
2. Dans la liste **Sélectionner une action**, sélectionnez **Configurer Analytics**.



3. Sur la page **Configurer Insight**, sélectionnez **Activer la collecte de données Geo pour Web et HDX Insight**.



**Créer un bloc IP privé** Citrix ADM peut reconnaître l'emplacement d'un client lorsque l'adresse IP privée du client est ajoutée au serveur Citrix ADM. Par exemple, si l'adresse IP d'un client se situe dans la plage d'un bloc d'adresse IP privé associé à la ville A, Citrix ADM reconnaît que le trafic provient de la ville A pour ce client.

Pour créer un bloc IP :

1. Dans Citrix ADM, accédez à **Analytics > Paramètres > Blocs IP**, puis cliquez sur **Ajouter**.
2. Dans la page **Créer des blocs IP**, spécifiez les paramètres suivants :
  - **Nom.** Spécifiez un nom pour le bloc d'adresses IP privées
  - **Adresse IP de départ.** Spécifiez la plage d'adresses IP la plus basse pour le bloc d'adresses IP.
  - **Adresse IP de fin.** Spécifiez la plage d'adresses IP la plus élevée pour le bloc d'adresses IP.

- **Pays.** Sélectionnez le pays dans la liste.
- **Région.** En fonction du pays, la région est renseignée automatiquement, mais vous pouvez sélectionner votre région.
- **Ville.** En fonction de la région, la ville est renseignée automatiquement, mais vous pouvez sélectionner votre ville.
- **Latitude de la ville et longitude de la ville.** En fonction de la ville que vous sélectionnez, la latitude et la longitude sont renseignées automatiquement.

3. Cliquez sur **Créer** pour terminer.

## ← Create IP Blocks

Name\*  
 ?

Start IP Address\*

End IP Address\*  
 ?

Country\*  
 ?

Region\*

City\*

City Latitude\*

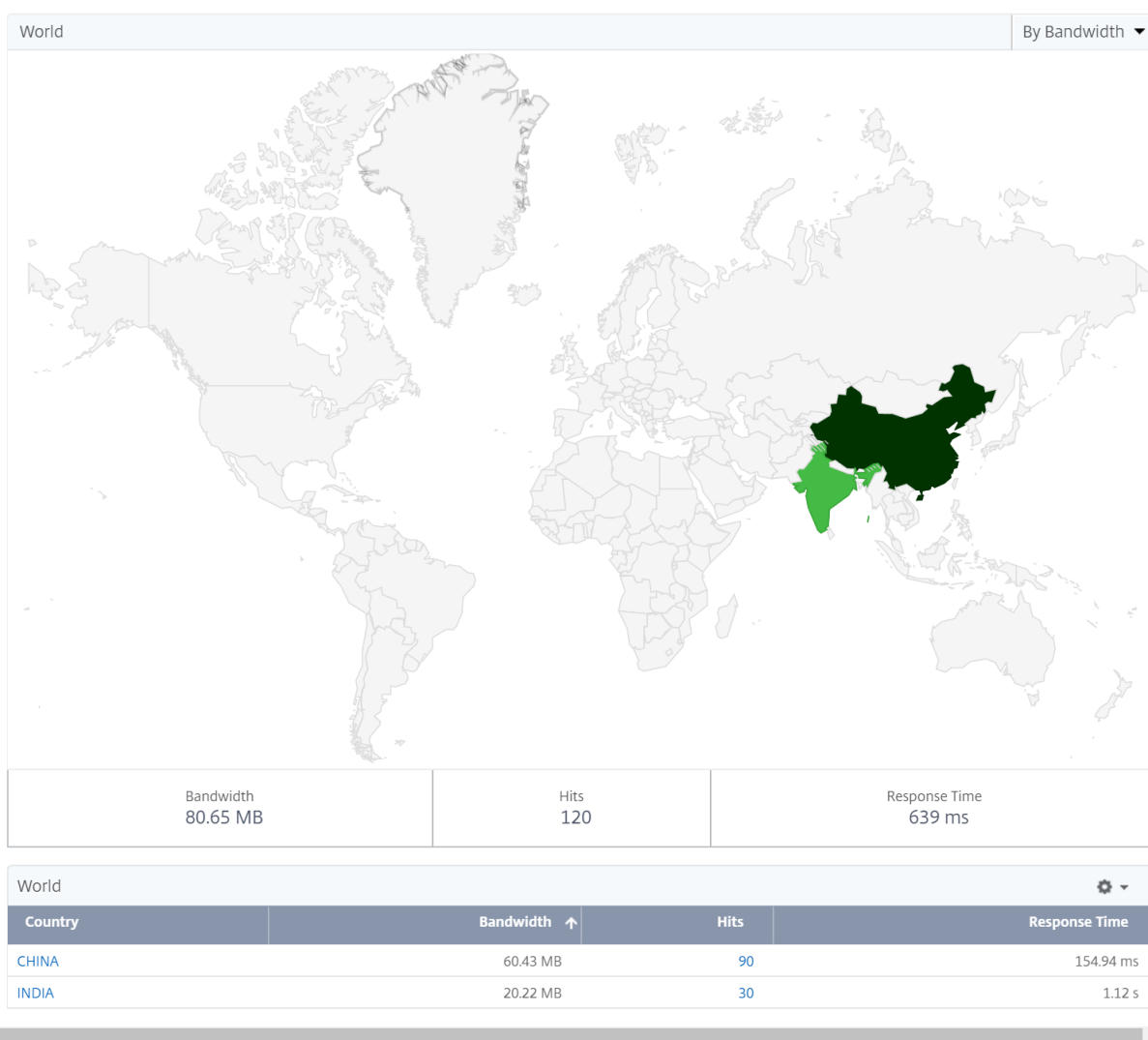
City Longitude\*



**Blocs IP publics** Citrix ADM peut également reconnaître l'emplacement d'un client si le client utilise une adresse IP publique. Citrix ADM possède son fichier CSV d'emplacement intégré qui correspond à l'emplacement basé sur la plage d'adresses IP du client. Pour utiliser un bloc IP public, la seule condition est que vous devez activer l'activation de la collecte de données géographiques à partir de la page Configurer Insight.

Remarque

Citrix ADM a besoin d'une connexion Internet pour afficher les géomaps d'un lieu géographique particulier. Une connexion Internet est également nécessaire pour exporter le GeoMap aux formats .pdf, .png ou .jpg.



**Pour exporter le rapport de ce tableau de bord :**

Pour exporter le rapport de cette page, cliquez sur l'icône **Exporter** en haut à droite de cette page. Sur la page **Exporter**, vous pouvez effectuer l'une des opérations suivantes :

1. Sélectionnez l'onglet **Exporter maintenant** . Pour afficher et enregistrer le rapport au format PDF, JPEG, PNG ou CSV.
2. Sélectionnez l'onglet **Planifier l'exportation**. Pour planifier le rapport sur une base quotidienne, hebdomadaire ou mensuelle et l'envoyer par e-mail ou par message Slack.

#### Remarque

- Si vous sélectionnez Périodicité **hebdomadaire**, veillez à sélectionner les jours de semaine pendant lesquels vous souhaitez que le rapport soit planifié.
- Si vous sélectionnez Périodicité **mensuelle**, veillez à saisir tous les jours, séparés par des virgules, pendant lesquels vous voulez que le rapport soit planifié.

## Configurer les seuils

Vous pouvez créer des seuils et le recevoir une notification chaque fois que la valeur seuil est franchie. Dans un déploiement classique, vous pouvez définir des seuils pour :

- Suivez les différents indicateurs des applications
- Faciliter la planification
- Recevez une notification chaque fois que la valeur métrique de l'application dépasse le seuil défini

Pour configurer le seuil :

1. Accédez à **Analytics > Paramètres > Seuils** .
2. Sur la page **Seuils**, cliquez sur **Ajouter**.  
La page **Créer un seuil** s'affiche.
3. Spécifiez les détails suivants :
  - a) **Nom** : spécifiez un nom pour créer un événement.
  - b) **Type de trafic** - Dans la liste, sélectionnez WEB.
  - c) **Entité** - Dans la liste, sélectionnez la catégorie ou le type de ressource. Par défaut, « applications » est sélectionné comme entité.
  - d) **Clé de référence** : une clé de référence est générée automatiquement en fonction du type de trafic et de l'entité que vous avez sélectionnés.
  - e) **Durée** - Dans la liste, sélectionnez l'intervalle de temps pour lequel vous souhaitez surveiller l'entité. Vous pouvez surveiller les entités pendant une heure, une journée ou une semaine.

## ← Create Threshold

Name\*  
 ?

Traffic Type\*  
 ▾

Entity\*  
 ▾ ?

Reference Key

Duration\*  
 ▾

- f) Dans la section **Configurer la règle**, créez une règle en choisissant la mesure, un comparateur requis et indiquez une valeur de seuil.

**Configure Rule**

Metric\*  
 ▾ ?

Comparator\*  
 ▾

Value\*  
 ?

- g) Dans la section **Paramètres des notifications**, sélectionnez **Activer le seuil** et le mode d'alerte pour lequel vous souhaitez recevoir les alertes.

**Notification Settings**

Enable Threshold ?

Notify through Email ?

Email Distribution List\*  
 ▾

Notify through SMS ?

SMS Distribution List\*  
 ▾

Notify through Slack ?

▾

4. Cliquez sur **Créer**.

## HDX Insight

February 1, 2024

HDX Insight fournit une visibilité de bout en bout du trafic HDX vers Citrix Virtual Apps and Desktops via Citrix ADC. Il permet également aux administrateurs d'afficher en temps réel les mesures de latence des clients et du réseau, les rapports historiques, les données de performance de bout en bout et de résoudre les problèmes de performances. La disponibilité des données de visibilité en temps réel et historiques permet à Citrix Application Delivery Management (ADM) de prendre en charge une grande variété de cas d'utilisation.

Pour que des données apparaissent, vous devez activer AppFlow sur vos serveurs virtuels Citrix Gateway. AppFlow peut être fourni par le protocole IPFIX ou la méthode LogStream.

**Remarque** Pour autoriser l'enregistrement des calculs du temps d'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, que l'utilisateur a créée au cours de 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 d'imprimante et le mappage de lecteur client.

Vous pouvez également accéder à **HDX Insight > Applications** et cliquer sur **Durée de lancement** pour afficher le temps nécessaire au lancement de l'application. Vous pouvez également consulter l'agent utilisateur de tous les utilisateurs connectés en accédant à **HDX Insight-> Users**.

**Remarque** HDX insight prend en charge les partitions d'administration configurées dans les instances de Citrix ADC exécutées sur la version 12.0 du logiciel.

Les clients légers suivants prennent en charge HDX Insight :

- Clients légers WYSE basés sur Windows
- Clients légers basés sur WYSE Linux
- Clients légers WYSE ThinOS
- Clients légers 10Zig basés sur Ubuntu

## Identification de la cause première des problèmes de performances lentes

### Scénario 1

L'utilisateur rencontre des retards lors de l'accès à Citrix Virtual Apps and Desktops.

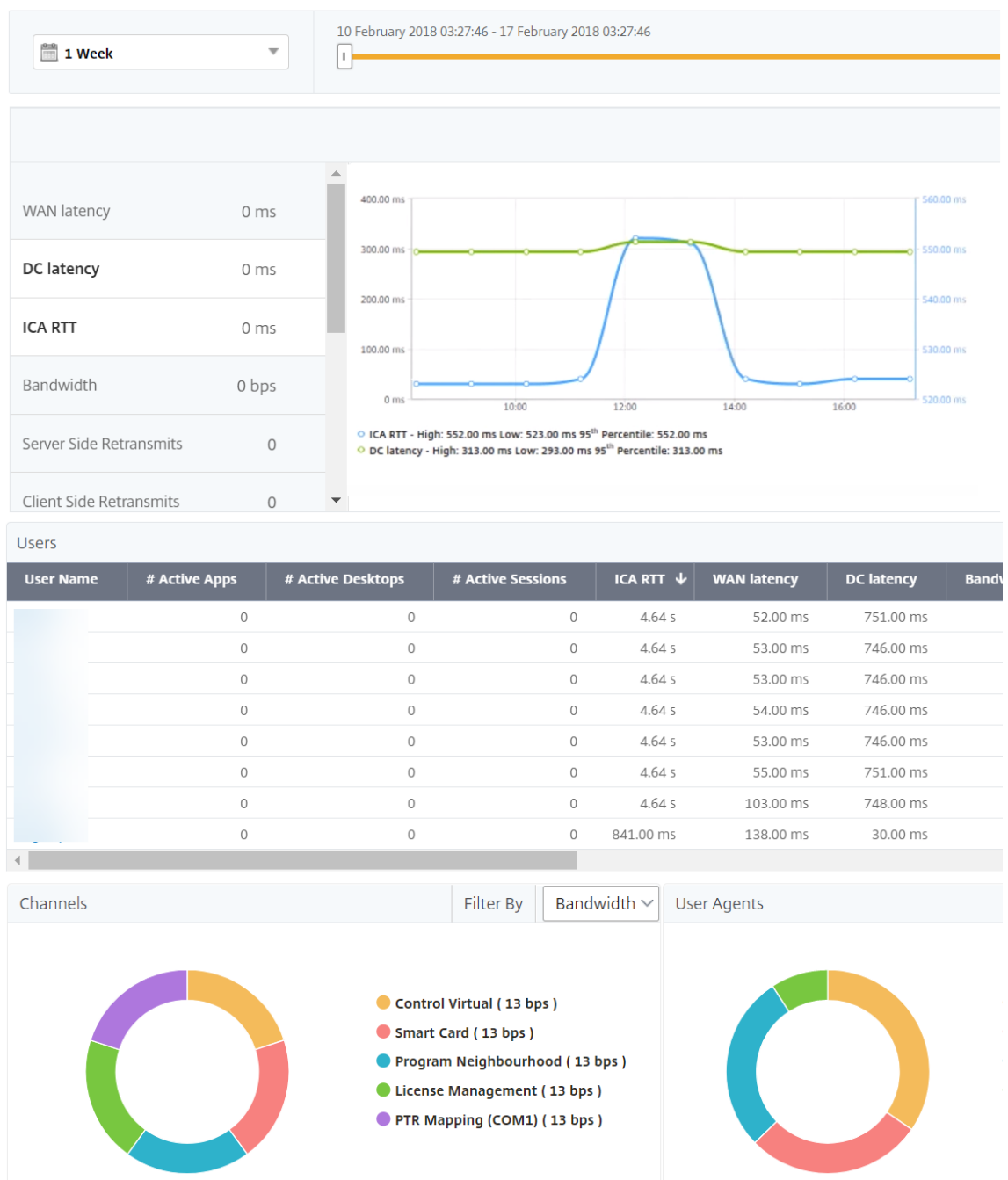
Les retards peuvent être dus à une latence sur le réseau du serveur, à des retards de trafic ICA causés par le réseau du serveur ou à une latence sur le réseau client.

Pour identifier la cause première du problème, analysez les indicateurs suivants :

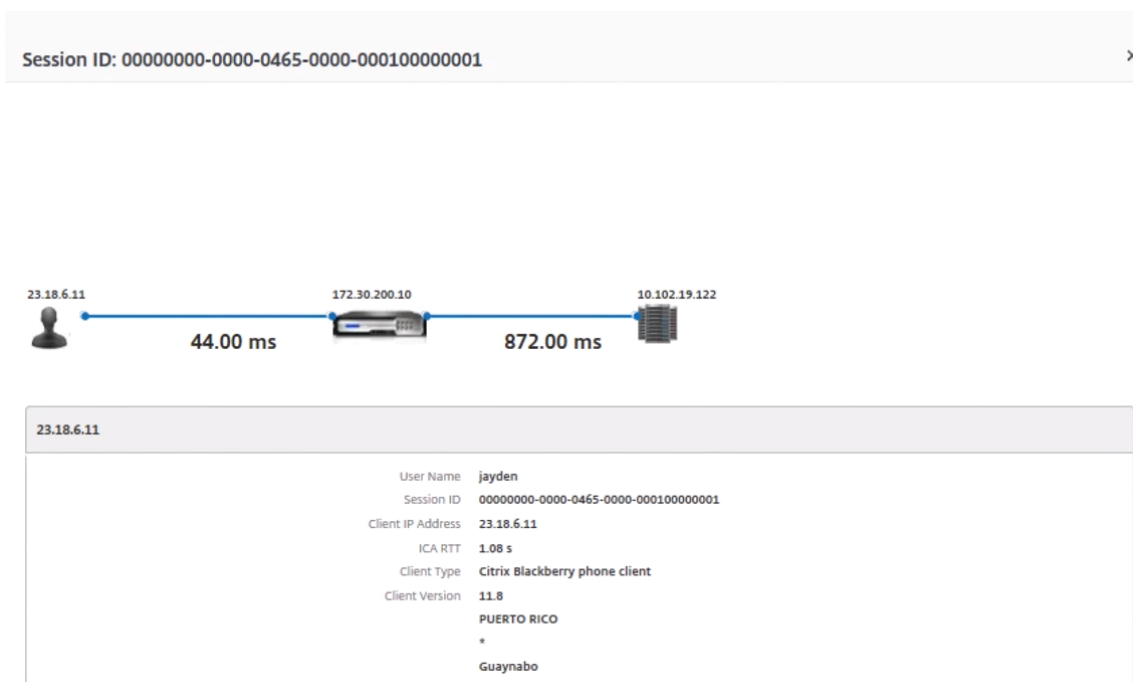
- Latence WAN
- Latence DC
- Délai d'hôte

### Pour afficher les mesures client :

1. Sous l'onglet **Analytics**, accédez à **HDX Insight > Utilisateurs**.
2. Faites défiler la page 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 du WAN** est de 52 millisecondes et les **délais d'hôte** sont 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 Apps or Desktops

Ce retard peut être dû à une latence sur le réseau du serveur, à des retards de trafic ICA-causés par le réseau du serveur, à une latence sur le réseau client ou au temps nécessaire pour lancer une application.

Pour identifier la cause première du problème, analysez les indicateurs suivants :

- Latence WAN
- Latence DC
- Retard de l'hôte

### Pour afficher les mesures utilisateur :

1. Dans l'onglet **Analytics**, accédez à **HDX Insight > Users**.
2. Faites défiler vers le bas et cliquez sur le nom d'utilisateur.

3. Dans la représentation graphique, notez les valeurs Latence WAN, Latence DC et RTT pour la session particulière.
4. Dans le tableau **Sessions en cours**, notez que le délai d'hôte est élevé.

Current Sessions									
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 *****	555.00 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 des statistiques utilisateur supplémentaires, telles que l'instabilité du WAN et les retransmissions côté serveur si vous utilisez Citrix ADM exécutant le logiciel 11.1 build 51.21 ou version ultérieure. Pour afficher ces mesures, accédez à **Analytics > HDX Insight > Utilisateurs**, puis sélectionnez un nom d'utilisateur. Les mesures utilisateur apparaissent dans le tableau en regard du graphique.





## Géomaps pour HDX Insight

La fonctionnalité Citrix ADM Geomaps affiche l'utilisation des applications dans différents emplacements géographiques sur une carte. Les administrateurs peuvent utiliser ces informations pour comprendre les tendances de l'utilisation des applications dans divers emplacements géographiques.

Vous pouvez configurer Citrix ADM pour afficher les cartes géographiques d'un emplacement géographique ou d'un réseau local particulier en spécifiant la plage d'adresses IP privées (adresses IP de début et de fin) de l'emplacement.

Vous pouvez également afficher les détails historiques et actifs des utilisateurs à partir des cartes géographiques dans HDX Insight. Accédez à **Analytics > HDX Insight** et, dans la section Monde de la carte, cliquez sur le pays ou la région pour lequel vous souhaitez afficher les détails. Vous pouvez approfondir la hiérarchie vers le bas pour afficher les informations par ville et par état.

### Pour configurer une géomap pour les centres de données :

Sous l'onglet **Analytics**, accédez à **Paramètres > Blocs IP** pour configurer les géomaps pour un emplacement particulier.

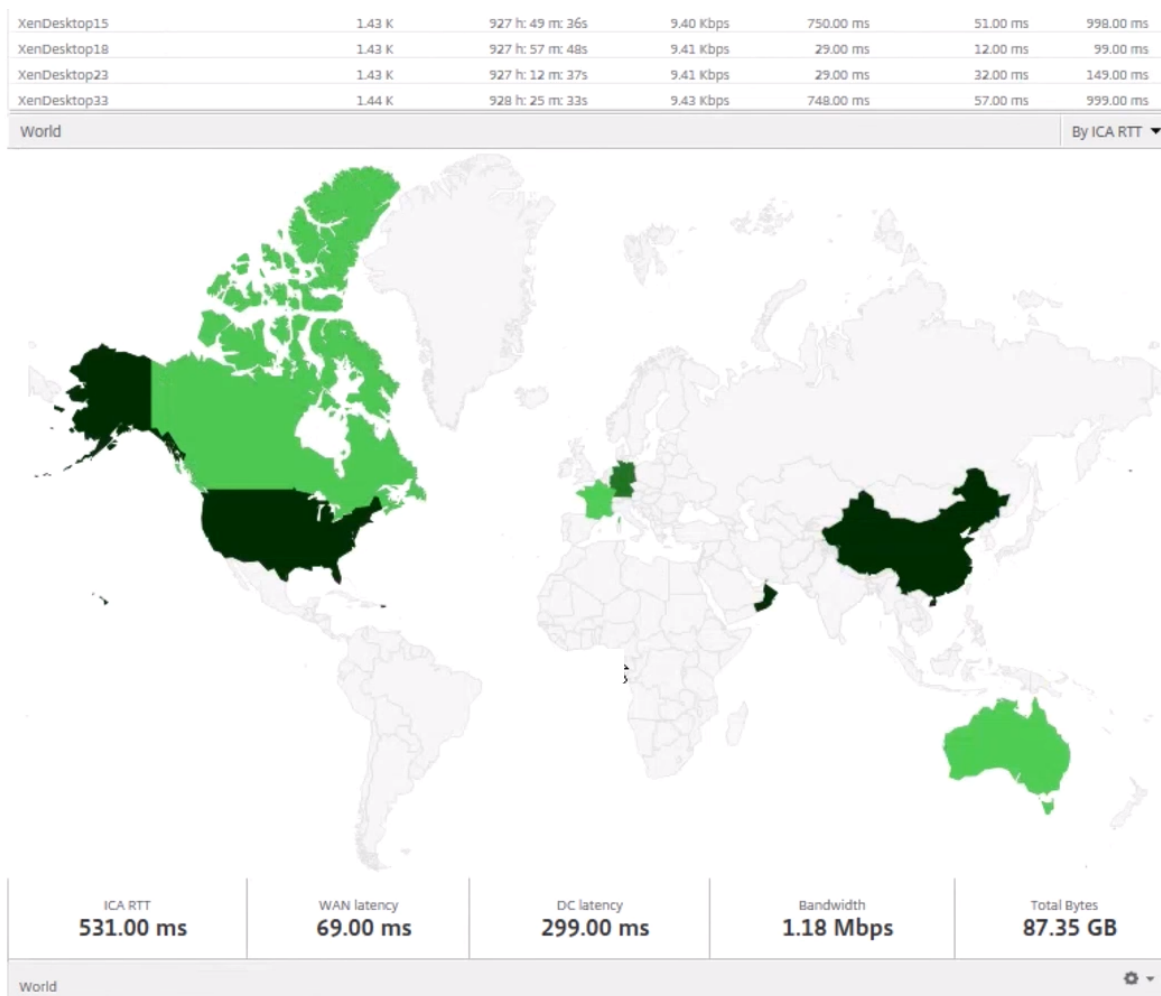
## Cas d'utilisation

Imaginez un scénario dans lequel l'organisation ABC a deux succursales, l'une à Santa Clara et l'autre en Inde.

Les utilisateurs de Santa Clara utilisent l'appliance Citrix Gateway sur Sclara.x.com pour accéder au trafic VPN. Les utilisateurs indiens utilisent l'appliance Citrix Gateway sur India.x.com pour accéder au trafic VPN.

Pendant un intervalle de temps particulier, disons de 10 heures à 17 heures, les utilisateurs de Santa Clara se connectent à Sclara.x.com pour accéder au trafic VPN. La plupart des utilisateurs accèdent au même Citrix Gateway, ce qui entraîne un retard dans la connexion au VPN, de sorte que certains utilisateurs se connectent à India.x.com au lieu de Sclara.x.com.

Un administrateur Citrix ADC analysant le trafic peut utiliser la fonctionnalité géomap pour afficher le trafic dans les bureaux de Santa Clara. La carte montre que le temps de réponse au bureau de Santa Clara est très élevé, car le bureau de Santa Clara ne dispose que d'une seule appliance Citrix Gateway via laquelle les utilisateurs peuvent accéder au trafic VPN. L'administrateur peut donc décider d'installer un autre Citrix Gateway, de sorte que les utilisateurs disposent de deux appliances Citrix Gateway locales via lesquelles accéder au VPN.



### Limitations

Si les instances Citrix ADC disposent d'une licence Enterprise, les seuils définis sur Citrix 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

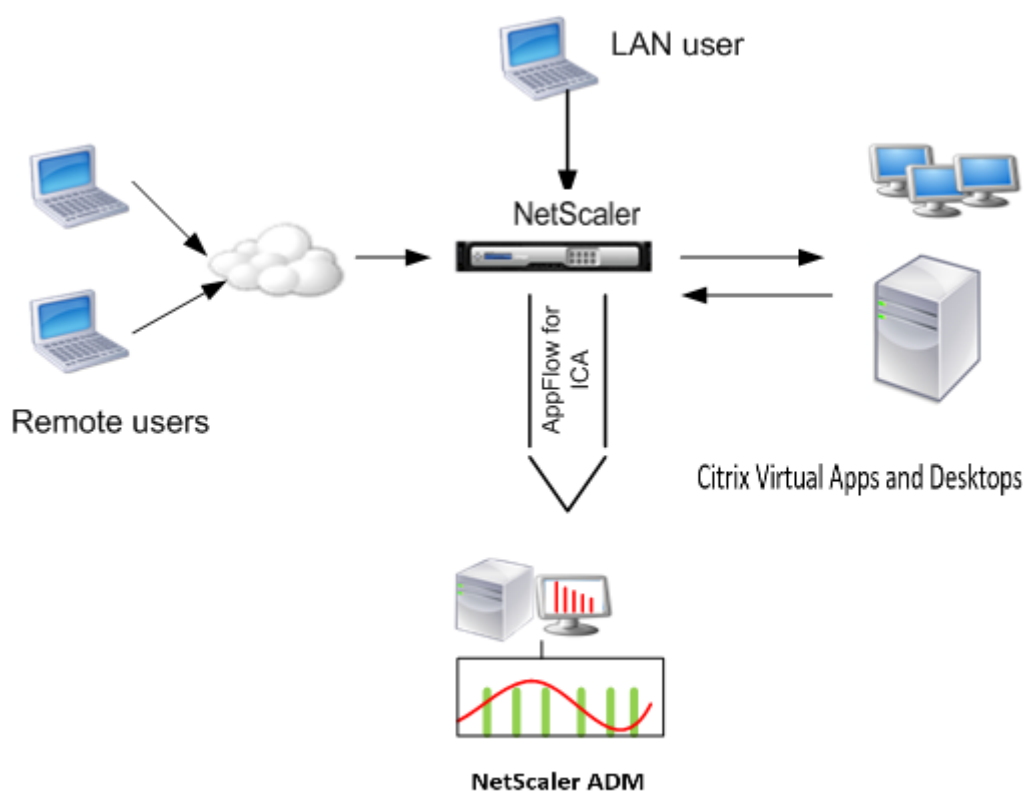
HDX Insight permet au service informatique d'offrir une expérience utilisateur exceptionnelle en offrant une visibilité de bout en bout sans précédent sur le trafic ICA qui passe par les instances Citrix ADC ou les appliances Citrix SD-WAN, et fait partie de Citrix Application Delivery Management (ADM) Analytics. HDX Insight fournit des fonctionnalités de business intelligence et d'analyse des défaillances convaincantes et puissantes pour le réseau, les bureaux virtuels, les applications et la structure des applications. HDX Insight peut à la fois trier instantanément les problèmes des utilisateurs, collecter des données sur les connexions de bureau virtuel et générer des enregistrements AppFlow et les présenter sous forme de rapports visuels.

La configuration permettant la collecte de données dans Citrix ADC diffère selon la position de l'appliance dans la topologie de déploiement.

### **Activation de la collecte de données pour la surveillance des Citrix ADC déployés en mode utilisateur LAN**

Les utilisateurs externes qui accèdent aux applications Citrix Virtual Apps and Desktops doivent s'authentifier sur Citrix Gateway. Toutefois, les utilisateurs internes peuvent ne pas avoir besoin d'être redirigés vers Citrix Gateway. En outre, dans un déploiement en mode transparent, l'administrateur doit appliquer manuellement les stratégies de routage afin que les demandes soient redirigées vers l'appliance Citrix ADC.

Pour surmonter ces difficultés et pour que les utilisateurs LAN se connectent directement aux applications Citrix Virtual Apps and Desktops, vous pouvez déployer l'appliance Citrix ADC en mode utilisateur LAN en configurant un serveur virtuel de redirection de cache, qui agit en tant que proxy SOCKS sur l'appliance Citrix Gateway.



**Remarque** L'appliance Citrix ADM et Citrix Gateway résident dans le même sous-réseau.

Pour surveiller les appliances Citrix ADC déployées dans ce mode, ajoutez d'abord l'appliance Citrix ADC à l'inventaire NetScaler Insight, activez AppFlow, puis consultez les rapports sur le tableau de bord.

Après avoir ajouté l'appliance Citrix ADC à l'inventaire Citrix ADM, vous devez activer AppFlow pour la collecte de données.

**Remarque**

- Sur une instance ADC, vous pouvez naviguer jusqu'à **Système > AppFlow > Collectors**, pour vérifier si le collecteur (c'est-à-dire Citrix ADM) est opérationnel ou non. L'instance Citrix ADC envoie des enregistrements AppFlow à Citrix ADM à l'aide de NSIP. Mais l'instance utilise son SNIP pour vérifier la connectivité avec Citrix ADM. Assurez-vous donc que le SNIP est configuré sur l'instance.
- Vous ne pouvez pas activer la collecte de données sur un Citrix ADC déployé en mode utilisateur LAN à l'aide de l'utilitaire de configuration Citrix ADM.
- Pour des informations détaillées sur les commandes et leur utilisation, consultez la 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 un appliance Citrix ADC à l'aide de l'interface de ligne de commande :

À l'invite de commandes, procédez comme suit :

1. Connectez-vous à une appliance.
2. Ajoutez un serveur virtuel de redirection de cache proxy avec l'IP et le port proxy, et spécifiez le type de service HDX.

**add cr vserver** <name> <servicetype> [<ipaddress> <port>] [-cacheType <cachetype>] [ - cltTimeout <secs>]

Exemple

```
1 add cr vserver cr1 HDX 10.12.2.2 443 - cacheType FORWARD -
  cltTimeout 180
2 <!--NeedCopy-->
```

**Remarque** Si vous accédez au réseau LAN à l'aide d'une appliance Citrix Gateway, ajoutez une action à appliquer par une stratégie correspondant au trafic VPN.

**add vpn trafficAction** <name> <qual> [-HDX ( ON or OFF )]

**add vpn trafficPolicy** <name> <rule> <action>

Exemple

```
1 add vpn trafficAction act1 tcp -HDX ON
2
3 add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
4 <!--NeedCopy-->
```

3. Ajoutez Citrix ADM en tant que collecteur d'applications sur l'appliance Citrix ADC.

**add appflow collector** <name> -IPAddress <ip\_addr>

Exemple :

```
1 add appflow collector MyInsight -IPAddress 192.168.1.101
2 <!--NeedCopy-->
```

4. Créez une action Appflow et associez le collecteur à l'action.

**add appflow action** <name> -collectors <string> ...

Exemple :

```
1 add appflow action act -collectors MyInsight
2 <!--NeedCopy-->
```

5. Créez une stratégie Appflow pour spécifier la règle de génération du trafic.

**add appflow policy** <policyname> <rule> <action>

Exemple :

```
1 add appflow policy pol true act
2 <!--NeedCopy-->
```

6. Liez la stratégie appflow à un point de liaison global.

**bind appflow global** <policyname> <priority> **-type** <type>

Exemple :

```
1 bind appflow global pol 1 -type ICA_REQ_DEFAULT
2 <!--NeedCopy-->
```

**Remarque** La valeur du type doit être ICA\_REQ\_OVERRIDE ou ICA\_REQ\_DEFAULT afin de s'appliquer au trafic ICA.

7. Définissez la valeur du paramètre FlowRecordInterval pour Appflow sur 60 secondes.

**set appflow param -flowRecordInterval** 60

Exemple :

```
1 set appflow param -flowRecordInterval 60
2 <!--NeedCopy-->
```

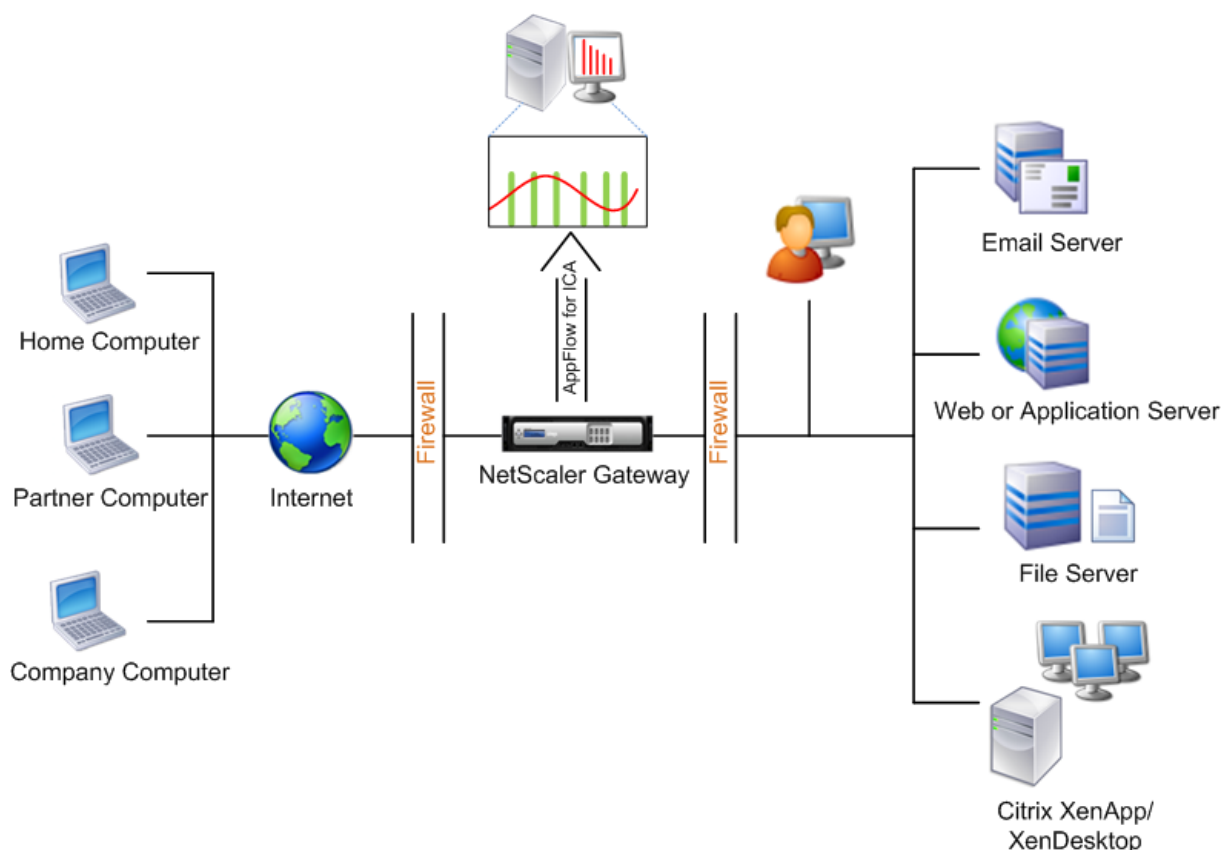
8. Enregistrez la configuration. Type : `save ns config`

## Activation de la collecte de données pour les appliances Citrix Gateway déployées en mode Single-Hop

Lorsque vous déployez Citrix Gateway en mode à saut unique, il se trouve à la périphérie du réseau. L'instance Gateway fournit des connexions ICA proxy à l'infrastructure de mise à disposition des ordinateurs de bureau. Le déploiement à saut unique est le déploiement le plus simple et le plus courant. Le mode à saut unique assure la sécurité lorsqu'un utilisateur externe essaie d'accéder au réseau interne d'une organisation.

En mode saut unique, les utilisateurs accèdent aux appliances Citrix ADC via un réseau privé virtuel (VPN).

Pour commencer à collecter les rapports, vous devez ajouter l'appliance Citrix Gateway à l'inventaire Citrix Application Delivery Management (ADM) et activer AppFlow sur ADM.



#### Pour activer la fonctionnalité AppFlow à partir de Citrix ADM :

1. Dans un navigateur Web, tapez l'adresse IP du Citrix ADM (par exemple, <http://192.168.100.1>).
2. Dans **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Accédez à **Réseaux > Instances**, puis sélectionnez l'instance Citrix ADC que vous souhaitez activer l'analyse.
4. Dans le menu déroulant **Sélectionner une action**, sélectionnez **Configurer Analytics**.
5. Sélectionnez les serveurs virtuels VPN, puis cliquez sur **Activer AppFlow**.
6. Dans le champ **Activer AppFlow**, tapez **true** et sélectionnez **ICA**.
7. Cliquez sur **OK**.

Remarque : Les commandes suivantes sont exécutées en arrière-plan lorsque vous activez AppFlow en mode à saut unique. Ces commandes sont explicitement spécifiées ici à des fins de dépannage.

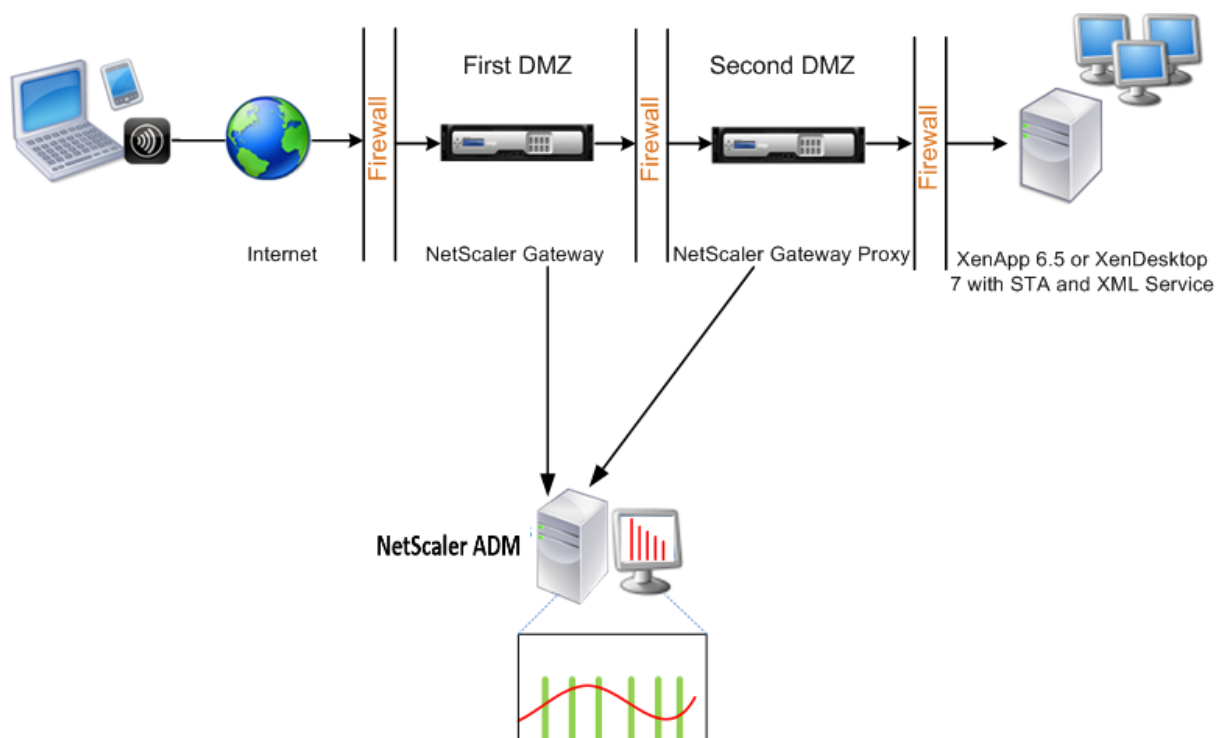
- `add appflow collector <name> -IPAddress <ip_addr>`
- `add appflow action <name> -collectors <string>`

- set appflow param -flowRecordInterval <secs>
- disable ns feature AppFlow
- enable ns feature AppFlow
- add appflow policy <name> <rule> <expression>
- set appflow policy <name> -rule <expression>
- bind vpn vserver <vsname> -policy <string> -type <type> -priority <positive\_integer>
- set vpn vserver <name> -appflowLog ENABLED
- save ns config

Les données de canal virtuel EUEM font partie des données HDX Insight que Citrix ADM reçoit des instances de Gateway. Le canal virtuel EUEM fournit les données sur ICA RTT. Si le canal virtuel EUEM n'est pas activé, les données HDX Insight restantes sont toujours affichées sur Citrix ADM.

### Activation de la collecte de données pour les appliances Citrix Gateway déployées en mode Double Hop

Le mode double saut Citrix Gateway offre une protection supplémentaire au réseau interne d'une organisation car un attaquant doit pénétrer plusieurs zones de sécurité ou zones démilitarisées (DMZ) pour atteindre les serveurs du réseau sécurisé. Si vous souhaitez analyser le nombre de sauts (appliances Citrix Gateway) à travers lesquels les connexions ICA passent, ainsi que les détails sur la latence sur chaque connexion TCP et son rapport avec la latence ICA totale perçue par le client, vous devez installer Citrix ADM afin que les appliances Citrix Gateway rapportent ces statistiques de l'état civil.





Citrix Gateway dans la première DMZ gère les connexions utilisateur et exécute les fonctions de sécurité d'un VPN SSL. Cette passerelle Citrix Gateway chiffre les connexions utilisateur, détermine comment les utilisateurs sont authentifiés et contrôle l'accès aux serveurs du réseau interne.

Citrix Gateway dans la deuxième DMZ sert de périphérique proxy Citrix Gateway. Cette passerelle Citrix Gateway permet au trafic ICA de traverser la deuxième zone démilitarisée pour terminer les connexions utilisateur à la batterie de serveurs.

Le Citrix ADM peut être déployé soit dans le sous-réseau appartenant à l'appliance Citrix Gateway dans la première zone démilitarisée, soit dans le sous-réseau appartenant à la seconde zone démilitarisée de l'appliance Citrix Gateway. Dans l'image ci-dessus, Citrix ADM et Citrix Gateway de la première DMZ sont déployés dans le même sous-réseau.

En mode double saut, Citrix ADM collecte les enregistrements TCP d'une appliance et les enregistrements ICA de l'autre appliance. Une fois que vous avez ajouté les appliances Citrix Gateway à l'inventaire Citrix ADM et activé la collecte de données, chacune des appliances exporte les rapports en suivant le nombre de sauts et l'ID de chaîne de connexion.

Pour que Citrix ADM identifie l'appliance qui exporte des enregistrements, chaque appliance est spécifiée avec un nombre de sauts et chaque connexion est spécifiée avec un ID de chaîne de connexion. Le nombre de sauts représente le nombre d'appliances Citrix Gateway via lesquelles le trafic circule d'un client vers les serveurs. L'ID de chaîne de connexion représente les connexions de bout en bout entre le client et le serveur.

Citrix ADM utilise le nombre de sauts et l'ID de chaîne de connexion pour corréliser les données des appliances Citrix Gateway et générer les rapports.

Pour surveiller les appliances Citrix Gateway déployées dans ce mode, vous devez d'abord ajouter Citrix Gateway à l'inventaire Citrix ADM, activer AppFlow sur Citrix ADM, puis consulter les rapports sur le tableau de bord Citrix ADM.

### **Activation de la collecte de données sur Citrix ADM**

Si vous activez Citrix ADM pour commencer à collecter les détails ICA à partir des deux appliances, les détails collectés sont redondants. Il s'agit des deux appliances qui signalent les mêmes mesures. Pour remédier à cette situation, vous devez activer AppFlow pour ICA sur l'une des premières appliances Citrix Gateway, puis activer AppFlow pour TCP sur la seconde appliance. Ce faisant, l'une des appliances exporte les enregistrements ICA AppFlow et l'autre appliance exporte les enregistrements TCP AppFlow. Cela permet également d'économiser le temps de traitement lors de l'analyse du trafic ICA.

### **Pour activer la fonctionnalité AppFlow à partir de Citrix ADM :**

1. Dans un navigateur Web, tapez l'adresse IP du Citrix ADM (par exemple, <http://192.168.100.1>).

2. Dans **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Accédez à **Réseaux > Instances**, puis sélectionnez l'instance Citrix ADC que vous souhaitez activer l'analyse.
4. **Dans le menu déroulant Sélectionner une action**, sélectionnez **Configurer Analytics**.
5. Sélectionnez les serveurs virtuels VPN, puis cliquez sur **Activer AppFlow**.
6. Dans le champ **Activer AppFlow**, tapez **true** et sélectionnez **ICA/TCP** pour le trafic ICA et le trafic TCP respectivement.

**Remarque** Si la journalisation AppFlow n'est pas activée pour les services ou groupes de services respectifs sur l'appliance Citrix ADC, le tableau de bord Citrix ADM n'affiche pas les enregistrements, même si la colonne Insight indique Enabled.

7. Cliquez sur **OK**.

### Configuration des appliances Citrix Gateway pour exporter des données

Après avoir installé les appliances Citrix Gateway, vous devez configurer les paramètres suivants sur les appliances Citrix Gateway pour exporter les rapports vers Citrix ADM :

- Configurez les serveurs virtuels des appliances Citrix Gateway dans la première et la deuxième zone démilitarisée pour communiquer entre eux.
- Liez le serveur virtuel Citrix Gateway dans la deuxième zone DMZ au serveur virtuel Citrix Gateway dans la première zone DMZ.
- Activez le double saut sur Citrix Gateway dans la deuxième DMZ.
- Désactivez l'authentification sur le serveur virtuel Citrix Gateway dans la deuxième DMZ.
- Permettre à l'une des appliances Citrix Gateway d'exporter des enregistrements ICA
- Activez l'autre appliance Citrix Gateway pour exporter des enregistrements TCP :
- Activez le chaînage des connexions sur les deux appliances Citrix Gateway.

### Configuration de Citrix Gateway à l'aide de l'interface de ligne de commande :

1. Configurez le serveur virtuel Citrix Gateway dans la première zone DMZ pour qu'il communique avec le serveur virtuel Citrix Gateway dans la deuxième zone DMZ.

```
add vpn nextHopServer <name> <nextHopIP> <nextHopPort> [-secure(ON or OFF)] [-imgGifToPng] ...
```

```
add vpn nextHopServer nh1 10.102.2.33 8443 -secure ON
```

2. Liez le serveur virtuel Citrix Gateway dans la deuxième zone DMZ au serveur virtuel Citrix Gateway dans la première zone DMZ. Exécutez la commande suivante sur Citrix Gateway dans la première DMZ :

```
bind vpn vserver <name> -nextHopServer <name>
```

```
bind vpn vserver vs1 -nextHopServer nh1
```

3. Activez le double saut et AppFlow sur Citrix Gateway dans la deuxième DMZ.

```
set vpn vserver <name> [- doubleHop ( ENABLED or DISABLED )] [- appflowLog ( ENABLED or DISABLED )]
```

```
set vpn vserver vphop2 -doubleHop ENABLED -appFlowLog ENABLED
```

4. Désactivez l'authentification sur le serveur virtuel Citrix Gateway dans la deuxième DMZ.

```
set vpn vserver<name> [-authentication (ON or OFF)]
```

```
set vpn vserver vs -authentication OFF
```

5. Activez l'une des appliances Citrix Gateway pour exporter des enregistrements TCP.

```
bind vpn vserver<name> [-policy<string> -priority<positive_integer>] [-type<type>]
```

```
bind vpn vserver vpn1 -policy appflowpol1 -priority 101 -type OTHERTCP_REQUEST
```

6. Activez l'autre appliance Citrix Gateway pour exporter des enregistrements ICA :

```
bind vpn vserver<name> [-policy<string> -priority<positive_integer>] [-type<type>]
```

```
bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type ICA_REQUEST
```

7. Activez le chaînage des connexions sur les deux appliances Citrix Gateway :

```
set appFlow param [-connectionChaining (ENABLED or DISABLED)]
```

```
set appflow param -connectionChaining ENABLED
```

### Configuration de Citrix Gateway à l'aide de l'utilitaire de configuration :

1. Configurez Citrix Gateway dans la première DMZ pour communiquer avec Citrix Gateway dans la deuxième DMZ et lier Citrix Gateway dans la deuxième DMZ à Citrix Gateway dans la première DMZ.
  - a) Sous l'onglet **Configuration**, développez **Citrix Gateway** et cliquez sur **Serveurs virtuels**.
  - b) Dans le volet droit, double-cliquez sur le serveur virtuel et dans le groupe Avancé, développez **Applications publiées**.
  - c) Cliquez sur **Serveur de saut suivant** et liez un serveur de saut suivant à la deuxième appliance Citrix Gateway.
2. Activez le double saut sur Citrix Gateway dans la deuxième DMZ.

- a) Sous l'onglet **Configuration**, développez **Citrix Gateway** et cliquez sur **Serveurs virtuels**.
  - b) Dans le volet droit, double-cliquez sur le serveur virtuel, puis dans le groupe **Paramètres de base**, cliquez sur l'icône de modification.
  - c) Développez **Plus**, sélectionnez **Double saut** et cliquez sur **OK**.
3. Désactivez l'authentification sur le serveur virtuel sur Citrix Gateway dans la deuxième zone démilitarisée.
- a) Dans l'onglet **Configuration**, développez **Citrix Gateway** et cliquez sur **Virtual Servers**.
  - b) Dans le volet droit, double-cliquez sur le serveur virtuel, puis dans le groupe **Paramètres de base**, cliquez sur l'icône de modification.
  - c) Développez **Plus** et décochez **Activer l'authentification**.
4. Activez l'une des appliances Citrix Gateway pour exporter des enregistrements TCP.
- a) Dans l'onglet **Configuration**, développez **Citrix Gateway** et cliquez sur **Virtual Servers**.
  - b) Dans le volet droit, double-cliquez sur le serveur virtuel et dans le groupe **Avancé**, développez **Stratégies**.
  - c) Cliquez sur l'icône + et dans la liste déroulante **Choose Policy**, sélectionnez **AppFlow** et dans la liste déroulante **Choose Type**, sélectionnez **Other TCP Request**.
  - d) Cliquez sur **Continuer**.
  - e) Ajoutez une liaison de stratégie, puis cliquez sur **Fermer**.
5. Activez l'autre appliance Citrix Gateway pour exporter des enregistrements ICA :
- a) Dans l'onglet **Configuration**, développez **Citrix Gateway** et cliquez sur **Virtual Servers**.
  - b) Dans le volet droit, double-cliquez sur le serveur virtuel, puis dans le groupe **Avancé**, développez **Stratégies**.
  - c) Cliquez sur l'icône + et dans la liste déroulante **Choose Policy**, sélectionnez **AppFlow** et dans la liste déroulante **Choose Type**, sélectionnez **Other TCP Request**.
  - d) Cliquez sur **Continuer**.
  - e) Ajoutez une liaison de stratégie, puis cliquez sur **Fermer**.
6. Activez le chaînage des connexions sur les deux appliances Citrix Gateway.
- a) Sous l'onglet **Configuration**, accédez à **Systeme > Appflow**.
  - b) Dans le volet droit, dans le groupe **Paramètres**, cliquez sur **Modifier les paramètres Appflow**.

- c) Select **Chaîne de connexion** et cliquez sur **OK**.
7. Configurez Citrix Gateway dans la première DMZ pour communiquer avec Citrix Gateway dans la deuxième DMZ et lier Citrix Gateway dans la deuxième DMZ à Citrix Gateway dans la première DMZ.
  - a) Sous l'onglet Configuration, développez **Citrix Gateway** et cliquez sur **Serveurs virtuels**.
  - b) Dans le volet droit, double-cliquez sur le serveur virtuel, puis dans le groupe **Avancé**, développez **Applications publiées**.
  - c) Cliquez sur **Serveur de saut suivant** et liez un serveur de saut suivant à la deuxième appliance Citrix Gateway.
8. Activez le double saut sur Citrix Gateway dans la deuxième DMZ.
  - a) Sous l'onglet Configuration, développez **Citrix Gateway** et cliquez sur **Serveurs virtuels**.
  - b) Dans le volet droit, double-cliquez sur le serveur virtuel, puis dans le groupe **Paramètres de base**, cliquez sur l'icône Modifier.
  - c) Développez **Plus**, sélectionnez **Double Hop** et cliquez sur **OK**.
9. Désactivez l'authentification sur le serveur virtuel sur Citrix Gateway dans la deuxième zone démilitarisée.
  - a) Dans l'onglet Configuration, développez Citrix Gateway et cliquez sur **Virtual Servers**.
  - b) Dans le volet droit, double-cliquez sur le serveur virtuel, puis dans le groupe **Paramètres de base**, cliquez sur l'icône d'édition.
  - c) Développez **Plus** et décochez **Activer l'authentification**.
10. Activez l'une des appliances Citrix Gateway pour exporter des enregistrements TCP.
  - a) Sous l'onglet Configuration, développez **Citrix Gateway** et cliquez sur **Serveurs virtuels**.
  - b) Dans le volet droit, double-cliquez sur le serveur virtuel, puis dans le groupe **Avancé**, développez **Stratégies**.
  - c) Cliquez sur l'icône **+** et dans la liste 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**.
11. Activez l'autre appliance Citrix Gateway pour exporter des enregistrements ICA.
  - a) Sous l'onglet Configuration, développez **Citrix Gateway** et cliquez sur **Serveurs virtuels**.

- b) Dans le volet droit, double-cliquez sur le serveur virtuel, puis dans le groupe Avancé, développez **Stratégies**.
  - c) Cliquez sur l'icône+ et dans la liste déroulante **Choose Policy** , sélectionnez **AppFlow** et dans la liste déroulante **Choose Type** , sélectionnez **Other TCPRequest**.
  - d) Cliquez sur **Continuer**.
  - e) Ajoutez une liaison de stratégie, puis cliquez sur **Fermer**.
12. Activez le chaînage des connexions sur les deux appliances Citrix Gateway.

### **Activation de la collecte de données pour la surveillance des Citrix ADC déployés en mode transparent**

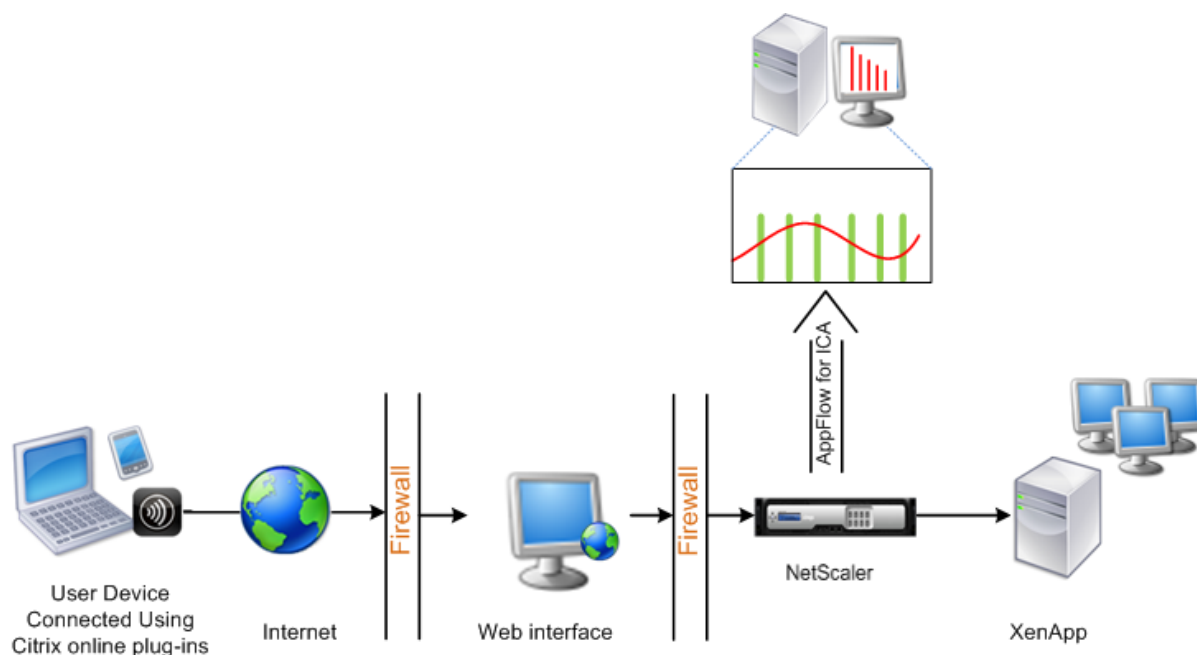
Lorsqu'un Citrix ADC est déployé en mode transparent, les clients peuvent accéder directement aux serveurs, sans aucun serveur virtuel intermédiaire. Si une appliance Citrix ADC est déployée en mode transparent dans un environnement Citrix Virtual Apps and Desktop, le trafic ICA n'est pas transmis via un VPN.

Après avoir ajouté Citrix ADC à l'inventaire Citrix ADM, vous devez activer AppFlow pour la collecte de données. L'activation de la collecte de données dépend du périphérique et du mode. Dans ce cas, vous devez ajouter Citrix ADM en tant que collecteur AppFlow sur chaque appliance Citrix ADC, et vous devez configurer une stratégie Appflow pour collecter tout le trafic ICA ou un trafic spécifique qui traverse l'appliance.

#### **Remarque**

- Vous ne pouvez pas activer la collecte de données sur un Citrix ADC déployé en mode transparent à l'aide de l'utilitaire de configuration Citrix ADM.
- Pour des informations détaillées sur les commandes et leur utilisation, consultez la section [Référence des commandes](#).
- Pour plus d'informations sur les expressions de stratégie, consultez la section [Politiques et expressions](#).

La figure suivante illustre le déploiement réseau d'un Citrix ADM lorsqu'un Citrix ADC est déployé en mode transparent :



**Pour configurer la collecte de données sur un appliance Citrix ADC à l'aide de l'interface de ligne de commande :**

À l'invite de commandes, procédez comme suit :

1. Connectez-vous à une appliance.
2. Spécifiez les ports ICA sur lesquels l'apppliance Citrix ADC écoute le trafic.

```
1 set ns param --icaPorts <port>...
2 <!--NeedCopy-->
```

**Exemple :**

```
1 set ns param -icaPorts 2598 1494
2 <!--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 de flux d'applications sur l'apppliance Citrix ADC.

```
1 add appflow collector <name> -IPAddress <ip_addr>
2 <!--NeedCopy-->
```

**Exemple :**

```
1 add appflow collector MyInsight -IPAddress 192.168.1.101
2 <!--NeedCopy-->
```

**Remarque** Pour afficher les collecteurs de flux d'applications configurés sur l'apppliance Citrix ADC, utilisez la **commande show appflow collector**.

4. Créez une action Appflow et associez le collecteur à l'action.

```
1 add appflow action <name> -collectors <string> ...
2 <!--NeedCopy-->
```

**Exemple :**

ajouter Appflow Action Act -Collectors MyInsight

5. Créez une stratégie Appflow pour spécifier la règle de génération du trafic.

```
1 add appflow policy <polycyname> <rule> <action>
2 <!--NeedCopy-->
```

**Exemple :**

```
1 add appflow policy pol true act
2 <!--NeedCopy-->
```

6. Liez la stratégie appflow à un point de liaison global.

```
1 bind appflow global <polycyname> <priority> -type <type>
2 <!--NeedCopy-->
```

**Exemple :**

```
1 bind appflow global pol 1 -type ICA_REQ_DEFAULT
2 <!--NeedCopy-->
```

**Remarque** La valeur du **type** doit être ICA\_REQ\_OVERRIDE ou ICA\_REQ\_DEFAULT afin de s'appliquer au trafic ICA.

7. Définissez la valeur du paramètre FlowRecordInterval pour Appflow sur 60 secondes.

```
1 set appflow param -flowRecordInterval 60
2 <!--NeedCopy-->
```

**Exemple :**

```
1 set appflow param -flowRecordInterval 60
2 <!--NeedCopy-->
```

8. Enregistrez la configuration. Type : `save ns config`



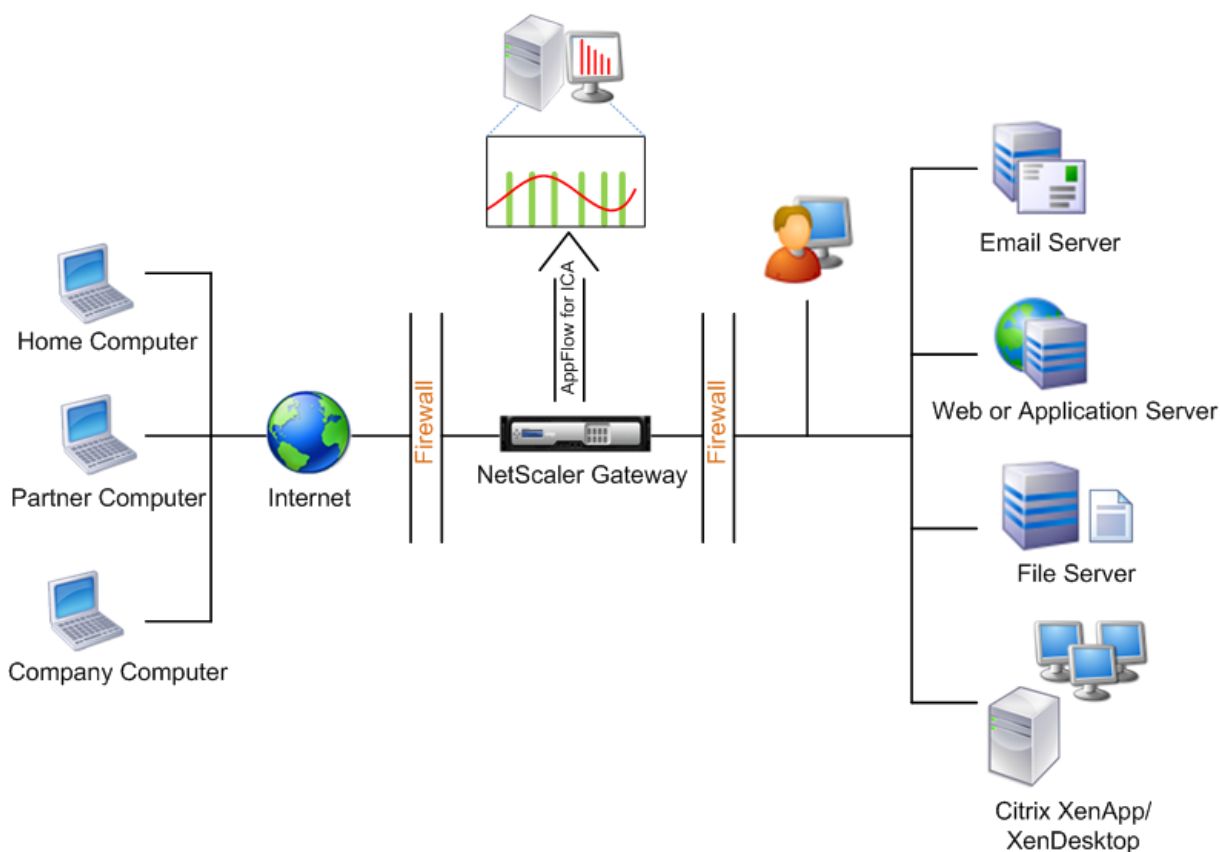
## Activer la collecte de données pour les appliances Citrix Gateway déployées en mode à saut unique

February 1, 2024

Lorsque vous déployez Citrix Gateway en mode à saut unique, il se trouve à la périphérie du réseau. L'instance Gateway fournit des connexions ICA proxy à l'infrastructure de mise à disposition des ordinateurs de bureau. Le déploiement à saut unique est le déploiement le plus simple et le plus courant. Le mode à saut unique assure la sécurité lorsqu'un utilisateur externe essaie d'accéder au réseau interne d'une organisation.

En mode saut unique, les utilisateurs accèdent aux appliances Citrix ADC via un réseau privé virtuel (VPN).

Pour commencer à collecter les rapports, vous devez ajouter l'appliance Citrix Gateway à l'inventaire Citrix Application Delivery Management (ADM) et activer AppFlow sur ADM.



### Pour activer la fonctionnalité AppFlow à partir d'ADM :

1. Dans un navigateur Web, tapez l'adresse IP du Citrix ADM (par exemple, <http://192.168.100.1>).
2. Dans **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'adminis-

trateur.

3. Accédez à **Infrastructure > Instances** , puis sélectionnez l'instance NetScaler pour laquelle vous souhaitez activer les analyses.
4. Dans la liste déroulante **Action**, sélectionnez **Activer ou désactiver les informations**.
5. Sélectionnez les **serveurs virtuels VPN**, puis cliquez sur **Activer AppFlow**.
6. Dans le champ **Activer AppFlow**, tapez **true** et sélectionnez **ICA**.
7. Cliquez sur **OK**.

**Remarque** Les commandes suivantes sont exécutées en arrière-plan lorsque vous activez AppFlow en mode single hop. Ces commandes sont explicitement spécifiées ici à des fins de dépannage.

- add appflow collector <name> -IPAddress <ip\_addr>
- add appflow action <name> -collectors <string>
- set appflow param -flowRecordInterval <secs>
- disable ns feature AppFlow
- enable ns feature AppFlow
- add appflow policy <name> <rule> <expression>
- set appflow policy <name> -rule <expression>
- bind vpn vserver <vsname> -policy <string> -type <type> >-priority <positive\_integer>
- set vpn vserver <name> -appflowLog ENABLED
- save ns config

Les données de canal virtuel EUEM font partie des données HDX Insight que Citrix ADM reçoit des instances de Gateway. Le canal virtuel EUEM fournit les données sur ICA RTT. Si le canal virtuel EUEM n'est pas activé, les données HDX Insight restantes sont toujours affichées sur Citrix ADM.

## Activez la collecte de données pour surveiller les ADC NetScaler déployés en mode transparent

February 1, 2024

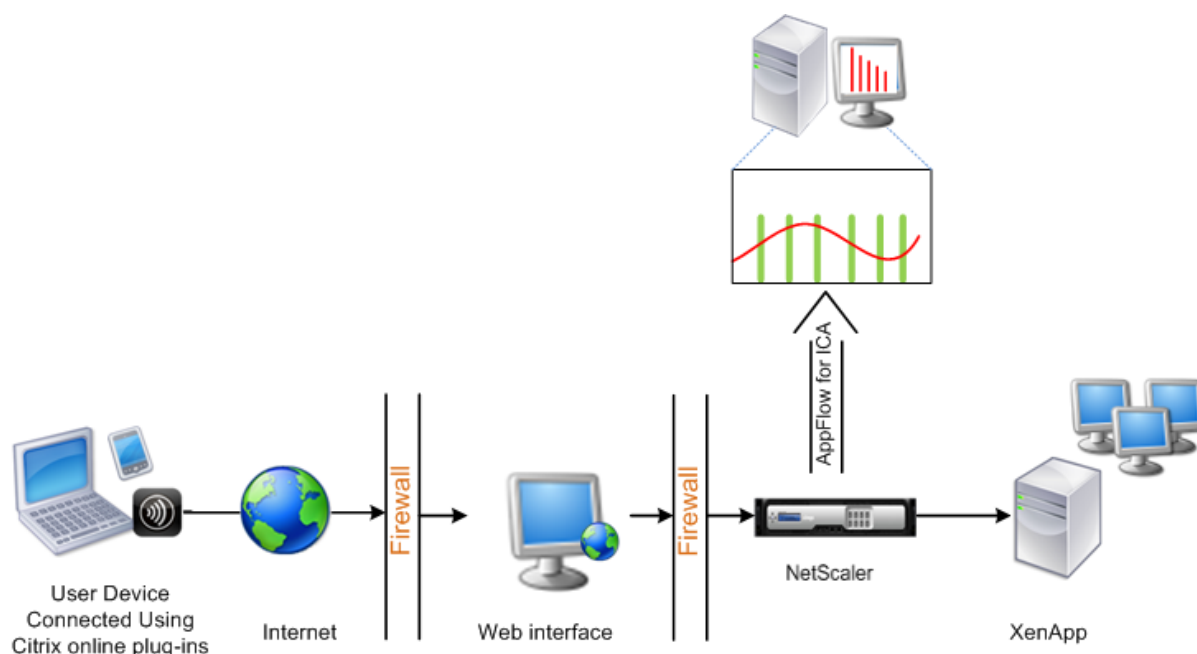
Lorsqu'un NetScaler ADC est déployé en mode transparent, les clients peuvent accéder directement aux serveurs, sans qu'aucun serveur virtuel n'intervienne. Si une appliance NetScaler est déployée en mode transparent dans un environnement Citrix Virtual Apps and Desktops, le trafic ICA n'est pas transmis via un VPN.

Après avoir ajouté Citrix ADC à l'inventaire Citrix ADM, vous devez activer AppFlow pour la collecte de données. L'activation de la collecte de données dépend du périphérique et du mode. Dans ce cas, vous devez ajouter Citrix ADM en tant que collecteur AppFlow sur chaque appliance NetScaler, et vous devez configurer une stratégie Appflow pour collecter tout le trafic ICA ou un trafic spécifique qui traverse l'appliance.

### Remarque

- Vous ne pouvez pas activer la collecte de données sur un NetScaler ADC déployé en mode transparent à l'aide de l'utilitaire de configuration Citrix ADM.
- Pour des informations détaillées sur les commandes et leur utilisation, consultez la section [Référence des commandes](#).
- Pour plus d'informations sur les expressions de stratégie, consultez la section [Politiques et expressions](#).

La figure suivante montre le déploiement réseau d'un Citrix ADM lorsqu'un NetScaler ADC 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.

```
1 set ns param --icaPorts \<port\>...
2 <!--NeedCopy-->
```

**Exemple :**

```
1 set ns param -icaPorts 2598 1494
2 <!--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 de flux d'applications sur l'appliance NetScaler.

```
1 add appflow collector <name> -IPAddress <ip_addr>
2 <!--NeedCopy-->
```

**Exemple :**

```
1 add appflow collector MyInsight -IPAddress 192.168.1.101
2 <!--NeedCopy-->
```

**Remarque** Pour afficher les collecteurs de flux d'applications configurés sur l'appliance NetScaler, utilisez la commande `show appflow collector`.

4. Créez une action Appflow et associez le collecteur à l'action.

```
1 add appflow action <name> -collectors <string> ...
2 <!--NeedCopy-->
```

**Exemple :**

```
1 add appflow action act -collectors MyInsight
2 <!--NeedCopy-->
```

5. Créez une stratégie Appflow pour spécifier la règle de génération du trafic.

```
1 add appflow policy <policyname> <rule> <action>
2 <!--NeedCopy-->
```

**Exemple :**

```
1 add appflow policy pol true act
2 <!--NeedCopy-->
```

6. Liez la stratégie appflow à un point de liaison global.

```
1 bind appflow global <polycname> <priority> -type <type>
2 <!--NeedCopy-->
```

**Exemple :**

```
1 bind appflow global pol 1 -type ICA_REQ_DEFAULT
2 <!--NeedCopy-->
```

**Remarque** La valeur du **type** doit être ICA\_REQ\_OVERRIDE ou ICA\_REQ\_DEFAULT afin de s'appliquer au trafic ICA.

7. Définissez la valeur du paramètre FlowRecordInterval pour Appflow sur 60 secondes.

```
1 set appflow param -flowRecordInterval 60
2 <!--NeedCopy-->
```

8. Enregistrez la configuration.

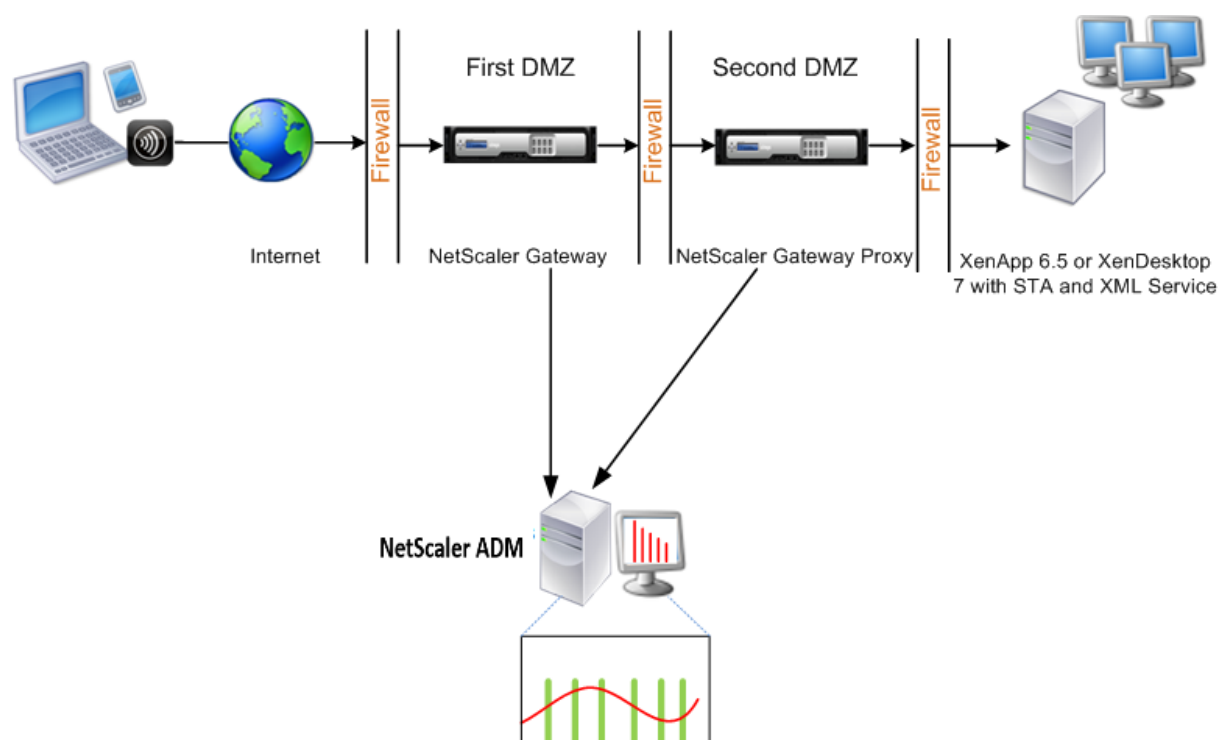
```
1 save ns config
2 <!--NeedCopy-->
```

## Activer la collecte de données pour les appliances Citrix Gateway déployées en mode double saut

February 1, 2024

Le mode double saut Citrix Gateway offre une protection supplémentaire au réseau interne d'une organisation car un attaquant doit pénétrer plusieurs zones de sécurité ou zones démilitarisées (DMZ) pour atteindre les serveurs du réseau sécurisé. Si vous souhaitez analyser le nombre de sauts (appliances Citrix Gateway) à travers lesquels les connexions ICA passent, ainsi que les détails sur la latence sur chaque connexion TCP et son rapport avec la latence ICA totale perçue par le client, vous devez installer Citrix ADM afin que les appliances Citrix Gateway rapportent ces statistiques de l'état civil.

Figure 3. Citrix ADM déployé en mode double saut



Citrix Gateway dans la première DMZ gère les connexions utilisateur et exécute les fonctions de sécurité d'un VPN SSL. Cette passerelle Citrix Gateway chiffre les connexions utilisateur, détermine comment les utilisateurs sont authentifiés et contrôle l'accès aux serveurs du réseau interne.

Citrix Gateway dans la deuxième DMZ sert de périphérique proxy Citrix Gateway. Cette passerelle Citrix Gateway permet au trafic ICA de traverser la deuxième zone démilitarisée pour terminer les connexions utilisateur à la batterie de serveurs.

Le Citrix ADM peut être déployé soit dans le sous-réseau appartenant à l'appliance Citrix Gateway dans la première zone démilitarisée, soit dans le sous-réseau appartenant à la seconde zone démilitarisée de l'appliance Citrix Gateway. Dans l'image ci-dessus, Citrix ADM et Citrix Gateway de la première DMZ sont déployés dans le même sous-réseau.

En mode double saut, Citrix ADM collecte les enregistrements TCP d'une appliance et les enregistrements ICA de l'autre appliance. Une fois que vous avez ajouté les appliances Citrix Gateway à l'inventaire Citrix ADM et activé la collecte de données, chacune des appliances exporte les rapports en suivant le nombre de sauts et l'ID de chaîne de connexion.

Pour que Citrix ADM identifie l'appliance qui exporte des enregistrements, chaque appliance est spécifiée avec un nombre de sauts et chaque connexion est spécifiée avec un ID de chaîne de connexion. Le nombre de sauts représente le nombre d'appliances Citrix Gateway via lesquelles le trafic circule d'un client vers les serveurs. L'ID de chaîne de connexion représente les connexions de bout en bout entre le client et le serveur.

Citrix ADM utilise le nombre de sauts et l'ID de chaîne de connexion pour corréliser les données des

appliances Citrix Gateway et générer les rapports.

Pour surveiller les appliances Citrix Gateway déployées dans ce mode, vous devez d'abord ajouter Citrix Gateway à l'inventaire Citrix ADM, activer AppFlow sur Citrix ADM, puis consulter les rapports sur le tableau de bord Citrix ADM.

### Activation de la collecte de données sur Citrix ADM

Si vous activez Citrix ADM pour commencer à collecter les détails ICA à partir des deux appliances, les détails collectés sont redondants. Il s'agit des deux appliances qui signalent les mêmes mesures. Pour remédier à cette situation, vous devez activer AppFlow pour TCP sur l'un des premiers dispositifs Citrix Gateway, puis activer AppFlow pour ICA sur le second dispositif. Ce faisant, l'une des appliances exporte les enregistrements ICA AppFlow et l'autre appliance exporte les enregistrements TCP AppFlow. Cela permet également d'économiser le temps de traitement lors de l'analyse du trafic ICA.

#### Pour activer la fonctionnalité AppFlow à partir de Citrix ADM :

1. Accédez à **Infrastructure** > **Instances** , puis sélectionnez l'instance NetScaler pour laquelle vous souhaitez activer les analyses.
2. Dans la liste déroulante **Action**, sélectionnez **Activer ou désactiver les informations**.
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 et 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 Citrix ADM n'affiche pas les enregistrements, même si la colonne Insight indique Activé.

5. Cliquez sur **OK**.

### Configuration des appliances Citrix Gateway pour exporter des données

Après avoir installé les appliances Citrix Gateway, vous devez configurer les paramètres suivants sur les appliances Citrix Gateway pour exporter les rapports vers Citrix ADM :

- Configurez les serveurs virtuels des appliances Citrix Gateway dans la première et la deuxième zone démilitarisée pour communiquer entre eux.
- Liez le serveur virtuel Citrix Gateway dans la deuxième zone DMZ au serveur virtuel Citrix Gateway dans la première zone DMZ.
- Activez le double saut sur Citrix Gateway dans la deuxième DMZ.

- Désactivez l'authentification sur le serveur virtuel Citrix Gateway dans la deuxième DMZ.
- Permettre à l'une des appliances Citrix Gateway d'exporter des enregistrements ICA
- Activez l'autre appliance Citrix Gateway pour exporter des enregistrements TCP :
- Activez le chaînage des connexions sur les deux appliances Citrix Gateway.

### Configuration de Citrix Gateway à l'aide de l'interface de ligne de commande :

1. Configurez le serveur virtuel Citrix Gateway dans la première zone DMZ pour qu'il communique avec le serveur virtuel Citrix Gateway dans la deuxième zone DMZ.

---

**add vpn nextHopServer** [**\*\*-secure\*\***(ON OFF)] [**-imgGifToPng**] ...

---

```
1 add vpn nextHopServer nh1 10.102.2.33 8443 -secure ON
2 <!--NeedCopy-->
```

2. Liez le serveur virtuel Citrix Gateway dans la deuxième zone DMZ au serveur virtuel Citrix Gateway dans la première zone DMZ. Exécutez la commande suivante sur Citrix Gateway dans la première DMZ :

**bind vpn vsrver** <name> **-nextHopServer** <name>

```
1 bind vpn vsrver vs1 -nextHopServer nh1
2 <!--NeedCopy-->
```

3. Activez le double saut et AppFlow sur Citrix Gateway dans la deuxième DMZ.

---

**set vpn vsrver** (DISABLED) [**- appflowLog** (DISABLED)]  
**vsrver** [**\*\*- doubleHop\*\*** (ENABLED ENABLED)]

---

```
1 set vpn vsrver vpnhop2 -doubleHop ENABLED -appFlowLog ENABLED
2 <!--NeedCopy-->
```

4. Désactivez l'authentification sur le serveur virtuel Citrix Gateway dans la deuxième DMZ.

---

**set vpn vsrver** [**\*\*-authentication\*\*** (ON OFF)]

---

```
1 set vpn vsrver vs -authentication OFF
2 <!--NeedCopy-->
```

5. Activez l'une des appliances Citrix Gateway pour exporter des enregistrements TCP.

**bind vpn vsrver**<name> [**-policy**<string> **-priority**<positive\_integer>] [**-type**<type>]



```

1 bind vpn vserver vpn1 -policy appflowpol1 -priority 101 -type
  OTHERTCP_REQUEST
2 <!--NeedCopy-->

```

6. Activez l'autre appliance Citrix Gateway pour exporter des enregistrements ICA :

**bind vpn vserver**<name> [-**policy**<string> -**priority**<positive\_integer>] [-**type**<type>]

```

1 bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
  ICA_REQUEST
2 <!--NeedCopy-->

```

7. Activez le chaînage des connexions sur les deux appliances Citrix Gateway :

---

**set appFlow** DISABLED)]  
**param** [-**connectionChaining** (ENABLED

---

```

1 set appflow param -connectionChaining ENABLED
2 <!--NeedCopy-->

```

### Configuration de Citrix Gateway à l'aide de l'utilitaire de configuration :

1. Configurez Citrix Gateway dans la première DMZ pour communiquer avec Citrix Gateway dans la deuxième DMZ et lier Citrix Gateway dans la deuxième DMZ à Citrix Gateway dans la première DMZ.
  - a) Dans l'onglet **Configuration**, développez **Citrix Gateway** et cliquez sur **Serveurs virtuels**.
  - b) Dans le volet droit, double-cliquez sur le serveur virtuel et dans le groupe Avancé, développez **Applications publiées**.
  - c) Cliquez sur **Serveur de saut suivant** et liez un serveur de saut suivant au deuxième dispositif Citrix Gateway.
2. Activez le double saut sur Citrix Gateway dans la deuxième DMZ.
  - a) Sous l'onglet **Configuration**, développez **Citrix Gateway** et cliquez sur **Serveurs virtuels**.
  - b) Dans le volet droit, double-cliquez sur le serveur virtuel, puis dans le groupe **Paramètres de base**, cliquez sur l'icône de modification.
  - c) Développez **Plus**, sélectionnez **Double saut** et cliquez sur **OK**.
3. Désactivez l'authentification sur le serveur virtuel sur Citrix Gateway dans la deuxième zone démilitarisée.
  - a) Dans l'onglet **Configuration**, développez **Citrix Gateway** et cliquez sur **Virtual Servers**.

- b) Dans le volet droit, double-cliquez sur le serveur virtuel, puis dans le groupe **Paramètres de base**, cliquez sur l'icône Modifier.
  - c) Développez **Plus** et décochez **Activer l'authentification**.
4. Activez l'une des appliances Citrix Gateway pour exporter des enregistrements TCP.
  - a) Dans l'onglet **Configuration**, développez **Citrix Gateway** et cliquez sur **Virtual Servers**.
  - b) Dans le volet droit, double-cliquez sur le serveur virtuel et dans le groupe **Avancé**, développez **Stratégies**.
  - c) Cliquez sur l'icône + et dans la liste **Choose Policy**, sélectionnez **AppFlow** et dans la liste **Choose Type**, sélectionnez **Other TCP Request**.
  - d) Cliquez sur **Continuer**.
  - e) Ajoutez une liaison de stratégie, puis cliquez sur **Fermer**.
5. Activez l'autre appliance Citrix Gateway pour exporter des enregistrements ICA :
  - a) Dans l'onglet **Configuration**, développez **Citrix Gateway** et cliquez sur **Virtual Servers**.
  - b) Dans le volet droit, double-cliquez sur le serveur virtuel et, dans le groupe **Avancé**, développez **Stratégies**.
  - c) Cliquez sur l'icône + et dans la liste déroulante **Choisir une stratégie**, sélectionnez **AppFlow** et dans la liste **Choisir un type**, sélectionnez **Autre demande TCP**.
  - d) Cliquez sur **Continuer**.
  - e) Ajoutez une liaison de stratégie, puis cliquez sur **Fermer**.
6. Activez le chaînage des connexions sur les deux appliances Citrix Gateway.
  - a) Sous l'onglet **Configuration**, accédez à **Système > Appflow**.
  - b) Dans le volet droit, dans le groupe **Paramètres**, cliquez sur **Modifier les paramètres de flux d'applications**.
  - c) Select **Chaîne de connexion** et cliquez sur **OK**.

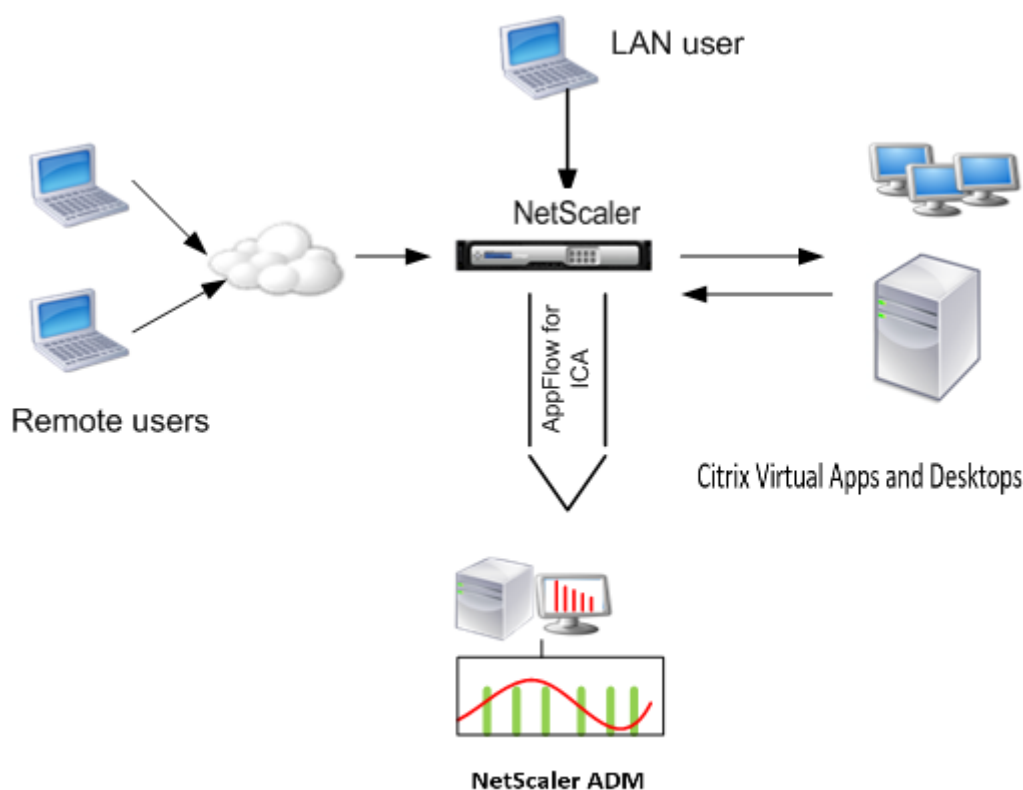
## Activez la collecte de données pour surveiller les ADC NetScaler déployés en mode utilisateur LAN

February 1, 2024

Les utilisateurs externes qui accèdent aux applications Citrix Virtual Apps and Desktops doivent s'authentifier sur Citrix Gateway. Toutefois, les utilisateurs internes peuvent ne pas avoir besoin d'être redirigés vers Citrix 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 de cache, qui agit comme un proxy SOCKS sur l'appliance Citrix Gateway.

Figure 4. Citrix ADM déployé en mode utilisateur LAN



### Remarque

L'appliance Citrix ADM et Citrix Gateway résident dans le même sous-réseau.

Pour surveiller les appliances Citrix déployées dans ce mode, ajoutez d'abord l'appliance Citrix à l'inventaire NetScaler Insight, activez AppFlow, puis consultez les rapports sur le tableau de bord.

Après avoir ajouté l'appliance Citrix à l'inventaire Citrix ADM, vous devez activer AppFlow pour la collecte de données.

**Remarque**

- Vous ne pouvez pas activer la collecte de données sur un NetScaler ADC déployé en mode utilisateur LAN à l'aide de l'utilitaire de configuration Citrix ADM.
- Pour des informations détaillées sur les commandes et leur utilisation, consultez la section Référence des commandes .
- Pour plus d'informations sur les expressions de stratégie, voir Stratégies et expressions .

**Pour configurer la collecte de données sur 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.

```
1 add cr vserver <name> <servicetype> [<ipaddress> <port>] [-
  cacheType <cachetype>] [ - cltTimeout <secs>]
2 <!--NeedCopy-->
```

**Exemple :**

```
1 add cr vserver cr1 HDX 10.12.2.2 443 - cacheType FORWARD -
  cltTimeout 180
2 <!--NeedCopy-->
```

**Remarque** Si vous accédez au réseau LAN à l'aide d'une appliance Citrix Gateway, ajoutez une action à appliquer par une stratégie correspondant au trafic VPN.

```
1 add vpn trafficAction** \<name> \<qual> \[-HDX ( ON | OFF )\]
2
3 add vpn trafficPolicy** \<name> \<rule> \<action>
4 <!--NeedCopy-->
```

**Exemple :**

```
1 add vpn trafficAction act1 tcp -HDX ON
2
3 add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
4 <!--NeedCopy-->
```

3. Ajoutez Citrix ADM en tant que collecteur d'applications sur l'appliance Citrix ADC.

```
1 add appflow collector** \<name> \*\*-IPAddress\*\* \\<ip\\_addr
  \\>
2 <!--NeedCopy-->
```

**Exemple :**

```
1 add appflow collector MyInsight -IPAddress 192.168.1.101
2 <!--NeedCopy-->
```

4. Créez une action Appflow et associez le collecteur à l'action.

```
1 add appflow action** \<name\> \*\*-collectors\*\* \<string\> ...
2 <!--NeedCopy-->
```

**Exemple :**

```
1 add appflow action act -collectors MyInsight
2 <!--NeedCopy-->
```

5. Créez une stratégie Appflow pour spécifier la règle de génération du trafic.

```
1 add appflow policy** \<polycyname\> \<rule\> \<action\>
2 <!--NeedCopy-->
```

**Exemple :**

```
1 add appflow policy pol true act
2 <!--NeedCopy-->
```

6. Liez la stratégie appflow à un point de liaison global.

```
1 bind appflow global** \<polycyname\> \<priority\> \*\*-type\*\* \<
  type\>
2 <!--NeedCopy-->
```

**Exemple :**

```
1 bind appflow global pol 1 -type ICA_REQ_DEFAULT
2 <!--NeedCopy-->
```

**Remarque** La valeur du type doit être ICA\_REQ\_OVERRIDE ou ICA\_REQ\_DEFAULT afin de s'appliquer au trafic ICA.

7. Définissez la valeur du paramètre FlowRecordInterval pour Appflow sur 60 secondes.

```
1 set appflow param -flowRecordInterval 60
2 <!--NeedCopy-->
```

**Exemple :**

```
1 set appflow param -flowRecordInterval 60
2 <!--NeedCopy-->
```

8. Enregistrez la configuration.
-

```
1 save ns config
2 <!--NeedCopy-->
```

## Créer des seuils et configurer des alertes pour HDX Insight

February 1, 2024

HDX Insight on Citrix Application Delivery Management (ADM) vous permet de surveiller le trafic HDX transitant par les instances Citrix ADC. Citrix ADM vous permet de définir des seuils sur différents compteurs utilisés pour surveiller le trafic Insight. Vous pouvez également configurer des règles et créer des alertes dans Citrix ADM.

Le type de trafic HDX est associé à diverses entités telles que les applications, les postes de travail, les passerelles, les licences et les utilisateurs. Chaque entité peut contenir différentes mesures qui leur sont associées. Par exemple, l'entité d'application est associée à un certain nombre d'accès, à la bande passante consommée par l'application et au temps de réponse du serveur. Une entité utilisateur peut être associée à la latence WAN, à la latence DC, à la RTT ICA et à la bande passante consommée par un utilisateur.

La gestion des seuils pour HDX Insight dans Citrix ADM vous a permis de créer des règles de manière proactive et de configurer des alertes chaque fois que les seuils définis sont dépassés. Cette gestion des seuils est désormais étendue pour configurer un groupe de règles de seuil. Vous pouvez désormais surveiller le groupe au lieu de suivre des règles individuelles. Un groupe de règles de seuil comprend une ou plusieurs règles de seuil définies par l'utilisateur pour des mesures choisies parmi des entités telles que des utilisateurs, des applications et des postes de travail. Chaque règle est surveillée par rapport à une valeur attendue que vous entrez lors de la création de la règle. Dans le cas d'une entité utilisateur, le groupe de seuil peut également être associé à une géolocalisation.

Une alerte est générée sur Citrix ADM uniquement si toutes les règles du groupe de seuils configuré sont violées. Par exemple, vous pouvez surveiller une application en fonction du nombre total de lancements de sessions et également du nombre de lancements d'applications sous la forme d'un groupe de seuil. Une alerte est générée uniquement si les deux règles ne sont pas respectées. Cela vous permet de définir des seuils plus réalistes pour une entité.

Voici quelques exemples :

- Règle de seuil 1 : le RTT ICA (métrique) pour les utilisateurs (entité) doit être  $\leq 100$  ms
- Règle de seuil 2 : la latence WAN (métrique) pour les utilisateurs (entité) doit être  $\leq 100$  ms

Un exemple de groupe de seuil peut être : {Règle de seuil 1 + Règle de seuil 2}

Pour créer une règle, vous devez d'abord sélectionner l'entité que vous souhaitez surveiller. Choisissez ensuite une mesure lors de la création d'une règle. Par exemple, vous pouvez sélectionner l'entité d'applications, puis sélectionner Nombre total de lancement de session ou Nombre de lancement d'applications. Vous pouvez créer une règle pour chaque combinaison d'une entité et d'une métrique. Utilisez les comparateurs fournis (>, <, >= et <=) et saisissez une valeur seuil pour chaque métrique.

### Remarque

Si vous ne souhaitez pas surveiller plusieurs entités au sein d'un même groupe, vous devez créer un groupe de règles de seuil distinct pour chaque entité.

Lorsque la valeur d'un compteur dépasse la valeur d'un seuil, Citrix ADM génère un événement pour signaler un dépassement de seuil, et une alerte est créée pour chaque événement.

Vous devez configurer la façon dont vous recevez l'alerte. Vous pouvez activer l'affichage de l'alerte sur Citrix ADM et/ou recevoir l'alerte par e-mail ou par SMS sur votre appareil mobile. Pour les deux dernières actions, vous devez configurer le serveur de messagerie ou le serveur SMS sur Citrix ADM.

Les groupes de seuils peuvent également être liés aux géolocalisations pour la surveillance géographique spécifique de l'entité utilisateur.

## Exemples de cas d'utilisation

ABC Inc. est une entreprise mondiale qui a des bureaux dans plus de 50 pays. L'entreprise dispose de deux centres de données, l'un à Singapour et l'autre en Californie qui hébergent Citrix Virtual Apps and Desktops. Les employés de l'entreprise accèdent aux Citrix Virtual Apps and Desktops dans le monde entier à l'aide de Citrix Gateway et de la redirection basée sur Citrix GSLB. Eric, administrateur Citrix Virtual Apps and Desktops d'ABC Inc., souhaite suivre l'expérience utilisateur dans tous ses bureaux afin d'optimiser la diffusion des applications et des ordinateurs de bureau pour un accès en tout lieu et à tout moment. 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 ICA pour un emplacement proche du centre de données peut être de 5 à 10 ms, tandis que le même pour un emplacement distant peut être 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 spécifiques à la zone géographique pour chaque emplacement et être alerté par e-mail ou par SMS en cas de violation par zone. Eric est également capable de combiner le suivi de plusieurs mesures au sein d'un groupe de règles de seuil et de limiter la cause profonde aux problèmes de capacité, le cas échéant. Eric est désormais en mesure de suivre de manière proactive tout écart

sans avoir à se soucier de la complexité de la recherche manuelle à travers toutes les mesures du portefeuille Citrix Virtual Apps and Desktops.

**Pour créer un groupe de règles de seuil et configurer des alertes pour HDX Insight à l'aide de Citrix ADM :**

1. Dans Citrix ADM, accédez à **Analytics > Paramètres > Seuils**. Dans la page **Seuils** qui s'ouvre, cliquez sur **Ajouter**.
2. Sur la page **Créer des seuils et des alertes**, spécifiez les informations suivantes :
  - a) **Nom**. Entrez un nom pour créer un événement pour lequel Citrix ADM génère une alerte.
  - b) **Type de trafic**. Dans la liste déroulante, sélectionnez HDX.
  - c) **Entité**. Dans la liste déroulante, 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 liste déroulante, 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.

The screenshot shows a 'Create Threshold' form with the following fields and values:

- Name\***: ABC-users
- Traffic Type\***: HDX
- Entity\***: Users
- Reference Key**: UserName
- Duration\***: Day

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.



### Add Rules

Metric\*

ICA RTT (seconds)
▼
?

Comparator\*

>
▼
?

Value\*

500
?

OK

Close

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.

**Configure Rule**

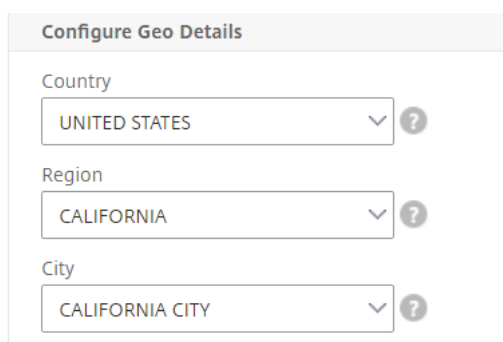
Add Rule

Delete

■	Metric
<input type="checkbox"/>	ICA RTT (seconds) > 500
<input type="checkbox"/>	WAN latency (ms) > 100

#### 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.



**Configure Geo Details**

Country  
UNITED STATES

Region  
CALIFORNIA

City  
CALIFORNIA CITY

5. Cliquez sur **Activer les seuils** pour permettre à Citrix ADM de commencer à surveiller les entités.
6. Vous pouvez également configurer des actions telles que les notifications par e-mail et les notifications par SMS.
7. Cliquez sur **Créer** pour créer un groupe de règles de seuil.

## Affichage des rapports et des mesures HDX Insight

February 1, 2024

HDX insights fournit une visibilité complète des rapports et des mesures relatifs au trafic HDX sur vos instances Citrix ADC.

Vous pouvez afficher les métriques HDX de n'importe quelle entité sélectionnée. Les vues comprennent les catégories d'entités suivantes :

- **Utilisateurs** : affiche les rapports de tous les utilisateurs accédant aux Citrix Virtual Apps and Desktops 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 Citrix ADC qui agissent comme des passerelles pour le trafic entrant.
- **Bureaux** : affiche les rapports des bureaux utilisés dans la période sélectionnée.
- **Licences** : affiche les rapports pour le nombre total de licences VPN SSL utilisées dans le créneau horaire spécifié.

### Remarque

La valeur Licences ne s'applique pas aux appliances Citrix SD-WAN.

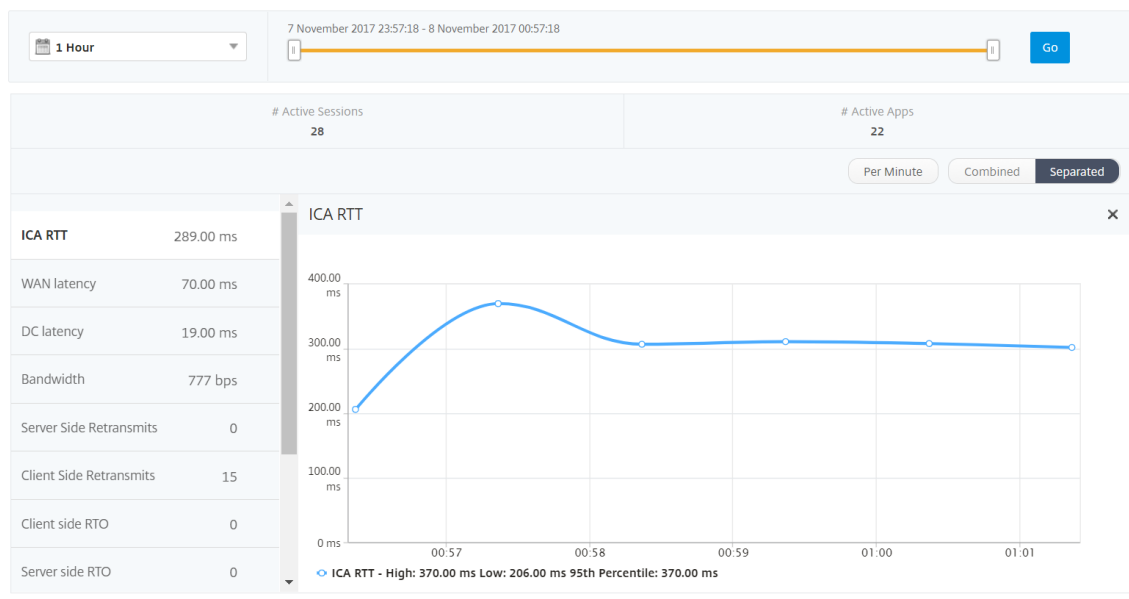
## Rapports et mesures de la vue utilisateur

06 nov. 2017

Les rapports et les mesures de cette vue sont affichés par utilisateur de Citrix Virtual Apps and Desktops.

### Pour accéder à la vue Utilisateurs :

1. Connectez-vous à votre Citrix ADM à l'aide d'un navigateur Web pris en charge.
2. Accédez à **Analytics > HDX Insight > Utilisateurs**



Les rapports et mesures de la vue utilisateur comprennent les sections suivantes :

- Vue récapitulative
- Par vue utilisateur
- Vue par session utilisateur

### Vue récapitulative

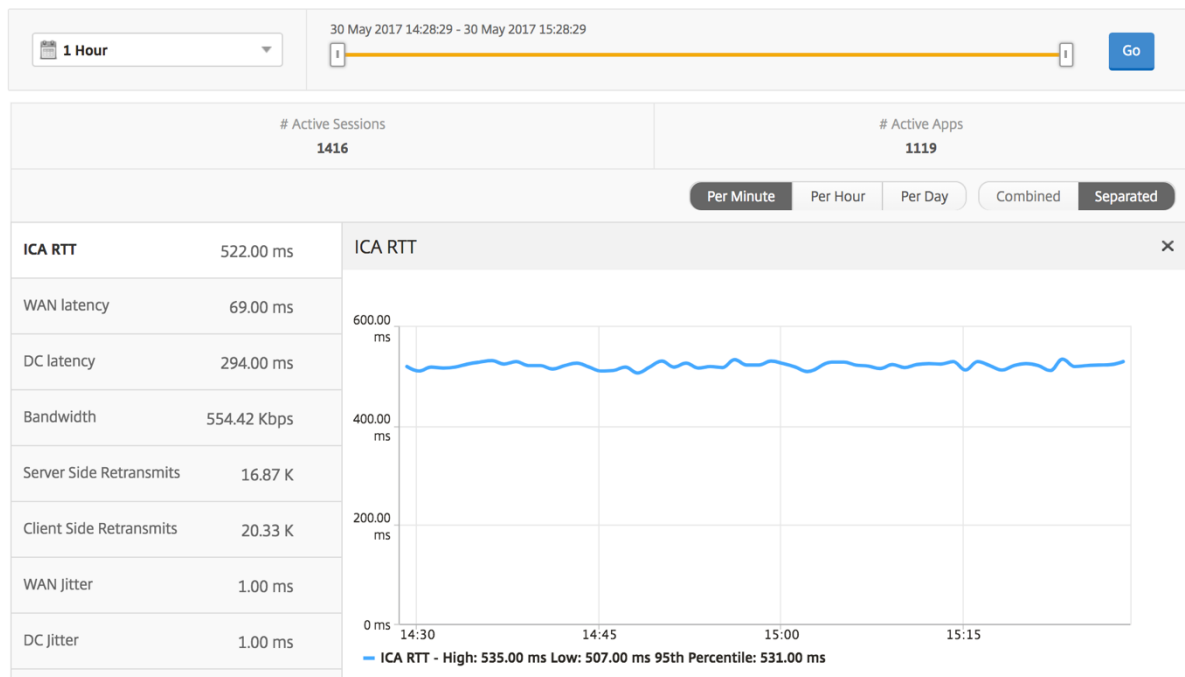
La vue récapitulative affiche les rapports de tous les utilisateurs qui se sont connectés au cours de la chronologie sélectionnée. Toutes les métriques/rapports de cette vue affichent les valeurs qui leur correspondent pour la période sélectionnée, sauf indication contraire.

### 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 and Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre Citrix Gateway et les serveurs VDI, CVAD ou StoreFront.
Bande passante	Nombre total d'octets par seconde pris pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de la retransmission s'est produit sur la connexion entre Citrix ADC et le serveur principal.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.



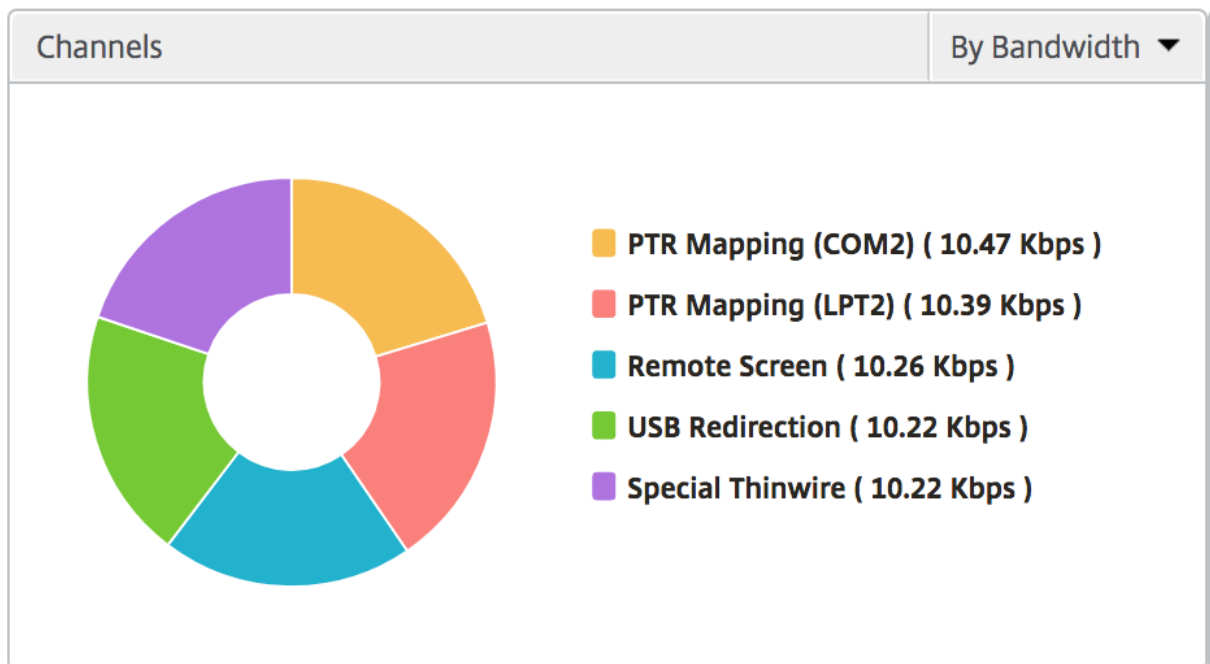
**Rapport User Summary** Voici les mesures spécifiques à ce rapport.

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 and Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre Citrix Gateway et les serveurs VDI, CVAD ou StoreFront.
Bande passante	Nombre total d'octets par seconde pris pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et le serveur principal.

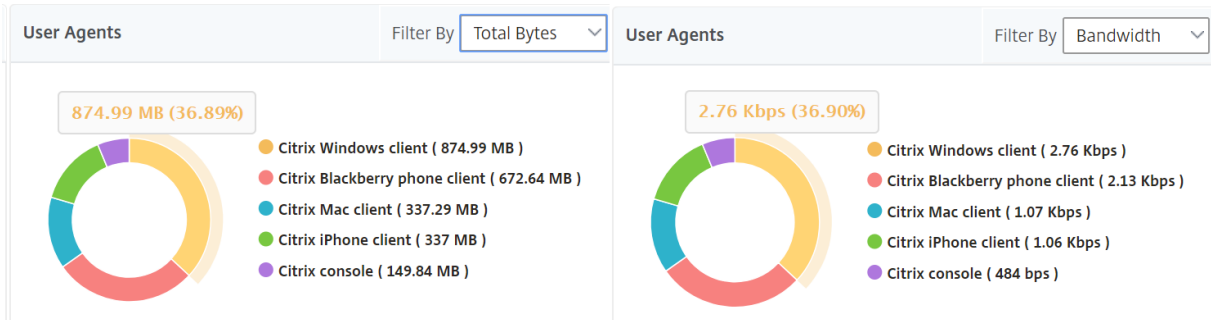
Mesures	Description
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de la retransmission s'est produit sur la connexion entre Citrix ADC et le serveur principal.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.
Nb total d'applications lancées	Total des applications lancées par l'utilisateur au cours de la période sélectionnée.
Nb total d'octets	Nombre total d'octets consommés par l'utilisateur pendant la période sélectionnée.
Ordinateurs de bureau actifs	Nombre total de Citrix Virtual Desktops actifs au cours d'un intervalle de temps donné.

Users									
User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT	WAN latency	DC latency	Bandwidth	Server Side Retransmits	Client Side Retransmits
liam	59	59	118	999.00 ms	57.00 ms	751.00 ms	47.25 Kbps	3.74 K	0
jayden	59	59	118	999.00 ms	52.00 ms	751.00 ms	47.06 Kbps	3.71 K	0
florinl	59	0	59	997.00 ms	52.00 ms	754.00 ms	23.66 Kbps	1.88 K	0
ramas	59	0	59	997.00 ms	778.00 ms	1.00 ms	7.03 Kbps	0	0
omerp	59	0	59	997.00 ms	57.00 ms	754.00 ms	23.80 Kbps	1.89 K	0
grahmm	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.80 Kbps	1.89 K	0
ryan	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.69 Kbps	1.88 K	0
rajivs	59	0	59	801.00 ms	11.00 ms	1.00 ms	23.97 Kbps	0	0
alexisc	117	0	118	622.00 ms	56.00 ms	392.00 ms	47.67 Kbps	1.88 K	0
juan	59	59	118	169.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	0
lennoxl	59	0	59	169.00 ms	31.00 ms	30.00 ms	23.86 Kbps	0	0
daniel	59	59	118	149.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	0
woojunek	58	0	59	149.00 ms	31.00 ms	30.00 ms	23.85 Kbps	0	0
parkerf	59	0	59	149.00 ms	31.00 ms	30.00 ms	23.88 Kbps	0	0
randybr	59	59	118	99.00 ms	11.00 ms	29.00 ms	47.71 Kbps	0	0
bradp	177	0	177	74.00 ms	27.00 ms	1.00 ms	71.75 Kbps	0	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 utilisateur** Les agents utilisateurs représentent la bande passante globale/nombre total d’octets consommés par chaque client récepteur sous la forme d’un graphique en donut. Chaque segment coloré du graphique représente un client destinataire. La longueur du segment dépend du nombre d’utilisateurs qui lancent leurs applications sur ce client récepteur. Vous pouvez également trier les mesures par bande passante ou par nombre total d’octets.



Cliquez sur chaque segment pour afficher les détails des utilisateurs utilisant ce client récepteur.

User Details 🔄

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 de seuils** Les mesures de nombre de violations des seuils représentent le nombre de seuils violés au cours de la période sélectionnée.

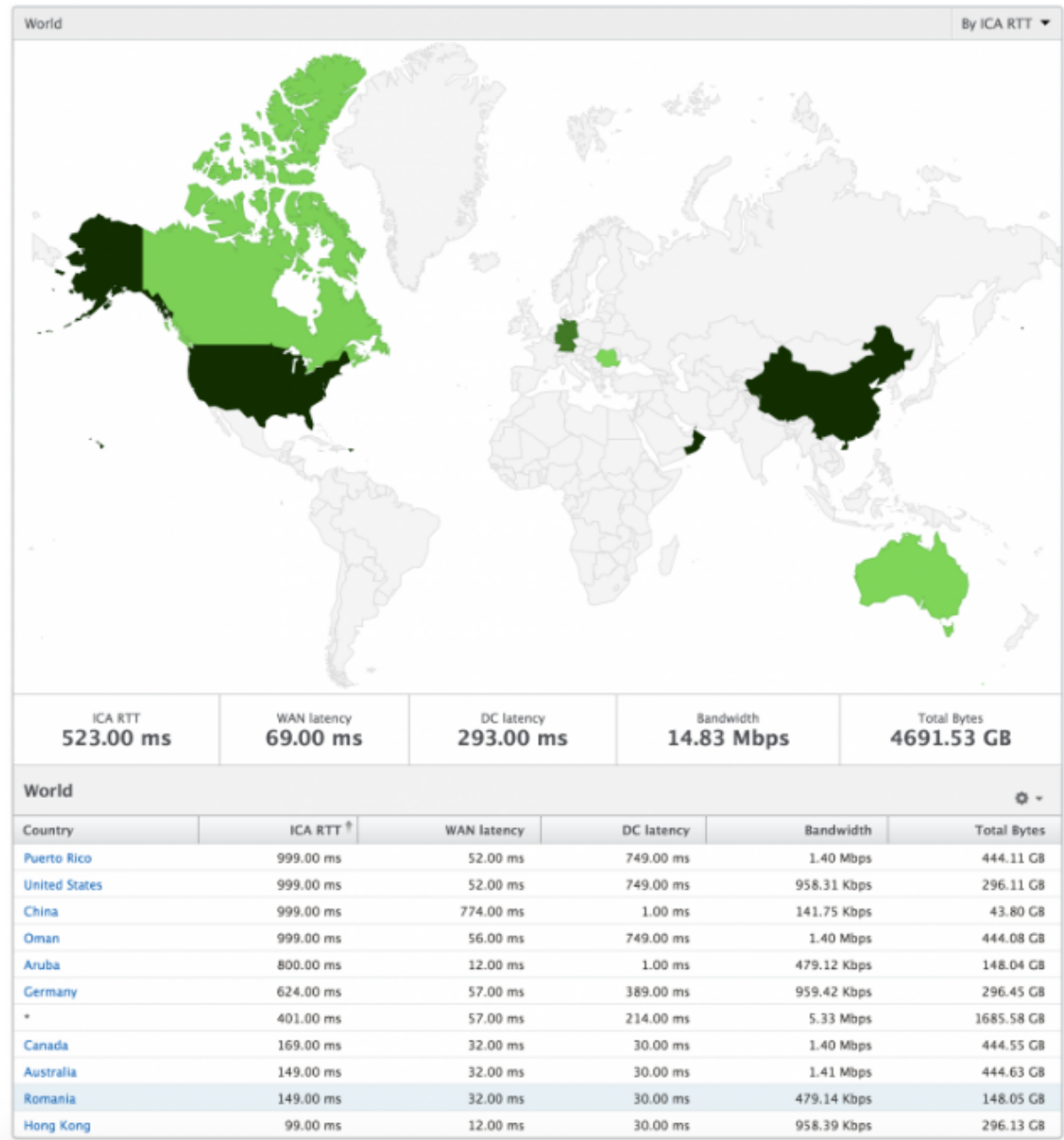
**Carte du monde** La vue Carte du monde dans HDX insights permet aux administrateurs de visualiser les détails des utilisateurs historiques et actifs d’un point de vue géographique. Les administrateurs peuvent avoir une vue du monde du système, une exploration vers un pays particulier et plus loin dans les villes ainsi qu’en cliquant sur la région. Les administrateurs peuvent approfondir l’exploration vers le bas pour afficher les informations par ville et par État. À partir de Citrix ADM version 12.0 et ultérieure, vous pouvez effectuer une exploration vers le bas vers les utilisateurs connectés à partir d’un emplacement géographique.

Les détails suivants peuvent être consultés sur la carte du monde dans un aperçu HDX, et la densité de chaque mesure est affichée sous la forme d’une carte thermique :

- RTT ICA
- Latence WAN
- Latence DC
- Bande passante



- Nb total d'octets



### Vue par utilisateur

La vue par utilisateur fournit des rapports détaillés sur l'expérience utilisateur final pour un utilisateur sélectionné particulier.

#### Pour accéder aux mesures spécifiques d'un utilisateur :

1. Connectez-vous à votre Citrix ADM à l'aide d'un navigateur Web pris en charge.

2. Accédez à **Analytics > HDX Insight > Utilisateurs**.
3. Sélectionnez un utilisateur particulier dans le rapport récapitulatif Utilisateurs.

**Graphique linéaire** Le graphique en courbes affiche le résumé de toutes les mesures pour l'utilisateur sélectionné particulier pendant la période sélectionnée.

**Rapport Sessions en cours/terminées** Ce rapport est pertinent pour toutes les sessions utilisateur en cours/terminées pour l'utilisateur sélectionné. Ces mesures peuvent être triées par heure de début, reconnections de session et nombre d'ACR.

---

Métriques	Description
ID de session	Une identité unique pour une session ICA.
Type de session	Application/Bureau.
État	Vert/rouge pour les sessions actives/inactives.
Délai d'hôte	Délai moyen du trafic ICA transitant par les Citrix ADC causé par le réseau du serveur.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Bande passante de session	La bande passante consommée par la session quel que soit l'intervalle de temps.
Octets par intervalle	Nombre d'octets consommés par la session pendant cet intervalle de temps particulier.
Start Time	Heure de début de la session.
Temps d'activité	Durée de la session.
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 récepteur - Client Windows Citrix
Version du client	Version du Receiver.
MSI	Boolean (Oui/Non). Indique si la session est mult flux ICA.
Reconnections 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.
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, le mode utilisateur/transparent de Citrix Gateway.
Pays	Pays à partir duquel la session a été créée.
Région	Région à partir de laquelle la session a été créée.
City	Ville à partir de laquelle la session a été créée.
État de l'USB	Actif/Inactif -Vert/Rouge.
Nombre d'instances USB acceptées	Le nombre d'instances USB acceptées.
Nombre d'instances USB rejetées	Le nombre d'instances USB rejetées.
Nombre d'instances USB arrêtées	Le nombre d'instances USB arrêtées.
Nom d'hôte du client	Le nom d'hôte du client.
Nombre de basculements HA	Nombre de fois où le basculement HA s'est produit.
Motif de la résiliation	Affiche la raison de l'arrêt d'une session. Par exemple, délai d'expiration de session ICA, session terminée par l'utilisateur.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre Citrix Gateway et les serveurs VDI, CVAD ou StoreFront.
Nb total d'octets	Nombre total d'octets consommés par l'utilisateur pendant la période sélectionnée.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et le serveur principal.

---

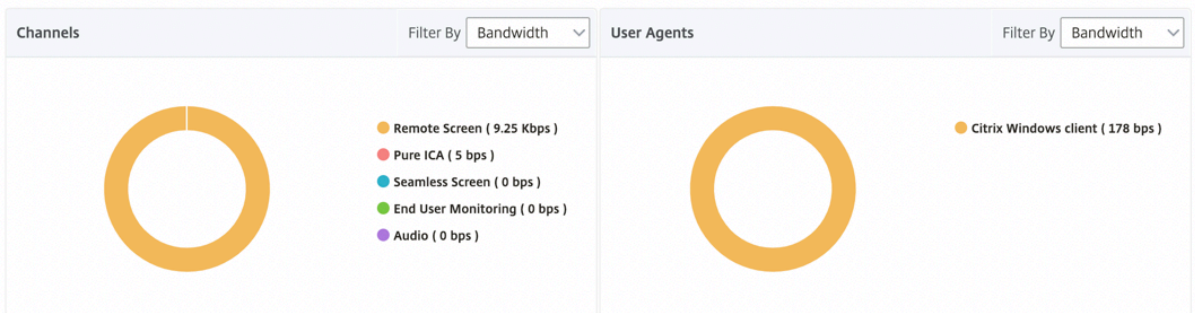
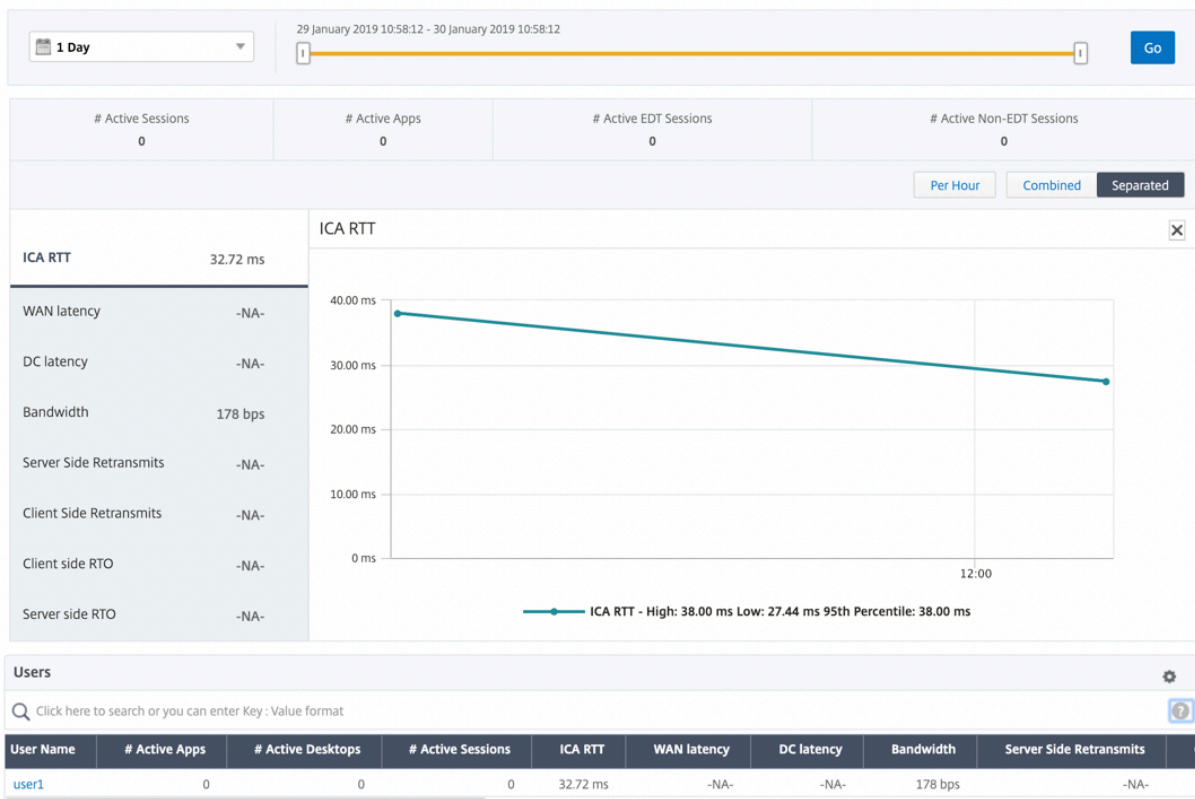
Métriques	Description
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de la retransmission s'est produit sur la connexion entre Citrix ADC et le serveur principal.

---

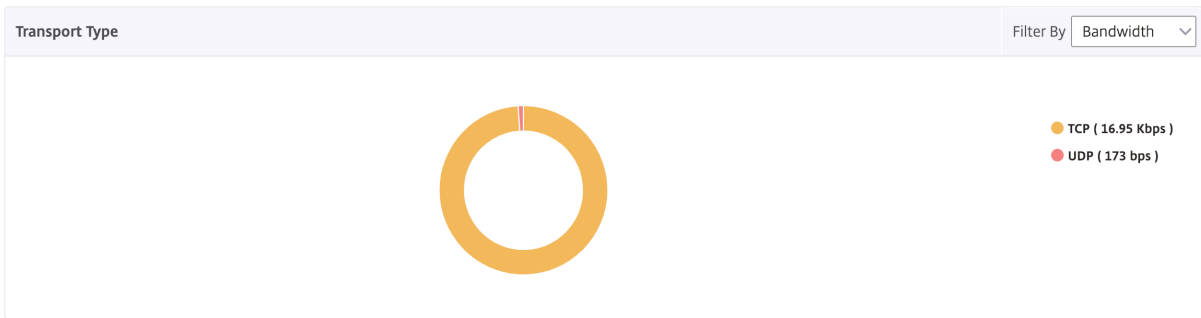
### **Prise en charge de l'EDT dans HDX Insight**

Citrix Application Delivery Management (ADM) prend désormais en charge le transport de données éclairé (EDT) pour afficher les analyses pour HDX Insight. En d'autres termes, ADM prend désormais en charge les protocoles UDP et TCP. La prise en charge d'EDT pour Citrix Gateway garantit une expérience utilisateur haute définition en session des bureaux virtuels pour les utilisateurs exécutant Citrix Receiver.

HDX Insight affiche désormais le nombre de sessions EDT et de sessions non EDT dans le rapport des sessions actives. Le tableau Utilisateurs affiche un rapport détaillé de tous les utilisateurs du système. Le tableau présente des mesures telles que la latence WAN, la latence DC, les retransmissions, les RTO et certaines de ces mesures ne sont pas disponibles pour les utilisateurs qui ont des sessions EDT car elles sont calculées à partir de la pile TCP actuellement. Par conséquent, ils apparaîtront sous la forme « NA ».



Un nouveau graphique en anneau a été introduit pour vous permettre de voir la bande passante consommée par l'utilisateur ainsi que le nombre total d'octets en fonction du type de protocole utilisé par les utilisateurs.



**Remarque**

EDT dans HDX Insight est pris en charge sur Citrix ADM à partir de la version 12.1 build 50.28 et est disponible sur les instances ADC à partir de la version 12.1 build 49.23.

**Mesures HDX Insight disponibles à partir de Citrix ADM 12.0 et versions ultérieures :**

Latence côté client L7	La latence moyenne L7 observée entre le client ICA et l'instance de Citrix ADC. Cette mesure est utile pour les périphériques non Citrix présents dans le chemin de remise.
Latence côté serveur L7	Latence moyenne L7 observée entre l'appareil Citrix ADC et l'application virtuelle Citrix. Cette mesure est utile pour les périphériques non Citrix présents dans le chemin de remise.
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.

Current Sessions									
Diagram	Session ID	Total Bytes	Bandwidth per Interval	Session Type	ICA RTT	Bytes per Interval	WAN latency	DC latency	Host Delay
	0000...000001	209.84 KB	11.58 Kbps	Application	854 ms	209.84 KB	83.00 ms	771 ms	4.00 ms
	0000...000001	127.18 KB	40.70 Kbps	Application	848 ms	127.18 KB	65.00 ms	710 ms	4.00 ms

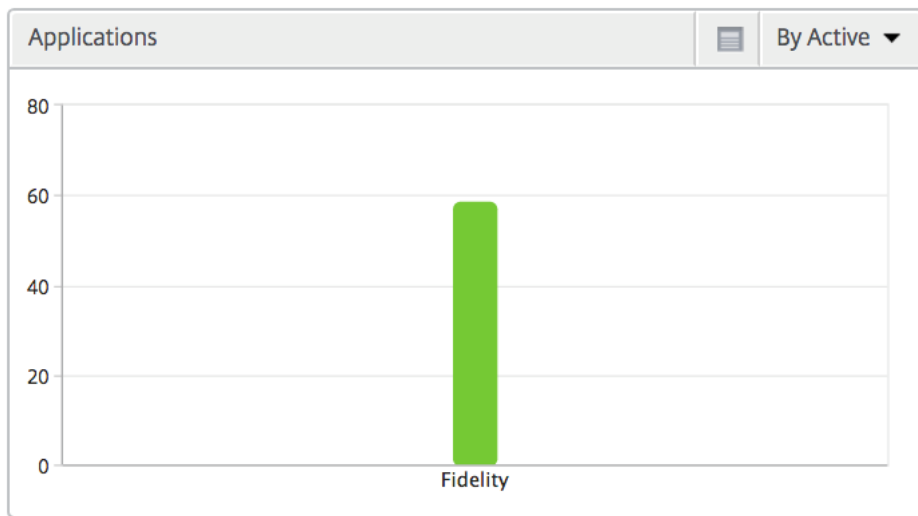
Terminated Sessions								
Session ID	Session Type	ICA RTT	WAN latency	DC latency	Bandwidth per Interval	Session Bandwidth	Total Bytes	Bytes per Interval
0000...000001	Application	1.01 s	59.00 ms	763.00 ms	9.40 Kbps	9.40 Kbps	1.38 MB	1.38 MB
0000...000001	Desktop	971.00 ms	59.00 ms	733.00 ms	8.82 Kbps	8.82 Kbps	1.29 MB	1.29 MB
0000...000001	Application	998.00	51.00 ms	732.00 ms	9.91 Kbps	9.91 Kbps	1.45 MB	1.45 MB

**Utilisateurs de bureau** Ce tableau donne un aperçu des sessions Citrix Virtual Desktop pour un utilisateur particulier. Ces mesures peuvent être triées par nombre de lancements de postes de travail et bande passante.

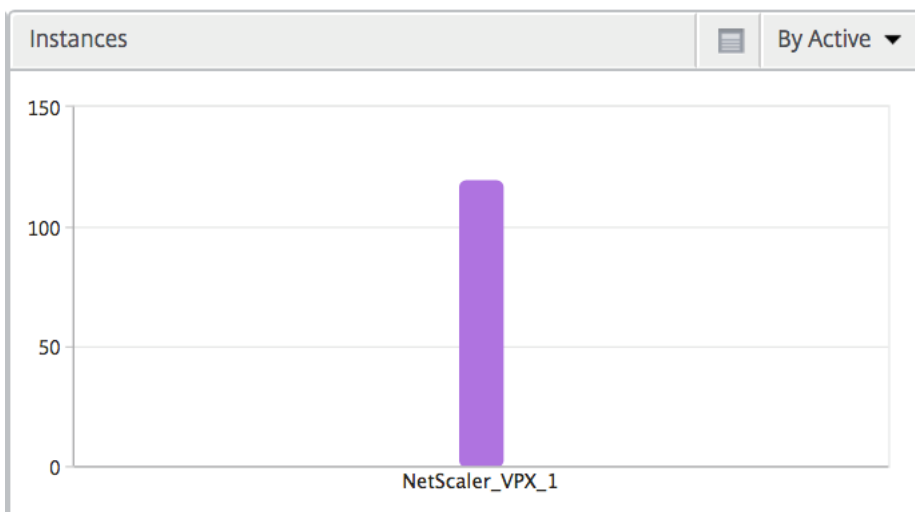
Mesures	Description
Nom	Nom du bureau virtuel Citrix.
Nombre de lancements de bureaux	Nombre de fois que l'ordinateur de bureau a été lancé.
Bande passante	Nombre total d'octets par seconde pris pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre Citrix Gateway et les serveurs VDI, CVAD ou StoreFront.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.

Desktop Users					
Name	Desktop Launch Count	Bandwidth	DC latency	WAN latency	ICA RTT
XenDesktop33	177	9.38 Kbps	749.00 ms	57.00 ms	1.00 s

**Applications** Un graphique à barres représentant les applications triées par Actif, le nombre total de sessions lancées, le nombre total de lancements d'applications et la durée de lancement.

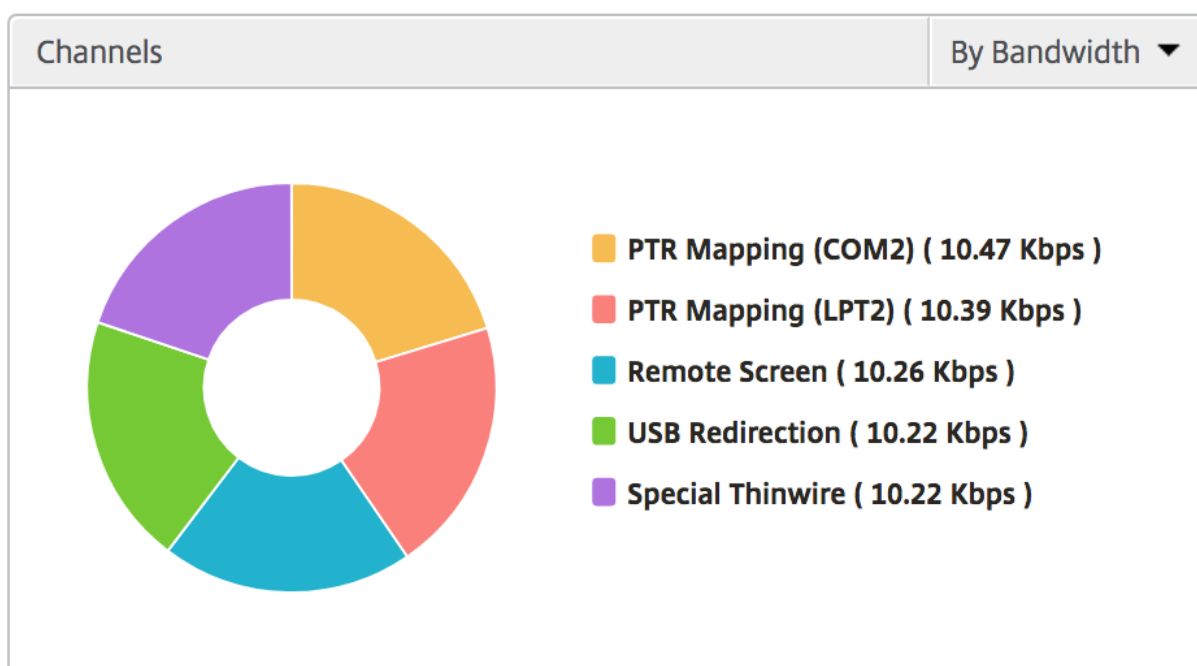


**Instances** Graphique à barres représentant les instances Citrix ADC triées par applications actives et totales

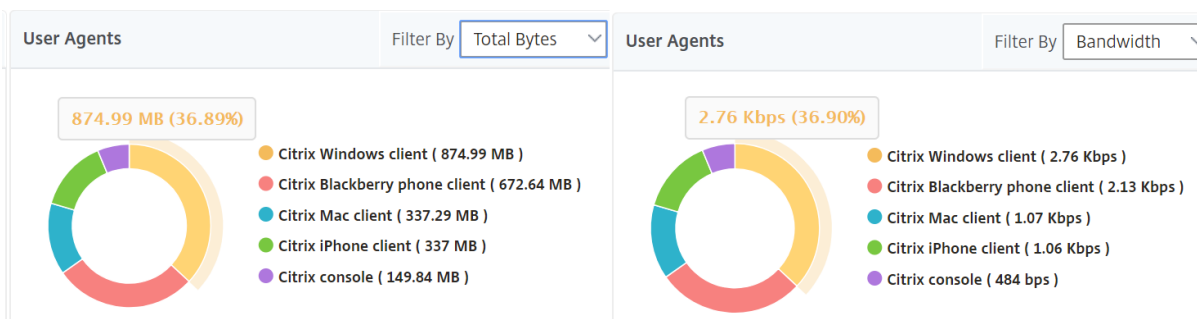


**Canaux** Les canaux représentent la bande passante globale ou le nombre total d'octets consommés par chaque canal virtuel ICA sous la forme d'un graphique en anneau. Vous pouvez également trier les mesures par bande passante ou Nombre total d'octets.





**Agents utilisateur** Les agents utilisateur 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.



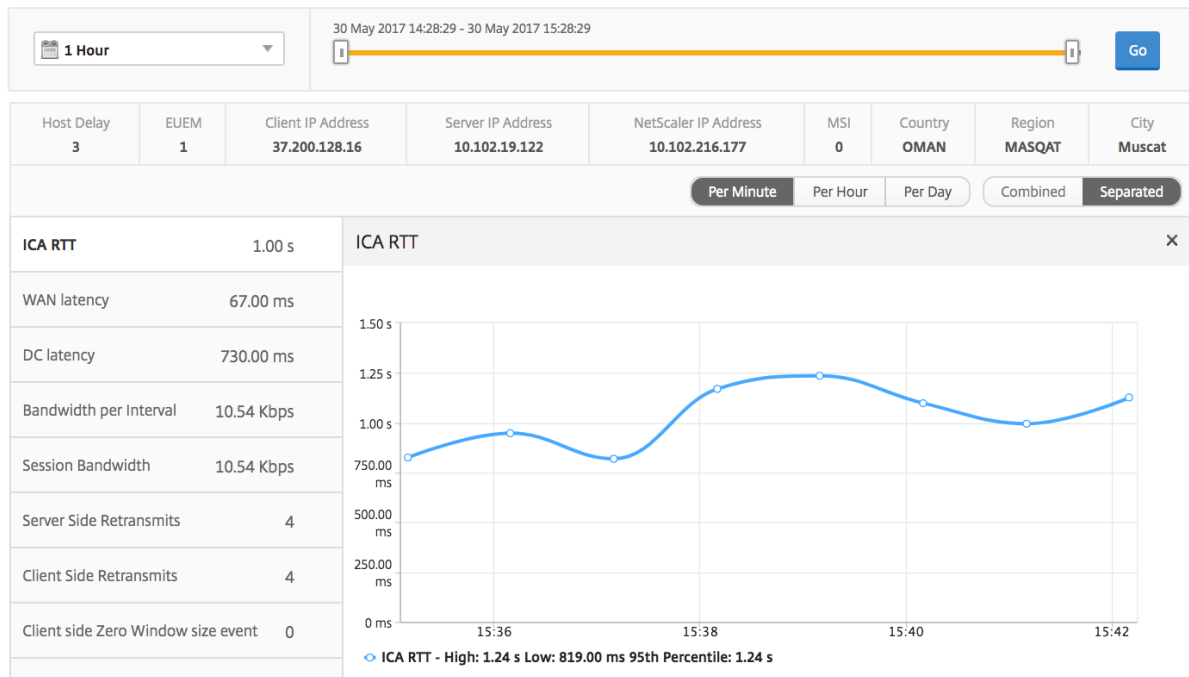
**Vue par session utilisateur** La vue par session utilisateur fournit des rapports pour la session d'un utilisateur sélectionné particulier.

**Pour afficher les mesures de la session d'un utilisateur sélectionné :**

1. Connectez-vous à votre Citrix ADM à l'aide d'un navigateur Web pris en charge.
2. Accédez à **Analytics > HDX Insight > Utilisateurs**.
3. Select un utilisateur particulier dans la section **Rapport récapitulatif de l'utilisateur**.
4. Sélectionnez une session dans la colonne **Sessions en cours** ou **Sessions terminées**.

**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 Citrix Virtual Apps actives.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre Citrix Gateway et les serveurs VDI, CVAD ou StoreFront.
Bande passante de session	La bande passante consommée par la session quel que soit l'intervalle de temps.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de la retransmission s'est produit sur la connexion entre Citrix ADC et le serveur principal.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.
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.

Active Applications				By # Active Sessions
Name	# Active Sessions	Launch Duration	# Active Apps	
Fidelity	1	557.00 ms	1	

**Sessions connexes** La section Sessions associées affiche les sessions associées des sessions de l'utilisateur sélectionné. La relation peut être sélectionnée comme serveurs communs ou Citrix ADC commun.

Related Sessions											By Common Server
Session ID	Session Type	User Name	State	ICA RTT	WAN latency	DC latency	Bandwidth per Interval	Total Bytes	Total Bytes	Byte	
0000...000001	Application	grahmm	●	1.021 s	51.00 ms	737 ms	9.26 Kbps	9.26 Kbps	977.73 KB		
0000...000001	Application	liam	●	955 ms	50.00 ms	733 ms	10.91 Kbps	10.91 Kbps	1.26 MB		
0000...000001	Application	grahmm	●	1.058 s	38.00 ms	817 ms	10.27 Kbps	10.27 Kbps	367.24 KB		

## Rapports et mesures Application View

Les rapports et les mesures de cette vue sont axés sur Citrix Virtual Apps.

**Pour accéder à la vue Application :**

1. Connectez-vous à votre Citrix ADM à l'aide d'un navigateur Web pris en charge.
2. Accédez à **Analytics > HDX Insight > Applications**.

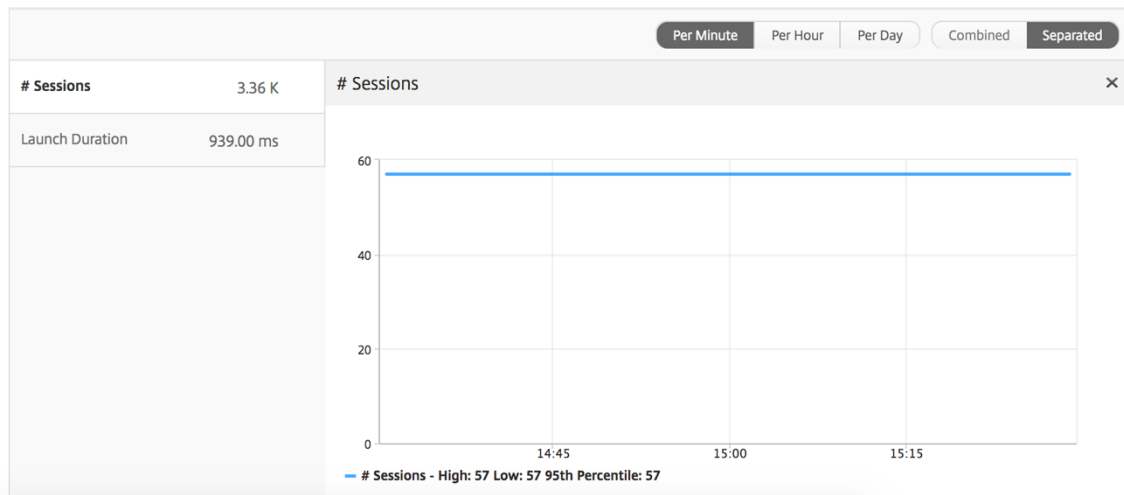
### Vue récapitulative

La vue récapitulative affiche les rapports de toutes les applications qui sont connectées au cours de la chronologie sélectionnée.

Toutes les métriques/rapports ci-dessous, sauf mention explicite, auront les valeurs qui leur correspondent pour la période sélectionnée.

### Graphique linéaire

Métriques	Description
Nombre de sessions	Nombre total de séances pendant un intervalle de temps donné.
Durée du lancement	Temps moyen requis pour lancer une application.



### Rapport Synthèse des applications

Métriques	Description
Nom	Nom des Citrix Virtual Apps.

Métriques	Description
Nb total de sessions lancées	Nombre total de sessions Citrix Virtual Apps actives au cours de l'intervalle de temps donné.
Nb total d'applications lancées	Nombre total de Citrix Virtual Apps lancées au cours de l'intervalle de temps donné.
Durée de lancement	Temps moyen requis pour lancer Citrix Virtual Apps.

Applications			
Name	Total App Launch Count	Launch Duration	Total Session Launch count
Microsoft Outlook	531	514.00 ms	531
Microsoft Visio	354	555.00 ms	354
Microsoft Word	354	557.00 ms	354
Microsoft Excel	354	555.00 ms	354

### Rapport sur les applications actives

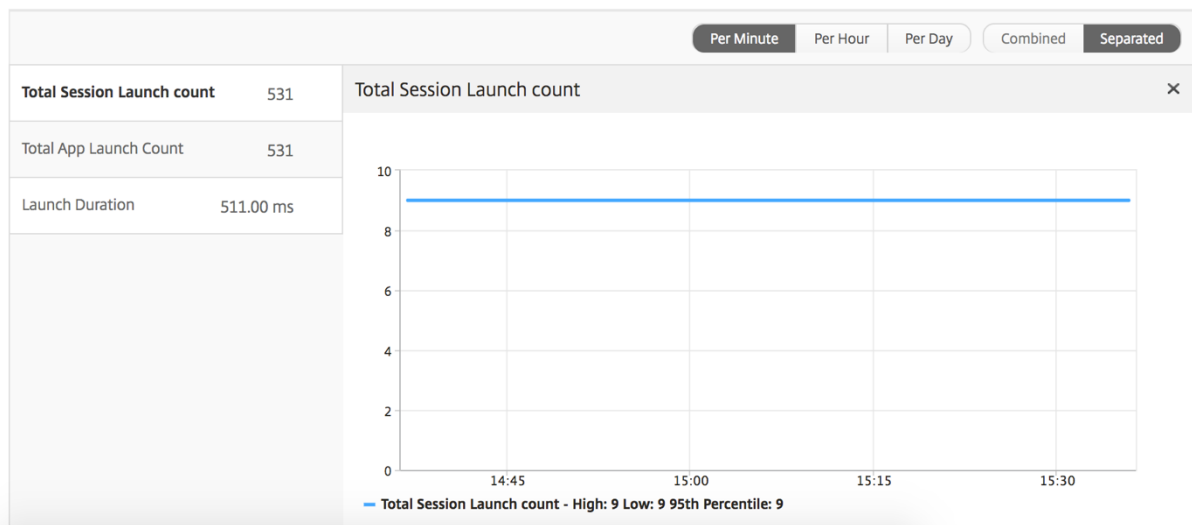
Métriques	Description
Nom	Nom de l'application virtuelle Citrix.
État	Affiche l'état de l'application : Vert-Actif, Rouge-Inactif
Nombre de sessions actives	Nombre de sessions utilisateur actives utilisant cette application pendant un intervalle de temps donné.
Nombre d'applications actives	Nombre de sessions actives pour cette application.

Active Applications			
Name	State	# Active Sessions	# Active Apps
Communicator	●	60	60
Fidelity	●	60	60
GoToMeeting	●	60	60
...	...	..	..

**Rapport sur les seuils** Le rapport sur les seuils représente le nombre de seuils franchis lorsque l'entité est sélectionnée en tant qu'*application* au cours de la période sélectionnée. Pour plus d'informations, consultez [comment créer des seuils](#).

## Graphique linéaire

Métriques	Description
Nombre de sessions actives	Ce nombre indique le nombre de sessions Citrix Virtual Apps and Desktops actives.
Durée du lancement	Temps moyen requis pour lancer une application.



## Rapport des sessions en cours

Métriques	Description
ID de session	Une identité unique pour une session ICA.
Type de session	Application/Bureau.
État	Vert/rouge pour les sessions actives/inactives.
Délai d'hôte	Délai moyen du trafic ICA transitant par les Citrix ADC causé par le réseau du serveur.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Bande passante de session	La bande passante consommée par la session quel que soit l'intervalle de temps.
Octets par intervalle	Nombre d'octets consommés par la session pendant cet intervalle de temps particulier.
Start Time	Heure de début de la session.

Métriques	Description
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 Apps.
Adresse IP NetScaler	IP de gestion NetScaler (NSIP).
Type de client	Type de récepteur - Client Windows Citrix
Version du client	Version du Receiver.
MSI	Boolean (Oui/Non). Indique si la session est multiflux ICA.
Reconnexions de session	Nombre de fois où la session s'est reconnectée.
Nb d'ACR	Nombre total de fois où un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, le mode utilisateur/transparent de Citrix Gateway.
Pays	Pays à partir duquel la session a été créée.
Région	Région à partir de laquelle la session a été créée.
City	Ville à partir de laquelle la session a été créée.
État de l'USB	Actif/Inactif -Vert/Rouge.
Nombre d'instances USB acceptées	Le nombre d'instances USB acceptées.
Nombre d'instances USB rejetées	Le nombre d'instances USB rejetées.
Nombre d'instances USB arrêtées	Le nombre d'instances USB arrêtées.
Nom d'hôte du client	Le nom d'hôte du client.
Nombre de basculements HA	Nombre de fois où le basculement HA s'est produit.
Motif de la résiliation	Affiche la raison de l'arrêt d'une session. Par exemple, délai d'expiration de session ICA, session terminée par l'utilisateur.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.

Métriques	Description
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre Citrix Gateway et les serveurs VDI, CVAD ou StoreFront.
Nb total d'octets	Nombre total d'octets consommés par l'utilisateur pendant la période sélectionnée.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de la retransmission s'est produit sur la connexion entre Citrix ADC et le serveur principal.
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 Apps.
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	La latence moyenne L7 observée entre le client ICA et l'instance de Citrix ADC. Cette mesure est utile pour les périphériques non Citrix présents dans le chemin de remise.
Latence côté serveur L7	Latence moyenne L7 observée entre l'appareil Citrix ADC et Citrix Virtual Apps. Cette mesure est utile pour les périphériques non Citrix présents dans le chemin de remise.

Diagram	Session ID	Session Type	ICA RTT	Host Delay	Start Time	Up Time	Client IP Address	Server IP Address	NetScaler IP Address
	0000...000001	Application	1.012 s	2.00 ms	2017-6-12 15:39:58	0 h: 0 m: 59s	23.18.6.21	10.102.19.122	10.102.216.177
	0000...000001	Application	880 ms	1.00 ms	2017-6-12 15:39:58	0 h: 0 m: 59s	1.2.16.12	10.102.60.50	10.102.216.219

### Vue par session d'application

L'affichage par session d'application affiche les rapports pour une session d'application sélectionnée particulière.

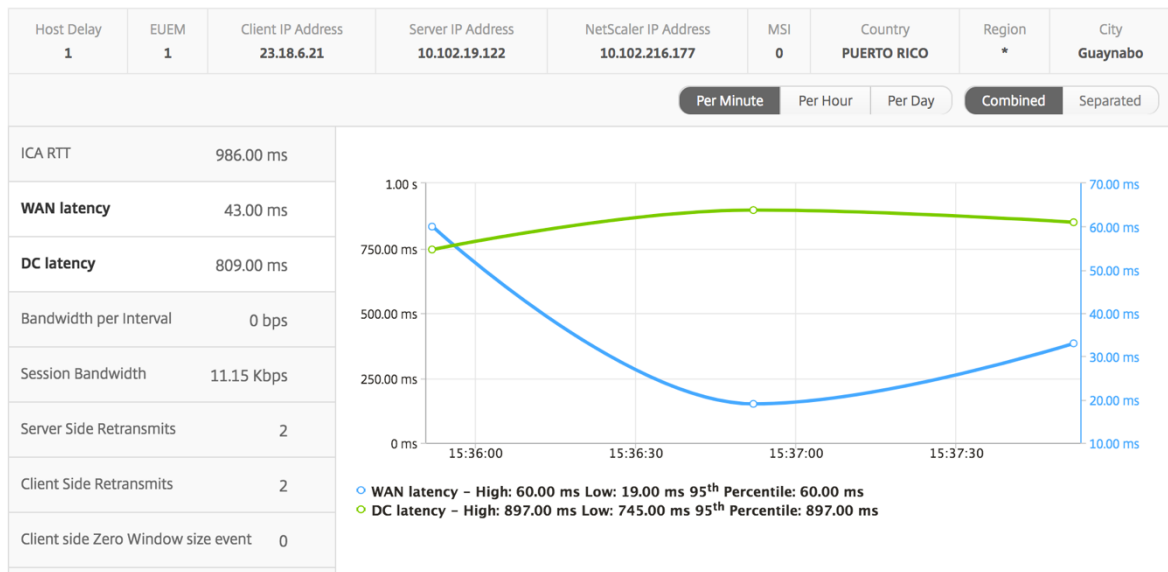
#### Pour afficher les rapports de session :

1. Connectez-vous à votre Citrix ADM à l'aide d'un navigateur Web pris en charge.
2. Accédez à **Analytics > HDX Insight > Applications**.
3. Sélectionnez un utilisateur particulier dans le rapport récapitulatif des applications.
4. Sélectionné une session à partir du rapport des sessions en cours.

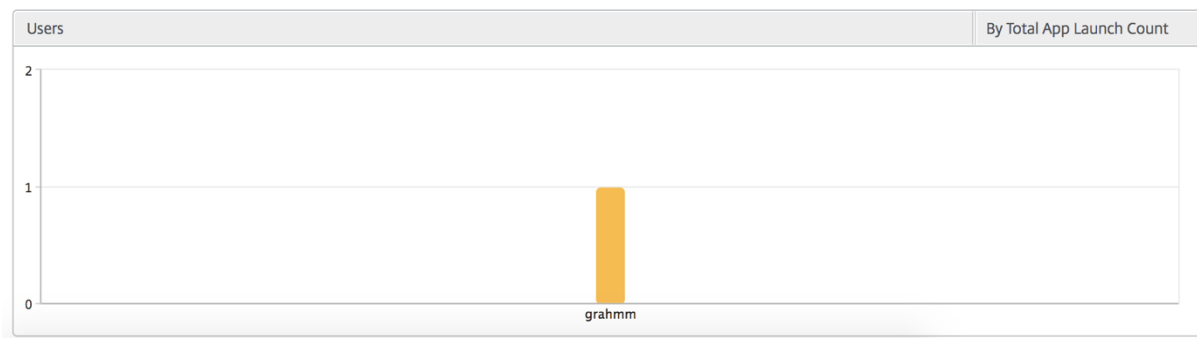
### Graphique linéaire

Métriques	Description
Reconnexions de session	Nombre de fois où la session s'est reconnectée.
Nb d'ACR	Nombre total de fois où un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.

Métriques	Description
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. Autrement dit, de Citrix ADC à l'utilisateur final.
Événement de taille de fenêtre nulle côté serveur	Latence causée par le côté serveur du réseau. C'est-à-dire, de Citrix ADC aux serveurs 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 sur la connexion entre Citrix ADC et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
Bande passante de session	La bande passante consommée par la session quel que soit l'intervalle de temps.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de la retransmission s'est produit sur la connexion entre Citrix ADC et le serveur principal.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.



**Graphique à barres utilisateur** Le graphique à barres de l'utilisateur représente les utilisateurs connectés à cette application particulière.



## Rapports et mesures de la vue de bureau

Les rapports et les mesures de cette vue sont axés sur les Citrix Virtual Desktops.

### Pour accéder à la vue Bureau :

1. Connectez-vous à votre Citrix ADM à l'aide d'un navigateur Web pris en charge.
2. Accédez à **Analytics > HDX Insight > Bureau**.

### Vue récapitulative

La vue récapitulative affiche les rapports de tous les Citrix Virtual Desktops qui sont connectés au cours de la chronologie sélectionnée.

Toutes les métriques/rapports ci-dessous, sauf mention explicite, auront les valeurs qui leur correspondent pour la période sélectionnée.

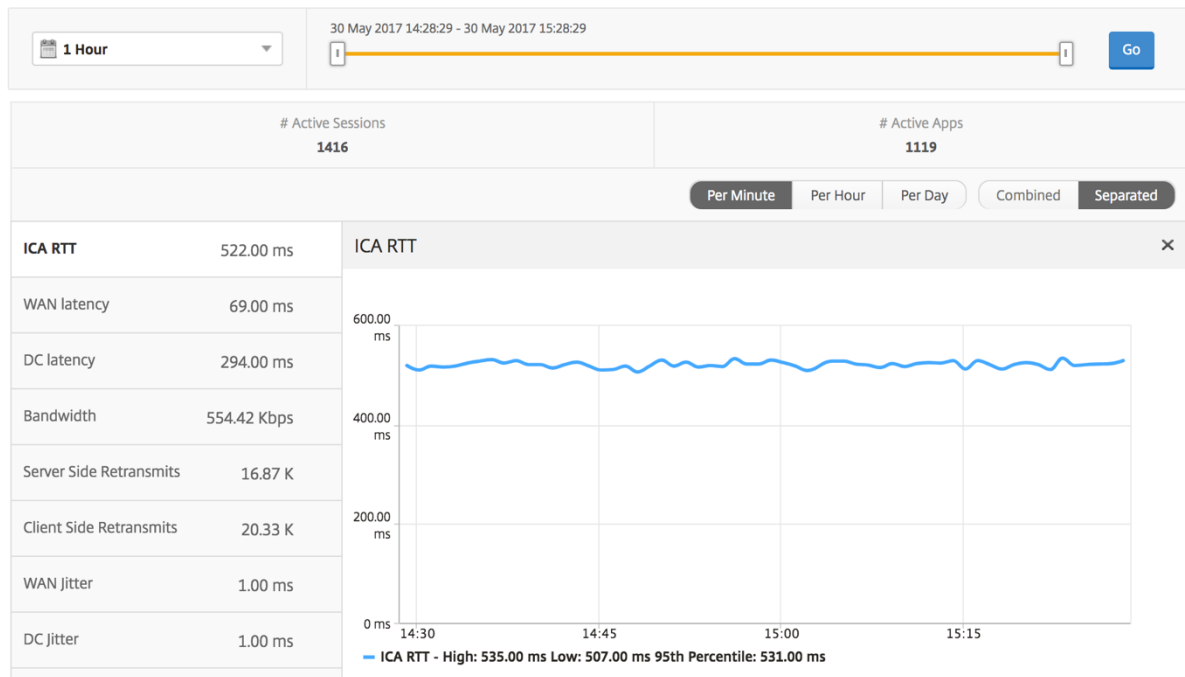
### Graphique linéaire

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 Citrix Virtual Apps actives.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre Citrix Gateway et les serveurs VDI, CVAD ou StoreFront.
Bande passante	Nombre total d'octets par seconde pris pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de la retransmission s'est produit sur la connexion entre Citrix ADC et le serveur principal.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.

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 de synthèse des bureaux**

Métriques

Description

Active Sessions	Nombre total de sessions Citrix Virtual Desktops actives pendant un intervalle de temps donné.
Ordinateurs de bureau actifs	Nombre total de Citrix Virtual Desktops actifs au cours d'un intervalle de temps donné.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre Citrix Gateway et les serveurs VDI, CVAD ou StoreFront.

Métriques	Description
Bande passante	Nombre total d'octets par seconde pris pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Nb total d'octets	Nombre total d'octets consommés par l'utilisateur pendant la période sélectionnée.

User Name	# Active Desktops	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
liam	60	1.00 s	56.00 ms	746.00 ms	9.27 Kbps	251.24 MB
jayden	60	1.00 s	52.00 ms	746.00 ms	9.27 Kbps	251.34 MB
juan	60	169.00 ms	32.00 ms	30.00 ms	9.26 Kbps	250.99 MB
daniel	60	149.00 ms	31.00 ms	30.00 ms	9.26 Kbps	251.02 MB
randyb	60	99.00 ms	11.00 ms	30.00 ms	9.26 Kbps	250.97 MB

**Rapport sur les seuils** Le rapport de seuil représente le nombre de seuils dépassés lorsque l'entité est sélectionnée en tant que Bureau au cours de la période sélectionnée. Pour plus d'informations, consultez [comment créer des seuils](#).

### Par vue Bureau

La vue par poste de travail fournit des rapports détaillés sur l'expérience utilisateur pour un Citrix Virtual Desktop sélectionné.

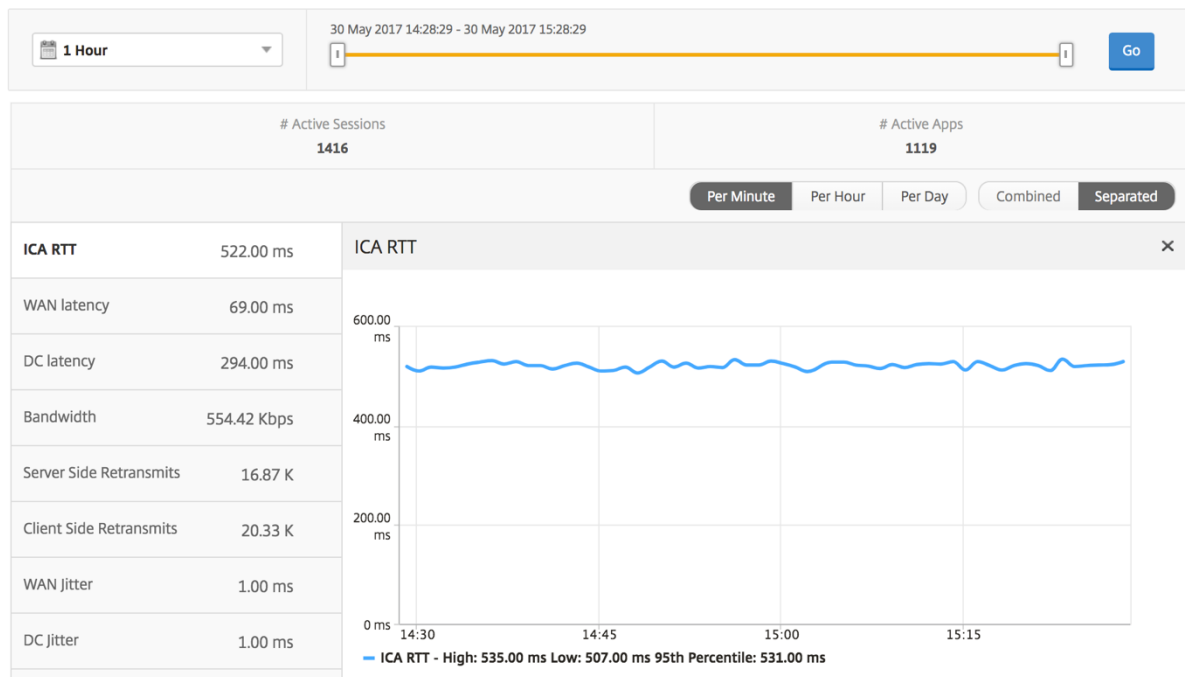
#### Pour accéder à la vue Bureau spécifique :

1. Connectez-vous à votre Citrix ADM à l'aide d'un navigateur Web pris en charge.
2. Accédez à **Analytics > HDX Insight > Bureau**.
3. Sélectionnez un **poste de travail** particulier dans le **rapport récapitulatif des ordinateurs de bureau**.

### Graphique linéaire

Métriques	Description
Nombre de sessions actives	Ce nombre indique le nombre de sessions Citrix Virtual Apps and Desktops actives.
Nbre d'applications actives	Ce nombre indique le nombre de sessions Citrix Virtual Apps actives.

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 est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est est-à-dire entre Citrix Gateway et les serveurs VDI, CVAD ou StoreFront.
Bande passante	Nombre total d'octets par seconde pris pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de la retransmission s'est produit sur la connexion entre Citrix ADC et le serveur principal.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.



**Rapport 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 démarrages de postes de travail et bande passante.

Mesures	Description
Nom	Nom du bureau virtuel Citrix.
Nombre de démarrages de bureaux	Nombre de fois que l'ordinateur de bureau a été lancé.
Bande passante	Nombre total d'octets par seconde pris pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre Citrix Gateway et les serveurs VDI, CVAD ou StoreFront.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.



Desktop Users					By Desktop Launch Count ▾
Name	Desktop Launch Count ↕	Bandwidth	DC latency	WAN latency	ICA RTT
XenDesktop33	177	9.38 Kbps	749.00 ms	57.00 ms	1.00 s

**Rapport Actif/Inactif des postes de travail utilisateur** Les mesures suivantes peuvent être triées en fonction de la bande passante par intervalle, des reconnexion de session et du nombre d'ACR.

Mesures	Description
ID de session	Une identité unique pour une session ICA.
Type de session	Application/Bureau.
État	Vert/rouge pour les sessions actives/inactives.
Délai d'hôte	Délai moyen du trafic ICA transitant par les Citrix ADC causé par le réseau du serveur.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Bande passante de session	La bande passante consommée par la session quel que soit l'intervalle de temps.
Octets par intervalle	Nombre d'octets consommés par la session pendant cet intervalle de temps particulier.
Start Time	Heure de début de la session.
Temps d'activité	Durée de la session.
Adresse IP cliente	IP de l'utilisateur final.
Adresse IP du serveur	Adresse IP du serveur Backend/Citrix Virtual Apps.
Adresse IP NetScaler	IP de gestion NetScaler (NSIP).
Type de client	Type de récepteur - Client Windows Citrix
Version du client	Version du Receiver.
MSI	Boolean (Oui/Non). Indique si la session est multiframe ICA.
Reconnexions de session	Nombre de fois où la session s'est reconnectée.
Nb d'ACR	Nombre total de fois où un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.

---

Mesures	Description
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, le mode utilisateur/transparent de Citrix Gateway.
Pays	Pays à partir duquel la session a été créée.
Région	Région à partir de laquelle la session a été créée.
City	Ville à partir de laquelle la session a été créée.
État de l'USB	Actif/Inactif -Vert/Rouge.
Nombre d'instances USB acceptées	Le nombre d'instances USB acceptées.
Nombre d'instances USB rejetées	Le nombre d'instances USB rejetées.
Nombre d'instances USB arrêtées	Le nombre d'instances USB arrêtées.
Nom d'hôte du client	Le nom d'hôte du client.
Nombre de basculements HA	Nombre de fois où le basculement HA s'est produit.
Motif de la résiliation	Affiche la raison de l'arrêt d'une session. Par exemple, délai d'expiration de session ICA, session terminée par l'utilisateur.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre Citrix Gateway et les serveurs VDI, CVAD ou StoreFront.
Nb total d'octets	Nombre total d'octets consommés par l'utilisateur pendant la période sélectionnée.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.

Mesures	Description
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de la retransmission s'est produit sur la connexion entre Citrix ADC et le serveur principal.
Nom de l'image VDI	Nom du Citrix Virtual Desktops auquel l'utilisateur est connecté

### Diagramme

User Desktops Active								By Bandwidth per Interval	
Diagram	Session ID	VDI Image Name	ICA RTT	WAN latency	DC latency	Host Delay	Bandwidth per Interval	Session Bandwidth	Total B
	0000...000001	XenDesktop33	1.094 s	48.00 ms	767 ms	5.00 ms	12.87 Kbps	12.87 Kbps	1.63
	0000...000001	XenDesktop33	1.007 s	37.00 ms	691 ms	4.00 ms	9.27 Kbps	9.27 Kbps	1.35
	0000...000001	XenDesktop33	0.94 s	53.00 ms	747 ms	5.00 ms	8.30 Kbps	8.30 Kbps	1.25

### Vue par 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. Connectez-vous à votre Citrix ADM à l'aide d'un navigateur Web pris en charge.
2. Accédez à **Analytics > HDX Insight > Bureau**.
3. Sélectionnez un poste de travail particulier dans le **rapport récapitulatif des postes** de travail.
4. Sélectionnez une session dans le rapport des sessions en cours.

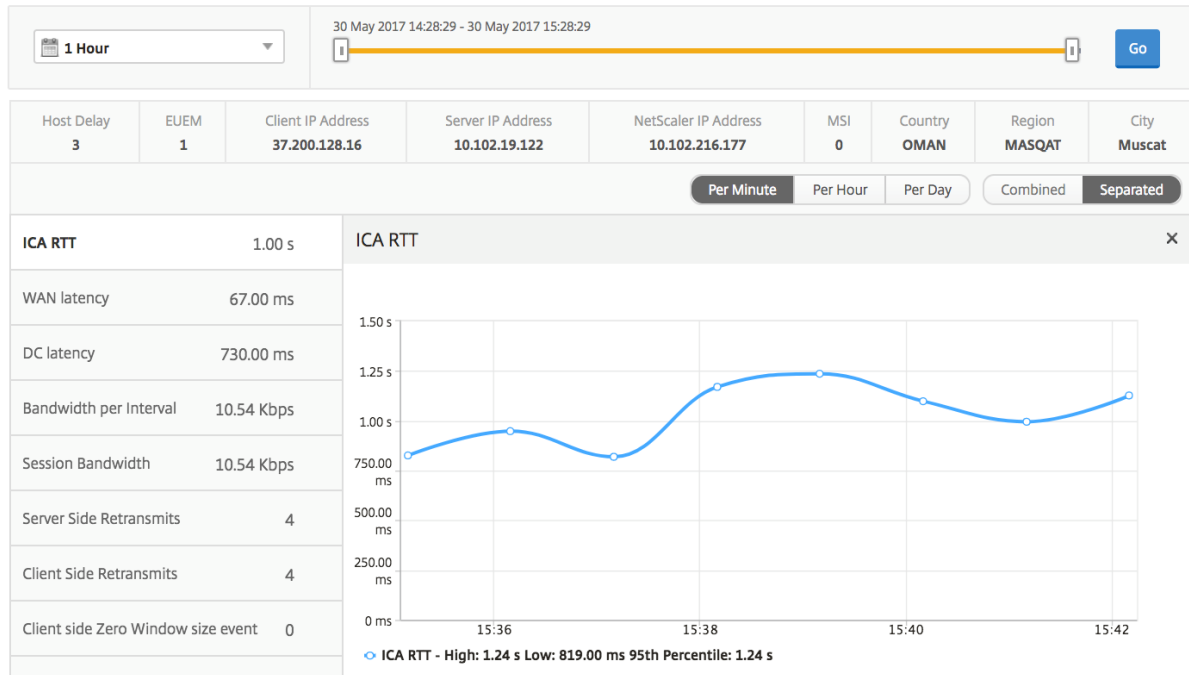
**Graphique chronologique** La vue par session utilisateur fournit des rapports pour la session d'un utilisateur sélectionné particulier.

#### Pour afficher les mesures de la session d'un utilisateur sélectionné :

1. Connectez-vous à votre Citrix ADM à l'aide d'un navigateur Web pris en charge.
2. Accédez à **Analytics > HDX Insight > Utilisateurs**.
3. Select un utilisateur particulier dans la section **Rapport récapitulatif de l'utilisateur**.
4. Sélectionnez une session dans la colonne **Sessions en cours** ou **Sessions terminées**.

Mesures	Description
Reconnexions de session	Ce nombre indique le nombre de sessions Citrix Virtual Apps and Desktops actives.
Nb d'ACR	Ce nombre indique le nombre de sessions Citrix Virtual Apps actives.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre Citrix Gateway et les serveurs VDI, CVAD ou StoreFront.
Bande passante de session	La bande passante consommée par la session quel que soit l'intervalle de temps.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de la retransmission s'est produit sur la connexion entre Citrix ADC et le serveur principal.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.

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 Sessions de bureau associées** Les mesures suivantes peuvent être triées en fonction de la bande passante par intervalle, des reconnexions de session et du nombre d’ACR.

Mesures	Description
ID de session	Une identité unique pour une session ICA.
Type de session	Application/Bureau.
État	Vert/rouge pour les sessions actives/inactives.
Délai d’hôte	Délai moyen du trafic ICA transitant par les Citrix ADC causé par le réseau du serveur.
Bande passante par intervalle	La bande passante consommée par la session pendant cet intervalle de temps particulier.
Bande passante de session	La bande passante consommée par la session quel que soit l’intervalle de temps.

Mesures	Description
Octets par intervalle	Nombre d'octets consommés par la session pendant cet intervalle de temps particulier.
Start Time	Heure de début de la session.
Temps d'activité	Durée de la session.
Adresse IP cliente	IP de l'utilisateur final.
Adresse IP du serveur	Adresse IP du serveur Backend/Citrix Virtual Apps.
Adresse IP NetScaler	IP de gestion NetScaler (NSIP).
Type de client	Type de récepteur - Client Windows Citrix
Version du client	Version du Receiver.
MSI	Boolean (Oui/Non). Indique si la session est multiflux ICA.
Reconnexions de session	Nombre de fois où la session s'est reconnectée.
Nb d'ACR	Nombre total de fois où un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, le mode utilisateur/transparent de Citrix Gateway.
Pays	Pays à partir duquel la session a été créée.
Région	Région à partir de laquelle la session a été créée.
City	Ville à partir de laquelle la session a été créée.
État de l'USB	Actif/Inactif -Vert/Rouge.
Nombre d'instances USB acceptées	Le nombre d'instances USB acceptées.
Nombre d'instances USB rejetées	Le nombre d'instances USB rejetées.
Nombre d'instances USB arrêtées	Le nombre d'instances USB arrêtées.
Nom d'hôte du client	Le nom d'hôte du client.
Nombre de basculements HA	Nombre de fois où le basculement HA s'est produit.
Motif de la résiliation	Affiche la raison de l'arrêt d'une session. Par exemple, délai d'expiration de session ICA, session terminée par l'utilisateur.

Mesures	Description
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre Citrix Gateway et les serveurs VDI, CVAD ou StoreFront.
Nb total d'octets	Nombre total d'octets consommés par l'utilisateur pendant la période sélectionnée.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre Citrix ADC et l'utilisateur final. Une valeur élevée de cette mesure ne signifie pas que l'expérience utilisateur ne sera pas transparente, mais indique une utilisation élevée de la bande passante due aux retransmissions.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit lors de la connexion entre Citrix ADC et l'utilisateur final.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois où le serveur a signalé une fenêtre TCP zéro.
RTO rapide côté serveur	Nombre de fois où le délai d'expiration de la retransmission s'est produit sur la connexion entre Citrix ADC et le serveur principal.

User Desktops Active								By Bandwidth per Interval	
Diagram	Session ID	VDI Image Name	ICA RTT	WAN latency	DC latency	Host Delay	Bandwidth per Interval	Session Bandwidth	Total B
	0000...0000001	XenDesktop33	1.094 s	48.00 ms	767 ms	5.00 ms	12.87 Kbps	12.87 Kbps	1.63
	0000...0000001	XenDesktop33	1.007 s	37.00 ms	691 ms	4.00 ms	9.27 Kbps	9.27 Kbps	1.35
	0000...0000001	XenDesktop33	0.914 s	53.00 ms	747 ms	5.00 ms	8.38 Kbps	8.38 Kbps	1.25

## Rapports et mesures Instance View

Les rapports et les métriques de la vue d'instance sont axés sur la ou les instances Citrix ADC.

### Pour accéder à la vue Instance :

1. Connectez-vous à votre Citrix ADM à l'aide d'un navigateur Web pris en charge.
2. Accédez à **Analytics > HDX Insight > Instances**.

Les rapports et mesures de vue d'instance comprennent les sections suivantes :

- Vue récapitulative de l'instance
- Vue par instance

### Vue Résumé de l'instance

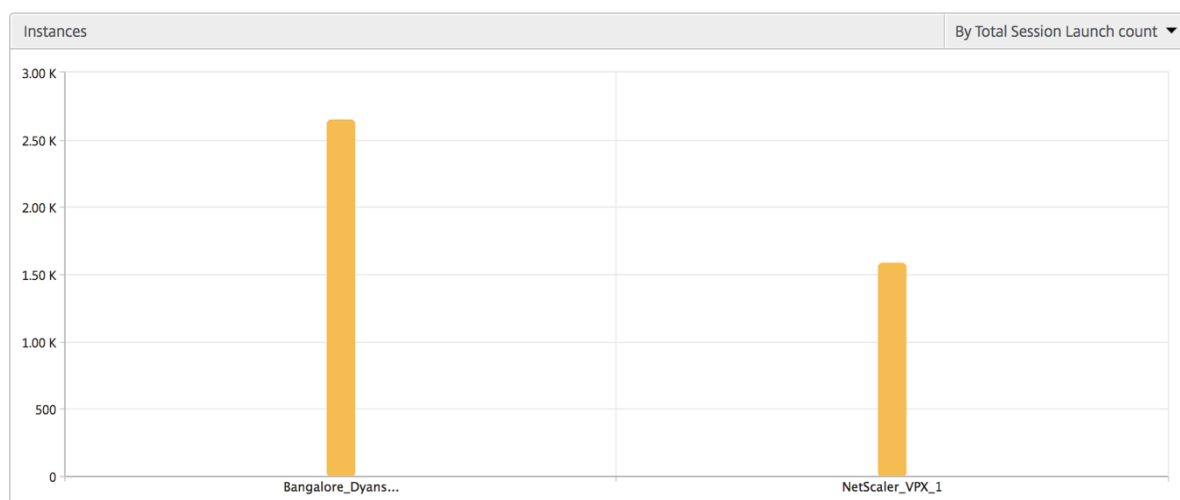
Cette vue est appelée vue récapitulative car elle affiche les rapports pour toutes les instances Citrix ADC qui sont ajoutées à Citrix ADM.

Toutes les métriques/rapports ci-dessous, sauf mention explicite, auront les valeurs qui leur correspondent pour la période sélectionnée.

### Graphique à barres d'instance

Ce graphique affiche l'instance par rapport au nombre total de lancement de session

Total Apps qui peut être sélectionné dans le menu déroulant en haut à droite sur le canevas du graphique.





## Rapport Instance/Active Instances Summary

Métriques	Description
Nom	Nom d'hôte de l'instance Citrix ADC.
Adresse IP	Adresse IP NetScaler.
Nb total de sessions lancées	Nombre total de sessions utilisateur uniques créées au cours d'un intervalle de temps donné.
Nb total d'applics	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
<a href="#">Bangalore_Dyansty(10.102.216.219)</a>	10.102.216.219	2.65 K	2.12 K	-NA-
<a href="#">NetScaler_VPX_1(10.102.216.177)</a>	10.102.216.177	1.59 K	1.24 K	-NA-

Active Instances					
Name	IP Address	# Active Sessions	# Active Apps	# Active Desktops	Type
<a href="#">NetScaler_VPX_1(10.102.216.177)</a>	10.102.216.177	538	417	120	-NA-
<a href="#">Bangalore_Dyansty(10.102.216.219)</a>	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 se produire pour plusieurs raisons, telles que l'utilisation de versions non prises en charge de Citrix Virtual Apps and Desktops, d'une version non prise en charge du type Receiver ou Receiver, etc. Ce tableau indique l'adresse IP et le nombre de flux ignorés. Ces récepteurs peuvent ne pas faire partie des récepteurs de liste blanche ; par conséquent, ces sessions sont ignorées de la surveillance.

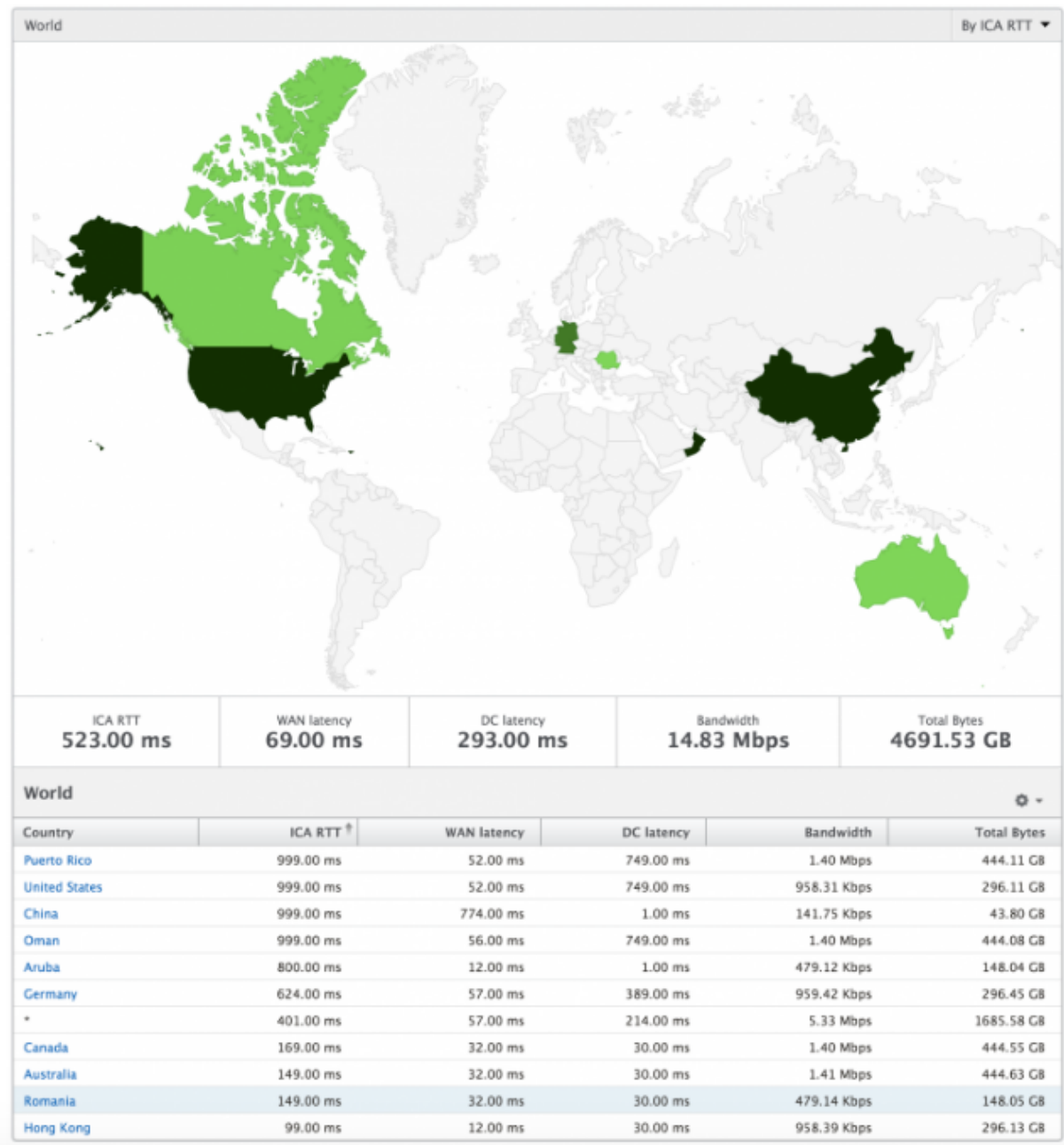
Skipped Flows	
IP Address	Skipped Count
10.105.2.141	1
10.105.2.142	1

**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 leurs recherches pour afficher les informations par ville et par État. À partir de Citrix ADM version 12.0 et ultérieure, vous pouvez effectuer une exploration vers le bas vers les utilisateurs connectés à partir d'un emplacement Geo.

Les détails suivants peuvent être visualisés sur la carte du monde dans HDX Insight, 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



### Vue par instance

La vue par instance fournit des rapports détaillés sur l'expérience utilisateur final pour une instance Citrix ADC sélectionnée particulière.

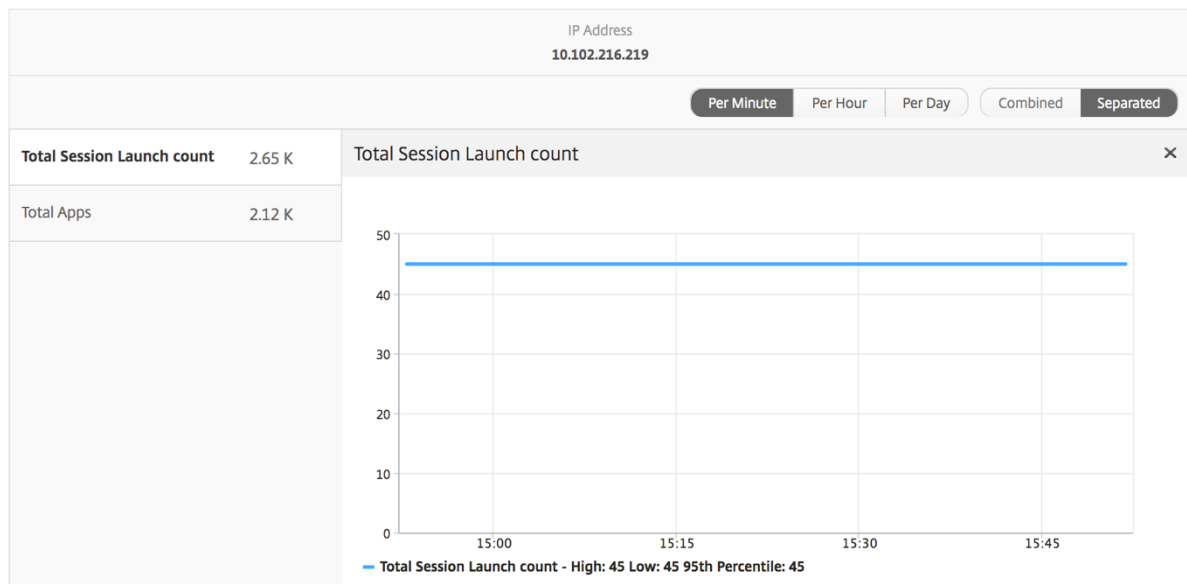
#### Pour accéder à la vue Instance :

1. Connectez-vous à votre Citrix ADM à l'aide d'un navigateur Web pris en charge.
2. Accédez à **Analytics > HDX Insight > Instances**.

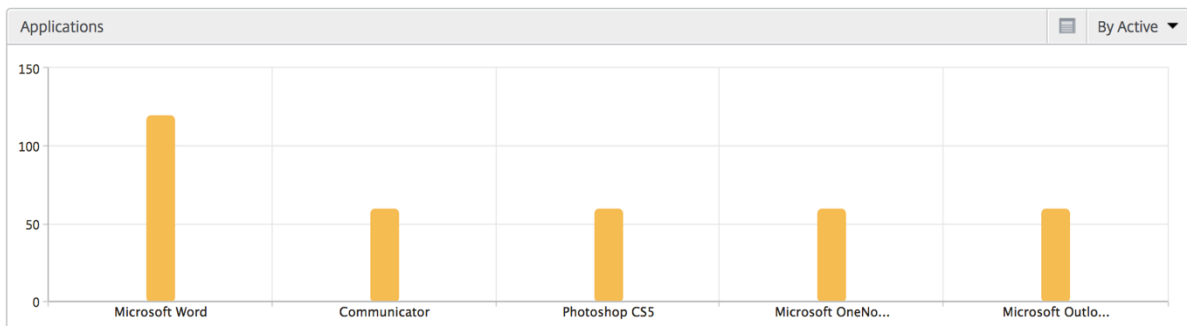
3. Sélectionnez une instance particulière dans le **rapport Récapitulatif de l'instance**.

### 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 Apps 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.

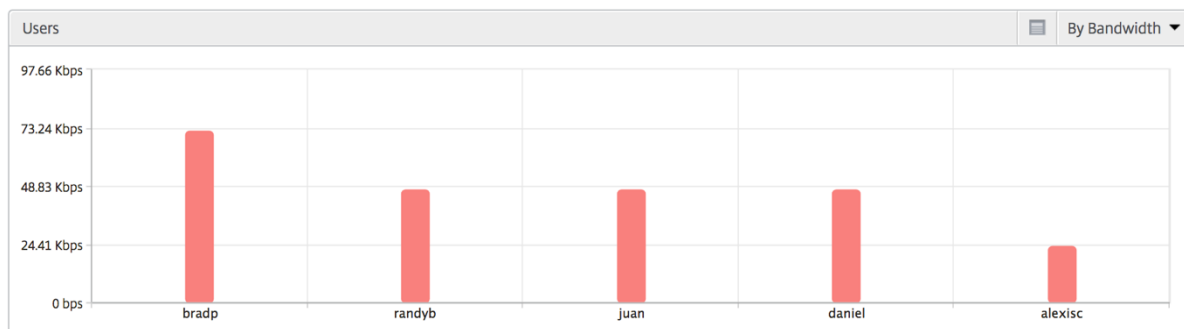


**Graphique à barres des applications** Affiche les 5 meilleures applications en fonction des critères suivants : par applications actives, nombre total de sessions lancées, nombre total de lancements d'applications ou durée de lancement.



**Graphique à barres des utilisateurs** Le graphique à barres Utilisateurs affiche les 5 premiers utilisateurs selon les critères suivants

- Bande passante
- Latence WAN
- Latence DC
- RTT ICA



**Rapport Utilisateurs de bureau** Ce tableau donne un aperçu des sessions Citrix Virtual Desktop pour un utilisateur particulier. Ces mesures peuvent être triées par nombre de lancements de postes de travail et bande passante.

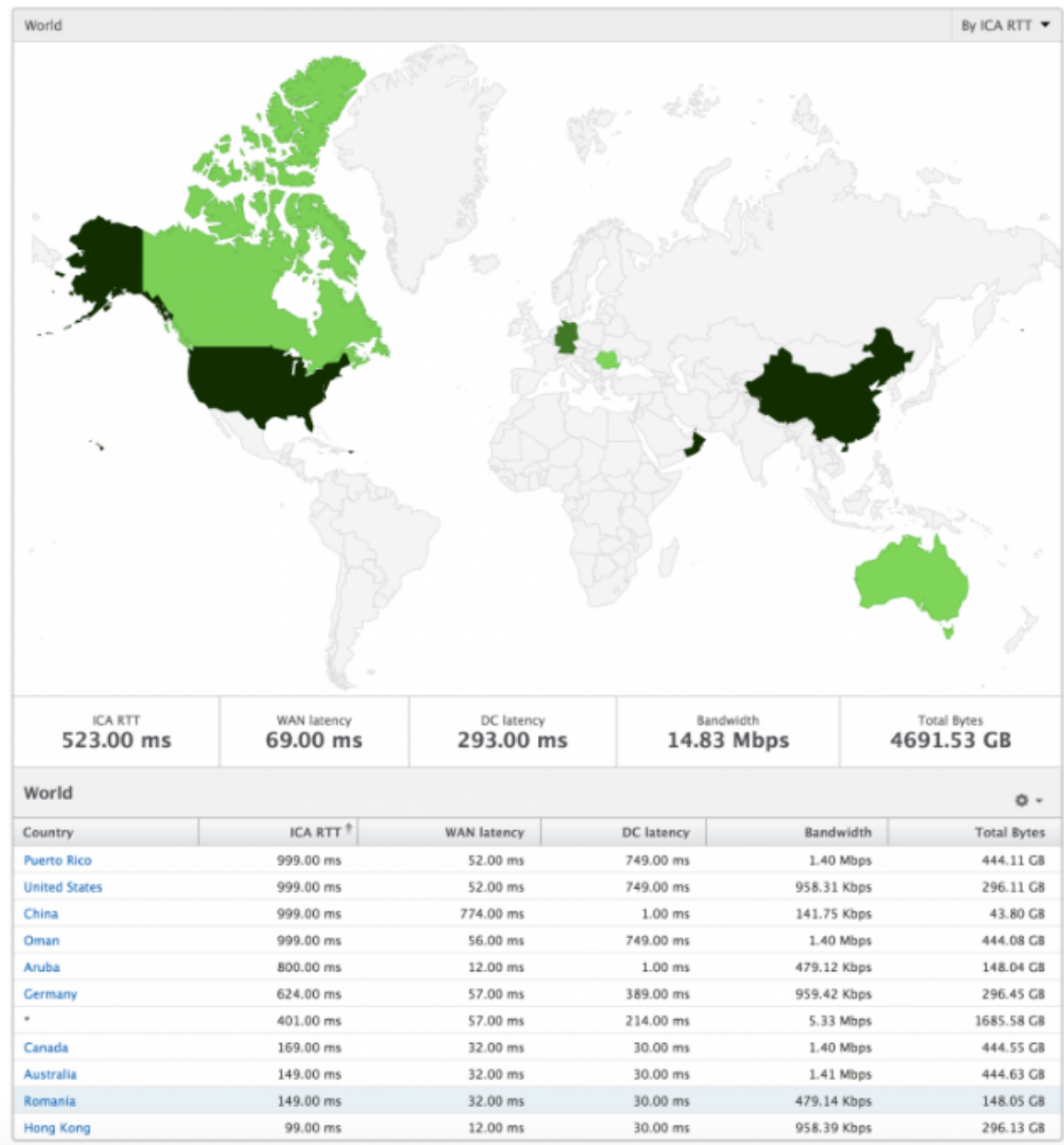
Mesures	Description
Nom	Nom du bureau virtuel Citrix.
Nombre de lancements de bureaux	Nombre de fois que l'ordinateur de bureau a été lancé.
Bande passante	Nombre total d'octets par seconde pris pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire entre Citrix Gateway et les serveurs VDI, CVAD ou StoreFront
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de Citrix ADC à l'utilisateur final.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.

Desktop Users						By Desktop Launch Count ▾
Name	Desktop Launch Count ↕	Bandwidth	DC latency	WAN latency	ICA RTT	
XenDesktop33	177	9.38 Kbps	749.00 ms	57.00 ms	1.00 s	

**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 leurs recherches pour afficher les informations par ville et par État. À partir de Citrix ADM version 12.0 et ultérieure, vous pouvez effectuer une exploration vers le bas vers les utilisateurs connectés à partir d'un emplacement Geo.

Les détails suivants peuvent être visualisés sur la carte du monde dans HDX Insight, 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 License View

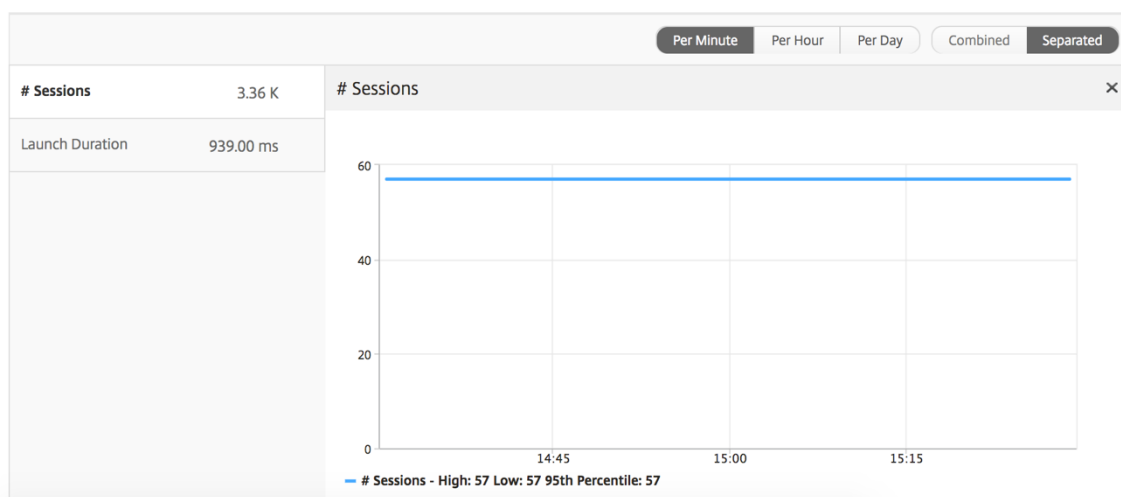
La vue de licence donne des détails sur les informations de licence Citrix Gateway.

#### Pour accéder à la vue Licence :

1. Connectez-vous à votre Citrix ADM à l'aide d'un navigateur Web pris en charge.
2. Accédez à **Analytics > HDX Insight > Licences**.

## Graphique linéaire

Métriques	Description
Licences utilisées	Les licences CCU Citrix Gateway utilisées pendant la chronologie sélectionnée. Chaque nombre représente le nombre de sessions utilisateur. Cela est indépendant des sessions d'application et de bureau lancées par cet utilisateur.
Nombre total de licences	Nombre total de licences Citrix Gateway CCU disponibles pour le client.



**Rapport sur les seuils** Le rapport de seuil représente le nombre de seuils dépassés lorsque l'entité est sélectionnée en tant que Licence au cours de la période sélectionnée. Pour plus d'informations, consultez [comment créer des seuils](#).

## Rapports et mesures d'affichage des applications

February 1, 2024

Les rapports et les mesures de cette vue sont axés sur Citrix Virtual Apps.

### Pour accéder à la vue Application :

1. Connectez-vous à votre Citrix ADM à l'aide d'un navigateur Web pris en charge.



2. Accédez à **Analytics > HDX Insight > Applications**.

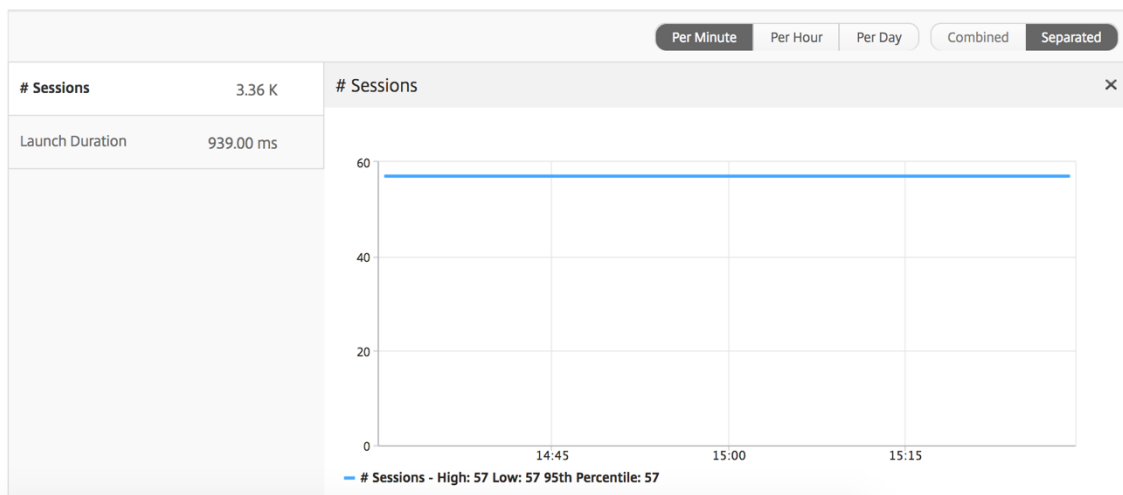
### Vue récapitulative

La vue récapitulative affiche les rapports de toutes les applications qui sont connectées au cours de la chronologie sélectionnée.

Toutes les métriques/rapports ci-dessous, sauf mention explicite, auront les valeurs qui leur correspondent pour la période sélectionnée.

### Graphique en courbes

Mesures	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 de synthèse des applications

Métriques	Description
Nom	Nom de l'application virtuelle Citrix.

Métriques	Description
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 de Citrix Virtual Apps lancées au cours de l'intervalle de temps donné.
Durée de lancement	Temps moyen nécessaire pour lancer les Citrix Virtual Apps.

Applications			
Name	Total App Launch Count	Launch Duration	Total Session Launch count
Microsoft Outlook	531	514.00 ms	531
Microsoft Visio	354	555.00 ms	354
Microsoft Word	354	557.00 ms	354
Microsoft Excel	354	555.00 ms	354

### Rapport sur les applications actives

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.

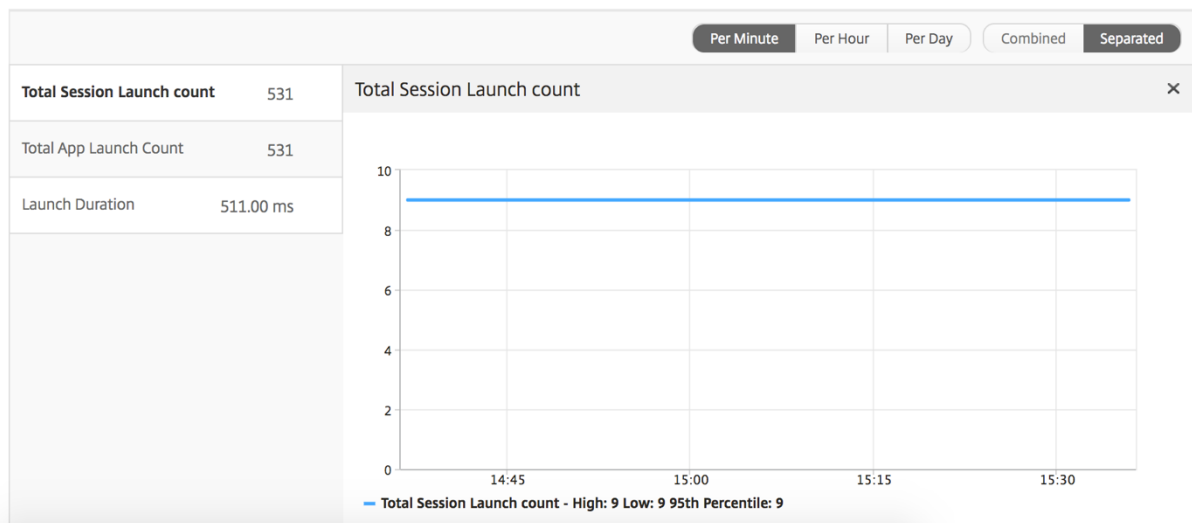
Active Applications			
Name	State	# Active Sessions	# Active Apps
Communicator	●	60	60
Fidelity	●	60	60
GoToMeeting	●	60	60
...	...	--	--

### Rapport sur les seuils

Le rapport sur les seuils représente le nombre de seuils dépassés 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 en courbes

Mesures	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 sur les 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 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.

Métriques	Description
Start Time	Heure de début de la session.
Temps d'activité	Durée de la session.
Adresse IP cliente	IP de l'utilisateur final.
Adresse IP du serveur	Adresse IP du serveur Backend/Citrix Virtual App.
Adresse IP NetScaler	IP de gestion NetScaler (NSIP).
Type de client	Type de récepteur - Citrix Windows Client, etc.
Version du client	Version du Receiver.
MSI	Boolean (Oui/Non). Indique si la session est multiflux ICA.
Reconnexions de session	Nombre de fois où la session s'est reconnectée.
Nb d'ACR	Nombre total de fois où un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, le mode utilisateur/transparent de Citrix Gateway.
Pays	Pays à partir duquel la session a été créée.
Région	Région à partir de laquelle la session a été créée.
City	Ville à partir de laquelle la session a été créée.
État de l'USB	Actif/Inactif -Vert/Rouge.
Nombre d'instances USB acceptées	Le nombre d'instances USB acceptées.
Nombre d'instances USB rejetées	Le nombre d'instances USB rejetées.
Nombre d'instances USB arrêtées	Le nombre d'instances USB arrêtées.
Nom d'hôte du client	Le nom d'hôte du client.
Nombre de basculements HA	Nombre de fois où le basculement HA s'est produit.
Motif de la résiliation	Affiche la raison de l'arrêt d'une session. Par exemple, délai d'expiration de session ICA, session terminée par l'utilisateur.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.

Métriques	Description
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	Le nom d'utilisateur de l'utilisateur accédant à cette Citrix Virtual Apps 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. Ces mesures sont utiles dans le cas où des périphériques non Citrix sont présents dans le chemin de remise.
Latence côté serveur L7	Latence L7 moyenne observée entre le périphérique NetScaler et Citrix Virtual Apps. Ces mesures sont utiles dans le cas où des périphériques non Citrix sont présents dans le chemin de remise.

Diagram	Session ID	Session Type	ICA RTT	Host Delay	Start Time	Up Time	Client IP Address	Server IP Address	NetScaler IP Address
	0000...000001	Application	<a href="#">1.012 s</a>	2.00 ms	2017-6-12 15:39:58	0 h: 0 m: 59s	23.18.6.21	10.102.19.122	10.102.216.177
	0000...000001	Application	<a href="#">880 ms</a>	1.00 ms	2017-6-12 15:39:58	0 h: 0 m: 59s	1.2.16.12	10.102.60.50	10.102.216.219

### Vue par session d'application

L'affichage par session d'application affiche les rapports pour une session d'application sélectionnée particulière.

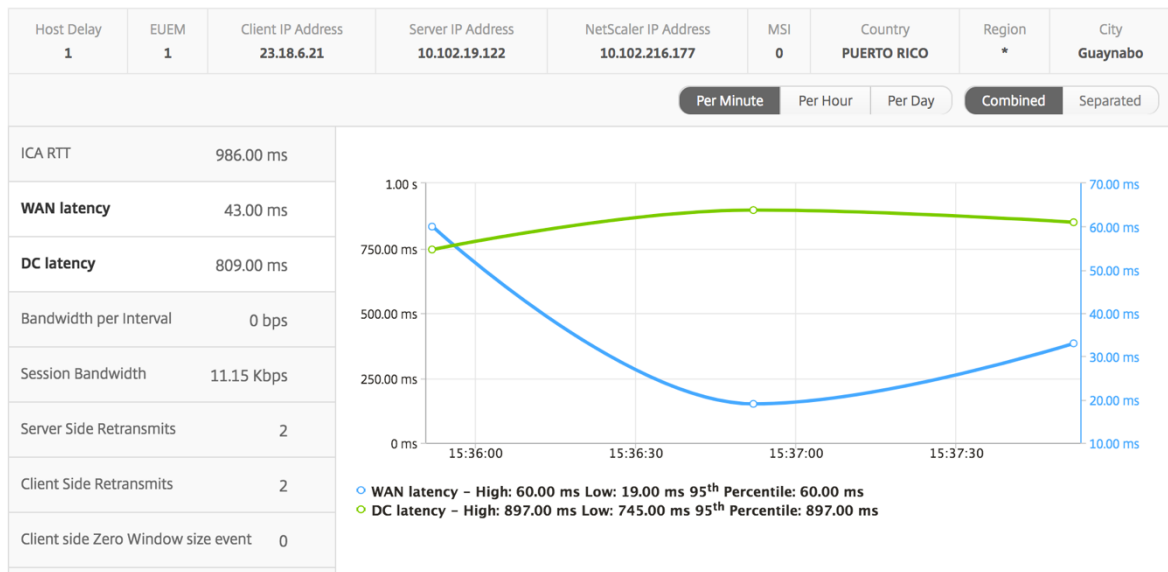
#### Pour afficher les rapports de session :

1. Accédez à **Analytics > HDX Insight > Applications**.
2. Sélectionnez un utilisateur particulier dans le rapport récapitulatif des applications.
3. Sélectionné une session à partir du rapport des sessions en cours.

### Graphique en courbes

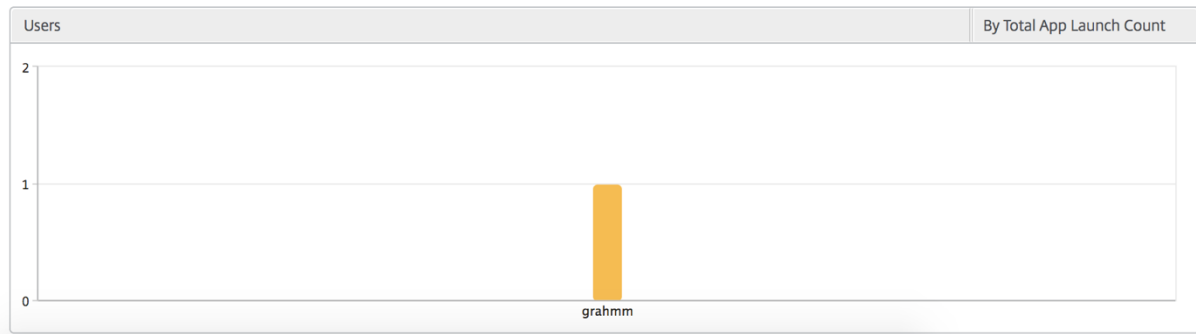
Mesures	Description
Reconnexions de session	Nombre de fois où la session s'est reconnectée.

Mesures	Description
Nb d'ACR	Nombre total de fois où un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.
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. Connectez-vous à votre Citrix ADM à l'aide d'un navigateur Web pris en charge.
2. Accédez à **Analytics > HDX Insight > Bureau** .



## Vue récapitulative

La vue récapitulative affiche les rapports de tous les Citrix Virtual Desktops qui sont connectés au cours de la chronologie sélectionnée.

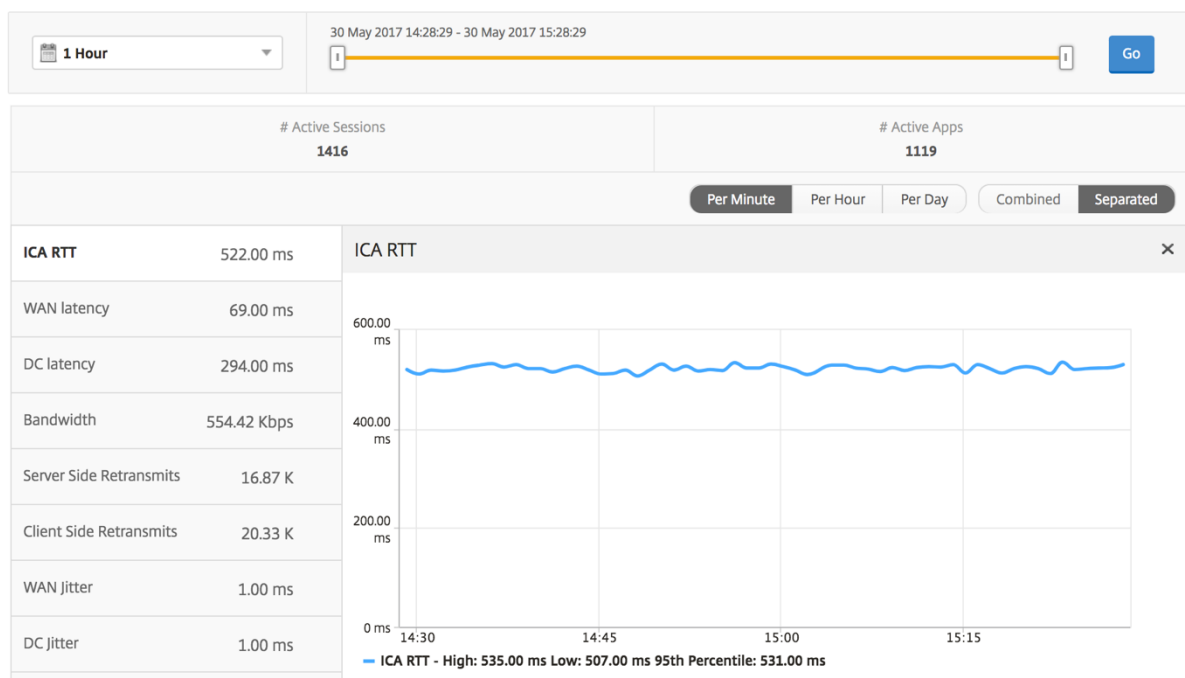
Toutes les métriques/rapports ci-dessous, sauf mention explicite, auront les valeurs qui leur correspondent pour la période sélectionnée.

## Graphique en courbes

---

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 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.

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.
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 des postes de travail

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.

Desktop Users							Search	
User Name	# Active Desktops	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes		
liam	60	1.00 s	56.00 ms	746.00 ms	9.27 Kbps	251.24 MB		
jayden	60	1.00 s	52.00 ms	746.00 ms	9.27 Kbps	251.34 MB		
juan	60	169.00 ms	32.00 ms	30.00 ms	9.26 Kbps	250.99 MB	WAN latency	
daniel	60	149.00 ms	31.00 ms	30.00 ms	9.26 Kbps	251.02 MB		
randyb	60	99.00 ms	11.00 ms	30.00 ms	9.26 Kbps	250.97 MB		

## 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

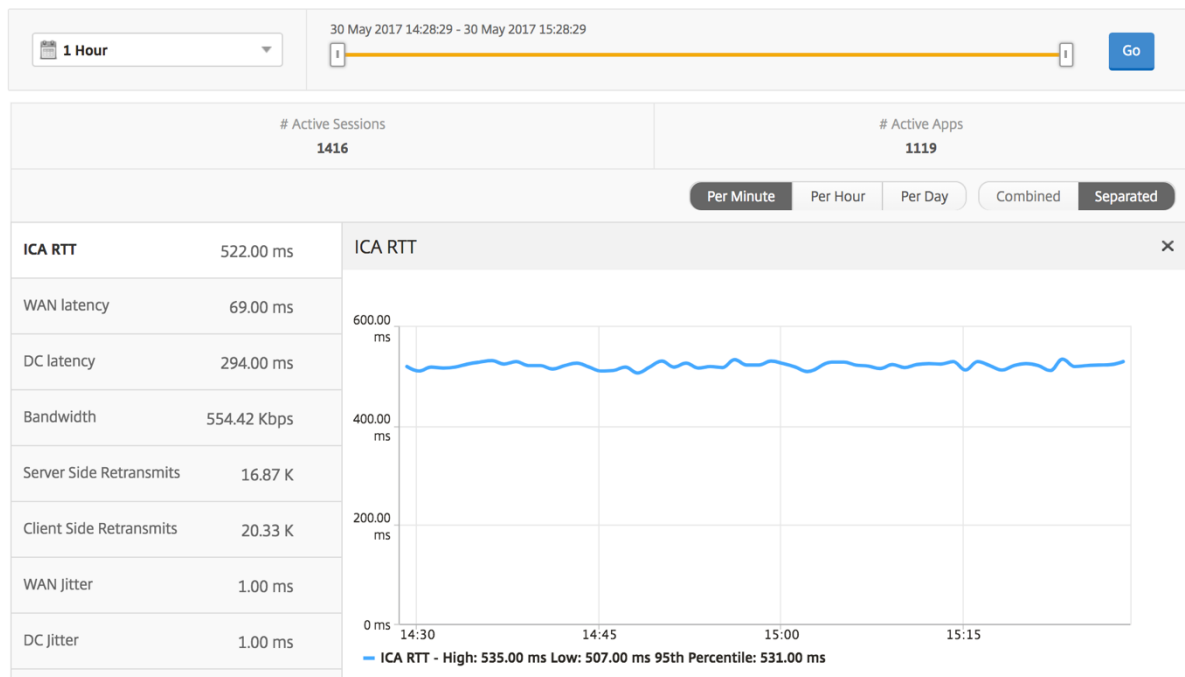
La vue par poste de travail fournit des rapports détaillés sur l'expérience utilisateur pour un Citrix Virtual Desktop sélectionné.

### 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 en courbes**

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 Citrix Virtual Apps actives.
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.

Desktop Users					By Desktop Launch Count ▾
Name	Desktop Launch Count ↑	Bandwidth	DC latency	WAN latency	ICA RTT
XenDesktop33	177	9.38 Kbps	749.00 ms	57.00 ms	1.00 s

### Rapport sur les postes de travail actifs/inactifs

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 de récepteur - Citrix Windows Client, etc.
Version du client	Version du Receiver.
MSI	Boolean (Oui/Non). Indique si la session est mult flux ICA.
Reconnexions de session	Nombre de fois où la session s'est reconnectée.
Nb d'ACR	Nombre total de fois où un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.

---

Mesures	Description
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, le mode utilisateur/transparent de Citrix Gateway.
Pays	Pays à partir duquel la session a été créée.
Région	Région à partir de laquelle la session a été créée.
City	Ville à partir de laquelle la session a été créée.
État de l'USB	Actif/Inactif -Vert/Rouge.
Nombre d'instances USB acceptées	Le nombre d'instances USB acceptées.
Nombre d'instances USB rejetées	Le nombre d'instances USB rejetées.
Nombre d'instances USB arrêtées	Le nombre d'instances USB arrêtées.
Nom d'hôte du client	Le nom d'hôte du client.
Nombre de basculements HA	Nombre de fois où le basculement HA s'est produit.
Motif de la résiliation	Affiche la raison de l'arrêt d'une session. Par exemple, délai d'expiration de session ICA, session terminée par l'utilisateur.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de 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

User Desktops Active								By Bandwidth per Interval	
Diagram	Session ID	VDI Image Name	ICA RTT	WAN latency	DC latency	Host Delay	Bandwidth per Interval	Session Bandwidth	Total B
	0000...000001	XenDesktop33	1.094 s	48.00 ms	767 ms	5.00 ms	12.87 Kbps	12.87 Kbps	1.63
	0000...000001	XenDesktop33	1.007 s	37.00 ms	691 ms	4.00 ms	9.27 Kbps	9.27 Kbps	1.35
	0000...000001	XenDesktop33	0.941 s	53.00 ms	747 ms	5.00 ms	8.30 Kbps	8.30 Kbps	1.25

**Vue par session de bureau**

La vue par session de bureau fournit des rapports pour une session Citrix Virtual Desktops sélectionnée.

**Pour accéder à la vue de session Bureau :**

1. Accédez à **Analytics > HDX Insight > Bureau** .
2. Sélectionnez un poste de travail particulier dans le **rapport récapitulatif des postes** de travail.
3. Sélectionnez une session dans le rapport des sessions en cours.

**Graphique chronologique**

La vue par session utilisateur fournit des rapports pour la session d'un utilisateur sélectionné particulier.

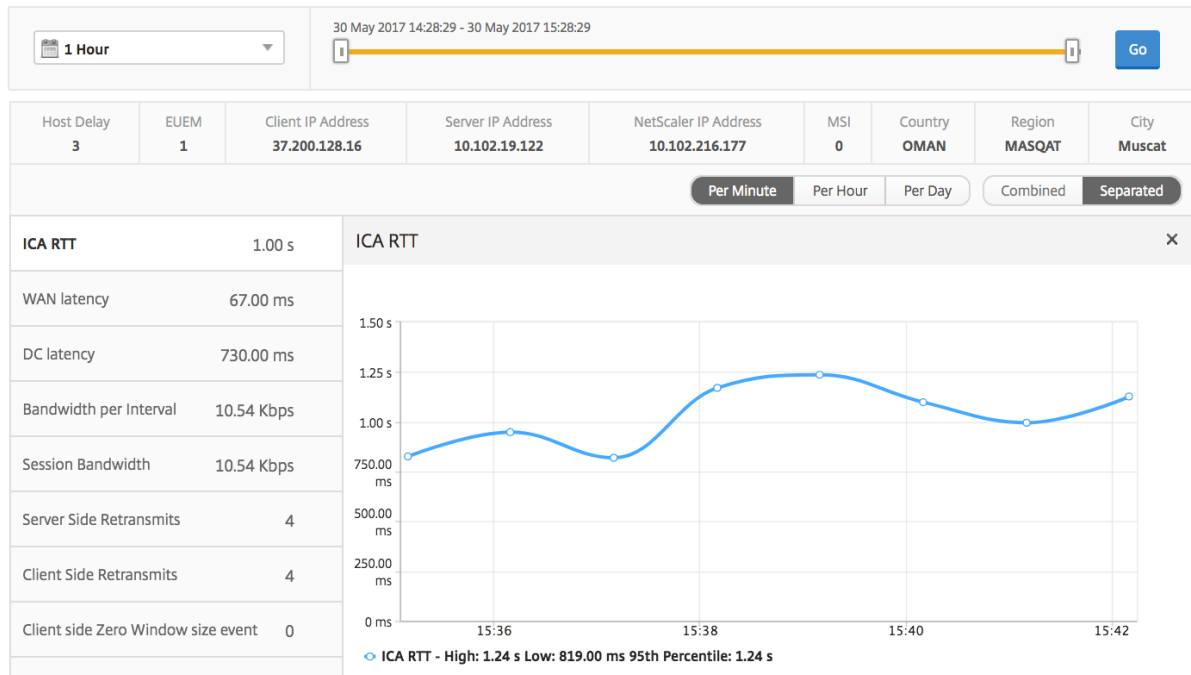
**Pour afficher les mesures de la session d'un utilisateur sélectionné :**



1. Accédez à **Analytics > HDX Insight > Utilisateurs**.
2. Select un utilisateur particulier dans la section **Rapport récapitulatif de l'utilisateur**.
3. Sélectionnez une session dans la colonne **Sessions en cours** ou **Sessions terminées**.

Mesures	Description
Reconnexions de session	Ce nombre indique le nombre de sessions Citrix Virtual Apps and Desktops actives.
Nb d'ACR	Ce nombre indique le nombre de sessions Citrix Virtual Apps actives.
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 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.



### Rapport sur les sessions de bureau associées

Les mesures suivantes peuvent être triées en fonction de la bande passante par intervalle, des reconnections 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.

---

Mesures	Description
Octets par intervalle	Nombre d'octets consommés par la session pendant cet intervalle de temps particulier.
Start Time	Heure de début de la session.
Temps d'activité	Durée de la session.
Adresse IP cliente	IP de l'utilisateur final.
Adresse IP du serveur	Adresse IP du serveur Backend/Citrix Virtual App.
Adresse IP NetScaler	IP de gestion NetScaler (NSIP).
Type de client	Type de récepteur - Citrix Windows Client, etc.
Version du client	Version du Receiver.
MSI	Boolean (Oui/Non). Indique si la session est multiflux ICA.
Reconnexions de session	Nombre de fois où la session s'est reconnectée.
Nb d'ACR	Nombre total de fois où un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, le mode utilisateur/transparent de Citrix Gateway.
Pays	Pays à partir duquel la session a été créée.
Région	Région à partir de laquelle la session a été créée.
City	Ville à partir de laquelle la session a été créée.
État de l'USB	Actif/Inactif -Vert/Rouge.
Nombre d'instances USB acceptées	Le nombre d'instances USB acceptées.
Nombre d'instances USB rejetées	Le nombre d'instances USB rejetées.
Nombre d'instances USB arrêtées	Le nombre d'instances USB arrêtées.
Nom d'hôte du client	Le nom d'hôte du client.
Nombre de basculements HA	Nombre de fois où le basculement HA s'est produit.
Motif de la résiliation	Affiche la raison de l'arrêt d'une session. Par exemple, délai d'expiration de session ICA, session terminée par l'utilisateur.

Mesures	Description
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de 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

User Desktops Active									
Diagram	Session ID	VDI Image Name	ICA RTT	WAN latency	DC latency	Host Delay	Bandwidth per Interval	Session Bandwidth	Total B
	0000...000001	XenDesktop33	<a href="#">1.094 s</a>	48.00 ms	767 ms	5.00 ms	12.87 Kbps	12.87 Kbps	1.63
	0000...000001	XenDesktop33	<a href="#">1.007 s</a>	37.00 ms	691 ms	4.00 ms	9.27 Kbps	9.27 Kbps	1.35
	0000...000001	XenDesktop33	<a href="#">0.94 s</a>	53.00 ms	747 ms	5.00 ms	8.38 Kbps	8.38 Kbps	1.35

## Afficher les rapports et les mesures de l'utilisateur

February 1, 2024

Les rapports et les mesures de cette vue sont affichés par utilisateur de Citrix Virtual Apps and Desktops.

### Pour accéder à la vue Utilisateurs :

1. Connectez-vous à votre Citrix ADM à l'aide d'un navigateur Web pris en charge.
2. Accédez à **Analytics > HDX Insight > Utilisateurs**

### Vue récapitulative

La vue récapitulative affiche les rapports de tous les utilisateurs qui se sont connectés au cours de la chronologie sélectionnée. Toutes les métriques/rapports de cette vue affichent les valeurs qui leur correspondent pour la période sélectionnée, sauf indication contraire.

### Pour modifier la période sélectionnée :

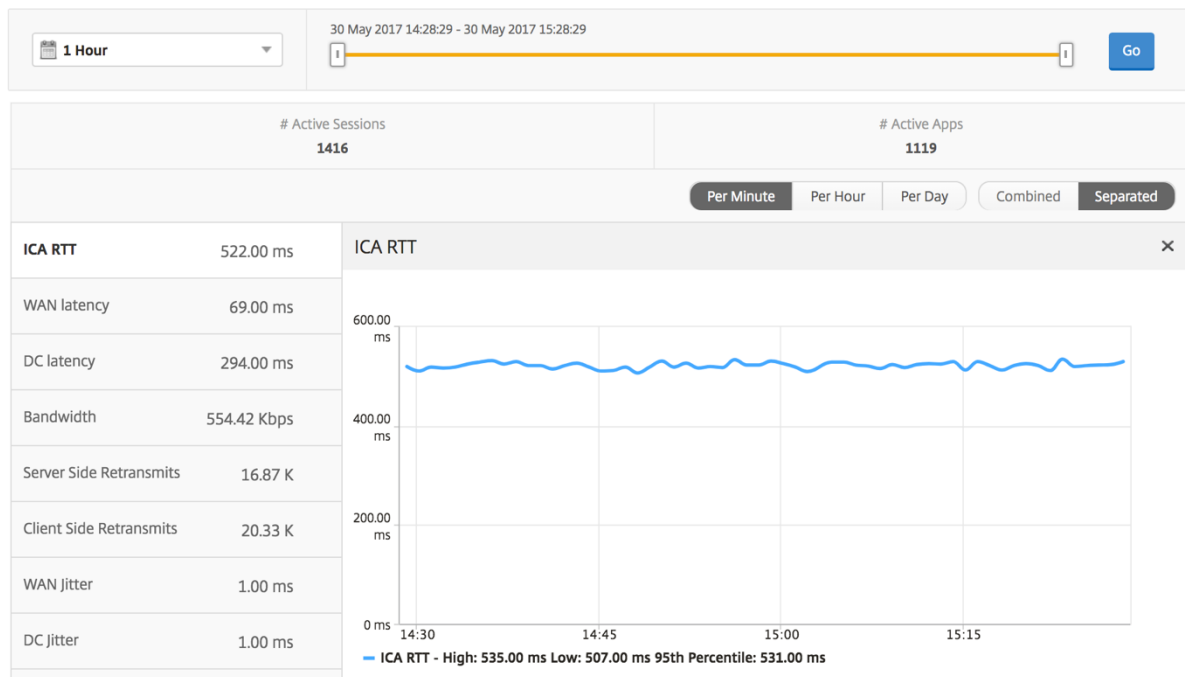
1. Utilisez la liste déroulante de la période ou le curseur temporel pour définir l'intervalle de temps souhaité.
2. Cliquez sur **OK**.

### Graphique en courbes

---

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 Citrix Virtual Apps actives.
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.

Mesures	Description
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 de synthèse 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	L'ICA RTT est le décalage d'écran que l'utilisateur rencontre lorsqu'il interagit avec une application ou un poste de travail hébergé 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	Nombre total d'octets par seconde pris pour la communication de bout en bout pendant l'intervalle de temps sélectionné.

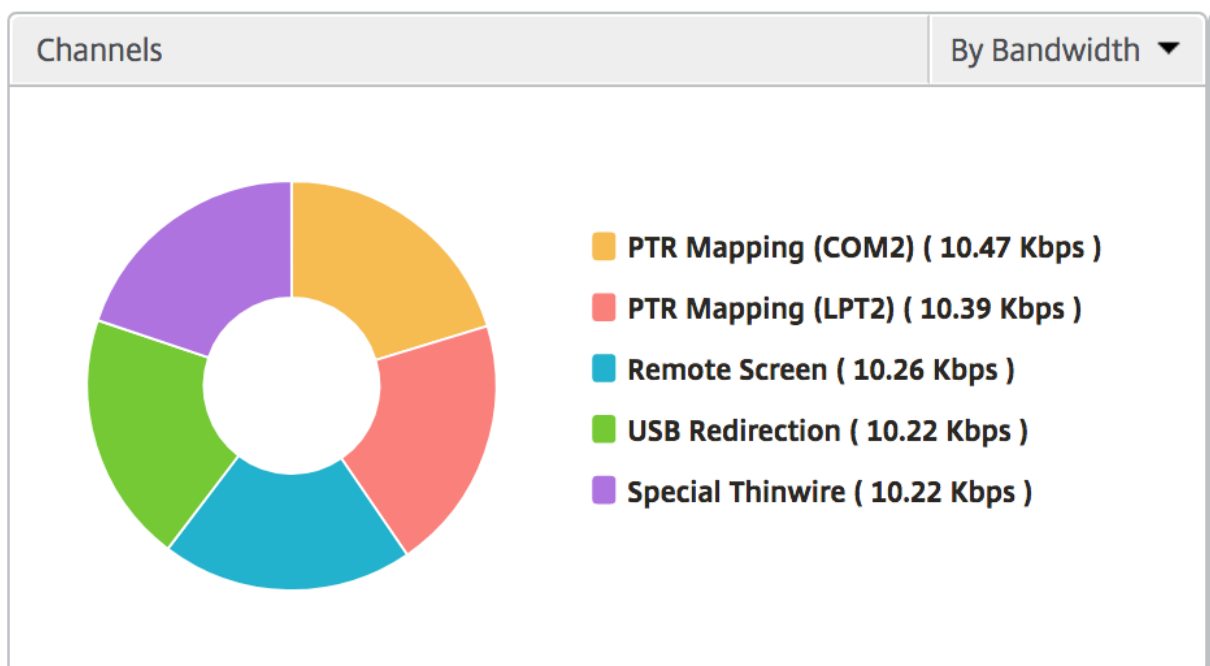
Mesures	Description
Retransmissions côté serveur	Nombre de paquets retransmis lors de la connexion entre NetScaler et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis lors de la connexion entre NetScaler et l'utilisateur final. Une valeur élevée de cette mesure ne signifie 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									
User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT	WAN latency	DC latency	Bandwidth	Server Side Retransmits	Client Side Retransmits
liam	59	59	118	999.00 ms	57.00 ms	751.00 ms	47.25 Kbps	3.74 K	0
jayden	59	59	118	999.00 ms	52.00 ms	751.00 ms	47.06 Kbps	3.71 K	0
florinl	59	0	59	997.00 ms	52.00 ms	754.00 ms	23.66 Kbps	1.88 K	0
ramas	59	0	59	997.00 ms	778.00 ms	1.00 ms	7.03 Kbps	0	0
omerp	59	0	59	997.00 ms	57.00 ms	754.00 ms	23.80 Kbps	1.89 K	0
grahmm	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.80 Kbps	1.89 K	0
ryan	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.69 Kbps	1.88 K	0
rajivs	59	0	59	801.00 ms	11.00 ms	1.00 ms	23.97 Kbps	0	0
alexisc	117	0	118	622.00 ms	56.00 ms	392.00 ms	47.67 Kbps	1.88 K	0
juan	59	59	118	169.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	0
lennoxl	59	0	59	169.00 ms	31.00 ms	30.00 ms	23.86 Kbps	0	0
daniel	59	59	118	149.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	0
woojunek	58	0	59	149.00 ms	31.00 ms	30.00 ms	23.85 Kbps	0	0
parkerf	59	0	59	149.00 ms	31.00 ms	30.00 ms	23.88 Kbps	0	0
randyby	59	59	118	99.00 ms	11.00 ms	29.00 ms	47.71 Kbps	0	0
bradp	177	0	177	74.00 ms	27.00 ms	1.00 ms	71.75 Kbps	0	0

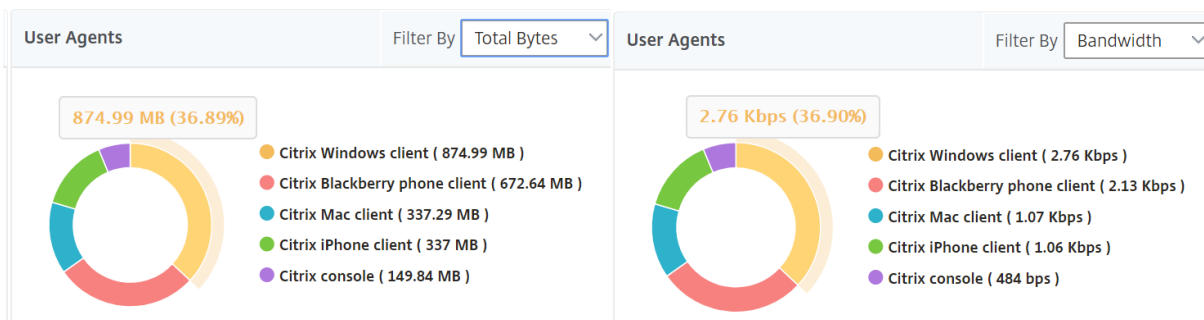
### Canaux

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 utilisateur

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 de seuils

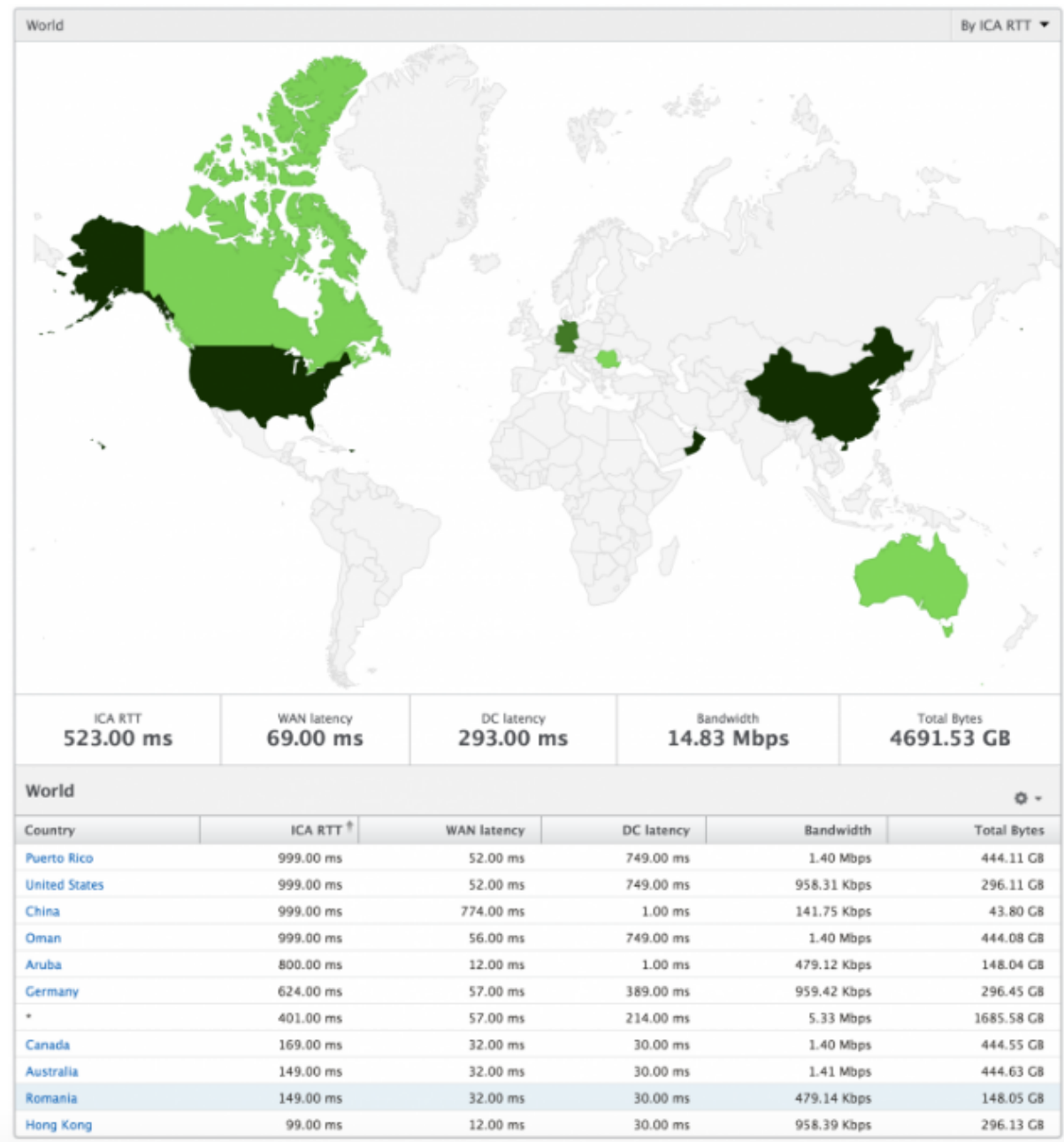
Les mesures de nombre de violations des seuils représentent le nombre de seuils violés au cours de la période sélectionnée. Pour plus d'informations, découvrez [comment créer des seuils et des alertes](#).

## 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 simplement sur la région. Les administrateurs peuvent approfondir leurs recherches pour afficher les informations par ville et par État. À partir de Citrix ADM version 12.0 et ultérieure, vous pouvez effectuer une exploration vers le bas vers les utilisateurs connectés à partir d'un emplacement Geo.

Les détails suivants peuvent être visualisés sur la carte du monde dans HDX Insight, 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



### 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. Accédez à **Analytics > HDX Insight > Utilisateurs**.
2. Sélectionnez un utilisateur particulier dans le rapport récapitulatif Utilisateurs.

## Graphique en courbes

Le graphique en courbes affiche le résumé de toutes les mesures pour l'utilisateur sélectionné particulier pendant la période sélectionnée.

## Rapport sur les sessions en cours ou 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, reconnections 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 de récepteur - Citrix Windows Client, etc.
Version du client	Version du Receiver.
MSI	Boolean (Oui/Non). Indique si la session est multiflux ICA.
Reconnections de session	Nombre de fois où la session s'est reconnectée.
Nb d'ACR	Nombre total de fois où un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.

---

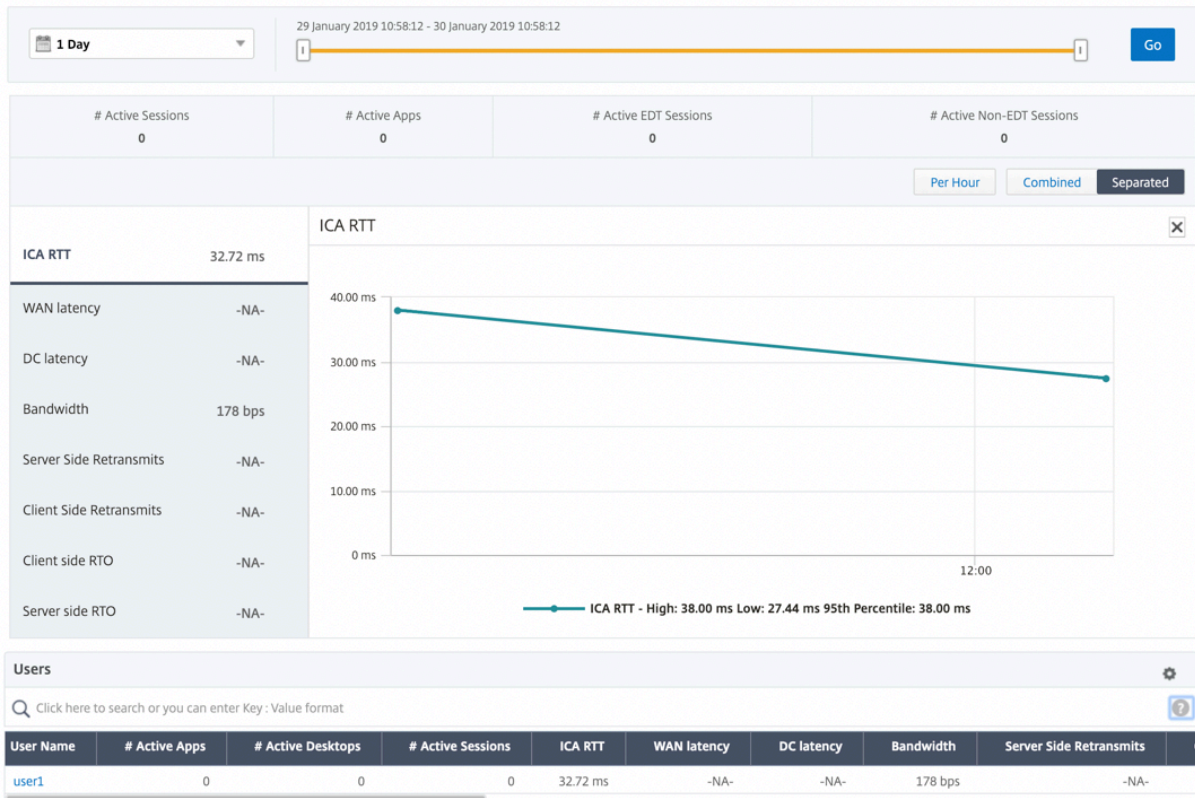
Mesures	Description
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, le mode utilisateur/transparent de Citrix Gateway.
Pays	Pays à partir duquel la session a été créée.
Région	Région à partir de laquelle la session a été créée.
City	Ville à partir de laquelle la session a été créée.
État de l'USB	Actif/Inactif -Vert/Rouge.
Nombre d'instances USB acceptées	Le nombre d'instances USB acceptées.
Nombre d'instances USB rejetées	Le nombre d'instances USB rejetées.
Nombre d'instances USB arrêtées	Le nombre d'instances USB arrêtées.
Nom d'hôte du client	Le nom d'hôte du client.
Nombre de basculements HA	Nombre de fois où le basculement HA s'est produit.
Motif de la résiliation	Affiche la raison de l'arrêt d'une session. Par exemple, délai d'expiration de session ICA, session terminée par l'utilisateur.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps and Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire de 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.

### Prise en charge de l'EDT dans HDX Insight

Citrix Application Delivery Management (ADM) prend désormais en charge le transport de données éclairé (EDT) pour afficher les analyses pour HDX Insight. En d'autres termes, ADM prend désormais en charge les protocoles UDP et TCP. La prise en charge d'EDT pour Citrix Gateway garantit une expérience utilisateur haute définition en session des bureaux virtuels pour les utilisateurs exécutant Citrix Receiver.

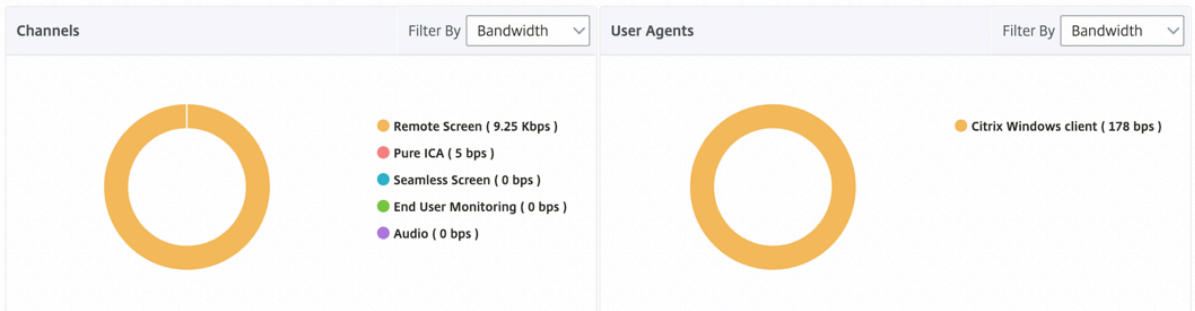
HDX Insight affiche désormais le nombre de sessions EDT et de sessions non EDT dans le rapport des sessions actives. Le tableau Utilisateurs affiche un rapport détaillé de tous les utilisateurs du système. Le tableau présente des mesures telles que la latence WAN, la latence DC, les retransmissions, les RTO et certaines de ces mesures ne sont pas disponibles pour les utilisateurs qui ont des sessions EDT car elles sont calculées à partir de la pile TCP actuellement. Par conséquent, ils apparaîtront sous la forme « NA ».



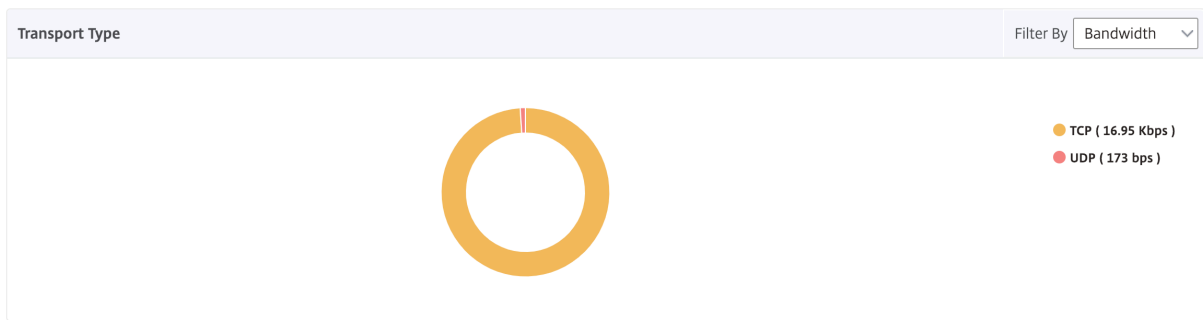
Users

Click here to search or you can enter Key : Value format

User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT	WAN latency	DC latency	Bandwidth	Server Side Retransmits
user1	0	0	0	32.72 ms	-NA-	-NA-	178 bps	-NA-



Un nouveau graphique en anneau a été introduit pour vous permettre de voir la bande passante consommée par l'utilisateur ainsi que le nombre total d'octets en fonction du type de protocole utilisé par les utilisateurs.



**Mesures HDX Insight disponibles à partir de Citrix ADM 12.0 et versions ultérieures :**

Latence côté client L7	Latence L7 moyenne observée entre le client ICA et l'instance NetScaler. Ces mesures sont utiles dans le cas où des périphériques non Citrix sont présents dans le chemin de remise.
Latence côté serveur L7	Latence L7 moyenne observée entre l'appareil NetScaler et l'application virtuelle Citrix. Ces mesures sont utiles dans le cas où des périphériques non Citrix sont 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.

Current Sessions									
Diagram	Session ID	Total Bytes	Bandwidth per Interval	Session Type	ICA RTT	Bytes per Interval	WAN latency	DC latency	Host Delay
	0000...000001	209.84 KB	11.58 Kbps	Application	854 ms	209.84 KB	83.00 ms	771 ms	4.00 ms
	0000...000001	127.18 KB	40.70 Kbps	Application	848 ms	127.18 KB	65.00 ms	710 ms	4.00 ms

Terminated Sessions								
Session ID	Session Type	ICA RTT	WAN latency	DC latency	Bandwidth per Interval	Session Bandwidth	Total Bytes	Bytes per Interval
0000...000001	Application	1.01 s	59.00 ms	763.00 ms	9.40 Kbps	9.40 Kbps	1.38 MB	1.38 MB
0000...000001	Desktop	971.00 ms	59.00 ms	733.00 ms	8.82 Kbps	8.82 Kbps	1.29 MB	1.29 MB
0000...000001	Application	998.00	51.00 ms	732.00 ms	9.91 Kbps	9.91 Kbps	1.45 MB	1.45 MB



## Utilisateurs de bureau

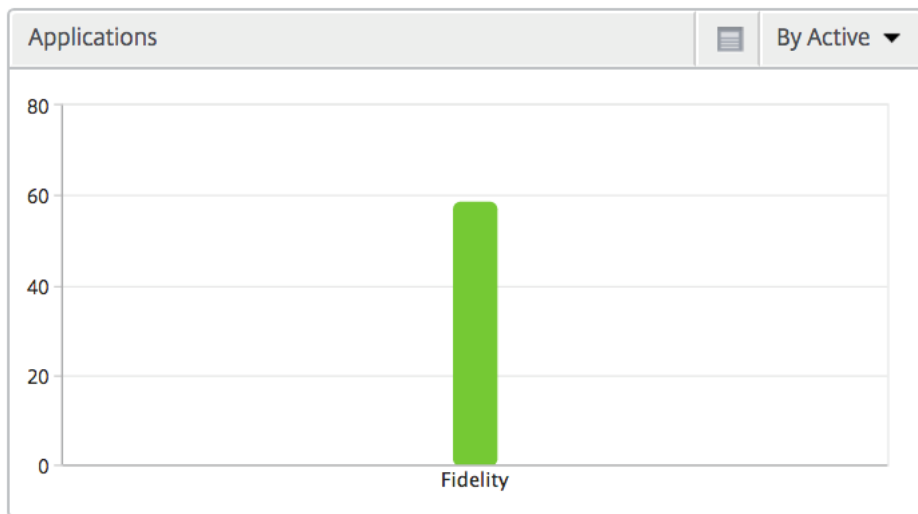
Ce tableau donne un aperçu des sessions Citrix Virtual Desktop pour un utilisateur particulier. Ces mesures peuvent être triées par nombre de lancements de postes de travail et bande passante.

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 and Desktops respectivement.

Desktop Users						By Desktop Launch Count ▾
Name	Desktop Launch Count ↕	Bandwidth	DC latency	WAN latency	ICA RTT	
XenDesktop33	177	9.38 Kbps	749.00 ms	57.00 ms	1.00 s	

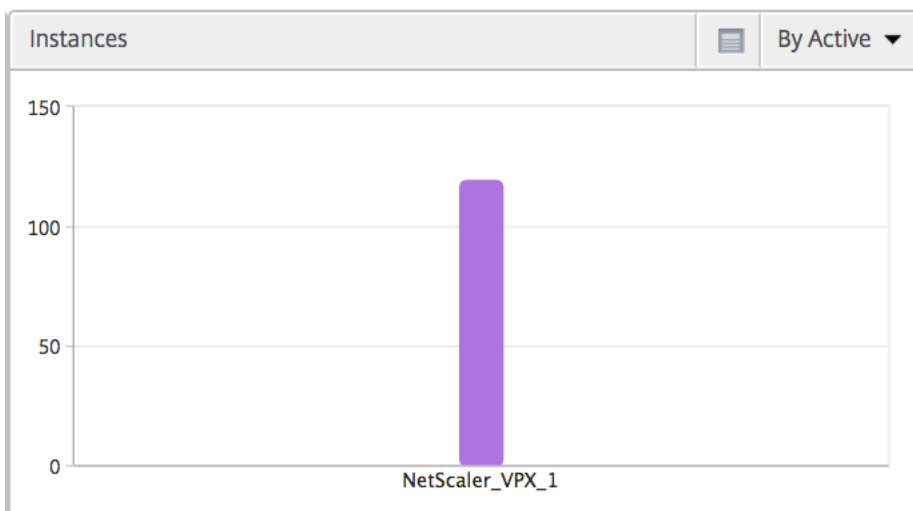
## Applications

Un graphique à barres représentant les applications triées par Actif, le nombre total de sessions lancées, le nombre total de lancements d'applications et la durée de lancement.



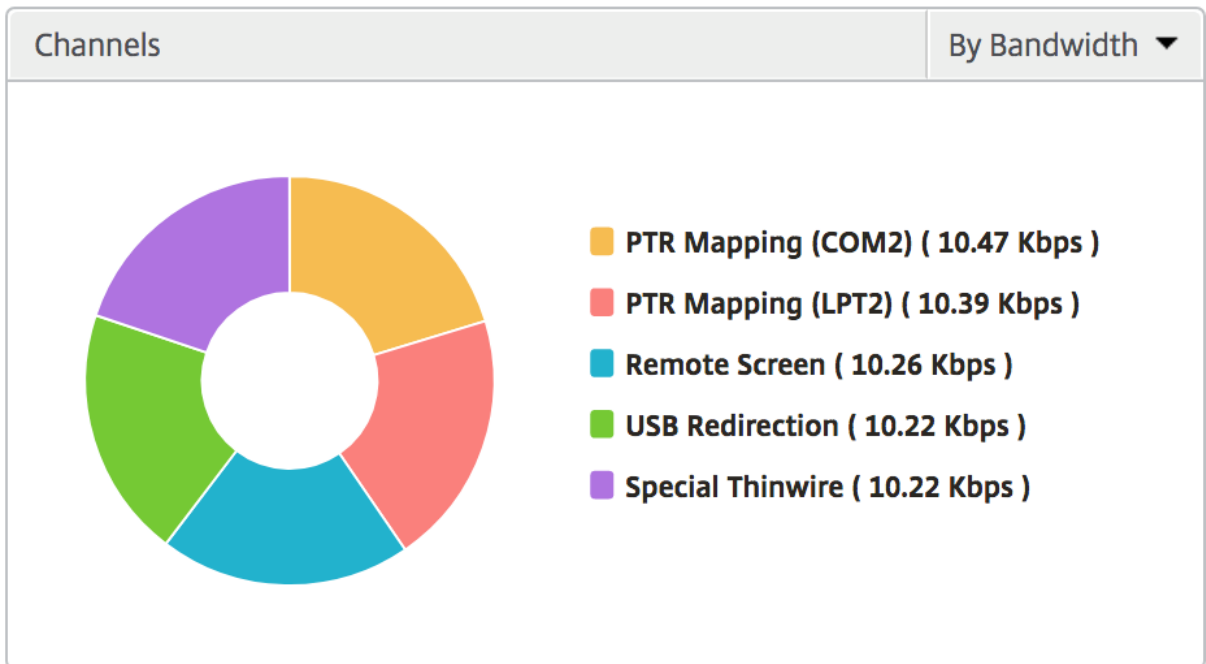
### Instances

Un graphique à barres représentant les instances NetScaler triées par applications actives et par nombre total d'applications



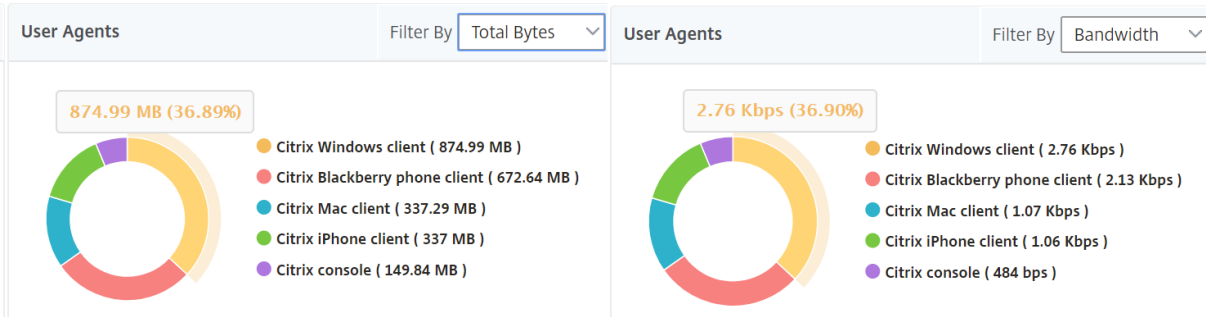
### Canaux

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 utilisateur

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.



### Vue par session utilisateur

La vue par session utilisateur fournit des rapports pour la session d'un utilisateur sélectionné particulier.

#### Pour afficher les mesures de la session d'un utilisateur sélectionné :

1. Accédez à **Analytics > HDX Insight > Utilisateurs**.
2. Select un utilisateur particulier dans la section **Rapport récapitulatif de l'utilisateur**.

3. Sélectionnez une session dans la colonne **Sessions en cours** ou **Sessions terminées** .

### Graphique chronologique

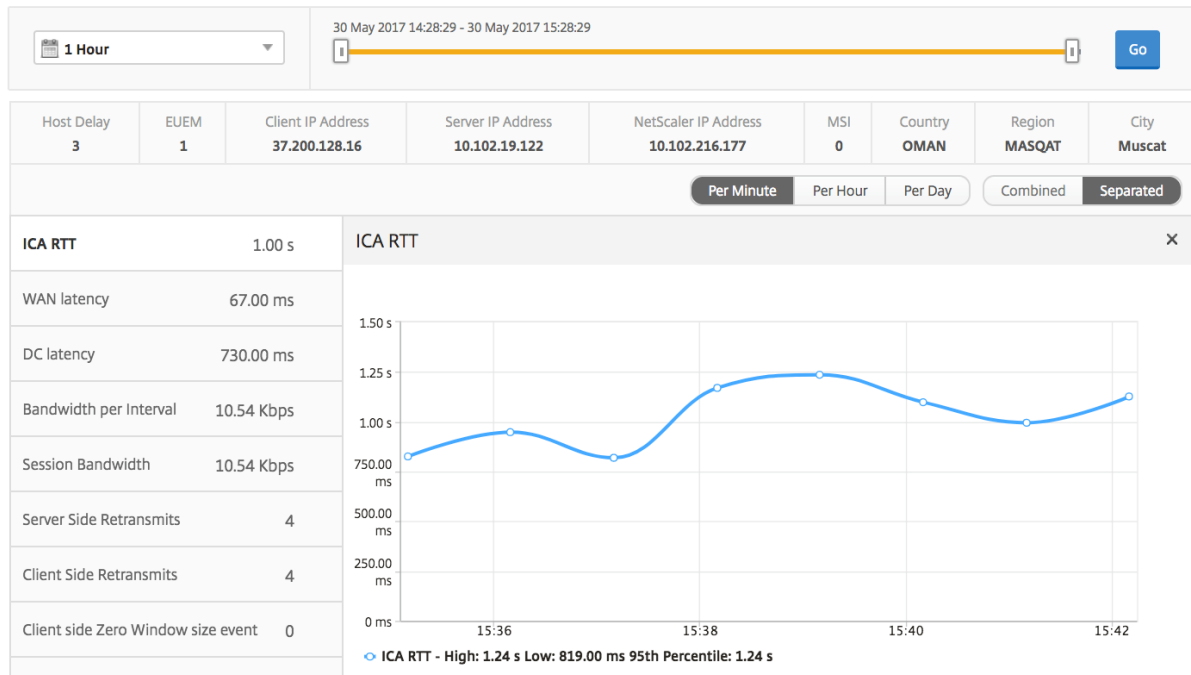
Mesures	Description
Reconnexions de session	Ce nombre indique le nombre de sessions Citrix Virtual Apps and Desktops actives.
Nb d'ACR	Ce nombre indique le nombre de sessions actives de Citrix Virtual App.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec 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 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.

Active Applications				By # Active Sessions
Name	# Active Sessions	Launch Duration	# Active Apps	
Fidelity	1	557.00 ms	1	

**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.

Related Sessions										By Common Server
Session ID	Session Type	User Name	State	ICA RTT	WAN latency	DC latency	Bandwidth per Interval	Total Bytes	Total Bytes	Bytes
0000...000001	Application	grahmm	●	<a href="#">1.021 s</a>	51.00 ms	737 ms	9.26 Kbps	9.26 Kbps	977.73 KB	
0000...000001	Application	liam	●	<a href="#">955 ms</a>	50.00 ms	733 ms	10.91 Kbps	10.91 Kbps	1.26 MB	
0000...000001	Application	qrahmm	●	<a href="#">1.058 s</a>	38.00 ms	817 ms	10.27 Kbps	10.27 Kbps	367.24 KB	

## Rapports et mesures d’affichage d’instance

February 1, 2024

Les rapports et les mesures de la vue d’instance sont centrés sur les instances NetScaler.

### Pour accéder à la vue Instance :

1. Connectez-vous à votre Citrix ADM à l’aide d’un navigateur Web pris en charge.
2. Accédez à **Analytics > HDX Insight > Instances**.

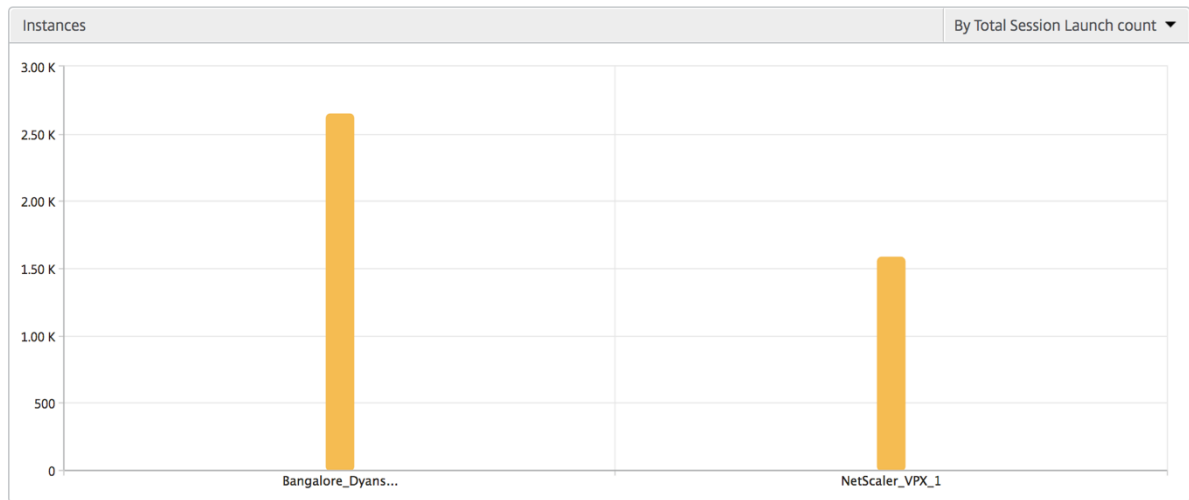
### Vue récapitulative de l’instance

Cette vue est appelée vue récapitulative car elle affiche les rapports de toutes les instances NetScaler ajoutées à Citrix ADM.

Toutes les métriques/rapports ci-dessous, sauf mention explicite, auront les valeurs qui leur correspondent pour la période sélectionnée.

### Graphique à barres d’instance

Ce graphique affiche l’instance par rapport au nombre total de lancement de session et au nombre total d’applications qui peuvent être sélectionnées dans la liste déroulante située en haut à droite sur ADCevas du graphique.



### Rapport récapitulatif des instances et des instances actives

Mesures	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
<a href="#">Bangalore_Dyansty(10.102.216.219)</a>	10.102.216.219	2.65 K	2.12 K	-NA-
<a href="#">NetScaler_VPX_1(10.102.216.177)</a>	10.102.216.177	1.59 K	1.24 K	-NA-

Active Instances					
Name	IP Address	# Active Sessions	# Active Apps	# Active Desktops	Type
<a href="#">NetScaler_VPX_1(10.102.216.177)</a>	10.102.216.177	538	417	120	-NA-
<a href="#">Bangalore_Dyansty(10.102.216.219)</a>	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, comme l'utilisation de versions non prises en charge de Citrix Virtual Apps and Desktops, d'une version non prise en charge d'un récepteur ou d'un type de récepteur, etc. Ce tableau indique l'adresse IP et le nombre de flux ignorés. Ces récepteurs peuvent ne pas faire partie des récepteurs de liste blanche ; par conséquent, ces sessions sont ignorées de la surveillance.

Veuillez visiter **Erreur! Référence du lien hypertexte non valide.** pour plus de détails sur les questions liées à l'analyse ICA.

Skipped Flows	
IP Address	Skipped Count
10.105.2.141	1
10.105.2.142	1

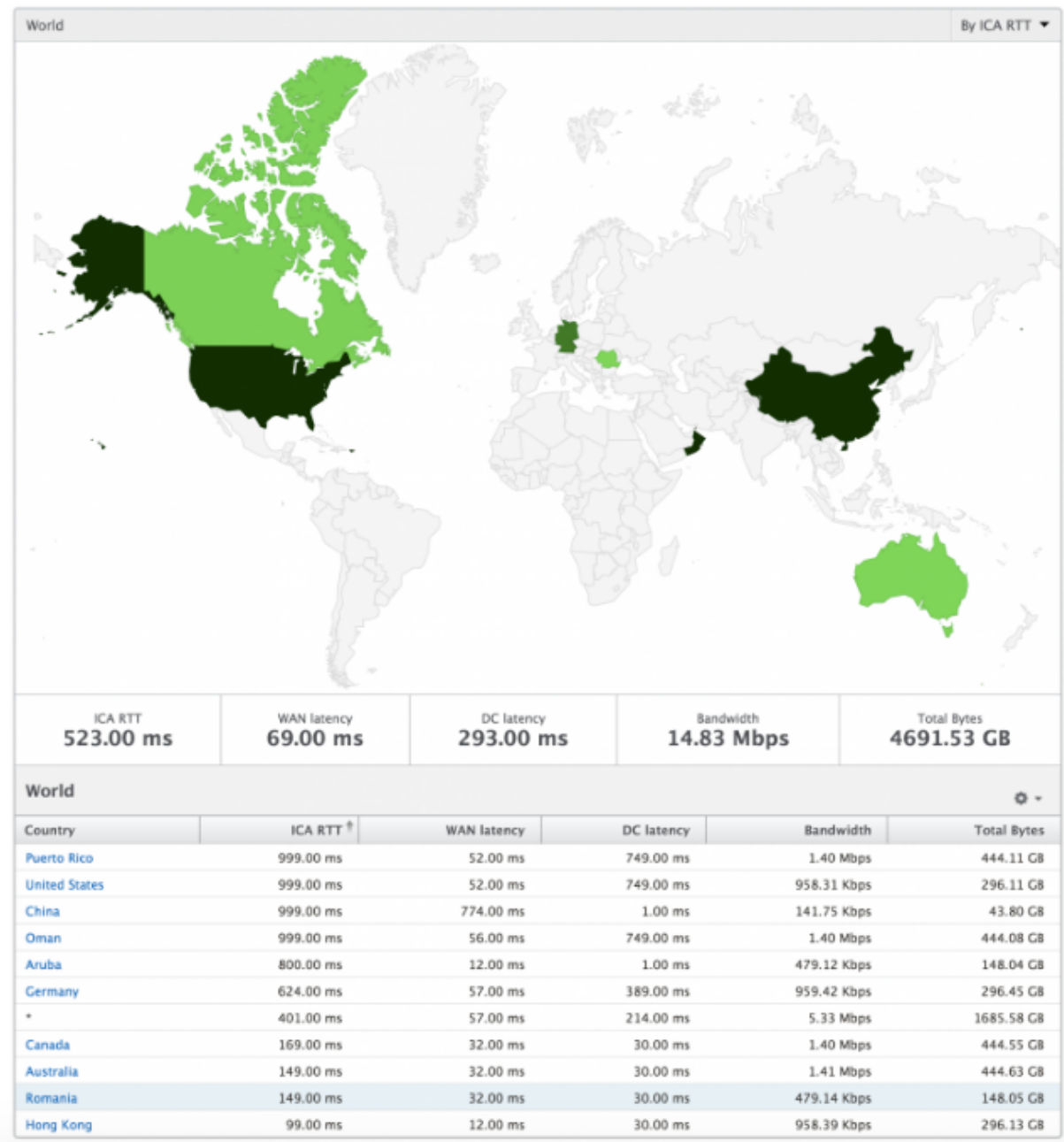
## Vue globale

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 leurs recherches pour afficher les informations par ville et par État. À partir de Citrix ADM version 12.0 et ultérieure, vous pouvez effectuer une exploration vers le bas vers les utilisateurs connectés à partir d'un emplacement Geo.

Les détails suivants peuvent être visualisés sur la carte du monde dans HDX Insight, 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





## Vue par instance

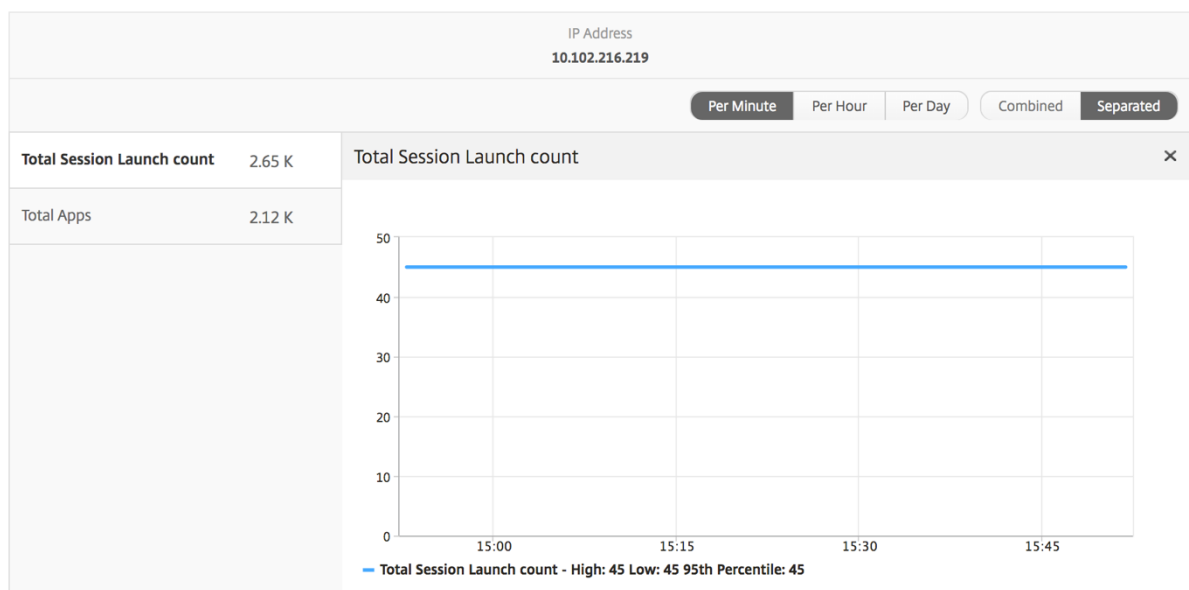
La vue par instance fournit des rapports détaillés sur l'expérience de l'utilisateur final pour une instance NetScaler sélectionnée en particulier.

### Pour accéder à la vue Instance :

1. Accédez à **Analytics > HDX Insight > Instances**.
2. Sélectionnez une instance particulière dans le **rapport Récapitulatif de l'instance**.

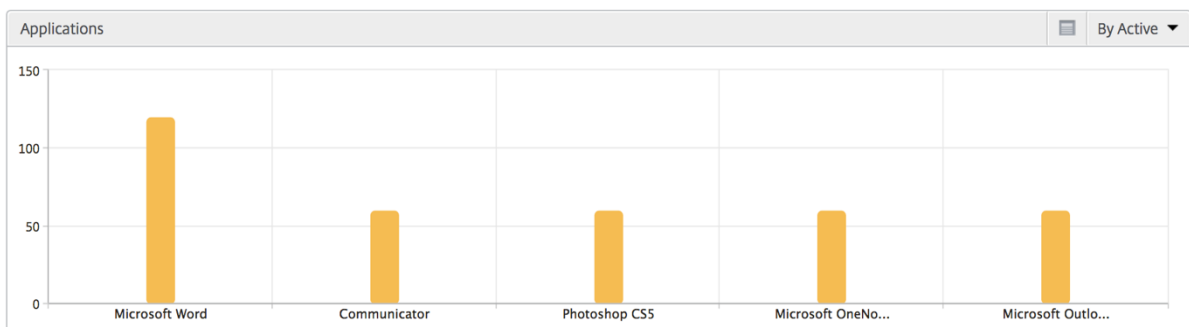
### Graphique en courbes

Mesures	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 Apps 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

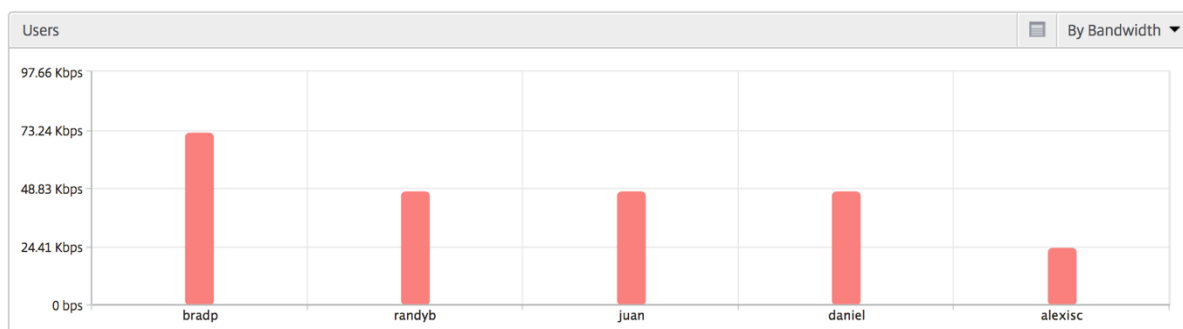
Affiche les 5 meilleures applications en fonction des critères suivants : par applications actives, nombre total de sessions lancées, nombre total de lancements d'applications ou durée de lancement.



## 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 and Desktops respectivement.

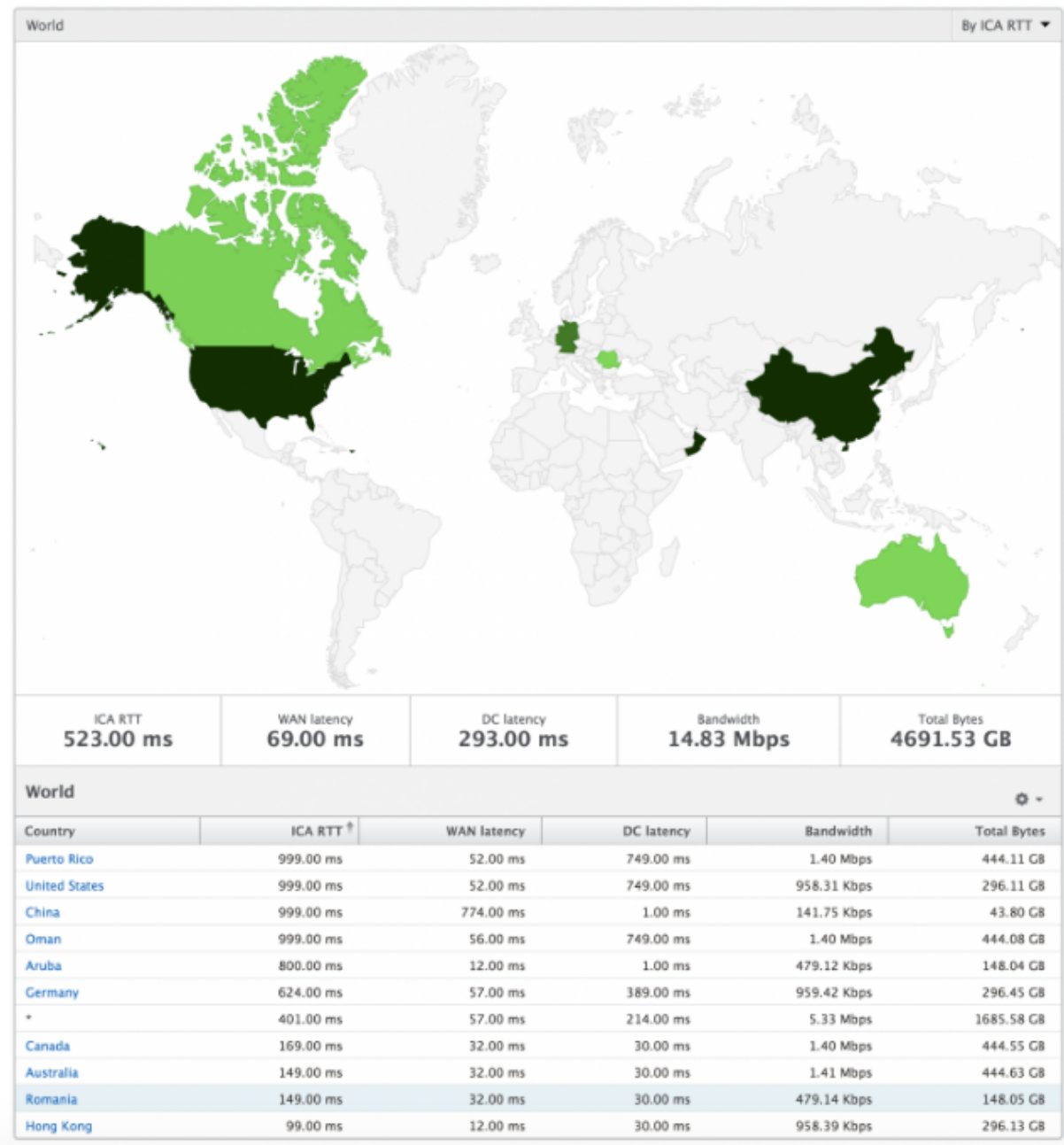
Desktop Users					By Desktop Launch Count ▾
Name	Desktop Launch Count ↕	Bandwidth	DC latency	WAN latency	ICA RTT
XenDesktop33	177	9.38 Kbps	749.00 ms	57.00 ms	1.00 s

### Vue globale

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 leurs recherches pour afficher les informations par ville et par État. À partir de Citrix ADM version 12.0 et ultérieure, vous pouvez effectuer une exploration vers le bas vers les utilisateurs connectés à partir d'un emplacement Geo.

Les détails suivants peuvent être visualisés sur la carte du monde dans HDX Insight, et la densité de chaque mesure est affichée sous la forme d'une carte thermique :

- RTT ICA
- Latence WAN
- Latence DC
- Bande passante
- Nb total d'octets



## Rapports et mesures d’affichage des licences

February 1, 2024

La vue de licence donne des détails sur les informations de licence Citrix Gateway.

**Pour accéder à la vue Licence :**

1. Connectez-vous à votre service NetScaler MA à l'aide d'un navigateur Web compatible.
2. Accédez à **Analytics > HDX Insight > Licences**.

## Graphique en courbes

---

Mesures	Description
Licences utilisées	Les licences CCU Citrix Gateway utilisées pendant la chronologie sélectionnée. Chaque nombre représente le nombre de sessions utilisateur. Cela est indépendant des sessions d'application et de bureau lancées par cet utilisateur.
Nombre total de licences	Nombre total de licences Citrix Gateway CCU disponibles pour le client.

---

! [image localisée] (/en-us/netscaler-application-delivery-management-software/media/hdx-line-chart.png)

## Rapport sur les seuils

Le rapport de seuil représente le nombre de seuils dépassés lorsque l'*entité* est sélectionnée en tant que Licence au cours de la période sélectionnée. Pour plus d'informations, consultez [comment créer des seuils et des alertes](#).

## Résoudre les problèmes HDX Insight

February 1, 2024

Si la solution HDX Insight ne fonctionne pas comme prévu, le problème peut provenir de l'un des éléments suivants. Reportez-vous aux listes de contrôle dans les sections correspondantes pour le dépannage.

- Configuration de HDX Insight.
- Connectivité entre Citrix ADC et Citrix ADM.
- Génération d'enregistrements pour le trafic HDX/ICA dans Citrix ADC.
- Population des enregistrements dans Citrix ADM.

## Liste de contrôle de configuration HDX Insight

- Assurez-vous que la fonctionnalité AppFlow est activée dans Citrix ADC. Pour plus de détails, consultez [Activation d'AppFlow](#).
- Vérifiez la configuration HDX Insight dans la configuration en cours d'exécution de Citrix ADC.  
Exécutez la `show running | grep -i <appflow_policy>` commande pour vérifier la configuration HDX Insight. Assurez-vous que le type de liaison est ICA REQUEST. Par exemple ;  
`bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST`  
Pour le mode transparent, le type de liaison doit être ICA\_REQ\_DEFAULT. Par exemple ;  
`bind appflow global afp 100 END -type ICA_REQ_DEFAULT`
- Pour le déploiement d'une passerelle d'accès ou d'un saut unique, assurez-vous que la stratégie HDX Insight AppFlow est liée au serveur virtuel VPN, où le trafic HDX/ICA circule.
- Pour le mode transparent ou le mode utilisateur LAN, assurez-vous que les ports ICA 1494 et 2598 sont définis.
- Vérifier le paramètre « appflowlog » dans Citrix Gateway ou le serveur virtuel VPN est activé pour Access Gateway ou le déploiement à double saut. Pour plus de détails, consultez [Activation d'AppFlow pour les serveurs virtuels](#).
- Cochez « Connection Chaining » est activé dans Citrix ADC double saut. Pour plus de détails, reportez-vous à la section [Configuration des dispositifs Citrix Gateway pour exporter des données](#).
- Après le basculement HA si les détails HDX Insight sont analysés, cochez le paramètre ICA « enableSRonHAFailover » est activé. Pour plus de détails, consultez la section [Fiabilité de session sur la paire haute disponibilité Citrix ADC](#).

## Liste de contrôle de la connectivité entre Citrix ADC et Citrix ADM

- Vérifiez l'état du collecteur AppFlow dans Citrix ADC. Pour de plus amples informations, consultez [Comment vérifier l'état de la connectivité entre Citrix ADC et AppFlow Collector](#).
- Vérifiez les hits de stratégie AppFlow HDX Insight.  
Exécutez la commande `show appflow policy <policy_name>` pour vérifier les accès à la stratégie AppFlow.  
Vous pouvez également accéder à **Système > AppFlow > Stratégies** dans l'interface graphique pour vérifier les accès à la stratégie AppFlow.
- Validez tout pare-feu bloquant les ports AppFlow 4739 ou 5557.

## Génération d'enregistrement pour le trafic HDX/ICA dans Citrix ADC

Exécutez la commande `tail -f /var/log/ns.log | grep -i "default ICA Message"` pour la validation du journal. En fonction des journaux générés, vous pouvez utiliser ces informations pour le dépannage.

- Journal : **connexion ICA d'analyse ignorée - HDX Insight non pris en charge pour cet hôte**  
**Cause** : Versions de Citrix Virtual Apps and Desktops non prises en charge  
**Solution** : mettez à niveau les serveurs Citrix Virtual Apps and Desktops vers une version prise en charge.
- Journal : **Type de client reçu 0x53, NON pris en charge**  
**Cause** : Version non prise en charge de l'application Citrix Workspace  
**Solution** : mettez à niveau Citrix Workspace App vers une version prise en charge. Pour plus d'informations, consultez [l'application Citrix Workspace](#).
- Journal : **Erreur de Expand Packet - Ignorer tout le traitement hdx pour ce flux**  
**Cause** : problème de décompression du trafic ICA  
**Solution** : Aucun rapport n'est disponible pour cette session ICA tant qu'une nouvelle session n'est pas établie.
- Journal : **Transition non valide : NS\_ICA\_ST\_FLOW\_INIT/NS\_ICA\_EVT\_INVALID -> NS\_ICA\_ST\_UNINIT**  
**Cause** : problème lors de l'analyse de la poignée de main ICA  
**Solution** : Aucun rapport n'est disponible pour cette session ICA en particulier tant qu'une nouvelle session n'est pas établie.
- Log : **RTT EUEM ICA manquant**  
**Cause** : Impossible d'analyser les données de canal de surveillance de l'expérience utilisateur final  
**Solution** : Assurez-vous que le service de surveillance de l'expérience utilisateur final est démarré sur les serveurs Citrix Virtual Apps and Desktops. Assurez-vous que vous utilisez les versions prises en charge de l'application Citrix Workspace.
- Journal : **en-tête de canal non valide**  
**Cause** : Impossible d'identifier l'en-tête du canal  
**Solution** : Aucun rapport n'est disponible pour cette session ICA en particulier tant qu'une nouvelle session n'est pas établie.



- Log : **code d'évitement**

Si vous voyez l'une des valeurs suivantes pour le code d'évitement, les détails Insight sont analysés.

Le code d'évitement 0 indique que l'enregistrement a été exporté avec succès depuis Citrix ADC.

Code d'évitement	Message d'erreur	Cause de l'erreur
100	NS_ICA_ERR_NULL_FRAG	Erreur lors de la gestion des fragments ICA, probablement en raison de conditions de mémoire
101	NS_ICA_ERR_INVALID_HS_CMD	Commande de prise de contact non valide reçue
102	NS_ICA_ERR_REduc_PARAM_CNT	Paramètre non valide spécifié pour l'initialisation de l'expandeur V3
103	NS_ICA_ERR_REduc_INIT	Impossible d'initialiser correctement le module d'extension V3
104	NS_ICA_ERR_REduc_PARAM_BYTES	Nombre d'octets insuffisant pour affecter un codeur à un canal
105	NS_ICA_ERR_INVALID_CHANNEL	Numéro de canal ICA non valide
106	NS_ICA_ERR_INVALID_DECODER	Décodeur non valide spécifié pour un canal
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_CODE	Codeur d'extension : Octets consommés plus que le nombre d'octets disponibles

Code d'événement	Message d'erreur	Cause de l'erreur
112	NS_ICA_ERR_REDUCE_BYTES_OOR	Erreur : dépassement de données non compressées
113	NS_ICA_ERR_REDUCE_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_REDUCE_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
122	NS_ICA_ERR_INSUFFICIENT_CHANNEL_BYTES	Nombre de 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_LEN	Longueur non valide détectée lors du traitement de données de canal ICA pures

Code d'événement	Message d'erreur	Cause de l'erreur
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	Header de canal incorrect détecté
130	NS_ICA_ERR_CGP_PARSE_RECONNECT_FAILED	Négociation de la session reconnectée a échoué
131	NS_ICA_ERR_DISABLE_SR_NON_SUPPORTED	SR désactivation de SR non prise en charge
132	NS_ICA_ERR_REDUCE_NOT_V3	Version du réducteur ICA non prise en charge
133	NS_ICA_ERR_HS_COMPRESSION_DISABLED	Compression désactivée, non respectée par l'hôte
134	NS_ICA_ERR_IDENT_PROTO	Impossible d'identifier le protocole ICA ou CGP, vu avec des récepteurs incorrects
135	NS_ICA_ERR_INVALID_SIGNATURE	Signature ICA ou chaîne magique incorrecte
136	NS_ICA_ERR_PARSE_RAW	Erreur lors de l'analyse du paquet de négociation ICA
137	NS_ICA_ERR_INCOMPLETE_PKT	Paquet incomplet reçu lors de la négociation
138	NS_ICA_ERR_ICAFRAME_TOO_LARGE	ICAFRAME 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

Code d'événement	Message d'erreur	Cause de l'erreur
142	NS_ICA_ERR_UNSUPPORTED_RECEIVER_VERSION	Erreur générée pour ce récepteur (client) car il n'est pas dans la liste blanche
143	NS_ICA_ERR_LOOKUP_RECONNECT_TIMEOUT	Impossible de détecter l'état d'analyse pour le cookie de reconnexion du client
144	NS_ICA_ERR_SYNCUP_RECONNECT_TIMEOUT	Longueur de cookie de reconnexion non valide détectée après la reconnexion du client
145	NS_ICA_ERR_INVALID_RECONNECT_COOKIE	Cookie de reconnexion du client a manqué la contrainte nécessaire
146	NS_ICA_ERR_INVALID_CLIENT_VERSION	Version de version de récepteur non valide reçue du client
147	NS_ICA_ERR_UNKNOWN_CLIENT_IP	Produit GUID 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_INSUFFBYTES	Octets insuffisants rencontrés pour une commande transparente
151	NS_ICA_ERR_EUEM_INSUFFBYTE	Nombre d'octets insuffisant pour la commande EUEM
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

Code d'événement	Message d'erreur	Cause de l'erreur
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_INVALID_STATE	État non valide pour une commande crypt dans le chiffrement de base
161	NS_ICA_ERR_BASICCRYPT_INVALID_CRYPTCMD	Commande crypt non valide dans le chiffrement de base
162	NS_ICA_ERR_ADVCRYPT_INVALID_STATE	État non valide pour une commande crypt dans le chiffrement RC5
163	NS_ICA_ERR_ADVCRYPT_INVALID_CRYPTCMD	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_REDUCED	Le serveur ne prend pas en charge Reducer version 3
167	NS_ICA_ERR_CLIENT_NOT_REDUCED	Le client ne prend pas en charge Reducer version 3
168	NS_ICA_ERR_ICAP_INSUFFBYTE	Nombre d'octets inattendu dans la poignée de main ICA
169	NS_ICA_ERR_HIGHER_RECONSEQ	Numéro de séquence de reprise CGP supérieur à partir de la reconnexion post-homologue
170	NS_ICA_ERR_DESCRINFO_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

Code d'évitement	Message d'erreur	Cause de l'erreur
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_TIMEOUT	Erreur lors de la récupération du ticket de reconnexion du service dans le nœud de service
180	NS_ICA_ERR_SN_HIGHER_RECONNECT_SEQ	Erreur lors de la réception d'un numéro de séquence de reconnexion supérieur dans le nœud
181	NS_ICA_ERR_DISABLE_HDXINSIGHT_NONNSAP	Erreur lors de la désactivation de HDXInsight pour les connexions non-NSAP

**Exemples de journaux :**

```
Jan 9 22:57:02 <local0.notice> 10.106.40.223 01/09/2020:22:57:02 GMT
ns-223 0-PPE-2 : default ICA Message 1234 0 : "Session setup data
send: Session GUID [57af35043e624abab409f5e6af7fd22c], Client IP/
Port [10.105.232.40/52314], Server IP/Port [10.106.40.215/2598], MSI
Client Cookie [Non-MSI], Session setup time [01/09/2020:22:56:49
GMT], Client Type [0x0052], Receiver Version [19.12.0.23], User [
user1], Client [10.105.232.40], Server [WIN2K12-215], Ctx Flags [0
x8820220228], Track Flags [0x1775010c3fc], Skip Code [0]"
```

```
Jan 9 22:55:41 <local0.notice> 10.106.40.223 01/09/2020:22:55:41
```

```
GMT ns-223 0-PPE-0 : default ICA Message 156 0 : "Skipping ICA flow
: Session GUID [4e3a91175ebcbe686baf175eec7e0200], Client IP/Port
[10.105.232.40/60059], Server IP/Port [10.106.40.219/2598], MSI
Client Cookie [Non-MSI], Session setup time [01/09/2020:22:55:39
GMT], Client Type [0x0052], Receiver Version [19.12.0.23], User [
user1], Client [10.105.232.40], Server [10.106.40.219], Ctx Flags [0
x8820220008], Track Flags [0x1600010c040], Skip Code [171]"
```

## Compteurs d'erreurs

Différents compteurs sont capturés par analyse ICA. Le tableau suivant répertorie les différents compteurs pour l'analyse ICA.

Exécutez la commande `nsconmsg -g hdx -d statswt0` pour afficher les détails du compteur.

Nom du compteur HDX	Motif	Catégorie (Statistiques/Erreur/-Diagnostics)
hdx_tot_ica_conn	Indique le nombre total de connexions Pure ICA détectées par NS. Incrémenté chaque fois qu'une connexion ICA basée sur la signature ICA d'un PCB client est détectée.	Statistiques
hdx_tot_cgp_conn	Indique le nombre total de connexions CGP détectées par NS (Session Reliability ON). Incrémenté chaque fois qu'une connexion CGP basée sur la signature CGP d'un PCB client est détectée.	Statistiques
hdx_dbgsym tot_udt_conn	Indique le nombre total de connexions ICA UDP détectées par NS	Statistiques
hdx_dbgsym tot_nsap_conn	Indique le nombre total de connexions prises en charge par NSAP détectées par NS	Statistiques

Nom du compteur HDX	Motif	Catégorie (Statistiques/Erreur/Diagnostics)
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
hdx_bg_ag_user	Nombre total d'accès utilisateur Access Gateway	Statistiques/Diagnostics
hdx_bg_lan_user	Nombre total d'accès en mode utilisateur LAN	Statistiques/Diagnostics
hdx_basic_enc	Indique le nombre de connexions ICA utilisant le chiffrement de base	Statistiques/Diagnostics
hdx_advanced_enc	Indique le nombre de connexions ICA utilisant le chiffrement avancé basé sur RC5	Statistiques/Diagnostics
dx_dbg_wanscaler_on_clientside	Nombre total de connexions CGP/ICA avec Citrix SD-WAN côté client	Statistiques/Diagnostics
hdx_dbg_wanscaler_on_serverside	Nombre total de connexions CGP/ICA avec Citrix SD-WAN côté serveur	Statistiques/Diagnostics
hdx_dbg_reconnected_session	Nombre total de demandes de reconnexion du client sans erreur Citrix ADC	Statistiques/Diagnostics



Nom du compteur HDX	Motif	Catégorie (Statistiques/Erreur/-Diagnostics)
hdx_dbg_host_rejected_ns_reconn	Nombre total d'hôtes rejetés de demandes de reconnexion par client	Statistiques/Diagnostics
hdx_euem_available	Indique le nombre de connexions pour lesquelles le canal de surveillance de l'expérience utilisateur final est disponible. Le canal de surveillance de l'expérience utilisateur final est nécessaire pour collecter des statistiques telles que ICA RTT.	Statistiques/Diagnostics
hdx_err_disabled_sr	La fiabilité de session est désactivée à l'aide du bouton nsapimgr. La session ne fonctionne pas pour cette session.	Erreur
hdx_err_skip_no_msi	La fonctionnalité MSI du serveur XA/XD est absente. Cela indique une ancienne version du serveur, HDX Insight ignore cette connexion.	Error
hdx_err_skip_old_server	Ancienne version de serveur non prise en charge	Erreur
hdx_err_clnt_not_whitelist	Récepteur client non dans la liste blanche, 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

Nom du compteur HDX	Motif	Catégorie (Statistiques/Erreur/-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
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

Nom du compteur HDX	Motif	Catégorie (Statistiques/Erreur/-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 Citrix ADC.

### Population d'enregistrements dans Citrix ADM liste de contrôle

- Exécutez la commande `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: ica_"` et vérifiez les journaux pour confirmer que Citrix ADM reçoit des enregistrements AppFlow.
- Confirmez que l'instance Citrix ADC est ajoutée à Citrix ADM.
- Validez que le serveur virtuel Citrix Gateway/VPN est sous licence Citrix ADM.
- Assurez-vous que le réglage des paramètres multi-sauts est activé pour le double saut.

- Assurez-vous que Citrix Gateway est autorisé pour le deuxième saut dans le déploiement à double saut.

### **Avant de contacter le support technique Citrix**

Pour une résolution rapide, assurez-vous de disposer des informations suivantes avant de contacter le support technique Citrix :

- Détails du déploiement et de la topologie du réseau.
- Versions de Citrix ADC et de Citrix ADM.
- Versions du serveur Citrix Virtual Apps and Desktops.
- Versions de Client Receiver
- Nombre de sessions ICA actives lorsque le problème s'est produit.
- Pack de support technique capturé en exécutant la `show techsupport` commande à l'invite de commande Citrix ADC.
- Pack de support technique capturé pour Citrix ADM.
- Traces de paquets capturées sur tous les Citrix ADC.  
Pour démarrer une trace de paquets, tapez, `start nstrace -size 0'`  
Pour arrêter une trace de paquets, tapez, `stop nstrace`
- Collectez les entrées dans la table ARP du système en exécutant la `show arp` commande.

### **Problèmes connus**

Reportez-vous aux notes de publication de Citrix ADC pour connaître les problèmes connus sur HDX Insight.

## **Gateway Insight**

February 1, 2024

Dans un déploiement Citrix Gateway, la visibilité des détails d'accès d'un utilisateur est essentielle pour résoudre les problèmes d'échec d'accès. En tant qu'administrateur réseau, vous voulez savoir quand un utilisateur n'est pas en mesure de se connecter à Citrix Gateway et connaître l'activité de l'utilisateur et les raisons de l'échec de l'ouverture de session, mais ces informations ne sont généralement pas disponibles sauf si l'utilisateur envoie une demande de résolution.

Gateway Insight offre une visibilité sur les défaillances rencontrées par tous les utilisateurs, quel que soit le mode d'accès, au moment de la connexion à Citrix Gateway. Vous pouvez consulter la liste de tous les utilisateurs disponibles, le nombre d'utilisateurs actifs, le nombre de sessions actives, ainsi que les octets et les licences utilisés par tous les utilisateurs à tout moment. Vous pouvez consulter l'analyse des points de terminaison (EPA), l'authentification, l'authentification unique (SSO) et les échecs de lancement d'applications pour un utilisateur. Vous pouvez également consulter les détails des sessions actives et interrompues d'un utilisateur.

Gateway Insight fournit également une visibilité sur les raisons de l'échec du lancement d'applications pour les applications virtuelles. Cela améliore votre capacité à résoudre tout type de problème d'échec de connexion ou de lancement d'application. Vous pouvez afficher le nombre d'applications lancées, le nombre de sessions totales et actives, le nombre total d'octets et la bande passante 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.

Vous pouvez consulter le nombre de passerelles, le nombre de sessions actives, le nombre total d'octets et la bande passante utilisés par toutes les passerelles associées à une appliance Citrix Gateway à tout moment. Vous pouvez afficher les échecs de l'EPA, de l'authentification, de l'authentification unique et du lancement d'application pour une Gateway. Vous pouvez également afficher les détails de tous les utilisateurs associés à une Gateway et leur activité d'ouverture de session.

Tous les messages du journal sont stockés dans la base de données Citrix ADM, afin que vous puissiez consulter les détails des erreurs pour n'importe quelle période. Vous pouvez également afficher un résumé des échecs d'ouverture de session et déterminer à quel stade du processus d'ouverture de session un échec s'est produit.

### **Points à noter**

- Gateway Insight est pris en charge sur les déploiements suivants :
  - Access Gateway
  - Unified Gateway
- La version et la version de Citrix ADM doivent être identiques ou ultérieures à celles de l'appliance Citrix Gateway.
- Une heure de rapports Gateway Insight peut être consultée pour les instances Citrix ADC avec licence Enterprise. Une licence Platinum est requise pour consulter les rapports Gateway Insight au-delà d'une heure.

## Limitations

- Citrix Gateway ne prend pas en charge Gateway Insight lorsque la méthode d'authentification est configurée en tant qu'authentification basée sur un certificat.
- Pour les rapports Gateway Insight, les informations de géolocalisation ne sont pas fournies par l'appliance Citrix ADC.
- Les connexions utilisateur réussies, la latence et les détails au niveau de l'application pour les applications et les bureaux ICA virtuels sont visibles uniquement sur le tableau de bord des utilisateurs HDX Insight.
- En mode double saut, la visibilité des défaillances sur l'appliance Citrix Gateway dans la deuxième zone démilitarisée n'est pas disponible.
- Les problèmes d'accès au bureau RDP (Remote Desktop Protocol) ne sont pas signalés.
- Gateway Insight est pris en charge pour les types d'authentification suivants. Si un autre type d'authentification est utilisé, vous pouvez constater certaines incohérences dans Gateway Insight.
  - Stockage local
  - LDAP
  - RADIUS
  - TACACS
  - SAML
  - OTP natif

## Activation de Gateway Insight

Pour activer Gateway Insight pour votre appliance Citrix Gateway, vous devez d'abord ajouter l'appliance Citrix Gateway à Citrix ADM. Vous devez ensuite activer AppFlow pour le serveur virtuel représentant l'application VPN. Pour plus d'informations sur l'ajout d'un appareil à Citrix ADM, consultez la section Ajout d'appareils.

### Remarque

Pour afficher les échecs de l'analyse des points de terminaison (EPA) dans Citrix ADM, vous devez activer l'authentification AppFlow, l'autorisation et l'audit de la journalisation des noms d'utilisateur sur l'appliance Citrix Gateway.

## Pour activer AppFlow pour un serveur virtuel dans Citrix ADM

1. Connectez-vous à Citrix ADM.

2. Accédez à **Réseaux > Instances** et sélectionnez l'instance pour laquelle vous souhaitez activer AppFlow.
3. Dans la liste **Sélectionner une action**, sélectionnez **Configurer Analytics**.
4. Dans la page **Configurer Insight**, sous **Configurer Analytics**, sélectionnez **Citrix Gateway**.
5. Sélectionnez le serveur virtuel pour lequel vous souhaitez activer AppFlow, puis cliquez sur **Activer AppFlow**.
6. Dans l'écran **Activer AppFlow**, dans la liste **Sélectionner une expression**, cliquez sur true.
7. En regard de **Mode transport**, activez la case à cocher **Logstream**.

**Enable AppFlow**

Select Expression \*

Citrix Gateway

true

true

Transport Mode  IPFIX  Logstream

ICA

TCP

HTTP

If there is a firewall between Citrix ADM and the Citrix ADC instance, please make sure the TCP port 5557 is open. This is to allow ADM to collect AppFlow traffic.

OK

Cancel

### Remarque

Vous pouvez choisir IPFIX ou `Logstream` comme mode de transport.

8. Cliquez sur **OK**.

### Pour activer l'authentification, l'autorisation et l'audit AppFlow dans la journalisation du nom d'utilisateur sur une appliance Citrix Gateway à l'aide de l'interface graphique

1. Accédez à **Configuration > Système > AppFlow > Paramètres**, puis cliquez sur **Modifier les paramètres AppFlow**.
2. Dans l'écran **Configurer les paramètres d'AppFlow**, sélectionnez **Nom d'utilisateur AAA**, puis cliquez sur **OK**.

## Affichage des rapports Gateway Insight

Dans Citrix ADM, vous pouvez consulter les rapports de tous les utilisateurs, applications et passerelles associés aux appliances Citrix Gateway, ainsi que les détails d'un utilisateur, d'une application ou d'une passerelle en particulier. Dans la section **Présentation**, vous pouvez afficher les échecs de l'EPA, de l'authentification unique, de l'authentification et du lancement d'application. Vous pouvez également afficher un résumé des différents modes de session utilisés par les utilisateurs pour ouvrir une session, des types de clients et du nombre d'utilisateurs connectés chaque heure.

### Pour afficher les échecs d'EPA, d'authentification unique, d'authentification, d'autorisation et de lancement d'application

1. Dans Citrix ADM, accédez à **Analytics > Gateway Insight**.
2. Sélectionnez la période pour laquelle vous souhaitez afficher les détails de l'utilisateur. Vous pouvez utiliser le curseur temporel pour personnaliser davantage la période sélectionnée. Cliquez sur **Go**.
3. Cliquez sur les onglets EPA (End Point Analysis), Authentification, Autorisation, SSO (Single Sign On) ou Lancement d'application pour afficher les détails de l'échec.

#### Overview

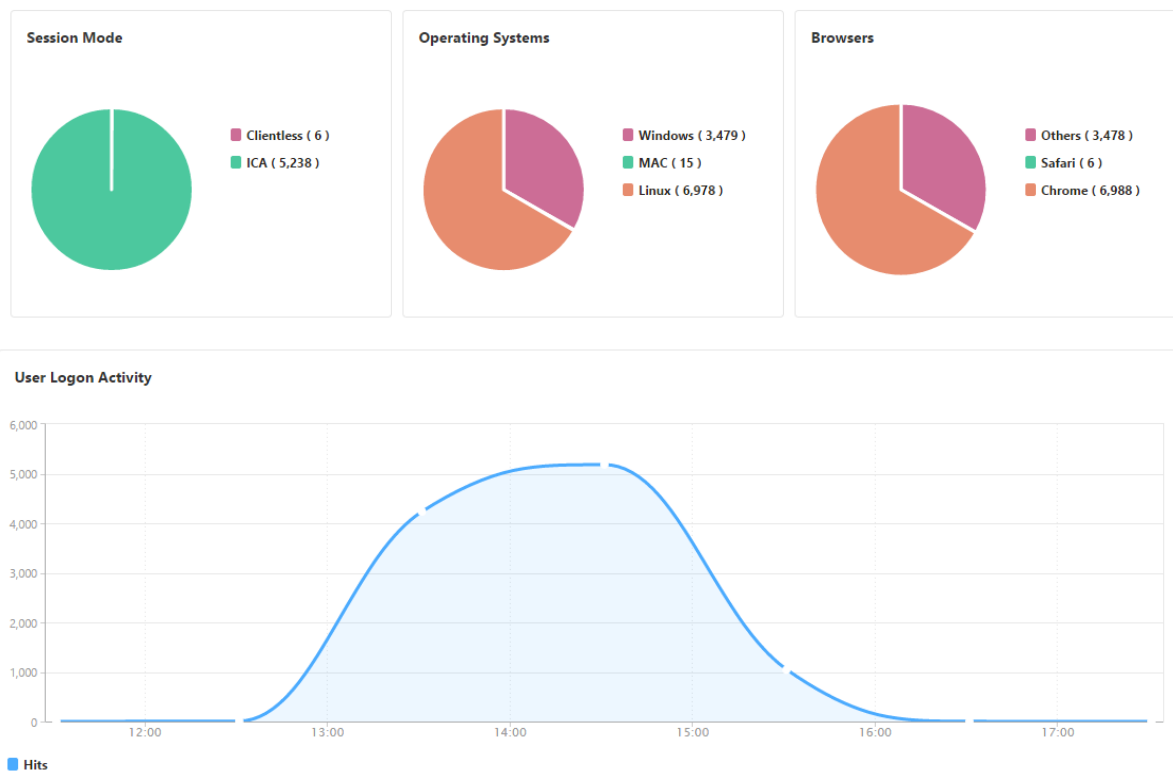


### Pour afficher un résumé des modes de session, des clients et du nombre d'utilisateurs

Dans Citrix ADM, accédez à **Analytics > Gateway Insight**, faites défiler vers le bas pour afficher les rapports.



## General Summary

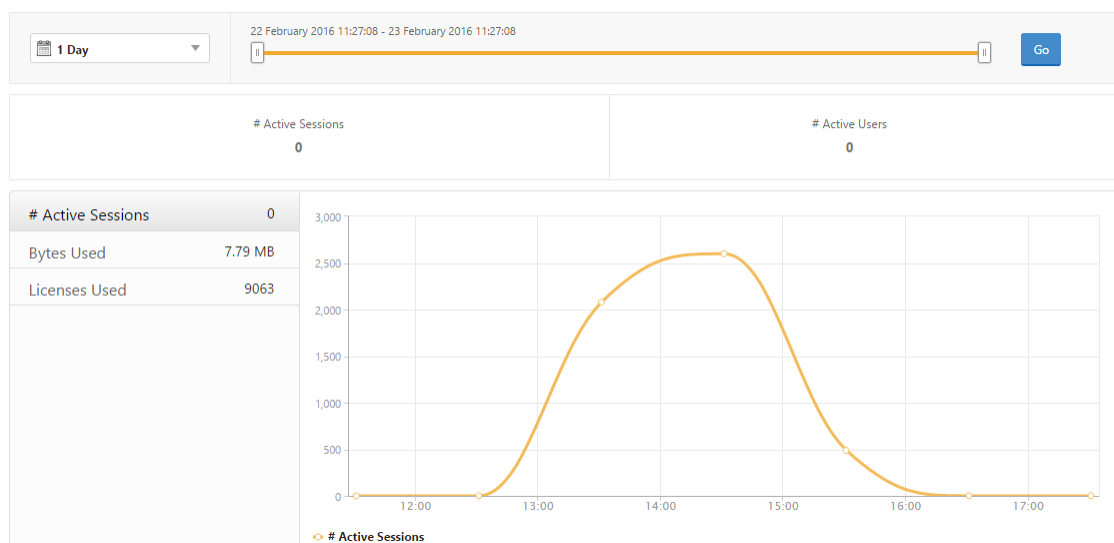


## Affichage des rapports Gateway Insight pour les utilisateurs

Vous pouvez consulter les rapports de tous les utilisateurs associés aux appliances Citrix Gateway. Vous pouvez consulter l'EPA, l'authentification, le SSO et les échecs de lancement d'applications d'un utilisateur. Vous pouvez également consulter les détails des sessions actives et interrompues d'un utilisateur.

### Pour afficher les détails de l'utilisateur

1. Dans Citrix ADM, accédez à **Analytics > Gateway Insight > Utilisateurs**.
2. Sélectionnez la période pour laquelle vous souhaitez afficher les détails de l'utilisateur. Vous pouvez utiliser le curseur temporel pour personnaliser davantage la période sélectionnée. Cliquez sur **Go**.
3. Vous pouvez désormais afficher le nombre d'utilisateurs actifs, le nombre de sessions actives, les octets et les 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.

Users		Active Users	
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**, vous pouvez cliquer sur un utilisateur dans la colonne **Nom** d'utilisateur pour afficher les échecs de lancement de l'EPA, de l'authentification unique, de l'authentification unique et de l'application, ainsi que d'autres détails pour cet utilisateur.

## Affichage des rapports Gateway Insight pour les applications

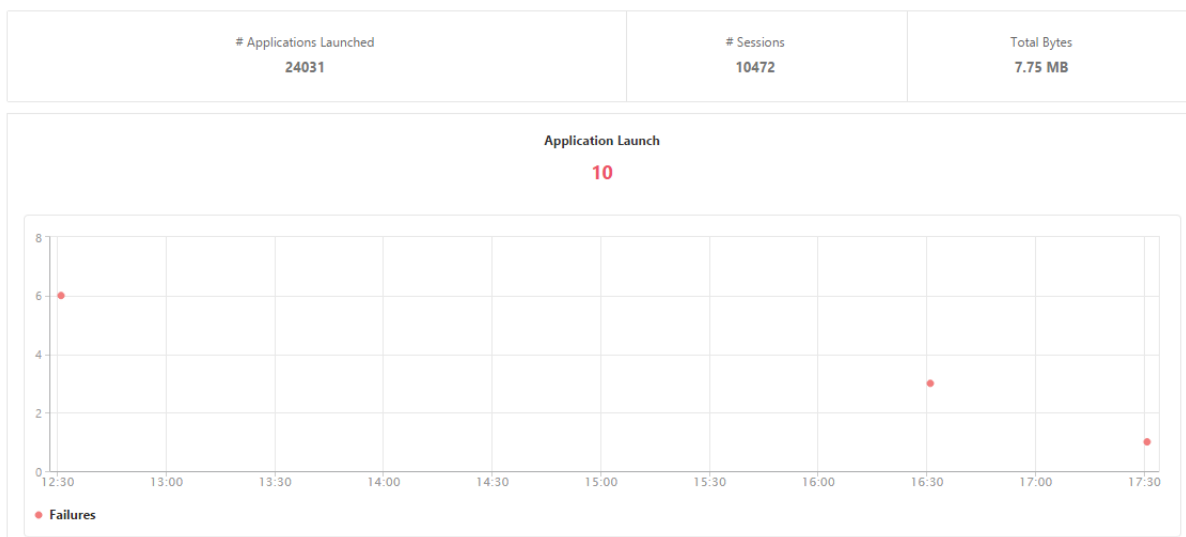
Vous pouvez afficher le nombre d'applications lancées, le nombre de sessions totales et actives, le nombre total d'octets et la bande passante consommés par les applications. Vous pouvez afficher les détails des utilisateurs, des sessions, de la bande passante et des erreurs de lancement d'une application.

### Pour afficher les détails de l'application

1. Dans Citrix ADM, accédez à **Analytics > Gateway Insight > Applications**.

- 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.

ICA Applications		Other 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.

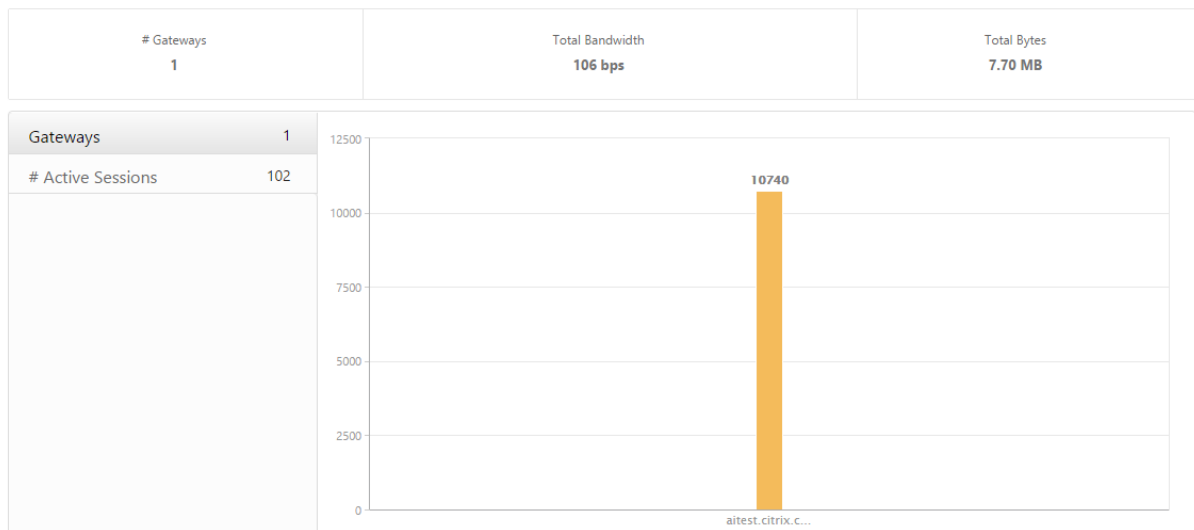
### Affichage des rapports Gateway Insight pour les passerelles

Vous pouvez afficher le nombre de passerelles, le nombre de sessions actives, le nombre total d'octets et la bande passante utilisés par toutes les passerelles associées à une appliance Citrix Gateway à tout moment. Vous pouvez afficher les échecs de l'EPA, de l'authentification, de l'authentification unique et du lancement d'application pour une Gateway. Vous pouvez également afficher les détails de tous les utilisateurs associés à une Gateway et leur activité d'ouverture de session.

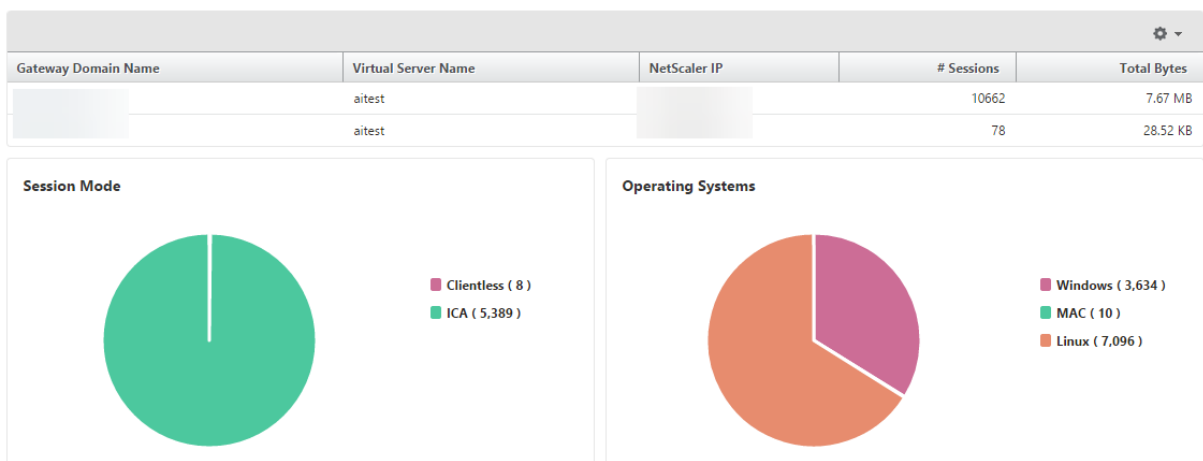
### Pour afficher les détails de la Gateway

1. Dans **Citrix ADM**, accédez à **Analytics > Gateway Insight > Passerelles**.
2. Sélectionnez la période pour laquelle vous souhaitez afficher les détails de la Gateway. Vous pouvez utiliser le curseur temporel pour personnaliser davantage la période sélectionnée. Cliquez sur **Go**.

Vous pouvez désormais afficher à tout moment le nombre de passerelles, le nombre de sessions actives, le nombre total d'octets et la bande passante utilisés par toutes les passerelles associées à une appliance Citrix Gateway.



Faites défiler vers le bas pour afficher les détails de la Gateway tels que le nom de domaine de la passerelle, le nom du serveur virtuel, l'adresse IP NetScaler, les modes de session et le nombre total d'octets.



Vous pouvez cliquer sur une Gateway dans la colonne **Nom de domaine de la Gateway** pour afficher les échecs de l'EPA, de l'authentification, de l'authentification unique et du lancement d'application,

ainsi que d'autres détails pour une passerelle.

## Exportation de rapports

Vous pouvez enregistrer les rapports Gateway Insight avec tous les détails affichés dans l'interface graphique au format PDF, JPEG, PNG ou CSV sur votre ordinateur local. Vous pouvez également planifier l'exportation des rapports vers des adresses e-mail spécifiées à différents intervalles.

### Remarque

- Les utilisateurs disposant d'un accès en lecture seule ne peuvent pas exporter de rapports.
- Les rapports de carte géographique sont exportés uniquement si Citrix ADM dispose d'une connexion Internet.

### Pour exporter un rapport

1. Dans l'onglet **Tableau de bord**, dans le volet droit, cliquez sur le bouton **d'exportation**.
2. Sous **Exporter maintenant**, sélectionnez le format requis, puis cliquez sur **Exporter**.

### Pour planifier l'exportation :

1. Dans l'onglet **Tableau de bord**, dans le volet droit, cliquez sur le bouton **d'exportation**.
2. Sous **Planifier l'exportation**, spécifiez les détails et cliquez sur **Planifier**.

### Pour ajouter un serveur de messagerie ou une liste de distribution de messagerie :

1. Dans l'onglet **Configuration**, accédez à **Système > Notifications > E-mail**.
2. Dans le volet droit, sélectionnez **Serveur de messagerie** pour ajouter un serveur de messagerie ou sélectionnez **Liste de distribution de messagerie pour créer une liste** de distribution de messagerie.
3. Spécifiez les détails et cliquez sur **Créer**.

### Pour exporter l'intégralité du tableau de bord Gateway Insight :

1. Dans l'onglet **Tableau de bord**, dans le volet droit, cliquez sur le bouton **d'exportation**.
2. Sous **Exporter maintenant**, sélectionnez Format **PDF**, puis cliquez sur **Exporter**.

## Cas d'utilisation de Gateway Insight

Les cas d'utilisation suivants montrent comment utiliser Gateway Insight pour gagner en visibilité sur les détails d'accès, les applications et les passerelles des utilisateurs sur les dispositifs Citrix Gateway.

## Un utilisateur ne peut pas se connecter à l'appliance Citrix Gateway ou aux serveurs Web internes

En tant qu'administrateur Citrix Gateway, vous surveillez les appliances Citrix Gateway via Citrix ADM et vous souhaitez savoir pourquoi un utilisateur ne parvient pas à se connecter ou à quel stade du processus de connexion l'échec s'est produit.

Citrix ADM vous permet d'afficher les détails des erreurs de connexion de l'utilisateur aux étapes suivantes du processus de connexion :

- Authentification
- Analyse des points finaux (EPA)
- Single Sign-On

Dans Citrix ADM, vous pouvez rechercher un utilisateur en particulier, puis afficher tous les détails de cet utilisateur.

### Pour rechercher un utilisateur :

Dans Citrix ADM, accédez à **Analytics > Gateway Insight** et, dans la zone de texte **Search for Users**, spécifiez l'utilisateur que vous souhaitez rechercher.

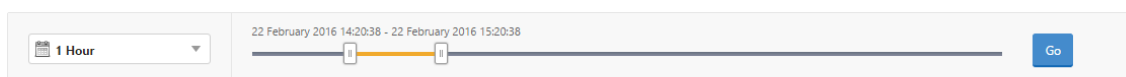
### Échec de l'authentification

Vous pouvez afficher les erreurs d'authentification telles que les informations d'identification incorrectes ou l'absence de réponse du serveur d'authentification. Si vous avez configuré l'authentification en deux étapes, vous pouvez voir si les étapes primaire, secondaire ou les deux ont échoué.

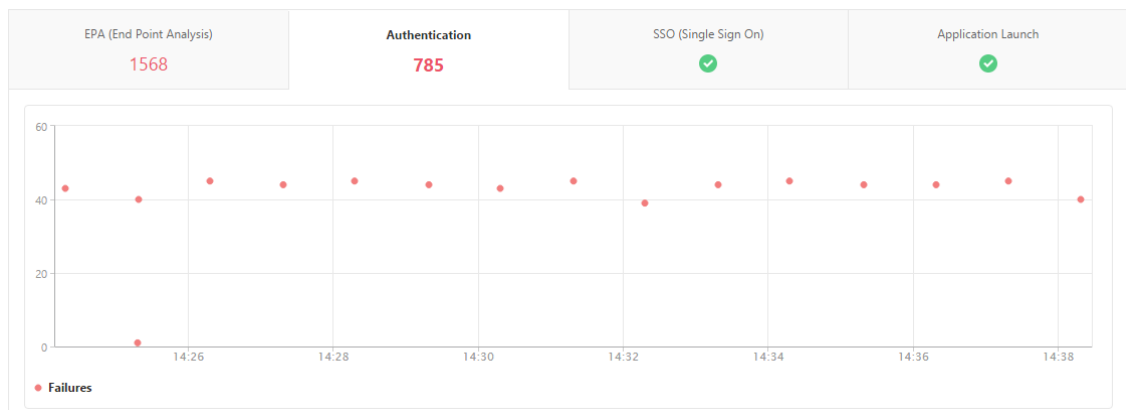
### Pour afficher les détails de l'échec d'authentification :

1. Dans Citrix ADM, accédez à **Analytics > Gateway Insight**.
2. Dans la section **Vue d'ensemble**, sélectionnez la période pour laquelle vous souhaitez afficher les erreurs d'authentification. Vous pouvez utiliser le curseur temporel pour personnaliser davantage la période sélectionnée. Cliquez sur **Go**.

#### Overview



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** de la table affiche la raison de l'échec de l'ouverture de session et la colonne **État** affiche à quel stade d'une authentification en deux étapes l'échec s'est produit.

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	State	Authentication Type	Authentication Server IP Address	Gateway Domain Name
user1684	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3137	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:26:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3276	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1731	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:38:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3227	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:29:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1676	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3355	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3170	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:27:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3177	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:28:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1639	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1705	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:36:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr

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 la flèche vers le bas, comme indiqué dans la capture d'écran suivante.

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	State	Authentication Type	Authentication Server IP Address	Gateway Domain Name
user1684	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3137	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:26:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3276	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1731	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:38:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3227	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:29:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1676	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3355	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3170	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:27:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3177	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:28:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1639	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1705	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:36:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr

## Échec de l'EPA

Vous pouvez afficher les échecs de l'EPA au stade de la pré-authentification ou de la post-authentification.

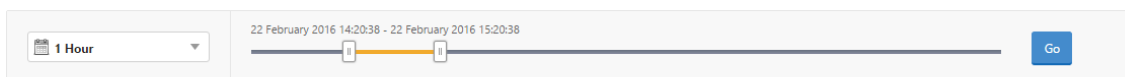
### Important :

- Les défaillances EPA ne sont signalées que lorsque des expressions classiques sont configurées.
- Les échecs EPA ne sont pas signalés si l'expression avancée est configurée dans la stratégie de pré-authentification ou de post-authentification.
- Les défaillances EPA ne sont pas signalées si l'EPA est configuré comme l'un des facteurs d'un flux d'authentification nFactor.

### Pour afficher les détails des échecs EPA :

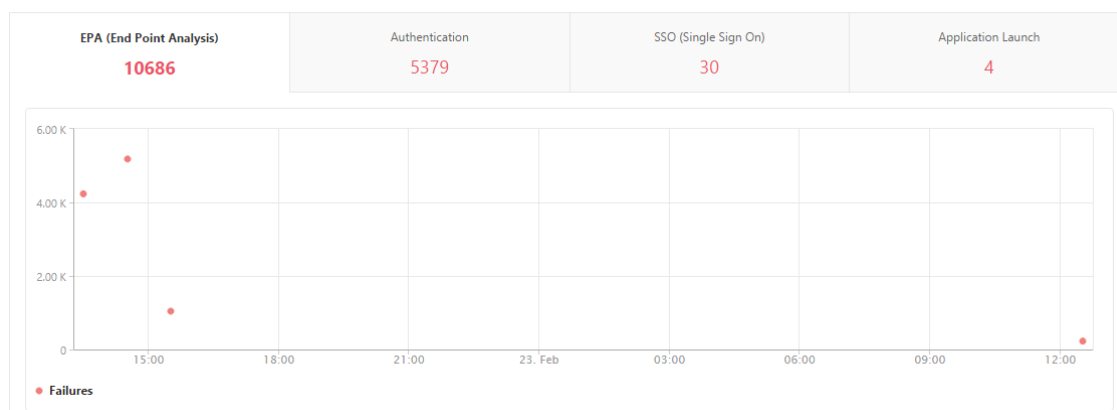
1. Dans Citrix ADM, accédez à **Analytics > Gateway Insight**.
2. Dans la section Vue d'ensemble, sélectionnez la période pour laquelle vous souhaitez afficher les erreurs EPA. Vous pouvez utiliser le curseur temporel pour personnaliser davantage la période sélectionnée. Cliquez sur **Go**.

#### Overview



3. Cliquez sur l'onglet **EPA (End Point Analysis)**. Vous pouvez afficher le nombre d'erreurs EPA à tout moment dans le graphique **Failures**.





Faites défiler la page vers le bas pour afficher les détails de chaque erreur EPA, tels que le **nom d'utilisateur**, **l'adresse IP NetScaler**, **l'adresse IP de la passerelle**, **le VPN**, **l'heure d'erreur**, **le nom de la stratégie**, **le nom de domaine de passerelle**, etc., dans le tableau du même onglet. La colonne **Description de l'erreur** du tableau affiche la raison de l'échec EPA et la colonne **Nom de la stratégie** affiche la stratégie qui a entraîné l'échec.

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	Policy Name	EPA Method	Gateway Domain Name
user1097	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1098	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1491	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1633	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 3:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user17	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1774	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user197	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com

Vous pouvez cliquer sur un utilisateur dans la colonne **Nom d'utilisateur** pour afficher les erreurs EPA et d'autres détails pour cet utilisateur.

Vous pouvez personnaliser le tableau pour ajouter ou supprimer des colonnes à l'aide de la flèche vers le bas.

**Remarque**

Citrix Gateway ne signale pas les échecs EPA lorsque l'expression « ClientSecurity » est configurée en tant que règle de stratégie de session VPN.

**Défaillances SSO**

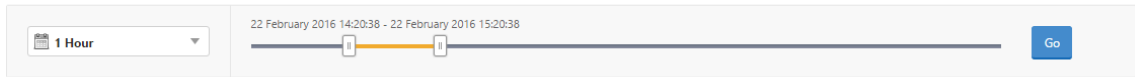
Vous pouvez consulter tous les échecs SSO à tout moment pour un utilisateur accédant à n'importe quelle application via l'appliance Citrix Gateway.

**Pour afficher les détails des défaillances SSO :**

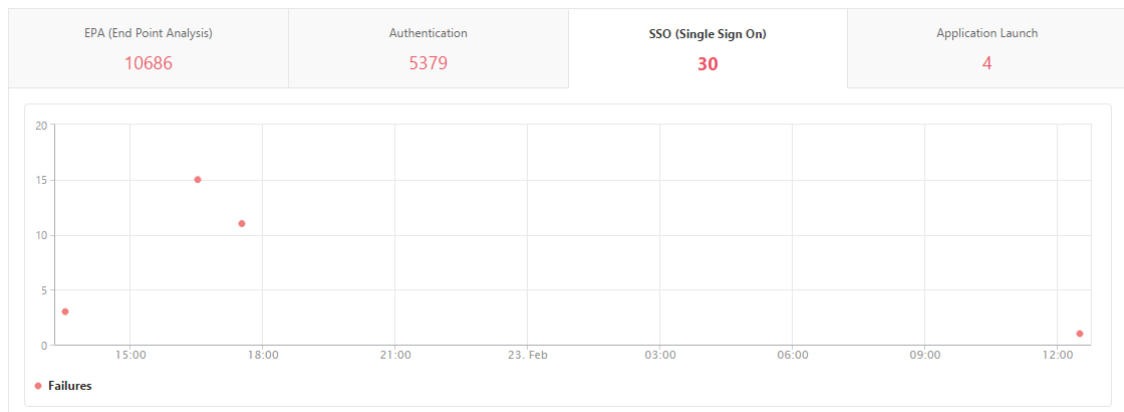
1. Dans Citrix ADM, accédez à **Analytics > Gateway Insight**.

2. Dans la section Vue d'ensemble, sélectionnez la période pour laquelle vous souhaitez afficher les erreurs d'SSO. Vous pouvez utiliser le curseur temporel pour personnaliser davantage la période sélectionnée. Cliquez sur **Go**.

**Overview**



3. Cliquez sur l'onglet **SSO (Single Sign On)**. Vous pouvez afficher le nombre d'erreurs SSO à tout moment dans le graphique Failures.



Faites défiler vers le bas pour afficher les détails de chaque erreur d'authentification seule (**nom d'utilisateur, adresse IP NetScaler, heure d'erreur, description de l'erreur, nom de la ressource, etc.**) dans le tableau du même onglet.

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	SSO Method	Gateway Domain Name
user11	10.102.61.201	10.102.61.210	10.144.2.35	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 5:30:54 PM	Single Sign ON failed	11	NTLM	aitest.citrix.com
user5	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/23/2016, 12:30:54 PM	Single Sign ON failed	1	Basic	aitest.citrix.com
user31	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user23	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 4:30:54 PM	Single Sign ON failed	15	NTLM	aitest.citrix.com

Vous pouvez cliquer sur un utilisateur dans la colonne **Nom d'utilisateur** pour afficher les erreurs SSO et d'autres détails pour cet utilisateur.

Vous pouvez personnaliser le tableau pour ajouter ou supprimer des colonnes à l'aide de la flèche vers le bas.

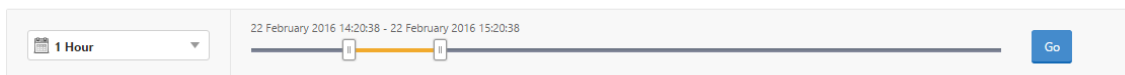
## Après une connexion réussie à Citrix Gateway, un utilisateur n'est pas en mesure de lancer une application virtuelle

En cas d'échec du lancement d'une application, vous pouvez obtenir une visibilité sur les raisons, telles que l'inaccessible Secure Ticket Authority (STA) ou le serveur Citrix Virtual Apps, ou un ticket STA non valide. Vous pouvez afficher l'heure à laquelle l'erreur s'est produite, les détails de l'erreur et la ressource pour laquelle la validation STA a échoué.

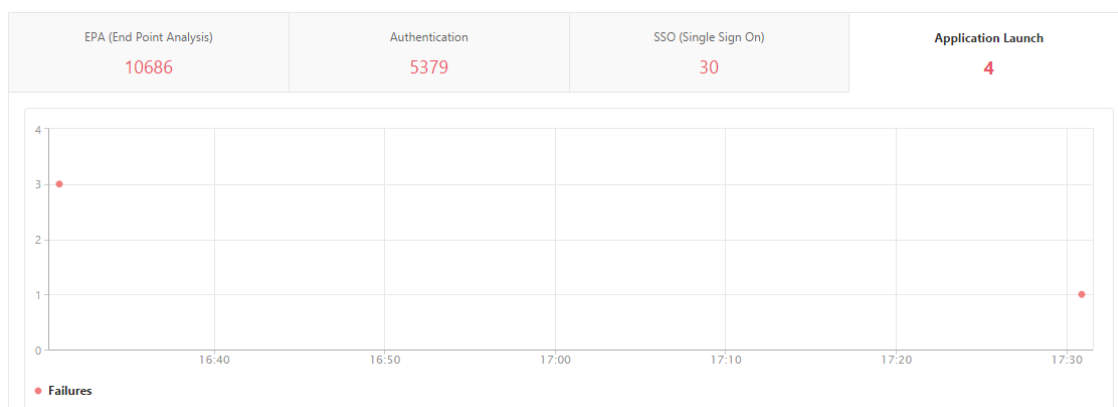
### Pour afficher les détails de l'échec de lancement de l'application :

1. Dans Citrix ADM, accédez à **Analytics > Gateway Insight**.
2. Dans la section **Vue d'ensemble**, sélectionnez la période pour laquelle vous souhaitez afficher les erreurs d'SSO. Vous pouvez utiliser le curseur temporel pour personnaliser davantage la période sélectionnée. Cliquez sur **Go**.

#### Overview



3. Cliquez sur l'onglet **Lancement de l'application**. Vous pouvez afficher le nombre d'échecs de lancement d'application à tout moment dans le graphique **Échec**.



Faites défiler vers le bas pour afficher les détails de chaque erreur de lancement d'application, telles que l'**adresse IP NetScaler**, le **temps d'erreur**, la **description de l'erreur**, le **nom de ressource**, le **nom de domaine de la passerelle**, etc., dans le tableau du même onglet. La colonne **Description de l'erreur** du tableau affiche l'adresse IP du serveur STA et la colonne **Nom de la ressource** affiche les détails de la ressource pour laquelle la validation STA a échoué.

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	STA IP Address	Error Time	Error Description	Error Count	Resource Name	Gateway Domain Name
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 5:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	code.jquery.com	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	cdn.kendostatic.com	aitest.citrix.com

Vous pouvez cliquer sur un utilisateur dans la colonne **Nom d'utilisateur** pour afficher les erreurs de lancement de l'application et d'autres détails pour cet utilisateur.

Vous pouvez personnaliser le tableau pour ajouter ou supprimer des colonnes à l'aide de la flèche vers le bas.

**Après avoir lancé une nouvelle application avec succès, un utilisateur souhaite afficher le nombre total d'octets et de bande passante consommés par cette application**

Une fois que vous avez lancé une nouvelle application avec succès, dans Citrix ADM, vous pouvez afficher le total des octets et de la bande passante consommés par cette application.

**Pour afficher le nombre total d'octets et de bande passante consommés par une application :**

Dans Citrix ADM, accédez à **Analytics > Gateway Insight > Applications**, faites défiler vers le bas et, sous l'onglet **Autres applications**, cliquez sur l'application pour laquelle vous souhaitez afficher les détails.

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.

Applications > 10.102.61.249

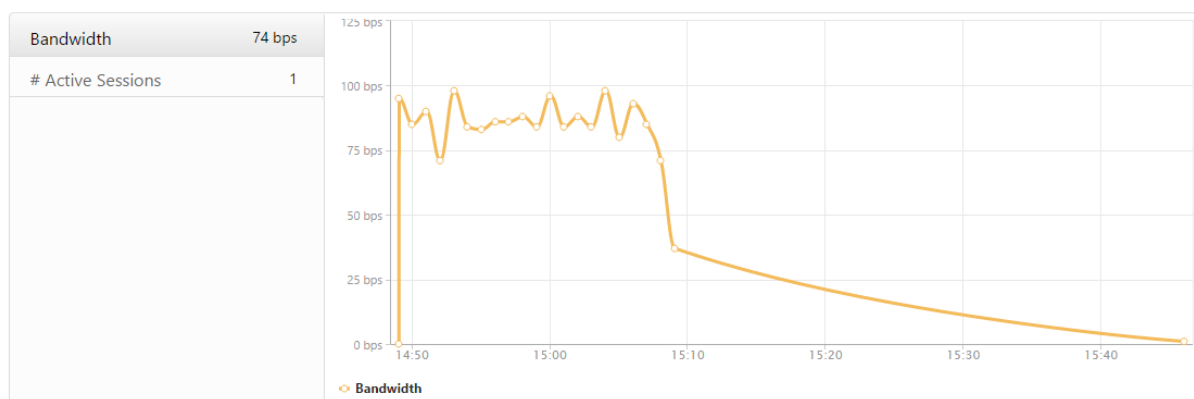
29 February 2016 14:46:41 - 29 February 2016 15:46:41

1 Hour

Go

App Type	# Sessions	Total Bytes
OTHER	781	781.95 KB

Vous pouvez également afficher la bande passante consommée par cette application.



**Un utilisateur s’est connecté à Citrix Gateway avec succès, mais ne peut pas accéder à certaines ressources réseau dans le réseau interne**

Avec Gateway Insight, vous pouvez déterminer si l’utilisateur a accès aux ressources réseau ou non. Vous pouvez également afficher le nom de la stratégie qui a entraîné l’échec.

**Pour afficher l’accès utilisateur aux ressources :**

1. Dans Citrix ADM, **accédez à Analytics > Gateway Insight > Applications.**
2. Sur l’écran qui apparaît, faites défiler l’écran vers le bas et dans l’onglet **Autres applications**, sélectionnez l’application à laquelle l’utilisateur n’a pas pu se connecter.

ICA Applications		Other Applications		
Name	# Sessions	Bandwidth	Total Bytes	
10.102.61.249	2499	32 bps	2.36 MB	
c.go-mpulse.net	2	0 bps	1.53 KB	
cdn.kendostatic.com	1	0 bps	805	
code.jquery.com	1	0 bps	1.51 KB	
engtools.citrite.net	2	0 bps	160	
onebug.citrite.net	2	1 bps	86.21 KB	
rock.citrite.net	1	0 bps	120	

3. Faites défiler la page vers le bas et dans le tableau **Utilisateurs**, tous les utilisateurs ayant accès à cette application sont affichés.

**Différents utilisateurs peuvent utiliser différents déploiements Citrix Gateway ou se connecter à Citrix Gateway via différents modes d’accès. L’administrateur doit être en mesure d’afficher les détails sur les types de déploiement et les modes d’accès**

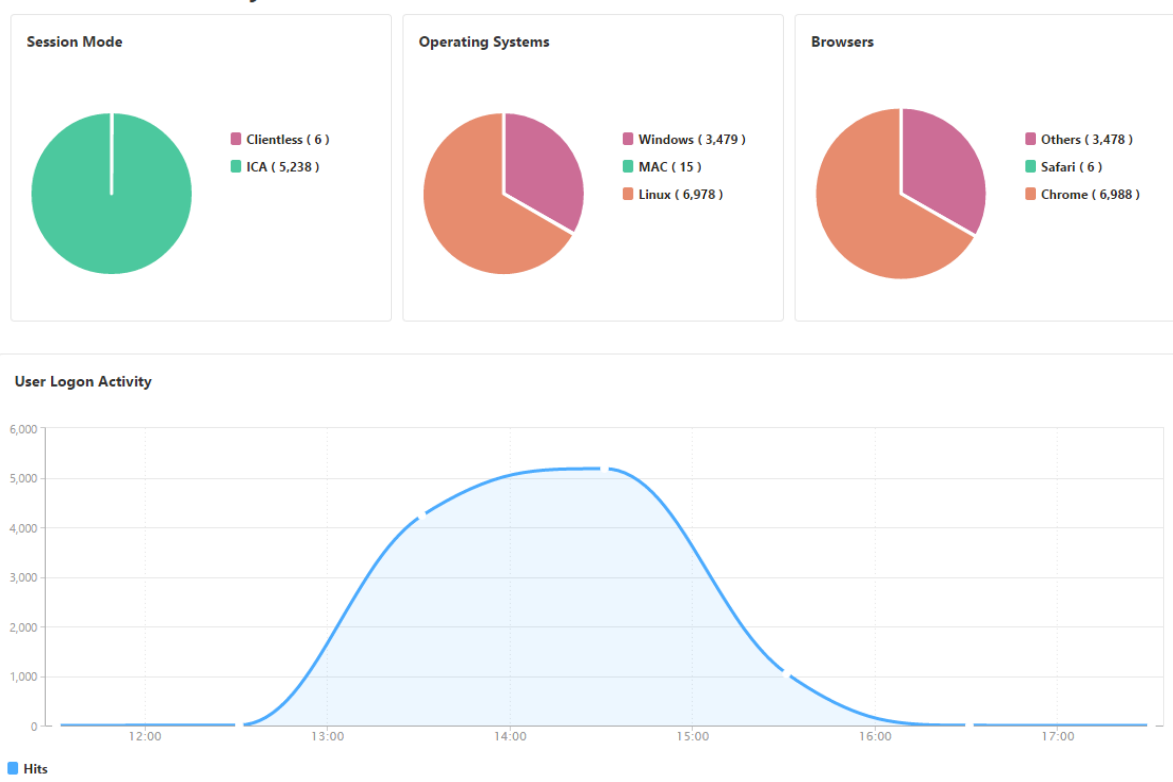
Avec Gateway Insight, vous pouvez afficher un résumé des différents modes de session utilisés par les utilisateurs pour ouvrir une session, les types de clients et le nombre d’utilisateurs connectés chaque heure. Vous pouvez également déterminer si le déploiement d’un utilisateur est une passerelle unifiée

ou un déploiement Citrix Gateway classique. Pour les déploiements de Gateway unifiée, vous pouvez afficher le nom et l'adresse IP du serveur virtuel de commutation de contenu et le nom du serveur virtuel VPN.

**Pour afficher le résumé des modes de session, du type de clients et du nombre d'utilisateurs connectés :**

1. Dans Citrix ADM, accédez à **Analytics > Gateway Insight**.
2. Dans la section **Vue d'ensemble**, faites défiler la page vers le bas pour afficher les graphiques **Mode session**, **Systèmes d'exploitation**, **Navigateurs** et **Activité d'ouverture de session utilisateur** affichent les différents modes de session utilisés par les utilisateurs pour ouvrir une session, les types de clients et le nombre d'utilisateurs connectés toutes les heures.

**General Summary**



**Résoudre les problèmes liés à Gateway Insight**

February 1, 2024

Si la solution Gateway Insight ne fonctionne pas comme prévu, le problème peut provenir de l'un des éléments suivants. Reportez-vous aux listes de contrôle dans les sections correspondantes pour le

dépannage.

- Configuration de Gateway Insight.
- Problème de connectivité entre Citrix ADC et Citrix ADM.
- Génération d'enregistrements dans Citrix ADC.
- Validations dans Citrix ADM.

### Liste de contrôle de la configuration Gateway Insight

- Assurez-vous que la fonctionnalité AppFlow est activée dans Citrix ADC. Pour plus de détails, consultez [Activation d'AppFlow](#).
- Vérifiez la configuration Gateway Insight dans la configuration en cours d'exécution de Citrix ADC.

Exécutez la `show running | grep -i <appflow_policy>` commande pour vérifier la configuration de Gateway Insight. Assurez-vous que le type de liaison est REQUEST. Par exemple ;

```
bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
```

- 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](#)
- Vérifiez le paramètre « appflowlog » dans le serveur virtuel Citrix Gateway/VPN. Pour plus de détails, consultez [Activation d'AppFlow pour les serveurs virtuels](#).

### Liste de contrôle de la connectivité entre Citrix ADC et Citrix ADM

- Vérifiez l'état du collecteur AppFlow dans Citrix ADC. Pour de plus amples informations, consultez [Comment vérifier l'état de la connectivité entre Citrix ADC et AppFlow Collector](#).
- Vérifiez les accès à la stratégie AppFlow Gateway Insight.

Exécutez la commande `show appflow policy <policy_name>` pour vérifier les accès à la stratégie AppFlow.

Vous pouvez également accéder à **Système > AppFlow > Stratégies** dans l'interface graphique pour vérifier les accès à la stratégie AppFlow.

- Validez tout pare-feu bloquant les ports AppFlow 4739 ou 5557.

## Liste de contrôle de la génération d'enregistrements dans Citrix ADC

- Exécutez la `nsconmsg -d stats -g ai_tot` commande et vérifiez les incréments de statistiques dans Citrix ADC.
- Capturez les journaux nstrace et vérifiez les paquets CFLOW pour confirmer que Citrix ADC exporte les enregistrements AppFlow.

## Validations dans Citrix ADM

- Exécutez la `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: vpn_"` commande pour vérifier les journaux pour confirmer que Citrix ADM reçoit des enregistrements AppFlow.
- Assurez-vous que l'instance Citrix ADC est ajoutée à Citrix ADM.
- Assurez-vous que le serveur virtuel Citrix Gateway/VPN est sous licence dans Citrix ADM.

## Statistiques de Gateway Insight

Les statistiques suivantes de Gateway Insight 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

## Contactez le support technique Citrix

Pour une résolution rapide, assurez-vous de disposer des informations suivantes avant de contacter le support technique Citrix :

- Détails du déploiement et de la topologie du réseau.



- Versions de Citrix ADC et de Citrix ADM.
- Offre groupée de support technique pour Citrix ADC et Citrix ADM.
- nstrace capture pendant le numéro.

## Problèmes connus

Consultez les notes de mise à jour de Citrix ADC pour les problèmes connus sur Gateway Insight.

## Security Insight

February 1, 2024

Les applications Web et de services Web exposées à Internet sont devenues de plus en plus vulnérables aux attaques. Pour protéger les applications contre les attaques, vous devez disposer d'une visibilité sur les menaces, de données exploitables en temps réel sur les attaques et de recommandations sur les contre-mesures. Security Insight fournit une solution sur un seul écran pour vous aider à évaluer l'état de sécurité de votre application et à prendre des mesures correctives pour sécuriser vos applications.

### Remarque

Security Insight est pris en charge sur Citrix Application Delivery Management (ADM) avec les appliances Citrix ADC exécutant sur la version 11.0 Build 65.31 et ultérieure.

## Fonctionnement de Security Insight

Security Insight est une solution intuitive d'analyse de la sécurité basée sur un tableau de bord qui vous donne une visibilité totale sur l'environnement de menace associé à vos applications. Des informations sur la sécurité sont incluses dans Citrix ADM et elles génèrent périodiquement des rapports basés sur vos configurations de sécurité système Application Firewall et Citrix ADC. Les rapports contiennent les renseignements suivants pour chaque application :

- **Indice de menace.** Système de classement à un chiffre indiquant la criticité des attaques sur l'application, que l'application soit protégée ou non par une appliance Citrix ADC. Plus les attaques sur une application sont critiques, plus l'indice de menace pour cette application est élevé. Les valeurs varient de 1 à 7.

L'indice des menaces est basé sur les informations d'attaque. Les informations relatives à l'attaque, telles que le type de violation, la catégorie d'attaque, l'emplacement et les détails du client, vous donnent un aperçu des attaques visant l'application. Les informations de violation

sont envoyées à Citrix ADM uniquement lorsqu'une violation ou une attaque se produit. Un grand nombre de violations et de vulnérabilités conduisent à une valeur d'indice de menace élevée.

- **Indice de sécurité.** Système de notation à un chiffre indiquant la manière dont vous avez configuré en toute sécurité les instances Citrix ADC pour protéger les applications contre les menaces et les vulnérabilités externes. Plus les risques pour la sécurité d'une application sont faibles, plus l'indice de sécurité est élevé. Les valeurs varient de 1 à 7.

L'index de sécurité tient compte à la fois de la configuration du pare-feu de l'application et de la configuration de sécurité du système Citrix ADC. Pour un indice de sécurité élevé, les deux configurations doivent être solides. Par exemple, si des vérifications rigoureuses du pare-feu d'application sont en place mais que les mesures de sécurité du système Citrix ADC, telles qu'un mot de passe fort pour l'utilisateur nsroot, n'ont pas été adoptées, les applications se voient attribuer une valeur d'indice de sécurité faible.

- **Informations exploitables.** Informations dont vous avez besoin pour abaisser l'indice de menace et augmenter l'indice de sécurité, ce qui améliore considérablement la sécurité des applications. Par exemple, vous pouvez consulter des informations sur les violations, les configurations de sécurité existantes et manquantes pour le pare-feu des applications et d'autres fonctionnalités de sécurité, le taux d'attaque des applications, etc.

## Configurer Security Insight

Citrix ADM prend en charge Security Insight à partir de toutes les instances Citrix ADC sur lesquelles un pare-feu d'application est configuré.

Pour configurer des informations de sécurité sur une instance ADC, configurez d'abord un profil de pare-feu d'application et une stratégie de pare-feu d'application. Bien que vous puissiez ensuite lier la stratégie de pare-feu d'application globalement, Citrix recommande que la stratégie soit liée au serveur virtuel.

Pour afficher les analyses sur Citrix ADM, activez la fonctionnalité AppFlow sur l'instance, configurez un collecteur, une action et une stratégie AppFlow, et liez la stratégie globalement. Ici aussi, bien que vous puissiez ensuite lier la stratégie de pare-feu de l'application globalement, Citrix recommande que la stratégie soit liée au serveur virtuel. Citrix vous recommande également d'utiliser Citrix ADM pour déployer des configurations AppFlow sur les instances ADC. Lorsque vous configurez le collecteur, vous devez spécifier l'adresse IP du serveur Citrix ADM sur lequel vous souhaitez surveiller les rapports.

### Pour configurer des informations de sécurité sur une instance Citrix ADC :

1. Exécutez les commandes suivantes pour configurer un profil et une stratégie de pare-feu d'application et lier la stratégie de pare-feu d'application globalement ou au serveur virtuel d'équili-

brage de charge.

---

**add appfw profile** [**\*\*-defaults\*\*** ( basic advanced )]

---

**set appfw profile** <name> [**-startURLAction** <startURLAction> ...]

**add appfw policy** <name> <rule> <profileName>

**bind appfw global** <policyName> <priority>

ou,

**bind lb vserver** <lb vserver> **-policyName** <policy> **-priority** <priority>

```

1 add appfw profile pr_appfw -defaults advanced
2 set appfw profile pr_appfw -startURLAction log stats learn
3 add appfw policy pr_appfw_pol "HTTP.REQ.HEADER("Host").EXISTS"
  pr_appfw
4 bind appfw global pr_appfw_pol 1
5 or,
6 bind lb vserver outlook -policyName pr_appfw_pol -priority " 20
  "
7 <!--NeedCopy-->

```

2. Exécutez les commandes suivantes pour activer la fonctionnalité AppFlow, configurer un collecteur, une action et une stratégie AppFlow et lier la stratégie globalement ou au serveur virtuel d'équilibrage de charge :

**add appflow collector** <name> **-IPAddress** <ipaddress>

---

**set appflow param** **DISABLED** )]

[**-SecurityInsightRecordInterval** ]

[**\*\*-SecurityInsightTraffic\*\*** ( ENABLED

---

**add appflow action** <name> **-collectors** <string>

**add appflow policy** <name> <rule> <action>

**bind appflow global** <policyName> <priority> [<gotoPriorityExpression>] [**-type** <type>]

ou,

**bind lb vserver** <vserver> **-policyName** <policy> **-priority** <priority>

```

1 add appflow collector col -IPAddress 10.102.63.85
2 set appflow param -SecurityInsightRecordInterval 600 -
  SecurityInsightTraffic ENABLED
3 add appflow action act1 -collectors col
4 add appflow action af_action_Sap_10.102.63.85 -collectors col

```

```

5 add appflow policy poli true act1
6 add appflow policy af_policy_Sap_10.102.63.85 true
  af_action_Sap_10.102.63.85
7 bind appflow global poli 1 END -type REQ_DEFAULT
8 or,
9 bind lb vserver Sap -policyName af_action_Sap_10.102.63.85 -
  priority " 20 "
10 <!--NeedCopy-->

```

**Pour activer AppFlow depuis Citrix ADM, procédez comme suit :**

1. Dans un navigateur Web, saisissez l’adresse IP du **Citrix ADM** (par exemple, <http://192.168.100.1>).
2. Dans **Nom d'utilisateur** et **Mot de passe**, entrez les informations d’identification de l’administrateur.
3. Accédez à **Réseaux > Instances**, puis sélectionnez l’instance Citrix ADC que vous souhaitez activer AppFlow.
4. Dans la liste **Sélectionner une action**, sélectionnez **Configurer Analytics**.
5. Sélectionnez les serveurs virtuels, puis cliquez sur **Activer AppFlow**.
6. Dans le champ **Activer AppFlow**, tapez **true** et sélectionnez **Security Insight**.
7. Cliquez sur **OK**.

### Enable AppFlow

Select Expression

Load Balancing

▼

true

**Transport Mode**  IPFIX  Logstream

Web Insight

Client Side Measurement

Security Insight

If there is a firewall between Citrix ADM and the Citrix ADC instance, please make sure the TCP port 5557 is open. This is to allow ADM to collect AppFlow traffic.

OK

Cancel

## Afficher les emplacements géographiques pour les rapports Security Insight

Les rapports Security Insight incluent les emplacements géographiques exacts d'où proviennent les demandes des clients. Vous pouvez afficher les emplacements géographiques dans Citrix ADM. Le fichier de base de données géo intégré dans Citrix ADC contient la plupart des adresses IP publiques. Le fichier est disponible à l'emplacement `/var/netScaler/inbuilt_db` dans Citrix ADC.

### Pour activer les emplacements géographiques :

Exécutez les commandes suivantes pour activer la journalisation géographique et la journalisation au format CEF :

- **add locationFile** <Complete path with the DB filename>
- **définir les paramètres appfw -GeolocationLogging ON**
- **définir les paramètres appfw -CEFLogging ON**

Si aucune adresse IP n'est disponible dans le fichier de base de données géo, vous pouvez ajouter l'adresse IP de l'emplacement géographique. Outre l'adresse IP, vous pouvez également ajouter un nom de ville/état/pays ainsi que les coordonnées de latitude et de longitude de chaque emplacement.

Ouvrez le fichier de base de données géo avec un éditeur de texte, tel que l'éditeur vi, et ajoutez une entrée pour chaque emplacement.

L'entrée doit être dans le format suivant :

```
\<start IP\>,\<end IP\>,,\<country\>,\<state\>,,\<city\>,,longitude,  
latitude
```

Par exemple,

```
1 4.17.142.224,4.17.142.239,,US,New York,,Harrison,,73.7304,41.0568  
2 <!--NeedCopy-->
```

## Réputation IP

Vous pouvez utiliser NetScaler Insight Center pour surveiller et gérer la réputation IP de votre trafic entrant. Vous pouvez configurer des stratégies pour ajouter d'autres adresses IP comme étant malveillantes et créer une liste de blocs personnalisée.

Pour en savoir plus sur la configuration et l'utilisation de la réputation IP, consultez [Réputation IP](#).

## Surveiller la réputation IP

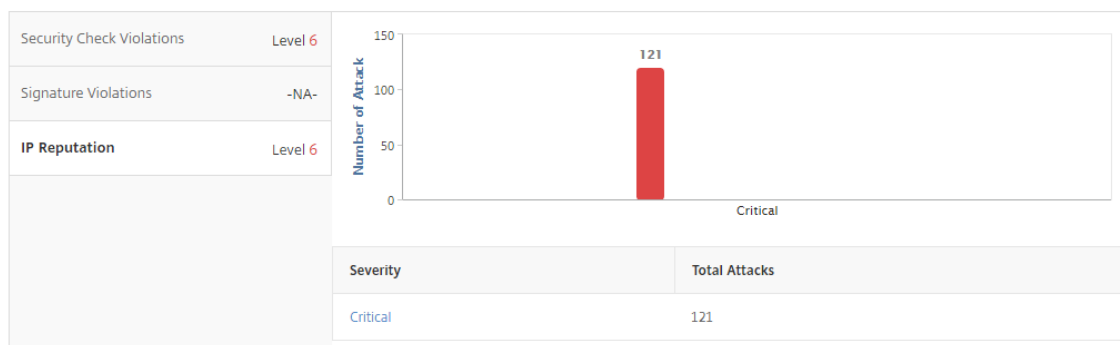
La fonctionnalité Réputation IP fournit des informations relatives aux attaques sur les adresses IP malveillantes. Par exemple, il signale le score de réputation IP, la catégorie de réputation IP, le temps d'attaque de réputation IP, l'adresse IP du périphérique et des détails sur l'adresse IP du client.

Le score de réputation IP indique le risque associé à une adresse IP. Le score a les suivantes sont les plages :

Score de réputation IP	Niveau de risque
1–20	Risque élevé
21–40	Suspect
41–60	Risque modéré
61–80	Risque faible
81–100	Fiable

### Pour surveiller la réputation d'IP :

1. Accédez à **Analytics > Security Insight**, puis sélectionnez l'application que vous souhaitez surveiller.
2. Dans l'onglet **Index des menaces**, sélectionnez **Réputation IP**.



3. Sélectionnez une gravité pour afficher plus de détails sur les attaques qui se trouvaient à ce niveau. Vous pouvez cliquer sur le graphique à barres ou dans le tableau sous le graphique.
4. Sélectionnez la période pour laquelle vous souhaitez afficher les détails. Vous pouvez utiliser le curseur temporel pour personnaliser davantage la période sélectionnée. Ensuite, cliquez sur **Aller**.

## IP Reputation

IP Reputation Attack Time	Device IP Address	Source IP Address	IP Reputation Category	Severity	IP Reputation Score	HTT
NA	10.102.60.27	10.102.63.79	0	Critical	0	POST

5. Pour personnaliser l’affichage, cliquez sur le bouton Paramètres.

## IP Reputation

IP Reputation Attack Time	Device IP Address	Source IP Address	IP Reputation Category	Severity	IP Reputation Score	HTTP Method
NA	10.102.60.27	10.102.63.79	0	Critical	0	POST
NA	10.102.60.27	10.102.63.79	0	Critical	0	POST

## Seuils

Vous pouvez définir et consulter les seuils relatifs à l’indice de sécurité et à l’indice de menace des applications dans Security Insight.

### Pour définir un seuil :

1. Accédez à **Analytics > Paramètres > Seuils**, puis sélectionnez **Ajouter**.
2. Sélectionnez le type de trafic comme **Sécurité** dans le champ **Type de trafic** et saisissez les informations requises dans les autres champs appropriés tels que le nom, la durée et l’entité.
3. Dans la section **Configurer une règle**, utilisez les champs **Mesure**, **Comparateur** et **Valeur** pour définir un seuil.

Par exemple, “Threat Index” > “>” “5”

4. Dans les **Paramètres de notification**, sélectionnez le type de notification.
5. Cliquez sur **Créer**.

### Pour afficher les franchissement des seuils :

1. Accédez à **Analytics > Security Insight > Périphériques**, puis sélectionnez l'instance Citrix ADC.
2. Dans la section **Application**, vous pouvez afficher le nombre de violations de seuil survenues pour chaque serveur virtuel dans la colonne **Violation de seuil**.

## Cas d'utilisation de Security Insight

Les cas d'utilisation suivants décrivent comment utiliser les informations de sécurité pour évaluer l'exposition aux menaces des applications et améliorer les mesures de sécurité.

### Obtenez une vue d'ensemble de l'environnement des menaces

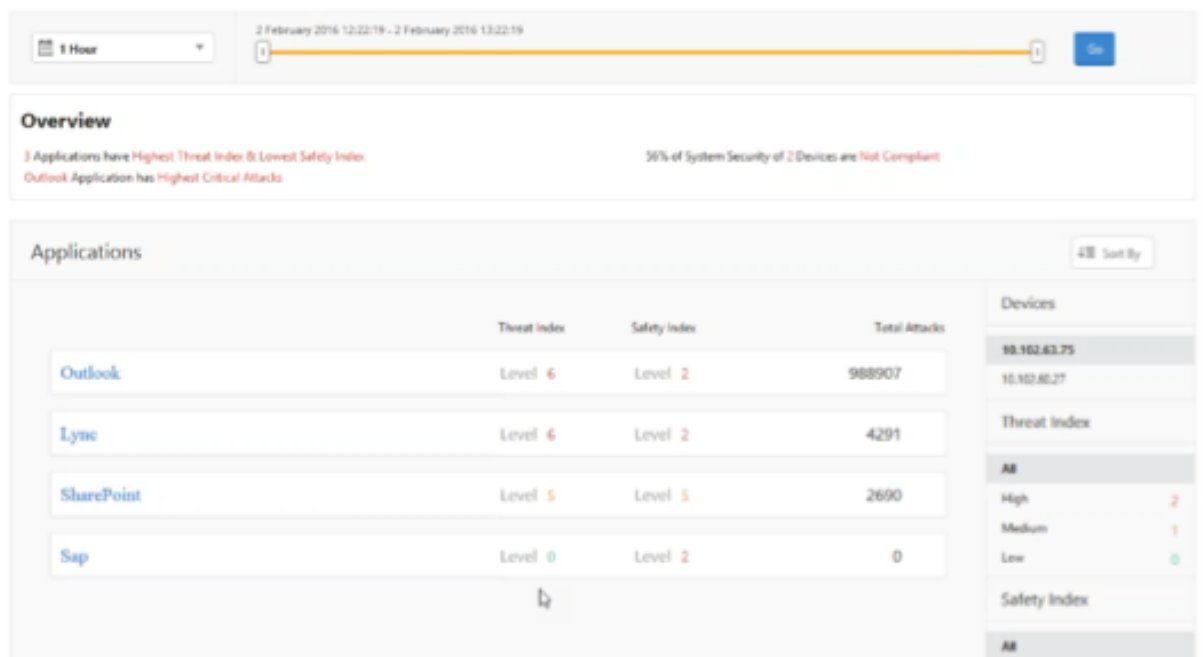
Dans ce cas d'utilisation, vous disposez d'un ensemble d'applications exposées à des attaques et vous avez configuré Citrix ADM pour surveiller l'environnement de menace. Vous devez consulter régulièrement l'indice de menace, l'indice de sécurité, ainsi que le type et la gravité des attaques que les applications ont pu subir. Cette revue vous permet de vous concentrer d'abord sur les applications qui nécessitent le plus d'attention. Le tableau de bord d'informations sur la sécurité fournit un résumé des menaces rencontrées par vos applications pendant la période de votre choix et pour un périphérique Citrix ADC sélectionné. Il affiche la liste des applications, leurs indices de menace et de sécurité, ainsi que le nombre total d'attaques pour la période choisie.

Par exemple, vous pouvez surveiller Microsoft Outlook, Microsoft Lync, SharePoint et une application SAP, et vous pouvez consulter un résumé de l'environnement de menace pour ces applications.

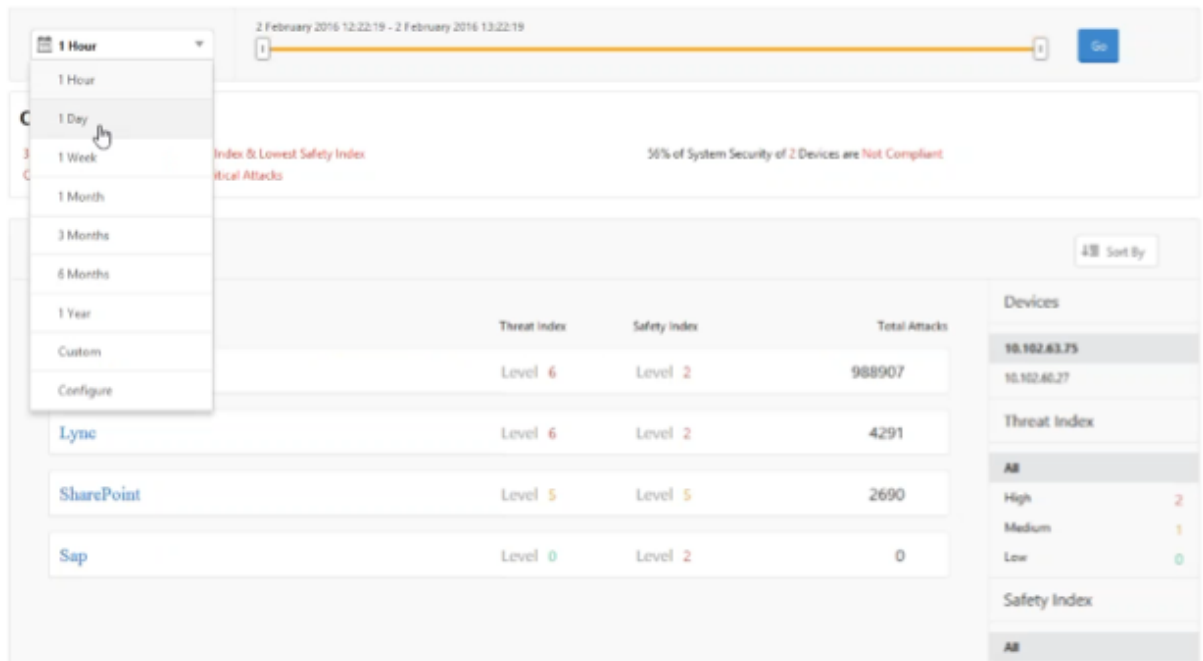
Pour obtenir un résumé de l'environnement de menace, ouvrez une session sur **Citrix ADM**, puis accédez à **Analytics > Security Insight**.

Les informations clés sont affichées pour chaque application. La période par défaut est de 1 heure.





Pour afficher les informations d'une période différente, sélectionnez une période dans la liste située en haut à gauche.



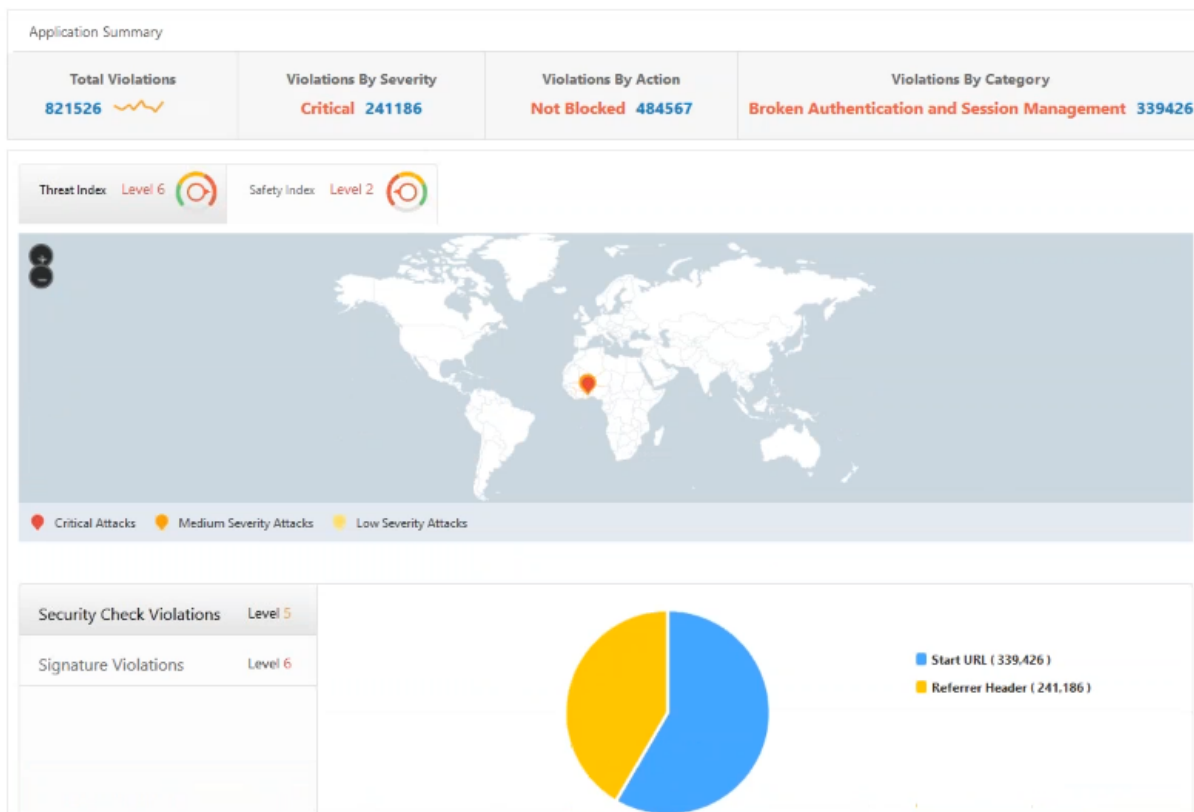
Pour afficher un résumé pour une autre instance Citrix ADC, sous **Périphériques**, cliquez sur l'adresse IP de l'instance Citrix ADC. Pour trier la liste des applications par colonne donnée, cliquez sur l'en-tête de colonne.

### Déterminer l'exposition aux menaces d'une application

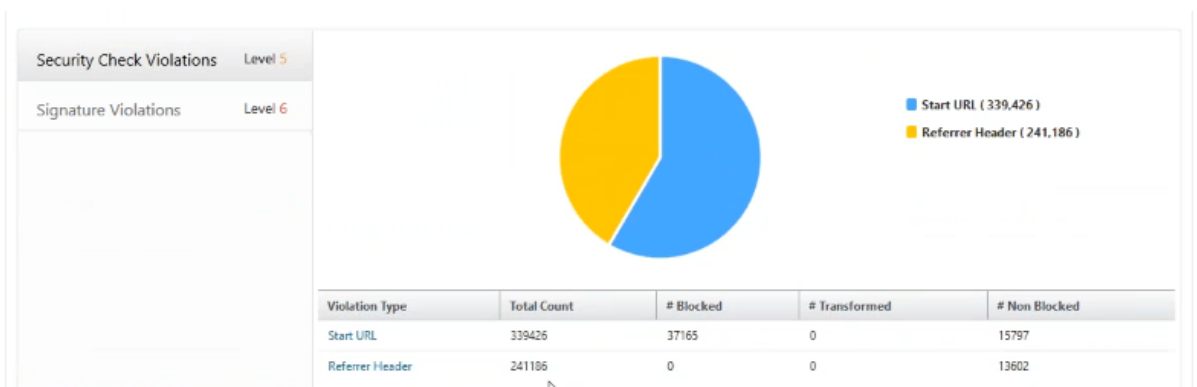
Pour identifier les applications qui ont un indice de menace élevé et un indice de sécurité faible dans le tableau de bord Security Insight, vous souhaitez déterminer l'exposition aux menaces avant de décider de les sécuriser. Autrement dit, vous voulez déterminer le type et la gravité des attaques qui ont dégradé leurs valeurs d'index. Vous pouvez déterminer l'exposition à la menace d'une application en consultant le résumé de l'application.

Dans cet exemple, Microsoft Outlook a une valeur d'indice de menace de 6 et vous voulez savoir quels facteurs contribuent à cet indice de menace élevé.

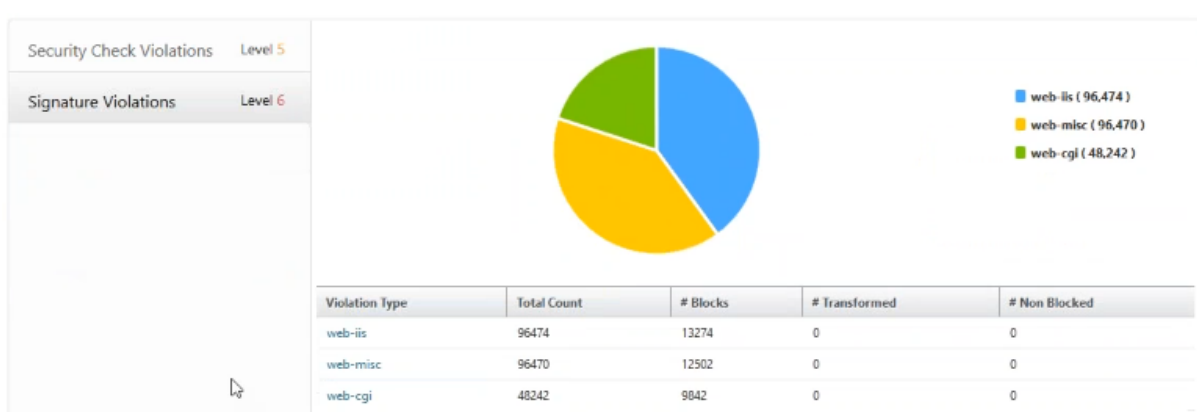
Pour déterminer l'exposition à la menace de Microsoft Outlook, dans le tableau de bord **Security Insight**, cliquez sur **Outlook**. Le résumé de l'application inclut une carte qui identifie l'emplacement géographique du serveur.



Cliquez sur **Index des menaces > Violations de vérification de sécurité** et consultez les informations de violation qui s'affichent.



Cliquez sur **Violations de signature** et consultez les informations de violation qui s'affichent.

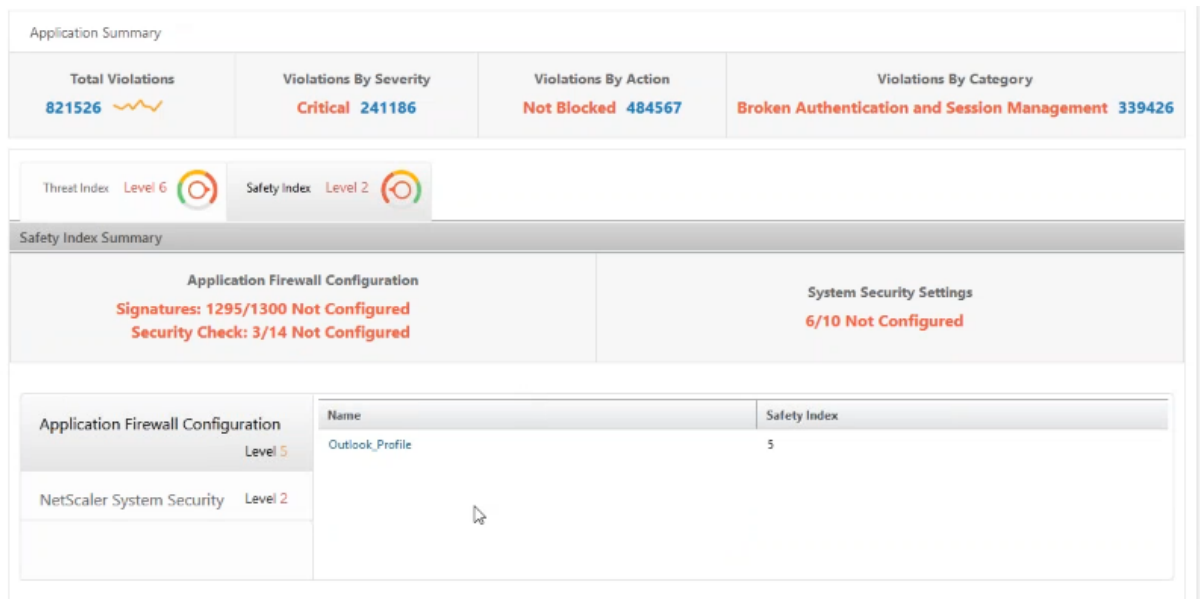


### Déterminer la configuration de sécurité existante et manquante pour une application

Après avoir examiné l'exposition aux menaces d'une application, vous souhaitez déterminer quelles configurations de sécurité des applications sont en place et quelles configurations sont manquantes pour cette application. Vous pouvez obtenir ces informations en consultant le résumé de l'indice de sécurité de l'application.

Le résumé de l'indice de sécurité fournit des informations sur l'efficacité des configurations de sécurité suivantes :

- **Configuration du pare-feu des applications.** Indique le nombre d'entités de signature et de sécurité qui ne sont pas configurées.
- **Sécurité du système NetScaler.** Indique combien de paramètres de sécurité système ne sont pas configurés.

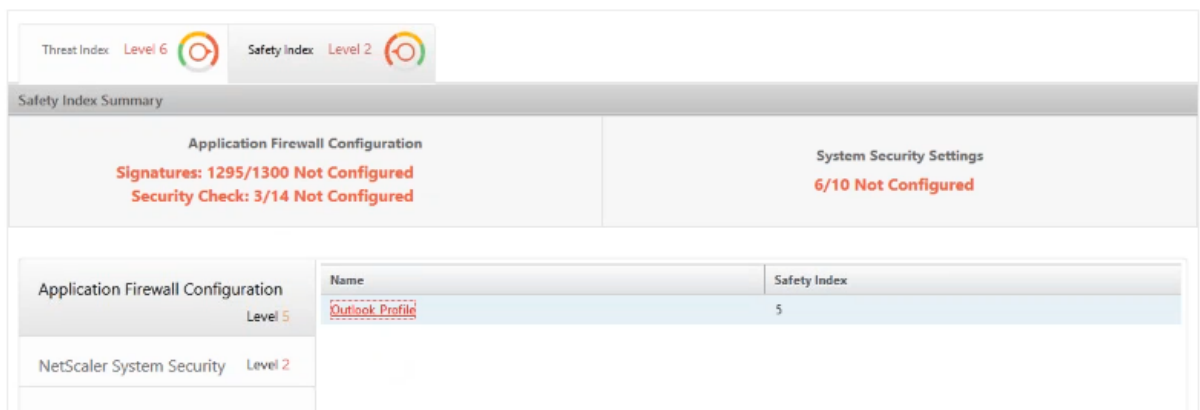


Dans le cas d'utilisation précédent, vous avez examiné l'exposition aux menaces de Microsoft Outlook, qui a une valeur d'indice de menace de 6. Maintenant, vous voulez savoir quelles configurations de sécurité sont en place pour Outlook et quelles configurations peuvent être ajoutées pour améliorer son indice de menace.

Dans le tableau de bord **Security Insight**, cliquez sur **Outlook**, puis cliquez sur l'onglet **Safety Index**. Examiner les renseignements fournis dans la zone **Résumé de l'indice de sécurité**.



Sur le nœud **Configuration du pare-feu d'application**, cliquez sur **Outlook\_Profile** et vérifiez les informations de vérification de sécurité et de violation de signature dans les graphiques à secteurs.





Vérifiez l'état de configuration de chaque type de protection dans le tableau récapitulatif du pare-feu de l'application. Pour trier le tableau d'une colonne, cliquez sur l'en-tête de colonne.

Application Firewall Summary

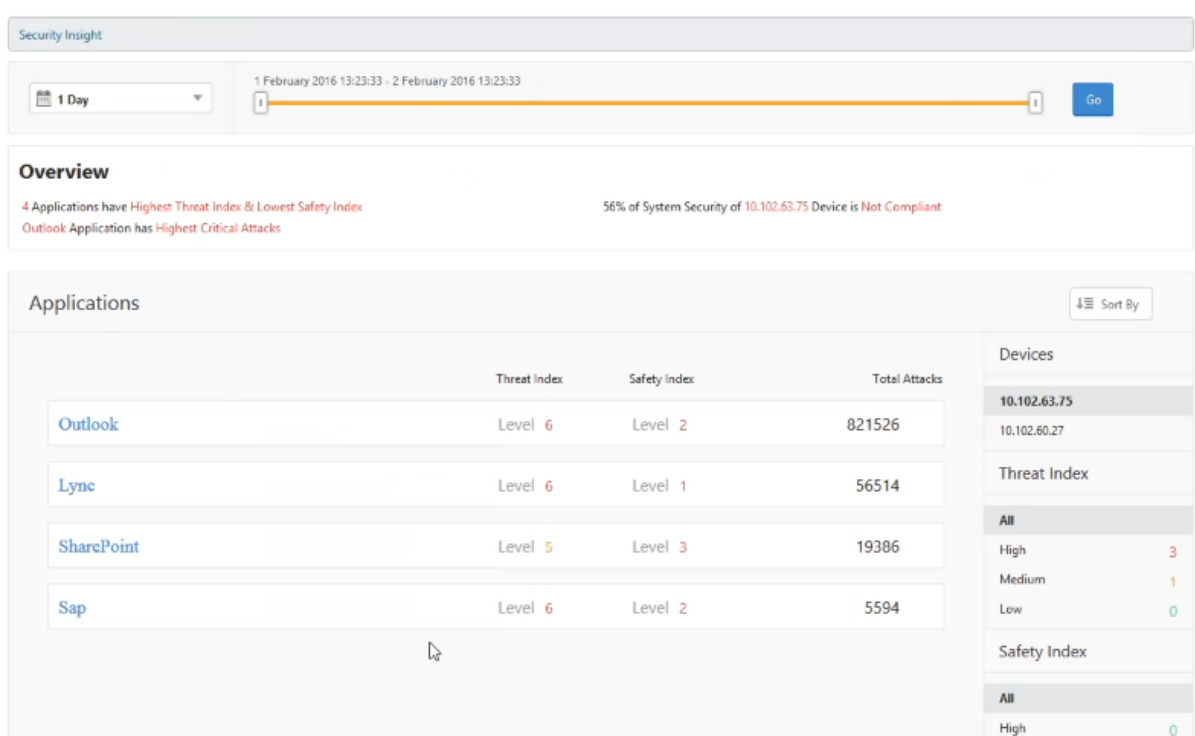
Protections	Configuration Status
XML Attachment	Not Configured
XML DoS	Not Configured
XML Format	Not Configured
XML SOAP Fault	Not Configured
XML SQL	Not Configured
XML Validation	Not Configured
XML WSI	Not Configured
XML XSS	Not Configured
Buffer Overflow	Log Stat Block
Buffer Overflow	Log Block
Content Type	Log

Cliquez sur le nœud **NetScaler System Security** et passez en revue les paramètres de sécurité du système et les recommandations Citrix pour améliorer l'index de sécurité des applications.

### Identifier les applications nécessitant une attention immédiate

Les applications qui nécessitent une attention immédiate sont celles qui présentent un indice de menace élevé et un indice de sécurité faible.

Dans cet exemple, Microsoft Outlook et Microsoft Lync ont une valeur d'indice de menace élevée de 6, mais Lync a le plus faible des deux index de sécurité. Par conséquent, vous devrez peut-être concentrer votre attention sur Lync avant d'améliorer l'environnement de menace pour Outlook.



### Déterminer le nombre d'attaques au cours d'une période donnée

Vous pouvez déterminer le nombre d'attaques survenues sur une application donnée à un moment donné ou étudier le taux d'attaque pour une période donnée.

Sur la page Security Insight, cliquez sur n'importe quelle application et, dans le **résumé de l'application**, cliquez sur le nombre de violations. La page Total des violations affiche les attaques de manière graphique pendant une heure, un jour, une semaine et un mois.



Le tableau Récapitulatif des applications fournit des détails sur les attaques. Certains d'entre eux sont les suivants :

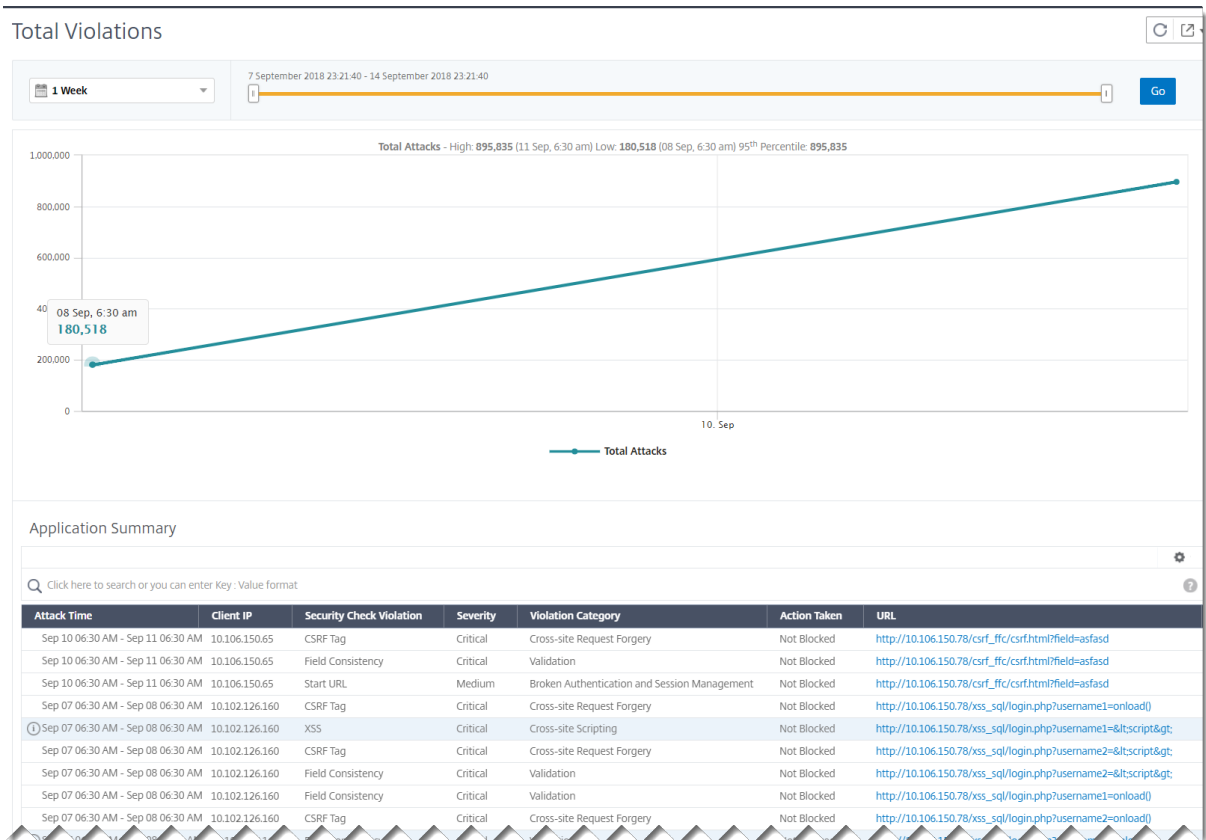
- Temps d'attaque
- Adresse IP du client à partir duquel l'attaque s'est produite
- Gravité
- Catégorie de violation
- URL d'origine de l'attaque, et d'autres détails.

Application Summary

Click here to search or you can enter Key : Value format

Attack Time	Client IP	Security Check Violation	Severity	Violation Category	Action Taken	URL	Transaction ID
Sep 11 11:05 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0
Sep 11 10:22 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0
Sep 11 11:02 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0
Sep 11 10:46 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0
Sep 11 10:57 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0
Sep 11 11:11 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0
Sep 11 10:50 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0
Sep 11 10:54 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0
Sep 11 11:02 PM	10.106.150.66	Field Consistency	Critical	Validation	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0
Sep 11 10:46 PM	10.106.150.66	CSRF Tag	Critical	Cross-site Request Forgery	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0
Sep 11 11:10 PM	10.106.150.66	Field Consistency	Critical	Validation	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0
Sep 11 10:50 PM	10.106.150.66	CSRF Tag	Critical	Cross-site Request Forgery	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0
Sep 11 10:54 PM	10.106.150.66	Field Consistency	Critical	Validation	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0
Sep 11 11:05 PM	10.106.150.66	CSRF Tag	Critical	Cross-site Request Forgery	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0
Sep 11 11:05 PM	10.106.150.66	Field Consistency	Critical	Validation	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=&lt;javascript&gt;	0

Bien que vous puissiez toujours afficher l'heure de l'attaque dans un rapport horaire comme indiqué dans l'image, vous pouvez maintenant afficher la plage de temps d'attaque pour les rapports agrégés, même pour les rapports quotidiens ou hebdomadaires. Si vous sélectionnez « 1 jour » dans la liste de périodes, le rapport Security Insight affiche toutes les attaques qui sont agrégées et le temps d'attaque est affiché dans une plage d'une heure. Si vous choisissez « 1 semaine » ou « 1 mois », toutes les attaques sont agrégées et le temps d'attaque est affiché dans une plage d'un jour.



### Obtenir des informations détaillées sur les violations de sécurité

Vous pouvez afficher la liste des attaques sur une application et obtenir des informations sur le type et la gravité des attaques, les actions entreprises par l'instance Citrix ADC, les ressources demandées et la source des attaques.

Par exemple, vous pouvez déterminer le nombre d'attaques sur Microsoft Lync bloquées, les ressources demandées et les adresses IP des sources.

Sur le tableau de **bord Security Insight**, cliquez sur **Lync > Nombre total de violations**. Dans le tableau, cliquez sur l'icône de filtre dans l'en-tête de colonne **Action prise**, puis sélectionnez **Bloqué**



Application Summary									
Security Check Violation	Severity	Violation Category	Action Taken	Location	Signature Violation	Violation Name	Violation Value	Found In	
0	Start URL	Critical	Broken Authentication and Session Management	Blocked	uri/test1.html			Form Field	
0	Start URL	Critical	Broken Authentication and Session Management	Blocked	uri/test2.html			Form Field	
0	Start URL	Critical	Broken Authentication and Session Management	Blocked	http://10.102.63.82/uri/test3.html			Form Field	
0	Start URL	Critical	Broken Authentication and Session Management	Blocked	http://10.102.63.82/uri/test4.html			Form Field	
0	Start URL	Critical	Broken Authentication and Session Management	Blocked	http://10.102.63.82/uri/test5.html			Form Field	
0	Start URL	Critical	Broken Authentication and Session Management	Blocked	http://10.102.63.82/uri/test6.html			Form Field	
0	Start URL	Critical	Broken Authentication and Session Management	Blocked	http://10.102.63.82/uri/test7.html			Form Field	
0	Start URL	Critical	Broken Authentication and Session Management	Blocked	http://10.102.63.82/uri/test8.html			Form Field	
0	Start URL	Critical	Broken Authentication and Session Management	Blocked	http://10.102.63.82/uri/test10.html			Form Field	
0	Start URL	Critical	Broken Authentication and Session Management	Blocked	http://10.102.63.82/uri/test9.html			Form Field	
0	Start URL	Critical	Broken Authentication and Session Management	Blocked	http://10.102.63.82/uri/test11.html			Form Field	
0	Start URL	Critical	Broken Authentication and Session Management	Blocked	http://10.102.63.82/uri/test12.html			Form Field	

Pour plus d’informations sur les ressources demandées, consultez la colonne **URL**. Pour plus d’informations sur les sources des attaques, consultez la colonne **IP du client**.

### Afficher les détails des expressions du journal

Les instances de Citrix ADC utilisent des expressions de journal configurées avec le profil de pare-feu d’application pour prendre des mesures en cas d’attaques sur une application de votre entreprise. Dans Security Insight, vous pouvez afficher les valeurs renvoyées pour les expressions de journal utilisées par l’instance de Citrix ADC. Ces valeurs incluent l’en-tête de la requête, le corps de la requête, etc. Outre les valeurs d’expression de journal, vous pouvez également afficher le nom de l’expression de journal et le commentaire de l’expression de journal définie dans le profil Application Firewall que l’instance de Citrix ADC a utilisée pour exécuter l’attaque.

**Conditions préalables** Assurez-vous que vous :

- Configurez les expressions de journal dans le profil du pare-feu d’application. Pour plus d’informations, consultez la section [Pare-feu d’application](#).
- Activez le paramètre Security Insights basé sur l’expression de journal dans Citrix ADM. Procédez comme suit :
  1. Accédez à **Analytics > Paramètres**, puis cliquez sur **Activer les fonctionnalités pour Analytics**.
  2. Dans la page Activer la fonctionnalité pour Analytics, sélectionnez **Activer Security Insight** dans la section **Log Expression Security Insight Setting**, puis cliquez sur **OK**.

← Enable Features for Analytics

**Multihop Settings**

Enable the Multihop feature if the network deployment has more than one NetScaler appliance or NetScaler Gateway appliance between a single client and a server connection. NetScaler MAS analyses the number of hops for NetScaler Gateway appliances through which the ICA connections pass. NetScaler MAS also collects and correlates the AppFlow records from all the appliances.

Enable Multihop ?

**Adaptive Threshold Settings**

Enable the adaptive threshold functionality feature to send a syslog message to the syslog server if the maximum number of hits on a URL is greater than the threshold value set. The feature dynamically sets the threshold value in NetScaler MAS for the maximum number of hits on each URL.

Enable Adaptive Threshold

**TCP Insight Settings**

Enable the TCP Insight feature of NetScaler MAS to provide an easy and scalable solution for monitoring the metrics of the optimization techniques and congestion control strategies (or algorithms) used in NetScaler appliances to avoid network congestion in data transmission.

Enable TCP Insight

**Web Insight Settings**

Enable the Web Insight feature to allow NetScaler MAS to retrieve the performance reports of web applications (load balancing and content switching virtual servers) that are bound to the NetScaler ADC. Web Insight enables visibility into enterprise web applications and allows IT administrators to monitor all web applications being served by the NetScaler ADC by providing integrated and real-time monitoring of applications.

Enable Web Insight

**Log Expression Based Security Insights Settings**

Enable Log Expression based Security Insights to report log expression data configured with Application Firewall profile.

Enable Security Insight ?

OK Close

Par exemple, vous pouvez afficher les valeurs de l'expression de journal renvoyée par l'instance de Citrix ADC pour l'action qu'elle a effectuée pour une attaque sur Microsoft Lync dans votre entreprise.

Dans le tableau de bord Security Insight, accédez à **Lync > Total des violations**. Dans le **tableau Résumé de l'application**, cliquez sur l'URL pour afficher les détails complets de la violation dans la page **Informations sur la violation**, y compris le nom de l'expression de journal, le commentaire et les valeurs renvoyées par l'instance Citrix ADC pour l'action.

- Gateway Insight >
- Security Insight >
- Settings >
- Troubleshooting >
- Orchestration >
- System >
- Downloads

**Violation Information** ✕

Violation Information

Attack Time	NA
Signature Violation	
Violation Name	
Violation Value	
Security Check Violation	Start URL
Violation Category	Broken Authentication and Session Management
Threat Index	5
Severity	Medium
Action Taken	Blocked
URL	http://10.102.60.245/csrf_ffc/ffc.html?field1=asfasd
Found In	Other Location
Client IP	10.102.63.79
Location	Bangalore
Total Attacks	1

Log Expression Name	Log Expression Comment	Log Expression Value
LGEXPR7	http request contains keyword	false
LGEXPR8	http request contains header	false
LGEXPR6	http method expression	GET /csrf_ffc/ffc.html?field1=asfasd HTTP/1.1 User-Agent: curl/7.19.7 (x86_64-pc-linux-gnu) libcurl/7.19.7 OpenSSL/0.9.8k zlib/1.2.3.3 libidn/1.15 Host: 10.102.60.245 Accept: */*
LGEXPR3	http method expression	true
LGEXPR4	http request contains header	
LGEXPR1	http request header contains user agent	curl/7.19.7 (x86_64-pc-linux-gnu) libcurl/7.19.7 OpenSSL/0.9.8k zlib/1.2.3.3 libidn/1.15
LGEXPR2	http method expression	false
LGEXPR5	http method expression	

### Déterminez l'indice de sécurité avant de déployer la configuration

Des violations de sécurité se produisent après le déploiement de la configuration de sécurité sur une instance Citrix ADC, mais vous pouvez évaluer l'efficacité de la configuration de sécurité avant de la déployer.

Par exemple, vous pouvez évaluer l'indice de sécurité de la configuration de l'application SAP sur l'instance Citrix ADC avec l'adresse IP 10.102.60.27.

Dans le tableau de bord **Security Insight**, sous **Périphériques**, cliquez sur l'adresse IP de l'instance Citrix ADC que vous avez configurée. Vous pouvez voir que l'indice de menace et le nombre total d'attaques sont 0. L'index des menaces est un reflet direct du nombre et du type d'attaques sur l'application. Aucune attaque indique que l'application n'est soumise à aucune menace.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

860

The screenshot shows the NetScaler Application Delivery Management interface. At the top, there is a time range selector set to '1 Day' and a date range from '1 February 2016 13:33:35' to '2 February 2016 13:33:35'. Below this is an 'Overview' section with the following text: '4 Applications have Highest Threat Index & Lowest Safety Index' and '56% of System Security of 10.102.63.75 Device is Not Compliant'. A note states 'Outlook Application has Highest Critical Attacks'. The main section is titled 'Applications' and contains a table with columns for Application Name, Threat Index, Safety Index, and Total Attacks. The applications listed are Lync, Sap, Outlook, and SharePoint. To the right of the table is a 'Devices' section showing IP addresses 10.102.63.75 and 10.102.60.27, and a 'Threat Index' section with a table showing counts for High, Medium, and Low threat levels.

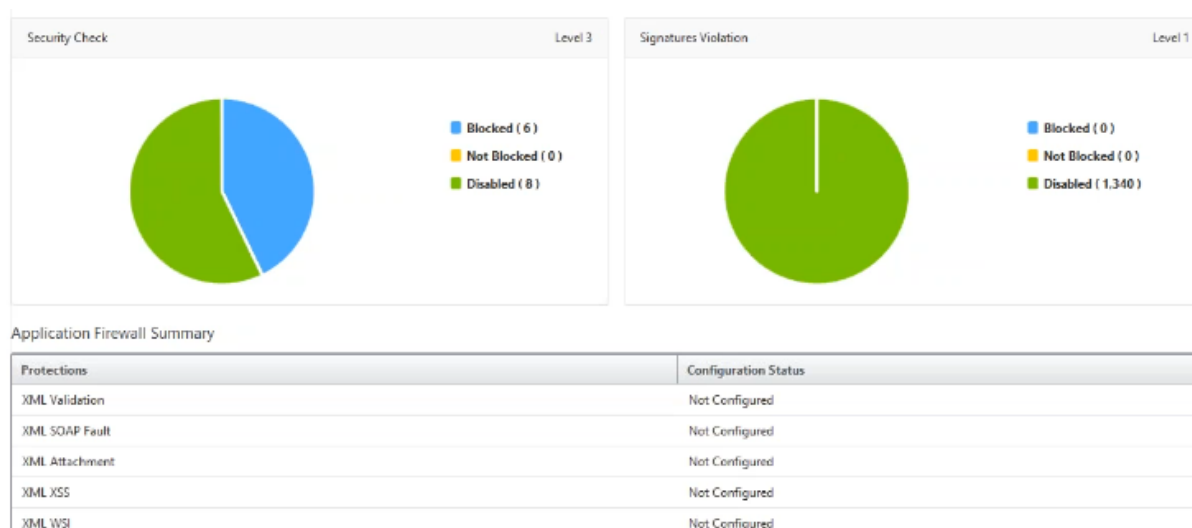
Application	Threat Index	Safety Index	Total Attacks
Lync	Level 6	Level 2	4922
Sap	Level 0	Level 3	0
Outlook	Level 0	Level 6	0
SharePoint	Level 0	Level 6	0

Cliquez sur **SAP > Indice de sécurité > Profil SAP\_et** évaluez les informations relatives à l'indice de sécurité qui s'affichent.

The screenshot shows the 'Application Summary' section for SAP. It includes four summary cards: 'Total Violations' (5594), 'Violations By Severity' (Critical 5846), 'Violations By Action' (Blocked 5846), and 'Violations By Category' (Cross-site Scripting 5846). Below these is a 'Threat Index' (Level 6) and 'Safety Index' (Level 2) section with circular progress indicators. The 'Safety Index Summary' section contains two cards: 'Application Firewall Configuration' (Signatures: 1295/1300 Not Configured, Security Check: 3/14 Not Configured) and 'System Security Settings' (6/10 Not Configured). At the bottom, there is a table for 'Application Firewall Configuration' with columns for Name and Safety Index.

Configuration	Name	Safety Index
Application Firewall Configuration Level 2	Sap_Profile	2
NetScaler System Security Level 2		

Dans le résumé du pare-feu de l'application, vous pouvez afficher l'état de configuration des différents paramètres de protection. Si un paramètre est défini pour consigner ou si un paramètre n'est pas configuré, un indice de sécurité inférieur est attribué à l'application.



## SSL Insight

February 1, 2024

SSL Insight fournit une visibilité sur les transactions Web sécurisées (HTTPS) et permet aux administrateurs informatiques de surveiller toutes les applications Web sécurisées desservies par l’Citrix ADC en fournissant une surveillance intégrée et en temps réel et historique des transactions Web sécurisées. Avec cette visibilité, l’administrateur peut évaluer les éléments suivants :

- **Déterminer l’impact des modifications de configuration sur l’utilisation** par les clients : l’administrateur peut comprendre l’impact sur les clients d’une modification de configuration, telle que la désactivation de SSLv3 ou la suppression d’un chiffrement tel que RC4-MD5. Cela peut être fait en évaluant les données de transaction historiques sur ce protocole et en chiffrement.
- **Quantifier les performances du client** : l’administrateur peut comprendre l’impact sur le temps de réponse de l’application en fonction des chiffres/protocoles SSL utilisés ou des certificats négociés.
- **Sécurité** des applications : déterminez si les transactions de l’une des applications s’exécutent sur des protocoles de sécurité, des chiffrements ou un niveau de clé faible.

Lorsque SSL Analytics est activé sur une instance Citrix ADC, les statistiques SSL sont enregistrées et consignées pour chaque transaction SSL. Les statistiques montrent les détails du flux SSL. En outre, chaque connexion réussie est enregistrée et affichée par Citrix Application Delivery Management (ADM) Analytics.

SSL Insight fournit les informations critiques suivantes, affichées par Citrix ADM Analytics :

- Version du protocole SSL négociée
- Chiffrement négocié et force du chiffrement
- Algorithme de hachage de signature du certificat utilisé
- Type et taille du certificat
- Erreurs SSL frontend et backend

#### Remarque

Pour des connexions SSL réussies, la journalisation SSL AppFlow a lieu à la fin de chaque transaction.

### Conditions préalables

- L'instance Citrix ADC sur laquelle vous souhaitez configurer SSL Insight doit exécuter le logiciel Citrix ADC version 11.1 51.21 et supérieure. Exécutez les commandes suivantes sur l'instance ADC exécutant 11.1 51.21 pour activer Logstream en tant que type de transport pour SSL Insight.

1. `enable ns mode ulfd`

2. `add ulfd server <IP Address of the ADM>`

Pour les instances ADC exécutant la version 12.0 et supérieure, sélectionnez Logstream comme type de transport tout en activant AppFlow à partir d'ADM.

- La version et le build de Citrix ADM doivent être égaux ou supérieurs à la version et au build de Citrix ADC. Par exemple, si vous avez installé Citrix ADM 11.1 build 61.7, assurez-vous d'avoir installé Citrix ADC 11.1 build 60.14 ou version antérieure.

### Configuration de SSL Insight

Les mesures SSL Insight sont incluses dans les rapports Web Insight si vous activez les éléments suivants :

- Activez AppFlow pour Web Insight sur chaque instance de Citrix ADC.
- Activez le mode ULFD sur chaque instance de Citrix ADC.
- Activez les paramètres AppFlow requis sur chaque instance de Citrix ADC.

## Activation de la fonctionnalité AppFlow

### Remarque

Vous pouvez activer la fonctionnalité AppFlow à partir de Citrix ADM ou de chaque instance Citrix ADC.

### Pour activer la fonctionnalité AppFlow à partir de Citrix ADM :

1. Accédez à **Réseaux > Instances**, puis sélectionnez l'instance Citrix ADC sur laquelle vous souhaitez activer les analyses.
2. Dans la liste **Sélectionner une action**, sélectionnez **Configurer Analytics**.
3. Sélectionnez les serveurs virtuels, puis cliquez sur **Activer AppFlow**.
4. Dans le champ Activer AppFlow, tapez **true** et sélectionnez **Web Insight**.
5. Répétez les étapes 3 à 6 sur chaque instance de Citrix ADC.
6. Cliquez sur **OK**.

### Enable AppFlow

Select Expression \*

Load Balancing

▼

Transport Mode  IPFIX  Logstream

Web Insight

Client Side Measurement

Security Insight

If the AppFlow for a virtual server is enabled on more than one Application Delivery Management appliance, then the appliance on which the AppFlow is enabled most recently has the highest priority for collecting the information.

OK

Cancel

### Remarque

Vous ne pouvez pas activer la collecte de données sur un serveur virtuel si l'état de fonctionnement du serveur virtuel est autre que UP.

**Pour activer la fonctionnalité AppFlow à l'aide de l'interface utilisateur graphique Citrix ADC :**

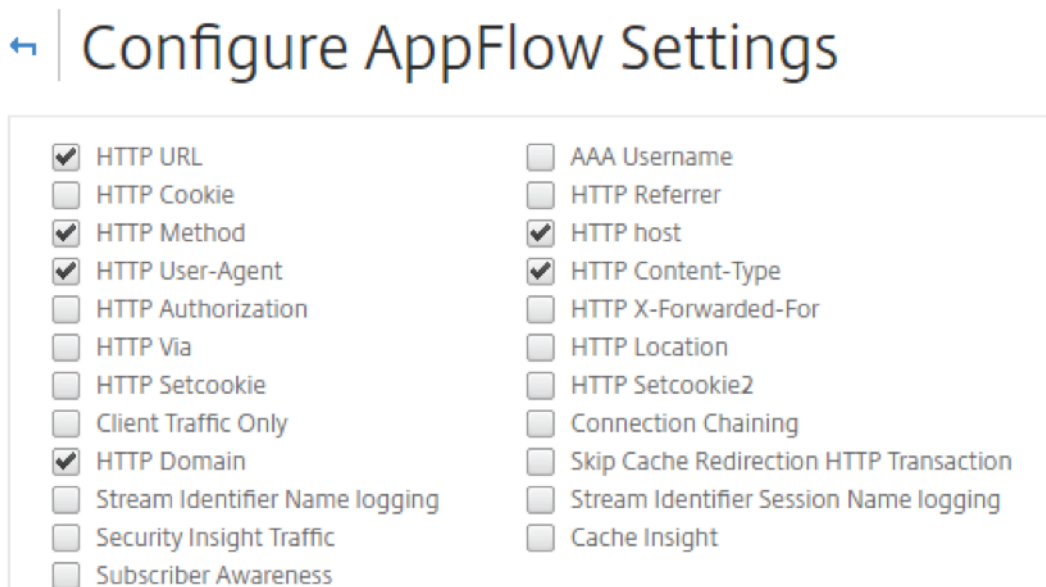
Dans l'interface graphique d'une instance Citrix ADC, accédez à **Configuration > Système > Paramètres**, cliquez sur **Configurer les fonctionnalités avancées**, puis sélectionnez **AppFlow**.

**Activation des paramètres SSL Insight**

Sur chaque instance Citrix ADC, vous devez activer certains paramètres HTTP pour afficher les enregistrements SSL Insight dans Citrix ADM.

**Pour activer les paramètres SSL Insight à partir de l'utilitaire de configuration Citrix ADC :**

1. Accédez à **Configuration > Système > AppFlow**, puis cliquez sur **Modifier les paramètres d'AppFlow**.
2. Cochez les cases suivantes : **Domaine HTTP, Hôte HTTP, Méthode HTTP, URL HTTP, Agent utilisateur HTTP, Type de contenu HTTP**.
3. Cliquez sur **OK**.



**Affichage des mesures SSL Insight**

Les mesures SSL Insight dans Citrix ADM fournissent une vue détaillée des performances des transactions SSL servies par les instances Citrix ADC. Vous pouvez afficher les mesures SSL Insight au niveau du client, du serveur ou de l'application, ainsi que les mesures des transactions de succès et d'échec



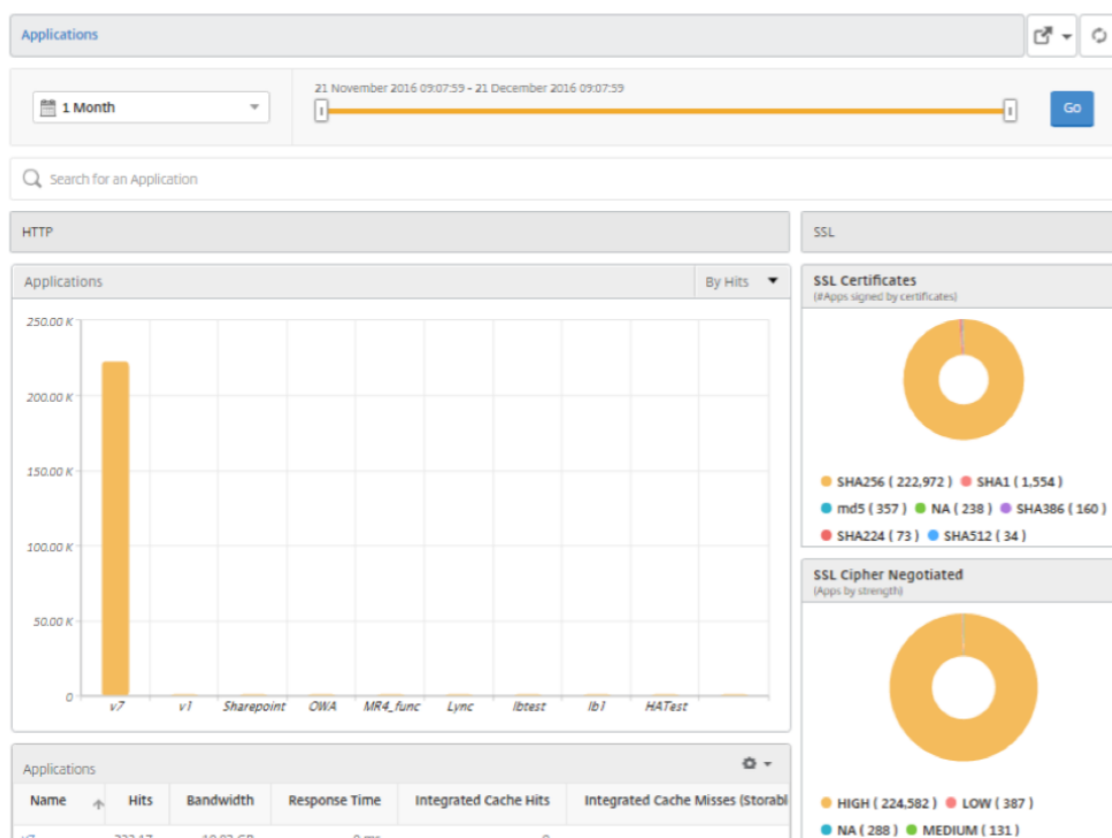
SSL. À l'aide de ces mesures, vous pouvez analyser et optimiser vos paramètres HTTPS Citrix ADC et les paramètres de certificat SSL, et suivre les problèmes de performances.

**Pour surveiller les mesures SSL Insight dans Citrix ADM :**

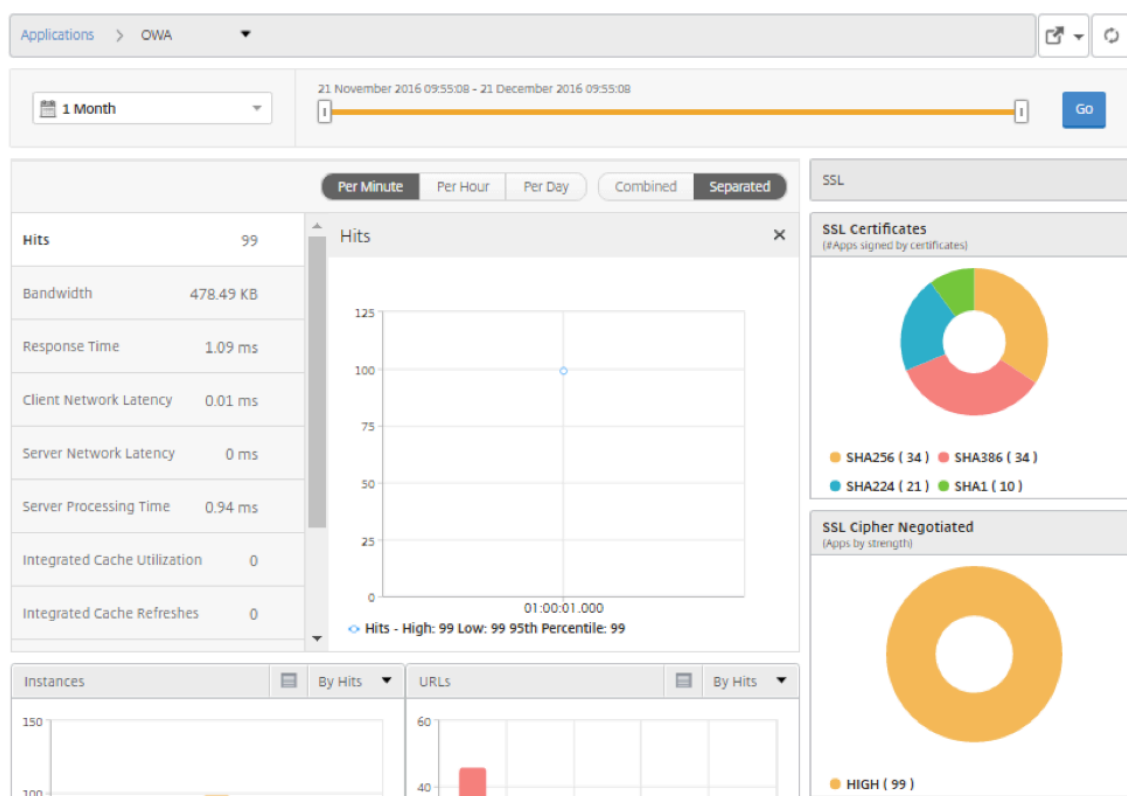
1. Dans l'onglet **Analytics** , accédez à Web Insight et cliquez sur le nœud **Client**, **Serveur** ou **Application** pour afficher les mesures relatives aux clients, au serveur ou aux applications, respectivement.
2. Dans le volet supérieur gauche, dans la liste des périodes, sélectionnez la période dont vous souhaitez afficher les mesures. Vous pouvez personnaliser la période à l'aide du curseur temporel. Cliquez sur **OK**.
3. Les mesures SSL Insight apparaissent sous forme de graphiques à secteurs, sur lesquels vous pouvez cliquer pour plus de détails.

**Remarque**

Les graphiques à secteurs affichent les mesures de toutes les applications, clients ou serveurs.



4. Pour afficher les détails d'une application, d'un client ou d'un serveur spécifique, cliquez sur la valeur correspondante dans le graphique à barres.



5. Pour afficher les transactions SSL en échec, dans la section SSL, sélectionnez le bouton radio de la section SSL.

### Cas d'utilisation : obtenir une vue d'ensemble des transactions SSL des applications, des clients ou des serveurs

Le cas d'utilisation suivant décrit comment vous pouvez utiliser SSL Insight pour évaluer l'utilisation de divers paramètres SSL dans les applications, les clients et les serveurs, et améliorer les mesures de sécurité.

Considérez que vous disposez d'un ensemble d'applications qui utilisent des transactions SSL (HTTPS) pour la communication et que vous avez configuré Citrix ADM pour surveiller les composants SSL. Il se peut que vous deviez examiner fréquemment les demandes afin que vous puissiez d'abord vous concentrer sur les applications qui nécessitent le plus d'attention. Le tableau de bord SSL Insight fournit un résumé des différents paramètres SSL utilisés par vos applications sur une période de temps de votre choix et pour un périphérique Citrix ADC sélectionné. Ils sont :

- Certificats SSL
- Protocoles SSL
- Cipher SSL négocié
- Force des clés SSL

- Échec SSL —Frontend
- Échec SSL —Backend

**SSL Usage**  
SSL usage by certificates, protocols, ciphers negotiated and key strength

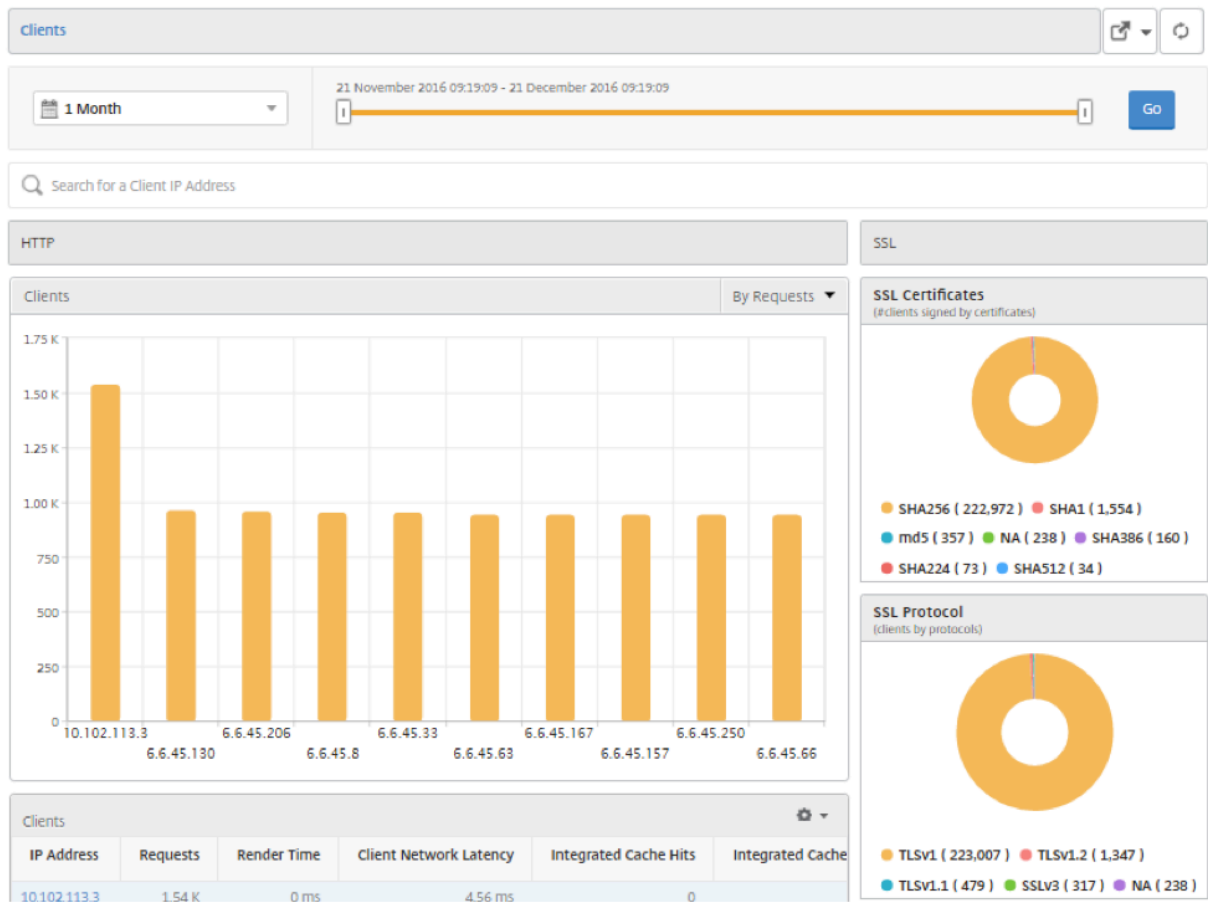
Certificates	Protocols	Ciphers	Key Strength
<b>4</b>	<b>2</b>	<b>1</b>	<b>4</b>

**Certificates** Protocols Ciphers Key Strength

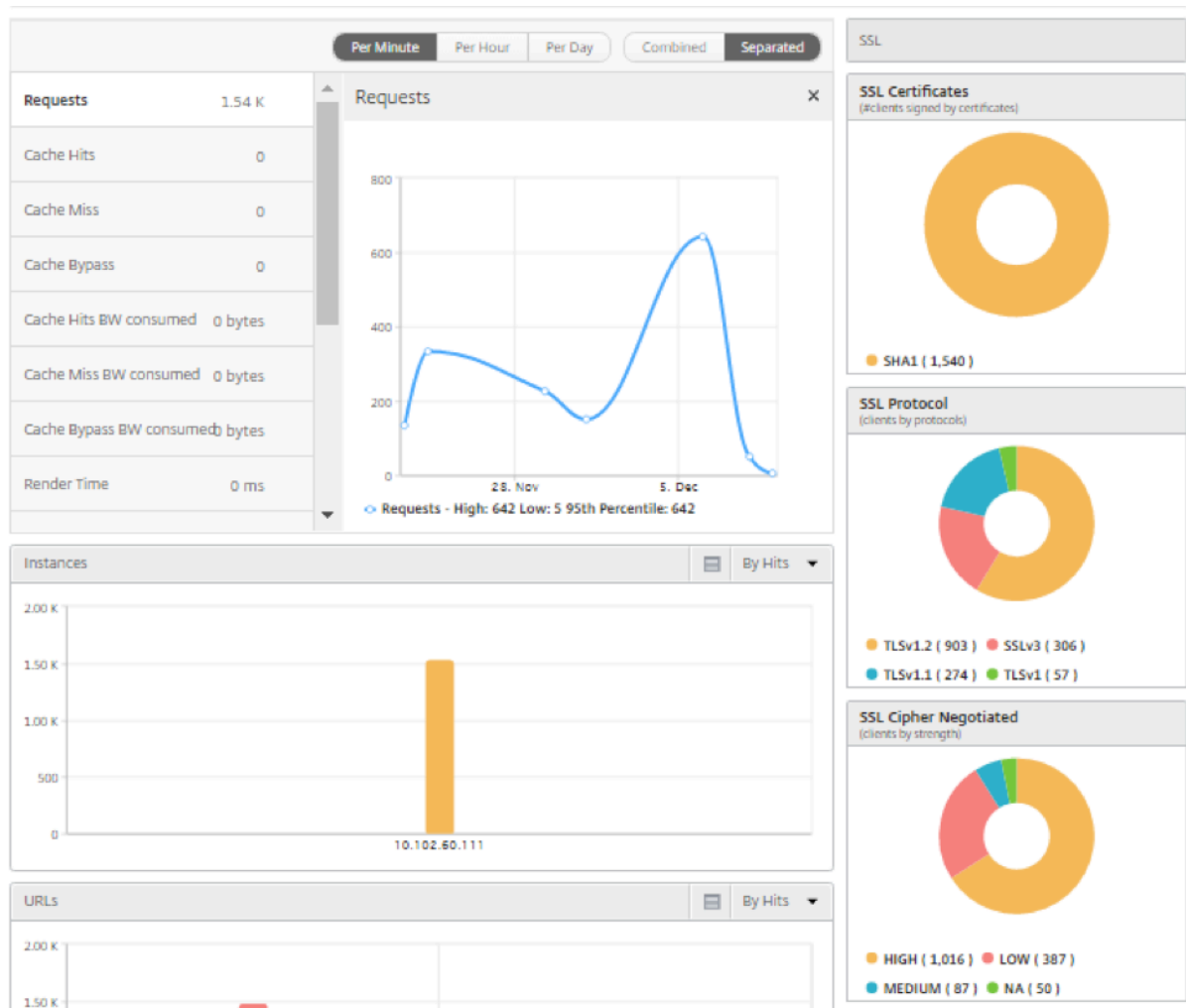
CERTIFICATES	NO. OF OCCURENCES
SHA1	6.1M
SHA256	3.5M
SHA224	863.2K
SHA384	664.5K

[See more](#)

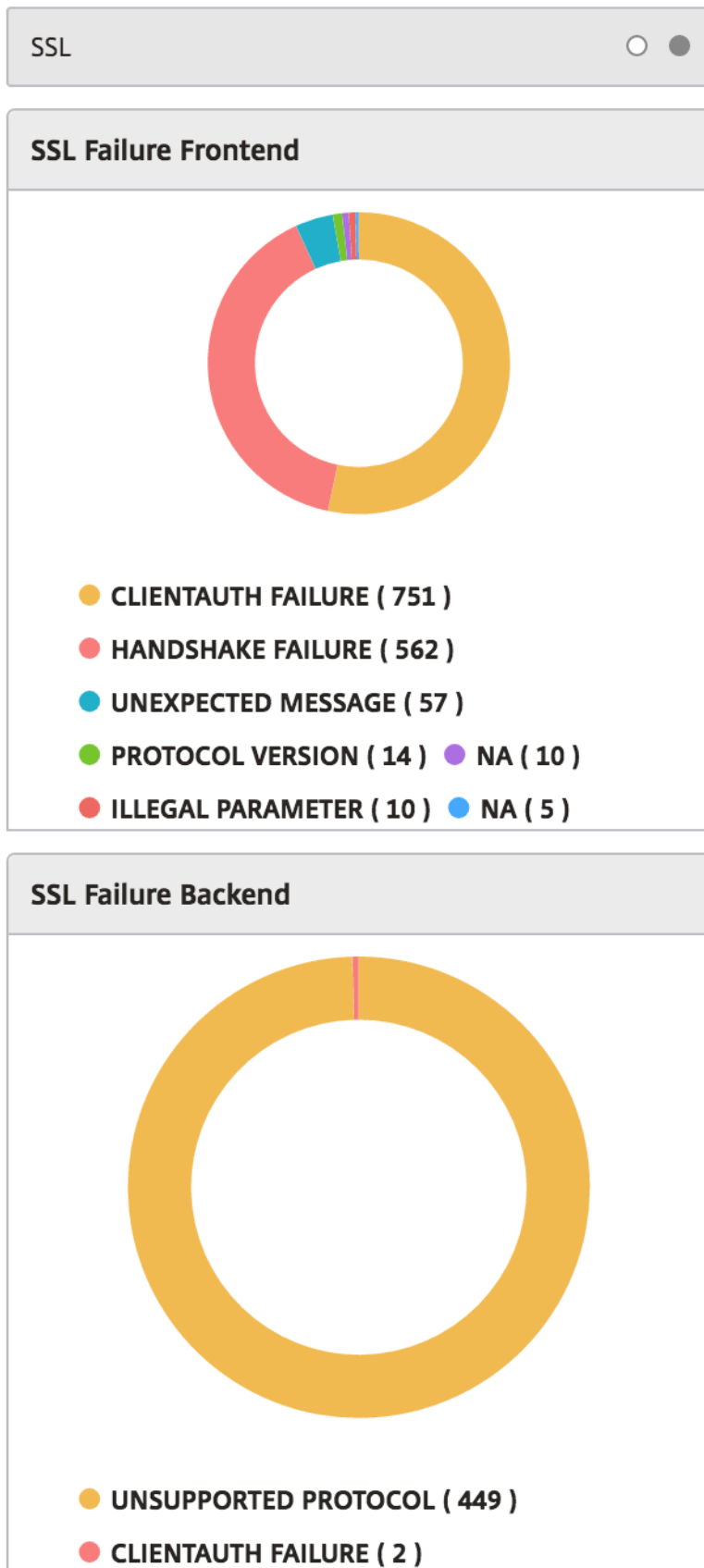
Dans l'exemple suivant, vous pouvez voir la liste des clients (identifiés par leurs adresses IP) et les accès SSL par client. En outre, à droite, vous pouvez afficher les paramètres SSL pour tous les clients.



Pour afficher les détails SSL d'un client, sélectionnez le client sur le graphique à barres ou dans le tableau situé sous le graphique. Dans l'exemple suivant, les transactions du client sélectionné utilisent un certificat SSL SHA1 et quatre protocoles principaux : TLSv1.2, TLSv1.1, TLSv1 et SSLv3. Vous pouvez également voir que des chiffrements de diverses forces ont été négociés. Le code couleur indique la force du protocole SSL, qui vous donne des informations sur les chiffrements faibles et les chiffrements forts.



De même, pour afficher les informations sur les transactions SSL ayant échoué, sélectionnez le bouton radio de la section **SSL**. Les défaillances frontales et dorsales SSL sont affichées séparément dans deux graphiques circulaires. Dans l'exemple suivant, vous pouvez voir que les principales erreurs SSL back-end sont des échecs Handshake et que les erreurs SSL front-end majeures sont des paramètres illégaux.



## TCP Insight

February 1, 2024

La fonctionnalité TCP Insight de Citrix Application Delivery Management (ADM) fournit une solution simple et évolutive pour surveiller les mesures des techniques d'optimisation et des stratégies (ou algorithmes) de contrôle de la congestion utilisées dans les appliances Citrix ADC afin d'éviter la congestion réseau dans la transmission des données. Cette fonctionnalité utilise la fonctionnalité « TCP Speed Report », qui mesure les performances de téléchargement ou de chargement de fichiers TCP avec et sans optimisation TCP.

Vous pouvez afficher les principales mesures de la couche de transport, telles que le volume de données, le débit et la vitesse, et utiliser ces informations pour mesurer le volume de trafic desservi par les instances Citrix ADC et valider les avantages de l'optimisation TCP. Des ventilations par direction de flux (du client vers Citrix ADC et de Citrix ADC vers le serveur d'origine), par port TCP et par réseau local virtuel sont fournies pour les mesures.

### Conditions préalables

Avant de commencer à configurer la fonctionnalité TCP Insight, assurez-vous que les conditions préalables suivantes sont remplies :

- Les instances Citrix ADC s'exécutent sur la version logicielle 11.1 build 51.21 ou ultérieure.
- Vous avez installé Citrix ADM s'exécutant sur la version 11.1 build 51.21 ou ultérieure du logiciel.
- Tous les serveurs virtuels configurés pour une application sont sous licence pour la gestion et la surveillance sur Citrix ADM.

Pour plus d'informations sur les licences Citrix ADM, consultez la section [Licences](#).

### Configuration matérielle requise pour Citrix ADM:

---

Composant	Exigences
RAM	8 GB
CPU virtuel	4
	<b>Remarque</b> Citrix vous recommande d'utiliser 8 processeurs pour de meilleures performances.
Espace de stockage	120 GB

Composant

Exigences

**Remarque** Citrix vous recommande d'utiliser 500 Go pour de meilleures performances.

---

## Activation de TCP Insight

Avant de pouvoir afficher les métriques TCP Insight, vous devez activer la fonctionnalité sur Citrix ADM.

### Pour activer TCP Insight :

1. Ouvrez une session sur Citrix ADM à l'aide des informations d'identification de l'administrateur.
2. Accédez à **Analytics > Paramètres**, puis cliquez sur **Activer les fonctionnalités pour Analytics**.
3. Sur la page **Activer les fonctionnalités pour Analytics**, sélectionnez **Activer TCP Insight**.
4. Dans la fenêtre de confirmation, cliquez sur **OK**.

## Affichage des métriques TCP Insight dans Citrix ADM

Après avoir activé TCP Insight dans Citrix ADM, vous pouvez afficher les informations clés de la couche de transport telles que le mode de trafic (données Internet ou mobiles), le volume de données, le débit, les interfaces, les ports, la vitesse de téléchargement moyenne, la vitesse de téléchargement moyenne.

### Pour afficher les mesures TCP Insight dans Citrix ADM :

Accédez à **Analytics > TCP Insight**.

Vous pouvez placer le pointeur de la souris sur les graphiques à barres pour afficher le volume de données des techniques de transport correspondantes. Vous pouvez également afficher le volume de données et d'autres mesures dans le tableau situé sous le graphique.

#### Remarque

Vous pouvez personnaliser les mesures affichées dans le graphique à l'aide de l'icône des paramètres sur le tableau. Vous pouvez également sélectionner la période à laquelle les mesures se rapportent et utiliser le curseur temporel pour ajuster la période.

Vous pouvez également consulter des mesures concernant des éléments tels que les interfaces, les ports et les débits en les sélectionnant dans la liste TCP Insight.



## Cas d'utilisation

Les cas d'utilisation suivants illustrent certaines des manières d'utiliser TCP Insight sur les appliances Citrix ADC :

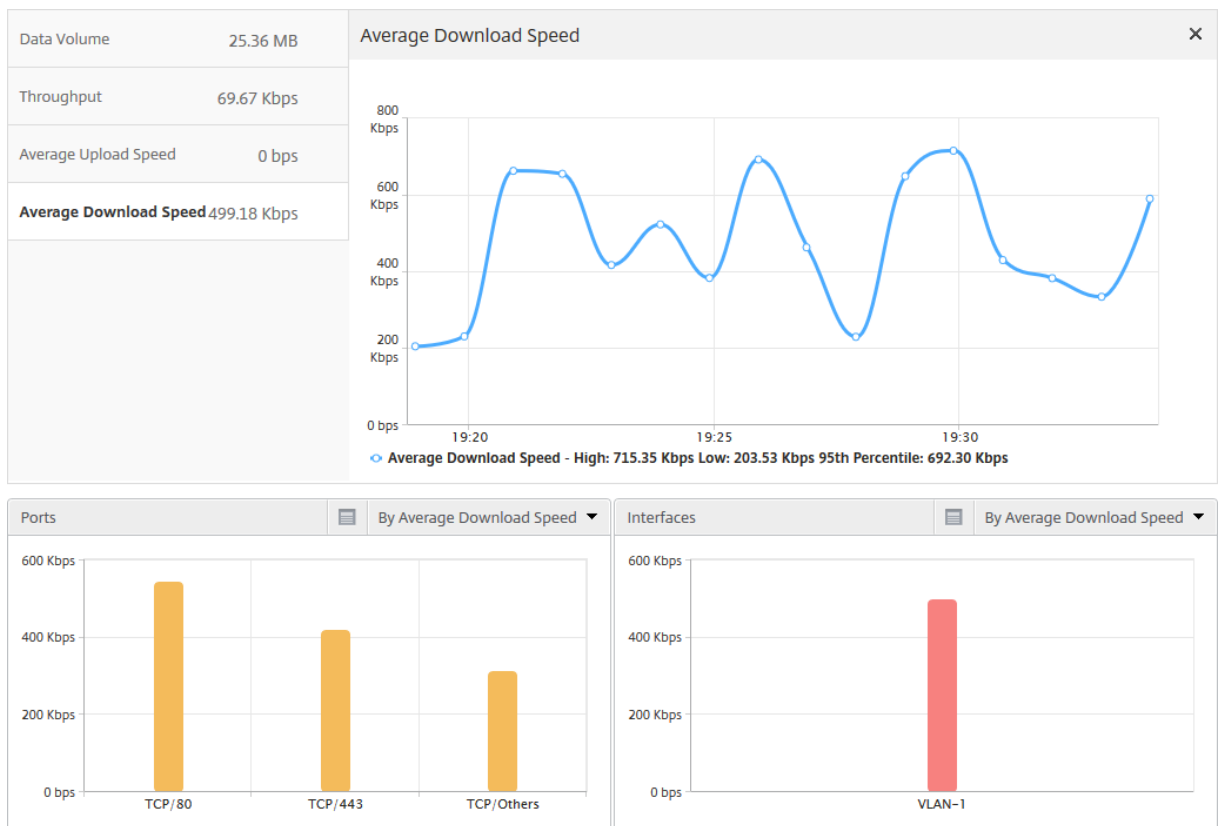
- Évaluez les avantages de l'optimisation TCP
- Régler les paramètres TCP
- Mesurer l'impact de l'optimisation TCP sur le volume de trafic

### Évaluez les avantages de l'optimisation TCP

Dans quelle mesure l'optimisation TCP de Citrix ADC bénéficie-t-elle réellement à un réseau mobile (radio) ou d'entreprise (Internet) ? Vous pouvez visualiser la vitesse des transferts de données effectués via TCP et comparer les performances optimisées et non optimisées. Ces mesures sont affichées séparément pour les directions de téléchargement et de téléchargement (toujours côté radio/client), et pour différents ports de destination, HTTP (80) et HTTPS (443).

En examinant les métriques TCP Insight, vous pouvez quantifier l'amélioration de la vitesse obtenue grâce à l'optimisation des flux TCP.

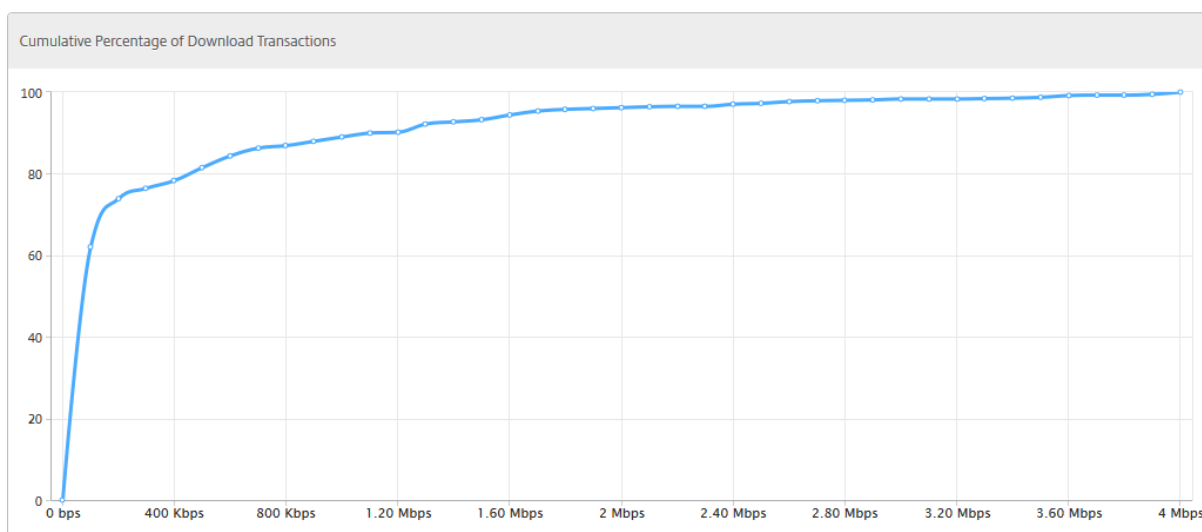
Pour afficher un résumé de ces paramètres, connectez-vous à Citrix ADM et cliquez sur l'onglet **TCP Insight**. Ensuite, cliquez sur **Côtés** et sélectionnez **Internet** ou **Radio** dans le graphique à barres ou dans le tableau situé sous le graphique.



### Régler les paramètres TCP

L'utilisation de différents profils TCP peut générer des sorties différentes pour le même trafic. Dans de telles situations, vous pouvez consulter et comparer les mesures de vitesse des périodes pendant lesquelles Citrix ADC exécute différents profils d'optimisation TCP. Vous pouvez utiliser les résultats pour ajuster les paramètres TCP afin d'accélérer la transmission et développer un profil TCP qui maximise l'expérience perçue par les utilisateurs sur un réseau client spécifique.

Pour afficher les rapports, connectez-vous à Citrix ADM. Ensuite, dans l'onglet **TCP Insight**, cliquez sur **Débits** et sélectionnez le débit souhaité dans le graphique à barres ou dans le tableau situé sous le graphique.

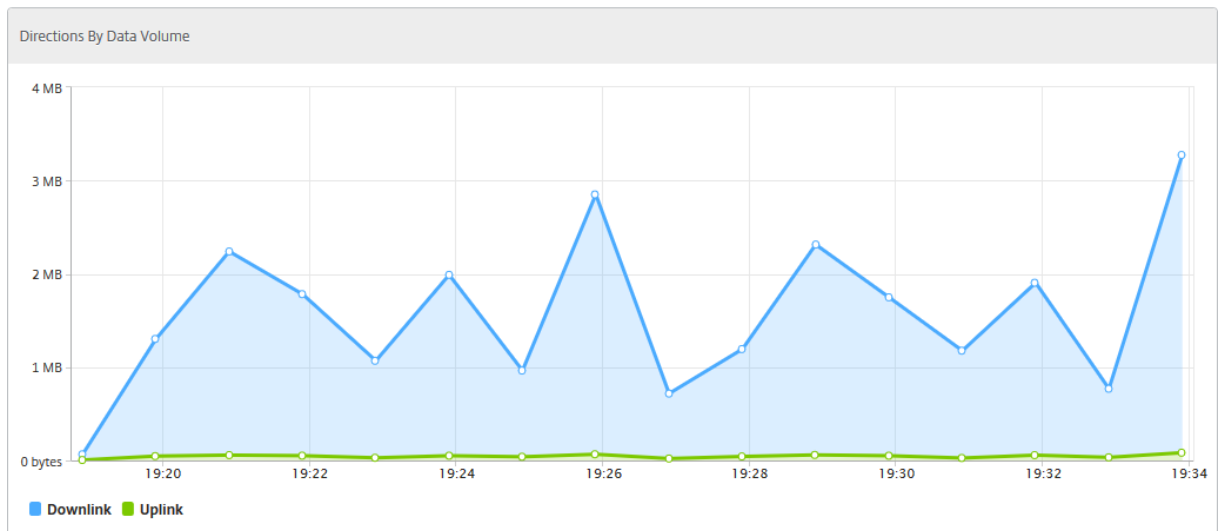


### Mesurer l'impact de l'optimisation TCP sur le volume de trafic

Les mesures du volume/débit de données de la couche IP gérées par une instance Citrix ADC peuvent être comparées entre différentes périodes afin d'évaluer l'effet de l'optimisation TCP sur la consommation de données des abonnés. Les mesures peuvent être appliquées séparément pour chaque côté du réseau (côté radio ou côté Internet), pour différents segments de trafic (délimités par différentes interfaces ou VLAN), pour chaque direction (liaison descendante ou liaison montante) et pour différents ports de destination (HTTP et HTTPS). La comparaison peut être utilisée pour confirmer que l'optimisation du protocole TCP encourage les abonnés à consommer davantage de données.

Pour obtenir un résumé des mesures, connectez-vous à Citrix ADM et, dans l'onglet **TCP Insight**, cliquez sur **Sides**, puis sélectionnez **Internet** ou **Radio** dans le graphique à barres ou dans le tableau situé sous le graphique.

Vous pouvez également sélectionner une autre période dans la liste des heures. Vous pouvez personnaliser la période à l'aide du curseur de période.

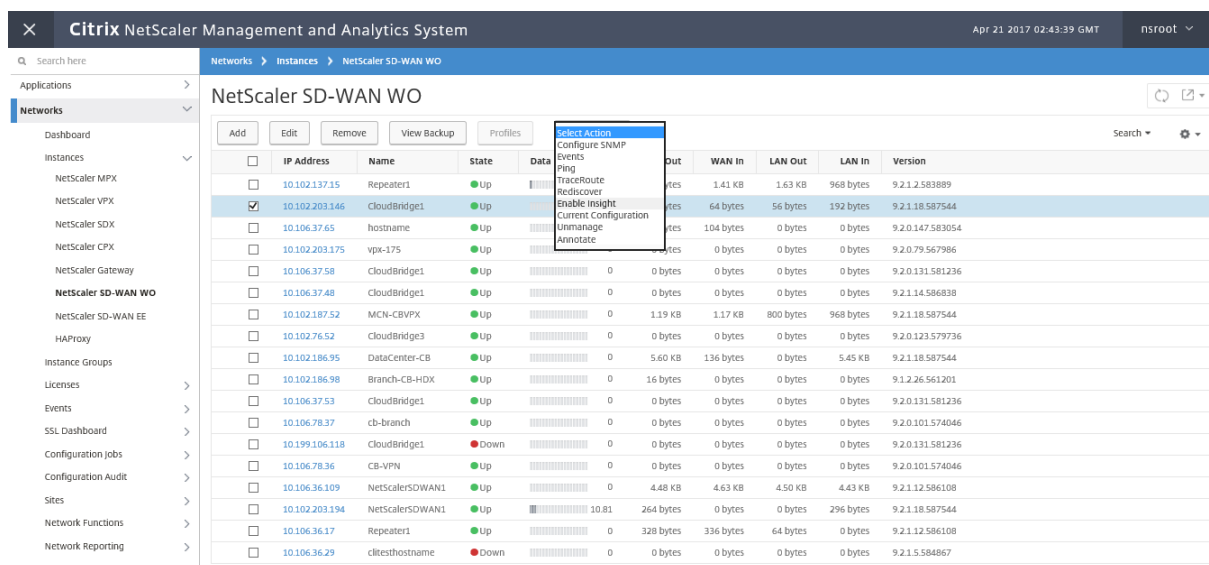


## WAN Insight

February 1, 2024

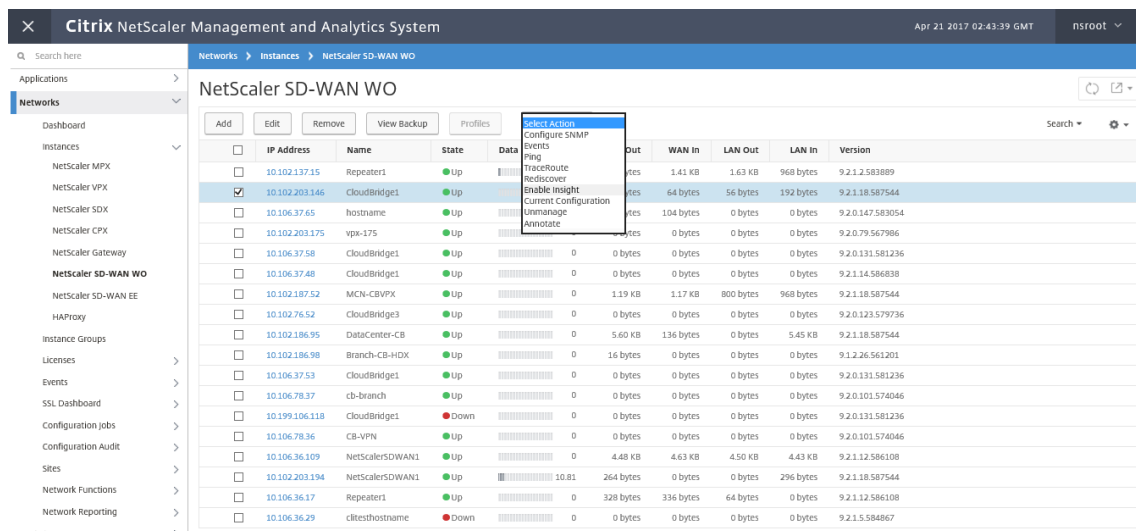
Les appliances d'optimisation WAN SD-WAN (WO) Citrix optimisent la livraison d'un grand nombre d'applications via le WAN, en améliorant l'efficacité du flux de données sur le réseau entre le centre de données et les sites de succursale. L'analyse WAN Insight permet aux administrateurs de surveiller facilement le trafic WAN accéléré et non accéléré qui circule entre le centre de données et les appliances d'optimisation WAN des succursales. WAN Insight fournit une visibilité sur les clients, les applications et les succursales sur le réseau, pour aider à résoudre efficacement les problèmes réseau. Les rapports en direct et historiques vous permettent de résoudre les problèmes de manière proactive, le cas échéant.

L'activation de l'analyse sur l'appliance d'optimisation du réseau étendu du centre de données permet à Citrix Application Delivery Management (ADM) de collecter des données et de fournir des rapports et des statistiques pour le centre de données et les appliances d'optimisation du réseau étendu des succursales.



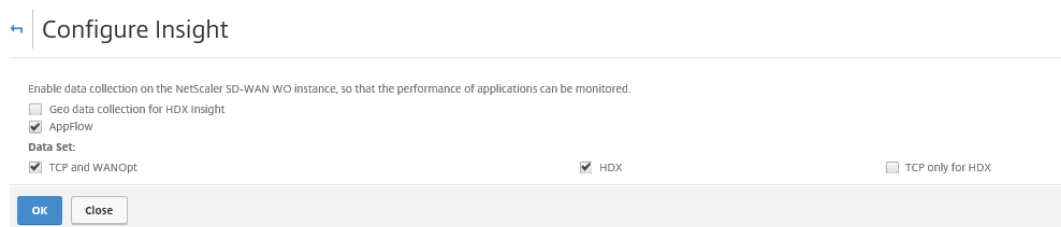
## Pour activer les analyses sur l'applicance d'optimisation WAN :

1. Dans un navigateur Web, saisissez l'adresse IP du Citrix ADM (par exemple, <http://192.168.100.1>).
2. Dans les champs **Nom d'utilisateur** et Mot de **passé**, entrez les informations d'identification de l'administrateur.
3. Accédez à **Réseaux > Instances > Citrix SD-WAN**, puis sélectionnez l'instance WO SD-WAN.



4. Dans la liste déroulante **Sélectionner une action**, sélectionnez **Configurer Analytics**.
5. Sélectionnez les paramètres suivants selon les besoins :
  - **Collecte de données géo pour HDX Insight** : partage l'adresse IP du client avec l'API Google Geo.
  - **AppFlow** : Commence à collecter des données à partir d'instances d'optimisation WAN.

- **TCP et WanOpt** : fournit des rapports TCP et WanOpt Insight.
- **HDX** : fournit des rapports HDX Insight.
- **TCP uniquement pour HDX** : fournit TCP uniquement pour les rapports HDX Insight.



6. Cliquez sur **OK**.

#### **Pour afficher les rapports WAN Insight :**

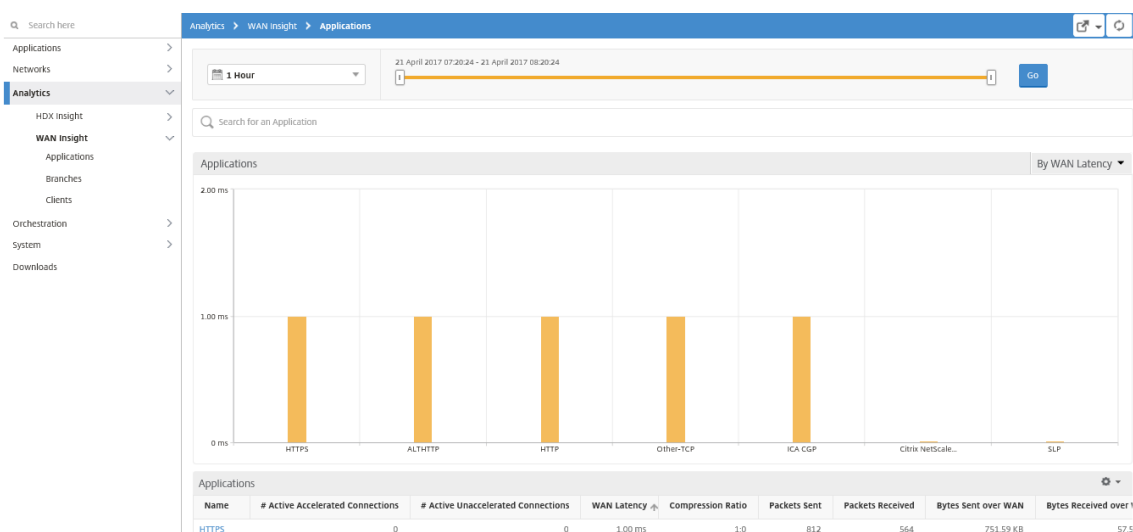
1. Dans un navigateur Web, saisissez l'adresse IP du Citrix ADM (par exemple, <http://192.168.100.1>).
2. Dans les champs **Nom d'utilisateur** et Mot de **pass** , entrez les informations d'identification de l'administrateur.
3. Accédez à **Analytics > WAN Insight**.

#### **Remarque**

L'option WAN Insight n'est visible qu'après avoir ajouté une instance SD-WAN WO à Citrix ADM.

Vous pouvez consulter les rapports suivants :

- **Applications** : affiche les statistiques d'utilisation et de performance de toutes les applications pendant la durée sélectionnée.
- **Branches** : affiche les statistiques d'utilisation et de performances de toutes les appliances de branche d'optimisation WAN.
- **Clients** : affiche les statistiques d'utilisation et de performance de tous les clients accédant aux appliances d'optimisation WAN, dans chaque branche.



Les mesures suivantes sont affichées :

Métrique	Description
Connexions accélérées actives	Nombre de connexions WAN actives accélérées.
Connexions actives non accélérées	Nombre de connexions WAN actives qui ne sont pas accélérées.
Latence WAN	Retard, en millisecondes, ressenti par l'utilisateur lorsqu'il interagit avec une application.
Taux de compression	Rapport de compression des données entre la succursale et le datacenter pour la durée sélectionnée.
Paquets envoyés	Nombre de paquets que l'apppliance d'optimisation WAN a envoyés sur le réseau pendant la durée sélectionnée.
Paquets reçus	Nombre de paquets que l'apppliance d'optimisation WAN a reçus du réseau pendant la durée sélectionnée.
Octets envoyés sur le WAN	Nombre d'octets que l'apppliance d'optimisation de Citrix WAN a envoyés sur le réseau étendu pendant la durée sélectionnée.
Octets reçus sur le WAN	Nombre d'octets que l'apppliance d'optimisation WAN a reçus du WAN pendant la durée sélectionnée.

Métrique	Description
LAN RTO	Nombre de fois où l'apppliance d'optimisation WAN a dépassé le délai de retransmission vers le réseau local pendant la durée sélectionnée.
RTO WAN	Nombre de fois que l'apppliance d'optimisation du WAN a dépassé le délai de retransmission vers le WAN pendant la durée sélectionnée.
Retransmettre des paquets (LAN)	Nombre de paquets que l'apppliance d'optimisation WAN a retransmis au réseau LAN pendant la durée sélectionnée.
Retransmettre des paquets (WAN)	Nombre de paquets que l'apppliance d'optimisation WAN a retransmis au réseau WAN pendant la durée sélectionnée.

---

## Video Insight

February 1, 2024

La fonctionnalité Video Insight fournit une solution simple et évolutive pour surveiller les indicateurs des techniques d'optimisation vidéo utilisées par les appliances Citrix ADC afin d'améliorer l'expérience client et l'efficacité opérationnelle, offrant des avantages tels que :

- Gérez le réseau en cas de congestion aux heures de pointe.
- Améliorez la cohérence de la lecture vidéo et réduisez le blocage vidéo.
- Activez de nouvelles offres de services vidéo (par exemple, des services vidéo en rafale).
- Permettez aux clients de sélectionner la meilleure qualité vidéo durable.
- Offrez une expérience utilisateur cohérente à l'abonné.

Tout en optimisant le trafic vidéo, l'apppliance Citrix ADC utilise un mécanisme spécial pour accélérer dynamiquement le débit vidéo et une technique d'échantillonnage aléatoire pour estimer les économies réalisées grâce à la technique d'optimisation. Pour plus d'informations sur la fonctionnalité d'optimisation vidéo Citrix ADC, consultez [Optimisation vidéo](#). Lorsque vous intégrez l'apppliance Citrix ADC à Citrix Application Delivery Management (ADM), il recueille des informations clés à partir des données vidéo qui transitent par l'apppliance Citrix ADC. Vous pouvez utiliser ces informations pour comparer les performances optimisées et non optimisées du trafic vidéo ABR, déterminer les économies dues à l'optimisation, etc.



### Remarque

Les statistiques des sessions non optimisées fournies dans Citrix ADM correspondent aux sessions sélectionnées pour un échantillonnage aléatoire dans l'apppliance Citrix ADC. Pour plus d'informations sur l'échantillonnage aléatoire, voir [Optimisation vidéo](#).

Video Insight dans Citrix ADM fournit des mesures pour les types de trafic vidéo suivants :

- Vidéos à téléchargement progressif (PD) via HTTP
- Vidéos ABR via HTTP
- Vidéos ABR via HTTPS
- Vidéos YouTube ABR sur QUIC

## Configuration de Video Insight

### Remarque

Video Insight est pris en charge sur les instances Citrix ADC dotées d'une licence Citrix ADC Premium. La licence Citrix ADC Premium est prise en charge pour les plates-formes Citrix ADC Telco (VPX T1000 et VPX-T).

Pour configurer Video Insight sur une instance Citrix ADC, activez d'abord la fonctionnalité AppFlow, configurez un collecteur, une action et une stratégie AppFlow et liez la stratégie globalement. Lorsque vous configurez le collecteur, vous devez spécifier l'adresse IP du serveur Citrix ADM sur lequel vous souhaitez surveiller les rapports.

Pour configurer des informations vidéo sur une instance Citrix ADC, exécutez les commandes suivantes pour configurer un profil et une stratégie AppFlow et lier la stratégie AppFlow globalement.

```
add appflow collector <name> -IPAddress <ipaddress> -port <port_number> -Transport logstream
```

```
set appflow param -videoInsight ENABLED
```

```
add appflow action <name> -collectors <string> -videoAnalytics ENABLED
```

```
add appflow policy <name> <rule> <action>
```

```
bind appflow global <policyName> <priority> [<gotoPriorityExpression>] [-type <type>]
```

```
enable ns mode ulfd
```

```
activer la fonctionnalité appflow
```

## Sample

```

1 add appflow collector col1 -IPAddress 10.106.76.15 -port 5557 -
  Transport logstream
2 set appflow param -videoInsight ENABLED
3 add appflow action act1 -collectors col1 -videoAnalytics ENABLED
4 add appflow policy appol true act1
5 bind appflow global appol 1
6 enable ns mode ulfd
7 enable feature appflow
8 <!--NeedCopy-->

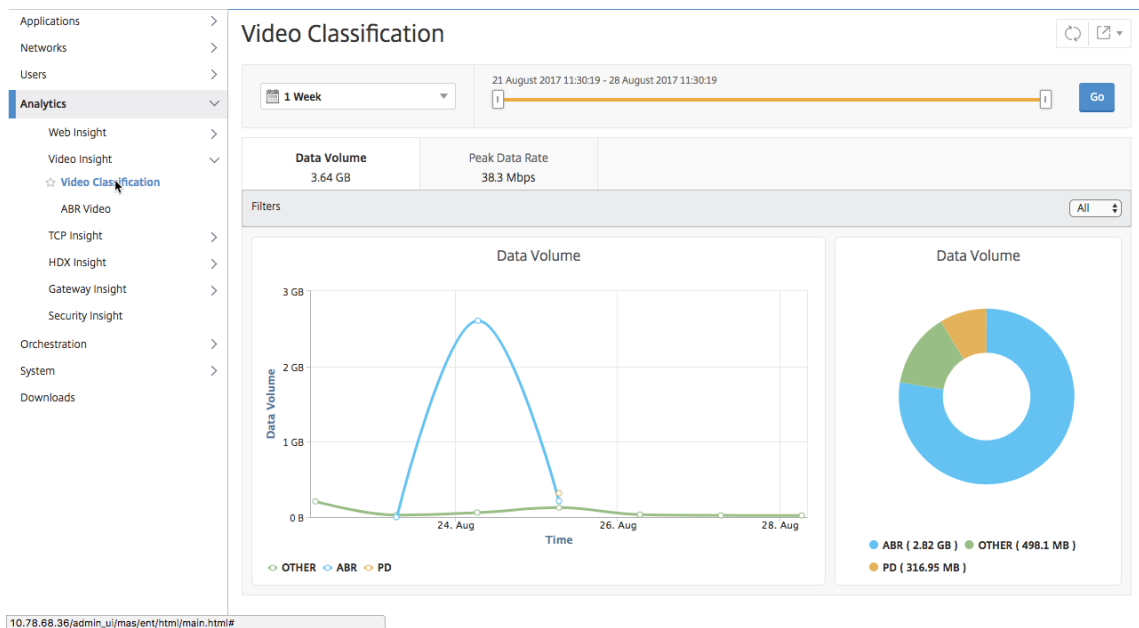
```

## Affichage des mesures Video Insight dans Citrix ADM

Après avoir activé Video Insight dans Citrix ADM, vous pouvez afficher des mesures d'optimisation vidéo telles que la classification vidéo, le volume de données, le débit de pointe et les lectures vidéo ABR. Ces mesures vous aident à analyser votre réseau et à optimiser les vidéos pour améliorer l'expérience des abonnés, l'efficacité opérationnelle et d'autres critères de performance.

### Pour afficher les mesures Video Insight dans Citrix ADM :

1. Dans un navigateur Web, tapez l'adresse IP de l'appliance virtuelle Citrix ADM (par exemple, <http://192.168.100.1>).
2. Dans **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Accédez à **Analytics > Insight vidéo**.



### Remarque

Les valeurs fournies par la légende **OTHER** dans les graphiques représentent les données non ABR et non-DP dans le trafic vidéo en fonction du filtre que vous avez sélectionné :

- **All** —Somme des données non-ABR (HTTP, HTTPS et QUIC) et non-PD (HTTP) dans le trafic vidéo.
- **HTTP** —Somme des données non ABR et non PD dans le trafic vidéo.
- **HTTPS** : somme des données vidéo non ABR dans le trafic vidéo.
- **QUIC** —Somme des données vidéo non ABR dans le trafic vidéo.

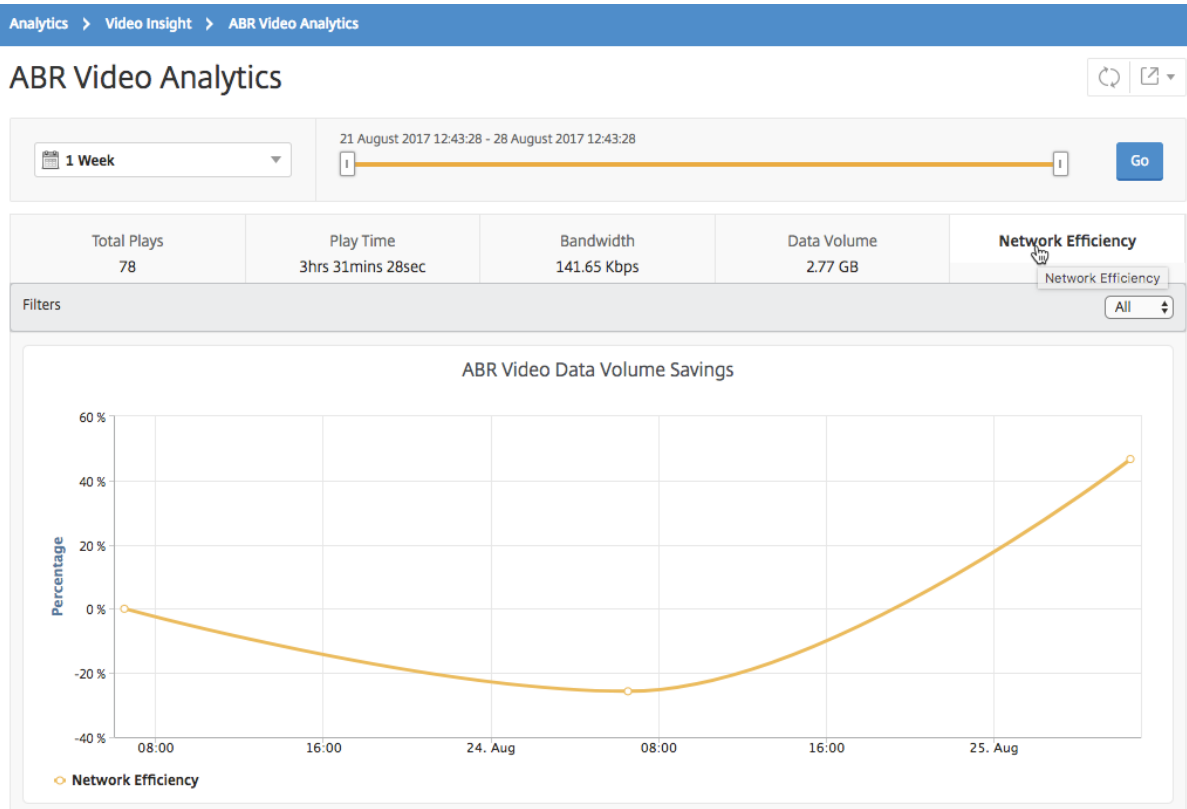
## Afficher l'efficacité du réseau

February 1, 2024

Pour une période donnée, Citrix Application Delivery Management (ADM) fournit un graphique qui montre le rapport entre les sessions vidéo optimisées et non optimisées dans la période. Il affiche également le pourcentage de bande passante économisé grâce à l'optimisation. Le pourcentage de bande passante économisée est calculé à l'aide de la formule suivante :

**Pourcentage de bande passante sauvegardée** = Volume de **données vidéo ABR optimisé moyen** / **Moyenne du volume de données vidéo ABR non optimisé**.

Pour connaître le pourcentage de bande passante économisé grâce à l'optimisation, connectez-vous à Citrix ADM, accédez à **Analytics > Video Insight** , puis cliquez sur **ABR Video**. Ensuite, dans le volet droit, sélectionnez une période dans la liste déroulante. Vous pouvez personnaliser davantage la période en utilisant le curseur temporel. Cliquez sur **Aller** et sélectionnez l'onglet **Efficacité réseau**.



## Comparer le volume de données utilisé par les vidéos ABR optimisées et non optimisées

February 1, 2024

Pour une période donnée, Citrix Application Delivery Management (ADM) affiche le volume de données utilisé par les vidéos ABR optimisées et non optimisées., afin que vous puissiez comparer les deux volumes.

Pour voir le volume de données utilisé par les vidéos ABR, connectez-vous à Citrix ADM, accédez à **Analytics > Video Insight** et cliquez sur **ABR Video** . Ensuite, dans le volet droit, sélectionnez une période dans la liste déroulante. Vous pouvez personnaliser davantage la période en utilisant le curseur temporel. Cliquez sur **Aller** et sélectionnez l'onglet **Volume de données**.

Vous pouvez utiliser la liste déroulante **Filtres** pour sélectionner les vidéos HTTP, HTTPS ou QUIC ABR.

## ABR Video Analytics

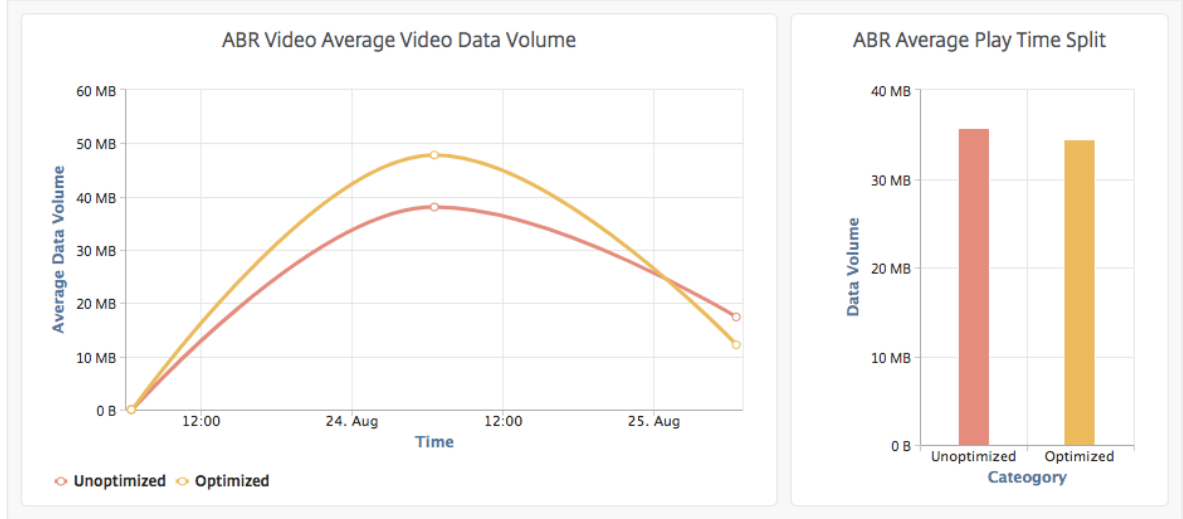


1 Week 21 August 2017 12:43:28 - 28 August 2017 12:43:28

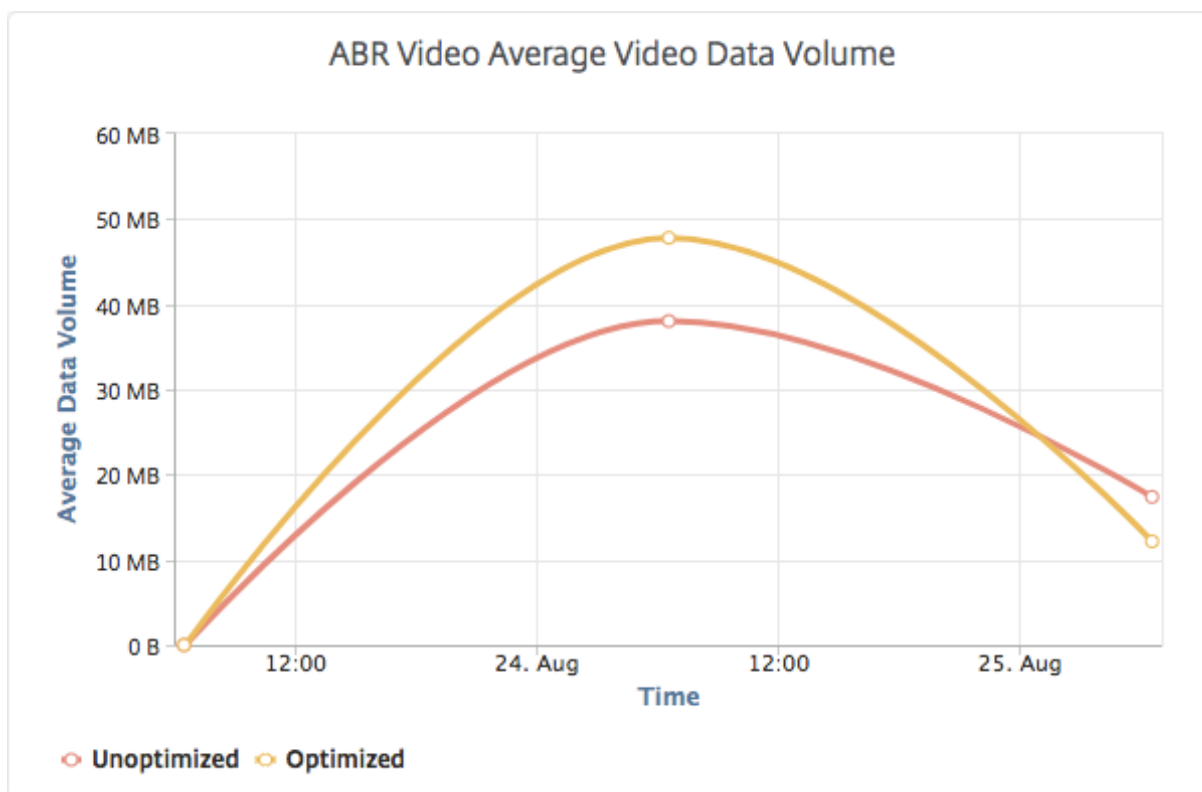
**Go**

Total Plays 78	Play Time 3hrs 31mins 28sec	Bandwidth 141.65 Kbps	<b>Data Volume</b> 2.77 GB	Network Efficiency
-------------------	--------------------------------	--------------------------	-------------------------------	--------------------

Filters All ▾



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

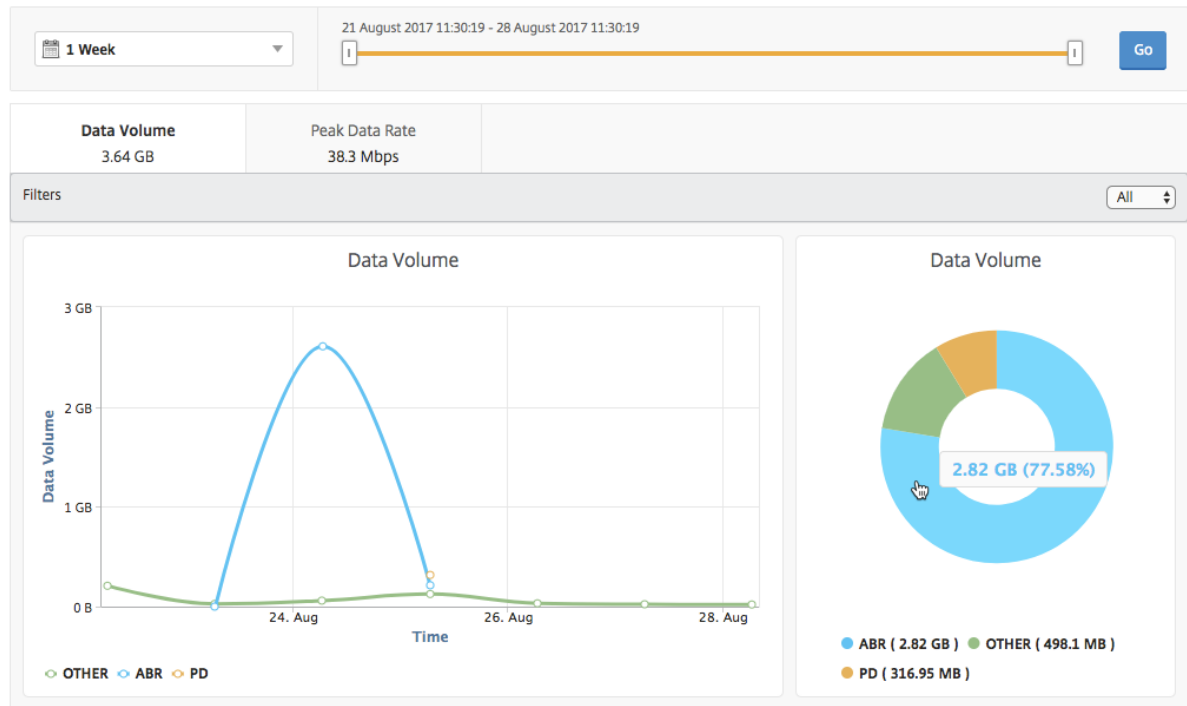
February 1, 2024

L'apppliance Citrix ADC détecte le trafic vidéo crypté ou non crypté sur votre réseau et le type de streaming vidéo (DP ou ABR). Citrix Application Delivery Management (ADM) affiche ces mesures et le volume de données consommé par le trafic vidéo pendant une période définie.

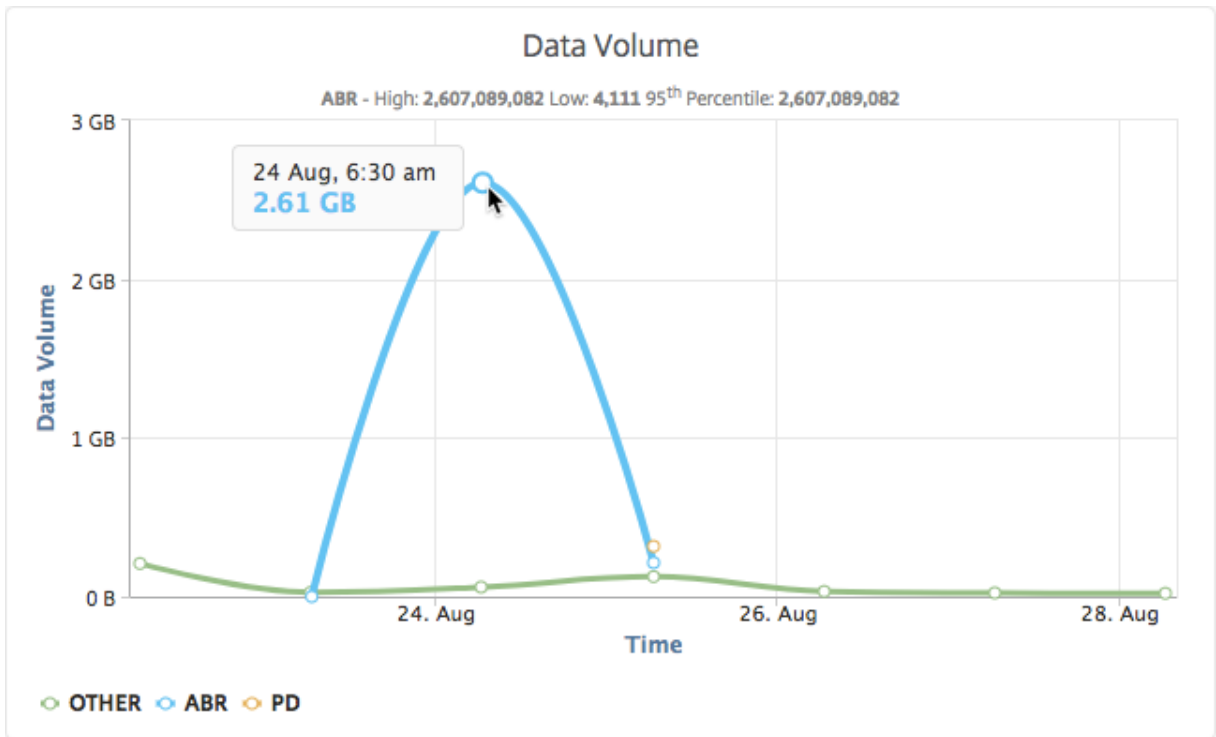
Pour voir les types de vidéos et le volume de données consommé, connectez-vous à Citrix ADM, accédez à **Analytics > Video Insight** et cliquez sur **Classification** des vidéos. Ensuite, dans le volet droit, sélectionnez une période dans la liste déroulante. Vous pouvez personnaliser davantage la période en utilisant le curseur temporel. Cliquez sur **Go**.

Vous pouvez utiliser la liste déroulante **Filtres** pour sélectionner le trafic HTTP, HTTPS ou QUIC.

## Video Classification

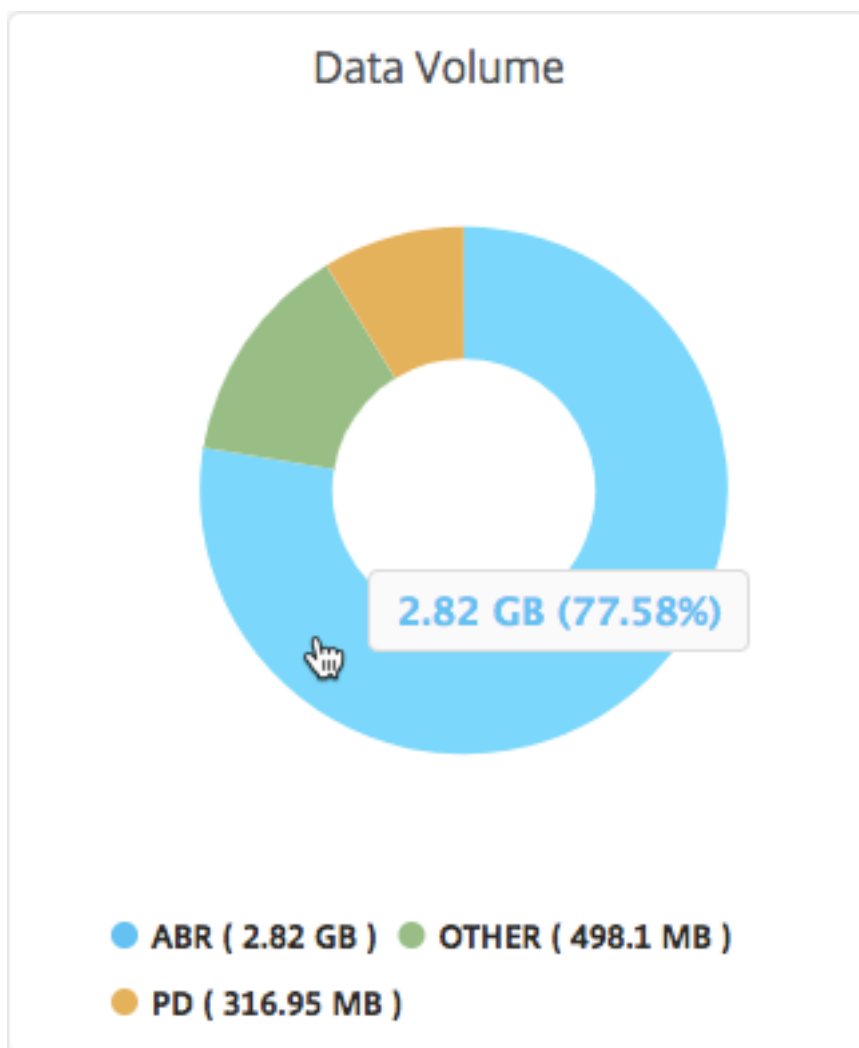


L'onglet **Volume de données** fournit un graphique linéaire et un graphique circulaire indiquant les types de flux de trafic vidéo à partir de votre réseau et le volume de données consommé par votre réseau. Vous pouvez placer le pointeur de la souris sur le graphique linéaire pour afficher les données consommées pendant une période donnée :



En outre, vous pouvez placer le pointeur de la souris sur le graphique à secteurs pour afficher le pourcentage de volume de données consommé par un type particulier de trafic vidéo.





## Comparer le temps de lecture optimisé et non optimisé des vidéos ABR

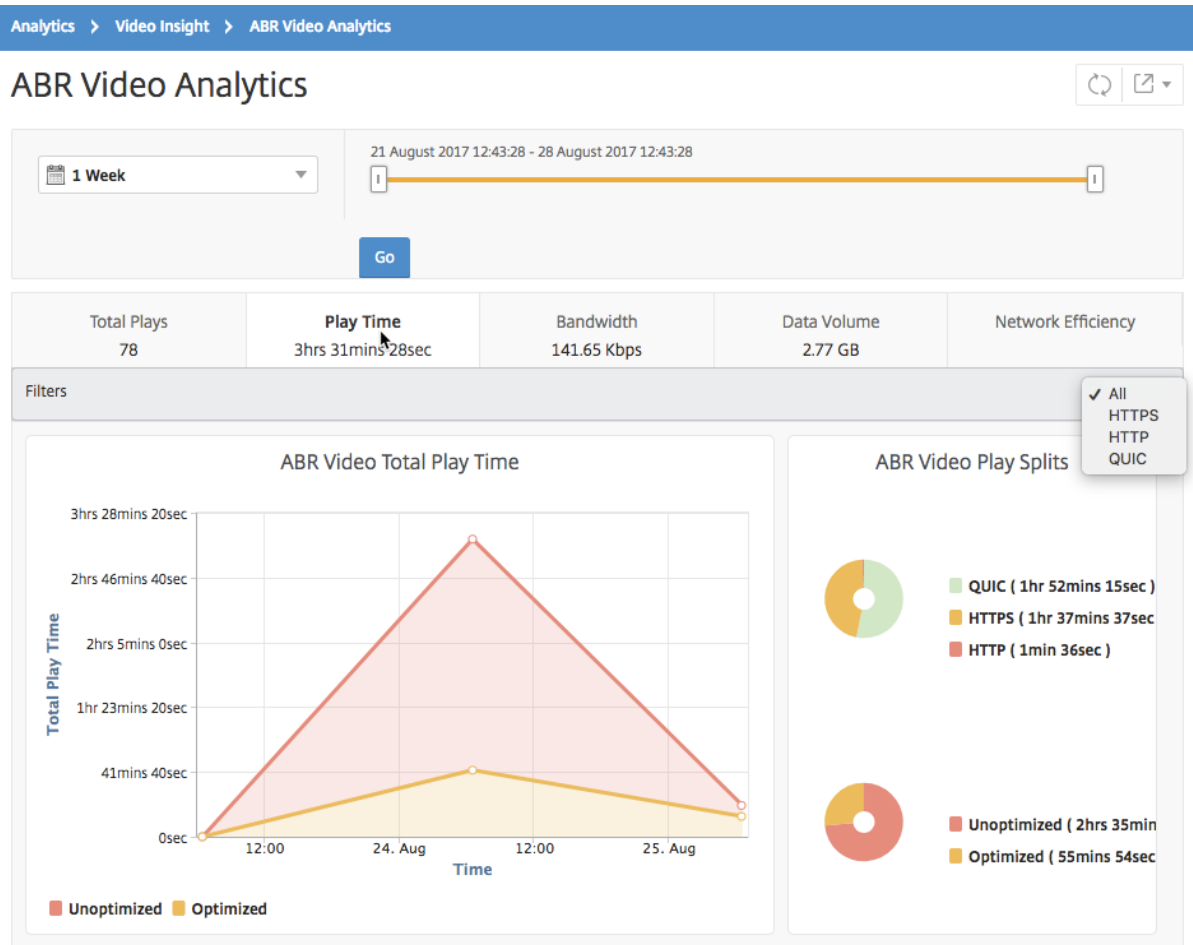
February 1, 2024

Pour une période donnée, Citrix Application Delivery Management (ADM) fournit la durée de lecture des vidéos ABR et vous permet également de comparer la durée de lecture des vidéos ABR optimisées et non optimisées sur votre réseau.

Pour afficher la durée de lecture, connectez-vous à Citrix ADM, accédez à **Analytics > Video Insight** et cliquez sur **ABR Video**. Ensuite, dans le volet droit, sélectionnez une période dans la liste déroulante. Vous pouvez personnaliser davantage la période en utilisant le curseur temporel. Cliquez sur **Aller** et sélectionnez l'onglet **Temps de lecture**.

Vous pouvez utiliser la liste déroulante **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 vidéos ABR optimisées et non optimisées 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

## ABR Video Analytics



21 August 2017 12:43:28 - 28 August 2017 12:43:28

Total Plays 78	<b>Play Time</b> 3hrs 31mins 28sec	Bandwidth 141.65 Kbps	Data Volume 2.77 GB	Network Efficiency
-------------------	---------------------------------------	--------------------------	------------------------	--------------------

Filters All



## Comparer la consommation de bande passante des vidéos ABR optimisées et non optimisées

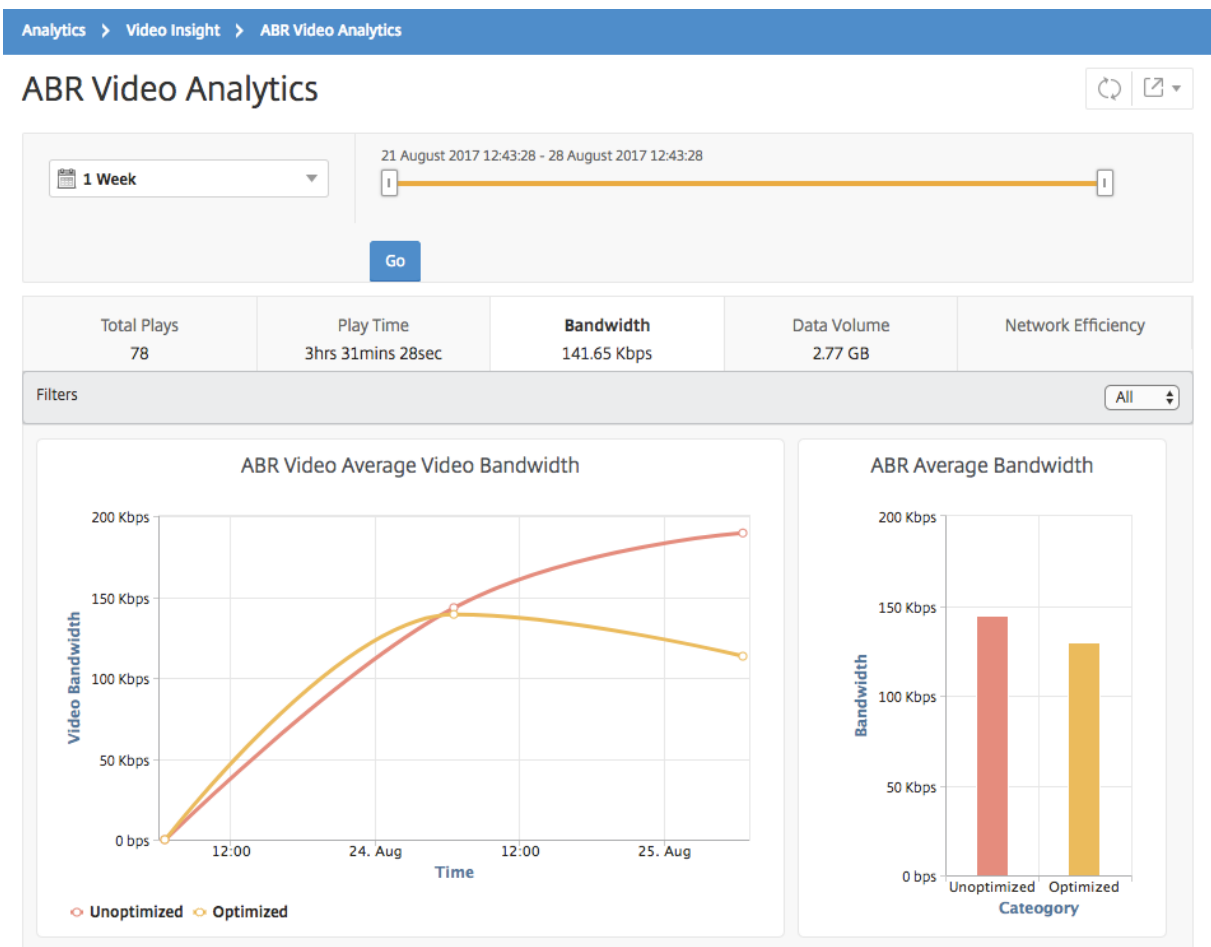
February 1, 2024

Pour une période donnée, Citrix Application Delivery Management (ADM) fournit la bande passante consommée par les vidéos ABR optimisées et non optimisées et vous permet également de comparer la bande passante consommée par les vidéos ABR optimisées et non optimisées de votre réseau en fonction des éléments suivants :

- Temps de jeu
- Volume de données

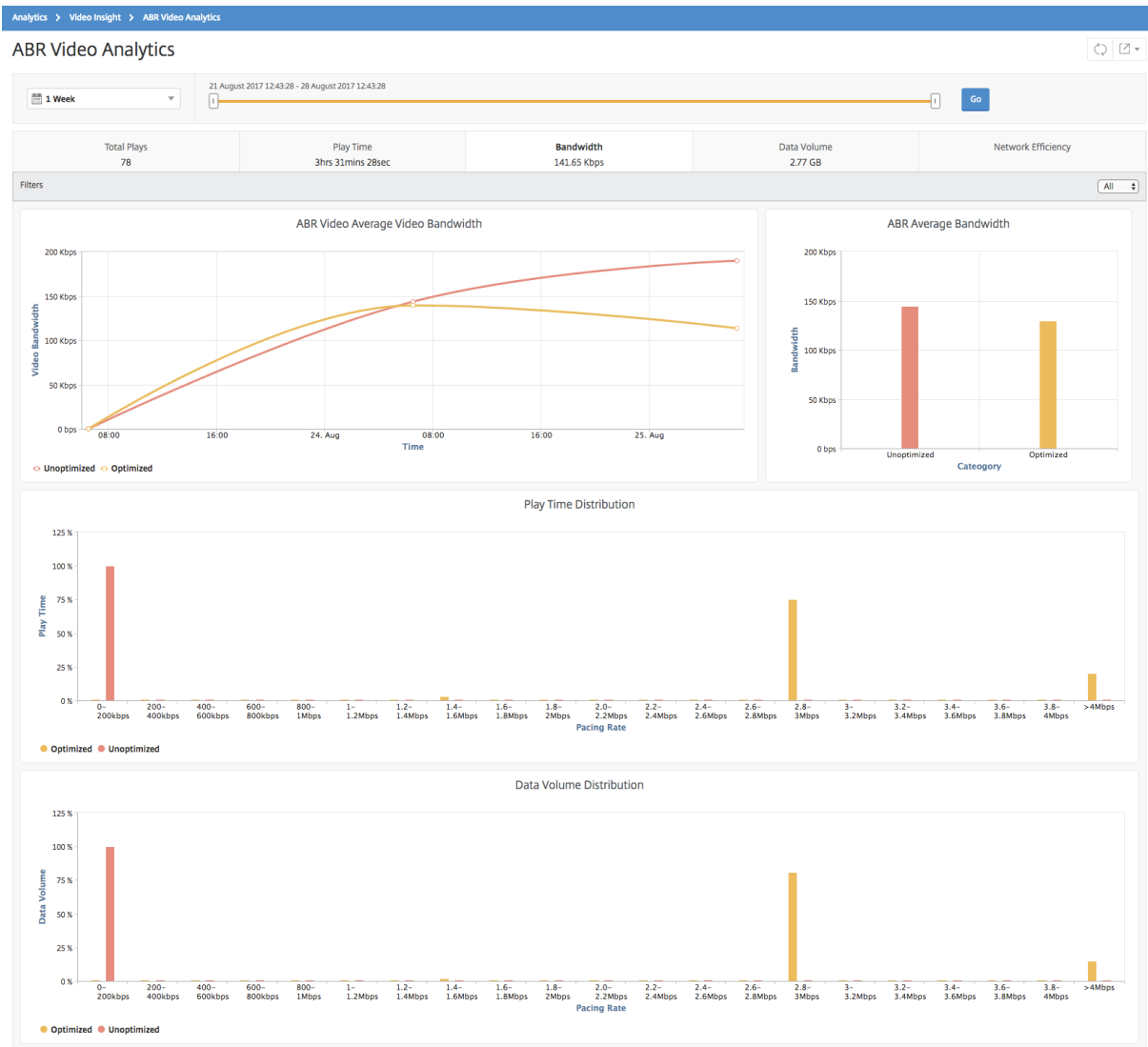
Pour consulter la consommation de bande passante, connectez-vous à Citrix ADM, accédez à **Analytics > Video Insight** et cliquez sur **ABR Video Analytics**. Ensuite, dans le volet droit, sélectionnez une période dans la liste déroulante. Vous pouvez personnaliser davantage la période en utilisant le curseur temporel. Cliquez sur **Aller** et sélectionnez l'onglet **Bande passante**.

Vous pouvez utiliser la liste déroulante **Filtres** pour sélectionner les vidéos HTTP, HTTPS ou QUIC ABR.



Pour la période sélectionnée, l'onglet Bande passante fournit un graphique linéaire et un graphique à secteurs décrivant les éléments suivants :

- Bande passante moyenne consommée par les vidéos ABR optimisées et non optimisées.
- Bande passante consommée en fonction de la répartition du temps de lecture entre les vidéos ABR optimisées et non optimisées.
- Bande passante consommée en fonction du volume de données distribué entre les vidéos ABR optimisées et non optimisées.



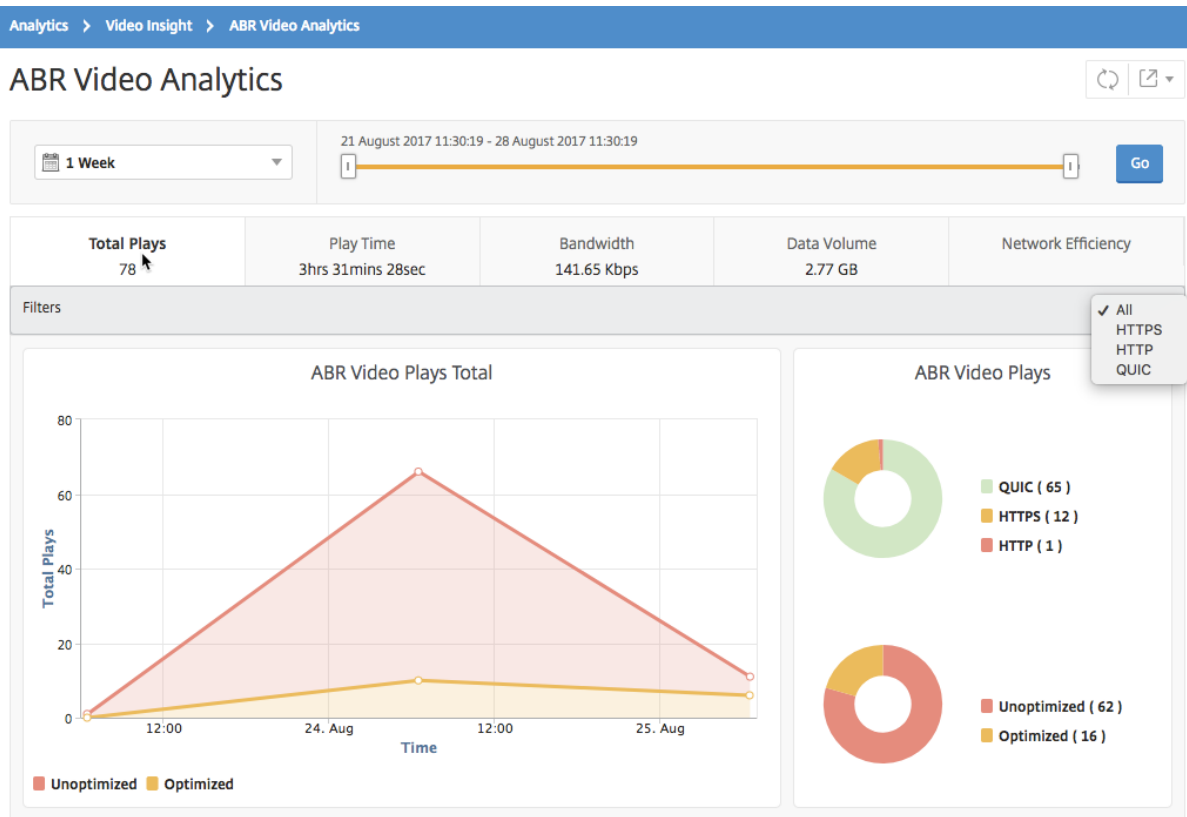
## Comparer le nombre optimisé et non optimisé de lectures de vidéos ABR

February 1, 2024

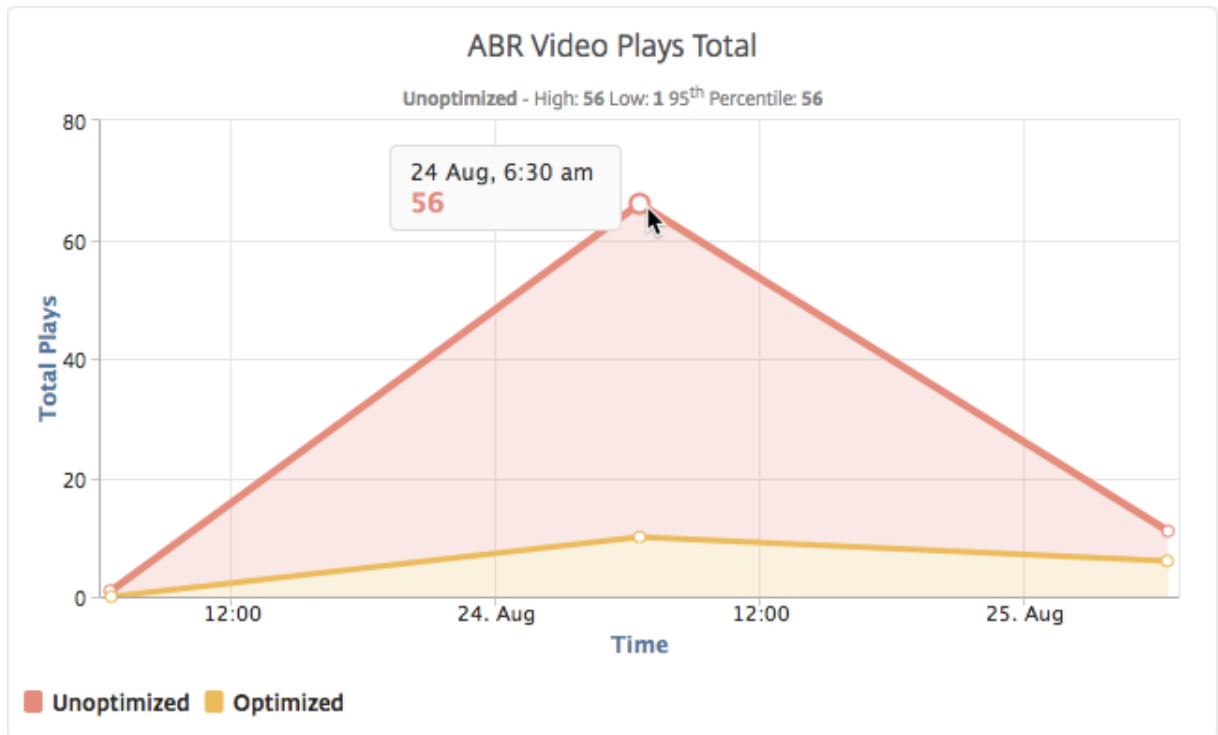
Pour une période donnée, Citrix Application Delivery Management (ADM) affiche le nombre de lectures de vidéos ABR et vous permet de comparer le nombre de lectures optimisées et non optimisées dans votre réseau.

Pour connaître le nombre de lectures, connectez-vous à Citrix ADM, accédez à **Analytics > Video Insight**, puis cliquez sur **ABR Video Analytics**. Ensuite, dans le volet droit, sélectionnez une période dans la liste déroulante. Vous pouvez personnaliser davantage la période en utilisant le curseur temporel. Cliquez sur **Aller** et sélectionnez l'onglet **Nombre de Lecture**.

Vous pouvez utiliser la liste déroulante **Filtres** pour sélectionner les vidéos HTTP, HTTPS ou QUIC ABR.

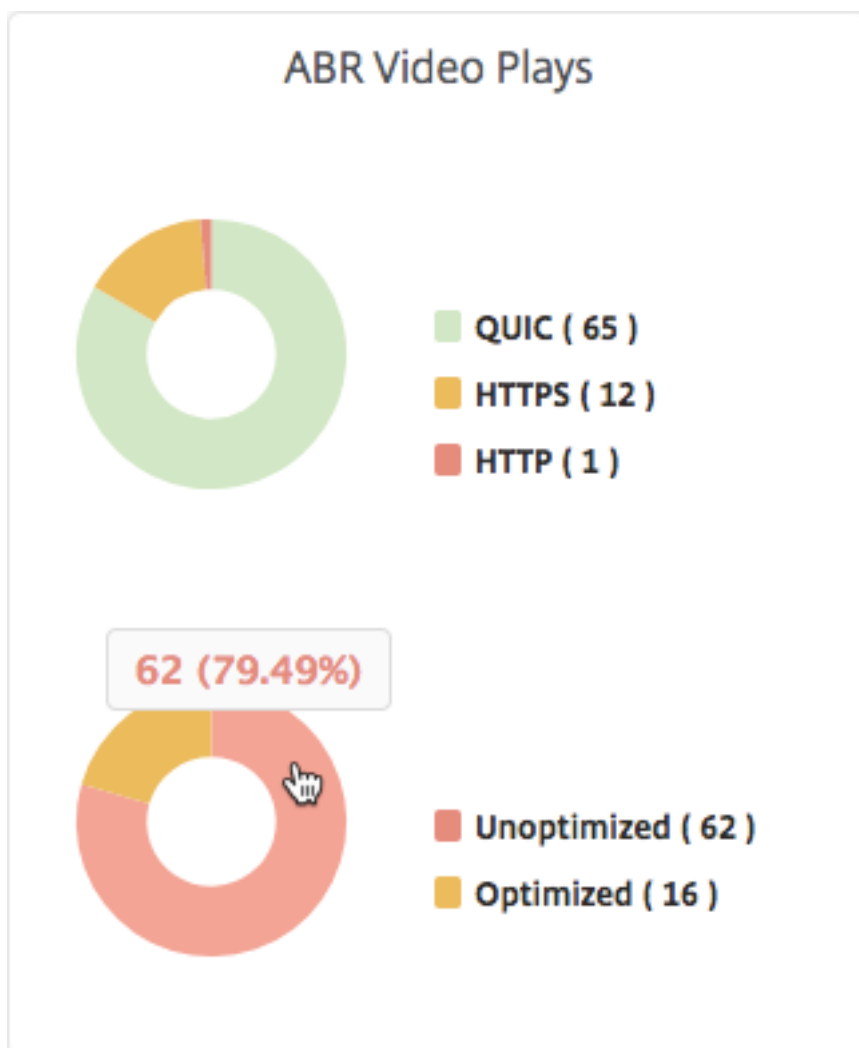


L'onglet **Nombre de lectures** fournit un graphique linéaire et un graphique à secteurs décrivant le nombre de lectures de vidéos ABR de votre réseau et le nombre de lectures optimisées et non optimisées de vidéos ABR de votre réseau pour la période sélectionnée. Vous pouvez placer le pointeur de la souris sur le graphique linéaire pour afficher le nombre de lectures au cours d'une période donnée :



En outre, vous pouvez pointer votre souris sur le graphique à secteurs pour afficher le pourcentage de lectures optimisées et non optimisées et le pourcentage de vidéos ABR chiffrées et non chiffrées pour la période sélectionnée.





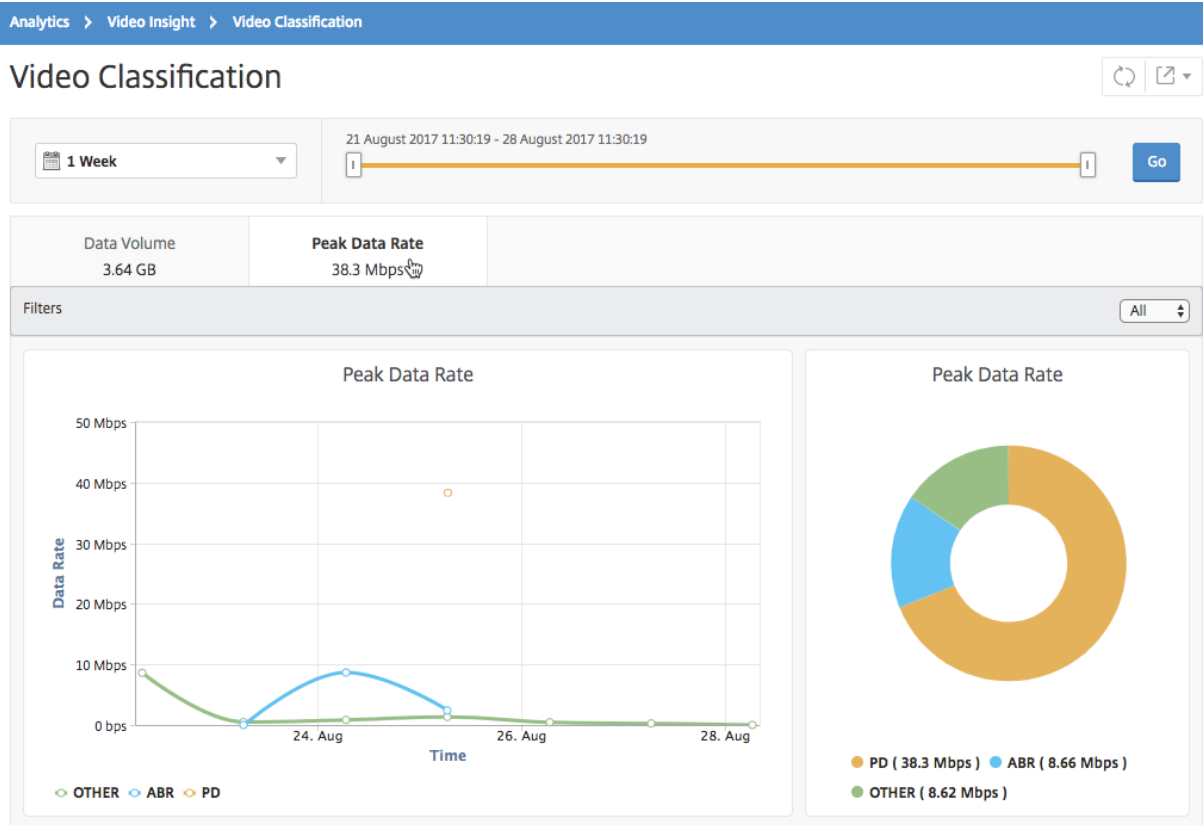
## Afficher le débit de données de pointe pour une période spécifique

February 1, 2024

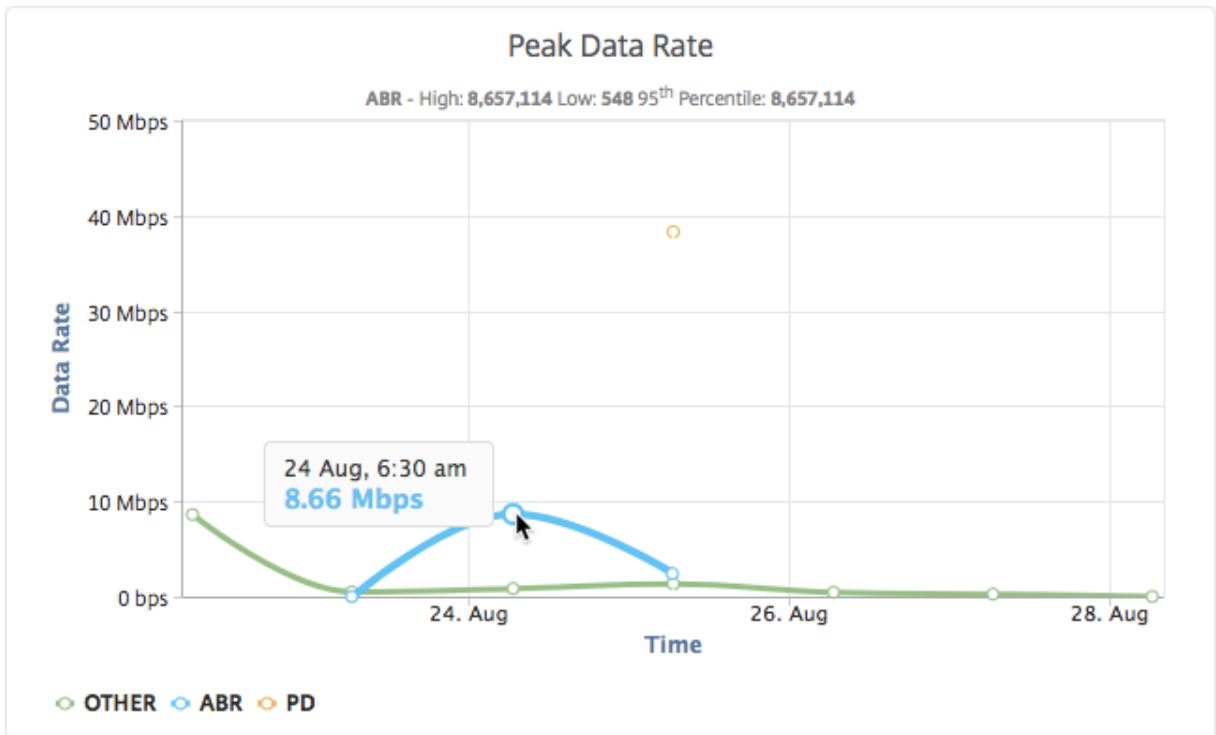
Citrix Application Delivery Management (ADM) vous indique le débit de pointe ou le débit de données du trafic vidéo sur votre réseau.

Pour connaître le débit maximal du trafic vidéo, connectez-vous à Citrix ADM, accédez à **Analytics > Video Insight**, puis cliquez sur **Classification** des vidéos . Ensuite, dans le volet droit, sélectionnez une période dans la liste déroulante. Vous pouvez personnaliser davantage la période en utilisant le curseur temporel. Cliquez sur **Aller** et sélectionnez l'onglet **Taux de données de pointe**.

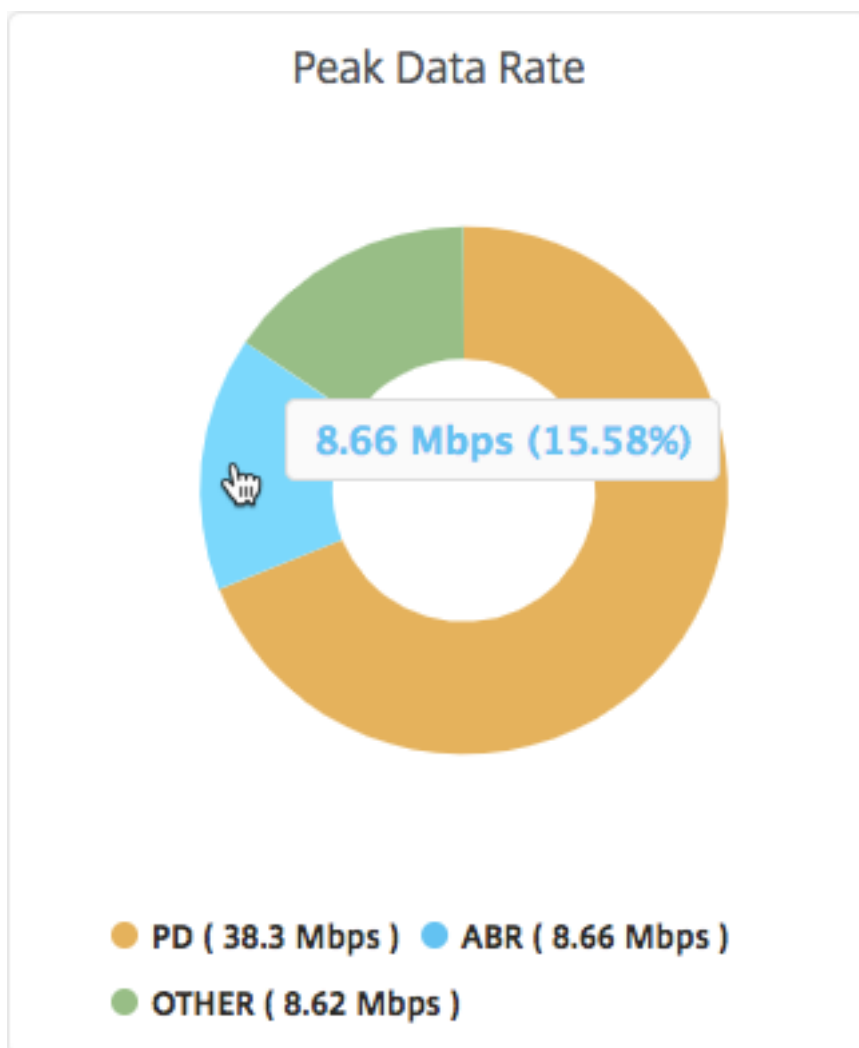
Vous pouvez utiliser la liste déroulante **Filtres** pour sélectionner le trafic HTTP, HTTPS ou QUIC.



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.



## Analyse de Secure Web Gateway

February 1, 2024

Une appliance Citrix Secure Web Gateway (SWG) située à la périphérie du réseau de l'entreprise fait office de proxy Internet. L'appliance peut fonctionner en mode proxy transparent ou en mode proxy explicite et propose des contrôles pour intercepter le trafic Internet, y compris HTTPS. La décision d'intercepter, de contourner ou de bloquer toute demande est prise en fonction des stratégies configurées sur l'appliance. Un utilisateur est authentifié avant de se connecter au réseau de l'entreprise. Toutes les demandes et réponses sont marquées à l'utilisateur et les activités de l'utilisateur sont enregistrées dans l'appliance. Pour plus d'informations, consultez [Citrix Secure Web Gateway](#).

Lorsque vous intégrez Citrix Application Delivery Management (ADM) à une appliance Citrix SWG, l'activité utilisateur enregistrée et les enregistrements suivants sur l'appliance sont exportés vers Citrix

ADM à l'aide de logstream. Citrix ADM rassemble et présente des informations sur les activités des utilisateurs, telles que les sites Web visités et la bande passante dépensée. Il signale également l'utilisation de la bande passante et les menaces détectées, telles que les logiciels malveillants et les sites de phishing. Vous pouvez utiliser ces mesures clés pour surveiller votre réseau et prendre des mesures correctives avec l'appliance Citrix SWG.

#### **Pour intégrer une appliance Citrix SWG à Citrix ADM :**

1. Sur l'appliance Citrix SWG, lors de la configuration de Secure Web Gateway, activez **Analytics** et fournissez les détails de l'instance Citrix ADM que vous souhaitez utiliser pour les analyses.
2. Dans Citrix ADM, ajoutez l'appliance Citrix SWG en tant qu'instance à Citrix ADM. Pour plus d'informations, consultez [Ajouter des instances à Citrix ADM](#).

## **Tableaux de bord**

February 1, 2024

24 mai 2018

Citrix Application Delivery Management (ADM) fournit deux tableaux de bord, le tableau de bord du **trafic sortant et le tableau de bord des utilisateurs**. Ces tableaux de bord affichent plusieurs graphiques qui résument les sites Web ou les applications accessibles depuis le réseau d'entreprise ainsi que les activités effectuées par les utilisateurs de votre réseau.

### **Tableau de bord du trafic sortant**

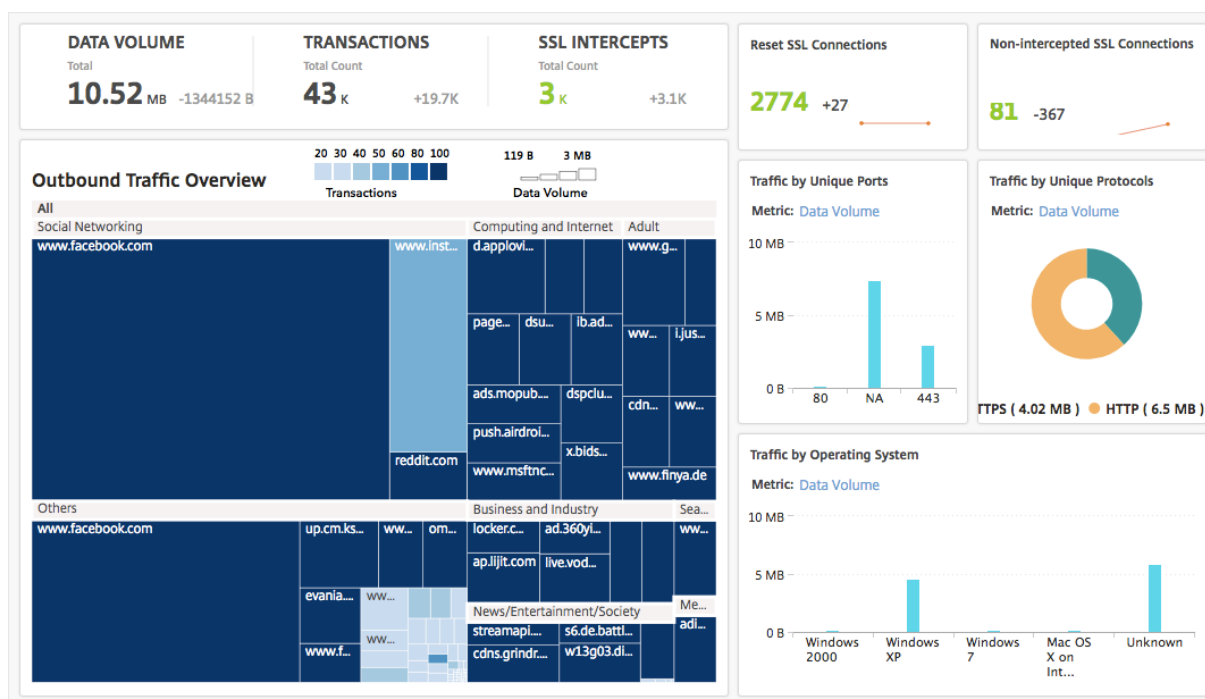
Le tableau de **bord du trafic sortant** fournit un résumé des URL ou des domaines auxquels vous accédez depuis votre réseau. Il fournit une vue globale de toutes les URL ou domaines en fonction du nombre de transactions ou du volume de données consommé par les URL ou les domaines.

Il fournit également des détails tels que les suivants :

1. Quantité de bande passante consommée par les URL ou les domaines auxquels vous accédez depuis votre réseau.
2. Nombre de transactions qui se sont produites lors de l'accès aux URL et aux domaines à partir de votre réseau.
3. Nombre de connexions SSL interceptées par l'appliance Citrix SWG lors des transactions.
4. Nombre de connexions SSL non interceptées par l'appliance Citrix SWG pendant les transactions.

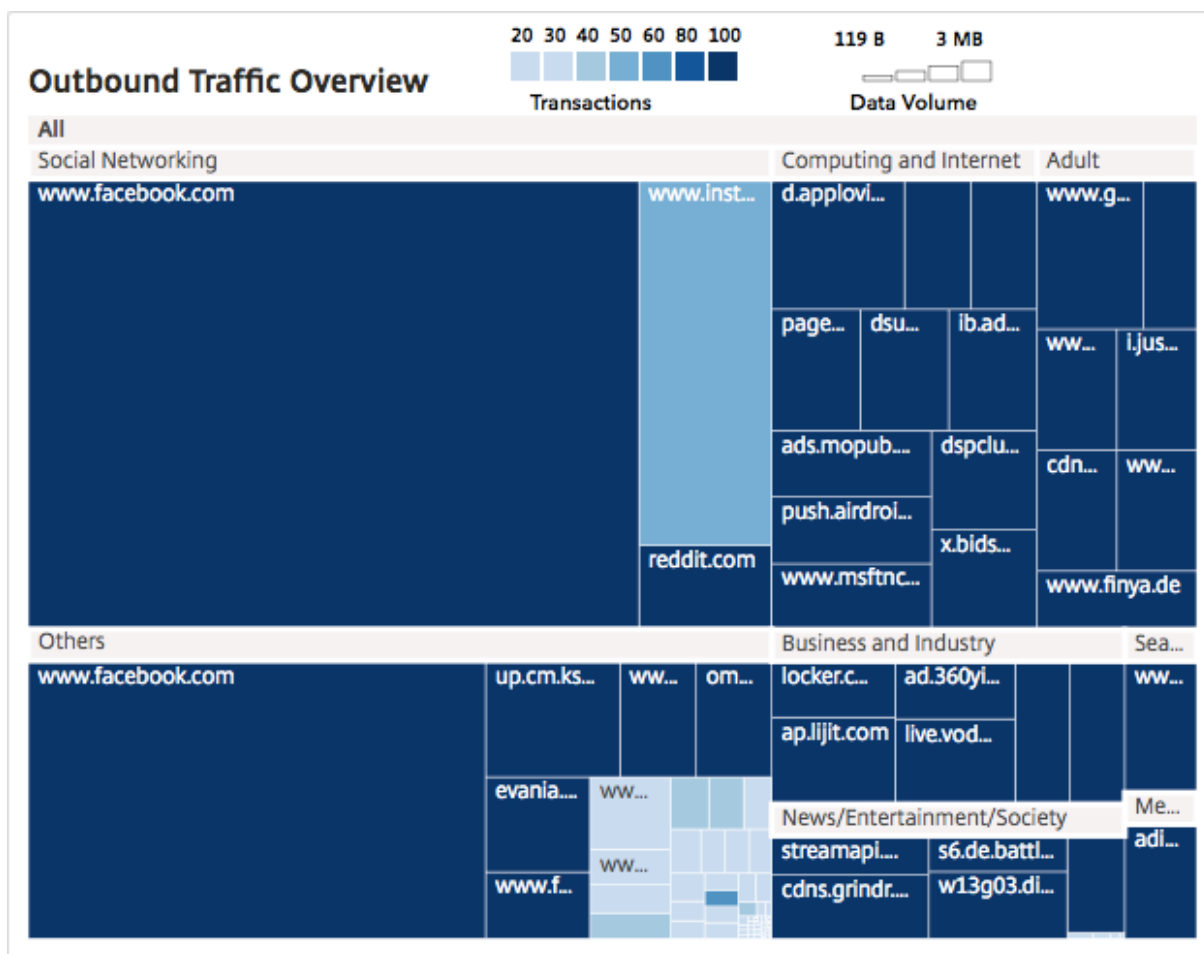
5. Nombre de connexions SSL réinitialisées par l'apppliance Citrix SWG lors des transactions.
6. Quantité de trafic Web transmis, en fonction du port utilisé pour transmettre le trafic, du protocole utilisé par le trafic Web et des systèmes d'exploitation clients utilisés pour transmettre le trafic.

Pour accéder au tableau de bord du trafic sortant, accédez à **Applications > Tableau de bord du trafic sortant**.



### Afficher le trafic sortant du réseau

Le tableau de **bord Trafic sortant** comprend un volet **Aperçu du trafic sortant**. Dans le volet **Vue d'ensemble du trafic sortant**, Citrix ADM regroupe les URL ou domaines accessibles en catégories, telles que Shopping, Actualités, Réseaux sociaux, etc. Le volet **Aperçu du trafic sortant** affiche les URL ou les domaines auxquels vous accédez depuis votre réseau sous forme de nœuds dans les catégories d'URL. Les nœuds sont dimensionnés en fonction du volume de données consommé lors de l'accès à l'URL ou au domaine. La couleur du nœud indique le nombre de transactions qui se sont produites lors de l'accès à l'URL ou au domaine.



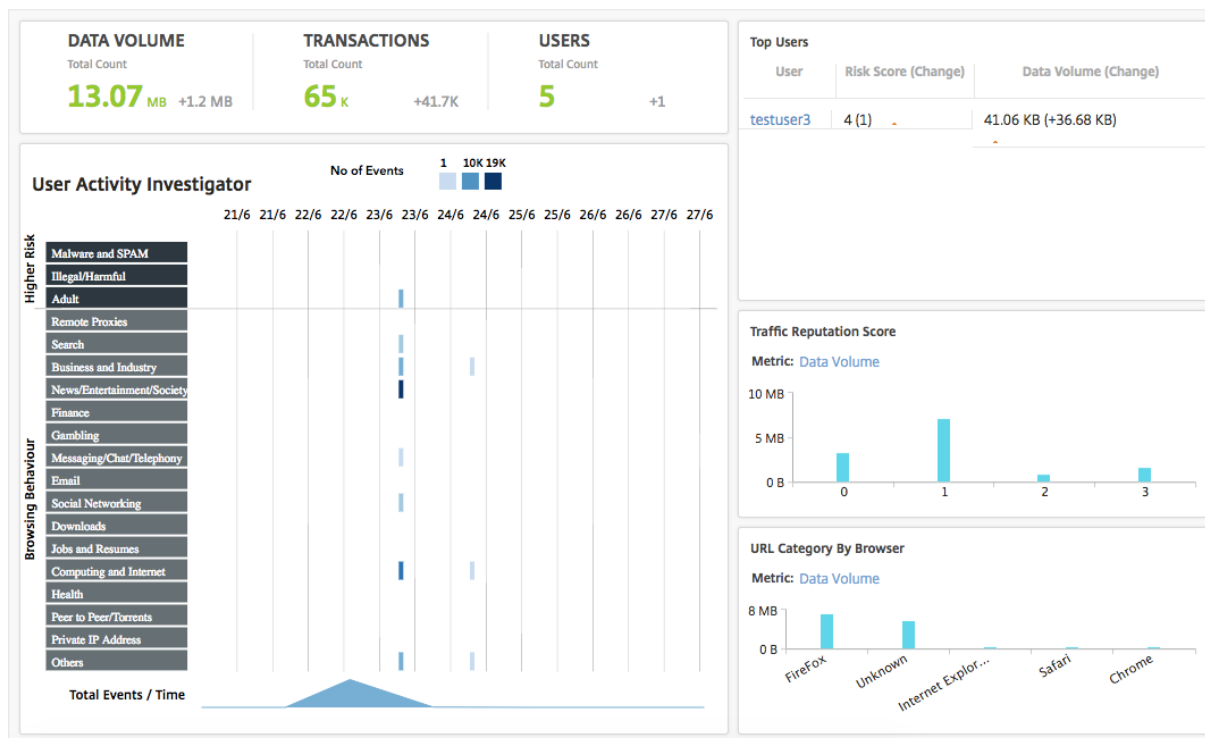
Vous pouvez cliquer sur une catégorie pour filtrer les graphiques afin d’afficher les détails relatifs à la catégorie pour la période spécifiée.

## Tableau de bord utilisateur

Le **tableau de bord des utilisateurs** affiche un récapitulatif des activités effectuées par les utilisateurs dans votre entreprise. Il fournit des indicateurs clés que vous pouvez utiliser pour déterminer les éléments suivants :

1. Comportement de navigation des utilisateurs de votre entreprise.
2. Catégories d’URL auxquelles les utilisateurs de votre entreprise accèdent.
3. Les cinq principaux utilisateurs, en fonction de leurs scores de risque et de la bande passante qu’ils consomment. Pour plus d’informations sur le score de risque, voir Score de risque.
4. Navigateurs utilisés pour accéder aux URL ou aux domaines.
5. Montant du trafic Web généré par les utilisateurs, en fonction du score de réputation de trafic.

Pour accéder au Tableau de **bord utilisateur**, accédez à **Utilisateurs > Tableau de bord**.



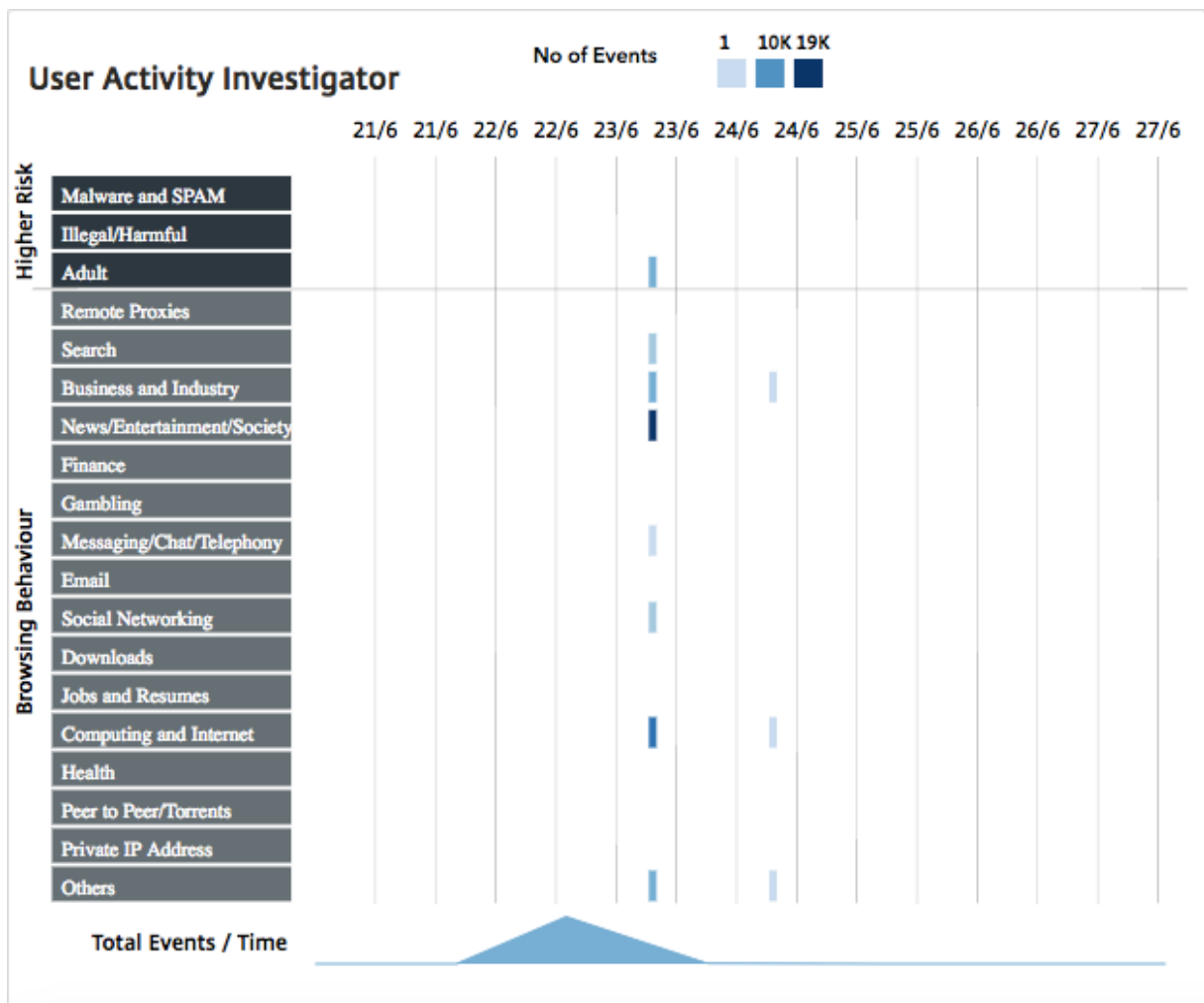
Vous pouvez cliquer sur un utilisateur dans le volet Principaux **utilisateurs** pour filtrer les graphiques afin d’afficher les détails de l’activité Web réalisée par l’utilisateur au cours de la période spécifiée.

### Investigateur des activités des utilisateurs

Le **tableau de bord del'utilisateur comprend un volet de recherche d'activité utilisateur** qui affiche diverses activités Web effectuées par les utilisateurs. Il affiche les catégories d’URL auxquelles les utilisateurs accèdent pendant la période sélectionnée, ainsi que les différents événements déclenchés par catégorie d’URL. Vous pouvez cliquer sur les événements pour obtenir les détails du niveau de transaction.

L’**enquêteur d'activité utilisateur** affiche des informations clés telles que le comportement de navigation de l’utilisateur, les activités à haut risque de l’utilisateur et les événements déclenchés, par catégorie d’URL. Les événements sont présentés sous forme de légendes rectangulaires sur le graphique. Chacune des légendes est agrégée à intervalles d’une minute si la durée sélectionnée est d’une heure, et à intervalles d’une heure si la durée sélectionnée est d’un jour.





Ces légendes sont agrégées et sont codées par couleur en fonction du nombre d'événements qui se sont produits. Vous pouvez placer le pointeur de la souris sur une légende pour afficher des détails tels que l'heure et le nombre d'événements agrégés pour la légende sélectionnée. Vous pouvez personnaliser la période du graphique en sélectionnant une heure dans la liste déroulante des périodes.

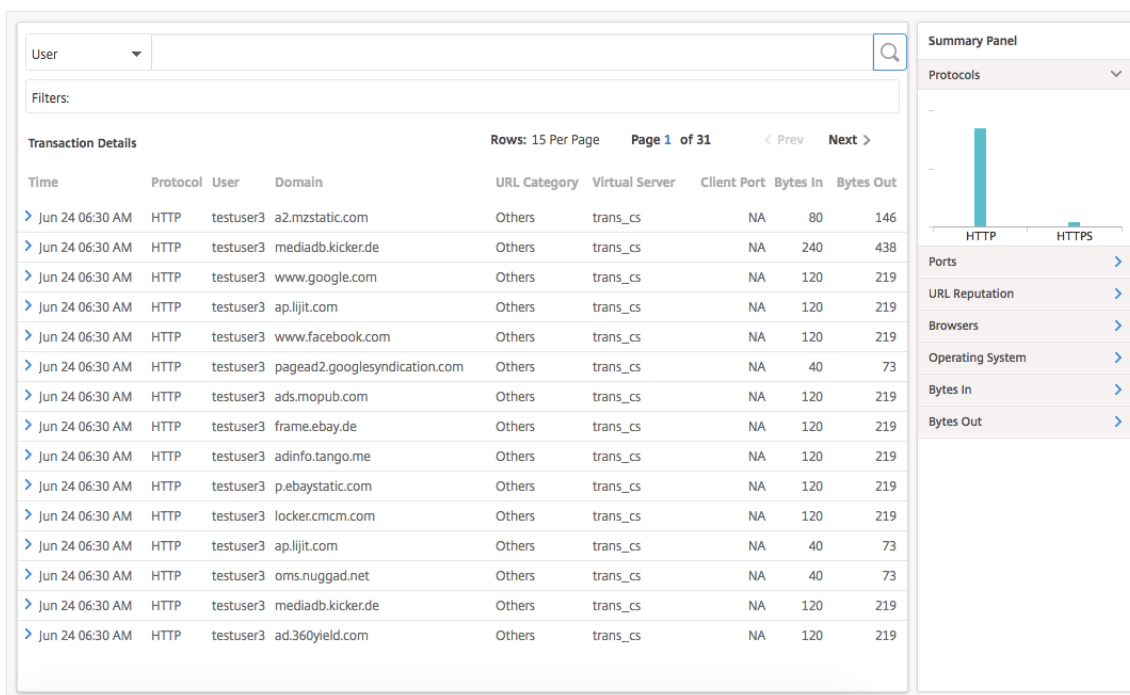
Vous pouvez cliquer sur les événements pour obtenir plus de détails sur les transactions.

### Transactions des utilisateurs

La page Transactions utilisateur affiche les détails des transactions utilisateur dans votre réseau. Il fournit des informations au niveau des transactions, telles que :

1. Heure à laquelle la transaction a eu lieu
2. Protocole utilisé pour la transaction
3. Nom d'utilisateur
4. Domaine auquel l'utilisateur a accédé

5. Catégorie d'URL
6. Serveur proxy utilisé pour intercepter la transaction
7. Détails du port client
8. Octets entrants
9. Octets sortants



**Panneau récapitulatif** Le **panneau de synthèse** affiche toutes les mesures des transactions qui sont visibles dans le volet **Détails de la transaction** . Ce panneau vous permet de trier et d'afficher les transactions dans le volet **Détails des transactions** en sélectionnant ou en désélectionnant les indicateurs. Le **panneau de synthèse** affiche les mesures suivantes :

Mesures	Description
Protocoles	Protocoles utilisés dans les transactions
Ports	Ports utilisés pour les transactions
Réputation d'URL	Score de réputation d'URL
Navigateurs	Navigateurs utilisés pour les transactions
Système d'exploitation	Système d'exploitation utilisé pour les transactions
Octets entrants	Quantité de données reçues via l'appliance Citrix SWG.

---

Mesures	Description
Octets sortants	Quantité de données envoyées via l'apppliance Citrix SWG.

---

### Score de risque

Le score de risque est un système de notation utilisé dans Citrix ADM pour déterminer les risques associés aux utilisateurs de votre entreprise. Citrix ADM attribue un score de risque en fonction du score de réputation d'URL attribué par l'apppliance Citrix SWG aux URL consultées par les utilisateurs de votre réseau. Pour plus d'informations sur le score de réputation d'URL, consultez [Score de réputation d'URL](#). Le tableau suivant décrit les scores de risque attribués par Citrix ADM.

---

Cote de risque	Description
1	L'activité Web de l'utilisateur n'est pas perçue comme une menace ou n'est pas anormale.
2	L'activité Web de l'utilisateur ne présente aucune menace perçue ou n'est pas anormale, mais l'utilisateur accède à des « sites inconnus », pour lesquels aucun score de réputation d'URL n'est attribué.
3	Aucune menace n'est détectée dans l'activité Web de l'utilisateur, mais celui-ci a tenté d'accéder à des sites potentiellement vulnérables ou affiliés à des sites potentiellement vulnérables.
4	Utilisateur potentiellement compromis.
5	L'activité Web de l'utilisateur est anormale et l'utilisateur a accédé à des sites malveillants connus.

---

### Cas d'utilisation

February 1, 2024

## Surveillance des interceptions SSL

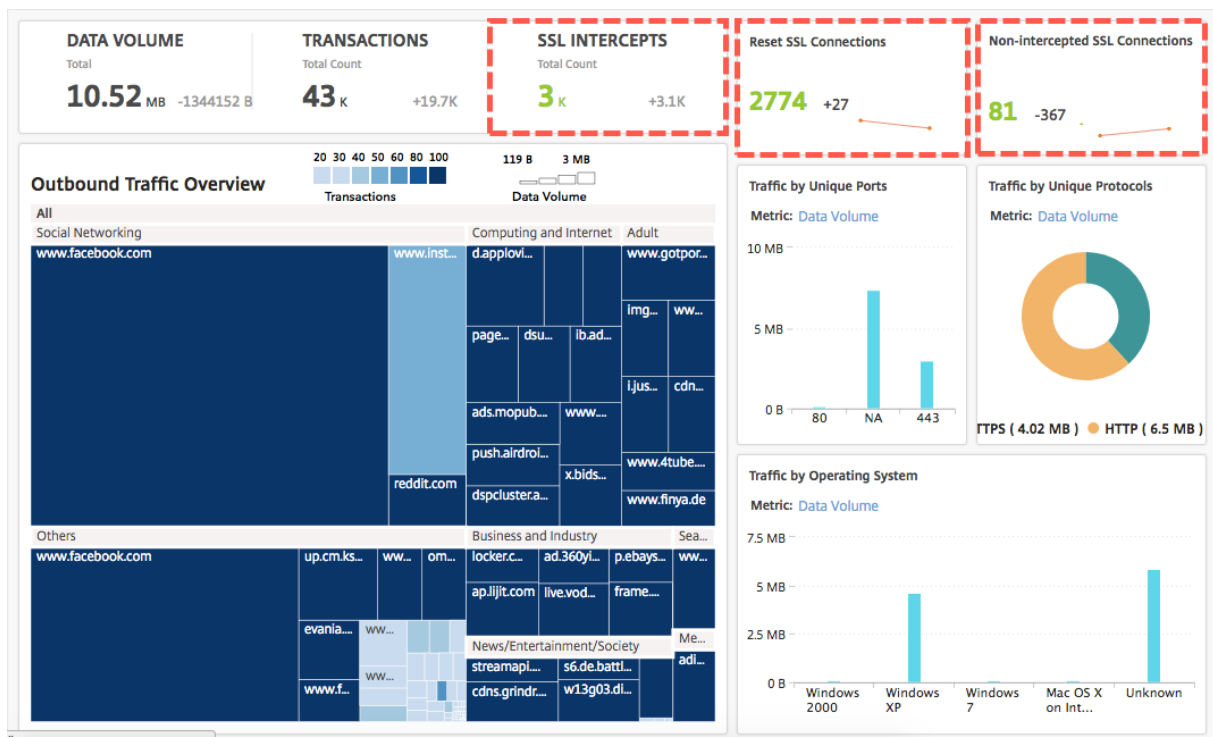
Une appliance Citrix SWG vous permet d'inspecter votre trafic sortant chiffré. Vous pouvez intercepter, contourner ou bloquer toutes les requêtes HTTPS sur la base des stratégies configurées sur l'appliance. Citrix Application Delivery Management (ADM) fournit les détails suivants sur les connexions SSL dans le tableau de **bord du trafic sortant** pour une période sélectionnée :

- Nombre de connexions SSL interceptées, non interceptées et réinitialisées par l'appliance Citrix SWG
- Détails de la transaction des connexions SSL

À l'aide de ces informations, vous pouvez affiner les stratégies de votre appliance Citrix SWG afin d'inspecter efficacement le trafic sortant chiffré. Pour plus d'informations, consultez [Citrix Secure Web Gateway](#).

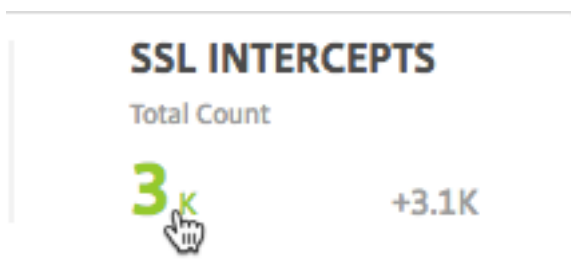
### Pour afficher le nombre de connexions SSL interceptées, non interceptées et réinitialisées :

Accédez à **Applications > Tableau de bord du trafic sortant**. Le tableau de bord du trafic hors-bord affiche le nombre de connexions SSL interceptées, non interceptées et réinitialisées.



### Pour afficher les détails de transaction des connexions SSL interceptées :

1. Accédez à **Applications > Tableau de bord du trafic sortant**.
2. Dans le tableau de **bord du trafic hors-bord**, cliquez sur le nombre total dans la section **INTERCEPTS SSL**.



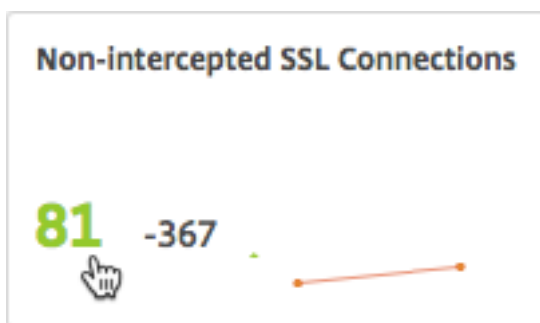
Les détails de transaction des connexions SSL interceptées au cours de la période sélectionnée sont affichés sur la page **Détails de la transaction**.

Transaction Details							Rows: 15 Per Page		Page 1 of 2		< Prev Next >	
Time	Protocol	User	Domain	URL Category	Virtual Server	Client Port	Bytes In	Bytes Out				
> Jun 24 06:30 AM	HTTPS	testuser3	www.facebook.com	Others	starcs	NA	338	0				
> Jun 23 06:31 AM	HTTPS	testuser3	a2.mzstatic.com	Social Networking	starcs	NA	337	0				
> Jun 23 06:31 AM	HTTPS	testuser3	www.facebook.com	Others	starcs	NA	338	0				
> Jun 23 06:31 AM	HTTPS	testuser3	m.momondo.pt	News/Entertainment/Society	starcs	NA	668	0				
> Jun 23 06:31 AM	HTTPS	testuser3	adinfo.tango.me	Messaging/Chat/Telephony	starcs	NA	674	0				
> Jun 23 06:31 AM	HTTPS	testuser3	locker.cmc.com	Business and Industry	starcs	NA	674	0				
> Jun 23 06:31 AM	HTTPS	testuser3	www.instagram.com	Others	starcs	443	2448	30032				
> Jun 23 06:31 AM	HTTPS	testuser3	s6.de.battleknight.gameforge.com	News/Entertainment/Society	starcs	NA	708	0				
> Jun 23 06:31 AM	HTTPS	testuser3	www.facebook.com	Social Networking	starcs	80	1671	0				
> Jun 23 06:31 AM	HTTPS	testuser3	www.facebook.com	Others	starcs	443	2228	0				
> Jun 23 06:31 AM	HTTPS	testuser3	www.facebook.com	Social Networking	starcs	443	34400	1775373				
> Jun 23 06:31 AM	HTTPS	testuser3	www.instagram.com	Social Networking	starcs	NA	12280	150313				
> Jun 23 06:31 AM	HTTPS	testuser3	www.facebook.com	Social Networking	starcs	NA	6127	0				
> Jun 23 06:31 AM	HTTPS	testuser3	www.instagram.com	Social Networking	starcs	443	33497	405990				
> Jun 23 06:31 AM	HTTPS	testuser3	www.instagram.com:443	Others	starcs	443	1560	3081				

Vous pouvez également filtrer les détails des transactions par utilisateur et par catégorie d'URL.

**Pour consulter les détails des transactions relatives aux connexions SSL sur lesquelles le trafic n'a pas été intercepté, procédez comme suit :**

1. Accédez à **Applications > Tableau de bord du trafic sortant**.
2. Dans le tableau de **bord du trafic hors-bord**, cliquez sur le nombre total dans la section **Connexions SSL non interceptées**.



Les détails de transaction des connexions SSL sur lesquelles le trafic n’a pas été intercepté pendant la période sélectionnée apparaissent dans la page **Détails de la transaction**.

User

▼

🔍

Filters: Not Intercept X
Remove all

Transaction Details

Rows: 15 Per Page

Page 1 of 2

< Prev
Next >

Time	User	Domain	SSL Executed Action	SSL Policy Action	Reset	Not-Intercepted
Jun 24 06:30 AM	testuser3	p.ebaystatic.com	2	2	0	1
Jun 24 06:30 AM	testuser3	frame.ebay.de	2	2	0	1
Jun 24 06:30 AM	testuser3	www.google.com	2	2	0	1
Jun 24 06:30 AM	testuser3	ap.lijit.com	2	2	0	1
Jun 23 06:31 AM	testuser3	adyoulike.omnitags.com	2	2	0	1
Jun 23 06:31 AM	administrator	www.facebook.com	2	2	0	8
Jun 23 06:31 AM	testuser3	www.immobilienscout24.de	2	2	0	1
Jun 23 06:31 AM	testuser3	p.ebaystatic.com	2	2	0	2
Jun 23 06:31 AM	testuser3	pcache-pv-eu1.badooocdn.com	2	2	0	1
Jun 23 06:31 AM	testuser3	pagead2.google syndication.com	2	2	0	1
Jun 23 06:31 AM	testuser3	streamapi.majorleaguegaming.com	2	2	0	2
Jun 23 06:31 AM	testuser3	live.vodafone.de	2	2	0	2
Jun 23 06:31 AM	testuser3	www.fnnya.de	2	2	0	2
Jun 23 06:31 AM	testuser3	www.google.co.in	2	2	0	1
Jun 23 06:31 AM	testuser3	reiseauskunft.bahn.de	2	2	0	2

Summary Panel

SSL Executed Action ▼

2

SSL Policy Action ▼

2

Vous pouvez également filtrer les détails des transactions par utilisateur et par catégorie d’URL.

**Pour afficher les détails des transactions des connexions SSL qui sont réinitialisées, procédez comme suit :**

1. Accédez à **Applications > Tableau de bord du trafic sortant**.
2. Dans le tableau de **bord du trafic hors-bord**, cliquez sur le nombre total dans la section **Réinitialiser les connexions SSL** .



Les détails de transaction des connexions SSL sur lesquelles le trafic n’a pas été intercepté pendant la période sélectionnée apparaissent sur la page **Détails de la transaction**.

The image displays a "Transaction Details" table and a "Summary Panel". The table lists transactions with columns for Time, User, Domain, SSL Executed Action, SSL Policy Action, Reset, and Not-intercepted. The Summary Panel shows two bar charts: "SSL Executed Action" with a value of 3, and "SSL Policy Action" with values for 0 and 1.

Time	User	Domain	SSL Executed Action	SSL Policy Action	Reset	Not-intercepted
Jun 24 06:30 AM	testuser3	www.facebook.com	3	1	1	0
Jun 23 06:31 AM	testuser3	s6.de.battleknight.gameforge.com	3	0	2	0
Jun 23 06:31 AM	administrator	www.facebook.com	3	1	2426	0
Jun 23 06:31 AM	testuser3	m.momondo.pt	3	0	2	0
Jun 23 06:31 AM	testuser3	adinfo.tango.me	3	0	2	0
Jun 23 06:31 AM	testuser3	locker.cmc.com	3	0	2	0
Jun 23 06:31 AM	testuser3	a2.mzstatic.com	3	0	1	0
Jun 23 06:31 AM	testuser3	www.facebook.com	3	1	338	0

Vous pouvez également filtrer les détails des transactions en fonction de l'utilisateur et de la catégorie d'URL.

### Inspection des terminaux

Les stratégies que vous avez configurées sur une appliance Citrix SWG spécifient la manière dont l'appliance enregistre toutes les activités des utilisateurs effectuées dans votre entreprise. Citrix ADM fournit des mesures clés que vous pouvez utiliser pour déterminer :

1. Comportement de navigation des utilisateurs de votre entreprise.
2. Catégories d'URL auxquelles les utilisateurs de votre entreprise accèdent.

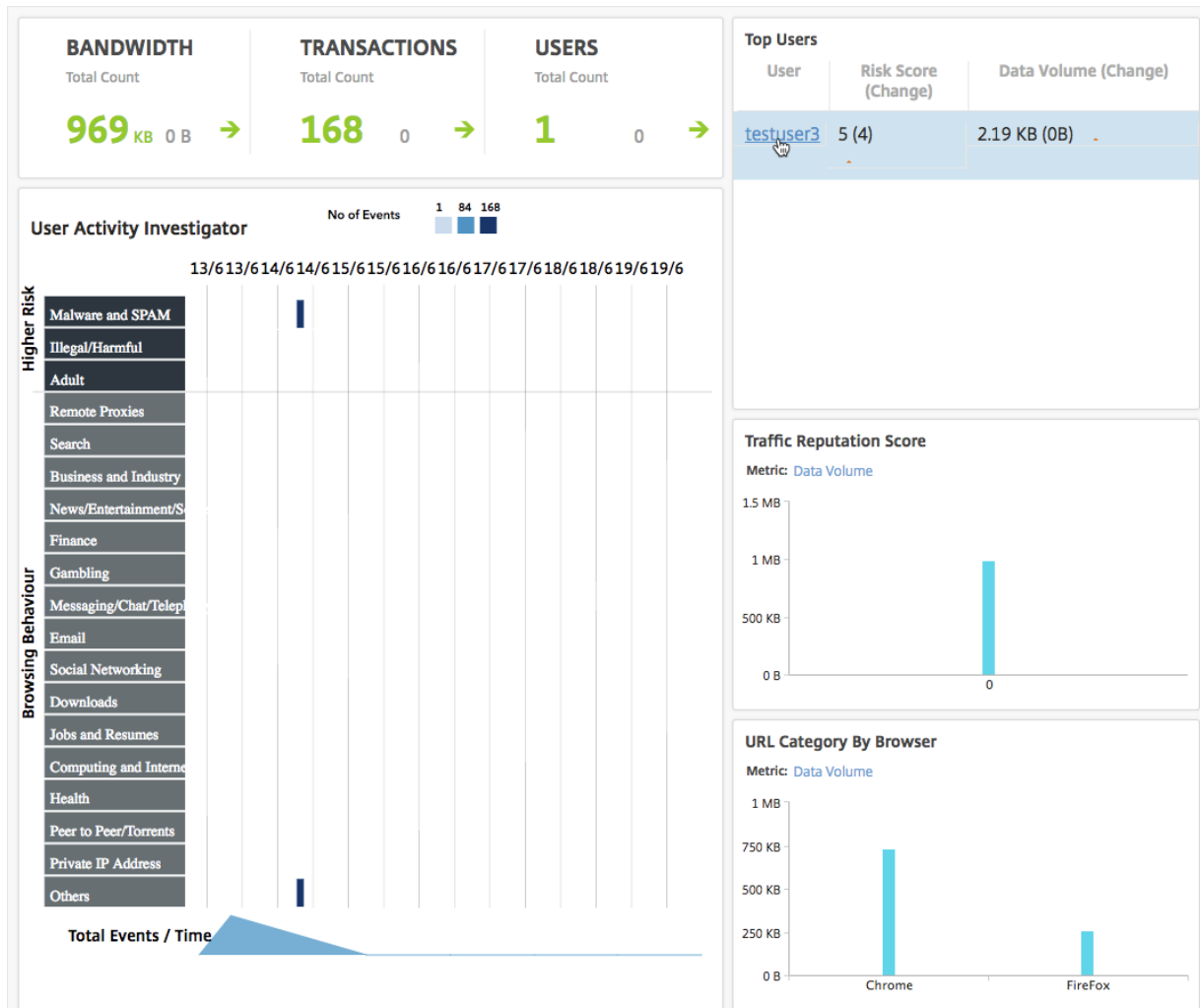
3. Les cinq principaux utilisateurs, en fonction de leurs scores de risque et de la bande passante qu'ils consomment. Pour plus d'informations sur les scores de risque, consultez [Score de risque](#).
4. Navigateurs utilisés pour accéder aux URL ou aux domaines.
5. Montant du trafic Web généré par les utilisateurs, en fonction du score de réputation de trafic.

Par exemple, si un utilisateur avec l'ID utilisateur testuser3 accède en permanence à des sites liés à des logiciels malveillants de votre entreprise, Citrix ADM identifie l'utilisateur comme un utilisateur ayant une activité à haut risque et lui attribue un score de risque plus élevé. Les informations testuser3 sont affichées dans la section **Utilisateurs les plus importants** du tableau de **bord des utilisateurs**.

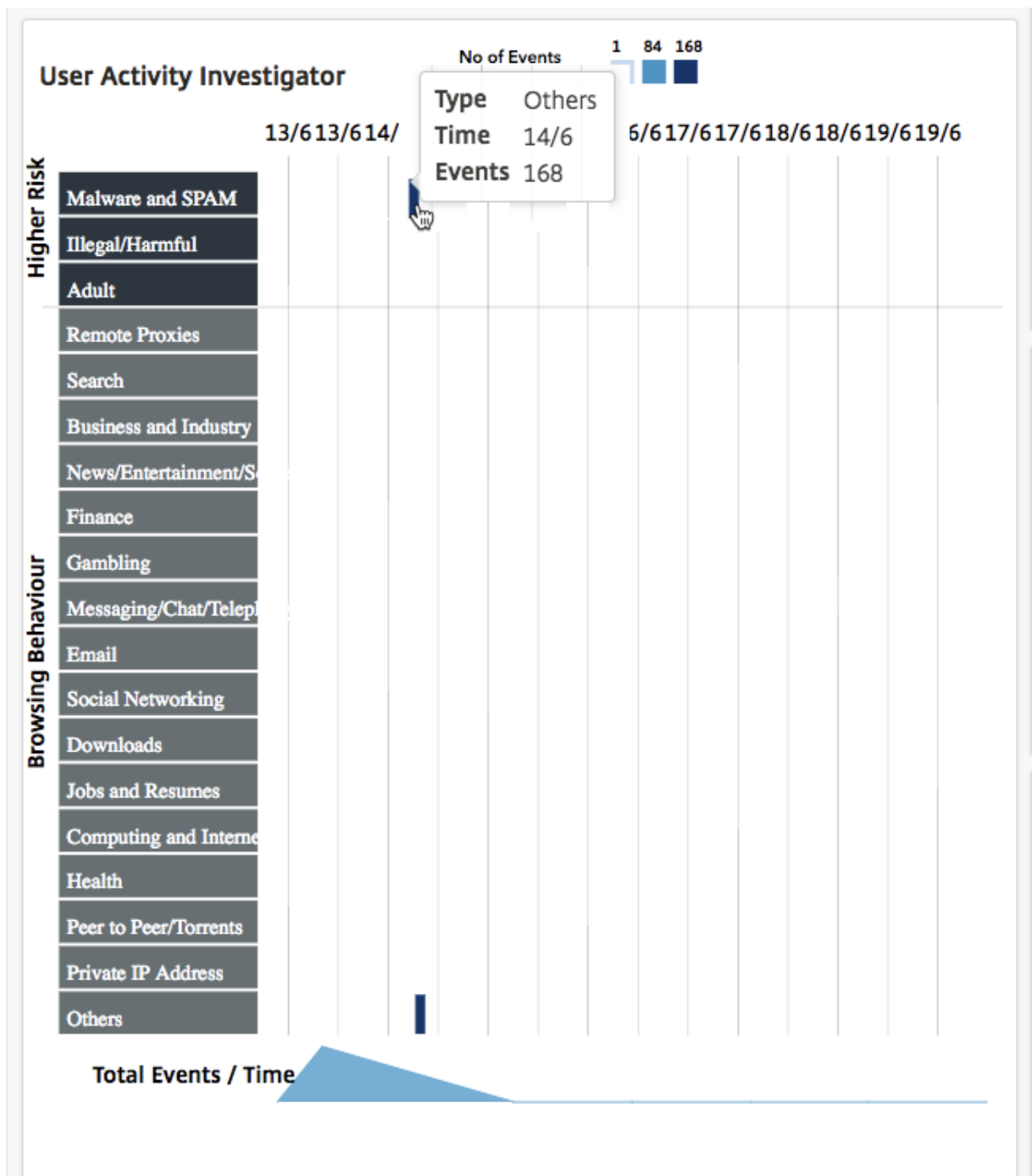
Top Users		
User	Risk Score (Change)	Data Volume (Change)
<a href="#">testuser3</a>	5 (4)	2.19 KB (0B) <span style="color: red;">▲</span>

Vous pouvez cliquer sur testuser3 pour filtrer le tableau de bord **utilisateur** afin d'afficher toutes les mesures clés liées à testuser3.





Dans le volet **Enquête sur l'activité de l'utilisateur**, l'activité à haut risque de testuser3 s'affiche sous forme d'événements dans les catégories d'URL respectives.



Vous pouvez passer la souris sur les événements pour afficher le nombre d'événements, et vous pouvez cliquer sur les événements pour examiner les transactions qui ont eu lieu pendant les événements.

Users > Dashboard > Transactions

User: [dropdown] [search icon]

Filters: URL Category: Others X User: testuser3 X [Remove all]

Transaction Details Rows: 20 Per Page Page 1 of 4 < Prev Next >

Time	Protocol	User	Domain	URL Category	Virtual Server	Client Port	Bytes In	Bytes Out
> Jun 14 06:30 AM	HTTPS	testuser3	dev.visualwebsiteoptimizer.com	Others	testswg	80	40	1043
> Jun 14 06:30 AM	HTTPS	testuser3	edellroot.badssl.com:443	Others	testswg	443	237	79
> Jun 14 06:30 AM	HTTPS	testuser3	dev.visualwebsiteoptimizer.com:443	Others	testswg	443	247	79
> Jun 14 06:30 AM	HTTPS	testuser3	no-common-name.badssl.com:443	Others	testswg	443	242	79
> Jun 14 06:30 AM	HTTPS	testuser3	connect.facebook.net:443	Others	testswg	443	237	79
> Jun 14 06:30 AM	HTTPS	testuser3	www.malwaredomainlist.com:443	Others	testswg	443	242	79
> Jun 14 06:30 AM	HTTPS	testuser3	www.vizury.com	Others	testswg	80	80	2453
> Jun 14 06:30 AM	HTTPS	testuser3	www.google.co.in:443	Others	testswg	443	233	79
> Jun 14 06:30 AM	HTTPS	testuser3	ecc256.badssl.com:443	Others	testswg	443	234	79
> Jun 14 06:30 AM	HTTPS	testuser3	hbchat.senseforth.com	Others	testswg	80	1040	74789
	OS	Windows 7		URL Category			0	
	HTTP Req Method	GET		User Agent			Firefox	
	HTTP Res Status	???		Client IP Address			10.144.8.12	
> Jun 14 06:30 AM	HTTPS	testuser3	sha512.badssl.com:443	Others	testswg	443	234	79
> Jun 14 06:30 AM	HTTPS	testuser3	revoked.badssl.com:443	Others	testswg	443	235	79
> Jun 14 06:30 AM	HTTPS	testuser3	hbsearch.senseforth.com:443	Others	testswg	443	240	79
> Jun 14 06:30 AM	HTTPS	testuser3	gp.symcd.com	Others	testswg	80	80	2197
> Jun 14 06:30 AM	HTTPS	testuser3	cbc.badssl.com:443	Others	testswg	443	231	79
> Jun 14 06:30 AM	HTTPS	testuser3	null.badssl.com:443	Others	testswg	443	232	79
> Jun 14 06:30 AM	HTTPS	testuser3	self-signed.badssl.com:443	Others	testswg	443	239	79
> Jun 14 06:30 AM	HTTPS	testuser3	invalid-expected-sct.badssl.com:443	Others	testswg	443	248	79
> Jun 14 06:30 AM	HTTPS	testuser3	www.google-analytics.com:443	Others	testswg	443	241	79
> Jun 14 06:30 AM	HTTPS	testuser3	search.services.mozilla.com:443	Others	testswg	443	619	79

Summary Panel

Protocols

Ports

URL Reputation

Browsers

Operating System

Bytes In

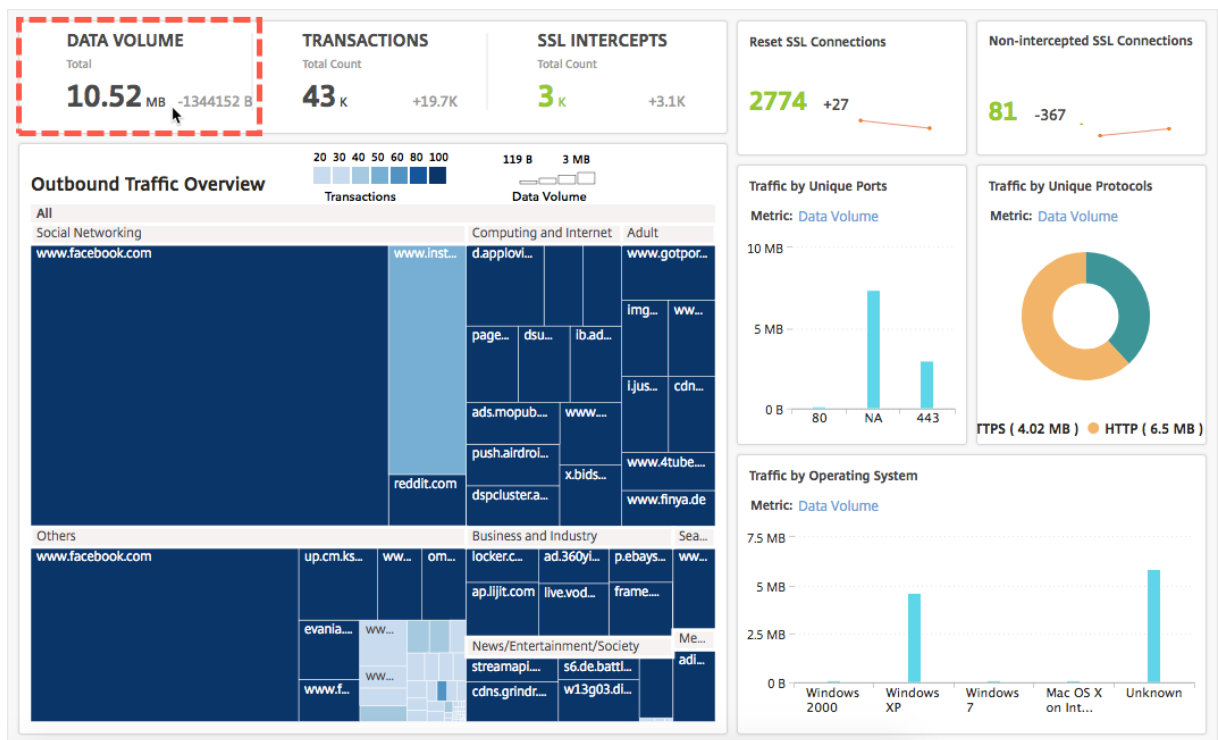
Bytes Out

Grâce à ces informations, vous pouvez déterminer si le système de l'utilisateur est infecté par un logiciel malveillant ou comprendre le modèle de consommation de bande passante de l'utilisateur et affiner vos stratégies Citrix SWG. Pour plus d'informations, consultez la [documentation de Citrix Secure Web Gateway](#).

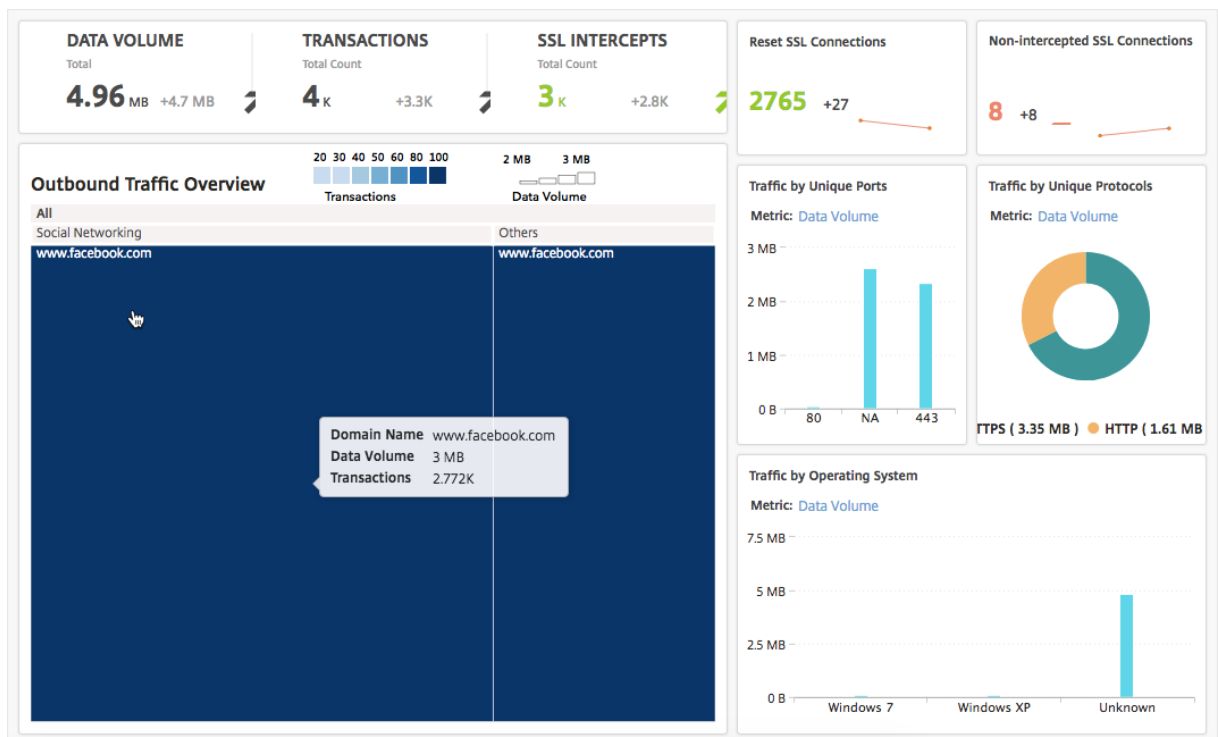
### Signaler la consommation de bande passante

Le Tableau de **bord du trafic sortant** et le Tableau de **bord des utilisateurs** fournissent plusieurs graphiques qui résument les sites Web ou les applications accessibles à partir du réseau d'entreprise, ainsi que les activités effectuées par les utilisateurs de votre réseau.

Le tableau de **bord du trafic sortant** fournit les détails de la consommation du volume de données par les URL ou les domaines auxquels vous avez accédé depuis votre réseau. Accédez à **Applications > Tableau de bord du trafic sortant**, où les détails du volume de données sont affichés dans la section **Volume de données**.

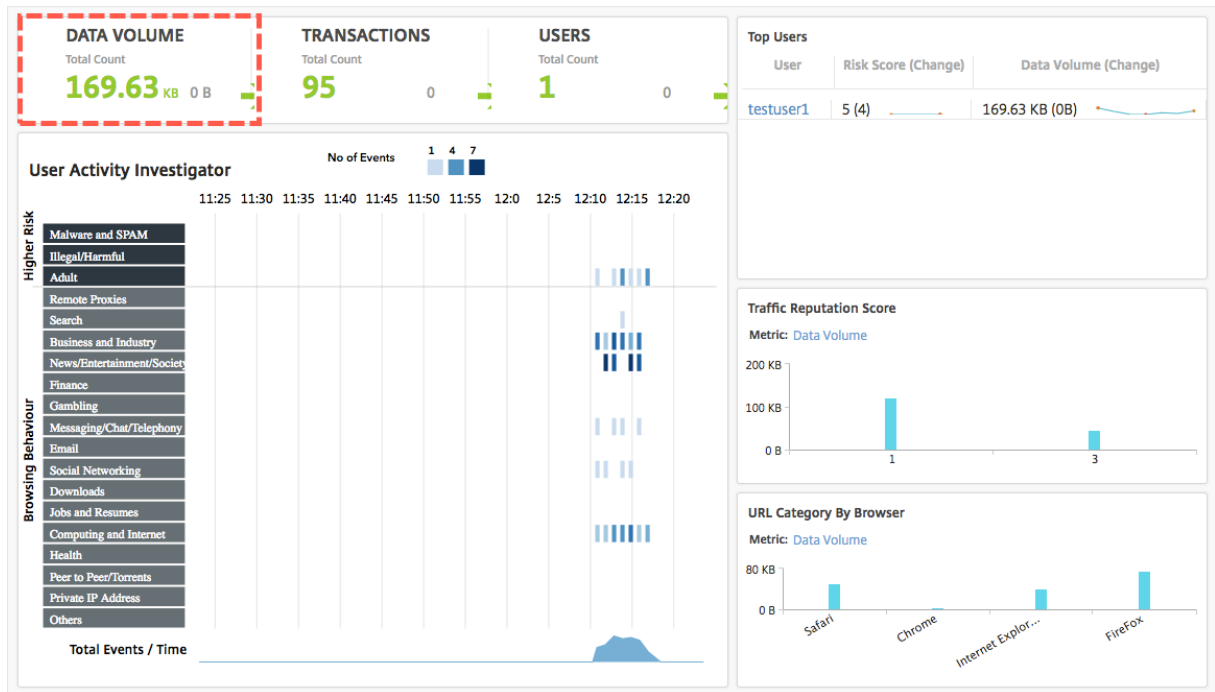


Dans le volet **Aperçu du trafic** sortant, vous pouvez cliquer sur un domaine ou une URL pour afficher les détails du volume de données consommé par le domaine ou l'URL.

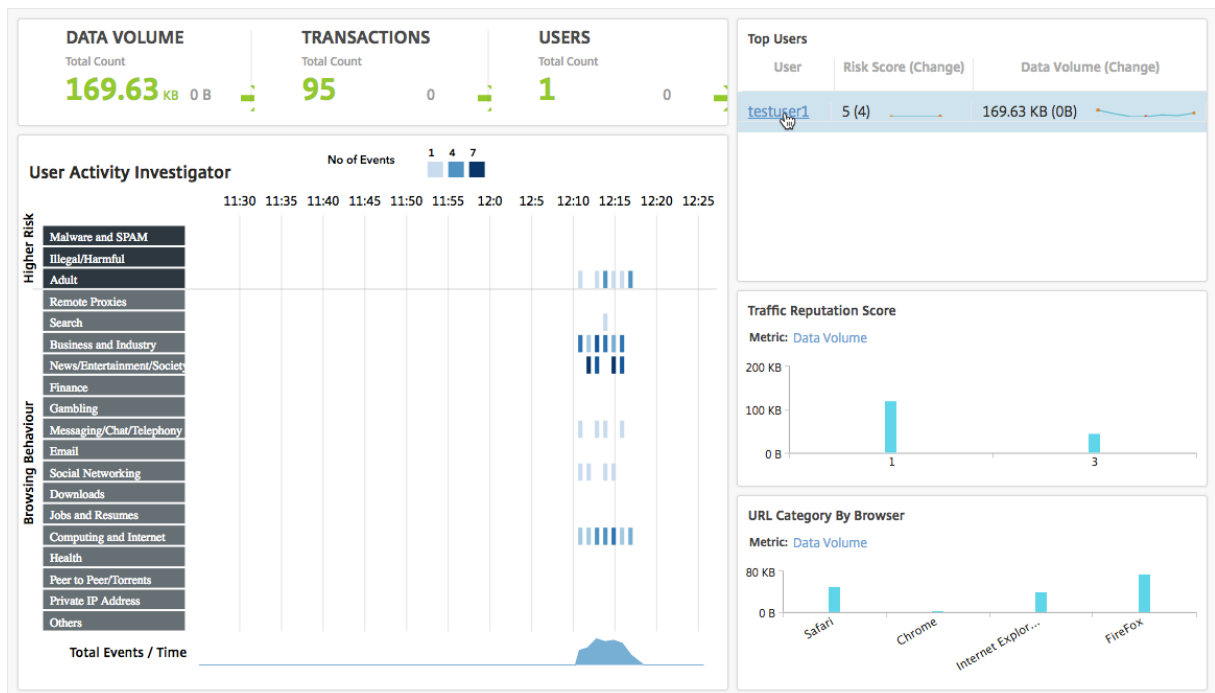


Le **tableau de bord utilisateur** fournit des détails sur la bande passante consommée par les utilisateurs de votre réseau. Accédez à **Utilisateurs > Tableau de bord** pour afficher les détails de la bande

passante consommée par les utilisateurs dans la section **VOLUME DE DONNÉES** du **Tableau de bord utilisateur**.



Vous pouvez afficher les détails de la bande passante consommée par un utilisateur en le sélectionnant dans la section **Utilisateurs les plus importants**. La section **VOLUME DE DONNÉES** et les autres mesures clés du graphique sont filtrées pour l'utilisateur sélectionné.



En utilisant ces détails, vous pouvez comprendre la consommation de bande passante et la raison de

la consommation. Par exemple, si un utilisateur accède à des sites Web de réseaux sociaux et que cela entraîne une consommation de bande passante importante, l'administrateur peut accéder à l'appliance Citrix SWG et configurer une fonctionnalité de liste d'URL pour contrôler l'accès aux sites Web. Pour plus d'informations, consultez la [rubrique Cas d'utilisation : Filtrage d'URL à l'aide d'un jeu d'URL personnalisé](#).

## Affichage de la distribution du trafic sortant

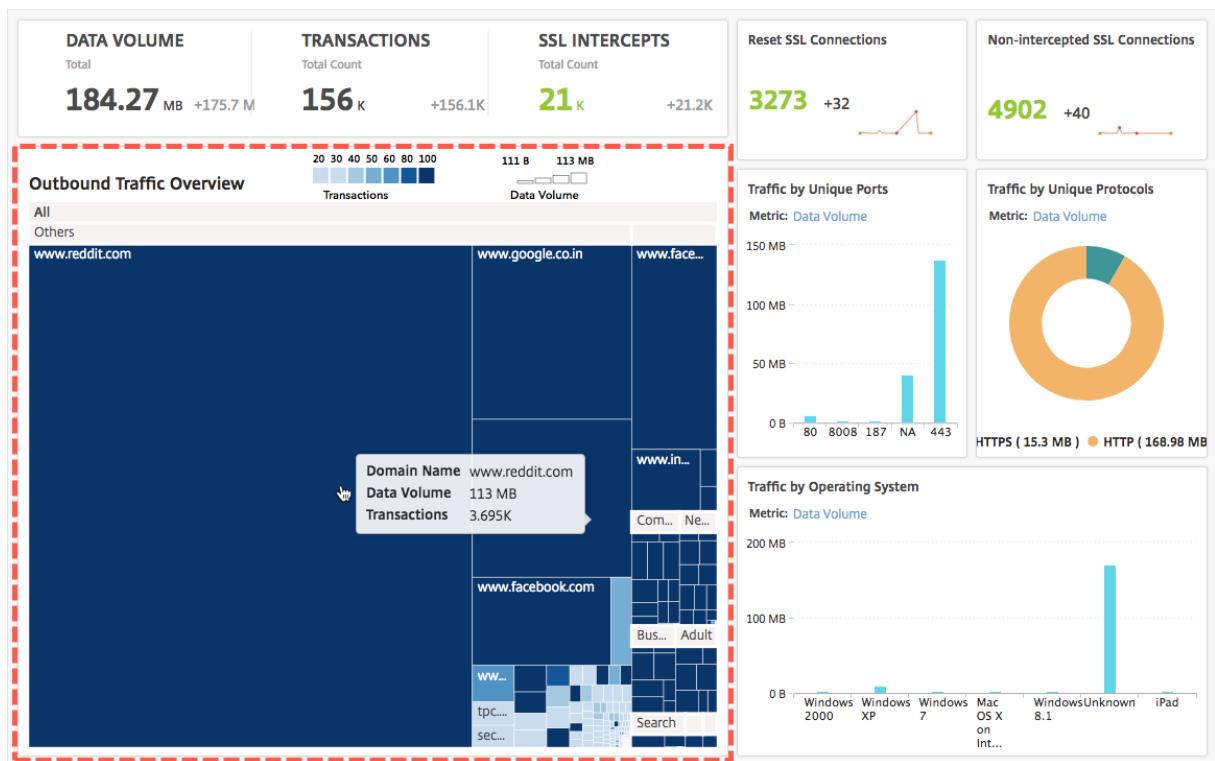
L'appliance Citrix SWG fournit des fonctionnalités de catégorisation et de filtrage d'URL que vous pouvez utiliser pour classer les URL accessibles depuis votre réseau. Dans Citrix ADM, le tableau de **bord du trafic sortant** inclut un volet **Présentation du trafic sortant**. Dans le volet **Vue d'ensemble du trafic sortant**, Citrix ADM regroupe les URL ou domaines accessibles en catégories, telles que Shopping, Actualités, Mobile, etc. pour afficher la distribution du trafic sortant dans votre réseau. Pour une période donnée, vous pouvez cliquer sur l'URL pour comprendre les éléments suivants :

1. Bande passante consommée en accédant à l'URL
2. Transactions survenues lors de l'accès à l'URL
3. Nombre de connexions SSL qui ont été interceptées, non interceptées et réinitialisées lors de l'accès à l'URL

Grâce à ces informations, vous pouvez comprendre le schéma du trafic sortant et prendre des décisions correctives, par exemple s'il faut bloquer certaines URL.

### Pour consulter la distribution du trafic sortant :

Accédez à **Applications > Tableau de bord du trafic sortant**. Le tableau de **bord du trafic hors-bord** affiche les URL dans le volet **Présentation du trafic sortant** :



Si vous souhaitez afficher les détails d’une URL particulière, sélectionnez l’URL.

Grâce à ces informations, vous pouvez comprendre le schéma du trafic sortant et contrôler votre trafic réseau à l’aide d’un filtre d’URL configuré sur votre appliance SWG. Pour plus d’informations, consultez [Filtrage d’URL](#).

## Orchestration

February 1, 2024

Dans le cadre d’un réseau défini par logiciel (SDN), un contrôleur d’application logicielle gère un réseau et ses activités plutôt que le matériel qui prend en charge le réseau. En d’autres termes, le SDN permet aux administrateurs réseau de virtualiser une connectivité réseau physique en une connectivité réseau logique et de gérer les services réseau à l’aide d’un outil de gestion centralisée basé sur un logiciel. Le SDN permet aux ingénieurs réseau et aux administrateurs de répondre à l’évolution rapide des besoins de l’entreprise.

Bien que les avantages les plus connus du SDN soient la programmabilité du trafic, une plus grande agilité, la capacité de créer une supervision réseau basée sur des stratégies et la mise en œuvre de l’automatisation du réseau, certains des avantages spécifiques du SDN sont énumérés ci-dessous :

- Approvisionnement réseau centralisé

- Sécurité réseau accrue au niveau granulaire
- Coûts d'exploitation réduits
- Niveaux accrus d'abstraction du cloud
- Diffusion de contenu garantie
- Réduction des temps d'arrêt du réseau

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

### **VMware NSX Manager**

Citrix ADM s'intègre à la plate-forme de virtualisation réseau VMware pour automatiser le déploiement, la configuration et la gestion des services Citrix ADC. Cette intégration évite les complexités traditionnelles associées à la topologie de réseau physique, permettant aux administrateurs vSphere/vCenter de déployer par programmation les services Citrix ADC plus rapidement.

VMware NSX Manager présente des pare-feu logiques, des commutateurs, des routeurs, des ports et d'autres éléments de réseau pour permettre la mise en réseau virtuelle entre divers hyperviseurs, systèmes de gestion du cloud et matériels réseau associés. Il prend également en charge la mise en réseau externe et les services de sécurité.

La fonctionnalité Cloud Orchestration de Citrix ADM permet l'intégration des produits Citrix ADC avec VMware NSX et offre les fonctionnalités suivantes :

- Possibilité d'allouer un VPX à la demande préprovisionné à une certaine Gateway Edge dans le cadre de l'insertion de service.
- Possibilité de configurer des fonctionnalités avancées de Citrix ADC telles que SSL et CS ainsi que l'équilibrage de charge de base via des modèles d'application sur les instances qui s'exécutent dans l'environnement NSX.
- Possibilité de désallouer un VPX d'une passerelle Edge donnée dans le cadre de la suppression du service et de réattribuer le même VPX à une autre passerelle Edge.
- Possibilité de déployer rapidement les fonctions Citrix ADC à partir de la console vCenter dans le cadre du flux de travail de déploiement de toute l'infrastructure requise pour une application.

Avantages :

- Allocation automatisée et à la demande de nouveaux services ADC dans le cadre d'un flux de travail de déploiement d'applications



- Configuration simplifiée des fonctionnalités ADC avancées spécifiques à l'application grâce à des modèles d'application
- Séparation des tâches entre plusieurs locataires et modèle de consommation en libre-service, tout en fournissant aux administrateurs du cloud un point de contrôle unique
- Intégration plus facile avec les API Citrix ADM, qui aident à prendre en charge les utilisations futures imprévues.

Pour plus d'informations sur la façon de configurer VMware NSX Manager sur Citrix ADM, consultez [Intégration de dispositifs Citrix ADC à VMware NSX Manager](#).

### **Mode hybride ACI Cisco**

Cisco ACI a introduit la prise en charge du mode hybride dans la version 1.3 (2f). En mode hybride, vous pouvez effectuer l'automatisation du réseau via l'APIC (Application Policy Infrastructure Controller), tout en déléguant la configuration L4-L7 à Citrix ADM, qui agit en tant que Gestionnaire de périphériques dans l'APIC.

La solution Citrix ADC Hybrid Mode est prise en charge par un package de périphériques en mode hybride et Citrix ADM. Vous devez télécharger le package de périphérique en mode hybride dans l'APIC. Pour plus d'informations, consultez [Automatisation Citrix ADC à l'aide de Citrix ADM en mode hybride de Cisco ACI](#).

## **OpenStack : intégrer des instances Citrix ADC**

February 1, 2024

La fonctionnalité Cloud Orchestration de Citrix Application Delivery Management (ADM) permet l'intégration des produits Citrix ADC à la plate-forme OpenStack. En utilisant cette fonctionnalité avec la plate-forme OpenStack, les utilisateurs d'OpenStack peuvent utiliser la fonction d'équilibrage de charge (LBaaS) du Citrix ADC. Après cela, les utilisateurs OpenStack peuvent déployer leurs configurations d'équilibrage de charge à partir d'OpenStack dans l'instance de Citrix ADC.

Les sections suivantes fournissent une brève description des fonctionnalités du workflow d'intégration Citrix ADM et OpenStack.

### **Pilote Citrix ADC pour LBaaS OpenStack Neutron**

Le plugin OpenStack Neutron LBaaS inclut un pilote Citrix ADC qui permet à OpenStack de communiquer avec Citrix ADM. OpenStack utilise ce pilote pour transférer toute configuration d'équilibrage

de charge effectuée via les API LBAaS à Citrix ADM, qui crée la configuration d'équilibrage de charge sur les instances Citrix ADC souhaitées. OpenStack utilise également le pilote pour appeler Citrix ADM à intervalles réguliers afin de récupérer l'état des différentes entités (telles que les VIP et les pools) de toutes les configurations d'équilibrage de charge à partir des Citrix ADC. Le logiciel de pilote Citrix ADC pour la plate-forme OpenStack est fourni avec Citrix ADM. Pour télécharger et installer les pilotes, vous devez d'abord installer Citrix ADM et lancer l'application.

## **Enregistrez Citrix ADM et OpenStack l'un avec l'autre**

Vous devez d'abord enregistrer les informations OpenStack sur Citrix ADM. Spécifiez l'adresse IP du Controller OpenStack et les informations d'identification de l'utilisateur d'administration du cloud, ainsi que les informations d'identification de l'utilisateur du pilote ADC OpenStack Citrix. Vous pouvez ensuite spécifier les mêmes informations d'identification de connexion dans la section Citrix ADC\_Driver du fichier de configuration Neutron (neutron.conf) afin que le pilote Citrix ADC dans OpenStack puisse se connecter à Citrix ADM pendant les configurations LB.

Une fois OpenStack et Citrix ADM enregistrés les uns avec les autres, les deux peuvent se parler. En outre, les utilisateurs OpenStack peuvent utiliser leurs informations d'identification existantes dans OpenStack pour se connecter à l'interface utilisateur Citrix ADM afin de vérifier les performances de leurs configurations LB dans les Citrix ADC.

## **Locataires dans OpenStack**

Dans OpenStack, un client est également appelé projet. Un locataire est un groupe d'utilisateurs ; un locataire ou un projet peut également être défini comme un ensemble de ressources (calcul, réseau, stockage, etc.) attribuées à un groupe isolé d'utilisateurs.

## **Stratégies de placement**

Les stratégies de placement offrent la flexibilité nécessaire pour décider de l'instance Citrix ADC utilisée dans chaque configuration d'équilibrage de charge créée par les utilisateurs. Alternativement, Citrix ADM propose également une option permettant d'affecter une instance Citrix ADC en fonction des locataires OpenStack.

## **Paquets de services**

Les packages de services sont des ensembles qui relient des stratégies/SLA, des spécifications de configuration des appareils ou du provisionnement automatique et des stratégies de locataire/de placement. Un package de services est généralement défini en termes de stratégies d'isolation fournies au locataire.

Voici quelques points relatifs aux packages de services :

- Un locataire ne peut pas participer à plus d'un ensemble de services.
- Plusieurs locataires peuvent être associés au même package de services.
- Dans un service package défini pour le provisionnement automatique, les instances virtuelles Citrix ADC peuvent être créées à partir d'un seul type de plate-forme (sur la plate-forme SDX ou sur la plate-forme OpenStack Compute).

### **Fonctionnalités prises en charge sur LBaaS V1 et LBaaS V2**

Alors que le pilote LBaaS V1 dans OpenStack prend en charge les opérations à partir de l'interface utilisateur OpenStack Horizon, le pilote LBaaS V2 ne prend en charge que les opérations en ligne de commande.

La liste suivante répertorie les fonctionnalités prises en charge sur LBaaS V1 et LBaaS V2 sur OpenStack :

- LBaaS V1
  - Équilibrage de charge
- LBaaS V2
  - Équilibrage de charge
  - Déchargement SSL avec des certificats gérés par Barbican, Key Manager dans OpenStack
  - Ensembles de certificats (y compris les autorités de certification intermédiaires)
  - Support SNI

Ce document fournit des informations sur :

- Scénario de cas d'utilisation
- Intégration de Citrix ADM avec OpenStack Workflow
- [Prerequisites](#)
- [Tâches de pré-configuration dans Citrix ADM et OpenStack](#)
- [Étapes de configuration pour LBaaS V1 à l'aide d'Horizon](#)
- [Étapes de configuration pour LBaaS V2 à l'aide de la ligne de commande](#)
- [Provisionnement manuel de l'instance Citrix ADC VPX sur OpenStack](#)
- [Intégration de Citrix ADM avec OpenStack Heat Services](#)
- [Surveillance des applications OpenStack dans Citrix ADM](#)

## Scénario de cas d'utilisation

Le scénario de cas d'utilisation suivant explique le flux de travail d'intégration de Citrix ADM avec la plate-forme OpenStack :

Une entreprise, Example-Cloud-Provider, a utilisé des composants OpenStack pour configurer un cloud afin de fournir une infrastructure à ses locataires. Steve est l'administrateur de ce fournisseur de cloud, tandis que Tom est un locataire de l'infrastructure cloud de l'Example-Cloud-Provider. L'organisation de Tom, Example-Sportsonline.com, nécessite deux serveurs S1 et S1, et Tom nécessite également un périphérique Citrix ADC dédié pour équilibrer la charge du trafic entre les serveurs S1 et S2 sur la plate-forme OpenStack.

Pour répondre à cette exigence, Steve doit installer et configurer OpenStack et Citrix ADM, et les préparer à travailler les uns avec les autres. Steve doit créer un compte locataire nommé Example-SportsOnline dans OpenStack, puis allouer des ressources au compte locataire. Steve doit également créer différents identifiants de connexion (utilisateurs) pour Example-SportsOnline afin de gérer ses ressources et sa configuration. Tom peut désormais créer les deux serveurs S1 et S2 sur OpenStack pour gérer le trafic dans son organisation.

Steve doit enregistrer les détails OpenStack auprès de Citrix ADM et configurer le pilote LBaaS Citrix ADC dans le composant réseau OpenStack, Neutron. Une fois l'enregistrement terminé, Citrix ADM affiche les détails de tous les locataires dans OpenStack. Steve peut sélectionner Example-SportsOnline dans la liste qui souhaite les fonctionnalités de Citrix ADC LBaaS et configurer Tom pour obtenir un Citrix ADC dédié alloué pour ses configurations d'équilibrage de charge dans Citrix ADM.

Pour cela, Steve peut soit provisionner une instance Citrix ADC VPX sur la couche de calcul (Nova) d'OpenStack à l'aide de l'interface utilisateur Citrix ADM, soit permettre à MAS de provisionner automatiquement une instance Citrix ADC VPX à la demande, lorsque Tom effectue sa configuration LB dans OpenStack. Dans les deux cas, Citrix ADM gère l'instance VPX. Pour ce faire, Steve crée un package de service dans Citrix ADM, et définit les conditions du package de service qui ont été convenues dans le SLA avec Tom. Par exemple, Steve sélectionne la stratégie d'isolement « dédiée » pour fournir une instance dédiée pour fournir des configurations d'équilibrage de charge à Tom. Autrement dit, Steve sélectionne une instance non partagée pour Tom dans le package de services. Il attribue ensuite de nombreuses instances Citrix ADC VPX au service package, et associe Example-SportsOnline, ainsi que d'autres locataires, qui ont besoin d'un Citrix ADC dédié au service package. Par conséquent, lorsque Tom effectue sa première configuration d'équilibrage de charge, Citrix ADM attribue l'une des instances Citrix ADC VPX du service package à Example-SportsOnline et déploie également sa configuration dans ce Citrix ADC.

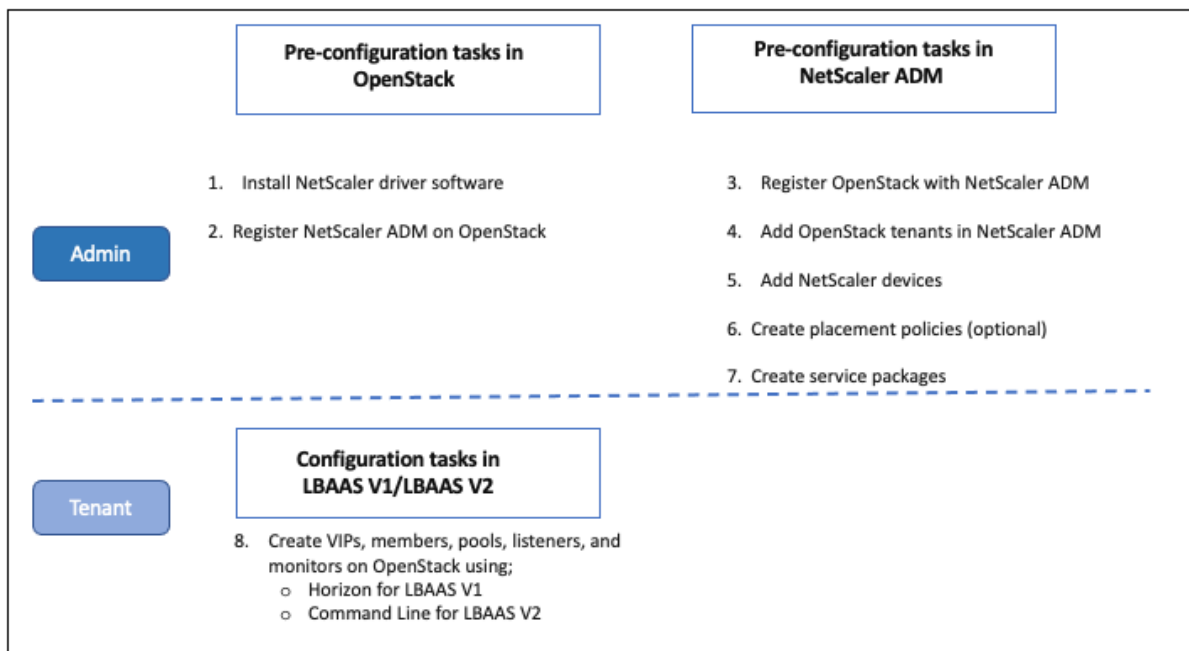
Tom peut désormais créer des configurations d'équilibrage de charge en créant des pools, des adresses IP virtuelles (VIP) et des moniteurs de santé à l'aide d'OpenStack LBAAS/UI. Les pools et les VIP dans OpenStack sont déployés en tant que groupes de services et serveurs virtuels sur l'instance de Citrix ADC. Tom peut également créer des moniteurs de santé pour surveiller les serveurs et

envoyer le trafic des applications uniquement aux serveurs qui sont UP à tout moment et accessibles depuis Citrix ADC.

La configuration d'équilibrage de charge créée dans OpenStack est désormais implémentée sur l'instance de Citrix ADC. Une fois entièrement configurée, l'instance Citrix ADC VPX reprend ensuite la fonctionnalité d'équilibrage de charge et commence à accepter le trafic de l'application et équilibre la charge le trafic entre les serveurs S1 et S2 créés par Tom.

## Intégration de Citrix ADM au flux de travail OpenStack

L'organigramme suivant illustre le flux de travail que vous devez suivre lorsque vous configurez LBaaS V1 et LBaaS V2.



## Conditions préalables

February 1, 2024

Avant d'intégrer l'instance virtuelle Citrix ADC à la plate-forme OpenStack, assurez-vous que les conditions suivantes sont remplies :

## Configuration logicielle requise pour Citrix ADM et OpenStack

- Citrix ADM 12.1 est installé sur un poste de travail Hypervisor pris en charge qui répond à la configuration matérielle minimale requise.
- Les composants OpenStack sont installés et en cours d'exécution.
- Citrix ADM 12.1 prend en charge les versions d'OpenStack suivantes : Newton, Ocata et Pike.

## Configuration matérielle requise pour Citrix ADM

Le tableau suivant répertorie les ressources informatiques virtuelles que vous devez disposer sur votre serveur OpenStack pour installer les instances virtuelles Citrix ADC.

Composant	Exigences
RAM	8 GB
CPU virtuel	8
Espace de stockage	500 GB
Interfaces réseau virtuelles	1
Débit	1 Gbit/s ou 100 Mbit/s

### Remarque

Les exigences en matière de mémoire et de disque dur spécifiées ci-dessus concernent le déploiement de Citrix ADM sur la plate-forme OpenStack, étant donné qu'aucune autre machine virtuelle n'est exécutée sur l'hôte. La configuration matérielle requise pour OpenStack dépend du nombre de machines virtuelles qui s'y exécutent.

## Tâches de pré-configuration dans Citrix ADM et OpenStack

February 1, 2024

Cette section vous aide à effectuer les tâches de pré-configuration avant de configurer Citrix Application Delivery Management (ADM) et OpenStack.

## Installation de Citrix ADM

Installez Citrix ADM sur un Hypervisor pris en charge. Pour plus d'informations sur la façon de télécharger et d'installer Citrix ADM, consultez [Déploiement de Citrix ADM](#).


## Installation du pilote Citrix ADC et enregistrement de Citrix ADM sur OpenStack

Téléchargez l'offre groupée Citrix ADC pour OpenStack à partir de la page Téléchargements Citrix ADM.

### Pour installer le pilote Citrix ADC sur la plate-forme OpenStack à l'aide de l'interface graphique Citrix ADM :

1. Dans Citrix ADM, cliquez sur **Téléchargements**. La page **Téléchargements** de Citrix ADM fournit des liens pour télécharger le **bundle Citrix ADC pour le logiciel OpenStack** requis pour les versions Newton, Ocata et Pike OpenStack.
2. Téléchargez le dernier fichier tar du bundle Citrix ADC dans un répertoire temporaire (par exemple, /tmp) dans OpenStack Controller. Ce bundle inclut le pilote LBaaS V2 et le plug-in Heat pour toutes les versions d'OpenStack.

Downloads for OpenStack

 Citrix ADC bundle for OpenStack. Contains Citrix ADC LBaaS drivers and Heat plugin. Citrix ADC bundle for OpenStack has Heat plugin and drivers for both OpenStack LBaaS V1 and V2. The Citrix ADC bundle files provided here includes the following drivers and plugins: LBaaS V1 and LBaaS V2 drivers for OpenStack Liberty and Mitaka releases, LBaaS V2 driver for OpenStack Newton release and Heat plug-in for Heat across OpenStack releases

3. Exécutez la commande suivante pour extraire les fichiers du fichier tar du pilote Citrix ADC :  
`tar -xvzf <name_of_tar_file>`
4. Si vous avez un OpenStack <Release Name> setup, à l'invite, tapez la commande suivante :

```
cd <Release Name>
```

#### Exemple :

```
cd Newton
```

5. Exécutez la commande suivante pour installer le pilote et spécifier l'adresse IP Citrix ADM, le mot de passe du pilote Citrix ADC que vous avez configuré lorsque vous avez enregistré OpenStack auprès de Citrix ADM et le protocole :

```
./install.sh --ip=<NetScaler_MAS_IP> --password=<password> --protocol=<protocol> --neutron-lbaas-path <neutron-lbaas-directory-path>
```

#### Exemple pour la configuration d'OpenStack à nœud unique :

```
./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --neutron-lbaas-path=/opt/stack/neutron-lbaas
```

### Exemple de configuration d'OpenStack à plusieurs nœuds :

```
./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --  
neutron-lbaas-path=/usr/lib/python2.7/site-packages
```

#### Remarque

Fournir le chemin du répertoire neutron-lbaas du système est facultatif. La fourniture du chemin d'accès peut aider le script à trouver les pilotes.

Une fois que Citrix ADM est enregistré avec succès sur OpenStack, vous pouvez vous connecter à Citrix ADM à l'aide de vos informations d'identification utilisateur OpenStack.

Une fois que Citrix ADM est enregistré avec succès sur OpenStack, redémarrez les services OpenStack Neutron.

## Enregistrement d'OpenStack avec Citrix ADM

### Pour enregistrer OpenStack auprès de Citrix ADM à l'aide de l'interface graphique Citrix ADM :

1. Dans Citrix ADM, accédez à **Orchestration > Cloud Orchestration > OpenStack**.
2. Cliquez sur **Configurer les paramètres OpenStack**.
3. Dans la page **Configurer les paramètres OpenStack**, vous pouvez définir les paramètres pour configurer OpenStack dans Citrix ADM. Vous avez deux options ici - Par défaut et Personnalisé.

Pour les versions Newton et Ocata d'OpenStack, vous pouvez utiliser le type de déploiement par défaut ou personnalisé. Mais pour la version Pike, vous devez utiliser un type de déploiement personnalisé pour enregistrer OpenStack auprès de Citrix ADM.

#### • Type de déploiement par défaut

Sélectionnez **Par défaut**, si les services OpenStack s'exécutent sur les ports par défaut. Par exemple, le portail par défaut pour les services Neutron est 9696, le portail par défaut pour les services Keystone est 5000.

1. Adresse IP du Contrôleur OpenStack - Adresse IP du contrôleur OpenStack (le service KeyStone et le service Neutron doivent être accessibles sur cette adresse IP). Par exemple, entrez l'adresse IP 10.102.205.23.
2. Nom d'utilisateur d'administration OpenStack - nom d'utilisateur administratif du Contrôleur OpenStack. Par exemple, entrez admin1.
3. Mot de passe : mot de passe de l'utilisateur administratif du contrôleur OpenStack.
4. OpenStack Admin Tenant : nom du locataire administratif sur OpenStack. Par exemple, entrez admin.



### OpenStack Details

Configure access details of OpenStack controller which can be used by NetScaler Console. NetScaler Console will use these credentials to create NetScaler virtual appliances, to reserve IPs, to fetch tenants/flavours/images etc

Openstack Deployment Type\*

Default  Customized

OpenStack Controller IP Address/FQDN\*

HTTPS  HTTP

Neutron Service URL/FQDN\*

Keystone Service URL/FQDN\*

Keystone Admin Service URL/FQDN\*

Nova Service URL/FQDN\*

Glance Service URL/FQDN\*

OpenStack Admin Username\*

Password\*

OpenStack Admin Tenant\*

 ⓘ

- **Type de déploiement personnalisé**

Sélectionnez le type de déploiement comme **personnalisé** si les services OpenStack s'exécutent sur des ports différents des ports par défaut. Si ces services sont exécutés sur des ports différents, spécifiez-les ici. L'enregistrement des versions OpenStack Newton et Ocata avec Citrix ADM est différent de l'enregistrement de la version OpenStack Pike.

**Newton et Ocata Version d'OpenStack :**

1. Spécifiez les numéros de port pour les différents services OpenStack si vous enregistrez la version Newton d'OpenStack.
2. Spécifiez le nom d'utilisateur, le mot de passe et le nom d'utilisateur du locataire d'administration OpenStack comme vous l'aviez indiqué précédemment dans les paramètres **par défaut**.

### OpenStack Details

Configure access details of OpenStack controller which can be used by NetScaler Console. NetScaler Console will use these credentials to create NetScaler virtual appliances, to reserve IPs, to fetch tenants/flavours/images etc

Openstack Deployment Type\*

Default  Customized

OpenStack Controller IP Address/FQDN\*

HTTPS  HTTP

Neutron Service URL/FQDN\*

Keystone Service URL/FQDN\*

Keystone Admin Service URL/FQDN\*

Nova Service URL/FQDN\*

Glance Service URL/FQDN\*

OpenStack Admin Username\*

Password\*

OpenStack Admin Tenant\*

 ⓘ

### Pike Release d'OpenStack :

Si vous enregistrez la version Pike d'OpenStack, entrez les détails des services OpenStack comme indiqué dans l'image suivante. Vous devez également spécifier le nom d'utilisateur d'OpenStack Admin, le mot de passe et le nom d'utilisateur du locataire d'administration OpenStack comme dans Paramètres par défaut.

OpenStack Details

Configure access details of OpenStack controller which can be used by NetScaler Console. NetScaler Console will use these credentials to create NetScaler virtual appliances, to reserve IPs, to fetch tenants/flavours/images etc

Openstack Deployment Type\*

Default  Customized

OpenStack Controller IP Address/FQDN\*

HTTPS  HTTP

Neutron Service URL/FQDN\*

Keystone Service URL/FQDN\*

Keystone Admin Service URL/FQDN\*

Nova Service URL/FQDN\*

Glance Service URL/FQDN\*

OpenStack Admin Username\*

Password\*

OpenStack Admin Tenant\*

 ⓘ

1. Dans la section **OpenStack Neutron LBaaS - Informations d'identification utilisées par Citrix ADC Driver**, définissez le mot de passe du pilote Citrix ADC pour le compte d'utilisateur du pilote ADC OpenStack Citrix. Citrix ADM authentifie les appels à partir du pilote ADC OpenStack Citrix à l'aide de ces informations d'identification. Vous devez spécifier le même mot de passe lorsque vous exécutez le script d'installation du pilote Citrix ADC dans le Controller OpenStack.

OpenStack - Credentials Used by NetScaler Driver and Heat

Configure an account in NetScaler Console that can be used by NetScaler driver and Heat, present in OpenStack Controller, to contact NetScaler Console. Once configured here, provide these credentials in the [citrix\_adc\_driver] section of neutron configuration file /etc/neutron/neutron.conf .

NetScaler Username

NetScaler Password\*

 ⓘ
 

Confirm NetScaler Password\*

 ⓘ

2. Cliquez sur **OK**.

## Création d'un locataire sur OpenStack

Créez un projet ou un locataire sur OpenStack, ajoutez des utilisateurs au projet ou au locataire et attribuez des rôles à tous les utilisateurs. KeyStone, le service Identity dans OpenStack fournit des services d'authentification pour chaque service OpenStack. Le service d'authentification utilise une combinaison de domaines, de projets (locataires), d'utilisateurs et de rôles.

Pour plus d'informations sur la création d'un projet et sur l'exécution d'autres tâches dans OpenStack, consultez la documentation d'OpenStack sur <http://docs.openstack.org/>.

## Ajout de locataires OpenStack

1. Dans Citrix ADM, accédez à **Orchestration >Cloud Orchestration> OpenStack >Locataires OpenStack**, puis cliquez sur **Ajouter**.
2. Dans la page **Ajouter des locataires OpenStack**, cliquez sur **+Ajouter**, puis sélectionnez le locataire OpenStack.
3. Cliquez sur **OK**.

Selon que vous utilisez une instance pré-provisionnée ou le provisionnement automatique de l'instance lorsque vous intégrez OpenStack, procédez à l'une des deux tâches suivantes :

- Préprovisionner les périphériques Citrix ADC
- Provisionnement automatique des périphériques Net Scaler VP X sur OpenStack

## Provisionnement des périphériques Citrix ADC

Selon que vous utilisez une instance pré-provisionnée ou le provisionnement automatique de l'instance lorsque vous intégrez OpenStack, procédez à l'une des deux tâches suivantes :

- Préprovisionner les périphériques Citrix ADC
- Provisionnement automatique des périphériques Net Scaler VP X sur OpenStack

## Préprovisionnement des périphériques Citrix ADC

Installez le périphérique Citrix ADC sur l'une des plateformes d'hyperviseur telles que Citrix Hypervisor, KVM ou ESX, et ajoutez l'instance à Citrix ADM. Citrix ADM gère ensuite ce périphérique qui équilibre la charge du trafic dans les serveurs.

### Pour ajouter une instance Citrix ADC VPX existante dans Citrix ADM :

1. Dans Citrix ADM, accédez à **Infrastructure >Instances >Citrix ADC VPX**, puis cliquez sur **Ajouter**.

2. Sur la page **Ajouter un Citrix ADC VPX**, spécifiez l'adresse IP de l'instance Citrix ADC VPX et sélectionnez un profil d'instance dans la liste **Nom du profil**. Le profil d'instance contient les informations d'identification utilisées pour ouvrir une session au Citrix ADC VPX. Vous pouvez également créer un profil d'instance en cliquant sur l'icône +. Cliquez sur **OK**.

### **Provisionnement automatique des périphériques Citrix ADC**

Téléchargez l'image d'instance Citrix ADC requise à partir de la page de téléchargement Citrix, puis téléchargez-la sur Glance, le service OpenStack Imaging. La disponibilité d'une image sur Glance vous permet de configurer une instance Citrix ADC à la demande lors de l'attribution de l'instance au locataire.

#### **Pour provisionner automatiquement les périphériques Citrix ADC VPX sur OpenStack :**

1. Dans Citrix ADM, accédez à **Orchestration > Cloud Orchestration > OpenStack**.
2. Cliquez sur **Paramètres de déploiement**.
3. Définissez les paramètres suivants :
  - a) Réseau de gestion : sélectionnez le réseau de gestion sur OpenStack, auquel le Citrix ADC VPX provisionné automatiquement est connecté.
  - b) Nom du profil : sélectionnez le profil dans la liste déroulante. Citrix ADM utilise le mot de passe contenu dans ce profil pour configurer de nouvelles instances Citrix ADC VPX provisionnées automatiquement.
  - c) Licences : fournissez les codes d'activation de licence (LAC) Citrix ADM utilisés pour la licence de nouvelles instances Citrix ADC provisionnées automatiquement. Citrix ADM provisionne les instances Citrix ADC sur le calcul OpenStack dans le réseau de gestion, puis déclenche l'installation de licence sur ces instances à l'aide du code de licence spécifié. L'instance de Citrix ADC télécharge ensuite les fichiers de licence à partir du site Web Citrix à l'aide de la LAC spécifiée ici.
  - d) Citrix ADC VPX Image in Glance : sélectionnez l'image Citrix ADC VPX disponible dans OpenStack Glance qui est utilisée pour créer une instance VPX Citrix ADC.
  - e) Paramètres proxy : fournit des détails sur le serveur proxy Citrix ADC pour l'installation des licences. Cela peut être nécessaire lorsque Citrix ADC n'a pas accès direct à Internet via le réseau de gestion.
4. Cliquez sur **OK**.

## Création d'un service package dans Citrix ADM

### Pour créer des packages de services pour un locataire dans Citrix ADM :

1. Dans Citrix ADM, accédez à **Orchestration > Cloud Orchestration > OpenStack > Service Packages**, puis cliquez sur **Ajouter**.
2. Dans la page **Service Package**, spécifiez les paramètres suivants :
  - a) Name : nom du package de service. Par exemple, entrez SVC-PKG-GOLD.
  - b) Allocation d'instance Citrix ADC : type d'allocation d'instance défini dans le package de services basé sur lequel les ressources d'instance Citrix ADC sont allouées à un locataire. Sélectionnez **Dédié**. Pour plus d'informations sur les stratégies, consultez [Stratégies d'isolation des packages de services](#).
  - c) Provisioning d'instance Citrix ADC : sélectionnez **Instance existante** pour allouer une instance Citrix ADC existante à un locataire. Si vous souhaitez créer des instances Citrix ADC pendant la configuration elle-même, sélectionnez **Create Instance OnDemand**.
  - d) Citrix ADC Instance Type - sélectionnez **Citrix ADC VPX**.

#### Remarque

Sélectionnez Citrix ADC VPX pour allouer des instances Citrix ADC préprovisionnées hébergées sur la plate-forme SDX.

3. Cliquez sur **Continuer** pour associer un locataire à un package de services.

#### Remarque

Activer le **provisionnement de la paire d'instances Citrix ADC pour la haute disponibilité**, si vous déployez les instances Citrix ADC en mode haute disponibilité.

4. **Dans la section Affecter des instances**, cliquez sur **Ajouter**, puis sélectionnez l'instance Citrix ADC que vous souhaitez affecter au locataire, puis cliquez sur **Continuer**.
5. Dans la section **Affecter des locataires OpenStack ou des stratégies de placement**, sous **Locataires OpenStack**, cliquez sur **Ajouter**, puis sélectionnez le locataire.
6. Cliquez sur **Continuer**, puis sur **Terminé**.

#### Remarque

Si la stratégie n'est pas trouvée, le mécanisme de secours est rétabli et Citrix ADM attribue des instances Citrix ADC en fonction des locataires. Si le locataire ne fait partie d'aucun package de services, Citrix ADM affiche un message d'erreur indiquant : « Le locataire <admin> ne fait partie d'aucun Service Package et il n'y a aucun Service Package par défaut. »

## Création de stratégies de placement (facultatif)

Les stratégies d'isolation ne sont pas uniquement basées sur les locataires. Vous pouvez créer des stratégies de placement flexibles, où elles sont basées non seulement sur le nom ou l'ID du locataire, mais également sur d'autres attributs personnalisés.

### Pour créer des stratégies de placement pour un locataire dans Citrix ADM :

1. Dans Citrix ADM, accédez à **Orchestration > Cloud Orchestration > OpenStack > Stratégie de placement**, puis cliquez sur **Ajouter**.
2. Dans la page **Ajouter une stratégie de placement**, définissez les paramètres suivants :
  - a) Nom : entrez un nom pour la stratégie de placement
  - b) Exemples d'expressions : sélectionnez un exemple d'expression dans la liste. Ces exemples sont utiles pour élaborer la stratégie de placement.
  - c) Expression : une expression booléenne est renseignée dans ce champ en fonction de l'exemple d'expression que vous avez sélectionné dans le champ précédent. Modifiez les noms des champs selon vos besoins.

3. Cliquez sur **OK**.

### **Activation du trafic à partir d'instances Citrix ADC vers les serveurs principaux via le réseau client**

Par défaut, dans le workflow d'orchestration OpenStack, les instances Citrix ADC sont liées dynamiquement à l'équilibreur de charge ou aux réseaux clients et aux réseaux membres ou serveurs.

Dans certains déploiements, les serveurs sont également accessibles via les réseaux clients et peuvent être routés via la Gateway client. Dans de tels cas, les instances Citrix ADC ne doivent pas être liées aux réseaux de serveur, mais elles doivent être liées uniquement aux réseaux clients.

Effectuez le paramètre suivant pour configurer le trafic via la Gateway client.

Accédez à **Orchestration > Cloud Orchestration > OpenStack > Paramètres de déploiement**, puis sélectionnez l'option **Provisionner uniquement le réseau VIP et acheminer le trafic de pool via le réseau VIP**.

Citrix ADM configure ensuite l'instance Citrix ADC sur les réseaux clients en ajoutant un SNIP dans ce réseau et ajoute une route par défaut à la Gateway réseau client. Cela permet à l'instance d'atteindre les serveurs via la Gateway client.

### **Provisionnement automatique des périphériques Citrix ADC VPX déployés sur la plate-forme Citrix ADC SDX**

Ajoutez la plate-forme Citrix ADC SDX dans Citrix ADM, de sorte que Citrix ADM provisionne les instances sur cette plate-forme à la demande.

#### **Pour provisionner automatiquement les instances Citrix ADC déployées sur la plate-forme Citrix ADC SDX :**

1. Dans l'interface graphique Citrix ADM, accédez à **Réseaux > Instances > Citrix ADC SDX**, puis cliquez sur **Ajouter** pour ajouter une plate-forme Citrix ADC SDX.
2. Accédez à **Orchestration > Cloud Orchestration > OpenStack > Paramètres de déploiement**.
3. Dans la **section Réseau** de gestion, sélectionnez le réseau de gestion sur OpenStack auquel le SDX Citrix ADC provisionné automatiquement est connecté.
  - a) Dans **Nom du profil**, sélectionnez le profil dans la liste déroulante. Citrix ADM utilise le mot de passe contenu dans ce profil pour configurer de nouvelles instances Citrix ADC VPX provisionnées automatiquement.
  - b) Cliquez sur **OK**.



4. Pour provisionner la plate-forme Citrix ADC SDX dans OpenStack, accédez à **Orchestration > Cloud Orchestration > OpenStack > Service Package**.
  - a) Cliquez sur **Ajouter** pour créer un nouveau service package.
  - b) Entrez le nom du package de services.
  - c) Dans le champ **Allocation d'instance Citrix ADC**, sélectionnez **Dédié**.
  - d) Dans le champ **Citrix ADC Instance Provisioning**, sélectionnez **Create Instance OnDemand** et dans le champ **Auto Provisioning Platform**, sélectionnez **Citrix ADC SDX**.
  - e) Par défaut, seules les instances Citrix ADC VPX sont provisionnées sur la plate-forme SDX Citrix ADC.
  - f) Cliquez sur **Continuer**.
  - g) Dans la section **Paramètres de mise en service automatique**, définissez les propriétés **des ressources**.
    - i. Champ de **débit**. Entrez 1000 Mbps.
    - ii. Champ **Version de Citrix ADC**. Dans la liste, sélectionnez la bonne version de l'image Citrix ADC VPX présente sur la plate-forme Citrix ADC SDX. [Configurer LBaaS V2 à l'aide de la ligne de commande](#)
  - h) Dans la section **Plates-formes SDX Citrix ADC**, cliquez sur **Ajouter** pour ajouter la plate-forme SDX au service package.
  - i) Cliquez sur **Continuer**.
  - j) Dans la section **Configurer les locataires d'OpenStack**, cliquez sur **Ajouter** pour ajouter les locataires. Vous pouvez également ajouter de nouveaux locataires en cliquant sur **Nouveau**.
  - k) Cliquez sur **Terminé**.
5. Les implémentations de l'API LBaaS V2 sont effectuées à l'aide de commandes LBaaS Neutron. Connectez-vous à n'importe quel client Neutron et exécutez les tâches de configuration. Pour plus d'informations sur l'exécution des commandes de configuration, voir [Configuration de LBaaS V2 à l'aide de la ligne de commande](#).

## Configurer LBaaS V1 à l'aide d'Horizon

February 1, 2024

Tom peut désormais se connecter au portail OpenStack Horizon, créer un pool LBaaS et sélectionner un sous-réseau dans lequel se trouvent tous les membres de ce pool. Tom doit ajouter une adresse IP virtuelle (VIP) et attribuer cette adresse VIP au pool qu'il a créé. Tom peut également effectuer cette opération en ligne de commande ou via des API. Les clients externes pour les serveurs de Tom peuvent se connecter à cette adresse VIP, qui est hébergée sur l'Citrix ADC attribué, et Citrix ADC distribue toutes les requêtes aux membres du pool sur les ports configurés.

Les membres du pool LBaaS sont les serveurs équilibrés de charge qui sont ajoutés au pool sélectionné. Tom peut attribuer un poids et un port à chacun de ces membres.

Les moniteurs de santé sont utilisés pour surveiller la santé et le bon fonctionnement de tous les membres du pool. Tom peut créer un modèle de surveillance de l'état de santé dans OpenStack en spécifiant les limites de délai, de délai d'expiration et de nouvelle tentative, ainsi qu'en spécifiant la méthode, le chemin de l'URL et les codes HTTP attendus en cas de succès. Après avoir créé un moniteur, Tom doit associer le moniteur au pool précédemment créé.

Pour plus d'informations sur la façon de créer des pools et d'autres tâches de configuration LBaaS dans OpenStack, consultez la [documentation OpenStack](#).

#### **Important**

LBaaS V1 n'est pas pris en charge dans la version Liberty d'OpenStack. Pour plus d'informations, consultez les [notes de version d'OpenStack](#).

## **Configurer LBaaS V2 à l'aide de la ligne de commande**

February 1, 2024

LBaaS V2 prend en charge le téléchargement SSL avec les certificats gérés par Barbican, les lots de certificats (y compris les autorités de certification intermédiaires), la prise en charge SNI ainsi que les fonctions régulières d'équilibrage de charge. LBaaS V2 ne prend en charge que l'interface de ligne de commande pour exécuter des tâches de configuration. Les implémentations de l'API LBaaS V2 sont effectuées à l'aide de commandes LBaaS Neutron.

#### **Remarque**

Téléchargez le certificat et la clé du service Barbican lorsque vous avez besoin d'une fonctionnalité de téléchargement SSL. Effectuez les étapes 1, 2 et 3 si le téléchargement SSL est pris en charge, sinon continuez à partir de l'[étape 4](#) pour créer un équilibreur de charge, un écouteur, un pool et un membre.

1. Téléchargez le certificat vers le service Barbican à l'aide de la commande suivante :

barbican secret store --payload-content-type <content\_type> --name <certificate\_name> --payload<certificate\_location>

**Exemple :** barbican secret store --payload-content-type='text/plain' --name='hp\_server\_certificate' --payload='hp\_server/tmp/server\_certificate'

```
stack@ubuntu:/opt/stack/devstack$ barbican secret store --payload-content-type='text/plain' --name='server-cert5' --payload="$(cat /tmp/server_certificate)"
Starting new HTTP connection (1): 10.106.43.15
Starting new HTTP connection (1): 10.106.43.15
-----
| Field      | Value
|-----|-----|
| Secret href | http://localhost:9311/v1/secrets/e364fa82-87ef4-4873-9efe-55108875ef58
| Name        | server-cert5
| Created     | None
| Status      | None
| Content types | (u'default': u'text/plain')
| Algorithm   | aes
| Bit length  | 256
| Secret type | opaque
| Mode        | cbc
| Expiration  | None
|-----|-----|
stack@ubuntu:/opt/stack/devstack$
```

2. Télécharger la touche vers le service Barbican à l'aide de la commande suivante :

magasin secret barbican --payload-content-type <content\_type> --name <key\_name> --payload <key\_location>

**Exemple :** barbican secret store --payload-content-type='text/plain' --name='shp\_server\_key' --payload='hp-server/tmp/server\_key'

```
stack@ubuntu:/opt/stack/devstack$ barbican secret store --payload-content-type='text/plain' --name='server-key5' --payload="$(cat /tmp/server_key5)"
Starting new HTTP connection (1): 10.106.43.15
Starting new HTTP connection (1): 10.106.43.15
-----
| Field      | Value
|-----|-----|
| Secret href | http://localhost:9311/v1/secrets/1b9e1a93-2aeb-4101-8002-e52acab987b0
| Name        | server-key5
| Created     | None
| Status      | None
| Content types | (u'default': u'text/plain')
| Algorithm   | aes
| Bit length  | 256
| Secret type | opaque
| Mode        | cbc
| Expiration  | None
|-----|-----|
stack@ubuntu:/opt/stack/devstack$
```

**Remarque**

Lorsque vous exécutez ces deux commandes Barbican pour charger le certificat et la clé, les champs href Secret fournissent un emplacement ou une URL. C'est là que le certificat et la clé sont stockés sur le système sur lequel OpenStack est installé. Copiez ces liens et fournissez ces liens en tant que paramètres lorsque vous créez le conteneur sur le service Barbican à l'étape 3.

3. Créez un conteneur dans le service Barbican pour stocker le certificat et la clé à l'aide de la commande suivante :

Dans la commande, remplacez <certificate\_url> par l'URL que vous avez obtenue à partir du champ secret href lorsque vous avez téléchargé le certificat. De même, remplacez <key\_url> par l'URL que vous avez obtenue à partir du champ secret href lorsque vous avez téléchargé la clé.

barbican secret container create --name<container\_name> --type<container\_type> --secret<certificate\_url> --secret<key\_url>

**Example:** barbican secret container create --name='hp\_container' --type='certificate' --secret='certificate=http://localhost:9311/v1/secrets/e36a4a82-87e4-4873-9efe-55108875ef58 --secret="private\_key=http://localhost:9311/v1/secrets/1b9e1a93-2aeb-4101-8002-e52acab987b0"

```
stack@ubuntu:/opt/stack/devstack$ barbican secret container create --name='hp_container' --type='certificate' --secret='certificate=http://localhost:9311/v1/secrets/e36a4a82-87e4-4873-9efe-55108875ef58' --secret="private_key=http://localhost:9311/v1/secrets/1b9e1a93-2aeb-4101-8002-e52acab987b0"
Starting new HTTP connection (1): 10.106.43.15
Starting new HTTP connection (1): 10.106.43.15
Starting new HTTP connection (1): localhost
-----
| Field | Value |
-----
| Container href | http://localhost:9311/v1/containers/d688676f-c256-4a0d-b84d-a310419dc0aa |
| Name | hp_container |
| Created | None |
| Status | ACTIVE |
| Type | certificate |
| Certificate | http://localhost:9311/v1/secrets/e36a4a82-87e4-4873-9efe-55108875ef58 |
| Intermediates | None |
| Private Key | http://localhost:9311/v1/secrets/1b9e1a93-2aeb-4101-8002-e52acab987b0 |
| PK Passphrase | None |
| Consumers | None |
-----
stack@ubuntu:/opt/stack/devstack$
```

Copiez la valeur href du conteneur. Vous devez fournir le lien vers le conteneur lors de la création de l'écouteur à l'étape 6.

4. Définissez les variables d'environnement dans OpenStack. Les variables permettent aux commandes du client OpenStack de communiquer avec les services OpenStack.

**Exemple :**

```
export OS_PASSWORD=hp
export OS_AUTH_URL=http://10.106.43.15:35357/v2.0/
export OS_USERNAME=hp_user
export OS_TENANT_NAME=hp
export OS_IDENTITY_API_VERSION=2.0
export BARBICAN_ENDPOINT="http://10.106.43.15:9311/"
```

```
stack@ubuntu:/opt/stack/devstack$ export OS_PASSWORD=hp
stack@ubuntu:/opt/stack/devstack$ export OS_AUTH_URL=http://10.106.43.15:35357/v2.0/
stack@ubuntu:/opt/stack/devstack$ export OS_USERNAME=hp_user
stack@ubuntu:/opt/stack/devstack$ export OS_TENANT_NAME=hp
stack@ubuntu:/opt/stack/devstack$ export OS_IDENTITY_API_VERSION=2.0
stack@ubuntu:/opt/stack/devstack$ export BARBICAN_ENDPOINT="http://10.106.43.15:9311/"
stack@ubuntu:/opt/stack/devstack$
```

**Remarque**

Définissez ces variables pour chaque session SSH avant d'exécuter d'autres commandes. Pour plus d'informations sur les variables d'environnement OpenStack, consultez [Variables d'environnement OpenStack](#).

5. Créez un équilibreur de charge à l'aide de la commande suivante :

neutron lbaas-loadbalancer-create --name <loadbalancer-name> <subnet-name> --provider <netscaler>

**Exemple :** neutron lbaas-loadbalancer-create --name hp-lb-test hp-sub1 --provider netscaler

```
stack@ubuntu:/opt/stack/devstack$ neutron lbaas-loadbalancer-create --name hp-lb-test hp-sub1 --provider netscaler
Created a new loadbalancer:
+-----+
| Field | Value |
+-----+
| admin_state_up | True |
| description | |
| id | 746d730b-3b63-418f-a816-d8dd5472963c |
| listeners | |
| name | hp-lb-test |
| operating_status | OFFLINE |
| provider | netscaler |
| provisioning_status | PENDING_CREATE |
| tenant_id | 0f30b93cd0cd4482b92d033e1628aa8f |
| vip_address | 15.0.0.27 |
| vip_port_id | 36636748-15c1-4ec3-9328-496ee74e64fc |
| vip_subnet_id | 0bb433c4-4b90-4de0-803f-9df92aa46ac4 |
+-----+
stack@ubuntu:/opt/stack/devstack$
```

L'état passe de PENDING\_CREATE à ACTIVE après la création de l'équilibreur de charge.

```
+-----+
| id | name | vip_address | provisioning_status | provider |
+-----+
| 0d5e8e17-41c2-41bb-aab5-2b3f8f5af4c5 | hp-lb8 | 15.0.0.25 | ACTIVE | netscaler |
| 1092f752-aa25-4262-aacc-014725fe2921 | hp_lb3 | 15.0.0.19 | ACTIVE | netscaler |
| 41dbe490-6d9c-4ce5-8d88-bb55953f5961 | hp-lb7 | 15.0.0.24 | ACTIVE | netscaler |
| 746d730b-3b63-418f-a816-d8dd5472963c | hp-lb-test | 15.0.0.27 | ACTIVE | netscaler |
| 9d65f6a4-5be5-44fd-a4bd-0808084557b0 | hp-lb1 | 15.0.0.18 | ACTIVE | netscaler |
| cf8ee4b7-a9f5-41c5-a76a-cd2520e0a7a3 | hp-lb6 | 15.0.0.23 | ACTIVE | netscaler |
| f7f7dd6e-28eb-40f2-b26c-e541138c6a06 | hp-lb4 | 15.0.0.20 | ERROR | netscaler |
+-----+
```

6. Créez un processus d'écoute à l'aide de la commande suivante :

neutron lbaas-listener-create --loadbalancer <loadbalancer-name> --name <listener-name> --protocol <protocol\_type> --protocol-port <port\_number> --default-tls-container-id <container\_url>

**Exemple :** neutron lbaas-listener-create --name hp-lb-test-list --loadbalancer hp-lb-test --protocol TERMINATED\_HTTPS --protocol-port 443 --default-tls-container-id http://10.106.43.15:9311/v1/containers/d688676f-c256-4a0d-b84d-a310419dc0aa

**Remarque**

Si vous créez un écouteur sans prise en charge du déchargement SSL, exécutez la commande suivante sans fournir d'emplacements au conteneur :

neutron lbaas-listener-create --loadbalancer <loadbalancer-name> --name <listener-name> --protocol <protocol\_type> --protocol-port <port\_number>

```
stack@ubuntu:/opt/stack/devstack$ neutron lbaas-listener-create --name hp-lb-test-list --loadbalancer hp-lb-test --protocol TERMINATED_HTTPS --protocol-port 443 --default-tls-container-id http://10.106.43.15:9311/v1/containers/d688676f-c256-4a0d-b84d-a310419dc0aa
Created a new listener:
-----
| Field | Value |
-----+-----+-----
| admin_state_up | True |
| connection_limit | -1 |
| default_pool_id | |
| default_tls_container_id | http://10.106.43.15:9311/v1/containers/d688676f-c256-4a0d-b84d-a310419dc0aa |
| description | |
| id | 734a0361-153d-4983-bc2c-55a3ec2ff6fb |
| loadbalancers | [{"id": "746d730b-3b63-418f-a816-d8dd5472963c"}] |
| name | hp-lb-test-list |
| protocol | TERMINATED_HTTPS |
| protocol_port | 443 |
| sni_container_ids | |
| tenant_id | 0f30b93cd0cd4482b92d033e1628aa8f |
-----
stack@ubuntu:/opt/stack/devstack$
```

7. Créez un pool à l'aide de la commande suivante :

`neutron lbaas-pool-create --lb-algorithm <algorithm_type> --listener <listener-name> --protocol <protocol_type> --name <pool-name>`

**Exemple** : `neutron lbaas-pool-create --lb-algorithm LEAST_CONNECTIONS --listener demolis-tener --protocol http --name demopool`

```
stack@ubuntu:/opt/stack/devstack$ neutron lbaas-pool-create --lb-algorithm ROUND_ROBIN --listener hp-lb-test-list --protocol HTTP --name hp-lb-test-pool
Created a new pool:
-----
| Field | Value |
-----+-----+-----
| admin_state_up | True |
| description | |
| healthmonitor_id | |
| id | 714c44d0-5cf7-4ef8-b84d-f6d3a258c770 |
| lb_algorithm | ROUND_ROBIN |
| listeners | [{"id": "734a0361-153d-4983-bc2c-55a3ec2ff6fb"}] |
| members | |
| name | hp-lb-test-pool |
| protocol | HTTP |
| session_persistence | |
| tenant_id | 0f30b93cd0cd4482b92d033e1628aa8f |
-----
stack@ubuntu:/opt/stack/devstack$
```

8. Créez un membre à l'aide de la commande suivante :

`neutron lbaas-member-create --subnet <subnet-name> --address <ip-address of the web server> --protocol-port <port_number> <pool-name>`

**Exemple** : `neutron lbaas-member-create --subnet hp-sub1 --address 15.0.0.15 --protocol-port 80 hp-lb-test-pool`

```
stack@ubuntu:/opt/stack/devstack$ neutron lbaas-member-create --subnet hp-sub1 --address 15.0.0.15 --protocol-port 80 hp-lb-test-pool
Created a new member:
-----
| Field | Value |
-----+-----+-----
| address | 15.0.0.15 |
| admin_state_up | True |
| id | ced7a563-5ecc-474f-8d2a-cb69923215b0 |
| protocol_port | 80 |
| subnet_id | 0bb433c4-4b90-4de0-803f-9df92aa46ac4 |
| tenant_id | 0f30b93cd0cd4482b92d033e1628aa8f |
| weight | 1 |
-----
stack@ubuntu:/opt/stack/devstack$
```

## Surveillance des applications OpenStack dans Citrix ADM

Vos locataires peuvent se connecter à Citrix Application Delivery Management (ADM) à l'aide de leurs informations d'identification OpenStack pour surveiller les VIP et les pools créés à partir d'OpenStack à partir de n'importe quel navigateur. L'URL doit être au format suivant :

`http://<mas\_ip>/<admin\_ui>/mas/ent/html/cc/<tenant\_main.html`

Où <mas-ip-address>, est l'adresse IP Citrix ADM qui est enregistrée avec OpenStack.

#### Remarque

- Les VIP OpenStack correspondent aux serveurs virtuels dans Citrix ADM.
- Les pools OpenStack correspondent aux groupes de services dans Citrix ADM.
- Les membres du pool OpenStack correspondent aux membres du groupe de services dans Citrix ADM.

## Configurer la commutation de contenu de couche 7

February 1, 2024

Citrix Application Delivery Management (ADM) orchestre avec OpenStack pour configurer les fonctionnalités de commutation de couche 7 (L7) ou de commutation basée sur le contenu sur des instances Citrix ADC. La commutation de contenu diffère du simple équilibrage de charge en ce sens que des types spécifiques de requêtes peuvent être dirigés vers des serveurs spécifiques. Lorsque les configurations L7 sont créées dans OpenStack avec une instance Citrix ADC en tant que fournisseur, Citrix ADM affecte une instance Citrix ADC et déploie des configurations de commutation de contenu et de répondeur correspondant aux configurations L7. Les instances de Citrix ADC peuvent ensuite distribuer et équilibrer la charge des demandes utilisateur en fonction des caractéristiques de couche applicative des demandes.

La fonction d'équilibrage de charge de la couche 7 (L7) d'OpenStack combine l'équilibrage de charge et la commutation de contenu pour optimiser la diffusion de types spécifiques de contenu. Cela améliore les performances de l'équilibreur de charge en exécutant uniquement les stratégies applicables au contenu. L'équilibrage de charge de couche 7 facilite également l'efficacité de l'infrastructure applicative. La possibilité de séparer le contenu en fonction du type, de l'URI ou des données permet une meilleure allocation des ressources physiques dans l'infrastructure applicative. Par exemple, un utilisateur final naviguant vers `http://example-sports.com/about-us` doit être servi par un pool de serveurs hébergeant du contenu sur l'entreprise et les services, tandis qu'un utilisateur naviguant vers `http://example-sports.com/shopping-cart-football` doit être servi par un pool différent de serveurs qui permet aux utilisateurs de faire des achats en ligne.

Dans la commutation L7, un équilibreur de charge est implémenté en tant que serveur virtuel de commutation de contenu qui accepte les requêtes HTTP des utilisateurs et les distribue aux serveurs d'applications. La commutation L7 ou la commutation de contenu vous permet de disposer d'un point

d'entrée unique pour accéder à divers services dorsaux (par exemple, non seulement aux applications Web, aux portails de services Web, aux courriers électroniques, mais également à la gestion mobile, au contenu dans différentes langues, etc.). En d'autres termes, vous pouvez fournir une adresse IP publique pour tous les services que vous offrez à vos utilisateurs.

Contrairement à l'équilibrage de charge de niveau inférieur, la commutation de couche 7 ne nécessite pas que tous les serveurs du pool disposent du même contenu. Une configuration d'équilibreur de charge utilisant la commutation L7 s'attend à ce que les applications ou les serveurs principaux de différents pools aient un contenu différent. Les commutateurs L7 peuvent diriger les requêtes sur la base de l'URI, de l'hôte, des en-têtes HTTP ou tout autre élément du message de l'application. Les serveurs d'applications doivent essentiellement servir des types de contenu spécifiques. Par exemple, un serveur peut servir uniquement des images, un autre peut exécuter des langages de script côté serveur, tels que PHP et ASP, et un autre peut servir du contenu statique tel que HTML, CSS et JavaScript.

## Règles L7

Les attributs suivants sont définis dans une règle pour évaluer le trafic et sont comparés aux valeurs définies dans la règle :

- **hostname** : Le nom d'hôte dans la requête HTTP est comparé au paramètre value dans la règle. Par exemple, « www.example-sports.com ».
- **chemin** : la partie chemin de l'URI HTTP est comparée au paramètre value de la règle. Par exemple, « www.example-sports.com/shopping-cart/football\_pump.html »
- **file\_type** : la dernière partie de l'URI est comparée au paramètre value de la règle. Par exemple, txt, html, jpg, png, xls, et d'autres.
- **header** : l'en-tête défini dans le paramètre clé est comparé au paramètre value de la règle.
- **cookie** : le cookie nommé par le paramètre clé est comparé au paramètre value de la règle. La valeur du champ d'en-tête de demande de cookie contient une paire nom/valeur d'informations stockées pour cette URL ; la syntaxe générale est la suivante : Cookie : nom=valeur. Par exemple, une règle qui recherche un cookie nommé « stores » dont la valeur commence par « football- » ressemblera à ceci : type = Cookie, compare\_type=startsWith, key = stores value = football-.

## Types de comparaison

Lors de l'évaluation du trafic, la stratégie L7 compare les expressions suivantes aux attributs définis dans la règle.



- `regex` : correspondance d'expressions régulières de type Perl
- `starts_with` : chaîne commençant par
- `ends_with` : La chaîne se termine par
- `contains` : La chaîne contient
- `equal_to` : Chaîne égale à

#### Remarque

Les attributs `hostname`, `path`, `header` et `cookie` prennent en charge tous les types de comparaison, mais l'attribut `file_type` prend uniquement en charge `regex` et `equal_to`.

## Stratégies L7

Une stratégie L7 traite le trafic HTTP entrant et renvoie une valeur « vraie » lorsque toutes les règles définies dans la stratégie sont respectées.

Dans toute stratégie L7, toutes les règles sont logiquement associées à un opérateur AND. Une demande doit respecter toutes les règles pour que la stratégie renvoie une valeur « vraie ». L'action entreprise par l'équilibreur de charge est basée sur la valeur renvoyée par la stratégie. Vous pouvez créer une deuxième stratégie avec la même action pour réaliser une opération OR logique entre les règles.

Par exemple, vous pouvez créer une stratégie dans laquelle la requête HTTP entrante peut contenir les mots « EXAMPLE-SPORTS », « SPORTS-FOOTBALL » ou « EXAMPLE-FOOTBALL », afin que l'équilibreur de charge prenne les mesures appropriées pour transmettre ces demandes au pool de serveurs de la société de commerce électronique Example-Sports pour diffuser le contenu demandé. Vous pouvez créer une autre stratégie qui prend la même action, mais qui correspond à « exemple sport », « exemple sports-football » ou « exemple football. » Lorsqu'un utilisateur envoie une requête HTTP avec l'un de ces six mots clés, l'équilibreur de charge transmet la demande au serveur Example-Sports.

Selon les règles définies dans la stratégie, une stratégie L7 peut effectuer l'une des actions suivantes :

- Rediriger vers le pool : transmettez la demande au pool de serveurs d'applications identifié par les règles associées à la stratégie L7. En d'autres termes, vous pouvez créer une règle d'application pour diriger les demandes vers un pool d'équilibreurs de charge spécifique en fonction du nom de domaine. Par exemple, vous pouvez créer une règle qui dirige certaines demandes vers `example-football.com` vers `pool_1`, et d'autres demandes vers `example-sports-online_purchase.com` vers `pool_2`.
- Redirection vers une URL : envoyez au client une réponse HTTP de redirection dans laquelle l'en-tête de la réponse de localisation contient le nouvel emplacement. Le navigateur mettra

à jour la barre d'adresse avec le nouvel emplacement et émettra une nouvelle demande. Les cas d'utilisation sont nombreux. Par exemple, si l'adresse d'un site Web a changé, vous pouvez rediriger les demandes vers la nouvelle adresse au lieu de les supprimer. Ou, pendant la maintenance du site Web, vous pouvez rediriger les utilisateurs vers un site en lecture seule.

- Rejeter - Rejette la demande et n'effectue aucune autre action. Par exemple, vous pouvez renvoyer une réponse 401 non autorisée pour refuser l'accès aux utilisateurs pour les pages Web restreintes.

Une configuration de commutation de contenu se compose d'un serveur virtuel de commutation de contenu, d'une configuration d'équilibrage de charge consistant en serveurs et services virtuels d'équilibrage de charge, et de stratégies de commutation de contenu. Après avoir créé votre serveur virtuel de commutation de contenu et vos stratégies, vous liez chaque stratégie au serveur virtuel de commutation de contenu. Lorsque vous liez la stratégie au serveur virtuel de commutation de contenu, vous spécifiez le serveur virtuel d'équilibrage de charge cible. Lorsqu'une demande atteint le serveur virtuel de commutation de contenu, le serveur virtuel applique les stratégies de commutation de contenu associées à cette demande. La priorité de la stratégie définit l'ordre dans lequel les stratégies liées au serveur virtuel de commutation de contenu sont évaluées.

Tout pool doté de l'ID d'écouteur peut être affecté en tant que pool par défaut de serveurs virtuels vers lesquels le trafic est redirigé. Le pool est étroitement lié à un écouteur et n'est associé à un auditeur que par la mise en œuvre d'une stratégie L7. Un pool peut également être créé directement sous un équilibreur de charge sans nécessairement être lié à un auditeur. Dans ce cas, le pool est créé dans un état « pending\_create ». Les stratégies L7 étant étroitement liées aux auditeurs, une stratégie L7 contenant l'ID du pool doit être créée et mise en œuvre pour que le pool devienne « actif » et commence à recevoir des demandes de trafic.

Un pool peut être desservi par plusieurs stratégies L7, mais il reste dans l'état « actif » si au moins une stratégie y est attachée. Lorsque la dernière stratégie est supprimée, le pool revient à l'état « pending\_create » jusqu'à ce qu'une autre stratégie soit créée et associée à celle-ci. Si le pool lui-même est supprimé, toutes les requêtes HTTP qu'il aurait reçues autrement sont redirigées vers le pool par défaut.

### **Mappage entre les stratégies OpenStack L7 et les entités Citrix ADC**

---

OpenStack	Entité Citrix ADC	Description
-----------	-------------------	-------------

Stratégie L7 avec action REDIRECT_TO_POOL	Stratégie de commutation de contenu > Action de commutation de contenu	Citrix ADM crée une stratégie de commutation de contenu liée au serveur virtuel de commutation de contenu et associée à une action de commutation de contenu spécifiant le pool cible de serveurs d'applications pour la récupération de contenu et la présentation à l'utilisateur.
Stratégie L7 avec action REDIRECT_TO_URL	Stratégie du répondeur > Action du répondeur	Citrix ADM crée une stratégie de répondeur liée au serveur virtuel de commutation de contenu et associée à une action de répondeur qui spécifie l'URL cible à présenter aux utilisateurs.
Stratégie L7 avec action REJECT	Stratégie de répondeur > Supprimer la demande	Citrix ADM crée une stratégie de répondeur liée au serveur virtuel de commutation de contenu et associée à une action de répondeur qui supprime la demande.

Si l'action d'une stratégie L7 qui évalue « true » redirige le trafic vers un pool qui est à l'état « create\_pending », Citrix ADM implémente le pool spécifié avec un serveur virtuel d'équilibrage de charge. Citrix ADM crée une stratégie de commutation de contenu à partir de la stratégie L7 et utilise l'action de commutation de contenu correspondante pour rediriger les demandes vers le serveur virtuel d'équilibrage de charge associé à ce pool. Si une seconde stratégie L7 redirige vers le même pool, Citrix ADM crée une stratégie de commutation de contenu et une action de commutation de contenu pour rediriger le trafic vers le serveur virtuel d'équilibrage de charge existant associé au pool.

### Positionnement des stratégies

L'évaluation des stratégies L7 dans OpenStack est déterminée par leurs priorités. Dans OpenStack, par défaut, les stratégies se voient attribuer des priorités dans l'ordre dans lequel elles sont créées. La stratégie créée en premier est numérotée « 1 », et les stratégies créées par la suite sont numérotées

consécutivement. Vous pouvez toutefois modifier les priorités des stratégies et leur attribuer des priorités différentes. Les stratégies sont toujours évaluées dans l'ordre de leurs priorités. La première stratégie qui correspond à une demande spécifique est toujours exécutée en premier.

Lors de la création de stratégies, notez les points suivants :

- Si vous attribuez à une nouvelle stratégie la même priorité qu'une stratégie existante, la nouvelle stratégie prend cette priorité. La priorité de la stratégie existante est abaissée. Si nécessaire, les priorités des autres stratégies sont également abaissées afin de conserver l'ordre dans lequel les stratégies sont évaluées.
- Si vous créez une nouvelle stratégie sans spécifier de poste, la nouvelle stratégie sera simplement ajoutée à la liste.
- Si vous créez une nouvelle stratégie et que vous lui attribuez une position supérieure au nombre de stratégies figurant déjà dans la liste, la nouvelle stratégie sera ajoutée à la liste, c'est-à-dire qu'elle aura toujours la priorité disponible suivante. Par exemple, s'il existe trois stratégies A, B et C avec les priorités 1, 2 et 3, et si vous créez une stratégie et que vous attribuez une priorité de 8, la priorité de la nouvelle stratégie devient 4.
- Si vous ajoutez une stratégie à la liste ou si vous supprimez une stratégie de la liste, les valeurs de position de la stratégie sont réorganisées à partir de 1 sans omettre de chiffres. Par exemple, si la stratégie A, B, C et D a des valeurs de position de 1, 2, 3 et 4 et si vous supprimez la stratégie B de la liste, la stratégie C prend désormais la deuxième position et la stratégie D prend la troisième position.

Dans Citrix ADM, il existe toujours une stratégie par défaut associée à un serveur csvserver avec une priorité de 1. Cette stratégie par défaut spécifie le nombre de connexions TCP qu'un serveur lbvserver doit traiter à un moment donné. Par conséquent, lorsque les stratégies de répondeur et les stratégies de commutation de contenu correspondantes sont créées dans Citrix ADC, elles reçoivent toujours une priorité 1 supérieure à la priorité de la stratégie L7 correspondante. Par exemple, lorsqu'une stratégie L7 avec une priorité de 1 est évaluée et qu'une stratégie de commutation de contenu est créée avec une priorité de 2. De même, lorsqu'une stratégie L7 avec une priorité de 2 est évaluée et qu'une stratégie de réponse est créée avec une priorité de 3.

Dans OpenStack, les stratégies « rejet » et/ou « redirect\_to\_url » sont d'abord évaluées, puis la stratégie « redirect\_to\_pool » est évaluée. Dans une instance de Citrix ADC, les stratégies de répondeur sont toujours évaluées en premier pour supprimer la demande ou présenter à l'utilisateur une adresse Web redirigée, et les stratégies de commutation de contenu sont évaluées en dernier. Cet ordre d'évaluation ne provoque généralement aucun conflit si les stratégies de changement de contenu et de réponse s'excluent mutuellement. Autrement dit, deux stratégies L7 ne devraient pas avoir d'expressions identiques. Les expressions dérivées doivent être ajoutées dans les stratégies de changement de réponse et de contenu afin d'éviter de tels conflits. Par exemple, écrivez une expression pour rejeter toutes les demandes sur "sports-football.com" et une autre expression pour

autoriser les requêtes à “example-sports-football.com.” Créez les stratégies L7 de sorte que toutes les stratégies de réponse pour rejeter la demande soient organisées en haut de la liste d'évaluation, suivies des stratégies de réponse pour le web direct, suivies des stratégies de changement de contenu.

Dans Citrix ADM, il existe toujours une stratégie par défaut associée à un serveur csvserver avec une priorité de 1. Cette stratégie par défaut spécifie le nombre de connexions TCP qu'un serveur lbvserver doit traiter à un moment donné. Par conséquent, lorsque les stratégies de répondeur et les stratégies de commutation de contenu correspondantes sont créées dans Citrix ADC, elles reçoivent toujours une priorité 1 supérieure à la priorité de la stratégie L7 correspondante. Par exemple, lorsqu'une stratégie L7 avec une priorité de 1 est évaluée et qu'une stratégie de commutation de contenu est créée avec une priorité de 2. De même, lorsqu'une stratégie L7 avec une priorité de 2 est évaluée et qu'une stratégie de réponse est créée avec une priorité de 3.

Dans OpenStack, les stratégies « rejet » et/ou « redirect\_to\_url » sont d'abord évaluées, puis la stratégie « redirect\_to\_pool » est évaluée. Dans Citrix ADC, les stratégies de réponse sont toujours évaluées en premier pour supprimer la demande ou présenter à l'utilisateur une adresse Web redirigée, et les stratégies de commutation de contenu sont évaluées en dernier. Cet ordre d'évaluation ne provoque généralement aucun conflit si les stratégies de changement de contenu et de réponse s'excluent mutuellement. Autrement dit, deux stratégies L7 ne devraient pas avoir d'expressions similaires. Des expressions dérivées similaires doivent être ajoutées dans les stratégies de changement de réponse et de contenu afin d'éviter de tels conflits. Par exemple, écrivez une expression pour rejeter toutes les demandes sur “sports-football.com” et une autre expression pour autoriser les requêtes à “example-sports-football.com.” Créez les stratégies L7 de sorte que toutes les stratégies de réponse pour rejeter la demande soient organisées en haut de la liste d'évaluation, suivies des stratégies de réponse pour le web direct, suivies des stratégies de changement de contenu.

## Tâches de configuration

Les implémentations de la stratégie et des actions L7 sont effectuées via les commandes Neutron LBaaS.

Définissez les variables d'environnement dans OpenStack et créez l'équilibreur de charge (par exemple, LB1). Une fois l'équilibreur de charge correctement créé, créez le module d'écoute et les pools (par exemple, L1, P1 et P2), puis ajoutez des membres et des moniteurs aux pools. Par exemple, P1 est le pool par défaut pour L1, tandis que P2 est le pool lié à LB1 et gérant les serveurs d'applications.

Pour plus d'informations sur la façon de configurer LBaaS V2 à l'aide de la ligne de commande, consultez [Configuration de LBaaS V2 à l'aide de la ligne de commande](#).

Les commandes suivantes créent les stratégies et définissent les actions spécifiques :

**Créer une stratégie L7 pour supprimer les demandes**

```
1 neutron lbaas-l7policy-create --name <L7 policy name> --listener <
  listener name> --action<action-name>
```

**Exemple :**

```
neutron lbaas-l7policy-create --name policy11 --action REJECT --listener L1
```

La commande ci-dessus crée et lie policy11, une stratégie de répondeur, au serveur de commutation de contenu pour rejeter les demandes. Aucune règle n'ayant été créée pour cette stratégie, celle-ci est considérée comme « fausse » et la demande est rejetée.

**Créer une stratégie L7 pour rediriger les demandes vers une URL particulière**

```
1 neutron lbaas-l7policy-create --name <L7 policy name> --listener <
  listener name> --action <action-name> --redirect-url <redirect-url>
```

**Exemple :**

```
neutron lbaas-l7policy-create --name policy12 --action REDIRECT_TO_URL --listener admin-list1 --
  redirect-url http://example-sports/about-us.html
```

La commande ci-dessus crée une action de répondeur pour rediriger les demandes vers une URL, crée une stratégie de répondeur avec action et lie cette stratégie au serveur virtuel de commutation de contenu.

```
1 neutron lbaas-l7rule-create --type HOST_NAME --compare-type CONTAINS --
  value <value-string> <L7 policy name>
2
3 neutron lbaas-l7rule-create --type PATH --compare-type CONTAINS --value
  <value-string> <L7 policy name>
```

Les deux règles ci-dessus peuvent être connectées à un opérateur AND pour dériver l'expression de la stratégie de répondeur.

**Créer une stratégie L7 pour rediriger les demandes vers un pool**

```
1 neutron lbaas-l7policy-create --name <L7 policy name> --listener <
  listener name> --action <action-name> --redirect-pool <redirect-pool
  >
```

**Exemple :**

```
neutron lbaas-l7policy-create --name policy13 --action REDIRECT_TO_POOL --listener admin-list1 --
  redirect-pool admin-pool2
```

S'il s'agit de la première stratégie L7, la commande ci-dessus implémente P2 en même temps que LB1, crée l'action de redirection de commutation de contenu et redirige les demandes vers LB1. Si P2 existe déjà, la commande crée l'action de redirection de commutation de contenu et redirige les requêtes vers LB1.

## Provisioning manuel de l'instance Citrix ADC VPX sur OpenStack

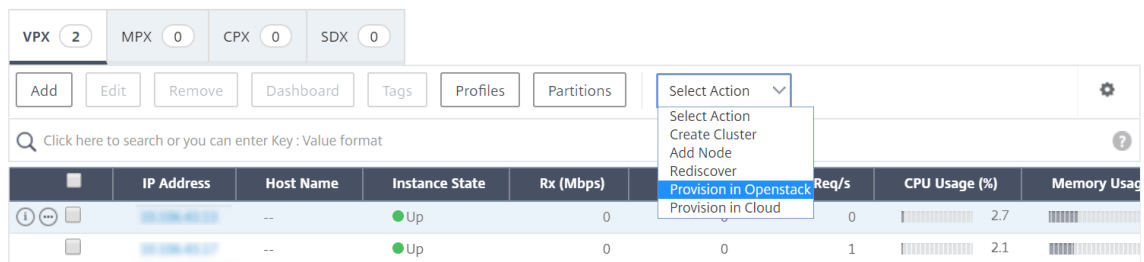
February 1, 2024

Dans quelques réseaux d'entreprise, les instances Citrix ADC VPX ne peuvent pas se connecter au serveur de licences Citrix pour télécharger automatiquement les licences, pour des raisons de sécurité. Dans un tel scénario, vous devez déployer manuellement des instances Citrix ADC VPX sur la plate-forme OpenStack. À l'aide du code d'activation de licence (LAC) que vous avez reçu de Citrix, téléchargez la licence Citrix ADC VPX appropriée et enregistrez-la sur votre système local.

### Pour provisionner manuellement une instance Citrix ADC VPX sur OpenStack :

1. Installez le logiciel de pilote Citrix ADC et enregistrez Citrix Application Delivery Management (ADM) sur OpenStack
  - a) Dans Citrix ADM, accédez à **Orchestration > Cloud Orchestration > OpenStack**.
  - b) Cliquez sur **Configurer les paramètres OpenStack**. Dans la page **Configurer les paramètres OpenStack**, vous pouvez définir les paramètres pour configurer OpenStack dans Citrix ADM. Vous avez deux options ici : par **défaut** et **Personnalisé**.
  - c) Sélectionnez **Par défaut**, si les services OpenStack s'exécutent sur les ports par défaut.
2. Accédez à **Orchestration > Cloud Orchestration > OpenStack**, puis cliquez sur **Paramètres de déploiement**.
  - a) **Réseau de gestion** : sélectionnez le réseau de gestion sur OpenStack, auquel le Citrix ADC VPX provisionné automatiquement est connecté.
  - b) **Nom du profil** : sélectionnez le profil dans la liste déroulante. Citrix ADM utilise le mot de passe contenu dans ce profil pour configurer de nouvelles instances Citrix ADC VPX provisionnées automatiquement.
  - c) Citrix ADC VPX Image in Glance : sélectionnez l'image Citrix ADC VPX disponible dans OpenStack Glance qui est utilisée pour créer une instance VPX Citrix ADC. La liste déroulante affiche uniquement les images présentes sur OpenStack Glance.
3. Dans Citrix ADM, accédez à **Orchestration > Cloud Orchestration > OpenStack > Service Packages**, puis cliquez sur **Ajouter**.
4. Dans la page **Service Package**, spécifiez les paramètres suivants :
  - a) **Nom** : nom du package de service. Par exemple, entrez SVC-PKG-GOLD.
  - b) **Allocation d'instance Citrix ADC** - sélectionnez **Dédié** ou **Partitionné** comme type d'allocation d'instance défini dans le package de services.

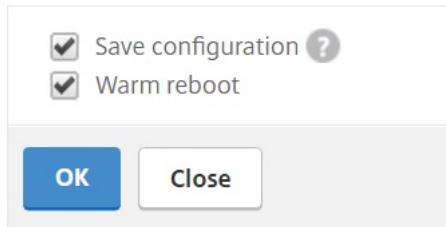
- c) **Citrix ADC Instance Provisioning** : sélectionnez **Create Instance OnDemand** pour créer des instances Citrix ADC lors de la configuration elle-même.
  - d) **Plateforme de provisionnement automatique** - sélectionnez **OpenStack Compute**. Par défaut, Citrix ADC VPX sera sélectionné comme type d'instance.
  - e) **Affecter des locataires OpenStack ou des stratégies de placement**- section, sous Locataires OpenStack, cliquez sur **Ajouter**, puis sélectionnez le locataire.
  - f) Cliquez sur **Continuer**, puis sur **Terminé**.
5. Accédez à **Système > Administration système > Modifier les paramètres système** et sélectionnez **http** dans la liste déroulante.
  6. Accédez à **Réseaux > Instances > Citrix ADC VPX**.
  7. Dans la page **Citrix ADC VPX**, cliquez sur la liste déroulante **Admin** et sélectionnez **Provisionner le périphérique**.



- a) Sur la page **Device Provisioning**, entrez le nom du périphérique et sélectionnez le service package que vous avez créé à l'étape précédente.
  - b) Cliquez sur **OK**.
8. Accédez à l'onglet **Orchestration > Cloud Orchestration > OpenStack > Requêtes**. Sélectionnez la demande et cliquez sur **Tâches** pour afficher les tâches. Lorsque l'état de la tâche devient **Terminé**, cela signifie que le Citrix ADC VPX est provisionné dans Citrix ADM.
  9. Accédez à **Réseaux > Instances > Citrix ADC VPX** pour vérifier que l'instance Citrix ADC VPX s'affiche dans la page Citrix ADC VPX.
  10. Cliquez sur l'instance Citrix ADC VPX. Lorsque l'instance Citrix ADC VPX s'ouvre dans la fenêtre de votre navigateur, connectez-vous à l'instance. Accédez à **Configuration > Système > Licences** et ajoutez manuellement la nouvelle licence. Pour plus d'informations sur la façon d'ajouter une nouvelle licence, consultez [Vue d'ensemble des licences Citrix ADC](#).
  11. Redémarrez l'instance Citrix ADC VPX.



## Reboot

A dialog box titled "Reboot" with two checked options: "Save configuration" (with a help icon) and "Warm reboot". At the bottom, there are two buttons: "OK" (blue) and "Close" (white).

12. Après quelques minutes, vous pouvez vous connecter à OpenStack et dans **System > Instances**, vous pouvez voir que l'instance Citrix ADC VPX est déployée sur OpenStack.
13. Les implémentations de l'API LBaaS V2 sont effectuées à l'aide de commandes LBaaS Neutron. Connectez-vous à n'importe quel client Neutron et exécutez les tâches de configuration. Pour plus d'informations sur l'exécution des commandes de configuration, voir [Configuration de LBaaS V2 à l'aide de la ligne de commande](#).

## Provisionnement de l'instance Citrix ADC VPX sur OpenStack à l'aide de StyleBook

February 1, 2024

Dans le workflow d'orchestration OpenStack, Citrix Application Delivery Management (ADM) utilise désormais le StyleBook « os-cs-lb-mon » pour déployer des configurations LBaaS sur des instances Citrix ADC attribuées au locataire OpenStack. Un pack de configuration est créé pour chaque équilibreur de charge créé par l'utilisateur OpenStack.

L'utilisation de StyleBooks pour la configuration dans le workflow OpenStack offre les avantages suivants :

- Meilleure visualisation en visualisant tous les objets de configuration.
- Fiabilité grâce à la restauration.
- Prise en charge de divers types d'instance Citrix ADC (Citrix ADC HA, partitions, VPX, CPX, MPX et autres).
- Personnalisation à l'aide de vos propres StyleBooks pour déployer la configuration pour les locataires OpenStack.

En tant qu'administrateur Citrix ADM, accédez à **Applications > Configurations** pour afficher le pack de configuration déployé sur l'instance Citrix ADC.

Vous pouvez effectuer les tâches suivantes :

- Faites défiler l'écran pour afficher le pack de configuration « os-cs-lb-mon » déployé pour l'équilibreur de charge.
- Cliquez sur **Afficher la définition** dans le panneau StyleBook « os-cs-lb-mon » pour vérifier la configuration déployée sur les instances.
- Cliquez sur **Afficher l'objet** pour afficher la liste des objets ou entités Citrix ADC déployés sur les instances.

### Points à noter avant de Provisioning des instances à l'aide de StyleBooks

À partir de Citrix ADM 12.1 build 49.23, l'architecture du flux de travail d'orchestration OpenStack a été mise à jour. Le workflow utilise désormais Citrix ADM StyleBooks pour configurer les instances Citrix ADC. Si vous effectuez une mise à niveau vers Citrix ADM 12.1 build 49.23 à partir de la version 12.0 ou de la version 12.1 build 48.18, vous devez exécuter le script de migration suivant :

```
1 /mps/scripts/migration_scripts/migrate_configurations.py
2 <!--NeedCopy-->
```

- L'exécution du script de migration crée des packs de configuration du StyleBook « os-cs-lb-mon » correspondant aux configurations OpenStack existantes.
- L'exécution de ce script de migration est obligatoire si des configurations OpenStack ont été déployées à partir de ces versions antérieures.
- Vous pouvez déployer de nouvelles configurations sur les instances à l'aide du StyleBook « os-cs-lb-mon » uniquement après avoir exécuté le script de migration à partir de la version 12.1 build 49.23.
- Toutes les configurations tentées à partir d'OpenStack échouent jusqu'à ce que le script de migration soit exécuté.

#### Remarque

- Une fois que vous exécutez le script de migration, vous ne pouvez pas passer à la version précédente de Citrix ADM.
- Assurez-vous d'avoir mis à niveau les pilotes Citrix ADC pour OpenStack LBaaS V2 vers la dernière version. Utilisez les fichiers groupés Citrix ADC fournis avec la dernière version 49.23 de Citrix ADM 12.1.

Les implémentations de l'API LBaaS V2 sont effectuées à l'aide de commandes LBaaS Neutron. Connectez-vous à n'importe quel client Neutron et exécutez les tâches de configuration. Pour plus d'informations sur l'exécution des commandes de configuration, voir Configuration de [LBaaS V2 à l'aide de la ligne de commande](#) .

## Prise en charge des licences d'enregistrement et de récupération VPX et des licences groupées pour l'environnement OpenStack

February 1, 2024

Dans le workflow d'orchestration OpenStack, Citrix Application Delivery Management (ADM) crée des instances Citrix ADC VPX à la demande lorsque vous sélectionnez un service package avec **OpenStack Compute**. Maintenant, la page Service Package de la fonctionnalité Orchestration de Citrix ADM est améliorée pour fournir la licence requise pour être installée sur les instances Citrix ADC VPX créées à la demande. Les licences fournies peuvent être soit une licence d'enregistrement et de départ VPX ou une licence groupée.

Pour utiliser cette fonctionnalité, vous devez d'abord télécharger les licences dans Citrix ADM, puis créer des packages de services qui utilisent le calcul OpenStack.

- S'il s'agit d'une licence d'enregistrement et de départ, vous pouvez choisir la licence à installer parmi les différentes licences disponibles.

## ← Service Package

### Service Level Agreement

Name **sp-nova**

### Auto Provision Settings

#### Resources

Maximum Number of Instances to Auto Provision\*

Flavor\*

Install License

VPX Licenses     Pooled License

License Type\*

Enterprise     Platinum     Standard

Model\*

- S'il s'agit d'une licence de pool, vous pouvez sélectionner à la fois la bande passante et le type d'édition de licence à installer.

## ← Service Package

**Service Level Agreement**

Name **sp-nova**

---

**Auto Provision Settings**

**Resources**

Maximum Number of Instances to Auto Provision\*

Flavor\*

Install License

VPX Licenses     Pooled License

License Type\*

Enterprise     Platinum     Standard

Available Bandwidth

Bandwidth\*

Bandwidth Unit\*

Chaque fois que vous déployez votre premier équilibreur de charge avec Citrix ADM en tant que fournisseur, Citrix ADM crée l'instance Citrix ADC VPX et installe la licence spécifiée dans le service package sur l'instance nouvellement créée.

En outre, lorsque vous supprimez une instance d'équilibrage de charge existante, cette instance n'est plus nécessaire. L'instance est désaffectée et la licence est renvoyée à Citrix ADM. Cela permet une utilisation optimale des licences disponibles dans Citrix ADM.

### Remarque

Lorsque Citrix ADM est déployé en mode haute disponibilité, considérez que les licences sont téléchargées sur l'ADM actif ou principal Citrix, MAS-HA-1. Lorsque vous déployez la première

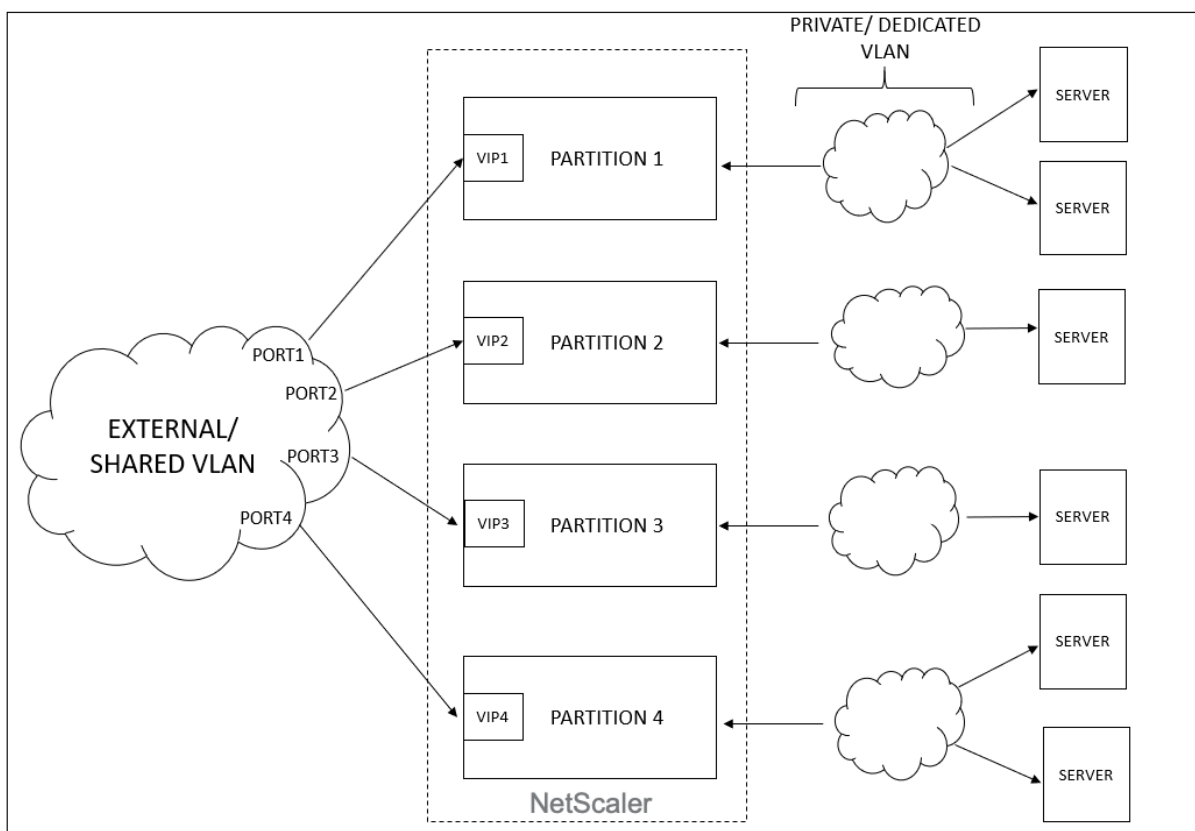
demande et que Citrix ADM crée les instances Citrix ADC VPX, l'instance extrait les licences requises de MAS-HA-1. À un moment ultérieur, supposons que le Citrix ADM secondaire, MAS-HA-2, qui n'a pas les licences est actif maintenant. L'instance ADC VPX ne peut pas retirer la licence de MAS-HA-2 maintenant et, par conséquent, l'instance ne peut pas être créée pour les nouveaux utilisateurs.

Dans ce cas, assurez-vous que MAS-HA-1 est UP et qu'il est maintenant le nœud principal actuel. Autrement dit, basculer manuellement l'Citrix ADM de MAS-HA-2 vers MAS-HA-1. Après cela, vous devez réessayer la configuration à partir d'OpenStack et les instances seront recréées avec des licences appropriées. Pour plus d'informations sur la prise en charge des licences dans le déploiement haute disponibilité Citrix ADM, consultez [Haute disponibilité](#).

### **Prise en charge du VLAN partagé pour les partitions d'administration**

February 1, 2024

Pour les locataires qui se connectent à partir de réseaux privés, Citrix Application Delivery Management (ADM) prend en charge la stratégie d'isolement afin que chaque locataire dispose de sa propre partition dédiée, d'un VLAN dédié et de serveurs dédiés. Pour les locataires qui se connectent à partir de réseaux publics, un VLAN dédié nécessitera trop d'adresses IP pour être utilisé. Un VLAN partagé contourne ce problème en créant une adresse IP virtuelle sur chaque partition, créant ainsi un seul sous-réseau IP.



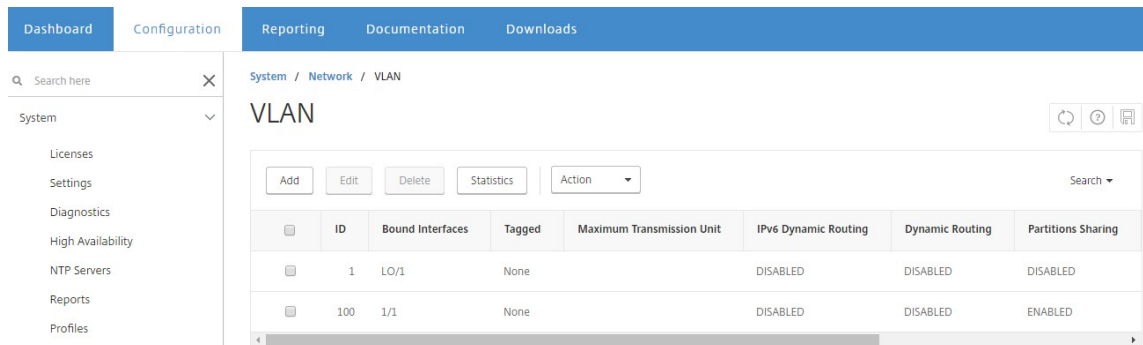
Lorsqu'un locataire configure un VIP ou un écouteur, une partition d'administrateur est créée dans le périphérique Citrix ADC pour ce locataire. Toute la configuration de l'équilibreur de charge est poussée vers la partition d'administration qui est créée. Si le locataire utilise un réseau partagé ou un réseau externe pour créer un équilibreur de charge, le VLAN de ce réseau est ajouté et la fonctionnalité de partage est activée. Lorsqu'un autre locataire utilise le même réseau partagé pour créer son équilibreur de charge, le VLAN n'est pas ajouté à l'Citrix ADC, mais le VLAN est également lié à la deuxième partition. Ainsi, tout locataire qui utilise le même réseau partagé obtient une partition qui est liée au même VLAN.

Citrix ADM prend en charge l'adresse MAC de destination virtuelle. Lorsque les locataires partagent un VLAN, Citrix ADM attribue différentes adresses MAC à la partition sur le périphérique Citrix ADC. Cela permet de partager un VLAN entre des partitions ou entre tous les locataires et tous les domaines de trafic.

### Configuration du VLAN partagé à partir d'une instance Citrix ADC

1. Dans une instance Citrix ADC, accédez à **Configuration > Système > Réseau > VLAN**, sélectionnez un profil VLAN, puis cliquez sur **Modifier** pour définir le paramètre de partage de partition.
2. Dans la page **Configurer le VLAN**, activez la case à cocher **Partage de partitions**.

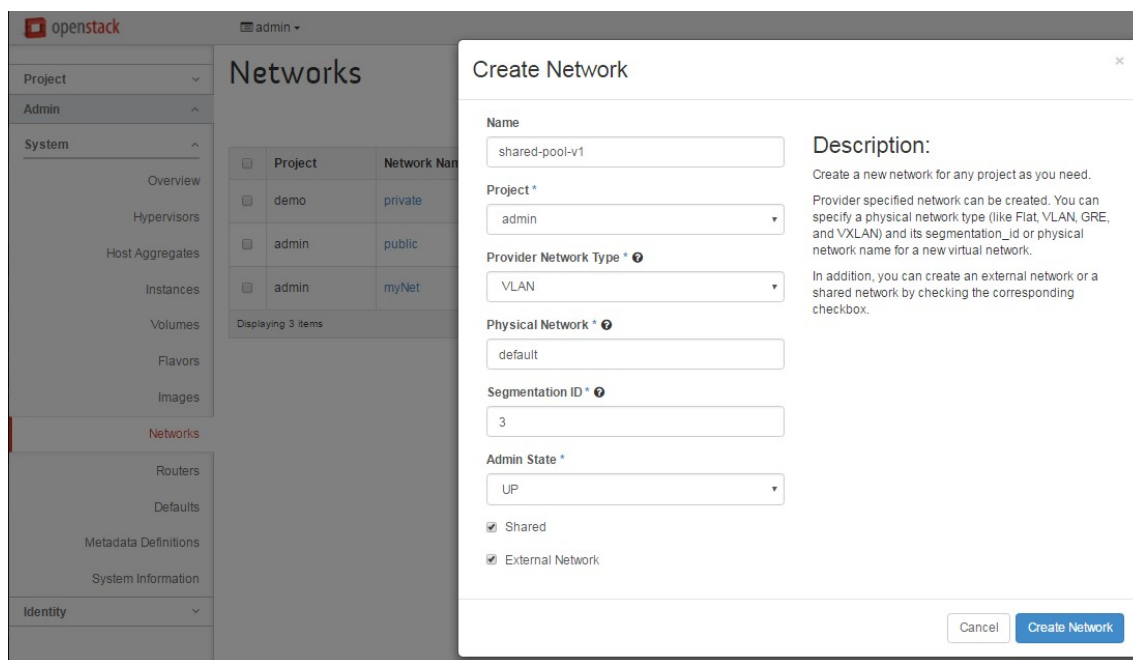
3. Cliquez sur **OK**.



### Configuration du VLAN partagé à partir d'OpenStack Orchestration

1. Dans OpenStack, accédez à **Admin > Système > Réseaux**, puis cliquez sur **Créer un réseau**.
2. Dans **Create Network**, définissez les paramètres suivants :
  - a) Nom : entrez le nom du réseau
  - b) Projet : sélectionnez un projet dans la liste déroulante
  - c) Type de réseau du fournisseur : sélectionnez le **VLAN** dans la liste déroulante. Cela définit que le réseau virtuel est établi en tant que VLAN.
  - d) Réseau physique : le réseau physique par défaut est sélectionné ici. Vous pouvez le modifier.
  - e) État de l'administrateur : par défaut, l'état administratif du réseau est UP
  - f) Sélectionnez Réseau **partagé** et **externe** pour définir que le VLAN est partagé et utilise un réseau externe.
3. Cliquez sur **Créer un réseau**.





## Flux de travail de licence d'essai

February 1, 2024

Lors du provisionnement automatique de l'instance Citrix ADC VPX à l'aide de l'orchestration OpenStack, Citrix Application Delivery Management (ADM) utilise OpenStack Compute pour lancer une instance Citrix ADC VPX. L'instance Citrix ADC VPX nouvellement provisionnée contacte le portail de licences Citrix pendant la configuration et utilise le code d'activation de licence (LAC) pour télécharger et installer automatiquement les fichiers de licence.

### Licences d'essai

Le personnel du support technique utilise des licences d'essai lorsqu'il installe des périphériques Citrix ADM et Citrix ADC VPX sur le terrain. Une licence d'essai ou d'évaluation pour Citrix ADC VPX est valide pendant 90 jours. S'il est nécessaire d'évaluer plus d'un Citrix ADC ou de prolonger le test après 90 jours, une nouvelle licence d'évaluation doit être demandée. Au lieu de l'installation automatique des fichiers de licence d'essai, Citrix ADM vous propose une solution alternative. Vous pouvez télécharger manuellement les fichiers de licence et les installer sur Citrix ADC VPX pour terminer l'installation de l'instance.

Si Citrix ADC VPX ne peut pas se connecter à Internet, configurez Citrix ADM pour qu'il agisse en tant que serveur proxy pour Citrix Licensing Portal et installez les fichiers de licence.

Les instances Citrix ADC VPX disposant d'une licence d'essai peuvent communiquer avec Citrix ADM sur HTTP uniquement. Pour configurer la communication HTTP dans Citrix ADM, accédez à **Système > Administration système**, puis cliquez sur **Modifier les paramètres système**. Sélectionnez **http** dans la liste déroulante pour définir la méthode de communication, puis cliquez sur **OK**.

## ← | Modify System Settings

Communication with instance(s)\*

http ▼

- Secure Access Only
- Enable Session Timeout
- Allow Basic Authentication
- Enable nsrecover Login
- Enable Certificate Download
- Enable Shell access for non-nsroot User

## Intégration avec les services OpenStack Heat

February 1, 2024

Les LBaaS OpenStack Neutron permettent des services d'équilibrage de charge de base, tels que l'équilibrage de charge, le déchargement SSL et la commutation de contenu, pour les applications. LBaaS est géré via une API RESTful, et l'API permet aux locataires d'effectuer des appels REST pour créer, mettre à jour et supprimer des objets LBaaS. Étant donné que LBaaS fournit des services d'équilibrage de charge, il n'autorise pas l'utilisation des fonctionnalités Citrix ADC plus avancées au cours du processus d'orchestration. Le plug-in Citrix ADC Heat surmonte cette limitation.

## **Service d'orchestration thermique**

Le service d'orchestration OpenStack Heat permet de déployer des applications cloud complexes sur la base de modèles. Le modèle d'orchestration Heat (HOT) décrit l'infrastructure d'une application cloud sous forme de fichiers texte lisibles et inscriptibles par des humains, et pouvant être gérés par des outils de contrôle de version. Le langage structuré YAML est utilisé pour écrire ces modèles. Le modèle HOT vous permet de créer la plupart des types de ressources OpenStack et spécifie les relations entre les ressources définies dans celui-ci. Le plug-in Citrix ADC Heat vous permet de configurer les fonctionnalités ADC (Advanced Application Delivery Controller) sur n'importe quelle instance Citrix ADC.

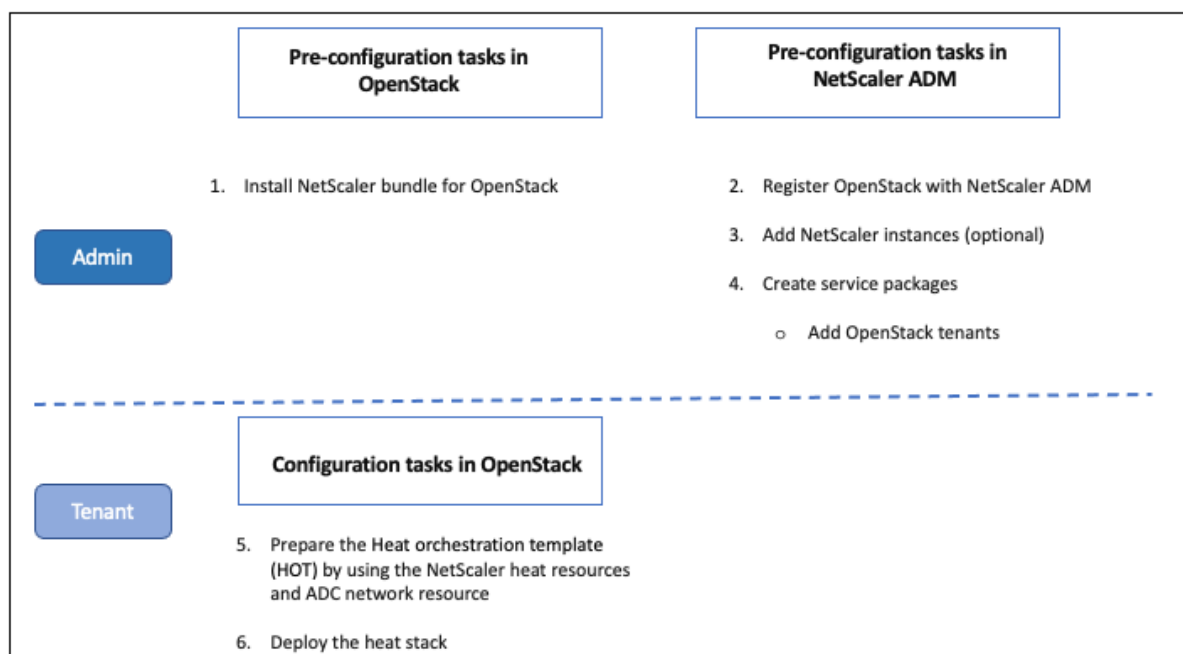
## **Citrix ADC StyleBooks**

Citrix Application Delivery Management (ADM) StyleBooks peut être utilisé pour créer et configurer des fonctionnalités Citrix ADC. Tout comme les modèles Heat, les StyleBooks sont également écrits en YAML. Un StyleBooks distinct peut être créé pour chaque fonctionnalité, et un StyleBooks unique peut être utilisé pour déployer des configurations sur plusieurs instances Citrix ADC.

Lors de l'intégration de Citrix ADC avec OpenStack, Citrix ADM publie tous les StyleBooks Citrix ADM en tant que ressource dans le service Heat. Cela inclut à la fois les StyleBooks livrés avec Citrix ADM et les StyleBooks créés par l'utilisateur à un moment ultérieur. Le modèle Heat vous permet de configurer les fonctionnalités avancées des Citrix ADC à l'aide de ces ressources StyleBooks.

## **Workflow pour configurer des instances Citrix ADC à l'aide de la chaleur**

L'organigramme suivant illustre le workflow de déploiement de la pile de chaleur :



Effectuez les tâches suivantes en tant qu'administrateur de cloud :

**Pour configurer les services Heat dans OpenStack :**

1. Télécharger les offres groupées Citrix ADC pour OpenStack

Installez les bundles Citrix ADC dans OpenStack. Dans Citrix ADM, accédez à **Téléchargements** et téléchargez les bundles de pilotes Citrix ADC, dézippez les bundles et copiez le contenu du dossier Heat dans le répertoire des ressources du moteur Heat dans OpenStack. Le chemin d'accès au répertoire est le suivant :

/opt/stack/heat/heat/engine/resources/netscaler\_resources

2. Créez une section « netscaler\_plugin » dans le fichier heat.conf et mettez à jour les paramètres suivants dans cette section :

[netscaler\_plugin]

- a) Lorsque la communication est http, les paramètres sont mis à jour comme suit :

NMA\_BASE\_URI=<http://10.146.103.45:80>

NMA\_USERNAME=

NMA\_PASSWORD=

- b) Lorsque la communication est en https, les paramètres sont mis à jour comme suit :

NMA\_BASE\_URI=https://common\_name\_used\_in\_certificate

NMA\_USERNAME=<openstack\_driver\_username

NMAS\_PASSWORD=<openstack\_driver\_password>

SSL\_CERT\_VERIFY=<True\_or\_False>

CERT\_FILE\_PATH= <path\_of\_the\_certificate\_file>

Si l'utilisateur définit `ssl_cert_verify` comme étant « False », Citrix ADM envoie `verify=false` dans les appels de requête, ce qui désactive la validation du certificat SSL. Si `ssl_cert_verify` est défini sur « True » et que l'entrée `cert_file_path` est présente, Citrix ADM envoie ce chemin dans le paramètre de vérification de la requête, sinon Citrix ADM envoie `verify=true`.

#### Remarque

Pour déployer Citrix ADM en mode « Haute disponibilité », mettez à jour les paramètres suivants dans le fichier `heat.conf` :

NMAS\_BASE\_URI= <ip address of the front-end virtual server>

### 3. Redémarrez le service Heat dans OpenStack.

Lorsque vous redémarrez les services Citrix ADC Heat dans OpenStack, tous les Citrix ADM Style-Books définis sont importés dans Heat en tant que ressources. En outre, la ressource réseau Citrix ADC et la ressource de certificat sont importées dans OpenStack en tant que ressources Citrix ADC Heat.

### 4. Enregistrez Citrix ADM avec OpenStack.

- a) Dans Citrix ADM, accédez à **Orchestration > Cloud Orchestration > OpenStack**, puis cliquez sur **Configurer les paramètres OpenStack**.
- b) Dans la page **Configurer les paramètres OpenStack**, vous pouvez définir les paramètres pour configurer OpenStack. Deux options s'offrent à vous : par défaut et personnalisé.
- c) Sélectionnez **Par défaut** si les services OpenStack s'exécutent sur les ports par défaut. Entrez les paramètres suivants :
  - i. Adresse IP du contrôleur OpenStack
  - ii. Nom d'utilisateur de l'administrateur
  - iii. Mot de passe
  - iv. Locataire administrateur OpenStack
  - v. Pilote Citrix ADC et mot de passe Heat

#### Remarque II

s'agit du même mot de passe (NMAS\_PASSWORD) que vous avez entré dans le fichier heat.conf.

5. Créez des packages de services et définissez les SLA avec votre locataire.

Un locataire est créé dans Citrix ADM pour chaque utilisateur lors de l'enregistrement OpenStack, et les informations de locataire sont utilisées à la fois par le pilote LBaaS et par le plug-in Heat. Le plug-in Heat utilise ces informations pour contacter Citrix ADM afin d'importer StyleBooks en tant que ressources Heat dans OpenStack.

#### Remarque

Pour plus d'informations sur la création de packages de services et d'autres tâches de pré-configuration dans Citrix ADM et OpenStack, consultez la section [Intégration de Citrix ADM à OpenStack Platform](#).

6. Observez que tous les stylebooks pertinents dans Citrix ADM sont importés dans OpenStack Heat en tant que ressources. Notez également que la ressource réseau Citrix ADC et la ressource de certificat Citrix ADC sont importées dans OpenStack Heat en tant que ressources.

#### Remarque

Actuellement, vous ne pouvez utiliser que les StyleBooks livrés avec Citrix ADM.

Votre locataire peut désormais créer le modèle Heat dans OpenStack, entrer les valeurs des paramètres Heat requis et déployer la pile Heat. Lorsque la pile Heat est déployée, la configuration est transmise à Citrix ADM et les instances Citrix ADC requises sont configurées.

### Pour préparer le modèle de chaleur et lancer la pile de chaleur :

1. Dans OpenStack, le locataire peut créer un modèle d'orchestration Heat (HOT) à l'aide des ressources Heat.
2. Dans OpenStack Horizon, l'administrateur du client peut accéder à **Projet >Orchestration >Stacks** pour créer le modèle Heat et lancer le Heat Stack. Il existe deux manières de créer HOT :
  - **Fichier** : sélectionnez le modèle mis à jour dans le répertoire local
  - **Saisie directe** : copiez et collez le contenu YAML du modèle dans la fenêtre

#### Remarque

Une fois le stack déployé avec succès, le locataire peut le mettre à jour à l'aide du modèle Change Stack. Mais les informations de sous-réseau et l'adresse IP virtuelle (VIP) fournies initialement lors de la création de la pile ne peuvent pas être modifiées.

Une fois que le locataire a déployé la pile, accédez à **Orchestration >Cloud Orchestration>OpenStack>Demandes** dans Citrix ADM pour observer les listes de tâches. En outre, accédez à **Applications >Configuration** dans Citrix ADM pour observer que les instances Citrix ADC sont correctement configurées sous la forme de packs de configuration StyleBooks.

**Exemple d'un Citrix ADM StyleBooks :**

L'image suivante montre un exemple de construction d'un Citrix ADM StyleBooks et explique brièvement les composants. Pour plus d'informations sur les StyleBooks Citrix ADM et sur la façon d'utiliser les StyleBooks livrés, consultez [StyleBooks](#).

```

name: lb-vserver
description: "This stylebook defines a load balancing virtual server configuration."
display-name: "Load Balancing Virtual Server (HTTP)"
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
import-stylebooks:
  -
    namespace: netScaler.nitro.config
    prefix: ns
    version: "10.5"
parameters:
  -
    name: name
    type: string
    required: true
  -
    name: ip
    type: ipaddress
    required: true
  -
    name: lb-alg
    type: string
    allowed-values:
      - ROUNDROBIN
      - LEASTCONNECTION
    default: ROUNDROBIN
components:
  -
    name: my-lbvserver-comp
    type: ns::lbvserver
    properties:
      name: $parameters.name
      servicetype: HTTP
      ipv46: $parameters.ip
      port: 80
      lbmethod: $parameters.lb-alg

```

**Exemple d'un modèle de chaleur :**

L'image suivante montre la structure d'un modèle de chaleur défini dans YAML et pointe vers les ressources StyleBooks et Citrix ADC importées en tant que ressources de chaleur.

```

heat_template_version: '2015-10-15'
parameter_groups:
- description: servers
  label: servers
  parameters: [server_ips, server_port]
- description: vip ip
  label: VIP IP
  parameters: [lb-virtual-ip, lb-virtual-port, lb-service-type]
- description: lb-appname
  parameters: [lb-appname]
parameters:
  lb-appname: {description: This is the lb-name, label: LB-NAME, type: string}
  lb-service-type:
    constraints:
      - allowed values: [HTTP, SSL, TCP, UDP, ANY]
      default: HTTP
      description: This is lb-service-type
      label: Service-type
      type: string
  lb-virtual-ip: {description: This is LB vip, label: VIP, type: string}
  lb-virtual-port: {description: This is virtual port, label: Virtual-port, type: string}
  server_ips: {description: Ip address of servers, label: IP of server, type: comma_delimited_list}
  server_port: {description: Port of server, label: Server port, type: string}
resources:
  sb_config:
    properties:
      lb-appname: {get_param: lb-appname}
      lb-service-type: {get_param: lb-service-type}
      lb-virtual-ip: {get_param: lb-virtual-ip}
      lb-virtual-port: {get_param: lb-virtual-port}
      mas_device_handle:
        get_attr: [network_resource_NS, mas_device_handle]
      svc-servers:
        repeat:
          for each:
            ipvar%: {get_param: server_ips}
            template:
              ip: ipvar%
              port: {get_param: server_port}
            type: Citrix::NetScaler::Stylebook_com_citrix_adc_stylebooks_1_0_lb
  network_resource_NS:
    properties:
      subnets: [c07d727c-37a6-493a-ab4e-b96d9ddab560]
    type: Citrix::NetScaler::NetscalerNetworkConfigurator

```

version of the Heat template

parameter groups - declares the input parameter groups and order

parameter groups - declares the input parameters

resources - declares template resources; in this example declares the StyleBook resources

resources - declares template resources; in this example declares the NetScaler network resources

Pour plus d'informations sur les services Heat et la façon de créer des modèles, consultez la [documentation OpenStack Heat](#).

## Stratégies d'isolement des packages de services

February 1, 2024

### Stratégie d'isolement dédiée

Chaque locataire associé au package de service Citrix Application Delivery Management (ADM) d'une stratégie dédiée se voit attribuer une instance Citrix ADC parmi les instances qui font partie de ce service package. Cette instance Citrix ADC affectée n'est pas partagée avec d'autres locataires.



## ← Service Package

### Service Level Agreement

Application Delivery Management allocates Citrix ADC Appliances for tenants

Name\*

Citrix ADC Instance Allocation\*

Dedicated    Partition    Shared   [?](#)

Citrix ADC Instance Provisioning\*

Existing Instance    Create Instance OnDemand

Auto Provision Platform

CitrixADC SDX    OpenStack Compute

Citrix ADC Instance Type

**CitrixADC VPX**

### Stratégie d'isolement de partition

Chaque locataire associé au service package de stratégie de partition se voit attribuer une partition d'administration logique dédiée d'une instance Citrix ADC qui fait partie du service package.

## ← Service Package

### Service Level Agreement

Application Delivery Management allocates Citrix ADC Appliances for tenants

Name\*

Citrix ADC Instance Allocation\*

Dedicated  Partition  Shared

Citrix ADC Instance Provisioning\*

Existing Instance  Create Instance OnDemand

Citrix ADC Instance Type

CitrixADC VPX  CitrixADC MPX

### Stratégie d'isolement partagée

Les locataires associés au service package partagent les instances Citrix ADC qui font partie du service package. Toutes les configurations d'un locataire sont affectées à une instance Citrix ADC. Dans ce mode, les configurations de plusieurs locataires peuvent être hébergées sur la même instance de Citrix ADC. Vous pouvez sélectionner **Citrix ADC VPX** ou **Citrix ADC MPX** comme type de périphérique. Vous pouvez choisir d'utiliser une seule instance Citrix ADC ou plusieurs instances au service package. Autrement dit, plusieurs locataires peuvent partager une ou plusieurs instances virtuelles du périphérique Citrix ADC.

#### Remarque

Ajouter des instances Citrix ADC SDX dans les packages de service en tant qu'instances Citrix ADC VPX uniquement, car un Citrix ADC SDX dispose d'un VPX Citrix ADC.

## ← Service Package

### Service Level Agreement

Application Delivery Management allocates Citrix ADC Appliances for tenants during their LB configuration. The following settings determine the SLA that is agreed for the tenants of this service package.

Name\*

Citrix ADC Instance Allocation\*

Dedicated  Partition  Shared

Citrix ADC Instance Type

CitrixADC VPX  CitrixADC MPX

Number of instances to allot per Policy/Tenant

Allot one instance  Allot many instances

Placement Method\*

 ⓘ

#### Remarque

Vous pouvez également créer des stratégies de placement flexibles, où les stratégies sont basées non seulement sur le nom ou l’ID du locataire, mais également sur d’autres attributs personnalisés. Pour plus d’informations sur les stratégies de placement flexibles, consultez [Allocation flexible des appareils basée sur des règles](#).

## Attribution de périphériques flexible basée sur des règles

February 1, 2024

Citrix Application Delivery Management (ADM) attribue des instances virtuelles Citrix ADC aux locataires, en fonction des contrats de niveau de service convenus avec les locataires. L’attribution d’instances virtuelles aux locataires crée une relation un-à-un entre l’instance et le locataire,

dans laquelle un locataire ne peut être affecté qu'à un seul package de services dans le centre de données.

Dans certaines situations, les locataires peuvent nécessiter plus d'une instance, ou l'attribution d'instances peut ne pas être basée sur les locataires comme critère, mais sur d'autres facteurs tels que l'ID réseau ou l'application. Dans de tels cas, Citrix ADM vous permet de définir avec précision des stratégies de placement basées sur des expressions définies par l'utilisateur afin d'affecter une configuration d'équilibrage de charge à l'une des instances gérées.

Les stratégies de placement offrent la flexibilité nécessaire pour décider de l'instance Citrix ADC utilisée dans chaque configuration d'équilibrage de charge créée par les utilisateurs. Les stratégies de placement flexibles dans Citrix ADM fournissent une option ajoutée à la méthode existante d'attribution d'instances Citrix ADC en fonction des locataires.

### Remarque

Vous pouvez attribuer des instances aux locataires manuellement ou utiliser des stratégies de placement pour attribuer des instances en fonction des expressions créées. Vous ne pouvez pas utiliser ces deux méthodes simultanément sur un même package de services.

Les stratégies de placement sont basées sur des expressions booléennes définies sur les propriétés des principaux objets de configuration LBaaS, tels que les pools et les équilibreurs de charge. L'interface utilisateur de stratégie de placement dans Citrix ADM fournit des expressions prédéfinies que vous pouvez choisir pour définir une stratégie personnalisée. Vous pouvez créer plusieurs stratégies de placement pour différentes expressions. Ainsi, chaque locataire peut disposer de plusieurs appareils définis selon ses besoins.

Vous devez d'abord sélectionner une expression correspondant à un objet racine qui doit être configuré ultérieurement. L'objet racine peut être un objet pool dans le cas de LBaaS V1, et un objet d'équilibrage de charge dans le cas de LBaaS V2. Ainsi, les placements basés sur la stratégie Citrix ADM sont pris en charge pour les API LBaaS V1 et V2. Ces stratégies de placement sont ensuite associées aux packages de services. Une fois que l'objet racine est placé dans une instance, les objets successifs du modèle sont ajoutés à l'instance.

Par exemple, l'objet de configuration du pool peut avoir les propriétés suivantes :

- tenant\_id
- nom
- description
- protocol
- lb\_method
- subnet\_id

- subname\_name
- admin\_state\_up
- état
- network\_id
- network\_type
- segmentation\_id
- subnet\_cidr
- subnet\_gateway\_ip

Les exemples suivants présentent certaines expressions qui utilisent les propriétés du pool pour définir une expression pour la stratégie :

1. Expression de stratégie basée sur le nom de pool  
`config["pools"]["name"] == "high-end-pool"`
2. Expression de stratégie basée sur le nom de sous-réseau de pool  
`config["pools"]["subnet_name"] == "us-west-payment-subnet1"`
3. Expression de stratégie basée sur le nom du sous-réseau d'équilibrage de charge  
`config["loadbalancers"]["subnet_name"] == "mas-subnet"`

## Ajout d'une stratégie de placement

1. Dans la page d'accueil de Citrix ADM, accédez à **Orchestration > Cloud Orchestration > Stratégie de placement**, puis cliquez sur **Ajouter**.
2. Dans la page **Ajouter une stratégie de placement**, définissez les paramètres suivants :
  - a) Nom : entrez un nom pour la stratégie de placement
  - b) Expressions fréquemment utilisées : sélectionnez une expression dans la liste déroulante.
  - c) Expression : une expression logique (booléenne) est renseignée dans ce champ en fonction de l'expression que vous avez sélectionnée dans le champ précédent. Modifiez les noms des champs selon vos besoins.

### Remarque

Lorsque vous créez plusieurs stratégies, assurez-vous qu'elles sont exclusives les unes aux autres.

## ← Add Placement Policy

Name\*

Sample Expressions\*

Expression\*

3. Cliquez sur **OK**.
4. Accédez à **Orchestration > Cloud Orchestration > OpenStack > Service Packages**, puis cliquez sur **Ajouter**.
5. Sur la page **Service Package**, définissez les paramètres suivants :

- a) Nom : entrez le nom du package de services
- b) Stratégie d'isolation : sélectionnez **une stratégie partagée**

Dans la stratégie d'isolement partagée, la configuration d'équilibrage de charge d'un locataire coexiste avec la configuration d'équilibrage de charge des autres locataires de l'appareil alloué au locataire.

- c) Type de périphérique : sélectionnez un **Citrix ADC VPX** ou **Citrix ADC MPX** préprovisionné. Sélectionnez **Allocation d'un périphérique** si vous souhaitez que toutes les configurations d'équilibrage de charge d'un locataire soient liées à un périphérique. Sélectionnez **Allocation de plusieurs périphériques** si vous souhaitez que chaque configuration d'équilibreur de charge d'un locataire soit distribuée sur plusieurs périphériques en fonction des stratégies de placement.

### Remarque

Citrix ADC SDX doit être ajouté dans les packages de service en tant qu'instances Citrix ADC VPX uniquement, car un Citrix ADC SDX possède un VPX Citrix ADC.

- d) Méthode de placement - sélectionnez **Moins configurés**

Lorsque Moins configurés est sélectionné, l'instance Citrix ADC qui a le moins de membres de pool configuré à ce moment est choisie comme périphérique pour le locataire.

## ← Service Package

### Service Level Agreement

Application Delivery Management allocates Citrix ADC Appliances for tenants

Name\*

Citrix ADC Instance Allocation\*

Dedicated     Partition     Shared

Citrix ADC Instance Type

CitrixADC VPX     CitrixADC MPX

Number of instances to allot per Policy/Tenant

Allot one instance     Allot many instances

Placement Method\*

 ?

6. Cliquez sur **Continuer**.

7. Dans la section **Affecter des périphériques**, ajoutez les périphériques Citrix ADC disponibles à la liste des périphériques configurés.

### Assign Devices

Available (1) [Select All](#)

 +

Configured (1) [Remove All](#)

 -

▶

◀

8. Cliquez sur **Continuer**.
9. Dans la section **Affecter des stratégies de placement/Locataires OpenStack**, ajoutez la stratégie de placement que vous avez créée précédemment.

**Assign Placement Policies/OpenStack Tenants**

Tenants assigned to one shared Service Package should not have overlapping IP addresses in their networks.

Placement Policies
  OpenStack Tenants

**Available (1)** Select All

http\_region\_pp +

**Configured (1)** Remove All

admin\_pp\_policy -

▶  
◀

Continue
Cancel

**Remarque**

Si la stratégie n'est pas trouvée, le mécanisme de secours est rétabli et Citrix ADM attribue des instances Citrix ADC en fonction des locataires. Si le locataire ne fait partie d'aucun package de services, Citrix ADM affiche un message d'erreur indiquant : « Le locataire <admin> ne fait partie d'aucun Service Package et il n'y a aucun Service Package par défaut. »

10. Cliquez sur **Continuer**, puis sur **Terminé**.

## NSX Manager : Provisioning manuel des instances Citrix ADC

February 1, 2024

Citrix Application Delivery Management (ADM) s'intègre à la plate-forme de virtualisation réseau VMware pour automatiser le déploiement, la configuration et la gestion des services Citrix ADC. Cette intégration évite les complexités traditionnelles associées à la topologie de réseau physique, permettant aux administrateurs vSphere/vCenter de déployer par programmation les services Citrix ADC plus rapidement.



Cet article fournit une liste des tâches que vous devez effectuer sur VMware NSX Manager et sur Citrix ADM.

#### Remarque

Assurez-vous que VMware NSX for vSphere 6.2 et versions ultérieures est installé et configuré, et que les passerelles périphériques, les machines DLR et les machines virtuelles qui doivent être équilibrées de charge sont déjà créés.

### Conditions préalables

- Installez VMware ESXi version 4.1 ou ultérieure avec du matériel répondant à la configuration minimale requise.
- Installez VMware Client sur une station de travail de gestion qui répond à la configuration système minimale requise.
- Installez VMware OVF Tool (requis pour VMware ESXi version 4.1) sur une station de travail de gestion répondant à la configuration minimale requise.
- Installez Citrix ADM sur l'un des hyperviseurs pris en charge.

Pour connaître les tâches d'installation de Citrix ADM build 12.1, sur l'un des hyperviseurs pris en charge, reportez-vous à la section [Déploiement de Citrix ADM](#).

### Configuration matérielle requise pour VMware ESXi

Le tableau suivant répertorie les ressources informatiques virtuelles dont vous avez besoin sur votre serveur VMware ESXi pour installer une appliance virtuelle Citrix ADM.

---

Composant	Exigences
RAM	8 GB
CPU virtuel	8
Espace de stockage	500 GB
Interfaces réseau virtuelles	1
Débit	1 Gbit/s

---

### Remarque

Les exigences en matière de mémoire et de disque dur spécifiées ci-dessus concernent le déploiement de Citrix ADM sur le serveur VMware ESXi, étant donné qu'aucune autre machine virtuelle ne s'exécute sur l'hôte. La configuration matérielle requise pour le serveur VMware ESXi dépend du nombre de machines virtuelles qui s'y exécutent.

## Configuration de VMware NSX

- Créez un pool d'instances Citrix ADC VPX de différentes capacités, qui sont ajoutées aux différents services packages.

Par exemple :

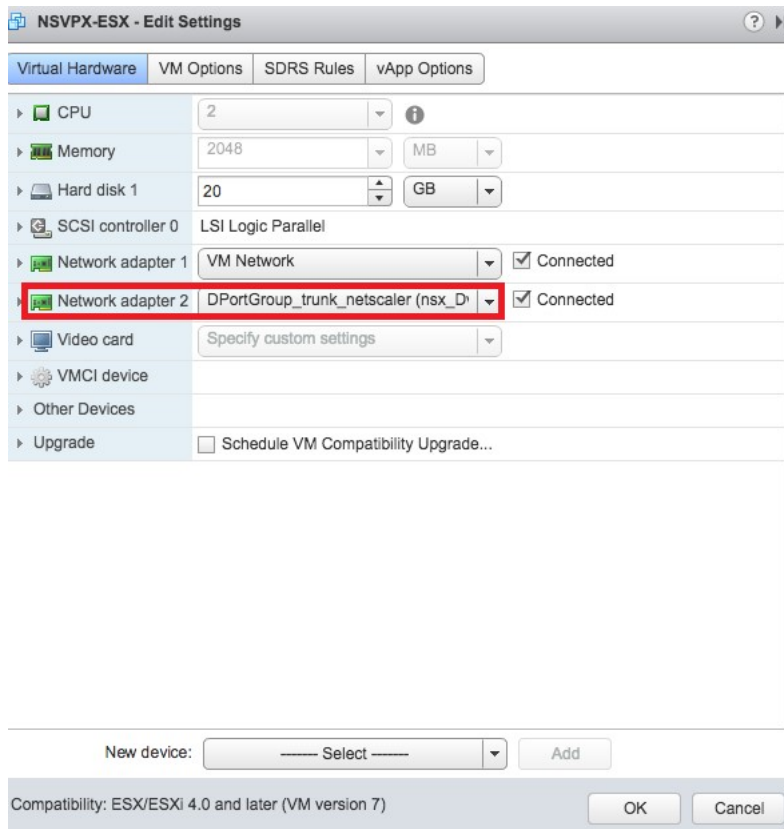
- Créez cinq instances Citrix ADC VPX de VPX1000 (1 Gbit/s). Ces instances sont ajoutées au package de service Gold.
  - Créez cinq instances Citrix ADC VPX de VPX10 (10 Mbit/s). Ces instances sont ajoutées au package de service Bronze.
1. Dans vSphere Client, accédez à **Networking** et créez un groupe de ports de type VLAN Trunking avec plage, par exemple, 101-105 (vous pouvez même fournir la plage complète, mais créer un groupe de ports de type VLAN pour uniquement les VLAN requis).

The screenshot shows the 'New Distributed Port Group' configuration window. On the left, there are three steps: '1 Select name and location', '2 Configure settings' (which is selected), and '3 Ready to complete'. The main area is titled 'Configure settings' and contains the following fields:

- Port binding: Static binding
- Port allocation: Elastic
- Number of ports: 8
- Network resource pool: (default)
- VLAN type: VLAN trunking
- VLAN trunk range: 0-4094
- Advanced:  Customize default policies configuration

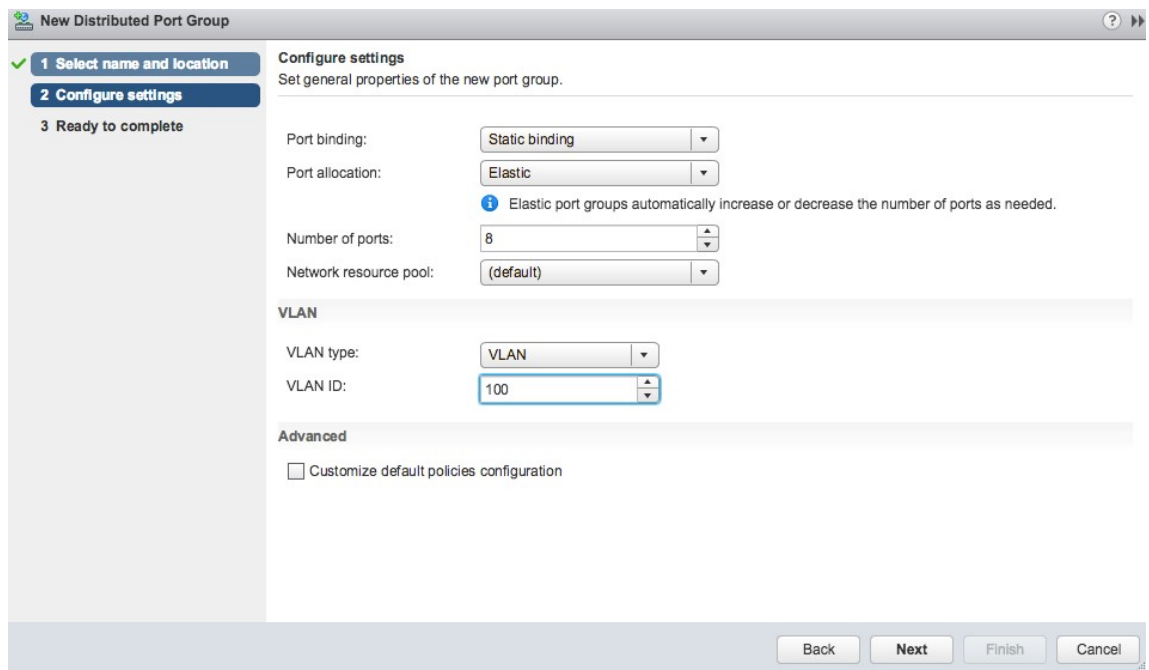
At the bottom right, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

2. Créez une nouvelle interface pour chaque instance Citrix ADC VPX et attachez-la au groupe de ports de jonction de la plage de VLAN créé ci-dessus.



3. Dans vSphere Client, accédez à **Mise en réseau** et créez un groupe de ports de type VLAN.

Par exemple, si le groupe de ports tronqués initial a été créé avec la plage 101 à 105, créez cinq groupes de ports VLAN un par VLAN, c'est-à-dire un groupe de ports avec VLAN 101, un autre avec VLAN102, etc., jusqu'à VLAN 105.



## Ajout d'une instance Citrix ADC VPX dans Citrix ADM

Ajoutez des instances Citrix ADC VPX dans Citrix ADM et spécifiez la plage de VLAN du groupe tronqué pour chaque périphérique.

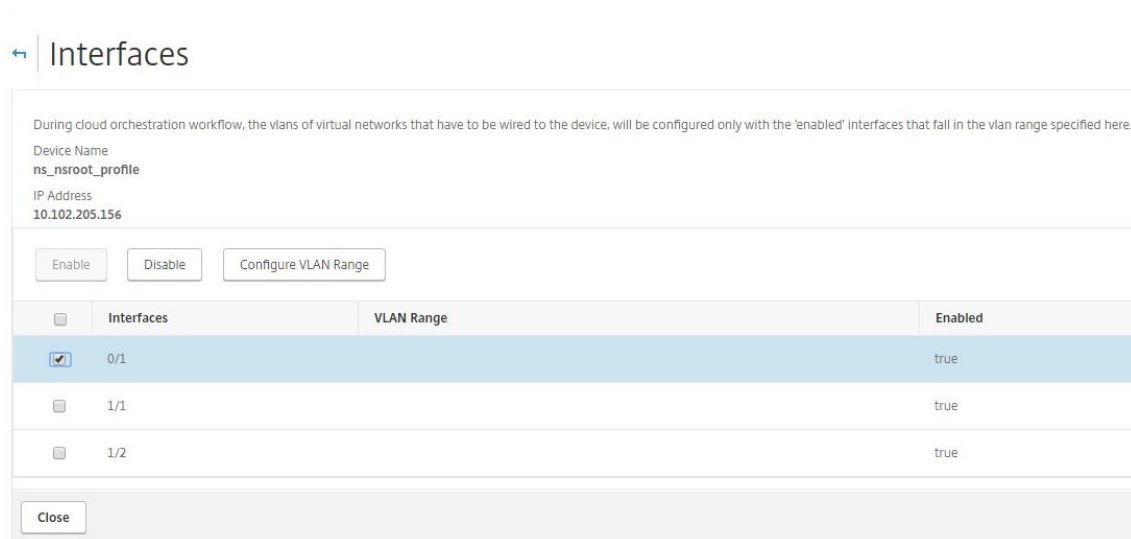
1. Dans Citrix ADM, accédez à **Infrastructure > Instances > Citrix ADC VPX**, puis cliquez sur **Ajouter**.
2. Sur la page **Ajouter un Citrix ADC VPX**, spécifiez les noms d'hôte des instances, l'adresse IP de chaque instance ou une plage d'adresses IP, puis sélectionnez un profil d'instance dans la liste **Profile Name**. Vous pouvez également créer un profil d'instance en cliquant sur l'icône +.
3. Cliquez sur **OK**.
4. Sélectionnez l'instance Citrix ADC VPX nouvellement ajoutée dans la liste de la page **Citrix ADC VPX**, puis cliquez sur le bouton flèche vers le bas dans le champ **Action**. Sélectionnez **Configurer les interfaces pour l'orchestration**.

### Citrix ADC

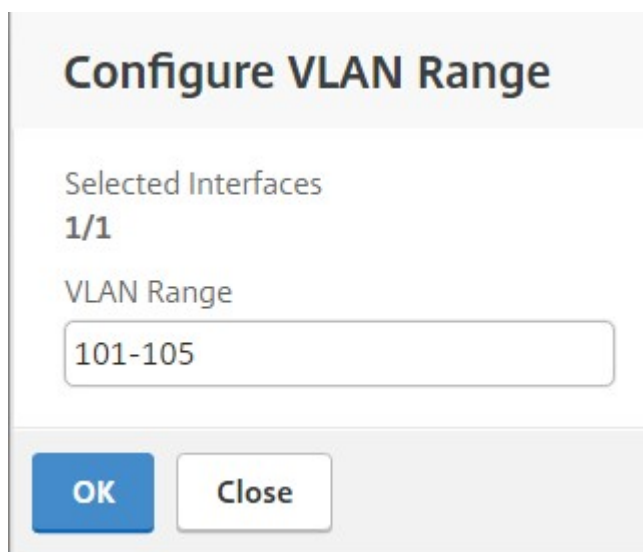
The screenshot shows the Citrix ADC VPX management interface. At the top, there are filters for VPX (19), MPX (1), CPX (0), and SDX (0). Below these are buttons for Add, Edit, Remove, Dashboard, Tags, Profiles, and Partitions. A search bar is present with the text "Click here to search or you can enter Key : Value format". The main table lists instances with columns for checkboxes, IP Address, Host Name, Instance State, and Rx (Mbps). The first instance is selected. An action menu is open, showing options like Backup/Restore, Show Events, Create Cluster, Reboot, Ping, TraceRoute, Rediscover, Unmanage, Annotate, Configure SNMP, Configure Syslog, Configure Analytics, Configure GSLB site, **Configure Interfaces for Orchestration**, Replicate Configuration, Add Cloud Platform Zone Details, and Provision in Openstack.

	IP Address	Host Name	Instance State	Rx (Mbps)
<input checked="" type="checkbox"/>	10.102.29.60	--	● Up	
<input type="checkbox"/>	10.102.29.170	--	● Up	
<input type="checkbox"/>	10.102.29.175	--	● Up	
<input type="checkbox"/>	10.102.29.180	--	● Up	
<input type="checkbox"/>	10.102.29.200	--	● Up	
<input type="checkbox"/>	10.102.126.36	beta	● Out of Service	
<input type="checkbox"/>	10.102.166.4	10.102.166.4	● Down	
<input type="checkbox"/>	10.102.166.5	kranthi-2	● Down	
<input type="checkbox"/>	10.102.166.6	VPX03	● Down	

5. Sur la page **Interfaces**, sélectionnez l'interface de gestion, puis cliquez sur **Désactiver** pour désactiver le VLAN de la liaison à l'interface de gestion.



6. Sur la page **Interfaces**, sélectionnez l'interface requise, puis cliquez sur **Configurer VLAN Range**.
7. Entrez la plage de VLAN configurée dans NSX Manager, cliquez sur **OK**, puis cliquez sur **Fermer**.

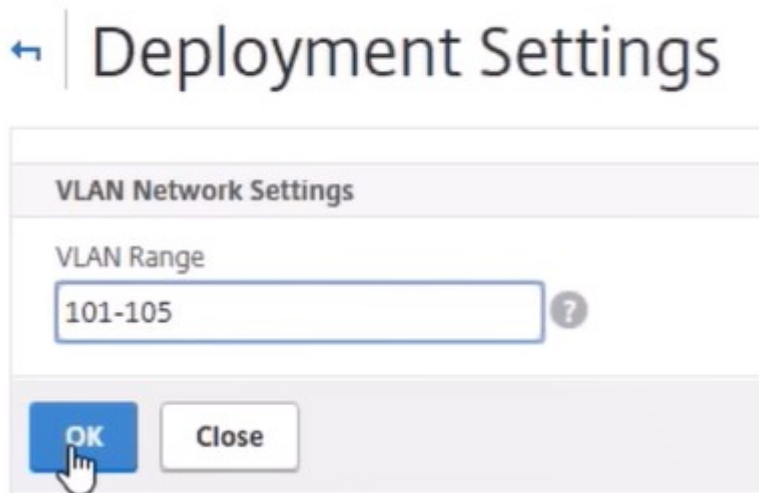


## Enregistrement de VMware NSX Manager auprès de Citrix ADM

Enregistrez VMware NSX manager auprès de Citrix ADM pour créer un canal de communication entre eux.

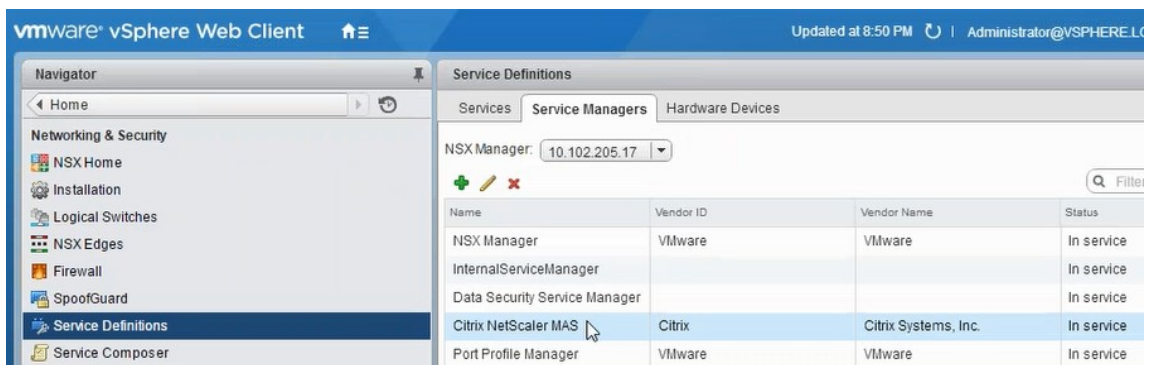
1. Dans Citrix ADM, accédez à **Orchestration > SDN Orchestration > VMware NSX Manager** dans la liste déroulante, puis cliquez sur **Configurer les paramètres de NSX Manager**.
2. Dans la page **Configurer les paramètres de NSX Manager**, définissez les paramètres suivants :
  - a) Adresse IP de NSX Manager : adresse IP de NSX Manager.

- b) Nom d'utilisateur de NSX Manager - Nom d'utilisateur administratif de NSX Manager.
  - c) Mot de passe - Mot de passe de l'utilisateur administratif de NSX Manager.
3. Dans la section **Compte Citrix ADM utilisé par NSX Manager**, définissez le nom d'utilisateur et le mot de passe du pilote Citrix ADC pour NSX Manager. Citrix ADM authentifie les demandes de configuration d'équilibrage de charge à partir de NSX Manager à l'aide de ces informations d'identification d'ouverture de session.
  4. Cliquez sur **OK**.
  5. Accédez à **Orchestration > Système > Paramètres de déploiement**. Fournissez la plage de VLAN configurée dans le groupe de ports tronqués.



6. Ouvrez une session sur NSX Manager sur vSphere Web Client et accédez à **Définitions de service > Gestionnaire de services**.

Vous pouvez afficher Citrix Citrix ADM comme l'un des gestionnaires de services. Cela indique que l'enregistrement réussit et qu'un canal de communication est établi entre le gestionnaire NSX et Citrix ADM.



## Création d'un Service Package dans Citrix ADM

1. Dans Citrix ADM, accédez à **Orchestration > SDN Orchestration > VMware NSX Manager > Service Packages**, puis cliquez sur **Ajouter** pour ajouter un nouveau service package.
2. Dans la page **Service Package**, dans la section **Paramètres de base**, définissez les paramètres suivants :
  - a) Nom : entrez le nom d'un package de services
  - b) Stratégie d'isolement : par défaut, la stratégie d'isolement est définie sur Dédié
  - c) Type de périphérique : par défaut, le type de périphérique est défini sur Citrix ADC VPX

### Remarque

Ces valeurs sont définies par défaut dans cette version et vous ne pouvez pas les modifier.

- d) Cliquez sur **Continuer**.

## ← Service Package

**Service Level Agreement**

Application Delivery Management allocates Citrix ADC Appliances for tenants during their LB configuration.

Name\*

Citrix ADC Instance Allocation\*

Dedicated
  Partition
  Shared

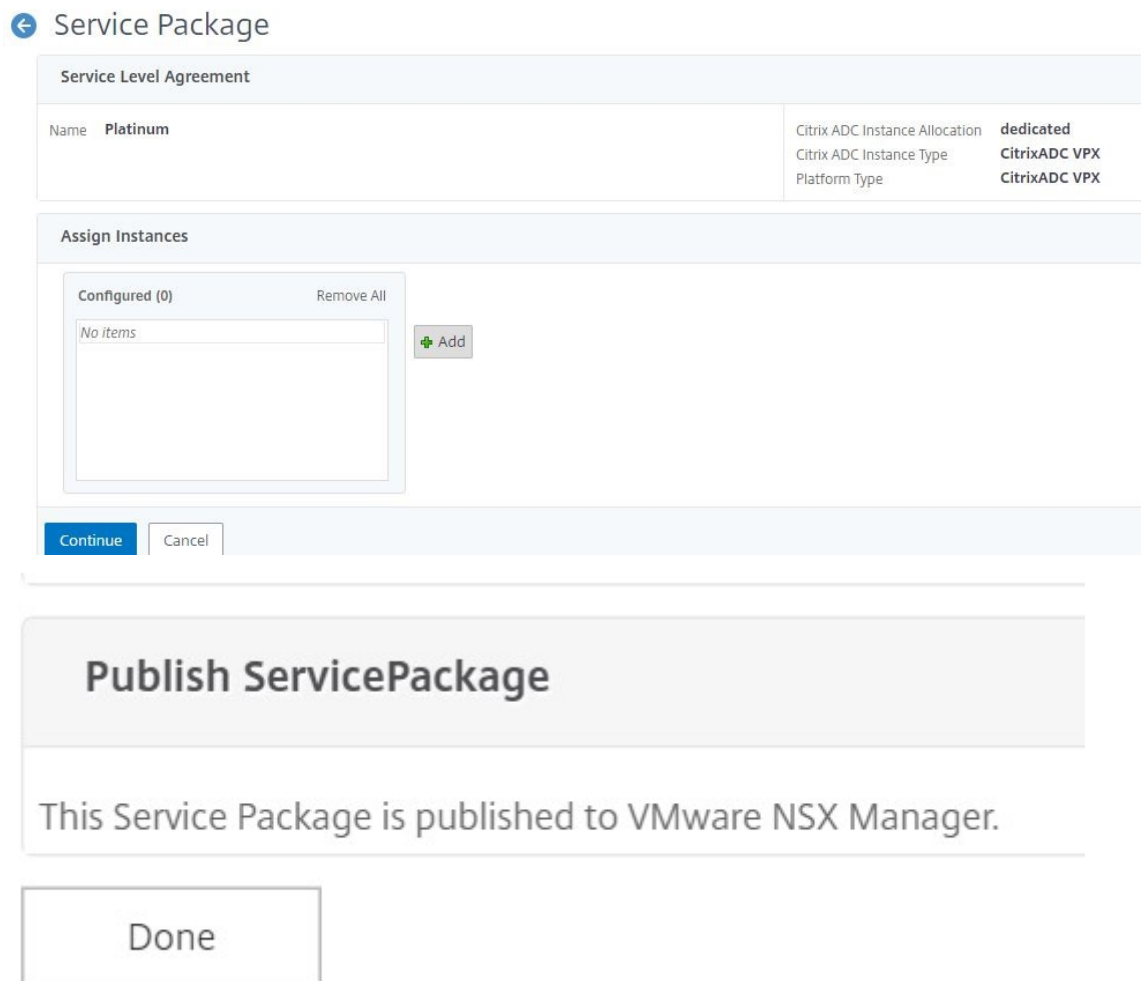
Citrix ADC Instance Provisioning\*

Existing Instance
  Create Instance OnDemand

Citrix ADC Instance Type

CitrixADC VPX
  CitrixADC MPX

3. Dans la section **Affecter des périphériques**, sélectionnez le VPX préconfiguré pour ce package, puis cliquez sur **Continuer**.
4. Dans la section **Publier le service package**, cliquez sur **Continuer** pour publier le service package sur VMware NSX, puis cliquez sur **Terminé**.



Cette procédure configure un package de service dans NSX Manager. Plusieurs périphériques peuvent être ajoutés à un service et plusieurs tronçons peuvent utiliser le même service package pour télécharger l'instance Citrix ADC VPX vers Citrix ADM.

5. Ouvrez une session sur NSX Manager sur vSphere Web Client et accédez à **Définitions de service** > **Services**.

Vous pouvez voir que le package de service Citrix ADM est enregistré.

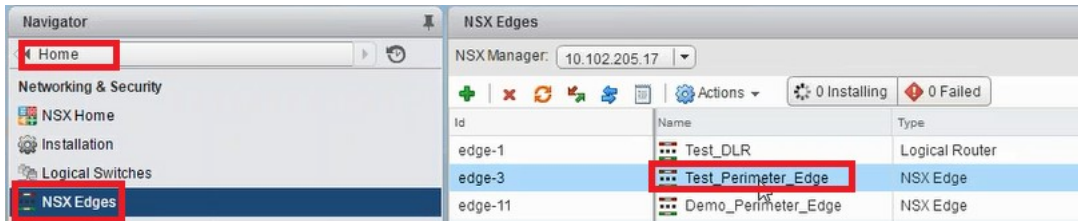




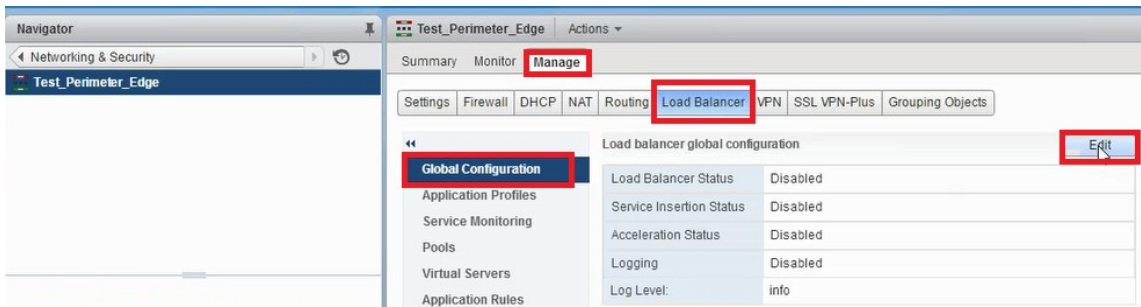
## Exécution de l'insertion du service d'équilibrage de charge pour Edge

Effectuer l'insertion du service d'équilibrage de charge sur la Gateway NSX Edge créée précédemment (déchargez la fonction d'équilibrage de charge de NSX LB vers Citrix ADC).

1. Dans NSX Manager, accédez à **Accueil > NSX Edge**, puis sélectionnez la Gateway périphérique que vous avez configurée.



2. Cliquez sur **Gérer**, puis sur l'onglet **Équilibreur** de charge, sélectionnez **Configuration globale**, puis cliquez sur **Modifier**.



3. Sélectionnez **Activer l'équilibreur** de charge, **Journalisation**, **Activer l'insertion de service** pour les activer.
  - a) Dans **Définition de service**, sélectionnez le package de service qui a été créé dans Citrix ADM et publié sur NSX Manager.



4. Sélectionnez les cartes réseau d'exécution existantes et cliquez sur l'icône Modifier pour modifier les cartes réseau d'exécution qui doivent être connectées lorsque Citrix ADC VPX est alloué.

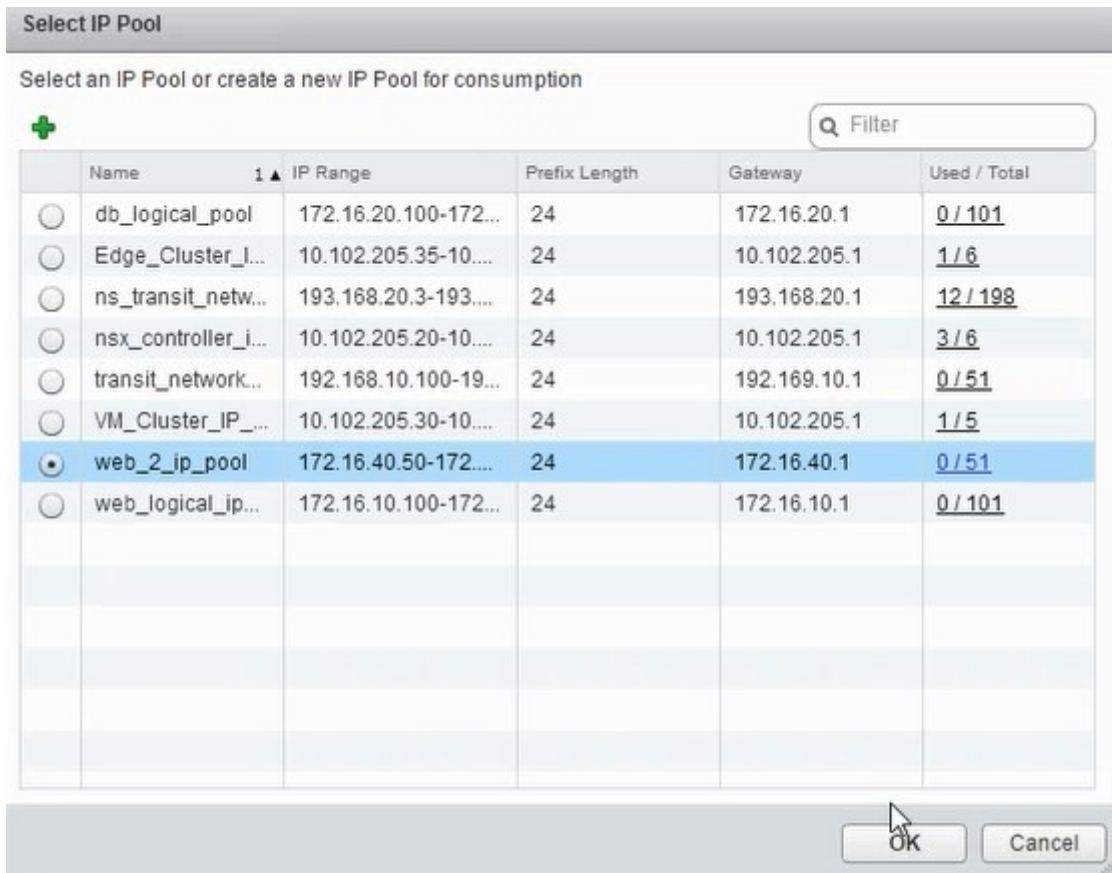
Name	Connected To	ConnectivityType	IP Address	Subnet Mask	Gateway Address
mgmt_if					10.102.205.102
transit_if	Web_2_logical_net	Data	172.16.40.102	255.255.255.0	172.16.40.102
vnic2					
vnic3					

5. Modifiez le nom de la carte réseau, spécifiez le type de connectivité en tant que **données**, puis cliquez sur **Modifier**.

6. Sélectionnez le commutateur logique Web approprié.

7. Dans le **mode d'allocation IP primaire**, sélectionnez Pool IP dans la liste déroulante, puis cliquez sur le bouton flèche vers le bas dans le champ Pool IP.

8. Dans la fenêtre **Sélectionner un pool d'adresses IP**, sélectionnez le pool d'adresses IP approprié, puis cliquez sur **OK**.

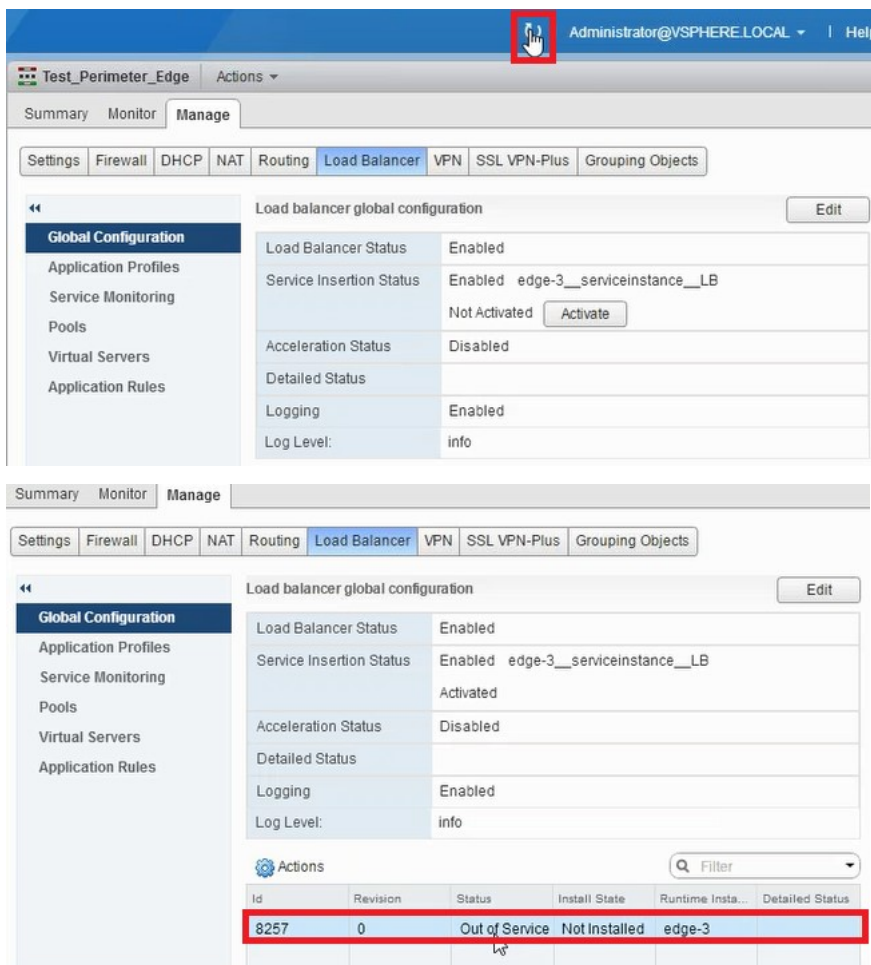


L'adresse IP est acquise et est définie comme adresse IP réseau source dans l'appliance Citrix ADC VPX. Une Gateway L2 est créée dans NSX Manager pour mapper le VXLAN au VLAN.

#### Remarque

Toutes les interfaces de données sont connectées en tant que cartes réseau d'exécution, et elles doivent faire 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**.

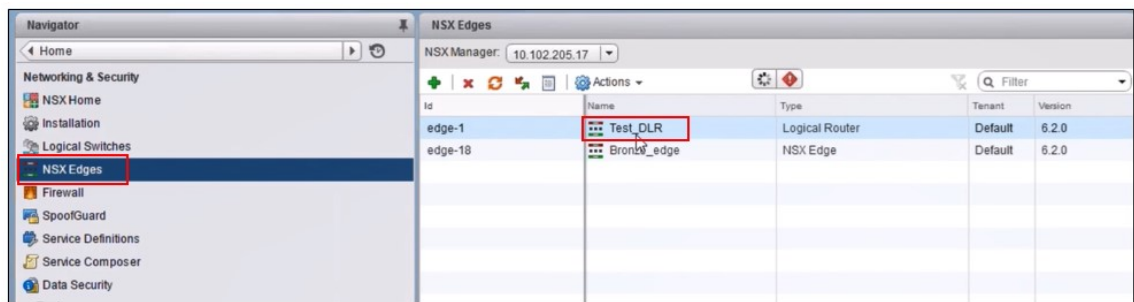
Id	Revision	Status	Install State	Runtime Insta...	Detailed Status
8257	2	In Service	Enabled	vm-267	

### Remarque

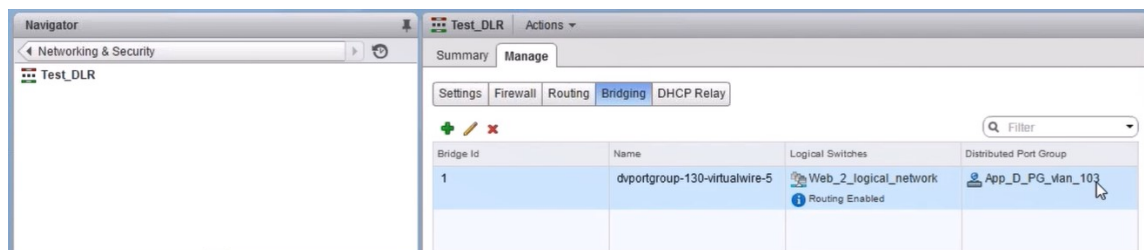
Dans Citrix ADM, accédez à **Orchestration** > **Demandes** pour afficher les détails de progression de l'insertion du service LB.

## Affichage de la passerelle L2 sur NSX Manager

1. Ouvrez une session sur NSX Manager sur vSphere Web Client, accédez à **NSX Edgeet** sélectionnez le DLR créé.



2. Dans la page DLR, accédez à **Gérer > Bridging**. Vous pouvez voir la Gateway L2 affichée dans la liste.

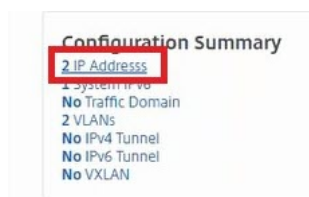


**Remarque**

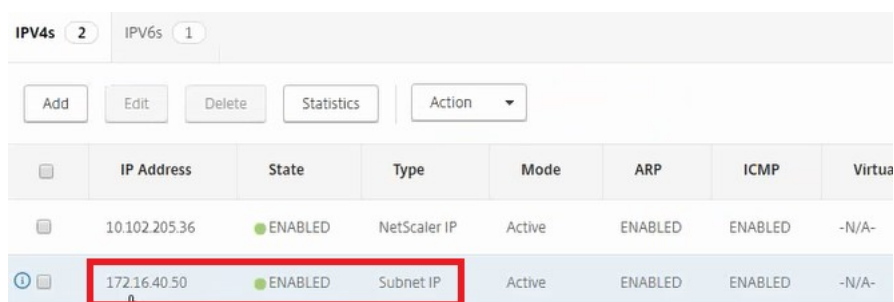
Une Gateway L2 est créée pour chaque interface de données.

**Affichage de Citrix ADC alloué**

1. Ouvrez une session sur l'instance Citrix ADC VPX à l'aide de l'adresse IP affichée dans Citrix ADM. Ensuite, accédez à **Configuration > Système > Mise en réseau**. Dans le volet droit, vous pouvez voir que les deux adresses IP sont ajoutées. Cliquez sur le lien hypertexte de l'adresse IP pour afficher les détails.



L'adresse IP du sous-réseau est identique à l'adresse IP de l'interface Web ajoutée dans le NSX.



2. Accédez à **Configuration > Système > Licences** pour afficher les licences appliquées à cette instance.

### Configuration d'une instance Citrix ADC VPX à l'aide de Stylebook

1. Dans Citrix ADM, accédez à **Orchestration > SDN Orchestration > Configurer NSX Manager > Edge Gateways**.

Notez l'adresse IP de l'instance Citrix ADC qui est allouée à la passerelle Edge respective sur laquelle la configuration d'équilibrage de charge via Stylebooks doit être appliquée.

2. Créez un nouveau Stylebook. Accédez à **Applications > Configuration**, importez le StyleBook et sélectionnez-le dans la liste.

Pour créer un nouveau livre de styles, voir [Créer votre propre livre de styles](#).

3. Spécifiez des valeurs pour tous les paramètres requis.

The screenshot shows the 'Application Configuration / Choose StyleBook / Deploy Configuration' form in Citrix ADM. The form is divided into several sections:

- Basic Configuration:**
  - Load Balanced Application Name\*: web\_app
  - Load Balanced App Virtual IP address\*: 172 . 16 . 40 . 100
  - Application Servers IP Addresses\*: 172 . 16 . 40 . 21 and 172 . 16 . 40 . 22
  - Application Server Port\*: 80
- Advanced Load Balancer Settings:**
  - Load Balanced App Virtual Port\*: 80
  - Load Balanced App Persistence Type: SOURCEIP
  - Load Balanced App Algorithm: LEASTCONNECTION
  - Load Balanced App Client Timeout: (empty field)
- Advanced Application Server Settings:**
  - Service Group UseProxyPort: (empty dropdown)
  - Service Group CIP: (empty dropdown)
  - Preserve Client Source IP (USIP): (empty dropdown)
  - Service Group CIP Header: (empty field)

4. Spécifiez l'instance Citrix ADC VPX sur laquelle vous souhaitez exécuter ces paramètres de configuration.

The screenshot shows the 'Advanced Configurations' dialog box. The 'Target Instance' field is highlighted with a red box and contains the text 'Click to select'. Below this field is a 'Dry Run' checkbox. At the bottom of the dialog are 'Create' and 'Close' buttons.



5. Sélectionnez l'instance IP mentionnée précédemment, puis cliquez sur **Sélectionner**.

	IP Address	Host Name	State	Host IP Address	CPU Usage (%)	Memory Usage (%)	Build Version
<input checked="" type="radio"/>	10.102.205.36	--	<span style="color: green;">●</span>	--	0.6	11.85	11.1: Build 39.2.nc

6. Cliquez sur **Créer** pour appliquer la configuration sur le périphérique sélectionné.

Advanced Application Server Settings

Advanced Configurations

Target Instance

10.102.205.36

Dry Run

**Créer** Close

### Affichage de la configuration de l'équilibreur de charge

1. Ouvrez une session sur l'instance Citrix ADC VPX, accédez à **Configuration > Gestion du trafic > Équilibrage de charge** pour afficher le serveur virtuel d'équilibrage de charge créé.

Dashboard Configuration Reporting Documentation Downloads

Traffic Management / Load Balancing

## Load Balancing

**Load Balancing**

The load balancing feature distributes user requests for applications among multiple servers that all host (or mirror) the same application. This feature also provides fault tolerance: when a server that hosts an application becomes unavailable, the feature distributes user requests to other available servers.

To set up load balancing:

- Configure a virtual server.
- Configure a service representing the application running on the server.
- Bind the service to the virtual server.
- Optionally, configure a monitor and bind it to the service.
- Optionally, configure persistence and a load balancing method.

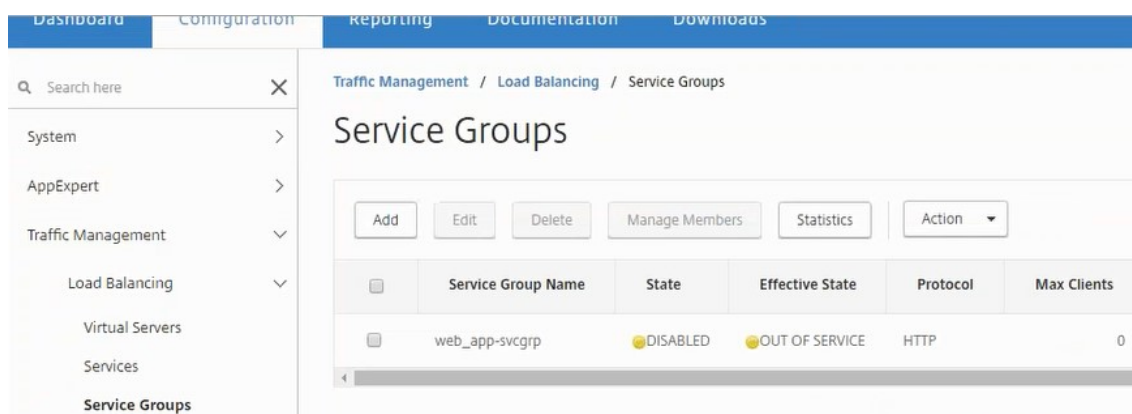
**Settings**

Change SIP settings

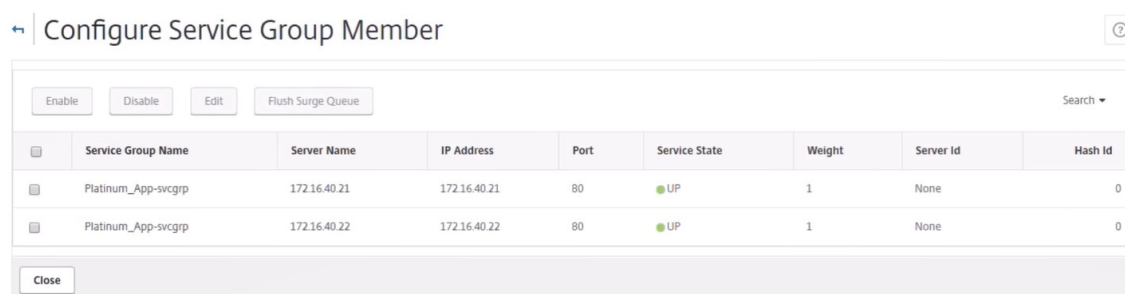
**Configuration Summary**

**1 Load Balancing Virtual Server**

Vous pouvez également afficher les groupes de services créés.



2. Sélectionnez le groupe de services, puis cliquez sur **Gérer les membres**. La page **Configurer un membre de groupe de services** affiche les membres associés au groupe de services.



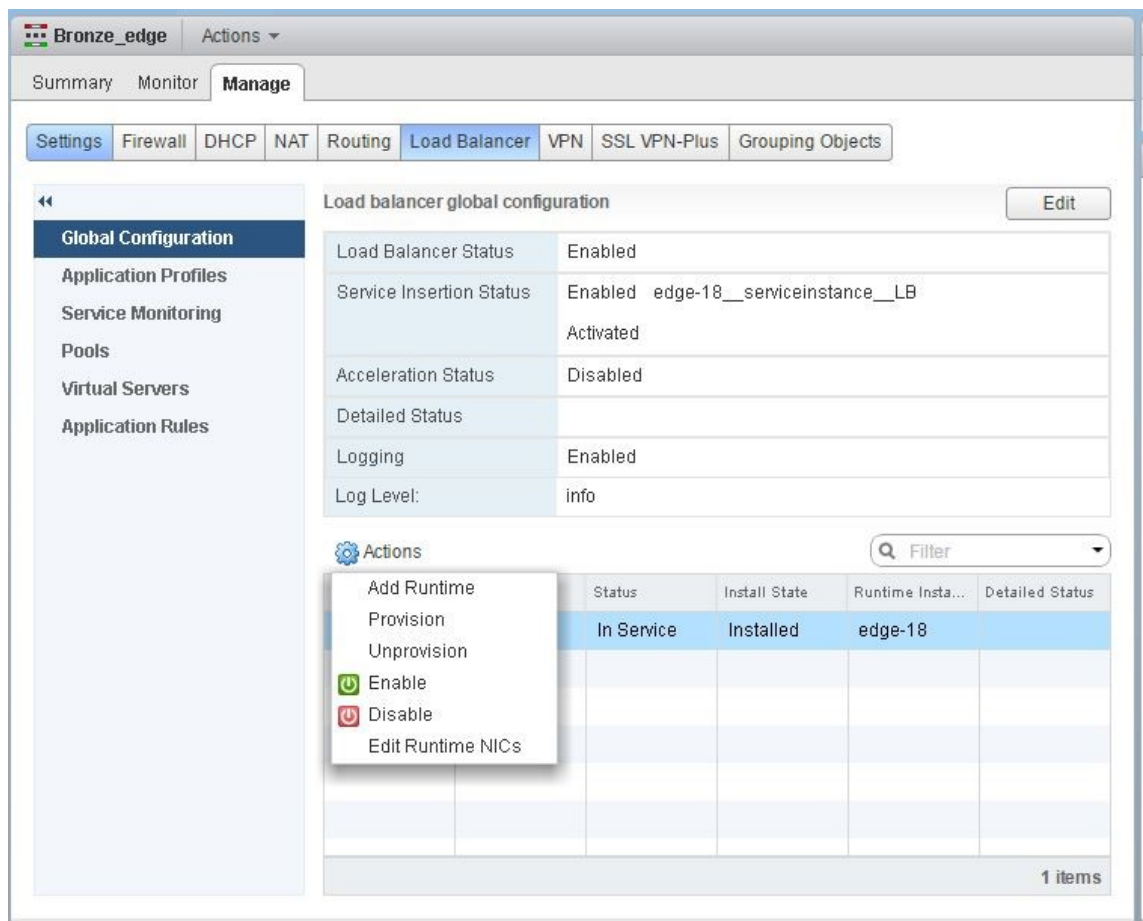
## Suppression du service d'équilibrage de charge

1. Dans Citrix ADM, accédez à **Applications > Configuration**, puis cliquez sur l'icône **X** pour supprimer la configuration de l'application.
2. Ouvrez une session sur NSX Manager sur vSphere Web Client et accédez à la Gateway périphérique à laquelle l'instance Citrix ADC VPX est connectée.
3. Accédez à **Gérer > Équilibreur de charge > Configuration globale**, cliquez avec le bouton droit sur l'entrée d'exécution, puis cliquez sur **Déprovisionner**.

### Remarque Les passerelles

Edge dans NetScaler MAS correspondent aux entrées d'exécution dans le gestionnaire NSX.





L'instance Citrix ADC VPX est rendue hors service.

4. Dans Citrix ADM, accédez à **Orchestration > SDN Orchestration > Configurer NSX Manager > Edge Gateways**. Vérifiez que le mappage respectif de Edge Gateway avec l'instance supprimée n'est pas présent.

## NSX Manager : Provisioning automatique des instances Citrix ADC

February 1, 2024

### Vue d'ensemble

Citrix Application Delivery Management (ADM) s'intègre à la plate-forme de virtualisation réseau VMware pour automatiser le déploiement, la configuration et la gestion des services Citrix ADC. Cette intégration évite les complexités traditionnelles associées à la topologie de réseau physique,

permettant aux administrateurs vSphere/vCenter de déployer par programmation les services Citrix ADC plus rapidement.

Lors de l'insertion et de la suppression du service d'équilibrage de charge sur VMware NSX Manager, Citrix ADM provisionnent et détruit dynamiquement les instances de Citrix ADC. Ce Provisioning dynamique nécessite l'automatisation des attributions de licences Citrix ADC VPX dans Citrix ADM. Lorsque les licences Citrix ADC sont téléchargées vers Citrix ADM, Citrix ADM joue le rôle de serveur de licences.

## Conditions préalables

### Remarque

Cette intégration est prise en charge uniquement pour **VMware NSX for vSphere 6.1 ou version antérieure**.

- Citrix ADM, version 12.1 installation en haute disponibilité et installé sur ESX.
- Citrix ADC VPX, version 12.1
- Licences Citrix ADC VPX pour les instances Citrix ADC VPX, version 12.1
- Installez VMware ESXi version 4.1 ou ultérieure avec du matériel répondant à la configuration minimale requise.
- Installez VMware Client sur une station de travail de gestion qui répond à la configuration système minimale requise.
- Installez VMware OVF Tool (requis pour VMware ESXi version 4.1) sur une station de travail de gestion répondant à la configuration minimale requise.

## Déploiement haute disponibilité des instances Citrix ADM et Citrix ADC

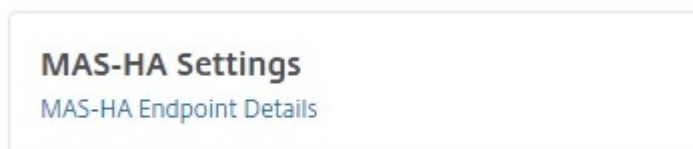
Pour provisionner le programme d'installation de Citrix ADM HA, installez le fichier image Citrix ADM que vous avez téléchargé à partir du site de téléchargement Citrix. Pour plus d'informations sur la façon de configurer Citrix ADM HA, consultez [Déploiement de Citrix ADM en haute disponibilité](#).

## Configuration des détails du point de terminaison Citrix ADM HA

Pour intégrer VMware NSX Manager à Citrix ADM déployé en mode HA, vous devez d'abord entrer l'adresse IP virtuelle de l'instance d'équilibrage de charge Citrix ADC. Vous devez également télécharger le fichier de certificat présent sur le serveur virtuel d'équilibrage de charge de Citrix ADC vers le système de fichiers Citrix ADM.

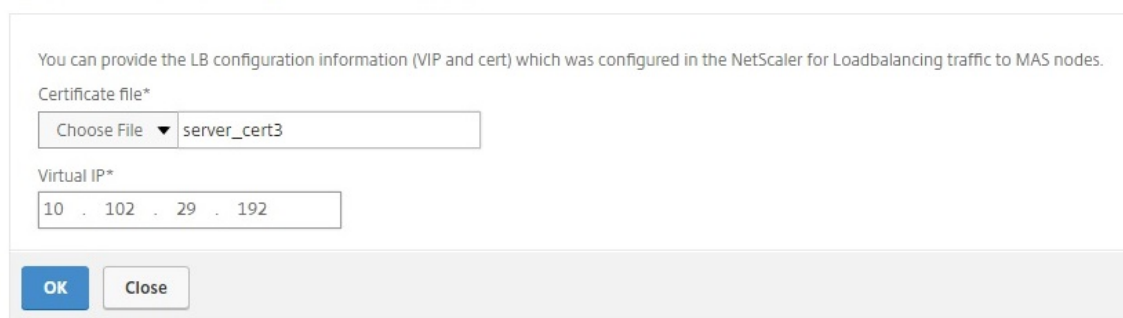
### Pour fournir des informations de configuration d'équilibrage de charge dans Citrix ADM :

1. Dans le nœud Citrix ADM HA, accédez à **Système > Déploiement**.
2. Cliquez sur **Paramètres HA** dans le coin supérieur droit et dans la page **Paramètres MAS-HA**, cliquez sur **Détails du point de terminaison MAS-HA**.



3. Sur la page **Détails du point de terminaison MAS-HA**, téléchargez le même certificat qui est déjà présent sur l'instance d'équilibrage de charge Citrix ADC.
4. Entrez l'adresse IP virtuelle de l'instance d'équilibrage de charge Citrix ADC et cliquez sur **OK**.

### ← MAS-HA Endpoint Details

A screenshot of a configuration form titled "MAS-HA Endpoint Details". It contains a text box for "Certificate file\*" with a "Choose File" button and the text "server\_cert3". Below it is a "Virtual IP\*" text box containing "10 . 102 . 29 . 192". At the bottom are "OK" and "Close" buttons. A note at the top says: "You can provide the LB configuration information (VIP and cert) which was configured in the NetScaler for Loadbalancing traffic to MAS nodes."

## Enregistrement de VMware NSX Manager auprès de Citrix ADM

Lorsque vous configurez deux serveurs Citrix ADM en haute disponibilité, les deux nœuds de serveur sont en mode actif-passif. Ouvrez une session sur le nœud serveur Citrix ADM principal pour enregistrer VMware NSX manager auprès de Citrix ADM dans HA, afin de créer un canal de communication entre eux.

### Pour enregistrer VMware NSX manager auprès de Citrix ADM dans HA :

1. Dans le nœud serveur Citrix ADM principal, accédez à **Orchestration > SDN Orchestration > VMware NSX Manager**.
2. Cliquez sur **Configurer les paramètres de NSX Manager**.
3. Dans la page **Configurer les paramètres de NSX Manager**, définissez les paramètres suivants :
  - a) Adresse IP de NSX Manager : adresse IP de NSX Manager.
  - b) Nom d'utilisateur de NSX Manager - Nom d'utilisateur administratif de NSX Manager.

- c) Mot de passe - Mot de passe de l'utilisateur administratif de NSX Manager.
4. Dans la section Compte Citrix ADM utilisé par NSX Manager, définissez le mot de passe du pilote Citrix ADC pour NSX Manager.
5. Cliquez sur **OK**.

## Télécharger des licences dans Citrix ADM

Téléchargez les licences Citrix ADC VPX vers Citrix ADM, afin que Citrix ADM puisse attribuer automatiquement des licences aux instances pendant l'orchestration avec NSX.

### Pour installer des fichiers de licence sur Citrix ADM :

1. Dans Citrix ADM, accédez à **Réseaux > Licences**.
2. Dans la section **Fichiers de licence**, sélectionnez l'une des options suivantes :
  - a) **Télécharger des fichiers de licences à partir d'un ordinateur local** : si un fichier de licence est déjà présent sur votre ordinateur local, vous pouvez le télécharger sur Citrix ADM. Pour ajouter des fichiers de licence, cliquez sur **Parcourir** et sélectionnez le fichier de licence (.lic) que vous souhaitez ajouter. Cliquez ensuite sur **Terminer**.
  - b) **Utiliser le code** d'accès à la licence : Citrix envoie par e-mail le code d'accès aux licences (LAC) pour les licences que vous achetez. Pour ajouter des fichiers de licence, entrez le LAC dans la zone de texte, puis cliquez sur **Obtenir des licences**.

#### Remarque

À tout moment, vous pouvez ajouter d'autres licences à Citrix ADM à partir des paramètres de licence.

License Server Port Settings

Proxy Server Port <b>0</b>	License Server Port <b>27000</b>
-------------------------------	-------------------------------------

License Files

You must upload the license files to this license server. If a license file is already present on your local computer, you can upload it to this license server, allocate licenses from the Citrix licensing portal.

Upload license files from a local computer  
 Use license access code

License Expiry Information

Feature	Count	Days To Expiry
<i>No items</i>		

## Télécharger des images Citrix ADC VPX dans Citrix ADM

Ajoutez les images Citrix ADC à Citrix ADM afin que Citrix ADM utilise ces images comme défini dans le service package.

### Pour télécharger des images Citrix ADC VPX dans Citrix ADM :

1. Dans Citrix ADM, accédez à **Orchestration > SDN Orchestration > VMware NSX Manager > Images ESX NSVPX**.
2. Cliquez sur **Télécharger**, puis sélectionnez le package zip Citrix ADC VPX dans le dossier de stockage local.

## Création de packages de services dans Citrix ADM

Créez des packages de services dans Citrix ADM pour définir l'ensemble de SLA, qui indique comment les ressources Citrix ADC sont allouées.

### Pour créer des packages de service dans Citrix ADM :

1. Dans Citrix ADM, accédez à **Orchestration > SDN Orchestration > VMware NSX Manager > Service Packages**, puis cliquez sur **Ajouter** pour ajouter un nouveau service package.
2. Dans la page **Service Package**, dans la section **Paramètres de base**, définissez les paramètres suivants :
  - a) Nom : nom d'un package de services
  - b) Stratégie d'isolement - sélectionnez **Dédié**

- c) Provisioning d'instance Citrix ADC - sélectionnez **Créer une instance à la demande**
  - d) Plateforme de provisionnement automatique - sélectionnez **CitrixADC SDX**
  - e) Cliquez sur **Continuer**.
3. Dans la section **Paramètres de provisionnement automatique**, sélectionnez le package zip Citrix ADC VPX récemment téléchargé pour le déployer sur la plate-forme NSX, sélectionnez la licence correspondante, puis cliquez sur **Continuer**.

**Remarque**

Dans **la section Haute disponibilité**, cochez la case pour provisionner les instances Citrix ADC pour HA.

**Auto Provision Settings**

**Resources**

Netscaler VPX Package for ESX\*

NSVPX-ESX-11.1-49.81\_nc.zip ▼

License\*

VPX8000\_Enterprise, 2number ▼

vCPUs\*

2

Memory in MB\*

2048

**High Availability**

A high availability (HA) deployment can provide uninterrupted operation

Provision pair of NetScaler appliances for High Availability.

**Continue** **Cancel**

**Remarque**

Le nom de la licence affiché dans la zone de liste illustrée dans la figure ci-dessus, VPX8000\_Enterprise, 2number est un exemple et est expliqué comme suit :

- VPX - la licence consiste à déployer des instances Citrix ADC VPX
- 8000 - la bande passante consommable est de 8 Go
- Enterprise : Citrix propose trois types de licences : Standard, Enterprise et Platinum

- 2number : deux instances Citrix ADC VPX peuvent être déployées à l'aide de cette licence

Le nom de la licence affichée dans la zone de liste **Licence** dépend de la licence que vous avez achetée auprès de Citrix.

4. Cliquez sur **Continuer**.
5. Le package de services est publié sur NSX Manager. Dans NSX Manager, accédez à **Définitions de service > Gestionnaires de service**. Vous pouvez afficher Citrix ADM comme l'un des gestionnaires de services. Cela indique que l'enregistrement est réussi et que la communication bidirectionnelle est établie entre le gestionnaire NSX et Citrix ADM.

#### Remarque

Pour Citrix ADM en déploiement haute disponibilité, les licences sont chargées uniquement dans le nœud de serveur de licences Citrix ADM. Les nœuds Citrix ADM sont en mode actif-passif.

## Effectuer l'insertion du service d'équilibrage de charge pour Edge

Effectuez l'insertion du service d'équilibrage de charge sur la passerelle NSX Edge existante, c'est-à-dire déchargez la fonction d'équilibrage de charge de l'équilibreur de charge NSX vers Citrix ADC.

### Pour insérer un service d'équilibrage de charge sur NSX Edge Gateway :

1. Dans NSX Manager, accédez à **Accueil > Mise en réseau et sécurité > NSX Edges**, puis double-cliquez pour sélectionner la passerelle Edge que vous avez configurée.
2. Cliquez sur **Gérer**, puis sur l'onglet **Équilibreur** de charge, sélectionnez **Configuration globale**, puis cliquez sur **Modifier**.
3. Sélectionnez **Activer l'équilibreur de charge** et **Activer l'insertion de services** pour les activer.
4. Dans **Définition du service**, sélectionnez le package de service qui a été publié sur NSX Manager.
5. Configurez une carte réseau virtuelle pour l'interface de gestion et une ou plusieurs cartes réseau virtuelles pour les interfaces de données. Sélectionnez les réseaux à gérer et les données en conséquence.

#### Remarque

Sélectionnez l'option Pool IP en mode Allocation IP principale. Citrix ADM ne prend pas en charge l'allocation manuelle ou DHCP des adresses IP.

6. Cliquez sur l'icône d'actualisation pour voir la création de l'heure d'exécution.

**Remarque**

Étant donné que vous déployez deux instances Citrix ADC VPX dans le déploiement HA, deux temps d'exécution sont créés dans le gestionnaire NSX.

Vous devrez peut-être actualiser l'écran pour afficher les temps d'exécution affichés à l'écran.

7. Sélectionnez l'heure d'exécution, cliquez sur **Actions**, puis sélectionnez **Installer** dans le menu contextuel. Pour HA, répétez cette opération pour l'autre temps d'exécution également.
8. Lorsque les deux machines virtuelles démarrent, la valeur de Status passe à « En service » et celle de Install State passe à « Enabled ».

**Remarque**

Vous devrez peut-être actualiser l'écran pour afficher le changement d'état.

9. Dans Citrix ADM, accédez à **Orchestration > Demandes** pour afficher les détails de progression de l'insertion de service. Vous pouvez voir qu'une demande de création et de mise à jour de l'heure d'exécution a été envoyée à Citrix ADM. Lorsque l'heure d'exécution a été mise à jour, sélectionnez la demande et cliquez sur le bouton **Tâches** pour afficher que Citrix ADM a été ajouté dans NSX Manager.

Pour HA, il y aura deux demandes pour créer et mettre à jour deux fois d'exécution dans Citrix ADM. Lorsque les deux temps d'exécution ont été mis à jour, sélectionnez les deux demandes et cliquez sur le bouton **Tâches** pour afficher que deux nœuds Citrix ADM HA ont été ajoutés dans NSX Manager.

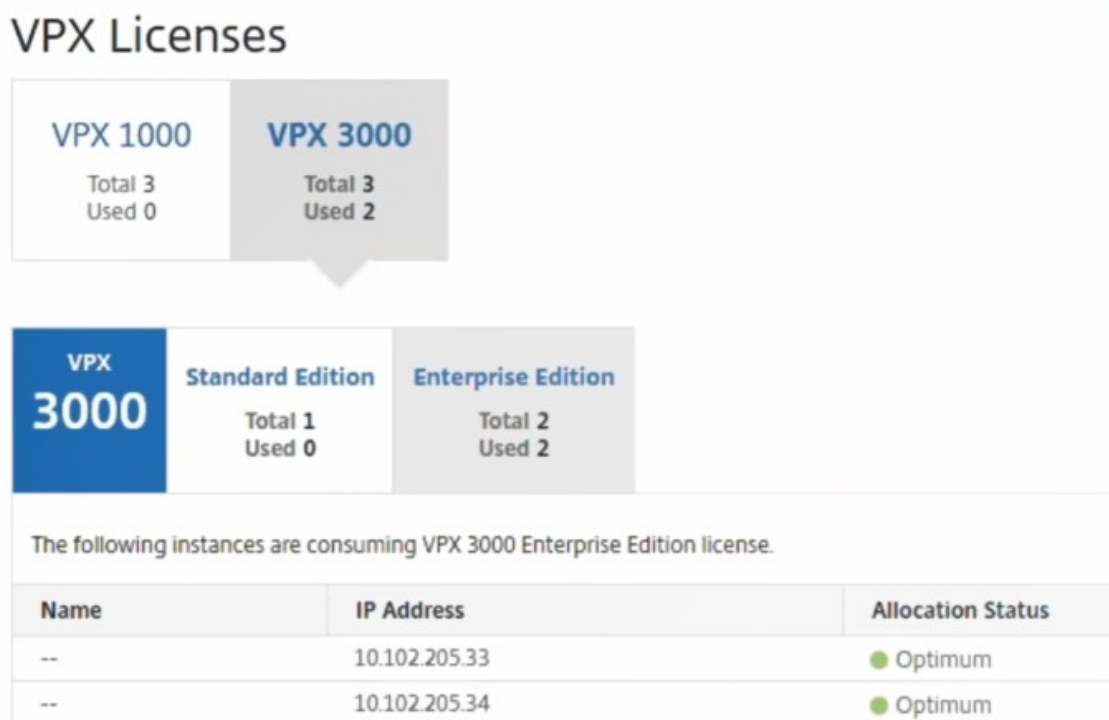
10. Dans Citrix ADM, accédez à **Orchestration > SDN Orchestration > VMware NSX Manager > Edge Gateways**. Dans le panneau de droite, vous pouvez afficher que Citrix ADC VPX a été ajouté à NSX Edge Gateway.

Pour HA, vous pouvez voir que deux instances Citrix ADC VPX en mode HA ont été ajoutées à la passerelle NSX Edge.

11. Dans Citrix ADM, accédez à **Réseaux > Licences > Licences VPX Licences**. Sélectionnez la licence Citrix ADC VPX et l'édition que vous avez installée.

Les instances Citrix ADC VPX qui sont en mode HA consomment deux licences et l'état s'affiche à l'écran comme ci-dessous.





Lorsque l'insertion du service est terminée, vous pouvez utiliser StyleBooks pour configurer les instances Citrix ADC selon l'une des deux méthodes suivantes :

- Configurer les services d'équilibrage de charge sur Citrix ADC VPX dans l'interface graphique de VMware NSX Manager
- Configurer les services d'équilibrage de charge sur Citrix ADC VPX dans l'interface graphique Citrix ADM

### **Configurer les services d'équilibrage de charge sur Citrix ADC 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.

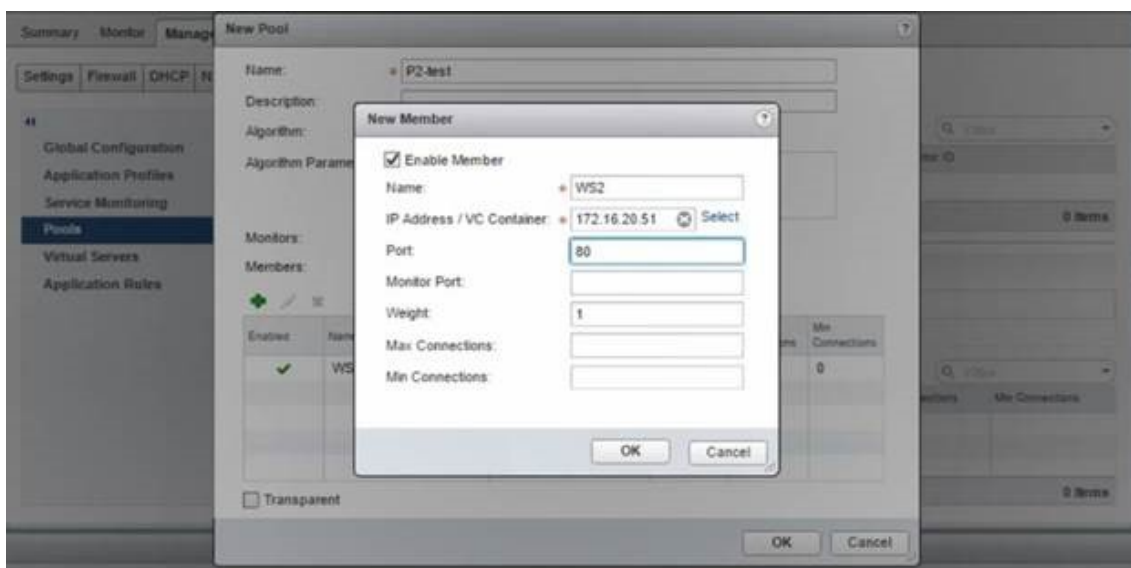
Dans NSX Manager, accédez à **Accueil > Mise en réseau et sécurité > NSX Edges**, puis double-cliquez pour sélectionner la passerelle Edge que vous avez configurée.

#### **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.

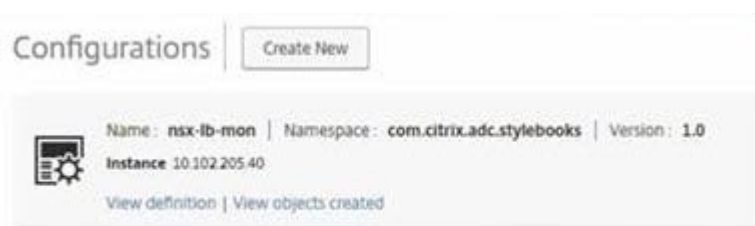


## Créer des serveurs virtuels

Créez un ensemble de serveurs virtuels et attribuez un pool à chaque serveur virtuel.

1. Cliquez sur **Gérer**, puis sur l'onglet Équilibreur de charge, sélectionnez **Serveurs virtuels**, puis cliquez sur l'icône “+” pour ajouter un serveur virtuel et définissez les paramètres suivants :
  - a) Profil d'application : par défaut, le profil de service que vous avez créé dans Citrix ADM s'affiche.

- b) Name : nom du serveur virtuel.
  - c) Adresse IP : cliquez sur Sélectionner pour sélectionner un pool d'adresses IP existant ou créer un nouveau pool d'adresses IP.
  - d) Pool par défaut : sélectionnez le pool par défaut dans la liste déroulante.
2. Cliquez sur **OK**.
  3. Dans Citrix ADM, accédez à **Orchestration > Demandes** pour afficher les détails de l'avancement de la création de service sur une ou plusieurs instances Citrix ADC sélectionnées.
  4. Dans Citrix ADM, accédez à **Applications > Configuration** et vérifiez que le pack de configuration « nsx-lb-mon » a été créé.



## Configurer les services d'équilibrage de charge sur Citrix ADC VPX dans l'interface graphique Citrix ADM

Déployez des configurations d'équilibrage de charge sur l'instance Citrix ADC à l'aide de Citrix ADM StyleBooks. Pour HA, la configuration est déployée sur les deux instances Citrix ADC qui sont en HA.

### Pour créer des packs de configuration via StyleBooks :

1. Dans Citrix ADM, accédez à **Applications > Configuration > Créer un nouveau**, puis sélectionnez le **StyleBook HTTP/SSL LoadBalancing (with Monitors)** dans la liste. Le StyleBook s'ouvre en tant que page d'interface utilisateur sur laquelle vous entrez les valeurs de tous les paramètres définis dans ce StyleBook.
2. Spécifiez des valeurs pour tous les paramètres requis.
3. Sélectionnez l'instance Citrix ADC VPX cible qui est provisionnée dans l'environnement NSX, puis cliquez sur **Créer** pour appliquer la configuration sur le périphérique sélectionné. Pour le déploiement HA, sélectionnez les instances en mode HA.

## Vérifier la création de serveurs virtuels et de groupes de services dans les instances Citrix ADC VPX

Vous pouvez voir que les groupes de services et les serveurs virtuels sont créés en vous connectant à l'instance Citrix ADC VPX.

### Pour afficher les groupes de services et les serveurs virtuels :

1. Ouvrez une session sur l'instance Citrix ADC VPX. Pour le déploiement HA, vous devez ouvrir une session sur les deux instances Citrix ADC qui sont en HA.
2. Accédez à **Configuration > Système > Mise en réseau**. Dans le volet droit, vous pouvez voir les adresses IP ajoutées. Cliquez sur le lien hypertexte de l'adresse IP pour afficher les détails. Vous pouvez constater que l'adresse IP du sous-réseau est identique à l'adresse IP de l'interface Web ajoutée dans NSX.
3. Accédez ensuite à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels** et affichez les détails du serveur virtuel.
4. Accédez ensuite à **Groupes de services et affichez** les détails des groupes de services.
5. Enfin, accédez à **Configuration > Système > Licences** pour afficher les licences appliquées à cette instance.

### Supprimer les services d'équilibrage de charge

Lorsque les services d'équilibrage de charge ne sont plus requis sur les instances Citrix ADC VPX déployées sur le gestionnaire NSX, vous pouvez supprimer les insertions de service effectuées précédemment.

### Pour supprimer la configuration et l'insertion de service :

1. Dans Citrix ADM, accédez à **Applications > Configuration**, sélectionnez la configuration de l'application créée, puis supprimez la configuration en cliquant sur l'icône « X ».
2. Dans NSX Manager, accédez à la Gateway périphérique à laquelle l'instance Citrix ADC VPX est connectée. Accédez à **Gérer > Équilibreur de charge Configuration globale**, cliquez avec le bouton droit sur l'entrée d'exécution, puis cliquez sur **Déprovisionner**. La machine virtuelle est rendue hors service.
3. Dans Citrix ADM, accédez à **Orchestration > Cloud Orchestration > Edge Gateways**. Vérifiez que le mappage respectif de la Gateway Edge à l'instance supprimée ne doit pas être présent.

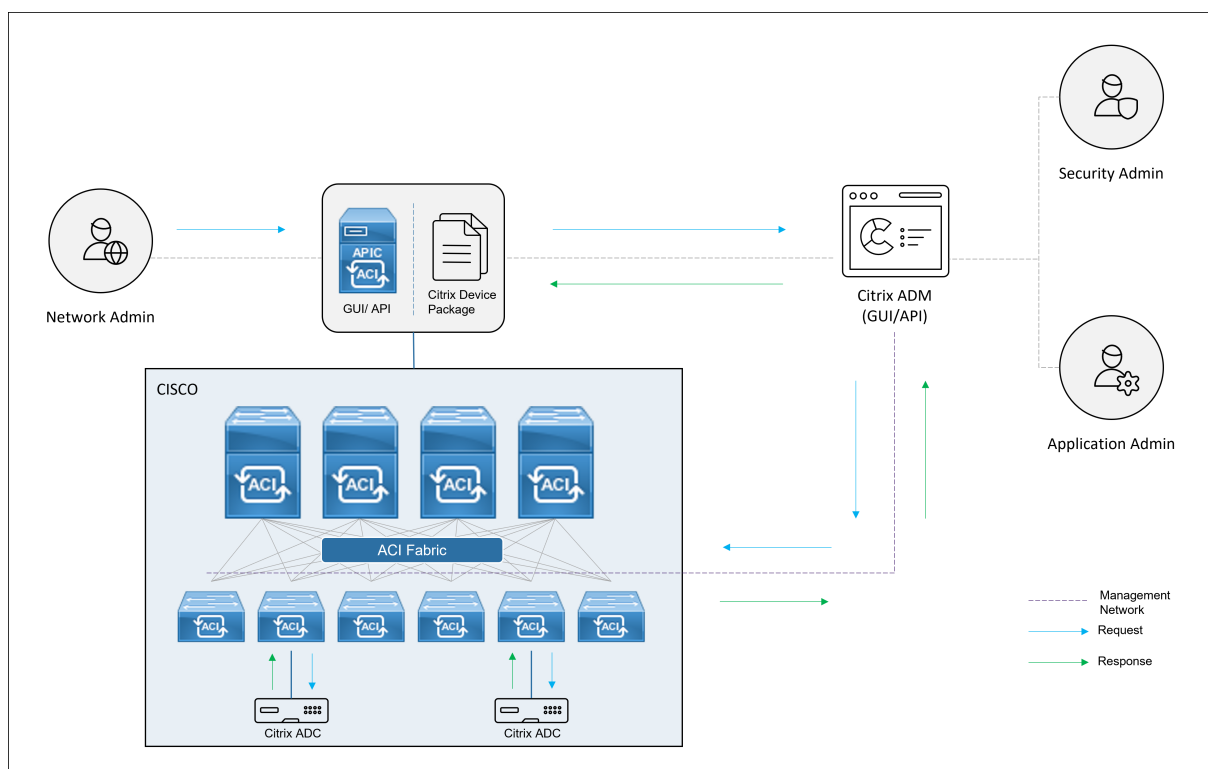
## Automatisation Citrix ADC à l'aide de Citrix ADM en mode hybride ACI Cisco

February 1, 2024

Cisco ACI a introduit la prise en charge du mode hybride dans la version 1.3 (2f). En mode hybride, vous pouvez automatiser le réseau via l'Application Policy Infrastructure Controller (APIC), tout en déléguant la configuration L4-L7 à Citrix Application Delivery Management (ADM), qui agit en tant que gestionnaire de périphériques dans l'APIC.

La solution Citrix ADC Hybrid Mode est prise en charge par un package de périphériques en mode hybride et Citrix ADM. Vous devez télécharger le package de périphérique en mode hybride dans l'APIC. Ce package fournit toutes les entités configurables réseau L2-L3 à partir de Citrix ADC. La parité des applications est mappée par StyleBook de Citrix ADM à l'APIC. En d'autres termes, StyleBook sert de référence entre les configurations L2-L3 et L4-L7 pour une application donnée. Vous devez fournir un nom StyleBook lors de la configuration des entités réseau à partir de l'APIC pour Citrix ADC.

L'illustration suivante fournit une vue d'ensemble de Citrix ADC dans une solution en mode hybride :



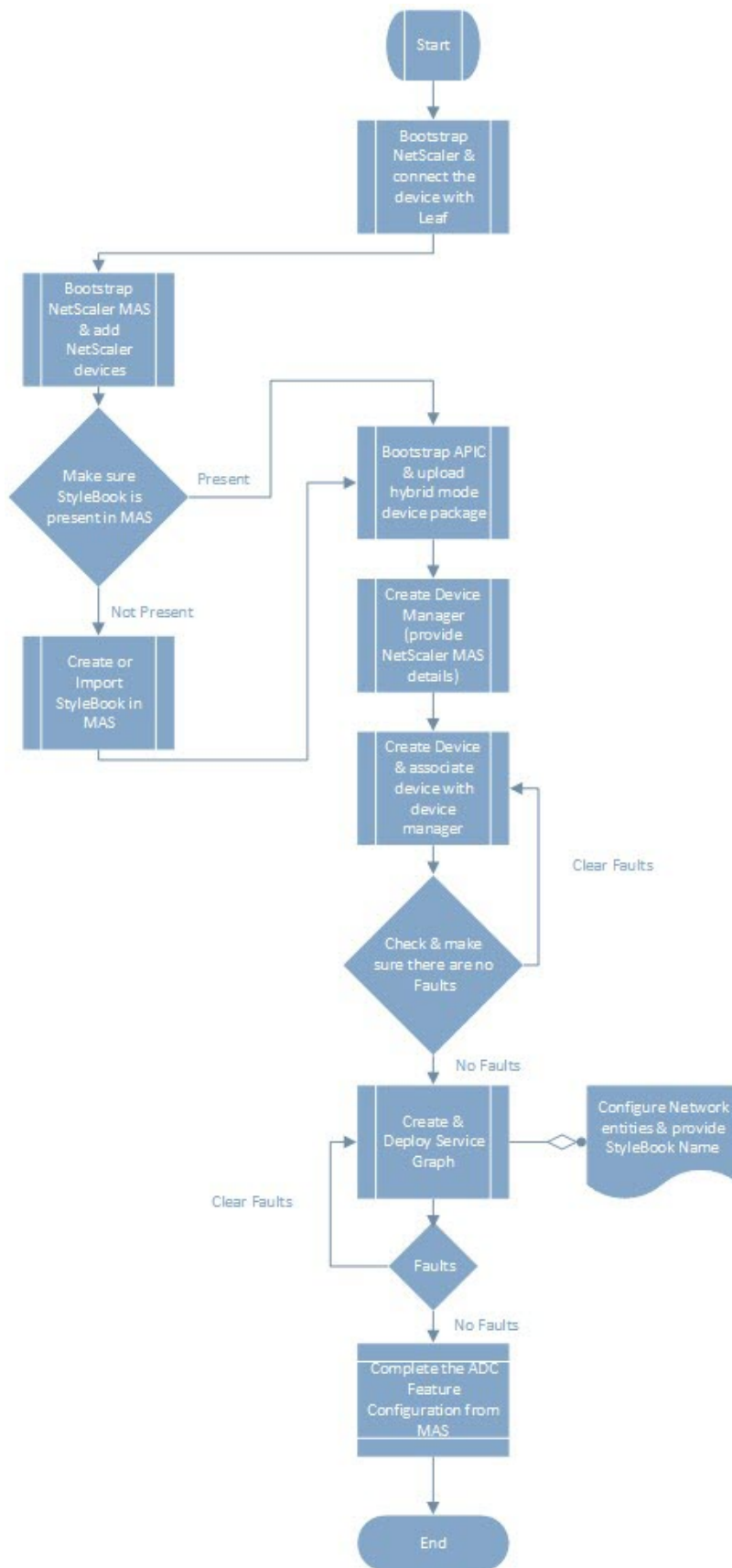
En mode hybride, la configuration de Citrix ADC est effectuée dans les deux phases suivantes :

1. L'assemblage du réseau est effectué à partir du Cisco APIC

## 2. La configuration est effectuée à partir de Citrix ADM

Pour toute application donnée, un administrateur réseau doit fournir des détails spécifiques au réseau, tels que les adresses IP, le port, le VLAN (automatisé), etc., dans le cadre de la création et du déploiement du graphique de service dans l'APIC Cisco. Ces détails de configuration sont ensuite transmis à Citrix ADM via le package de l'appareil, et Citrix ADM les traite en interne et configure le Citrix ADC. Un administrateur d'application crée la configuration liée à l'ADC de l'application à l'aide de StyleBook dans Citrix ADM, puis ces configurations sont transmises de Citrix ADM vers Citrix ADC. Le Cisco APIC et le Citrix ADM communiquent avec l'ADC via le réseau de gestion.

Le diagramme suivant montre un flux de travail Citrix ADC dans la solution hybride :



## Conditions préalables

February 1, 2024

Assurez-vous que :

- Vous avez une connaissance conceptuelle des composants Cisco ACI et des Citrix ADC.
  - Pour plus d'informations sur Cisco ACI et ses composants, consultez la documentation produit à l'adresse suivante :<http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html>.
  - Pour plus d'informations sur les Citrix ADC, consultez la documentation produit Citrix ADC à l'adresse :<http://docs.citrix.com/>.
- Tous les composants requis de Cisco ACI, y compris un Cisco APIC dans le centre de données, sont configurés et configurés. Pour plus d'informations sur Cisco ACI et ses composants, consultez la documentation produit à l'adresse suivante :<http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html>.
- Vous avez installé Citrix ADC 11.1 ou version ultérieure.
- Vous avez configuré les Citrix ADC dans Cisco ACI afin qu'ils puissent être gérés à l'aide de l'APIC Cisco.
- Vous avez déployé Citrix Application Delivery Management (ADM) dans votre environnement. Pour plus d'informations, consultez [Citrix ADM 12.1](#).
- La connectivité de gestion d'APIC à Citrix ADM et ADC est établie.
- Prenez note de :
  - Interfaces de connexion et adresses IP utilisées pour la gestion et la connectivité des chemins de données.
  - Détails du commutateur Leaf-switch : adresses IP Citrix ADC, ports, interfaces, etc.

### Remarque

Dans cette version, la solution en mode hybride prend en charge Citrix ADC dans un contexte unique, c'est-à-dire que les partitions d'administration ne sont pas prises en charge.



## Configurer Citrix ADC en mode hybride à l'aide de Cisco APIC et Citrix ADM

February 1, 2024

Effectuez les tâches suivantes pour configurer un Citrix ADC en mode hybride à l'aide de Cisco APIC et de Citrix Application Delivery Management (ADM) :

1. Ajoutez des instances Citrix ADC dans votre structure à Citrix ADM. Pour obtenir des instructions, consultez la section [Ajout d'une instance à Citrix ADM](#).
2. Utilisez Citrix ADM pour créer un StyleBook pour l'application. Pour obtenir des instructions, consultez [Création d'un StyleBook pour l'application à l'aide de Citrix ADM](#).
3. Importez le package de périphériques en mode hybride Citrix ADC dans Cisco APIC. Pour obtenir des instructions, reportez-vous à la section [Importation du package de périphériques en mode hybride Citrix ADC dans Cisco APIC](#)
4. Ajoutez Citrix ADM en tant que gestionnaire de périphériques dans l'APIC Cisco. Pour obtenir des instructions, reportez-vous à la section [Ajout de Citrix ADM en tant que gestionnaire de périphériques dans Cisco APIC](#)
5. Utilisez Cisco APIC pour ajouter un périphérique Citrix ADC dans Cisco ACI. Pour obtenir des instructions, reportez-vous à la section [Ajout de Citrix ADC en tant que périphérique dans Cisco ACI](#)
6. Créez et déployez un modèle de graphe de service. Pour obtenir des instructions, consultez [Création et déploiement d'un graphique de service](#)
7. Configurez les paramètres L4-L7 à l'aide de StyleBook dans Citrix ADM. Pour obtenir des instructions, voir [Configurer le paramètre L4-L7 à l'aide de StyleBook à partir de Citrix ADM](#)
8. Attacher ou détacher les événements de point de terminaison de l'APIC Cisco. Pour plus d'informations, consultez [Attachement ou détachement d'événements de point de terminaison d'APIC](#)

## Créer un StyleBook pour une application à l'aide de Citrix ADM

February 1, 2024

Un StyleBook est un modèle de configuration que vous pouvez utiliser pour créer et gérer des configurations Citrix ADC pour n'importe quelle application. Vous pouvez créer un StyleBook pour configurer

une fonctionnalité Citrix ADC spécifique, telle que l'équilibrage de charge, le déchargement SSL ou la commutation de contenu. Vous pouvez concevoir un StyleBook pour créer des configurations pour un déploiement d'application d'entreprise tel que Microsoft Exchange ou Lync. Pour plus d'informations, consultez [StyleBooks](#).

Vous pouvez créer votre propre StyleBook pour votre application ou modifier et utiliser l'APIC-HTTP-LB StyleBook fourni avec Citrix Application Delivery Management (ADM).

Pour créer votre propre StyleBook pour votre application dans Citrix ADM, consultez [Comment créer vos propres StyleBooks](#).

Lors de la création du StyleBook, assurez-vous de suivre le modèle de graphe de service de l'APIC dans le StyleBook. En d'autres termes, le graphique de service de l'APIC pour n'importe quelle application suit le modèle du consommateur et du fournisseur connectés via une fonction ADC. Le consommateur et le fournisseur sont représentés sous la forme d'un groupe terminal (EPG) et entretiennent une relation individuelle. Le même modèle doit également être suivi dans StyleBook, où le fournisseur EPG doit être représenté en tant que groupe de services et chaque point final en tant que membre du groupe de services. Le nœud de fonction ADC doit être représenté par un serveur virtuel (par exemple, un serveur virtuel d'équilibrage de charge) et il doit exister une relation 1:1 entre le serveur virtuel et le groupe de services.

Cela capture essentiellement l'essence du graphe de service et vous permet de gérer l'événement d'attachement ou de détachement depuis l'APIC, où un événement d'attachement lie le point final au groupe de services correspondant et un événement de détachement le dissocie. Vous devez vous assurer que le graphique de service et le StyleBook sont identiques pour une automatisation fluide des configurations réseau L2-L3 aux configurations L4-L7 dotées de fonctionnalités ADC.

## Importer le package de périphériques en mode hybride Citrix ADC dans Cisco APIC

February 1, 2024

Le package de périphériques en mode hybride est un package léger comparé à un mode entièrement géré. Seuls les paramètres réseau L2-L3 sont disponibles via le modèle de périphérique. Le modèle de périphérique ne comporte qu'une seule fonction ADC générique définie, et quatre profils de fonctions basés sur le déploiement de Citrix ADC dans la structure (par exemple, un bras et deux bras et le même avec RHI). Le nom du package Périphérique en mode **hybride est NetScaler Hybrid Mode Device package 12.0 Build 56.20**. Recherchez le package d'appareils en mode hybride sur le [site de téléchargement Citrix](#), téléchargez-le et importez le package d'appareils dans l'APIC.

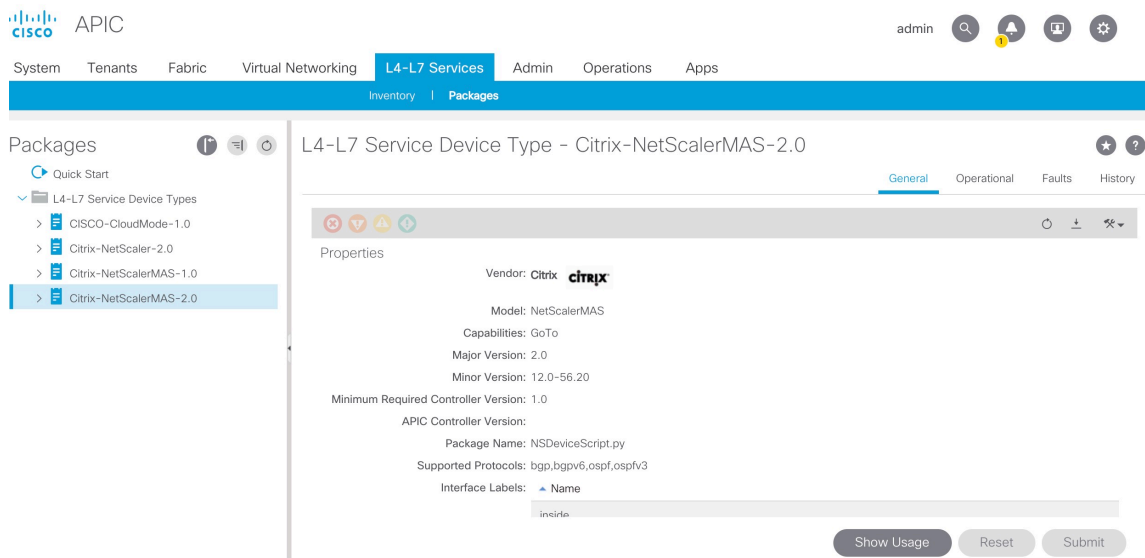
### Remarque

L'ensemble de dispositifs en mode hybride peut coexister avec un ensemble de dispositifs en mode entièrement géré.

### Pour importer le package de périphériques en mode hybride dans l'APIC à l'aide de l'interface graphique APIC, procédez comme suit :

1. Dans la barre de menu, cliquez sur l'onglet **Services L4-L7** et sélectionnez le panneau **Packages**.
2. Dans le volet de **navigation**, cliquez avec le bouton droit sur **Types de périphériques L4-L7** et sélectionnez **Importer un package de périphériques**.
3. Dans la boîte de dialogue **Importer le package de périphériques**, cliquez sur **Parcourir** pour sélectionner le package de périphériques en mode hybride Citrix ADC téléchargé.
4. Cliquez sur **Envoyer**.

Après avoir importé avec succès le package de périphériques dans l'APIC, dans le volet de **navigation**, vous pouvez afficher les détails du package de périphériques en cliquant sur le nom de l'appareil.



### Important

Après avoir importé le package de l'appareil, assurez-vous que l'APIC ne présente aucun défaut. Vous pouvez afficher les défauts en cliquant sur l'onglet **Défauts** dans la fenêtre Types de périphériques.

## Ajouter Citrix ADM en tant que gestionnaire de périphériques dans Cisco APIC

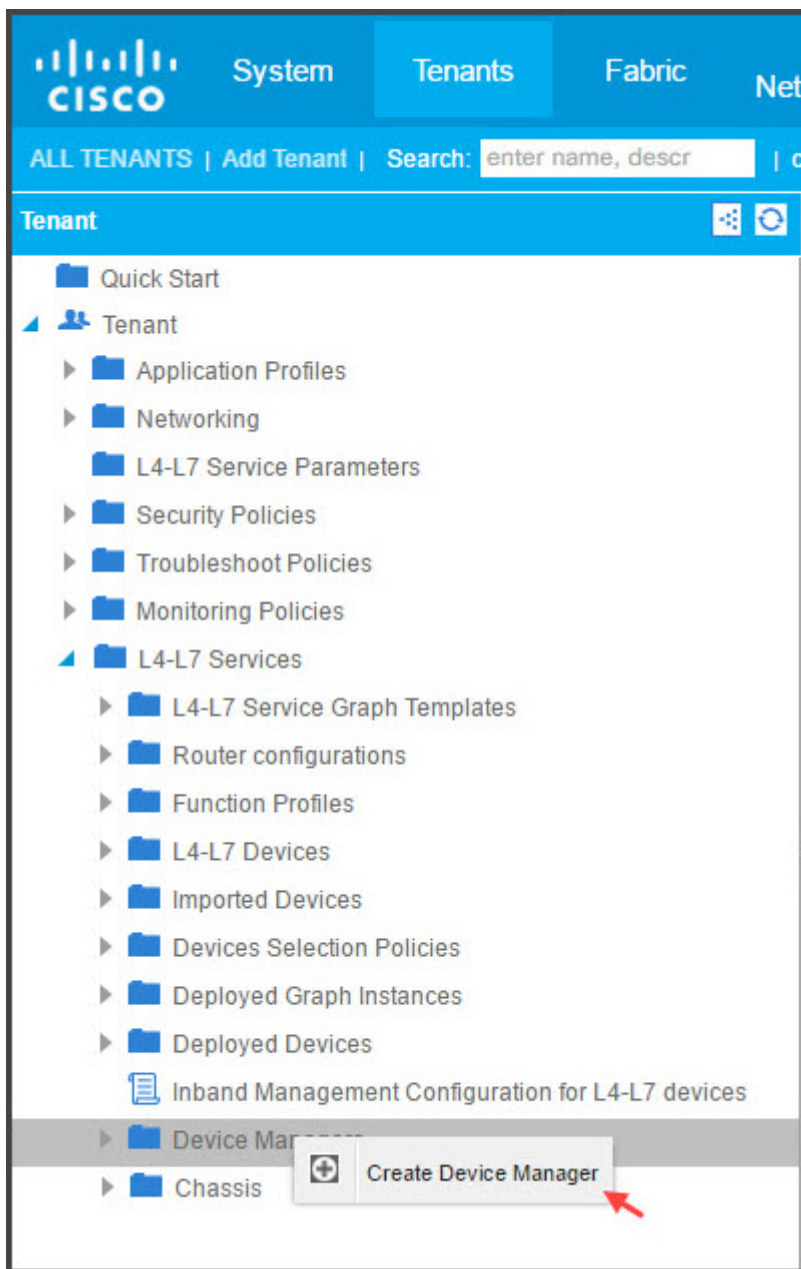
February 1, 2024

24 mai 2018

Citrix Application Delivery Management (ADM) agit en tant que gestionnaire de périphériques centralisé pour Citrix ADC déployé sur Cisco ACI. Vous devez ajouter Citrix ADM en tant que gestionnaire de périphériques dans l'APIC Cisco.

**Pour ajouter Citrix ADM en tant que gestionnaire de périphériques dans l'APIC à l'aide de l'interface graphique APIC :**

1. Dans la barre de menus, accédez à **Locataires > Tous les Locataires**.
2. Dans le volet **Travail**, double-cliquez sur le nom du locataire.
3. Dans le volet de **navigation**, sélectionnez **\*tenant\_name\* > Services L4-L7**.
4. Cliquez avec le bouton droit sur **Gestionnaires de périphériques**, puis cliquez sur **Créer un gestionnaire de périphériques**.



5. Dans la boîte de dialogue **Créer le Gestionnaire de périphériques**, procédez comme suit :
  - a) Dans le champ **Nom du Gestionnaire de périphériques**, entrez un nom pour le déploiement Citrix ADM que vous souhaitez enregistrer en tant que gestionnaire de périphériques.
  - b) Dans la liste déroulante **Gestion EPG**, sélectionnez l'EPG de gestion.
  - c) Dans la liste déroulante **Type de Gestionnaire de périphériques**, sélectionnez **Citrix-DevMGR-1.0**.
  - d) Dans le champ **Gestion**, cliquez sur + et ajoutez les détails de l'adresse IP et du port du

déploiement Citrix ADM.

- e) Dans le champ **Nom d'utilisateur**, entrez le nom d'utilisateur pour accéder à Citrix ADM.
- f) Dans les champs **Mot de passe** et **Confirmer le mot** de passe, entrez le mot de passe pour accéder à Citrix ADM.
- g) Cliquez sur **SUBMIT**.

**Create Device Manager**

Please enter device manager info below.

Device Manager Name: MAS1

Management EPG: select an option  
This is required only for inband management.

Device Manager Type: Citrix-DevMgr-1.0

Management:

Host	Port
10.102.102.21	80

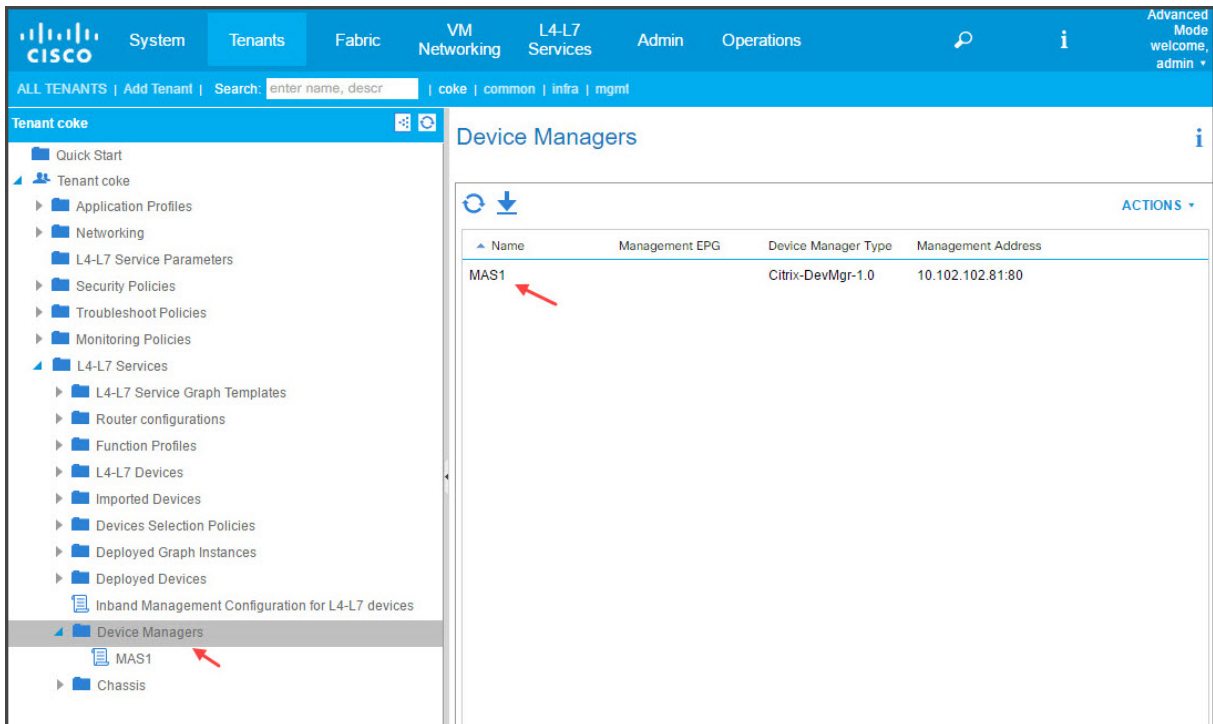
Username: nsroot

Password: .....

Confirm Password: .....

**SUBMIT** **CANCEL**

Une fois que Citrix ADM est correctement enregistré en tant que gestionnaire de périphériques dans l'APIC, le gestionnaire de périphériques est ajouté et s'affiche dans le volet de **navigation**. Pour afficher le gestionnaire de périphériques enregistré, dans le volet de navigation, accédez à **\*nom\_tenant\*** > **Services L4-L7 > Gestionnaire de périphériques**.



**Remarque**

Assurez-vous qu'il n'y a aucun problème de connectivité entre l'APIC Cisco et Citrix ADM et que vous fournissez les mêmes informations d'identification que vous utilisez pour accéder à Citrix ADM. Assurez-vous également que le compte dispose de privilèges d'administrateur.

**Important**

Après avoir importé le package de l'appareil, assurez-vous que l'APIC ne présente aucun défaut. Vous pouvez afficher les défauts en cliquant sur l'onglet **Défauts** dans la fenêtre Types de périphériques.

Vous pouvez également enregistrer Citrix ADM en tant que gestionnaire de périphériques à l'aide d'API. Voici un exemple de charge utile XML qui montre comment vous pouvez utiliser des API pour ajouter Citrix ADM en tant que gestionnaire de périphériques.

```

1 <polUni>
2   <fvTenant name="coke">
3     <vnsDevMgr name="MAS1">
4       <vnsRsDevMgrToMDevMgr tDn="uni/infra/mDevMgr-Citrix-DevMgr
-1.0" />
5       <vnsCMgmts name="devMgmt" host="10.102.102.81" port="80"/>
6       <vnsCCred name="username" value="nsroot"/>
7       <vnsCCredSecret name="password" value="*****"/>
8     </vnsDevMgr>
9   </fvTenant>
10 </polUni>

```

## Ajouter Citrix ADC en tant que périphérique dans Cisco ACI à l'aide d'APIC

February 1, 2024

Vous devez ajouter un Citrix ADC en tant que périphérique L4-L7 à l'APIC pour l'automatisation du réseau. L'APIC effectue l'assemblage réseau entre Leaf et le périphérique Citrix ADC, en fonction du graphique de service déployé. Vous devez configurer les paramètres de base de la configuration du périphérique, tels que les adresses IP de gestion de la configuration, le gestionnaire de périphériques et les informations d'identification.

### Pour enregistrer le Citrix ADC en tant que périphérique dans l'APIC à l'aide de l'interface graphique APIC :

1. Dans la barre de menus, accédez à **Locataires > Tous les Locataires**.
2. Dans le volet **Travail**, double-cliquez sur le nom du locataire.
3. Dans le volet de **navigation**, sélectionnez **\*tenant\_name\*** > **Services L4-L7 > Appareils L4-L7**.
4. Dans le volet Travail, sélectionnez **Actions > Créer des périphériques L4-L7**.
5. Dans la boîte de dialogue **Créer des périphériques L4-L7**, dans la section **Général**, procédez comme suit :
  - a) Cochez la case **Géré**.
  - b) Dans le champ **Nom**, entrez le nom de l'appareil.
  - c) Dans la liste déroulante **Type de service**, sélectionnez **ADC**.
  - d) Dans le champ **Type de périphérique**, sélectionnez **Physique**.

**Remarque**

Assurez-vous que pour VMware ESX, vous sélectionnez Virtual et associez le domaine Virtual Machine Manager (VMM) correspondant.

  - e) Dans la liste déroulante **Domaine physique**, sélectionnez le domaine physique.
  - f) Dans le champ **Mode**, sélectionnez **Nœud unique** ou **Cluster HA**, selon vos besoins.
  - g) Dans la liste déroulante **Device Package**, sélectionnez **Citrix-NetScalerMAS-1.0**.
  - h) Dans la liste déroulante **Modèle**, sélectionnez le modèle de périphérique. Par exemple, Citrix ADC-MPX ou Citrix ADC-VPX.
6. Dans la section **Connectivité**, sélectionnez **Out-Of-Bandou In-Band** dans le champ **Connectivity APIC to Device Management**, en fonction de la configuration de Citrix ADC dans la structure.



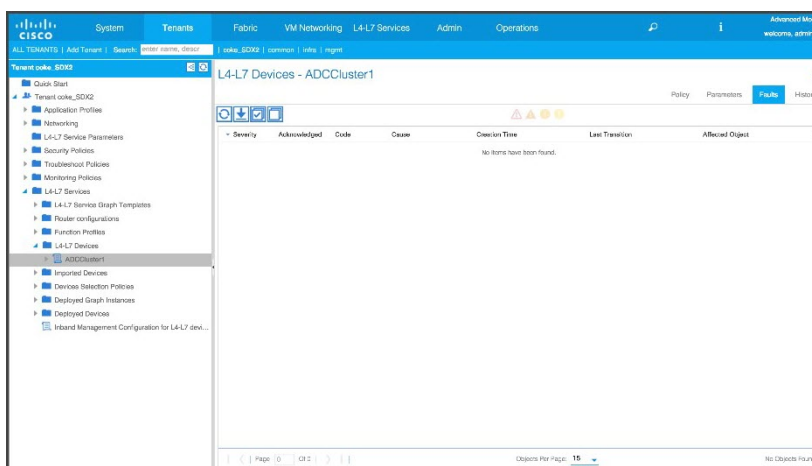
7. Dans la section **Informations d'identification**, spécifiez le nom d'utilisateur et le mot de passe pour l'accès au périphérique.
8. Dans les sections **Appareil 1** et **Appareil 2**, respectivement, terminez la configuration liée à la gestion.
9. Dans la section **Cluster**, complétez la configuration liée à la gestion du cluster. Assurez-vous que dans la liste déroulante **Device Manager**, vous sélectionnez le gestionnaire de périphériques que vous avez créé dans [Ajout de Citrix ADM en tant que gestionnaire de périphériques dans Cisco APIC](#)

10. Cliquez sur **SUIVANT**. La page Configuration de l'appareil s'affiche. Le package de périphériques en mode hybride ne fournit pas de détails de configuration spécifiques au périphérique et au cluster, tels que la haute disponibilité, les fonctionnalités et les modes d'activation/désactivation, la configuration pour NTP, SNMP, les alarmes SNMP, etc. Ces configurations doivent être effectuées à l'aide de Citrix ADM.
11. Cliquez sur **FINISH**. Lorsque vous avez correctement enregistré l'appareil dans l'APIC, l'appareil est ajouté et s'affiche dans le volet de navigation. Pour afficher l'appareil enregistré, dans le volet de navigation, accédez à **\*tenant\_name\* > Services L4-L7 > Appareils L4-L7 > Device\_name**.

### Important

Après avoir enregistré l'appareil, assurez-vous que l'APIC ne présente aucun défaut. Vous

vous pouvez afficher les défauts en cliquant sur l'onglet **Défauts** dans le volet de **travail** .



Vous pouvez également enregistrer un périphérique Citrix ADC à l'aide d'API. Voici un exemple de charge utile XML pour ajouter un périphérique L4-L7 :

```

1  <polUni>
2
3      <fvTenant name="coke">
4
5          <vnsLDevVipname="ADCCluster1"funcType="GoTo" svcType="ADC">
6
7              <vnsRsMDevAtt tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0" />
8
9              <vnsRsALDevToPhysDomP tDn="uni/phys-phys"/>
10
11              <vnsCMgmt name="devMgmt"host="10.102.102.67"port="80"/>
12
13              <vnsCCred name="username" value="nsroot"/>
14
15              <vnsCCredSecret name="password" value="****"/>
16
17              <vnsRsALDevToDevMgr tnVnsDevMgrName="MAS1"/>
18
19              <vnsCDev name="ADC1" devCtxLbl="C1">
20
21                  <vnsCIif name="1_1">
22
23                      <vnsRsCIifPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1
24                          /33]"/>
25
26                  </vnsCIif>
27
28                  <vnsCIif name="1_2">
29
30                      <vnsRsCIifPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1
31                          /35]"/>

```

```
31     </vnsCIf>
32
33     <vnsCMgmt name="devMgmt" host="10.102.102.65" port="80"/>
34
35     <vnsCCred name="username" value="nsroot"/>
36
37     <vnsCCredSecret name="password" value="****"/>
38
39     </vnsCDev>
40
41     <vnsCDev name="ADC2" devCtxLbl="C1">
42
43     <vnsCIf name="1_1">
44
45     <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1
46         /34]"/>
47
48     </vnsCIf>
49
50     <vnsCIf name="1_2">
51
52     <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1
53         /36]"/>
54
55     </vnsCIf>
56
57     <vnsCMgmt name="devMgmt" host="10.102.102.66" port="80"/>
58
59     <vnsCCred name="username" value="nsroot"/>
60
61     <vnsCCredSecret name="password" value="****"/>
62
63     </vnsCDev>
64
65     <vnsLIIf name="outside">
66
67     <vnsRsMetaIf tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/
68         mIfLbl-outside"/>
69
70     <vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC1/
71         cIf-1_1"/>
72
73     <vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC2/
74         cIf-1_1"/>
75
76     </vnsLIIf>
77
78     <vnsLIIf name="inside">
79
80     <vnsRsMetaIf tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/
81         mIfLbl-inside"/>
82
83     <vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC1/
```

```
78         cIf-1_2"/>
79     <vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC2/
80         cIf-1_2"/>
81 </vnsLIIf>
82
83 </vnsLDevV
84
85 </fvTenant>
86
87 </polUni>
```

## Créer et déployer un graphique de service

February 1, 2024

Vous devez utiliser des modèles de graphique de service Cisco APIC dans APIC pour créer et déployer les Citrix ADC. Assurez-vous d'utiliser le profil de fonction ADC lors de la création et du déploiement d'un graphique de service.

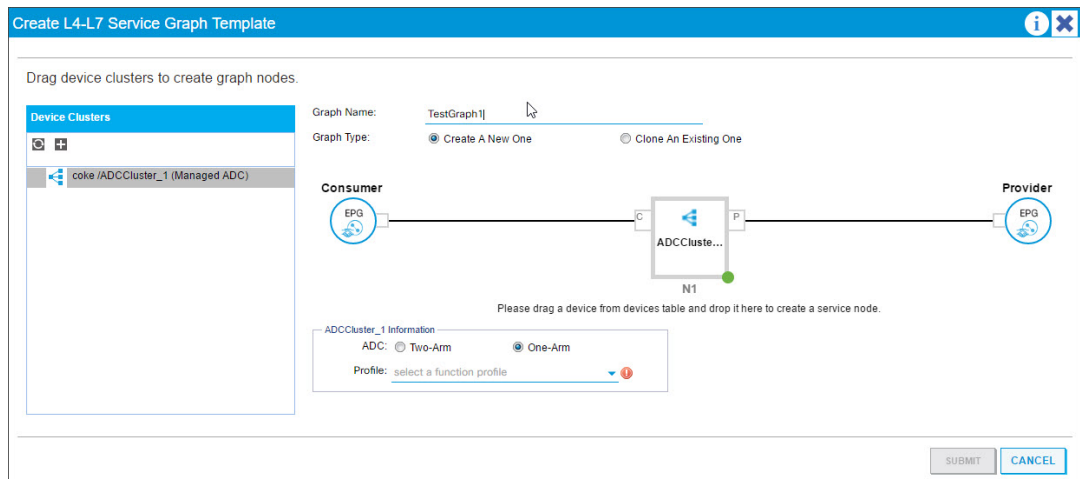
Une fois le graphique configuré dans l'APIC, l'APIC automatise la configuration des périphériques sur la base des définitions de fonctions, de la connectivité des périphériques à la structure et des entités configurées dans le cadre du déploiement du graphique. L'APIC automatise également la configuration réseau, telle que l'allocation de VLAN et sa liaison, dans le cadre de la création du graphe de service, et la configuration est supprimée une fois que vous supprimez le graphique de l'APIC.

Un graphe de service est représenté sous la forme de deux niveaux ou plus d'une application, la fonction de service appropriée étant insérée entre eux. Un graphe de service est inséré entre les EPG source et destination par un contrat.

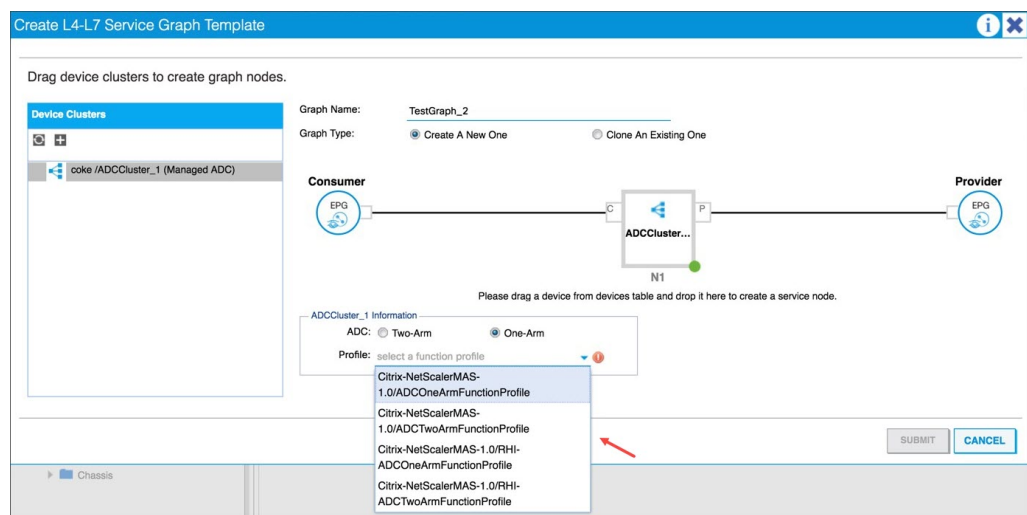
**Pour créer un graphique de service à l'aide de l'interface graphique APIC, procédez comme suit :**

1. Dans la barre de menus, accédez à **Locataires > Tous les Locataires**.
2. Dans le volet **Travail**, double-cliquez sur le nom du locataire.
3. Dans le volet de **navigation**, sélectionnez **\*tenant\_name\* > L4-L7 Services > L4-L7 Service Graph Templates**.
4. Dans le volet **Travail**, sélectionnez **Actions > Créer un modèle de diagramme de service L4-L7**.
5. Dans la boîte de dialogue **Créer un modèle de graphe de service L4-L7**, dans la section Clusters de périphériques, sélectionnez un cluster de périphériques et procédez comme suit :

- a) Dans le champ **Nom du graphique**, entrez le nom du modèle de graphe de service.
- b) Dans le champ **Type de graphique**, sélectionnez **Créer un nouveau graphique**.
- c) Dans la section **Device Cluster**, faites glisser l'appareil et déposez-le entre le groupe de points de terminaison du consommateur et le groupe de points de terminaison du fournisseur pour créer un nœud de service.



- d) Dans la section **<L4-L7device\_name information>**, procédez comme suit :
  - i. Dans le champ **ADC**, sélectionnez **un bras** ou **deux bras**, selon le mode de déploiement de l'Citrix ADC dans l'atelier.
  - ii. Dans la liste déroulante **Profil**, sélectionnez le profil de fonction fourni dans le package de périphériques.

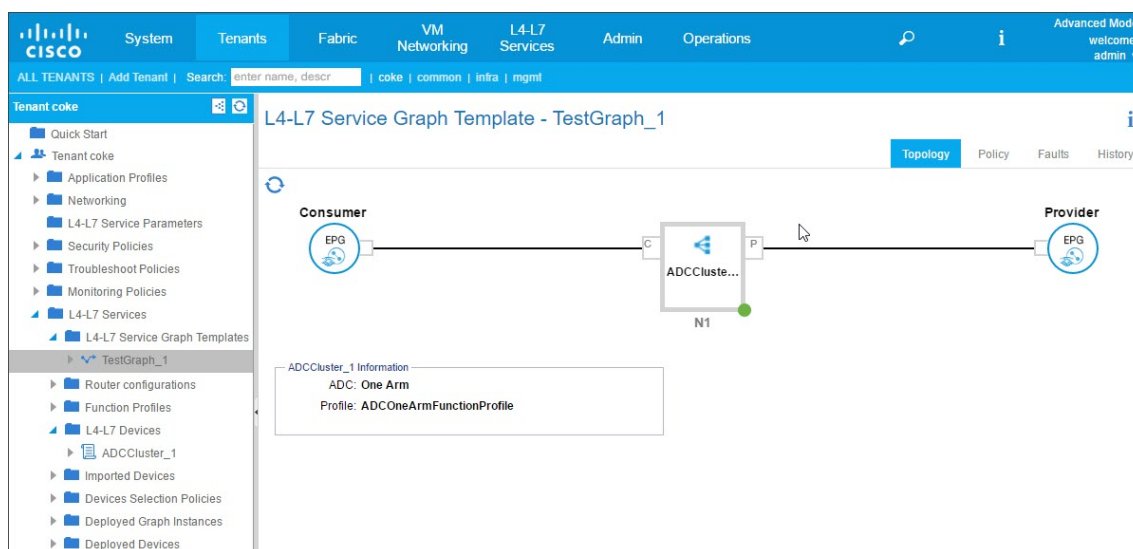


- iii. Cliquez sur **SUBMIT**.

6. Dans le volet **de navigation**, cliquez sur le modèle de graphe de service. L'écran présente une topologie graphique du modèle de graphe de service.

### Remarque

Le Cisco APIC prend en charge la notion de connecteurs, et ces connecteurs sont visibles dans le nœud ADCCluster. Les connecteurs définissent la direction du trafic réseau et le script de périphérique qui lie dynamiquement le VLAN alloué à une adresse IP virtuelle (VIP) ou IP de sous-réseau (SNIP), selon que la connexion est externe ou interne. Les VLAN sont également liés à des interfaces spécifiques utilisées pour le trafic entrant et sortant.

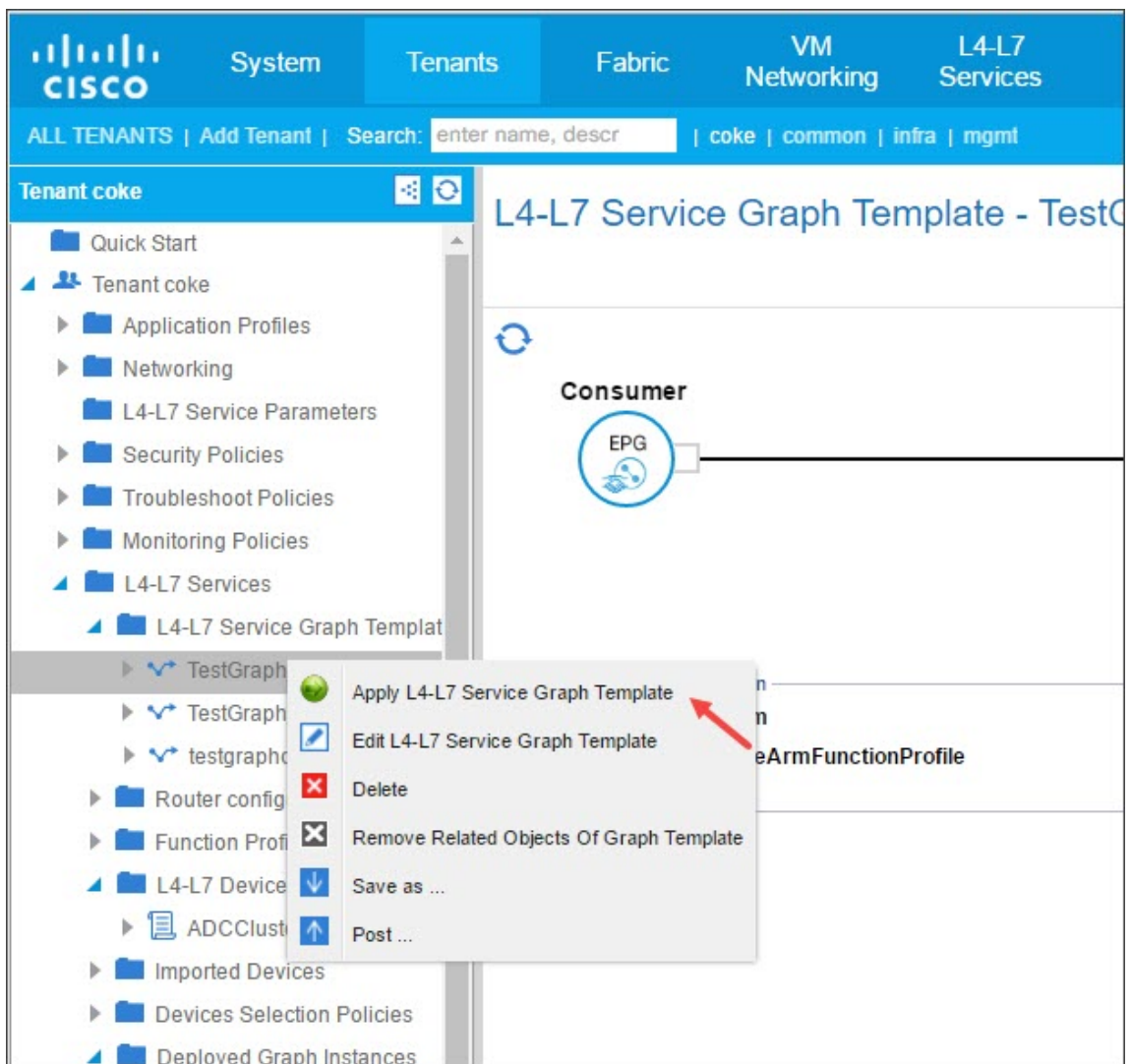


### Application du modèle Service Graph aux groupes de points de terminaison

Après avoir créé le modèle de graphe de service, vous devez appliquer le modèle de graphique de service créé à l'aide de l'interface graphique APIC.

**Pour appliquer le modèle de graphique des services, procédez comme suit :**

1. Dans la barre de menus, accédez à **Locataires > Tous les Locataires**.
2. Dans le volet **Travail**, double-cliquez sur le nom du locataire.
3. Dans le volet de navigation, choisissez **\*tenant\_name\* > L4-L7 Services > L4-L7 Service Graph Templates**.
4. Cliquez avec le bouton droit sur le **template\_name** et cliquez sur **Appliquer le modèle de graphe de service L4-L7**.

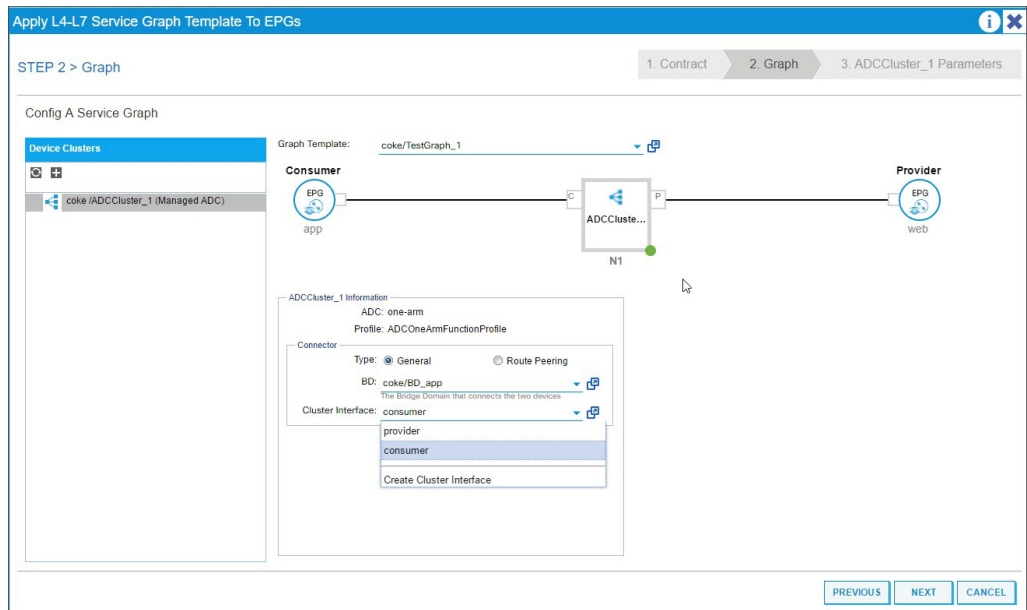


5. Dans la boîte de dialogue **Appliquer le modèle de graphe de service L4-L7 aux EPG**, dans la section **Informations EPG**, renseignez les champs suivants :
  - a) Dans la liste déroulante **Consumer EPG/External Network**, sélectionnez le groupe de terminaux consommateurs.
  - b) Dans la liste déroulante **Provider EPG/External Network**, sélectionnez le groupe de terminaux fourni.
  - c) Dans la section **Informations sur le contrat**, renseignez les champs appropriés. Les informations du contrat sont spécifiques à l'APIC Cisco et sont configurées dans le cadre des stratégies de sécurité associées aux EPG.

- d) Cliquez sur **Suivant**.
- e) Dans la liste déroulante **Modèle de graphique**, sélectionnez le modèle de graphique de service que vous avez créé.
- f) Dans la section **Connecteur**, procédez comme suit :
  - i. Dans le champ **Type**, sélectionnez Général.
  - ii. Dans la liste déroulante **BD**, sélectionnez le domaine du pont. Les détails du connecteur font partie du domaine de pont qui fait partie du modèle d'infrastructure Cisco APIC.
  - iii. Dans la liste déroulante **Interface de cluster**, sélectionnez l'interface de cluster appropriée pour le domaine de pont sélectionné.

L'APIC Cisco utilise les domaines de pont sélectionnés pour le trafic de chemin de données entre le périphérique Citrix ADC et la structure, comme requis par le modèle de graphe de service sélectionné.



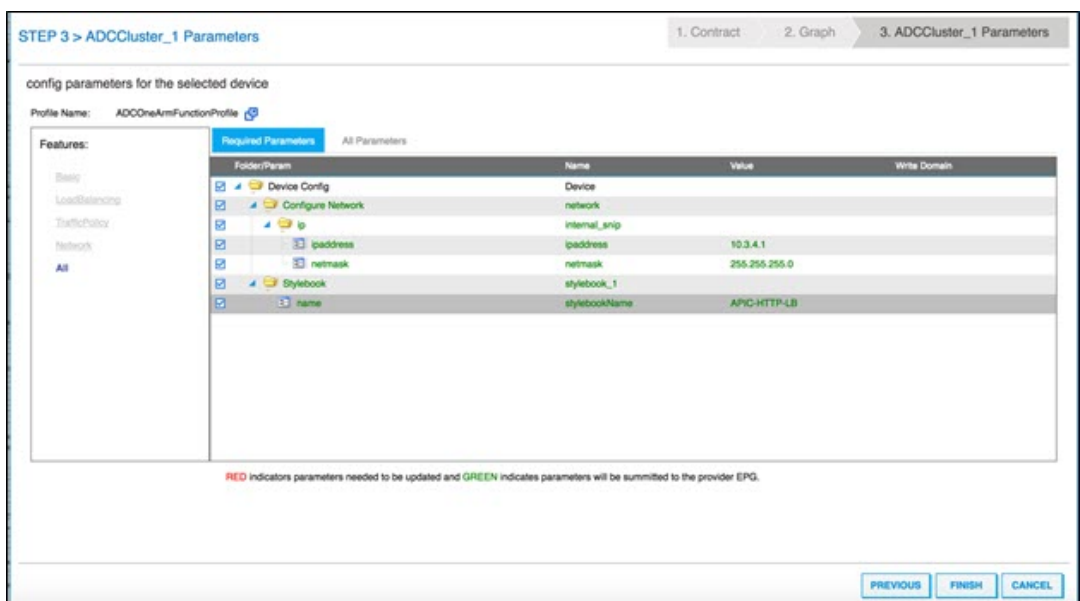


iv. Cliquez sur **Suivant**.

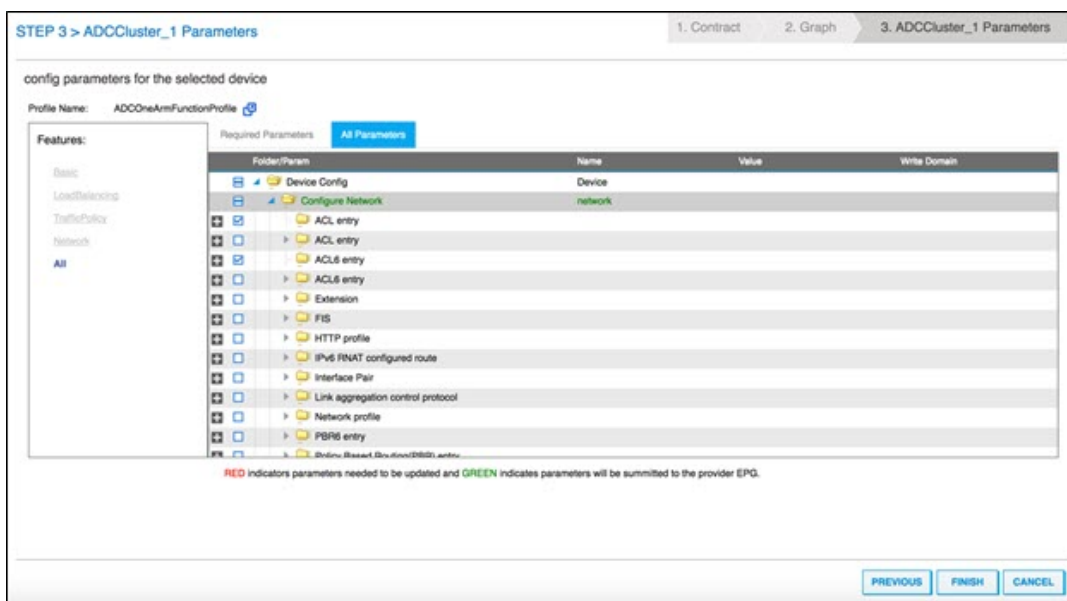
Sur l'écran **Paramètres**, dans l'onglet **Paramètres requis**, entrez les détails spécifiques à la L2-L3, tels que l'adresse IP requise par le profil. L'autre paramètre clé est le nom Style-Book. Il peut s'agir du StyleBook **APIC-HTTP-LB** intégré fourni dans Citrix Application Delivery Management (ADM), ou vous pouvez fournir le nom du StyleBook que vous avez créé dans [Création d'un StyleBook pour l'application à l'aide de Citrix ADM](#)

**Remarque**

Le nom StyleBook lie les détails du graphe de service à la configuration L4-L7 créée avec Citrix ADM pour une application donnée.



L'interface graphique Cisco APIC vous permet de filtrer les paramètres sur la base de fonctionnalités (par exemple, l'équilibrage de charge). Vous pouvez afficher et définir tous les paramètres obligatoires dans l'onglet **Paramètres requis**, et vous pouvez afficher et définir tous les autres paramètres liés à la fonctionnalité dans l'onglet **Tous les paramètres**.



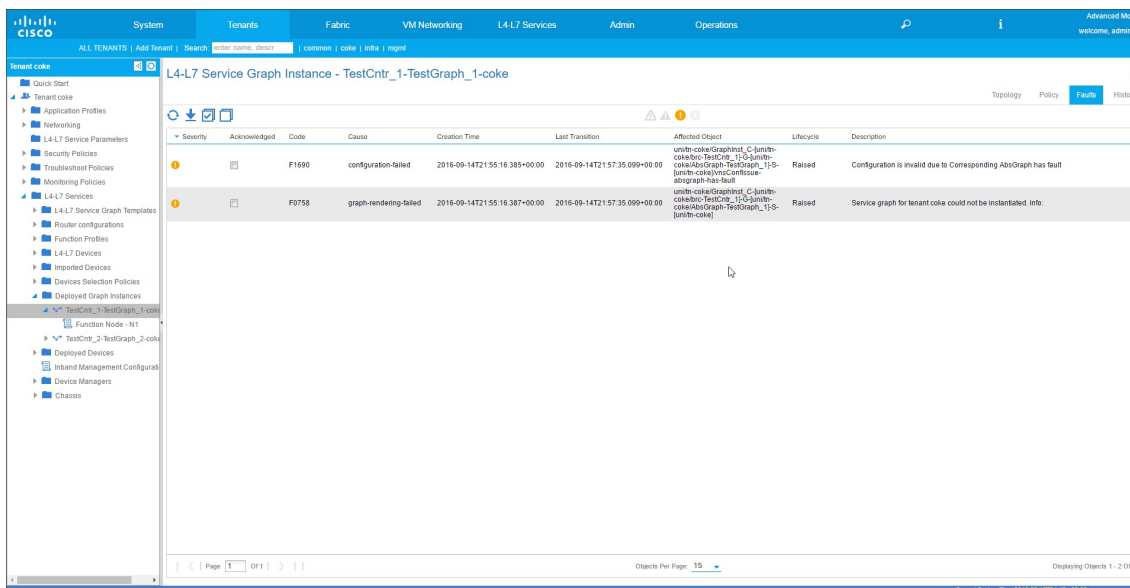
### Remarque

Par défaut, un profil à bras unique intégré nécessite que vous fournissiez des informations SNIP telles que l'adresse IP et le masque de réseau. Vous pouvez afficher d'autres paramètres réseau en cliquant sur **Tous les paramètres** et en développant l'arborescence **Configurer le réseau** dans l'interface graphique Cisco APIC. Cette liste répertorie tous les paramètres réseau pris en charge par Citrix ADC. Vous pouvez instancier n'importe quelle entité et fournir des valeurs pour les attributs répertoriés à partir de l'interface graphique Cisco APIC.

### 6. Cliquez sur **Terminer**.

#### Important

Après avoir appliqué le modèle de graphe de service, assurez-vous que le graphe déployé ne présente aucune erreur. Vous pouvez afficher les défauts en cliquant sur l'onglet **Défauts** dans le volet de **travail**.



Dans le cadre du déploiement Service Graph, le package de périphérique en mode hybride transmet les détails de configuration de l'APIC Cisco vers l'Citrix ADM. Citrix ADM traite en interne ces configurations vers l'Citrix ADC respectif et renvoie la réponse à l'APIC. Un déploiement de graphe réussi n'aura pas de problème, et le Citrix ADC est correctement mis en réseau avec la structure pour le graphique correspondant.

L'APIC prend en charge différentes façons de configurer et de déployer des graphiques à l'aide d'API, et le déploiement de graphiques inclut diverses dépendances sur certaines constructions spécifiques à APIC, telles que le locataire, le contrat, le VLAN et l'espace de noms.

L'exemple d'approche suivant illustre l'une des manières d'utiliser les API de l'APIC pour créer et déployer des graphes L4 à L7, en supposant que les artefacts spécifiques à l'APIC sont déjà configurés dans l'APIC.

**Important**

Assurez-vous d'utiliser ces charges utiles XML comme référence et d'apporter les modifications appropriées au code XML avant de les utiliser dans votre environnement.

Voici un exemple de création et de déploiement du graphe de service à l'aide d'API :

- a) Créer un profil d'application
- b) Créer les détails d'un graphique de service
- c) Joindre le graphique de service à un contrat

Voici un exemple de charge utile XML pour créer un AppProfile. AppProfile contient des EPG, et le fournisseur EPG contient les entités spécifiques à Citrix ADC, les attributs et leurs valeurs. Dans l'exemple de charge utile XML suivant, les entités réseau spécifiques à Citrix ADC telles que le NSIP sont créées avec un ensemble d'attributs et un nom de StyleBook.

```

1 <polUni>
2   <fvTenant name="coke">
3     <!-- Application Profile -->
4     <fvAp dn="uni/tn-coke/ap-sap" name="sap">
5       <!-- EPG 1 -->
6       <fvAEPg dn="uni/tn-coke/ap-sap/epg-web" name="web">
7         <fvRsBd tnFvBDName="BD_web" />
8         <!-- ----- CONFIG PAYLOAD ----- -->
9         <vnsFolderInst ctrctNameOrLbl="Ctrct1"
graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="Network" name=
"Network">
10           <vnsFolderInst ctrctNameOrLbl="Ctrct1"
graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="nsip" name="
snip1">
11             <vnsParamInst key="ipaddress" name="ip1"
value="110.110.110.2"/>
12             <vnsParamInst key="netmask" name="netmask1
" value="255.255.255.0"/>
13             <vnsParamInst key="type" name="tye" value=
"SNIP"/>
14             <vnsParamInst key="dynamicrouting" name="
dynamicrouting" value="DISABLED"/>
15             <vnsParamInst key="hostroute" name="
hostroute" value="DISABLED"/>
16           </vnsFolderInst>
17           <vnsFolderInst ctrctNameOrLbl="Ctrct1"
graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="nsip" name="
snip2">
18             <vnsParamInst key="ipaddress" name="ip2"
value="220.220.220.2"/>
19             <vnsParamInst key="netmask" name="netmask2
" value="255.255.255.0"/>
20             <vnsParamInst key="type" name="tye" value=
"SNIP"/>
21             <vnsParamInst key="dynamicrouting" name="
dynamicrouting" value="DISABLED"/>
22             <vnsParamInst key="hostroute" name="
hostroute" value="DISABLED"/>
23           </vnsFolderInst>
24         </vnsFolderInst>
25         <vnsFolderInst ctrctNameOrLbl="Ctrct1"
graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="Stylebook"
name="stylebook_1">
26           <vnsParamInst name="stylebookName" key="name"
value="APIC-HTTP-LB"/>
27         </vnsFolderInst>
28         <vnsFolderInst ctrctNameOrLbl="Ctrct1"
graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="
internal_network" name="internal_network">
29           <vnsCfgRelInst name="internal_network_key" key
="internal_network_key" targetName="Network/snip1"/>
30         </vnsFolderInst>
31       </vnsFolderInst ctrctNameOrLbl="Ctrct1"

```

```

graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="
external_network" name="external_network">
32     <vnsCfgRelInst name="external_network_key" key
="external_network_key" targetName="Network/snip2"/>
33     </vnsFolderInst>
34     <vnsFolderInst ctrctNameOrLbl="Ctrct1"
graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="mFCngStylebook
" name="mFCngStylebook_1">
35         <vnsCfgRelInst name="Stylebook_key" key="
Stylebook_key" targetName="stylebook_1"/>
36         </vnsFolderInst>
37         <!-- ----- END CONFIG PAYLOAD ----- -->
38         <fvSubnet ip="110.110.110.110/24" scope="shared"/>
39         <fvRsProv tnVzBrCPName="Ctrct1"></fvRsProv>
40         <fvRsDomAtt tDn="uni/phys-sepg" />
41         <fvRsPathAtt tDn="topology/pod-1/paths-101/pathep
-[eth1/38]" encap="vlan-3703" instrImedcy="immediate"/>
42         </fvAEPg>
43         <!-- EPG 2 -->
44         <fvAEPg dn="uni/tn-coke/ap-sap/epg-app" name="app">
45             <fvRsCons tnVzBrCPName="Ctrct1"/>
46             <fvRsBd tnFvBDName="BD_app" />
47             <fvSubnet ip="220.220.220.220/24" scope="shared"/>
48             <fvRsPathAtt tDn="topology/pod-1/paths-101/pathep
-[eth1/37]" encap="vlan-3704" instrImedcy="immediate"/>
49             <fvRsDomAtt tDn="uni/phys-sepg" />
50         </fvAEPg>
51     </fvAp>
52 </fvTenant>
53 </polUni>
54 <!--NeedCopy-->

```

Voici un exemple de charge utile XML pour créer des détails de graphe de service :

```

1 <polUni>
2   <fvTenant name="coke">
3     <vnsAbsGraph name = "Graph1">
4       <vnsAbsTermNodeProv name = "Input1">
5         <vnsAbsTermConn name = "C1"></vnsAbsTermConn>
6       </vnsAbsTermNodeProv>
7       <vnsAbsNode name="ADC" funcType="GoTo">
8         <vnsAbsFuncConn name = "outside" attNotify="true">
9           <vnsRsMConnAtt tDn="uni/infra/mDev-Citrix-
NetScalerMAS-1.0/mFunc-ADCFunction/mConn-external" />
10        </vnsAbsFuncConn>
11        <vnsAbsFuncConn name = "inside" attNotify="true">
12          <vnsRsMConnAtt tDn="uni/infra/mDev-Citrix-
NetScalerMAS-1.0/mFunc-ADCFunction/mConn-internal" />
13        </vnsAbsFuncConn>
14        <vnsRsNodeToMFunc tDn="uni/infra/mDev-Citrix-
NetScalerMAS-1.0/mFunc-ADCFunction"/>
15        <vnsRsDefaultScopeToTerm tDn="uni/tn-coke/AbsGraph
-Graph1/AbsTermNodeProv-Input1/outtmnl"/>

```

```

16         <vnsRsNodeToAbsFuncProf tDn="uni/infra/mDev-Citrix
-NetScalerMAS-1.0/absFuncProfContr/absFuncProfGrp-
ADCCOneArmServiceProfileGroup/absFuncProf-A
17 DCCOneArmFunctionProfile"/>
18         <vnsRsNodeToLDev tDn="uni/tn-coke/lDevVip-
ADCCcluster1"/>
19         </vnsAbsNode>
20         <vnsAbsTermNodeCon name = "Output1">
21             <vnsAbsTermConn name = "C6"></vnsAbsTermConn>
22         </vnsAbsTermNodeCon>
23         <vnsAbsConnection name = "CON1">
24             <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph
-Graph1/AbsTermNodeCon-Output1/AbsTConn" />
25             <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph
-Graph1/AbsNode-ADC/AbsFConn-outside" />
26         </vnsAbsConnection>
27         <vnsAbsConnection name = "CON2">
28             <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph
-Graph1/AbsNode-ADC/AbsFConn-inside" />
29             <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph
-Graph1/AbsTermNodeProv-Input1/AbsTConn" />
30         </vnsAbsConnection>
31     </vnsAbsGraph>
32 </fvTenant>
33 </poUni>
34 <!--NeedCopy-->

```

Voici un exemple de charge utile XML pour attacher le graphique de service à un contrat :

```

1 <poUni>
2     <fvTenant name="coke">
3         <vzBrCP name="Ctrct1">
4             <vzSubj name="http">
5                 <vzRsSubjGraphAtt tnVnsAbsGraphName="Graph1"/>
6             </vzSubj>
7         </vzBrCP>
8     </fvTenant>
9 </poUni>
10 <!--NeedCopy-->

```

## Configurer les paramètres L4-L7 à partir de Citrix ADM à l'aide de StyleBook

February 1, 2024

24 mai 2018

Dans Citrix Application Delivery Management (ADM), vous pouvez afficher les détails du graphique

de service déployé dans l'onglet **Orchestration**, sous **Cisco ACI**. La vue tabulaire affiche les détails du graphique de service tels que le nom du graphique, le nom du locataire, le contexte, le nom du StyleBook et l'état de la configuration du réseau.

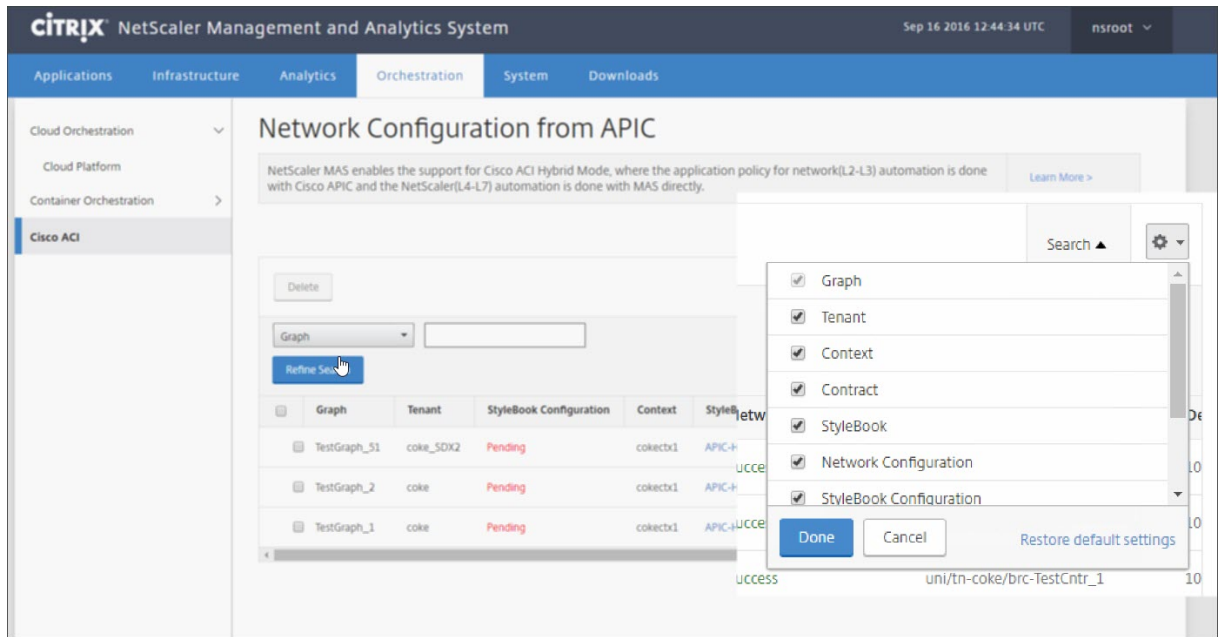
The screenshot shows the NetScaler Management and Analytics System interface. The top navigation bar includes 'Applications', 'Infrastructure', 'Analytics', 'Orchestration', 'System', and 'Downloads'. The left sidebar shows 'Cloud Orchestration', 'Cloud Platform', 'Container Orchestration', and 'Cisco ACI'. The main content area is titled 'Network Configuration from APIC' and contains a table with the following data:

Graph	Tenant	StyleBook Configuration	Context	StyleBook	Network Configuration	Contract	De
TestGraph_51	coke_SDX2	Pending	cokectx1	APIC-HTTP-LB	Success	uni/tn-coke_SDX2/brc-TestCntr_1	10
TestGraph_2	coke	Pending	cokectx1	APIC-HTTP-LB	Success	uni/tn-coke/brc-TestCntr_2	10
TestGraph_1	coke	Pending	cokectx1	APIC-HTTP-LB	Success	uni/tn-coke/brc-TestCntr_1	10

### Remarque

Si le graphe est supprimé de l'APIC Cisco, la configuration correspondante est supprimée du périphérique, y compris la configuration L4-L7.

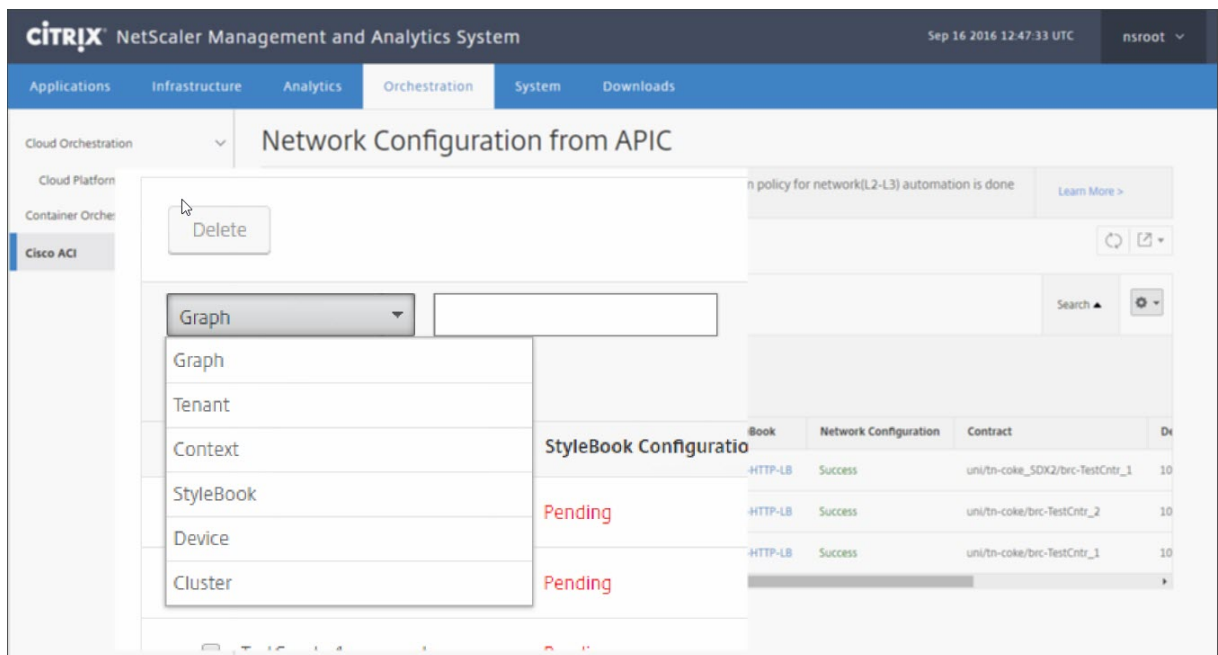
En outre, la vue tabulaire vous permet de trier n'importe quelle colonne affichée dans le tableau et de filtrer les données à l'aide de l'option Rechercher. Vous pouvez également personnaliser les détails des colonnes en sélectionnant ou en désélectionnant les noms des colonnes dans la liste déroulante :



Vous pouvez également cliquer sur le bouton **Rechercher** et utiliser les options de recherche pour filtrer les données. Vous pouvez sélectionner n'importe quelle colonne dans la liste déroulante et saisir une valeur correspondante pour filtrer les données affichées dans le tableau.

#### Remarque

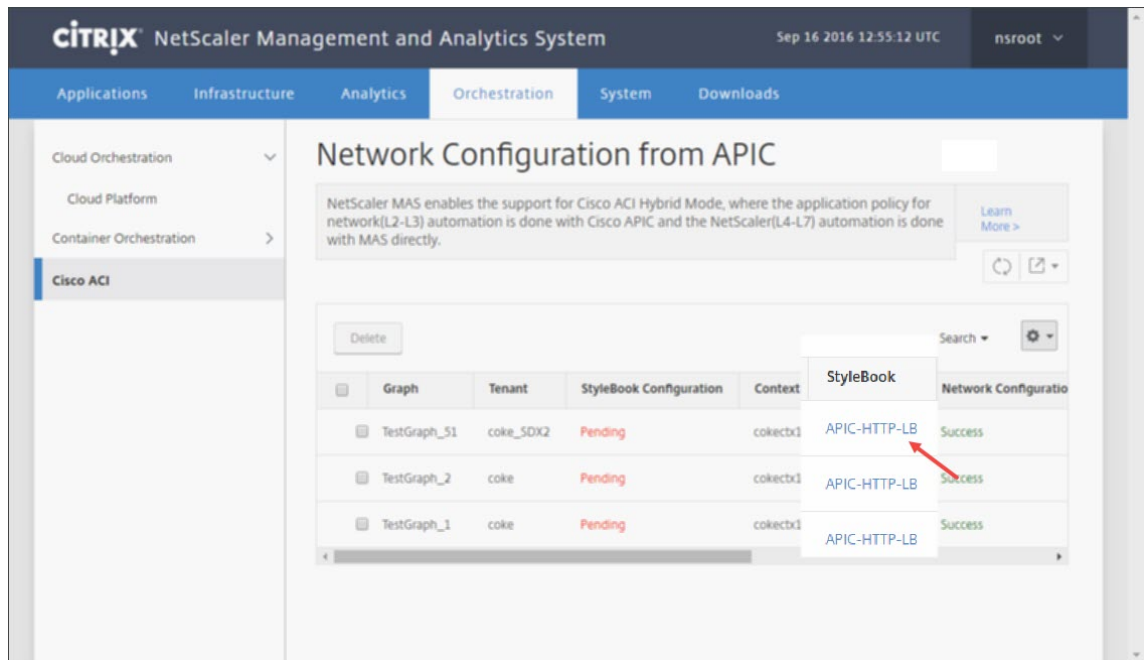
La fonctionnalité de recherche distingue les majuscules et minuscules et vous devez fournir les critères de recherche exacts.



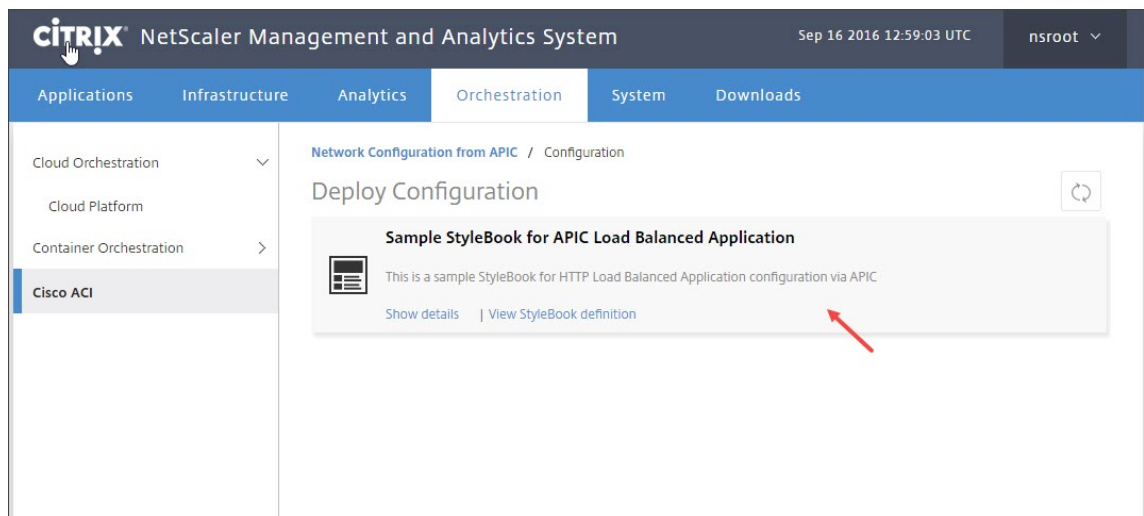
Pour déployer la configuration L4-L7 à l'aide de StyleBook dans Citrix ADM :



1. Cliquez sur le nom du StyleBook qui apparaît sous forme d'URL dans la vue tabulaire.

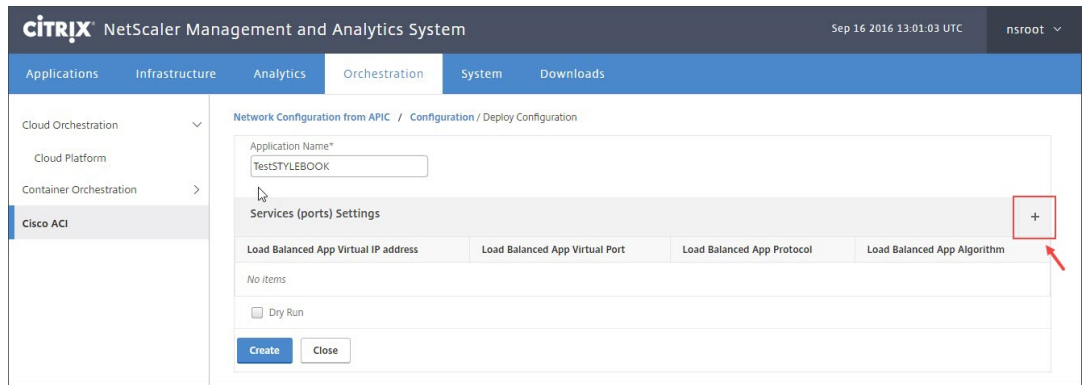


2. Dans la fenêtre Configuration, double-cliquez sur **StyleBook**.

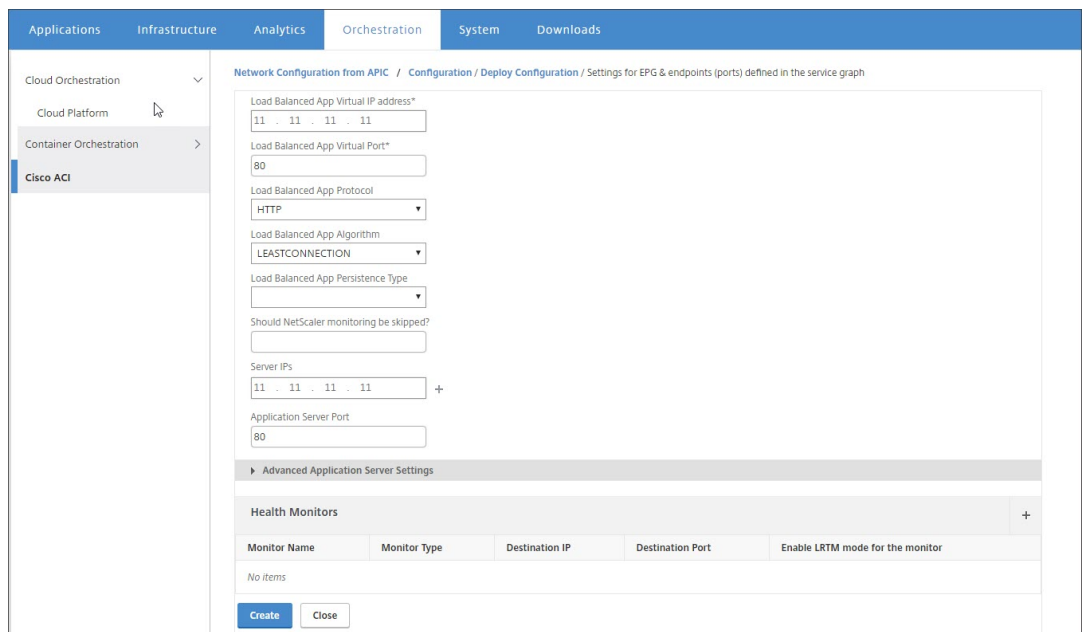


3. Dans la fenêtre Configuration du déploiement, procédez comme suit :

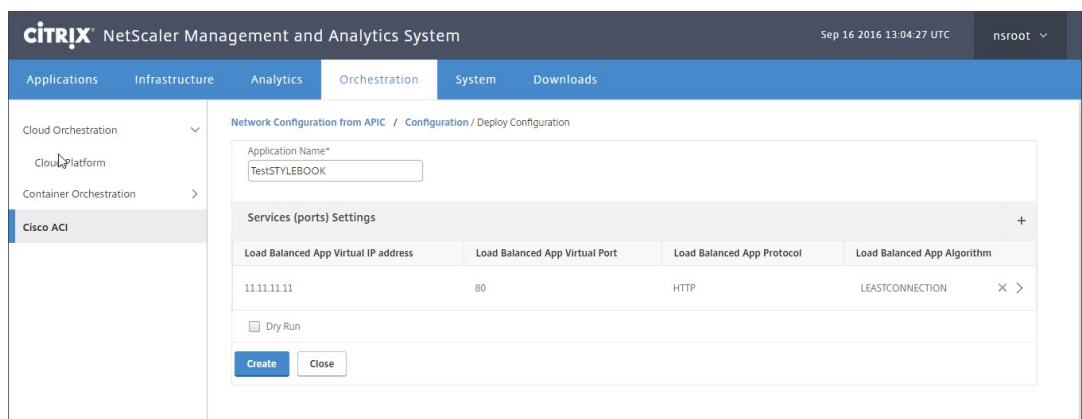
- Dans le champ **Nom de l'application**, entrez le nom de la configuration des fonctionnalités ADC qui correspond au graphe de service de l'application dans l'APIC.
- Dans la section Paramètres du service (ports), cliquez sur **+**.



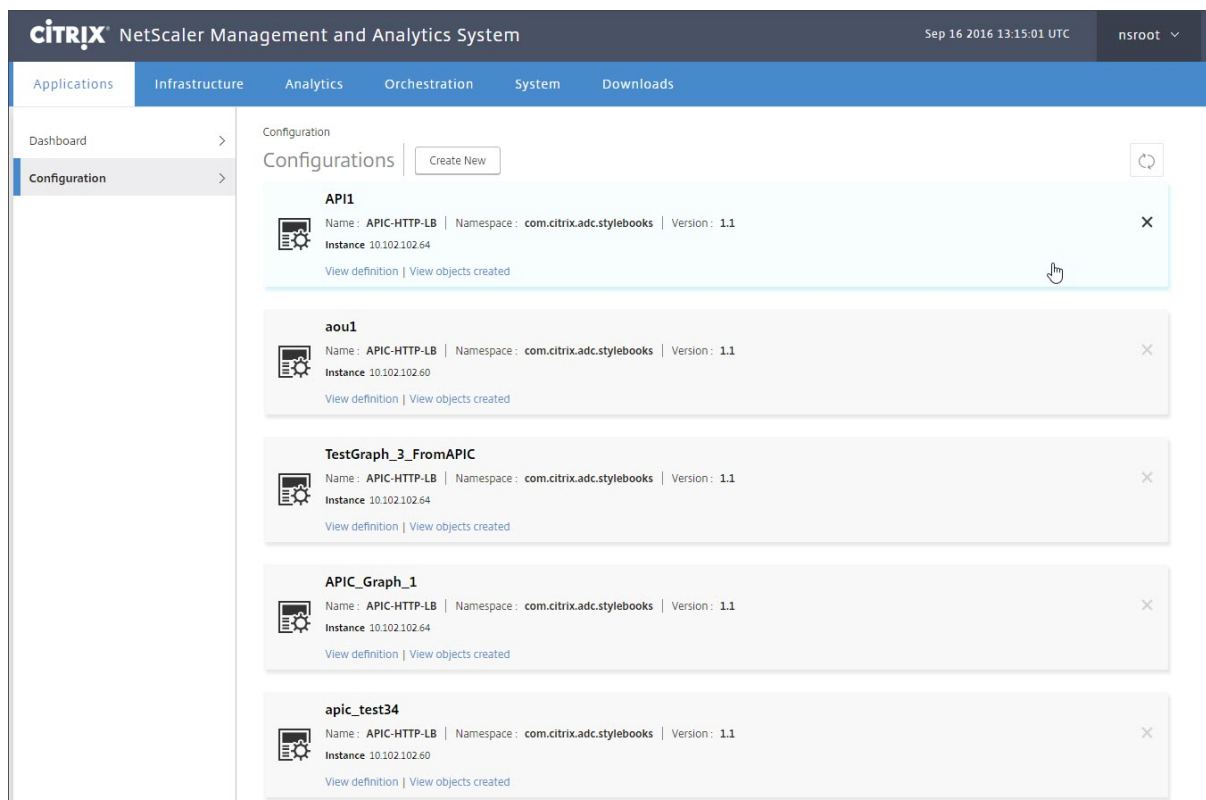
c) Dans les **paramètres pour l'EPG et les points de terminaison (ports) définis dans la fenêtre du graphique des services**, entrez les valeurs du paramètre renseigné à partir du StyleBook et cliquez sur **Créer**.



d) Cliquez sur **Créer**.



La configuration L4-L7 spécifiée dans le StyleBook est déployée, dans Citrix ADM. Vous pouvez afficher la configuration StyleBook à partir de l'onglet **Application**, en accédant à **Application > Configuration**.



## Attacher et détacher les événements de point de terminaison d'APIC

February 1, 2024

La solution en mode hybride gère implicitement l'attachement ou le détachement des événements de point de terminaison du Cisco APIC. Lorsque l'APIC Cisco déclenche un événement de point de terminaison attachement, le servicegroup\_servicegroupmember\_binding est automatiquement déclenché par le StyleBook dans Citrix Application Delivery Management (ADM), et le point de terminaison est délié lors de l'événement de point de terminaison détacher.

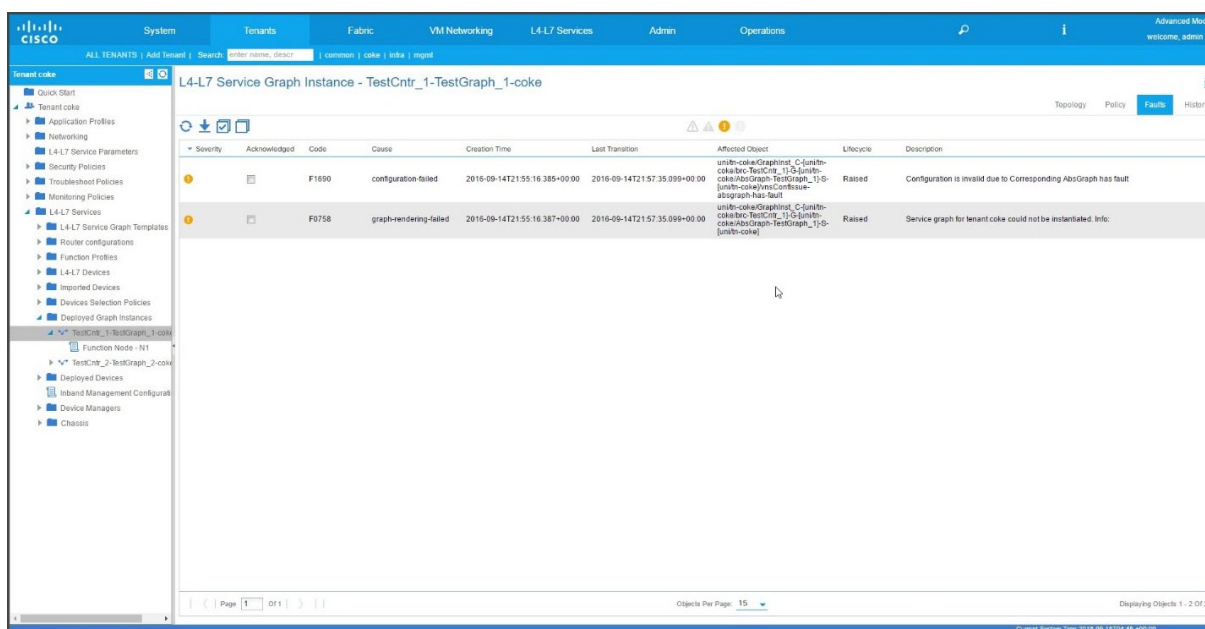
En outre, si vous n'avez pas déployé la configuration L4-L7 dans citrix ADM avant que l'événement de point de terminaison d'attache ou de détachement ne soit déclenché dans Cisco l'APIC, la solution conservera les adresses IP d'attache dans la base de données. Ces adresses IP sont liées au groupe de services correspondant après la création du groupe de services via StyleBook.

## Rapports d'erreurs APIC

February 1, 2024

Lorsque vous déployez un package de périphériques Citrix ADC dans Cisco ACI, le Cisco APIC signale toute défaillance. Vous pouvez afficher les rapports d'erreurs à n'importe quel niveau de l'APIC (par exemple, périphérique, locataire, EPG ou graphique de service). La capture d'écran ci-dessous montre un rapport d'erreur au niveau de l'appareil. Pour plus d'informations sur les défauts, consultez [http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/faults/guide/b\\_APIC\\_Faults\\_Errors/b\\_IFC\\_Faults\\_Errors\\_chapter\\_01.html](http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/faults/guide/b_APIC_Faults_Errors/b_IFC_Faults_Errors_chapter_01.html).

Sélectionnez une entité APIC et cliquez sur l'onglet **Faults** pour afficher les erreurs signalées par l'APIC pour cette entité.



## Journaux générés par Citrix ADM

February 1, 2024

Citrix Application Delivery Management (ADM) fournit une journalisation complète qui peut aider à résoudre les problèmes. Les journaux générés (**admin.log**) sont situés à : **/var/controlcenter/log/**

Vous pouvez ouvrir une session sur Citrix ADM et utiliser l'interpréteur de commandes pour accéder à la structure de répertoire Citrix ADM. Voici un exemple d'extrait d'un journal Citrix ADM pour le déploiement de graphe d'un APIC.

```
1 2016-06-29 10:58:33,816 DEBUG APIC Config = {
2 (0, '', 5230): {
3 'dn': u'uni/vDev-[uni/tn-coke_SDx2/lDevVip-ADCHybridMode_1]-tn-[uni/tn
   -coke_SDx2]-ctx-cokectx1', 'state': 1, 'transaction': 0, '
   ackedstate': 0, 'tenant': 'coke_SDx2', 'ctxName': 'cokectx1', '
   value': {
4 (10, '', 'ADCHybridMode_1_Consumer_1'): {
5 'state': 1, 'transaction': 0, 'cifs': {
6 'ADCHybridMode_1_Device_1': '1_1' }
7 , 'ackedstate': 0 }
8 , (7, '', '2129920_32778'): {
9 'state': 1, 'tag': 273, 'type': 1, 'ackedstate': 0, 'transaction': 0 }
10 , (1, '', 5790): {
11 'transaction': 0, 'ackedstate': 0, 'value': {
12 (3, 'ADCFunction', 'N1'): {
13 'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
14 (4, 'mFCngNetwork', 'mFCngnetwork'): {
15 'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
16 (6, 'Network_key', 'network_key'): {
17 'state': 1, 'transaction': 0, 'target': 'network', 'ackedstate': 0 }
18 }
19 }
20 , (4, 'internal_network', 'internal_network'): {
21 'connector': 'provider', 'state': 1, 'transaction': 0, 'ackedstate':
   0, 'value': {
22 (6, 'internal_network_key', 'internal_network_key'): {
23 'state': 1, 'transaction': 0, 'target': 'network/internal_snip', '
   ackedstate': 0 }
24 }
25 }
26 , (2, 'external', 'consumer'): {
27 'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
28 (9, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
29 'state': 1, 'transaction': 0, 'target': '
   ADCHybridMode_1_Consumer_1_2129920_32778', 'ackedstate': 0 }
30 }
31 }
32 , (4, 'mFCngStylebook', 'mFCngStylebook'): {
33 'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
34 (6, 'Stylebook_key', 'Stylebook_key'): {
35 'state': 1, 'transaction': 0, 'target': 'stylebook_1', 'ackedstate': 0
   }
36 }
37 }
38 , (2, 'internal', 'provider'): {
39 'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
40 (9, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
41 'state': 1, 'transaction': 0, 'target': '
   ADCHybridMode_1_Consumer_1_2129920_32778', 'ackedstate': 0 }
42 }
43 }
44 }
45 }
```

```

46  }
47  , 'state': 1, 'absGraph': 'HybridModeGraph_1', 'rn': u'vGrp-[uni/tn-
    coke_SDx2/GraphInst_C-[uni/tn-coke_SDx2/brc-TestCntr_3]-G-[uni/tn-
    coke_SDx2/AbsGraph-HybridModeGraph_1]-S-[uni/tn-coke_SDx2]]' }
48  , (4, 'Network', 'network'): {
49  'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
50  (4, 'nsip', 'internal_snip'): {
51  'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
52  (5, 'type', 'type'): {
53  'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'SNIP' }
54  , (5, 'hostroute', 'hostroute'): {
55  'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'DISABLED' }
56  , (5, 'ipaddress', 'ipaddress'): {
57  'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': '10.1.1.1' }
58  , (5, 'dynamicrouting', 'dynamicRouting'): {
59  'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'ENABLED' }
60  , (5, 'netmask', 'netmask'): {
61  'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': '255.255.255.0
    ' }
62  }
63  }
64  }
65  }
66  , (8, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
67  'state': 1, 'transaction': 0, 'vif': 'ADCHybridMode_1_Consumer_1', '
    ackedstate': 0, 'encap': '2129920_32778' }
68  , (4, 'Stylebook', 'stylebook_1'): {
69  'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
70  (5, 'name', 'stylebookName'): {
71  'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'APIC-HTTP-LB'
    }
72  }
73  }
74  }
75  , 'txid': 10000 }
76  }
77
78  2016-06-29 10:58:33,816 DEBUG get Graph Return details = {
79  'graphDN': u'uni/vDev-[uni/tn-coke_SDx2/lDevVip-ADCHybridMode_1]-tn-[
    uni/tn-coke_SDx2]-ctx-cokectx1', (1, '', 5790): {
80  'state': 1, 'graphrn': u'vGrp-[uni/tn-coke_SDx2/GraphInst_C-[uni/tn-
    coke_SDx2/brc-TestCntr_3]-G-[uni/tn-coke_SDx2/AbsGraph-
    HybridModeGraph_1]-S-[uni/tn-coke_SDx2]]' }
81  , 'tenantName': 'coke_SDx2', 'StyleBookName': 'APIC-HTTP-LB', '
    graphInstanceName': 'HybridModeGraph_1', 'context': 'cokectx1', '
    graphInstanceId': 5790 }
82
83  2016-06-29 10:58:33,827 DEBUG SUCCESS created track 2.0
84  2016-06-29 10:58:33,833 DEBUG SUCCESS updated track with new task 2
85  2016-06-29 10:58:33,851 DEBUG SUCCESS updated track with new task 1
86  2016-06-29 10:58:33,867 DEBUG fn_wrapper:long_operation_thread_id:<
    eventlet.greenthread.GreenThread object at 0x80aa5c7d0>
87  2016-06-29 10:58:33,867 DEBUG ++++++ Service Audit Call for Device

```

```

      Details = 10.102.102.62 ++++++
88     2016-06-29 10:58:33,867 DEBUG Inside APIC Cred Col If = 2
89     2016-06-29 10:58:33,867 DEBUG Host name from device =
      ADCHybridMode_1
90     "InProgress","message":null,"replication_status":"","target":
      10.102.102.81","operation":"POST","entity_type":"apic",
      entity_id":null }
91   }
92
93     2016-06-29 10:58:44,141 DEBUG Save config Response = {
94     "errorcode": 0, "message": "Done", "severity": "NONE" }
95
96     2016-06-29 10:58:44,141 DEBUG ++++++ getContextAwareFlag = True
97     2016-06-29 10:58:44,141 DEBUG ++++++ get context tenant name from
      Config ++++++
98     2016-06-29 10:58:44,141 DEBUG ++++++ getContextTenantName = {
99     'state': 1, 'ctxName': 'coectx1', 'tenant': 'coke_SDX2', 'vdev': 5230
      }
100    ++++++
101     2016-06-29 10:58:44,142 DEBUG Service health details = {
102    }
103    collection length = 0
104     2016-06-29 10:58:44,142 DEBUG Count details Total = 0 Up = 0 Down =
      0
105     2016-06-29 10:58:44,142 DEBUG Health Score details Up = 0
106     2016-06-29 10:58:44,142 DEBUG Service HEALTH final collection = {
107    ((0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1')): {
108    'faults': [], 'state': 0, 'health': [(0, '', 5230), (1, '', 5790),
      (3, 'ADCFunction', 'N1')], 0) }
109    }
110
111     2016-06-29 10:58:44,142 DEBUG ++++++getServiceHealth Fault List =
      []
112     2016-06-29 10:58:44,142 DEBUG Service HEALTH final response = {
113    'devs': 'ADCHybridMode_1_Device_1', 'faults': [], 'state': 0, 'health'
      : [([(0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1')], 0)] }
114
115     2016-06-29 10:58:44,236 DEBUG RESPONSE from NSLOGOUT = {
116     "errorcode": 0, "message": "Done", "severity": "NONE" }
117    , sessionId = ##
      D2EAFA7CFCD73119E6C5E78D8BCB2E842829C971C1DC7E99850949DAE0029F2191B5E7EDF2764
118
119     2016-06-29 10:58:44,237 DEBUG ++++++ Faults respCol = {
120     '10.102.102.62': {
121     u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
      u'NONE', 'operation_name': 'add_op' }
122    }
123    , (7, '', '2129920_32778'): {
124    'vlan': {
125    u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
      u'NONE', 'operation_name': 'add_op' }
126    }

```



```

127 , (((0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1'), (2, '
      internal', 'provider'))), 'nsip'): {
128 'vlan_nsip_binding': {
129 u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
      u'NONE', 'operation_name': 'bind_op' }
130 }
131 , (((0, '', 5230), (4, 'Network', 'network')), (4, 'nsip', '
      internal_snip'))): {
132 'nsip': {
133 u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
      u'NONE', 'operation_name': 'add_op' }
134 }
135 , (): {
136 }
137 , (8, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
138 'vlan_interface_binding': {
139 u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
      u'NONE', 'operation_name': 'bind_op' }
140 }
141 }
142
143 2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg
      = Done, statusCode = add_op
144 2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg
      = Done, statusCode = add_op
145 2016-06-29 10:58:44,237 DEBUG Fault details oprName = bind_op,
      erMsg = Done, statusCode = bind_op
146 2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg
      = Done, statusCode = add_op
147 2016-06-29 10:58:44,238 DEBUG Fault details oprName = bind_op,
      erMsg = Done, statusCode = bind_op
148 2016-06-29 10:58:44,238 DEBUG ++++++ ServiceAudit response
      = {
149 'faults': [], 'state': 0, 'health': [] }
150
151 2016-06-29 10:58:44,238 DEBUG APIC Graph Details = {
152 'graphDN': u'uni/vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[
      uni/tn-coke_SDX2]-ctx-cokectx1', (1, '', 5790): {
153 'state': 1, 'graphrn': u'vGrp-[uni/tn-coke_SDX2/GraphInst_C-[uni/tn-
      coke_SDX2/brc-TestCntr_3]-G-[uni/tn-coke_SDX2/AbsGraph-
      HybridModeGraph_1]-S-[uni/tn-coke_SDX2]]' }
154 , 'tenantName': 'coke_SDX2', 'StyleBookName': 'APIC-HTTP-LB', '
      graphInstanceName': 'HybridModeGraph_1', 'context': 'cokectx1', '
      graphInstanceId': 5790 }
155
156 2016-06-29 10:58:44,242 DEBUG Journal Processing: Database task:
      create apic_graph
157 2016-06-29 10:58:44,264 DEBUG SUCCESS created task 2
158 2016-06-29 10:58:44,269 DEBUG SUCCESS updated track with new task 2
159 2016-06-29 10:58:44,308 DEBUG ++++++ get IP and Connector
      collection from Config with type 22 for attach & detach event
      ++++++
160 2016-06-29 10:58:44,308 DEBUG ----- connector with IP List = {

```



```

161 0: [], 1: [], 3: [] }
162
163 2016-06-29 10:58:44,308 DEBUG ----- attachIpList = [] dettachIpList
      = []
164 2016-06-29 10:58:44,308 DEBUG ----- In _attachDettachIps
      attachIpList = [] dettachIpList = []
165 2016-06-29 10:58:44,312 DEBUG ----- In _attachDettachIps row = {
166 'deviceIP': u'10.102.102.62', 'responseToAPIC': None, 'graphDN': u'uni
      /vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[uni/tn-
      coke_SDX2]-ctx-cokectx1', 'apicGraphState': None, 'serviceGroupName
      ': None, 'configPackId': None, 'tenantName': u'coke_SDX2', '
      styleBookName': u'APIC-HTTP-LB', 'graphInstanceName': u'
      HybridModeGraph_1', 'context': u'cokectx1', 'serviceGroupPort':
      None, 'graphInstanceId': 5790, 'createDate': None, 'serviceGroupIP'
      : None }
167
168 <!--NeedCopy-->

```

## Journaux générés par le package de périphériques en mode hybride

February 1, 2024

Le package de périphériques Citrix ADC Hybrid Mode génère des journaux liés à la configuration et des journaux liés à la surveillance. Les journaux générés se trouvent à l'adresse **/data/devicescript/Citrix.NetScalerMas.1.0/logs**.

Voici un exemple de fragment de **debug.logd** d'un Cisco APIC :

```

1 2016-06-28 03:06:53.879767 DEBUG Thread-20 18723 [10.102.102.62,
      24063] Device manager details ip = 10.102.102.81, port = 80
2 2016-06-28 03:06:53.879856 DEBUG Thread-20 18724 [10.102.102.62,
      24063] ++++++ serviceAudit request ++++++
3 2016-06-28 03:06:53.879929 DEBUG Thread-20 18725 [10.102.102.62,
      24063] ++++++ getStyleBookObjects ++++++
4 2016-06-28 03:06:53.879995 DEBUG Thread-20 18726 [10.102.102.62,
      24063] NMAS collection A3 = (4, 'Stylebook', 'stylebook_1') B3 =
      {
5  'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
6  (5, 'name', 'stylebookName'): {
7  'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'APIC-HTTP-LB'
      }
8  }
9  }
10
11 2016-06-28 03:06:53.880045 DEBUG Thread-20 18727 [10.102.102.62,
      24063] NMAS collection styleBookName= APIC-HTTP-LB
12 2016-06-28 03:06:53.880093 DEBUG Thread-20 18728 [10.102.102.62,
      24063] NMAS collection retCol= {

```

```
13 'Stylebook': 'APIC-HTTP-LB', 'tuple': ((0, '', 5230), (4, 'Stylebook',
    'stylebook_1')) }
14
15 2016-06-28 03:06:53.880140 DEBUG Thread-20 18729 [10.102.102.62,
    24063] ++++ devMgrStyleBookUrl = http://10.102.102.81/stylebook
    /nitro/v1/config/stylebooks/com.citrix.adc.stylebooks/1.1/APIC-
    HTTP-LB
16 2016-06-28 03:06:54.135240 DEBUG Thread-20 18730 [10.102.102.62,
    24063] ++++ Response from styleBookresCode serviceAudit = {
17 u'stylebook': {
18 u'uses_built_in_namespaces': {
19 u'netScaler.nitro.config': u'10.5' }
20 , u'name': u'APIC-HTTP-LB', u'used_by_stylebooks': [], u'namespace': u
    'com.citrix.adc.stylebooks', u'source': u'---\nname: APIC-HTTP-LB\
    namespace: com.citrix.adc.stylebooks\nversion: "1.1"\ndisplay-name
    : "Sample StyleBook for APIC Load Balanced Application"\
    ndescription: "This is a sample StyleBook for HTTP Load Balanced
    Application configuration via APIC"\nschema-version: "1.0"\nimport-
    stylebooks: \n - \n namespace: netScaler.nitro.config\n
    prefix: ns\n version: "10.5"\n - \n namespace: "com.citrix.
    adc.stylebooks"\n prefix: "stlb"\n version: "1.1"\nparameters
    -default-sources:\n - stlb::APIC-ROOT\nsubstitutions:\n lb-name(
    appname, port): $appname + "-" + str($port) + "-lb"\n sg-name(
    appname, port): $appname + "-" + str($port) + "-sg"\n
    healthmonitor[]:\n true: "NO"\n false: "YES"\ncomponents: \n
    - \n name: lbvserver\n type: ns::lbvserver\n repeat:
    $parameters.app-services\n repeat-item: app\n properties: \
    n name: $substitutions.lb-name($parameters.appname, $app.
    virtual-port)\n ipv46: $app.virtual-ip\n port: $app.
    virtual-port\n servicetype: $app.protocol\n lbmethod?:
    $app.algorithm\n persistencetype?: $app.persistence\n - \n
    name: svcgrp\n type: ns::servicegroup\n repeat: $parameters.
    app-services\n repeat-item: app\n properties: \n name:
    $substitutions.sg-name($parameters.appname, $app.virtual-port)\
    n servicetype: $app.protocol\n useproxyport?: $app.sg-
    advanced.useproxyport\n usip?: $app.sg-advanced.usip\n
    cip?: $app.sg-advanced.cip\n cipheader?: $app.sg-advanced.
    cipheader\n healthmonitor?: $substitutions.healthmonitor($app.
    skip_healthmonitor)\n components: \n -\n name:
    lbvserver-svg-binding\n type: ns::
    lbvserver_servicegroup_binding\n properties: \n
    name: $substitutions.lb-name($parameters.appname, $app.virtual-port
    )\n servicegroupname: $parent.properties.name\n - \
    n name: svg-members\n type: ns::
    servicegroup_servicegroupmember_binding\n condition: $app.
    server-ips\n repeat: $app.server-ips\n repeat-item:
    serverip\n properties: \n ip: $serverip\n
    port: $app.server-port\n servicegroupname: $parent.
    properties.name\noutputs: \n - \n name: lbvservers\n value:
    $components.lbvserver\n - \n name: servicegroups\n value:
    $components.svcgrp', u'version': u'1.1', u'uses_stylebooks': [{
21 u'version': u'1.1', u'namespace': u'com.citrix.adc.stylebooks', u'name
    ': u'APIC-ROOT' }
```

```
22 ] }
23 }
24
25 2016-06-28 03:06:54.359142 DEBUG Thread-20 18731 [10.102.102.62,
    24063] +++++ Dev Mgr request details devMgrUrl = http://
    10.102.102.81/admin/v1/apic
26 2016-06-28 03:06:54.359221 DEBUG Thread-20 18732 [10.102.102.62,
    24063] +++++ Response from Device Mgr serviceAudit = {
27 "APIC":[] }
28
29 2016-06-28 03:06:54.359266 DEBUG Thread-20 18733 [10.102.102.62,
    24063] +++++ serviceAudit response = {
30 "APIC":[] }
31
32 2016-06-28 03:06:54.359306 DEBUG Thread-20 18734 [10.102.102.62,
    24063] +++++ serviceAudit response headers content type
    = application/json; charset=utf-8
33 2016-06-28 03:06:54.359394 DEBUG Thread-20 18735 [10.102.102.62,
    24063] +++++ serviceAudit response headers = {
34 'content-length': '11', 'job_id': 'ctxt-f4db2883-e42c-4262-a35f-04628
    c4ad5ea', 'x-content-type-options': 'nosniff', 'transfer-encoding':
    'chunked', 'connection': 'close', 'date': 'Wed, 29 Jun 2016
    10:58:33 GMT', 'x-frame-options': 'SAMEORIGIN', 'content-type': '
    application/json; charset=utf-8' }
35
36 2016-06-28 03:06:54.359480 DEBUG Thread-20 18736 [10.102.102.62,
    24063] +++++ pollingURL = http://10.102.102.81/admin/v1
    /journalcontexts/ctxt-f4db2883-e42c-4262-a35f-04628c4ad5ea
37 2016-06-28 03:06:54.359713 DEBUG Thread-20 18737 [10.102.102.62,
    24063] +++++ pollingStatus = True, pollingTime = 0
38 2016-06-28 03:06:54.483228 DEBUG Thread-20 18738 [10.102.102.62,
    24063] +++++ pollingResponse json = {
39 u'journalcontext': {
40 u'status': u'In Progress', u'scopes': [], u'entity_id': None, u'name':
    u'Create apic', u'operation': u'POST', u'entity_type': u'apic', u'
    service_name': u'admin', u'start_time': u'2016-06-29T10
    :58:33.760565', u'is_default': u'false', u'end_time': None, u'
    target': u'10.102.102.81', u'message': None, u'id': u'ctxt-f4db2883
    -e42c-4262-a35f-04628c4ad5ea', u'replication_status': u'' }
41 }
42
43 2016-06-28 03:07:04.493074 DEBUG Thread-20 18739 [10.102.102.62,
    24063] +++++ pollingStatus = True, pollingTime = 1
44 2016-06-28 03:07:04.587595 DEBUG Thread-20 18767 [10.102.102.62,
    24063] +++++ pollingResponse json = {
45 u'journalcontext': {
46 u'status': u'In Progress', u'scopes': [], u'entity_id': None, u'name':
    u'Create apic', u'operation': u'POST', u'entity_type': u'apic', u'
    service_name': u'admin', u'start_time': u'2016-06-29T10
    :58:33.760565', u'is_default': u'false', u'end_time': None, u'
    target': u'10.102.102.81', u'message': None, u'id': u'ctxt-f4db2883
    -e42c-4262-a35f-04628c4ad5ea', u'replication_status': u'' }
47 }
```

```
48
49     2016-06-28 03:07:14.597812 DEBUG Thread-20 18790 [10.102.102.62,
      24063] ++++++ pollingStatus = True, pollingTime = 2
50     2016-06-28 03:07:14.692590 DEBUG Thread-20 18791 [10.102.102.62,
      24063] ++++++ pollingResponse json = {
51     u'journalcontext': {
52     u'status': u'Finished', u'scopes': [], u'entity_id': None, u'name': u'
      Create apic', u'operation': u'POST', u'entity_type': u'apic', u'
      service_name': u'admin', u'start_time': u'2016-06-29T10
      :58:33.760565', u'is_default': u'false', u'end_time': u'2016-06-29
      T10:58:44.486919', u'target': u'10.102.102.81', u'message': u'Done'
      , u'id': u'ctxt-f4db2883-e42c-4262-a35f-04628c4ad5ea', u'
      replication_status': u'' }
53     }
54
55     2016-06-28 03:07:14.692932 DEBUG Thread-20 18793 [10.102.102.62,
      24063] Attempts 1
56     2016-06-28 03:07:14.693031 DEBUG Thread-20 18794 [10.102.102.62,
      24063] Cluster (u'uni/tn-coke_SDx2/lDevVip-ADCHybridMode_1', (0,
      '', 5230)), transaction: 0
57     2016-06-28 03:07:14.693147 DEBUG Thread-20 18795 [10.102.102.62,
      24063] Attempts for {
58     'name': 'ADCHybridMode_1', 'host': '10.102.102.62', 'virtual': False,
      'devs': {
59     'ADCHybridMode_1_Device_1': {
60     'state': 0, 'virtual': False, 'manager': {
61     'hosts': {
62     '10.102.102.81': {
63     'port': 80 }
64     }
65     , 'name': 'NMA_S_1', 'creds': {
66     'username': 'nsroot', 'password': '<hidden>' }
67     }
68     , 'version': '11.0', 'host': '10.102.102.62', 'port': 80, 'creds': {
69     'username': 'nsroot', 'password': '<hidden>' }
70     }
71     }
72     , 'manager': {
73     'hosts': {
74     '10.102.102.81': {
75     'port': 80 }
76     }
77     , 'name': 'NMA_S_1', 'creds': {
78     'username': 'nsroot', 'password': '<hidden>' }
79     }
80     , 'contextaware': True, 'port': 80, 'creds': {
81     'username': 'nsroot', 'password': '<hidden>' }
82     }
83     is 0
84     2016-06-28 03:07:14.693339 DEBUG Thread-20 18796 [10.102.102.62,
      24063] Deleting (u'uni/tn-coke_SDx2/lDevVip-ADCHybridMode_1',
      (0, '', 5230))
85     2016-06-28 03:07:14.693379 DEBUG Thread-20 18797 [10.102.102.62,
```

```
      24063] pending: False, delete: False, txId: None
86      2016-06-28 03:07:14.693517 DEBUG Thread-20 18798 [10.102.102.62,
      24063] Faults: []
87      2016-06-28 03:07:14.693558 DEBUG Thread-20 18799 [10.102.102.62,
      24063] Health: []
88      2016-06-28 03:07:14.693914 DEBUG Thread-20 18800 [10.102.102.62,
      24063] Send num: 761, type: 220, len: 382
89 <!--NeedCopy-->
```

## Package de périphériques Citrix ADC en mode Cloud Orchestrator de Cisco ACI

February 1, 2024

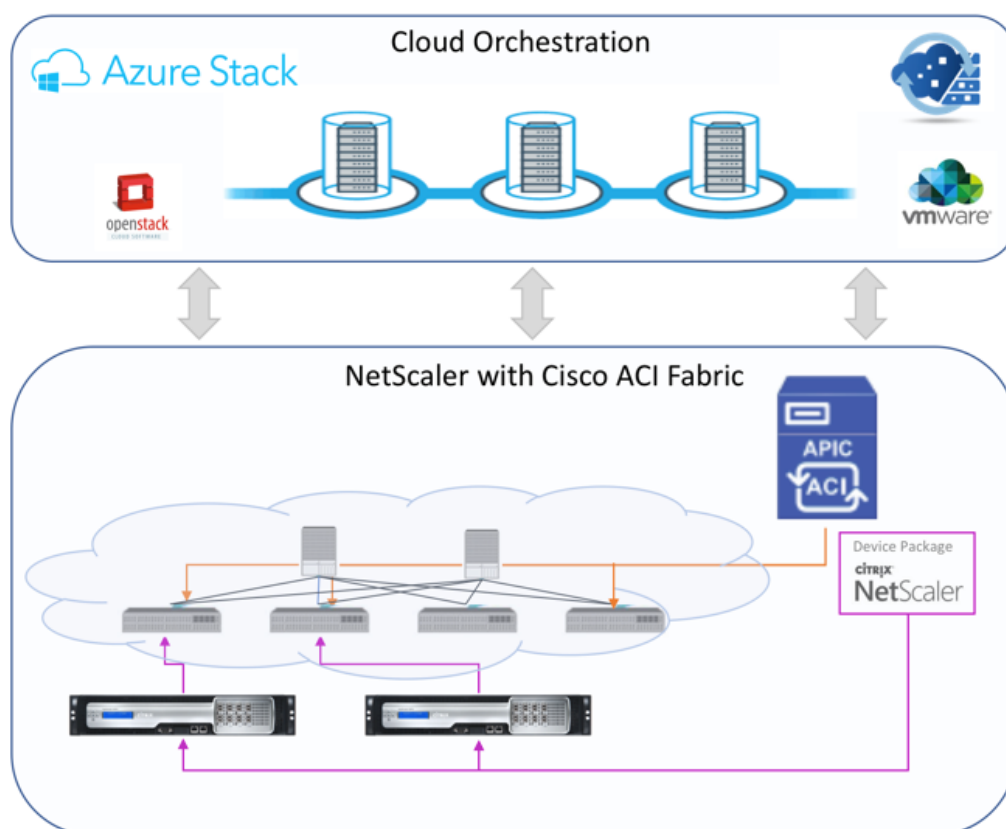
Avec Application Policy Infrastructure Controller (APIC) version 3.1, Citrix ADC et Cisco ACI étendent le portefeuille d'intégration conjoint pour fournir une nouvelle solution répondant aux besoins des clients. Le nouveau mode d'intégration, le mode ACI Cloud Orchestrator\*, simplifie les intégrations L4-L7 en supprimant la complexité de la configuration grâce à des paramètres normalisés. La solution fonctionne de manière transparente pour automatiser les services L4-L7, atteindre les objectifs de déploiement d'applications agiles, de flexibilité opérationnelle et de simplicité.

Le mode orchestrateur de cloud Cisco ACI à l'aide de la solution Citrix ADC offre les avantages suivants :

- L'automatisation des services L4-L7 réduit les erreurs humaines.
- L'intégration prédéfinie de la solution Cisco ACI vous aide à réduire le temps de déploiement et augmente les performances des applications, telles que les applications Web, les machines virtuelles et SQL.
- Visibilité entièrement intégrée sur la santé des applications telles que les applications Web, les machines virtuelles et SQL sur les composants réseau physiques et virtuels.

Le mode Orchestrator cloud ACI vous offre désormais plus de choix pour utiliser la nouvelle interface graphique APIC simplifiée directement ou en sélectionnant n'importe quel orchestrateur de cloud, tel que Cisco Cloud Center, Windows Azure Pack, OpenStack, vRealize ou tout autre en fonction de vos préférences. Cette nouvelle modification est réalisée en exposant un ensemble d'attributs ADC en tant que schéma ADC. Ces attributs sont mappés dans les profils de fonction des packages d'appareils. Vous pouvez fournir des valeurs pour ces attributs lors du Provisioning du service ADC par l'orchestrateur de cloud (Cisco Cloud Center ou Wireless Application Protocol (WAP)).

L'illustration suivante fournit une vue d'ensemble de Citrix ADC dans une solution d'orchestration cloud :

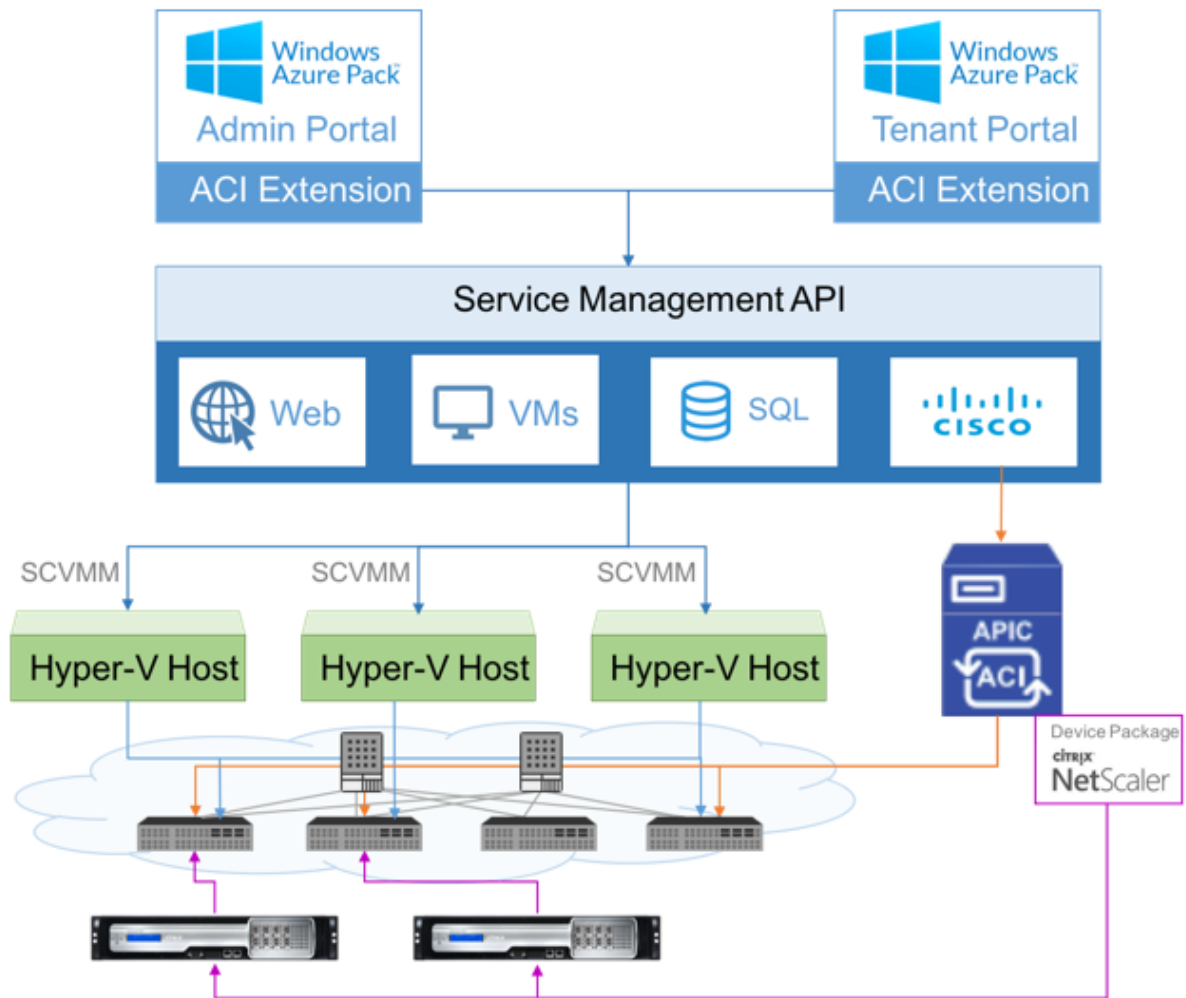


La solution en mode d'orchestrateur de cloud utilisant Microsoft Azure Pack implique de nombreux points d'intégration, tels qu'Azure Pack vers Cisco APIC, Cisco APIC vers System Central Virtual Machine Manager (SCVMM) et Cisco APIC vers Citrix ADC. En tant que locataire dans le cloud privé, vous pouvez activer le NAT, fournir des services réseau et ajouter un équilibreur de charge.

Azure Pack prend en charge les portails des locataires et des administrateurs, et chacun d'eux possède son propre ensemble d'opérations pouvant être effectuées.

- En tant qu'administrateur, vous pouvez effectuer des tâches administratives telles que l'enregistrement ACI, la plage d'adresses IP virtuelles, l'association d'appareils Citrix ADC avec le cloud de machines virtuelles et la création de comptes d'utilisateurs locataires.
- En tant que locataire, vous pouvez effectuer des tâches telles que vous connecter au portail locataire Azure Pack et configurer le réseau, les domaines de pont et le routage et le transfert virtuels (VRF), et pouvez utiliser les fonctionnalités d'équilibrage de charge Citrix ADC et RNAT.

L'illustration suivante fournit une vue d'ensemble d'Azure Pack dans une solution en mode cloud :



**Important**

- L'administrateur du cloud peut faciliter la tâche avec le schéma L4-L7 pris en charge par l'APIC et toute modification supplémentaire peut être effectuée par l'administrateur APIC directement dans l'APIC. Cela vous permet de configurer et de déployer Citrix ADC au même niveau que l'ensemble des fonctionnalités prises en charge.
- Les locataires peuvent déployer plusieurs adresses VIP avec différents ports pour le même réseau. Vous devez vous assurer que la combinaison IP et port est unique.
- Le package d'appareils Citrix ADC prend uniquement en charge le déploiement à contexte unique. Chaque locataire reçoit une instance Citrix ADC dédiée.
- Le protocole d'application sans fil (WAP) prend en charge les appliances Citrix ADC MPX et les appliances Citrix ADC VPX (y compris les instances Citrix ADC VPX déployées sur la plateforme Citrix ADC SDX).

Le package d'appareils en mode orchestrateur cloud prend en charge à la fois le mode entièrement géré et le mode gestionnaire de services. Le package de mode entièrement géré prend en charge une grande variété de profils de fonction, tels que l'équilibrage de charge simple, la commutation de contenu, le déchargement SSL et d'autres profils. Ces profils de fonction couvrent un ensemble complet de fonctionnalités et le mode de déploiement de Citrix ADC. De même, le package de périphériques en mode gestionnaire de services prend en charge la configuration à un et deux bras et le déploiement de Citrix ADC à l'aide d'APIC. Citrix Application Delivery Management (ADM) agit en tant que gestionnaire de services pour APIC et vous pouvez utiliser Citrix ADM pour configurer les paramètres Citrix ADC L4-L7.

### Remarque

En mode gestionnaire de services (mode hybride), vous ne pouvez pas réutiliser ou réattribuer la même adresse IP du serveur, qui est déjà présente dans l'appliance Citrix ADC.

Le profil de fonction du mode Orchestrator Cloud possède un ensemble de paramètres mappés au schéma ADC des APIC et l'orchestrateur utilise ces paramètres. L'orchestrateur de cloud fournit les valeurs des paramètres ADC (VIP, tout en provisionnant Citrix ADC via APIC). L'orchestrateur communique avec les API de l'APIC et transmet les détails spécifiques à l'ADC dans le cadre de la charge utile d'un profil de fonction spécifique. En interne, APIC extrait les valeurs et les transmet au package de périphérique qui configure l'Citrix ADC en interne.

Pour plus d'informations sur la liste complète des schémas ADC, qui sont pris en charge par les API Cisco, reportez-vous au Guide de déploiement des services [Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 3.x and earlier](#).

Le package de périphériques en mode entièrement géré prend en charge les profils de fonctions suivants :

1. LB-HTTP-One-Arm-ProfileCM
2. LB-HTTP-Two-Arm-ProfileCM
3. LB-HTTP-Two-Arm-ServiceBackendProfileCM
4. CS-HTTP-LB-Service-ProfileCM
5. CS-SSL-LB-Service-ProfileCM
6. LB-SSL-ProfileCM
7. SSLVServerProfileInlineModeCM
8. WebVServerProfileWithRHICM
9. WebInlineVServerProfileWithRHICM
10. WebAnywhereVServerProfileWithRHICM



11. SSLVServerProfileForAnywhereModeCM
12. SSLAnywhereServerProfileCM
13. WebVServerProfileCM
14. WebInlineVServerProfileCM
15. WebAnywhereVServerProfileCM
16. CSLBServerProfileCM
17. GSLBServerProfileCM
18. CMPServerProfileCM
19. CRServerProfileC
20. DNSServerProfileCM
21. DSServerProfileCM
22. ICServerProfileCM
23. SSLVPNServerProfileCM
24. AppFWServerProfileCM
25. AAAServerProfileCM
26. AAASyslogServerProfileCM
27. IPv6WebInlineVServerProfileCM

Le package d'appareils en mode de gestion des services prend en charge les profils de fonction du mode cloud suivants :

1. ADCOneArmFunctionProfileCM
2. AADCTwoArmFunctionProfileCM
3. RHI-ADCOneArmFunctionProfileCM
4. RHI-ADCTwoArmFunctionProfileCM

Citrix ADC prend en charge les profils de fonction mentionnés ci-dessus. L'APIC prend en charge un sous-ensemble de ces paramètres dans le schéma ADC. Si des attributs non pris en charge par Cisco ACI sont présents dans le profil de fonction, vous devez cloner le profil de fonction du mode orchestrateur de cloud et fournir les valeurs pour tous les attributs non pris en charge par APIC et enregistrer les attributs. Plus tard, l'orchestrateur peut utiliser le profil de fonction récemment cloné.

Le package d'appareils en mode Citrix Cloud prend en charge Citrix ADC 12.0 et le mode gestionnaire de services utilise également Citrix ADM 12.0. Le package de l'appareil a changé la version du modèle

de 1.0 à 2.0 et peut être utilisé comme nouvelle installation. Le package d'appareils en mode Orchestrator Cloud ne peut pas être mis à niveau à partir des versions précédentes du package d'appareils car la version du modèle a

Les packages d'appareils en mode Orchestrator Cloud peuvent également être utilisés dans le cadre d'un déploiement régulier. Le package n'oblige pas l'utilisateur à provisionner Citrix ADC via un orchestrateur de cloud. Le package de l'appareil est compatible uniquement avec APIC et APIC avec un orchestrateur de cloud.

## Capacité du pool de Citrix ADC

February 1, 2024

La capacité mise en commun Citrix ADC vous permet de partager des licences de bande passante ou d'instance entre différents facteurs de forme ADC. Pour les instances basées sur un abonnement à un processeur virtuel, vous pouvez partager la licence de processeur virtuel entre les instances. Utilisez cette capacité groupée pour les instances qui se trouvent dans le centre de données ou les clouds publics. Lorsqu'une instance n'a plus besoin des ressources, elle vérifie la capacité allouée dans le pool commun. Réutilisez la capacité libérée vers d'autres instances ADC qui ont besoin de ressources.

Vous pouvez utiliser les licences groupées pour optimiser l'utilisation de la bande passante en garantissant l'allocation de bande passante nécessaire à une instance et pas plus que ce dont elle a besoin. Augmentez ou diminuez la bande passante allouée à une instance au moment de l'exécution sans affecter le trafic. Avec les licences de capacité groupée, vous pouvez automatiser le Provisioning des instances.

### Comment fonctionnent les licences de capacité groupées Citrix ADC

La capacité mise en pool Citrix ADC comprend les composants suivants :

- Les instances Citrix ADC, qui peuvent être classées dans les catégories suivantes :
  - Matériel à capacité nulle
  - Instances VPX autonomes ou instances CPX
- Pool de bande passante
- Pool d'instances
- Citrix ADM configuré en tant que serveur de licences

## Matériel à capacité nulle

Lorsqu'elles sont gérées via la capacité mise en commun Citrix ADC, les instances MPX et SDX sont appelées « matériel à capacité nulle » car ces instances ne peuvent pas fonctionner tant qu'elles n'ont pas retiré les ressources de la bande passante et des pools d'instances. Par conséquent, 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. Toutefois, vous ne pouvez pas utiliser la capacité mise en commun Citrix ADC vers une autre instance matérielle Citrix ADC.

Gérez et installez les licences de plateforme. Vous devez installer une licence de plate-forme manuellement, en utilisant le numéro de série du matériel ou le code d'accès à la licence. Une fois qu'une licence de plate-forme est installée, elle est verrouillée sur le matériel et ne peut pas être partagée entre les instances matérielles Citrix ADC à la demande. Toutefois, vous pouvez déplacer manuellement la licence de plate-forme vers une autre instance matérielle Citrix ADC.

Les instances ADC MPX exécutant le logiciel ADC version 11.1 build 54.14 ou ultérieure et les instances SDX ADC exécutant 11.1 build 58.13 ou version ultérieure prennent en charge la capacité groupée ADC. Pour en savoir plus, voir le **tableau 1. Capacité groupée prise en charge pour les instances MPX et SDX**.

## Instances Citrix ADC VPX autonomes

Les instances Citrix ADC VPX exécutant le logiciel Citrix ADC version 11.1 Build 54.14 et ultérieure sur les hyperviseurs suivants prennent en charge la capacité mise en commun :

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM

Les instances Citrix ADC VPX exécutant le logiciel Citrix ADC version 12.0 Build 51.24 et versions ultérieures sur les hyperviseurs et plates-formes cloud suivants prennent en charge la capacité groupée

- Microsoft Hyper-V
- AWS
- Microsoft Azure

### Remarque

Pour activer la communication entre Citrix ADM et Microsoft Azure ou AWS, un tunnel IPSEC doit

être configuré. Pour plus d'informations, consultez [Ajouter des instances Citrix ADC VPX déployées dans le cloud à Citrix ADM](#).

Contrairement au matériel à capacité nulle, VPX ne nécessite pas de licence de plate-forme. Pour traiter le trafic, il doit extraire la bande passante et une licence d'instance du pool.

## Instances Citrix ADC CPX autonomes

Les instances Citrix ADC CPX déployées sur un hôte Docker prennent en charge la capacité en pool. Contrairement au matériel à capacité nulle, le CPX ne nécessite pas de licence de plate-forme. Pour traiter le trafic, il doit extraire une licence d'instance du pool.

## Pool de bande passante

Le pool de bande passante est la bande passante totale qui peut être partagée par les instances Citrix ADC, physiques et virtuelles. Le pool de bande passante comprend des pools distincts pour chaque édition logicielle (Standard, Enterprise et Platinum). Une instance Citrix ADC donnée ne peut pas avoir de bande passante provenant de différents pools récupérés simultanément. Le pool de bande passante à partir duquel il peut extraire la bande passante dépend de l'édition logicielle pour laquelle il est licencié.

## Pool d'instances

Le pool d'instances définit le nombre d'instances VPX ou CPX pouvant être gérées via la capacité mise en commun Citrix ADC ou le nombre d'instances VPX dans une instance SDX-Z.

Lorsqu'elle est retirée du pool, une licence déverrouille les ressources des instances MPX-Z, SDX-Z, VPX et CPX, y compris les CPUS/PES, les cœurs SSL, les paquets par seconde et la bande passante.

### Remarque

Le service de gestion d'un SDX-Z ne consomme pas d'instance.

## Serveur de licences Citrix ADM

La capacité groupée Citrix ADC utilise le logiciel Citrix 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 Citrix ADM pour gérer des licences de capacité groupée sans licence ADM.

Lors de la récupération de licences à partir d'un pool de bande passante et d'instances, le facteur de forme Citrix ADC et le numéro de modèle matériel sur un matériel à capacité nulle déterminent

- La bande passante minimale et le nombre d'instances qu'une instance Citrix ADC doit extraire avant d'être fonctionnelle.
- La bande passante maximale et le nombre d'instances qu'un Citrix ADC peut extraire.
- L'unité de bande passante minimale pour chaque sortie de bande passante. L'unité de bande passante minimale est la plus petite unité de bande passante qu'un Citrix ADC doit extraire d'un pool. Toute extraction doit être un multiple entier de l'unité de bande passante minimale. Par exemple, si l'unité de bande passante minimale d'un Citrix ADC est de 1 Gbit/s, 100 Gbit/s peuvent être récupérés, mais pas 200 Mbit/s ou 150,5 Gbit/s. L'unité de bande passante minimale est différente de la bande passante minimale requise. Une instance Citrix ADC ne peut fonctionner qu'après avoir obtenu une licence avec au moins la bande passante minimale. Une fois la bande passante minimale atteinte, l'instance peut extraire plus de bande passante avec l'unité de bande passante minimale.

Les tableaux 1, 2 et 3 résument la bande passante maximale/les instances, la bande passante/les instances minimales et l'unité de bande passante minimale pour toutes les instances NetScaler prises en charge. Le tableau 4 résume les exigences de licence pour différents formats. Pour toutes les instances Citrix ADC prises en charge :

**Tableau 1 Capacité groupée prise en charge pour les instances MPX et SDX**

Ligne de produits	Bande passante maximale (Gbit/s)	Bande passante minimale (Gbps)	Instances minimales	Nombre maximum d'instances	Unité de bande passante minimale
<b>MPX 5900Z</b>	10	1	S/O	S/O	1 Gbit/s
<b>MPX 8005Z</b>	15	5	SO	SO	1 Gbit/s
<b>MPX 8900Z</b>	33	5	SO	SO	1 Gbit/s
<b>Série MPX-14000Z</b>	100	20	SO	SO	1 Gbit/s
<b>Série MPX-15000Z</b>	100	20	SO	SO	1 Gbit/s
<b>MPX-25000Z-40G</b>	200	100	SO	SO	1 Gbit/s
<b>Série MPX-24000Z</b>	150	100	40	80	1 Gbit/s
<b>SDX 8015Z</b>	15	2	1	5	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
<b>SDX 89XX series</b>	33	10	2	7	1 Gbit/s
<b>Série SDX-115XX</b>	42	7	2	20	1 Gbit/s
<b>Série SDX-14000Z</b>	100	10	2	25	1 Gbit/s
<b>SDX 15000Z-50G</b>	100	10 (Remarque : 20 Gbit/s pour les versions inférieures à 12.1 54.x)	2 (Remarque : 5 instances pour les versions inférieures à 12.1 54.x)	55	1 Gbit/s
<b>SDX : 15 000 Hz</b>	100	10 (Remarque : 20 Gbit/s pour les versions inférieures à 12.1 54.x)	2 (Remarque : 5 instances pour les versions inférieures à 12.1 54.x)	55	1 Gbit/s
<b>Série SDX-22XXX</b>	120	20	10	80	1 Gbit/s
<b>SDX-25000Z-40G</b>	200	50	10	115	1 Gbit/s
<b>SDX 26000Z-100G</b>	200	50	10	115	1 Gbit/s
<b>SDX 26000Z</b>	200	50	10	115	1 Gbit/s
<b>SDX 26000Z-50S</b>	200	50	10	115	1 Gbit/s
<b>SDX 8005Z</b>	15	2	1	2	1 Gbit/s
<b>Série SDX-24000Z</b>	150	50	10	80	1 Gbit/s

Remarque

La bande passante minimale et les instances sont applicables aux instances SDX exécutant les versions suivantes et supérieures : 11.1 64.x, 12.0 63.x et 12.1 54.x.

La quantité minimale d'achat est différente de la configuration minimale requise.

**Tableau 2. Capacité groupée prise en charge pour les instances CPX**

	Bande passante maximale (Gbit/s)	Bande passante minimale (Gbps)	Instances minimales	Nombre maximum d' instances	Unité de bande passante minimale
<b>CPX</b>	10	1	1	1	10 Mbit/s

**Tableau 3. Capacité groupée prise en charge pour les instances VPX sur les hyperviseurs et les services cloud**

	Bande passante maximale (Gbit/s)	Bande passante minimale (Mbps)	Instances minimales	Nombre maximum d' instances	Unité de bande passante minimale
<b>Citrix Hypervisor</b>	40 Gbits/s	10 Mbit/s	1	1	10 Mbit/s
<b>VMware ESXI</b>	100 Gbit/s	10 Mbit/s	1	1	10 Mbit/s
<b>Linux KVM</b>	100 Gbit/s	10 Mbit/s	1	1	10 Mbit/s
<b>Microsoft Hyper-V</b>	3 Gbits/s	10 Mbit/s	1	1	10 Mbit/s
<b>AWS</b>	5 Gbits/s	10 Mbit/s	1	1	10 Mbit/s
<b>Azure</b>	3 Gbits/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.

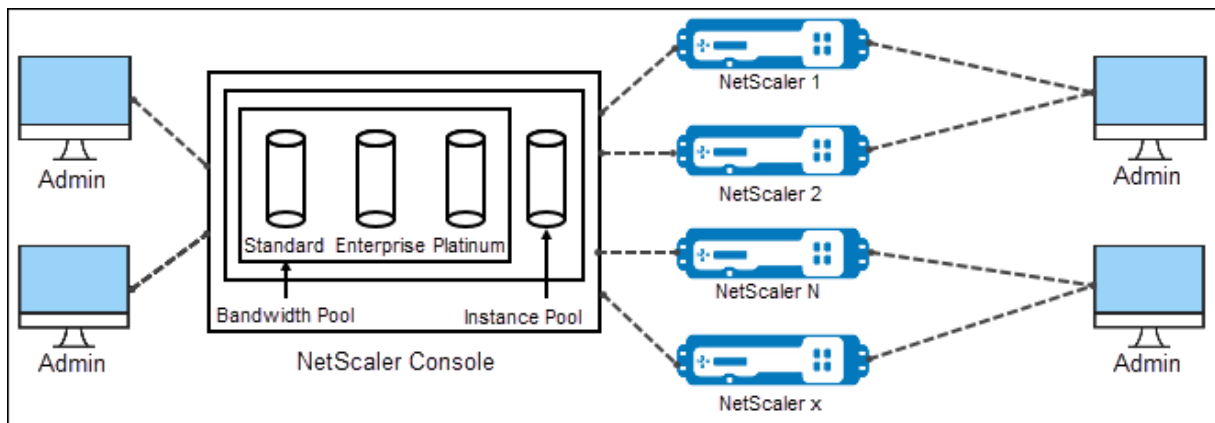
**Tableau 4. Exigence de licence pour différents facteurs de forme**

Ligne de produits	Achat de matériel à capacité nulle	Abonnement Bandwidth & Edition	Abonnement aux instances
<b>MPX</b>	Licence requise	Licence requise	-
<b>SDX</b>	Licence requise	Licence requise	Licence requise
<b>VPX</b>	-	Licence requise	Licence requise
<b>CPX</b>	-	-	Licence requise

## Configurer la capacité du pool de Citrix ADC

February 1, 2024

Citrix Application Delivery Management (ADM) est le serveur de licences pour toutes les instances Citrix ADC ajoutées à ADM. Vous pouvez télécharger les fichiers de licence de capacité groupée (pool de bande passante ou pool d'instances) sur le serveur de licences. Vous pouvez attribuer des licences du pool de licences aux instances Citrix ADC à la demande. Vous pouvez attribuer les licences depuis Citrix ADM ou extraire les licences depuis les instances Citrix ADC (MPX-Z /SDX-Z/VPX/CPX) en fonction de la capacité minimale et maximale de l'instance.



## Versions matérielles et logicielles prises en charge



Version du logiciel Citrix ADC	Matériel Citrix ADC MPX à capacité zéro	Matériel Citrix ADC SDX à capacité zéro	Hyperviseurs pris en charge pour Citrix ADC VPX
11.1 Build 54.14 et versions ultérieures	MPX-14000Z, MPX-14000Z-40G, MPX-25000Z-40G	SDX-14000Z, SDX-14000Z-40G, SDX-25000Z-40G	VMware ESX 6.0, Citrix Hypervisor, KVM Linux
12.0 Build 51.24 et versions ultérieures			Microsoft Hyper-V, Amazon AWS, Microsoft Azure

### Configuration de Citrix ADM en tant que serveur de licences

Vous pouvez configurer Citrix ADM en tant que serveur de licences pour la capacité groupée Citrix ADC. Une instance Citrix ADC peut obtenir de la bande passante ou une licence d'instance de deux manières, ou les deux :

- Une instance Citrix ADC peut lancer la demande de retrait auprès de Citrix ADM pour obtenir sa bande passante et/ou ses licences d'instance.
- Les licences peuvent être attribuées à une instance Citrix ADC via Citrix ADM.

#### Remarque

La capacité groupée s'affiche sur Citrix ADM uniquement si des licences groupées sont ajoutées au Citrix ADM.

Les modes de fonctionnement des instances Citrix ADC qui utilisent la capacité groupée Citrix ADC sont les suivants :

- **Optimum**—L'instance fonctionne avec une capacité de licence appropriée.
- **Incompatibilité** de capacité : l'instance s'exécute avec une capacité inférieure à celle configurée par l'utilisateur.
- **Grace**- L'instance fonctionne sous licence Grace.
- **Grace & Mismatch**—L'instance s'exécute en mode Grace mais avec une capacité inférieure à celle configurée par l'utilisateur.
- **Non disponible**: l'instance n'est pas enregistrée auprès de Citrix ADM pour la gestion ou la communication Nitro entre Citrix ADM et l'instance ne fonctionne pas.
- **Non attribuée**—La licence n'est pas attribuée à l'instance.

#### Pour installer des fichiers de licence sur Citrix ADM :

1. Dans un navigateur Web, saisissez l'adresse IP du **Citrix ADM** (par exemple, <http://192.168.100.1>).

2. Dans **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Accédez à **Réseaux > Licences**.
4. Dans la section **Fichiers de licence**, sélectionnez l'une des options suivantes :

- **Télécharger des fichiers de licences à partir d'un ordinateur local** : si un fichier de licence est déjà présent sur votre ordinateur local, vous pouvez le télécharger sur Citrix ADM. Pour ajouter des fichiers de licence, cliquez sur **Parcourir** et sélectionnez le fichier de licence (.lic) que vous souhaitez ajouter. Cliquez ensuite sur **Terminer**.

#### Remarque

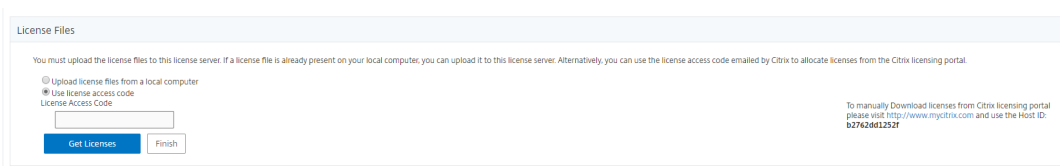
Si les fichiers de licence chargés n'ajoutent pas les licences dans la capacité Citrix ADC Pooled, vous pouvez sélectionner les fichiers de licences et cliquer sur **Appliquer les licences** pour ajouter les licences au pool.



The screenshot shows the 'License Server Port Settings' interface. It contains three columns of information:

Proxy Server Port	License Server Port	Vendor Daemon Port
0	27000	7279
The Proxy Server Port used by Citrix ADC instances to access the Citrix licensing portal for license allocation	The License Server Port used by Citrix ADC instances to communicate with the license server	The Daemon Port used by Citrix ADC instances to communicate with the license server

- **Utiliser le code d'accès à la licence** : Citrix envoie par e-mail le code d'accès à la licence (LAC) pour les licences que vous achetez. Pour ajouter des fichiers de licence, entrez le LAC dans la zone de texte, puis cliquez sur **Obtenir des licences**.



The screenshot shows the 'License Files' section. It contains the following text and controls:

You must upload the license files to this license server. If a license file is already present on your local computer, you can upload it to this license server. Alternatively, you can use the license access code emailed by Citrix to allocate licenses from the Citrix licensing portal.

Upload license files from a local computer  
 Use license access code

License Access Code

To manually Download licenses from Citrix licensing portal please visit <http://www.myCitrix.com> and use the Host ID: 0274236012931

#### Remarque

À tout moment, vous pouvez ajouter d'autres licences à Citrix ADM à partir des paramètres de licence.

**Pour attribuer des licences Citrix ADC Pooled Capacity à partir de Citrix ADM, procédez comme suit :**

#### Remarque

Si vous n'avez pas enregistré l'instance Citrix ADC auprès de Citrix ADM, vous pouvez retirer des licences auprès de Citrix ADM, mais vous ne pouvez pas les attribuer à partir de Citrix ADM à l'instance à capacité groupée Citrix ADC activée.

Assurez-vous que les conditions préalables suivantes sont remplies avant d'allouer des licences de capacité groupée aux instances ADC.

## Prérequis

Avant de pouvoir gérer les licences de pool de votre instance via Citrix ADM, vous devez enregistrer l'instance Citrix ADC auprès de Citrix ADM. Dans l'interface graphique de Citrix ADC, accédez à **Système > Licences > Gérer les licences** et cochez la case **Enregistrer auprès de Citrix ADM pour la gérabilité** lors de l'ajout de l'adresse IP Citrix ADM.

System / Licenses / Manage Licenses

### Licenses

If a license is already present on your local computer, you can upload it to this NetScaler appliance. Alternatively, you can use this appliance's serial number, or the license access code emailed by Citrix, to allocate licenses from the Citrix licensing portal.

To use pooled licenses, select Use pooled licensing and check out licenses from a license server.

Upload license files

Use License Access Code

Use pooled licensing

Server Name/IP Address\*

10.102.29.55

License Port\*

27000

Register with NetScaler MAS for manageability

Username\*

nsroot

Password\*

.....

Continue

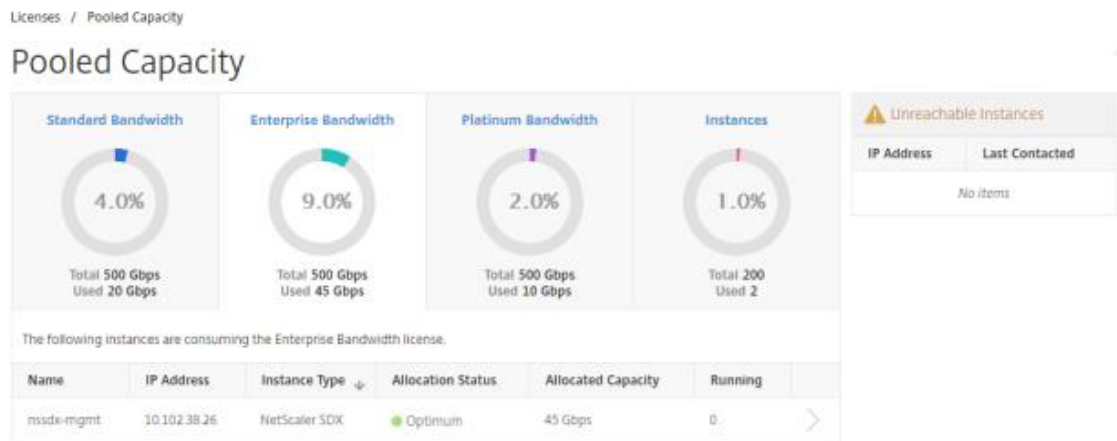
Back

## Remarque

Dans les champs **Nom d'utilisateur** et **Mot de passe** de l'écran ci-dessus, entrez les informations d'identification Citrix ADM.

Une fois l'instance enregistrée auprès du serveur de licences, attribuez les licences comme suit :

1. Dans un navigateur Web, saisissez l'adresse IP de **Citrix ADM** (par exemple, <http://192.168.100.1>).
2. Dans **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Dans l'onglet Configuration, accédez à **Réseaux > Licences > Capacité** groupée.
4. Cliquez sur le pool de licences que vous souhaitez gérer.
5. Sélectionnez une instance Citrix ADC dans la liste des instances disponibles en cliquant sur **le bouton** .



- Si vous souhaitez modifier ou libérer une allocation de licence, cliquez sur **Modifier l'allocation** ou **Libérer l'allocation**.

Licenses / Pooled Capacity / 10.102.29.91

10.102.29.91			Change allocation	Release allocation
Edition Platinum	Instances 1	Bandwidth 10 Mbps		

- Si vous cliquez sur **Modifier l'allocation**, une fenêtre contextuelle contenant les licences disponibles sur le serveur de licences s'affiche.

### Change License Allocation ✕

License edition  
Advanced ▾

TYPE	TOTAL	AVAILABLE	ALLOCATE
Instances	50	49	1
Bandwidth	510 Gbps	500 Gbps	10000 <input type="text"/> Mbps

- Vous pouvez choisir l'allocation de bande passante ou d'instance à l'instance Citrix ADC en définissant les **options** de la liste déroulante Allouer. Après avoir effectué vos sélections, cliquez sur **Allouer**.
- Vous pouvez également modifier l'édition de licence allouée à partir des options déroulantes de la fenêtre Modifier l'allocation de licence.

## Configuration de la capacité groupée Citrix ADC sur MPX-Z

MPX-Z est l'appliance Citrix ADC MPX compatible avec les capacités groupées Citrix ADC. MPX-Z prend en charge le regroupement de bande passante pour les licences Platinum, Enterprise ou Standard.

MPX-Z a besoin des licences de sa plate-forme avant de pouvoir se connecter au serveur de licences. Vous pouvez installer la licence de la plateforme MPX-Z en téléchargeant le fichier de licence depuis un ordinateur local ou en utilisant le numéro de série matériel de l'instance, ou le code d'accès à la licence dans la section **Système > Licences** de l'interface graphique de l'instance Citrix ADC. Si vous supprimez la licence de la plateforme MPX-Z, la fonctionnalité de capacité groupée est désactivée et toutes les licences extraites sont enregistrées 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.

## Configuration de la capacité groupée Citrix ADC sur une instance Citrix ADC VPX

Une instance Citrix ADC VPX à capacité groupée peut extraire des licences d'un pool de bande passante (éditions Platinum/Enterprise/Standard). Vous pouvez utiliser l'interface graphique de Citrix ADC 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, elle récupère automatiquement les licences groupées requises pour sa capacité configurée.

## Allocation de licences de pool à une instance Citrix ADC MPX-Z ou Citrix ADC VPX

### Pour allouer vos licences :

1. Dans un navigateur Web, tapez l'adresse IP de l'instance Citrix ADC (par exemple, <http://192.168.100.1>).
2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.

3. Dans l'onglet Configuration, accédez à **Système > Licences > Gérer les licences**, cliquez sur **Ajouter une nouvelle licence** et sélectionnez **Utiliser les licences groupées**.

System / Licenses / Manage Licenses

### Licenses

If a license is already present on your local computer, you can upload it to this NetScaler appliance. Alternatively, you can use this appliance's serial number, or the license access code emailed by Citrix, to allocate licenses from the Citrix licensing portal.

To use pooled licenses, select Use pooled licensing and check out licenses from a license server.

Upload license files  
 Use License Access Code  
 Use pooled licensing

Server Name/IP Address\*

License Port\*

Register with NetScaler MAS for manageability

Username\*

Password\*

4. Entrez les détails du serveur de licences dans le champ **Nom du serveur/Adresse IP**.
5. Si vous souhaitez gérer les licences de pool de votre instance via Citrix ADM, cochez la case **S'inscrire auprès de Citrix ADM pour la géabilité** et entrez les informations d'identification ADM.
6. Sélectionnez l'édition de la licence et la bande passante requise, cliquez sur **Obtenir des licences**.

**Allocate licenses** ✕

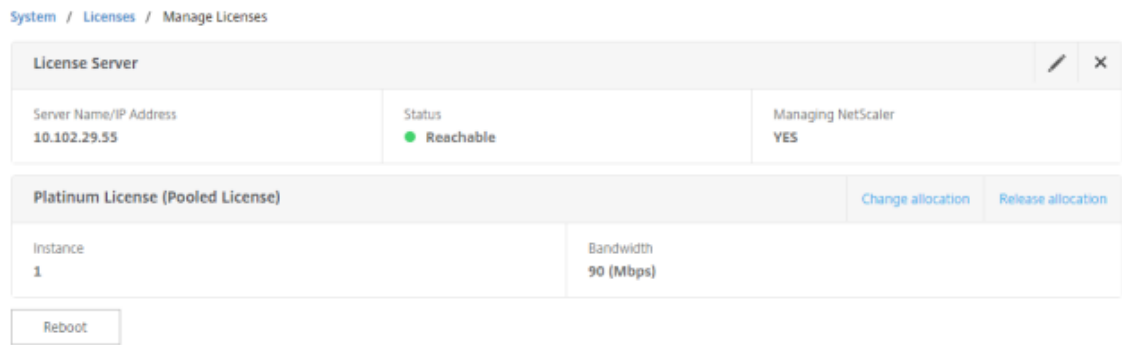
10.102.29.55 (License Server)

Platinum ▾

Pool	Total	Available	Allocate
Instance	200	198	1

Bandwidth 500 Gbps 490 Gbps   Mbps

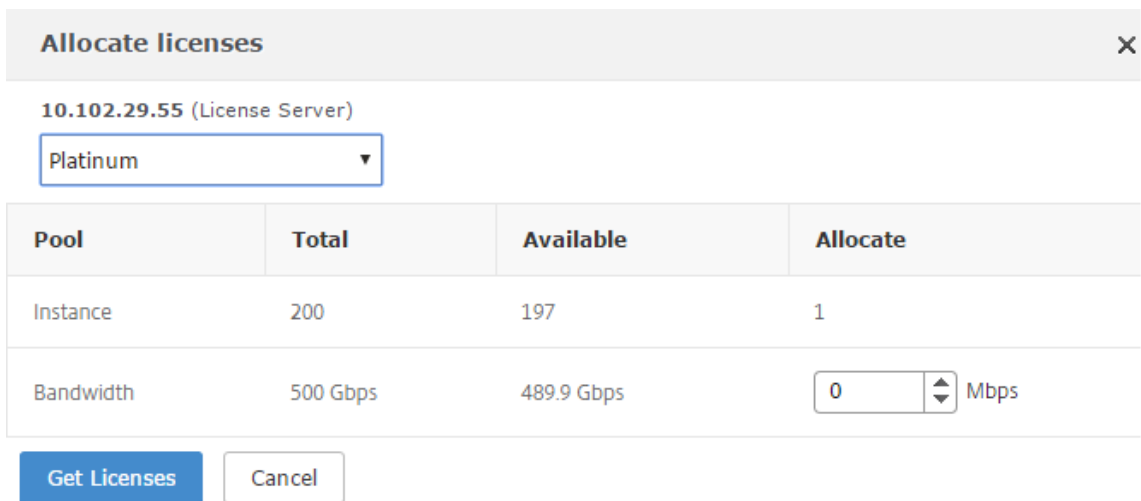
7. Vous pouvez modifier ou libérer l'allocation de licence en sélectionnant **Modifier l'allocation** ou **Libérer l'allocation**.



8. Si vous cliquez sur **Modifier l'allocation**, une fenêtre contextuelle affiche les licences disponibles sur le serveur de licences.

**Remarque**

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.



9. Vous pouvez allouer de la bande passante ou des instances à l'instance Citrix ADC à partir de la liste déroulante **Allouer**. Cliquez ensuite sur **Obtenir des licences**.
10. Vous pouvez choisir l'édition de licence et la bande passante requise dans les listes déroulantes de la fenêtre contextuelle.

**Remarque**

L'allocation de bande passante doit être un multiple de l'unité de bande passante minimale.

## Configuration de la capacité groupée Citrix ADC sur SDX-Z

Une instance SDX-Z est une instance à capacité groupée de Citrix ADC SDX. SDX-Z prend en charge le regroupement de bande passante pour les éditions Platinum, Enterprise et Standard, ainsi que le regroupement d'instances. Une fois que vous avez appliqué la licence de plate-forme SDX-Z, le service de gestion propose des options permettant de récupérer les licences depuis et vers le serveur de licences, et d'allouer de la capacité de bande passante aux instances Citrix ADC exécutées sur la plate-forme SDX-Z.

### Remarque

Les instances Citrix ADC VPX exécutées sur SDX-Z ne peuvent pas extraire directement les licences depuis ou vers le serveur de licences. Cela peut être fait par le service de gestion dans SDX.

Vous pouvez installer la licence de la plateforme SDX-Z soit en téléchargeant le fichier de licence depuis l'ordinateur local, soit en utilisant le numéro de série matériel de l'instance, soit le code d'accès à la licence.

Si vous supprimez la licence de la plateforme SDX-Z, la fonctionnalité de capacité groupée est désactivée et toutes les licences sont réenregistrées sur le serveur de licences.

### Remarque

Si vous redémarrez l'instance, elle vérifie les licences groupées requises pour sa capacité configurée.

## Capacité du pool sur Citrix ADC SDX

### Pool d'instances :

Une appliance SDX peut provisionner le même nombre d'instances que celles disponibles dans le pool d'instances de l'appliance SDX.

### Pool de bande passante :

Lors du provisionnement de l'instance Citrix ADC, la bande passante est allouée à l'instance. Vous pouvez sélectionner l'édition et la bande passante requise pour provisionner une instance Virtual Citrix ADC. Le service de gestion permet au provisionnement de se poursuivre uniquement si l'instance dispose d'une bande passante suffisante pour l'édition demandée. Vous êtes averti si la bande passante est insuffisante.

### Remarque

La modification de la bande passante ne nécessite pas de redémarrage de l'instance.



## Allocation de licences de pool à une instance Citrix ADC SDX-Z

### Pour allouer vos licences :

1. Dans un navigateur Web, saisissez l'adresse IP de votre instance Citrix ADC SDX-Z (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**, puis à **Pooled Capacity**.

System / Manage Licenses

### Licenses

<input type="checkbox"/>	Name	Last Modified	Size
<input type="checkbox"/>	CNS_SDX-Z_1SERVER_RetailLic	2016-08-16 03:10:40	961 bytes

---

**Pooled licenses**

You must now add a license server to this NetScaler SDX appliance and allocate the licenses from the license server.

Licensing Server Name or IP Address\*

Port Number\*

Register with NetScaler MAS

User Name\*

Password\*

4. Entrez les détails du serveur de licences dans le champ **Nom du serveur/Adresse IP**.
5. Si vous souhaitez gérer les licences de pool de votre instance via Citrix ADM, activez la case à cocher **Enregistrer auprès de Citrix ADM** et entrez les informations d'identification ADM.
6. Vous pouvez modifier ou libérer l'allocation de licence en sélectionnant **Modifier l'allocation** ou **Libérer l'allocation**.

#### Remarque

Les licences extraites sont stockées dans un pool distinct par l'ADM.

System / Manage Licenses

The following license files are present on this Appliance. Select **Add New License** to upload more licenses. To delete a license, select the license and click **Delete**.

	Name	Last Modified	Size
<input type="checkbox"/>	CNS_SDX-Z_1SERVER_Retail.lic	2016-08-16 03:10:40	961 bytes

**License Server** ✎ ✕

IP Address 10.102.29.55	Status <span style="color: green;">●</span> <b>Reachable</b>
----------------------------	---

**Pooled Capacity** [Change Allocation](#) [Release Allocation](#)

Instance		Platinum Bandwidth (Gbps)		Enterprise Bandwidth (Gbps)		Standard Bandwidth (Gbps)	
2 <small>Total</small>	0 <small>Used</small>	10 <small>Total</small>	0 <small>Used</small>	45 <small>Total</small>	0 <small>Used</small>	20 <small>Total</small>	0 <small>Used</small>

7. Pour modifier l'allocation de licence pour une instance VPX spécifique dans l'instance SDX-Z, sélectionnez l'instance dans la section **Instances**, puis cliquez sur **Modifier l'allocation**. Une nouvelle fenêtre affiche les licences disponibles.

← Change Allocation

Name

IP Address

Feature License\*  
 For more information about NetScaler editions, see [Citrix NetScaler Editions](#)

Pool	Total	Available	Allocate
Instance	2	1	1
Bandwidth	2 Gbps	1 Gbps	Allocation Mode* <input type="text" value="Fixed"/>
			Throughput (Mbps)* <input type="text" value="2000"/>

8. Vous pouvez modifier l'édition de bande passante de l'instance dans la liste déroulante **Feature License** et la bande passante requise dans le champ **Débit (mbps)**. Cliquez ensuite sur **Done**.

**Remarque**

L'allocation de bande passante doit être un multiple entier de l'unité de bande passante minimale du facteur de forme correspondant.

## Configuration de la capacité groupée Citrix ADC sur une instance Citrix ADC CPX

Lors du provisionnement de l'instance Citrix ADC CPX, vous pouvez configurer l'instance Citrix ADC CPX pour utiliser la capacité groupée Citrix ADC. Dans la commande **docker run**, vous devez fournir les informations relatives au serveur de licences Citrix ADC. L'instance Citrix ADC CPX extrait les licences du pool d'instances.

### Remarque

Par défaut, l'instance Citrix ADC CPX extrait une licence d'instance du pool d'instances et le débit est automatiquement défini sur 1 000 Mbit/s. Vous ne pouvez pas modifier la bande passante de 1 000 Mbit/s allouée à l'instance.

Vous pouvez télécharger Citrix ADC CPX depuis le Docker App Store. Sur l'hôte Docker, pour télécharger Citrix ADC CPX, exécutez la commande suivante :

```
1 docker pull store/citrix/netscalercpx: <version>
2
3 <!--NeedCopy-->
```

### Pour configurer la capacité groupée Citrix ADC lors du provisionnement de l'instance Citrix ADC CPX :

Lors du provisionnement d'une instance Citrix ADC CPX, définissez le serveur de licences Citrix comme variable d'environnement dans la commande **docker run**, comme indiqué ci-dessous :

```
1 docker run -dt -P -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<LS_PORT> --name
   <container_name> --ulimit core=-1 -e EULA=yes -v <host_dir>:/cpx --
   cap-add=NET_ADMIN <REPOSITORY>:<TAG>
2
3 <!--NeedCopy-->
```

Où :

- <LS\_IPADDRESS>est l'adresse IP du serveur de licences Citrix.
- <LS\_PORT>est le port du serveur de licences Citrix. Par défaut, le port est 27000.

## Mettre à niveau une licence perpétuelle dans Citrix ADC MPX vers Citrix ADC Pooled Capacity

February 1, 2024

L'appliance Citrix ADC MPX avec licence perpétuelle peut être mise à niveau vers la licence Citrix ADC Pooled Capacity. La mise à niveau vers la licence Citrix ADC Pooled Capacity vous permet d'allouer des

licences à partir du pool de licences aux appliances Citrix ADC à la demande. Vous pouvez également configurer la licence Citrix ADC Pooled Capacity pour les instances Citrix ADC configurées en mode haute disponibilité. Pour configurer une licence Citrix ADC Pooled Capacity pour les instances Citrix ADC MPX en mode haute disponibilité, voir Mettre à niveau la licence perpétuelle de la paire Citrix ADC MPX High Availability vers Citrix ADC Pooled Capacity.

#### Important

Pour mettre à niveau l'appliance Citrix ADC MPX vers la licence Citrix ADC Pooled Capacity, vous devez télécharger la licence MPX-Z vers l'appliance.

#### Pour passer à la capacité groupée Citrix ADC :

1. Dans un navigateur Web, tapez l'adresse IP de l'appliance Citrix ADC, par exemple <http://192.168.100.1>.
2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification de l'administrateur.
3. Sur la page **Bienvenue**, cliquez sur **Continuer**.
4. Téléchargez la licence à capacité nulle (licence MPX-Z). Sous l'onglet Configuration, accédez à **Système > Licences**.
5. Dans le volet d'informations, cliquez sur **Gérer les licences**, puis sur Ajouter une **nouvelle licence**.
6. Dans la page **Licences**, sélectionnez **Charger des fichiers de licence** et cliquez sur **Parcourir** pour sélectionner la licence de capacité nulle de votre machine locale.
7. Une fois la licence téléchargée, cliquez sur **Redémarrer** pour redémarrer l'appliance.

Assurez-vous qu'aucune configuration n'est enregistrée avant de redémarrer l'appliance.

#### Avertissement

Après l'application de la licence MPX-Z, les fonctionnalités, y compris le téléchargement SSL sur l'appliance, deviennent sans licence. L'appliance arrête le traitement des demandes HTTPS.

Si l'option **Accès sécurisé uniquement** est activée sur l'appliance avant la mise à niveau, vous ne pouvez pas vous connecter à l'appliance via l'interface graphique Citrix ADM à l'aide de HTTPS.

8. Sur la page **Confirmer**, cliquez sur **Oui**.
9. Après le redémarrage de l'appliance, connectez-vous à l'appliance.

10. Sur la page d'accueil, cliquez sur la section **Licences**.

The screenshot shows the NetScaler configuration wizard interface. At the top, there are navigation tabs: Dashboard, Configuration (selected), Reporting, Documentation, and Downloads. A notification bell icon is in the top right. Below the tabs is a 'Welcome!' section with instructions: 'Use this wizard for initial configuration of your NetScaler appliance. To configure or to change a previously configured setting, click each of the sections below. If a parameter has already been configured, a check mark appears within a green circle. An orange circle containing a dash indicates that you have chosen to skip this section.'

The main content area contains four configuration steps, each with an icon, a title, a description, and a progress indicator:

- NetScaler IP Address**: IP address at which you access the NetScaler for configuration, monitoring, and other management tasks. Parameters: NetScaler IP Address (10.217.1.231), Netmask (255.255.255.0). Progress: 1 (green checkmark).
- Subnet IP Address**: Specify an IP address for your NetScaler to communicate with the backend servers. Parameter: Subnet IP Address (Not configured). Progress: 2 (orange circle with dash).
- Host Name, DNS IP Address, and Time Zone**: Specify a host name to identify your NetScaler, an IP address for a DNS server to resolve domain names, and the time zone in which your NetScaler is located. Parameters: Host Name (undefined), DNS IP Address (Not configured), Time Zone (CoordinatedUniversalTime). Progress: 3 (orange circle with dash).
- Licences**: Upload licenses from your local computer or allocate licenses from the Citrix licensing portal. You can also allocate pooled capacity from an on-premise license server. There are 3 license file(s) present on this NetScaler. Progress: 4 (orange circle with dash).

The 'Licences' step is highlighted with a red dashed border. A blue 'Continue' button is located at the bottom left of the wizard.

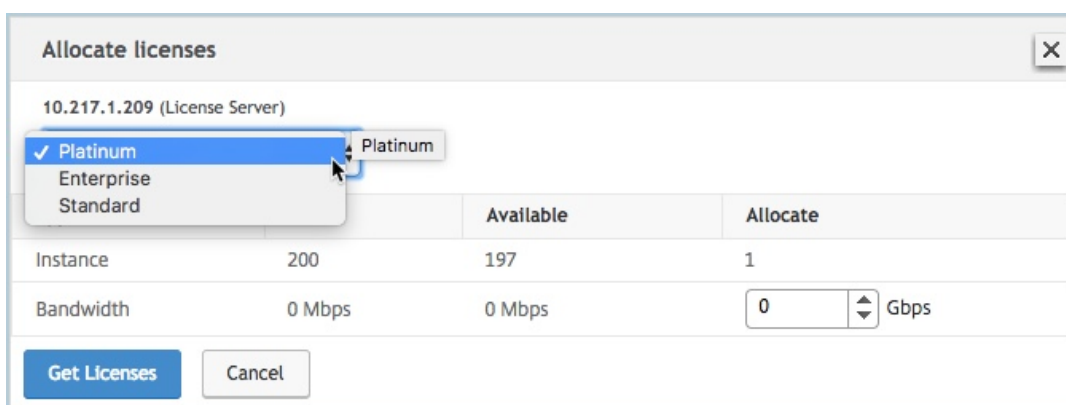
11. Dans la section **Serveur de licences**, procédez comme suit :

The screenshot shows the 'Configuration' tab of the NetScaler Application Delivery Management interface. At the top, there are navigation tabs: 'Dashboard', 'Configuration', 'Reporting', 'Documentation', and 'Downloads'. Below these, there are two buttons: 'Add New License' and 'Delete'. A table lists licenses with columns for a checkbox and 'Name'. One license is listed: 'CNS\_MPX-Z\_1SERVER\_Retail.lic'. Below the table is a section titled 'License Server' with the following fields:

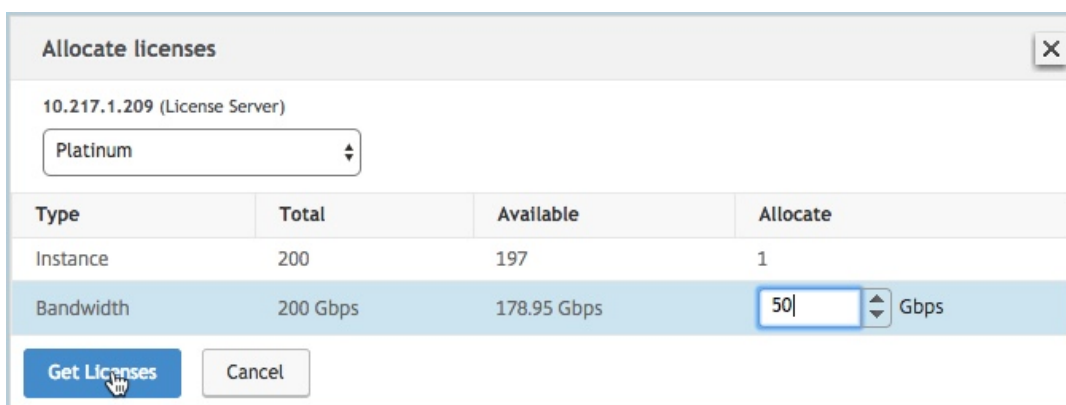
- Server Name/IP Address\*: 10.217.1.209
- License Port\*: 27000
- Register with Licensing Server for manageability
- User Name\*: nsroot
- Password\*: [masked with dots]

At the bottom of the form are two buttons: 'Continue' and 'Cancel'.

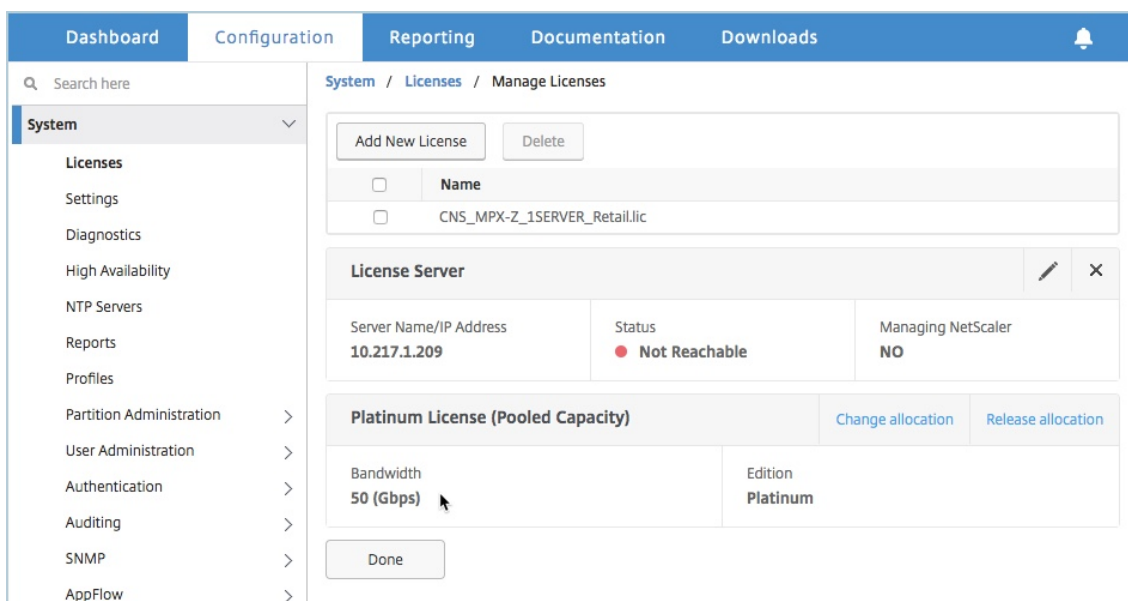
- a) Dans le champ **Nom du serveur/Adresse IP**, entrez les détails du serveur de licences.
  - b) Dans le champ **Port de licence**, entrez le port du serveur de licences. Valeur par défaut : 27000.
  - c) Si vous souhaitez gérer les licences de pool de votre instance via Citrix ADM, activez la case à cocher **Enregistrer auprès du serveur de licences pour la géabilité** et entrez les informations d'identification ADM.
  - d) Cliquez sur **Continuer**.
12. Dans la fenêtre Allouer des licences, procédez comme suit :
- a) Sélectionnez l'édition de licence dans la liste déroulante.



- b) Affectez la bande passante à l’appliance Citrix ADC à partir du menu **Allouer** et cliquez sur **Obtenir des licences**.



- c) Lorsque vous y êtes invité, cliquez sur **Redémarrer** pour redémarrer l’appliance.
13. Une fois que l’appliance Citrix ADC MPX redémarre, connectez-vous à l’appliance Citrix ADC MPX. Sur la page **Bienvenue**, cliquez sur **Continuer**.  
La page **Licences** répertorie toutes les fonctionnalités sous licence.
14. Accédez à **Système > Licences** et cliquez sur **Gérer les licences**.  
Sur la page **Gérer les licences**, vous pouvez afficher les détails du serveur de licences, de l’éditio



## Mettez à niveau la licence perpétuelle de la paire Citrix ADC MPX High Availability vers la capacité groupée Citrix ADC

Pour les appliances Citrix ADC MPX configurées en mode haute disponibilité, vous devez configurer Citrix ADC Pooled Capacity sur les instances Citrix ADC principale et secondaire de la paire HA. Vous devez allouer des licences de la même capacité aux instances Citrix ADC principale et secondaire de la paire HA. Par exemple, si vous souhaitez 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 afin de pouvoir allouer une capacité de 1 Gbit/s chacune aux instances Citrix ADC principale et secondaire de la paire HA.

### Important

Pour mettre à niveau l'appliance Citrix ADC MPX afin d'utiliser la licence Citrix ADC Pooled Capacity, vous devez télécharger le MPX-Z sur l'appliance.

### Conditions préalables

Assurez-vous de télécharger la licence MPX-Z sur les instances principale et secondaire de la paire HA.

### Pour télécharger la licence MPX-Z sur les instances Citrix ADC MPX dans la paire HA :

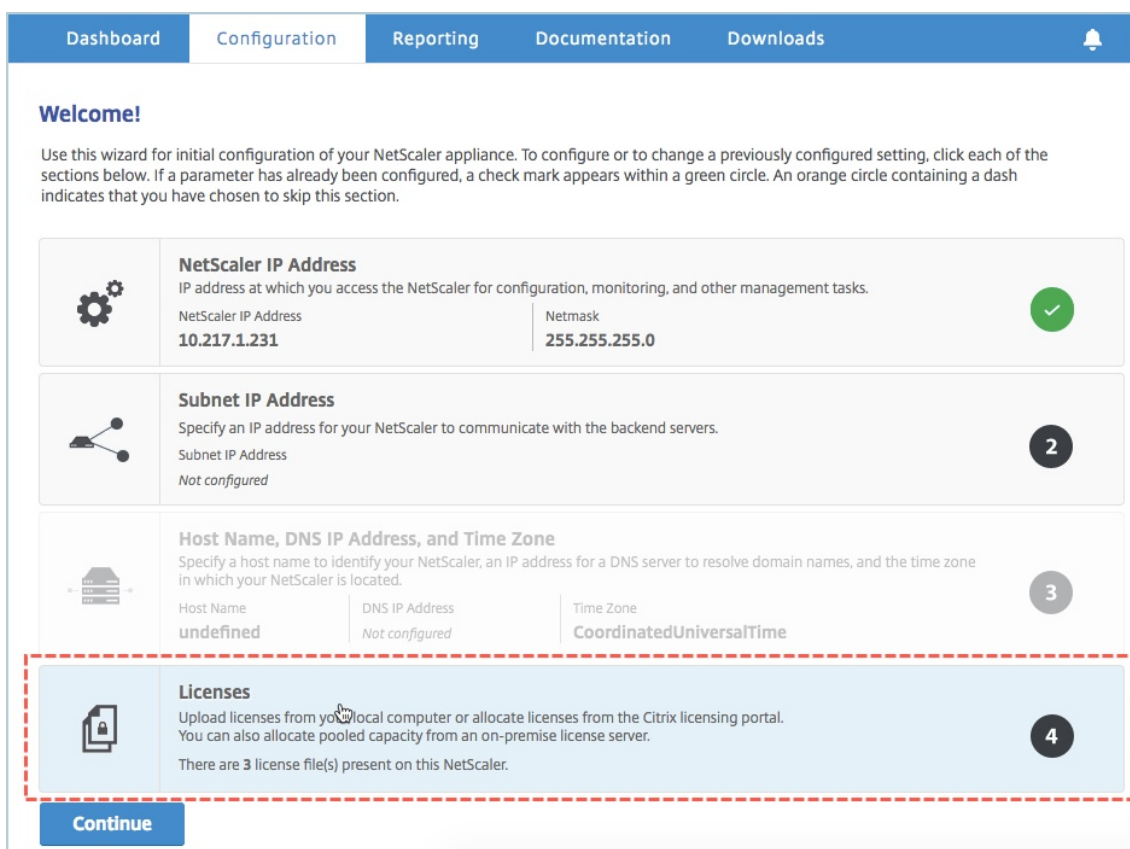
1. Dans un navigateur Web, saisissez l'adresse IP de l'appliance, telle que <http://192.168.100.1>.
2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification de l'administrateur.
3. Sur la page **Bienvenue**, cliquez sur **Continuer**.



4. Téléchargez la licence à capacité nulle (licence MPX-Z). Sous l'onglet **Configuration**, accédez à **Système > Licences**.
5. Dans le volet d'informations, cliquez sur **Gérer les licences**, cliquez sur **Ajouter une nouvelle licence**.
6. Dans la page **Licences**, sélectionnez **Charger des fichiers de licence** et cliquez sur **Parcourir** pour sélectionner la licence de capacité nulle de votre machine locale.  
Une fois la licence téléchargée, vous êtes invité à redémarrer l'appliance.
7. Cliquez sur **Redémarrer** pour redémarrer l'appliance.
8. Sur la page **Confirmer**, cliquez sur **Oui**.

**Pour mettre à niveau une configuration HA existante vers la capacité groupée Citrix ADC :**

1. Connectez-vous à l'instance secondaire Citrix ADC MPX. Dans un navigateur Web, tapez l'adresse IP de l'appliance Citrix ADC, par exemple <http://192.168.100.1>.
2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification de l'administrateur.
3. Sur la page d'**accueil**, cliquez sur la section **Licences**.

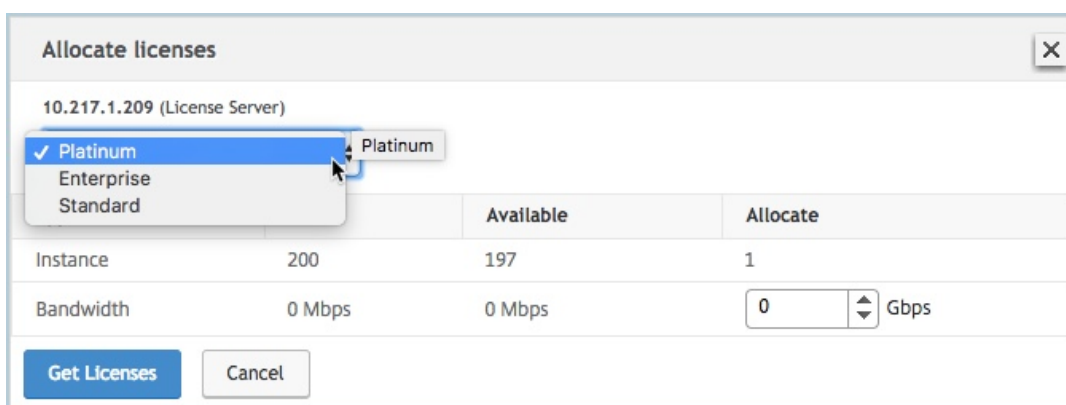


4. Dans la section **Serveur de licences**, procédez comme suit :

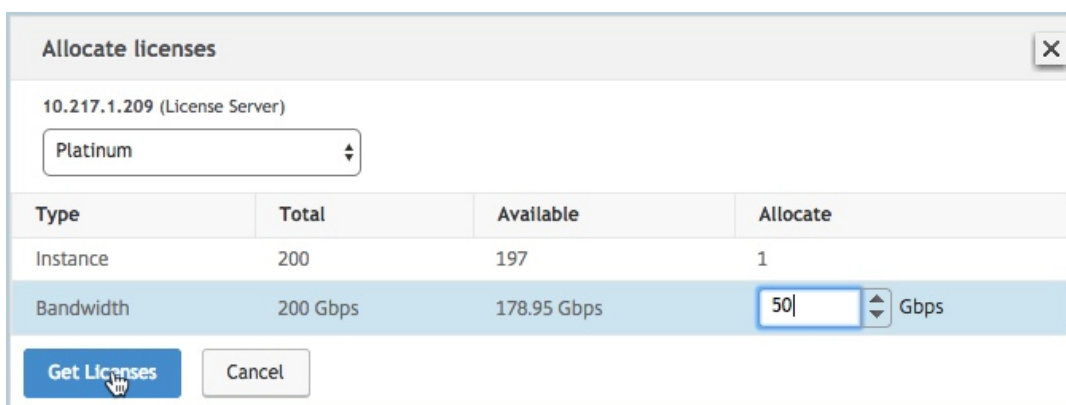
The screenshot shows the NetScaler Configuration page with the following elements:

- Navigation tabs: Dashboard, Configuration (selected), Reporting, Documentation, Downloads.
- Buttons: Add New License, Delete.
- Table with columns: Name. One entry is visible: CNS\_MPX-Z\_1SERVER\_Retail.lic.
- Section: License Server.
- Form fields:
  - Server Name/IP Address\*: 10.217.1.209
  - License Port\*: 27000
  - Register with Licensing Server for manageability
  - User Name\*: nsroot
  - Password\*: [masked]
- Buttons: Continue, Cancel.

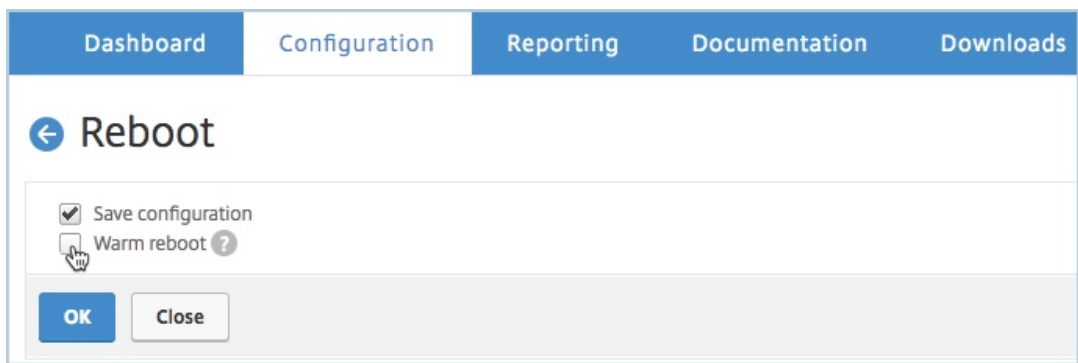
- a) Dans le champ **Nom du serveur/Adresse IP**, entrez les détails du serveur de licences.
  - b) Dans le champ **Port de licence**, entrez le port du serveur de licences. Valeur par défaut : 27000.
  - c) Si vous souhaitez gérer les licences de pool de votre instance via Citrix ADM, activez la case à cocher **Enregistrer auprès du serveur de licences pour la géabilité** et entrez les informations d'identification ADM.
  - d) Cliquez sur **Continuer**.
5. Dans la fenêtre **Allouer des licences**, procédez comme suit :
- a) Sélectionnez l'édition de licence dans la liste déroulante.



- b) Affectez la bande passante à l’appliance Citrix ADC à partir du menu **Allouer** et cliquez sur **Obtenir des licences**.



- c) Lorsque vous y êtes invité, cliquez sur **Redémarrer** pour redémarrer l’appliance.  
Après le redémarrage de l’appliance Citrix ADC MPX secondaire, il devient l’appliance Citrix ADC MPX principale dans la paire HA.
6. Connectez-vous à l’appliance Citrix ADC MPX principale existante et redémarrez l’appliance. Procédez comme suit :
- Dans un navigateur Web, tapez l’adresse IP de l’appliance Citrix ADC, par exemple <http://192.168.100.1>.
  - Dans les champs **Nom d’utilisateur** et **Mot de passe**, tapez les informations d’identification de l’administrateur.
  - Sur la page **Bienvenue**, cliquez sur **Continuer**.
  - Dans l’onglet **Configuration**, cliquez sur **Système**.
  - Sur la page **Système**, cliquez sur **Redémarrer**.
  - Sur la page **Redémarrage**, sélectionnez **Redémarrage à chaud** et cliquez sur **OK**.



Après le redémarrage de l'apppliance Citrix ADC MPX principale, il devient l'apppliance Citrix ADC MPX secondaire dans la paire HA. Si nécessaire, vous pouvez modifier l'instance principale et secondaire de la paire HA à votre configuration de paire HA d'origine à l'aide de la commande suivante sur n'importe quelle instance de la paire HA :

```
1 > force ha failover
2 <!--NeedCopy-->
```

## Mettre à niveau une licence perpétuelle dans un SDX Citrix ADC vers une capacité groupée Citrix ADC

February 1, 2024

Une appliance Citrix ADC SDX avec licence perpétuelle peut être mise à niveau vers une licence Citrix ADC Pooled Capacity. La mise à niveau vers la licence Citrix ADC Pooled Capacity vous permet d'attribuer des licences du pool de licences aux appliances Citrix ADC à la demande. Vous pouvez également configurer la licence Citrix ADC Pooled Capacity pour les instances Citrix ADC configurées en mode haute disponibilité.

### Important

Pour mettre à niveau l'apppliance SDX vers la licence Citrix ADC Pooled Capacity, vous devez télécharger la licence SDX-Z sur l'apppliance.

### Pour mettre à niveau la capacité mise en commun Citrix ADC :

1. Dans un navigateur Web, saisissez l'adresse IP de l'apppliance SDX ADC, par exemple <http://192.168.100.1>.
2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, tapez les informations d'identification de l'administrateur.
3. Sur la page **Bienvenue**, cliquez sur **Continuer**.

4. Téléchargez la licence à capacité nulle. Sous l'onglet Configuration, accédez à **Système > Licences**.
5. Accédez à **Système > Licences**.
6. Sur la page **Licences**, cliquez sur **Gérer les licences**, puis sur **Ajouter une nouvelle licence**.
7. 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. Puis, cliquez sur **Terminer**.

Une fois la licence à capacité zéro appliquée correctement, la section **Licences groupées** apparaît sur la page **Licences**.

8. 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.
- b) Dans le champ **Numéro de port**, entrez le port du serveur de licences. Valeur par défaut : 27000.
- c) Si vous souhaitez gérer les licences de pool de votre instance via Citrix ADM, activez la case à cocher **Enregistrer auprès de Citrix ADM** et entrez les informations d'identification ADM.
- d) Cliquez sur **Obtenir licences**.

9. Dans la fenêtre **Allouer les licences**, spécifiez les instances et la bande passante requises, puis cliquez sur **Allouer**.

TYPE	TOTAL	AVAILABLE	ALLOCATE
Instances	35	35	2
Premium Bandwidth	0 (Gbps)	0 (Gbps)	0
Advanced Bandwidth	500 (Gbps)	500 (Gbps)	80
Standard Bandwidth	0 (Gbps)	0 (Gbps)	0

Sur la page **Gérer les licences**, vous pouvez afficher les détails du serveur de licences, de l'éditio de licence et des instances allouées et de la bande passante à partir du pool.

Instance	Premium Bandwidth (Gbps)	Advanced Bandwidth (Gbps)	Standard Bandwidth (Gbps)
2 Total   0 Used	0 Total   0 Used	80 Total   0 Used	0 Total   0 Used

## Capacité mise en commun Citrix ADC sur les instances Citrix ADC en mode cluster

February 1, 2024

Vous pouvez configurer la capacité mise en commun Citrix ADC sur les instances Citrix ADC configurées en tant que cluster. Les conditions préalables à la configuration de la capacité groupée sur les instances Citrix ADC en mode cluster sont les suivantes :

- Les instances doivent être exécutées individuellement en mode de licence à capacité groupée pour former le cluster.
- Toutes les instances doivent être exécutées avec la même bande passante.

- Toutes les instances doivent extraire la capacité mise en commun à partir du même ADM (Citrix Application Delivery Management).
- Les nouvelles instances ne peuvent pas être ajoutées à un cluster Citrix ADC existant, sauf si leur capacité et les configurations Citrix ADM sont identiques à celles des instances existantes du cluster.

Toute extraction de capacité depuis le cluster Citrix ADC attribuera la même capacité à tous les nœuds du cluster et à la sortie Bande passante = bande passante fournie \* nombre de nœuds.

Par exemple, si vous extrayez 50 Mbit/s de bande passante du cluster Citrix ADC et que le cluster comprend 12 instances, chaque instance reçoit automatiquement 50 Mbit/s ; et 600 Mbit/s sont retirés du pool.

#### Remarque

Si une ou plusieurs instances du cluster ne répondent plus, le cluster continue de fonctionner avec la capacité des instances restantes.

**Pour allouer la capacité groupée Citrix ADC aux instances Citrix ADC en mode cluster, procédez comme suit :**

1. Dans un navigateur Web, saisissez l'adresse IP de l'adresse **IP du cluster** (CLIP) (par exemple, <http://192.168.100.1>).
2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Dans l'onglet **Configuration**, accédez à **Système > Licences > Gérer les licences**, cliquez sur **Ajouter une nouvelle licence** et sélectionnez **Utiliser les licences groupées**.
4. Entrez le nom ou l'adresse du serveur de licences dans le champ **Nom du serveur/Adresse IP**.
5. Si vous souhaitez gérer les licences de pool de votre instance via Citrix ADM, activez la case à cocher **Enregistrer auprès de Citrix ADM pour la gérabilité** et entrez les informations d'identification ADM.
6. Sélectionnez l'édition de la licence et la bande passante requise, puis cliquez sur **Obtenir des licences**.

**Allocate licenses** ✕

10.102.29.55 (License Server)

Platinum ▼

Pool	Total	Available	Allocate
Instance	200	198	1
Bandwidth	500 Gbps	490 Gbps	<input style="width: 50px;" type="text" value="50"/> <span style="font-size: 1.2em;">↕</span> Mbps

7. Vous pouvez modifier ou libérer l'allocation de licence en sélectionnant **Modifier l'allocation** ou **Libérer l'allocation**.

System / Licenses / Manage Licenses

License Server ✎ ✕

Server Name/IP Address 10.102.29.55	Status ● Reachable	Managing NetScaler YES
--	-----------------------	---------------------------

Platinum License (Pooled License) Change allocation Release allocation

Instance 1	Bandwidth 90 (Mbps)
---------------	------------------------

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.



**Allocate licenses**
✕

10.102.29.55 (License Server)

Platinum ▼

Pool	Total	Available	Allocate
Instance	200	197	1
Bandwidth	500 Gbps	489.9 Gbps	<input style="width: 50px;" type="text" value="0"/> <input style="width: 20px;" type="button" value="▼"/> <span style="margin-left: 5px;">Mbps</span>

Get Licenses
Cancel

9. Vous pouvez allouer de la bande passante ou des instances à l'instance Citrix ADC à partir de la liste déroulante **Allouer**. Cliquez ensuite sur **Obtenir des licences**.
10. Vous pouvez choisir l'édition de licence et la bande passante requise dans les listes déroulantes de la fenêtre contextuelle.

**Remarque**

Un redémarrage n'est pas nécessaire si vous modifiez l'allocation de bande passante, mais un redémarrage à chaud est requis si vous modifiez l'édition de la licence.

## Contrôle de l'intégrité

February 1, 2024

Le serveur de licences surveille en permanence l'intégrité de l'instance à capacité groupée Citrix ADC. Les instances communiquent par le biais de messages périodiques au serveur de licences. Si quelques messages consécutifs ne sont pas reçus, le serveur de licences signale que la connectivité a été perdue.

Vous pouvez créer des notifications personnalisées pour compléter les alarmes par défaut.

### Période de grâce

Lorsqu'une instance à capacité groupée Citrix ADC est dans un état sain et que le serveur de licences cesse de répondre, l'instance continue de fonctionner avec la capacité actuelle pendant 30 jours. Si la connectivité au serveur de licences n'est pas restaurée après 30 jours, l'instance perd sa capacité et arrête le traitement du trafic.

## Notifications et alarmes

Les notifications peuvent être activées à partir de Citrix Application Delivery Management (ADM) pour toute action effectuée sur l'instance. Outre les paramètres de notification personnalisés, certaines alarmes sont configurées par défaut. Par exemple : pour configurer une alarme pour réapprovisionner un pool qui a épuisé un certain pourcentage de sa capacité, accédez à **Infrastructure > Licence > Paramètres > Paramètres de notification** et cliquez sur le bouton Modifier.

### Notification Settings

What would you like to be notified about?

Notify me on license usage  
 To replenish a pool that has reached  % of its capacity

How would you like to be notified?

Email  
 Add Test

SMS (Text Message)  
 Add

Slack  
 PagerDuty  
 ServiceNow

Expiry of licenses

How many days before the license expires do you want to be notified?

Save
Close

## Comportements attendus lorsque des problèmes surviennent

February 1, 2024

Voici les comportements attendus des serveurs de licences et des instances Citrix ADC lorsqu'ils éprouvent les problèmes décrits :

### Le serveur de licences cesse de répondre

#### Avertissement

Le serveur de licences ne répond pas. Citrix ADC continuera de fonctionner avec la capacité actuelle pendant 30 jours. Après 30 jours, si la connectivité au serveur de licences n'est pas restaurée, l'instance Citrix ADC perd sa capacité actuelle et arrête le traitement du trafic.

Si le serveur de licences cesse de répondre, l'instance Citrix ADC entre dans la période de grâce jusqu'à ce que la connectivité soit restaurée.

### L'instance à capacité groupée Citrix ADC activée cesse de répondre

Si l'instance à capacité groupée Citrix ADC cesse de répondre et que le serveur de licences est dans un état sain, le serveur de licences vérifie toutes les licences de l'instance Citrix ADC après 10 minutes. Lorsque l'instance redémarre, elle envoie une demande pour extraire toutes les licences du serveur de licences.

### Le serveur de licences et l'instance à capacité groupée Citrix ADC cessent de répondre

Si le serveur de licences et l'instance à capacité groupée Citrix ADC redémarrent et rétablissent la connexion, le serveur de licences consigne-toutes ses licences après 10 minutes, et les instances à capacité groupée Citrix ADC activées extraient automatiquement les licences une fois le redémarrage terminé.

### L'instance à capacité groupée Citrix ADC s'arrête gracieusement

Lors d'un arrêt gracieux, vous pouvez choisir de vérifier les licences dans ou de conserver les licences qui ont été allouées avant l'arrêt gracieux. Si vous choisissez d'archiver les licences, l'instance à capacité groupée Citrix ADC est sans licence après le 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 l'extraction échoue en raison de l'absence de capacité disponible dans le pool, Citrix ADC vérifie l'inventaire des licences de pool Citrix Application Delivery Management (ADM) et vérifie toute capacité disponible. Une alarme SNMP est déclenchée pour notifier cette condition à l'utilisateur si Citrix ADC n'est pas en cours d'exécution avec la pleine capacité selon la configuration. Si aucune capacité n'est disponible dans le pool de bande passante, l'instance activée par la capacité de pool deviendra sans licence.

## Le réseau perd la connectivité

### Message d'erreur (syslog)

Le serveur de licences ne répond pas.

Si le serveur de licences et les instances à capacité groupée Citrix ADC sont dans des états sains mais que la connectivité réseau est perdue, les instances continuent à fonctionner avec leur capacité actuelle pendant 30 jours. Après 30 jours, si la connectivité au serveur de licences n'est pas restaurée, les instances perdent leur capacité et arrêtent le traitement du trafic, et le serveur de licences contrôle toutes ses licences. Une fois que le serveur de licences rétablit la connectivité avec les instances Citrix ADC, les instances retirent à nouveau les licences.

## Configurer les contrôles d'expiration pour les licences de capacité du pool

February 1, 2024

Vous pouvez désormais configurer le seuil d'expiration des licences pour les licences à capacité groupée Citrix ADC. En définissant des seuils, Citrix Application Delivery Management (ADM) envoie des notifications par e-mail ou SMS lorsqu'une licence doit expirer. Une interruption SNMP et une notification sont également envoyées lorsque la licence a expiré sur Citrix ADM.

Un événement est généré lorsqu'une notification d'expiration de licence est envoyée et cet événement peut être consulté sur Citrix ADM.

### Pour configurer les contrôles d'expiration de licence :

1. Accédez à **Réseaux > Licences**.
2. Dans la page **Paramètres de licence**, sous la section **Informations d'expiration de licence**, vous trouverez les détails des licences qui vont expirer :

- **Fonctionnalité** : Type de licence qui va expirer.
  - **Nombre** : nombre de serveurs virtuels ou d'instances qui seront affectés.
  - **Jours jusqu'à l'expiration** : Nombre de jours avant l'expiration de la licence.
3. Dans la section **Paramètres de notification**, cliquez sur l'icône **Modifier** et spécifiez le seuil d'alerte. Vous pouvez définir un pourcentage de capacité de licences groupées à utiliser pour notifier les administrateurs.
  4. Choisissez le type de notification que vous souhaitez envoyer en cochant la case appropriée. Les types de notification sont les suivants :
    - a) **Profil de messagerie** : Spécifiez un serveur de messagerie et les détails du profil. Un e-mail est déclenché lorsque vos licences sont sur le point d'expirer.
    - b) **Profil SMS** : Spécifiez un serveur de service de messages courts (SMS) et les détails du profil. Un message SMS est déclenché lorsque vos licences sont sur le point d'expirer.
  5. Ensuite, indiquez quand vous souhaitez envoyer la notification en termes de nombre de jours avant l'expiration de la licence.
  6. Cliquez sur **Enregistrer**.

#### Remarque

Lorsque vous ajoutez de nouvelles licences au pool, les instances Citrix ADC utilisent les nouvelles licences à l'expiration de leurs licences existantes.

## Licence d'enregistrement et de départ Citrix ADC VPX

February 1, 2024

Vous pouvez allouer des licences VPX aux instances Citrix ADC VPX à la demande à partir de Citrix Application Delivery Management (ADM). Les licences sont stockées et gérées par Citrix ADM, qui dispose d'une structure de licences qui permet un approvisionnement en licences évolutif et automatisé. Une instance Citrix ADC VPX peut récupérer la licence auprès de Citrix ADM lorsqu'une instance Citrix ADC VPX est provisionnée, ou récupérer sa licence auprès de Citrix ADM lorsqu'une instance est supprimée ou détruite.

### Conditions préalables

Assurez-vous que les conditions préalables suivantes sont remplies :

- Vous utilisez une image Citrix ADC VPX exécutant la version 12.0 du logiciel.  
Par exemple : NSVPX-ESX-12.0-xx.xx\_NC.zip
- Vous avez installé Citrix ADM exécutant la version 12.0.  
Par exemple : MAS-ESX-12.0-xx.xx.zip

#### Remarque

Pour gérer les licences VPX existantes par Citrix ADM, vous devez réhéberger les licences vers Citrix ADM.

## Installation de licences dans Citrix ADM

#### Remarque

Avant d'installer les licences, redémarrez l'appliance virtuelle Citrix ADM si vous avez modifié l'édition du logiciel ou la bande passante.

### Pour installer des fichiers de licence sur Citrix ADM :

1. Dans un navigateur Web, tapez l'adresse IP du Citrix ADM (par exemple, <http://192.168.100.1>).
2. Dans Nom d'utilisateur et Mot de passe, entrez les informations d'identification de l'administrateur.
3. Accédez à **Réseaux > Licences**.
4. Dans la section **Fichiers de licence**, sélectionnez l'une des options suivantes :
  - **Télécharger des fichiers de licences à partir d'un ordinateur local** : si un fichier de licence est déjà présent sur votre ordinateur local, vous pouvez le télécharger sur Citrix ADM. Pour ajouter des fichiers de licence, cliquez **sur** Parcourir et sélectionnez le fichier de licence (.lic) que vous souhaitez ajouter. Cliquez ensuite sur **Terminer**.
  - **Utiliser le code d'accès à la licence** : Citrix envoie par e-mail le code d'accès à la licence (LAC) pour les licences que vous achetez. Pour ajouter des fichiers de licence, entrez le LAC dans la zone de texte, puis cliquez sur **Obtenir des licences**.

#### Remarque

Assurez-vous d'être connecté à Internet avant d'utiliser le code BAC pour installer les licences.

À tout moment, vous pouvez ajouter d'autres licences à Citrix ADM à partir des paramètres de licence.

## Vérification

Vous pouvez afficher les licences disponibles et allouées dans l'interface graphique Citrix ADM.

### Pour afficher les licences :

1. Dans un navigateur Web, tapez l'adresse IP de Citrix ADM (par exemple, <http://192.168.100.1>).
2. Dans **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Sous l'onglet Configuration, accédez à **Réseaux > Licences > Licences VPX**.

## VPX Licenses

Name	IP Address	Allocation Status	Running
--	10.102.29.99	● Optimum	

4. Vous pouvez afficher les licences allouées dans le tableau sous la section Licences disponibles.

## Allocation de licences VPX à une instance Citrix ADC VPX à l'aide de l'interface graphique Citrix ADC

1. Dans un navigateur Web, tapez l'adresse IP de l'instance Citrix ADC (par exemple, <http://192.168.100.1>).
2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Dans l'onglet Configuration, accédez à **Système > Licences > Gérer les licences**, cliquez sur **Ajouter une nouvelle licence** et sélectionnez **Utiliser les licences à distance**.
4. Entrez les détails du serveur de licences dans le **champ** Nom du serveur/**Adresse IP**.

- Si vous souhaitez gérer les licences VPX de votre instance via Citrix ADM, cochez la case **Enregistrer auprès de Citrix ADM** et entrez les informations d'identification Citrix ADM.

System / Licenses / Manage Licenses

### Licenses

If a license is already present on your local computer, you can upload it to this NetScaler appliance. Alternatively, you can use this appliance's serial number, or the license access code emailed by Citrix, to allocate licenses from the Citrix licensing portal.

To use pooled licenses, select Use pooled licensing and check out licenses from a license server.

Upload license files  
 Use License Access Code  
 Use remote licensing

Remote Licensing mode  
 CICO Licensing

Server Name/IP Address\*  
 10.102.29.97

License Port\*  
 27000

Register with NetScaler MAS  
 Username\*  
 nsroot  
 Password\*  
 \*\*\*\*\*

To manually Download licenses from Citrix licensing portal please visit <http://www.mycitrix.com> and use the Host ID: 005056a82f6e

- Sélectionnez l'édition de licence avec la bande passante requise, cliquez sur **Obtenir des licences**.

Allocate licenses			
10.102.29.97 (License Server)			
	License	Available	Total
<input checked="" type="checkbox"/>	VE8000	2	2
<input type="checkbox"/>	VS1000	1	1
<input type="checkbox"/>	VE200	1	1
<input type="checkbox"/>	VS25	1	1

- Cliquez sur **Redémarrer**, votre instance Citrix ADC VPX redémarrera.
- Vous pouvez modifier ou libérer l'allocation de licence en accédant à **Système > Licences > Gérer les licences**, puis en sélectionnant **Modifier l'allocation** ou **Release allocation**.



System / Licenses / Manage Licenses

License Server		
Server Name/IP Address 10.102.29.97	Status ● Reachable	Managing NetScaler NO
Capacity		<a href="#">Change allocation</a> <a href="#">Release allocation</a>
License VS3000	Bandwidth 3000	
<input type="button" value="Done"/>		

- 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**.

**Allocate licenses** ✕

10.102.29.97 (License Server)

	License	Available	Total
<input checked="" type="radio"/>	VE8000	1	1
<input type="radio"/>	VS8000	1	1

### Allocation de licences VPX à une instance Citrix ADC VPX à l'aide de l'interface de ligne de commande Citrix ADC CLI

- Dans un client SSH, entrez l'adresse IP de l'instance Citrix ADC et ouvrez une session à l'aide des informations d'identification de l'administrateur.
- Pour ajouter un serveur de licences, entrez la commande suivante :

```

1 add ns licenseserver (<licenseServerIP> | <serverName>) [-port <
  port number >]
2 <!--NeedCopy-->

```

```

> add ns licenseserver 10.102.29.97 -port 27000
Done

```

- Pour afficher les licences disponibles sur le serveur de licences, entrez la commande suivante :

```

1 sh licenseserverpool
2 <!--NeedCopy-->

```

```

> sh licenseserverpool
Instance Total           : 0
Instance Available      : 0
Standard Bandwidth Total : 0 Mbps
Standard Bandwidth Availabe : 0 Mbps
Enterprise Bandwidth Total : 0 Mbps
Enterprise Bandwidth Available : 0 Mbps
Platinum Bandwidth Total : 0 Mbps
Platinum Bandwidth Available : 0 Mbps
VPX25S Total            : 1
VPX25S Available        : 1
VPX200E Total           : 1
VPX200E Available       : 1
VPX1000S Total          : 1
VPX1000S Available      : 1
VPX8000E Total          : 2
VPX8000E Available      : 1
Done

```

4. Pour attribuer une licence à l’appliance Citrix ADC VPX, entrez la commande suivante :

```

1 set capacity -platform V[S/E/P][Bandwidth]
2 <!--NeedCopy-->

```

```

> set capacity -platform VE8000
Warning: The configuration changes will not take effect until the system is rebooted

```

### Allocation de licences VPX à une instance Citrix ADC VPX à l’aide de l’API

Dans un navigateur Web ou un client API, ouvrez une session sur l’instance Citrix ADC VPX à l’aide des informations d’identification de l’administrateur.

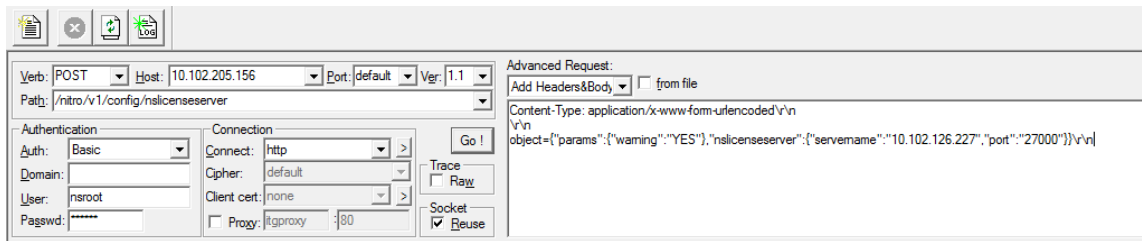
#### Pour ajouter un serveur de licences :

1. Définissez le type de demande sur **Valider**.
2. Définissez le chemin vers /nitro/v1/config/nslicensingserver.
3. Définissez la charge utile comme suit :

```

1 content-type: application/x-www-form-urlencoded\r\n
2 \r\n
3 object= {
4   "params" ;{
5     "warning" : "yes" }
6   , "nslicensing server" ;{
7     "servername" : " <Citrix ADM IP> " , " port " : " 27000 " }
8   }
9   \r\n
10 <!--NeedCopy-->

```



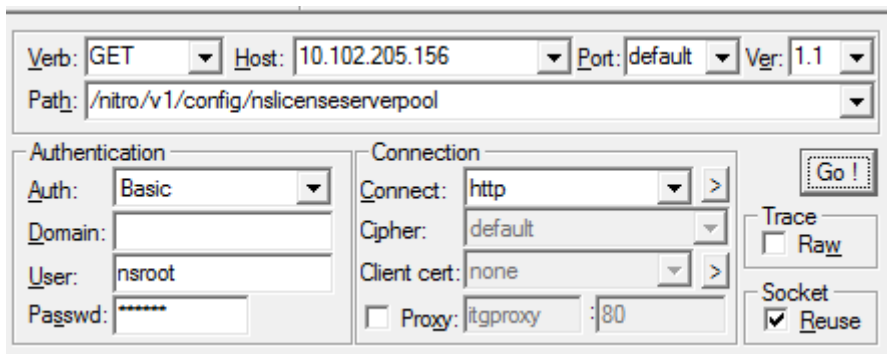
Citrix ADM répond à la demande. L'exemple de réponse suivant montre un succès.

```

i RESPONSE: *****\n
h HTTP/1.1 201 Created\r\n
h Date: Fri, 06 Jan 2017 19:03:21 GMT\r\n
h Server: Apache\r\n
h Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
h Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
h Pragma: no-cache\r\n
h Content-Length: 57\r\n
h Content-Type: application/json; charset=utf-8\r\n
h \r\n
d { "errorcode": 0, "message": "Done", "severity": "NONE" }
← finished.
    
```

**Pour afficher les licences disponibles sur le serveur de licences :**

1. Définissez le type de demande sur **Get**.
2. Définissez le chemin d'accès à /nitro/v1/config/nslicenseserverpool



Citrix ADM répond à la demande. L'exemple de réponse suivant montre le succès et la liste des licences disponibles sur le serveur de licences.

```

1 RESPONSE: *****\n
2 HTTP/1.1 200 OK\r\n
3 Date: Fri, 06 Jan 2017 19:18:54 GMT\r\n
4 Server: Apache\r\n
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
7 Pragma: no-cache\r\n
8 Content-Length: 1874\r\n
9 Content-Type: application/json; charset=utf-8\r\n
10 \r\n
11 { "errorCode": 0, "message": "Done", "severity": "NONE", "nslicenserverpool": { "instancetotal": 0, "instanceavailable": 0, "standardbandwidthtotal":
12 0, "standardbandwidthavailable": 0, "enterprisebandwidthtotal": 0, "enterprisebandwidthavailable": 0, "platinumbandwidthtotal": 0, "platinumbandwidthav
13 ailable": 0, "cpxinstancetotal": 0, "cpxinstanceavailable": 0, "vpx1stotal": 0, "vpx1savailable": 0, "vpx1ptotal": 0, "vpx1pavailable": 0, "vpx5total"
14 : 0, "vpx5savailable": 0, "vpx5ptotal": 0, "vpx5pavailable": 0, "vpx10total": 0, "vpx10savailable": 0, "vpx10etotal": 0, "vpx10eavailable": 0, "vpx10p
15 total": 0, "vpx10pavailable": 0, "vpx25total": 0, "vpx25savailable": 0, "vpx25etotal": 0, "vpx25eavailable": 0, "vpx25ptotal": 0, "vpx25pavailable": 0
16 , "vpx50total": 0, "vpx50savailable": 0, "vpx50etotal": 0, "vpx50eavailable": 0, "vpx50ptotal": 0, "vpx50pavailable": 0, "vpx100total": 0, "vpx100sav
17 ailable": 0, "vpx100etotal": 0, "vpx100eavailable": 0, "vpx100ptotal": 0, "vpx100pavailable": 0, "vpx200total": 0, "vpx200savailable": 0, "vpx200etota
18 l": 0, "vpx200eavailable": 0, "vpx200ptotal": 0, "vpx200pavailable": 0, "vpx500total": 0, "vpx500savailable": 0, "vpx500eto
19 tal": 0, "vpx500eavailable": 0, "vpx500ptotal": 0, "vpx500pavailable": 0, "vpx1000total": 0, "vpx1000savailable": 0, "vpx1000etotal": 0, "vpx1000eavail
20 able": 0, "vpx1000ptotal": 0, "vpx1000pavailable": 0, "vpx2000total": 0, "vpx2000pavailable": 0, "vpx3000total": 0, "vpx3000savailable": 0, "vpx3000e
21 total": 0, "vpx3000eavailable": 0, "vpx3000ptotal": 0, "vpx3000pavailable": 0, "vpx4000total": 0, "vpx4000pavailable": 0, "vpx5000total": 0, "vpx5000
22 savailable": 0, "vpx5000etotal": 0, "vpx5000eavailable": 0, "vpx5000ptotal": 0, "vpx5000pavailable": 0, "vpx8000total": 1, "vpx8000savailable": 1, "vp
23 x8000etotal": 2, "vpx8000eavailable": 1, "vpx8000ptotal": 1, "vpx8000pavailable": 1 } }
24 finished.

```

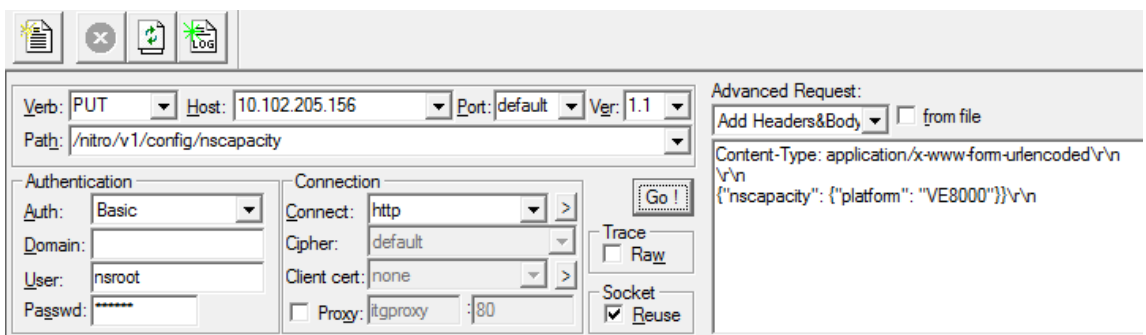
### Pour attribuer une licence à l’appliance Citrix ADC VPX :

1. Définissez le type de demande sur **Valider**.
2. Définissez le chemin vers /nitro/v1/config/nscapacity.
3. Définissez la charge utile comme suit :

```

1 content-type: application/x-www-form-urlencoded\r\n
2 \r\n
3 {
4   "nscapacity":{
5     "platform" : "VE8000" }
6 }
7 \r\n
8 <!--NeedCopy-->

```



Citrix ADM répond à la demande. L’exemple de réponse suivant montre un succès.

```
1 RESPONSE: *****\n
2 HTTP/1.1 200 OK\r\n
3 Date: Fri, 06 Jan 2017 19:16:21 GMT\r\n
4 Server: Apache\r\n
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
7 Pragma: no-cache\r\n
8 Content-Length: 57\r\n
9 Content-Type: application/json; charset=utf-8\r\n
10 \r\n
11 { "errorCode": 0, "message": "Done", "severity": "NONE" }
12 finished.
```

## Configurer les vérifications d'expiration pour les licences d'archivage/de récupération Citrix ADC VPX

Vous pouvez désormais configurer le seuil d'expiration de licence pour les licences Citrix ADC VPX. En définissant des seuils, Citrix ADM envoie des notifications par e-mail ou SMS lorsqu'une licence doit expirer. Une interruption SNMP et une notification sont également envoyées lorsque la licence a expiré sur Citrix ADM.

Un événement est généré lorsqu'une notification d'expiration de licence est envoyée et cet événement peut être consulté sur Citrix ADM.

### Pour configurer les contrôles d'expiration de licence :

1. Accédez à **Réseaux > Licences**.
2. Dans la page **Paramètres de licence**, sous la section **Informations d'expiration de licence**, vous trouverez les détails des licences qui vont expirer :
  - **Fonctionnalité** : Type de licence qui va expirer.
  - **Nombre** : nombre de serveurs virtuels ou d'instances qui seront affectés.
  - **Jours jusqu'à l'expiration** : Nombre de jours avant l'expiration de la licence.
3. Dans la section **Paramètres de notification**, cliquez sur l'icône **Modifier** et spécifiez le seuil d'alerte. Vous pouvez définir un pourcentage de capacité de licences groupées à utiliser pour notifier les administrateurs.
4. Choisissez le type de notification que vous souhaitez envoyer en cochant la case appropriée. Les types de notification sont les suivants :
  - a) **Profil de messagerie** : Spécifiez un serveur de messagerie et les détails du profil. Un e-mail est déclenché lorsque vos licences sont sur le point d'expirer.

- b) **Profil SMS** : Spécifiez un serveur de service de messages courts (SMS) et les détails du profil. Un message SMS est déclenché lorsque vos licences sont sur le point d’expirer.
5. Ensuite, indiquez quand vous souhaitez envoyer la notification en termes de nombre de jours avant l’expiration de la licence.
6. Cliquez sur **Enregistrer**.

## Licences de processeur virtuel Citrix ADC

February 1, 2024

Les administrateurs de centres de données tels que vous optent pour de nouvelles technologies qui simplifient les fonctions réseau tout en réduisant les coûts et en améliorant l’évolutivité. La nouvelle architecture de centre de données doit inclure au minimum les fonctionnalités suivantes :

- Réseau défini par logiciel (SDN)
- Virtualisation des fonctions réseau (NFV)
- Virtualisation de réseau (NV)
- Micro-services

Un tel mouvement nécessite également que les exigences logicielles soient dynamiques, flexibles et agiles pour répondre aux besoins de l’entreprise en constante évolution. Les licences devraient également être gérées par un outil de gestion centralisé offrant une visibilité complète de l’utilisation.

## Licences de processeur virtuel pour Citrix ADC VPX

Auparavant, les licences Citrix ADC VPX étaient attribuées en fonction de la consommation de bande passante par les instances. Un Citrix ADC VPX est limité à l’utilisation d’une bande passante spécifique et d’autres mesures de performance en fonction de l’édition de licence à laquelle il est lié. Pour augmenter la bande passante disponible, vous devez passer à une édition de licence qui fournit davantage de bande passante. Dans certains scénarios, la bande passante requise peut être moindre, mais elle est plus importante pour d’autres performances L7, telles que le protocole SSL, le TPS, le débit de compression, etc. La mise à niveau de la licence Citrix ADC VPX peut ne pas convenir dans de tels cas. Mais vous devrez peut-être encore acheter une licence avec une large bande passante pour débloquer les ressources système requises pour un traitement intense en CPU. Citrix ADM prend désormais en charge l’allocation de licences à l’instance Citrix ADC en fonction des exigences du processeur virtuel.

Dans la fonctionnalité de licence basée sur l’utilisation du processeur virtuel, la licence spécifie le nombre de processeurs auxquels un Citrix ADC VPX particulier a droit. Ainsi, le Citrix ADC VPX peut

retirer des licences uniquement pour le nombre de processeurs virtuels qui s'exécutent sur lui à partir du serveur de licences. Citrix ADC VPX récupère les licences en fonction du nombre de CPU s'exécutant dans le système. Citrix ADC VPX ne prend pas en compte les processeurs inactifs lors de l'extraction des licences.

Similaire à la capacité de licence mise en commun et aux fonctionnalités de licence CICO, le serveur de licences Citrix ADM gère un ensemble distinct de licences CPU virtuelles. Ici aussi, les trois éditions gérées pour les licences de processeurs virtuels sont standard, Enterprise et Platinum. 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. Vous devez redémarrer Citrix ADC VPX après avoir vérifié les licences.

**Pour configurer le serveur de licences dans Citrix ADC VPX à l'aide de l'interface graphique :**

1. Dans Citrix ADC VPX, accédez à **Système > Licences** et cliquez sur **Gérer les licences**.
2. Sur la page **Licence**, cliquez sur **Ajouter une nouvelle licence**.
3. Sur la page **Licences**, sélectionnez l'option **Utiliser les licences à distance**.
4. Sélectionnez les **licences CPU** dans la liste des **modes de licence à distance**.
5. Entrez l'adresse IP du serveur de licences et le numéro de port.
6. Cliquez sur **Continuer**.

Upload license files  
 Use License Access Code  
 Use remote licensing

Remote Licensing Mode

CPU Licensing ▾

Server Name/IP Address\*

10.217.220.60

License Port\*

27000

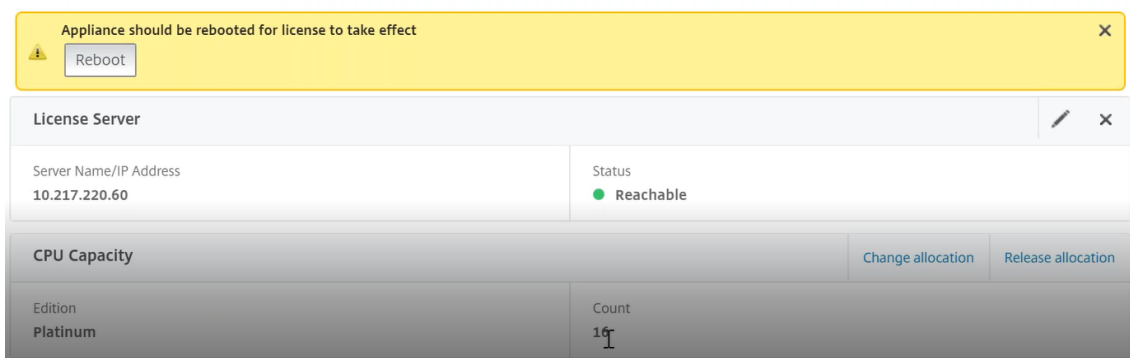
Register with NetScaler MAS

**Remarque**

Vous devez toujours enregistrer l'instance Citrix ADC VPX auprès de Citrix ADM. Si ce n'est déjà fait, activez **Enregistrer auprès de Citrix ADM** et saisissez les informations d'identi-

figuration de connexion Citrix ADM.

7. Dans la fenêtre **Allouer des licences**, sélectionnez le type de licence. La fenêtre affiche le total et les processeurs virtuels disponibles, ainsi que les processeurs qui peuvent être alloués. Cliquez sur **Obtenir licences**.
8. Cliquez sur **Redémarrer** sur la page suivante pour demander les licences.



### Remarque

Vous pouvez également libérer la licence actuelle et vérifier à partir d'une autre édition. Par exemple, vous exécutez déjà une licence d'édition Standard sur votre instance. Vous pouvez libérer cette licence, puis passer à l'édition Enterprise.

## Configuration du serveur de licences dans la licence Citrix ADC VPX à l'aide de l'interface de ligne de commande CLI

Dans la console Citrix ADC VPX, tapez les commandes suivantes pour les deux tâches suivantes :

1. Pour ajouter le serveur de licences au Citrix ADC VPX :

```
1 add licenseserver <IP address of the license server>
2 <!--NeedCopy-->
```

2. Pour demander les licences :

```
1 set capacity -vcpu - edition platinum
2 <!--NeedCopy-->
```

Lorsque vous y êtes invité, redémarrez l'instance en tapant la commande suivante :

```
1 reboot -w
2 <!--NeedCopy-->
```

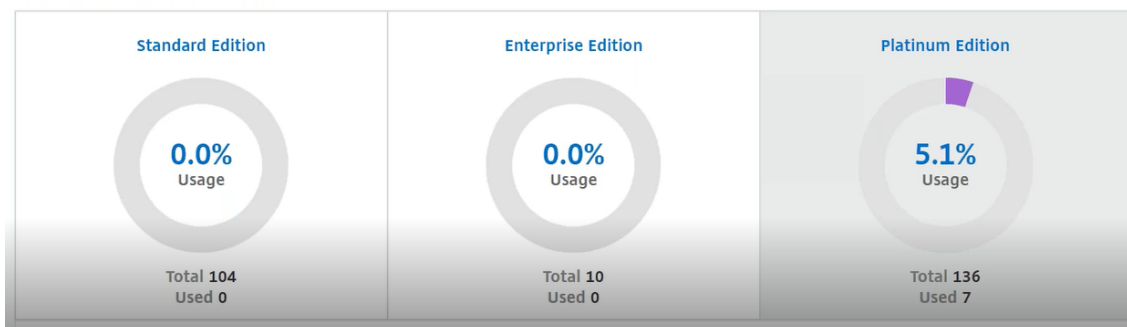
## Gestion des licences de processeur virtuel sur Citrix ADM

1. Dans Citrix ADM, accédez à **Réseaux > Licences > Licences de processeur virtuel**.



2. La page affiche les licences allouées pour chaque type d'édition de licence.
3. Cliquez sur le numéro figurant dans chaque beignet pour afficher les instances Citrix ADC qui utilisent cette licence.

### Virtual CPU Licenses



## Licence de processeur virtuel pour Citrix ADC CPX

Lors du provisionnement de l'instance Citrix ADC CPX, vous pouvez configurer l'instance Citrix ADC CPX pour extraire les licences du serveur de licences en fonction de l'utilisation du processeur sur l'instance.

Citrix ADC CPX s'appuie sur le serveur de licences, exécuté sur Citrix ADM, pour gérer les licences. Citrix ADC CPX extrait les licences du serveur de licences lors de son démarrage. Les licences sont réarchivées sur le serveur de licences lorsque le Citrix ADC CPX s'arrête.

Vous pouvez télécharger Citrix ADC CPX depuis le Docker App Store. Sur l'hôte Docker, pour télécharger Citrix ADC CPX, exécutez la commande suivante :

```
1 docker pull store/citrix/netscalercpx:<version>
2 <!--NeedCopy-->
```

Il existe trois types de licences disponibles pour les licences CPX :

1. Licences d'abonnement au processeur virtuel prises en charge pour CPX et VPX
2. Licences de capacité groupée
3. Licences CP1000 prenant en charge un ou plusieurs vCPU pour CPX uniquement

### Pour configurer des licences d'abonnement vCPU lors du Provisioning de l'instance CPX Citrix ADC :

Vous devez spécifier le nombre de licences vCPU utilisées par l'instance Citrix ADC CPX.

- Cette valeur est entrée en tant que variable d'environnement via Docker, Kubernetes ou Mesos/Marathon.

- La variable cible est « CPX\_CORES ». Le CPX peut prendre en charge de 1 à 7 cœurs.

Pour spécifier 2 cœurs, vous pouvez exécuter la commande docker run comme suit :

```
1 docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
  -e EULA=yes -e CPX_CORES=2
2 <!--NeedCopy-->
```

Lors du Provisioning d'une instance Citrix ADC CPX, définissez le serveur de licences Citrix ADC en tant que variable d'environnement dans la commande **docker run** comme indiqué ci-dessous :

```
1 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
2 <!--NeedCopy-->
```

Où,

- <LS\_IP\_ADDRESS> est l'adresse IP du serveur de licences Citrix ADC.
- <LS\_PORT> est le port du serveur de licences Citrix ADC. Par défaut, le port est 27000.

#### Remarque

Par défaut, l'instance CPX Citrix ADC extrait la licence du pool d'abonnements vCPU. L'instance CPX vérifie le nombre « n » de licences si l'instance est exécutée avec « n » processeurs.

#### Pour configurer les licences Citrix ADC Pooled Capacity ou CP1000 lors du Provisioning de l'instance CPX Citrix ADC :

Si vous souhaitez récupérer les licences de l'instance CPX à l'aide du pool de licences (basé sur la bande passante) ou du pool privé CPX (CP1000 ou basé sur un pool privé), vous devez fournir les variables d'environnement en conséquence.

Par exemple, les opérations suivantes peuvent être effectuées :

```
1 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
2 <!--NeedCopy-->
```

**CP1000.** Cette commande déclenche l'extraction depuis le pool CP1000 (pool privé CPX). L'instance CPX Citrix ADC extrait ensuite le nombre « n » d'instances pour le nombre « n » de cœurs spécifiés pour CPX\_CORES. Le cas d'utilisation le plus courant est de spécifier n = 1 pour une extraction d'une instance unique. Les cas d'utilisation du CPX multicœur utilisent « n » vCPU (où « n » est compris entre 1 et 7).

```
1 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
```

2 <!--NeedCopy-->

**Capacité mise en commun.** Cette commande vérifie une licence du pool d'instances et consomme 1000 Mbit/s de bande passante du pool de bande passante platine tout en permettant à CPX de s'exécuter jusqu'à 2000 Mbit/s. Dans les licences groupées, les 1000 premiers Mbps ne sont pas facturés.

#### Remarque

Spécifiez le nombre de processeurs virtuels correspondant à la bande passante cible souhaitée lors du retrait du pool de bande passante, comme indiqué dans le tableau suivant :

Nombre de cœurs (vCPU)	Bande passante maximale
1	1000 Mbit/s
2	2000 Mbits/s
3	3 500 Mbit/s
4	5000 Mbits/s
5	6500 Mbits/s
6	8000 Mbits/s
7	9300 Mbit/s

## Gérer les instances Citrix SD-WAN

February 1, 2024

Citrix ADM vous permet de surveiller, de gérer et d'afficher les analyses des appliances Citrix SD-WAN dans votre réseau. Le tableau d'interopérabilité suivant fournit des informations sur les fonctionnalités de Citrix ADM actuellement prises en charge dans chacune des éditions de la plate-forme Citrix SD-WAN.

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

Édition Plate-forme	Détection	Configuration	Surveillance	Rapports (rapports de surveillance réseau)	Gestion des événements	HDX Insight	WAN Insight
Citrix SD-WAN WANOP	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Citrix SD-WAN SE	Oui	Non	Non	Non	Non	Non	Non
Citrix SD-WAN PE	Oui	Non	Non	Non	Non	Oui	Non

### Versions Citrix SD-WAN prises en charge par Citrix ADM

Édition Plateforme	Version Citrix SD-WAN	Version de Citrix ADM
Citrix SD-WAN WANOP	Citrix CloudBridge 7.4 et versions ultérieures	Citrix ADM 11.0 et versions ultérieures
Citrix SD-WAN SE	Citrix SD-WAN 9.3.0 et versions ultérieures	Citrix ADM 12.0.53.8 et versions ultérieures
Citrix SD-WAN PE	Citrix SD-WAN 9.3.0 et versions ultérieures	Citrix ADM 12.0.53.8 et versions ultérieures

Vous pouvez ajouter une appliance WANOP Citrix SD-WAN en tant qu'instance gérée sur Citrix ADM. Pour plus d'informations, consultez [Ajouter des instances à Citrix ADM](#). Vous pouvez afficher les informations WAN, HDX, Network Reports et Event Reports pour les instances WANOP Citrix SD-WAN.

Citrix ADM permet aux appliances Citrix SD-WAN Standard Edition (SE) et Enterprise Edition (EE) de s'enregistrer en tant qu'instances gérées sur Citrix ADM.

Pour ajouter une appliance Citrix SD-WAN SE/PE/AE à Citrix ADM, configurez Citrix ADM en tant que collecteur AppFlow sur les appliances Citrix SD-WAN SE/PE/AE. L'appliance Citrix SD-WAN SE/PE/AE s'ajoute en tant qu'instance gérée sur Citrix ADM. L'appliance SD-WAN SE/PE/AE envoie ensuite les données d'analyse à Citrix ADM.

Vous pouvez définir Citrix ADM en tant que collecteur AppFlow sur chaque périphérique SE/PE/AE SD-WAN individuellement, ou utiliser Citrix SD-WAN Center pour exporter la configuration vers les appliances gérées.

Pour plus d'informations, consultez la section [Ajout d'instances Citrix SD-WAN SE/PE/AE dans Citrix ADM](#).

Pour une appliance Citrix SD-WAN PE, vous pouvez afficher des enregistrements de données HDX ou des données multi-sauts, en fonction de la configuration AppFlow. Une appliance Citrix SD-WAN SE fournit uniquement des données multi-sauts. Pour plus d'informations, consultez [Affichage des rapports et des mesures HDX Insight](#) et [Affichage des données d'analyse pour un déploiement multi-sauts](#).

Cette page fournit des liens d'accès rapide vers les rubriques que vous pouvez consulter pour configurer Citrix ADM et gérer vos appliances WANOP SD-WAN à l'aide de Citrix ADM.

## **Présentation de Citrix ADM**

[À propos de Citrix ADM](#)

[Architecture](#)

[Comment Citrix ADM découvre des instances](#)

[Comment Citrix ADM communique avec les instances gérées](#)

## **Déploiement Citrix ADM**

[Déployer Citrix ADM avec Citrix Hypervisor](#)

[Déployer Citrix ADM avec Microsoft Hyper-V](#)

[Déployez Citrix ADM avec VMware ESXi](#)

[Déployer Citrix ADM avec le serveur KVM Linux](#)

[Déployer Citrix ADM en mode haute disponibilité](#)

[Migrer de NetScaler Insight Center vers Citrix ADM](#)

[Intégrer Citrix ADM avec Director](#)

## **Gestion des instances**

[Comment ajouter des instances à Citrix ADM](#)

[Comment créer des groupes d'instances sur Citrix ADM](#)

[Comment faire pour sauvegarder et restaurer une instance à l'aide de Citrix ADM](#)

## **Gestion de la configuration**

[Comment créer des tâches de configuration à partir de commandes correctives sur Citrix ADM](#)

[Procédure de planification des tâches créées à l'aide de modèles intégrés dans Citrix ADM](#)

[Replanifier des travaux configurés à l'aide de modèles intégrés dans Citrix ADM](#)

[Comment réutiliser les tâches de configuration exécutées](#)

## **Analytics**

[WAN Insight](#)

[HDX Insight](#)

[Comment afficher les rapports réseau pour les instances WANOP Citrix SD-WAN](#)

[Comment configurer des seuils adaptatifs](#)

[Comment configurer la synthèse des bases de données pour Analytics](#)

[Comment créer des seuils et des alertes à l'aide de Citrix ADM](#)

## **Gestion des événements**

[Comment faire pour définir l'âge des événements pour Citrix ADM](#)

[Procédure de planification d'un filtre d'événement à l'aide de Citrix ADM](#)

[Comment faire pour définir des notifications par e-mail répétées pour des événements à partir de Citrix ADM](#)

[Comment faire pour supprimer des événements à l'aide de Citrix ADM](#)

[Comment afficher les rapports d'événements pour les instances WANOP Citrix SD-WAN](#)

[Comment modifier la gravité signalée des événements survenant sur les instances NetScaler](#)

[Comment afficher le résumé des événements dans Citrix ADM](#)

[Comment faire pour afficher la gravité des événements et les biais des interruptions SNMP sur le tableau de bord de l'infrastructure de Citrix ADM](#)

## **Authentification**

[Comment mettre en cascade des serveurs d'authentification externes](#)

[Comment ajouter des serveurs d'authentification RADIUS](#)

[Comment ajouter des serveurs d'authentification LDAP](#)

[Comment ajouter des serveurs d'authentification TACACS](#)

[Comment extraire un groupe de serveurs d'authentification dans Citrix ADM](#)

[Comment activer l'authentification locale de secours](#)

## **Système Citrix ADM**

[Gestion du système Citrix ADM](#)

[Procédure de mise à niveau de Citrix ADM](#)

[Comment faire pour générer un fichier de support technique pour Citrix ADM](#)

[Comment faire pour sauvegarder et restaurer votre serveur Citrix ADM dans un déploiement à serveur unique](#)

[Comment faire pour sauvegarder et restaurer une configuration Citrix ADM dans une paire HA](#)

[Comment faire pour activer l'accès Shell pour les utilisateurs non par défaut dans Citrix ADM](#)

[Comment faire pour configurer le serveur NTP sur Citrix ADM](#)

[Comment faire pour configurer les paramètres SSL pour Citrix ADM](#)

[Comment faire pour configurer l'intervalle de purge Syslog pour Citrix ADM](#)

[Comment afficher les informations d'audit de Citrix ADM](#)

[Comment faire pour configurer les paramètres de notification système de Citrix ADM](#)

[Comment surveiller l'utilisation du processeur, de la mémoire et du disque de Citrix ADM](#)

[Comment faire pour configurer un groupe de chiffrement pour Citrix ADM](#)

[Procédure de création d'interruptions SNMP, de gestionnaires et d'utilisateurs sur Citrix ADM](#)

[Comment faire pour attribuer un nom d'hôte à un serveur Citrix ADM](#)

[Comment faire pour configurer les paramètres de nettoyage du système pour Citrix ADM](#)

[Comment faire pour configurer les paramètres de sauvegarde système à l'aide de Citrix ADM](#)

[Comment faire pour configurer et afficher les alarmes système sur Citrix ADM](#)

## **Ajouter des instances Citrix SD-WAN**

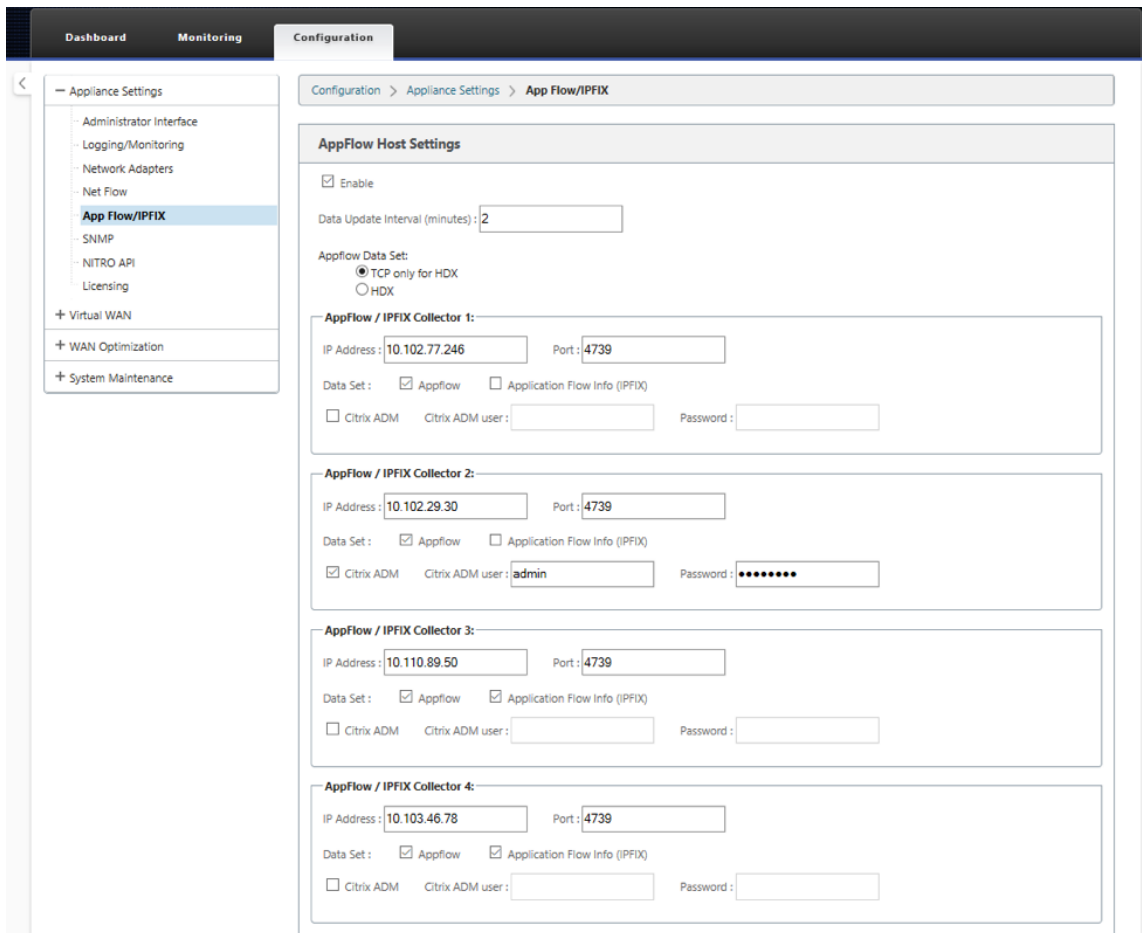
February 1, 2024

Configurez Citrix ADM en tant que collecteur AppFlow sur l'apppliance Citrix SD-WAN SE/PE pour ajouter ces instances dans Citrix ADM. Les appliances Citrix SD-WAN SE/PE sont enregistrées en tant qu'instances gérées sur Citrix ADM et leurs enregistrements AppFlow sont collectés. Pour une appliance Citrix SD-WAN PE, vous pouvez activer le modèle **TCP uniquement pour HDX** ou le modèle **HDX**. Le modèle **TCP uniquement pour HDX** fournit des données multi-sauts. Le modèle **HDX** fournit des données HDX, il doit être activé uniquement sur l'apppliance Data Center.

Vous pouvez configurer Citrix ADM en tant que collecteur AppFlow sur l'apppliance SE/PE/AE SD-WAN, ou vous pouvez configurer Citrix ADM en tant que collecteur AppFlow à l'aide du Centre SD-WAN et exporter la configuration vers les appliances gérées par celui-ci.

**Pour configurer Citrix ADM en tant que collecteur AppFlow sur une appliance Citrix SD-WAN SE/PE/AE :**

1. Dans l'interface Web SD-WAN SE/PE/AE, accédez à **Configuration > Appflow/IPfix**
2. Choisissez **Activer**.



3. Dans le champ **Intervalle de mise à jour des données**, spécifiez l'intervalle de temps, en minutes, auquel les rapports AppFlow sont exportés vers le collecteur AppFlow.



#### Remarque

Si Citrix ADM est le collecteur AppFlow, l'intervalle de mise à jour des données doit être de 1 minute.

#### 4. Procédez comme suit :

- Choisissez **HDX** pour envoyer des données d'aperçu HDX au collecteur AppFlow. Cela doit être activé sur les appliances de branche.
- Choisissez **TCP uniquement pour HDX**, pour envoyer des données multi-sauts au collecteur AppFlow.

#### Remarque

L'option de modèle **HDX** est disponible uniquement pour l'appliance Citrix SD-WAN PE, elle doit être activée sur l'appliance Data Center

5. Dans le champ **Adresse IP**, tapez l'adresse IP du système de collecte AppFlow externe (serveur Citrix ADM).
6. Dans le champ **Port**, tapez le numéro de port sur lequel le système collecteur AppFlow externe écoute. La valeur par défaut est 4739.
7. Activez la case à cocher **Citrix ADM** pour spécifier que Citrix ADM est le collecteur AppFlow.

#### Remarque

- Citrix ADM ne prend actuellement pas en charge la collection IPFIX.
- Vous pouvez ajouter jusqu'à quatre collecteurs AppFlow. Citrix ADM ou tout collecteur AppFlow prenant en charge le protocole IPFIX.

8. Entrez les informations d'identification du serveur Citrix ADM
9. Cliquez sur **Appliquer les paramètres**.

Les appliances Citrix SD-WAN SE/PE sont découvertes et répertoriées sur Citrix ADM. Les appliances Citrix SD-WAN SE/PE envoient les données d'analyse à Citrix ADM. Pour plus d'informations, consultez [AppFlow et IPFIX](#).

#### **Pour configurer Citrix ADM en tant que collecteur AppFlow à l'aide de Citrix SD-WAN Center :**

1. Dans l'interface utilisateur de gestion du Citrix SD-WAN Center, accédez à **Configuration** > Paramètres de **l'appliance**.
2. Accédez à la section **AppFlow/IPFIX** et choisissez **Inclure dans le fichier**.

### 3. Sélectionnez **Activer IPFIX/AppFlow Collection**.

4. Dans le champ **Intervalle de mise à jour des données**, spécifiez l'intervalle de temps, en minutes, auquel les rapports AppFlow sont exportés vers le collecteur AppFlow.

#### Remarque

Si Citrix ADM est le collecteur AppFlow, l'intervalle de mise à jour des données doit être de 1 minute.

5. Procédez comme suit :

- Choisissez **HDX** pour envoyer des données d'aperçu HDX au collecteur AppFlow.
- Choisissez **TCP pour HDX**, pour envoyer des données d'informations multi-sauts au collecteur AppFlow. Cela doit être activé sur les appliances de branche.

#### Remarque

L'option de modèle **HDX** est disponible uniquement pour l'appliance Citrix SD-WAN PE, elle doit être activée sur l'appliance Data Center.

6. Dans le champ **IPFIX/AppFlow Collector**, tapez l'adresse IP du système de collecte AppFlow externe (serveur Citrix ADM).
7. Dans le champ **Port**, tapez le numéro de port sur lequel le système collecteur AppFlow externe écoute. La valeur par défaut est 4739.
8. Activez la case à cocher **Citrix ADM** pour spécifier que Citrix ADM est le collecteur AppFlow.
9. Entrez les informations d'identification du serveur Citrix ADM.

#### Remarque

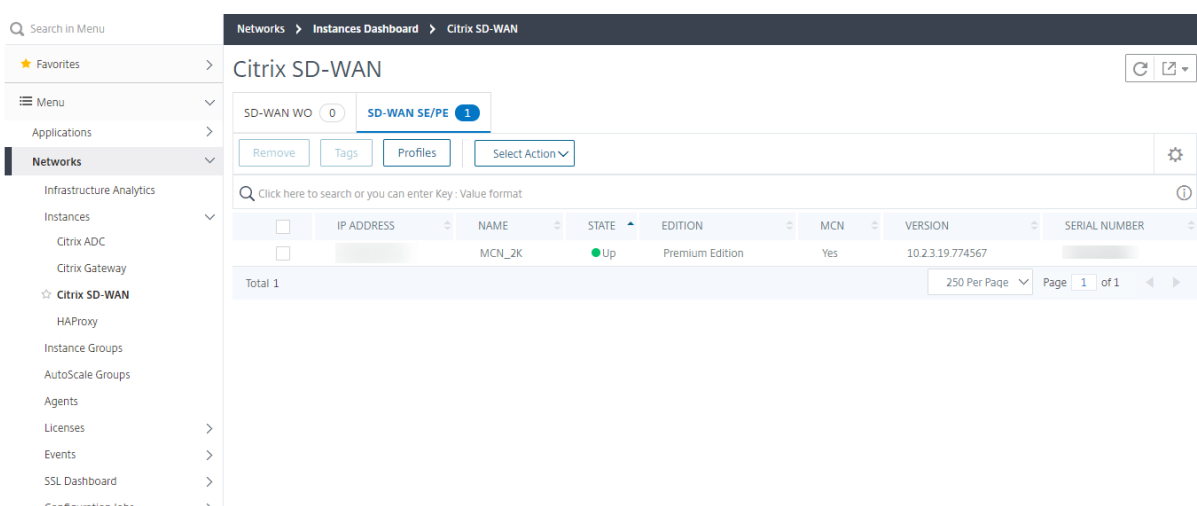
Vous pouvez ajouter jusqu'à quatre collecteurs AppFlow. Citrix ADM ou tout collecteur AppFlow prenant en charge le protocole IPFIX.

10. Enregistrez et exportez la configuration vers les appliances gérées.

Pour plus d'informations, consultez [Comment configurer et exporter les paramètres du dispositif vers des dispositifs gérés](#).

Pour plus d'informations sur la configuration de Citrix ADM en tant que collecteur AppFlow à l'aide de Citrix SD-WAN Center, [AppFlow et IPFIX](#).

Les appliances Citrix SD-WAN SE/PE sont découvertes et répertoriées par Citrix ADM. Les appliances Citrix SD-WAN SE/PE sont découvertes et répertoriées dans Citrix ADM. Pour afficher les appliances Citrix SD-WAN SE/PE découvertes, dans l'interface Web Citrix ADM, accédez à **Réseaux > Instances > Citrix SD-WAN** et sélectionnez **SD-WAN SE/PE/AE**.



Vous pouvez afficher l'adresse IP, le nom, l'état actuel, l'édition du logiciel et la version des appliances découvertes. Vous pouvez également voir si l'appliance est un nœud de Controller maître (MCN) ou non.

Vous pouvez effectuer les actions suivantes :

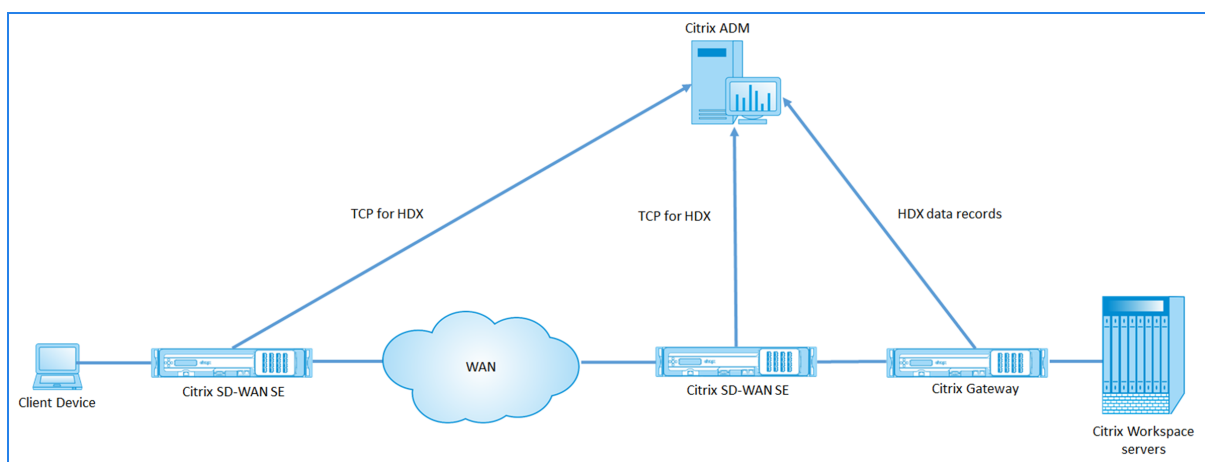
- Afficher et supprimer les profils d'instance.
- Supprimez des instances de Citrix ADM.
- Redécouvrez les instances.

Pour une appliance Citrix SD-WAN PE, vous pouvez afficher des enregistrements de données HDX ou des données multi-sauts, en fonction de la configuration AppFlow. Une appliance Citrix SD-WAN SE fournit uniquement des données multi-sauts. Pour plus d'informations, consultez [Affichage des rapports et des mesures HDX Insight](#) et [Affichage des données d'analyse Citrix SD-WAN pour un déploiement multi-sauts](#).

## Afficher les données d'analyse Citrix SD-WAN pour un déploiement multi-sauts

February 1, 2024

Un déploiement de réseau à sauts multiples comporte plusieurs appareils entre le client et le serveur, comme illustré dans la figure suivante. Dans ce type de déploiement, les appliances Citrix SD-WAN SE et Citrix Gateway sont ajoutés à Citrix ADM et AppFlow est activé.



Citrix ADM identifie l'appliance à partir de laquelle il reçoit les données, en fonction du nombre de sauts et de l'ID de chaîne de connexion. Le nombre de sauts représente le nombre d'appareils par lesquels le trafic circule du client vers le serveur. L'ID de chaîne de connexion représente les connexions de bout en bout entre le client et le serveur.

Citrix ADM utilise le nombre de sauts et l'ID de chaîne de connexion pour corréler les données des appliances et génère les rapports.

Pour que les appliances Citrix SD-WAN SE envoient les données d'analyse à Citrix ADM, vous devez configurer l'adresse IP virtuelle de Citrix Gateway comme adresse IP DPI ICA et définir le numéro de port DPI ICA sur 443.

### Pour configurer les paramètres DPI de l'ICA :

1. **\*\*Dans l'interface utilisateur de l'appliance Citrix SD-WAN SE, accédez \*\*à l'éditeur de configuration> Avancé \*\* Global > \*\*Applications \*\* Paramètres\*\***
2. Sélectionnez **Activer l'inspection approfondie des paquets > Activer l'inspection approfondie des paquets pour les applications Citrix ICA > Activer l'inspection ICA multi-flux**

## Settings

Enable Deep Packet Inspection

Enable Deep Packet Inspection for Citrix ICA Applications

Citrix ICA Deep Packet Inspection Settings

Enable Multi-Stream ICA

DPI ICA IP and Port List

DPI ICA IP-1: <input type="text" value="192.168.29.2/4"/>	DPI ICA Port-1: <input type="text" value="2599"/>
DPI ICA IP-2: <input type="text" value="192.170.29.3/5"/>	DPI ICA Port-2: <input type="text" value="2600"/>
DPI ICA IP-3: <input type="text" value="192.170.100.3/5"/>	DPI ICA Port-3: <input type="text" value="2601"/>
DPI ICA IP-4: <input type="text" value="192.160.23.3/5"/>	DPI ICA Port-4: <input type="text" value="8008"/>
DPI ICA IP-5: <input type="text"/>	DPI ICA Port-5 : <input type="text"/>

Apply

Revert

3. Dans le champ **DPI ICA IP-1**, entrez l'adresse IP virtuelle et le préfixe Citrix Gateway.
4. Dans le champ **DPI ICA Port-1**, entrez le numéro de port 443.
5. Cliquez sur **Appliquer** et exportez la configuration vers l'appliance à l'aide du processus de gestion des modifications.

Dans Citrix ADM, pour chaque session ICA active, vous pouvez afficher un diagramme de session dans HDX Insight. Les diagrammes de session fournissent des informations détaillées sur les appareils situés sur le chemin de connexion. Ils fournissent également un aperçu de la latence côté client/côté serveur entre un périphérique réseau et son prochain saut immédiat. Ces informations vous permettent d'identifier la cause première du retard et de résoudre les problèmes de performances.

Citrix SD-WAN SE n'envoie pas d'enregistrements de données HDX. Il fournit uniquement des informations TCP pour HDX. Les données HDX insights sont fournies par les périphériques HDX insights de votre réseau (par exemple, Citrix ADC ou Citrix Gateway).

L'appliance Citrix SD-WAN PE peut envoyer des données TCP pour HDX ou des données d'information HDX, en fonction de la configuration AppFlow de l'appliance. Le modèle HDX doit être activé sur l'

appliance Data Center.

**Remarque**

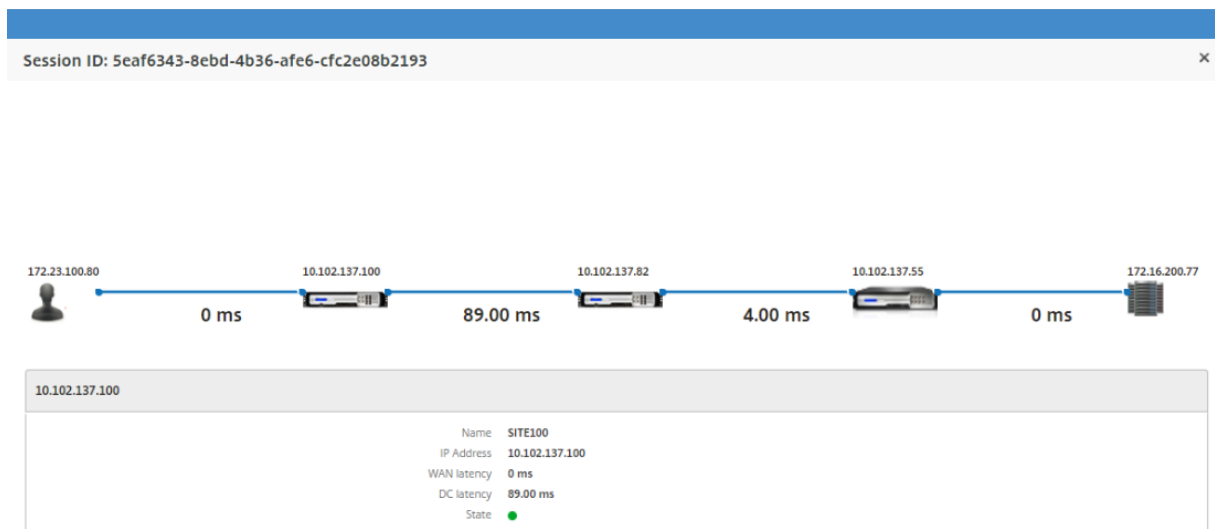
Dans un déploiement à sauts multiples, assurez-vous qu'un seul des périphériques réseau envoie des données HDX Insight. Les autres périphériques réseau peuvent envoyer du TCP pour les données HDX.

**Pour afficher les données multi-sauts, procédez comme suit :**

**Dans l'interface Web Citrix ADM, accédez à HDX Insight > Utilisateurs > Sessions en cours ou HDX > Insight > Applications > Sessions en cours et cliquez sur l'icône de diagramme.**

The screenshot shows the Citrix ADM interface. On the left is a navigation menu with categories like Video Insight, HDX Insight, Users, Applications, Desktops, Instances, Licenses, Gateway Insight, WAN Insight, Security Insight, Orchestration, System, and Downloads. The main area displays session details for 'WAN latency' with a value of 67.00 ms. Below this is a line graph titled 'WAN latency' showing latency over time from 23:47:00 to 23:48:30. The graph shows a relatively flat line around 65-70 ms. Below the graph is a table of 'Current Sessions' with columns: Diagram, Session ID, Session Type, ICA RTT, WAN latency, DC latency, Host Delay, Bandwidth per Interval, Session Bandwidth, and Tot. The first row shows a session with Session ID 'b70c\_f9ffcc', Session Type 'Application', ICA RTT '39 ms', WAN latency '45.00 ms', DC latency '0 ms', Host Delay '0 ms', Bandwidth per Interval '5.88 Kbps', and Session Bandwidth '5.88 Kbps'. A red box highlights the 'Diagram' icon in the first row of the table.

Le diagramme de topologie du réseau apparaît.



Cliquez sur n'importe quel élément du réseau pour afficher plus d'informations.

**Remarque**

Les informations affichées dépendent de l'élément de réseau sélectionné.

Les paramètres suivants apparaissent pour les appliances Citrix :

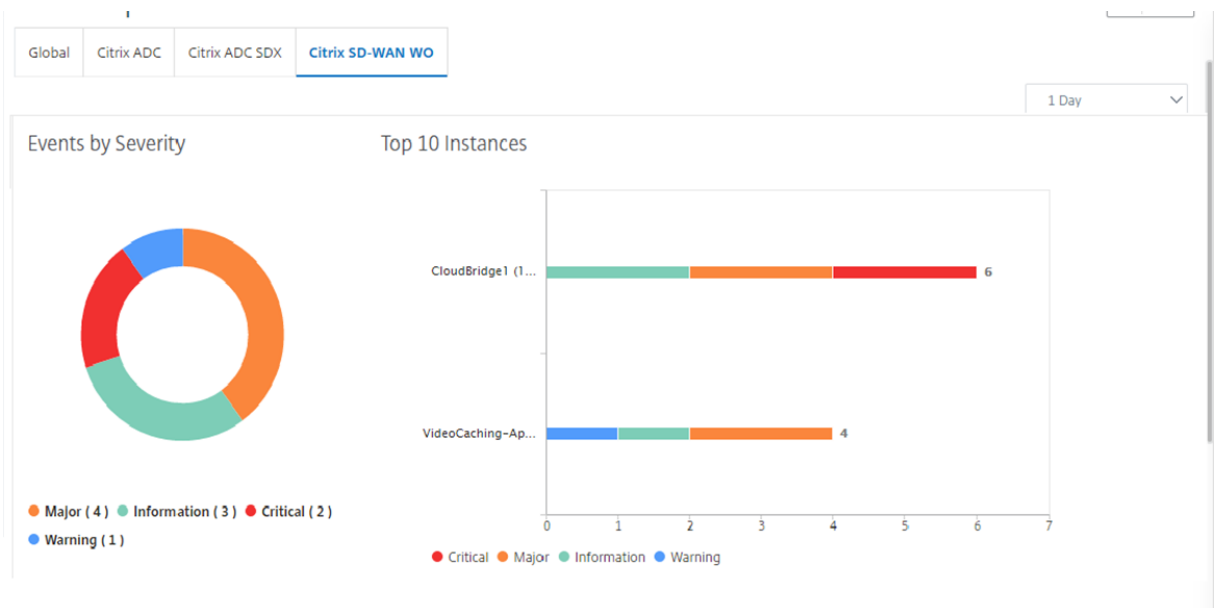
- **Nom** : nom de l'appliance Citrix.
- **Adresse IP** : adresse IP de l'appliance.
- **Latence WAN** : latence causée par le côté client du réseau. C'est-à-dire de l'appliance Citrix à l'utilisateur final.
- **Latence DC** : latence causée par le côté serveur du réseau. C'est-à-dire de l'appliance Citrix aux serveurs principaux.
- **État** : État d'accessibilité de l'appareil.

**Voir les rapports d'événements des instances de Citrix SD-WAN WANOP**

February 1, 2024

Vous pouvez afficher les événements des 10 premières instances WANOP SD-WAN sous forme de représentation graphique en accédant à **Réseaux > Événements > Rapports** et en sélectionnant **Citrix SD-WAN WO**.

Les événements sont affichés en fonction de leur gravité pour chaque instance, vous pouvez cliquer sur chaque gravité pour en savoir plus sur le nombre d'événements, le moment où ils se sont produits et la catégorie à laquelle ils appartiennent.



## Afficher les rapports réseau des instances de Citrix SD-WAN WANOP

February 1, 2024

Vous pouvez afficher les rapports liés au réseau d'optimisation WAN dans Citrix ADM, à l'aide de ces données, vous pouvez résoudre les problèmes réseau ou analyser le comportement de vos périphériques Citrix SD-WAN WANOP. Vous pouvez consulter les rapports de statistiques réseau de vos périphériques d'optimisation WAN au cours des dernières heures, une journée, une semaine ou un mois.

Vous pouvez consulter les rapports suivants :

Rapports	Description
Accélération	Utilisez ce rapport pour analyser le schéma du trafic accéléré (KBPS par classe de service) et le nombre de connexions TCP accélérées passant par l'appliance d'optimisation WAN. Cela inclut le nombre de connexions TCP passant par le périphérique d'optimisation WAN qui subissent une accélération, le nombre de connexions ouvertes et semi-fermées sélectionnées pour l'accélération et le nombre de connexions semi-ouvertes qui sont candidates pour accélération.
Passer la connexion	Utilisez ce rapport pour afficher les connexions non accélérées du périphérique d'optimisation WAN.
Classe de service	Utilisez ce rapport pour afficher les économies de bande passante envoyées et recevoir en fonction du type de classe de service défini pour le périphérique d'optimisation WAN.
Application	Utilisez ce rapport pour afficher le volume de données envoyé et reçu en bits par seconde pour les applications exécutées sur le périphérique d'optimisation WAN.
Utilisation de l'UC	Utilisez ce rapport pour afficher l'utilisation de l'UC du périphérique d'optimisation WAN sous forme de pourcentage.



Rapports	Description
Augmentation de la capacité	Utilisez ce rapport pour afficher le taux de compression d'envoi cumulé pour le périphérique d'optimisation WAN.
Réduction des données	Utilisez ce rapport pour afficher la transmission et recevoir des économies de bande passante en pourcentage. Vous pouvez également analyser la bande passante de transmission et recevoir séparément des valeurs d'économie de bande passante pour le périphérique d'optimisation WAN.
Utilisation des liens	Utilisez ce rapport pour afficher l'utilisation du lien de transmission et recevoir l'utilisation du lien pour l'optimisation du réseau étendu sous forme de pourcentage.
Utilisation du plugin	Utilisez ce rapport pour afficher le nombre de plugins connectés au périphérique d'optimisation WAN.
Perte de paquets	Utilisez ce rapport pour afficher les paquets envoyés par lien et les paquets reçus par lien pour les liens définis dans le périphérique d'optimisation WAN.
Débit	Utilisez ce rapport pour afficher le volume de liaison envoyé et le volume de liaison reçu en bits par seconde pour le périphérique d'optimisation WAN.
QoS	Utilisez ce rapport pour afficher le volume QoS envoyé et QoS Recevoir en bits par seconde pour le périphérique d'optimisation WAN.

**Pour afficher les rapports réseau WANOP Citrix SD-WAN :**

1. Dans Citrix ADM, accédez à **Réseaux > Network Reporting > Citrix SD-WAN WO**.
2. Dans la liste déroulante **Nom** du rapport, sélectionnez un rapport à afficher.
3. **Dans la liste déroulante Instances**, sélectionnez l'instance WANOP Citrix SD-WAN pour laquelle vous souhaitez afficher le rapport.
4. Dans la liste déroulante **Durée**, sélectionnez l'intervalle de temps.

5. Cliquez sur **Exécuter**.

## Sauvegarder les instances de Citrix SD-WAN WANOP

February 1, 2024

Vous pouvez sauvegarder l'état actuel d'une instance et utiliser ultérieurement les fichiers sauvegardés pour restaurer l'instance au même état. Il est recommandé de sauvegarder une instance avant de la mettre à niveau ou pour des raisons de précaution. Une sauvegarde d'un système stable vous permet de restaurer le système à un point stable au cas où il devient instable. Il existe plusieurs façons d'effectuer des sauvegardes et des restaurations sur une instance WANOP Citrix SD-WAN. Vous pouvez également sauvegarder et restaurer des instances à l'aide de l'interface graphique, de l'interface de ligne de commande ou utiliser Citrix ADM pour effectuer des sauvegardes. Citrix ADM sauvegarde l'état actuel de vos instances WANOP Citrix SD-WAN gérées à l'aide des appels NITRO, du protocole SSH (Secure Shell) et du protocole SCP (Secure Copy).

### Configuration des paramètres de sauvegarde d'instance

Avant d'effectuer une sauvegarde de l'instance WANOP Citrix SD-WAN dans Citrix ADM, vous devez configurer les paramètres de sauvegarde d'instance sur Citrix ADM.

#### Pour configurer les paramètres de sauvegarde d'instance :

1. Dans Citrix ADM, accédez à **Système > Administration système**. Dans le volet droit, sous Paramètres de **sauvegarde**, sélectionnez **Paramètres de sauvegarde d'instance**.
2. Sélectionnez **Activer les sauvegardes d'instance**. Cette option est activée par défaut.
3. Sélectionnez **Mot de passe Protect File** pour chiffrer le fichier de sauvegarde. Le chiffrement du fichier de sauvegarde garantit la sécurité des informations sensibles contenues dans le fichier de sauvegarde.
4. Dans le champ **Nombre de fichiers de sauvegarde à conserver**, spécifiez le nombre de fichiers de sauvegarde à conserver dans Citrix ADM. Vous pouvez conserver jusqu'à 50 fichiers de sauvegarde.

#### Remarque

Chaque fichier de sauvegarde nécessite une certaine exigence de stockage. Citrix vous recommande de stocker un nombre optimal de fichiers de sauvegarde sur Citrix ADM en fonction de vos besoins.

← Configure Instance Backup Settings

Enable Instance Backups

Select password protect option to encrypt the backup file. This ensures that all the sensitive information inside backup file is secure.

Password Protect file

Password\*

.....

Confirm Password\*

.....

Number of Backup Files to retain\*

5

Note: Encrypted backup can be downloaded to your local machine but contents cannot be visible. Only MAS can use backup file for restore purpose. Restoring encrypted backup will prompt for password.

5. Définissez les paramètres de planification de sauvegarde. Choisissez l’une des options suivantes :

- **Basé sur l’intervalle** : un fichier de sauvegarde est créé dans Citrix ADM après l’expiration de l’intervalle spécifié. L’intervalle de sauvegarde par défaut est de 12 heures.
- **Basé sur le temps** - Vous pouvez spécifier l’heure dans le format « heures:minutes » à laquelle la sauvegarde doit se produire. Citrix ADM permet jusqu’à quatre sauvegardes quotidiennes sur les instances.

▼ Backup Scheduling Settings

Scheduling Option

Interval Based  Time Based

Specify time for daily Backup (Maximum-limit: 4)

Add Time

00:00 ×

06:00 ×

12:00 ×

18:00 × +

**Remarque**

Ignorez la section **Paramètres Citrix ADC** ; ces paramètres ne sont pas applicables aux instances WANOP Citrix SD-WAN.

6. Sélectionnez **Activer le transfert externe** pour transférer les fichiers de sauvegarde d’instance

vers un emplacement externe. Entrez les valeurs des champs suivants :

- **Serveur** : adresse IP du serveur externe.
- **Nom d'utilisateur** : nom d'utilisateur du serveur externe
- **Mot de passe** : Mot de passe du serveur externe.
- **Port** : numéro de port utilisé pour communiquer avec le serveur externe.
- **Protocole de transfert** : Protocole à utiliser pour transférer les fichiers de sauvegarde de Citrix ADM vers le serveur externe.

Vous pouvez également supprimer le fichier de sauvegarde de Citrix ADM après l'avoir transféré sur le serveur externe.

#### External Transfer

Enable External Transfer

Server\*

192 . 10 . 10 . 1

User Name\*

davidT

Password\*

.....

Port\*

-1

Transfer Protocol

SCP  SFTP  FTP

Directory Path\*

/test/nsbackups/

Delete file from NetScaler Management and Analytics System after transfer

7. Cliquez sur **OK**.

#### Remarque

Citrix ADM envoie un piège SNMP ou une notification Syslog à lui-même en cas d'échec de sauvegarde pour l'une des instances WANOP Citrix SD-WAN sélectionnées.

## Création d'une sauvegarde d'une instance WANOP Citrix SD-WAN

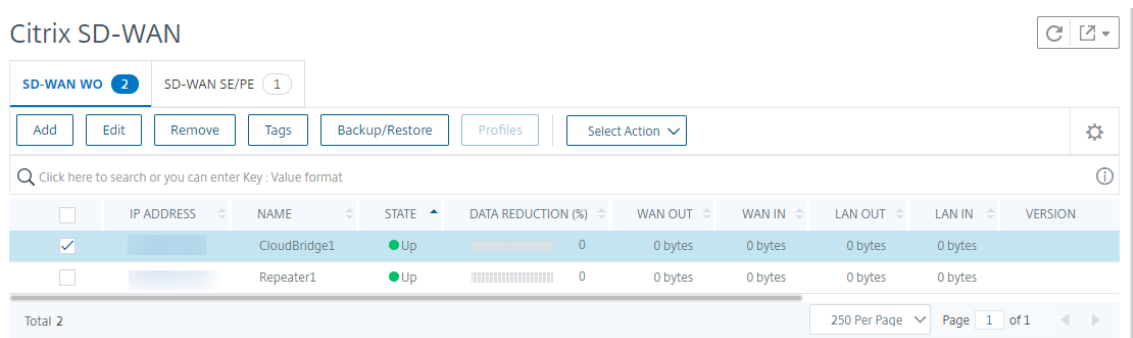
La procédure de création d'une sauvegarde pour l'instance WANOP Citrix SD-WAN s'applique à un utilisateur administrateur, à l'aide du profil nsroot par défaut.

Pour plus d'informations sur, comment un utilisateur personnalisé peut reprendre la sauvegarde d'une instance WANOP Citrix SD-WAN, reportez-vous à la section [Création d'une sauvegarde d'instance WANOP Citrix SD-WAN](#) pour les utilisateurs personnalisés de cette rubrique.

Assurez-vous qu'une instance Citrix SD-WAN WANOP est ajoutée à Citrix ADM. Pour plus d'informations, reportez-vous à la section [Ajout d'une instance à Citrix ADM](#).

### Pour créer une sauvegarde pour l'instance WANOP Citrix SD-WAN :

1. Dans Citrix ADM, accédez à **Réseaux > Instances > Citrix SD-WAN**.
2. Dans **SD-WAN WO**, sélectionnez l'instance WANOP Citrix SD-WAN à sauvegarder, puis cliquez sur **Sauvegarde/Restaurer**.



The screenshot shows the Citrix SD-WAN management interface. At the top, there are tabs for 'SD-WAN WO' (selected) and 'SD-WAN SE/PE'. Below the tabs are buttons for 'Add', 'Edit', 'Remove', 'Tags', 'Backup/Restore', 'Profiles', and 'Select Action'. A search bar is present with the text 'Click here to search or you can enter Key : Value format'. Below the search bar is a table with the following columns: IP ADDRESS, NAME, STATE, DATA REDUCTION (%), WAN OUT, WAN IN, LAN OUT, LAN IN, and VERSION. The table contains two rows: 'CloudBridge1' and 'Repeater1'. The 'CloudBridge1' row is selected, indicated by a checkmark in the first column. The 'STATE' column shows 'Up' with a green dot. The 'DATA REDUCTION (%)' column shows '0' with a progress bar. The 'WAN OUT', 'WAN IN', 'LAN OUT', and 'LAN IN' columns show '0 bytes'. The 'VERSION' column is empty. At the bottom of the table, it says 'Total 2' and '250 Per Page'.

	IP ADDRESS	NAME	STATE	DATA REDUCTION (%)	WAN OUT	WAN IN	LAN OUT	LAN IN	VERSION
<input checked="" type="checkbox"/>		CloudBridge1	Up	0	0 bytes	0 bytes	0 bytes	0 bytes	
<input type="checkbox"/>		Repeater1	Up	0	0 bytes	0 bytes	0 bytes	0 bytes	

3. Dans la page **Fichiers de sauvegarde**, cliquez sur **Sauvegarder**.
4. Chiffrez votre fichier de sauvegarde à l'aide de l'une des options suivantes :
  - Sélectionnez **Fichier protégé par mot de passe** et entrez un mot de passe pour chiffrer les fichiers de sauvegarde.
  - Sélectionnez **Utiliser le mot de passe global** pour utiliser le mot de passe global que vous avez spécifié sur la page des paramètres de sauvegarde de l'instance.
5. Cliquez sur **Créer une sauvegarde**

## Création d'une sauvegarde de l'instance WANOP Citrix SD-WAN pour les utilisateurs personnalisés

Si vous avez créé un utilisateur personnalisé avec des privilèges d'administrateur dans l'instance WANOP Citrix SD-WAN, suivez la procédure suivante pour ajouter une instance et reprendre cette instance à l'aide de Citrix ADM.

L'opération de sauvegarde par les utilisateurs personnalisés n'est pas prise en charge sur les plates-formes WANOP SD-WAN 400/800/1000WS/2000/2000WS/3000/4000/5000/4100/5100.

### Remarque

Citrix vous recommande d'utiliser le profil nsroot par défaut, lors de la création de la sauvegarde des plates-formes avancées Citrix SD-WAN dans Citrix ADM.

### Pour ajouter une instance WANOP Citrix SD-WAN et effectuer une sauvegarde pour un utilisateur personnalisé :

1. Dans Citrix ADM, accédez à **Réseaux > Instances > Citrix SD-WAN** et sélectionnez **SD WAN WO**.
2. Cliquez sur **Ajouter**.
3. Dans le champ **Adresse IP**, entrez l'adresse IP de l'instance WANOP Citrix SD-WAN.
4. Cliquez sur **Ajouter** en regard **du champ Nom du profil** pour créer un nouveau profil. La fenêtre **Créer un profil de WO Citrix SD-WAN** apparaît.

← Create Citrix SD-WAN WO Profile

Profile Name\*  
New-admin-profile

User Name\*  
nsroot

Password\*  
\*\*\*\*\*

Community\*  
\*\*\*\*\*

Protocol for Citrix SD-WAN WO communication is https.

Create Close

5. Dans le **champ Nom du profil**, entrez un nom pour le profil.
6. Dans le champ **Nom d'utilisateur**, entrez le nom d'utilisateur de l'utilisateur personnalisé que vous créez sur l'instance WANOP SD-WAN.
7. Dans le **champ Mot de passe**, entrez le mot de passe que vous avez défini pour l'utilisateur personnalisé dans l'instance WANOP SD-WAN.
8. Dans le champ **Communauté**, entrez la chaîne de communication SNMP configurée sur l'appli-  
ance WANOP SD-WAN. (par exemple : public)
9. Cliquez sur **Créer**.
10. Dans le champ **Nom du profil**, sélectionnez le profil nouvellement créé et cliquez sur **OK**.

11. Accédez à **Réseaux > Instances > Citrix SD-WAN**.
12. Dans **SD-WAN WO**, sélectionnez l'instance WANOP Citrix SD-WAN que vous venez d'ajouter, puis cliquez sur **Sauvegarde/Restaurer**.

Citrix SD-WAN ↻ ↗

SD-WAN WO 2 SD-WAN SE/PE 1

Add Edit Remove Tags Backup/Restore Profiles Select Action ▾ ⚙️

🔍 Click here to search or you can enter Key : Value format ℹ️

<input type="checkbox"/>	IP ADDRESS	NAME	STATE	DATA REDUCTION (%)	WAN OUT	WAN IN	LAN OUT	LAN IN	VERSION
<input checked="" type="checkbox"/>		CloudBridge1	● Up	0	0 bytes	0 bytes	0 bytes	0 bytes	
<input type="checkbox"/>		Repeater1	● Up	0	0 bytes	0 bytes	0 bytes	0 bytes	

Total 2 250 Per Page ▾ Page 1 of 1

13. Dans la page **Fichiers de sauvegarde**, cliquez sur **Sauvegarder**.
14. Chiffrez votre fichier de sauvegarde à l'aide de l'une des options suivantes :
  - Sélectionnez **Fichier protégé par mot de passe** et entrez un mot de passe pour chiffrer les fichiers de sauvegarde.
  - Sélectionnez **Utiliser le mot de passe global** pour utiliser le mot de passe global que vous avez spécifié sur la page des paramètres de sauvegarde de l'instance.



**Remarque**

Vous pouvez télécharger le fichier de sauvegarde chiffré sur votre ordinateur local, mais vous ne pouvez pas afficher son contenu. Seul Citrix ADM peut utiliser ces fichiers de sauvegarde à des fins de restauration. La restauration d'une sauvegarde cryptée demandera le mot de passe.

15. Cliquez sur **Créer une sauvegarde**.

**Important**

1. Pour une appliance Citrix SD-WAN WANOP VPX, Citrix ADM sauvegarde uniquement le fichier de configuration CB Broker .

a) Pour une plate-forme WANOP Citrix SD-WAN avancée, Citrix ADM sauvegarde les éléments suivants :

- Fichier de configuration du broker CB
- Fichier de configuration NTP
- DNS
- Fichier de configuration SNMPD
- Fichier de configuration Syslog
- Certificat SSL, clés et stratégies
- Fichier de base de données SVM
- Composants (au format XML)
- Ressources (au format XML)

Les fichiers sauvegardés dans les dossiers respectifs sont répertoriés dans le tableau suivant. Notez que si un nom de dossier est suivi d'un « \* », tous les fichiers de ce dossier sont sauvegardés.

Répertoire	Sous-répertoire ou fichiers
/br_broker/	CB-6bbb660A/ ws.conf
/etc/	resolv.conf
/mps/	mps_devices.xml
/mpsconfig/	ssl/*, ntp.conf, snmpd.conf, syslog.conf
/mpsdb/	mpsdb_dump.sql
/ns/	NS-6CBB660A/*

/var/

*mps/policy/, mps/ssl\_certs/  
sdx\_default\_ssl\_cert, mps/ssl\_keys/  
sdx\_default\_ssl\_key, mps/tenants/*

## Gérer les instances HaProxy

February 1, 2024

HAProxy est un équilibreur de charge open source qui peut équilibrer la charge n'importe quel service TCP ou HTTP. Pour plus d'informations sur HAProxy, reportez-vous à la section <http://www.haproxy.org/>.

Citrix Application Delivery Management (Citrix ADM) prend en charge HaProxy version 1.4.24 ou ultérieure. Lorsque vous ajoutez un hôte sur lequel vous avez provisionné les instances HAProxy à Citrix ADM, Citrix ADM détecte les instances HAProxy sur l'hôte et vous permet de les surveiller. Il vous montre les types d'informations suivants sur la configuration HaProxy sur les instances :

- Frontend —Comment les demandes doivent être transmises au back-end.
- Backend —Ensemble de serveurs qui reçoivent les demandes transférées.
- Serveurs : serveurs parmi lesquels la charge HaProxy équilibre le trafic.

Pour plus d'informations, consultez <http://www.haproxy.org/download/1.7/doc/configuration.txt>.

Citrix ADM fournit également un tableau de bord des applications HAProxy sur lequel vous pouvez surveiller les frontends en temps réel. Pour plus d'informations, consultez [Tableau de bord de l'application HAProxy](#).

## Ajouter des instances HAProxy à Citrix ADM

February 1, 2024

Dans Citrix Application Delivery Management (Citrix ADM), vous devez ajouter manuellement les détails de l'hôte sur lequel vous avez provisionné l'instance HaProxy. Après avoir ajouté ces détails, Citrix ADM découvre automatiquement les instances HaProxy provisionnées sur l'hôte et les ajoute à Citrix ADM Inventory. Il détecte également tous les frontends, backends et serveurs configurés sur les instances HAProxy, et traite les frontends comme des applications découvertes.

## Conditions préalables

Assurez-vous d'avoir :

- Déploiement d'une instance HaProxy sur un hôte dans votre déploiement. Pour plus d'informations, consultez <http://www.haproxy.org/#docs>.
- Identifié et décidé du nombre de frontends pour lesquels vous souhaitez afficher les statistiques d'application dans le tableau de bord de l'application HaProxy. Par défaut, le tableau de bord des applications HaProxy affiche les statistiques de 30 applications découvertes. Pour plus d'informations sur HAProxy App Dashboard, voir Tableau de [bord de l'application HAProxy](#) Si vous souhaitez afficher les statistiques de plus de 30 applications découvertes, vous devez acheter une licence distincte. Pour plus d'informations, consultez la section [Licences tierces](#).

### Important

Citrix ADM nécessite l'accès à l'hôte afin de découvrir les instances HaProxy qu'il comporte. Vous pouvez fournir l'accès à Citrix ADM en fournissant la paire de clés SSH de l'hôte ou en utilisant le mot de passe de l'hôte. Si vous souhaitez fournir un accès à l'aide de la paire de clés SSH, assurez-vous de générer la paire de clés privées et publiques SSH dans l'hôte et d'ajouter la clé publique aux clés autorisées sur l'hôte. En outre, le compte d'utilisateur SSH doit disposer d'autorisations de superutilisateur.

### Pour ajouter une instance HaProxy à Citrix ADM :

1. Dans un navigateur Web, saisissez l'adresse IP de **Citrix Application Delivery Management** (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 par défaut de l'administrateur sont « ns-root » et « nsroot ».
3. Accédez à **Réseaux > Instances**. Sous **Instances**, sélectionnez **HAProxy** et cliquez sur **Ajouter**.
4. Dans la boîte de dialogue **Ajouter un hôte HaProxy**, procédez comme suit :

## ← Add HAProxy Host

IP Address\*

 ?

HAProxy Profile\*

▼
 

?

Site\*

▼

Agent

 >

Tags

+

1. Dans le champ **Adresse IP**, entrez l'adresse IP de l'hôte sur lequel vous avez provisionné les instances HAProxy.
  - a) Dans le menu **Profil HaProxy**, sélectionnez un profil HaProxy existant ou créez et sélectionnez un nouveau profil HaProxy. Pour créer un profil HaProxy, cliquez sur **Ajouter**.
    - i. Dans la boîte de dialogue **Ajouter un profil HAProxy**, procédez comme suit :

### Add HAProxy Profile

Profile Name\*  
 ?

User Name\*  
 ?

Password\*  
 ?

- i. Dans le champ **Nom du profil**, entrez le nom du profil.
  - ii. Dans les champs **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'utilisateur de l'hôte.
  - iii. Cliquez sur **Créer**.
2. Dans le menu **Site**, sélectionnez un site HaProxy. Pour créer et ajouter un nouveau site au menu, cliquez sur **Ajouter**.
  3. Dans le menu **Agent**, sélectionnez un agent.
  4. Dans les champs Balises, saisissez les valeurs de manière appropriée.
  5. Cliquez sur **OK**.

Citrix ADM détecte les instances HAProxy mises en service sur l'hôte et vous pouvez afficher toutes les instances HAProxy sous l'onglet **Instances**.

#### HAProxy

HAProxy Hosts 2 **Instances 5**

View Configuration View Backup Dashboard Hard Restart Soft Restart Search ▾

<input type="checkbox"/>	Host IP Address	Configuration Path	State	Version	CPU Usage (%)	Memory Usage (%)
<input type="checkbox"/>	10.102.205.59	lb_testportal3.cfg	● Up	1.4.24	0	0.10
<input type="checkbox"/>	10.102.205.59	lb_testportal1.cfg	● Up	1.4.24	0	0.10
<input type="checkbox"/>	10.102.205.59	lb_testportal4.cfg	● Up	1.4.24	0	0.10
<input type="checkbox"/>	10.102.205.178	lb_mas.cfg	● Up	1.4.24	0	0.10
<input type="checkbox"/>	10.102.205.59	lb_testportal2.cfg	● Up	1.4.24	0	0.10

## Affichage de la configuration d'une instance HaProxy

Pour afficher la configuration d'une instance HAProxy dans Citrix ADM, accédez à **Réseaux > Instances > HAProxy** et, sous l'onglet, **Instances**, sélectionnez l'instance HAProxy et cliquez sur **Afficher la configuration**.

```
Configuration ×
global
    log /dev/log local0
    log /dev/log local1 notice
    chroot /var/lib/haproxy
    user haproxy
    group haproxy
    daemon

    stats socket /var/run/haproxy.sock mode 600 level admin

defaults
    log global
    mode http
    option httplog
    option dontlognull
    contimeout 5000
    clitimeout 50000
    srvtimeout 50000
    errorfile 400 /etc/haproxy/errors/400.http
    errorfile 403 /etc/haproxy/errors/403.http
    errorfile 408 /etc/haproxy/errors/408.http
    errorfile 500 /etc/haproxy/errors/500.http
    errorfile 502 /etc/haproxy/errors/502.http
    errorfile 503 /etc/haproxy/errors/503.http
    errorfile 504 /etc/haproxy/errors/504.http

frontend http-in_1
    bind 10.102.205.59:8061
    acl host_api hdr(host) -i 10.102.205.59
    default_backend api_backend1

frontend http-in_2
    bind 10.102.205.59:8062
    acl host_api hdr(host) -i 10.102.205.59
```

## Tableau de bord de l'application HaProxy

February 1, 2024

Le tableau de bord des applications fournit des statistiques en temps réel sur tous les frontends HAProxy surveillés par Citrix Application Delivery Management (Citrix ADM). Il répertorie les frontends en tant qu'applications discrètes et fournit des informations sur les transactions, le débit et les sessions des applications.

### Important

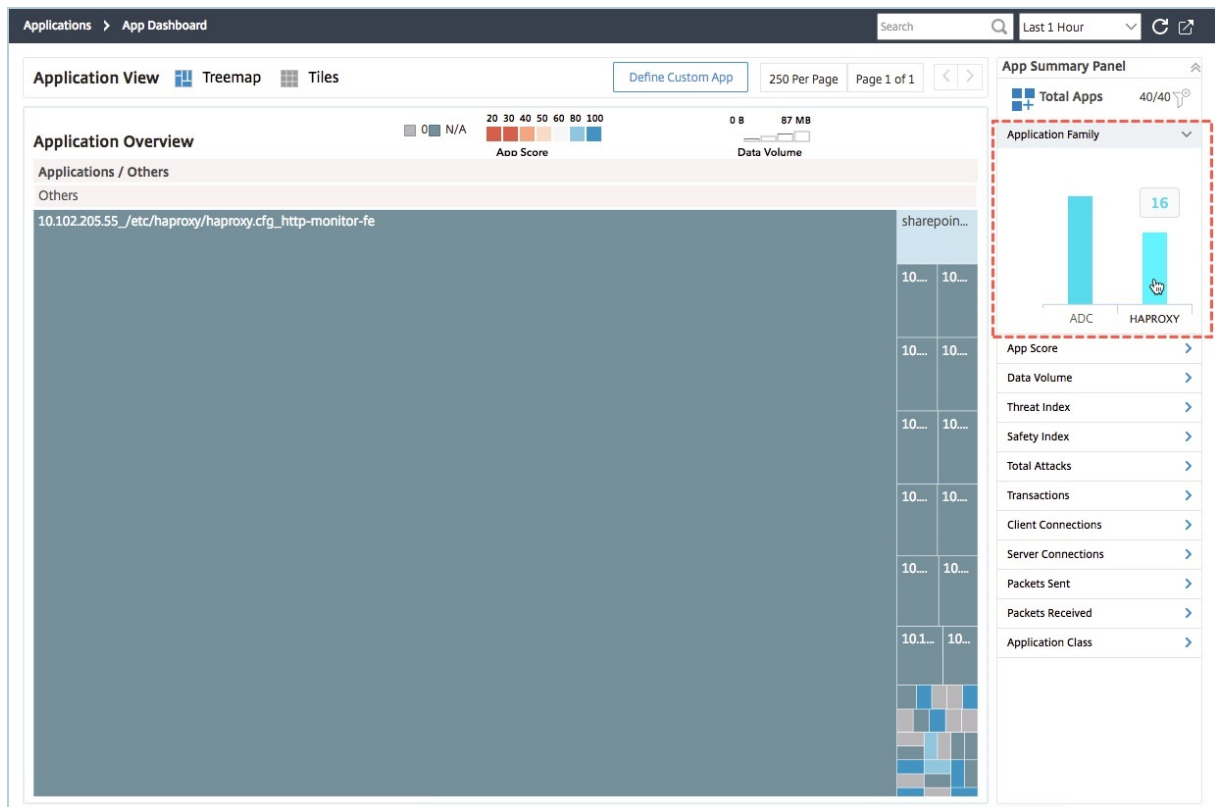
Assurez-vous d'activer les **statistiques** dans le fichier de configuration de l'instance HaProxy. Pour activer les **statistiques**, modifiez votre fichier de configuration HaProxy et, après la section

des valeurs par défaut, ajoutez une entrée similaire à celle de l'exemple suivant :

```

1 listen stats :9000 # Listen on localhost:9000
2 mode http
3 stats enable # Enable stats page
4 stats hide-version # Hide HAProxy version
5 stats realm Haproxy\ Statistics # Title text for popup window
6 stats uri /haproxy_stats # Stats URI
7 stats auth Username:Password # Authentication credentials
8 <!--NeedCopy-->
    
```

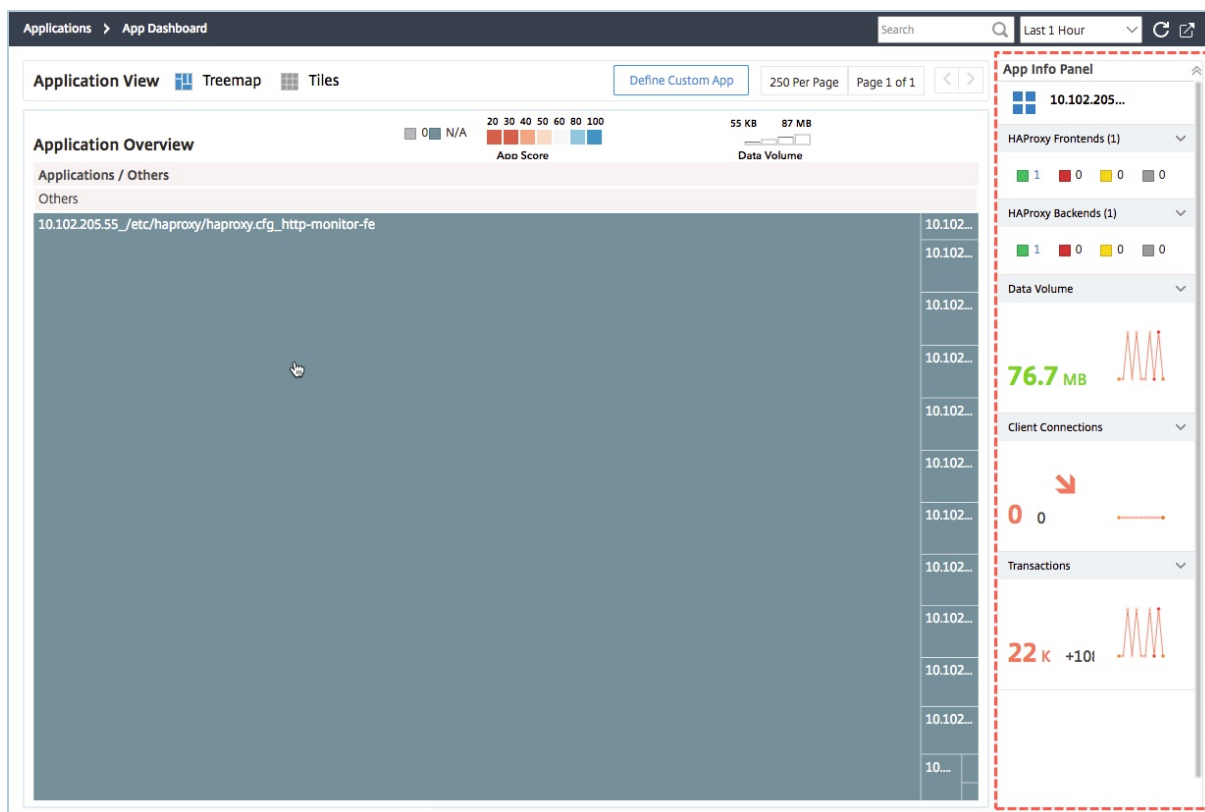
Pour accéder à l'application HAProxy sur le tableau de bord des applications dans Citrix ADM, après avoir ajouté les instances HAProxy à Citrix ADM, accédez à **Applications > Tableau de bord**. Vous pouvez filtrer le tableau de bord pour afficher uniquement l'application HAProxy. Pour filtrer le tableau de bord, sélectionnez **HAPROXY** affiché sous la section **Famille d'applications** dans le panneau Informations récapitulatives de l'application.



### Afficher les mesures clés de l'application HaProxy

Le panneau Infos sur l'application se trouve au premier niveau lorsque vous effectuez une exploration vers le bas sur une application HaProxy. Il affiche les métriques et les composants clés de l'application, ainsi que son état. Par exemple, pour toute application HaProxy sélectionnée, le panneau Infos sur l'application affiche le nombre total de frontends HaProxy, le nombre total de backends HaProxy, le

volume de données, la tendance des connexions client et les transactions. Pour afficher les mesures clés de l'application HAProxy, cliquez sur la vignette de l'application HAProxy dans le tableau de bord de l'application. Le panneau Informations sur l'application remplace ensuite le panneau Résumé de l'application .



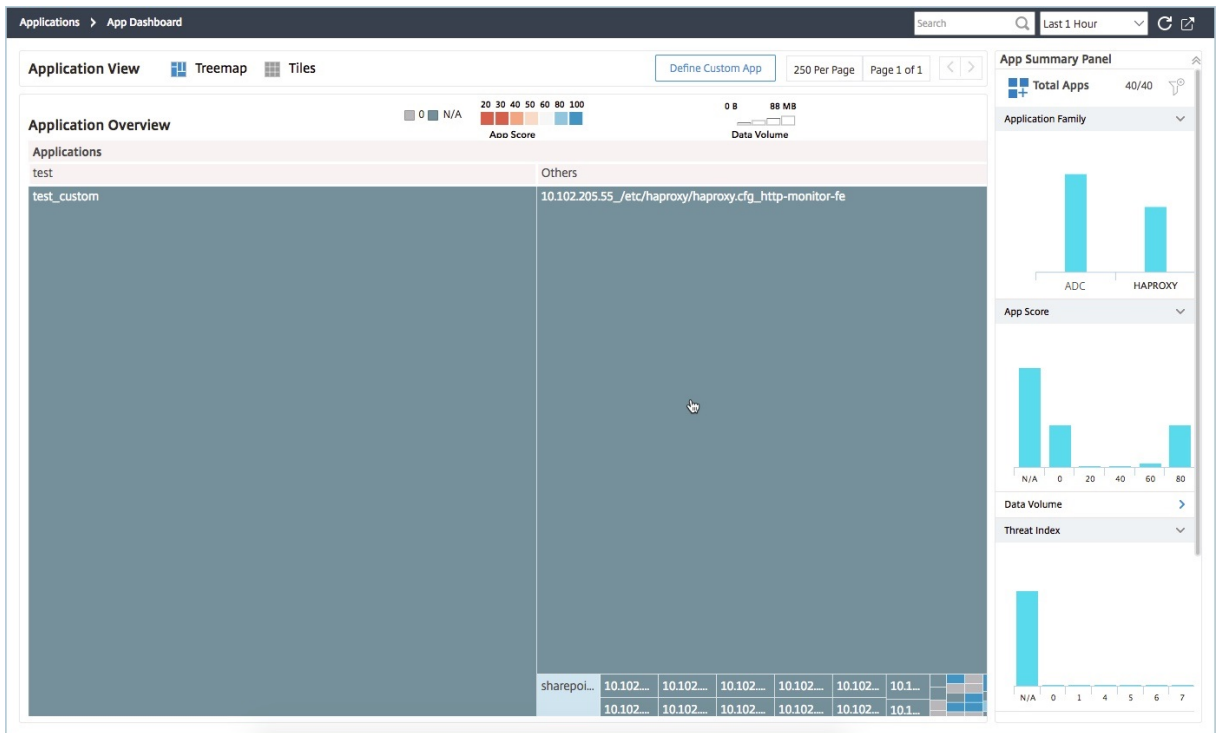
## Voir les performances en temps réel de l'application HaProxy

Citrix ADM vous permet de visualiser les performances en temps réel de vos applications HaProxy. Il fournit les détails suivants en temps réel de l'application HaProxy sélectionnée :

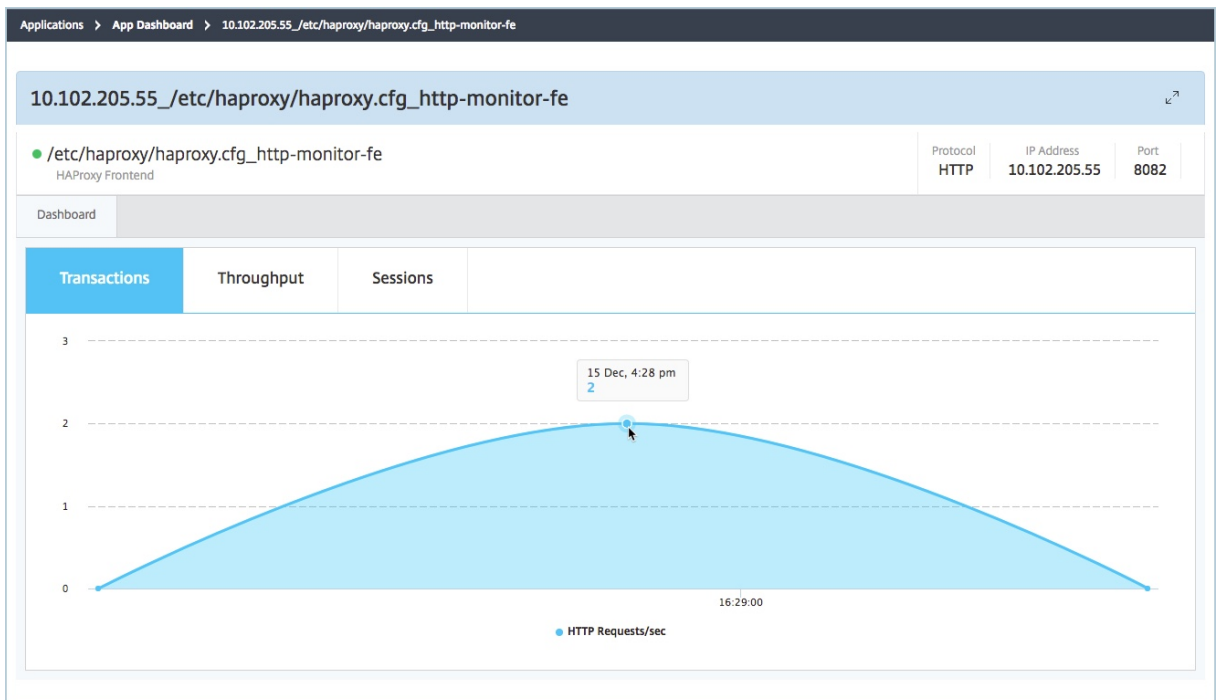
- **Transactions.** Transactions effectuées par l'application.
- **Débit.** Débit de l'application.
- **Sessions.** Nombre de sessions établies par la demande.

Pour afficher les performances en temps réel de votre application HAProxy, dans le Tableau de **bord des applications**, double-cliquez sur la vignette de l'application HAProxy.

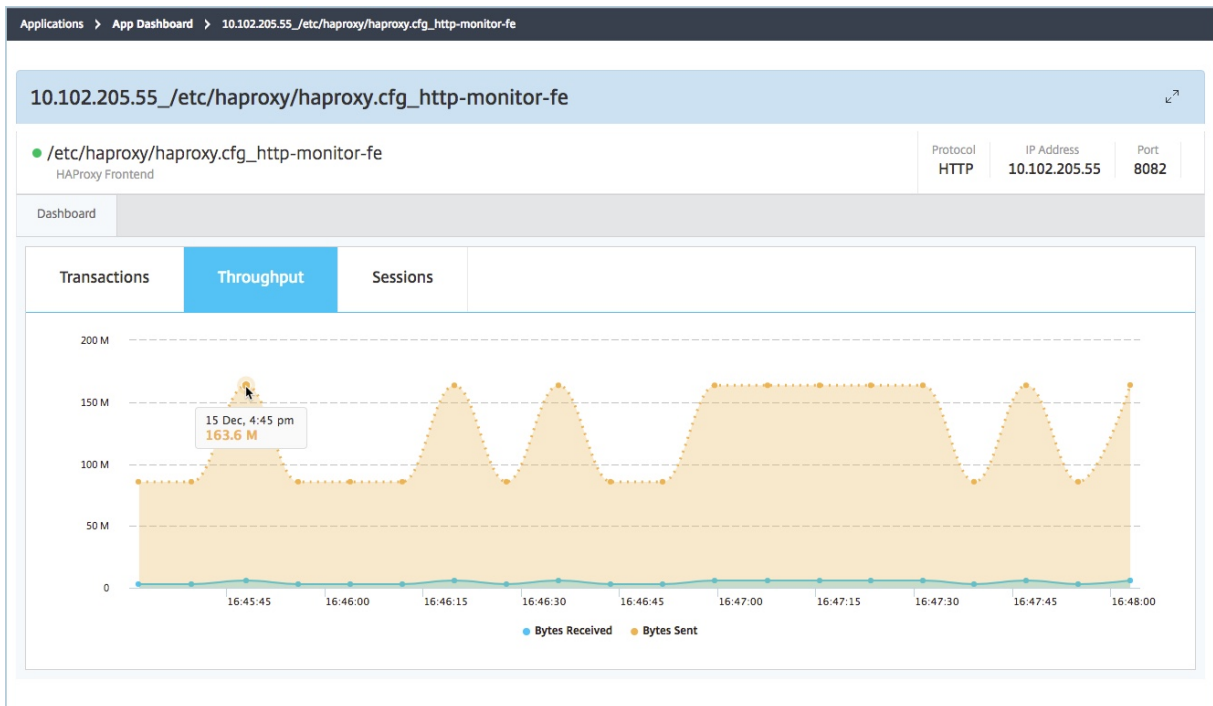




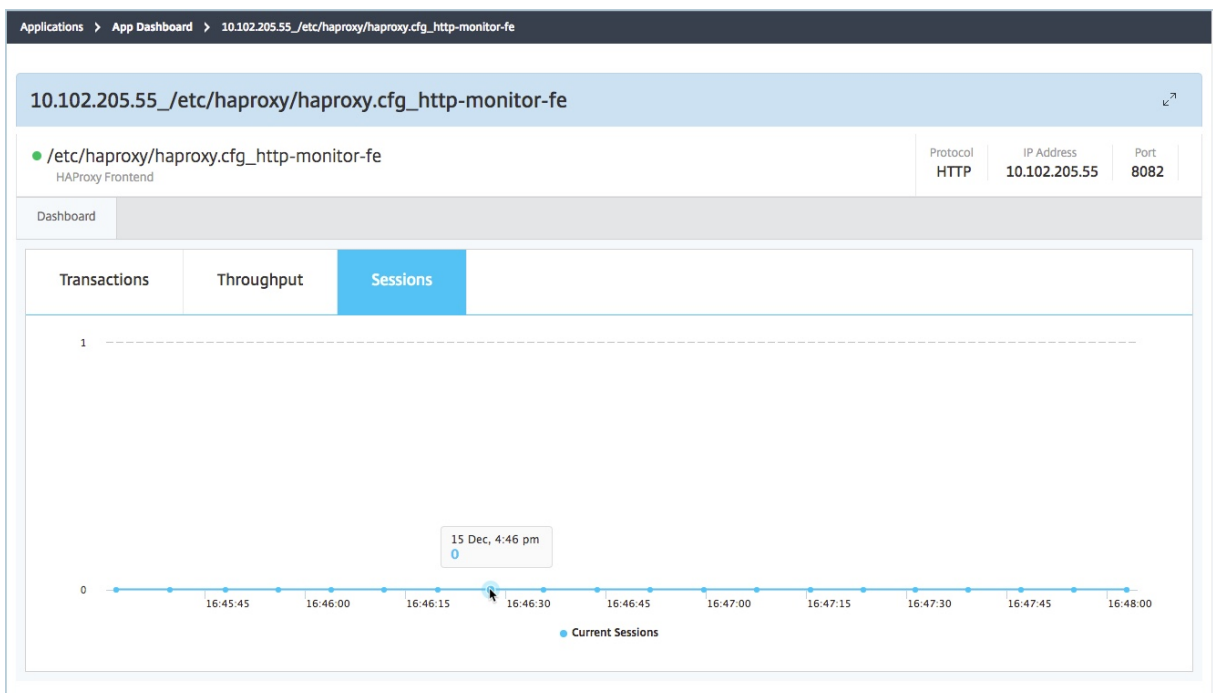
Par défaut, l'onglet **Transactions** est sélectionné et les transactions en temps réel effectuées par l'application sont affichées.



Pour afficher le débit en temps réel de l'application, cliquez sur l'onglet **Débit**.



Vous pouvez cliquer sur l'onglet **Sessions** pour afficher en temps réel le nombre de sessions établies par l'application.

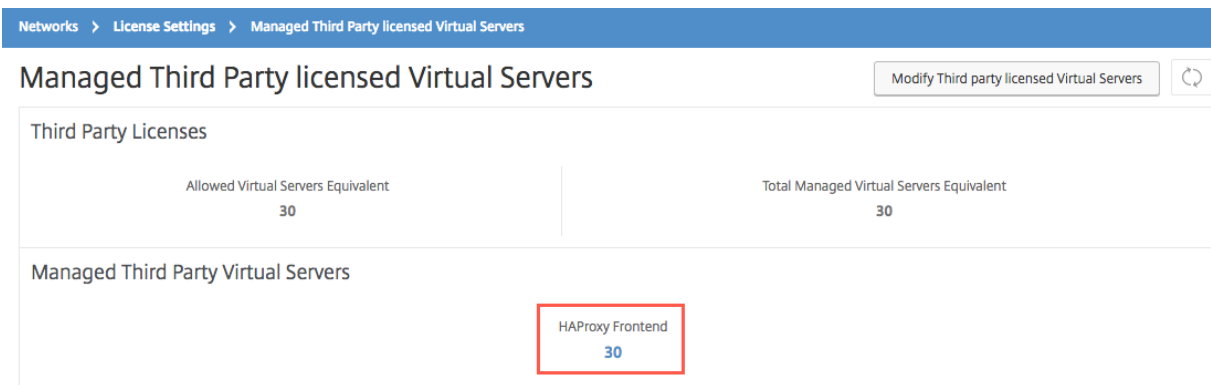


## Licences tierces

February 1, 2024

Après avoir ajouté les hôtes à Citrix Application Delivery Management (Citrix ADM), Citrix ADM découvre automatiquement les instances HaProxy mises en service sur les hôtes et les ajoute à Citrix ADM Inventory. Il détecte également tous les frontends, backends et serveurs configurés sur les instances HaProxy et considère les frontends comme des applications découvertes.

Vous pouvez gérer et surveiller toutes les applications découvertes, mais par défaut, le tableau de bord des applications HaProxy affiche les statistiques des applications pour 30 applications découvertes. Pour plus d'informations sur le tableau de bord des applications HaProxy, consultez Tableau de bord des applications HaProxy. Si vous souhaitez afficher les statistiques d'application de plus de 30 applications découvertes, vous devez acheter une licence distincte.



The screenshot shows the 'Managed Third Party licensed Virtual Servers' page in Citrix ADM. The breadcrumb trail is 'Networks > License Settings > Managed Third Party licensed Virtual Servers'. The page title is 'Managed Third Party licensed Virtual Servers' with a 'Modify Third party licensed Virtual Servers' button and a refresh icon. The main content area is divided into two sections: 'Third Party Licenses' and 'Managed Third Party Virtual Servers'. The 'Third Party Licenses' section shows two metrics: 'Allowed Virtual Servers Equivalent' at 30 and 'Total Managed Virtual Servers Equivalent' at 30. The 'Managed Third Party Virtual Servers' section shows a table with one entry: 'HAProxy Frontend' with a value of 30, which is highlighted with a red box.

Les licences pour les frontends supplémentaires sont disponibles dans des packs de serveurs virtuels de 100. Vous pouvez obtenir une licence valide et l'installer à l'aide de l'interface graphique Citrix ADM.

### Installation des licences tierces

Vous pouvez installer une licence sur Citrix ADM pour afficher les statistiques d'application de plus de 30 applications découvertes.

#### Pour installer une licence :

1. Dans un navigateur Web, saisissez l'adresse IP du **NetScaler Management and Analytics System** (par exemple, <http://192.168.100.1>).
2. Dans **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Accédez à **Réseaux > Licences**.

4. Dans la section **Fichiers de licence**, sélectionnez l'une des options suivantes :

- **Téléchargez les fichiers de licence depuis un ordinateur local.** Si une licence est déjà présente sur votre ordinateur local, cliquez sur Parcourir et sélectionnez le fichier de licence (.lic) que vous souhaitez utiliser pour allouer vos licences. Cliquez sur **Terminer**.
- **Utiliser le code d'activation de licence** - Citrix envoie un e-mail au BAC pour la licence que vous avez achetée. Entrez le BAC dans la zone de texte, puis cliquez sur **Obtenir des licences**.

**Remarque**

Si vous sélectionnez cette option, le système NetScaler Management and Analytics doit être connecté à Internet ou un serveur proxy doit être disponible.

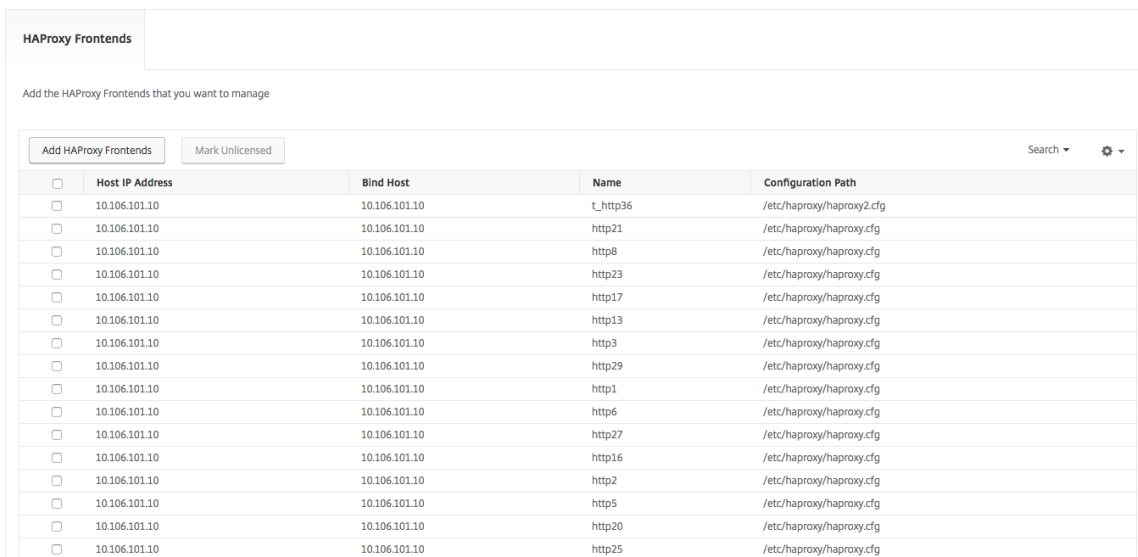
Vous pouvez vérifier les licences installées sur votre Citrix ADM en accédant à **Réseaux > Licences > Licenciestierces**.

## Gestion des licences tierces

Citrix ADM sélectionne de manière aléatoire les applications découvertes dans les instances HaProxy et les octroie automatiquement des licences. Si vous souhaitez modifier les applications découvertes sélectionnées, vous devez annuler manuellement la licence des applications découvertes sous licence, puis allouer les licences aux applications découvertes que vous souhaitez mettre sous licence.

### Pour gérer les licences tierces :

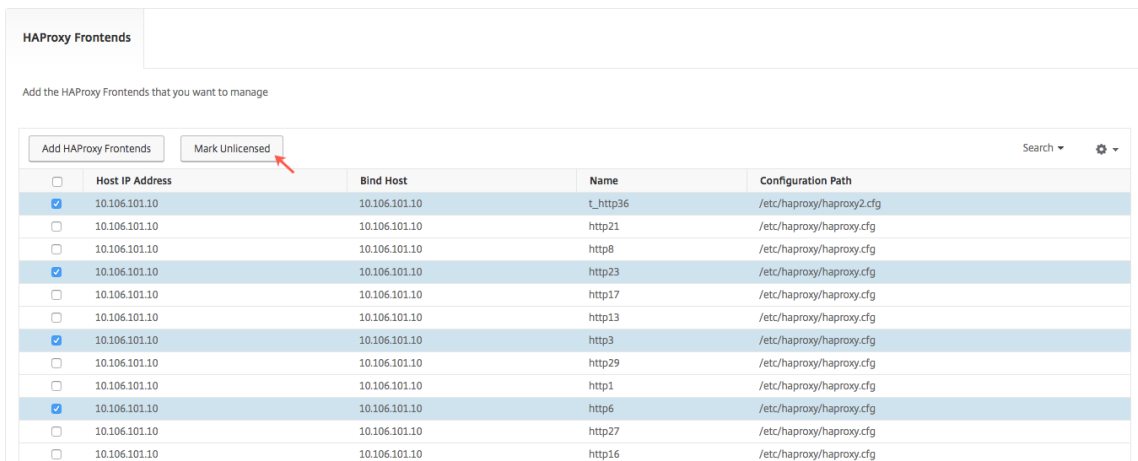
1. Accédez à **Réseaux > Licences > Licenciestierces** et cliquez sur **Modifier les serveurs virtuels sous licence tierce partie**. Le tableau de bord affiche les frontends gérés.



The screenshot shows the 'HAProxy Frontends' management page. At the top, there are buttons for 'Add HAProxy Frontends' and 'Mark Unlicensed'. Below is a table with the following columns: Host IP Address, Bind Host, Name, and Configuration Path. The table contains 17 rows of data, each with a checkbox in the first column.

<input type="checkbox"/>	Host IP Address	Bind Host	Name	Configuration Path
<input type="checkbox"/>	10.106.101.10	10.106.101.10	t_http36	/etc/haproxy/haproxy2.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http21	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http8	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http23	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http17	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http13	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http3	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http29	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http1	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http6	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http27	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http16	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http2	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http5	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http20	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http25	/etc/haproxy/haproxy.cfg

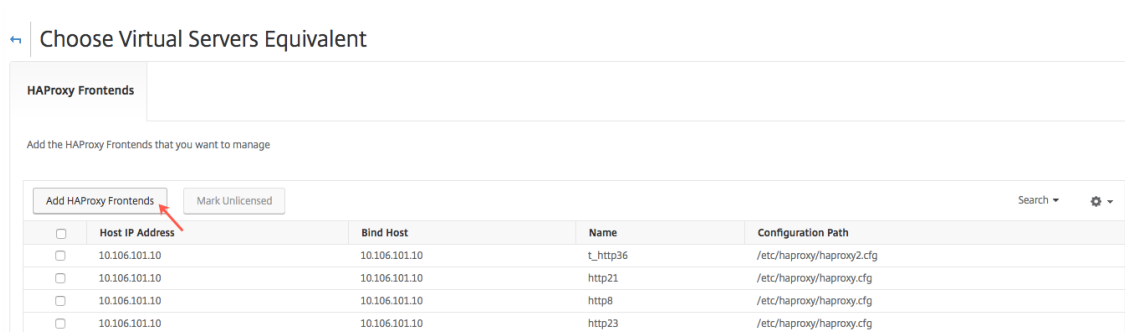
2. Sélectionnez les frontends dans la liste **Marquer sans licence**, puis cliquez sur **Terminer** pour libérer les licences.



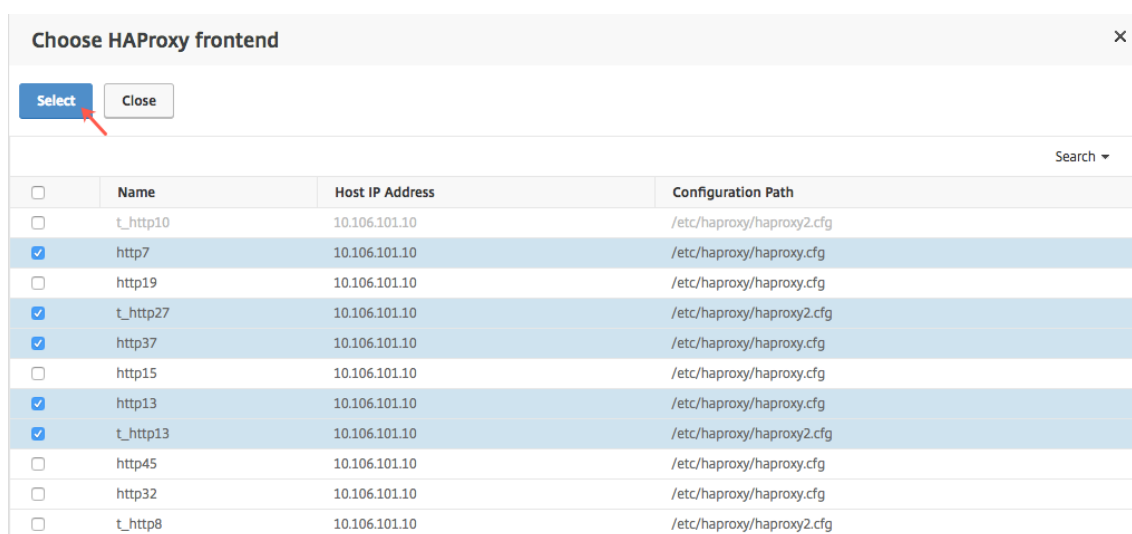
This screenshot is similar to the previous one, but several rows in the table are highlighted in blue, indicating they are selected. A red arrow points to the 'Mark Unlicensed' button. The selected rows are: t\_http36, http23, http3, http6, and http27.

<input type="checkbox"/>	Host IP Address	Bind Host	Name	Configuration Path
<input checked="" type="checkbox"/>	10.106.101.10	10.106.101.10	t_http36	/etc/haproxy/haproxy2.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http21	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http8	/etc/haproxy/haproxy.cfg
<input checked="" type="checkbox"/>	10.106.101.10	10.106.101.10	http23	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http17	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http13	/etc/haproxy/haproxy.cfg
<input checked="" type="checkbox"/>	10.106.101.10	10.106.101.10	http3	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http29	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http1	/etc/haproxy/haproxy.cfg
<input checked="" type="checkbox"/>	10.106.101.10	10.106.101.10	http6	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http27	/etc/haproxy/haproxy.cfg
<input type="checkbox"/>	10.106.101.10	10.106.101.10	http16	/etc/haproxy/haproxy.cfg

3. Après avoir libéré les licences, ou si vous avez déjà des licences disponibles, cliquez sur **Ajouter des frontends HaProxy**.



4. Dans la boîte de dialogue **Choisir le frontal HaProxy**, sélectionnez les frontends sans licence dans la liste et cliquez sur **Sélectionner**.



5. Cliquez sur **Terminer maintenant**.

## Contrôle d'accès basé sur les rôles pour les instances HaProxy

February 1, 2024

Citrix Application Delivery Management (Citrix ADM) utilise le contrôle d'accès basé sur les rôles (RBAC) fin pour contrôler l'accès aux objets de configuration. Par exemple, vous pouvez créer des utilisateurs et leur donner accès à des instances particulières de HaProxy, et vous pouvez spécifier une autorisation d'affichage/lecture seule pour le tableau de bord de l'application HaProxy. Pour plus d'informations, consultez [Contrôle d'accès basé sur les rôles dans Citrix ADM](#).

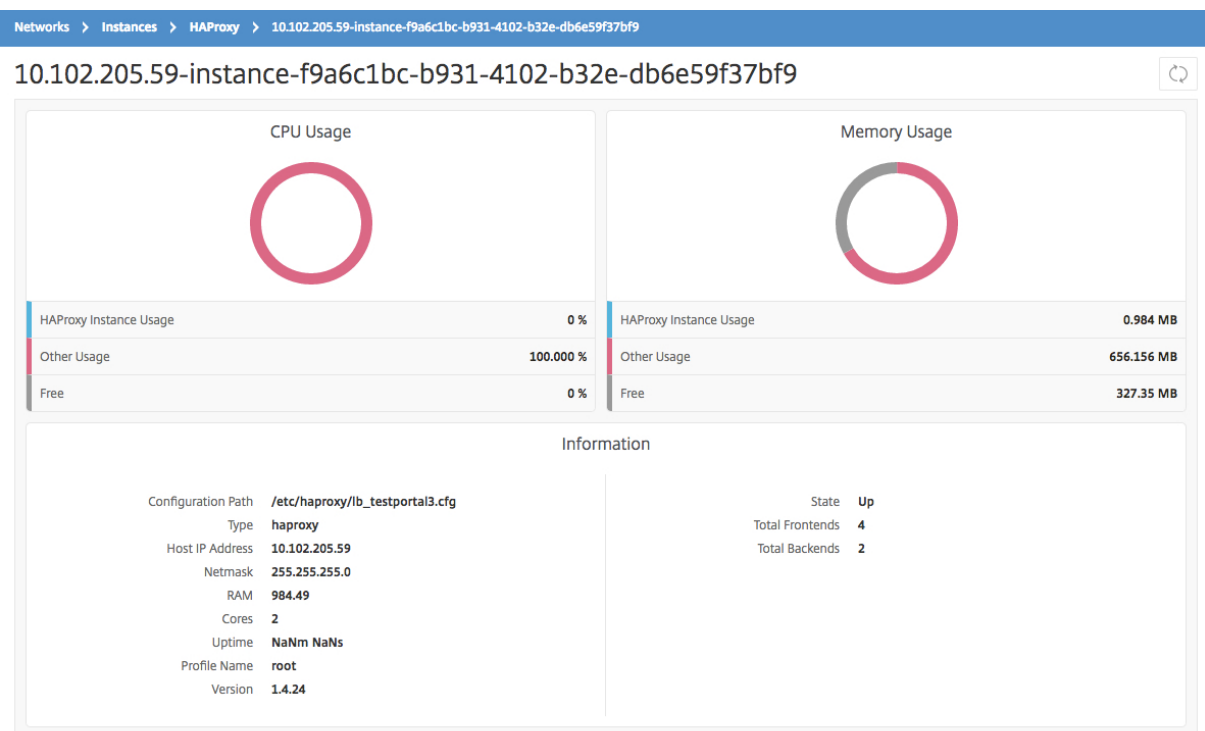
## Surveiller les instances HaProxy

February 1, 2024

Le tableau de bord HAProxy dans Citrix Application Delivery Management (Citrix ADM) affiche des graphiques qui vous aident à suivre l'utilisation du processeur et de la mémoire d'une instance HAProxy. Le tableau de bord affiche également des graphiques indiquant les éléments suivants :

- Pourcentage de CPU utilisé par l'instance HAProxy sur l'hôte.
- Pourcentage de CPU utilisé par d'autres entités sur l'hôte.
- Pourcentage de CPU restant sur l'hôte.
- Pourcentage de mémoire utilisée par l'instance HAProxy sur l'hôte.
- Pourcentage de mémoire utilisée par d'autres entités sur l'hôte.
- Pourcentage de mémoire restante sur l'hôte.

Pour surveiller une instance HAProxy dans Citrix ADM, accédez à l'onglet **Réseaux > Instances > HAProxy > Instances**, sélectionnez l'instance HAProxy, puis cliquez sur **Tableau de bord**.



## Afficher les détails des frontends configurés sur les instances HaProxy

February 1, 2024

Citrix Application Delivery Management (Citrix ADM) signale les détails suivants du frontal configuré sur une instance HAProxy :

- **Adresse IP de l'hôte.** Adresse IP de l'hôte
- **Chemin de configuration.**Chemin de configuration absolu de l'instance HaProxy sur l'hôte.
- **Nom.** Nom de l'interface qui gère le trafic entrant.
- **Lier l'hôte.** Adresse IP à laquelle le frontend est lié.
- **Port de liaison.** Port auquel le frontend est lié.

**Pour afficher le frontal configuré sur les instances HAProxy :**

Dans Citrix ADM, accédez à **Réseaux > Fonctions réseau > HAProxy > Frontends.**

[Dashboard](#) / [HAProxy](#) / [Frontends](#)

## Frontends

<input type="checkbox"/>	Host IP Address	Configuration Path	Name	Bind Host	Bind Port
<input type="checkbox"/>	10.102.205.132	haproxy.cfg	http-in	*	80
<input type="checkbox"/>	10.102.205.132	haproxy7.cfg	http-i21n	*	820
<input type="checkbox"/>	10.102.205.132	haproxy4.cfg	http-in	*	80
<input type="checkbox"/>	10.102.205.132	haproxy9.cfg	http-in	*	820
<input type="checkbox"/>	10.102.205.132	haproxy11.cfg	http-i22n	*	8014
<input type="checkbox"/>	10.102.205.132	haproxy6.cfg	http-i22n	*	8014
<input type="checkbox"/>	10.102.205.132	haproxy8.cfg	http-in	*	810
<input type="checkbox"/>	10.102.205.132	haproxy1.cfg	http-in	*	80
<input type="checkbox"/>	10.102.205.132	haproxy6.cfg	http-i1n	*	8025
<input type="checkbox"/>	10.102.205.132	haproxy7.cfg	http-i11	*	8011
<input type="checkbox"/>	10.102.205.132	haproxy6.cfg	http-i1	*	8051
<input type="checkbox"/>	10.102.205.132	haproxy7.cfg	http-i11n	*	8021

## Afficher les détails des backends configurés sur les instances HAProxy

February 1, 2024

Citrix Application Delivery Management (Citrix ADM) signale les détails suivants d'une application principale configurée sur une instance HAProxy :

- **Adresse IP de l'hôte.** Adresse IP de l'hôte.
- **Chemin de configuration.** Chemin d'instance HAProxy sur l'hôte.



- **Nom.** Nom du moteur vers lequel le trafic est transféré.
- **Algorithme.** Algorithme d'équilibrage de charge utilisé pour équilibrer le trafic.

**Pour afficher le moteur configuré sur les instances HAProxy :**

Dans Citrix ADM, accédez à **Réseaux > Fonctions réseau > HAProxy > Backends.**

Backends ↻ ↗

<input type="checkbox"/>	Host IP Address	Configuration Path	Name	Algorithm
<input type="checkbox"/>	10.102.205.59	lb_testportal4.cfg	api_backend2	roundrobin
<input type="checkbox"/>	10.102.205.59	lb_testportal3.cfg	api_backend2	roundrobin
<input type="checkbox"/>	10.102.205.59	lb_testportal2.cfg	api_backend1	roundrobin
<input type="checkbox"/>	10.102.205.178	lb_mas.cfg	api_backend2	roundrobin
<input type="checkbox"/>	10.102.205.59	lb_testportal4.cfg	api_backend1	roundrobin
<input type="checkbox"/>	10.102.205.59	lb_testportal1.cfg	api_backend2	roundrobin
<input type="checkbox"/>	10.102.205.178	lb_mas.cfg	api_backend1	roundrobin
<input type="checkbox"/>	10.102.205.59	lb_testportal1.cfg	api_backend1	roundrobin
<input type="checkbox"/>	10.102.205.59	lb_testportal2.cfg	api_backend2	roundrobin
<input type="checkbox"/>	10.102.205.59	lb_testportal3.cfg	api_backend1	roundrobin

## Afficher les détails des serveurs configurés sur les instances HAProxy

February 1, 2024

Citrix Application Delivery Management (Citrix ADM) signale les détails suivants des serveurs configurés sur une instance HAProxy :

- **Adresse IP de l'hôte.** Nom de l'hôte.
- **Chemin de configuration.**Chemin absolu du fichier de configuration d'instance HAProxy sur l'hôte.
- **Nom du backend.** Nom du moteur dans la configuration HAProxy.
- **Nom.** Nom du serveur dans la configuration HAProxy.
- **Adresse du serveur.** Adresse IP du serveur.
- **Port serveur.** Port utilisé par le serveur.

**Pour afficher les serveurs configurés sur les instances HAProxy :**

Dans Citrix ADM, accédez à **Réseaux > Fonctions réseau > HAProxy > Serveurs.**

Servers ↻ ↗

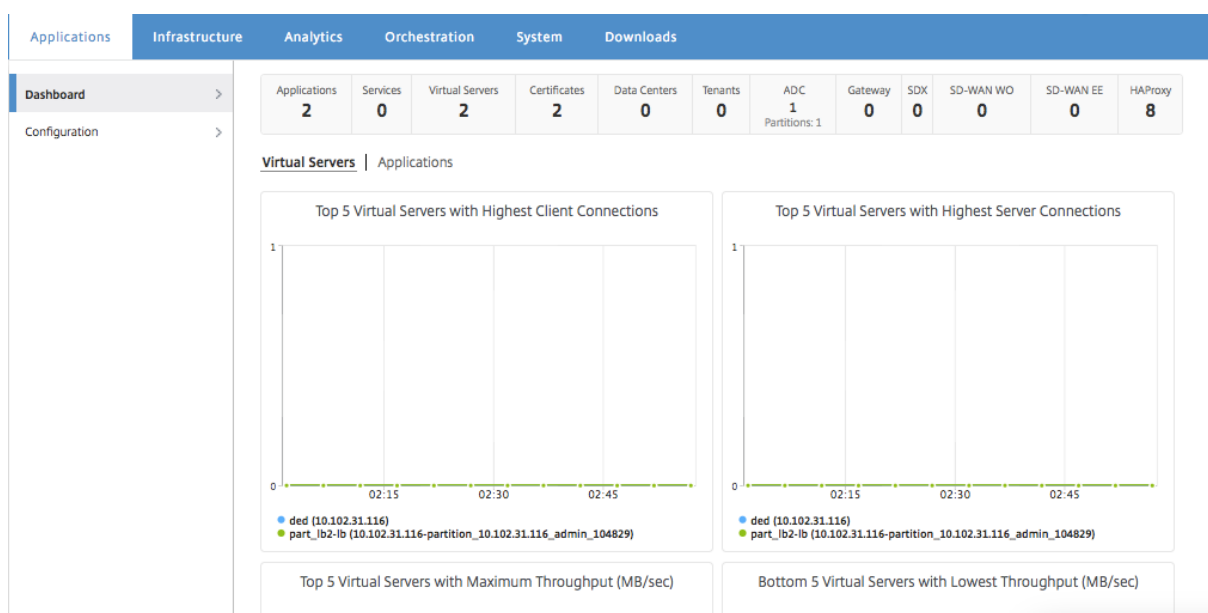
<input type="checkbox"/>	Host IP Address	Configuration Path	Backend Name	Name	Server Address	Server Port
<input type="checkbox"/>	10.102.205.178	lb_mas.cfg	api_backend1	api_machine_1	10.102.31.178	80
<input type="checkbox"/>	10.102.205.59	lb_testportal3.cfg	api_backend1	api_machine_1	10.102.31.178	80
<input type="checkbox"/>	10.102.205.59	lb_testportal4.cfg	api_backend1	api_machine_1	10.102.31.178	80
<input type="checkbox"/>	10.102.205.59	lb_testportal2.cfg	api_backend1	api_machine_1	10.102.31.178	80
<input type="checkbox"/>	10.102.205.59	lb_testportal1.cfg	api_backend1	api_machine_1	10.102.31.178	80

## Afficher les instances HaProxy avec le plus grand nombre de frontends ou de serveurs

February 1, 2024

Dans le tableau de bord des applications, Citrix Application Delivery Management (Citrix ADM) affiche le nombre d'instances HAProxy qu'il découvre et répertorie les cinq premières instances HAProxy configurées avec le plus grand nombre de frontaux ou de serveurs.

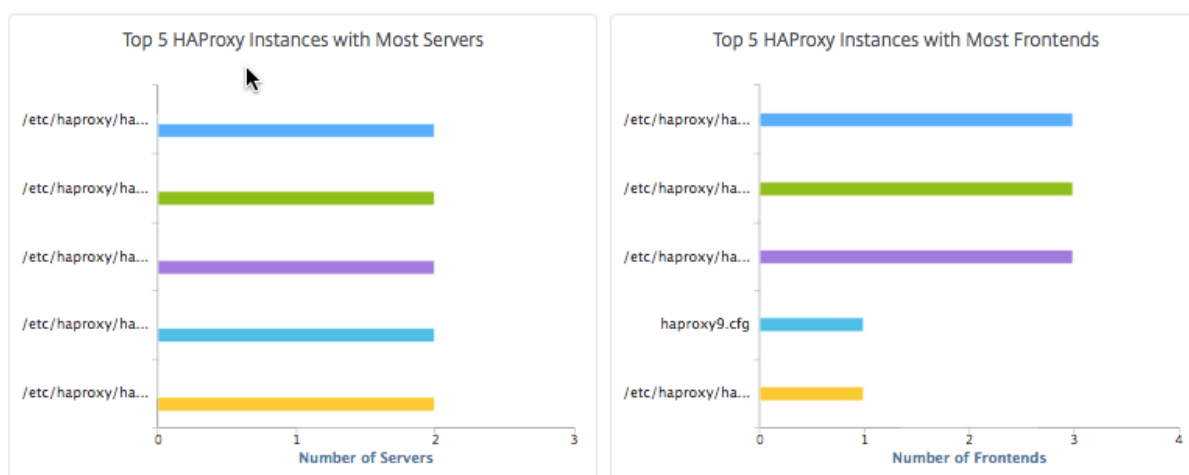
Pour afficher le tableau de bord des applications, dans Citrix ADM, accédez à **Applications > Tableau de bord**.



Le nombre d'instances HaProxy découvertes par Citrix ADM s'affiche dans la ligne supérieure, comme indiqué ci-dessous :

Applications	Services	Virtual Servers	Certificates	Data Centers	Tenants	ADC	Gateway	SDX	SD-WAN WO	SD-WAN EE	HAProxy
2	0	2	2	0	0	1 Partitions: 1	0	0	0	0	8

Pour afficher la liste des cinq instances HaProxy les plus configurées avec le plus grand nombre de frontends ou le plus grand nombre de serveurs, faites défiler le tableau de bord vers le bas :



## Redémarrer une instance HAProxy

February 1, 2024

Pour redémarrer une instance HAProxy à partir de l'interface graphique Citrix Application Delivery Management (Citrix ADM), vous pouvez sélectionner un redémarrage dur ou un redémarrage progressif.

### Redémarrage dur

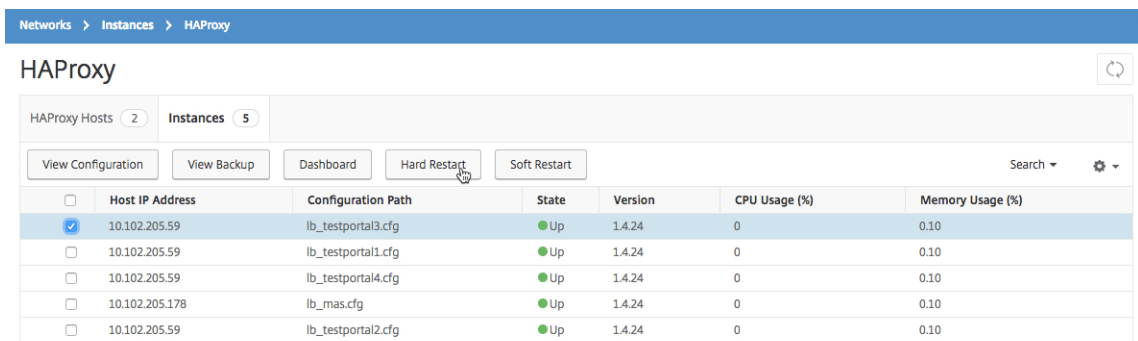
Le redémarrage dur interrompt le processus HAProxy sur l'instance et ferme toutes les connexions établies. Après le redémarrage, un nouveau processus haproxy est créé et les nouvelles connexions suivantes sont traitées par le nouveau processus HAProxy.

### Redémarrage progressif

Le redémarrage progressif délègue le processus HAProxy du port d'écoute, mais le processus HAProxy continue de traiter les connexions existantes jusqu'à leur fermeture. Un nouveau processus HAProxy est créé pour traiter les nouvelles connexions.

**Pour redémarrer une instance HAProxy, procédez comme suit :**

1. Accédez à **Réseaux > Instances > HAProxy** et cliquez sur l'onglet **Instance**.
2. Sous l'onglet **Instance**, sélectionnez l'instance HAProxy que vous souhaitez redémarrer.
3. Cliquez sur **Redémarrer dur** pour redémarrer l'instance HAProxy ou cliquez sur **Redémarrer logiciel** pour redémarrer l'instance HAProxy.



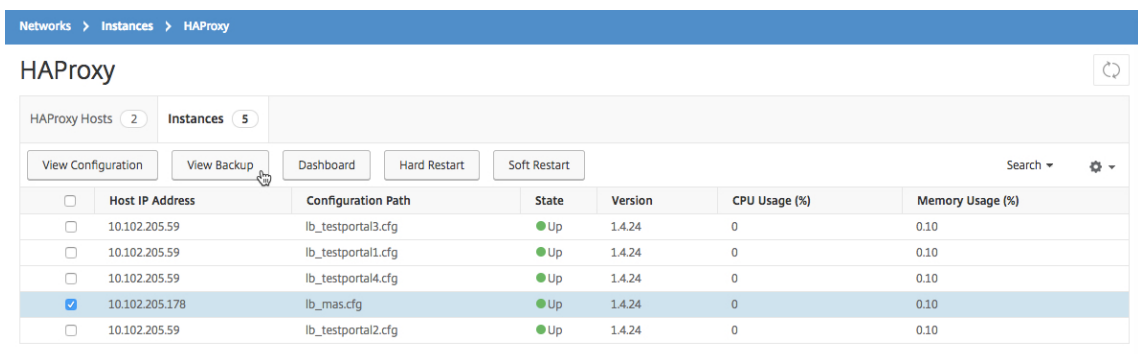
## Sauvegarder et restaurer une instance HaProxy

February 1, 2024

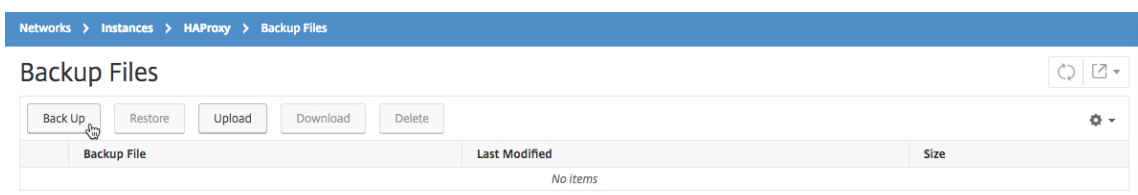
Vous pouvez sauvegarder l'état actuel d'une instance HAProxy dans un fichier de configuration HAProxy. Si l'instance devient instable, vous pouvez utiliser le fichier backedup pour restaurer l'instance à l'état stable.

### Pour sauvegarder une instance HaProxy à l'aide de Citrix ADM :

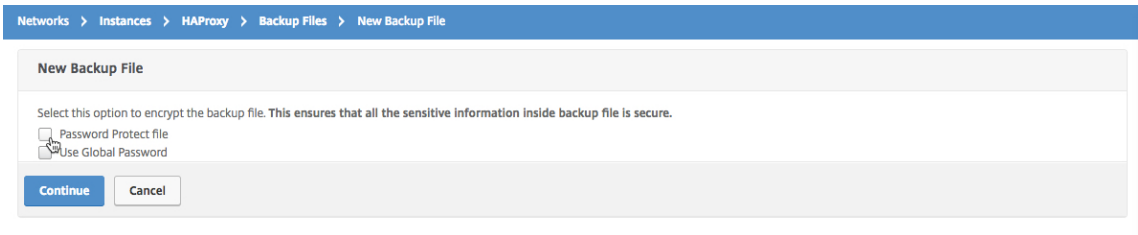
1. Dans Citrix Application Delivery Management (Citrix ADM), accédez à **Réseaux > Instances > HAProxy**.
2. Dans la page **HaProxy**, cliquez sur l'onglet **Instances**.
3. Sélectionnez l'instance HAProxy à sauvegarder, puis cliquez sur **Afficher la sauvegarde**.



4. Sur la page **Fichiers de sauvegarde**, cliquez sur **Sauvegarder**.



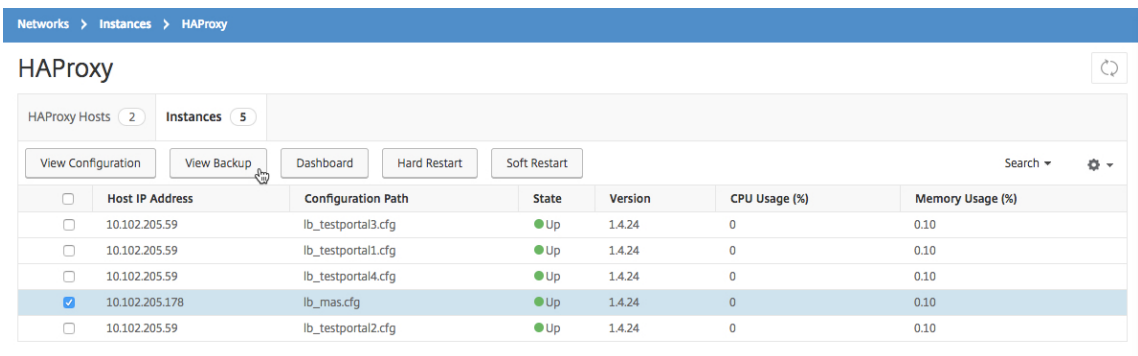
5. Vous pouvez choisir de chiffrer votre fichier de sauvegarde pour plus de sécurité.



6. Cliquez sur **Continuer**.

**Pour restaurer une instance à l'aide de Citrix ADM :**

1. Accédez à **Réseaux > Instances > HAProxy**.
2. Sur la page **HaProxy**, cliquez sur l'onglet **Instances**.
3. Sélectionnez l'instance à restaurer, puis cliquez sur **Afficher la sauvegarde**.



4. Dans la page **Fichiers de sauvegarde**, sélectionnez le fichier de sauvegarde à restaurer, puis cliquez sur **Restaurer**.



**Remarque**

Lorsque vous restaurez une instance, le logiciel Citrix ADM redémarre l'instance HAProxy.

**Modifier le fichier de configuration HaProxy**

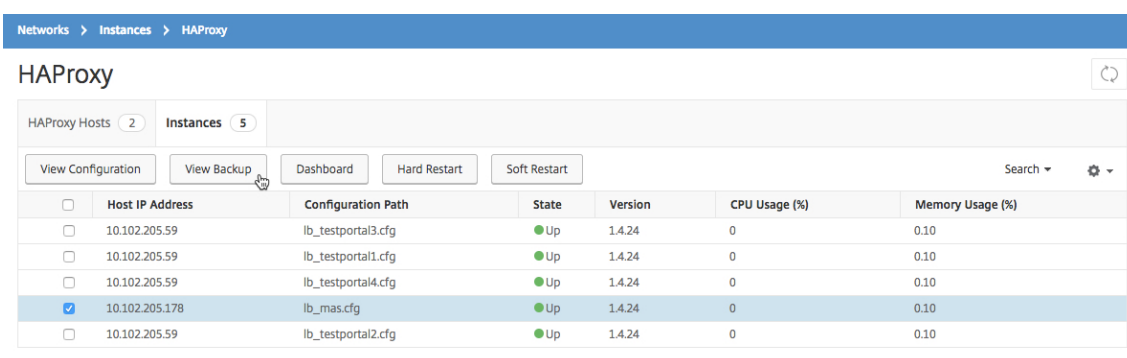
February 1, 2024

Vous pouvez mettre à jour le frontend, le backend, le serveur et d'autres paramètres dans le fichier de configuration HaProxy existant. Pour modifier le fichier de configuration HaProxy :

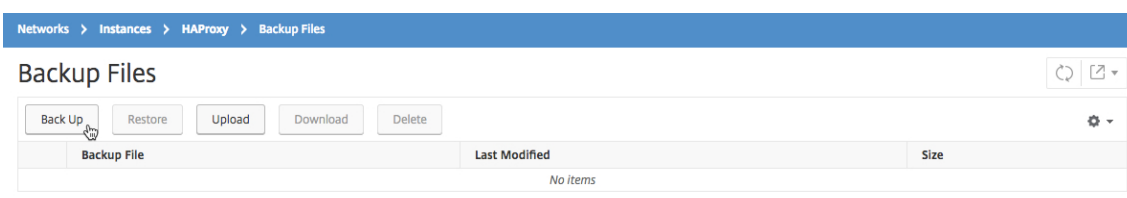
- Sauvegardez le fichier de configuration HAProxy.
- Téléchargez le fichier de configuration de sauvegarde HaProxy et modifiez-le hors connexion.
- Télécharger le fichier de configuration HaProxy mis à jour dans Citrix Application Delivery Management (Citrix ADM)
- Restaurez l'instance HaProxy avec le fichier de sauvegarde mis à jour.

**Pour modifier le fichier de configuration HAProxy à l'aide de Citrix ADM :**

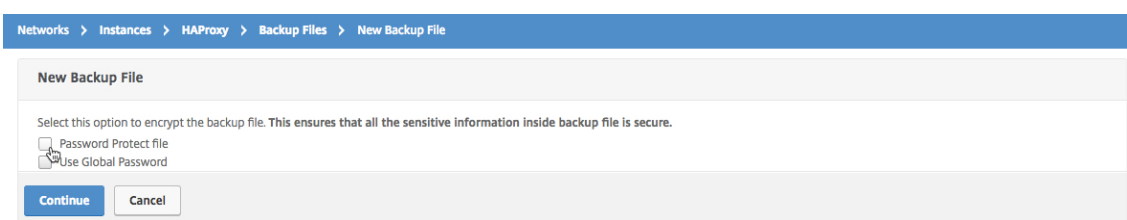
1. Dans Citrix ADM, accédez à **Réseaux > Instances > HAProxy**.
2. Sur la page **HaProxy**, cliquez sur l'onglet **Instances**.
3. Sélectionnez l'instance HAProxy à sauvegarder, puis cliquez sur **Afficher la sauvegarde**.



4. Sur la page **Fichiers de sauvegarde**, cliquez sur **Sauvegarder**.



5. Cliquez sur **Continuer**.



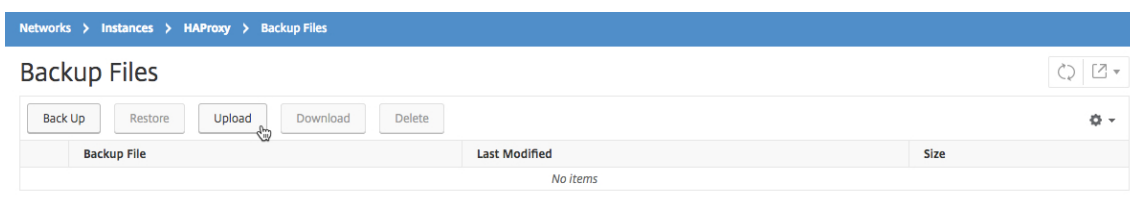
**Remarque**

Ne chiffrez pas le fichier de sauvegarde.

- Sur la page **Fichiers de sauvegarde**, sélectionnez le fichier de sauvegarde et cliquez sur **Télécharger**.



- À l'aide d'un éditeur de texte, modifiez le fichier de configuration HAProxy.
- Dans la page **Fichiers de sauvegarde**, cliquez sur **Télécharger** pour parcourir et sélectionner le fichier de configuration HaProxy mis à jour.



Une fois le fichier de configuration HaProxy mis à jour téléchargé, il est répertorié sur la page **Fichiers de sauvegarde**.

- Sélectionnez le fichier de configuration HaProxy mis à jour et cliquez sur **Restaurer**.

## Gérer les paramètres système

February 1, 2024

Le tableau suivant décrit comment configurer les paramètres système de votre Citrix ADM.

| Si vous voulez... | Procédez comme suit... |

-	
Configurer le message du jour	Vous pouvez désormais créer un message de bienvenue dans Citrix ADM. Vous pouvez utiliser cette fonctionnalité pour définir des messages de rappel pour vous-même ou pour l'utilisateur qui ouvre une session sur Citrix ADM. Accédez à <b>System</b> > <b>System Parameters</b> et cliquez sur <b>Configure Daily Message</b> . Cliquez sur <b>Activate Message</b> , tapez le message dans la zone de message, puis cliquez sur <b>OK</b> .
Arrêtez Citrix ADM	Accédez à <b>System</b> > <b>System Administration</b> . Vous pouvez cliquer sur <b>Stop Citrix ADM</b> pour arrêter complètement Citrix ADM. <b>Remarque</b> Une fois que vous avez arrêté Citrix ADM, vous ne pouvez redémarrer Citrix ADM qu'à partir de l'hyperviseur sur lequel vous l'avez installé.

| Configurer les paramètres de l'assistant de configuration | Accédez à **Système** > **Administration système**. Sous **Configurer Citrix ADM**, sélectionnez **Paramètres de l'assistant de configuration**. Vous pouvez sélectionner l'option **Citrix ADM Network** pour modifier les paramètres réseau, tels que l'adresse IP de Citrix ADM et son mot de passe. Vous pouvez cliquer sur **Paramètres système** pour modifier le nom d'hôte, le mode de communication avec les instances ou le fuseau horaire local. |

| Configurer les paramètres réseau | Accédez à **Système** > **Administration système**. Dans **Configurer Citrix ADM**, sélectionnez **Configuration réseau**. L'interface graphique affiche les certificats et clés SSL installés sur Citrix ADM. |

| Afficher le certificat SSL | Accédez à **Système** > **Administration système**. Dans **Configurer Citrix ADM**, sélectionnez **Afficher le certificat SSL**. L'interface graphique affiche les certificats et clés SSL installés sur Citrix ADM. |

| Modifier fuseau horaire | Accédez à **Système** > **Administration du système**. Dans **Paramètres système**, sélectionnez **Modifier le fuseau horaire**. Dans la liste déroulante **Fuseau** horaire, sélectionnez le fuseau horaire de l'horloge de votre appliance Citrix ADM. |

| Changer nom d'hôte | Accédez à **Système** > **Administration système**. Dans **Paramètres système**, sélectionnez **Modifier le nom** d'hôte. Entrez un nom d'hôte qui sera utilisé pour identifier votre Citrix ADM, de sorte que lorsque vous générez la licence universelle pour Citrix ADM Gateway, le nom d'hôte soit affiché dans la licence. |

| Modifier les paramètres du système | Accédez à **Système** > **Administration du système**. Sous **Paramètres système**, sélectionnez **Modifier les paramètres système**. Ensuite, cochez ou désactivez les cases à cocher pour activer ou désactiver les fonctionnalités suivantes : Accès sécurisé uniquement, Activer le délai d'expiration de la session, Autoriser l'authentification de base, Activer la connexion nsrecover, Activer le téléchargement du certificat, Activer l'accès Shell pour les utilisateurs n'appartenant pas à nsroot, Demander les informations d'identification de l'utilisateur pour la connexion par exemple |

| Configurer les paramètres SSL | Accédez à **Système** > **Administration système**. Sous **Paramètres système**, sélectionnez **Configurer les paramètres SSL** pour afficher les paramètres de protocole actuels et les suites de chiffrement appliquées. Si vous souhaitez modifier l'un des paramètres, sous **Modifier les paramètres**, sélectionnez **Paramètres du protocole** ou **Suites de chiffrement**. |

| Activer la fonctionnalité des paramètres d'amélioration de l'expérience utilisateur | Accédez à **Système** > **Administration système**. Sous **Paramètres système**, sélectionnez **Configurer les paramètres d'amélioration de l'expérience utilisateur**, puis cochez la case **Activer CUXIP**. Si vous cochez cette case, les statistiques d'utilisation sont collectées dans le seul but d'améliorer l'interface utilisateur graphique. Les données reçues sont utilisées uniquement par les ingénieurs de Citrix et ne sont partagées avec personne. |

| Mettre à niveau Citrix ADM | Accédez à **Système** > **Administration système**. Dans le sous-titre **Administration du système**, sélectionnez **Mettre à niveau Citrix ADM**, puis sélectionnez le



nouveau fichier image. Vous pouvez sélectionner un fichier qui se trouve déjà sur l'apppliance virtuelle Citrix ADM ou télécharger un fichier depuis votre ordinateur local. |

| Redémarrez Citrix ADM | Accédez à **Système** > **Administration système**. Dans le sous-titre **Administration du système**, sélectionnez **Redémarrer Citrix ADM**. Une boîte de dialogue apparaît, vous demandant de confirmer votre action. Cliquez sur **Oui**. |

| Configurer les paramètres de nettoyage du système (pour le nettoyage des anciennes données) | Accédez à **Système** > **Administration système**. Sous **Paramètres d'élagage**, sélectionnez **Paramètres d'élagage du système**. Dans le champ **Données à conserver (jours)**, entrez le nombre de jours pendant lesquels vous souhaitez conserver les données dans le système. |

| Configuration des paramètres de sauvegarde du système | Accédez à **Système** > **Administration système**. Dans **Paramètres de sauvegarde**, sélectionnez **Paramètres de sauvegarde du système**, puis entrez le nombre de sauvegardes système à conserver sur l'apppliance Citrix ADM. Vous pouvez également choisir de chiffrer les fichiers de sauvegarde et spécifier un emplacement externe vers lequel les transférer. Les fichiers de sauvegarde transférés peuvent être conservés ou supprimés du système. |

| Configurer les paramètres de sauvegarde de l'instance | Accédez à **Système** > **Administration système**. Dans **Paramètres de sauvegarde**, sélectionnez **Paramètres de sauvegarde** des instances et entrez l'intervalle de temps (en heures) auquel vous souhaitez créer un fichier de sauvegarde sauvegardant toutes les instances gérées par Citrix ADM. Vous pouvez spécifier le nombre de fichiers de sauvegarde à conserver et indiquer s'il faut les chiffrer afin qu'ils ne soient pas accessibles sans mot de passe. |

| Afficher les statistiques du système | Accédez à **Système** > **Statistiques**. Un graphique linéaire affiche des informations telles que l'utilisation du processeur, de la mémoire et de l'utilisation du disque. |

| Afficher et gérer les sessions | Accédez à **Système** > **Sessions**. Vous pouvez ensuite voir toutes les sessions actives, avec des détails. Pour mettre fin à une session, cochez la case correspondante et cliquez sur **Annuler la session**. |

| Ajouter ou modifier un locataire | Accédez à **Système** > **Locataires** et ajoutez un nouveau locataire ou modifiez les paramètres d'un locataire existant. Vous pouvez fournir des informations supplémentaires, telles que le nom de l'unité organisationnelle, le département et l'URL du locataire. |

| Modifier la stratégie de verrouillage des utilisateurs | Accédez à **Système** > **Administration des utilisateurs**. Dans **Configuration utilisateur**, sélectionnez **Configuration du verrouillage utilisateur**, puis cochez la case **Activer le verrouillage utilisateur**. Vous pouvez spécifier le nombre de tentatives non valides qu'un utilisateur peut effectuer avant que son compte ne soit désactivé, ainsi que la durée pendant laquelle la stratégie de verrouillage des utilisateurs est active. |

| Modifier la complexité du mot de passe | Accédez à **Système** > **Administration des utilisateurs**. Dans **Configuration utilisateur**, sélectionnez **Stratégie de mot** de passe, puis cochez la case **Activer la complexité des mots** de passe. Dans le champ **Longueur minimale du mot** de

passer, entrez le nombre minimum de caractères requis pour un mot de passe sur Citrix ADM. |

| Ajouter ou modifier un utilisateur | Accédez à **Système** > **Administration** des utilisateurs > Utilisateurs. Sous Utilisateurs, ajoutez un nouvel utilisateur ou modifiez les paramètres d'un utilisateur existant. Lorsque vous ajoutez un utilisateur, vous pouvez activer des options telles que l'authentification externe, le délai d'expiration de la session et l'affectation de l'utilisateur à des groupes spécifiques. |

| Ajouter ou modifier un groupe d'utilisateurs | Accédez à **Système** > **Administration des utilisateurs** > **Groupes**. Sous **Groupes**, ajoutez un nouveau groupe ou modifiez les paramètres d'un groupe existant. Lorsque vous ajoutez un groupe, vous pouvez activer des options telles que l'attribution d'autorisations au groupe, la configuration d'un délai d'expiration de session, l'attribution d'utilisateurs au groupe et l'autorisation d'accéder à certaines applications ou à toutes les applications sur Citrix ADM. |

| Modifier la configuration d'authentification | Accédez à **Système** > **Authentification** > **Authentification**. Sous **Authentification**, sélectionnez **Configuration de l'authentification**, puis sélectionnez le type de serveur d'authentification. |

| Ajouter ou modifier un serveur RADIUS | Accédez à **Système** > **Authentification** > **RADIUS**. Sous **RADIUS**, ajoutez un nouveau serveur RADIUS ou modifiez les paramètres d'un serveur RADIUS existant en saisissant ou en modifiant les paramètres réseau. |

| Ajouter ou modifier un serveur LDAP | Accédez à **Système** > **Authentification** > **LDAP**. Sous LDAP, ajoutez un nouveau serveur LDAP ou modifiez les paramètres d'un serveur LDAP existant en saisissant ou en modifiant les paramètres réseau. |

| Ajouter ou modifier un serveur TACACS | Accédez à **Système** > **Authentification** > **TACACS**. Sous **TACACS**, ajoutez un nouveau serveur TACACS ou modifiez les paramètres d'un serveur TACACS existant en saisissant ou en modifiant les paramètres réseau. |

| Ajouter ou modifier un serveur Syslog | Accédez à **Système** > **Audit** > **Serveurs Syslog**. Sous **Serveurs Syslog**, ajoutez un nouveau serveur Syslog ou modifiez les paramètres d'un serveur Syslog existant en saisissant ou en modifiant les paramètres réseau. Vous pouvez fournir des informations supplémentaires en sélectionnant le type de niveaux de journalisation que vous souhaitez surveiller. |

| Lire les messages Syslog | Accédez à **Système** > **Audit**. Sous **Messages d'audit**, sélectionnez **Messages Syslog**. Les résumés de tous les fichiers journaux du système sont affichés dans le Syslog Viewer. Vous pouvez sélectionner le fichier syslog que vous souhaitez afficher dans la liste déroulante Fichier. En outre, les fichiers syslog peuvent être filtrés davantage par module, type d'événement et gravité. |

| Configurer les paramètres de purge du Syslog | Accédez à **Système** > **Audit**. Dans **Paramètres**, sélectionnez **Paramètres de purge Syslog**, puis entrez le nombre de jours pendant lesquels les données Syslog doivent être conservées avant leur suppression de Citrix ADM. |

| Afficher les événements du système | Accédez à **Système** > **Événements**. Vous pouvez ensuite voir toutes les actualités, avec des détails. |

| Ajouter ou modifier un serveur NTP | Accédez à **Système** > **Serveurs NTP**. Ajoutez un nouveau serveur NTP ou modifiez les paramètres d'un serveur NTP existant. |

| Configuration des paramètres NTP | Accédez à **Système** > **Serveurs NTP**. Cliquez sur **Paramètres NTP** et entrez les détails de configuration du serveur dans les champs prévus à cet effet. |

| Activer la synchronisation NTP | Accédez à **Système** > **Serveurs NTP**. Pour synchroniser l'heure affichée sur le serveur NTP avec votre horloge locale, cochez la case **Activer la synchronisation NTP**. |

| Ajouter ou modifier des groupes de chiffrement | Accédez à **Système** > **Groupes de chiffrement** pour ajouter un nouveau groupe de chiffrement ou modifier les paramètres d'un groupe de chiffrement existant. Vous devez saisir une description de votre groupe de chiffrement et l'affecter à une suite de chiffrement. |

| Configurer les paramètres de notification | Accédez à **Système** > **Notifications**. Sous **Paramètres**, sélectionnez **Modifier les paramètres de notification**. Choisissez les actions pour lesquelles vous souhaitez envoyer les notifications, puis sélectionnez E-**mail**, **SMS** ou les deux. |

| Configurer les paramètres du résumé des événements | Accédez à **Système** > **Notifications**. Sous **Paramètres**, sélectionnez **Configurer les paramètres de l'Event Digest**. Après avoir décoché la case **Désactiver le résumé des événements**, vous pouvez définir une période de récurrence et choisir une liste de distribution par e-mail pour envoyer les notifications du résumé des événements. |

| Ajouter ou modifier des serveurs de messagerie | Accédez à **Système** > **Notifications** > E-**mail**. Sous E-**mail**, sélectionnez l'onglet **Serveurs** de messagerie pour ajouter un nouveau serveur de messagerie ou modifier les paramètres d'un serveur de messagerie existant. Vous pouvez activer des contrôles supplémentaires pour vous assurer que l'authentification est requise pour accéder au serveur de messagerie ou pour spécifier que votre serveur de messagerie prend en charge l'authentification SSL. |

| Ajouter ou modifier des listes de distribution d'e-mails | Accédez à **Système** > **Notifications** > E-**mail**. Sous E-**mail**, sélectionnez l'onglet **Liste de distribution d'e-mails** pour ajouter une nouvelle liste de distribution d'e-mails ou modifier les paramètres d'une liste de distribution d'e-mails existante. |

| Ajouter ou modifier des serveurs SMS | Accédez à **Système** > **Notifications** > **SMS**. Sous **SMS**, sélectionnez l'onglet **Serveur SMS** pour ajouter un nouveau serveur SMS ou modifier les paramètres d'un serveur SMS existant. |

| Ajouter ou modifier des listes de distribution de SMS | Accédez à **Système** > **Notifications** > **SMS**. Sous **SMS**, sélectionnez l'onglet **Liste de distribution SMS** pour ajouter une nouvelle liste de distribution SMS ou modifier les paramètres d'une liste de distribution SMS existante. |

| Configurer l'ID du moteur SNMP | Accédez à **Système** > **SNMP**. Dans **Paramètres**, sélectionnez **Configurer l'ID du moteur** et spécifiez l'ID du moteur. |

| Configuration du MIB SNMP | Accédez à **Système** > **SNMP** . Dans **Paramètres** , sélectionnez **Configurer la MIB SNMP** et entrez les détails de la MIB SNMP. |

| Configuration des pièges SNMP | Accédez à **Système** > **SNMP** > **Destinations d'interruptions** . Sous **Interruptions SNMP** , ajoutez une nouvelle destination d'interruption SNMP ou modifiez les paramètres d'une destination d'interruption SNMP existante. |

| Ajouter ou modifier un gestionnaire SNMP | Accédez à **Système** > **SNMP** > **Gestionnaires** . Sous **Gestionnaire SNMP** , ajoutez un nouveau gestionnaire SNMP ou modifiez les paramètres d'un gestionnaire SNMP existant. |

| Ajouter ou modifier un utilisateur SNMP | Accédez à **Système** > **SNMP** > **Utilisateurs** . Sous **Utilisateur SNMP** , ajoutez un nouvel utilisateur SNMP ou modifiez les paramètres d'un utilisateur SNMP existant. |

| Ajouter ou modifier des vues SNMP | Accédez à **Système** > **SNMP** > **Vues** . Sous **Affichage SNMP** , ajoutez une nouvelle vue SNMP ou modifiez les paramètres d'une vue SNMP existante. |

| Modifier les alarmes | Accédez à **Système** > **Alarmes** et sélectionnez l'alarme dont vous souhaitez modifier les paramètres. Les alarmes vous permettent de surveiller l'état de santé de votre serveur Citrix ADM. |

| Afficher le journal des tâches | Accédez à **Système** > **Diagnostics** > **Journaux des tâches** . Vous pouvez ensuite voir tous les journaux de tâches, avec des détails. Vous pouvez consulter des informations supplémentaires en sélectionnant un journal des tâches et en consultant son journal des périphériques, puis en consultant le journal des commandes du journal du périphérique sélectionné. |

| Générez le dossier de support technique | Accédez à **Système** > **Diagnostics** > **Support technique** . Sous **Support technique** , cliquez sur **Générer un fichier de support technique** pour générer une archive (fichier TAR) des données et statistiques Citrix ADM, que vous pouvez envoyer au support Citrix pour vous aider à résoudre un problème. |

| Configurer les paramètres de fuseau horaire des rapports sur le tableau | Accédez à **Système** > **Paramètres d'analyse** . Dans **Paramètres d'analyse** , sélectionnez **Configurer les paramètres** de fuseau horaire des rapports du tableau de bord pour définir votre heure locale ou votre fuseau GMT par défaut pour les rapports affichés sur votre tableau de bord. |

| Configurer le délai d'expiration de la session ICA | Accédez à **Système** > **Paramètres d'analyse** . Dans **Paramètres d'analyse** , sélectionnez **Configurer le délai d'expiration de la session** ICA et entrez la durée pendant laquelle une session ICA peut rester inactive avant d'être interrompue. |

| Configuration des fonctionnalités d'analyse | Accédez à **Système** > **Paramètres d'analyse** . Dans **Paramètres d'analyse** , sélectionnez **Configurer les fonctionnalités** pour activer les paramètres multi-sauts et les paramètres de seuil adaptatifs. Si vous cochez la case **Activer le multihop** , Citrix ADM collecte et met en corrélation les enregistrements AppFlow de toutes les appliances déployées avec plusieurs instances Citrix ADC entre un client et un serveur. Si vous cochez la case **Activer le seuil adaptatif** , un message Syslog est envoyé au serveur Syslog chaque fois que le nombre de visites sur une URL est supérieur à sa valeur de seuil. |

| Configuration des paramètres de base de données | Accédez à **Systeme** > **Paramètres d'analyse** . Dans **Paramètres d'analyse** , sélectionnez **Configurer les fonctionnalités** pour activer les paramètres d'index de base de données et les paramètres de nettoyage de base de données. En cochant la case **Activer l'indexation des bases de données**, vous pouvez faciliter l'interrogation efficace de la base de données Citrix ADM. Si vous cochez la case **Activer le nettoyage de la base de données**, une tentative de nettoyage de la base de données est répétée si une charge importante sur Citrix ADM empêche le nettoyage à l'heure prévue. |

| Configuration des paramètres de cache de base de données | Accédez à **Systeme** > **Paramètres d'analyse** . Sous **Paramètres d'analyse** , sélectionnez **Configurer les paramètres du cache** de base de données pour stocker localement le contenu de la base de données dans le cache, afin de pouvoir consulter ce contenu sans avoir besoin d'accéder au serveur de base de données. |

| Configuration des paramètres d'enregistrement de données | Dans **Paramètres d'analyse** , sélectionnez **Configurer les paramètres d'enregistrement de données** . Vous pouvez activer des fonctionnalités pour les paramètres suivants : paramètres du journal des enregistrements de données, paramètres de persistance de la durée des données, paramètres du rapport Web Insight, paramètres de collecte de données SLA Web Insight, paramètres de collecte de données URL Web Insight , paramètres des paramètres d'URL |

| Configurer la gestion des SLA pour des adresses IP Citrix ADC spécifiques | Accédez à **Systeme** > **Paramètres d'analyse** > **Gestion des SLA** . Dans la liste affichée, sélectionnez l'adresse IP Citrix ADC d'une appliance sur laquelle vous souhaitez gérer le SLA en termes de temps de réponse du serveur, d'accès par seconde et d'utilisation de la bande passante. |

| Configurer la durée de conservation des enregistrements de base de données pour chaque niveau de synthèse d'Insight | Accédez à **Systeme** > **Paramètres Analytics** > **Synthèse de la base** de données. Spécifiez la durée pendant laquelle vous souhaitez conserver les données Insight sur Citrix ADM. Vous pouvez choisir de stocker ces données toutes les heures, tous les jours ou une fois par minute. |

| Ajouter ou modifier des seuils adaptatifs | Accédez à **Systeme** > **Paramètres d'analyse** > **Seuils adaptatifs** . Sous **Seuils adaptatifs** , ajoutez un nouveau seuil adaptatif ou modifiez les paramètres d'un seuil adaptatif existant. La fonctionnalité de seuil adaptatif définit la valeur de seuil pour le nombre maximum de visites sur chaque URL. Si le nombre maximum de visites sur une URL est supérieur à la valeur seuil définie pour l'URL, un message Syslog est envoyé à un serveur Syslog externe. L'intervalle entre les valeurs de seuil peut être de jours ou de semaines. |

| Ajouter ou modifier un seuil et des alertes | Accédez à **Systeme** > **Paramètres Analytics** > **Seuils** . Sous **Seuils** , ajoutez une nouvelle limite ou modifiez les paramètres d'un seuil existant. Vous pouvez fournir des actions supplémentaires lors de la création ou de la modification d'un seuil, par exemple en l'activant, en envoyant des notifications par e-mail ou par SMS, ou en configurant une règle pour le seuil. |

| Téléchargez des fichiers de certificats SSL et des clés SSL | Accédez à **Systeme** > **Paramètres avancés** > **Fichiers de certificats SSL** . Sous **Fichiers de certificats SSL** , sélectionnez l'

onglet **Certificats SSL** pour télécharger un nouveau certificat SSL. De même, sous **Fichiers de certificats SSL**, sélectionnez l'onglet **Clés SSL** pour télécharger une nouvelle clé SSL. |

| Afficher ou modifier le (s) calendrier (s) d'exportation des rapports | Accédez à **Système** > **Paramètres avancés** > **Programmes d'exportation**. Vous pouvez ensuite voir tous les calendriers d'exportation, avec des détails. Vous pouvez modifier n'importe quel calendrier d'exportation dans la liste affichée ici. |

| Planifier l'exportation d'un rapport | Accédez à **Système** > **Paramètres avancés** > **Programmes d'exportation**. Pour ajouter un nouveau calendrier, cliquez sur le bouton à l'extrême droite, puis sélectionnez l'onglet **Exportation du calendrier**. Spécifiez les détails et cliquez sur **Planifier**. |

| Utilisez les fonctionnalités de sauvegarde et de restauration | Accédez à **Système** > **Paramètres avancés** > **Fichiers de sauvegarde** pour créer une sauvegarde des paramètres actuels du Citrix ADM. Vous pourrez utiliser ultérieurement ces fichiers sauvegardés pour restaurer le Citrix ADM à l'état dans lequel vous l'avez sauvegardé. Citrix recommande d'utiliser cette fonctionnalité avant d'effectuer une mise à niveau, et en général par mesure de précaution. |

| Installer un certificat SSL | Accédez à **Système** > **Administration système**. Dans **Configurer Citrix ADM**, sélectionnez **Installer le certificat SSL**. Vous pouvez sélectionner un fichier de certificat et un fichier de clé SSL qui se trouvent déjà sur l'appliance virtuelle Citrix ADM, ou vous pouvez télécharger les fichiers depuis votre ordinateur local. Vous devez saisir le mot de passe Citrix ADM dans le champ Mot de passe pour installer correctement le certificat SSL. |

| Informations d'identification rapides pour la connexion à l'instance | Accédez à **Système** > **Modifier les paramètres du système**. Activez les informations d'identification rapides **pour la connexion à l'instance** pour demander aux utilisateurs de saisir leurs informations d'identification d'instance lors de toute opération de configuration sur des instances Citrix ADC. |

| Activer la purge automatique des données | Accédez à **Système** > **Administration système**. Sous **Paramètres d'élégage**, sélectionnez Paramètres **d'élégage du système**. Cochez la case **Activer la purge automatique des données** pour permettre à Citrix ADM de purger les données lorsque l'utilisation du disque atteint la valeur seuil définie. Lorsque cette fonctionnalité est activée, Citrix ADM purge les données relatives aux événements, aux syslogs, aux rapports de performances et aux analyses jusqu'à ce que l'utilisation du disque soit inférieure à la valeur seuil définie. Cliquez sur l'icône Modifier pour modifier la valeur seuil d'utilisation du disque. |

|

## Configurer les paramètres de sauvegarde du système

February 1, 2024

Vous devez définir vos paramètres de sauvegarde système initiaux avant de devoir sauvegarder et

restaurer le système Citrix Application Delivery Management (ADM).

1. Accédez à **Système > Administration système**. Sous **Paramètres de sauvegarde**, cliquez sur **Paramètres de sauvegarde système**.
2. Dans la page **Configurer les paramètres de sauvegarde du système**, spécifiez les éléments suivants :
  - Nombre de sauvegardes à conserver. Vous ne pouvez conserver que 10 sauvegardes.
  - Chiffrez le fichier de sauvegarde.
  - Activez le transfert externe. Vous pouvez transférer une copie d'une copie de votre fichier de sauvegarde vers un autre système par mesure de précaution. Lorsque vous souhaitez restaurer la configuration, vous devez d'abord télécharger le fichier sur le serveur Citrix ADM, puis effectuer l'opération de restauration. Spécifiez le serveur, le nom d'utilisateur et le mot de passe, le port, le protocole de transfert à utiliser et le chemin d'accès au répertoire. Pour en savoir plus sur le transfert externe, consultez la section [Transférer un fichier de sauvegarde Citrix ADM vers un système externe](#).
3. Cliquez sur **OK**.

## ← Configure System Backup Settings

Previous backups to retain\*

Encrypt Backup File

Enable External Transfer

Backup happens everyday at 00:30.

**OK** Close

## Configurer un serveur NTP

February 1, 2024

Vous pouvez configurer un serveur NTP (Network Time Protocol) dans Citrix Application Delivery Management (ADM) pour synchroniser son horloge avec le serveur NTP. La configuration d'un serveur NTP

garantit que l'horloge Citrix ADM possède les mêmes paramètres de date et d'heure que les autres serveurs du réseau.

#### Pour configurer un serveur NTP sur Citrix ADM :

1. Accédez à **Système > Serveurs NTP**, puis cliquez sur **Ajouter**.
2. Dans la page **Créer un serveur NTP**, entrez les détails suivants :
  - **Nom du serveur/adresse IP** —Entrez le nom de domaine ou l'adresse IP du serveur NTP. Le nom ou l'adresse IP ne peuvent pas être modifiés après avoir ajouté le serveur NTP.
  - Intervalle **minimum d'interrogation** : spécifiez la valeur minimale de l'intervalle entre les messages NTP transmis, en secondes sous la forme d'une puissance de 2. Par exemple, si vous souhaitez que l'intervalle minimal 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.
  - **Préférez** —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**.

← | Create NTP Server

Server Name / IP Address\*  
Test NTP Server

Minimum Poll Interval  
6

Maximum Polling Interval  
11

Key Identifier  
1

Autokey  
 Preferred

Create Close



### Pour activer la synchronisation NTP sur Citrix ADM :

1. Accédez à **Système** > **Serveurs NTP**.
2. Cliquez sur **Synchronisation NTP** et **activez la case à cocher Activer la synchronisation NTP**.
3. Cliquez sur **OK**.



#### Remarque

Vous pouvez trouver les messages de journalisation NTP dans le répertoire `/var/log` dans le fichier `/var/log/ntpd.log` fichier.

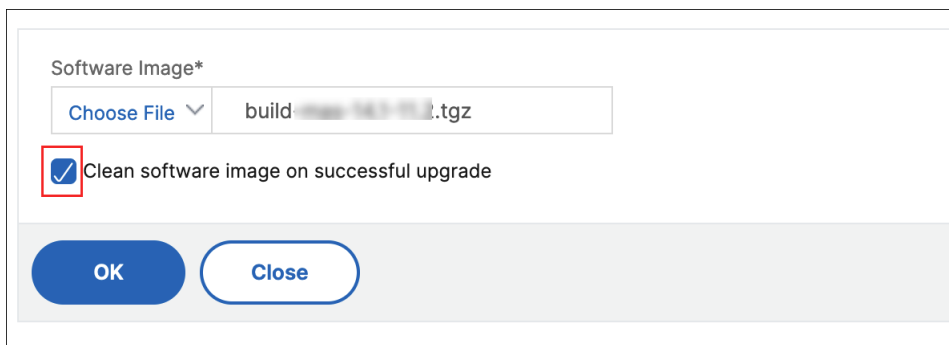
## Mettre à niveau Citrix ADM

February 1, 2024

Chaque version de Citrix Application Delivery Management (ADM) offre des fonctionnalités nouvelles et mises à jour avec des fonctionnalités améliorées. Une liste complète des améliorations est répertoriée dans les notes de mise à jour accompagnant l'annonce de publication. Prenez le temps de lire les notes de mise à jour avant de mettre à jour le logiciel. Il est important de comprendre le cadre de licences et les types de licences avant de commencer à mettre à niveau.

### Pour mettre à niveau Citrix ADM :

1. Accédez à **Système** > **Administrations système**. Sous le sous-titre **Administration système**, cliquez sur **Mettre à niveau Citrix ADM**.
2. Sur la page Mettre à niveau Citrix ADM, téléchargez un nouveau fichier image en sélectionnant **Local** (votre ordinateur local) ou **Appliance** (le fichier de certificat doit être présent sur l'appliance virtuelle Citrix ADM).  
Par défaut, l'image logicielle est nettoyée après une mise à niveau réussie.
3. Cliquez sur **OK**.



## Comment réinitialiser le mot de passe pour Citrix ADM

February 1, 2024

La procédure de réinitialisation du mot de passe pour Citrix ADM peut différer selon les hyperviseurs sur lesquels il est hébergé. Si vous avez modifié votre mot de passe par défaut et souhaitez rétablir le mot de passe par défaut, vous pouvez réinitialiser le mot de passe en redémarrant le nœud Citrix ADM.

### Citrix Hypervisor utilisant XenCenter :

1. Connectez-vous à Citrix Hypervisor à l'aide de XenCenter.
2. Sélectionnez le nœud Citrix ADM, cliquez avec le bouton droit de la souris et sélectionnez **Redémarrer**.
3. Sous l'onglet **Console**, appuyez sur **CTL + C** pour interrompre la séquence de démarrage.

```

iPXE (http://ipxe.org) 00:04.0 C900 PCI2.10 PMM+00100010+00111020 C900
Press F12 for boot menu.
Boot device: CD-Rom - failure: could not read boot disk
Boot device: Hard Disk - success.
BTX loader 1.00 BTX version is 1.02
Consoles: internal video/keyboard
BIOS drive C: is disk0
BIOS 632kB/3931136kB available memory

FreeBSD/x86 bootstrap loader, Revision NS1.2
Loading /boot/defaults/loader.conf
/mas-12.1-50.28 text=0x9aac71 data=0x1cf79e30+0x4db1d0 syms=[0x8+0xc59a0+0x8+0xb
74211
Press [Ctrl-C] for command prompt, or any other key to boot immediately.
booting [/mas-12.1-50.28] in 2 seconds...
    
```

4. Exécutez la commande **boot -s** à l'invite OK.

```

iPXE (http://ipxe.org) 00:04.0 C900 PCI2.10 PMM+00100010+00111020 C900
Press F12 for boot menu.

Boot device: CD-Rom - failure: could not read boot disk
Boot device: Hard Disk - success.

BTX loader 1.00  BTX version is 1.02
Consoles: internal video/keyboard
BIOS drive C: is disk0
BIOS 632kB/3931136kB available memory

FreeBSD/x86 bootstrap loader, Revision NS1.2
Loading /boot/defaults/loader.conf
/mas-12.1-50.28 text=0x9aac71 data=0x1cf79e30+0x4db1d0 syms=[0x8+0xc59a0+0x8+0xb
7421]
\
Press [Ctrl-C] for command prompt, or any other key to boot immediately.
Booting [/mas-12.1-50.28] in 1 second...

Type '?' for a list of commands, 'help' for more detailed help.
OK_

```

Citrix ADM redémarre et affiche le message suivant :

```

talk_to_backend: xn_num_q 1 max_q 16 err 0
xn0: backend features:xbd0: 122880MB <Virtual Block Device> at device/vbd/768 on
xenbus_front0
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: usb0
uhub0: 2 ports with 2 removable, self powered
Root mount waiting for: usb0
ugen0.2: <QEMU 0.10.2> at usb0
ums0: <Endpoint1 Interrupt Pipe> on usb0
ums0: 3 buttons and [Z] coordinates ID=0
Trying to mount root from ufs:/dev/md0c
NS-KERN /dev/md0 for compatibilitu
Enter full pathname of shell or RETURN for /bin/sh: █

```

5. Appuyez sur **Entrée** pour obtenir l'invite /u@.

```

xn0: backend features:xbd0: 122880MB <Virtual Block Device> at device/vbd/768 on
xenbusb_front0
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: usb0
uhub0: 2 ports with 2 removable, self powered
Root mount waiting for: usb0
ugen0.2: <QEMU 0.10.2> at usb0
ums0: <Endpoint1 Interrupt Pipe> on usb0
ums0: 3 buttons and [Z] coordinates ID=0
Trying to mount root from ufs:/dev/md0c
NS-KERN /dev/md0 for compatibility
Enter full pathname of shell or RETURN for /bin/sh:
\nu@

```

6. Montez la partition flash à l'aide de la commande suivante :

```
mount dev/ad0s1a /flash
```

```

xenbusb_front0
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: usb0
uhub0: 2 ports with 2 removable, self powered
Root mount waiting for: usb0
ugen0.2: <QEMU 0.10.2> at usb0
ums0: <Endpoint1 Interrupt Pipe> on usb0
ums0: 3 buttons and [Z] coordinates ID=0
Trying to mount root from ufs:/dev/md0c
NS-KERN /dev/md0 for compatibility
Enter full pathname of shell or RETURN for /bin/sh:
\nu@mount dev/ad0s1a /flash
\nu@

```

7. Delete /flash/mpsconfig/master.passwd  
 8. Delete rm -rf /etc/passwd  
 9. Créez un fichier à l'aide de la commande suivante :

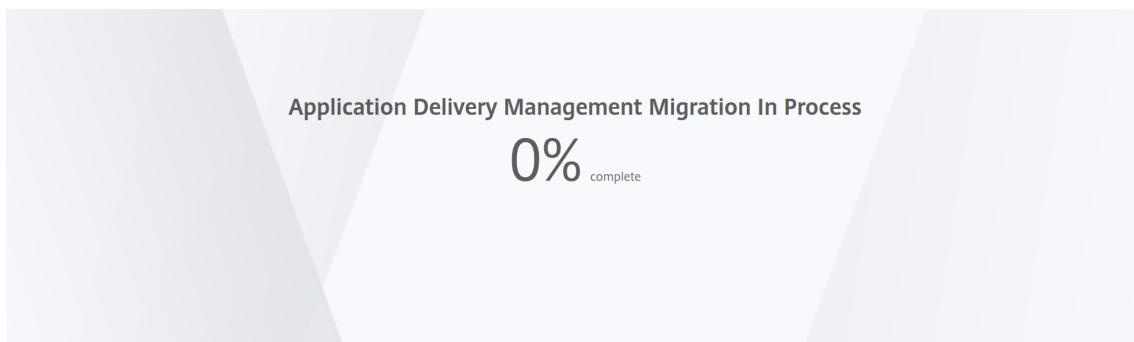
```
touch /flash/mpsconfig/.recover
```

Le mot de passe est maintenant réinitialisé au mot de passe par défaut.

10. Exécutez la commande **Reboot** pour redémarrer Citrix ADM.

```
xbd0: attaching as ad0
SMP: AP CPU #4 Launched!
SMP: AP CPU #5 Launched!
SMP: AP CPU #3 Launched!
SMP: AP CPU #1 Launched!
SMP: AP CPU #6 Launched!
SMP: AP CPU #2 Launched!
SMP: AP CPU #7 Launched!
vmbus_vec: 48
UM uuid: /vm/ad003cd0-2774-eac7-b10d-afb9fbf73321
UUID hex: ad003cd02774eac7b10dafb9fbf73321
GEOM: ad0s1: geometry does not match label (16h,63s != 255h,63s) (proceeding anyway)
Root mount waiting for: usb0
uhub0: 2 ports with 2 removable, self powered
Root mount waiting for: usb0
ugen0.2: <QEMU 0.10.2> at usb0
ums0: <Endpoint1 Interrupt Pipe> on usb0
ums0: 3 buttons and [Z] coordinates ID=0
Trying to mount root from ufs:/dev/md0c
NS-KERN /dev/md0 for compatibility
Enter full pathname of shell or RETURN for /bin/sh:
\nu@mount dev/ad0s1a /flash
\nu@touch /flash/mpsconfig/.recover
\nu@reboot
```

11. Accédez à l'interface graphique Citrix ADM et attendez que le redémarrage soit terminé.



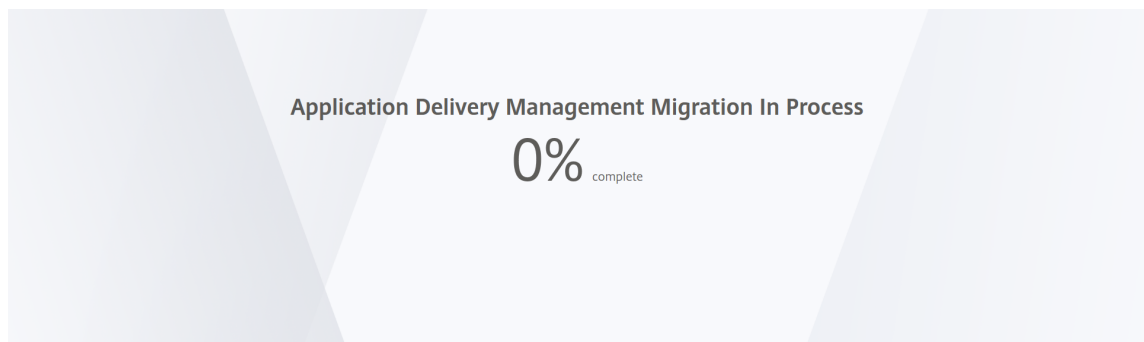
Vous pouvez maintenant utiliser les informations d'identification *nsroot/nsroot* pour ouvrir une session à partir de l'interface graphique et *nsrecover/nsroot* pour ouvrir une session à partir de l'Hypervisor.

**Esx utilisant vSphere :**

1. Connectez-vous à ESX à l'aide de vSphere.
2. Sélectionnez le nœud Citrix ADM, cliquez avec le bouton droit, puis sélectionnez **Redémarrer**.
3. Sous l'onglet **Console**, appuyez sur **CTL +C** pour interrompre la séquence de démarrage.

```
iPXE (http://ipxe.org) 00:04.0 C900 PCI2.10 PMM+00100010+00111020 C900
Press F12 for boot menu.
Boot device: CD-Rom - failure: could not read boot disk
Boot device: Hard Disk - success.
BTX loader 1.00 BTX version is 1.02
Consoles: internal video/keyboard
BIOS drive C: is disk0
BIOS 632kB/3931136kB available memory
FreeBSD/x86 bootstrap loader, Revision NS1.2
Loading /boot/defaults/loader.conf
/mas-12.1-50.28 text=0x9aac71 data=0x1cf79e30+0x4db1d0 syms=[0x8+0xc59a0+0x8+0xb
7421]
Press [Ctrl-C] for command prompt, or any other key to boot immediately.
booting [/mas-12.1-50.28] in 2 seconds...
```

4. Exécutez la commande **boot -s** dans l'invite OK.  
Le Citrix ADM redémarre.
5. Appuyez sur **Entrée** pour obtenir l'invite /u@.
6. Montez la partition flash à l'aide de la commande suivante :  
`mount dev/da0s1a /flash`
7. `Delete /flash/mpsconfig/master.passwd`
8. `Delete rm -rf /etc/passwd`
9. 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.
10. Exécutez la commande **Reboot** pour redémarrer Citrix ADM.
11. Accédez à l'interface graphique Citrix ADM et attendez que le redémarrage soit terminé.



Vous pouvez désormais utiliser les informations d'identification *nsroot/nsroot* pour ouvrir une

session à partir de l'interface graphique et *nsrecover/nsroot* pour ouvrir une session à partir du serveur ESX.

### Hyper-V utilisant le gestionnaire Hyper-V :

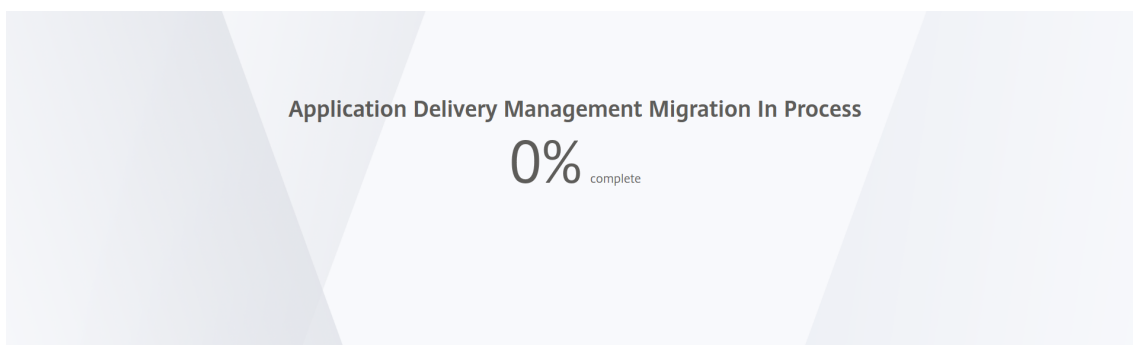
1. Connectez-vous à Hyper-V à l'aide du gestionnaire Hyper-V.
2. Sélectionnez le nœud Citrix ADM, cliquez avec le bouton droit, puis sélectionnez **Redémarrer**.
3. Sous l'onglet **Console**, appuyez sur **CTL +C** pour interrompre la séquence de démarrage.

```
IPXE (http://ipxe.org) 00:04.0 C900 PCI2.10 PMM+00100010+00111020 C900
Press F12 for boot menu.
Boot device: CD-Rom - failure: could not read boot disk
Boot device: Hard Disk - success.
BTX loader 1.00 BTX version is 1.02
Consoles: internal video/keyboard
BIOS drive C: is disk0
BIOS 632kB/3931136kB available memory

FreeBSD/x86 bootstrap loader, Revision NS1.2
Loading /boot/defaults/loader.conf
/mas-12.1-50.28 text=0x9aac71 data=0x1cf79e30+0x4db1d0 syms=[0x8+0xc59a0+0x8+0xb
7421]

Press [Ctrl-C] for command prompt, or any other key to boot immediately.
booting [/mas-12.1-50.28] in 2 seconds...
```

4. Exécutez la commande **boot -s** à l'invite OK.  
Le Citrix ADM redémarre.
5. Appuyez sur **Entrée** pour obtenir l'invite /u@.
6. Montez la partition flash à l'aide de la commande suivante :  
`mount dev/ad0s1a /flash`
7. `Delete /flash/mpsconfig/master.passwd`
8. `Delete rm -rf /etc/passwd`
9. 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.
10. Exécutez la commande **Reboot** pour redémarrer Citrix ADM.
11. Accédez à l'interface graphique Citrix ADM et attendez que le redémarrage soit terminé.



Vous pouvez maintenant utiliser les informations d'identification *nsroot/nsroot* pour ouvrir une session à partir de l'interface graphique et *nsrecover/nsroot* pour ouvrir une session à partir du gestionnaire hyper-v.

**Serveur KVM Linux (SSH to KVM Server à l'aide de n'importe quel client SSH) :**

1. Connectez-vous à Citrix ADM à l'aide d'un client SSH sur le serveur KVM.
2. Redémarrez Citrix ADM.
3. Appuyez sur **CTL + C** pour interrompre la séquence de démarrage peu après l'affichage du message **Loading /boot/defaults/loader.conf**.
4. À l'invite OK, exécutez la commande suivante :  

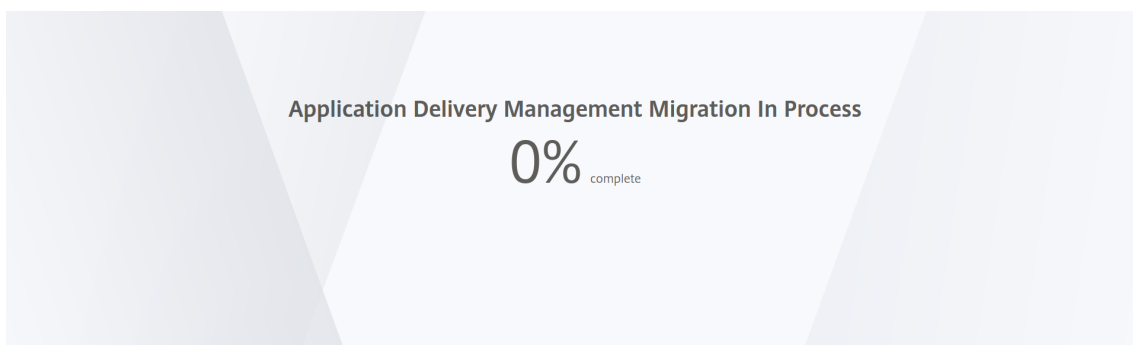
```
set console='comconsole,vidconsole'
```
5. Exécutez la commande **boot -s** pour redémarrer Citrix ADM.
6. Une fois que le message **Enter full path of shell ou RETURN for /bin/sh :** s'affiche, appuyez sur **Entrée** pour obtenir l'invite `/u@`.
7. Montez la partition flash à l'aide de la commande suivante :  

```
mount dev/vtbd0s1a /flash
```
8. `Delete /flash/mpsconfig/master.passwd`
9. `Delete rm -rf /etc/passwd`
10. 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.
11. Exécutez la commande **Reboot** pour redémarrer Citrix ADM.
12. Accédez à l'interface graphique Citrix ADM et attendez que le redémarrage soit terminé.





Vous pouvez désormais utiliser les informations d'identification *nsroot/nsroot* pour ouvrir une session à partir de l'interface graphique et *nsrecover/nsroot* pour ouvrir une session à partir de la console SSH.

## Configurer l'intervalle de purge de syslog

February 1, 2024

Syslog est un protocole standard de journalisation. Il comprend deux composants : le module d'audit Syslog, qui s'exécute sur l'instance Citrix Application Delivery Controller (ADC), et le serveur Syslog, qui peut s'exécuter soit sur le système d'exploitation FreeBSD sous-jacent de l'instance Citrix ADC, soit sur un système distant. SYSLOG utilise User Datagram Protocol (UDP) pour le transfert de données.

Syslog permet d'isoler le système qui génère les informations et le système qui stocke les informations. Vous pouvez consolider les informations de journalisation et obtenir des informations à partir des données collectées. Vous pouvez également configurer syslog pour consigner différents types d'événements.

Pour limiter la quantité de données syslog stockées dans la base de données, vous pouvez spécifier l'intervalle suivant lequel vous souhaitez purger les données syslog. Vous pouvez spécifier le nombre de jours après lesquels les données syslog suivantes seront supprimées de Citrix Application Delivery Management (ADM) :

- Données Syslog génériques
- Données AppFirewall
- Données Citrix Gateway

Vous pouvez également configurer l'intervalle de purge de Citrix Gateway par type de syslog. Cet intervalle de purge a priorité sur l'intervalle de purge configuré pour conserver les données Citrix Gateway.

**Pour configurer les paramètres d'intervalle de purge Syslog pour Citrix ADM, procédez comme suit :**

1. Accédez à **Système > Administration système**. Sous **Paramètres d'élagage**, cliquez sur **Paramètres d'élagage de l'instance Syslog**.
2. Dans la page **Configurer les paramètres de purge Syslog de l'instance**, spécifiez **Conserver les données génériques Syslog**. Tapez le nombre de jours pendant lesquels Citrix ADM conserve les messages syslog génériques.

## ← Configure Instance Syslog Prune Settings

You can specify the number of days after which the following syslog data will be deleted from the Citrix ADM server.

Retain Syslog Generic Data\*

 ?

OK

Close

## Configurer les paramètres de nettoyage du système

February 1, 2024

Pour limiter la quantité de données de reporting stockées dans la base de données de votre logiciel Citrix Application Delivery Management (ADM), vous pouvez la nettoyer. Vous pouvez spécifier l'intervalle pendant lequel Citrix ADM conserve les données de reporting réseau, les événements, les journaux d'audit et les journaux de tâches. Par défaut, ces données sont nettoyées toutes les 24 heures (à 00.00 heures).

### Remarque

La valeur que vous spécifiez ne peut pas dépasser 30 jours ou être inférieure à 15 jours.

**Pour configurer les paramètres de nettoyage du système pour les rapports de performances à l'aide de Citrix ADM :**

1. Accédez à **Système > Administration système**. Sous **Paramètres d'élagage**, cliquez sur **Paramètres d'élagage du système**.
2. Dans la page **Configurer les paramètres de nettoyage du système**, spécifiez le nombre de jours pendant lesquels les données doivent être conservées, puis cliquez sur **OK**.

Configure System Prune Settings

Data to keep (days)\*  
15 ⓘ

Pruning happens every day at 00:00

Auto Prune Details:

Enable Automatic Data Prune

Pruning starts when any one of the criteria is met – data prune threshold value or data to keep (days). Whichever is met first, takes precedence over the other.

Data Prune Threshold Value (%)  
80

Save

Vous pouvez activer la purge automatique en cochant la case **Activer la purge automatique des données** . Une alarme est déclenchée lorsque l'utilisation du disque dépasse la **valeur de seuil de purge des données configurée** .

Vous pouvez configurer et activer l'alarme **DiskUtilizationHigh** (par défaut) et spécifier les éléments suivants :

- **Gravité**, telle que Critique.
- **Seuil d'alarme**. Entrez la valeur pour laquelle la gravité de l'événement est calculée.
- **Heure**. Durée (en minutes) après laquelle vous voulez déclencher l'alarme.

## Configure Alarm

Alarm Name  
diskUtilizationHigh

Enable Alarm

Severity  
Critical

Alarm Threshold  
80

Time (minutes)  
5

## Activer l'accès shell pour les utilisateurs non par défaut

February 1, 2024

Vous pouvez activer l'accès shell pour les utilisateurs autres que par défaut dans Citrix Application Delivery Management (ADM). Vous pouvez utiliser cette fonctionnalité pour activer et configurer le mode de communication avec les instances.

### Remarque

Par défaut, l'accès shell est désactivé pour les utilisateurs autres que par défaut.

### Pour activer l'accès shell pour les utilisateurs autres que par défaut dans Citrix ADM :

1. Dans Citrix ADM, accédez à **Système > Administration système**.

2. Dans **Paramètres système**, cliquez sur **Modifier les paramètres système**.
3. Sur la page **Modifier les paramètres système**, configurez les paramètres suivants :
  - **Communication avec les instances** : sélectionnez le protocole de communication.
  - **Accès sécurisé** : activez l'accès sécurisé pour Citrix ADM.
  - **Activer le délai d'expiration de la session** : spécifiez la période pendant laquelle vous souhaitez conserver une session inactive.
  - **Autoriser l'authentification de base** - Autoriser le service de gestion à accepter les informations d'identification fournies à l'aide du protocole d'authentification de base.
  - **Activer la connexion nsrecover** - Activer la connexion nsrecover sur Management Service.
  - **Activer le téléchargement de certificats** : vous permet de télécharger des certificats à partir de l'Citrix ADC ajouté.
  - **Activer l'accès à l'environnement de ligne de commande pour un utilisateur non nsroot** - Activer l'accès à l'environnement de ligne de commande pour les utilisateurs autres que par défaut dans Citrix ADM.
  - **Demander les informations d'identification utilisateur pour la connexion à l'instance** - Autoriser les utilisateurs à entrer leurs informations d'identification utilisateur lors de la connexion à des instances à partir de Citrix ADM.
4. Cliquez sur **OK**.

## Récupérer des serveurs Citrix ADM inaccessibles

February 1, 2024

Citrix Application Delivery Management (ADM) fournit désormais un outil de maintenance de base de données pour effectuer le nettoyage de la base de données système. Vous pouvez maintenant lancer l'outil utilitaire Citrix ADM pour vous connecter au système de fichiers, supprimer quelques composants et rendre la base de données accessible. Le script de récupération Citrix ADM est un outil qui aide à récupérer de l'espace dans le système de fichiers en effaçant les tables et fichiers de base de données anciens ou inutilisés. L'outil vous aide à parcourir les tables et les fichiers de la base de données par étapes successives et affiche l'espace occupé sur le système de fichiers par les éléments respectifs. Une fois que vous avez sélectionné les tables de base de données et les fichiers à supprimer, l'outil les supprime du système de fichiers après confirmation.

## Comment faire pour utiliser le script de récupération de base de données Citrix ADM pour un déploiement autonome Citrix ADM

Utilisez la procédure suivante dans un déploiement Citrix ADM serveur unique pour vous connecter au système de fichiers, supprimer quelques composants et rendre la base de données accessible, puis effectuer les opérations de restauration.

1. À l'aide d'un client SSH ou de la console de votre hyperviseur, connectez-vous à Citrix ADM et saisissez la commande suivante :

```
Last login: Fri Nov 30 09:51:19 2018 from 10.252.241.100
Have a nice daybash-3.2# /mps/mas_recovery/mas_recovery.py
```

2. Lorsque l'écran affiche un message d'avertissement pour arrêter quelques processus Citrix ADM, tapez « y » et appuyez sur la touche **Entrée**.

L'écran suivant apparaît alors que le système détermine les composants de la base de données que vous pouvez supprimer sans affecter les fichiers principaux du système.

```
-----
***** Citrix ADM Cleanup Utility *****
-----

This utility helps you gain disk space by performing cleanup.

Checking whether DB is accessible...

DB is accessible.

Please wait. Gathering data. This will take some time.

<----->
```

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.

```

----- SUMMARY -----
      DB component                Current size
      -----
Analytics ----- 184.58 MB
Perf Reports ----- 43.73 MB
App Summary ----- 12.03 MB
App Health Summary ----- 6.33 MB
App Counter Data ----- 5.30 MB
Device Syslogs ----- 56.00 KB
Device Events ----- 40.00 KB

      Filesystem component        Current size
      -----
Citrix ADM Images ----- 15.51 GB
Core Files ----- 718.37 MB
Citrix ADC Images ----- 453.32 MB
Techsupport Bundles ----- 439.35 MB
Device Backup ----- 131.79 MB
Citrix ADM Backup ----- 35.21 KB
Citrix ADC VPX ESXi Images ----- 0.00 B
Citrix ADC SDX Images ----- 0.00 B
Citrix ADC CPX images ----- 0.00 B

-----

Do you wish to proceed with cleanup?
[y/n]: 

```

4. Vous pouvez sélectionner le composant de base de données spécifique qui doit être nettoyé et saisir le numéro correspondant. Appuyez sur la touche **Entrée**.

Par exemple, pour effectuer le nettoyage du catalogue système, sélectionnez l'option 8 dans le menu de sélection des **composants DB** et tapez « y », puis appuyez sur la touche **Entrée** pour poursuivre le nettoyage du catalogue système.

**Remarque**

Citrix ADM inclut des tables utilisateur appelées catalogue système. Le catalogue système est un emplacement dans la base de données Citrix ADM où un système de gestion de base de données relationnelle stocke les métadonnées de schéma, telles que des informations sur les tables et les colonnes et les enregistrements internes. Les tables du catalogue système sont comme des tables régulières qui peuvent accumuler des lignes gonflées et mortes au fil du temps et, par conséquent, nécessitent un nettoyage périodique pour des performances optimales. C'est une bonne pratique de tenir régulièrement ces tableaux. L'activité libère non seulement de l'espace disque, mais améliore également les performances globales de la base de données et, par conséquent, de l'Citrix ADM.

```

***** Citrix ADM Cleanup Utility *****
-----
                                DB components
                                -----

Enter the number corresponding to the menu entry.
You can input multiple space separated numbers.
E.g. '1 2 4' will select entries numbered 1, 2, and 4.

[0] Go back and start again
[1] Analytics ----- 184.58 MB
[2] Perf Reports ----- 41.84 MB
[3] App Summary ----- 11.84 MB
[4] App Health Summary ----- 6.09 MB
[5] App Counter Data ----- 5.09 MB
[6] Device Syslogs ----- 56.00 KB
[7] Device Events ----- 40.00 KB
[8] Clean System Catalog
[9] Select all
[10] Continue without selecting

Your input: 8
Are you sure you want to CLEAN SYSTEM CATALOG tables?

[y/n]: y
    
```

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 ».



```

***** Citrix ADM Cleanup Utility *****
-----
                        Filesystem components
                        -----

Enter the number corresponding to the menu entry.
You can input multiple space separated numbers.
E.g. '1 2 4' will select entries numbered 1, 2, and 4.

[0] Go back and start again
[1] Citrix ADM Images ----- 15.51 GB
[2] Core Files ----- 718.37 MB
[3] Citrix ADC Images ----- 453.32 MB
[4] Techsupport Bundles ----- 439.35 MB
[5] Device Backup ----- 131.79 MB
[6] Citrix ADM Backup ----- 35.21 KB
[7] Citrix ADC VPX ESXi Images 0.00 B
[8] Citrix ADC SDX Images --- 0.00 B
[9] Citrix ADC CPX images --- 0.00 B
[10] Select all
[11] Continue without selecting

Your input: 11
    
```

5. Tapez « y » et appuyez à nouveau sur la touche **Entrée** sur l'écran de confirmation final.

```

***** Citrix ADM Cleanup Utility *****
-----
                        FINAL CONFIRMATION

                        These components will be cleaned.

                        DB components
                        -----

                        >> System Catalog

No data has been deleted yet.

If you choose to proceed, all ADM processes will be stopped
for the remainder of the cleanup.

Do you wish to proceed with cleanup?
[y/n]:
    
```

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.

```

-----
***** Citrix ADM Cleanup Utility *****
-----
                          SUMMARY
-----
                          DB components
                          -----
Component name           Present size           Size cleared
-----
System Catalog ----- 189.15 MB ----- 0.00 B
Cleanup complete.
Note that even empty tables in DB may appear to occupy some
space, this is expected.

To prevent potential unpredictable behavior, we STRONGLY recommend
rebooting the ADM now.

Do you want to REBOOT the ADM?
[y/n]: 

```

6. Tapez « y » et appuyez sur la touche **Entrée** pour redémarrer Citrix ADM.

Assurez-vous de redémarrer Citrix ADM après le nettoyage du système. Attendez environ 30 minutes pour que les opérations de base de données internes se terminent après le redémarrage de Citrix ADM. Vous devez ensuite pouvoir vous connecter à la base de données Citrix ADM. Si ce n'est pas le cas, exécutez à nouveau le script de récupération pour libérer plus d'espace. Lorsque Citrix ADM est opérationnel, il doit fonctionner comme prévu.

#### Remarque

La taille actuelle de la table de catalogue système n'est jamais égale à zéro après le nettoyage. En effet, seules les lignes vides sont supprimées de la table et la table peut avoir des entrées valides même après leur nettoyage.

## Comment faire pour utiliser le script de récupération de base de données Citrix ADM pour un déploiement haute disponibilité Citrix ADM

Le système de base de données pour les serveurs Citrix ADM dans un déploiement à haute disponibilité est en mode de synchronisation continue. Lors de l'utilisation du nouvel outil de récupération de base de données, vous n'avez pas besoin de répliquer la procédure sur les deux serveurs Citrix ADM.

1. À l'aide d'un client SSH ou d'une console d'hyperviseur, connectez-vous au nœud principal.
2. Exécutez la commande suivante :

```
/mps/mas_recovery/mas_recovery.py
```

3. Suivez la procédure de l'étape 2 disponible pour le script de récupération de déploiement autonome Citrix ADM

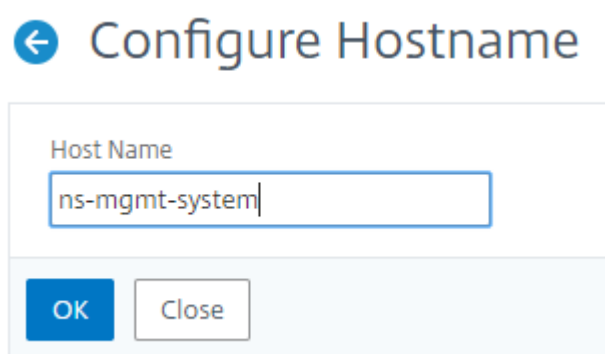
## Attribuer un nom d'hôte à un serveur Citrix ADM

February 1, 2024

Pour identifier un serveur Citrix Application Delivery Management (ADM), vous pouvez lui attribuer un nom d'hôte. Le nom d'hôte s'affiche sur la licence universelle pour Citrix ADM.

### Pour attribuer un nom d'hôte à un serveur Citrix ADM :

1. Dans Citrix ADM, accédez à **Système > Administration système**.
2. Sous **Paramètres système**, cliquez sur **Modifier le nom d'hôte**.
3. Dans la page **Configurer le nom d'hôte**, entrez un nom d'hôte et cliquez sur **OK**.



← Configure Hostname

Host Name

ns-mgmt-system

OK Close

## Sauvegarder et restaurer votre serveur Citrix ADM

February 1, 2024

Vous pouvez effectuer des sauvegardes périodiques de votre serveur Citrix ADM. Vous pouvez sauvegarder et restaurer les fichiers de configuration, les détails de l'instance, les données système, etc. Avant de procéder à la mise à niveau, sauvegardez les fichiers de configuration du serveur ADM pour des raisons de précaution.

La sauvegarde comprend les composants suivants :

- Fichiers de configuration Citrix ADM :
  - SNMP
  - Fichiers de configuration du serveur Syslog
  - Fichiers NTP

- Certificats SSL
- Fichiers du Centre de contrôle
- Sauvegardes des instances Citrix ADC gérées par le serveur Citrix ADM.
- Modèles d'audit de configuration.
- Données système stockées dans la base de données :
  - Liste des locataires et des utilisateurs créée.
  - Configuration du serveur d'authentification externe (LDAP, RADIUS, etc.).
  - Tâches de configuration et modèles de tâches créés.
- Données d'infrastructure et d'application stockées dans la base de données :
  - Données provenant d'instances Citrix ADC ajoutées et gérées.
  - Détails du profil d'instance, détails de version, détails du groupe d'instances, etc.
  - Application statique (groupe de serveurs virtuels) créée par l'administrateur.
- Paramètres SNMP.

**Remarque** Les données, les événements et les messages syslog Analytics sont exclus de la sauvegarde.

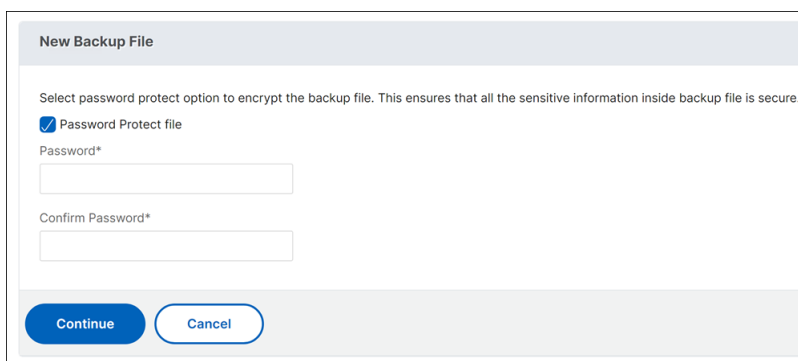
## Sauvegardez la configuration Citrix ADM

Par défaut, le serveur Citrix ADM sauvegarde la configuration toutes les 24 heures (à 00,30 heures). Vous pouvez également planifier et sélectionner l'heure de la sauvegarde. Vous pouvez également déplacer une copie du fichier sauvegardé vers un autre système.

La sauvegarde est stockée sous forme de fichier TAR compressé qui peut également être crypté. Par défaut, trois fichiers de sauvegarde sont conservés dans le serveur. Pour éviter tout problème d'espace disque faible, vous pouvez stocker un maximum de 10 fichiers de sauvegarde sur votre serveur Citrix ADM. Toutefois, Citrix vous recommande de stocker certaines copies de vos fichiers de sauvegarde sur le serveur ou de transférer les fichiers vers un autre système par mesure de précaution.

### Pour sauvegarder une configuration Citrix ADM :

1. Accédez à **Système > Paramètres avancés > 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.



### Remarque

Vous pouvez également définir un fichier de sauvegarde pour le chiffrement en accédant à **Système > Paramètres de sauvegarde du système**, puis en sélectionnant **Chiffrer le fichier de sauvegarde**.

## Transférer un fichier de sauvegarde Citrix ADM vers un système externe

Vous pouvez transférer une copie du fichier de sauvegarde vers un autre système par mesure de précaution. Lorsque vous souhaitez restaurer la configuration, téléchargez d'abord le fichier sur le serveur Citrix ADM, puis effectuez l'opération de restauration.

### Pour transférer un fichier de sauvegarde Citrix ADM :

1. Accédez à **Système > Paramètres avancés > 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.

Vous pouvez également définir les détails des systèmes externes en accédant à **Système > Paramètres de sauvegarde du système**.

4. Vous pouvez supprimer le fichier de sauvegarde de Citrix ADM après le transfert en cochant la case **Supprimer le fichier de Application Delivery Management après le transfert**.
5. Cliquez sur **OK** pour effectuer le transfert.

#### Remarque

Pour enregistrer une copie du fichier de sauvegarde dans votre système local, accédez à **Système > Paramètres avancés > Fichiers de sauvegarde**, sélectionnez le fichier à copier, puis cliquez sur **Télécharger**.

## Restaurer la configuration Citrix ADM à partir d'un fichier de sauvegarde

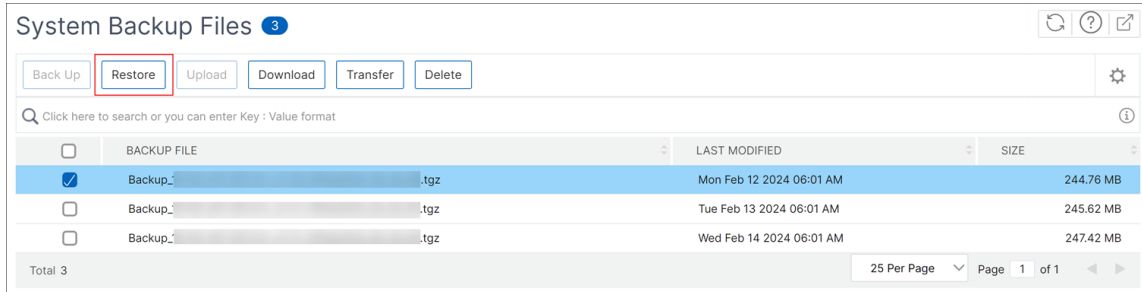
Lorsque vous restaurez la configuration Citrix ADM à partir d'un fichier précédemment sauvegardé, l'opération de restauration efface le fichier de sauvegarde, puis restaure la configuration. L'opération de restauration supprime la configuration existante et la remplace par la configuration du fichier de sauvegarde.

#### Remarque

L'opération de restauration échoue si le fichier de sauvegarde est renommé ou si le contenu du fichier de sauvegarde est modifié.

**Pour restaurer une configuration Citrix ADM à partir d'un fichier de sauvegarde :**

1. Accédez à **Système** > **Paramètres avancés** > **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 charger le fichier, accédez à **Système** > **Paramètres avancés** > **Fichiers de sauvegarde**, puis cliquez sur **Télécharger**.

## Afficher les informations d'audit

January 23, 2024

Syslog est un protocole standard de journalisation. Il comprend deux composants : le module d'audit Syslog, qui s'exécute sur l'instance Citrix Application Delivery Controller (ADC), et le serveur Syslog, qui peut s'exécuter soit sur le système d'exploitation FreeBSD sous-jacent de l'instance Citrix ADC, soit sur un système distant. SYSLOG utilise User Datagram Protocol (UDP) pour le transfert de données.

Syslog permet d'isoler le système qui génère les informations et le système qui stocke les informations. Vous pouvez consolider les informations de journalisation et obtenir des informations à partir des données collectées. Vous pouvez également configurer syslog pour consigner différents types d'événements.

Vous pouvez surveiller les messages Syslog générés par un périphérique Citrix ADC si vous configurez l'appareil pour rediriger les messages Syslog vers Citrix Application Delivery Management (ADM). Vous pouvez planifier une tâche pour créer des serveurs Syslog qui génèrent différents types de données Syslog à l'aide de la fonctionnalité de modèles intégrés de Citrix ADM.

Tout d'abord, configurez un serveur syslog vers lequel l'instance peut envoyer des informations de journal. Ensuite, spécifiez le format de date et d'heure pour l'enregistrement des messages du journal.

### **Pour configurer un serveur Syslog sur Citrix ADM :**

1. Accédez à **Système > Audit**. Sous **Résumé de la configuration**, sélectionnez **Serveurs Syslog**. Vous pouvez également accéder à **Système > Audit > Serveurs Syslog**.
2. **Sur la page** Serveur Syslog, **cliquez sur Ajouter**.
3. Dans la page **Créer un serveur Syslog**, entrez les valeurs suivantes :
  - **Nom** : nom du serveur Syslog.
  - **Adresse IP** : adresse IP du serveur Syslog.
  - **Port** : port du serveur Syslog.
4. Choisissez les niveaux de journalisation (Tous, Aucun ou Personnalisé). En conséquence, sélectionnez les niveaux de gravité.
5. Cliquez sur **Créer**.

### **Pour configurer le format de date et d'heure Syslog sur Citrix ADM, procédez comme suit :**

1. Accédez à **Système > Audit**. Dans **Résumé de la configuration**, sélectionnez **Serveurs Syslog**.
2. Dans la page **Serveur Syslog**, sélectionnez un serveur syslog, puis cliquez sur **Paramètres Syslog**.
3. Dans la page **Configurer les paramètres Syslog**, spécifiez le format de date et d'heure.
4. Cliquez sur **OK**.

### **Pour afficher les messages Syslog sur Citrix ADM :**

Vous pouvez désormais consulter tous vos messages Syslog générés sur vos instances Citrix ADC gérées si vous avez configuré votre instance pour rediriger les messages Syslog vers le serveur Citrix ADM. Les messages Syslog sont stockés de manière centralisée dans la base de données du serveur Citrix ADM et seront disponibles sur le Syslog Viewer à des fins d'audit. Vous pouvez consolider ces informations de journalisation et dériver des rapports analytiques à partir des données collectées.

Vous pouvez filtrer ces informations par module, type d'événement et gravité. Vous pouvez également configurer syslog pour consigner différents types d'événements.

Pour afficher le **visualiseur Syslog**, accédez à **Système > Audit**. Sur la page **Audit**, sous **Messages d'audit**, sélectionnez **Messages Syslog**. Choisissez les filtres appropriés pour afficher les messages du journal de votre système.



## Syslog Messages

Syslog Viewer (4 results)
Sort: Newest first ↕
🔄

Go
⋮

Dec 03 2018 11:21:13 <span style="background-color: #007bff; color: white; padding: 2px;">Info</span>	GUI: CMD_EXECUTED: User nsroot - Remote_ip 10.252.240.142 - Command "login login tenant_name=Owner,password=*****,Secret=*****,challenge_response=*****,token=878335e1 3d869b7,client_port=-1,cert_verified=false,sessionId=*****,session_timeout=900,permission=superuser" - Status "Done"
Dec 03 2018 10:49:57 <span style="background-color: #007bff; color: white; padding: 2px;">Info</span>	GUI: CMD_EXECUTED: User nsroot - Remote_ip 10.252.240.227 - Command "login login tenant_name=Owner,password=*****,Secret=*****,challenge_response=*****,token=2f8ac227 524a8ed,client_port=-1,cert_verified=false,sessionId=*****,session_timeout=900,permission=superuser" - Status "Done"
Dec 03 2018 09:46:04 <span style="background-color: #007bff; color: white; padding: 2px;">Info</span>	GUI: CMD_EXECUTED: User nsroot - Remote_ip 10.252.240.97 - Command "login login tenant_name=Owner,password=*****,Secret=*****,challenge_response=*****,token=b3bc0b4c fad71ff,client_port=-1,cert_verified=false,sessionId=*****,session_timeout=900,permission=superuser" - Status "Done"
Nov 21 2018 10:24:26 <span style="background-color: #007bff; color: white; padding: 2px;">Info</span>	GUI: CMD_EXECUTED: User nsroot - Remote_ip 10.252.241.240 - Command "login login tenant_name=Owner,password=*****,Secret=*****,challenge_response=*****,token=4d381cfb 98db967,client_port=-1,cert_verified=false,sessionId=*****,session_timeout=900,permission=superuser" - Status "Done"

**Filter By**

- ▶ Module
- ▶ Event Type
- ▶ Severity

Apply

## Configurer les paramètres SSL

February 1, 2024

SSL (Secure Socket Layer) et TLS (Transport Layer Security) sont des protocoles de mise en réseau de sécurité couramment utilisés qui fournissent une communication chiffrée entre les utilisateurs et les serveurs. Vous pouvez configurer les paramètres SSL sur Citrix Application Delivery Management (ADM) et spécifier le type de clients qui se connectent au système.

### Pour configurer les paramètres SSL pour Citrix ADM :

1. Accédez à **Système > Administration système**. Sous **Paramètres système**, cliquez sur **Configurer les paramètres SSL**.
2. Sur la page **Paramètres SSL**, passez en revue les paramètres de protocole actuels et les suites de chiffrement appliquées au système.
3. Pour modifier les paramètres du protocole, accédez à **Modifier les paramètres > Paramètres du protocole** et apportez les modifications souhaitées.
4. Pour modifier les suites de chiffrement appliquées, accédez à **Modifier les paramètres > Suites de chiffrement** et apportez les modifications souhaitées.
5. Cliquez sur **OK**, puis sur **Fermer**.

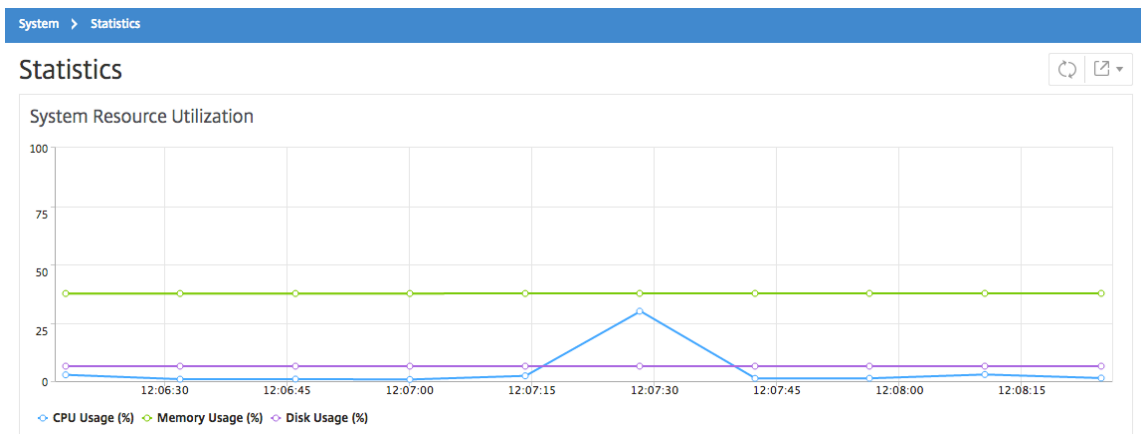
## Surveiller l'utilisation du processeur, de la mémoire et du disque

January 23, 2024

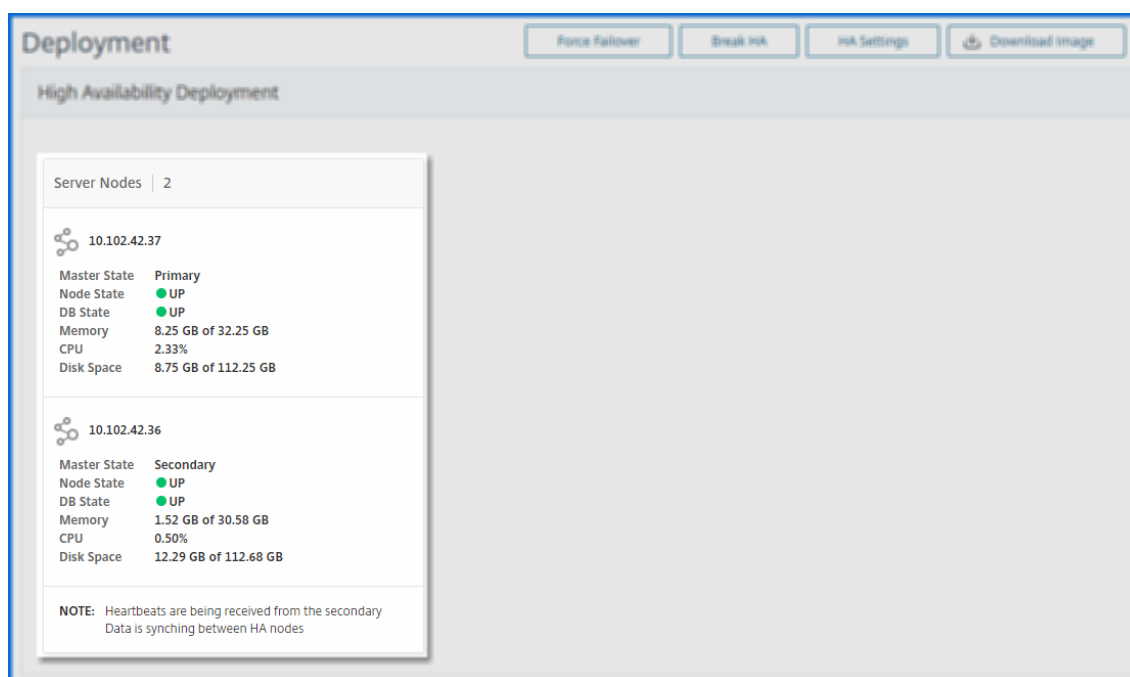
Vous pouvez utiliser les informations conservées dans les journaux et les statistiques. Ces informations sont également affichées dans des rapports qui vous aident à configurer et à gérer Citrix Application Delivery Management (ADM).

Pour surveiller l'utilisation du processeur, de la mémoire et du disque

- **Déploiement autonome.** Accédez à **Système > Statistiques**. Vous pouvez afficher en temps réel les graphiques d'utilisation du processeur, de la mémoire et du disque.



- **Déploiement haute disponibilité.** Accédez à **Système > Déploiement**. Les statistiques relatives à la mémoire, au processeur, à l'espace disque et aux instances gérées sont affichées numériquement comme illustré dans la figure suivante :



## Configurer les paramètres de notification système

February 1, 2024

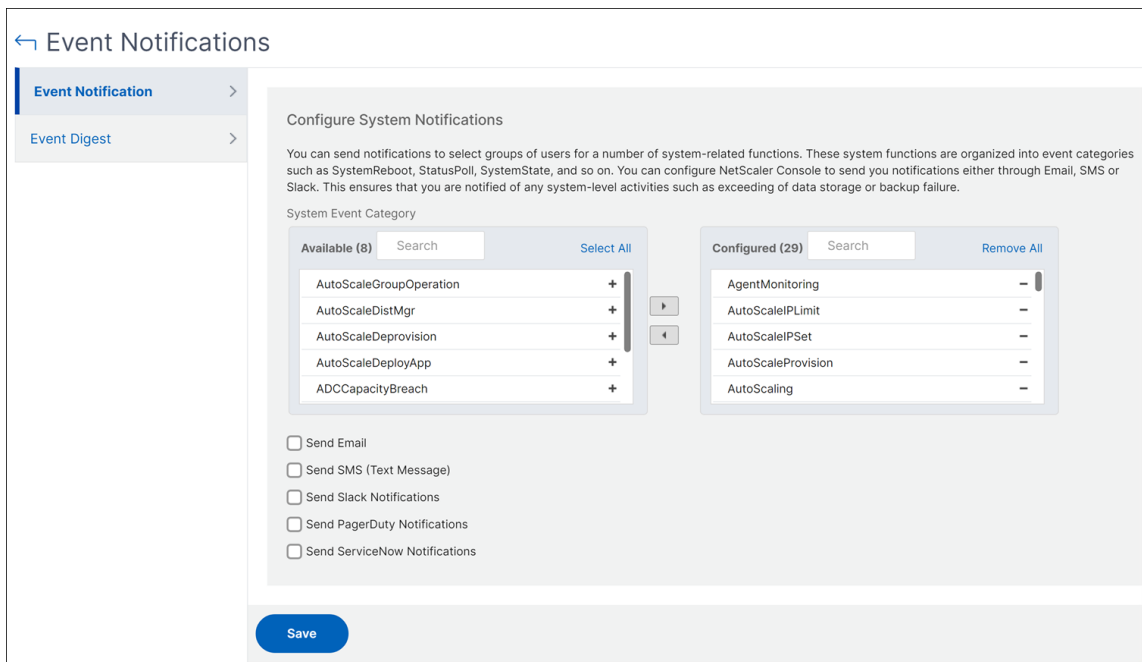
Vous pouvez envoyer des notifications à certains groupes d'utilisateurs pour un certain nombre de fonctions liées au système. Ces fonctions système sont organisées en catégories d'événements telles que SystemReboot, StatusPoll, SystemState, etc. Vous pouvez configurer Citrix Application Delivery Management (ADM) pour vous envoyer des notifications par e-mail ou SMS. Vous devez configurer un serveur de messagerie et/ou un serveur de Gateway SMS (Short Message Service) pour envoyer des notifications par courrier électronique et texte aux utilisateurs. Cela garantit que vous êtes averti de toute activité au niveau du système, comme l'ouverture de session de l'utilisateur ou le redémarrage du système.

Par exemple, vous pouvez envoyer une notification par e-mail à deux utilisateurs lorsqu'une personne tente de se connecter à Citrix ADM à l'aide de l'interface de ligne de commande et que la tentative d'ouverture de session échoue. Vous devez configurer la notification système en sélectionnant la catégorie UserLogin et créer un serveur de notification par e-mail ou choisir une liste de distribution de messagerie existante à laquelle envoyer la notification.

### Pour configurer les paramètres de notification système sur Citrix ADM :

1. Accédez à **Système > Notifications**. Sous **Paramètres**, cliquez sur **Modifier les paramètres de notification**.

2. Sur la page **Configurer les paramètres de notification système**, sous **Catégorie**, sélectionnez une catégorie telle que **UserLogin**.



3. Sélectionnez **Envoyer un e-mail**, puis sélectionnez une distribution de courrier électronique dans la liste déroulante ou cliquez sur l'icône “+” pour créer une nouvelle liste de distribution de courrier électronique comme illustré dans la figure ci-dessous. Si vous souhaitez envoyer des notifications par SMS, sélectionnez **Envoyer un SMS (message texte)** et créez une liste de distribution de SMS en cliquant sur l'icône « + » et en spécifiant les détails du serveur SMS.

← Create Email Distribution List

Name\*  
System-Notifications ⓘ

Email Servers\*  
192.0.2.35 Add Edit ⓘ

From  
admin@example.com ⓘ

To\*  
john@example.com ⓘ

Cc  
Email Address(s) to be included in Cc list

Bcc  
Email Address(s) to be included in Bcc list ⓘ

Create Close

Une fois que les notifications sont définies pour certaines catégories d'événements, chaque fois qu'un événement appartenant à cette catégorie se produit, une notification est envoyée aux destinataires par e-mail ou SMS. Dans cet exemple, vous pouvez voir une notification par e-mail lorsqu'un utilisateur ne parvient pas à se connecter à Citrix ADM à l'aide de l'interface de ligne de commande.

**Time:** Mon, 24 Apr 2017 14:32:12 GMT  
**Category:** UserLogin  
**Severity:** Major  
**Information:** Invalid "CLI" login for user nsroot from client IP Address 10.252.240.56  
**Action:** No Action Required.

Les notifications système sont envoyées pour les événements suivants :

Catégorie	Cause
BackupFailure	La sauvegarde du système échoue
DataStorageExceeded	Le stockage de base de données dépasse la limite spécifiée dans la licence
DeviceBackupFailure	La sauvegarde de l'instance échoue

Catégorie	Cause
HAMonitoring	Le basculement de la haute disponibilité du système se produit, aucun battement de cœur du nœud homologue et une défaillance de synchronisation de la base de données se produit
HealthMonitoring	L'utilisation du processeur, de la RAM ou du disque dépasse la valeur seuil
LicensePool	Le pool de licences dépasse la valeur seuil
Licences	La licence échoue lorsqu'elle est appliquée
PasswordRecovery	La récupération du mot de passe échoue ou réussit
PerfCounterThresholdHigh	La valeur du compteur de performance dépasse la limite
PerfCounterThresholdNormal	La valeur du compteur de performance est normale
PolicyFailed	L'une des stratégies du système échoue
RemoteDeviceBackupFailure	La sauvegarde de l'instance distante échoue
RemoteSystemBackupFailure	La sauvegarde du système à distance échoue
RemoteSystemBackupNormal	La sauvegarde du système à distance réussit
SSLCertThreshold	Le seuil pour un certificat est dépassé
StatusPoll	Toute modification de l'état d'une instance
SubSystemState	Toute modification de l'état du sous-système
SystemReboot	Le système est redémarré
SystemState	Toute modification de l'état du système
TrapConfigFailure	Un échec se produit lors de l'ajout d'un piège SNMP sur une instance
UserLogin	L'authentification de l'utilisateur échoue

## Générer un fichier de support technique

February 1, 2024

Citrix vous recommande de générer une archive des données et des statistiques de Citrix Application Delivery Management (ADM) avant de contacter le support technique pour résoudre un problème. L'archive est un fichier TAR que vous pouvez envoyer à l'équipe de support technique.

#### Remarque

Pour les serveurs Citrix ADM en mode haute disponibilité, vous pouvez générer un fichier de support technique à partir de l'un 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 Citrix ADM :

1. Accédez à **Système > Diagnostics > Support technique**, puis cliquez sur **Générer un fichier de support technique**.
2. Dans la page **Générer un fichier de support**, sélectionnez les options suivantes :
  - **Collecter les journaux de débogage** —Sélectionnez cette option pour collecter les journaux afdécoder.
  - **Durée** : saisissez la durée pendant laquelle les journaux de débogage doivent être collectés. Cette option ne s'affiche que si vous activez l'option **Collecter les journaux de débogage**.
  - **Collecter la distribution des données** : sélectionnez cette option pour collecter des journaux distincts et divers à partir de la base de données.

```
1 The archive file is created as a TAR file.
2
3 For example, the archive file that is created might be named as
  follows: Citrix_ADM_<ADM_IP_address>_<DDMMYY>_<time_stamp>.
  tar.gz
```

1. Vous pouvez envoyer les fichiers de support technique à l'équipe de support de deux manières :
  - a) Vous pouvez télécharger le fichier depuis l'interface graphique d'ADM vers votre stockage local, puis utiliser un navigateur Web pour le télécharger vers CIS.
  - b) Vous pouvez également télécharger les fichiers de support technique sur le site Web Citrix Insight Services (CIS) en exécutant un script sur la console ADM.
    - i. À l'aide de SSH, connectez-vous à la console ADM.
    - ii. Passer à l'invite Shell et tapez :  
`/mps/collector_upload.pl`

La commande complète est donnée ci-dessous avec les attributs que vous devez fournir :

```
1 /mps/collector_upload.pl [-proxy [<proxy_user>:<proxy_password>@]<  
    proxy_host>:<proxy_port>] [-user <user>] [-password <password>] [-sr  
    <sr>] [-description <description>] [-debug] <file>  
2 <!--NeedCopy-->
```

L'avantage de l'exécution du script Perl est que vous n'avez pas à télécharger le fichier de support technique d'ADM sur votre système local, puis à le télécharger sur CIS. En option, vous pouvez télécharger le fichier vers CIS directement à l'aide d'un proxy de la console ADM.

Assurez-vous d'avoir un compte sur CIS. Vous pouvez utiliser les informations d'identification de votre compte Citrix pour télécharger des fichiers vers CIS.

Et si vous n'avez pas de serveur proxy ? Ou que faire si vous rencontrez des problèmes avec les proxys de transfert SSL ? (Cela peut se produire si le script Perl ne fait pas confiance au certificat racine du serveur proxy.)

Vous pouvez toujours télécharger le fichier directement depuis le shell ADM vers CIS.

#### Remarque

Vous pouvez toujours télécharger le fichier et l'envoyer par e-mail à l'équipe de support technique Citrix si ADM ne parvient pas à télécharger le fichier vers CIS depuis la console. Vous pouvez également télécharger le fichier depuis ADM sur votre stockage local, puis utiliser un navigateur Web pour le télécharger vers CIS.

## Configurer un groupe de chiffrement

January 23, 2024

Un groupe de chiffrement est un ensemble de suites de chiffrement que vous liez à un serveur virtuel, un service ou un groupe de services SSL sur l'instance ADC (Citrix Application Delivery Controller). Une suite de chiffrement comprend un protocole, un algorithme d'échange de clés (Kx), un algorithme d'authentification (Au), un algorithme de chiffrement (Enc) et un algorithme de code d'authentification des messages (Mac).

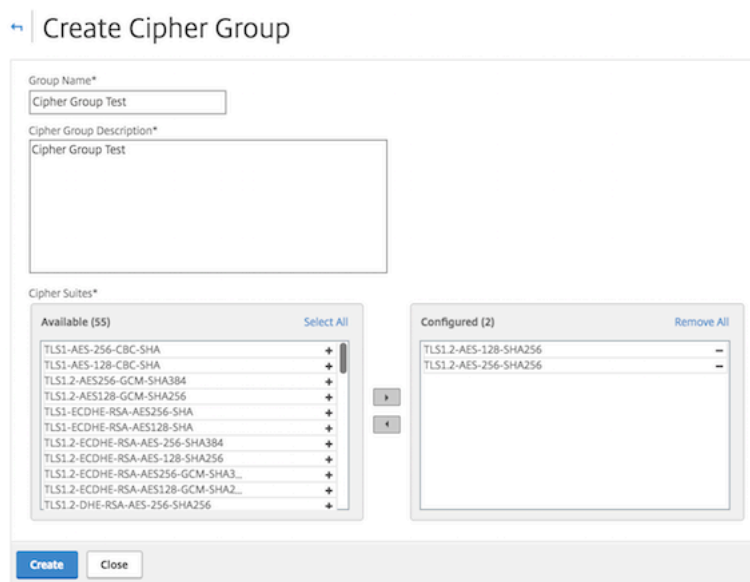
### Pour ajouter un groupe de chiffrement sur Citrix ADM :

1. Accédez à **Système > Groupes de chiffrement**, puis cliquez sur **Ajouter**.
2. 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.

3. Cliquez sur **Créer**.



## Créer une destination d'interruptions SNMP, une communauté de gestionnaires et des utilisateurs

February 1, 2024

Chaque fois qu'une condition anormale se produit sur Citrix ADM, une interruption SNMP est générée. Les interruptions sont ensuite envoyées à un périphérique distant appelé serveur de destination d'interruptions ou *destination d'interruptions SNMP*. Vous pouvez interroger l'agent SNMP pour obtenir des informations spécifiques au système à partir d'un périphérique distant appelé *gestionnaire SNMP*. L'agent recherche ensuite les données demandées dans la base d'informations de gestion (MIB) et envoie les données au gestionnaire SNMP.

### Pour créer une destination d'interruption SNMP sur Citrix ADM :

1. Accédez à **Système > SNMP > Destinations d'interruptions**.
2. Sous **Interruptions SNMP**, cliquez sur **Ajouter** pour créer une interruption SNMP, puis spécifiez les détails suivants :
  - **Version**. Sélectionnez la version SNMP à utiliser.

- **Serveur de destination.** Nom ou adresse IP de la destination de l'interception.
- **Port.** Entrez le port de destination du piège. Le port est défini sur 162 par défaut.
- **Communauté.** Spécifiez la chaîne communautaire à utiliser lors de l'envoi d'un trap à l'auditeur trap.

3. Cliquez sur **Créer**.

#### Remarque

Si vous créez une destination d'interruption SNMP v3, spécifiez les informations d'identification utilisateur SNMP auxquelles vous souhaitez lier l'interruption. Pour ajouter des informations d'identification utilisateur SNMP, cliquez sur **Insérer**, puis ajoutez l'utilisateur dans la liste des utilisateurs SNMP disponibles.

#### Pour créer une communauté de gestionnaires SNMP, procédez comme suit :

1. Accédez à **Système > SNMP > Gestionnaires**.
2. Sous **Gestionnaire SNMP**, cliquez sur **Ajouter** pour créer une communauté de gestionnaires SNMP, puis spécifiez les détails suivants :
  - **Gestionnaire SNMP.** Entrez le nom ou l'adresse IP du gestionnaire SNMP.
  - **Communauté.** Spécifiez la chaîne de communauté à utiliser lors de l'envoi d'interruptions à l'auditeur de trappes.
3. Vous pouvez éventuellement cocher la case **Activer le réseau de gestion** pour spécifier le masque de **réseau, qui est le masque** de sous-réseau du réseau du gestionnaire SNMP.
4. Cliquez sur **Créer**.

#### Pour créer un utilisateur SNMP :

1. Accédez à **Système > SNMP > Utilisateurs**.
2. Sous **Utilisateur SNMP**, cliquez sur **Ajouter**.
3. Entrez le nom d'utilisateur et attribuez un niveau de sécurité à l'utilisateur depuis le menu.
4. En fonction du niveau de sécurité que vous avez attribué à l'utilisateur, fournissez des protocoles d'authentification supplémentaires, tels que des protocoles d'authentification, des mots de passe de confidentialité et attribuez des vues SNMP.

## Configurer et afficher les alarmes système

February 1, 2024

Vous pouvez activer et configurer un ensemble d’alarmes pour surveiller l’intégrité de vos serveurs Citrix Application Delivery Management (ADM). Vous devez configurer les alarmes système pour vous assurer que vous êtes conscient de tout problème système critique ou majeur. Par exemple, vous pouvez être averti si l’utilisation de l’UC est élevée ou s’il y a plusieurs échecs de connexion au serveur. Pour certaines catégories d’alarmes, telles que CPUUsageHigh ou MemoryUsageHigh, vous pouvez définir des seuils et définir la gravité (critique ou majeure, par exemple) pour chacune d’entre elles. Pour certaines catégories, telles que InventoryFailed ou LoginFailure, vous ne pouvez définir que la gravité. Lorsque le seuil est enfreint pour une catégorie d’alarme (par exemple, MemoryUsageHigh) ou lorsqu’un événement se produit correspondant à la catégorie d’alarme (par exemple, **LoginFailure**), un message est enregistré dans le système et vous pouvez afficher le message sous la forme d’un message syslog. Vous pouvez également configurer les notifications pour recevoir un e-mail ou un SMS correspondant à vos paramètres d’alarme.

Vous pouvez attribuer ou modifier la gravité d’une alarme. Les niveaux de gravité que vous pouvez attribuer sont Critique, Majeur, Mineur, Avertissement et Informatif.

Considérez un scénario dans lequel vous souhaitez surveiller chaque fois qu’une tentative de sauvegarde a échoué. Vous pouvez activer l’alarme BackupFailed et lui attribuer une gravité, telle que Major. Chaque fois que Citrix ADM tente de sauvegarder les fichiers système et lorsque la tentative échoue, une alarme est déclenchée. Vous pouvez afficher le message sur Citrix ADM ou recevoir des notifications par e-mail ou SMS.

Pour configurer l’alarme, vous devez sélectionner l’alarme BackupFailed et spécifier le niveau de gravité Major. L’alarme est activée par défaut.

### Pour configurer et afficher une alarme système à l’aide de Citrix ADM :

1. Accédez à **Système > Alarmes**.

Name	Status	Severity	Threshold	Time (minutes)
<input checked="" type="checkbox"/> backupFailed	Enabled	Major	-NA-	-NA-
<input type="checkbox"/> cpuUsageHigh	Enabled	--	80	0
<input type="checkbox"/> cpuUsageNormal	Enabled	--	-NA-	-NA-
<input type="checkbox"/> dataStorageExceeded	Enabled	--	-NA-	-NA-
<input type="checkbox"/> dataStorageNormal	Enabled	--	-NA-	-NA-
<input type="checkbox"/> devicebackupFailed	Enabled	--	-NA-	-NA-
<input type="checkbox"/> diskUtilizationHigh	Enabled	--	80	0
<input type="checkbox"/> diskUtilizationNormal	Enabled	--	-NA-	-NA-
<input type="checkbox"/> haDatabaseOutOfSync	Enabled	--	-NA-	-NA-

2. Sélectionnez l’alarme à configurer (par exemple, BackupFailed) et cliquez sur **Modifier** pour modifier ses paramètres.
3. L’alarme est activée par défaut. Attribuez un niveau de gravité (exemple : Majeur), puis cliquez sur **OK**.

### Remarque

Pour certaines alarmes, vous ne pouvez pas définir de seuil.

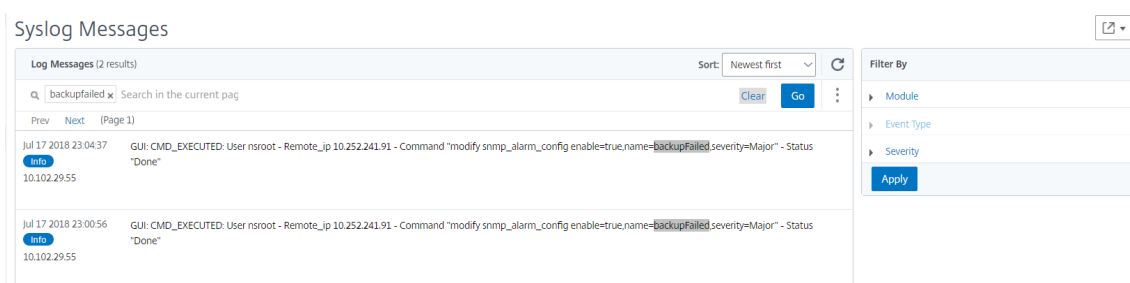
Lorsque l'alarme est déclenchée, vous pouvez afficher l'événement généré sous la forme d'un message syslog.

### Pour afficher l'événement généré par l'alarme BackupFailed à l'aide de Citrix ADM :

1. Accédez à **Système > Audit**.
2. Dans la page **Audit**, sous **Messages d'audit**, sélectionnez **Messages Syslog**.

3. Dans le champ de recherche, saisissez le nom de l'alarme.

Dans cet exemple, vous pouvez voir qu'un événement a été généré pour une tentative de sauvegarde ayant échoué.



Vous pouvez également définir des notifications pour vous envoyer un e-mail ou un SMS (Short Message Service) lorsqu'une alarme est déclenchée. Pour plus d'informations sur la façon de configurer les notifications système, consultez [Comment configurer les paramètres de notification système de Citrix ADM](#).

## Citrix ADM en tant que serveur proxy API

February 1, 2024

En plus de pouvoir recevoir des demandes d'API REST NITRO pour ses propres fonctionnalités de gestion et d'analyse, Citrix Application Delivery Management (Citrix ADM) peut fonctionner en tant que serveur proxy API REST pour ses instances gérées. Au lieu d'envoyer des demandes d'API directement aux instances gérées, les clients d'API REST peuvent envoyer les demandes d'API à Citrix ADM. Citrix ADM peut faire la différence entre les demandes d'API auxquelles il doit répondre et les demandes d'API qu'il doit transférer inchangées à une instance gérée.

En tant que serveur proxy API, Citrix ADM vous offre les avantages suivants :

- **Validation des demandes d'API.** Citrix ADM valide toutes les demandes d'API par rapport aux stratégies de sécurité configurées et de contrôle d'accès basé sur les rôles (RBAC). Citrix ADM

est également conscient des locataires et veille à ce que l'activité API ne dépasse pas les limites des locataires.

- **Audit centralisé.** Citrix ADM gère un journal d'audit de toutes les activités d'API liées à ses instances gérées.
- **Gestion de session.** Citrix ADM libère les clients API de la tâche consistant à gérer des sessions avec des instances gérées.

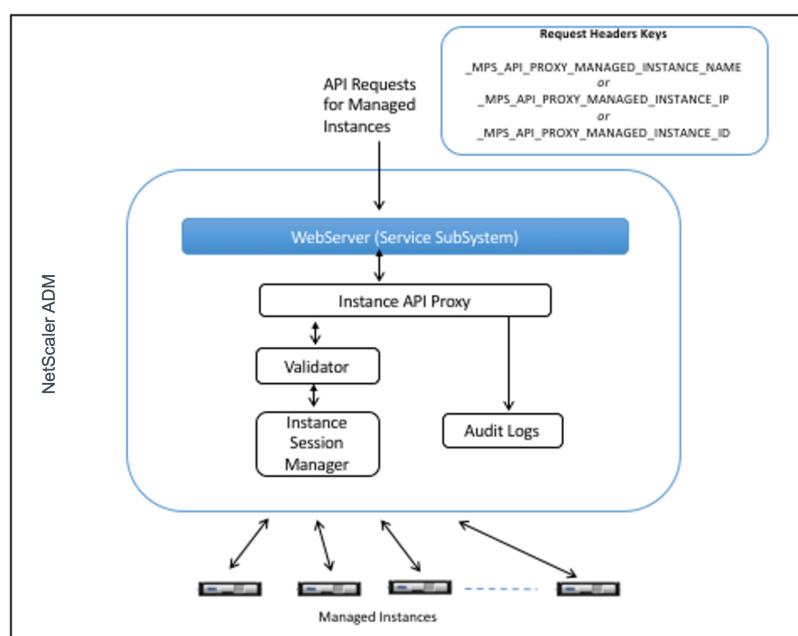
### Comment Citrix ADM fonctionne en tant que serveur proxy d'API

Lorsque vous souhaitez que Citrix ADM transporte une requête à une instance gérée, vous configurez le client API pour inclure l'un des en-têtes HTTP suivants dans la requête API :

- `_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.

La présence de l'un de ces en-têtes HTTP permet à Citrix ADM d'identifier une requête API comme une requête qu'elle doit transférer à une instance gérée. La valeur de l'en-tête permet à Citrix ADM d'identifier l'instance gérée vers laquelle il doit transférer la demande.

Ce flux est représenté dans la figure suivante :



Comme indiqué dans la figure ci-dessus, lorsque l'un de ces en-têtes HTTP apparaît dans une requête, Citrix ADM traite la demande comme suit :

1. Sans modifier la demande, Citrix ADM transmet la demande au moteur proxy de l'API d'instance.
2. Le moteur proxy de l'API d'instance transmet la demande d'API à un validateur et consigne les détails de la demande d'API dans le journal d'audit.
3. Le validateur s'assure que la demande ne viole pas les stratégies de sécurité configurées, les stratégies RBAC, les limites de location, etc. Il effectue des vérifications supplémentaires, telles qu'une vérification pour déterminer si l'instance gérée est disponible.

Si la demande d'API est valide et peut être transférée à l'instance gérée, Citrix ADM identifie une session qui est maintenue par le gestionnaire de session d'instance, puis envoie la demande à l'instance gérée.

### Comment utiliser Citrix ADM en tant que serveur proxy API

Les exemples suivants montrent les demandes d'API REST qu'un client API envoie à un serveur Citrix ADM dont l'adresse IP est 192.0.2.5. Citrix ADM est requis pour transférer les demandes, inchangées, vers une instance gérée avec l'adresse IP 192.0.2.10. Tous les exemples utilisent l'en-tête `_MPS_API_PROXY_MANAGED_INSTANCE_IP`.

Avant d'envoyer les demandes d'API Citrix ADM, le client API doit :

- Connectez-vous à Citrix ADM
- Obtenir un ID de session
- Incluez l'ID de session dans les demandes d'API suivantes.

La demande d'API d'ouverture de session est de la forme suivante :

```
1  POST /nitro/v2/config/login HTTP/1.1
2  Host: 192.0.2.5
3  Content-Type: application/json
4  Accept: application/json
5  Cache-Control: no-cache
6
7  {
8
9      "login":
10     {
11
12         "username":"*****",
13         "password":"*****"
14     }
15 }
16
17
18 <!--NeedCopy-->
```

Citrix ADM répond à la demande d'ouverture de session avec une réponse qui inclut l'ID de session. L'exemple de corps de réponse suivant affiche un ID de session :

```
1 {
2
3
4   "errorCode": 0,
5   "message": "Done",
6   "operation": "add",
7   "resourceType": "login",
8   "username": "*****",
9   "tenant_name": "Owner",
10  "resourceName": "*****",
11  "login": [
12    {
13
14      "tenant_name": "Owner",
15      "permission": "superuser",
16      "session_timeout": "36000",
17      "challenge_token": "",
18      "username": "",
19      "login_type": "",
20      "challenge": "",
21      "client_ip": "",
22      "client_port": "-1",
23      "cert_verified": "false",
24      "sessionid": "##
25      D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D",
26      "token": "b2f3f935e93db6a"
27    }
28  ]
29 }
30 }
31
32 <!--NeedCopy-->
```

### Exemple 1 : Récupérer des statistiques de serveur virtuel d'équilibrage de charge

Le client doit envoyer à Citrix ADM une demande d'API du formulaire suivant :

```
1   GET /nitro/v1/stat/lbvserver HTTP/1.1
2   Host: 192.0.2.5
3   _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
4   Cookie: SESSID=##
5       D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
6   Accept: application/json
7   Cache-Control: no-cache
8 <!--NeedCopy-->
```

**Exemple 2 : Créer un serveur virtuel d'équilibrage de charge**

Le client doit envoyer à Citrix ADM une demande d'API du formulaire suivant :

```
1   POST /nitro/v1/config/lbvserver/sample_lbvserver HTTP/1.1
2   Host: 192.0.2.5
3   _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
4   Cookie: SESSID=##
        D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
5   Content-Type: application/json
6   Accept: application/json
7   Cache-Control: no-cache
8
9   {
10  "lbvserver":{
11  "name":"sample_lbvserver","servicetype":"HTTP","ipv46":"10.102.1.11","
        port":"80" }
12  }
13
14  <!--NeedCopy-->
```

**Exemple 3 : Modifier un serveur virtuel d'équilibrage de charge**

Le client doit envoyer à Citrix ADM une demande d'API du formulaire suivant :

```
1   PUT /nitro/v1/config/lbvserver HTTP/1.1
2   Host: 192.0.2.5
3   SESSID: ##
        D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
4   _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
5   Content-Type: application/json
6   Accept: application/json
7   Cache-Control: no-cache
8
9   {
10  "lbvserver":{
11  "name":"sample_lbvserver","appflowlog":"DISABLED" }
12  }
13
14  <!--NeedCopy-->
```

**Exemple 4 : Suppression d'un serveur virtuel d'équilibrage de charge**

Le client doit envoyer à Citrix ADM une demande d'API du formulaire suivant :

```
1   DELETE /nitro/v1/config/lbvserver/sample_lbvserver HTTP/1.1
2   Host: 192.0.2.5
3   Cookie: SESSID=##
        D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
```



```

4     _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
5     Cache-Control: no-cache
6
7 <!--NeedCopy-->

```

## FAQ

February 1, 2024

Cette section fournit la FAQ sur les fonctionnalités suivantes de Citrix Application Delivery Management (Citrix ADM). Cliquez sur le nom d'une fonctionnalité dans le tableau suivant pour afficher la liste des questions fréquentes relatives à cette fonctionnalité.

Analytics	Authentification	Gestion de la configuration
Gestion des certificats	Déploiement	Déploiement (reprise après sinistre)
Gestion des événements	Gestion des instances	StyleBooks
Gestion du système		

### Analytics

#### Dois-je activer le canal virtuel EUEM sur les instances Citrix Gateway déployées en mode single hop ?

Les données de canal virtuel EUEM font partie des données HDX Insight que Citrix ADM reçoit des instances de Gateway. Le canal virtuel EUEM fournit les données sur ICA RTT. Si le canal virtuel EUEM n'est pas activé, les données HDX Insight restantes sont toujours affichées sur Citrix ADM.

Un canal virtuel EUEM est un service par défaut exécuté sur les applications Citrix Virtual Desktop (VDA). S'il n'est pas en cours d'exécution, démarrez le processus « Citrix End User Experience Monitoring » dans les services VDA.

#### Comment activer Citrix ADM pour surveiller le trafic des applications Web et des postes de travail virtuels ?

1. Accédez à **Infrastructure > Instances** , puis sélectionnez l'instance Citrix Application Delivery Controller (Citrix ADC) sur laquelle vous souhaitez activer les analyses.

2. Sélectionnez **Enable/Disable Insight** dans la liste déroulante **Action** .
3. Sur la page **Configure Insight** qui s'ouvre, sélectionnez tous les serveurs virtuels sur lesquels vous souhaitez activer les analyses, puis cliquez sur **Activer AppFlow** . Pour plus de détails, consultez [Comment activer Analytics sur les instances](#).

#### Remarque

Pour les instances Citrix ADC de version 11.0, version 65.30 et versions ultérieures, il n'existe aucune option sur Citrix ADM pour activer Security Insight explicitement. Assurez-vous de configurer les paramètres AppFlow sur les instances Citrix ADC, de sorte que Citrix ADM commence à recevoir le trafic Security Insight avec le trafic Web Insight. Pour plus d'informations sur la façon de définir les paramètres AppFlow sur les instances Citrix ADC, consultez [Pour définir les paramètres AppFlow à l'aide de l'utilitaire de configuration](#).

#### **Après avoir ajouté les instances de Citrix ADC, Citrix ADM commence-t-il automatiquement à collecter des informations analytiques ?**

Non. Vous devez d'abord activer les analyses sur les serveurs virtuels hébergés dans les instances Citrix ADC gérées par Citrix ADM. Pour plus de détails, consultez [Comment activer les analyses sur les instances](#) .

#### **Dois-je accéder à l'appliance Citrix ADC individuelle pour activer les analyses ?**

Non. Toute la configuration est effectuée à partir de l'interface utilisateur Citrix ADM, qui répertorie les serveurs virtuels hébergés sur l'instance Citrix ADC spécifique. Pour plus de détails, consultez [Comment activer les analyses sur les instances](#) .

#### **Quels sont les types de serveurs virtuels qui peuvent être répertoriés sur une instance Citrix ADC pour activer les analyses ?**

Actuellement, l'interface utilisateur de Citrix ADM répertorie les serveurs virtuels suivants pour activer les analyses :

- Serveur virtuel d'équilibrage de charge
- Serveur virtuel de commutation de contenu
- Serveur virtuel VPN
- Serveur virtuel de redirection de cache

## **Comment attacher un disque supplémentaire à Citrix ADM ?**

Pour attacher un disque supplémentaire à Citrix ADM :

1. Arrêtez la machine virtuelle Citrix ADM.
2. Dans l'Hypervisor, attachez un disque supplémentaire de la taille de disque requise à la machine virtuelle Citrix ADM.

Par exemple, Considérons que vous souhaitez augmenter l'espace disque à 200 Go, dans une machine virtuelle Citrix ADM de 120 Go. Dans ce scénario, vous devez associer un espace disque de 200 Go au lieu de 80 Go. Les 200 Go d'espace disque nouvellement attachés seront utilisés pour stocker les données de base de données, les fichiers journaux Citrix ADM. L'espace disque existant de 120 Go sera utilisé pour stocker les fichiers principaux, les fichiers journaux du système d'exploitation, etc.

3. Démarrez la machine virtuelle Citrix ADM.

## **Que voulez-vous dire par les collecteurs ne sont pas configurés sur les instances Citrix ADC ?**

Un collecteur reçoit les enregistrements AppFlow générés par l'appliance Citrix ADC.

Citrix ADM reçoit le trafic Security Insight et Web Insight des instances Citrix ADC lorsque la fonctionnalité AppFlow est activée. Lorsque vous activez la fonctionnalité AppFlow sur une instance Citrix ADC, vous devez spécifier au moins un collecteur auquel les enregistrements AppFlow sont envoyés. Si les collecteurs ne sont pas configurés sur les instances Citrix ADC, Citrix ADM ne reçoit pas le trafic provenant des instances.

Par exemple, cinq instances Citrix ADC sont ajoutées à Citrix ADM. Si aucun collecteur n'est spécifié pour deux instances, aucun trafic ne circule vers Citrix ADM. Les diagnostics en libre-service détectent le problème et affichent le problème comme « Les collecteurs ne sont pas configurés sur 2 instances. »

Pour plus d'informations sur la façon de configurer la fonctionnalité AppFlow, consultez [Configuration de la fonctionnalité AppFlow](#).

## **Authentification**

### **Qu'est-ce que l'équilibrage de charge des demandes d'authentification ?**

La fonction d'équilibrage de charge du serveur d'authentification permet à Citrix ADM d'équilibrer la charge des demandes d'authentification qui sont dirigées vers les serveurs d'authentification 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 Citrix ADM.

### **Ai-je une alternative lorsque l'authentification externe échoue ?**

Il peut arriver que l'authentification externe échoue complètement, même si vous avez mis en cascade plusieurs serveurs. Par exemple, les serveurs externes peuvent devenir inaccessibles ou les informations d'identification d'un nouvel utilisateur n'ont peut-être été saisies sur aucun des serveurs d'authentification externes. Pour empêcher le verrouillage des utilisateurs dans une telle situation, vous pouvez activer l'authentification locale de secours. Pour plus de détails, consultez [Authentification locale de secours](#).

### **Qu'est-ce que l'authentification locale de secours ?**

L'authentification locale de secours est une option permettant d'authentifier vos utilisateurs localement en cas d'échec de l'authentification externe. Si l'authentification externe échoue, Citrix ADM accède à la base de données utilisateur locale pour authentifier vos utilisateurs.

Dans Citrix ADM, accédez à **Système > Authentification > Configuration de l'authentification**. Sur cette page, vous pouvez ajouter plusieurs serveurs d'authentification externes en cascade et sélectionner l'option **Activer l'authentification locale de secours**.

### **Qu'est-ce que l'extraction de groupes d'utilisateurs externes ?**

Si vous avez ajouté des serveurs externes pour authentifier les utilisateurs, vous pouvez importer (extraire) des groupes d'utilisateurs existants dans Citrix ADM. Vous devez importer des groupes d'utilisateurs une seule fois et leur accorder une autorisation de groupe plutôt que d'importer des utilisateurs

individuels et de leur accorder des autorisations individuelles. Il n'est pas nécessaire de recréer les utilisateurs sur Citrix ADM.

### **Pourquoi devons-nous attribuer des autorisations de groupe ?**

Lorsque vous utilisez la fonctionnalité d'équilibrage de charge de Citrix ADC, vous pouvez intégrer Citrix ADM à des serveurs d'authentification externes et importer des informations de groupe d'utilisateurs à partir des serveurs d'authentification. Connectez-vous à Citrix ADM et créez manuellement les mêmes informations de groupe dans Citrix ADM et attribuez des autorisations à ces groupes. L'autorisation utilisateur et groupe d'utilisateurs est gérée dans Citrix ADM et non dans le serveur externe. Les utilisateurs disposent de différentes autorisations d'accès basées sur les rôles sur les serveurs externes. Configurez également les mêmes autorisations pour les utilisateurs dans Citrix ADM. Au lieu de configurer les autorisations individuellement pour chaque utilisateur, vous pouvez configurer une autorisation au niveau du groupe afin que les membres du groupe d'utilisateurs puissent accéder à des services spécifiques sur les serveurs virtuels à charge équilibrée. Les autorisations typiques que vous pouvez attribuer sont des autorisations pour gérer les instances Citrix ADC, les instances Citrix SDX, les serveurs virtuels, etc., afin que les utilisateurs de ce groupe puissent gérer uniquement ces instances ou serveurs virtuels. Vous pouvez modifier ultérieurement les autorisations accordées aux utilisateurs au niveau du groupe. Vous pouvez même supprimer un ou plusieurs groupes d'utilisateurs ; les autres utilisateurs du groupe continuent de fonctionner sur Citrix ADM.

### **Gestion de la configuration**

#### **Puis-je effectuer la configuration de plusieurs instances Citrix ADC simultanément à l'aide de Citrix ADM ?**

Oui, vous pouvez utiliser des tâches de configuration pour effectuer la configuration sur plusieurs instances de Citrix ADC.

#### **Que sont les tâches de configuration sur Citrix ADM ?**

Une tâche est un ensemble de commandes de configuration que vous pouvez créer et exécuter sur une ou plusieurs instances gérées. Vous pouvez créer des tâches pour apporter des modifications de configuration entre les instances, répliquer les configurations sur plusieurs instances de votre réseau et enregistrer et lire des tâches de configuration à l'aide de l'interface utilisateur graphique Citrix ADM. Vous pouvez également convertir les tâches enregistrées en commandes CLI.

Vous pouvez utiliser la fonctionnalité Travaux de configuration de Citrix ADM pour créer une tâche de configuration, envoyer des notifications par e-mail et vérifier les journaux d'exécution des tâches créées.

### **Puis-je planifier des tâches à l'aide de modèles intégrés dans Citrix ADM ?**

- Oui ! Vous pouvez planifier une tâche à l'aide de l'option de modèle intégrée. Une tâche est un ensemble de commandes de configuration que vous pouvez exécuter sur une ou plusieurs instances gérées. Par exemple, vous pouvez utiliser l'option de modèle intégrée pour planifier une tâche de configuration des serveurs syslog. Vous pouvez choisir d'exécuter le travail immédiatement ou de planifier l'exécution ultérieure.

Vous pouvez enregistrer la configuration d'une tâche créée précédemment et l'exécuter à nouveau après avoir modifié les commandes, les paramètres, la source de configuration et les instances ciblées. Ceci est utile lorsque le même ensemble de commandes doit être exécuté sur une instance différente, ou lorsque le travail rencontre une erreur et arrête l'exécution ultérieure.

### **Gestion des certificats**

#### **La suppression de certificats SSL à partir de Citrix ADM entraîne-t-elle la suppression de certificats à partir d'instances Citrix ADC ?**

Non

### **Déploiement**

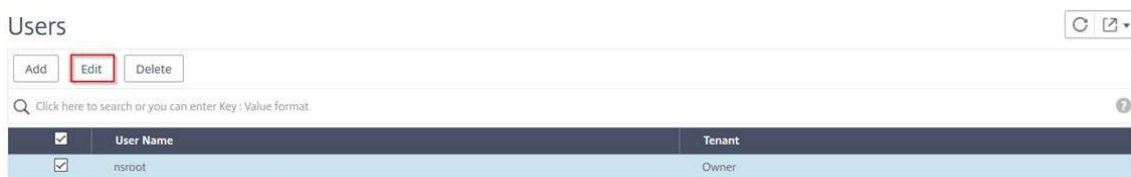
#### **Quels sont le nom d'utilisateur et le mot de passe par défaut ?**

- Une fois la configuration réseau initiale terminée, vous pouvez vous connecter à Citrix ADM à partir de l'hyperviseur ou de la console SSH, en utilisant le nom d'utilisateur et le mot de passe par défaut (nsrecover/nsroot).
- Le nom d'utilisateur et le mot de passe par défaut pour se connecter à partir de l'interface graphique sont *nsroot/nsroot*.

#### **Comment modifier le mot de passe par défaut ?**

Pour modifier le mot de passe :

1. Dans Citrix ADM, accédez à **Système > Administration des utilisateurs > Utilisateurs**.  
La page Utilisateurs s'affiche.
2. Sélectionnez le nom d'utilisateur **nsroot** et cliquez sur **Modifier**.



La page Configurer l'utilisateur système s'affiche.

3. Sélectionnez **Modifier le mot de passe** et créez un mot de passe de votre choix.

User Name\*

 ?

Password\*

 ?

Confirm Password\*

 ?

4. Cliquez sur **OK**.

Vous pouvez maintenant utiliser le nouveau mot de passe pour vous connecter à partir de l'interface graphique et de l'Hypervisor ou de la console SSH.

Remarque

Vous ne pouvez pas modifier le nom d'utilisateur.

### Comment réinitialiser le mot de passe ?

Vous pouvez consulter cette [documentation](#) pour réinitialiser le mot de passe.

### Dans une paire HA, si le mot de passe est modifié dans le nœud principal et si l'option Break HA pair est sélectionnée ultérieurement, quel est le comportement ?

Vous pouvez vous connecter aux deux nœuds autonomes à l'aide de votre nouveau mot de passe.

### Si deux serveurs autonomes ont des mots de passe différents, quel est l'impact du déploiement de ces deux serveurs en paire HA ?

Il est recommandé d'avoir un mot de passe par défaut pour les deux serveurs lorsque vous déployez deux serveurs autonomes sur une paire HA.

**La configuration HA est terminée, mais l'interface utilisateur du nœud principal n'est pas accessible. Quelle peut être la raison ?**

Quelques minutes sont nécessaires pour que la configuration soit prise en compte. Vous pouvez réessayer d'y accéder au bout de quelques minutes.

**La configuration HA est terminée, mais l'interface graphique de l'adresse IP flottante n'est pas accessible. Quelle peut être la raison ?**

Après la configuration de la haute disponibilité, vous devez d'abord accéder à l'interface graphique du nœud principal et terminer le déploiement. Pour plus d'informations, consultez [Déployer le nœud principal et le nœud secondaire en tant que paire haute disponibilité](#). Une fois le déploiement terminé, le serveur redémarre et se prépare pour le déploiement haute disponibilité. Vous pouvez ensuite accéder à l'interface graphique de l'adresse IP flottante.

**Quelle base de données est prise en charge dans Citrix ADM autonome et Citrix ADM HA ?**

Citrix ADM autonome et Citrix ADM HA prennent en charge PostgreSQL.

**Quelle est la perte de données potentielle pour le nœud secondaire ?**

Le nœud secondaire écoute les messages de pulsation que le nœud principal envoie via la base de données Citrix ADM. Si le nœud secondaire ne reçoit pas les pulsations pendant plus de 180 secondes, le nœud secondaire effectue une vérification basée sur SSH sur le nœud principal. Si le battement de cœur et la vérification basée sur SSH échouent, le nœud principal est considéré comme étant hors service.

Dans ce scénario, le nœud secondaire prend le relais en tant que nœud principal et la période de 180 secondes peut être considérée comme la perte de données possible pour le nœud secondaire.

**Que se passe-t-il si le nœud principal est en panne ?**

Le nœud secondaire prend le relais et devient le nœud principal.

**Comment réinstaller le nœud défaillant ?**

Il est recommandé d'installer une nouvelle version de machine virtuelle. Pour réinstaller :

1. Brisez la paire HA. Accédez à **Système > Déploiement**  
La page de déploiement s'affiche. Cliquez sur **Break HA**



2. Supprimez le nœud défaillant de l'Hypervisor.
3. Importez le fichier image .xva dans l'hyperviseur.
4. Dans l'onglet Console, configurez Citrix ADM avec les configurations réseau initiales. Pour plus d'informations, consultez [Enregistrer et déployer le premier serveur \(nœud principal\)](#) et [Enregistrer et déployer le deuxième serveur \(nœud secondaire\)](#).
5. [Redéployez la paire HA.](#)

### **Citrix ADM prend-il en charge le stockage SAN ?**

Citrix vous recommande d'héberger le disque dur virtuel Citrix ADM sur un stockage local. Lorsqu'il est hébergé sur des périphériques de stockage dans un SAN, Citrix ADM peut ne pas fonctionner comme prévu.

### **Citrix ADM prend-il en charge les disques supplémentaires ?**

Oui. Une nouvelle installation de la paire Citrix ADM HA alloue 120 Go de stockage par défaut. Pour plus de 120 Go de stockage, vous pouvez ajouter un disque supplémentaire pour un maximum de 3 To de stockage. L'ajout de plusieurs disques supplémentaires n'est pas pris en charge.

### **Après avoir désactivé la paire HA, qu'advient-il de l'adresse IP flottante configurée ?**

L'adresse IP flottante ne sera plus accessible et vous devrez redéployer la paire haute disponibilité.

### **Puis-je donner une autre adresse IP flottante pendant le redéploiement ?**

Oui. Vous pouvez configurer une nouvelle adresse IP flottante.

### **Pourquoi l'interface utilisateur du nœud secondaire n'est-elle pas accessible ?**

Le nœud secondaire est uniquement un serveur de réplica en lecture et agit en tant que nœud principal uniquement si le nœud principal est en panne pour une raison quelconque. Citrix recommande d'accéder à l'interface utilisateur du nœud principal ou à l'interface graphique de l'adresse IP flottante.

**Si le nœud principal est hors service pendant une longue période, les configurations peuvent-elles toujours être effectuées à l'aide de l'interface graphique d'adresse IP flottante ?**

Oui. Vous pouvez continuer à effectuer des configurations et les configurations sont enregistrées dans le nœud secondaire. Après le retour du nœud principal, toutes les configurations sont synchronisées.

**S'il est nécessaire de modifier l'adresse IP du nœud principal ou l'adresse IP du nœud secondaire ou l'adresse IP flottante à l'avenir (par exemple, en la changeant en IPv6), quelles sont les solutions recommandées ?**

La modification des adresses IP dans la paire HA n'est pas prise en charge sans casser la paire HA.

Pour mettre à jour l'adresse IP du nœud principal ou du nœud secondaire :

1. Brisez la paire HA. Accédez à **Système > Déploiement**.

La page Déploiement s'affiche. Cliquez sur **Break HA**

- a) Ouvrez une session sur le nœud principal à l'aide d'un client SSH ou à partir de l'hyperviseur.
- b) Utilisez `nsrecover` comme nom d'utilisateur et entrez le mot de passe que vous avez défini.
- c) Entrez **networkconfig**. Exécutez la procédure de l'**étape 3** disponible dans [Enregistrer et déployer le premier serveur \(nœud principal\)](#).  
Lors de la configuration réseau initiale, vous pouvez fournir une adresse IP différente.
- d) Effectuez la même procédure pour le nœud secondaire et continuez avec la procédure de l'**étape 3** disponible dans [Enregistrer et déployer le deuxième serveur \(nœud secondaire\)](#).

Pour mettre à jour l'adresse IP flottante :

1. Accédez à **Système > Déploiement**.

La page Déploiement s'affiche.

- a) Cliquez sur **Paramètres HA**.
- b) Cliquez sur **Configurer l'adresse IP flottante pour le mode haute disponibilité**.
- c) Entrez l'adresse IP flottante et cliquez sur **OK**.

**ADM prend en charge les processeurs AMD ?**

Non ADM ne prend pas en charge les processeurs AMD

## **Déploiement (reprise après sinistre)**

### **Quelle est la fréquence de la réplication entre le site principal et le site de reprise après sinistre ?**

La réplication entre le site principal et le site de reprise après sinistre s'effectue en temps réel.

### **Après avoir lancé le script de sauvegarde sur le site de reprise après sinistre, le site de reprise après sinistre devient-il le site principal temporaire, jusqu'à ce que le site principal soit restauré et pleinement opérationnel ?**

Non. Le site de reprise après sinistre deviendra désormais le site principal.

### **Si l'option Break HA paire est sélectionnée, les deux nœuds fonctionnent comme un serveur autonome. Étant donné que la prise en charge de la reprise après sinistre ne s'applique pas au serveur autonome, qu'advient-il du site DR si la paire Break HA est sélectionnée**

Si vous sélectionnez l'option Break HA pair, la réplication entre le site principal et le site DR est interrompue. Vous devez reconfigurer le site DR dans le cadre du redéploiement de la paire HA.

## **Gestion des événements**

### **Comment puis-je suivre tous les événements qui ont été générés sur mes instances Citrix ADC gérées à l'aide de Citrix ADM ?**

En tant qu'administrateur réseau, vous pouvez afficher des détails tels que les modifications de configuration, les conditions de connexion, les défaillances matérielles, les violations de seuil et les changements d'état d'entité sur vos instances Citrix ADC, ainsi que les événements et leur gravité sur des instances spécifiques. Vous pouvez utiliser le tableau de bord des événements Citrix ADM pour afficher les rapports générés pour les détails de gravité des événements critiques sur toutes vos instances Citrix ADC.

### **Quelles sont les règles de l'événement ?**

À l'aide de Citrix ADM, vous pouvez configurer des règles pour surveiller des événements spécifiques. Les règles d'événement facilitent la surveillance d'un grand nombre d'événements générés dans votre infrastructure Citrix ADM.

Vous pouvez filtrer un ensemble d'événements en configurant des règles avec des conditions spécifiques et en affectant des actions aux règles. Lorsque les événements générés répondent aux critères de filtre de la règle, l'action associée à la règle est exécutée.

Les conditions pour lesquelles vous pouvez créer des filtres sont la gravité, les instances Citrix ADC, la catégorie et les objets de défaillance. Les actions que vous pouvez attribuer aux événements sont l'envoi d'une notification par e-mail, le transfert d'interruptions SNMP depuis les instances Citrix ADC gérées vers Citrix ADM et l'envoi d'une notification par SMS.

## **Gestion des instances**

### **Que sont les centres de données dans Citrix ADM ?**

Un centre de données Citrix ADM est un regroupement logique des instances de Citrix ADC dans un emplacement géographique spécifique. Chaque serveur peut surveiller et gérer plusieurs instances Citrix ADC au sein d'un datacenter. Vous pouvez utiliser le serveur Citrix ADM pour gérer des données telles que syslog, le flux de trafic d'application et les interruptions SNMP à partir des instances gérées. Pour plus d'informations sur la configuration des centres de données, voir Procédure de configuration des centres de données pour les géomaps dans Citrix ADM.

### **Quels sont les différents appareils Citrix pris en charge par Citrix ADM ?**

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

- Citrix MPX
- Citrix VPX
- Citrix SDX
- Citrix CPX
- Citrix Gateway
- Citrix SD-WAN WO
- Citrix SD-WAN PE

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

### **Qu'est-ce qu'un profil d'instance ?**

Un profil d'instance est utilisé par Citrix ADM pour accéder à une instance particulière.

Un profil d'instance contient le nom d'utilisateur et le mot de passe permettant d'accéder à une ou plusieurs instances. Un profil par défaut est disponible pour chaque type d'instance. Par exemple, le profil ns-root-profile est le profil par défaut pour les instances Citrix ADC. Il contient les informations d'identification de l'administrateur Citrix ADC par défaut. Lorsque vous modifiez les informations d'identification requises pour accéder aux instances, vous pouvez définir des profils d'instance personnalisés pour ces instances.

### **Pouvons-nous ajouter un nombre illimité d'instances SD-WAN dans Citrix ADM ? Citrix ADM peut-il gérer tous les compteurs scalaires et vectoriels pour le SD-WAN ?**

Actuellement, il n'existe aucune limite de licence sur les instances SD-WAN pouvant être ajoutées à Citrix ADM. Citrix ADM dispose d'un ensemble de rapports intégrés qui interrogent en interne les compteurs scalaires et vectoriels.

### **Puis-je redécouvrir plusieurs instances Citrix VPX dans Citrix ADM ?**

Oui, vous pouvez redécouvrir plusieurs instances Citrix **VPX** dans Citrix ADM pour connaître les derniers états et configurations des instances.

Accédez à **Réseaux > Instances > NetScaler VPX**, sélectionnez les instances que vous souhaitez redécouvrir, puis dans la liste déroulante **Action**, cliquez sur **Redécouvrir**. Pour plus d'informations, consultez [Comment redécouvrir plusieurs instances VPX](#).

### **Citrix ADM peut-il être installé sur Citrix SDX ?**

Non

## **StyleBooks**

### **Peut-on utiliser StyleBooks pour configurer différentes instances Citrix ADC exécutées sur différentes versions du logiciel Citrix ADC ?**

Oui, vous pouvez utiliser StyleBooks pour configurer différentes instances Citrix ADC exécutées sur différentes versions s'il n'y a pas d'écart entre les commandes d'une version différente.

### **Lorsqu'un StyleBook est utilisé pour configurer plusieurs instances Citrix ADC en même temps et que la configuration d'une instance Citrix ADC échoue, que se passe-t-il ?**

Si l'application de la configuration à une instance Citrix ADC échoue, la configuration n'est plus appliquée et les configurations déjà appliquées sont annulées.

## **Les sauvegardes Citrix ADC effectuées via Citrix ADC incluent-elles des configurations appliquées via StyleBooks ?**

Oui

## **Gestion du système**

### **Puis-je attribuer un nom d'hôte à mon serveur Citrix ADC ?**

Oui, vous pouvez attribuer un nom d'hôte pour identifier votre serveur Citrix ADM. Pour attribuer un nom d'hôte, accédez à **Système > Administration système > Paramètres système**, puis cliquez sur **Modifier le nom d'hôte**.

Le nom d'hôte s'affiche sur la licence universelle pour Citrix ADM. Pour plus d'informations, consultez [Comment attribuer un nom d'hôte à un serveur Citrix ADM](#).

### **Puis-je sauvegarder et restaurer ma configuration Citrix ADM ?**

Oui, vous pouvez sauvegarder les fichiers de configuration (fichiers NTP et certificats SSL), les données système, les données d'infrastructure et d'application, ainsi que tous vos paramètres SNMP. Si votre Citrix ADM devient instable, vous pouvez utiliser les fichiers sauvegardés pour restaurer votre Citrix ADM à un état stable.

Pour sauvegarder et restaurer la configuration de votre Citrix ADM, accédez à **Système > Paramètres avancés > Fichiers de sauvegarde**, puis cliquez sur **Sauvegarder** ou **Restaurer** selon le cas. Pour plus d'informations, consultez [Comment sauvegarder et restaurer la configuration sur Citrix ADM](#).

Citrix vous recommande d'utiliser cette fonctionnalité avant d'effectuer une mise à niveau ou pour des raisons de précaution.

### **Que sont les seuils et les alertes sur Citrix ADM ?**

Vous pouvez définir des seuils et des alertes pour surveiller l'état d'une instance Citrix ADC et surveiller les entités sur les instances gérées.

Lorsque la valeur d'un compteur dépasse le seuil, Citrix ADM génère une alerte signalant un problème lié aux performances. Lorsque la valeur du compteur revient à la valeur d'effacement spécifiée dans le seuil, l'événement est annulé.

### **Puis-je générer un fichier de support technique pour Citrix ADM ?**

Oui. Citrix vous recommande de générer une archive des données et des statistiques Citrix ADM avant de contacter le support technique pour déboguer un problème. L'archive est un fichier TAR que vous pouvez envoyer à l'équipe de support technique.

Vous pouvez générer un fichier de support technique contenant des journaux de débogage, la durée de collecte des journaux de débogage et des journaux distincts et divers de la base de données Citrix ADM.

Pour configurer et envoyer un fichier de support technique, accédez à **Système > Diagnostics > Support technique**, puis cliquez sur Générer un fichier de support technique. Pour plus d'informations, consultez [Comment générer un fichier de support technique pour Citrix ADM](#).

### **Qu'est-ce que la purge de syslog ?**

Syslog est un protocole standard pour la journalisation. Syslog permet d'isoler le système qui génère les informations et le système qui stocke les informations. Vous pouvez consolider les informations de journalisation et obtenir des informations à partir des données collectées. Vous pouvez également configurer syslog pour consigner différents types d'événements.

Pour limiter la quantité de données syslog stockées dans la base de données, vous pouvez spécifier l'intervalle suivant lequel vous souhaitez purger les données syslog. Vous pouvez spécifier le nombre de jours après lesquels toutes les données Syslog génériques, AppFirewall et Citrix Gateway seront supprimées de Citrix ADM.

### **Puis-je configurer le serveur NTP sur Citrix ADM ?**

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

Pour configurer un serveur NTP, accédez à **Système > Serveurs NTP**, puis cliquez sur **Ajouter**. Pour plus d'informations, consultez [Comment configurer le serveur NTP sur Citrix ADM](#).

### **À partir de quelle version le déploiement HA actif-passif Citrix ADM est-il pris en charge ?**

Le mode de déploiement HA actif-passif de Citrix ADM est pris en charge à partir de Citrix ADM version 12.0 build 51.24.

**J’avais une configuration HA active-active Citrix ADM et j’avais configuré une appliance Citrix ADC avec un serveur virtuel d’équilibrage de charge dessus pour un accès unifié à l’interface utilisateur graphique. Comment mettre à jour cette configuration ?**

Après avoir mis à niveau la paire Citrix ADM HA en mode actif-passif, vous devez exécuter la commande suivante sur l’appliance Citrix ADC pour mettre à jour la configuration de l’équilibrage de charge :

```
add lb monitor MAS_Monitor TCP-ECV -send "GET /mas_health HTTP/1.1\r\nAccept-Encoding: identity\r\nUser-Agent: NetScaler-Monitor\r\nConnection: close\r\n\r\n"-recv "{\n"status-code":0, "is_passive":0}"-LRTM DISABLED
```

**Puis-je configurer l’équilibrage de charge de la paire Citrix ADM HA sur une instance Citrix ADC à l’aide du port 443 ?**

Non, vous ne pouvez pas configurer l’équilibrage de charge de la paire Citrix ADM HA sur une instance Citrix ADC à l’aide du port 443.

Lorsque vous configurez les moniteurs [http-ecv](#) et [https-ecv](#) sur Citrix ADC, il ne surveille pas correctement les nœuds Citrix ADM HA.

**Un fichier de sauvegarde du serveur Citrix ADM peut-il être utilisé pour restaurer la configuration d’un autre serveur Citrix ADM ?**

Oui

**Une fois que Citrix ADM a sauvegardé une instance Citrix ADC, ce fichier de sauvegarde peut-il être utilisé pour restaurer la configuration d’une autre instance Citrix ADC via Citrix ADM ?**

Oui. Téléchargez le fichier de sauvegarde Citrix ADM, téléchargez-le dans le référentiel de sauvegarde d’une autre instance Citrix ADC et restaurez cette instance. Assurez-vous que les informations réseau et les informations d’authentification ne sont pas en conflit. Par exemple, vérifiez les conflits d’adresse IP ou de port, ainsi que les profils de mots de passe incompatibles. Assurez-vous également que l’instance VPX restaurée possède la même adresse NSIP et la même licence Citrix ADC que celle qui a été sauvegardée.

Avant de restaurer une instance dans une paire de haute disponibilité, assurez-vous que les adresses IP et l’état (primaire ou secondaire) stockés dans le fichier de sauvegarde correspondent à ceux de la configuration HA d’origine. Vérifiez également que les nouvelles licences principales et secondaires possèdent le même type de licence Citrix ADC.



**Pouvons-nous forcer Citrix ADM à utiliser une adresse SNIP pour communiquer avec les instances Citrix ADC, au lieu d'utiliser l'adresse NSIP du serveur Citrix ADM ?**

Oui, vous pouvez ajouter une adresse SNIP (avec la gestion activée) dans Citrix ADM pour la communication avec les instances Citrix ADC.

**Lorsque je sauvegarde des instances Citrix ADC dans Citrix ADM, le résultat est-il une sauvegarde complète ou une sauvegarde de base ?**

Les sauvegardes des instances de Citrix ADC par Citrix ADM sont des sauvegardes complètes.

**Existe-t-il un guide de dépannage pour Citrix ADM ?**

Oui. Voir <https://support.citrix.com/article/CTX224502>.

**Comment les instances Citrix ADC sont-elles gérées lors d'un basculement sur incident Citrix ADM HA ?**

Si la vérification basée sur les pulsations et SSH échoue, le nœud principal est considéré comme inactif et le nœud secondaire prend le relais en tant que nœud principal. Toutes les instances de Citrix ADC sont mises à jour avec les derniers détails du nœud principal comme destination d'interruption SNMP par défaut.

Le nouveau nœud principal (actif) Citrix ADM vérifie si le nœud précédemment actif a été configuré en tant que collecteur AppFlow ou serveur syslog. Le cas échéant, 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 Citrix ADM HA qui est tombé en panne revient en panne ?**

Après la remise en service, le nœud Citrix ADM reste passif sauf si le nœud actif bascule

**Comment les instances Citrix ADC sont-elles distribuées sur les nœuds Citrix ADM HA ?**

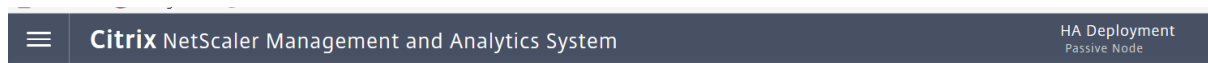
Toutes les instances Citrix ADC sont gérées par le nœud Citrix ADM principal.

### **Comment les licences de serveurs virtuels sont-elles gérées en cas de basculement de Citrix ADM HA ?**

Si le nœud principal Citrix ADM sur lequel les licences de serveur virtuel sont appliquées tombe en panne, le nouveau nœud principal gère les licences de serveur virtuel pendant une période de grâce de 30 jours. Les licences doivent être réappliquées sur le nouveau primaire avant la fin de la période de grâce. Pour d'autres solutions, contactez le support Citrix.

### **Un équilibreur de charge est-il obligatoire pour une installation Citrix ADM HA ?**

Non, mais s'il n'y a pas d'équilibrage de charge, les nœuds Citrix ADM doivent être accessibles via leurs propres adresses IP. Le nœud passif est marqué par la balise « Passif », et Citrix recommande de ne pas créer de configuration sur le nœud passif.



### **Citrix ADM prend-il en charge une base de données externe ?**

Non

### **Une instance Citrix ADC gérée par Citrix ADM peut-elle être utilisée comme équilibreur de charge pour Citrix ADM HA ?**

Oui

### **Quelles données sont synchronisées entre les nœuds Citrix ADM HA ?**

La base de données Citrix ADM complète est synchronisée et les dossiers suivants sont synchronisés :

- /var/mps/tenants/root/
- /var/mps/ns\_images/
- /var/mps/sdx\_images/
- /var/mps/xen\_nsvpx\_images/
- /var/mps/cbwanopt\_images/
- /var/mps/sdwanvw\_images/
- /var/mps/mps\_images/
- /var/mps/ssl\_certs/
- /var/mps/ssl\_keys/

- /mpsconfig/ssl/
- /var/mps/sauvegarde/
- /var/mps/esx\_nsvpx\_images/
- /var/mps/locdb/



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).

---