Citrix Application Delivery Management service

Machine translated content

Disclaimer

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

Contents

Généralités

April 29, 2021

Citrix Application Delivery Management (anciennement NetScaler Management and Analytics Service) est une solution Web permettant de gérer tous les déploiements Citrix, y compris Citrix ADC MPX, Citrix ADC VPX, Citrix ADC SDX, Citrix ADC CPX, Citrix ADC BLX, Citrix Gateway, Citrix Secure Web Gateway et Citrix SD-WAN déployées sur site ou sur le cloud.

Vous pouvez utiliser cette solution cloud pour gérer, surveiller et dépanner l'ensemble de l'infrastructure de livraison d'applications globales à partir d'une console unique, unifiée et centralisée basée sur le cloud. Citrix Application Delivery Management (ADM) fournit toutes les fonctionnalités nécessaires pour configurer, déployer et gérer rapidement la livraison des applications dans les déploiements Citrix ADC et dispose d'une analyse complète de l'intégrité, des performances et de la sécurité des applications.

Citrix ADM offre les avantages suivants :

- **Agile** — Facile à utiliser, à mettre à jour et à consommer. Le modèle de service de Citrix ADM est disponible sur le cloud, ce qui facilite l'utilisation, la mise à jour et l'utilisation des fonctionnalités fournies par Citrix ADM. La fréquence des mises à jour, combinée à la fonctionnalité de mise à jour automatisée, améliore rapidement votre déploiement Citrix ADC.
- **Temps de mise en valeur plus** rapide — Atteinte plus rapide des objectifs commerciaux. Contrairement au déploiement local traditionnel, vous pouvez utiliser votre service Citrix ADM en quelques clics. Vous économisez non seulement le temps d'installation et de configuration, mais vous évitez également de perdre du temps et des ressources sur les erreurs potentielles.
- **Gestion multisite** : panneau unique pour les instances dans les datacenters multi-sites. Avec Citrix ADM, vous pouvez gérer et surveiller les Citrix ADC qui sont dans différents types de déploiements. Vous disposez d'une gestion unique pour les ADC Citrix déployées sur site et dans le cloud.
- **Efficacité opérationnelle** — Une façon optimisée et automatisée d'atteindre une productivité opérationnelle plus élevée. Avec Citrix ADM, vos coûts d'exploitation sont réduits en économisant du temps, de l'argent et des ressources sur la maintenance et la mise à niveau des déploiements matériels traditionnels.

Fonctionnement de Citrix ADM

Citrix ADM est disponible en tant que service sur Citrix Cloud. Après vous être inscrit à Citrix Cloud et avoir commencé à utiliser le service, installez les agents dans votre environnement réseau ou lancez l'agent intégré dans les instances. Ajoutez ensuite les instances que vous souhaitez gérer au service.

Un agent active la communication entre Citrix ADM et les instances gérées dans votre centre de données. L'agent collecte des données à partir des instances gérées de votre réseau et les envoie à Citrix ADM.

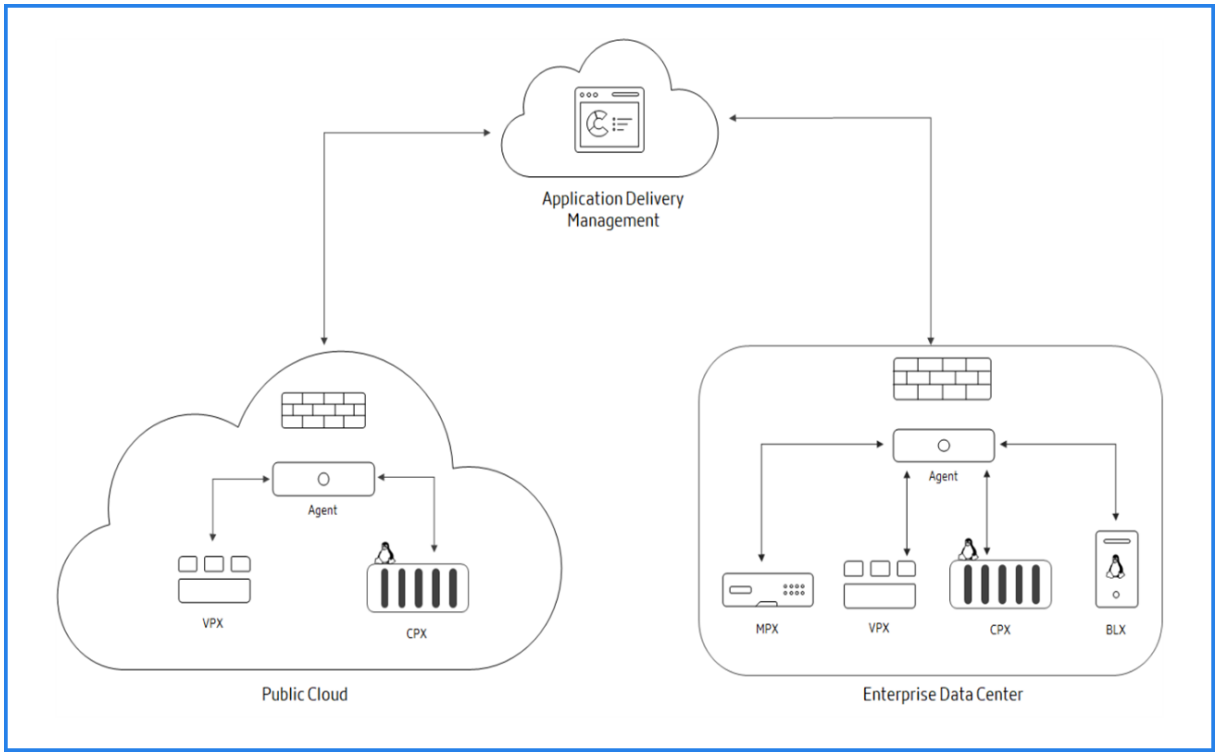
Lorsque vous ajoutez une instance à Citrix ADM, elle s'ajoute implicitement en tant que destination d'interruption et collecte l'inventaire de l'instance.

Le service recueille les détails de l'instance, tels que :

- Nom d'hôte
- Version du logiciel
- Configuration en cours d'exécution et enregistrée
- Certificats
- Entités configurées sur l'instance, etc.

Citrix ADM interroge périodiquement les instances gérées pour collecter des informations.

L'image suivante illustre la communication entre le service, les agents et les instances :



Notes de publication

April 29, 2021

Les notes de mise à jour Citrix Application Delivery Management (Citrix ADM) décrivent les nouvelles fonctionnalités, les améliorations apportées aux fonctionnalités existantes, les problèmes résolus et les problèmes connus disponibles dans une version de service.
Les notes de publication comprennent une ou plusieurs des sections suivantes :

- **Nouveautés** : les nouvelles fonctionnalités, les améliorations apportées aux fonctionnalités existantes et les correctifs disponibles dans la version actuelle.
- **Problèmes connus**: les problèmes qui existent dans la version actuelle et leurs solutions de contournement, le cas échéant.
- **Communiqués précédents**: les nouvelles fonctionnalités et améliorations publiées dans les versions précédentes.

Nouveautés

April 29, 2021

Cette rubrique répertorie les nouvelles fonctionnalités, les améliorations apportées aux fonctionnalités existantes et les correctifs disponibles dans une version.

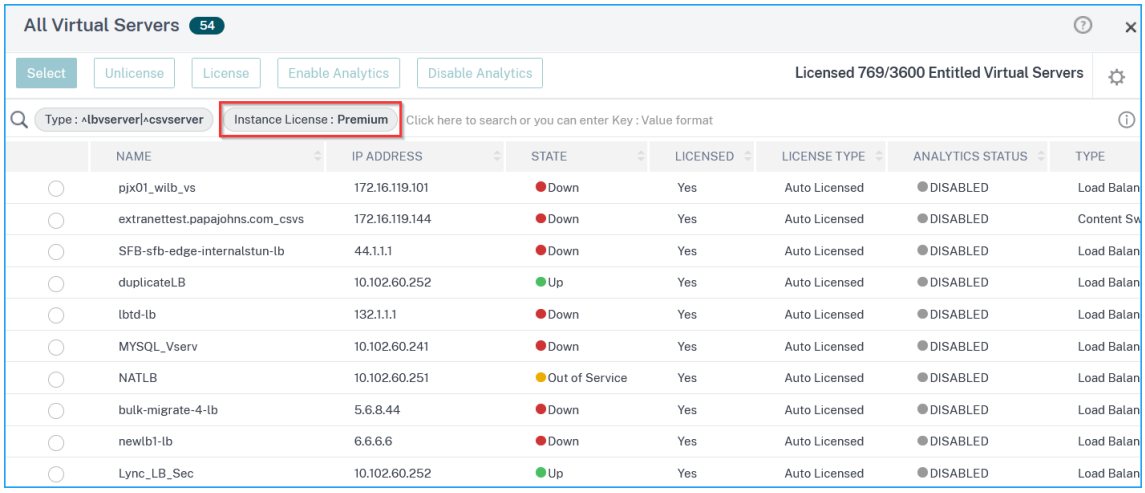
Les agents Citrix Application Delivery Manager (ADM) sont, par défaut, automatiquement mis à niveau vers la dernière version de Citrix ADM. Vous pouvez afficher les détails de l'agent sur la page **Réseaux > Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour de plus amples informations, consultez la section Configuration des paramètres de mise à niveau de l'agent.

Avril 17, 2021

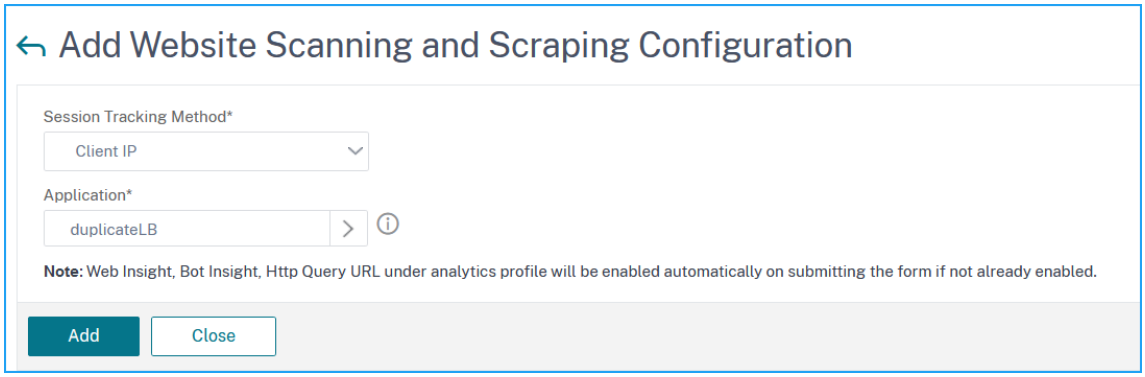
Améliorations apportées aux violations de sécurité

Dans **Analytics > Sécurité > Violations**de sécurité, vous pouvez désormais afficher les améliorations suivantes :

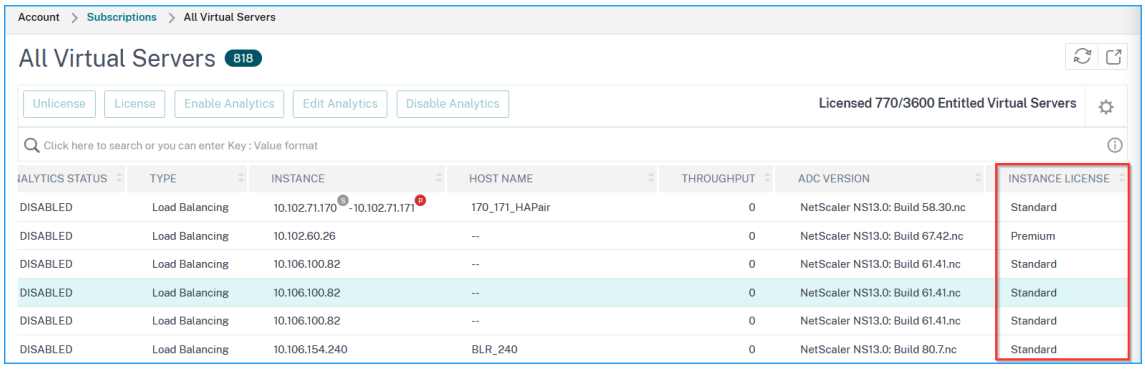
- Lorsque vous activez l'analyse pour les violations de **prise en charge de compte**, d' **analyse de site Web**et de **grattage de contenu**, les **analyses de sécurité avancées** et **Web Insight** paramètres sont également activées automatiquement.
- Dans l'option Paramètres, lorsque vous sélectionnez l'application pour configurer les paramètres requis pour les violations de **prise en charge de compte**, d' **analyse de site Web**et de **grattage de contenu**, le filtre de licence Premium est appliqué. Cette amélioration vous permet de visualiser et de sélectionner uniquement les applications sous licence premium.



- À partir de l'option Paramètres, la page de configuration des prérequis d' **analyse et de raclage de site Web** vous permet de sélectionner d'abord la **méthode de suivi de session**, puis l'application.



- La page **Tous les serveurs virtuels** de **Compte > Abonnements** affiche l'option **Licence d'instance** qui vous permet d'analyser le type de licence de l'instance.



[NSADM-68058]

Afficher les violations de sécurité dans App Dashboard

Dans **Analytics > Sécurité > Violations de sécurité > Présentation de l'application**, les détails de violation que vous avez pu consulter pour WAF et Bot sont désormais disponibles dans le Tableau de **bord des applications**. Accédez à **Applications > Tableau de bord**, sélectionnez une application, puis cliquez sur l'onglet **Sécurité** pour afficher les violations WAF et Bot applicables à l'application sélectionnée.

Outre la visibilité des performances et de l'utilisation de l'application, cette amélioration vous permet également de visualiser les détails de la violation dans une vue à un seul volet.

[NSADM-66876]

Le code couleur de l'adresse IP change dynamiquement pour indiquer l'état de l'instance

Dans l'interface graphique ADM, sous **Réseau > Instances > Citrix ADC**, dans la colonne Adresse IP, les codes de couleur des marques d'adresses IP changent dynamiquement pour indiquer l'état de l'instance. Par exemple, si une instance principale particulière est à l'état « up », le code de couleur de la marque circulaire P pour l'adresse IP correspondante devient vert. En outre, vous pouvez survoler la marque circulaire pour vérifier l'état de l'instance. Auparavant, les codes de couleur pour les adresses IP étaient statiques : bleu pour primaire et gris pour le secondaire.

[NSADM-67681]

Problème résolu

Pour les certificats SSL, l'interface graphique ADM affiche le type d'émetteur comme « Non recommandé », même si les certificats sont configurés dans les paramètres du tableau de **bord SSL**.

[NSHELP-26123]

Mars 30, 2021

Bot Insight - Afficher le message du journal pour la gestion des robots

Dans **Analytics > Sécurité > Violations de sécurité > Vue d'ensemble de l'application**, sous **Bot**, lorsque vous sélectionnez une application et cliquez sur **Journaux** pour afficher les détails du robot, vous pouvez désormais afficher la catégorie de bot identifiée comme signature et l'ID de signature. L'ID de signature vous permet d'analyser si le bot détecté est un bon bot ou un mauvais bot. Pour toute autre catégorie de bot, l'ID de signature affiche N/A.

Pour plus d'informations sur la catégorie et l'ID de signature, reportez-vous à la section Mise à jour de la signature.

[NSADM-63099]

Violation de la sécurité de l'application

Dans **Analytics > Sécurité > Violations de sécurité > Toutes les violations**, vous pouvez désormais afficher la détection dynamique des robots de frappe et de souris sous la catégorie Violation BOT. Pour de plus amples informations, consultez la section Violation de la sécurité.

[NSADM-61855]

Problèmes résolus

- Dans Infrastructure Analytics, le terme de l'interface utilisateur « Paquet abandonné » pour les compteurs de violation SSL (limite de CPU PE, limite PPS, limite de débit, limite de débit SSL, limite de TPS SSL) est désormais remplacé par « brèches de limite de débit ».

  [NSADM-69007]

- Le bundle de support technique généré par ADM ne parvient pas à décompresser.

  [NSHELP-26726]

Mars 17, 2021

Protégez votre organisation à l'aide d'un avis de sécurité

Citrix ADM Security Advisory vous aide à identifier les instances ADC affectées par Citrix Common Vulnerabilities and Exposures (CVE) et à appliquer les correctifs appropriés. L'avis met en évidence les CVE Citrix exposant vos instances ADC à des risques et recommande des mesures d'atténuation et des correctifs. Vous pouvez consulter les recommandations et prendre les mesures appropriées, en utilisant le service ADM pour appliquer les mesures d'atténuation et les correctifs.

Voici les fonctionnalités de l'avis de sécurité :

- Analyse : inclut l'analyse du système par défaut et l'analyse à la demande.
  - Analyse système : analyse toutes les instances gérées par défaut une fois par semaine. ADM décide de la date et de l'heure des analyses du système, et vous ne pouvez pas les modifier.
  - Analyse à la demande : vous permet d'analyser manuellement les instances si nécessaire. Si le temps écoulé après la dernière analyse du système est important, vous pouvez exécuter une analyse à la demande pour évaluer la posture de sécurité actuelle. Ou analyse après une correction ou une atténuation, afin d'évaluer la posture révisée.
- Analyse d'impact CVE : affiche les résultats de tous les CVE ayant un impact sur votre infrastructure et toutes les instances ADC ayant un impact, et suggère des mesures correctives et des mesures d'atténuation. Utilisez ces informations pour appliquer des mesures d'atténuation et de correction afin de corriger les risques de sécurité.
- Rapports CVE : stocke des copies des cinq dernières analyses. Vous pouvez télécharger ces rapports et les analyser.
- Référentiel CVE : offre une vue détaillée de tous les CVE liés à l'ADC annoncés par Citrix depuis décembre 2019 et susceptibles d'avoir un impact sur votre infrastructure ADC. Vous pouvez utiliser cette vue pour comprendre les CVE dans la portée des avis de sécurité et pour en savoir plus sur le CVE.

Pour de plus amples informations, consultez la section Avis de sécurité.

[NSADM-69280]

Nouvelles fonctionnalités ajoutées au flux de travail d'intégration à faible contact Citrix

Le nouveau flux de travail d'intégration à faible contact Citrix est livré avec une interface graphique améliorée avec plusieurs nouvelles fonctionnalités et une meilleure expérience utilisateur. Deux nouveaux onglets, Avis de sécurité et Avis de mise à niveau, sont introduits. Citrix ADM Security Advisory vous avertit des vulnérabilités mettant vos instances ADC en danger et recommande des mesures d'atténuation et des correctifs. Vous pouvez utiliser l'avis de mise à niveau pour vérifier les instances ADC qui approchent de la fin de vie (EOL) ou sur des versions plus anciennes. Nous pouvons mettre à niveau ces CAN vers les dernières versions et bénéficier des dernières améliorations et correctifs. Pour en savoir plus, voir Intégration à faible contact des instances Citrix ADC à l'aide du service Citrix ADM connect.

[NSADM-69280]

Surveiller le cycle de vie des instances ADC à l'aide de l'avis de mise à niveau Citrix ADM

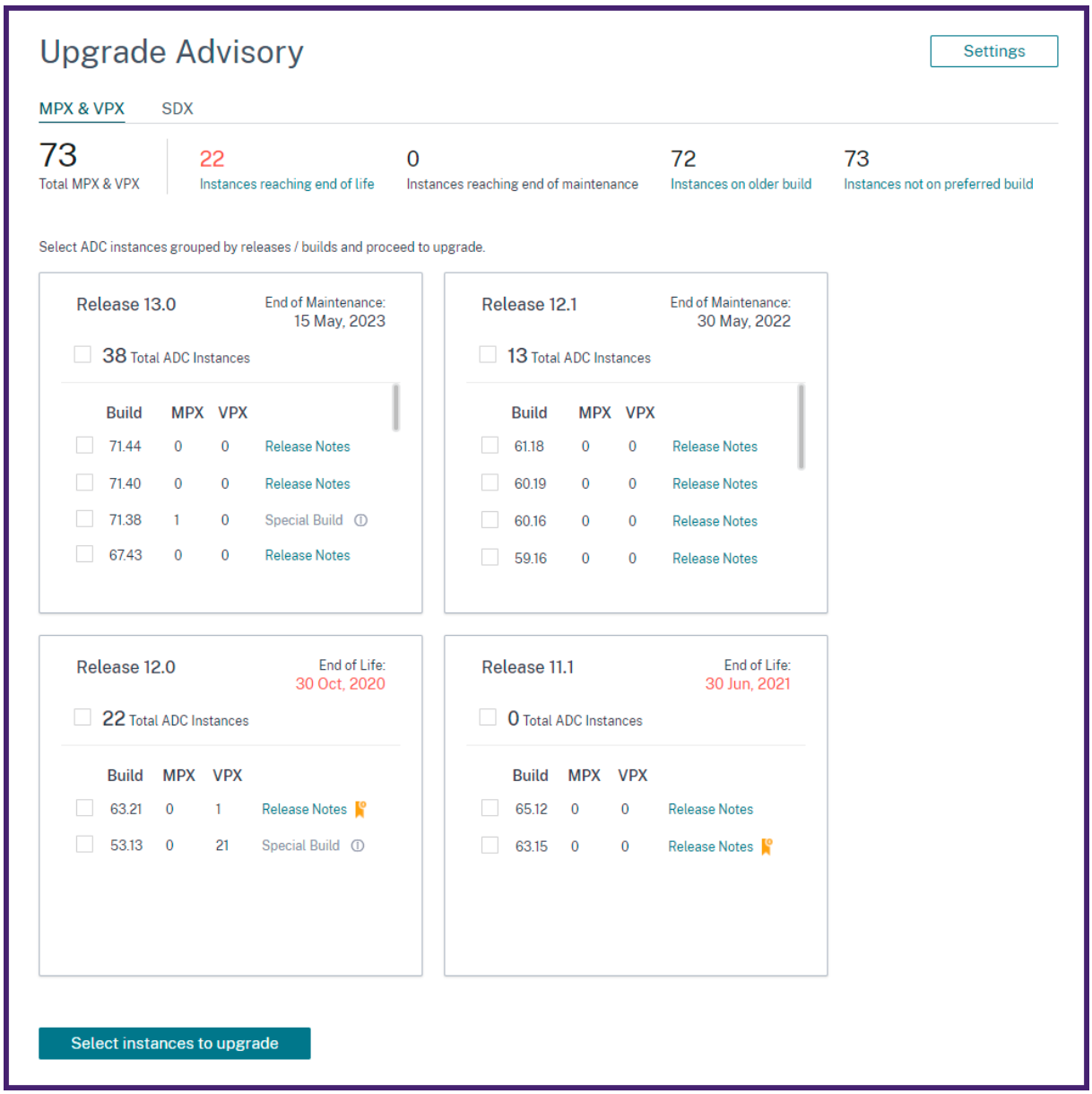
L'avis de mise à niveau Citrix ADM vous aide à surveiller le cycle de vie de vos instances ADC. En tant qu'administrateur réseau, vous pouvez gérer de nombreuses instances exécutées sur différentes ver-

sions d'ADC dans Citrix ADM. La surveillance du cycle de vie de chaque instance ADC peut être une tâche lourde. Pour faciliter ce processus, l'avis de mise à niveau d'ADM fournit les informations suivantes :

- Identifie les instances atteignant ou atteintes EOL ou EOM. Ainsi, vous pouvez planifier les mises à niveau ADC avant la date EOL ou EOM.
- Surligne les instances qui ne sont pas sur la dernière version ou version. Vous pouvez mettre à niveau ces instances vers la dernière version ou la version pour bénéficier de nouvelles fonctionnalités et corrections de bogues.
- Met en surbrillance les instances qui ne sont pas sur les versions ADC préférées. Certaines organisations peuvent avoir des builds ADC préférés pour leurs instances. Dans ADM, vous pouvez définir la version préférée pour votre organisation en fonction des fonctionnalités, des problèmes résolus et d'autres considérations. Ensuite, passez en revue et mettez à niveau les instances qui ne sont pas sur les versions préférées. Les instances exécutant les versions préférées sont indiquées par une icône en étoile.
- Met en surbrillance les instances exécutées sur les versions ou versions les plus populaires. Les instances exécutant les versions populaires sont indiquées par une icône de ruban.

Après avoir examiné les points susmentionnés, vous pouvez continuer à créer un travail de maintenance pour mettre à niveau des instances ADC à partir de la page Avis de mise à niveau.

> L'avis de mise à niveau**important**
>
> ne surveille que l'EOM ou l'EOL des versions du logiciel ADC. Il ne vérifie pas l'EOL des appliances matérielles ADC.



Pour de plus amples informations, consultez la section Avis de mise à.

[NSADM-56646]

Analyser la cause première de la lenteur de l'application

La lenteur des applications est une préoccupation majeure pour toute organisation, car elle entraîne un impact commercial ou une productivité. Dans **Applications > Web Insight**, vous pouvez désormais afficher une nouvelle mesure, Applications with Response Time Anomalies. En utilisant cette mesure, en tant qu'administrateur, vous pouvez analyser si la lenteur de l'application résulte des éléments suivants :

- Latence réseau client

- Latence réseau du serveur
- Temps de traitement du serveur

Pour de plus amples informations, consultez la section Analyser la cause première de la lenteur de l'application.

[NSADM-63170]

03 mars, 2021

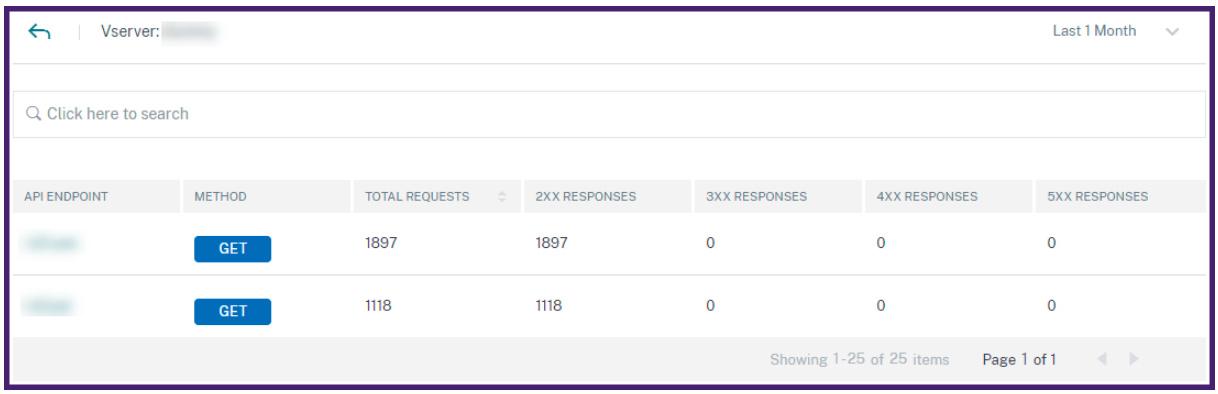
Découvrir les points de terminaison API dans ADM

Vous pouvez désormais découvrir les points de terminaison de l'API qui se trouvent dans votre organisation à l'aide de la passerelle API. Dans Citrix ADM, la page **Applications > passerelle API > Découverte d'API** affiche les points de terminaison d'API qui font partie des instances ADC et des déploiements d'API.

Dans la découverte d'API, lorsque vous sélectionnez un serveur virtuel ou un déploiement d'API, l'interface graphique ADM affiche les points de terminaison de l'API et leurs détails tels que :

- **Méthode** - Il affiche la méthode utilisée dans un point de terminaison API. Par exemple, `GET` et les `POST` méthodes
- **Total requêtes** - Il affiche le nombre de demandes d'API sur le point de terminaison de l'API.
- **Status de réponse** - Il affiche le nombre pour chaque état de réponse. Par exemple, `2xx`, `3xx`, `4xx`, et `5xx`.
- **Found in Spec** - Cette colonne apparaît uniquement pour les déploiements d'API. Parfois, les API internes qui ne font pas partie de la définition de l'API peuvent recevoir du trafic de l'extérieur. Cette colonne vous permet d'identifier si le point de terminaison de l'API et la méthode observée font partie de la définition de l'API.

Serveurs virtuels :

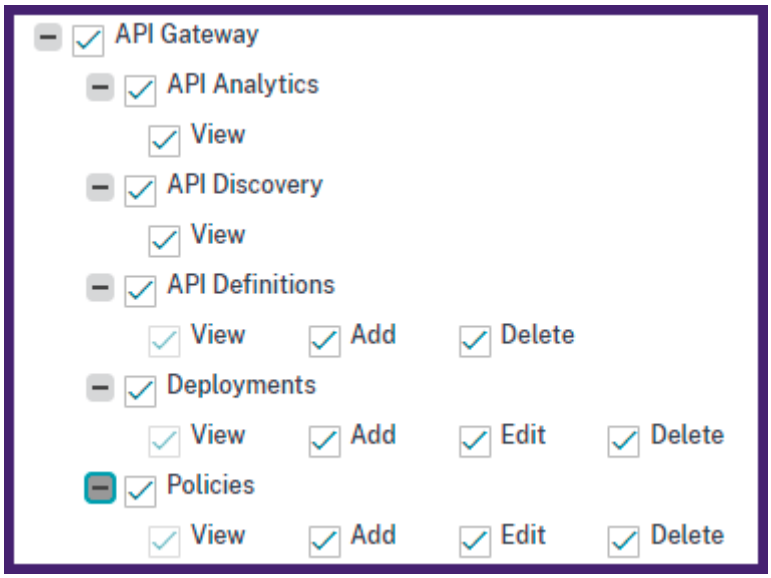


Déploiements d'API :

[NSAPISEC-1234]

Accorder des autorisations de gestion et de configuration de passerelle API

En tant qu'administrateur, vous pouvez créer une stratégie d'accès pour accorder des autorisations utilisateur pour la configuration et la gestion de passerelle API. Les autorisations utilisateur peuvent être afficher, ajouter, modifier et supprimer. Pour ce faire, accédez à **Compte > Administration des utilisateurs > Stratégies d'accès**.



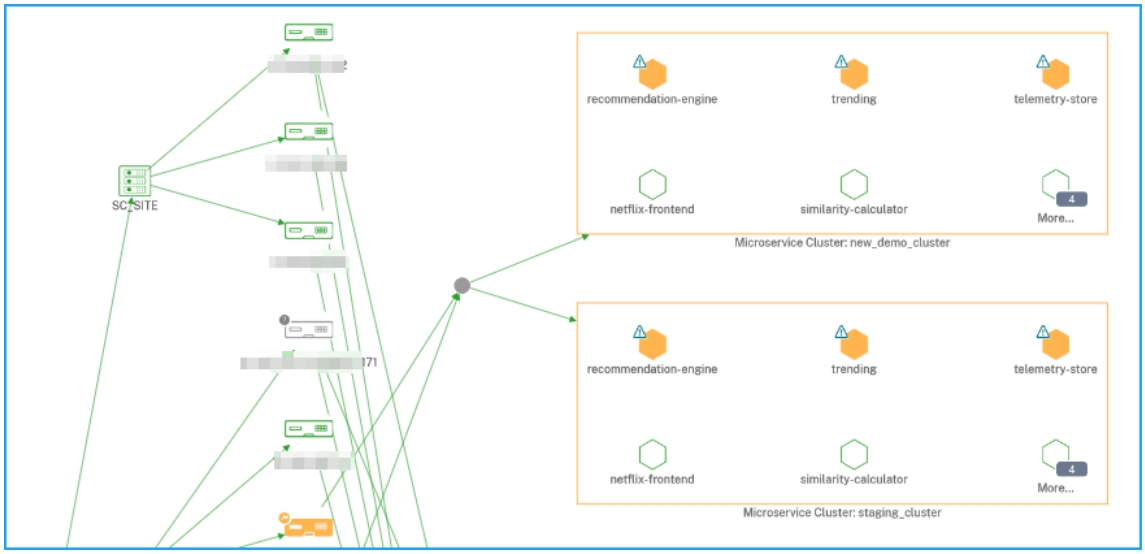
[NSADM-63097]

Graphique des améliorations apportées au service global

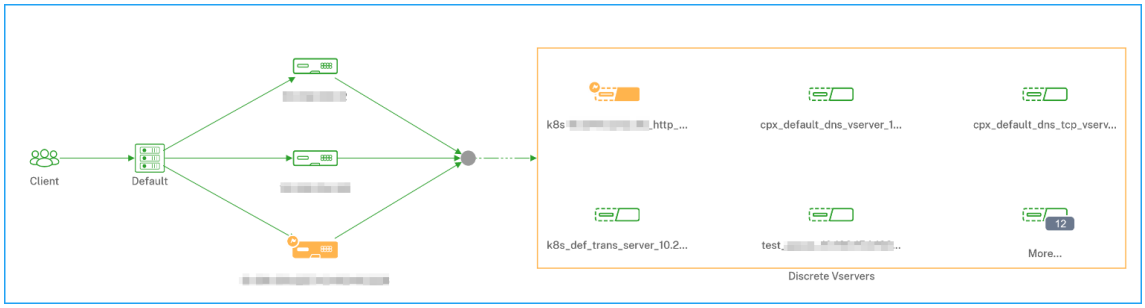
Dans **Applications > Graphique de service > Global**, vous pouvez désormais afficher :

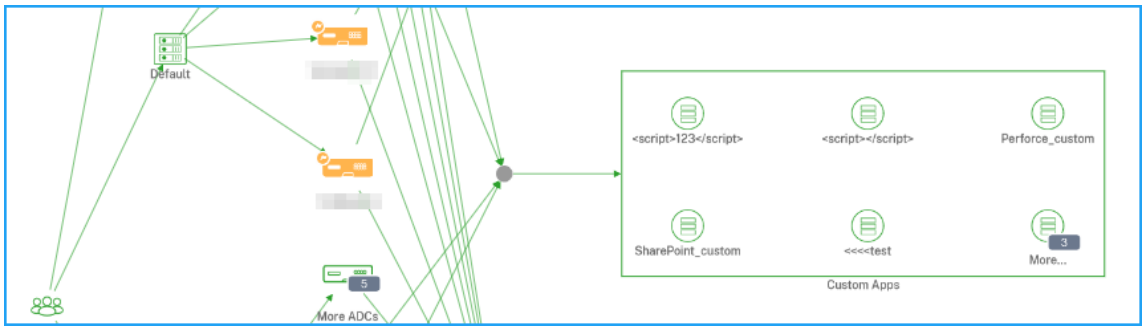
- Les microservices basés sur le nom du cluster.

  > **Remarque**
  >
  > Vous ne pouvez afficher les microservices que pour trois clusters.



- La vue améliorée des serveurs virtuels discrets et des applications personnalisées





Intégration Venafi dans Citrix ADM

Pour maintenir la sécurité numérique, vous devez automatiser la gestion des certificats SSL dans votre environnement. Les certificats SSL expirés peuvent entraîner des risques de sécurité. Vous pouvez désormais configurer les serveurs Venafi Trust Protection Platform pour gérer les certificats SSL à partir de l'interface graphique du service ADM.

Avec l'intégration Venafi, vous pouvez réémettre des certificats et automatiser le renouvellement des certificats installés sur les instances ADC, via l'interface graphique du service ADM. Pour de plus amples informations, consultez la section Automatisation de la gestion des certificats SSL.

[NSADM-58047]

Problèmes résolus

- Lorsque vous créez un travail dans **Réseaux > Travaux de configuration** et sélectionnez la fréquence d'exécution comme jour spécifique d'une semaine ou date d'un mois, le travail planifié ne s'exécute pas en fonction de l'heure spécifiée.

  [NSHELP-26034]

- ADM ne parvient pas à enregistrer ou à mettre à jour sans serveur DNS, lorsqu'un serveur proxy est activé et que l'agent ne parvient pas à obtenir son adresse IP.

  [NSHELP-25835]

- Pour les utilisateurs non administrateurs, les données des services GSLB prennent plus d'une minute pour s'afficher sous **Réseaux > Fonctions réseau > GSLB** dans l'interface graphique ADM.

  [NSHELP-25740]

- Vous recevez des notifications par e-mail sur les seuils du pool de licences, même lorsqu'il n'est pas configuré.

  [NSHELP-25723]

- Dans **Gateway Insight**, lorsque vous planifiez un rapport (**Exporter des rapports > Planifier l'exportation**), le rapport généré affiche **Page introuvable**.

  [NSHELP-25496]

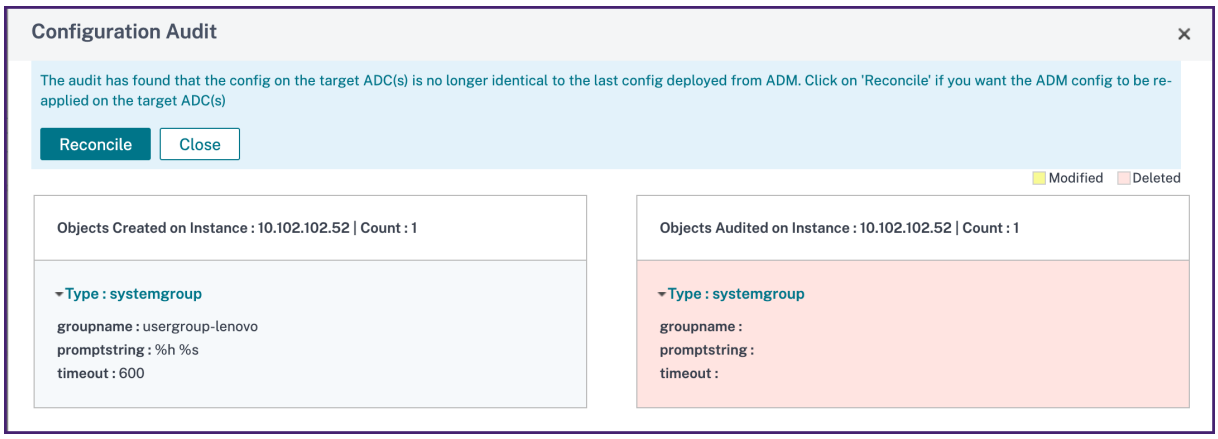
- Parfois, l'interface graphique ADM ne parvient pas à afficher les licences d'instance.

  [NSADM-67697]

11 février 2021

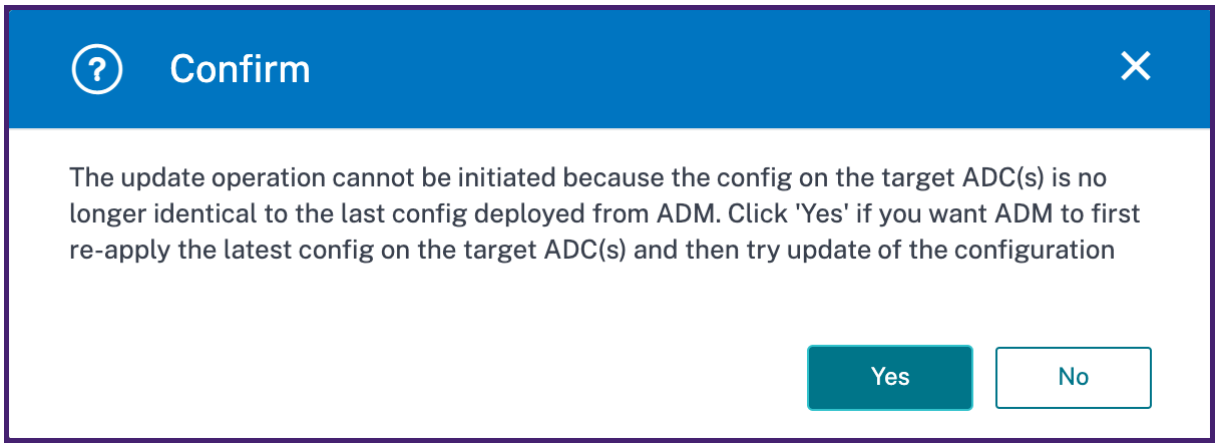
Réconcilier la configuration de votre StyleBook

Lorsque vous vérifiez la configuration ADC avec le pack de configuration StyleBook, vous pouvez désormais concilier les modifications ou les dérives détectées sur l'instance ADC. Cette action restaure la configuration ADC pour qu'elle corresponde à la version du pack de configuration sur ADM.



Considérez que vous avez créé un objet sur l'instance ADC à l'aide de la configuration StyleBook. Si cet objet est supprimé de l'instance ADC, la page **Audit de configuration** identifie la modification et vous permet de la rapprocher. L'action **Réconcilier** restaure l'objet supprimé sur l'instance ADC tel que défini dans le pack de configuration.

Si des modifications ou des dérives détectées lors de la mise à jour du pack de configuration, un message de confirmation s'affiche pour rapprocher les modifications.



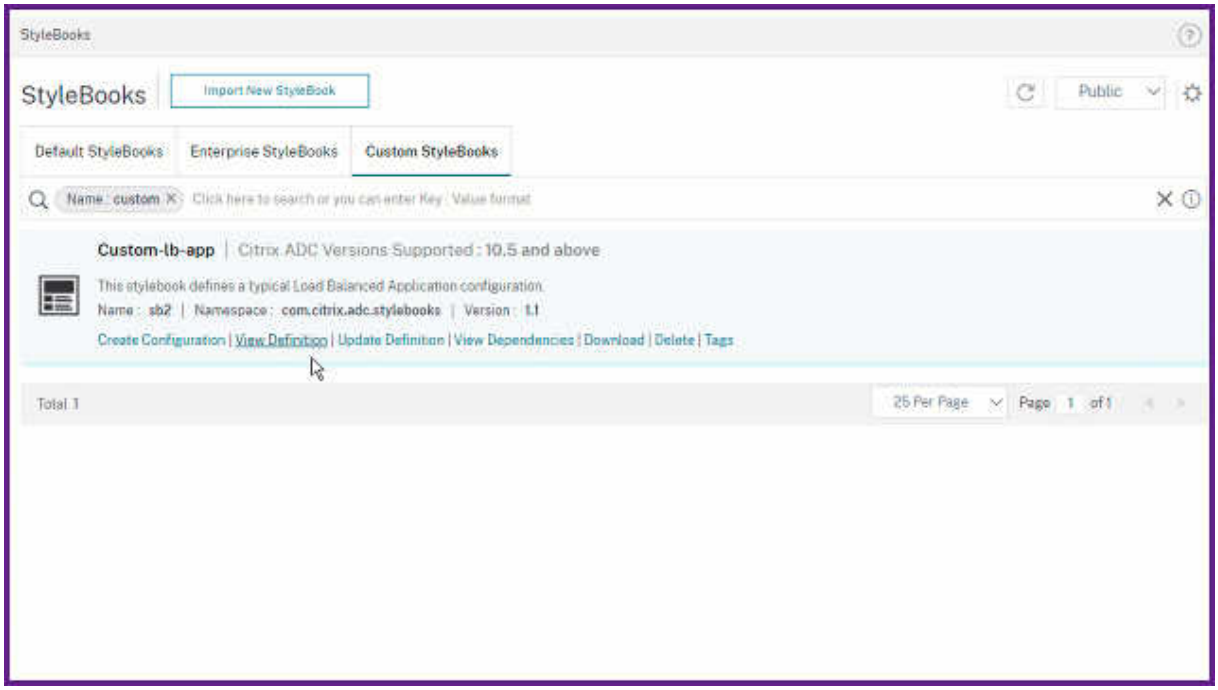
[NSADM-62742]

Mettre à jour les définitions de StyleBook personnalisées dans l'interface graphique

Vous pouvez maintenant mettre à jour une définition StyleBook personnalisée à partir de l'interface graphique ADM elle-même.

> **Remarque**
>
> Avant de mettre à jour la définition StyleBook à partir de l'interface graphique ADM, vérifiez ce qui suit :
>
> - La définition StyleBook n'a pas de StyleBooks dépendants.

- Aucun pack de configuration n'est créé à partir de la définition de StyleBook.



Plus tôt, vous avez dû faire ce qui suit :

1. Téléchargez le StyleBook.
2. Supprimez-le du SMA.
3. Mettez à jour la définition hors connexion.
4. Importez le à ADM.

Avec cette fonctionnalité, vous pouvez mettre à jour la définition en place.

[NSADM-67726]

Nouveau type de données et fonctions IP intégrées à la définition de StyleBook

Les StyleBooks ADM prennent désormais en charge le type de `ipnetwork` données pour faciliter les nouvelles fonctions IP. Ce type de données comporte deux parties. La première partie est l'adresse IP et la deuxième partie est le masque de réseau.

Le masque de réseau est représenté à l'aide d'une longueur de masque de réseau (`netmask-len`) ou d'une adresse IP de masque de réseau (`netmask_ip`). La longueur du masque de réseau est un entier compris entre 0 et 32 et 0 à 128 pour une adresse IPv6. Il est utilisé pour déterminer le nombre d'adresses IP dans un réseau.

Voici les nouvelles fonctions IP intégrées :

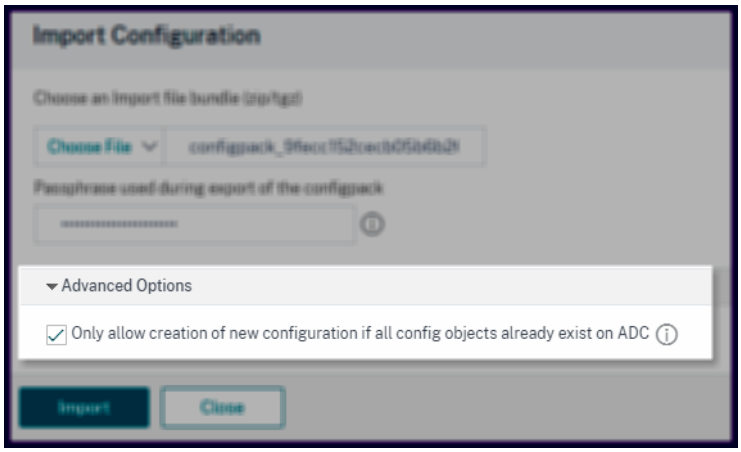
- `ip_network()` : Retourne une notation réseau IP lorsqu'il reçoit l'adresse IP et la longueur du masque réseau en entrée.

- `network_ip()` : Retourne la première adresse IP du réseau IP spécifié.
- `subnets()` : Retourne la liste des sous-réseaux à partir du réseau IP spécifié et de la longueur du masque de réseau.
- `netmask_ip()` : Retourne l'adresse IP du masque de réseau pour le réseau IP spécifié.
- `broadcast_ip()` : renvoie l'adresse IP de diffusion pour le réseau IP spécifié.
- `cidr()` : Retourne une notation CIDR pour le réseau IP spécifié.
- `is_cidr()`: Cette fonction accepte une `ipnetwork` valeur. Et, il renvoie `True` si la valeur spécifiée correspond à la notation CIDR du réseau IP.
- `is_in_network()`: Cette fonction accepte `ipnetwork` et `ipaddress` valorise. Et, il renvoie `True` si l'adresse IP spécifiée existe dans le réseau IP spécifié.

[NSADM-56083]

Introduction d'une option avancée lors de l'importation d'une configuration StyleBook

Dans **StyleBooks > Configurations**, l'option **Importer la configuration** inclut désormais une option avancée. Cette option est utile lorsque vous importez le pack de configuration qui contient déjà les objets de configuration sur l'instance ADC.



Considérez que la même instance ADC est ajoutée sur deux serveurs ADM. Et, l'un des serveurs ADM a déployé un pack de configuration sur cette instance ADC. Si vous souhaitez migrer ce pack de configuration vers un autre serveur (ou vers le service ADM), exportez-le sur votre ordinateur local. Ensuite, utilisez cette option sur le serveur ADM sur lequel vous souhaitez importer le pack de configuration. Cette option l'importe sans redéployer les objets de configuration sur l'instance ADC.

[NSADM-62743]

Afficher l'analyse de l'API pour tout le trafic d'API

La page **Passerelle API > Analytics** d'API affiche désormais toutes les demandes d'API et réponses. Auparavant, cette page affichait uniquement le trafic API qui configurait la limite de débit ou la stratégie

d’authentification.

[NSADM-62936]

Graphique des améliorations apportées au service

Dans le graphique des services Microservices, en tant qu’administrateur, vous pouvez maintenant analyser :

- Nombre d’accès entre les services en fonction de la largeur de l’arête.
- Les raisons des services en examen ou en état critique.

Icône Service	Description
	La largeur de l’arête indique le nombre de coups. Plus la largeur d’arête est grande ou supérieure, indique que le nombre de coups est plus élevé.
	Le service avec une icône d’avertissement indique que le service a des erreurs.
	Le service avec une icône de chronomètre indique que le service présente des problèmes de latence ou de temps de réponse.
	Le service avec des icônes de chronomètre et d’avertissement indique que le service présente à la fois des erreurs et des problèmes de latence/temps de réponse.

> **Remarque**
>
> Si un service n’a pas d’icône d’avertissement ou de chronomètre, il indique que le service présente des anomalies ou une rupture de seuil pour les Hits.

[NSADM-65798]

Problèmes résolus

- Dans **Gateway Insight**, lorsque vous planifiez un rapport (**Exporter des rapports > Planifier l'exportation**), le rapport généré affiche « Page introuvable ».

  [NSHELP-25496]

- Lorsque vous ajoutez une instance ADC dans ADM, si vous sélectionnez SNMP v2 comme profil Citrix ADC, l'adresse IP ADM est ajoutée en tant que gestionnaire SNMP.

  [NSHELP-26245]

- Dans **Réseaux > Travaux de configuration**, le travail de configuration planifié ne s'exécute pas en fonction de l'heure spécifiée lorsque la **fréquence d'exécution** est définie comme suit :

  - Jour spécifique d'une semaine.
  - Date spécifique d'un mois.

  [NSHELP-26034]

- ADM ne parvient pas à s'enregistrer ou à mettre à jour sans serveur DNS lorsque les conditions suivantes sont remplies :

  - Un serveur proxy est activé.
  - L'agent ne parvient pas à obtenir son adresse IP.

  [NSHELP-25835]

- Parfois, l'interface graphique ADM ne parvient pas à afficher les licences d'instance.

  [NSADM-67697]

29 janvier 2021

IPAM affiche les ressources de l'adresse IP allouée

Vous pouvez désormais afficher plus de détails sur les adresses IP allouées à partir d'un réseau IPAM :

- **Module** : Affiche le module ADM qui a réservé l'adresse IP. Par exemple, si l'adresse IP est réservée par StyleBooks, cette colonne affiche StyleBooks comme module.
- **Type de ressource** : Affiche le type de ressource dans ce module. Pour le module StyleBooks, seul le type de ressource configurations utilise le réseau IPAM. Ainsi, il affiche Configurations sous cette colonne.
- **ID de ressource** : affiche l'ID de ressource exact avec un lien. Cliquez sur ce lien pour accéder à la ressource qui utilise l'adresse IP. Pour le type de ressource de configuration, il affiche l'ID du pack de configuration en tant qu'ID de ressource.

[NSADM-62751]

Problèmes résolus

Vous ne pouvez pas supprimer une instance Citrix ADC SDX de Citrix ADM si l'instance est configurée en tant que nom de domaine complet et contient un trait d'union (« - ») dans le nom.
[NSHELP-26022]

ADM ne parvient pas à enregistrer ou à mettre à jour sans serveur DNS, lorsqu'un serveur proxy est activé et que l'agent ne parvient pas à obtenir son adresse IP.
[NSHELP-25835]

January 13, 2021

Graphique des services — Voir les principales tendances métriques des services

Dans le graphique de service, vous pouvez désormais utiliser la vue tabulaire pour voir :

- Mesures clés pour le service
- Mesures clés entre un service source et un service de destination

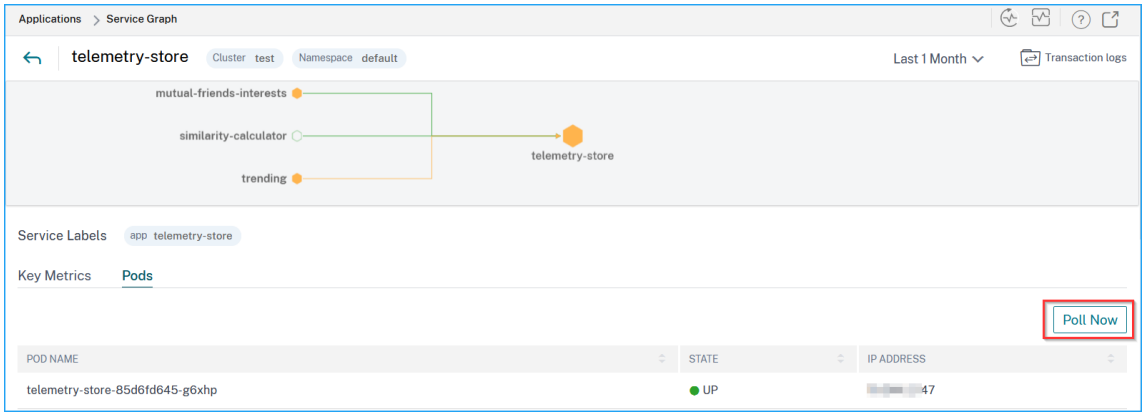
En tant qu'administrateur, à l'aide de ces mesures clés, vous pouvez analyser les tendances des signaux dorés pour la durée sélectionnée. Pour de plus amples informations, consultez la section Afficher les détails du service.

[NSADM-65163]

Graphique de service - Utilisez l'option Sondage maintenant pour obtenir l'état du conteneur

Dans le graphique de service, vous pouvez maintenant utiliser l'option Sondage maintenant pour obtenir le dernier statut du module. L'option Sondage maintenant récupère le dernier état du conteneur à partir du cluster.

1. Cliquez sur un nœud et sélectionnez **Afficher les détails**
2. Dans l'onglet **Pods**, cliquez sur **Sondage maintenant**



[NSADM-62963]

Nouvel attribut StyleBook pour ajouter une liste dynamique

Dans la définition **StyleBook**, vous pouvez maintenant ajouter l' `allow-new-values` attribut pour ajouter une liste dynamique pour un paramètre. Lorsqu'un utilisateur sélectionne ce StyleBook pour créer une configuration, il peut ajouter de nouvelles valeurs à la liste.

Vous pouvez utiliser les `allowed-values` attributs `allow-new-values` et dans une combinaison. Cette combinaison vous permet de définir une liste de valeurs valides pour un paramètre et d'accepter de nouvelles valeurs.

Exemple :

```
-
      name: port
      type: tcp-port
      allowed-values:
            - 80
            - 81
            - 8080
      allow-new-values: true
<!--NeedCopy-->
```

Dans cet exemple, un utilisateur peut choisir entre 80, 81, 8080 ou entrer une nouvelle valeur pour le port de paramètre lors de la création/mise à jour d'un pack de configuration. Pour de plus amples informations, consultez la section Allow-new-values.

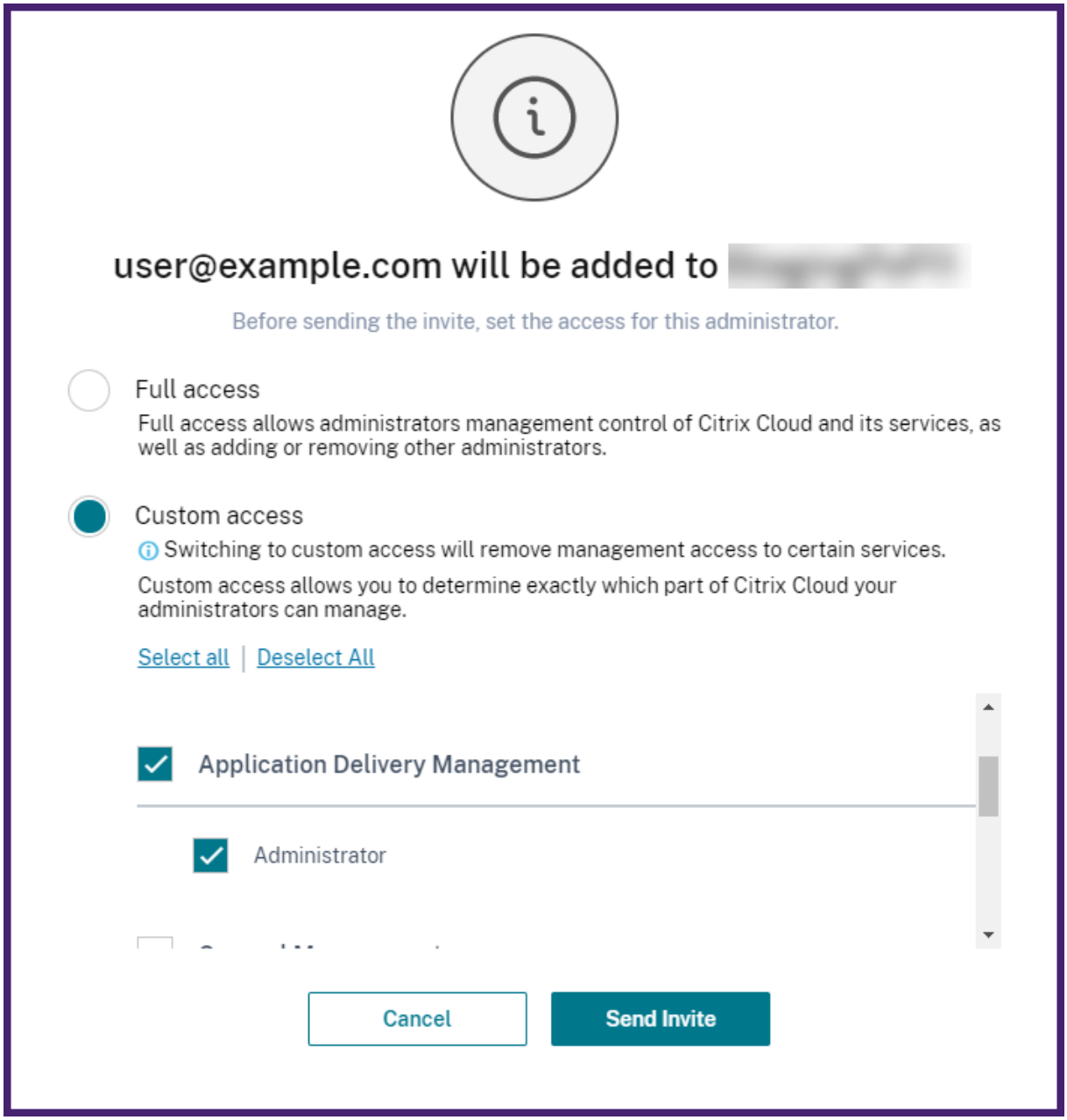
[NSADM-62749]

Inviter des utilisateurs disposant d'un accès personnalisé au service ADM

En tant que super-administrateur, vous pouvez désormais inviter de nouveaux utilisateurs disposant de l'accès personnalisé à utiliser le service ADM. Cette option vous permet de limiter l'accès utilisateur

uniquement au service ADM dans Citrix Cloud. Auparavant, vous n'étiez pas en mesure d'inviter les utilisateurs à accéder uniquement au service ADM. Donc, vous avez dû envoyer une invitation avec l'accès complet.

Pour inviter de nouveaux utilisateurs dans Citrix Cloud, accédez à **Gestion des accès aux identités > Administrateurs**. Dans l'option Accès personnalisé, sélectionnez **Gestion de la livraison des applications**. Par défaut, le rôle **Administrateur** est sélectionné.



Le lien d'invitation est envoyé à l'adresse e-mail de l'utilisateur spécifiée. De plus, l'utilisateur peut se connecter à Citrix ADM avec ce lien en tant qu'administrateur. Avec un accès administratif, l'utilisateur peut effectuer les opérations suivantes :

- Ajoutez et gérez des instances ADC dans ADM.
- Déployez des configurations sur des instances ADC à l'aide de StyleBook.
- Configurez des licences de capacité groupée pour les instances ADC.
- Créez et configurez des groupes de Autoscale.

> **Remarque**
>
> L'administrateur peut accéder à l'interface graphique ADM à partir de Citrix Cloud. Toutefois, la page **Compte > Administration de l'utilisateur** est restreinte. Un super administrateur peut accorder l'accès à cette page si nécessaire.

Pour plus d'informations sur l'envoi d'une invitation et la configuration des utilisateurs, reportez-vous à la section Configurer les utilisateurs sur Citrix ADM.

[NSADM-55384]

Problèmes résolus

- Dans Gateway Insight, le nombre total affiché sous Gateway est incorrect.

  [NSHELP-25729]

- Lorsque vous sélectionnez Enregistrement et lecture sous Source de configuration dans **Réseaux > Travaux de configuration > Créer un travail**, le message d'erreur suivant s'affiche :

  ```
  Unable to get config diff for: <instance IP>
  ```

  [NSADM-63986]

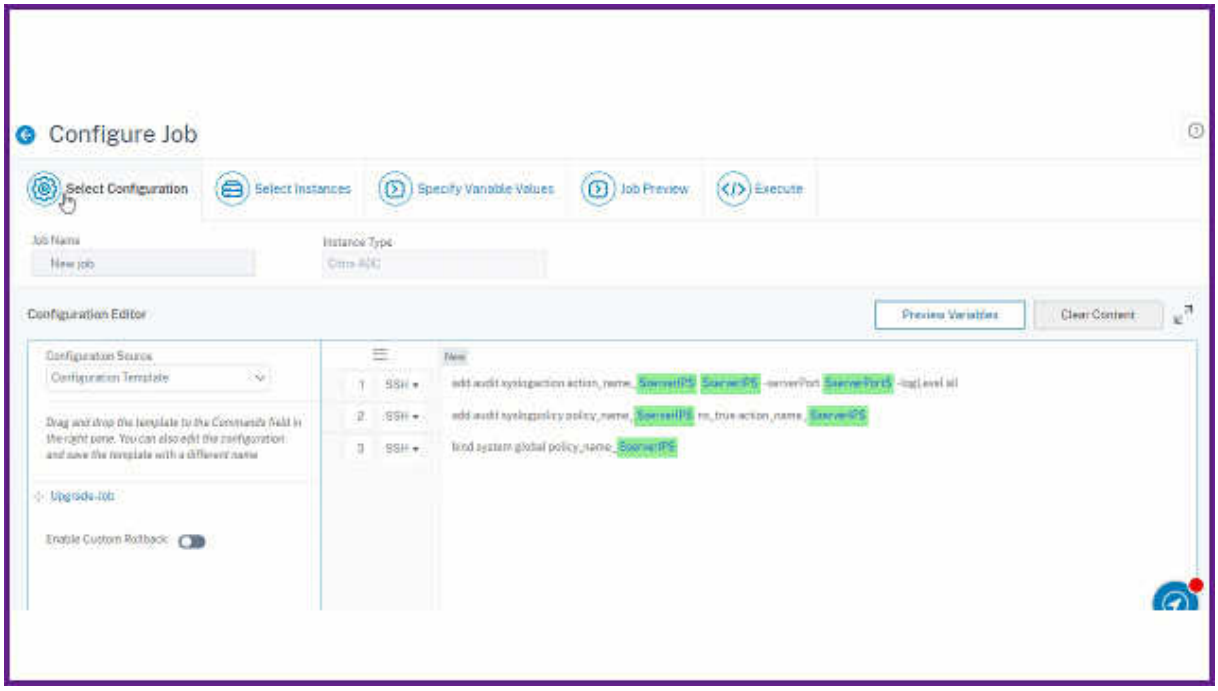
- Si vous fournissez une expression rationnelle non valide dans une application pour un groupe et que vous sélectionnez quelques applications manuellement, les applications sélectionnées manuellement ne sont pas visibles si la regex n'est pas valide.

  [NSHELP-25739]

December 17, 2020

Basculer les onglets d'une tâche de configuration existante

Lorsque vous modifiez une tâche de configuration existante, vous pouvez désormais passer à n'importe quel onglet. Par exemple, si vous êtes dans l'onglet **Sélectionner une configuration**, vous pouvez basculer vers l'onglet **Aperçu des travaux**. Plus tôt, vous étiez en mesure d'aller seulement linéairement à l'onglet suivant. Par exemple, à partir de l'onglet **Sélectionner une configuration**, vous n'avez pu accéder qu'à l'onglet **Sélectionner des instances**.

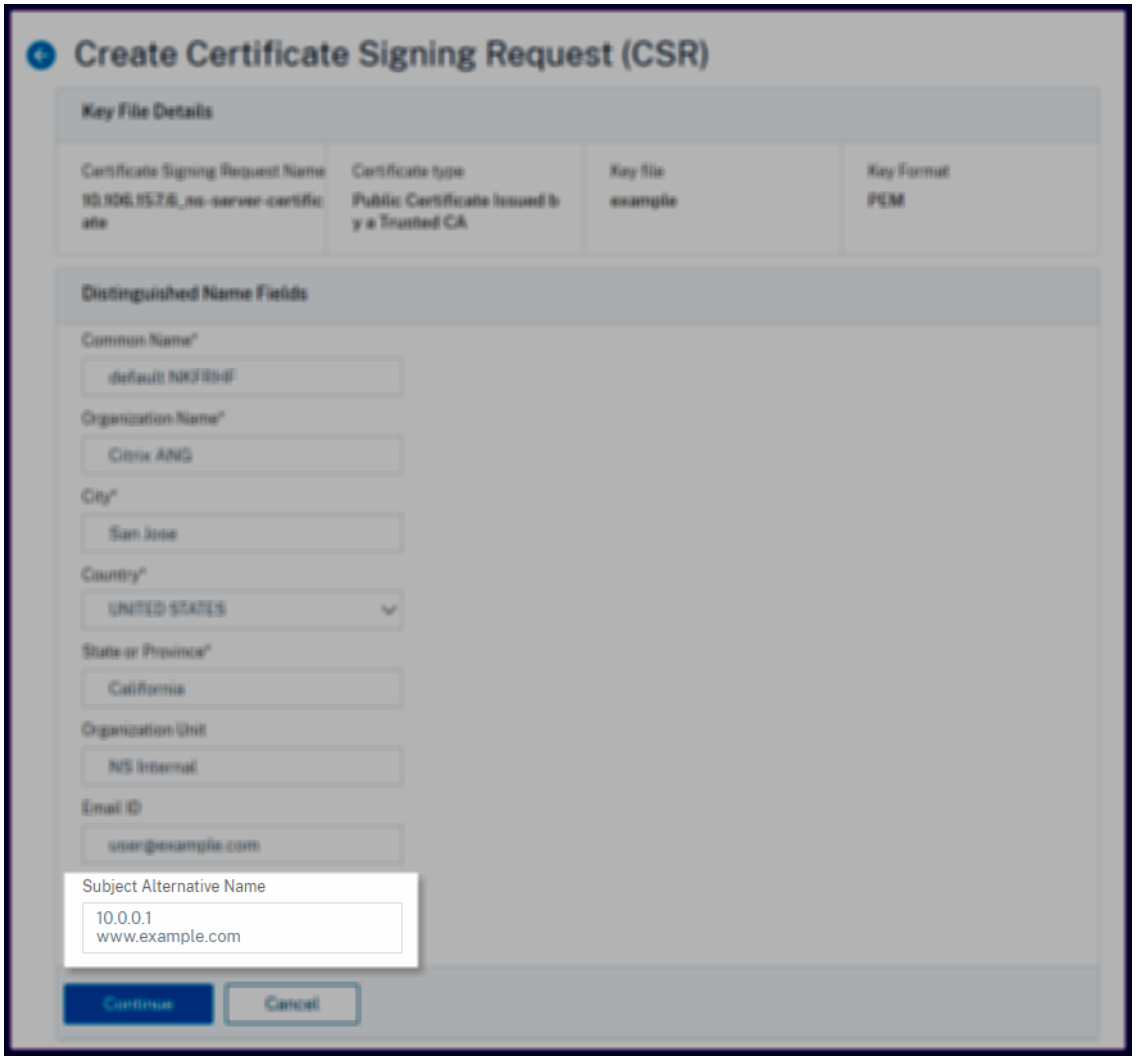


[NSADM-42944]

Créer un CSR avec des noms alternatifs d’objet

Vous pouvez désormais créer une demande de signature de certificat (CSR) avec des noms alternatifs d’objet. Avec cette fonctionnalité, vous pouvez sécuriser plusieurs domaines avec un seul certificat.

Lors d’une création CSR du certificat SSL sélectionné, vous pouvez désormais inclure plusieurs noms alternatifs d’objet. Ces valeurs peuvent être des noms de domaine et des adresses IP. Pour de plus amples informations, consultez la section Créer une demande de signature de certificat (CSR).



[NSADM-51556]

Violation de la sécurité de l'application

Dans Violations de sécurité, vous pouvez désormais afficher la **prise en charge de compte pour Citrix Gateway** sous la catégorie Violation de bot. Pour de plus amples informations, consultez la section Catégories de violation.

[NSADM-57698]

Bot insights - Afficher les catégories de bot pour les applications mobiles (Android)

Dans Bot Insight, vous pouvez désormais afficher les catégories de robots suivantes qui sont détectées via un réseau mobile :

- Limite de débit client Web

- Limite de débit Android
- Périphérique client Web
- Appareil Android

Pour de plus amples informations, consultez la section Perspectives de.

[NSADM-57724]

Problèmes résolus

- Dans **Réseaux > Événements > Récapitulatif**des événements, lorsque vous cliquez sur un événement Citrix ADC SDX, l'interface graphique redirige vers la page Événement mais n'affiche aucune donnée.

  [NSHELP-25630]

- Le service ADM ne respecte pas le délai d'expiration de la session de connexion et l'API de déconnexion. Par conséquent, la session utilisateur reste valide.

  [NSADM-63819]

- Lorsque vous supprimez les utilisateurs de Citrix Cloud, les noms d'utilisateurs supprimés continuent d'apparaître dans Citrix ADM dans **Paramètres** > **Administration** des **utilisateurs > Utilisateurs**.

  [NSADM-5882]

02 décembre 2020

Afficher les anomalies dans l'utilisation de l'application

En tant qu'administrateur, vous devez vérifier comment l'application est utilisée. Les mesures de clé d'application peuvent vous aider à identifier l'utilisation de l'application. Étant donné que la plage de trafic vers l'application est imprévisible, des écarts inhabituels de performances de l'application peuvent survenir pendant une durée spécifique. Dans de tels scénarios, en tant qu'administrateur, vous pouvez voir ces anomalies soudaines et vous assurer que si un dépannage immédiat est nécessaire. Citrix ADM détecte de telles anomalies et fournit les détails nécessaires.

Pour de plus amples informations, consultez la section Utilisation des applications et anomalies.

[NSADM-54677]

Choisir les niveaux de sensibilité pour les violations de sécurité

Pour les violations de connexions client excessives et d'analyse de site Web, vous pouvez désormais créer un profil de vérification du comportement et choisir le niveau de sensibilité comme Faible,

Moyen et Élevé. En créant un profil, vous pouvez décider comment Citrix ADM signale le nombre total d'anomalies pour ces violations.

Pour de plus amples informations, consultez la section Configurer les profils de vérification du comportement.

[NSADM-59536]

Utilisation du processeur de l'application pour calculer le score de l'application

En tant qu'administrateur, vous pouvez désormais surveiller le processeur utilisé par une application. Vous pouvez également configurer des seuils pour l'utilisation du processeur de l'application afin de déterminer le score final de l'application. La page Configurer le score de l'application vous permet de sélectionner **Utilisation du processeur de l'application** et de configurer les valeurs de seuil bas et élevé.

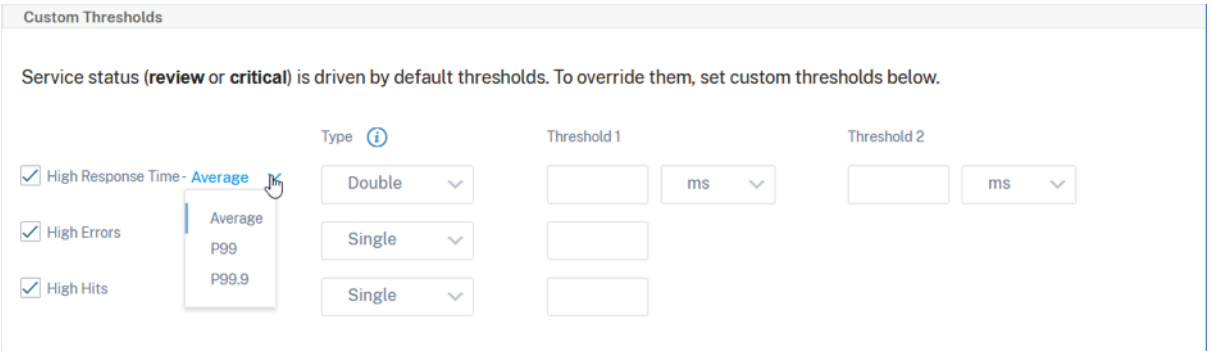
Pour plus d'informations, veuillez consulter Utilisation moyenne de l'UC des applications et Sélectionner les composants du score de l'application et définir des seuils.

[NSADM-57468]

Configurer les seuils dans le graphique de service

Dans le graphique de service, vous pouvez maintenant sélectionner et configurer des seuils pour les mesures suivantes afin de calculer le score et le statut du service :

- Temps de réponse élevé (moyenne, P99 et P99,9)
- Erreurs élevées
- Hits élevés



> **Remarque**
>
> Citrix ADM calcule le score final et le statut du service en fonction des mesures sélectionnées. Par exemple, si vous sélectionnez uniquement Hits élevés pour la configuration du seuil, Citrix ADM

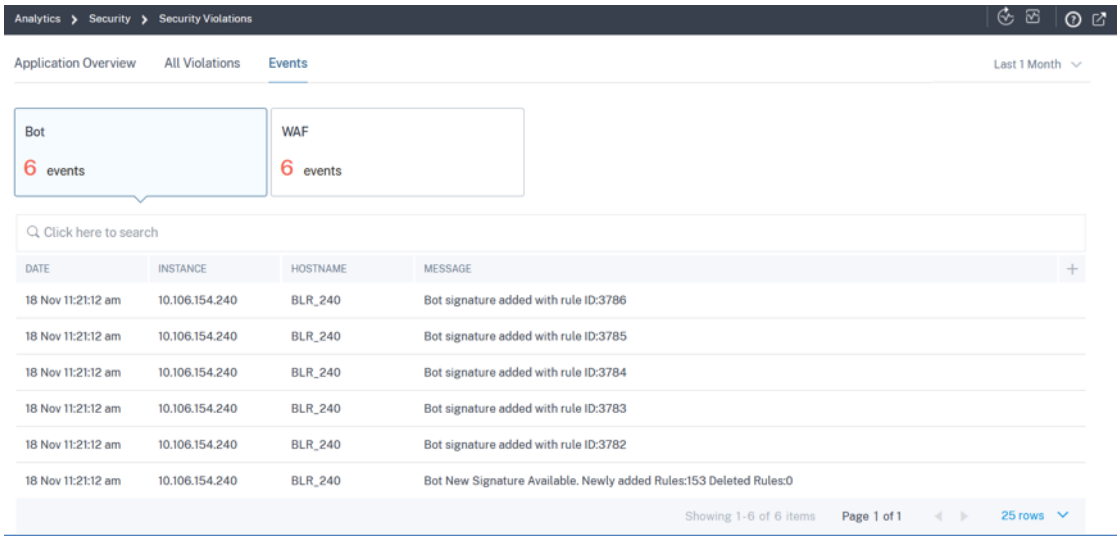
> utilise le seuil par défaut (temps de réponse = 200 ms et nombre d'erreurs = 0) et les résultats élevés pour calculer le score de service.

Pour de plus amples informations, consultez la section Configurer les seuils dans le graphique de service.

[NSADM-59731]

Afficher l'historique des événements dans les violations de sécurité

Dans les violations de sécurité, vous pouvez désormais afficher l'historique des événements pour obtenir des informations sur les robots et des informations sur la sécurité. Accédez à **Analytics > Sécurité > Violations** de sécurité et cliquez sur l'onglet **Événements** pour afficher les événements bot et WAF.



[NSADM-62684]

Amélioration de l'analyse de l'infrastructure

Dans Infrastructure Analytics, quelques mises à jour thématiques sont apportées à l'interface utilisateur afin d'améliorer l'expérience utilisateur.

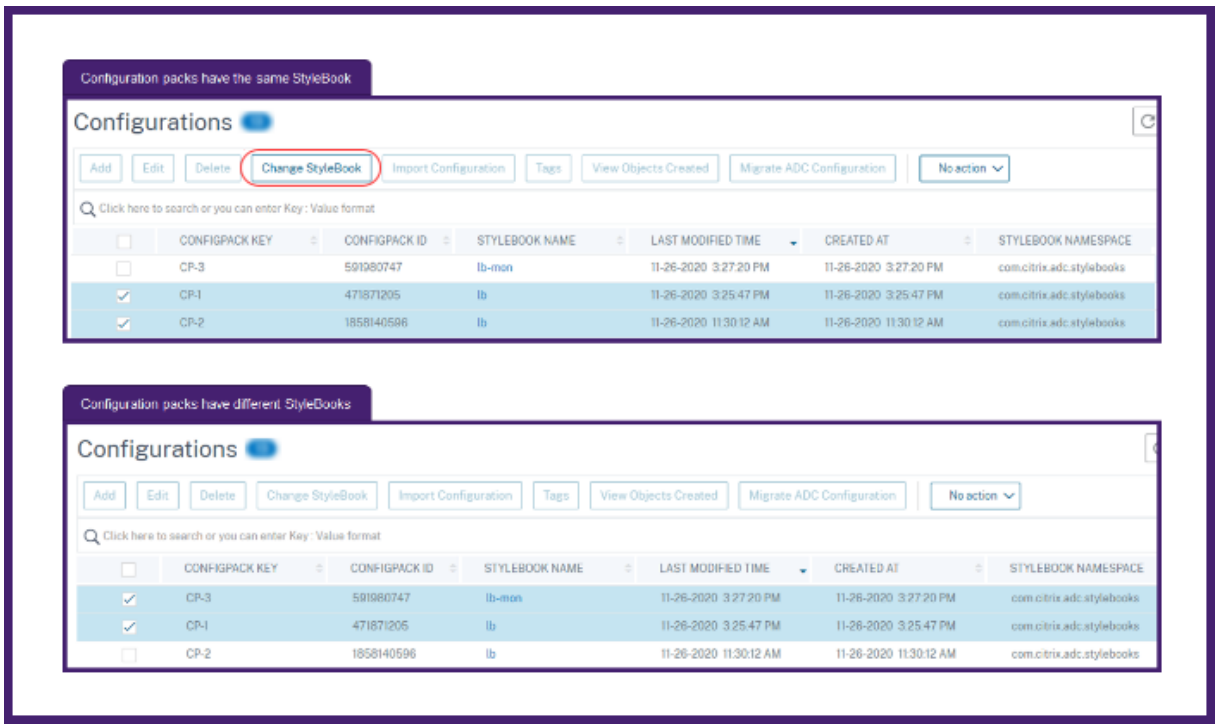
[NSADM-57697]

Modifier le StyleBook de plusieurs packs de configuration à la fois

Vous pouvez maintenant modifier le StyleBook de plusieurs packs de configuration à la fois. Lorsque vous remplacez un StyleBook existant par un nouveau, vous pouvez modifier le StyleBook de tous les

packs de configuration associés ou de plusieurs packs de configuration associés en une seule opération. Auparavant, vous deviez sélectionner chaque pack de configuration un par un pour modifier leur StyleBook.

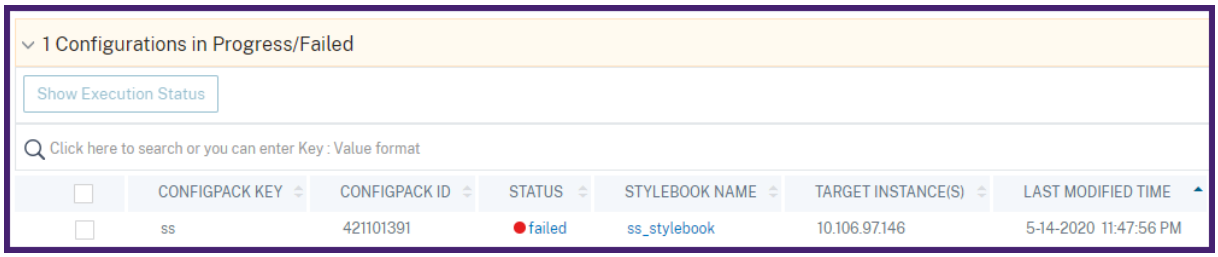
> **Remarque**
>
> Veillez à sélectionner les packs de configuration associés au même StyleBook. Sinon, l'option Modifier le livre de style devient indisponible.



Pour les packs de configuration sélectionnés, l'ADM modifie correctement le StyleBook lorsque les conditions suivantes sont remplies :

- Tous les paramètres de configuration du StyleBook existant doivent être présents dans le StyleBook sélectionné.
- Les nouveaux paramètres du StyleBook sélectionné sont facultatifs.

Pour voir la progression des packs de configuration sélectionnés, sélectionnez **Configurations en cours ou en échec** dans la page **Configurations**.



Pour de plus amples informations, consultez la section Modifier le StyleBook qui comporte plusieurs

packs de configuration.

[NSADM-57941]

Modifier le type d'accès d'une application de Autoscale

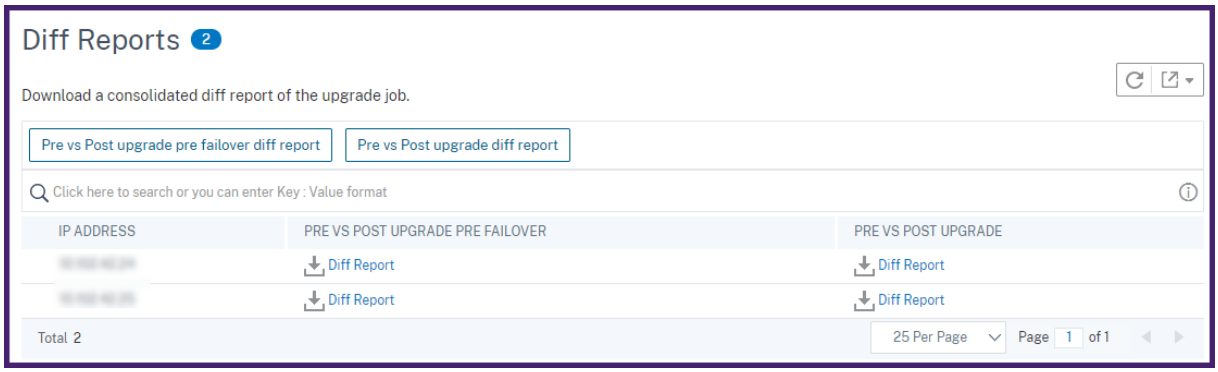
L'ADM prend désormais en charge la modification du type d'accès pour les applications de mise à l'Autoscale qui ont une distribution de trafic DNS ou Route 53. Ainsi, vous pouvez modifier le type d'accès pour toutes les applications de Autoscale.
Auparavant, la modification du type d'accès était prise en charge uniquement pour les applications qui avaient une distribution de trafic ALB ou NLB.

[NSADM-57029]

Télécharger un rapport de diff consolidé d'une tâche de mise à niveau ADC

Vous pouvez désormais télécharger un rapport de diff consolidé d'une tâche de mise à niveau d'ADC. Ce rapport contient les différences entre les sorties du script pré-mise à niveau et post-mise à niveau. Ainsi, vous pouvez déterminer quelles modifications ont eu lieu sur l'instance ADC après la mise à niveau.

> **Remarque**
>
> Le rapport diff n'est généré que si vous spécifiez le même script dans les étapes de pré-mise à niveau et de post-mise à niveau. Par conséquent, veillez à sélectionner Utiliser le même script que Pré-mise à niveau dans les étapes de post-mise à niveau.



Vous pouvez télécharger les types de rapports diff suivants :

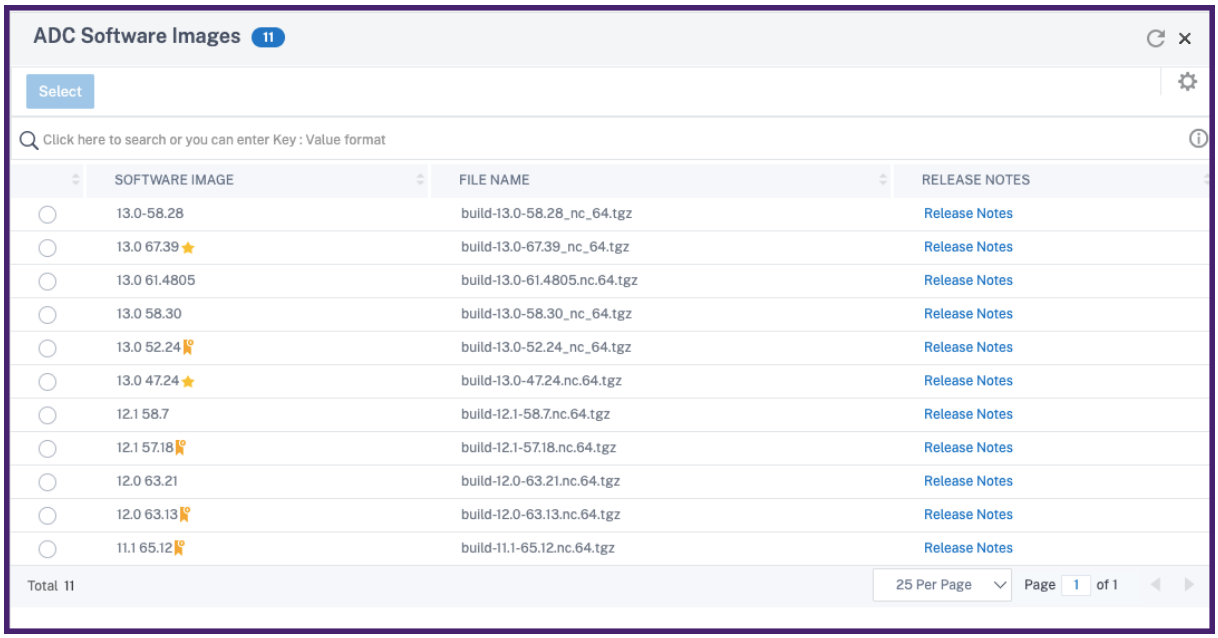
- **Rapport de différentiel pré-basculement avant la mise à niveau et après mise à niveau**
- **Pré c. Rapport sur les diff post-mise à niveau**

Pour de plus amples informations, consultez la section Télécharger un rapport de diff consolidé d'une tâche de mise à niveau ADC.

[NSADM-50200]

Sélectionner une image ADC sans la charger

Lorsque vous créez une tâche de mise à niveau ADC, vous pouvez maintenant sélectionner une image ADC sans la charger. Cette option répertorie toutes les images ADC disponibles sur le site Web Citrix Téléchargements. L'image ADC sélectionnée est téléchargée à partir du service Citrix Download.



Pour de plus amples informations, consultez la section Utiliser les tâches pour mettre à niveau les instances de Citrix ADC.

[NSADM-52471]

Problème résolu

Lorsqu'un utilisateur accède à la page **Abonnement** et clique sur **Licence**, l'erreur **Non autorisé** s'affiche, même si l'utilisateur dispose d'autorisations d'affichage ou de modification sur la page **Abonnement**.

[NSHELP-25351]

Le service ADM ne respecte pas le délai d'expiration de la session de connexion et l'API de déconnexion. Par conséquent, la session utilisateur reste valide.

[NSADM-63819]

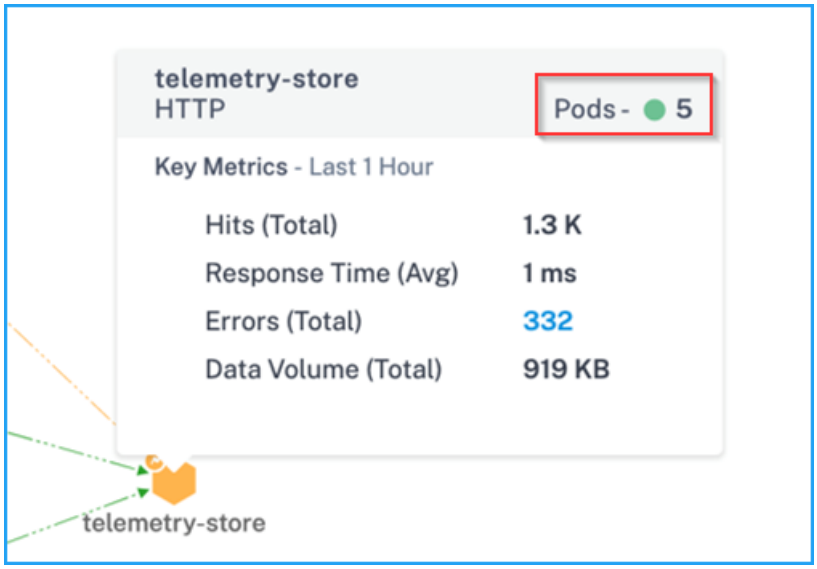
Dans **Analytics > Sécurité > Violations**de sécurité, l'indicateur de **connexions client excessives** n'affiche pas d'anomalies même lorsque le volume élevé de connexions client est reçu.

[NSADM-64548]

11 novembre 2020

Graphique de service — Affiche tous les détails du module back-end associé

Dans le graphique de service, lorsque vous placez le pointeur de la souris sur un service, vous pouvez désormais afficher le nombre total de pods associés au service.



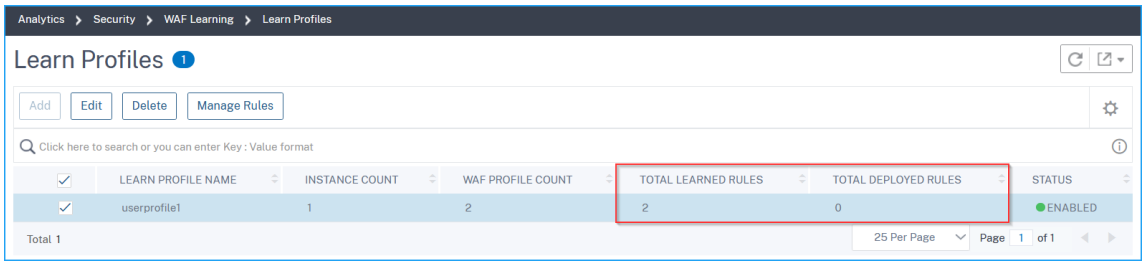
Pour de plus amples informations, consultez la section Afficher les détails du service.

[NSADM-47395]

Améliorations du moteur d'apprentissage WAF

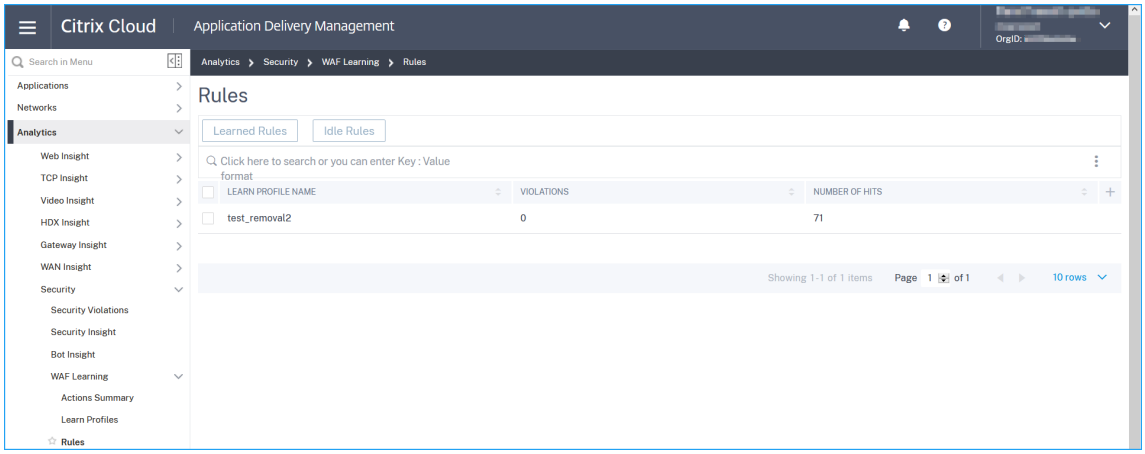
Dans le moteur d'apprentissage WAF, vous pouvez désormais afficher les améliorations suivantes :

- Dans la page **Apprendre les profils**, vous pouvez afficher les règles **totales acquises et les règlestotales déployées**.

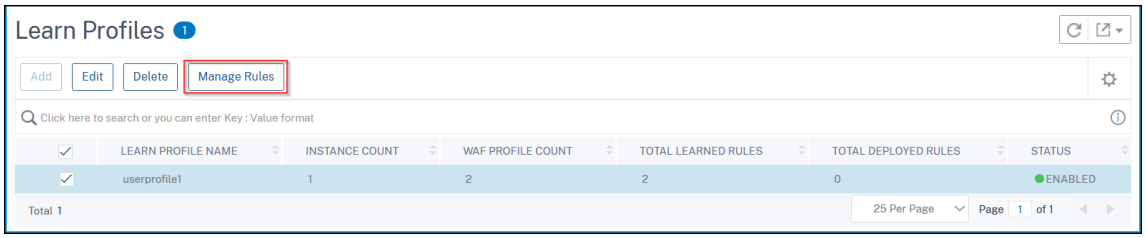


- La page **Règles** n'est plus disponible. L'option **Gérer les règles** est ajoutée à la page **Apprendre les profils**. Les informations pertinentes sur les règles apprises, les règles d'inactivité et les règles déployées sont accessibles en sélectionnant le nom du profil et en cliquant sur le bouton **Gérer les règles**.

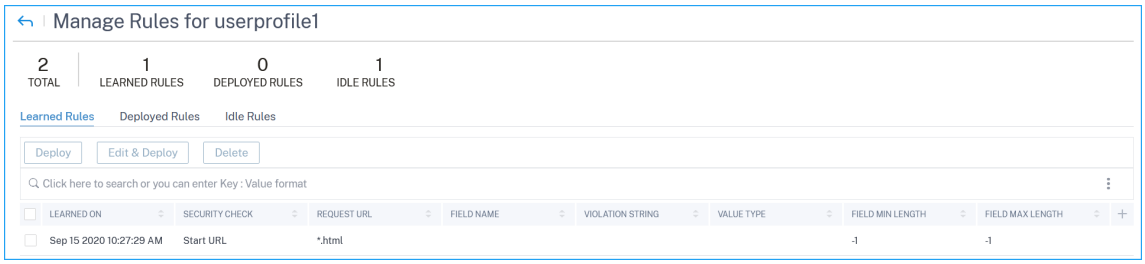
  Plus tôt :



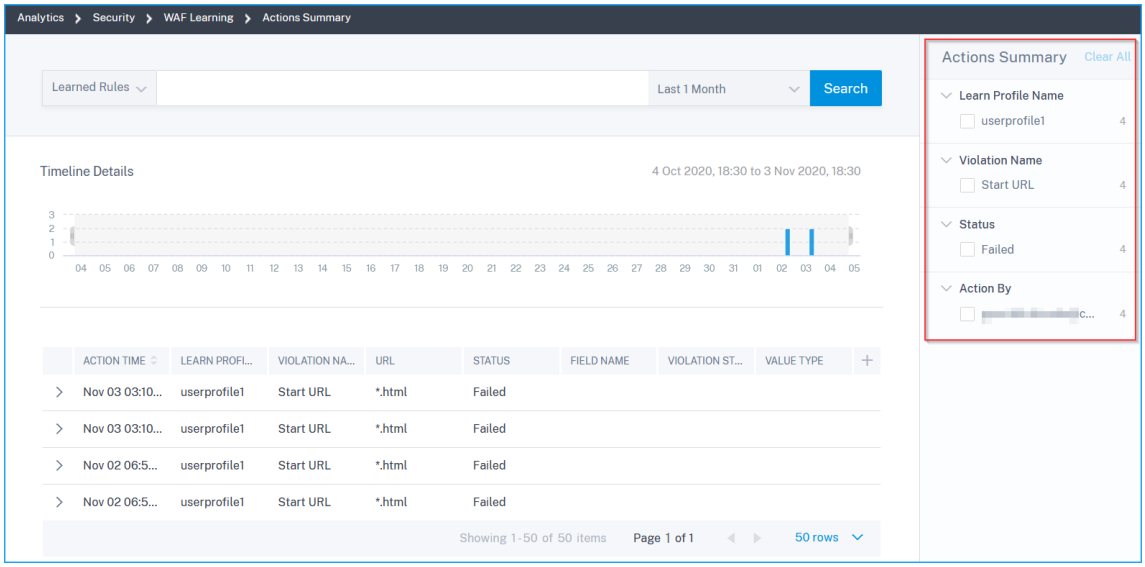
Maintenant :



- Après avoir cliqué sur **Gérer les règles**, vous pouvez afficher le total des règles, le total des règles apprises, le total des règles déployées et le total des règles d'inactivité pour le profil sélectionné.



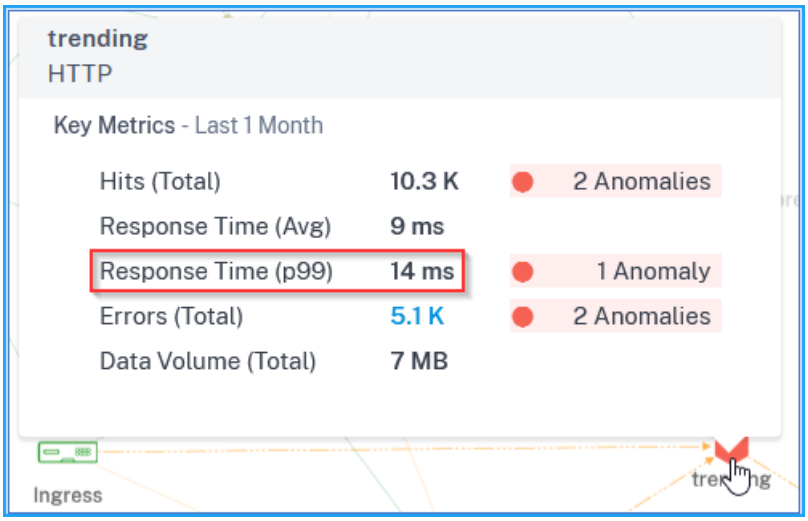
- Dans la page **Récapitulatif des actions**, vous pouvez filtrer les résultats en sélectionnant les options sous **Synthèse des actions**.



Pour de plus amples informations, consultez la section Moteur d'apprentissage WAF.

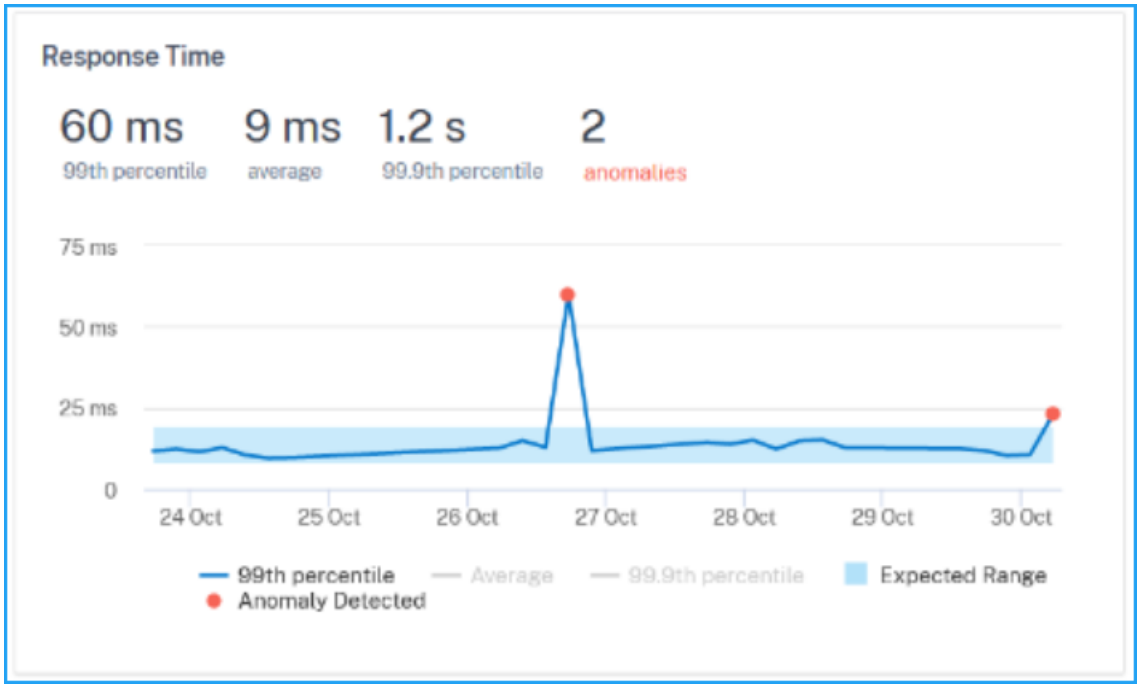
Graphique de service — Afficher Pxx la valeur du temps de réponse du service

Dans le graphique de service, lorsque vous placez le pointeur de la souris sur un service, vous pouvez désormais afficher la Pxx valeur du temps de réponse.



Temps de réponse (p99) : indique que 99 % du temps de réponse du service pour la durée sélectionnée est inférieur à la valeur **p99**.

Lorsque vous effectuez une hiérarchisation vers le bas pour afficher les détails du service, vous pouvez également afficher le 99e centile et le 99,9e centile du temps de réponse pour la durée sélectionnée.



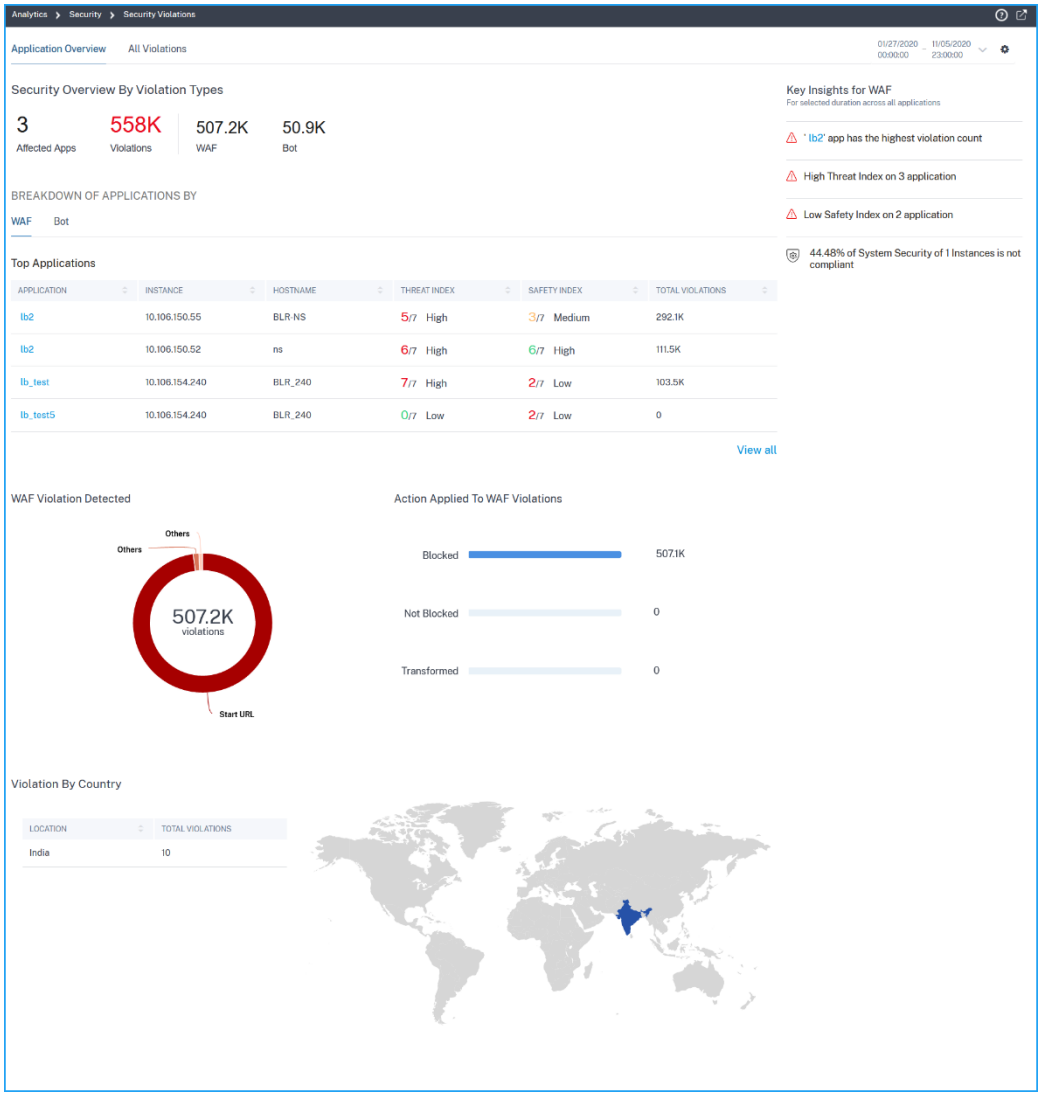
En tant qu'administrateur, en utilisant la pxx valeur, vous pouvez mieux comprendre le temps de réponse du service. Pour de plus amples informations, consultez la section Afficher les détails du service.

[NSADM-57729]

Violations de la sécurité des applications — Visualisez les applications avec des informations sur la sécurité et des détails

Dans **Analytics > Sécurité > Violations de sécurité**, vous pouvez désormais visualiser les applications avec une visibilité complète sur les détails des menaces associés à la fois dans les informations de sécurité et les informations sur les robots. La page **Violations de sécurité** dispose désormais des options **Toutes les violations** et **Vue d'ensemble des applications**.

- **Toutes les violations** : affiche les détails de la violation de sécurité de l'application.
- **Présentation de l'application** : affiche une vue d'ensemble avec des informations telles que le total des violations, le total des violations WAF et Bot, les applications les plus populaires, les violations par pays, etc.



Pour de plus amples informations, consultez la section Afficher les détails des violations de sécurité des applications.

[NSADM-57174]

Graphique de service - Surveillez les services Kubernetes à l'aide des mesures du signal doré

Les mesures de signal doré pour les services exécutés dans un cluster Kubernetes font référence à un ensemble de mesures qui vous permettent de détecter des anomalies potentielles pendant une durée spécifique. Lorsque vous avez 100 s de microservices dans le cluster Kubernetes, il peut être difficile d'identifier un service qui présente des problèmes fréquents. Les trois mesures clés suivantes sont les mesures de signal doré que Citrix ADM service graph peut vous aider à identifier les anomalies potentielles pour un service Kubernetes :

- Accès

- Temps de réponse (Moyen) et Temps de réponse (P99)
- Erreurs

En tant qu'administrateur, à l'aide de ces mesures, vous pouvez :

- Identifier l'état du service
  - **Critique** — Le service présente des anomalies ou une rupture de seuil dans plusieurs mesures
  - **Examen** — Le service présente des anomalies ou une violation du seuil dans l'une des mesures
  - **Bon** — Service sans anomalie ni rupture du seuil
- Analyser le nombre d'anomalies identifiées dans chaque mesure
- Résoudre le problème et éviter tout impact majeur

Pour de plus amples informations, consultez la section Afficher les détails du service.

[NSADM-56399]

Problème résolu

StyleBooks

- Dans StyleBooks, les packs de configuration existants affichent une date non valide dans le champ **Créé à**.

[NSADM-62160]

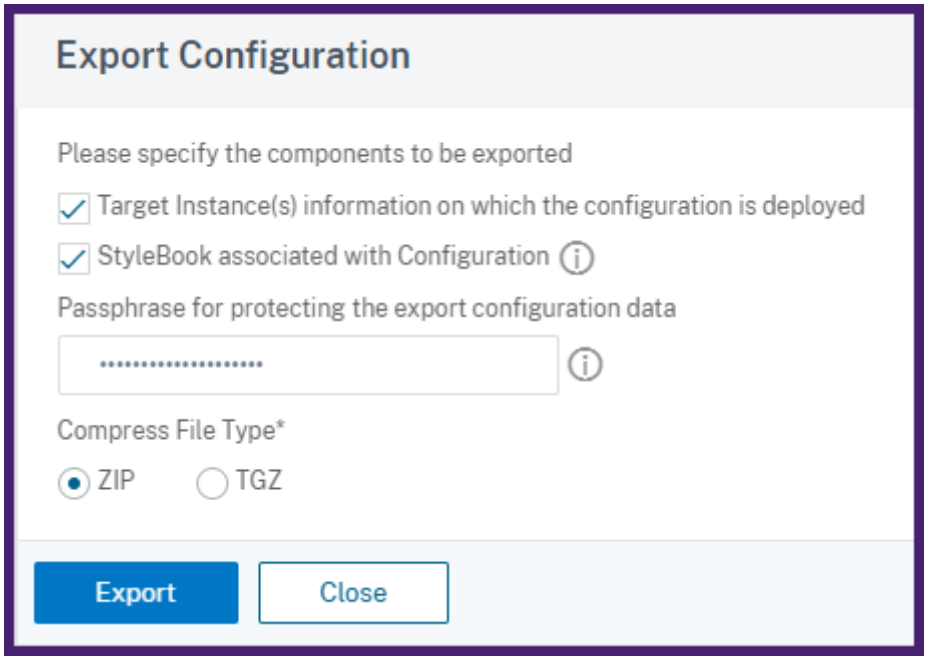
27 octobre 2020

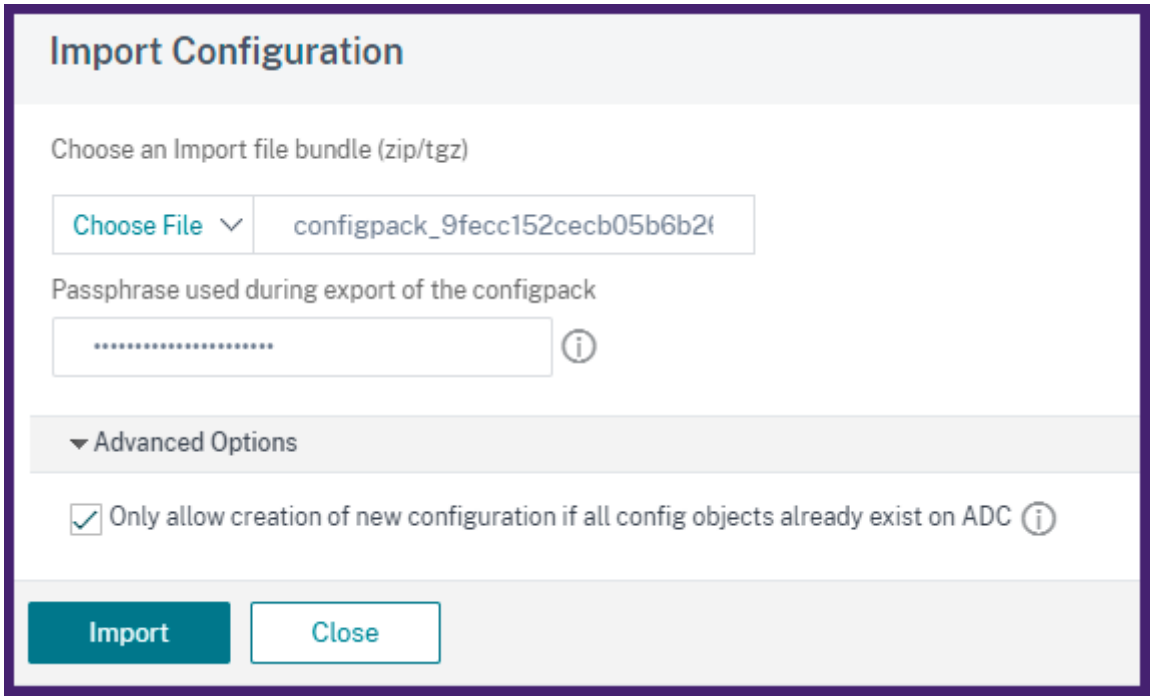
Exporter ou importer un pack de configuration StyleBook

Vous pouvez désormais exporter ou importer un pack de configuration tel que StyleBooks. Avec cette fonctionnalité, vous pouvez facilement partager la configuration de StyleBook à un autre serveur ADM. Auparavant, vous deviez télécharger un StyleBook, l'importer sur un autre serveur ADM, puis créer une configuration à partir de celui-ci.

Lorsque vous exportez un pack de configuration, un `tgz` ou `zip` bundle se télécharge sur votre ordinateur local. Ce bundle inclut un fichier JSON avec tous les paramètres définis dans un pack de configuration. Il contient également des informations sur les instances cibles si spécifié. Pour le pack de configuration d'un StyleBook personnalisé, vous pouvez inclure le StyleBook dans le bundle d'exportation. Spécifiez une phrase secrète pour chiffrer le bundle d'exportation. Cette phrase secrète sécurise les données sensibles d'un pack de configuration.

Vous pouvez importer un pack de configuration depuis votre ordinateur local vers un autre serveur ADM. Pour importer un pack de configuration, utilisez la phrase secrète spécifiée lors de l'exportation. Pour de plus amples informations, consultez la section Exporter ou importer des packs de configuration.





[NSADM-57935]

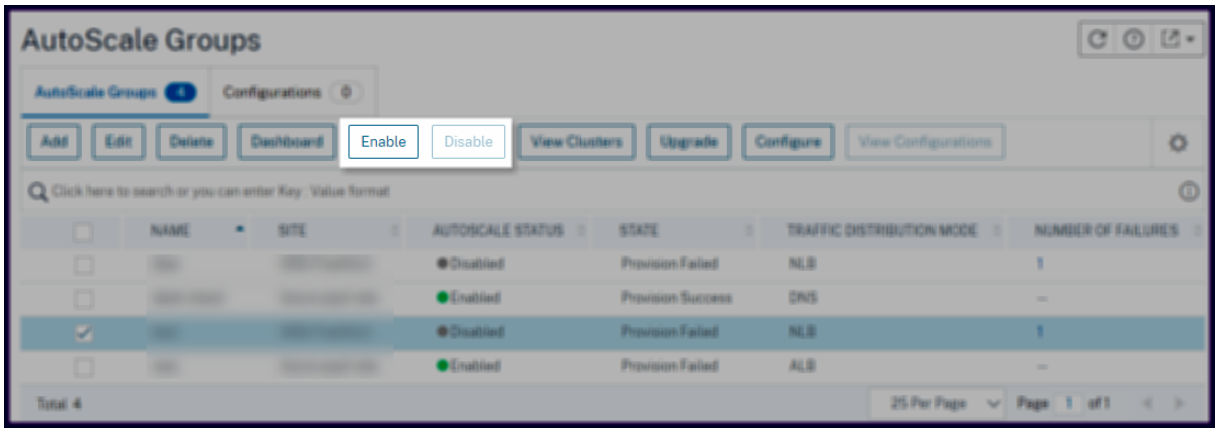
Configurer un serveur ADM uniquement pour la fonctionnalité de licence groupée

En tant qu'administrateur, vous pouvez désormais configurer un serveur ADM uniquement pour la fonctionnalité de licence groupée. Cette configuration est utile lorsque vous disposez des mandats réglementaires pour restreindre les données ADC dans une zone. Le service ADM reçoit uniquement les données de licence de vos instances ADC. De plus, vous pouvez allouer dynamiquement des licences de capacité groupée entre vos instances ADC déployées dans le monde entier. Pour de plus amples informations, consultez la section Configurer le service ADM uniquement en tant que serveur de licences.

[NSADM-47930]

Activer ou désactiver un groupe de mise Autoscale sans le modifier

Vous pouvez désormais activer ou désactiver un groupe de mise Autoscale sans le modifier. Les options d'activation ou de désactivation s'affichent désormais dans la page **Réseaux > Groupes de mise à l'échelle automatique**. De plus, vous pouvez toujours activer ou désactiver un groupe Autoscale dans l'option **Modifier**.



[NSADM-57802]

Exécuter des scripts personnalisés aux différentes étapes de mise à niveau de l'ADC

Les scripts personnalisés sont utilisés pour vérifier les modifications avant et après une mise à niveau d'instance ADC. Une mise à niveau d'instance comporte plusieurs étapes. Vous pouvez désormais spécifier ces scripts à exécuter dans les étapes suivantes :

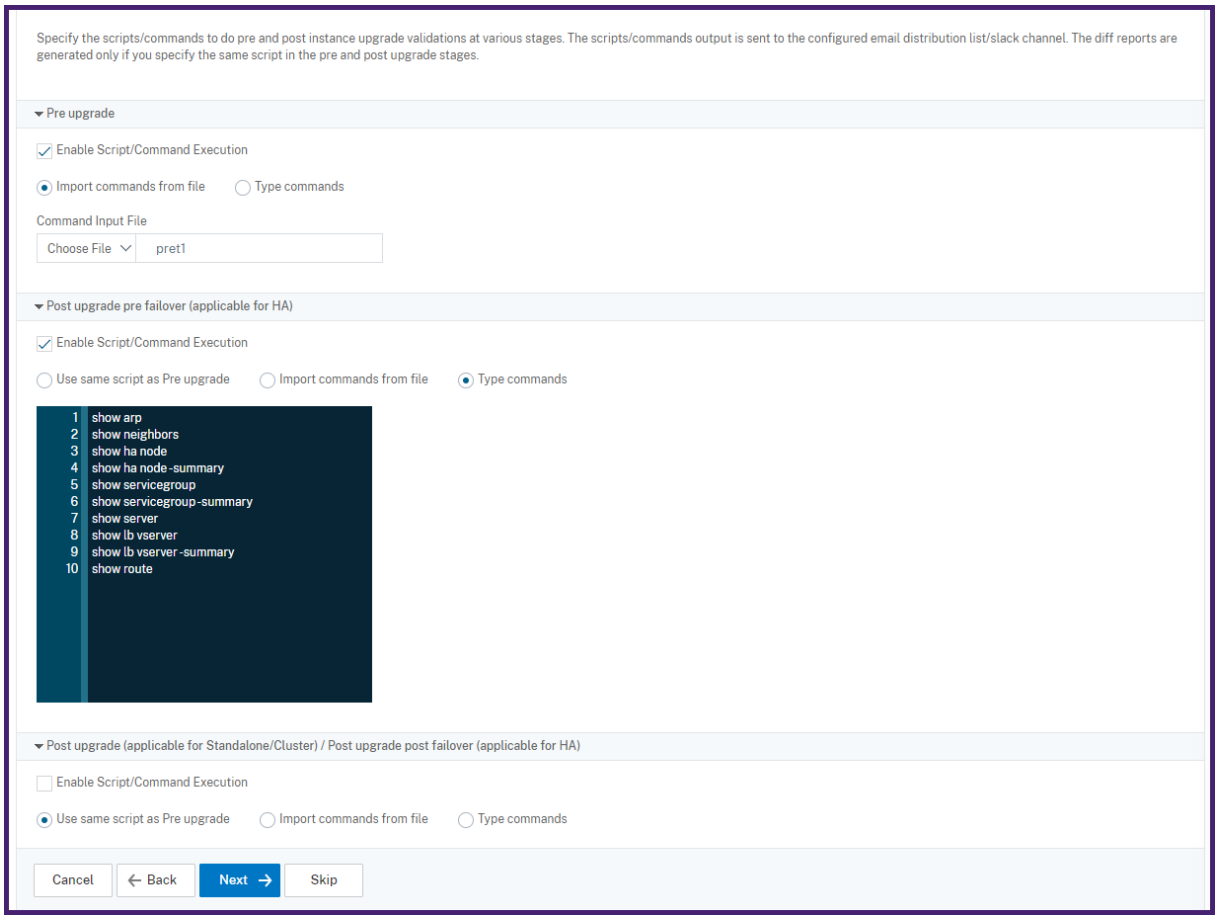
- **Prémise à niveau** : le script spécifié s'exécute avant la mise à niveau d'une instance.
- **Après la mise à niveau avant basculement (applicable pour HA)** : Cette étape s'applique uniquement au déploiement haute disponibilité. Le script spécifié s'exécute après la mise à niveau des nœuds, mais avant leur basculement.

- **Post upgrade (applicable pour autonome)/Post upgrade post basculement (applicable pour HA)** : Le script spécifié s'exécute après la mise à niveau d'une instance dans le déploiement autonome. Dans le déploiement haute disponibilité, le script s'exécute après la mise à niveau des nœuds et leur basculement sur incident.

Avec cette fonctionnalité, vous pouvez vérifier les modifications apportées à chaque étape de la mise à niveau de l'instance.

> **Remarque**
>
> Assurez-vous d'activer l'exécution du script aux étapes requises. Sinon, les scripts spécifiés ne s'exécutent pas.

Vous pouvez importer un fichier script ou taper des commandes directement dans l'interface graphique ADM. Dans les étapes de post-mise à niveau, vous pouvez utiliser le même script spécifié dans l'étape de pré-mise à niveau. Pour de plus amples informations, consultez la section Utiliser les tâches pour mettre à niveau les instances de Citrix ADC.

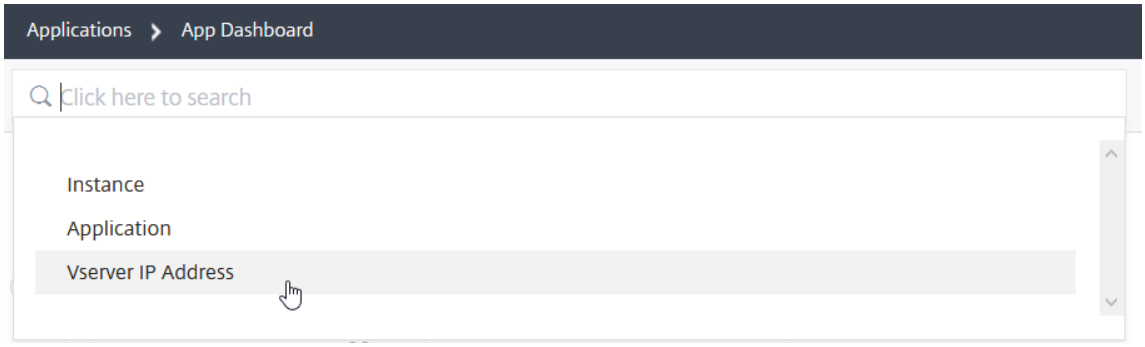


[NSADM-56649]

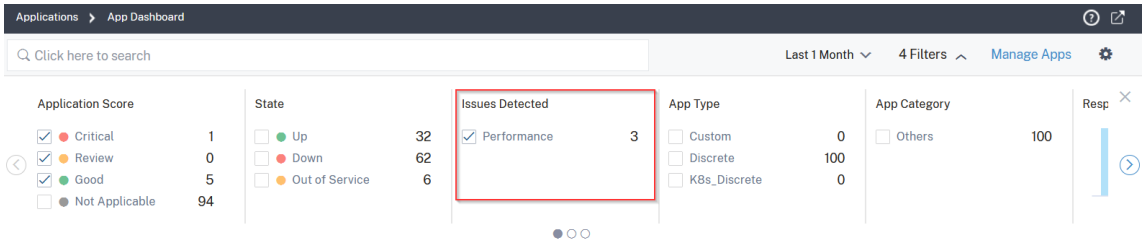
Améliorations du tableau de bord des applications

Vous pouvez désormais afficher les améliorations suivantes dans le Tableau de bord des applications :

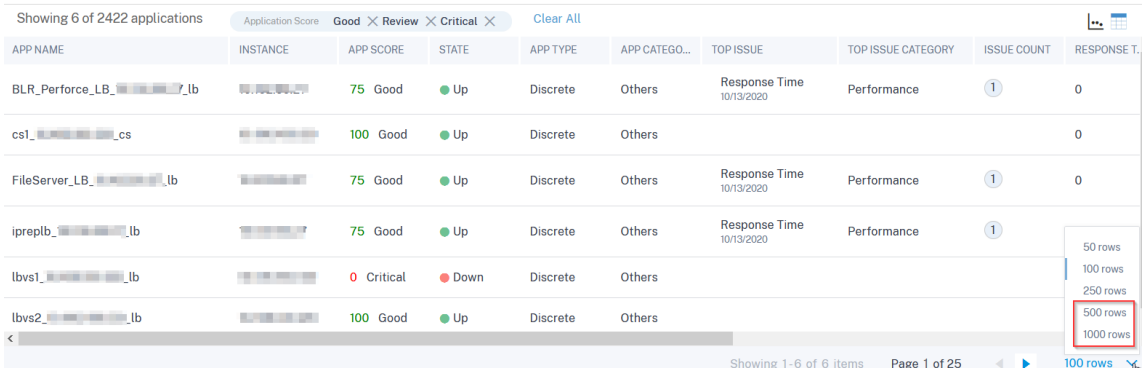
- Dans la barre de recherche, vous pouvez filtrer les résultats en fonction de l'adresse IP du serveur virtuel.



- Vous pouvez obtenir la liste des applications touchées par un problème spécifique en sélectionnant le type de problème (Performances, Instance Health, Config et System Resources) dans le filtre.



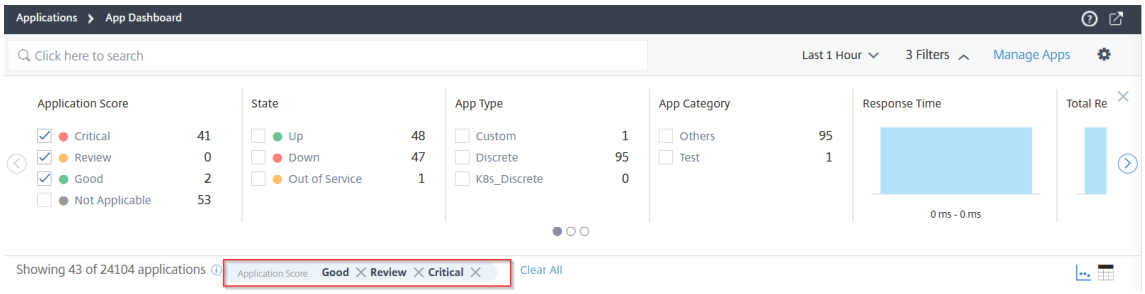
- La vue tabulaire vous permet de sélectionner l'option 500 lignes et 1000 lignes pour afficher le nombre maximal d'applications.



> **Remarque**
>
> Si vous sélectionnez l'option 500 lignes ou 1000 lignes, Citrix ADM prend environ 20 secondes pour afficher toutes les applications.
>
> Une fois toutes les applications chargées, vous pouvez sélectionner l'option d'affichage

> graphique.

- Par défaut, vous pouvez afficher les applications ayant le statut Critique, Révision et Bon. Pour afficher les applications qui ont le statut N/A, vous devez sélectionner Non applicable sous le filtre.



- Dans le problème du temps de réponse du serveur, vous pouvez afficher les détails des anomalies, après avoir sélectionné le serveur virtuel.

[NSADM-57049]

Problèmes résolus

Système

- Dans **Compte > Administration des utilisateurs > Groupes**, si un utilisateur externe fait partie de plusieurs groupes et qu'aucune application n'est sélectionnée pour un ou plusieurs groupes, l'utilisateur externe ne peut pas afficher le serveur virtuel ou d'autres entités.

  [NSHELP-25181]

- Dans **Compte > Administration des utilisateurs > Groupes**, lorsque vous ajoutez ou modifiez un groupe avec des instances SDX, la création ou la modification du groupe prend plus de temps que d'habitude.

  [NSHELP-25081]

Système de licences

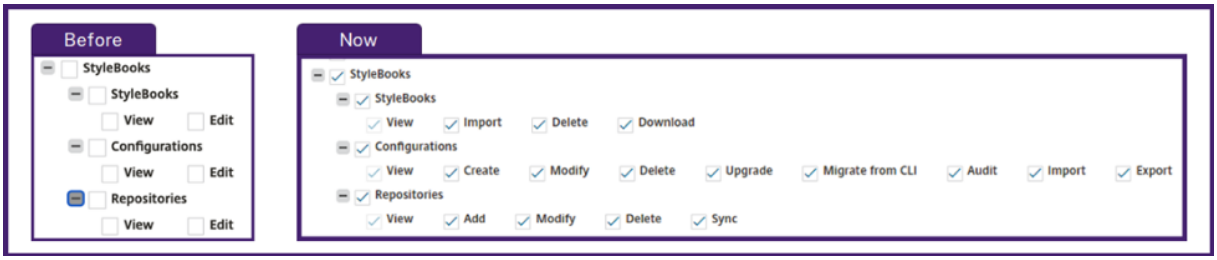
Lorsque vous allouez des licences à des instances non gérées, le pourcentage d'allocation de licences apparaît incorrectement dans le graphique en donut.

[NSADM-60798]

14 octobre 2020

Accorder de nouvelles autorisations StyleBook aux utilisateurs

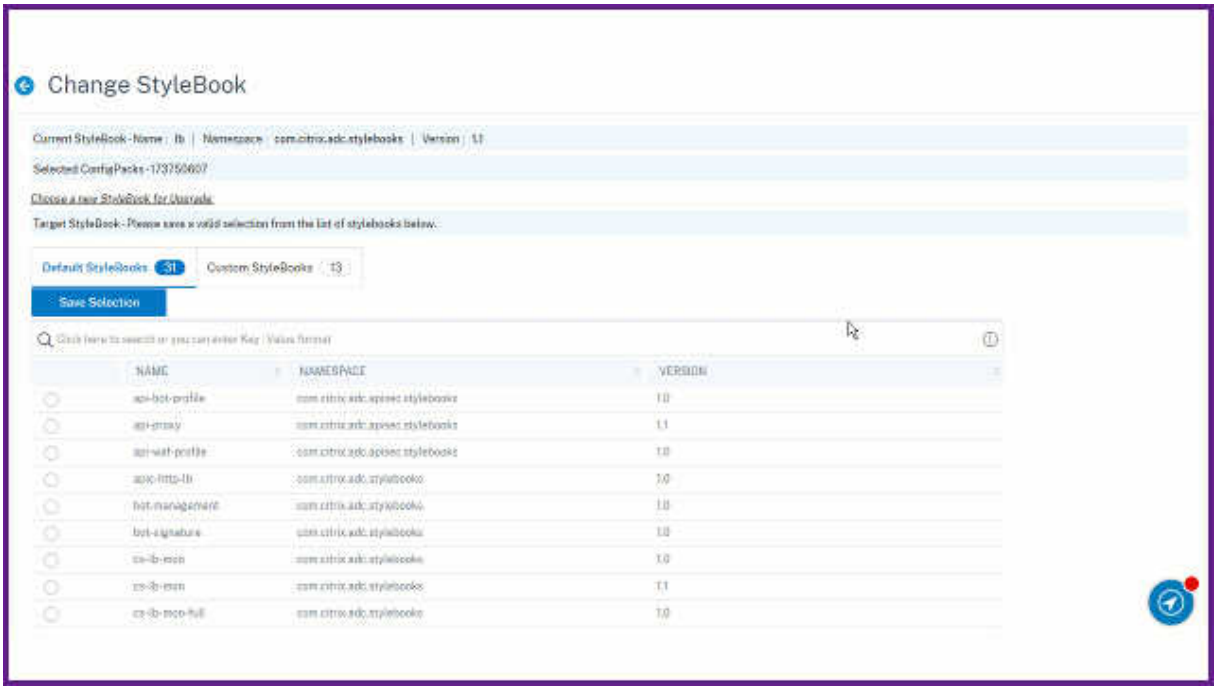
En tant qu'administrateur, lorsque vous créez une stratégie d'accès, vous pouvez désormais accorder de nouvelles autorisations StyleBook aux utilisateurs, telles que l'importation, la suppression, le téléchargement, etc. Pour ce faire, accédez à **Comptes > Administration des utilisateurs > Stratégies d'accès** et cliquez sur **Ajouter**. Auparavant, vous étiez en mesure de sélectionner uniquement les autorisations d'affichage et de modification. Pour de plus amples informations, consultez la section Accorder des autorisations StyleBook aux utilisateurs.



[NSADM-57672]

Modifier un pack de configuration pour modifier son StyleBook

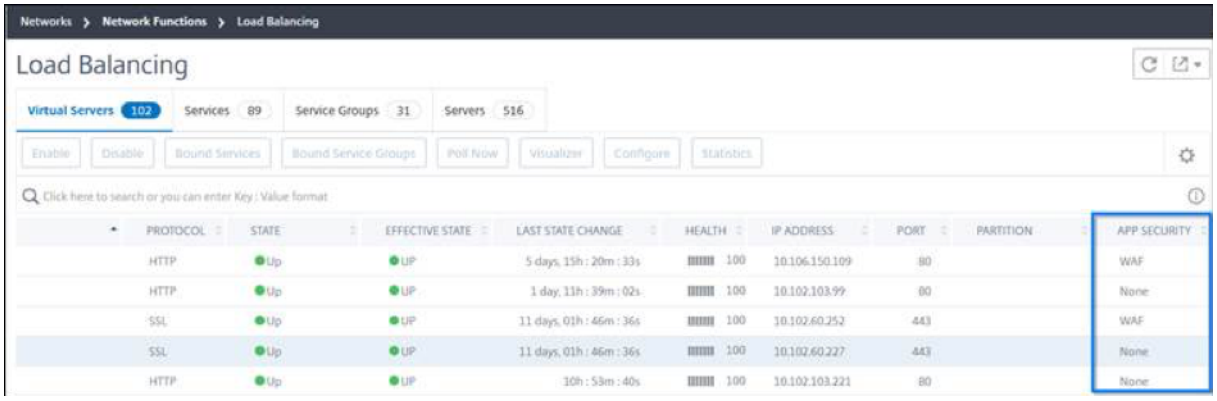
Vous pouvez maintenant modifier un pack de configuration pour modifier son StyleBook. Auparavant, vous étiez en mesure de le faire en utilisant l'option Migrer ConfigPack. Pour de plus amples informations, consultez la section Modifier le StyleBook d'un pack de configuration.



[NSADM-58245]

Fonctions réseau : ajout de la colonne App Security

Dans **Réseaux > Fonctions réseau > Équilibrage de charge et Changement de contenu**, vous pouvez désormais afficher la colonne **App Security**x.



En tant qu'administrateur, vous pouvez analyser si les serveurs virtuels sont liés avec :

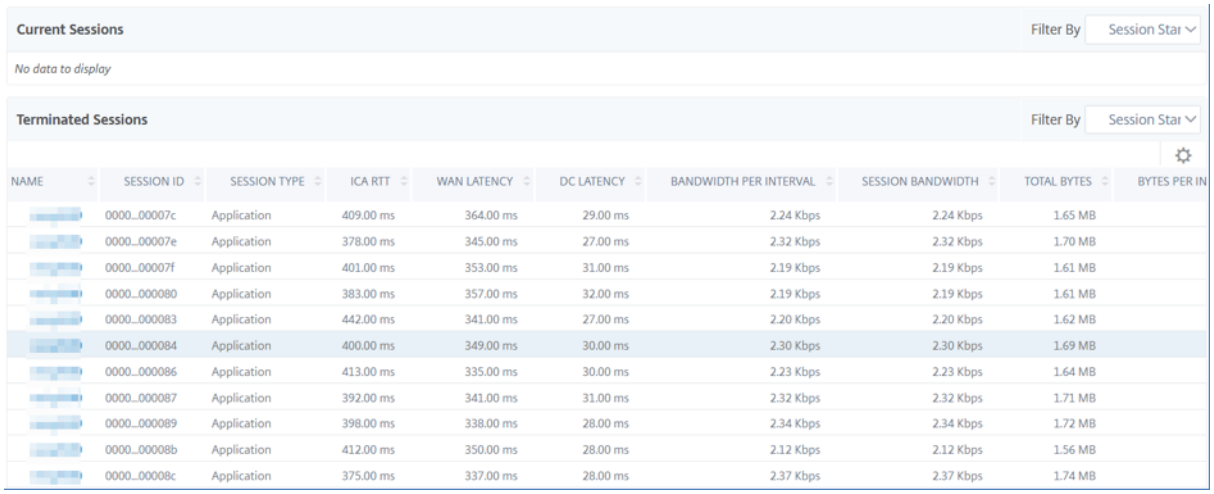
- **WAF** — Le serveur virtuel est configuré avec la stratégie App Firewall et affiche les violations de sécurité WAF.
- **Bot** — Le serveur virtuel est configuré avec la stratégie de bot et affiche les violations de sécurité des robots.
- **Bot, WAF** — Le serveur virtuel est configuré avec des stratégies de pare-feu d'application et de bot et affiche les violations de sécurité WAF et Bot.
- **Aucun** — Le serveur virtuel n'est configuré ni avec des stratégies de pare-feu d'application ni de robot.

Pour de plus amples informations, consultez la section Afficher les détails des violations de sécurité des applications.

[NSADM-54300]

HDX Insight : Améliorations pour afficher tous les utilisateurs des sessions actives et terminées

Dans **Analytics > HDX Insight > Utilisateurs**, vous pouvez désormais visualiser une vue consolidée de tous les utilisateurs des sessions actives et terminées.



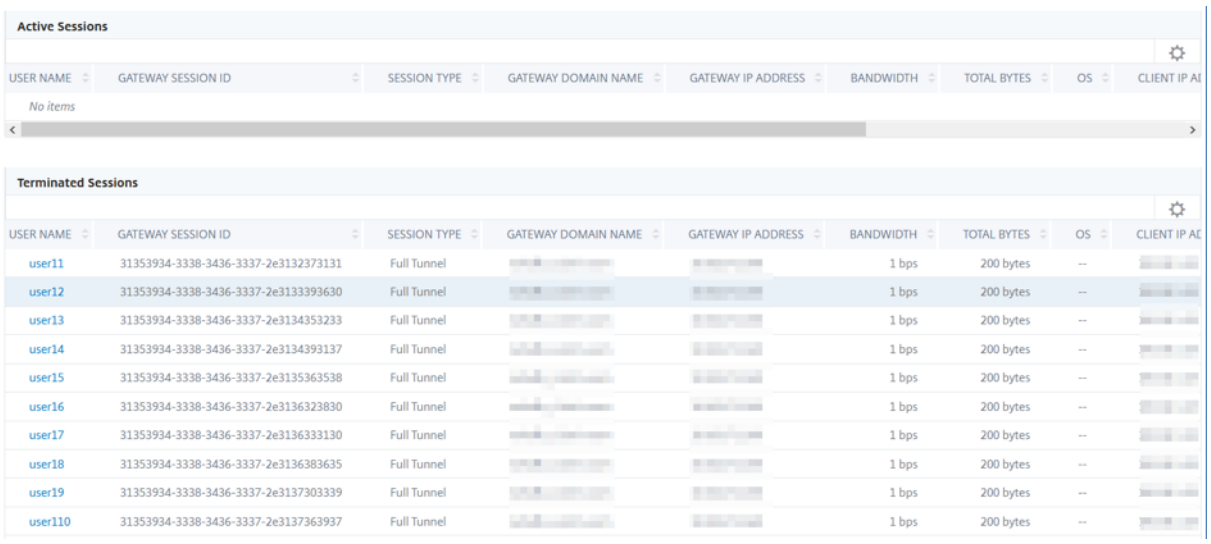
En tant qu'administrateur, cette amélioration vous permet de :

- Afficher tous les détails des utilisateurs dans une visualisation à un seul volet
- Éliminer la complexité de la sélection de chaque utilisateur et de voir les sessions actives et terminées

[NSADM-57685]

Gateway Insight : Améliorations pour afficher tous les utilisateurs des sessions actives et terminées

Dans **Analytics > Gateway Insight > Utilisateurs > Utilisateurs de passerelle**, vous pouvez désormais visualiser une vue consolidée de tous les utilisateurs actifs et des sessions terminées.



En tant qu'administrateur, cette amélioration vous permet de :

- Afficher tous les détails des utilisateurs dans une visualisation à un seul volet

- Éliminer la complexité de la sélection de chaque utilisateur et de voir les sessions actives et terminées

[NSADM-60800]

Security Insight — Afficher la violation de grammaire d'injection SQL

Dans Security Insight, vous pouvez désormais afficher un nouveau type de violation, Grammaire d'injection SQL. Pour générer la violation de Grammaire d'injection SQL dans Security Insight, vous devez configurer les commandes suivantes dans l'instance Citrix ADC :

1. `add ns ip <IP> <subnet mask> -type SNIP`
2. `add lb vs http_vs http <VS_IP> 80`
3. `add service http_svc <SVC_IP> http 80`
4. `bind lb vs http_vs http_svc`
5. `add appfw profile abc -startURLAction none -SQLInjectionGrammar ON -SQLInjectionType None`
6. `set appfw settings -defaultProfile abc`

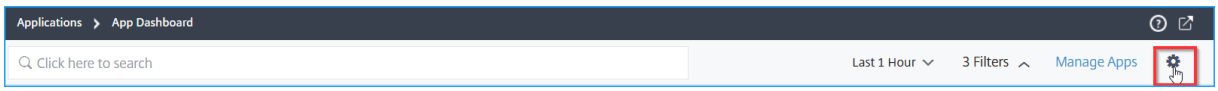
Pour de plus amples informations, consultez la section Security Insight.

Tableau de bord des applications : sélectionnez les composants App Score et configurez les seuils

Dans le **Tableau de bord des applications**, en tant qu'administrateur, vous pouvez désormais choisir les composants et configurer les seuils pour le calcul du score de l'application. **App Score** est le système de notation qui définit :

- Comment une application fonctionne bien
- Si l'application fonctionne bien en termes de réactivité

Accédez à **Applications > Tableau de bord**, puis sélectionnez l'icône Paramètres pour afficher les composants du score de l'application.



Pour de plus amples informations, consultez la section Sélectionnez les composants App Score et définissez des seuils.

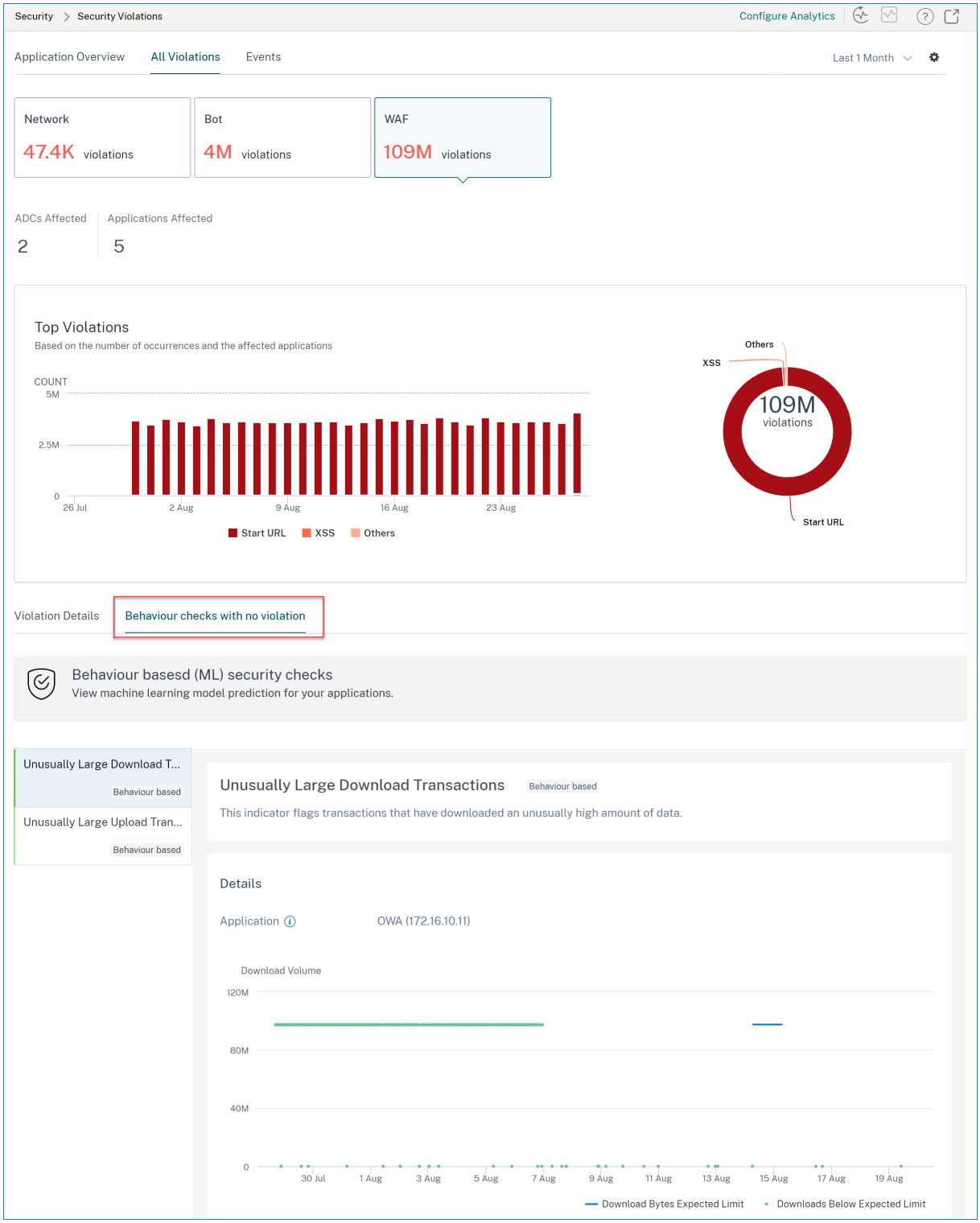
[NSADM-52870]

Violations de sécurité des applications : visualisez les prédictions en fonction des schémas de trafic

Dans **Analytics > Sécurité > Violations**de sécurité, pour toutes les violations de sécurité (WAF et bot), à l'exception des détails de violation, vous pouvez désormais visualiser une prévision de trafic de 3 semaines basée sur l'algorithme d'apprentissage automatique. En tant qu'administrateur, cette prédiction de 3 semaines vous permet de :

- Analyser le schéma de trafic même si aucune violation n'est observée
- Prendre des actions de dépannage pour les schémas de trafic inhabituels observés à partir des prévisions
- Observez que Citrix ADM traite les données, en dehors des anomalies

Dans la page **Violations de sécurité**, cliquez sur l'onglet **Vérifications de comportement sans violation** pour afficher la prévision de trafic de 3 semaines.



Pour de plus amples informations, consultez la section Violations de la sécurité.

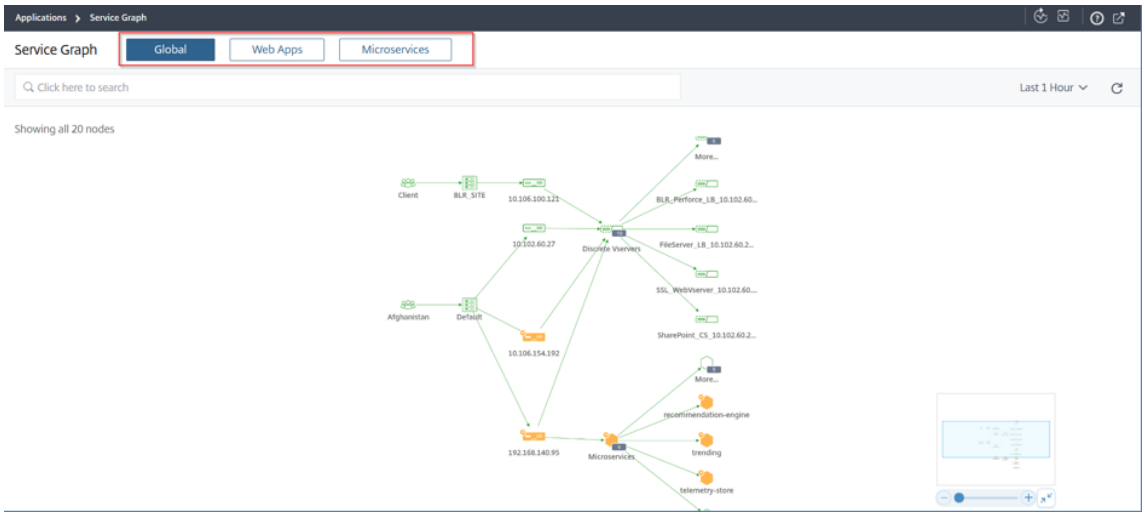
[NSADM-58721]

Graphique des améliorations apportées au service

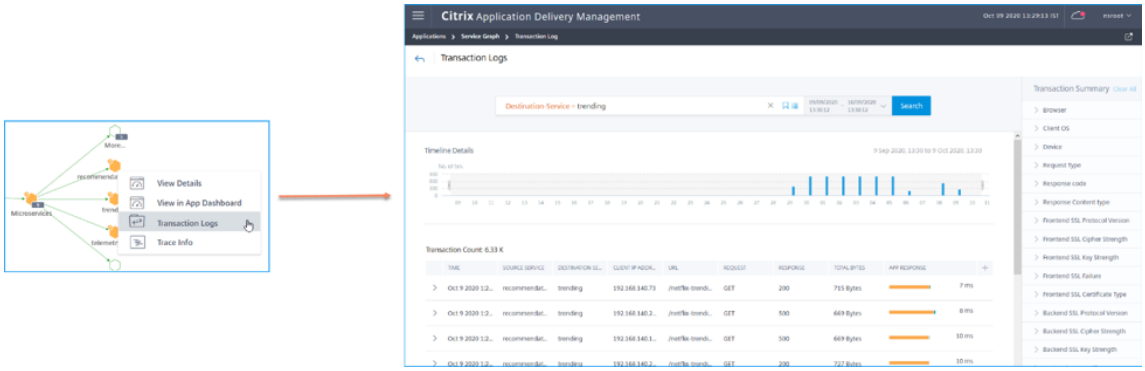
Dans **Applications > Service Graph**, vous pouvez désormais afficher les améliorations suivantes :

- La page du graphique de service comporte trois onglets :
  - **Global** : affiche le graphique de service pour les applications sur toutes les instances Citrix ADC
  - **Apps Web** : affiche le graphique des services pour les applications Web à 3 niveaux (équilibrage de charge, commutation de contenu et GSLB)
  - **Microservices** — Affiche le graphique de service pour les microservices Kubernetes

  Cliquez sur chaque onglet pour afficher le graphique de service correspondant.



- À partir du graphique de service global, vous pouvez accéder aux détails du microservice. Cliquer sur un service et sélectionner l'option redirige vers son interface graphique respective.



- Le graphique de service des microservices comporte une barre de recherche, où vous pouvez pointer la souris et sélectionner les catégories suivantes pour créer le filtre :

- **Localisation géographique du client** — Affiche l'entrée et ses services auxquels le client accède.
- **Ingress-IP** — Affiche tous les services associés à l'entrée

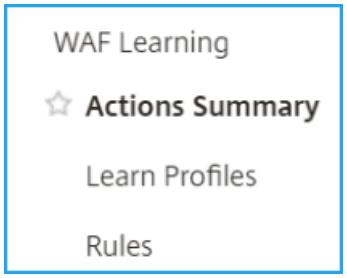
[NSADM-57696]

29 septembre 2020

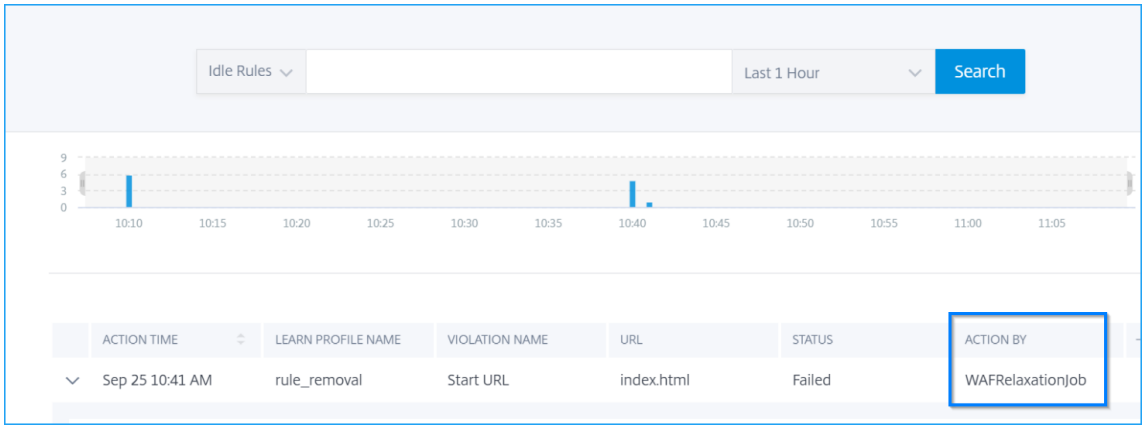
Améliorations du moteur d'apprentissage WAF

Dans le moteur d'apprentissage WAF, vous pouvez désormais afficher les améliorations suivantes :

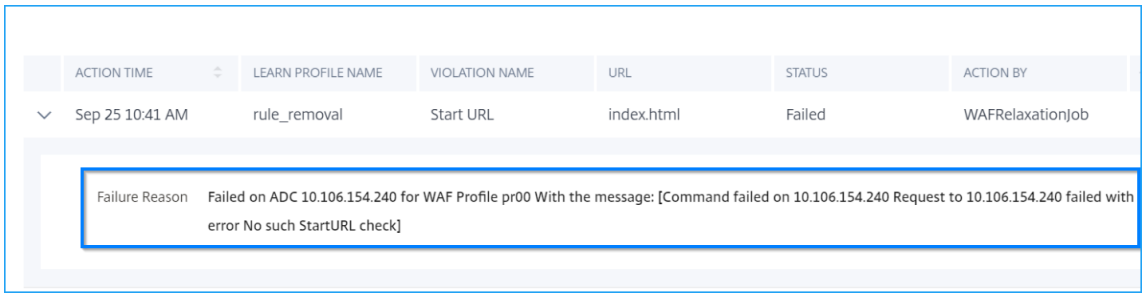
- **WAF Learning > Tableau de bord** est remplacé par **WAF Learning > Résumé des actions**



- L'option **Action par** vous permet de comprendre si les règles apprises sont déployées automatiquement par Citrix ADM ou si l'administrateur a sélectionné manuellement l'option **Déployer** ou **Ignorer**.



- Si une règle d'apprentissage déployée a échoué, vous pouvez afficher la raison de l'échec dans la page **Récapitulatif des actions**.

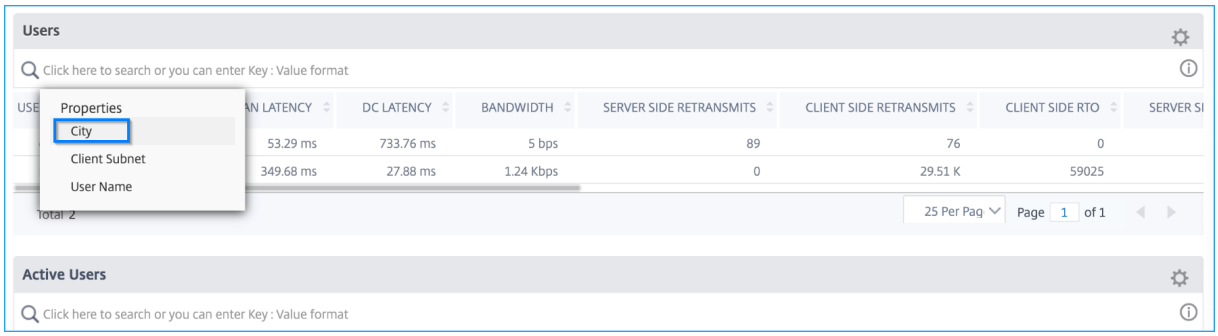


- Pour chaque profil appris configuré, vous pouvez afficher jusqu'à 1 million de règles apprises.

  [NSADM-57220]

HDX insights — Recherche en utilisant le nom de ville

Dans les informations HDX, vous pouvez désormais filtrer les résultats en fonction du nom de la ville.

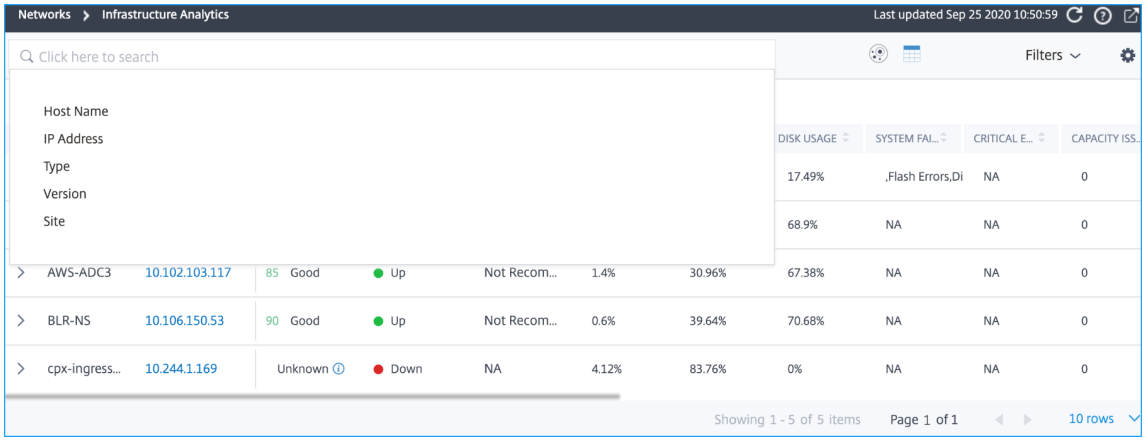


[NSADM-57366]

Analyse d'infrastructure — Attributs de recherche

Dans **Infrastructure Analytics**, vous pouvez désormais placer le curseur de la souris sur la barre de recherche et sélectionner les attributs de recherche suivants pour filtrer les résultats :

- Nom d'hôte
- Adresse IP
- Type
- Version
- Site

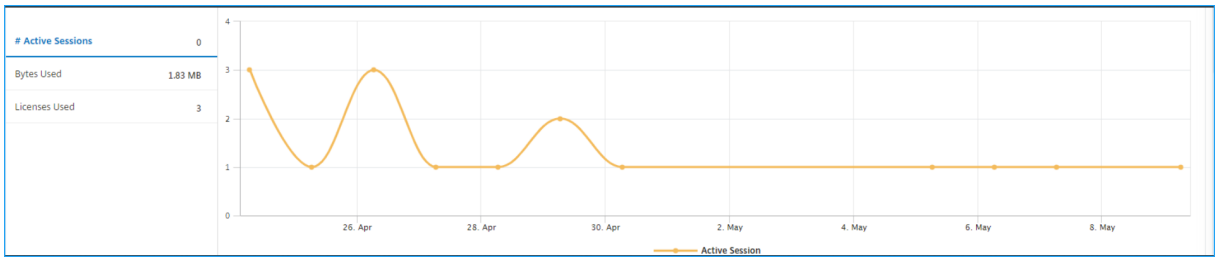


[NSADM-59453]

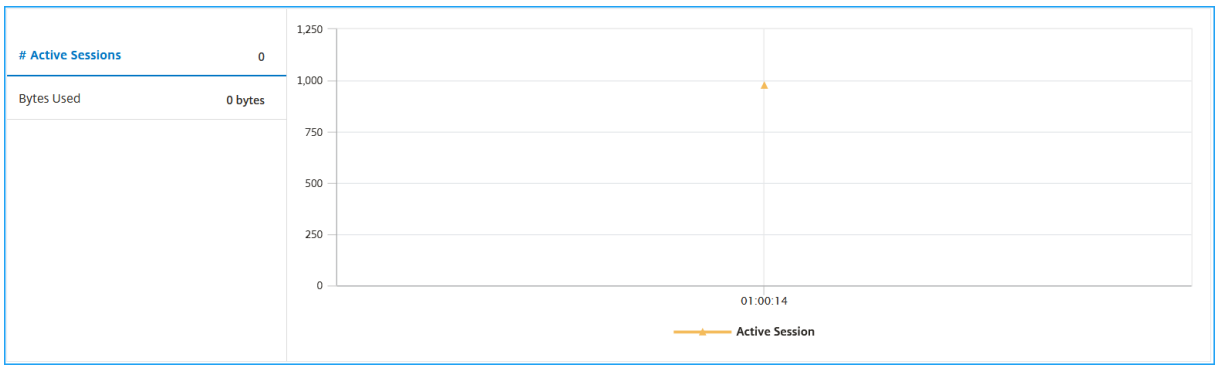
Amélioration de Gateway Insight

Dans **Gateway Insight > Utilisateurs**, les informations de licence sont maintenant supprimées.

Plus tôt :



Maintenant :

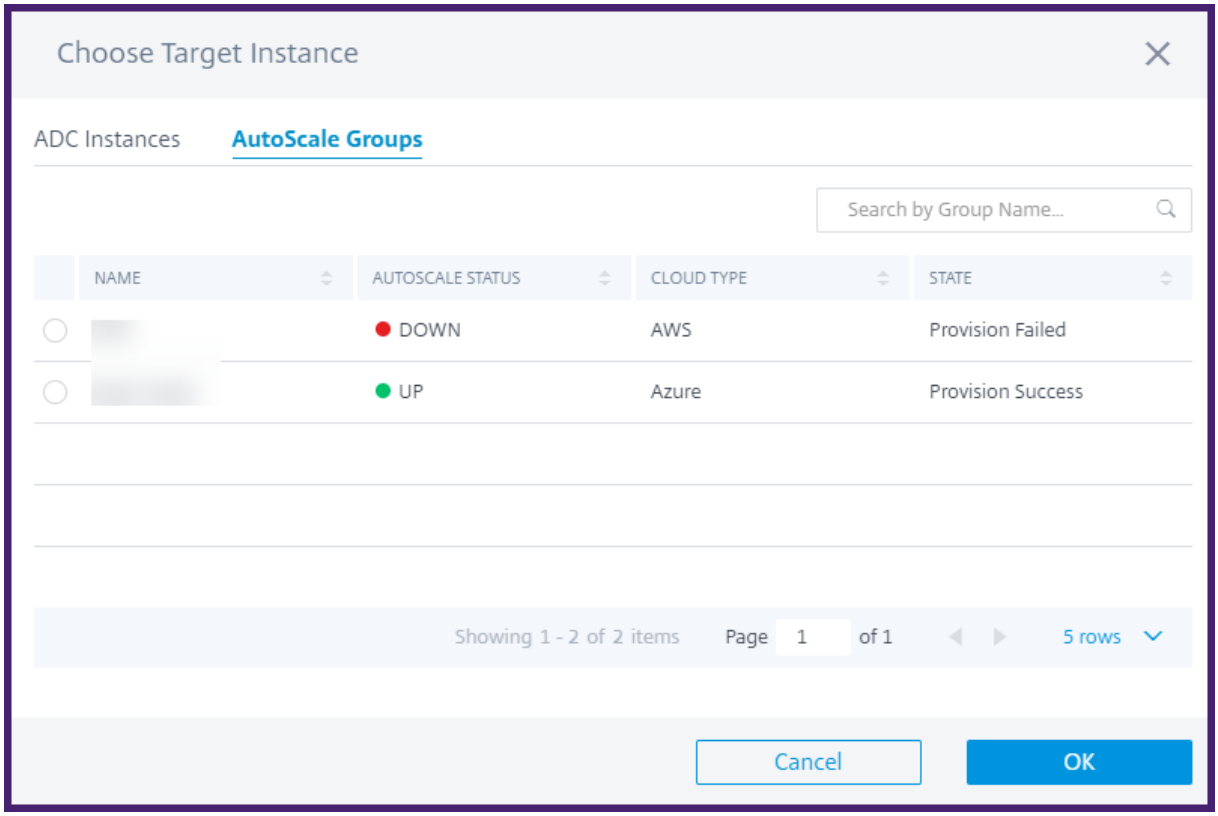


[NSADM-53494]

Migrer la configuration ADC vers un groupe de mise à Autoscale à l'aide du générateur de configuration StyleBook

Dans le générateur de configuration StyleBooks, vous pouvez désormais migrer la configuration ADC vers un groupe de mise à Autoscale. Pour ce faire, sélectionnez le groupe de mise à l'Autoscale requis

en tant qu'instance cible.



[NSADM-51470]

Problèmes résolus

Déploiement

L'image de l'agent ADM ne fonctionne pas dans le type d'instance AWS M5. Avec ce correctif, les pilotes pris en charge sont ajoutés pour que l'image de l'agent ADM fonctionne dans les types d'instance M5.

[NSHELP-24250]

Réseaux

Lorsque vous exécutez une tâche de configuration avec le caractère « < », la tâche échoue.

[NSADM-53465]

16 septembre 2020

Intégration faible tactile des instances ADC à l'aide du service ADM connect

Vous pouvez désormais utiliser le nouveau flux de travail d'intégration du service Citrix ADM, qui fournit un moyen plus rapide d'intégrer les instances ADC au service ADM et d'obtenir une visibilité sur votre déploiement multicloud hybride. La fonctionnalité d'intégration automatique de ce flux de travail exploite la nouvelle fonctionnalité de connexion du service ADM dans les instances ADC, qui permet aux instances ADC d'être connectées au service ADM. Pour de plus amples informations, consultez la section Intégration à faible contact des instances Citrix ADC à l'aide du service Citrix ADM connect.

> **Remarque**
>
> Ce flux de travail est déployé (GA) de manière progressive, via la version canari. Vous recevrez un courriel lorsque cette fonctionnalité sera disponible dans votre environnement de service ADM.

[NSADM-51952]

Graphique de service Kubernetes - Synthèse des transactions client

Dans le graphique de service Kubernetes, vous pouvez désormais afficher les journaux de transactions détaillés pour tous les clients à partir d'un emplacement spécifique. En utilisant cette fonctionnalité, vous pouvez afficher :

- Temps de réponse > 500 ms
- erreurs 5xx

> **Remarque**
>
> Vous ne pouvez afficher que quelques exemples de transactions 2xx et 4xx pour le client sélectionné.

Cette fonctionnalité vous permet non seulement d'examiner visuellement les transactions détaillées, mais aussi de comprendre les mesures (telles que RTT client, SSL et temps de réponse du serveur) réparties sur le client, l'ADC et le serveur.

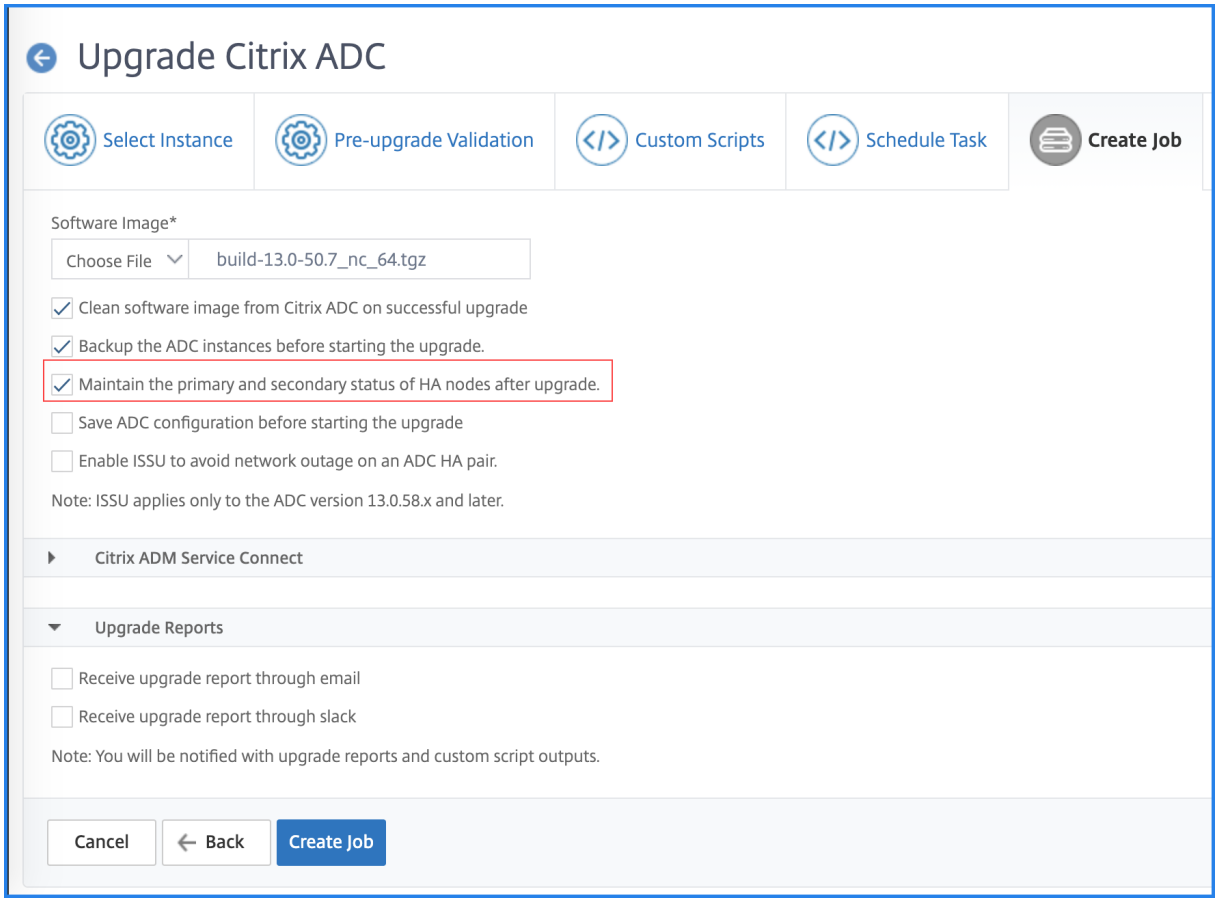
Pour de plus amples informations, consultez la section Afficher les mesures client.

[NSADM-58342]

Maintenir l'état des nœuds haute disponibilité ADC après la mise à niveau

Lorsque vous créez un travail de mise à niveau pour une paire ADC haute disponibilité, une nouvelle option **Maintenir le statut principal et secondaire des nœuds HA après la mise à niveau** apparaît. Cette option apparaît sous l'onglet **Créer une tâche**. Sélectionnez cette option si vous souhaitez que le travail de mise à niveau lance un basculement après la mise à niveau de chaque nœud. Auparavant,

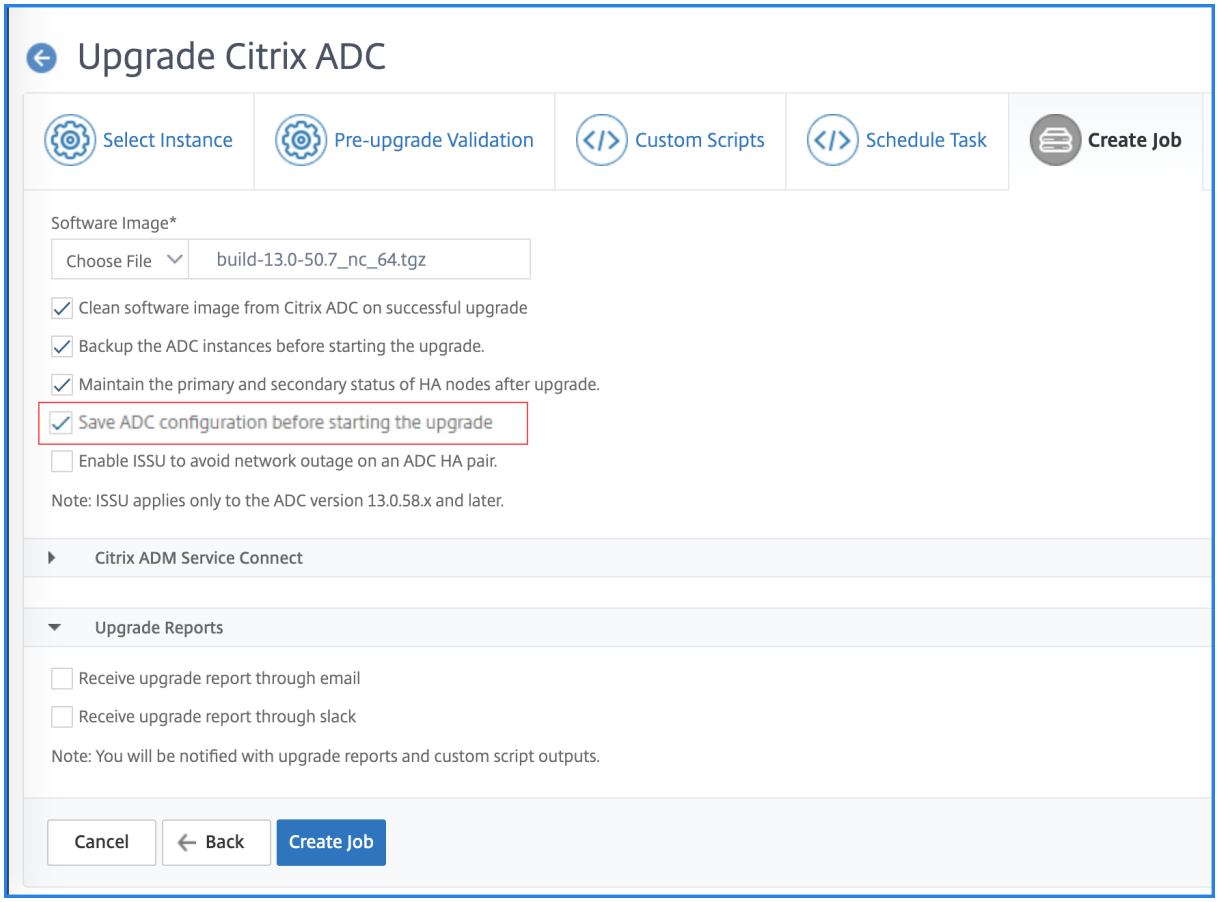
il n'y avait pas d'option GUI, et le travail de mise à niveau initiait le basculement par défaut, après la mise à niveau de chaque nœud.



[NSADM-47736]

Enregistrer la configuration ADC avant une mise à niveau

Lorsque vous créez un travail de mise à niveau pour une instance ADC, vous pouvez désormais enregistrer la configuration ADC en cours d'exécution avant de mettre à niveau l'instance. Sélectionnez l'option **Enregistrer la configuration ADC avant de démarrer l'option de mise à niveau** sous l'onglet **Créer une tâche**.



[NSADM-52470]

Problème résolu

Analytics

Impossible de redimensionner les colonnes dans la page **Analytics > HDX Insight > Utilisateurs**.

[NSHELP-24288]

02 septembre 2020

Modifier le type d'accès d'une application Autoscale

Vous pouvez maintenant modifier le type d'accès d'une application Autoscale. Lorsque vous modifiez le type d'accès, vous pouvez également modifier les éléments suivants :

- Type de nom de domaine complet
- Nom de domaine
- Zone du domaine.

[NSADM-52810]

Améliorations de API Gateway

La fonctionnalité de passerelle API est maintenant améliorée avec les fonctionnalités suivantes :

- Analytics API : lorsque vous cliquez sur Voir plus pour développer une vignette, vous pouvez rechercher des instances et des points de terminaison d'API par leurs noms partiels. Consultez Afficher l'analyse de l'API.
- Déploiements : activez l'analyse pour un déploiement d'API. Consultez Activer l'analyse de l'API.
- Stratégies : Configurez les stratégies WAF et BOT pour un déploiement d'API. Consultez Ajouter des stratégies à une définition d'API.

  > **Remarque**
  >
  > Avant de configurer les stratégies WAF et BOT, assurez-vous de créer un profil dans ADM à l'aide de StyleBooks. Les StyleBooks par défaut suivants sont ajoutés pour créer des profils :
  >
  > `api-waf-profile`
  >
  > `api-bot-profile`

  Pour de plus amples informations, consultez la section Créer des profils WAF et BOT à l'aide de StyleBook.

[NSADM-52804]

Inclure des icônes dans le pack StyleBooks

Lorsque vous importez plusieurs StyleBooks à partir d'un lot, vous pouvez désormais inclure des icônes dans chaque StyleBook. Téléchargez les icônes et le `icon_mapping.json` fichier `resources` dans le dossier. Si le nom du fichier d'icône et le nom de StyleBook correspondent, les icônes sont automatiquement mappées aux StyleBooks. Sinon, mappez StyleBooks et icônes dans le `icon_mapping.json` fichier comme suit :

```
<StyleBook file name> : <icon file name>
```

Si vous spécifiez uniquement l' `defaulticon` entrée, tous les StyleBooks du bundle sont mappés à l'icône spécifiée.

```
defaulticon: <icon file name>
```

Dans **Application > StyleBooks**, les StyleBooks importés apparaissent avec les icônes mappées.

Pour de plus amples informations, consultez la section Importer des StyleBooks personnalisés.

[NSADM-52330]

Améliorations de la page Capacité groupée

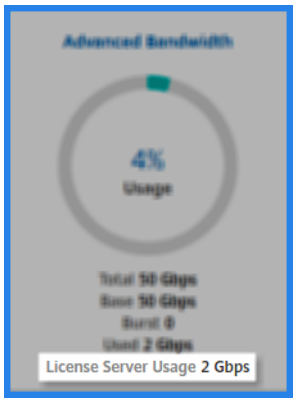
La **page Capacité groupée** est désormais améliorée avec les modifications suivantes de l'interface graphique :

- **Instances non gérées** : il s'agit d'un nouvel onglet. Il affiche les instances qui sont découvertes mais non gérées dans Citrix ADM. Auparavant, ces instances étaient répertoriées dans l'onglet Tableau de bord avec l'état de licence non gérée.

- Statut de licence : dans cette colonne, les statuts suivants sont supprimés :
  - Non géré
  - Synchronisation en cours

  La colonne **Détails de l'allocation** est maintenant supprimée de la liste des instances.

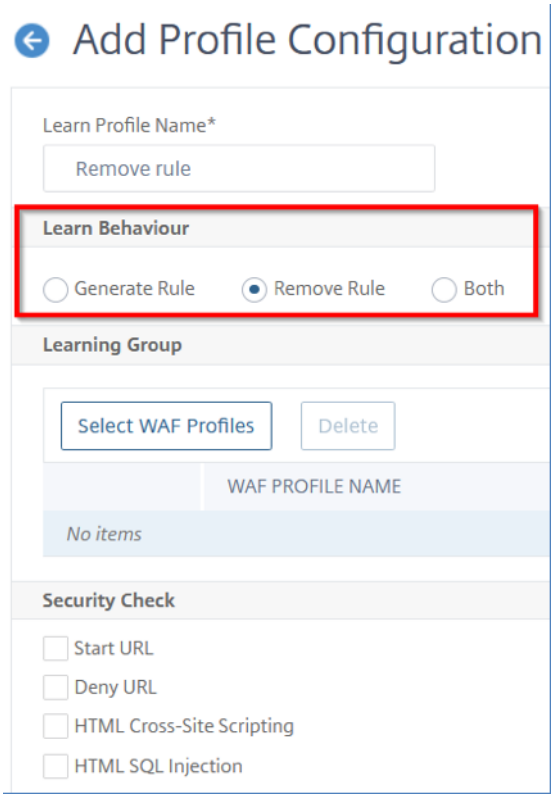
- Utilisation du serveur de licences - Un nouvel indicateur est ajouté au graphique d'utilisation. Il affiche la consommation de capacité groupée du serveur de licences.



[NSADM-52770]

WAF Learning Engine - Prise en charge de la suppression des règles

Vous pouvez maintenant modifier le comportement d'apprentissage pour supprimer les règles de relaxation, si aucun trafic entrant avec des vérifications de sécurité n'est reçu dans l'instance Citrix ADC. Accédez à **Analytics > Sécurité > Apprentissage WAF > Apprendre les profils**, puis cliquez sur **Ajouter** pour afficher les options Apprendre le comportement.



- **Générer une règle** : génère la règle d'exception et permet à l'administrateur de déployer ou d'ignorer la règle.
- **Supprimer la règle** : supprime la règle d'exception lorsque le temps d'inactivité configuré dépasse le seuil.
- **Les deux** — Génère les règles d'exception et supprime la règle lorsqu'il n'y a pas de trafic entrant.

Vous pouvez appliquer l'option de règle de suppression uniquement pour les vérifications de sécurité suivantes :

- URL de démarrage
- Refuser URL
- Scriptage inter-sites HTML
- Injection SQL HTML

Lorsqu'une règle est supprimée, une notification est générée dans Slack, SMS, Email et ServiceNow. Vous pouvez également afficher les détails dans le tableau de **bord d'apprentissage WAF**.

Pour de plus amples informations, consultez la section Configurer le profil d'apprentissage.

[NSADM-52871]

Violations de la sécurité des applications -

Dans **Violations de sécurité des applications**, vous pouvez désormais afficher **les scanners de site Web** sous la catégorie Violation BOT. Pour de plus amples informations, consultez la section Violation de la sécurité.

[NSADM-53289]

Violations de sécurité des applications - Réseau

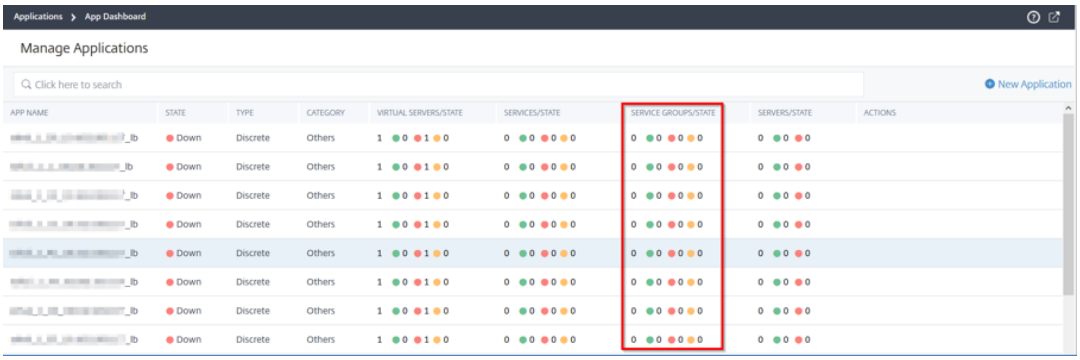
Dans **Violations de sécurité des applications**, vous pouvez désormais afficher les attaques de petites fenêtres sous la catégorie Violation réseau. Pour de plus amples informations, consultez la section Violation de la sécurité.

[NSADM-46023]

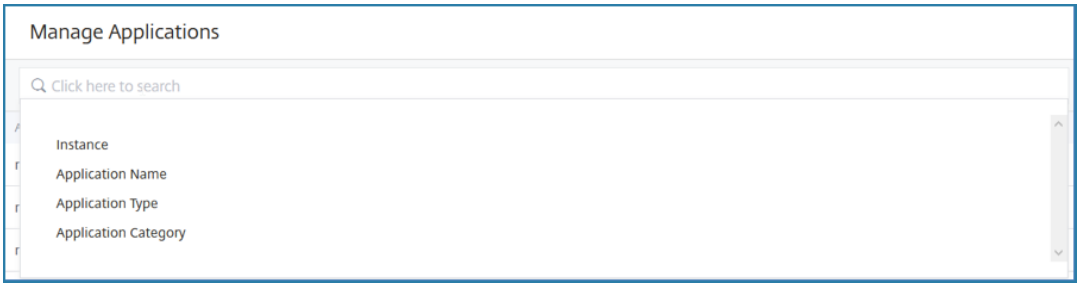
Améliorations apportées au tableau de bord

Dans le **Tableau de bord des applications**, vous pouvez désormais afficher les améliorations suivantes :

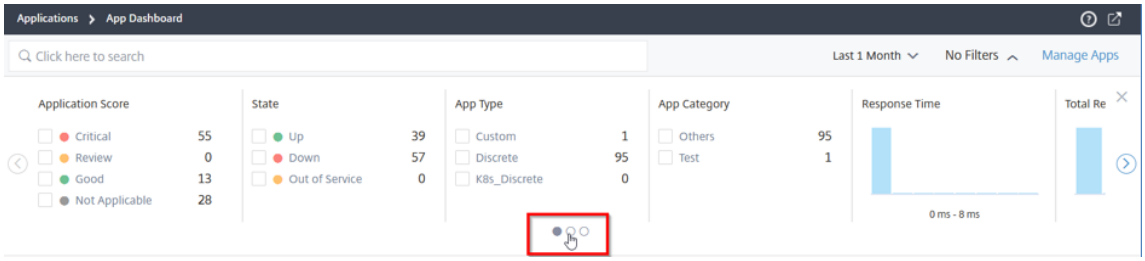
- Dans la page **Gérer les applications** :
  - Vous pouvez afficher le nombre total de groupes de services et le statut des groupes de services qui sont En haut, en bas ou en dehors du statut.



  - Vous pouvez placer le pointeur de la souris sur la barre de recherche et sélectionner la catégorie pour affiner la recherche.



- Dans la page **Tableau de bord de l'application**, la barre de défilement est remplacée par un curseur carrousel qui vous permet d'accéder facilement à toutes les options.



[NSADM-52759]

Tableau de bord Web Insight

Vous pouvez désormais afficher une fonctionnalité Web Insight améliorée qui fournit une visibilité sur les mesures détaillées pour les applications Web, les clients et les instances Citrix ADC. Cette amélioration Web Insight vous permet d'évaluer et de visualiser les informations complètes de l'application du point de vue des performances et de l'utilisation ensemble. En tant qu'administrateur, vous pouvez afficher Web Insight pour :

- Une application. Accédez à **Applications > Tableau de bord**, cliquez sur une application, puis sélectionnez l'onglet **Web Insight** pour afficher les mesures détaillées. Pour de plus amples informations, consultez la section Analyse de l'utilisation des applications.
- Toutes les applications. Accédez à **Applications > Web Insight** et cliquez sur chaque onglet (Applications, Clients, Instances) pour afficher les mesures suivantes :

Applications	Clients	Instances
Application	Clients	Mesures d'instance
Serveurs	Loocations géo	Applications
Domaines	Méthodes de requête HTTP	Domaines
Emplacements géographiques	État de la réponse HTTP	URL
URL	URL	Méthodes de requête HHTP
Méthodes de requête HTTP	OS	État de la réponse HTTP
État de la réponse HTTP	Navigateurs	Clients
Erreurs SSL	Erreurs SSL	Serveurs
Utilisation de SSL	Utilisation de SSL	OS
-	-	Navigateurs

Pour de plus amples informations, consultez la section Tableau de bord Web Insight.

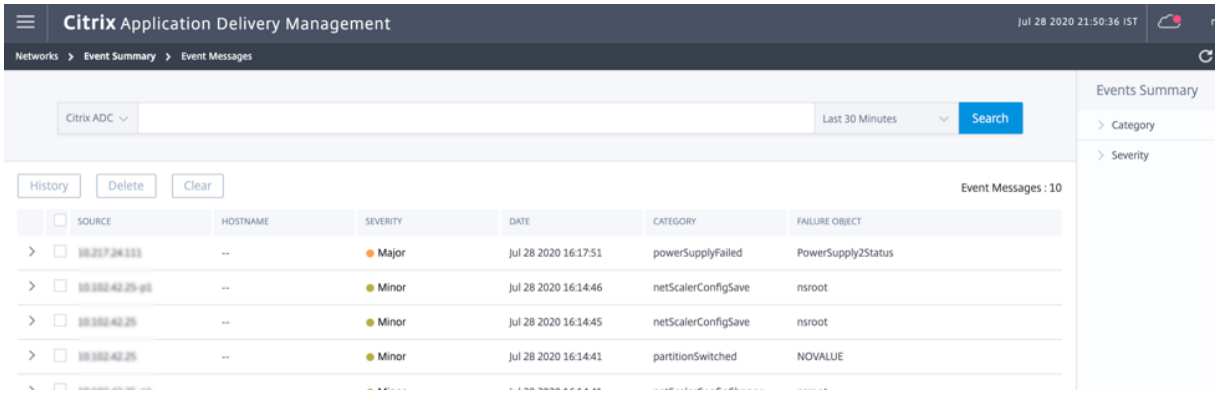
Prise en charge de l'agent ADM sur GCP

Les agents Citrix ADM sont désormais pris en charge sur Google Cloud Platform (GCP). Pour de plus amples informations, consultez Installer l'agent Citrix ADM sur GCP

[NSADM-31980]

Nouvelle fonctionnalité de recherche pour les messages d'événement

Dans **Réseaux > Événements > Messages**d'événements, vous pouvez désormais utiliser des opérateurs logiques tels que `AND`/`OR` la recherche. Vous pouvez également filtrer les données à l'aide de périodes personnalisées. En outre, le panneau récapitulatif des événements fournit un dénombrement de chaque catégorie d'événement et de gravité.



Problèmes résolus

Analytics

Le rapport d'analyse dans Citrix ADM affiche uniquement des données de 14 à 28 jours, même après que la durée est sélectionnée comme 1 mois

[NSHELP-23836]

Système

ADM ne génère pas le pack de support technique de l'agent si la taille du fichier est grande.
[NSHELP-24620]

Système de licences

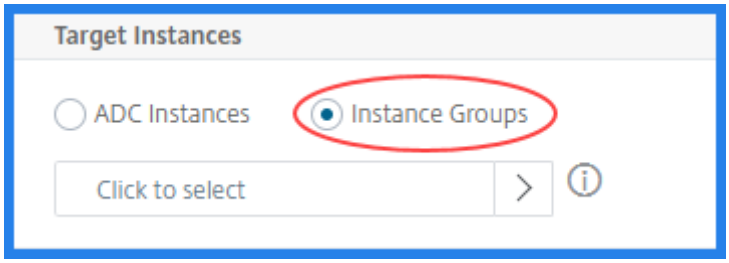
Lors de l'installation d'un fichier de licence sur l'interface graphique ADM à l'aide d'un code d'accès à la licence (**Réseaux > Licences > Ajouter un fichier**de licence), le message « Échec de l'analyse des informations de licence » s'affiche. Le problème se produit si les fichiers de licence sont stockés sur un serveur Jazz, ce qui n'est pas pris en charge. Avec ce correctif, les serveurs Jazz sont pris en charge pour ajouter des fichiers de licence à ADM.

[NSADM-59338]

17 août 2020

Sélection des groupes d'instances cibles pour déployer un pack de configuration

Lorsque vous ajoutez une nouvelle configuration dans la page **StyleBooks > Configurations**, vous pouvez désormais sélectionner un groupe d'instances ADC pour déployer un pack de configuration. Et, cette configuration s'applique à toutes les instances du groupe. Pour ce faire, sélectionnez **Groupes d'instances** dans la section **Instances cibles**.



[NSADM-56605]

Spécifier une adresse IP à partir du réseau IPAM

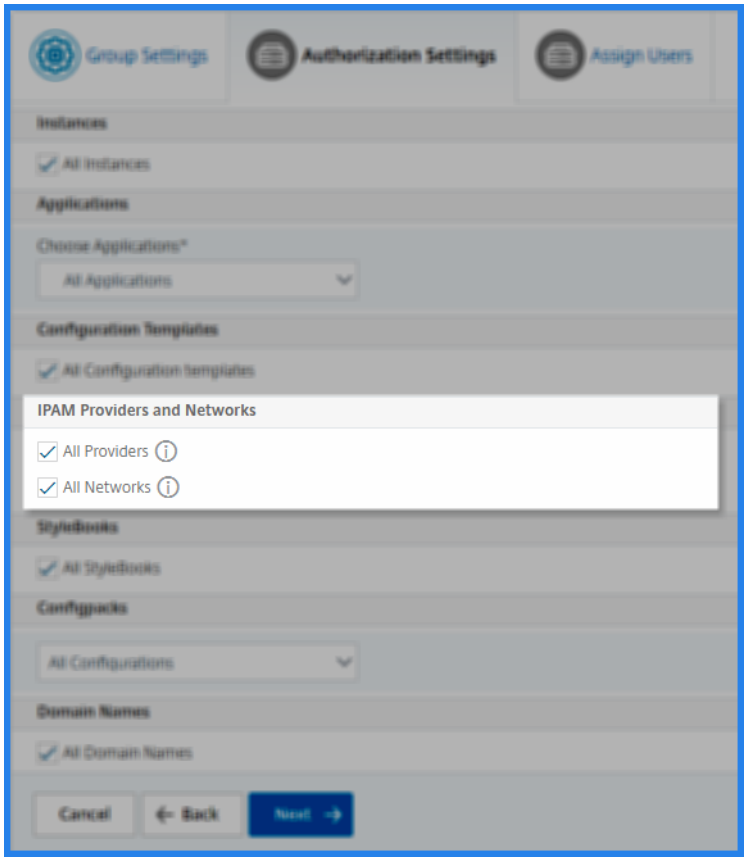
Lorsque vous définissez la valeur de l' `dynamic-allocation` attribut sur true dans la définition **StyleBook**, un utilisateur peut désormais spécifier une adresse IP à partir du réseau IPAM sélectionné. L'ADM attribue l'adresse IP spécifiée à un serveur virtuel.

[NSADM-56068]

Gérer l'autorisation de l'utilisateur à IPAM

En tant qu'administrateur, vous pouvez désormais sélectionner des **fournisseurs et des réseaux IPAM** et accorder l'accès à un utilisateur ou à un groupe.

1. Accédez à la page **Système > Administration des utilisateurs**.
2. Ajoutez des fournisseurs et des réseaux IPAM dans l'onglet **Paramètres d'autorisation**.



[NSADM-54377]

Améliorations apportées aux fonctions intégrées de StyleBook

Lors de la création de définitions StyleBook, utilisez les fonctions intégrées suivantes avec leurs fonctionnalités améliorées :

- `replace()` — Remplace désormais les caractères ou les chaînes spécifiés dans la liste. Auparavant, vous n'étiez pas en mesure de fournir une entrée de liste à cette fonction.
- `ip()` — Accepte maintenant une valeur entière et la convertit en une adresse IP équivalente. Il prend également en charge l'ajout d'adresses IP et la soustraction.
- **`int`**`()` — Accepte maintenant une adresse IPv4 et retourne sa valeur entière équivalente.

[NSADM-56310],[NSADM-55209]

Utiliser les nouvelles fonctions intégrées de StyleBook

Lors de la création de définitions StyleBook, ADM StyleBooks prend désormais en charge les fonctions intégrées suivantes :

- `distinct()` - Extrait les éléments uniques d'une liste d'entrée.

- `split()` - Divise une chaîne d'entrée en listes.

[NSADM-56103],[NSADM-55958]

Configurer une application de groupe Autoscale sans StyleBooks

Vous pouvez désormais configurer une application sur un groupe de mise à l'Autoscale ADC sans sélectionner StyleBooks. Toutefois, si vous souhaitez utiliser StyleBooks à l'avenir, modifiez et soumettez à nouveau cette application, sélectionnez **Oui** dans la fenêtre de confirmation.

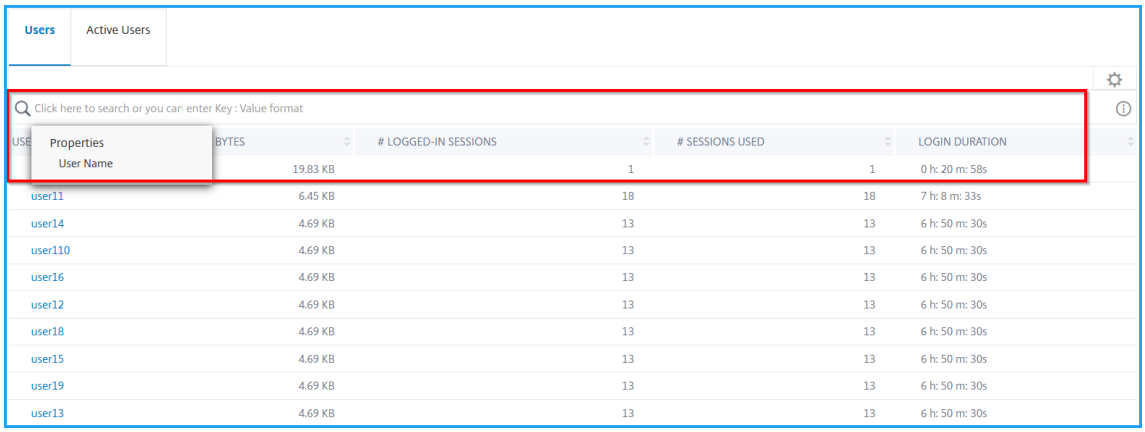
Auparavant, la sélection StyleBook était obligatoire pour configurer une application de groupe mise à Autoscale.

[NSADM-52814]

Amélioration de Gateway Insight

Dans **Gateway Insight**, vous pouvez maintenant afficher :

- Barre de recherche qui vous permet de filtrer les résultats en fonction du nom d'utilisateur. Accédez à **Analytics > Gateway Insight > Utilisateurs** pour afficher la barre de recherche **Utilisateurs** et **Utilisateurs actifs**. Placez le pointeur de la souris sur la barre de recherche, sélectionnez **Nom d'utilisateur**et tapez un nom d'utilisateur pour filtrer les résultats.



- Carte géographique qui affiche les informations sur les utilisateurs en fonction de la position géographique des utilisateurs. En tant qu'administrateur, cette carte géographique vous permet d'afficher le récapitulatif du nombre total d'utilisateurs, du total des applications et du nombre total de sessions pour un emplacement spécifique.

  1. Accédez à **Analytics > Gateway Insight** pour afficher la carte géographique
  2. Cliquez sur un pays. Par exemple, États-Unis
     La carte géographique affiche les détails tels que la liste des utilisateurs, les sessions actives, les sessions terminées, les applications pour le pays sélectionné.

- Carte géographique pour les passerelles qui vous permet de filtrer les utilisateurs en fonction d'un emplacement particulier.

    1. Accédez à **Analytics > Gateway Insight > Gateways**
    2. Sélectionnez un nom de domaine de passerelle pour afficher la carte géographique
    3. Cliquez sur un pays. Par exemple, les États-Unis

       La carte géographique affiche les détails tels que la liste des utilisateurs, les sessions actives, les sessions terminées, les applications pour le pays sélectionné.

[NSADM-55504],[NSADM-55506]

Violations de sécurité des applications — Réseau

Dans les **violations de sécurité des applications**, vous pouvez désormais afficher l' **attaque d'inondation SYN** sous la catégorie Violation réseau. Pour de plus amples informations, consultez la section Violations de la sécurité.

[NSADM-46021]

Améliorations apportées au graphique Global Service

Dans Global Service Graph, vous pouvez désormais utiliser la barre de recherche pour filtrer les résultats. En tant qu'administrateur, cette barre de recherche vous permet de réduire rapidement une instance/client/application/centre de données particulier, lorsque vous avez :

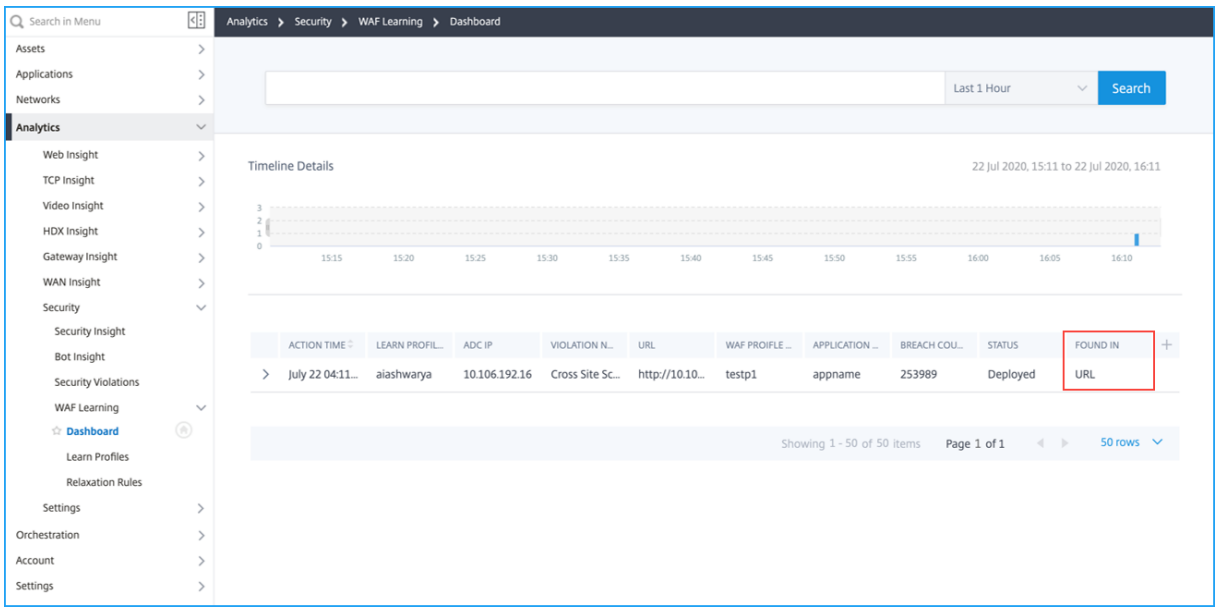
- Une grande entreprise avec de nombreux centres de données
- Configuration de nombreuses instances Citrix ADC pour chaque centre de données
- Configuration de nombreuses applications déployées ou accessibles via chaque instance Citrix ADC
- Clients accédant à l'application depuis différents emplacements

Pour de plus amples informations, consultez Service Graph - Vue holistique de toutes les applications

[NSADM-52149]

Amélioration des messages de journal en cas de violation de script intersite

Le tableau de bord **WAF Learning** avec violation de script inter-site déployée vous permet désormais d'afficher un nouvel attribut. Ce nouvel attribut spécifie l'emplacement de violation de script intersite. L'emplacement de violation peut être le champ de formulaire, l'URL, l'en-tête, le cookie ou d'autres emplacements.



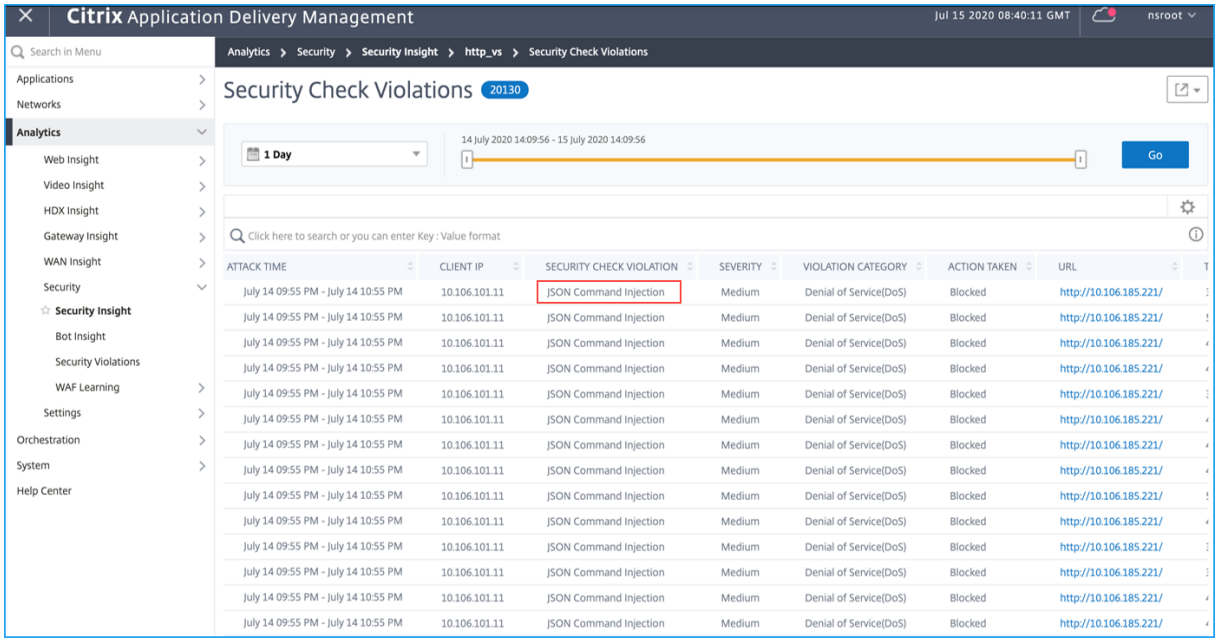
[NSADM-52941]

Security Insight — Injection de commandes JSON

Dans **Security Insight**, vous pouvez désormais afficher un nouveau type de violation, JSON Command Injection. Pour générer la violation d'injection de commandes JSON dans Security Insight, vous devez configurer la commande suivante dans l'instance Citrix ADC :

```
add appfw profile abc_js -type JSON -startURLaction none -starturlclosure
off -jsoncmdinjectionaction block log stats -jsoncmdinjectiontype cmdkeyword
```

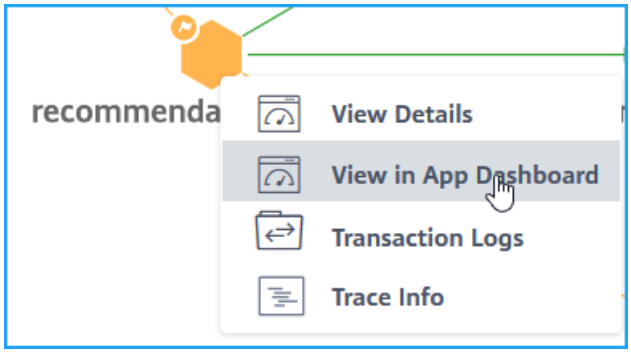
Après avoir configuré, vous pouvez afficher l'attaque par injection de commandes JSON dans Security Insight.



[NSADM-52869]

Graphique de service pour l'application Kubernetes — Afficher les détails de l'application dans le tableau de bord de l'application

Dans le graphique de service, lorsque vous cliquez sur un service et que vous sélectionnez **Afficher dans le tableau de bord de l'application**, les détails de l'application sélectionnée s'affichent dans le tableau de **bord de l'application**.



Pour de plus amples informations, consultez la section Détails de la demande pour les applications de microservices.

[NSADM-56583]

Afficher les informations de sécurité et les détails des attaques sur les robots dans les violations de sécurité des applications

Dans **App Security Violation**, vous pouvez désormais afficher les informations de sécurité et les détails des attaques de robot dans les catégories **WAF** et **Bot** respectivement. Accédez à **Analytics > Sécurité > Violations** de sécurité pour afficher les violations suivantes :

WAF	Bot
Dépassement de tampon	Crawler
Type de contenu	Feed Fetcher
Cohérence des	Vérificateur de liens
Balisage de formulaire CSRF	Marketing
Refuser URL	Scraper
Cohérence des champs de formulaire	Créateur de capture d'écran
Formats de champs	Moteur de recherche
Nombre maximal de téléchargements	Agent de service
En-tête du référent	Moniteur de site
Commerce sécurisé	Tester de vitesse
Objet sécurisé	Outil
Injection SQL HTML	Sans catégorie
URL de démarrage	Analyseur de virus
Script intersite **(XSS)**	Analyseur de vulnérabilité
DoS XML	Attente DeviceFP dépassée
Format XML	DeviceFP non valide
XML WSI	Réponse Captcha non valide
XML SSL	Tentatives de captcha dépassées
Pièce jointe XML	Réponse Captcha valide
Erreur SOAP XML	Captcha client en sourdine
Validation XML	Temps d'attente Captcha dépassé
Autres	Limite de taille de demande dépassée
Réputation IP	Limite de débit dépassée
HTTP DOS	Liste de blocage (IP, sous-réseau, expression de stratégie)

WAF	Bot
Petite fenêtre TCP	Autoriser la liste (IP, sous-réseau, expression de stratégie)
Violation signature	Demande de zéro pixel
Type de téléchargement de fichier	IP source
Script inter-site JSON **(XSS)**	Hôte
JSON SQL	Géolocalisation
JSON DOS	URL
Injection commande	
Induire le type de contenu XML	
Détournement de cookies	

[NSADM-54296]

Analyse de pointe de l'utilisation et des périodes de réduction - Évaluez les limites d'échelle des applications et identifiez les 5 principales fenêtres de maintenance des applications

En tant qu'administrateur, vous devez analyser le trafic et trouver le bon moment pour décider :

- Lorsque vous souhaitez mettre à l'échelle l'application dans l'environnement de production
- Lorsque vous souhaitez planifier le temps d'arrêt de l'application

La fonctionnalité d'analyse d'utilisation maximale et des périodes creuses dans Citrix ADM vous permet d'analyser les mesures clés pour une durée sélectionnée. À partir de ces mesures, vous pouvez analyser le trafic et décider quand vous souhaitez augmenter l'application Web ou planifier un temps d'arrêt planifié.

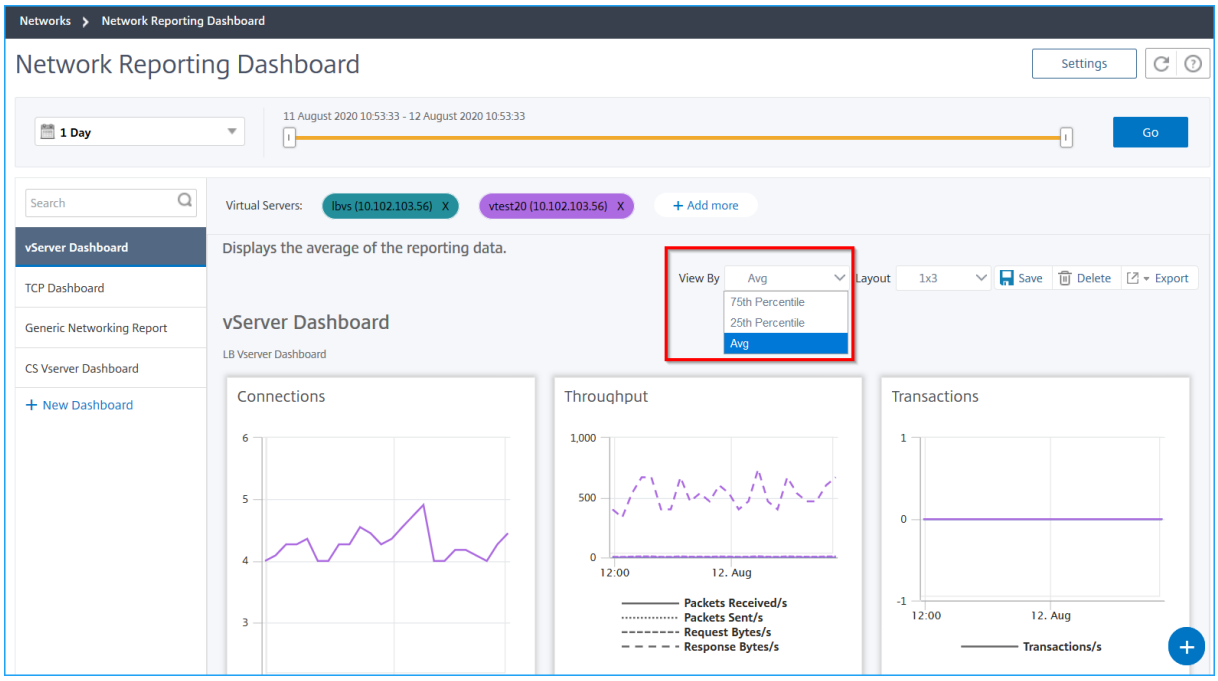
Pour de plus amples informations, consultez la section Analyse de pointe de l'utilisation des applications et des périodes creuses.

[NSADM-52167],[NSADM-52140]

Afficher les données de reporting réseau en appliquant des agrégations

Vous pouvez désormais appliquer des agrégations aux données de performances réseau et afficher les performances des applications sur le tableau de bord. Vous pouvez également exporter les résultats

en fonction de vos besoins. En utilisant ces agrégations appliquées aux données, vous pouvez analyser et vous assurer que toutes les ressources sont utilisées de manière optimale. Accédez à **Réseau > Rapports réseau** et sélectionnez la durée d'un jour ou plus tard pour obtenir l'option Afficher par.



Dans les données existantes, vous pouvez appliquer des agrégations en sélectionnant l'option dans la liste **Afficher par**. Pour de plus amples informations, consultez Afficher les données de reporting réseau en appliquant des filtres d'agrégation

[NSADM-56494]

Sélectionnez le type de licence d'évaluation dans le déploiement intelligent

Vous pouvez désormais découvrir la solution ADM Autoscale à l'aide de la licence d'évaluation. Lorsque vous choisissez l'option **Smart Deployment** pour déployer des instances ADC dans AWS, vous pouvez désormais sélectionner le type de licence **d'évaluation**. Cette option vous permet de déployer le produit Citrix ADC VPX Express. Et, il peut mettre à Autoscale jusqu'à trois instances.

[NSADM-52143]

Problèmes résolus

Système de licences

Les licences dans Citrix ADM sont désactivées en raison du redémarrage de l'agent.

[NSHELP-23539]

Réseaux

L'état de l'agent Citrix ADM s'affiche `reset:requested`, même après la réussite de l'enregistrement de l'agent.

[NSHELP-23413]

StyleBooks

Lorsque vous configurez une application de groupe Mise à l'Autoscale à l'aide de StyleBooks par défaut, elle ne prend pas en charge les types de moniteurs DNS et UDP. Avec ce correctif, les versions du groupe Autoscale suivantes StyleBooks sont mises à jour :

- lb-mon-autoscale-v1.5
- cs-lb-mon-autoscale-v1.4

[NSADM-55982]

24 juillet 2020

Violations de sécurité des applications - Réseau

Vous pouvez désormais afficher l'attaque Smack par segment dans le cadre des violations réseau dans les violations de sécurité des applications. Pour de plus amples informations, consultez la section Violations de la sécurité.

[NSADM-46025]

Graphique de service pour les applications Kubernetes - Afficher les mesures client pour résoudre les problèmes

Dans Service Graph pour les applications Kubernetes, vous pouvez désormais afficher l'emplacement à partir duquel le client accède au service. En tant qu'administrateur, vous pouvez visualiser les mesures client et analyser les problèmes qui se produisent à partir du client.

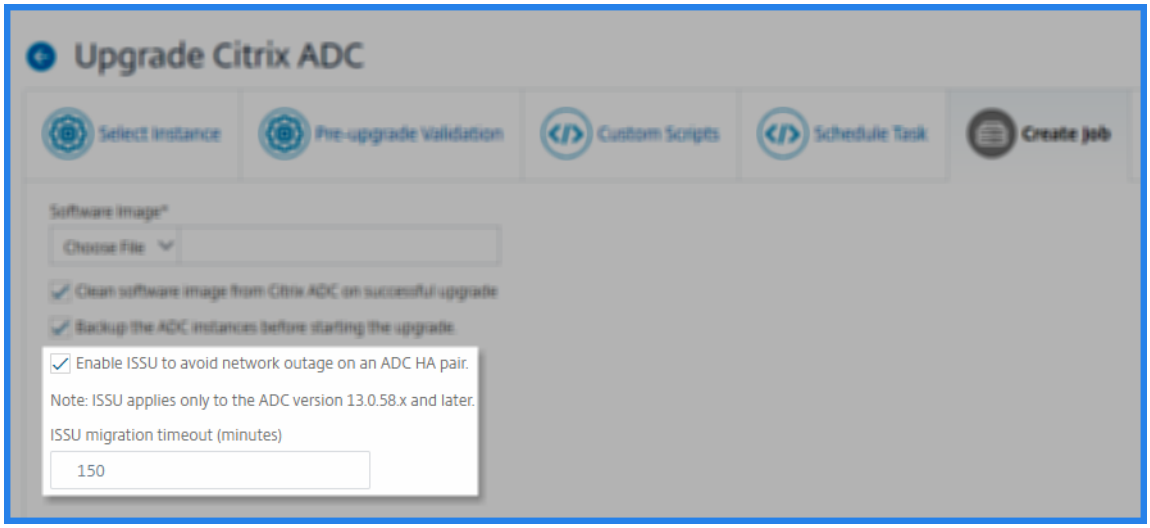
Pour de plus amples informations, consultez la section Afficher les détails dans le graphique de service.

[NSADM-54335]

Prise en charge de la mise à niveau logicielle en service

Vous pouvez maintenant sélectionner l'option ISSUE (In-Service-Software-Upgrade) lors de la création d'un travail de mise à niveau. ISSU garantit la mise à niveau zéro temps d'arrêt sur une paire ADC haute disponibilité. La fonctionnalité ISSU fournit une fonctionnalité de migration qui respecte les

connexions existantes lors de la mise à niveau. Ainsi, vous pouvez mettre à niveau une paire ADC HA sans temps d'arrêt.



[NSADM-43357]

Lister dynamiquement les réseaux de gestion des adresses IP ADM (IPAM) dans StyleBooks

Vous pouvez désormais créer un StyleBook qui permet à un utilisateur de sélectionner un réseau ADM IPAM à partir duquel il alloue automatiquement une adresse IP. La liste des réseaux IPAM est extraite dynamiquement d'ADM. Auparavant, vous étiez en mesure de sélectionner les réseaux IPAM mentionnés dans la définition de **StyleBook**.

Un nouvel attribut `dynamic-allocation` est maintenant ajouté dans la définition du paramètre de `type:ipaddress`. Il peut prendre **`true`** ou **`false`** en tant qu'entrée. Lorsque vous définissez sa valeur sur **`true`**, un utilisateur peut sélectionner un réseau dans la liste des réseaux IPAM présents dans ADM. Ensuite, l'ADM alloue automatiquement une adresse IP à partir du réseau sélectionné.

Exemple :

```
1   -
2     name: virtual-ip
3     label: "Load Balancer IP Address"
4     type: ipaddress
5     dynamic-allocation: true
6     required: true
7  <!--NeedCopy-->
```

Dans cet exemple, le `virtual-ip` champ répertorie les réseaux IPAM qui sont dans ADM. Sélectionnez un réseau dans la liste pour allouer automatiquement une adresse IP à partir du réseau. L'adresse IP est libérée sur le réseau lorsque la configuration est supprimée.

[NSADM-54246]

Améliorations des autorisations utilisateur des StyleBooks et des packs de configuration

En tant qu'administrateur, vous pouvez désormais avoir un meilleur contrôle sur l'autorisation de StyleBooks et de packs de configuration spécifiques à des groupes d'utilisateurs dans la page **Compte > Administration des utilisateurs > Groupes**. Les sections **StyleBooks** et **Configpacks** dans **Paramètres d'autorisation** sont désormais améliorées avec les modifications suivantes :

- **StyleBooks** — Vous pouvez désormais spécifier la liste autorisée de StyleBooks à l'aide d'une expression de filtre pouvant contenir des expressions régulières.

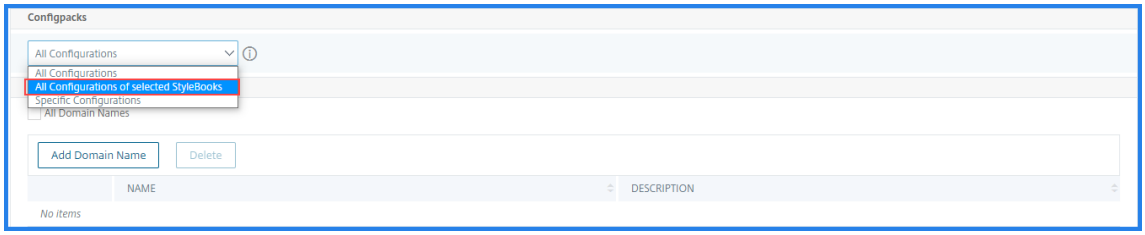
  Exemple :

  ```
  name=lb-mon|lb AND namespace=com.citrix.adc.stylebooks AND version=1.0
  ```

  Cette requête répertorie les StyleBooks qui remplissent les conditions suivantes :

  - Le nom de StyleBook est `lb-mon` ou `lb`.
  - L'espace de noms StyleBook est `com.citrix.adc.stylebooks`.
  - La version StyleBook est `1.0`.

- **Packs de configuration** : vous pouvez désormais autoriser l'utilisateur pour les packs de configuration appartenant aux StyleBooks sélectionnés. Pour ce faire, sélectionnez **Toutes les configurations des StyleBooks sélectionnés** dans la section **Configpacks**.

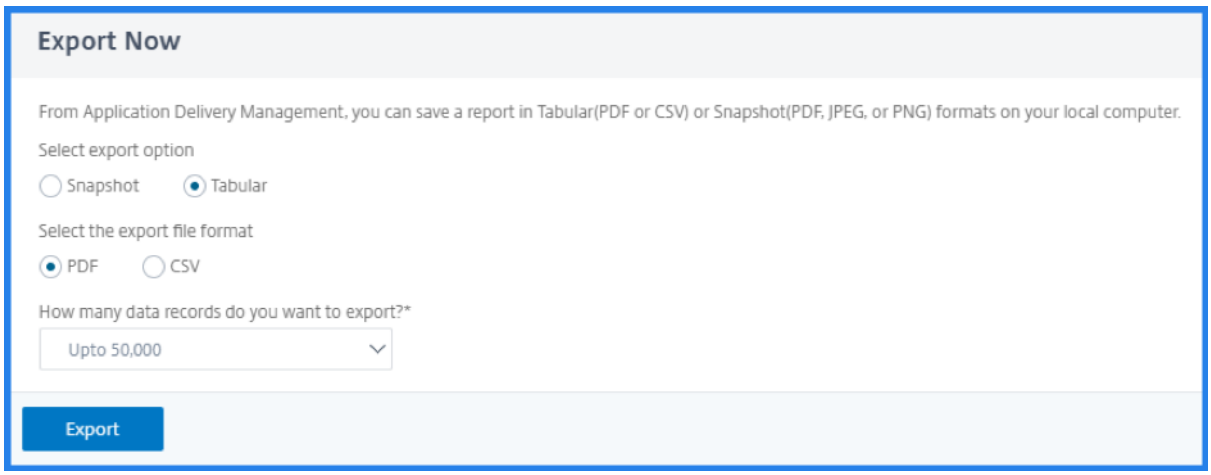


[NSADM-52334]

15 juillet 2020

Exporter les rapports ADM dans un format tabulaire

Vous pouvez désormais exporter des rapports ADM sous forme de tableau ou d'instantané. Vous pouvez également choisir le nombre d'enregistrements de données à exporter dans un format tabulaire. Auparavant, vous étiez en mesure d'exporter des rapports uniquement sous forme d'instantané.

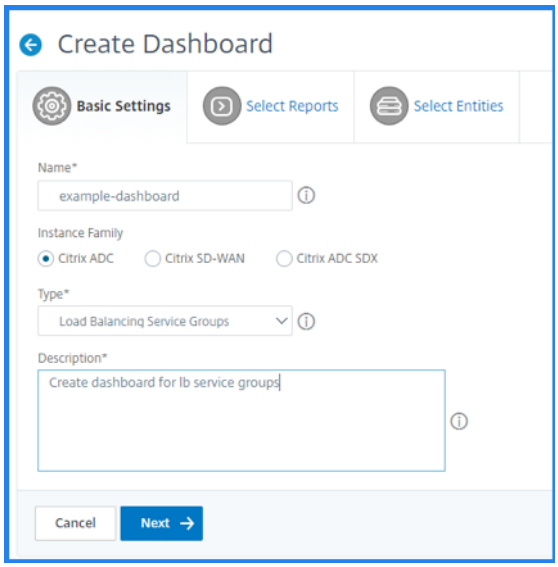


Pour de plus amples informations, consultez la section Exporter ou planifier des rapports d'exportation.

[NSADM-52461]

Générer des rapports réseau pour les groupes de services d'équilibrage de charge

Vous pouvez désormais créer un tableau de bord de reporting réseau pour les groupes de services d'équilibrage de charge et les services. Auparavant, vous étiez en mesure de créer un tableau de bord pour les services d'équilibrage de charge uniquement.



Ce tableau de bord peut afficher les rapports suivants pour les groupes de services sélectionnés :

- Connexions : pour les compteurs de connexions client et serveur.
- Débit : pour les compteurs d'octets de requête et de réponse.
- Délai avant le premier octet (TTFB) : temps moyen nécessaire pour envoyer un paquet de demande à un groupe de services et recevoir le premier paquet du groupe de services. Ce temps

de réponse est appelé TTFB.

Pour de plus amples informations, consultez la section Rapports sur le réseau.

[NSADM-51596]

Prise en charge de l'authentification, de l'autorisation et de l'audit des rapports d'interrogation et de réseau

Citrix ADM interroge désormais les événements d'authentification, d'autorisation et d'audit (Citrix ADC AAA) à partir d'une instance ADC et vous permet de visualiser leur tendance dans Network Reporting. L'interface graphique ADM inclut les rapports réseau Citrix ADC AAA suivants pour créer un tableau de bord :

- **Succès de l'authentification HTTP vs échecs**
- **Succès de l'authentification non-HTTP vs échecs**
- **Sessions AAA**
- **Sessions AAA actuelles**
- **Sessions ICAOnly actuelles**
- **Connexions ICAOnly actuelles**
- **Connexion ICA (SmartAccess) actuelle**
- **Réussite et échecs de l'authentification**

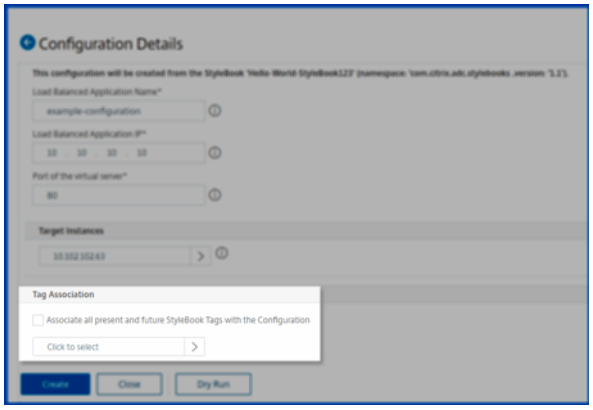
Pour de plus amples informations, consultez la section Rapports sur le réseau.

[NSADM-51372]

Associer les balises StyleBook à leur configuration

Dans StyleBooks, le terme **Label** est renommé **Tag**. Vous pouvez désormais associer les balises StyleBook à son pack de configuration. Ainsi, vous pouvez rechercher les packs de configuration à l'aide des balises StyleBook lui-même.
Lorsque vous créez un pack de configuration, utilisez l'une des options suivantes dans la section **Association de balises** :

- **Associer toutes les balises StyleBook présentes et futures à la configuration** : cette option associe toutes les balises StyleBook à un pack de configuration. Il veille également à associer les nouvelles balises que vous pourriez ajouter aux StyleBooks à l'avenir.
- **Sélectionner les balises** : cette option affiche les balises du StyleBook sélectionné. Vous pouvez sélectionner les balises StyleBook requises et les associer à un pack de configuration.



Pour de plus amples informations, consultez la section Créer une balise pour le StyleBook.

[NSADM-53600]

Les StyleBooks prennent en charge les paramètres

Vous pouvez désormais contrôler dynamiquement l'apparence d'un paramètre ou sa valeur initiale dans l'écran de configuration StyleBook en fonction de la valeur spécifiée dans un autre paramètre. Pour ce faire, utilisez l' `dependent-parameters` attribut dans la définition du paramètre. Cet attribut est nouvellement ajouté en tant que nouveau `gui` sous-attribut.
Spécifiez cet attribut sur un paramètre source qui contrôle le comportement du paramètre sur le formulaire. Dans cet attribut, vous pouvez inclure plusieurs conditions qui contrôlent d'autres paramètres.
Par exemple, un protocole de paramètre source peut avoir un certificat de paramètre dépendant, qui n'apparaît que si la valeur du paramètre de protocole est SSL.
Chaque condition peut avoir les attributs suivants :

- `target-parameter` : spécifiez le paramètre cible auquel cette condition s'applique.
- `matching-values` : spécifiez la liste des valeurs du paramètre source qui déclenche l'action.
- `action` : spécifiez l'une des actions suivantes sur le paramètre ciblé :
  - `read-only` : le paramètre est en lecture seule.
  - `show` : le paramètre apparaît dans le formulaire s'il est masqué.
  - `hide` : le paramètre est supprimé du formulaire.
  - `set-value` : la valeur du paramètre est définie sur la valeur spécifiée dans l'attribut value
- `value` : la valeur du paramètre cible si l'action est `set-value`

Lorsqu'une entrée utilisateur correspond aux valeurs spécifiées sur le paramètre source, l'apparence ou la valeur du paramètre cible change en fonction de l'action spécifiée.

Pour de plus amples informations, consultez la section paramètres dépendants.

[NSADM-52329]

Afficher les utilisateurs qui ont créé ou mis à jour une configuration StyleBook

Dans **StyleBook > Configurations**, une nouvelle colonne est ajoutée qui affiche les utilisateurs qui ont créé ou mis à jour le pack de configuration pour la dernière fois. Si vous souhaitez filtrer les packs de configuration par utilisateurs, sélectionnez l'option Créé par dans la liste des propriétés pour filtrer les packs de configuration.

[NSADM-52336]

Utiliser un script pour activer l'agent zéro contact dans AWS

Lorsque vous lancez un agent ADM dans AWS, vous pouvez désormais spécifier un script d'enregistrement automatique de l'agent en tant que données utilisateur. Un exemple de script est fourni dans Installer l'agent Citrix ADM sur AWS. Ce script récupère les détails d'authentification à partir du gestionnaire de secrets AWS et exécute le script deployment.py pour enregistrer l'agent auprès du service ADM.
Alternativement, vous pouvez toujours effectuer l'une des opérations suivantes :

- Spécifiez les détails d'authentification réels dans les données utilisateur qui enregistrent automatiquement l'agent lors du démarrage.
- Utilisez le script deployment_type.py pour enregistrer un agent après qu'il démarre correctement. Pour de plus amples informations, consultez la section Installer l'agent Citrix ADM sur AWS.

[NSADM-55322]

Apprentissage WAF dans Citrix ADM

En tant qu'administrateur, vous pouvez désormais configurer des profils d'apprentissage pour générer la liste des règles de relaxation :

- Uniquement pour les applications Web sélectionnées
- Uniquement pour les noms de profil sélectionnés

Pour de plus amples informations, consultez la section Configurer le profil d'apprentissage.

[NSADM-49494]

Violations de sécurité des applications - Réseau

Outre les violations de sécurité des applications existantes, vous pouvez désormais afficher les violations suivantes dans le cadre des violations réseau :

- Attaque de désynchronisation HTTP
- Attaque de Bleichenbacher

Pour de plus amples informations, consultez la section Détails sur la violation de sécurité des applications.

[NSADM-49468],[NSADM-46460]

Afficher les mesures d'entrée et les détails de la pénétration pour le dépannage

Dans le graphique de service, vous pouvez maintenant afficher :

- Mesures de pénétration
- Détails de la pénétration (exploration vers le bas)
- Le type de pénétration utilisé
  - **Tier 1** : Citrix Ingress Controller dans le cluster Kubernetes configure une instance Citrix ADC (VPX/MPX/SDX/BLX) en dehors du cluster Kubernetes.
  - **Tier 2** : Citrix Ingress Controller s'exécute en tant que sidecar avec l'instance Citrix ADC CPX dans le cluster Kubernetes.

    > Remarque : Vous pouvez afficher l'entrée de niveau 1 et l'entrée de niveau 2 uniquement si vous avez configuré une architecture à deux niveaux (entrée de niveau 1 à l'aide d'ADC en tant que MPX/VPX/SDX/BLX et entrée de niveau 2 en utilisant ADC comme CPX) dans le cluster Kubernetes.

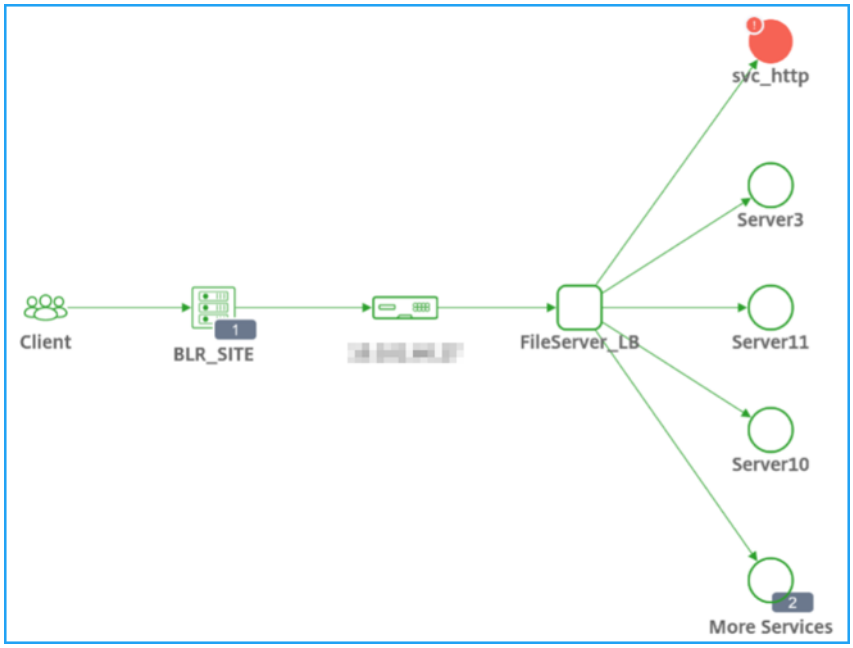
Pour de plus amples informations, consultez Afficher les détails d'entrée pour résoudre les problèmes

[NSADM-53755]

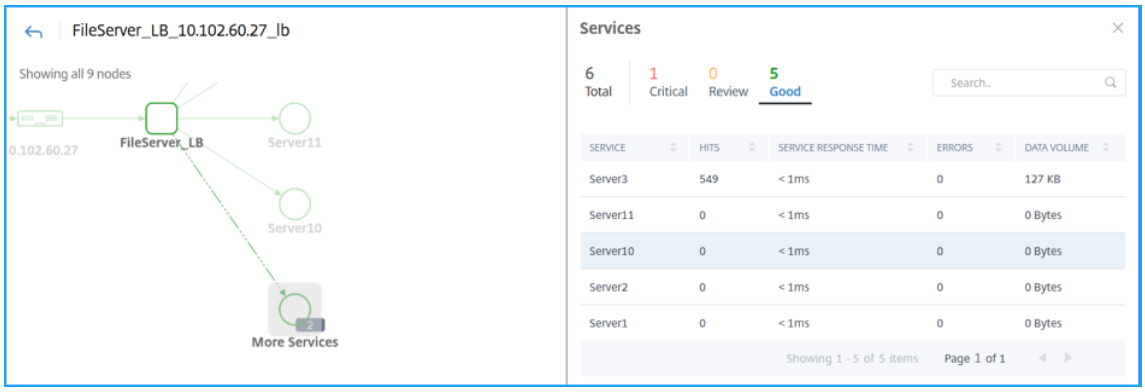
Graphique des services d'applications Web à 3 niveaux

Le graphique des services d'applications Web à 3 niveaux est désormais improvisé avec les modifications suivantes :

- Les services sont regroupés et seuls les quatre services les plus faibles sont affichés.

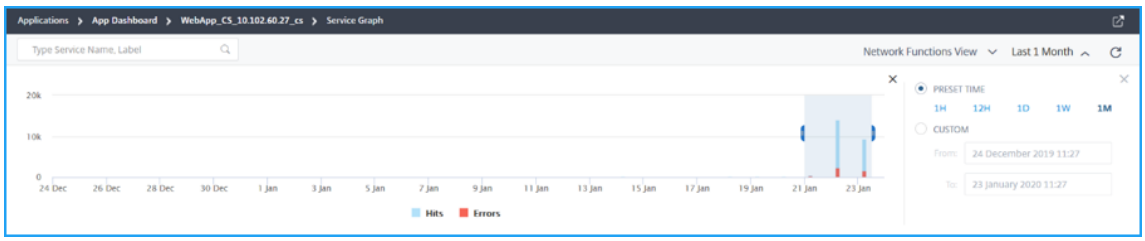


Cliquez sur **Plus de services** pour afficher tous les services en fonction de leur statut, tels que **Critical**, **Review**et **Bon**.

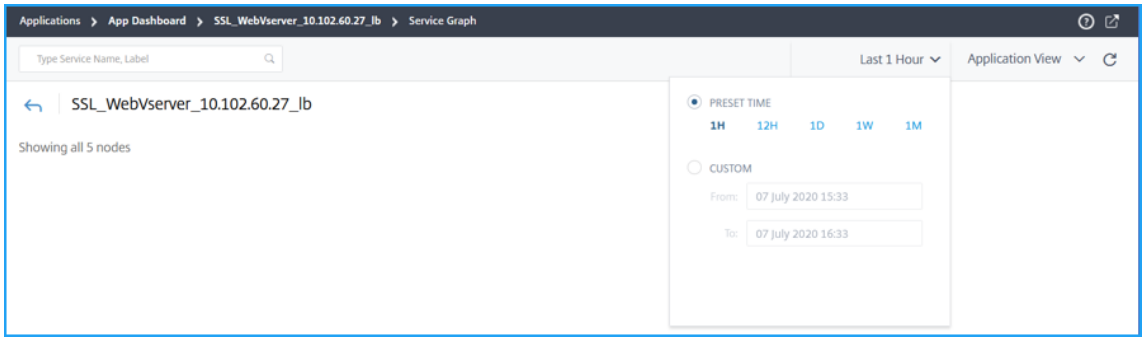


- Le graphique à barres **Hits and Erreurs** n'est pas visible.

  Plus tôt

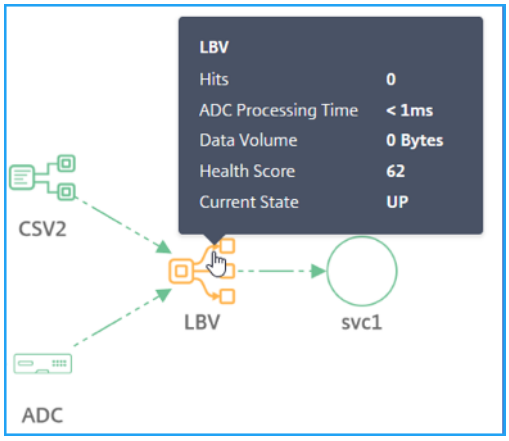


  Maintenant

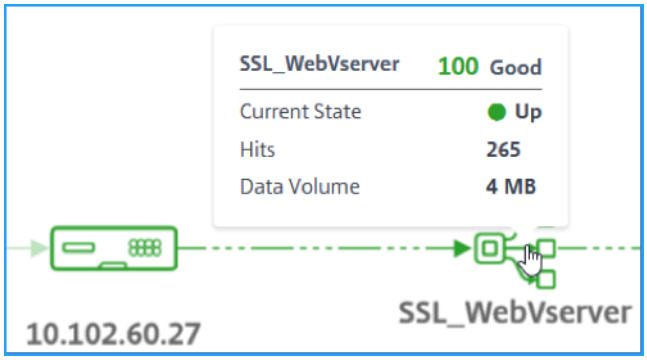


- Les mesures des fonctions réseau sont mises à jour.

  Plus tôt



  Maintenant

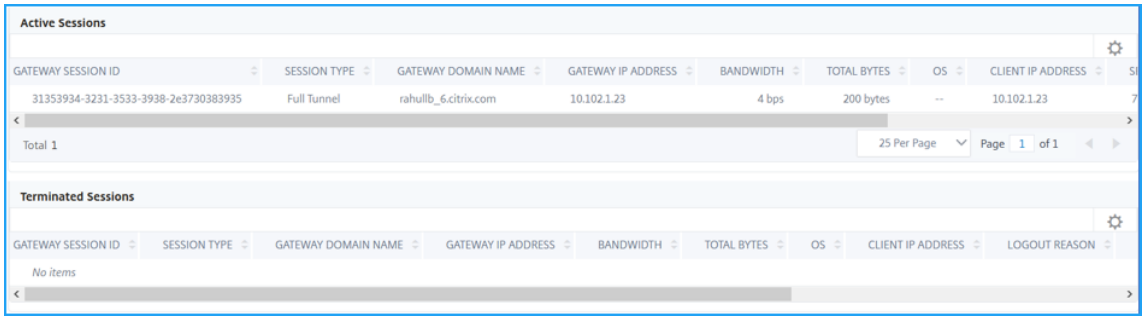


[NSADM-52147]

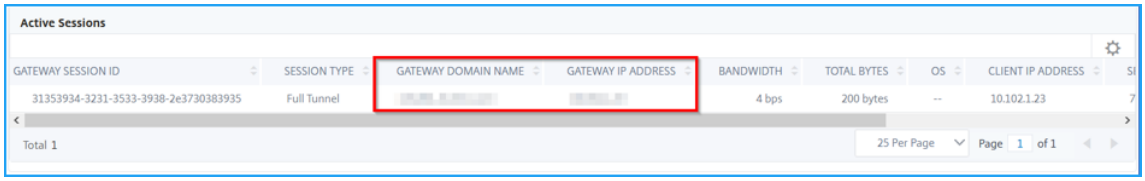
Amélioration de Gateway Insight

Dans Gateway Insight, vous pouvez désormais afficher les améliorations suivantes pour les utilisateurs de la passerelle. En tant qu'administrateur, ces améliorations vous permettent d'obtenir des informations utilisateur complètes lorsque vous exportez le rapport. Accédez à **Analytics > Gateway Insight > Utilisateurs** et sélectionnez un utilisateur à afficher :

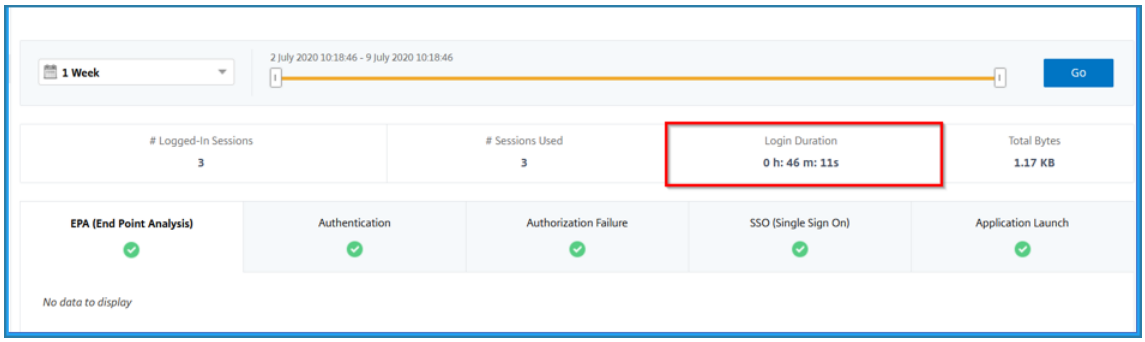
- L'utilisateur **Sessions actives et Sessionsterminées**.



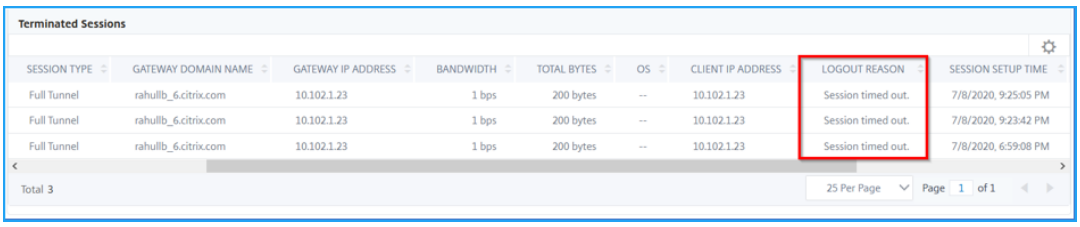
- Le nom de domaine de la passerelle et l'adresse IP de la passerelle dans les **sessions actives**.



- Durée de connexion de l'utilisateur.



- Raison de la session de déconnexion de l'utilisateur. Les raisons de déconnexion peuvent être :
  - Session expirée
  - Déconnecté en raison d'une erreur interne
  - Déconnecté en raison de la session inactive expiré
  - L'utilisateur s'est déconnecté
  - L'administrateur a arrêté la session



[NSADM-52763], [NSADM-52767], [NSADM-52764], [NSADM-53496]

Prise en charge de l'agent intégré pour les instances SDX

Les agents intégrés Citrix ADM sont désormais disponibles sur les instances SDX. En outre, vous pouvez lancer l'agent intégré à l'aide de `MASTools`. Pour en savoir plus, voir Configurer l'agent intégré ADC pour gérer les instances

Problèmes résolus

Analytics

Lorsque ADM recueille les informations de mesure ADC, l'utilisation du processeur devient élevée.

[NSADM-56374]

Systèmes

Lorsque vous activez **les informations d'identification et de connexion d'instance** dans la page **Paramètres système**, l'interface graphique ADM n'affiche pas les informations de licence dans le tableau de bord **Instance**.

[NSHELP-23944]

Réseaux

Sous **Réseaux > Licences**, l'interface graphique ADM affiche des informations de licence incorrectes pour les instances gérées, si le nombre d'instances gérées dépasse la limite maximale de 58 instances. Avec le correctif, la limite pour les instances maximales est augmentée à 1000.

[NSHELP-23956]

30 juin 2020

Violations de sécurité des applications : adresses IP uniques excessives par géo

L' **indicateur Excès d'adresses IP uniques par géo** vous permet désormais d'afficher une carte géographique qui affiche le total des anomalies en fonction des régions. Le graphique indique les détails de violation pertinents de la région sélectionnée.

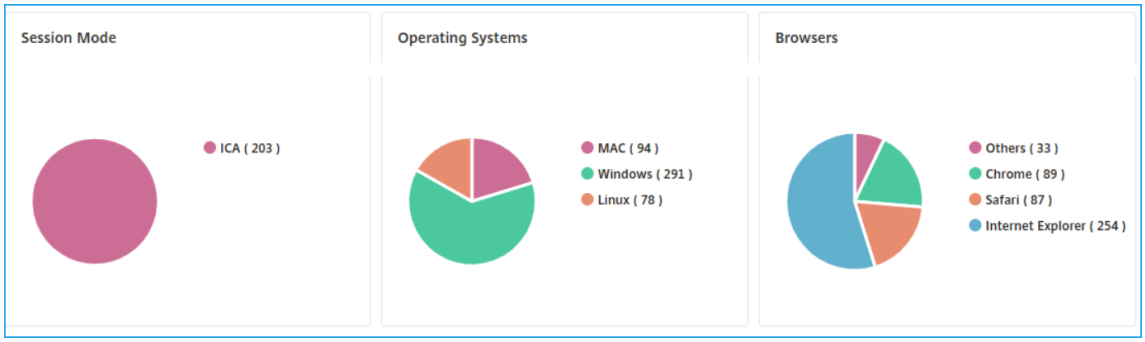
Pour de plus amples informations, consultez la section IPs uniques excessifs par géo.

[NSADM-52555]

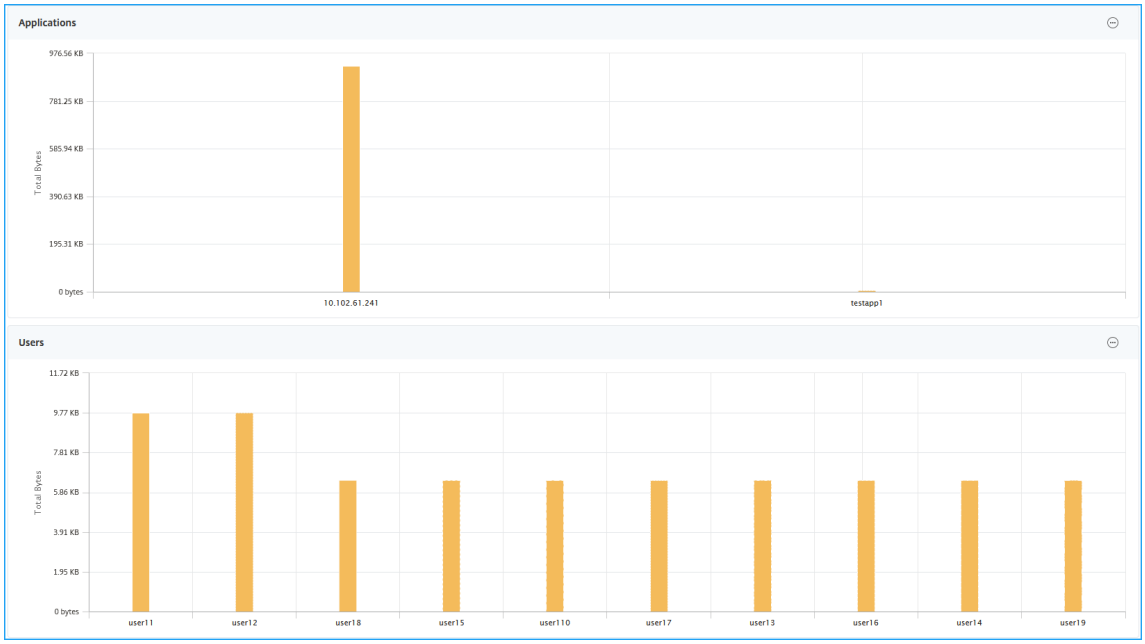
Amélioration de Gateway Insight

Dans Gateway Insight, vous pouvez désormais afficher les améliorations suivantes :

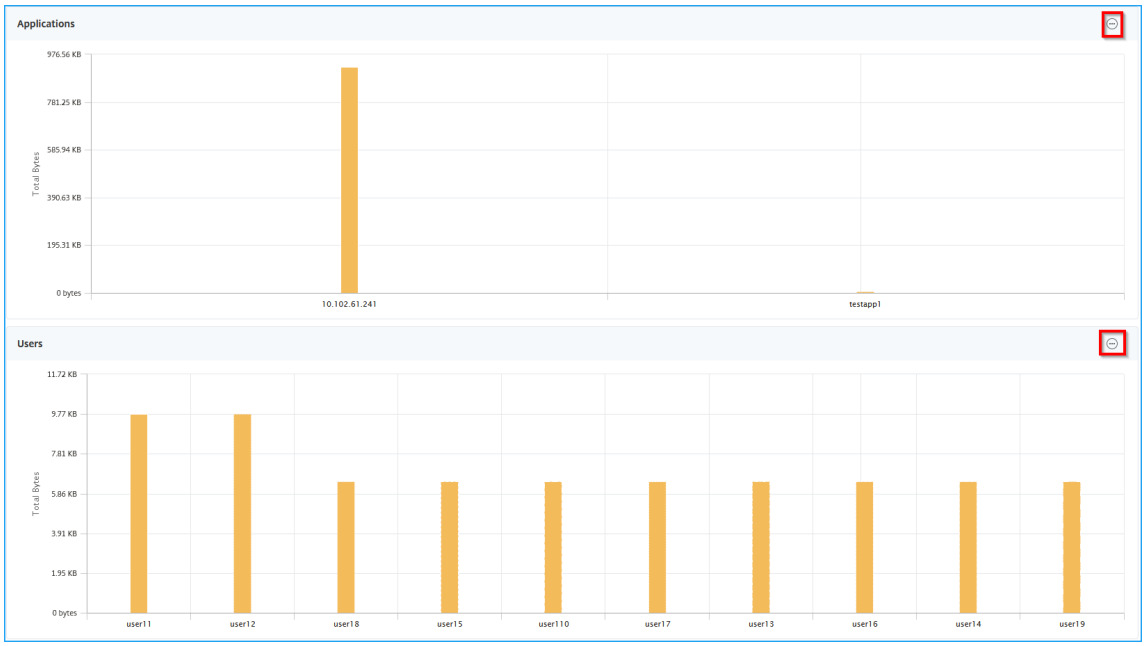
- **Détails de l'utilisateur** - Vous pouvez afficher des informations pour chaque utilisateur associé aux appliances de passerelle ADC. Accédez à **Analytics** > **Gateway Insight** > **Utilisateurs** et cliquez sur un utilisateur pour afficher les informations relatives à l'utilisateur sélectionné, comme le mode session, le système d'exploitation et les navigateurs.



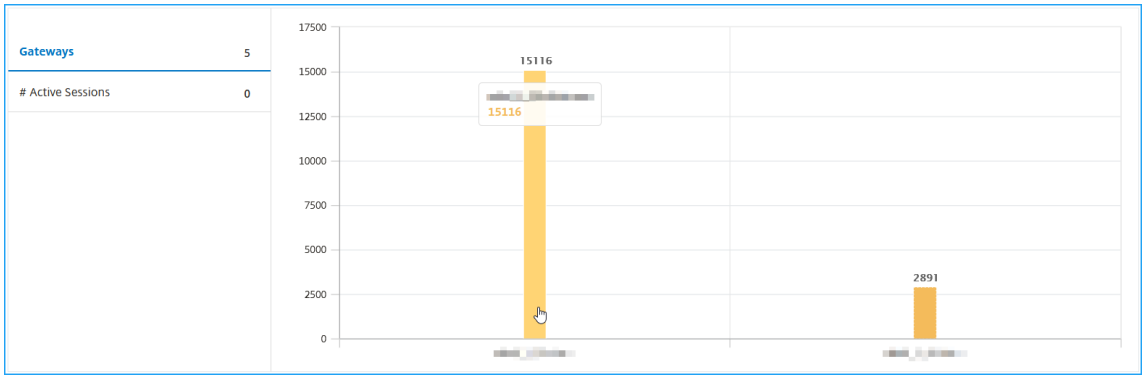
- **Utilisateurs et applications pour la passerelle sélectionnée** - Accédez à **Analytics** > **Gateway Insight** > **Gateway** et cliquez sur un nom de domaine de passerelle pour afficher les 10 principales applications et les 10 principaux utilisateurs associés à la passerelle sélectionnée.



- **Afficher plus d'option pour les applications et les utilisateurs** : pour plus de 10 applications et utilisateurs, vous pouvez cliquer sur l'icône Plus dans Applications et utilisateurs pour afficher tous les détails des utilisateurs et applications associés à la passerelle sélectionnée.



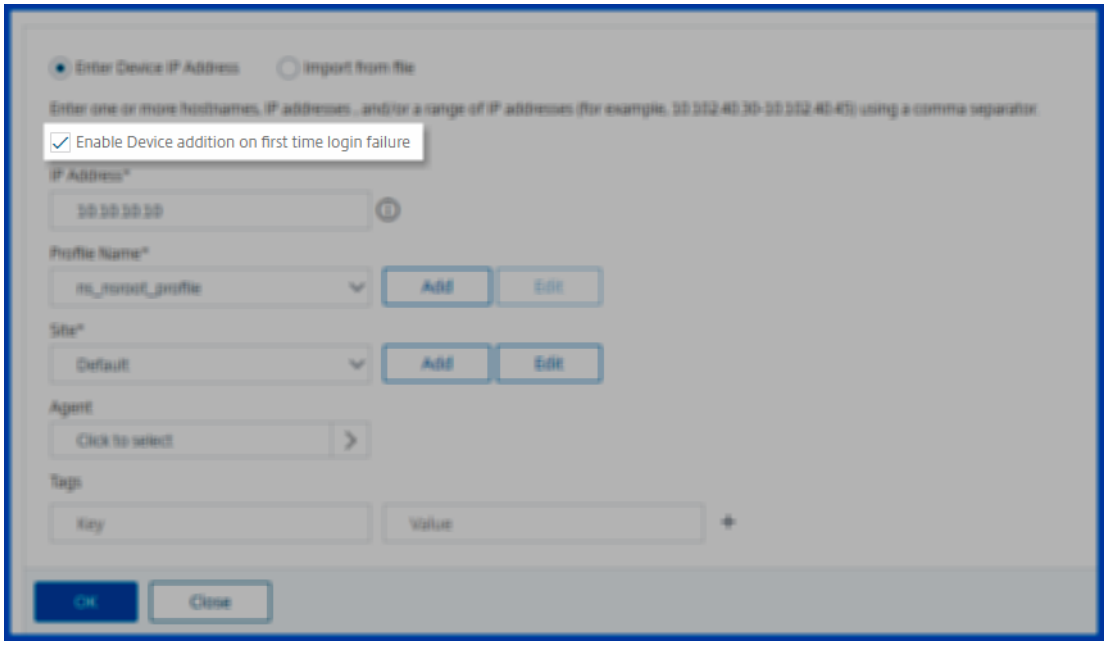
- **Afficher les détails en cliquant sur le graphique à barres** — Lorsque vous cliquez sur un graphique à barres, vous pouvez afficher les détails pertinents. Par exemple, accédez à **Analytics > Gateway Insight > Gateway** et cliquez sur le graphique à barres de passerelle pour afficher les détails de la passerelle.



[NSADM-53489], [NSADM-53508], [NSADM-53906], [NSADM-52768]

Possibilité d'ajouter une instance ADC sans informations d'identification valides

Lorsque vous ajoutez une instance dans Citrix ADM pour la première fois, vous pouvez désormais l'ajouter même sans informations d'identification valides. Une fois l'instance ajoutée, elle apparaît dans l'état DOWN dans la page **Réseaux > Instance > Citrix ADC**, avec un avertissement Échec de la connexion. Spécifiez les informations d'identification correctes pour gérer l'instance dans ADM.



Si l'instance n'est pas sous licence, l'option **License** apparaît lorsque vous sélectionnez l'instance. Cliquez sur **License** pour appliquer la licence à une instance à partir du pool de licences.

[NSADM-44856]

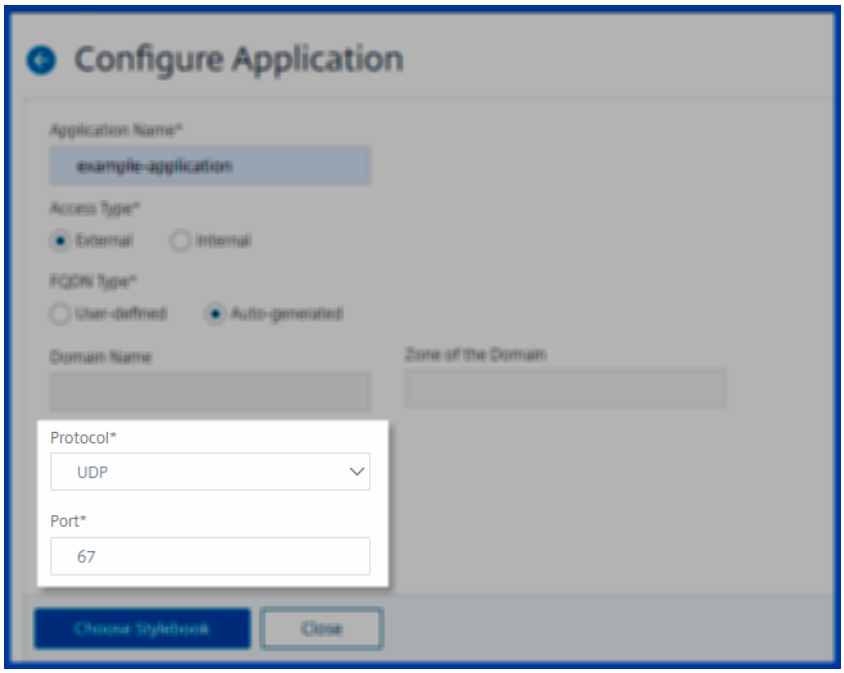
Afficher le pool d'instances ADC FIPS sous la page Capacité groupée

Les instances FIPS ADC peuvent désormais extraire des licences du pool d'instances FIPS. Par conséquent, l'interface graphique ADM affiche les licences groupées allouées aux instances FIPS sous la page **Réseaux > Licences > Licences de bande passante > Capacité groupée**.

[NSADM-51207]

Les applications de groupe Autoscale dans Azure prennent en charge le trafic UDP

Les applications du groupe Autoscale qui sont dans Azure peuvent désormais recevoir du trafic UDP. Lorsque vous configurez une application sur le groupe Mise à l'Autoscale, sélectionnez le protocole **UDP** et la valeur de port pour autoriser le trafic UDP.



Avec cette fonctionnalité, les livres StyleBooks du groupe de mise à l'Autoscale suivants sont récemment ajoutés pour configurer une application :

- `lb-mon-autoscale-v1.4`
- `cs-lb-mon-autoscale-v1.3`

[NSADM-53288]

Problèmes résolus

Système de licences

L'état de la licence d'instance apparaît comme **Sync-In-Progress** au lieu de **Managed** lorsque les conditions suivantes sont remplies :

1. Les licences multiples appartiennent à la même édition et au même pool.
2. Une instance ADC retirait la licence du pool.

[NSADM-55928]

Système

- Les messages Syslog n'apparaissent pas dans l'interface graphique ADM.

  [NSADM-55822]

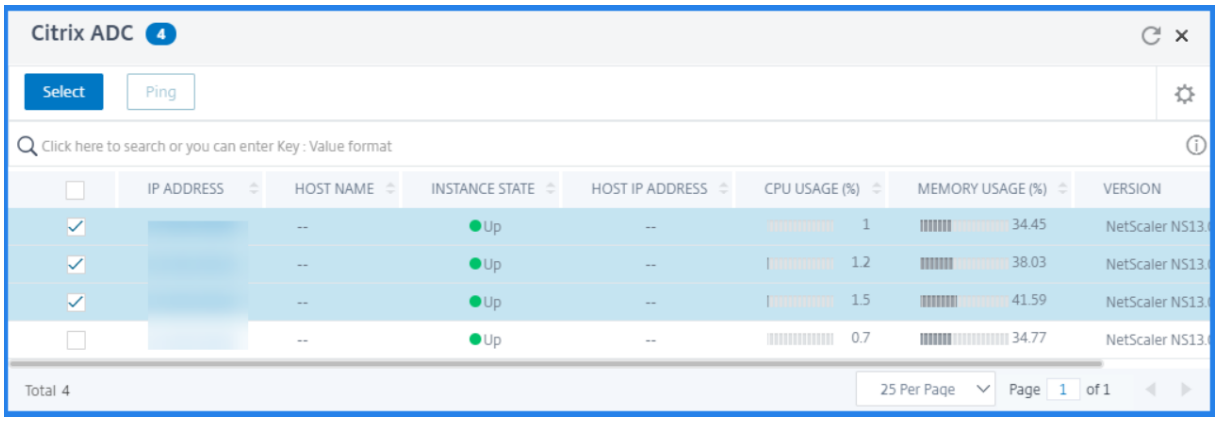
- Lorsque vous modifiez le groupe de l'utilisateur, l'erreur de complexité du mot de passe apparaît.

  [NSHELP-23497]

22 juin 2020

Sélection simultanée de plusieurs instances cibles

Lorsque vous souhaitez déployer le même pack de configuration sur plusieurs instances ADC, vous pouvez maintenant sélectionner simultanément les instances ADC requises. Auparavant, vous deviez sélectionner les instances une par une pour déployer le pack de configuration. Avec cette fonctionnalité, vous pouvez également filtrer les instances pour sélectionner les instances requises.



[NSADM-50115]

Afficher la distribution d'instance par leurs versions mineures

Le tableau de bord des instances affiche désormais la distribution des instances gérées par leurs versions mineures. Le graphique Version vous aide à visualiser le nombre de périphériques pour chaque version mineure.

[NSADM-42183]

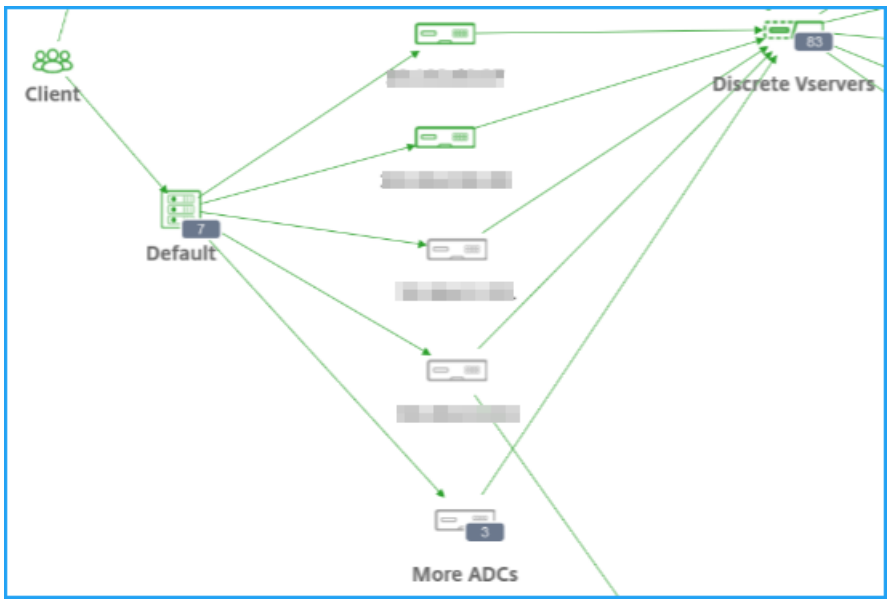
Graphique des améliorations apportées au service global

En tant qu'administrateur, la vue à volet unique du graphique de service global peut être difficile pour vous de surveiller les vues de l'infrastructure vers les applications, lorsque vous avez :

- Une grande entreprise avec de nombreux centres de données
- Configuration de nombreuses instances Citrix ADC pour chaque centre de données
- Configuration de nombreuses applications déployées ou accessibles via chaque instance Citrix ADC

Le graphique de service global amélioré élimine désormais la vue désorganisée et vous permet d'afficher :

- Le centre de données regroupé avec son nombre total d'instances Citrix ADC
- Seules les quatre premières instances Citrix ADC à faible score de chaque centre de données



Cliquez sur **Autres ADC** pour afficher toutes les instances Citrix ADC en sélectionnant les onglets d'état respectifs (Critique, Révision, Bon et Non applicable). Cliquez sur l'adresse IP de l'instance pour afficher les détails de l'instance tels que le score d'instance, les mesures clés et les problèmes associés à l'instance ADC.

> **Remarque**
>
> Vous pouvez également cliquer sur l'instance à partir du graphique de service global pour afficher les détails de l'instance Citrix ADC.

[NSADM-53249]

Problèmes résolus

Analytics

- Dans **Web Transaction Analytics**, les recherches enregistrées ne sont pas affichées après une actualisation de page.

  [NSADM-53722]

- Dans **Analytics** > **Web Insight**, les données attendues ne sont pas affichées pour toutes les pages de mesures (Client, Serveur, URL, méthodes de demande, statut de réponse, agents utilisateurs et systèmes d'exploitation)

  [NSADM-53632]

- Même après avoir configuré le RBAC approprié, les **applications dans Applications** > Tableau de **bord des applications** et les serveurs virtuels dans **Fonction réseau** > **Équilibrage de charge** n'affichent pas les données attendues, une fois qu'un nouveau stylebook ou configpack est ajouté par l'utilisateur du groupe.

  [NSHELP-23101]

GUI

- Dans une connexion VPN, ADM ne peut pas se connecter à l'interface graphique ADC en utilisant SSO (Single Sign On).

  [NSHELP-23099]

04 juin 2020

Diffusez votre application AWS en trois étapes lors de votre première connexion

Lorsque vous vous connectez à l'interface graphique ADM pour la première fois, vous pouvez fournir une application qui se trouve dans AWS à l'aide d'instances ADC en seulement trois étapes :

1. Enregistrez votre compte AWS auprès du service Citrix ADM en créant un profil d'accès au cloud.
2. Préparez votre environnement AWS en spécifiant la région AWS, les détails VPC et les licences ADC.

   L'environnement AWS comprend une infrastructure AWS, un agent ADM et un groupe ADM Autoscale. Au cours de cette étape, ADM crée les éléments suivants :

   - Une pile CloudFormation dans AWS pour créer l'infrastructure requise qui inclut des sous-réseaux, des groupes de sécurité, des passerelles NAT, etc.
   - Agent ADM dans le VPC pour gérer les instances ADC.

- Un groupe de mise à Autoscale ADC. Vous pouvez personnaliser ce groupe ultérieurement dans la page **Réseaux > Groupe de Autoscale**.

3. Après une préparation de l'environnement réussie, configurer des applications en utilisant StyleBooks pour livrer votre application.

Après la première ouverture de session, si vous souhaitez mettre à l'Autoscale des instances ADC, reportez-vous à la section Mise à l'échelle automatique de Citrix ADC à l'aide de Citrix ADM.

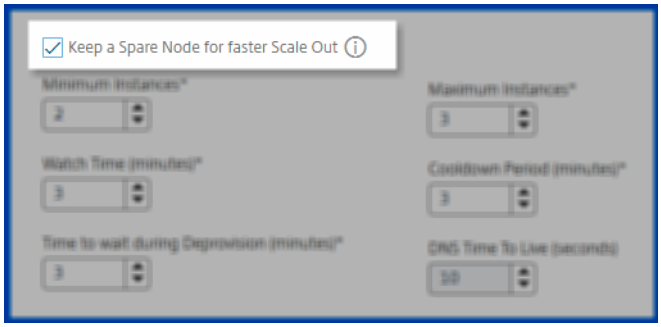
Pour de plus amples informations, consultez la section Mise en route.

[NSADM-47626]

Maintenir un nœud de rechange dans votre groupe Autoscale

Lorsque vous spécifiez des paramètres pour créer un groupe de mise à l'Autoscale, vous pouvez désormais choisir de conserver un nœud de rechange pour accélérer la mise à l'échelle.

ADM met en service un nœud de secours avant que l'action de mise à l'échelle ne se produise et l'arrête. Lorsque l'action de scale-out se produit pour le groupe Mise à l'Autoscale, l'ADM démarre le nœud de rechange déjà provisionné. En conséquence, il réduit le temps nécessaire pour la mise à l'échelle.



Pour de plus amples informations, consultez la section Configurer les paramètres de mise à l'échelle automatique.

[NSADM-48191]

Configurer une application de groupe Autoscale à l'aide du nom de domaine complet généré

Lorsque vous configurez une application pour le groupe Mise à l'Autoscale, vous pouvez désormais sélectionner un type de nom de domaine complet généré automatiquement. Cette option génère automatiquement le nom de domaine et de zone.

Si vous choisissez le type de nom de domaine complet défini par l'utilisateur, vous devez spécifier le nom de domaine et de zone pour configurer une application. Pour de plus amples informations, consultez la section configurer des applications en utilisant StyleBooks.

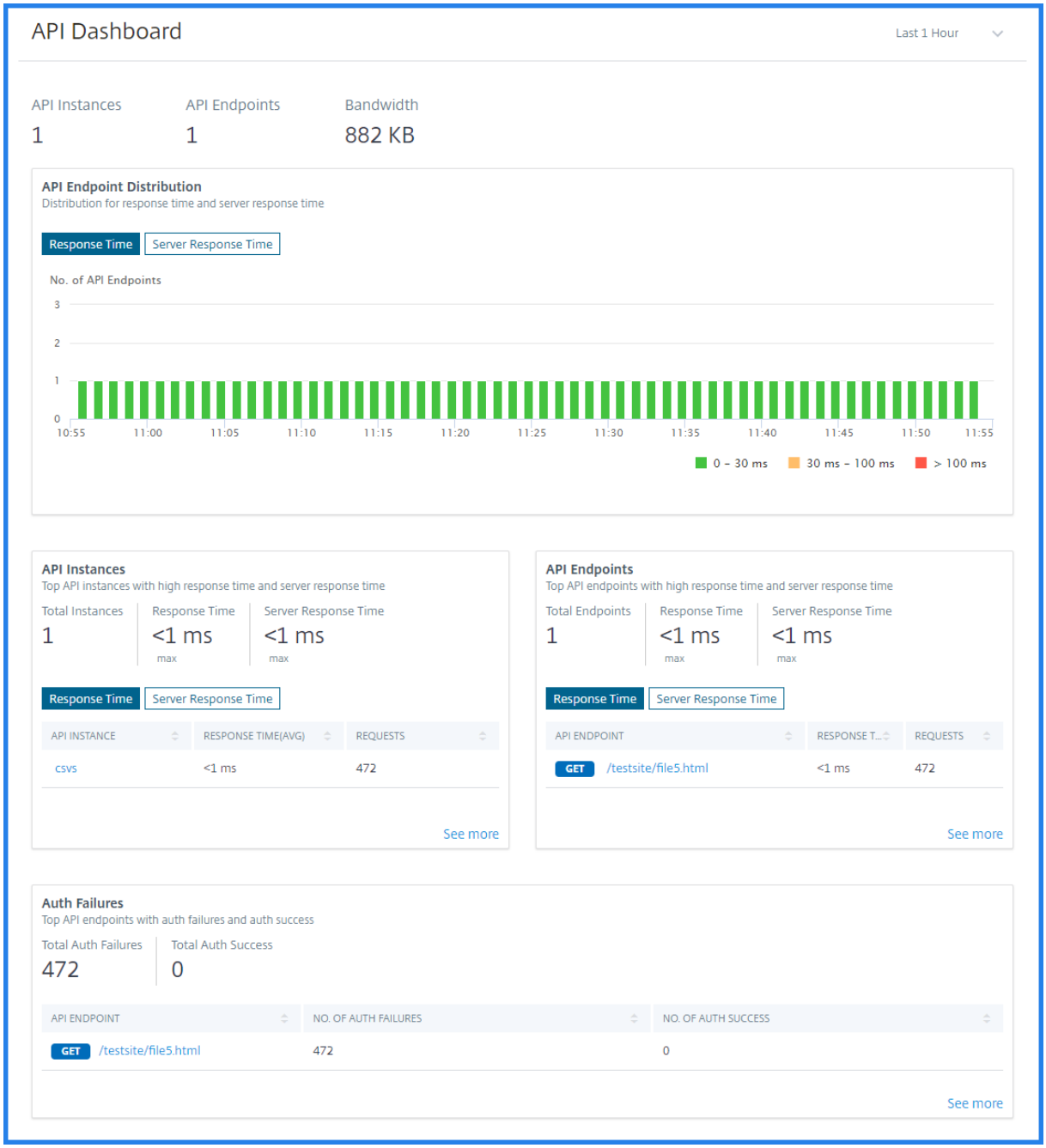
[NSADM-51494]

Surveiller les instances d'API et les points de terminaison dans ADM

En tant qu'administrateur, vous pouvez ajouter et déployer des définitions d'API sur une passerelle API dans Citrix Application Delivery Management (ADM). Avec cette fonctionnalité, vous pouvez ajouter des stratégies pour définir les critères de sélection du trafic afin d'authentifier les demandes d'API entrantes.

La page **API Analytics** affiche les mesures suivantes des instances et des points de terminaison API :

- Distribution du temps de réponse des applications et du serveur pour les points de terminaison API.
- Points de terminaison d'API qui ont un temps de réponse élevé pour les applications et le serveur.
- Les points de terminaison API qui ont plus de requêtes et de bande passante.
- Emplacements à partir desquels les points de terminaison reçoivent des demandes d'API.
- Tendance des demandes d'API totales et abandonnées vers un point de terminaison.
- État de la réponse HTTPS.
- Consommation de bande passante du point de terminaison API.
- Erreurs SSL et utilisation sur un point de terminaison API.



Pour de plus amples informations, consultez la section Gérer les définitions d'API.

[NSADM-47869]

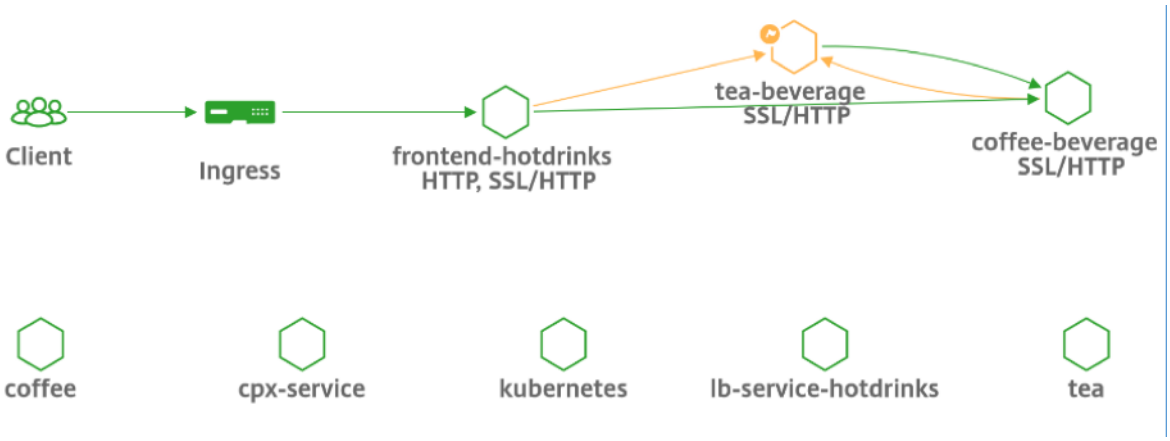
Graphique des améliorations apportées au service

Le graphique des services est mis à jour avec quelques changements thématiques. Vous pouvez également bénéficier de quelques mises à jour mineures de l'interface utilisateur :

- Lien FAQ — Pour afficher d'autres scénarios de dépannage pour le graphique de service qui af-

fichent un problème partiel et aucun problème de données.

- Modification de la mesure du temps de traitement ADC : cette mesure affiche 0, au lieu de < 1 ms. Cette modification s'applique uniquement aux instances ADC dont le statut est hors service ou en panne.
- Hexagone pour représenter une application de microservice — Le graphique de service affiche désormais une application de microservice dans le symbole hexagonal.



- Afficher les détails de l'instance ADC — Cliquez sur une instance ADC à partir du graphique de service pour les**applications (Applications > [nom de l'application] > Graphique de service**). Cette page affiche les détails de l'instance ADC tels que le score d'instance, les mesures clés et les problèmes.
- Graphique de service global pour afficher les applications de microservice : les applications de microservice apparaissent en fonction des seuils configurés.

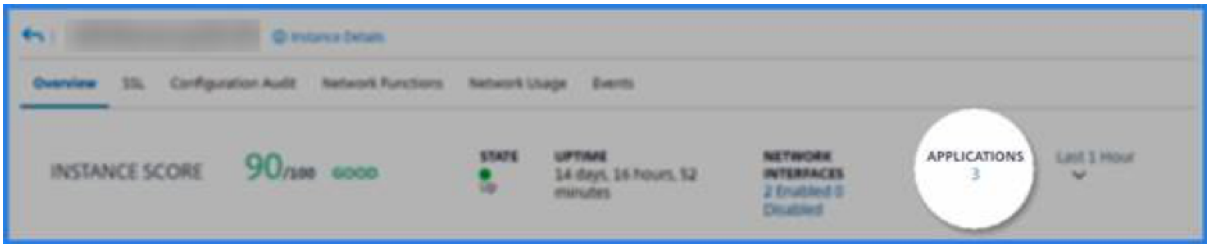
Selon le score, vous pouvez afficher les applications de microservice en rouge (critique), orange (examen) et vert (bon).

- Filtre d'espace de noms pour afficher les services correspondants — Le graphique de service affiche désormais les services correspondants ainsi que le client et l'entrée.

[NSADM-51973]

Afficher les applications à partir de la page Analyse de l'infrastructure

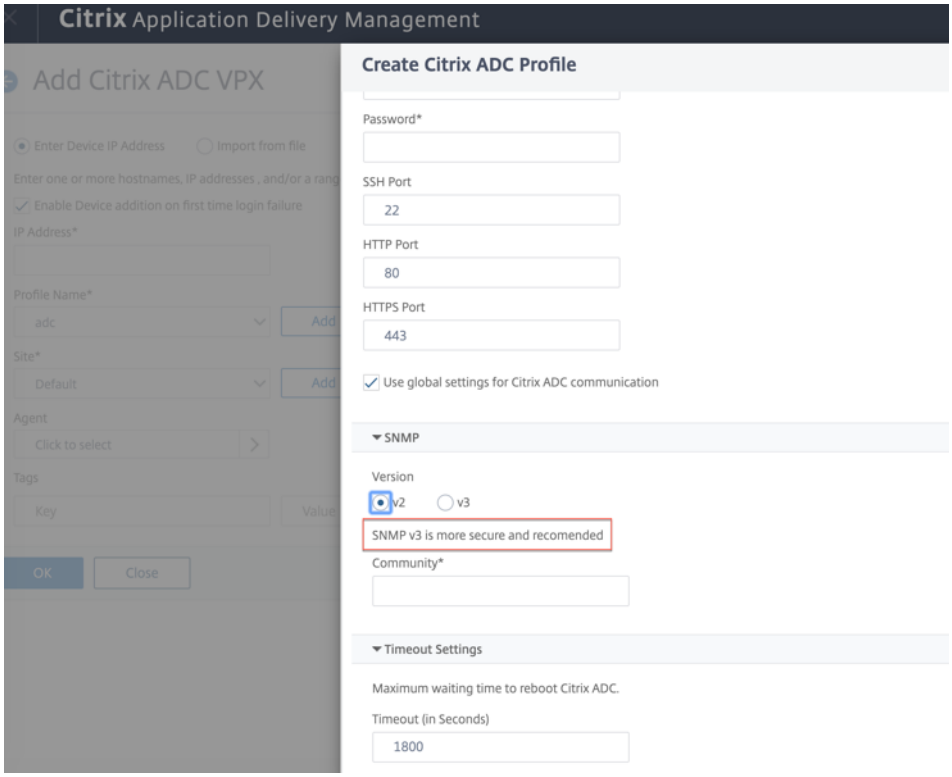
Lorsque vous sélectionnez une instance dans la page Analyse de l'infrastructure, vous pouvez afficher le nombre d'applications déployées sur l'instance. Cliquez sur le lien Applications pour afficher ces applications.



[NSADM-43848]

Un nouveau texte d'interface utilisateur pour SNMP V2

Lors de l'ajout d'une instance ADC dans l'interface graphique ADM, sous **SNMP**, si vous sélectionnez SNMP V2 maintenant, le message suivant s'affiche : « SNMP V3 est plus sécurisé et recommandé. « Par défaut, SNMP V3 est sélectionné.

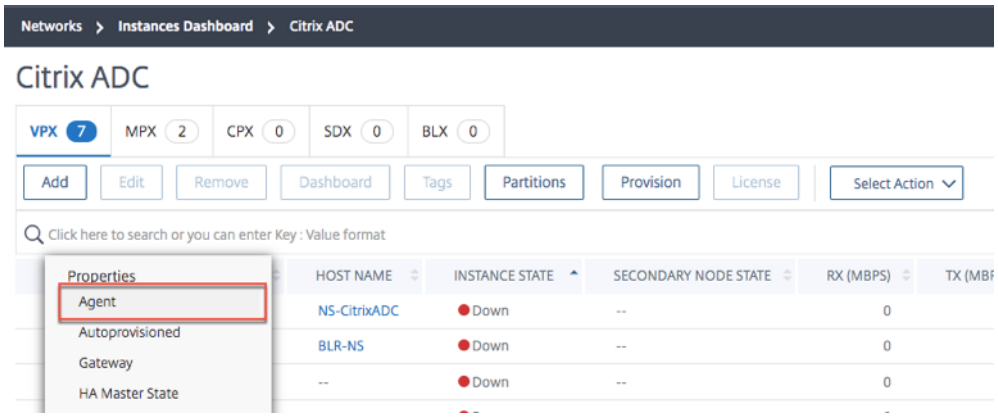


Pour de plus amples informations, consultez la section Ajout d'instances.

[NSADM-51179]

Agent en tant que nouvelle propriété de recherche

Sous **Réseaux > Instances > Citrix ADC**, vous pouvez désormais rechercher des instances par l'agent associé. Cliquez sur l'icône de recherche et sélectionnez **Propriétés > Agent**.

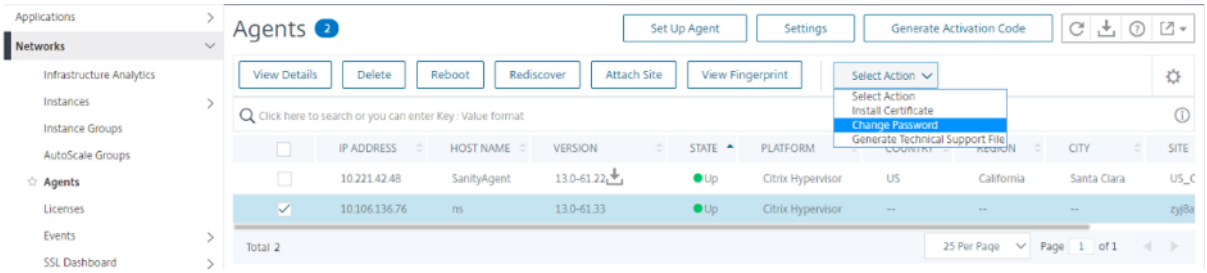


Pour de plus amples informations, consultez la section Comment rechercher des instances à l'aide de valeurs de balises et de propriétés.

[NSADM-47424]

Modifier le mot de passe de l'agent

Pour assurer la sécurité de votre infrastructure, vous pouvez désormais modifier le mot de passe par défaut d'un agent.
Pour modifier le mot de passe, dans l'interface graphique, accédez à **Réseaux > Agents**, puis cliquez sur **Sélectionner une action** et sélectionnez **Modifier le mot de passe**.

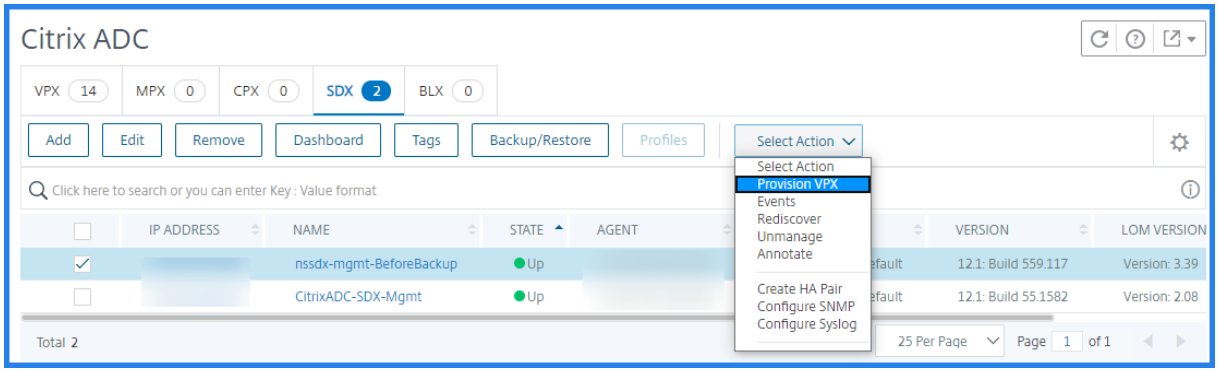


Pour de plus amples informations, consultez la section Mise en route.

[NSADM-47521]

Utiliser ADM pour provisionner des instances ADC sur SDX

Vous pouvez désormais provisionner une ou plusieurs instances Citrix ADC sur l'appliance SDX, à l'aide d'ADM. Le service ADM déploie implicitement l'instance Citrix ADC sur l'appliance SDX, puis télécharge les détails de configuration de l'instance.



Pour de plus amples informations, consultez la section Provisionner des instances VPX ADC sur SDX à l'aide d'ADM.

[NSADM-23845]

Problèmes résolus

Analytics

Dans Gateway Insight, le rapport d'exportation pour le format CSV ne fonctionne pas comme prévu.

[NSHELP-22780]

GUI

Le menu Enregistrer les favoris affiche parfois une erreur javascript.

[NSADM-52856]

Système de licences

Les exceptions de délai d'attente non gérées et les conditions de blocage entraînent la fonctionnalité de licence groupée ne fonctionne pas comme prévu.

[NSHELP-22729]

15 mai 2020

Afficher les détails de diagnostic pour des données partielles ou incomplètes dans le graphique de service

Après avoir terminé la configuration de graphique de service requise et ajouté le cluster Kubernetes dans Citrix ADM, le graphique de service commence à remplir les données. Dans certains scénarios, vous pouvez observer que le graphique de service affiche des données partielles ou aucune donnée. Voici quelques-unes des raisons possibles pour les données partielles ou l'absence de données dans le graphique de service :

- L'itinéraire statique n'est pas configuré
- L'état du cluster Kubernetes est en panne
- Échec de l'enregistrement CPX
- Les serveurs virtuels CPX ne sont pas sous licence
- La configuration d'analyse requise n'est pas définie qui empêche le graphique de service de charger toutes les données

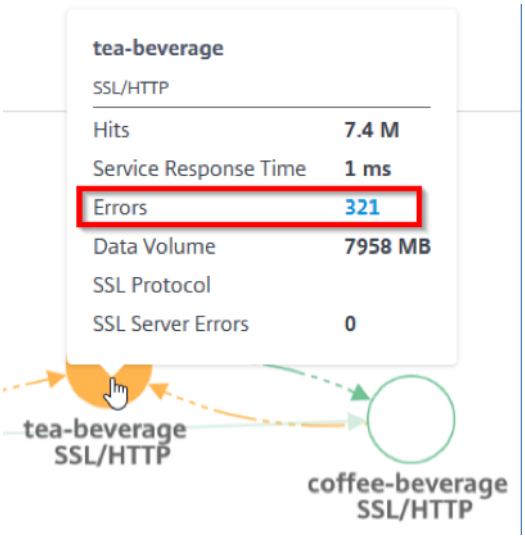
En tant qu'administrateur, vous pouvez avoir du mal à analyser les raisons lorsque vous voyez la fonction de graphique de service affichant des données partielles ou aucune donnée.

La page du graphique de service vous permet désormais d'afficher les raisons possibles et les actions requises pour résoudre les problèmes de données partielles ou aucun problème de données.
Pour plus d'informations, reportez-vous à la section Afficher les détails du diagnostic.

[NSADM-47865]

Un processus simplifié pour afficher les erreurs dans le graphique de service

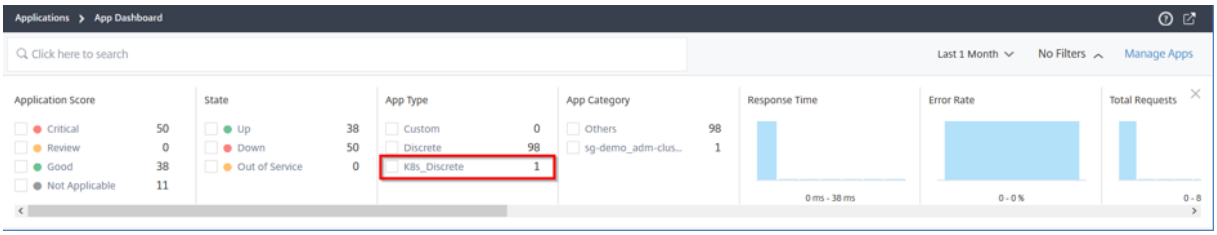
Dans le graphique de service, le processus d'affichage des erreurs HTTP et SSL est simplifié. Vous pouvez maintenant afficher le total des erreurs en plaçant le pointeur de la souris sur un service erroné et en cliquant sur le nombre d'erreurs.



[NSADM-47864]

Afficher les applications de microservice dans le tableau de bord des applications

Dans **App Dashboard**, vous pouvez afficher les détails des applications de microservice configurées à partir de l'instance Citrix ADC CPX dans le cluster Kubernetes. Le filtre **Type d'application** dispose d'une nouvelle option **K8S_discrete** qui vous permet d'appliquer le filtre et d'afficher les détails de l'application de microservice.



Pour de plus amples informations, consultez la section Afficher les détails de l'application de microservice.

[NSADM-47863]

Apprentissage WAF dans Citrix ADM

Citrix Web App Firewall (WAF) protège vos applications Web contre les attaques malveillantes telles que l'injection SQL et les scripts inter-sites. Pour prévenir les violations de données et assurer la protection de sécurité adéquate, vous devez surveiller votre trafic à la recherche de menaces et de données exploitables en temps réel sur les attaques. Parfois, les attaques signalées peuvent être faussement positives et ces attaques doivent être fournies à titre d'exception.
Le moteur d'apprentissage de Citrix ADM est un filtre répétitif qui permet à WAF d'apprendre le comportement (les activités normales) de vos applications Web. Sur la base de la surveillance, le moteur

génère une liste de règles ou d'exceptions suggérées pour chaque vérification de sécurité appliquée au trafic HTTP. En tant qu'administrateur, vous pouvez ensuite afficher la liste des violations dans Citrix ADM et décider de déployer ou d'ignorer.
Pour plus d'informations, reportez-vous à la section Apprentissage WAF dans Citrix ADM.

[NSADM-44341]

Violations de sécurité des applications - IPs uniques excessives par géo

Outre les violations existantes de sécurité des applications, vous pouvez désormais afficher les **adresses IP uniques excessives par géo** dans la catégorie Bot. L'indicateur **IPs uniques par géo excessif** vous permet d'analyser et de bloquer les mauvais robots en effectuant plus de visites à une application Web à partir d'un emplacement particulier.
Pour plus d'informations, reportez-vous à la section IPs uniques excessives par géo.

[NSADM-43982]

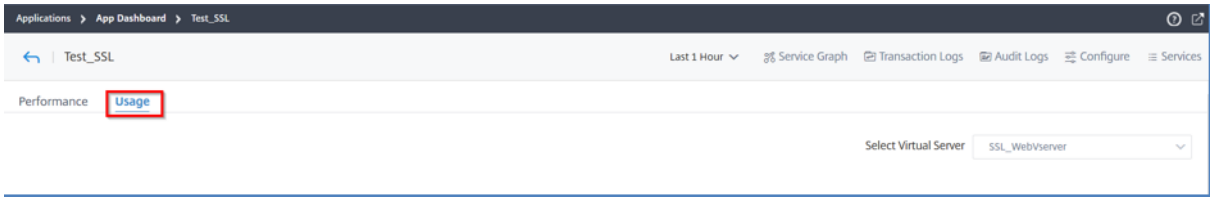
Analyse de l'utilisation des applications

Les propriétaires d'applications doivent avoir la capacité d'évaluer et de visualiser l'application complète du point de vue de la performance et de l'utilisation.

Le tableau de bord des applications improvisé vous permet de visualiser toutes les performances de l'application et les mesures d'utilisation ensemble. Lorsque vous cliquez sur une application, parallèlement aux mesures de performances de l'application existantes, l'onglet **Utilisation** affiche les détails des mesures qui vous aident à :

- Comprenez l'utilisation de votre application.
- Corréler les écarts de performances avec les mesures d'utilisation.

Si l'application dispose de deux serveurs virtuels ou plus, sélectionnez le serveur virtuel dans la liste.



À l'aide du Tableau de bord des applications, en tant qu'administrateur, vous pouvez visualiser une vue à volet unique pour les mesures suivantes :

- Clients
- Serveurs
- Emplacements géographiques
- URL

- État de la réponse HTTP
- Système d'exploitation
- Navigateurs
- Erreurs SSL
- Utilisation de SSL

Pour de plus amples informations, consultez la section Analyse de l'utilisation des applications.

Graphique de service global : une visualisation holistique des utilisateurs, de l'infrastructure et des applications

> **Remarque**
>
> Cette fonctionnalité est en prévisualisation.

La fonction de graphique de service global vous permet d'obtenir une visualisation holistique de la `clients to infrastructure to application` vue. À partir de cette vue graphique de service à volet unique, en tant qu'administrateur, vous pouvez :

- Comprendre la région à partir de laquelle les utilisateurs accèdent aux applications spécifiques (applications Web à 3 niveaux et applications microservices)
- Visualiser la vue de l'infrastructure (instance Citrix ADC) que la demande du client est traitée
- Comprendre si les problèmes surviennent à partir du client, de l'infrastructure ou de l'application
- Exercer davantage vers le bas pour résoudre le problème

Accédez à **Applications > Graphiques de service > Graphique de service global** pour afficher :

- Détails de bout en bout de toutes les applications connectées du client aux serveurs back-end.
- Toutes les instances Citrix ADC connectées à ses centres de données respectifs. **Remarque** : Vous pouvez afficher les centres de données uniquement si vous disposez d'applications GSLB.
- Les informations sur les mesures du client.
- Informations sur les mesures Citrix ADC.
- Toutes les instances Citrix ADC qui ont des applications discrètes, des applications personnalisées et des applications de microservice discrètes.
- Les quatre applications les plus faibles qui appartiennent à des applications personnalisées, des applications discrètes et des applications de microservices.
- Informations sur les mesures pour les quatre serveurs virtuels les plus bas.
- Les applications (applications discrètes, applications personnalisées et applications de microservices) sont des statuts tels que **Critique**, **Review**, **Bon**et **Non applicable**.

Pour de plus amples informations, consultez la section Vue holistique de toutes les applications dans le graphique de service.

[NSADM-47425]

Personnaliser le filtre StyleBooks pour fournir l'autorisation de l'utilisateur

En tant qu'administrateur, vous pouvez autoriser des StyleBooks spécifiques à un utilisateur dans la page **Compte > Administration de l'utilisateur > Groupes**. Vous pouvez désormais utiliser une requête Filtre personnalisée pour rechercher StyleBooks. Une requête est une chaîne de paires clé-valeur où les clés sont les suivantes :

- Nom
- Espace de noms
- Version

Par exemple :

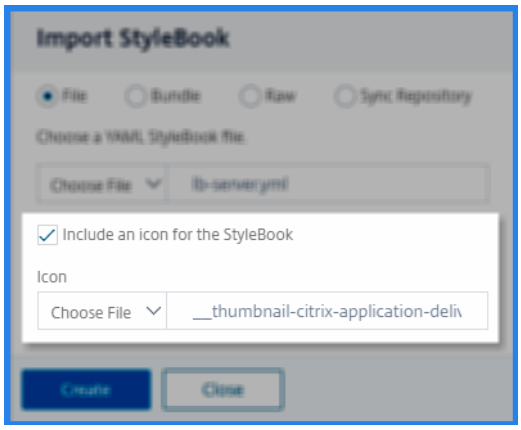
```
name=lb-mon OR namespace=com.citrix.adc.stylebooks OR version=1.0
```

Le résultat de la recherche répertorie les StyleBooks en fonction de la paire clé-valeur spécifiée. En fonction de la requête spécifiée, l'ADM fournit l'accès de l'utilisateur à ces stylebooks.Pour plus d'informations, reportez-vous à la section Configurer des groupes sur Citrix ADM.

[NSADM-49446]

Importer des StyleBooks avec une icône

Lorsque vous importez un StyleBook, vous pouvez désormais y inclure une icône. Dans **Applications > StyleBook**, le StyleBook importé apparaît avec une icône.



Pour de plus amples informations, consultez Importer des StyleBooks personnalisés

[NSADM-45810]

Utiliser les nouvelles fonctions intégrées dans StyleBooks

Lors de la création de définitions StyleBook, ADM StyleBooks prend désormais en charge les fonctions intégrées suivantes :

- `startswith()` — Détermine si une chaîne commence par un préfixe donné. En savoir plus.

- `contains()` — Détermine si une chaîne contient une sous-chaîne donnée. En savoir plus.
- `endswith()` — Détermine si une chaîne se termine par un suffixe donné. En savoir plus.] (/en-us/citrix-application-delivery-management-service/stylebooks/stylebooks-grammar/built-in-functions.html #endswith)
- `substring()` — Extrait une sous-chaîne d'une chaîne. En savoir plus.] (/en-us/citrix-application-delivery-management-service/stylebooks/stylebooks-grammar/built-in-functions.html #substring)

[NSADM-45889]

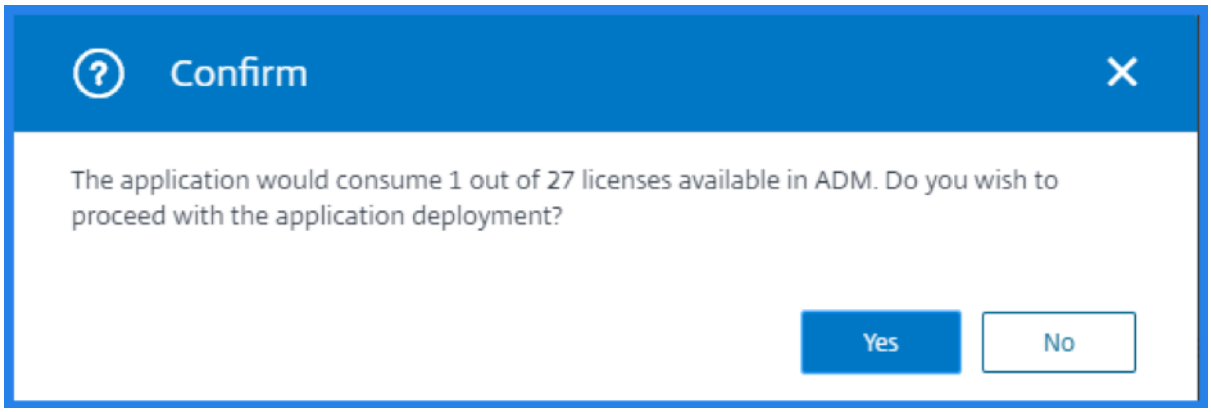
Le générateur de configuration StyleBook prend en charge la fonctionnalité WAF ADC

Le générateur de configuration StyleBook reconnaît et prend désormais en charge la fonctionnalité WAF dans une configuration source ADC. Pour plus d'informations sur les fonctionnalités ADC prises en charge, reportez-vous à la section Migrer la configuration de l'application Citrix ADC à l'aide de StyleBooks Configuration Builder.

[NSADM-48941]

Confirmer la consommation de licence avant le déploiement de

Lorsque vous créez une application à l'aide de StyleBooks, vous pouvez confirmer la consommation de licence requise avant de déployer l'application. Le message suivant s'affiche une fois que vous avez terminé les étapes de création d'une application :



Cliquez sur **Oui** pour le message de confirmation. ADM attribue les licences requises à une application. Auparavant, vous deviez activer l'option Serveurs virtuels sous licence automatique pour créer une application à l'aide de StyleBooks. Désormais, vous pouvez toujours créer une application même si l'option Serveurs virtuels sous licence automatique est désactivée.

Pour de plus amples informations, consultez la section Créer une application à l'aide de StyleBook.

[NSADM-51306, NSADM-47184]

Problèmes résolus

Réseaux

Lorsque vous exportez un rapport CSV pour tous les rapports de performances, y compris le rapport des serveurs virtuels d'équilibrage de charge, le rapport exporté apparaît vide.

[NSHELP-22465]

Sous Réseaux > Audit de configuration > Rapports d'audit, pour une instance ADC sélectionnée, les actions suivantes ne fonctionnent pas :

- Historique des versions diff
- Pré c. Diff post-mise à niveau
- Téléchargement de la configuration

[NSADM-51310]

Les scripts de mise à niveau ne parviennent pas à télécharger et le message d'erreur « Fichier introuvable » s'affiche. Ce problème se produit lorsque vous téléchargez les scripts après une tâche de mise à niveau de maintenance est terminée avec succès.

[NSADM-48809]

Analytics

Les indicateurs de transaction de téléchargement et de téléchargement exceptionnellement volumineux dans l'interface graphique Citrix ADM n'affichent pas les données d'analyse comme prévu.

NSADM-50930]

28 avril 2020

Afficher les détails des violations de sécurité des applications

Outre les violations réseau existantes, vous pouvez désormais afficher les violations pour les catégories de robots et WAF. Voici les violations que vous pouvez visualiser dans Citrix ADM :

BOT	WAF
Connexions client excessives	Transactions de chargement exceptionnellement élevées
Prise en charge de compte	Transactions de téléchargement exceptionnellement élevées
Volume de téléchargement exceptionnellement élevé	IPs uniques excessifs

BOT	WAF
Taux de demandes exceptionnellement élevé	
Volume de téléchargement exceptionnellement élevé	

Pour de plus amples informations, consultez la section Afficher les détails des violations de sécurité des applications.

[NSADM-40227], [NSADM-43969], [NSADM-43974], [NSADM-43977], [NSADM-43980], [NSADM-43984]

Afficher les rapports des mises à jour des signatures de bot

Dans Bot insights, vous pouvez désormais afficher les mises à jour des signatures de bot dans l'**historique des événements**, lorsque :

- De nouvelles signatures de bot sont ajoutées dans les instances de Citrix ADC.
- Les signatures de bot existantes sont mises à jour dans les instances de Citrix ADC.

Accédez à **Analytics > Sécurité > Bot Insight** et affichez le résumé des mises à jour de signature sous **Historique des événements**.

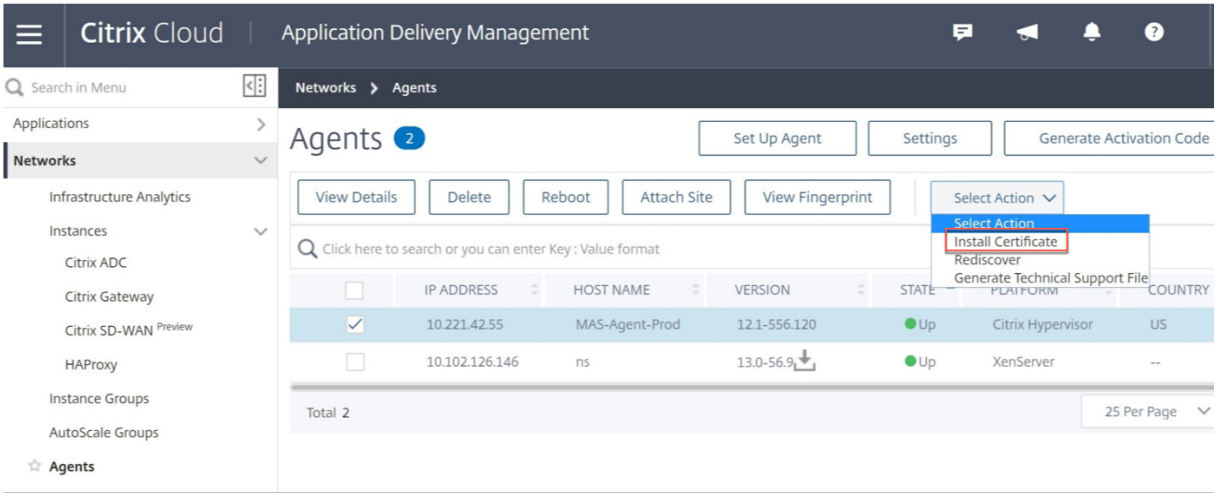
Pour de plus amples informations, consultez la section Perspectives de.

[NSADM-40228]

Installer un certificat d'agent

Pour répondre à vos exigences de sécurité, vous pouvez désormais télécharger un certificat vers l'agent ADM à l'aide de l'interface graphique ADM. Pour installer le certificat, à partir de l'interface graphique, accédez à **Réseaux > Agents**, puis cliquez sur **Sélectionner une action** et sélectionnez **Installer le certificat**.

Pour de plus amples informations, consultez la section Mise en route.



[NSADM-47904]

Spécifier des chaînes de type textuel dans un nouveau format

Les chaînes textuelles peuvent prendre des entrées complexes telles que PI Expressions dans leur format d'origine sans caractère d'échappement (par exemple, \\).

Pour inclure des expressions PI dans une définition StyleBook et conserver son format dans la sortie, vous pouvez désormais les spécifier à l'aide de la syntaxe suivante :

- La nouvelle syntaxe :

```
~{
<pi-expression> }
~

Example:

~{
"HTTP.REQ.COOKIE.VALUE("jsessionid") ALT HTTP.REQ.URL.BEFORE_STR(
    "=").AFTER_STR(";jsessionid=") ALT HTTP.REQ.URL.AFTER_STR(";
    jsessionid=")" }
~
<!--NeedCopy-->
```

- L'ancienne syntaxe :

```
 " <pi-expression>\" "

Example:

```



```
""HTTP.REQ.COOKIE.VALUE(\\"jsessionid\\") ALT HTTP.REQ.URL.
    BEFORE_STR(\\"=\\").AFTER_STR(\\";jsessionid=\\") ALT HTTP.REQ
    .URL.AFTER_STR(\\";jsessionid=\\")""

<!--NeedCopy-->
```

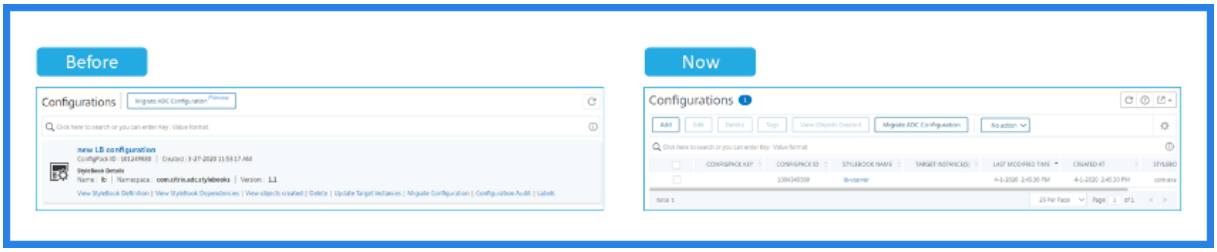
Les expressions PI spécifiées ne modifient pas leur format dans la sortie.

[NSADM-45888]

Configurations StyleBooks - vue liste

L'interface graphique ADM affiche les configurations StyleBooks dans la vue liste. Auparavant, il était affiché dans une vue tuile.

Avec cette modification, vous pouvez trier les configurations StyleBook par en-tête de colonne. Par exemple, vous pouvez trier les configurations selon LAST MODIFIED TIME.

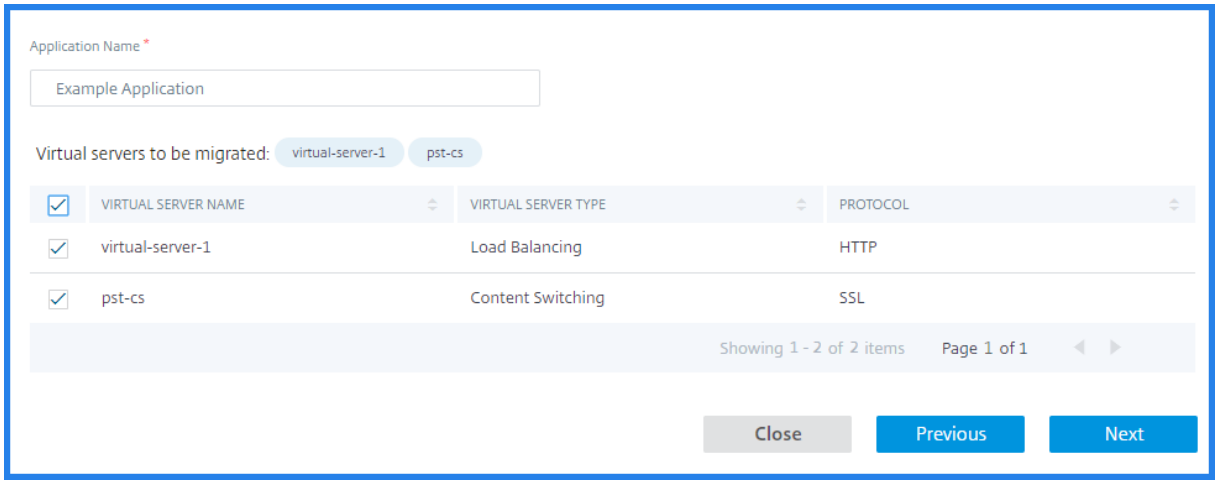


[NSADM-48918]

Migrer plusieurs serveurs virtuels à l'aide du générateur de configuration

Dans le générateur de configuration StyleBooks, vous pouvez désormais sélectionner un ou plusieurs serveurs virtuels que vous souhaitez migrer de la source de configuration vers l'instance cible. Auparavant, vous étiez en mesure de sélectionner un seul serveur virtuel à migrer en même temps.

Avec cette fonctionnalité, vous pouvez sélectionner et migrer les serveurs virtuels nécessaires qui crée une application vers l'instance cible.



[NSADM-49602]

Problèmes résolus

Analytics

- Dans **Security Insight**, lorsque vous utilisez le curseur temporel, le **résumé de l'application** s'affiche vide.

[NSADM-50809]

Applications

- Lorsque vous sélectionnez une **application dans le tableau de bord**Application, la valeur de la mesure **Temps de réponse** sous **Mesures clés** s'affiche dans un format incorrect.

  [NSADM-50274]

- La page **Gérer les applications** s'affiche vide lorsque :
  - Vous supprimez une application personnalisée. Seulement après avoir cliqué sur le bouton Actualiser affiche les autres applications
  - Vous modifiez le nombre de lignes à afficher
  - Vous cliquez sur la page suivante si plusieurs pages sont disponibles

  [NSADM-50224]

- Dans Service Graph for Applications, les détails de transaction de bout en bout du client à service ne sont pas renseignés dans le cas où la transaction se produit via des serveurs avec IPv.6

  [NSADM-50201]

Réseaux

- Dans **la tâche de configuration**, lorsque vous sélectionnez **Instance** dans la liste **Source de configuration** et que vous sélectionnez **Exécuter la configuration** ou l'option **Configuration enregistrée**, un message d'erreur `Please provide Citrix ADC IP Address` s'affiche.

  [NSADM-50810]

- Un problème d'indentation entraîne l'échec de l'enregistrement de l'agent

  [NSADM-50596]

- Dans **Configuration Audit**, lorsque vous exportez le rapport au format CSV, aucune donnée n'est affichée. L'interface graphique Citrix ADM se bloque également parfois, lorsque vous effectuez plusieurs exportations.

  [NSADM-48322]

StyleBooks

- Un message d'erreur incorrect est rendu lors de la compilation d'une dépendance StyleBook.

  [NSADM-50466]

Infra

- Informations de journal pour toute activité `mpsgroup` à afficher dans Citrix ADM.

  [NSHELP-22370]

14 avril 2020

Prise en charge de l'IPAM dans ADM

ADM prend en charge la gestion des adresses IP (IPAM) pour attribuer et libérer automatiquement des adresses IP dans les configurations gérées par ADM. Vous pouvez attribuer des adresses IP à partir de réseaux ou de plages d'adresses IP définies à l'aide des fournisseurs IP suivants :

- Fournisseur IPAM intégré ADM.
- Solution IPAM Infoblox. Pour de plus amples informations, consultez la section Infoblox DDI.

Actuellement, vous pouvez utiliser ADM IPAM dans :

- **StyleBooks** : allouer automatiquement des adresses IP aux serveurs virtuels lorsque vous créez des configurations.
- **Ingress de Kubernetes** : Affectez automatiquement une adresse IP virtuelle à une configuration d'entrée dans un cluster Kubernetes.

Vous pouvez également suivre les adresses IP allouées et disponibles dans chaque réseau ou plage d'adresses IP gérée par ADM. Pour de plus amples informations, consultez la section Configurer IPAM.

[NSADM-48377]

Déployer des applications internes dans un groupe Autoscale

Vous pouvez désormais déployer des applications internes et externes dans un groupe de mise à Autoscale pour utiliser la solution de mise à l'échelle automatique ADM. Auparavant, vous étiez en mesure de déployer uniquement des applications externes.
Pour déployer une application interne dans le groupe Mise à l'échelle automatique, reportez-vous à Configuration Autoscale dans AWS la section et Configuration Autoscale dans Azure.

[NSADM-47520]

Nouvelles colonnes ajoutées dans le tableau de bord SSL

De nouvelles colonnes sont ajoutées aux onglets suivants dans le tableau de **bord SSL** :

- Certificats SSL — La colonne Effectif clé est ajoutée. Vous pouvez filtrer les certificats SSL à l'aide de la valeur de la clé.
- Protocoles SSL — La colonne Type de protocole est ajoutée. Vous pouvez filtrer les protocoles SSL à l'aide du type de protocole.

[NSADM-42191]

Afficher les détails des violations de sécurité des applications

Les applications Web exposées à Internet sont devenues extrêmement vulnérables aux attaques. Citrix ADM vous permet de visualiser les détails des violations exploitables pour protéger les applications contre les attaques. Accédez à **Sécurité** > **Violations de sécurité** pour une solution à volet unique pour :

- Accédez aux violations de sécurité des applications suivantes :
  - HTTP lent Loris
  - DNS Lent Loris
  - Publication lente HTTP
  - `NXDomain` Attaque d'inondation
- Prendre des mesures correctives pour sécuriser les applications

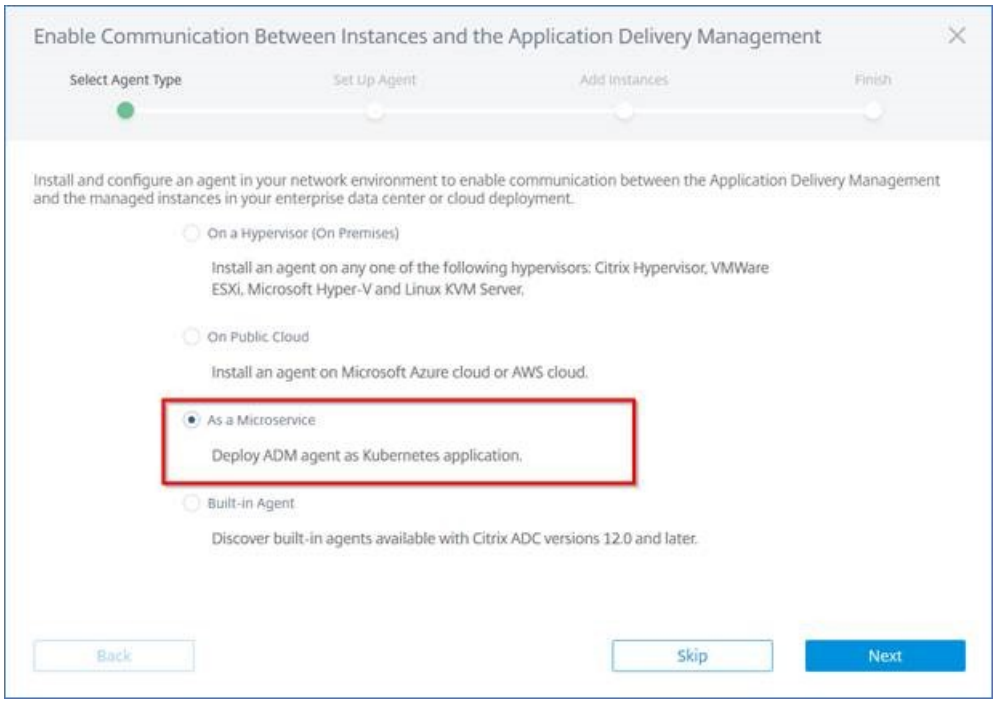
Pour de plus amples informations, consultez la section Afficher les détails des violations de sécurité des applications.

[NSADM-48069]

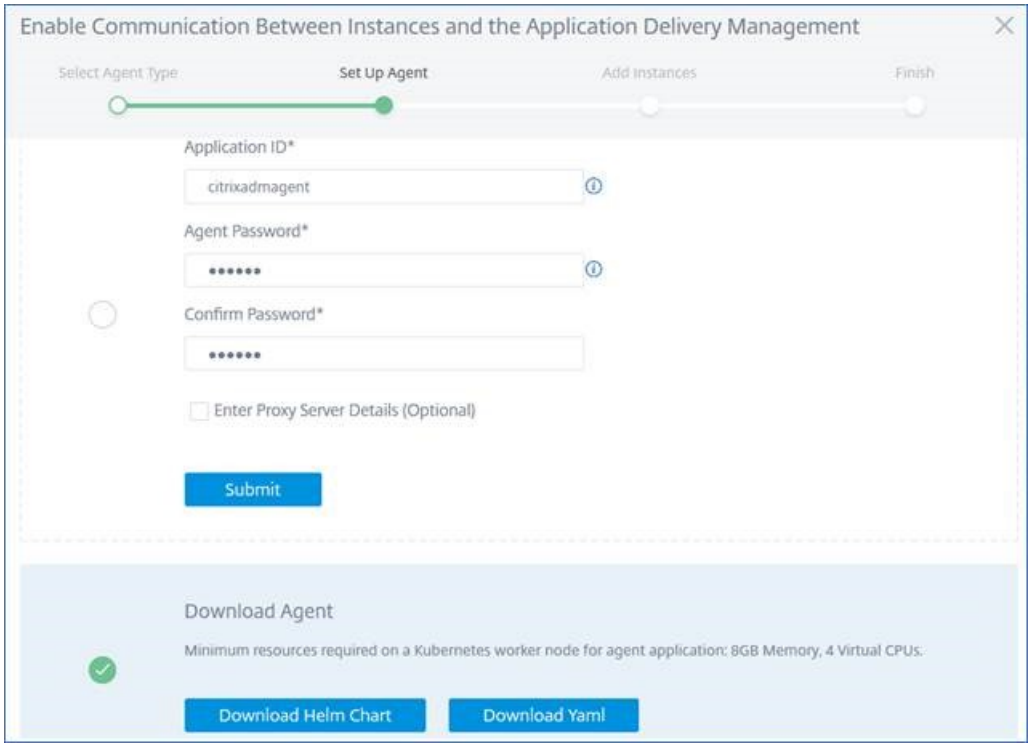
Déployer l'agent Citrix ADM en tant que microservice

Vous pouvez désormais déployer un agent Citrix ADM en tant que microservice dans le cluster Kubernetes. Dans Citrix ADM,

1. Accédez à **Réseaux** > **Agents**, puis cliquez sur **Configurer l'agent**
2. Cliquez sur **Démarrer**, sélectionnez l'option **En tant que microservice**, puis cliquez sur **Suivant**



3. Spécifiez les paramètres suivants :
   a) **ID d'application** — ID de chaîne permettant de définir le service de l'agent dans le cluster Kubernetes et de distinguer cet agent des autres agents du même cluster
   b) **Mot de passe de l'agent** — Spécifiez un mot de passe pour que CPX utilise ce mot de passe pour embarquer le service CPX to ADM via l'agent
   c) **Confirmer le mot de passe** — Spécifiez le même mot de passe pour
   d) Cliquez sur **Soumettre**
4. Après avoir cliqué sur **Soumettre**, vous pouvez télécharger le tableau YAML ou Helm Chart



5. Dans le maître Kubernetes, enregistrez le fichier YAML et utilisez la commande `kubectl create -f <yaml file>`

   Pour de plus amples informations, consultez Mise en route

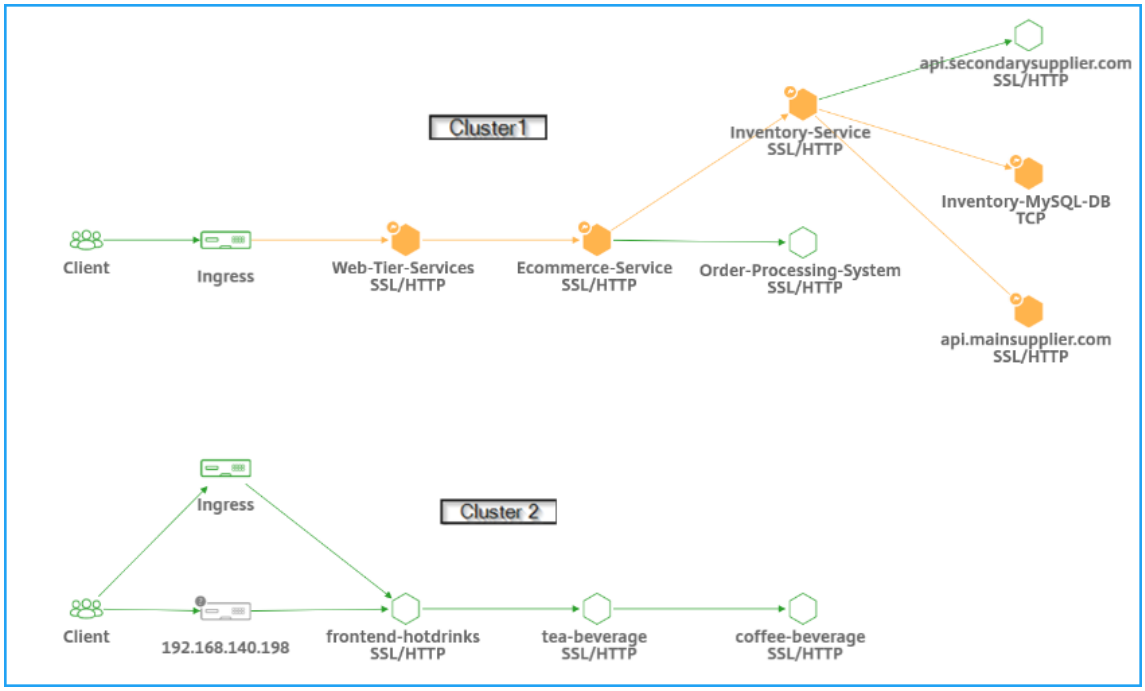
[NSADM-43971]

31 mars 2020

Afficher plusieurs clusters et plus de filtres dans le graphique de service

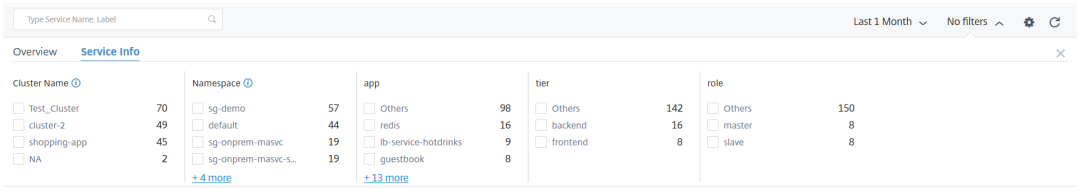
Dans le graphique de service, vous pouvez maintenant afficher :

- Services associés à chaque cluster.



- Plus de filtres pour :
  - **Cluster** : affiche tous les services applicables au ou aux clusters sélectionnés.
  - **Espace de noms** : affiche tous les services applicables à l'espace de noms sélectionné.

    > **Remarque**
    >
    > Selon les étiquettes configurées pour le service dans la définition de service YAML de Kubernetes, vous pouvez également afficher d'autres options de filtre.



[NSADM-43985]

Suivi distribué

Dans le graphique de service, vous pouvez désormais utiliser les informations de trace pour :

- Analyser les performances globales du service
- Visualiser le flux de communication entre le service sélectionné et ses services interdépendants
- Identifier le service qui indique des erreurs et dépanner le service erroné

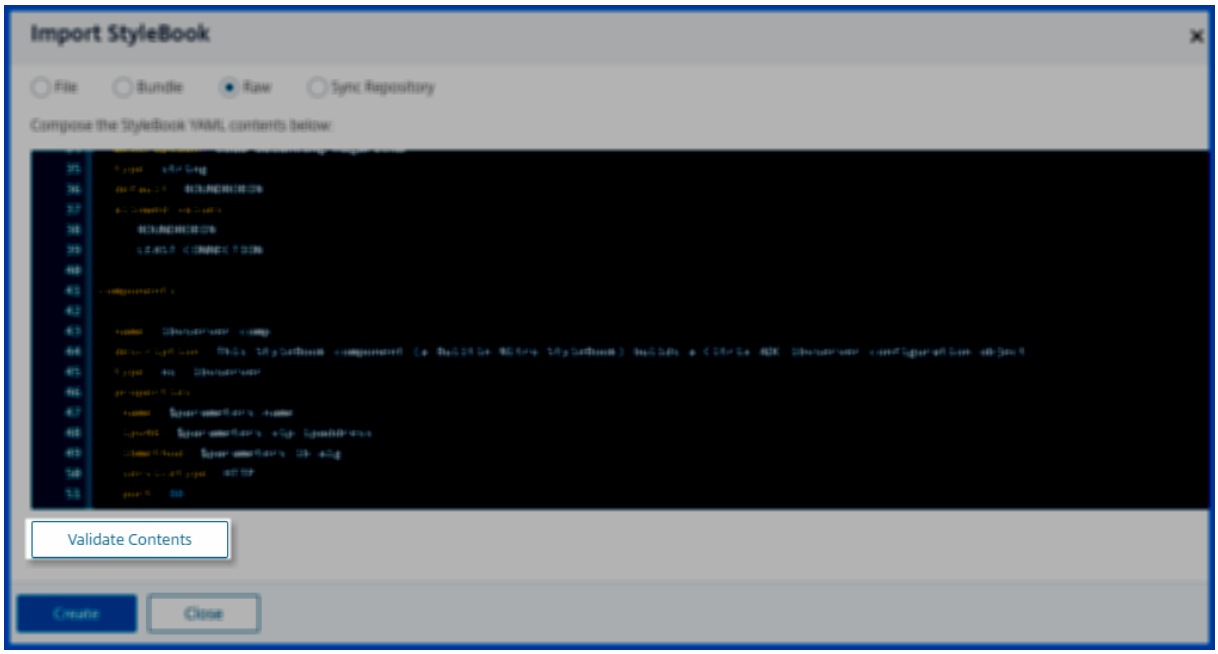
- Affichez les détails des transactions entre le service sélectionné et son service interdépendant. Pour de plus amples informations, consultez Suivi distribué

[NSADM-43976]

Valider le contenu du livre StyleBook avant d'importer dans ADM

Lorsque vous composez un StyleBook dans l'éditeur ADM YAML, vous pouvez maintenant vérifier les erreurs de grammaire StyleBook sans les importer dans ADM.

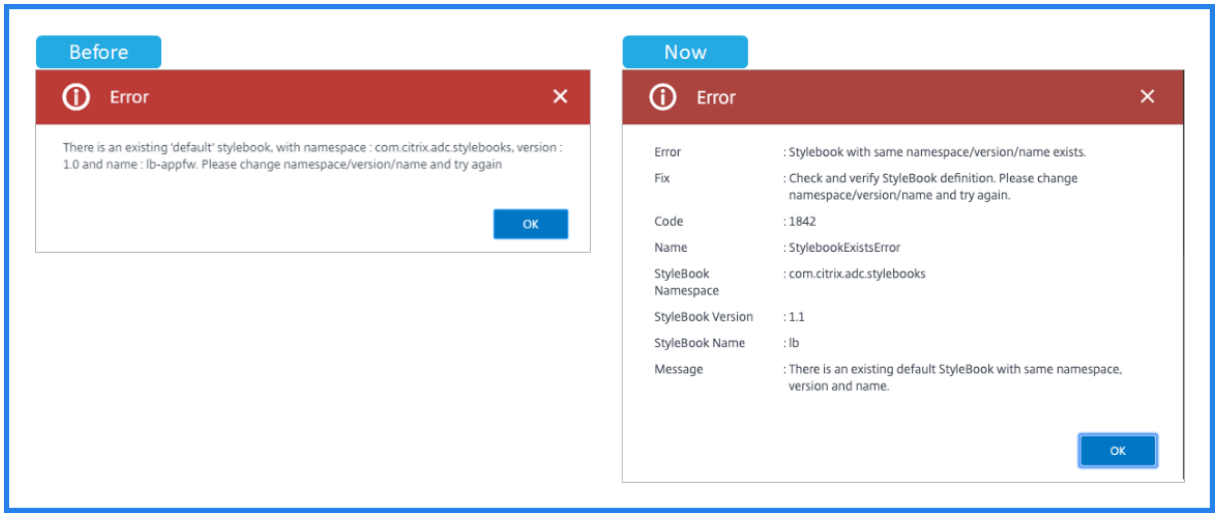
S'il y a des erreurs dans le contenu StyleBook, l'interface graphique ADM affiche les détails de l'erreur. Vous pouvez corriger les erreurs indiquées et continuer à modifier ou importer le StyleBook.



[NSADM-47978]

Affichage des messages d'erreur StyleBooks amélioré

L'interface graphique ADM affiche un message d'erreur si vous importez un StyleBook contenant des erreurs de grammaire StyleBook. Certains messages d'erreur sont désormais organisés pour afficher les détails de l'erreur. Les détails de l'erreur incluent Erreur, Correctif, Code, Nom et plus encore selon les types d'erreur. Le champ **Corriger** fournit des informations pour résoudre un problème.



[NSADM-44274]

Importer des StyleBooks à partir de n'importe quel dossier dans un référentiel GitHub

Vous pouvez désormais synchroniser les fichiers StyleBook avec ADM à partir de n'importe quel dossier d'un référentiel GitHub. Auparavant, vous étiez en mesure d'importer ou de synchroniser uniquement les fichiers StyleBook présents dans le dossier **racine du référentiel GitHub**.

Pour de plus amples informations, consultez la section Importer et synchroniser les StyleBooks à partir du référentiel GitHub.

[NSADM-46147]

Audit de la configuration ADC par rapport au pack de configuration

Dans **StyleBooks** > **Configurations**, vous pouvez désormais comparer explicitement les modifications apportées par un pack de configuration StyleBook à la configuration ADC actuelle. Avec cette fonctionnalité, vous pouvez effectuer les opérations suivantes :

- Détectez la dérive de configuration entre le pack de configuration StyleBook et la configuration ADC.
- Identifiez tous les objets modifiés et supprimés de ADC qui ne reflètent pas les modifications apportées par le pack de configuration.

Pour comparer les modifications du pack de configuration à la configuration des CAN, cliquez sur **Audit de configuration** dans le pack de configuration souhaité.

Pour de plus amples informations, consultez la section Audit de la configuration ADC par rapport au pack de configuration.

[NSADM-45866]

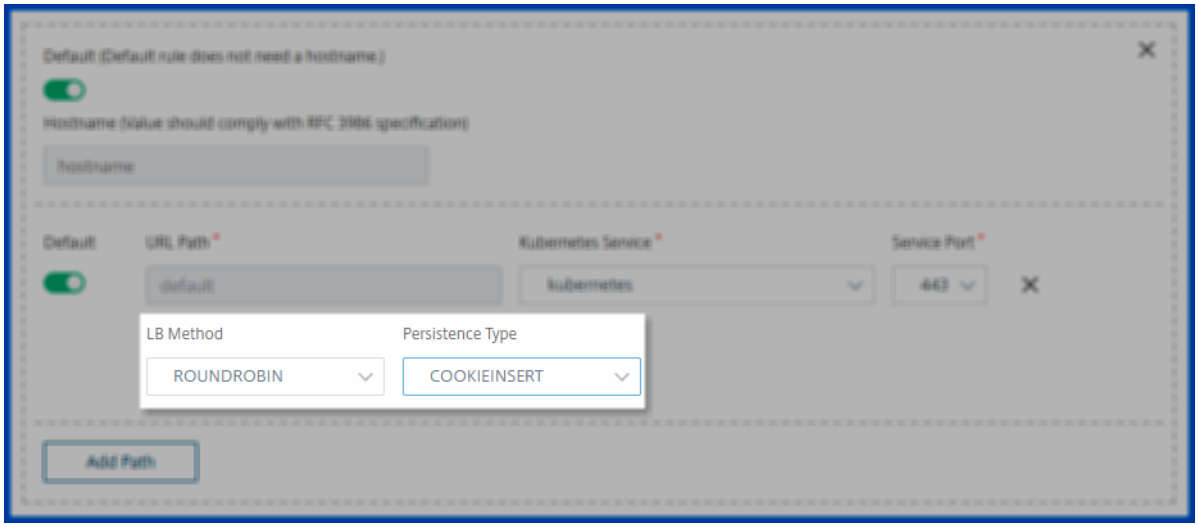
Prise en charge des annotations Citrix pour déployer une configuration d'entrée

Lorsque vous ajoutez des règles de routage de contenu à une configuration d'entrée, vous pouvez désormais inclure les annotations Citrix suivantes dans l'interface graphique ADM :

- **Méthode LB** : sélectionnez la méthode d'équilibrage de charge préférée pour le service Kubernetes sélectionné.
- **Type de persistance** : sélectionnez le type de persistance d'équilibrage de charge préféré pour le service Kubernetes sélectionné.

Après avoir ajouté les règles de routage de contenu, vous pouvez afficher la méthode LB et le type de persistance sélectionnés dans la spécification d'entrée. Examinez et déployez la configuration d'entrée.

Pour de plus amples informations, consultez la section Déployer la configuration d'entrée.



[NSADM-48414]

Les instances indiquent le type de déploiement avec une notation

Dans l'interface graphique ADM, les adresses IP de l'instance indiquent désormais le type de déploiement. Les notations suivantes décrivent le type de déploiement :

- En paire haute disponibilité, P — Serveur principal et S — Serveur secondaire.
- Cluster C
- Groupe de mise à l'échelle automatique A-

Si une instance n'a pas de notation, elle indique le déploiement autonome.

[NSADM-41859]

03 mars 2020

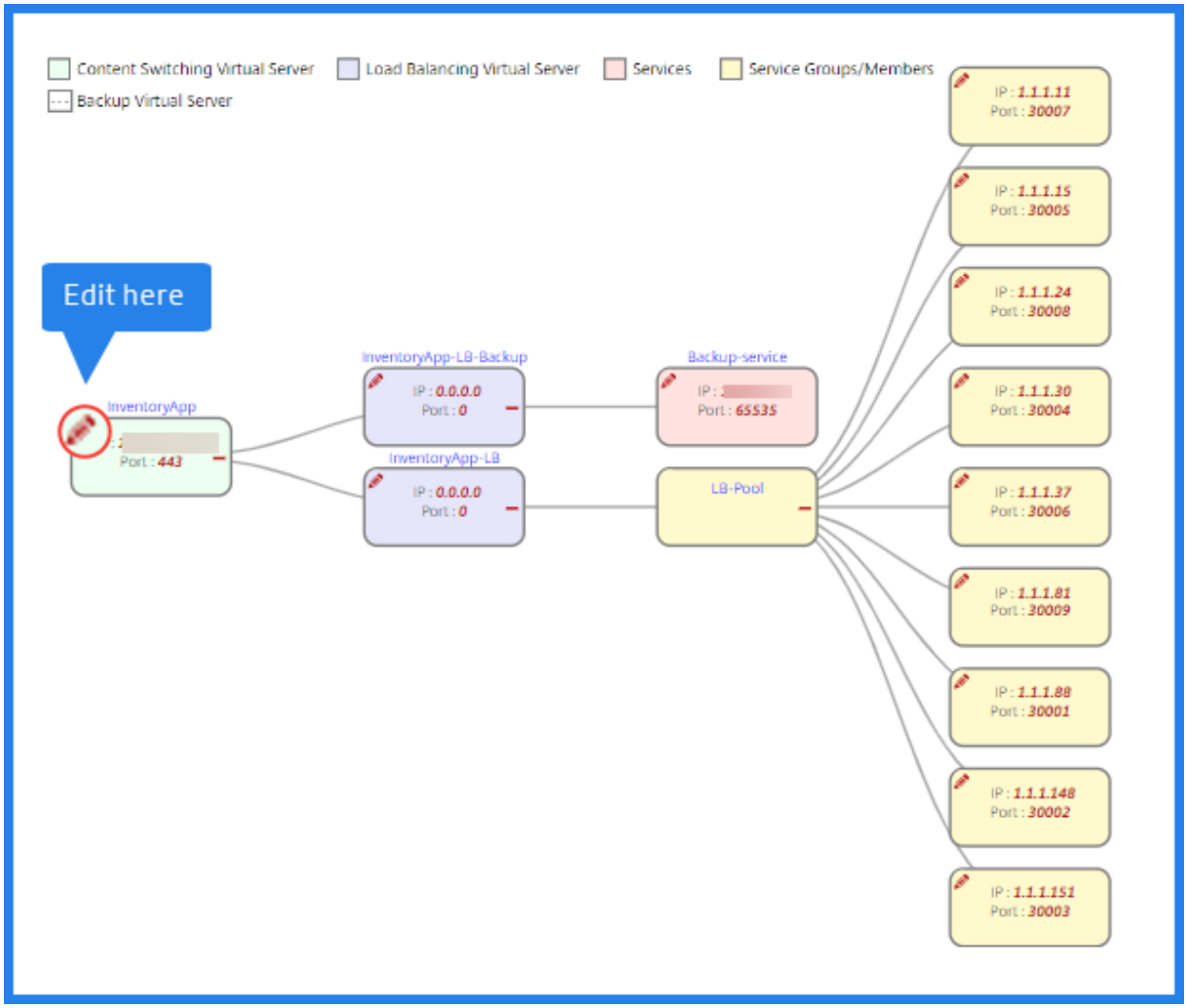
Modifier les attributs de déploiement dans StyleBooks Configuration Builder

> **Remarque**
>
> Cette fonctionnalité est en prévisualisation.

StyleBooks Configuration Builder vous aide à créer un StyleBook de configuration d'application et un pack de configuration à partir d'une configuration ADC existante. Le générateur de configuration automatise également la migration de la configuration de l'application d'une instance ADC vers une autre instance.

L'Assistant Générateur de configuration vous permet désormais de modifier les attributs de déploiement de l'application sélectionnée avant de créer un StyleBook et un pack de configuration. Vous pouvez maintenant modifier l'adresse IP et la valeur de port des serveurs virtuels, des services et des membres du groupe de services dans la configuration d'origine.

Une fois la création et la migration de l'application terminée, un ConfigPack est créé dans Citrix ADM avec son StyleBook correspondant. Ce pack de configuration contient les nouvelles adresses IP et les nouvelles valeurs des ports. Pour afficher le ConfigPack créé, accédez à **Applications > StyleBooks > Configurations**.



Pour de plus amples informations, consultez la section Migrer la configuration de l'application ADC à l'aide du Générateur de configuration Style.

[NSADM-44197]

Possibilité d'afficher toutes les applications mais de modifier uniquement un sous-ensemble d'applications

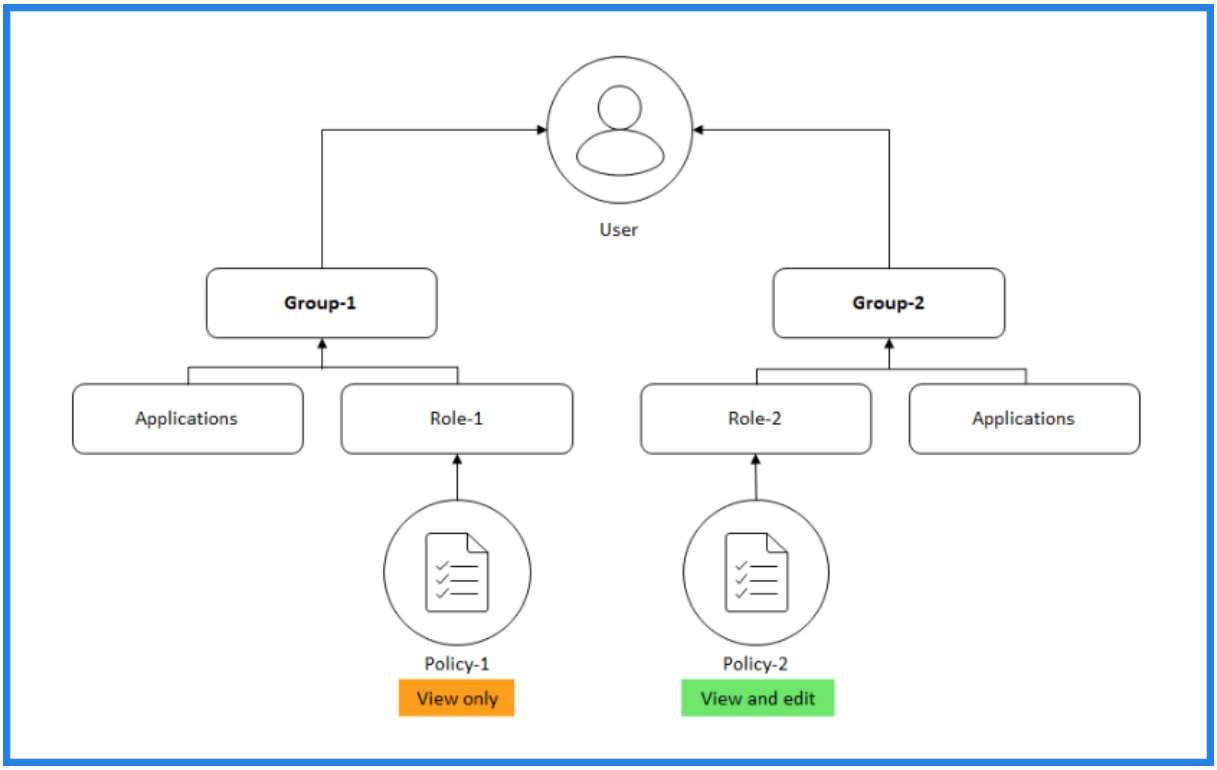
Lorsqu'un administrateur ajoute un utilisateur à un groupe qui a des paramètres de stratégie d'accès différents, l'utilisateur est mappé à plusieurs étendues d'autorisation et stratégies d'accès.

Dans ce cas, ADM accorde à l'utilisateur l'accès aux applications en fonction de la portée d'autorisation spécifique.

Considérez un utilisateur qui est affecté à un groupe doté de deux stratégies Stratégie-1 et Stratégie-2.

- Policy-1 — Affiche uniquement les autorisations pour les applications.
- Policy-2 — Afficher et modifier l'autorisation des applications.

Maintenant, l'utilisateur peut afficher les applications spécifiées dans Policy-1. En outre, cet utilisateur peut afficher et modifier les applications spécifiées dans la stratégie 2. L'accès à la modification des applications du groupe 1 est restreint car il n'est pas sous la portée de l'autorisation du groupe 1.



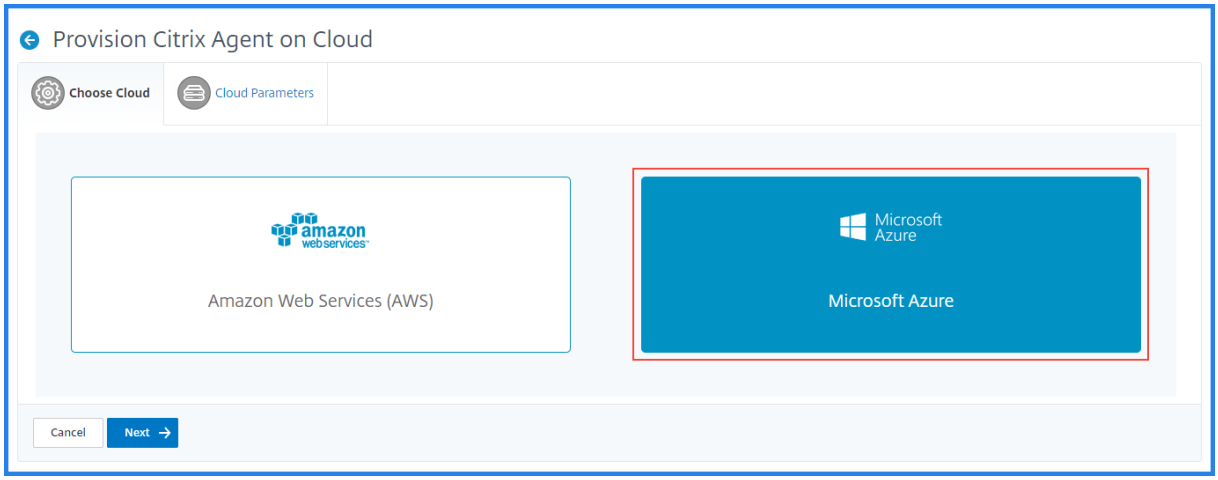
Auparavant, ADM considérait l'union de toutes les autorisations de groupe pour autoriser un utilisateur. Sur la base de l'exemple ci-dessus, l'utilisateur a pu visualiser et modifier toutes les applications de Group-1 et Group-2. Grâce à cette autorisation, l'utilisateur a pu modifier les ressources qui n'étaient pas principalement autorisées par la stratégie d'accès.

Pour de plus amples informations, consultez Comment l'accès utilisateur change en fonction de la portée d'autorisation

[NSHELP-5854]

Provisionner l'agent Citrix ADM sur Azure

Vous pouvez désormais provisionner un agent ADM sur Azure à l'aide de l'interface graphique ADM. L'agent ADM sur Azure s'inscrit automatiquement auprès de Citrix ADM, vous pouvez afficher l'agent enregistré dans la page **Réseaux > Agents**. Pour provisionner un agent ADM sur Azure, reportez-vous à la section Provisionner l'agent Citrix ADM sur Azure.

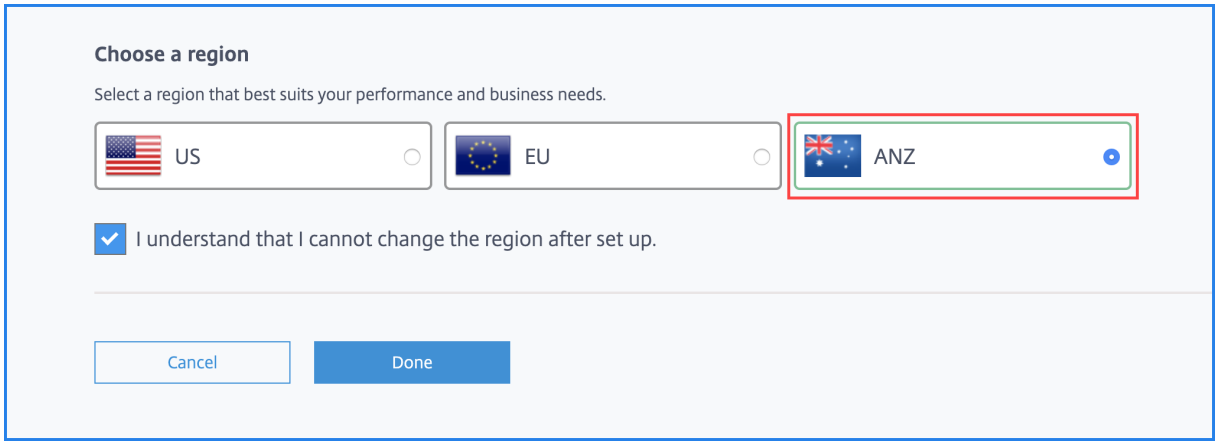


Vous pouvez également installer l'agent Citrix ADM à partir de la Place de Azure Marketplace. Pour de plus amples informations, consultez la section Installation de l'agent Citrix ADM sur Azure.

Sélectionnez la région Australie pour configurer le service ADM

Vous pouvez maintenant sélectionner la région Australie (ANZ) pour configurer le service ADM. Citrix ADM prend désormais en charge les régions suivantes :

- États-Unis (US)
- Europe (UE)
- Australie (ANZ)



Pour de plus amples informations, consultez la section Mise en route.

[NSADM-44447]

Exécuter des scripts personnalisés avant et après la tâche de maintenance de la mise à niveau

Lorsque vous mettez à niveau votre instance ADC en créant un travail de maintenance, ADM effectue une vérification préalable de la validation des instances que vous souhaitez mettre à niveau. L'onglet

Validation avant la mise à niveau vérifie les éléments suivants sur les instances sélectionnées :

- Vérifie les personnalisations.
- Vérifie l'utilisation du disque et affiche une erreur si l'espace disque est faible.
- Vérifie les problèmes matériels du disque.

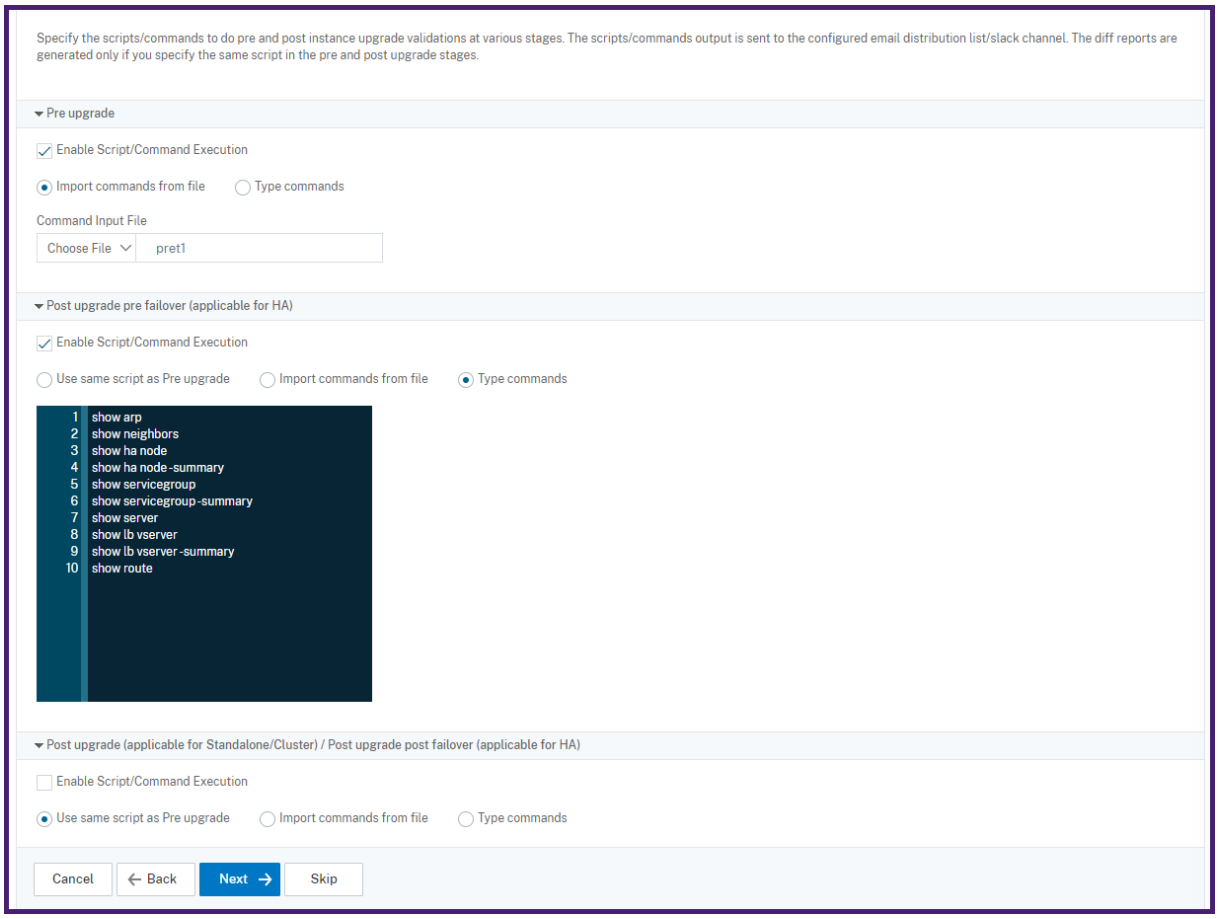
Vous pouvez supprimer les instances ayant échoué et créer un travail de maintenance de mise à niveau.

Dans les **scripts personnalisés**, spécifiez des scripts personnalisés à exécuter avant et après une mise à niveau d'instance. Utilisez l'une des méthodes suivantes pour exécuter les commandes :

- Importer des commandes à partir d'un fichier.
- Tapez des commandes directement sur l'interface graphique Citrix ADM.

Ces scripts vous aident à vérifier les modifications avant et après la mise à niveau. Par exemple :

- Version de l'instance avant et après la mise à niveau.
- État des interfaces, des nœuds haute disponibilité, des serveurs virtuels et des services avant et après la mise à niveau.
- Les statistiques des serveurs et services virtuels.
- Les routes dynamiques.



Pour de plus amples informations, consultez la section Utiliser des tâches pour mettre à niveau des instances Citrix ADC.

[NSADM-40534]

Télécharger l'image de mise à niveau vers une instance pendant l'exécution du travail

Si vous planifiez une tâche de maintenance de mise à niveau, vous pouvez décider quand vous souhaitez charger une image de mise à niveau vers une instance ADC. Dans Créer un travail, choisissez l'une des options suivantes :

- **Télécharger maintenant** : cette option télécharge immédiatement l'image vers une instance.
- **Charger au moment de l'exécution** : cette option télécharge l'image vers une instance ADC lorsque l'ADM exécute la tâche de maintenance de mise à niveau planifiée.

Pour de plus amples informations, consultez la section Planifier la mise à niveau des instances Citrix ADC.

[NSADM-44855]

Les groupes de Autoscale ADM prennent en charge les types d'instance AWS C5, M5 et C5n

Si vous choisissez de créer des groupes de mise à Autoscale ADM sur le cloud AWS, vous pouvez désormais provisionner des instances ADC avec les types d'instances AWS C5, M5 et C5n. Vous pouvez sélectionner ces types d'instance pour obtenir une mise à l'échelle automatique ADM haute performance.

> **Remarque**
>
> L'interface graphique ADM remplit automatiquement les types d'instance AWS recommandés pour la version ADC sélectionnée. Consultez Créer des groupes de mise à l'échelle automatique.

Pour plus d'informations sur les types d'instance AWS, reportez-vous à la section Types d'instance AWS.

[NSADM-40089]

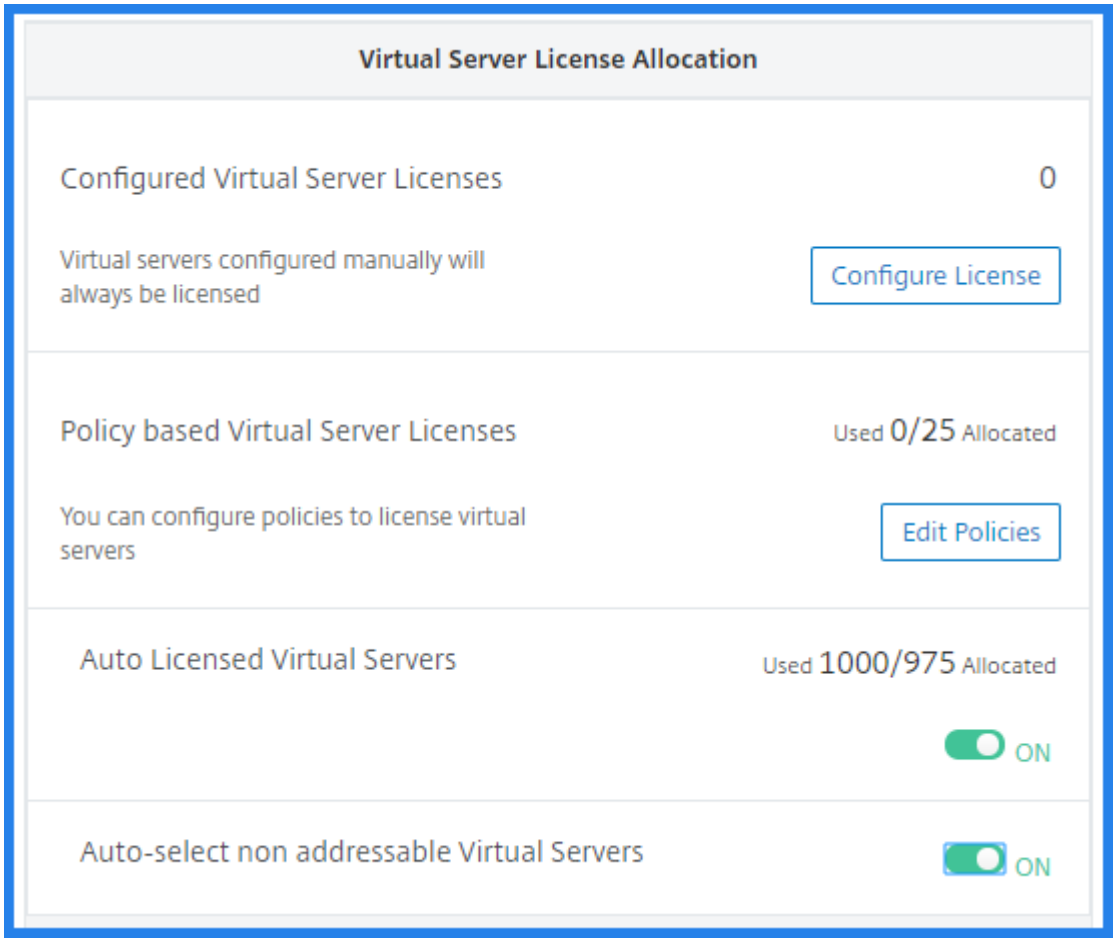
Appliquer une licence aux serveurs virtuels à l'aide d'une stratégie

Dans **Abonnements**, vous pouvez désormais configurer une stratégie pour appliquer une licence aux serveurs virtuels. Auparavant, vous n'étiez en mesure d'appliquer des licences qu'à des serveurs virtuels manuellement ou automatiquement. Vous pouvez maintenant appliquer une licence à l'aide d'une stratégie ou d'un manuel ou automatique.

En utilisant la stratégie, vous pouvez contrôler le nombre de serveurs virtuels que vous souhaitez attribuer une licence automatique. Appliquez une licence aux serveurs virtuels des instances sélectionnées uniquement.

Lorsque vous modifiez une stratégie, vous pouvez spécifier les éléments suivants :

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



Les options **Serveurs virtuels sous licence automatiqueet Sélection automatique des serveurs virtuels non adressables**sont désormais indépendantes. Auparavant, vous étiez en mesure d'activer la**sélection automatique des serveurs virtuels non adressables**uniquement si vous

activez les**serveurs virtuels sous licence automatique**.

[NSADM-35724]

Voir les problèmes de capacité ADC dans le SMA

Lorsqu'une instance ADC a consommé la plus grande partie de sa capacité disponible, la suppression de paquets peut se produire lors du traitement du trafic client. Ce problème provoque de faibles performances dans une instance ADC. En comprenant ces problèmes de capacité ADC, vous pouvez allouer plus de licences de manière proactive afin de stabiliser les performances de ADC.

Pour afficher les problèmes de capacité de l'ADC,

1. Accédez à **Réseaux > Analyse de l'infrastructure**.
2. Développez l'instance pour laquelle vous souhaitez afficher les problèmes de capacité.

L'ADM interroge ces événements toutes les cinq minutes à partir de l'instance ADC et affiche les baisses de paquets ou les incréments de compteur de limite de vitesse s'il existe. Les problèmes sont classés selon les paramètres de capacité suivants :

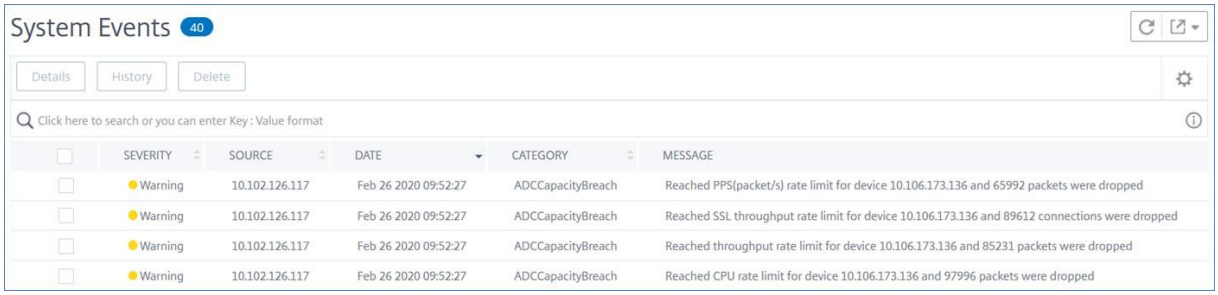
- **Limite de débit atteinte** : nombre de paquets abandonnés dans l'instance après que la limite de débit est atteinte.
- **Limite de CPU PE atteinte** : nombre de paquets abandonnés sur toutes les cartes réseau après que la limite de CPU PE est atteinte.
- **Limite PPS atteinte** : nombre de paquets abandonnés dans l'instance après que la limite PPS est atteinte.
- **Limite de débit SSL** : nombre de fois que la limite de débit SSL est atteinte.
- **Limite de taux TPS SSL** : Nombre de fois que la limite TPS SSL a été atteinte.

L'ADM calcule le score d'instance sur le seuil de capacité défini.

- Seuil bas — 1 incrément de dépassement de paquets ou de compteur de limite de taux
- Seuil élevé : 10000 paquets baisse ou incrément du compteur de limite de taux

Par conséquent, lorsqu'une instance ADC franchit le seuil de capacité, le score d'instance est affecté.

Lorsque les paquets diminuent ou que le compteur de limite de vitesse s'incrémente, un événement est généré sous la catégorie `ADCCapacityBreach`. Pour afficher ces événements, accédez à **Comptes > Événements système**.



Si vous souhaitez afficher les statistiques de limite de taux ADC pour la période sélectionnée (heure/jour/semaine/mois), accédez à **Réseau > Rapports réseau**.

[NSADM-40183]

Afficher les détails du service dans le graphique de service

Dans Service Graph, placez le pointeur de la souris sur un service et cliquez sur un service pour afficher les options suivantes :

- **Afficher les détails**
- **Journaux de transactions** - Permet d'afficher les détails des transactions HTTP et SSL sur HTTP. Pour plus d'informations, voir Afficher les journaux de transactions Web.

L'option **Afficher les détails** vous permet d'afficher :

- Nom du cluster où le service est hébergé.
- L'espace de noms et les étiquettes de service du service
- Tous les services entrants et sortants associés au service sélectionné
- **Mesures de clé de service dans un format graphique telles que les accès, le**temps de réponse du service**, les**erreurs HTTP**, le**volume de données, les erreurs front-end****SSL, les erreurs back-end**SSL, les **erreurs front-endTCP et les erreurs back-end**TCP**

À l'aide de ces tendances de mesures clés, vous pouvez analyser les performances du service pour la durée sélectionnée.

Pour de plus amples informations, consultez la section Afficher les détails du service.

[NSADM-41297]

Afficher le graphique de service pour les applications (GSLB)

> **Remarque**
>
> Cette fonctionnalité est en prévisualisation.

Vous pouvez désormais afficher les applications GSLB dans Service Graph pour afficher les éléments suivants :

- Comment l'application est configurée (avec l'application GSLB, le centre de données, l'instance ADC, les serveurs virtuels CS et LB)
- Vues de bout en bout du client aux services
- Le nom du centre de données où les demandes client sont traitées et les mesures Citrix ADC du centre de données associées
- L'état du serveur virtuel GSLB, tel que Critical, Review et Good. Citrix ADM affiche l'état du serveur virtuel en fonction du score de l'application.
- **Critique (rouge)** : indique quand le score de l'application est < 40
- **Avis (orange)** - Indique quand le score de l'application est compris entre 40 et 75
- **Bon (vert)** - Indique lorsque le score de l'application est > 75

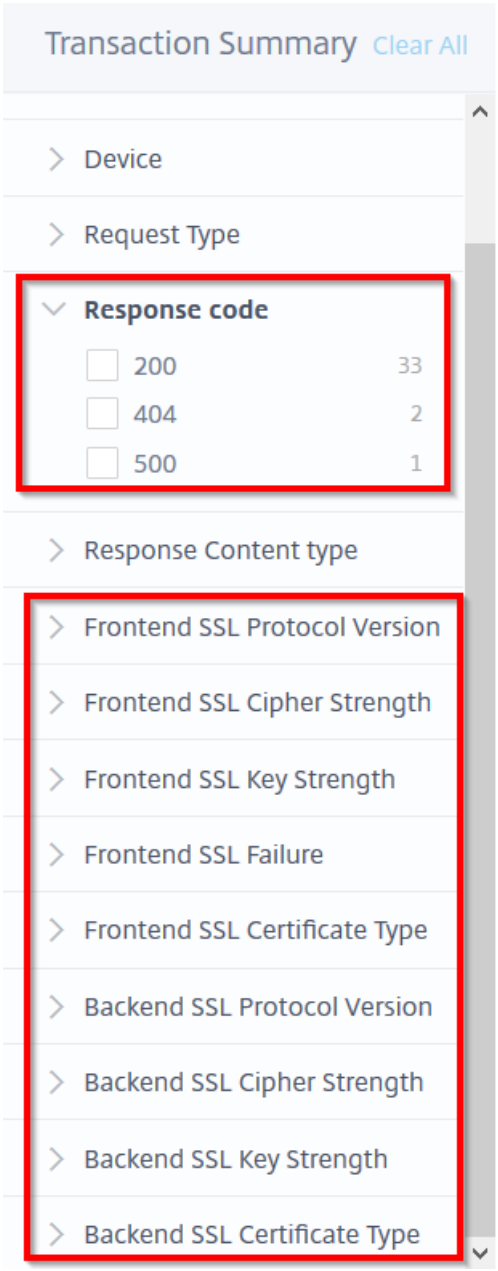
Pour de plus amples informations, consultez la section Graphique de service.

[NSADM-43967]

Afficher les mesures 4xx et SSL dans le panneau Synthèse des transactions

Le panneau **Synthèse des transactions Web d'analyse des transactions** vous permet désormais d'afficher les éléments suivants :

- Erreurs 4xx
- Mesures front-end SSL et back-end SSL



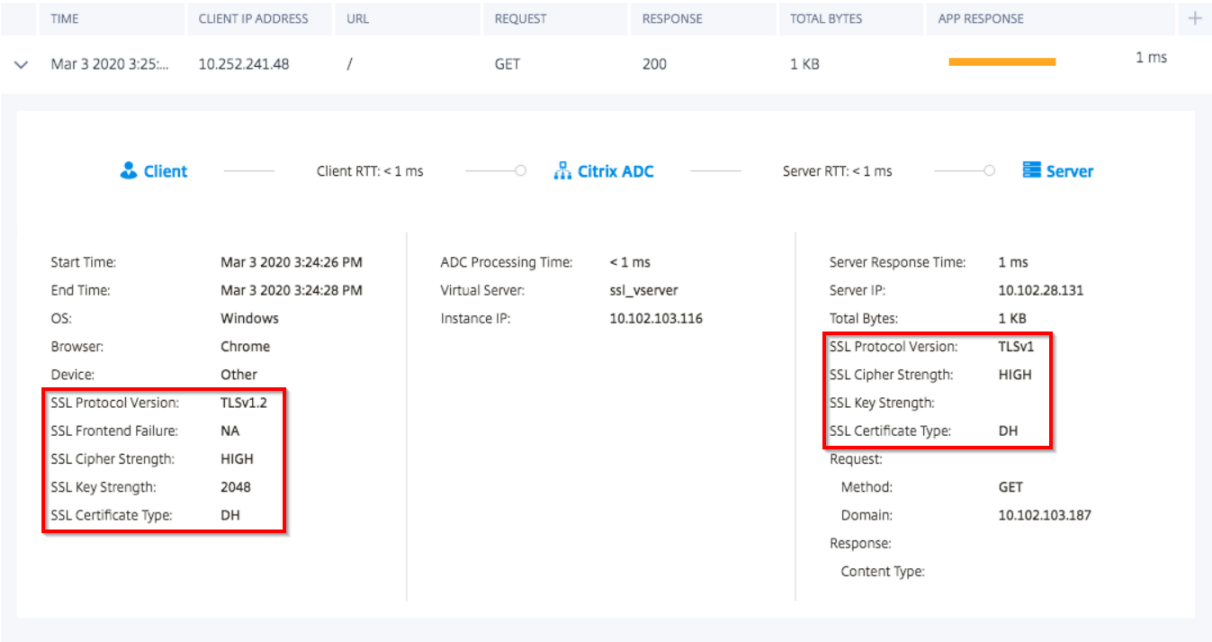
Pour plus de détails, consultez Afficher les analyses pour les transactions Web.

[NSADM-43841]

Afficher les mesures SSL dans l'analyse des transactions Web

Lorsque vous cliquez sur une transaction dans l'analyse des transactions Web, vous pouvez désormais afficher d'autres mesures pour les transactions SSL. À partir de ces mesures, vous pouvez analyser si les erreurs SSL se produisent à partir du client ou du serveur.

Les mesures suivantes sont affichées pour le client et le serveur :

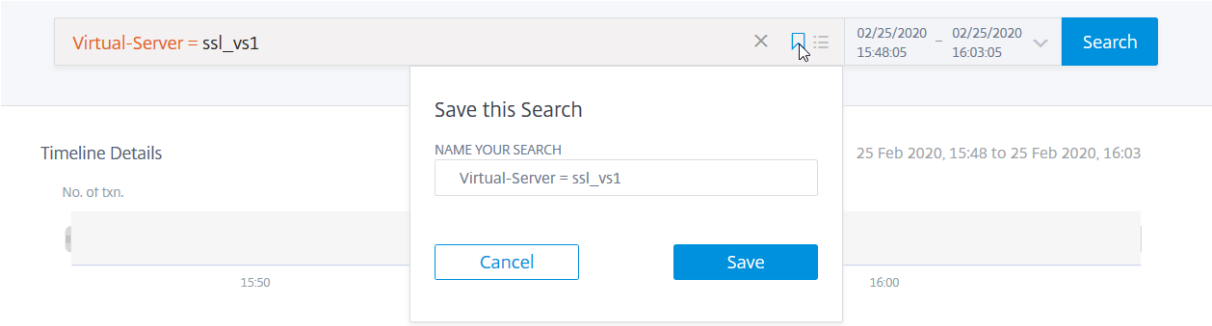


Pour plus de détails, consultez Afficher les analyses pour les transactions Web.

[NSADM-43844]

Enregistrer l'option de recherche dans l'analyse des transactions Web Recherche avancée

L'option de recherche avancée de l'analyse des transactions Web vous permet désormais d'enregistrer les requêtes de recherche. Vous pouvez ensuite cliquer sur la requête de recherche enregistrée dans la liste, au lieu d'utiliser à nouveau les suggestions et les opérateurs.
Pour enregistrer une requête de recherche, cliquez sur l'icône de signet, spécifiez le nom de votre choix, puis cliquez sur **Enregistrer**.



Pour plus de détails, consultez Afficher les analyses pour les transactions Web.

[NSADM-43843]

Problèmes résolus

Applications

- Le tableau de bord Application n'affiche pas les applications de la paire ADC HA et du cluster.

[NSADM-47668]

- Citrix ADM affiche un message d'erreur dans le tableau de bord des applications si aucun agent n'est ajouté.

[NSADM-47444]

- Tableau de bord de l'application est affiché vide dans le navigateur **IE 11**.

[NSADM-47812]

Analytics

- Si vous activez la mesure côté client sur les instances ADC AppFlow, le processus de fichier journal du décodeur Citrix ADM AppFlow échoue.

[NSHELP-21462]

Réseaux

- Le nom d'hôte ADC n'est pas affiché dans **Fonctions réseau > GSLB**.

[NSADM-47335]

- Le tableau de bord **Network Reporting** n'affiche pas les données complètes pour une durée d'un mois.

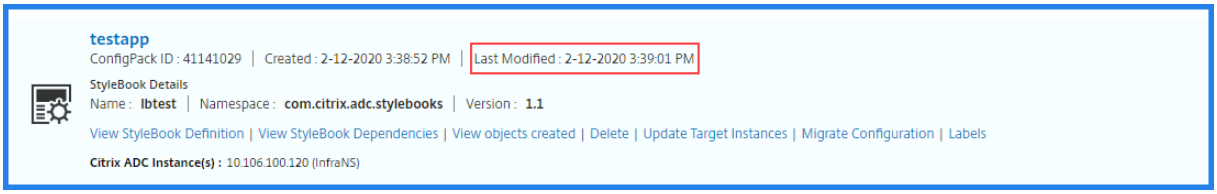
[NSHELP-21731]

11 février 2020

Fonctionnalités nouvelles et améliorées

La configuration StyleBooks affiche une nouvelle colonne

Dans **Applications** > **StyleBooks** > **Configurations**, une configuration StyleBook (pack de configuration) affiche désormais l'heure de la dernière mise à jour sur la vignette de configuration.



[NSADM-45811]

Problèmes résolus

Analytics

- Les rapports hebdomadaires pour les informations Web Insight et HDX ne sont pas affichés.

  [NSADM-46149]

Applications

- La durée par défaut dans le Tableau de bord des applications pour afficher l'analyse des applications est modifiée à 15 minutes.

  [NSADM-46980]

- Lorsque vous créez une application personnalisée à l'aide de la configuration StyleBook, les options de modification et de suppression ne fonctionnent pas comme prévu.

  [NSADM-46821]

Système de licences

- L'option de capacité groupée n'apparaît pas sous Type de licence de bande passante pour la première fois.

  Solution de contournement :

  1. Sélectionnez Licences CPU virtuelles dans la liste Type de licence.
  2. Remplacez la sélection par Licence de bande passante pour sélectionner l'option Capacité groupée.

  [NSADM-40129]

Réseaux

- Lorsque vous créez un travail de configuration avec de nombreuses commandes, l'option **Abandonner** n'est pas affichée dans l'onglet **Action**.

  [NSADM-47041]

03 février 2020

Fonctionnalités nouvelles et améliorées

Graphique de service pour les applications

À l'aide de la fonction de graphe de service du tableau de bord de l'application, vous pouvez afficher :

- Détails sur la configuration de l'application (avec un serveur virtuel de commutation de contenu et un serveur virtuel d'équilibrage de charge)
- Vues de bout en bout des clients aux services
- Emplacement à partir duquel le client accède à l'application
- Détails des mesures pour les serveurs clients, les services et les serveurs virtuels
- Si les erreurs proviennent du client ou du service
- Le service, le serveur virtuel et l'état du client, tels que **Critical**, **Review**et **Bon**.

Pour de plus amples informations, consultez la section Graphique de service.

[NSADM-41898]

Un tableau de bord amélioré

À l'aide du tableau de bord de l'application, vous pouvez désormais afficher les nouvelles fonctionnalités suivantes :

- Statut de la demande (Critique, Passable, Bon et Non Applicable)
- Détails de la configuration de l'application (équilibrage de charge ou changement de contenu)
- Détails des services associés à l'application sélectionnée
- Détails des mesures pour l'application sélectionnée, tels que le temps de réponse de l'application, le débit, les demandes par seconde, le pourcentage d'erreur, le nombre total de connexions et le volume de données sous forme de graphique
- Toutes les questions applicables à la demande sélectionnée

Pour de plus amples informations, consultez la section Applications.

[NSADM-32894]

Indicateurs de performance dans App Analytics

Citrix ADM affiche désormais les nouveaux indicateurs de performance d'application suivants qui se produisent dans l'application Web Citrix ADC :

- Type de persistance incorrect
- Serveur instable (5xx)
- Recommandation de réutilisation de session (SSL)
- Trafic en temps réel SSL
- En-têtes HTTP exceptionnellement volumineux
- Hits de limite de file d'attente de réassemblage TCP
- Accumulation dans la file d'attente de surtension

Vous pouvez afficher ces problèmes d'application en accédant à **Applications > Tableau de bord**, puis en sélectionnant une application.

Pour de plus amples informations, consultez la section Indicateurs de performance pour l'analyse des applications.

[NSADM-39779]

Prise en charge du pare-feu d'applications Web dans Citrix ADM

Les nouvelles stratégies de protection du pare-feu d'application Web (WAF) suivantes sont activées dans Security Insight, qui mettent en évidence les modèles de violation pour WAF :

- APPFW_BUFFEROVERFLOW_QUERY
- APPFW_BUFFEROVERFLOW_TOTAL_HDR

[NSADM-43541]

Configuration StyleBooks affichage nom d'hôte de l'instance ADC

Une configuration StyleBooks (pack de configuration) affiche désormais le nom d'hôte de l'instance ADC ainsi que l'adresse IP sur la vignette de configuration. Vous pouvez désormais rechercher des configurations StyleBook à l'aide du nom d'hôte ou de son adresse IP.

[NSADM-42517]

Supprimer les clusters Kubernetes inaccessibles

Vous pouvez désormais supprimer Kubernetes Ingresses du service ADM même lorsque le cluster est inaccessible ou n'existe plus. Après avoir supprimé les Ingresses sur le cluster, vous pouvez également supprimer le cluster parent quelle que soit son accessibilité.

[NSADM-45612]

Traiter les événements d'entrée avec la classe Citrix Ingress

Citrix ADM ServiceNow traite les événements d'entrée qui ont une annotation de classe Citrix Ingress (`kubernetes.io/ingress.class: Citrix`) uniquement. En outre, les spécifications d'entrée générées par le service ADM contiennent des annotations de classe Citrix Ingress.

[NSADM-45613]

Configurer la licence de capacité groupée sur les instances FIPS Citrix ADC

Vous pouvez désormais configurer une licence de capacité groupée sur Citrix ADC MPX et VPX FIPS licence. Pour de plus amples informations, consultez la section Configurer la capacité groupée.

[NSADM-31742]

Nouvelle heure d'interrogation par défaut pour les entités de fonction réseau

La durée d'interrogation par défaut des entités de fonction réseau passe de 30 à 60 minutes. Par défaut, le service Citrix ADM interroge automatiquement les entités de fonctions réseau configurées toutes les 60 minutes.

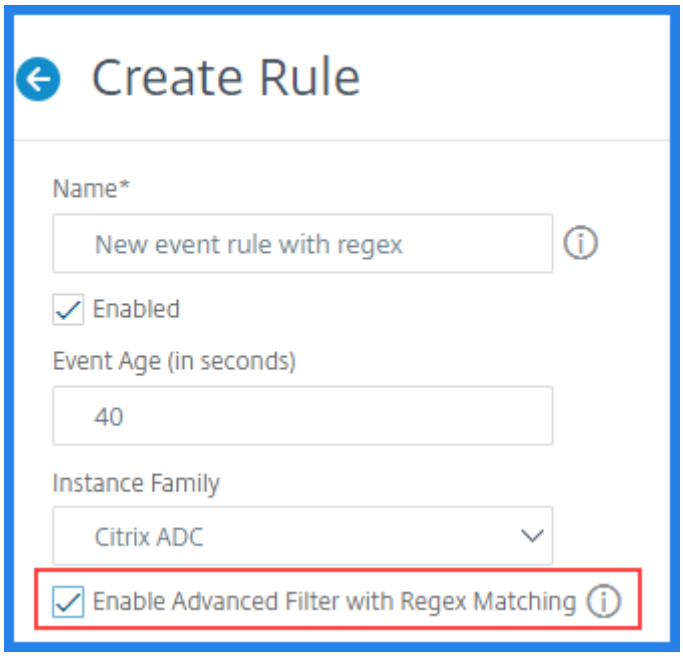
Pour de plus amples informations, consultez la section Procédure d'interrogation par Citrix ADM des instances et des entités gérées.

[NSADM-44078]

Filtre avancé avec correspondance des motifs regex

Vous pouvez désormais filtrer les objets d'échec, les commandes de configuration et les messages à l'aide de la correspondance des motifs d'expression régulière. Auparavant, vous étiez en mesure d'utiliser uniquement le modèle astérisque (*) correspondant pour filtrer les événements.

Pour de plus amples informations, consultez la section Définir une règle d'événement.



[NSADM-43614]

Afficher et modifier des rapports d'exportation spécifiques aux entités

Citrix ADM affiche des rapports d'exportation planifiée spécifiques aux entités sous des entités ADM individuelles, que vous pouvez afficher, modifier ou supprimer. Par exemple, pour afficher les rapports d'exportation des instances Citrix ADC, accédez à **Réseau > Instances > Citrix ADC** et cliquez sur l'icône d'exportation. La page **Exporter les rapports** affiche tous les rapports d'exportation des in-

stances ADC. Auparavant, les rapports d'exportation planifiée d'ADM étaient répertoriés sous **Compte > Programmes d'exportation**.

Pour de plus amples informations, consultez la section Exporter ou planifier des rapports d'exportation.

[NSADM-43329]

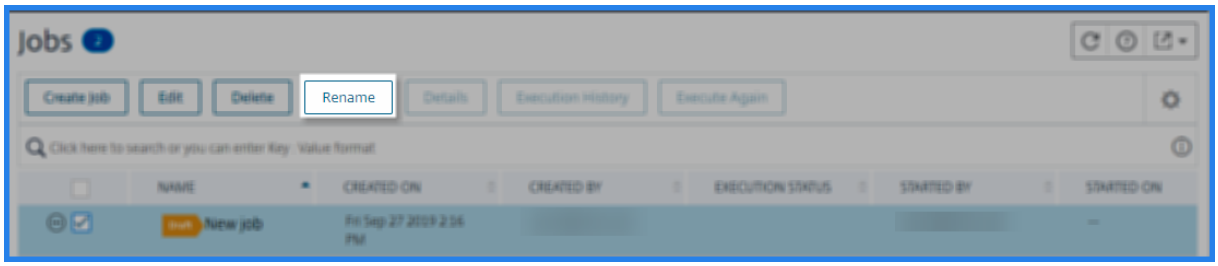
Afficher et télécharger les certificats SSL Citrix ADC

L'interface graphique Citrix ADM affiche tous les certificats SSL des instances Citrix ADC découvertes. Pour afficher et télécharger des certificats SSL d'instances ADC, accédez à **Réseaux > Tableau de bord SSL > Fichiers de certificats SSL sur Citrix ADC**.

[NSHELP-6556]

Renommer les tâches de configuration et les modèles

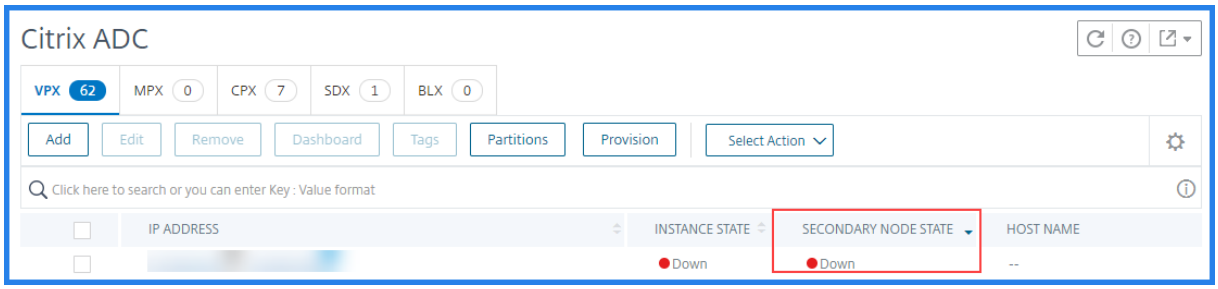
Vous pouvez désormais renommer les tâches de configuration personnalisées et les modèles d'audit personnalisés dans Citrix ADM.



[NSADM-42945, NSHELP-6488]

Une nouvelle colonne pour l'état d'instance secondaire

Dans l'interface graphique Citrix ADM, vous pouvez désormais vérifier l'état de l'instance secondaire d'une paire haute disponibilité, sous **Réseaux > Instances**. Par exemple, lorsque vous cliquez sur **Citrix ADC**, vous voyez une nouvelle colonne pour l'état de l'instance secondaire. L'interface graphique Citrix ADM affiche l'état de l'instance secondaire sur la page Vue d'ensemble de l'instance. Vous pouvez maintenant afficher l'état sous la colonne **État du nœud secondaire** et Tableau de bord.



[NSHELP-6236]

Problèmes résolus

- Dans **App Dashboard**, lorsque vous définissez une application personnalisée à l'aide de StyleBooks, les StyleBooks apparaissent en bas de la page, ce qui était difficile à parcourir.

  Avec ce correctif, les StyleBooks apparaissent sur la nouvelle page. Après avoir spécifié les détails du StyleBook sélectionné, la nouvelle application apparaît dans le Tableau de **bord de l'application**.

  [NSADM-45241]

- Si vous téléchargez un fichier comportant plusieurs périodes (.) dans le nom de fichier pour créer un travail de configuration, l'interface graphique Citrix ADM affiche une erreur. Par conséquent, aucune tâche de configuration n'est créée.

  [NSADM-45748]

17 décembre 2019

Fonctionnalités nouvelles et améliorées

Prise en charge du basculement de l'agent Citrix ADM

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

Pour obtenir un basculement de l'agent, sélectionnez les agents Citrix ADM requis un par un et attachez-les au même site. Pour de plus amples informations, consultez la section Configurer les agents Citrix ADM pour un déploiement multisite.

[NSADM-30048]

Afficher la dérive de configuration Citrix ADC en deux modes

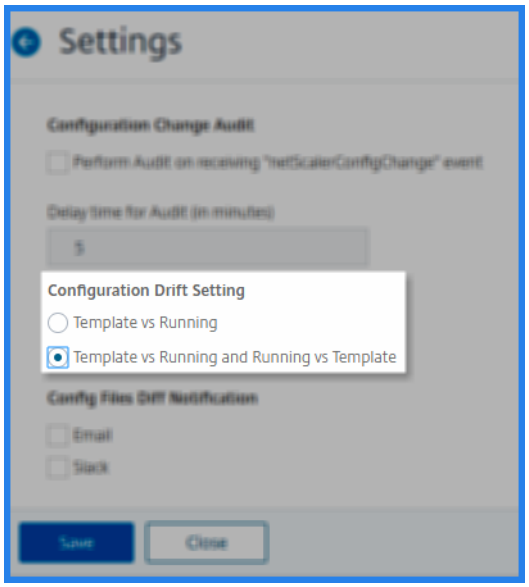
Dans l'interface graphique Citrix ADM, vous pouvez désormais afficher la dérive de configuration en deux modes.

1. **Modèle vs en cours d'exécution** : le service ADM compare la configuration du modèle d'audit à la configuration en cours d'exécution sur l'instance.
2. **Modèle vs Exécution et Exécution vs Modèle** : Le service ADM compare la configuration des deux façons :

- Compare la configuration du modèle d'audit avec la configuration en cours d'exécution sur l'instance.
- Compare la configuration en cours d'exécution sur l'instance avec le modèle d'audit.

Après comparaison, l'interface graphique Citrix ADM affiche la différence entre le modèle d'audit et la configuration en cours d'exécution. En outre, il affiche les commandes permettant de corriger la configuration en cours d'exécution par rapport au modèle d'audit.

Par défaut, le paramètre Modèle vs dérive en cours d'exécution est sélectionné. Pour modifier le paramètre de dérive, dans l'interface graphique d'ADM, sélectionnez **Paramètres** dans la page **Vérification de la configuration**.



Pour de plus amples informations, consultez la section Modèle vs Courir Diff.

[NSHELP-6463]

Exécuter un travail de configuration sur un nœud secondaire Citrix ADC

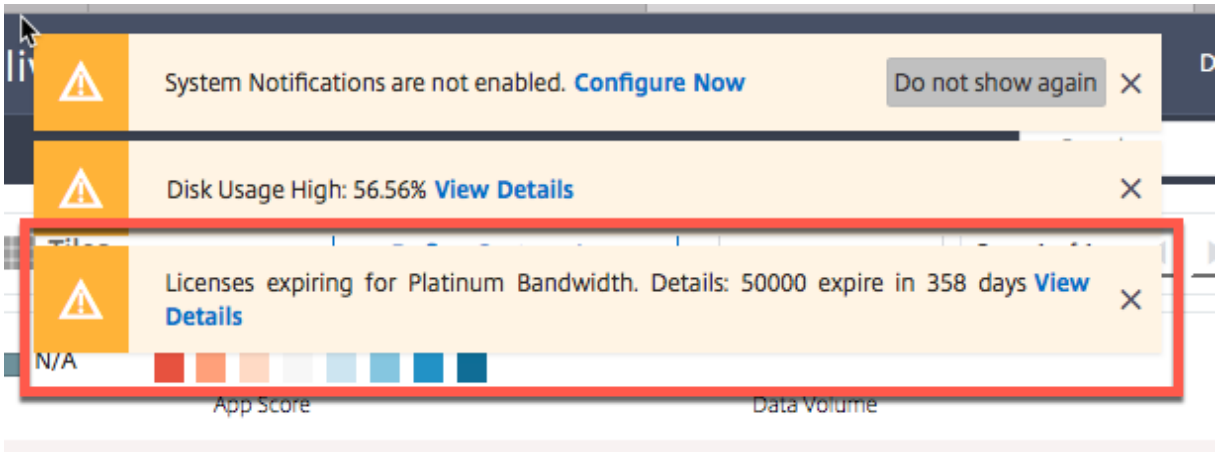
Dans une paire Citrix ADC haute disponibilité, vous pouvez désormais sélectionner le nœud principal ou le nœud secondaire ou les deux nœuds pour exécuter un travail de configuration. Si vous ne spécifiez pas le nœud, le travail de configuration s'exécute automatiquement sur le nœud principal.

Auparavant, vous étiez en mesure d'exécuter des tâches de configuration uniquement sur le nœud principal. Pour de plus amples informations, consultez la section Comment créer un travail de configuration.

[NSHELP-6567]

Notification d'expiration pour la licence d'enregistrement de départ

Lorsque vous vous connectez au service ADM, un message d'alerte système s'affiche si votre licence d'extraction d'enregistrement est sur le point d'expirer. Pour obtenir l'alerte, vous devez configurer la notification de licence. Pour plus d'informations sur la configuration, reportez-vous à la section Vérifications d'expiration pour les licences de serveur virtuel.



[NSADM-42655]

Détails de la bande passante dans la notification de licence de capacité groupée

La notification d'expiration pour les licences de capacité groupée ADM inclut désormais des détails sur la bande passante. Vous pouvez voir la bande passante qui est sur le point d'expirer hors du pool total. Auparavant, les détails de bande passante étaient disponibles uniquement dans l'interface graphique. Pour obtenir une notification d'expiration, vous devez configurer le service ADM. Pour de plus amples informations, consultez la section Vérifications d'expiration pour les licences de serveur virtuel.

[NSADM-39332]

Afficher les détails de l'instance dans Infrastructure Analytics

Dans l'analyse d'infrastructure, lorsque vous cliquez sur une adresse IP d'instance, vous pouvez désormais afficher les détails suivants dans l'onglet **Vue d'ensemble** :

- Score d'instance, catégories de problèmes affectant le score d'instance et autres détails d'instance.
- Mesures clés de l'instance telles que l'utilisation du processeur, l'utilisation de la mémoire, le débit, les requêtes HTTPs/s, les connexions TCP et les transactions SSL.
- Détails de tous les problèmes qui affectent le score d'instance.

Pour de plus amples informations, consultez la section Analyse d'infrastructure.

[NSADM-42276]

Problèmes connus

April 29, 2021

Citrix Application Delivery Management (Citrix ADM) présente les problèmes connus suivants :

Analytics

Dans Gateway Insight, lorsque vous planifiez un rapport (**Exporter des rapports > Planifier l'exportation)**, le rapport généré affiche « Page introuvable ».

[NSHELP-26283]

Réseaux

- Dans l'interface graphique de l' **avis de sécurité** sous **Réseaux>Instance Advisory>Avis de sécurité**, tous les CVE peuvent ne pas apparaître, et un seul CVE peut apparaître dans les rapports ou le tableau de bord consultatif.

  Solution : cliquez sur **Analyser maintenant** pour exécuter une analyse à la demande. Une fois l'analyse terminée, tous les CVE dans la portée (environ 15) apparaissent dans l'interface graphique ou le rapport.

[NSADM-69920]

- Lorsque vous abandonnez un travail de configuration en cours, les commandes réussies ne sont pas annulées si l'option **Annuler les commandes réussies** est sélectionnée pour l'option **Sur l'échec de la commande** dans la page Paramètres d' **exécution**.

[NSADM-34246]

- ADM ne communique pas avec les instances ADC BLX via SSH, et certaines fonctionnalités ADC telles que Config Audit et Config Jobs peuvent ne pas fonctionner avec BLX.

  [NSADM-68985]

Système de licences

Lorsque vous choisissez des licences Citrix ADM pour créer un groupe de mise à l'Autoscale, les licences regroupées n'apparaissent pas.

[NSADM-62727]

Communiqués précédents

April 29, 2021

Cette rubrique est la liste des versions précédentes de Citrix Application Delivery Management (Citrix ADM).

03 décembre 2019

Fonctionnalités nouvelles et améliorées

Configurer les seuils dans Service Graph

En tant qu'administrateur, vous pouvez désormais configurer des seuils pour les services Kubernetes. Citrix ADM affiche l'état du service (Critique, Révision et Bon) en fonction du temps de réponse du service et du nombre d'erreurs. Par défaut, vous pouvez afficher le seuil par défaut (temps de réponse du service = 200 ms et nombre d'erreurs = 0) appliqué à tous les services.

Pour de plus amples informations, consultez Configurer les seuils dans Service Graph

[NSADM-41290]

Mesures TCP et SSL pour les services

Dans Service Graph, en dehors des détails de transaction HTTP, vous pouvez désormais afficher les dépendances et les mesures des services TCP et SSL. Le graphique de service est maintenant affiché avec le protocole utilisé par les services. À l'aide des mesures TCP et SSL, vous pouvez :

- Afficher les détails de connexion TCP entre les services
- Déterminer si les problèmes liés à TCP proviennent du service source ou de destination
- Afficher si l'erreur SSL provient du service source ou de destination
- Afficher la version du protocole SSL utilisée par les services SSL

Pour de plus amples informations, consultez la section Graphique de service.

[NSADM-41295],[NSADM-41296]

Configurer l'intervalle de keep-alive

Vous pouvez maintenant configurer keep-alive interne pour maintenir la connexion entre le service ADM et l'agent. La durée interne doit être de 30 à 120 secondes. Pour configurer l'intervalle, à partir de l'interface graphique du service ADM, accédez à **Paramètres > Paramètres système > Configurations système > Agent et fuseau horaire**.

[NSADM-43641]

Prise en charge de l'aide contextuelle

Pour améliorer l'expérience utilisateur, l'interface graphique Citrix ADM dispose désormais d'un panneau d'aide. Lorsque vous ouvrez une session au service ADM, cliquez sur le point d'interrogation (?) dans le coin supérieur droit de l'écran de service pour lancer le panneau **d'aide**.

Ce panneau d'aide comprend des options permettant d'afficher les informations suivantes :

- Aide contextuelle : Lancez du contenu spécifique à l'écran de l'interface utilisateur que vous consultez. Actuellement, le lien d'aide s'ouvre dans un nouvel onglet du navigateur et affiche le contenu contextuel de la documentation produit.
- Documentation : Lancez la page d'aperçu de la documentation du service ADM et accédez au contenu souhaité.
- Forum de discussion : Lancez le site du forum pour voir ce que notre communauté d'experts discute.
- Comment acheter : Lancez le site citrix.com à partir duquel vous pouvez acheter le service ADM.
- Support client : Lancez le site d'assistance pour contacter notre équipe de support.

[NSADM-39656]

Problèmes résolus

Réseaux

Sous **GUI ADM > Réseaux > Analyse de l'infrastructure**, lorsque vous cliquez sur **Vue Circle Pack** ou **Vue tabulaire** dans le coin supérieur droit, la page n'est pas rendue correctement sur le navigateur Firefox.

[NSADM-40660]

Dans la page d'ajout d'un groupe de mise à l'Autoscale (**GUI ADM > Réseaux > Groupes de mise à l'échelle automatique > Ajouter**), l'option permettant de sélectionner l'édition de licence (par exemple, Citrix ADC VPX Advanced Edition-10 Mbps) apparaît sous l'onglet **Paramètres Cloud** au lieu de l'onglet **Licence** .

[NSADM-43759]

La notification par e-mail, SMS ou Slack configurée pour l'expiration du certificat SSL ADC ne fonctionne pas.

[NSADM-44008]

Analytics

Si le collecteur AppFlow a un nom personnalisé, la fonctionnalité d'analyse ADM peut être désactivée.

[NSADM-43723]

Novembre 12, 2019

Fonctionnalités nouvelles et améliorées

Augmentez la bande passante avec les licences de rafale

Les licences de rafale sont un programme spécial qui fournit une bande passante supplémentaire ou des licences d'instance à la capacité groupée. Pour l'abonnement CPU virtuel, il ajoute des licences CPU virtuelles. Lorsque votre limite d'abonnement de base est atteinte, vous pouvez utiliser des licences facilement disponibles sans avoir à acheter une nouvelle licence. Ces licences en rafale sont facturées en fonction de votre utilisation réelle par mois. Le programme de licence de rafale n'est disponible que pour certains clients en fonction des besoins.

Vous pouvez consulter un résumé mensuel et annuel pour suivre votre utilisation de la bande passante de la capacité mise en commun. Pour afficher l'utilisation de la licence, accédez à la page **Capacité groupée > Utilisation des licences** dans l'interface graphique Citrix ADM.

[NSADM-36649]

Afficher les mesures d'entrée et de client dans le graphique de service

Dans le graphique de service, la carte réseau est désormais affichée avec les services connectés via une entrée. Vous pouvez maintenant afficher :

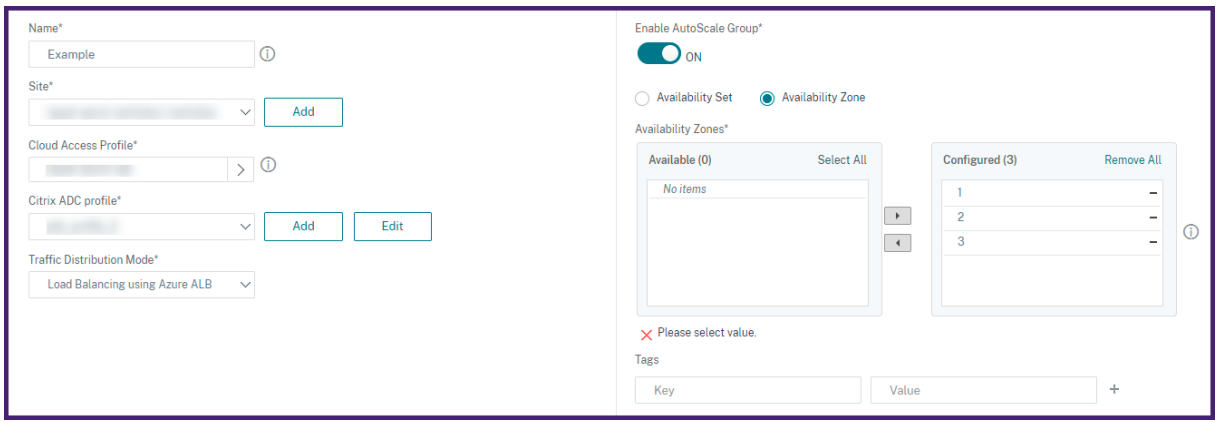
- Temps moyen pris par les instances ADC (MPX, VPX et CPX) pour traiter les demandes.
- Le client RTT pour la communication entre le client et Ingress.

Pour de plus amples informations, consultez Service Graph pour les applications cloud natives (Kubernetes)

[NSADM-41287]

Prise en charge du jeu de disponibilité Azure pour les groupes Citrix ADM Autoscale

Lorsque vous créez un groupe de mise à Autoscale sur le service Citrix ADM pour mettre à Autoscale des instances Citrix ADC VPX déployées sur le cloud Azure, vous pouvez désormais sélectionner **Jeu de disponibilité** ou **Zone de disponibilité**. Auparavant, **la zone de disponibilité** était la seule option.



Pour de plus amples informations, consultez la section Configuration.

[NSADM-42598]

Problèmes résolus

Réseaux

Lorsque vous sélectionnez un serveur virtuel, cliquez sur l'onglet **Visualizer** sous **ADM GUI > Réseaux > Fonctions réseau > Commutation de contenu**, le message d'erreur suivant s'affiche :
"Erreur : échec de l'obtention de Citrix ADC Configuration."

[NSADM-42066]

La fonction réseau GSLB prend plus de temps de traitement pour les mesures Citrix ADC. Ce problème ajoute la latence lors de la détection d'un site GSLB et ne correspond pas aux périphériques ADC dans Citrix ADM analytics. Ce problème peut se produire lorsque vous configurez plusieurs périphériques GSLB pour plusieurs locataires.

[NSADM-40997]

Orchestration

Lorsque vous modifiez un cluster Kubernetes préexistant dans le service Citrix ADM, l'erreur suivante apparaît : « Erreur en réponse » et état de la réponse « 500 ».
Avec ce correctif, ADM reconfigure le cluster Kubernetes sur l'agent avec les valeurs modifiées. De plus, l'interface graphique Citrix ADM affiche un message indiquant l'état de la reconfiguration du cluster. Voici les statuts possibles de la configuration du cluster :

- Citrix ADM a été ajouté avec succès au cluster Kubernetes.
- Le jeton ne dispose pas des privilèges requis pour configurer le cluster modifié.
- Citrix ADM n'a pas pu se connecter au cluster Kubernetes.

[NSADM-41023]

Analytics

Lorsque vous activez l'analyse, Web Insight est sélectionné par défaut dans l'interface graphique ADM.

[NSADM-40606]

17 octobre 2019

Fonctionnalités nouvelles et améliorées

Analyse de l'infrastructure améliorée avec de nouveaux indicateurs supplémentaires

Outre les indicateurs existants, vous pouvez désormais afficher les nouveaux indicateurs supplémentaires suivants dans Infrastructure Analytics afin d'enrichir les scores d'instance d'Citrix ADC :

- En-tête IP mal formé
- Mauvaises sommes de contrôle L4
- Augmentation de l'utilisation du processeur grâce au déplacement d'IP
- Direction excessive des paquets
- Supprime les paquets TCP en raison de la limite de remontage
- Boucle de couche 2
- Incompatibilité VLAN avec le tag

Pour de plus amples informations, consultez la section Analyse de l'infrastructure améliorée avec de nouveaux indicateurs.

[NSADM-39152]

Option de téléchargement de l'image de l'agent

Vous pouvez maintenant télécharger la dernière image de l'agent à partir de l'interface utilisateur ADM même lorsqu'aucun agent n'est présent dans le service ADM. Pour de plus amples informations, consultez la section Configuration des paramètres de mise à niveau de l'agent.

[NSADM-40097]

Gérer les configurations d'entrée de Kubernetes sur plusieurs clusters

Kubernetes utilise la fonction Ingress à travers laquelle le trafic client accède aux microservices d'une application. Les instances d'Citrix ADC peuvent agir en tant qu'entrée dans les applications exécutées dans un cluster Kubernetes. Les instances de Citrix ADC deviennent un équilibreur de charge et un proxy vers le trafic (Nord-Sud) entre les clients et les microservices à l'intérieur du cluster Kubernetes.

De plus, les instances mettent à jour les points de terminaison des microservices au fur et à mesure qu'ils changent dans l'environnement Kubernetes.

Vous pouvez configurer plusieurs instances ADC pour qu'elles agissent comme une entrée et affecter chaque ADC à différentes applications en fonction de la stratégie d'entrée. Spécifiez les éléments suivants pour déployer une configuration d'entrée :

- **Cluster** : cluster Kubernetes sur lequel vous souhaitez déployer une configuration Ingress. Pour ajouter un cluster Kubernetes, reportez-vous à **Orchestration > Kubernetes > Cluster**.
- **Stratégies** : les stratégies décident de l'instance ADC, du cluster et de l'espace de noms pour déployer une configuration d'entrée. Pour définir une stratégie, accédez à **Orchestration > Kubernetes > Stratégies**.
- **Configuration d'entrée** : cette configuration inclut les règles de commutation de contenu et les chemins d'URL correspondants des microservices et de leurs ports. Vous pouvez également spécifier les certificats SSL/TLS à l'aide d'un secret Kubernetes pour décharger le trafic HTTPS sur l'instance ADC.

Citrix ADM mappage automatiquement les configurations d'entrée et les instances ADC. Citrix ADM sélectionne l'instance ADC et héberge une configuration d'entrée en fonction des stratégies d'entrée spécifiées. Pour afficher l'état du déploiement d'entrée, accédez à **Orchestration > Kubernetes > Insertion**.

Pour chaque configuration d'entrée réussie, Citrix ADM génère un ConfigPack StyleBooks. Le ConfigPack représente la configuration ADC appliquée à l'instance ADC qui correspond à la configuration Ingress. Pour afficher le pack de configuration, accédez à **Applications** > **StyleBooks** > **Configurations**.

Pour de plus amples informations, consultez la section Gérer la configuration de Kubernetes Ingress dans Citrix ADM.

[NSADM-40847]

Autoriser les entités de fonction réseau à un utilisateur

En tant qu'administrateur, vous pouvez sélectionner des entités de fonction réseau spécifiques et accorder l'accès à un utilisateur. Avec cette option, vous pouvez gérer l'accès utilisateur à un niveau individuel des entités de fonction réseau. Avec cette fonctionnalité, vous pouvez attribuer dynamiquement des autorisations spécifiques à l'utilisateur ou au groupe au niveau de l'entité.

Pour autoriser les entités de fonction réseau, choisissez l'option **Sélectionner les types d'entités individuels** lors de la configuration d'un groupe. Vous pouvez autoriser les types d'entités de fonction réseau suivants dans l'interface utilisateur graphique Citrix ADM :

- Applications (serveurs virtuels)

- Service
- Groupes de services
- Serveurs

Vous pouvez ajouter des entités individuelles ou sélectionner toutes les entités sous le type d'entité requis pour accorder l'accès à un utilisateur. Pour de plus amples informations, consultez la section Configuration de groupes sur Citrix ADM.

L'option **Appliquer sur les entités liées autorise également** les entités liées au type d'entité sélectionné. Par exemple, si vous sélectionnez une application et que vous sélectionnez **Appliquer également sur les entités liées**, les entités liées à une application sont également autorisées.

Vous pouvez sélectionner les entités de fonction réseau à l'aide d'expressions régulières. Les entités sont découvertes en fonction des expressions régulières spécifiées. Lorsque vous sélectionnez l'option Autoriser les entités liées pour les entités découvertes, l'utilisateur peut accéder automatiquement aux entités liées à l'entité sélectionnée.

> **Remarque**
>
> Assurez-vous d'avoir sélectionné un seul type d'entité si vous souhaitez autoriser des entités liées.

[NSHELP-6078]

Nouveau diagramme d'audit de configuration

Le graphique **État du fichier de configuration Citrix ADC** est ajouté à la page **Audit de configuration** . Ce graphique vous indique l'état des fichiers Citrix ADC présents dans le`nsconfig` dossier. Citrix ADM enregistre et compare les modifications apportées aux fichiers dans le dossier `nsconfig` et affiche les différences.

Avec ce graphique, vous pouvez vérifier si des fichiers sont ajoutés, modifiés ou supprimés dans le `nsconfig` dossier.

Par exemple : si le fichier de licence est mis à jour sur une instance ADC, vous pouvez vérifier la date de la dernière mise à jour de ce fichier et prendre les mesures appropriées.

Vous pouvez définir une alerte pour recevoir des notifications sur l'événement d'état du fichier modifié. Sous **Config Files Diff Notification**, vous pouvez spécifier des informations d'e-mail ou de marge. Pour de plus amples informations, consultez la section Modifications de l'audit de configuration entre les instances.

[NSADM-36469]

Problèmes résolus

Réseaux

- Les `certkeys` téléchargés à partir de Citrix ADM sont endommagés.

  [NSADM-41630]

- Lorsque vous créez un groupe de mise à Autoscale dans **Réseaux** > **Groupes de mise à l'échelle automatique**, les balises HTML sont visibles dans l'onglet **Licence**.

  [NSADM-42234]

Orchestration

Lorsqu'un agent Citrix ADM est modifié ou non valide, le cluster ne peut pas être supprimé.

[NSADM-41021]

03 octobre 2019

Les agents Citrix Application Delivery Manager (ADM) sont, par défaut, automatiquement mis à niveau vers la dernière version de Citrix ADM. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour de plus amples informations, consultez la section Configuration des paramètres de mise à niveau de l'agent.

Fonctionnalités nouvelles et améliorées

Générer des rapports réseau pour les services d'équilibrage de charge

Vous pouvez désormais créer un tableau de bord de génération de rapports réseau pour les services d'équilibrage de charge. Ce tableau de bord peut afficher les rapports suivants pour les services sélectionnés :

- Connexions : pour les compteurs de connexions client et serveur.
- Débit : pour les compteurs d'octets de requête et de réponse.
- Temps du premier octet (TTFB) : temps moyen nécessaire pour envoyer un paquet de requête à un service et recevoir le premier paquet du service. Ce temps de réponse est appelé TTFB.

Pour plus d'informations sur la création d'un tableau de bord de rapports réseau, reportez-vous à la sectionRapports réseau.

[NSADM-18228]

Problème résolu

Réseaux

Lorsqu'un utilisateur RBAC se connecte à l'interface graphique ADM, un message d'erreur s'affiche si l'utilisateur a accès à un menu enfant mais non à son parent.

[NSHELP-20409]

18 septembre 2019

Les agents Citrix Application Delivery Manager (ADM) sont, par défaut, automatiquement mis à niveau vers la dernière version de Citrix ADM. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour de plus amples informations, consultez la section Configuration des paramètres de mise à niveau de l'agent.

Fonctionnalités nouvelles et améliorées

Générer automatiquement des incidents dans ServiceNow à l'aide du service Citrix ADM

Vous pouvez générer automatiquement des incidents ServiceNow pour les événements Citrix ADC, les événements de certificat SSL et les événements de licence Citrix ADM.

- **Événements Citrix ADC** : Citrix ADM peut générer les incidents ServiceNow pour un ensemble sélectionné d'événements Citrix ADC à partir d'instances Citrix ADC gérées sélectionnées.

  Pour envoyer des notifications ServiceNow pour les événements Citrix ADC à partir des instances gérées, vous devez configurer une règle d'événement et affecter l'action de règle comme **Envoyer des notifications ServiceNow**.

  Créez une règle d'événement sur le service ADM en accédant à **Réseaux** > **Événements** > **Règles**. Pour de plus amples informations, consultez la section Envoyer des notifications ServiceNow.

- **Le certificat SSL et les événements de licence ADM** : Citrix ADM peut générer les incidents ServiceNow pour l'expiration du certificat SSL et les événements d'expiration de la licence ADM.

  Pour envoyer des notifications ServiceNow pour l'expiration du certificat SSL, reportez-vous à la sectionExpiration du certificat SSL.

  Pour envoyer des notifications ServiceNow concernant l'expiration de la licence ADM, reportez-vous à la sectionExpiration de la licence Citrix ADM.

> **Important**
>
> - Cette fonctionnalité est prise en charge uniquement sur ServiceNow Cloud.
> - Assurez-vous que Citrix Cloud ITSM Adapter est configuré pour ServiceNow et intégré au

> service Citrix ADM. Consultez Intégrer Citrix ADM Service à l'instance ServiceNow.

[NSADM-23783]

Afficher les analyses pour les attaques de bot

Vous pouvez désormais afficher des informations sur les techniques de détection de bot configurées sur vos instances Citrix ADC. Accédez à **Analytics** > **Bot Insight** pour afficher les attaques de bot pour vos instances Citrix ADC. Activez **Bot Insight** pour afficher les analyses des attaques de bot.

Pour de plus amples informations, consultez la section Bot Insight.

[NSADM-36648]

Gérer le service Citrix ADM avec un compte Express

À partir de cette version, lorsque vous créez un compte de service Citrix ADM, un compte de licence Express vous est automatiquement attribué. Une licence d'essai distincte n'est plus requise. Si vous êtes déjà sur la période d'essai, votre compte est converti en compte Express après la fin de la période d'essai.

Si votre abonnement à la licence Citrix ADM et votre période de grâce se termine, votre compte est converti en compte Express.

Pour de plus amples informations, consultez la section Compte Citrix ADM Express.

[NSADM-31715]

Personnaliser les commandes d'annulation pour créer des tâches de configuration

Lorsque vous créez un travail de configuration, vous pouvez désormais spécifier les commandes d'annulation souhaitées à exécuter en cas d'échec de commande. Vous pouvez activer l'option de restauration personnalisée en accédant à **Réseaux** > **Travaux de configuration** .

[NSADM-31710]

Un conseil d'information pour la recherche avancée

Une info-bulle est ajoutée qui décrit les opérateurs et opérateurs logiques utilisés pour la recherche de messages syslog et de messages de journal d'audit. Pour afficher l'info-bulle, cliquez sur la barre de recherche sur l'interface graphique ADM, puis cliquez sur **Besoin d'aide**.

Pour de plus amples informations, consultez la section Rechercher des messages de syslog.

[NSADM-38406]

Problèmes résolus

Système de licences

- Lorsque vous modifiez le fuseau horaire dans l'utilisation des licences de local à GMT, il ne change pas l'heure personnalisée en GMT. De plus, le rapport sur l'utilisation des licences n'est pas généré.

[NSADM-17670]

Réseaux

- Lorsque vous cliquez sur **l'option Interroger maintenant** dans **Réseaux** > **Fonctions réseau**, l'interface graphique Citrix ADM se bloque pendant un certain temps et les données ne sont pas récupérables.

[NSHELP-20143]

- Citrix ADM affiche un message d'erreur « Au moins un agent est nécessaire pour que la licence fonctionne », même après la suppression de tous les fichiers et qu'aucun agent n'est ajouté.

[NSADM-38386]

Orchestration

- Dans Citrix ADM, lorsque vous ajoutez plusieurs clusters, Citrix ADM affiche uniquement 1 informations de cluster dans **Orchestration** > **Clusters** .

[NSHELP-41020]

03 septembre 2019

Les agents Citrix Application Delivery Manager (ADM) sont, par défaut, automatiquement mis à niveau vers la dernière version de Citrix ADM. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour de plus amples informations, consultez la section Configuration des paramètres de mise à niveau de l'agent.

Fonctionnalités nouvelles et améliorées

Service Graph pour les applications cloud natives (Kubernetes)

À l'aide de la fonctionnalité Service Graph dans Citrix ADM, vous pouvez :

- Assurez l'observabilité de bout en bout des performances globales de votre application.

- Identifiez les goulots d'étranglement créés par l'interdépendance des différents composants de vos applications.
- Recueillir des informations sur les dépendances des différents composants de vos applications.
- Surveillez les services au sein du cluster Kubernetes.
- Surveillez le service qui présente des problèmes.
- Vérifiez les facteurs qui contribuent aux problèmes de performance.
- Afficher la visibilité détaillée des transactions HTTP de service.
- Analysez les mesures suivantes :
  - Nombre total de visites
  - Temps de réponse du service
  - Volume de données
  - Erreurs

Pour de plus amples informations, consultez la section Service Graph pour les applications cloud natives (Kubernetes).

[NSADM-23832]

Modifier les paramètres d'instance dans Citrix ADM

Citrix ADM vous fournit les options permettant de modifier les paramètres d'instance. Ces paramètres sont applicables aux instances Citrix ADM découvertes. Pour modifier les paramètres de gestion d'instance, accédez à **Paramètres** > **Paramètres système** > **Paramètres d'instance** .

[NSADM-37277]

Problèmes résolus

Réseaux

- Dans **Réseaux** >**Fonctions réseau** > **Équilibrage de charge**, l'interface graphique graphique Citrix ADM prend plus de temps pour afficher les serveurs virtuels.

  [NSHELP-20050]

- Lors de la création du groupe Mise à l'Autoscale, l'onglet Paramètres de mise à l'Autoscale a manqué le nombre minimal d'informations sur les instances Citrix ADC. Par conséquent, Citrix ADM ne parvient pas à mettre à Autoscale les instances ADC.

  [NSADM-40501]

- Dans Citrix ADM, lorsque vous essayez de télécharger et d'installer des certificats et des fichiers de clé sur des instances de Citrix ADC découvertes par le biais d'agents, une erreur peut s'afficher.

  [NSADM-34558]

Système

- Lorsque le service Citrix ADM détecte une instance avec l'agent, la requête NITRO utilise le protocole HTTP au lieu du protocole configuré dans le profil. Cette communication NITRO se produit lors de la surveillance planifiée de l'inventaire, des statistiques ou de l'entité.

  [NSADM-39555]

- L'interface graphique Citrix ADM ne répond plus lorsque vous utilisez la navigation suivante pour activer l'analyse :

  1. Accédez à **Comptes** > **Abonnement** .
  2. Cliquez sur **Équilibrage de charge**.
  3. Cliquez sur **Activer Analytics**.

  [NSADM-40760]

Août 13, 2019

Les agents Citrix Application Delivery Manager (ADM) sont, par défaut, automatiquement mis à niveau vers la dernière version de Citrix ADM. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour de plus amples informations, consultez la section Configuration des paramètres de mise à niveau de l'agent.

Fonctionnalités nouvelles et améliorées

Consulter les licences d'ADM pour les groupes de mise à Autoscale ADM

Vous pouvez désormais utiliser les licences ADC présentes dans le service Citrix ADM pour concéder des licences aux instances Citrix ADC provisionnées pour les groupes de mise à l'Autoscale ADM.

Un nouvel onglet **Licence** est disponible dans la page **Créer un groupe AutoScale** . Cet onglet vous permet de configurer la capacité groupée, les licences VPX et les licences CPU virtuelles lors de la création du groupe Mise à l'Autoscale. Ainsi, lorsqu'une nouvelle instance est provisionnée pour le groupe Mise à l'Autoscale, le type de licence déjà configuré est automatiquement appliqué à l'instance provisionnée.

Lorsque les instances provisionnées sont détruites ou déprovisionnées, les licences appliquées sont automatiquement renvoyées à Citrix ADM.

Auparavant, vous pouvez uniquement configurer les licences Citrix ADC disponibles sur le site de vente cloud respectif lors de la création du groupe Mise à l'Autoscale. Ainsi, lorsqu'une nouvelle instance est provisionnée pour le groupe Mise à l'Autoscale, la licence est obtenue à partir de son site de vente en nuage.

Pour plus d'informations, consultez les liens suivants :

- Conditions de licence AWS
- Conditions de licence Azure

[NSADM-37694, NSADM-33422]

Migration simplifiée de la configuration des applications Citrix ADC à l'aide de StyleBooks

> **Remarque**
>
> Cette fonctionnalité est en prévisualisation

Le Générateur de configuration StyleBooks vous aide à créer un StyleBook de configuration d'application Citrix ADC à partir d'une configuration ADC existante. Cette fonctionnalité automatise également la migration de configuration d'application d'une instance Citrix ADC vers une autre instance.
Vous démarrez la migration en spécifiant l'une des sources de configuration suivantes :

- Une instance d'Citrix ADC : cette option détecte les applications actives sur l'instance d'ADC sélectionnée.
- Un ensemble de commandes CLI : cette option analyse les commandes CLI et extrait les applications à l'intérieur.

Une fois la source spécifiée, ADM découvre toutes les applications trouvées dans la source. Vous pouvez ensuite sélectionner la configuration de l'application que vous souhaitez migrer vers l'instance ADC cible. Pour de plus amples informations, consultez la section Migrer la configuration de l'application Citrix ADC.

Après la migration, un ConfigPack est créé dans Citrix ADM avec son StyleBook correspondant. Pour afficher le ConfigPack, accédez à **Applications** > **StyleBooks** > **Configurations**.

[NSADM-36438]

Mise à niveau simplifiée des instances de Citrix ADC dans le groupe Autoscale

Vous pouvez désormais mettre à niveau en toute transparence toutes les instances des services cloud qui font partie du groupe Autoscale. Pour plus d'informations, veuillez consulter la section Planifier la mise à niveau du groupe Autoscale.

> **Remarque**
>
> Pendant la mise à niveau, la mise à l'échelle automatique des instances de Citrix ADC est désactivée pour le groupe de mise à l'échelle automatique sélectionné.

Après la mise à niveau, si le groupe Autoscale provisionne une nouvelle instance, la nouvelle instance a la même version spécifiée au moment de la mise à niveau.

[NSADM-34401, NSADM-34285]

Rechercher les messages du journal d'audit Citrix ADM à l'aide de filtres

Vous pouvez désormais utiliser des filtres pour rechercher les messages du journal d'audit Citrix ADM, affiner vos résultats et trouver exactement ce que vous recherchez. Les nouvelles catégories de filtres sont la source, l'événement, la gravité et le message.

Pour rechercher les messages du journal d'audit pour toutes les applications présentes dans l'ADM, à partir de l'interface graphique ADM, accédez à **Réseaux** > **Fonctions réseau** > **Audit** .

Pour rechercher les messages du journal d'audit pour une application spécifique sur l'ADM, à partir de l'interface graphique ADM, accédez à **Application** > **Tableau de bord** et sélectionnez le serveur virtuel pour lequel vous souhaitez rechercher les messages du journal d'audit. Cliquez ensuite sur l'onglet **Journal d'audit**.

Pour de plus amples informations, consultez Afficher et exporter les messages syslog

[NSADM-38705]

Problèmes résolus

Compte

- L'option**Serveurs Syslog** n'est désormais pas disponible dans l'interface graphique Citrix ADM.

  [NSADM-39256]

Analytics

- Lorsque vous activez l'analyse, la collecte de données Geo est également activée par défaut, mais les géomaps n'étaient pas affichés dans Citrix ADM.

  [NSADM-39543]

Réseaux

- Certains serveurs virtuels sous licence deviennent sans licence après la mise à niveau. Ce problème a entraîné une perte de données analytiques.

  [NSADM-39379]

- Le nombre total de serveurs virtuels s'affichait de manière incorrecte dans le tableau de bord Fonctions réseau.

  [NSADM-39512]

- Lorsque vous configurez des rapports à l'aide de **l'option Planifier l'exportation**, les rapports reçus par courriel/slack affichent un écran vide.

  [NSADM-38974]

- Si le nombre de threads dans le sous-système d'événements dépasse 15, Citrix ADM ne parvient pas à traiter les Syslogs. Dans cette version, la limite de thread est augmentée à 20.

  [NSADM-39518]

Juillet 31, 2019

Les agents Citrix Application Delivery Manager (ADM) sont, par défaut, automatiquement mis à niveau vers Citrix ADM 13.0 build 41.12. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour de plus amples informations, consultez la section Configuration des paramètres de mise à niveau de l'agent.

Fonctionnalités nouvelles et améliorées

Analyse des transactions Web

L'analyse des transactions Web vous permet de rechercher plusieurs transactions détaillées pour afficher un code de réponse 5xx erroné. Dans la page **Synthèse des mouvements**, vous pouvez également afficher les transactions détaillées pour un temps de réponse plus lent. Cette fonctionnalité vous permet non seulement d'examiner les transactions détaillées, mais également de comprendre visuellement la mesure de temps de réponse répartie entre le client, le ADC et le serveur.

Cette fonctionnalité est intégrée au Tableau de bord des applications et vous pouvez accéder à la page Récapitulatif des transactions pour Erreur serveur - 5XX. Pour de plus amples informations, consultez la section Analyse des transactions Web pour les erreurs de serveur.

[NSADM-34701]

Deux nouveaux indicateurs pour les marqueurs

Les**événements critiques** et les **événements majeurs** sont les nouveaux indicateurs ajoutés à un marqueur. Dans **Réseaux** > **Instances**, les marqueurs sur une carte désignent les sites créés dans Citrix ADM. Maintenant, le nombre d'événements critiques et majeurs qui se sont produits sur les instances apparaît sur les marqueurs. Ces informations vous aident à évaluer rapidement les événements qui nécessitent votre attention.

Pour de plus amples informations, consultez la section Surveillance des sites distribués à l'échelle mondiale dans Citrix ADM.

[NSADM-38638]

Analytics intelligents des applications utilisant l'apprentissage automatique et des algorithmes basés sur des règles

Intelligent App Analytics vous permet d'identifier les problèmes de performances des applications à l'aide d'algorithmes basés sur des règles et d'apprentissage automatique. En utilisant ces algorithmes, en tant qu'administrateur, vous pouvez identifier plus rapidement l'analyse des causes premières des performances de l'application. Auparavant, lorsque vous double-cliquez sur une application, vous étiez en mesure d'afficher des analyses pour des composants tels que le temps de réponse, l'utilisation moyenne du processeur, l'utilisation de la mémoire, etc. Vous pouvez maintenant afficher les nouveaux indicateurs suivants :

- Anomalies de retard du serveur (utilise un algorithme d'apprentissage automatique)
- Événements de compilation de session (utilise un algorithme basé sur des règles)
- Événements de volets de service (utilise un algorithme basé sur des règles)

Pour de plus amples informations, consultez Analyse intelligente des applications

[NSADM-33674]

Analyse de l'infrastructure améliorée avec de nouveaux indicateurs

Auparavant, en utilisant Infrastructure Analytics dans Citrix ADM, vous étiez en mesure de surveiller les scores d'instance Citrix ADC en corrélant plusieurs sources de données. Vous pouvez désormais afficher de nouveaux indicateurs dans Infrastructure Analytics pour enrichir le score d'instance d'Citrix ADC. Ces nouveaux indicateurs aident également les administrateurs à analyser rapidement la cause première des problèmes.

Dans Citrix ADM, accédez à **Réseaux** > **Analyse de l'infrastructure** pour afficher les indicateurs suivants :

- Échec de l'allocation de port

- Aucune configuration d'itinéraire par défaut
- Conflit de propriété intellectuelle
- Conflit VRID
- VLAN inadéquation
- Attaque de petite fenêtre TCP
- Incompatibilité du nom du site GSLB

Pour de plus amples informations, consultez Analyse d'infrastructure

[NSADM-30188]

Problèmes résolus

Système

Si le nombre de threads dans le sous-système d'événements dépasse 15, Citrix ADM ne parvient pas à traiter les Syslogs. Dans cette version, la limite de thread est augmentée à 20.

[NSADM-39518]

16 juillet 2019

Les agents Citrix Application Delivery Manager (ADM) sont, par défaut, automatiquement mis à niveau vers Citrix ADM 13.0 build 40.24. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour de plus amples informations, consultez la section Configuration des paramètres de mise à niveau de l'agent.

Fonctionnalités nouvelles et améliorées

Option permettant d'activer ou de désactiver les tâches de planification

Vous pouvez désormais activer ou désactiver les tâches de planification telles que la sauvegarde d'instance, l'audit de configuration d'instance, les rapports réseau d'instance et les certificats SSL d'instance. Auparavant, ces tâches étaient activées par défaut, sans aucune option pour les désactiver.

Pour activer ou désactiver une tâche de planification, à partir de l'interface graphique Citrix ADM, accédez à **Paramètres, Paramètres système et Fonctionnalités configurables**.

[NSADM-36650]

Activer l'analyse dans les partitions via Logstream en mode de transport

Lorsque vous créez des partitions d'administration sur vos instances gérées, vous pouvez afficher séparément les rapports d'analyse sur Citrix ADM pour chaque partition d'administration. Citrix ADM affichait précédemment des rapports d'analyse consolidés basés sur l'adresse IP des instances et utilisait **IPFIX** comme mode de transport. Vous pouvez maintenant sélectionner **Logstream** comme mode de transport pour obtenir des rapports d'analyse pour les partitions d'administration.

> **Remarque**
>
> Pour la version Citrix ADC **antérieure à 13.0 36.27**, **IPFIX**est l'option par défaut pour le **mode de transport**. Pour Citrix ADC **ultérieur à 13.0 36.27**, vous pouvez sélectionner **Logstream**ou **IPFIX**en mode de transport

1. Accédez à **Réseaux** > **Instances** > **Citrix ADC**, puis sélectionnez le type d'instance. Par exemple, VPX.
2. Cliquez sur **Partitions**.
3. Sur la page **Partitions d'administration**, sélectionnez la partition et, dans la liste **Sélectionner une action**, sélectionnez **Configurer Analytics** .
4. Sélectionnez le serveur virtuel, puis cliquez sur **Activer Analytics**.
5. Dans la fenêtre **Activer Analytics** :
   a) Sélectionnez le type d'aperçu (Web Insight)

      > **Remarque**
      >
      > Pour Partitions, seul Web Insight est pris en charge.

   b) Sélectionnez **Logstream** comme mode de transport
   c) L'expression est true par défaut
   d) Cliquez sur **OK**.

[NSADM-30252]

Appliquer des licences de serveur virtuel et activer l'analyse dans un flux de travail unique

Le processus de licence des serveurs virtuels, puis d'activation de l'analyse sur les serveurs virtuels sous licence, a été simplifié. Auparavant, pour activer l'analyse pour n'importe quel serveur virtuel, vous devez accéder à **Réseaux** > **Instances** > **Citrix ADC**, puis sélectionner le serveur virtuel pour activer l'analyse. Si les serveurs virtuels ne sont pas sous licence pour une instance :

- Vous devez d'abord concéder une licence au serveur virtuel en accédant à **Compte** > **Abonnement**

- Ensuite, accédez à nouveau à **Réseaux** > **Instances** > **Citrix ADC** pour activer l'analyse du serveur virtuel.

Citrix ADM élimine désormais ce double processus et vous permet de concéder des licences aux serveurs virtuels et d'appliquer des analyses dans un flux de travail unique.

Pour de plus amples informations, consultez Activer les analyses

[NSADM-32893]

Prise en charge des licences de capacité groupée dans plusieurs centres de données

Vous pouvez désormais partager le pool de licences entre plusieurs centres de données. Les licences groupées ajoutées à Citrix ADM peuvent être utilisées pour allouer des licences aux instances Citrix ADC gérées.

Pour importer automatiquement des licences à partir de votre compte Citrix Cloud :

1. Accédez à **Réseaux** > **Licences**.
2. Dans l'onglet **Fichier de licence**, cliquez sur **Ajouter un fichier de licence** .
3. Sélectionnez l'option Utiliser le code d'accès de licence.
4. Cliquez sur **Obtenir les licences**.
5. Sélectionnez le produit dans la liste.
6. Cliquez sur **Download (Télécharger)**.

Pour de plus amples informations, consultez la section Configurer la capacité groupée.

[NSADM-36695]

Accorder des autorisations Enable-Disable aux utilisateurs

Vous pouvez appliquer les stratégies d'accès définies par l'utilisateur à un utilisateur, un groupe ou un rôle. Ces stratégies vous permettent de définir des autorisations utilisateur pour les fonctionnalités Citrix ADM.

Dans cette version, l'option **Enable-Disable** est ajoutée uniquement aux fonctionnalités des **fonctions réseau** qui permettent l'activation ou la désactivation de l'action. Cette autorisation vous permet également d'exécuter l'action **Interroger maintenant** .

Lorsque vous accordez l'autorisation **Enable-Disable** à un utilisateur, l'autorisation **View** est également accordée. Vous ne pouvez pas désélectionner cette option. Pour accorder l'autorisation **Enable-Disable** à une fonctionnalité, voirConfiguration des stratégies d'accès sur Citrix ADM

> **Remarque**
>
> Avant la mise à niveau, si vous avez accordé l'autorisation **Modifier** pour une fonctionnalité, les autorisations **Enable-Disable** et **View** sont également accordées. Vous ne pouvez pas désélectionner les options sélectionnées automatiquement.

[NSADM-37684, NSHELP-18635]

Prise en charge de l'ajout d'instances Citrix ADC BLX dans Citrix ADM

L'appliance Citrix ADC BLX est un progiciel léger qui s'exécute sur votre matériel serveur préféré. Vous pouvez désormais gérer les instances Citrix ADC BLX à l'aide de Citrix ADM. Pour plus d'informations, consultezAjout d'instancesetConfigurer la capacité groupée

[NSADM-29983]

Autorisation basée sur les applications simplifiée pour les utilisateurs RBAC

Dans Citrix ADM, en tant qu'administrateur, vous pouvez désormais autoriser d'autres administrateurs pour les applications requises sans nécessairement avoir à sélectionner des instances. Auparavant, vous devez sélectionner les instances, puis sélectionner les applications à partir de ces instances. Et il peut y avoir des cas où un administrateur n'est pas nécessaire de savoir quelle instance Citrix ADC l'application est hébergée. Avec cette fonctionnalité, vous pouvez sélectionner directement les applications.

Pour ajouter des applications à un groupe :

1. Accédez à **Comptes** > **Administration des utilisateurs** > **Groupes** .
2. Cliquez sur **Ajouter**.

   La page Créer un groupe système s'affiche.
3. Spécifiez les détails requis dans la page **Paramètres du groupe**, puis cliquez sur **Suivant** .
4. Dans la page **Paramètres d'autorisation**, sélectionnez l'une des options suivantes dans la liste **Choisir des applications** :
   - **Toutes les applications** : Cette option est sélectionnée par défaut. Il ajoute toutes les applications présentes dans Citrix ADM.
   - **Toutes les applications des instances sélectionnées** : Cette option apparaît uniquement si vous sélectionnez des instances dans la catégorie **Toutes les instances** . Il ajoute toutes les applications présentes sur l'instance.
   - **Applications spécifiques** : cette option vous permet d'ajouter les applications requises auxquelles les utilisateurs doivent accéder. Cliquez sur **Ajouter des applications** et sélectionnez les applications requises dans la liste.

5. Cliquez sur **Créer un groupe**.

   Pour de plus amples informations, consultez la section Configuration de groupes sur Citrix ADM.

[NSADM-37213]

Accéder à l'interface graphique de l'instance de Citrix ADC en cliquant sur le nom d'hôte

Auparavant, vous étiez en mesure d'accéder à l'interface graphique en utilisant uniquement l'adresse IP. Vous pouvez désormais accéder à une interface graphique d'instance de Citrix ADC à partir de Citrix ADM en cliquant sur le nom d'hôte ou l'adresse IP de l'instance.

Pour de plus amples informations, consultez la section Ajout d'instances.

[NSADM-37503]

Rechercher les messages du journal syslog et de l'audit à l'aide de filtres

Vous pouvez désormais utiliser des filtres pour rechercher des messages syslog et des messages de journal d'audit afin de réduire vos résultats et de trouver exactement ce que vous recherchez. Les nouvelles catégories de filtres sont instance, module, événement, gravité et message, qui sont identiques pour les messages syslog et journal d'audit.

Pour rechercher des messages syslog, à partir de l'interface graphique ADM, accédez à **Réseaux** > **Événements** > **Messages Syslog** .

Pour rechercher les messages du journal d'audit, à partir de l'interface graphique ADM, accédez à **Compte**> **Messages du journal d'audit**.

Pour plus d'informations sur la recherche, reportez-vous à la sectionAfficher et exporter les messages syslog.

[NSADM-25835]

Découverte automatique d'entités

Lorsque vous ajoutez une entité sur une instance de Citrix ADC configurée sur Citrix ADM, l'entité s'affiche automatiquement sur l'ADM dans les 10 minutes. De plus, tout changement dans l'entité est immédiatement répercuté sur le SMA.

Pour que cette fonctionnalité fonctionne, SNMP doit être activé pour l'instance ADC via ADM. Pour activer SNMP, à partir de l'interface graphique ADM, accédez à **Réseaux** > **Instances** > **Citrix ADC** . Sélectionnez l'instance, cliquez sur le menu **Sélectionner une action**, puis cliquez sur **Configurer SNMP** .

En outre, si vous configurez des serveurs virtuels en bloc sur l'instance de Citrix ADC, certains des serveurs virtuels apparaissent automatiquement dans les 10 minutes. Les autres serveurs virtuels peuvent prendre plus de temps (jusqu'à 20 minutes).

[NSADM-23622]

Nouvel onglet pour le Provisioning des instances Citrix ADC sur le cloud

Vous pouvez désormais provisionner rapidement une instance Citrix ADC VPX sur le cloud Microsoft Azure et le cloud AWS en cliquant sur **Provisionner** sur l'interface graphique Citrix ADM. Accédez à **Réseaux** > **Instances** > **Citrix ADC** pour afficher l'option Provisionnement. Auparavant, l'option de provisionnement était imbriquée dans la liste **Sélectionner une action** . Pour déprovisionner, sélectionnez l'instance et cliquez sur **Déprovisionner**.

Pour plus d'informations, consultez :

Provisionnement d'instances Citrix ADC VPX sur AWS

Provisionnement d'instances Citrix ADC VPX sur Microsoft Azure

[NSADM-38057]

Colonnes Agent et Site

Vous pouvez désormais afficher les informations sur le site et l'agent lorsque vous affichez une instance dans **Réseaux > Instances > Citrix ADC**.

[NSADM-38057]

Problèmes résolus

Réseaux

- La valeur de latence dans Citrix ADM est affichée sous la forme 0 ms et elle a été remplacée par < 1 ms.

[NSADM-38207]

- Citrix ADM a découvert des instances CPX en tant qu'instances MPX. Ce problème est maintenant résolu.

[NSADM-37725]

- `masd` échec de la commande de redémarrage sur les agents. Ce problème est maintenant résolu.

[NSADM-37447]

Paramètres

- Dans le tableau de bord Contrôle d'accès, les données de la période suivant l'expiration de l'abonnement au service Citrix ADM n'apparaissent pas. Ce problème se produit si vous avez également un abonnement pour le service de contrôle d'accès.

[NSADM-37827]

02 juillet 2019

Les agents Citrix Application Delivery Manager (ADM) sont, par défaut, automatiquement mis à niveau vers Citrix ADM 13.0 build 39.14. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour de plus amples informations, consultez la section Configuration des paramètres de mise à niveau de l'agent.

Fonctionnalités nouvelles et améliorées

Transfert d'un fichier de sauvegarde vers un système externe

Vous pouvez transférer 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 de sauvegarde sur le serveur Citrix ADM, puis effectuer l'opération de restauration.

Pour transférer un fichier de sauvegarde Citrix ADM :

1. Accédez à **Réseaux > Instances > Citrix ADC**, puis sélectionnez le type d'instance. Par exemple, VPX.
2. Sélectionnez l'instance et dans la liste **Sélectionner une action**, sélectionnez **Sauvegarde/Restaurer** .
3. Sélectionnez le fichier de sauvegarde, puis cliquez sur **Transférer**.

   La page **Transférer le fichier de sauvegarde** s'affiche. Spécifiez les paramètres suivants :

   a) **Serveur** - Adresse IP du système sur lequel vous souhaitez transférer le fichier de sauvegarde.

   b) **Nom d'utilisateur** et **mot de passe** : informations d'identification de l'utilisateur du nouveau système, dans lequel les fichiers sauvegardés sont copiés.

   c) **Port** — Numéro de port du système vers lequel les fichiers sont transférés.

   d) **Protocole de transfert** : protocole utilisé pour effectuer le transfert de fichier de sauvegarde. Vous pouvez sélectionner les protocoles SCP, SFTP ou FTP pour transférer le fichier de sauvegarde.

e) **Chemin d'accès au répertoire** : emplacement où le fichier sauvegardé est transféré sur le nouveau système.

4. Cliquez sur **OK**.

[NSADM-31702]

Changement de nom pour les types de licence

Les types de licence suivants sont renommés :

Noms de licence existants	Nouveaux noms de licence
Standard	Norme (pas de changement)
Entreprise	Avancé
Platinum	Premium

[NSADM-36694]

Mettre à jour un certificat SSL installé et créer un CSR

Vous pouvez maintenant mettre à jour un certificat SSL installé et créer une demande de signature de certificat (CSR).

- **Mettre à jour un certificat installé**

Après avoir reçu un certificat renouvelé de l'autorité de certification (CA), vous pouvez mettre à jour les certificats existants à partir de Citrix ADM, sans ouvrir de session sur chaque instance de Citrix ADC. Pour mettre à jour un certificat SSL, une clé ou les deux à partir de Citrix ADM :

1. Accédez à **Réseaux > Tableau de bord SSL**.
2. Cliquez sur l'un des graphiques pour afficher la liste des certificats SSL.
3. Dans 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 cliquer sur **Mettre à jour** dans le coin supérieur droit de la page Certificat SSL.
4. Sur la page **Mettre à jour le certificat SSL**, modifiez le certificat, la clé ou les deux, en fonction de vos besoins, puis cliquez sur **OK** .

- **Créer une CSR**

Une demande de signature de certificat (CSR) est un bloc de texte chiffré généré sur le serveur sur lequel le certificat est utilisé. Il contient des informations 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. 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 une 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 :
   a) **Charger une clé** - Pour charger votre fichier de clé, sélectionnez Local (votre machine locale) ou Appliance (le fichier de clé doit être présent sur l'instance virtuelle Citrix ADM).
   b) **Créer une clé** - Spécifiez les paramètres suivants :

Algorithme de chiffrement	Type de clé (par exemple, RSA)
Nom du fichier de clé	Nom du fichier dans lequel la clé RSA est stockée.
Taille de la clé	Taille de la clé en bits.
Valeur de l'exposant public	Choisissez 3 ou F4 dans la liste fournie. Cette valeur fait partie de l'algorithme de chiffrement requis pour créer votre clé RSA.
Format de clé	Le PEM par défaut est sélectionné. PEM est le format de clé recommandé pour votre certificat SSL.
Algorithme de codage PEM	Dans la liste, sélectionnez l'algorithme (DES ou DES3) que vous souhaitez utiliser pour chiffrer la clé RSA générée. Si vous sélectionnez cet algorithme, vous devez fournir une phrase secrète PEM.
Phrase de passe PEM	Si vous avez choisi l'algorithme d'encodage PEM, entrez une phrase secrète.
Confirmer la phrase secrète PEM	Confirmez votre phrase secrète PEM.

5. Cliquez sur **Continue**.
6. Sur la page suivante, fournissez plus de détails. 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. Vous obtenez un certificat valide de CA à l'adresse e-mail que vous avez soumise le CSR.

[NSADM-37278]

Nouvelles informations dans Citrix ADM Analytics

Vous pouvez désormais afficher les informations suivantes sous Analytics dans Citrix ADM :

- Video Insight
- TCP Insight
- WAN Insight
- Analyse de proxy de transfert SSL

[NSADM-36692]

Provisionner les instances de Citrix ADC en mode haute disponibilité sur AWS et Azure

À présent, vous provisionnez des instances Citrix ADC en mode haute disponibilité sur les clouds AWS et Microsoft Azure, à l'aide de Citrix ADM.
Pour déployer, procédez comme suit :

1. Accédez à **Réseaux > Instances > Citrix ADC**.
2. Dans **VPX**, cliquez sur **Sélectionner une action**et sélectionnez **Provisionner dans Public Cloud**.
3. Dans la page **Provisionner Citrix ADC VPX**, sélectionnez le service cloud dans lequel vous souhaitez provisionner les instances Citrix ADC VPX.
4. Dans **Paramètres de base**, sélectionnez **HA**dans la liste **Type d'instance**.
5. Sélectionnez le **type de zone** parmi les options suivantes :
   - **Zone unique** : Cette option déploie les instances Citrix ADC VPX dans la même zone.
   - **Multizone** : cette option déploie les instances Citrix ADC VPX sur plusieurs zones. Assurez-vous de spécifier les détails du réseau dans **Paramètres du nuage** pour chaque zone créée sur votre nuage.

Pour plus d'informations, veuillez consulter Provisionner Citrix ADC VPX sur AWS et Provisionner Citrix ADC VPX sur Microsoft Azure.

[NSADM-31108, NSADM-30099]

Nouveaux champs facultatifs pour afficher les instances de Citrix ADC à partir de Citrix ADM

Les nouveaux champs facultatifs suivants sont ajoutés pour afficher les instances de Citrix ADC à partir de Citrix ADM. Pour sélectionner ces champs, accédez à **Citrix ADM GUI > Réseaux > Instances > Citrix ADC**, puis cliquez sur l'icône Paramètres.

- État du maître HA
- État de synchronisation de la haute disponibilité
- Profil administrateur
- Santé
- Temps d'activité
- ID du modèle
- Moteurs de paquets
- Cartes SSL
- UC
- Version matérielle
- Version LOM
- ID d'hôte
- Numéro de série
- Numéro de série codé
- UUID

Voici un exemple où l'icône des paramètres et les nouveaux champs sont mis en surbrillance.

[NSHELP-6170]

Problèmes résolus

Réseaux

- Lorsque vous tentez de mettre à niveau une instance Citrix ADC SDX via Citrix ADM, la mise à niveau échoue et le message d'erreur suivant s'affiche :


```
"SCP: Unable to open a session on <IP address of the SDX instance>.
Agent id not found"
```

[NSHELP-19767]

- Si vous créez plusieurs groupes de mise à Autoscale dans la même région, le déploiement de l'application pour ces groupes de mise Autoscale peut échouer. Ce problème se produit lorsque vous sélectionnez ALB comme mode de distribution du trafic pour ces groupes de Autoscale.

  [NSLB-4934]

Système

- Lorsqu'un super administrateur Citrix ADM invite d'autres utilisateurs de Citrix Cloud, l'autorisation par défaut pour les utilisateurs invités est admin, à l'exception de l'administration des utilisateurs. (Pour afficher l'administration des utilisateurs, accédez à l' **interface graphique Citrix ADM > Systèmes > Administration des utilisateurs**.) Auparavant, l'autorisation par défaut était en lecture seule. Pour de plus amples informations, consultez la section Configuration du contrôle d'accès basé sur les rôles.

  [NSADM-37914]

19 juin 2019

Les agents Citrix Application Delivery Manager (ADM) sont, par défaut, automatiquement mis à niveau vers Citrix ADM 13.0 build 38.20. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour de plus amples informations, consultez la section Configuration des paramètres de mise à niveau de l'agent.

Fonctionnalités nouvelles et améliorées

Onglet Groupes de services GSLB

L'interface utilisateur graphique Citrix ADM affiche désormais l'onglet **Groupes de services** sous **Réseaux** > **Fonctions réseau** > **GSLB** .
Sous cet onglet, vous pouvez voir tous les groupes de services pour les instances découvertes sur l'ADM. À l'aide **de l'onglet Groupes de services**, vous pouvez effectuer des tâches telles que l'activation et la désactivation d'une entité de groupe de services et la vérification des membres et des serveurs virtuels liés à cette entité. En outre, vous pouvez interroger l'entité pour obtenir son dernier statut.

31 mai 2019

Les agents Citrix Application Delivery Manager (ADM) sont, par défaut, automatiquement mis à niveau vers Citrix ADM 13.0 build 37.26. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour de plus amples informations, consultez la section Configuration des paramètres de mise à niveau de l'agent.

Fonctionnalités nouvelles et améliorées

Analyse de l'infrastructure — panneau Récapitulatif

Vous pouvez maintenant afficher les statistiques d'instance Citrix ADC pour la **configuration SSL** et la **déviation de configuration** dans le panneau **Résumé** .

- **Configuration SSL** — Permet d'afficher les instances sur lesquelles des certificats SSL sont installés avec :
  - **Émetteur : Non recommandé** - Citrix ne recommande pas l'émetteur du certificat SSL.
  - **Algorithme : Non recommandé** - Les algorithmes de signature des certificats SSL installés sur l'instance ADC ne répondent pas aux normes Citrix.
  - **Force clé : Non recommandé** - La force clé des certificats SSL ne répond pas aux normes Citrix.
- **Déviation de configuration** — Permet d'afficher la liste des instances qui ont les écarts de configuration pour :
  - **Saved vs Running** - La différence entre la configuration enregistrée sur l'instance et la configuration en cours d'exécution sur la même instance.
  - **Running vs Template** - Le modèle vs Running inclut tous les modèles autres que **Saved vs Running** .

[NSADM-24161]

Notification de règle de signature dans Citrix ADM

Menace basée sur la signature indique la détection des menaces connues en fonction de la signature assignée. Chaque fois que vous ajoutez un objet signature à Citrix ADC Web AppFirewall, Citrix ADM envoie des notifications par courrier électronique, slack, PagerDuty, message d'événement et informations de sécurité. Pour de plus amples informations, consultez la section signatures.

Lorsque vous créez une règle d'événement dans Citrix ADM, vous pouvez maintenant afficher une nouvelle catégorie appelée **AppFWNewSignatuReadded**. Pour activer les notifications pour les nouveaux objets de signature ajoutés à Citrix ADC Web AppFirewall, créez une règle d'événement :

1. Accédez à **Réseaux** > **Événements** > **Règles**, puis cliquez sur **Ajouter** .
2. Dans le panneau **Catégorie**, tapez`signature` dans la barre de recherche, puis sélectionnez **AppFWNewSignatuReadded** .
3. Pour créer une règle d'événement, reportez-vous à la sectionCréer des règles d'événement.

Après avoir créé la règle d'événement, vous recevez des notifications basées sur l'action de règle d'événement configurée. Pour afficher les notifications :

- Accédez à **Réseaux** > **Événements** > **Message d'événement** .
- Accédez à **Analytics** > **Security Insight**, puis sélectionnez l'instance pour laquelle vous souhaitez afficher les notifications de signature.

  Les notifications de signature sont répertoriées sous l'onglet **Historique des événements** .

[NSADM-34153]

Prise en charge de l'ajout d'étiquettes à StyleBooks

Vous pouvez maintenant ajouter des étiquettes à n'importe quel StyleBook dans Citrix ADM. Les étiquettes sont des paires clé-valeur qui vous permettent de regrouper StyleBooks à l'aide de critères différents. Vous pouvez utiliser ces étiquettes lors de la recherche ou du filtrage de StyleBooks dans Citrix ADM. Pour de plus amples informations, consultez Créer une étiquette pour le StyleBook

[NSADM-34877]

La mise à l'échelle automatique Citrix ADM dans Microsoft Azure prend en charge l'équilibrage de charge Azure pour la distribution du trafic

La mise à l'échelle automatique des instances de Citrix ADC dans Microsoft Azure prend en charge deux modes de distribution du trafic :

- via le gestionnaire de trafic Azure
- via l'équilibreur de charge Azure

Pour de plus amples informations, consultez Mise à l'échelle automatique de Citrix ADC VPX dans Microsoft Azure à l'aide de Citrix ADM

[NSADM-33423]

Problèmes résolus

Réseaux

- Lorsque vous essayez d'exécuter un travail de configuration abandonné, vous pouvez voir une erreur « Demande non valide ».

  [NSADM-34242]

- Lorsque vous sélectionnez l'option **Attacher un site** dans la page **Ajouter des agents**, Citrix ADM ne met pas à jour le site de l'instance qui appartient à ce site ou à cet agent.

  [NSADM-35049]

- Lors de la création ou de la configuration d'un groupe d'instances, l'interface utilisateur graphique Citrix ADM peut afficher deux fois les adresses IP des instances Citrix ADC haute disponibilité. La sélection d'une adresse IP permet d'ajouter les deux instances au groupe d'instances.

  Ce correctif s'applique à la création d'un groupe d'instances après la mise à niveau. Pour les groupes créés précédemment, vous devez supprimer les entrées dupliquées du groupe

  [NSHELP-19176]

Paramètres

Lorsque l'agent Citrix ADM ne reçoit pas la valeur de temps correcte du serveur d'applications, les informations n'apparaissent pas dans Citrix ADM.

[NSHELP-18898]

avril 25, 2019

Les agents Citrix Application Delivery Manager (ADM) sont, par défaut, automatiquement mis à niveau vers Citrix ADM 13.0 build 36.21. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour de plus amples informations, consultez la section Configuration des paramètres de mise à niveau de l'agent.

Fonctionnalités nouvelles et améliorées

Possibilité de définir la page de destination par défaut

Dans le portail Citrix Application Delivery Management (ADM), vous pouvez définir votre page préférée comme page de destination par défaut. Cliquez sur l'icône de signet dans l'onglet que vous souhaitez définir comme page de destination par défaut.

Voici un exemple pour définir le tableau de bord SSL comme page de destination par défaut :

[NSADM-21938]

Générer un fichier de support technique pour l'agent Citrix ADM

Vous pouvez générer un fichier de support technique pour un agent Citrix ADM sélectionné, à partir de l'interface graphique. En outre, vous pouvez télécharger ce fichier et l'envoyer au support technique Citrix pour enquête et dépannage.

[NSADM-30238]

Améliorations du tableau de bord de l'analyse de l'infrastructure

Le tableau de bord de l'analyse de l'infrastructure a été mis à jour pour incorporer les modifications thématiques et les colonnes des tableaux sont redimensionnées pour une meilleure lisibilité. Vous pouvez maintenant cliquer sur le nom d'hôte pour accéder à l'instance dans le tableau de bord instancié. Il existe également quelques mises à jour mineures dans l'interface utilisateur qui améliorent l'expérience utilisateur de l'utilisation du tableau de bord Analyse de l'infrastructure.

[NSADM-30191]

Problèmes résolus

Analytics

- Dans **HDX Insight** > **Utilisateurs**, une adresse IP du client différente est affichée dans la session sélectionnée dans le tableau Sessions en cours que l'adresse IP affichée dans le tableau Sessions en cours.

  [NSHELP-6395, TSK0715071]

Applications

- L'interface graphique Citrix ADM ne répond plus lors de l'activation d'AppFlow pour plusieurs serveurs virtuels dans certains cas spécifiques. Ce problème se produit généralement lorsque vous sélectionnez plusieurs types de serveurs d'équilibrage de charge qui incluent TCP et si TCP est au début de la liste.

  Solution : effectuez un tri sur la colonne « Type de service » dans un ordre croissant. Par conséquent, les types TCP se déplacent vers le bas de la liste, puis activez AppFlow.

  [NSADM-35039]

- Actuellement, les e-mails envoyés par Citrix ADM ne contiennent pas les valeurs de seuil dépassées.

  [NSHELP-6093]

Réseaux

- Lorsque vous recherchez des modèles de configuration à l'aide des critères de recherche Type, Citrix ADM affiche True ou False. Notez que « True = modèles de configuration par défaut » et « False = modèles de configuration personnalisés ». Vous devez choisir en conséquence.

  [NSADM-34802]

- Lorsque vous créez une règle d'événement avec Supprimer l'action, pour les instances découvertes par l'intermédiaire d'agents, les événements sont supprimés même après l'expiration de l'heure planifiée.

  [NSADM-35023]

- Le profil Slack n'est pas visible dans le module Config Job lors de l'envoi du rapport au canal Slack.

  [NSADM-35079]

- Lorsque vous supprimez un Citrix ADC VPX qui a des partitions de Citrix SDX, le VPX ADC est supprimé de Citrix ADM mais les partitions sont toujours conservées.

  [NSADM-34829]

avril 04, 2019

Les agents Citrix Application Delivery Manager (ADM) sont, par défaut, automatiquement mis à niveau vers Citrix ADM 13.0 build 35.17. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour de plus amples informations, consultez la section Configuration des paramètres de mise à niveau de l'agent.

Fonctionnalités nouvelles et améliorées

Amélioration de l'interface utilisateur lors de l'abandon d'une tâche de configuration

L'option d'abandon a maintenant été supprimée pour l'action Ignorer erreur et Continuer. Vous ne pouvez pas abandonner les travaux de configuration en cours d'exécution si vous sélectionnez l'option **Ignorer l'erreur et continuer** pour le mode d'exécution d'échec de commande.

[NSADM-32836]

Possibilité d'afficher le type de tri dans les colonnes dans les tables Citrix ADM

Dans la vue par défaut Citrix ADM, bien que vous puissiez trier les colonnes dans l'ordre requis, les en-têtes de colonne disposent désormais d'un indicateur indiquant si les enregistrements sont or-

ganisés dans l'ordre croissant ou décroissant. Cette modification est appliquée aux pages Citrix ADM appropriées.

[NSADM-21463]

Changement de thème dans l'interface graphique Citrix ADM

L'interface graphique Citrix ADM a maintenant été mise à jour avec des changements de thème dans quelques-unes des pages. Vous remarquerez peut-être que les fenêtres de confirmation et d'erreur s'affichent désormais avec un nouveau thème de couleur et un ensemble de nouvelles polices.

[NSADM-22535]

Problèmes résolus

Analytics

- Lorsque vous accédez à **Utilisateurs** > **Transactions**, il se peut que le rapport des transactions ne s'affiche pas pour plus de 0,1 million de transactions.

  [NSHELP-18785]

- Lorsque Citrix ADM gère deux passerelles Citrix ADC portant le même nom, Citrix ADM ne parvient pas à différencier les sessions appartenant à ces passerelles Citrix ADC.

  [NSHELP-18716]

- Le tableau de bord de l'application n'affiche pas les mesures appropriées dans le panneau récapitulatif de l'application pour les applications configurées sur la paire Citrix ADC haute disponibilité.

  [NSHELP-18733]

- Dans le Tableau de bord de l'application, certains caractères tels que Volume de données ne s'affichent pas correctement lorsque la longueur de la chaîne est longue.

  [NSADM-31818]

- Le tableau de bord de l'application n'affiche pas les données correctes, car les informations sur l'UC et la mémoire du nœud ne sont pas ajoutées à tous les serveurs virtuels.

  [NSHELP-18736]

- AppFlow n'est pas pris en charge sur le serveur virtuel de redirection de cache. Par conséquent, l'option « Activer AppFlow » est supprimée pour le serveur virtuel CR dans Citrix ADM.

  [NSHELP-18817]

Système de licences

- Citrix ADM ne lit pas la configuration du port de licence lorsqu'il est configuré en tant que serveur de licences.

  [NSADM-33966]

Système

- Dans la vue par défaut, lorsque vous triez les colonnes dans l'ordre requis, la colonne ne possédait pas l'indicateur pour indiquer si le tri est dans l'ordre croissant ou décroissant. Maintenant, des indicateurs sont fournis pour indiquer si les enregistrements sont organisés par ordre croissant ou décroissant. Cette modification est appliquée aux pages Citrix ADM appropriées.

  [NSHELP-18647]

01 avril 2019

Les agents Citrix Application Delivery Manager (ADM) sont, par défaut, automatiquement mis à niveau vers Citrix ADM 13.0 build 34.25. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour de plus amples informations, consultez la section Configuration des paramètres de mise à niveau de l'agent.

Fonctionnalités nouvelles et améliorées

Prise en charge de la génération de rapports réseau pour les instances Citrix SDX dans ADM

Citrix ADM vous permet de générer des rapports non seulement pour les instances au niveau global, mais aussi pour les entités telles que les serveurs virtuels et les interfaces réseau. La famille d'instances comprend désormais des instances Citrix ADC, Citrix SDX et Citrix SD-WAN.

[NSADM-25092]

Prise en charge de la création de packs de configuration à l'aide de StyleBooks sans sélectionner d'instances

Citrix ADM vous permet de créer des packs de configuration à l'aide des StyleBooks sans sélectionner les instances. Vous pouvez ensuite mettre à jour le pack de configuration en sélectionnant les instances cibles sur lesquelles vous souhaitez déployer la configuration. La fonctionnalité vous permet de créer des packs de configuration pour vos applications, même si vous n'êtes pas en mesure d'accéder aux instances.

[NSADM-25552]

Citrix ADM Autoscaling dans Microsoft Azure prend en charge uniquement le trafic DNS à l'aide du gestionnaire de trafic Azure

> **Remarque**
>
> Cette fonctionnalité est actuellement en prévisualisation.

La mise à l'échelle automatique Citrix ADM ajoute ou supprime des nœuds de cluster Citrix ADC dans Azure en fonction de l'utilisation réelle des ressources réseau. Citrix ADM collecte des statistiques (utilisation du processeur, utilisation de la mémoire et débit) à partir des clusters provisionnés à l'Autoscale. Ces statistiques sont évaluées par rapport à la valeur de seuil configurée par le client. La mise à l'échelle ou la mise à l'échelle est déclenchée selon que les statistiques dépassent le seuil maximal ou fonctionnent en dessous du seuil minimal.

Les avantages des fonctions de mise à l'échelle automatique sont les suivants :

- Garantit que l'application est opérationnelle tout le temps, quelles que soient les exigences du trafic.
- Les instances de Citrix ADC sont ajoutées et supprimées dynamiquement pour une configuration manuelle sans contact.
- La gestion DNS est automatique.
- Permet une meilleure gestion des coûts.

La mise à l'échelle automatique dans Microsoft Azure prend en charge uniquement le trafic DNS à l'aide du gestionnaire de trafic Azure.

> **Remarque**
>
> Actuellement, la distribution du trafic utilisant ALB n'est pas prise en charge.

Pour utiliser la fonctionnalité Mise à l'Autoscale, vous devez créer des groupes de Autoscale et déployer l'application à l'aide de StyleBooks. Cette version prend en charge la mise à l'échelle automatique des applications dans le jeu d'échelle de machine virtuelle Microsoft Azure. Pour plus d'informations, voir Configurer une application pour le groupe Mise à l'Autoscale.

[NSADM-31259]

Amélioration de l'interface utilisateur Citrix ADM

Cette version améliore l'expérience de l'interface utilisateur dans le portail Citrix ADM. Voici les faits saillants de ces modifications d'interface utilisateur :

Les versions LOM sont applicables uniquement aux appliances Citrix ADC SDX. Par conséquent, dans la page Instances Dashboard, les versions de LOM sont affichées uniquement pour les appliances Citrix ADC SDX.

Le bouton **Supprimer les filtres** est fourni dans la page Messages Syslog. Auparavant, cette option était présente sous Syslog Messages dans la navigation de gauche.

[MSADM- 32322]

Amélioration de l'interface graphique pour afficher les données en fonction de la durée du temps

Vous pouvez désormais utiliser la liste des intervalles de temps et sélectionner la durée pour afficher les détails des analyses d'applications et des rapports d'événements.

[NSADM-22529]

Prise en charge de PagerDuty dans Citrix ADM

Auparavant, dans l'interface graphique Citrix ADM, vous pouvez envoyer des notifications par courrier électronique, SMS et Slack. Vous pouvez désormais envoyer des notifications à PagerDuty en fonction de vos configurations que vous avez effectuées dans PagerDuty. PagerDuty vous permet de configurer des notifications telles que e-mail, SMS, notification push et appel téléphonique sur le numéro enregistré.

Vous pouvez sélectionner votre profil PagerDuty comme l'une des options pour obtenir des notifications pour les fonctionnalités suivantes :

- Events : liste des événements générés pour les instances Citrix ADC.
- Licences : liste des licences actuellement actives, sur le point d'expirer, etc.
- Certificats SSL — Liste des certificats SSL actuellement actifs, sur le point d'expirer, etc.

Avant d'ajouter un profil PagerDuty dans Citrix ADM, vérifiez que vous avez terminé les configurations requises dans PagerDuty. Pour de plus amples informations, consultez la section Documentation PagerDuty.

[NSADM-25940]

Problèmes résolus

Analytics

- Lorsque vous activez AppFlow pour les serveurs virtuels de redirection de cache, vous pouvez voir un message d'erreur et vous ne pouvez peut-être pas activer AppFlow pour ce serveur virtuel.

  [NSHELP-18817]

Applications

- Sur le panneau d'informations du tableau de bord de l'application et les pages détaillées du tableau de bord de l'application, les données sous le titre « Transactions » affichaient différemment. Il s'agissait de données cumulatives sur un endroit et de taux de transaction à l'autre endroit. Avec ce correctif, les données sont désormais affichées correctement en tant que transactions totales et la section Tendances des mesures clés affiche les transactions par seconde.

  [NSHELP-18799]

Réseaux

- Vous pouvez voir des échecs dans l'enregistrement CPX dans Citrix ADM, car l'agent de service ADM n'autorise pas la demande d'enregistrement automatique CPX.

  [NSADM-33020]

- Lorsque vous devez mettre à jour un certificat SSL existant, accédez à **Réseaux** > Tableau de **bord SSL** . Le tableau de bord SSL affiche les détails des certificats SSL Citrix ADC, des serveurs virtuels SSL et des protocoles SSL. Cliquez sur l'un des liens « total » des certificats pour afficher les détails relatifs aux certificats SSL, aux serveurs virtuels SSL ou aux protocoles SSL. Maintenant, lorsque vous sélectionnez un certificat et que vous cliquez sur **Mettre à jour**, vous n'avez pas besoin de spécifier le format du certificat que vous mettez à jour. Citrix ADM peut désormais dériver le format à partir des fichiers de certificat précédemment téléchargés.

  [NSHELP-18763]

Système

- Lorsque vous accédez à **Système** > **Événements** et sélectionnez un événement et cliquez sur **Historique**, l' **Historique des événements** affiche l'écran principal Événements et non l'historique attendu pour cet événement. Vous devez fermer la page Historique des événements et répéter la sélection pour afficher l'historique correct de cet événement. Ce problème est maintenant résolu.

  [NSHELP-18651]

- Vous n'avez pas pu effectuer une recherche dans les tables Citrix ADM à l'aide de caractères spéciaux. ADM vous permet maintenant de rechercher en utilisant des caractères spéciaux comme, $, &, ou '.

  [NSHELP-5927]

28 février 2019

Les agents Citrix Application Delivery Manager (ADM) sont, par défaut, automatiquement mis à niveau vers Citrix ADM 13.0 build 33.23. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** >

Agents. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour de plus amples informations, consultez la section Configuration des paramètres de mise à niveau de l'agent.

Fonctionnalités nouvelles et améliorées

Prise en charge de la mise à l'échelle automatique des instances Citrix ADC déployées dans Microsoft Azure

> **Remarque**
>
> Cette fonctionnalité est en prévisualisation.

La fonctionnalité de mise à l'échelle automatique Citrix ADM prend désormais en charge la mise à l'échelle des instances de Citrix ADC dans Microsoft Azure. La fonctionnalité de mise à l'échelle automatique Citrix ADM ajoute ou supprime les nœuds de cluster Citrix ADC déployés dans Azure en fonction de l'utilisation réelle des ressources réseau. Citrix ADM collecte des statistiques (utilisation du processeur, utilisation de la mémoire et débit) à partir des clusters provisionnés à l'Autoscale. Ces statistiques sont évaluées par rapport à la valeur de seuil configurée par le client. Selon que les statistiques dépassent le seuil maximal ou fonctionnent en dessous du seuil minimum, l'échelle d'entrée ou d'extension est déclenchée respectivement.

Les avantages des fonctions de mise à l'échelle automatique sont les suivants :

- Garantit que l'application est opérationnelle tout le temps, quelles que soient les exigences du trafic.
- Les instances de Citrix ADC sont ajoutées et supprimées dynamiquement pour une configuration manuelle sans contact.
- La gestion DNS est automatique.
- Permet une meilleure gestion des coûts.

La mise à l'échelle automatique dans Microsoft prend en charge deux modes de distribution du trafic :

- via le gestionnaire de trafic Azure
- via l'équilibreur de charge Azure

Pour utiliser la fonctionnalité Mise à l'Autoscale, vous devez créer des groupes de Autoscale et déployer l'application à l'aide de StyleBooks.

> **Remarque La**
>
> mise à l'Autoscale du back-end n'est pas prise en charge dans cette version de Citrix ADM.

[NSADM-24780]

Prise en charge de l'affichage de l'activation des analyses sur la page des serveurs virtuels de licences

Citrix ADM affiche désormais la liste des serveurs virtuels sur lesquels l'analyse est activée. Accédez à **Réseaux** > **Licences** et, dans la section Serveurs virtuels sous licence, cliquez sur le bouton pour sélectionner les serveurs virtuels à octroyer des licences. Sélectionnez l'un des types de serveurs virtuels et sélectionnez l'onglet **Licence** . La colonne **Logging AppFlow** affiche les analyses activées sur les serveurs virtuels.

[NSADM-25857]

Affichage consolidé de tous les serveurs virtuels sur la page des licences des serveurs virtuels

Citrix ADM affiche désormais une vue consolidée de tous les serveurs virtuels du réseau. Vous pouvez désormais accéder à **Réseaux** > **Licences** et, dans la section Serveurs virtuels sous licence, cliquez sur le bouton pour sélectionner les serveurs virtuels à octroyer des licences. La page **Licence des serveurs virtuels** affiche un onglet, **Tous les serveurs virtuels**, qui répertorie tous les serveurs virtuels indépendamment du fait qu'ils sont l'équilibrage de charge, le changement de contenu ou tout autre type de serveurs virtuels. Vous pouvez sélectionner les serveurs virtuels requis et leur appliquer des licences.

[NSADM-25194]

Prise en charge de l'affichage des détails d'une instance à partir de la page d'analyse de l'infrastructure

La fonctionnalité Analyse de l'infrastructure dans Citrix ADM vous aide à visualiser les facteurs qui ont entraîné ou pourraient entraîner un problème sur les instances. Vous pouvez maintenant cliquer sur l'adresse IP de l'instance dans la vue tabulaire pour afficher plus de détails sur cette instance en tant qu'affichage du tableau de bord. Le tableau de bord de l'instance présente une vue d'ensemble de l'instance dans laquelle vous pouvez voir le processeur, la mémoire et l'utilisation du disque de l'instance. Vous pouvez également voir les détails relatifs à la gestion des certificats SSL, à l'audit de configuration, aux fonctions réseau et à un rapport réseau qui indique l'utilisation réseau détaillée de l'instance.

[NSADM-30194]

Problèmes résolus

Analytics

- Lors de la configuration de l'analyse sur une instance ADC, lorsque vous recherchez les détails du serveur virtuel, puis annulez la recherche, ADM peut également répertorier les serveurs virtuels d'autres instances ADC.

  [NSHELP-18623]

- Si vous êtes un utilisateur disposant d'autorisations « lecture seule », vous ne pouvez pas voir les icônes associées au diagnostic dans aucune des pages analytiques.

  [NSHELP-6407]

- Lorsque vous configurez AppFlow pour l'instance WO SD-WAN dans Citrix ADM, l'adresse IP de l'agent de service n'est pas configurée comme adresse IP du collecteur. Avec ce correctif, l'agent est configuré pour recevoir les données AppFlow à partir des instances WO SD-WAN.

  [NSADM-32565]

Hybride et multi-cloud

- **AWS Autoscale** : vous pouvez utiliser l'image Citrix ADC version 12.1 build 51.16 pour créer des groupes de mise Autoscale.

Réseaux

- Dans **Réseaux** > **Audit de configuration**, il peut y avoir une situation lorsque vous cliquez sur les instances dans la section « 10 premières instances par modification de configuration », ADM peut ne pas afficher de données pour cette instance. En outre, lorsque vous sélectionnez une période particulière, par exemple, « quotidiennement », puis sélectionnez une instance dans la section « 10 premières instances par modification de configuration », ADM peut afficher des données pour une période différente.

  [NSHELP-18452]

- Considérez un scénario lorsque vous accédez à **Réseaux** > **Audit de configuration** . Dans la section « Top 10 instances par modification de configuration », lorsque vous placez votre souris sur ADC, l'infobulle peut ne pas afficher les informations complètes sur ADC. Cela est dû à la limitation du nombre de caractères que l'info-bulle peut afficher.

  [NSHELP-18470]

- Citrix ADM ne parvient pas à traiter les paquets SNMPv3 reçus de l'instance ADC par intermittence. Cet échec peut se produire après la mise à niveau de l'instance de Citrix ADC ou de Citrix ADM lui-même, ou le redémarrage de l'instance ADC. De tels échecs peuvent se produire parce que la mémoire non valide (mémoire libérée) est utilisée pour une autre allocation de mémoire.

  [NSHELP-5880]

Système

- Ce problème est remarqué après la mise à niveau vers Citrix ADM version 12.1 build 50.28. Considérez que vous accédez à **Système** > **Administration des utilisateurs** > **Groupe** et créez un

groupe d'utilisateurs. Là, vous désélectionnez d'abord toutes les options de l'onglet **Autorisation**, puis sélectionnez manuellement quelques instances et terminez la création du groupe. Lorsque vous modifiez ultérieurement le même groupe et que vous sélectionnez l'onglet **Autorisation**, les instances ne sont plus affichées.

[NSHELP-18442]

- Vous pouvez remarquer que vous n'êtes pas en mesure d'ajouter des serveurs virtuels GSLB dans des groupes d'utilisateurs dans les deux scénarios suivants :

  1. Lors de la création d'un groupe : Lorsque vous essayez d'ajouter quelques serveurs virtuels GSLB supplémentaires à une liste existante de serveurs virtuels GSLB.
  2. Lors de la modification d'un groupe existant : lorsque vous essayez d'ajouter des serveurs GSLB à un groupe existant qui a déjà une liste de serveurs virtuels GSLB.

  [NSHELP-18152]

08 février 2019

Les agents Citrix Application Delivery Manager (ADM) sont, par défaut, automatiquement mis à niveau vers Citrix ADM 13.0 build 32.32. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour de plus amples informations, consultez la section Configuration des paramètres de mise à niveau de l'agent.

Cette version est une amélioration de la version 32.30 de Citrix ADM 13.0. Diverses améliorations, y compris la plateforme et l'analyse, ont été apportées dans cette version pour améliorer encore les performances de Citrix ADM.

28 janvier 2019

Les agents Citrix Application Delivery Manager (ADM) sont, par défaut, automatiquement mis à niveau vers Citrix ADM 13.0 build 32.30. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour de plus amples informations, consultez la section Configuration des paramètres de mise à niveau de l'agent.

Fonctionnalités nouvelles et améliorées

Prise en charge de la visualisation de tous les nœuds actifs sur le tableau de bord

Citrix ADM prend désormais en charge l'affichage de tous les nœuds actifs pour un cluster créé sur AWS. Vous pouvez afficher le nombre de nœuds actifs qui font partie de la zone de disponibilité à tout

moment. Pour de plus amples informations, consultez la section Tableau de bord de mise à l'échelle automatique.

[NSADM-25785]

Prise en charge de l'exportation du tableau de bord Network Reporting

Vous pouvez planifier une exportation périodique de la page du tableau de bord Network Reporting. Par exemple, vous pouvez définir une option pour générer un rapport de tableau de bord chaque semaine pendant l'heure précédente. Le rapport a été généré chaque semaine pour l'heure et la date définies par l'utilisateur et non basé sur le tableau de bord actuel. Avec la nouvelle amélioration, le rapport remplace l'horodatage et l'heure définies et affiche l'état du tableau de bord. Pour de plus amples informations, consultez la section Exportation de rapports réseau.

[NSADM-20017]s

Prise en charge de la visualisation des rapports Insight uniquement pour les applications autorisées

L'analyse Citrix ADM prend désormais en charge l'autorisation basée sur l'adresse IP virtuelle. Lorsque vous autorisez les utilisateurs à accéder à un ensemble d'applications ou de serveurs virtuels spécifiques, les utilisateurs peuvent désormais voir les rapports d'analyse uniquement pour les applications (serveurs virtuels) auxquelles ils sont autorisés.

[NSADM-17971]

Prise en charge de la planification de l'exportation de rapports dans Citrix ADM

Citrix ADM prend en charge la planification de l'exportation de rapports sur différentes pages. Vous pouvez effectuer diverses actions lors de la planification de l'exportation des rapports.

- Planifier la génération et l'exportation du rapport à intervalles réguliers.
- Spécifiez les paramètres de périodicité de génération de rapport et créez un profil de messagerie vers lequel le rapport est exporté.
- Exportez les rapports vers un canal Slack désigné.

Cette amélioration est similaire à la fonctionnalité présente dans Citrix ADM Software.

[NSADM-24829]

Janvier 16, 2019

Les agents Citrix Application Delivery Manager (ADM) sont, par défaut, automatiquement mis à niveau vers Citrix ADM 13.0 build 30.15. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** >

Agents. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour de plus amples informations, consultez la section Configuration des paramètres de mise à niveau de l'agent.

Des améliorations de la plate-forme ont été apportées dans cette version pour améliorer les performances.

04 janvier 2019

Les agents Citrix Application Delivery Manager (ADM) sont, par défaut, automatiquement mis à niveau vers Citrix ADM 13.0 build 30.14. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour de plus amples informations, consultez la section Configuration des paramètres de mise à niveau de l'agent.

07 décembre 2018

Cette version inclut des améliorations et des corrections de bogues.

Les agents Citrix Application Delivery Manager (ADM) sont, par défaut, automatiquement mis à niveau vers Citrix ADM 13.0 build 30.14. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour de plus amples informations, consultez la section Configuration des paramètres de mise à niveau de l'agent.

Fonctionnalités nouvelles et améliorées

Analyse de l'infrastructure

> **Remarque**
>
> Cette fonctionnalité est actuellement disponible en aperçu.

La fonctionnalité d'analyse Citrix ADM Infrastructure rassemble toutes les données collectées à partir des instances de Citrix ADC dans une représentation visuelle sur une seule page sur Citrix ADM. La fonctionnalité Analyse de l'infrastructure vous aide à visualiser les facteurs qui ont entraîné ou pourraient entraîner un problème sur les instances. Cette visualisation vous aide également à déterminer les actions à effectuer pour empêcher le problème et sa récurrence.

Pour afficher l'analyse de l'infrastructure dans une vue circle-pack, effectuez les opérations suivantes :

1. Accédez à **Réseaux > Analyse de l'infrastructure**.
2. Sélectionnez l'icône de vue Circle-Pack.

Pour de plus amples informations, consultez la section Analyse de l'infrastructure.

[NSADM-23680]

Intégration de Citrix ADM avec Citrix Virtual Citrix Director

Citrix ADM est désormais intégré à Citrix Director. Cela permet à Director d'afficher les rapports HDX Insight à partir de Citrix ADM dans la page de détails Réseau et Utilisateur et fournit des informations spécifiques à l'utilisateur, aux applications, aux postes de travail, aux instances et aux licences.
Pour plus d'informations, reportez-vous à la section Intégration de Citrix ADM avec Citrix Virtual Citrix Director.

[NSADM-17085]

Prise en charge du téléchargement des certificats SSL

Vous pouvez désormais télécharger les certificats SSL à partir de Citrix ADM en accédant à **Réseaux** > Tableau de **bord SSL** . Sélectionnez un certificat SSL et cliquez sur **Télécharger** dans la liste Action. Pour de plus amples informations, consultez la section Télécharger les certificats SSL.

[NSADM-19790]

Prise en charge de la sauvegarde et de la restauration des instances Citrix ADC SDX

Il est désormais possible de sauvegarder et de restaurer une instance Citrix ADC SDX à partir de Citrix ADM. Pour de plus amples informations, consultez la section Sauvegarde et restauration des instances de Citrix ADC.

[NSADM-19882]

Problèmes résolus

Applications

- Dans la logique d'agrégation du tableau de bord de l'application, la dernière valeur du volume de données est conservée en tant que compteur total. Mais parfois, les valeurs sont perçues plus élevées, ce qui est considérablement plus élevé que la dernière valeur.

  [718359]

19 novembre 2018

Cette version inclut des améliorations et des corrections de bogues.

Les agents Citrix Application Delivery Manager (Citrix ADM) sont, par défaut, automatiquement mis à niveau vers Citrix ADM 12.1 build 505.130. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour de plus amples informations, consultez la section Configuration des paramètres de mise à niveau de l'agent.

Fonctionnalités nouvelles et améliorées

Configurer AppFlow sur plusieurs serveurs virtuels et afficher les informations de progression

Lorsque vous configurez AppFlow sur plusieurs serveurs virtuels en même temps, une fenêtre contextuelle affiche la progression étape par étape de la configuration AppFlow. Les informations indiquent le nombre de serveurs virtuels configurés au niveau de l'instance. Les informations de progression sont utiles lorsque vous configurez AppFlow sur de nombreux serveurs virtuels.

> **Remarque**
>
> Citrix ADM prend en charge IPFIX comme mode de transport par défaut lors de la configuration d'AppFlow sur des serveurs virtuels. À partir de la version 12.0 de Citrix ADC, Citrix ADM prend en charge **Logstream**et vous devez sélectionner explicitement **Logstream**, si nécessaire.

Lors de l'activation d'AppFlow sur les instances Citrix Gateway, assurez-vous de sélectionner ICA ou TCP comme mode de transport. Si vous sélectionnez les deux, ICA a priorité sur TCP. La sélection de HTTP avec ICA ou TCP est autorisée. Pour plus d'informations sur l'activation d'AppFlow à l'aide d'ADM, voirActivation d'AppFlow à l'aide de Citrix ADM

Problèmes résolus

Analytics

- Lorsque le nom du serveur virtuel dépasse 60 caractères, le nom de l'action AppFlow dépasse 128 caractères. L'activation de la configuration de ces noms d'actions peut entraîner l'arrêt de fonctionnement de l'instance ADC.

  [717663]

- Un délai plus long est nécessaire pour activer les configurations AppFlow effacées pour plusieurs serveurs virtuels sur une instance ADC.

  [717675]

Réseaux

- Bien que vous puissiez télécharger un certificat ou un fichier de clé de certificat depuis votre système de stockage local vers Citrix ADM, les autorisations de « lecture » pour ces fichiers ne sont pas conservées par ADM. Lorsque de tels fichiers sont téléchargés par ADM vers des instances ADC respectives, ADC affiche ces fichiers comme des fichiers non valides.

  [716691]

- Parfois, Citrix ADM peut ne pas être en mesure de communiquer avec les services de confiance Citrix en raison d'une gestion incorrecte des exceptions. Il se peut que vous ne puissiez pas vous connecter au service Citrix ADM. Il pourrait y avoir aussi des fuites de ressources sur le service ADM.

  [717571]

- Lorsque vous configurez deux règles d'événement qui correspondent au même événement, mais qui ont des âges d'événement différents, Citrix ADM considère uniquement la règle dont l'âge d'événement est inférieur est configuré. Avec ce correctif, Citrix ADM considère les deux règles d'événement.

  [716930]

- Les messages Syslog sont affichés dans plusieurs pages dans Citrix ADM. Lorsque vous recherchez des messages Syslog dans une page en entrant un mot clé, les mêmes résultats de recherche ne sont pas conservés lorsque vous passez à une autre page. Vous devez effectuer une recherche à nouveau en entrant le même mot-clé. Avec ce correctif, Citrix ADM affiche le résultat de la recherche dans toutes les pages.

  [715671]

27 octobre 2018

Cette version inclut des améliorations et des corrections de bogues.

Les agents Citrix Application Delivery Manager (Citrix ADM) sont, par défaut, automatiquement mis à niveau vers Citrix ADM 12.1 build 504.131. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour plus de détails, consultez Configuration des paramètres de mise à niveau de l'agent.

Fonctionnalités nouvelles et améliorées

Possibilité de contrôler le nombre de messages Syslog affichés

Par défaut, Citrix ADM affiche 50 messages Syslog dans chaque page. Vous pouvez désormais afficher davantage de messages sur une page en choisissant 100, 250, 500 ou 1 000 messages par page.

Problèmes résolus

Analytics

- Si vous disposez d'autorisations en lecture seule, vous ne pouvez pas voir les icônes de diagnostic dans aucune vue d'analyse.

  [715785]

Applications

- Citrix ADM n'affiche pas le nombre de transactions et le volume de flux de données pour les applications GSLB sur le tableau de bord de l'application.

  [716878]

- Citrix ADM n'affiche aucune information pour les serveurs virtuels liés aux applications créées sur des instances ADC déployées en haute disponibilité.

  [716906]

Réseaux

- Le sous-système de performances Citrix ADM se bloque toutes les quelques heures, ce qui a un impact sur les rapports réseau.

  [715483]

- Le sous-système de performances Citrix ADM signale une utilisation élevée de l'UC qui a un impact sur les rapports réseau.

  [716235]

- Si ASG est déployé dans plusieurs zones de disponibilité, la suppression gracieuse/non gracieuse des serveurs back-end peut ne pas prendre en charge le groupe de mise à l'échelle automatique Amazon EC2.

  [716031]

- Lorsque vous exportez des certificats SSL en fonction d'une option de recherche, le rapport CSV répertorie tous les certificats SSL quels que soient les critères de recherche.

  [714674]

- Lorsque vous accédez à Réseaux > Événements, les événements ne sont pas affichés dans l'ordre pour la première fois. Si vous cliquez sur l'en-tête de colonne Date, les événements apparaissent triés chronologiquement.

  [716615]

- Par intermittence, Citrix ADM peut manquer de collecter des points de données pour le rapport quotidien. Cela aura une incidence sur les rapports hebdomadaires et mensuels.

  [716778]

Système

- Vous pouvez désormais trier les fichiers dans l'interface graphique Citrix ADM en fonction des dates au lieu de les trier sous forme de chaîne.

  [715491]

Octobre 12, 2018

Cette version inclut des améliorations et des corrections de bogues.

Par défaut, les agents Citrix ADM sont automatiquement mis à niveau vers Citrix ADM 12.1 build 502.127. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour plus de détails, consultez Configuration des paramètres de mise à niveau de l'agent.

Fonctionnalités nouvelles et améliorées

Prise en charge des sessions EDT dans les rapports HDX Insight

Le HDX Insight affiche maintenant le nombre de sessions EDT et de sessions non-EDT dans le cadre du rapport sur les sessions actives. Le tableau Utilisateurs affiche un rapport détaillé de tous les utilisateurs du système. En outre, un nouveau graphique en donut 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.

Prise en charge de l'affichage des serveurs virtuels d'équilibrage de charge et de commutation de contenu dans le rapport Web Insight

Les rapports Web Insight affichent désormais les données des serveurs virtuels d'équilibrage de charge qui sont liés à des serveurs virtuels de commutation de contenu. Vous pouvez afficher les données des deux serveurs virtuels séparément. Pour plus de détails, consultez Serveurs d'équilibrage de charge liés aux serveurs de commutation de contenu.

Prise en charge de l'affichage des instances de Citrix ADC en haute disponibilité et en cluster dans les rapports Web Insight

Les rapports d'analyse Citrix ADM affichent désormais des rapports pour les instances ADC déployées en mode haute disponibilité et en mode cluster. Le nombre total de lancements de session et le nombre total d'applications dans ces deux scénarios en tant que rapport combiné au lieu de rapports individuels pour chaque instance du groupe.

> **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 pendant la période jusqu'à ce que les données persistent.
> - Pour les instances ADC déployées en mode cluster, l'ID/Nom de domaine d'observation est remplacé par le nom d'hôte CLIP et CLIP. Toutes les données précédemment collectées continuent de signaler le domaine d'observation ID/Nom de domaine d'observation. Pour plus de détails, consultez Instances Citrix ADC déployées en mode haute disponibilité et en mode cluster.

Ajout d'une instance Citrix ADC CPX dans Citrix ADM

Citrix ADM a été amélioré pour soutenir les améliorations apportées aux fonctionnalités CPX. L'instance Citrix ADC CPX est maintenant ajoutée dans Citrix ADM de l'une des deux manières suivantes :

- En fournissant une adresse IP pour le CPX ainsi qu'un profil de périphérique si l'instance CPX est utilisée pour gérer le trafic Nord-Sud
- En fournissant l'adresse IP de l'hôte Docker, si l'instance Citrix ADC CPX n'est pas accessible par Citrix ADM. C'est-à-dire si le CPX est nécessaire pour gérer le trafic Est-Ouest dans un datacenter.

Si le périphérique est découvert via une adresse IP Docker, l'adresse IP de la base de données est représentée par NSIP_DOCKERIP. Si le périphérique est découvert via un NSIP accessible du CPX, l'adresse IP est représentée par le NSIP du CPX dans la base de données ADM.

Le processus d'ajout d'une instance CPX est maintenant similaire à la façon dont d'autres types ADC tels que VPX ou MPX sont ajoutés dans ADM. Fournir le profil de périphérique vous permet de configurer le port SSH, HTTP, HTTPS dans le profil de périphérique plutôt que de les configurer explicitement. De plus, l'enregistrement de CPX dans le SMA a été amélioré. Lorsqu'un CPX démarre, Citrix ADM détecte et enregistre automatiquement l'instance CPX.

Vous n'avez pas besoin d'ajouter un hôte Docker dans Citrix ADM pour découvrir les instances CPX de Citrix ADC.

Prise en charge de la mise à l'échelle automatique des instances Citrix ADC déployées dans AWS

La fonctionnalité de mise à l'échelle automatique Citrix ADM prend désormais en charge la mise à l'échelle des instances de Citrix ADC dans AWS. La fonctionnalité de mise à l'échelle automatique Citrix ADM ajoute ou supprime les nœuds de cluster Citrix ADC déployés dans AWS selon le moment et dans quelle mesure les serveurs back-end mise à l'Autoscale. Citrix ADM collecte des statistiques (utilisation du processeur, utilisation de la mémoire, débit) à partir des clusters provisionnés à l'Autoscale. Ces statistiques sont évaluées par rapport à la valeur configurée par le client. Selon que les statistiques dépassent le seuil maximal ou fonctionnent en dessous du seuil minimum, l'échelle d'entrée ou d'extension est déclenchée respectivement.

Les avantages des fonctions de mise à l'échelle automatique sont les suivants :

- Garantit que l'application est opérationnelle tout le temps, quelles que soient les exigences du trafic.
- Les instances de Citrix ADC sont ajoutées et supprimées dynamiquement pour une configuration manuelle sans contact.
- La gestion DNS est automatique.
- Permet une meilleure gestion des coûts.

Pour utiliser la fonctionnalité Mise à l'Autoscale, vous devez créer des groupes de Autoscale et déployer l'application à l'aide de StyleBooks. Pour plus de détails, consultez Mise à l'échelle automatique de Citrix ADC dans AWS à l'aide de Citrix ADM.

Problèmes résolus

Analytics

- Le tableau Résumé des applications dans les rapports Security Insight > Total Violations affiche le temps d'attaque sous la forme « NA- » pour tous les enregistrements historiques.

  [715905]

Réseaux

- Les statistiques des serveurs virtuels ne sont pas affichées si les serveurs virtuels font partie d'instances Citrix ADC déployées en haute disponibilité.

  [715243]

- Lorsque vous ajoutez un serveur virtuel GSLB dans Citrix ADM qui fait partie d'une application personnalisée, ADM peut ne pas afficher les statistiques correctement pour le serveur GSLB ajouté.

  [715639]

- Lorsque vous ajoutez la plate-forme Citrix ADC SDX dans ADM, et si la version du SDX ADC est inférieure à 11.0, le tableau de bord de SDX visible dans Citrix ADM peut afficher des erreurs.

[715803]

Système

- Parfois, il se peut que vous ne puissiez pas redémarrer les instances de Citrix ADC à partir de Citrix ADM. En effet, certaines instances nécessitent plus de dix minutes pour redémarrer et Citrix ADM n'attend que dix minutes pour redémarrer les instances. Avec ce correctif, vous pouvez maintenant configurer le temps de redémarrage Citrix ADM jusqu'à 30 minutes.

  [716178]

14 septembre 2018

Cette version inclut des améliorations et des corrections de bogues.

Par défaut, les agents Citrix ADM sont automatiquement mis à niveau vers Citrix ADM 12.1 build 502.127. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour plus de détails, consultez Configuration des paramètres de mise à niveau de l'agent.

Fonctionnalités nouvelles et améliorées

Incluant le temps d'attaque agrégé dans les rapports Security Insight

Le rapport **Total Violations** dans Security Insight affiche la durée de l'attaque sous la forme « NA » si la durée sélectionnée est supérieure à une heure. Maintenant, si vous sélectionnez « 1 jour » dans la liste, le rapport 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. Pour plus de détails, consultez Security Insight.

[686874]

Problèmes résolus

Système

- Dans Citrix ADM, lorsque vous modifiez les profils d'administration utilisateur, les instances de Citrix ADC ne sont pas redécouvertes et vous ne pouvez pas ouvrir une session sur les instances de Citrix ADC. Les instances ne sont pas mises à jour avec les nouveaux détails de l'utilisateur et les instances utilisent toujours les profils d'administration initialement appliqués.

  [699435]

Réseaux

- Les deux problèmes suivants sont remarqués dans Citrix ADM liés aux serveurs virtuels :
  - Lorsqu'un serveur virtuel est configuré avec un serveur DNS qui possède plusieurs adresses IP, Citrix ADM ne peut pas découvrir ces serveurs virtuels.
  - Lorsqu'un serveur virtuel contient des caractères non anglais dans le commentaire ou dans tout autre champ, Citrix ADM renvoie une erreur et ne peut pas détecter les serveurs virtuels pour cette instance.

  [713472]

Août 23, 2018

Cette version inclut des améliorations et des corrections de bogues.

Par défaut, les agents Citrix ADM sont automatiquement mis à niveau vers Citrix ADM 12.1 build 501.123. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour plus de détails, consultez Configuration des paramètres de mise à niveau de l'agent.

Fonctionnalités nouvelles et améliorées

Renommer le service de gestion et d'analyse NetScaler

NetScaler Management and Analytics Service est désormais renommé Citrix Application Delivery Management (ADM). Cela fait partie du portefeuille de produits unifiés Citrix.

Vous pouvez remarquer de nouveaux noms dans nos produits et la documentation produit. Ceci est le résultat de l'expansion du portefeuille Citrix et de la stratégie cloud. Pour plus d'informations sur le portefeuille unifié Citrix, reportez-vous à la sectionguide des produits Citrix.
L'implémentation de cette transition dans nos produits et leur documentation est en cours.

- Le contenu intégré au produit et à la documentation peut encore contenir les anciens noms. Par exemple, vous pouvez voir des instances des anciens noms dans le texte de la console, les messages, les noms de répertoire/fichier, les captures d'écran et les diagrammes.
- Il est possible que certains éléments (tels que les commandes) conservent leurs anciens noms pour éviter de casser les scripts clients existants.
- La documentation produit associée et les autres ressources (telles que les vidéos et les billets de blog) auxquelles la documentation de ce produit renvoie peuvent toujours contenir des noms anciens.

[715090]

Problèmes résolus

Réseaux

- Les entrées en double sont affichées lorsque vous filtrez toutes les entrées répertoriées dans la fonction réseau, telles que l'équilibrage de charge, la commutation de contenu, la redirection de cache, et d'autres.

  [704095]

- Lorsque vous accédez à **Réseaux** > **Instances** et sélectionnez **Configurer Analytics** pour une instance Citrix ADC pour activer Insight sur les serveurs virtuels, la page **Configurer Analytics** ne reflète pas les détails du serveur virtuel si les serveurs virtuels ont un « espace » dans leurs noms.

  [713945]

- Lorsque vous configurez des collecteurs directement configurés sur l'instance Citrix ADC, le champ de colonne **Mode de transport** de la page Configurer Analytics n'affiche aucune donnée.

  [713946]

Août 03, 2018

Cette version inclut des améliorations et des corrections de bogues.

Par défaut, les agents Citrix ADM sont automatiquement mis à niveau vers Citrix ADM 12.1 build 500.126. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour plus de détails, consultez Configuration des paramètres de mise à niveau de l'agent.

Nouveautés

Importation et synchronisation GitHub pour StyleBooks

Vous pouvez désormais utiliser la fonctionnalité « Référentiels » dans Citrix ADM pour importer et synchroniser directement les StyleBooks à partir de référentiels GitHub. Vous pouvez synchroniser StyleBooks à partir de plusieurs dépôts GitHub. StyleBooks créés dans GitHub et importés à partir de référentiels GitHub dépendent toujours des stratégies RBAC Citrix ADM de la même manière que StyleBooks importés manuellement. Vous pouvez configurer un référentiel GitHub à l'aide d'un nom d'utilisateur et d'un mot de passe GitHub ou d'un jeton d'API.

> **Remarque**
>
> - Vous pouvez uniquement importer et synchroniser les StyleBooks qui ne sont pas asso-

> ciés aux StyleBooks dépendants (c'est-à-dire que toutes les configurations du StyleBook doivent être définies dans ce fichier).
> - La synchronisation à partir d'un référentiel GitHub doit être initiée manuellement à partir de l'interface graphique ou de l'API Citrix ADM (autrement dit, l'importation de StyleBooks ne se produit pas automatiquement en fonction de l'activité de validation GitHub).

Pour plus de détails, consultez Importation et synchronisation de StyleBooks à partir du référentiel GitHub

[699790]

Utilisation de StyleBooks pour créer des serveurs virtuels d'équilibrage de charge avec pare-feu d'application

Vous pouvez désormais automatiser la configuration de la fonctionnalité Citrix WAF (Web Application Firewall) à l'aide du nouveau WAF StyleBook par défaut dans Citrix ADM. Ce StyleBook permet aux utilisateurs de créer un serveur virtuel d'équilibrage de charge avec les stratégies et paramètres de pare-feu d'application associés.

> **Remarque**
>
> Avant de pouvoir configurer les signatures du pare-feu d'application, vous devez créer les objets signatures dans l'instance de Citrix ADC à partir du modèle d'objet signatures par défaut approprié. Vous ne pouvez pas configurer ou modifier les objets de signatures par défaut via le WAF StyleBook.

Pour de plus amples informations, consultez la section Pare-feu d'application Web StyleBook.

[708597]

Possibilité de modifier le mot de passe pour l'agent Citrix ADM

Vous pouvez maintenant exécuter le script « change_agent_system_password.py » sur la ligne de commande qui vous permet de mettre à jour le mot de passe de l'agent Citrix ADM après avoir déployé l'agent. Pour plus de détails, consultez Modification du mot de passe de l'agent après l'enregistrement de l'agent.

[712517]

Problèmes résolus

Réseaux

- Lors de la création de tâches de configuration à l'aide du modèle de configuration maître, vous devrez peut-être télécharger le même fichier de configuration plusieurs fois après avoir modifié

le fichier. Vous pouvez télécharger le fichier avec succès la première fois. Les téléchargements ultérieurs échouent sans notification de l'utilisateur.

Solution : cela se produit en raison du comportement par défaut du navigateur. Si vous souhaitez télécharger à nouveau le même fichier après des modifications, cliquez sur Précédent pour accéder à l'onglet Sélectionner les instances, puis cliquez sur Suivant et chargez à nouveau le même fichier.

[711593]

- Citrix ADM n'est pas en mesure d'analyser tous les membres du groupe de services liés

  [712022]

Analytics

- Il n'est pas possible d'afficher des informations dans Web Insight lorsque vous accédez à Citrix ADM avec des privilèges en lecture seule.

  [713404]

- Lorsque vous modifiez un bloc IP créé précédemment dans la page **Configurer les blocs IP** sous **Analytics** > **Paramètres** en modifiant la ville, la région et le pays, et lorsque vous essayez de modifier à nouveau les paramètres, la page Configurer les blocs IP affichait le nom de la ville précédente. Cette version résout ce problème.

  [712110]

- Il se peut qu'une table se répand sur plusieurs pages, car Citrix ADM n'affiche que 25 entrées de ligne dans une page. Auparavant, vous pouviez trier les entrées de ligne uniquement sur la page en cours. Les autres pages n'ont jamais affiché d'entrées triées. Vous pouvez maintenant trier le tableau dans n'importe quelle page et toutes les pages de ce tableau afficheront les résultats triés.

  > **Remarque** Cette fonctionnalité ne fonctionne que si le nombre d'enregistrements dans une table est inférieur à 25 000.

  [689564]

Problèmes connus

Applications

- Lorsque vous accédez à **Réseaux** > **Instances** et que vous sélectionnez **Configurer Analytics** pour une instance de Citrix ADC pour activer Insight sur les serveurs virtuels, la page **Configurer Analytics** ne reflète pas l'état correct du serveur virtuel si le serveur virtuel ont un « espace »

dans leurs noms. Par exemple, bien que la journalisation AppFlow soit activée sur le serveur virtuel, elle peut être affichée comme « désactivée » sur la page **Configurer Analytics** .

[713945]

- Lorsque vous configurez des collecteurs directement sur l'instance de Citrix ADC, le champ de colonne Mode de transport de la page Configurer Analytics n'affiche aucune donnée.

  [713946]

Analytics

- Dans certains cas, les nœuds HDX Insight et Citrix Gateway Insight peuvent ne pas être affichés sur l'interface graphique graphique Citrix ADM.

  Solution : actualisez la page et réessayez.

  [690327]

Réseaux

- Les entrées en double sont affichées lorsque vous filtrez toutes les entrées répertoriées dans la fonction réseau, telles que l'équilibrage de charge, la commutation de contenu, la redirection de cache, et d'autres.

  [704095]

- Lorsque vous accédez à Réseaux > Instances et sélectionnez « Configurer Analytics » pour une instance de Citrix ADC afin d'activer Insight sur les serveurs virtuels, la page Configurer Analytics ne reflète pas les détails du serveur virtuel si les serveurs virtuels ont un « espace » dans leur nom.

  [713945]

- Lorsque vous configurez des collecteurs directement configurés sur l'instance de Citrix ADC, le champ de colonne Mode transport de la page Configurer Analytics n'affiche aucune donnée.

  [713946]

Paramètres

- Lorsque vous supprimez les utilisateurs de Citrix Cloud, les noms d'utilisateur supprimés continuent d'apparaître dans Citrix ADM dans Paramètres > Administration des utilisateurs > Utilisateurs.

  [686581]

Juillet 12, 2018

Cette version inclut des corrections de bogues.

Par défaut, les agents Citrix ADM sont automatiquement mis à niveau vers la version 516.126. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour plus de détails, consultez Configuration des paramètres de mise à niveau de l'agent.

Nouveautés

Bouton de test pour la configuration du courrier électronique pour les notifications d'événements Citrix ADM

Lors de l'envoi d'e-mails pour les notifications d'événements, vous pouvez envoyer un e-mail de test pour tester les paramètres configurés. Le bouton « Test » vous permet désormais d'envoyer un e-mail de test après avoir configuré un serveur de messagerie, des listes distribuées associées et d'autres paramètres. Cette fonctionnalité garantit que les paramètres fonctionnent correctement. Pour plus de détails, consultez Créer des règles d'événement.

[684948]

Personnalisation de la ligne d'objet de l'e-mail de notification d'événement

Dans un grand réseau qui a de nombreux serveurs virtuels configurés, vous pouvez, en tant qu'administrateur, recevoir un grand nombre d'e-mails chaque jour. Mais vous pouvez voir le nom de l'entité affectée dans la fenêtre contextuelle du courrier lorsque le courrier est reçu afin que vous puissiez déterminer l'entité affectée sans avoir à ouvrir l'e-mail. Sous **Réseaux** > **Événement** > **Règles**, lorsque vous créez une règle et définissez des règles de notification par e-mail, vous avez désormais la possibilité d'inclure des informations supplémentaires telles que le nom de l'entité affectée (objet d'échec). Pour plus de détails, reportez-vous à la section Créer des règles d'événement.

[705142]

Améliorations de la fonctionnalité de capacité mise en commun

Quelques modifications ont été apportées à la page des licences regroupées dans les instances Citrix ADM pour Citrix VPX. Un nouvel ensemble d'états a été introduit lorsque vous allouez des licences dans le pool de licences aux instances Citrix ADC à la demande. Les États sont les suivants :

- Attribué
- Grace
- Synchronisation en cours

- Partiellement alloué
- Périphérique non géré
- Attribué. Non appliqué à l'appareil
- Connexion perdue

De plus, quelques détails supplémentaires sur l'état de l'allocation de licences ont été ajoutés à Citrix ADM. Pour plus de détails, consultez Capacité groupée.

[709975]

Disponibilité des fonctionnalités de licence dans Citrix ADM

Citrix ADM héberge désormais une bande passante et un pool d'instances communes qui serveurs les instances Citrix VPX et MPX ajoutées dans Citrix ADM. À partir de ce pool commun, chaque instance Citrix ADC de votre datacenter, indépendamment de la plate-forme ou du facteur de forme, vérifie une licence d'instance et seulement autant de bande passante qu'elle en a besoin. Pour plus de détails, consultez Capacité groupée.

[709679]

Prise en charge des licences automatiques configurables pour les serveurs virtuels non adressables

Citrix ADM, par défaut, n'applique pas automatiquement les licences aux serveurs virtuels non adressables. Pour les 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, ainsi que lorsque vous devez sélectionner les nouveaux serveurs virtuels non adressables chaque fois qu'ils sont ajoutés à votre réseau.

La nouvelle option dans Citrix ADM sous **Réseaux** > **Licences** > **Licences système** est « 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**
>
> - Citrix ADM, par défaut, ne sélectionne toujours pas automatiquement les serveurs virtuels non adressables pour les licences.
> - L'analyse des applications (Tableau de bord des applications) est la seule analyse prise en charge actuellement sur les serveurs virtuels non adressables sous licence. Pour de plus amples informations, consultez Gestion des abonnements

[707843]

Possibilité de provisionner des instances Citrix ADC VPX sur AWS à l'aide de Citrix ADM

Citrix ADM vous permet désormais de provisionner les instances Citrix ADC VPX sur la plate-forme Amazon Web Services (AWS) en tant que déploiement autonome. Citrix ADC VPX sur AWS vous permet d'utiliser les fonctionnalités de cloud computing AWS et d'utiliser les fonctionnalités d'équilibrage de charge et de gestion du trafic Citrix ADC pour leurs besoins professionnels. Citrix ADC sur AWS prend en charge toutes les fonctionnalités de gestion du trafic d'une appliance Citrix ADC physique. Pour plus de détails, consultez Provisionnement d'instances Citrix ADC VPX sur AWS.

[680526]

Problèmes résolus

Haute disponibilité

- Si vous configurez un nœud dans une paire d'instances de Citrix ADC en mode haute disponibilité avec l'adresse IP dans la plage 171.31.200.x, cette paire d'instances de Citrix ADC ne sont pas découvertes par Citrix ADM.

  [710589]

Réseaux

- Lors de la création de tâches de configuration à l'aide du modèle de configuration maître, vous devrez peut-être télécharger le même fichier de configuration plusieurs fois après avoir modifié le fichier. Vous pouvez télécharger le fichier avec succès la première fois. Les téléchargements ultérieurs échouent sans notification de l'utilisateur.

  Solution : cela se produit en raison du comportement par défaut du navigateur. Si vous souhaitez télécharger à nouveau le même fichier après des modifications, cliquez sur Précédent pour accéder à l'onglet Sélectionner les instances, puis cliquez sur Suivant et chargez à nouveau le même fichier.

  [711593]

- Les données du rapport de synthèse d'événements Networks sont tronquées en raison de problèmes de formatage.

  [704980]

- Les rapports d'événements basés sur SNMP v3 ne fonctionnent pas après la mise à niveau de Citrix ADM vers la version 12.1. Citrix recommande la solution de contournement suivante pour les instances de Citrix ADC dans la version 12.1, version 48.13 ajoutée dans Citrix ADM.

  Solution : utilisez les interruptions SNMP v2 jusqu'à ce que le problème SNMP v3 soit résolu et publié.

[710564]

- Lorsque Citrix ADC instances basculement lorsqu'il est déployé en mode haute disponibilité, le processus mas_afdecoder ne reçoit pas de notification pour mettre à jour les informations de licence. Le processus mas_afdecoder supprime le paquet de données reçu du nœud principal et, par conséquent, les rapports Web Insight n'apparaissent pas sur l'interface graphique graphique Citrix ADM.

  [711503]

Système

- L'enregistrement de l'agent échoue si le nom de la ville a un caractère Unicode.

  [711737]

- Lorsque vous tentez d'activer un nouvel agent Citrix ADM, vous pouvez recevoir un message d'erreur « ID d'instance non valide ».

  [706527]

StyleBooks

- Sharepoint StyleBook doit prendre en charge le protocole SSL pour tous les services back-end.

  [706507]

- Le champ Auteur affiche null dans la réponse API utilisée pour récupérer des informations sur un StyleBook.

  [711021]

Problèmes connus

Analytics

- Dans certains cas, les nœuds HDX Insight et Citrix Gateway Insight peuvent ne pas être affichés sur l'interface graphique graphique Citrix ADM.

  Solution : actualisez la page et réessayez.

  [690327]

Réseaux

- Les entrées en double sont affichées lorsque vous filtrez toutes les entrées répertoriées dans la fonction réseau, telles que l'équilibrage de charge, la commutation de contenu, la redirection de cache, et d'autres.

[704095]

Paramètres

- Lorsque vous supprimez les utilisateurs de Citrix Cloud, les noms d'utilisateur supprimés continuent d'apparaître dans Citrix ADM dans Paramètres > Administration des utilisateurs > Utilisateurs.

  [686581]

14 juin 2018

Cette version inclut des corrections de bogues.

Par défaut, les agents Citrix ADM sont automatiquement mis à niveau vers la version 515.116. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour plus de détails, consultez Configuration des paramètres de mise à niveau de l'agent.

Nouveautés

Contrôle d'accès basé sur le rôle sur les domaines GSLB

Vous pouvez désormais autoriser uniquement les utilisateurs autorisés à effectuer la configuration GSLB à l'aide de StyleBooks car RBAC est actuellement pris en charge sur les domaines GSLB également.

Citrix ADM prend désormais en charge une nouvelle entité appelée "Nom de domaine DNS." Dans Citrix ADM, accédez à **Réseaux** > **Nom de domaine DNS** et ajoutez les entrées de noms de domaine DNS. Accédez à **Système** > **Administration des utilisateurs** > **Groupes** . Définissez les paramètres RBAC pour un groupe d'utilisateurs sur des noms de domaine sélectionnés à partir de la liste de noms de domaine disponible.

Ce paramètre RBAC s'applique à vos utilisateurs lorsqu'ils tentent de configurer GSLB à l'aide de StyleBooks. Les utilisateurs ne peuvent utiliser qu'un ou plusieurs noms de domaine DNS qu'ils sont autorisés à utiliser.

[706988]

Amélioration de la fonctionnalité de recherche d'instances de Citrix ADC

Considérons un scénario dans lequel Citrix ADM gère de nombreuses instances de Citrix ADC. Vous pouvez avoir la possibilité de rechercher l'inventaire des instances en fonction de certains paramètres de recherche. Citrix ADM propose désormais deux critères de recherche : les balises et les propriétés

pour rechercher efficacement un sous-ensemble d'instances de Citrix ADC qui qualifie les paramètres de recherche.

Exemple : considérez que vous souhaitez rechercher toutes les instances de Citrix ADC qui se trouvent sur la version 12.0 et qui sont à l'état UP. Pour plus de détails, consultez Créer des balises et assigner à des instances.

[709997]

Possibilité de marquer des instances de Citrix ADC

Les balises sont des termes ou des mots clés que vous pouvez affecter à une instance de Citrix ADC pour associer une description supplémentaire sur l'instance de Citrix ADC. Citrix ADM vous permet désormais d'associer vos instances Citrix ADC avec des balises. Ces balises vous permettent de regrouper, d'identifier et de rechercher les instances de Citrix ADC. Pour plus de détails, consultez Créer des balises et assigner à des instances.

[708603]

Possibilité d'envoyer des notifications d'événements à Slack

Auparavant, dans l'interface graphique Citrix ADM, vous aviez la possibilité d'envoyer des notifications par e-mail pour les événements. Vous pouvez maintenant envoyer une notification d'événement à Slack canal également.

Configurez ADCal Slack requis en fournissant le nom de profil et l'URL webhook dans l'interface graphique Citrix ADM. Les notifications d'événement sont ensuite envoyées à ce canal. Pour plus de détails, consultez Créer des règles d'événement.

[656472]

Problèmes résolus

Réseaux

- Vous ne pouvez pas configurer AppFlow sur des serveurs virtuels si Citrix ADM est configuré avec une autre interface que 0/1. [705330]
- Ne pas inclure d'espaces blancs dans les noms[708003]de modèles d'audit de configuration

StyleBooks

- Vous ne pouvez pas créer d'entité à l'aide de StyleBooks lorsque vous avez défini des en-têtes personnalisés dans le StyleBook. [709094]

Paramètres

- Bien que vous puissiez voir les notifications système concernant la déconnexion des utilisateurs, il est possible que vous ne receviez pas de notifications par e-mail. [704344]
- Citrix ADM ne parvient pas à prévalider l'instance de Citrix ADC si les détails NTP sont ajoutés dans le fichier rc.netscaler. Vous pouvez désormais sélectionner ces instances Citrix ADC et les supprimer lors de la mise à niveau des instances. [708466]
- Citrix ADC exporte les enregistrements « plusieurs applications terminate » pour la même application. Cela provoque le blocage du `afdcoder` processus Citrix ADM. [709462]

Haute disponibilité

- Lorsqu'une instance de Citrix ADC en mode haute disponibilité est affectée à un groupe d'utilisateurs et si la paire d'instances échoue, l'instance n'est plus affectée au groupe d'utilisateurs. [709202]

Problèmes connus

Analytics

- Dans certains cas, les nœuds HDX Insight et Citrix Gateway Insight peuvent ne pas être affichés sur l'interface graphique graphique Citrix ADM. **Solution** : actualisez la page et réessayez. [690327]

Réseaux

- Les entrées en double sont affichées lorsque vous filtrez toutes les entrées répertoriées dans la fonction réseau, telles que l'équilibrage de charge, la commutation de contenu, la redirection de cache, et d'autres. [704095]

Paramètres

- Lorsque vous supprimez les utilisateurs de Citrix Cloud, les noms d'utilisateurs supprimés continuent d'apparaître dans Citrix ADM dans **Paramètres** > **Administration** des **utilisateurs > Utilisateurs**. [686581]

24 mai 2018

Cette version inclut des corrections de bogues.

Par défaut, les agents Citrix ADM sont automatiquement mis à niveau vers la version 514.117. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier

l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour plus de détails, consultez Configuration des paramètres de mise à niveau de l'agent.

Problèmes résolus

Réseaux

- Considérez un scénario dans lequel vous disposez d'un accès RBAC uniquement aux nœuds Réseaux, Analytics et Système. Le comportement par défaut est que le premier nœud du volet de navigation, c'est-à-dire, Réseaux doit être la page de destination lorsque vous accédez à Citrix ADM. Mais maintenant, le nœud Analytics est la page de destination. [705347]
- Lorsque vous créez une tâche de configuration à l'aide d'Internet Explorer 11.0, Firefox version 31.0 et Google Chrome version 31.0, l'erreur suivante s'affiche :

```
SCRIPT5017: Syntax error in regular expression rdx.js (61,583910)
   "
<!--NeedCopy-->
```

  [707767]
- Un message d'état « No Diff » s'affiche dans le graphique des violations de modèle d'audit Citrix ADC lorsque deux modèles d'audit planifiés interrogeant la même instance ont une instance avec des violations. [708404]
- Vous ne pouvez pas modifier ou modifier le nom du modèle d'audit.[708407]
- Dans les modèles d'audit, le caractère '&' des valeurs variables est remplacé par le caractère '&' dans le fichier d'entrée.[708766]
- Lorsque vous définissez un seuil pour les instances sous Network Reporting, la liste des instances inclut les instances Citrix ADC SDX en plus des instances Citrix ADC.
  [707980]
- Lorsque vous ajoutez Citrix SD WAN instance WO à Citrix ADM, la connexion SNMP échoue et l'interface graphique ne répond pas.
  [709146]

Analytics

- Lorsque vous filtrez un rapport Gateway Insight en fonction du nom d'utilisateur, Citrix ADM ne parvient pas à filtrer les détails spécifiques à l'utilisateur.
  [701514]
- Le processus mas_afdecoder échoue parfois lorsqu'il y a un volume élevé de transactions HTTP.
  [706509]

Problèmes connus

Analytics

- Dans certains cas, les nœuds HDX Insight et Citrix Gateway Insight peuvent ne pas être affichés sur l'interface graphique graphique Citrix ADM.
  Solution : actualisez la page et réessayez.
  [690327]

Réseaux

- Les entrées en double sont affichées lorsque vous filtrez toutes les entrées répertoriées dans la fonction réseau, telles que l'équilibrage de charge, la commutation de contenu, la redirection de cache, et d'autres.
  [704095]

Paramètres

- Lorsque vous supprimez les utilisateurs de Citrix Cloud, les noms d'utilisateurs supprimés continuent d'apparaître dans Citrix ADM dans **Paramètres** > **Administration** des **utilisateurs > Utilisateurs**.
  [686581]

04 mai 2018

Cette version inclut des corrections de bogues.

Par défaut, les agents Citrix ADM sont automatiquement mis à niveau vers la version 513.120. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour plus de détails, consultez Configuration des paramètres de mise à niveau de l'agent.

Problèmes résolus

Analytics

- La vue graphique combinée dans HDX Insight montre un fuseau horaire incorrect. [703906]
- La génération du rapport Web Insight s'arrête en raison d'un calcul incorrect du temps de réponse de transaction POST HTTP. [707146]

Réseaux

- Lorsque les rapports sont exportés au format .csv, la colonne de temps affiche les données au format « epoch » et non au format lisible par l'utilisateur.
  [704828]
- Le résumé d'exécution d'une tâche de configuration s'affiche comme terminé sur Citrix ADM, même lorsque les commandes de la tâche de configuration ne sont pas entièrement exécutées sur l'instance de Citrix ADC.
  [707317]

Problèmes connus

Analytics

- Dans certains cas, les nœuds HDX Insight et Citrix Gateway Insight peuvent ne pas être affichés sur l'interface graphique graphique Citrix ADM.
  Solution : actualisez la page et réessayez.
  [690327]

Réseaux

- Les entrées en double sont affichées lorsque vous filtrez toutes les entrées répertoriées dans la fonction réseau, telles que l'équilibrage de charge, la commutation de contenu, la redirection de cache, et d'autres.
  [704095]

Paramètres

- Lorsque vous supprimez les utilisateurs de Citrix Cloud, les noms d'utilisateurs supprimés continuent d'apparaître dans Citrix ADM dans **Paramètres** > **Administration** des **utilisateurs > Utilisateurs**.
  [686581]

avril 12, 2018

Cette version inclut de nouvelles fonctionnalités et corrections de bugs.

Par défaut, les agents Citrix ADM sont automatiquement mis à niveau vers la version 512.119. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour plus de détails, consultez Configuration des paramètres de mise à niveau de l'agent.

Nouveautés

Possibilité de masquer StyleBooks par défaut à partir de Citrix ADM

Vous pouvez désormais masquer tous les StyleBooks par défaut dans la liste des StyleBooks disponibles dans Citrix ADM. Accédez à **Applications** > **Configurations** > **Paramètres** . Activez la case à cocher **Masquer les styles par défaut** . Tous les StyleBooks par défaut sont désormais masqués et ne sont pas accessibles à vos utilisateurs. Vous pouvez masquer davantage la page **Paramètres** elle-même des utilisateurs. En utilisant la fonctionnalité RBAC, vous pouvez créer une stratégie d'accès appropriée où la page Paramètres peut être rendue inaccessible aux utilisateurs. Accédez à **Compte** > **Administration des utilisateurs** > **Stratégies d'accès**. Créez une stratégie et, dans la section Autorisations, désélectionnez Paramètres sous **Tous** > **Applications** > **Configuration** . Pour de plus amples informations, consultez la section Masquer tous les StyleBooks par défaut.

[686914]

Possibilité de rechercher tous les StyleBooks définis par l'utilisateur dans Citrix ADM

Citrix ADM vous permet désormais de rechercher StyleBooks en fonction de leur type. Autrement dit, vous pouvez désormais rechercher tous les StyleBooks personnalisés dans la page de liste StyleBooks dans Citrix ADM. Pour de plus amples informations, consultez la section Utiliser des StyleBooks personnalisés.

[681949]

Problèmes résolus

Analytics

- Si le trafic AppFlow provient d'un cluster Citrix ADC, Citrix ADM ne stocke pas les données pendant plus de sept jours.
  [706348]

Réseaux

- Lorsque vous importez un modèle ou utilisez un modèle de configuration pour créer une tâche, les valeurs de variable ne sont pas affichées. Cliquez sur **Terminé** après l'aperçu pour afficher les valeurs des variables.
  [705884]
- Les travaux de configuration ne sont pas exécutés complètement lorsque plusieurs tâches de configuration sont exécutées simultanément avec de nombreuses commandes et dans plusieurs cas. L'exécution des tâches est stagnée et apparaît dans l'état « en cours ».
  [706201]

- Les modèles de configuration sont téléchargés sur Citrix ADM même si l'importation des modèles de configuration est annulée.
  [706219]
- Dans Citrix ADM, lorsque vous accédez à **Réseaux** > **Événements** > Messages **Syslog, les messages**les plus anciens s'affichent en premier, bien que la fenêtre Tri affiche l'option « Plus récent en premier ». Seulement lorsque vous sélectionnez « Le plus ancien d'abord », puis sélectionnez « Le plus récent d'abord », les messages s'affichent correctement.
  [702305]
- Si vous configurez la règle d'événement « supprimer » pour un événement en plus des autres règles d'événement, Citrix ADM exécute toutes les règles d'événement configurées.
  [702517]

Système

- Vous ne pouvez pas accéder à nouveau à la même instance de Citrix ADC après la fermeture malgré l'utilisation d'informations d'identification d'authentification unique.
  [699435]

Problèmes connus

Analytics

- Dans certains cas, les nœuds HDX Insight et Citrix Gateway Insight peuvent ne pas être affichés sur l'interface graphique graphique Citrix ADM.
  Solution : actualisez la page et réessayez.
  [690327]

Paramètres

- Lorsque vous supprimez les utilisateurs de Citrix Cloud, les noms d'utilisateur supprimés continuent d'apparaître dans Citrix ADM dans **Paramètres** > **Administration** des **utilisateurs > Utilisateurs**.
  [686581]

22 mars 2018

Cette version inclut de nouvelles fonctionnalités et corrections de bugs.

Par défaut, les agents Citrix ADM sont automatiquement mis à niveau vers la version 511.118. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour plus de détails, consultez Configuration des paramètres de mise à niveau de l'agent.

Nouveautés

Présentation du centre d'aide dans Citrix ADM

Citrix ADM dispose désormais d'un centre d'aide qui vous permet d'accéder aux liens pour les différentes tâches que vous pourriez effectuer. Par exemple, vous pouvez apprendre à embarquer Citrix ADM pour la première fois. Vous pouvez également consulter les dernières notes de mise à jour ou apprendre comment gérer vos abonnements.

[706025]

Configuration d'instances Citrix ADC en tant que proxy ADFS à l'aide d'un StyleBook

Vous pouvez désormais configurer une instance Citrix ADC pour qu'elle fonctionne en tant que proxy inverse pour Active Directory Federation Services (ADFS 2.0) à l'aide de StyleBooks. L'instance de Citrix ADC peut désormais étendre l'expérience d'authentification unique (SSO) pour les clients authentifiés Active Directory aux ressources situées en dehors du centre de données d'entreprise. L'instance peut désormais prendre en charge l'authentification ADFS active et passive. Pour de plus amples informations, consultez la section Microsoft ADFS Proxy StyleBook.

[696203]

Améliorations du tableau de bord de l'instance

Le tableau de bord par instance dans Citrix ADM affiche les données interrogées à partir d'une instance spécifique. Par défaut, chaque minute, les instances gérées sont interrogées pour la collecte de données. Des 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 permanence à l'aide d'appels NITRO. En tant qu'administrateur, vous pouvez afficher toutes ces données collectées sur une seule page. Vous pouvez également 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 >** (Type d'instance). Sélectionnez l'instance à afficher et cliquez sur **Tableau de bord**.

L'onglet **Vue d'ensemble** qui affiche l'UC, l'utilisation de la mémoire et les événements d'une instance spécifique. Vous pouvez afficher d'autres tableaux de bord spécifiques à une instance pour obtenir des informations plus détaillées sur votre instance. Les autres onglets sont : SSL, audit de configuration, fonctions réseau et utilisation du réseau.

[687676]

Améliorations de l'inventaire réseau

Vous pouvez maintenant afficher la liste complète des instances gérées par Citrix ADM. Vous pouvez afficher le rapport d'inventaire en accédant à **Réseaux > Tableau de bord** et en cliquant sur **Toutes les instances** dans le coin supérieur droit de votre écran. Le nouvel état d'inventaire affiche les informations suivantes :

- Toutes les instances
- Versions d'instance
- Numéros de série

[687676]

Indicateur de progression des sondages

Vous pouvez maintenant afficher l'état de votre action d'interrogation pour les instances sur Citrix ADM. Auparavant, lorsque vous choisissez l'action **Interroger maintenant** (par exemple les certificats, les audits de configuration et la découverte), l'interface graphique affichait uniquement lorsque l'interrogation était lancée. Maintenant, vous pouvez voir la progression de l'interrogation, quand elle est en cours et si elle est terminée, ainsi que les informations extraites de l'instance pendant l'action d'interrogation.

Pour de plus amples informations, consultez la section Interrogation des instances et entités Citrix ADC.

[688916]

Problèmes résolus

- Sur la page **Paramètres > Abonnements**, la consommation de données de stockage peut apparaître supérieure à la limite de stockage autorisée de 5 Go.
  [689330]
- Vous ne pouvez pas mettre à niveau les instances SD-WAN WO ou Citrix ADC SDX Citrix à partir de Citrix ADM 506.119 build.
  [699814]
- La barre de navigation Citrix Cloud n'est pas visible lorsque vous ouvrez une session à l'aide d'Internet Explorer 11.
  [702339]

Problèmes connus

Réseaux

- Dans Citrix ADM, lorsque vous accédez à Réseaux > Événements > Messages Syslog, les messages les plus anciens sont affichés en premier, bien que la fenêtre Trier affiche l'option « Nouveau en

premier ». Seulement lorsque vous sélectionnez « Le plus ancien d'abord », puis sélectionnez « Le plus récent d'abord », les messages s'affichent correctement.
[702305]

Analytics

- Dans certains cas, les nœuds HDX Insight et Citrix Gateway Insight peuvent ne pas être affichés sur l'interface graphique graphique Citrix ADM.
  Solution : actualisez la page et réessayez.
  [690327]

Paramètres

- Lorsque vous supprimez les utilisateurs de Citrix Cloud, les noms d'utilisateurs supprimés continuent d'apparaître dans Citrix ADM dans **Paramètres** > **Administration** des **utilisateurs > Utilisateurs**.
  [686581]

mars 3, 2018

Cette version inclut de nouvelles fonctionnalités et corrections de bugs.

Par défaut, les agents Citrix ADM sont automatiquement mis à niveau vers la version 510.120. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour plus de détails, consultez Configuration des paramètres de mise à niveau de l'agent.

Nouveautés

Tableau de bord amélioré des rapports réseau

Vous pouvez désormais créer des tableaux de bord personnalisés avec plusieurs widgets qui affichent différentes données de reporting. Vous pouvez afficher plusieurs rapports pour n'importe quel nombre de serveurs virtuels et jusqu'à dix instances sur votre tableau de bord personnalisé. Vous pouvez également personnaliser la durée de vos rapports et les exporter pour une analyse plus approfondie. Pour de plus amples informations, consultez la section Rapports réseau.

[702016]

Personnaliser la durée du rapport

Vous pouvez désormais utiliser le curseur pour personnaliser la durée des rapports générés sur l'interface graphique Citrix ADM. Auparavant, vous étiez en mesure de générer et d'afficher des

rapports pendant une heure, un jour, une semaine ou un mois. Pour de plus amples informations, consultez la section Rapports réseau.

[666018]

Nouveaux rapports réseau

Vous pouvez désormais générer et exporter des rapports de performances pour chaque interface de l'instance d'Citrix ADC sélectionnée. Les données de performances collectées sont basées sur les compteurs sélectionnés et les données transmises et reçues par l'instance de Citrix ADC. Pour de plus amples informations, consultez la section Rapports réseau.

[683417]

Vous pouvez désormais générer des rapports pour les instances Citrix ADC sélectionnées pour le débit et la bande passante. À l'aide des rapports de débit générés, vous pouvez surveiller les données de rapports réseau pour chaque instance spécifique dans le tableau de bord Network Reporting. Pour de plus amples informations, consultez la section Rapports réseau.

[687555]

Déploiement de la suite Oracle E-Business sur des instances de Citrix ADC à l'aide de StyleBook

Vous pouvez désormais utiliser StyleBooks pour définir le processus de déploiement d'équilibrage de charge pour Oracle E-Business Suite 12.2 avec Citrix ADC. La configuration de l'équilibrage de charge consiste en la définition des serveurs et services virtuels d'équilibrage de charge liés aux serveurs virtuels LB et liés aux serveurs Oracle E-Business Suite individuels. Pour de plus amples informations, consultez la section Oracle e-business StyleBook.

[679553]

Intégration de StyleBooks avec le tableau de bord de l'application pour créer des configurations sur des instances de Citrix ADC

Citrix ADM vous permet désormais de créer des applications personnalisées à l'aide de StyleBooks personnalisés ou par défaut. StyleBooks simplifie la tâche de gestion des configurations Citrix ADC complexes pour vos applications. Ainsi, lorsque vous définissez des applications personnalisées sur la page du tableau de bord de l'application, vous pouvez désormais sélectionner un StyleBook présent dans Citrix ADM. Citrix ADM crée ensuite la configuration sur les instances Citrix ADC cibles en fonction du StyleBook sélectionné. Citrix ADM crée également une application personnalisée composée de tous les serveurs virtuels du pack de configuration.

> **Remarque**
>
> Une application personnalisée et un pack de configuration sont créés si des licences Citrix ADM suffisantes sont disponibles et si la licence de serveur virtuel n'est pas définie sur manuelle. Pour de plus amples informations, consultez la section Créer une définition d'application.

[684460]

Possibilité de migrer des packs de configuration existants vers un autre StyleBook

Citrix ADM vous permet désormais de migrer (ou de mettre à niveau) votre pack de configuration vers un nouveau StyleBook sans supprimer et recréer le pack de configuration. Cette fonctionnalité vous permet de conserver toutes les configurations sur les instances cibles.

Considérez que les paramètres du nouveau StyleBook sont un surensemble de ceux du StyleBook existant. Ensuite, Citrix ADM peut migrer votre pack de configuration vers le nouveau StyleBook sans avoir à saisir à nouveau des valeurs de paramètre.

> **Remarque**
>
> Ceci suppose que tous les nouveaux paramètres faisant partie du nouveau StyleBook sont facultatifs.

Pendant la migration, Citrix ADM effectue une différence de configuration entre la configuration existante et la nouvelle configuration générée par le nouveau StyleBook. Citrix ADM décide ensuite quels objets de configuration doivent être ajoutés, supprimés ou mis à jour sur les instances Citrix ADC cibles.

Il n'y a aucune restriction dans la migration de votre config pack entre deux StyleBooks dans Citrix ADM. Vous pouvez également rétablir le pack de configuration migré vers le précédent StyleBook. Pour de plus amples informations, consultez la section Migrer le pack de configuration d'un StyleBook vers un autre StyleBook.

[699789]

Afficher l'ID de règle de signature dans le rapport Security Insight

Le rapport Security Insight pour les violations de signature inclut désormais l'ID de règle de chaque signature.

Pour de plus amples informations, consultez la section Security Insight.

[701416]

Problèmes résolus

Analytics

- L'augmentation des appels NITRO fait que Citrix ADM cesse de répondre.
  [696032]

Réseaux

- Citrix ADM n'affiche pas le nombre de fichiers de sauvegarde dans la page Paramètres de sauvegarde système.
  [703421]
- Un message d'avertissement s'affiche aux utilisateurs avant la soumission, lorsque plus de serveurs virtuels autorisés sont sélectionnés sous **Réseaux** > **Paramètres de licence** > **Licences système**.[687058]

Problèmes connus

Réseaux

- Dans Citrix ADM, lorsque vous accédez à Réseaux > Événements > Messages Syslog, les messages les plus anciens sont affichés en premier, bien que la fenêtre Trier affiche l'option « Nouveau en premier ». Seulement lorsque vous sélectionnez « Le plus ancien d'abord », puis sélectionnez « Le plus récent d'abord », les messages s'affichent correctement.
  [702305]

Analytics

- Dans certains cas, les nœuds HDX Insight et Citrix Gateway Insight peuvent ne pas être affichés sur l'interface graphique graphique Citrix ADM.
  Solution : actualisez la page et réessayez.
  [690327]

Paramètres

- Sur la page **Paramètres** > **Abonnements**, la consommation de données de stockage peut apparaître supérieure à la limite de stockage de 5 Go.
  [689330]
- Lorsque vous supprimez les utilisateurs de Citrix Cloud, les noms d'utilisateurs supprimés continuent d'apparaître dans Citrix ADM dans **Paramètres** > **Administration** des **utilisateurs > Utilisateurs**.
  [686581]
- Vous ne pouvez pas mettre à niveau les instances Citrix SD-WAN WO ou Citrix ADC SDX Citrix à partir de Citrix ADM.
  [699814]

Problème d'interface graphique

- La barre de navigation Citrix Cloud n'est pas visible lorsque vous ouvrez une session à l'aide d'Internet Explorer 11.
  [702339]

9 février 2018

Cette version inclut de nouvelles fonctionnalités et corrections de bugs.

Par défaut, les agents Citrix ADM sont automatiquement mis à niveau vers la version 509.119. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour plus de détails, consultez Configuration des paramètres de mise à niveau de l'agent.

Nouveautés

Améliorations du tableau de bord des applications

Dans l'interface graphique Citrix ADM, les modifications suivantes ont été apportées pour améliorer la convivialité du tableau de bord de l'application :

1. Le score d'*application 0* représente le nombre de serveurs virtuels d'application qui sont en panne ou hors service. Ce score d'*application 0* fait désormais partie de la légende de score d'application existante en mode Tableau de bord d'application.
2. Le panneau récapitulatif de l'application affiche désormais le texte "*Affichage des applications N/N*" au lieu du précédent "*Total des applications N/N*." Prenons un exemple où vous choisissez 60 dans le graphique de score de l'application. Il y a 16 applications sur un total de 26 qui ont un score d'application compris entre 40 et 60. Le panneau récapitulatif de l'application affiche "*Affichage 16/26 Applications*." Si aucun critère n'est sélectionné, le panneau récapitulatif de l'application affiche "*Affichage de 26/26 Applications*."
3. Le panneau récapitulatif de l'application affiche désormais un nouveau graphique pour filtrer les applications en fonction des catégories applicables. Un nouveau graphique de catégories d'application est ajouté au panneau récapitulatif de l'application. Ce graphique affiche un histogramme pour toutes les catégories définies dans Citrix ADM. Toutes les applications discrètes apparaissent désormais sous la catégorie "*Autres*" et les applications personnalisées apparaissent sous leur nom de catégorie respectif. Ces noms de catégorie sont attribués lors de la définition d'applications personnalisées.

Pour de plus amples informations, consultez la section Analyse et gestion des applications.

[695980]

Possibilité de sélectionner l'état du serveur virtuel d'équilibrage de charge et le pourcentage d'intégrité en tant que paramètre pour filtrer les applications

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 regroupées pour avoir la valeur de santé comprise entre 0 % et 100 %.

L'intégrité du serveur virtuel représente l'intégrité des serveurs virtuels regroupés sous des applications discrètes. 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.

Pour de plus amples informations, consultez la section Analyse et gestion des applications.

[694425]

Agent Citrix ADM intégré dans une instance de Citrix ADC

Les instances Citrix ADC exécutant la version 12.0 build 56.20 et versions ultérieures incluent un agent intégré Citrix ADM. Cet agent active la communication entre l'instance et Citrix ADM. Vous n'avez pas besoin d'installer un agent externe.

Les fonctionnalités de gestion, de surveillance et de tableau de bord des applications sont prises en charge pour les instances de Citrix ADC à l'aide d'agents intégrés. Les fonctionnalités suivantes ne sont pas prises en charge : Web Insight, SSL Insight, HDX Insight, Citrix Gateway Insight, Security Insight et Intelligent App Analytics.

Pour utiliser cet agent intégré, vous devez mettre à niveau votre instance Citrix ADC vers la version 12.0 build 56.20 et lancer l'agent.

> **Remarque**L'agent
>
> intégré est disponible uniquement sur les types d'instance Citrix ADC suivants :
>
> - Appliance Citrix ADC MPX
> - Appliance Citrix ADC VPX
> - Citrix Gateway
> - Citrix Secure Web Gateway

Pour plus d'informations et d'instructions sur l'utilisation de l'agent intégré, consultez les articles suivants :

- Prise en main de Citrix ADM
- Lancer l'agent intégré

[694701]

Prise en charge de Web Insight

Citrix ADM prend désormais en charge Web Insight. La fonctionnalité Web Insight offre une visibilité sur les applications Web d'entreprise. Il permet aux administrateurs informatiques de surveiller toutes les applications Web desservies par l'Citrix ADC en fournissant une surveillance intégrée et en temps réel des applications. Pour de plus amples informations, consultez la section Web Insight.

Web Insight traite les données à partir de Citrix ADC à l'aide d'un algorithme d'approximation. Il fournit les 1 000 enregistrements les plus importants des mesures liées aux applications Web de votre entreprise.

[688206]

Prise en charge des informations SSL

Citrix ADM prend désormais en charge SSL Insight. La fonctionnalité SSL Insight fournit une visibilité sur les transactions sécurisées sur le Web (HTTPS). Il permet aux administrateurs informatiques de surveiller toutes les applications Web desservies par l'Citrix ADC en fournissant une surveillance intégrée, en temps réel et historique des transactions Web. Pour de plus amples informations, consultez la section SSL Insight.

SSL insights traite les données de Citrix ADC à l'aide d'un algorithme d'approximation. Il fournit les 1 000 enregistrements les plus importants des mesures liées aux transactions Web dans votre entreprise.

[688206]

Prise en charge des enregistrements d'authentification SAML dans Citrix Gateway Insight

Citrix Gateway Insight fournit désormais des informations sur les échecs d'authentification SAML. Vous pouvez afficher les échecs d'authentification SAML sous l'onglet **Authentification** de la page **Analytics > Citrix Gateway Insight > Vue d'ensemble** .

[634094]

Possibilité d'ajouter des instances Citrix ADC aux sites en fournissant des informations de localisation

Citrix ADM vous permet désormais d'ajouter des instances de Citrix ADC et de les associer à des sites. Lors de la découverte d'une instance, vous pouvez créer un site ou sélectionner un site existant. Fournissez les détails de l'agent Citrix ADM et associez toujours l'agent au site.

Pour ajouter une instance :

1. Accédez à **Réseaux** > **Instances**.

2. Sélectionnez le type d'instance Citrix ADC et cliquez sur **Ajouter**.
3. Entrez l'adresse IP et sélectionnez le profil.
4. Sélectionnez le site et l'agent.
5. Cliquez sur l'icône de modification en regard du champ Agent.
6. Sélectionnez l'agent, cliquez sur **Joindre le site**, puis sélectionnez le site requis.
7. Cliquez sur **OK**.

L'instance est désormais associée au site. Accédez au tableau de bord Réseaux pour afficher les instances nouvellement ajoutées sous le site associé.

Pour de plus amples informations, consultez la section Comment surveiller les sites distribués à l'échelle mondiale.

[702019]

Possibilité de découvrir des instances Citrix ADC avec la même adresse IP privée

Vous pouvez désormais découvrir des instances Citrix ADC avec les mêmes adresses IP privées sur différents réseaux lorsque des instances sont enregistrées à l'aide de l'agent intégré à l'aide de Citrix ADM.

[699962]

Problèmes résolus

Réseaux

- Des valeurs incorrectes pour les clés DH (Diffie-Hellman) et Ephemeral RSA sont affichées si un profil SSL portant des propriétés différentes est attaché à un serveur virtuel SSL. Les valeurs sont affichées correctement uniquement pour les adresses IP de serveur virtuel SSL qui n'ont pas de profil SSL.
  [702680]
- Les entrées de service ou de groupe de services en double sont affichées pour chaque service ou groupe de services de partition après un basculement vers Citrix ADC. Ce problème ne se produit pas avec les services ou les groupes de services qui appartiennent à la partition par défaut.
  [699224]

Problèmes connus

Analytics

- Dans certains cas, les nœuds HDX Insight et Citrix Gateway Insight peuvent ne pas être affichés sur l'interface graphique graphique Citrix ADM.

Solution : actualisez la page et réessayez.
[690327]

Paramètres

- Sur la page **Paramètres** > **Abonnements**, la consommation de données de stockage peut apparaître supérieure à la limite de stockage de 5 Go.
  [689330]
- Lorsque vous supprimez les utilisateurs de Citrix Cloud, les noms d'utilisateurs supprimés continuent d'apparaître dans Citrix ADM dans **Paramètres** > **Administration** des **utilisateurs > Utilisateurs**.
  [686581]
- Vous ne pouvez pas mettre à niveau les instances Citrix SD-WAN WO ou Citrix ADC SDX Citrix à partir de Citrix ADM.
  [699814]

Problème d'interface graphique

- La barre de navigation Citrix Cloud n'est pas visible lorsque vous ouvrez une session à l'aide d'Internet Explorer 11.
  [702339]

Janvier 18, 2018

Cette version inclut de nouvelles fonctionnalités et corrections de bugs.

Par défaut, les agents Citrix ADM sont automatiquement mis à niveau pour générer 508.116. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour plus de détails, consultez Configuration des paramètres de mise à niveau de l'agent.

Nouveautés

Importer un certificat à partir d'une instance Citrix ADC spécifique

Vous pouvez désormais importer un certificat à partir d'une instance d'Citrix ADC spécifique et l'appliquer à d'autres instances d'ADC Citrix ciblées à partir de l'interface graphique d'Citrix ADM. Avec cette amélioration, vous n'avez pas besoin de télécharger le certificat sur votre système local, puis d'appliquer le certificat téléchargé aux instances sélectionnées. Pour de plus amples informations, consultez la section Comment faire pour installer des certificats SSL sur une instance de Citrix ADC.

[688029]

Afficher les rapports réseau pour plusieurs instances Citrix ADC

Citrix ADM vous permet de choisir plusieurs instances Citrix ADC (et jusqu'à cinq serveurs virtuels) tout en générant un rapport réseau. Vous pouvez désormais surveiller simultanément les données de rapports réseau pour plusieurs instances.

Vous pouvez également exporter et planifier le rapport généré à partir de la fonctionnalité **Network Reporting** sur Citrix ADM. Pour de plus amples informations, consultez la section Rapports réseau.

[665989]

Mise à niveau de l'instance Citrix ADC en mode haute disponibilité

Le processus de mise à niveau de vos instances Citrix ADC en mode Haute disponibilité à partir de Citrix ADM a été amélioré. Vous pouvez créer une tâche de maintenance pour mettre à niveau la paire HA en deux étapes. Vous pouvez d'abord planifier ou effectuer la mise à niveau sur le nœud initial, puis planifier la mise à niveau pour le deuxième nœud ultérieurement. L'administrateur ne peut procéder à la mise à niveau du deuxième nœud que si la mise à niveau du premier nœud est réussie.

> **Remarque**
>
> - Actuellement, le deuxième nœud de la paire HA est mis à niveau en premier, et la mise à niveau pour le premier nœud est planifiée ultérieurement.
> - La synchronisation et la propagation des nœuds sont désactivées jusqu'à ce que les deux nœuds soient mis à niveau correctement.
> - Vous voyez un avertissement si vos nœuds de la paire HA sont sur des versions ou versions différentes lorsque le premier nœud est en cours de mise à niveau. Vous pouvez annuler le processus de mise à niveau pour le deuxième nœud jusqu'à ce qu'ils soient dans la même version et version. Ou vous pouvez le programmer pour une heure ultérieure, une fois que les nœuds sont dans la même version et version.

Pour de plus amples informations, consultez la section Procédure de mise à niveau des instances Citrix ADC.

[694907]

Afficher les entités liées pour les serveurs

Vous pouvez désormais afficher les entités liées sur vos instances Citrix ADC gérées pour un serveur spécifique. Vous pouvez maintenant voir ce qui suit :

1. Vous pouvez désormais afficher les services liés et les groupes de services liés pour un serveur d'équilibrage de charge sélectionné.

   Accédez à **Réseaux** > **Fonctions réseau** > **Équilibrage de charge** > **Serveurs** . Sélectionnez un serveur, puis cliquez sur **Afficher les services liés** ou **Afficher les groupes de services liés**

. Sur la page Services liés, vous pouvez activer ou désactiver le service et interroger l'entité. De même, sur la page Groupes de services liés, vous pouvez activer ou désactiver le groupe de services, afficher les membres du groupe de services liés et interroger l'entité.

2. Vous pouvez afficher les serveurs virtuels LB liés pour un serveur sur un serveur virtuel Commutation de contenu.

   Accédez à **Réseaux** > **Fonctions réseau** > **Commutation de contenu** . Sélectionnez un serveur, puis cliquez sur **Afficher les serveurs virtuels LB liés**. Sur la page Serveurs LB liés, vous pouvez activer ou désactiver le serveur virtuel et l'interroger.

   > **Remarque** Lorsque vous sélectionnez un serveur virtuel Content Switching, puis cliquez sur **Afficher le serveur virtuel LB lié** . Citrix ADM répertorie le serveur LB par défaut et le serveur virtuel LB cible basé sur des stratégies.

3. Vous pouvez afficher les serveurs virtuels LB cible liés pour un serveur sur un serveur virtuel de redirection de cache.

   Accédez à **Réseaux** > **Fonctions réseau** > **Redirection du cache** . Une nouvelle colonne **Serveur virtuel LB cible** s'affiche sur la page Serveurs virtuels de redirection de cache qui répertorie le nom du serveur virtuel LB cible.

[698772]

Afficher les détails du débit pour les serveurs virtuels sous licence

Vous pouvez gérer et allouer des licences à vos serveurs virtuels en fonction des détails de débit (c'est-à-dire la somme des octets de demande et des octets de réponse). Ceci s'affiche sous la forme d'une colonne sur la page **Licences système** . Vous pouvez trier la colonne **Débit** pour voir quel serveur virtuel utilise moins ou plus de débit et allouer les licences en conséquence.

Pour afficher les détails du débit :

1. Accédez à **Réseaux** > **Licences** > **Licences système** .
2. Dans la page **Licences système**, sous **Serveurs virtuels gérés**, vérifiez que l'option **Sélection automatique des Serveurs virtuels** est **désactivée** . Vous pouvez désormais sélectionner explicitement les serveurs virtuels que vous souhaitez gérer.
3. Pour choisir des serveurs virtuels, sélectionnez **Cliquez pour sélectionner**.
4. Sur la page **Choisir des serveurs virtuels**, vous pouvez désormais voir les détails du débit sous la forme d'une colonne sous chaque onglet serveur virtuel.

[687056]

Nouveau flux de configuration pour la configuration des agents et l'ajout d'instances de Citrix ADC

Citrix ADM fournit désormais une nouvelle interface graphique intuitive permettant de configurer les agents Citrix ADM et d'ajouter des instances Citrix ADC à Citrix ADM. Pour de plus amples informations, consultez la section Mise en route.

[700033]

Prise en charge du SDK Python pour StyleBooks

Dans Citrix ADM, le SDK Python prend désormais en charge les appels NITRO pour StyleBooks.

[672420]

Afficher des informations supplémentaires sur les instances Citrix ADC

Vous pouvez désormais afficher des informations sur les paramètres suivants de l'instance de Citrix ADC sur Citrix Citrix ADM.

- **ID du modèle** : affiche l'ID du modèle dérivé du type de licence appliqué à une instance de Citrix ADC. Vous pouvez afficher l'ID du modèle dans la page Instances et dans le tableau de bord de l'instance.
- **ID d'hôte** : affiche l'ID d'hôte, qui est l'ID Mac d'une instance de Citrix ADC. L'ID d'hôte est utilisé pour générer la licence de l'instance. Vous pouvez afficher l'ID d'hôte sur la page Instances et sur le tableau de bord de l'instance.
- **UUID NetScaler** : Unique Identificateur (UUID) qui identifie des périphériques Internet ou des données uniques. Un algorithme génère l'UUID à l'aide de valeurs basées sur l'adresse réseau de l'instance. Vous pouvez afficher l'UUID NetScaler dans le tableau de bord de l'instance.
- **CPU** : Affiche la fréquence actuelle du CPU. Les CPU fonctionnent à différentes fréquences en fonction de la capacité de charge. L'augmentation/diminution de MHz est déterminée par le processeur, l'architecture de la carte mère et la température. Vous pouvez afficher les détails d'utilisation de l'UC dans le tableau de bord de l'instance.
- **Fabriqué le** : affiche la date de fabrication d'une instance de Citrix ADC dans le tableau de bord de l'instance.

> **Remarque** Par défaut, l'ID de modèle et l'ID d'hôte d'une instance ne s'affichent pas sur la page Instance.

Pour afficher les nouveaux paramètres :

1. Accédez à **Réseaux** > **Instances** et sélectionnez le type d'instance Citrix ADC pour lequel vous souhaitez afficher les informations relatives aux paramètres.
2. Pour afficher l'ID de modèle et l'ID d'hôte :
    a) Dans le coin supérieur droit, cliquez sur l'icône **Paramètres** en regard de **Rechercher** .

b) Sélectionnez ID de modèle et ID d'hôte, puis cliquez sur **Terminé**.
Les valeurs ID de modèle et ID d'hôte sont affichées comme illustré dans l'image suivante.

c) Pour afficher l'ID d'hôte, l'UUID NetScaler, l'UC et la date de fabrication dans le tableau de bord :

i. Sélectionnez l'instance et cliquez sur **Tableau de bord**.

ii. Dans la section **Informations**, vous pouvez afficher les détails de **Model ID**, **Host ID**, **NetScaler UUID**, **CPU** et **Fabriqué sur** comme illustré dans l'image suivante.

[699550, 700266]

Problèmes résolus

Analytics

- Lors de l'accès aux rapports de session dans HDX Insight, Citrix ADM échoue par intermittence. [701042]

Réseaux

- Lorsque des requêtes proxy API de périphérique sont envoyées à Citrix ADM, il renvoie Content-Length et Transfer-Encoding dans l'en-tête de réponse, ce qui est contraire à la RFC 2616. [700717]
- Actuellement, les autorisations pour certaines ressources dépendantes (ns_lbvserver, ns_csvserver, etc.) sont accordées dans le cadre de l'autorisation de fonctionnalité Network Reporting. Mais dans le cadre de la nouvelle amélioration, ces autorisations ne doivent être accordées que si les utilisateurs ont accès au nœud correspondant sous Fonctions réseau. Par exemple, si les utilisateurs souhaitent exécuter les rapports sur les serveurs virtuels d'équilibrage de charge, ils doivent avoir accès uniquement aux serveurs virtuels d'équilibrage de charge sous Fonctions réseau et vice versa.
[700859]

Problèmes connus

Analytics

- Dans certains cas, les nœuds HDX Insight et Citrix Gateway Insight peuvent ne pas être affichés sur l'interface graphique graphique Citrix ADM.
Solution : actualisez la page et réessayez.
[690327]

Paramètres

- Sur la page **Paramètres** > **Abonnements**, la consommation de données de stockage peut apparaître supérieure à la limite de stockage de 5 Go.
  [689330]
- Lorsque vous supprimez les utilisateurs de Citrix Cloud, les noms d'utilisateurs supprimés continuent d'apparaître dans Citrix ADM dans **Paramètres** > **Administration** des **utilisateurs > Utilisateurs**.
  [686581]
- Vous ne pouvez pas mettre à niveau les instances Citrix SD-WAN WO ou Citrix ADC SDX Citrix à partir de Citrix ADM.
  [699814]

Décembre 28, 2017

Cette version inclut de nouvelles fonctionnalités et corrections de bugs.

Par défaut, les agents Citrix ADM sont automatiquement mis à niveau vers la version 507.114. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour plus de détails, consultez Configuration des paramètres de mise à niveau de l'agent.

Nouveautés

Configuration des stratégies d'accès pour RBAC sur Citrix ADM pour les sous-nœuds de fonctions réseau

La gestion des stratégies d'accès pour le contrôle d'accès basé sur les rôles (RBAC) dans Citrix ADM vous permet désormais de configurer les autorisations pour les sous-nœuds de fonctions réseau également. Les paramètres de stratégie d'accès peuvent être configurés pour tous les sous-nœuds tels que les serveurs virtuels, les services, les groupes de services et les serveurs. Actuellement, vous pouvez fournir une telle autorisation d'accès de niveau granulaire uniquement pour les sous-nœuds sous le nœud d'équilibrage de charge et aussi pour les sous-nœuds sous le nœud GSLB. Pour plus d'informations, consultez Configuration des stratégies d'accès sur Citrix Application Delivery Management.

[692034]

Possibilité d'exporter et de planifier des rapports pour les fonctions réseau sélectionnées

Vous pouvez générer un rapport complet pour certaines fonctions réseau, telles que l'équilibrage de la charge, la commutation de contenu, la redirection de cache, l'équilibrage de la charge de serveur global (GSLB), l'authentification et Citrix Gateway dans Citrix ADM. Ce rapport vous permet d'avoir

une vue de haut niveau du mappage entre les instances d'Citrix ADC, les partitions et les entités liées correspondantes (serveurs virtuels, groupes de services et services) présentes dans le réseau. Vous pouvez exporter ces rapports au format de fichier .csv.

Le rapport affiche les données de serveur virtuel suivantes :

- Adresse IP de NetScaler
- Nom d'hôte
- Données de partition
- Type de serveur virtuel
- Nom du serveur virtuel
- Serveur virtuel LB cible
- Nom du service
- Nom du groupe de services.

Pour plus d'informations, voir Procédure d'exportation ou de planification de l'exportation des rapports de fonctions réseau.

[696259]

Importation de StyleBooks à l'aide de fichiers ou de paquets ZIP

Citrix ADM vous permet d'importer plusieurs StyleBooks au format YAML. Vous pouvez compresser plusieurs fichiers YAML StyleBook au format zip (.zip) ou tarball (.tgz, .gz). Pour de plus amples informations, consultez la section Procédure d'utilisation de StyleBooks définis par l'utilisateur.

[694938]

Exclusion des certificats Citrix ADC par défaut dans le tableau de bord SSL

Citrix ADM vous permet d'afficher ou de masquer les certificats Citrix ADC par défaut s'affichant sur les graphiques SSL Dashboard en fonction de vos préférences. 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 graphique Citrix ADM.
2. Sur la page **Tableau de bord SSL**, cliquez sur **Paramètres**.
3. Dans la page **Paramètres**, cliquez sur l'icône Modifier.
4. Dans la section **Paramètres du filtre de certificat**, désactivez la case à cocher **Afficher les certificats par défaut** .

Pour plus d'informations, consultez Exclusion des certificats Citrix ADC par défaut sur le tableau de bord SSL.

[687609]

Problèmes résolus

Réseaux

- Pour créer une tâche de configuration à l'aide de modèles définis par l'utilisateur à partir de la liste de modèles, vous devez faire glisser les modèles vers l'éditeur et modifier les variables en fournissant de nouvelles valeurs. Mais lorsque le travail de configuration est exécuté, les variables ne sont pas remplacées par les nouvelles valeurs fournies par vous. [698812]
- Dans Citrix ADM, lorsque l'âge de l'événement est défini dans une règle pour un événement, ces événements ne sont pas visibles dans l'interface graphique. En outre, comme les entités EntityUp, EntityDown et EntityOFS sont corrélées, elles doivent être mises à jour pour le même événement. Mais ces pièges sont vus séparément dans les messages d'événement. [699487]
- Lorsque Citrix ADM exporte les rapports HDX Insight, la valeur de bande passante du canal n'est pas correcte. [700011]
- Citrix ADM affiche un message dans Events indiquant toujours que les licences expirent dans les 30 prochains jours, bien que les licences expirent avant cela. [696976]

Problèmes connus

Analytics

- Dans certains cas, les nœuds HDX Insight et Citrix Gateway Insight peuvent ne pas être affichés sur l'interface graphique graphique Citrix ADM.

Solution : actualisez la page et réessayez. [690327]

Réseaux

- Actuellement, les autorisations pour certaines ressources dépendantes (`ns\\_lbvserver`, `ns\\_csvserver etc`) sont données dans le cadre de l'autorisation de fonctionnalité Network Reporting. Mais dans le cadre de la nouvelle amélioration, ces autorisations ne doivent être accordées que si les utilisateurs ont accès au nœud correspondant sous Fonctions réseau. Par exemple, si les utilisateurs souhaitent exécuter les rapports sur les serveurs virtuels d'équilibrage de charge, ils doivent avoir accès uniquement aux serveurs virtuels d'équilibrage de charge sous Fonctions réseau et vice versa. [700859]

Paramètres

- Sur la page **Paramètres** > **Abonnements**, la consommation de données de stockage peut apparaître supérieure à la limite de stockage de 5 Go. [689330]
- Lorsque vous supprimez les utilisateurs de Citrix Cloud, les noms d'utilisateurs supprimés continuent d'apparaître dans Citrix ADM dans **Paramètres** > **Administration** des **utilisateurs > Utilisateurs**. [686581]

- Vous ne pouvez pas mettre à niveau les instances SD-WAN WO ou Citrix ADC SDX Citrix à partir de Citrix ADM 506.119 build. [699814]

07 décembre 2017

Cette version inclut de nouvelles fonctionnalités et corrections de bugs.

Par défaut, les agents Citrix ADM sont automatiquement mis à niveau vers la version 506.122. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour plus de détails, consultez Configuration des paramètres de mise à niveau de l'agent.

Nouveautés

Améliorations apportées au Multicloud GLB StyleBook pour prendre en charge le déploiement parent-enfant et les algorithmes GLB basés sur les statistiques

La solution d'équilibrage de charge globale (GLB) permet aux utilisateurs de distribuer les demandes des clients sur plusieurs centres de données et serveurs d'applications. Les centres de données sont distribués sur plusieurs clouds et les serveurs d'applications sont déployés sur site. Cette solution prend en charge les fonctionnalités suivantes :

- Topologie parent-enfant. La topologie est utilisée lorsque des algorithmes GLB basés sur des statistiques sont utilisés pour configurer des nœuds GLB et LB. Cette topologie est également utilisée si les nœuds LB sont déployés sur une autre instance Citrix ADC.
- La persistance des débordements. Le serveur virtuel de sauvegarde continue de traiter les demandes qu'il reçoit, même après que la charge sur le principal soit inférieure au seuil.
- Protocole Internet version 6 (IPv6).
- Méthodes GLB basées sur les paramètres métriques, non métriques et basées sur la proximité.

Utilisez le « Multi-cloud GLB StyleBook » version 1.1 pour exécuter la configuration GLB sur l'instance GLB Citrix ADC sélectionnée. Utilisez le Multi-Cloud GLB StyleBook for LB Node pour configurer un nœud LB à la fois afin de créer une topologie parent-enfant GLB dans l'un des cas suivants :

- Si vous utilisez les algorithmes GLB basés sur des métriques (moindres paquets, moins de connexions, moins de bande passante) pour configurer les nœuds GLB et LB
- Si les nœuds LB sont déployés sur une autre instance Citrix ADC
- Si vous souhaitez configurer la persistance du site

Vous pouvez configurer jusqu'à 1024 sites enfants.

Pour de plus amples informations, consultez la section Équilibrage global de charge Citrix ADC pour les déploiements hybrides et multi-cloud.

[694250]

Prise en charge de RBAC pour StyleBooks lors de la création de groupes

Citrix ADM vous permet d'ajouter des StyleBooks sélectionnés auxquels votre utilisateur peut accéder lors de la création de groupes d'utilisateurs.

Pour ajouter des StyleBooks sélectionnés à des groupes :

1. Dans Citrix ADM, accédez à **Système** > **Administration des utilisateurs** > **Groupes**.
2. Cliquez sur **Ajouter**.
3. Dans la zone **Nom du groupe**, tapez le nom du groupe et sélectionnez le rôle requis.
4. Dans l'onglet **Applications et modèles**, désactivez la case à cocher StyleBooks et sélectionnez les StyleBooks requis auxquels votre utilisateur peut accéder.
5. Dans l'onglet **Sélectionner** les utilisateurs, sélectionnez les utilisateurs à ajouter au groupe
6. Cliquez sur **Terminer**.

Pour de plus amples informations, consultez la section Configuration de groupes sur Citrix Application Delivery Management.

[657834, 664844]

Fournir une description pour les groupes

Dans Citrix ADM, lorsque vous créez des groupes, vous pouvez maintenant taper une description de votre groupe dans la zone **Description du groupe** . Fournir une bonne description du groupe. Une bonne description vous aide à mieux comprendre le rôle et la fonction du groupe à un moment ultérieur. Pour de plus amples informations, consultez la section Configuration de groupes sur Citrix Application Delivery Management.

[685186]

Intégration de Citrix ADM Intelligent App Analytics

La fonctionnalité Intelligent App Analytics de Citrix ADM surveille les serveurs virtuels et les services configurés pour une application et affiche des informations critiques à leur sujet. Cette fonctionnalité vous aide à surveiller, gérer et prendre des décisions lors d'interruptions et d'autres événements. Voici quelques fonctionnalités clés de Intelligent App Analytics :

- Utilise des algorithmes d'apprentissage automatique
- Apprend le comportement du trafic
- Distinction entre les modèles acceptables et les modèles non acceptables
- Fournit des informations claires aux administrateurs
- Permet aux administrateurs de prendre les mesures appropriées

Pour de plus amples informations, consultez la section Analyse intelligente des applications.

[698730]

Enregistrer automatiquement l'agent Citrix ADM dans AWS auprès de Citrix ADM

Vous pouvez désormais enregistrer automatiquement l'agent Citrix ADM auprès de Citrix ADM en fournissant les détails de l'URL de service et du code d'activation de Citrix ADM lors du déploiement de l'agent Citrix ADM dans Amazon Web Service (AWS). Pour de plus amples informations, consultez la section Installation de Citrix ADM Agent sur AWS.

[688901]

Audit de configuration lorsque Citrix ADM reçoit une interruption SNMP ChangeConfig

Lorsqu'une modification de configuration se produit dans une instance de Citrix ADC dans le réseau, l'instance met à jour la configuration. L'instance envoie ensuite une interruption SNMP ConfigChange à Citrix ADM. Vous pouvez activer Citrix ADM pour exécuter l'audit de configuration sur cette instance. Vous pouvez configurer Citrix ADM pour générer un diff d'audit de configuration, chaque fois qu'il reçoit une interruption SNMP ConfigChange. Pour de plus amples informations, consultez la section Comment générer un Diff d'audit de configuration pour les interruptions SNMP ConfigChange.

[682007]

Prise en charge de la planification des tâches de maintenance

Vous pouvez désormais planifier toutes les tâches de maintenance suivantes à une date et une heure spécifiques à l'aide de Citrix ADM.

- Mise à niveau des instances de Citrix ADC
- Mise à niveau des instances WAN-WO Citrix SD
- Mise à niveau des instances Citrix ADC SDX
- Configurer la paire HA d'instances Citrix ADC
- Convertir une paire d'instances HA en cluster

Vous pouvez également configurer la notification par e-mail lors de la planification de la tâche de maintenance. Une fois configuré, une notification par e-mail est envoyée chaque fois qu'une tâche est exécutée ou planifiée.

[681934]

Visualiseur/Éditeur YAML intégré pour afficher/créer des définitions StyleBook

Citrix ADM vous fournit un éditeur YAML intégré qui vous permet de composer votre StyleBook qui correspond aux instructions YAML. Le contenu est validé par rapport aux normes YAML et toute déviation est mise en évidence. Vous pouvez ensuite corriger le contenu et importer le StyleBook dans Citrix ADM. L'éditeur YAML intégré offre deux avantages lors de l'écriture de votre propre StyleBook :

- Code couleur. Le codage couleur du contenu vous aide à différencier facilement les clés et les valeurs définies dans le contenu YAML.
- Validation YAML. Le contenu est validé pour toute erreur YAML lorsque vous tapez et toute déviation est immédiatement mise en surbrillance.

Pour de plus amples informations, consultez la section Procédure d'utilisation de StyleBooks définis par l'utilisateur.

[695951]

Affichage de StyleBooks privés dans l'interface graphique Citrix ADM

Au fur et à mesure que le nombre de StyleBooks - publics et privés augmente, vous devez avoir la possibilité de rechercher le StyleBook particulier auquel vous souhaitez accéder. Vous devez également pouvoir afficher les deux types de StyleBooks séparément. Dans l'interface graphique Citrix ADM lorsque vous accédez à Applications > StyleBooks, vous pouvez afficher une liste de StyleBooks présents dans le système. Les deux types de StyleBooks ont des icônes distinctes qui les déclarent privés ou publics. Pour de plus amples informations, consultez la section Comment afficher différents groupes de StyleBooks.

[686913]

Intégration du tableau de bord de l'application

Dans Citrix ADM, la fonctionnalité d'analyse et de gestion des applications est étendue pour prendre en charge les applications HAProxy. Le tableau de bord Application fournit une vue complète de toutes les applications surveillées par Citrix ADM, c'est-à-dire les applications Citrix ADC et HAProxy. Les applications discrètes HaProxy sont créées automatiquement pour chaque frontal HaProxy géré. Vous pouvez également regrouper ces applications pour former des applications personnalisées similaires aux applications Citrix ADC.

> **Remarque**
>
> App Activity investigator n'est pas disponible pour les applications HAProxy. Pour de plus amples informations, consultez la section Applications HAProxy dans le tableau de bord des applications.

[693309]

Exportation de rapports du tableau de bord des applications et du tableau de bord de sécurité

Citrix ADM vous permet d'exporter les pages Tableau de bord des applications et Tableau de bord de sécurité sous forme de rapports.

1. Dans la page **Tableau de bord de l'application**, 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 est téléchargé sur votre système. Actuellement, vous pouvez télécharger les rapports d'une seule application à la fois. Pour de plus amples informations, consultez la section Exporter les rapports du tableau de bord de l'application et du tableau de bord de la sécurité.

[693753]

Configuration du score d'application dans Citrix ADM

Citrix ADM vous permet de configurer App Scores. Le calcul de l'App Score est basé sur les valeurs moyennes des trois composantes clés suivantes :

- Score de performance (score APDEX de l'application)
- Ressource d'instance Citrix ADC
- Ressource serveur

Les scores d'application sont affichés pour toutes les applications découvertes et les applications personnalisées que vous définissez dans le tableau de bord de l'application. Pour de plus amples informations, consultez la section Analyse des performances des applications.

[693758]

Affichage des détails de franchissement de seuil pour les composants AppScore sur App Activity Investigator

L'application Activity Investigator de l'onglet Tableau de bord affiche les informations clés d'une application sélectionnée, telles que les composants de l'application Score, les erreurs, les événements et les anomalies. Chacune des légendes est agrégée à un intervalle d'une minute si la durée sélectionnée est d'une heure, et à un intervalle d'une heure, 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.

[693769]

Création de seuils et configuration de règles et d'alertes pour HDX Insight

La gestion des seuils pour HDX Insight dans Citrix ADM vous permet de configurer de manière proactive les alertes chaque fois que les seuils définis sont dépassés. Cette gestion des seuils est étendue pour configurer un groupe de règles de seuil et surveiller le groupe au lieu de règles individuelles. Un

groupe de règles de seuil comprend une ou plusieurs règles de seuil définies par l'utilisateur pour les mesures choisies à partir d'entités telles que les utilisateurs, les applications et les postes de travail avec une valeur attendue.

[652441]

Création de seuils et configuration de règles, d'alertes et de géolocalisation pour HDX Insight

La gestion des seuils pour HDX Insight dans Citrix ADM vous permet de configurer de manière proactive les alertes chaque fois que les seuils définis sont dépassés. Cette gestion des seuils est étendue pour configurer un groupe de règles de seuil et surveiller le groupe au lieu de règles individuelles. Un groupe de règles de seuil comprend une ou plusieurs règles de seuil définies par l'utilisateur pour les mesures choisies à partir d'entités telles que les utilisateurs, les applications et les postes de travail avec une valeur attendue. Les groupes de seuils peuvent également être liés à des géolocalisations pour la surveillance géographique spécifique de l'entité utilisateur.

[652447]

Problèmes résolus

Réseaux

- Dans l'interface graphique Citrix ADM, le nom d'hôte de l'instance Citrix ADC n'apparaît pas sur la page de détails du certificat SSL. Avec ce correctif, le nom d'hôte est visible.
  1. Dans Citrix ADM, accédez à **Réseaux** > **Tableau de bord SSL**.
  2. Sur la page **Tableau de bord SSL**, cliquez à l'intérieur de l'un des cercles.
  3. Sélectionnez un certificat dans la page **Certificats SSL**, puis cliquez sur **Détails**.[670374]
- Lors de la planification des paramètres de sauvegarde d'instance, il existe une différence de quelques heures entre l'heure planifiée de la sauvegarde et l'heure affichée sur l'interface graphique Citrix ADM. [695489]
- Si vous essayez d'exporter deux graphiques à partir de la page Rapports réseau dans l'interface graphique Citrix ADM, seul le premier graphique est exporté en tant que rapport. Avec ce correctif, tous les graphiques de la page Rapports réseau sont maintenant exportés.

  > **Remarque**
  >
  > Les rapports sont exportés au format .pdf, .png ou .jpeg. [699380]
- Dans Citrix ADM, si vous accédez à **Réseaux** > **Travaux de configuration** > **Tâches de maintenance**et sélectionnez **Mettre à niveau NetScaler**, la mise à niveau des instances Citrix ADC échoue. [692538]

Haute disponibilité

- La sauvegarde d'instance Citrix ADC est déclenchée pour les instances principales et secondaires Citrix ADC lorsque les instances sont déployées en haute disponibilité. [698903]
- Lorsque les instances Citrix ADC dans le programme d'installation de haute disponibilité échouent et si le nouveau principal est inaccessible à partir de Citrix ADM, l'instance n'est plus visible dans l'interface graphique de Citrix ADM. [697017]

Paramètres

- Les tâches de maintenance dans Citrix ADM ne fonctionnent pas. [696952]

Problèmes connus

Analytics

- Dans certains cas, les nœuds HDX Insight et Gateway Insight peuvent ne pas être affichés sur l'interface graphique graphique Citrix ADM.
  Solution : actualisez la page et réessayez. [690327]

Paramètres

- Sur la page **Paramètres** > **Abonnements**, la consommation de données de stockage peut apparaître supérieure à la limite de stockage de 5 Go. [689330]
- Lorsque vous supprimez les utilisateurs de Citrix Cloud, les noms d'utilisateurs supprimés continuent d'apparaître dans Citrix ADM dans **Paramètres** > **Administration** des **utilisateurs > Utilisateurs**. [686581]
- Vous ne pouvez pas mettre à niveau les instances SD-WAN WO ou Citrix ADC SDX Citrix à partir de Citrix ADM 506.119 build. [699814]

17 novembre 2017

Cette version inclut de nouvelles fonctionnalités et corrections de bugs.

Par défaut, les agents Citrix ADM sont automatiquement mis à niveau vers la version 505.117. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour plus de détails, consultez Configuration des paramètres de mise à niveau de l'agent.

Nouveautés

Prise en charge du serveur proxy pour les agents sur Citrix ADM

Vous pouvez désormais connecter vos agents à Citrix ADM à l'aide d'un serveur proxy. Grâce à cette amélioration, les agents transmettent toutes leurs données au serveur proxy, qui envoie ensuite les données à Citrix ADM via Internet.

Pour transférer des données à l'aide du serveur proxy, tapez les détails du serveur proxy sur l'agent à l'aide du script suivant : proxy_input.py, puis suivez les instructions fournies par le script pour entrer plus d'informations. L'agent récupère ces informations lorsqu'il se connecte à Citrix ADM à l'aide du serveur proxy.

Vous pouvez authentifier votre serveur proxy en fournissant vos informations de nom d'utilisateur et de mot de passe. Lorsque l'agent envoie les données, le serveur proxy authentifie les informations d'identification de l'utilisateur avant de les transférer à Citrix ADM.

> **Remarque Le** serveur proxy prend uniquement en charge l'authentification de base.

[697617]

Activation de l'authentification unique pour Google Apps dans les instances de Citrix ADC à l'aide de StyleBook

L'authentification unique par défaut Google Apps StyleBook dans Citrix ADM vous permet d'activer l'authentification unique pour les applications Google dans les instances de Citrix ADC. StyleBook configure l'instance de Citrix ADC en tant que fournisseur d'identité SAML pour authentifier les utilisateurs pour accéder à Google Apps. Pour de plus amples informations, consultez la section Comment utiliser SSO Google Apps StyleBook.

[697027]

Capacité d'évaluer la tendance d'utilisation maximale de l'application avec les performances de l'application

Vous pouvez maintenant évaluer la tendance d'utilisation maximale d'une application. Vous pouvez également comparer son impact sur les performances de l'application en fonction du score de l'application à partir du tableau de bord des applications dans Citrix ADM. Vous pouvez utiliser la tendance d'utilisation maximale et l'impact des performances sur les informations de l'application et apporter les modifications nécessaires à votre déploiement. Cela aide à améliorer les performances de l'application.

Pour afficher la tendance d'utilisation maximale d'une application, accédez à **Applications> Tableau de bord de l'application**. Sélectionnez l'application et cliquez sur**Utilisation maximale**.

Pour de plus amples informations, consultez Tendance de l'utilisation des applications

[688208]

Problèmes résolus

Réseaux

- Dans la page Citrix ADM **ConfigurationsTâches**> Tâches, si une ligne a un fond bleu, le bouton**Créer un travail**est désactivé. Avec ce correctif, le bouton**Créer un travail** est actif et n'est pas désactivé. [695397]
- Dans Citrix ADM **Networks** > **Evénements** > **Messages d'événement**, lorsque vous essayez de trier les messages d'événement en fonction de la date, le tri ne se produit pas correctement. Les messages sont triés dans l'ordre inverse dans la direction des flèches de tri. Par exemple, lorsque les messages sont triés de plus en plus récents, la flèche pointe vers le haut. [696737]
- Il y a une erreur de validation lorsque vous téléchargez le fichier ns.conf dans Citrix ADM pour des conseils de configuration. [696920]
- Un message d'interruption envoyé à Citrix ADM affiche le nom de l'entité ainsi que l'adresse IP du serveur virtuel d'où provient l'interruption et le port. L'exemple suivant montre le nom de l'entité dans le message d'interruption reçu par Citrix ADM :

```
1     Entity Name
2      server_svc_NSSVC_IPFIX_10.102.29.150:4739       (service_10
          .102.29.150_33554)_DOWN
3  <!--NeedCopy-->
```

- Citrix ADM n'affiche pas le nom de l'entité, l'adresse IP et le numéro de port en tant que paramètres distincts dans la colonne Message de la table **Réseaux** > **Événements** > **Messages d'événement**.[696639]
- Dans une règle événementielle, lorsque vous exécutez un script contenant un message contenant de l'espace (» «), le script n'est pas activé. [696896]
- Certains rapports réseau prennent plus de temps à générer dans Citrix ADM. Lorsque ces rapports sont planifiés pour être exportés, les rapports incomplets sont exportés. Avec ce correctif, Citrix ADM attend que les rapports soient générés complètement avant de les exporter. [695500]
- Dans Citrix ADM, vous ne pouvez pas exporter des rapports pour certaines vues tabulaires et tableaux de bord. Avec ce correctif, vous pouvez désormais exporter le contenu des tables et des tableaux de bord. [670226]
- Dans Citrix ADM, considérez que vous êtes dans une vue liste et que vous avez navigué plus loin dans des pages spécifiques. Vous ne pouvez pas revenir en arrière à l'aide du volet de navigation situé sur le côté gauche de l'interface graphique. Vous devrez peut-être naviguer à l'aide de la chapelure en haut de la page. Par exemple, considérez que vous êtes actuellement dans la page **Réseaux** > **Instances** > **NetScaler VPX** > **Sauvegarde/restauration** . Lorsque vous sélectionnez le type d'instance Citrix ADC sous **Réseaux** > **Instances**, la page de liste d'instance Citrix ADC

correspondante ne s'ouvre pas après avoir cliqué sur NetScaler VPX dans le volet de navigation. [684922]

- Dans Citrix ADM, la mise à niveau de l'instance Citrix ADC à l'aide de Citrix ADM échoue. Si vous accédez à **Réseaux** > **Tâches de configuration** > **Tâches de maintenance**et sélectionnez **Mettre à niveau NetScaler**, la mise à niveau des instances Citrix ADC échoue. [692538]
- Les modèles d'audit de configuration qui doivent être exécutés à un moment spécifique sont également exécutés lors de l'interrogation globale, ce qui entraîne une exécution répétée des modèles d'audit de configuration. [697157]
- L'audit de configuration utilisant des valeurs de variables spécifiques ne fonctionne pas pour les instances Citrix ADC qui sont en mode HA. [696990]
- Vous ne pouvez pas charger le fichier d'entrée pour les valeurs de variables lors de la création d'un modèle d'audit de configuration. [697137]
- Dans Citrix ADM, toute erreur lors du traitement du rapport d'audit de configuration entraîne l'envoi d'un courrier vide aux destinataires du courrier. [697138]

Paramètres

- Au moment de l'enregistrement et du déploiement des nœuds dans Citrix ADM dans HA, le mot de passe des deux nœuds doit être le mot de passe par défaut « ns root. « L'enregistrement du nœud échoue si le mot de passe est différent de `nsroot`. [691836]
- Dans Citrix ADM, lorsque vous entrez des caractères spéciaux tels que « & » dans les champs de saisie, tels que nom et description, « & » est remplacé par « & ». [692656]
- Dans Citrix ADM, lorsque vous entrez des caractères spéciaux tels que « & » dans les champs de saisie tels que nom et description, « & » remplace « & ». [692656]
- Vous pouvez ajouter des applications à un groupe et spécifier une regex pour appliquer les critères de recherche pour ajouter des applications au groupe. Dans ce cas, lorsque vous modifiez un groupe plusieurs fois, le nom de l'application est converti en une expression rationnelle non valide. Cela provoque l'échec du RBAC et les utilisateurs peuvent voir toutes les applications.

  1. Dans Citrix ADM, accédez à **Système** > **Administration des utilisateurs** > **Groupes**, puis cliquez sur **Ajouter** . Entrez le nom du groupe et, dans **l'onglet Paramètres d'autorisation**, sélectionnez l'application requise et ajoutez-la au groupe, puis cliquez sur **Créer un groupe** .
  2. Lorsque vous souhaitez ajouter une expression rationnelle, accédez à la page **Groupes**, sélectionnez le groupe et cliquez sur **Modifier** .

3. Dans **l'onglet Paramètres d'autorisation**, ajoutez l'expression rationnelle dans la zone de texte **Ajouter une expression régulière** et enregistrez les paramètres.
4. Si vous modifiez à nouveau le groupe, dans l'onglet **Paramètres d'autorisation**, vous pouvez constater que le nom de l'application que vous avez ajoutée précédemment est converti en regex. Comme il s'agit d'une regex non valide, RBAC échoue et votre utilisateur peut voir toutes les applications. [696515]

Haute disponibilité

- Lorsque les instances de Citrix ADC dans le programme d'installation HA échouent et si le nouveau serveur principal est inaccessible à partir de Citrix ADM, l'instance n'est plus visible dans l'interface graphique de Citrix ADM. [697017]
- Lorsque vous restaurez un fichier de sauvegarde à partir d'une instance de Citrix ADC dans une paire qui est dans l'installation HA vers une autre instance de la même paire, cette instance de Citrix ADC devient inaccessible en raison d'un conflit dans l'adresse IP. Citrix ADM vérifie si l'adresse IP du fichier de sauvegarde et l'adresse IP de l'instance sur laquelle la restauration est effectuée sont identiques. Si les adresses IP ne correspondent pas, un message d'erreur s'affiche et la restauration est arrêtée. [686829]
- Lorsque vous mettez à niveau une paire d'instances de Citrix ADC qui sont en HA, les instances de Citrix ADC sont instables. Les instances peuvent devoir attendre un certain temps avant de répondre aux appels NITRO envoyés par Citrix ADM.
- Avec ce correctif, vous pouvez définir un temps d'attente dans le profil d'instance de sorte que Citrix ADM attend l'heure définie avant d'envoyer un appel NITRO aux instances. Le temps d'attente par défaut est de 60 secondes. [690860]

Problèmes connus

Analytics

- Dans certains cas, les nœuds HDX Insight et Gateway Insight peuvent ne pas être affichés sur l'interface graphique graphique Citrix ADM.
  Solution : actualisez la page et réessayez. [690327]

Réseaux

- Dans Citrix ADM, si vous accédez à **Réseaux** > **Travaux de configuration** > **Tâches de maintenance** et sélectionnez **Mettre à niveau NetScaler**, la mise à niveau des instances de Citrix ADC échoue. [692538]

Paramètres

- Sur la page **Paramètres** > **Abonnements**, la consommation de données de stockage peut apparaître supérieure à la limite de stockage de 5 Go. [689330]
- Lorsque vous supprimez les utilisateurs de Citrix Cloud, les noms d'utilisateurs supprimés continuent d'apparaître dans Citrix ADM dans **Paramètres** > **Administration** des **utilisateurs > Utilisateurs**. [686581]
- Les tâches de maintenance dans Citrix ADM ne fonctionnent pas. [696952]

Octobre 27, 2017

Cette version inclut de nouvelles fonctionnalités et corrections de bugs.

Par défaut, les agents Citrix ADM sont automatiquement mis à niveau vers la version 504.115. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**. Vous pouvez également spécifier l'heure à laquelle vous souhaitez que les mises à niveau de l'agent se produisent. Pour plus de détails, consultez Configuration des paramètres de mise à niveau de l'agent.

Nouveautés

Possibilité d'importer et d'exporter les modèles de configuration

Vous pouvez exporter les modèles de configuration et importer le modèle vers le même client ou un autre locataire dans Citrix ADM. Les données du modèle exportées (telles que les commandes de configuration, les définitions de variables et les paramètres) ne sont pas perdues après l'importation.

Pour exporter le modèle de configuration, accédez à **Réseaux > Travaux de configuration > Modèles de configuration**. Sélectionnez le modèle de configuration et cliquez sur **Exporter**. Les modèles de configuration exportés sont enregistrés dans le système local dans un format de fichier **JSON** . Vous pouvez ensuite importer ce fichier vers le même locataire ou un autre locataire dans Citrix ADM pour créer un modèle de configuration. Pour importer le modèle de configuration, cliquez sur **Importer** et sélectionnez le fichier **JSON** que vous avez enregistré localement.

Pour de plus amples informations, consultez la section Procédure d'importation et d'exportation de modèles de configuration.

[691585]

Prise en charge de la différence d'historique des révisions et du modèle d'audit pour les partitions d'administration

La différence d'historique des révisions et le modèle d'audit pour la partition administrateur sont désormais pris en charge dans Citrix ADM.

La différence d'historique des révisions pour la partition administrateur 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 avec les autres (exemple : Révision de configuration - 1 avec Révision de configuration -2) ou avec la configuration en cours d'exécution ou enregistrée avec Révision de configuration. Outre 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.

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 dans la configuration en cours d'exécution de l'instance avec le modèle d'audit est affichée dans la colonne « Modèle vs exécution du 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.

[657300]

Possibilité d'ajouter plusieurs modèles de différents types dans les tâches de configuration

Vous pouvez maintenant ajouter plusieurs modèles de différents types dans l'éditeur de tâches de configuration tout en créant une tâche de configuration. Pour ajouter plusieurs modèles, accédez à **Réseaux > Travaux de configuration** et cliquez sur **Créer un travail**. Dans la page **Créer un travail**, entrez le nom du travail et sélectionnez le type d'instance. Dans la liste déroulante **Source de configuration**, vous pouvez sélectionner la source requise, puis faire glisser plusieurs modèles dont vous avez besoin vers l'éditeur de configuration. Les types de source de modèle sont **Modèle de configuration**, **Modèle intégré**, **Configuration principale**, **Enregistrement et lecture**, **Instance**et **Fichier**.

Pour de plus amples informations, consultez la section Comment créer une tâche de configuration sur Citrix ADM.

[686881]

Possibilité de conserver les valeurs de variable en entrée dans les travaux de configuration

Dans Citrix ADM, lors de la création des tâches de configuration, les valeurs de variable d'entrée spécifiées, y compris les fichiers d'entrée, sont maintenant conservées. Vous pouvez afficher et modifier ces valeurs ainsi que les fichiers d'entrée que vous avez téléchargés précédemment lors de la création de la tâche de configuration. Pour afficher les valeurs des variables en entrée, accédez à **Réseau > Travaux de configuration**, sélectionnez le travail et cliquez sur **Modifier**. Dans l'onglet **Spécifier les valeurs de variable**, vous pouvez afficher les valeurs de variable persistante. Le fichier d'entrée que vous avez téléchargé précédemment persiste également. Vous pouvez télécharger le fichier d'entrée, le modifier, puis télécharger le même fichier d'entrée sans changer le nom.

[691584]

Possibilité de réorganiser des commandes dans l'éditeur de tâches de configuration

Vous pouvez maintenant réorganiser et réorganiser les commandes dans l'éditeur de tâches de configuration. Vous pouvez maintenant déplacer les commandes 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.

[684164]

Configuration des paramètres de taille des rapports réseau pour Citrix ADM

Vous pouvez maintenant configurer l'intervalle de taille des données de rapports réseau dans Citrix ADM. Cela limite la quantité de données de rapports réseau stockées dans la base de données du serveur Citrix ADM. Par défaut, l'élagage se produit toutes les 24 heures (à 01.00 heures) pour les données historiques du réseau.

[692461]

Possibilité de prévisualiser et de modifier les variables dans le travail de configuration

Dans Citrix ADM, vous pouvez désormais prévisualiser toutes les variables que vous avez définies lors de la création ou de la modification d'une tâche de configuration dans une vue consolidée unique.

Cliquez sur l'onglet **Aperçu des variables** dans l' **éditeur de tâches de configuration** pour afficher un aperçu des variables dans une vue consolidée unique. Une nouvelle fenêtre contextuelle s'affiche et affiche tous les paramètres des variables telles que Nom, Nom d'affichage, Type et valeur par défaut sous forme de tableau. Vous pouvez également modifier ces paramètres. Cliquez sur **Terminé** après avoir modifié ou modifié l'un des paramètres.

Vous pouvez effectuer l'une des opérations suivantes pour prévisualiser toutes les variables dans une vue consolidée unique :

- **Création d'une tâche de configuration**. Accédez à **Réseaux > Travaux de configuration**, sélectionnez **Créer un travail**. Sur la page **Créer un travail**, vous pouvez prévisualiser toutes les variables.
- **Modification d'une tâche de configuration**. Accédez à **Réseau > Travaux de configuration**, sélectionnez le nom du travail et cliquez sur **Modifier**. Sur la page **Configurer le travail**, vous pouvez prévisualiser toutes les variables qui ont été ajoutées lors de la création du travail de configuration.

[684166]

Prise en charge des caractères génériques pour l'ajout dynamique d'applications à des groupes dans Citrix ADM

Lorsque vous ajoutez des applications à un groupe dans Citrix ADM, vous pouvez utiliser regex pour rechercher et ajouter les applications qui répondent aux critères regex aux groupes. Les utilisateurs liés à ces groupes ne peuvent accéder qu'à ces applications spécifiques. L'expression regex spécifiée est conservée dans Citrix ADM. Lorsqu'une nouvelle application est ajoutée au système, Citrix ADM applique les critères de recherche à la nouvelle application et l'application qui répond aux critères devient dynamiquement partie du groupe. Vous n'avez pas besoin d'ajouter manuellement la nouvelle application au groupe. Les applications sont mises à jour dynamiquement dans le système, et les utilisateurs du groupe respectif peuvent voir les applications sous les modules appropriés dans Citrix ADM.

Pour de plus amples informations, consultez la section Configuration de groupes sur Citrix ADM.

[692032]

Affectation de valeurs de variable spécifiques dans les modèles d'audit de configuration

Citrix ADM vous permet de créer des variables et d'attribuer des valeurs à des variables tout en créant des modèles d'audit de configuration. Dans l'onglet **Spécifier les valeurs de variable** sous **Réseaux** > **Audit de configuration** > **Modèles d'audit** > **Ajouter** > **Créer un modèle**, vous disposez de deux options pour affecter des valeurs aux variables :

1. Valeurs de**variables communes pour toutes les instances**. Sélectionnez cette option pour entrer des valeurs communes aux variables répertoriées sur cette page pour l'instance sélectionnée.
2. **Charger le fichier d'entrée pour les valeurs de variables**. Sélectionnez cette option pour télécharger le fichier, entrez des valeurs pour les variables, puis téléchargez le fichier dans Citrix ADM.

Pour de plus amples informations, consultez la section Création de modèles d'audit.

[691127]

Exportation du rapport Diff d'audit de configuration

Citrix ADM vous permet de télécharger le rapport de diff 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, ainsi que d'exporter un rapport de diff granulaire pour chaque paire de modèle d'instance.

Pour de plus amples informations, consultez la section Affichage des rapports d'audit.

[679736]

Possibilité de planifier un modèle d'audit de configuration et un rapport de vérification de configuration par e-mail

Citrix ADM permet d'exécuter tous les modèles d'audit sous **Réseaux** > **Audit de configuration** > **Modèles d'audit** à une heure planifiée individuellement ou globalement selon vos besoins. Vous pouvez planifier l'exécution du modèle d'audit de configuration à une heure spécifique plutôt que de l'exécuter à une heure par défaut configurée par le système. Lorsque vous sélectionnez **Personnaliser l'**option de planification du modèle, vous pouvez planifier l'exécution du modèle tous les jours, un jour spécifique de la semaine ou un jour spécifique du mois. Pour chaque option, vous devez également entrer l'heure de planification à laquelle Citrix ADM doit exécuter le modèle. Citrix ADM vous fournit les options suivantes pour planifier l'exportation du rapport de diff d'audit de configuration.

- **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 des modèles**. Utilisez cette option pour configurer l'heure et la fréquence auxquelles les modèles doivent être exécutés.
- **Envoyer le rapport par e-mail**. Utilisez cette option pour configurer le profil de messagerie auquel le rapport diff doit être envoyé en tant que pièce jointe.

Pour de plus amples informations, consultez la section Création de modèles d'audit.

[681957]

Possibilité de visualiser les dépendances d'un StyleBook sous forme de graphique

Vous pouvez maintenant visualiser toutes les dépendances d'un StyleBook, c'est-à-dire tous les autres StyleBooks dont dépend votre StyleBook sélectionné. Les dépendances sont créées à la suite de la composition de nouveaux StyleBooks à l'aide de ceux existants. Les dépendances sont visualisées sous la forme d'un graphique de boîtes et de flèches, où chaque boîte représente un StyleBook et chaque flèche représente une dépendance de direction entre un StyleBook et son dépendant. Accédez à **Applications** > **Configurations** > **StyleBooks** et dans la liste des StyleBooks qui s'affichent dans le panneau de droite, cliquez sur le lien **Afficher les dépendances** du StyleBook que vous souhaitez visualiser.

[697175]

Téléchargement de StyleBooks personnalisés et des StyleBooks personnalisés dépendants

Vous pouvez maintenant télécharger un StyleBook personnalisé et ses StyleBooks dépendants au format YAML sur votre système sous forme de fichier ZIP ou TGZ. Dans Citrix ADM, accédez à **Applications** > **Configurations** > **StyleBooks** et, dans la liste des StyleBooks qui s'affiche dans le panneau de droite, cliquez sur le lien **Télécharger** pour le StyleBook que vous souhaitez télécharger.

> **Remarque** Vous ne pouvez pas télécharger StyleBooks par défaut.

[696383]

Suppression de StyleBooks personnalisés et des StyleBooks personnalisés dépendants

Vous pouvez supprimer un StyleBook personnalisé et ses StyleBooks dépendants du système de dossiers Citrix ADM. Accédez à **Applications** > **Configurations** > **StyleBooks** et à partir de la liste des StyleBooks qui s'affiche dans le panneau de droite, puis cliquez sur l'icône "**X** " située à droite du StyleBook que vous souhaitez supprimer. Vous avez la possibilité de supprimer uniquement le fichier ou tous les StyleBooks dépendants aussi.

> **Remarque** Vous ne pouvez pas supprimer StyleBooks par défaut.

[696384]

Gérer et surveiller les instances HAProxy

Vous pouvez désormais gérer et surveiller les instances HAProxy dans votre déploiement à l'aide de Citrix ADM. Lorsque vous ajoutez un hôte HAProxy à Citrix ADM, il détecte automatiquement les instances HAProxy sur l'hôte et vous permet de les gérer et de les surveiller en fournissant les éléments suivants :

- **HaProxy App Dashboard** : Affiche les statistiques en temps réel des fronts sur les instances HaProxy. Le tableau de bord répertorie les applications frontales en tant qu'applications découvertes et affiche les transactions en temps réel, le débit et les informations de session sur les applications.
- **Possibilité de redémarrer une instance HAProxy** : vous pouvez redémarrer une instance HAProxy à partir de l'interface graphique de Citrix ADM. En outre, vous pouvez effectuer un redémarrage dur ou un redémarrage progressif d'une instance HAProxy à partir de l'interface graphique Citrix ADM.

Pour de plus amples informations, consultez la section Gestion et surveillance des instances HAProxy.

[637830]

Problèmes résolus

Les problèmes suivants ont été résolus dans cette version.

Analytics

- La fonctionnalité Analytics n'affiche aucune donnée si vous avez ajouté des instances Citrix ADC CPX dans Citrix ADM.
  Solution : n'ajoutez aucune instance Citrix ADC CPX à Citrix ADM. [694792]

Agents

- Si vous accédez à **Réseaux** > **Agents** et essayez de télécharger un agent à partir de l'écran **Agents**, vous pouvez voir une erreur telle que « Fichier introuvable ».
  Solution : pour télécharger un agent, accédez à **Paramètres** > **Configurer l'agent**, sélectionnez l'Hypervisor, puis cliquez sur **Télécharger l'image**. [695998]

Problèmes connus

Les problèmes connus suivants existent dans cette version :

Analytics

- Dans certains cas, les nœuds HDX Insight et Gateway Insight peuvent ne pas être affichés sur l'interface graphique graphique Citrix ADM.
  Solution : actualisez la page et réessayez. [690327]

Réseaux

- Dans Citrix ADM, la mise à niveau de l'instance Citrix ADC à l'aide de Citrix ADM échoue. Si vous accédez à **Réseaux** > **Tâches de configuration** > **Tâches de maintenance**et sélectionnez **Mettre à niveau NetScaler**, la mise à niveau des instances Citrix ADC échoue. [692538]
- Les modèles d'audit de configuration qui doivent être exécutés à un moment spécifique sont également exécutés lors de l'interrogation globale, ce qui entraîne une exécution répétée des modèles d'audit de configuration. [697157]
- L'audit de configuration utilisant des valeurs de variables spécifiques ne fonctionne pas pour les instances de Citrix ADC qui sont en mode HA. [696990]
- Vous ne pouvez pas télécharger le fichier d'entrée pour les valeurs de variables lors de la création d'un modèle d'audit de configuration. [697137]
- Dans Citrix ADM, toute erreur lors du traitement du rapport d'audit de configuration entraîne l'envoi d'un courrier vide aux destinataires du courrier. [697138]

Paramètres

- Sur la page **Paramètres** > **Abonnements**, la consommation de données de stockage peut apparaître supérieure à la limite de stockage de 5 Go. [689330]

- Lorsque vous supprimez les utilisateurs de Citrix Cloud, les noms d'utilisateurs supprimés continuent d'apparaître dans Citrix ADM dans **Paramètres** > **Administration** des **utilisateurs > Utilisateurs**. [686581]
- Dans Citrix ADM, lorsque vous entrez des caractères spéciaux tels que « & » dans les champs de saisie tels que nom et description, « & » remplace « & ». [692656]
- Les tâches de maintenance dans Citrix ADM ne fonctionnent pas. [696952]
- Vous pouvez ajouter des applications à un groupe et spécifier une regex pour appliquer les critères de recherche pour ajouter des applications au groupe. Dans ce cas, lorsque vous modifiez un groupe plusieurs fois, le nom de l'application est converti en une expression rationnelle non valide. Cela provoque l'échec du RBAC et les utilisateurs peuvent voir toutes les applications.

  1. Dans Citrix ADM, accédez à **Paramètres** > **Administration des utilisateurs** > **Groupes**, puis cliquez sur **Ajouter** . Entrez le nom du groupe et, dans **l'onglet Paramètres d'autorisation**, sélectionnez l'application requise et ajoutez-la au groupe, puis cliquez sur **Créer un groupe** .
  2. Lorsque vous souhaitez ajouter une expression rationnelle, accédez à la page **Groupes**, sélectionnez le groupe et cliquez sur **Modifier** .
  3. Dans **l'onglet Paramètres d'autorisation**, ajoutez l'expression rationnelle dans la zone de texte **Ajouter une expression régulière** et enregistrez les paramètres.
  4. Si vous modifiez à nouveau le groupe, dans l'onglet **Paramètres d'autorisation**, vous pouvez constater que le nom de l'application que vous avez ajoutée précédemment est converti en regex. Comme il s'agit d'une regex non valide, RBAC échoue et votre utilisateur peut voir toutes les applications.

  [696515]

Octobre 7, 2017

Cette version inclut de nouvelles fonctionnalités et corrections de bugs.

Les agents Citrix ADM sont automatiquement mis à niveau vers la version 503.115. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**.

Nouveautés

Les améliorations suivantes sont disponibles dans cette version.

Configurer l'heure de mise à niveau de l'agent

Par défaut, un agent est mis à niveau automatiquement lorsqu'une version plus récente est disponible. Toutefois, vous pouvez spécifier l'heure à laquelle vous souhaitez que la mise à niveau de l'agent se produise. Si vous sélectionnez une heure spécifique, les agents sont mis à niveau à cette heure spécifiée, mais dans le fuseau horaire où vos agents sont déployés. Pendant la mise à niveau, il peut y avoir un temps d'arrêt d'environ 30 minutes. Pour spécifier l'heure de mise à niveau de l'agent, accédez à **Réseaux** > **Agents**, cliquez sur **Configurer les paramètres de mise à niveau**, puis spécifiez quand vous souhaitez que l'agent soit mis à niveau. Pour plus de détails, consultez Configuration des paramètres de mise à niveau de l'agent.

Accès à l'interface graphique d'une instance Citrix ADC managée à partir de Citrix ADM

Vous pouvez désormais accéder à l'interface graphique d'une instance de Citrix ADC gérée à partir de Citrix ADM. Pour gérer et surveiller les instances de Citrix ADC, ajoutez-les à Citrix ADM. Vous pouvez ensuite y accéder à partir de Citrix ADM. Assurez-vous que vous êtes connecté au réseau Citrix.

Pour accéder à une interface graphique d'instance de Citrix ADC à partir de Citrix ADM, accédez à **Réseaux** > **Instances** . Sous Instances, sélectionnez le type d'instance à afficher (par exemple, Citrix ADC VPX), puis cliquez sur l'adresse IP de l'instance à laquelle vous souhaitez accéder.

[693970]

Gérer les instances SWG Citrix à partir de Citrix ADM

Citrix ADM prend désormais en charge la découverte, la gestion et la surveillance des instances de Citrix Secure Web Gateway (SWG). Vous pouvez afficher les instances SWG Citrix sous **Réseaux** > **Instances**, comme illustré dans l'image suivante :

[692493]

Prise en charge du délai de grâce après l'expiration de la licence

Une fois la licence expirée, Citrix ADM fournit un délai de grâce de 90 jours. Pendant la période de grâce, les données collectées par Citrix ADM sont conservées pendant 30 jours et les configurations sont conservées pendant 90 jours. Pendant la période de grâce, vous ne pouvez pas accéder à Citrix ADM.

[691069]

Prise en charge de l'interrogation spécifique à l'entité

Citrix ADM vous permet d'interroger des entités spécifiques configurées sur une instance. Cela réduit le temps d'actualisation requis par Citrix ADM pour afficher le statut le plus récent des entités liées

à une instance. Vous pouvez à présent interroger les entités suivantes pour 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. Pour une documentation détaillée, reportez-vous à la sectionProcédure d'interrogation des instances et entités Citrix ADC.

[692958]

Problèmes résolus

Les problèmes suivants ont été résolus dans cette version.

Agent

- Si vous utilisez un agent provisionné sur le cloud Microsoft Azure, les instances gérées associées à cet agent apparaissent dans l'état d'arrêt dans l'interface graphique Citrix ADM. [690941]
- Une fois l'enregistrement de l'agent terminé, il se peut que vous ne puissiez pas vous connecter à l'agent à partir de la console de l'Hypervisor. [691181]

Réseaux

- Dans Citrix ADM, lors de la création de tâches de configuration, les fichiers ne sont pas téléchargés automatiquement. Vous devez sélectionner les fichiers que vous souhaitez télécharger et cliquer sur le bouton **Télécharger**. Le bouton **Télécharger** n'est pas disponible maintenant et le fichier est téléchargé automatiquement après avoir sélectionné les fichiers que vous souhaitez télécharger. [686889]
- Dans **Réseaux** > **Travaux de configuration** > **Aperçu**, vous pouvez afficher les commandes d'annulation associées du travail de configuration sur la page d'aperçu. [687621]

Paramètres

- Dans Citrix ADM, la sauvegarde de la plate-forme avancée Citrix SD-WAN WO n'est pas compatible avec le profil de périphérique défini par l'utilisateur. [690508]

Problèmes connus

Les problèmes connus suivants existent dans cette version :

Agents

- Si vous accédez à **Réseaux** > **Agents** et essayez de télécharger un agent à partir de l'écran **Agents**, vous pouvez voir une erreur telle que « Fichier introuvable ».
  Solution : pour télécharger un agent, accédez à **Paramètres**> **Configurer l'agent**, sélectionnez l'Hypervisor, puis cliquez sur **Télécharger l'image**. [695998]

Analytics

- Dans certains cas, les nœuds HDX Insight et Gateway Insight peuvent ne pas être affichés sur l'interface graphique graphique Citrix ADM.
  Solution : actualisez la page et réessayez. [690327]
- La fonctionnalité Analytics n'affiche aucune donnée si vous avez ajouté des instances Citrix ADC CPX dans Citrix ADM.
  Solution : n'ajoutez pas d'instances Citrix ADC CPX à Citrix ADM. [694792]

Réseaux

- Dans Citrix ADM, la mise à niveau de l'instance Citrix ADC à l'aide de Citrix ADM échoue. Si vous accédez à **Réseaux > Travaux de configuration > Tâches de maintenance** et sélectionnez **Mettre à niveau NetScaler**, la mise à niveau des instances de Citrix ADC échoue. [692538]
- Dans Citrix ADM, dans la zone de texte de saisie de formulaire lorsque vous entrez des caractères spéciaux tels que « & » dans les champs de saisie tels que nom et description, « & » remplace « & ». [692656]

Paramètres

- Sur la page **Paramètres** > **Abonnements**, la consommation de données de stockage peut apparaître supérieure à la limite de stockage de 5 Go. [689330]
- Lorsque vous supprimez les utilisateurs de Citrix Cloud, les noms d'utilisateurs supprimés continuent d'apparaître dans Citrix ADM dans **Paramètres** > **Administration** des **utilisateurs > Utilisateurs**. [686581]

> **Remarque :** les étiquettes [XXXXXX] sont des ID de suivi internes utilisés par l'équipe Citrix ADM.

14 septembre 2017

Cette version inclut de nouvelles fonctionnalités et corrections de bugs.

Les agents Citrix ADM sont automatiquement mis à niveau vers la version 502.119. Vous pouvez afficher les détails de l'agent sur la page **Réseaux** > **Agents**.

Nouveautés

Les améliorations suivantes sont disponibles dans cette version.

Solution d'équilibrage de charge globale Citrix ADC pour les déploiements hybrides et multi-cloud

La solution GLB (Global Load Balancing) permet aux utilisateurs de distribuer les demandes client sur plusieurs datacenters dans plusieurs clouds et sur des serveurs d'applications déployés sur site. Cette solution prend en charge les déploiements cloud multicloud et hybride. Les principaux avantages de cette solution sont :

- Vous permet de créer, de gérer et de surveiller des nœuds GLB à travers des emplacements géographiques à partir d'une console unifiée unique.
- Offre la flexibilité nécessaire pour déplacer une partie de l'infrastructure vers le cloud.
- Prise en charge de la topologie active-passive pour la reprise après sinistre
- Prend en charge plusieurs méthodes d'équilibrage de charge globales, telles que Proximité statique, Round Robin, Hash IP source et Round Trip Time.

Le « Multi-Cloud GLB StyleBook » associé dans Citrix ADM aide à fournir une interface utilisateur unique pour la gestion de tous les nœuds GLB dans plusieurs datacenters. Les avantages de l'utilisation d'un StyleBook sont les suivants :

- La modification de la configuration existante est facile car les changements doivent être effectués en un seul endroit.
- Pousser la configuration vers tous les nœuds GLB à l'aide de StyleBooks est plus rapide.

Pour une documentation complète, reportez-vous à la sectionÉquilibrage global de charge Citrix ADC pour les déploiements hybrides et multi-cloud.

[691937]

Gérer et surveiller les instances HAProxy (Aperçu)

Vous pouvez désormais gérer et surveiller les instances HAProxy dans votre déploiement à l'aide de Citrix ADM. Lorsque vous ajoutez un hôte HAProxy à Citrix ADM, il détecte automatiquement les instances HAProxy sur l'hôte et vous permet de les gérer et de les surveiller en fournissant les éléments suivants :

- **HaProxy App Dashboard** : Affiche les statistiques en temps réel des fronts sur les instances HaProxy. Le tableau de bord répertorie les applications frontales en tant qu'applications découvertes et affiche les transactions en temps réel, le débit et les informations de session sur les applications.

- **Possibilité de redémarrer une instance HAProxy** : vous pouvez redémarrer une instance HAProxy à partir de l'interface graphique de Citrix ADM. En outre, vous pouvez effectuer un redémarrage dur ou un redémarrage progressif d'une instance HAProxy à partir de l'interface graphique Citrix ADM.

Pour de plus amples informations, consultez la section Gestion et surveillance des instances HAProxy.

[637830]

Ignorer l'option sur l'écran Expérience utilisateur pour la première fois Citrix ADM

Citrix ADM vous permet désormais d'ignorer l'étape d'inscription de l'agent et d'accéder directement au tableau de bord de l'application Citrix ADM. Pour ignorer l'enregistrement de l'agent, sur la page **Configurer l'agent**, cliquez sur **Ignorer** .

En outre, la page d'expérience utilisateur pour la première fois Citrix ADM inclut désormais une vidéo qui fournit une vue d'ensemble de ce service Citrix Cloud.

[693963]

Améliorations apportées à la page Abonnements

La page Abonnements affiche désormais le résumé des abonnements, les serveurs virtuels et les serveurs virtuels tiers. Vous pouvez afficher les modifications suivantes sur la page **Paramètres** > **Abonnements** .

- Récapitulatif des licences par type de serveur virtuel.
- Licences d'équilibrage de charge tierces.
- Possibilité de sélectionner ou de désélectionner des serveurs virtuels sous licence automatique.

Vous pouvez également cliquer sur les types de serveurs virtuels pour afficher la liste des serveurs virtuels sur lesquels les licences sont appliquées.

Pour plus d'informations, consultez la section « Affichage des serveurs virtuels sous licence » dansGestion des abonnements.

[693954]

Problèmes résolus

Les problèmes suivants ont été résolus dans cette version.

Réseaux

- Si le proxy de contrôle n'est pas disponible pendant le processus de démarrage de l'agent, l'agent n'est pas en mesure de récupérer les paramètres d'interruptions SNMP à partir de Citrix ADM et toutes les interruptions reçues à partir d'instances Citrix ADC sont supprimées. [687027]
- Lorsque vous configurez une règle pour surveiller des événements spécifiques dans Citrix ADM, les e-mails ne sont pas envoyés pour les événements qui correspondent aux critères de filtre. [688985]
- La fonctionnalité de mise à niveau de Citrix ADC dans les tâches de maintenance n'est pas prise en charge dans Citrix ADM. Mais, vous pouvez toujours afficher l'option dans l'interface graphique. [689068]
- Dans Citrix ADM, l'icône Hamburger (icône de menu dans le coin gauche) devient l'icône Fermer (X) lorsque vous cliquez sur pour ouvrir le menu déroulant Navigation. Avec ce correctif, si nous ouvrons une page de configuration, par exemple, Ajouter une instance, Configurer Insight, et d'autres, le panneau de menu de navigation est masqué et l'icône "**X**" est désactivée. [687203]
- Dans **Réseaux** > **Événements** > **Messages d'événement**, lorsque vous sélectionnez un événement et cliquez sur l'onglet **Détails**, les valeurs des paramètres suivants tels que Nom d'utilisateur, Commande de configuration, Statut d'autorisation, Statut d'exécution et Type d'entité sont manquantes sur la page **Détails des événements**. [686791]
- Dans **Réseaux > Fonctions réseau > Équilibrage de charge > Groupes de services**, vous pouvez désormais filtrer les applications par ID et l'utiliser dans le kit SDK Python. [692061]
- Dans **Réseaux > Fonctions réseau > Équilibrage de charge > Serveurs virtuels**, pour certains serveurs virtuels d'équilibrage de charge qui sont à l'état UP pendant plus de 248 jours, la colonne **UP Depuis**affiche des valeurs incorrectes. [693146]

Paramètres

- Dans Citrix ADM, si vous créez un nom de groupe comportant des espaces, certaines fonctionnalités, telles que la récupération d'applications, qui utilisent des noms de groupe pour les autorisations peuvent ne pas fonctionner comme prévu. [692629]
- La mise à niveau des instances de Citrix ADC en mode HA à partir de Citrix ADM échoue car le nœud secondaire prend un certain temps pour redémarrer, provoquant le basculement forcé du principal à l'échec. [693119]

StyleBooks

- Le "*****" est accepté comme entrée valide pour le `tcp-port` paramètre dans la commande CLI. [694155]

Problèmes connus

Les problèmes connus suivants existent dans cette version :

Agent

- Si vous utilisez un agent provisionné sur le cloud Microsoft Azure, les instances gérées associées à cet agent apparaissent à l'état de panne dans l'interface graphique Citrix ADM. [690941]
- Une fois l'enregistrement de l'agent terminé, il se peut que vous ne puissiez pas vous connecter à l'agent à partir de la console de l'Hypervisor.
  Solution : connectez-vous à l'agent à l'aide d'un client SSH. [691181]

Analytics

- Dans certains cas, les nœuds HDX Insight et Gateway Insight peuvent ne pas être affichés sur l'interface graphique graphique Citrix ADM.
  Solution : actualisez la page et réessayez. [690327]
- La fonctionnalité Analytics n'affiche aucune donnée si vous avez ajouté des instances Citrix ADC CPX dans Citrix ADM.
  Solution : n'ajoutez aucune instance Citrix ADC CPX à Citrix ADM. [0694792]

Paramètres

- Sur la page **Paramètres** > **Abonnements**, la consommation de données de stockage peut apparaître supérieure à la limite de stockage de 5 Go. [689330]
- Lorsque vous supprimez les utilisateurs de Citrix Cloud, les noms d'utilisateur supprimés continuent d'apparaître dans Citrix ADM dans **Paramètres** > **Administration** des **utilisateurs > Utilisateurs**.[686581]

> **Remarque :** les étiquettes [XXXXXX] sont des ID de suivi internes utilisés par l'équipe Citrix ADM.

Août 25, 2017

Cette version inclut de nouvelles fonctionnalités et corrections de bugs.

Nouveautés

Les améliorations suivantes sont disponibles dans cette version.

Mises à niveau de Citrix ADM Evergreen Agent

Dans Citrix ADM, les agents s'exécutant sur la version logicielle 12.0 build 501.117 et ultérieure sont automatiquement mis à niveau vers des versions plus récentes et recommandées par Citrix ADM. Pour activer cette fonctionnalité pour vos agents Citrix ADM, vous devez mettre à niveau manuellement vos agents existants vers Citrix ADM version 12.0 build 501.117.

Problèmes résolus

Les problèmes suivants ont été résolus dans cette version.

Réseaux

- Dans Citrix ADM, si vous essayez de supprimer les certificats par défaut des instances de Citrix ADC découvertes, un message d'erreur s'affiche. Maintenant, une fois que vous sélectionnez les certificats par défaut, le bouton « Supprimer » est désactivé.
  [687610]
- Dans Citrix ADM, si vous supprimez une instance de Citrix ADC, les objets d'échec associés aux instances de Citrix ADC respectives ne sont pas supprimés.
  [690059]
- Les rapports d'événements (Réseaux > Événements > Rapports) ne s'affichent pas si la durée sélectionnée est « 1 mois ».
  [692054]
- Dans Citrix ADM, lors de l'interrogation des entités, si le nombre d'instances de Citrix ADC à découvrir est très élevé, l'interface utilisateur Citrix ADM risque de ne plus répondre.
  Solution : fermez votre navigateur Web et reconnectez-vous à votre Citrix ADM après 10-15 minutes.
  [692617]

Intégration

- Après avoir intégré un nouveau client dans Citrix ADM, et une fois que vous cliquez sur le bouton « Gérer », il peut afficher l'erreur « Page ne fonctionne pas » pour la première fois.
  [691018]

Problèmes connus

Les problèmes connus suivants existent dans cette version :

Agent

- Si vous utilisez un agent provisionné sur le cloud Microsoft Azure, les instances gérées associées à cet agent apparaissent à l'état de panne dans l'interface graphique Citrix ADM. [690941]
- Une fois l'enregistrement de l'agent terminé, il se peut que vous ne puissiez pas vous connecter à l'agent à partir de la console de l'Hypervisor.
  Solution : connectez-vous à l'agent à l'aide d'un client SSH. [691181]

Analytics

- Dans certains cas, les nœuds HDX Insight et Gateway Insight peuvent ne pas être affichés sur l'interface graphique graphique Citrix ADM.
  Solution : actualisez la page et réessayez. [690327]

Réseaux

- Si le proxy de contrôle n'est pas disponible pendant le processus de démarrage de l'agent, l'agent n'est pas en mesure de récupérer les paramètres d'interruption SNMP à partir de Citrix ADM et toutes les interruptions reçues des instances de Citrix ADC sont supprimées.
  Solution : Exécutez `masd restart` sur l'agent lorsque la connectivité à Citrix ADM a été établie. [687027]
- Lorsque vous configurez une règle pour surveiller des événements spécifiques dans Citrix ADM, les e-mails ne sont pas envoyés pour les événements qui correspondent aux critères de filtre. [688985]
- La fonctionnalité de mise à niveau de Citrix ADC dans les tâches de maintenance n'est pas prise en charge dans Citrix ADM. Mais, vous pouvez toujours afficher l'option dans l'interface graphique. [689068]

Paramètres

- Sur la page **Paramètres** > **Abonnements**, la consommation de données de stockage peut apparaître supérieure à la limite de stockage de 5 Go. [689330]
- Lorsque vous supprimez les utilisateurs de Citrix Cloud, les noms d'utilisateurs supprimés continuent d'apparaître dans Citrix ADM dans **Paramètres** > **Administration** des **utilisateurs > Utilisateurs**. [686581]

> **Remarque :** les étiquettes [XXXXXX] sont des ID de suivi internes utilisés par l'équipe Citrix ADM.

Août 13, 2017

Ceci est une version de correction de bug. Il n'y a pas de nouvelles fonctionnalités dans cette version.

Problèmes résolus

Les problèmes suivants ont été résolus dans cette version.

Analytics

- Lors de l'utilisation des informations HDX dans Citrix ADM, les géomaps peuvent ne pas fonctionner pour les blocs IP créés via le bloc IP privé. [691947]

- Lors de la création de deux sites de blocage IP, l'emplacement géographique du premier site IP n'est pas affiché correctement. Si vous supprimez et recréez le premier site IP, la carte géographique n'affiche aucune information sur le premier site IP. [691965]

Réseaux

Pour faciliter le débogage dans Citrix ADM, les fichiers journaux du sous-système affichent les noms des locataires pour les exceptions de base de données renvoyées. [692663]

Problèmes connus

Les problèmes connus suivants existent dans cette version :

Agent

- Si vous utilisez un agent provisionné sur le cloud Microsoft Azure, les instances gérées associées à cet agent apparaissent à l'état de panne dans l'interface graphique Citrix ADM. [690941]
- Une fois l'enregistrement de l'agent terminé, il se peut que vous ne puissiez pas vous connecter à l'agent à partir de la console de l'Hypervisor.
  Solution : connectez-vous à l'agent à l'aide d'un client SSH. [691181]

Analytics

- Dans certains cas, les nœuds HDX Insight et Gateway Insight peuvent ne pas être affichés sur l'interface graphique graphique Citrix ADM.
  Solution : actualisez la page et réessayez. [690327]

Réseaux

- Si le proxy de contrôle n'est pas disponible pendant le processus de démarrage de l'agent, l'agent n'est pas en mesure de récupérer les paramètres d'interruption SNMP à partir de Citrix ADM et toutes les interruptions reçues des instances de Citrix ADC sont supprimées.
  Solution : Exécutez `masd restart` sur l'agent lorsque la connectivité à Citrix ADM a été établie. [687027]
- Lorsque vous configurez une règle pour surveiller des événements spécifiques dans Citrix ADM, les e-mails ne sont pas envoyés pour les événements qui correspondent aux critères de filtre. [688985]
- La fonctionnalité de mise à niveau de Citrix ADC dans les tâches de maintenance n'est pas prise en charge dans Citrix ADM. Mais, vous pouvez toujours afficher l'option dans l'interface graphique. [689068]

Intégration

- Après avoir intégré un nouveau client dans Citrix ADM, et une fois que vous cliquez sur le bouton « Gérer », il peut afficher l'erreur « Page ne fonctionne pas » pour la première fois.
  Solution :
  attendez une heure (60 minutes) et reconnectez-vous. Le retard est dû au temps de provisionnement du nouveau locataire. [691018]

Paramètres

- Sur la page **Paramètres** > **Abonnements**, la consommation de données de stockage peut apparaître supérieure à la limite de stockage de 5 Go. [689330]
- Lorsque vous supprimez les utilisateurs de Citrix Cloud, les noms d'utilisateurs supprimés continuent d'apparaître dans Citrix ADM dans **Paramètres** > **Administration** des **utilisateurs > Utilisateurs**. [686581]

> **Remarque :** les étiquettes [XXXXXX] sont des ID de suivi internes utilisés par l'équipe Citrix ADM.

Août 10, 2017

Cette version inclut de nouvelles fonctionnalités et corrections de bugs.

Nouveautés

Les améliorations suivantes sont disponibles dans cette version.

Supprimer les messages Syslog dans Citrix ADM

Citrix ADM reçoit tous les syslogs configurés qui lui sont envoyés par les instances Citrix ADC gérées. En raison du grand nombre de messages syslog, les syslogs occupent un grand espace dans la base de données. Beaucoup de ces messages peuvent ne pas être d'importance pour vous et vous pouvez ne pas obtenir que les messages syslog importants.

Vous pouvez maintenant supprimer certains des syslogs reçus sur Citrix ADM en configurant des filtres. Les deux filtres que vous pouvez utiliser pour supprimer les journaux syslogs sont la gravité et la facilité. Vous pouvez supprimer les messages provenant d'une ou plusieurs instances de Citrix ADC.

Vous pouvez également utiliser des modèles de texte pour rechercher et supprimer des messages. Citrix ADM supprime tous les messages qui correspondent aux critères spécifiés. Les Syslogs supprimés ne sont pas visibles sur Citrix ADM et ne sont pas stockés dans la base de données client. Par conséquent, une grande quantité d'espace est enregistrée sur le serveur de stockage.

Pour plus d'informations, consultez : Comment supprimer les messages Syslog dans Citrix ADM

[6779274]

Générer et afficher des rapports sur les entités d'équilibrage de charge configurées sur les instances Citrix ADC

Vous pouvez générer des rapports sur les entités d'équilibrage de charge, telles que les serveurs virtuels et les services configurés sur des instances Citrix ADC gérées. Vous pouvez afficher les rapports consolidés de toutes les entités. Ces rapports vous permettent d'avoir une vue de haut niveau des éléments suivants :

- Instances Citrix ADC
- Équilibrage de charge des serveurs virtuels
- Partitions d'administration
- Services
- Groupes de services

Le rapport consolidé vous aide à créer un mappage entre ces entités. Pour plus d'informations, consultez : Comment générer des rapports pour les entités d'équilibrage de charge

[663174]

Enregistrer les valeurs de variable lorsqu'un travail de configuration est enregistré pour une exécution ultérieure

Lors de la création de tâches de configuration, vous pouvez spécifier des valeurs variables, mais enregistrer et exécuter le travail ultérieurement ou planifier l'exécution ultérieure de la tâche. Dans un tel scénario, Citrix ADM conserve désormais les valeurs de variable dans les tâches enregistrées.

[637830]

Prise en charge du port SSH personnalisé pour les instances Citrix ADC

Vous pouvez désormais spécifier un port SSH défini par l'utilisateur pour la communication entre Citrix ADM et les instances de Citrix ADC.

Pour définir le port SSH pour les profils d'instance

1. Connectez-vous à Citrix ADM à l'aide d'un navigateur Web pris en charge.
2. Accédez à **Réseaux** et sélectionnez le type d'instance de l'instance Citrix ADC que vous souhaitez découvrir dans Citrix ADM.
3. Cliquez sur **Profils**.
4. Dans la page **Profils d'administration**, cliquez sur **Ajouter** .
5. Dans le **port SSH**, tapez le numéro de port SSH personnalisé configuré pour les instances Citrix ADC pour communiquer avec Citrix ADM.
6. Cliquez sur **OK**.

[689369]

Problèmes résolus

Les problèmes suivants ont été résolus dans cette version.

Agent

Par défaut, seul l'utilisateur super administrateur (le premier utilisateur de votre organisation à s'inscrire et à ouvrir une session à Citrix ADM) a l'autorisation de générer le code d'activation requis pour enregistrer un agent sur le service. Un administrateur délégué (chaque utilisateur suivant qui ouvre une session) n'a pas l'autorisation de générer le code d'activation. Lorsqu'un administrateur délégué clique sur Générer le code d'activation, l'erreur suivante apparaît : « Non autorisé à effectuer cette opération. «
[690576]

Analyse et gestion des applications

Le tableau de bord des applications dans Citrix ADM affiche des mesures de sécurité incorrectes pour les applications personnalisées.

[689041]

Réseaux

- Lorsque vous configurez une règle pour surveiller des événements spécifiques dans Citrix ADM, les interruptions SNMP ne sont pas envoyées à des destinations d'interruptions externes. [689018]
- Lorsque vous configurez une règle pour surveiller des événements spécifiques dans Citrix ADM, tâche n'est pas exécutée pour les événements qui correspondent aux critères de filtre que vous avez spécifiés. [688986]
- Lorsque vous configurez une règle pour surveiller des événements spécifiques dans Citrix ADM, les événements ne sont pas supprimés pour la période configurée. [688988]
- Lorsque vous créez un groupe dans Citrix ADM à partir de Paramètres > Administration des utilisateurs > Groupe, le message de succès indiquant que le groupe est créé s'affiche avant que toutes les étapes de l'Assistant soient terminées. [684944]

Problèmes connus

Les problèmes connus suivants existent dans cette version :

Agent

- Si vous utilisez un agent provisionné sur le cloud Microsoft Azure, les instances gérées associées à cet agent apparaissent à l'état de panne dans l'interface graphique Citrix ADM. [690941]
- Une fois l'enregistrement de l'agent terminé, il se peut que vous ne puissiez pas vous connecter à l'agent à partir de la console de l'Hypervisor.
  Solution : connectez-vous à l'agent à l'aide d'un client SSH. [691181]

Analytics

- Dans certains cas, les nœuds HDX Insight et Gateway Insight peuvent ne pas être affichés sur l'interface graphique graphique Citrix ADM.
  Solution : actualisez la page et réessayez. [690327]

Réseaux

- Si le proxy de contrôle n'est pas disponible pendant le processus de démarrage de l'agent, l'agent n'est pas en mesure de récupérer les paramètres d'interruption SNMP à partir de Citrix ADM et toutes les interruptions reçues des instances de Citrix ADC sont supprimées.
  Solution : Exécutez `masd restart` sur l'agent lorsque la connectivité à Citrix ADM a été établie. [687027]
- Lorsque vous configurez une règle pour surveiller des événements spécifiques dans Citrix ADM, les e-mails ne sont pas envoyés pour les événements qui correspondent aux critères de filtre. [688985]
- La fonctionnalité de mise à niveau de Citrix ADC dans les tâches de maintenance n'est pas prise en charge dans Citrix ADM. Mais, vous pouvez toujours afficher l'option dans l'interface graphique. [689068]

Intégration

- Après avoir intégré un nouveau client dans Citrix ADM, et une fois que vous cliquez sur le bouton « Gérer », il peut afficher l'erreur « Page ne fonctionne pas » pour la première fois.
  Solution :
  attendez une heure (60 minutes) et reconnectez-vous. Le retard est dû au temps nécessaire pour Provisioning le nouveau locataire. [691018]

Paramètres

- Sur la page **Paramètres** > **Abonnements**, la consommation de données de stockage peut apparaître supérieure à la limite de stockage de 5 Go. [689330]
- Lorsque vous supprimez les utilisateurs de Citrix Cloud, les noms d'utilisateurs supprimés continuent d'apparaître dans Citrix ADM dans **Paramètres** > **Administration** des **utilisateurs > Utilisateurs**. [686581]

> **Remarque :** les étiquettes [XXXXXX] sont des ID de suivi internes utilisés par l'équipe Citrix ADM.

Juillet 23, 2017

Ceci est une version de correction de bug. Il n'y a pas de nouvelles fonctionnalités dans cette version.

Problèmes résolus

Les problèmes suivants ont été résolus dans cette version.

Citrix Cloud

Après vous être connecté à citrix.cloud.com, cliquez sur le bouton **Gérer** de la vignette Citrix ADM affiche l'erreur suivante "page non disponible."
[690267]

Réseaux

Si vous avez activé l'accès sécurisé uniquement sur vos instances de Citrix ADC, ces instances ne sont pas détectées correctement dans Citrix ADM et l'état peut apparaître comme « hors service » une fois le processus de découverte terminé.
[690431]

Problèmes connus

Les problèmes connus suivants existent dans cette version :

Agent

- Si vous utilisez un agent provisionné sur le cloud Microsoft Azure, les instances gérées associées à cet agent apparaissent à l'état de panne dans l'interface graphique Citrix ADM. [690941]
- Une fois l'enregistrement de l'agent terminé, il se peut que vous ne puissiez pas vous connecter à l'agent à partir de la console de l'Hypervisor.
  Solution : connectez-vous à l'agent à l'aide d'un client SSH. [691181]
- Par défaut, seul l'utilisateur super administrateur (le premier utilisateur de votre organisation à s'inscrire et à ouvrir une session à Citrix ADM) a l'autorisation de générer le code d'activation requis pour enregistrer un agent sur le service. Un administrateur délégué (chaque utilisateur suivant qui ouvre une session) n'a pas l'autorisation de générer le code d'activation. Lorsqu'un administrateur délégué clique sur **Générer le code d'activation**, l'erreur suivante apparaît : "Non autorisé à effectuer cette opération."

Solution : lesuper administrateur doit attribuer les autorisations requises à l'administrateur délégué. Pour plus de détails, consultez Comment attribuer des autorisations supplémentaires à des utilisateurs d'administration délégués. [690576]

Analytics

- Dans certains cas, les nœuds HDX Insight et Gateway Insight peuvent ne pas être affichés sur l'interface graphique graphique Citrix ADM.
  Solution : actualisez la page et réessayez. [690327]

Analyse et gestion des applications

- Si vous utilisez le navigateur Safari sur le système d'exploitation Microsoft Windows, App Dashboard et Security Analytics Dashboard ne se chargent pas. Vous pouvez voir d'autres fonctionnalités de Citrix ADM. [688617]
- Le tableau de bord des applications dans Citrix ADM affiche des mesures de sécurité incorrectes pour les applications personnalisées. [689041]

Réseaux

- Si le proxy de contrôle n'est pas disponible pendant le processus de démarrage de l'agent, l'agent n'est pas en mesure de récupérer les paramètres d'interruption SNMP à partir de Citrix ADM et toutes les interruptions reçues des instances de Citrix ADC sont supprimées.
  Solution : Exécutez `masd restart` sur l'agent lorsque la connectivité à Citrix ADM a été établie. [687027]
- Lorsque vous configurez une règle pour surveiller des événements spécifiques dans Citrix ADM, les e-mails ne sont pas envoyés pour les événements qui correspondent aux critères de filtre. [688985]
- Lorsque vous configurez une règle pour surveiller des événements spécifiques dans Citrix ADM, tâche n'est pas exécutée pour les événements qui correspondent aux critères de filtre que vous avez spécifiés. [688986]
- Lorsque vous configurez une règle pour surveiller des événements spécifiques dans Citrix ADM, les événements ne sont pas supprimés pour la période configurée. [688988]
- Lorsque vous configurez une règle pour surveiller des événements spécifiques dans Citrix ADM, les interruptions SNMP ne sont pas envoyées à des destinations d'interruptions externes. [689018]
- La fonctionnalité de mise à niveau de Citrix ADC dans les tâches de maintenance n'est pas prise en charge dans Citrix ADM. Mais, vous pouvez toujours afficher l'option dans l'interface graphique. [689068]

Paramètres

- Sur la page **Paramètres** > **Abonnements**, la consommation de données de stockage peut apparaître supérieure à la limite de stockage de 5 Go. [689330]
- Vous pouvez être déconnecté de Citrix ADM brusquement.
  Solution : connectez-vous à nouveau à Citrix ADM. [689012]
- Lorsque vous supprimez les utilisateurs de Citrix Cloud, les noms d'utilisateurs supprimés continuent d'apparaître dans Citrix ADM dans **Paramètres** > **Administration** des **utilisateurs > Utilisateurs**. [686581]

> **Remarque :** les étiquettes [XXXXXX] sont des ID de suivi internes utilisés par l'équipe Citrix ADM.

Juillet 16, 2017

Ceci est une version de correction de bug. Il n'y a pas de nouvelles fonctionnalités dans cette version.

Problèmes résolus

Les problèmes suivants ont été résolus dans cette version :

Analytics

- Lorsque vous utilisez l'agent Citrix ADM dans AWS (AWS), les données d'analyse ne sont pas affichées en tant que package de télémétrie qui contient des fonctionnalités ULFD est manquant dans l'AMI de l'agent. [690225]
- L'exportation de rapports vers PDF/JPEG/PNG ne fonctionne pas dans Citrix ADM. [683778]
- Si vous activez Insight à partir de Citrix ADM, la coche en regard de AppFlow n'apparaît pas activée. Toutefois, la configuration permettant d'activer AppFlow est transmise aux instances Citrix ADC. [688309]

Réseaux

- Vous ne pouvez pas télécharger un fichier de commandes lors de la création d'une tâche de configuration, bien que **Réseaux** > **Travaux de configuration** > **Créer un travail** affiche l'option permettant de charger un fichier.
  [688967]
- L'enregistrement de l'agent échoue si vous utilisez la casse de titre dans le nom du client. Par exemple, `Haroldmas`, `kimiRKN`.
  [689648]

Problèmes connus

Les problèmes connus suivants existent dans cette version :

Analyse et gestion des applications

- Si vous utilisez le navigateur Safari sur le système d'exploitation Microsoft Windows, App Dashboard et Security Analytics Dashboard ne se chargent pas. Vous pouvez voir d'autres fonctionnalités de Citrix ADM. [688617]
- Le tableau de bord des applications dans Citrix ADM affiche des mesures de sécurité incorrectes pour les applications personnalisées. [689041]

Réseaux

- Si le proxy de contrôle n'est pas disponible pendant le processus de démarrage de l'agent, l'agent n'est pas en mesure de récupérer les paramètres d'interruption SNMP à partir de Citrix ADM et toutes les interruptions reçues des instances de Citrix ADC sont supprimées.
  Solution : Exécutez `masd restart` sur l'agent lorsque la connectivité à Citrix ADM a été établie. [687027]
- Lorsque vous configurez une règle pour surveiller des événements spécifiques dans Citrix ADM, les e-mails ne sont pas envoyés pour les événements qui correspondent aux critères de filtre. [688985]
- Lorsque vous configurez une règle pour surveiller des événements spécifiques dans Citrix ADM, tâche n'est pas exécutée pour les événements qui correspondent aux critères de filtre que vous avez spécifiés. [688986]
- Lorsque vous configurez une règle pour surveiller des événements spécifiques dans Citrix ADM, les événements ne sont pas supprimés pour la période configurée. [688988]
- Lorsque vous configurez une règle pour surveiller des événements spécifiques dans Citrix ADM, les interruptions SNMP ne sont pas envoyées à des destinations d'interruptions externes. [689018]
- La fonctionnalité de mise à niveau de Citrix ADC dans les tâches de maintenance n'est pas prise en charge dans Citrix ADM. Mais, vous pouvez toujours afficher l'option dans l'interface graphique. [689068]

Paramètres

- Sur la page **Paramètres** > **Abonnements**, la consommation de données de stockage peut apparaître supérieure à la limite de stockage de 5 Go. [689330]
- Vous pouvez être déconnecté de Citrix ADM brusquement.
  Solution : connectez-vous à nouveau à Citrix ADM. [689012]

- Lorsque vous supprimez les utilisateurs de Citrix Cloud, les noms d'utilisateurs supprimés continuent d'apparaître dans Citrix ADM dans **Paramètres** > **Administration** des **utilisateurs > Utilisateurs**. [686581]

> **Remarque :** les étiquettes [XXXXXX] sont des ID de suivi internes utilisés par l'équipe Citrix ADM.

30 juin 2017

Il s'agit de la première version de Citrix ADM. Pour obtenir la liste des fonctionnalités disponibles, reportez-vous à la sectionCaractéristiques et solutions.

Les problèmes connus suivants existent dans cette version :

Analytics

- L'exportation de rapports vers PDF/JPEG/PNG ne fonctionne pas dans Citrix Citrix ADM. [683778]
- Si vous activez Insight à partir de Citrix ADM, la coche en regard de AppFlow n'apparaît pas activée. Toutefois, la configuration permettant d'activer AppFlow est poussée vers les instances Citrix ADC. [688309]

Analyse et gestion des applications

- Si vous utilisez le navigateur Safari sur le système d'exploitation Microsoft Windows, App Dashboard et Security Analytics Dashboard ne se chargent pas. Vous pouvez voir d'autres fonctionnalités de Citrix ADM. [688617]
- Le tableau de bord des applications dans Citrix ADM affiche des mesures de sécurité incorrectes pour les applications personnalisées. [689041]

Réseaux

- Si le proxy de contrôle n'est pas disponible pendant le processus de démarrage de l'agent, l'agent ne peut pas récupérer les paramètres d'interruption SNMP à partir de Citrix ADM, et toutes les interruptions reçues des instances de Citrix ADC sont supprimées.
  Solution : Exécutez `masd restart` sur l'agent lorsque la connectivité à Citrix ADM a été établie. [687027]
- Vous ne pouvez pas télécharger un fichier de commandes lors de la création d'une tâche de configuration, bien que **Réseaux** > **Travaux de configuration** > **Créer un travail** affiche l'option permettant de charger un fichier. [688967]
- Lorsque vous configurez une règle pour surveiller des événements spécifiques dans Citrix ADM, les e-mails ne sont pas envoyés pour les événements qui correspondent aux critères de filtre. [688985]

- Lorsque vous configurez une règle pour surveiller des événements spécifiques dans Citrix ADM, le travail n'est pas exécuté pour les événements qui correspondent aux critères de filtre que vous avez spécifiés. [688986]
- Lorsque vous configurez une règle pour surveiller des événements spécifiques dans Citrix ADM, les événements ne sont pas supprimés pour la période configurée. [688988]
- Lorsque vous configurez une règle pour surveiller des événements spécifiques dans Citrix ADM, les interruptions SNMP ne sont pas envoyées à des destinations d'interruptions externes. [689018]
- La fonctionnalité de mise à niveau de Citrix ADC dans les tâches de maintenance n'est pas prise en charge dans Citrix ADM. Mais, vous pouvez toujours afficher l'option dans l'interface graphique. [689068]

Paramètres

- Sur la page **Paramètres** > **Abonnements**, la consommation de données de stockage peut apparaître supérieure à la limite de stockage de 5 Go. [689330]
- Vous pouvez être déconnecté de Citrix ADM brusquement.
  Solution : reconnectez-vous à Citrix ADM. [689012]
- Lorsque vous supprimez des utilisateurs de Citrix Cloud, les noms d'utilisateurs supprimés continuent d'apparaître dans Citrix ADM dans **Paramètres** > **Administration** des **utilisateurs > Utilisateurs** . [686581]

> **Remarque :** les étiquettes [XXXXXX] sont des ID de suivi internes utilisés par l'équipe Citrix ADM.

Mise en route

April 29, 2021

Ce document vous explique comment commencer à intégrer et configurer Citrix Application Delivery Management (Citrix ADM) pour la première fois. Ce document est destiné aux administrateurs réseau et d'applications qui gèrent les périphériques réseau Citrix (Citrix ADC, SD-WAN WO, Citrix Gateway, Citrix Secure Web Gateway, etc.). 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.

[Avant de commencer l'intégration, assurez-vous d'examiner lesconfiguration requise pour le navigateur/en-us/citrix-application-delivery-management-service/system-requirements.html#supported-browsersconfiguration requise pour l'installation de l'agent/en-us/citrix-application-delivery-management-service/system-requirements.html#agent-installation-requirements[([])], les et les exigences portuaires/en-us/citrix-application-delivery-management-service/system-requirements.html#ports().]

Étape 1 : Inscrivez-vous à Citrix Cloud

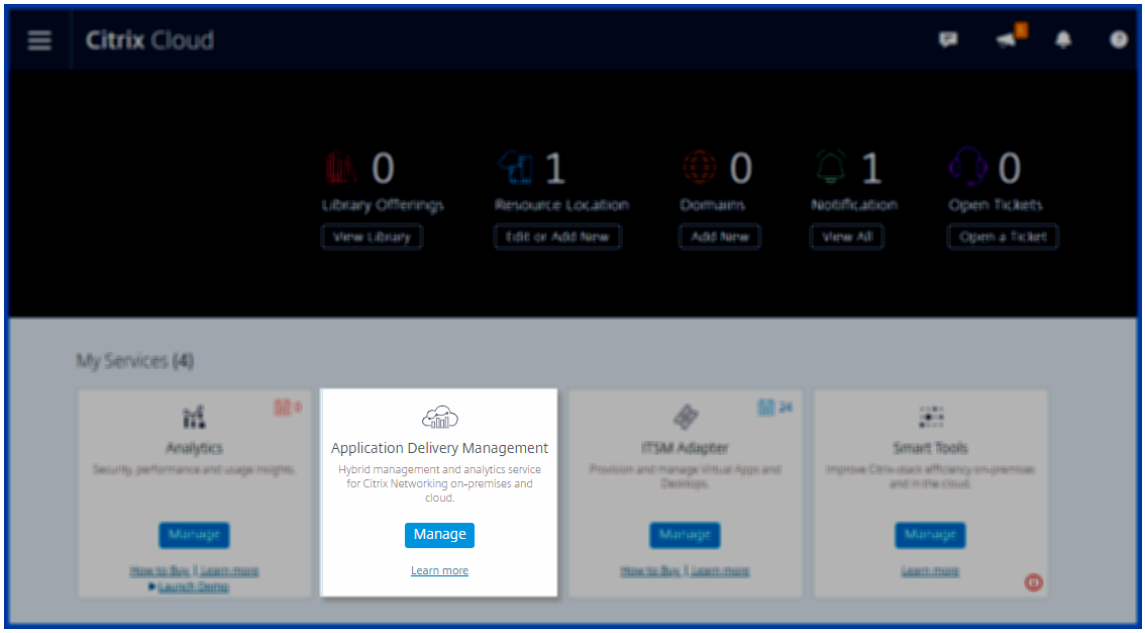
Pour commencer à utiliser Citrix ADM, vous devez d'abord créer un compte d'entreprise Citrix Cloud ou rejoindre un compte existant créé par un autre membre de votre entreprise. Pour des processus détaillés et des instructions sur la procédure à suivre, reportez-vous à la section Inscription à Citrix Cloud.

Étape 2 : Gérer Citrix ADM avec un compte Express

Après vous être connecté à Citrix Cloud, procédez comme suit :

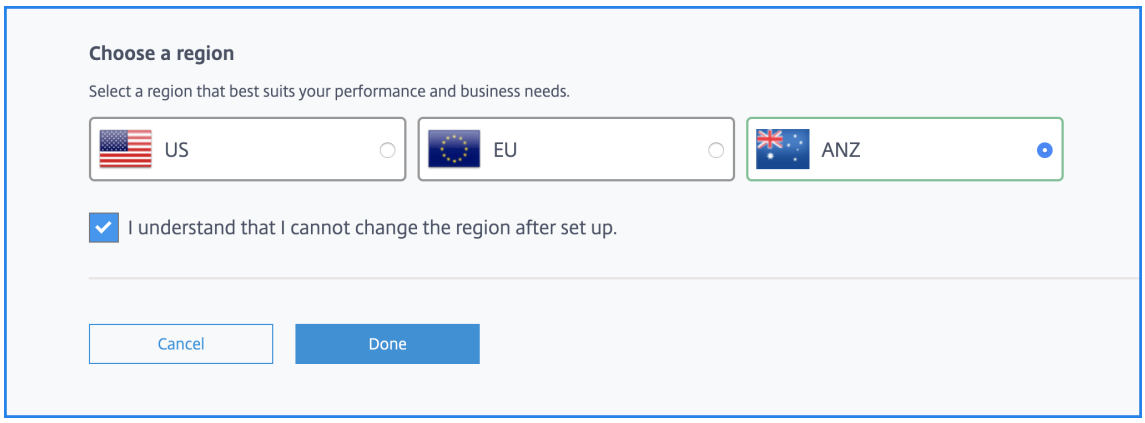
1. Accédez à la section **Services disponibles**.
2. Dans la vignette **Application Delivery Management**, cliquez sur **Gérer** .

   La vignette **Application Delivery Management** se déplace vers la section **Mes services** .



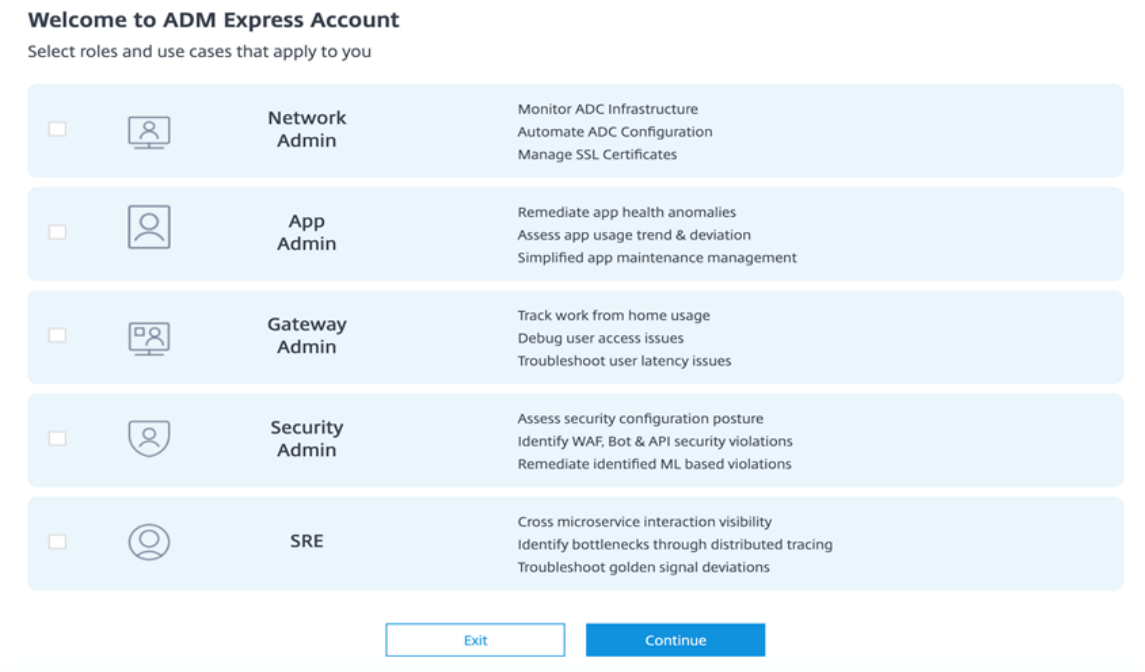
3. Sélectionnez l'une des régions suivantes qui répond aux besoins de votre entreprise :

   - États-Unis (US)
   - Europe (UE)
   - Australie (ANZ)

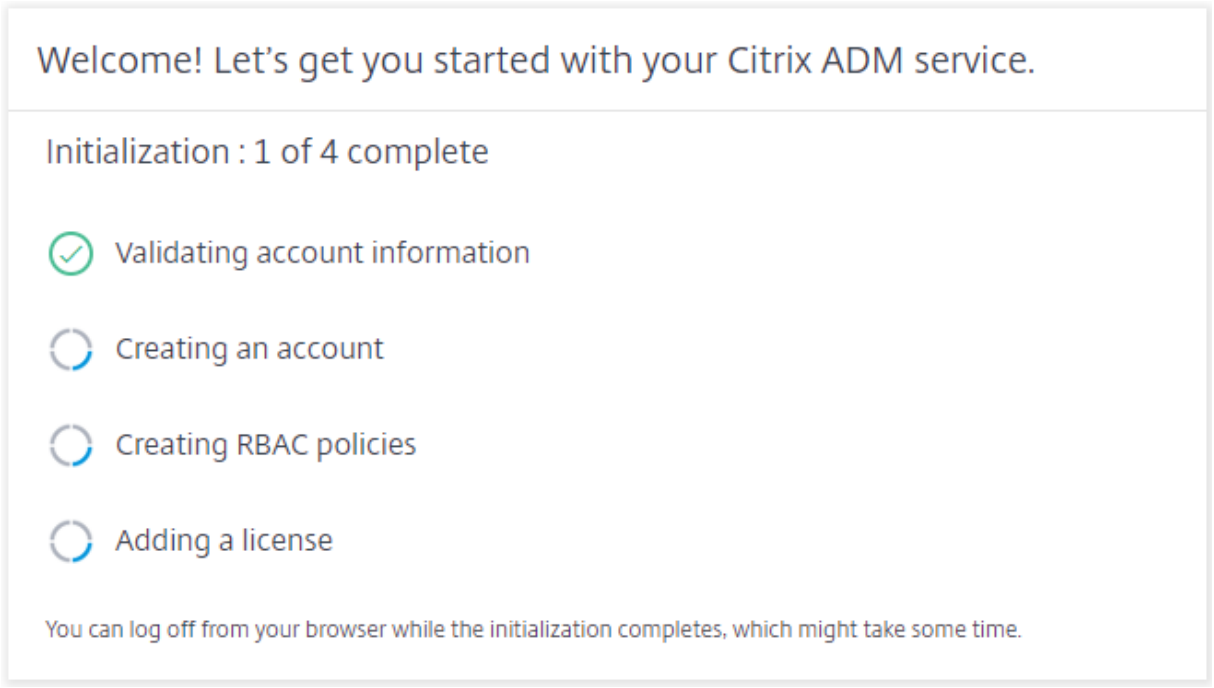


> **Important**
>
> Vous ne pouvez pas modifier la région ultérieurement.

4. Sélectionnez les rôles et les cas d'utilisation qui s'appliquent à vous.

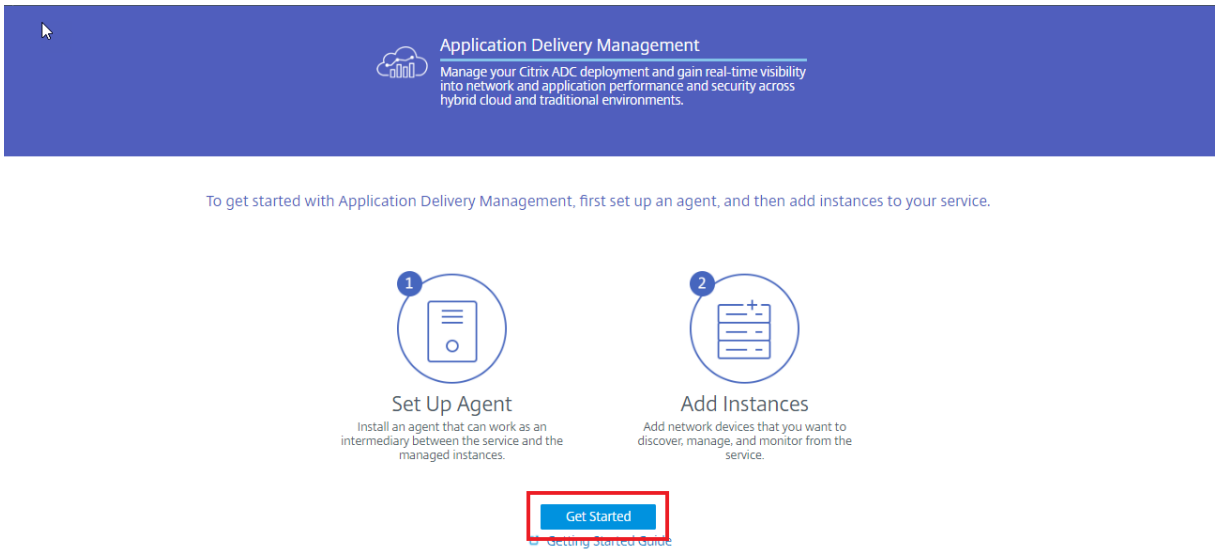


Vous pouvez vous déconnecter du navigateur pendant que l'initialisation se termine en arrière-plan, ce qui peut prendre un certain temps.



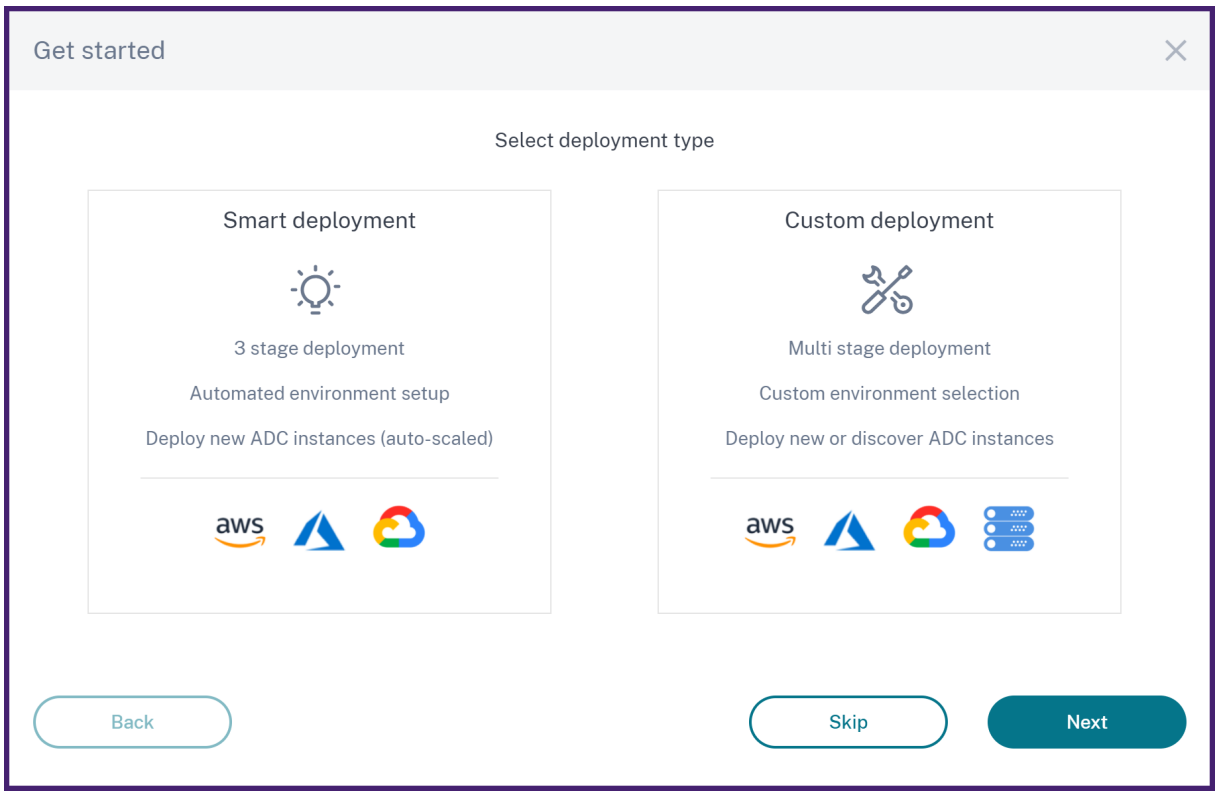
> **Remarque**
>
> Citrix affecte un compte Express pour gérer les ressources ADM. Si votre compte Citrix ADM Express reste inactif pendant 90 jours, le compte est supprimé. Pour de plus amples informations, consultez la section Gérer Citrix ADM Service à l'aide d'un compte Express.

Lorsque vous vous reconnectez à votre compte Citrix Cloud, l'écran de l' **interface graphique Citrix ADM** s'affiche. Cliquez sur **Démarrer** pour commencer à configurer le service pour la première fois.



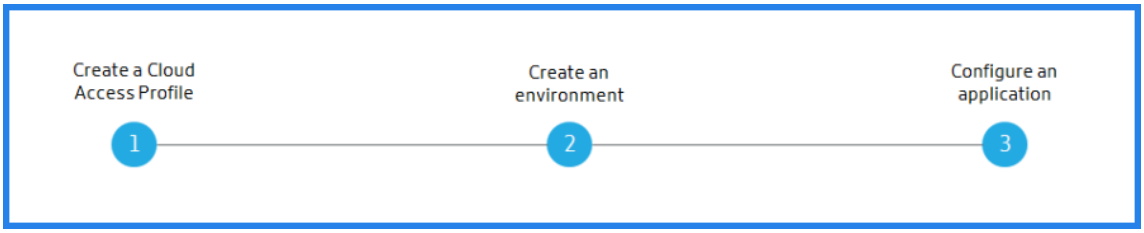
Étape 3 : Sélectionner un type de déploiement ADC

Sélectionnez l'une des options de déploiement suivantes qui répond aux besoins de votre entreprise :



- Déploiement intelligent - Cette option est une configuration d'environnement automatisée permettant de déployer de nouvelles instances ADC. Il installe automatiquement un agent pour activer la communication entre Citrix ADM et les instances gérées.

  Cette option prend actuellement en charge l'environnement AWS uniquement. En trois étapes, vous pouvez fournir une application présente dans AWS à l'aide d'instances ADC.

- Déploiement personnalisé - Cette option est un déploiement multi-étapes. Vous pouvez sélectionner chaque option d'environnement et déployer ou découvrir des instances ADC.

Sélectionner un déploiement intelligent

Cette option de déploiement crée l'infrastructure suivante dans AWS :

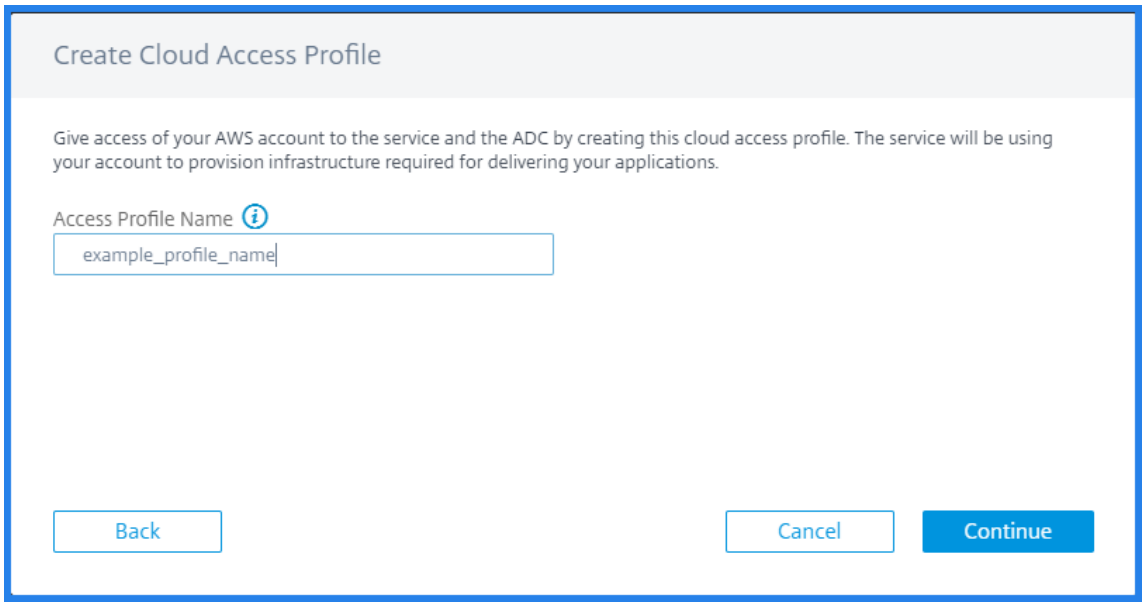
- Une pile CloudFormation dans AWS pour créer l'infrastructure requise qui inclut des sous-réseaux, des groupes de sécurité, des passerelles NAT, etc.
- Agent ADM dans le VPC pour gérer les instances ADC.
- Un groupe de mise à Autoscale ADC. Vous pouvez personnaliser ce groupe ultérieurement dans la page **Réseaux > Groupe de Autoscale**.

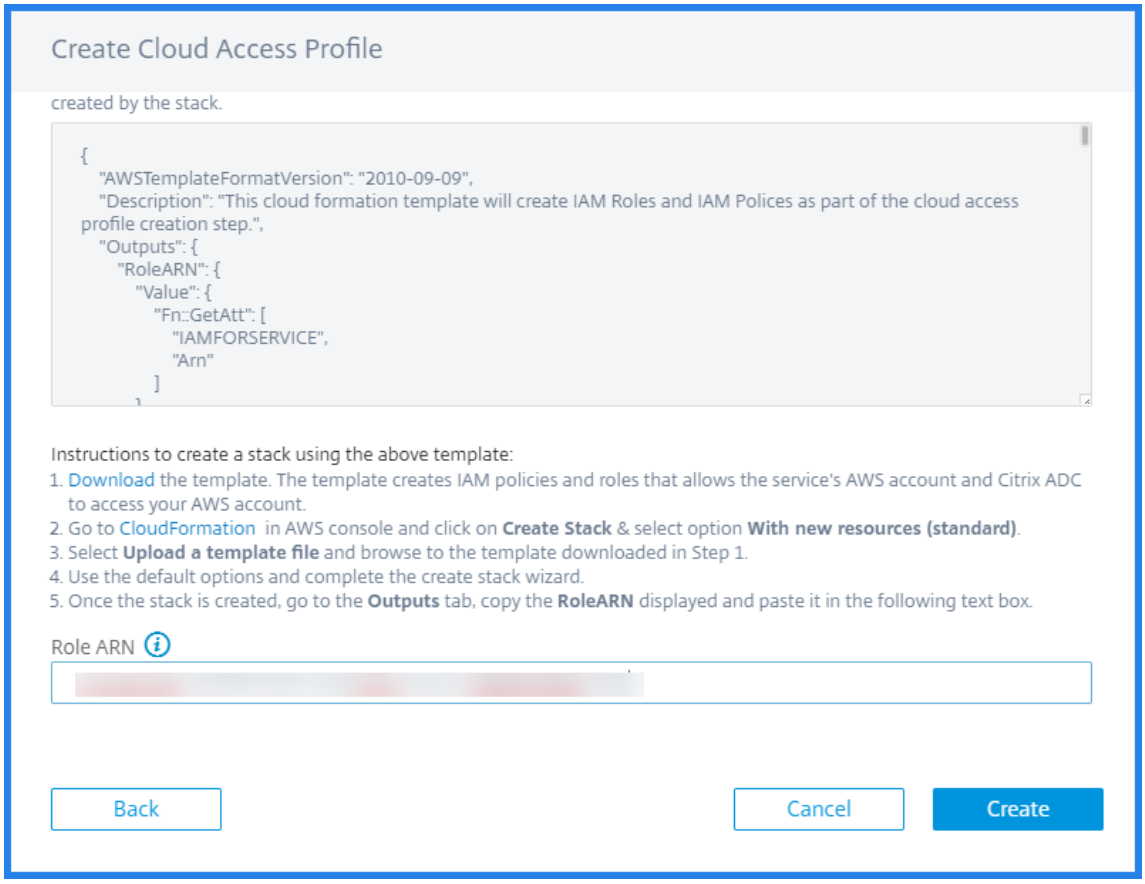
Avant de déployer des instances ADC, vérifiez les éléments suivants :

1. Vous possédez déjà un compte AWS.
2. Vous avez créé un utilisateur IAM avec toutes les autorisations administratives.

Pour déployer des instances ADC, effectuez les opérations suivantes :

1. Spécifiez **le nom du profil d'accès** et l' **ARN de rôle** pour créer un profil d'accès au cloud.



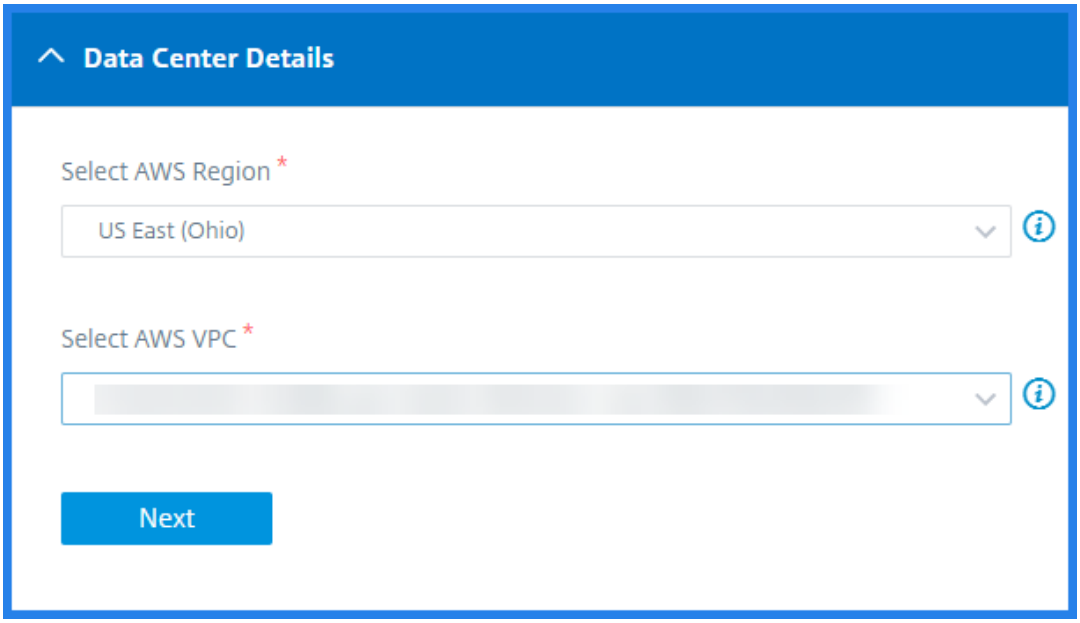


Le service ADM utilise le profil d'accès au cloud pour accéder à un compte AWS.

2. Spécifiez les détails suivants pour préparer l'environnement AWS :

   a) Dans **Détails du centre de données**, sélectionnez **Région AWSet AWS VPC** où vous souhaitez déployer des instances ADC.

   AWS VPC répertorie les VPC présents dans la **région AWS**sélectionnée.



b) Dans **ADC Autoscale Group Details**, spécifiez les éléments suivants pour mettre à l'échelle automatique des instances ADC dans le cloud AWS :

- **Nom du groupe de mise à l'Autoscale** : nom permettant d'identifier un groupe de mise à l'échelle automatique.
- **Zones de disponibilité** : sélectionnez les zones dans lesquelles vous souhaitez créer les groupes Mise à l'Autoscale.

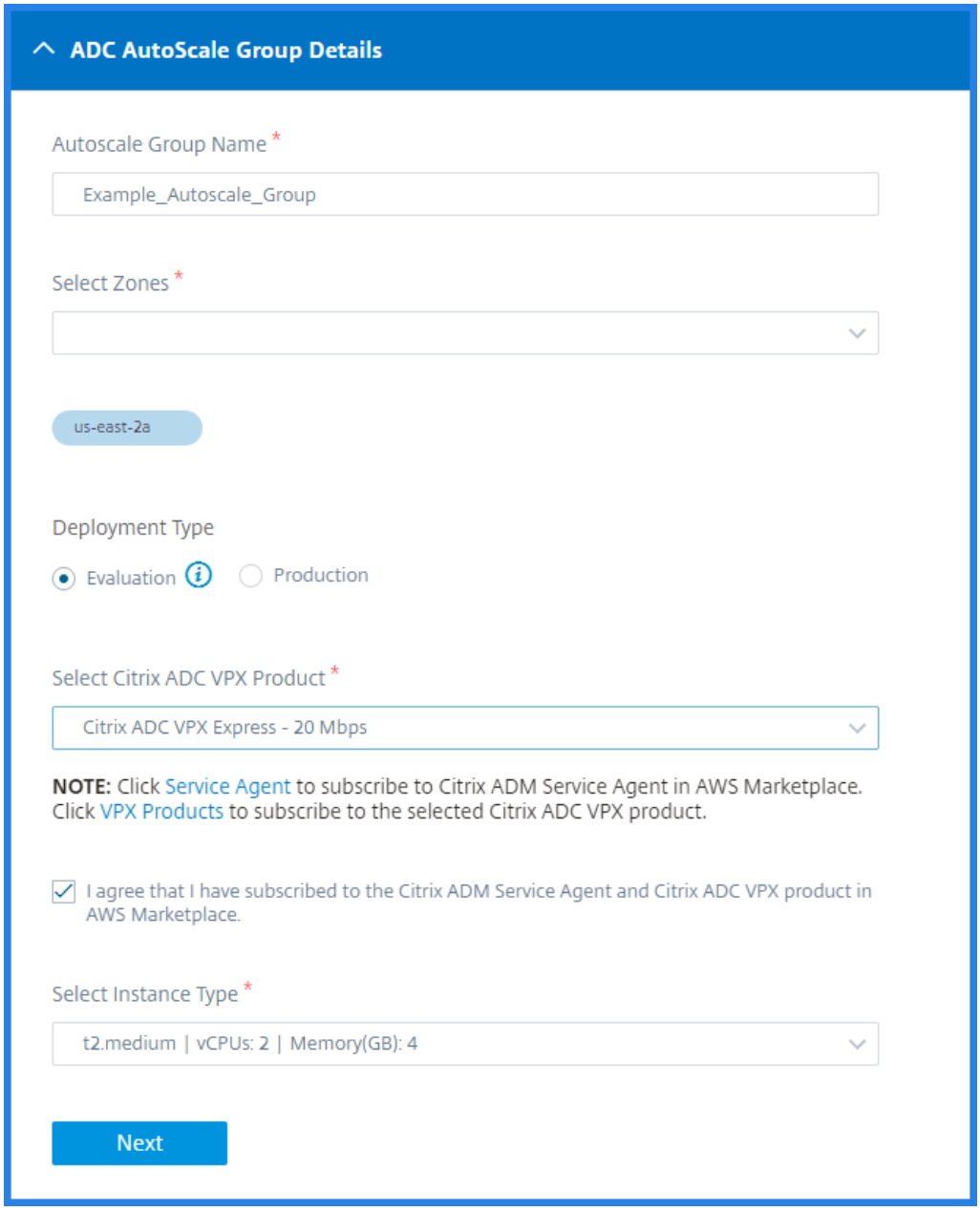
  Vous pouvez sélectionner plusieurs zones dans la liste.
- **Type de déploiement** : sélectionnez **l'option Évaluation** ou **Production**.

  Si vous souhaitez évaluer la solution de mise à l'Autoscale ADM avant d'acheter la licence de production, sélectionnez l'option **Évaluation**.

  > **Important**
  >
  > – L'option d'évaluation ne prend en charge qu'une seule zone de disponibilité.
  > - Avec l'option d'évaluation, vous pouvez sélectionner uniquement Citrix ADC VPX Express. De plus, la solution de Autoscale ADM peut évoluer jusqu'à trois instances ADC.
- **Produit Citrix ADC VPX** - Sélectionnez les licences pour provisionner les instances ADC.

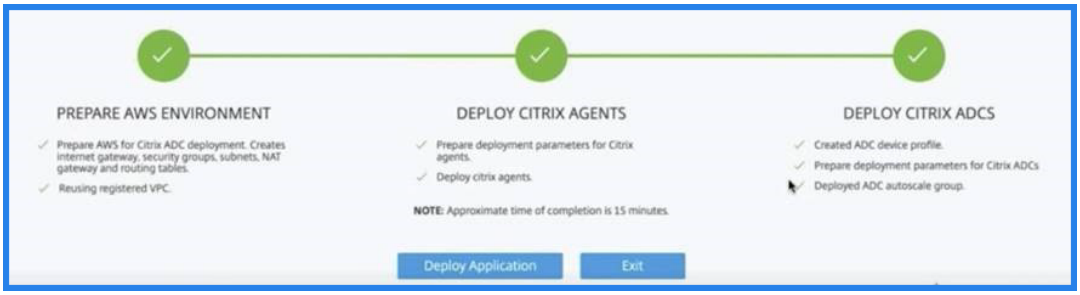
  Abonnez-vous à la licence sélectionnée sur AWS Marketplace et revenez à cette page.

  Vérifiez et sélectionnez le message de consentement de l'utilisateur.
- **Type d'instance** : sélectionnez le type d'instance requis.



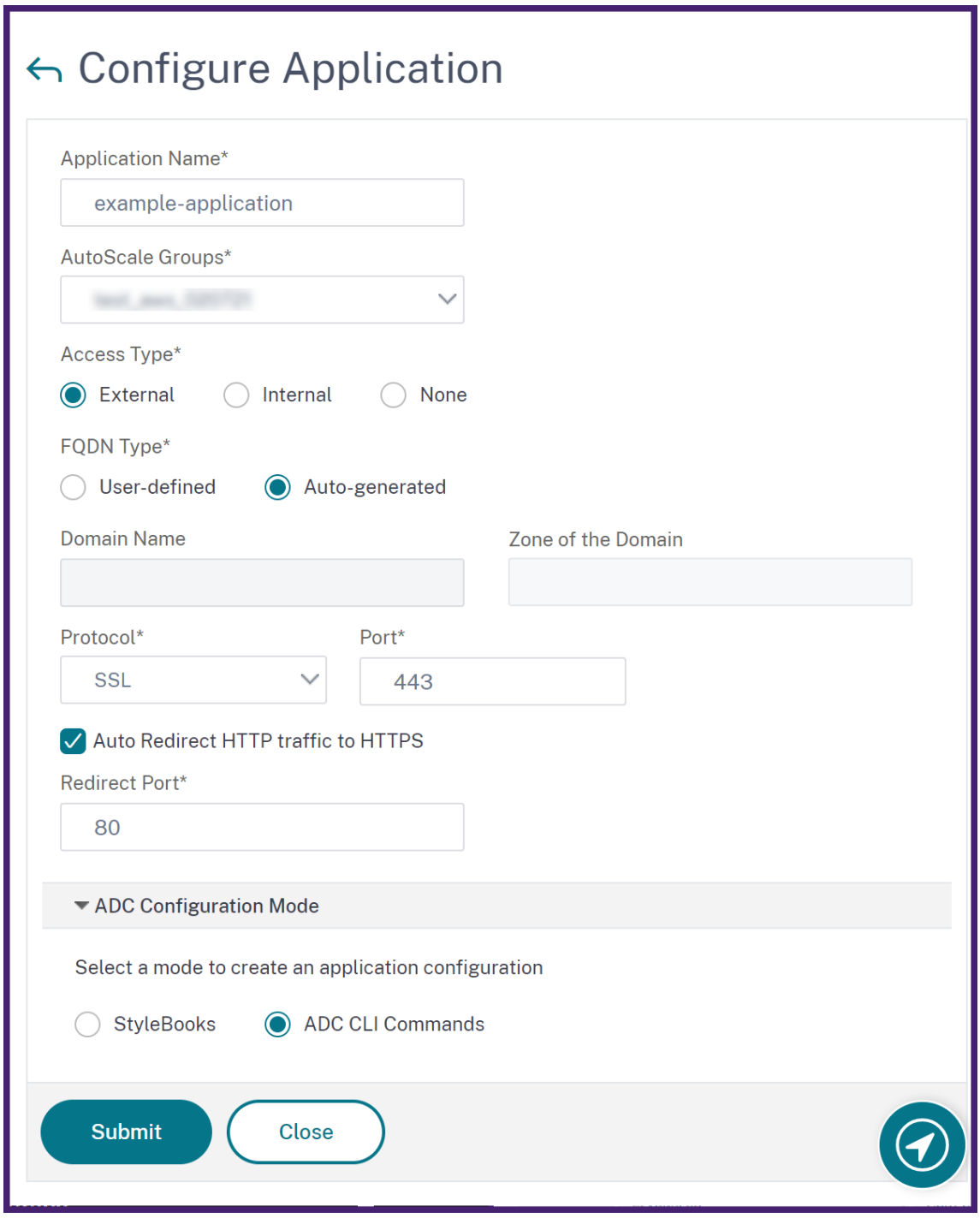
c) Cliquez sur **Suivant**.

Après la validation réussie, cliquez sur **Créer** pour déployer des instances ADC dans AWS et créer un groupe de Autoscale.

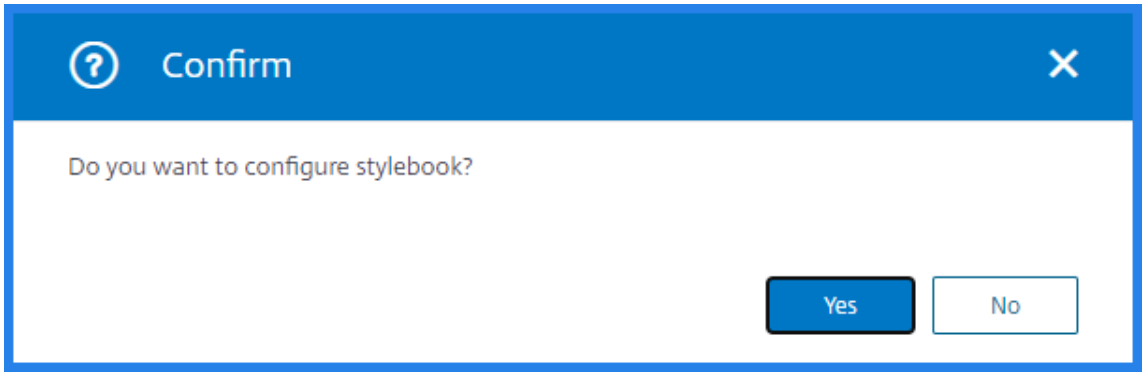


3. Après le déploiement ADC réussi, cliquez sur **Déployer l'application**.

    a) Dans **Configurer l'application**, spécifiez les détails nécessaires et cliquez sur **Soumettre**.



Si vous souhaitez configurer une application à l'aide de StyleBooks, sélectionnez **Oui** dans la fenêtre de confirmation.



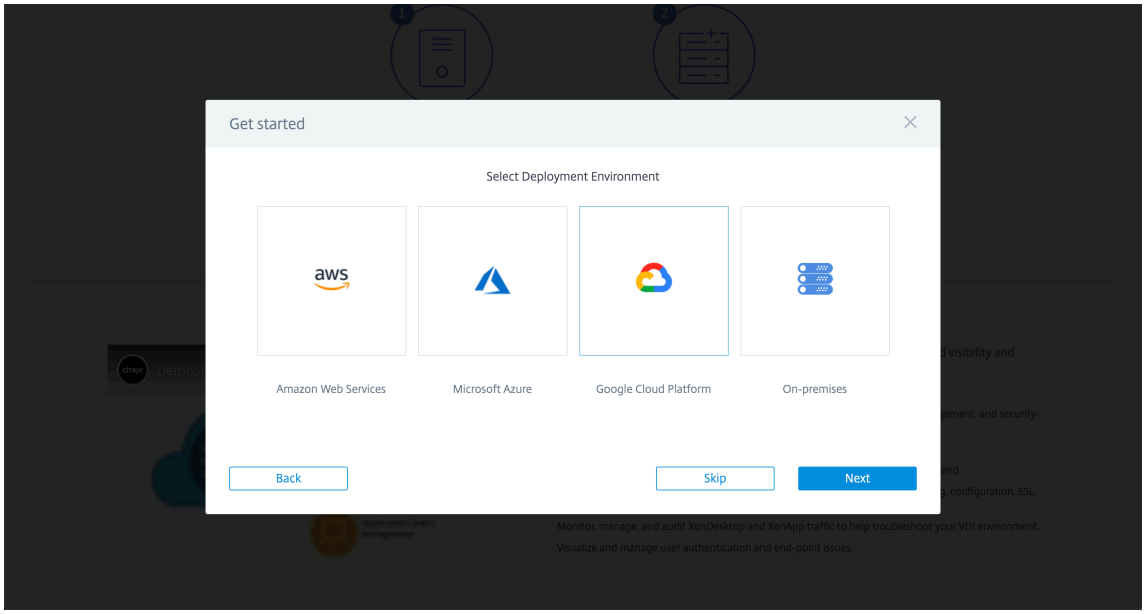
Pour de plus amples informations, consultez la section Configurer une application pour le groupe Autoscale.

Sélectionner un déploiement personnalisé

Cette option permet un déploiement en plusieurs étapes. Sélectionnez cette option pour découvrir les instances ADC de différents environnements. Avec cette option, vous pouvez également déployer de nouvelles instances en spécifiant des options d'environnement personnalisées.

Procédez comme suit pour déployer ou découvrir des instances ADC :

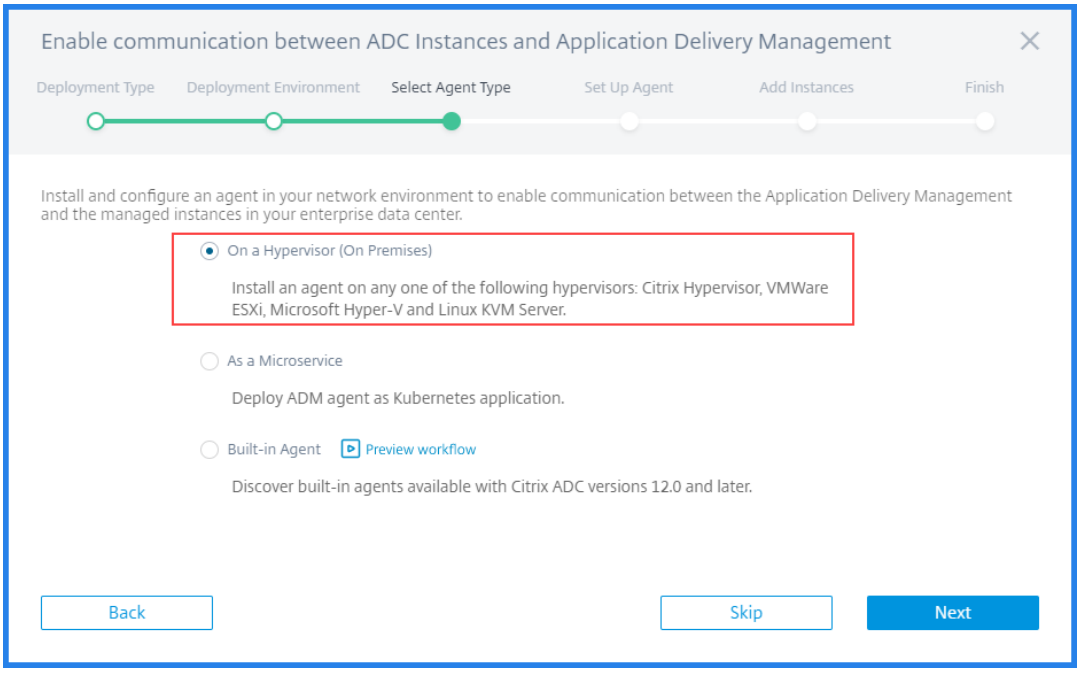
1. Sélectionnez l'un des environnements suivants :
    - **Amazon Web Services**
    - **Microsoft Azure**
    - **Plate-forme Google Cloud**
    - **Sur site**



2. Installez Citrix ADM Agent pour activer la communication entre Citrix ADM et les instances gérées dans votre centre de données ou cloud.

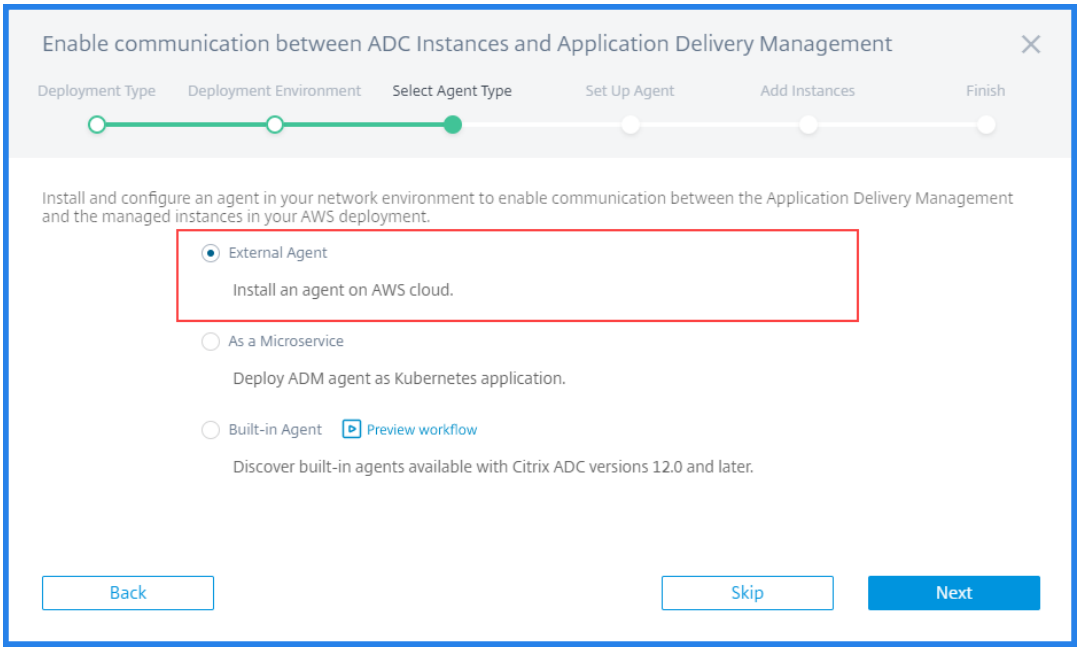
   L'étape **Sélectionner le type** d'agent varie les options d'installation de l'agent en fonction de l'environnement sélectionné.

   - **Sur site** - Si vous sélectionnez **Sur site**, vous pouvez installer un agent sur les hyperviseurs suivants :
     - Citrix Hypervisor
     - VMware ESXi
     - Microsoft Hyper-V
     - Serveur KVM Linux

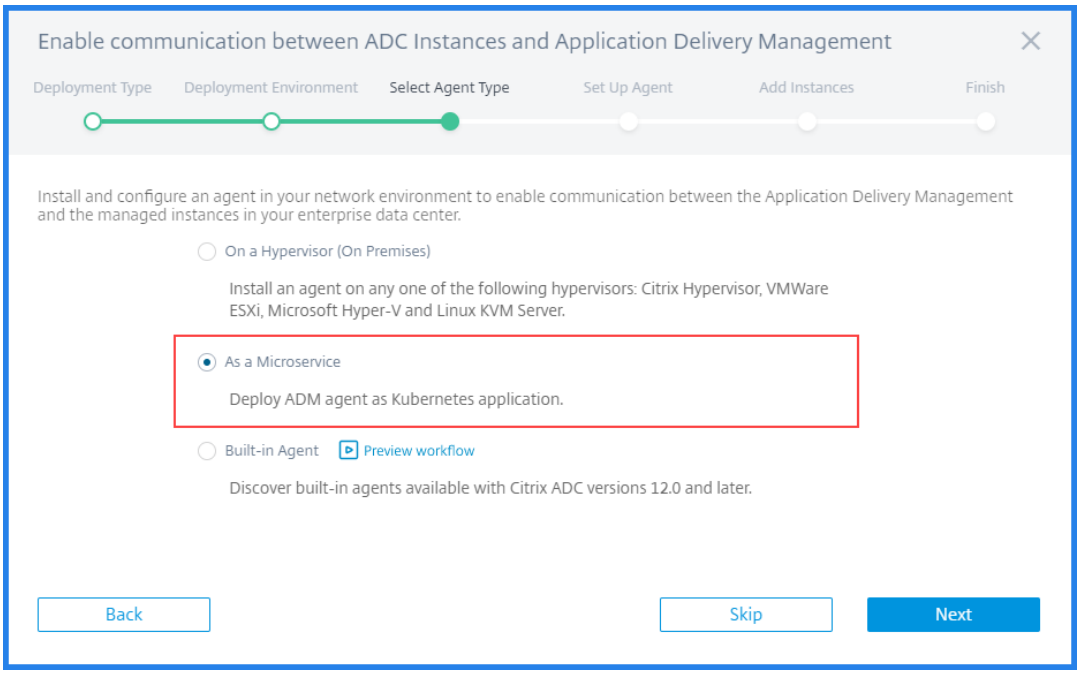


   - **Clouds publics** - Si vous sélectionnez **Amazon Web Services**, **Microsoft Azure** ou **Google Cloud Platform**, vous pouvez installer un agent en externe sur le cloud sélectionné.

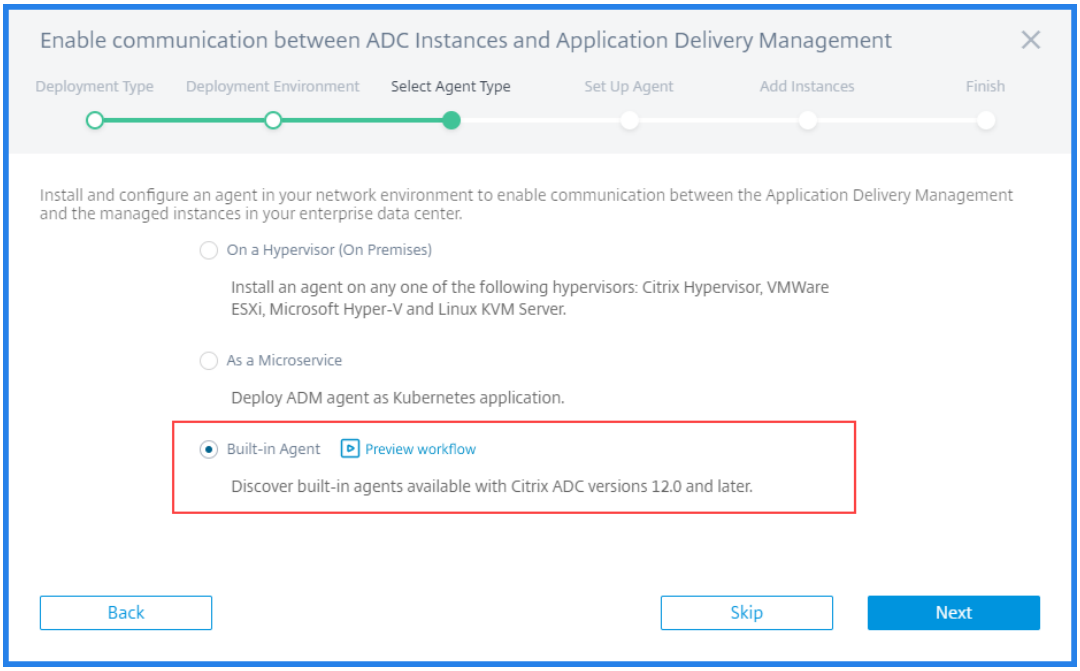
     Voici un exemple d'image pour l'environnement AWS.



- **En tant que microservice** - Pour déployer un agent en tant qu'application Kubernetes.



- **Agent intégré** : pour découvrir les agents intégrés disponibles avec Citrix ADC version 12.0 ou ultérieure.



3. Cliquez sur **Suivant**.

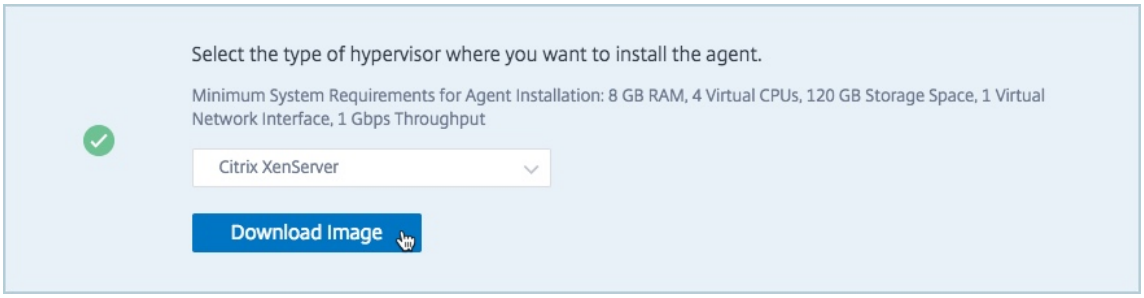
   Les étapes d'installation d'un agent varient selon chaque option. Les liens suivants vous guident vers les étapes spécifiques d'installation d'un agent :

   - Hyperviseur
   - Agent externe
   - En tant que microservice
   - Agent intégré

Installer un agent sur un Hypervisor

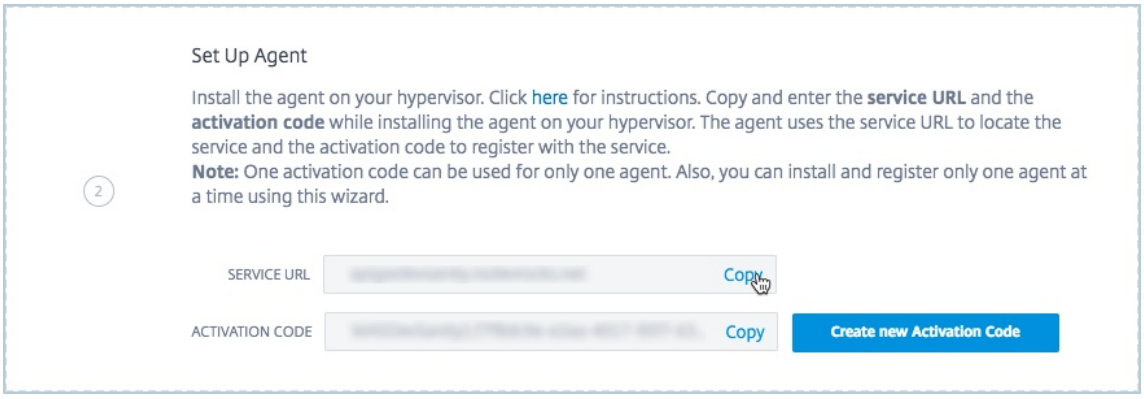
Procédez comme suit pour configurer un agent ADM sur un hyperviseur :

1. Sélectionnez l'hyperviseur et cliquez sur **Télécharger l'image** pour télécharger l'image de l'agent sur votre système local.



   Une URL de service et un code d'activation sont générés et affichés sur l'interface graphique.

2. Copiez l'URL du service et un code d'activation.



3. Spécifiez l'URL du service copié et le code d'activation lors de l'installation de l'agent sur votre hyperviseur.

   L'agent utilise l'URL du service pour localiser le service et le code d'activation pour s'inscrire auprès du service. Pour obtenir des instructions détaillées sur l'installation d'un agent sur votre Hypervisor local, reportez-vous à la sectionInstaller l'agent Citrix ADM sur site.

4. Après l'installation réussie de l'agent, revenez à la page **Configurer l'agent** et cliquez sur **Enregistrer l'agent**.

Prochaine étape : Ajouter des instances.

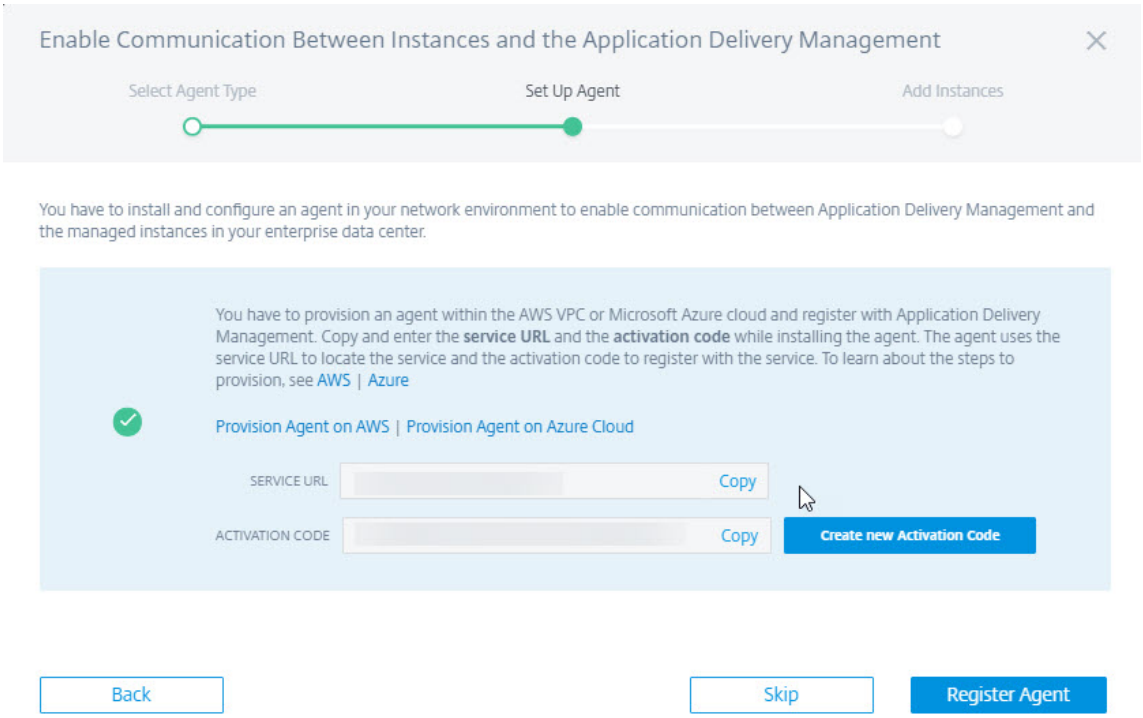
> **Remarque**
>
> Si vous ne souhaitez pas ajouter d'agents lors de la configuration initiale, cliquez sur **Ignorer** pour vérifier les fonctionnalités fournies par Citrix ADM. Vous pouvez ajouter les agents et instances ultérieurement. Pour ajouter des agents ultérieurement, accédez à **Paramètres > Configurer les agents**. Pour obtenir des instructions sur l'ajout d'instances ultérieurement, reportez-vous à la sectionAjout d'instances.

Installer un agent sur un nuage public

Vous n'avez pas besoin de télécharger l'image de l'agent à partir de la page **Configurer l'agent** . L'image de l'agent est disponible sur le site de vente en nuage respectif.

1. Copiez et enregistrez l'URL du service et le code d'activation à utiliser lors de l'installation de l'agent.

   Si vous souhaitez un nouveau code d'activation, cliquez sur **Créer un nouveau code d'activation**, puis copiez et enregistrez le code à utiliser lors de l'installation de l'agent.



- Pour obtenir des instructions détaillées sur l'installation d'un agent sur le cloud Microsoft Azure, reportez-vous à la sectionInstallation de Citrix ADM Agent sur Microsoft Azure Cloud.
- Pour obtenir des instructions détaillées sur l'installation d'un agent sur AWS, reportez-vous à la sectionInstallation de Citrix ADM Agent sur AWS.
- Pour obtenir des instructions détaillées sur l'installation d'un agent sur Google Cloud, reportez-vous à la section Installer l'agent Citrix ADM sur GCP.

2. Après l'installation réussie de l'agent, revenez à la page **Configurer l'agent** et cliquez sur **Enregistrer l'agent**.

Prochaine étape : Ajouter des instances.

Installer un agent en tant que microservice

Vous pouvez déployer un agent Citrix ADM en tant que microservice dans le cluster Kubernetes pour afficher le **graphique de service** dans Citrix ADM.

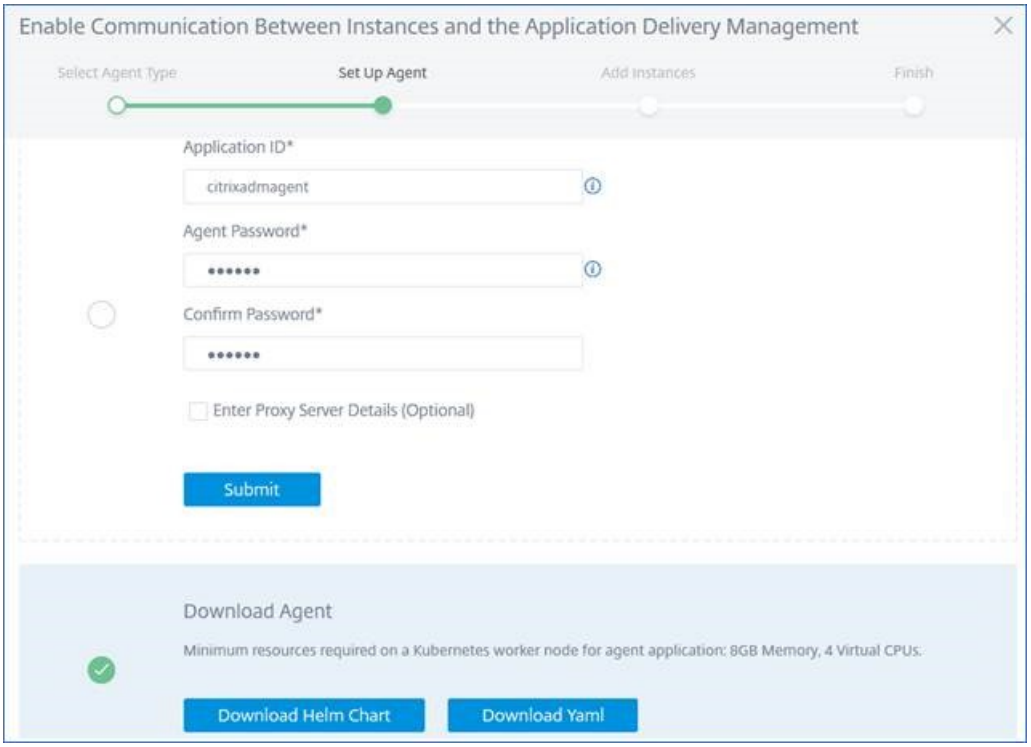
Pour plus d'informations sur la façon de commencer avec le graphique de service, reportez-vous à la section Configuration d'un graphique de service.

1. Spécifiez les paramètres suivants :

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

b) **Mot de passe de l'agent** : spécifiez un mot de passe permettant à CPX d'utiliser ce mot de passe pour embarquer le service CPX to ADM via l'agent.

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



d) Cliquez sur **Soumettre**.

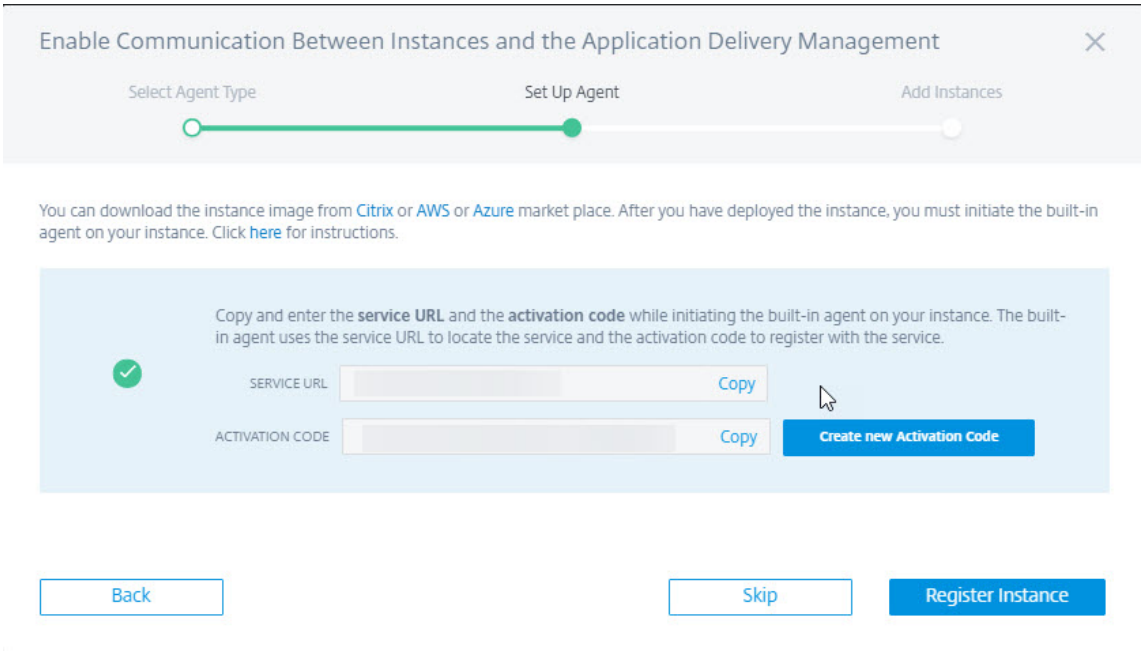
2. Après avoir cliqué sur **Soumettre**, vous pouvez télécharger le tableau YAML ou Helm Chart.
3. Cliquez sur **Fermer**.

   Pour de plus amples informations, consultez la section Installer l'agent Citrix ADM dans le cluster Kubernetes.

Utiliser l'agent intégré dans l'instance de Citrix ADC

Les instances de Citrix ADC dans votre environnement incluent un agent intégré. Vous pouvez lancer l'agent intégré et l'utiliser pour établir la communication entre l'instance et Citrix ADM.

1. Copiez l' **URL du service** généré et le **code d'activation**. Enregistrez-les pour les utiliser lors du lancement de l'agent intégré sur votre instance de Citrix ADC.



Pour obtenir des instructions détaillées sur le lancement de l'agent intégré sur votre instance de Citrix ADC, reportez-vous à la sectionLancer l'agent intégré sur l'instance de Citrix ADC.

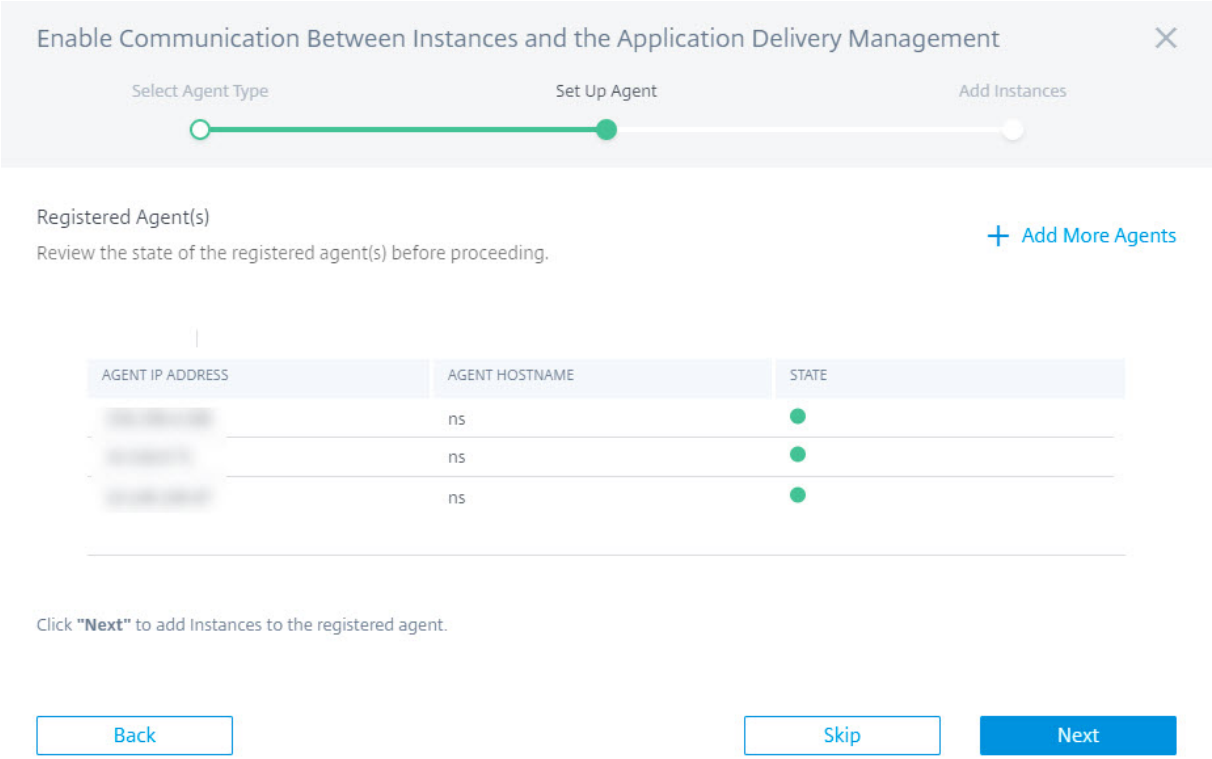
2. Une fois l'agent intégré lancé, revenez à la page **Configurer l'agent** et cliquez sur **Enregistrer l'instance**.

Prochaine étape : Ajouter des instances.

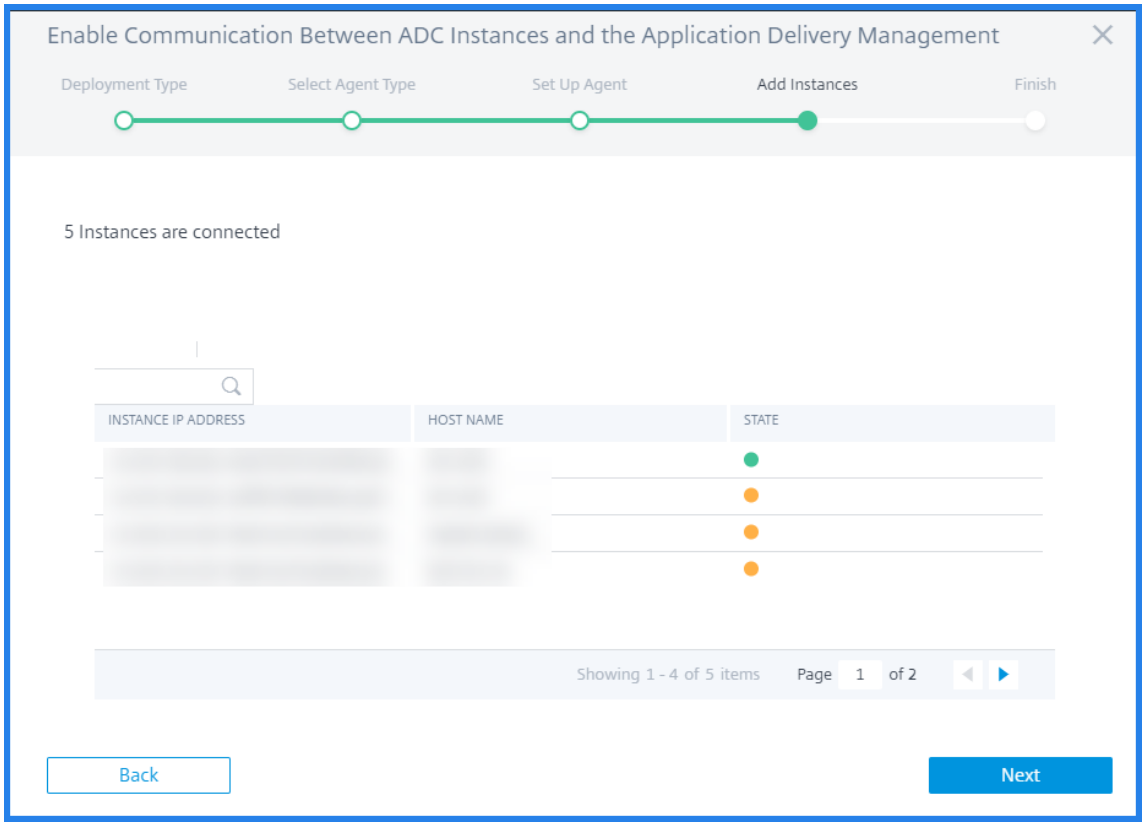
Ajouter des instances à Citrix ADM

Les instances sont des appliances réseau ou des appliances virtuelles que vous souhaitez découvrir, gérer et surveiller à partir de Citrix ADM. Pour gérer et surveiller ces instances, vous devez ajouter les instances au service.

Après avoir réussi l'installation et l'enregistrement de l'agent, les agents sont affichés sur la page **Configurer l'agent**. Lorsque l'état de l'agent est à l'état UP, désigné par un point vert à côté de celui-ci, cliquez sur **Suivant** pour commencer à ajouter des instances au service.



1. Dans la page **Ajouter des instances**, affichez les instances ADC qui sont connectées à l'agent enregistré. Assurez-vous que l'instance est dans l'état **Up** et cliquez sur **Suivant**.

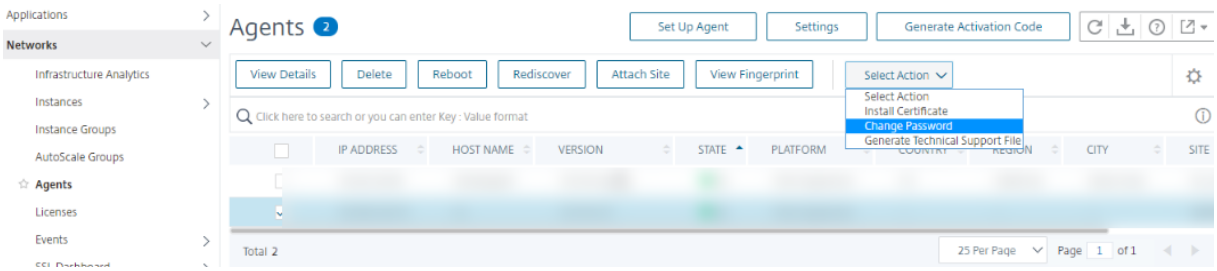


2. Cliquez sur **Terminé** pour terminer votre configuration initiale et commencer à gérer votre déploiement.

> **Remarque**
>
> Si vous ne souhaitez pas ajouter d'instances lors de la configuration initiale, vous pouvez cliquer sur **Terminé** pour terminer l'installation et ajouter les instances ultérieurement. Pour obtenir des instructions sur l'ajout d'instances ultérieurement à Citrix ADM, reportez-vous à la sectionAjout d'instances.

Actions d'agent

Après avoir configuré votre service ADM, vous pouvez appliquer diverses actions à un agent. Accédez à **Réseaux > Agents**.



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

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

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

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

Configurer l'agent intégré ADC pour gérer les instances

April 29, 2021

Un agent intégré est disponible sur les instances Citrix ADC MPX, VPX, Gateway exécutant la version `12.1.48.13` et les versions ultérieures et sur les instances Citrix ADC SDX exécutant la version 13.0 61.x et les versions ultérieures et 12.1 58.x et ultérieures. Vous pouvez lancer cet agent sur l'instance ADC au lieu d'installer un agent dédié dans votre centre de données ou cloud public. L'agent intégré permet la communication entre l'instance et le service Citrix ADM.

> **Remarque**
>
> L'agent intégré est disponible uniquement sur les types d'instance Citrix ADC suivants :
>
> - Citrix ADC MPX
> - Citrix ADC VPX
> - Citrix ADC SDX
> - Citrix Gateway

L'agent intégré est idéal pour les déploiements ADC autonomes ou de paires HA plus petits. Si vous disposez de plusieurs instances ADC, utilisez un agent dédié pour les déploiements. Cet agent garantit que vous disposez de meilleures capacités d'agrégation de données que l'agent intégré. Pour de plus amples informations, consultez la section Installer un agent sur site.

Le service Citrix ADM prend en charge la gestion et la surveillance des instances Citrix ADC à l'aide d'agents intégrés. Toutefois, les fonctionnalités suivantes ne sont pas prises en charge dans l'agent intégré :

- Tableau de bord de l'application
- Web Insight
- Perspectives SSL
- Aperçu HDX
- Perspectives de
- Informations sur la sécurité

- Analyses avancées
- Licences groupées

Vous pouvez passer d'un agent intégré à un agent externe. Pour de plus amples informations, consultez la section Transition d'un agent intégré à un agent externe.

Conditions préalables

Avant de configurer un agent intégré sur l'instance Citrix ADC, vérifiez ce qui suit :

- L'instance Citrix ADC (MPX, VPX ou Gateway) s'exécute sur la version `12.1.48.13` ou une version ultérieure. L'instance SDX exécute la version `13.0.61.x` et les versions ultérieures.
- Un serveur de noms DNS est ajouté sur l'instance Citrix ADC.

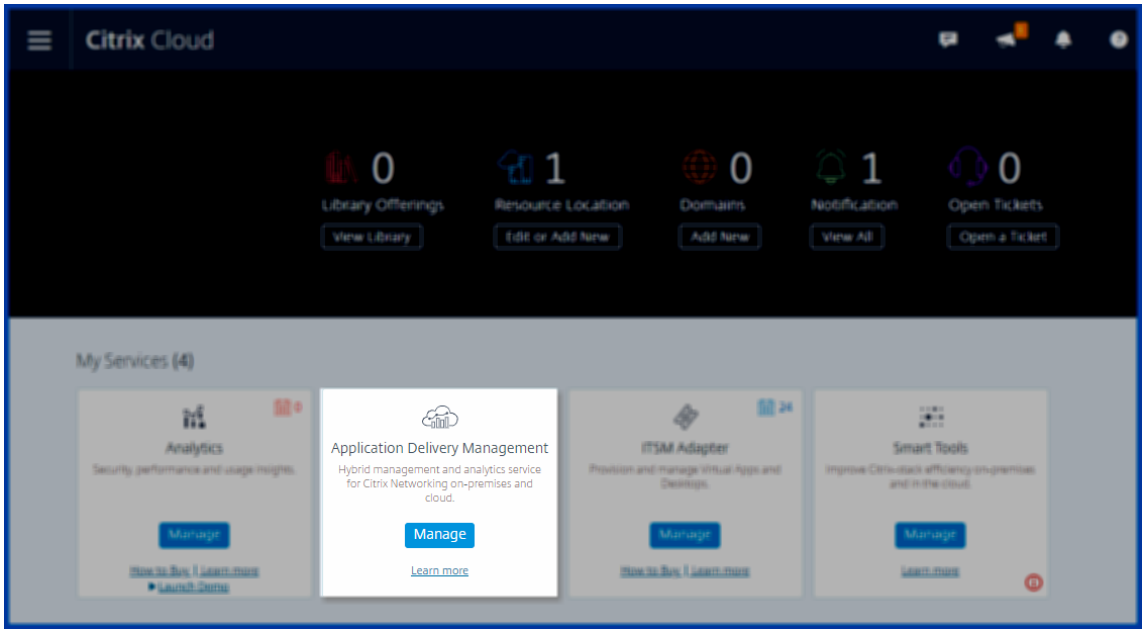
  Pour de plus amples informations, consultez la section Ajouter un serveur de noms.
- Vous disposez d'un compte Citrix Cloud. Pour de plus amples informations, consultez la section Ouvrir un compte sur Citrix Cloud.

> **Remarque**
>
> Pour plus d'informations sur les ports et les autres configurations système requises, reportez-vous à la section Configuration système requise.

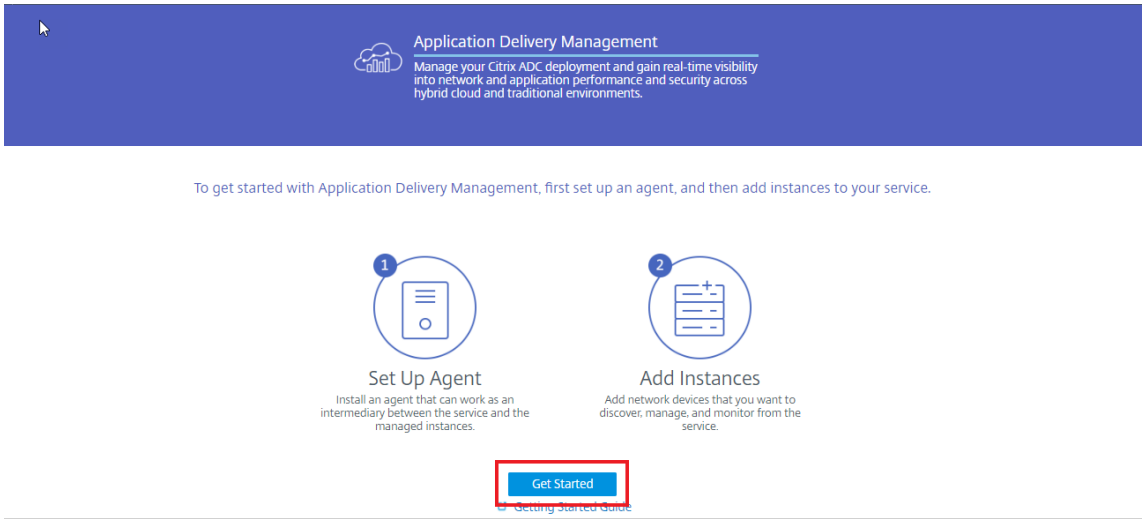
Configurer l'agent intégré

Effectuez les tâches suivantes pour configurer l'agent intégré ADC :

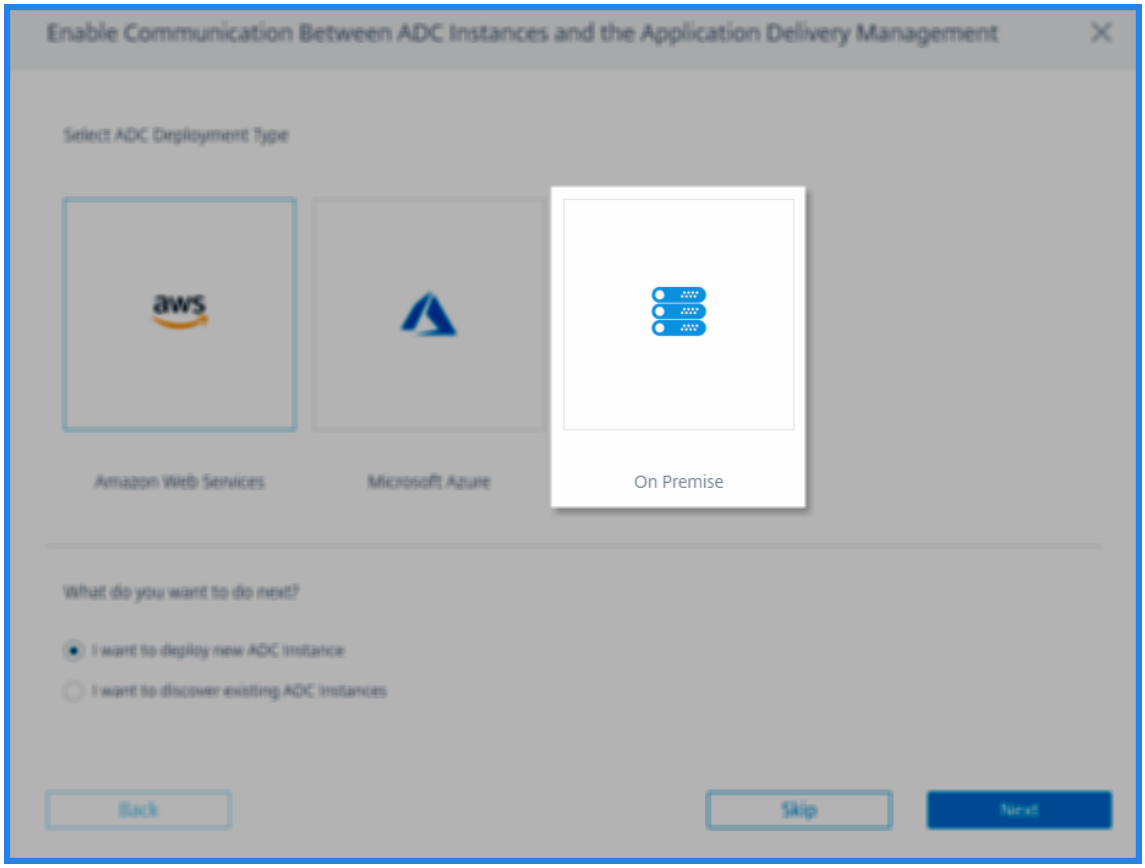
1. Connectez-vous à Citrix Cloud.
2. Dans la vignette **Application Delivery Management**, cliquez sur **Gérer**. Sélectionnez ensuite la région qui correspond à vos besoins commerciaux. Pour de plus amples informations, consultez Gérer Citrix ADM avec un compte Express



3. Cliquez sur **Démarrer**.

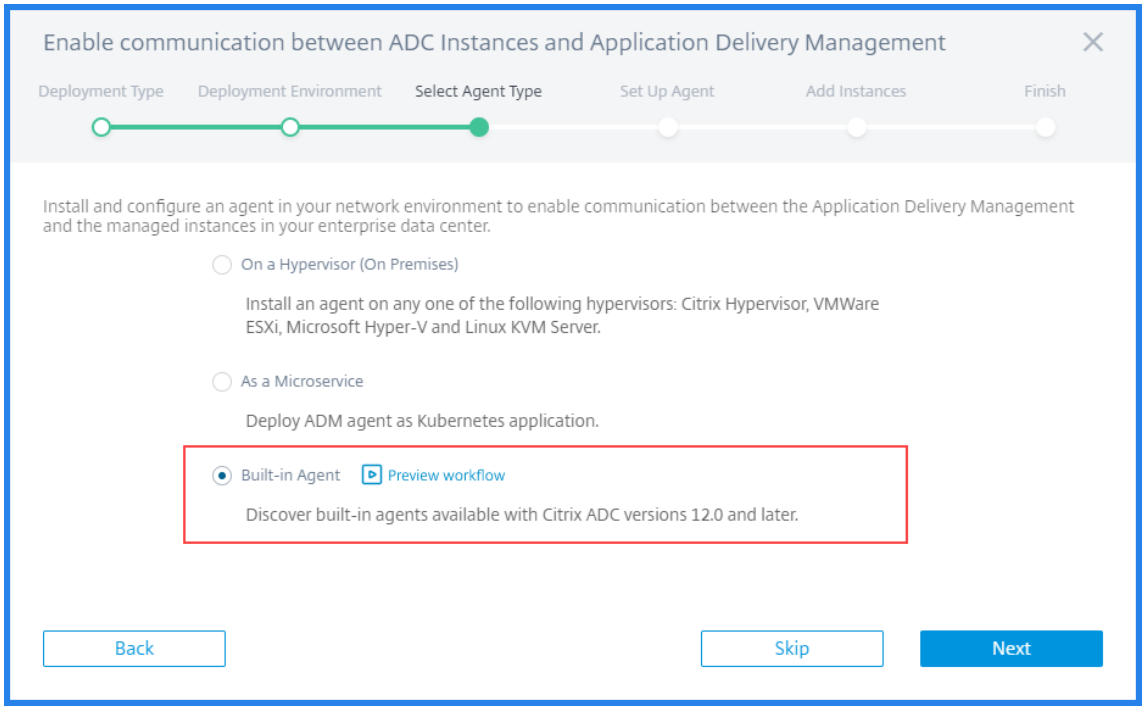


4. Sélectionnez **Sur site** comme type de déploiement ADC.



5. Sélectionnez **Agent intégré**.

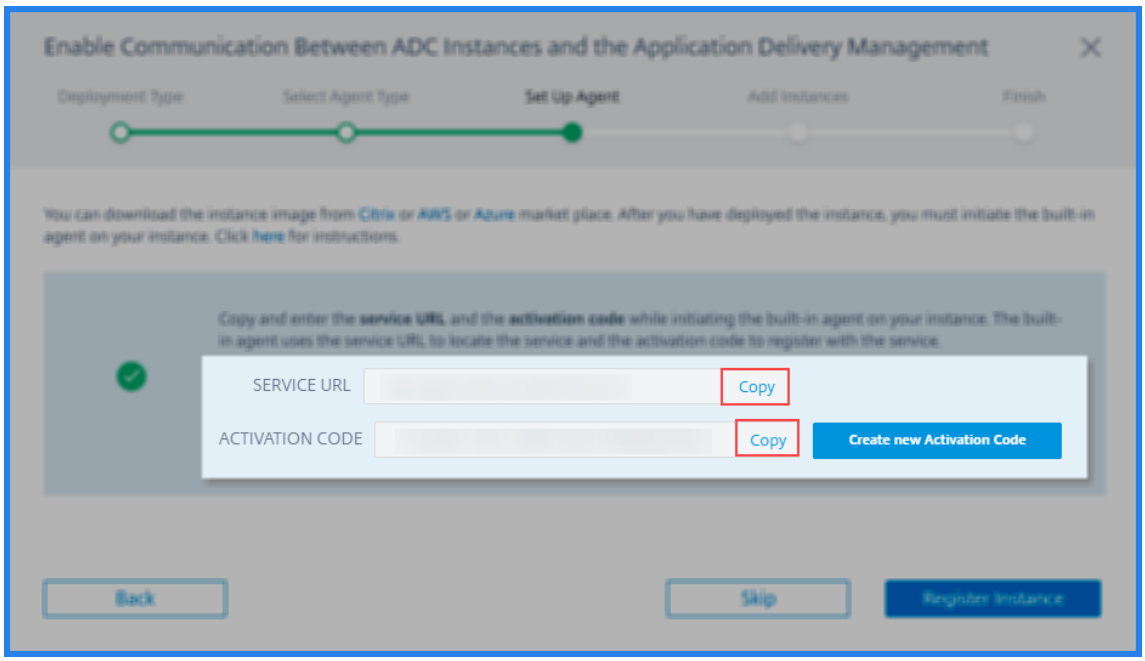
> **Important**
>
> Pour utiliser l'agent intégré, votre instance Citrix ADC doit être en version `12.1` version `48.13` et supérieure.



Une URL de service et un code d'activation sont générés et affichés sur l'interface graphique.

6. Copiez l'**URL du service** et le **code d'activation**.

   L'agent utilise l'URL du service pour localiser le service et le code d'activation pour s'inscrire auprès du service. Ignorez l'étape 7 si vous êtes client MPX ou Gateway.



7. Lancez l'agent intégré à l'aide d'un client SSH. Les utilisateurs de la passerelle doivent ignorer cette étape.

a) Connectez-vous à votre instance Citrix ADC. Pour de plus amples informations, consultez la section Accéder à un Citrix ADC.

b) Accédez au `/var/mastools/scripts` répertoire et tapez la commande suivante :

Sur l'instance SDX

```
./mastool_int.sh <user-name> <service-url> <activation-code> -sdx
<!--NeedCopy-->
```

ou

```
./mastool_init.sh <device-profile-name> <service-url> <activation-code> -sdx -profile

<!--NeedCopy-->
```

> Remarque
>
> ADM découvre toutes les instances VPX exécutées sur ce SDX et vous n'avez pas à enregistrer les instances VPX individuellement.

Sur les instances VPX ne s'exécutant pas sur une appliance SDX et sur les instances MPX et Gateway

Si la version d'image ADM est inférieure à 13.0 61.x ou 12.1 57.x, vous devez vérifier la `mastools` version en tapant la commande `cat /var/mastools/version.conf`. Si la sortie est `0.0-0.0`, c'est la première fois.

Tapez l'une des commandes suivantes indiquées ci-dessous, en fonction de la version du logiciel.

Version de l'image ADC	Est-ce que mastools_version `0.0-0.0` ?	Commande pour l'enregistrement avec le profil	Commande pour l'enregistrement sans profil
Inférieur à 13,0 61.xx et 12,1 57,xx	Oui	`./mastools_init.sh <device_profile_nam> <service_url> "MAS;<activation_code>"-profile`	`./mastools_init.sh <user_name> <pwd> <service_url> "MAS;<activation_code>"`

Version de l'image ADC	Est-ce que mastools_version `0.0-0.0` ?	Commande pour l'enregistrement avec le profil	Commande pour l'enregistrement sans profil
Inférieur à 13,0 61.xx et 12,1 57,xx	Non	`./mastools_init.sh <device_profile_name> <service_url> <activation_code> -profile`	`./mastools_init.sh <user_name> <pwd> <service_url> <activation_code>`
Supérieur à 13,0 61.x et 12,1 57.xx	Sans objet	`./mastools_init.sh <device_profile_nam> <service_url> <activation_code> -profile`	`./mastools_init.sh <user_name> <pwd> <service_url> <activation_code>`

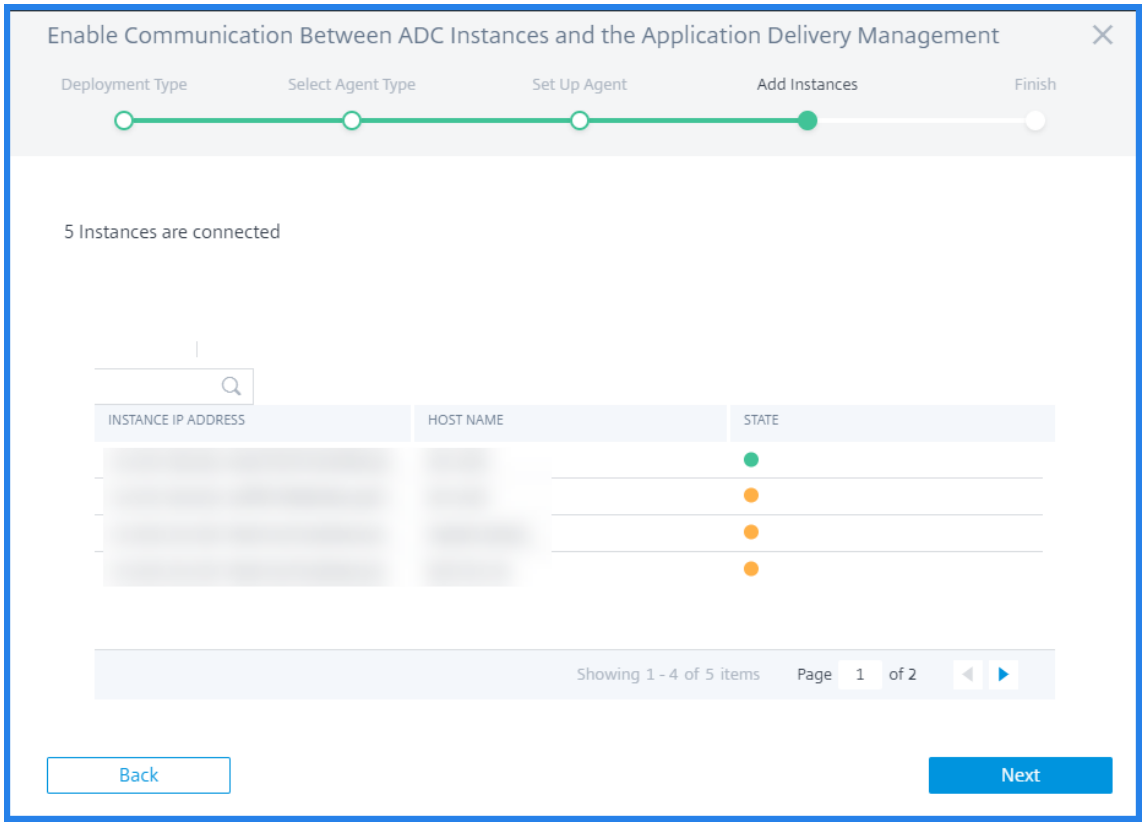
- Dans `<username>`, entrez le nom d'utilisateur Citrix ADC.
- Dans `<password>`, entrez le mot de passe ADC.
- Dans `<service_url>`, collez l'URL que vous avez copiée à l'étape précédente.
- Dans `<activation_code>`, collez le code d'activation que vous avez copié à l'étape précédente.

Pour les instances MPX, VPX et Gateway, une fois l'initialisation effectuée à l'aide de la `mastools` commande, la communication entre l'agent et le service ADM est établie. L'agent met automatiquement à niveau chaque fois qu'une version logicielle la plus récente est disponible. Cependant, à partir des versions ADC 12.1 57.18 et supérieures et ADC 13.0 61.48 et supérieures, l'agent intégré communique avec le service ADM sans initialisation et se met à niveau automatiquement vers la dernière version du logiciel régulièrement.
Pour les instances SDX, l'agent est livré avec la fonctionnalité de mise à niveau automatique dans toutes les versions prises en charge, soit 13.0 61.x et versions ultérieures et 12.1 58.x et versions ultérieures.

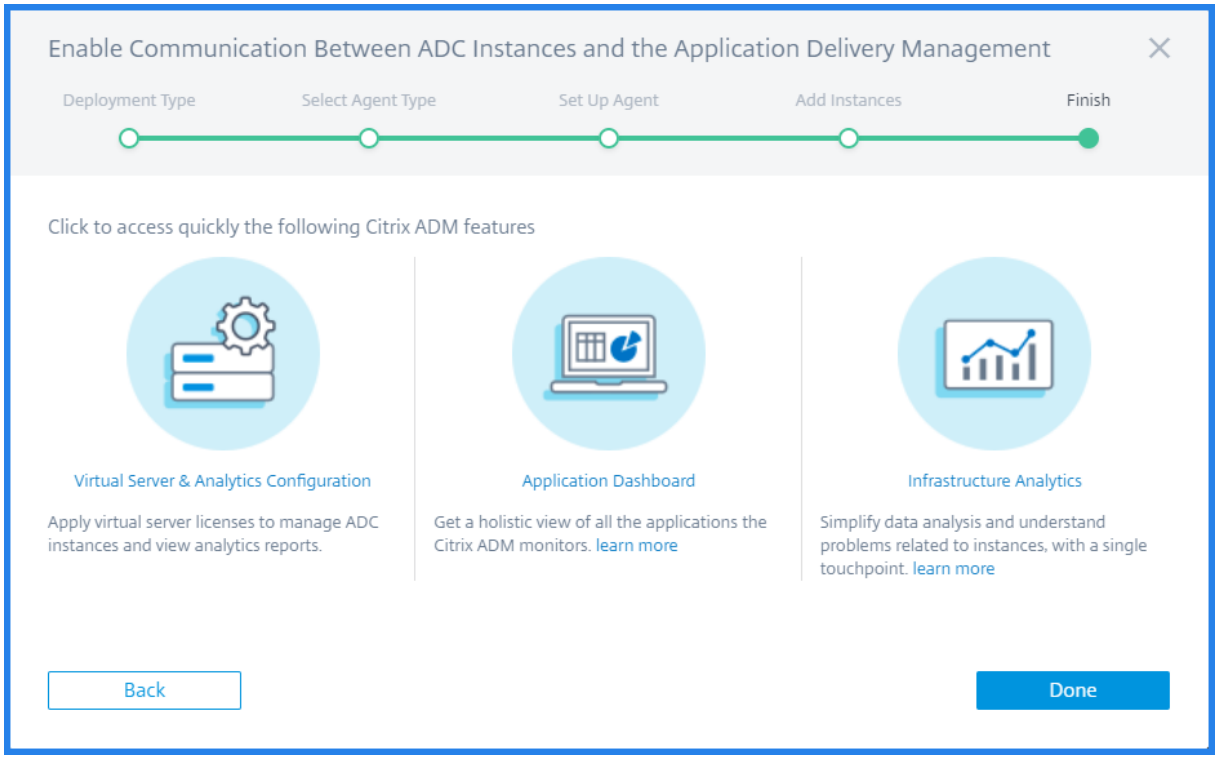
> Remarque
>
> Dans une paire HA, effectuez l'enregistrement sur le nœud principal. Si vous exécutez l'enregistrement sur le nœud secondaire, le message suivant s'affiche :
>
> **Exécutez la commande d'enregistrement sur le nœud principal.**

8. Revenez à la page du service ADM et cliquez sur **Enregistrer l'instance**.

9. Dans **Ajouter des instances**, affichez l'instance dans laquelle vous avez lancé l'agent intégré. Assurez-vous que l'instance est dans l'état **Up** et cliquez sur **Suivant**.



10. Cliquez sur **Terminé**.



Après avoir réussi la configuration intégrée de l'agent, vous pouvez accéder aux fonctionnalités ADM telles que :

- **Serveur virtuel et analytique** : appliquez des licences à votre serveur virtuel pour gérer les instances ADC. Pour de plus amples informations, consultez la section Gérer les abonnements.
- **Tableau de bord des applications** : permet d'afficher toutes les applications d'une manière holistique. Pour de plus amples informations, consultez la section Gestion des applications et tableau de bord.
- **Analyse de l'infrastructure** : cette fonctionnalité vous aide à visualiser les facteurs qui ont entraîné ou pourraient entraîner un problème sur les instances. Pour de plus amples informations, consultez la section Analyse d'infrastructure.

> Remarque
>
> Vous pouvez également configurer l'agent intégré en accédant à la page **Réseaux > Agents > Générer un code d'activation**. Copiez et collez l'URL et le code d'activation dans une instance ADC et découvrez cette instance.

Une fois l'agent intégré lancé, accédez à **Réseaux > Instances > Citrix ADC**. Cette page affiche les détails sur l'instance gérée découverte à l'aide de l'agent intégré.

Résolution des problèmes

Vous pouvez vérifier les journaux si l'enregistrement échoue ou si l'enregistrement réussit mais que l'agent intégré n'apparaît pas dans l'interface graphique ADM.

- Si l'enregistrement échoue, vérifiez les journaux dans `/var/mastools/logs/mastools_reg.py.log`
- Si l'enregistrement réussit, mais que l'agent intégré n'apparaît pas dans l'interface graphique ADM, vérifiez :
  - **MASTools_Upgrade** journaux dans `/var/mastools/logs/mastools_upgrade.log`
  - **Journaux binaires**`/var/log/mastoolsd.log`.

Installer l'agent Citrix ADM sur site

April 29, 2021

L'agent fonctionne comme intermédiaire entre Citrix Application Delivery Management (Citrix ADM) et les instances découvertes dans le centre de données.

Avant de commencer à installer l'agent, assurez-vous que vous disposez des ressources informatiques virtuelles requises que l'Hypervisor doit fournir pour chaque agent. Voici les exigences de l'agent.

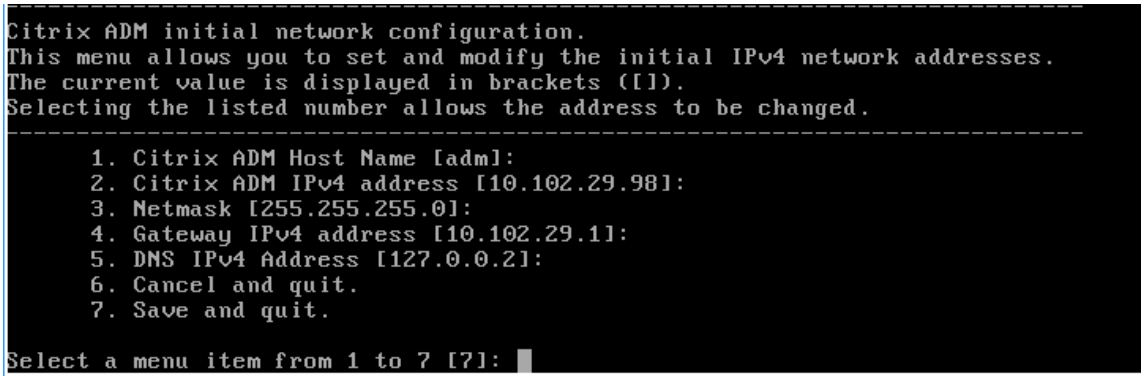
Composant	Exigences
RAM	32 Go
CPU virtuel	8
Espace de stockage	30 FR
Interfaces réseau virtuelles	1
Débit	1 Gbit/s

> **Remarque**
>
> Pour toutes les informations relatives aux ports et autres exigences, reportez-vous à la sectionConfiguration système requise.

Pour installer l'agent Citrix ADM :

1. Téléchargez l'image de l'agent comme indiqué à laMise en route.
2. Importez le fichier image de l'agent dans votre Hypervisor.
3. Dans l'onglet **Console**, configurez les options de configuration réseau initiales comme indiqué

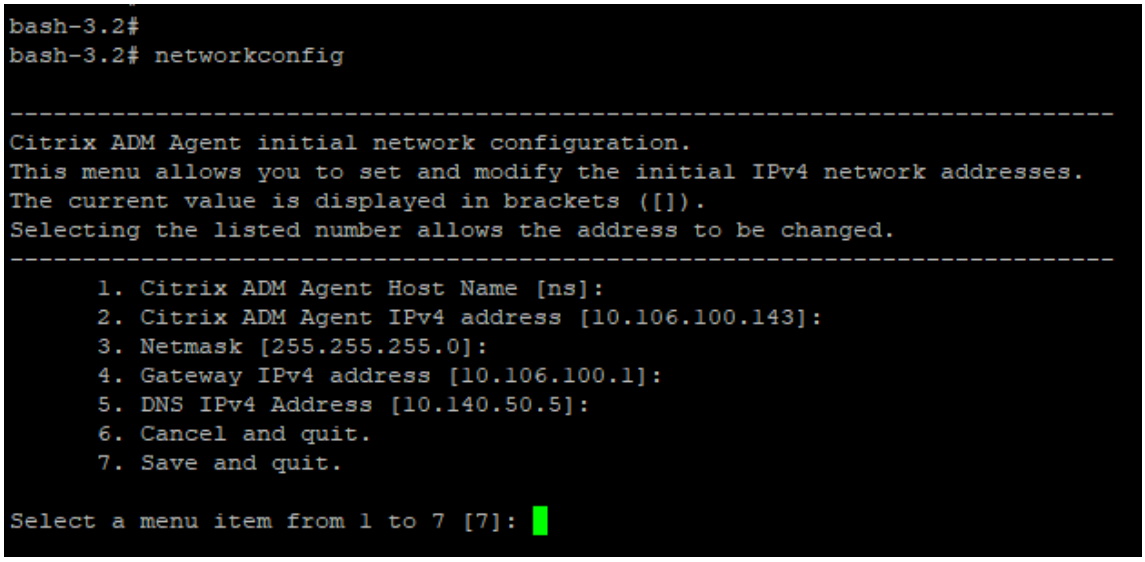
dans l'exemple suivant :



> **Remarque**
>
> Assurez-vous de configurer votre DNS pour autoriser l'accès Internet à votre agent Citrix ADM.

4. Après avoir terminé la configuration réseau initiale, enregistrez les paramètres de configuration. Lorsque vous y êtes invité, ouvrez une session à l'aide des informations d'identification par défaut (`nsrecover`/`nsroot`).

   Si vous souhaitez modifier les paramètres réseau configurés sur l'agent, tapez la commande `networkconfig` et suivez les invites de l'interface de ligne de commande.



5. S'il n'y a pas d'invite pour entrer l'URL du service, accédez à /mps dans l'agent Citrix ADM, puis exécutez l'un des scripts suivants :

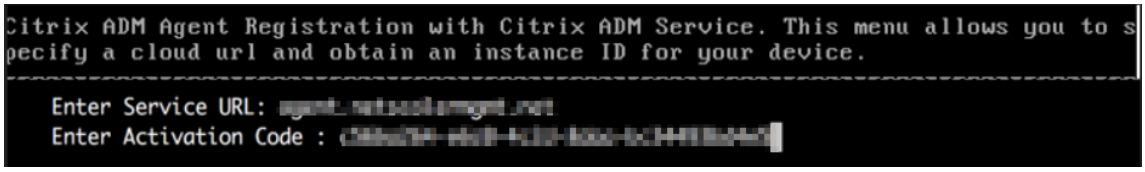
```
deployment_type.py
<!--NeedCopy-->
```

```
register_agent_cloud.py
```



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

6. Entrez l' **URL du service** et le **code d'activation** que vous avez enregistrés lorsque vous avez téléchargé l'image de l'agent. L'agent utilise l'URL du service pour localiser le service et le code d'activation pour s'inscrire auprès du service.



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

Une fois l'agent redémarré, accédez à l'interface graphique Citrix ADM et accédez à **Réseaux** > **Agents** pour vérifier l'état de l'agent.

Installer l'agent Citrix ADM sur le cloud Microsoft Azure

April 29, 2021

L'agent agit en tant qu'intermédiaire entre Citrix Application Delivery Management (Citrix ADM) et les instances gérées dans le datacenter d'entreprise ou dans le cloud.

Pour installer l'agent Citrix ADM sur le cloud Microsoft Azure, vous devez créer une instance de l'agent dans le réseau virtuel. Obtenez l'image de l'agent Citrix ADM à partir de la Place de Azure Marketplace, puis utilisez le portail Azure Resource Manager pour créer l'agent.

Avant de commencer à créer l'instance de l'agent Citrix ADM, assurez-vous que vous avez créé un réseau virtuel avec les sous-réseaux requis où l'instance réside. Vous pouvez créer des réseaux virtuels pendant le provisioning de machines virtuelles, mais sans la possibilité de créer différents sous-réseaux. Pour plus d'informations sur la création de réseaux virtuels, reportez-vous à la sectionhttp://azure.microsoft.com/en-us/documentation/articles/create-virtual-network.

Configurez la connectivité du serveur DNS et du VPN qui permet à une machine virtuelle d'accéder aux ressources Internet.

Conditions préalables

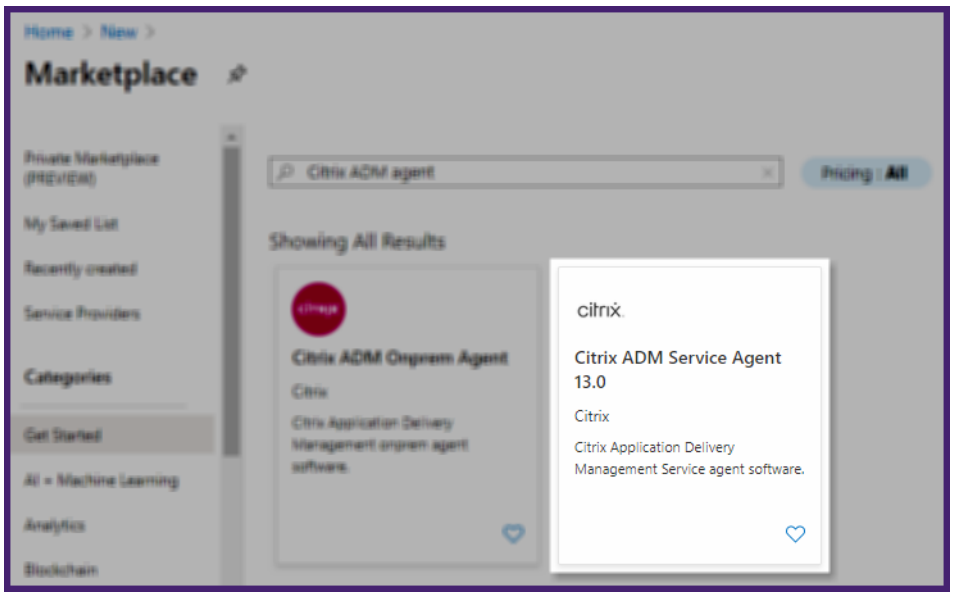
Assurez-vous d'avoir les éléments suivants :

- Un compte d'utilisateur Microsoft Azure
- Accès au Gestionnaire de ressources Microsoft Azure

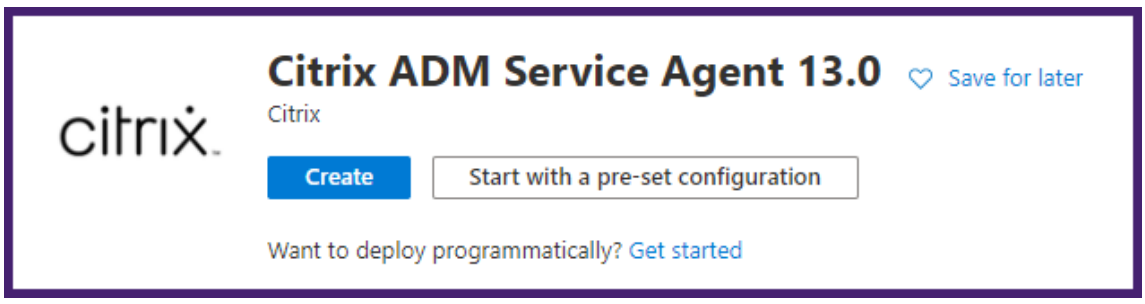
> **Remarque**
>
> - Citrix vous recommande de créer un groupe de ressources, un groupe de sécurité réseau, un réseau virtuel et d'autres entités avant de provisionner la machine virtuelle de l'agent Citrix ADM, afin que les informations réseau soient disponibles pendant le Provisioning.
> - Pour que l'agent Citrix ADM communique avec les instances Citrix ADM et Citrix ADC, assurez-vous que les ports recommandés sont ouverts. Pour plus d'informations sur les exigences en matière de port pour l'agent Citrix ADM, reportez-vous à la section Ports.

Pour installer l'agent Citrix ADM sur Microsoft Azure Cloud :

1. Connectez-vous au portail Azure (https://portal.azure.com) à l'aide de vos informations d'identification Microsoft Azure.
2. Cliquez sur **+Créer une ressource**.
3. Tapez `Citrix ADM Agent` dans la barre de recherche et sélectionnez **Agent de service Citrix ADM**.



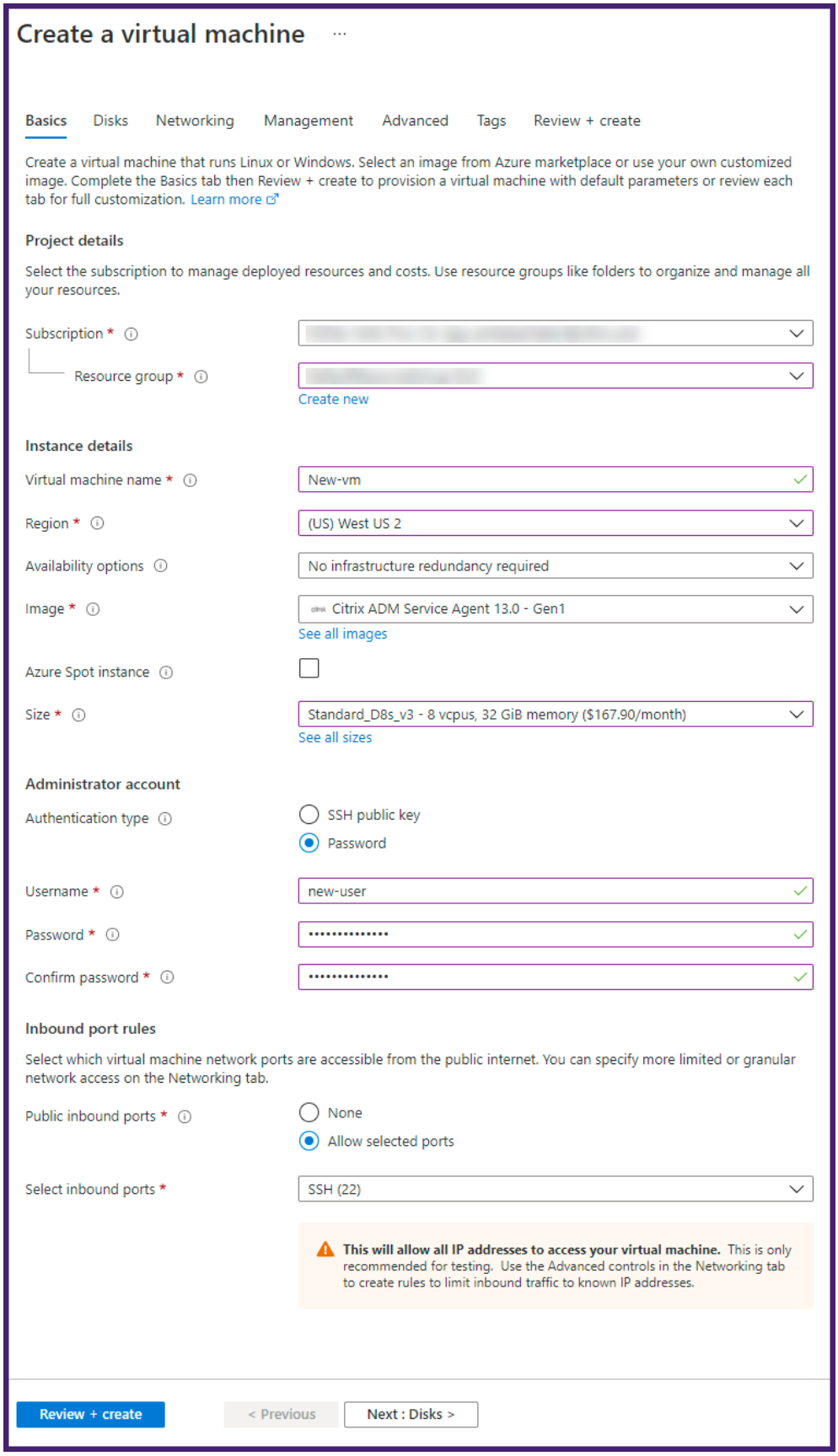
4. Cliquez sur **Créer**.



5. Dans le volet **Créer une machine virtuelle**, spécifiez les valeurs requises dans chaque section pour créer une machine virtuelle.

Notions de base :

Dans cet onglet, spécifiez les **détails du projet, lesdétails de l'instance**et le**compte d'administrateur**.



- **Groupe de ressources** : sélectionnez le groupe de ressources que vous avez créé dans la liste déroulante.

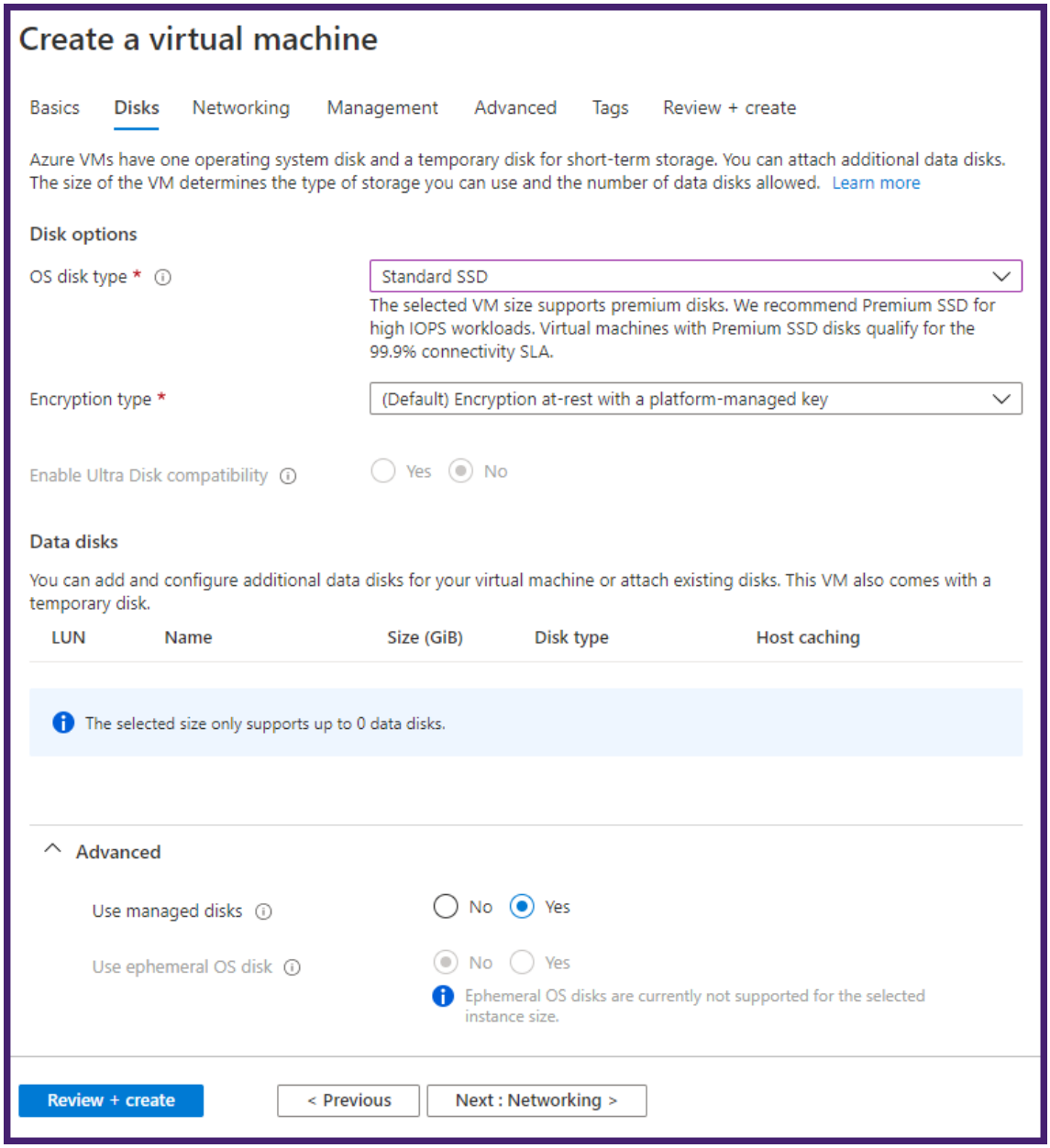
  > **Remarque**
  >
  > Vous pouvez créer un groupe de ressources à ce stade, mais Citrix vous recommande de créer un groupe de ressources à partir de groupes de ressources dans Azure Resource Manager, puis de sélectionner le groupe dans la liste déroulante.

- **Nom de la machine virtuelle** : spécifiez un nom pour l'instance de l'agent Citrix ADM.
- **Région** : sélectionnez la région dans laquelle vous souhaitez déployer un agent.
- **Options de disponibilité** : sélectionnez le jeu de disponibilité dans la liste.
- **Image** - Ce champ affiche l'image de l'agent déjà sélectionnée. Si vous souhaitez passer à une autre image d'agent, sélectionnez l'image souhaitée dans la liste.
- **Taille** : spécifiez le type et la taille du disque virtuel pour le déploiement de votre agent Citrix ADM.

  Sélectionnez le Type de disque virtuel pris en charge (**HDD** ou **SSD**) dans la liste.
- **Type d'authentification** : sélectionnez Mot de passe.
- **Nom d'utilisateur et mot de passe** : spécifiez un nom d'utilisateur et un mot de passe pour accéder aux ressources du groupe de ressources que vous avez créé.

Disques :

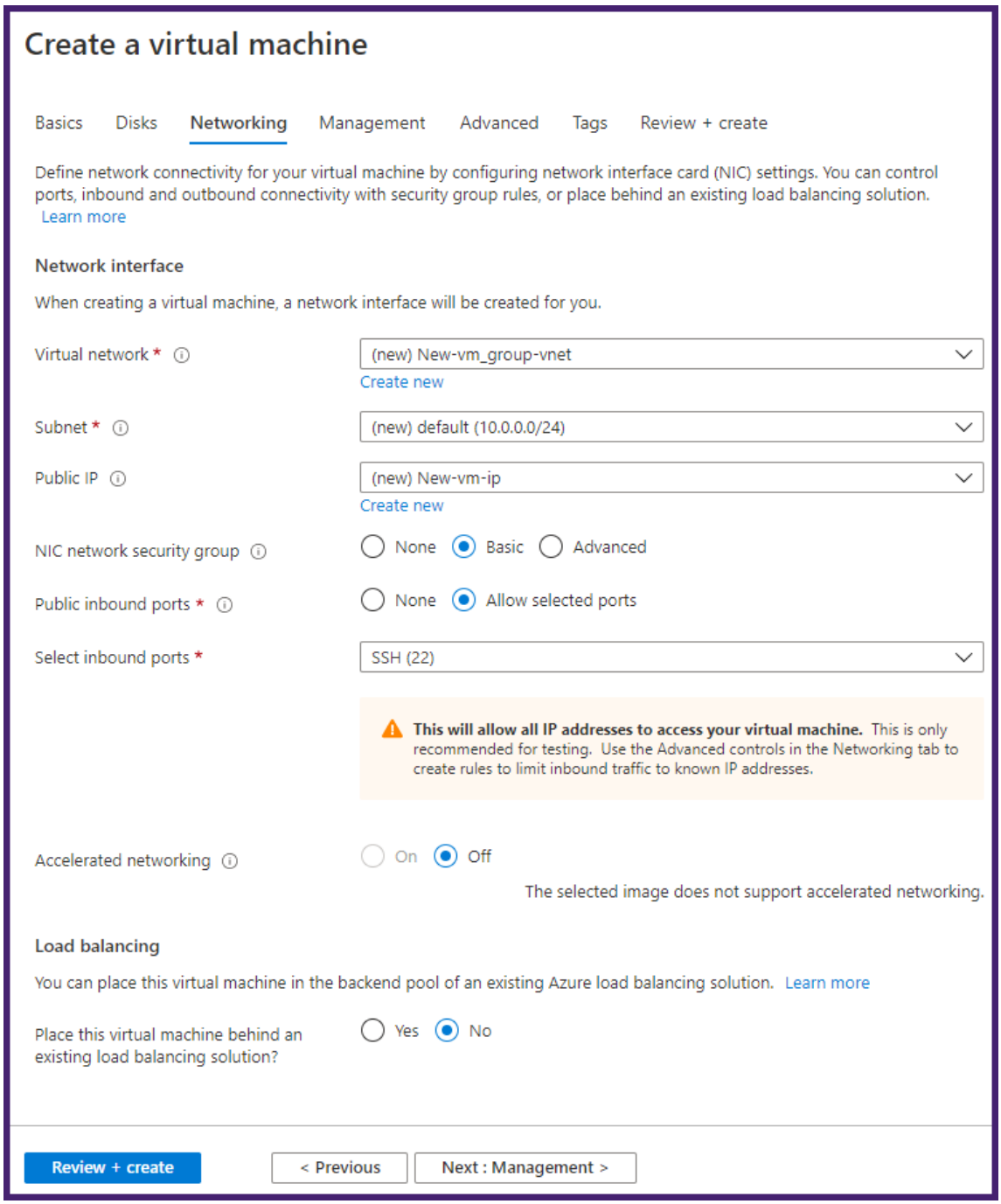
Dans cet onglet, spécifiez **les options Disque** et **Disques de données**.



- **Type de disque du système d'exploitation** - Sélectionnez le type de disque virtuel (disque dur ou SSD).

Mise en réseau :

Spécifiez les détails de mise en réseau requis :

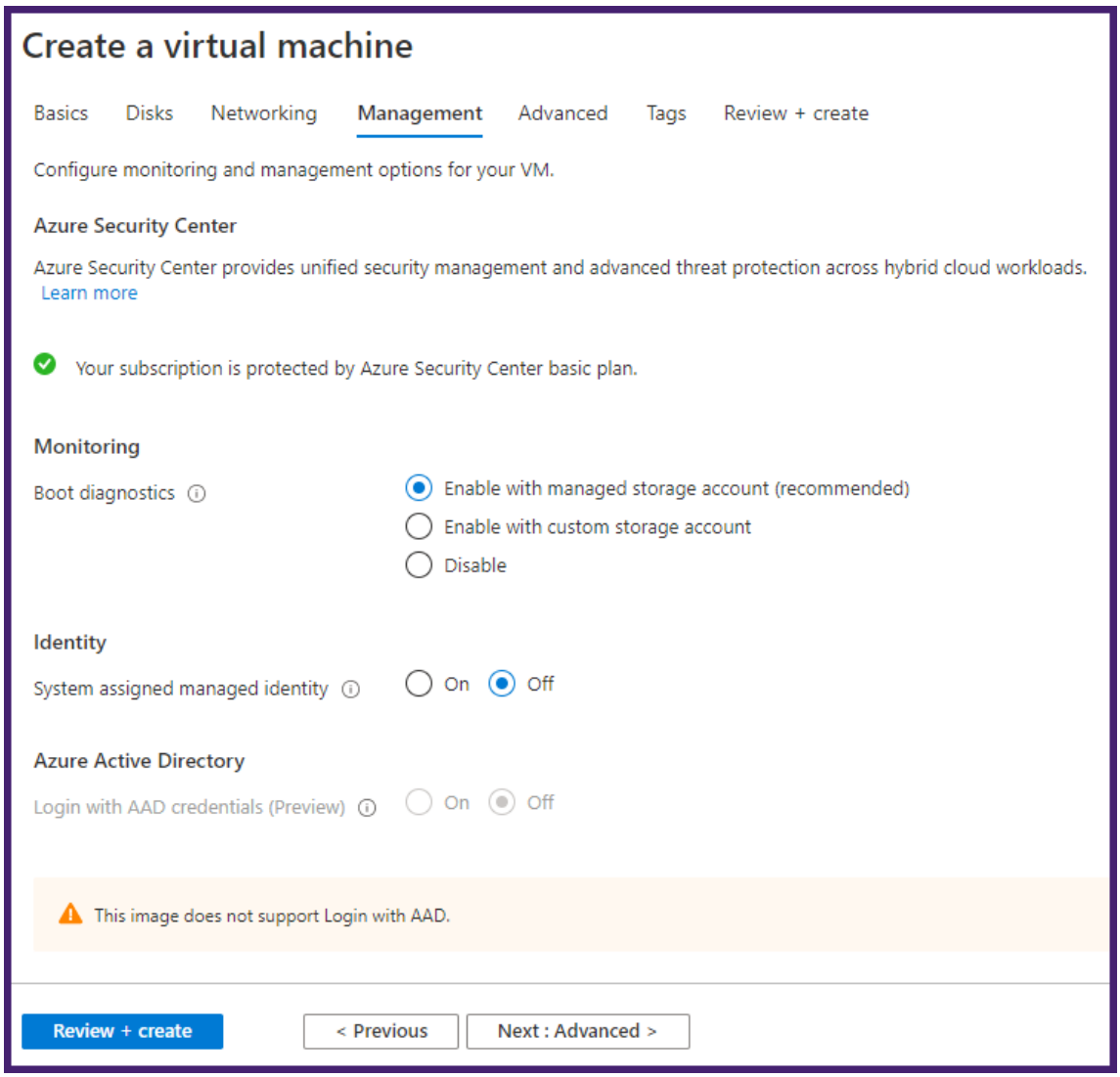


- **Réseau virtuel** : sélectionnez le réseau virtuel.
- **Sous-réseau** — Définit l'adresse du sous-réseau.
- **Adresse IP publique** — Sélectionnez l'adresse IP.
- **Groupe de sécurité réseau** : sélectionnez le groupe de sécurité que vous avez créé.
- **Sélectionnez les ports entrants** - Si vous autorisez les ports entrants publics, vérifiez que les règles entrantes et sortantes sont configurées dans le groupe de sécurité. Sélectionnez ensuite les ports entrants dans la liste. Pour plus de détails, consultez Conditions préal-

ables.

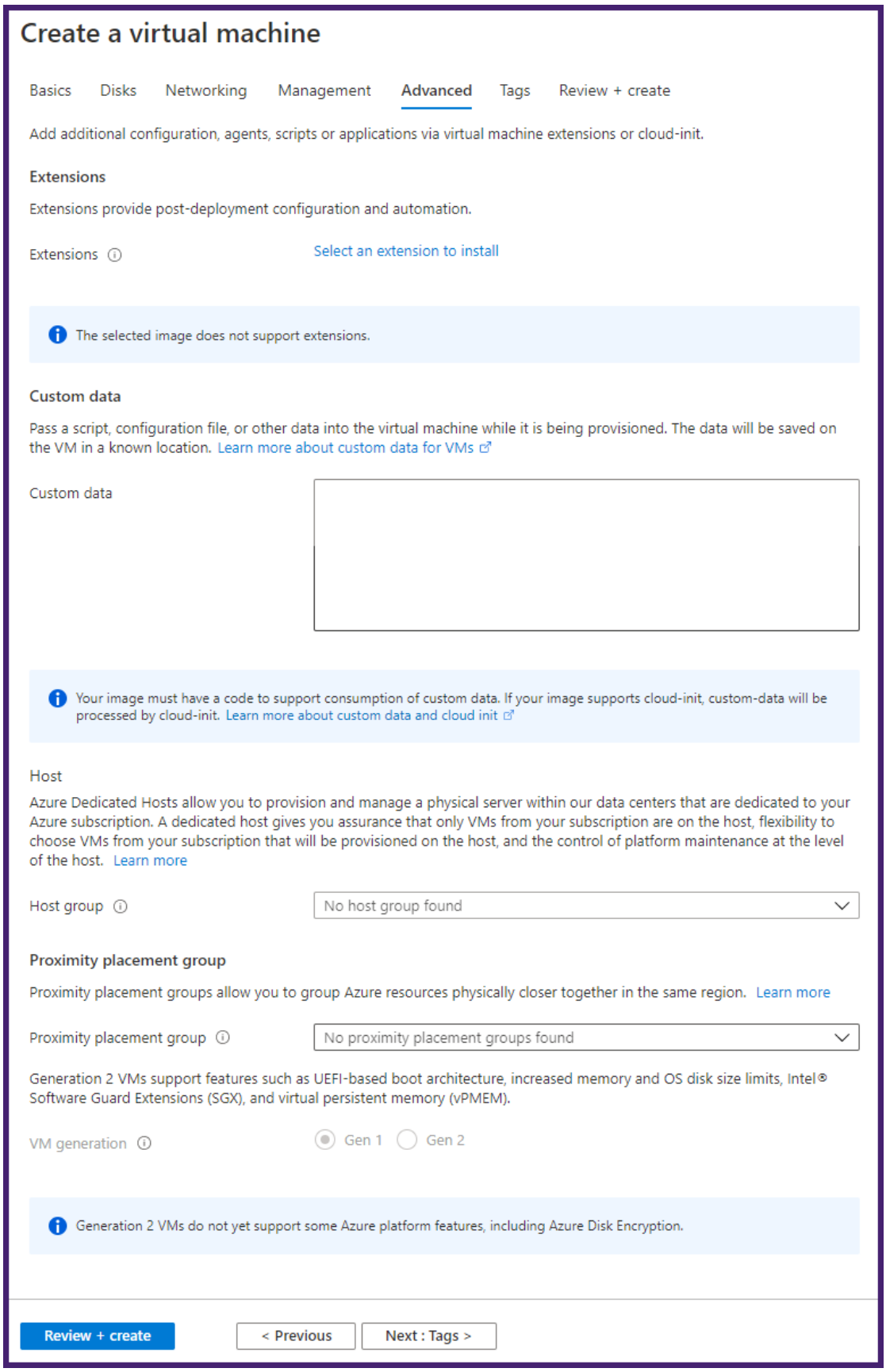
Gestion :

Spécifiez **Azure Security Center**, **Monitoring**et **Identity**.



Avancé :

Facultatif, spécifiez **Extensions**, **Données personnalisées**et **Groupe de placement de proximité**.



Dans **Données personnalisées**, vous pouvez spécifier un script d'enregistrement automatique de l'agent pour enregistrer l'agent auprès du service ADM. Voici un exemple de script qui exécute le script `deployment.py` et enregistre l'agent :

```
``python
#!/var/python/bin/python2.7
import os
import requests
import json
import time
import re
import logging
import logging.handlers
import boto3

'''
Vue d'ensemble du script :
Le script permet d'enregistrer un agent ADM auprés d'ADM. Passez-
   le dans userdata pour faire de l'agent ADM dans AWS pour s'
   enregistrer automatiquement au démarrage. Le flux de travail
   est le suivant
1)  Récupérer les informations d'identification de l'API du
   service ADM (ID et secret) à partir du magasin secret AWS (
   REMARQUE : vous devez attribuer un rôle IAM à l'agent ADM qui
   donnera l'autorisation de récupérer des secrets à partir de la
   boutique secréte AWS)
2)  Connectez-vous au service ADM avec les informations d'
   identification récupérées à l'étape 1
3)  Appelez le service ADM pour récupérer les informations d'
   identification (ServiceURL et jeton) pour l'enregistrement de l
   'agent
4)  Appelle l'enregistrement à l'aide des informations d'
   identification récupérées à l'étape 3
'''

'''
Ce sont les espaces réservés que vous devez remplacer en fonction
   de vos configurations d'installation
aws_secret_id : ID du secret AWS dans lequel vous avez stocké les
   informations d'identification ADM
La valeur des secrets doit être au format json suivant
{
  "adm_user_id_key": "YOUR_ID", " adm_user_secret_key": "
     YOUR_SECRET" }

```



```
'''

aws_secret_id = "<AWS_secret_id>"
adm_ip_or_hostname = "<YOUR_ADM_POP>.adm.cloud.com"

'''
Configurer un enregistreur spécifique avec le niveau de sortie
    souhaité et le nom du fichier journal
'''
log_file_name_local = os.path.basename (__file__)
LOG_FILENAME = '/var/log/' + 'bootstrap' + '.log'
LOG_MAX_BYTE = 50*1024*1024
LOG_BACKUP_COUNT = 20

logger = Logging.getLogger (__name__)
Logger.setLevel (Logging.debug)
logger_handler = logging.handlers.RotatingFileHandler(LOG_FILENAME
    , maxBytes=LOG_MAX_BYTE, backupCount=LOG_BACKUP_COUNT)
logger_fortmater = logging.Formatter(fmt='%(asctime)-2s:%(funcName
    )30s:%(lineno)4d: [%(levelname)s] %(message)s', datefmt="%Y-%m
    -%d %H:%M:%S")
logger_handler.setFormatter(logger_fortmater)
logger.addHandler(logger_handler)

class APIHandlerException(Exception):
    def __init__(self, error_code, message):
        self.error_code = error_code
        self.message = message

    def __str__(self):
        return self.message + ". Error code '" + str(self.
            error_code) + "'"

def parse_response(response, url, print_response=True):
    if not response.ok:
        if "reboot" in url:
            logger.debug('No response for url: reboot')
            resp = {
 "errorcode": "500", "message": "Error while reading response." }

            return resp

        if print_response:
            logger.debug('Response text for %s is %s' % (url,
                response.text))
```



```
67
68          response = json.loads(response.text)
69          logger.debug("ErrorCode - " + str(response['errorcode']) +
                ". Message -" + str(response['message']))
70          raise APIHandlerException(response['errorcode'], str(
                response['message']))
71      elif response.text:
72          if print_response:
73              logger.debug('Response text for %s is %s' % (url,
                    response.text))
74
75          result = json.loads(response.text)
76          if 'errorcode' in result and result['errorcode'] > 0:
77              raise APIHandlerException(result['errorcode'], str(
                    result['message']))
78          return result
79
80  def _request(method, url, data=None, headers=None, retry=3,
        print_response=True):
81      try:
82          response = requests.request(method, url, data=data,
                headers=headers)
83          result = parse_response(response, url, print_response=
                print_response)
84          return result
85      except [requests.exceptions.ConnectionError, requests.
            exceptions.ConnectTimeout]:
86          if retry > 0:
87              return _request(method, url, data, headers, retry-1,
                    print_response=print_response)
88          else:
89              raise APIHandlerException(503, 'ConnectionError')
90      except requests.exceptions.RequestException as e:
91          logger.debug(str(e))
92          raise APIHandlerException(500, str(e))
93      except APIHandlerException as e:
94          logger.debug("URL: %s, Error: %s, Message: %s" % (url, e.
                error_code, e.message))
95          raise e
96      except Exception as e:
97          raise APIHandlerException(500, str(e))
98
99  essayez :
100     '''Get the AWS Region'''
101     client = boto3.client ('s3')
```



```
    my_region = client.meta.region_name
    logger.debug("The rgion is %s" % (my_region))

    '''Creating a Boto cleint session'''
    session = boto3.session.session ()
    client = session.client (
        service_name='secretsmanager',
        region_name=mon_region
    )

    '''Getting the values stored in the secret with id: <
       aws_secret_id>'''
    get_id_value_response = client.get_secret_value(
        SecreId = aws_secret_id
    )
    adm_user_id = json.loads(get_id_value_response["SecretString"
       ])["adm_user_id_key"]
    adm_user_secret = json.loads(get_id_value_response["
       SecretString"])["adm_user_secret_key"]

except Exception as e:
    logger.debug("Fetching of ADM credentials from AWS secret
       failed with error: %s" % (str(e)))
    raise e

'''
Initialisation des gestionnaires d'API ADM courants
'''
mas_common_headers = {

    'Content-Type': "application/json",
    'Accept-type': "application/json",
    'Connection': "keep-alive",
    'isCloud': "true"
 }


'''
API pour se connecter à l'ADM et récupérer l'ID de session et l'ID
    de locataire
'''
url = "https://" + str(adm_ip_or_hostname) + "/nitro/v1/config/
   login"
payload = 'object={
 "login":{
```



```
 "ID":"' + adm_user_id + '","Secret":"' + adm_user_secret + '" }
  }
 '
essayez :
    response = _request("POST", url, data=payload, headers=
       mas_common_headers)
    sessionid = response["login"][0]["sessionid"]
    tenant_id = response["login"][0]["tenant_name"]
except Exception as e:
    logger.debug("Login call to the ADM failed with error: %s" % (
       str(e)))
    raise e

'''
API pour récupérer l'URL du service et le jeton à utiliser pour
   enregistrer l'agent auprés de l'ADM
'''
mas_common_headers['Cookie'] = 'SESSID=' + str(sessionid)
url = "https://" + str(adm_ip_or_hostname) + "/nitro/v1/config/
   trust_preauthtoken/" + tenant_id +"?customer="+ tenant_id
logger.debug("Fetching Service URL and Token.")
essayez :
    response = _request("GET", url, data=None, headers=
       mas_common_headers)
    service_name  = response["trust_preauthtoken"][0]["
       service_name"]
    token = response["trust_preauthtoken"][0]["token"]
    api_gateway_url = response["trust_preauthtoken"][0]["
       api_gateway_url"]
except Exception as e:
    logger.debug("Fetching of the Service URL Passed with error. %
       s" % (str(e)))
    raise e

'''
Exécution de la commande Register agent en utilisant les valeurs
   que nous avons récupérées précédemment
'''
essayez :
    registeragent_command = "registeragent -serviceurl "+
       api_gateway_url+" -activationcode "+service_name+"\;"+token
    file_run_command = "/var/python/bin/python2.7 /mps/
       register_agent_cloud.py "+registeragent_command
    logger.debug("Executing registeragent command: %s" % (
       file_run_command))
```

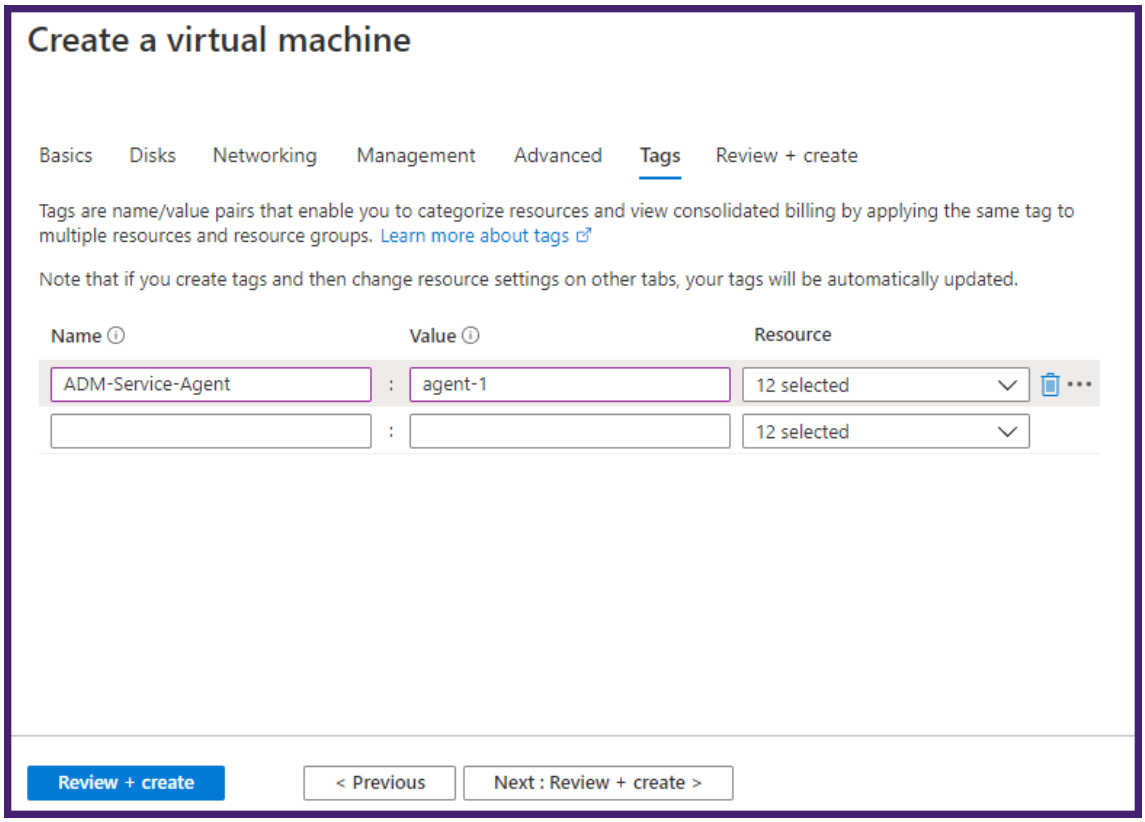


```
174     os.system(file_run_command)
175 except Exception as e:
176     logger.debug("Agent Registeration failed with error: %s" % (
            str(e)))
177         raise e
178 ```
```

Si vous spécifiez ce script d'enregistrement automatique, ignorez les étapes 7 et 8.

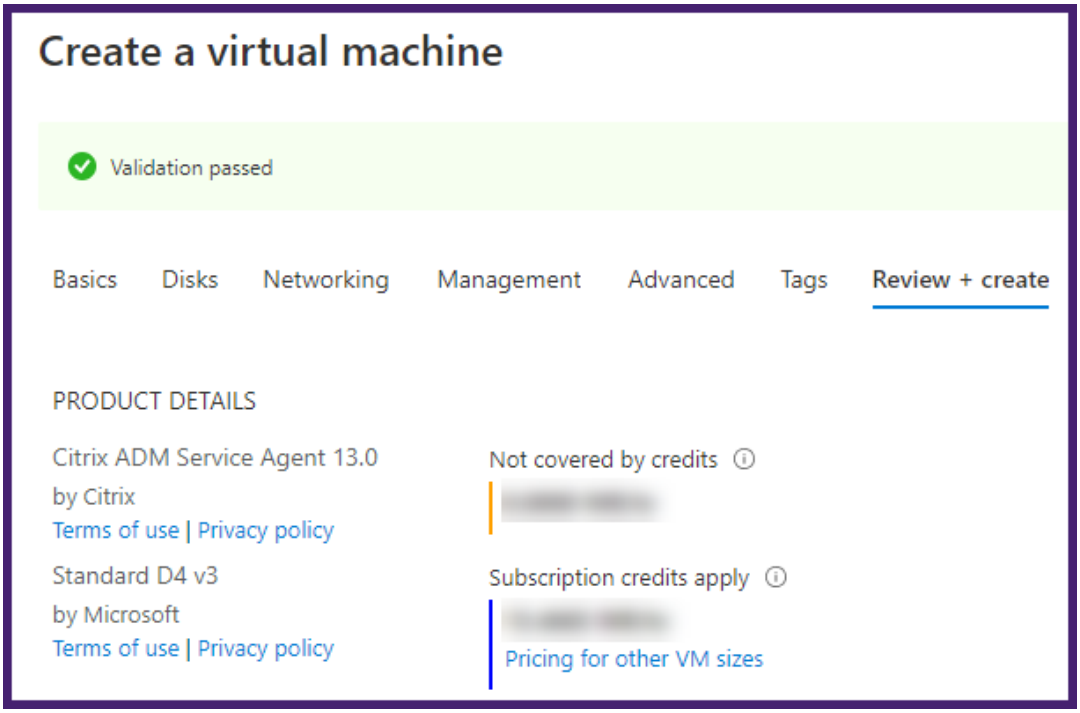
Balises :

Tapez la paire clé-valeur pour les balises de l'agent ADM. Une balise se compose d'une paire clé-valeur sensible à la casse. Ces balises vous permettent d'organiser et d'identifier facilement l'agent. Les balises sont appliquées à Azure et Citrix ADM.

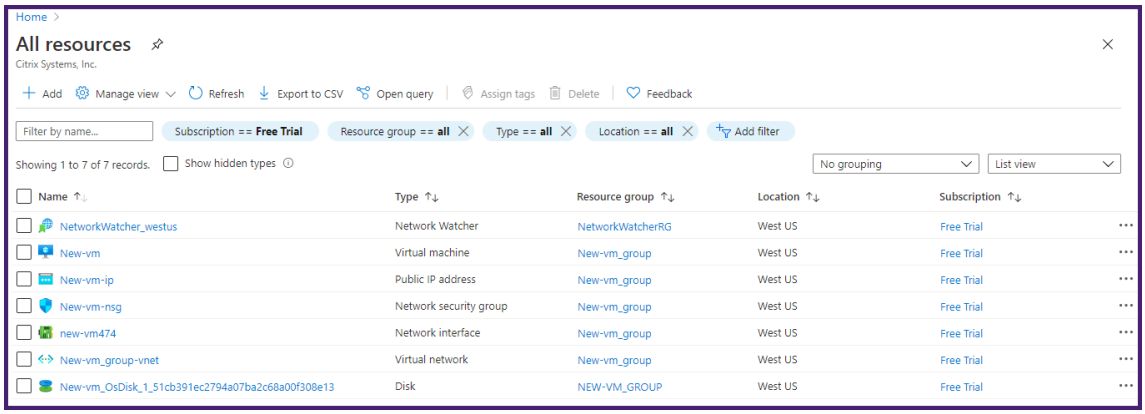


Les paramètres de configuration sont validés et l'onglet **Réviser et créer** affiche le résultat de la validation.

- Si la validation échoue, cet onglet affiche la raison de l'échec. Retournez à la section particulière et apportez les modifications nécessaires.
- Si la validation est valide, cliquez sur **Créer**. Le processus de déploiement de l'agent commence.



Le processus de déploiement peut prendre environ 10 à 15 minutes. Une fois le déploiement terminé, vous pouvez afficher votre machine virtuelle d'agent Citrix ADM dans votre compte Microsoft Azure.

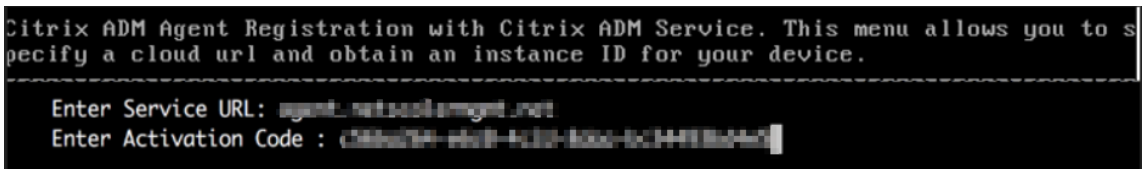


6. Une fois que l'agent est opérationnel, à l'aide d'un client SSH, connectez-vous à votre agent Citrix ADM à l'aide de l'**adresse IP publique**.

> **Remarque**
>
> ```
> - Si vous avez spécifié le nom d'utilisateur comme `nsrecover`, utilisez les informations d'identification de l'agent Citrix ADM par défaut (**nsrecover/nsroot**) pour vous connecter à la machine virtuelle.
> ```


> - Citrix vous recommande de modifier votre mot de passe par défaut après la première ouverture de session. Pour changer le mot de passe, tapez : **passwd nsroot**.

7. Entrez la commande suivante pour appeler l'écran de déploiement : **deployment_type.py**
8. Entrez l' **URL du service** et le **code d'activation** que vous avez copiés et enregistrés à partir de la page **Configurer les agents** dans Citrix ADM, comme indiqué dans Mise en route. L'agent utilise l'URL du service pour localiser le service et le code d'activation pour s'inscrire auprès du service.



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

Une fois l'agent redémarré, accédez à Citrix ADM et sur la page **Configurer l'agent**, sous **Agents découverts**, vérifiez l'état de l'agent.
‘‘‘

Installer l'agent Citrix ADM sur Amazon Web Services (AWS)

April 29, 2021

L'agent Citrix Application Delivery Management (Citrix ADM) fonctionne comme intermédiaire entre Citrix ADM et les instances découvertes dans le centre de données ou sur le cloud.

Conditions préalables

Pour lancer une AMI d'agent Citrix ADM dans un Cloud privé virtuel (VPC) Amazon Web Services (AWS) à l'aide de l'interface graphique Amazon, vous devez :

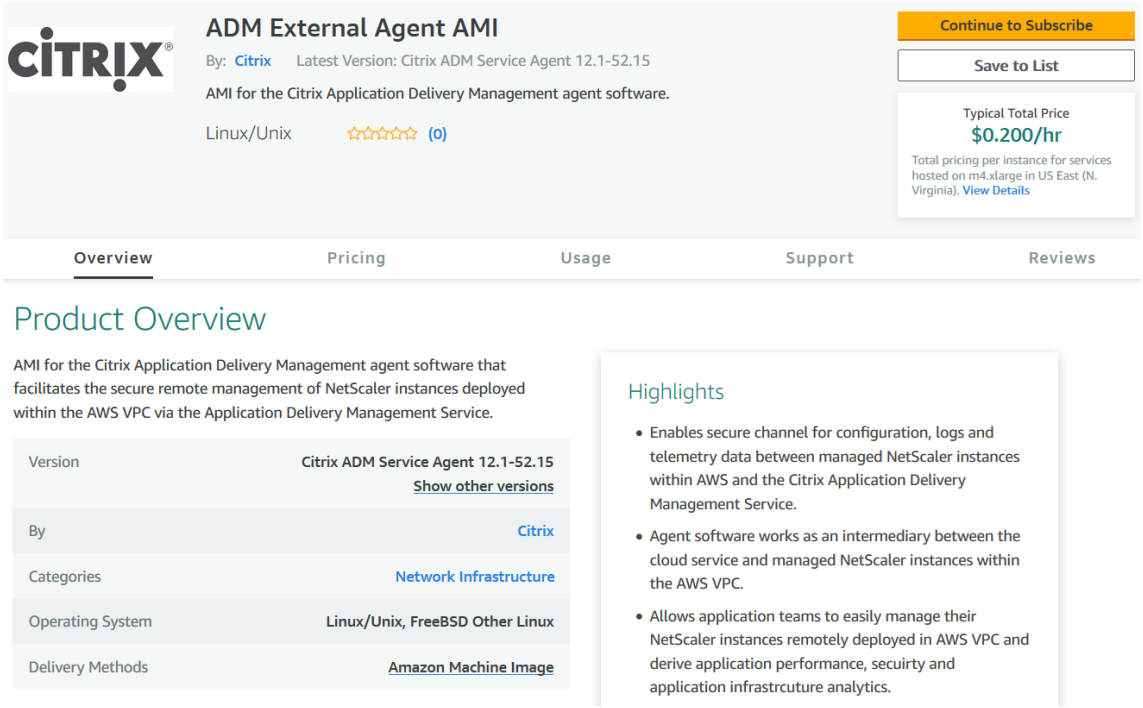
- Un compte AWS
- Un cloud privé virtuel (VPC) AWS
- Un compte IAM

> **Remarque**
>
> - Avant de provisionner une machine virtuelle d'agent ADM, Citrix recommande de créer un groupe de sécurité, un réseau privé virtuel, une paire de clés, un sous-réseau et d'autres entités. Ainsi, les informations réseau sont disponibles pendant le provisioning.

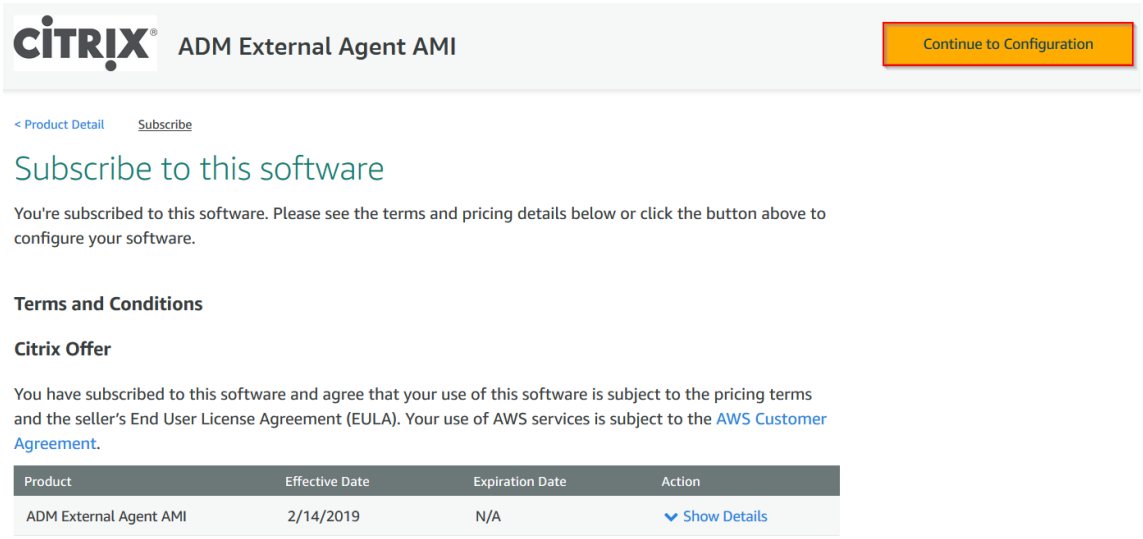
> • Pour qu'un agent Citrix ADM communique avec Citrix ADM et les instances Citrix ADC, assurez-vous que les ports recommandés sont ouverts. Pour plus d'informations sur la configuration de port requise pour un agent Citrix ADM, reportez-vous à la section Ports.

Pour installer l'agent Citrix ADM sur AWS :

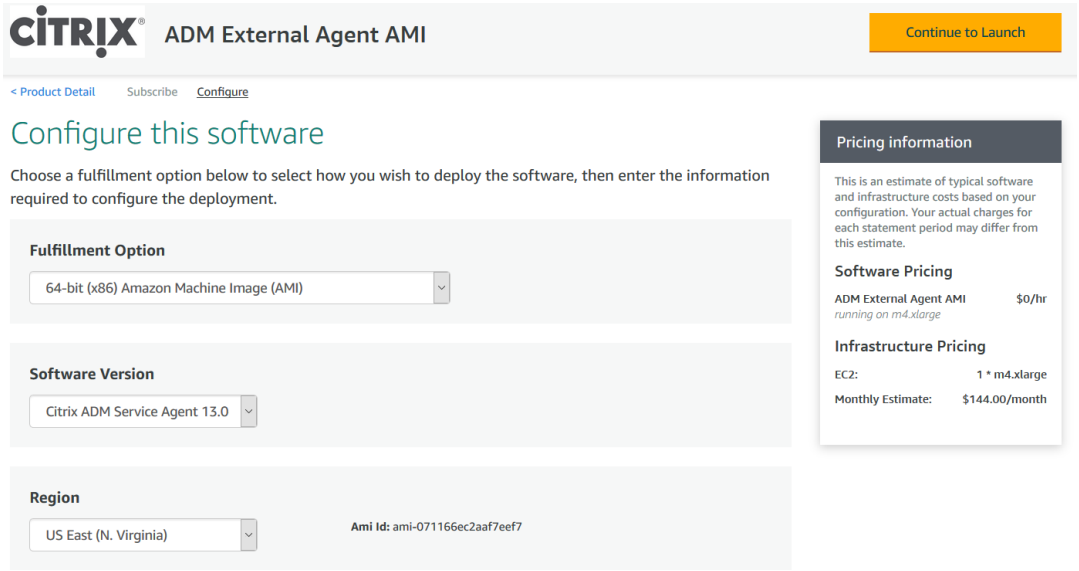
1. Connectez-vous à l'à l'Marketplace AWSaide de vos informations d'identification AWS.
2. Dans le champ de recherche, tapez **Citrix ADM Agent** pour rechercher l'AMI de l'agent Citrix ADM, puis cliquez sur **Exécuter** .
3. Dans la page de résultats de recherche, cliquez sur l' **AMI de l'agent externe ADM** dans la liste disponible.
4. Sur la page **AMI de l'agent externe ADM**, cliquez sur **Continuer pour vous abonner** .



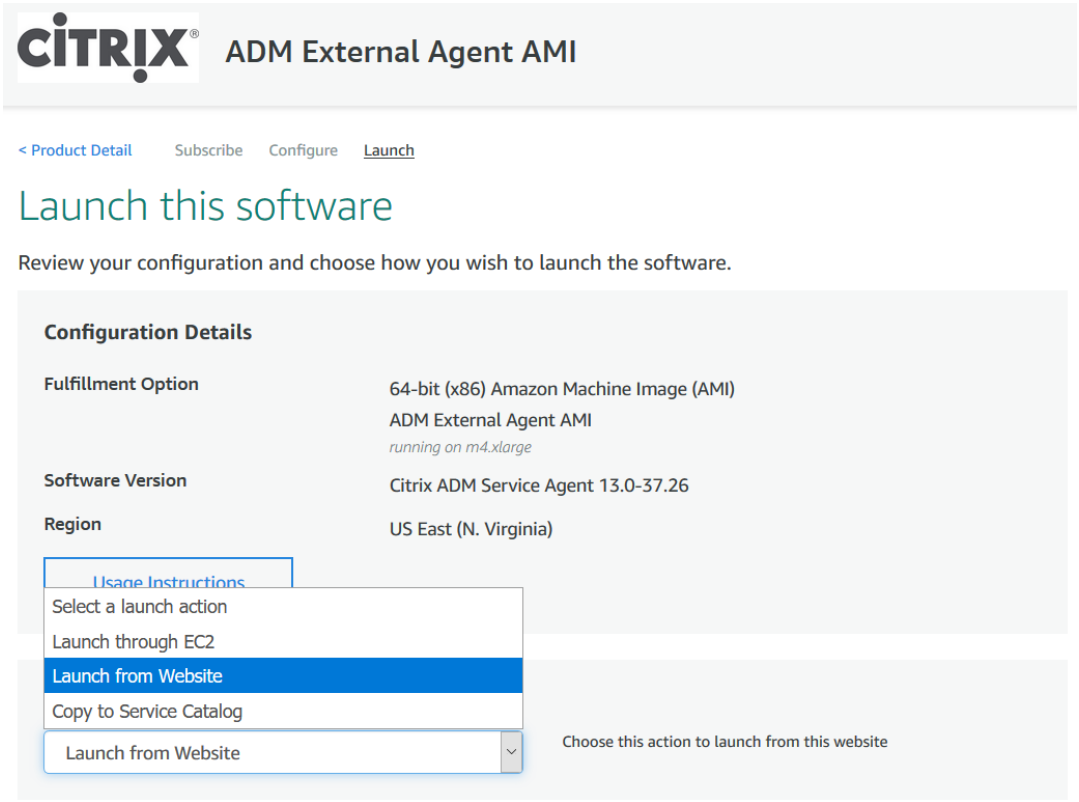
5. Une fois l'abonnement réussi, cliquez sur **Continuer vers la configuration**.



6. Sur la page **Configurer ce logiciel** :
   a) Sélectionnez l'AMI dans la liste des **options Expédié**.
   b) Sélectionnez la dernière version de l'agent Citrix ADM dans la liste **Version du logiciel** .
   c) Sélectionnez votre région dans la liste **Région** .
   d) Cliquez sur **Continuer pour lancer**



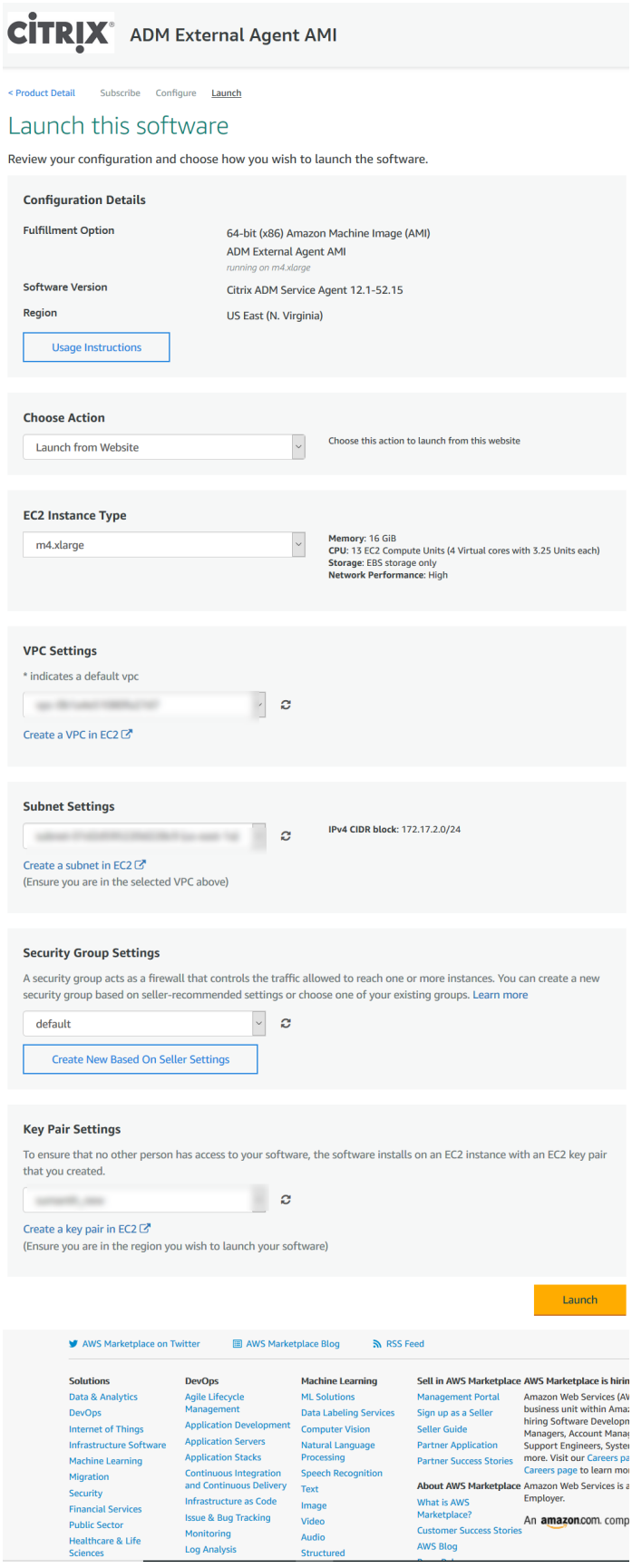
7. Sur la page **Lancer ce logiciel**, vous avez deux options pour enregistrer l'agent Citrix ADM :
   a) **Lancement à partir du site Web**
   b) **Lancement avec EC2**



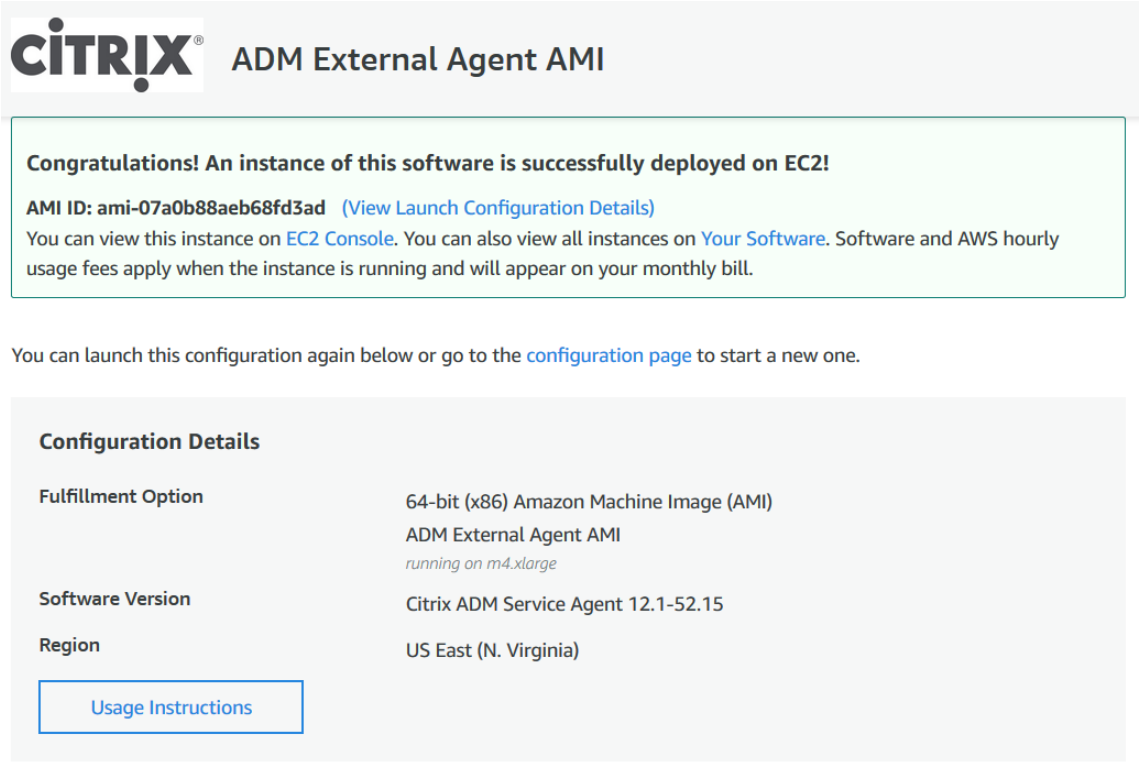
Lancement à partir d'un site Web

Pour lancer à partir d'un site Web, sélectionnez :

1. Type d'instance EC2 de la liste **Type d'instance EC2**
2. Un VPC de la liste des **paramètres du VPC** . Cliquez sur **Créer un VPC dans EC2** pour créer un VPC pour votre logiciel.
3. Un sous-réseau de la liste **Paramètres du sous-réseau** . Cliquez sur **Créer un sous-réseau dans EC2** pour créer un sous-réseau après avoir sélectionné le VPC.
4. Groupe de sécurité pour le pare-feu de la liste **Paramètres du groupe de sécurité**. Cliquez sur **Créer un nouveau paramètre basé sur les paramètres du vendeur** pour créer un groupe de sécurité.
5. Une paire de clés pour assurer la sécurité d'accès à partir de la liste **Paramètres des paires de clés** . Cliquez sur **Créer une paire de clés dans EC2** pour créer une paire de clés pour votre logiciel.
6. Cliquez sur **Lancer**



7. Le lancement à partir d'un site Web est couronné de succès.



> **Remarque**
>
> Le processus de déploiement peut prendre environ 10 à 15 minutes. Une fois le déploiement terminé, vous pouvez afficher votre machine virtuelle Citrix ADM agent sur votre compte AWS.

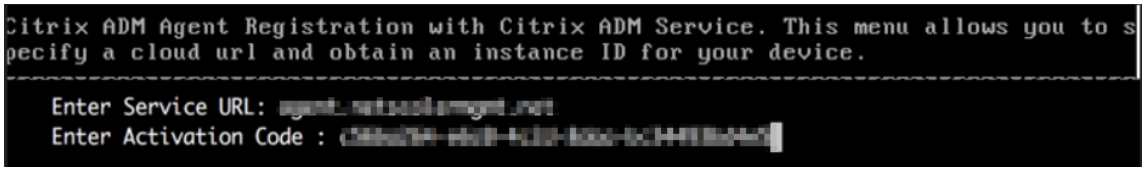
8. Une fois l'agent déployé, attribuez un nom à votre agent Citrix ADM.
9. Une fois l'agent opérationnel, attribuez une adresse IP élastique à votre agent Citrix ADM.

> **Remarque**
>
> L'adresse IP Elastic permet à l'agent Citrix ADM de communiquer avec Citrix ADM. Toutefois, une adresse IP élastique peut ne pas être requise si vous avez configuré la passerelle NAT pour acheminer le trafic vers Internet.

10. À l'aide d'un client SSH, connectez-vous à votre agent Citrix ADM à l'aide de l'adresse IP publique.

> **Remarque**
>
> Vous pouvez vous connecter à Citrix ADM Agent de l'une des manières suivantes :
>
> - Utilisez `nsrecover` comme nom d'utilisateur et ID d'instance AWS comme mot de passe.
> - Utilisez `nsroot` comme nom d'utilisateur et un clavier valide comme mot de passe.

11. Entrez la commande suivante pour appeler l'écran de déploiement : **deployment_type.py**
12. Entrez l' **URL du service** et le **code d'activation** que vous avez copiés et enregistrés à partir de la page **Configurer les agents** dans Citrix ADM, comme indiqué dans Mise en route. L'agent utilise l'URL du service pour localiser le service et le code d'activation pour s'inscrire auprès du service.



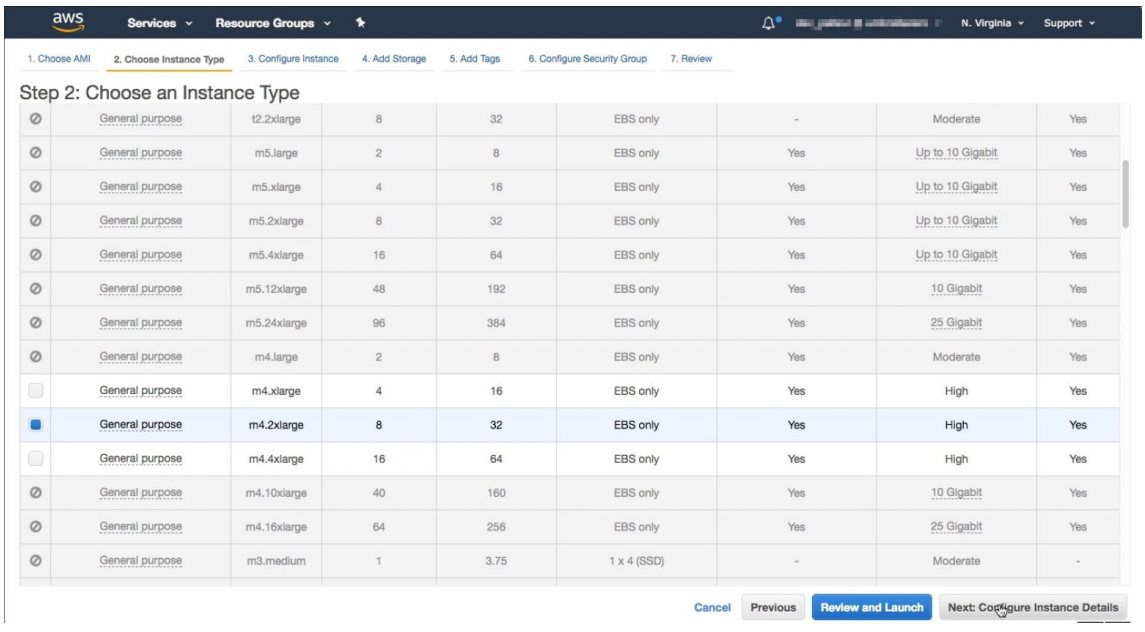
Une fois l'enregistrement de l'agent réussi, l'agent redémarre pour terminer le processus d'installation.

Une fois l'agent redémarré, accédez à Citrix ADM et sur la page **Configurer l'agent**, sous **Agents découverts**, vérifiez l'état de l'agent.

Lancement avec EC2

Pour lancer avec EC2, sélectionnez **Lancer via EC2** dans la liste **Choisir une action**, puis cliquez sur **Lancer** .

1. Dans la page **Choisir un type d'instance**, sélectionnez l'instance, puis cliquez sur **Suivant : Configurer les détails de l'instance**.



2. Dans la page **Configurer les détails de l'instance**, spécifiez les paramètres requis.

   Dans la section **Détails avancés**, vous pouvez activer un agent zéro contact en spécifiant des détails d'authentification ou un script dans le champ **Données utilisateur**.

- **Détails de l'authentification** : spécifiez l' **URL de service** et le **code d'activation** que vous avez copiés à partir de la page **Configurer les agents** dans Citrix ADM comme indiqué dans Mise en route. Entrez les détails dans le format suivant.

```
registeragent -serviceurl <apigatewayurl> -activationcode <
    activationcodevalue>
<!--NeedCopy-->
```

L'agent utilise ces informations pour s'enregistrer automatiquement auprès du service ADM pendant le démarrage.

- **Script** - Spécifiez un script d'enregistrement automatique de l'agent en tant que données utilisateur. Voici un exemple de script :

```
#!/var/python/bin/python2.7
import os
import requests
import json
import time
import re
import logging
import logging.handlers
import boto3

'''
Overview of the Script:
The script helps to register an ADM agent with ADM. Pass it
    in userdata to make ADM agent in AWS to autoregister on
    bootup. The workflow is as follows
1)  Fetch the ADM service API credentials (ID and secret)
    from AWS secret store (NOTE: you have to assign IAM role
    to the ADM Agent that will give permission to fetch
    secrets from AWS secret store)
2)  Login to ADM service with credentials fetched in step 1
3)  Call ADM service to fetch credentials (serviceURL and
    token) for agent registration
4)  Calls registration by using the credentials fetched in
    step 3
'''

'''
These are the placeholders which you need to replace
    according to your setup configurations
aws_secret_id: Id of the AWS secret where you have stored ADM
     Credentials
```



```
The secrets value should be in the following json format
{
 "adm_user_id_key": "YOUR_ID", " adm_user_secret_key": "
    YOUR_SECRET" }

'''

aws_secret_id = "<AWS_secret_id>"
adm_ip_or_hostname = "<YOUR_ADM_POP>.adm.cloud.com"

'''
Set up a specific logger with your desired output level and
   log file name
'''
log_file_name_local = os.path.basename(\_\_file\_\_)
LOG_FILENAME = '/var/log/' + 'bootstrap' + '.log'
LOG_MAX_BYTE = 50\*1024\*1024
LOG_BACKUP_COUNT = 20

logger = logging.getLogger(\_\_name\_\_)
logger.setLevel(logging.DEBUG)
logger_handler = logging.handlers.RotatingFileHandler(
   LOG_FILENAME, maxBytes=LOG_MAX_BYTE, backupCount=
   LOG_BACKUP_COUNT)
logger_fortmater = logging.Formatter(fmt='%(asctime)-2s:%(
   funcName)30s:%(lineno)4d: [%(levelname)s] %(message)s',
   datefmt="%Y-%m-%d %H:%M:%S")
logger_handler.setFormatter(logger_fortmater)
logger.addHandler(logger_handler)

class APIHandlerException(Exception):
    def \_\_init\_\_(self, error_code, message):
        self.error_code = error_code
        self.message = message

    def \_\_str\_\_(self):
        return self.message + ". Error code '" + str(self.
           error_code) + "'"

def parse_response(response, url, print_response=True):
    if not response.ok:
        if "reboot" in url:
            logger.debug('No response for url: reboot')
            resp = {
"errorcode": "500", "message": "Error while reading response.
```



```
        " }
61
62              return resp
63
64          if print_response:
65              logger.debug('Response text for %s is %s' % (url,
                    response.text))
66
67          response = json.loads(response.text)
68          logger.debug("ErrorCode - " + str(response['errorcode
                ']) + ". Message -" + str(response['message']))
69          raise APIHandlerException(response['errorcode'], str(
                response['message']))
70      elif response.text:
71          if print_response:
72              logger.debug('Response text for %s is %s' % (url,
                    response.text))
73
74          result = json.loads(response.text)
75          if 'errorcode' in result and result['errorcode'] > 0:
76              raise APIHandlerException(result['errorcode'],
                    str(result['message']))
77          return result
78
79  def _request(method, url, data=None, headers=None, retry=3,
        print_response=True):
80      try:
81          response = requests.request(method, url, data=data,
                headers=headers)
82          result = parse_response(response, url, print_response
                =print_response)
83          return result
84      except [requests.exceptions.ConnectionError, requests.
            exceptions.ConnectTimeout]:
85          if retry > 0:
86              return _request(method, url, data, headers, retry
                    -1, print_response=print_response)
87          else:
88              raise APIHandlerException(503, 'ConnectionError')
89      except requests.exceptions.RequestException as e:
90          logger.debug(str(e))
91          raise APIHandlerException(500, str(e))
92      except APIHandlerException as e:
93          logger.debug("URL: %s, Error: %s, Message: %s" % (url
                , e.error_code, e.message))
```



```
94              raise e
95          except Exception as e:
96              raise APIHandlerException(500, str(e))
97
98      try:
99          '''Get the AWS Region'''
100         client = boto3.client('s3')
101         my_region = client.meta.region_name
102         logger.debug("The rgion is %s" % (my_region))
103
104         '''Creating a Boto cleint session'''
105         session = boto3.session.Session()
106         client = session.client(
107             service_name='secretsmanager',
108             region_name=my_region
109         )
110
111         '''Getting the values stored in the secret with id: <
                aws_secret_id>'''
112         get_id_value_response = client.get_secret_value(
113             SecretId = aws_secret_id
114         )
115         adm_user_id = json.loads(get_id_value_response["
                SecretString"])["adm_user_id_key"]
116         adm_user_secret = json.loads(get_id_value_response["
                SecretString"])["adm_user_secret_key"]
117
118     except Exception as e:
119         logger.debug("Fetching of ADM credentials from AWS secret
                failed with error: %s" % (str(e)))
120         raise e
121
122     '''
123     Initializing common ADM API handlers
124     '''
125     mas_common_headers = {
126
127         'Content-Type': "application/json",
128         'Accept-type': "application/json",
129         'Connection': "keep-alive",
130         'isCloud': "true"
131      }
132
133
134     '''
```

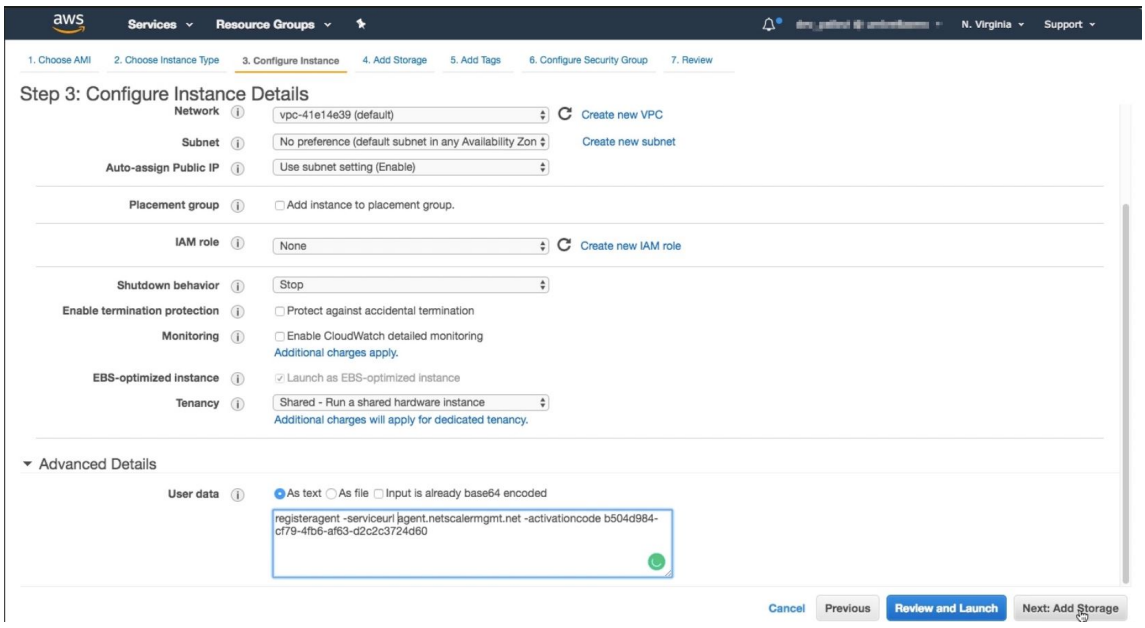


```
API to login to the ADM and fetch the Session ID and Tenant ID
'''
url = "https://" + str(adm_ip_or_hostname) + "/nitro/v1/config/login"
payload = 'object={
"login":{
"ID":"' + adm_user_id + '","Secret":"' + adm_user_secret + '"}
 }
'
try:
    response = _request("POST", url, data=payload, headers=mas_common_headers)
    sessionid = response["login"][0]["sessionid"]
    tenant_id = response["login"][0]["tenant_name"]
except Exception as e:
    logger.debug("Login call to the ADM failed with error: %s" % (str(e)))
    raise e

'''
API to fetch the service URL and Token to be used for registering the agent with the ADM
'''
mas_common_headers['Cookie'] = 'SESSID=' + str(sessionid)
url = "https://" + str(adm_ip_or_hostname) + "/nitro/v1/config/trust_preauthtoken/" + tenant_id +"?customer="+ tenant_id
logger.debug("Fetching Service URL and Token.")
try:
    response = _request("GET", url, data=None, headers=mas_common_headers)
    service_name  = response["trust_preauthtoken"][0]["service_name"]
    token = response["trust_preauthtoken"][0]["token"]
    api_gateway_url = response["trust_preauthtoken"][0]["api_gateway_url"]
except Exception as e:
    logger.debug("Fetching of the Service URL Passed with error. %s" % (str(e)))
    raise e

'''
Running the register agent command using the values we
```



```
        retrieved earlier
168     '''
169     try:
170         registeragent_command = "registeragent -serviceurl "+
                api_gateway_url+" -activationcode "+service_name+";"+
                token
171         file_run_command = "/var/python/bin/python2.7 /mps/
                register_agent_cloud.py "+registeragent_command
172         logger.debug("Executing registeragent command: %s" % (
                file_run_command))
173         os.system(file_run_command)
174     except Exception as e:
175         logger.debug("Agent Registeration failed with error: %s"
                % (str(e)))
176             raise e
177     <!--NeedCopy-->
```

Ce script récupère les détails d'authentification à partir du gestionnaire de secrets AWS et exécute le `deployment.py` script pour enregistrer l'agent auprès du service ADM.



Remarque

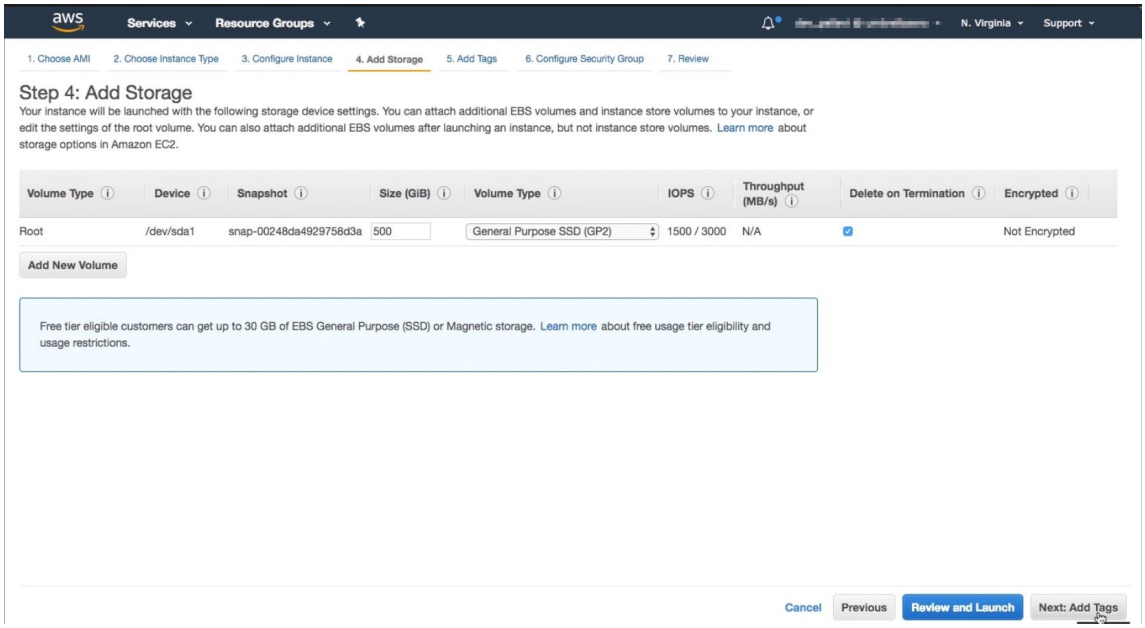
Bien que vous puissiez attribuer automatiquement une adresse IP publique, vous pouvez également attribuer une adresse IP élastique. L'attribution d'une adresse IP élastique est requise lorsque la passerelle NAT n'est pas configurée.

Si l'adresse IP élastique n'est pas définie dans cette étape, vous pouvez toujours le faire sur la console EC2. Vous pouvez créer une adresse IP élastique et l'associer à l'agent ADM en

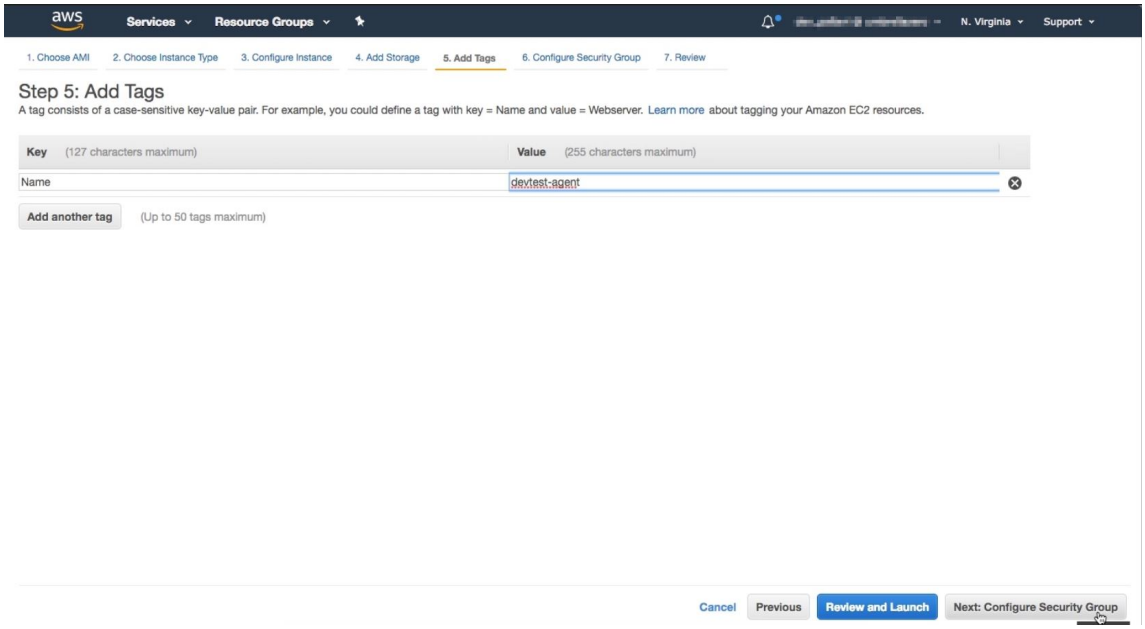
> utilisant l'ID d'instance ou l'ID ENI-ID.

Cliquez sur **Ajouter un stockage**.

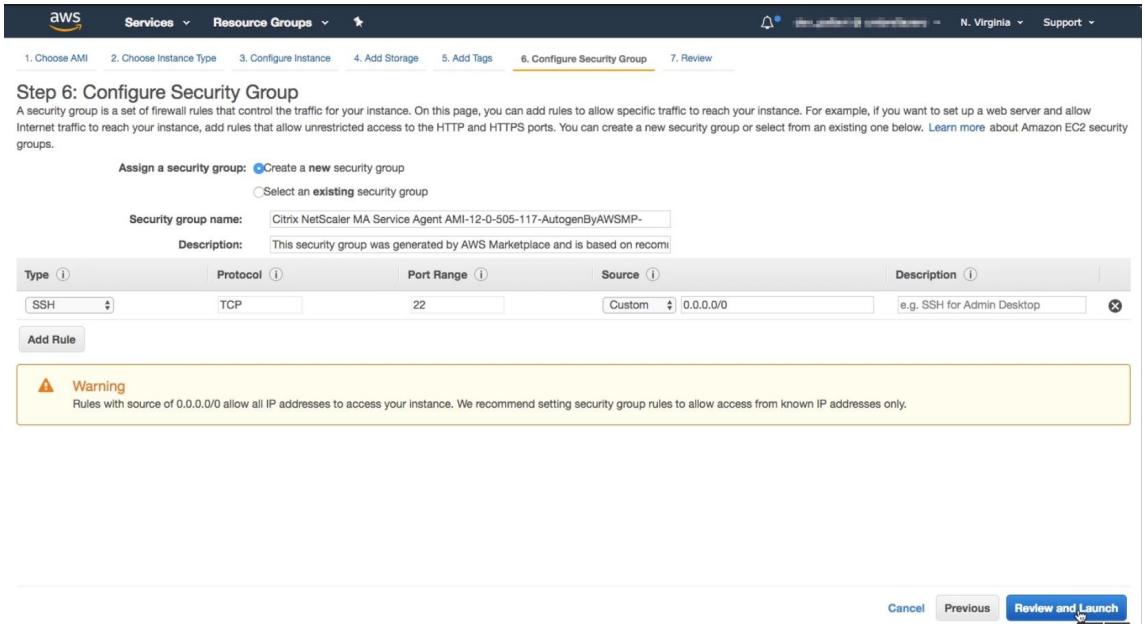
3. Dans la page **Ajouter du stockage**, configurez les paramètres du périphérique de stockage de l'instance, puis cliquez sur **Suivant : Ajouter des balises**.



4. Dans la page **Ajouter des balises**, définissez la balise de l'instance, puis cliquez sur **Suivant : Configurer le groupe de sécurité**.

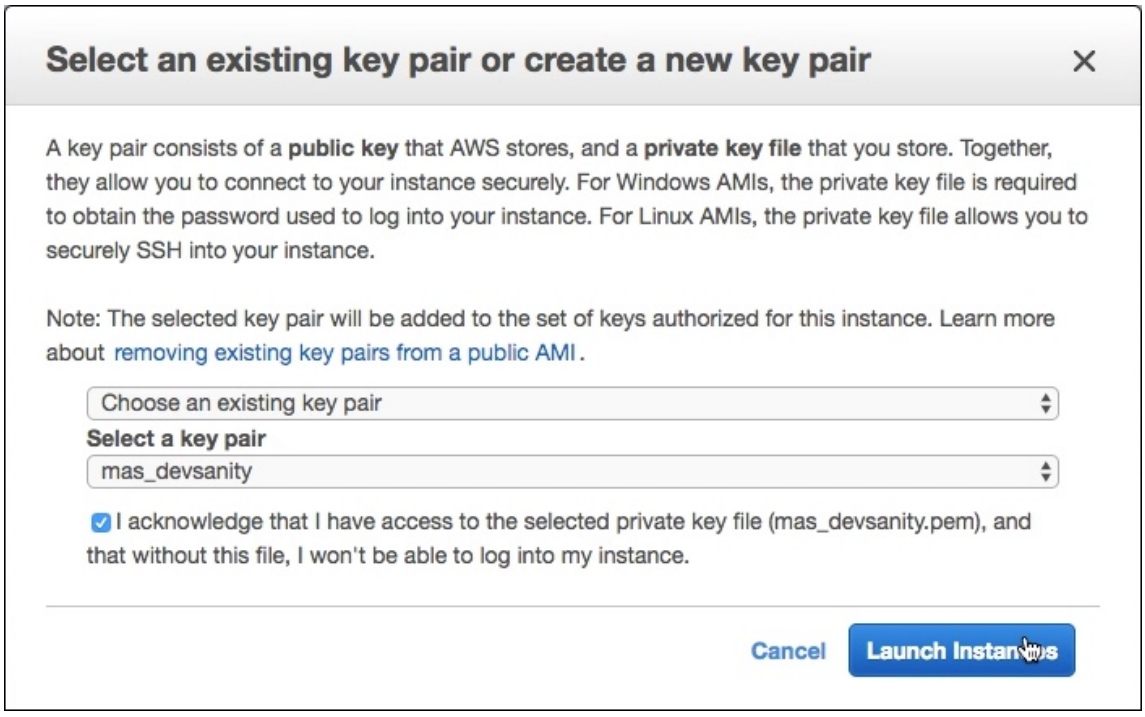


5. Dans la page **Configurer le groupe de sécurité**, ajoutez des règles pour autoriser un trafic spécifique à votre instance, puis cliquez sur **Réviser et lancer**.



6. Dans la page **Vérifier le lancement de l'instance**, passez en revue les paramètres de l'instance et cliquez sur **Lancer**.
7. Dans la boîte de dialogue **Sélectionner une paire de clés existante ou créer une nouvelle paire de clés**, créez une paire de clés. Vous pouvez également sélectionner parmi les paires de clés existantes.

   Acceptez l'accusé de réception et cliquez sur **Lancer les instances**.



Le processus de déploiement peut prendre environ 10 à 15 minutes. Une fois le déploiement terminé,

vous pouvez afficher votre machine virtuelle Citrix ADM agent sur votre compte AWS.

Installer l'agent Citrix ADM sur GCP

April 29, 2021

L'agent Citrix Application Delivery Management (Citrix ADM) fonctionne comme intermédiaire entre Citrix ADM et les instances découvertes dans le centre de données ou sur le cloud. Vous pouvez déployer l'agent sur Google Cloud Platform (GCP) pour faciliter la gestion à distance sécurisée des instances Citrix ADC déployées au sein du réseau virtuel Google cloud via Citrix ADM. Pour plus d'informations sur la manière dont l'agent ADM sur GCP fournit aux administrateurs informatiques, consultez le blog L'agent Citrix ADM est désormais disponible sur Google Cloud Platform Marketplace.

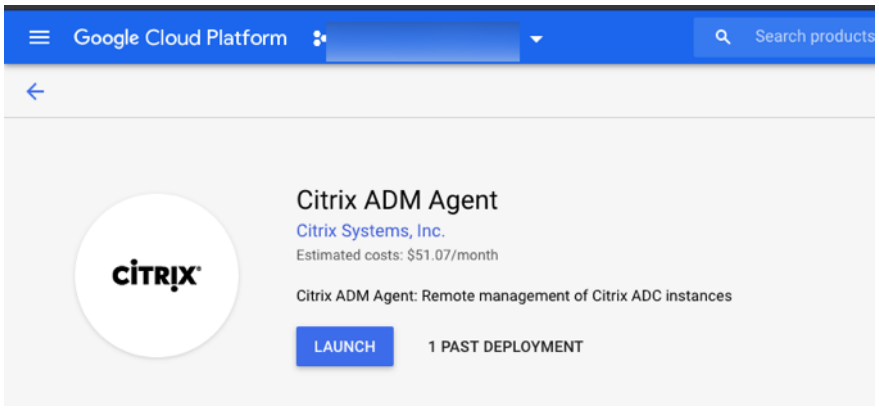
Conditions préalables

Pour installer un agent ADM sur GCP, vous avez besoin d'un compte GCP.

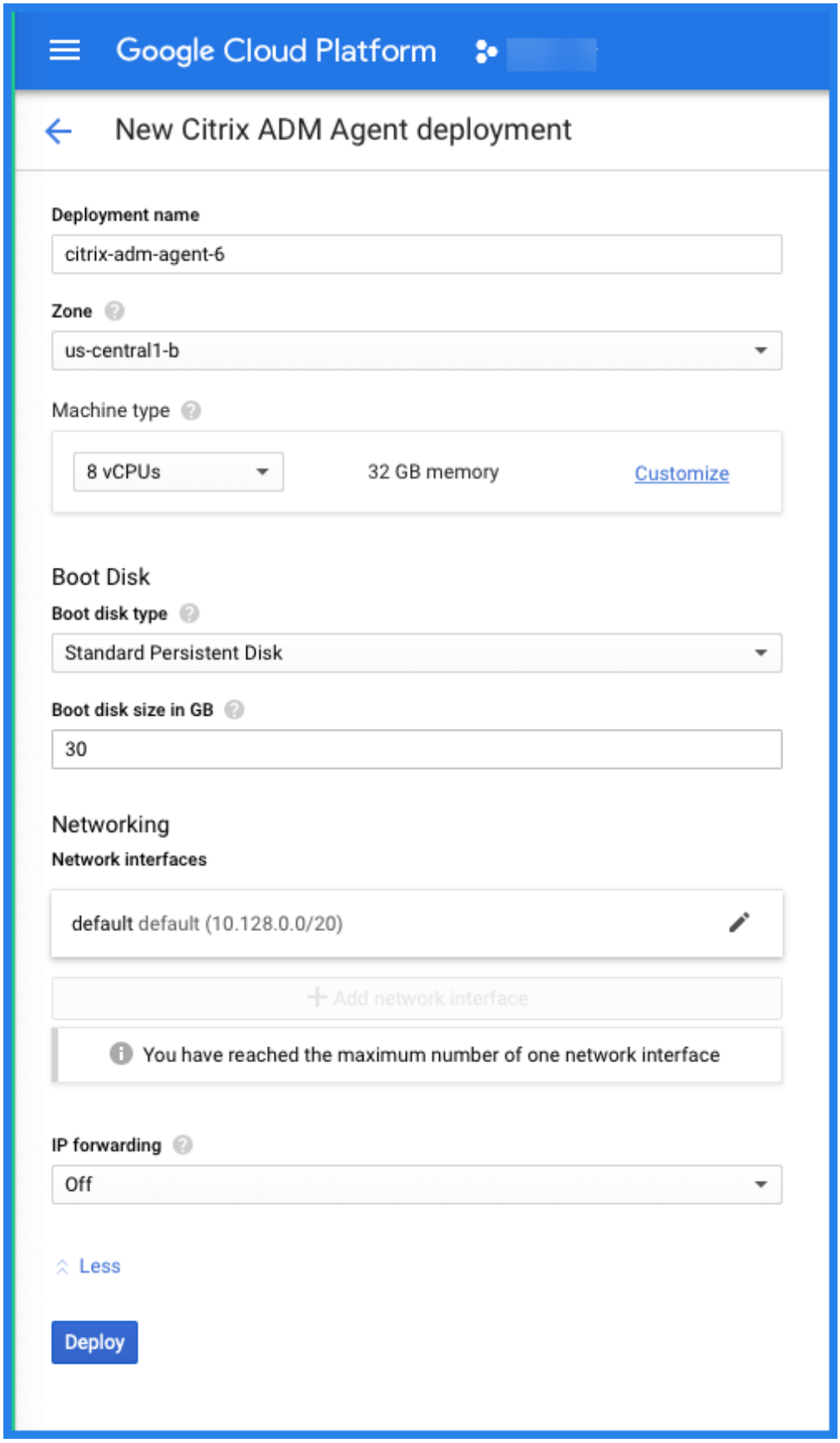
Installer l'agent Citrix ADM sur GCP

Procédez comme suit pour installer un agent ADM sur GCP.

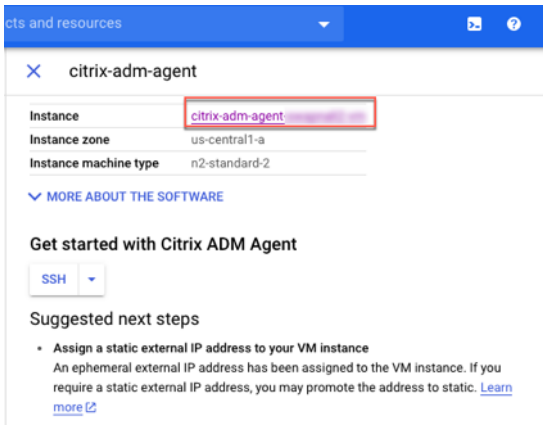
1. Connectez-vous à la console GCP (console.cloud.google.com) à l'aide de vos informations d'identification et accédez au site de vente.
2. Dans le champ de recherche, tapez **Citrix ADM Agent**.
3. Cliquez sur **Citrix ADM Agen**t dans le champ de résultats, puis cliquez sur **Lancer**.



4. Dans la page **Déploiement New Citrix ADM Agent**, la plupart des options sont définies par défaut. Vous pouvez modifier les configurations par défaut selon vos besoins et cliquer sur **Déployer**.



5. Une fois l'agent déployé, cliquez sur le lien d'instance et vérifiez les détails dans la **page Détails de l'instance de machine virtuelle**.

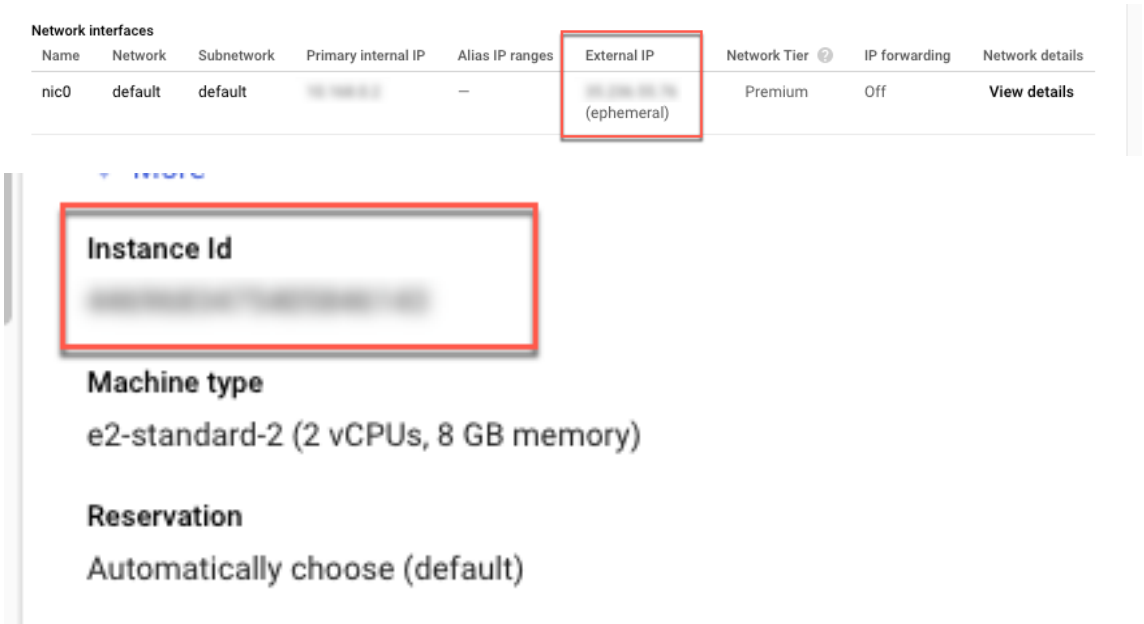


6. Connectez-vous à l'agent via un client SSH à l'aide de l'adresse IP externe de l'agent. Utilisez les commandes suivantes :

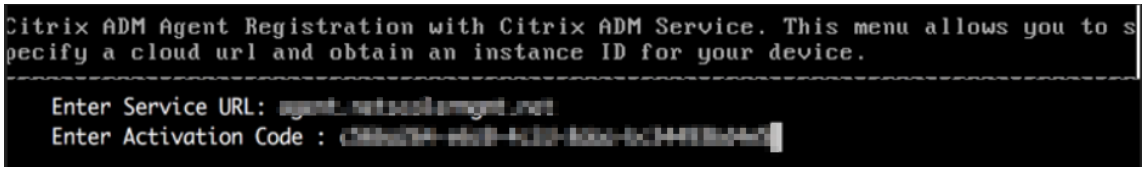
   ```
   ssh nsrecover@<external IP address of the agent>
   ```

   Mot de passe : ID d'instance

   Pouvez-vous trouver l'adresse IP externe et l'ID d'instance dans la page de **détails de l'instance de machine virtuelle**.



7. Entrez la commande suivante pour appeler l'écran de déploiement : **deployment_type.py**
8. Entrez l' **URL du service** et le **code d'activation** que vous avez copiés et enregistrés à partir de la page **Configurer les agents** dans Citrix ADM, comme indiqué dans Mise en route. L'agent utilise l'URL du service pour localiser le service et le code d'activation pour s'inscrire auprès du service.



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

Une fois l'agent redémarré, accédez à Citrix ADM et sur la page **Configurer l'agent**, sous **Agents découverts**, vérifiez l'état de l'agent.

Installer l'agent Citrix ADM dans le cluster Kubernetes

April 29, 2021

> **Remarque**
>
> La procédure d'installation d'un agent en tant que microservice est disponible dans la Mise en route section.

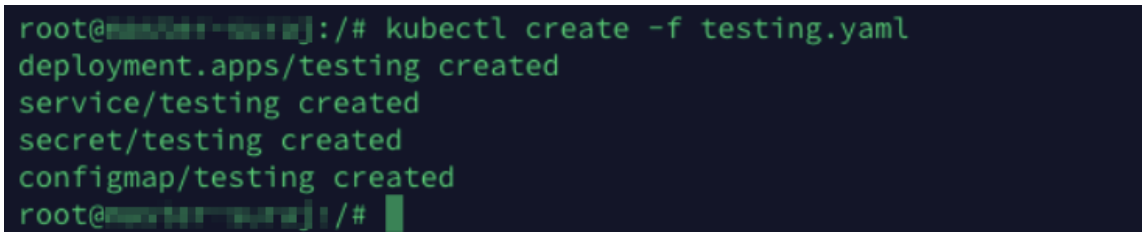
Dans le nœud maître Kubernetes :

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

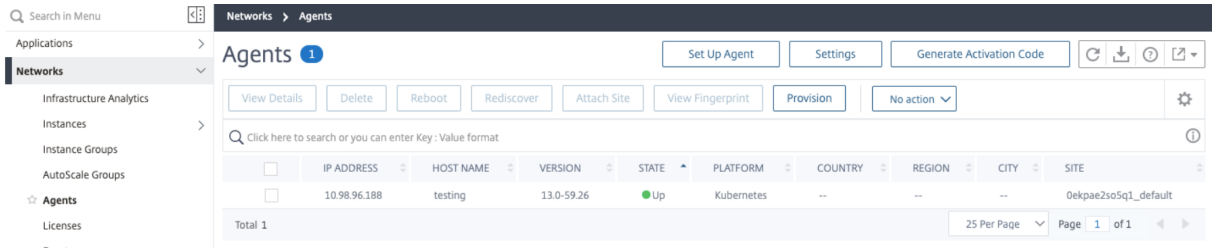
   ```
   kubectl create -f <yaml file>
   ```

   Par exemple, les opérations suivantes peuvent être effectuées : `kubectl create -f testing.yaml`

   L'agent est créé avec succès.



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



Comment obtenir de l'aide

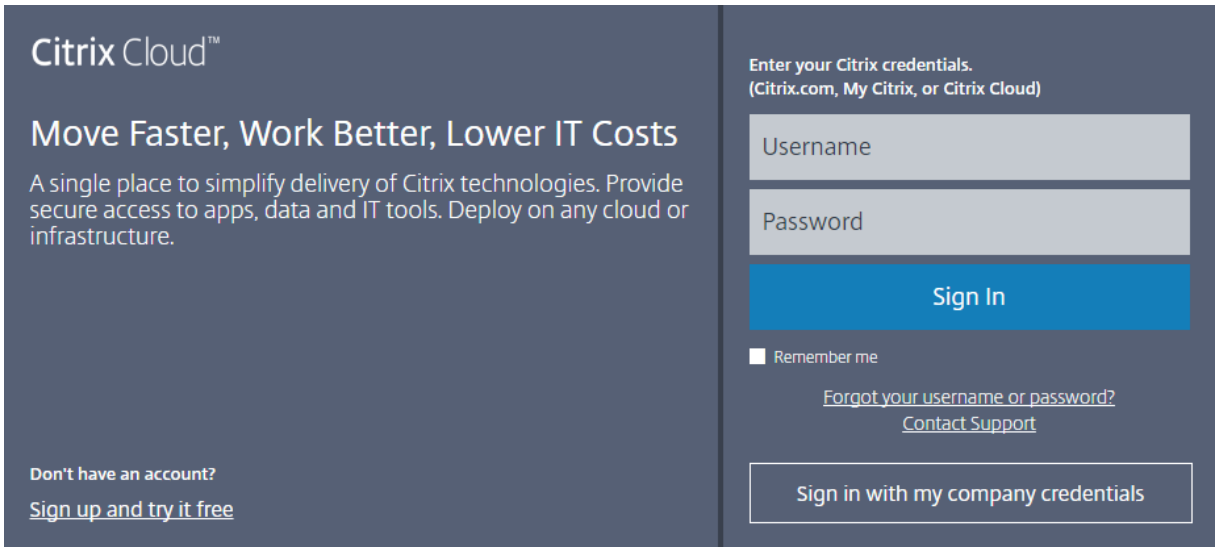
April 29, 2021

En tant qu'utilisateur Citrix Cloud, vous avez parfois besoin d'aide pour assurer le bon fonctionnement de notre infrastructure. Cette rubrique fournit plus d'informations sur les différentes options d'aide et de support et sur la façon d'y accéder.

Créer un compte Citrix Cloud

Si vous rencontrez une erreur lors de votre inscription à un compte Citrix Cloud, contactez le service client de Citrix.

Connectez-vous à votre compte



Si vous ne parvenez pas à vous connecter à votre compte Citrix Cloud :

- Assurez-vous que vous vous connectez avec l'adresse e-mail et le mot de passe que vous avez fournis lors de la création votre compte.
- Citrix Cloud vous invite automatiquement à réinitialiser votre mot de passe avant de pouvoir vous connecter, si :
  - Vous ne vous êtes pas connecté à Citrix Cloud depuis un certain temps
  - Votre mot de passe ne répond pas aux exigences de Citrix Cloud
- Pour plus d'informations, consultez la section Modification de votre mot de passe dans cet article.

- Si votre entreprise autorise les utilisateurs à se connecter à Citrix Cloud à l'aide de leurs informations d'identification d'entreprise au lieu d'un compte Citrix, cliquez sur **Se connecter avec mes identifiants d'entreprise** et entrez l'URL de connexion de votre entreprise. Vous pouvez ensuite entrer vos informations d'identification d'entreprise pour accéder au compte Citrix Cloud de votre entreprise. Si vous ne connaissez pas l'URL de connexion de votre entreprise, contactez l'administrateur de votre entreprise pour obtenir de l'aide.

Modifier votre mot de passe

Si vous avez oublié le mot de passe de votre compte Citrix Cloud, cliquez sur **Oublié votre nom d'utilisateur ou votre mot de passe ?**, et vous pouvez entrer l'adresse e-mail de votre compte. Vous recevez un e-mail pour réinitialiser votre mot de passe. Si vous ne recevez pas l'e-mail de réinitialisation du mot de passe ou si vous avez besoin de plus d'aide, contactez service client de Citrix.

Pour vous aider à préserver la sécurité du mot de passe de votre compte, Citrix Cloud peut vous inviter à réinitialiser votre mot de passe lorsque vous tentez de vous connecter. Cette invite s'affiche si :

- Votre mot de passe ne répond pas aux exigences de complexité de Citrix Cloud. Les mots de passe doivent comporter au moins 8 caractères et comprendre :
  - Au moins un chiffre
  - Au moins une lettre majuscule
  - Au moins un symbole : `! @ ## $ % ^ * ? + = –`
- Votre mot de passe inclut des mots du dictionnaire.
- Votre mot de passe est répertorié dans une base de données connue de mots de passe compromis.
- Vous ne vous êtes pas connecté à Citrix Cloud au cours des six derniers mois.

Lorsque vous y êtes invité, sélectionnez **Réinitialiser mot de passe** pour créer un nouveau mot de passe fort pour votre compte.

Forums de support Citrix Cloud

Sur les Forums de support Citrix Cloud, vous pouvez obtenir de l'aide, fournir des commentaires et des suggestions d'améliorations, consulter les conversations d'autres utilisateurs ou initier vos propres conversations.

Les membres du personnel de support Citrix suivent ces forums et sont prêts à répondre à vos questions. D'autres membres de la communauté Citrix Cloud peuvent également offrir de l'aide ou participer à la discussion.

Vous n'avez pas besoin de vous connecter pour lire les sujets du forum. Cependant, vous devez vous connecter pour publier ou répondre. Pour vous connecter, utilisez vos informations d'identification de compte Citrix existantes ou utilisez l'adresse e-mail et le mot de passe que vous avez fournis lors

de la création de votre compte Citrix Cloud. Pour créer un compte Citrix, accédez à Create or request an account (Créer ou demander un compte).

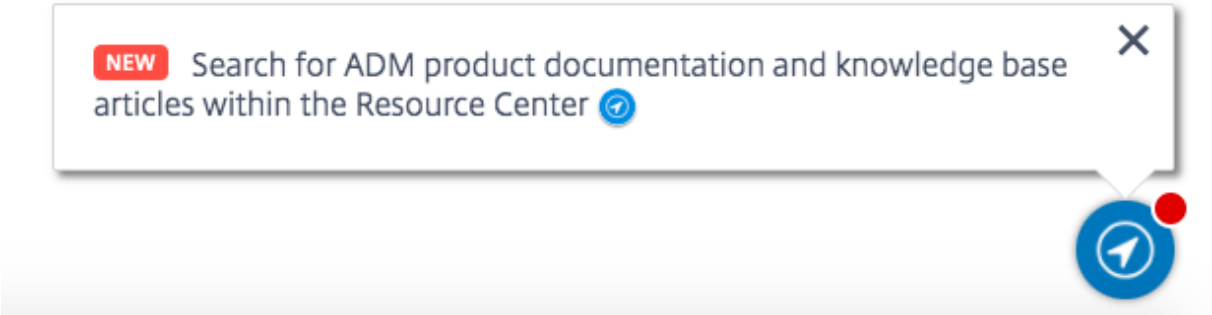
Articles de support et documentation

Citrix propose une multitude d'articles de support et de documentation produit pour vous aider à tirer le meilleur parti de Citrix Cloud et à résoudre de nombreux problèmes que vous pourriez rencontrer avec les produits Citrix.

Centre de ressources Citrix Cloud

Le Centre de ressources Citrix Cloud fournit plusieurs ressources pour vous aider à démarrer avec les services Citrix Cloud, en savoir plus sur les fonctionnalités et à résoudre les problèmes. Les ressources qui s'affichent sont applicables à la fonctionnalité ou au service de Citrix Cloud avec lequel vous travaillez actuellement. Par exemple, si vous vous trouvez dans la console de gestion du service Virtual Apps and Desktops, le Centre de ressources affiche les ressources suivantes.

Accédez au Centre de ressources à tout moment en cliquant sur l'icône bleue de la boussole située en bas à droite de la console Citrix Cloud.



- **Mise en route** : fournit une brève présentation guidée des tâches clés spécifiques au service avec lequel vous travaillez actuellement. Vous trouverez également des liens vers des ressources de formation et d'intégration pour vous aider à en savoir plus sur les fonctionnalités de service et à configurer vos utilisateurs finaux pour réussir.
- **Annonces** : fournit des notifications sur les fonctionnalités nouvellement publiées et des liens vers les communications Citrix importantes. Cliquez sur une notification de fonctionnalité pour recevoir une brève présentation guidée de l'entité.
- **Rechercher des articles** : fournit une liste des documents produit et des articles du Centre de connaissances pour les tâches courantes et vous aide à trouver d'autres articles, sans quitter Citrix Cloud. Entrez une requête de recherche dans le champ **Comment...** pour obtenir une

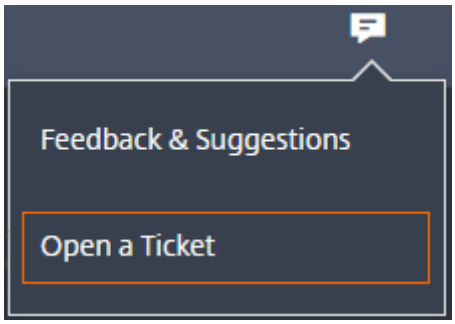
liste d'articles filtrée en fonction du service avec lequel vous travaillez. En général, les articles de support apparaissent en premier dans la liste, suivis des articles de documentation produit.

Citrix Tech Zone

Citrix Tech Zone contient de nombreuses informations pour vous aider à en savoir plus sur Citrix Cloud et d'autres produits Citrix. Vous trouverez ici des architectures de référence, des diagrammes, des vidéos et des documents techniques qui fournissent des informations sur la conception, la création et le déploiement des technologies Citrix.

Support technique

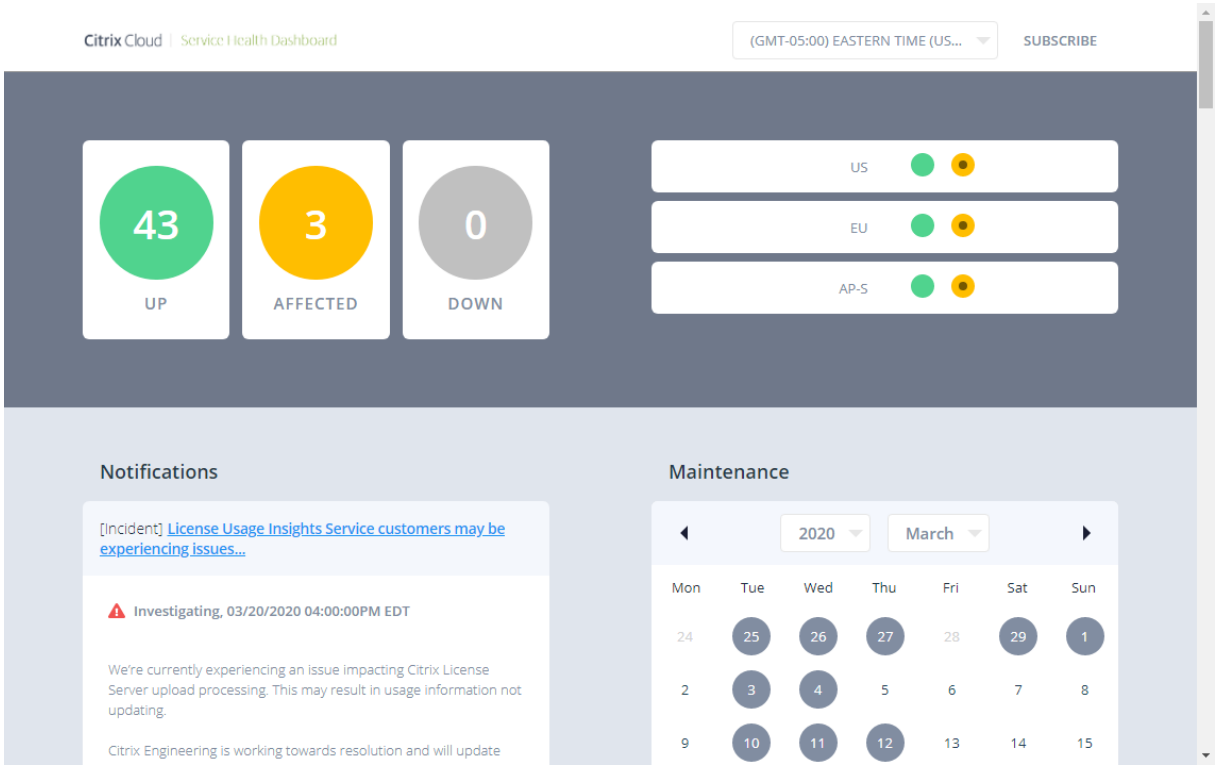
Si vous rencontrez un problème nécessitant une assistance technique, cliquez sur l'icône **Commentaires/support** dans le coin supérieur droit de l'écran, puis sélectionnez **Ouvrir un ticket**.



Cliquez sur **Accéder à My support**, puis sur **My Support** pour ouvrir un ticket via le portail My Support. Vous pouvez également utiliser le portail My Support pour suivre vos tickets existants et afficher vos droits de produit actuels.

tableau de bord de l'état de service

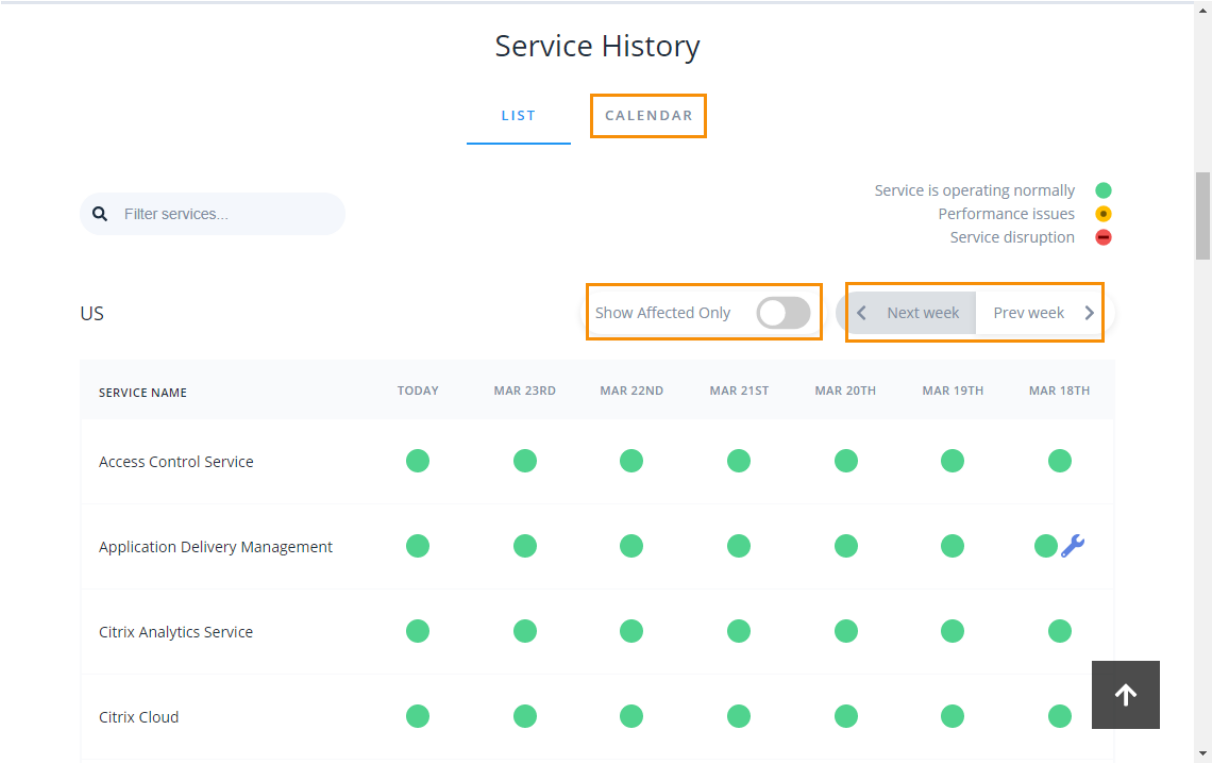
Le Tableau de bord d'intégrité du service Citrix Cloud fournit une vue d'ensemble de la disponibilité en temps réel de la plate-forme et des services Citrix Cloud dans chaque région géographique. Si vous rencontrez des problèmes avec Citrix Cloud, consultez le Tableau de bord d'intégrité du service pour vérifier que Citrix Cloud ou des services spécifiques fonctionnent normalement.



Utilisez le tableau de bord pour en savoir plus sur les conditions suivantes :

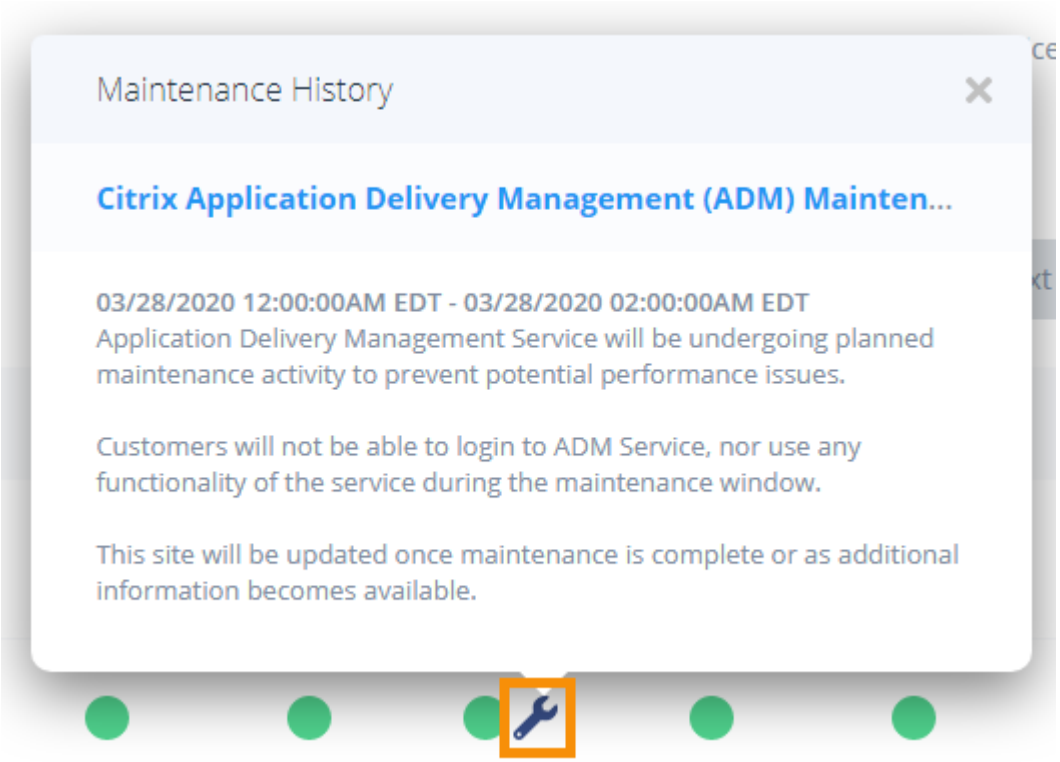
- État de disponibilité actuel de tous les services Citrix Cloud, regroupés par région géographique
- L'historique d'intégrité du service de chaque service pour les sept derniers jours (par défaut) ou pour les incréments de sept jours précédents
- Fenêtres de maintenance pour des services spécifiques

Par défaut, l'état d'intégrité du service est affiché sous la forme d'une liste, mais vous pouvez également l'afficher dans une vue de calendrier. Sélectionnez **Suivant** ou **Précédent** pour faire défiler l'historique d'intégrité du service par incréments de sept jours. Vous pouvez également filtrer la liste pour afficher uniquement les services concernés.

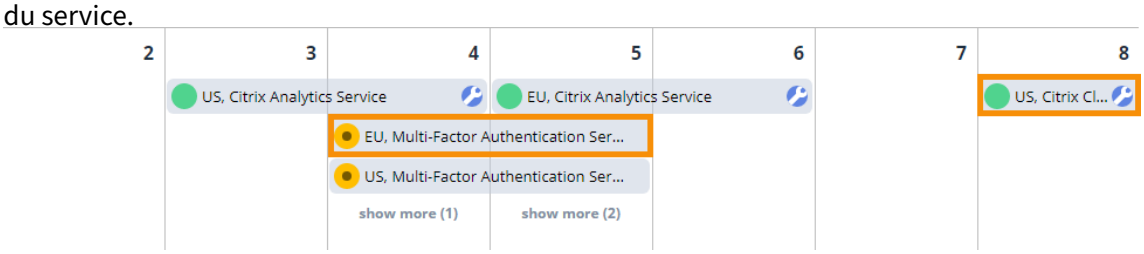


Pour afficher des informations plus détaillées sur l'incident de santé du service pour un service concerné :

- Dans la vue Liste, cliquez sur l'icône en regard de l'indicateur de service pour afficher des informations plus détaillées sur l'incident d'intégrité du service.

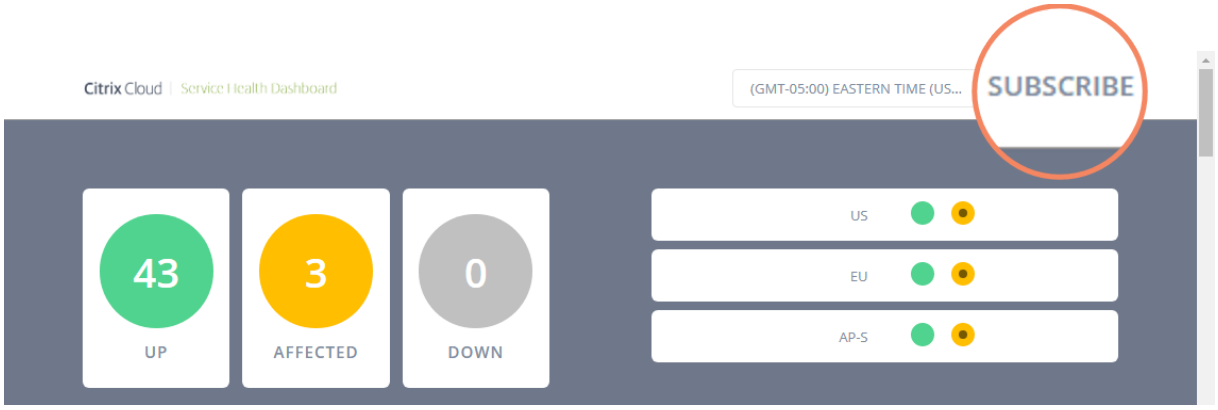


- Dans la vue Calendrier, cliquez sur l'entrée de service pour afficher l'état de l'incident d'intégrité du service.

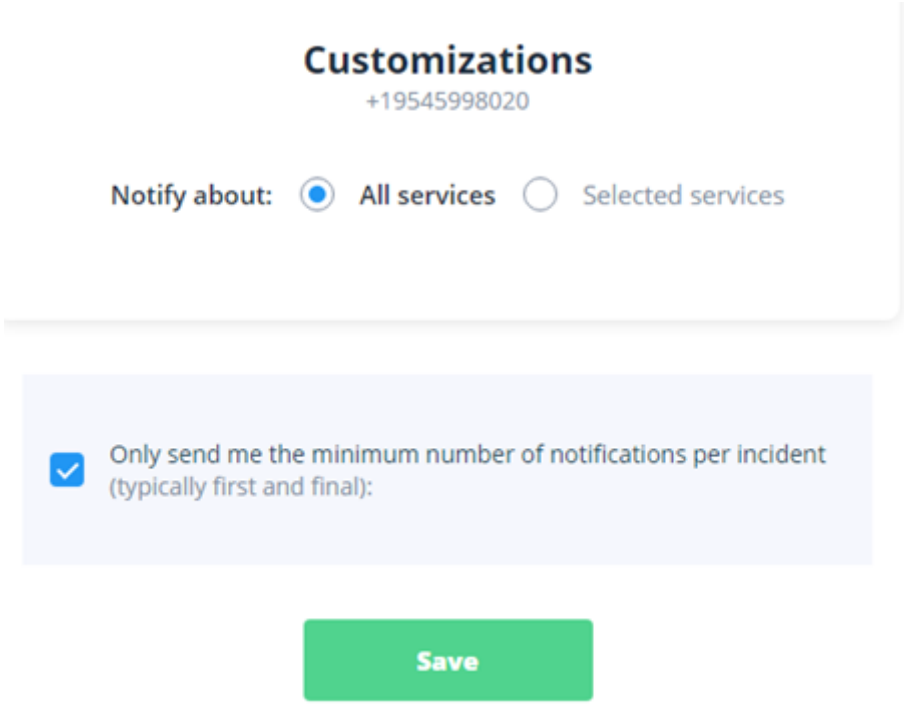


Abonnements à l'intégrité du service

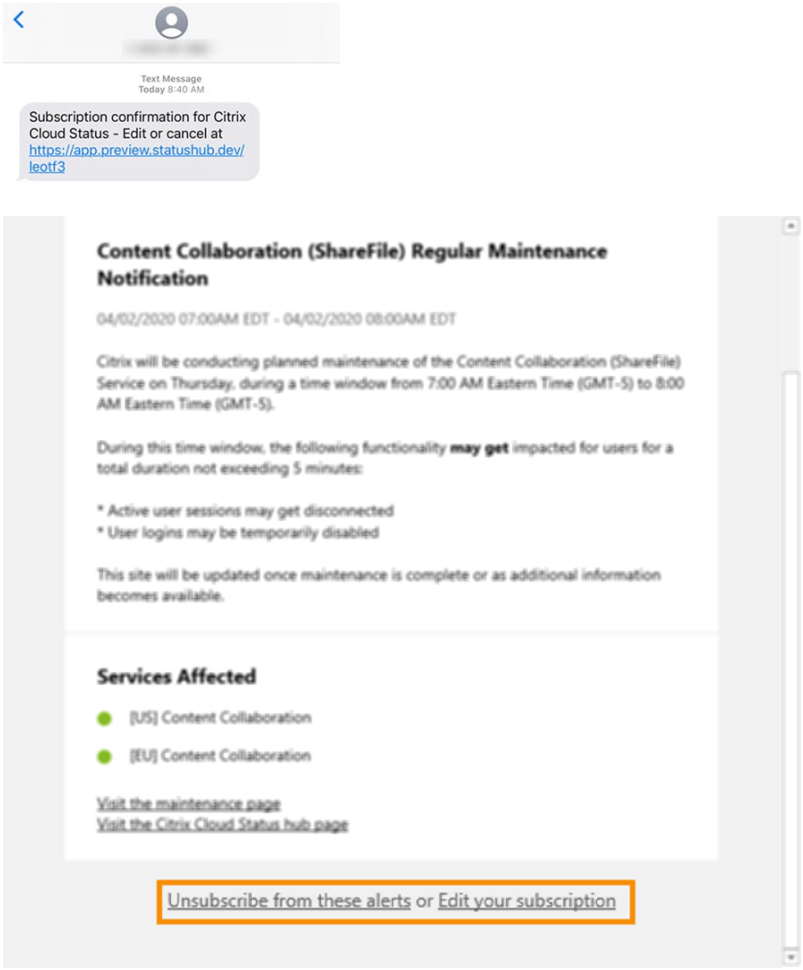
Pour recevoir des notifications d'intégrité du service, cliquez sur **S'abonner** dans l'angle supérieur droit du tableau de bord et sélectionnez la méthode de notification que vous souhaitez utiliser.



Vous pouvez vous abonner aux notifications pour tous les services ou uniquement les services que vous sélectionnez. Par défaut, vous recevez toutes les notifications pour un incident d'intégrité du service. Pour limiter la fréquence des notifications lors d'un incident, vous pouvez choisir de ne recevoir que la première et la dernière notification.



Selon la méthode d'abonnement, des liens vers la désinscription et la modification de vos préférences sont inclus dans le message de confirmation d'abonnement que vous recevez (par exemple, lorsque vous vous abonnez à des notifications téléphoniques) ou dans chaque message de notification (par exemple, lorsque vous vous abonnez à des notifications par e-mail).



Pour vous désabonner ou modifier vos préférences d'abonnement :

1. Recherchez une notification existante et sélectionnez le lien pour vous désabonner ou modifier vos préférences de notification.
2. Si vous vous désabonnez, sélectionnez **Se désabonner**, puis sélectionnez la méthode de notification que vous souhaitez annuler. Pour vous abonner à partir de toutes les méthodes de notification, sélectionnez **Supprimer tous les abonnements**.
3. Si vous modifiez les préférences, sélectionnez la méthode de notification, apportez les modifications appropriées aux services et aux notifications d'incident minimales, puis sélectionnez **Enregistrer**.

Intégration à faible contact des instances Citrix ADC à l'aide du service Citrix ADM connect

April 29, 2021

Au fur et à mesure que votre infrastructure hybride multicloud (HMC) se développe, les défis de gestion, de surveillance, d'analyse et de dépannage des instances ADC deviennent multiples. Un contrôleur centralisé offrant une visibilité sur votre infrastructure complète et toutes les applications qui s'exécutent sur elle devient le besoin de l'heure.

Dans le monde d'aujourd'hui, l'intégration de vos instances à un contrôleur central doit se faire de manière rapide, facile et à faible contact. En gardant ce besoin à l'esprit, le service Citrix ADM lance un nouveau flux de travail d'intégration, qui vous offre un moyen plus rapide d'obtenir une visibilité complète sur votre déploiement HMC.

Vue d'ensemble : composants du flux de travail d'intégration des services ADM

Les éléments constitutifs de ce flux de travail sont deux composants côté CAN : ADC service connect et Call Home.

- **Connexion au service ADM** : il s'agit d'une nouvelle fonctionnalité d'ADC qui permet l'intégration transparente des instances Citrix ADC sur le service Citrix ADM. Cette fonctionnalité permet à l'instance Citrix ADC de se connecter automatiquement au service Citrix ADM et d'envoyer des données système, d'utilisation et de télémétrie au service ADM. Sur la base de ces données, le service Citrix ADM vous fournit des informations et des recommandations sur votre infrastructure Citrix ADC. Comme l'identification rapide des problèmes de performance, l'utilisation élevée des ressources et les erreurs critiques.

  La connexion du service ADM est disponible sur les versions ADC suivantes :

  - Citrix ADC MPX et VPX image version 12.1 57.18 et versions ultérieures et 13.0 61.48 et ultérieures. Pour de plus amples informations, consultez la section Présentation du service Citrix ADM connect pour les appliances Citrix ADC.
  - Image de version Citrix ADC SDX 12.1 58.14 et versions ultérieures et 13.0 61.48 et ultérieures. Pour de plus amples informations, consultez la section Présentation du service Citrix ADM connect pour les appliances Citrix ADC SDX.

- **Call Home** : il s'agit d'une fonctionnalité existante dans ADC, qui surveille périodiquement les instances et télécharge automatiquement les données vers le serveur de support technique Citrix. Pour plus de détails, consultez Call Home. Les données collectées par Call Home sont également acheminées vers le service ADM pour activer ce nouveau flux de travail.

Toutes les instances ADC avec connectivité Internet ou Call Home, ou les instances activées avec la connexion du service ADM sont connectées au service ADM. Le service ADM commence à collecter les mesures pertinentes à partir de ces instances ADC via la route Call Home, la route de connexion du service ADM, ou les deux. Pour plus d'informations, veuillez consulter Gouvernance des données pour les instances MPX et VPX et Gouvernance des données pour les instances SDX.

À l'aide de ces données, le service ADM crée un inventaire des instances ADC pour chaque client (ID d'organisation unique), qui affiche une liste consolidée de vos instances ADC. Le service ADM utilise également ces données pour créer des informations sur vos instances ADC et Gateway, qui fournissent des informations utiles sur vos déploiements HMC, identifient les problèmes et recommandent des mesures pour les atténuer. Avant de pouvoir atténuer les problèmes, vous devez embarquer les instances ADC au service ADM.
Vous pouvez cocher **Sélectionner les instances ADC et passerelle à** intégrer et sélectionner les instances ADC que vous souhaitez intégrer au service ADM. Après avoir commencé, vous êtes guidé vers le processus d'intégration.

Le processus d'intégration automatique utilise ADM service connect, ce qui rend l'expérience automatisée, transparente et plus rapide. Pour les instances ADC sur des versions qui ne prennent pas en charge la connexion et l'intégration automatique du service ADM, le service ADM fournit l'intégration basée sur des scripts, qui est un processus semi-automatisé.

> **Remarque**
>
> L'intégration automatique et basée sur des scripts utilisent un agent intégré. Toutefois, ce flux de travail vous donne également la possibilité d'utiliser un agent externe pour l'intégration. Vous pouvez utiliser l'intégration basée sur un agent externe si vous souhaitez utiliser les licences groupées ou la suite analytique complète dans le service ADM. Ou si vous souhaitez utiliser les licences groupées et la suite analytique complète. L'agent intégré prend uniquement en charge la gestion et la surveillance.

Une visite rapide de l'intégration

Votre premier point de contact dans le parcours d'intégration est un e-mail initié par le produit. Voici un aperçu rapide du parcours d'intégration :

1. **E-mail initié par un produit Citrix** : vous recevez un e-mail du service ADM montrant quelques informations clés de votre infrastructure ADC et vous invitant à commencer avec le service ADM. Cliquez sur le lien fourni dans l'e-mail.
2. **Page de connexion Citrix Cloud** : vous devez vous connecter à Citrix Cloud à l'aide de vos informations d'identification **My Citrix** .
3. **Page d'accueil du service Citrix ADM** : vous obtenez une vue d'ensemble du service ADM et de ses avantages.
4. **Informations sur vos instances ADC et Gateway** : vous obtenez des informations détaillées sur votre infrastructure ADC globale, y compris des conseils sur la sécurité (conseils sur les CVE actuels de Citrix), des conseils de mise à niveau (conseils basés sur les calendriers EOM/EOL), des mesures clés, des tendances et des problèmes affectant les performances d'ADC et santé et recommande un moyen d'atténuer les problèmes.

5. **Sélectionnez les instances ADC et Gateway à**intégrer : vous obtenez une vue consolidée de votre inventaire ADC. Vous pouvez sélectionner les instances ADC que vous souhaitez utiliser pour le service ADM.
6. **Instances ADC embarqués à ADM** : en fonction des instances ADC sélectionnées pour l'intégration, ADM vous guide dans le processus d'intégration. Par défaut, l'agent intégré est sélectionné pour l'intégration automatique.
7. Tableau de**bord de l'interface graphique ADM** : une fois l'intégration terminée, vous êtes guidé vers le tableau de bord des instances ADM.

> **Remarque**
>
> Ce flux de travail est déployé (GA) de manière progressive, via la version canari. Vous recevez un e-mail lorsque cette fonctionnalité est disponible dans votre environnement de service ADM.

Pour plus de détails sur chacune de ces méthodes d'intégration, reportez-vous à la section Instances Citrix ADC embarqués à l'aide de la connexion du service Citrix ADM.

Instances Citrix ADC embarqués à l'aide de la connexion du service Citrix ADM

April 29, 2021

Vous trouverez ci-dessous un guide étape par étape pour vous aider à démarrer avec le service ADM. Avant de commencer, lisez comment le service Citrix ADM lance un nouveau flux de travail d'intégration, qui vous offre un moyen plus rapide d'obtenir une visibilité complète sur votre déploiement multicloud hybride (HMC). Consultez Intégration à faible contact des instances Citrix ADC à l'aide du service Citrix ADM connect.

Étape 1 : Commencez

Vous recevez un courriel de la part du service ADM montrant quelques informations clés de votre infrastructure ADC et vous invitant à commencer avec le service ADM.

citrix

Security and Upgrade Advisory with Citrix ADM service

Hello [redacted],

Org ID - [redacted]

As a valued Citrix customer, your application delivery infrastructure security is our top concern. To help keep your infrastructure secure, we just launched **security advisory and upgrade advisory** for your Citrix ADCs as part of Citrix ADM service.

These new features will identify outdated software deployed in your ADC fleet, notify you of known vulnerabilities in these releases, and suggest steps you can take to remediate these issues.

Below, you'll see a preview of these advisories and other key insights customized to your infrastructure. More information and recommended actions are available when you get started with Citrix ADM service for free.

Top insights on your ADC & Gateway infrastructure

These insights are based on data provided via Call Home and/or Citrix ADM service connect.

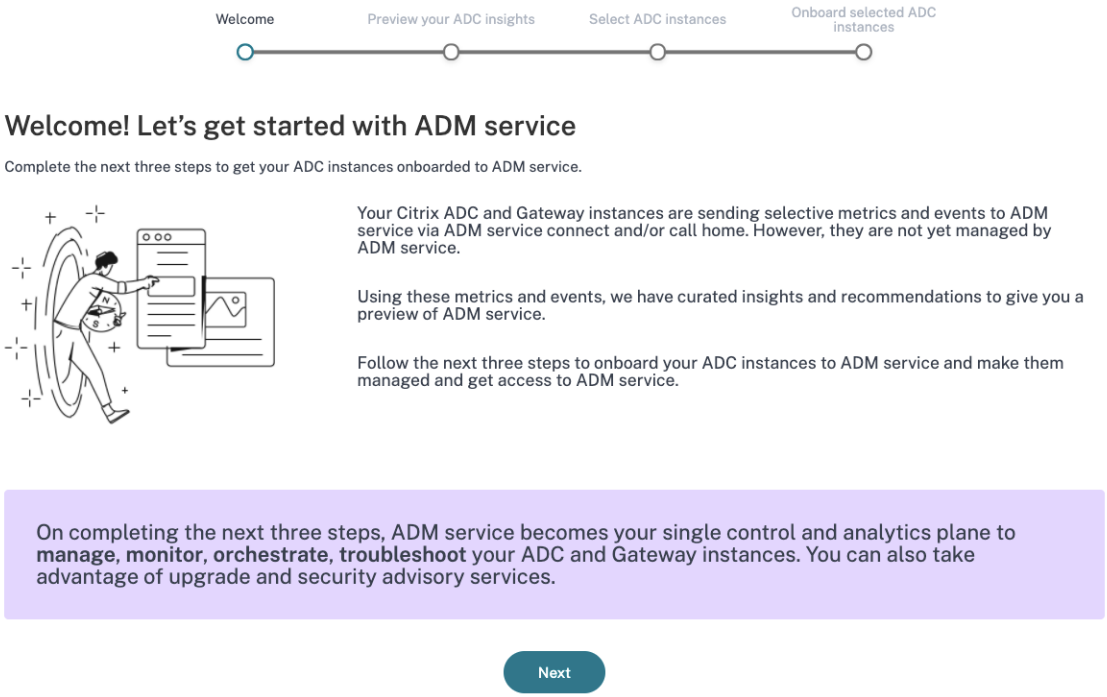
ADC instances by platforms

101	101	0	0
Total	VPX	SDX	MPX

Security Advisory	**101 ADC** instances are on versions with known common vulnerability exposures (CVEs). *This advisory is based on ADC build version scan only & more conclusive & exhaustive security advisory insights can be seen after onboarding all your ADCs to ADM Svc*
Upgrade Advisory	**101 ADC** instances are on older builds and releases.
ADC deployment	**1 ADC** instance is not deployed as High Availability (HA) pair. Citrix ADM recommends HA pair for production ADC instances.
Recent events	No critical events reported on any ADC.
Resource utilization	All ADC instances have CPU usage < 50% All ADC instances have memory usage < 50%

To get more details and recommendations on these insights, **onboard your ADC instances to Citrix ADM service today.**

1. Dans l'e-mail, cliquez sur **Démarrer** pour lancer le processus d'intégration.
2. Connectez-vous à Citrix Cloud à l'aide de vos informations d'identification My Citrix/Citrix Cloud.
3. Dans la page de destination du service Citrix ADM, prenez un moment pour lire pourquoi vous êtes là et les avantages de l'utilisation d'ADM.



4. Cliquez sur **Suivant**. La page **Insights sur vos instances ADC et Gateway** s'ouvre.

Les étapes suivantes agissent comme un flux de travail guidé pour vous donner un aperçu de ce qu'ADM peut offrir et vous aider à intégrer vos instances ADC au service ADM en toute transparence.

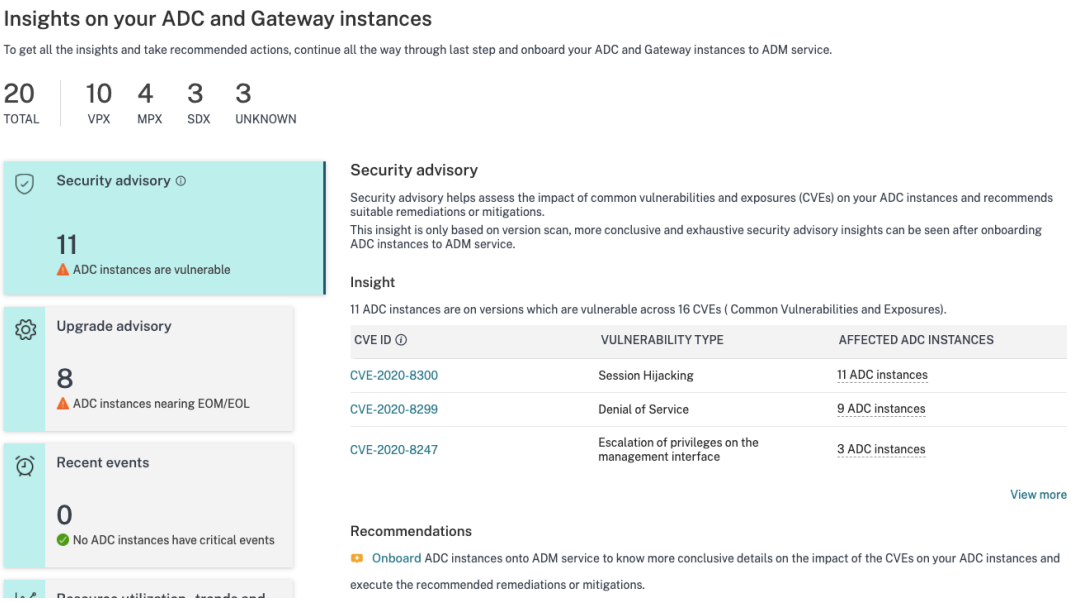
Étape 2 : Informations sur vos instances ADC et Gateway

Cette page d'informations utilise les données collectées par le biais du service Call Home ou ADM Service Connect, ou les deux services Call Home et ADM se connectent pour fournir des informations sur vos instances ADC. Cette page vous donne des informations sur votre infrastructure ADC globale, y compris des conseils sur la sécurité (conseils sur les CVE Citrix actuels), des conseils de mise à niveau (conseils basés sur les calendriers EOM/EOL), des mesures clés, des tendances, et met en évidence les problèmes affectant les performances et l'intégrité des ADC, et vous recommande des moyens d'atténuer les problèmes. Ces informations et recommandations ne constituent qu'un petit aperçu de la pléthore d'avantages et de valeur ajoutée que le service ADM a à offrir. Pour obtenir de nombreux avantages, des informations détaillées et être en mesure d'exécuter les actions recommandées, vous devez embarquer les instances ADC dans ADM.

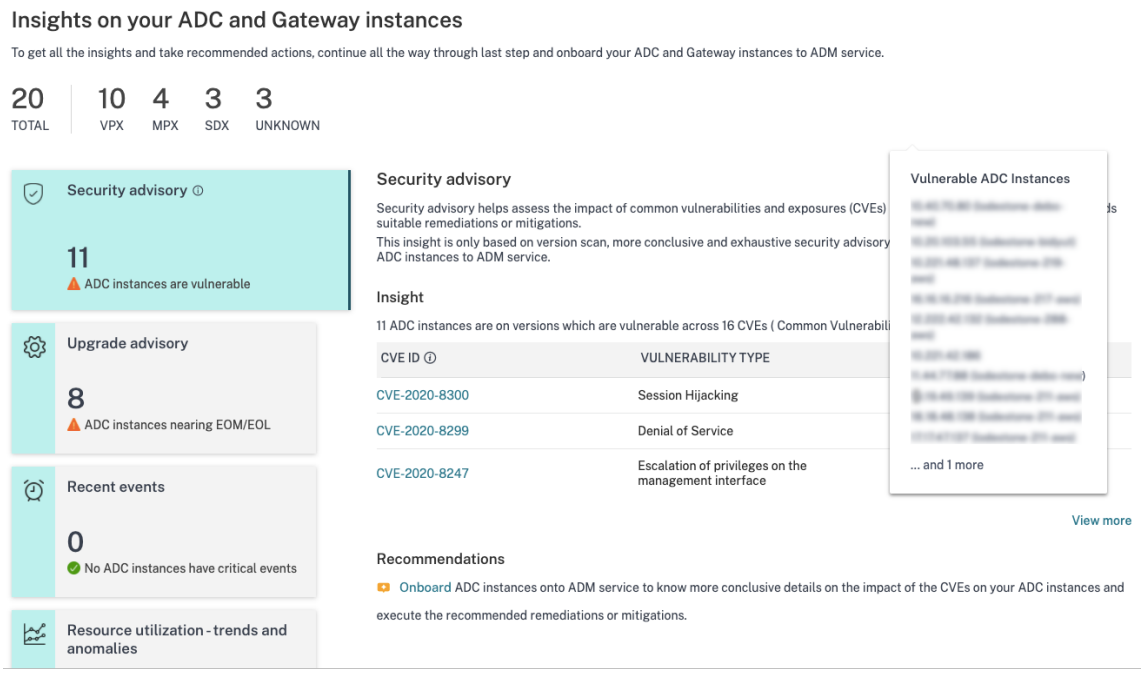
Les points de vue et les recommandations sont classés dans les catégories suivantes :

- **Avis de sécurité** : Instances ADC embarquées pour obtenir les détails de l'impact CVE sur vos instances ADC et exécuter les correctifs ou les mesures d'atténuation recommandées.
- **Avis de mise à niveau** : les instances ADC intégrées sur ADM et mettez à niveau vos instances ADC qui ont atteint ou atteignent EOM/EOL ou qui sont sur des versions plus anciennes.
- **Événements récents** : des instances ADC embarqués à ADM pour surveiller plus de 200 événements sur une base régulière, et créer des règles pour recevoir des notifications par e-mail, PagerDuty, Slack, ServiceNow, prendre les mesures appropriées.
- **Utilisation des ressources - tendances et anomalies** : Instances ADC intégrées à ADM pour obtenir une vue complète de l'état des instances ADC, des problèmes de performances et des recommandations pour atténuer ces problèmes. Vous pouvez également évaluer l'utilisation prévue du processeur et de la mémoire pour vos instances ADC.
- **Conseils de déploiement ADC** : les instances ADC embarqués vers ADM et les configurer en tant que paire HA, à l'aide des travaux de configuration sur ADM.

1. **Avis de sécurité** : Citrix ADM Security Advisory vous avertit des vulnérabilités mettant vos instances ADC en danger et recommande des mesures d'atténuation et des correctifs. Vous pouvez vérifier l'ID CVE, le type de vulnérabilité et les instances ADC affectées. Le lien de l'ID CVE mène à l'article du bulletin de sécurité.



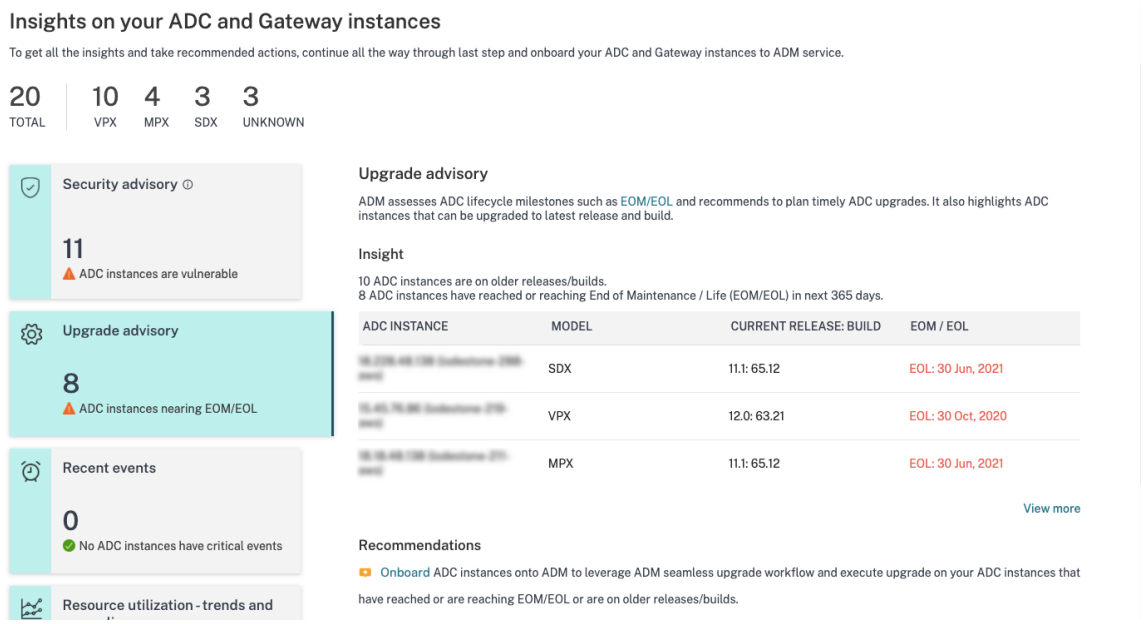
La recommandation vous guide à embarquer vos instances ADC au service ADM pour obtenir plus de détails sur l'impact CVE sur vos instances ADC et exécuter les mesures d'atténuation ou de correction recommandées. Cliquez sur les instances ADC affectées pour afficher les adresses IP des instances concernées.



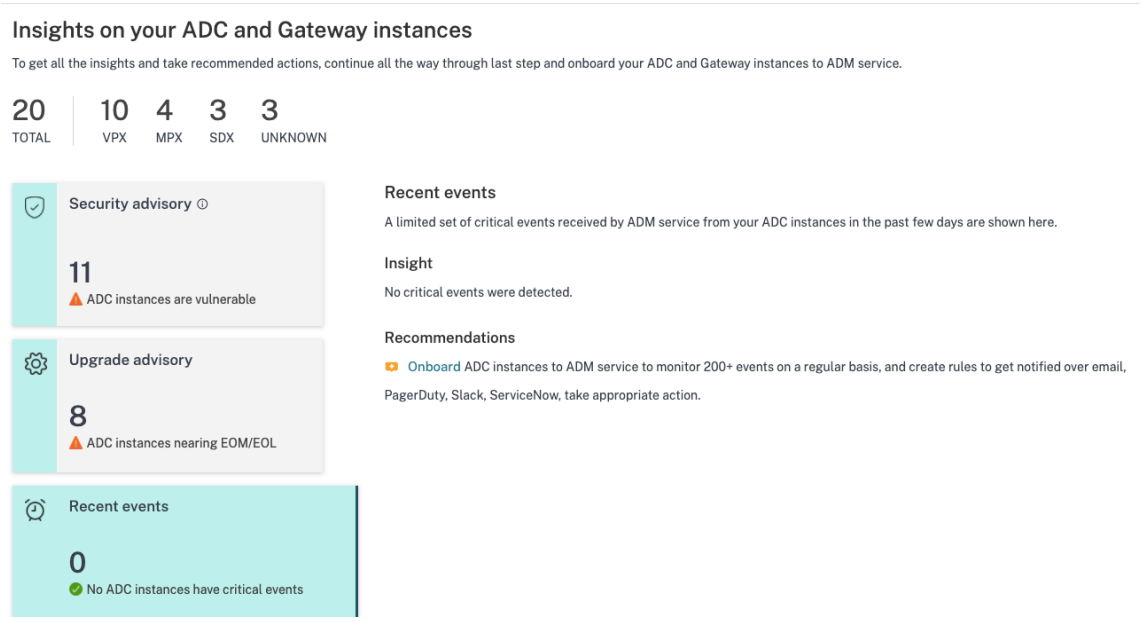
2. **Avis de mise**à niveau : Utilisez cet avis pour vérifier quelles instances ADC approchent EOM/EOL ou sont sur des versions plus anciennes.

   Sur la base de ces informations, ADM vous recommande de planifier une mise à niveau rapide avant EOM/EOL ou de bénéficier des dernières fonctionnalités et correctifs.

   Pour effectuer la mise à niveau, vous devez embarquer vos instances ADC vers le service ADM.

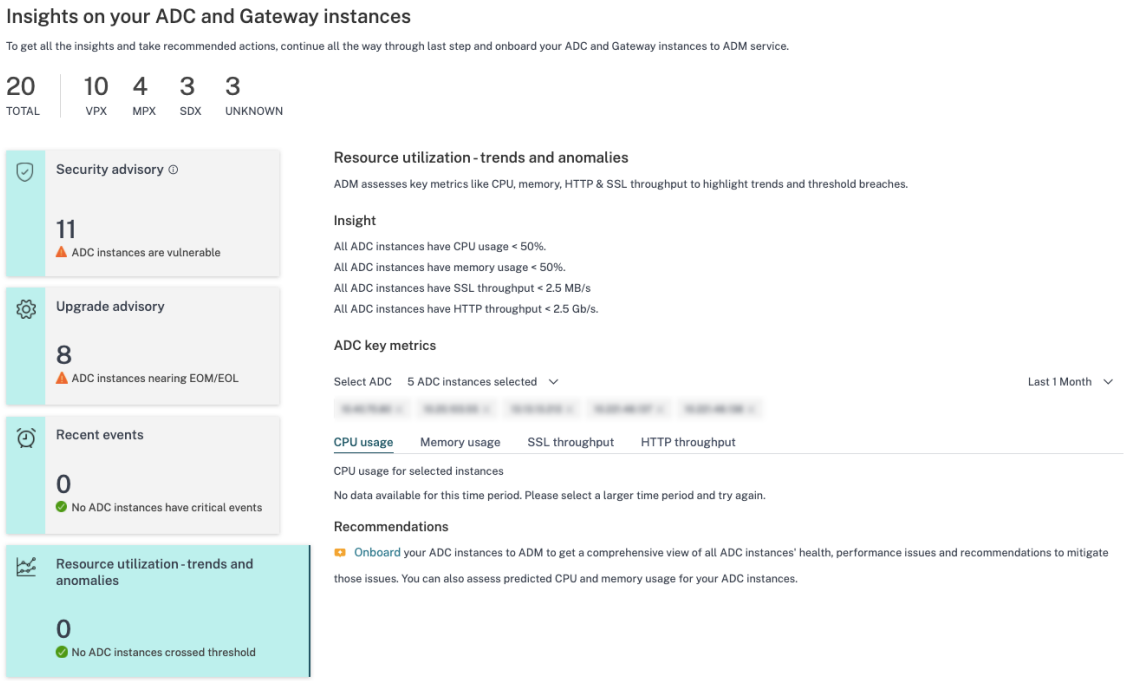


3. **Événements récents** : Obtenez des détails sur certaines erreurs critiques qui se sont produites sur les instances ADC et une liste des instances ADC sur lesquelles les erreurs se sont produites.

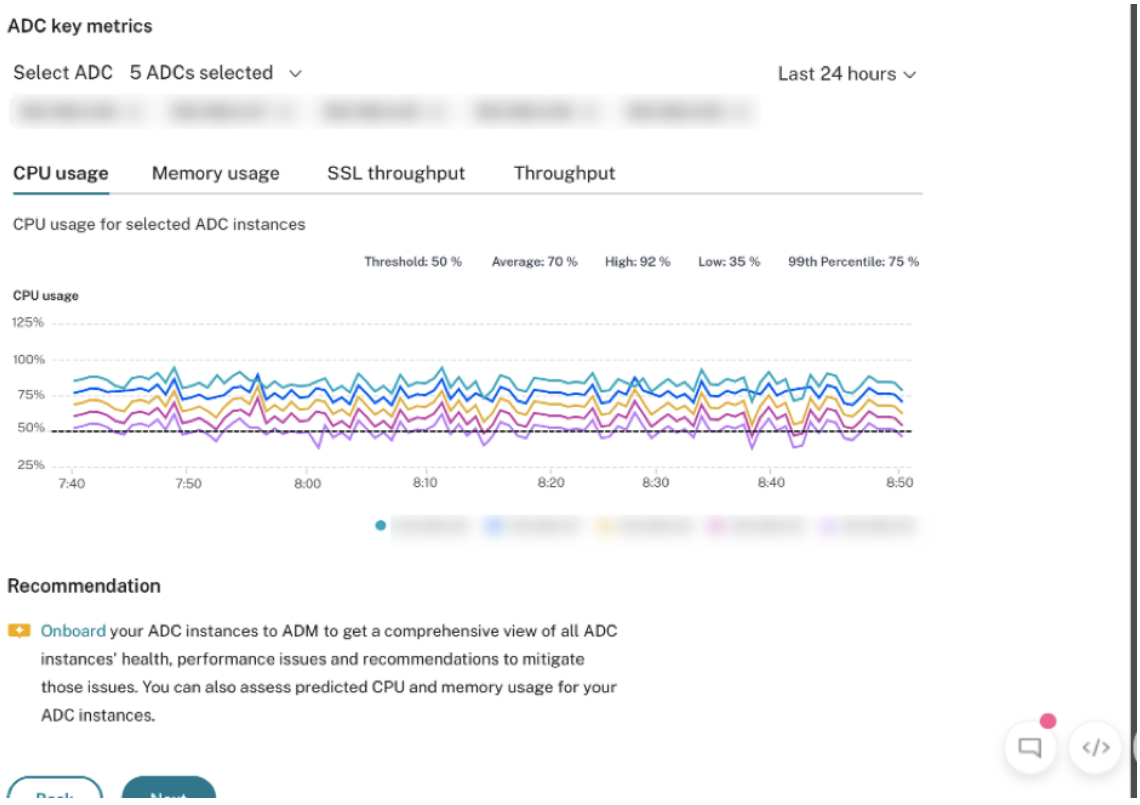


4. **Utilisation des ressources - tendances et anomalies** : trouvez des informations sur l'utilisation élevée des ressources pour le processeur, la mémoire, le débit HTTP et le débit SSL. Pour chaque point de vue, le SMA suggère des mesures recommandées. Pour avoir plus de visibilité sur ces informations et recommandations, vous devez intégrer vos instances ADC dans ADM. Quelques avantages après l'intégration sont les suivants :

    - Processeur : prédire l'utilisation du processeur pour les prochaines 24 heures sur ADM.
    - Mémoire : prédire l'utilisation de la mémoire pour les 24 prochaines heures sur ADM.
    - Débit SSL : visualisez l'optimisation en temps réel SSL avec des analyses d'applications intelligentes sur ADM.
    - Débit HTTP : Résoudre les problèmes de capacité de débit ADC avec Infrastructure Analytics.

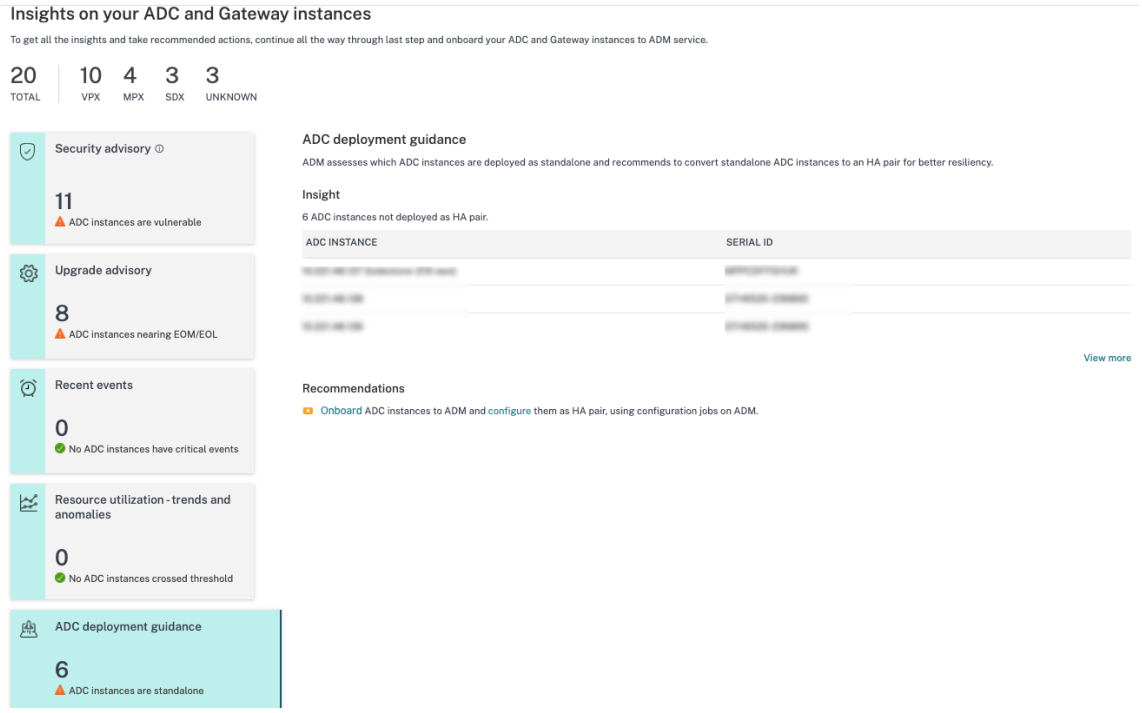


- **Mesures clés** : Obtenez des détails sur les mesures clés liées au processeur, à la mémoire, au débit HTTP, au débit SSL, et décelez les tendances anormales des mesures.



5. **Conseils de déploiement** : Bénéficiez d'une visibilité sur les instances ADC déployées en tant qu'ADC autonome. ADM recommande de configurer ces instances ADC en tant que paire HA

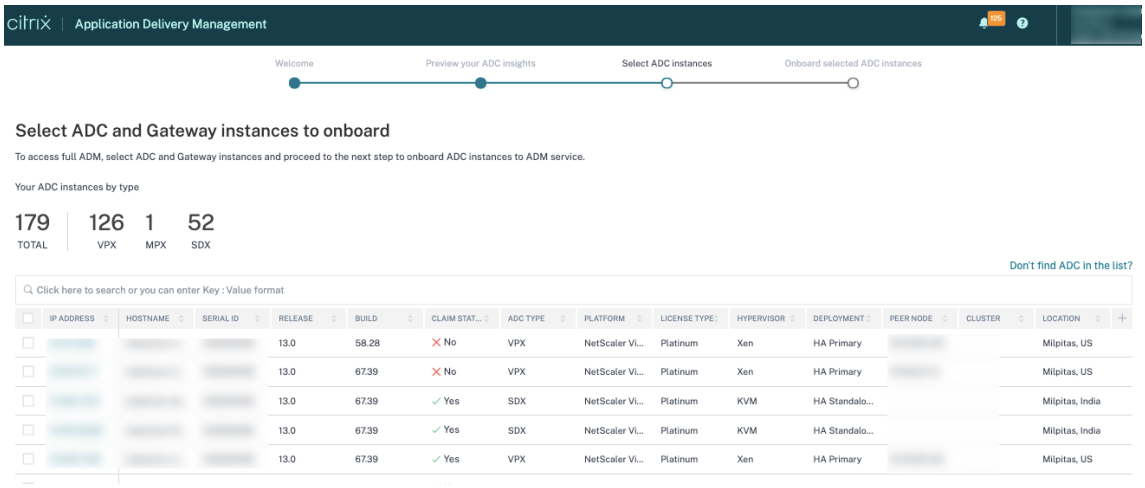
pour une meilleure résilience. Pour cela, vous devez embarquer vos instances ADC dans ADM, puis utiliser les tâches de maintenance pour configurer les instances en tant que paire HA.



Étape 3 : Sélectionner les instances ADC et Gateway à intégrer

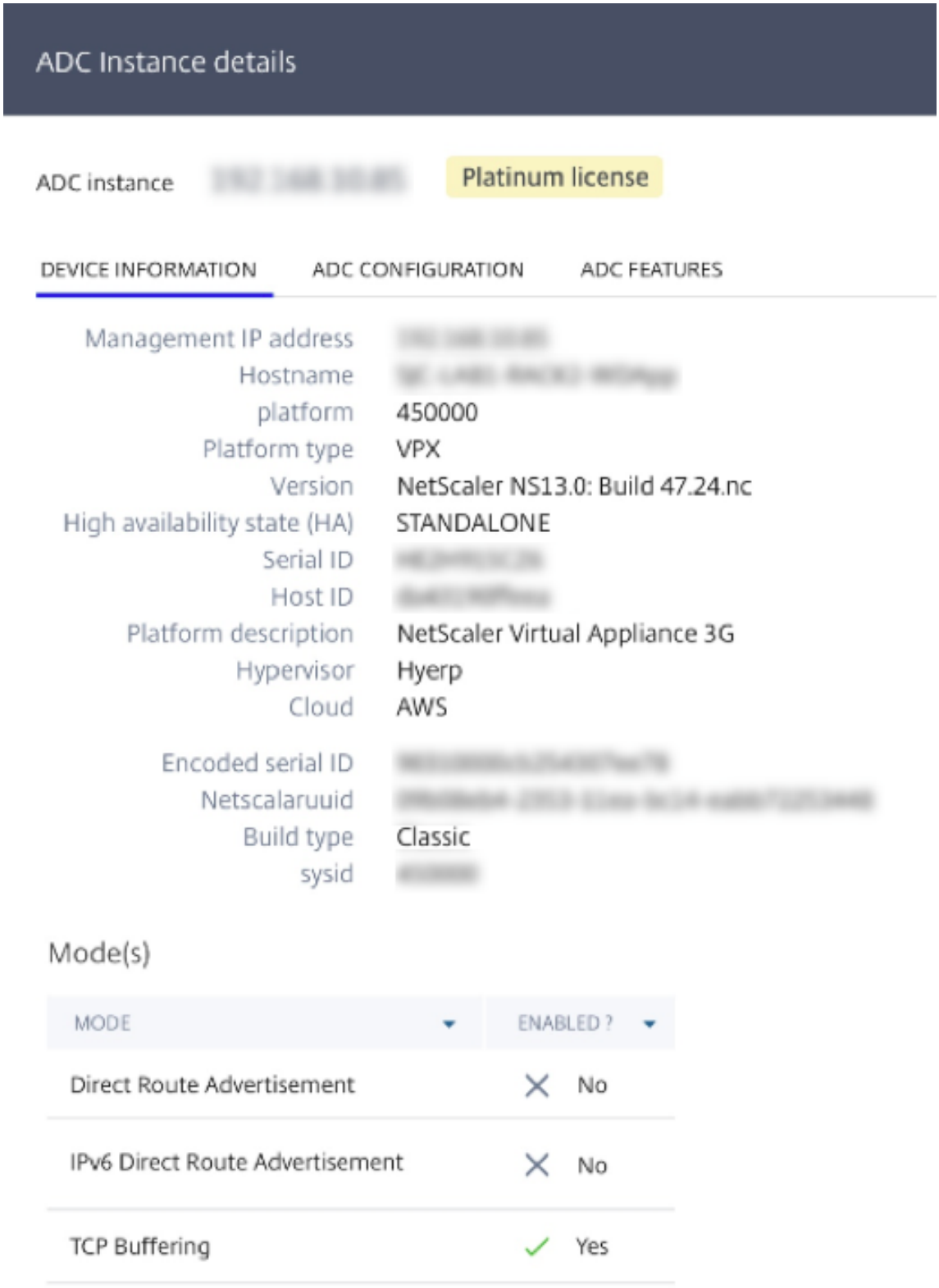
Cette page affiche toutes les instances ADC et Gateway de votre environnement. Affichez et sélectionnez les instances ADC et Gateway que vous souhaitez intégrer au service ADM, puis cliquez sur **Suivant**.

1. Affichez et sélectionnez les instances ADC que vous souhaitez embarquer au service ADM.

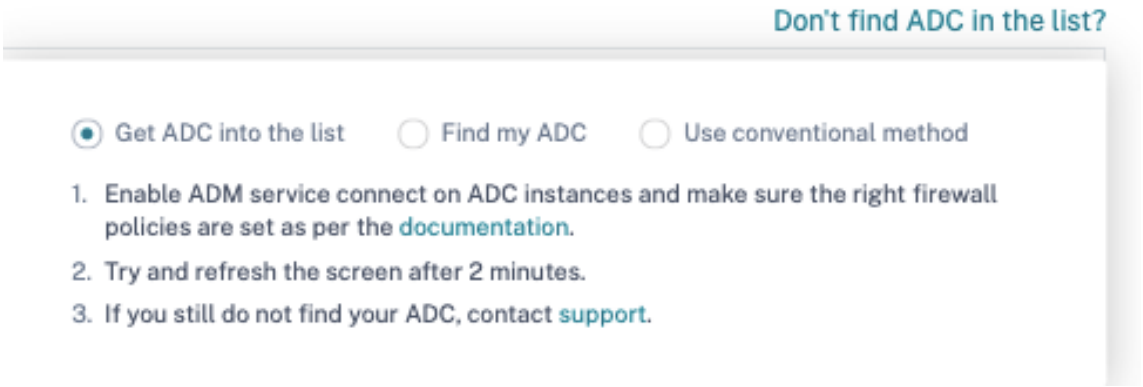


Si vous avez besoin de détails sur une instance telle que des informations sur le périphérique, la configuration de l'ADC, les fonctionnalités ADC disponibles ou les informations de licence,

cliquez sur l’adresse IP de l’instance sous l’instance ADC.

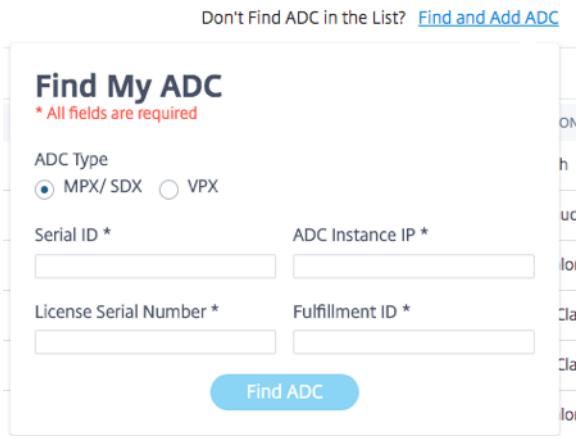


Si votre instance n'est pas répertoriée, utilisez l'option **Ne trouvez pas ADC dans la liste** située dans le coin supérieur droit.



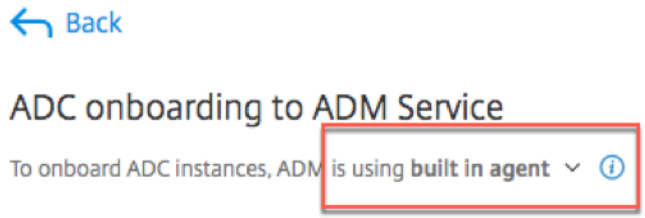
Vous pouvez procéder de trois façons : suivez les étapes indiquées sous **Get ADC dans la liste** ou utilisez l' **option Localiser mon ADC**. Si ces deux étapes ne vous aident pas, cliquez sur **Utiliser l'option méthode conventionnelle**, qui saute le flux de travail et vous emmène à travers la manière traditionnelle d'intégration des instances ADC.

Pour l' **option Rechercher mon ADC**, entrez les détails dans les champs obligatoires (ID série, adresse IP de l'instance ADC, numéro de série de licence et ID de traitement) et recherchez.



Étape 4 : Instances ADC embarqués vers ADM

Vous pouvez embarquez vos instances à l'aide de l'agent intégré (option par défaut) ou d'un agent externe.



Instances ADC intégrées à l'aide d'un agent intégré

L'intégration automatique et par script utilise l'agent intégré, défini par défaut.

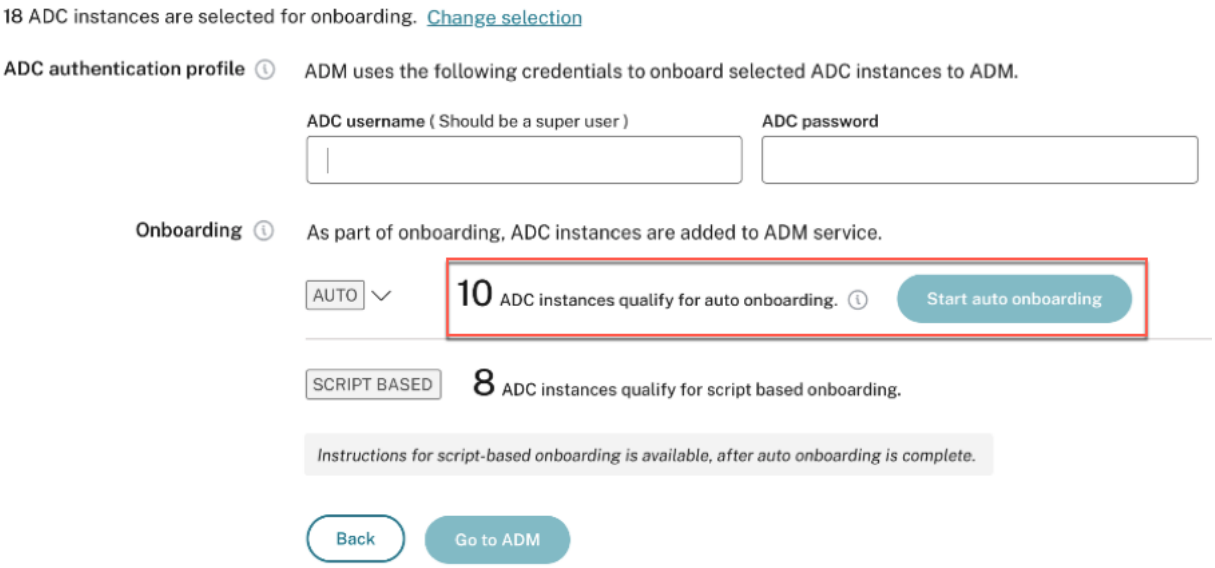
Auto-intégration : il n'est pris en charge que sur les versions ADC suivantes :

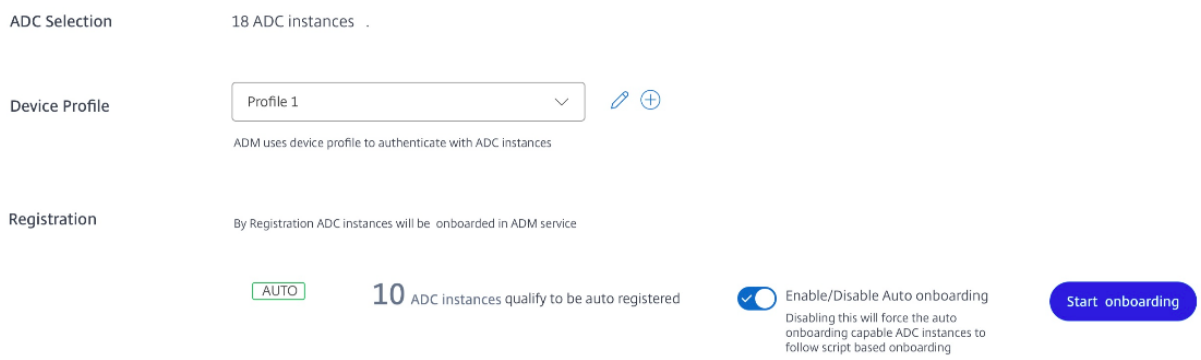
- Citrix ADC MPX et VPX image version 12.1 57.18 et versions ultérieures et 13.0 61.48 et ultérieures
- Version SDX image 13.0 61.48 et versions ultérieures et 12.1 58.14 et ultérieures

Pour sélectionner une autre instance ADC, cliquez sur **Modifier la sélection**.

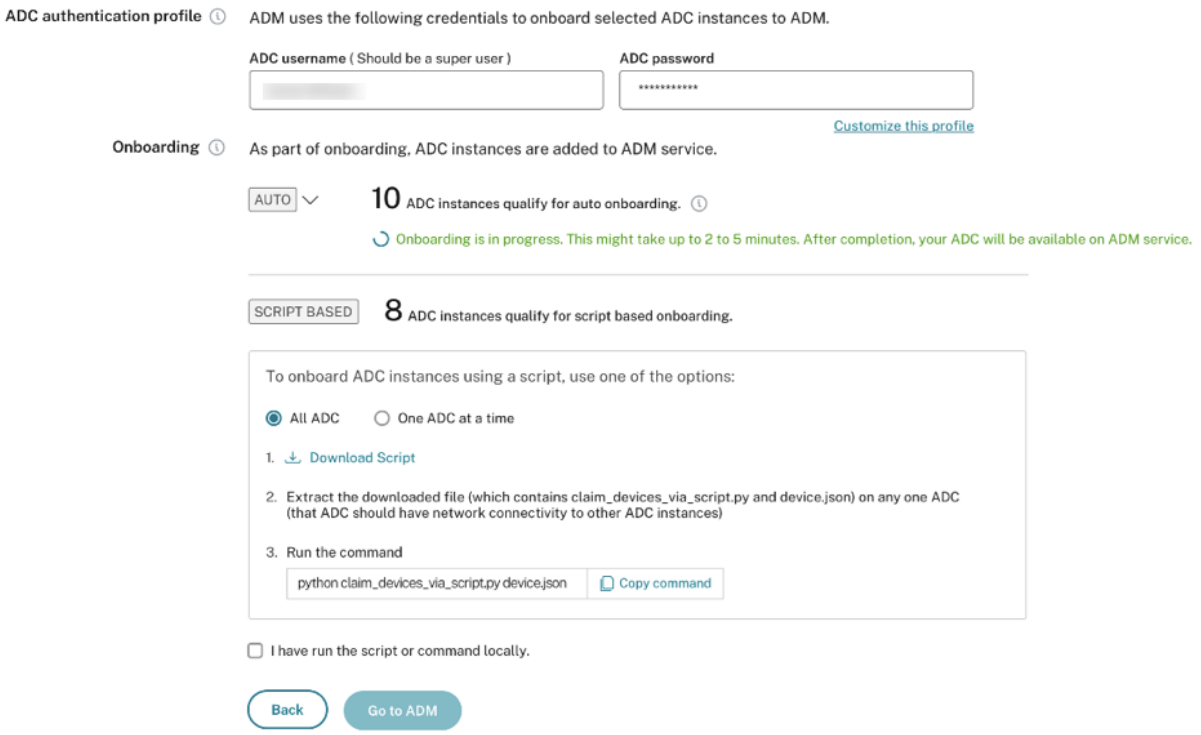
Sur le nombre total d'instances ADC sélectionnées, certaines instances peuvent être éligibles à l'intégration automatique (en fonction des critères de version minimum). Vous pouvez voir les instances qui remplissent les conditions d'intégration automatique.

Entrez le nom d'utilisateur et le mot de passe ADC. Ces informations d'identification doivent être des informations d'identification d'administrateur de l'utilisateur ADC, et ADM utilise ces informations d'identification pour embarquer ADC. Cliquez sur **Démarrer l'intégration pour embarquer** vos instances ADC sur ADM.





L'intégration automatique peut prendre jusqu'à 2 à 5 minutes.



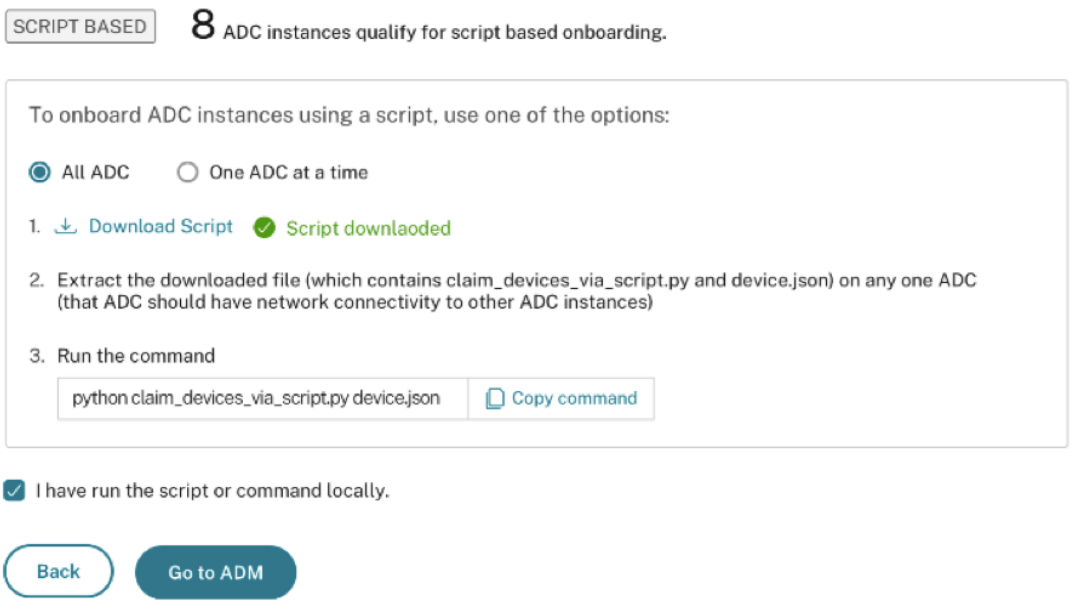
> **Remarque**
>
> Si vous ne souhaitez pas que les instances ADC s'embarquent automatiquement à ADM, vous pouvez désactiver l'intégration automatique et utiliser l'option basée sur les scripts pour l'intégration.

Intégration basée sur des scripts : une fois l'intégration automatique terminée, vous pouvez embarquer le reste des instances à l'aide de l'intégration basée sur des scripts. Utilisez l'une des options suivantes :

- **Option 1** : téléchargez le script, extrayez le fichier tar et exécutez-le sur l'une des instances ADC, à l'aide de la commande fournie sur l'interface utilisateur. Assurez-vous que l'instance ADC sur laquelle vous exécutez ce script dispose d'une connectivité réseau à toutes les autres instances

ADC sélectionnées.

- **Option 2** : Connectez-vous à la console CLI de chaque instance ADC et exécutez les commandes données sur l'interface utilisateur. Pour plus de détails, reportez-vous à l'étape 7 du document Configurer l'agent intégré ADC pour gérer les instances. Assurez-vous de générer un nouveau code d'activation unique pour chacune des instances ADC.

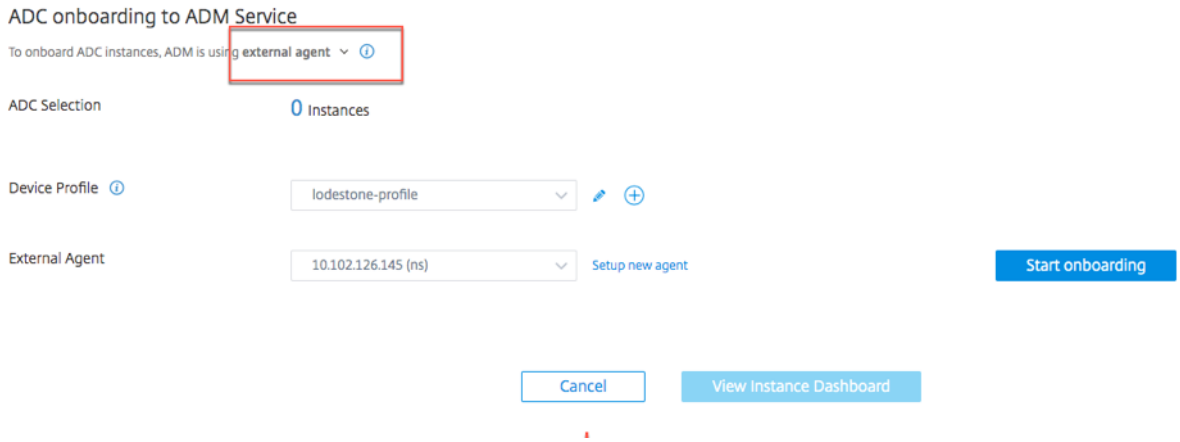


Après avoir intégré toutes vos instances, cliquez sur **Accéder à ADM** pour accéder au tableau de bord de l'interface utilisateur de gestion des instances ADM et explorer les différentes fonctionnalités.

> **Remarque**
>
> Si vous êtes un nouveau client sur le service ADM sans licence ADM, votre compte de service Citrix par défaut est un compte Express. Pour plus d'informations sur les droits de compte ADM, reportez-vous à la section Gérer les ressources Citrix ADM à l'aide du compte Express.

Instances ADC embarqués utilisant un agent externe

Vous pouvez utiliser l'intégration basée sur un agent externe si vous souhaitez utiliser des licences groupées ou la suite analytique complète dans le service ADM ou les deux utiliser les licences groupées et la suite analytique complète.



Procédez comme suit :

1. Sélectionnez un profil de périphérique.

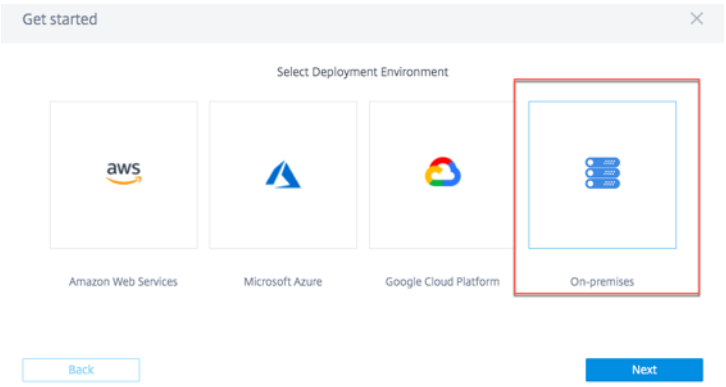
   > **Remarque**
   >
   > Pour des raisons de sécurité, vous ne pouvez pas utiliser les informations d'identification ADC par défaut (nsroot/nsroot) pour l'intégration.

2. Sélectionnez un agent externe et cliquez sur **Configurer un nouvel agent**.
3. Sélectionnez l'un des environnements suivants :

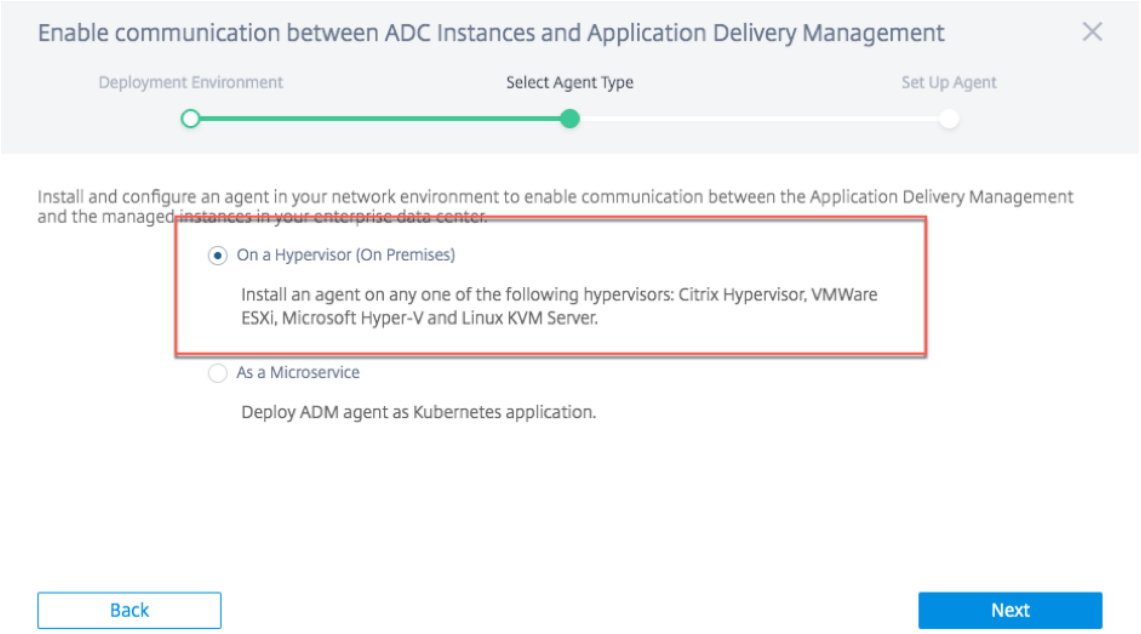
   - Amazon Web Services
   - Microsoft Azure
   - Plate-forme Google Cloud
   - Local

Installer un agent sur votre hyperviseur local

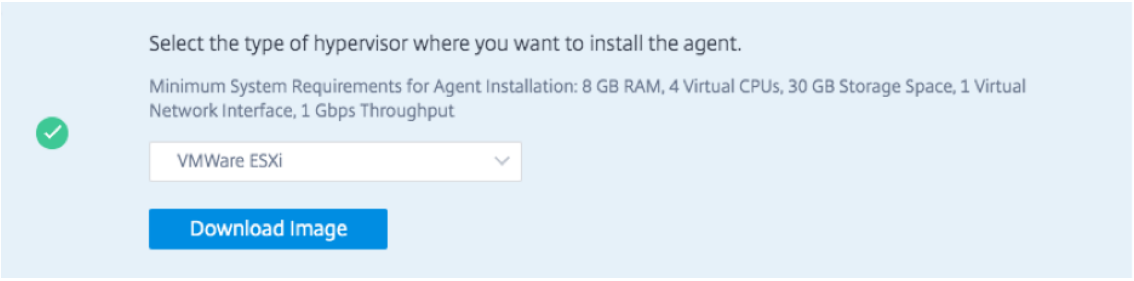
Si vous sélectionnez **Local**, vous pouvez installer l'agent sur les hyperviseurs suivants : Citrix Hypervisor, VMware ESXi, Microsoft Hyper-V, Linux KVM Server.



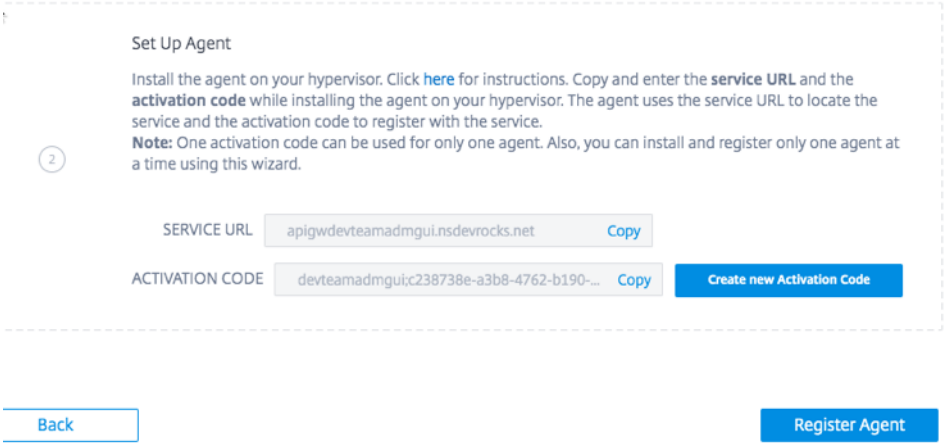
1. Sélectionnez **Sur un hyperviseur (sur site)** et cliquez sur **Suivant**.



2. Sélectionnez le type d'hyperviseur et téléchargez l'image, par exemple, VMware ESXi.



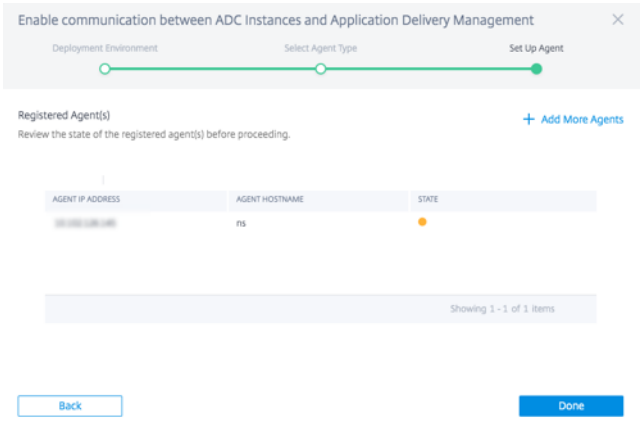
3. Utilisez l'URL du service et le code d'activation pour configurer l'agent.



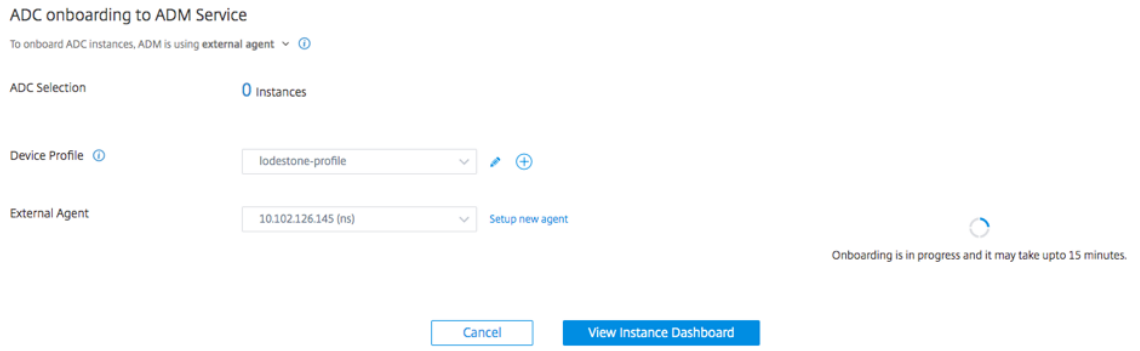
L'agent utilise l'URL du service pour localiser le service et le code d'activation pour s'inscrire auprès du service. Pour obtenir des instructions détaillées sur l'installation d'un agent sur votre

hyperviseur local, consultez Installer l'agent Citrix ADM sur site

4. Cliquez sur **Enregistrer l'agent**. Lorsque vous avez terminé, puis cliquez sur **Terminé** pour revenir à la page du service ADC d'intégration ADC.



5. Cliquez sur **Démarrer l'intégration**. Après avoir intégré toutes vos instances, cliquez sur **Afficher le tableau de bord des instances pour accéder au tableau** de bord de l'interface utilisateur de gestion des instances ADM et explorer les différentes fonctionnalités.



Installer un agent sur un nuage public

Vous pouvez installer l'agent dans l'un des environnements cloud suivants :

- Amazon Web Services
- Microsoft Azure
- Plate-forme Google Cloud

Pour plus d'informations, consultez les documents suivants :

- Installer l'agent Citrix ADM sur le cloud Microsoft Azure
- Installer l'agent Citrix ADM sur AWS
- Installer l'agent Citrix ADM sur GCP

Transition d'un agent intégré à un agent externe

April 29, 2021

Vous avez peut-être commencé à utiliser le service ADM à des fins de gestion et de surveillance uniquement, et ultérieurement, vous pouvez utiliser d'autres fonctionnalités telles que les licences groupées et l'analyse. Pour cela, vous devez passer de l'agent de service ADM intégré à un agent externe.

L'agent intégré prend uniquement en charge les fonctions de gestion et de surveillance ADM. Pour d'autres fonctionnalités ADM telles que les licences et les analyses groupées, vous avez besoin d'un agent externe. Ce document décrit les étapes de la transition d'un agent intégré ADM existant vers un agent externe basé sur un hyperviseur.

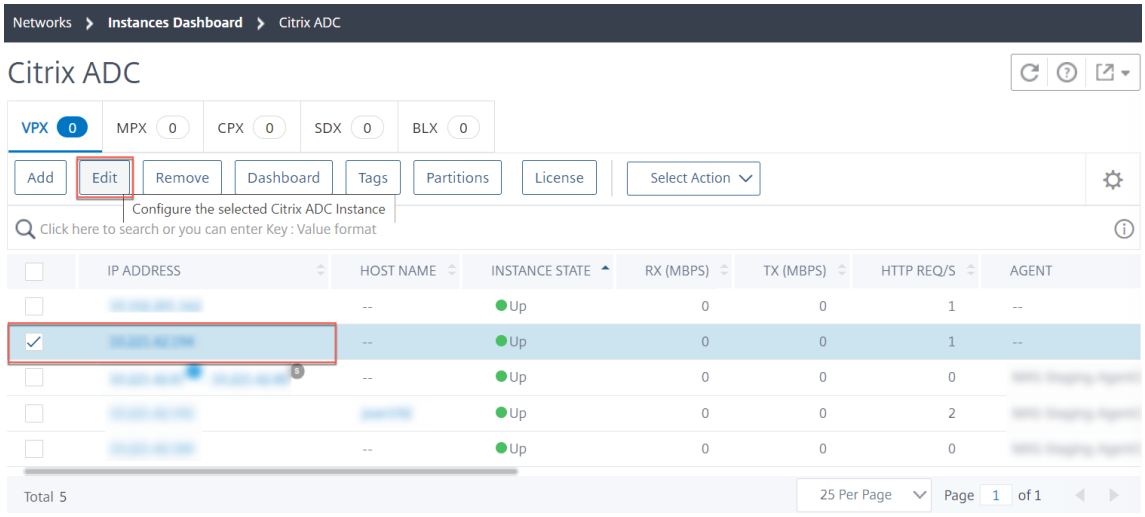
Avant de commencer

Installez un agent externe avant de commencer la transition. Suivez la procédure indiquée dans la rubrique Installer l'agent Citrix ADM sur site.

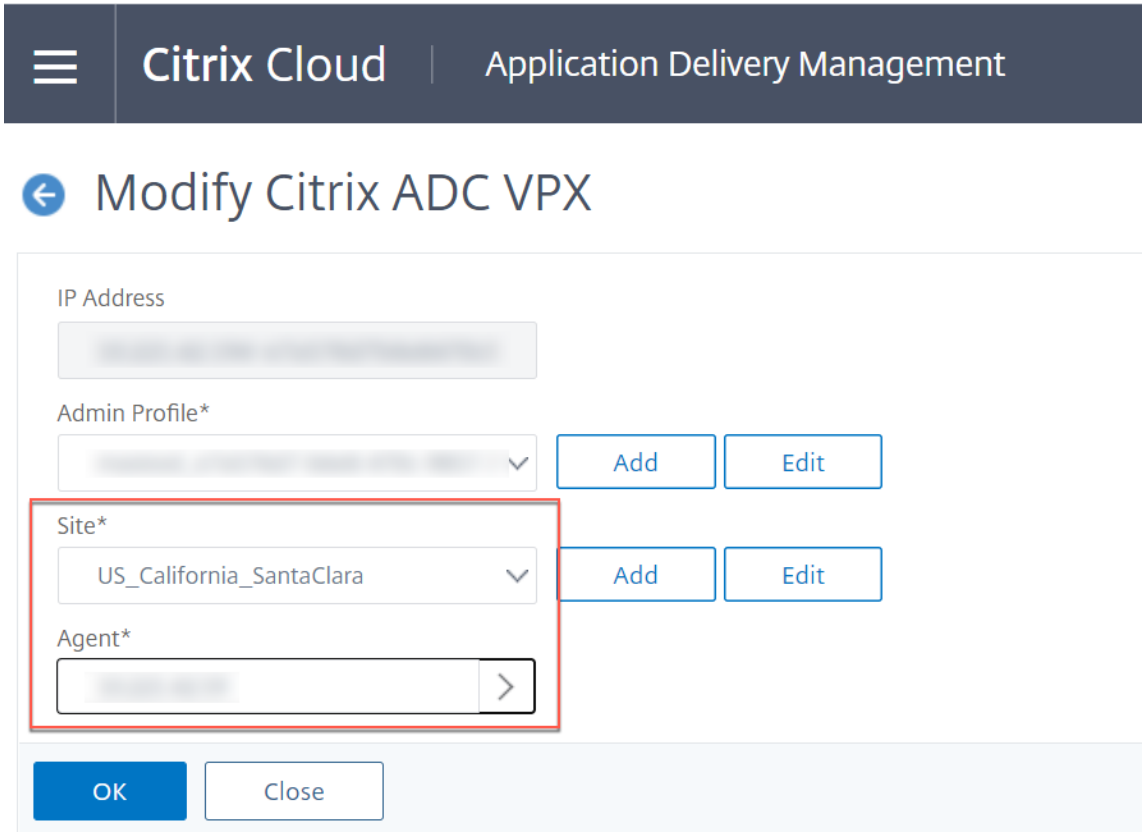
Transition d'un agent intégré à un agent externe

Procédez comme suit pour passer d'un agent intégré à un agent externe :

1. Dans l'interface graphique ADM, sous **Réseaux > Tableau de bord des instances > Citrix ADC**, sélectionnez l'instance Citrix ADC et cliquez sur **Modifier**.



2. Sélectionnez le site et l'agent, puis cliquez sur **OK**.



3. Sélectionnez à nouveau l'instance et cliquez sur **Sélectionner une action > Redécouvrir**.

Caractéristiques et solutions

April 29, 2021

Citrix Application Delivery Management (Citrix ADM) est compatible avec la plupart des fonctionnalités disponibles avec la version locale de Citrix ADM. Ce document décrit les fonctionnalités prises en charge sur le service.

Analyse et gestion des applications

La fonctionnalité d'analyse et de gestion des applications de Citrix ADM renforce l'approche centrée sur les applications pour vous aider à relever les différents défis liés à la livraison des applications. Cette approche vous donne une visibilité sur les scores de santé des applications, vous aide à déterminer les risques de sécurité et vous aide à détecter les anomalies dans les flux de trafic des applications et à prendre des mesures correctives.

- Analyse des performances des applications: App Score est le produit d'un système de notation qui définit la performance 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 fonctionnent.

- Analyse de la sécurité des applications: Le tableau de bord de la sécurité des applications fournit une vue globale de l'état de sécurité de vos applications. Par exemple, il affiche des mesures de sécurité clés telles que les violations de sécurité, les violations de signature, les indices de menaces. Le tableau de bord App Security affiche également des informations relatives aux attaques telles que les attaques SYN, les attaques de petites fenêtres et les attaques d'inondation DNS pour les instances Citrix ADC découvertes.
- Analyse intelligente des applications :La fonctionnalité Intelligent App Analytics fournit une solution simple et évolutive pour la surveillance et le dépannage des applications qui sont fournies via les appliances Citrix ADC. Intelligent App Analytics surveille non seulement tous les niveaux de transactions d'application, mais utilise également des techniques d'apprentissage automatique pour définir des modèles de trafic normaux dans votre réseau et détecter les anomalies. Cette fonctionnalité réduit le temps d'exécution global et améliore la disponibilité globale de l'application.

StyleBooks

StyleBooks simplifie la tâche de gestion des configurations Citrix ADC complexes pour vos applications. Un StyleBook est un modèle que vous pouvez utiliser pour créer et gérer des configurations de Citrix ADC. Vous pouvez créer un StyleBook pour configurer une fonctionnalité spécifique de Citrix ADC, ou concevoir un StyleBook pour créer des configurations pour un déploiement d'application d'entreprise tel que Microsoft Exchange ou Skype for Business.

Gestion des instances

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

> **Remarque**
>
> Actuellement, Citrix ADM prend en charge uniquement la fonctionnalité d'optimisation WAN pour les instances Citrix SD-WAN.

Gestion des événements

Les événements représentent les occurrences d'événements ou d'erreurs sur une instance Citrix ADC gérée. Par exemple, en cas de défaillance du système ou de modification de la configuration, un événement est généré et enregistré sur Citrix ADM. Voici les fonctionnalités associées que vous pouvez configurer ou afficher à l'aide de Citrix ADM :

- Création de règles d'événement
- Utilisation de Citrix ADM pour exporter des messages syslog

Gestion des certificats

Citrix ADM rationalise 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 approprié, la force

de la clé et les algorithmes corrects, tout en gardant un œil étroit sur les certificats inutilisés ou qui expirent bientôt.

Gestion de la configuration

Citrix ADM vous permet de créer des tâches de configuration qui vous aident à effectuer des tâches de configuration, telles que la création d'entités, la configuration de fonctionnalités, la réplication des modifications de configuration, les mises à niveau 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 Citrix ADM.

Audit de configuration

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

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

Gestion des licences

Permet de gérer les licences Citrix ADC en configurant Citrix ADM en tant que gestionnaire de licences.

- Capacité du pool de Citrix ADC: pool de licences commun à partir duquel votre instance Citrix ADC peut extraire une licence d'instance et uniquement autant de bande passante qu'elle en a besoin. Lorsque l'instance n'a plus besoin de ces ressources, elle les réintègre dans le pool commun, rendant les ressources disponibles pour les autres instances qui en ont besoin.
- Licences d'enregistrement et de sortie Citrix ADC VPX: Citrix ADM alloue des licences instances Citrix ADC VPX à la demande. 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.

Rapports réseau

Vous pouvez optimiser l'utilisation des ressources en surveillant vos rapports réseau sur Citrix ADM.

Analytics

Fournit un moyen simple et évolutif d'examiner les différentes informations des données des instances Citrix ADC pour décrire, prédire et améliorer les performances des applications. Vous pouvez utiliser simultanément une ou plusieurs fonctionnalités d'analyse.

- HDX Insight: fournit une visibilité de bout en bout pour le trafic ICA passant par Citrix ADC. HDX Insight permet aux administrateurs d'afficher en temps réel les mesures de latence client et réseau, les rapports historiques, les données de performances de bout en bout et de résoudre les problèmes de performances.
- Web Insight :Fournit une visibilité sur les applications Web d'entreprise. Il permet aux administrateurs informatiques de surveiller toutes les applications Web desservies par l'Citrix ADC en

fournissant une surveillance intégrée et en temps réel des applications. Web Insight traite les données à partir de Citrix ADC à l'aide d'un algorithme d'approximation. Il fournit les 1 000 enregistrements les plus importants des mesures liées aux applications Web de votre entreprise.

- 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, les octets et les 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 votre application et à prendre des mesures correctives pour sécuriser vos applications.
- SSL Insight :Fournit une visibilité sur les transactions sécurisées sur le Web (HTTPS). Il permet aux administrateurs informatiques de surveiller toutes les applications Web desservies par l'Citrix ADC en fournissant une surveillance intégrée, en temps réel et historique des transactions Web. SSL insights traite les données de Citrix ADC à l'aide d'un algorithme d'approximation. Il fournit les 1 000 enregistrements les plus importants des mesures liées aux transactions Web dans votre entreprise.

Contrôle d'accès basé sur les rôles

Le contrôle d'accès basé sur les rôles (RBAC) vous permet d'accorder des autorisations d'accès en fonction des rôles des utilisateurs individuels au sein de votre entreprise. Le premier utilisateur d'une organisation qui ouvre une session avec les informations d'identification Citrix Cloud a le rôle super administrateur qui, par défaut, dispose de toutes les autorisations d'accès. Les autres utilisateurs de cette organisation, qui sont ensuite créés par l'administrateur, se voient attribuer des rôles non admin.

Abonnements

Fournit une vue de tableau de bord des abonnements que vous avez achetés.

Vous êtes affecté à un compte Express par défaut. Avec ce compte, vous pouvez gérer des ressources ADM limitées. Pour de plus amples informations, consultez la section Gérer les ressources Citrix ADM à l'aide du compte Express.

Les fonctionnalités Citrix ADM suivantes ne sont actuellement pas disponibles :

- Déploiement
  - Migration de Citrix Insight Center vers Citrix ADM
  - Intégration de Citrix ADM avec Citrix Virtual Desktop Director
- Réseaux : Prise en charge de Citrix SD-WAN EE
- Analytics : TCP Insight, Video Insight et WAN Insight
- Paramètres système limités
- Orchestration

- Intégration avec OpenStack et VMware NSX Manager
- Automation Citrix ADC en mode hybride de Cisco ACI
- Container Orchestration : Intégration avec Mesos/Marathon et Kubernetes

Configuration système requise

April 29, 2021

Avant de commencer à utiliser Citrix Application Delivery Management (Citrix ADM), vous devez vérifier la configuration logicielle requise, la configuration requise du navigateur, les informations de port, les informations de licence et les limitations.

Navigateurs pris en charge

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

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

Configuration requise pour l'installation de l'agent

Installez et configurez un agent dans votre environnement réseau pour activer la communication entre Citrix ADM et les instances gérées de votre datacenter. Dans votre datacenter local, vous pouvez installer un agent sur le serveur KVM Citrix XenServer, VMware ESXi, Microsoft Hyper-V et Linux.

Les exigences de l'agent sont les ressources informatiques virtuelles que l'hyperviseur doit fournir pour chaque agent ADM. Le tableau suivant répertorie les exigences de l'agent pour bénéficier de toutes les fonctionnalités ADM :

Composant	Exigences
RAM	32 Go

Composant	Exigences
CPU virtuel	8
Espace de stockage	30 FR
Interfaces réseau virtuel	1
Débit	1 Gbit/s

Les exigences de l'agent pour utiliser uniquement la fonctionnalité de licence groupée, reportez-vous à la section Agent léger pour les licences groupées.

Vous pouvez également installer un agent sur Microsoft Azure, AWS ou Google Cloud. Citrix vous recommande d'utiliser les types de machines virtuelles suivantes à partir des sites de vente cloud respectifs pour bénéficier de toutes les fonctionnalités ADM :

Cloud	Exigences relatives	Type de machine virtuelle préféré
AWS	8 processeurs virtuels, 32 Go de RAM et 30 Go d'espace de stockage	`m4.2xlarge`
Microsoft Azure	8 processeurs virtuels, 32 Go de RAM et 30 Go d'espace de stockage	`Standard_D8s_v3`
Cloud Google	8 processeurs virtuels, 32 Go de RAM et 30 Go d'espace de stockage	`e2-standard-8`

Pour obtenir des instructions sur l'installation d'un agent, consultez les liens suivants :

- Installation de Citrix ADM Agent sur Microsoft Azure Cloud.
- Installation de Citrix ADM Agent sur AWS.
- Installation de Citrix ADM Agent sur Google Cloud.

Agent léger pour les licences groupées

Si vous envisagez d'utiliser le service ADM uniquement pour les licences groupées, vous pouvez utiliser un agent avec des spécifications inférieures, comme indiqué dans le tableau suivant :

Composant	Exigences
RAM	8 Go
CPU virtuel	4
Espace de stockage	30 FR

Ces agents ayant des spécifications inférieures (légers) ne sont pris en charge que sur le service ADM.

Citrix vous recommande d'utiliser les types de machines virtuelles suivantes à partir des sites de vente cloud respectifs pour utiliser uniquement la fonctionnalité de licence groupée :

Cloud	Exigences relatives	Type de machine virtuelle préféré
AWS	4 CPU virtuels, 8 Go de RAM et 30 Go d'espace de stockage	`m4.xlarge`. Ce type d'instance fournit 4 CPU virtuels, 16 Go de RAM et 30 Go d'espace de stockage. Citrix recommande ce type d'instance car il correspond à la plupart des exigences de l'agent parmi les types d'instance existants.
Microsoft Azure	4 CPU virtuels, 8 Go de RAM et 30 Go d'espace de stockage	`Standard_F4s_v2`
Cloud Google	4 CPU virtuels, 8 Go de RAM et 30 Go d'espace de stockage	`e2-standard-4`

> **Remarque**
>
> Vous devez désactiver les tâches de planification par défaut en accédant à **Paramètres > Paramètres système > Fonctionnalités configurables**.

Ports

Pour les communications entre les instances Citrix ADC et l'agent Citrix ADM, ou les instances Citrix SD-WAN et l'agent Citrix ADM, les ports suivants doivent être ouverts dans un agent Citrix ADM :

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

Type	Port	Détails	Direction de la communication
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	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

Type	Port	Détails	Direction de la communication
TCP	5557/5558	Pour les communications **logstream** (pour Security Insight, Web Insight et HDX Insight) de Citrix ADC à 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 et 7279	Ports de licence pour la communication entre le serveur de licences Citrix ADM et l'instance ADC. Ces ports sont également utilisés pour les licences groupées ADC.	Citrix ADC vers Citrix ADM
TCP	443/8443/7443	Port pour la communication entre l'agent Citrix ADM et Citrix ADM. L'agent ADM initie la communication à Citrix ADM.	Agent Citrix ADM vers Citrix ADM

Pour la communication entre l'agent Citrix ADM et Citrix ADM, assurez-vous que le port suivant est ouvert dans l'agent Citrix ADM :

Type	Port	Détails
HTTPS	443	Pour la communication entre l'agent Citrix ADM et Citrix ADM.

> **Remarque**
>
> Le point de terminaison de Citrix ADM est le même que l'URL de service générée lors de la tentative d'inscription de l'agent. L'agent utilise l'URL du service pour localiser Citrix ADM.

Assurez-vous que les points de terminaison suivants sont sur la liste blanche :

- Service de téléchargement :

```
https://download.citrixnetworkapi.net
<!--NeedCopy-->
```

- Service de confiance :

```
*.citrixnetworkapi.net
<!--NeedCopy-->
```

- URL de service :

```
*.agent.adm.cloud.com
*.adm.cloud.com
adm.cloud.com
<!--NeedCopy-->
```

- Service de sauvegarde ADC :

```
adm-prod-backup-\*.s3.amazonaws.com
adm-prod-backup-\*.s3.*amazonaws.com
<!--NeedCopy-->
```

Pour la communication entre l'agent Citrix ADM et Citrix Analytics Service, assurez-vous que les points de terminaison suivants sont sur la liste blanche :

Point de terminaison	États-Unis	UE
Hub d'événements	`https://cas-eh-ns-alias.servicebus.windows.net`	`https://cas-eh-ns-eu-alias.servicebus.windows.net`

FQDN obsolètes

Certains noms complets sont obsolètes pour l'utilisation suivante du service ADM. Pour vous aider à passer aux nouveaux FQDN sans interruption, les FQDN obsolètes continuent de fonctionner pendant un certain temps et seront progressivement éliminés.

Points de terminaison du service ADM	Ancien nom de domaine complet	Nouveau nom de domaine complet
Accès à l'interface utilisateur du service ADM	`netscalermas.cloud.com`	`adm.cloud.com`
Adresse URL du service	`agent.netscalermgmt.net`	`*.agent.adm.cloud.com` **Note** : La valeur de * dépendra du POP (point de présence) que vos données sont disponibles.
Interactions API	`netscalermas.cloud.com`	`api.adm.cloud.com`

Versions minimales de Citrix ADC requises

> Remarque
>
> Les versions 10.5, 11.0 et 12.0 de Citrix ADC ont déjà atteint la fin de vie (EOL). Pour plus d'informations, veuillez consulter le Tableau des produits. La version ADC recommandée est 12.1.

Fonctionnalité Citrix ADM	Version du logiciel Citrix ADC
StyleBooks	10.5 et versions ultérieures
Surveillance, création de rapports et configuration à l'aide de travaux	10.5 et versions ultérieures
Analytics	
HDX Insight	10.1 et versions ultérieures

Fonctionnalité Citrix ADM	Version du logiciel Citrix ADC
Gateway Insight	11.0.65.31 et versions ultérieures
Security Insight	11.0.65.31 et versions ultérieures

Configuration requise pour la gestion des instances Citrix SD-WAN

Versions WANOP SD-WAN minimales requises pour Citrix

Fonctionnalité Citrix ADM	Citrix CloudBridge/Citrix SD-WAN WO
Surveillance, création de rapports et configuration à l'aide des tâches Analytics	Citrix CloudBridge 7.4.0 et versions ultérieures
HDX Insight	Citrix CloudBridge 7.4.0 et versions ultérieures
WAN Insight	Citrix CloudBridge 7.4.0 et versions ultérieures

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

Éditions de la Plate-forme	Détection	Configuration	Surveillance	Rapports	Gestion des événe-ments (interrup-tions SNMP)	HDX Insight et WAN Insight Analytics	Multi-Hop Insight
Citrix SD-WAN WANOP	Oui	Oui	Oui	Oui	Oui	Oui	Oui

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

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

- Client léger Dell Wyse WTOS modèle R10L Rx0L
- NComputing N400
- Dell Wyse WTOS modèle CX0 C00X Xenith

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

Configuration requise pour la solution Citrix ADM Analytics

Versions minimales de Citrix Virtual Apps and Desktops requises

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

> **Remarque**
>
> La fonctionnalité Citrix Gateway (baptisée Access Gateway Enterprise pour les versions 9.3 et 10.x) doit être disponible sur l'instance de 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 une application Virtual App ou Desktop Citrix et accessibles via Citrix Receiver. Toutefois, cette fonctionnalité dépend du système d'exploitation sur lequel le 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 HDX Insight

Citrix ADM prend en charge les clients légers suivants pour la surveillance des instances de Citrix ADC exécutées sur le logiciel version 11.0 Build 65.31 et versions ultérieures :

- Clients légers basés sur Windows Dell Wyse
- Clients légers basés sur Dell Wyse Linux
- Clients légers basés sur Dell Wyse ThinOS
- Clients légers basés sur Ubuntu 10ZiG

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 installées des instances de Citrix ADC qui sont surveillées. Les rapports HDX Insight s'affichent uniquement

pour les appliances Citrix ADC Premium et Enterprise exécutées sur les versions logicielles 10.5 et ultérieures.

Licence/durée de Citrix ADC	5 minutes	1 heure	1 jour	1 semaine	> 1 Mois
Standard	Non	Non	Non	Non	Non
Avancé	Oui	Oui	Non	Non	Non
Premium	Oui	Oui	Oui	Oui	Oui

Systèmes d'exploitation pris en charge et versions de Citrix Receiver

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

OS	Version de Receiver
Windows	4.0 Édition Standard
Linux	13.0.265571 et versions ultérieures
Mac	11.8, build 238301 et versions ultérieures
HTML5	1.5*
Application Chrome	1.5*

* Applicable avec Citrix CloudBridge version 7.4 et ultérieure.

Licences

April 29, 2021

Citrix Application Delivery Management (ADM) nécessite une licence Citrix ADM vérifiée pour gérer et surveiller les instances Citrix ADC.

Voici les types de licences pris en charge pour Citrix ADM for Service :

Type de licence	En droit de
Serveur virtuel	10 serveurs virtuels et 5 Go de stockage par licence
Stockage	5 Go par licence
Licence Express	Le compte Citrix ADM Express est un compte par défaut pour gérer les ressources ADM.

Avec un compte Express, vous pouvez gérer des ressources ADM limitées. Pour de plus amples informations, consultez la section Gérer les ressources Citrix ADM à l'aide du compte Express.

Une fois la licence achetée expirée, vous aurez 60 jours de délai de grâce. Pendant la période de grâce, vous pouvez choisir les ressources ADM qui peuvent être gérées à l'aide d'un compte Express.

(Pour plus d'informations sur la mise en route d'un compte Express, consultezMise en route/en-us/citrix-application-delivery-management-service/getting-started.html[()]et pour gérer les abonnements, consultezGestion des abonnements[]/en-us/citrix-application-delivery-management-service/managing-subscriptions.html.)

Ajouter une licence

> Remarque :
>
> Vous pouvez ajouter uniquement une licence groupée pour les instances Citrix ADC.

Vous pouvez ajouter une licence groupée pour les instances de Citrix ADC dans Citrix ADM. Après avoir ajouté la licence, vous pouvez vérifier les informations de licence dans **Comptes** > **Abonnements** .

Pour ajouter une licence groupée :

1. Accédez à **Réseaux** > **Licences**.
2. Cliquez sur **Obtenir les licences** pour sélectionner le fichier de licence à partir de votre ordinateur local.
3. Sélectionnez le fichier de licence (.lic) et cliquez sur **OK**.

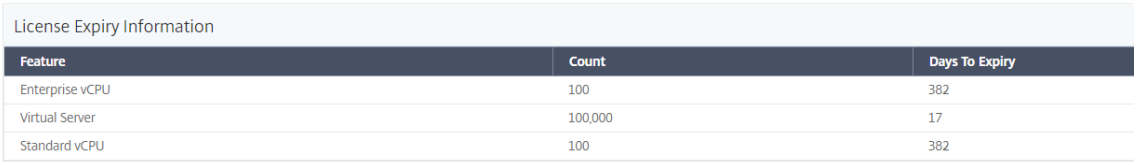
Vérifications d'expiration pour les licences de serveur virtuel

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

Pour afficher l'état des licences :

1. Accédez à **Réseaux** > **Licences**.

2. Dans la section **Informations sur l'expiration de la licence**, vous trouverez les détails des licences qui vont expirer :


License Expiry Information

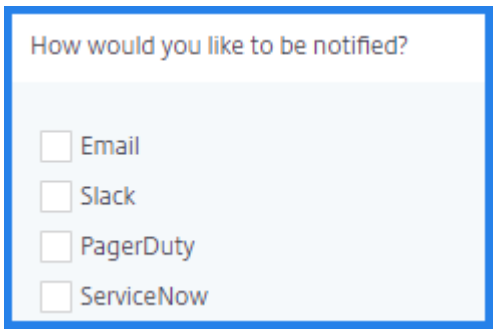
Feature	Count	Days To Expiry
Enterprise vCPU	100	382
Virtual Server	100,000	17
Standard vCPU	100	382

   - **Fonctionnalité** : Type de licence qui va expirer.
   - **Nombre** : nombre d'instances affectées.
   - **Jours avant l'expiration** : Nombre de jours restants avant l'expiration.

Pour configurer les paramètres de notification des licences :

1. Accédez à **Réseaux**> **Licences**.
2. Dans la section **Paramètres de notification**, cliquez sur l'icône en forme de crayon et modifiez les paramètres.
   a) **De quoi aimeriez-vous être averti ?** - Spécifiez le pourcentage de la capacité.
   b) **Comment aimeriez-vous être averti ?** - Sélectionnez les options de notification suivantes :
      - **E-mail** : spécifiez un serveur de messagerie et les détails du profil. Un e-mail est déclenché lorsque vos licences sont sur le point d'expirer.
      - **Slack** : spécifiez un profil de marge. Une notification est envoyée lorsque vos licences sont sur le point d'expirer.
      - **PagerDuty** - Spécifiez un profil PagerDuty. En fonction des paramètres de notification configurés dans votre portail PagerDuty, une notification est envoyée lorsque vos licences sont sur le point d'expirer.
      - **ServiceNow** - Une notification est envoyée au profil ServiceNow par défaut lorsque vos licences sont sur le point d'expirer.

        > **Important**
        >
        > Assurez-vous que Citrix Cloud ITSM Adapter est configuré pour ServiceNow et intégré au service Citrix ADM. Pour de plus amples informations, consultez la section Intégrer Citrix ADM Service à l'instance ServiceNow.



c) **Expiration des licences** - Indiquez les jours avant l'expiration de la licence, lorsque vous souhaitez recevoir une notification.

Gérer les ressources Citrix ADM à l'aide du compte Express

April 29, 2021

Le compte Citrix ADM Express est un compte par défaut pour gérer les ressources ADM. Ce compte est facilement disponible sur Citrix Cloud.

Ce compte offre les options de gestion des ressources ADM suivantes de votre choix :

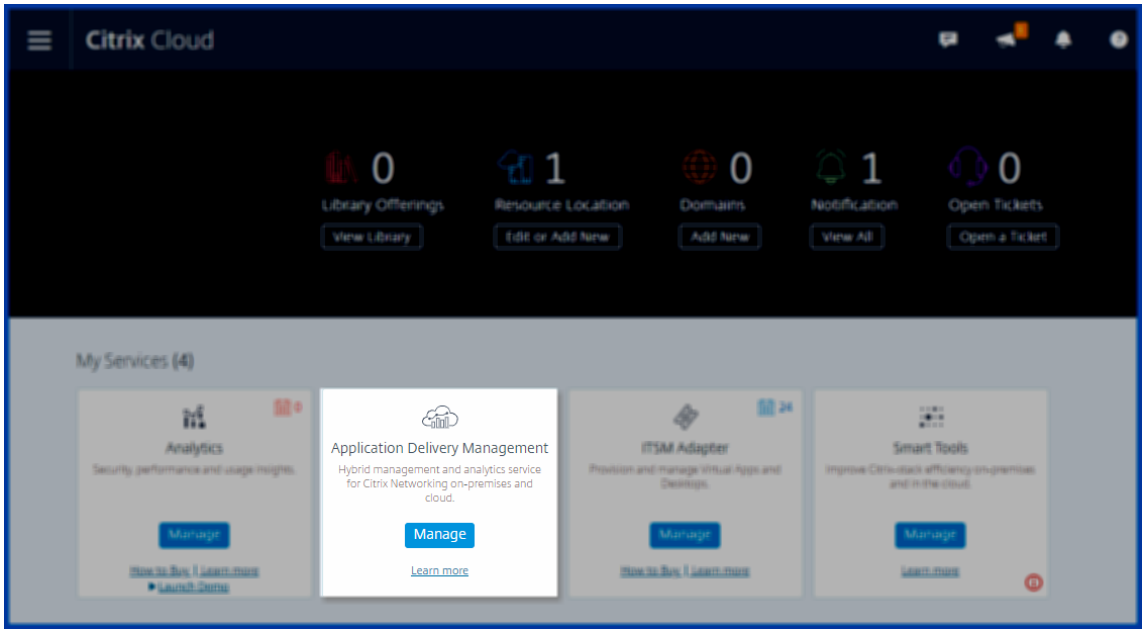
- Jusqu'à deux serveurs virtuels
- Jusqu'à deux tâches de configuration
- Jusqu'à deux packs de configuration StyleBooks

Pour gérer les ressources spécifiques avec un compte Express, vous devez sélectionner les ressources requises pendant la période de grâce. Si vous ne sélectionnez pas les ressources, le service ADM sélectionne automatiquement les ressources que vous pouvez gérer avec le compte Express.

> **Important**
>
> - Lorsque votre compte est converti en compte Express, le service ADM conserve les données de stockage jusqu'à 500 Mo ou les données d'un jour, selon la moindre des deux éventualités.
> - Si votre compte Citrix ADM Express reste inactif pendant 90 jours, le compte sera supprimé. L'équipe Citrix ADM envoie un rappel après 60 jours d'inactivité.

Pour gérer les ressources de ADM :

1. Connectez-vous à Citrix Cloud avec vos informations d'identification.
2. Cliquez sur **Gérer** dans la vignette **Citrix Application Delivery Management** .



Après la fin de votre licence d'abonnement Citrix ADM et de votre période de grâce, votre compte est converti en compte Express, sauf si vous renouvelez votre licence. Le compte Express vous aide à poursuivre votre activité en utilisant le service Citrix ADM. Pour renouveler votre licence Citrix ADM, rendez-vousCitrix Cloudou contactez le support technique.

Gestion des abonnements

April 29, 2021

Citrix Application Delivery Management (Citrix ADM) nécessite une licence vérifiée pour gérer et surveiller les instances Citrix ADC, les instances Citrix Gateway et les équilibreurs de charge tiers.

Vous pouvez gérer et surveiller n'importe quel nombre d'instances lorsque vous utilisez un compte Express ou lorsque vous êtes abonné à une licence valide. Toutefois, vous pouvez gérer les applications découvertes sur le tableau de bord de l'application, afficher les données d'analyse et surveiller les fonctions réseau et les rapports réseau uniquement pour le nombre de serveurs virtuels pour lesquels vous avez acheté des licences. Pour plus d'informations sur les ressources ADM que vous pouvez gérer avec le compte Express, reportez-vous à la sectionLe compte Citrix ADM Express.

Avec chaque licence installée, vous recevez une quantité limitée de données et de capacité pour gérer certains serveurs virtuels. Toutefois, vous pouvez également acheter et appliquer des licences de données uniquement pour reconstituer votre stockage de données.

Pour plus d'informations et d'instructions sur l'achat et la mise à niveau de vos licences Citrix ADM, reportez-vous à la sectionCitrix Application Delivery Management.

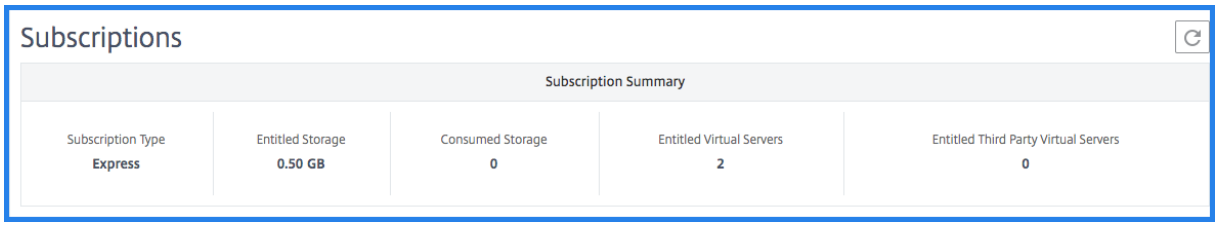
Le tableau suivant répertorie les licences Citrix requises pour utiliser certaines fonctionnalités Citrix ADM.

Groupe de fonctionnalités Citrix ADM	Fonctionnalités de Citrix ADM	Licence requise pour Citrix ADC et passerelle
Analytics	HDX Insight	Avancé (reporting < 1 heure) Premium (reporting = illimité)
Analytics	Security Insight	Licence Premium (ou) Advanced avec App Firewall
Analytics	Gateway Insight	Avancé (reporting < 1 heure) Premium (reporting = illimité)
Applications	Statistiques des applications (Tableau de bord des applications, Tableau de bord de sécurité des applications)	Informations relatives au Citrix Web App Firewall sur le tableau de bord de l'application et le tableau de bord de la sécurité des applications nécessitent une licence Premium (ou) Advanced with App Firewall
Applications	Gateway API	Licence Premium (ou) avancée
Applications	StyleBooks	S.O.
Applications	Gestion des stocks — Tableau de bord de l'infrastructure, groupes d'instances, tableaux de bord d'instance et sites	S.O.
Applications	Gestion des événements et Syslog	S.O.
Applications	Travaux de configuration, audit de configuration et conseils de configuration	S.O.
Applications	Rapports réseau (niveau Instance)	S.O.
Applications	Rapports réseau (niveau serveur virtuel)	S.O.

Groupe de fonctionnalités Citrix ADM	Fonctionnalités de Citrix ADM	Licence requise pour Citrix ADC et passerelle
Applications	Fonctions réseau (visibilité simple et gestion des serveurs virtuels, des services, des groupes de services, des serveurs)	S.O.
Applications	Gestion des certificats SSL (niveau Instance)	S.O.
Applications	Gestion des certificats SSL (niveau serveur virtuel)	S.O.
Système	Authentification RBAC et externe (niveau instance)	S.O.
Système	Authentification RBAC et externe (niveau serveur virtuel)	S.O.

Afficher les détails de l'abonnement

Vous pouvez afficher les licences installées sur votre Citrix ADM en accédant à **Compte** > **Abonnements** . Vous pouvez également afficher le résumé des licences, par exemple le type de licence abonnée, l'abonnement aux données et l'abonnement aux données consommées, ainsi que les serveurs virtuels autorisés et gérés et les serveurs virtuels tiers dans la section **Résumé des abonnements** .



Gérer les abonnements pour les serveurs virtuels tiers

Vous pouvez gérer et surveiller n'importe quel nombre d'hôtes HAProxy lorsque vous êtes sur la période d'essai ou lorsque vous avez souscrit à une licence valide. Toutefois, vous pouvez gérer les applications découvertes sur le tableau de bord de l'application HAProxy, afficher les données d'analyse et surveiller les fonctions réseau uniquement pour le nombre de serveurs virtuels tiers pour lesquels vous avez acheté des licences. Pendant la période d'essai, vous ne pouvez surveiller que 10 serveurs

virtuels ou applications tiers.

> **Remarque**
>
> Dans ce document, le serveur virtuel tiers fait référence au frontal HaProxy.

Gérer les serveurs virtuels

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

Points à noter :

- Par défaut, Citrix ADM attribue automatiquement des licences aux serveurs virtuels au hasard 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 serveurs virtuels installées, Citrix ADM, par défaut, concède tous les serveurs virtuels.

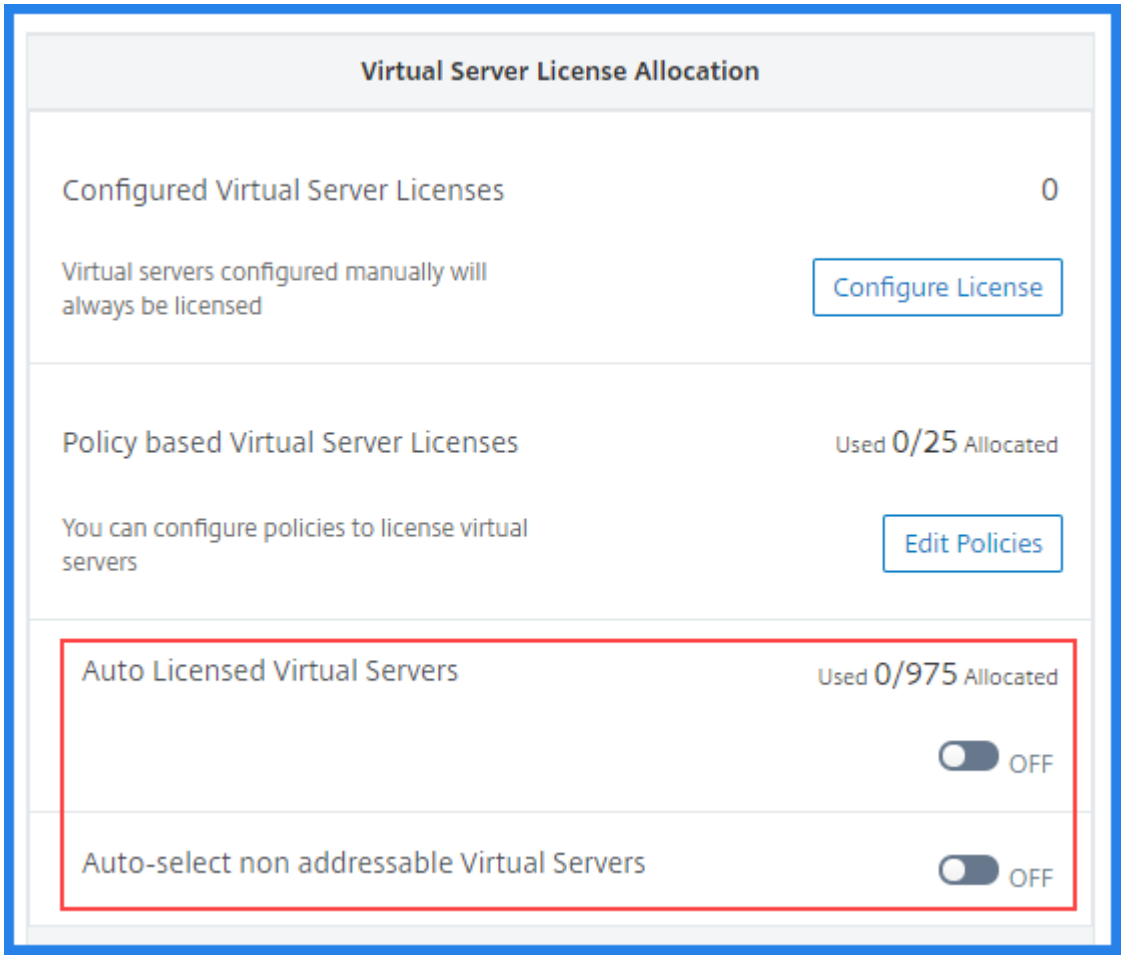
Pour sélectionner manuellement les serveurs virtuels ou restreindre les licences aux serveurs virtuels limités, vous devez d'abord désactiver la licence automatique des serveurs virtuels, puis sélectionner les serveurs virtuels que vous souhaitez gérer.

Pour désactiver la licence automatique des serveurs virtuels :

1. Accédez à **Compte > Abonnements**.

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

2. Dans l'**allocation de licence de serveur virtuel**, désactivez **les serveurs virtuels sous licence automatiqueet sélectionnez automatiquement les serveurs virtuels non adressables**.

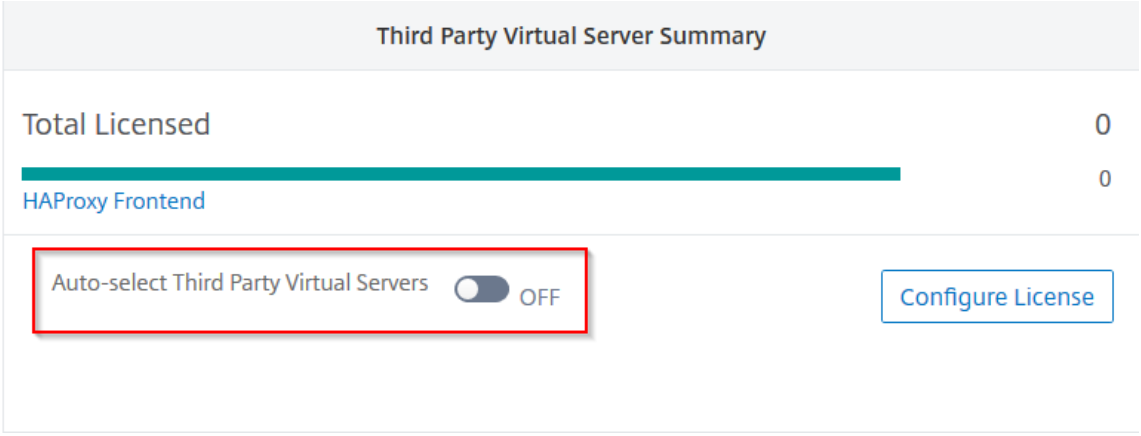


Pour sélectionner des serveurs virtuels tiers pour l'octroi de licences :

1. Accédez à **Compte** > **Abonnements**.

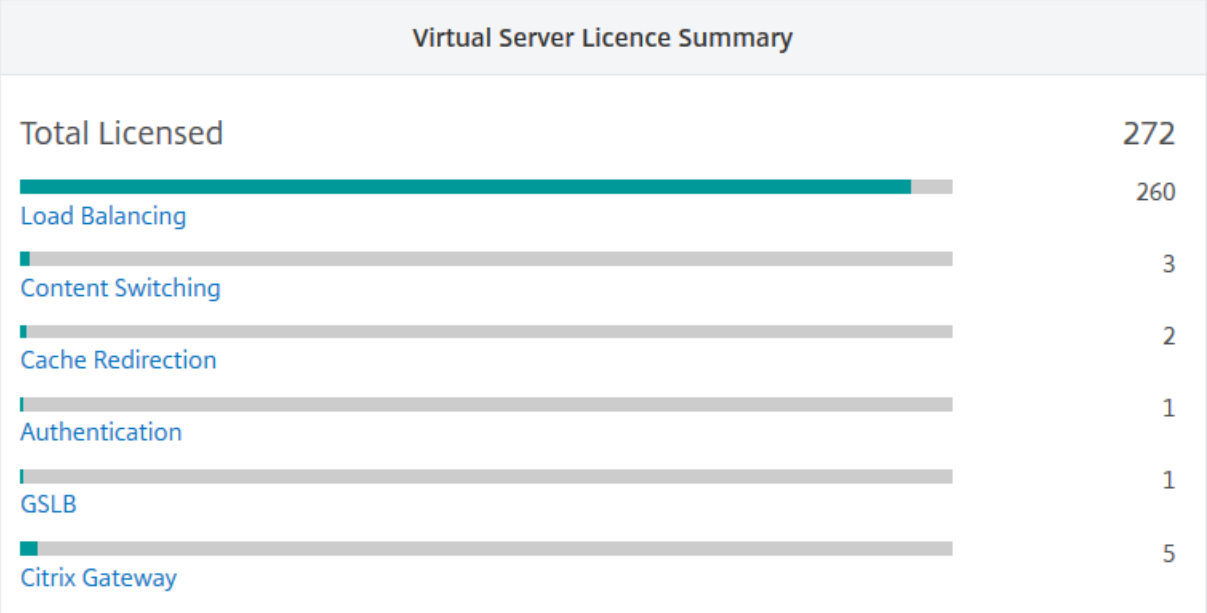
   Le tableau de bord affiche les licences de serveur virtuel disponibles, les serveurs virtuels gérés ainsi que le type de serveur virtuel et les informations d'expiration de licence.

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



Afficher les serveurs virtuels sous licence

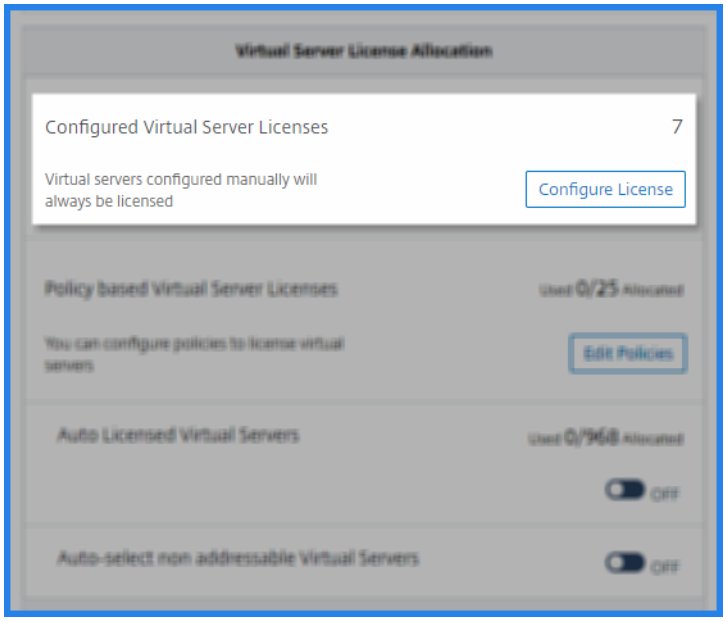
Une fois les licences appliquées aux serveurs virtuels, vous pouvez afficher les serveurs virtuels sous licence ou les serveurs virtuels tiers à partir de la page **Abonnements** . Pour afficher les serveurs virtuels sous licence, accédez à **Comptes > Abonnements** et cliquez sur le type de serveur virtuel dans la section **Total sous licence** du **Résumé des licences des serveurs virtuels** .



Appliquer manuellement des licences de serveur virtuel

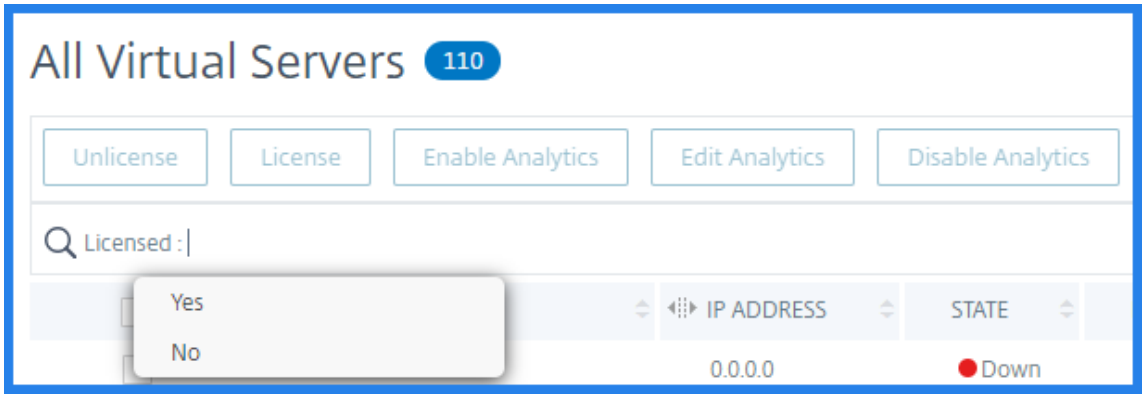
Vous pouvez appliquer manuellement des licences à un serveur virtuel individuel.

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



La page **Tous les serveurs virtuels** s'affiche.

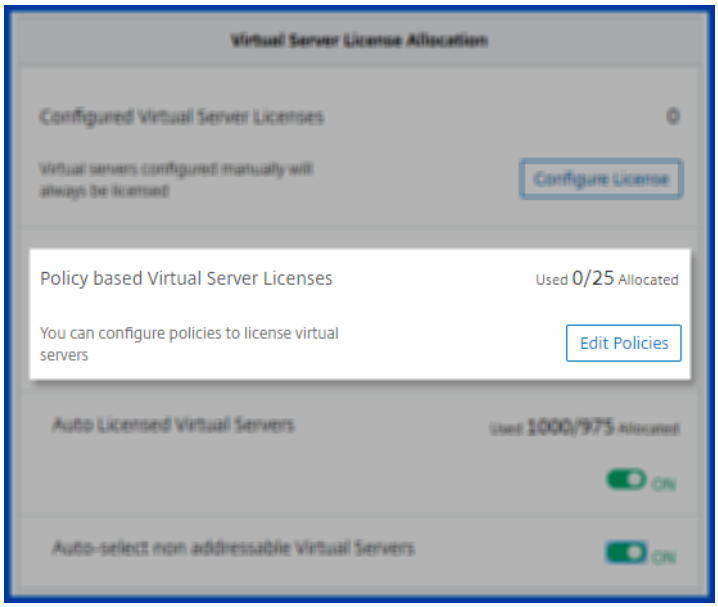
2. Filtrer les serveurs virtuels sans licence à l'aide de la propriété : `Licensed: No`.



3. Sélectionnez le serveur virtuel que vous souhaitez mettre sous licence.
4. Cliquez sur **Licence**.

Configurer les licences de serveur virtuel basées sur des stratégies

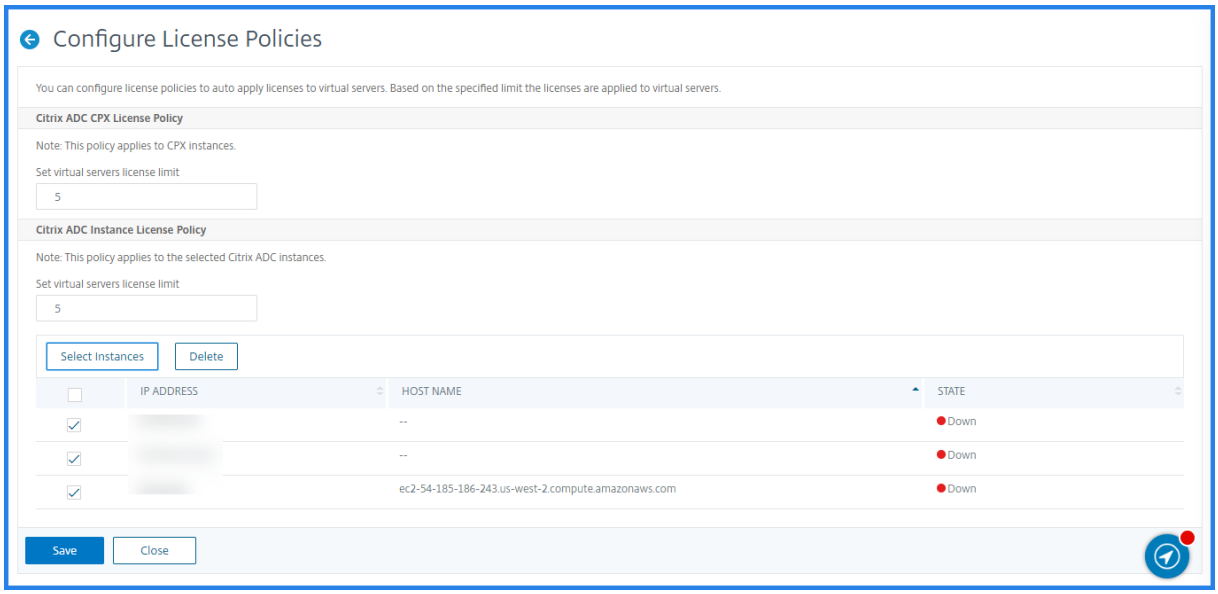
Vous pouvez configurer une stratégie pour appliquer une licence aux serveurs virtuels. Cette stratégie contrôle le nombre de serveurs virtuels que vous souhaitez attribuer automatiquement une licence. Il applique également des licences aux serveurs virtuels des instances sélectionnées uniquement.



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

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

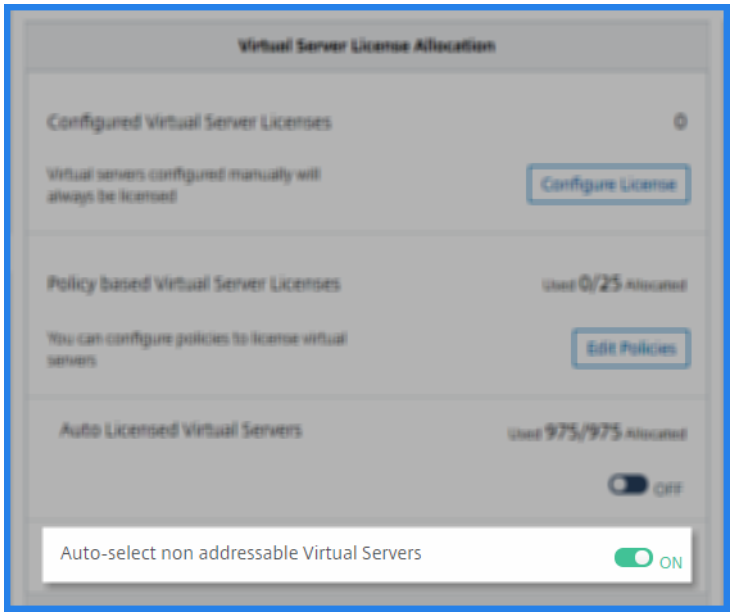
- Définissez la limite des serveurs virtuels sur certaines instances ADC (MPX/VPX/BLX) pour appliquer des licences. L'ADM applique des licences aux serveurs virtuels sur des instances ADC jusqu'à concurrence d'une limite spécifiée.
- Sélectionnez les instances ADC prioritaires pour appliquer des licences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



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

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

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



Remarque

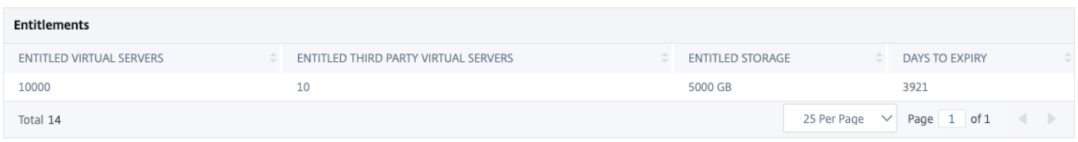
- Citrix ADM, par défaut, ne sélectionne toujours pas automatiquement les serveurs virtuels non adressables pour les licences.
- L'analyse des applications (Tableau de bord des applications) est la seule analyse prise en charge actuellement sur les serveurs virtuels non adressables sous licence.

Afficher les vérifications d'expiration pour les abonnements au serveur virtuel

Vous pouvez afficher l'état des licences installées avec l'expiration et la limite de stockage autorisée pour les licences dans Citrix ADM.

Pour afficher l'état des licences :

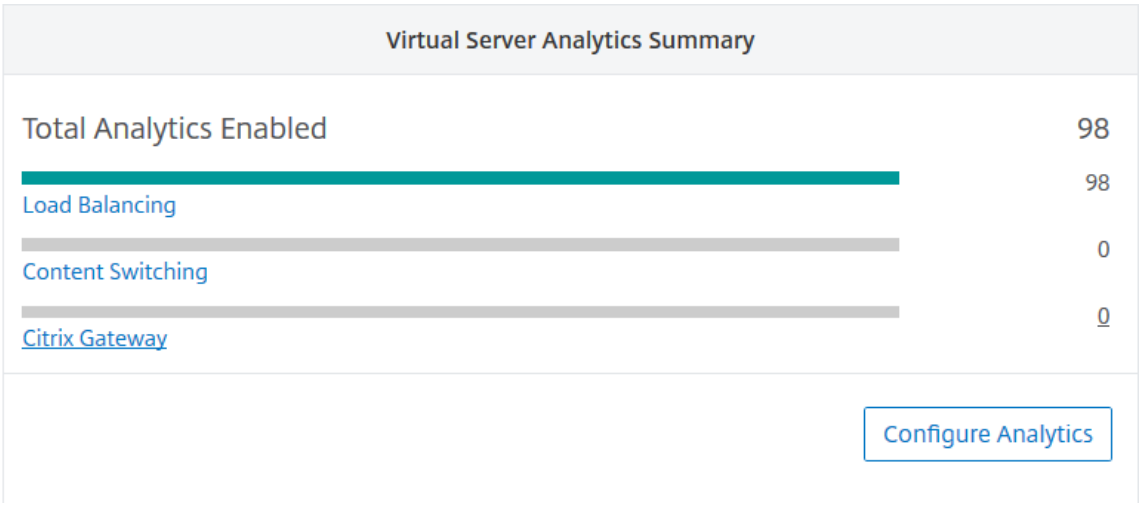
1. Accédez à **Compte** > **Abonnements**.
2. Dans la section **Droits**, vous pouvez afficher les détails des serveurs virtuels sous licence et les jours d'expiration :
   - **Intitulé Serveurs virtuels :** nombre de serveurs virtuels disponibles pour licence.
   - **Intitulé Serveurs virtuels tiers :** nombre de serveurs virtuels tiers que vous pouvez gérer avec la licence.
   - **Intitulé Stockage :** Limite de stockage de la licence.
   - **Jours avant l'expiration :** Nombre de jours restant avant l'expiration de la licence.



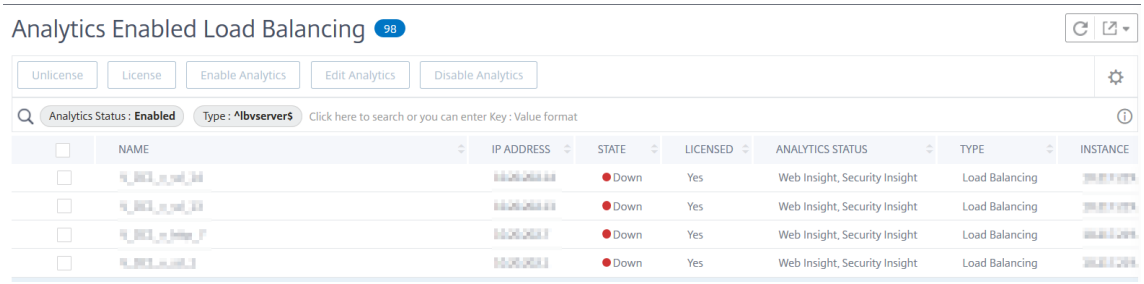
Afficher le type d'analyse activé sur les serveurs virtuels

Après avoir activé AppFlow sur les serveurs virtuels sélectionnés, vous pouvez afficher le type d'analyse activé sur les serveurs virtuels sous licence ou les serveurs virtuels tiers à partir de la page **Abonnements** .

1. Accédez à **Compte** > **Abonnements**.
2. Dans la section **Résumé de l'analyse des serveurs virtuels**, sélectionnez le type de serveurs virtuels sous licence.



3. La page Serveurs virtuels sous licence affiche la liste des serveurs virtuels sous licence. Sur cette page, la colonne **État de l'analyse** affiche le type d'analyse activé sur les serveurs virtuels.



Configuration

April 29, 2021

Une fois la configuration initiale terminée, vous devez configurer certains paramètres pour commencer à gérer complètement votre déploiement.

- Ajout de plusieurs agents. Le nombre d'agents à installer dépend du nombre d'instances gérées dans un centre de données ou un nuage et du débit total. Citrix recommande d'installer au

moins un agent pour chaque centre de données.

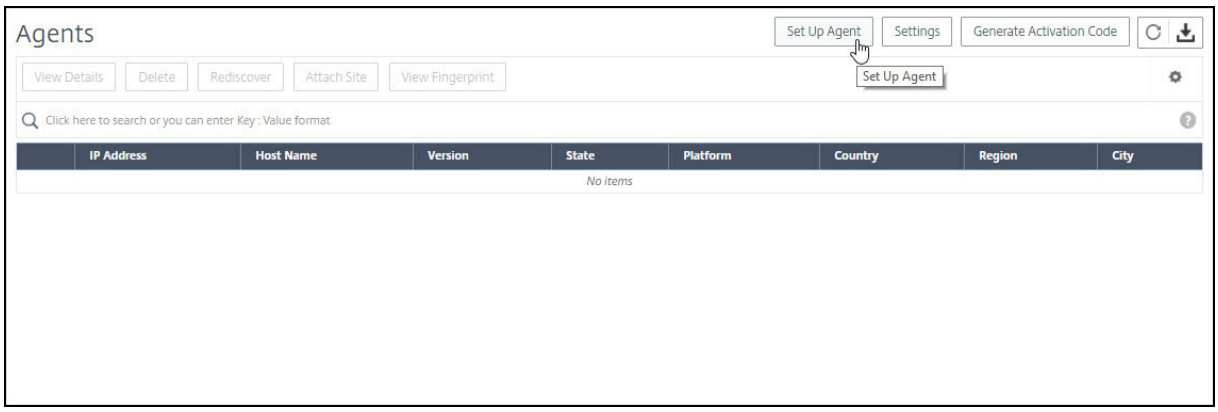
- Ajout d'instances. Vous pouvez ajouter des instances lors de la configuration de Citrix ADM pour lepremière foisou ultérieurement. Vous devez ajouter des instances au service pour commencer à les gérer et à les surveiller. Après avoir installé plusieurs agents, vous devez ajouter des instances et les associer aux agents.
- Activation de l'analyse. 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.
- Configuration de syslog sur les instances. Vous pouvez surveiller les événements syslog générés sur vos instances de Citrix ADC si vous avez configuré votre périphérique pour rediriger tous les messages syslog vers Citrix ADM. Pour surveiller les événements syslog, vous devez d'abord configurer Citrix ADM en tant que serveur syslog pour votre instance Citrix ADC.
- Configuration du contrôle d'accès basé sur les rôles. Citrix ADM fournit un contrôle d'accès basé sur les rôles (RBAC), qui vous permet d'accorder des autorisations d'accès en fonction des rôles d'utilisateurs individuels au sein de votre entreprise.
- Configuration des paramètres Analytics. Vous pouvez configurer certains paramètres pour garantir une expérience optimale de la fonctionnalité Analytics. Par exemple, vous pouvez spécifier la durée de stockage des données d'analyse historiques et définir des seuils et des alertes pour surveiller les mesures d'analyse souhaitées.

Ajout de plusieurs agents

April 29, 2021

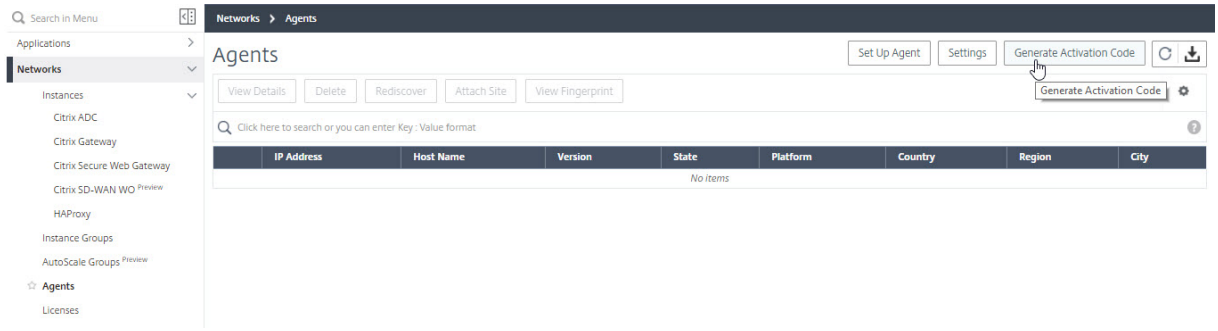
Le nombre d'agents à installer dépend du nombre d'instances gérées dans un centre de données et du débit total. Citrix recommande d'installer au moins un agent pour chaque centre de données.

Vous ne pouvez installer qu'un seul agent lorsque vous vous connectez au service pour la première fois. Pour ajouter plusieurs agents, terminez d'abord la configuration initiale, puis accédez à **Réseaux > Agents** et cliquez sur **Configurer l'agent.**



Téléchargez l'image de l'Hypervisor requis et installez l'agent en suivant les instructions de la section Commencer. Assurez-vous de copier l'URL du service et le code d'activation affichés à l'écran car vous devez entrer l'URL du service et le code d'activation lors de l'installation de l'agent sur votre Hypervisor. L'agent utilise l'URL du service pour localiser le service et le code d'activation pour s'inscrire auprès du service.

Vous pouvez utiliser la même image pour installer plusieurs agents dans votre Hypervisor. Toutefois, vous ne pouvez pas utiliser le même code d'activation sur plusieurs agents. Après avoir installé un agent, générez à nouveau le code d'activation pour l'agent suivant. Vous pouvez générer un nouveau code d'activation en accédant à **Réseaux > Agents**, puis cliquez sur **Générer un code d'activation**.



Une fois l'agent installé et enregistré avec succès, vérifiez l'état de l'agent sur l'interface graphique du service et ajoutez des instances à celui-ci.

> **Remarque**
>
> Vous pouvez également installer un agent Citrix ADM sur le cloud Microsoft Azure ou le cloud AWS. L'image de l'agent est disponible sur le site de vente en nuage respectif.
>
> - Pour obtenir des instructions sur l'installation d'un agent sur le cloud Microsoft Azure, reportez-vous à la section Installation de Citrix ADM Agent sur Microsoft Azure Cloud.
> - Pour obtenir des instructions sur l'installation d'un agent sur AWS, reportez-vous à la section Installation de Citrix ADM Agent sur AWS.

Configurer les agents Citrix ADM pour un déploiement multisite

April 29, 2021

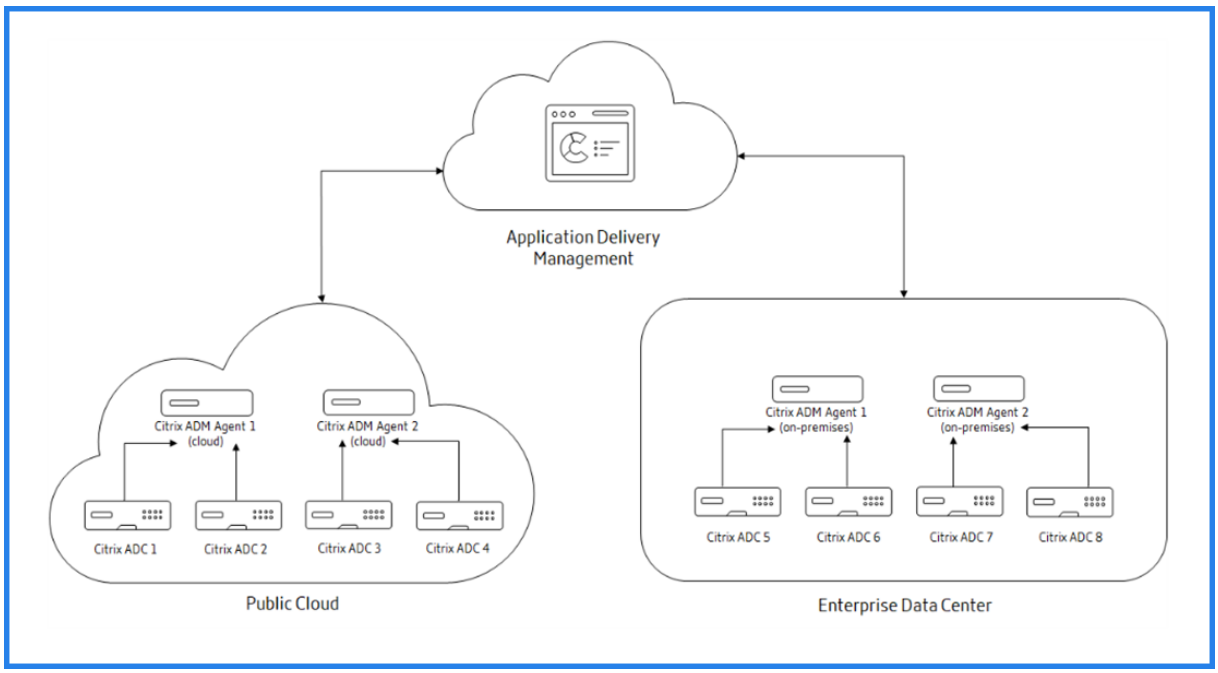
Les agents agissent en tant qu'intermédiaire entre le service Citrix ADM et les instances découvertes dans différents centres de données et clouds publics. Citrix ADM prend en charge le basculement de l'agent au sein d'un datacenter ou d'un cloud public.

Voici les avantages de l'installation d'agents :

- Les instances configurées à un agent envoient les données non traitées directement à l'agent au lieu du service Citrix ADM. L'agent effectue le premier niveau de traitement des données et envoie les données traitées au format compressé à Citrix ADM pour stockage.
- Les agents et les instances sont co-implantés dans le même centre de données ou cloud, de sorte que le traitement des données est 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 d'instances Citrix ADC bascule vers un autre agent disponible sur le même site.

Architecture

La figure suivante illustre les instances Citrix ADC configurées sur plusieurs agents dans un centre de données et un cloud public pour obtenir le basculement de l'agent :



Le cloud public dispose de quatre instances ADC et de deux agents ADM. Le centre de données d'entreprise dispose également de quatre instances ADC et de deux agents ADM. Chaque agent est configuré avec deux instances ADC.

Les agents reçoivent des données directement à partir des instances configurées. Une fois que l'agent reçoit les données, l'agent traite les données et les envoie au service Citrix ADM dans un format compressé. Les agents communiquent avec le serveur Citrix ADM via un canal sécurisé.

Sur le cloud public, lorsque **Citrix ADM Agent 1** devient inactif (état DOWN), le basculement de l'agent se produit. Le service Citrix ADM redistribue les instances ADC de **Citrix ADM Agent 1** avec **Citrix ADM Agent 2**. La redistribution d'instance se produit sur un centre de données d'entreprise si l'un des agents échoue dans le centre de données.

Pour installer un agent Citrix ADM, reportez-vous à la section Installer l'agent Citrix ADM.

Basculement sur incident de l'agent Citrix ADM

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

> **Important**
>
> - Le basculement de l'agent Citrix ADM ne prend pas en compte les instances CPX.
> - Assurez-vous que la fonctionnalité de basculement de l'agent est activée sur votre compte. Pour activer cette fonctionnalité, reportez-vous à la section Activer ou désactiver les fonctionnalités ADM.
> - Si un agent exécute un script, assurez-vous qu'il est présent sur tous les agents du site. Par conséquent, l'agent modifié peut exécuter le script après le basculement de l'agent.

Pour attacher un site à un agent dans l'interface graphique Citrix ADM :

1. Accédez à **Réseaux > Agents**.
2. Sélectionnez un agent que vous souhaitez attacher à un site.
3. Spécifiez le site dans la liste. Si vous souhaitez ajouter un nouveau site, cliquez sur **Ajouter**.
4. Cliquez sur **Enregistrer**.

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

Par exemple, deux agents 10.106.1xx.2x et 10.106.1xx.7x sont attachés et opérationnels sur le site Bangalore. Si un agent devient inactif, Citrix ADM le détecte et affiche l'état comme arrêté.

Lorsqu'un agent Citrix ADM devient inactif (état d'arrêt) dans un site, Citrix ADM attend quelques minutes que l'agent devienne actif (état de haut). Si l'agent reste inactif, Citrix ADM redistribue automatiquement les instances entre les agents disponibles sur le même site. Cette redistribution peut prendre environ 10-15 minutes.

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

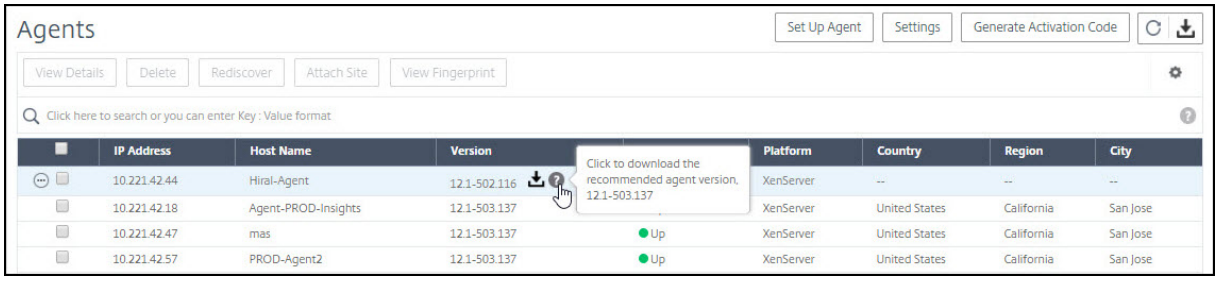
Les instances attachées et reconfigurées automatiquement aux agents du même site pour la destination d'interruptions, le serveur syslog et l'analyse.

Configuration des paramètres de mise à niveau de l'agent

April 29, 2021

Dans Citrix ADM, les agents s'exécutant sur la version logicielle 12.0 build 507.110 et ultérieure sont automatiquement mis à niveau vers des versions plus récentes et recommandées par Citrix ADM. L'agent est mis à niveau soit lorsqu'une nouvelle version est disponible, soit à un moment spécifié par vous.

Vous pouvez afficher la version actuelle et la version recommandée de vos agents en accédant à **Réseaux** > **Agents** .



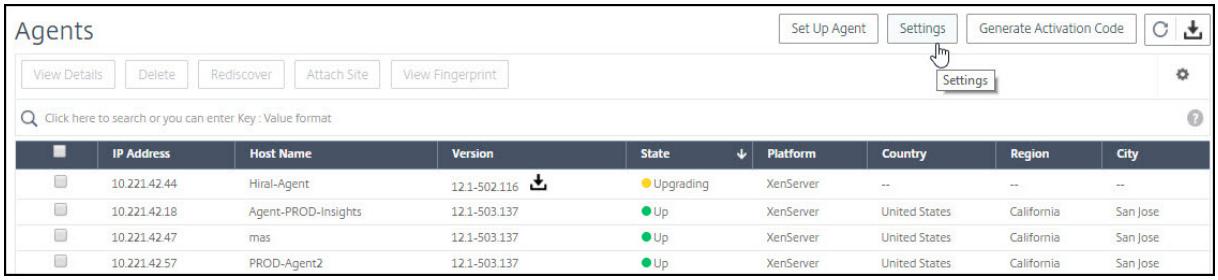
Par défaut, un agent est mis à niveau automatiquement lorsqu'une version plus récente est disponible. Toutefois, vous pouvez spécifier l'heure à laquelle vous souhaitez que la mise à niveau de l'agent se produise.

Si vous sélectionnez une heure spécifique, les agents sont mis à niveau à cette heure spécifiée, mais dans le fuseau horaire où vos agents sont déployés.

Pendant la mise à niveau, il peut y avoir un temps d'arrêt d'environ 30 minutes.

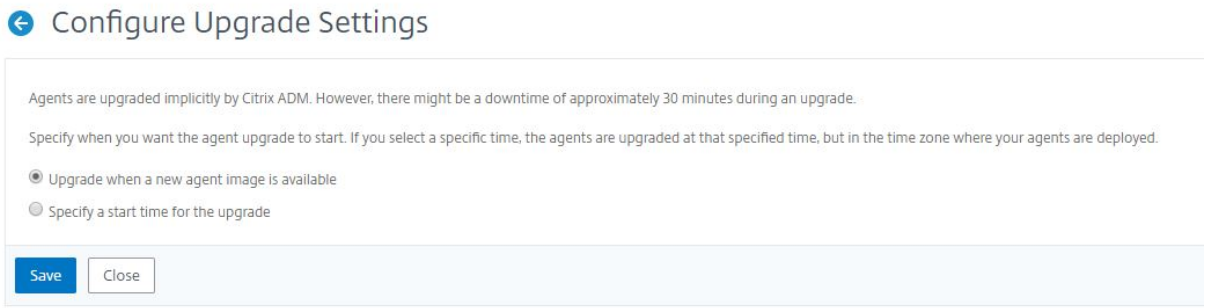
Pour configurer les paramètres de mise à niveau de l'agent :

Accédez à **Réseaux** > **Agents**, cliquez sur **Paramètres** .



Indiquez quand vous souhaitez que la mise à niveau de l'agent démarre. Vous pouvez choisir de mettre à niveau lorsqu'un nouvel agent est disponible ou définir une heure spécifique lorsque vous souhaitez que Citrix ADM met implicitement à niveau l'agent. L'heure que vous définissez est spécifique au fuseau horaire de l'agent.

Cliquez sur **Enregistrer** pour enregistrer vos paramètres. Ces paramètres persistent pour les futures mises à niveau de l'agent jusqu'à ce que vous modifiiez les paramètres.



Ajout d'instances

April 29, 2021

Vous pouvez ajouter des instances lors de la configuration de Citrix Application Delivery Management (Citrix ADM) pourpremière foisou version ultérieure.

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

- Citrix ADC MPX
- Citrix ADC VPX
- Citrix ADC SDX
- Citrix ADC CPX
- Citrix ADC BLX
- Citrix Gateway
- Citrix Secure Web Gateway

- Citrix SD-WAN WANOP

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.

> **Remarque**
>
> Citrix ADM prend uniquement en charge Citrix SD-WAN WANOP.

Spécifiez un profil d'instance que Citrix ADM peut utiliser pour accéder à l'instance. Ce profil d'instance contient le nom d'utilisateur et le mot de passe des instances que vous souhaitez ajouter au service. 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. Les informations d'identification de l'administrateur Citrix ADC par défaut définissent ce profil. 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 accéder aux interfaces graphiques des instances Citrix ADC à partir de Citrix ADM après avoir ajouté les instances dans Citrix ADM. Pour accéder aux instances de Citrix ADC à partir de Citrix ADM, vous devez être connecté au réseau Citrix.

> **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, l'adresse IP du cluster représente le cluster.
> - 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.

Pour ajouter une instance de Citrix ADC à Citrix ADM

> **Remarque**
>
> Effectuez cette tâche pour ajouter toutes les autres instances ADC à l'exception de l'instance CPX ADC.

1. Accédez à **Réseaux** > **Tableau de bord** et cliquez sur **Toutes les instances**. **Dans la page Instances**, cliquez sur **Nouveau** dans le coin supérieur droit de la page. Dans la page **Ajouter une instance**, dans **Type d'instance**, sélectionnez le type d'instance à ajouter.

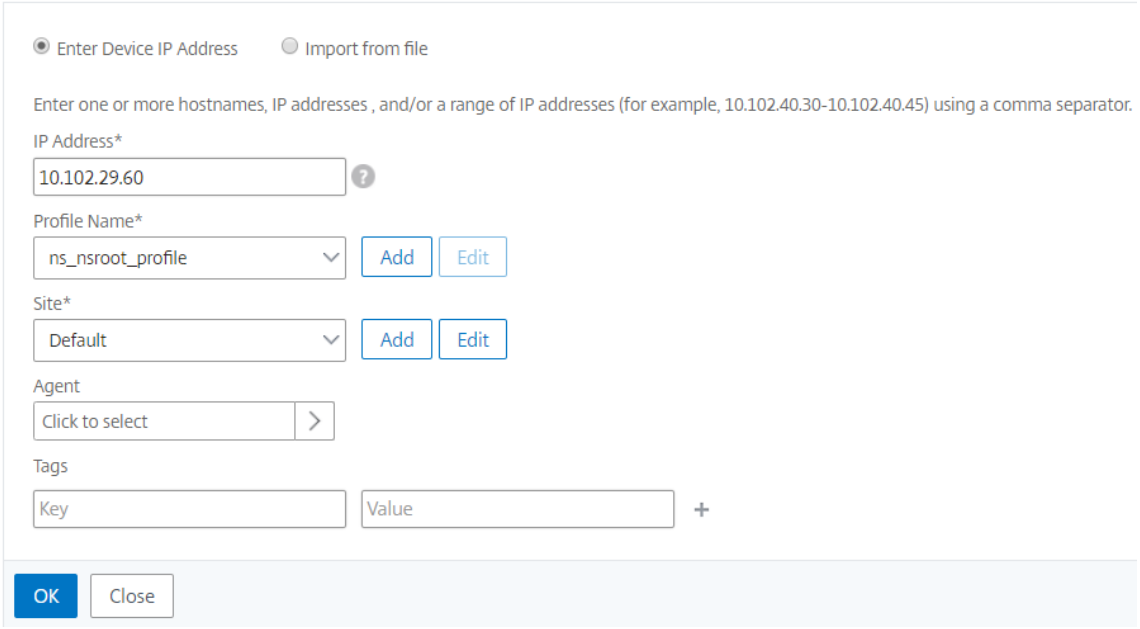
   Vous pouvez également accéder à **Réseaux**> **Instances**. Sous Instances, sélectionnez le type d'instance à ajouter (par exemple, Citrix ADC VPX), puis cliquez sur **Ajouter**.

2. 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.

3. (Facultatif) Sélectionnez **Activer l'ajout de périphérique en cas d'échec de connexion à la première fois**. Avec cette option, vous pouvez ajouter l'instance même sans informations d'identification valides.
4. Dans Nom du **profil**, sélectionnez le profil d'instance approprié ou créez un profil en cliquant sur l'icône **+** .
5. Dans **Site**, sélectionnez le site sur lequel vous souhaitez ajouter l'instance.
6. Dans **Agent**, sélectionnez l'agent auquel vous souhaitez associer les instances, puis cliquez sur **OK**.

   S'il n'y a qu'un seul agent configuré sur votre Citrix ADM, cet agent est sélectionné par défaut.



Pour ajouter une instance Citrix ADC CPX dans ADM

1. Accédez à **Réseaux** > **Instances**. Sous **Instances**, sélectionnez **Citrix ADC**et sélectionnez l'onglet CPX.
2. Cliquez sur **Ajouter**.
3. Sélectionnez l'une des options suivantes :

- **Entrez l'adresse IP du périphérique**. Spécifiez le nom d'hôte ou l'adresse IP de chaque instance, ou une plage d'adresses IP.
- **Importer à partir du fichier**. À partir de votre système local, téléchargez un fichier texte contenant les adresses IP de toutes les instances que vous souhaitez ajouter.

4. (Facultatif) Sélectionnez **Activer l'ajout de périphérique en cas d'échec de connexion à la première fois**. Avec cette option, vous pouvez ajouter l'instance même sans informations d'identification valides.
5. Dans le champ **IP routable /IP docker**, entrez l'adresse IP. L'adresse IP peut être soit l'instance Citrix ADC CPX (si elle est accessible), soit l'hôte Docker.
6. Dans le champ **Nom du profil**, sélectionnez le profil d'instance approprié ou créez un profil en cliquant sur l'icône +.

> **Remarque**
>
> Lorsque vous créez un profil, assurez-vous de spécifier les détails des ports HTTP, HTTPS, SSH et SNMP de l'hôte. Vous pouvez également spécifier la plage de ports publiés par l'hôte dans les champs Port de démarrage et Nombre de ports.

7. En option, sélectionnez le site sur lequel vous souhaitez déployer l'instance CPX. Vous pouvez également créer un site en cliquant sur **Ajouter**.
8. Si disponible, sélectionnez l'agent de service Citrix ADM dans la liste des agents.
9. Cliquez sur **OK** pour lancer le processus d'ajout d'instances à Citrix ADM.

> **Remarque**
>
> Si vous souhaitez redécouvrir une instance, effectuez les opérations suivantes :
>
> a) Accédez à **Réseaux** > **Instances** > **Citrix ADC** > **CPX** .
> b) Sélectionnez l'instance que vous souhaitez redécouvrir.
> c) **Dans la liste Sélectionner une action**, cliquez sur **Redécouvrir** .

Pour ajouter une instance Citrix ADC BLX autonome dans Citrix ADM

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

1. Accédez à **Réseaux** > **Instances** > **Citrix ADC**.
2. Dans l'onglet **BLX**, cliquez sur **Ajouter**.
3. (Facultatif) Sélectionnez **Activer l'ajout de périphérique en cas d'échec de connexion à la première fois**. Avec cette option, vous pouvez ajouter l'instance même sans informations d'identification valides.

4. Sélectionnez l'option **Autonome** dans la liste **Type d'instance**.
5. Dans le champ **Adresse IP**, spécifiez l'adresse IP de l'instance BLX.
6. Dans le champ **Adresse IP de l'hôte**, spécifiez l'adresse IP du serveur Linux sur lequel l'instance BLX est hébergée.
7. Dans la liste **Nom du profil**, sélectionnez le profil approprié pour une instance BLX ou créez un profil.

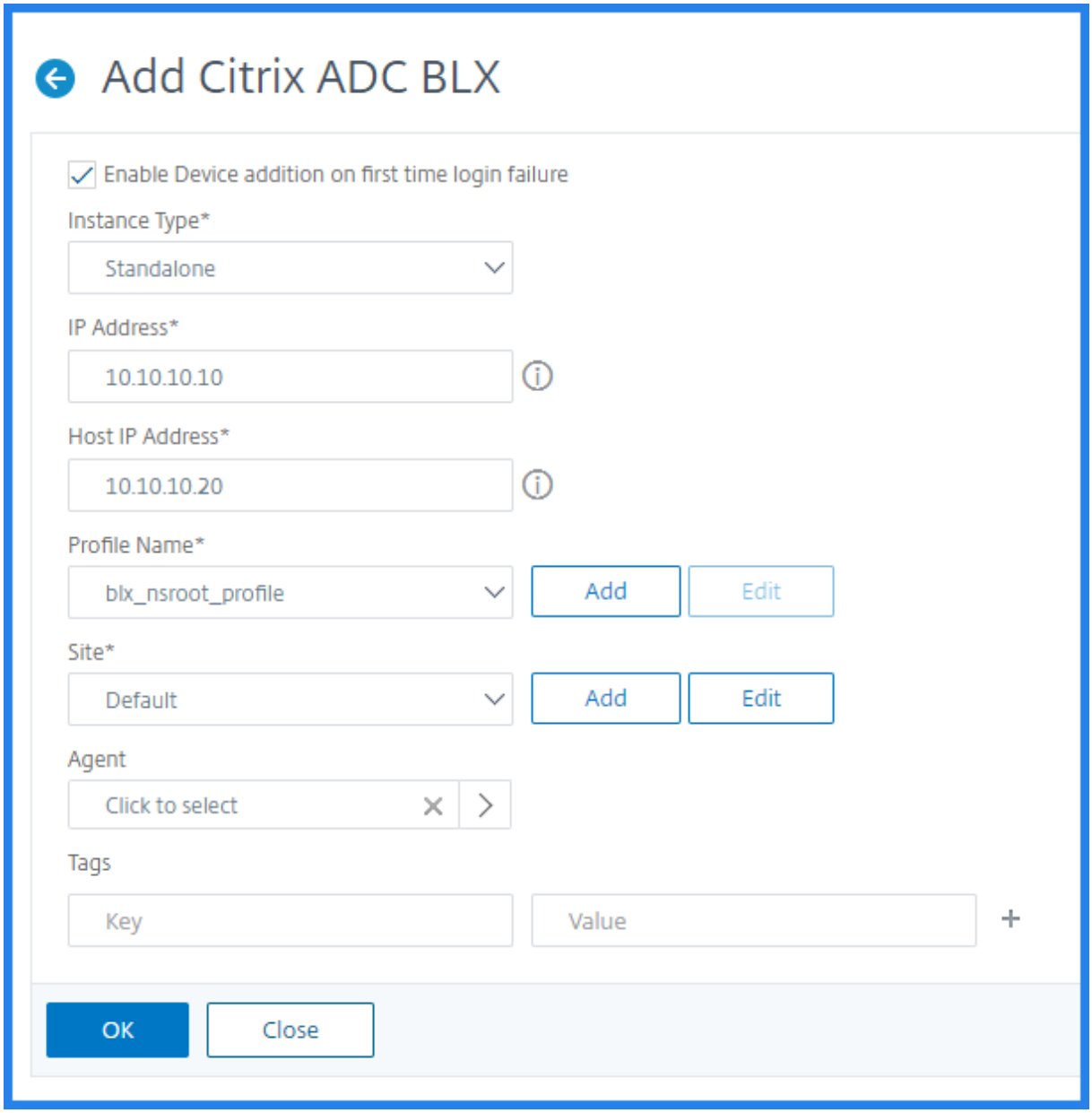
   Pour créer un profil, cliquez sur **Ajouter**.

   > **Important**
   >
   > Vérifiez que vous avez spécifié le nom d'utilisateur hôte et le mot de passe du serveur Linux dans le profil.

8. Dans la liste **Site**, sélectionnez le site sur lequel vous souhaitez ajouter une instance.

   Si vous souhaitez ajouter un site, cliquez sur **Ajouter**.
9. Dans la liste **Agent**, sélectionnez l'agent Citrix ADM auquel vous souhaitez associer l'instance.

   Si un seul agent est configuré sur votre Citrix ADM, cet agent est sélectionné par défaut.
10. Cliquez sur **OK**.



Pour ajouter des instances BLX Citrix ADC haute disponibilité dans Citrix ADM

Instances Citrix ADC BLX haute disponibilité qui s'exécutent sur différents serveurs Linux hôtes. Un serveur Linux ne peut pas héberger plus d'une instance BLX.

1. Dans l'onglet **BLX**, cliquez sur **Ajouter**.
2. (Facultatif) Sélectionnez **Activer l'ajout de périphérique en cas d'échec de connexion à la première fois**. Avec cette option, vous pouvez ajouter l'instance même sans informations d'identification valides.
3. Sélectionnez l'option **Haute disponibilité** dans la liste **Type d'instance**.

4. Dans le champ **Adresse IP**, spécifiez l'adresse IP de l'instance BLX.
5. Dans le champ **Adresse IP de l'hôte**, spécifiez l'adresse IP du serveur Linux sur lequel l'instance BLX est hébergée.
6. Dans le champ **Adresse IP homologue**, spécifiez l'adresse IP de l'instance BLX homologue.
7. Dans le champ **Adresse IP de l'hôte homologue**, spécifiez l'adresse IP du serveur Linux où l'instance BLX homologue est hébergée.
8. Dans la liste **Nom du profil**, sélectionnez le profil approprié pour une instance BLX ou créez un profil.

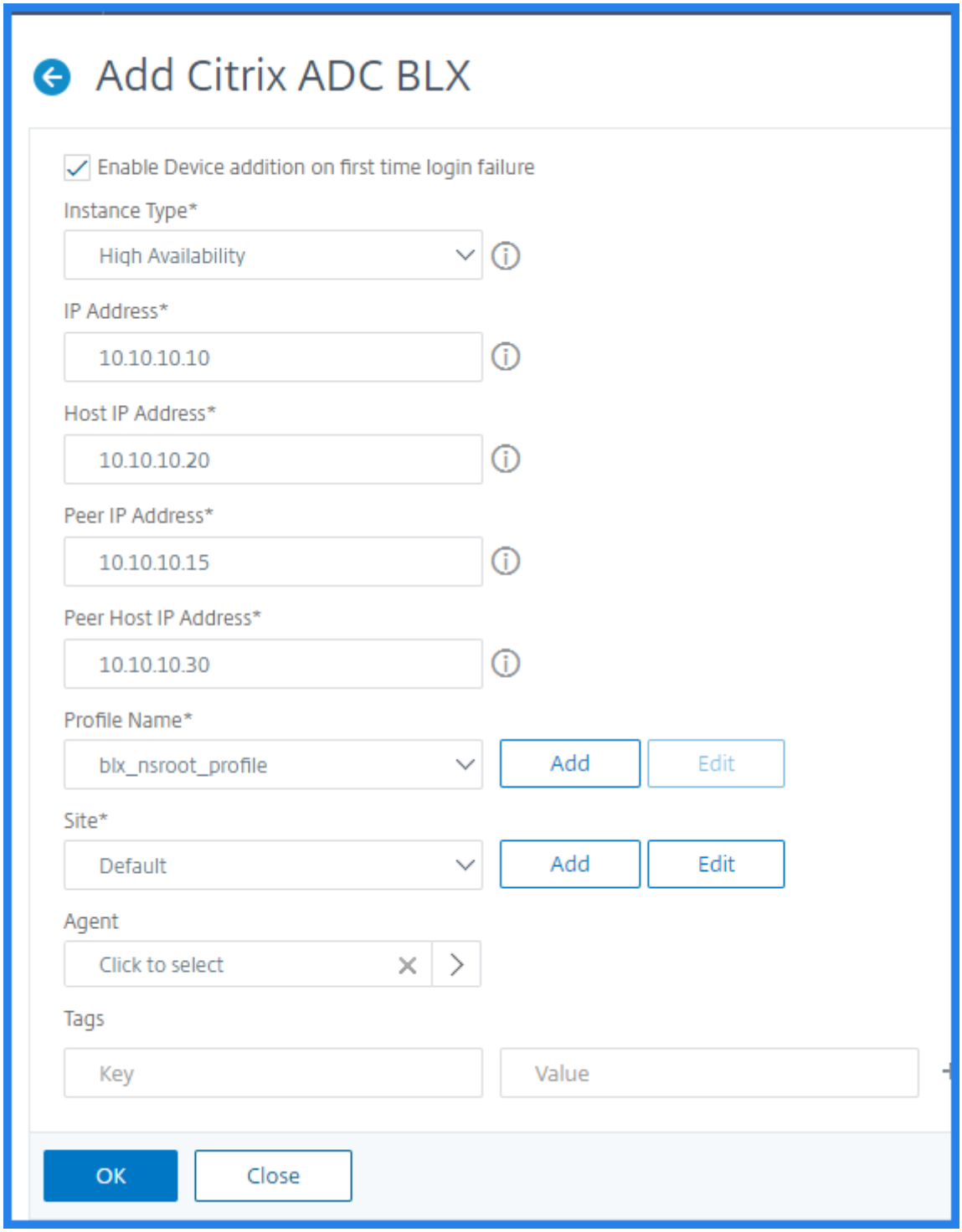
   Pour créer un profil, cliquez sur **Ajouter**.

   > **Important**
   >
   > Vérifiez que vous avez spécifié le nom d'utilisateur hôte et le mot de passe du serveur Linux dans le profil.

9. Dans la liste **Site**, sélectionnez le site sur lequel vous souhaitez ajouter une instance.

   Si vous souhaitez ajouter un site, cliquez sur **Ajouter**.
10. Dans la liste **Agent**, sélectionnez l'agent Citrix ADM auquel vous souhaitez associer l'instance.

    Si un seul agent est configuré sur votre Citrix ADM, cet agent est sélectionné par défaut.
11. Cliquez sur **OK**.

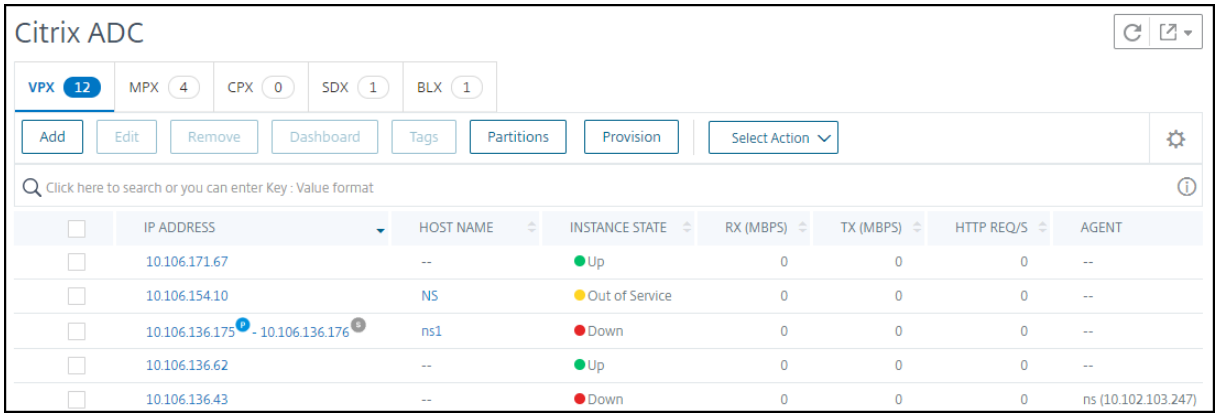


Pour accéder à une interface graphique d'instance à partir de Citrix ADM

1. Accédez à **Réseaux > Instances** > **Citrix ADC** .
2. Sélectionnez le type d'instance auquel vous souhaitez accéder (par exemple, VPX, MPX, CPX,

SDX ou BLX).

3. Cliquez sur l'adresse IP Citrix ADC ou le nom d'hôte requis.



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

Résoudre les avertissements d'instance

Un signe d'avertissement apparaît sur l'instance pour les raisons suivantes :

- **Échec de la connexion** - Lorsque vous ajoutez une instance sans informations d'identification valides, elle apparaît en état DOWN, avec un avertissement d'échec de connexion. Spécifiez les informations d'identification correctes pour gérer l'instance dans ADM.

  Si l'instance n'est pas sous licence, l'option **License** apparaît lorsque vous sélectionnez l'instance. Cliquez sur **License** pour appliquer la licence à une instance à partir du pool de licences.

- **Instance sans licence avec profil HTTPS** - Si une instance non licenciée utilise uniquement une connexion HTTPS, appliquez une licence à une instance à partir de l'interface graphique ADC.

Ajout d'instances HAProxy

April 29, 2021

Vous pouvez ajouter une instance HaProxy provisionnée sur un hôte en fournissant les détails de l'hôte lors de la configuration de Citrix Application Delivery Management (Citrix ADM) pour le première fois ou une version ultérieure.

Citrix ADM prend en charge HAProxy version 1.6.3 ou ultérieure et vous pouvez ajouter des instances HAProxy provisionnées sur les hôtes suivants à Citrix ADM :

- Ubuntu 14.0 ou version ultérieure

- Red Hat Enterprise Linux (RHEL) 6.0 ou version ultérieure
- SUSE 11.0 ou version ultérieure
- CentOS 6.0 ou version ultérieure
- AMI Amazon Linux

> **Remarque**
>
> Assurez-vous que l'hôte n'est pas configuré avec une chaîne d'invite personnalisée pour le shell. Le shell doit avoir **$** ou **#** comme chaîne d'invite.

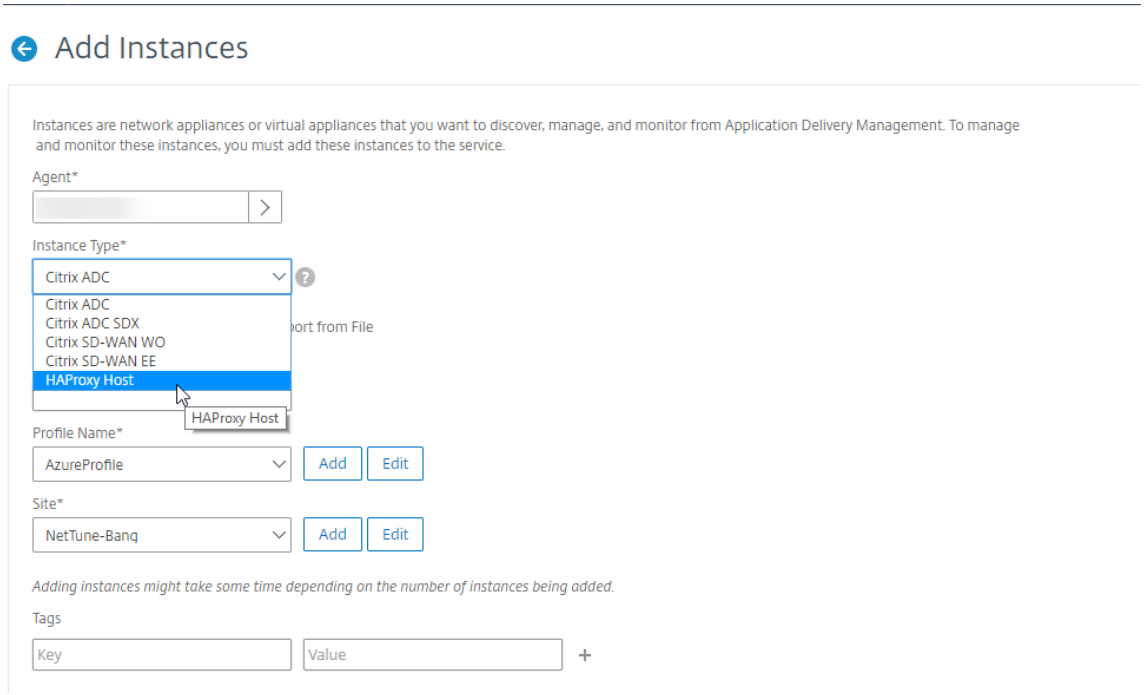
Pour ajouter des instances HAProxy, vous devez spécifier l'adresse IP de l'hôte sur lequel vous avez provisionné les instances HAProxy. Vous devez ensuite spécifier un profil HAProxy que Citrix ADM peut utiliser pour accéder à l'hôte. Ce profil HaProxy contient le nom d'utilisateur et le mot de passe de l'hôte que vous souhaitez ajouter au service.

> **Remarque**
>
> Assurez-vous que le compte d'utilisateur associé au nom d'utilisateur a :
>
> - Privilèges permettant d'exécuter la commande ps pour répertorier toutes les instances HAProxy sur l'hôte.
> - Autorisation de redémarrer l'instance HAProxy sur l'hôte.

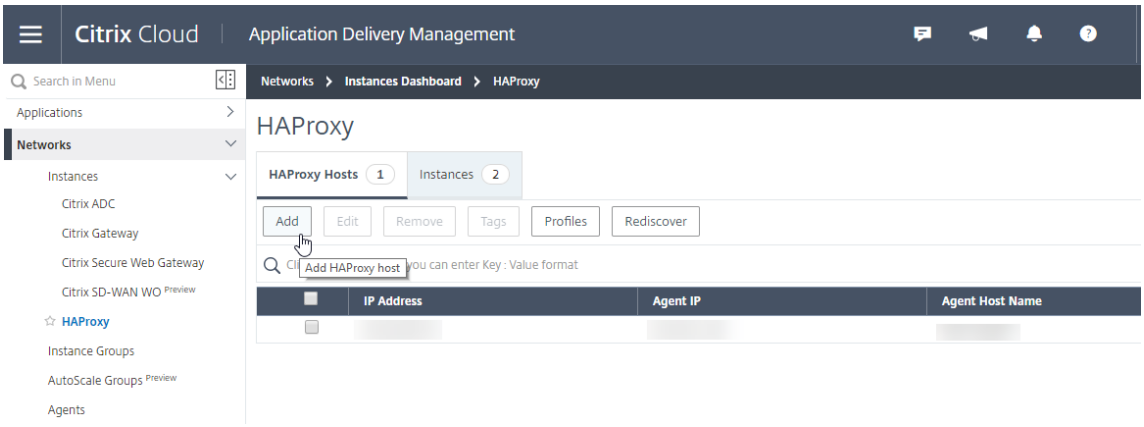
Après avoir ajouté l'hôte sur lequel vous avez provisionné les instances HAProxy à Citrix ADM, Citrix ADM accède à l'hôte à l'aide du protocole SSH. Il détecte automatiquement les instances HAProxy provisionnées sur l'hôte et les ajoute à l'inventaire Citrix ADM. Il découvre également tous les fronts, backends et serveurs configurés sur les instances HaProxy, et traite les fronts comme des applications découvertes.

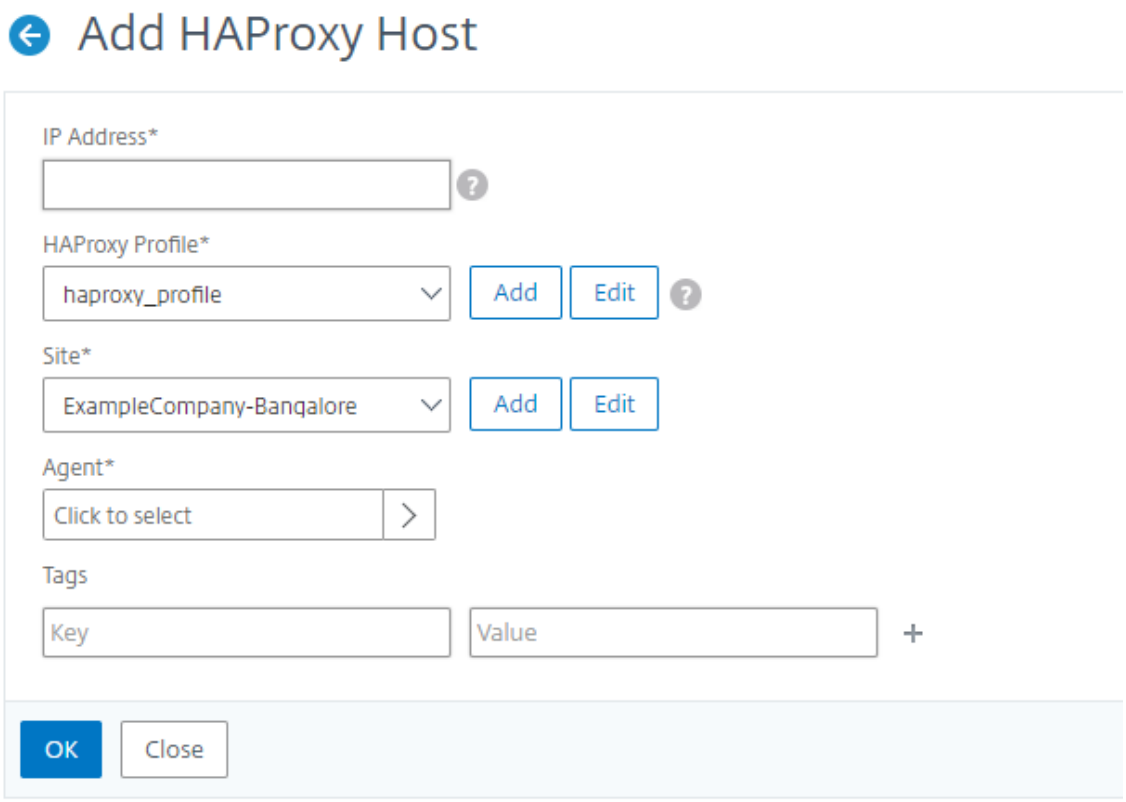
Pour ajouter des instances HAProxy à Citrix ADM :

1. Accédez à **Réseaux > Instances**, puis cliquez sur Nombre d'instances. Dans la section Instances, cliquez sur **Ajouter** dans le coin supérieur droit de la page. Dans la page Ajouter des instances, dans la liste déroulante **Type d'instance**, sélectionnez **Hôte HAProxy** .



Vous pouvez également accéder à **Réseaux > Instances**. Sous Instances, sélectionnez **HAProxy** et cliquez sur **Ajouter** .





2. Dans le champ **Adresse IP**, entrez l'adresse IP de l'hôte sur lequel vous avez provisionné les instances HAProxy.
3. Dans la liste déroulante **Profile HAProxy**, sélectionnez un profil HAProxy existant ou créez et sélectionnez un nouveau profil HAProxy. Pour créer un profil HaProxy, cliquez sur l'icône **+** .
4. Dans la boîte de dialogue **Ajouter un profil HAProxy**, procédez comme suit :
   a) Dans le champ **Nom du profil**, entrez un nom unique pour le profil HAProxy.
   b) Dans le champ **Nom d'utilisateur**, entrez le nom d'utilisateur utilisé pour accéder à l'hôte à l'aide du protocole SSH.

> **Remarque**
>
> Assurez-vous que le compte d'utilisateur associé au nom d'utilisateur dispose des éléments suivants :
>
> ```
> 1      -  Privilèges permettant d'exécuter la commande ps
>           pour répertorier toutes les instances HAProxy sur l
>           'hôte.
> ```

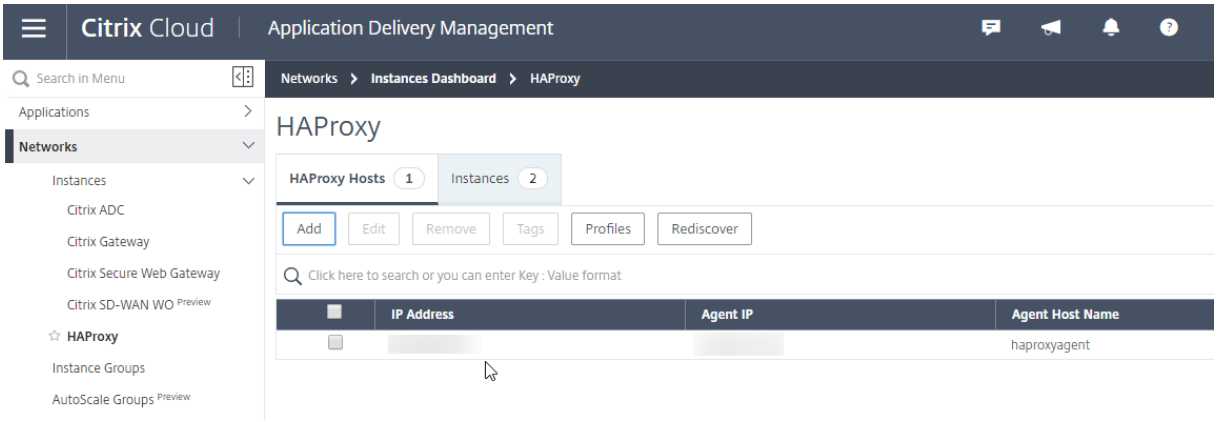

> • Autorisation de redémarrer l'instance HAProxy sur l'hôte.

c) Dans le champ **Mot de passe**, entrez le mot de passe de l'hôte.

d) Cliquez sur **Créer**.

5. Spécifiez un site pour l'instance.
6. Dans la liste déroulante **Agent**, sélectionnez l'agent auquel vous souhaitez associer les instances.
7. Dans le champ Tags, spécifiez une clé et les valeurs associées pour l'instance HAProxy. Les balises vous aident à classer et à identifier les instances. Par exemple, spécifiez Emplacement comme clé et Bangalore comme valeur. Vous pouvez également ajouter plusieurs valeurs pour une clé. Séparez les multiples valeurs par des virgules.
8. Sélectionnez **OK**.

Citrix ADM détecte les instances HAProxy provisionnées sur l'hôte et vous pouvez afficher toutes les instances HAProxy sous l'onglet **Instances** de la page **Réseaux > Instances > HAProxy** .



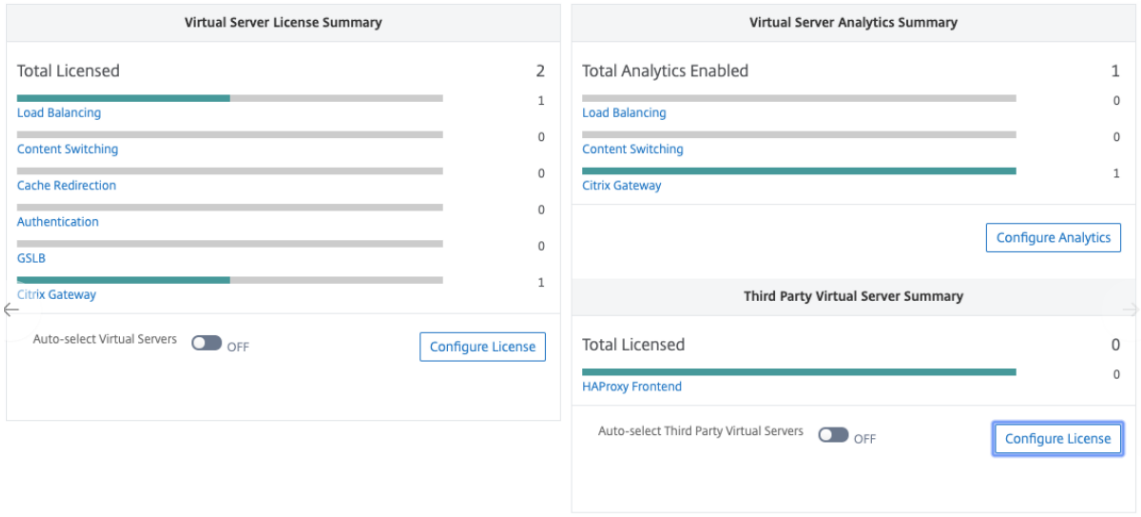
Gérer les licences et activer les analyses sur les serveurs virtuels

April 29, 2021

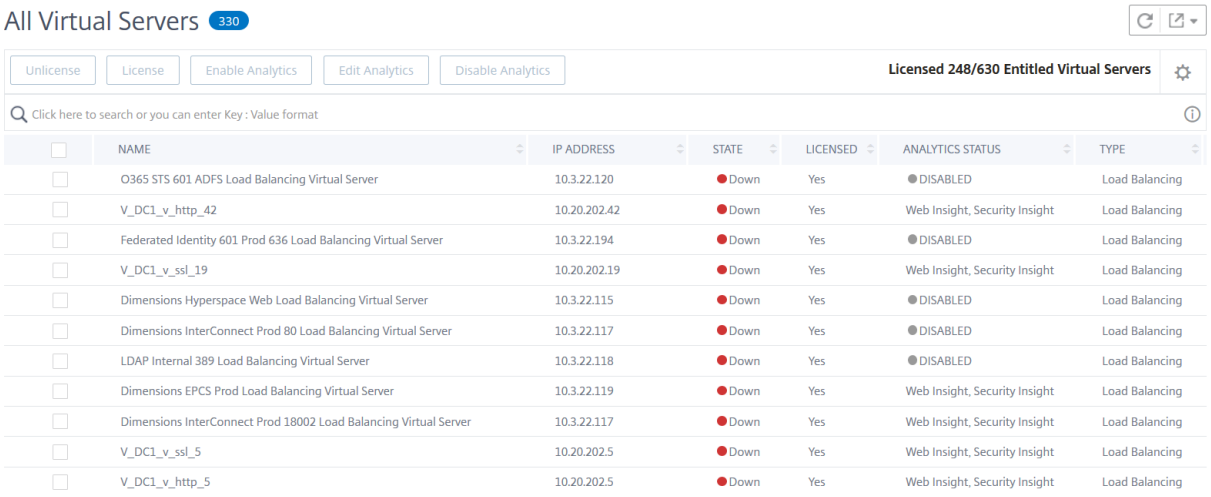
Le processus d'activation de l'analyse est simplifié. Vous pouvez désormais concéder une licence au serveur virtuel et activer l'analyse dans un flux de travail unique.

Accédez à **Compte** > **Abonnements** à :

- Afficher le **résumé des licences de serveur virtuel**
- Afficher le **résumé de l'analyse des serveurs virtuels**



Lorsque vous cliquez sur **Configurer la licence** ou **Configurer Analytics**, la page **Tous les serveurs virtuels**s'affiche.



Sur la page **Tous les serveurs virtuels**, vous pouvez :

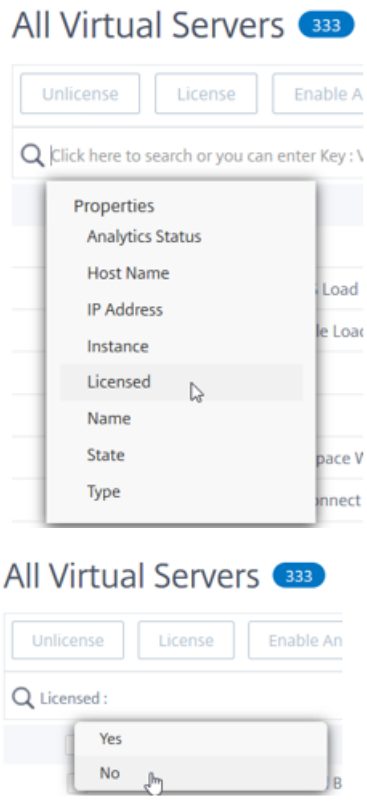
- Appliquer une licence pour les serveurs virtuels sans licence
- Supprimer la licence pour les serveurs virtuels sous licence
- Activer l'analyse sur les serveurs virtuels sous licence
- Modifier les analyses
- Désactiver l'analyse

> **Remarque**
>
> Les serveurs virtuels pris en charge pour activer l'analyse sont l'équilibrage de charge, la commutation de contenu et Citrix Gateway.

Gestion des licences sur les serveurs virtuels

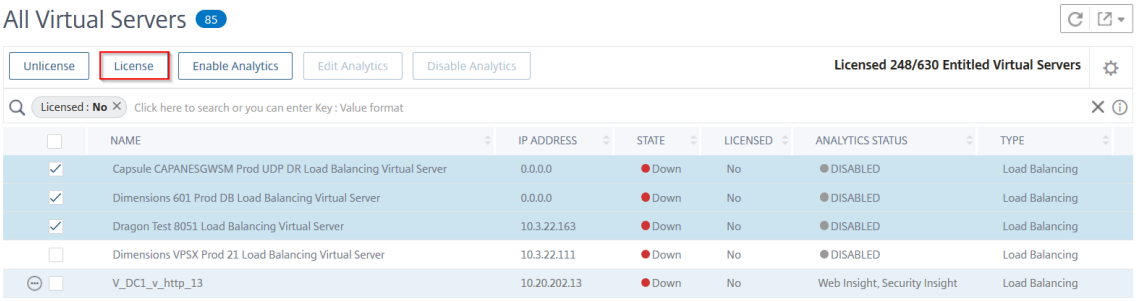
Pour concéder une licence aux serveurs virtuels, à partir de la page **Tous les serveurs virtuels** :

1. Cliquez sur la barre de recherche, sélectionnez **Licence**et sélectionnez **Non**.



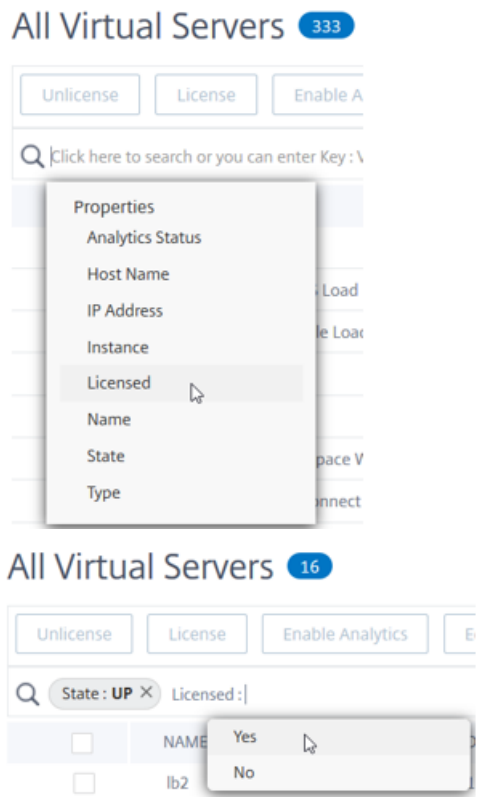
   Le filtre est maintenant appliqué et seuls les serveurs virtuels sans licence sont affichés.

2. Sélectionnez les serveurs virtuels, puis cliquez sur **Licence**.

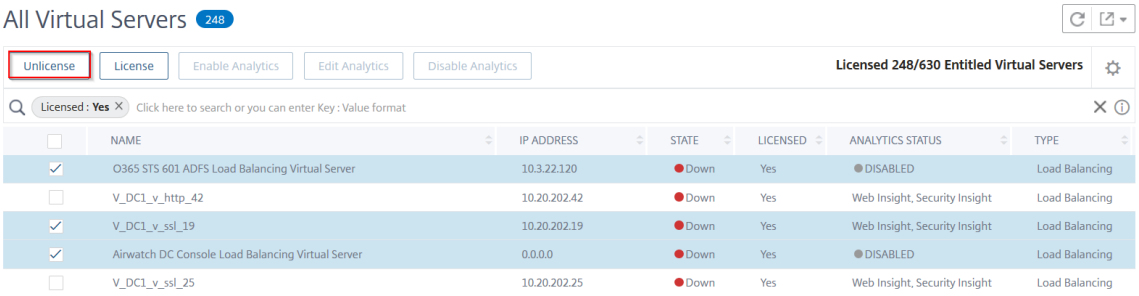


Pour annuler la licence des serveurs virtuels, à partir de la page **Tous les serveurs virtuels** :

1. Cliquez sur la barre de recherche, sélectionnez **Licence**, puis **Oui**.



2. Sélectionnez les serveurs virtuels et cliquez sur **Unlicense**.



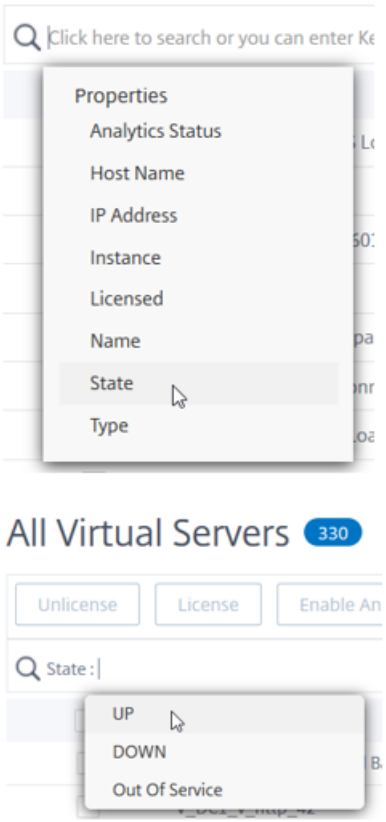
Activer l'analyse

Les conditions préalables à l'activation de l'analyse pour les serveurs virtuels sont les suivantes :

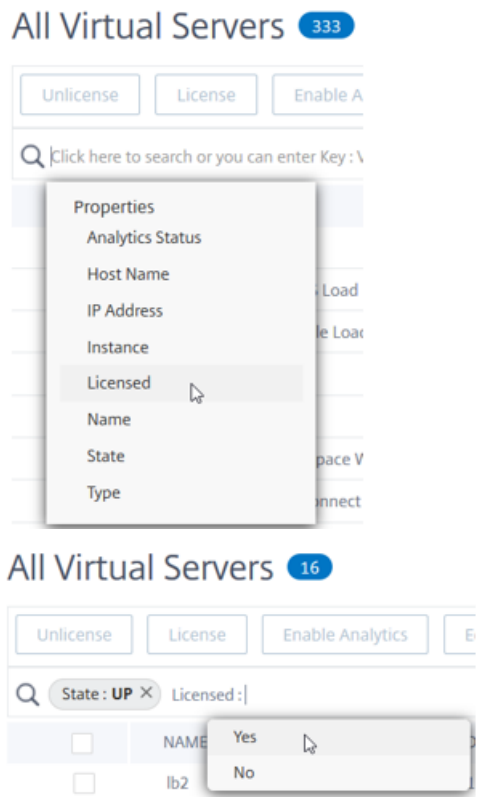
- Assurez-vous que les serveurs virtuels sont **sous licence**
- Assurez-vous que l'état de l'analyse est **désactivé**
- Assurez-vous que les serveurs virtuels sont en état **UP**

Vous pouvez filtrer les résultats pour identifier les serveurs virtuels mentionnés dans les conditions préalables.

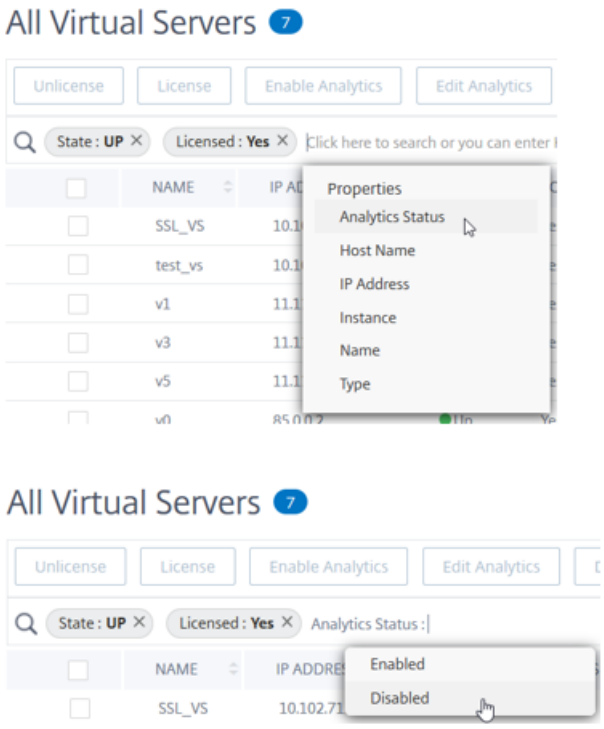
1. Cliquez sur la barre de recherche, sélectionnez **État**, puis sélectionnez **UP**.



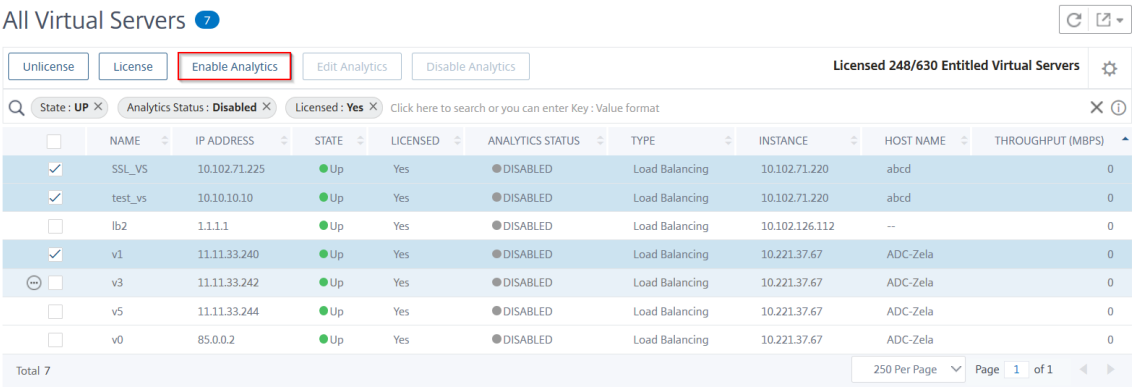
2. Cliquez sur la barre de recherche, sélectionnez **Licence**, puis sélectionnez **Oui**.



3. Cliquez sur la barre de recherche, sélectionnez **État de l'analyse**, puis sélectionnez **Désactivé**.



4. Après avoir appliqué les filtres, sélectionnez les serveurs virtuels, puis cliquez sur **Activer Analytics**.



5. Dans la fenêtre **Activer Analytics** :

   a) Sélectionnez les types d'informations (Web Insight ou Security Insight)

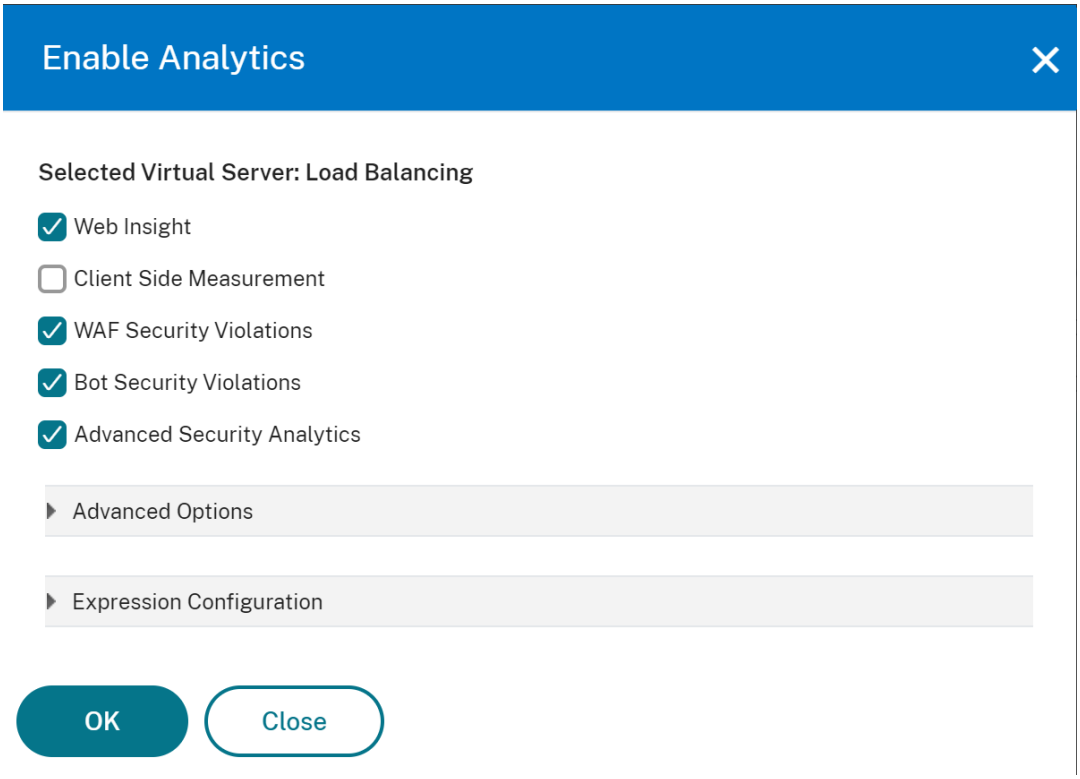
   b) Sélectionnez **Logstream** ou **IPFIX** comme mode de transport

> **Remarque**
>
> Pour Citrix ADC 12.0 ou version antérieure, **IPFIX** est l'option par défaut pour le mode de transport. Pour Citrix ADC 12.0 ou version ultérieure, vous pouvez sélectionner **Logstream** ou **IPFIX** comme mode de transport.

> Pour plus d'informations sur **IPFIX** et **Logstream**, reportez-vous à la section **Présentation de Logstream**.

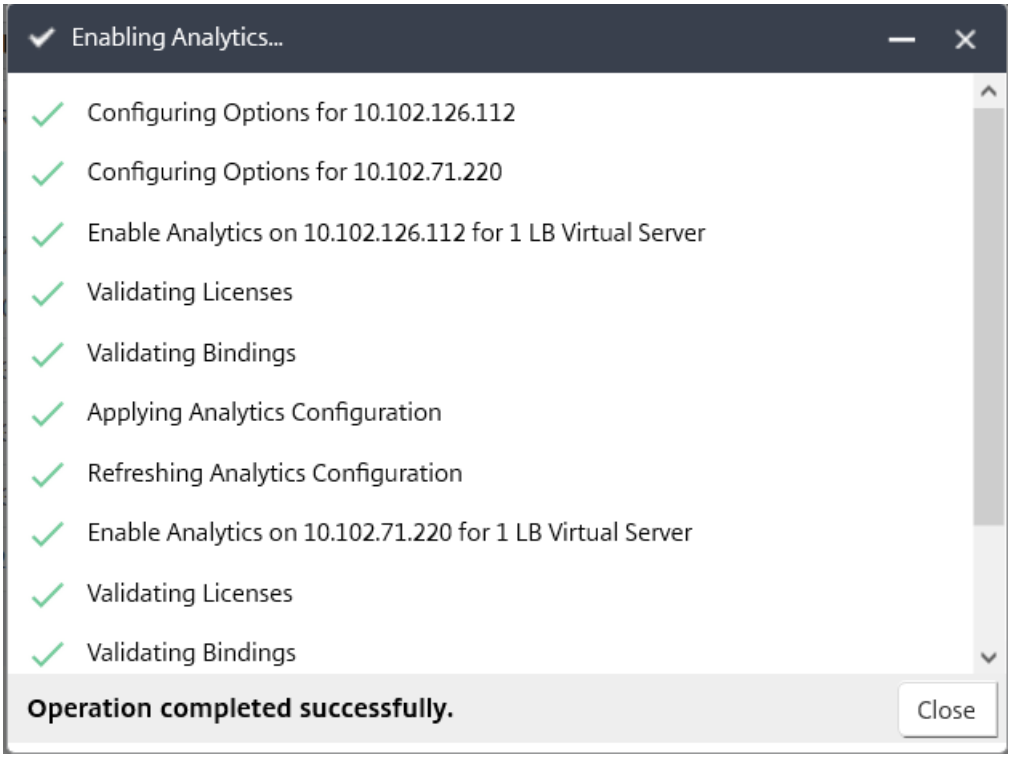
c) L'expression est true par défaut

d) Cliquez sur **OK**.



> **Remarque**
>
> ```
> - Si vous sélectionnez des serveurs virtuels qui ne sont pas sous licence, Citrix ADM accorde d'abord les licences à ces serveurs virtuels, puis active l 'analyse.
>
> - Pour les partitions d'administration, seul **Web Insight** est pris en charge
> ```
>
> - Pour les serveurs virtuels tels que la **redirection de cache**, **l'authentification**et **GSLB**, vous ne pouvez pas activer l'analyse. Un message d'erreur s'affiche.

Après avoir cliqué sur **OK**, Citrix ADM traite pour activer l'analyse sur les serveurs virtuels sélectionnés.

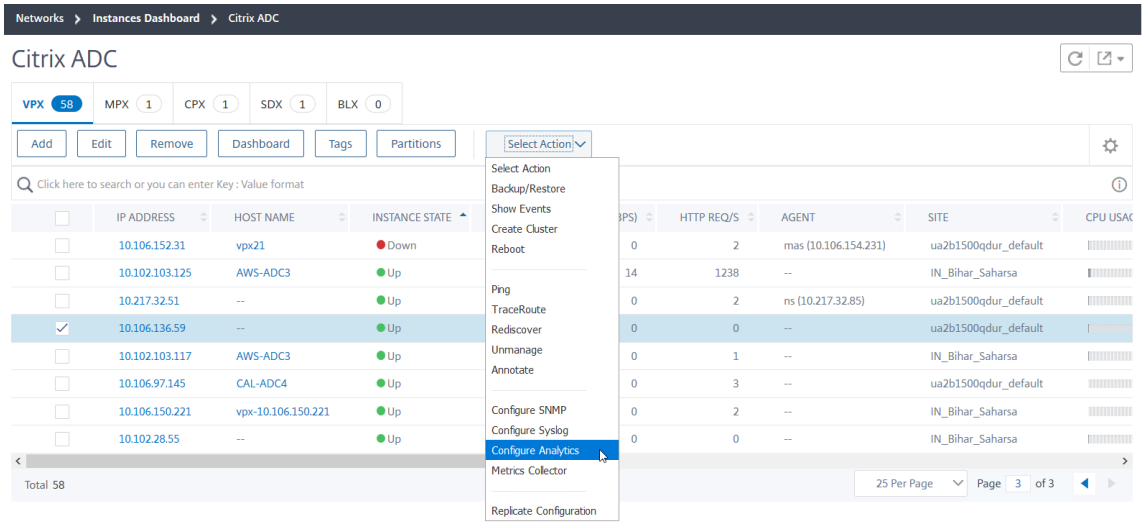


> **Remarque**
>
> Citrix ADM utilise Citrix ADC SNIP pour **Logstream** et NSIP pour **IPFIX**. Si un pare-feu est activé entre l'agent Citrix ADM et l'instance Citrix ADC, assurez-vous d'ouvrir le port suivant pour permettre à l'agent Citrix ADM de collecter le trafic AppFlow :
>
> | Mode de transport | IP source | Type | Port|
> |—| —|—|
> | **IPFIX** | NSIP | UDP | 4739|
> | **Logstream** | SNIP | TCP | 5557|

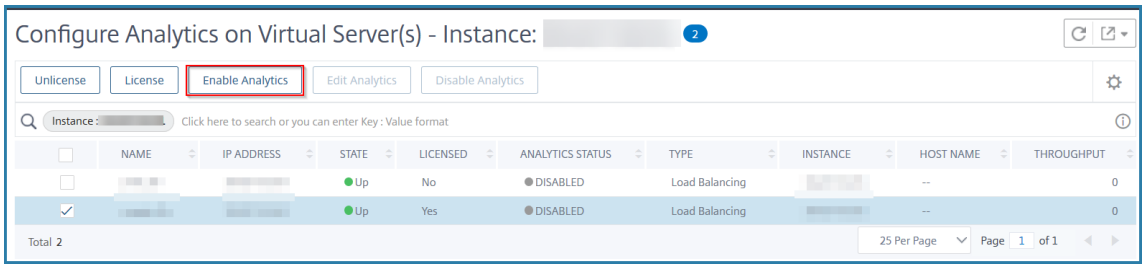
Activer l'analyse pour une instance

Vous pouvez également activer l'analyse pour une instance particulière :

1. Accédez à **Réseaux** > **Instances** > **Citrix ADC**, puis sélectionnez le type d'instance. Par exemple, VPX.
2. Sélectionnez l'instance et dans la liste **Sélectionner une action**, sélectionnez **Configurer Analytics**.



3. Sur la page **Configurer Analytics on Virtual Server (s)**, sélectionnez le serveur virtuel et cliquez sur **Activer Analytics**.



4. Dans la fenêtre **Activer Analytics** :

   a) Sélectionnez le type d'aperçu (Web Insight, Security Insight, Bot Insight)

   b) Sélectionnez **Logstream** ou **IPFIX** comme mode de transport

   > **Remarque**
   >
   > Pour Citrix ADC 12.0 ou version antérieure, **IPFIX** est l'option par défaut pour le mode de transport. Pour Citrix ADC 12.0 ou version ultérieure, vous pouvez sélectionner **Logstream** ou **IPFIX** comme mode de transport.
   >
   > Pour plus d'informations sur **IPFIX** et **Logstream**, reportez-vous à la section **Présentation de Logstream**.

   c) L'expression est true par défaut

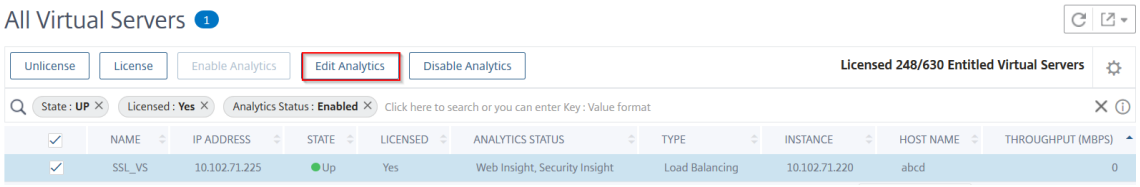
   d) Cliquez sur **OK**

   .

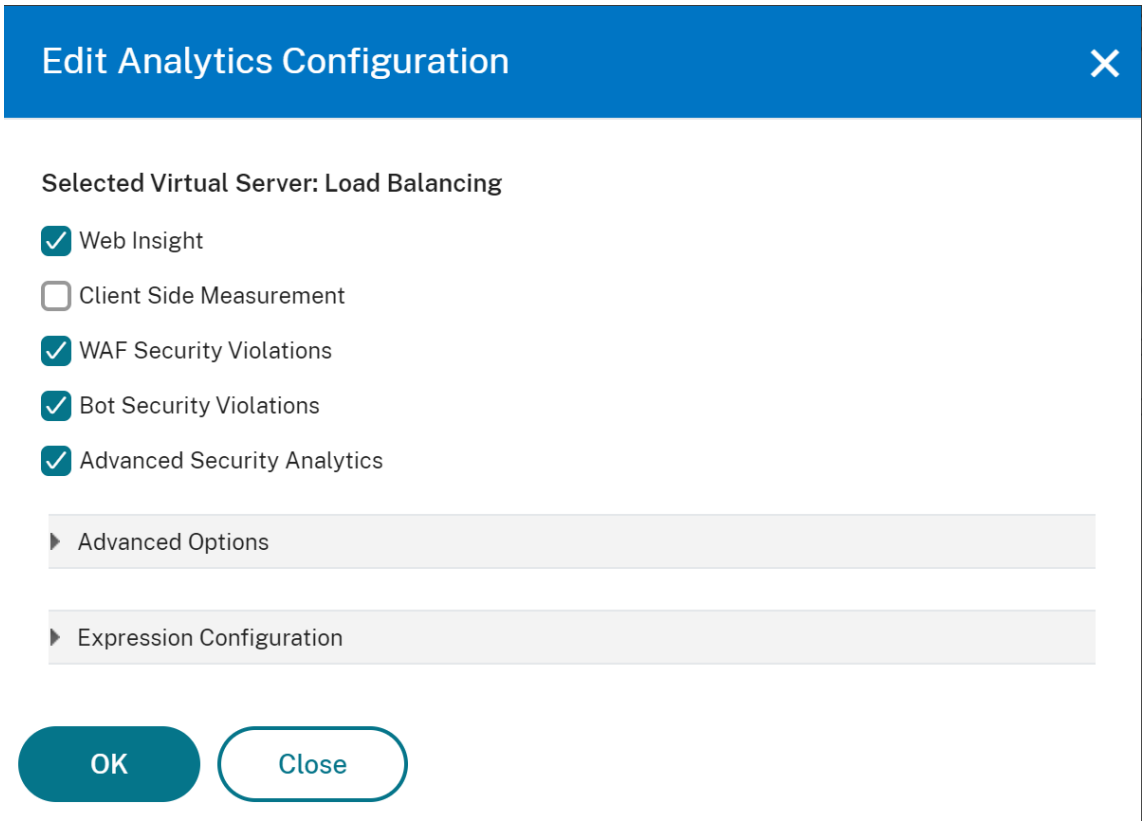
Modifier les analyses

Pour modifier les analyses sur les serveurs virtuels :

1. Sélectionner les serveurs virtuels
2. Cliquez sur **Modifier les analyses**



3. Modifiez les paramètres à appliquer dans la fenêtre **Modifier la configuration d'Analytics**
4. Cliquez sur **OK**.



Modifier les analyses d'une instance

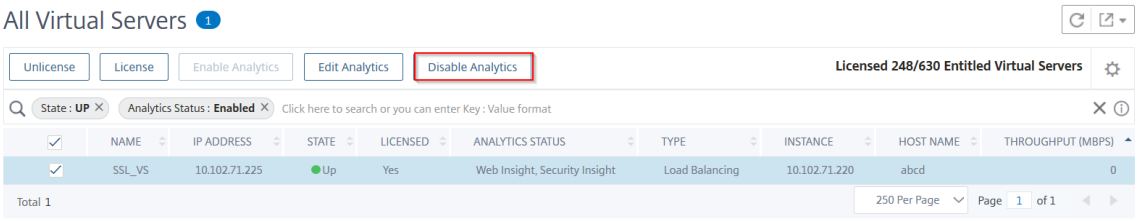
Vous pouvez également désactiver l'analyse pour une instance particulière :

1. Accédez à **Réseau > Instance > Citrix ADC** et sélectionnez le type d'instance. Par exemple, VPX.
2. Sélectionnez l'instance et cliquez sur **Modifier Analytics**

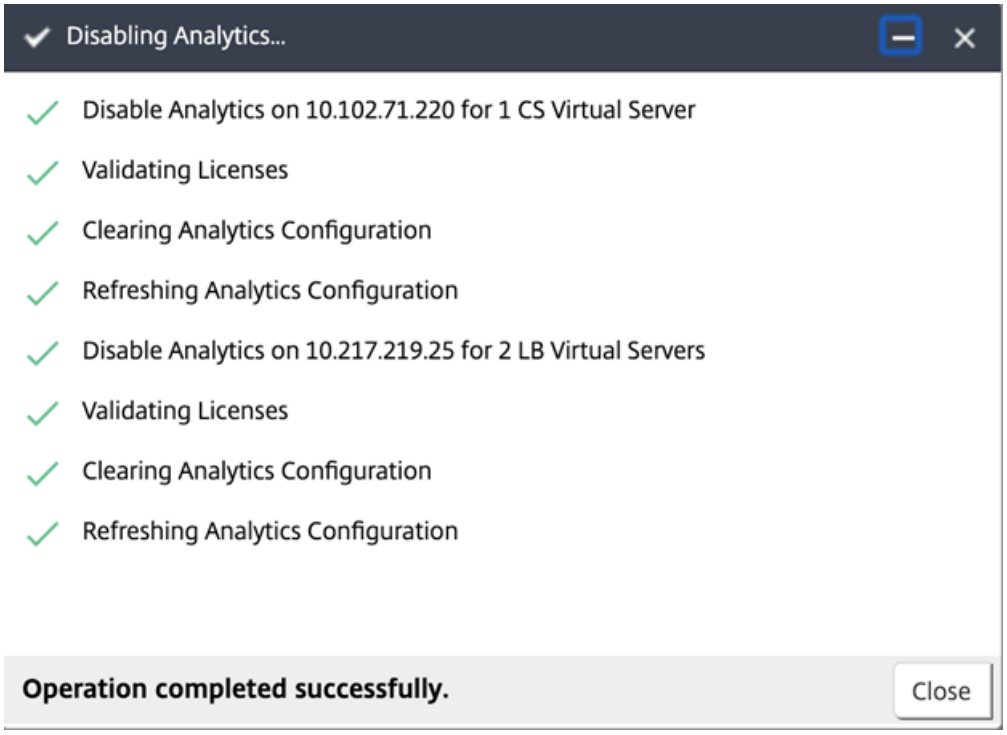
Désactiver l'analyse

Pour désactiver l'analyse sur les serveurs virtuels sélectionnés :

1. Sélectionner les serveurs virtuels
2. Cliquez sur **Désactiver l'analyse**



Citrix ADM désactive les analyses sur les serveurs virtuels sélectionnés



Configuration de syslog sur les instances

April 29, 2021

Le protocole syslog fournit un transport permettant aux instances de Citrix ADC d'envoyer des messages de notification d'événement à Citrix Application Delivery Management (Citrix ADM), qui est configuré en tant que collecteur ou serveur syslog pour ces messages.

Vous pouvez surveiller les événements syslog générés sur vos instances de Citrix ADC si vous avez configuré votre périphérique pour rediriger tous les messages syslog vers Citrix ADM. Pour surveiller les événements syslog, vous devez d'abord configurer Citrix ADM en tant que serveur syslog pour votre

instance Citrix ADC. Une fois l'instance configurée, tous les messages syslog sont redirigés vers Citrix ADM, de sorte que ces journaux puissent être affichés à l'utilisateur de manière structurée.

Syslog utilise le protocole UDP (User Datagram Protocol), port 514, pour la communication, et comme UDP est un protocole sans connexion, il ne fournit aucun accusé de réception aux instances. La taille du paquet syslog est limitée à 1024 octets et contient les informations suivantes :

- Installation
- Gravité
- Nom d'hôte
- Horodatage
- Message

Dans Citrix ADM, vous devez configurer les niveaux de gravité des ressources et des journaux sur les instances.

- **Facilité** - Les messages Syslog sont largement classés en fonction des sources qui les génèrent. Ces sources peuvent être le système d'exploitation, le processus ou une application. Ces catégories sont appelées installations et sont représentées par des entiers. Par exemple, 0 est utilisé par les messages du noyau, 1 est utilisé par les messages de niveau utilisateur, 2 est utilisé par le système de messagerie, etc. Les installations d'utilisation locale (de local0 à local7) ne sont pas réservées et sont disponibles pour un usage général. Par conséquent, les processus et les applications qui n'ont pas de valeurs d'installation préassignées peuvent être dirigés vers n'importe laquelle des huit installations d'utilisation locale.
- **Gravité** - La source ou la fonction qui génère le message syslog spécifie également la gravité du message à l'aide d'un entier à un chiffre, comme indiqué ci-dessous :

```
1 - Urgence : le systéme est inutilisable.

2 - Alerte : Des mesures doivent être prises immédiatement.

3 - Critique : conditions critiques.

4 - Erreur : conditions d'erreur.

5 - Avertissement : conditions d'avertissement.

6 - Avis : état normal mais significatif.

7 - Information : Messages d'information.

8 - Débogage : messages de niveau débogage.
```

Pour configurer syslog sur des instances Citrix ADC :

1. Dans Citrix ADM, accédez à **Réseaux** > **Instances**.
2. Sélectionnez l'instance Citrix ADC à partir de laquelle vous souhaitez que les messages syslog soient collectés et affichés dans Citrix ADM.
3. Dans la liste déroulante **Action**, sélectionnez **Configurer Syslog** .
4. Cliquez sur **Activer**.
5. Dans la liste déroulante **Facility**, sélectionnez une ressource locale ou de niveau utilisateur.
6. Sélectionnez le niveau de journal requis pour les messages syslog.
7. Cliquez sur **OK**.

Cela configure toutes les commandes syslog dans l'instance de Citrix ADC, et Citrix ADM commence à recevoir les messages syslog. Vous pouvez afficher les messages en accédant à **Réseaux** > **Événements** > **Messages Syslog** .

Configurer le contrôle d'accès basé sur les rôles

April 29, 2021

Citrix Application Delivery Management (Citrix ADM) fournit un contrôle d'accès basé sur les rôles (RBAC), qui vous permet d'accorder des autorisations d'accès en fonction des rôles des utilisateurs individuels au sein de votre entreprise.

Dans Citrix ADM, tous les utilisateurs sont ajoutés dans Citrix Cloud. En tant que premier utilisateur de votre organisation, vous devez d'abord créer un compte dans Citrix Cloud, puis vous connecter à l'interface utilisateur graphique Citrix ADM avec les informations d'identification Citrix Cloud. Vous disposez du rôle super administrateur et, par défaut, vous disposez de toutes les autorisations d'accès dans Citrix ADM. Plus tard, vous pouvez créer d'autres utilisateurs dans votre organisation dans Citrix Cloud.

Les utilisateurs qui sont créés ultérieurement et qui se connectent à Citrix ADM en tant qu'utilisateurs réguliers sont appelés administrateurs délégués. Ces utilisateurs, par défaut, disposent de toutes les autorisations, à l'exception des autorisations d'administration des utilisateurs. Toutefois, vous pouvez accorder des autorisations d'administration utilisateur spécifiques à ces utilisateurs admin délégués. Vous pouvez le faire en créant des stratégies appropriées et en les affectant à ces utilisateurs délégués. Les autorisations d'administration des utilisateurs se trouvent dans **Compte** > **Administration des utilisateurs** . Pour plus d'informations sur l'attribution d'autorisations spécifiques, reportez-vous à la sectionComment attribuer des autorisations supplémentaires à des utilisateurs d'administration délégués.

Pour plus d'informations sur la création de stratégies, de rôles, de groupes et sur la façon de lier les utilisateurs à des groupes, consultez les sections suivantes.

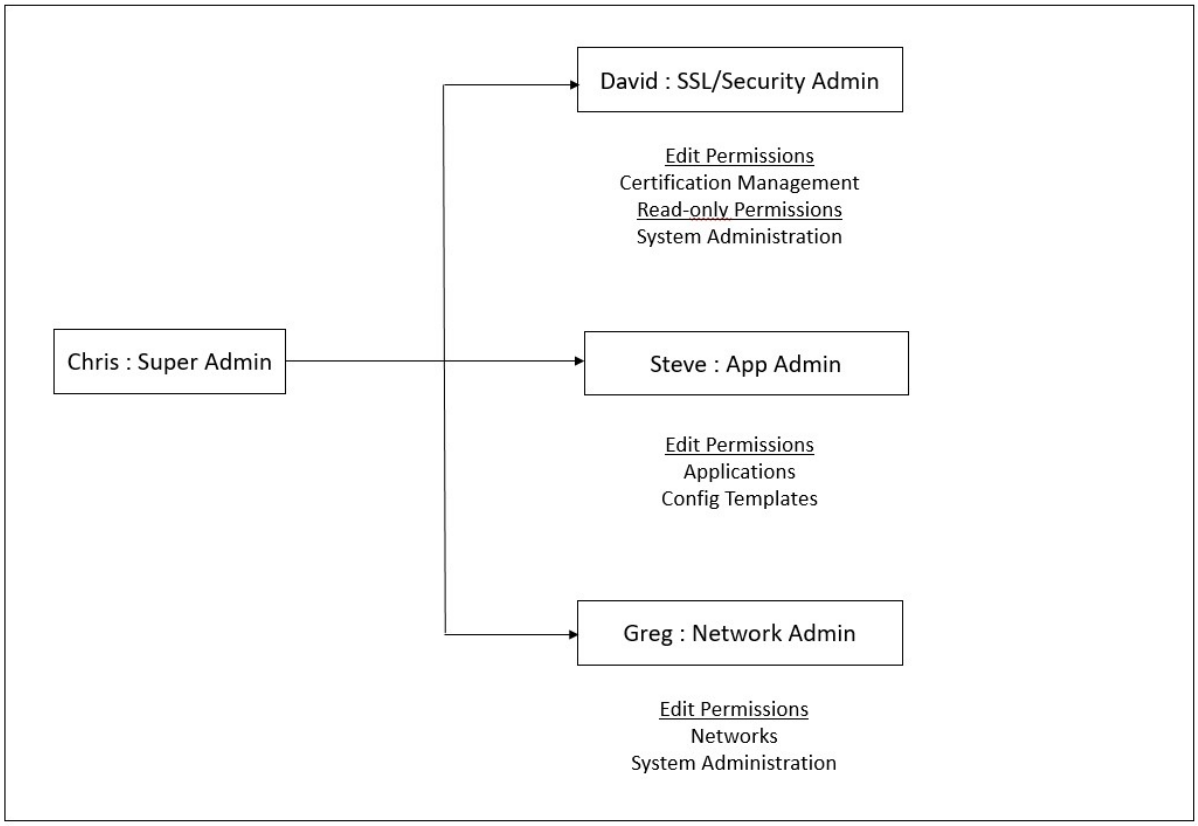
Exemple :

L'exemple suivant illustre comment le RBAC peut être réalisé dans Citrix ADM.

Chris, le chef du 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 disposer d'un accès complet pour la gestion et la surveillance des certificats SSL, mais doit disposer d'un accès en lecture seule pour les opérations d'administration système.
- Steve, administrateur d'applications, a besoin d'accéder uniquement à des applications spécifiques et uniquement à des modèles de configuration spécifiques.
- Greg, administrateur réseau, a besoin d'un accès à l'administration du système et du réseau.
- Chris doit également fournir RBAC à tous les utilisateurs, indépendamment du fait qu'ils soient locaux ou externes.

L'image suivante montre les autorisations dont disposent les administrateurs et les autres utilisateurs et leurs rôles dans l'organisation.



Pour fournir un contrôle d'accès basé sur le rôle à ses utilisateurs, Chris doit d'abord ajouter des utilisateurs dans Citrix Cloud et seulement après cela, il peut voir les utilisateurs dans Citrix ADM. Chris doit créer des stratégies d'accès pour chacun des utilisateurs en fonction de leur rôle. Les stratégies d'accès sont étroitement liées aux rôles. Ainsi, Chris doit également créer des rôles, puis il doit créer

des groupes car les rôles peuvent être attribués à des groupes uniquement et non à des utilisateurs individuels.

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 des stratégies. Après avoir créé des stratégies, vous pouvez créer des rôles, lier chaque rôle à une ou plusieurs stratégies et affecter des rôles aux utilisateurs. Vous pouvez également affecter des rôles à des groupes d'utilisateurs. Un groupe est une collection d'utilisateurs qui ont des autorisations en commun. Par exemple, les utilisateurs qui gèrent un centre de données particulier peuvent être affectés à un groupe. Un rôle est une identité accordée aux utilisateurs en les ajoutant à des groupes spécifiques en fonction de conditions spécifiques. Dans Citrix ADM, la création de rôles et de stratégies est spécifique à la fonctionnalité RBAC dans Citrix ADC. Les rôles et les stratégies peuvent être facilement créés, modifiés ou abandonnés 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 entités ou sur des ressources. Par exemple, considérez un administrateur SSL/Security et un administrateur d'application. Un administrateur SSL/Security doit avoir un accès complet aux fonctionnalités de gestion et de surveillance des certificats SSL, mais doit avoir un accès en lecture seule pour les opérations d'administration système. Les administrateurs d'applications sont en mesure d'accéder uniquement aux ressources comprises dans leur champ d'application.

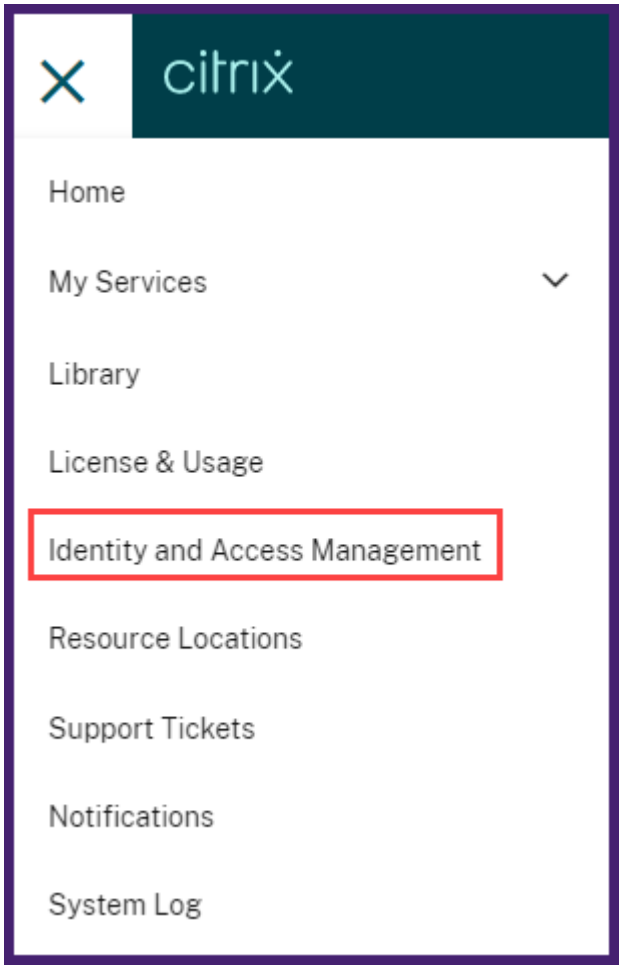
Par conséquent, dans votre rôle de Chris, le super administrateur, exécutez les exemples de tâches suivants dans Citrix ADM pour configurer les stratégies d'accès, les rôles et les groupes d'utilisateurs pour David qui est l'administrateur de sécurité de votre organisation.

Configurer les utilisateurs sur Citrix ADM

En tant que super administrateur, vous pouvez créer plus d'utilisateurs en configurant des comptes pour eux dans Citrix Cloud et non dans Citrix ADM. Lorsque les nouveaux utilisateurs sont ajoutés à Citrix ADM, vous ne pouvez définir leurs autorisations qu'en affectant les groupes appropriés à l'utilisateur.

Pour ajouter de nouveaux utilisateurs dans Citrix Cloud :

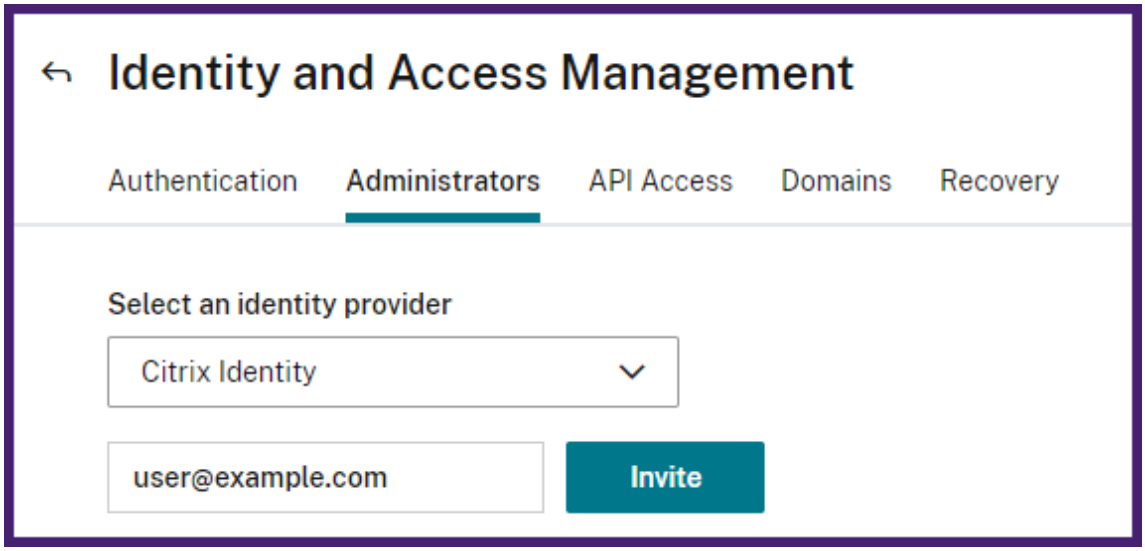
1. Dans l'interface graphique Citrix ADM, cliquez sur l'icône Hamburger en haut à gauche, puis sélectionnez **Gestion des identités et des accès**.



2. Dans la page Gestion des identités et des accès, sélectionnez l'onglet **Administrateurs** .

   Cet onglet répertorie les utilisateurs créés dans Citrix Cloud.

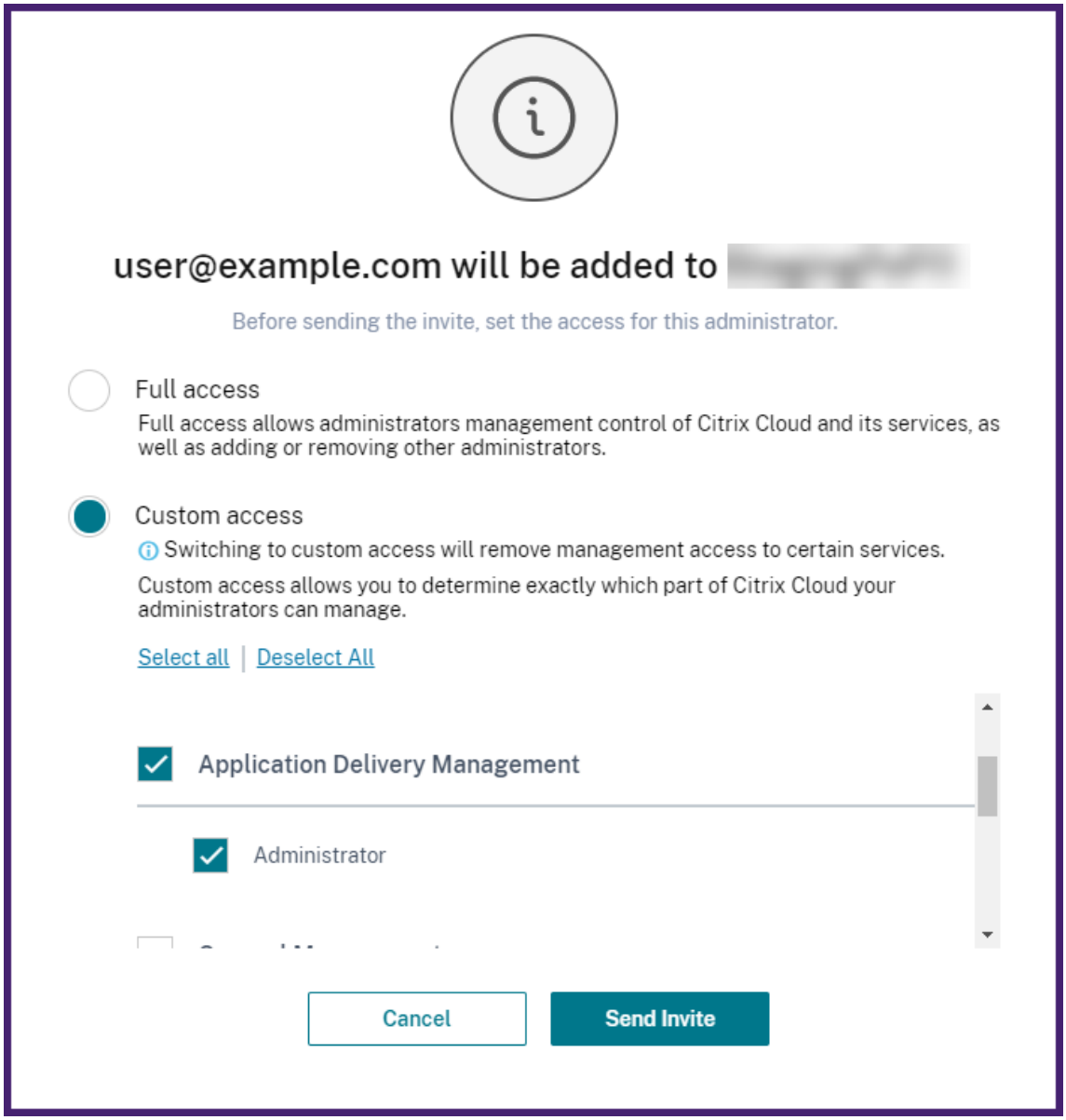
3. Sélectionnez **Citrix Identity** en tant que fournisseur d'identité.
4. Tapez l'adresse e-mail de l'utilisateur que vous souhaitez ajouter dans Citrix ADM, puis cliquez sur **Inviter**.



> **Remarque**
>
> L'utilisateur reçoit une invitation par e-mail de Citrix Cloud. L'utilisateur doit cliquer sur le lien fourni dans l'e-mail pour terminer le processus d'inscription en fournissant son nom complet et son mot de passe, puis ouvrir une session sur Citrix ADM à l'aide de ses informations d'identification.

5. Sélectionnez **Accès personnalisé** pour l'utilisateur spécifié.
6. Sélectionnez **Gestion de la livraison des applications**.

   Cette option sélectionne le rôle **Administrateur** par défaut.



7. Cliquez sur **Envoyer invitation**.

En tant qu'administrateur, vous ne voyez le nouvel utilisateur dans la liste des utilisateurs Citrix ADM qu'après que l'utilisateur se connecte à Citrix ADM.

Pour configurer des utilisateurs dans Citrix ADM :

1. Dans l'interface graphique Citrix ADM, accédez à **Compte** > **Administration de l'utilisateur** > **Utilisateurs**.
2. L'utilisateur s'affiche sur la page **Utilisateurs** .

3. Vous pouvez modifier les privilèges accordés à l'utilisateur en sélectionnant l'utilisateur et en cliquant sur **Modifier**. Vous pouvez également modifier les autorisations de groupe sur la page **Groupes** sous le nœud **Paramètres**.

> **Remarque**
>
> ```
> - Les utilisateurs sont ajoutés dans Citrix ADM à partir de Citrix Cloud uniquement. Par conséquent, même si vous disposez d'autorisations d'administrateur, vous ne pouvez pas ajouter ou supprimer des utilisateurs dans l'interface graphique Citrix ADM. Vous ne pouvez modifier que les autorisations de groupe. Les utilisateurs peuvent être ajoutés ou supprimés de Citrix Cloud.
>
> - Les détails de l'utilisateur apparaissent sur l'interface graphique du service uniquement aprés que l'utilisateur s'est connecté à Citrix ADM au moins une fois.
> ```

Configurer les stratégies d'accès sur Citrix ADM

Les stratégies d'accès définissent les autorisations. Une stratégie peut être appliquée à un groupe d'utilisateurs ou à plusieurs groupes en créant des rôles. Les rôles sont déterminés par des stratégies. 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. Citrix ADM propose cinq stratégies d'accès prédéfinies :

- **admin_policy**. Octroi l'accès à tous les nœuds Citrix ADM. L'utilisateur dispose à la fois des 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 ajouter, modifier et supprimer des opérations sur les ressources.
- **AdminExceptSystem_Policy**. Octroi l'accès aux utilisateurs pour tous les nœuds dans l'interface graphique Citrix ADM, à l'exception de l'accès au nœud Paramètres.
- **readonly_policy**. Octroi des autorisations en lecture seule. L'utilisateur peut afficher tout le contenu sur Citrix ADM mais n'est pas autorisé à effectuer des opérations.

- **appadmin_policy**. Octroi 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 peut 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.
- **appreadonly_policy**. Octroi des autorisations 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 ou de suppression, d'activation ou de désactivation.

Bien que vous ne puissiez pas modifier ces stratégies prédéfinies, vous pouvez créer vos propres stratégies (définies par l'utilisateur).

Auparavant, lorsque vous attribuez des stratégies aux rôles et lié les rôles à des groupes d'utilisateurs, vous pouvez fournir des autorisations pour les groupes d'utilisateurs au niveau du nœud dans l'interface graphique Citrix ADM. Par exemple, vous pouvez uniquement fournir des autorisations d'accès à l'intégralité du nœud d'équilibrage de charge. Vos utilisateurs avaient l'autorisation d'accéder à tous les sous-nœuds spécifiques à l'entité sous le nœud d'équilibrage de charge (par exemple, serveur virtuel, services, etc.) ou ils n'avaient pas l'autorisation d'accéder à un nœud sous **Équilibrage de charge**.

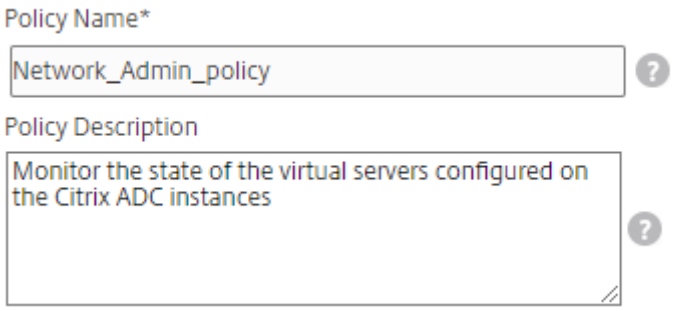
Dans Citrix ADM 507.x build et versions ultérieures, la gestion des stratégies d'accès est étendue pour fournir également des autorisations pour les sous-nœuds. Les paramètres de stratégie d'accès peuvent être configurés pour tous les sous-nœuds tels que les serveurs virtuels, les services, les groupes de services et les serveurs.

Actuellement, vous pouvez fournir une telle autorisation d'accès de niveau granulaire uniquement pour les sous-nœuds situés sous un nœud d'équilibrage de charge ainsi que pour les sous-nœuds sous le nœud GSLB.

Par exemple, en tant qu'administrateur, vous pouvez accorder à l'utilisateur une autorisation d'accès uniquement pour afficher les serveurs virtuels, mais pas les services back-end, les groupes de services et les serveurs d'applications dans le nœud d'équilibrage de charge. Les utilisateurs auxquels une telle stratégie leur est attribuée ne peuvent accéder qu'aux serveurs virtuels.

Pour créer des stratégies d'accès définies par l'utilisateur :

1. Dans l'interface graphique Citrix ADM, accédez à **Compte** > **Administration de l'utilisateur** > **Stratégies d'accès**.
2. Cliquez sur **Ajouter**.
3. Dans la page **Créer des stratégies d'accès**, dans le champ **Nom de la stratégie**, entrez le nom de la stratégie et entrez la description dans le champ **Description de la stratégie** .



La section **Autorisations** répertorie toutes les fonctionnalités Citrix ADM, avec des options permettant de spécifier l'accès en lecture seule, activer-désactiver ou modifier.

a) Cliquez sur l'icône (+) pour développer chaque groupe d'entités en plusieurs entités.

b) Activez la case à cocher Autorisation en regard du nom de la fonction pour accorder des autorisations aux utilisateurs.

- **Affichage :** Cette option permet à l'utilisateur d'afficher la fonctionnalité dans Citrix ADM.
- **Enable-Disable :** cette option est disponible uniquement pour les fonctionnalités **Fonctions réseau** qui permettent d'activer ou de désactiver l'action sur Citrix ADM. L'utilisateur peut activer ou désactiver la fonctionnalité. Et, un utilisateur peut également effectuer l'action **Sondage maintenant**.

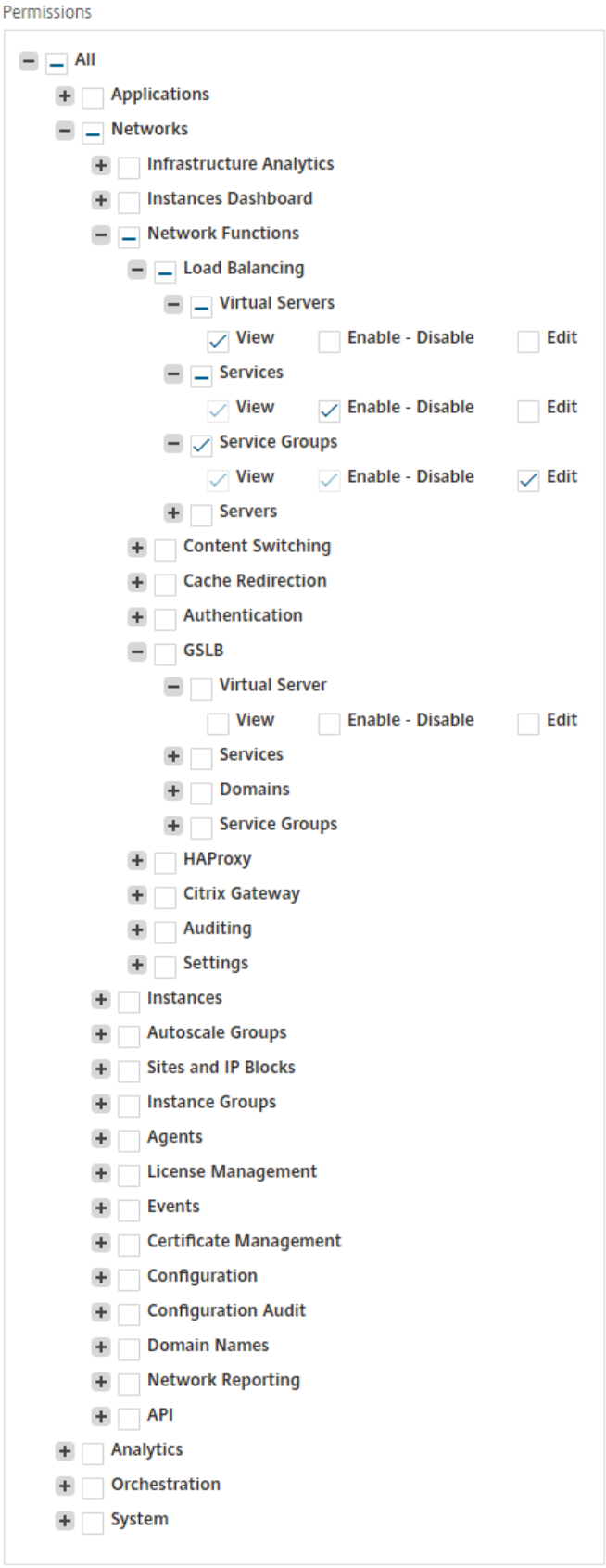
  Lorsque vous accordez l'autorisation **Activer-Désactiver** à un utilisateur, l'autorisation **Afficher** est également accordée. Vous ne pouvez pas désélectionner cette option.
- **Modifier :** Cette option accorde l'accès complet à l'utilisateur. L'utilisateur peut modifier la fonction et ses fonctions.

  Si vous accordez l'autorisation **Modifier**, les autorisations **View** et **Enable-Disable** sont accordées. Vous ne pouvez pas désélectionner les options sélectionnées automatiquement.

Si vous activez la case à cocher Fonction, elle sélectionne toutes les autorisations pour la fonctionnalité.

> **Remarque**
>
> Développez l'équilibrage de charge et GSLB pour afficher d'autres options de configuration.

Dans l'image suivante, les options de configuration de la fonctionnalité d'équilibrage de charge disposent d'autorisations différentes :



L'autorisation **View** est accordée à un utilisateur pour la fonctionnalité **Serveurs virtuels** . L'utilisateur peut afficher les serveurs virtuels d'équilibrage de charge dans Citrix ADM. Pour afficher les serveurs virtuels, accédez à **Réseaux** > **Fonctions réseau** > **Équilibrage de charge** et sélectionnez l'onglet **Serveurs virtuels** .

L'autorisation **Enable-Disable** est accordée à un utilisateur pour la fonctionnalité **Services** . Cette autorisation accorde également l'autorisation **View** . L'utilisateur peut activer ou désactiver les services liés à un serveur virtuel d'équilibrage de charge. En outre, l'utilisateur peut effectuer l'action **Sondage Now** sur les services. Pour activer ou désactiver des services, accédez à **Réseaux** > **Fonctions réseau** > **Équilibrage de charge** et sélectionnez l'onglet **Services**.

> **Remarque**
>
> Si un utilisateur dispose de l'autorisation **Enable-Disable**, l'action d'activation ou de désactivation sur un service est restreinte dans la page suivante :
>
> a) Accédez à **Réseaux** > **Fonctions réseau**.
>
> b) Sélectionnez un serveur virtuel et cliquez sur **Configurer**.
>
> c) Sélectionnez la page **Liaison de service de serveur virtuel d'équilibrage** de charge. Cette page affiche un message d'erreur si vous sélectionnez **Activer** ou **Désactiver** .

L'autorisation **Modifier** est accordée à un utilisateur pour la fonctionnalité **Groupes de services** . Cette autorisation accorde l'accès complet lorsque les autorisations **View** et **Enable-Disable** sont accordées. L'utilisateur peut modifier les groupes de services liés à un serveur virtuel d'équilibrage de charge. Pour modifier des groupes de services, accédez à **Réseaux** > **Fonctions réseau** > **Équilibrage de charge** et sélectionnez l'onglet **Groupes de services** .

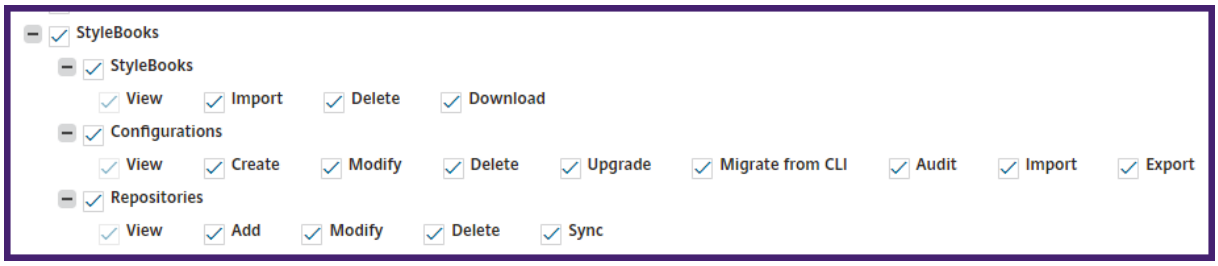
4. Cliquez sur **Créer**.

> **Remarque**
>
> Si vous sélectionnez **Modifier**, vous pouvez affecter en interne des autorisations dépendantes qui ne sont pas affichées comme 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.

Accorder des autorisations StyleBook aux utilisateurs

Vous pouvez créer une stratégie d'accès pour accorder des autorisations StyleBook telles que l'importation, la suppression, le téléchargement, etc.

> **Remarque**
>
> L'autorisation Afficher est automatiquement activée lorsque vous accordez d'autres autorisations StyleBook.



Configurer les rôles sur Citrix ADM

Dans Citrix 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-à-plusieurs entre les stratégies et les rôles. Vous pouvez lier un rôle à plusieurs stratégies et vous pouvez lier plusieurs rôles à une stratégie.

Par exemple, un rôle peut être lié à deux stratégies, l'une définissant les autorisations d'accès pour une entité et l'autre définissant les autorisations d'accès pour une autre entité. Une stratégie peut accorder l'autorisation d'ajouter des instances Citrix ADC dans Citrix ADM, et l'autre peut accorder l'autorisation de créer et de déployer un StyleBook et de configurer des instances Citrix ADC.

Lorsque plusieurs stratégies définissent les autorisations de mise à jour et de lecture seule pour une entité unique, les autorisations de mise à jour ont la priorité sur les autorisations de lecture seule.

Citrix ADM fournit cinq rôles prédéfinis :

- rôle**admin_role**. A accès à toutes les fonctionnalités Citrix ADM. (Ce rôle est lié à `adminpolicy` .)
- **Rôle AdminExceptSystem_Admin.** A accès à l'interface utilisateur graphique Citrix ADM, à l'exception des autorisations Paramètres. (Ce rôle est lié à AdminExceptSystem_Policy)
- **readonly_role**. Accès en lecture seule. (Ce rôle est lié à `readonlypolicy`.)
- **Rôle AppAdmin_.** Dispose d'un accès administratif uniquement aux fonctionnalités de l'application dans Citrix ADM. (Ce rôle est lié à AppAdminPolicy).
- **AppreAdonly_Rôle**. A un accès en lecture seule aux fonctionnalités de l'application. (Ce rôle est lié à AppreadOnlyPolicy.)

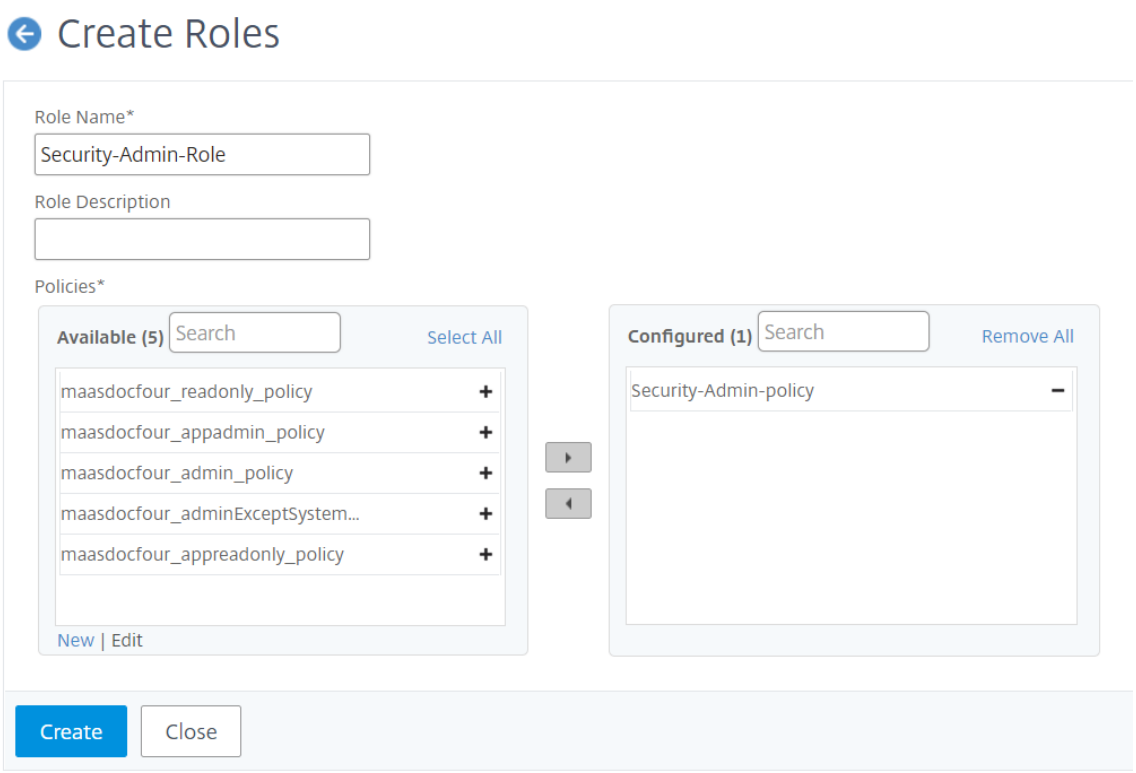
Bien que vous ne puissiez pas modifier les rôles prédéfinis, vous pouvez créer vos propres rôles (définis par l'utilisateur).

Pour créer des rôles et leur attribuer des stratégies :

1. Dans l'interface graphique Citrix ADM, accédez à **Compte** > **Administration de l'utilisateur** > **Rôles**.

2. Cliquez sur **Ajouter**.
3. Dans la page **Créer des rôles**, dans le champ **Nom du rôle**, entrez le nom du rôle et indiquez la description dans le champ **Description du rôle** (facultatif).
4. Dans la section **Stratégies**, ajoutez déplacer une ou plusieurs stratégies vers la liste **Configurées** .

> **Remarque**
>
> Les stratégies sont préfixées avec un ID de locataire (par exemple, `maasdocfour`) unique à tous les locataires.



> **Remarque**
>
> Vous pouvez créer une stratégie d'accès en cliquant sur **Nouveau**, ou vous pouvez accéder à **Compte**> **Administration des utilisateurs**> **Stratégies d'accès,**puis créer des stratégies.

5. Cliquez sur **Créer**.

Configurer des groupes sur Citrix ADM

Dans Citrix ADM, un groupe peut avoir un accès au niveau des fonctionnalités et des ressources. Par exemple, un groupe d'utilisateurs peut avoir accès uniquement aux instances Citrix ADC sélectionnées ; un autre groupe avec seulement quelques applications sélectionnées, etc.

Lorsque vous créez un groupe, vous pouvez attribuer des rôles au groupe, fournir un accès au groupe au niveau de l'application et affecter des utilisateurs au groupe. Tous les utilisateurs de ce groupe se voient attribuer les mêmes droits d'accès dans Citrix ADM.

Vous pouvez gérer un accès utilisateur dans Citrix ADM au niveau individuel des entités de fonction réseau. Vous pouvez attribuer dynamiquement des autorisations spécifiques à l'utilisateur ou au groupe au niveau de l'entité.

Citrix ADM traite les serveurs virtuels, les services, les groupes de services et les serveurs en tant qu'entités de fonction réseau.

- **Serveur virtuel (Applications)** : équilibrage de charge (`lb`), GSLB, commutation de contexte (`CS`), redirection du cache (`CR`), authentification (`Auth`) et Citrix Gateway (`vpn`)
- **Services** - Équilibrage de charge et services GSLB
- **Groupe de services** : équilibrage de charge et groupes de services GSLB
- **Serveurs - Serveurs** d'équilibrage de charge

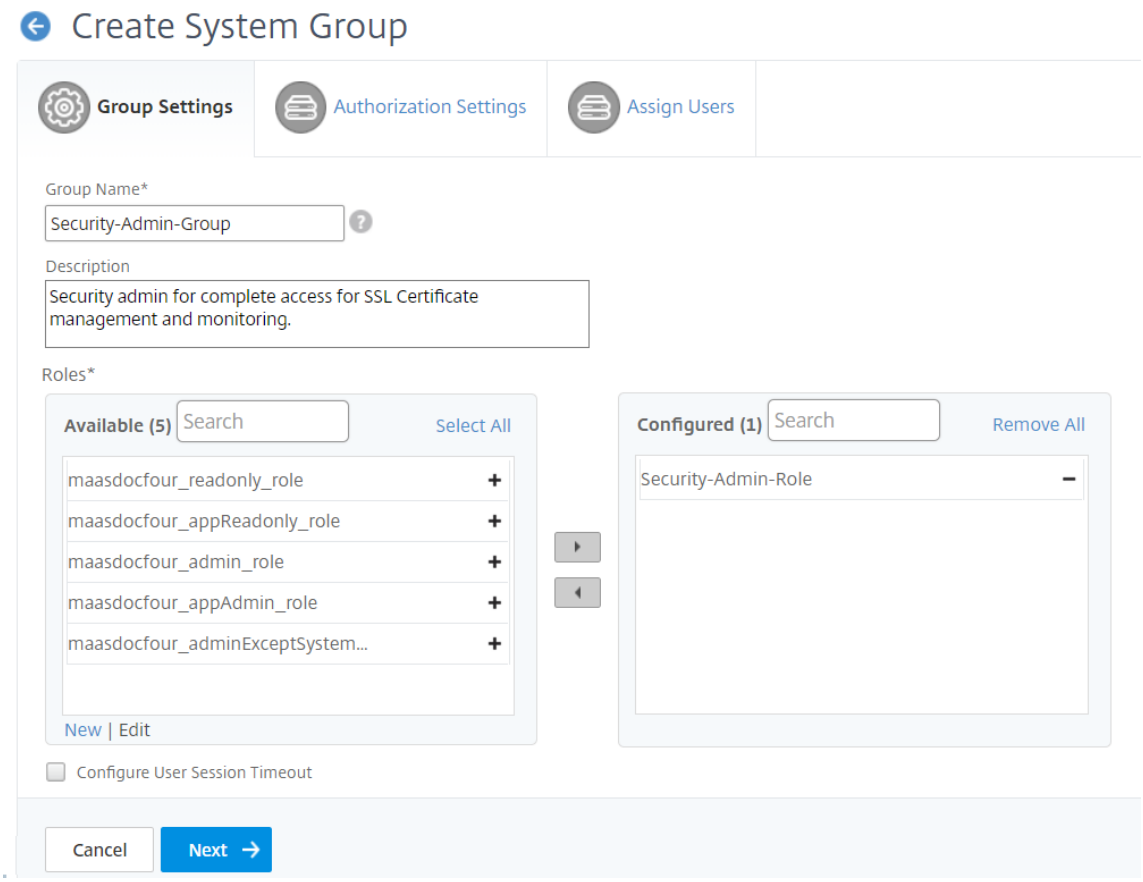
Pour créer un groupe :

1. Dans Citrix ADM, accédez à **Compte** > **Administration des utilisateurs** > **Groupes** .
2. Cliquez sur **Ajouter**.

   La page **Créer un groupe de systèmes** s'affiche.
3. Dans le champ **Nom du groupe**, entrez le nom du groupe.
4. Dans le champ **Description du groupe**, saisissez une description de votre groupe. Fournir une bonne description vous aide à comprendre le rôle et la fonction du groupe.
5. Dans la section **Rôles**, déplacez un ou plusieurs rôles vers la liste **Configuré** .

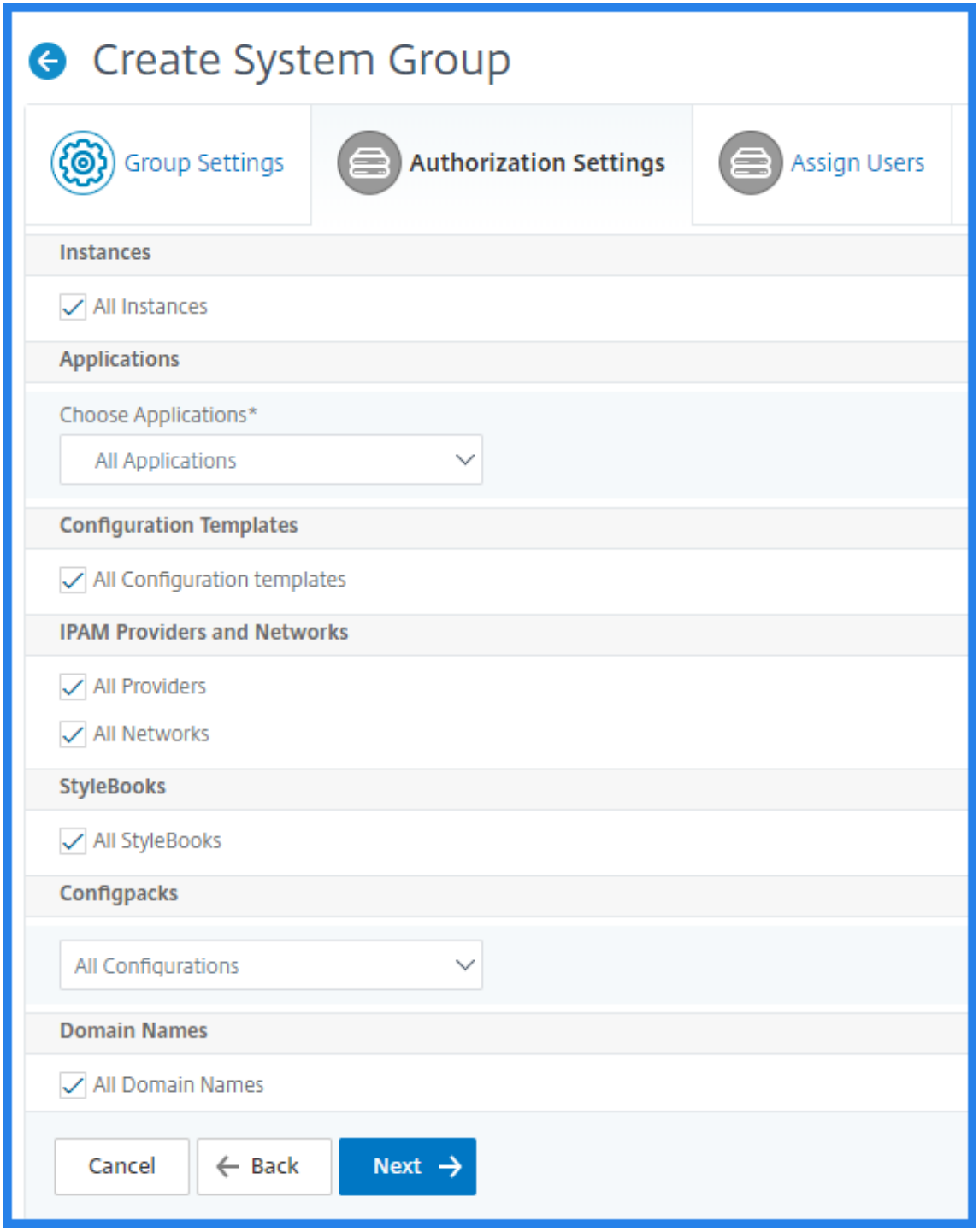
   > **Remarque**
   >
   > Les rôles sont préfixés avec un ID de locataire (par exemple, `maasdocfour`) unique à tous les locataires.
6. Dans la liste **Disponible**, vous pouvez cliquer sur **Nouveau** ou **Modifier** et créer ou modifier des rôles.

   Vous pouvez également accéder à **Comptes** > **Administration** des **utilisateurs > Utilisateurs**, puis créer ou modifier des utilisateurs.



7. Cliquez sur **Suivant**.
8. Dans l'onglet **Paramètres d'autorisation**, vous pouvez choisir des ressources parmi les catégories suivantes :

   - **Groupes de mise à l'échelle automatique**
   - **Instances**
   - **Applications**
   - **Modèles de configuration**
   - **Fournisseurs et réseaux IPAM**
   - **StyleBooks**
   - **Configpacks**
   - **Noms de domaine**



Vous pouvez sélectionner des ressources spécifiques parmi les catégories auxquelles les utilisateurs peuvent accéder.

Groupes de mise à l'échelle automatique :

Si vous souhaitez sélectionner les groupes de mise à l'Autoscale spécifiques que l'utilisateur peut afficher ou gérer, effectuez les opérations suivantes :

a) Désactivez la case à cocher **Tous les groupes d'échelle automatique** et cliquez sur **Ajouter des groupes d'échelle automatique** .

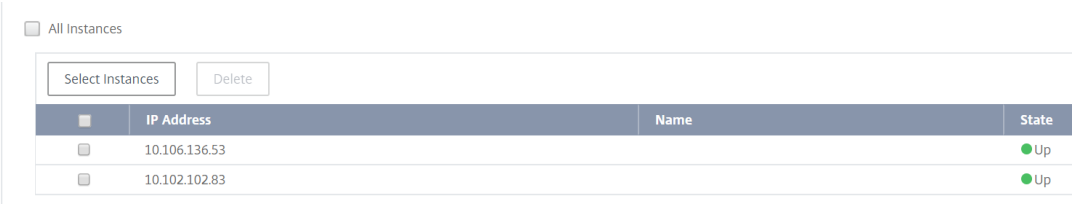
b) Sélectionnez les groupes de mise à l'échelle automatique requis dans la liste et cliquez sur **OK**.

Instances :

Si vous souhaitez sélectionner les instances spécifiques qu'un utilisateur peut afficher ou gérer, effectuez les opérations suivantes :

a) Désactivez la case à cocher **Toutes les instances** et cliquez sur **Sélectionner les instances** .

b) Sélectionnez les instances requises dans la liste et cliquez sur **OK**.



Applications :

La liste **Choisir des applications** vous permet d'accorder l'accès à un utilisateur pour les applications requises.

Vous pouvez accorder l'accès aux applications sans sélectionner leurs instances. Parce que les applications sont indépendantes de leurs instances pour accorder l'accès utilisateur.

Lorsque vous accordez à un utilisateur l'accès à une application, l'utilisateur est autorisé à accéder uniquement à cette application, indépendamment de la sélection d'instance.

Cette liste vous offre les options suivantes :

- **Toutes les applications :** cette option est sélectionnée par défaut. Il ajoute toutes les applications présentes dans Citrix ADM.
- **Toutes les applications des instances sélectionnées :** cette option n'apparaît que si vous sélectionnez des instances dans la catégorie **Toutes les instances** . Il ajoute toutes les applications présentes sur l'instance sélectionnée.
- **Applications spécifiques :** cette option vous permet d'ajouter les applications requises auxquelles les utilisateurs doivent accéder. Cliquez sur **Ajouter des applications** et sélectionnez les applications requises dans la liste.
- **Sélectionner un type d'entité individuelle :** Cette option vous permet de sélectionner le type spécifique d'entité de fonction réseau et les entités correspondantes.

  Vous pouvez ajouter des entités individuelles ou sélectionner toutes les entités sous le type d'entité requis pour accorder l'accès à un utilisateur.

L' option **Appliquer sur les entités liées autorise également**les entités liées au type d'entité sélectionné. Par exemple, si vous sélectionnez une application et que vous sélectionnez **Appliquer également sur les entités liées**, Citrix ADM autorise toutes les entités liées à l'application sélectionnée.

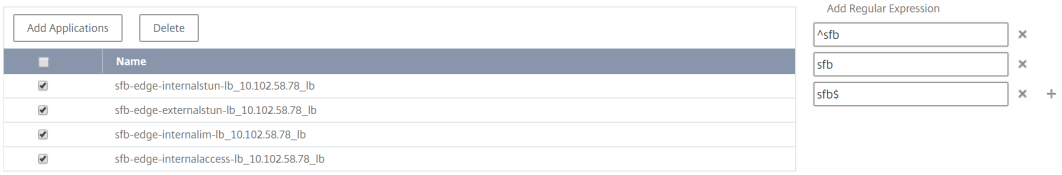
> **Remarque**
>
> Assurez-vous d'avoir sélectionné un seul type d'entité si vous souhaitez autoriser des entités liées.

Vous pouvez utiliser des expressions régulières pour rechercher et ajouter les entités de fonction réseau qui répondent aux critères d'expression rationnelle pour les groupes. L'expression regex spécifiée est conservée dans Citrix ADM. Pour ajouter une expression régulière, effectuez les opérations suivantes :

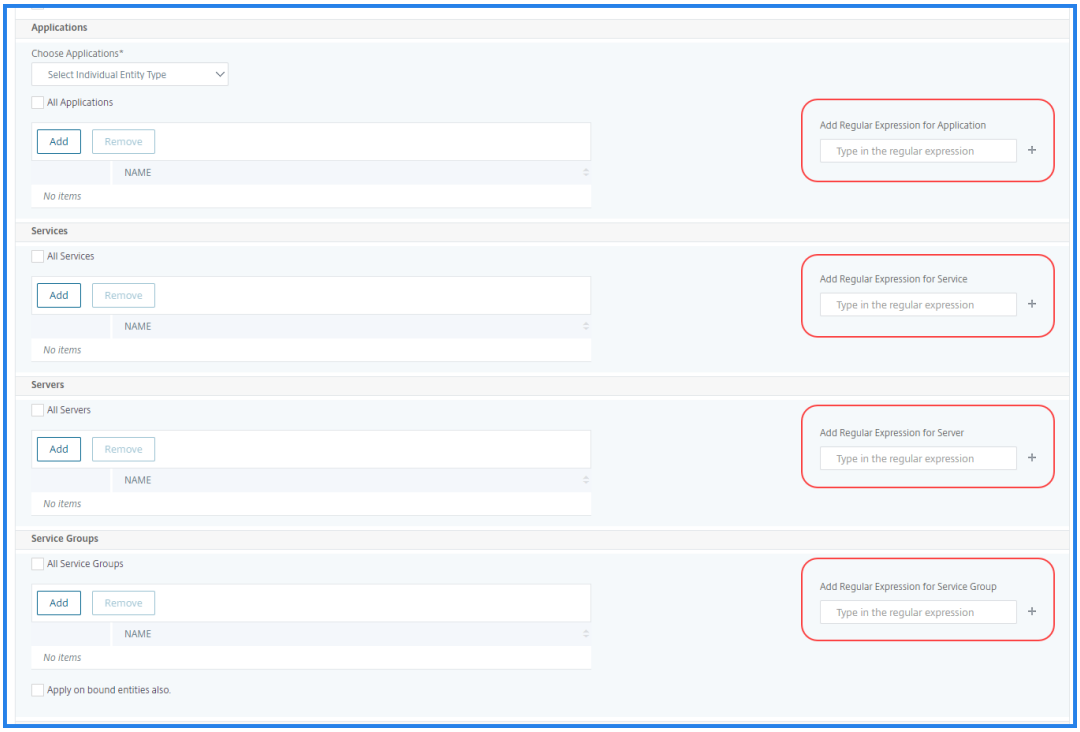
a) Cliquez sur **Ajouter une expression régulière**.

b) Spécifiez l'expression régulière dans la zone de texte.

L'image suivante explique comment utiliser l'expression régulière pour ajouter une application lorsque vous sélectionnez l'option **Applications spécifiques** :



L'image suivante explique comment utiliser l'expression régulière pour ajouter des entités de fonction réseau lorsque vous choisissez l'option **Sélectionner le type d'entité individuelle** :



Si vous souhaitez ajouter d'autres expressions régulières, cliquez sur l'icône **+** .

> **Remarque**
>
> L'expression régulière correspond uniquement au nom du serveur pour le type d'entité **Serveurs**et non à l'adresse IP du serveur.

Si vous sélectionnez l'option **Appliquer sur les entités liées également** pour une entité découverte, un utilisateur peut accéder automatiquement aux entités qui sont liées à l'entité découverte.

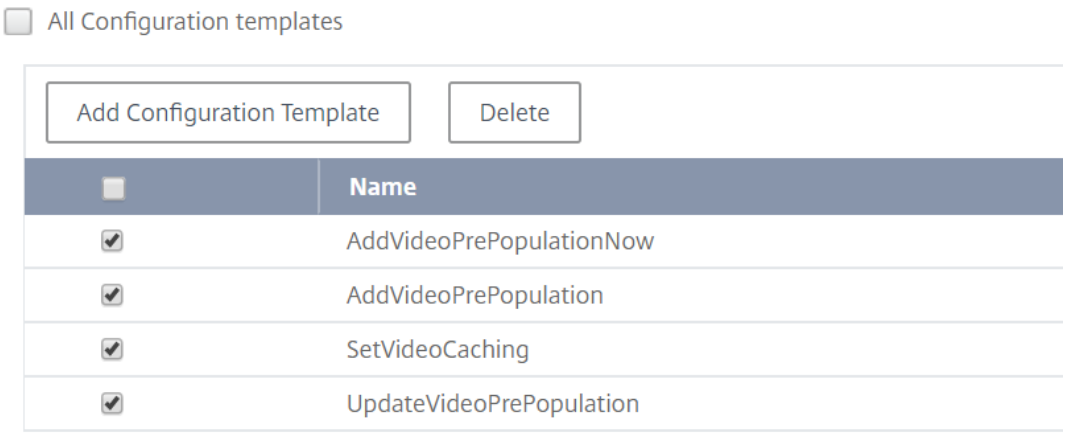
L'expression régulière est stockée dans le système pour mettre à jour l'étendue de l'autorisation. Lorsque les nouvelles entités correspondent à l'expression régulière de leur type d'entité, Citrix ADM met à jour la portée d'autorisation vers les nouvelles entités.

Modèles de configuration :

Si vous souhaitez sélectionner le modèle de configuration spécifique qu'un utilisateur peut afficher ou gérer, effectuez les opérations suivantes :

a) Désactivez la case à cocher **Tous les modèles de configuration** et cliquez sur **Ajouter un modèle de configuration** .

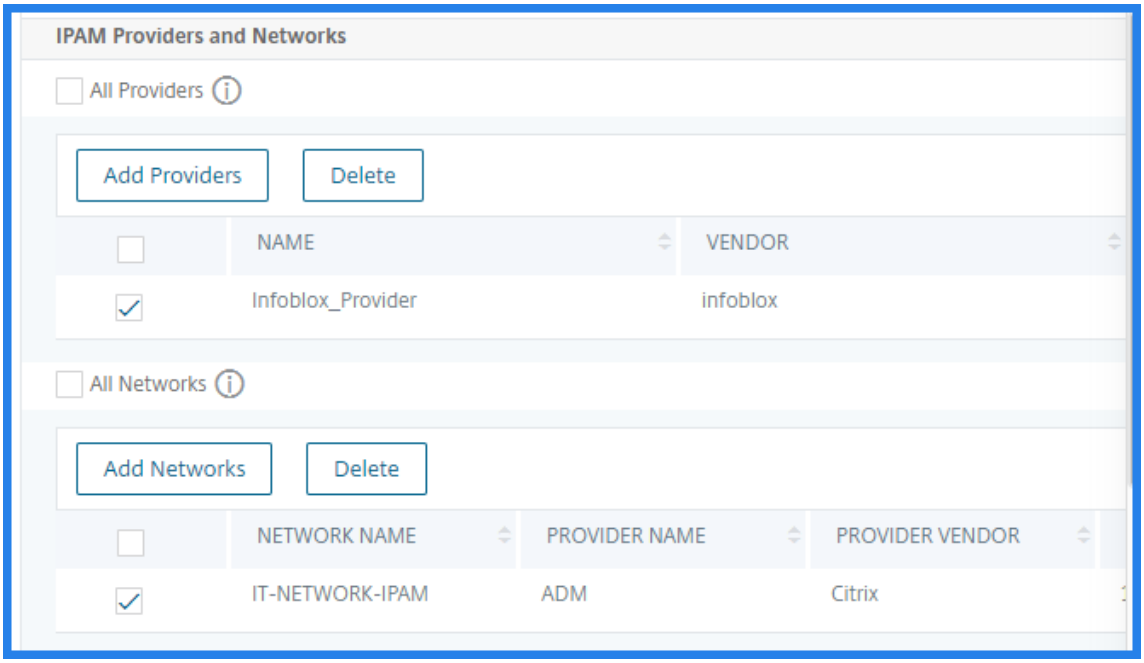
b) Sélectionnez le modèle requis dans la liste et cliquez sur **OK**.



Fournisseurs et réseaux IPAM :

Si vous souhaitez ajouter les fournisseurs et réseaux IPAM spécifiques qu'un utilisateur peut afficher ou gérer, effectuez les opérations suivantes :

- **Ajouter des fournisseurs** - Désactivez la case à cocher **Tous les fournisseurs** et cliquez sur **Ajouter des fournisseurs**. Vous pouvez sélectionner les fournisseurs requis et cliquer sur **OK**.
- **Ajouter des réseaux** - Désactivez la case à cocher **Tous les réseaux** et cliquez sur **Ajouter des réseaux**. Vous pouvez sélectionner les réseaux requis et cliquer sur **OK**.



StyleBooks:

Si vous souhaitez sélectionner le StyleBook spécifique qu'un utilisateur peut afficher ou gérer, effectuez les opérations suivantes :

a) Désactivez la case à cocher **Tous les StyleBooks** et cliquez sur **Ajouter un StyleBook au groupe**. Vous pouvez sélectionner des StyleBooks individuels ou spécifier une requête de filtre pour autoriser les StyleBooks.

Si vous souhaitez sélectionner les StyleBooks individuels, sélectionnez les StyleBooks dans le volet **StyleBooks individuels** et cliquez sur **Enregistrer la sélection**.

Si vous souhaitez utiliser une requête pour rechercher des StyleBooks, sélectionnez le volet **Filtres personnalisés**. Une requête est une chaîne de paires clé-valeur où les clés sont `name`, `namespace` et `version`.

Vous pouvez également utiliser des expressions régulières comme valeurs pour rechercher et ajouter des StyleBooks répondant aux critères de regex pour les groupes. Une requête de filtre personnalisée pour rechercher StyleBooks prend en charge les opérateurs `And` et `Or`.

Exemple :

```
1 name=lb-mon|lb AND namespace=com.citrix.adc.stylebooks AND
     version=1.0
2 <!--NeedCopy-->
```

Cette requête répertorie les StyleBooks qui remplissent les conditions suivantes :

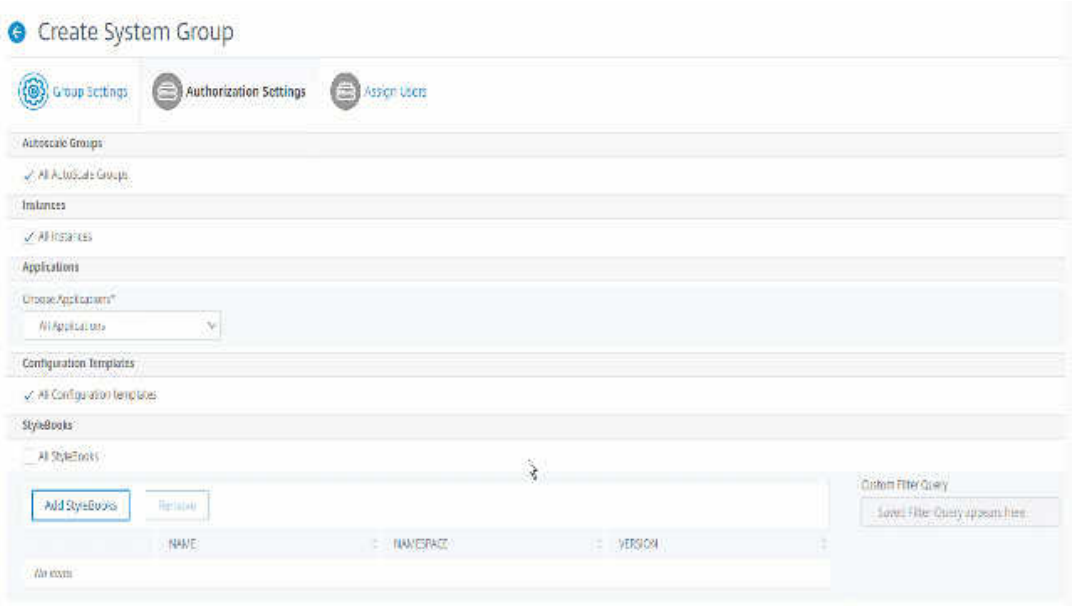
- Le nom de StyleBook est `lb-mon` ou `lb`.
- L'espace de noms StyleBook est `com.citrix.adc.stylebooks`.
- La version StyleBook est `1.0`.

Utilisez un opérateur `Or` entre des expressions de valeur définie à l'expression clé.

Exemple :

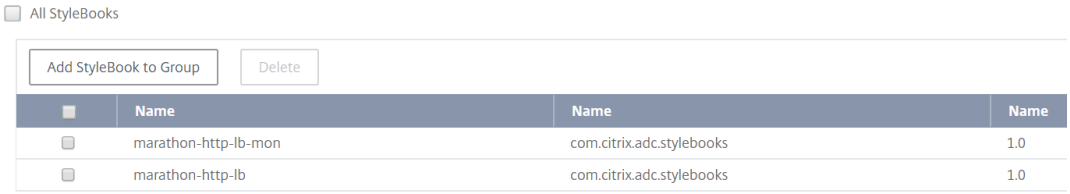
- La requête `name=lb-mon|lb` est valide. Il renvoie les StyleBooks ayant un nom `lb-mon` ou `lb`.
- La requête `name=lb-mon | version=1.0` n'est pas valide.

Appuyez sur `Enter` pour afficher les résultats de la recherche et cliquez sur **Enregistrer la requête**.



La requête enregistrée apparaît dans la **requête Filtres personnalisés**. En fonction de la requête enregistrée, l'ADM fournit aux utilisateurs l'accès à ces livres StyleBooks.

b) Sélectionnez les StyleBooks requis dans la liste et cliquez sur **OK**.

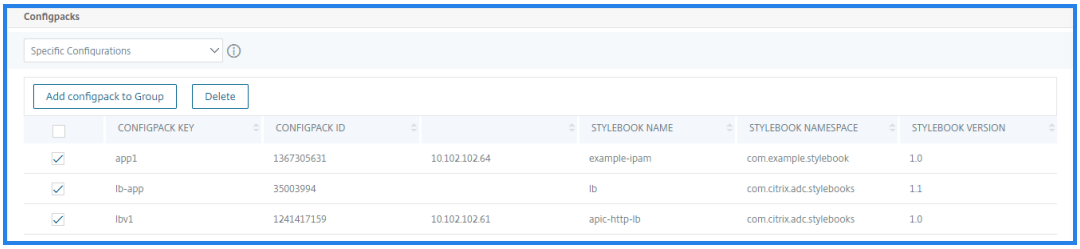


Vous pouvez sélectionner les StyleBooks requis lorsque vous créez des groupes et ajoutez des utilisateurs à ce groupe. Lorsque votre utilisateur sélectionne le StyleBook autorisé, tous les StyleBooks dépendants sont également sélectionnés.

Configpacks :

Dans **Configpacks**, sélectionnez l'une des options suivantes :

- **Toutes les configurations** : Cette option est sélectionnée par défaut. Il ajoute tous les packs de configuration qui sont dans ADM.
- **Toutes les configurations des StyleBooks sélectionnés** : Cette option ajoute tous les packs de configuration du StyleBook sélectionné.
- **Configurations spécifiques** : Cette option vous permet d'ajouter les packs de configuration requis.



Vous pouvez sélectionner les packs de configuration requis lorsque vous créez des groupes et ajoutez des utilisateurs à ce groupe.

Noms de domaine :

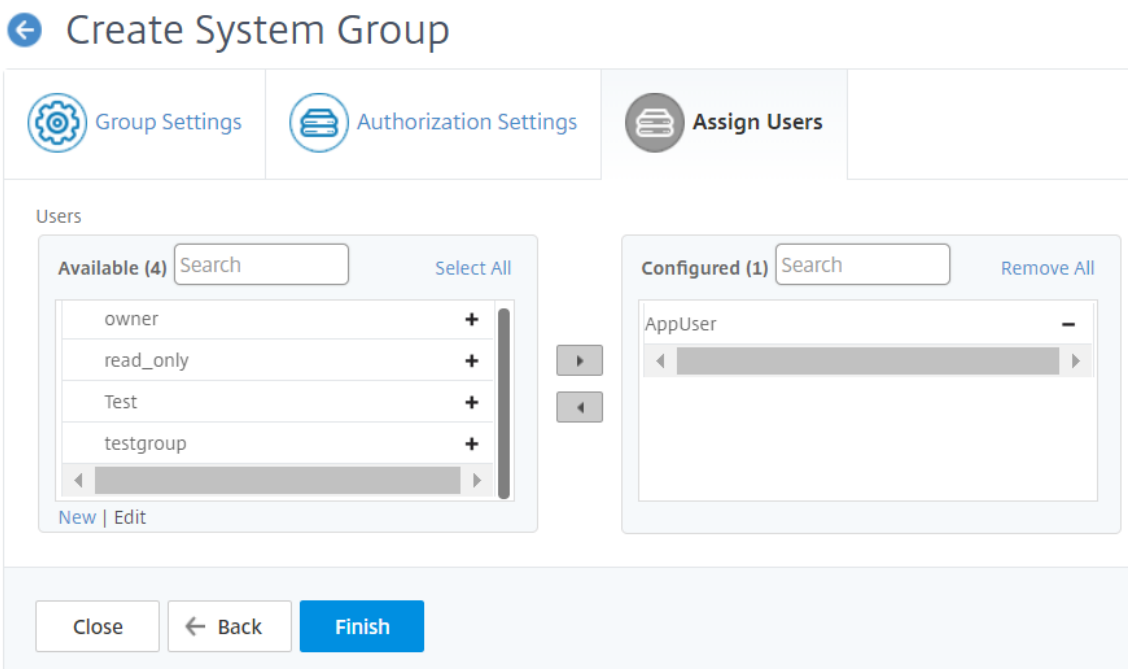
Si vous souhaitez sélectionner le nom de domaine spécifique qu'un utilisateur peut afficher ou gérer, effectuez les opérations suivantes :

a) Désactivez la case à cocher **Tous les noms de domaine** et cliquez sur **Ajouter un nom de domaine** .

b) Sélectionnez les noms de domaine requis dans la liste et cliquez sur **OK**.

9. Cliquez sur **Créer un groupe**.
10. Dans la section **Affecter des utilisateurs**, sélectionnez l'utilisateur dans la liste **Disponible** et ajoutez l'utilisateur à la liste **Configuré** .

> **Remarque**
>
> Vous pouvez également ajouter de nouveaux utilisateurs en cliquant sur **Nouveau**.



11. Cliquez sur **Terminer**.

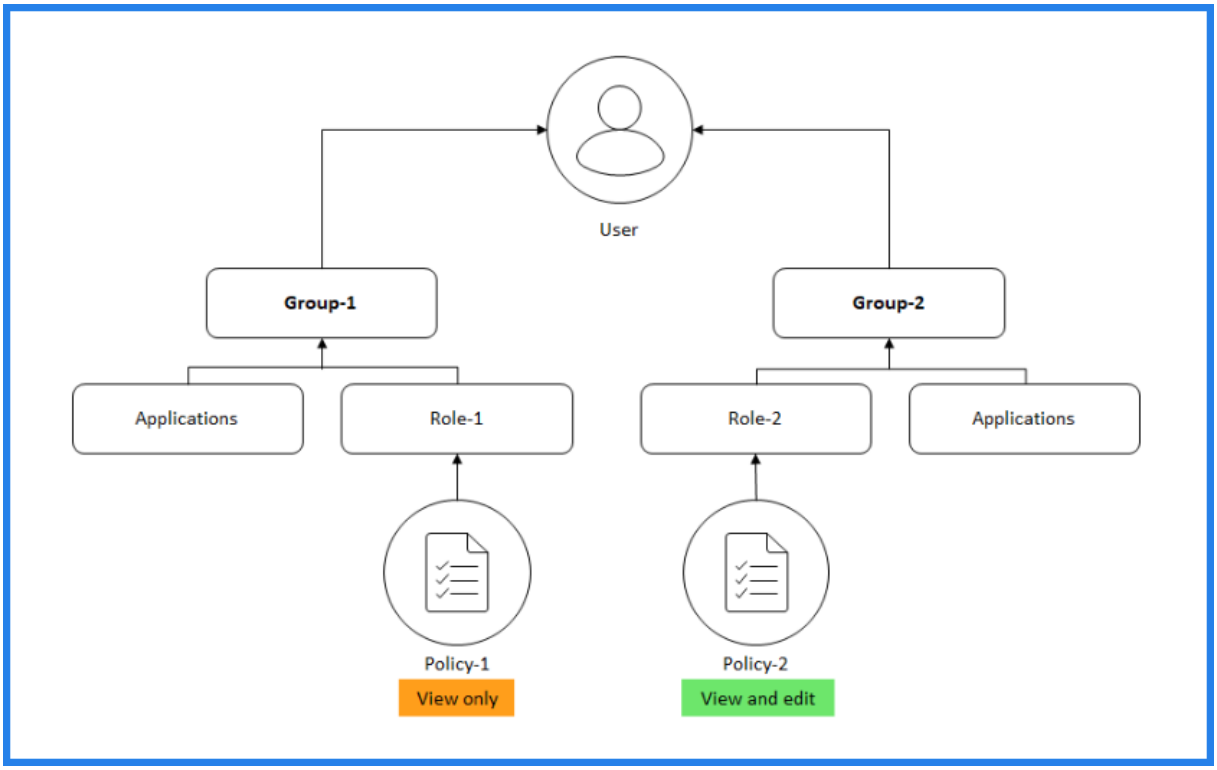
Comment l'accès utilisateur change en fonction de la portée d'autorisation

Lorsqu'un administrateur ajoute un utilisateur à un groupe qui a des paramètres de stratégie d'accès différents, l'utilisateur est mappé à plusieurs étendues d'autorisation et stratégies d'accès.

Dans ce cas, ADM accorde à l'utilisateur l'accès aux applications en fonction de la portée d'autorisation spécifique.

Considérez un utilisateur qui est affecté à un groupe doté de deux stratégies Stratégie-1 et Stratégie-2.

- **Policy-1** — Affiche uniquement les autorisations pour les applications.
- **Policy-2** — Afficher et modifier l'autorisation des applications.



L'utilisateur peut afficher les applications spécifiées dans la stratégie 1. En outre, cet utilisateur peut afficher et modifier les applications spécifiées dans la stratégie 2. L'accès à la modification des applications du groupe 1 est restreint car il n'est pas sous la portée de l'autorisation du groupe 1.

Limitations

Le RBAC n'est pas entièrement pris en charge par les fonctionnalités Citrix ADM suivantes :

- Analytics - Le RBAC n'est pas entièrement pris en charge par les modules analytiques. La prise en charge RBAC est limitée à un niveau d'instance et ne s'applique pas au niveau de l'application dans les modules d'analyse Gateway Insight, HDX Insight et Security Insight.

  - Exemple 1 : RBAC basé sur l'instance (pris en charge). Un administrateur qui a reçu quelques instances peut voir uniquement ces instances sous **HDX Insight** > **Périphériques**, et uniquement les serveurs virtuels correspondants sous **HDX Insight** > **Applications**, car RBAC est pris en charge au niveau de l'instance.
  - Exemple 2 : RBAC basé sur l'application (non pris en charge). Un administrateur qui a reçu quelques applications peut voir tous les serveurs virtuels sous **HDX Insight** > **Applications**, mais ne peut pas y accéder, car RBAC n'est pas pris en charge au niveau des applications.
- StyleBooks — Le RBAC n'est pas entièrement pris en charge pour StyleBooks.
  - Considérez une situation dans laquelle plusieurs utilisateurs ont accès à un seul StyleBook mais ont des autorisations d'accès pour différentes instances de Citrix ADC. Les utilisateurs peuvent créer et mettre à jour des packs de configuration sur leurs propres instances, mais pas sur d'autres instances car ils n'ont pas accès à ces instances autres que les leurs. Mais ils peuvent toujours afficher les packs de configuration et les objets créés sur des instances Citrix ADC autres que les leurs.

Configuration des paramètres Analytics

April 29, 2021

Avant de commencer à utiliser la fonctionnalité Analytics de Citrix Application Delivery Management (Citrix ADM) pour obtenir une visibilité sur vos données d'instance et d'application, il est recommandé de configurer quelques paramètres d'analyse pour garantir une expérience optimale de cette fonctionnalité.

Configuration de la synthèse des bases de données pour Analytics

La fonctionnalité Configurer la synthèse de base de données dans Citrix ADM vous permet de personnaliser la durée pendant laquelle vous souhaitez stocker les données d'analyse historiques de vos instances Citrix ADC. Vous pouvez choisir les types de synthèse de base de données suivants :

- Heures pendant lesquelles conserver les données par minute
- Jours pendant lesquels conserver les données par heure
- Jours pendant lesquels conserver les données quotidiennes

Pour configurer la synthèse de la base de données :

1. Dans un navigateur Web pris en charge, connectez-vous à votre Citrix ADM.
2. Accédez à **Paramètres > Paramètresd'analyse**>**Synthèse de la base** de données.

3. Cliquez sur le nom du type Insight pour lequel vous souhaitez configurer la synthèse de la base de données. Par exemple, si vous souhaitez configurer la synthèse de la base de données pour GatewayInsight, cliquez sur **GatewayInsight**.
4. Spécifiez la durée pendant laquelle vous souhaitez conserver les données Insight sur Citrix ADM, puis cliquez sur **OK.** Par exemple, pour Gateway Insight, vous pouvez stocker les données historiques minutieusement de vos analytiques pendant 2 heures, ou les données horaires pendant 1 jour.

Création de seuils et d'alertes pour Analytics

Vous pouvez définir des seuils et des alertes pour surveiller les mesures analytiques des serveurs virtuels gérés configurés sur les instances découvertes. Lorsque la valeur d'une mesure dépasse le seuil, Citrix ADM génère un événement pour signifier une violation de seuil.

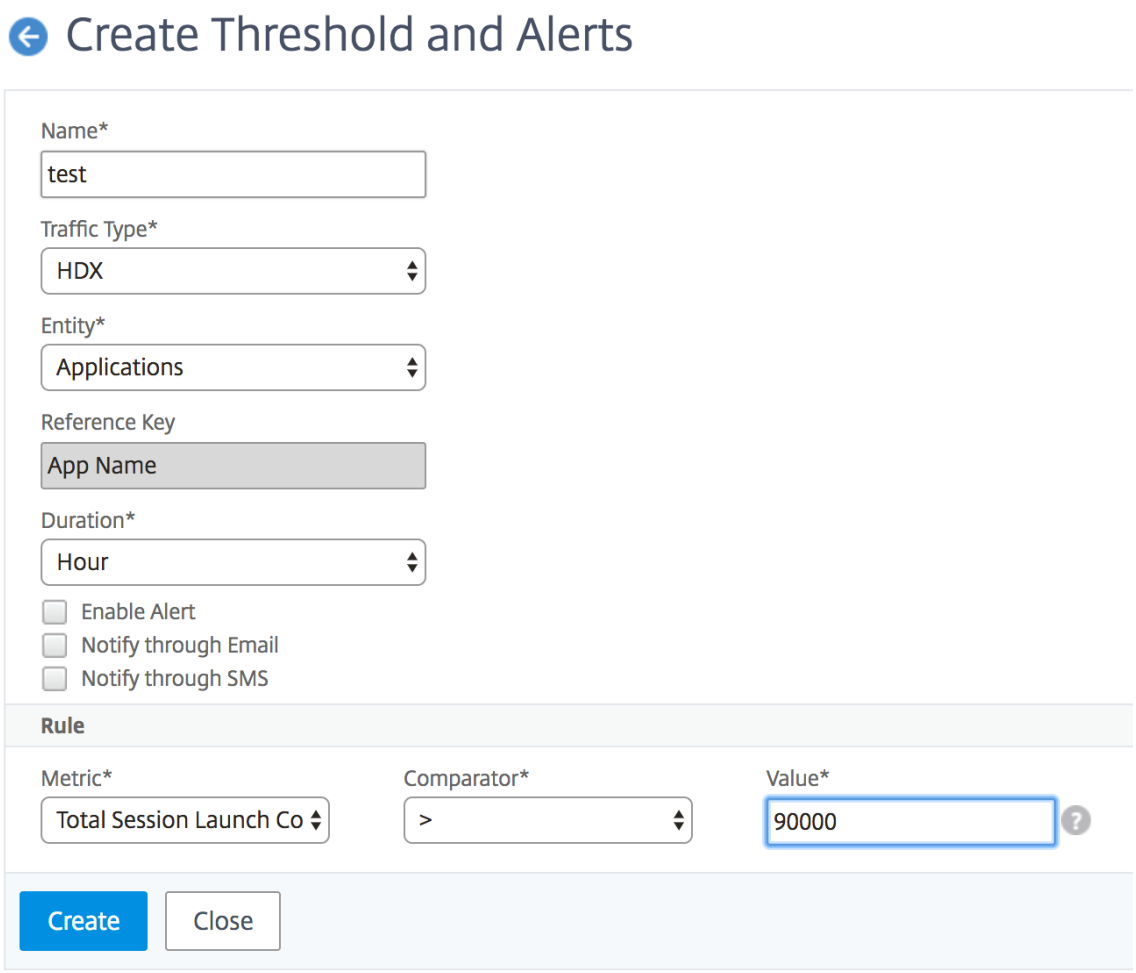
Vous pouvez également associer des actions aux seuils définis. Les actions comprennent l'affichage d'une alerte sur l'interface graphique, l'envoi d'e-mails comme configuré.

Par exemple, vous pouvez définir un seuil pour générer un événement pour l'aperçu HDX si la valeur ICA RTT d'un utilisateur dépasse 1 seconde. Vous pouvez également activer les alertes pour l'événement généré et envoyer les informations de violation de seuil à une liste de messagerie configurée.

Pour créer des seuils et des alertes pour les analyses :

1. Dans un navigateur Web pris en charge, connectez-vous à votre Citrix ADM.
2. Accédez à **Paramètres** > **Paramètres d'analyse** > **Seuils** .
3. Dans l'écran **Seuils**, cliquez sur **Ajouter** pour ajouter un nouveau seuil et configurer les alertes pour les seuils définis.
4. Dans la page **Créer des seuils et des alertes**, spécifiez les détails suivants :
    - **Nom** : nom permettant de configurer le seuil.
    - **Type de trafic** : type de trafic analytique pour lequel vous souhaitez configurer le seuil. Par exemple : HDX Insight, Security Insight.
    - **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 sélectionné et de l'entité.
    - **Durée** - Intervalle pour lequel vous souhaitez configurer le seuil.
5. Pour configurer les notifications par e-mail, activez la case à cocher correspondant aux seuils définis.

6. Dans la section **Règles**, spécifiez les éléments suivants :
   - **Mesure** — Mesure du type de trafic sélectionné pour configurer le seuil.
   - **Comparateur** : comparateur à la mesure sélectionnée (par exemple : <, >=).
   - **Valeur** : valeur de la mesure pour définir le seuil et appeler des alertes.
7. Cliquez sur **Créer**.



Comment attribuer plus d'autorisations à des utilisateurs d'administrateur délégué

April 29, 2021

Lorsque le premier utilisateur de votre organisation s'inscrit et ouvre une session à Citrix Application Delivery Management (Citrix ADM), cet utilisateur se voit attribuer les privilèges de

super-administrateur. Chaque utilisateur suivant qui ouvre une session se voit attribuer un rôle d'administrateur délégué par défaut. Un administrateur délégué n'a pas l'autorisation d'afficher et d'exécuter des tâches liées à l'administration de l'utilisateur ou aux paramètres RBAC.

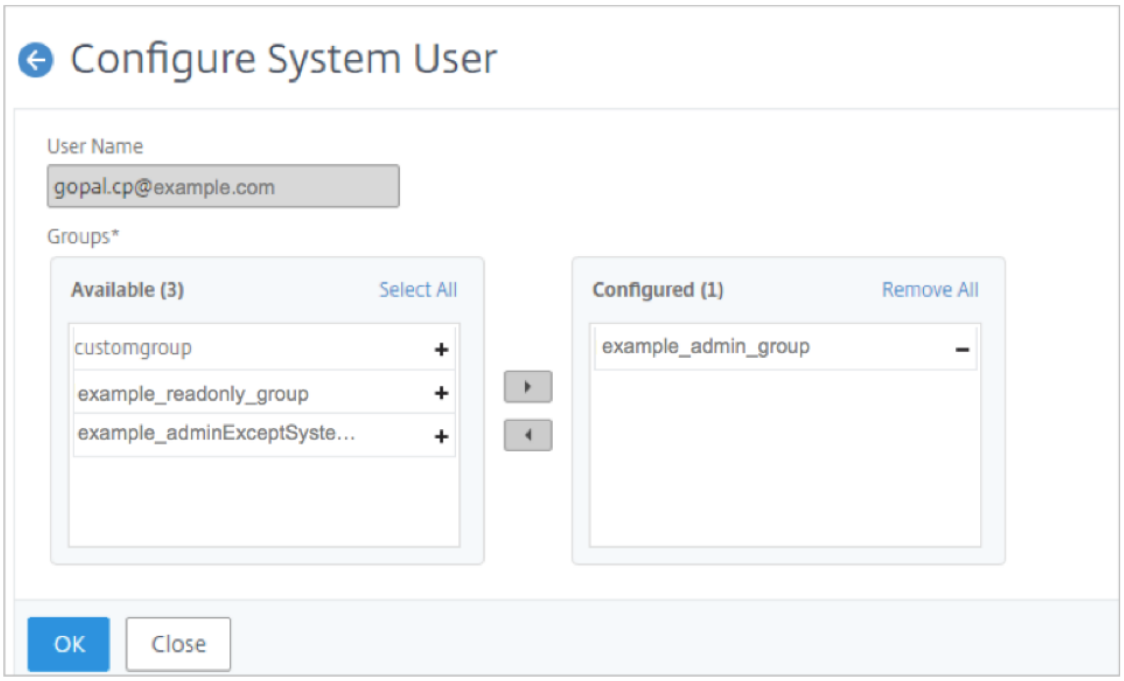
Toutefois, vous pouvez attribuer des privilèges de super-administrateur ou des rôles spécifiques non superadministrateur à un administrateur délégué afin que l'administrateur soit en mesure d'effectuer des tâches liées à l'administration des utilisateurs.

Pour plus d'informations sur le contrôle d'accès basé sur les rôles, reportez-vous à la section Configuration du contrôle d'accès basé sur les rôles.

Affectation d'autorisations Super Admin à un Admin délégué

Pour attribuer des autorisations de super administrateur à un administrateur délégué, un super administrateur doit affecter le groupe d'administration par défaut à un utilisateur administrateur délégué. Effectuez les tâches suivantes :

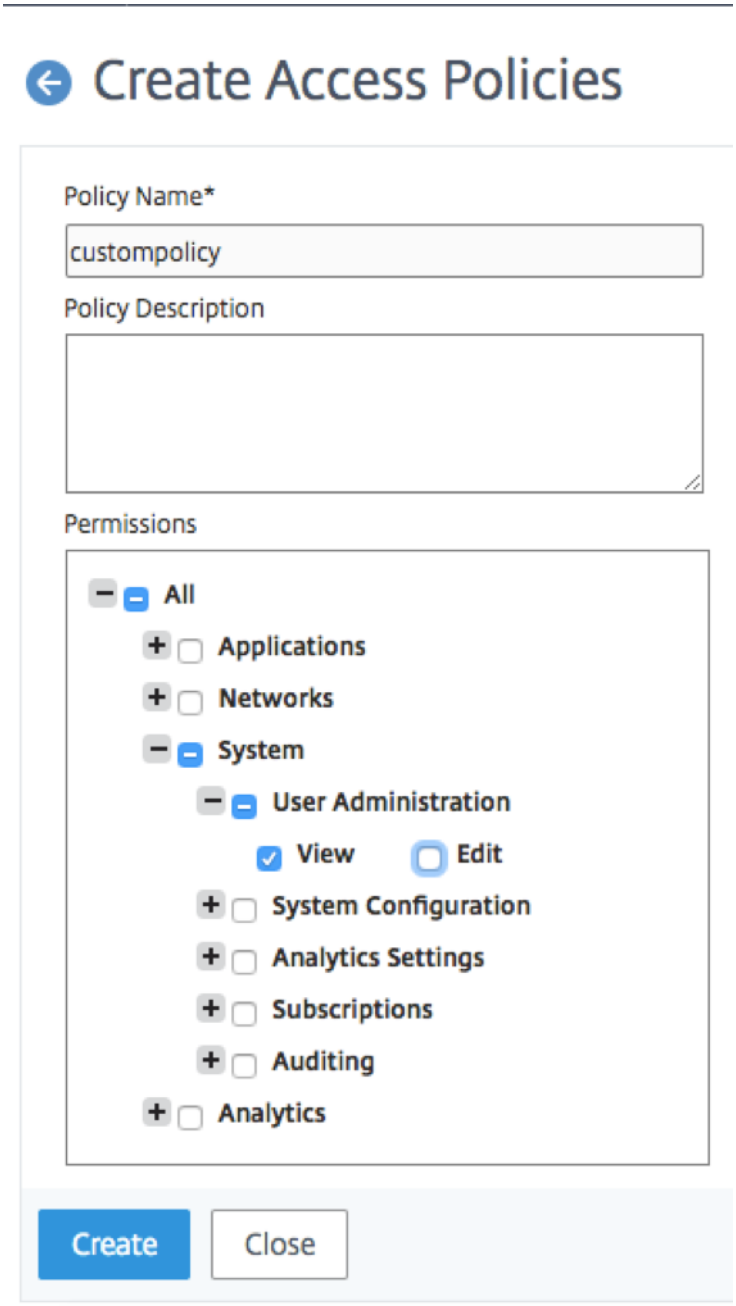
1. Connectez-vous à Citrix ADM en tant que super administrateur.
2. Accédez à **Compte** > **Administration des utilisateurs**> **Utilisateurs**.
3. Sélectionnez le nom d'utilisateur de l'administrateur délégué et cliquez sur **Modifier**.
4. Affectez le groupe ***<nom_tenant>*_admin_group** à l'administrateur délégué et cliquez sur **OK**. Par exemple, dans l'image suivante, « example_admin_group » est attribué à un utilisateur administrateur délégué.



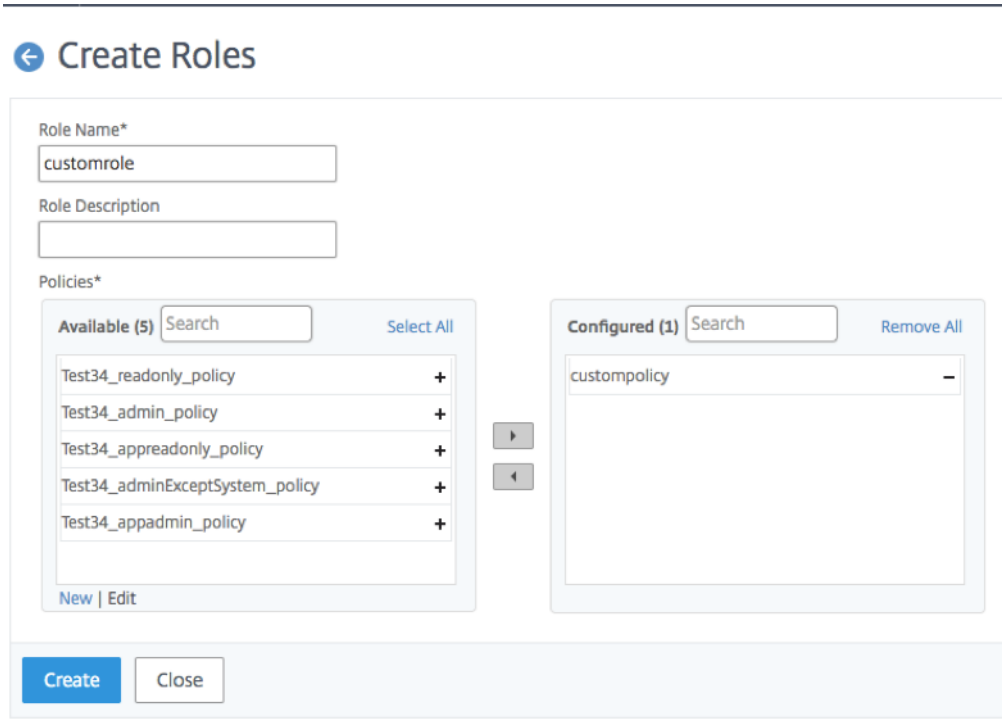
Affectation d'un rôle personnalisé à un administrateur délégué

Pour attribuer un rôle personnalisé à un administrateur délégué, le superadministrateur doit créer un groupe, un rôle et une stratégie et affecter à l'utilisateur administrateur délégué. Cela garantit que l'administrateur délégué dispose uniquement des autorisations requises. Effectuez les tâches suivantes :

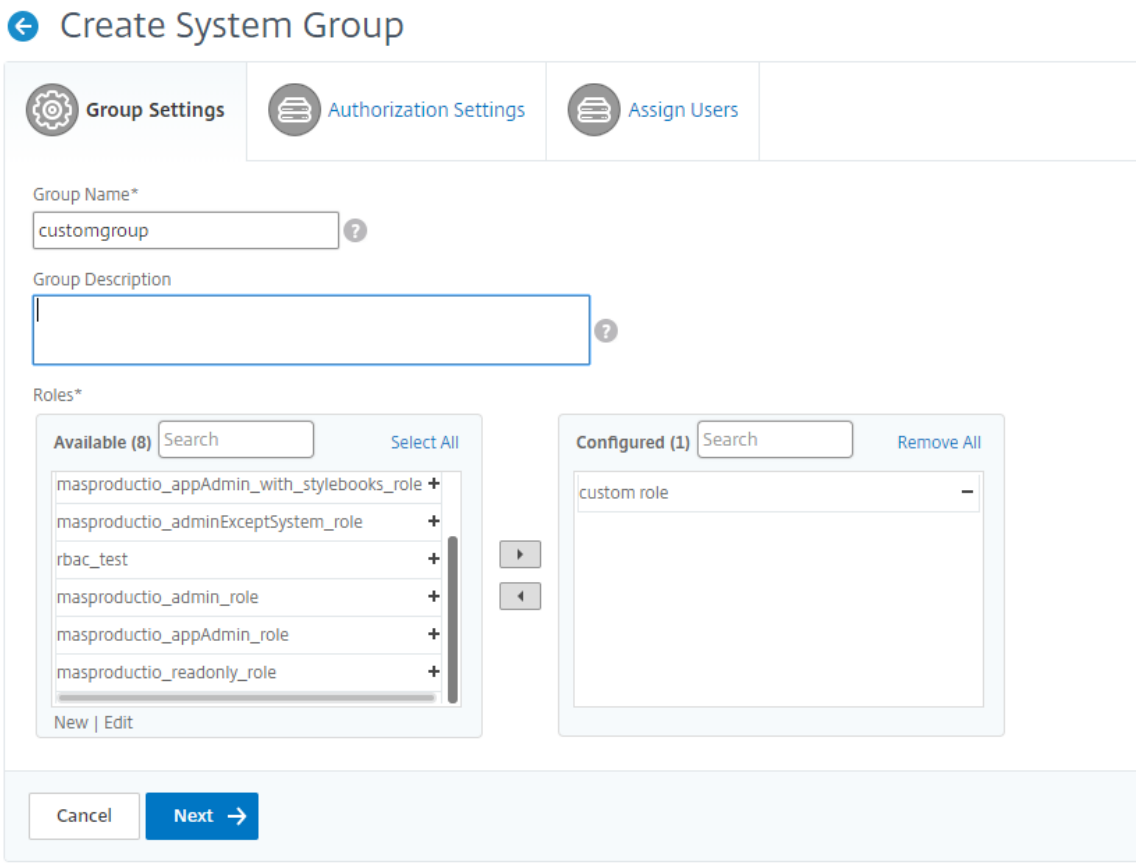
1. Connectez-vous à Citrix ADM en tant que super administrateur.
2. Accédez à **Compte** > **Administration des utilisateurs** > **Stratégies d'accès**. Sélectionnez **Ajouter** pour créer une stratégie d'accès avec les autorisations requises pour l'administrateur délégué. Dans cet exemple, une stratégie d'accès `custompolicy` est créée qui permet l'accès à l'affichage aux paramètres d'administration des utilisateurs.



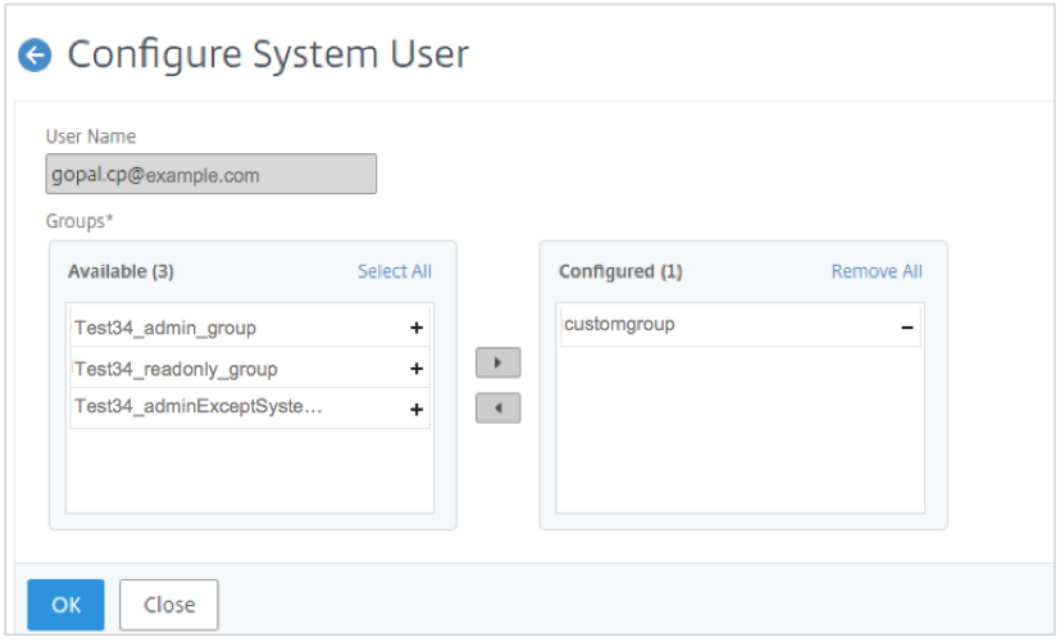
3. Accédez à **Compte** > **Administration des utilisateurs** > **Rôles** . Sélectionnez **Ajouter** pour créer un rôle et lier ce rôle à la stratégie d'accès que vous avez créée à l'étape précédente. Dans cet exemple, un rôle `customrole` est créé et lié à la stratégie `custompolicy` d'accès.



4. Accédez à **Compte** > **Administration des utilisateurs** > **Groupes** . Sélectionnez **Ajouter** pour créer un groupe et lier ce groupe au rôle que vous avez créé à l'étape précédente. Dans cet exemple, le groupe « groupe personnalisé » est créé et lié au rôle « rôle personnalisé ». «



5. Accédez à **Compte** > **Administration des utilisateurs> Utilisateurs**
6. Sélectionnez le nom d'utilisateur de l'administrateur délégué et cliquez sur **Modifier**.
7. Affectez le groupe que vous avez créé à l'étape précédente à l'utilisateur administrateur délégué. Dans cet exemple, l'utilisateur administrateur délégué est affecté au groupe `customgroup`.



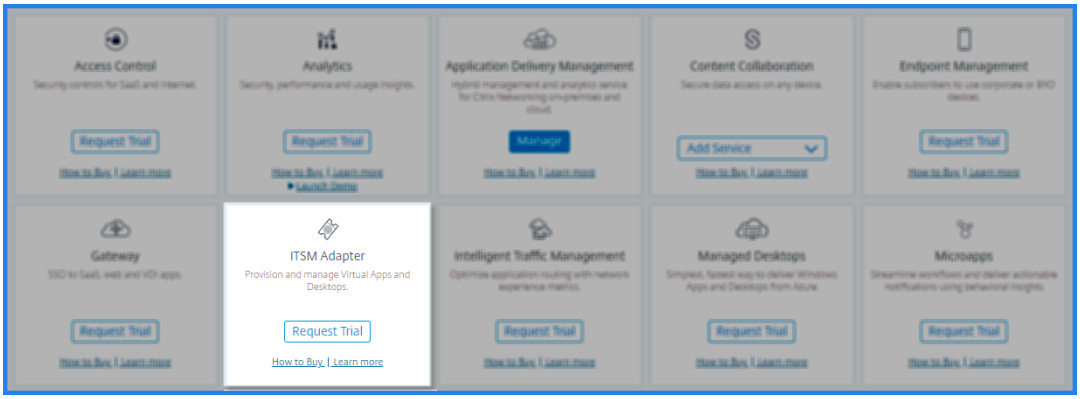
Intégrer Citrix ADM à l'instance ServiceNow

April 29, 2021

Lorsque vous souhaitez activer les notifications ServiceNow pour les événements Citrix ADC et ADM, vous devez intégrer Citrix ADM à l'instance ServiceNow. Pour intégrer ADM à l'instance ServiceNow, utilisezConnecteur Citrix ITSM. Le connecteur ITSM établit la communication entre Citrix ADM et l'instance ServiceNow. Pour de plus amples informations, consultez la section Fonctionnement de l'adaptateur ITSM.

Procédez comme suit pour intégrer Citrix ADM à ServiceNow à l'aide du connecteur ITSM :

1. S'abonner au service **Adapter ITSM** dans Citrix Cloud
    a) Sur la vignette **Adaptateur ITSM**, cliquez sur **Demander une évaluation** .



b) Accédez à **Identity Access and Management** > **API Access** et notez les informations **Client ID** et **Client Secret** .

2. Connectez-vous à votre instance ServiceNow avec des informations d'identification d'administrateur et effectuez les opérations suivantes :

   a) Accédez à la boutique ServiceNow. Téléchargez et installez le **connecteur ITSM Citrix**.

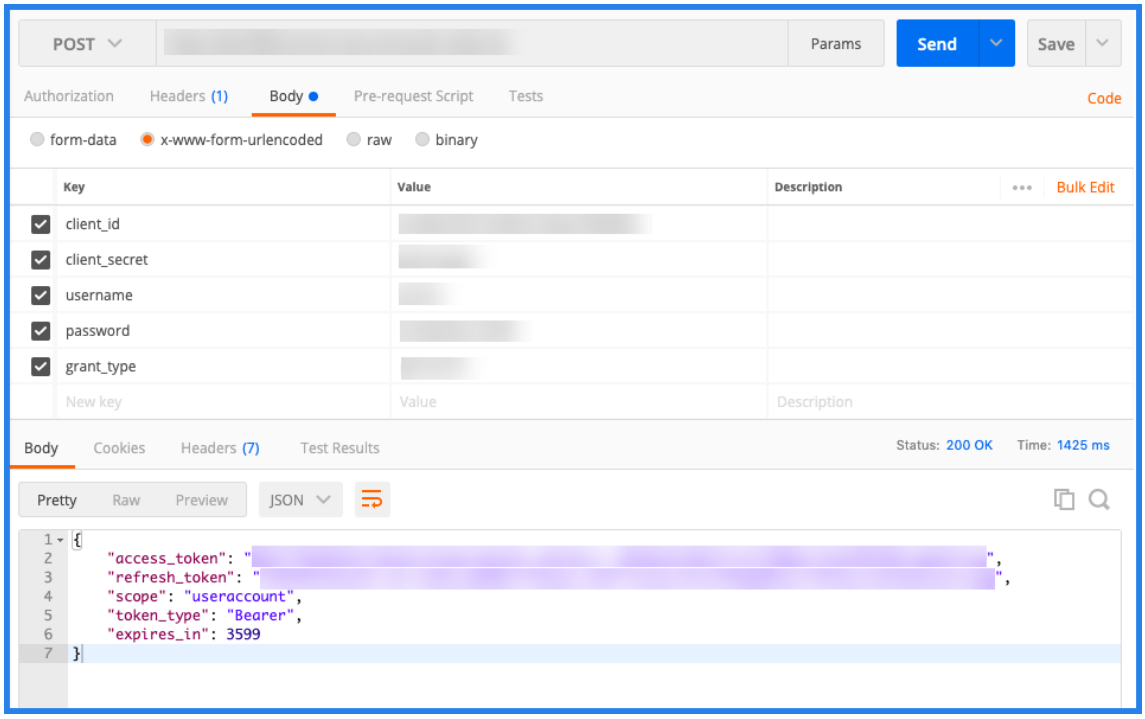
   b) Dans le volet **Citrix ITSM Connector**, sélectionnez **Accueil**, puis cliquez sur **Authentifier** . Tapez l'ID client et le secret que vous avez noté à partir de Citrix Cloud.

   c) Testez la connexion.

   d) Enregistrez la configuration. Un accusé de réception de ServiceNow apparaît indiquant que la connexion est active.

3. Créez un point de terminaison pour accéder à une instance ServiceNow. Voir Créer un point de terminaison pour que les clients puissent accéder à l'instance.

4. Obtenez les jetons d'accès et d'actualisation à l'aide de l'ID client et du secret client. Voir Jetons OAuth.

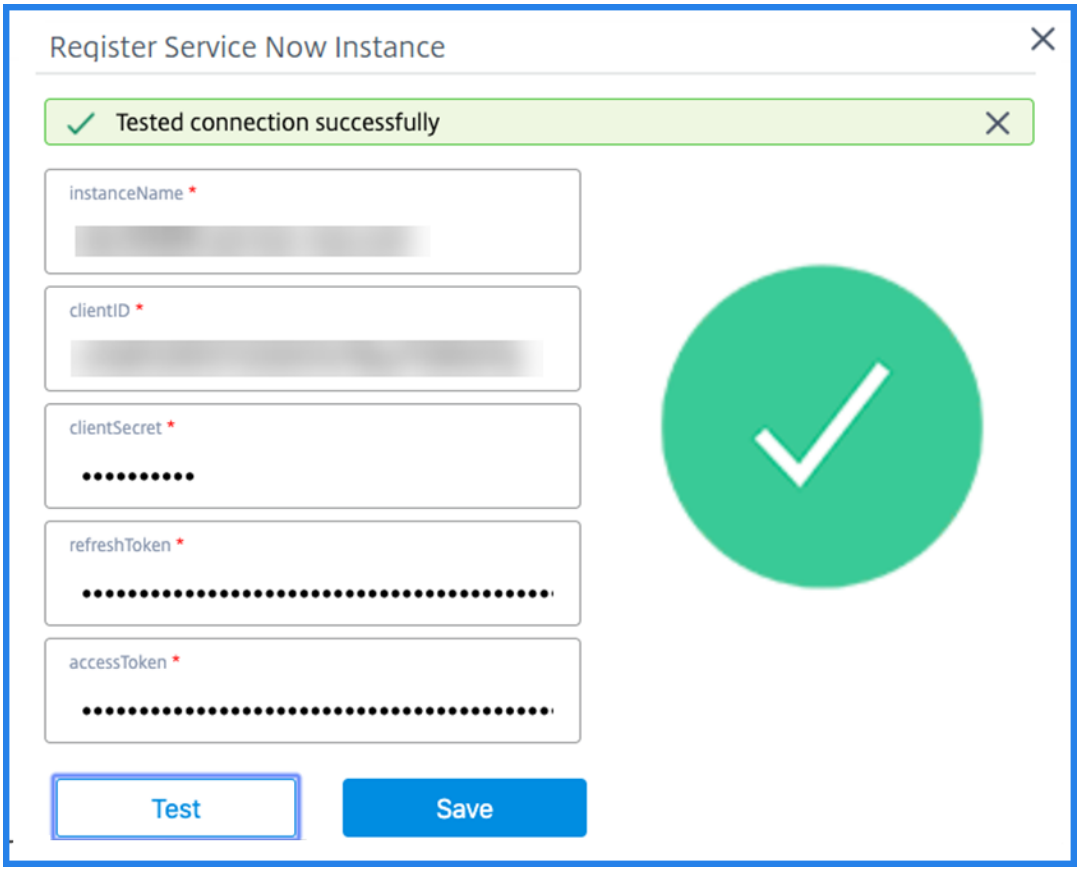


5. Dans l'adaptateur ITSM, ajoutez une instance ServiceNow :

   a) Dans l'onglet **Gérer**, sélectionnez Ajouter une instance ServiceNow.

   b) Spécifiez le **nom de l'instance**, l' **ID client, le secret client**, le**jeton d'actualisation**et le**jeton d'accès**.

   c) Cliquez sur **Tester**.



L'instance de ServiceNow est désormais connectée au service d'adaptateur ITSM.

d) Après avoir testé la connexion avec succès, cliquez sur **Enregistrer** pour ajouter une instance ServiceNow.

6. Testez la génération automatique de tickets ServiceNow dans Citrix ADM.

   a) Connectez-vous à Citrix ADM.

   b) Accédez à **Compte > Notifications** et sélectionnez **ServiceNow** .

   c) Sélectionnez le profil ServiceNow dans la liste.

   d) Cliquez sur **Test** pour générer automatiquement un ticket ServiceNow et vérifier la configuration.

      Si vous souhaitez afficher les tickets ServiceNow dans l'interface graphique Citrix ADM, sélectionnez **ServiceNow Tickets**.

Une fois l'instance ServiceNow enregistrée sur l'adaptateur ITSM, vous pouvez configurer des notifications ServiceNow pour les événements suivants dans l'interface graphique graphique Citrix ADM :

> **Important**
>
> Cette fonctionnalité est prise en charge sur ServiceNow Cloud.

- **Événements Citrix ADC** : Citrix ADM peut générer les incidents ServiceNow pour un ensemble sélectionné d'événements Citrix ADC à partir d'instances Citrix ADC gérées sélectionnées.

  Pour envoyer des notifications ServiceNow pour les événements Citrix ADC à partir des instances gérées, vous devez configurer une règle d'événement et affecter l'action de règle comme **Envoyer des notifications ServiceNow**.

  Créez une règle d'événement sur le service ADM en accédant à **Réseaux** > **Événements** > **Règles**. Pour de plus amples informations, consultez la section Envoyer des notifications ServiceNow.

- **Le certificat SSL et les événements de licence ADM** : Citrix ADM peut générer les incidents ServiceNow pour l'expiration du certificat SSL et les événements d'expiration de la licence ADM.

  Pour envoyer des notifications ServiceNow pour l'expiration d'un certificat SSL, reportez-vous à la sectionExpiration du certificat SSL.

  Pour envoyer des notifications ServiceNow concernant l'expiration d'une licence ADM, reportez-vous à la sectionExpiration de la licence Citrix ADM.

Exporter ou planifier des rapports d'exportation

April 29, 2021

Dans Citrix ADM, vous pouvez exporter un rapport complet pour la fonctionnalité Citrix ADM sélectionnée. Ce rapport fournit une vue d'ensemble du mappage entre les instances, les partitions et les détails correspondants.

Citrix ADM affiche des rapports d'exportation planifiée spécifiques aux entités sous des entités ADM individuelles, que vous pouvez afficher, modifier ou supprimer. Par exemple, pour afficher les rapports d'exportation des instances Citrix ADC, accédez à **Réseau > Instances > Citrix ADC** et cliquez sur l'icône d'exportation. Vous pouvez exporter ces rapports au format PDF, JPEG, PNG et CSV.

Dans **Exporter les rapports**, vous pouvez effectuer les actions suivantes :

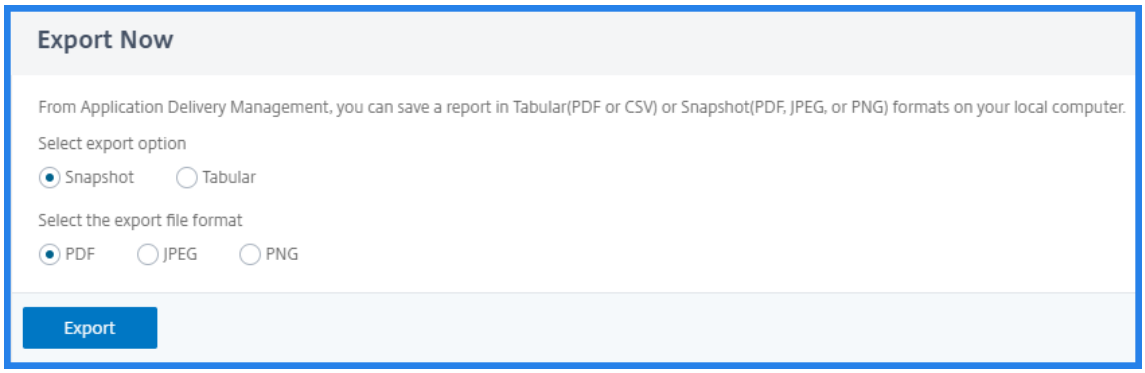
- Exporter un rapport vers un ordinateur local
- Planifier les rapports d'exportation
- Afficher, modifier ou supprimer les rapports d'exportation planifiés

Exporter un rapport

Pour exporter un rapport de l'ADM vers l'ordinateur local, effectuez les opérations suivantes :

1. Cliquez sur l'icône d'exportation dans le coin supérieur droit de la page.
2. Sélectionnez **Exporter maintenant**.

3. Sélectionnez l'une des options d'exportation suivantes :
    - **Snapshot** - Cette option exporte les rapports ADM sous la forme d'un instantané.
    - **Tabulaire** - Cette option exporte les rapports ADM dans un format tabulaire. Vous pouvez également choisir le nombre d'enregistrements de données à exporter dans un format tabulaire



4. Sélectionnez le format de fichier que vous souhaitez enregistrer le rapport sur votre ordinateur local.
5. Cliquez sur **Exporter**.

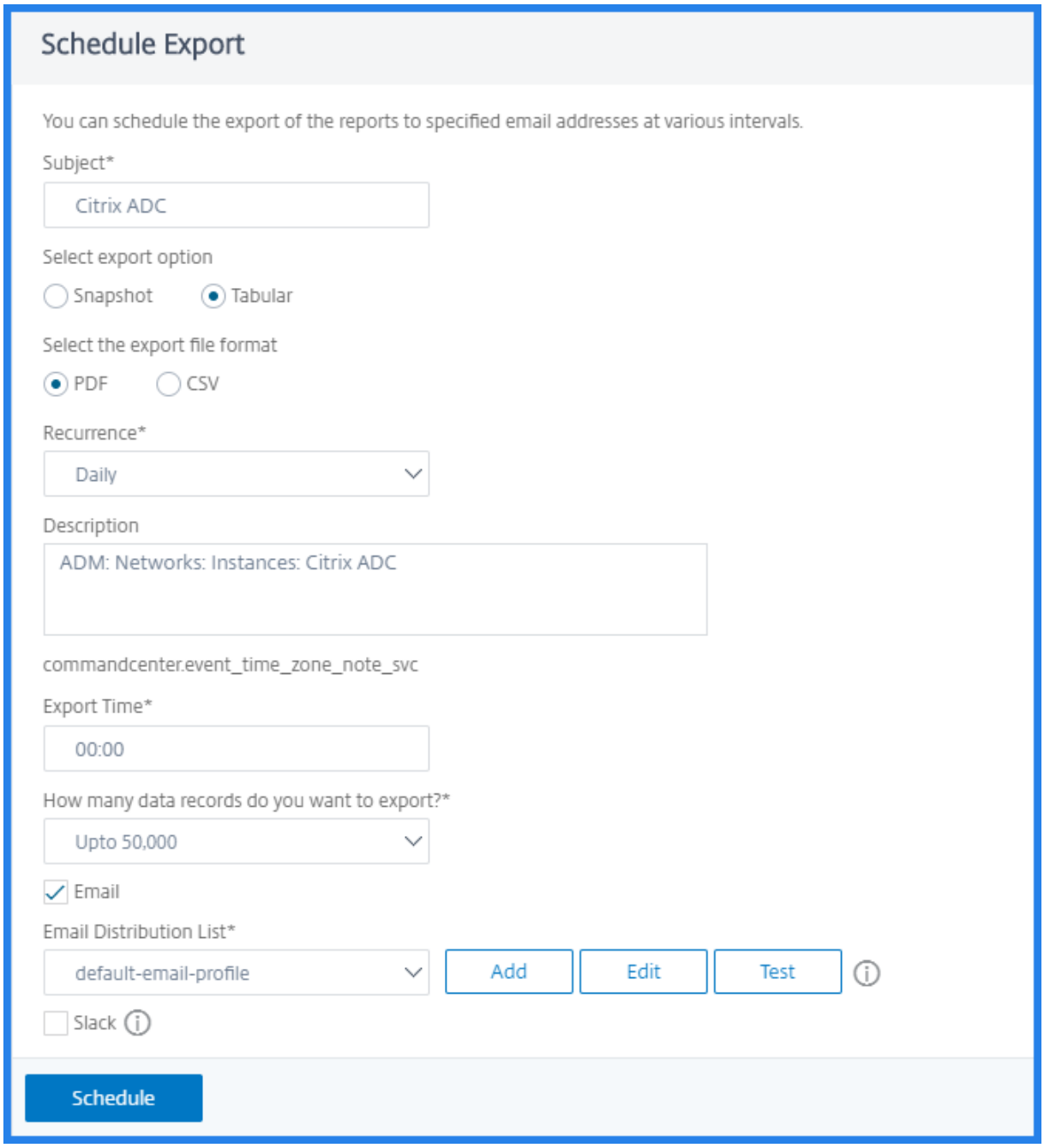
Planifier le rapport d'exportation

Pour planifier le rapport d'exportation à intervalles réguliers, spécifiez l'intervalle de récurrence. Citrix ADM envoie le rapport exporté vers le profil de courrier électronique ou de slack configuré.

1. Cliquez sur l'icône d'exportation dans le coin supérieur droit de la page.
2. Sélectionnez **Planifier l'exportation** et spécifiez les éléments suivants :
    - **Objet** - Par défaut, ce champ remplit automatiquement le nom de la fonction sélectionnée. Cependant, vous pouvez le réécrire avec un titre significatif.
    - **Option d'** exportation - Exporter les rapports ADM dans un instantané ou un format tabulaire. Vous pouvez également choisir le nombre d'enregistrements de données à exporter dans un format tabulaire
    - **Format** : sélectionnez le format de fichier que vous souhaitez recevoir le rapport sur le profil de courrier électronique ou de slack configuré.
    - **Récurrence** : sélectionnez **Quotidien**, **Hebdomadaire**ou **Mensuel** dans la liste.
    - **Description :** spécifiez la description significative d'un rapport.
    - **Heure d'exportation** : spécifiez l'heure à laquelle vous souhaitez exporter le rapport.
    - **E-mail** - Cochez la case et sélectionnez le profil dans la zone de liste. Si vous souhaitez ajouter un profil, cliquez sur **Ajouter**.

- **Slack** - Activez la case à cocher et sélectionnez le profil dans la zone de liste. Si vous souhaitez ajouter un profil, cliquez sur **Ajouter**.

3. Cliquez sur **Planifier**.



Afficher et modifier les rapports d'exportation planifiée

Pour afficher les rapports d'exportation, effectuez les opérations suivantes :

1. Cliquez sur l'icône d'exportation dans le coin supérieur droit de la page.

La page **Exporter le rapport** affiche tous les rapports d'exportation spécifiques à la fonction.

2. Sélectionnez le rapport à modifier, puis cliquez sur **Modifier**.

Avis de mise à

April 29, 2021

En tant qu'administrateur réseau, vous pouvez gérer de nombreuses instances ADC exécutées sur différentes versions ADC dans Citrix ADM. La surveillance du cycle de vie de chaque instance ADC peut être une tâche lourde. Vous devez visiter Tableau des produits Citrix, identifier les instances ADC qui atteignent ou atteignent la fin de vie (EOL) ou la fin de la maintenance (EOM). Ensuite, planifiez leur mise à niveau.

Pour faciliter ce processus, l'avis de mise à niveau Citrix ADM vous aide à surveiller le cycle de vie de vos instances ADC de la manière suivante :

- Identifie les instances atteignant ou atteintes EOL ou EOM. Ainsi, vous pouvez planifier les mises à niveau ADC avant la date EOL ou EOM.
- Surligne les instances qui ne sont pas sur la dernière version ou version. Vous pouvez mettre à niveau ces instances vers la dernière version ou version. Avec cette mise à niveau, vous recevez des mises à jour sur les nouvelles fonctionnalités et les problèmes résolus.
- Met en surbrillance les instances qui ne sont pas sur les versions ADC préférées. Certaines organisations peuvent avoir des builds ADC préférés pour leurs instances. Dans ADM, vous pouvez définir la construction préférée pour votre organisation en fonction de la stabilité de la génération, des fonctionnalités et d'autres considérations. Ensuite, passez en revue et mettez à niveau les instances qui ne sont pas sur les versions préférées. Les instances exécutant les versions préférées sont indiquées par une icône en étoile.
- Met en surbrillance les instances exécutées sur les versions ou versions les plus populaires. Les instances exécutant les versions populaires sont indiquées par une icône de ruban.

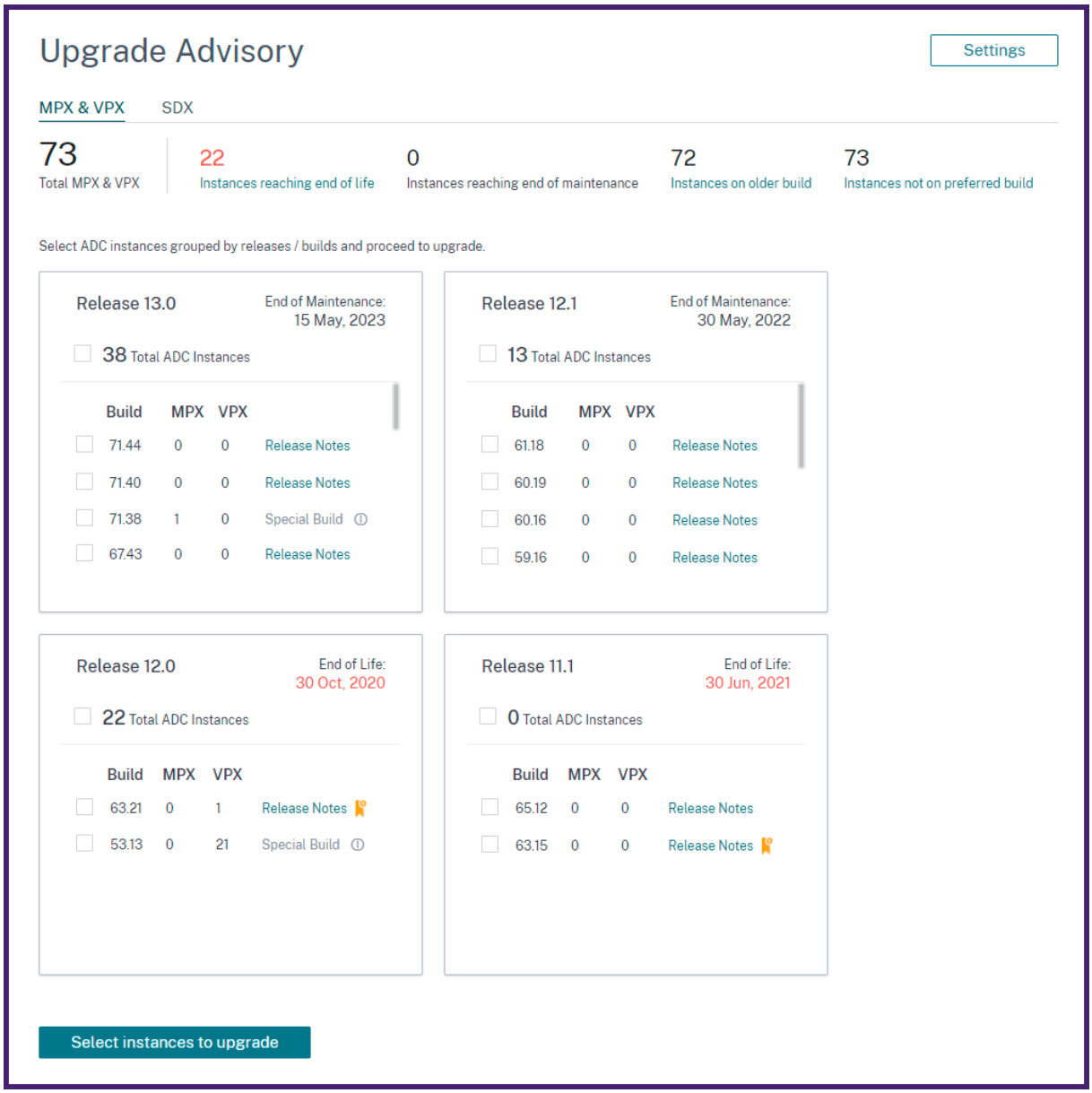
L'avis de mise à niveau fournit des liens vers les notes de version correspondantes. Avec ces informations, vous pouvez consulter et décider d'une version ADC pour la mise à niveau. Vous pouvez continuer à créer un travail de maintenance pour mettre à niveau des instances ADC à partir de la page Avis de mise à niveau.

> Avis de mise à niveau**important**
>
> surveille uniquement la fin de vie des versions du logiciel ADC. Il ne vérifie pas l'EOL des appareils ADC.

Consulter l'avis de mise

Naviguez **Réseaux > Avis d'instance > Avis de mise à niveau** et affichez les informations suivantes :

- Nombre total d'instances ADC.
- Les instances atteignant la fin de la vie.
- Instances atteignant la fin de la maintenance.
- Instances dans une version antérieure.
- Instances qui ne sont pas dans la construction préférée.
- Dates de fin de vie et de fin de maintenance pour les différentes versions CAN.



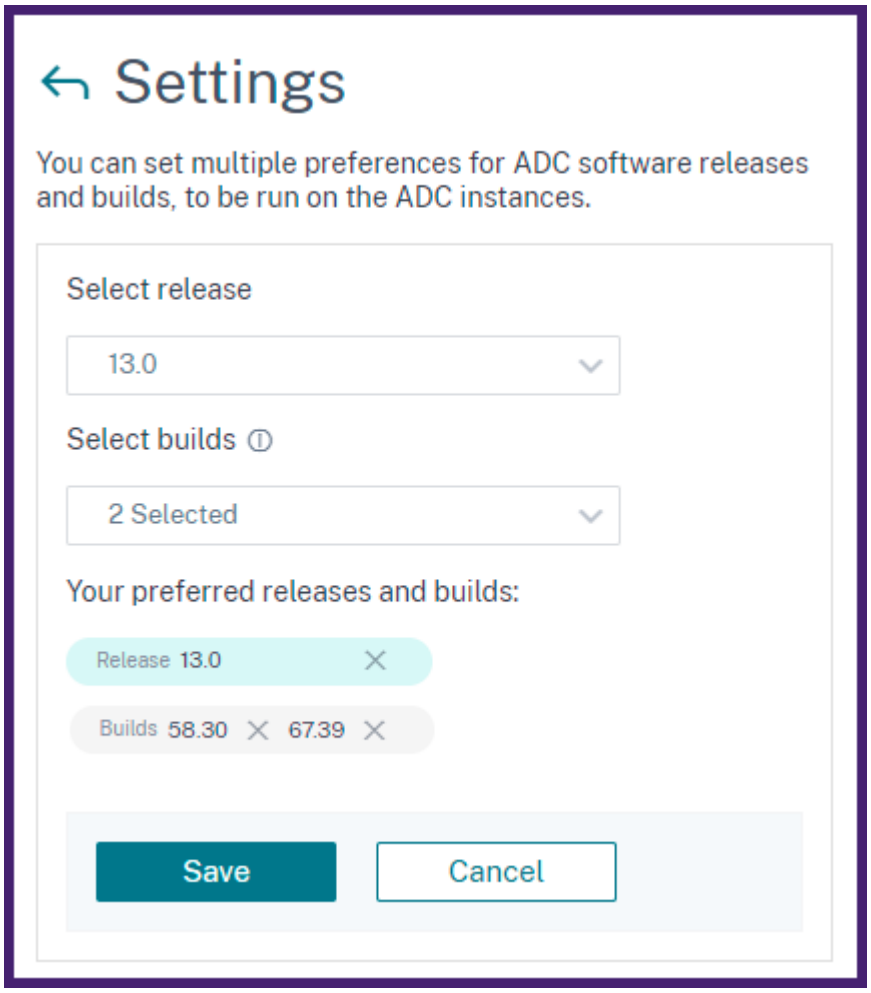
La page **Avis de mise à niveau** regroupe les instances ADC en fonction de leurs versions. Le lien **Notes de mise** à jour vous guide vers les notes de mise à jour spécifiques d'ADC. Examinez les nouvelles

fonctionnalités, les problèmes résolus et connus avant de décider de procéder à la mise à niveau. Vous pouvez sélectionner plusieurs instances ADC dans différentes versions à mettre à niveau à la fois. Lorsque vous procédez à une mise à niveau, elle crée un travail de mise à niveau. Consultez Mettre à niveau les instances ADC.

Définir les versions préférées

En tant qu'administrateur, vous pouvez définir une version ADC préférée pour l'organisation. Pour définir la construction préférée, procédez comme suit :

1. Dans **Réseaux > Avis d'instance > Avis de mise à niveau**, cliquez sur **Paramètres**.
2. Sélectionnez la version préférée et la génération.



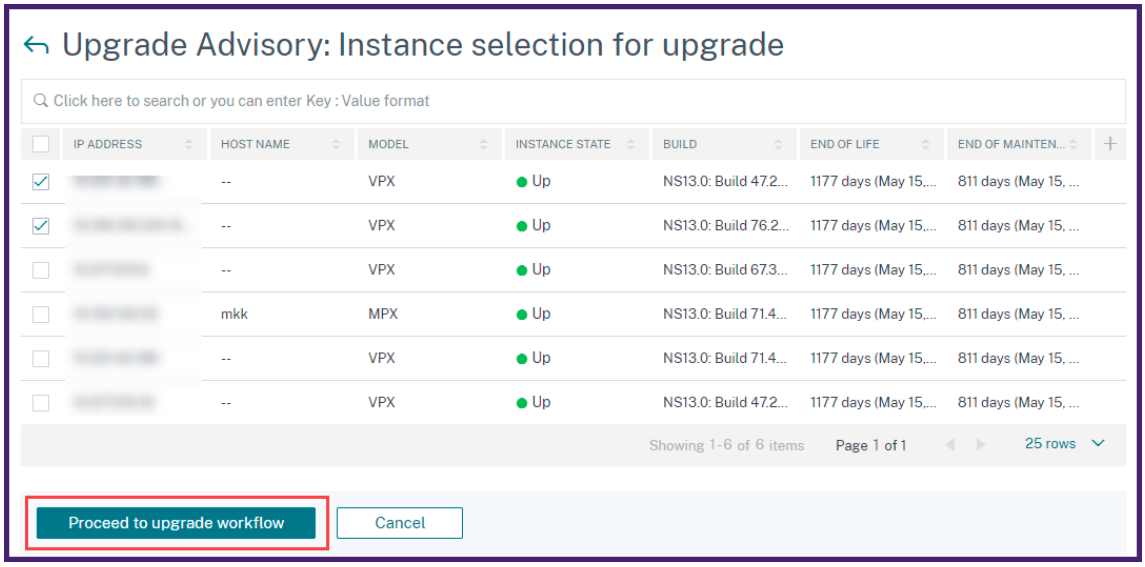
Dans cet exemple, les versions préférées sont `13.0-58.30` et `13.0-67.39`.

3. Cliquez sur **Enregistrer**.

Mettre à niveau les instances ADC

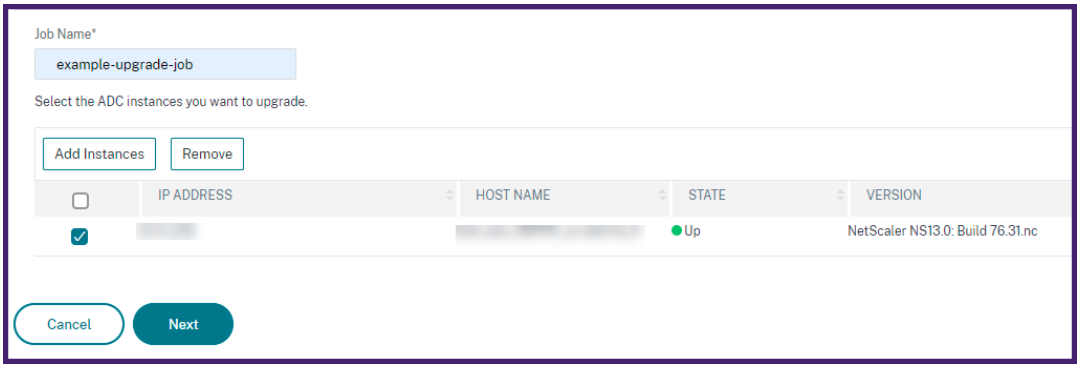
Dans la page **Avis de mise à niveau**, après votre examen, procédez comme suit pour mettre à niveau les instances ADC requises :

1. Sélectionnez les versions d'instance que vous souhaitez mettre à niveau, puis cliquez sur **Sélectionner les instances à mettre à niveau**.
2. Sélectionnez l'instance ADC à mettre à niveau et cliquez sur **Continuer pour mettre à niveau le workflow**.



Ce flux de travail crée une tâche de mise à niveau.

3. Dans l'onglet **Sélectionner une instance**,
   a) Spécifiez un nom pour le travail de mise à niveau.
   b) (Facultatif) si vous souhaitez ajouter d'autres instances, cliquez sur **Ajouter des instances**.



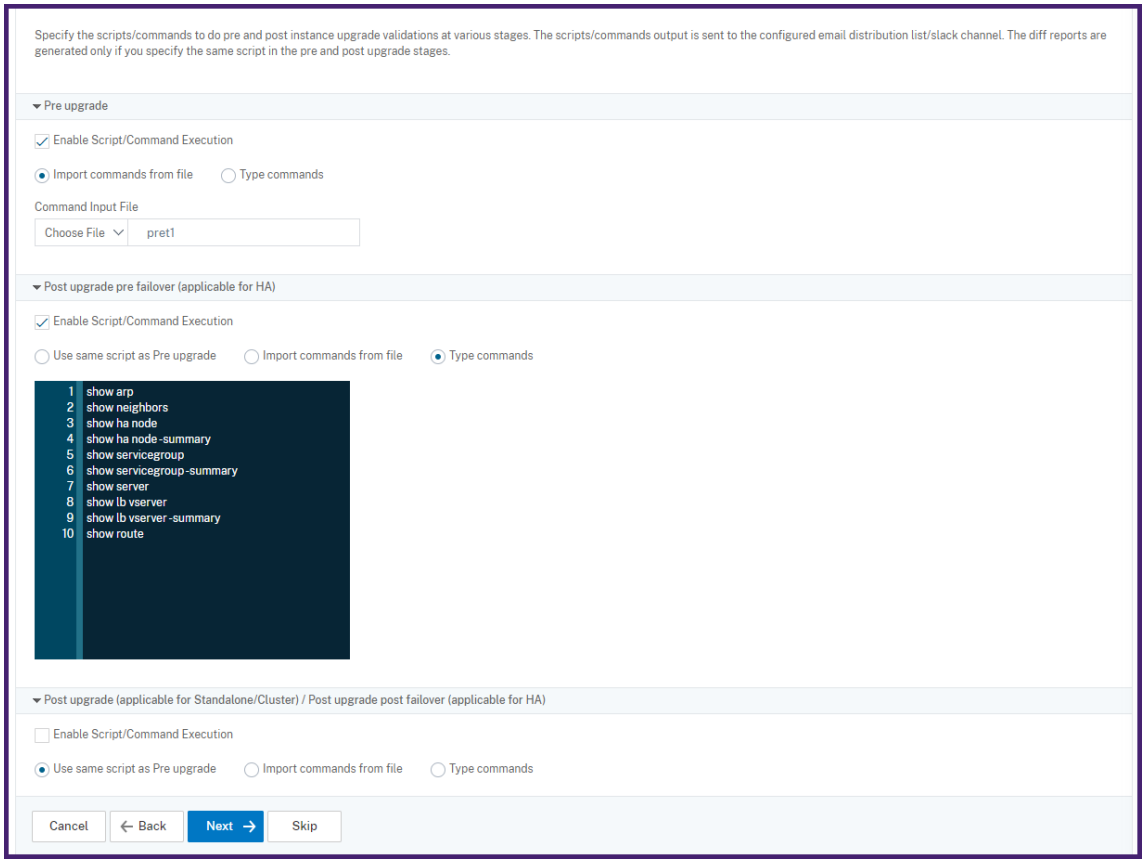
   c) Cliquez sur **Suivant**.

La validation préalable à la mise à niveau démarre.

4. Dans l'onglet **Validation pré-mise à niveau**, supprimez les instances ayant échoué et continuez.

   Si vous rencontrez un espace disque insuffisant sur une instance, vous pouvez vérifier et nettoyer l'espace disque. Consultez Nettoyer l'espace disque ADC.

5. Facultatif, dans l'onglet **Scripts personnalisés**, spécifiez les scripts à exécuter avant et après une mise à niveau d'instance.

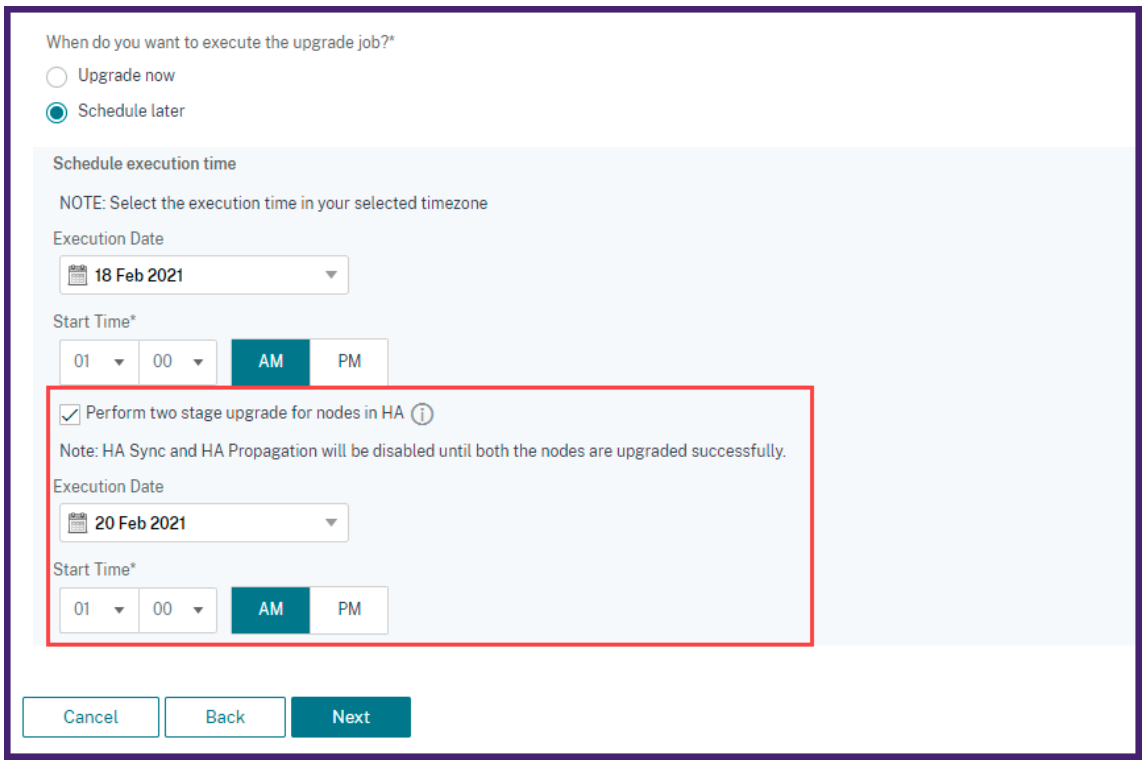


   Pour de plus amples informations, consultez la section Utiliser des scripts personnalisés.

6. Dans **Planifier la tâche**, sélectionnez l'une des options suivantes :

   - **Mise à niveau maintenant** - Le travail de mise à niveau s'exécute immédiatement.
   - **Planifier plus tard** - Sélectionnez cette option pour exécuter ce travail de mise à niveau ultérieurement. Spécifiez la **date d'exécution** et l'**heure de début** lorsque vous souhaitez mettre à niveau les instances.

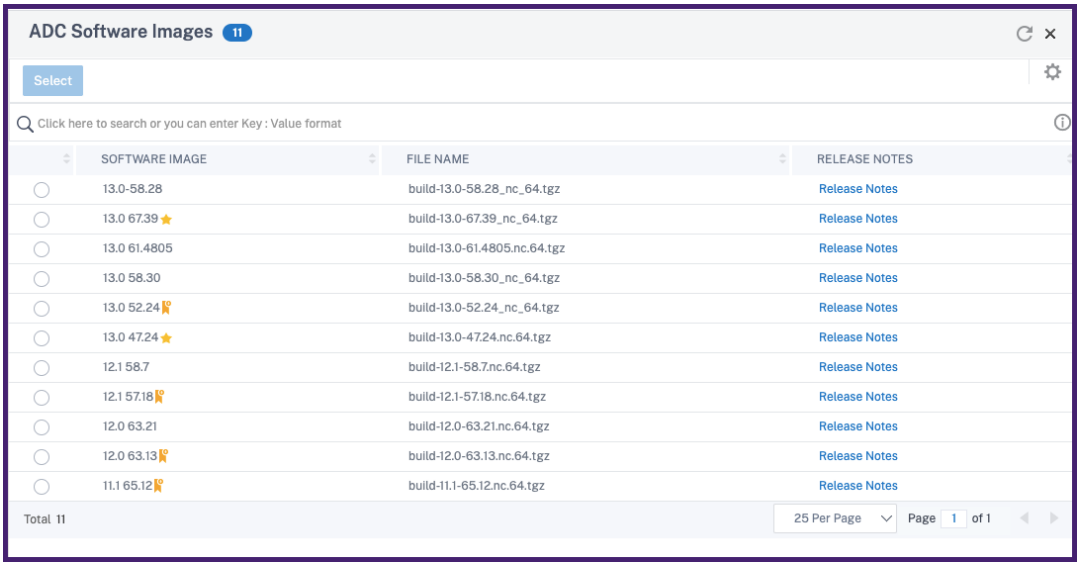
   Si vous souhaitez mettre à niveau une paire ADC haute disponibilité en deux étapes, sélectionnez Effectuer une mise à niveau en deux étapes pour les nœuds en HA.



Pour de plus amples informations, consultez la section Mettre à niveau la paire ADC haute disponibilité.

7. Dans l'onglet **Créer un travail**, spécifiez l'une des options suivantes :

   - **Sélectionnez l'image du logiciel ADC** : sélectionnez une image ADC dans la liste. Cette option répertorie toutes les images ADC disponibles sur le site Web Citrix Téléchargements.



   - **Télécharger l'image du logiciel ADC** : vous pouvez télécharger l'image à partir de votre ordinateur local ou de l'appliance ADC. Lorsque vous sélectionnez le dispositif

ADC, l'interface graphique ADM affiche les fichiers d'instance présents dans `/var/mps/mps_images`. Sélectionner l'image à partir de l'interface graphique ADM

Si vous planifiez le travail de mise à niveau, vous pouvez spécifier quand vous souhaitez télécharger l'image vers une instance :

- **Télécharger maintenant** : sélectionnez cette option pour télécharger l'image immédiatement. Toutefois, le travail de mise à niveau s'exécute à l'heure planifiée.
- **Charger au moment de l'exécution** : sélectionnez cette option pour télécharger l'image au moment de l'exécution du travail de mise à niveau.

Pour plus d'informations sur les autres options, reportez-vous à la section Options de mise à niveau ADC.

Avis de sécurité

April 29, 2021

Une infrastructure sûre, sécurisée et résiliente est la ligne de vie de toute organisation. Ainsi, l'organisation doit suivre les nouvelles vulnérabilités et expositions communes (CVE), évaluer l'impact des CVE sur leur infrastructure, comprendre les mesures d'atténuation et de correction, et planifier les mesures d'atténuation et de correction afin de résoudre les vulnérabilités.

L'avis de sécurité Citrix ADM met en évidence les CVE Citrix exposant vos instances ADC à des risques et recommande des mesures d'atténuation et des correctifs. Vous pouvez consulter les recommandations et prendre les mesures appropriées, en utilisant le service ADM pour appliquer les mesures d'atténuation et les correctifs.

Fonctions d'avis de sécurité

Les fonctions d'avis de sécurité suivantes vous aident à protéger votre infrastructure.

- Analyse : inclut l'analyse du système par défaut et l'analyse à la demande.
  - Analyse système : analyse toutes les instances gérées par défaut une fois par semaine. ADM décide de la date et de l'heure des analyses du système, et vous ne pouvez pas les modifier.
  - Analyse à la demande : vous permet d'analyser manuellement les instances si nécessaire. Si le temps écoulé après la dernière analyse du système est important, vous pouvez exécuter une analyse à la demande pour évaluer la posture de sécurité actuelle. Ou analyse après une correction ou une atténuation, afin d'évaluer la posture révisée.

- Analyse d'impact CVE : affiche les résultats de tous les CVE ayant un impact sur votre infrastructure et toutes les instances ADC ayant un impact, et suggère des mesures correctives et des mesures d'atténuation. Utilisez ces informations pour appliquer des mesures d'atténuation et de correction afin de corriger les risques de sécurité.
- Rapports CVE : stocke des copies des cinq dernières analyses. Vous pouvez télécharger ces rapports au format CSV et les analyser.
- Référentiel CVE : donne une vue détaillée de tous les CVE associés aux ADC annoncés par Citrix depuis décembre 2019, qui pourraient avoir un impact sur votre infrastructure ADC. Vous pouvez utiliser cette vue pour comprendre les CVE dans la portée des conseils de sécurité et pour en savoir plus sur le CVE.

Points à noter

Gardez à l'esprit les points suivants lors de l'utilisation de l'avis de sécurité :

- Instances prises en charge pour la détection CVE : tous les ADC (SDX, MPX, VPX, CPX, BLX) et passerelle.
- CVE pris en charge : tous les CVE après déc 2019.
- Portée d'ADC, versions de passerelle : la fonctionnalité est limitée aux versions principales. avis de sécurité n'inclut aucune version spéciale dans sa portée.
  - L'avis de sécurité est pris en charge dans les instances ADC exécutant des versions supérieures à 10.5 et non dans les instances exécutant les versions 10.5 et inférieures.
  - L'avis de sécurité n'est pas pris en charge dans la partition d'administration, les périphériques SD-WAN, HaProxy ou les périphériques hôtes HaProxy.
- Types d'analyse : l'avis de sécurité exécute des analyses de version et des analyses de configuration
  - Analyse des versions : vérifie si la version ADC est une version vulnérable. La logique utilisée est si un CVE est fixé sur la version xx.xx d'ADC, toutes les versions et versions inférieures à xx.xx build sont considérées comme vulnérables.
  - Analyse de configuration : analyse de la configuration ADC pour voir s'il existe un modèle de configuration spécifique qui la rend vulnérable.
- Les analyses n'affectent pas le trafic de production sur ADC et ne modifient aucune configuration ADC sur ADC.

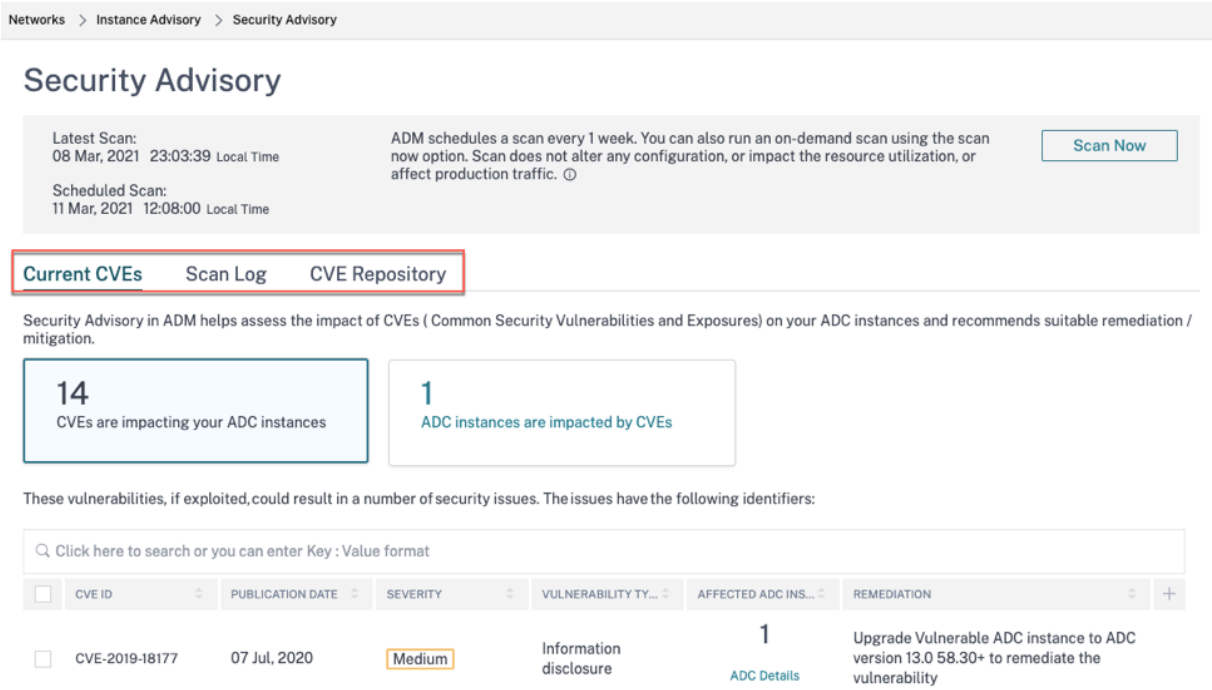
Comment utiliser le tableau de bord des conseils de sécurité

Pour accéder au tableau de bord **Avis de sécurité**, à partir de l'interface graphique ADM, accédez à **Réseaux > Avis d'instance > Avis de sécurité**. Le tableau de bord affiche l'état de vulnérabilité de

toutes les instances ADC que vous gérez via ADM. Les instances sont analysées une fois par semaine ; toutefois, vous pouvez les analyser à tout moment en cliquant sur **Analyser maintenant**.

Le tableau de bord comprend trois onglets :

- CVE actuels
- Journal d'analyse
- Référentiel CVE



> **Important**
>
> Dans l'interface graphique ou le rapport **Security Advisory**, tous les CVE peuvent ne pas apparaître, et vous ne voyez peut-être qu'un seul CVE. Pour contourner le problème, cliquez sur **Analyser maintenant** pour exécuter une analyse à la demande. Une fois l'analyse terminée, tous les CVE dans la portée (environ 15) apparaissent dans l'interface utilisateur ou le rapport.

CVE actuels

Cet onglet affiche le nombre de CVE ayant un impact sur vos instances (dans cet écran, capturez 14 CVE) ainsi que les instances qui sont affectées par les CVE (dans cet écran, capturez un). Les onglets ne sont pas séquentiels, et en tant qu'administrateur, vous pouvez basculer entre ces onglets en fonction de votre cas d'utilisation.

Le tableau indiquant le nombre de CVE ayant un impact sur les instances ADC contient les détails suivants.

ID**CVE : ID**du CVE ayant un impact sur les instances.

Date de publication : date à laquelle le bulletin de sécurité a été publié pour cette CVE.

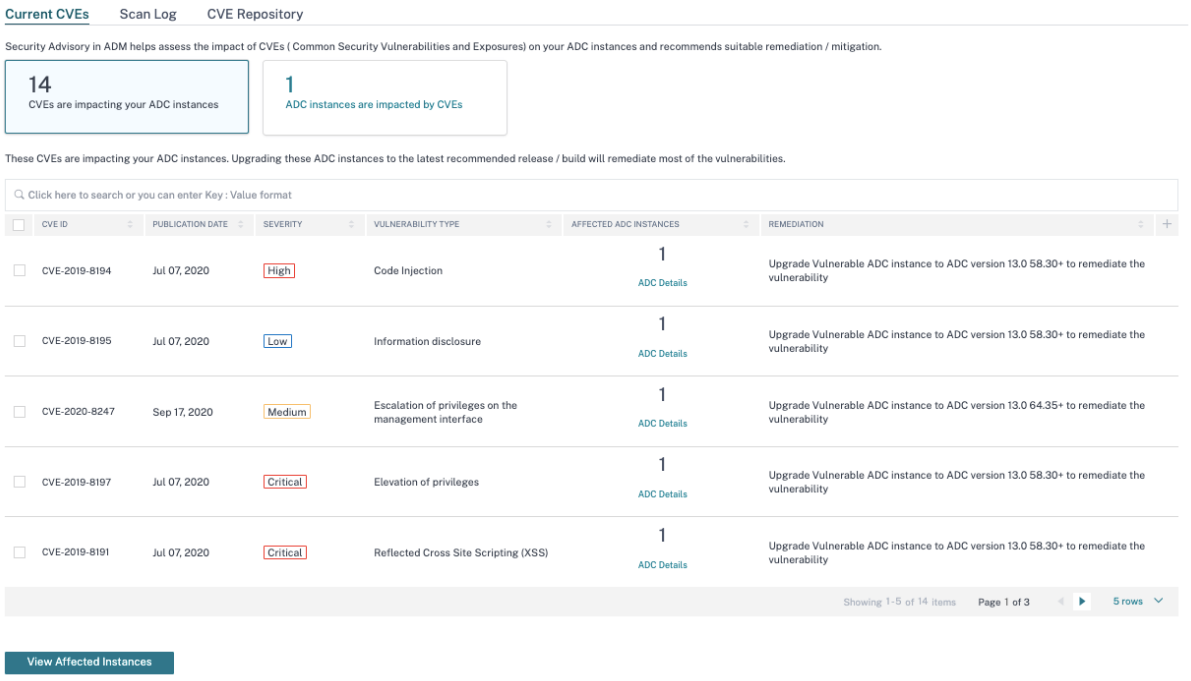
Score de gravité : type de gravité (élevé/moyen/critique) et score. Pour voir le score, passez la souris sur le type de gravité.

Type de vulnérabilité : type de vulnérabilité pour ce CVE.

Instances ADC affectées : le nombre d'instances sur lequel l'ID CVE a un impact. Lorsque vous survolez, la liste des instances ADC apparaît.

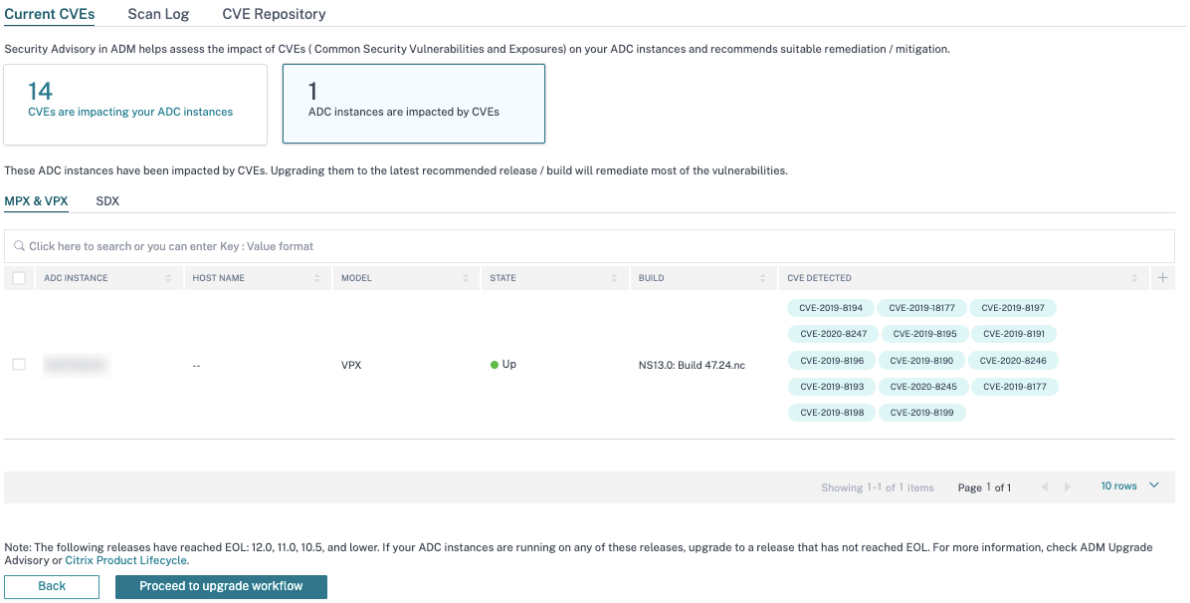
Correction : les correctifs disponibles, qui sont la mise à niveau de l'instance (généralement) ou l'application de packs de configuration.

La même instance peut être affectée par plusieurs CVE. Ce tableau vous aide à voir combien d'instances un CVE particulier ou plusieurs CVE sélectionnés ont un impact. Pour vérifier l'adresse IP de l'instance affectée, passez la souris sur les détails ADC sous **Instances ADC affectées**. Pour vérifier les détails de l'instance affectée, cliquez sur **Afficher les instances affectées** en bas du tableau.
Vous pouvez également ajouter ou supprimer des colonnes dans le tableau en cliquant sur le signe plus.



<number of> Les instances ADC sont affectées par l'onglet CVE affiche toutes les instances ADC gérées par ADM concernées. Le tableau indique l'adresse IP de l'ADC, le nom d'hôte, le numéro de modèle ADC, l'état de l'ADC, la version et la version du logiciel, ainsi que la liste des CVE ayant un impact sur le CAN.

Dans la capture d'écran suivante, une instance ADC est affectée. Vous ajoutez ou supprimez l'une de ces colonnes selon vos besoins, en cliquant sur le signe +.



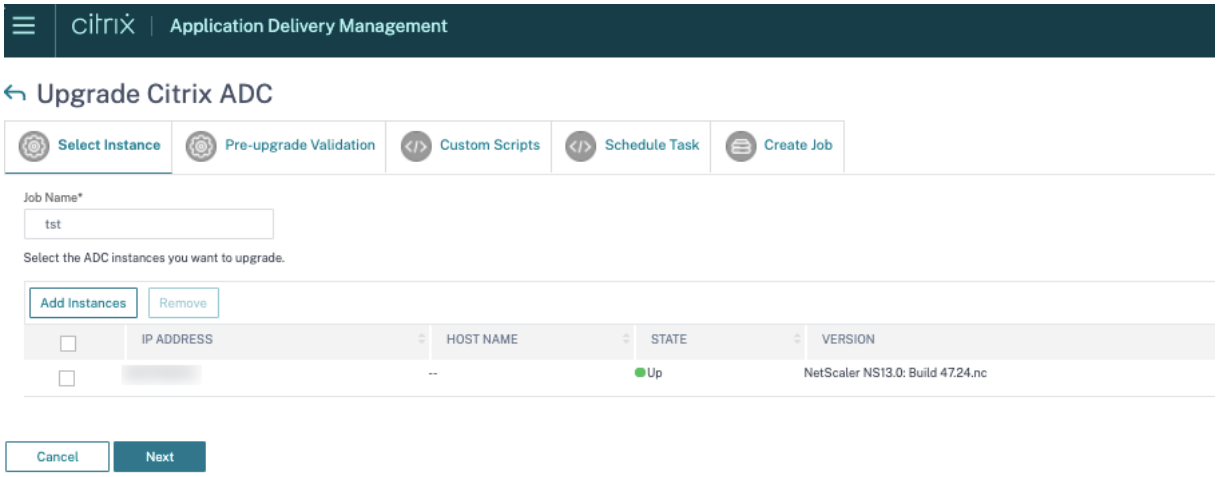
Pour résoudre le problème de vulnérabilité, sélectionnez l'instance ADC et appliquez la correction de recommandation, qui consiste à mettre à niveau l'instance.

- **Mise à niveau** : vous pouvez mettre à niveau les instances ADC vulnérables vers une version et une version avec le correctif. Ce détail peut être vu dans la colonne Correction. Pour mettre à niveau, sélectionnez l'instance, puis cliquez sur **Continuer à mettre à niveau le flux de travail**. Dans le workflow de mise à niveau, l'ADC vulnérable est automatiquement renseigné en tant qu'ADC cible.

> **Remarque**
>
> Les versions 12.0, 11,0, 10.5 et inférieures sont déjà en fin de vie (EOL). Si vos instances ADC s'exécutent sur l'une de ces versions, effectuez une mise à niveau vers une version prise en charge.

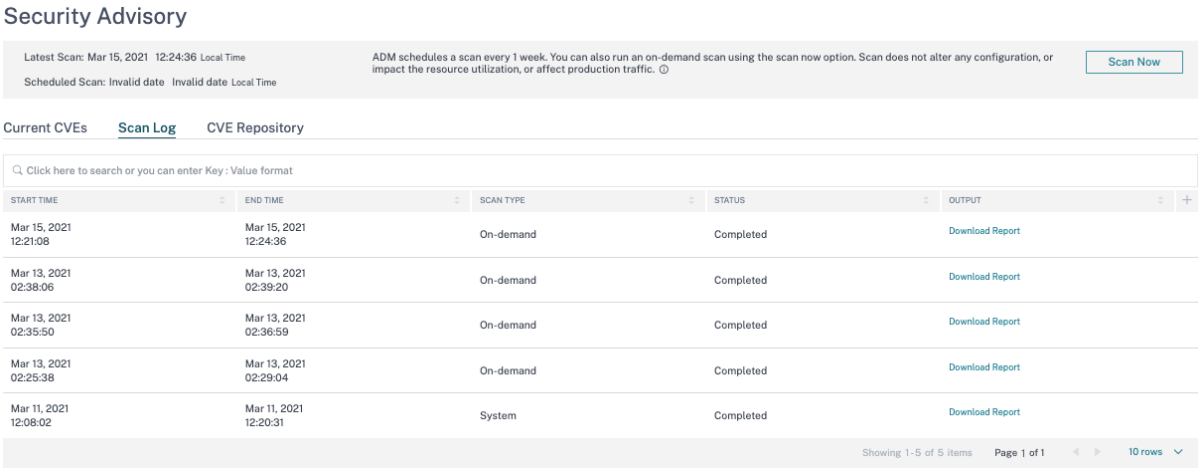
Le workflow de mise à niveau démarre. Pour plus d'informations sur l'utilisation d'ADM pour mettre à niveau des instances ADC, reportez-vous à la section Créer une tâche de mise à niveau ADC.

> **Remarque**
>
> La version et la version vers laquelle vous souhaitez mettre à niveau sont à votre discrétion. Consultez les conseils de la colonne Correction pour savoir quelles versions et versions ont le correctif de sécurité et sélectionnez donc une version et une version prises en charge, qui n'a pas encore atteint la fin de vie.



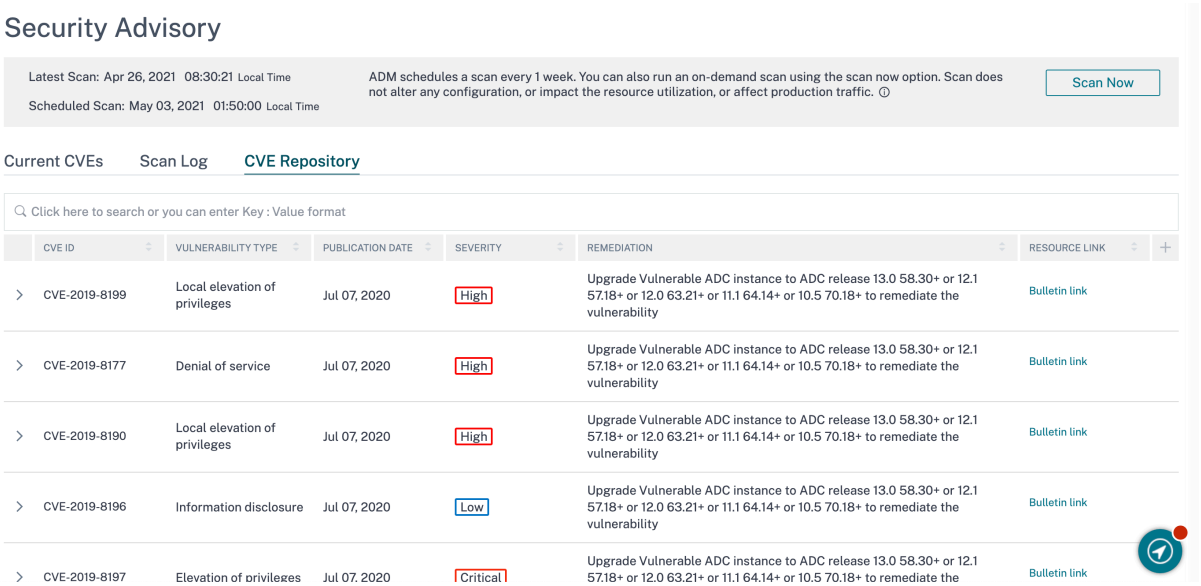
Journal d'analyse

L'onglet affiche les rapports des cinq dernières analyses, qui incluent à la fois des analyses système par défaut et des analyses à la demande lancées par l'utilisateur. Vous pouvez télécharger le rapport de chaque analyse au format CSV. Si une analyse à la demande est en cours, vous pouvez voir l'état d'achèvement ici. Si une analyse a échoué, l'état l'indique.



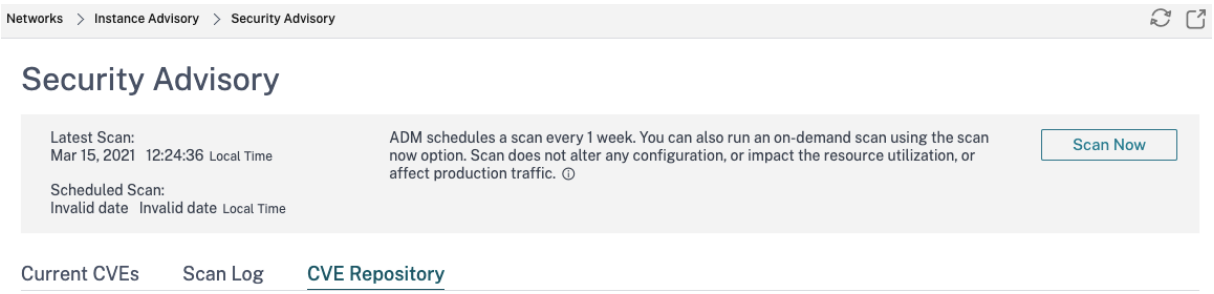
Référentiel CVE

Cet onglet contient les dernières informations de tous les CVE de décembre 2019, ainsi que les ID CVE, le type de vulnérabilité, la date de publication, le niveau de gravité, la correction et les liens vers les bulletins de sécurité.

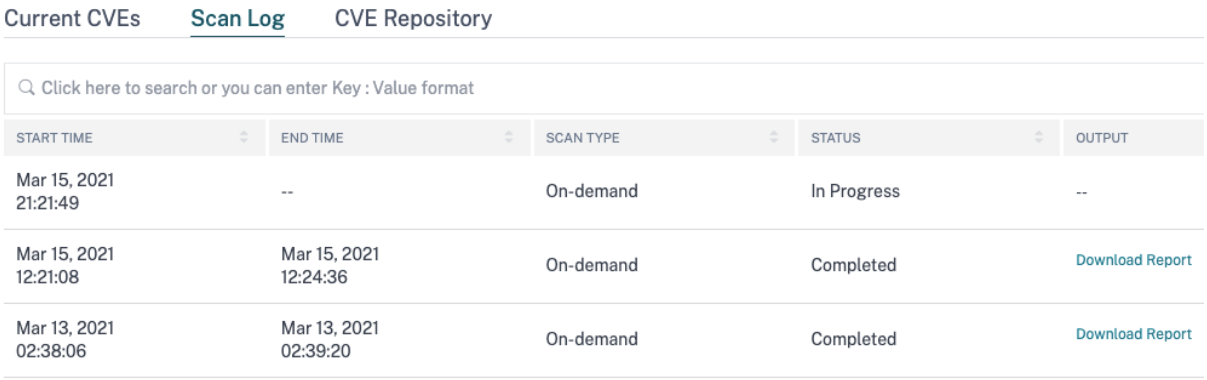


Scanner maintenant

L'avis de sécurité indique la date à laquelle les instances ont été analysées pour la dernière fois et quand la planification suivante est due. Vous pouvez également analyser les instances à tout moment, selon vos besoins. Cliquez sur Analyser maintenant pour obtenir le dernier rapport de sécurité de votre instance. ADM prend quelques minutes pour terminer l'analyse.



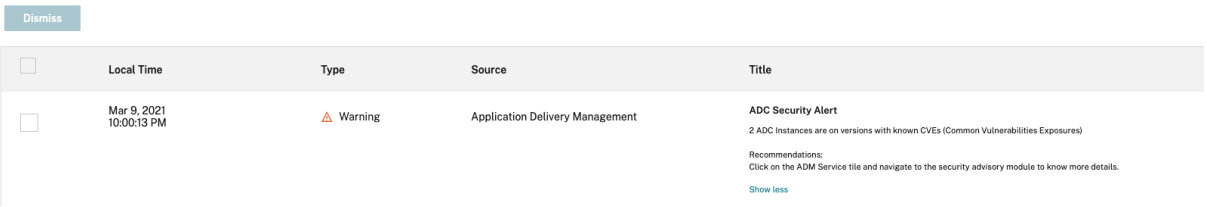
Une fois l'analyse terminée, les détails de sécurité révisés apparaissent dans l'interface graphique de l'avis de sécurité. Vous pouvez également trouver le rapport sous Journal de numérisation, que vous pouvez également télécharger.



> **Remarque**
>
> Le journal d'analyse affiche uniquement les journaux des cinq dernières analyses, qui peuvent être planifiées ou à la demande.

Notification

En tant qu'administrateur, vous recevez des notifications Citrix Cloud, qui indiquent le nombre d'instances ADC vulnérables. Pour voir les notifications, cliquez sur l'icône de cloche située dans le coin supérieur droit de l'interface graphique ADM.



Applications

April 29, 2021

La fonctionnalité d'analyse et de gestion des applications de Citrix ADM vous permet de surveiller les applications via une approche centrée sur les applications. Cette approche vous aide à :

- Vérifier le score et analyser la performance globale des applications
- Vérifiez les problèmes persistants avec le serveur ou le client
- Détecter les anomalies dans les flux de trafic des applications et prendre des mesures correctives

> **Remarque**
>
> Les applications font référence à un ou plusieurs serveurs virtuels configurés sur les instances (Citrix ADC).

Vous pouvez surveiller les applications pour une durée telle que 1 heure, 1 jour, 1 semaine et 1 mois.

Conditions préalables

- Assurez-vous d'avoir ajouté des instances de Citrix ADC dans Citrix ADM
- Assurez-vous que vous disposez d'une licence valide pour vos instances Citrix ADC. Pour de plus amples informations, consultez Système de licences
- Vérifiez que vous avez appliqué la licence pour les serveurs virtuels. Pour de plus amples informations, consultez Gestion des licences sur les serveurs virtuels

Présentation de l'application

Les applications peuvent être :

- Applications discrètes
- Applications personnalisées
- Applications de microservices (k8s_discrete)

Applications discrètes

Tous les serveurs virtuels sous licence sont appelés applications discrètes.

Applications personnalisées

Les serveurs virtuels sous une catégorie sont appelés applications personnalisées. En tant qu'administrateur, vous devez ajouter des applications personnalisées en fonction d'une catégorie. Vous pouvez ensuite gérer et surveiller les applications via le tableau de bord. Vous bénéficiez d'une facilité de surveillance d'applications spécifiques regroupées dans une seule catégorie.

Par exemple, vous pouvez créer une catégorie pour votre datacenter1 et ajouter ses instances ADC. Après avoir défini une catégorie et ajouté l'instance pour votre datacenter1, le tableau de bord de l'application s'affiche avec une catégorie distincte, comprenant toutes les applications liées à votre datacenter 1.

Points à noter

- Les applications discrètes qui sont ajoutées aux applications personnalisées sont supprimées des applications discrètes.
- Toutes les applications qui ne sont pas ajoutées à aucune catégorie sont disponibles en tant que **« autres »**.
- Par défaut, Citrix ADM vous permet d'ajouter des licences pour un maximum de 2 applications. Selon votre licence, vous pouvez sélectionner et appliquer des licences pour les applications que vous souhaitez surveiller.

Applications de microservices

Dans un cluster Kubernetes, Citrix fournit un contrôleur d'entrée pour Citrix ADC MPX (matériel), Citrix ADC VPX (virtualisé) et Citrix ADC CPX (conteneurisé). Pour de plus amples informations, consultez la section Contrôleur d'entrée Citrix.

Les applications discrètes qui sont configurées à l'aide des instances Citrix ADC CPX sont appelées applications de microservices.

Gestion des applications et tableau de bord des applications

April 29, 2021

Citrix ADM vous permet de gérer les applications à partir de la page **Applications** et d'afficher les détails de l'application à partir de la page **Tableau de bord**.

Mes Applications

La page **Applications** vous permet d'afficher toutes les applications personnalisées et discrètes.

À partir de la page Applications, en tant qu'administrateur, vous pouvez :

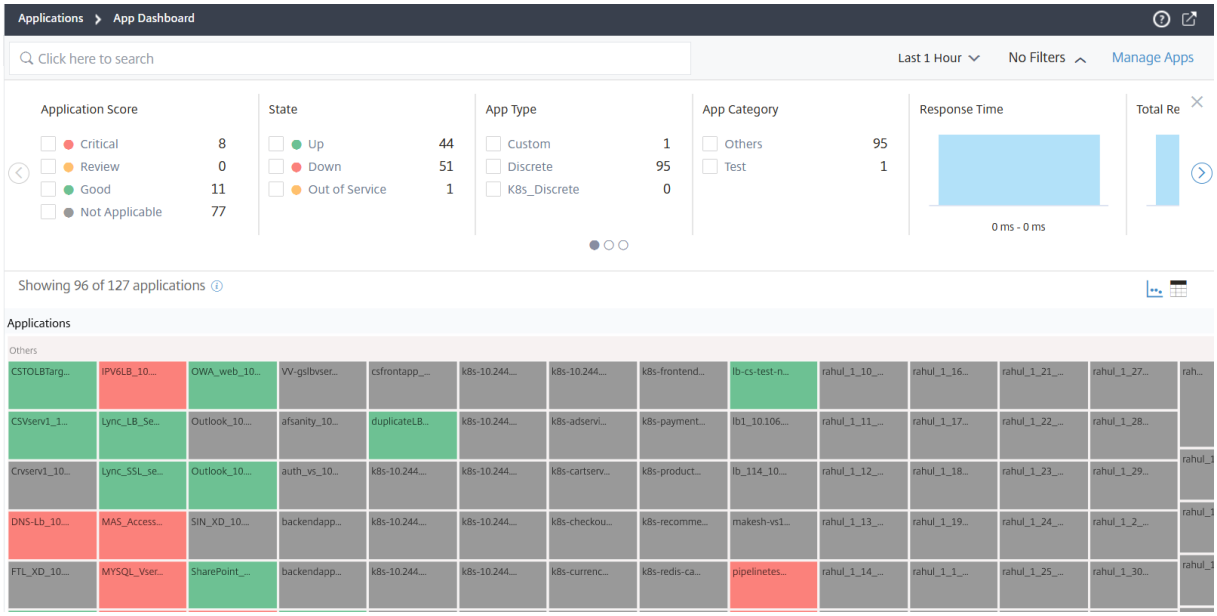
- Ajouter des applications
- Affichez les détails de l'application tels que le nom de l'application, le type d'application, la catégorie d'application, les serveurs virtuels associés, les services associés, etc.
- Modifier ou supprimer des applications personnalisées

Après avoir ajouté, modifié ou supprimé des applications, les détails sont immédiatement reflétés dans la page Applications.

Pour de plus amples informations, consultez la section Mes Applications.

Tableau de bord de l'application

Accédez à **Applications** > **Tableau de bord** pour afficher la liste des applications en mode tabulaire ou graphique.



Toutes les applications sont affichées dans le tableau de bord seulement après que les applications commencent à remplir les données. Dans le tableau de bord, cliquez sur une application pour afficher des informations détaillées sur les performances de l'application. Pour de plus amples informations, consultez la section Détails de l'application.

Si l'analyse de l'application n'est pas affichée même après une durée d'environ 10 à 15 minutes, effectuez les étapes de dépannage à l'adresse Résoudre les problèmes liés au tableau de bord.

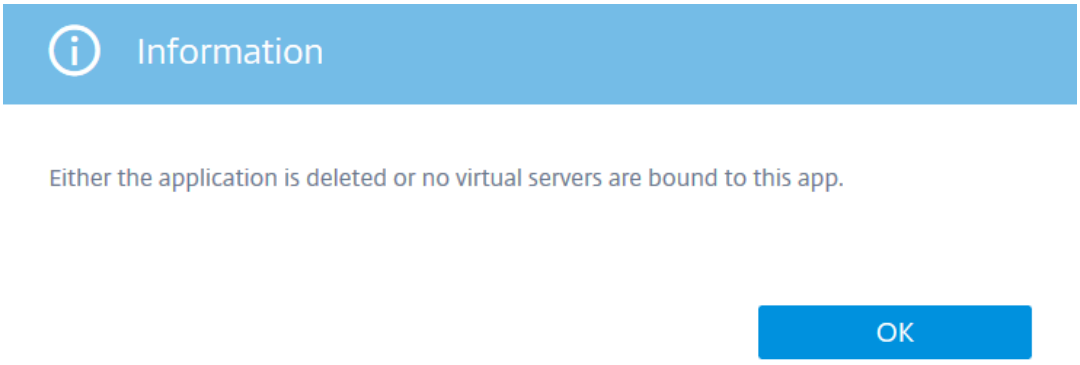
Mises à jour dans le nouveau comportement du tableau de bord par rapport au tableau de bord précédent

- Après avoir ajouté ou modifié une application personnalisée, il peut prendre quelques minutes pour refléter l'application dans le tableau de bord.
- Si vous supprimez une application personnalisée, le tableau de bord affiche toujours l'application supprimée, jusqu'à ce qu'ADM ait ses données analytiques (durée maximale d'un mois).

  Considérez un scénario selon lequel vous avez créé une application le 2 janvier 2020 et que vous l'avez supprimée le 4 janvier 2020. Dans ce scénario :

  - Le tableau de bord peut toujours afficher l'application supprimée le 4 janvier 2020, lorsque vous sélectionnez la durée des derniers 1 jour, 1 semaine et 1 mois.

- Le tableau de bord peut toujours afficher l'application supprimée le 5 janvier 2020, lorsque vous sélectionnez la durée des 1 dernières semaines et 1 mois.
- Lorsque la durée dépasse la date de suppression de l'application, l'application n'est pas affichée dans le tableau de bord. C'est-à-dire que le tableau de bord n'est pas affiché avec l'application supprimée le 6 janvier 2020 (pour le dernier jour), le 12 janvier 2020 (pour la dernière semaine), et après le 5 février 2020 (pour le dernier mois).
- Lorsque vous cliquez sur l'application supprimée dans le tableau de bord, le message suivant s'affiche.

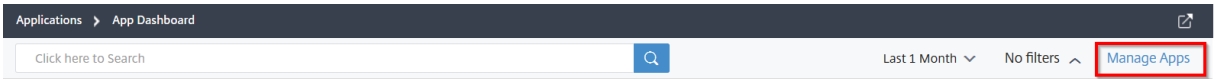


> **Remarque**
>
> Après avoir ajouté une application, si l'instance Citrix ADC associée est en panne, hors service ou inaccessible en raison d'un problème réseau temporaire :
>
> -Les applications associées à l'instance ADC ne sont visibles que dans la page **Applications**, mais pas dans le tableau de bord.
>
> -Les applications sont affichées dans le tableau de bord après l'exécution de l'instance ADC.

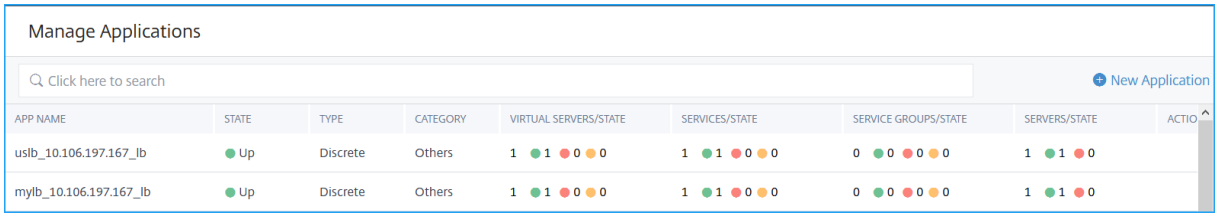
Mes Applications

April 29, 2021

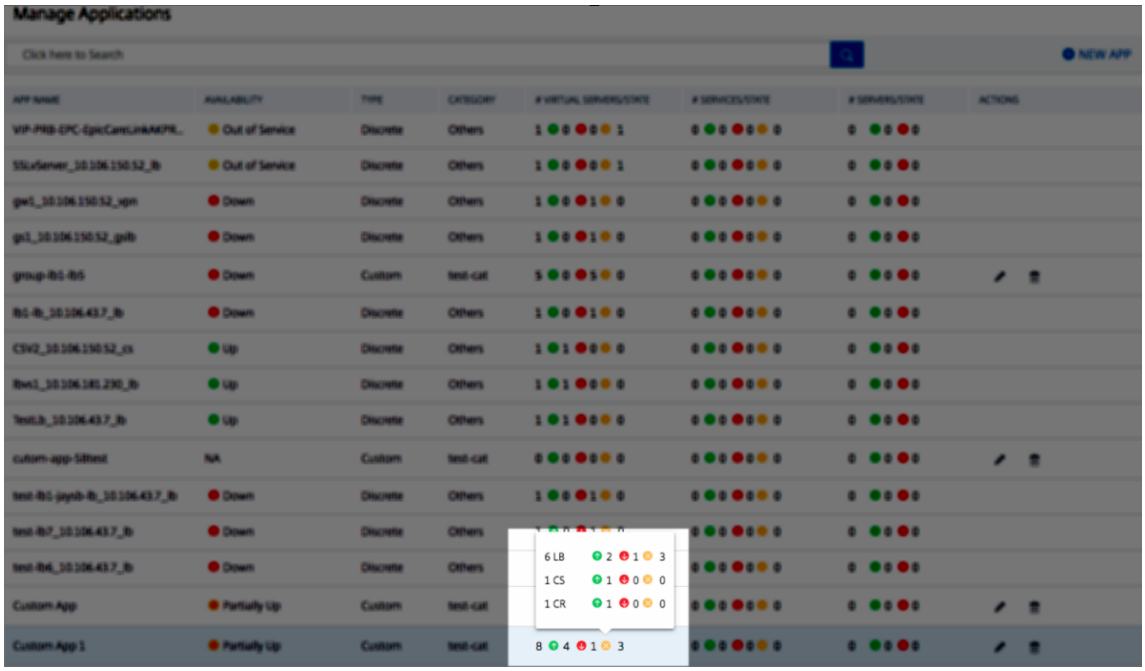
Dans le tableau de bord, cliquez sur **Gérer les applications** pour afficher les détails de l'application et ajouter, modifier ou supprimer des applications personnalisées.



Afficher les détails de l'application



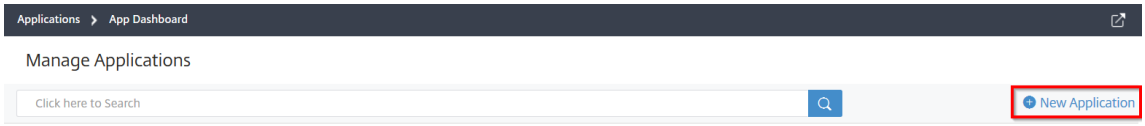
- **Nom de l'application** — Indique le nom de l'application
- **État— Indique l'état actuel de l'application, tel que Hors, **Absence**, **PartiellementHors, Absence de service**et**NA****
  - **Up** : tous les serveurs virtuels associés à l'application sont Up.
  - **Down** — Tous les serveurs virtuels associés à l'application sont en panne
  - **Partiellement en hausse** : l'un des virtuels associés à l'application est hors service ou hors service
  - **Out of Service** : tous les serveurs virtuels associés aux applications sont hors service
  - **NA** — Aucun serveur virtuel n'est configuré pour l'application
- **Type** — Indique si l'application appartient à Custom ou Discret
- **Catégorie** — Indique la catégorie d'application qui est groupée
- **Serveur virtuel/état** : indique le nombre total de serveurs virtuels configurés et l'état de tous les serveurs virtuels. Passez le pointeur de la souris pour afficher les détails tels que le nombre total de serveurs virtuels, le type de serveur virtuel et l'état du serveur virtuel



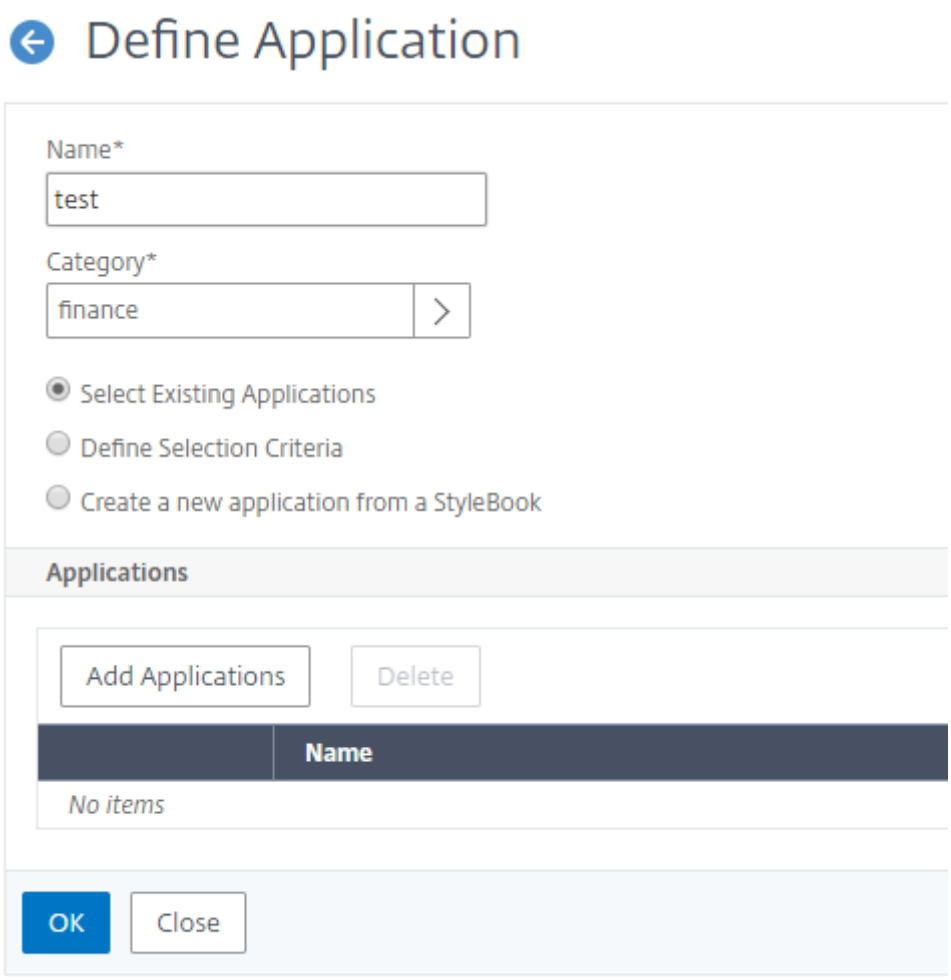
- **Services/état** — Indique le nombre total de services configurés et l'état de tous les services
- **Groupes de services/état** — Indique le nombre total de groupes de services configurés et l'état de tous les groupes de services
- **Servers/état** — Indique le nombre total de serveurs configurés pour l'application et l'état de tous les serveurs
- **Actions** : permet de modifier ou de supprimer les applications personnalisées

Ajouter une application

1. Cliquez sur **Nouvelle application** pour créer une application



   La page **Définir une application** s'affiche



> **Remarque**
>
> Vous pouvez également cliquer sur **Applications**, puis sélectionner **Nouvelle application** pour créer une application.

2. Définissez les paramètres suivants :

Champ	Description
Nom	Nom de l'application personnalisée. Par exemple, LB_TEST.
Catégorie	Catégorie dans laquelle vous pouvez regrouper les applications. Cliquez pour obtenir la page Catégorie d'application. Sélectionnez la catégorie et cliquez sur **Sélectionner**. Pour ajouter une catégorie :

Champ	Description
	1. Cliquez sur **Ajouter**
	2. Entrez le nom de votre choix.
	3. Cliquez sur **Créer**
Sélectionner des applications existantes	Permet de sélectionner les applications existantes ajoutées aux instances Citrix ADC.
Ajouter une application	Affiche tous les serveurs virtuels configurés sur les instances. Sélectionnez les applications dans la liste et cliquez sur **OK**.
Définir les critères de sélection	Option permettant de définir l'application par plage de serveurs virtuels ou par plage d'adresses IP du serveur/service d'origine.
	- **Serveur.** Spécifiez l'adresse IP du serveur ou du service, le nom du serveur ou le port du serveur principal sur lequel les applications s'exécutent. Vous pouvez entrer une adresse IP, une plage d'adresses IP ou une combinaison des deux, séparées par des virgules. Par exemple, vous pouvez entrer 10.102.29.20, 10.102.43.10-60, 10.216.43.45.
	- **Serveurs virtuels.** Vous pouvez spécifier l'une des options suivantes : l'adresse IP du serveur virtuel, le nom du serveur virtuel ou le port du serveur principal sur lequel les applications s'exécutent. Vous pouvez entrer une adresse IP ou une plage d'adresses IP ou une combinaison des deux, séparées par des virgules. Par exemple, vous pouvez entrer 10.102.29.20, 10.102.43.10-60, 10.216.43.45.
Créer une application à partir d'un StyleBook	Permet de créer une application à l'aide du StyleBook. Pour de plus amples informations, consultez la section Créer une application à l'aide du StyleBook.

a) Cliquez sur **OK**.

> **Remarque**
>
> Actuellement, Application Dashboard prend en charge uniquement l'équilibrage de charge et le changement de contenu des serveurs virtuels.

Le tableau de bord de l'application s'affiche désormais avec la catégorie et toutes les applications sont regroupées en dessous.

Lorsque vous créez une application à l'aide de StyleBooks, confirmez la consommation des licences requises pendant le déploiement de l'application.

Cliquez sur **Oui** pour le message de confirmation. ADM attribue les licences requises à une application.

Créer une application à l'aide du StyleBook

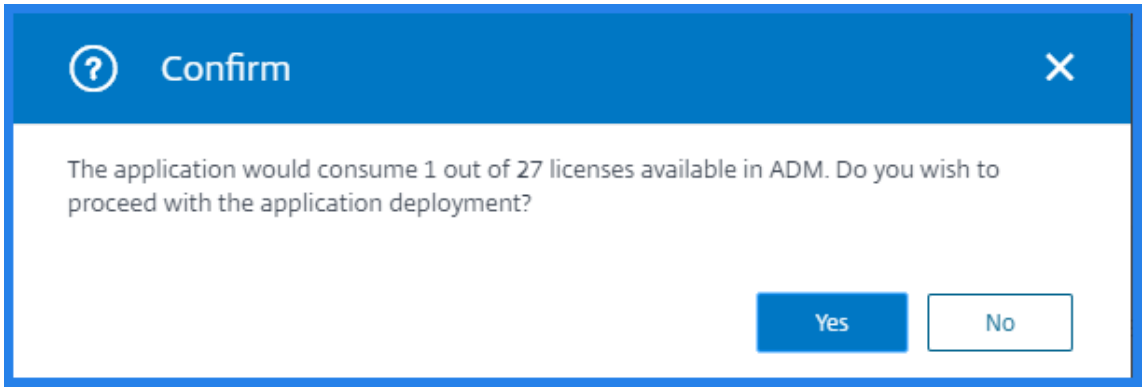
Pour créer une application à l'aide du StyleBook :

1. Dans Citrix ADM, accédez à **Applications** > **Tableau de bord** et cliquez sur **Définir une application personnalisée** pour créer une application personnalisée.
2. Dans la page **Définir une application**, tapez le nom de l'application dans le champ **Nom** .
3. Sélectionnez la catégorie d'application dans la section Catégorie. Citrix ADM vous permet de définir des catégories pour regrouper les applications définies par l'utilisateur. Vous pouvez également ajouter d'autres catégories si nécessaire.
4. Cliquez pour sélectionner **Créer une nouvelle application à partir d'un StyleBook**, puis cliquez sur **OK** .

   La page Choisir un styleBook s'affiche. Cette page contient tous les StyleBooks par défaut disponibles dans Citrix ADM.
5. Sélectionnez le StyleBook.
   La page **Détails de configuration** s'affiche.
6. Tapez les valeurs de tous les paramètres dans le StyleBook. Vous pouvez également cliquer sur View Definition pour afficher la construction du StyleBook avant de l'utiliser.

   Pour de plus amples informations, consultez la section Utiliser les styles par défaut.
7. Cliquez sur **Créer**.

   Un message de confirmation apparaît pour consommer les licences requises et déployer une application. Voici un exemple de message :

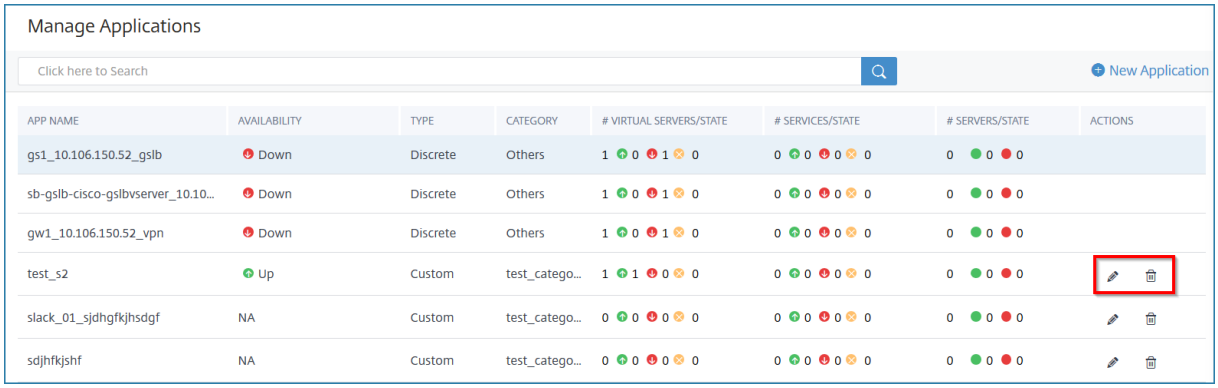


8. Cliquez sur **Yes**.

Vous pouvez également cliquer sur **Exécuter à sec** pour vérifier les configurations que Citrix ADM tente de créer sur l'instance Citrix ADC sélectionnée. Cette option est juste pour votre but de test pour voir la vérification finale des configurations. Même si l'option Dry Run réussit, la configuration réelle sur l'Citrix ADC sélectionné peut toujours échouer pour diverses raisons (conflit IP, instance inaccessible, etc.).

Modifier ou supprimer une application

À partir de la page **Applications**, vous pouvez modifier ou supprimer les applications personnalisées. Cliquez sur le bouton Modifier pour modifier une application et cliquez sur le bouton Supprimer pour supprimer l'application.



Exporter les rapports du tableau de bord de l'application et du tableau de bord de sécurité

Citrix ADM vous permet de prendre un instantané du tableau de bord de l'application en cours et de les exporter en tant que rapports. À intervalles fréquents, les administrateurs de l'application peuvent avoir besoin d'utiliser ces rapports pour mettre à jour les pénalités d'utilisation de l'application et de performances.

Avec cette fonctionnalité, les administrateurs peuvent extraire ces données sous forme de rapports .png, .jpeg ou .pdf.

> **Remarque**
>
> Contrairement aux autres options d'exportation de rapport dans Citrix ADM, vous pouvez exporter les rapports Tableau de bord des applications et Tableau de bord de sécurité uniquement sous forme de fichiers .pdf ou .png. Le format .csv n'est pas pris en charge actuellement.

Le rapport est téléchargé sur votre système. À partir des pages Tableau de bord des applications et Tableau de bord de la sécurité des applications, vous pouvez également accéder aux pages de deuxième niveau et les exporter en tant que rapports. Actuellement, vous pouvez télécharger les rapports d'une seule application à la fois.

Automatisation de la gestion des certificats SSL

April 29, 2021

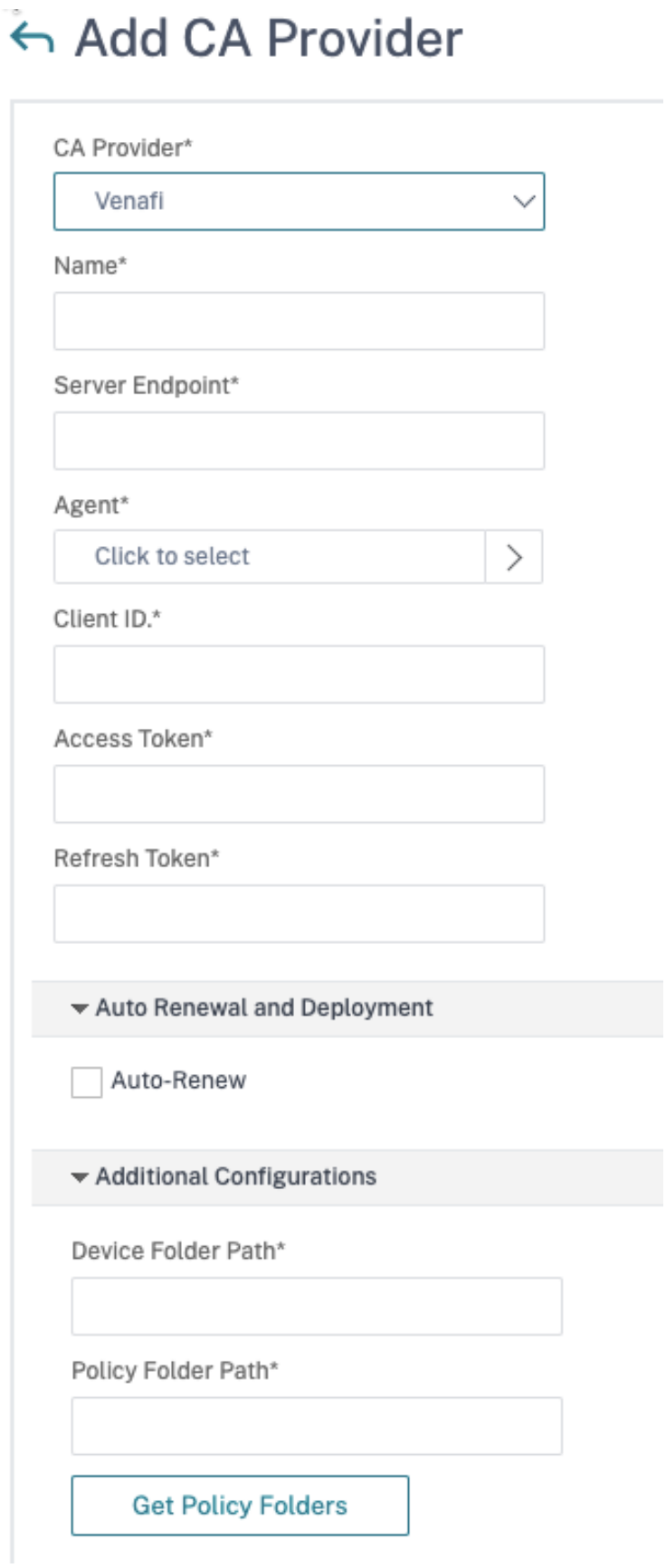
Pour maintenir la sécurité numérique, vous devez automatiser la gestion des certificats SSL dans votre environnement. Vous avez besoin de moyens de gérer et de surveiller de manière proactive tous les certificats, de vous avertir de la date d'expiration des certificats et de renouveler automatiquement les certificats avant leur expiration. Les certificats SSL expirés entraînent des risques de sécurité. Vous pouvez configurer les serveurs Venafi Trust Protection Platform avec ADM pour automatiser la gestion des certificats SSL installés sur les instances ADC.

En utilisant Venafi avec ADM, vous pouvez gérer les certificats SSL tout au long de leur cycle de vie. Vous pouvez effectuer les tâches suivantes dans le tableau de bord **Application** ADM :

- Vérifiez les problèmes SSL et les scores des applications.
- Résoudre les problèmes SSL et appliquer la correction suggérée.
- Vérifiez les certificats liés à une application.
- Créez, installez et renouvelez rapidement des certificats.
- Automatisez le renouvellement des certificats.
- Sécurisez les applications en liant les certificats générés aux serveurs virtuels ADC.
- Vérifiez tous les journaux liés à la tâche SSL sur une application particulière.

Configurer un serveur Venafi sur ADM

La configuration d'un serveur Venafi est un processus en deux étapes. Tout d'abord, vous ajoutez le serveur Venafi sur ADM. Ensuite, vous configurez les stratégies sur le serveur Venafi. Pour ajouter le serveur Venafi sur ADM, à partir de l'interface graphique ADM, naviguez **Réseau > Dashboard SSL > Autorité de certification tierce**. Cliquez sur **Add**.

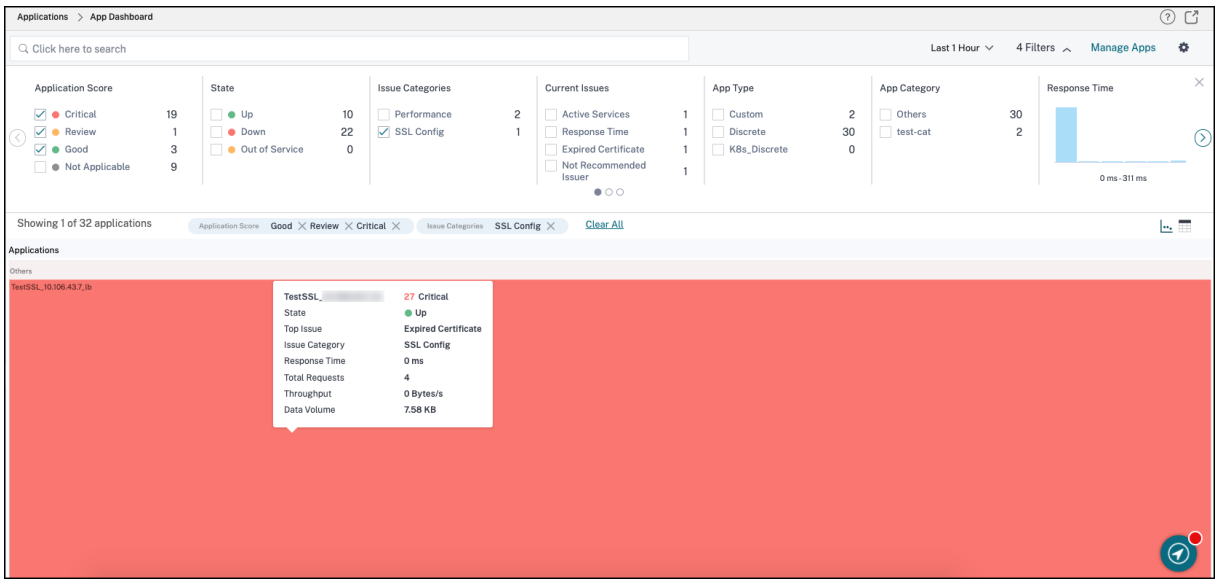


Entrez les détails dans les champs fournis. Cochez l'option **Renouvellement automatique** si vous souhaitez que les certificats soient renouvelés automatiquement. Pour plus de détails sur chaque champ, passez la souris sur le champ et cliquez sur l' `i` icône.

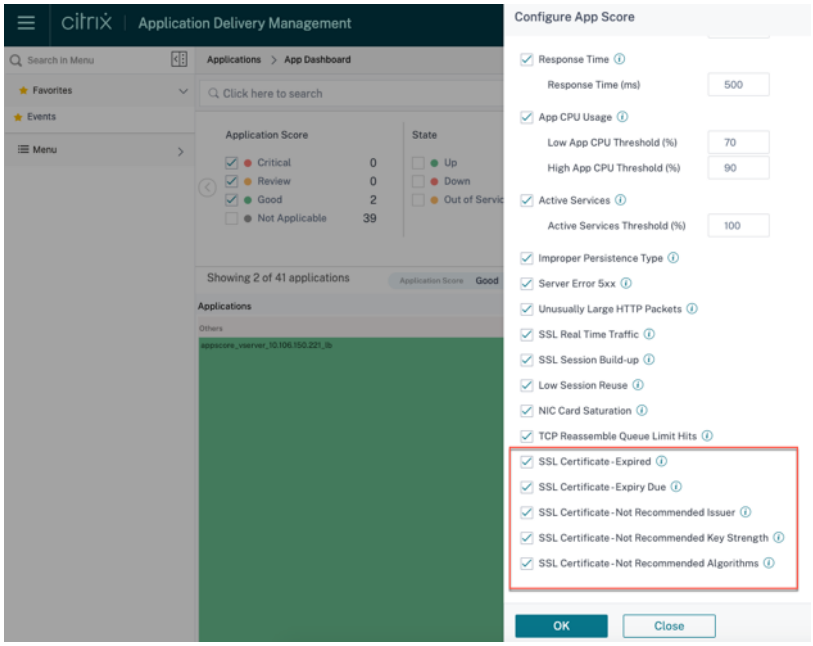
Après avoir configuré le serveur Venafi, vous pouvez utiliser le tableau de bord ADM pour gérer vos certificats SSL.

Gérer le cycle de vie des certificats SSL

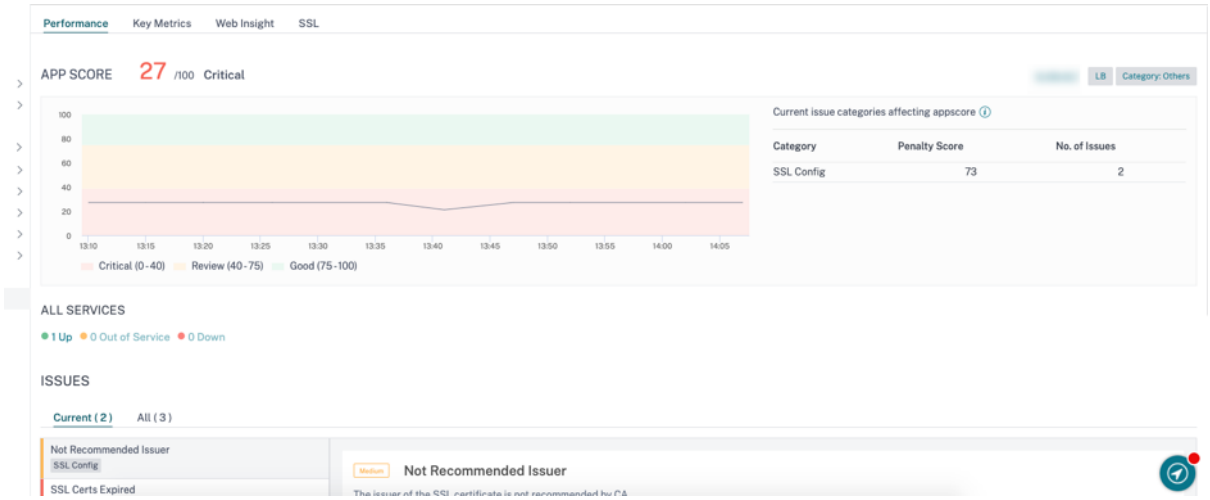
Le tableau de bord de l'application est un guichet unique pour gérer vos certificats SSL de bout en bout. Dans l'interface graphique ADM, accédez à **Applications > Tableau de bord des applications**. Sous **Catégories de problème**, sélectionnez **SSL Config**. Sous **Problèmes actuels**, vous pouvez voir les problèmes liés à SSL de vos applications. Pour afficher le rapport SSL, sous **Applications**, passez la souris sur l'application. Pour afficher les détails du rapport, cliquez sur l'application. Dans cet exemple, nous avons une application avec un score de 27.



En outre, vous pouvez filtrer vos problèmes à l'aide **des scores d'application** tels que critiques ou critiques. Les scores de l'application SSL sont basés sur les paramètres SSL, qui sont activés par défaut sous Paramètres **Gérer les applications** dans le coin supérieur droit du tableau de bord.

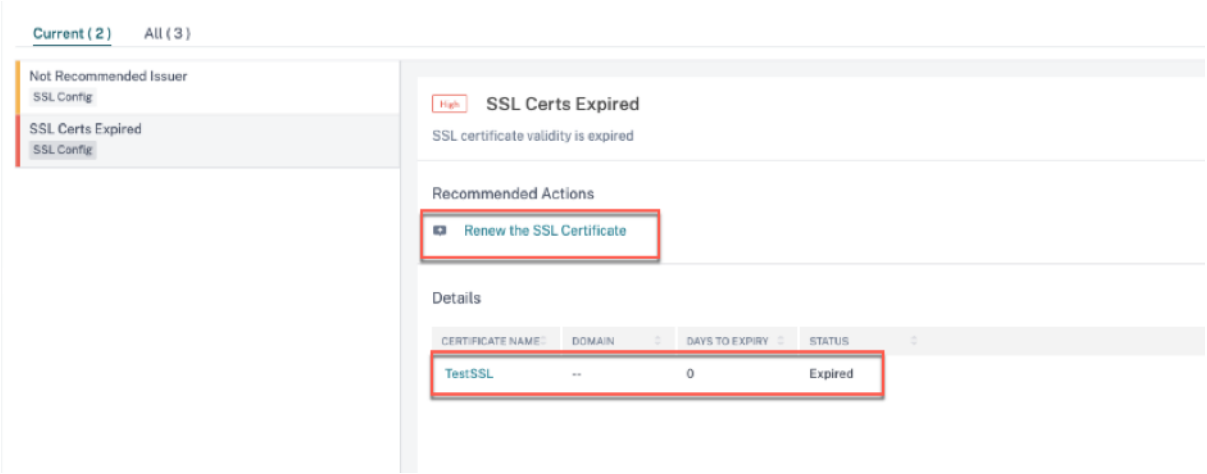


Pour désactiver l'un des paramètres SSL, désactivez la case et cliquez sur **OK**. Pour afficher les détails du rapport SSL, sous **Applications**, cliquez sur l'application pour laquelle vous souhaitez voir le rapport.



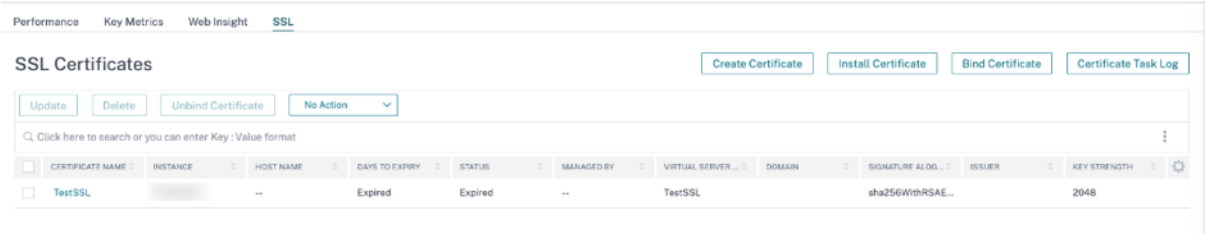
Vous pouvez vérifier le score de performances et faire défiler la page vers le bas pour afficher des détails tels que les serveurs virtuels de l'application et les certificats liés aux serveurs virtuels et les problèmes avec les certificats. Pour afficher les détails du certificat, cliquez sur le lien sous **Nom du certificat**. Pour un certificat expiré, pouvez-vous le renouveler.

Le renouvellement du certificat implique de créer le certificat, de l'installer et de le lier au serveur virtuel.

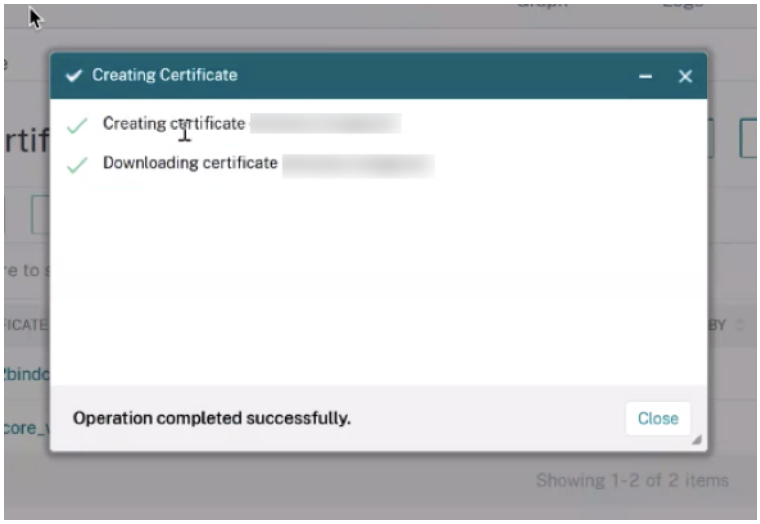


> **Remarque**
>
> Lorsque vous ajoutez un serveur Venafi sur ADM, si vous activez l'option de renouvellement automatique, les certificats sont automatiquement renouvelés avant l'expiration.

Cliquez sur **Renouveler le certificat SSL** pour accéder à l'onglet SSL, qui répertorie tous les certificats liés aux serveurs virtuels de l'application. Cet onglet vous permet de créer et d'installer des certificats et de les lier aux serveurs virtuels. En outre, vous pouvez vérifier tous les journaux liés à la tâche SSL sur une application particulière sur les journaux liés à la tâche SSL d'une application particulière.

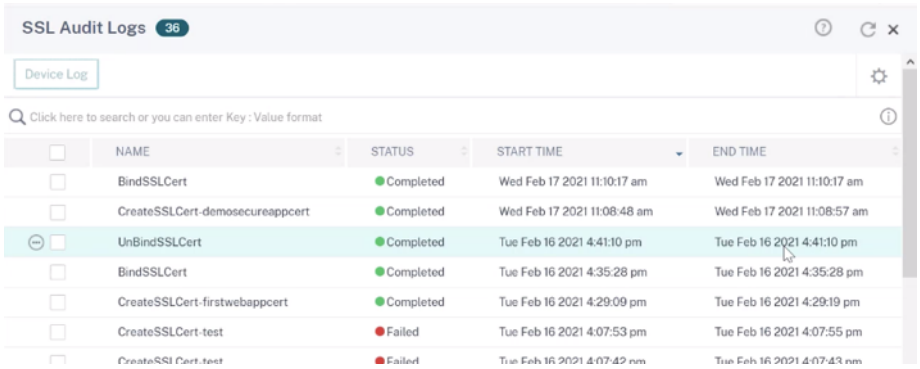


Pour créer un certificat, cliquez sur **Créer un certificat** et entrez les détails. Fournissez un mot de passe lorsque les certificats téléchargés sont chiffrés et cliquez sur **Créer**. ADM contacte le serveur Venafi pour créer le certificat. Cliquez sur **Fermer** lorsque le certificat est téléchargé.



Ensuite, sous l'onglet SSL, cliquez sur **Installer le certificat**. Sélectionnez le certificat téléchargé et cliquez sur **Installer**. Pour plus d'informations sur l'installation d'une certification SSL sur ADC, à l'aide d'ADM, consultez la section sur l'installation d'un certificat SSL à partir de Citrix ADM dans la rubrique Installer des certificats SSL sur une instance Citrix ADC.

Ensuite, cliquez sur **Lier le certificat**. Vous pouvez également délier un certificat si nécessaire. Après la prochaine interrogation SSL, le tableau de bord Application est actualisé avec les nouvelles données. Si vous souhaitez vérifier tous les journaux des tâches SSL d'une application particulière, cliquez sur **Journal des tâches de certificat**.

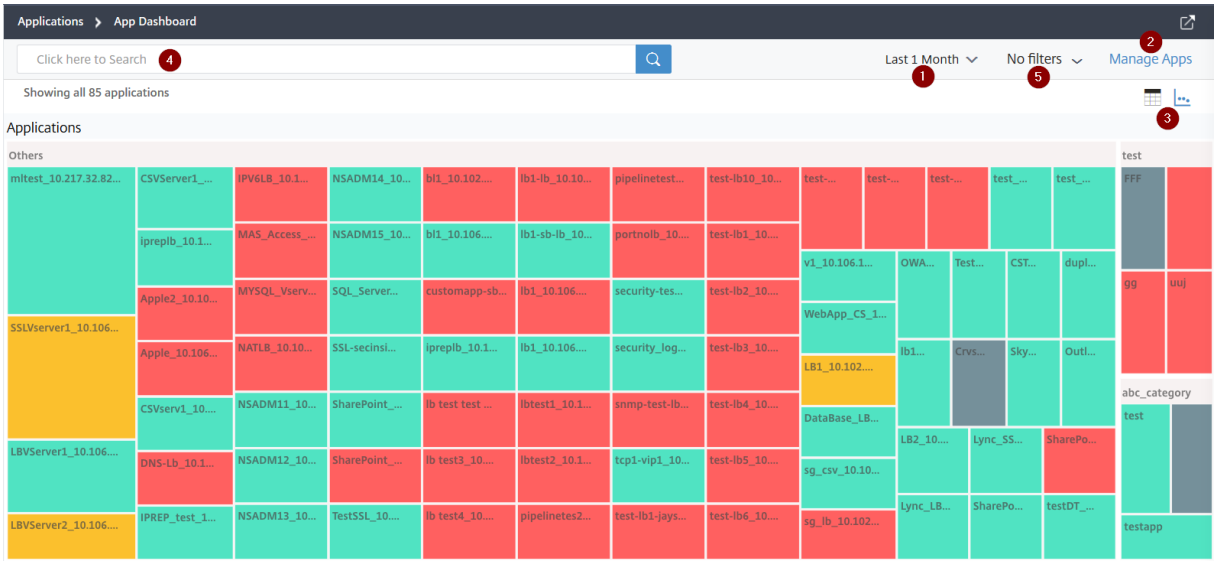


Vue d'ensemble du tableau de bord des applications

April 29, 2021

Le tableau de bord de l'application affiche les applications discrètes sous **Autres** et les applications personnalisées regroupées sous leurs catégories respectives.

Accédez à **Application** > **Tableau de bord** pour afficher le tableau de bord de l'application.



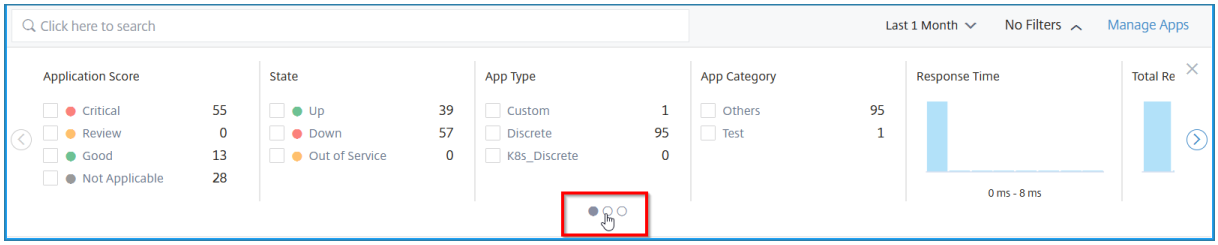
1 — Affiche les détails de l'application pour la durée sélectionnée, par exemple 1 heure, 1 jour, 1 semaine et 1 mois.

2 — Permet de gérer des applications et d'ajouter de nouvelles applications

3 — Permet d'afficher des applications en mode tableau ou en mode graphique

4 — Permet de rechercher une application à l'aide de la barre de recherche

5 — Permet d'appliquer des filtres pour afficher des applications. Cliquez pour afficher les détails.

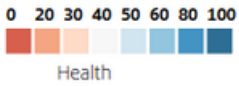


Vous pouvez sélectionner le curseur de carrousel qui vous permet d'accéder facilement à toutes les options.

Vous pouvez :

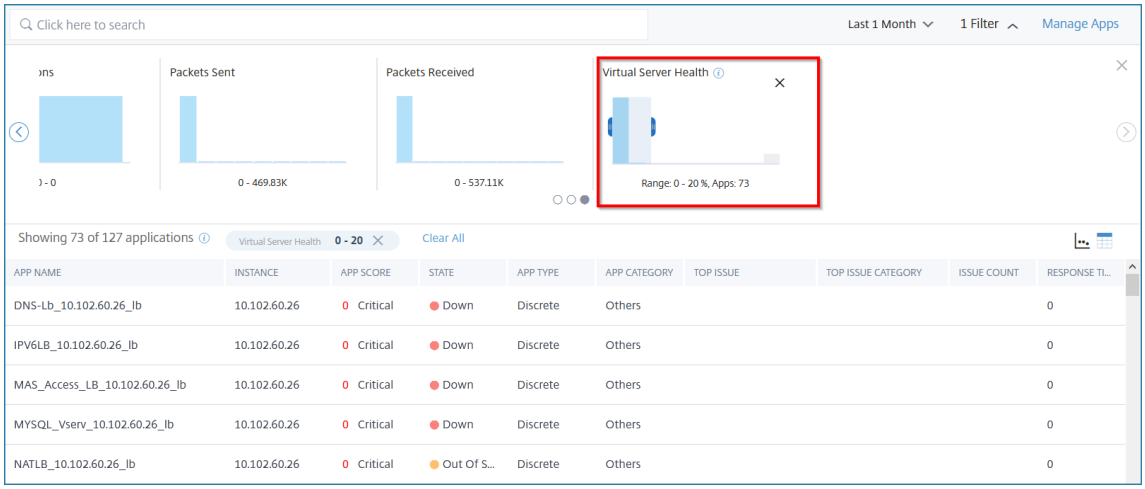
- Sélectionnez cette option pour afficher les applications en fonction des scores.
  - **Critique** : le score d'application est compris entre 0 et < 40
  - **Fair** — La note de candidature est comprise entre 40 et < 75
  - **Bon** — Le score d'application est supérieur à 75
  - **Non applicable** : aucun serveur virtuel n'est configuré pour l'application

    Le tableau suivant décrit les différences entre le score d'application précédent et le score d'application actuel.

Score de l'application (Critique, Examen, Bon, Sans objet)	Score d'application (vue antérieure avec légendes de couleur)
Le score est calculé comme **100 moins le score de pénalité de tous les problèmes actuels de l'application**	Le score est calculé comme **100 — (ressource serveur d'applications + ressource système Citrix ADC)**
Les applications sont affichées dans des couleurs telles que le **rouge (critique)**, l'**orange (critique)**, le **vert (bon)**et le **gris (sans objet)**	Les applications sont affichées dans des légendes de couleur. 

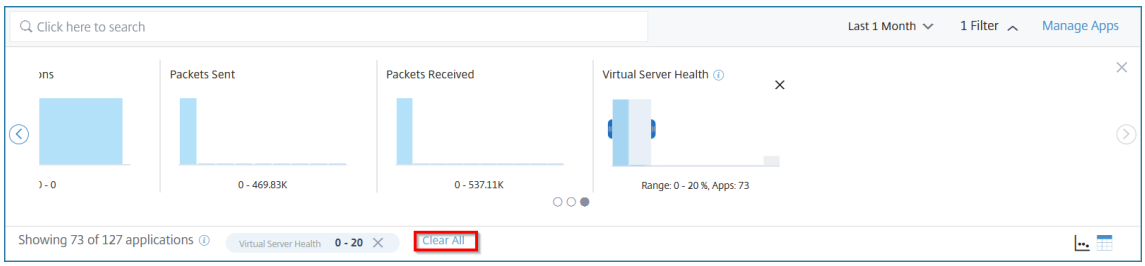
- Sélectionnez cette option pour afficher les applications en fonction de l'état de l'application, comme le haut, le bas et le hors service.
- Sélectionnez cette option pour afficher les applications en fonction du type d'application tel que Discret ou Personnalisé
- Sélectionnez pour afficher les applications en fonction des catégories regroupées sous
- Faites glisser l'histogramme pour appliquer des filtres et afficher les applications.

  Par exemple, si vous souhaitez afficher les applications dont l'intégrité du serveur virtuel est comprise entre 0 et 20, faites glisser l'histogramme d'intégrité du serveur virtuel pour filtrer les résultats.



> **Remarque**
>
> Vous pouvez également cliquer sur l'histogramme pour afficher les applications pertinentes.

Cliquez sur **Effacer tout** pour effacer le filtre appliqué.



Voici le résumé de l'application pour lequel vous pouvez appliquer des filtres :

- **Score d'application** : vous permet d'afficher les applications en fonction des critères **Critique**, **Review**, **Bon**et **Non applicable**.

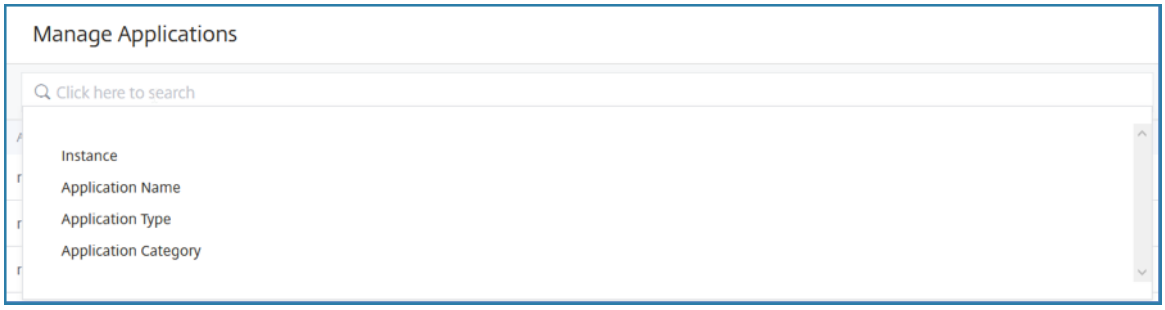
  > Remarque
  >
  > Par défaut, vous pouvez afficher les applications ayant le statut Critique, Révision et Bon. Pour afficher les applications dont le statut est N/A, vous devez sélectionner l'option **Non applicable**.

- **État** : permet d'afficher l'application en fonction de l'état de l'application, tel que **Désactiver**, et **Désactiver le service**.
- **Problèmes actuels** : permet d'obtenir une liste d'applications affectées par un problème spécifique, en choisissant le type de problème tel que **Performances**, **Instance Health**, **Config**et **System Resources**.
- **Type d'application** : permet d'afficher les applications en fonction du type d'application tel que les **services**personnalisés**,**discrets**et Kubernetes**.
- **Catégorie d'application** : permet d'afficher les applications en fonction de la catégorie affectée.
- **Temps de réponse** : histogramme qui affiche le temps de réponse moyen reçu par les applications.
- **Total des demandes** : histogramme qui affiche le nombre total de demandes reçues par les demandes.
- **Débit** : histogramme qui affiche le débit total du réseau traité par les applications.
- **Volume de données** : histogramme qui affiche le total des données traitées par les applications. Le volume de données est calculé par le nombre total d'octets de requête et d'octets de réponse pour les applications.
- **Connexions client** : histogramme qui affiche les connexions client moyennes établies par les applications.
- **Connexions serveur** : histogramme qui affiche les connexions serveur moyennes établies par les applications.

- **Paquets envoyés** : histogramme qui affiche le nombre total de paquets envoyés par les applications.
- **Paquets reçus** : histogramme qui affiche le nombre total de paquets reçus par les applications.
- **Santé du serveur virtuel** : histogramme qui affiche le total des applications entre la plage de score de 0 à 100 %. L'intégrité d'un serveur virtuel est (%) des services actifs associés à l'application. Par exemple, si un serveur virtuel est configuré avec 2 services et si l'un d'eux est en panne, le score est de 50 %.

Recherche et filtrage des résultats à l'aide de la barre de recherche

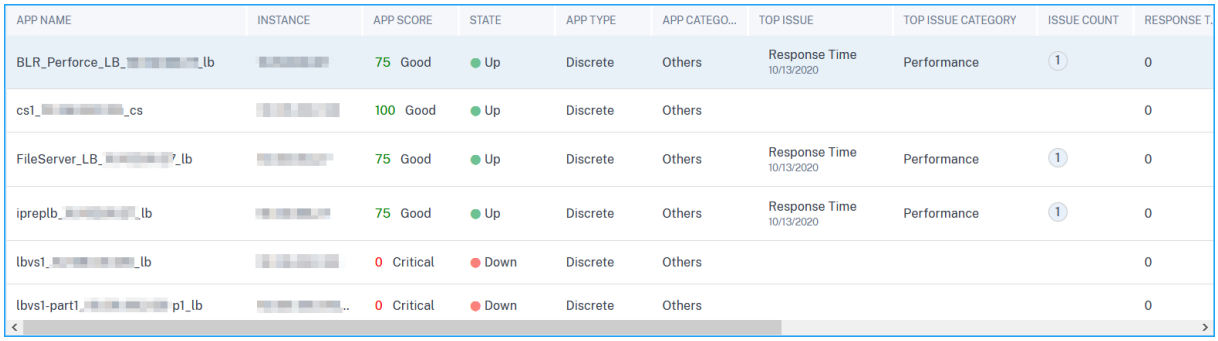
Vous pouvez placer le pointeur de la souris sur la barre de recherche et sélectionner la catégorie pour affiner la recherche.



Afficher les applications

April 29, 2021

Par défaut, le tableau de bord de l'application affiche toutes les applications. Selon vos besoins, vous pouvez utiliser l'option de filtre pour afficher les applications.



Le tableau de bord affiche les détails suivants de l'application :

- **Nom de l'application** — Indique le nom de l'application.

- **Instance** — Indique l'instance Citrix ADC.
- **Score de l'application** — Indique le score de l'application et le statut tel que **Critique**, **Bon**, **Fair**et **Non applicable**.
- **État— Indique la disponibilité actuelle de l'application, telle que Hors, **Descendez**, **PartiellementHors, Absence de service**et**NA**.**
  - **Up** : tous les serveurs virtuels associés à l'application sont Up.
  - **Down** : tous les serveurs virtuels associés à l'application sont Down.
  - **Partiellement en hausse** : l'un des virtuels associés à l'application est hors service ou hors service.
  - **Out of Service** : tous les serveurs virtuels associés aux applications sont hors service.
  - **NA** : aucun serveur virtuel n'est configuré pour l'application.
- **Type d'application** : indique le type d'application, tel que les **services**personnalisés**,**discrets**ou Kubernetes**.
- **Catégorie d'application** — Indique la catégorie qui est affectée à l'application.
- **Problème le plus** important : indique le problème qui a le nombre d'erreurs maximum sur l'application.
- **Catégorie d'émission la plus importante** — Indique la catégorie du problème.
- **Nombre de problèmes** — Indique le nombre total de problèmes pour l'application.
- **Temps de réponse** : indique le temps de réponse moyen pour répondre à partir de l'application.
- **Total des demandes** — Indique le nombre total de demandes reçues par la demande.
- **Débit** : indique le débit réseau total de l'application. Le débit est calculé par les octets Req/Sec + Res octets/Sec pour les serveurs virtuels.
- **Volume de données** — Indique le total des données traitées par l'application.
- **Connexions client** : indique les connexions client moyennes établies par l'application.
- **Connexions au serveur** : indique les connexions serveur moyennes établies par l'application.

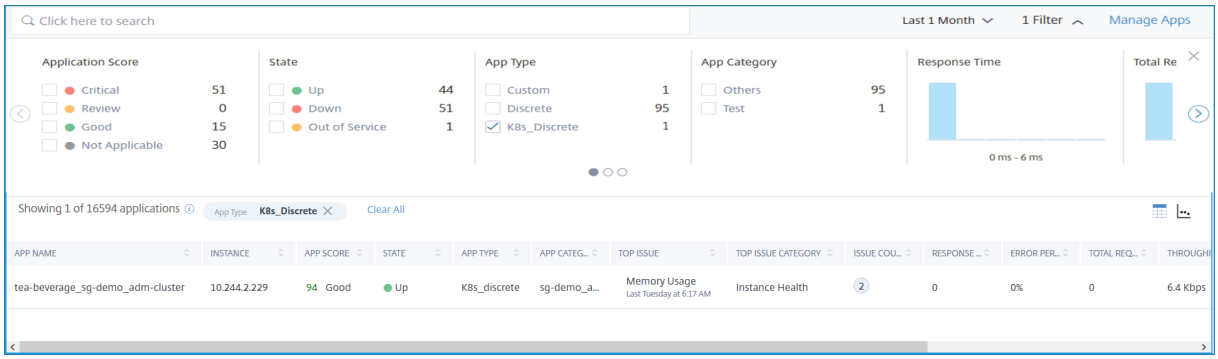
Afficher les applications de microservices

Pour afficher les applications de microservices, sélectionnez l'option **K8S_discrete** sous Filtre **Type d'application**.

Vous pouvez afficher les applications de microservice dans **App Dashboard** sous la forme de nom suivante :

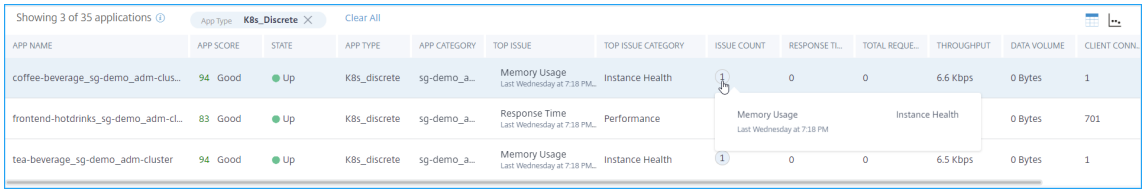
`<k8s service>_<k8s namespace>_<k8s cluster_name>`

Par exemple, `tea-beverage_sg-demo_adm-cluster` fait référence à un service nommé « tea-beverage » avec l'espace de noms de `sg-demo` dans le cluster `adm-cluster`.



Les mesures suivantes sont affichées dans le tableau de bord pour la durée sélectionnée :

- **Nom de l'application** — Indique le nom de l'application.
- **Instance** — Indique l'adresse IP de l'instance Citrix ADC CPX.
- **Score de l'application** — Indique le score de l'application.
  - **Critique** — Le score de l'application est compris entre 0 et < 40
  - **Évaluations** — Le score de l'application est compris entre 40 et < 75
  - **Bon** — Le score de l'application est supérieur à 75
- **État** : indique l'état actuel de la demande.
- **Catégorie d'application** — Indique le nom du cluster où l'application est hébergée.
- **Problème le plus** élevé — Indique les principaux problèmes qui affectent le score d'application actuel.
- **Catégorie d'émission la plus importante** — Indique la catégorie de problème affectant l'application.
- **Nombre de problèmes** — Indique le nombre total de problèmes affectant la demande. Placez le pointeur de la souris sur le nombre de problèmes pour afficher la vue d'ensemble des problèmes.



- **Délai de réponse** — Indique le temps de réponse moyen reçu par la demande.
- **Pourcentage d'erreur** : indique le pourcentage moyen d'erreurs 5xx pour l'application.

- **Total des demandes** — Indique le nombre total de demandes reçues par la demande.
- **Débit** : indique le débit total du réseau traité par l'application.
- **Volume de données** — Indique le total des données traitées par l'application. Le volume de données est calculé comme le total des octets de requête et des octets de réponse pour l'application.
- **Connexions client** : indique les connexions client moyennes établies par l'application. Cela peut également faire référence aux services sortants associés connectés au service sélectionné.
- **Connexions au serveur** : indique les connexions serveur moyennes établies par l'application. Cela peut également faire référence aux services entrants associés connectés au service sélectionné.

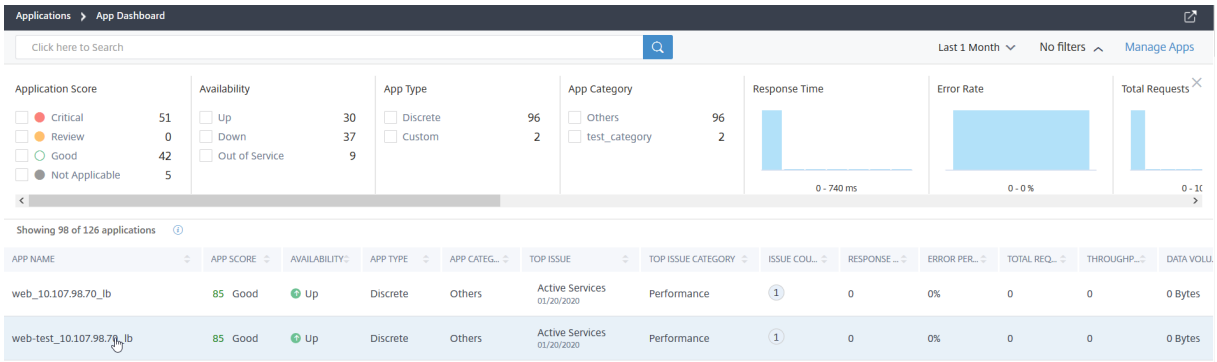
Cliquez sur l'option **+** pour ajouter ou supprimer les options à afficher dans le tableau de bord.

Cliquez sur une application pour afficher les détails de l'application. Pour plus d'informations, Détails de l'application Microservices

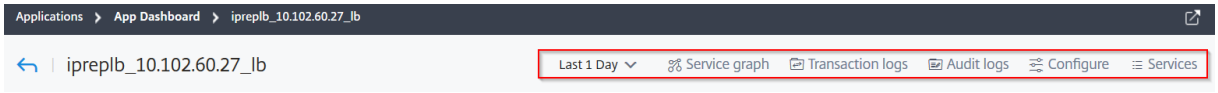
Détails de l'application

April 29, 2021

Cliquez sur une application dans le tableau de bord pour obtenir plus d'informations détaillées.



La page de l'application sélectionnée s'affiche.



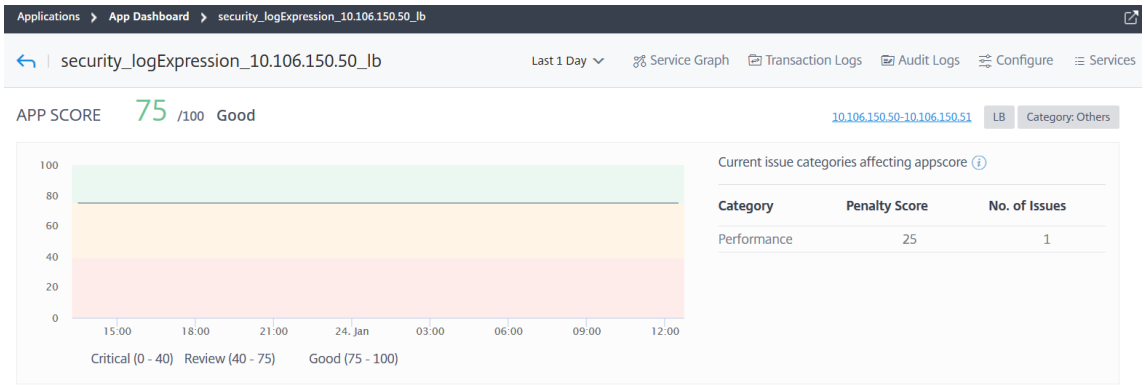
À partir de la page de détails de l'application :

- Sélectionnez la durée de temps dans la liste pour afficher les détails de la durée spécifique

- Cliquez sur **Graphique de service** pour afficher le graphique de service de l'application sélectionnée. Pour de plus amples informations, consultez Graphique de service pour les applications
- Cliquez **Journaux transactions** pour afficher les transactions détaillées de l'application sélectionnée
- Cliquez sur **Journaux d'audit** pour afficher les informations détaillées du journal d'audit
- Cliquez sur **Configurer** pour afficher ou modifier la configuration du service et du groupe de services pour l'application sélectionnée
- Cliquez sur **Service** pour afficher les services liés à l'application

Après avoir sélectionné la durée, les détails de l'application suivants s'affichent :

- **Score** de l'application — Score de l'application pour la durée sélectionnée. Le score final est calculé comme **100 moins la pénalité totale**.

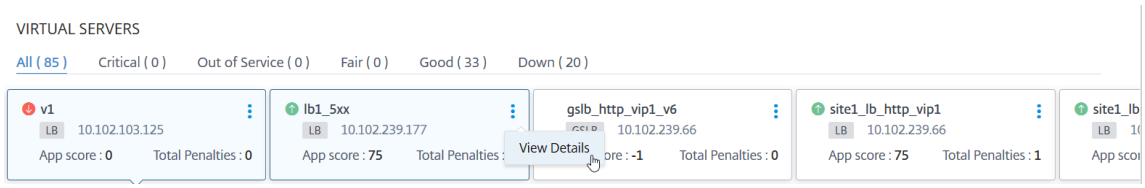


  Ce tableau de bord vous permet également d'afficher les problèmes actuels qui affectent le score de l'application. Vous pouvez afficher les détails des problèmes sous Problèmes.

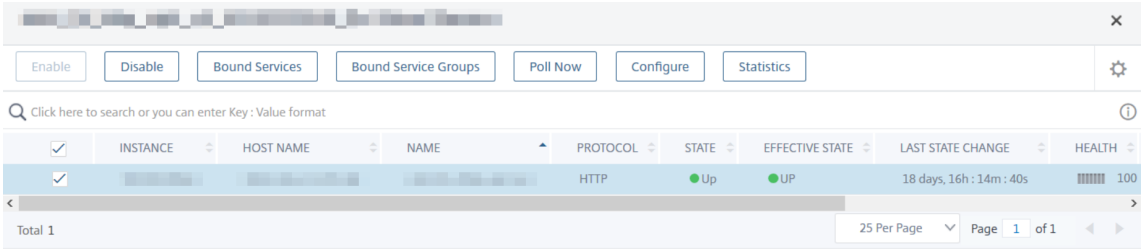
- **Serveurs virtuels** —

  > **Remarque**
  >
  > La section **Serveurs virtuels** s'affiche uniquement pour les applications personnalisées. Pour les applications discrètes, cliquez sur l'**adresse IP** pour afficher les détails du serveur virtuel.

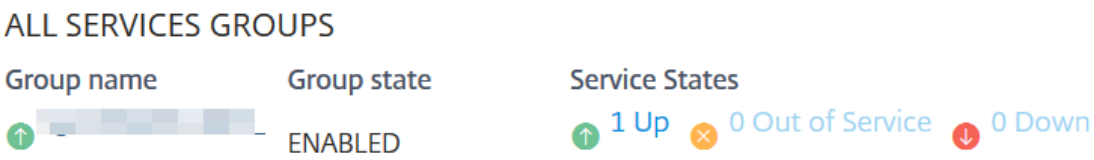
  Affiche tous les serveurs virtuels associés à l'application personnalisée



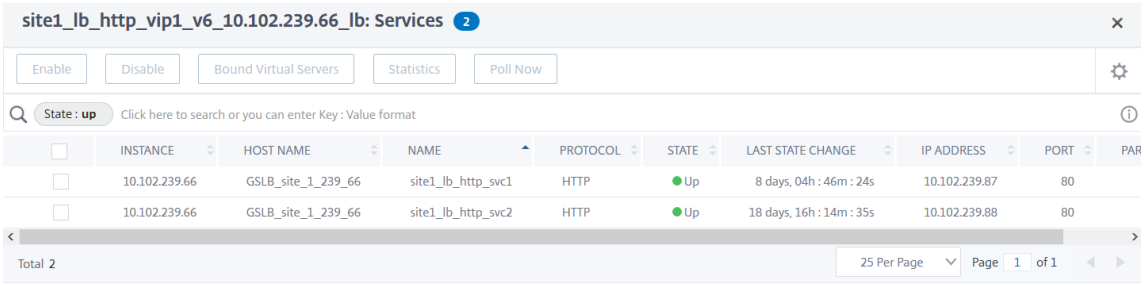
Cliquez sur **Afficher les détails** pour afficher et gérer les paramètres du serveur virtuel.



- **Tous les services** — Les services liés à l'application



Cliquez pour afficher les détails du service et pour gérer les paramètres du service



- **Problèmes** — Problèmes applicables à la demande sélectionnée. Vous pouvez afficher les problèmes suivants avec sa catégorie :

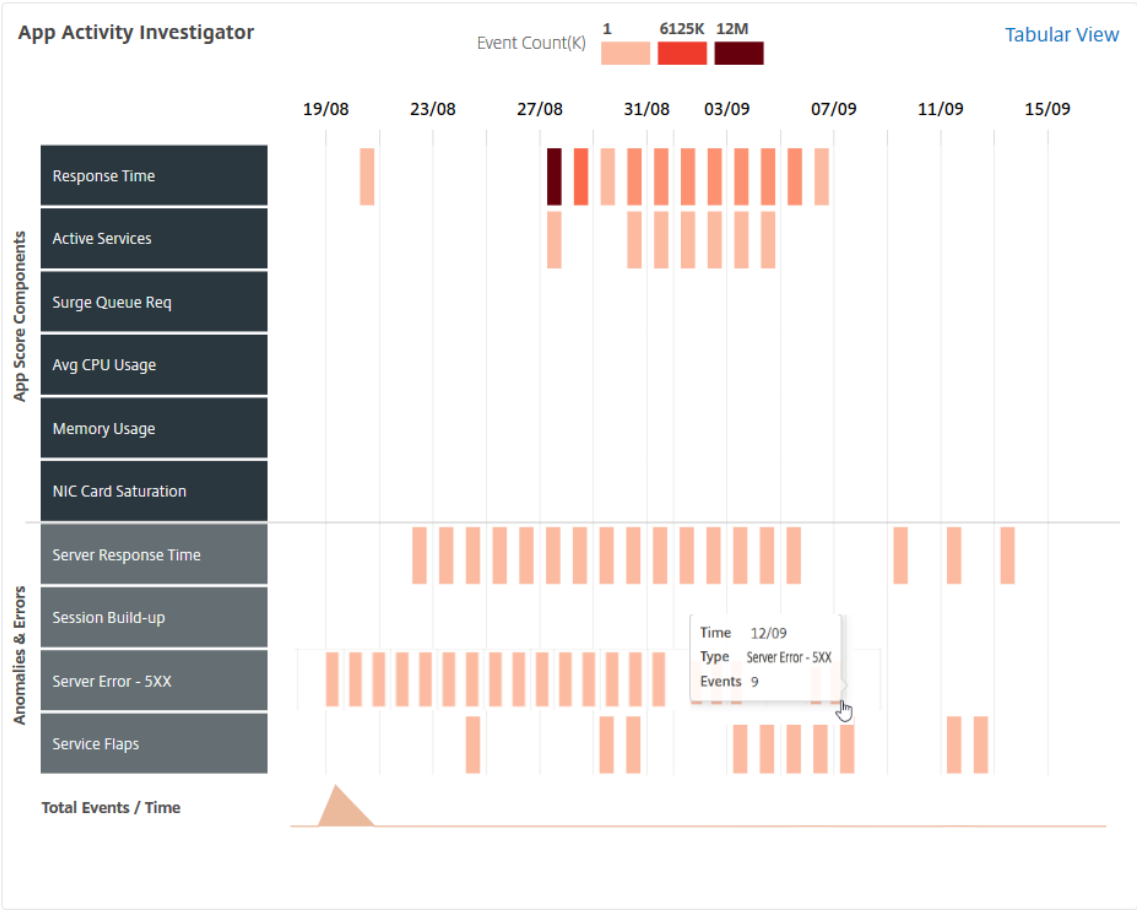
Performances	Santé de l'instance	Config	Ressources système
Temps de réponse	Utilisation moyenne de l'UC	Serveur instable	Type de persistance incorrect
Services actifs	Utilisation de mémoire	Paquets HTTP exceptionnellement volumineux	Saturation de la carte réseau
Réutilisation de session faible		TCP réassembler les hits de limite de file d'attente	
Utilisation du processeur de l'application			

Performances	Santé de l'instance	Config	Ressources système
Accumulation dans la file d'attente de surtension			
Trafic en temps réel SSL			
Accumulation de sessions			
Temps de réponse du serveur			
Volets de service			

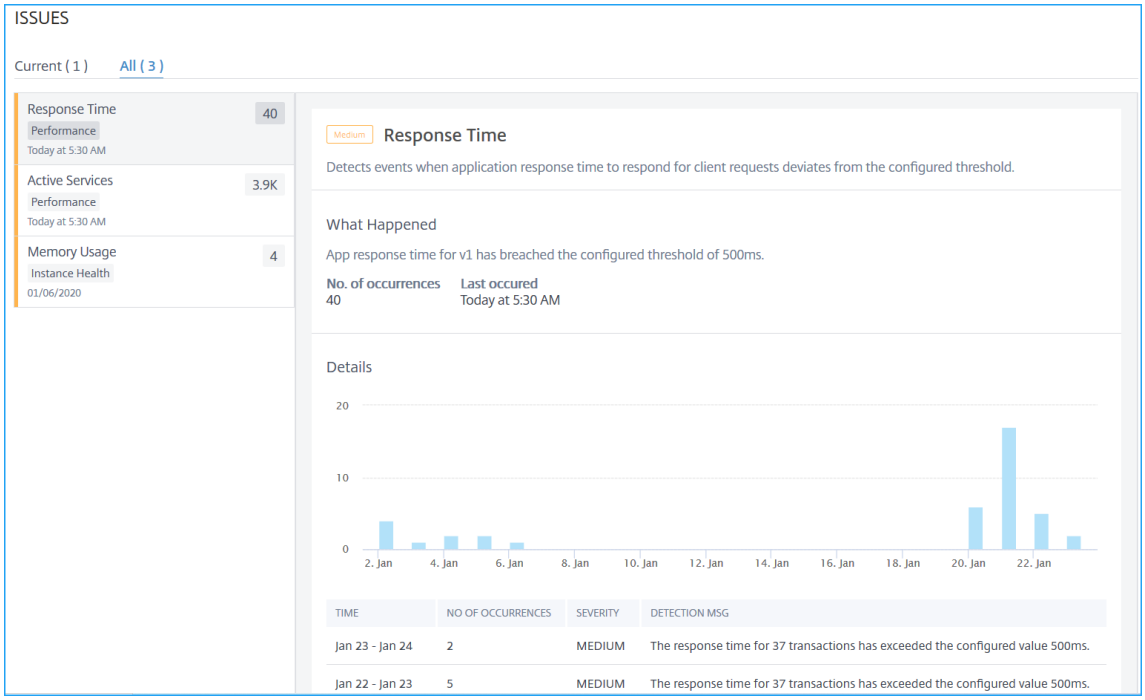
Cliquez sur chaque problème pour vérifier les détails tels que le message de détection, la date à laquelle le problème s'est produit, les actions recommandées et les détails.

Pour de plus amples informations, consultez la section Indicateurs de performance pour l'analyse des applications.

L'image suivante est la vue antérieure de la page de l' **explorateur d'activité de l'application** :

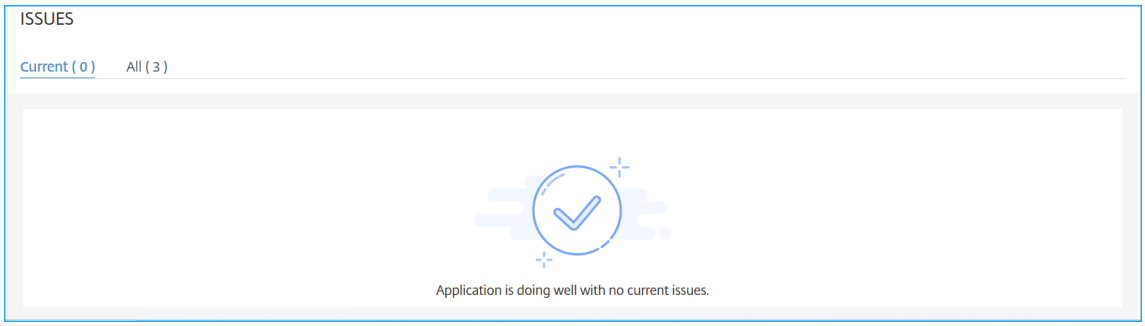


Vous pouvez désormais afficher tous les problèmes dans la section **Problèmes**, ainsi que la catégorie que vous avez pu afficher dans la page **Investigateur d'activité des applications**.

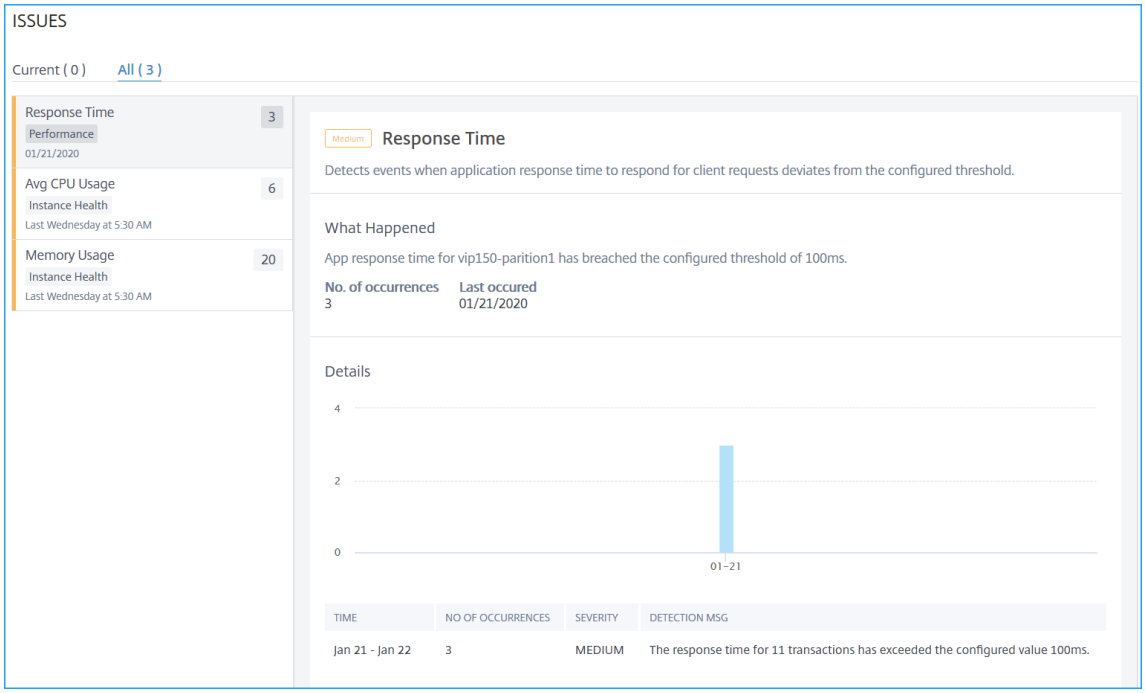


- Les problèmes qui s'affichent dans l'onglet **Courant** font référence aux problèmes d'application pour la durée de sélection.
- Les problèmes qui s'affichent dans l'onglet **Tous** font référence au nombre total de problèmes d'application.

L'exemple suivant est les problèmes d'application pour une durée d'un jour. L'onglet **Courant** indique aucun problème actuel n'affectant le score de l'application.



L'onglet **Tous** affiche le nombre total de problèmes détectés pour la durée d'un jour.



Analyse de l'utilisation optimale

April 29, 2021

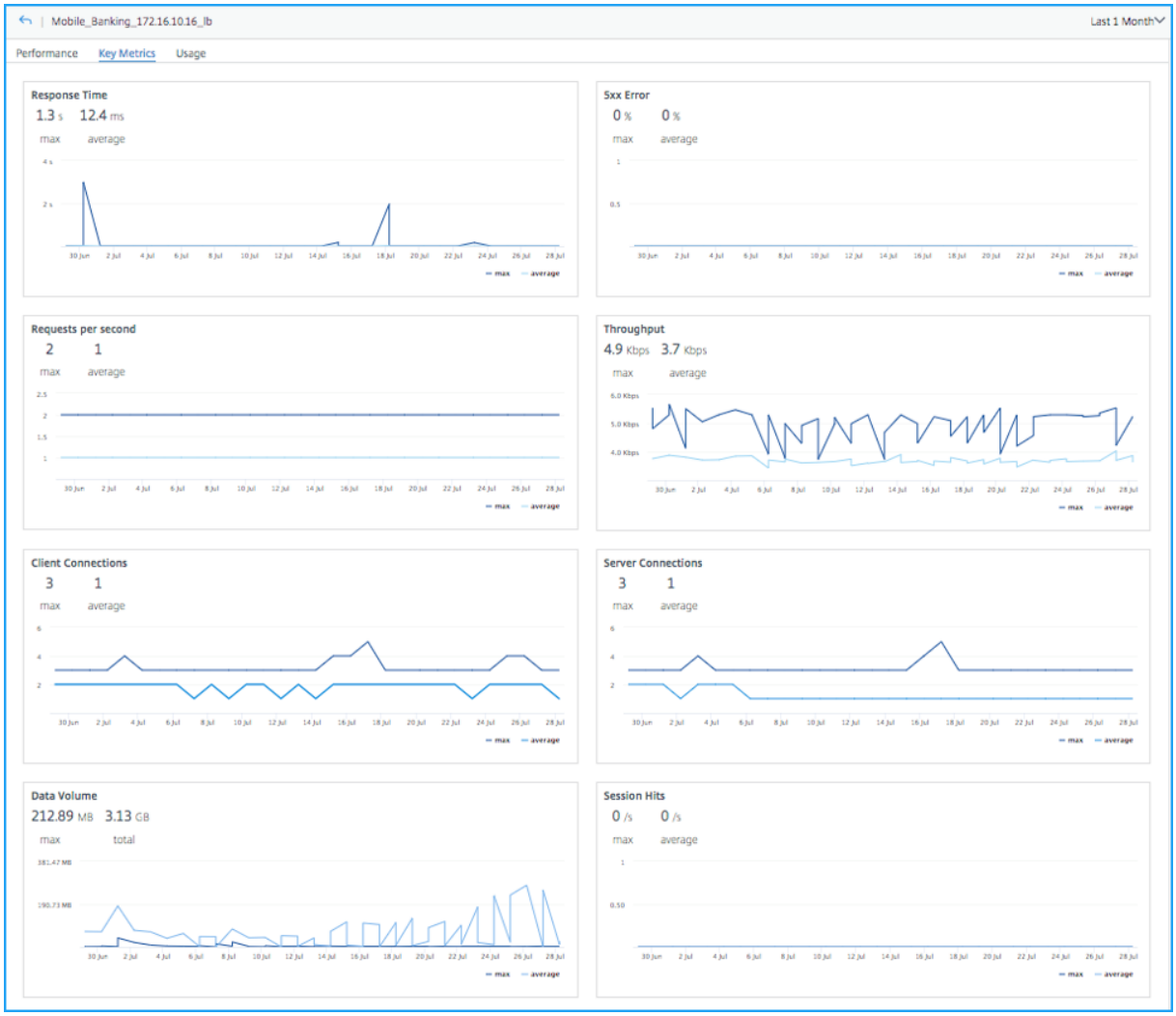
Une application Web peut recevoir un trafic élevé ou un faible trafic, et la plage de trafic pour chaque jour ou heure est certainement imprévisible. De même, une application Web nécessite également des temps d'arrêt pour une durée spécifique lors d'une maintenance planifiée ou d'une mise à niveau. En tant qu'administrateur, vous devez analyser le trafic et trouver le bon moment pour :

- Mise à l'échelle de l'application Web
- Planifier un temps d'arrêt d'une application Web

La fonctionnalité d'analyse d'utilisation maximale et des périodes creuses dans Citrix ADM vous permet d'analyser les mesures clés pour une durée sélectionnée. À partir de ces mesures, vous pouvez analyser le trafic et décider quand vous souhaitez augmenter l'application Web ou planifier un temps d'arrêt planifié.

Évaluer les limites d'échelle des applications

Cliquez sur une **application dans le Tableau de bord** de l'application et sélectionnez l'onglet **Mesures clés** pour visualiser la vue consolidée de toutes les mesures. Sélectionnez la durée dans la liste pour analyser les mesures.



Pour chaque mesure, vous pouvez afficher :

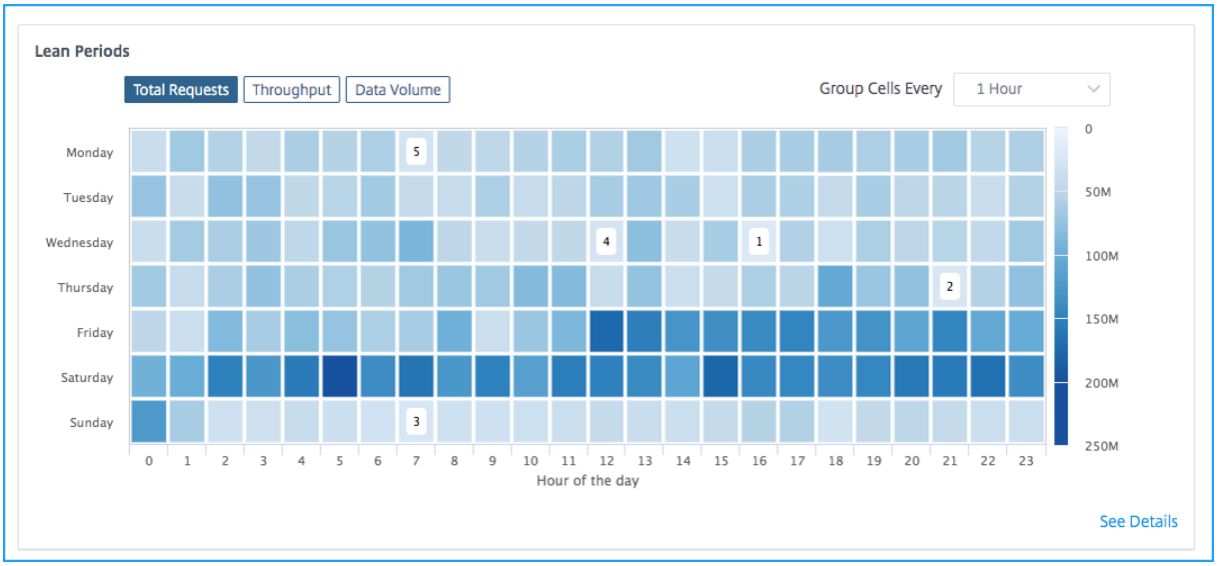
- **Max** — Indique la valeur maximale pour la durée sélectionnée
- **Moyenne** : indique la valeur moyenne de la durée sélectionnée.

Selon l'exemple de l'image, la valeur maximale du temps de réponse indique 1,3 s. À partir du graphique graphique, vous pouvez analyser le nombre de fois où le temps de réponse élevé s'est produit pour la durée sélectionnée. De même, vous pouvez également afficher les détails d'autres mesures, analyser si l'application a reçu un pic d'utilisation et prendre la décision d'augmenter l'environnement de production.

Identifier les 5 principales fenêtres de maintenance des applications

Cliquez sur une **application dans le Tableau de bord** de l'application et sélectionnez l'onglet **Mesures clés** pour afficher la période de repli de l'application. Un temps d'arrêt typique pour une application peut être de 1 heure, 2 heures ou 4 heures, selon les besoins. Vous pouvez sélectionner

l'heure dans la liste (1 heure, 2 heures ou 4 heures) que vous souhaitez planifier pour les temps d'arrêt. Après avoir sélectionné l'heure dans la liste, vous pouvez analyser le trafic pour des mesures telles que les demandes totales, le débit et le volume de données. Vous pouvez sélectionner le bon moment pour planifier un temps d'arrêt lorsque l'utilisation de l'application est moindre.
L'exemple suivant consiste à analyser le temps d'arrêt pour la durée d'une heure.



La vue Heatmap indique l'utilisation de l'application pour la durée sélectionnée. Plus la couleur est foncée (bleu), indique que l'utilisation de l'application est plus élevée.

La vue de la carte thermomégraphique suggère également les cinq premières périodes (1, 2, 3, 4 et 5) pour planifier le temps d'arrêt de l'application.

1 — Indique la première suggestion pour mercredi de 16h à 17h

2 — Indique la deuxième suggestion pour le jeudi de 21h à 22h

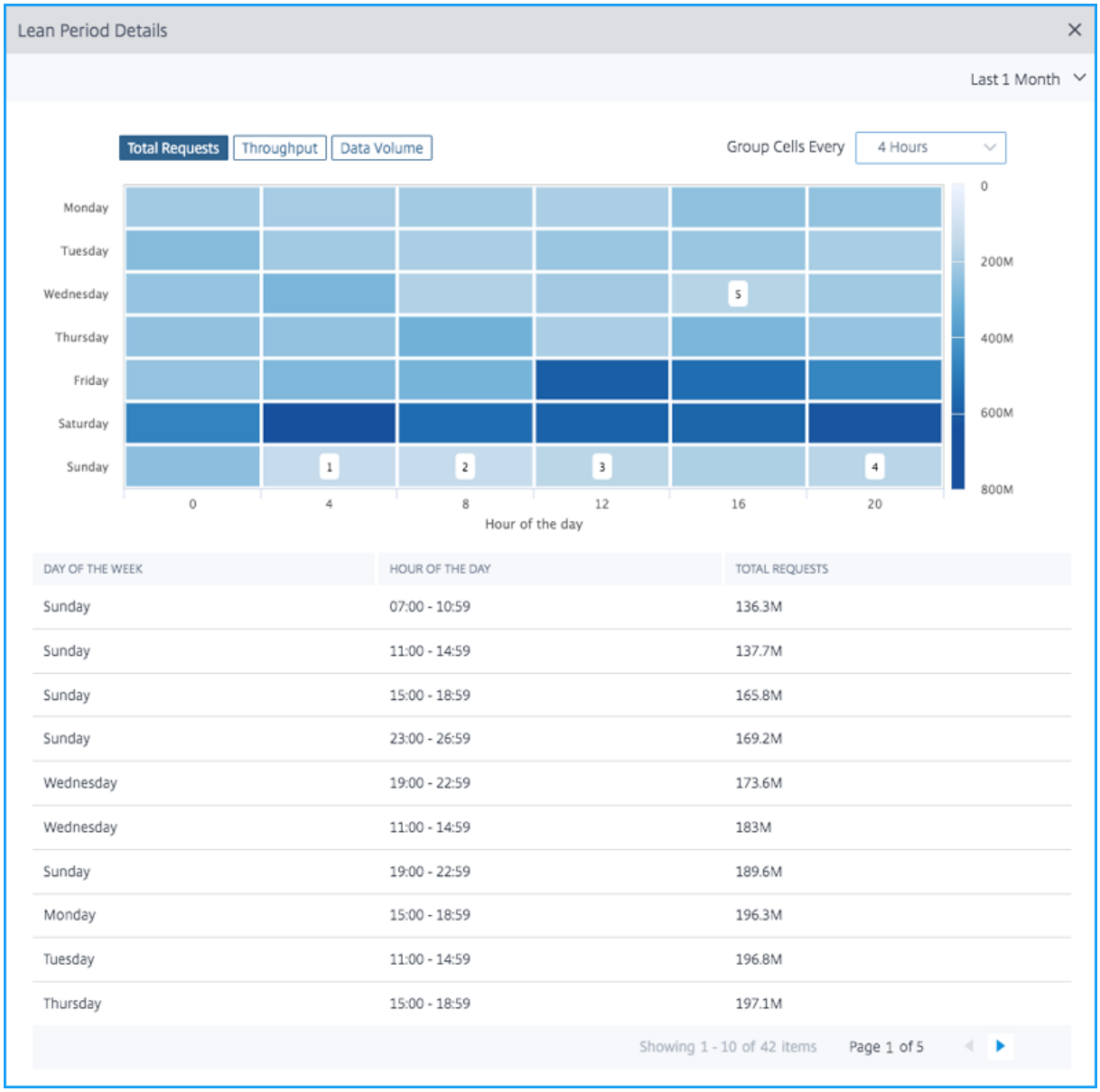
3 — Indique la troisième suggestion pour le dimanche de 7h à 20h

4 — Indique la quatrième suggestion pour mercredi de 12h à 13h

5 — Indique la cinquième suggestion pour le lundi de 7h à 20h

Vous pouvez également sélectionner n'importe quel autre jour et heure pour planifier un temps d'arrêt, après avoir analysé le trafic pour tous les autres jours.

Cliquez sur **Voir les détails** pour afficher d'autres informations détaillées. Cliquez sur l'onglet **Total des demandes**, **Débit**ou **Volume de données** pour afficher les détails des 5 premières périodes les moins importantes et également pour les autres jours.



Utilisation des applications et anomalies

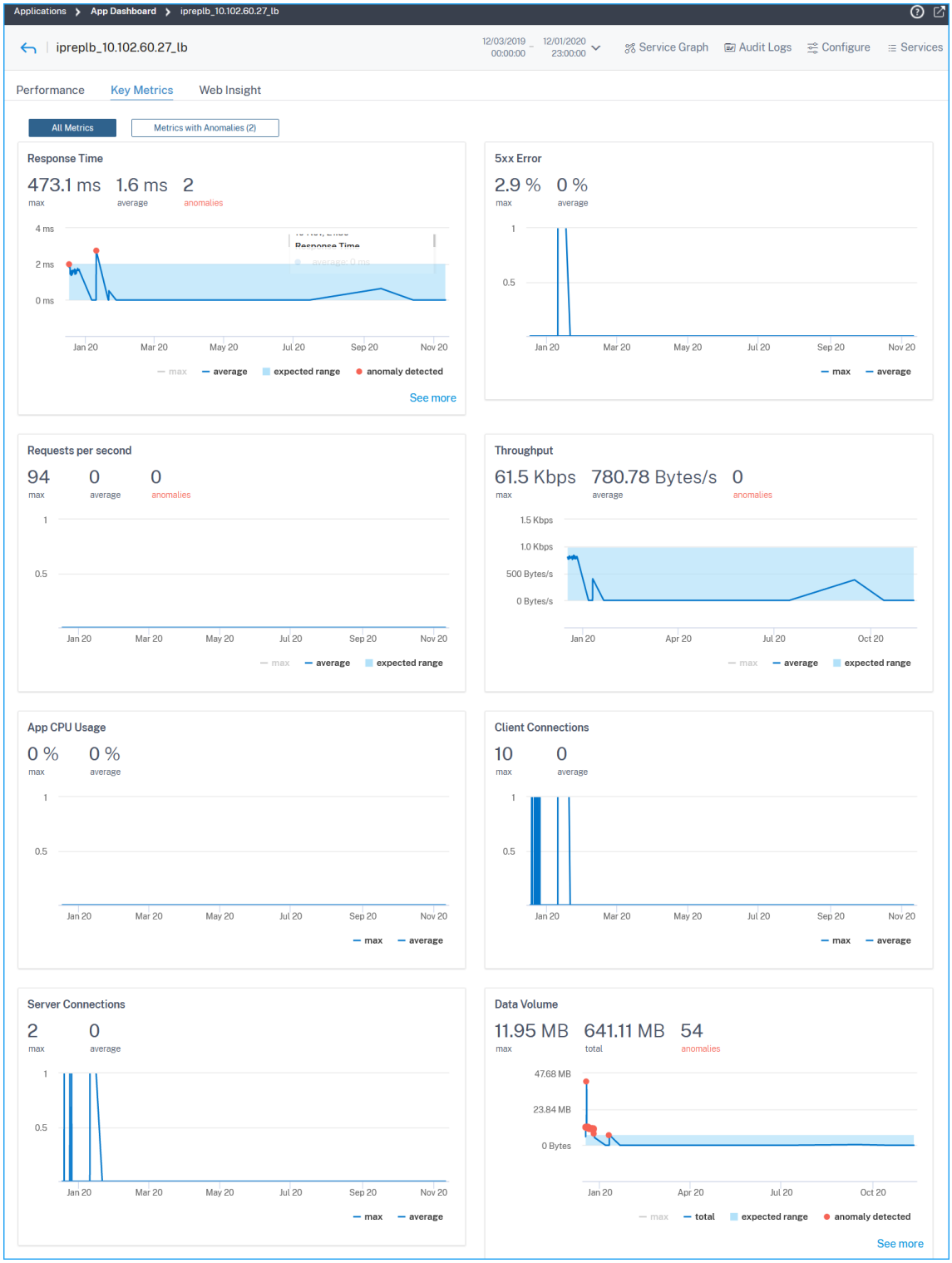
April 29, 2021

En tant qu'administrateur, vous devez vérifier comment l'application est utilisée. Les mesures de clé d'application peuvent vous aider à identifier l'utilisation de l'application. Étant donné que la plage de trafic vers l'application est imprévisible, des écarts inhabituels de performances de l'application peuvent survenir pendant une durée spécifique. Dans de tels scénarios, en tant qu'administrateur, vous pouvez consulter et analyser ces anomalies soudaines et vérifier si un dépannage immédiat est nécessaire.

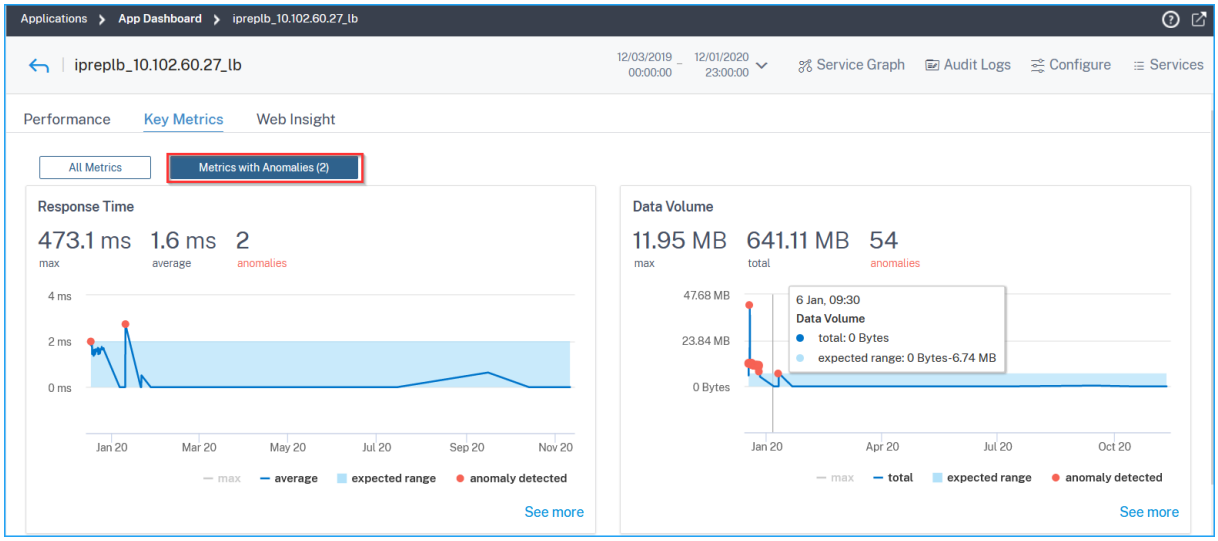
Citrix ADM détecte de telles anomalies et fournit les détails nécessaires. Accédez à **Applications > Tableau de bord**, cliquez sur une application, puis sélectionnez l'onglet **Mesures clés** . Citrix ADM surveille le schéma de trafic et analyse si les mesures clés se situent dans la plage attendue. S'il y a un écart par rapport à la plage attendue, Citrix ADM signale ces écarts comme des anomalies.

Vous pouvez afficher les anomalies pour les mesures clés suivantes :

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



Cliquez sur l'onglet **Mesures avec anomalies** pour afficher les détails.



Dans chaque mesure, vous pouvez également cliquer sur l'option **Voir plus** pour afficher les détails. L'exemple suivant concerne le volume de données d'application :

Vous pouvez voir :

- Graphique indiquant la valeur maximale, la valeur totale, la plage attendue et les anomalies
- **Actions recommandées** pour résoudre le problème
- Les détails de l'heure et de l'anomalie sous **Détails**

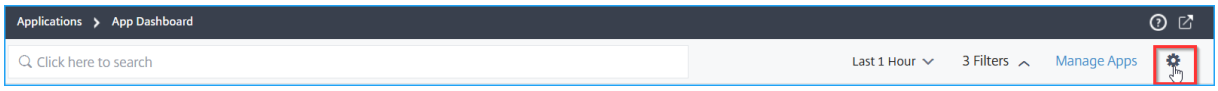
Sélectionnez les composants App Score et définissez des seuils

April 29, 2021

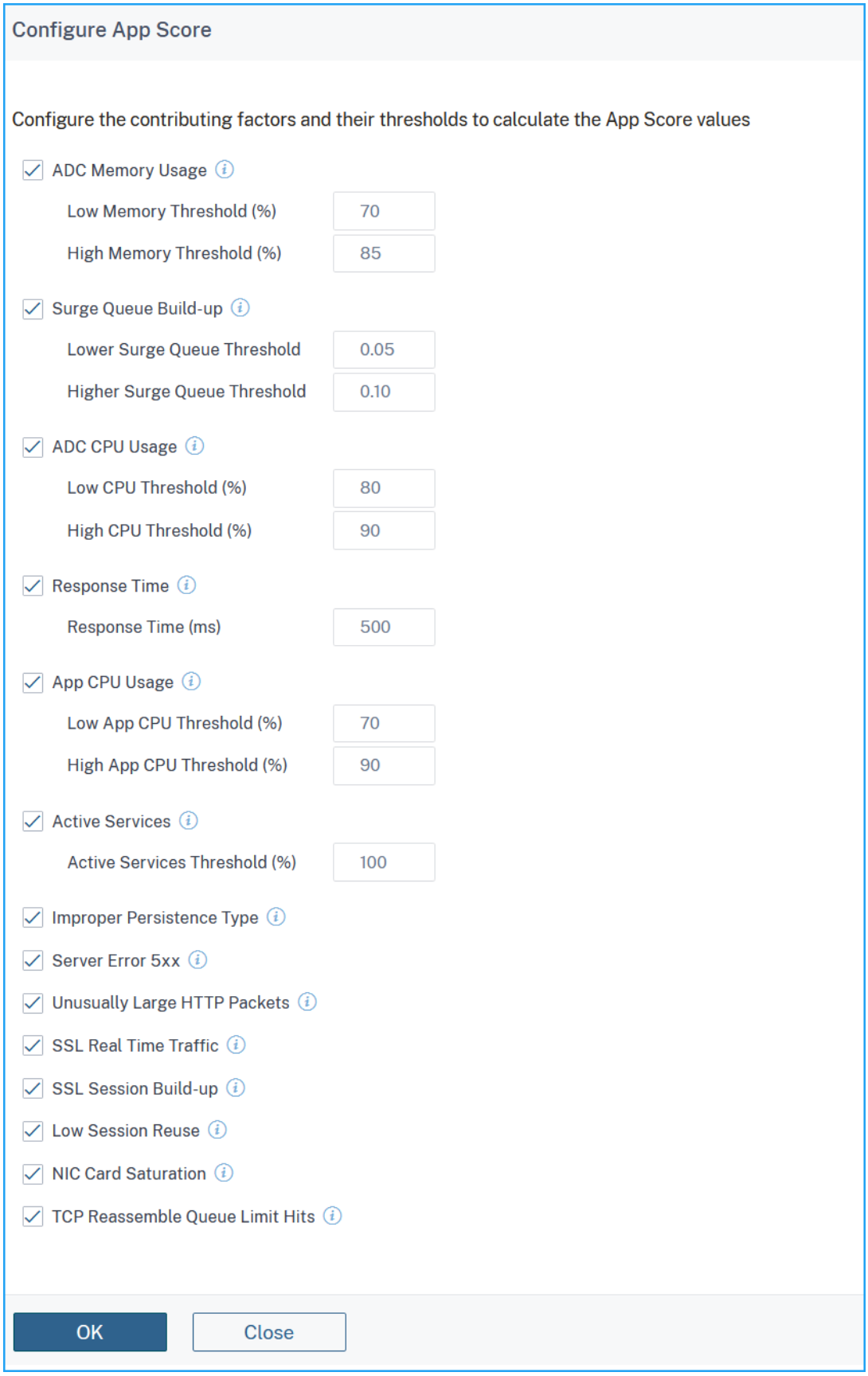
Dans le **Tableau de bord des applications**, en tant qu'administrateur, vous pouvez décider de sélectionner les composants et de configurer des seuils pour le calcul du score de l'application. App Score est le système de notation qui définit :

- Comment une application fonctionne bien
- Si l'application fonctionne bien en termes de réactivité

Accédez à **Applications > Tableau de bord**, puis sélectionnez l'icône Paramètres.



Dans la page **Configurer le score de l'application**, vous pouvez sélectionner les composants et configurer des seuils pour déterminer le score final de l'application.



Le calcul du score de l'application est basé sur les éléments suivants :

Composants App Score	Seuils configurés par l'utilisateur	Description
Utilisation de la mémoire ADC	Oui	Valeur de seuil faible et élevée pour l'utilisation totale de la mémoire dans l'instance Citrix ADC
Build de file d'attente de surtension	Oui	Valeur de seuil faible et élevée pour le nombre total de demandes de surtension qui sont en file d'attente et qui nécessitent une réponse.
Utilisation du processeur ADC	Oui	Valeur de seuil faible et élevé pour l'utilisation totale de l'UC dans l'instance Citrix ADC.
Temps de réponse	Oui	Intervalle de temps entre l'envoi d'un paquet de requête et la réception du premier paquet de réponse à partir du service configuré sur le serveur virtuel.
Utilisation du processeur de l'application	Oui	Valeur seuil faible et élevée pour l'utilisation totale de l'UC par l'application.
Services actifs	Oui	Valeur de seuil du pourcentage de services qui doivent être actifs et qui sont liés au serveur virtuel.
Type de persistance incorrect	Non	Indique si l'utilisation de persistance sur un serveur virtuel est faible.
Erreur serveur (5xx)	Non	Indique si le serveur Web répond avec des erreurs 5xx.

Composants App Score	Seuils configurés par l'utilisateur	Description
Paquets HTTP exceptionnellement volumineux	Non	Indique les occurrences, si les messages HTTP avec la taille d'en-tête HTTP dépassent les valeurs configurées dans l'instance Citrix ADC.
Trafic en temps réel SSL	Non	Analyse le trafic SSL pour identifier le trafic en temps réel et suggère des paramètres de configuration optimaux pour améliorer la latence.
Construction de session SSL	Non	Indique l'accumulation de session sur une période de temps, ce qui peut entraîner une grande quantité de mémoire est retenue par ces sessions dans l'instance Citrix ADC.
Réutilisation basse session	Non	Indique si le nombre réel de sessions réutilisées par l'instance Citrix ADC est inférieur.
Saturation de carte réseau	Non	Indique le nombre total de paquets rejetés par les interfaces.
TCP réassembler les hits de limite de file d'attente	Non	Indique si les paquets hors service sur une connexion TCP dépassent la taille de la file d'attente de paquets hors commande configurée.

Par défaut, tous les composants sont activés. Si vous désactivez un composant, Citrix ADM effectue le calcul final du score de l'application uniquement en fonction des composants sélectionnés.

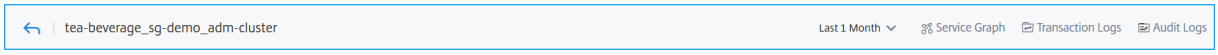
> Remarque
>
> Vous pouvez également continuer à configurer les seuils en accédant à **Analytics > Paramètres** et en cliquant sur **Configurer le score de l'application**. Pour de plus amples informations, consultez Créer un seuil et une alerte pour l'analyse des applications

Détails de la demande pour les applications de microservices

April 29, 2021

Cliquez sur une application de microservices dans le tableau de bord pour accéder à des informations plus détaillées.

La page de l'application sélectionnée s'affiche.

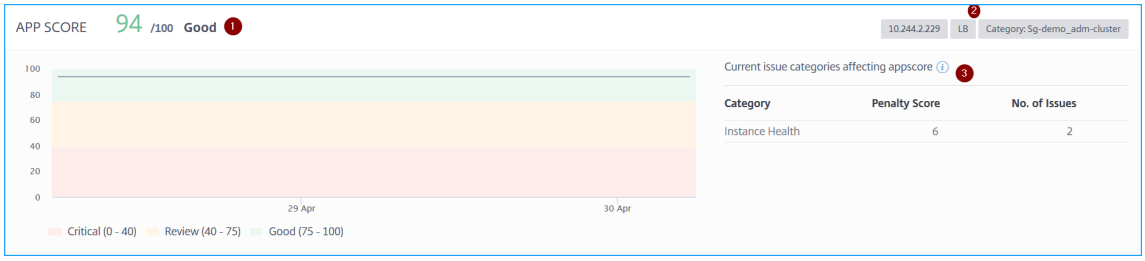


À partir de la page de détails de l'application :

- Sélectionnez la durée de temps dans la liste pour afficher les détails de la durée spécifique
- Cliquez sur **Graphique de service** pour afficher le graphique de service de l'application sélectionnée. Pour de plus amples informations, consultez Graphique de service pour les applications
- Cliquez **Journaux transactions** pour afficher les transactions détaillées de l'application sélectionnée
- Cliquez sur **Journaux d'audit** pour afficher les informations détaillées du journal d'audit

Après avoir sélectionné la durée, les détails de l'application suivants s'affichent :

- **Score** de l'application — Score de l'application pour la durée sélectionnée. Vous pouvez également afficher les problèmes d'application actuels, connus sous le nom de score de pénalité applicable en fonction de la catégorie de problème. Le score final est calculé comme **100 moins la pénalité totale**.



1 — Indique le score actuel de l'application

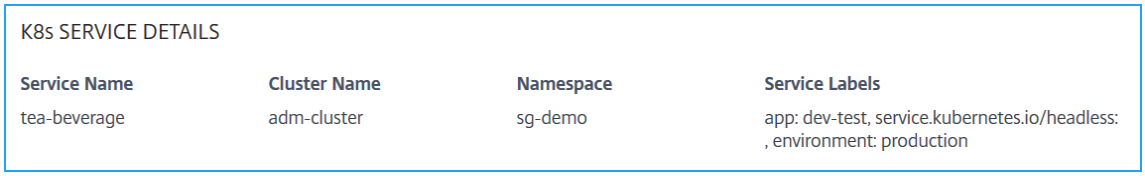
2 — Indique l'adresse IP CPX, le type d'application tel que l'équilibrage de charge ou la commutation de contenu, et l'espace de noms du service et le nom de cluster où le service est hébergé

3 — Indique les problèmes affectant le score de la demande actuelle

Ce tableau de bord vous permet également d'afficher les problèmes actuels qui affectent le score de l'application. Vous pouvez afficher les détails des problèmes sous Problèmes.

- **Détails du service K8s**

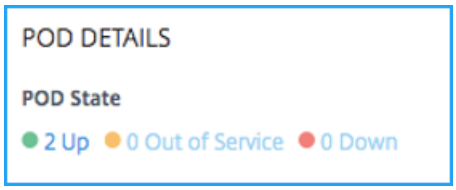
  Vous pouvez consulter les détails suivants :



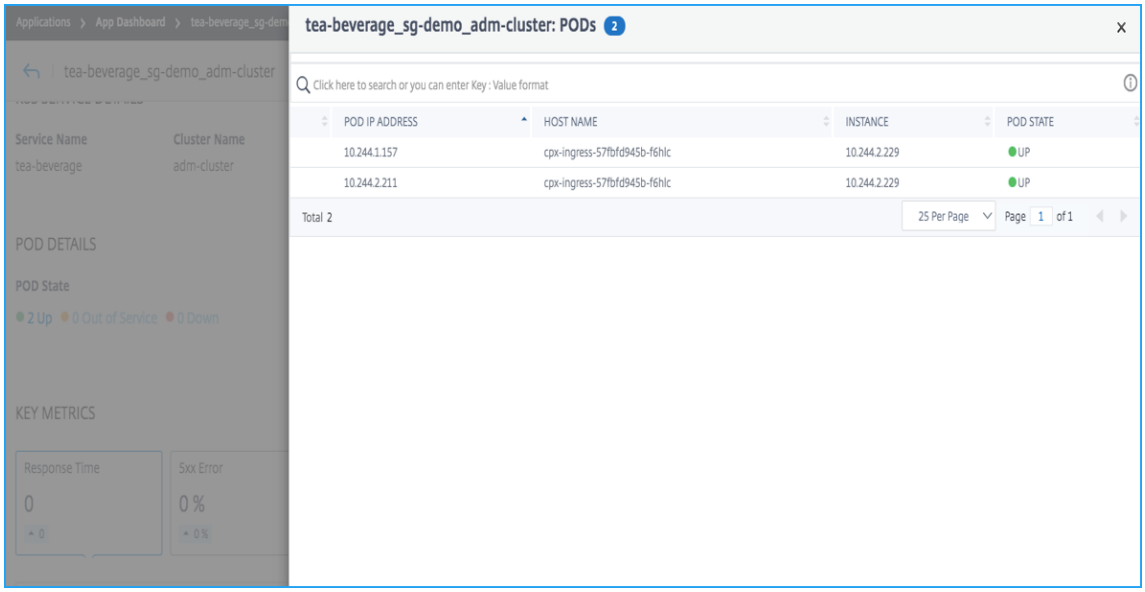
  - **Nom du service** — Nom du service
  - **Nom du cluster** — Nom du cluster dans lequel le service est hébergé
  - **Espace de noms** — Espace de noms attribué au service
  - **Étiquettes de service** — Étiquettes de service attribuées au service

- **Détails du Pod**

  Un conteneur est un groupe de conteneurs hébergés dans le cluster Kubernetes. Dans un conteneur, vous pouvez déployer plusieurs applications conteneurisées. Chaque module est associé à une adresse IP.



  Cliquez sur l'état du conteneur pour afficher les détails

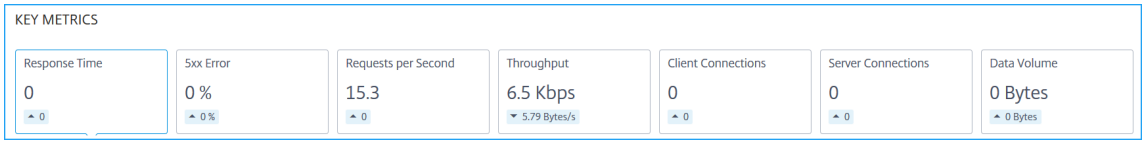


  - **Adresse IP du Pod** — Indique l'adresse IP du Pod
  - **Nom d'hôte** — Indique le nom d'hôte affecté au conteneur
  - **Instance** — Indique l'adresse IP CPX Citrix ADC
  - **état POD** — Indique l'état actuel du conteneur

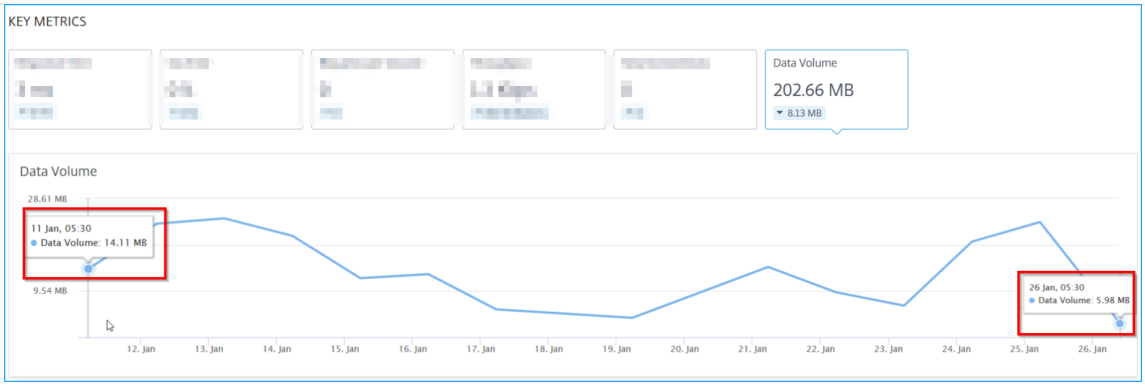
- **Mesures clés** — Les détails des mesures clés, tels que le **temps de réponse**, les **erreurs 5xx**, les **demandes par seconde**, le **débit**, les **connexions client, les connexionsserveur**et le**volume de données**, s'affichent.

  Dans chaque mesure, vous pouvez afficher la valeur moyenne et la valeur de différence pour la durée sélectionnée. La valeur de différence est calculée comme la **première valeur moins la dernière valeur** de la durée sélectionnée.

  Vous pouvez afficher les mesures d'instance suivantes dans un format graphique pour la durée sélectionnée :



  L'image suivante est un exemple de **volume de données** et la durée sélectionnée est de 1 mois. La valeur 202,66 Mo correspond au volume total de données pour la durée d'un mois et la valeur 8,13 Mo correspond à la valeur de différence. Dans le graphique, la première valeur est 14,11 et la dernière valeur est 5,98. La valeur de la différence est de 14,11 à 5,98 = 8,13 Mo.

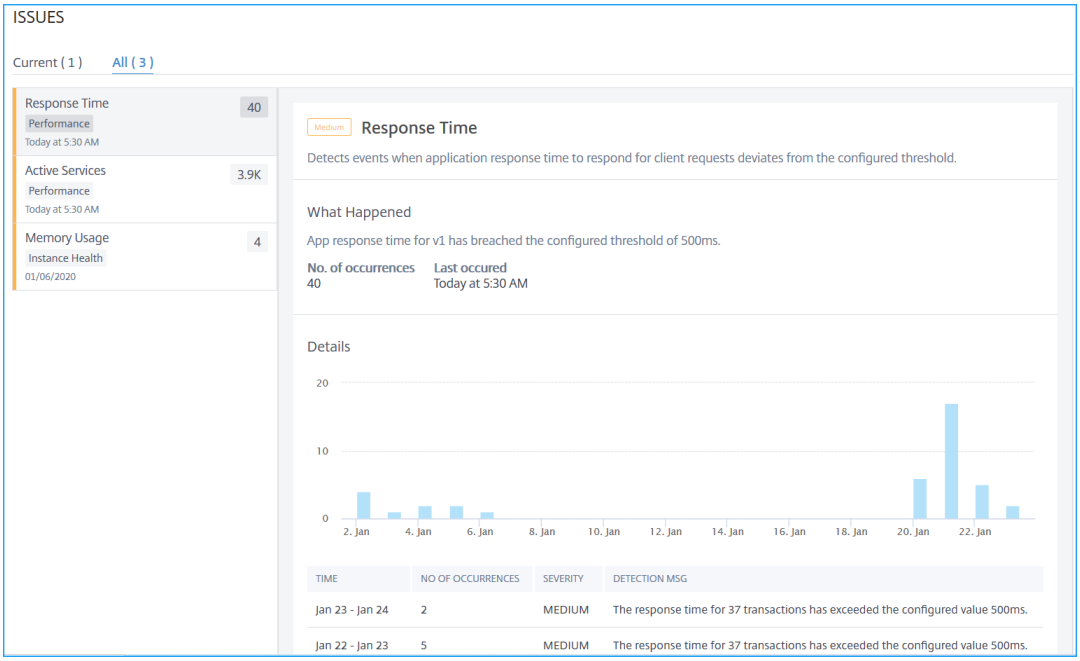


- **Questions** — Les questions qui s'appliquent à la demande sélectionnée. Vous pouvez afficher les problèmes suivants avec sa catégorie :

Performances	Santé de l'instance	Config	Ressources système
Temps de réponse	Utilisation moyenne de l'UC	Réponse élevée 5xx	Type de persistance incorrect
Réutilisation de session faible	Utilisation de mémoire	Paquets HTTP exceptionnellement volumineux	Saturation de la carte réseau
Accumulation dans la file d'attente de surtension		TCP réassembler les hits de limite de file d'attente	
Trafic en temps réel SSL			

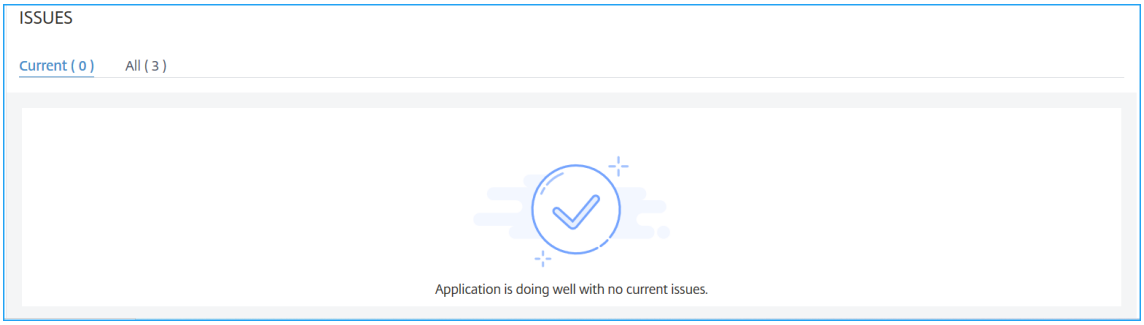
Cliquez sur chaque problème pour afficher les informations suivantes :

- Total des occurrences
- Actions recommandées pour résoudre le problème
- Les détails du problème tels que l'heure, le nom du service, le nombre total d'occurrences, la gravité et le message de détection



* Les problèmes qui s'affichent dans l'onglet **Courant** font référence aux problèmes d'application pour la durée de sélection.
* Les problèmes qui s'affichent dans l'onglet **Tous** font référence au nombre total de problèmes d'application.

L'exemple suivant est les problèmes d'application pour une durée d'un jour. L'onglet **Courant** indique aucun problème actuel n'affectant le score de l'application.



L'onglet **Tous** affiche le nombre total de problèmes détectés pour la durée d'un jour.

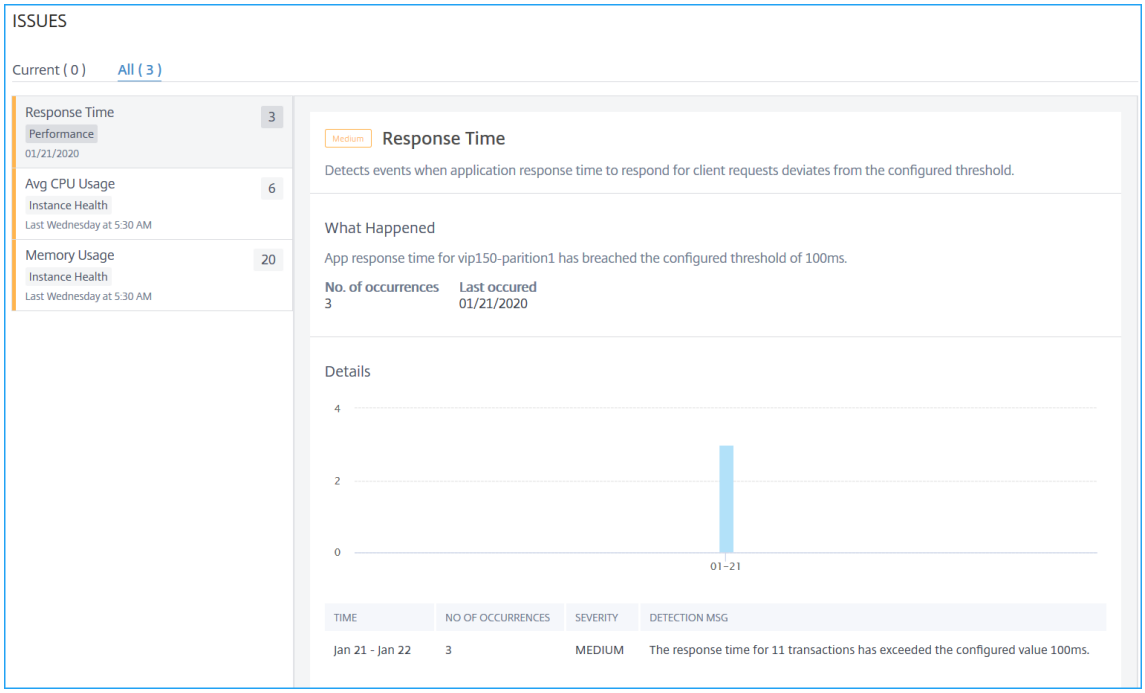


Tableau de bord Web Insight

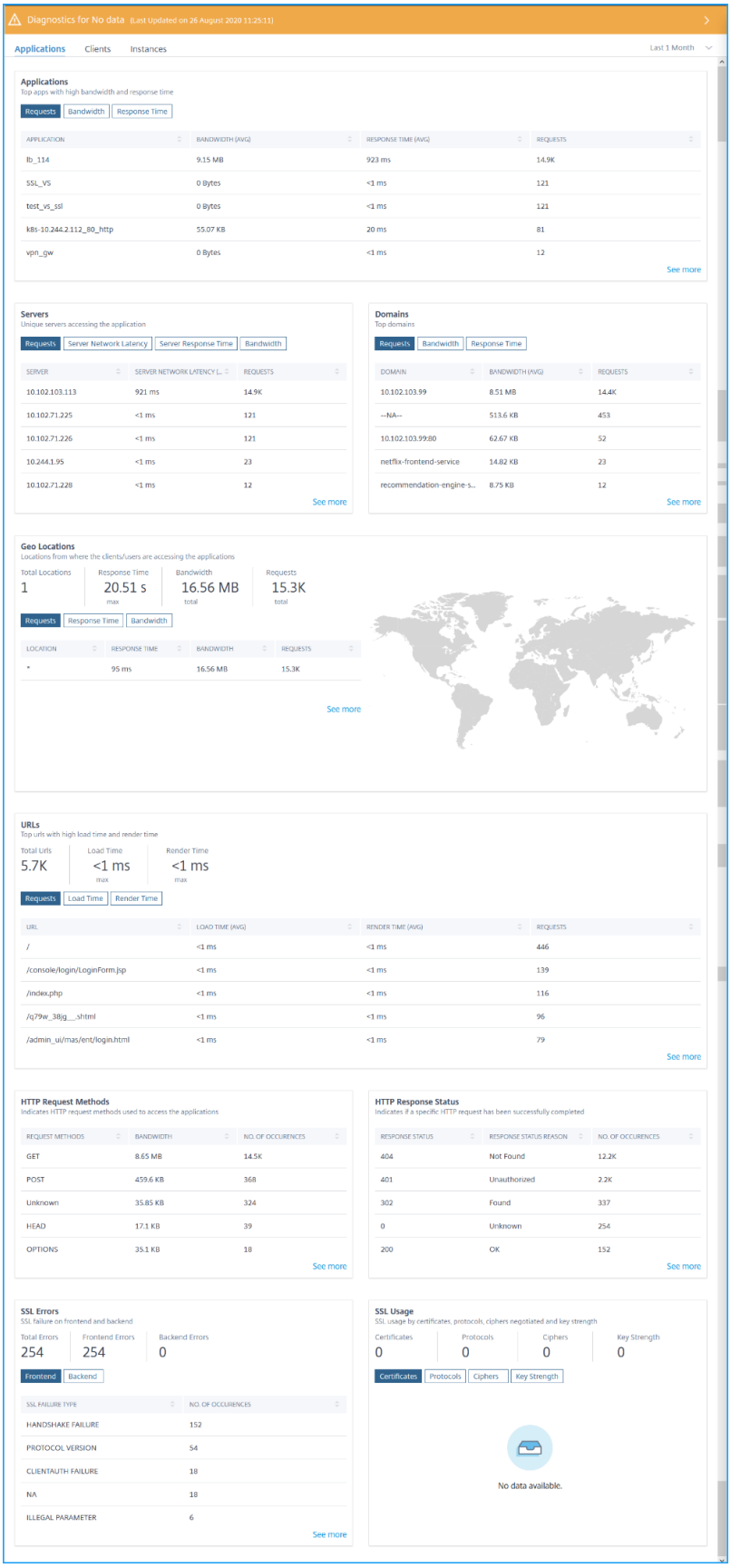
April 29, 2021

La fonctionnalité améliorée de Web Insight est augmentée et fournit une visibilité sur les mesures détaillées pour les applications Web, les clients et les instances Citrix ADC. Cette amélioration Web Insight vous permet d'évaluer et de visualiser l'application complète du point de vue des performances et de l'utilisation ensemble. En tant qu'administrateur, vous pouvez afficher Web Insight pour :

- Une application. Accédez à **Applications > Tableau de bord**, cliquez sur une application, puis sélectionnez l'onglet **Web Insight** pour afficher les mesures détaillées. Pour de plus amples informations, consultez la section Analyse de l'utilisation des applications.
- Toutes les applications. Accédez à **Applications > Web Insight** et cliquez sur chaque onglet (Applications, Clients, Instances) pour afficher les mesures suivantes :

Applications	Clients	Instances
Application avec anomalies de temps de réponse	Clients	Mesures d'instance
Applications	Emplacements géographiques	Applications
Serveurs	Méthodes de requête HTTP	Domaines

Applications	Clients	Instances
Domaines	État de la réponse HTTP	URL
Emplacements géographiques	URL	Méthodes de requête HTTP
URL	OS	État de la réponse HTTP
Méthodes de requête HTTP	Navigateurs	Clients
État de la réponse HTTP	Erreurs SSL	Serveurs
Erreurs SSL	Utilisation de SSL	OS
Utilisation de SSL		Navigateurs

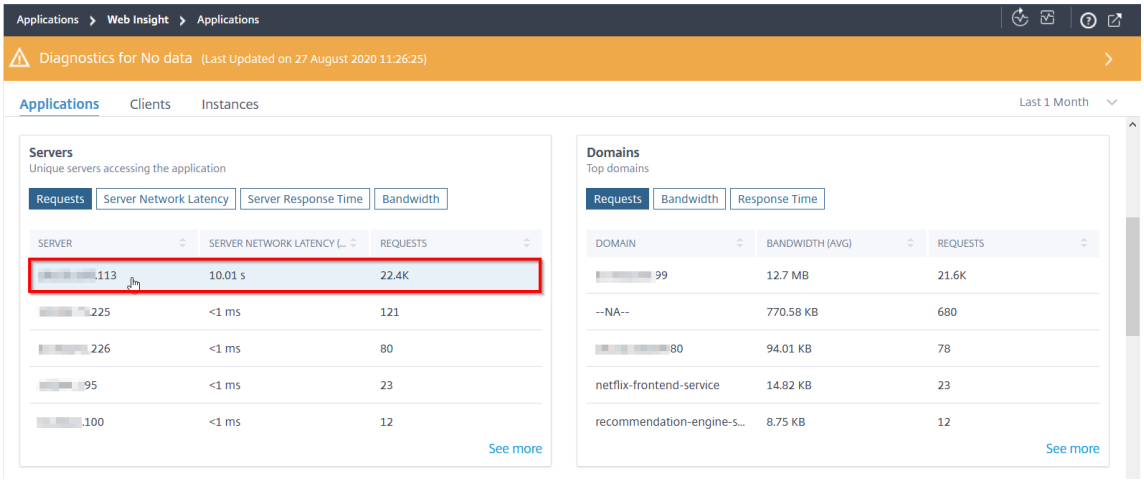


Dans chaque mesure, vous pouvez voir les 5 meilleurs résultats. Vous pouvez cliquer pour approfondir l'exploration vers le bas pour analyser le problème et prendre des mesures de dépannage plus rapidement.

> Remarque
>
> Dans certains scénarios, Citrix ADC peut ne pas être en mesure de calculer les valeurs RTT pour certaines transactions. Pour de telles transactions, Citrix ADC envoie la valeur zéro à Citrix ADM et Citrix ADM affiche RTT comme < 1 ms.

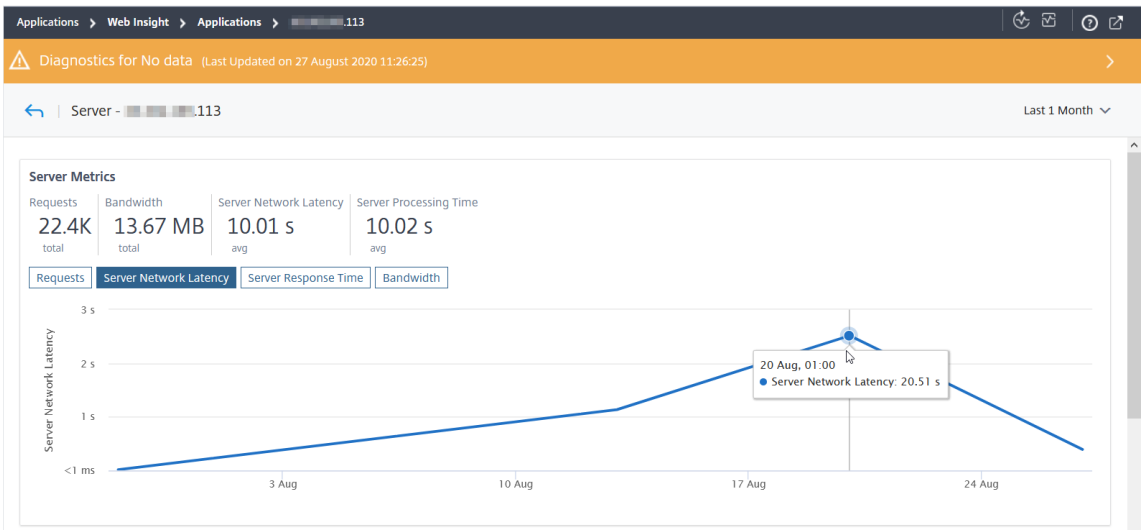
Par exemple, considérez que vous souhaitez analyser la latence du réseau du serveur pour une durée d'un mois et prendre la décision d'augmenter ou de réduire l'environnement de production. Pour analyser ceci :

1. Sélectionnez 1 dernier mois dans la liste et dans l'onglet **Applications**, faites défiler jusqu'à **Serveurs**, puis cliquez sur un serveur.



   Les détails des mesures pour le serveur sélectionné s'affichent.

2. Sélectionnez l'onglet **Latence réseau du serveur** pour analyser la latence.



La latence moyenne indique 10,01s et à partir du graphique, vous pouvez analyser que la latence réseau serveur pour le dernier mois semble être élevée. En tant qu'administrateur, vous pouvez prendre la décision d'étendre l'environnement de production.

Pour plus d'informations sur le cas d'utilisation de Web Insight, consultez Web Insight.

Analyser la cause première de la lenteur de l'application

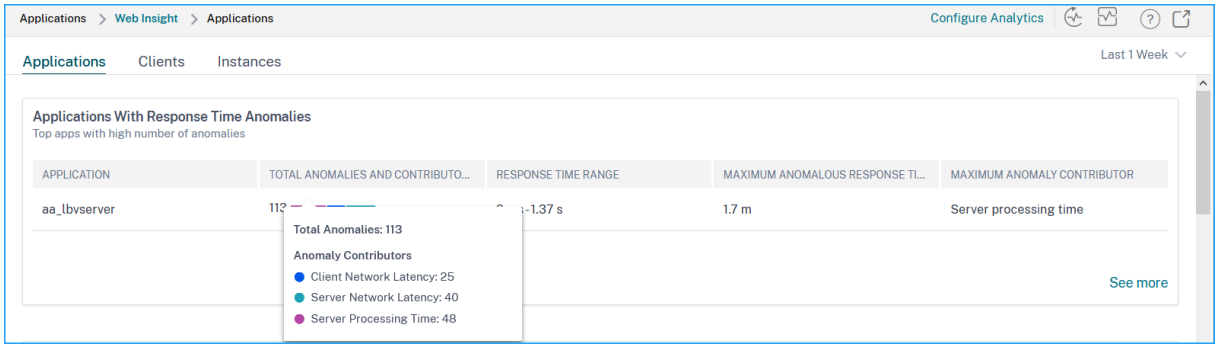
April 29, 2021

La lenteur des applications est une préoccupation majeure pour toute organisation, car elle entraîne un impact commercial ou une productivité. En tant qu'administrateur, vous devez vous assurer que toutes les applications fonctionnent de manière optimale afin d'éviter tout impact sur l'entreprise. Lorsque vos utilisateurs rencontrent une lenteur dans l'accès à l'application, vous devez vous assurer que le problème concerne :

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

Citrix ADM effectue des vérifications des anomalies toutes les heures et signale les anomalies pour le trafic d'une heure passée, en fonction de certaines conditions préalables. Par exemple, pour éviter des résultats faux positifs, si le temps de réponse est inférieur à 1 ms, les vérifications d'anomalie pour ces résultats sont ignorées.

La page **Applications > Web Insight** vous permet d'afficher les applications présentant des anomalies de temps de réponse pour la durée sélectionnée. La mesure **Applications avec anomalies de temps de réponse** affiche les cinq premières applications en fonction du total des anomalies. Cliquez sur **Voir plus** pour afficher toutes les applications.



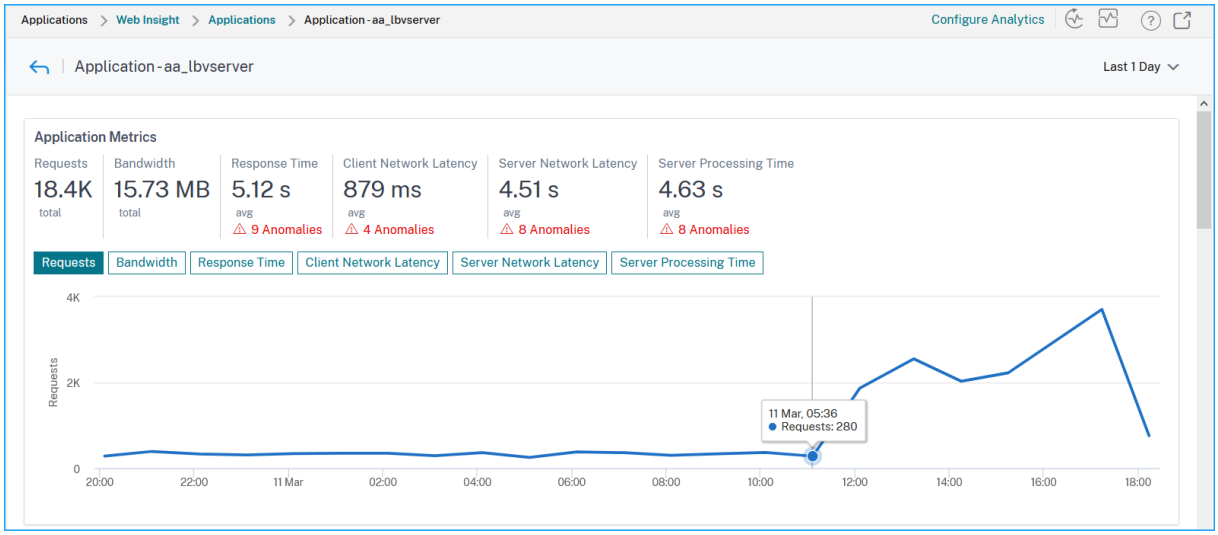
- **Application** — Indique le nom de l'application.
- **Total des anomalies et des contributeurs** — Indique le total des anomalies de l'application. Lorsque vous placez le pointeur de la souris, vous pouvez afficher le total des anomalies

provenant respectivement de la latence réseau client, de la latence réseau du serveur et du temps de traitement du serveur.

- **Plage de temps de réponse** : indique la plage de temps de réponse attendue de l'application.
- **Temps de réponse anormal maximal** : indique le temps de réponse le plus élevé de l'application.
- **Contributeur d'anomalie maximale** : indique si le nombre maximal d'anomalies pour l'application provient de la latence du réseau client, de la latence réseau du serveur ou du temps de traitement du serveur.

exploration vers le bas de l'application

Cliquez sur une application pour afficher les détails des **mesures d'application** pour la durée sélectionnée.



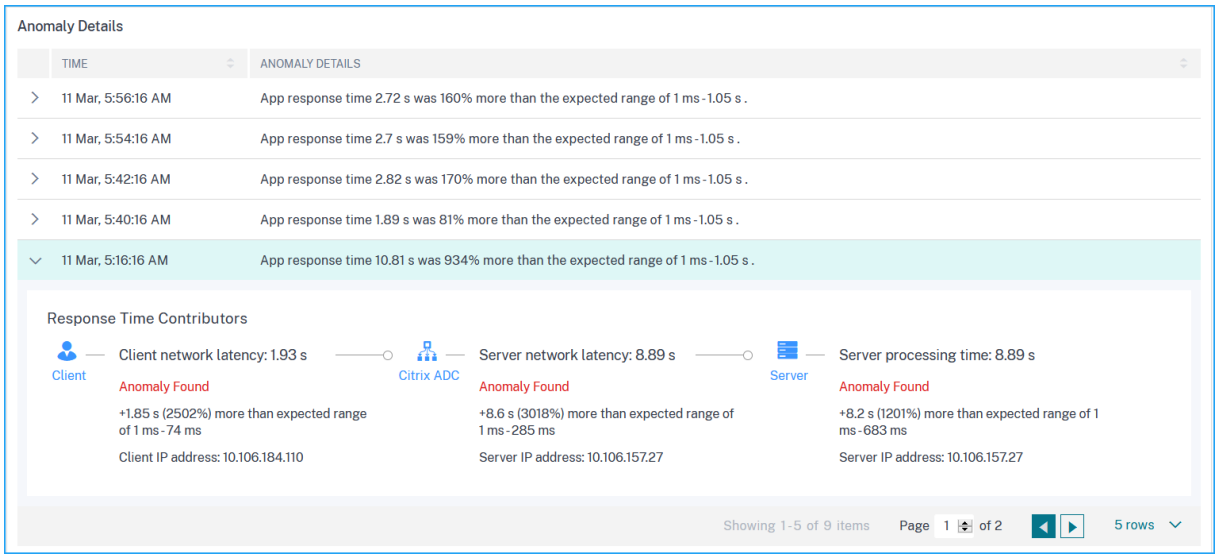
Les **mesures d'application** vous permettent d'afficher les éléments suivants :

- **Demandes** — Le total des demandes reçues par la demande
- **Bande passante** : bande passante totale traitée par l'application
- **Temps de réponse** — Temps de réponse moyen de l'application
- **Latence réseau client : latence** moyenne du réseau client (du client à l'ADC)
- **Latence réseau** du serveur : latence moyenne du réseau du serveur (de l'ADC au serveur)
- **Temps de traitement du serveur : temps** moyen de traitement du serveur (du serveur à l'ADC)

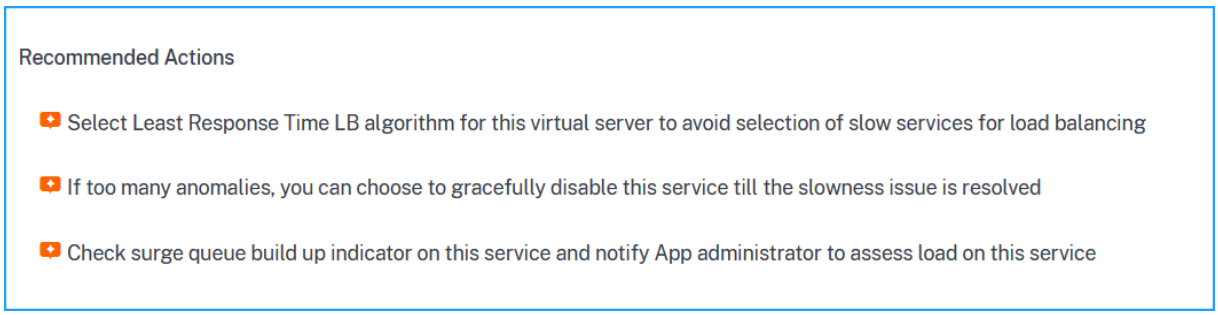
Si l'application présente des anomalies, vous pouvez voir si les anomalies proviennent de la latence du réseau client, de la latence du réseau du serveur ou du temps de traitement du serveur. Cliquez sur chaque onglet pour afficher les détails.

Temps de réponse

Sous **Détails des anomalies**, cliquez sur pour afficher les détails des contributeurs de temps de réponse (du client au serveur). L'exemple suivant présente une anomalie concernant la latence du réseau client, la latence réseau du serveur et le temps de traitement du serveur. Vous pouvez également afficher les plages attendues et la brèche qui s'est produite au-delà de la plage prévue.



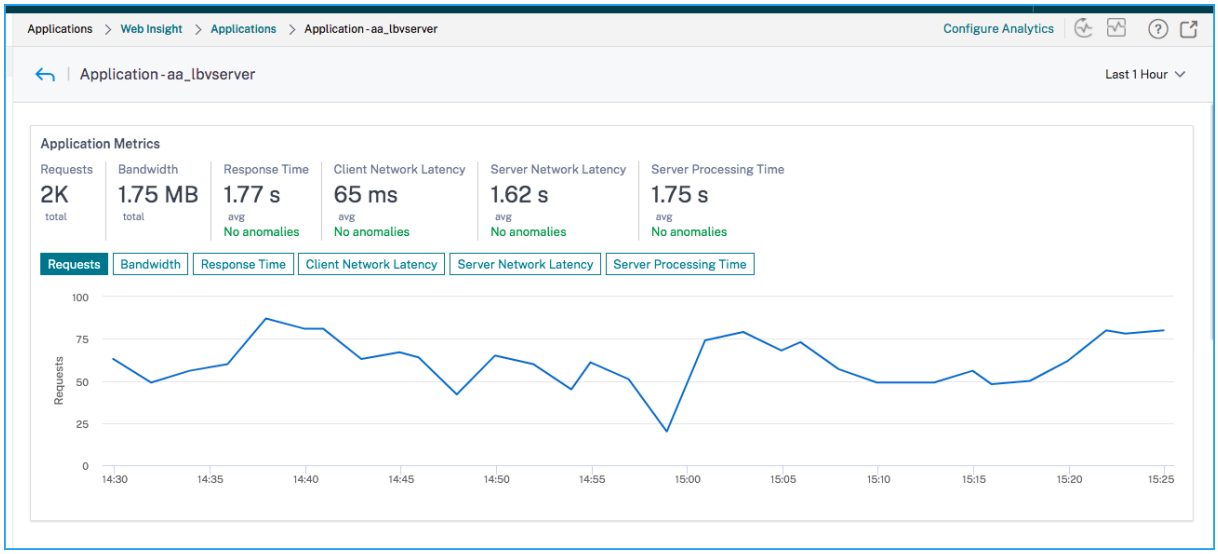
Les **actions recommandées** vous suggèrent les résolutions possibles pour les anomalies.



De même, vous pouvez cliquer sur les onglets **Latence réseau client, Latence**réseau**serveur et Temps de traitement** du serveur pour afficher :

- Anomalie qui a franchi la plage prévue.
- Actions recommandées qui vous suggèrent les résolutions possibles.

Si l'application fonctionne bien, vous pouvez afficher les mesures d'application comme aucune anomalie.



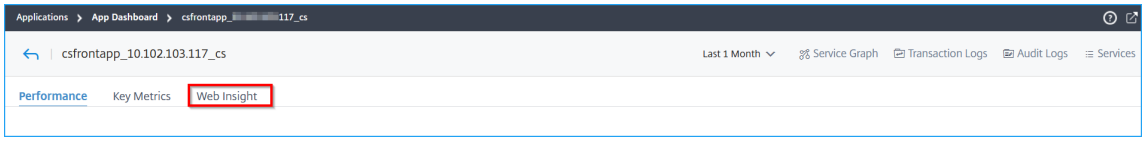
Analyse de l'utilisation des applications

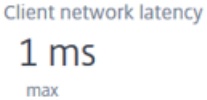
April 29, 2021

Les propriétaires d'applications doivent avoir la capacité d'évaluer et de visualiser l'application complète du point de vue de la performance et de l'utilisation.

Le tableau de **bord des applications** improvisé vous permet de visualiser toutes les performances de l'application et les mesures d'utilisation ensemble. Lorsque vous cliquez sur une application, en dehors des mesures de performances de l'application existantes, l'onglet **Web Insight** affiche les détails des mesures qui vous aident à :

- Comprenez l'utilisation de votre application.
- Corréler les écarts de performances avec les mesures d'utilisation.

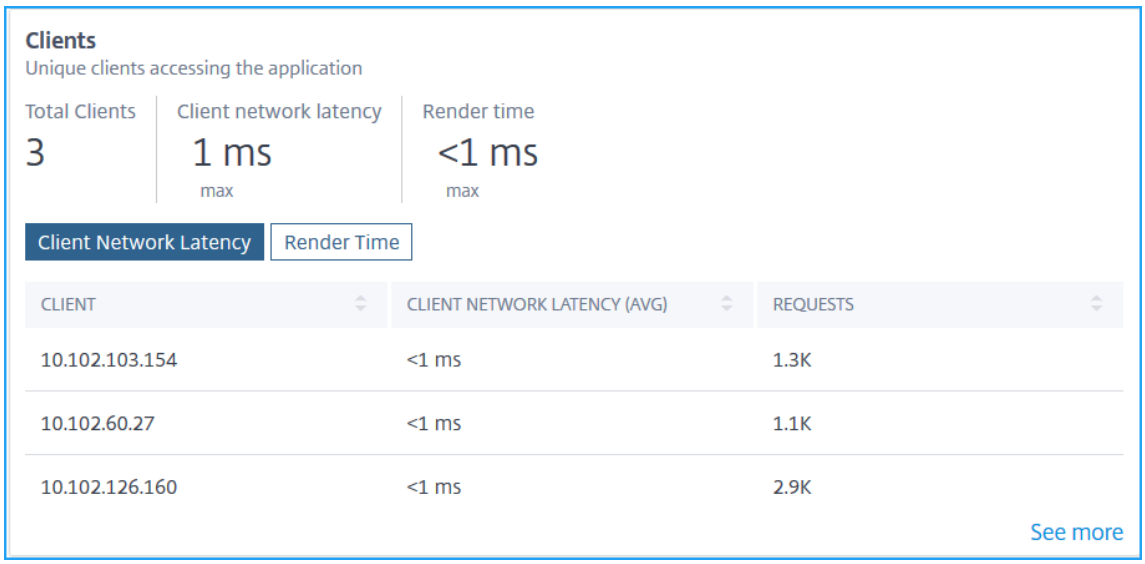


> **Remarque**
>
> Pour chaque mesure, vous pouvez afficher les options qui indiquent la valeur maximale et la valeur totale. Par exemple :
>
> - 
>
> - Latence maximale du réseau client pour la durée sélectionnée. Considérez que vous avez la latence réseau pour le client 1 = 30 ms, le client 2 = 15 ms et le client

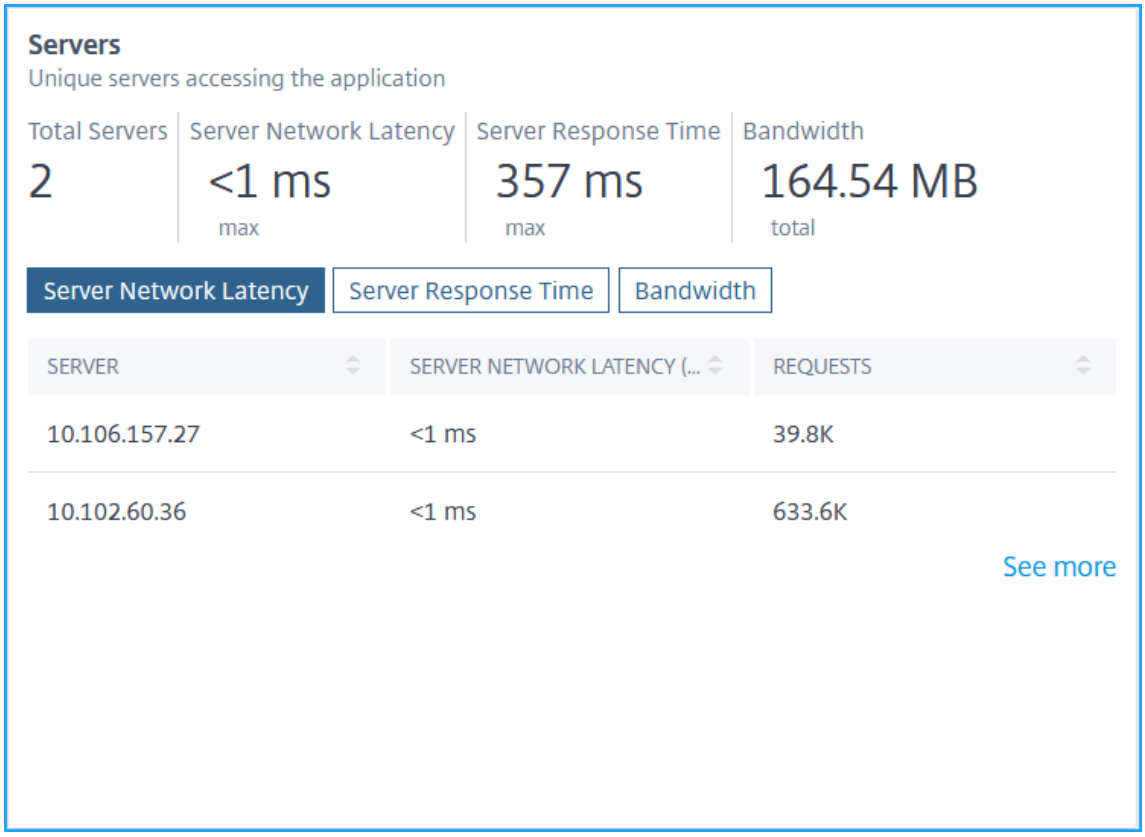
> 3 = 3 ms. Dans ce scénario, la **latence réseau client** affiche 30 ms.
>
> Bandwidth
> 164.54 MB
> total
> - Bande passante totale consommée sur tous les clients/serveurs disponibles pour la durée sélectionnée. Considérez que vous avez la consommation de bande passante pour le client 1 = 30 Mo, Client 2 = 45 Mo, Client 3 = 40 Mo. Dans ce scénario, la bande passante affiche (30 Mo + 45 Mo + 40 Mo) = 115 Mo.

Voici les mesures Web Insight que vous pouvez afficher à partir de l'onglet **Utilisation** :

- **Clients** — Affiche les informations pour les clients accédant à l'application :

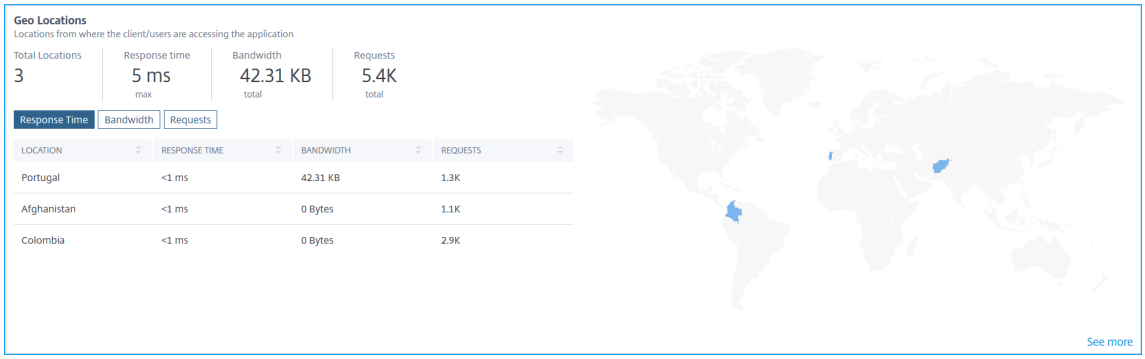


  - **Total clients** : affiche le nombre total de clients accédant à l'application.
  - **Latence réseau client** : affiche la latence réseau du client vers Citrix ADC. Cliquez sur l'onglet **Latence réseau client** pour afficher :
    - **Client** — Adresse IP du client.
    - **Latence réseau client (avg)** : latence réseau moyenne à partir du client.
    - **Demandes** : nombre total de demandes du client.
  - **Temps de rendu** : affiche le temps nécessaire pour rendre la réponse du serveur. Cliquez sur l'onglet **Temps de rendu** pour afficher :
    - **Client** — Adresse IP du client.
    - **Temps de rendu (moyenne)** : temps de rendu moyen à partir du client.
    - **Demandes** : nombre total de demandes du client.
- **Serveurs** : affiche les informations relatives aux serveurs accédant à l'application :



- **Total Serveurs** : affiche le nombre total de serveurs accédant à l'application.
- **Latence réseau du serveur** : affiche la latence réseau du serveur vers Citrix ADC. Cliquez sur l'onglet **Latence réseau du serveur** pour afficher :
  - **Serveur** — Adresse IP du serveur.
  - **Latence réseau du serveur (moy)** : latence réseau moyenne à partir du serveur.
  - **Requêtes** : nombre total de demandes provenant du serveur.
- **Temps de réponse du serveur** : affiche le temps nécessaire au serveur pour répondre aux demandes. Cliquez sur l'onglet **Temps de réponse du serveur** pour afficher :
  - **Serveur** — Adresse IP du serveur.
  - **Temps de réponse (moyenne)** : temps de réponse moyen du serveur.
  - **Requêtes** : nombre total de demandes provenant du serveur.
- **Bande passante** : affiche la bande passante totale consommée par les serveurs. Cliquez sur l'onglet **Bande passante** pour afficher :
  - **Serveur** — Adresse IP du serveur.
  - **Bande passante** : bande passante totale consommée à partir du serveur.
  - **Requêtes** : nombre total de demandes provenant du serveur.

- **Emplacements géographiques** : affiche les informations pour les clients accédant à l'application depuis un emplacement particulier :

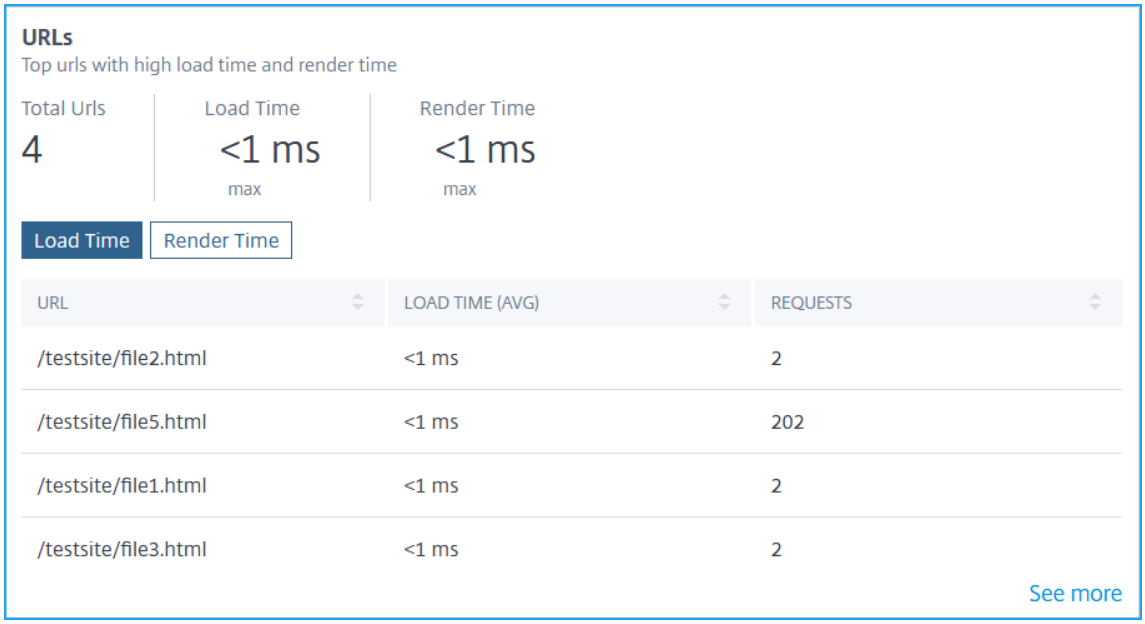


  - **Nombre total d'emplacements** : affiche le nombre total d'emplacements clients accédant à l'application.
  - **Temps de réponse** : affiche le temps de réponse à partir de l'emplacement du client.
  - **Bande passante** : affiche la bande passante totale consommée par les clients dans tous les emplacements.
  - **Demandes** : affiche le nombre total de demandes provenant de tous les emplacements clients.

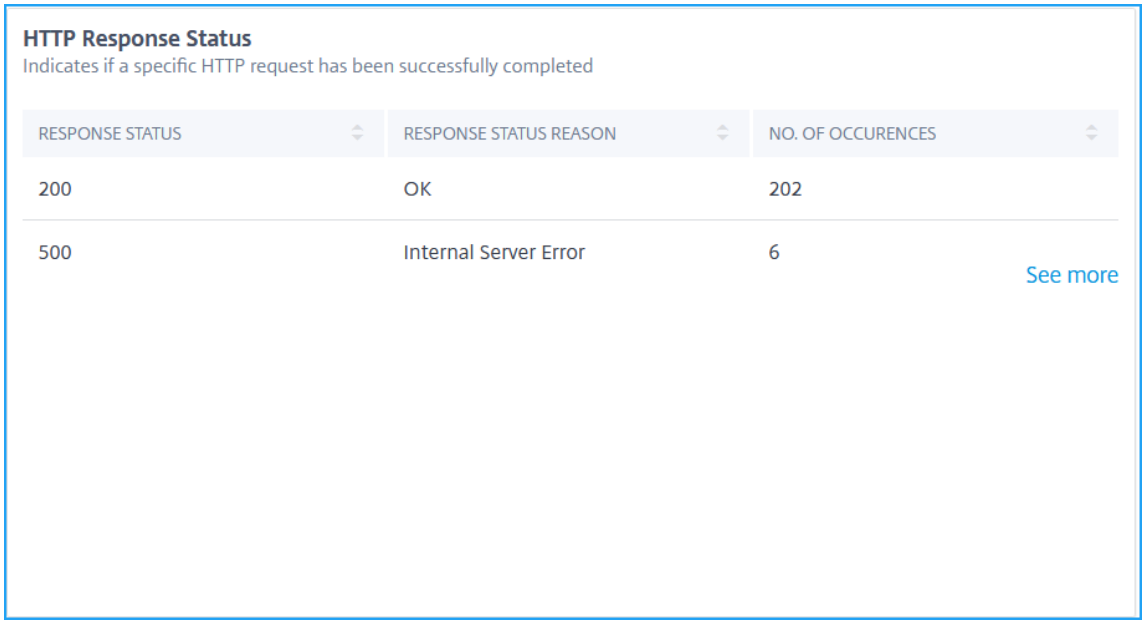
    Cliquez sur chaque onglet pour afficher :

    * **Emplacement** — Nom de l'emplacement.
    * Temps de**réponse : temps** de réponse moyen à partir de l'emplacement du client.
    * **Bande passante** : bande passante consommée à partir de l'emplacement client.
    * **Demandes** : nombre total de demandes provenant de l'emplacement client.

- **URL** : affiche les informations relatives aux URL avec un temps de chargement et de rendu élevés :

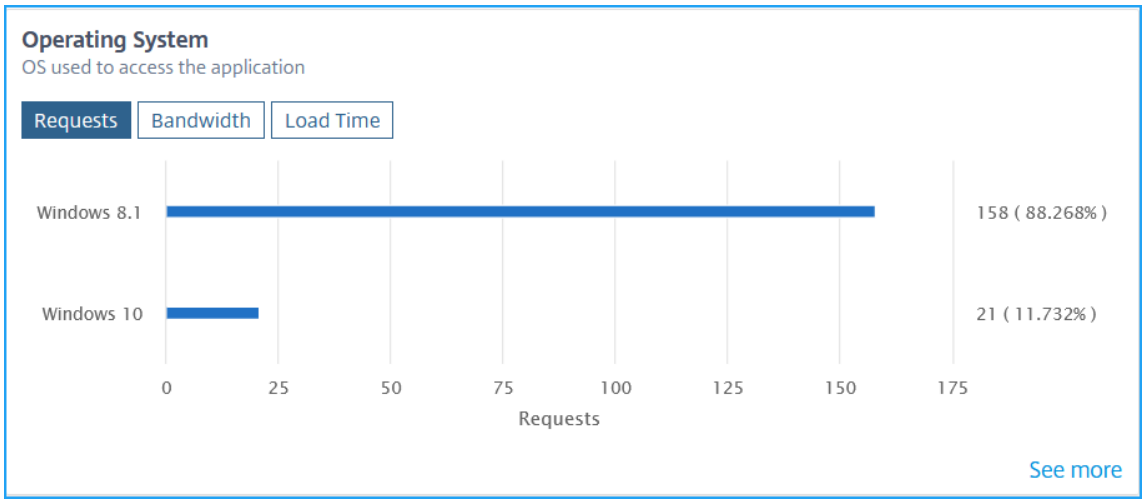


  - **Total des URL** : affiche le total des URL.
  - Heure de chargement : affiche le temps nécessaire au chargement de l'URL. Cliquez sur l'onglet **Temps de chargement** pour afficher :
    * **URL** — Nom de l'URL.
    * **Heure de chargement (moyenne)** : temps moyen de chargement de l'URL.
    * **Requêtes** — Nombre total de demandes provenant de l'URL.
  - **Temps de rendu** : affiche le temps nécessaire pour le rendu et l'affichage de l'URL. Cliquez sur l'onglet **Temps de rendu** pour afficher :
    * **URL** — Nom de l'URL.
    * **Temps de rendu (avg)** : temps moyen de rendu de l'URL.
    * **Requêtes** — Nombre total de demandes provenant de l'URL.
- **Statut de la réponse HTTP** : affiche les informations relatives à une requête HTTP terminée spécifique.



  - **État** de la réponse : affiche le code de réponse tel que 2xx, 4xx, 5xx, etc.
  - **Raison du statut** de la réponse — Affiche le motif de réponse, tel que l'erreur interne du serveur, Introuvable, etc.
  - **Nombre d'occurrences** : affiche le nombre total d'occurrences.

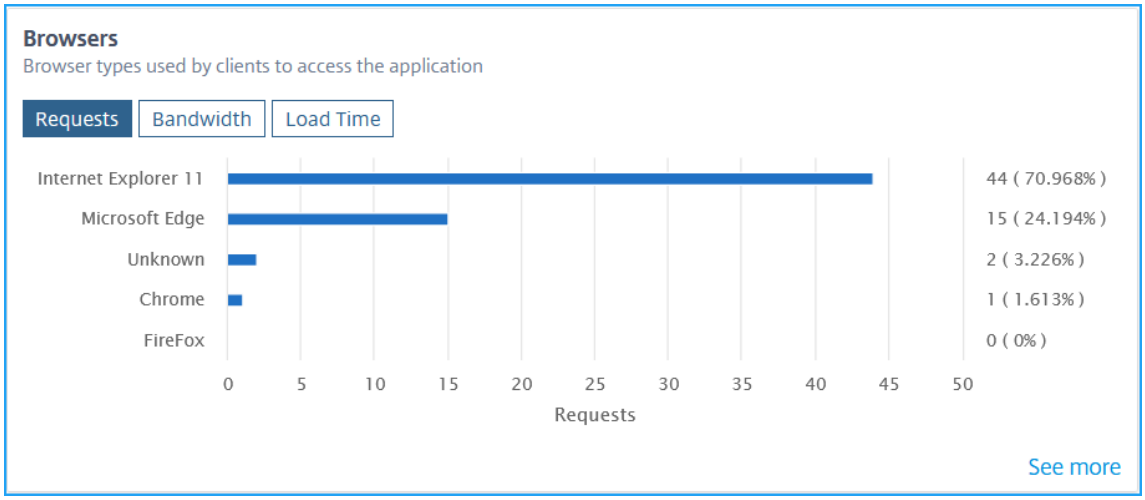
- **Système d'exploitation** : affiche les informations relatives au système d'exploitation qui accède à l'application.



  - **Demandes** : affiche le nombre total de demandes provenant de chaque système d'exploitation.
  - **Bande passante** : affiche la bande passante totale consommée par chaque système d'exploitation.

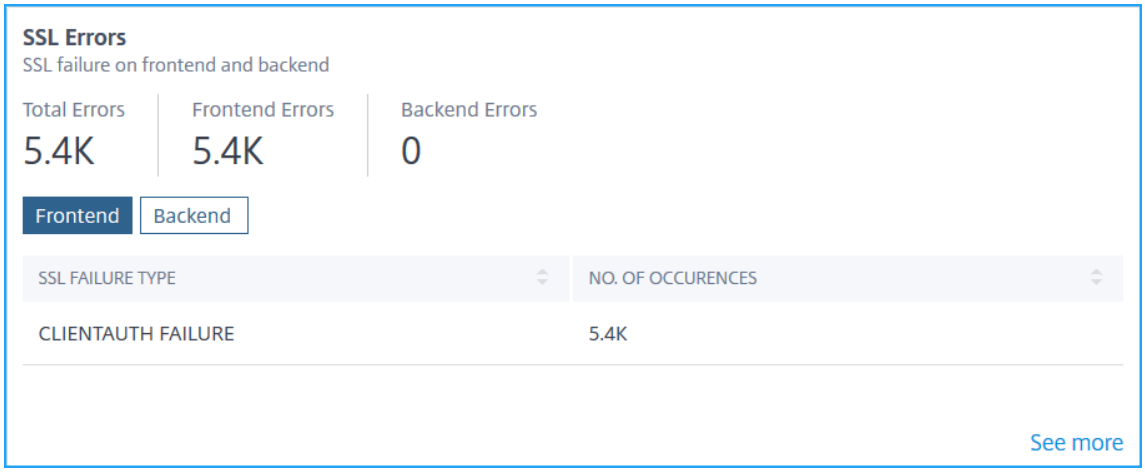
  - **Heure de chargement** : affiche le temps total nécessaire à chaque système d'exploitation pour charger à partir du serveur.

- **Navigateurs** : affiche les informations relatives aux types de navigateur utilisés par les clients pour accéder à l'application.



  - **Demandes** : affiche le nombre total de demandes provenant de chaque navigateur.
  - **Bande passante** : affiche la bande passante totale consommée par chaque navigateur.
  - **Temps de chargement** : affiche le temps total nécessaire au chargement d'un navigateur à partir du serveur.

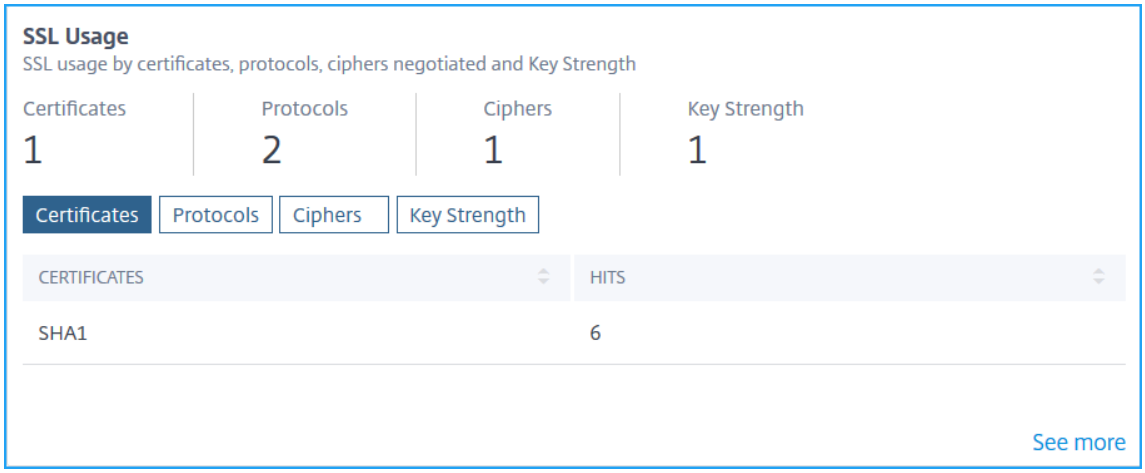
- **Erreurs SSL** — Affiche les informations relatives aux erreurs SSL provenant du serveur frontal et du serveur back-end.



  - **Nombre total d'erreurs** : affiche le total des occurrences d'erreur SSL.
  - **Frontend** — Affiche le total des erreurs SSL du serveur frontal. Cliquez sur l'onglet **Frontend** pour afficher le type d'erreur SSL et le nombre total d'occurrences.

  - **Backend** — Affiche le total des erreurs SSL du serveur principal. Cliquez sur l'onglet **Backend** pour afficher le type d'erreur SSL et le nombre total d'occurrences.

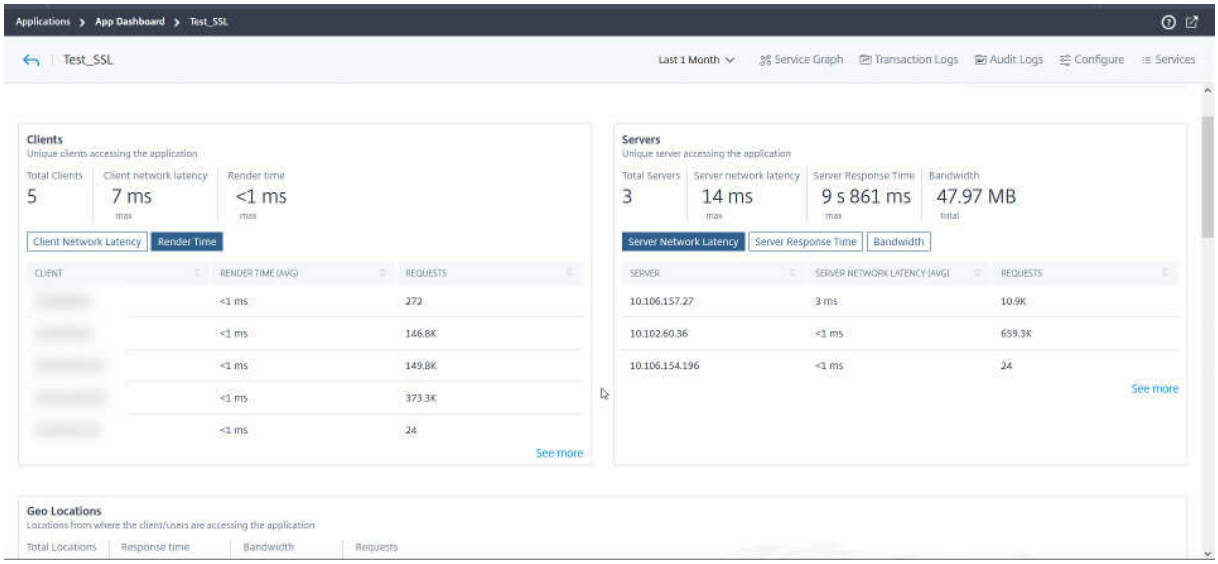
- **Utilisation de SSL** : affiche les informations relatives à l'utilisation du protocole SSL, telles que les certificats SSL, les protocoles, les chiffrements et la force de clé.



  - **Certificats** : affiche le nombre total de certificats SSL. Cliquez sur l'onglet **Certificats** pour afficher le nom du certificat et le nombre total de succès.
  - **Protocoles** : affiche le total des protocoles SSL. Cliquez sur l'onglet **Protocoles** pour afficher les détails avec le protocole SSL/TSL et le nombre total de succès.
  - **Ciphers** : affiche le nombre total de chiffrements. Cliquez sur l'onglet **Ciphers** pour afficher les détails de chaque nom de suite de chiffrement et le nombre total de succès.
  - **Force clé** : affiche la force de clé totale utilisée dans les certificats SSL. Cliquez sur l'onglet **Force clé** pour afficher les détails de chaque force clé et nombre total de coups.

Afficher les détails des mesures au format graphique

Pour chaque mesure, vous pouvez afficher plus de détails dans un format graphique en cliquant sur l'option **Voir plus**. Cliquez sur ** pour afficher les détails dans un format graphique.



Voici les détails que vous pouvez afficher pour chaque mesure après avoir cliqué sur l'option **Voir plus** :

Nom Insight	Mesures	Description
—-	—-	—-
Clients	Clients	Indique la liste des clients
	Temps de rendu (AVG)	Indique le temps moyen nécessaire au client pour rendre la réponse du serveur
	Latence réseau client (AVG)	Indique la latence réseau moyenne du client vers l'instance Citrix ADC
	Demandes	Indique le nombre total de demandes du client
Serveurs	Serveur	Indique la liste des serveurs
	Temps de traitement du serveur (AVG)	Indique le temps moyen nécessaire au serveur pour traiter les requêtes
	Latence réseau serveur (AVG)	Indique la latence réseau moyenne entre le serveur et l'instance Citrix ADC
	Accès	Indique le nombre total d'accès reçus par le serveur
Emplacements géographiques	Emplacements	Indique les emplacements du client
	Temps de réponse	Indique le temps de réponse total à partir de l'emplacement du client
	Bande passante	Indique la bande passante totale consommée à partir de l'emplacement
	Demandes	Indique le nombre total de demandes provenant de l'emplacement
URL	Temps de rendu (AVG)	Indique le temps moyen de chargement de la page à partir du serveur
	Temps de chargement (AVG)	Indique le temps moyen nécessaire pour le rendu et l'affichage de l'URL
	Accès	Indique le nombre total d'accès de l'URL
État de la réponse HTTP	Nom	Indique le nom d'état de la réponse tel que OK, Introuvable, Erreur interne du serveur, etc.
	État de la réponse	Indique le code d'état de réponse reçu du serveur tel que 200, 400, 500, etc.

	Accès	Indique le nombre total d'accès du code de réponse
	Bande passante	Indique la bande passante totale consommée
OS	OS	Indique le nom du système d'exploitation tel que Windows, MAC
	Temps de chargement	Indique le temps total nécessaire au chargement du système d'exploitation à partir du serveur
	Bande passante	Indique la bande passante totale consommée par le système d'exploitation
	Demandes	Indique le nombre total de demandes provenant du système d'exploitation
Navigateurs	Navigateurs	Indique le nom du navigateur tel que Mozilla Firefox, Chrome, etc.
	Temps de chargement	Indique le temps total nécessaire au chargement d'un navigateur à partir du serveur
	Bande passante	Indique la bande passante totale consommée par le navigateur
	Demandes	Indique le nombre total de demandes du navigateur
Erreurs SSL	Type de défaillance SSL	Indique le nom de l'erreur tel que CLIENTAUTH FAILURE
	Occurrences	Indique le nombre total d'occurrences pour l'erreur SSL
Utilisation SSL	Indique le nom du protocole et les versions telles que TLS, SSL
	Hits	Désigne le nombre total d'accès du protocole

Pour plus d'informations sur les cas d'utilisation Web Insight, reportez-vous à la section Web Insight.

Résoudre les problèmes liés au tableau de bord

April 29, 2021

Après avoir ajouté une application dans le Tableau de bord des applications, le tableau de bord affiche immédiatement les détails de configuration de base de l'application. Les détails de l'analyse des applications tels que le score de l'application, les mesures clés et les problèmes commencent à être remplis en quelques minutes (environ 10 à 15 minutes). Pour de plus amples informations, consultez la section Applications.

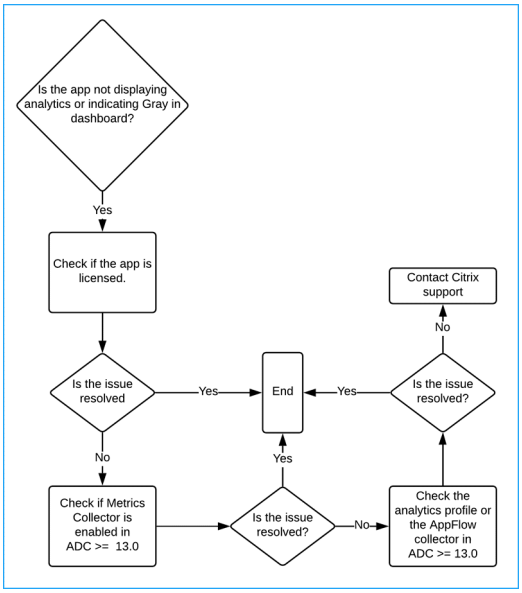
Vous devez vous assurer qu'il n'y a aucun problème avec le flux de données des métriques (collecteur AppFlow ou profil Analytics) à partir de l'instance Citrix ADC. Vous pouvez obtenir plus d'informations sur le collecteur AppFlow et le profil analytique dans ce document.

Ce document décrit les étapes de dépannage que vous devez effectuer lorsque :

- Si vous cliquez sur une application, les analyses de l'application sélectionnée n'affichent pas les données requises même après la durée mentionnée (10 à 15 minutes).
- L'application CS ou LB indique toujours la couleur grise (statut**Non applicable**) dans le Tableau de bord de l'application.

> **Remarque**
>
> Les procédures de dépannage mentionnées dans ce document ne s'appliquent qu'aux serveurs virtuels de **commutation de contenu** et d' **équilibrage de charge**.

Scénario de dépannage



L'application est sous licence

Vous devez vous assurer que l'application est autorisée.

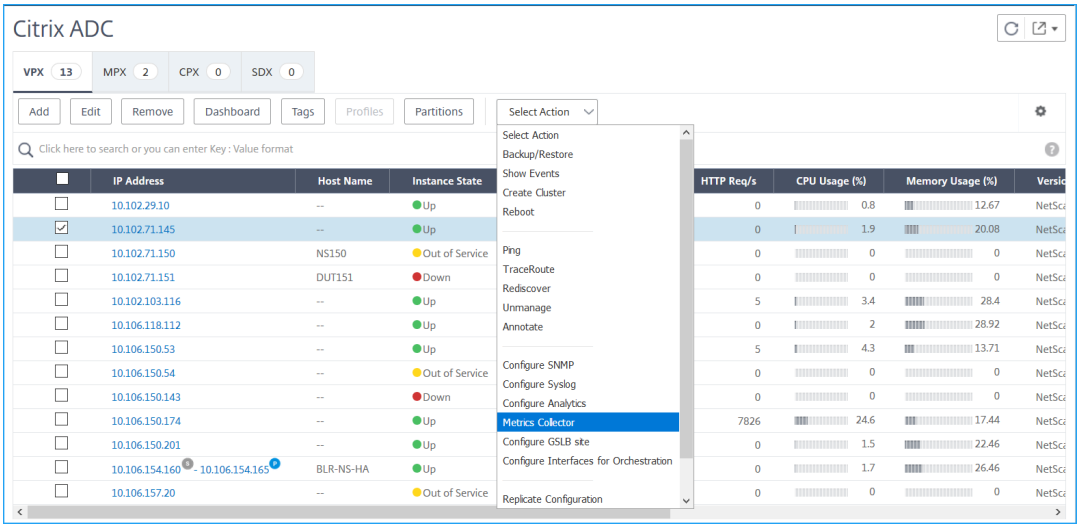
- **Service ADM** - Accédez à **Compte > Abonnements** et vérifiez si l'application est sous licence **Virtual Server License Summary**. Si l'application n'est pas sous licence, reportez-vous à la section Gérer les licences et activer les analyses sur les serveurs virtuels pour concéder une licence au serveur virtuel.
- **ADM sur site —** Accédez à **Système > Licensing & Analytics** et vérifiez si l'application est sous licence **Virtual Server License Summary**. Si l'application n'est pas sous licence, reportez-vous à la section Gérer les licences et activer les analyses sur les serveurs virtuels pour concéder une licence au serveur virtuel.

Le collecteur de mesures est activé

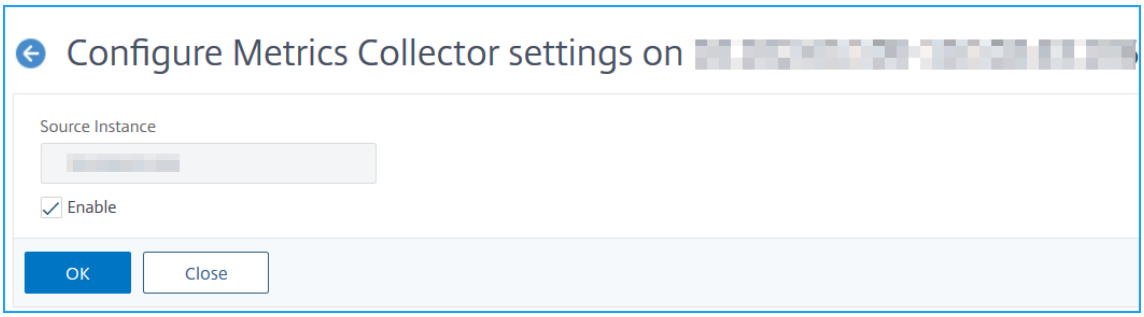
Vous devez vous assurer que **Metrics Collector** est activé dans l'instance Citrix ADC.

Pour Citrix ADC version 13.0 ou ultérieure, Metrics Collector est activé par défaut, une fois l'instance ADC ajoutée avec succès dans ADM. Pour vous assurer que le collecteur de mesures est activé :

1. Accédez à **Réseaux > Instances**. Sous Instances, sélectionnez le type d'instance (par exemple, Citrix ADC VPX).
2. Sélectionnez l'instance de Citrix ADC.
   a) **Dans la liste Sélectionner une action**, sélectionnez **Collecteur de mesures** .



3. Dans la page **Configurer les paramètres du collecteur** de mesures, vérifiez si l'option **Activer** est sélectionnée. Si ce n'est pas le cas, sélectionnez l'option **Activer** et cliquez sur **OK** .



Après avoir activé le collecteur de mesures et si vous n'êtes toujours pas en mesure d'afficher les données, validez :

- Le Collecteur AppFlow dans l'instance de Citrix ADC version 13.0 **antérieure à 47.x build**.
- Le profil analytique dans l'instance de Citrix ADC build **47.x ou version ultérieure**.

Conversion antérieure de l'instance Citrix ADC

Dans Citrix ADC :

1. Exécutez la commande suivante pour vous assurer que le collecteur est **UP** et s'exécute sur le port 5563 :

```
sh appflow collector af_collector_rest_<adm_receiver_ip>
```

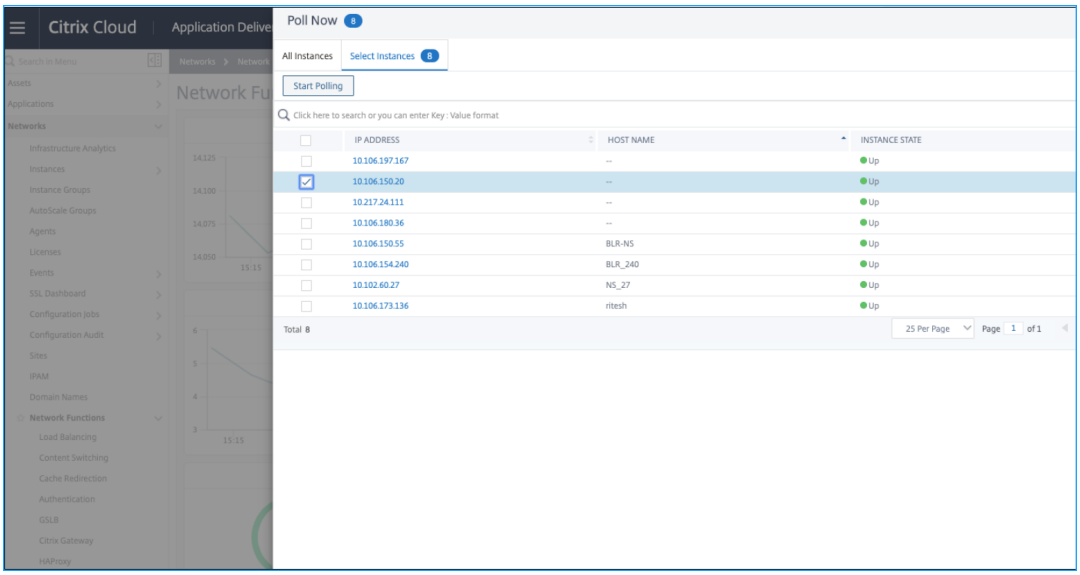


```
> sh appflow collector af_collector_rest_10.102.103.114
1) Name: af_collector_rest_10.102.103.114
IPv4 address: 10.102.103.114
Port: 5563
Netprofile:
Transport: rest
State: UP
Done
```

2. Si aucun collecteur n'est disponible, effectuez une interrogation manuelle d'instance dans Citrix ADM.

   a) Accédez à **Réseaux > Fonction réseau > Sondage maintenant**

   b) Sélectionnez l'instance et cliquez sur **Démarrer l'interrogation**.



   Si l'interrogation échoue, supprimez l'instance ADC d'ADM, puis ajoutez à nouveau l'instance ADC. Lorsque vous ajoutez l'instance ADC, le collecteur est ajouté sur ADC.

Si le collecteur indique l'état **Down** :

1. Vérifiez si SNIP est configuré.

```
> sh ip | grep SNIP
2)  10.106.150.34    0              SNIP            Active   Enabled  Enabled  NA      Enabled
```

   Si SNIP n'est pas configuré, vous devez configurer SNIP. Pour de plus amples informations, consultez la section Configuration de SNIP.

2. Assurez-vous que si l'instance ADC est accessible à ADM.

Vous pouvez valider en effectuant un test ping. Exécutez `ping -S <SNIP> <adm_receiver_ip>`.

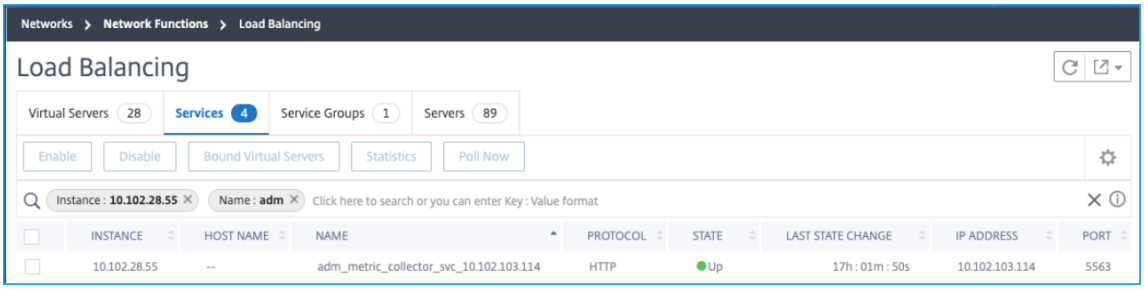
```
> ping -S 10.106.150.34 10.102.103.114
PING 10.102.103.114 (10.102.103.114) from 10.106.150.34: 56 data bytes
64 bytes from 10.102.103.114: icmp_seq=0 ttl=62 time=0.770 ms
64 bytes from 10.102.103.114: icmp_seq=1 ttl=62 time=0.446 ms
64 bytes from 10.102.103.114: icmp_seq=2 ttl=62 time=0.402 ms
```

Instance Citrix ADC versions ultérieures

Dans Citrix ADM, assurez-vous que le service collecteur de mesures est disponible :

1. Accédez à **Réseaux > Fonction réseau > Équilibrage de charge > Services**.
2. Dans la barre de recherche, filtrez par **instance : (adresse IP)** et **Nom : ADM**.
3. Vérifiez si `adm_metric_collector_svc_<adm_receiver ip>` est disponible. L'adresse IP peut être l'adresse IP de gestion ADM ou l'adresse IP de l'agent.

   Assurez-vous que ce service est en état **UP** et s'exécute sur le port 5563.



Si vous ne pouvez toujours pas afficher les données, assurez-vous que le service collecteur est lié au profil d'analyse de séries chronologiques dans Citrix ADC.

1. Connectez-vous à Citrix ADC
2. Exécutez la commande suivante :

   ```
   sh analytics profile ns_analytics_time_series_profile
   ```



```
> sh analytics profile ns_analytics_time_series_profile
1)  Name: ns_analytics_time_series_profile
    Collector: adm_metric_collector_svc_10.102.103.114
    Profile-type: timeseries
        Output Mode: avro
        Metrics: ENABLED
        Events: ENABLED
        Auditlog: DISABLED
    Reference Count: 0
 Done
```

Si le collecteur indique l'état **Down** :

1. Vérifiez si SNIP est configuré.

   ```
   > sh ip | grep SNIP
   2)  10.106.150.34    0             SNIP           Active   Enabled  Enabled  NA       Enabled
   ```

   Si SNIP n'est pas configuré, vous devez configurer SNIP. Pour de plus amples informations, consultez la section Configuration de SNIP.

2. Assurez-vous que si l'instance ADC est accessible à ADM.

   Vous pouvez valider en effectuant un test ping. Exécutez `ping -S <SNIP> <adm_receiver_ip>`.

   ```
   > ping -S 10.106.150.34 10.102.103.114
   PING 10.102.103.114 (10.102.103.114) from 10.106.150.34: 56 data bytes
   64 bytes from 10.102.103.114: icmp_seq=0 ttl=62 time=0.770 ms
   64 bytes from 10.102.103.114: icmp_seq=1 ttl=62 time=0.446 ms
   64 bytes from 10.102.103.114: icmp_seq=2 ttl=62 time=0.402 ms
   ```

3. Assurez-vous que la connectivité du trafic via telnet est capable de connecter le service.

   ```
   root@ns# telnet 10.102.103.114 5563
   Trying 10.102.103.114...
   Connected to 10.102.103.114.
   Escape character is '^]'.
   ^]
   telnet> q
   Connection closed.
   ```

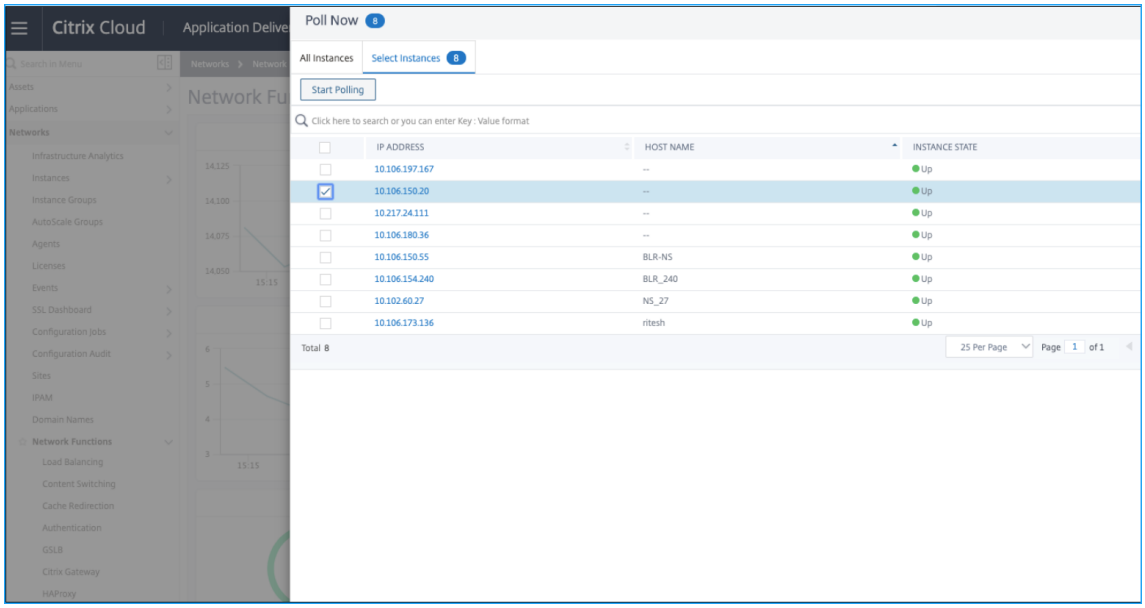
   Si telnet est capable de connecter le service, un pare-feu existe et bloque le flux de données de mesure. Vous devez résoudre le problème de blocage du pare-feu.

Si aucun service de collecteur n'est lié au profil analytique de séries chronologiques dans Citrix ADC, le collecteur s'affiche comme vide.

```
> sh analytics profile ns_analytics_time_series_profile
1)  Name: ns_analytics_time_series_profile
    Collector:
    Profile-type: timeseries
        Output Mode: avro
        Metrics: ENABLED
        Events: ENABLED
        Auditlog: DISABLED
    Reference Count: 0
 Done
```

Vous devez effectuer une interrogation manuelle d'instance dans Citrix ADM.

1. Accédez à **Réseaux > Fonction réseau > Sondage maintenant**
2. Sélectionnez l'instance et cliquez sur **Démarrer l'interrogation**.



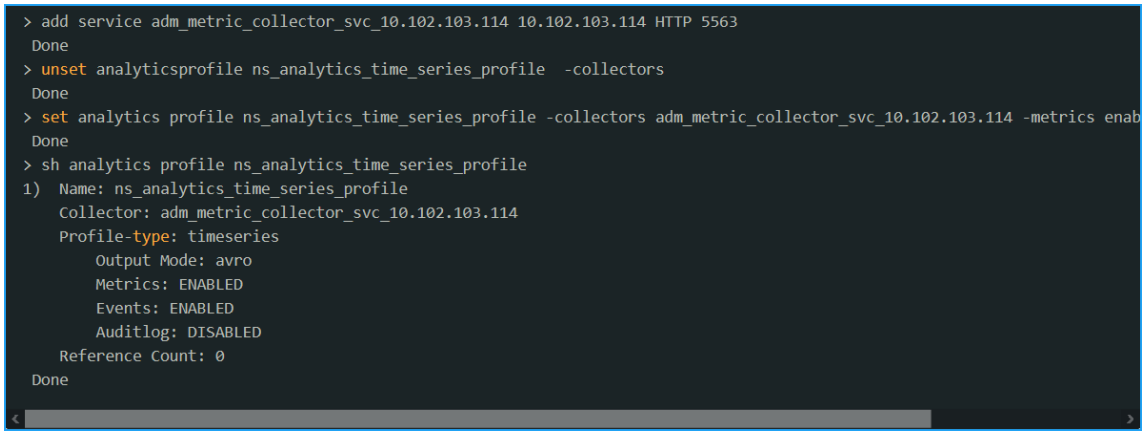
Si l'interrogation échoue, ajoutez le service collector directement à l'instance Citrix ADC à l'aide des commandes suivantes :

```
add service adm_metric_collector_svc_<adm_receiver_ip> <adm_receiver_ip
> HTTP 5563
```

```
unset analyticsprofile ns_analytics_time_series_profile -collectors
```

```
set analytics profile ns_analytics_time_series_profile -collectors
adm_metric_collector_svc_<adm_receiver_ip> -metrics enabled -events
enabled
```


Le profil des séries chronologiques analytiques est mis à jour.



Si le problème persiste même après avoir effectué toutes les étapes de dépannage mentionnées, contactez le **support Citrix**.

Créer un seuil et une alerte pour l'analyse des applications

April 29, 2021

L'analyse des applications sur Citrix ADM vous permet de surveiller les différents types de trafic passant par les instances Citrix ADC. Citrix ADM vous permet de définir des seuils sur les compteurs suivants pour surveiller le trafic et le score d'application.

Vous pouvez configurer des seuils et surveiller le score de l'application pour le processeur, la mémoire, les défausses de carte réseau et le temps de réponse.

Pour configurer le score d'application dans Citrix ADM :

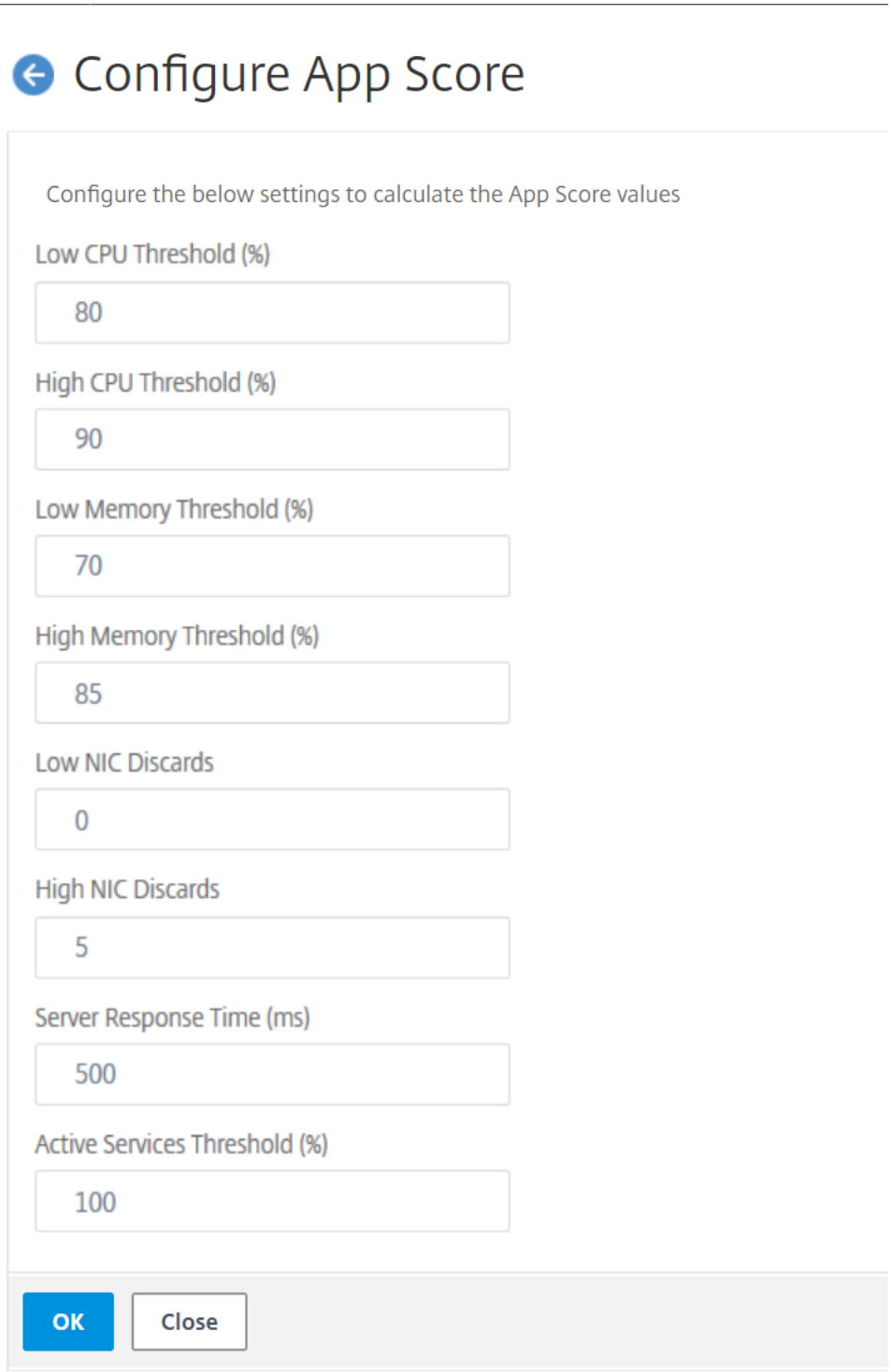
1. Dans Citrix ADM, accédez à **Analytics** > **Paramètres** .
2. Dans la page **Paramètres**, cliquez sur **Configurer le score de l'application**.
3. Sur la page **Configurer le score d'application**, entrez les valeurs des paramètres suivants :
    a) **Seuil CPU faible**. Valeur de seuil inférieure de l'utilisation totale de l'UC dans l'instance de Citrix ADC.
    b) **Seuil CPU élevé**. Valeur de seuil plus élevée de l'utilisation totale de l'UC dans l'instance de Citrix ADC.
    c) **Seuil de mémoire faible**. Valeur de seuil inférieure de l'utilisation totale de la mémoire dans l'instance de Citrix ADC.
    d) **Seuil de mémoire élevé**. Valeur de seuil plus élevée de l'utilisation totale de la mémoire dans l'instance de Citrix ADC.

e) **Faible carte réseau ignore le SLA**. Valeur de seuil inférieure des paquets rejetés par les interfaces.

f) La**carte réseau élevée rejette le SLA**. Valeur de seuil plus élevée des paquets rejetés par les interfaces.

g) **Temps de réponse**. Intervalle de temps entre l'envoi d'un paquet de requête et la réception du premier paquet de réponse du service configuré sur le serveur virtuel. La valeur par défaut configurée dans Citrix ADM est 500 ms.

h) **Seuil des services actifs**. Valeur de seuil du pourcentage de services qui doivent être actifs et liés au serveur virtuel.



4. Cliquez sur **OK**.

Analyse intelligente des applications

April 29, 2021

Intelligent App Analytics vous permet d'identifier les problèmes de performances des applications à l'aide d'algorithmes d'apprentissage automatique et de règles. La fonctionnalité Intelligent App Analytics de Citrix ADM :

- Fournit une solution simple et évolutive pour la surveillance et le dépannage des applications qui sont fournies via des instances Citrix ADC.
- Surveille tous les niveaux d'application afin de réduire les délais de résolution des problèmes et d'améliorer la disponibilité globale de l'application.

Dans un déploiement typique, des milliers de serveurs répondent aux besoins en données des utilisateurs. Le trafic envoyé à ces serveurs est équilibré en charge et surveillé par des serveurs virtuels configurés sur les appliances Citrix ADC. Chaque serveur virtuel est lié à plusieurs services représentant les serveurs back-end. Dans de tels déploiements, la fonctionnalité Intelligent App Analytics vous aide à :

- Surveiller, gérer et prendre des décisions en cas de pannes et d'autres événements
- Surveiller les serveurs virtuels et les services configurés pour une application
- Affichez des informations critiques sur les serveurs et services virtuels, afin de pouvoir modifier les configurations nécessaires pour obtenir des performances optimales des applications.

Accédez à **Application** > **Tableau de bord** et sélectionnez une application à afficher indicateurs de rendement dans la section **Problèmes**.

Configurer Intelligent App Analytics

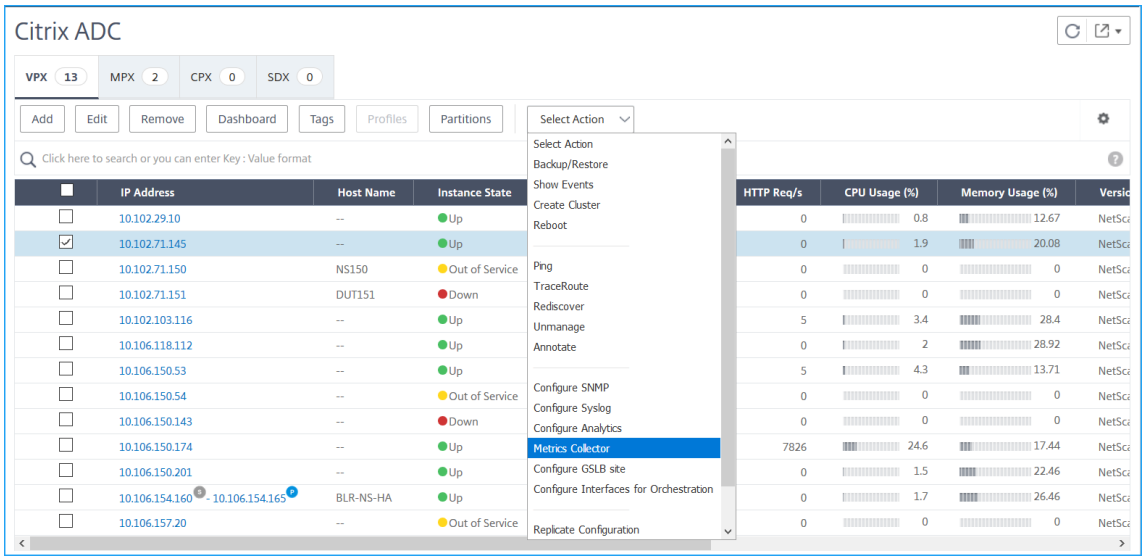
April 29, 2021

La fonctionnalité Intelligent App Analytics est prise en charge uniquement dans **Citrix ADC 12.1 Build 50.28 ou version ultérieure**. Metrics Collector transmet les données de compteur Citrix ADC vers Citrix ADM, qui est utilisé pour détecter les problèmes d'application. Pour utiliser la fonctionnalité Intelligent App Analytics, le **collecteur de mesures** doit être configuré sur chaque instance de Citrix ADC. Par défaut, le Collecteur de mesures est activé sur Citrix ADC, pendant que vous ajoutez l'instance à Citrix ADM.

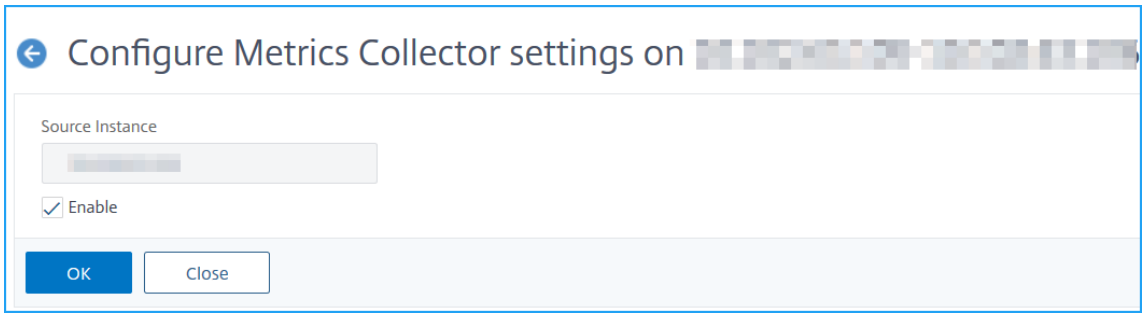
Pour vérifier si le collecteur de mesures est activé :

1. Accédez à **Réseaux > Instances**. Sous **Instances**, sélectionnez le type d'instance à surveiller (par exemple, Citrix ADC VPX).

2. Sélectionnez l'instance de Citrix ADC.
3. **Dans la liste Sélectionner une action**, sélectionnez **Collecteur de mesures** .



4. Dans la page **Configurer les paramètres du collecteur** de mesures, vérifiez si l'option **Activer** est sélectionnée. Si ce n'est pas le cas, sélectionnez l'option **Activer** et cliquez sur **OK** .



Une fois que l'option **Metrics Collector** est activée sur l'instance Citrix ADC, accédez à **Applications** > **Tableau de bord**. Sélectionnez une instance pour afficher les anomalies sous la section **Problèmes**.

Il est également recommandé d'activer l'analyse pour visualiser des problèmes tels que des transactions Web détaillées pour les erreurs de serveur (5xx). Pour de plus amples informations, consultez la section Activer les analyses.

Indicateurs de performance pour l'analyse des applications

April 29, 2021

Vous pouvez afficher les indicateurs de performances, ainsi que les catégories qui se produisent dans

les applications Web Citrix ADC. Pour afficher ces indicateurs, vous devez vous assurer d'activer les analyses et collecteur de mesures sur l'instance ADC :

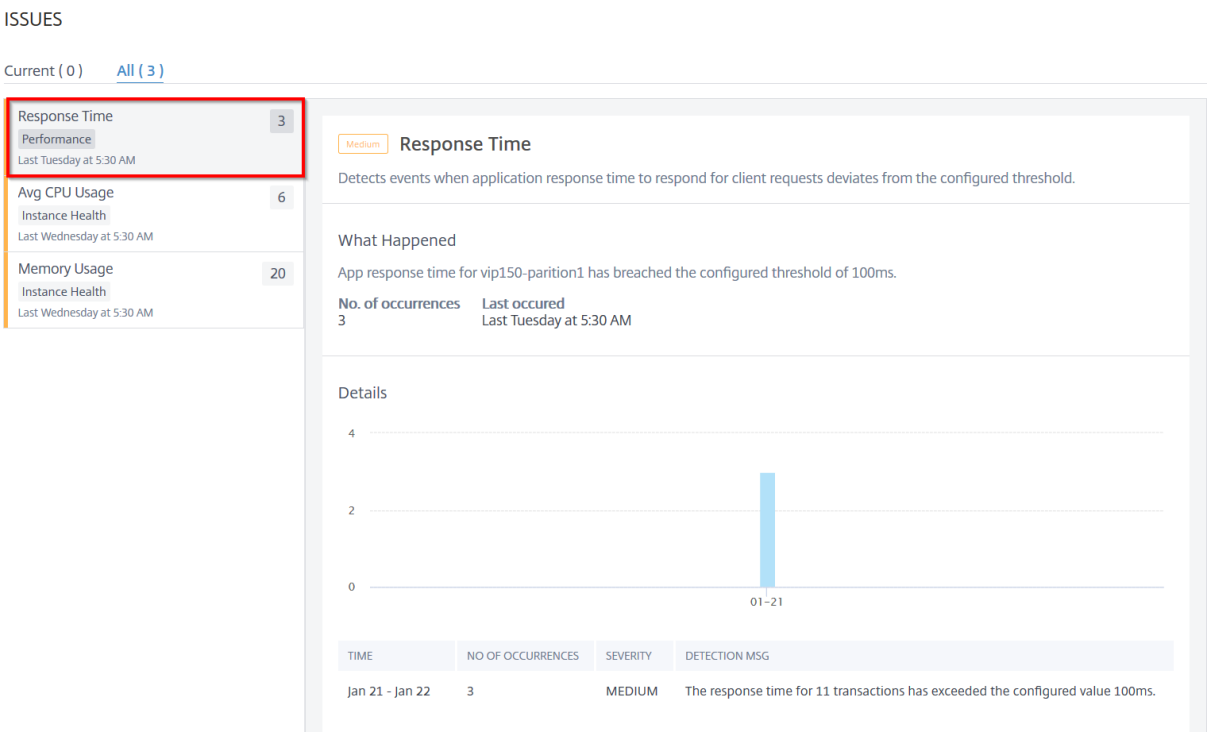
Après avoir activé le collecteur d'analyses et de mesures, vous pouvez afficher les indicateurs suivants en accédant à **Applications** > **Tableau de bord**, en sélectionnant une application et en faisant défiler jusqu'à la section **Problèmes** :

- Temps de réponse
- Services actifs
- Utilisation moyenne de l'UC
- Utilisation de mémoire
- Saturation de la carte réseau
- Volets de service
- Temps de réponse du serveur
- Réutilisation de session faible
- Type de persistance incorrect
- Serveur instable (5xx)
- Trafic en temps réel SSL
- Paquets HTTP exceptionnellement volumineux
- Hits de limite de file d'attente de réassemblage TCP
- Accumulation dans la file d'attente de surtension

Temps de réponse

July 1, 2020

Ce problème détecte lorsque le temps de réponse de l'application pour répondre aux demandes du client s'écarte de la valeur de seuil configurée. Cliquez sur l'onglet **Temps de réponse** pour afficher les détails du problème.



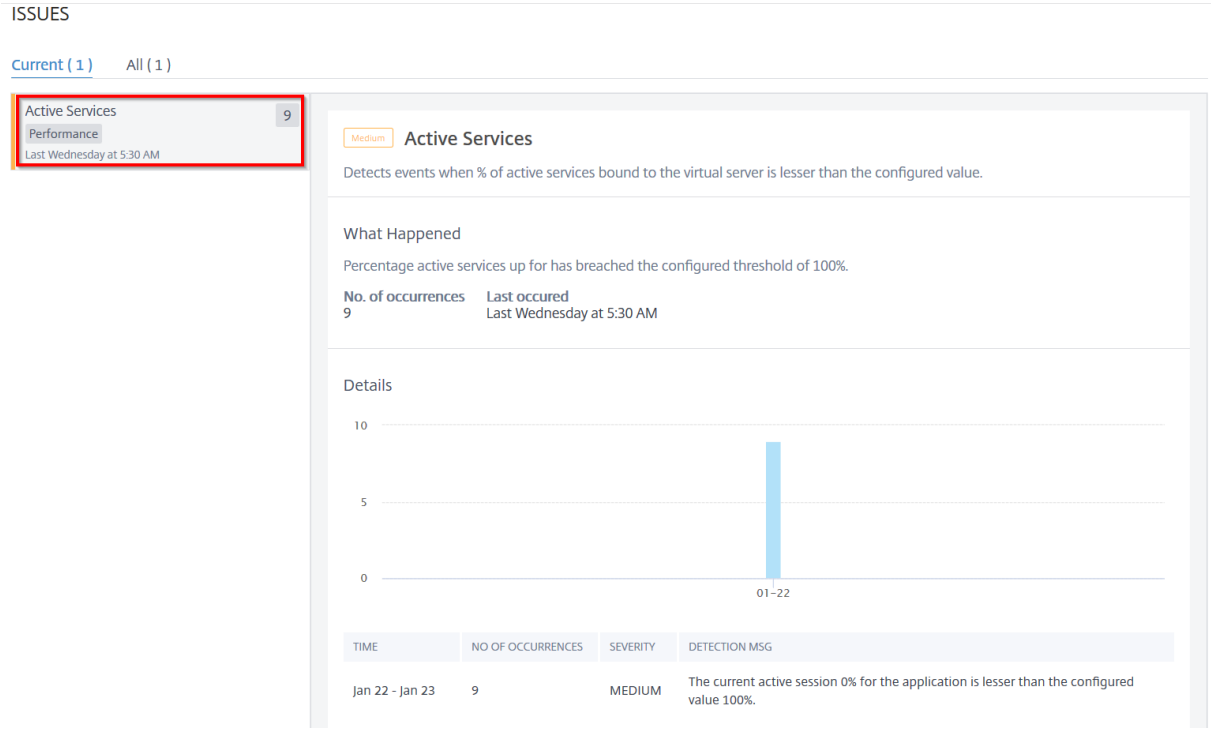
Sous **Détails**, vous pouvez afficher :

- Graphique indiquant le total des événements pour l'heure sélectionnée. Cliquez pour appliquer le filtre et afficher les détails
- Lorsque le problème est survenu
- Nombre total d'occurrences pour l'heure sélectionnée
- La gravité du problème, par exemple faible, moyen et élevé
- Message de détection indiquant le temps de réponse total de la transaction dépassant la valeur de seuil configurée

Services actifs

July 1, 2020

Ce problème détecte lorsque le% des services actifs liés au serveur virtuel est inférieur à la valeur de seuil configurée. Cliquez sur l'onglet **Services actifs** pour afficher les détails du problème.



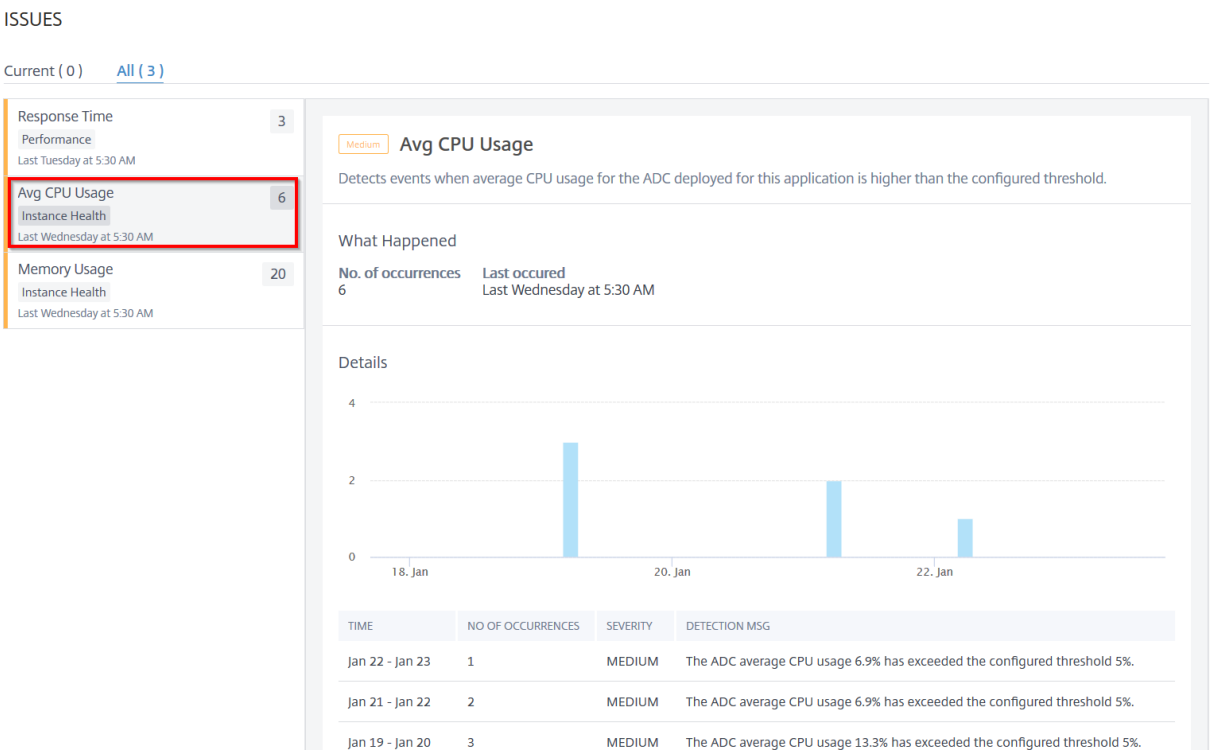
Sous **Détails**, vous pouvez afficher :

- Graphique indiquant le total des événements pour la durée sélectionnée. Cliquez pour appliquer le filtre et afficher les détails
- Lorsque le problème est survenu
- Nombre total d'occurrences pour la durée sélectionnée
- La gravité du problème, par exemple faible, moyen et élevé
- Message de détection indiquant le% de sessions de service actives et la valeur de seuil configurée

Utilisation moyenne de l'UC

July 1, 2020

Ce problème détecte lorsque l'utilisation du processeur ADC pour cette application dépasse la valeur de seuil configurée. Cliquez sur l'onglet **Utilisation moyenne de l'UC** pour afficher les détails du problème.



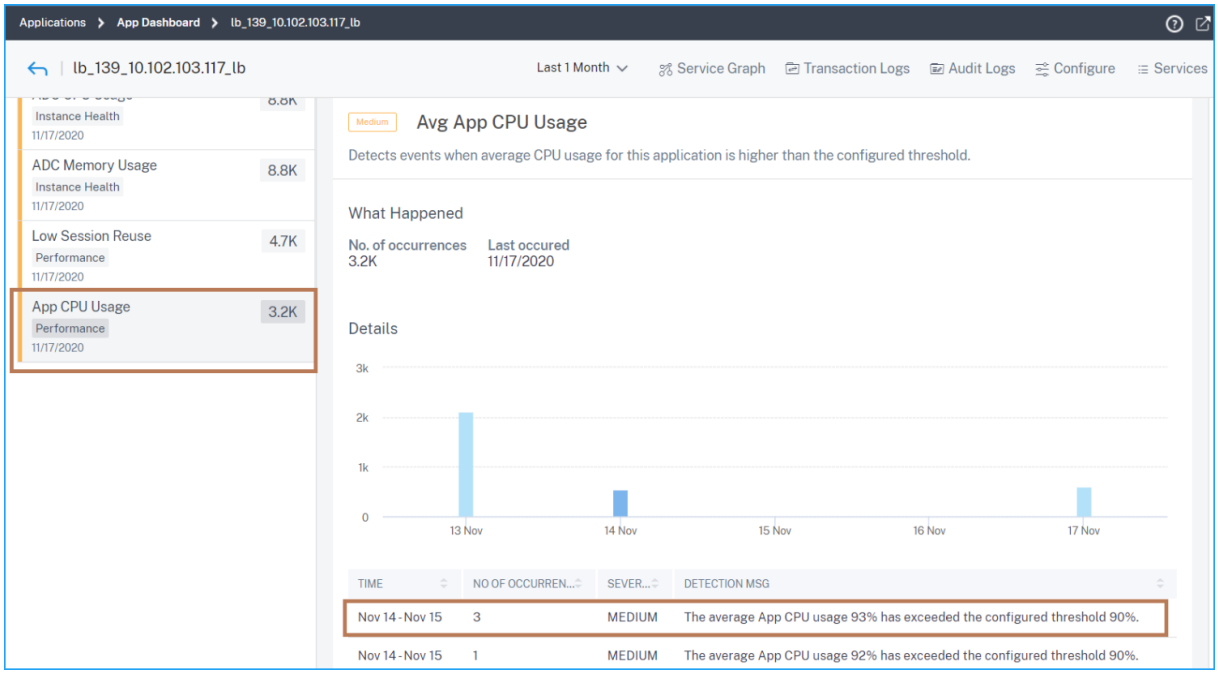
Sous **Détails**, vous pouvez afficher :

- Graphique indiquant le total des événements pour la durée sélectionnée. Cliquez pour appliquer le filtre et afficher les détails
- Lorsque le problème est survenu
- Nombre total d'occurrences pour la durée sélectionnée
- La gravité du problème, par exemple faible, moyen et élevé
- Message de détection indiquant l'utilisation moyenne du processeur ADC (%) et la valeur de seuil configurée

Utilisation moyenne du processeur de l'application

April 29, 2021

Ce problème détecte lorsque l'utilisation du processeur de l'application dépasse la valeur de seuil configurée. Cliquez sur l'onglet **Utilisation du processeur de l'application** pour afficher les détails du problème.



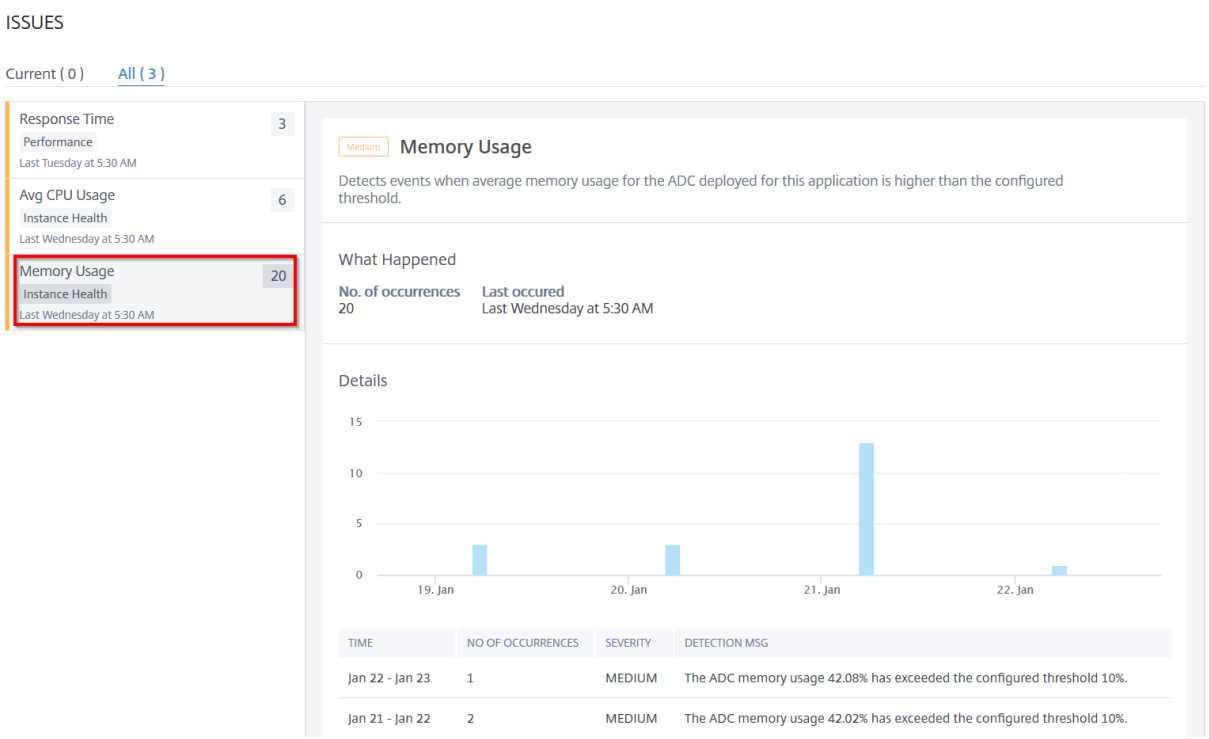
Sous **Détails**, vous pouvez afficher :

- Graphique indiquant le total des événements pour la durée sélectionnée. Cliquez pour appliquer le filtre et afficher les détails
- Lorsque le problème est survenu
- Nombre total d'occurrences pour la durée sélectionnée
- La gravité du problème, par exemple faible, moyen et élevé
- Message de détection indiquant le pourcentage d'utilisation moyenne du processeur de l'application et la valeur de seuil configurée

Utilisation de mémoire

April 29, 2021

Ce problème détecte lorsque l'utilisation de la mémoire ADC pour cette application dépasse la valeur de seuil configurée. Cliquez sur l'onglet **Utilisation de la mémoire** pour afficher les détails du problème.



Sous **Détails**, vous pouvez afficher :

- Graphique indiquant le total des événements pour la durée sélectionnée. Cliquez pour appliquer le filtre et afficher les détails
- Lorsque le problème est survenu
- Nombre total d'occurrences pour la durée sélectionnée
- La gravité du problème, par exemple faible, moyen et élevé
- Message de détection indiquant l'utilisation moyenne de la mémoire ADC (%) et la valeur de seuil configurée

Volets de service

April 29, 2021

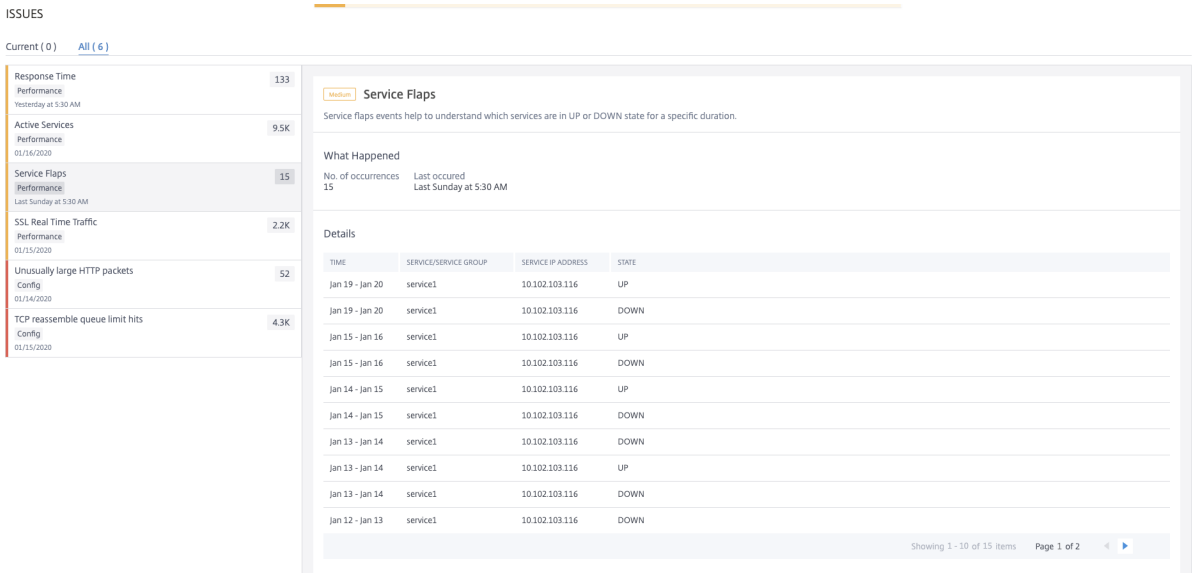
En tant qu'administrateur réseau, vous devez garantir une disponibilité optimale de l'application. En cas de problèmes de réseau ou de configuration, l'état et la disponibilité d'un serveur d'applications peuvent avoir une incidence sur les performances globales.

À l'aide des événements de volets de service, vous pouvez identifier l'application qui a des problèmes. Les événements de volets de service vous aident également à :

- Comprendre quel service est en état DOWN pour une durée spécifique

- Comprendre combien de services sont en état UP ou DOWN pour une durée spécifique

Cliquez sur l'onglet **Volets de service** pour afficher les détails des volets de service.



Vous pouvez afficher des détails tels que le nombre d'occurrences et l'heure de la dernière occurrence.

Sous **Détails**, vous pouvez afficher :

- Heure à laquelle s'est produite l'anomalie des volets de service
- Nom du groupe service/service
- L'adresse IP du service
- L'état actuel du service

Serveur instable

April 29, 2021

Dans certains scénarios, le serveur Web répond avec des codes d'état lorsqu'il est incapable de traiter les demandes pour des raisons telles que des demandes non valides, une surcharge temporaire ou la maintenance du serveur. Ces erreurs sont affichées avec des codes d'erreur, qui définissent différents scénarios des erreurs. Par exemple, les opérations suivantes peuvent être effectuées :

- **502 Passerelle incorrecte**
  Le serveur agit en tant que Gateway ou proxy et a reçu une réponse non valide du serveur en amont.
- **503 Service indisponible**
  Le serveur est actuellement indisponible. Les serveurs peuvent être surchargés ou coupés pour

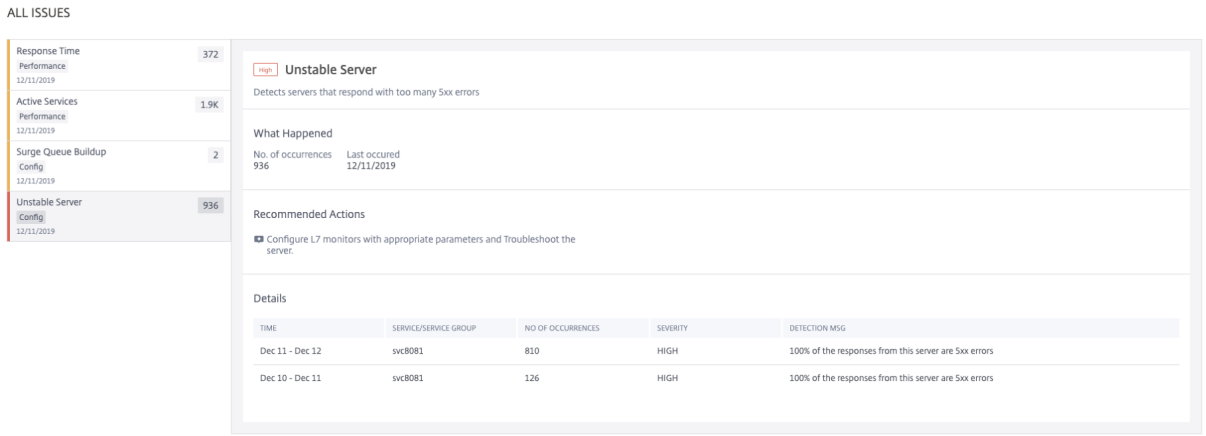
la maintenance.

- **504 Délai d'expiration de la Gateway**Le serveur agit en tant que passerelle ou proxy et n'a pas reçu de réponse en temps opportun du serveur en amont.

Il peut s'agir de conditions temporaires, mais il faut parfois mettre en œuvre une mesure corrective sur les serveurs Web pour rendre les pages Web disponibles.

À l'aide de l'indicateur **Serveur instable**, vous pouvez afficher ces échecs et prendre des décisions sur les mesures correctives pour surmonter les problèmes et vous assurer que les demandes des clients sont traitées et que les pages Web sont toujours disponibles.

Sélectionnez l'onglet **Serveur instable** pour afficher les détails du problème.



Les **actions recommandées** pour résoudre le problème sont les suivantes :

- Configurez les moniteurs L7 avec les paramètres appropriés pour le serveur qui répond par des erreurs 5xx. Un moniteur est une entité qui suit l'intégrité du service. L'appliance sonde périodiquement les serveurs à l'aide du moniteur lié à chaque service. Si un serveur ne répond pas dans un délai de réponse spécifié et que les sondes spécifiées échouent, le service est marqué DOWN. L'appliance effectue ensuite l'équilibrage de la charge entre les services restants. Pour plus d'informations sur la configuration d'un moniteur, voir Moniteurs personnalisés
- Dépannage du serveur

Sous **Détails**, vous pouvez afficher :

- Heure à laquelle s'est produite l'anomalie du serveur instable
- Nom du groupe service/service
- Total des occurrences
- La gravité de l'anomalie telle que élevée, faible et moyenne
- Message de détection indiquant le pourcentage des réponses de ce service signalant des erreurs 5xx

Pour plus d'informations sur la transaction Web d'erreur de serveur, voir Analyse des transactions Web pour les erreurs de serveur

Temps de réponse du serveur

April 29, 2021

La lenteur des applications est une préoccupation majeure pour toute organisation, car elle a un impact sur l'entreprise ou une productivité. En tant qu'administrateur, vous devez vous assurer que toutes les applications fonctionnent de manière optimale afin d'éviter tout impact sur l'entreprise.

Chaque application se comporte différemment et a des attentes de temps de réponse différentes. Lorsque vous disposez d'une batterie de serveurs volumineuse, les administrateurs doivent évaluer chaque application et définir des seuils pour le temps de réponse du serveur.

L'indicateur de **temps de réponse du serveur** aide les administrateurs à évaluer chaque application en fonction de l'algorithme d'apprentissage automatique. Cet indicateur indique :

- Temps de réponse élevé anormal
- Temps de réponse anormal faible

Cliquez sur l'onglet **Temps de réponse du serveur** pour afficher les détails du problème.

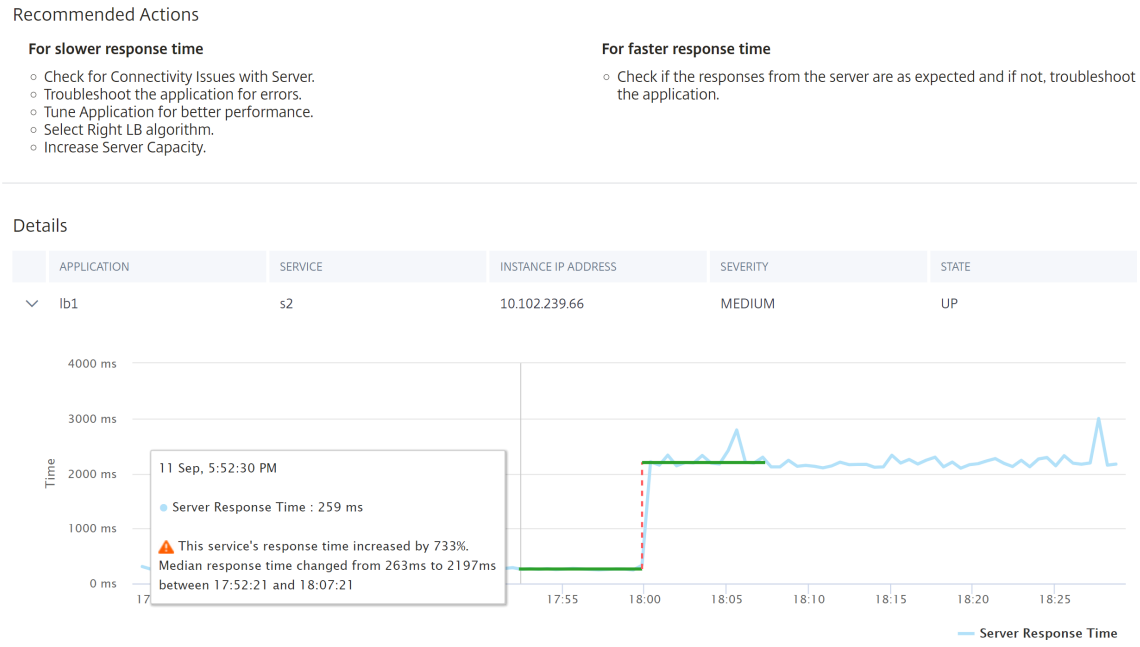
Les **actions recommandées** vous suggèrent de résoudre ces anomalies.

Sous **Détails**, vous pouvez afficher :

- L'application qui a l'anomalie
- Le service lié à l'application
- Adresse IP de l'instance Citrix ADC
- Type de gravité de l'anomalie
- L'état de la demande
- Graphique de temps de réponse du serveur pour la période sélectionnée
- Graphique médian glissant basé sur le temps de réponse du serveur
- Détails de l'anomalie

Citrix ADM détecte des anomalies pour un temps de réponse anormal élevé et un temps de réponse anormal faible.

- **Anomalie pour un temps de réponse anormal élevé du serveur**

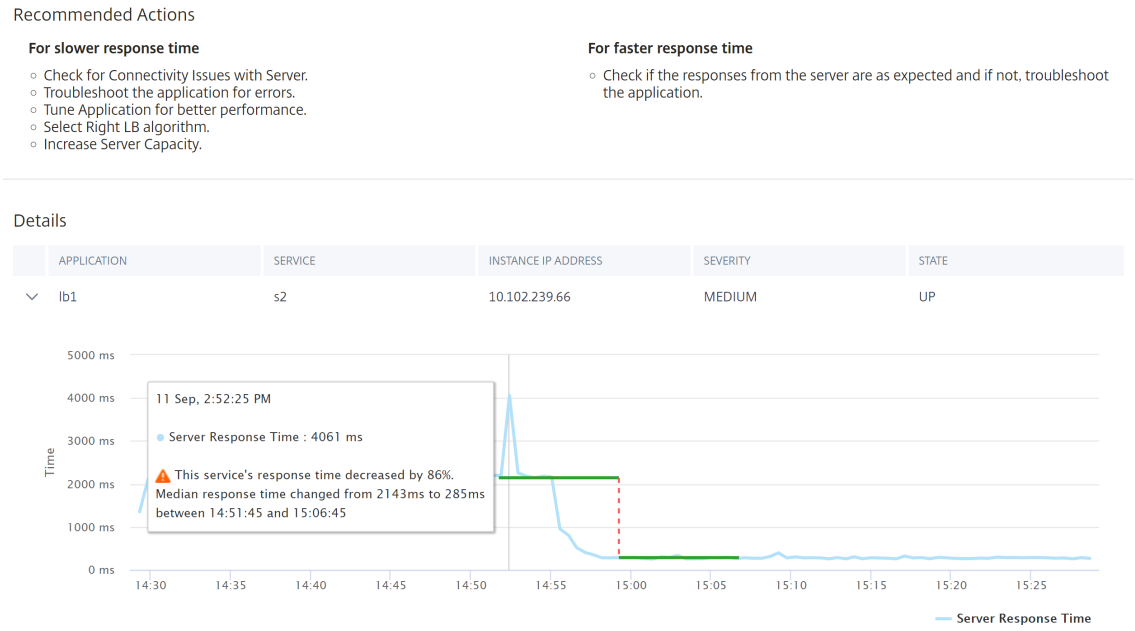


Citrix ADM compare le temps de réponse moyen du serveur pour une durée spécifique. Conformément à l'exemple illustré dans l'image, Citrix ADM compare le temps de réponse moyen du serveur entre 17:50 et 18:20.

Lorsque le temps de réponse du serveur commence à augmenter, Citrix ADM surveille davantage le temps de réponse du serveur pour une autre durée spécifique, puis détecte une anomalie pour le moment où le temps de réponse du serveur a commencé à augmenter.

Selon l'exemple illustré dans l'image, vous pouvez voir une anomalie a été détectée, mentionnant que le temps de réponse du serveur est augmenté de 733%, après avoir comparé le temps de réponse moyen du serveur entre 17:52 et 18:07.

- **Anomalie pour un temps de réponse anormal faible du serveur**



Citrix ADM compare le temps de réponse moyen du serveur pour une durée spécifique. Conformément à l'exemple illustré dans l'image, Citrix ADM compare le temps de réponse moyen du serveur entre 14:51 et 15:06.

Lorsque le temps de réponse du serveur commence à diminuer, Citrix ADM surveille davantage le temps de réponse du serveur pour une autre durée spécifique, puis détecte une anomalie pour le moment où le temps de réponse du serveur a commencé à diminuer.

Selon l'exemple illustré dans l'image, vous pouvez voir une anomalie a été détectée, mentionnant que le temps de réponse du serveur est diminué de 86%, après avoir comparé le temps de réponse moyen du serveur entre 14:51 et 15:06.

Construction de session

April 29, 2021

Pour toutes les transactions sécurisées, Citrix ADC effectue le processus de déchargement SSL pour la première transaction, puis stocke la session SSL en fonction de la configuration de la **réutilisation de session** .

Selon le taux de trafic, il y a une possibilité d'accumulation de session sur une période de temps, ce qui peut entraîner une grande quantité de mémoire étant bloquée par ces sessions dans Citrix ADC.

Les événements d'accumulation de session alertent les administrateurs et fournissent des actions recommandées pour résoudre cet événement. Cliquez sur l'onglet **Session Buildup** pour afficher les détails du problème

Sous **Détails**, vous pouvez afficher :

- Heure à laquelle s'est produite l'anomalie d'accumulation de session
- Nom du serveur virtuel
- La gravité de l'anomalie telle que élevée, faible et moyenne
- Message indiquant que **X** nombre de sessions SSL disponibles sur le serveur virtuel et actuellement, il y a **Y** nombre de poignées de main SSL par seconde dans la session de délai d'expiration configurée.

L' **action recommandée** pour corriger cette anomalie consiste à réduire le délai d'expiration de la session ou à désactiver la réutilisation de la session. Pour de plus amples informations, consultez la section Délai d'expiration de la session.

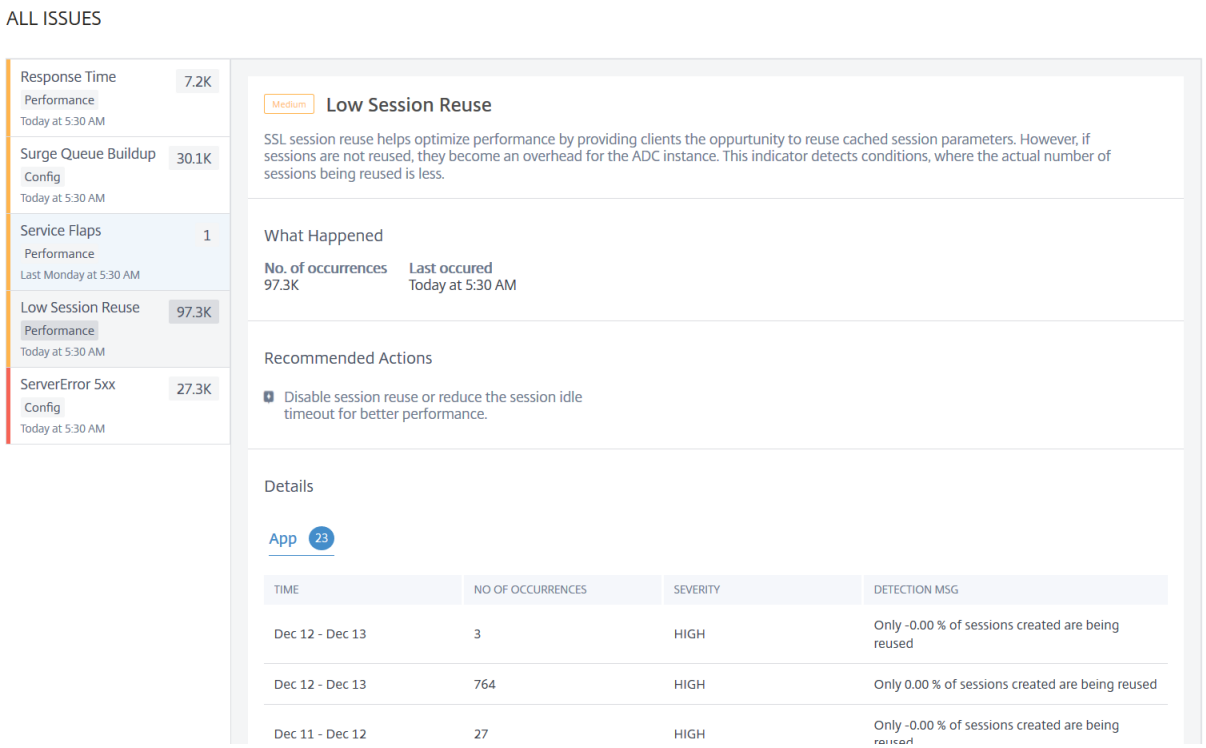
Réutilisation de session faible

April 29, 2021

Les instances Citrix ADC traitent les transactions SSL en déchargeant le processus de connexion SSL du serveur. À la réception de la réponse du serveur, l'instance Citrix ADC termine la transaction sécurisée avec le client. À l'aide des paramètres de session mis en cache, l'instance Citrix ADC termine le processus de handshake SSL pour les demandes consécutives.

Si ces sessions ne sont pas réutilisées, elles deviennent une surcharge pour les instances de Citrix ADC. À l'aide de l'indicateur **Réutilisation de session faible**, vous pouvez identifier si le nombre réel de sessions réutilisées est inférieur.

Cliquez sur l'onglet **Réutilisation de session basse** pour afficher les détails du problème.



L'**action recommandée** pour résoudre le problème consiste à désactiver la réutilisation de la session ou à réduire le délai d'expiration de la session. Pour de plus amples informations, consultez la section Réutilisation de session.

Sous **Détails**, vous pouvez afficher :

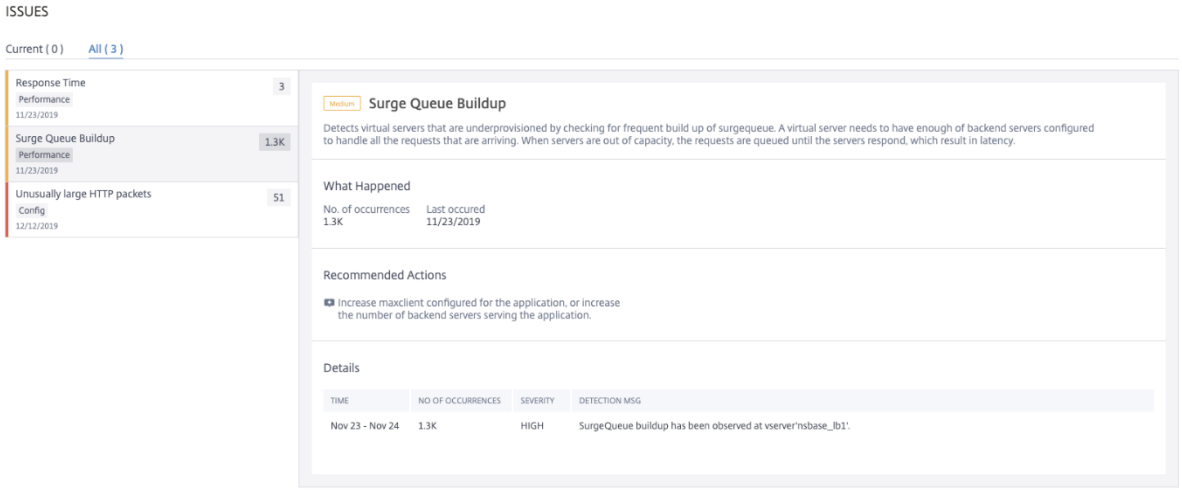
- Nombre total d'applications ayant une réutilisation de session faible
- Heure à laquelle s'est produite l'anomalie de réutilisation de session basse
- Total des occurrences
- La gravité de l'anomalie telle que élevée, faible et moyenne
- Message de détection indiquant que seulement% des sessions configurées sont réutilisées

Accumulation dans la file d'attente de surtension

April 29, 2021

Lorsqu'un serveur reçoit un surnombre de demandes, le serveur devient lent à répondre aux clients. Souvent, la surcharge provoque également les clients à recevoir des pages d'erreur. Un serveur virtuel doit disposer d'un nombre suffisant de serveurs back-end configurés pour gérer les demandes entrantes.

À l'aide de l'indicateur **d'accumulation de files d'attente de surtension**, vous pouvez afficher les serveurs virtuels qui ont accumulé de la file d'attente de surtension. Cliquez sur l'onglet Configuration de la **file d'attente de surtension** pour afficher les détails du problème.



Les **actions recommandées** pour résoudre le problème sont les suivantes :

- Augmentez la limite du nombre de connexions client. Pour de plus amples informations, consultez Définir une limite sur le nombre de connexions client
- Augmenter les serveurs back-end pour répondre aux demandes d'application

Sous **Détails**, vous pouvez afficher :

- Heure à laquelle s'est produite l'anomalie d'accumulation de la file d'attente de surtension
- Total des occurrences
- La gravité de l'anomalie telle que élevée, faible et moyenne
- Message de détection indiquant l'accumulation de files d'attente de surtension sur le serveur virtuel

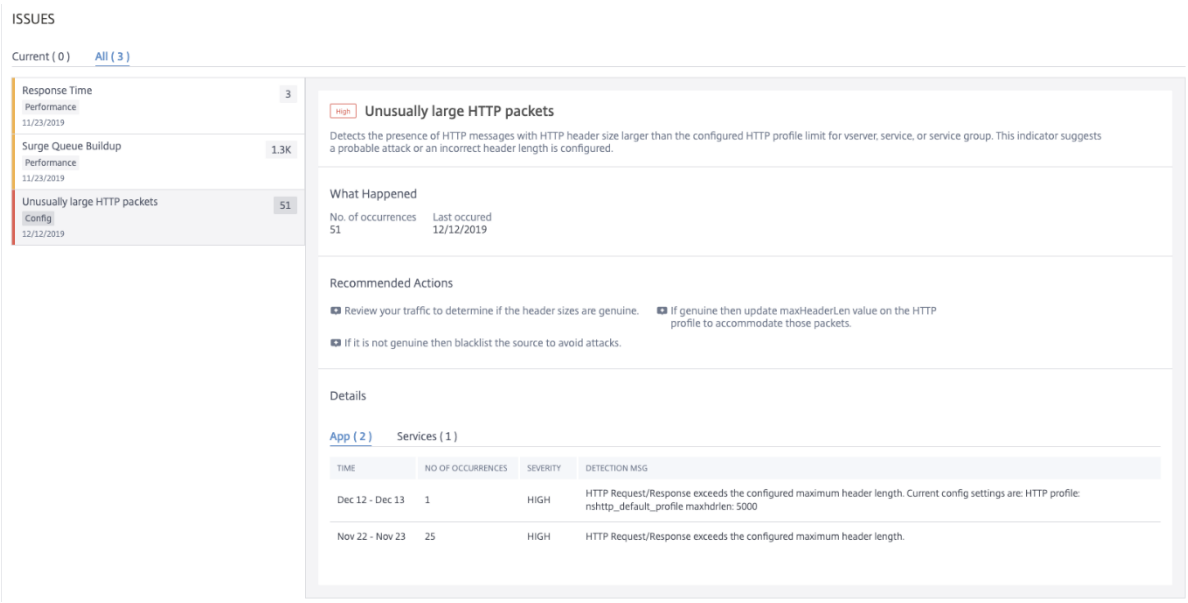
Paquets HTTP exceptionnellement volumineux

April 29, 2021

Une transaction HTTP utilise des messages demande-réponse entre le client et le serveur. Dans les messages de requête et de réponse, les en-têtes HTTP sont les valeurs affichées dans le protocole HTTP. Vous pouvez configurer la longueur d'en-tête HTTP dans un serveur virtuel, un service ou un groupe de services pour éviter les erreurs 4xx.

Lorsqu'une requête/réponse HTTP dépasse la longueur maximale d'en-tête, il peut s'agir d'une attaque possible. À l'aide **de l'indicateur Paquets HTTP de grande** taille, vous pouvez afficher les occurrences où les messages HTTP dont la taille d'en-tête HTTP dépasse les valeurs configurées.

Cliquez sur **l'onglet Paquets HTTP de grande taille** pour afficher les détails du problème.



Les **actions recommandées** pour résoudre le problème sont les suivantes :

- Vérifiez le trafic pour déterminer la taille de l'en-tête est authentique. Si la taille de l'en-tête est authentique, mettez à jour la valeur de l'en-tête sur le profil HTTP. Pour de plus amples informations, consultez la section Vérification du débordement de la mémoire tampon.
- Si la taille de l'en-tête n'est pas authentique, ajoutez la source à la liste de blocage pour éviter les attaques.

Sous **Détails**, vous pouvez afficher :

- L'heure qui s'est produite l'anomalie
- Total des occurrences
- La gravité de l'anomalie telle que élevée, faible et moyenne
- Message de détection indiquant la longueur d'en-tête HTTP actuelle configurée sur le serveur virtuel, le serveur ou le groupe de services

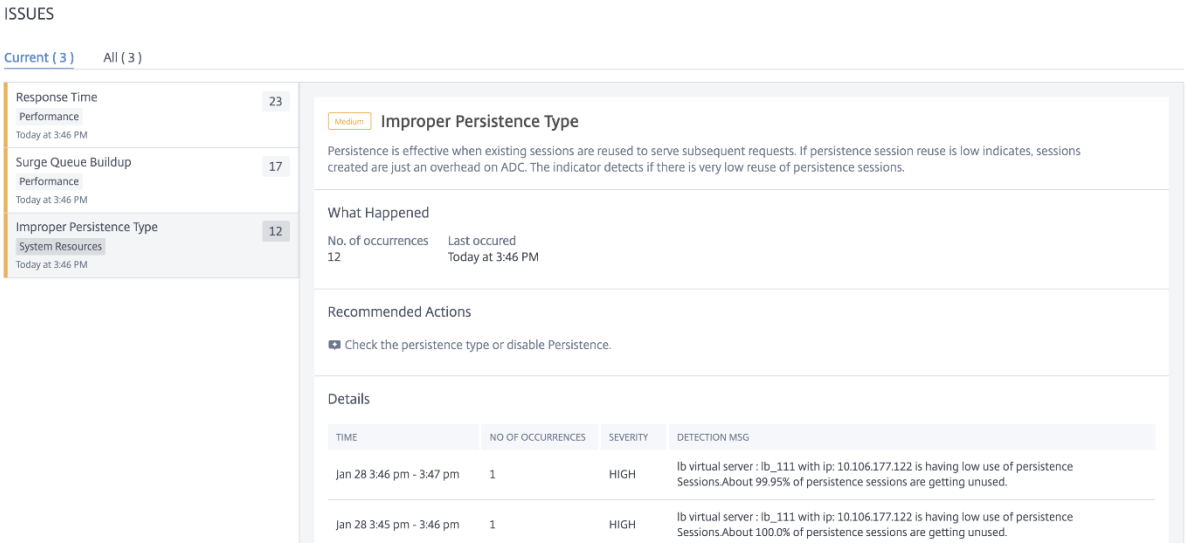
Type de persistance incorrect

April 29, 2021

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

La persistance est efficace lorsque les sessions existantes sont réutilisées pour répondre aux demandes ultérieures. Si la réutilisation des sessions de persistance est faible, les sessions créées sur ADC ne sont qu'une surcharge.

À l'aide de l'indicateur **type de persistance incorrecte**, vous pouvez déterminer si l'utilisation de la persistance sur un serveur virtuel est faible. Cliquez sur l'onglet **Type de persistance incorrecte** pour afficher les détails du problème.



L'**action recommandée** pour résoudre le problème consiste à vérifier le type de persistance ou à désactiver la persistance. Pour de plus amples informations, consultez la section Paramètres de persistance.

Sous **Détails**, vous pouvez afficher :

- L'heure qui s'est produite l'anomalie
- Total des occurrences
- La gravité de l'anomalie telle que élevée, faible et moyenne
- Message de détection indiquant le% de sessions non utilisées

TCP réassembler les hits de limite de file d'attente

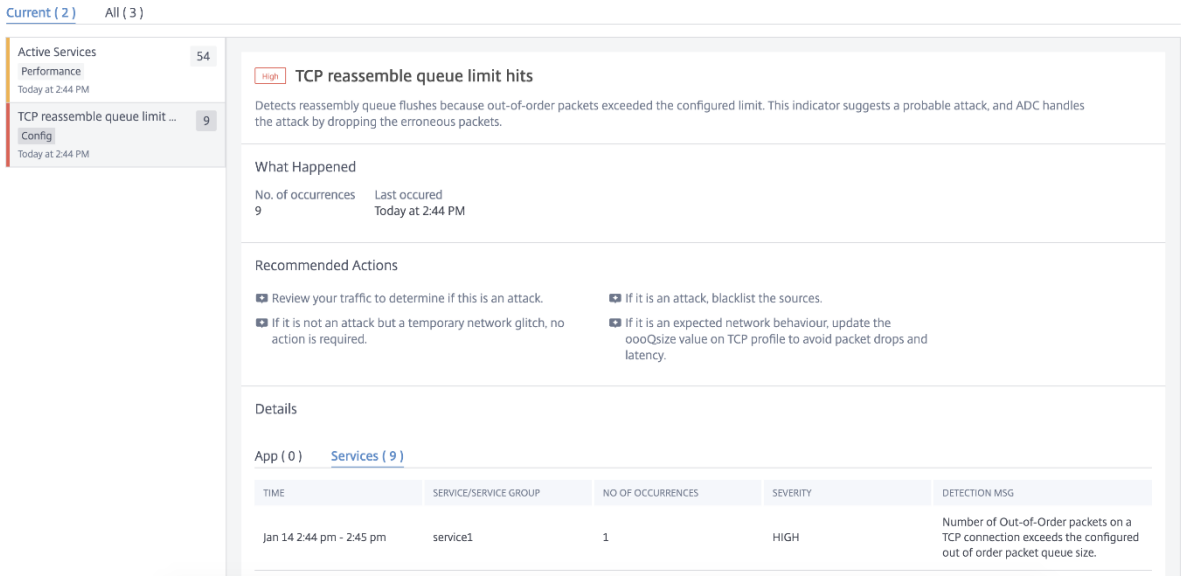
April 29, 2021

TCP maintient une file d'attente hors ordre pour conserver les paquets OOO dans la communication TCP. Ce paramètre affecte la mémoire Citrix ADC si la taille de la file d'attente est longue que les paquets doivent être conservés dans la mémoire d'exécution.

Cela doit être maintenu à un niveau optimisé en fonction du type de caractéristiques du réseau et des applications.

À l'aide de l'indicateur d'accès de **limite de file d'attente de réassemblage TCP**, vous pouvez voir si les paquets hors commande d'une connexion TCP dépassent la taille de file d'attente de paquets hors commande configurée.

Cliquez sur l'onglet **Réassembler les limites de la file d'attente TCP** pour afficher les détails du problème.



Les **actions recommandées** pour résoudre le problème sont les suivantes :

- Vérifiez le trafic et ajoutez la source à la liste de blocage s'il s'agit d'une attaque
- S'il s'agit d'un comportement réseau attendu, mettez à jour la valeur de taille des paquets hors ordre sur le profil TCP. Pour de plus amples informations, consultez Optimisation TCP
- S'il s'agit simplement d'un problème de réseau temporaire, aucune autre action n'est requise

Sous **Détails**, vous pouvez afficher :

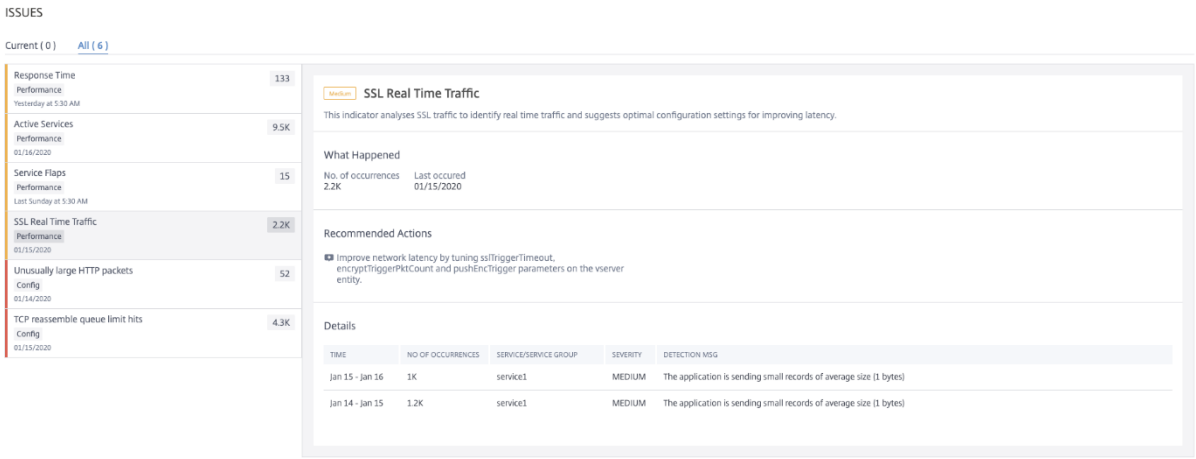
- L'heure qui s'est produite l'anomalie
- Total des occurrences
- La gravité de l'anomalie telle que faible, moyenne et élevée
- Message de détection indiquant le profil TCP actuel et les paramètres OOOQSize

Trafic en temps réel SSL

April 29, 2021

Dans l'instance de Citrix ADC, vous pouvez utiliser un profil SSL pour traiter le trafic SSL. Le profil SSL comprend certains paramètres SSL pour les serveurs virtuels, les services et les groupes de services. L'indicateur de **trafic en temps réel SSL** analyse le trafic SSL pour identifier le trafic en temps réel et suggère des paramètres de configuration optimaux pour améliorer la latence.

Cliquez sur l'onglet **Trafic en temps réel SSL** pour afficher les détails du problème.



L'**action recommandée** pour résoudre le problème consiste à améliorer la latence réseau en mettant à jour les paramètres SSL. Pour de plus amples informations, consultez la section Paramètres SSL globaux.

Sous **Détails**, vous pouvez afficher :

- L'heure qui s'est produite l'anomalie
- Nom du groupe service/service
- La gravité de l'anomalie telle que faible, moyenne et élevée
- Le message de détection avec le paramètre actuel sur l'application

Tableau de bord de la sécurité des applications

April 29, 2021

Le tableau **de bord Sécurité des applications** fournit une vue d'ensemble des mesures de sécurité pour les applications détectées/sous licence. Ce tableau de bord affiche les informations sur les at-

taques de sécurité pour les applications découvertes/sous licence, telles que les attaques de synchronisation, les attaques de petites fenêtres, les attaques DNS par inondation.

Pour afficher les mesures de sécurité sur le tableau de bord de sécurité de l'application :

1. Accédez à **Applications> Tableau de bord de sécurité** des applications.
2. Sélectionnez l'adresse IP de l'instance dans la liste Instance.

   Les rapports contiennent les renseignements suivants pour chaque application :

   - **Indice des menaces**. Système de notation à un chiffre qui indique la criticité des attaques sur l'application. Plus les attaques contre une application sont critiques, plus l'indice de menace pour cette application est élevé. Les valeurs varient de 1 à 7.

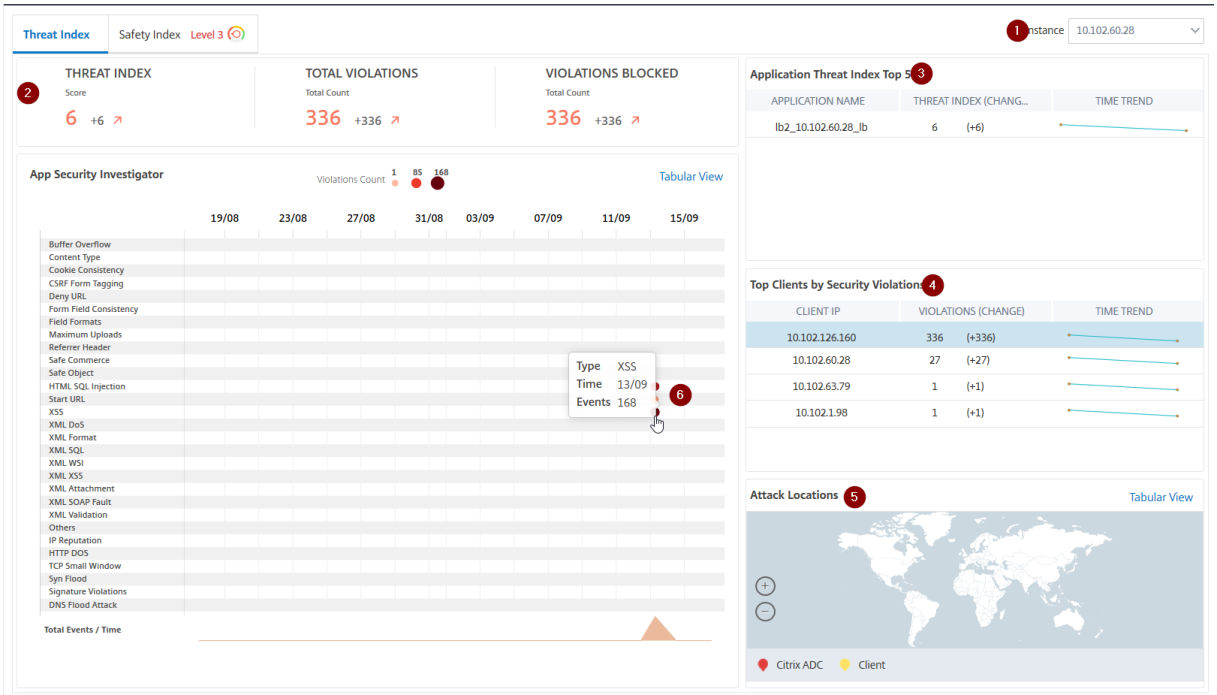
     L'indice des menaces est basé sur les informations d'attaque. Les informations relatives à l'attaque, telles que le type de violation, la catégorie d'attaque, l'emplacement et les détails du client, donnent un aperçu des attaques sur l'application. Les informations de violation sont envoyées à Citrix ADM uniquement lorsqu'une violation ou une attaque se produit. De nombreuses failles et vulnérabilités conduisent à un indice de menace élevé.

   - **Indice de sécurité**. Système de notation à un chiffre qui indique la sécurité avec laquelle vous avez configuré les instances de Citrix ADC pour protéger les applications contre les menaces et vulnérabilités externes. Plus les risques de sécurité pour une application sont faibles, plus l'indice de sécurité est élevé. Les valeurs varient de 1 à 7.

     L'index de sécurité tient compte à la fois de la configuration du pare-feu de l'application et de la configuration de sécurité du système Citrix ADC. Pour un indice de sécurité élevé, les deux configurations doivent être solides. Par exemple, si des vérifications rigoureuses du pare-feu des applications sont en place, mais que les mesures de sécurité du système Citrix ADC, telles qu'un mot de passe fort pour l'utilisateur nsroot, les applications se voient attribuer une valeur d'indice de sécurité faible.

Vous pouvez afficher les écarts signalés sur **App Security Investigator**.

Détails de l’index des menaces



1 - Affiche l’adresse IP de l’instance Citrix ADC pour laquelle vous pouvez afficher les détails.

2 - Affiche des détails tels que le score d’index des menaces, le nombre total de violations survenues et le nombre total de violations bloquées.

3 - Affiche le serveur virtuel de l’instance sélectionnée.

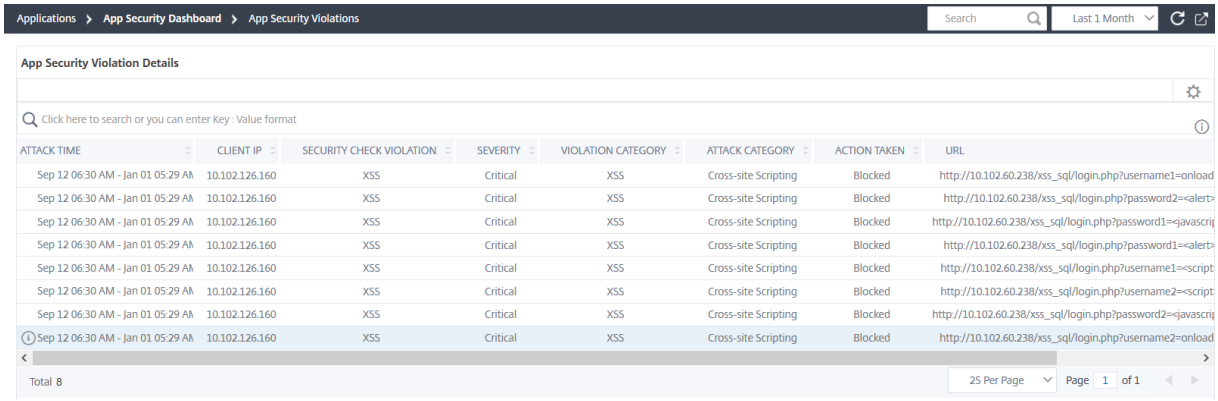
4 - Affiche les violations de sécurité basées sur les clients. Le graphique App Security Investigator s’affiche pour chaque client. Vous pouvez cliquer sur chaque adresse IP client pour afficher les résultats.

5 - Affiche les violations en mode carte et tabulaire.

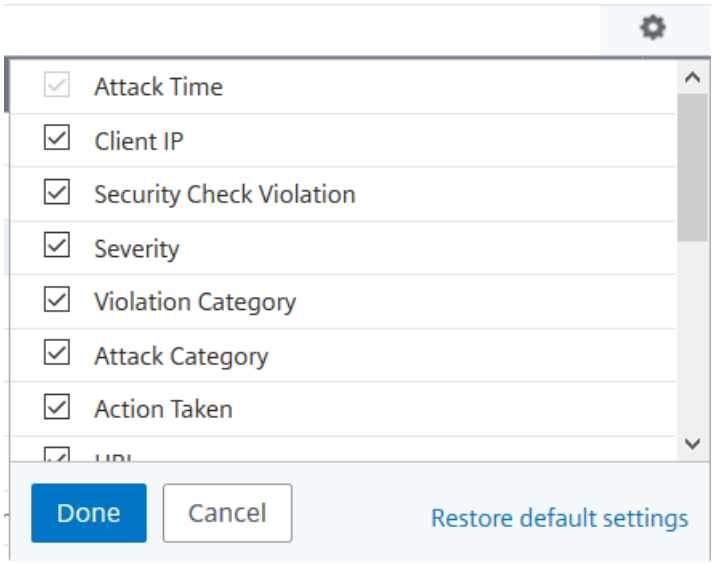
6 - Affiche les détails de la violation. Lorsque vous placez le pointeur de la souris sur le graphique, les détails tels que le type de violation, l’heure de l’attaque et le total des événements sont affichés.

Lorsque vous cliquez sur un graphique à bulles, les détails s’affichent dans la page **Détails des violations de sécurité des applications**. Par exemple, si vous souhaitez afficher plus de détails sur la violation de script intersite, cliquez sur le graphique rempli pour **XSS** dans **App Security Investigator**.

Les **détails des violations de sécurité de l’application** sont affichés avec des détails de violation tels que le temps d’attaque, la catégorie d’attaque, la gravité, l’URL, etc.



Vous pouvez également cliquer sur l'option **Paramètres** pour sélectionner les options que vous souhaitez afficher.



Détails de l'indice de sécurité

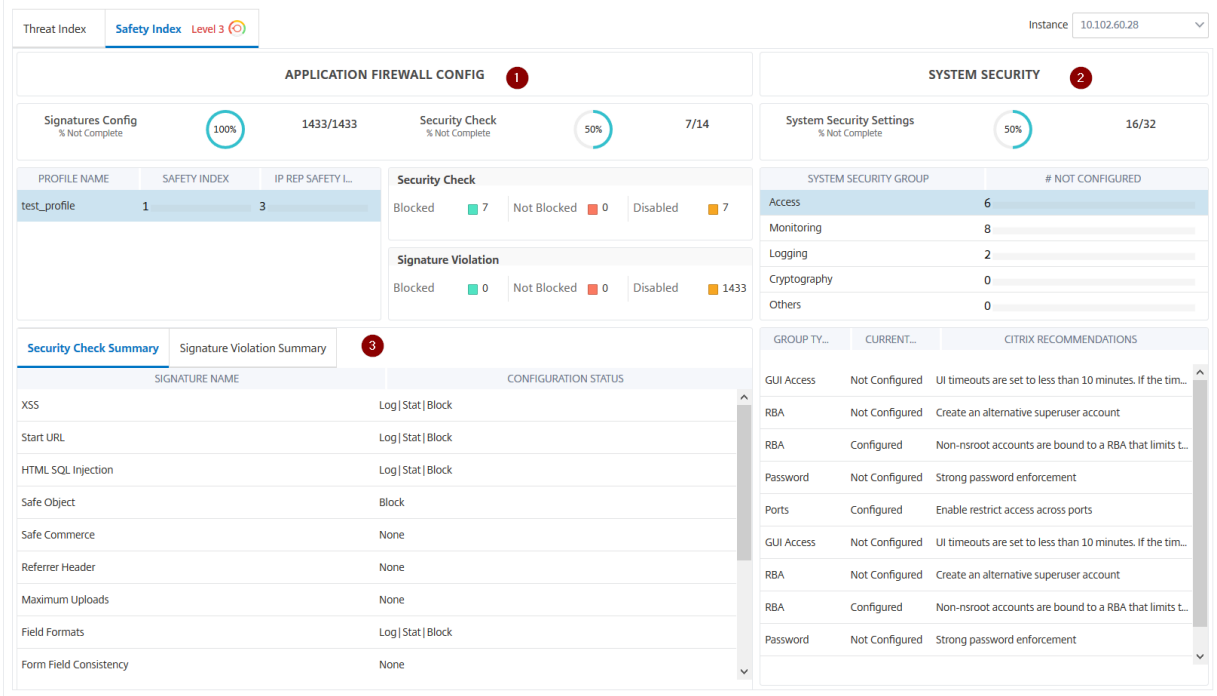
Après avoir examiné l'exposition à la menace d'une application, vous souhaitez déterminer quelles configurations de sécurité d'application sont en place et quelles configurations sont manquantes pour cette application. Vous pouvez obtenir ces informations en explorant le résumé de l'index de sécurité des applications.

Le résumé de l'indice de sécurité vous donne des informations sur l'efficacité des configurations de sécurité suivantes :

- **Configuration du pare-feu d'application**. Affiche le nombre d'entités de signature et de sécurité non configurées.
- **Citrix ADM System Security**. Indique combien de paramètres de sécurité système ne sont pas configurés.

Pour afficher les détails de l'**index de sécurité**, sélectionnez un serveur/application virtuel et cliquez sur l'onglet **Indice de sécurité** .

Les détails sont affichés.



1 - Affiche les informations détaillées pour les configurations du pare-feu d'application.

2 - Affiche les informations détaillées pour la sécurité du système. Cliquez sur chaque groupe de sécurité pour obtenir des détails sur l'état et les recommandations Citrix.

3 - Affiche le résumé de la vérification de sécurité et de la violation de signature.

Vous pouvez également afficher le résumé de l'environnement de menace en activant leSecurity Insightpour les serveurs virtuels, puis en accédant à **Analytics**> **Security Insight**. Pour plus d'informations sur le cas d'utilisation de l'indice de sécurité, voirSecurity Insight

Gateway API

April 29, 2021

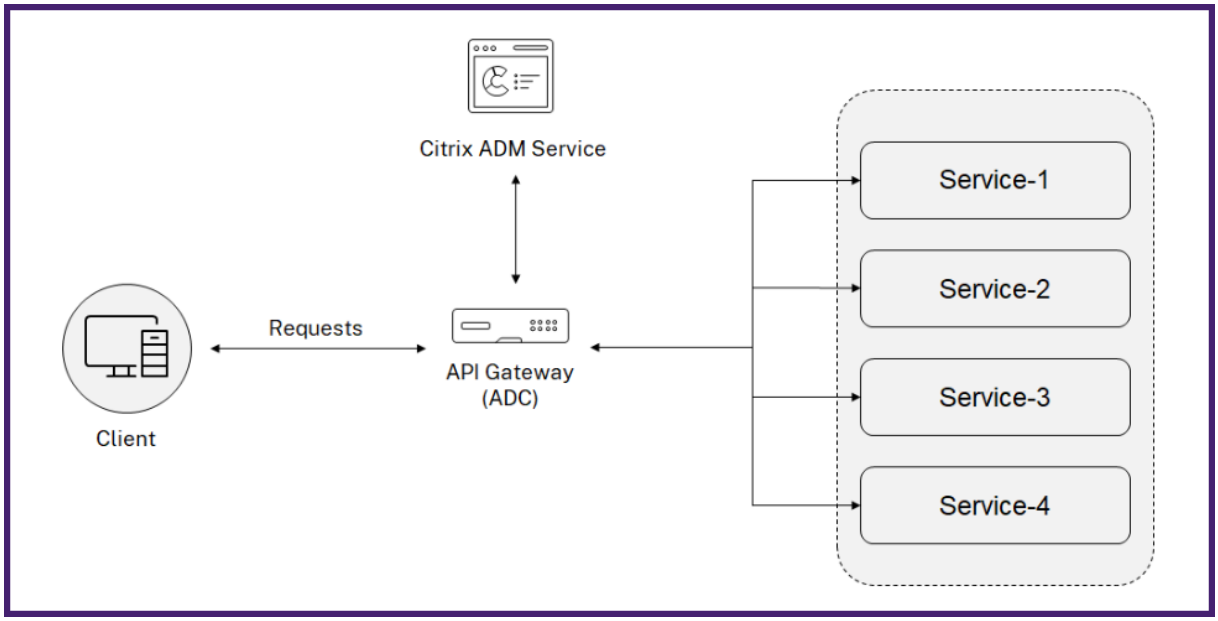
Une passerelle API sert de point d'entrée pour toutes les demandes adressées à vos points de terminaison API. De plus, garantit un accès sécurisé et fiable à tous les terminaux API et microservices de votre système.

Une passerelle API proxie toutes les demandes et réponses entre vos clients/applications API et les services d'API back-end. Il vous aide à configurer, gérer et sécuriser les points de terminaison API. Vous pouvez également créer et gérer des définitions d'API de l'une des manières suivantes :

- Télécharger le fichier de spécification OAS Swagger
- Créez votre propre définition d'API

Pour de plus amples informations, consultez la section Créer ou télécharger une définition d'API.

L'image suivante décrit comment la passerelle API reçoit la demande du client et envoie la réponse des services API back-end :



> **Remarque**
>
> Dans Citrix Application Delivery Management, cette fonctionnalité est disponible pour les utilisateurs disposant de licences Premium ou Advanced.

Avantages de la passerelle API

La passerelle API vous offre les avantages suivants :

- **Sécurise vos points de terminaison API** : la passerelle API ajoute une couche de sécurité et protège vos terminaux API et serveurs API back-end contre les attaques telles que :
  - Dépassement de tampon
  - Injection SQL

  - Scriptage intersite
  - Déni de service (Dos)

- **Surveille et améliore les performances**de l'API : la passerelle API fournit des services tels que le déchargement SSL, l'authentification, l'autorisation, la limitation des taux, etc. Ces services augmentent les performances de l'API et leur disponibilité.

  L'analyse de l'API vous offre la visibilité de vos mesures de performances API et des menaces sur vos points de terminaison d'API. Pour de plus amples informations, consultez la section Afficher l'analyse de l'API.

- **Gère le trafic API** : la passerelle API extrait la complexité de votre infrastructure API back-end.
- **Découverte des points de terminaison**de l'API : la passerelle API découvre les points de terminaison de l'API qui se trouvent dans votre organisation et ajoute à la page **Découverte d'API** .

Gérer la passerelle API

En tant qu'administrateur, vous pouvez créer des définitions d'API et déployer les instances d'API sur une passerelle API (ADC) dans Citrix ADM. Pour plus d'informations, consultez :

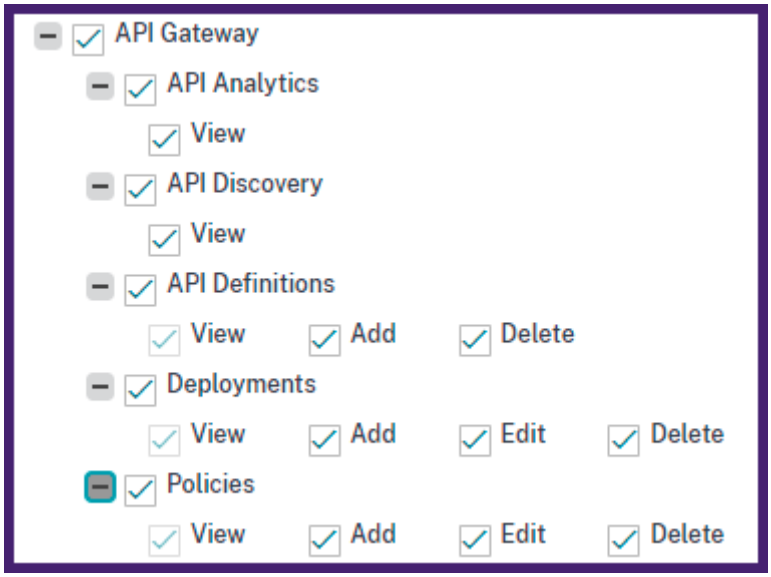
- Ajouter une définition d'API
- Déployer une instance API

Dans une passerelle API, vous pouvez appliquer des stratégies de sécurité. Pour savoir comment créer une stratégie API, reportez-vous à la section Ajouter des stratégies à un déploiement d'API.

Accorder des autorisations de gestion et de configuration de passerelle API

En tant qu'administrateur, vous pouvez créer une stratégie d'accès pour accorder des autorisations utilisateur pour la configuration et la gestion de passerelle API. Les autorisations utilisateur peuvent être afficher, ajouter, modifier et supprimer. Procédez comme suit pour accorder des autorisations :

1. Accédez à **Compte > Administration des utilisateurs > Stratégies d'accès**.
2. Cliquez sur **Add**.
3. Dans **Créer des stratégies d'accès**, spécifiez un nom de stratégie et la description.
4. Dans le champ **Autorisations**, développez **Applications**, puis **API Gateway**.
5. Sélectionnez les pages **API Gateway** requises. Sélectionnez ensuite les autorisations que vous souhaitez accorder.



> **Important**
>
> Assurez-vous d'accorder des autorisations pour les fonctionnalités nécessaires à l'utilisation d'une passerelle API. Par exemple, si vous accordez l'accès utilisateur à la page **Déploiements**, les fonctionnalités suivantes nécessitent également un accès utilisateur :
>
> - StyleBooks
> - IPAM
> - Équilibrage de charge (sous **Fonctions réseau**)
> - Commutation de contenu (sous **Fonctions réseau**)
> - Proxy API de périphérique (sous **API**)

Pour plus d'informations sur les stratégies d'accès, reportez-vous à la section Configurer les stratégies d'accès sur ADM.

Afficher l'analyse de l'API

April 29, 2021

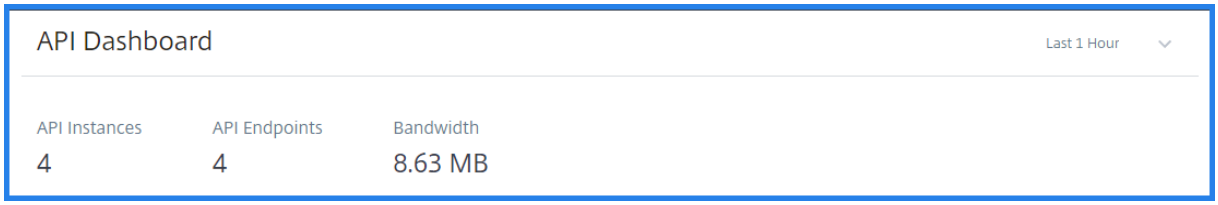
L'analyse des API permet une visibilité sur le trafic des API. Cette analyse permet aux administrateurs informatiques de surveiller les instances d'API et les points de terminaison servis par une passerelle API. Il fournit une surveillance périodique intégrée des demandes d'API.

Avant de surveiller l'analyse des API, assurez-vous d'effectuer les opérations suivantes :

1. Ajouter une définition d'API
2. Déployer une définition d'API
3. Ajouter une stratégie à une définition d'API

4. Appliquer une licence aux instances API
5. Activer Web Insight sur les instances API

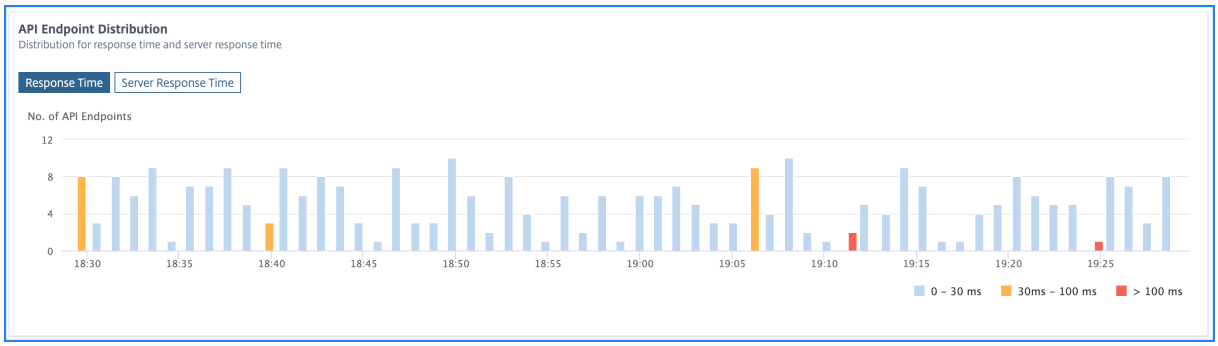
Dans **API Analytics**, vous pouvez surveiller le temps de réponse des instances d'API et des points de terminaison ajoutés dans le cadre des définitions d'API. Il affiche également la bande passante consommée par les instances d'API et les points de terminaison.



Par défaut, le tableau de bord affiche les analyses d'API pour la dernière heure. Vous pouvez sélectionner une durée pour afficher les analyses d'API pour cet intervalle. Cliquez sur **Voir plus** sur chaque vignette pour afficher la liste entière. Dans cette vue, vous pouvez rechercher des instances d'API et des points de terminaison par leurs noms partiels, à l'exception de la vignette **Emplacements géographiques**.

Distribution des points de terminaison API

Ce graphique affiche la répartition du temps de réponse des applications et du serveur pour les points de terminaison API. Vous pouvez identifier un point de terminaison d'API qui a un temps de réponse énorme et prendre les mesures nécessaires.

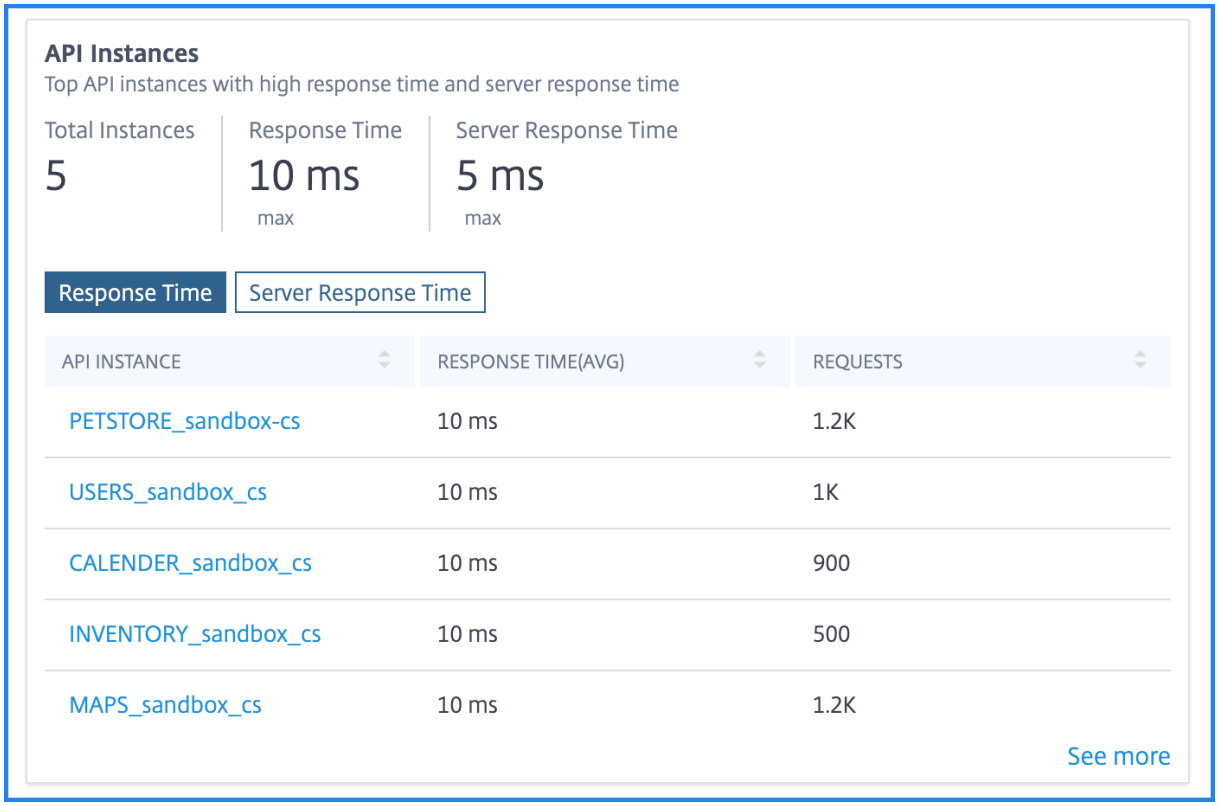


Les points de terminaison de l'API apparaissent dans l'une des couleurs suivantes en fonction de leurs limites de temps de réponse :

- **Bleu** — Si le temps de réponse est inférieur à 30 millisecondes.
- **Orange** — Si le temps de réponse est compris entre 30 et 100 millisecondes.
- **Rouge** — Si le temps de réponse est supérieur à 100 millisecondes.

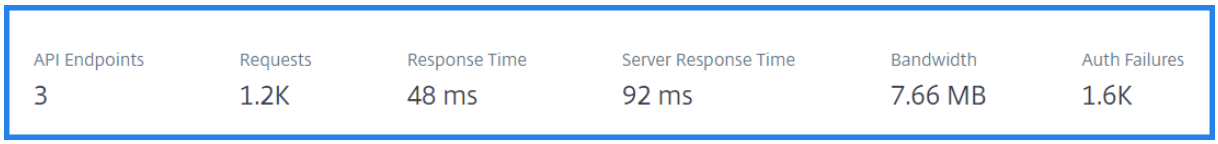
Instances API

La vignette **Instances d'API** affiche les principales instances d'API avec un temps de réponse élevé pour les applications et le serveur.



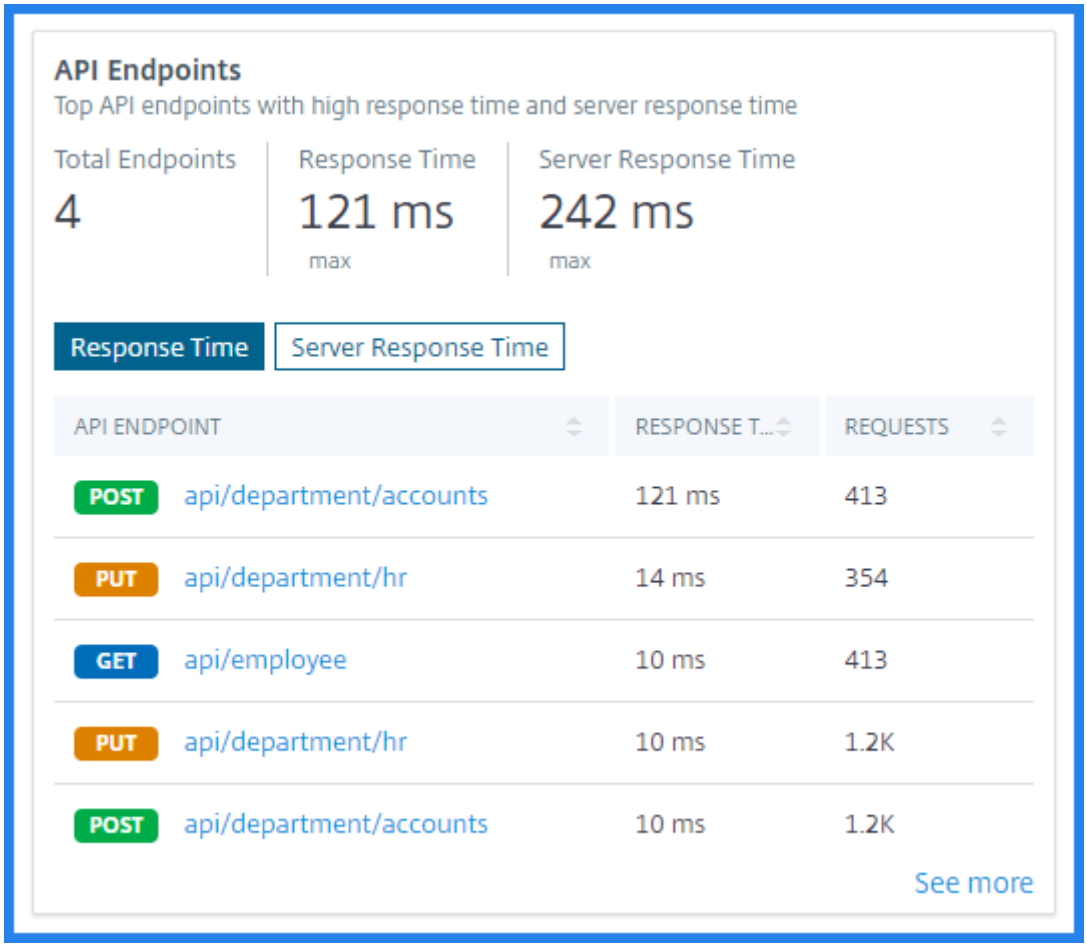
Sélectionnez une instance d'API pour afficher ses performances, son utilisation et ses détails de sécurité. L'instance d'API sélectionnée affiche les informations suivantes :

- Nombre de points de terminaison API
- Nombre de demandes
- Temps de réponse des applications et du serveur
- Bande passante consommée
- Échec de l'authentification



Points de terminaison d'API

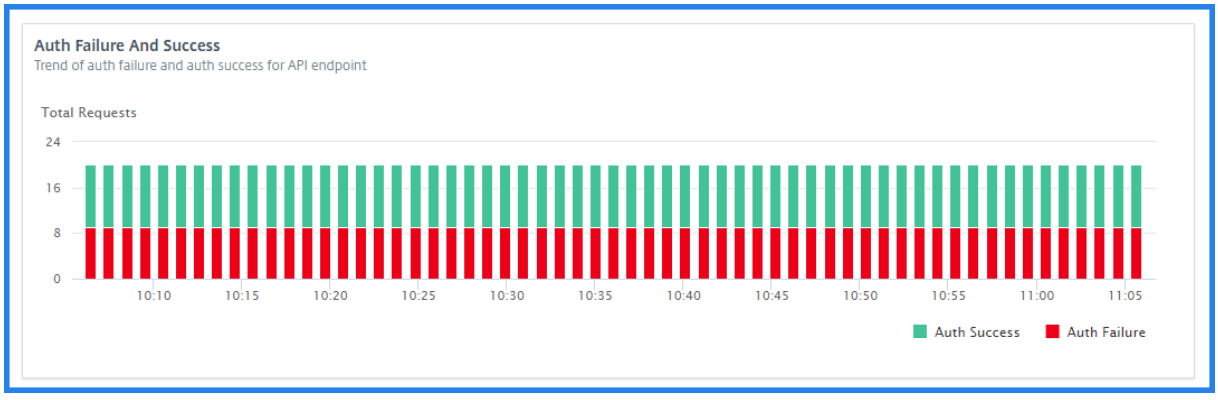
La vignette **API Endpoints** affiche les points de terminaison supérieurs avec un temps de réponse élevé pour les applications et le serveur.



Sélectionnez un point de terminaison d'API pour afficher les détails sur les performances, l'utilisation et la sécurité.

Échec de l'authentification

La vignette **Auth Failures** affiche les principaux points de terminaison de l'API qui présentent plus d'échecs d'authentification. L'échec ou le succès de l'authentification se produit en fonction de la stratégie ajoutée à une définition d'API.



Si vous souhaitez afficher l'échec et le taux de réussite de l'authentification dans un point de terminaison API, procédez comme suit :

1. Sélectionnez un point de terminaison dans les **points de terminaison API**.
2. Sélectionnez l'onglet **Sécurité**. Cet onglet affiche les échecs et réussites d'authentification dans le point de terminaison sélectionné.

Si vous souhaitez afficher l'échec et le taux de réussite de l'authentification dans les points de terminaison API d'une instance, procédez comme suit :

1. Sélectionnez une instance dans l' **instance API**.
2. Sélectionnez l'onglet **Sécurité**. Cet onglet affiche les échecs et réussites d'authentification dans les points de terminaison de l'instance sélectionnée.

Afficher différentes informations sur les API

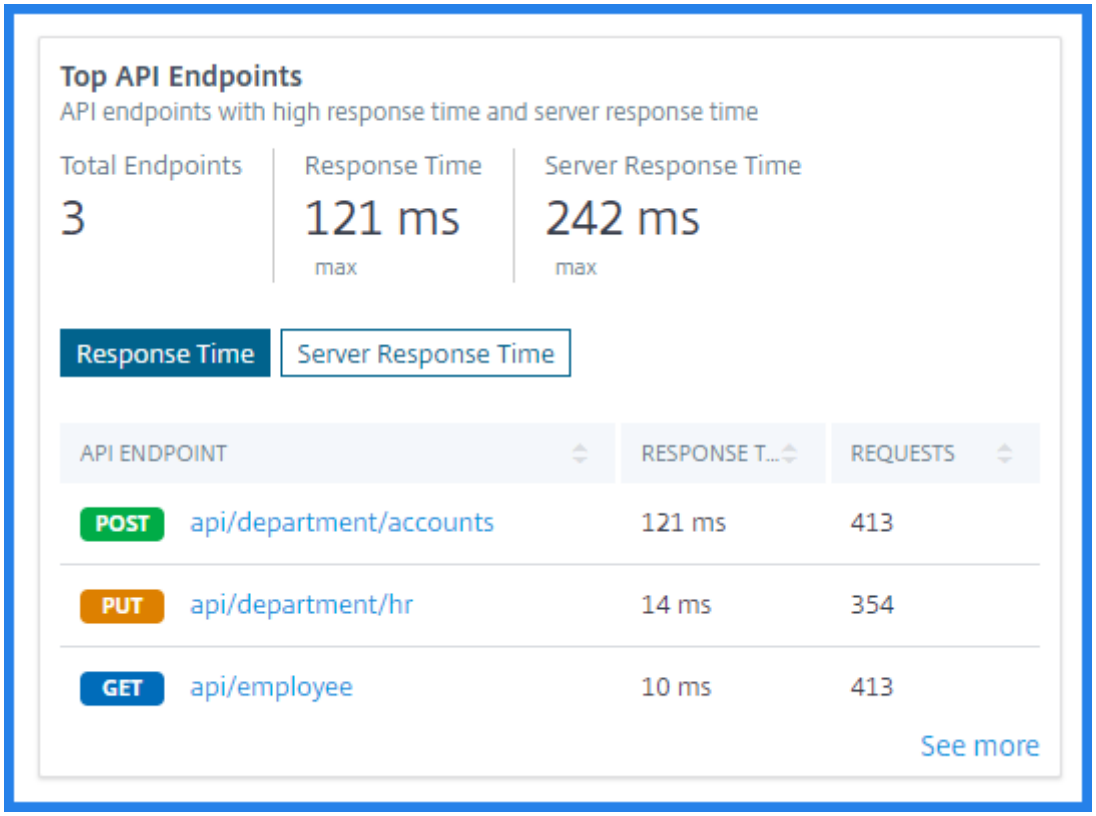
Naviguez dans API Analytics pour afficher des informations spécifiques sur les éléments suivants :

- Points de terminaison d'API les plus importants dans une instance
- API les plus consultées
- Géo-localisation d'un point de terminaison
- Statut de la réponse HTTPS
- Tendance des requêtes API
- Consommation de bande passante d'un point de terminaison
- Erreurs SSL et utilisation

Afficher les principaux points de terminaison de l'API dans une instance

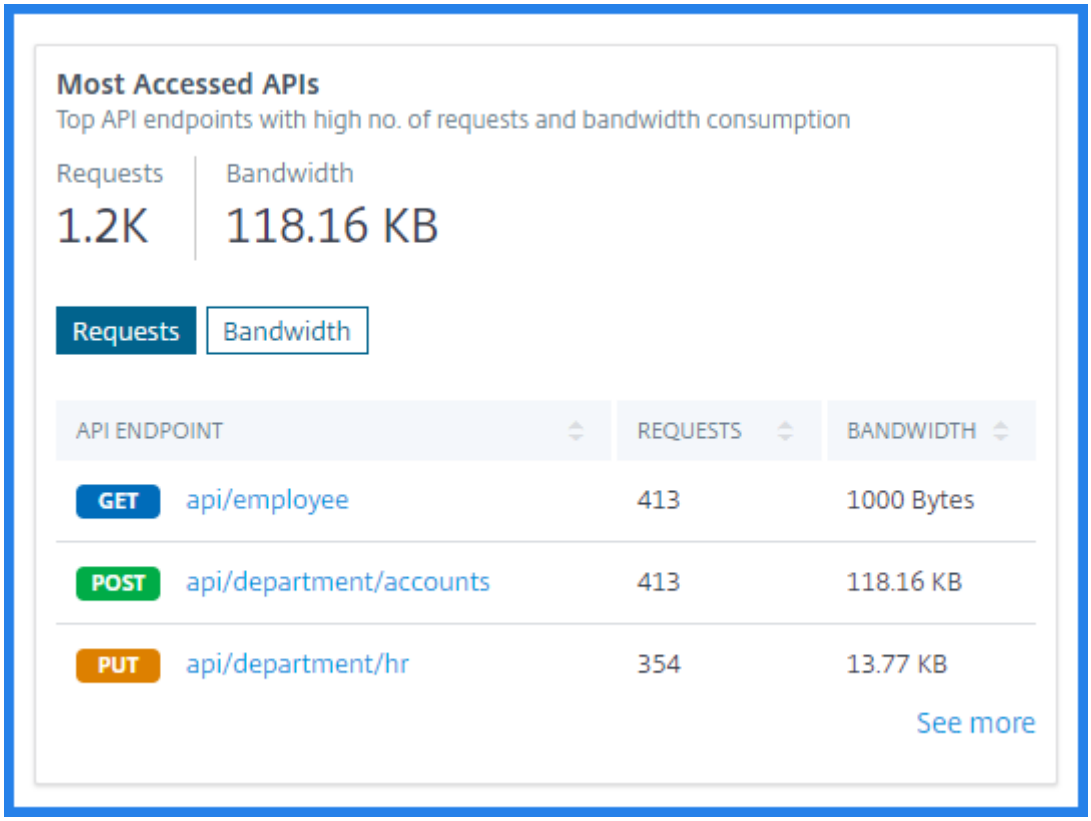
La page **API Analytics** affiche les points de terminaison les plus élevés ayant un temps de réponse élevé. Si vous souhaitez afficher des points de terminaison similaires d'une instance, sélectionnez une instance **dans les instances API**.

La vignette **Top API Endpoints** affiche les points de terminaison dont le temps de réponse des applications et du serveur est élevé.



Afficher les API les plus consultées

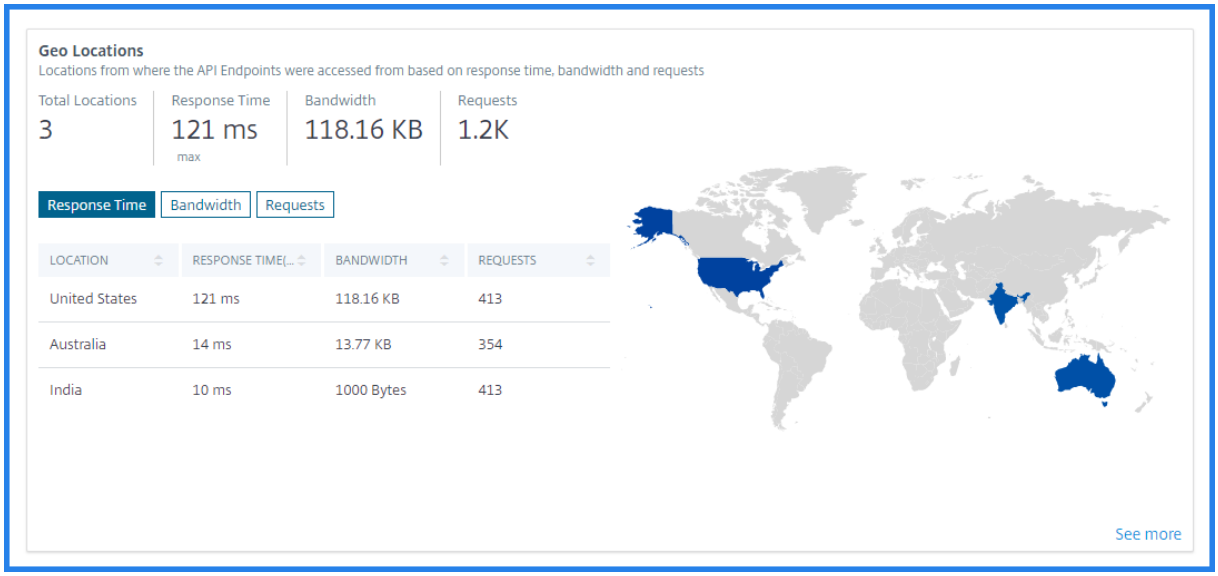
Dans **API Analytics**, sélectionnez une instance d'API à partir des instances d'API. La vignette **API les plus consultées** affiche les points de terminaison supérieurs qui ont plus de demandes et de bande passante.



Afficher la géolocalisation d'un point de terminaison

1. Dans **API Analytics**, sélectionnez l'une des options suivantes :
   - Sélectionnez une instance **dans les instances API** pour afficher les emplacements à partir desquels les points de terminaison de l'instance sélectionnée ont reçu des demandes.
   - Sélectionnez un point de terminaison dans les **points de terminaison API** pour afficher les emplacements à partir desquels le point de terminaison a reçu des demandes.
2. Dans **Performances et utilisation**, la vignette **Emplacements géographiques** apparaît.

   Vous pouvez trier les emplacements en fonction du temps de réponse, de la bande passante et des demandes.

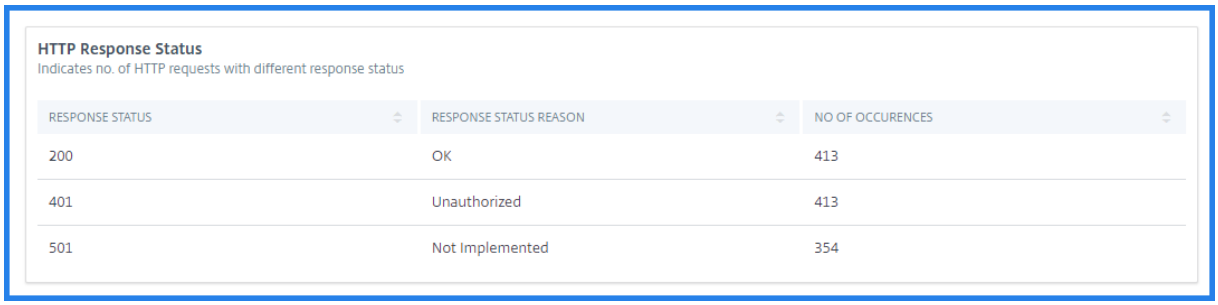


Afficher l'état de la réponse HTTPS

La vignette **Statut de la réponse HTTPS** affiche l'état de la réponse avec sa raison et ses occurrences. Vous pouvez afficher l'état de la réponse HTTPS de l'une des manières suivantes :

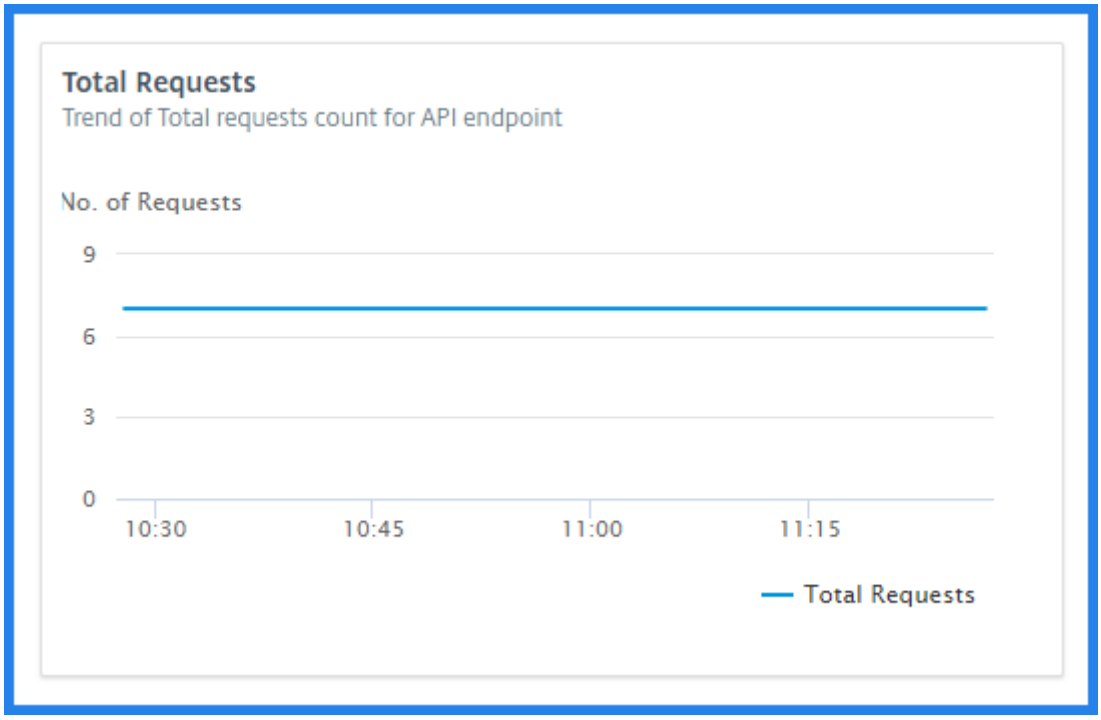
- Sélectionnez une instance dans les **instances API**.
- Sélectionnez un point de terminaison dans les **points de terminaison API**.

Cette vignette apparaît dans l'onglet **Performances et utilisation**.

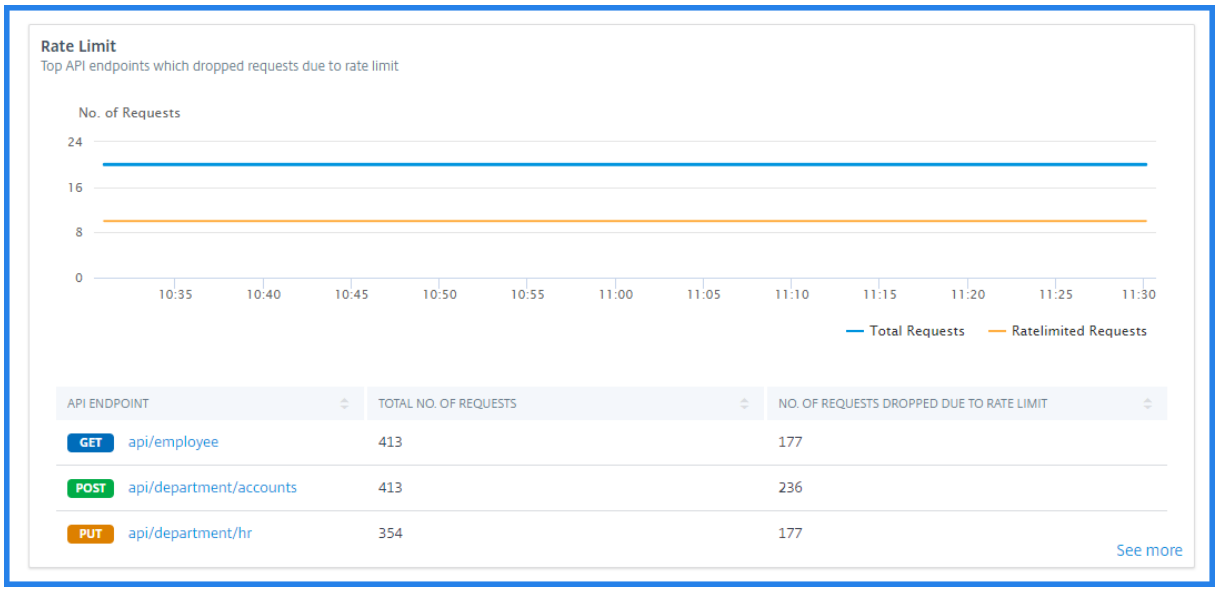


Voir la tendance des demandes d'API

Sélectionnez un point de terminaison dans les **points de terminaison API**. Dans **Performances et utilisation**, la vignette **Total des demandes** affiche la tendance du nombre total de demandes reçues par un point de terminaison.



Si vous souhaitez afficher la tendance des demandes abandonnées en raison d'une limite de débit, sélectionnez une instance **dans les instances API**. Dans **Sécurité**, la vignette **Limite de débit** affiche la tendance des demandes abandonnées. Il affiche également la tendance du nombre total de demandes reçues par un point de terminaison.



Avec cette comparaison, vous pouvez déterminer le nombre de demandes supprimées en raison d'une limite de taux entre le nombre total de demandes.

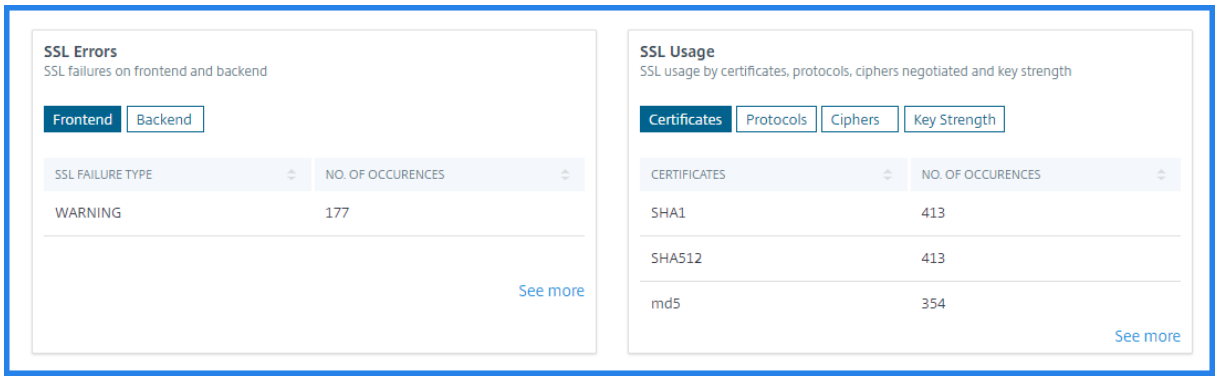
Afficher la consommation de bande passante d'un point de terminaison

Pour afficher la tendance de la consommation de bande passante par un point de terminaison, sélectionnez un point de terminaison dans les points de terminaison de l'API. La vignette **Bande passante** affiche un graphique de consommation de bande passante.

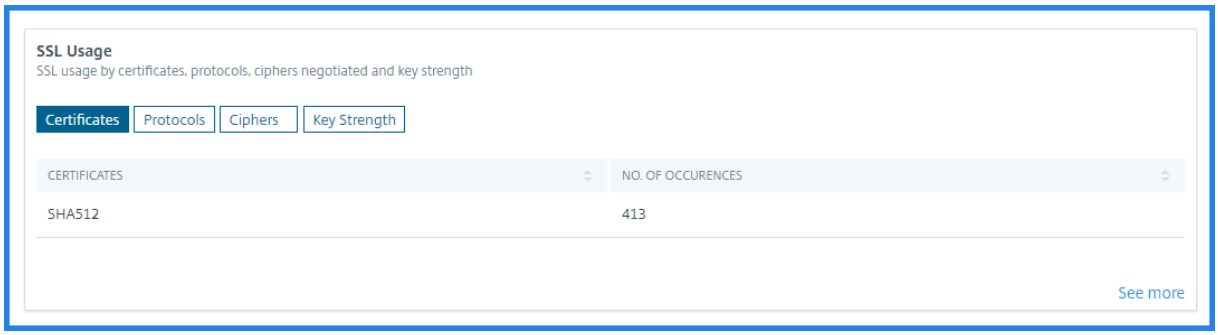
Afficher les erreurs SSL et l'utilisation

Sélectionnez une instance dans les **instances API**. Dans **Sécurité**, les vignettes suivantes apparaissent :

- **Erreurs SSL** — Affiche les échecs SSL survenus sur les clients et les serveurs d'applications.
- **Utilisation de SSL** : affiche les certificats SSL, les protocoles, le chiffrement et les points forts clés avec leurs occurrences.



Pour afficher l'utilisation de SSL dans un point de terminaison, sélectionnez un point de terminaison dans les points de terminaison de l'API. La vignette **Utilisation de SSL** apparaît dans l'onglet **Sécurité**.



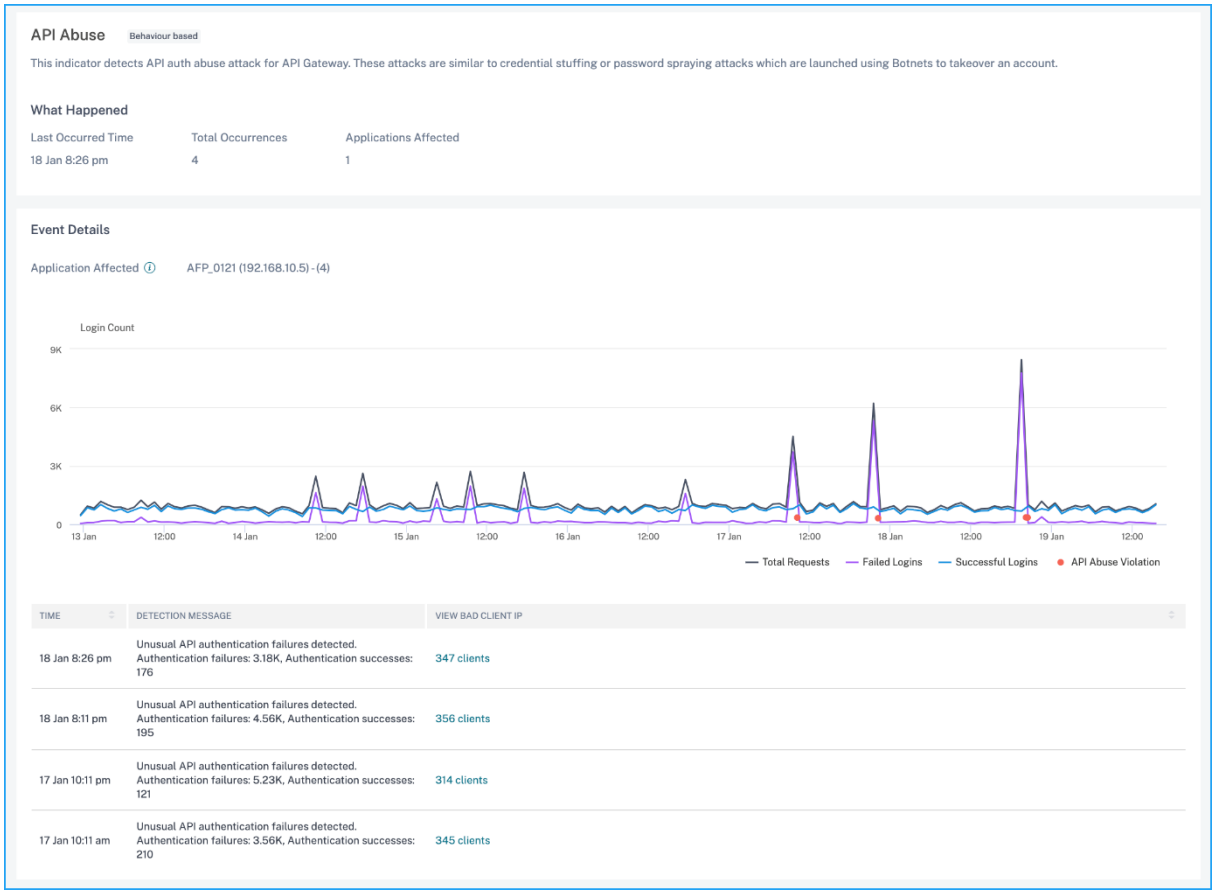
Afficher les violations de sécurité de l'API

Citrix ADM affiche les violations de sécurité sur une passerelle API. La menace à la sécurité peut être d'un réseau, d'un WAF ou d'un bot. Grâce à ces informations, vous pouvez prendre les mesures appropriées pour sécuriser votre instance. L'interface graphique ADM affiche les violations de sécurité de l'API suivantes :

Abus d'API

Les robots défectueux peuvent utiliser ou voler des authentifications API et effectuer divers types de cyberattaques telles que le remplissage des informations d'identification et la pulvérisation de mot de passe. Dans Citrix ADM, vous pouvez analyser ces activités inhabituelles d'ouverture de session pour les API.

À l'aide de l'indicateur d'abus d'API, en tant qu'administrateur, vous pouvez analyser si des robots défectueux ont tenté de prendre en charge la ressource cible, en utilisant l'authentification API.

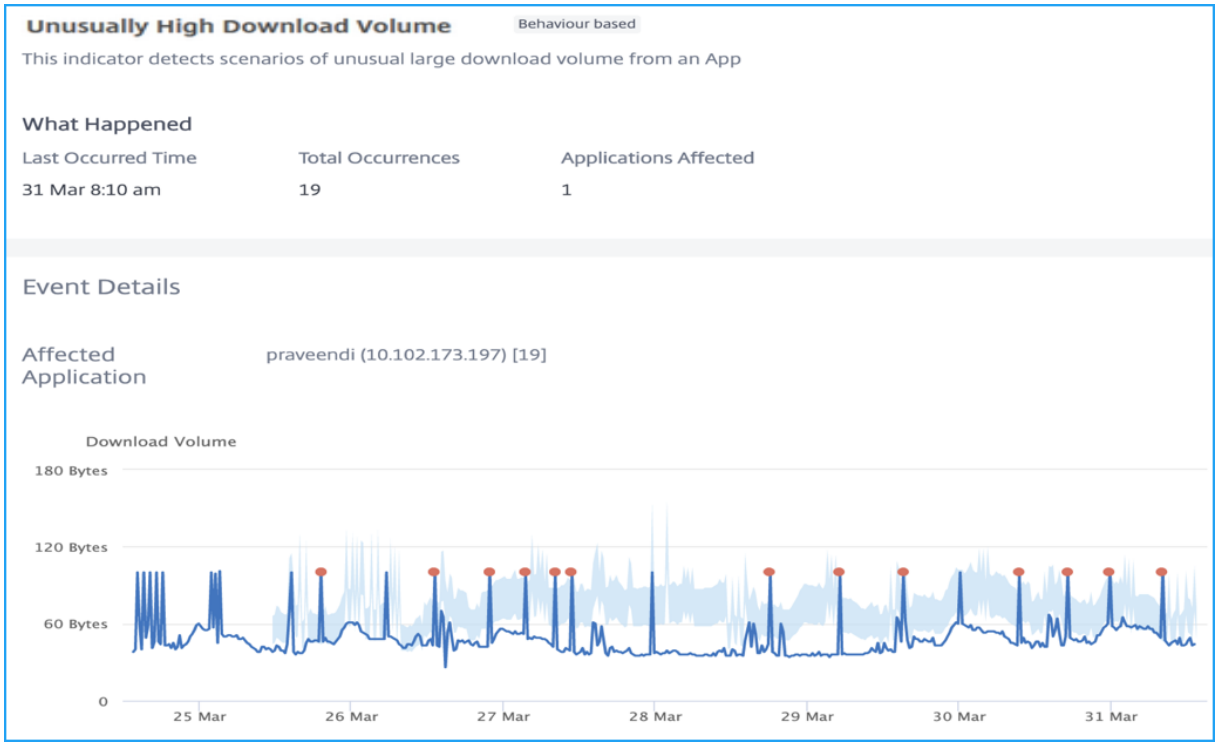


Pour de plus amples informations, consultez la section Abus d'API.

Exposition excessive des données

Un point de terminaison d'API peut avoir de grandes réponses aux demandes des clients. Cette condition est appelée exposition excessive aux données. Un attaquant peut identifier de telles failles pour obtenir plus d'informations à partir du point de terminaison.

Dans Citrix ADM, vous pouvez analyser les tailles de réponse qui sont plus élevées que d'habitude. De plus, vous pouvez prendre les mesures appropriées pour éviter une exposition excessive des données. L'interface graphique ADM affiche ces violations sous l'indicateur **Volume de téléchargement exceptionnellement élevé**. Vous pouvez analyser l'exposition excessive des données à partir du point de terminaison affecté et prendre les mesures appropriées.



Pour de plus amples informations, consultez la section Volume de téléchargement exceptionnellement élevé.

Créer ou télécharger une définition d'API

April 29, 2021

Une définition d'API est un document qui décrit une API à l'aide des normes de spécification OpenAPI (Swagger 2.0, OpenAPI 3.0.x). Cette définition peut contenir des chemins d'accès aux ressources API et des méthodes pour les exploiter. Vous pouvez ajouter des définitions d'API à ADM, puis les déployer sur une passerelle API (Citrix ADC).

Vous pouvez créer des définitions d'API de l'une des manières suivantes :

- Télécharger le fichier de spécification OAS Swagger
- Créez votre propre définition d'API

> **Remarque**
>
> Actuellement, ADM prend en charge l'analyse des fichiers de spécifications OAS qui utilisent **Swagger 2.0** ou **openapi 3.0.1**.

Télécharger la spécification OEA

Vous pouvez télécharger la spécification OEA dans l'interface graphique ADM.

1. Accédez à **Applications > API Gateway > Définitions d'API**.
2. Cliquez sur **Ajouter**.
3. Sélectionnez **Charger la spécification OAS**.

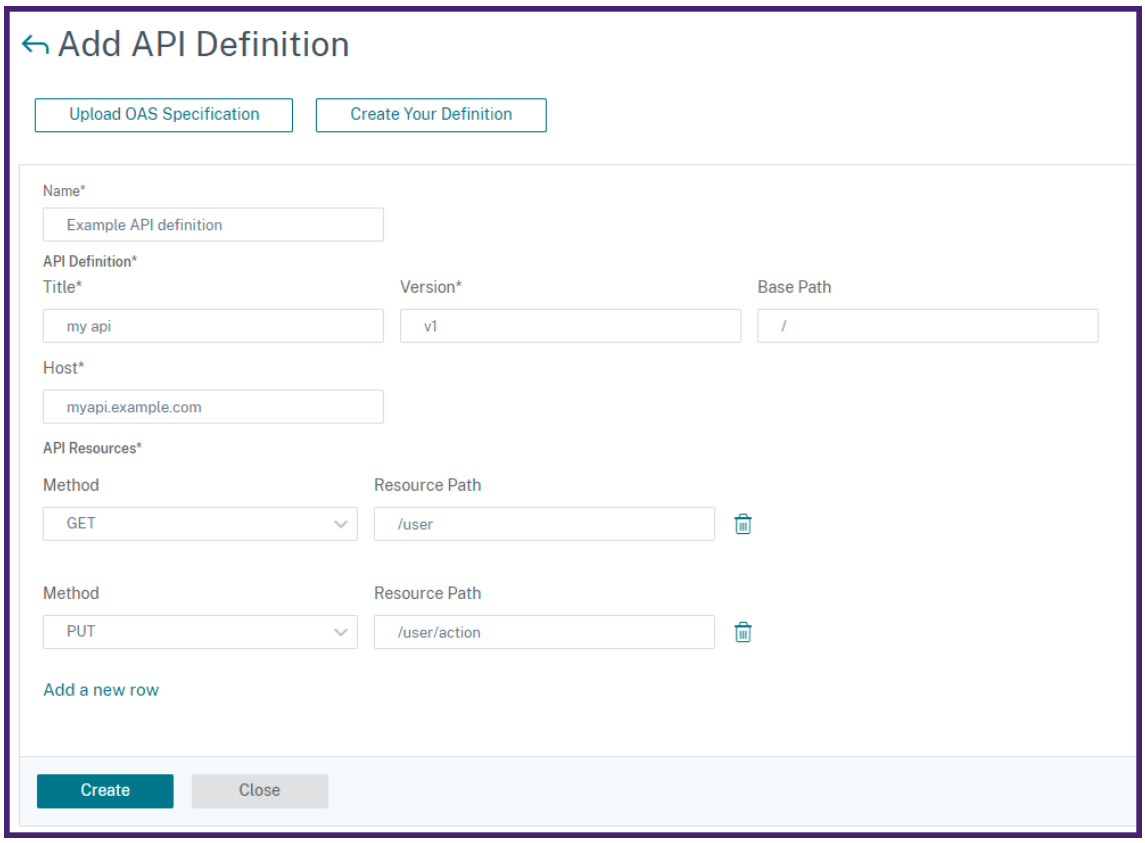
   > **Remarque**
   >
   > Assurez-vous que le fichier de spécification OAS est au format YAML ou JSON. Et, ce fichier ne doit pas contenir de références externes. Actuellement, ADM prend en charge la version 2.0 de Swagger.

4. Parcourez une spécification OEA à partir de votre ordinateur local et téléchargez vers ADM.

Créer une définition d'API

Vous pouvez créer votre propre définition d'API dans l'interface graphique ADM.

1. Accédez à **Applications > API Gateway > Définitions d'API**.
2. Cliquez sur **Ajouter**.
3. Sélectionnez **Créer votre définition** et spécifiez les éléments suivants :
   - **Nom** : nom de la définition de l'API.
   - **Définition de l'API** - Une définition doit inclure le titre, la version, le chemin de base et l'hôte. Vous pouvez spécifier un nom de domaine ou une adresse IP dans le champ **Hôte**.
   - **API Resources** - Ajoutez plusieurs ressources API à votre définition. Chaque ressource a un chemin d'accès et une méthode prise en charge.



4. Cliquez sur **Créer**.

Afficher les définitions de l'API

La page **Définitions de l'API** répertorie la définition téléchargée. Cliquez sur **Afficher pour afficher** les détails de définition d'API suivants :

- **Nom** — Affiche le nom d'une définition d'API.
- **Définition de l'API** : affiche le titre, la version, le chemin de base et l'hôte d'une définition.
- **Ressources API** : répertorie les ressources API dans une définition d'API et leurs méthodes pour les exploiter.

Ensuite, déployez cette définition sur une passerelle API.

Déployer une instance API

April 29, 2021

Procédez comme suit pour déployer une instance API :

1. Accédez à **Applications > Passerelle API > Déploiements**.
2. Cliquez sur **Add**.
3. Dans Informations **de base sur le déploiement**,
   a) Spécifiez le **nom du déploiement**.
   b) Dans **Target API Gateway**, sélectionnez une instance ADC comme passerelle API.
   c) Dans **Définitions d'API**, sélectionnez la définition d'API requise.
   d) Dans **API Proxy**, ajoutez un proxy API pour utiliser la passerelle API. Un proxy API est une adresse IP virtuelle frontale où la passerelle API reçoit le trafic API des clients. Spécifiez les détails suivants :
      - **Adresse IP**
      - **Port**
      - **Profil de sécurité TLS** : sélectionnez Élevé ou Moyen dans la liste. Si vous sélectionnez Élevé, il est mappé au profil SSL sécurisé sur une instance ADC.
      - **Certificat TLS**
      - **Clé TLS**

      > **Remarque**
      >
      > Charger le certificat TLS et la clé dans un format PEM.

      Vous pouvez également sélectionner un réseau IPAM pour allouer l'adresse IP. Pour afficher l'adresse IP allouée à partir du réseau IPAM, accédez à **Réseaux > IPAM**. Pour plus d'informations sur IPAM, reportez-vous à la section Configurer IPAM.
4. Dans **Services en amont**, cliquez sur **Ajouter** pour ajouter des serveurs API back-end où vous souhaitez transférer le trafic API. Vous pouvez configurer un service en amont avec son nom de domaine ou son adresse IP :
   a) Spécifiez un nom à un service en amont.
   b) Spécifiez le domaine.
   c) Dans **Services**, spécifiez une adresse IP et une valeur de port. Pour ajouter d'autres adresses IP, cliquez sur **Ajouter une nouvelle ligne**.
   d) Cliquez sur **Add**.
5. Dans **Routage**, spécifiez les détails suivants pour transférer le trafic API en fonction du préfixe du chemin de ressource :
   a) Spécifiez le nom de l'itinéraire.
   b) Sélectionnez une **ressource API** pour recevoir une demande d'API.

c) Sélectionnez un **service en amont** dans la liste où vous souhaitez transférer le trafic API.

6. Cliquez sur **Enregistrer** pour enregistrer la configuration de déploiement.

   Si vous souhaitez déployer la configuration sur la passerelle API, cliquez sur **Enregistrer et déployer**.

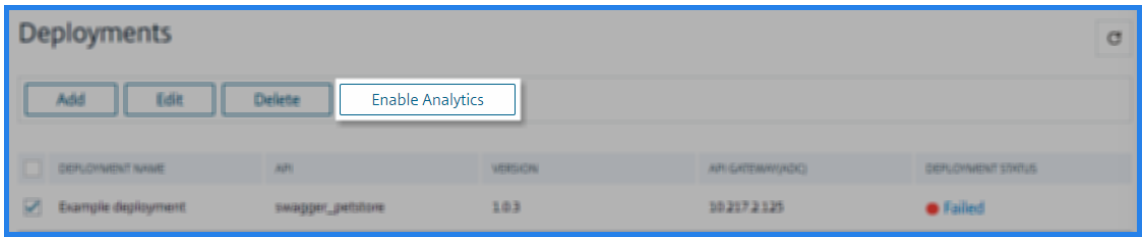
Activer l'analyse de l'API

Les conditions préalables suivantes sont les conditions requises pour activer les analyses pour un déploiement :

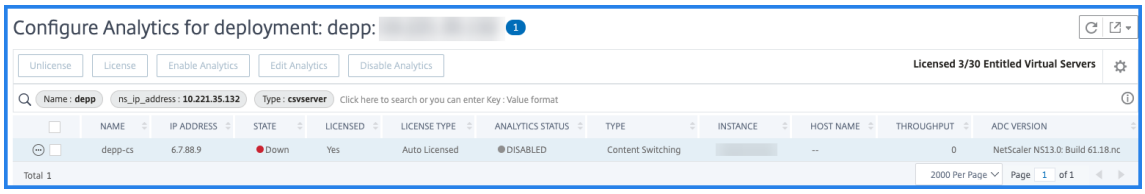
- Assurez-vous que les serveurs virtuels sont **sous licence**
- Assurez-vous que l'état de l'analyse est **désactivé**
- Assurez-vous que les serveurs virtuels sont en état **UP**

Pour activer l'analyse de l'API pour un déploiement, procédez comme suit :

1. Sélectionnez le déploiement auquel vous souhaitez activer l'analyse de l'API.
2. Cliquez sur **Activer Analytics**.



3. Dans la page **Configurer Analytics pour le déploiement**, sélectionnez le serveur virtuel, puis cliquez sur **Activer Analytics**.



4. Dans la fenêtre **Activer Analytics** :

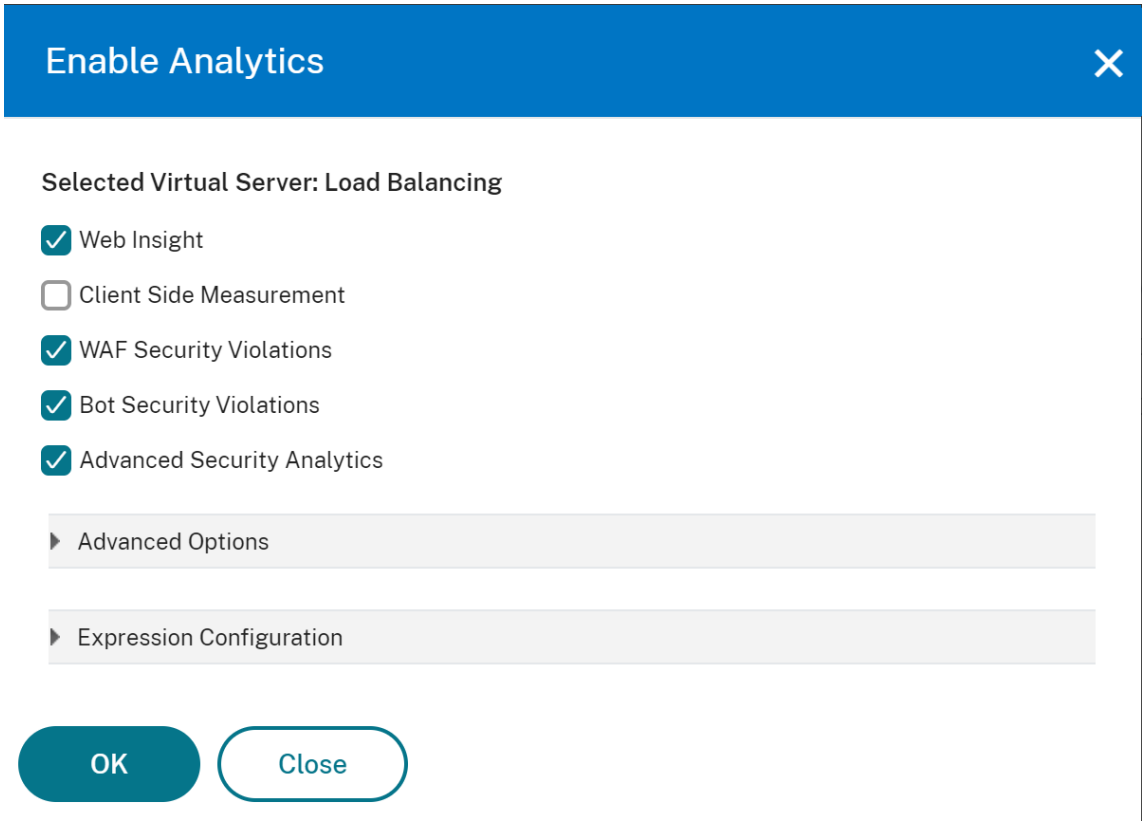
   a) Sélectionnez le type d'aperçu (Web Insight, Security Insight, Bot Insight)

   b) Sélectionnez **Logstream** ou **IPFIX** comme mode de transport.

   Pour plus d'informations sur IPFIX et Logstream, reportez-vous à la section Vue d'ensemble de Logstream.

   c) L'expression est vraie par défaut.

   d) Cliquez sur **OK**.



Les processus Citrix ADM pour activer l'analyse sur les serveurs virtuels sélectionnés.

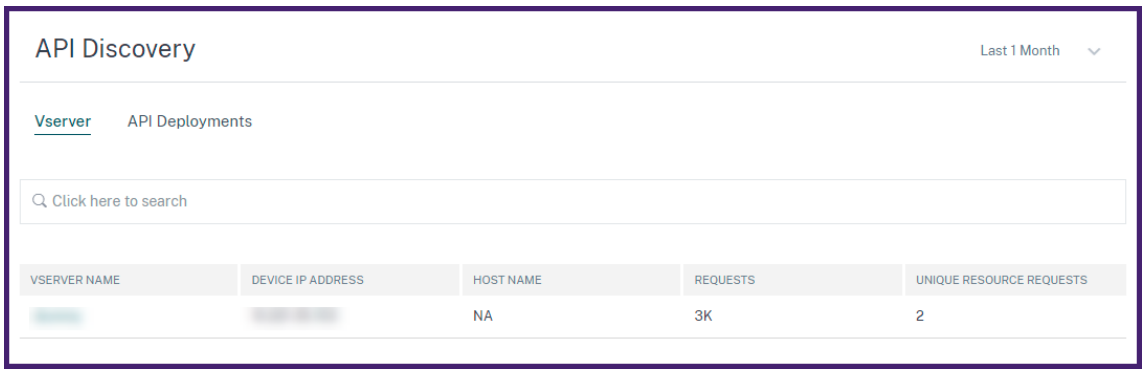
Découvrir les points de terminaison API

April 29, 2021

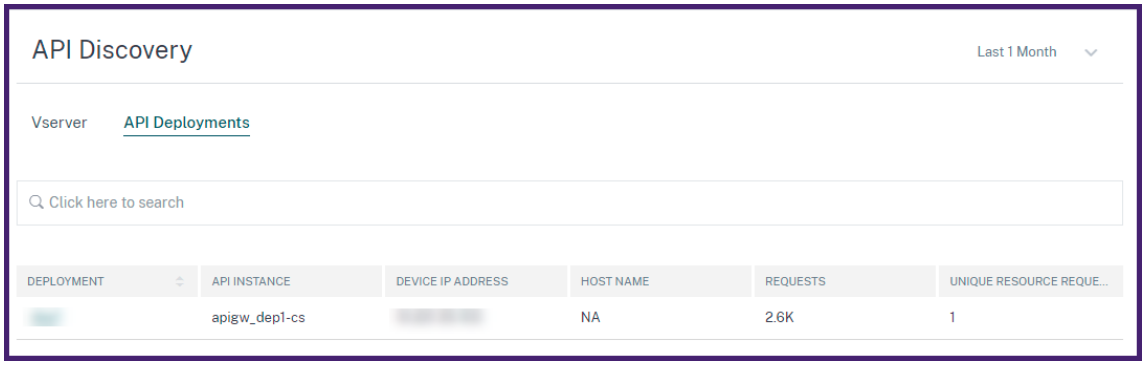
Vous pouvez afficher les points de terminaison API découverts qui se trouvent dans votre organisation à l'aide d'API Gateway. Citrix ADM découvre les points de terminaison de l'API en fonction du trafic d'API reçu sur les instances ADC et les déploiements d'API.

Dans Citrix ADM, la page **Applications > API Gateway > Découverte d'API** affiche les points de terminaison d'API découverts.

- **Serveurs virtuels** - L'onglet **Vserver** affiche les serveurs virtuels de vos instances ADC. Les serveurs virtuels apparaissent dans cet onglet lorsqu'ils reçoivent les demandes d'API pour la période spécifiée.



- **Déploiements d'API** - Cet onglet affiche les déploiements d'API déployés à partir d'ADM à l'aide d'une définition d'API. Cet onglet découvre les points de terminaison de l'API lorsque les déploiements d'API reçoivent les demandes d'API pour la période spécifiée. Pour ajouter et déployer une définition d'API, reportez-vous à la section Ajouter une définition d'API et Déployer les définitions de.



> **Remarque**
>
> - Assurez-vous de configurer les analyses et d'activer Web Insights sur les serveurs virtuels. Consultez Activer Web Insight sur les instances API.
> - Vous pouvez uniquement ajouter des stratégies aux points de terminaison de l'API découverts sous l'onglet **Déploiements d'API**.

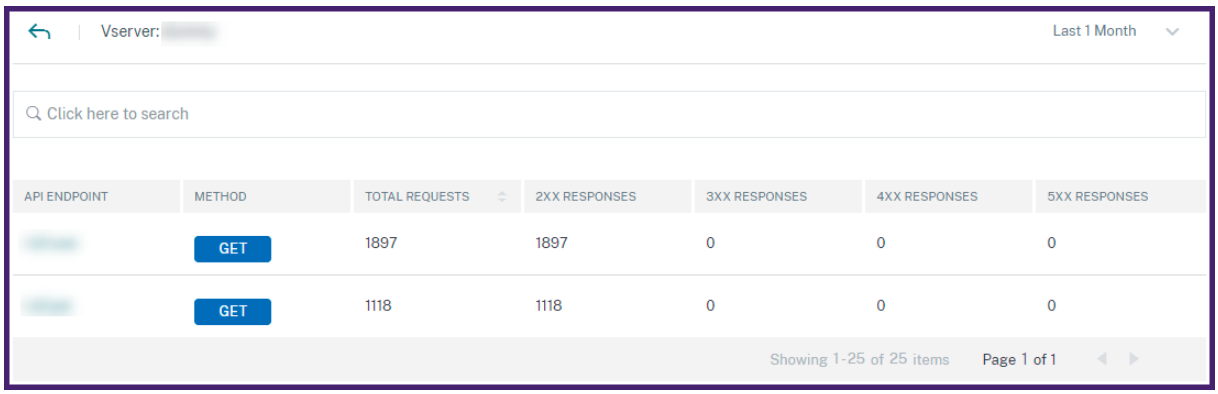
Afficher les points de terminaison API

Dans la **découverte d'API**, lorsque vous sélectionnez un serveur virtuel ou un déploiement d'API, l'interface graphique ADM affiche les points de terminaison de l'API et leurs détails tels que :

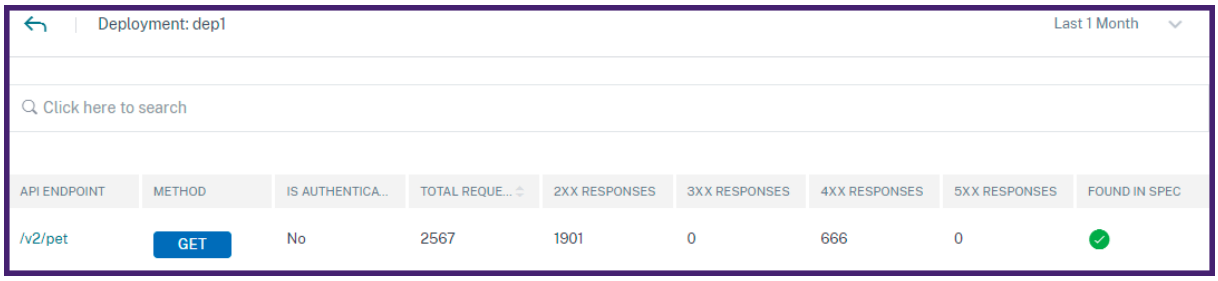
- **Méthode** - Il affiche la méthode utilisée dans un point de terminaison API. Par exemple, `GET` et les `POST` méthodes
- **Total requêtes** - Il affiche le nombre de demandes d'API sur le point de terminaison de l'API.
- **Status de réponse** - Il affiche le nombre pour chaque état de réponse. Par exemple, `2xx`, `3xx`, `4xx`, et `5xx`.

- **Found in Spec** - Cette colonne apparaît uniquement pour les déploiements d'API. Parfois, les API internes qui ne font pas partie de la définition de l'API peuvent recevoir du trafic de l'extérieur. Cette colonne vous permet d'identifier si le point de terminaison de l'API et la méthode observée font partie de la définition de l'API.

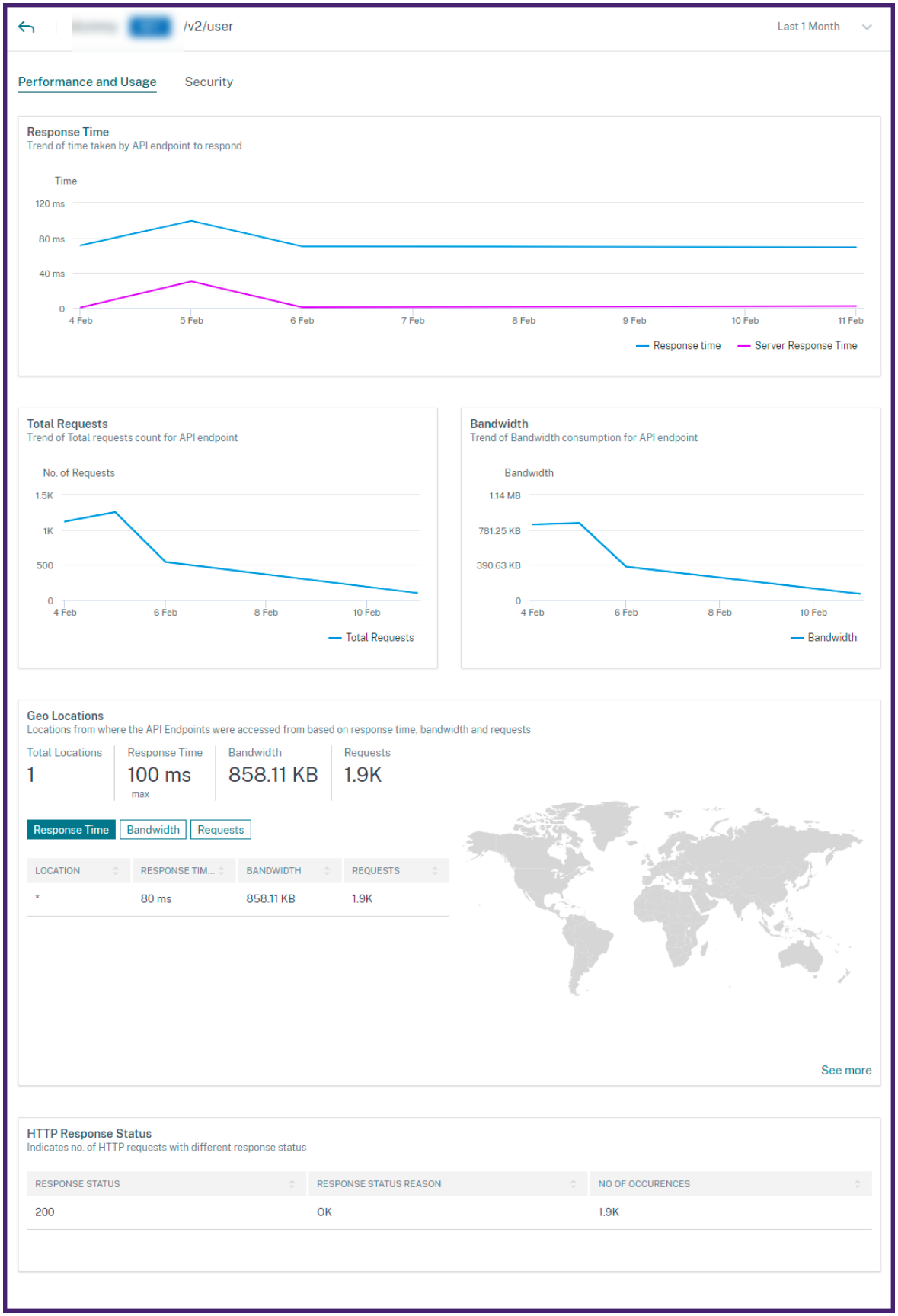
Serveurs virtuels :



Déploiements d'API :



Vous pouvez également sélectionner le point de terminaison API requis pour afficher son rapport d'analyse détaillé.



Pour plus d'informations sur chaque section, reportez-vous à la section Afficher l'analyse de l'API.

Ajouter des stratégies à un déploiement d'API

April 29, 2021

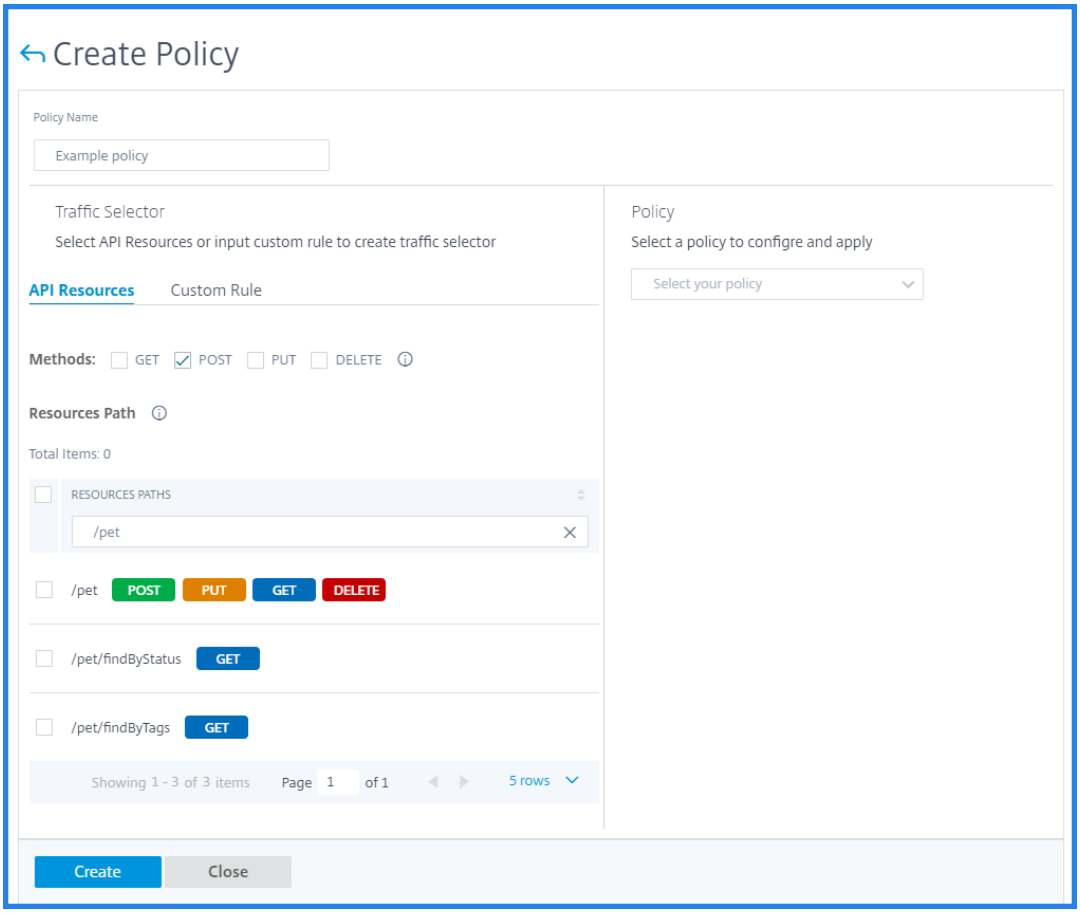
Vous pouvez configurer diverses stratégies de sécurité pour votre trafic API. Cette configuration nécessite que vous spécifiez les critères de sélection du trafic et les paramètres requis pour une stratégie. Procédez comme suit pour ajouter une stratégie à une définition d'API :

1. Accédez à **Applications > Passerelle API > Stratégie**.
2. Cliquez sur **Add**.
3. Spécifiez le nom d'un groupe de stratégies.
4. Sélectionnez un **déploiement** dans la liste.
5. Sélectionnez un **service en amont** dans la liste pour lequel vous souhaitez configurer des stratégies.
6. Cliquez sur **Ajouter** pour sélectionner des sélecteurs de trafic et un type de stratégie.

   Sélecteur de trafic : les critères de sélection du trafic incluent les chemins d'accès des ressources API ou les préfixes de chemin, les méthodes et la stratégie.

   Vous pouvez utiliser l'une des options suivantes pour spécifier des critères de sélection du trafic :

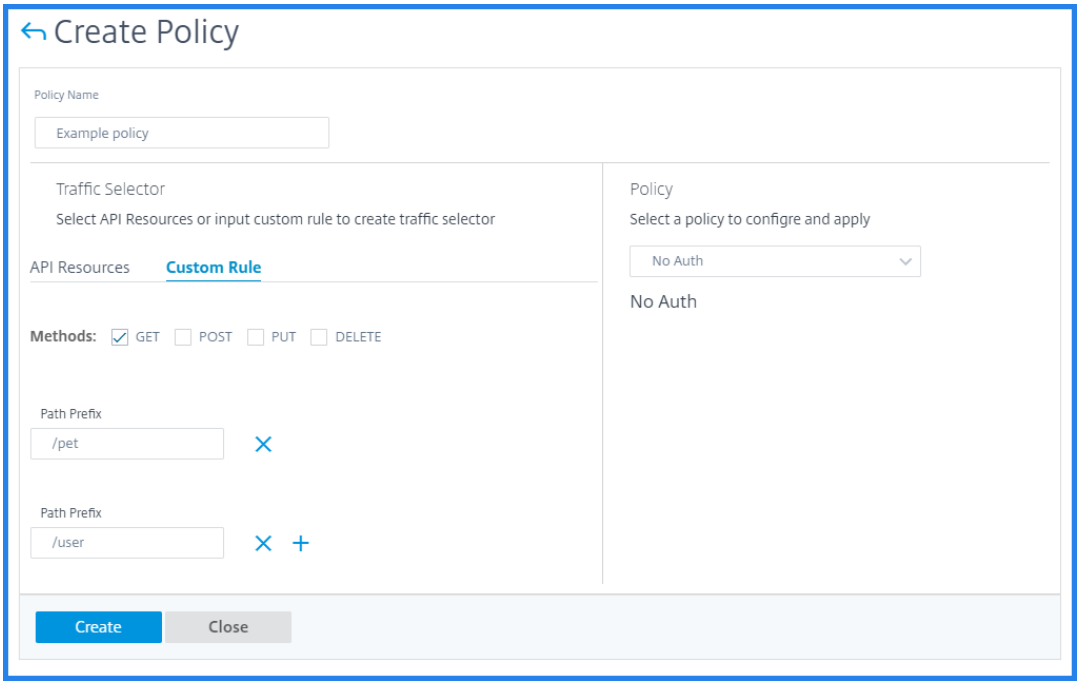
   - **Ressources API** : sélectionnez une ressource API et ses méthodes pour lesquelles vous souhaitez appliquer une stratégie. Vous pouvez rechercher des ressources et des méthodes d'API avec un mot clé.



Dans cet exemple, les ressources API avec `/user` qui ont la `POST` méthode sont répertoriées.

- **Règle personnalisée** : dans cet onglet, vous pouvez spécifier des préfixes de chemin personnalisés et plusieurs méthodes.

  La stratégie configurée s'applique à une demande d'API entrante qui correspond à la règle personnalisée pour la sélection du trafic API.



Dans cet exemple, la stratégie **No-Auth** s'applique aux ressources API qui ont le `/pet` préfixe et la `POST` méthode.

Dans **Stratégie**, sélectionnez une stratégie dans la liste que vous souhaitez appliquer à la ressource et à la méthode API sélectionnées. Pour plus d'informations sur chaque stratégie, reportez-vous à la section Types de stratégie.

7. Facultatif, vous pouvez déplacer des types de stratégie pour définir une priorité. Les types de stratégie ayant une priorité plus élevée s'appliquent en premier.
8. Cliquez sur **Enregistrer** pour ajouter une stratégie. Si vous souhaitez appliquer la stratégie immédiatement, cliquez sur **Enregistrer et appliquer**.

Types de stratégie

Lorsque vous configurez une stratégie API, vous pouvez sélectionner les stratégies suivantes que vous souhaitez appliquer à la ressource et à la méthode API :

- **Authentification et autorisation**
- **Limite de taux**
- **WAF**
- **BOT**
- **Réécriture d'en-tête**

Authentification et autorisation

Les ressources API sont hébergées sur un serveur d'applications ou d'API. Lorsque vous souhaitez appliquer des restrictions d'accès à ces ressources API, vous pouvez utiliser les stratégies d'authentification et d'autorisation. Ces stratégies vérifient si la demande d'API entrante dispose d'une autorisation nécessaire pour accéder à la ressource.

Utilisez les stratégies suivantes pour définir l'authentification et l'autorisation des ressources API sélectionnées :

'No-Auth'

Utilisez cette stratégie pour ignorer l'authentification sur le trafic sélectionné.

'Auth-Basique'

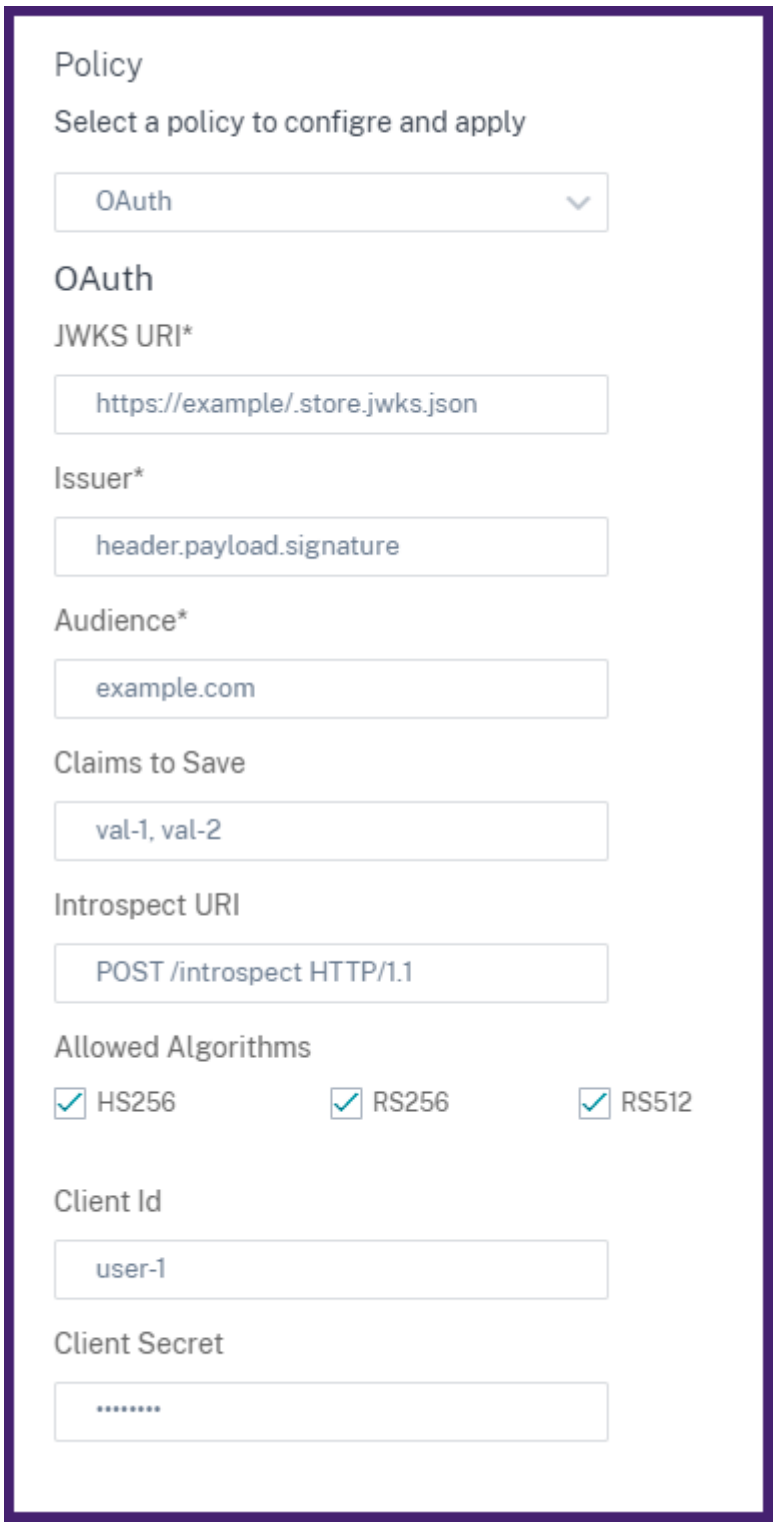
Cette stratégie spécifie l'authentification locale à utiliser avec le schéma d'authentification de base HTTP. Pour utiliser l'authentification locale, vous devez créer des comptes d'utilisateurs sur Citrix ADC.

OAuth

OAuth nécessite un fournisseur d'identité externe pour authentifier un client à l'aide d'OAuth2 et émettre un jeton d'accès. Lorsque le client fournit ce jeton en tant qu'informations d'identification d'accès à une passerelle API, le jeton est validé en fonction des valeurs configurées.

- **URI JWKS** - URL d'un point de terminaison qui a JWK (JSON Web Key) pour la vérification JWT (JSON Web Token)
- **Emetteur** - Identité (généralement une URL) du serveur d'authentification.
- **Audience** - Identité du service ou de l'application pour lequel le jeton est applicable.
- **Revendications à enregistrer** - Les autorisations d'accès sont représentées sous la forme d'un ensemble de revendications et de valeurs attendues. Spécifiez les valeurs de revendication au format CSV.
- **URI Introspect** - URL de point de terminaison introspection du serveur d'authentification. Cette URL est utilisée pour vérifier les jetons d'accès opaques. Pour plus d'informations sur ces jetons, reportez-vous à la section Configuration OAuth pour les jetons d'accès opaques.

  Après avoir spécifié l' **URI Introspect**, spécifiez l' **ID client** et le **secret client** pour accéder au serveur d'authentification.
- **Algorithmes autorisés** - Cette option vous permet de restreindre certains algorithmes dans les jetons entrants. Par défaut, toutes les méthodes prises en charge sont autorisées. Cependant, vous pouvez vérifier les algorithmes requis pour le trafic sélectionné.



En cas de validation réussie, la passerelle API accorde l'accès au client.

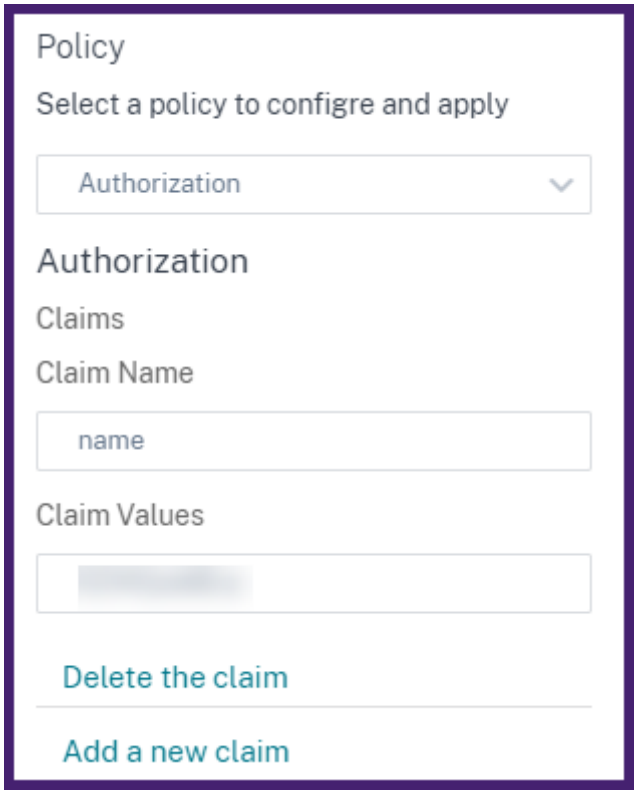
> **Important**

> Lorsque vous configurez un OAuth ou une **Auth-Basic** stratégie pour les ressources API sélectionnées, configurez la **Pas d'Auth** stratégie pour les ressources API restantes. Cette configuration indique explicitement que vous souhaitez ignorer l'authentification pour les ressources restantes.

Autorisation

Cette stratégie vérifie les autorisations requises pour accéder à une ressource API. Les autorisations d'accès sont représentées sous la forme d'un ensemble de revendications et de valeurs attendues. Pour configurer cette stratégie, sélectionnez **Ajouter une nouvelle revendication** et spécifiez les éléments suivants :

- Nom de la réclamation
- Valeurs de réclamation



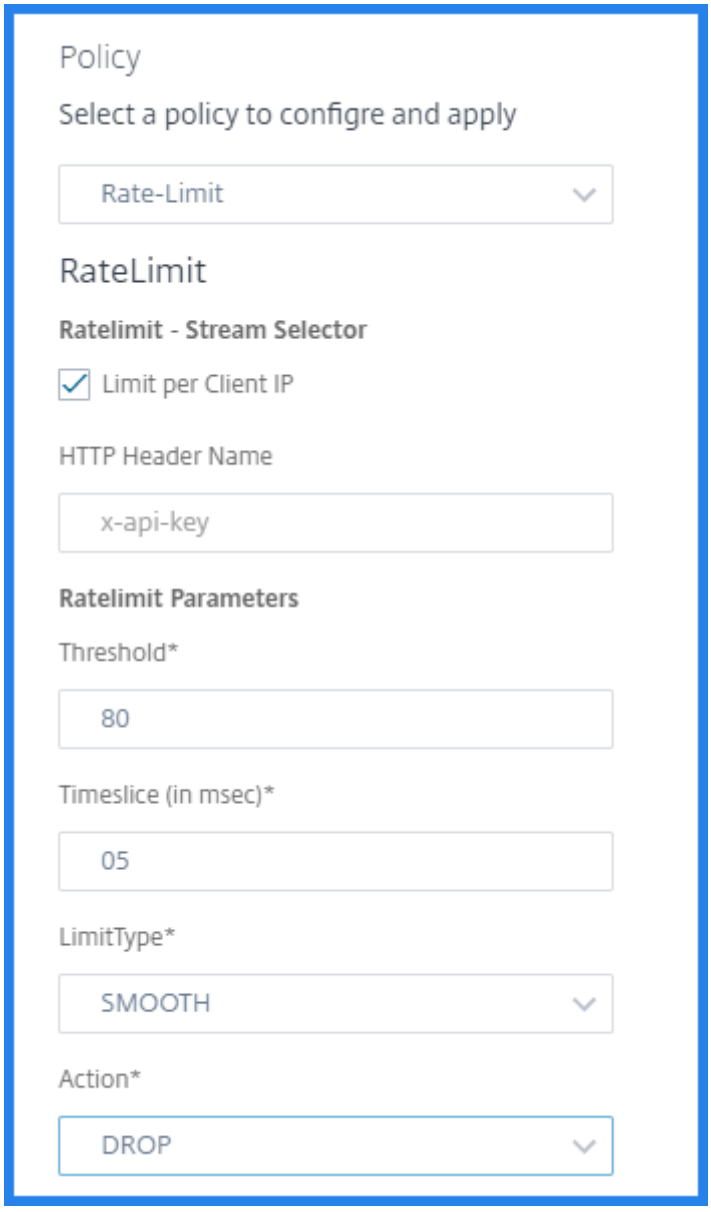
> La passerelle API**importante**
>
> nécessite à la fois des stratégies d'authentification et d'autorisation pour le trafic API. Par conséquent, vous devez configurer une stratégie d'autorisation avec une stratégie d'authentification. La stratégie d'authentification peut être OAuth ou [Auth-Basic] (#auth-basic).
>
> Même si vous n'avez aucune vérification d'autorisation, vous devez créer une stratégie d'autorisation avec des revendications vides. Sinon, la demande est refusée avec une erreur

> 403.

Politique de limite de taux

Spécifiez la charge maximale donnée à la ressource API sélectionnée. Avec cette stratégie, vous pouvez surveiller le taux de trafic de l'API et prendre des mesures préventives. Pour configurer cette stratégie, spécifiez les éléments suivants :

- **Nom d'en-tête HTTP** - Il s'agit d'une clé de sélection de trafic qui filtre le trafic pour identifier les requêtes API. De plus, la stratégie de limite de taux s'applique et surveille uniquement ces demandes d'API.
- **Seuil** : nombre maximal de demandes pouvant être autorisées dans l'intervalle spécifié.
- **Tranche temporelle** - Intervalle spécifié en microsecondes. Pendant cet intervalle, les demandes sont surveillées par rapport aux limites configurées. Par défaut, il est défini sur 1000 microsecondes (1 milliseconde).
- **Type de limite** : mode d'application de la stratégie de limite de taux. Vous pouvez sélectionner **Burst** ou **Lisser** le type de limite.
- **Action** : définit une action que vous souhaitez effectuer sur le trafic qui dépasse le seuil. Vous pouvez spécifier l'une des actions suivantes :
  - **DROP** : Supprime les requêtes au-dessus des limites de trafic configurées.
  - RESET :**Réinitialise**la connexion pour les requêtes.
  - **REDIRECT** : redirige le trafic vers le redirect_url configuré.
  - **RÉPONSE** : Répond avec la réponse standard (`429 Too many requests`).

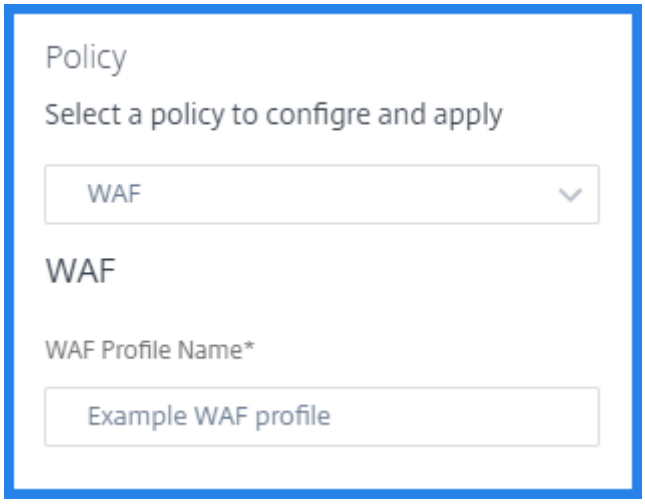


Politique WAF

Cette politique empêche les violations de sécurité, la perte de données et les éventuelles modifications non autorisées des sites Web qui accèdent à des informations sensibles sur les entreprises ou les clients.

Avant de configurer une stratégie WAF, créez un profil WAF dans Citrix ADM à l'aide du StyleBook.

Dans **Nom du profil WAF**, sélectionnez ou spécifiez le profil WAF que vous avez créé.

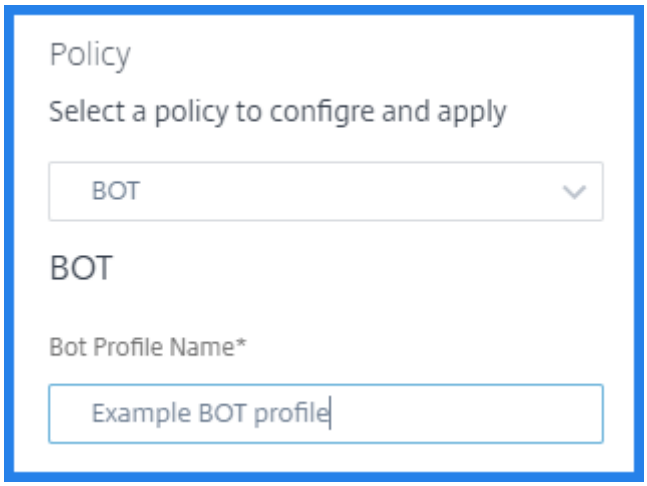


Politique BOT

Cette stratégie identifie les robots défectueux et protège votre appliance contre les attaques de sécurité avancées.

Avant de configurer une stratégie BOT, créez un profil BOT dans Citrix ADM à l'aide du styleBook.

Dans **Nom du profil de bot**, spécifiez le profil BOT que vous avez créé.



Réécriture d'en-tête

Cette stratégie vous aide à modifier l'en-tête des demandes d'API et des réponses. Si vous souhaitez remplacer la valeur dans l'en-tête HTTP, spécifiez ce qui suit :

- **Nom d'en-tête HTTP** : nom de fichier que vous souhaitez modifier dans l'en-tête de la demande.

  Exemple : `Host`

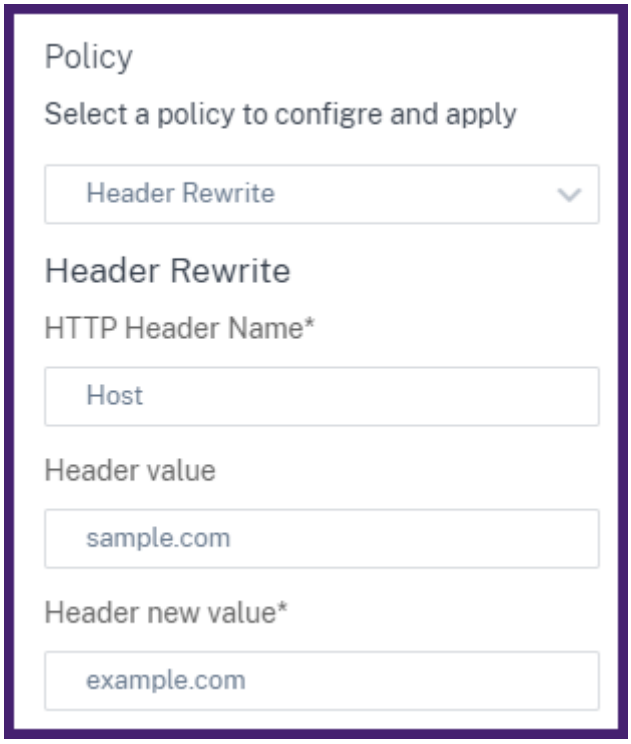
- **Valeur d'en-tête** : Facultatif, chaîne de valeur que vous souhaitez modifier dans le nom d'en-tête spécifié.

  Exemple : `sample.com`

- **Nouvelle valeur d'en-tête** : Nouvelle valeur pour remplacer la valeur d'en-tête spécifiée.

  Si aucune **valeur d'en-tête** n'est spécifiée, elle remplace toute valeur reçue par la valeur spécifiée par le **nom d'en-tête HTTP**.

  Exemple : `example.com`



Dans cet exemple, la stratégie de réécriture d'en-tête remplace `sample.comexample.com` dans le `Host` champ d'une demande d'API.

Graphique de service

April 29, 2021

La fonctionnalité de graphique de service dans Citrix ADM vous permet de surveiller tous les services dans une représentation graphique. Cette fonctionnalité vous permet également d'afficher une analyse détaillée et des mesures exploitables des services. Accédez à **Applications > Graphique de service** pour afficher le graphique de service pour :

- Applications configurées sur toutes les instances Citrix ADC

- Applications Kubernetes
- Applications Web à 3 niveaux

Graphique des services pour les applications sur toutes les instances Citrix ADC

La fonction de graphique de service global vous permet d'obtenir une visualisation holistique de la `clients to infrastructure to application` vue. À partir de cette vue graphique de service à volet unique, en tant qu'administrateur, vous pouvez :

- Comprendre la région à partir de laquelle les utilisateurs accèdent aux applications spécifiques (applications Web à 3 niveaux et applications microservices)
- Visualiser la vue de l'infrastructure (instance Citrix ADC) que la demande du client est traitée
- Comprendre si les problèmes surviennent à partir du client, de l'infrastructure ou de l'application
- Exercer davantage vers le bas pour résoudre le problème

Accédez à **Applications > Service Graph** et cliquez sur l'onglet **Global** pour afficher :

- Détails de bout en bout de toutes les applications connectées du client aux serveurs back-end
- Toutes les instances Citrix ADC connectées à ses centres de données respectifs

  > **Remarque**
  >
  > Vous pouvez afficher les centres de données uniquement si vous disposez d'applications GSLB.

- Informations sur les mesures du client
- Informations sur les mesures Citrix ADC
- Toutes les instances Citrix ADC qui ont des applications discrètes, des applications personnalisées et des applications de microservice distinctes
- Les 4 applications les plus faibles qui appartiennent à des applications personnalisées, des applications discrètes et des applications de microservices
- Informations sur les mesures pour les 4 serveurs virtuels les plus bas cotés
- Les applications (applications discrètes, applications personnalisées et applications de microservices) sont des statuts tels que **Critique**, **Review**, **Bon**et **Non applicable**.

Pour de plus amples informations, consultez la section Vue holistique des applications dans le graphique de service.

Graphique de service pour les applications Kubernetes

Accédez à **Applications > Service Graph** et cliquez sur l'onglet **Microservices** pour afficher :

- Garantir les performances globales des applications de bout en bout
- Identifier les goulots d'étranglement créés par l'interdépendance des différents composants de vos applications
- Recueillir des informations sur les dépendances des différents composants de vos applications
- Surveillance des services au sein du cluster Kubernetes
- Surveiller le service qui présente des problèmes
- Vérifier les facteurs qui contribuent aux problèmes de performance
- Afficher la visibilité détaillée des transactions HTTP de service
- Analyser les mesures HTTP, TCP et SSL
- Afficher les statistiques client et les détails de la synthèse des transactions client

En visualisant ces mesures dans Citrix ADM, vous pouvez analyser la cause première des problèmes et prendre les mesures de dépannage nécessaires plus rapidement. Le graphique de service affiche vos applications dans divers services de composants. Ces services s'exécutant à l'intérieur du cluster Kubernetes peuvent communiquer avec divers composants à l'intérieur et à l'extérieur de l'application. Pour commencer, reportez-vous à la section Configuration d'un graphique de service.

Graphique de service pour les applications Web à 3 niveaux

Accédez à **Applications > Service Graph** et cliquez sur l'onglet **Web Apps** pour afficher :

- Détails sur la configuration de l'application (avec un serveur virtuel de commutation de contenu et un serveur virtuel d'équilibrage de charge)

  Pour les applications GSLB, vous pouvez afficher les serveurs virtuels de centre de données, d'instance ADC, de CS et de LB.
- Transactions de bout en bout du client au service
- Emplacement à partir duquel le client accède à l'application
- Le nom du centre de données où les demandes client sont traitées et les mesures Citrix ADC du centre de données associées (uniquement pour les applications GSLB)
- Détails des mesures pour les serveurs clients, les services et les serveurs virtuels
- Si les erreurs proviennent du client ou du service
- Statut du service, tel que **Critique**, **Révision**et **Bon**. Citrix ADM affiche l'état du service en fonction du temps de réponse du service et du nombre d'erreurs.
  - **Critique (rouge)** - Indique quand le temps de réponse moyen du service > 200 ms ET le nombre d'erreurs > 0

  - **Review (orange)** - Indique quand le temps de réponse moyen du service > 200 ms OU le nombre d'erreurs > 0
  - **Bon (vert)** - Indique aucune erreur et le temps de réponse moyen du service < 200 ms
- Statut du client, tel que **Critique**, **Révision**et **Bon**. Citrix ADM affiche l'état du client en fonction de la latence du réseau client et du nombre d'erreurs.
  - **Critique (rouge)**- Indique lorsque la latence moyenne du réseau client > 200 ms ET le nombre d'erreurs > 0
  - **Review (orange)** - Indique lorsque la latence moyenne du réseau client > 200 ms OU le nombre d'erreurs > 0
  - **Bon (vert)** : indique l'absence d'erreur et la latence moyenne du réseau client < 200 ms
- État du serveur virtuel, tel que **Critique**, **Révision**et **Bon**. Citrix ADM affiche l'état du serveur virtuel en fonction du score de l'application.
  - **Critique (rouge)** : indique quand le score de l'application est < 40
  - **Avis (orange)** - Indique quand le score de l'application est compris entre 40 et 75
  - **Bon (vert)** - Indique lorsque le score de l'application est > 75

Points à noter :

- Seuls les serveurs virtuels d'équilibrage de charge, de commutation de contenu et de GSLB sont affichés dans le graphique de service.
- Si aucun serveur virtuel n'est lié à une application personnalisée, les détails ne sont pas visibles dans le graphique de service de l'application.
- Vous pouvez afficher les mesures pour les clients et les services dans le graphique de service uniquement si des transactions actives se produisent entre les serveurs virtuels et l'application Web.
- Si aucune transaction active n'est disponible entre les serveurs virtuels et l'application Web, vous pouvez uniquement afficher les détails dans le graphique de service en fonction des données de configuration telles que l'équilibrage de charge, la commutation de contenu, les serveurs virtuels GSLB et les services.
- Si des modifications ont été apportées à la configuration de l'application, cela peut prendre 10 minutes pour refléter dans le graphique de service.

Pour de plus amples informations, consultez la section Graphique de service pour les applications.

Configuration d'un graphique de service

April 29, 2021

Configuration logicielle requise

Distribution Kubernetes	Version Kubernetes	Interfaces réseau de conteneurs (CNI)	Version CPX	Version CIC	Version de l'agent Citrix ADM
Open source	v1.16.3	Flanelle, Calico ou Canal	13.0—47.103 ou ultérieur	1.6.1 ou version ultérieure	13.0—49.x ou version ultérieure

Vous pouvez configurer le cluster Kubernetes avec divers topologies de déploiement et le tableau suivant fournit les topologies qui sont prises en charge dans le graphique de service :

Topologie	Graphique de service pris en charge
Une entrée unifiée ou unifiée	Oui
Double niveau	Oui
Cloud	Oui, mais l'équilibreur de charge dans le nuage n'est pas affiché dans le graphique
Service mesh lite	Oui
Service mesh	Oui
Services de type LoadBalancer	Non
Services de type NodePort	Non

Pour terminer la configuration du graphique de service dans Citrix ADM, cliquez sur le type de topologie que vous avez configuré pour votre cluster Kubernetes et effectuez les procédures mentionnées :

- Topologie d'entrée unifiée ou unifiée
- Topologie à deux niveaux ou Service Mesh Lite
- Topologie de maillage de service

> **Remarque**
>
> La procédure de configuration du graphique de service pour les topologies à double niveau et service mesh lite reste la même.

Topologie d'entrée unifiée ou à niveau unique

Assurez-vous de suivre les étapes suivantes pour configurer la topologie d'entrée unifiée ou unique niveau. Pour de plus amples informations, consultez la section Procédures détaillées pour configurer la topologie d'entrée unifiée ou unique.

- Cluster Kubernetes configuré avec topologie d'entrée unique ou unifiée.
- Ajout Instance VPX, MPX, SDX, BLX dans Citrix ADM et activé **Web Insight**.
- Ajouté Cluster Kubernetes dans Citrix ADM.

Topologie à deux niveaux ou Service Mesh Lite

Assurez-vous de suivre les étapes suivantes pour configurer la topologie à double niveau ou service mesh lite. Pour de plus amples informations, consultez la section Procédures détaillées pour configurer la topologie à double niveau ou service mesh lite.

- Cluster Kubernetes configuré avec l'une des topologies prises en charge.
- Installez un Agent Citrix ADM et configuré pour activer la communication entre Citrix ADM et Kubernetes cluster ou instances gérées dans votre datacenter ou cloud.

  Vous pouvez également déployer un agent Citrix ADM en tant que microservice. Pour plus d'informations, consultez la **section Installer Citrix ADM Agent** dans Mise en route.
- Configuration Routes statiques sur l'agent Citrix ADM pour activer la communication entre Citrix ADM et Citrix ADC CPX.

  > **Remarque**
  >
  > Vous pouvez ignorer cette procédure si vous avez déployé l'agent Citrix ADM en tant que microservice dans le même cluster.
- Téléchargé exemples de fichiers de déploiement depuis le dépôt GitHub.
- Ajouté paramètres requis dans le fichier CPX YAML pour garantir l'enregistrement CPX avec Citrix ADM.
- Ajout d'un Instance VPX, MPX, SDX ou BLX dans Citrix ADM.
- Ajout du Cluster Kubernetes dans Citrix ADM.
- Déployé exemple d'application microservicea.

- Déployé Citrix ADC CPX et enregistré CPX auprès de ADM (applicable uniquement pour l'architecture à deux niveaux).
- Activé Sélection automatique des serveurs virtuels pour concéder une licence aux serveurs virtuels CPX.
- Activé Paramètres de transaction Web et de transaction TCP sur **All** for Citrix ADM agent pour obtenir les transactions HTTP et TCP.
- Envoyé trafic aux microservices.

Topologie de maillage de service

Assurez-vous de suivre les étapes suivantes pour configurer la topologie de maillage de service. Pour de plus amples informations, consultez la section Procédures détaillées pour configurer la topologie de maillage de service.

- Version de cluster Kubernetes configurée `1.14.0` avec l'une des topologies de maillage de service suivantes :
  - Citrix ADC CPX en tant que proxy sidecar pour Istio
  - Citrix ADC en tant que passerelle d'entrée pour Istio

  Pour de plus amples informations, consultez Architecture de déploiement de l'adaptateur Citrix ADC Istio
- API `admissionregistration.k8s.io/v1beta1` activée. Vous pouvez vérifier l'API en utilisant :

  ```
  kubectl api-versions | grep admissionregistration.k8s.io/v1beta1
  ```

  La sortie suivante indique que l'API est activée :

  ```
  admissionregistration.k8s.io/v1beta1
  ```
- Istio installé `istio v.1.3.0`.
- Installé Helm version 3.x.
- Installez un Agent Citrix ADM et configuré pour activer la communication entre Citrix ADM et Kubernetes cluster ou instances gérées dans votre datacenter ou cloud.

  Vous pouvez également déployer un agent Citrix ADM en tant que microservice. Pour plus d'informations, consultez la **section Installer Citrix ADM Agent** dans Mise en route.
- Configuration Routes statiques sur l'agent Citrix ADM pour activer la communication entre Citrix ADM et Citrix ADC CPX.

> **Remarque**
>
> Vous pouvez ignorer cette procédure si vous avez déployé l'agent Citrix ADM en tant que microservice dans le même cluster.

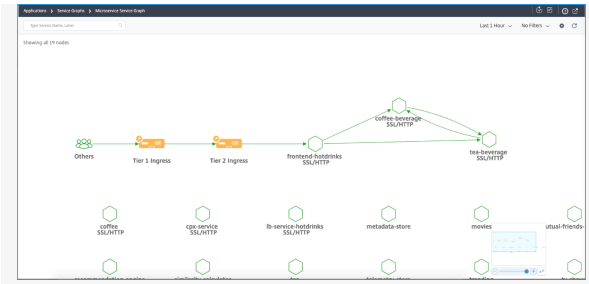
- Configurez le paramètres requis pour remplir les données de topologie de maillage de service.
- Déployé exemple d'applicationa.
- Ajout du Cluster Kubernetes dans Citrix ADM.
- Activé Sélection automatique des serveurs virtuels pour la licence des serveurs virtuels.
- Activé Paramètres de transaction Web et de transaction TCP sur **All** for Citrix ADM agent pour obtenir les transactions HTTP et TCP.
- Envoyé trafic aux microservices.

Après avoir terminé les procédures de configuration requises, vous pouvez afficher le graphique de service renseigné dans **Applications** > **Graphique de service** et dans l'onglet **Microservices**. Pour de plus amples informations, consultez la section Détails du graphique de service.

Afficher les détails dans le graphique de service

April 29, 2021

Après avoir ajouté le cluster Kubernetes dans Citrix ADM, il faut environ 10 minutes pour obtenir les données remplies dans le graphique de service. Accédez à **Application** > **Service Graph** et cliquez sur l'onglet **Microservices** pour afficher les détails du graphique de service.

Topologie à deux niveaux de service Mesh Lite	Topologie d'entrée unifiée à un seul page/unifié
	

- **Tier 1** : Citrix Ingress Controller dans le cluster Kubernetes configure une instance Citrix ADC (VPX/MPX/SDX/BLX) en dehors du cluster Kubernetes.
- **Tier 2** : Citrix Ingress Controller s'exécute en tant que sidecar avec l'instance Citrix ADC CPX dans

le cluster Kubernetes.

- **Ingress** : affiche pour toutes les autres topologies de déploiement.

Tableau de bord graphique de service

1 - Carte réseau de bout en bout de votre application qui montre comment vos services de composants communiquent

2 — Graphique qui indique les résultats et les erreurs pour une durée de temps spécifique

3 — Barre de recherche pour rechercher des services

4 — Liste de temps pour sélectionner la durée de l'heure

5 - Appliquer des filtres aux services d'affichage

6 — Icône de réglage

7 — Zoom avant et zoom arrière vue

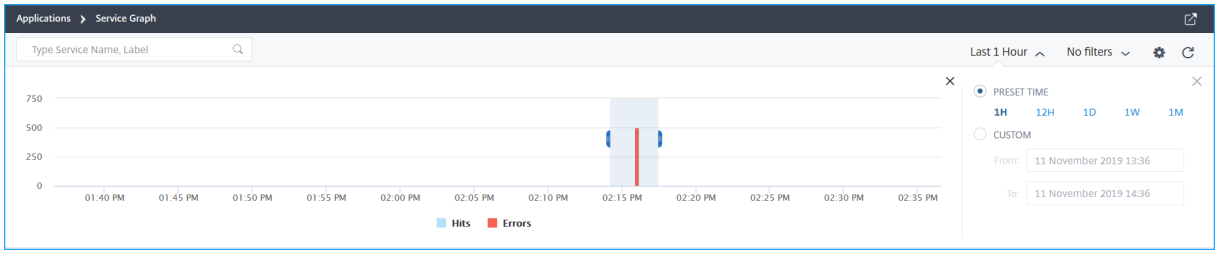
8 — Vue graphique ou vue tabulaire

En fonction de la durée sélectionnée, vous pouvez afficher le graphique de service.

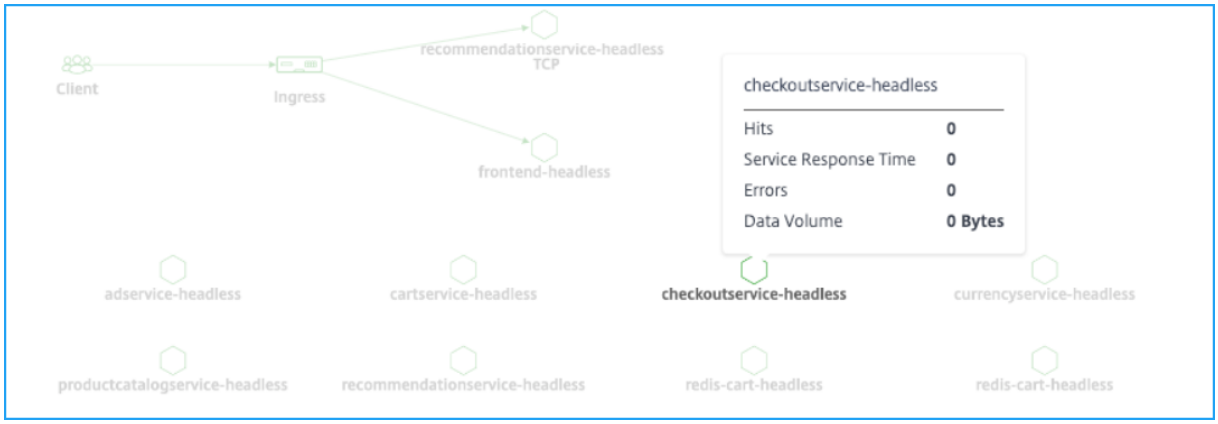
Icône Service	Description
	La largeur de l'arête indique le nombre de coups. Plus la largeur d'arête est grande ou supérieure, indique que le nombre de coups est plus élevé.
	Le service avec une icône d'avertissement indique que le service a des erreurs.
	Le service avec une icône de chronomètre indique que le service présente des problèmes de latence ou de temps de réponse.
	Le service avec des icônes de chronomètre et d'avertissement indique que le service présente à la fois des erreurs et des problèmes de latence/temps de réponse.

> **Remarque**
>
> Si un service n'a pas d'icône d'avertissement ou de chronomètre, il indique que le service présente des anomalies ou une rupture de seuil pour les Hits.

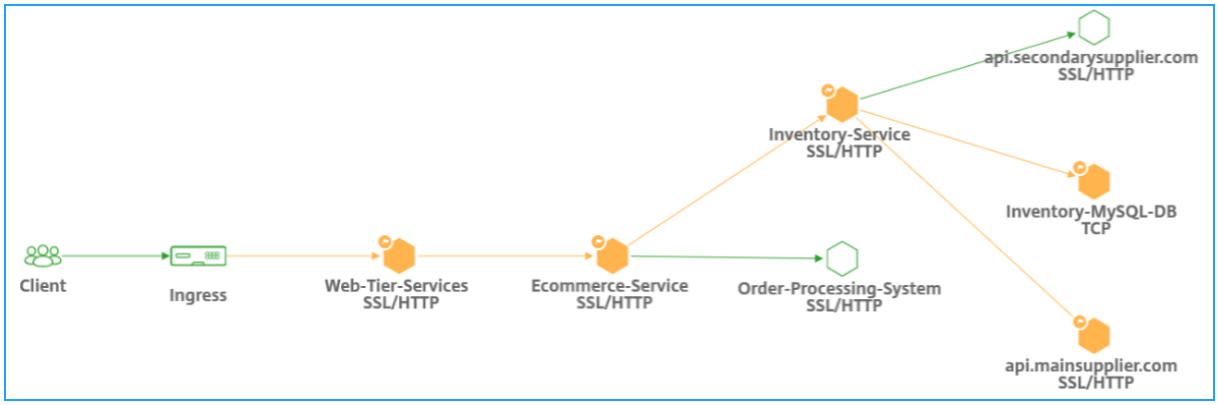
Sélectionnez dans le graphique la période qui indique les résultats à explorer plus bas pour plus d'informations.



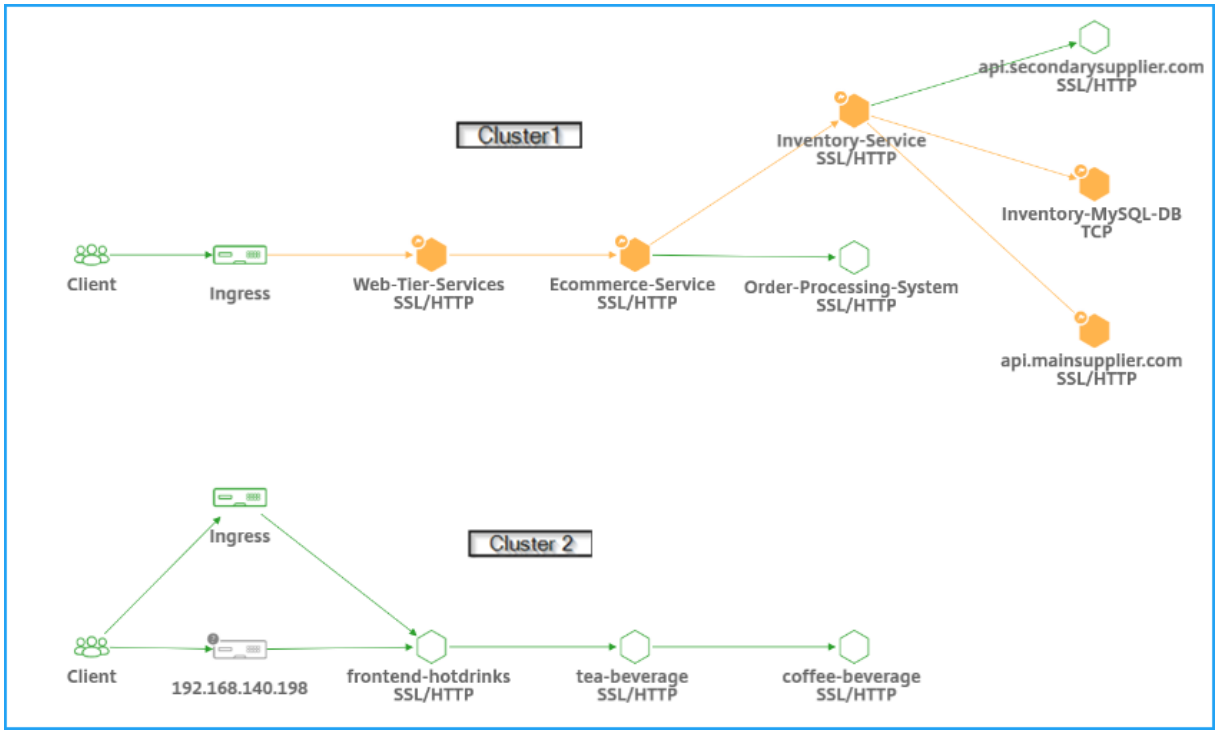
> **Remarque**
>
> Si aucune transaction active n'a été reçue par Citrix ADM, vous pouvez afficher uniquement les services qui sont équilibrés par l'instance Citrix ADC. Lorsque vous placez le pointeur de la souris sur un service, toutes les mesures sont affichées sous la forme 0.



Le graphique de service est maintenant affiché avec le protocole utilisé par les services. Considérez que vous avez les services suivants en cours d'exécution dans votre cluster Kubernetes, comme illustré dans l'image :



> **Remarque**
>
> Si vous avez ajouté plusieurs clusters dans **Orchestration** > **Kubernetes** > **Clusters**, vous pouvez afficher les services associés à chaque cluster.



Vous pouvez afficher l'état suivant pour vos services :

- **Critique (rouge)** - Le service présente des anomalies ou une rupture de seuil dans plusieurs mesures. Pour les seuils par défaut, l'état critique indique le temps moyen de réponse du service > 200 ms ET le nombre d'erreurs > 0
- **Review (orange)** - Le service présente des anomalies ou une violation de seuil dans l'une des mesures. Pour les seuils par défaut, l'état Review indique le temps moyen de réponse du service > 200 ms OU le nombre d'erreurs > 0
- **Bon (vert)** - Service sans anomalie ou sans rupture de seuil. Pour les seuils par défaut, Bon état indique l'absence d'erreur et le temps moyen de réponse du service < 200 ms

  Pour plus d'informations sur les anomalies, reportez-vous à la section Surveillez les services à l'aide des mesures du signal doré.

  Pour plus d'informations sur les seuils, reportez-vous à la section Configurer les seuils dans le graphique de service.

Les protocoles suivants vous permettent d'identifier le protocole utilisé par un service :

- **TCP** : indique que le service utilise le protocole TCP.
- **SSL, HTTP** : indique que le service utilise le protocole SSL sur HTTP.
- **SSL, TCP** — Indique que le service utilise le protocole SSL sur TCP.

> **Remarque**
>
> Le service sans protocole indique que le service utilise le protocole HTTP.

Afficher les tendances des mesures clés à l'aide de la vue tabulaire

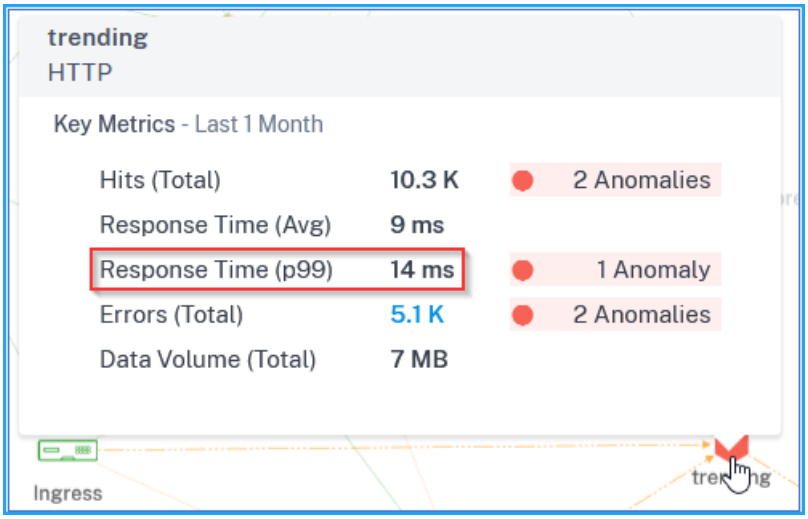
En utilisant la vue tabulaire, vous pouvez voir :

- Mesures clés pour le service
- Mesures clés entre un service source et un service de destination

En tant qu'administrateur, à l'aide de ces mesures clés, vous pouvez analyser les tendances des signaux dorés pour la durée sélectionnée. Pour de plus amples informations, consultez la section Afficher les détails du service.

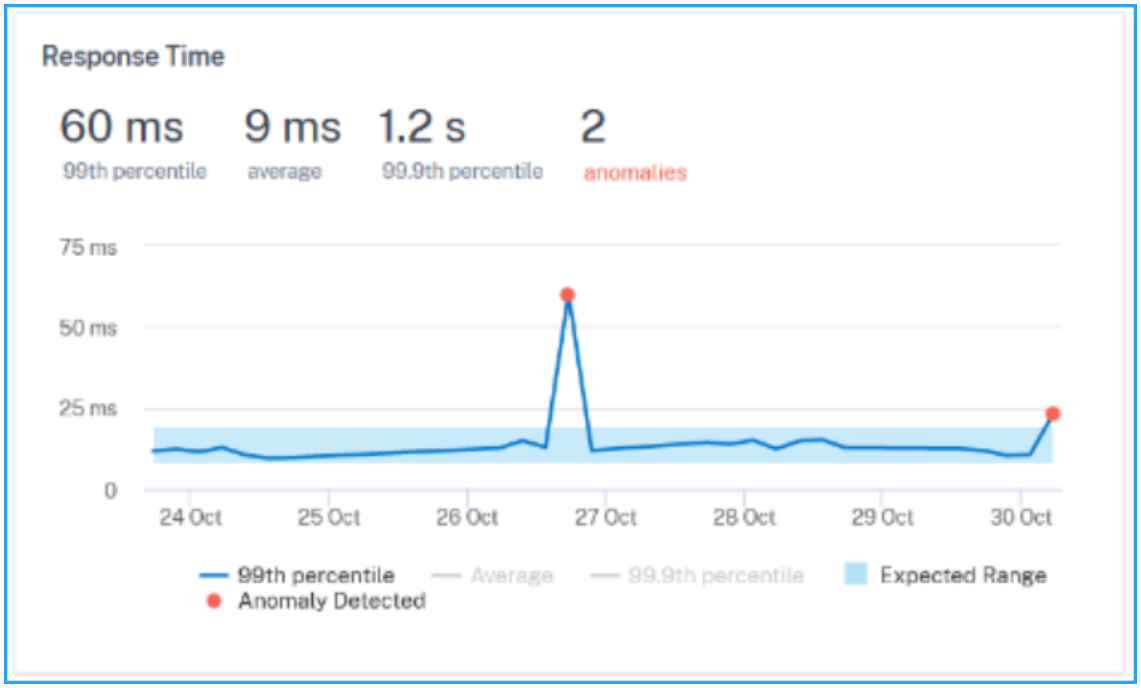
Afficher la valeur Pxx pour le temps de réponse du service

Placez le pointeur de la souris sur un service pour afficher la valeur Pxx pour le temps de réponse.



Temps de réponse (P99) : indique que 99 % des demandes pour la durée sélectionnée sont inférieures à la valeur P99.

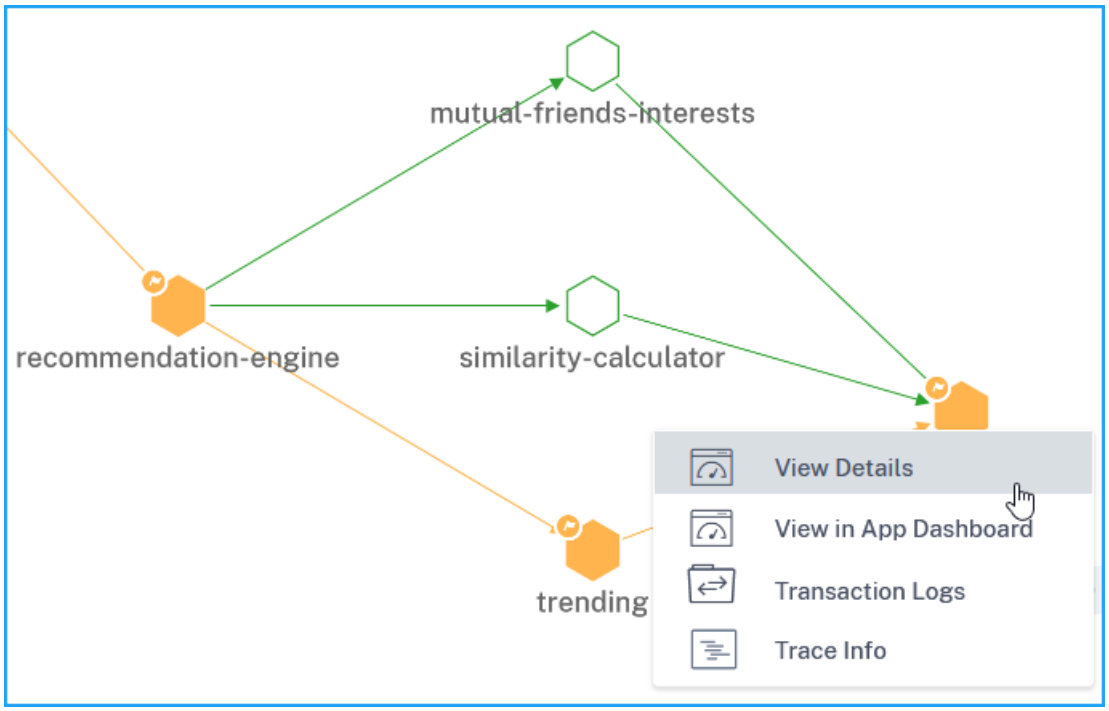
Lorsque vous effectuez une hiérarchisation vers le bas pour afficher les détails du service, vous pouvez également afficher le 99e centile et le 99,9e centile du temps de réponse pour la durée sélectionnée.



En tant qu'administrateur, en utilisant la valeur pxx, vous pouvez mieux comprendre le temps de réponse du service. Pour de plus amples informations, consultez la section Afficher les détails du service.

Afficher les détails du service

Cliquez sur un service pour afficher les options suivantes :

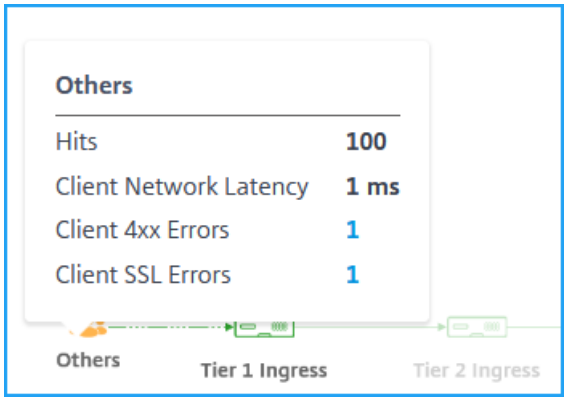


- **Afficher les détails** - Permet d'afficher les détails du service, tels que l'espace de noms, les étiquettes, le cluster où le service est hébergé, etc. Pour de plus amples informations, consultez la section Afficher les détails du service.
- **Afficher dans le tableau de bord des applications** : permet d'afficher les détails de l'application sélectionnée, tels que le score de l'application, les détails du service Kubernetes, les détails du module, etc. Pour de plus amples informations, consultez Détails de l'application Kubernetes
- **Journaux de transactions** - Permet d'afficher les détails des transactions HTTP et SSL sur HTTP. Pour de plus amples informations, consultez la section Afficher les analyses pour les transactions Web.
- **Trace Info** - Permet d'afficher le suivi distribué du service. Pour de plus amples informations, consultez la section Suivi distribué.

Afficher les mesures client

Vous pouvez afficher à partir de quel emplacement le client accède au service. En tant qu'administrateur, vous pouvez visualiser les mesures client et analyser les problèmes qui se produisent à partir du client.

Placez le pointeur de la souris sur une région cliente pour afficher les mesures.



- **Hits** - Indique le nombre total d'accès reçus par le client.
- **Latence réseau client** - Indique la latence moyenne du réseau client.
- **Erreurs client 4xx** - Indique le total des erreurs 4xx client.
- **Erreurs SSL client** - Indique le nombre total d'erreurs SSL client.

Blocs IP dans Citrix ADM - Citrix ADM peut reconnaître l'emplacement du client si le client utilise une adresse IP publique. Citrix ADM possède son fichier CSV d'emplacement intégré qui correspond à l'emplacement basé sur la plage d'adresses IP du client.

Citrix ADM peut reconnaître l'emplacement du client avec une adresse IP privée uniquement lorsque l'adresse IP est ajoutée au serveur Citrix ADM. Par exemple, si l'adresse IP du client appartient à une plage d'adresses IP privée associée à la ville A, Citrix ADM reconnaît que le trafic provient de la ville A pour ce client.

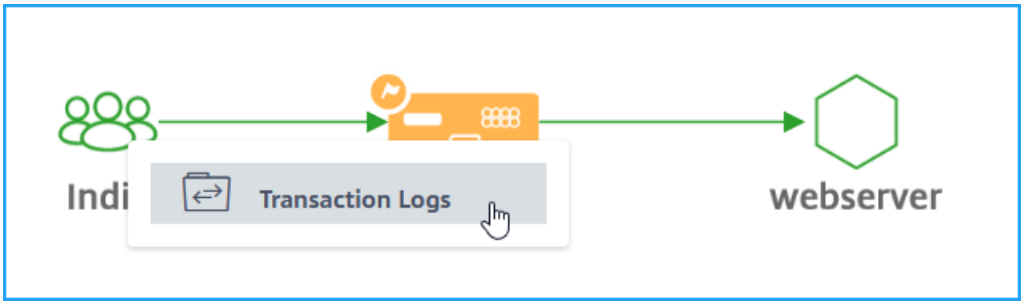
Pour de plus amples informations, consultez la section Créer un bloc IP privé.

Afficher le résumé des transactions client

Le résumé détaillé des transactions client vous permet d'afficher :

- Temps de réponse > 500 ms
- erreurs 5xx

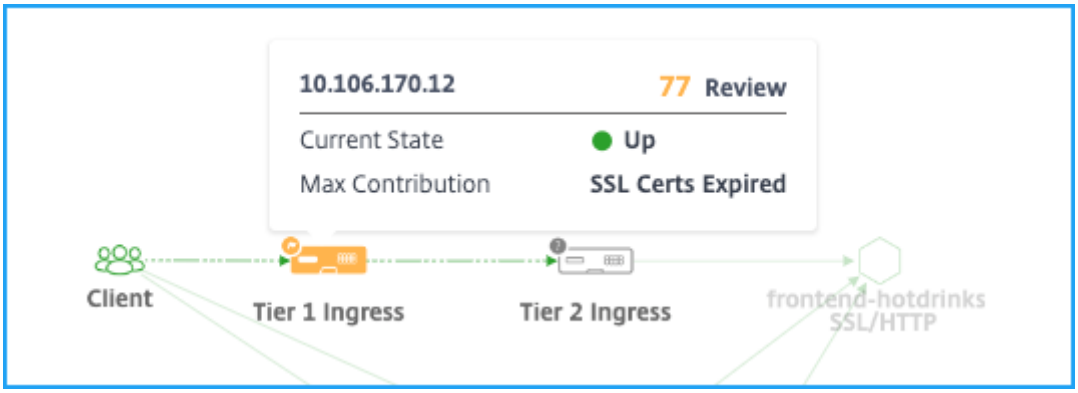
Cliquez sur un emplacement client et sélectionnez **Journaux de transactions**.



Pour de plus amples informations, consultez la section Analyse des transactions Web.

Afficher les mesures d'entrée

Vous pouvez afficher le type d'entrée utilisé dans le cluster Kubernetes.



- Adresse IP Citrix ADC et son score
- **État actuel** — Indique si l'instance Citrix ADC est Hors, Down ou Hors état
- **Contribution maximale** : indique le problème qui affecte le score d'instance

Pour la topologie à un seul niveau, vous ne pouvez afficher qu'une **entrée**unique.

Cliquez sur l' **entrée** pour approfondir l'exploration vers le bas pour plus de détails. Pour de plus amples informations, consultez la section Afficher les détails d'entrée pour résoudre les problèmes.

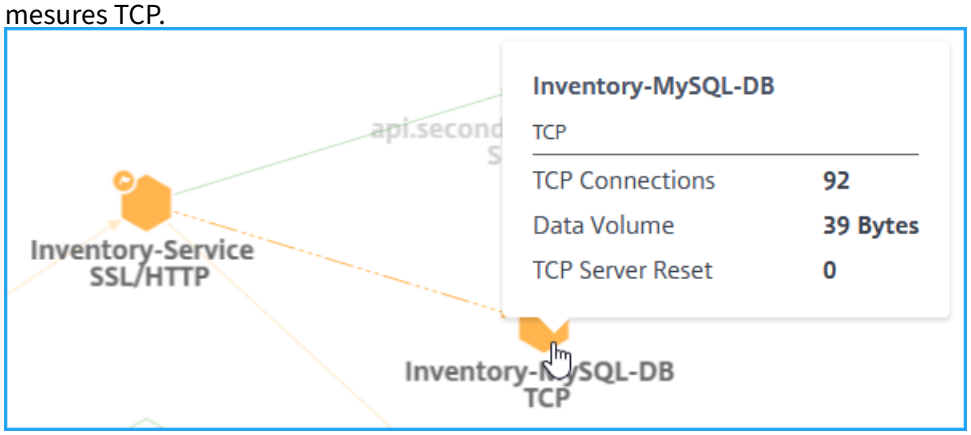
Afficher les mesures TCP et SSL

À l'aide des mesures TCP et SSL, vous pouvez :

- Afficher les détails de connexion TCP entre les services
- Déterminer si les problèmes liés à TCP proviennent du service source ou de destination
- Afficher si l'erreur SSL provient du service source ou de destination
- Afficher la version du protocole SSL utilisée par les services SSL

Mesures TCP

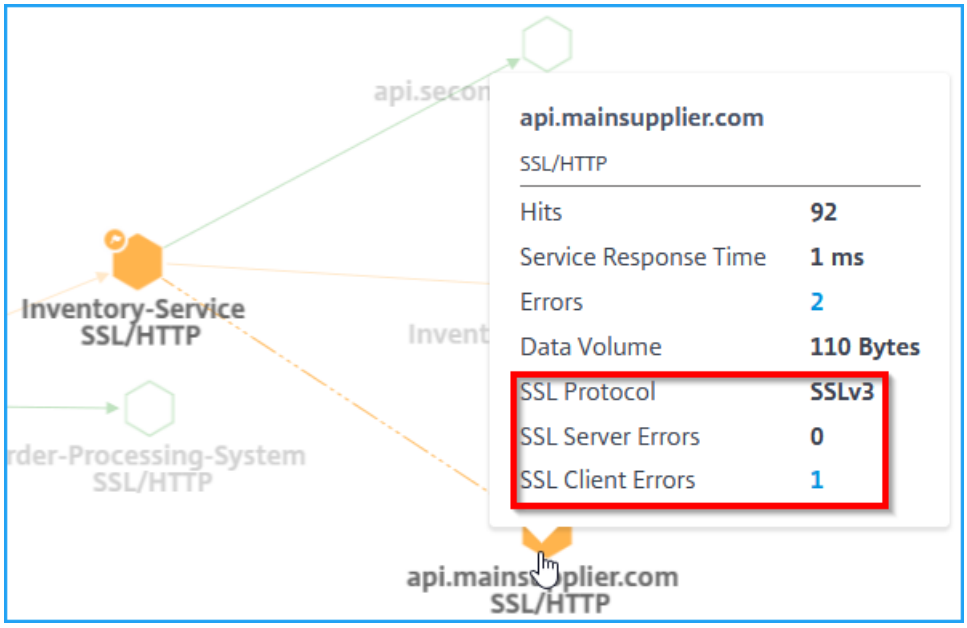
Placez le pointeur de la souris sur un service TCP ou son service entrant associé pour afficher les mesures TCP.



- **Connexions TCP** — Nombre total de connexions établies entre les services
- **Volume de données** — Total des données traitées par le service
- **Réinitialisation du serveur TCP : réinitialisations** TCP totales lancées à partir du serveur

Mesures SSL

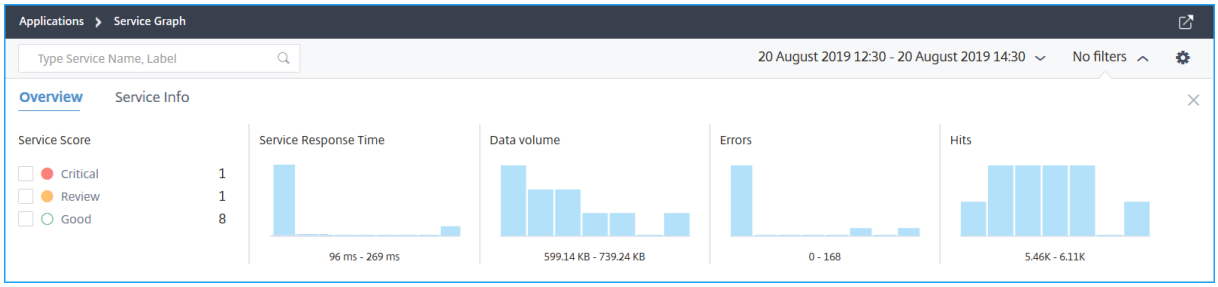
Placez le pointeur de la souris sur un service qui utilise le protocole SSL pour afficher les mesures SSL.



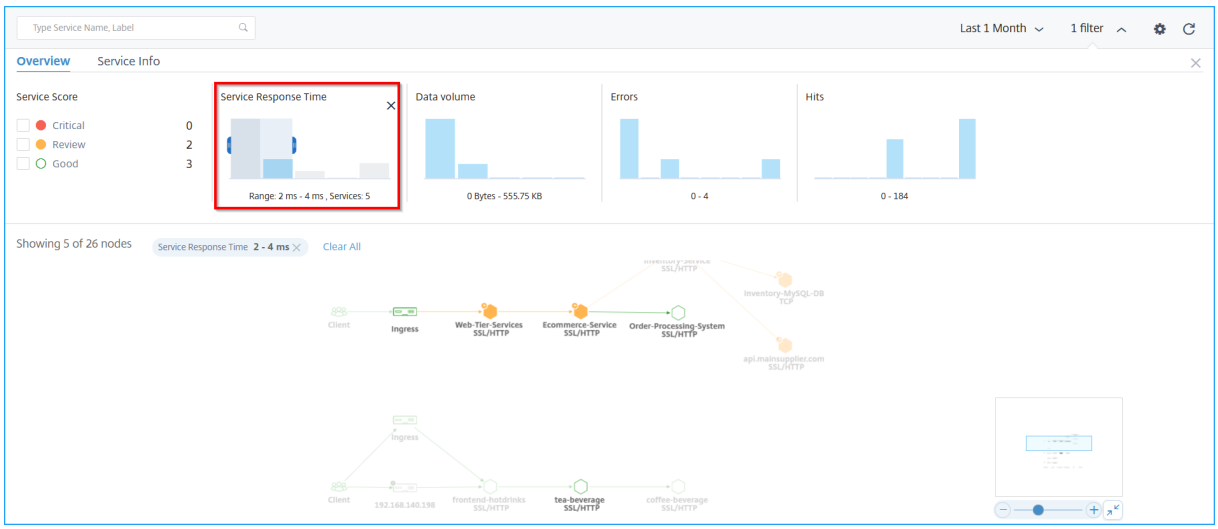
- **Erreurs du serveur SSL** : indique le nombre total d'erreurs SSL du serveur. (Par exemple, certificat SSL inconnu)
- **Protocole SSL** — Indique la version du protocole SSL utilisée par le service
- **Erreurs du client SSL** - Indiquez le total des erreurs SSL du client. (Par exemple, erreur d'authentification du client SSL)

Appliquer les filtres

Vous pouvez appliquer des filtres pour afficher des informations de service spécifiques. Cliquez sur la liste **Aucun filtre** pour obtenir les options de filtre.

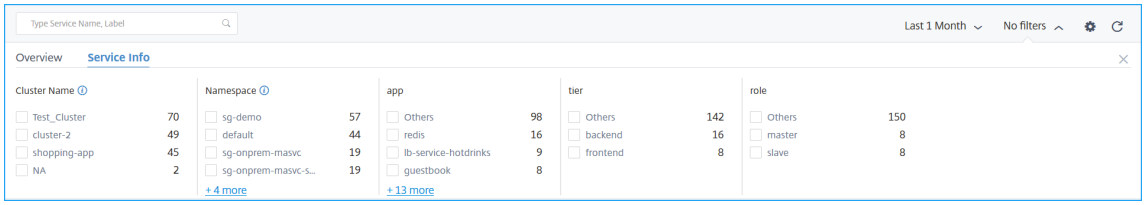


Par exemple, si vous souhaitez afficher les services dont la latence est inférieure à 150 ms, cliquez sur le graphique à barres sous **Temps de réponse du service** pour afficher les résultats.



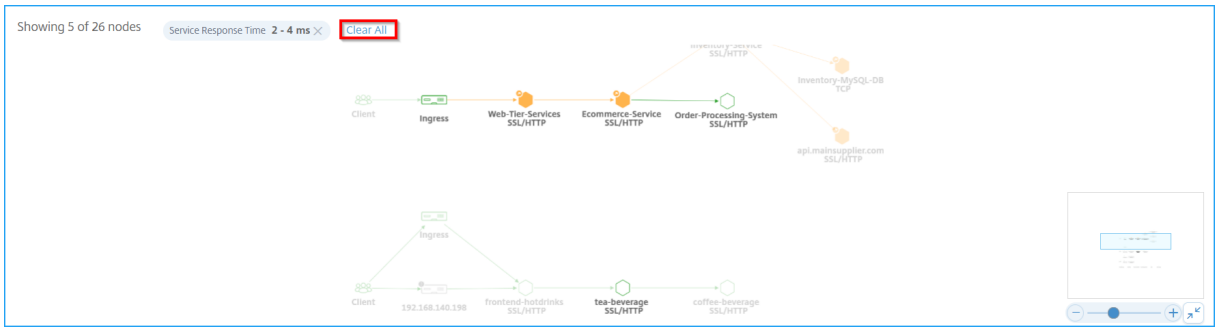
Cliquez sur **Infos sur le service** pour sélectionner et appliquer des filtres pour :

- **Cluster** : affiche tous les services applicables au ou aux clusters sélectionnés.
- **Espace de noms** : affiche tous les services applicables à l'espace de noms sélectionné.

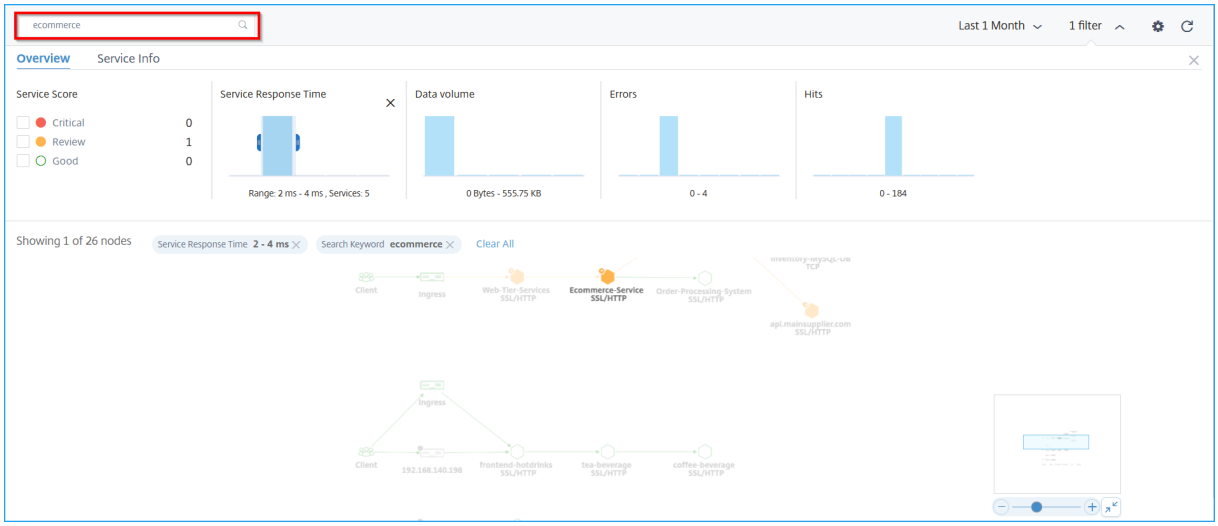


> Remarque
>
> Selon les étiquettes configurées pour le service dans la définition du service YAML de définition de service Kubernetes, vous pouvez également afficher d'autres options de filtre.

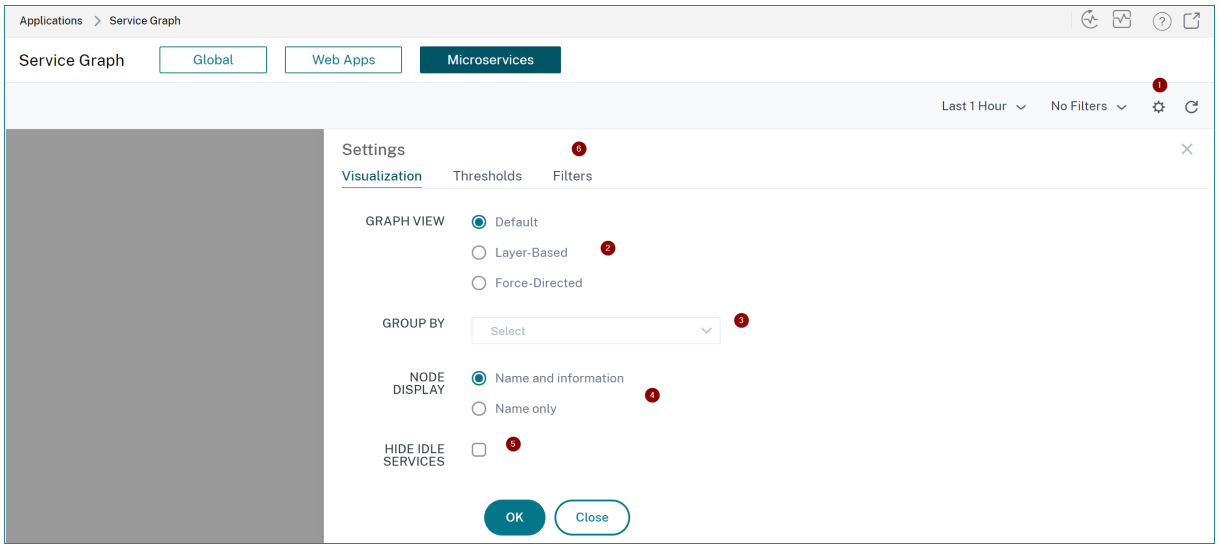
Cliquez sur **Effacer tout** pour effacer tous les filtres.



Vous pouvez également utiliser la zone de texte de recherche et taper un nom de service pour afficher les résultats sur le graphique de service.



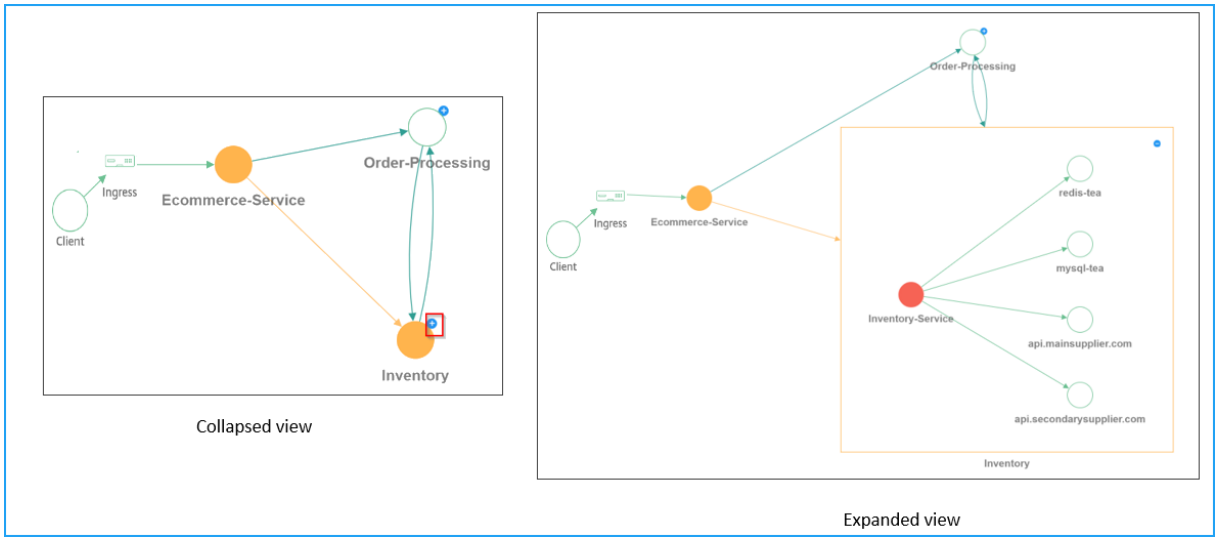
Utilisation de l’option Paramètres



1 — Icône Paramètres

2 — Options permettant d’afficher le graphique de service sous la forme de vues par défaut, Basé sur couche ou Force-Directed

3 — Sélectionnez les options dans la liste pour afficher les services en fonction des catégories. Après avoir sélectionné une catégorie dans la liste, cliquez sur **+** sur le graphique pour afficher tous les services

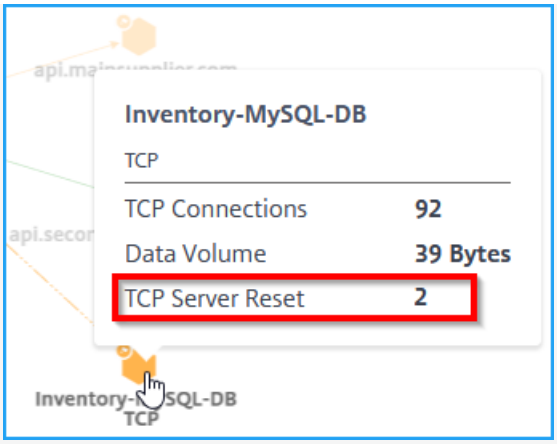


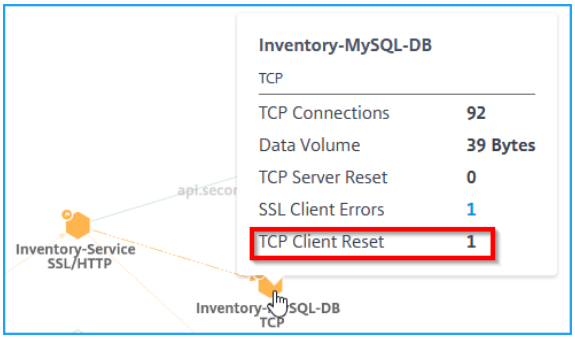
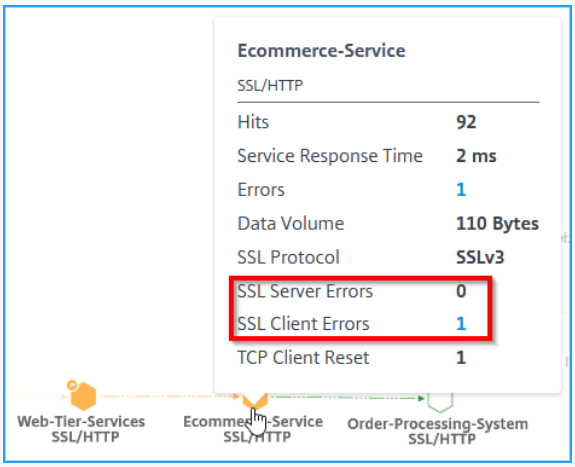
4 — Permet de sélectionner l'option sur la façon dont vous souhaitez afficher les services.

5 - Options pour enregistrer les paramètres ou pour réinitialiser la valeur par défaut.

Analyser les erreurs

Placez le pointeur de la souris sur un service qui indique des erreurs.

Error	Description
	La **réinitialisation du serveur TCP** indique le total des réinitialisations TCP initiées à partir du serveur.

Error	Description
	La **réinitialisation du client TCP** indique le total des réinitialisations TCP initiées par le client.
	Les erreurs du client SSL indiquent le nombre total d'erreurs SSL provenant du client. (Par exemple, erreur d'authentification du client SSL). Erreurs du serveur SSL Indiquez le total des erreurs SSL du serveur. (Par exemple, certificat SSL inconnu)

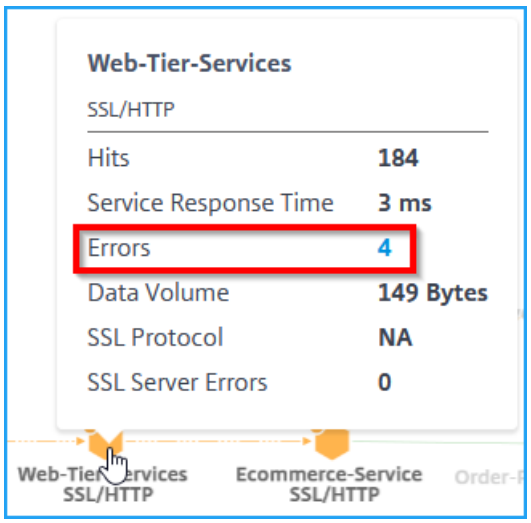
Remarque

- Le nombre d'erreurs client (quel que soit le type de protocole) s'affiche dans n'importe quel service si le nombre d'erreurs client est égal **ou supérieur à 1**.
- Le nombre d'erreurs de clients affiché pour n'importe quel service indique que les erreurs proviennent de l'extrémité du client.

Afficher les détails des transactions HTTP

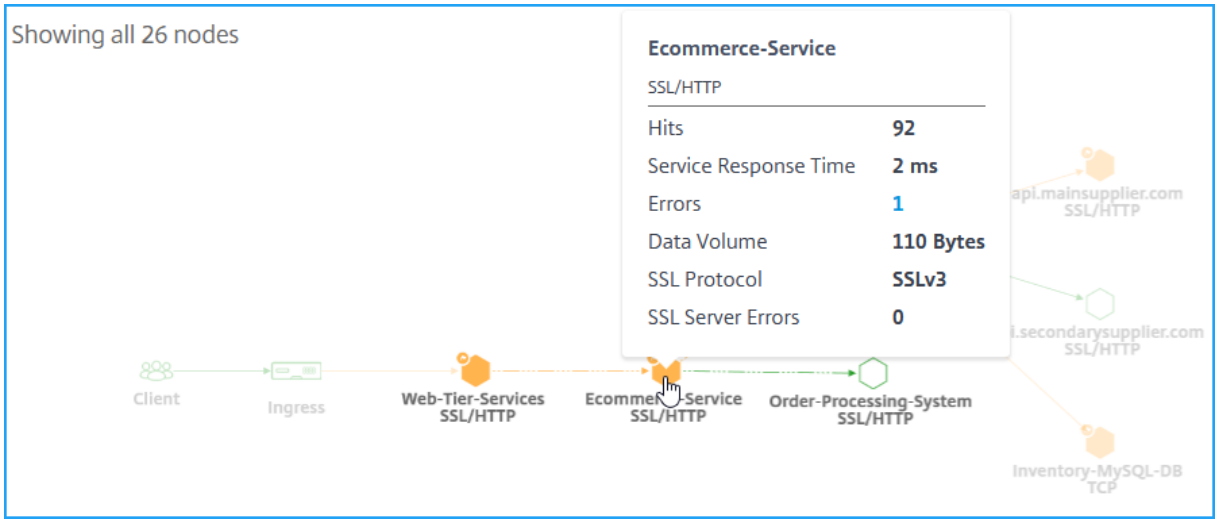
Remarque

Vous pouvez afficher les erreurs en plaçant le pointeur de la souris sur un service erroné et en cliquant sur le nombre de problèmes.

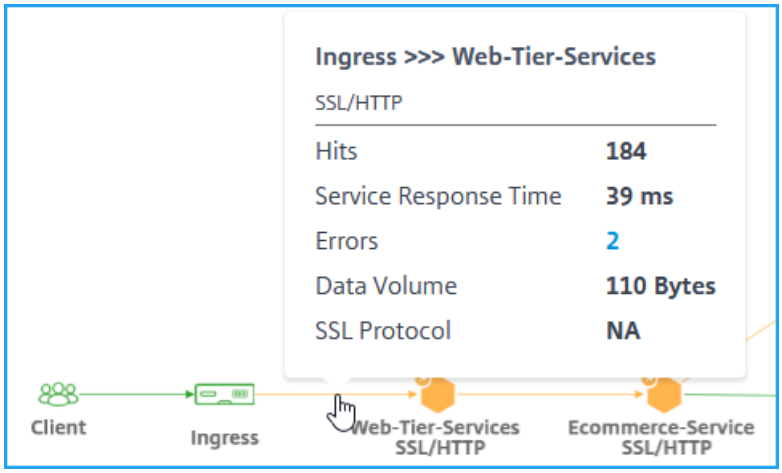


Selon l'exemple illustré dans l'image, vous pouvez afficher une carte réseau de bout en bout de votre application qui montre comment vos services de composants communiquent.

Lorsque vous placez le pointeur de la souris sur l' **Ecommerce-Service**, vous pouvez afficher les détails des mesures pour **Ecommerce-Service**.



Citrix ADM vous permet également d'afficher les détails des transactions entre les services et les services. Placez le pointeur de la souris pour afficher des détails tels que le nombre total d'erreurs, le temps de réponse moyen du service, etc. entre l'entrée et le service.



Hits : indique le nombre total de hits reçus par le service.

Temps de réponse du service — Indique le temps de réponse moyen prélevé par le service pour répondre pour le délai au premier octet (TTFB).

Erreurs : indique le total des erreurs telles que 4xx, 5xx, etc.

Volume de données : indique le volume total de données traitées par le service.

Protocole SSL — Indique la version du protocole SSL.

Cliquez sur la flèche située entre l'**entrée** et le **service** pour afficher les transactions détaillées.

Pour de plus amples informations, consultez la section Afficher les analyses pour les transactions Web.

Configurer les seuils dans le graphique de service

April 29, 2021

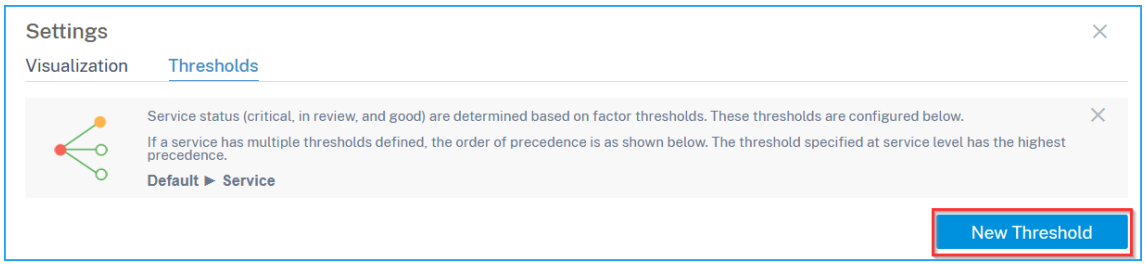
En tant qu'administrateur, vous pouvez configurer des seuils pour les services Kubernetes. Citrix ADM affiche l'état du service (Critique, Révision et Bon) en fonction du temps de réponse du service et du nombre d'erreurs. Par défaut, vous pouvez afficher le **seuil par défaut** (temps de réponse du service = 200 ms et nombre d'erreurs = 0) appliqué à tous les services.

> **Remarque**
>
> Vous ne pouvez pas supprimer le seuil par défaut.

Pour configurer un nouveau seuil :

1. Dans **Applications > Graphique de service**, cliquez sur l'onglet **Microservices** :
2. Cliquez sur l'icône des paramètres et sélectionnez l'onglet **Seuils**.

3. Cliquez sur **Nouveau seuil** pour configurer un nouveau seuil.



   La page **Nouveau seuil** s'affiche.

4. Configurez les paramètres suivants :

   a) **Nom** : spécifiez un nom pour le seuil.

   b) Sous **Microservices**, sélectionnez les services que vous souhaitez appliquer le seuil.

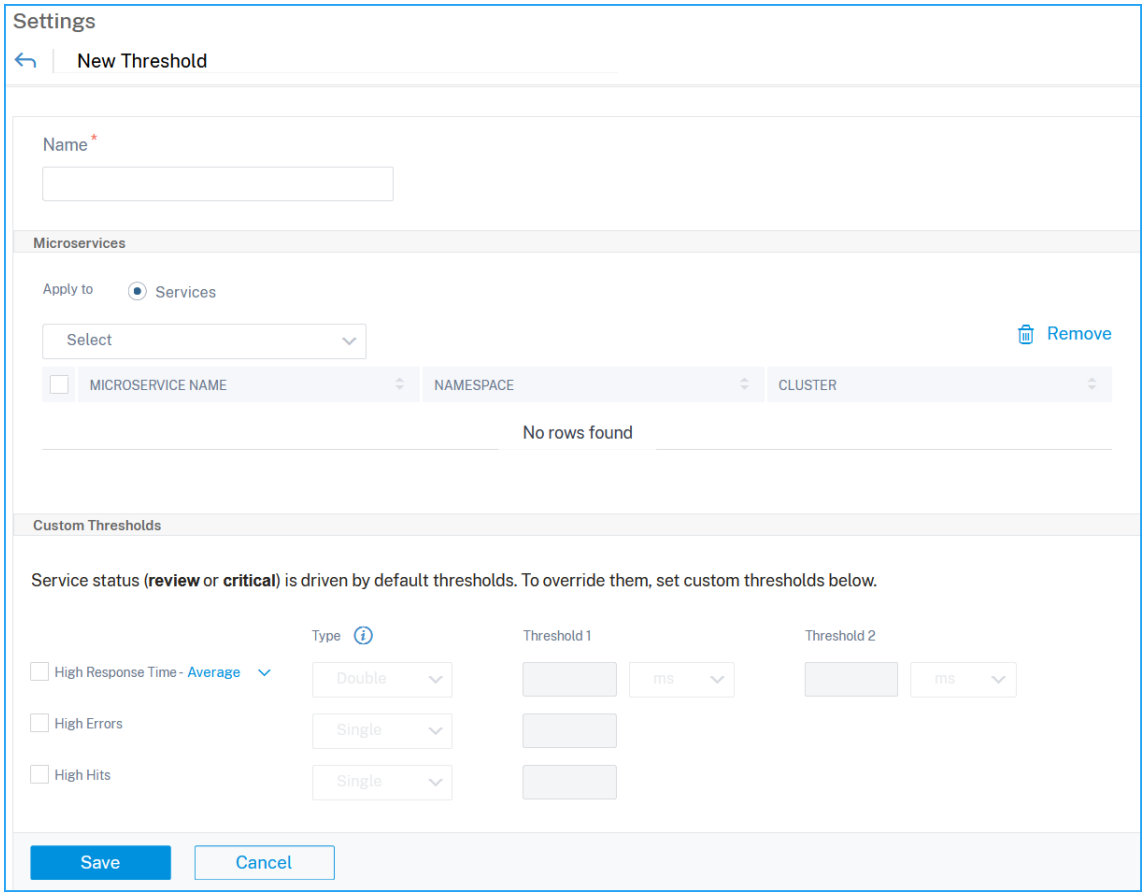
   c) Sous **Seuils**, sélectionnez **Simple** ou **Double** pour :

      - Temps de réponse élevé (moyenne, P99, P99.9)
      - Erreurs élevées
      - Hits élevés

   d) Spécifiez les valeurs de seuil.

   > **Remarque**
   >
   > Si vous sélectionnez le double seuil, assurez-vous :
   >
   > ```
   > - La valeur de seuil 1 est inférieure à la valeur de seuil 2. Par exemple, si vous configurez le seuil 1 comme 250 ms, le seuil 2 doit être de 251 ms ou plus.
   >
   > - La valeur de seuil 1 ne doit pas être la même que la valeur de seuil 2.
   > ```

5. Cliquez sur **Enregistrer**.



Le seuil est créé avec succès. Vous pouvez afficher les détails des **seuils** dans la page Seuils.

> **Remarque**
>
> Citrix ADM calcule le score final et le statut du service en fonction des mesures sélectionnées. Par exemple, si vous sélectionnez uniquement **Hits élevés** pour la configuration du seuil, Citrix ADM utilise le seuil par défaut (temps de réponse = 200 ms et nombre d'erreurs = 0) et les résultats élevés pour calculer le score et le statut du service.

Seuil unique

Lorsque vous configurez un seuil unique pour toutes les mesures ou les mesures sélectionnées, Citrix ADM :

- Compare les valeurs actuelles de chaque mesure avec les valeurs de seuil configurées dans chaque mesure
- Calcule la pénalité totale en fonction des seuils dépassés dans chaque mesure

> Remarque
>
> Si une mesure n'a pas dépassé la valeur seuil, la pénalité est calculée en conséquence

- Affiche le score de service et l'état du service en fonction du calcul de la pénalité

Double seuil

Lorsque vous configurez le double seuil pour toutes les mesures ou les mesures sélectionnées, Citrix ADM :

- Compare les valeurs actuelles de chaque mesure avec les valeurs de seuil configurées dans chaque mesure
- Vérifie si les valeurs actuelles sont :
  - Moins que le seuil 1
  - Entre le seuil 1 et le seuil 2
  - Supérieur au seuil 2
- Calcule la pénalité totale en fonction des seuils dépassés dans chaque mesure

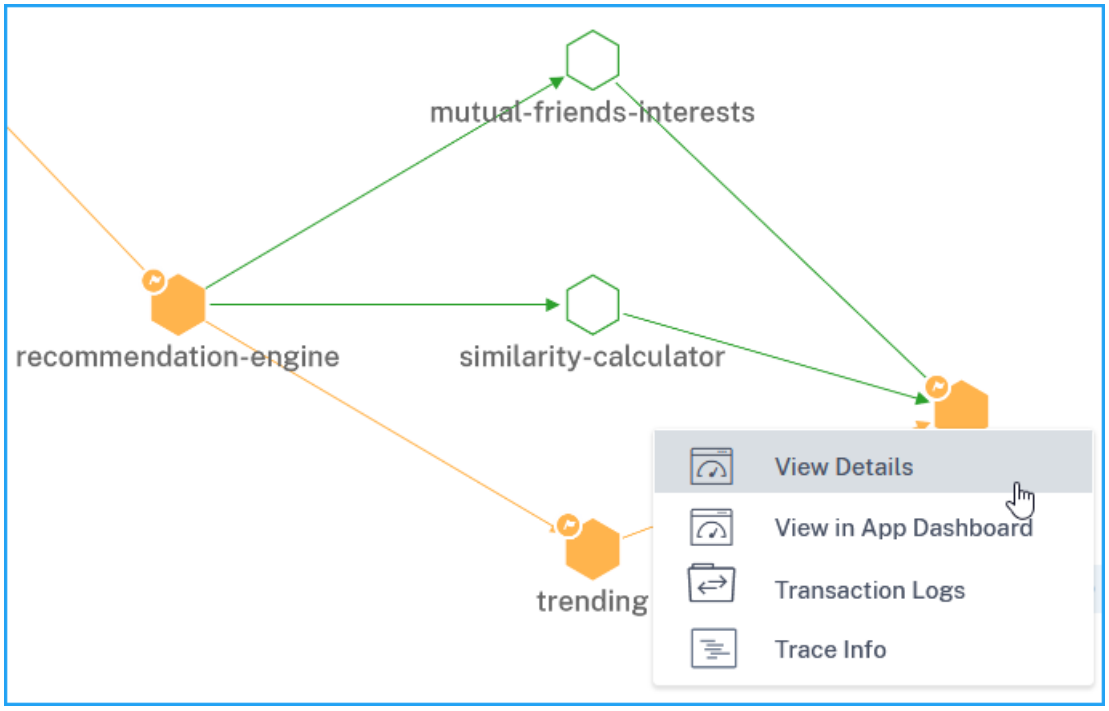
> Remarque
>
> Si une mesure n'a pas dépassé la valeur seuil, la pénalité est calculée en conséquence

- Affiche le score de service et l'état du service en fonction du calcul de la pénalité

Afficher les détails du service

April 29, 2021

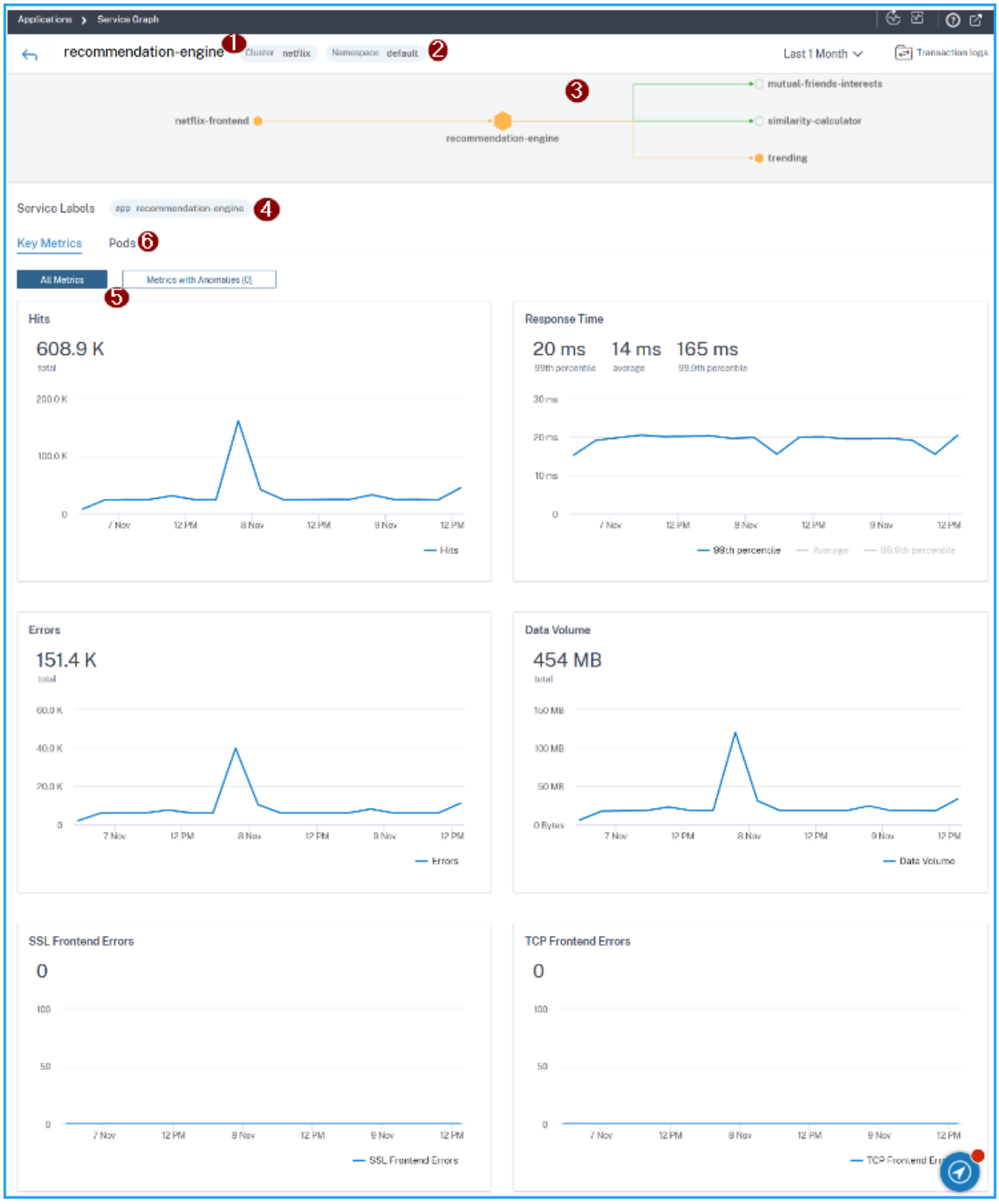
Cliquez sur un service et sélectionnez **Afficher les détails**.



La page des détails du service vous permet d'afficher :

- Nom du cluster dans lequel le service est hébergé (1)
- L'espace de noms et les étiquettes de service du service (2) (4)
- Tous les services entrants et sortants associés connectés au service sélectionné (3)
- Mesures de clé de service dans un format graphique telles que les accès, le temps de réponse, les erreurs, le volume de données, les erreurs frontales SSL et les erreurs frontales TCP. L'onglet **Mesures avec anomalies** vous permet d'afficher les anomalies pour une durée spécifique (5).

  Pour de plus amples informations, consultez la section Surveillez les services à l'aide des mesures du signal doré.
- Les pods backend associés au service (6).



À l'aide de ces tendances de mesures clés, vous pouvez analyser les performances du service pour une durée spécifique.

Par exemple, considérez qu'un service indique le temps de réponse du service > 700 ms pour toutes les demandes. En tant qu'administrateur, vous pouvez :

- Analyser la tendance de la mesure du temps de réponse du service pour une durée spécifique
- Résoudre le problème

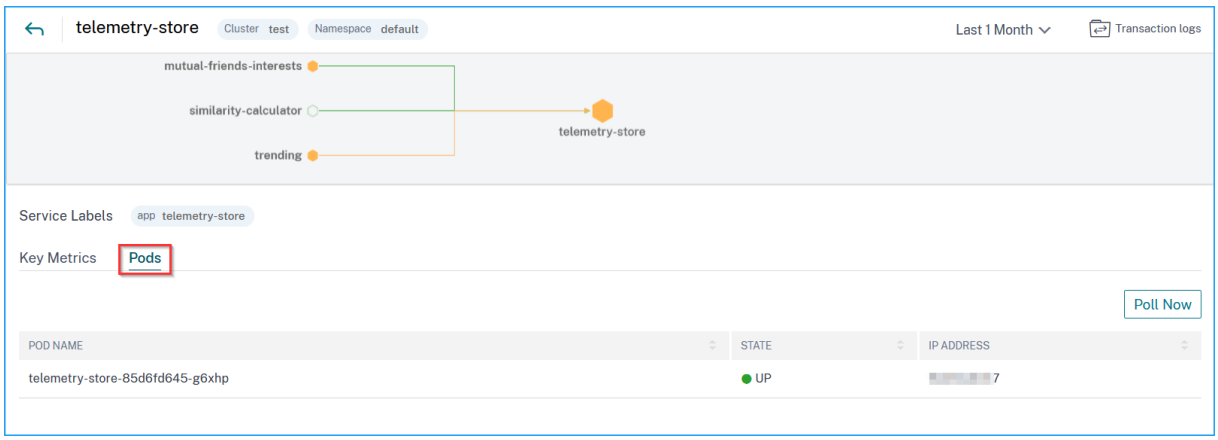
- Vérifiez à nouveau la mesure Temps de réponse du service pour analyser si le temps de réponse s'est amélioré

Détails des mesures

Mesures	Description
Accès	Nombre total de demandes reçues par le service
Erreurs	Nombre total d'erreurs HTTP du service
Temps de réponse du service	Temps de réponse moyen pris par le service pour répondre à la période de temps au premier octet (TTFB).
Volume de données	Volume total de données traité par le service
Erreurs front-end SSL	Nombre total d'erreurs front-end SSL provenant du service. Par exemple : SSL CLIENTAUTH FAILURE
Erreurs back-end SSL	Nombre total d'erreurs SSL back-end du service. Par exemple : Erreurs du client SSL
Erreurs back-end TCP	Nombre total d'erreurs de back-end TCP provenant du service. Par exemple : Réinitialisation du serveur TCP
Erreurs front-end TCP	Nombre total d'erreurs front-end TCP provenant du service. Par exemple : Réinitialisation du client TCP

Afficher les détails du module backend

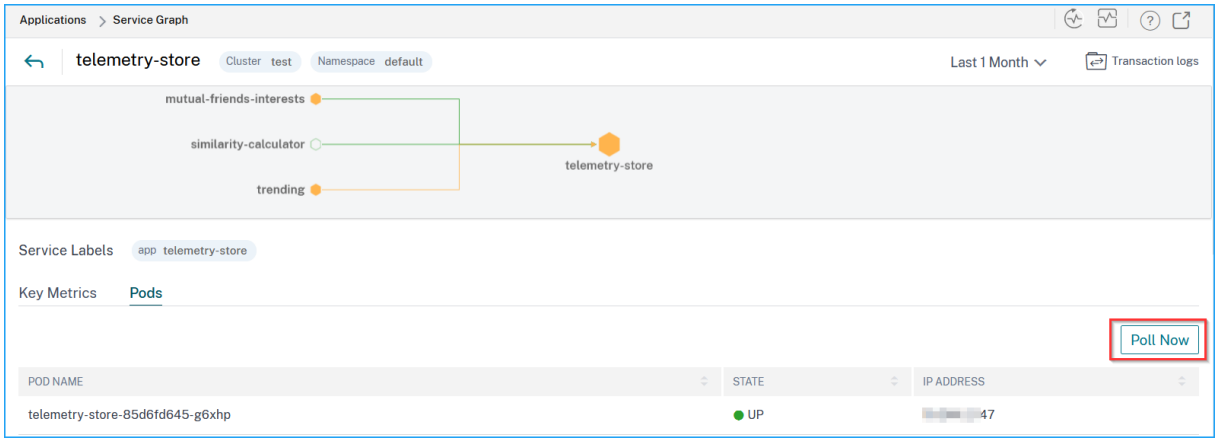
Cliquez sur l'onglet **Pods** pour afficher les pods backend associés au service.



- **Nom du module** — Indique le nom du module
- **Statut** : indique si le conteneur est en cours d'exécution (UP) ou non (DOWN).
- **Adresse IP** — Indique l'adresse IP du conteneur

Utilisez l'option Sondage maintenant pour obtenir l'état du conteneur

L'option **Sondage maintenant** récupère le dernier état du conteneur à partir du cluster.



Surveillez les services à l'aide des mesures du signal doré

Les mesures de signal doré dans les services exécutés dans le cluster Kubernetes font référence à un ensemble de mesures qui vous permettent de détecter des anomalies potentielles pendant une durée spécifique. Lorsque vous avez 100 s de microservices dans le cluster Kubernetes, il peut être difficile d'identifier un service qui présente des problèmes fréquents. Les trois mesures clés suivantes sont les mesures de signal doré que Citrix ADM service graph peut vous aider à identifier les anomalies potentielles pour un service Kubernetes :

- Accès

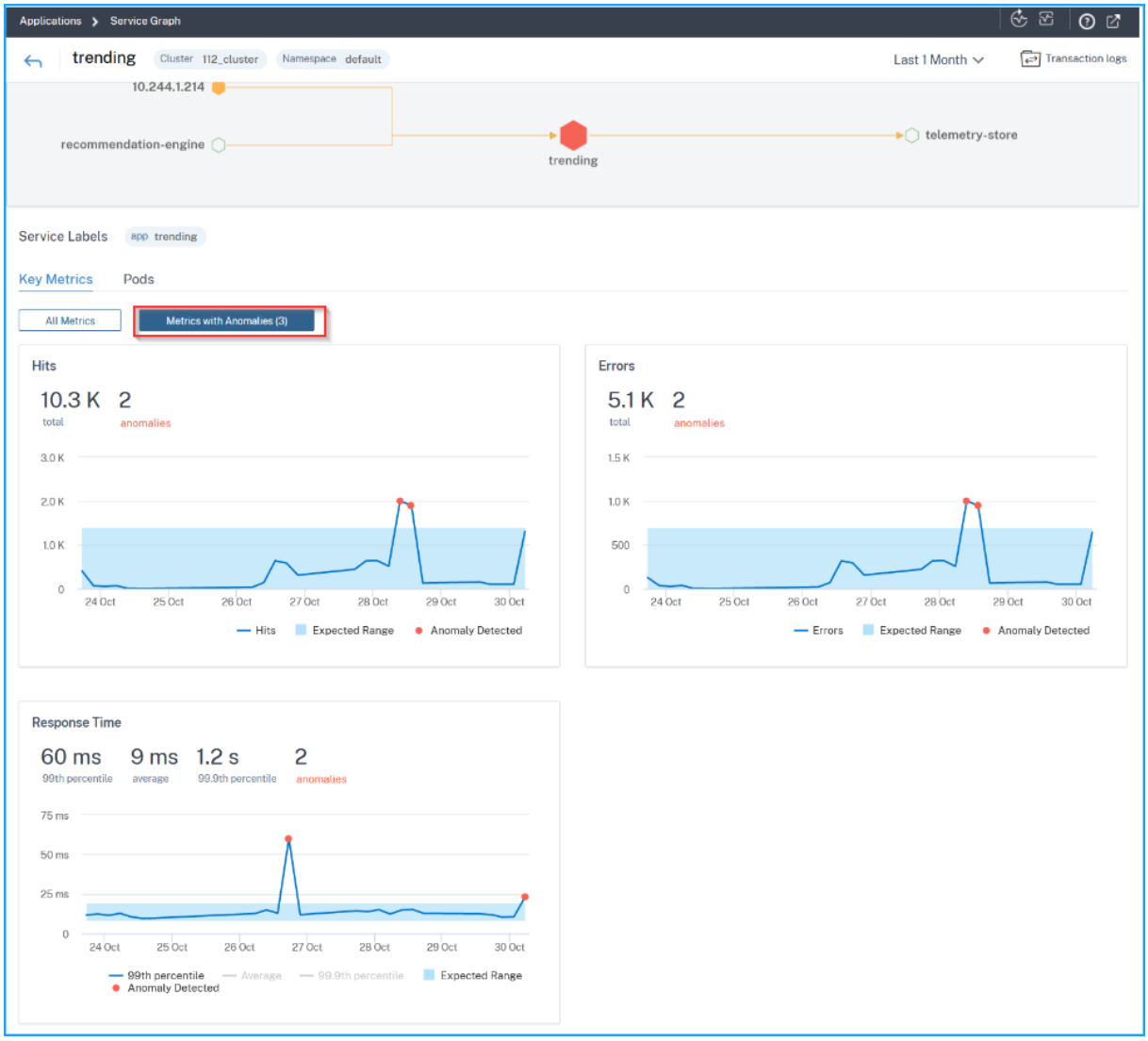
- Temps de réponse (Moyen) et Temps de réponse (P99)
- Erreurs

En tant qu'administrateur, à l'aide de ces mesures, vous pouvez :

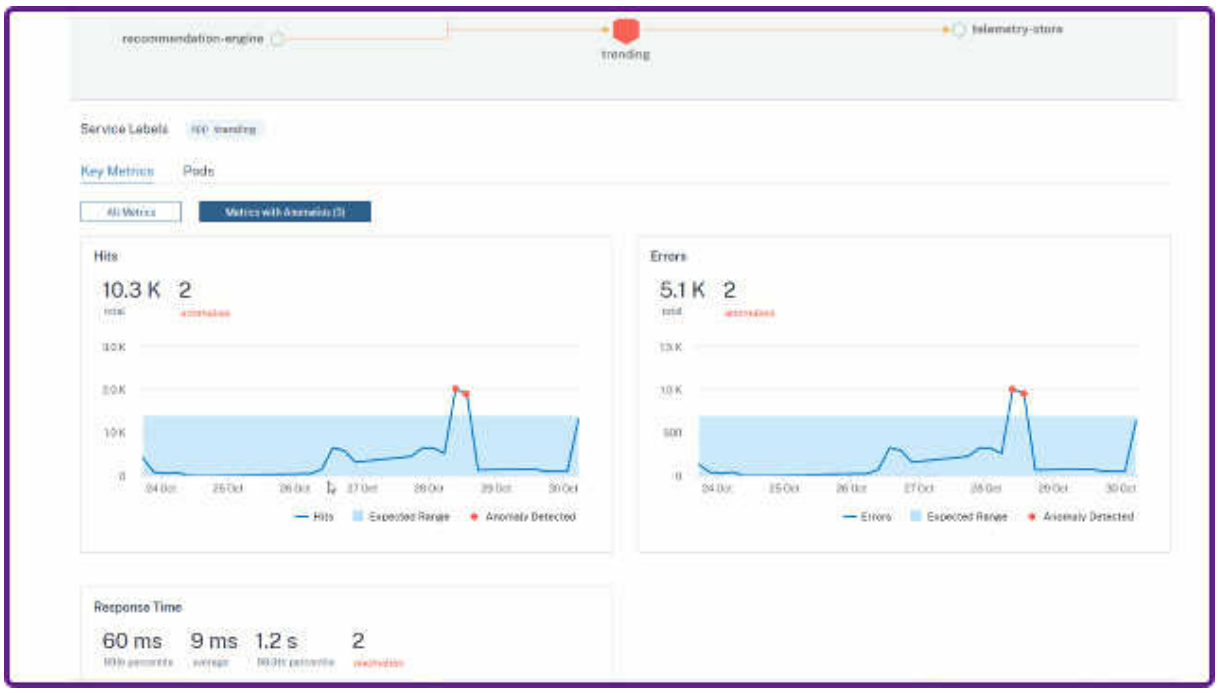
- Identifier l'état du service
  - **Critique** — Le service présente des anomalies ou une rupture de seuil dans plusieurs mesures
  - **Examen** — Le service présente des anomalies ou une violation du seuil dans l'une des mesures
  - **Bon** — Service sans anomalie ni rupture du seuil
- Analyser le nombre d'anomalies identifiées dans chaque mesure
- Résoudre le problème et éviter tout impact majeur

Identifier les anomalies

Lorsque vous cliquez sur un service et sélectionnez **Afficher les détails**, la page Détails du service affiche la vue d'ensemble de toutes les mesures. Cliquez sur l'onglet **Mesures avec anomalies** pour afficher les détails des anomalies.

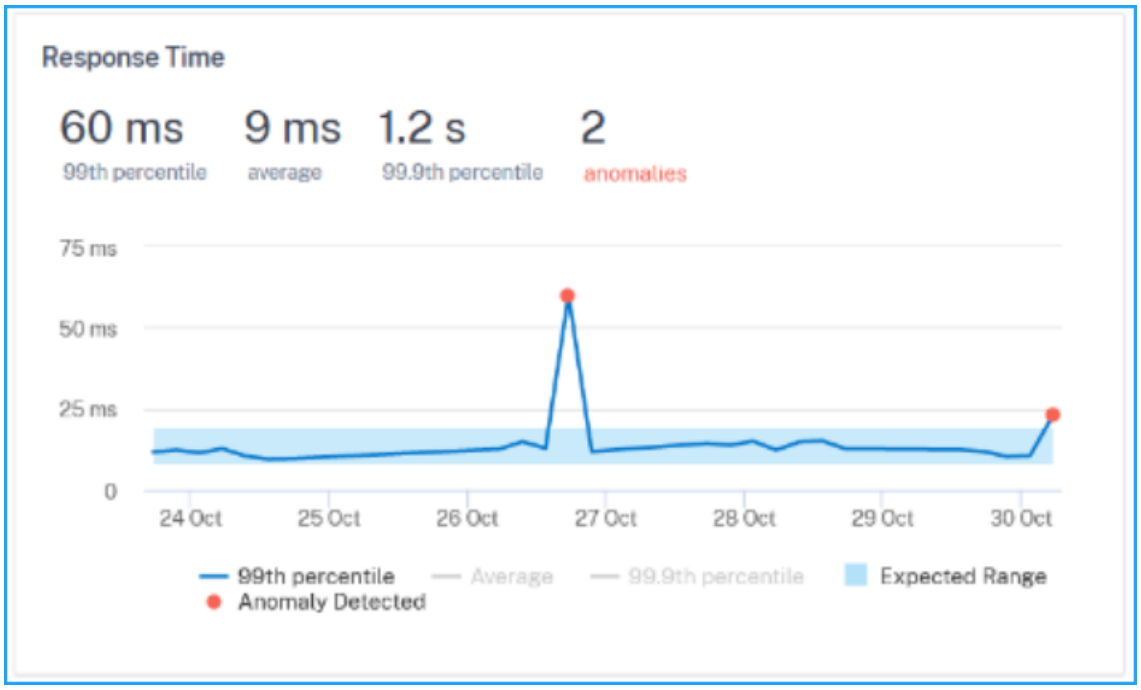


Pour chaque mesure, le graphique permet d'afficher les anomalies détectées chaque fois que la plage attendue dépasse. Vous pouvez cliquer sur les options pour filtrer les vues du graphique.



Considérez que vous souhaitez analyser les anomalies pour le temps de réponse du service (P99).

Sous **Temps de réponse**, vous pouvez afficher les détails suivants pour la durée sélectionnée :



- **99e centile** — Indique que 99 % des demandes pour la durée sélectionnée sont inférieures à 60 ms
- **Moyenne** — Indique le temps de réponse moyen du service
- **99,9e centile** — Indique le temps de réponse le plus élevé du service

- **Anomalies** — Indique le total des anomalies détectées

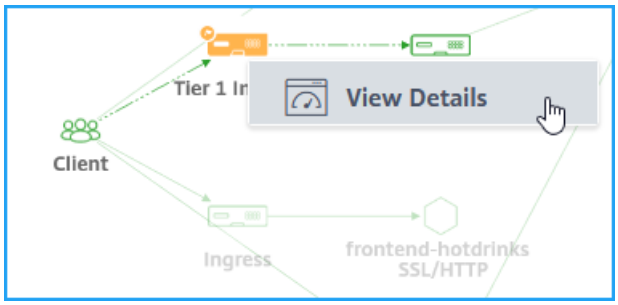
Le graphique vous permet également d'afficher la plage attendue pour la durée sélectionnée. Selon l'exemple, vous pouvez voir :

- La plage de temps de réponse attendue est comprise entre 1 ms et 9 ms.
- Deux anomalies détectées pour le service (une pour 60 ms et une autre pour 25 ms), parce que le temps de réponse du service a dépassé la plage prévue (entre 1 ms et 9 ms).

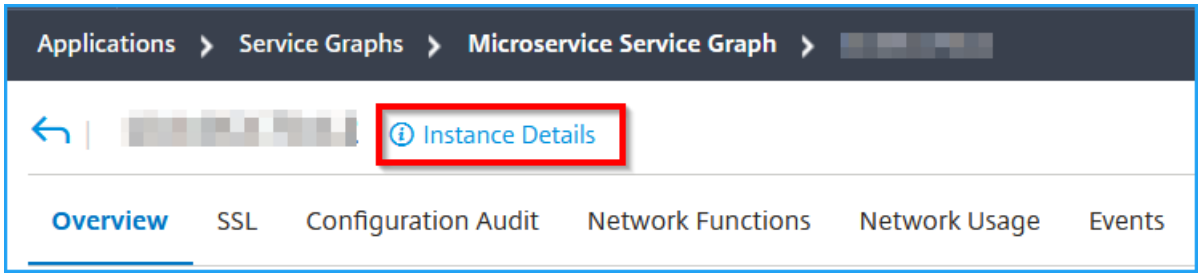
Afficher les détails d'entrée pour résoudre les problèmes

April 29, 2021

Dans le graphique de service, cliquez sur l'entrée et sélectionnez **Afficher les détails** pour visualiser les détails de l'instance Citrix ADC configurée pour le cluster Kubernetes.

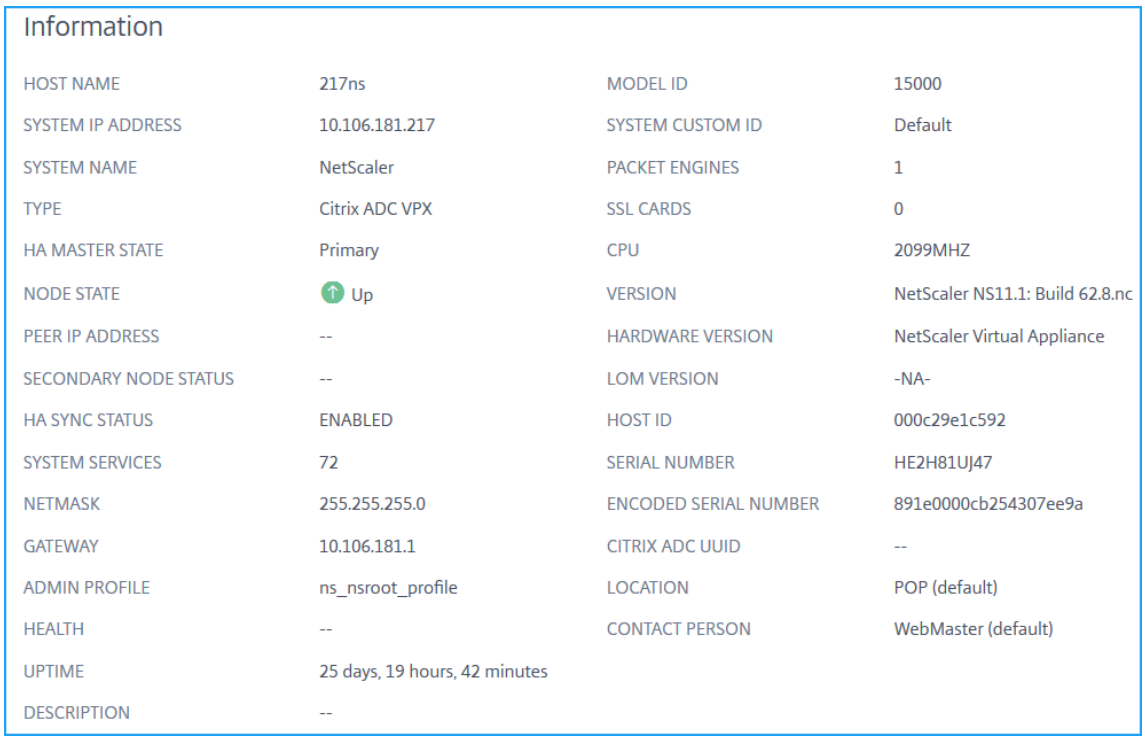


Cliquez sur **Détails de l'instance** pour afficher les détails.

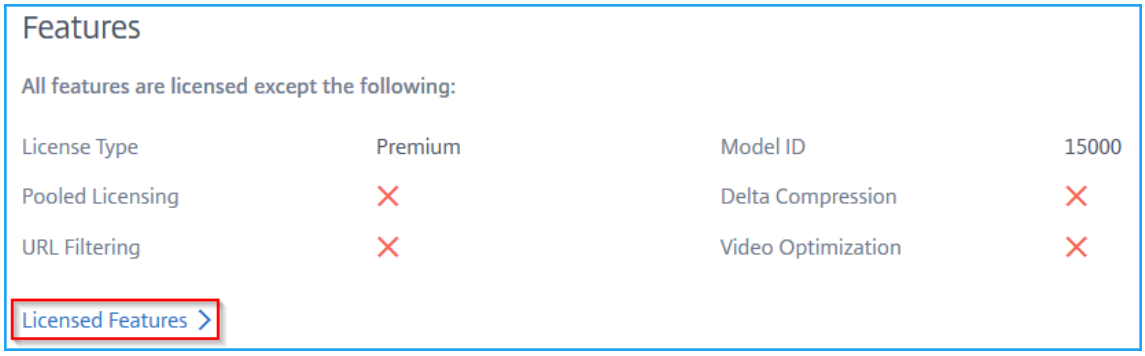


Les détails suivants s'affichent :

- **Informations** : détails d'instance tels que le type d'instance, le type de déploiement, la version, le modèle, etc.



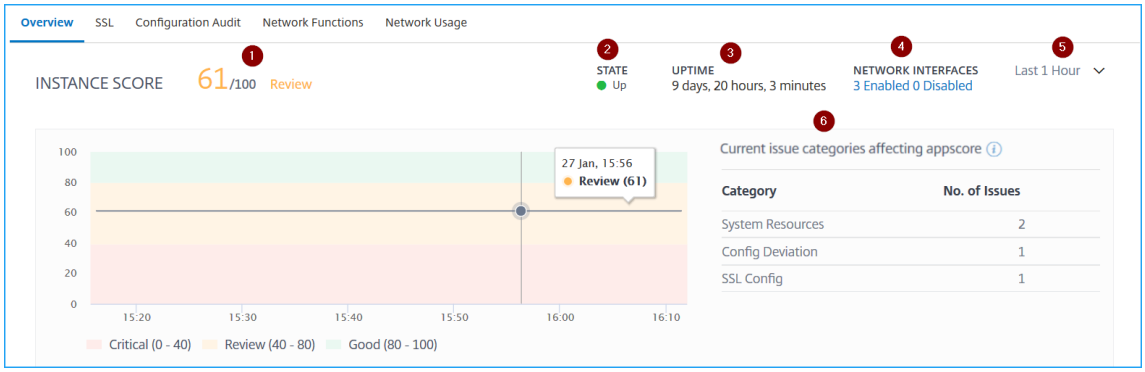
- **Fonctionnalités** : par défaut, les fonctionnalités qui ne sont pas sous licence sont affichées. Cliquez sur **Fonctionnalités sous licence** pour afficher les fonctionnalités sous licence.



- **Modes** : par défaut, tous les modes désactivés sur l'instance sont affichés. Cliquez sur **Afficher les modes activés** pour afficher les modes activés sur l'instance.

Le tableau de bord de l'instance présente une vue d'ensemble de l'instance dans laquelle vous pouvez voir les détails suivants :

- **Score d'instance**

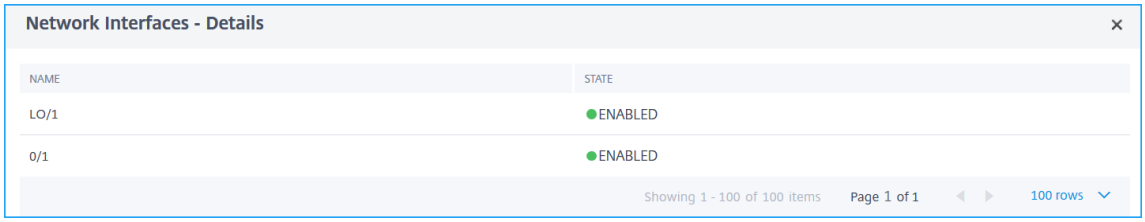


1 — Indique le score d'instance Citrix ADC actuel pour la durée sélectionnée. Le score final est calculé comme **100 moins les pénalités totales**. Le graphique affiche les plages de score pour la durée sélectionnée.

2 — Indique l'état actuel de l'instance Citrix ADC, par exemple En **haut**, **en bas**et **hors service**.

3 — Indique la durée pendant laquelle l'instance de Citrix ADC est en cours d'exécution.

4 — Indique le nombre total d'interfaces réseau activées et désactivées pour l'instance. Cliquez pour afficher les détails tels que le nom de l'interface réseau et l'état (activé ou désactivé).



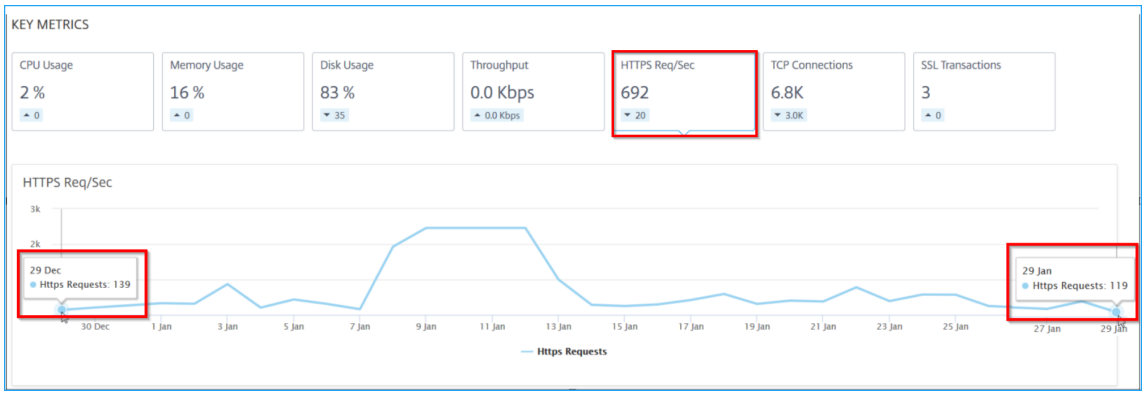
5 — Sélectionnez la durée dans la liste pour afficher les détails de l'instance.

6 — Affiche le nombre total de problèmes et la catégorie de problèmes de l'instance ADC.

- **Principales mesures**

  Cliquez sur chaque onglet pour afficher les détails. Dans chaque mesure, vous pouvez afficher la valeur moyenne et la valeur de différence pour l'heure sélectionnée.

  L'image suivante est un exemple pour HTTPS Req/Sec et la durée sélectionnée est pour 1 dernier mois. La valeur **692** est la moyenne HTTPS Req/Sec pour la durée du dernier mois et la valeur **20** est la valeur de différence. Dans le graphique, la première valeur est **139** et la dernière valeur est **119**. La valeur de la différence est **139 — 119 = 20**.



  Vous pouvez afficher les mesures d'instance suivantes dans un format graphique pour la durée sélectionnée :

  - **Utilisation de l'UC — % de CPU** moyen de l'instance pour la durée sélectionnée (s'affiche à la fois pour l'UC du paquet et pour l'UC de gestion).
  - **Utilisation de la mémoire** : % d'utilisation moyenne de la mémoire de l'instance pour la durée sélectionnée.
  - **Utilisation du disque** : en% d'espace disque moyen de l'instance pour la durée sélectionnée.
  - **Débit : débit** réseau moyen traité par l'instance pour la durée sélectionnée.
  - **Request/sec HTTPS** — Nombre moyen de demandes HTTPS reçues par l'instance pour la durée sélectionnée.

- Connexions**TCP : connexions** TCP moyennes établies par le client et le serveur pour la durée sélectionnée.
- **Transactions SSL — Transactions** SSL moyennes traitées par l'instance pour la durée sélectionnée.

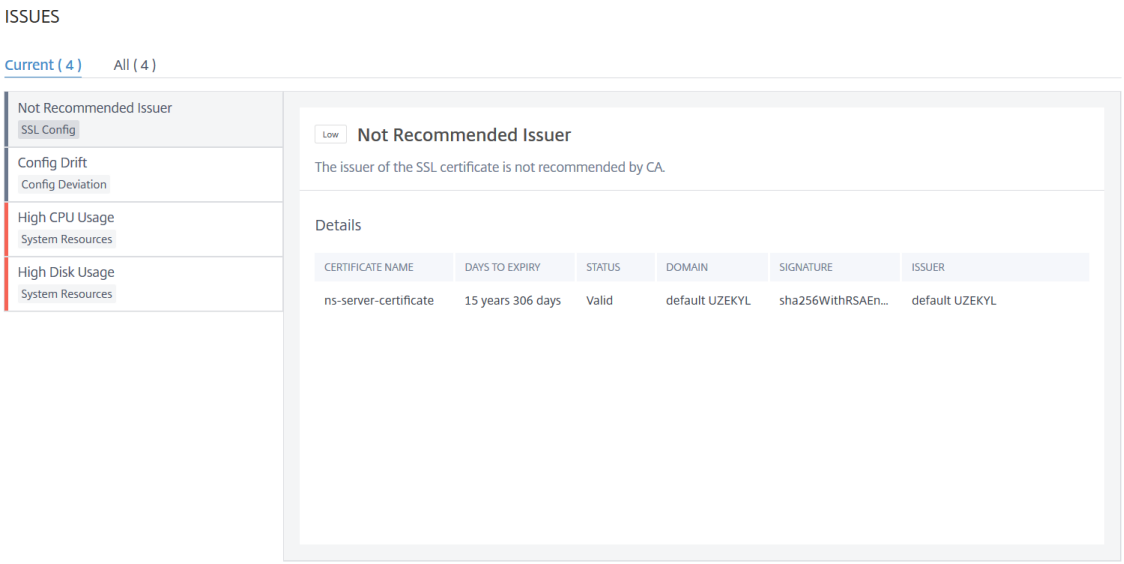
- **Problèmes**

  Vous pouvez afficher les problèmes suivants qui se produisent dans l'instance de Citrix ADC :

Catégorie de problème	Description	Problèmes
Ressources système	Affiche tous les problèmes liés à la ressource système Citrix ADC tels que le processeur, la mémoire, l'utilisation du disque, etc.	- Utilisation élevée du processeur
		- Utilisation élevée de la mémoire
		- Utilisation élevée du disque
		- Échec de la carte SSL
		- Panne de courant
		- Erreur de disque
		- Erreur Flash
		- Rejets de carte réseau
Configuration SSL	Affiche tous les problèmes liés à la configuration SSL sur l'instance de Citrix ADC.	- Certs SSL expirés
		- Émetteur non recommandé
		- Non recommandé Algo
		- Résistance de la clé non recommandée
Déviation de configuration	Affiche tous les problèmes liés aux tâches de configuration appliquées dans l'instance Citrix ADC.	- Config Drift
		- Running vs Template

Catégorie de problème	Description	Problèmes
Problèmes de capacité	Affiche les problèmes de capacité ADC. L'ADM interroge ces événements toutes les cinq minutes à partir de l'instance ADC et affiche les baisses de paquets ou les incréments de compteur de limite de vitesse s'il existe. Les problèmes sont classés en fonction des paramètres de capacité suivants.	- Limite de débit atteinte
		- Limite du processeur PE atteinte
		- Limite PPS atteinte
		- Limite de débit SSL
		- Limite de débit SSL TPS
Mise en réseau	Affiche les problèmes opérationnels qui se produisent dans les instances.	Pour de plus amples informations, consultez la section Analyse de l'infrastructure améliorée avec de nouveaux indicateurs.

Cliquez sur chaque onglet pour analyser et résoudre le problème. Par exemple, considérez qu'une instance présente les erreurs suivantes pour la durée sélectionnée :



- L'onglet **Actuel** affiche les problèmes opérationnels ADC actuels qui affectent le score de l'instance.
- L'onglet **Tout** affiche tous les problèmes infra détectés pour la durée sélectionnée.

Suivi distribué

April 29, 2021

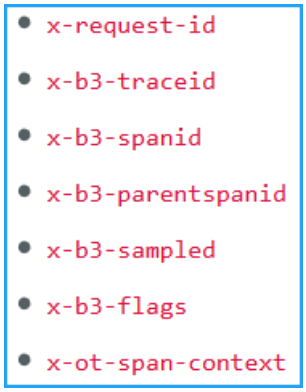
Dans le graphique de service, vous pouvez utiliser la vue de suivi distribué pour :

- Analysez la performance globale du service.
- Visualisez le flux de communication entre le service sélectionné et ses services interdépendants.
- Identifiez le service qui indique les erreurs et dépannez le service erroné.
- Afficher les détails de transaction entre le service sélectionné et chaque service interdépendant.

Conditions préalables

Pour afficher les informations de suivi du service, vous devez :

- Assurez-vous qu'une application conserve les en-têtes de trace suivants, tout en envoyant tout trafic est-ouest :



- Pour les **versions CIC antérieures à la version 1.7.23**, mettez à jour le fichier YAML CPX avec la valeur `NS_DISTRIBUTED_TRACING` et `yes`


```
# Add cic as a sidecar
- name: cic
  image: "quay.io/citrix/citrix-k8s-ingress-controller:1.5.6"
  env:
  - name: "EULA"
    value: "yes"
  - name: "NS_IP"
    value: "127.0.0.1"
  - name: "NS_PROTOCOL"
    value: "HTTP"
  - name: "NS_PORT"
    value: "80"
  - name: "NS_DEPLOYMENT_MODE"
    value: "SIDECAR"
  - name: "NS_ENABLE_MONITORING"
    value: "YES"
  - name: "NS_DISTRIBUTED_TRACING"
    value: "yes"
  - name: "NS_LOGPROXY"
    value: "coe-tracing.default.svc.cluster.local"
  - name: POD_NAME
    valueFrom:
      fieldRef:
        apiVersion: v1
        fieldPath: metadata.name
  - name: POD_NAMESPACE
    valueFrom:
      fieldRef:
        apiVersion: v1
        fieldPath: metadata.namespace
  args:
    - --ingress-classes
      watches-ingress
  imagePullPolicy: Always
```

- Pour les **versions CIC postérieures à 1.7.23**, vous devez utiliser un ConfigMap.

  ConfigMaps vous permet de séparer vos configurations de vos pods et de rendre vos charges de travail portables. Grâce à ConfigMaps, vous pouvez facilement modifier et gérer vos configurations de charge de travail et réduire le besoin de coder en dur les données de configuration en fonction des spécifications du module.

  Avec la prise en charge de ConfigMap, vous pouvez mettre à jour la configuration automatique-

ment tout en conservant le conteneur de Citrix ingress controller en cours d'exécution. Vous n'avez pas besoin de redémarrer le module après la mise à jour. Pour de plus amples informations, consultez la section Prise en charge de ConfigMap pour le contrôleur d'entrée.

À l'aide de ConfigMap, vous pouvez activer ou désactiver le suivi distribué, les événements, les journaux d'audit, etc. Pour utiliser le ConfigMap :

1. Créez un fichier YAML en utilisant les paramètres requis.

   Le suivi distribué est activé dans le fichier YAML suivant et d'autres variables telles que les journaux d'audit, les événements et les transactions sont désactivés :

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: cic-configmap
  namespace: default
data:
  LOGLEVEL: 'debug'
  NS_PROTOCOL: 'http'
  NS_PORT: '80'
  NS_HTTP2_SERVER_SIDE: 'ON'
  NS_ANALYTICS_CONFIG: |
    distributed_tracing:
      enable: 'true'
      samplingrate: 100
    endpoint:
      server: <ADM-AgentIP> / <ADM-AppserverIP>
    timeseries:
      port: 5563
      metrics:
        enable: 'true'
        mode: 'avro'
      auditlogs:
        enable: 'false'
      events:
        enable: 'false'
    transactions:
      enable: 'false'
      port: 5557
<!--NeedCopy-->
```

> Remarque
>
> Vous pouvez fournir les valeurs pour `Samplingrate` comprises entre 0 et 100. Citrix

> ADM affiche le nombre de transactions de suivi mentionné.

2. Déployez ConfigMap à l'aide de :

   ```
   kubectl create -f <configmap-yaml>.yaml
   ```

3. Modifiez le fichier CPX YAML et utilisez `envFrom` ou `args` pour spécifier les arguments suivants :

   ```
   envFrom:
    - configMapRef:
        name: cic-configmap
   <!--NeedCopy-->
   ```

   OU

   ```
   args:
     - --configmap
       default/cic-configmap
   ```

   La configuration YAML ConfigMap est déployée dans CIC.

4. Si vous souhaitez modifier la valeur d'une variable, modifiez les valeurs dans ConfigMap. Dans cet exemple, toutes les autres variables sont changées de **`false`** à **`true`**.

   ```
   apiVersion: v1
   kind: ConfigMap
   metadata:
     name: cic-configmap
     namespace: default
   data:
     LOGLEVEL: 'debug'
     NS_PROTOCOL: 'http'
     NS_PORT: '80'
     NS_HTTP2_SERVER_SIDE: 'ON'
     NS_ANALYTICS_CONFIG: |
       distributed_tracing:
         enable: 'true'
         samplingrate: 100
       endpoint:
         server: <ADM-AgentIP> / <ADM-AppserverIP>
       timeseries:
         port: 5563
         metrics:
           enable: 'true'
           mode: 'avro'
         auditlogs:
   ```



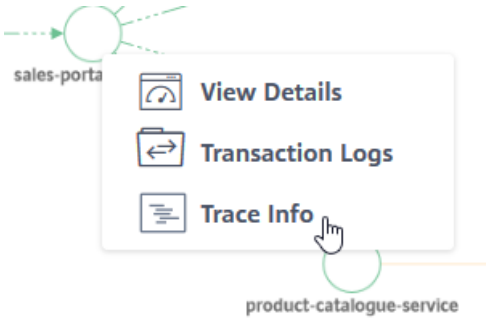
```
        enable: 'true'
      events:
        enable: 'true'
    transactions:
      enable: 'true'
      port: 5557
  <!--NeedCopy-->
```

5. Appliquez à nouveau ConfigMap à l'aide de la commande suivante :

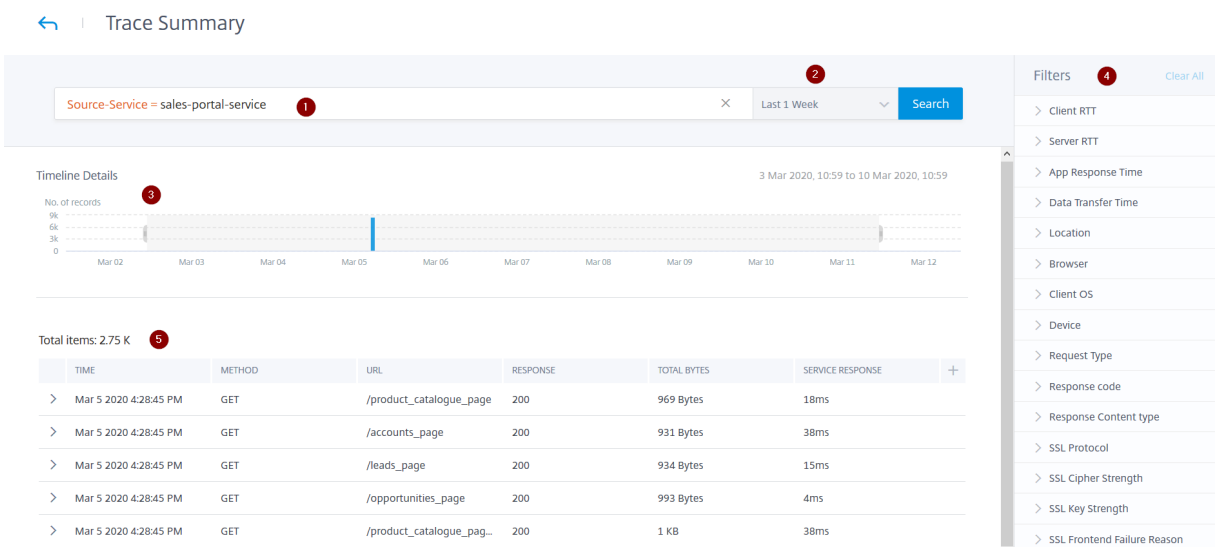
```
kubectl apply -f <yaml-file>.yaml
```

Afficher les détails du suivi du service

Dans le graphique de service, cliquez sur un service, puis sélectionnez **Infos de suivi**.



La page Récapitulatif du suivi s'affiche pour le service sélectionné.



Le **récapitulatif des traces** s'affiche :

- Une recherche avancée qui vous permet de rechercher des transactions avec des suggestions et des opérateurs (1). Pour de plus amples informations, consultez la section Recherche avancée.

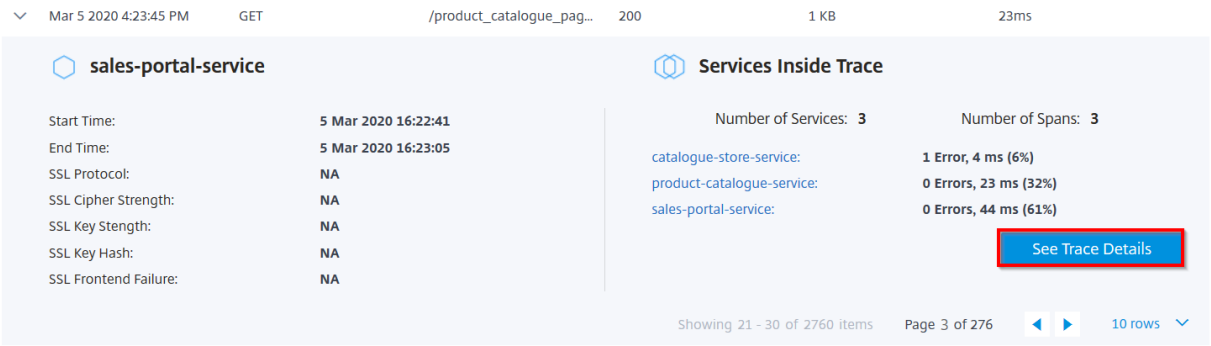
- Liste de durée de temps qui vous permet de sélectionner la durée de temps telle que 1 heure, 12 heures, 1 jour, 1 semaine, 1 mois et heure personnalisée (2).
- Graphique Détails de la chronologie qui vous permet de faire glisser et de sélectionner pour afficher les résultats pour une durée spécifique (3).
- Panneau Filtres qui vous permet de sélectionner des options dans chaque mesure (4).
- Détails de transaction pour le service sélectionné (5).

Afficher les détails de la transaction

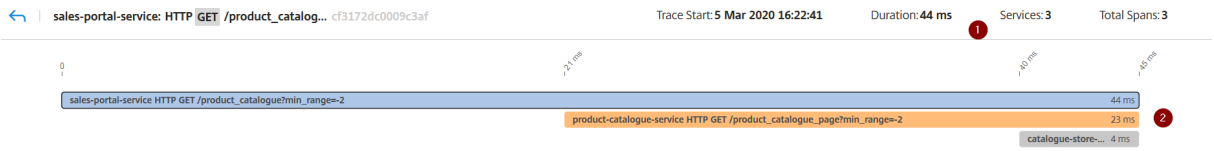
Cliquez sur une transaction pour effectuer une hiérarchisation vers le bas pour obtenir des informations détaillées. Vous pouvez afficher les détails de transaction pour le service sélectionné, tels que :

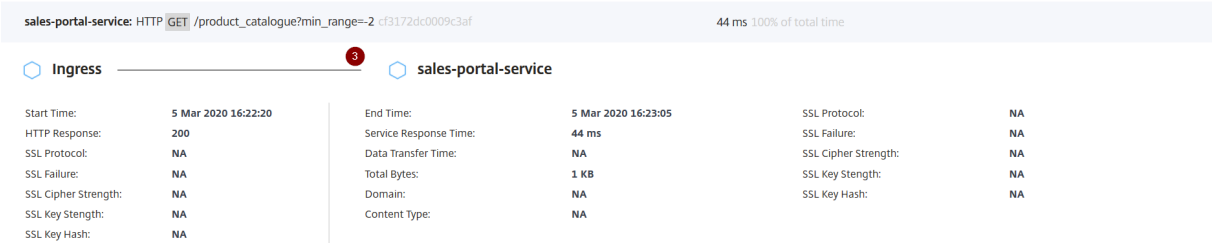
- Heure de début
- Heure de fin
- Mesures SSL
- Communication avec les services interdépendants (avec les erreurs et le temps de réponse avec chaque service).

L'exemple suivant indique une erreur de `catalogue-store-service`. Cliquez sur **Voir Détails du suivi** pour plus de détails.



La page Détails du suivi s'affiche.



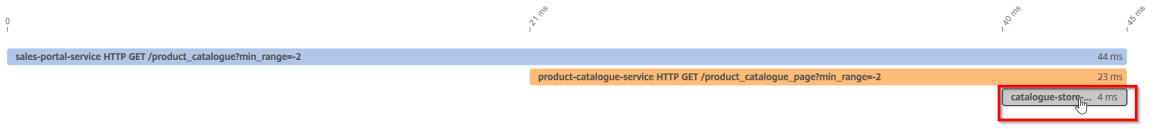


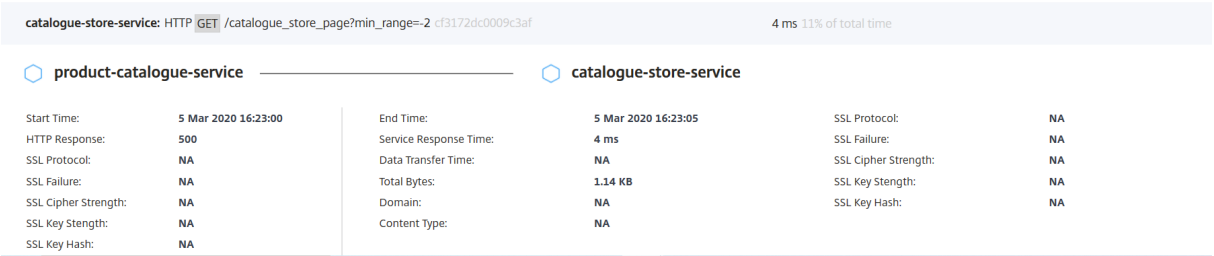
1 — Affiche l'heure de début, le temps de réponse, le total des services et les travées totales de la transaction.

2 — Affiche les détails du service sélectionné qui a communiqué avec ses services d'interdépendance. Vous pouvez cliquer sur chaque transaction pour afficher les détails.

3 — Affiche les détails de la transaction pour chaque service.

Selon l'exemple image, `catalogue-store-service` a indiqué une erreur. Cliquez sur la transaction disponible pour `catalogue-store-service`.

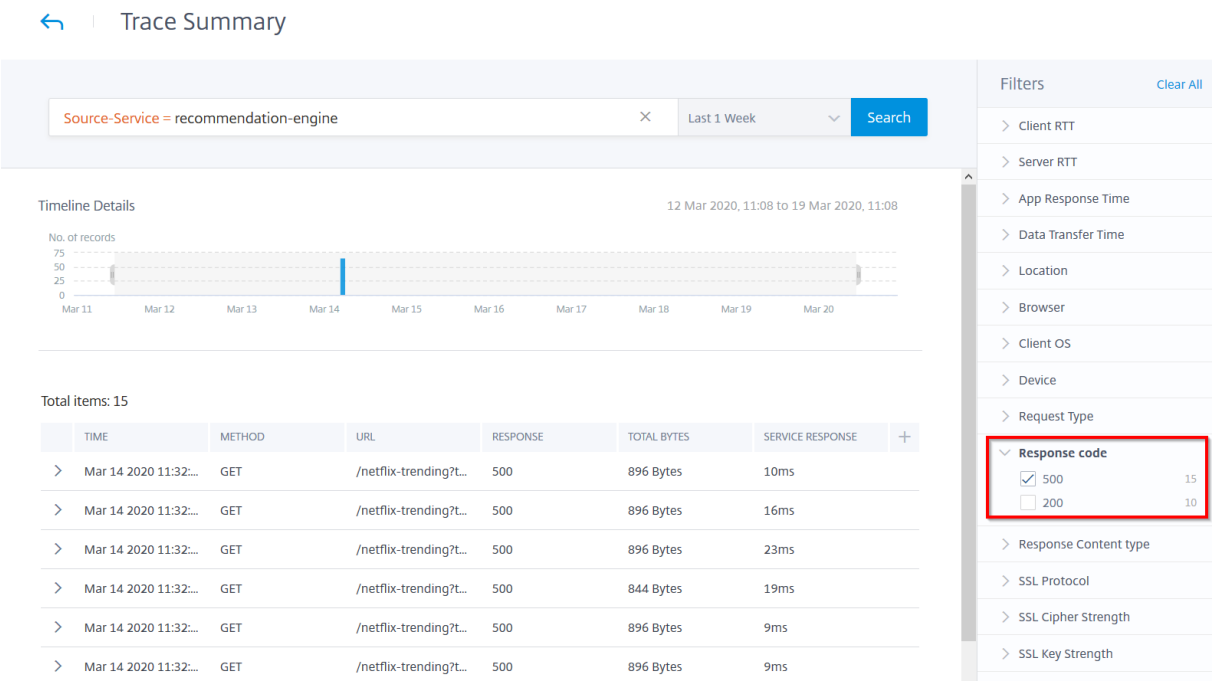




Les détails de transaction entre `product-catalogue-service` et `catalogue-store-service` indiquent la réponse HTTP comme 500. Avec ces détails, en tant qu'administrateur, vous pouvez analyser le service erroné et dépanner `product-catalogue-service` en tant que résolution.

Vous pouvez également filtrer les résultats en sélectionnant des options dans chaque mesure sous le

panneau **Filtres**. Par exemple, si vous souhaitez afficher toutes les transactions 5xx, cliquez sur **Code de réponse** et sélectionnez **500**.



- **RTT client** : durée de déplacement d'un paquet à partir du client.
- **RTT du serveur** : durée de déplacement d'un paquet à partir du serveur.
- Temps de**réponse de l'application : Temps**de réponse moyen de l'application
- **Temps de transfert**de données : taille de transfert de données et vitesse à laquelle la transmission peut se produire depuis/vers un service.
- **Emplacement** : l'emplacement du client
- **Navigateur** : types de navigateur utilisés par les clients. Par exemple : Chrome, Firefox.
- **Système d'exploitation client** : Système d'exploitation client basé sur les détails de l'agent utilisateur du navigateur.
- **Périphérique** : Périphériques basés sur les détails de l'agent utilisateur du navigateur. Par exemple : Tablette, Mobile.
- **Type de demande** : Type de demande de transaction. Par exemple : GET.
- **Code de réponse** : Code de réponse reçu du serveur. Par exemple : 501, 404, 200.
- **Type de contenu de réponse** : Type de contenu de transaction. Si la demande du client concerne text/html, la réponse du serveur doit être text/html.
- **Protocole SSL** : Version du protocole SSL utilisée par les clients. Par exemple : SSLv3.

- Force de**chiffrement SSL : force**de chiffrement basée sur la taille de la clé de certificat SSL telle que élevée, moyenne et basse.
- Résistance de**la clé SSL : La force**de chiffrement SSL est calculée à partir de la taille de la clé de certificat SSL. La longueur de clé définit la sécurité de l'algorithme SSL. Par exemple : 2048
- **Raison de l'échec du frontend**SSL : message d'erreur de connexion SSL frontal. Par exemple : SSL CLIENTAUTH FAILURE

Afficher les détails de diagnostic pour des données partielles ou incomplètes dans le graphique de service

April 29, 2021

Après avoir terminé le graphique de service requis configuration et ajouté le cluster Kubernetes dans Citrix ADM, le graphique de service commence à renseigner les données. Dans certains scénarios, vous pouvez observer que le graphique de service affiche des données partielles ou aucune donnée. Voici quelques-unes des raisons possibles pour les données partielles ou l'absence de données dans le graphique de service :

- L'itinéraire statique n'est pas configuré
- L'état du cluster Kubernetes est en panne
- Échec de l'enregistrement CPX
- Les serveurs virtuels CPX ne sont pas sous licence
- La configuration d'analyse requise n'est pas définie qui empêche le graphique de service de charger toutes les données

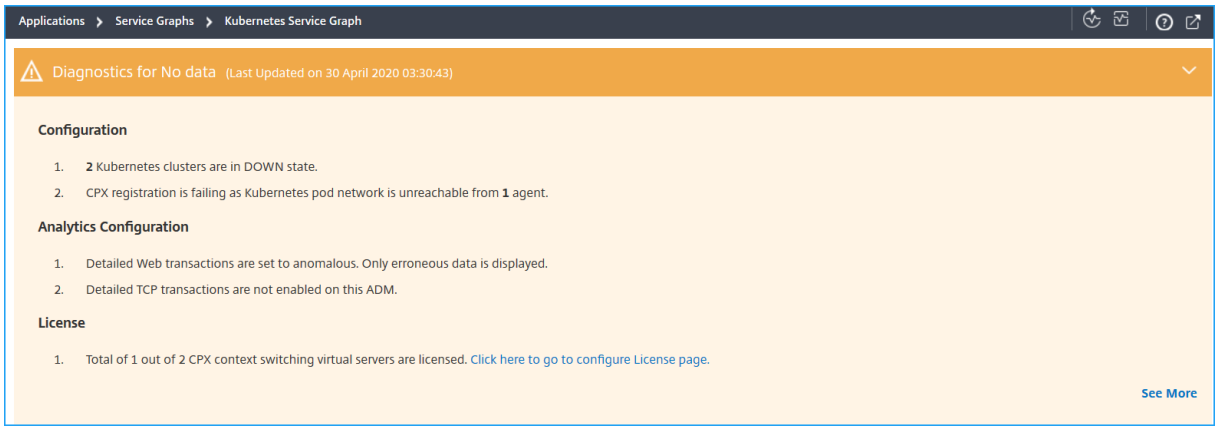
En tant qu'administrateur, vous pourriez avoir du mal à analyser les raisons lorsque vous voyez un graphique de service affichant des données partielles ou aucune donnée. La page Informations de diagnostic dans le graphique de service vous permet de voir les raisons possibles et les actions requises pour résoudre les problèmes de données partielles ou aucun problème de données.

Dans Citrix ADM, accédez à **Applications** > **Service Graph** et cliquez sur l'onglet **Microservices**.

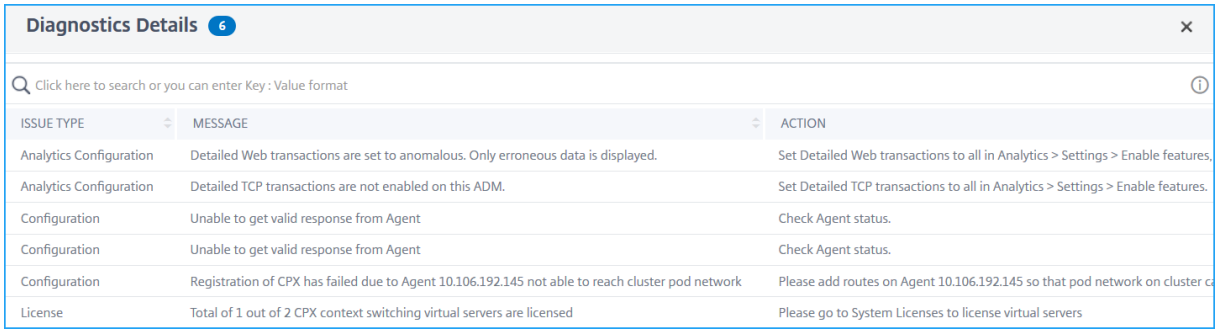
Diagnostics pour aucune donnée

Si le graphique de service n'affiche aucune donnée, le message de diagnostic suivant s'affiche.

Cliquez sur ** pour afficher les détails. Vous pouvez afficher les raisons possibles pour le graphique de service n'affichant aucune donnée. L'image suivante est un exemple pour aucune donnée dans le graphique de service.



Cliquez sur **Voir plus** pour afficher les détails des problèmes.

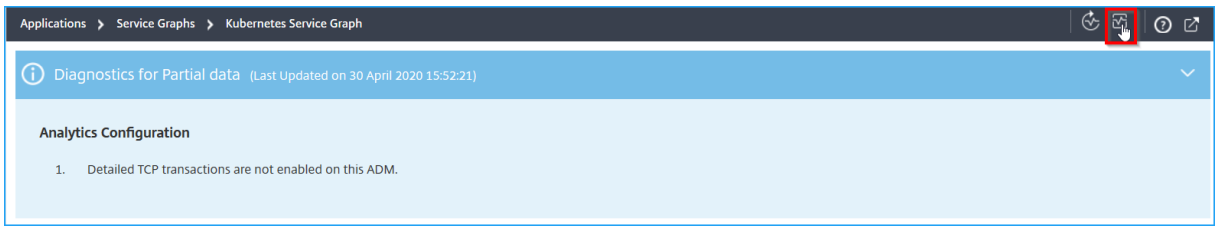


- **Type de problème** : indique si les problèmes se produisent à partir de la configuration, de la configuration d'analyse ou de la licence.
- **Message** — Indique ce qui a causé le problème.
- **Action** : indique quelle action doit être effectuée pour résoudre le problème.

Diagnostics des données partielles

Si le graphique de service est affiché uniquement avec des données partielles, cliquez sur le bouton **Afficher les diagnostics** pour afficher les informations de diagnostic.

L'exemple suivant indique que les transactions TCP sont désactivées.

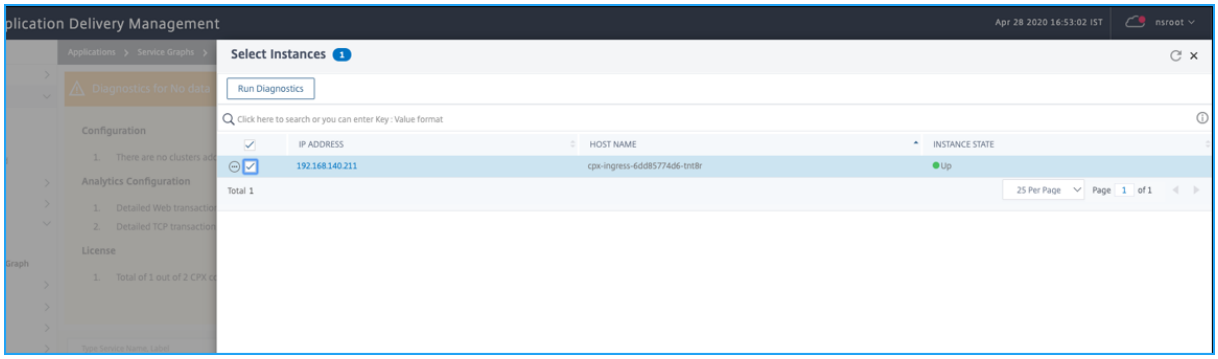


Pour cet exemple, vous devez activer les **paramètres de transaction TCP** sur **Tous** en accédant à **Analytics** > **Paramètres**.

Résolution des problèmes

En tant qu'administrateur, à l'aide de ces messages de diagnostic, vous pouvez valider ces problèmes et essayer de les résoudre. Après le dépannage, Citrix ADM exécute automatiquement une vérification de diagnostic périodique à un intervalle régulier. Une fois la vérification des diagnostics terminée, le problème de données partielles ou aucune donnée dans le graphique de service sera résolu.

Vous pouvez également cliquer sur **Exécuter les tests de diagnostic**, sélectionner les **instances CPX**, puis cliquer sur **Exécuter les tests de diagnostic**.



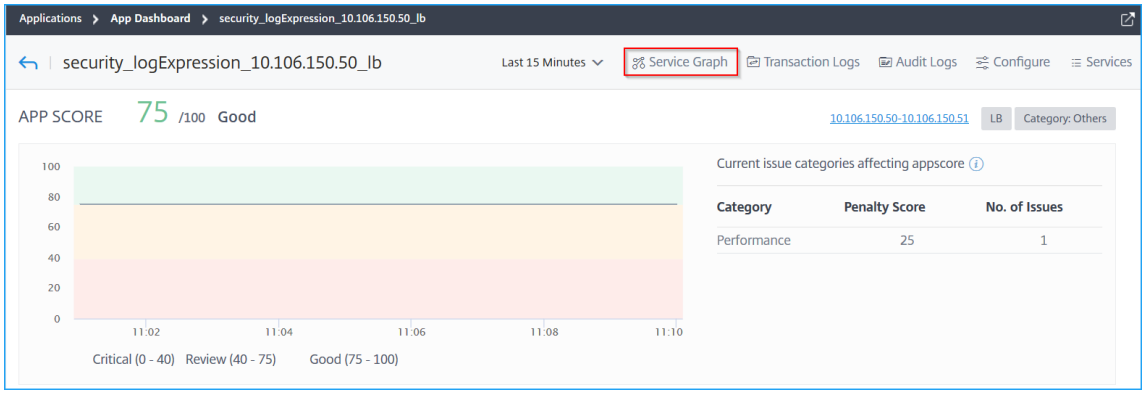
Graphique de service pour les applications Web à 3 niveaux

April 29, 2021

Pour afficher le graphique de service d'une application :

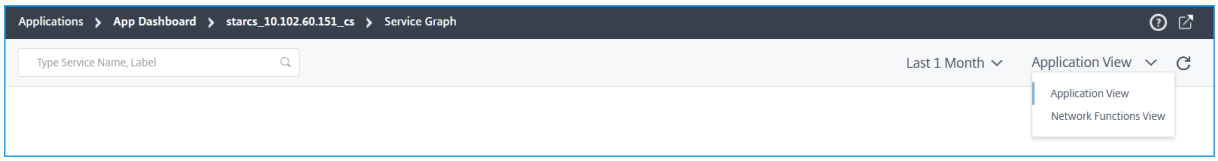
1. Accédez à **Applications** > **Tableau de bord**.
2. Sélectionnez une application.

   La page de détails de l'application s'affiche.
3. Sélectionnez la durée et cliquez sur **Service Graph**.



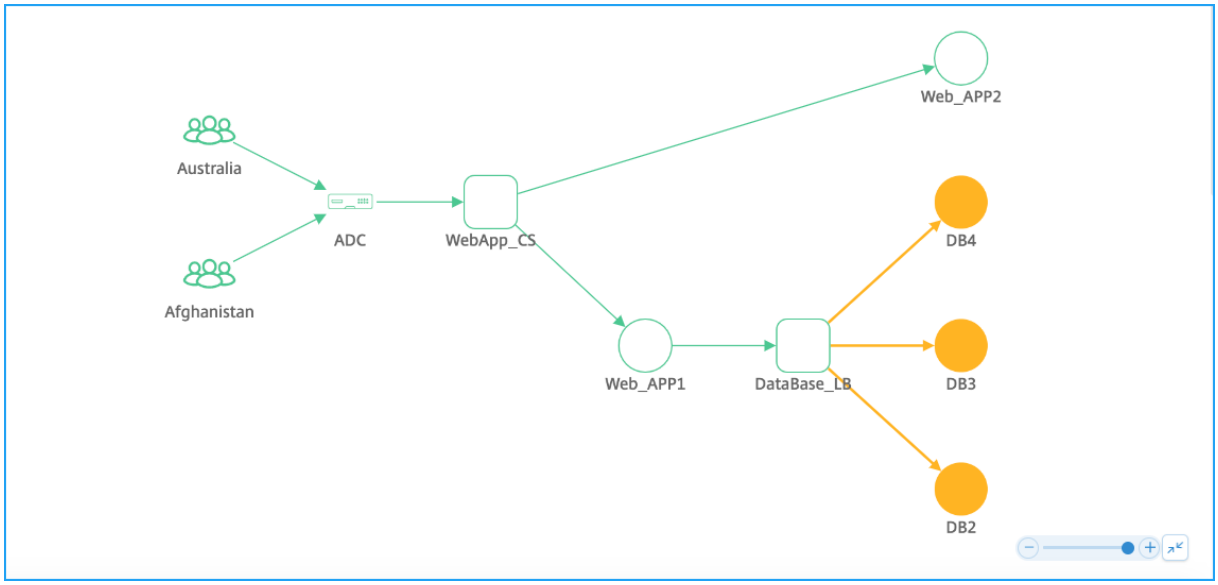
La page du graphique de service s'affiche pour l'application sélectionnée.

Vous pouvez afficher le graphique de service en **mode Application** ou en **mode Fonctions réseau**.

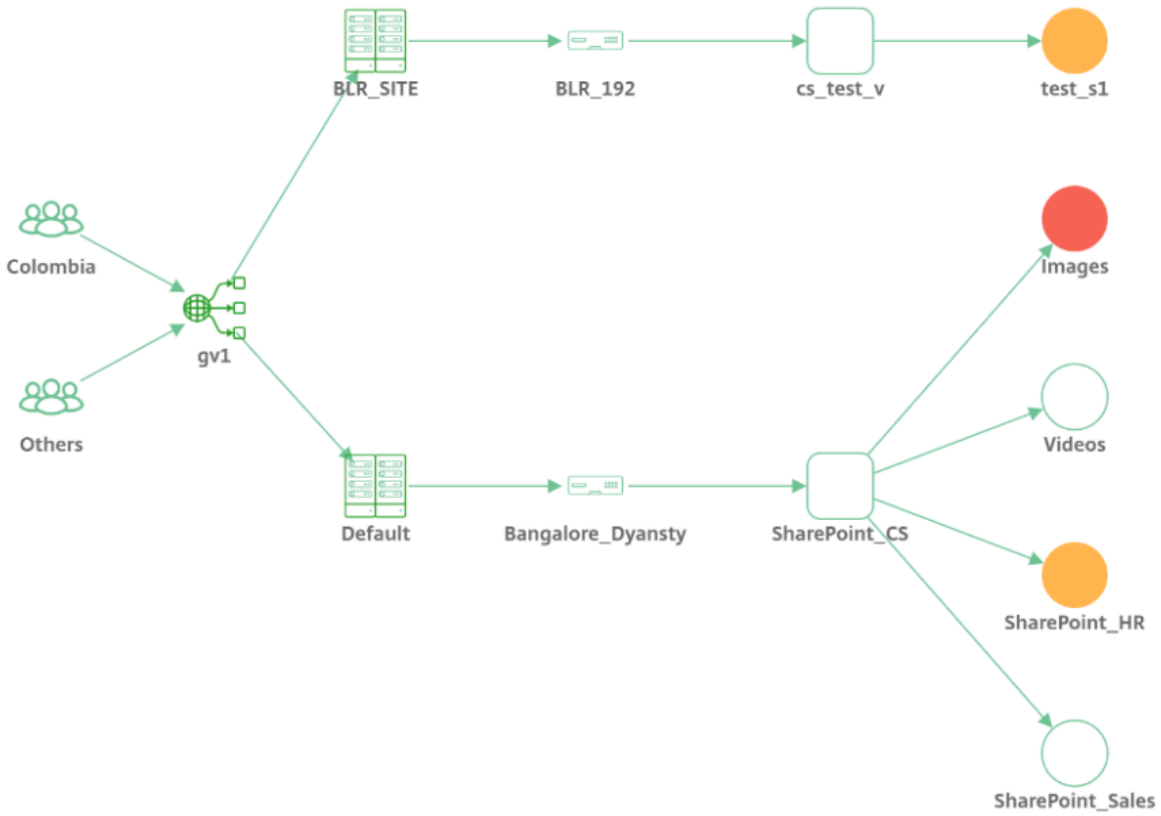


Vue de l'application

Affiche la vue d'ensemble de la configuration de l'application. Dans cette vue, vous pouvez visualiser la communication entre les applications client, ADC et Web.



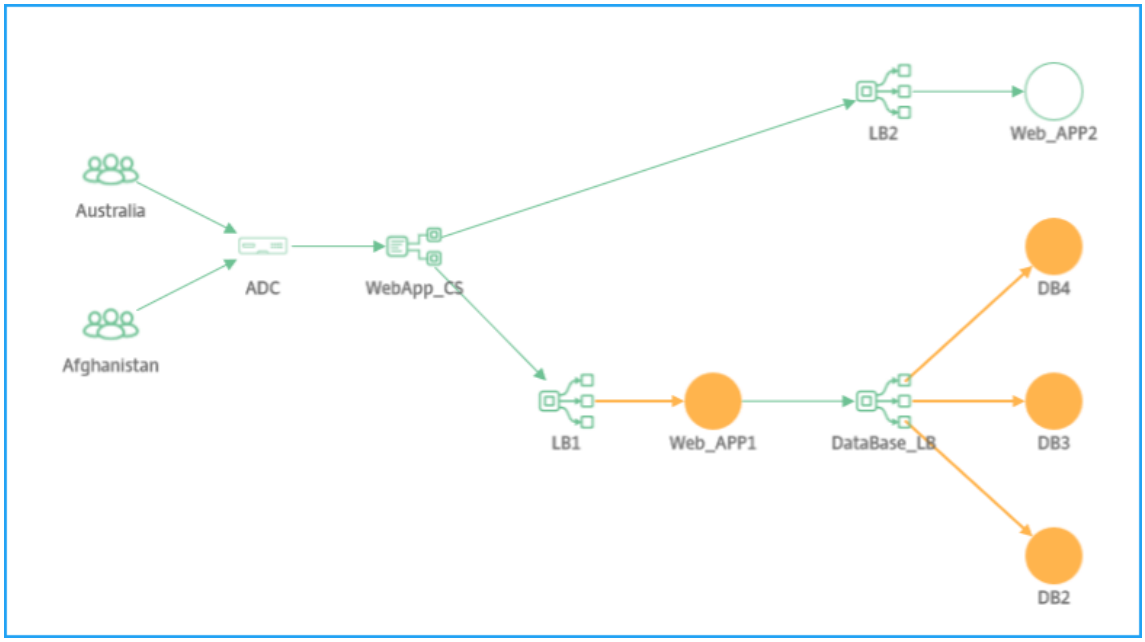
Pour une application GSLB, vous pouvez visualiser la communication entre le client, le centre de données, l'ADC et les services.



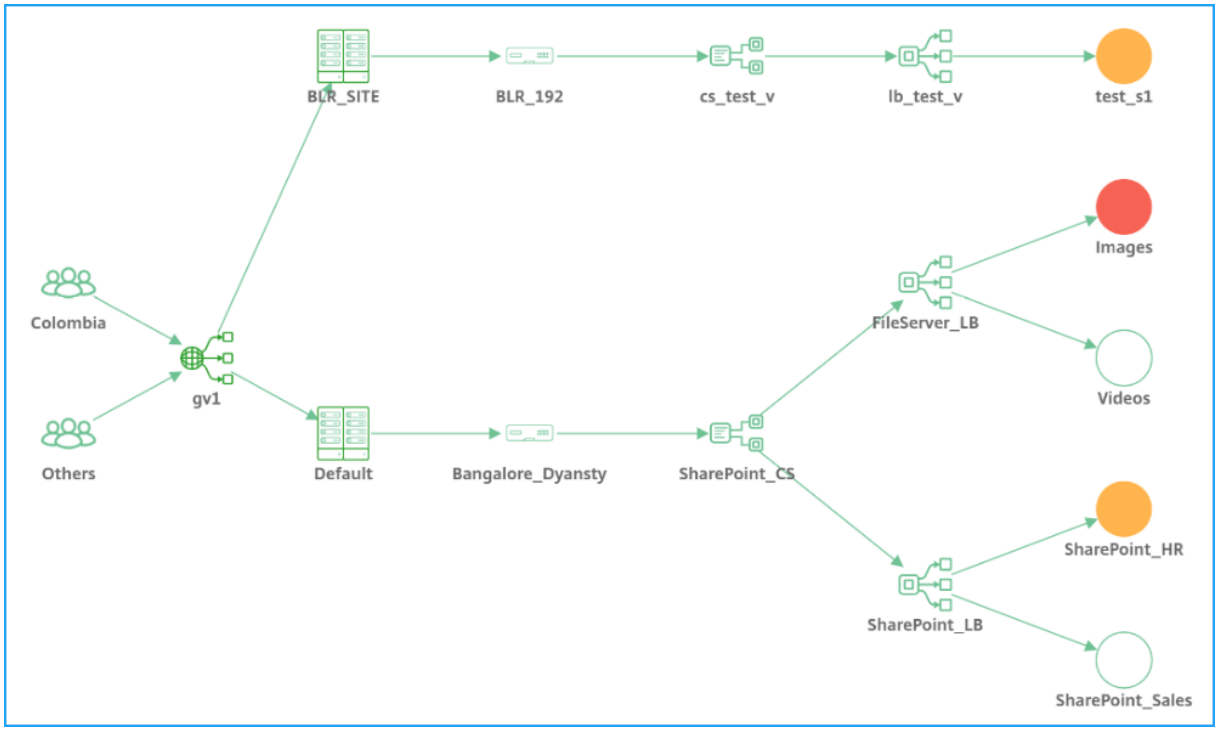
Vue des fonctions réseau

Affiche les serveurs virtuels associés à l'application. Dans cette vue, vous pouvez visualiser si ADC communique avec :

- Serveur virtuel de commutation de contenu pour accéder à l'application
- Serveur virtuel d'équilibrage de charge pour accéder à l'application
- Serveurs virtuels de commutation de contenu et d'équilibrage de charge pour accéder à l'application

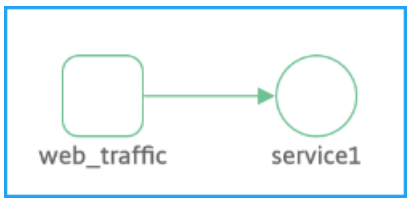


Pour l'application GSLB, les détails sont affichés avec le centre de données et Citrix ADC.

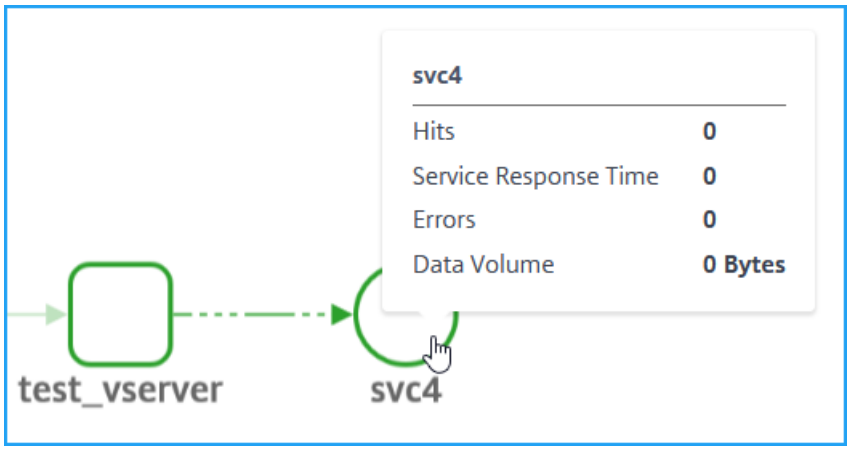


Affichage graphique de service pour aucune transaction active

Si aucune transaction active ne se produit entre ADC et l'application Web, le graphique de service affiche uniquement la configuration de base de l'application (sans client et ADC).



Lorsque vous placez le pointeur de la souris sur un service ou un serveur virtuel, les détails sont affichés sous la forme 0 pour toutes les mesures en raison de l'absence de transactions.

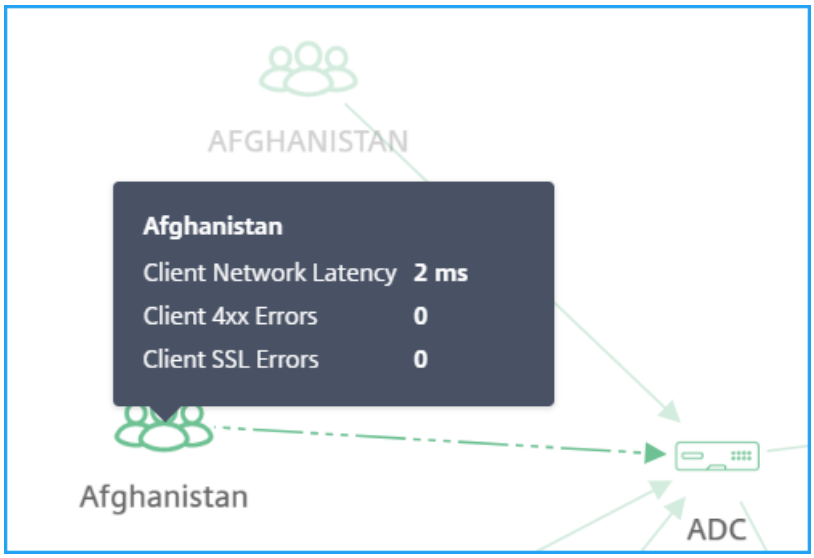


Analyser les mesures

Placez le pointeur de la souris sur chaque service pour afficher les détails des mesures en **mode Application** ou **Fonction réseau**.

Mesures client

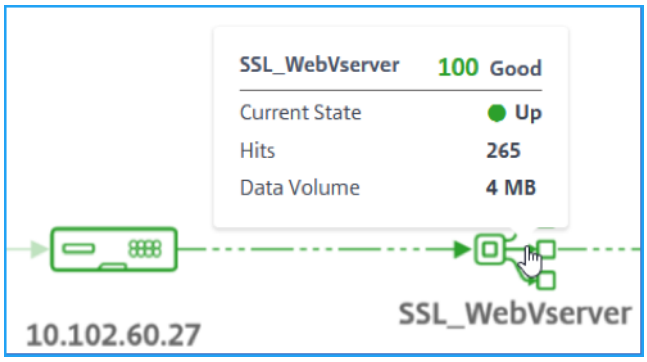
Placez le pointeur de la souris sur le client pour afficher les mesures du client.



- **Latence réseau client** : indique la latence réseau du client.
- **Erreurs 4xx client** — Indique le nombre total d'erreurs 4xx survenues à partir du client.
- **Erreurs SSL client** : indique le nombre total d'erreurs SSL provenant du client.

Mesures de fonction réseau

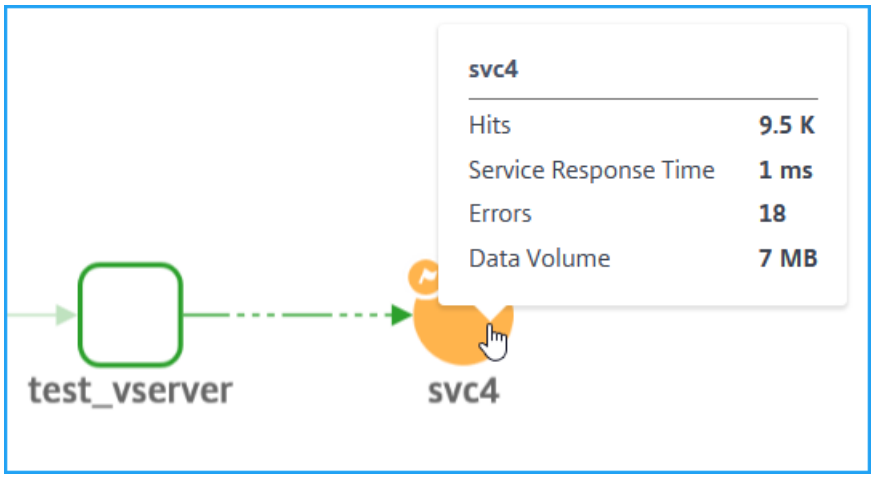
Placez le pointeur de la souris sur un service d'équilibrage de charge ou de commutation de contenu pour afficher les détails des mesures.



- **État actuel** — Indique l'état actuel du serveur virtuel
- **Hits** — Indique le nombre total d'accès reçus par le serveur virtuel
- **Volume de données** : indique le volume total de données traité par le serveur virtuel

Mesures de service

Placez le pointeur de la souris sur un service (application Web) pour afficher les mesures

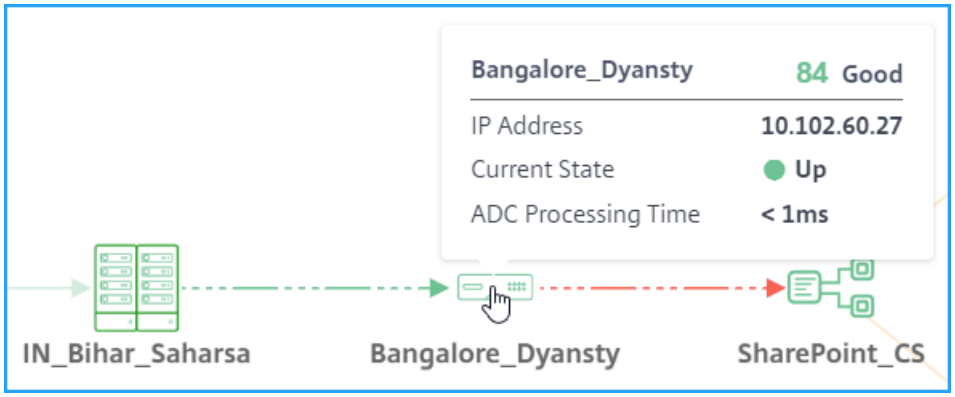


- **Hits** — Indique le nombre total d'accès reçus par le service
- **Temps de réponse du service** : indique le temps de réponse moyen du service

- **Erreurs** — Indique le total des erreurs se sont produites à partir du service
- **Volume de données** : indique le total des données traitées par le service

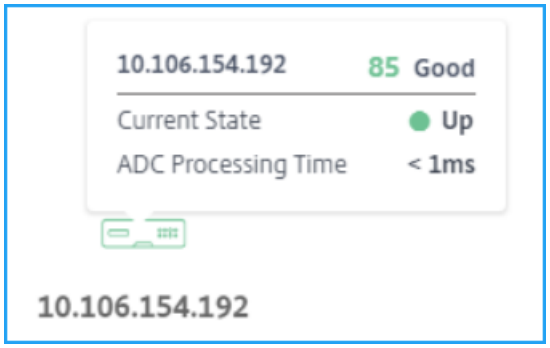
Mesures Citrix ADC (uniquement pour les applications GSLB)

Placez le pointeur de la souris sur ADC pour afficher les mesures.



- Affiche le nom d'hôte et le score ADC actuel. Le score est calculé en fonction des différents problèmes potentiels de Citrix ADC. Pour de plus amples informations, consultez la section Score d'instance.
- **Adresse IP** — Indique l'adresse IP Citrix ADC
- **État actuel** : indique l'état de Citrix ADC, par exemple : En haut, en bas ou hors service.
- **Temps de traitement ADC** : indique le temps de traitement moyen par l'instance ADC

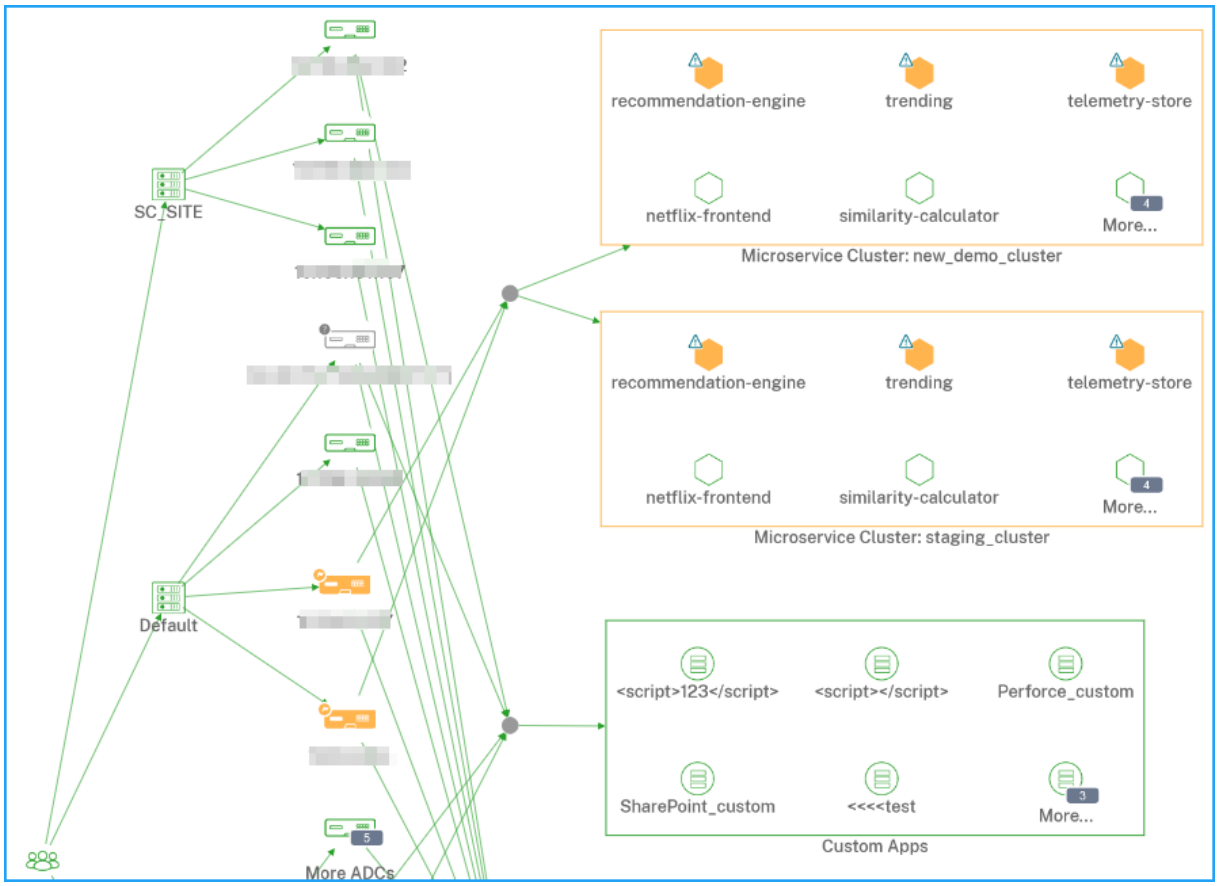
> **Remarque**
>
> Si aucun nom d'hôte n'est attribué à Citrix ADC :
>
> -l'adresse IP Citrix ADC est affichée à la place du nom d'hôte.
>
> -Dans les mesures, les informations d'adresse IP Citrix ADC ne s'affichent pas.



Vue holistique de toutes les applications dans le graphique de service

April 29, 2021

Accédez à **Applications** > **Graphique de service**, puis cliquez sur **Global**.



Le graphique de service affiche les éléments suivants pour la durée sélectionnée :

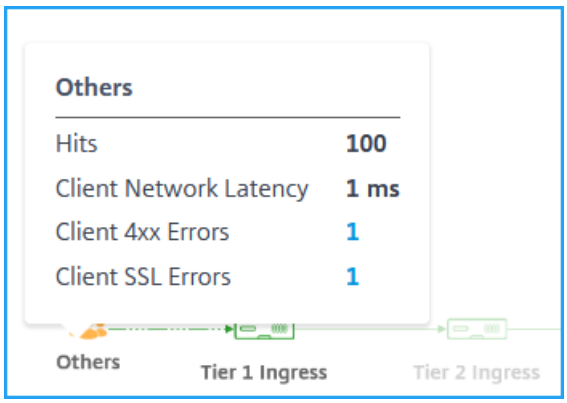
- Région à partir de laquelle les utilisateurs accèdent à l'application spécifique
- Centres de données où les instances Citrix ADC sont hébergées
- Nombre total d'applications discrètes de toutes les instances Citrix ADC

  > **Remarque**
  >
  > Si une instance Citrix ADC ne possède pas d'applications discrètes, la flèche vers le serveur virtuel discret à partir de l'instance Citrix ADC n'est pas visible

- Nombre total d'applications personnalisées de toutes les instances Citrix ADC
- Nombre total d'applications de microservice à partir de l'instance Citrix ADC CPX

Afficher les mesures client

Placez le pointeur de la souris sur une région cliente pour afficher les mesures.

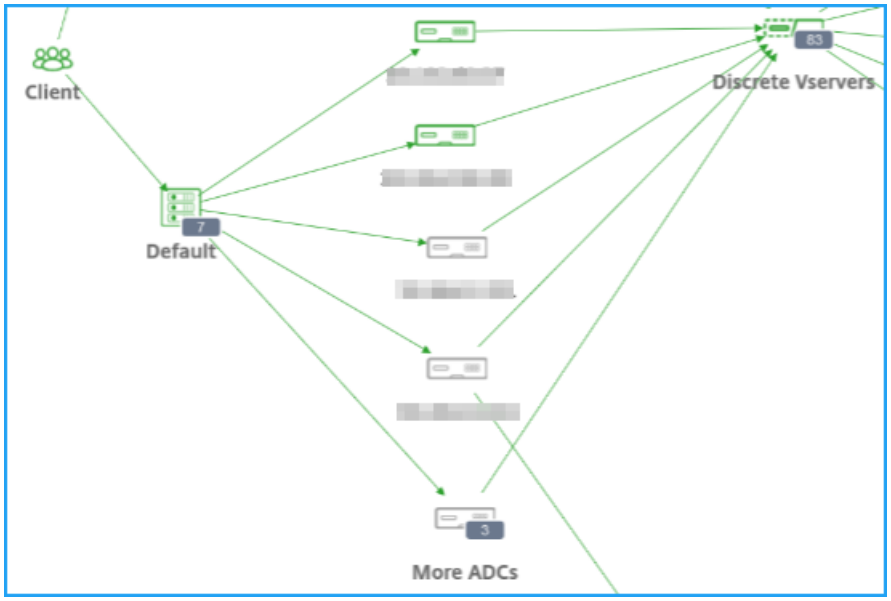


- **Latence réseau client** - Indique la latence moyenne du réseau client.
- **Erreurs client 4xx** - Indique le total des erreurs 4xx client.
- **Erreurs SSL client** - Indique le nombre total d'erreurs SSL client.

Afficher les détails de Citrix ADC

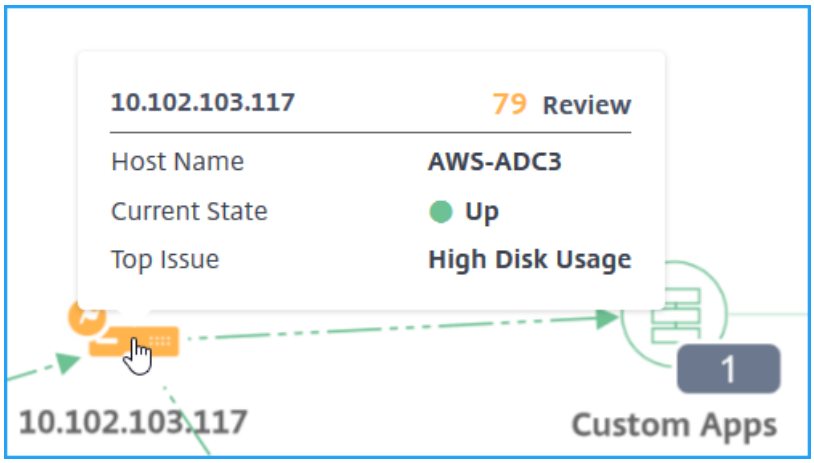
Le graphique de service vous permet d'afficher :

- Le centre de données regroupé avec son nombre total d'instances Citrix ADC
- Seules les 4 premières instances Citrix ADC à faible score de chaque centre de données



Cliquez sur **Autres ADC** pour afficher toutes les instances Citrix ADC en sélectionnant les onglets d'état respectifs (Critique, Révision, Bon et Non applicable).

Placez le pointeur de la souris sur une instance Citrix ADC pour afficher les mesures.



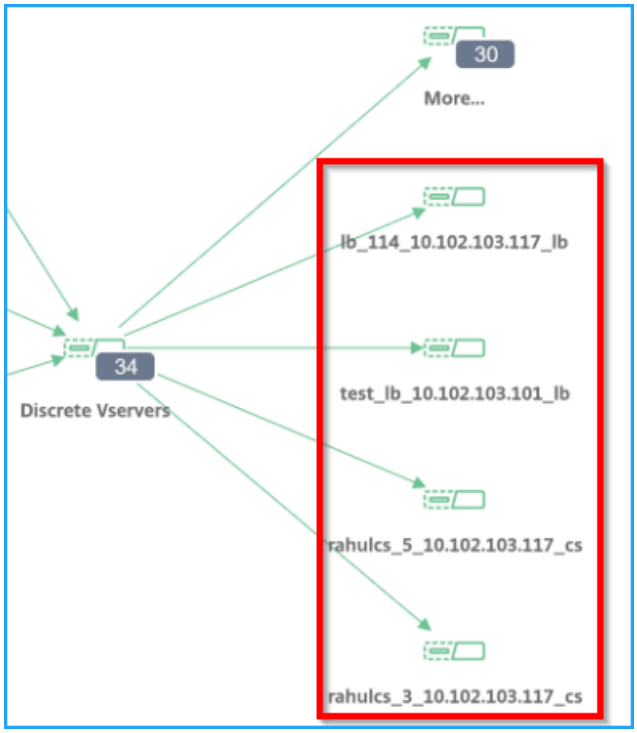
Vous pouvez voir :

- Adresse IP et score de l'instance Citrix ADC
- **Nom d'hôte** — Indique le nom d'hôte affecté à l'instance Citrix ADC
- **État actuel** — Indique l'état actuel de l'instance Citrix ADC, par exemple, en haut, en panne, en panne.
- **Problème le plus** élevé — Indique le problème le plus élevé qui affecte le score Citrix ADC actuel

Cliquez sur l'**instance Citrix ADC** pour afficher les détails de l'instance, tels que le score de l'instance, les mesures clés et les problèmes associés à l'instance ADC. Pour de plus amples informations, consultez la section Afficher les détails de l'instance dans Infrastructure Analytics.

Afficher les applications discrètes

Le graphique de service affiche les 4 applications discrètes notées les plus faibles.



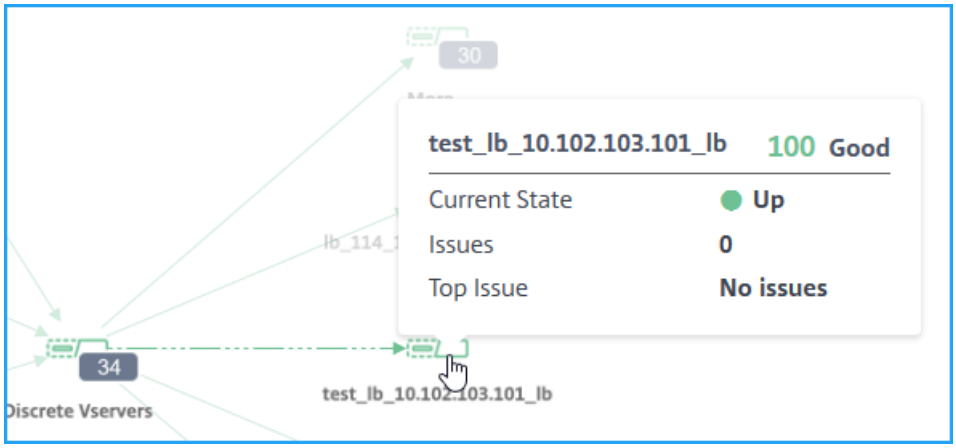
Considérez que vous avez les applications discrètes suivantes :

Nom app	Citrix ADC	AppScore	État de l'application
App1	10.102.29.50	35 (Critique)	Actif
App2	10.102.29.90	100 (Bon)	Bas
Appli 3	10.102.32.40	49 (Revue)	Actif
App4	10.102.113.208	92 (Bon)	Bas
App5	10.102.25.25	86 (Bon)	Actif
App6	10.102.29.41	77 (Bon)	Actif
App7	10.102.29.102	41 (Revue)	Actif

Dans ce scénario, vous pouvez afficher App1, App3, App6 et App 7 comme les 4 applications les plus faibles dans le graphique de service.

De même, vous pouvez également afficher les 4 applications les plus faibles pour les applications **personnalisées** et **Microservices**.

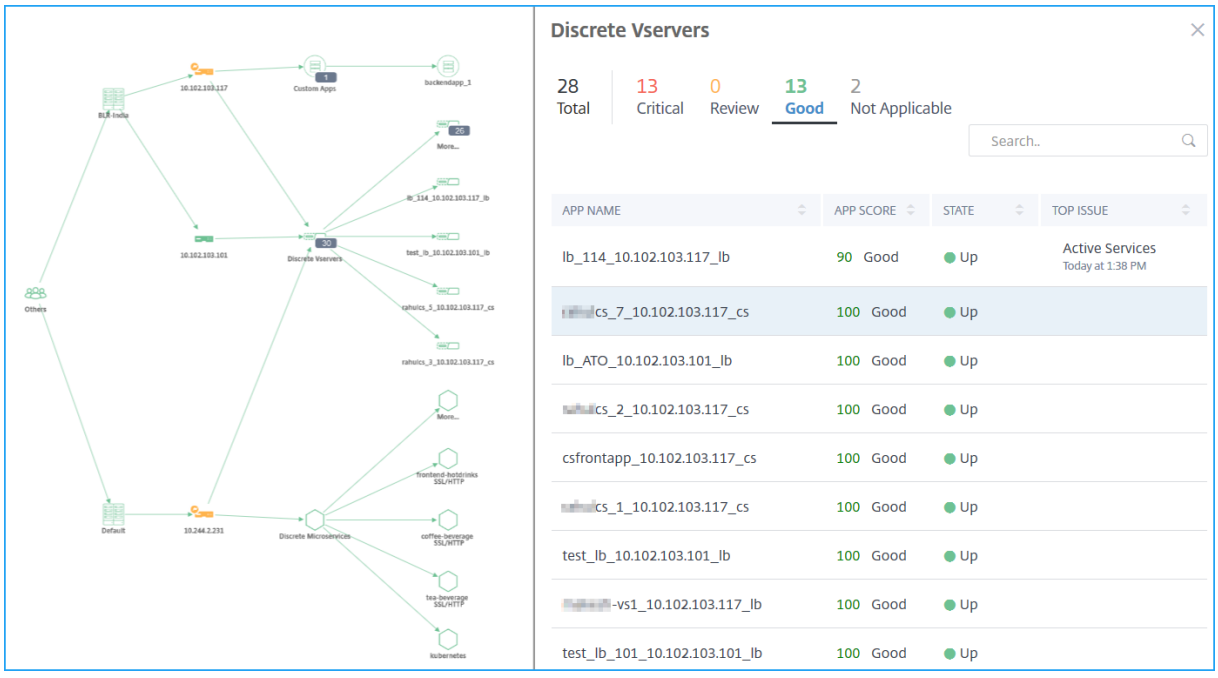
Placez le pointeur de la souris sur un service pour afficher les informations sur les mesures.



Vous pouvez voir :

- Le nom et le score de l'application
- **État actuel** — Indique l'état actuel de l'application, par exemple, haut ou bas
- **Questions** — Indique le nombre total de questions applicables à la demande
- **Problème le plus** élevé — Indique le problème le plus élevé qui a une incidence sur le score global des demandes

Cliquez sur **Plus** pour afficher toutes les applications discrètes. La page Serveur virtuel discret s'affiche comme illustré dans l'image suivante :

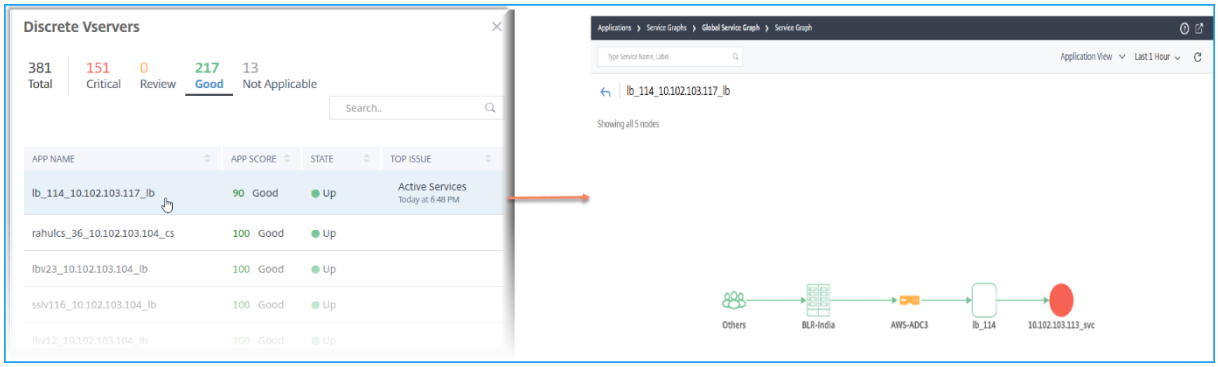


Les serveurs virtuels sont affichés en fonction de l'état.

- **Total** — Total des applications discrètes

- **Critique** — Le score de l'application est compris entre 0 et < 40
- **Évaluations** — Le score de l'application est compris entre 40 et < 75
- **Bon** — Le score de l'application est > 75
- **Non applicable** — L'application n'est liée à aucun serveur virtuel

Vous pouvez cliquer sur chaque onglet pour afficher les serveurs virtuels. Lorsque vous cliquez sur une application, le graphique de service de l'application sélectionnée s'affiche.



Pour de plus amples informations, consultez la section Graphique de service pour les applications.

Afficher les applications de microservices

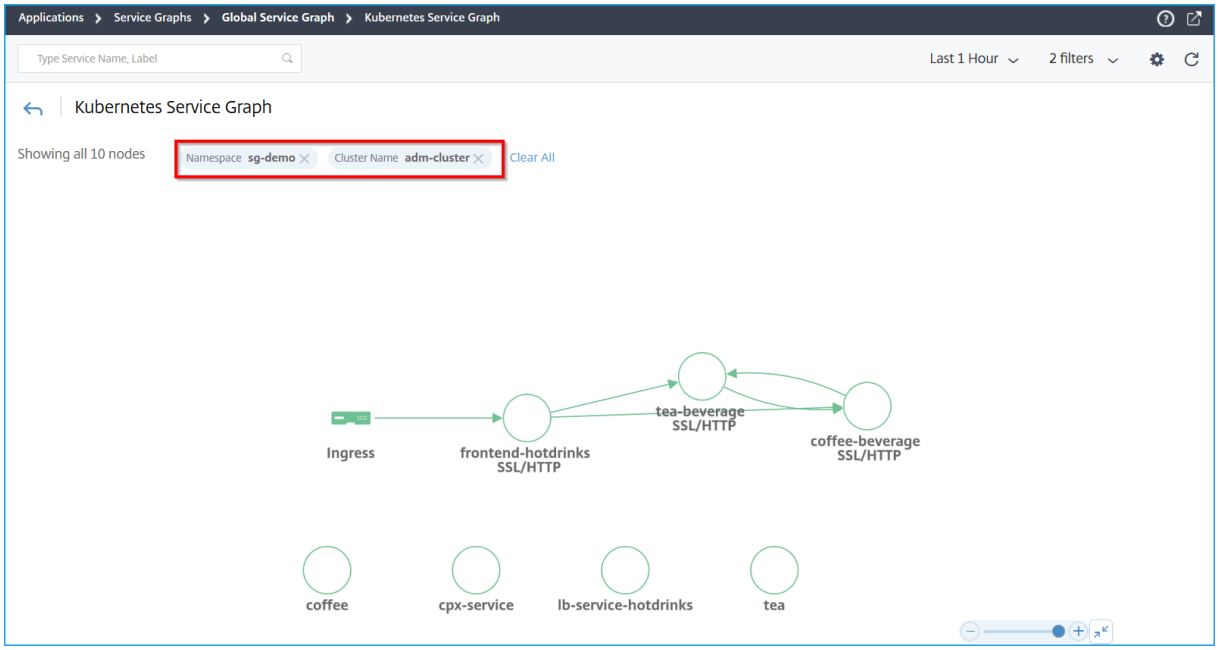
Le graphique de service affiche également toutes les applications de microservice appartenant aux clusters Kubernetes. Placez le pointeur de la souris sur un service pour afficher les détails des mesures.

Vous pouvez voir :

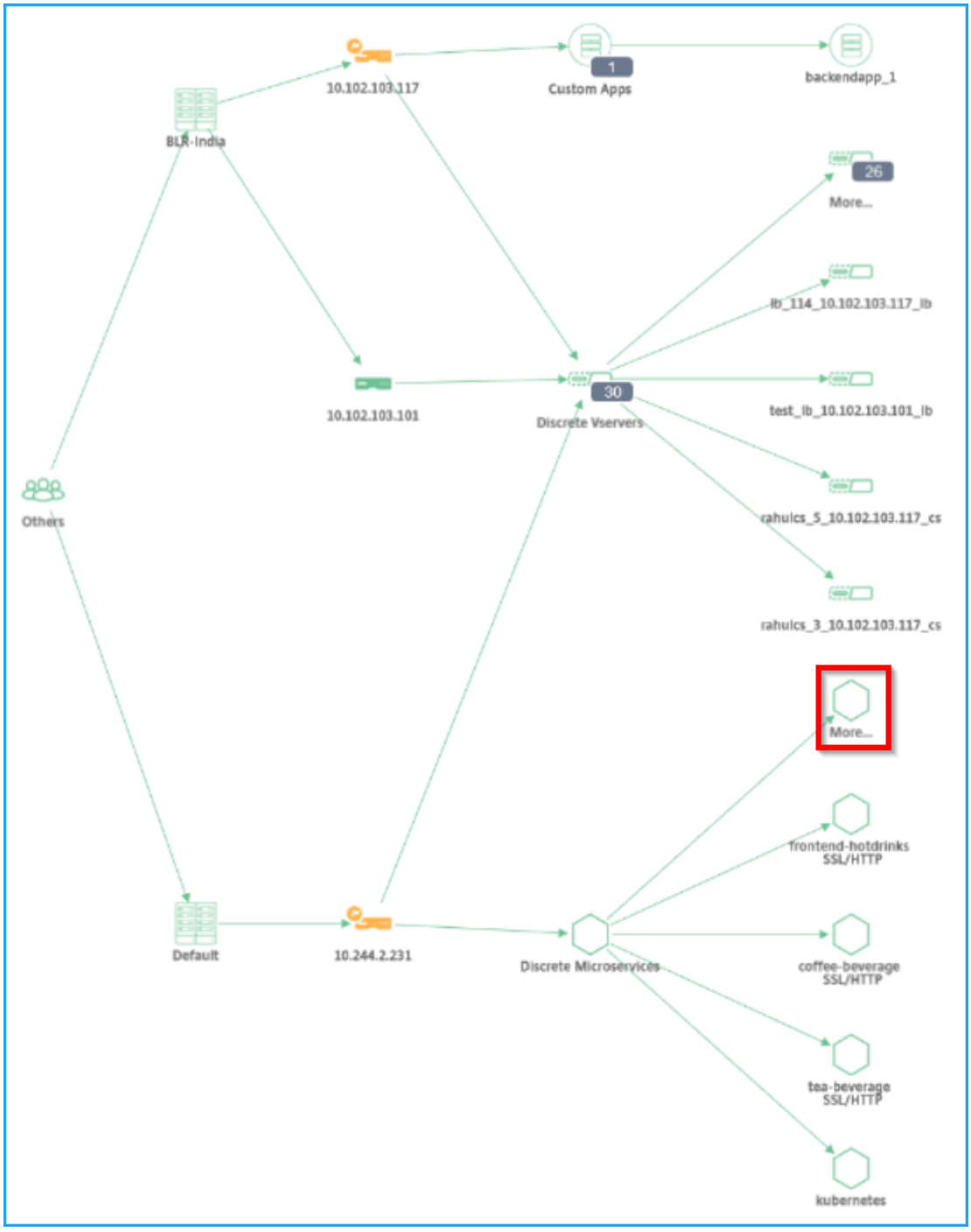
- Le nom du service
- Le protocole utilisé par le service tel que SSL, HTTP, TCP, SSL sur HTTP
- **Hits** — Nombre total d'accès reçus par le service
- **Temps de réponse du service** — Temps de réponse moyen pris par le service.

  (Temps de réponse = RTT client + demande le dernier octet — demande le premier octet)
- **Erreurs** — Les erreurs totales telles que 4xx, 5xx, et ainsi de suite
- **Volume de données** — Volume total de données traitées par le service
- **Espace de noms** — Espace de noms du service
- **Nom du cluster** — Nom du cluster où le service est hébergé
- **Erreurs SSL Server** : nombre total d'erreurs SSL provenant du service

Lorsque vous cliquez sur un service, le graphique de service Kubernetes pour le service sélectionné s'affiche, ainsi que l'espace de noms de service et les filtres de noms de cluster appliqués.



Cliquez sur **Plus** pour afficher le graphique des services Kubernetes qui contient tous les services. Pour plus d'informations sur le graphique de service Kubernetes, reportez-vous à la section Graphique de service pour les applications natives du cloud.



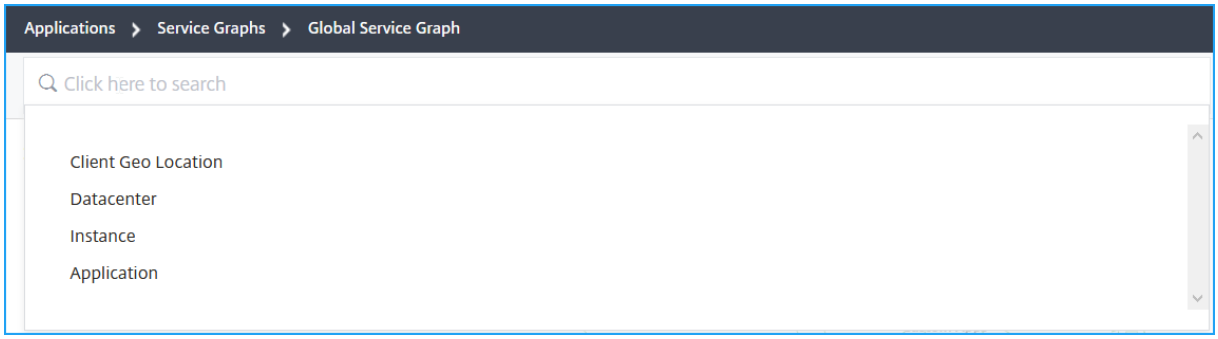
barre de recherche pour filtrer les résultats

Vous pouvez utiliser la barre de recherche pour filtrer les résultats. En tant qu'administrateur, cette barre de recherche vous permet de réduire rapidement une instance/client/application/centre de données particulier, lorsque vous avez :

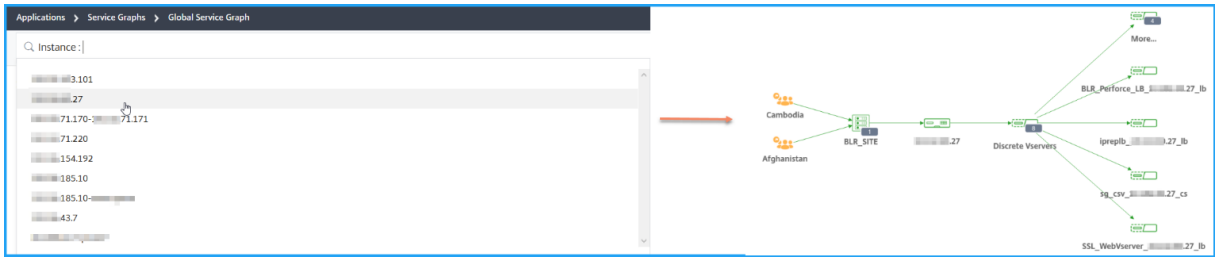
- Une grande entreprise avec de nombreux centres de données

- Configuration de nombreuses instances Citrix ADC pour chaque centre de données
- Configuration de nombreuses applications déployées ou accessibles via chaque instance Citrix ADC
- Clients accédant à l'application depuis différents emplacements

Placez le pointeur de la souris sur la barre de recherche et sélectionnez la catégorie que vous souhaitez créer le filtre.



Par exemple, si vous souhaitez afficher une instance ADC particulière, sélectionnez Instance dans la barre de recherche et sélectionnez l'adresse IP de l'instance. Le graphique de service global affiche l'instance sélectionnée et ses applications, centres de données et emplacements clients associés.



StyleBooks

April 29, 2021

StyleBooks simplifie la tâche de gestion des configurations Citrix ADC complexes pour vos applications. Un StyleBook est un modèle que vous pouvez utiliser pour créer et gérer des configurations de Citrix ADC. Vous pouvez créer un StyleBook pour configurer une fonctionnalité spécifique de Citrix ADC, ou concevoir un StyleBook pour créer des configurations pour un déploiement d'application d'entreprise tel que Microsoft Exchange ou Lync.

StyleBooks s'intègre parfaitement aux principes de l'infrastructure en tant que code qui est pratiquée par les équipes DevOps, où les configurations sont déclaratives et contrôlées par version. Les config-

urations sont également répétées et sont déployées dans leur ensemble. StyleBooks offre les avantages suivants :

- **Déclaratif** : StyleBooks sont écrits dans une syntaxe déclarative plutôt que impérative. 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 ADC particulière. Citrix ADM calcule la différence entre l'état existant sur un ADC et l'état souhaité que vous avez spécifié, et effectue 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 de ces configurations 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 distingue de manière unique de n'importe quel autre StyleBook du système. Toute modification apportée à un StyleBook nécessite une mise à jour de son numéro de version (ou de son nom ou de son espace de noms) pour conserver ce caractère unique. La mise à jour de version vous permet également de gérer plusieurs versions du même StyleBook.
- **Composable** : Une fois qu'un StyleBook est défini, le StyleBook peut être utilisé comme une unité pour construire d'autres StyleBooks. Vous pouvez éviter de répéter des modèles de configuration courants. Il vous permet également d'établir des blocs de construction standard dans votre organisation. Étant donné que les StyleBooks sont versionnés, les modifications apportées aux StyleBooks existants entraînent de nouveaux StyleBooks, garantissant ainsi que les StyleBooks dépendants ne sont jamais accidentellement cassés.
- **App-Centric** : StyleBooks peut être utilisé pour définir la configuration Citrix ADC d'une application complète. La configuration de l'application peut être abstraite en utilisant des 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 ADC complexe. Les configurations créées à partir de StyleBooks ne sont pas liées à l'infrastructure. Une configuration unique peut donc être déployée sur une ou plusieurs instances 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 terminée à l'aide de l'interface graphique Citrix ADM. Les auteurs de StyleBook n'ont pas besoin d'apprendre un nouveau langage GUI ou de créer séparément des pages et des formulaires d'interface utilisateur.
- **Piloté par API** : toutes les opérations de configuration sont prises en charge à l'aide de l'interface graphique Citrix ADM ou via les API REST. Les API peuvent être utilisées en mode synchrone ou asynchrone. En plus des 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 seul StyleBook pour créer plusieurs configurations. Chaque configuration est enregistrée en tant que config pack. 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 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 ou sur une instance différente. Un nouveau pack de configuration est créé pour cette configuration. Un pack de configuration est enregistré à la fois sur ADM et sur l'instance 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 StyleBooks pour créer des configurations à l'aide de l'interface graphique Citrix ADM ou à l'aide d'API.

Ce document contient les renseignements suivants :

- Comment afficher StyleBooks
- StyleBooks par défaut
- StyleBooks développés pour les applications professionnelles
- StyleBooks personnalisés
- API dans StyleBooks
- Grammaire StyleBooks

Groupes StyleBook

April 29, 2021

Il existe deux groupes StyleBook dans Citrix Application Delivery Management (ADM). Il s'agit des StyleBooks par défaut et des StyleBooks personnalisés. Qu'il s'agisse d'une valeur par défaut ou personnalisée, un StyleBook est un StyleBook public ou privé. Dans Citrix ADM, vous pouvez afficher tous les StyleBooks présents dans le système, quel que soit leur type ou leur état de visibilité. Vous pouvez également afficher un affichage graphique de la façon dont StyleBooks sont connectés les uns aux autres.

Ce document explique les différents types de StyleBooks. En outre, il explique les actions suivantes que vous pouvez effectuer sur les StyleBooks à partir de Citrix ADM :

- Téléchargez un StyleBook personnalisé et apportez des modifications, ou créez un StyleBook basé sur un StyleBook existant.

- Masquer les StyleBooks par défaut d'ADM.
- Supprimez un StyleBook personnalisé de Citrix ADM.
- Ajoutez des balises aux StyleBooks.

StyleBooks personnalisés et par défaut

- **StyleBooks par défaut** sont les StyleBooks livrés avec Citrix ADM et ils vous permettent de créer des configurations que vous pouvez déployer sur vos instances Citrix ADC. Vous ne pouvez pas supprimer StyleBooks par défaut, mais vous pouvez les masquer à partir de l'interface graphique ADM.
- **StyleBooks personnalisés** sont vos propres StyleBooks que vous avez importés dans Citrix ADM.

StyleBooks par défaut et personnalisé peuvent être publics ou privés.

Livres de style publics et privés

Les StyleBooks à partir desquels vous pouvez créer des packs de configuration peuvent être classés comme livres de style **publics**. C'est-à-dire qu'ils sont tous disponibles pour votre utilisation directe afin de créer des configurations à partir de l'interface graphique et des API Citrix ADM.

Mais, certains StyleBooks sont utilisés comme blocs de construction pour d'autres StyleBooks. De tels StyleBooks sont marqués comme **privés**. Les StyleBooks privés ne peuvent pas être directement utilisés pour créer des packs de configuration à partir de l'interface graphique Citrix ADM. Mais, vous pouvez toujours afficher et afficher ces StyleBooks sur Citrix ADM. Pour marquer l'un de vos StyleBooks personnalisés comme **privé**, définissez l'attribut private dans le StyleBook sur **true**. Vous pouvez toujours utiliser des StyleBooks privés pour créer des packs de configuration à l'aide des API Citrix ADM.

Exemple d'un StyleBook marqué comme privé

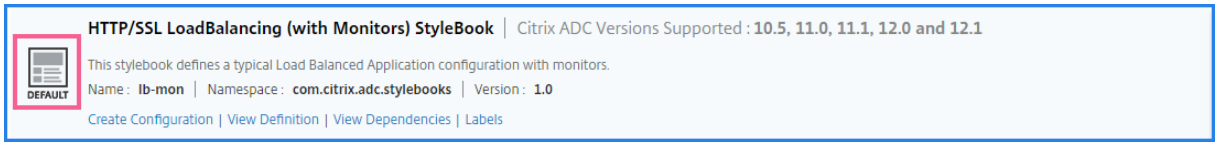
```
name: basic-lb-config
namespace: com.example.stylebooks
version: "0.1"
display-name: Load Balancing Configuration
description: |
    This StyleBook defines a simple load balancing configuration and is
        a building block to build other load balancing configurations.
schema-version: "1.0"
private: true
<!--NeedCopy-->
```


Afficher StyleBooks

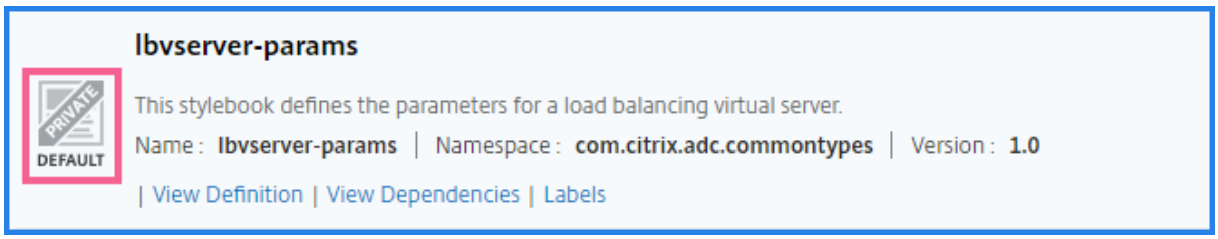
Le nombre de StyleBooks - par défaut et privé augmentent dans Citrix ADM. Vous pouvez rechercher le StyleBook particulier auquel vous souhaitez accéder. Vous pouvez également afficher les deux types de StyleBooks séparément.

Dans Citrix ADM, lorsque vous accédez à **Applications** > **StyleBooks**, vous pouvez afficher une liste de StyleBooks présents dans le système.

Un StyleBook public par défaut comporte l'icône suivante dans son panneau :

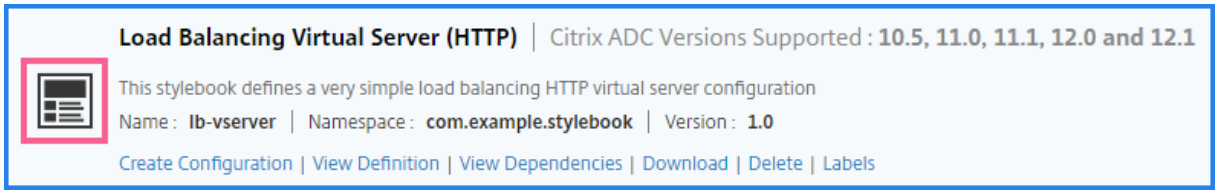


Attendu qu'un StyleBook privé par défaut possède une icône qui le déclare en tant que StyleBook privé :

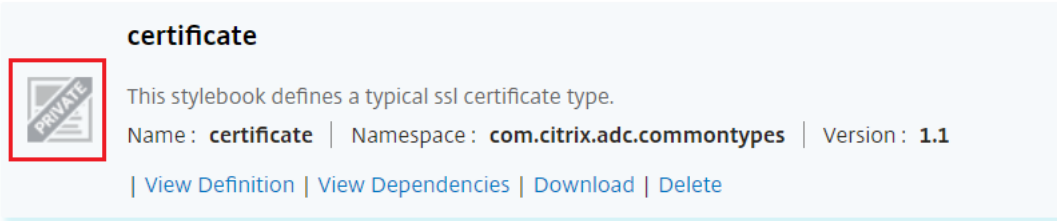


Bien que vous puissiez afficher la définition et les dépendances d'un StyleBook privé, vous ne pouvez pas créer de packs de configuration à partir d'un StyleBook privé à l'aide de l'interface graphique. Le but principal d'un StyleBook privé est de l'utiliser comme bloc de construction pour un autre StyleBook. L'utilisation des Building-Blocks-StyleBooks encourage la réutilisation des modèles de configuration courants.

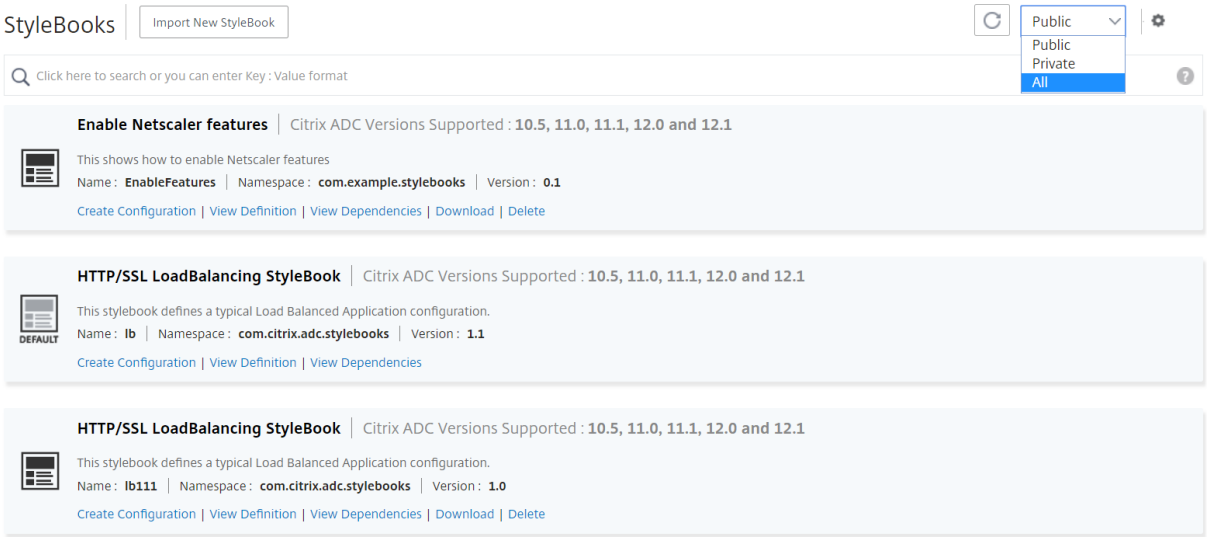
Un StyleBook public personnalisé a une icône différente, comme indiqué dans l'image suivante :



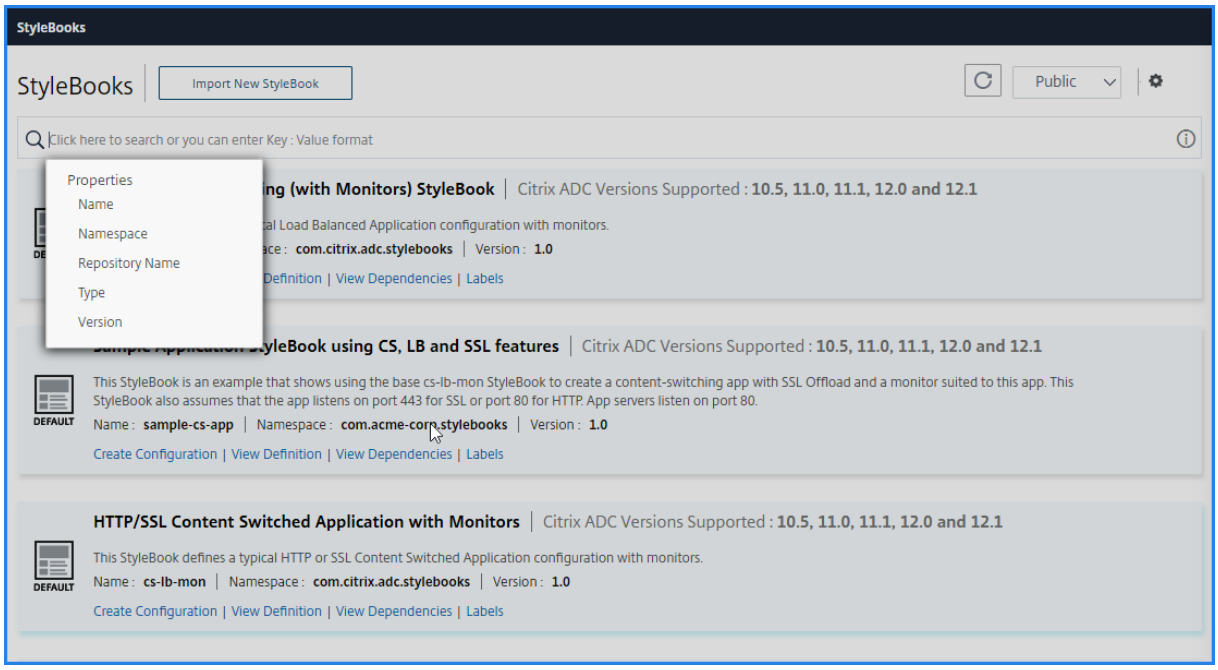
Alors qu'un StyleBook privé personnalisé apparaît avec cette icône :



En haut à droite de la page, vous pouvez voir une option permettant de sélectionner le type de StyleBooks à afficher. Il y a trois options - toutes, publiques ou privées StyleBooks. Cliquez sur l'une des options.



Vous pouvez également rechercher un StyleBook particulier en cliquant sur l'icône de recherche. Vous pouvez effectuer une recherche par nom, espace de noms et attributs de version ou une combinaison de ces options. L'opération de recherche n'est pas sensible à la casse.

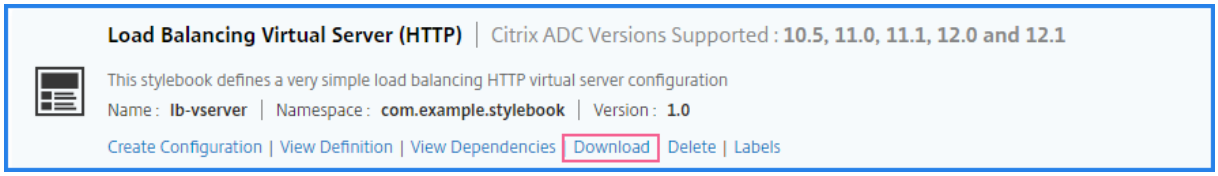


Télécharger des StyleBooks personnalisés

Pour télécharger les StyleBooks personnalisés à partir de Citrix ADM, accédez à **Applications** > **StyleBooks** > **Configurations**. Dans la liste des StyleBooks affichés dans le panneau de droite,

cochez l'option permettant de télécharger les StyleBooks personnalisés. Cliquez sur **Download (Télécharger)**. Si le StyleBook a des StyleBooks personnalisés dépendants, vous pouvez inclure les StyleBooks dépendants dans le bundle téléchargé.

> **Remarque**
>
> Vous pouvez télécharger des StyleBooks personnalisés marqués comme publics ou privés.

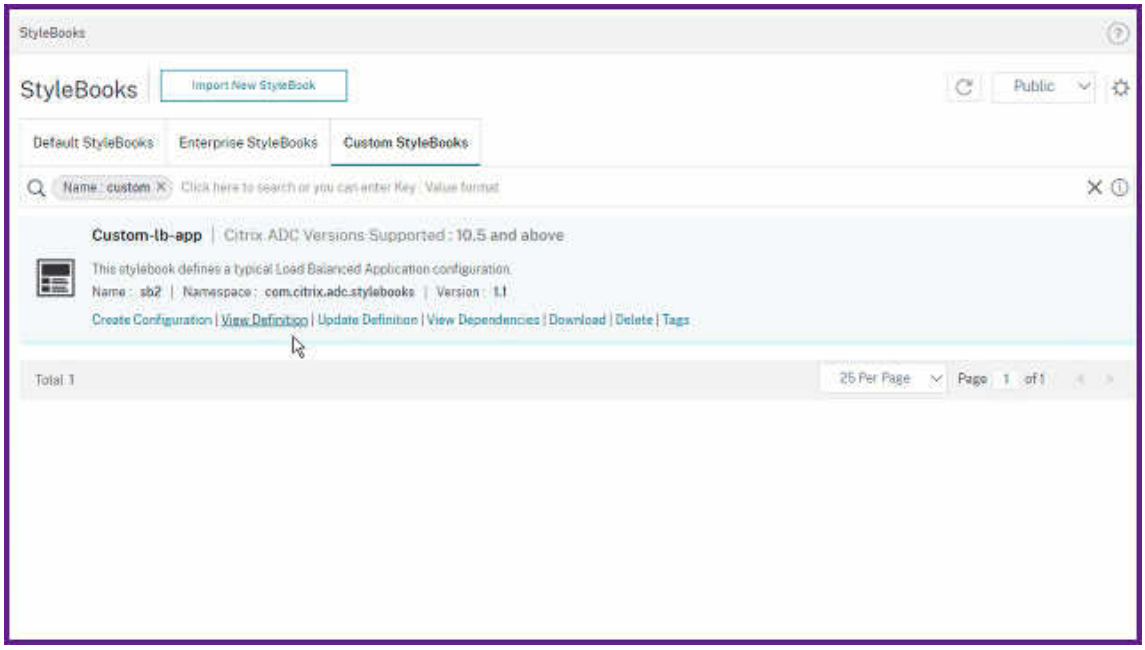


> **Remarque**
>
> Vous ne pouvez pas télécharger les StyleBooks par défaut de Citrix ADM. Vous pouvez afficher leurs définitions et dépendances. Pour ce faire, cliquez sur **les liens**Afficher la définition**et Afficher les dépendances** dans le panneau StyleBook.

Mettre à jour le StyleBook personnalisé

Vous pouvez mettre à jour les définitions de StyleBook personnalisées à partir de l'interface graphique ADM elle-même.

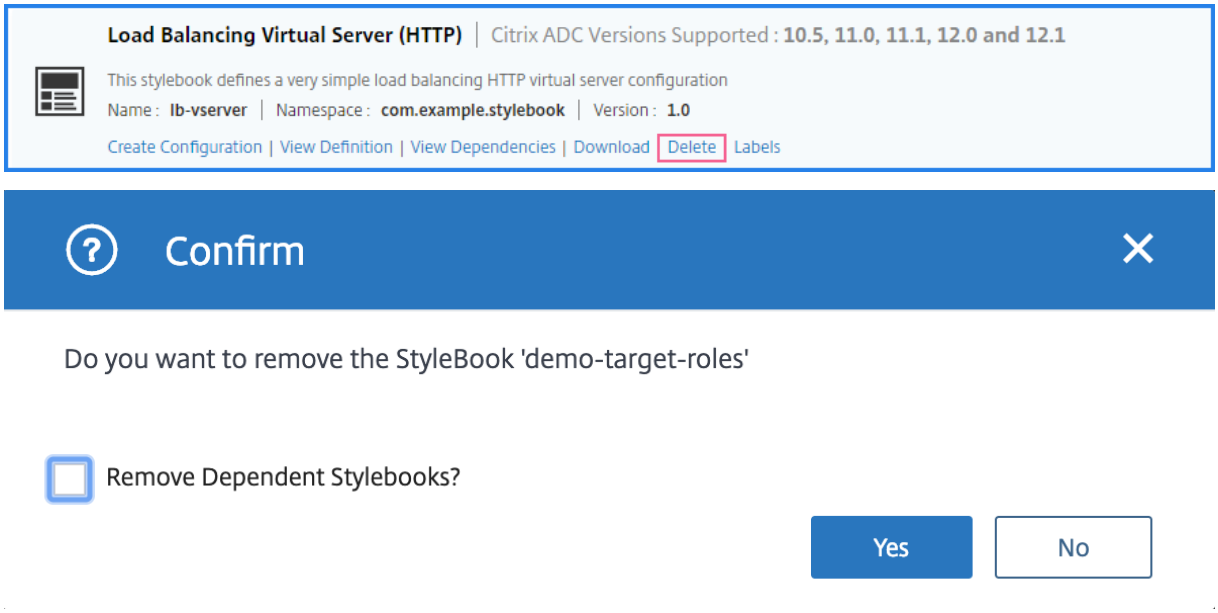
1. Accédez à **Applications > StyleBooks**.
2. Sélectionnez l'onglet **Livres styleBooks personnalisés**.
3. Sélectionnez **Mettre à jour la définition** dans le StyleBook que vous souhaitez mettre à jour.
4. Mettez à jour la définition selon les besoins et cliquez sur **Mettre à jour**.



5. Actualisez la page pour afficher les dernières modifications.

Supprimer des StyleBooks personnalisés

Vous pouvez également supprimer un StyleBook personnalisé en cliquant sur le bouton **Supprimer** . Une fenêtre contextuelle vous invite à confirmer si vous souhaitez supprimer le StyleBook de Citrix ADM. Si le StyleBook utilise d'autres StyleBooks personnalisés, vous pouvez choisir de supprimer ces StyleBooks en cochant la case.



> **Remarque**
>
> Ne supprimez pas un StyleBook personnalisé s'il a des StyleBooks dépendants dans Citrix ADM. Sinon, il casserait les StyleBooks existants.

Afficher les dépendances StyleBook

Une caractéristique importante et puissante de StyleBooks est qu'ils peuvent être utilisés comme blocs de construction pour d'autres StyleBooks. Vous pouvez importer un StyleBook dans un autre StyleBook. Un StyleBook importé est déclaré en tant que type et est utilisé par les composants ou les paramètres du second StyleBook. Vous pouvez étudier les StyleBooks par défaut existants dans Citrix ADM pour savoir comment un StyleBook peut être construit sur un autre StyleBook.

Citrix ADM vous permet d'afficher un affichage graphique de la manière dont StyleBooks sont connectés les uns aux autres. Cette représentation est particulièrement utile pour les StyleBooks complexes qui sont construits en utilisant d'autres StyleBooks comme blocs de construction. En regardant le graphique des dépendances, il est possible de voir les relations et les dépendances entre plusieurs StyleBooks.

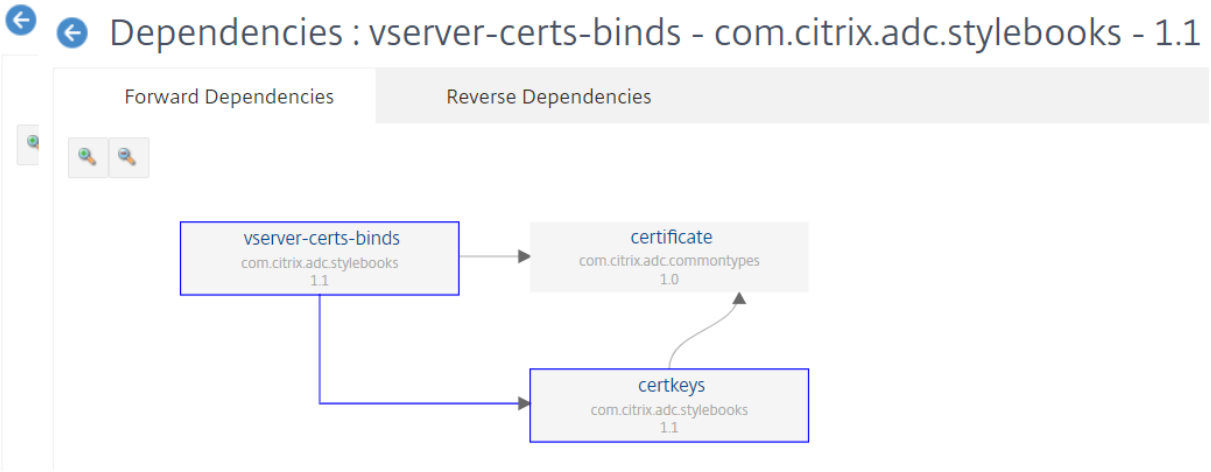
Un StyleBook utilisé par d'autres StyleBooks ne peut pas être supprimé du système car il briserait les StyleBooks existants. À l'aide de l'affichage du graphique des dépendances, vous pouvez identifier les StyleBooks qui empêchent la suppression d'un StyleBook.

Pour afficher les dépendances StyleBook

Dans Citrix ADM, accédez à **Applications** > **StyleBooks**. La page StyleBooks affiche tous les StyleBooks disponibles pour votre utilisation dans Citrix ADM. Faites défiler vers le bas et trouvez votre StyleBook. La vignette **StyleBook** affiche des liens permettant de créer une configuration, d'afficher la définition de StyleBook et d'afficher les dépendances StyleBook. Cliquez sur **Afficher les dépendances**.

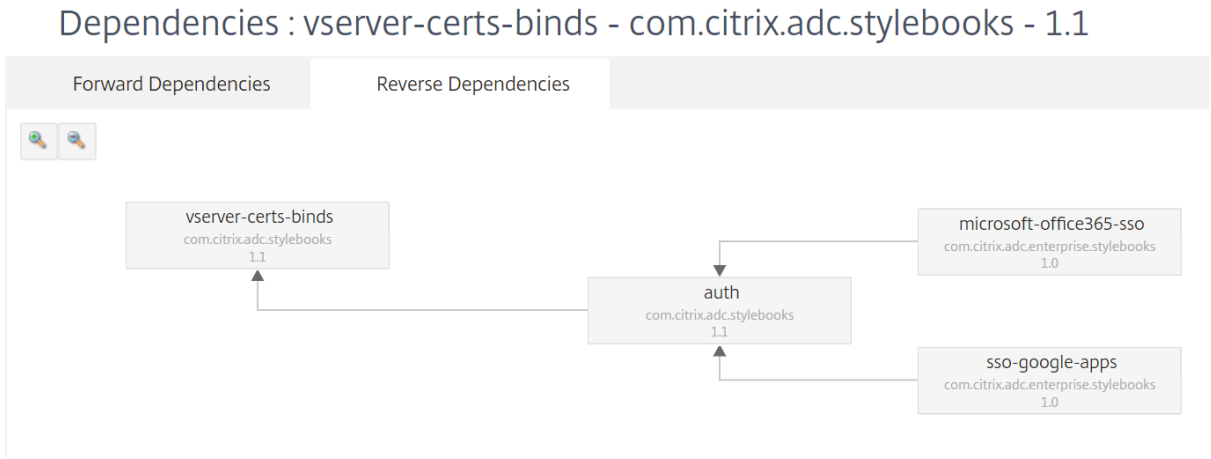
Dépendances de transfert

L' **onglet Dépendances** de transfert vous permet d'afficher 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 mis en surbrillance. Vous pouvez également cliquer sur les noms StyleBook pour afficher la définition de ce StyleBook.



Inverser les dépendances

L'onglet **Dépendances inversées** vous permet d'afficher graphiquement les StyleBooks qui utilisent votre StyleBook. Si vous suivez les flèches, vous pouvez voir que tous les StyleBooks dans l'affichage pointent vers votre StyleBook. Certains StyleBooks utilisent directement le StyleBook et certains StyleBook peuvent l'utiliser via un autre StyleBook.



Audit de la configuration ADC par rapport au pack de configuration

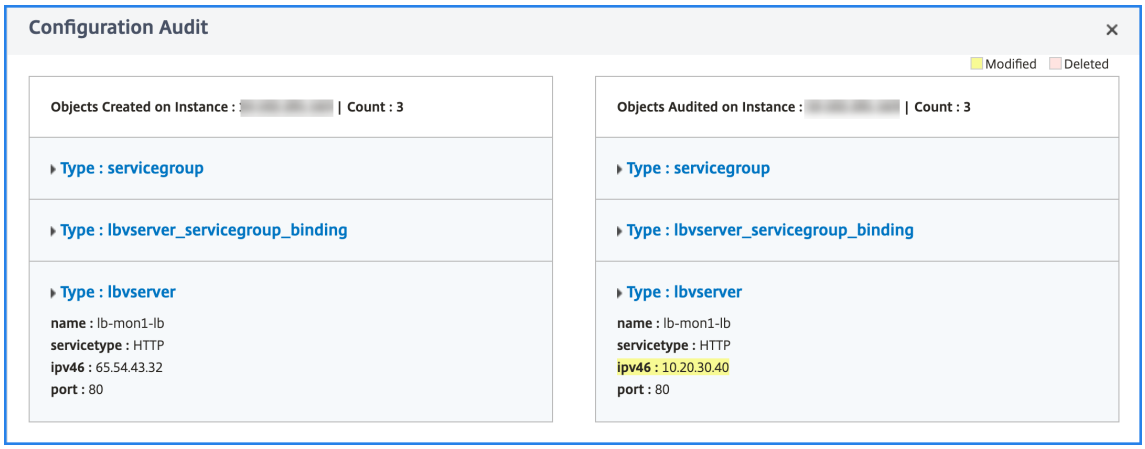
Vous pouvez comparer les modifications apportées par un pack de configuration StyleBook à la configuration ADC actuelle. Avec cette comparaison, vous pouvez effectuer les opérations suivantes :

- Détectez la dérive de configuration entre le pack de configuration StyleBook et la configuration ADC.
- Identifiez tous les objets modifiés et supprimés de ADC qui ne reflètent pas les modifications apportées par le pack de configuration.

Pour comparer les modifications du pack de configuration à la configuration des ADC, procédez comme suit.

1. Accédez à **Applications** > **StyleBooks** > **Configurations**.
2. Cliquez sur **Vérification de la configuration**.

   La page Audit de configuration affiche les objets créés et audités.

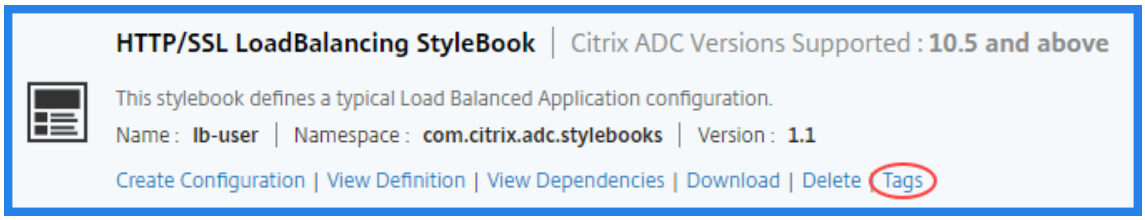


Créer une balise pour le StyleBook

Vous pouvez ajouter des balises à n'importe quel StyleBook dans Citrix ADM. Les balises sont des paires clé-valeur qui vous permettent de regrouper des StyleBooks à l'aide de critères différents. Vous pouvez utiliser ces balises lors de la recherche ou du filtrage de StyleBooks dans Citrix ADM.

Pour ajouter une balise au StyleBook :

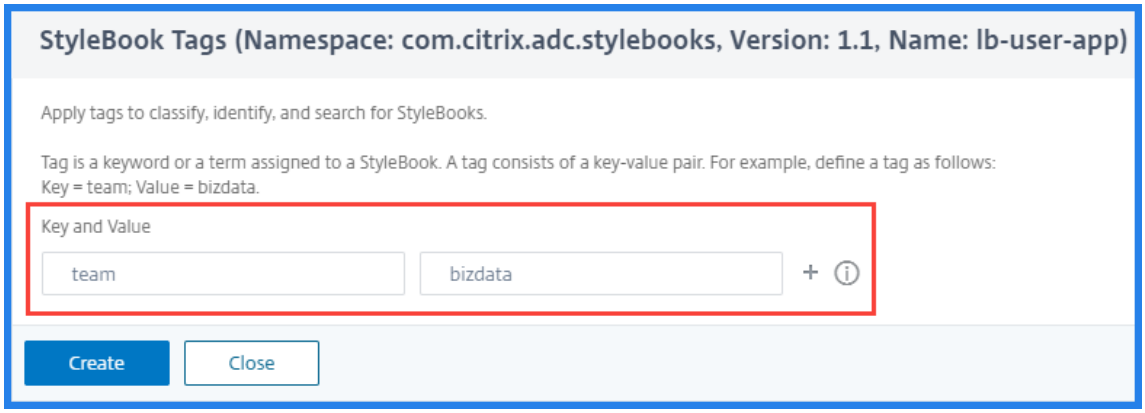
1. Accédez à **Applications** > **StyleBooks**.
2. Sélectionnez **Balises** dans le StyleBook pour lequel vous souhaitez ajouter des balises.



   Vous pouvez ajouter des balises à tous les types de StyleBooks.

3. Spécifiez les informations de **clé** et de **valeur** requises qui vous aident à filtrer le StyleBook.

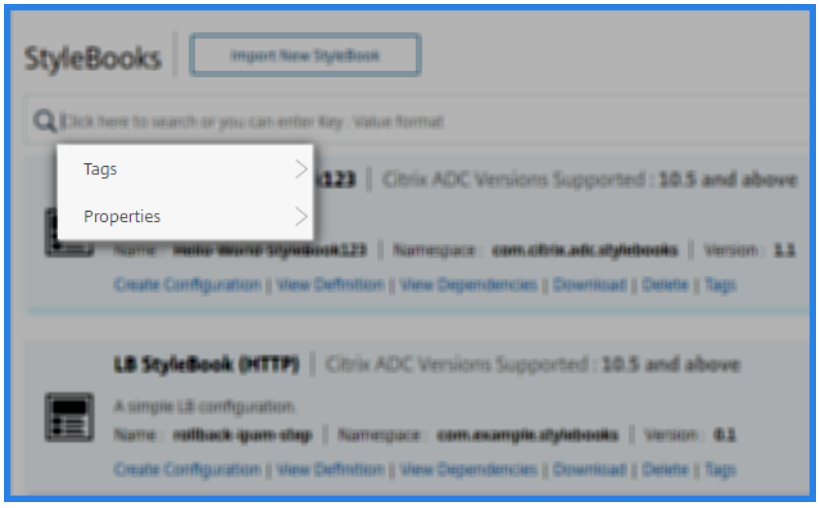
   Par exemple, key=Team et Value=BizData



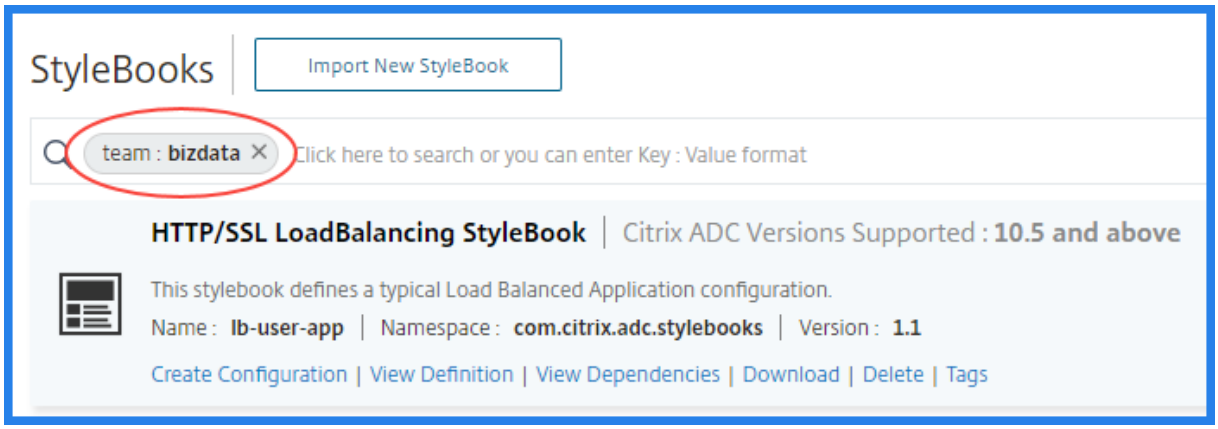
Pour ajouter d'autres balises, cliquez sur **+**.

4. Cliquez sur **Créer**.

Pour filtrer StyleBooks à l'aide de balises, dans la barre de recherche, cliquez sur **Balises** et sélectionnez clé et valeur dans la liste. Les StyleBooks correspondant à la balise spécifiée sont affichés.



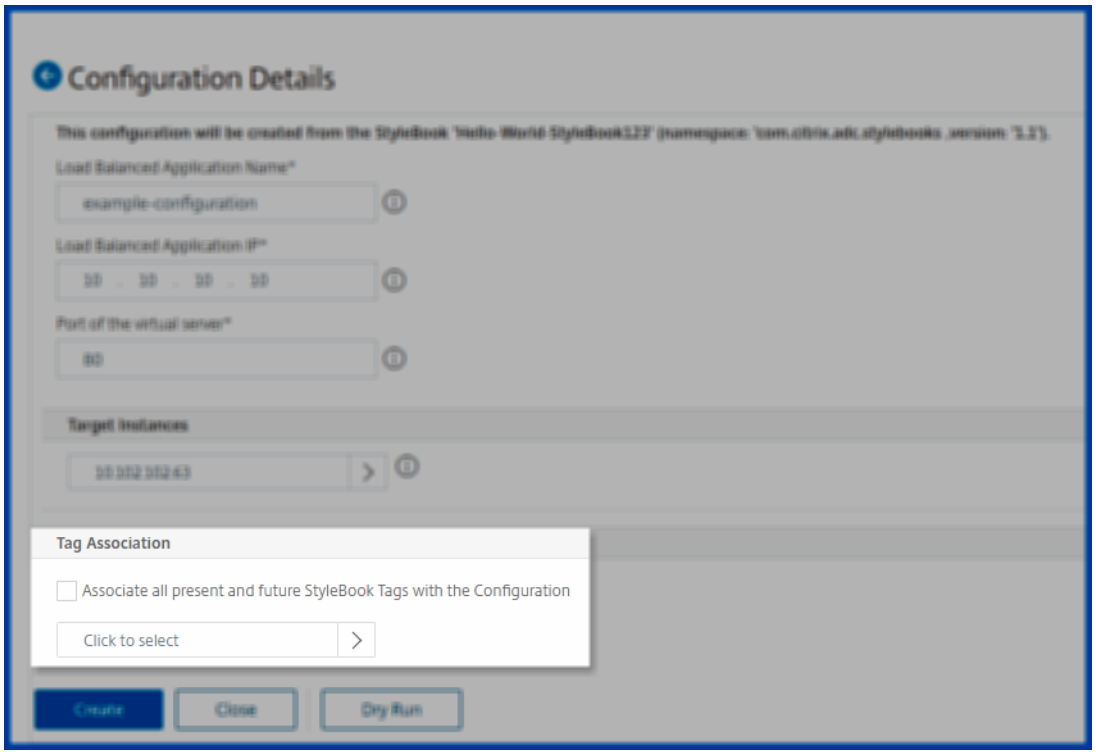
Voici un exemple de recherche pour les StyleBooks qui ont une balise où `key=team` et `value=bizdata` :



Vous pouvez associer les balises StyleBook à son pack de configuration. Ainsi, vous pouvez rechercher les packs de configuration à l'aide des balises StyleBook lui-même.

Lorsque vous créez un pack de configuration, utilisez l'une des options suivantes dans la section **Association de balises** :

- **Associer toutes les balises StyleBook présentes et futures à la configuration** : cette option associe toutes les balises StyleBook à un pack de configuration. Il veille également à associer les nouvelles balises que vous pourriez ajouter aux StyleBooks à l'avenir.
- **Sélectionner les balises** : cette option affiche les balises du StyleBook sélectionné. Vous pouvez sélectionner les balises StyleBook requises et les associer à un pack de configuration.



Importer et synchroniser les StyleBooks à partir du référentiel GitHub

April 29, 2021

Considérez un scénario où vous utilisez des processus CI/CD pour votre développement. Ou, un scénario dans lequel vous gérez tous le code source de l'application et les objets de déploiement dans GitHub.

Dans le référentiel GitHub, vous avez peut-être créé plusieurs StyleBooks pour déployer les configurations Citrix ADC et gérer ces StyleBooks. Ces StyleBooks sont également requis dans Citrix Applications and Delivery Management (ADM). Vous pouvez désormais importer directement ces StyleBooks

dans Citrix ADM. Vous n'avez pas besoin de les copier manuellement à partir de GitHub, puis de les télécharger dans Citrix ADM ou de synchroniser manuellement les fichiers dans ADM et GitHub.

Vous pouvez désormais définir un référentiel dans Citrix ADM qui représente un référentiel GitHub. Fournissez l'URL du référentiel GitHub et votre nom d'utilisateur ou jeton d'API créés dans GitHub. Cela signifie que seuls les utilisateurs autorisés disposant d'un compte valide dans GitHub peuvent importer et synchroniser les StyleBooks.

Après avoir créé le référentiel, vous pouvez synchroniser Citrix ADM avec votre référentiel GitHub. Citrix ADM se connecte à GitHub et importe les StyleBooks trouvés dans ce référentiel. ADM valide ensuite les StyleBooks et les ajoute à la liste des StyleBooks dans Citrix ADM. StyleBooks ne sont pas ajoutés à Citrix ADM s'ils échouent à la validation. Corrigez les erreurs et validez les versions mises à jour dans votre dépôt GitHub. Plus tard, vous pouvez essayer de les importer ou de les synchroniser à nouveau dans Citrix ADM.

> **Remarque**
>
> - Les fichiers StyleBooks peuvent être importés et synchronisés à partir de n'importe quelle branche d'un référentiel GitHub.
> - Vous pouvez importer et synchroniser les StyleBooks qui ont des StyleBooks dépendants qui leur sont également associés.
> - La synchronisation de StyleBooks à partir d'un référentiel GitHub doit être initiée manuellement à partir de l'interface graphique ou de l'API Citrix ADM. Autrement dit, actuellement, l'importation et la synchronisation de StyleBooks ne se produisent pas automatiquement en fonction de l'activité de validation de GitHub.

Ajouter un référentiel et importer StyleBooks à partir d'un référentiel GitHub

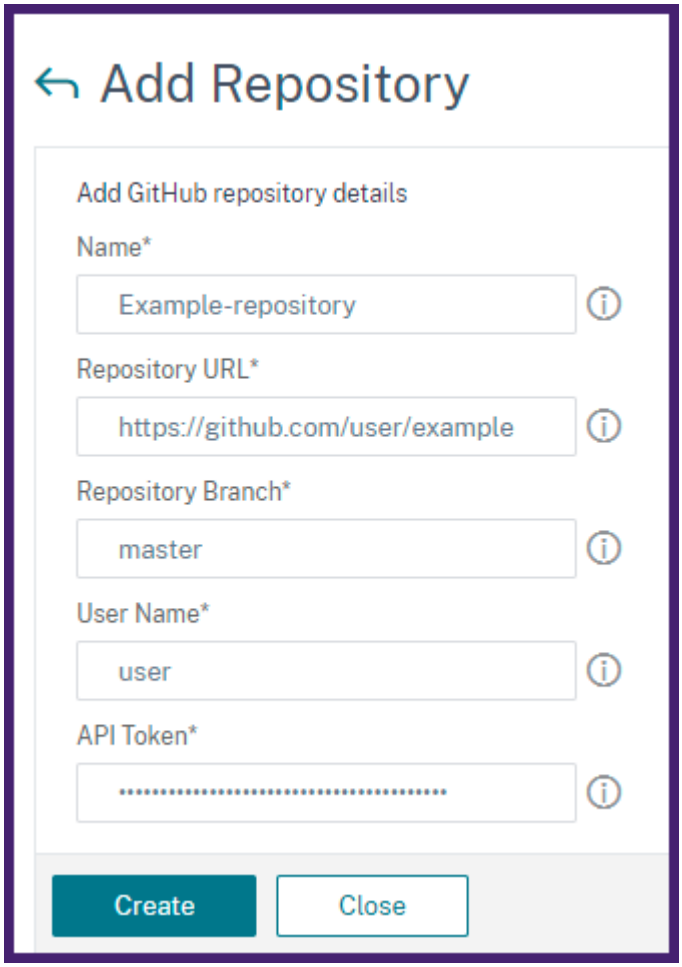
Avant de commencer, assurez-vous d'avoir un compte valide dans GitHub.

Vous pouvez importer des fichiers StyleBook vers ADM à partir de n'importe quel dossier du référentiel GitHub.

1. Dans Citrix ADM, accédez à **Applications** > **StyleBooks** > **Référentiels** .
2. Cliquez sur **Ajouter**. Dans la fenêtre **Ajouter un référentiel**, entrez les paramètres suivants :
    - **Nom** : saisissez le nom du référentiel. Ce nom peut être le même que le nom du référentiel dans GitHub ou un autre.
    - **URL du référentiel** - Saisissez l'URL du référentiel GitHub.
    - **Nom d'utilisateur** - Saisissez le nom d'utilisateur que vous utilisez pour accéder au compte GitHub.

- **API Token** - Ce jeton est utilisé pour accéder à votre référentiel GitHub. Pour plus d'informations sur la création de jetons API pour votre référentiel GitHub, consultez la documentation GitHub pour création de jetons d'accès personnels.

3. Cliquez sur **Créer**.



Le référentiel est créé dans Citrix ADM.

4. Pour importer ou synchroniser StyleBooks, sélectionnez le référentiel dans la page **Référentiels**, puis cliquez sur **Synchroniser** .

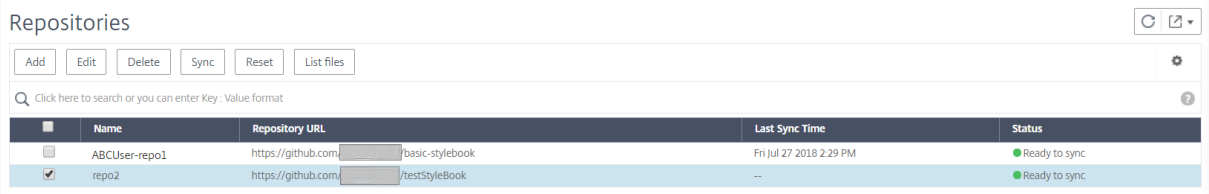
Les autres actions que vous pouvez utiliser ici sont :

- **Modifier**. Vous pouvez modifier l'URL du référentiel, le nom d'utilisateur et le jeton d'API.
- **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

> des ConfigPacks sont associés. Tout d'abord, supprimez tous les packs de configuration de ces StyleBooks. Vous pouvez ultérieurement supprimer le référentiel de Citrix ADM pour nettoyer les StyleBooks de ce référentiel.

- **Réinitialiser**. Vous pouvez supprimer tous les StyleBooks dans Citrix ADM synchronisés à partir de ce référentiel sans réellement supprimer l'entrée de référentiel de Citrix ADM.
- **Liste des fichiers**. Vous pouvez voir une liste de tous les StyleBooks présents dans Citrix ADM provenant du référentiel GitHub.



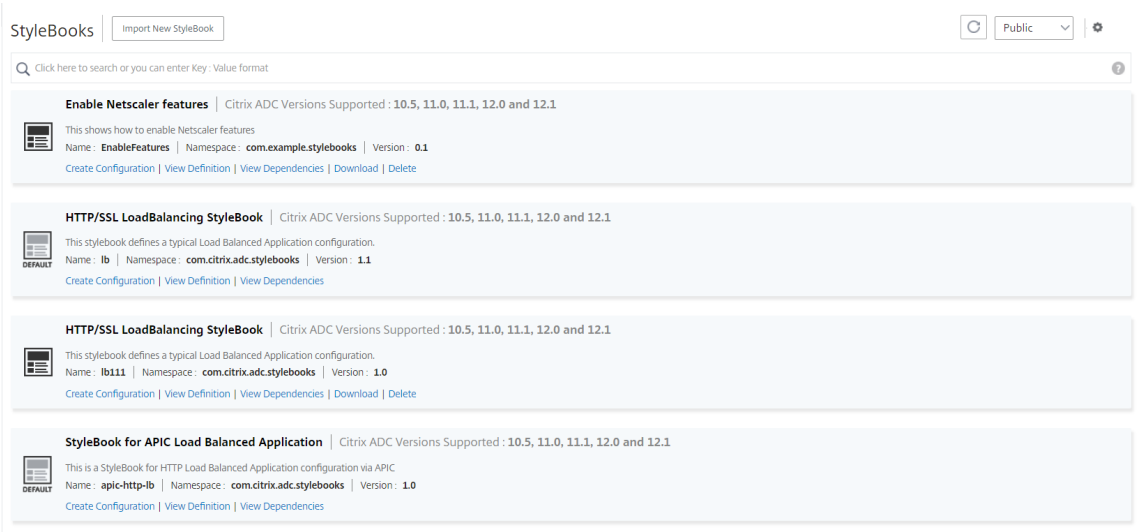
Utiliser StyleBooks par défaut

April 29, 2021

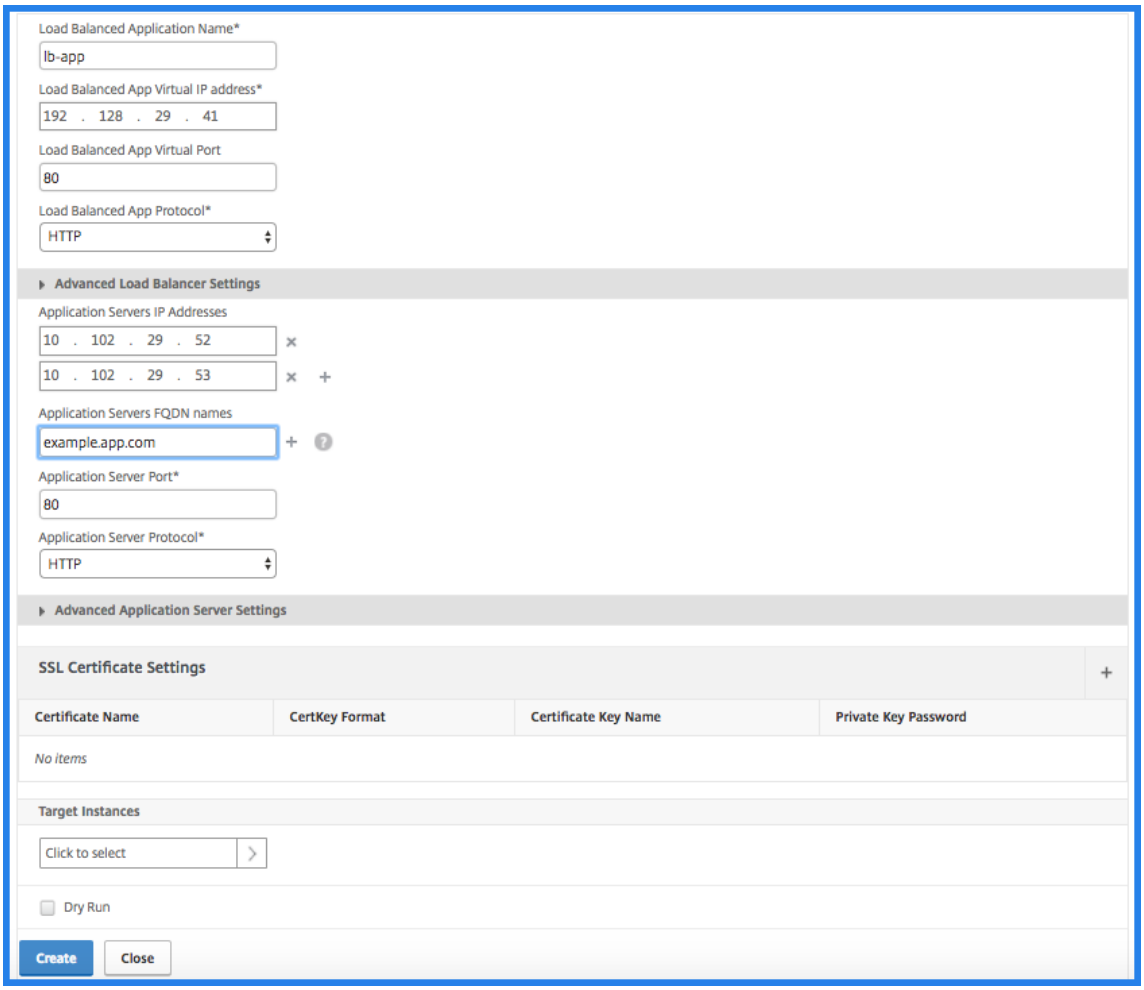
Un ensemble de StyleBooks par défaut est fourni avec Citrix Application Delivery Management (ADM). Lorsque vous utilisez un StyleBook par défaut, vous devez spécifier des valeurs pour les paramètres dans le StyleBook et sélectionner les adresses IP des instances Citrix ADC dans lesquelles vous souhaitez exécuter la configuration. Après avoir soumis la configuration, Citrix ADM valide les valeurs de paramètre que vous avez spécifiées, crée un graphique 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 dans Citrix ADM. Cette liste inclut à la fois les StyleBooks par défaut et personnalisés. Vous pouvez taper le nom du StyleBook dans le champ de recherche et appuyer sur la touche **Entrée** . Sinon, vous pouvez faire défiler la liste vers le bas pour trouver le StyleBook.

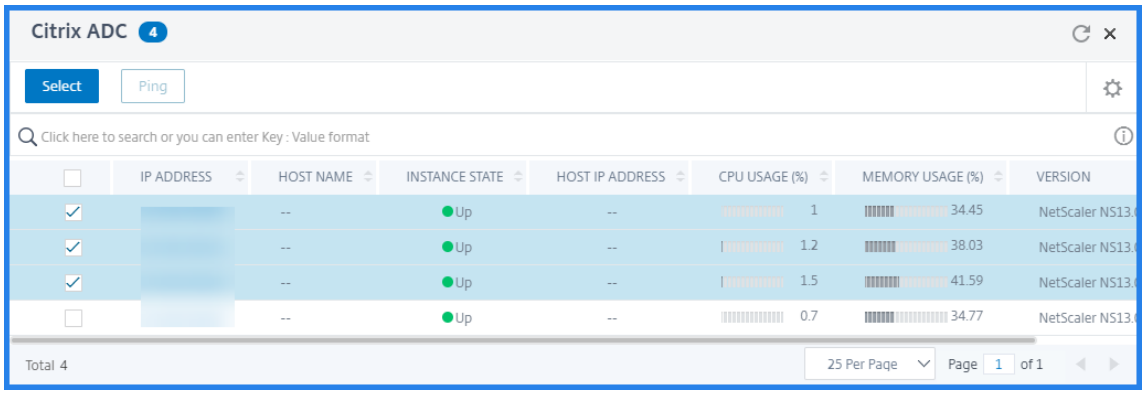


2. Cliquez sur **Créer une configuration**. Spécifiez les valeurs requises pour les paramètres.



3. Sous **Instances cibles**, sélectionnez l'adresse IP de l'instance Citrix ADC dans laquelle vous souhaitez exécuter la configuration. Vous pouvez sélectionner plusieurs instances pour exé-

cuter cette configuration.

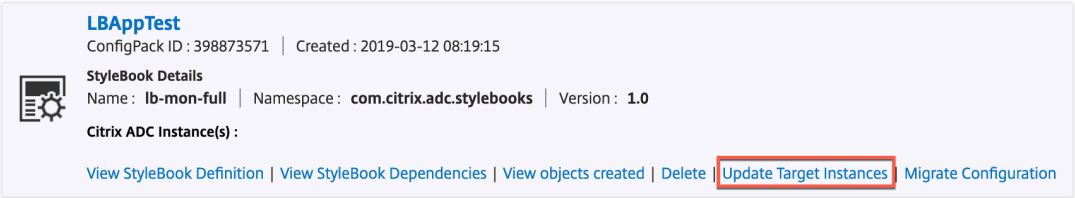


Remarque

Vous pouvez également créer un pack de configuration sans sélectionner les instances. Vous pouvez ensuite mettre à jour le pack de configuration en sélectionnant les instances cibles sur lesquelles vous souhaitez déployer la configuration. De même, vous pouvez supprimer toutes les instances cibles d'un pack de configuration sans supprimer le pack de configuration lui-même.

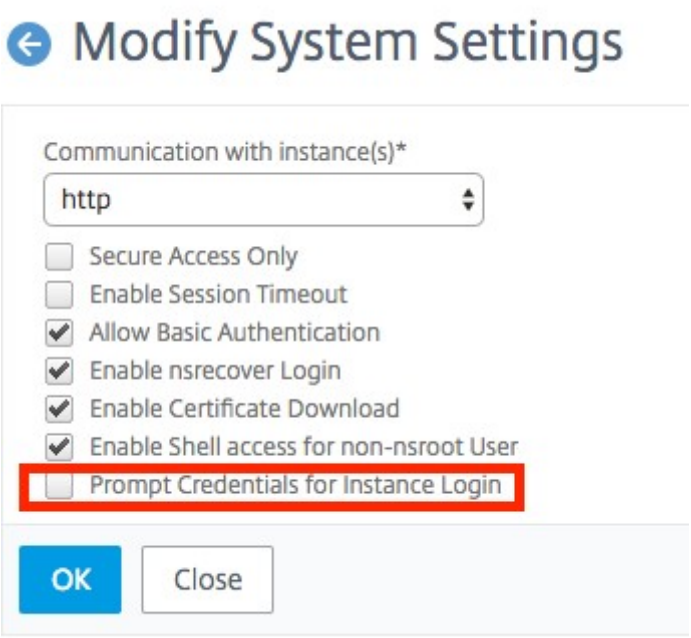
Cas d'utilisation : vous pouvez créer des packs de configuration pour vos applications, même si vous n'êtes pas en mesure d'accéder aux instances.

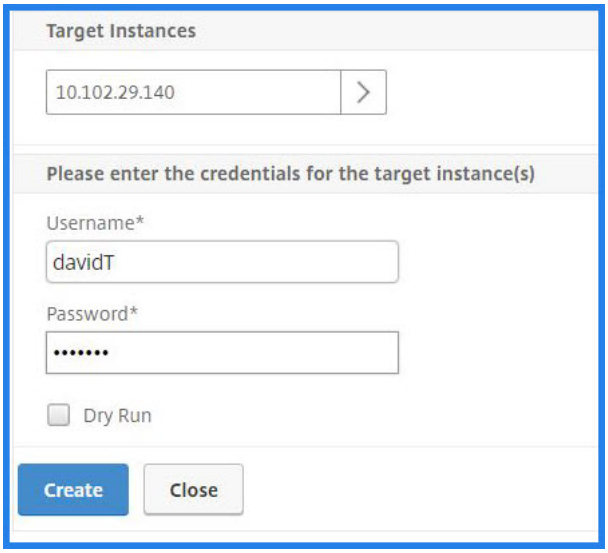
L'image suivante affiche un tel pack de configuration créé sans sélectionner une instance particulière. Cliquez sur **Mettre à jour les instances cibles**, puis sélectionnez les instances cibles pour déployer cette configuration.



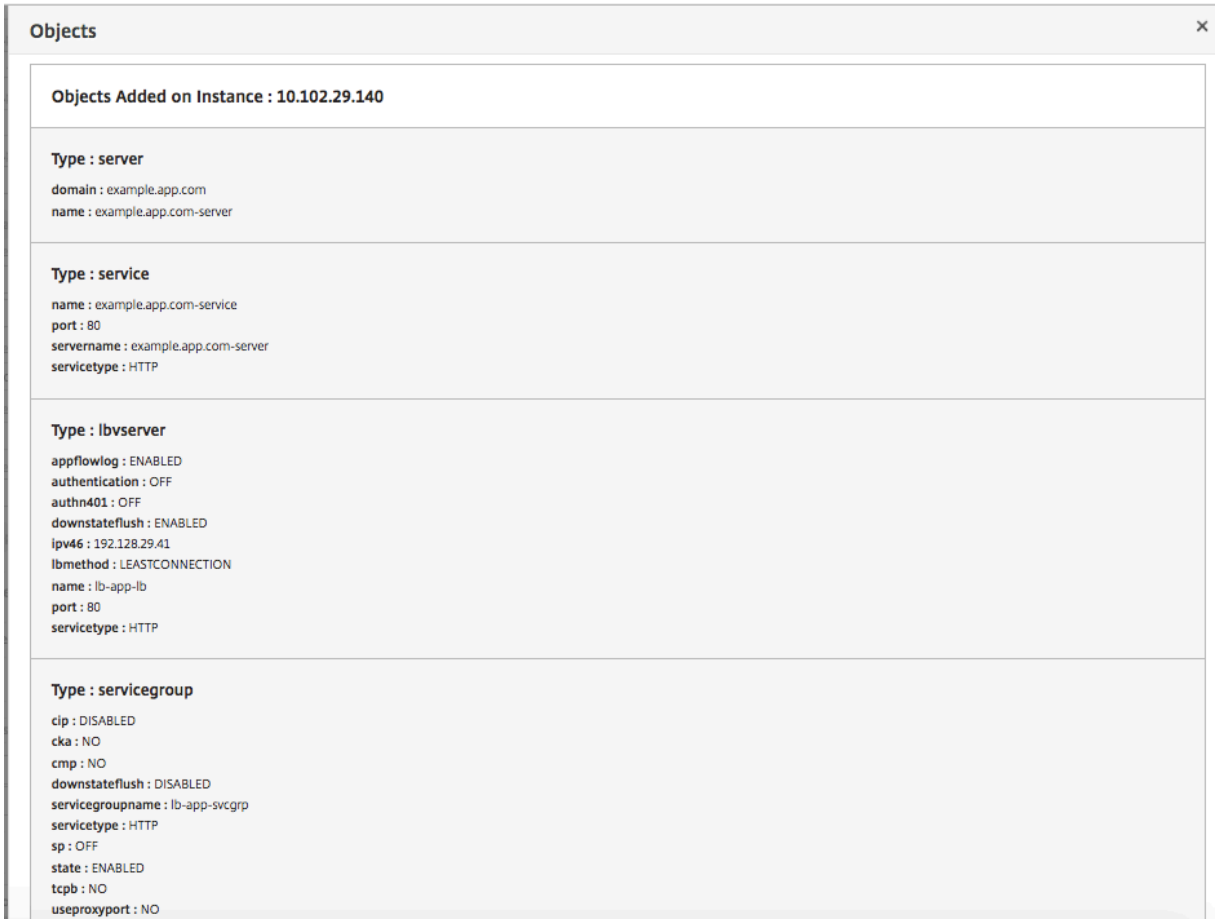
Si l'option **Inviter les informations d'identification pour la connexion d'instance** est activée dans **Citrix ADM** > **Système** > **Modifier les paramètres système> Modifier les paramètres système**, vous êtes invité à entrer vos informations d'identification de l'instance Citrix ADC lorsque vous exécutez les configurations sur le 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.

Cas d'utilisation : vous pouvez créer des packs de configuration pour vos applications, même si vous n'êtes pas en mesure d'accéder aux instances.





Si vous souhaitez tester ou valider votre configuration avant de l'exécuter sur l'instance Citrix ADC, sélectionnez **Exécuter 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.



1. Désactivez la case à **cocher Exécuter à sec** et cliquez sur **Créer** pour créer le pack de configuration et exécuter la configuration sur l'instance Citrix ADC. La configuration de StyleBook (pack de configuration) que vous avez créée apparaît dans la liste des configurations, comme illustré 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 maintenant examiner, mettre à jour ou supprimer cette configuration (pack de configuration) à l'aide de Citrix ADM.

Masquer tous les StyleBooks par défaut

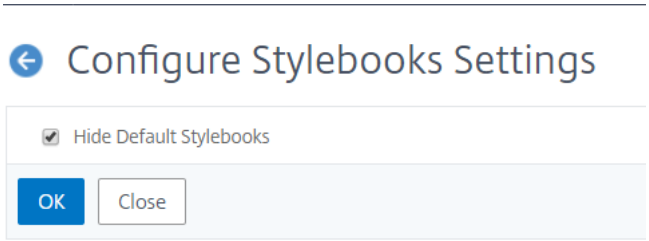
April 29, 2021

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 pouvez masquer tous les StyleBooks par défaut. Vous pouvez autoriser vos utilisateurs à afficher 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 est fournie où vous pouvez 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 ou non par les utilisateurs.
3. Pour masquer les StyleBooks par défaut, cliquez sur l'icône Modifier en haut à droite.
4. Dans la page **Configurer les paramètres de StyleBook**, sélectionnez **Masquer l'option StyleBooks par défaut** .
5. Cliquez sur **OK**.



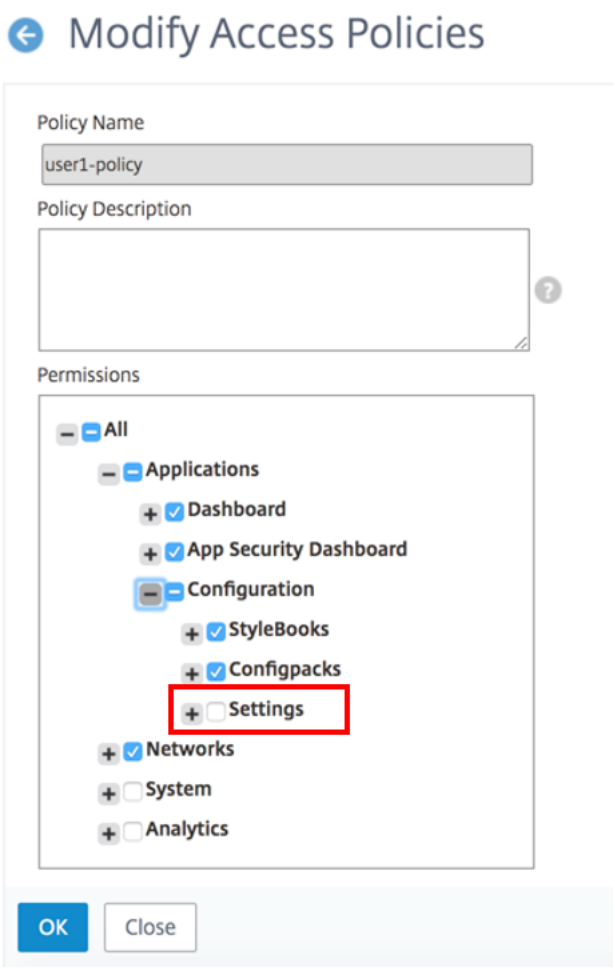
La page **Configurer les paramètres du StyleBook** est toujours visible pour les utilisateurs si vous n'avez pas choisi de masquer la page à l'aide de la fonctionnalité RBAC. Il se peut que les utilisateurs aient toujours la possibilité d'afficher les StyleBooks par défaut.

Pour masquer la page **Configurer les paramètres de StyleBook**, vous devez créer une stratégie et affecter cette stratégie aux utilisateurs qui ne doivent pas voir les livres StyleBooks par défaut.

Pour créer une stratégie RBAC :

1. Dans Citrix ADM, accédez à **Compte** > **Administration des utilisateurs** > **Stratégies d'accès** .
2. Cliquez sur **Ajouter** pour créer une stratégie.

3. Entrez le nom de la stratégie.
4. Dans la section **Autorisations**, assurez-vous que sous **Tous** > **Applications** > **Configuration** > **Paramètres** n'est pas sélectionné, 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 aux utilisateurs, reportez-vous à la sectionConfiguration du contrôle d'accès basé sur les rôles.

Migrer la configuration de l'application Citrix ADC à l'aide de StyleBooks Configuration Builder

April 29, 2021

StyleBooks Configuration Builder permet de migrer une configuration ADC existante vers StyleBooks.

Cette fonctionnalité automatise également la migration de la configuration de l'application d'une instance Citrix ADC vers une autre instance ou un groupe de mise à Autoscale.

Le Générateur de configuration fournit une application structurée StyleBook qui peut être utilisée pour toutes les variantes de la configuration ADC. Cette fonctionnalité vous aide à commencer avec StyleBooks sans connaissance approfondie de la grammaire et des constructions StyleBooks. Sinon, la connaissance de la grammaire et des constructions de StyleBooks est nécessaire pour créer un StyleBook.

Le Générateur de configuration crée également un pack de configuration qui reflète la même configuration ADC sur une nouvelle instance ADC. Avec ce pack de configuration, la configuration ADC initiale d'une instance ADC peut être dupliquée vers une autre instance ADC. La source de configuration initiale peut être l'une des suivantes :

- **Une instance Citrix ADC :** spécifiez l'instance dans laquelle la configuration de l'application que vous souhaitez dupliquer est hébergée.

  Le Générateur de configuration convertit la configuration ADC en StyleBook et en pack de configuration même si vous ne spécifiez pas l'instance cible. Vous pouvez ultérieurement utiliser ce pack de configuration pour migrer la configuration ADC vers d'autres instances ADC.

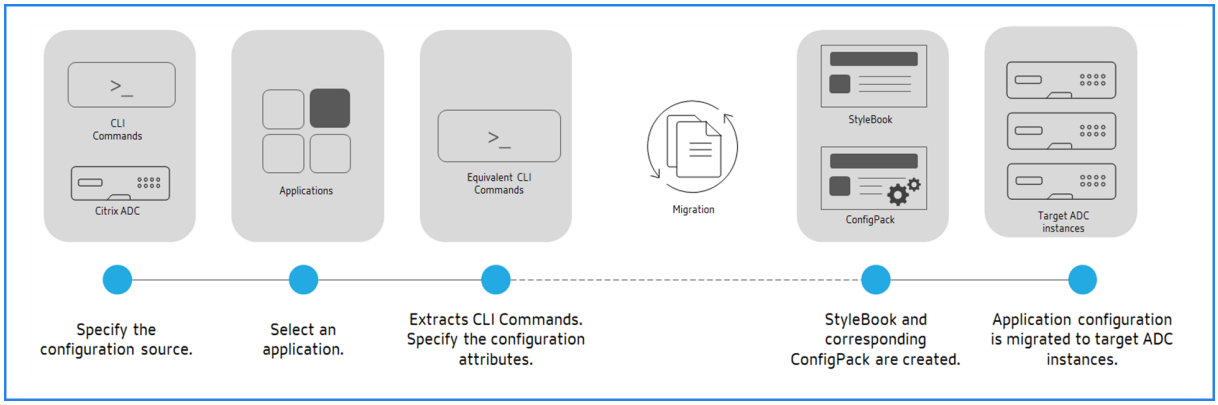
  Si l'instance cible est un groupe Mise à Autoscale, le pack de configuration apparaît dans la page **Réseau > Groupe de mise à l'échelle automatique**. Sous l'onglet **Configuration**.

- **Un ensemble de commandes CLI :** Collez la configuration à partir de `ns.conf` ou `Application config`.

Le Générateur de configuration identifie la liste des applications distinctes incorporées dans la configuration source. Lorsque vous sélectionnez la configuration de l'application qui vous intéresse, Configuration Builder extrait l'ensemble des commandes CLI de l'application sélectionnée. Ces commandes CLI sont extraites de la configuration source. Il identifie également les attributs de déploiement et de configuration qui peuvent nécessiter votre entrée.

- **Adresse IP/Ports** - Vous pouvez afficher et modifier l'adresse IP et le port des serveurs virtuels, des services, des membres du groupe de services à partir de la configuration d'origine.
- **Fichiers/Secrets de configuration** - Ces attributs peuvent être des mots de passe ou des certificats spécifiés dans la configuration source.

Après avoir spécifié les informations nécessaires, commencez à migrer ou à dupliquer la configuration de l'application sur une instance ADC cible.



Après la création et la migration de l'application, un pack de configuration est créé dans Citrix ADM à l'aide de `adc_nitro_application` StyleBook. Ce StyleBook est créé à partir des ressources ADC NITRO. Ce pack de configuration représente la configuration de l'application sur l'instance ADC cible. Pour afficher le pack de configuration créé, accédez à **Applications** > **StyleBooks** > **Configurations**.

Fonctionnalités de Citrix ADC prises en charge

StyleBook Configuration Builder reconnaît et prend en charge les fonctionnalités Citrix ADC suivantes dans la configuration source :

- Commutation de contenu
- Équilibrage de charge
- Surveillance
- Déchargement SSL
- Limitation du taux
- Réécrire
- Répondeur
- Pare-feu d'application Web (WAF)

Créer un StyleBook pour migrer la configuration de l'application Citrix ADC

La procédure suivante consiste à créer un StyleBook qui migre la migration d'application Citrix ADC dans Citrix ADM :

1. Accédez à **Applications** > **StyleBooks** > **Configurations**.
2. Cliquez sur **Migrer la configuration ADC**.
3. Cliquez sur **Démarrer**.
4. Dans **Spécifier la configuration**, sélectionnez la source de configuration :
    - **Importer à partir d'un ADC** : cette option détecte les applications actives sur l'instance ADC sélectionnée.

- **Importer à l'aide des commandes**CLI : cette option analyse les commandes CLI et extrait les applications des commandes CLI.

5. Spécifiez l'**instance ADC source** à partir de laquelle vous souhaitez migrer ou dupliquer la configuration de l'application.

   Pour migrer la configuration de l'application vers un groupe Mise à l'Autoscale, assurez-vous que les informations suivantes ne sont pas incluses dans la configuration source :

   - `IPset`
   - Profil de l'appareil
   - Protocole
   - Port

6. Spécifiez l'**instance ADC cible** vers laquelle vous souhaitez migrer ou dupliquer la configuration de l'application.

   Pour migrer une configuration d'application vers un groupe Mise à Autoscale, sélectionnez le groupe Mise à l'Autoscale dans la liste.

7. Dans **Définir une application**,

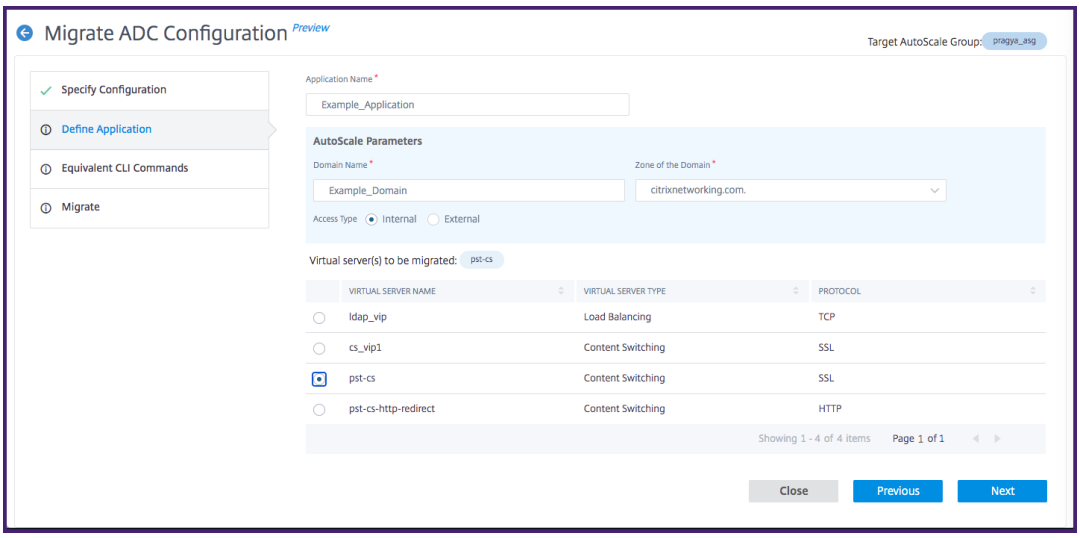
   a) Dans **Nom de l'application**, spécifiez le nom de l'application.

      Si l'instance cible est un groupe Mise à Autoscale, spécifiez les paramètres de mise à l'Autoscale suivants :

      - **Type d'accès** : vous pouvez utiliser la solution de mise à l'échelle automatique ADM pour des applications externes et internes. Sélectionnez le type d'accès à l'application requis.
      - **Nom de domaine** - Spécifiez le nom de domaine d'une application. Cette option n'est applicable que lorsque vous sélectionnez Type de nom de domaine complet défini par l'utilisateur.
      - **Zone du domaine** : sélectionnez le nom de zone d'une application dans la liste. Cette option n'est applicable que lorsque vous sélectionnez Type de nom de domaine complet défini par l'utilisateur.

        Ce nom de domaine et de zone redirige vers les serveurs virtuels dans Azure. Par exemple, si vous hébergez une application dans `app.example.com`, le `app` est le nom de domaine et `example.com` le nom de la zone.

   b) Sélectionnez les serveurs virtuels à migrer.



c) Cliquez sur **Suivant**.

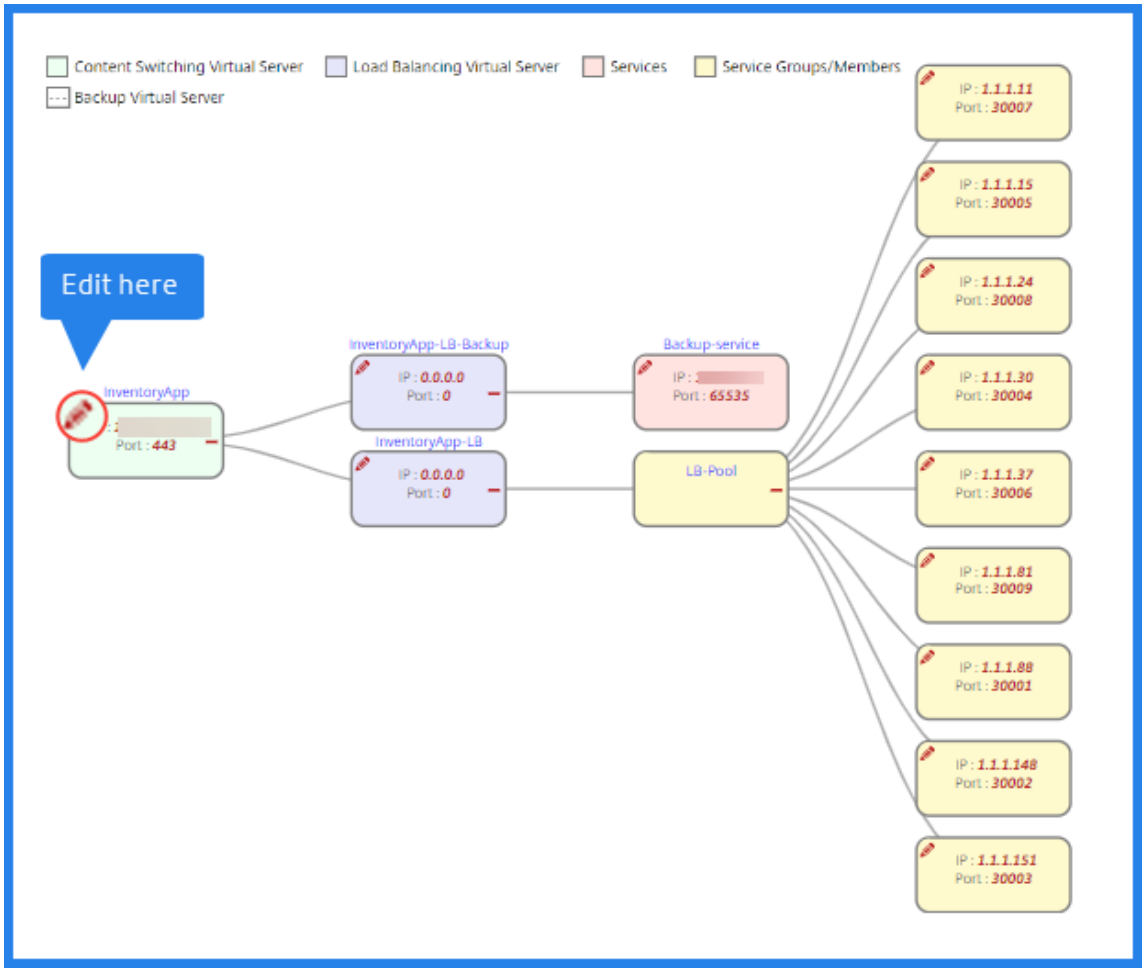
8. Dans **Commandes CLI équivalentes**, passez en revue les commandes et cliquez sur **Suivant**.

   Ces commandes sont spécifiques à la configuration de l'application sélectionnée.

   > **Remarque**
   >
   > Vous pouvez également ajouter ou modifier la configuration si nécessaire.

9. Dans **Attributs de déploiement**, vous pouvez afficher et modifier l'adresse IP et le port des serveurs virtuels, des services et des membres du groupe de services.

   Pour modifier l'adresse IP et le port, cliquez sur l'icône de modification sur le serveur virtuel, le service ou le membre du groupe de services dans le diagramme de flux.



> **Remarque**
>
> Si l'instance cible est un groupe Autoscale, la modification de l'adresse IP frontale est désactivée.

Cet onglet n'apparaît que dans les cas suivants :

- Les instances source et cible sont différentes.
- Importez des configurations à l'aide des commandes CLI.

10. Dans **Attributs de configuration**, spécifiez les détails nécessaires et cliquez sur **Suivant**.

    Cet onglet répertorie les secrets tels que les clés pour déchiffrer les mots de passe et les certificats.

    > **Remarque**
    >
    > Avant de commencer la migration, les configurations manquées ou non prises en charge sont affichées dans l'un des onglets suivants :
    >
    > - **Configurations non prises en charge**

> - **Configurations globales non prises en charge**
>
> Pour migrer ces configurations avec succès, vous devez appliquer séparément les configurations manquées ou non prises en charge sur l'instance cible. Et, cliquez sur **Suivant**.

11. Dans **Migrer**, cliquez sur **Migrer**.

Limitations

- Les expressions nommées et `responderhtmlpages` mentionnées dans l'instance source ne sont pas identifiées. Assurez-vous de configurer les expressions nommées et `responderhtmlpages` sur l'instance cible avant la migration.
- Si la source a une configuration pour `servicegroup` et surveille la liaison comme suit :

  ```
  bind serviceGroup <Name> <Port> -monitorName <Monitor_Name>
  ```

  L'erreur suivante apparaît :

  ```
  1  CLI Command conversion failed: 100 - No such command [{
  2   "errorcode": 1090, "message": "No such argument [XXX]", "
         severity": "ERROR"  }
  3  ]
  4  <!--NeedCopy-->
  ```

  Cette erreur se produit car Citrix ADC enregistre la liaison entre le groupe de services et le moniteur dans un format non valide. Ce problème est résolu à partir de Citrix ADC 12.1.52.15 build.

SSO Google Apps StyleBook

April 29, 2021

Google Apps est une collection d'outils de cloud computing, de productivité et de collaboration, de logiciels et de produits 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 une seule fois pour tous les services à l'aide de leurs informations d'identification d'entreprise.

L'OSO Citrix Application Delivery Management (ADM) Google Apps StyleBook vous permet d'activer l'OSO pour Google Apps via des instances Citrix ADC. StyleBook configure l'instance de Citrix ADC en tant que fournisseur d'identité SAML pour authentifier les utilisateurs pour accéder à Google Apps.

L'activation de l'SSO pour les applications Google dans une instance de Citrix ADC à l'aide de ce StyleBook entraîne 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. Liaison du serveur d'authentification LDAP et de la stratégie à votre serveur virtuel d'authentification configuré sur l'instance

Détails de configuration :

Le tableau suivant répertorie les versions logicielles minimales requises pour que cette intégration fonctionne correctement. Le processus d'intégration prend également en charge les versions supérieures de la même.

Produit	Version minimale requise
Citrix ADC	Version 11.0, licence avancée/Premium

Les instructions suivantes supposent que vous avez déjà créé les entrées DNS externes et 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 Microsoft SSO Google Apps StyleBook dans votre réseau d'entreprise.

Pour déployer SSO Google apps StyleBook

1. Dans Citrix ADM, accédez à **Applications** > **Configurations** > **StyleBooks** . La page StyleBooks affiche tous les StyleBooks disponibles pour votre utilisation dans Citrix ADM. Faites défiler vers le bas et recherchez **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 d'applications Google SSO à déployer sur votre réseau.
    b) **Authentification Adresse IP virtuelle**. Adresse IP virtuelle utilisée par le serveur virtuel Citrix ADC AAA auquel la stratégie d'IdP SAML des applications Google est liée.
    c) **Expression de règle SAML**. Par défaut, l'expression Citrix ADC Policy (PI) suivante est utilisée : HTTP.REQ.HEADER (« Referrer ») .CONTAINS (« google »). Mettez à jour ce champ

avec une autre expression si votre besoin est différent. Cette expression de stratégie correspond au trafic auquel ces paramètres SSO SAML sont appliqués et s'assure que l'en-tête Referrer provient d'un domaine Google.

4. La section Paramètres d'IdP SAML vous permet de configurer votre instance Citrix ADC en tant que fournisseur d'identité SAML en créant le profil et la stratégie d'IdP SAML utilisés par le serveur virtuel Citrix ADC 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_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 correspondant à cet ID.

   c) **URL du service aux consommateurs d'assertion**. Entrez l'URL du fournisseur de services où le fournisseur d'identité Citrix ADC doit envoyer les assertions SAML après l'authentification utilisateur réussie. L'URL du service consommateur d'assertion peut être initiée sur le site du serveur du fournisseur d'identité ou sur le site du fournisseur de services.

   d) Il existe d'autres champs facultatifs que vous pouvez saisir dans cette section. Par exemple, vous pouvez définir les options suivantes :

      i. Profil de liaison SAML (la valeur 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 (par défaut est AES256), et d'autres paramètres.

      > **Remarque**
      >
      > Citrix vous recommande de conserver les paramètres par défaut car ces paramètres ont été testés pour prendre en charge 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 PI Citrix ADC 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 de domaine puissent se connecter à l'instance de Citrix ADC à l'aide de leurs adresses de messagerie d'entreprise, vous devez configurer les éléments suivants :

   a) **Base LDAP (Active Directory)**. Entrez le nom de domaine de base pour le domaine dans lequel les comptes d'utilisateur résident dans Active Directory (AD) pour lequel vous souhaitez autoriser l'authentification. Par exemple, `dc=netscaler,dc=com`

   b) **LDAP (Active Directory) Bind DN**. Ajoutez un compte de domaine (à l'aide d'une adresse e-mail pour faciliter la configuration) qui dispose des droits de parcourir l'arborescence AD. Par exemple, `cn=Manager,dc=netscaler,dc=com`

   c) **Mot de passe du nom unique de liaison LDAP (Active Directory)**. Entrez le mot de passe du compte de domaine pour l'authentification.

   d) Voici quelques autres champs que vous devez saisir dans cette section :

      i. Adresse IP du serveur LDAP à laquelle Citrix ADC se connecte pour authentifier les utilisateurs

      ii. Nom de domaine complet du serveur LDAP

      > **Remarque**
      >
      > Vous devez spécifier au moins l'un des deux 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 IdP SAML, 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 à partir du 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 `.pem` et `.der` extensions.

d) **Nom de la clé de certificat**. Entrez le nom de la clé privée du certificat.

e) **Fichier de clé de certificat**. Sélectionnez le fichier contenant la clé privée du certificat à partir de votre système local ou de Citrix ADM.

f) **Mot de passe de clé privée**. Si votre fichier de clé privée est protégé par une phrase secrète, saisissez-le dans ce champ.

g) Vous pouvez également activer la case à cocher Paramètres avancés de certificat pour entrer des détails tels que la période de notification d'expiration du certificat, activer ou désactiver le moniteur d'expiration du certificat.

7. Le cas échéant, vous pouvez sélectionner Certificat IdP SSL CA si le certificat IdP SAML entré ci-dessus nécessite l'installation d'un certificat public CA sur Citrix ADC. Assurez-vous de sélectionner « Est un certificat d'autorité de certification » dans les paramètres avancés.

8. Le cas échéant, vous pouvez sélectionner Certificat SSL SP SAML pour spécifier le certificat SSL Google (clé publique) utilisé pour valider les demandes d'authentification de Google Apps (SAML SP).

9. Cliquez sur **Instances cibles** et sélectionnez l'instance (s) Citrix ADC sur laquelle déployer cette configuration d'authentification SSO Google Apps. Cliquez sur **Créer** pour créer la configuration et déployer la configuration sur les instances Citrix ADC sélectionnées.

> **Remarque**
>
> Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter des instances Citrix ADC récemment découvertes dans Citrix ADM à la liste des instances disponibles dans cette fenêtre.

Également,

> **Conseil**

```
> Citrix recommande qu'avant d'exécuter la configuration réelle, vous s
  électionnez **Exécuter à sec** pour confirmer visuellement les
  objets de configuration créés sur les instances Citrix ADC cibles
  par le StyleBook.
```

SSO Office 365 StyleBook

April 29, 2021

Microsoft™ Office 365 est une suite d'applications de productivité et de collaboration basées sur le cloud fournies par Microsoft sur la base d'un abonnement. Il inclut les applications serveur populaires de Microsoft telles que 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 se connectant à la console d'administration
- Ouverture de session unique pour tous les services Microsoft Office 365 à l'aide de leurs informations d'identification d'entreprise.

L'authentification SSO Office 365 StyleBook vous permet d'activer l'authentification SSO pour Microsoft Office 365 via des instances de 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 SSO pour Microsoft Office 365 dans une instance de 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. Liaison du serveur d'authentification LDAP et de la stratégie 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 prend également en charge les versions supérieures de la même.

Produit	Version minimale requise
Citrix ADC	11.0, Licence avancée/Premium

Les instructions suivantes supposent que vous avez déjà créé les entrées DNS externes et internes appropriées. Ces entrées sont essentielles pour acheminer les demandes d'authentification vers une adresse IP surveillée par Citrix ADC.

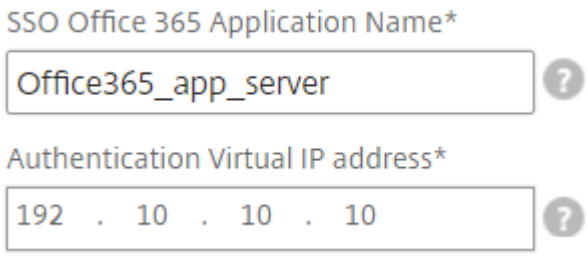
Les instructions suivantes vous aident à implémenter l'authentification SSO Office 365 StyleBook dans votre réseau d'entreprise.

Pour déployer l'authentification 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 vers le bas et recherchez l' **authentification SSO Office 365 StyleBook**. Cliquez sur **Créer une configuration**.

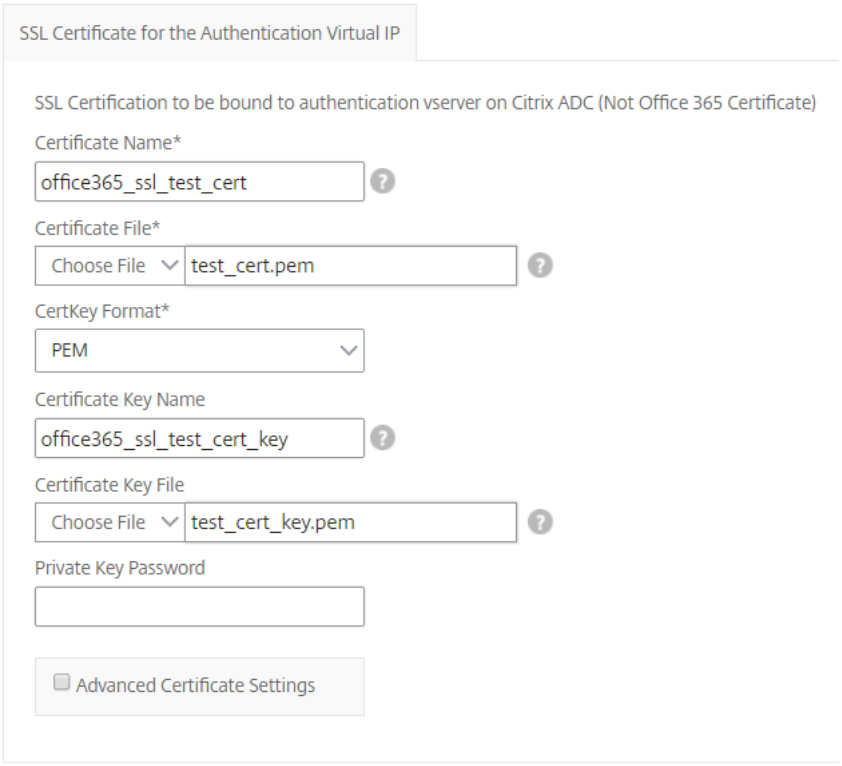
2. Le StyleBook s'ouvre sous la forme d'une page d'interface utilisateur sur laquelle vous pouvez entrer les valeurs de tous les paramètres définis dans ce StyleBook.
3. Entrez des valeurs pour les paramètres suivants :
   a) **Nom de l'application**. Nom de la configuration SSO Microsoft Office 365 à déployer dans votre réseau.
   b) **Authentification Adresse IP virtuelle**. Adresse IP virtuelle à utiliser par le serveur virtuel Citrix ADC AAA auquel la stratégie d'IdP SAML Microsoft Office 365 est liée.



4. Dans la section **Paramètres** des **certificats SSL**, entrez les noms du certificat SSL et de 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 de Citrix ADC.

5. Sélectionnez les fichiers respectifs dans votre dossier de stockage local. Vous pouvez également saisir le mot de passe de clé privée pour charger les clés privées chiffrées au format PEM.



6. Vous pouvez également activer la case à cocher **Paramètres de certificat avancés**. Ici, vous pouvez entrer des détails tels que la période de notification d'expiration du certificat, activer ou désactiver le moniteur d'expiration du certificat.
7. Le cas échéant, vous pouvez cocher **Certificat d'autorité de certification SSL pour l'authentification IP virtuelle** case à cocher si le certificat SSL nécessite l'installation d'un certificat public d'autorité de certification sur Citrix ADC. Assurez-vous de choisir « Est un certificat d'autorité de certification » dans la section **Paramètres de certificat avancés** ci-dessus.
8. Dans la section **Paramètres LDAP pour Office 365**, entrez les détails suivants pour authentifier les utilisateurs Office 365. Pour autoriser les utilisateurs de domaine à se connecter à l'instance de Citrix ADC à l'aide de leurs adresses de messagerie d'entreprise, configurez les éléments suivants :
    a) **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`
    b) **LDAP (Active Directory) Bind DN**. Ajoutez un compte de domaine (à l'aide d'une adresse e-mail pour faciliter la configuration) qui dispose des droits de parcourir l'arborescence AD. Par exemple, `cn=Manager,dc=netscaler,dc=com`
    c) **Mot de passe du nom unique de liaison LDAP (Active Directory)**. Entrez le mot de passe

du compte de domaine pour l'authentification.

d) Voici quelques autres champs que vous devez saisir dans cette section :

   i. Adresse IP du serveur LDAP à laquelle Citrix ADC se connecte pour authentifier les utilisateurs.

   ii. Nom de domaine complet du serveur LDAP.

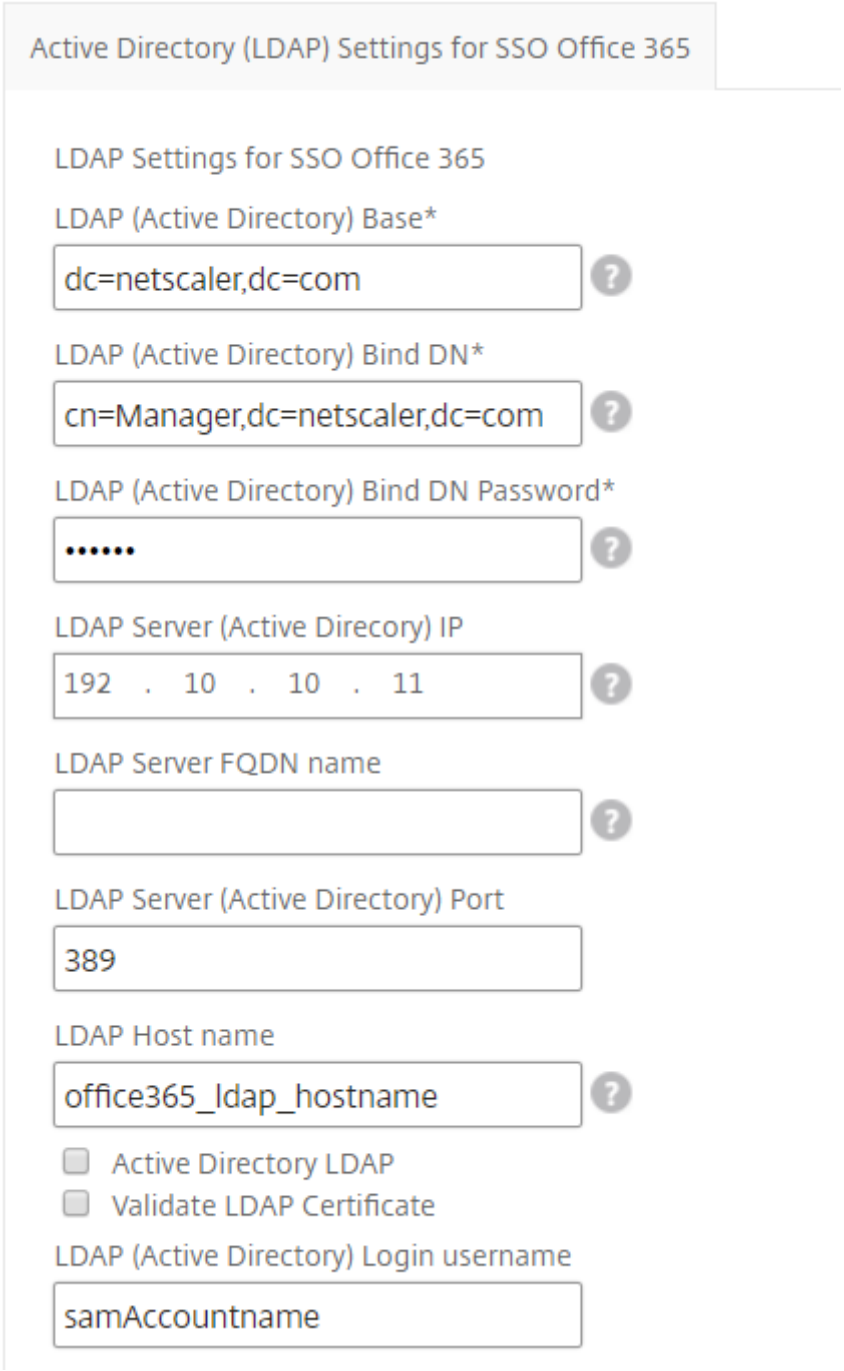
   > **Remarque**
   >
   > Vous devez spécifier au moins l'un des deux ci-dessus - l'adresse IP du serveur LDAP ou le nom de domaine complet.

   iii. Port serveur LDAP auquel Citrix ADC se connecte pour authentifier les utilisateurs (389 par défaut). LDAPS utilise 636.

   iv. Nom d'hôte LDAP. Le nom d'hôte est utilisé pour valider le certificat LDAP si la validation est activée (par défaut, elle est désactivée).

   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.



9. Dans la section **Certificat IdP SAML**, vous pouvez spécifier les détails des certificats SSL utilisés pour l'assertion SAML.

   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.

   c) **Format CertKey**. Sélectionnez le format du certificat et des fichiers de clé privée dans la

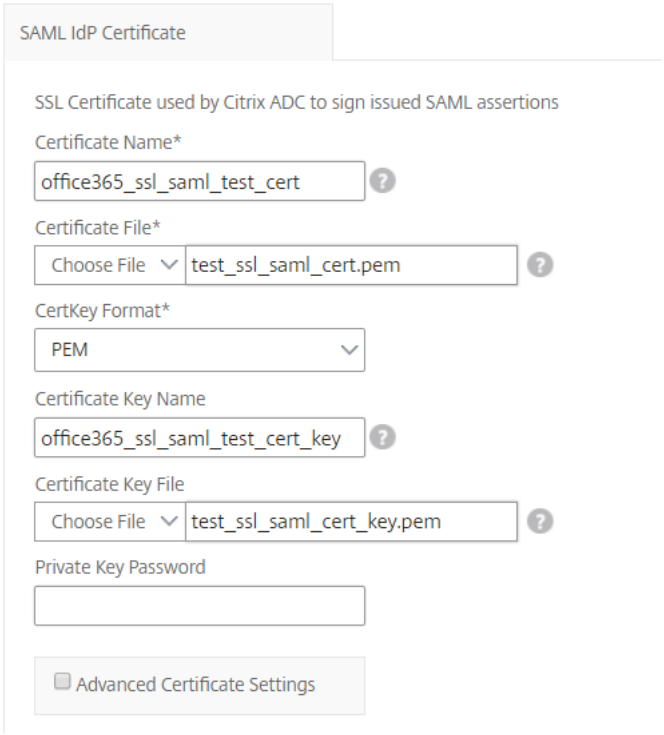
zone de liste déroulante. Les formats pris en charge sont les extensions .pem et .der.

d) **Nom de la clé de certificat**. Entrez le nom de la clé privée du certificat.

e) **Fichier de clé de certificat**. Sélectionnez le fichier contenant la clé privée du certificat à partir de votre système local.

f) **Mot de passe de clé privée** : saisissez la phrase secrète qui protège votre fichier de clé privée.

Vous pouvez également activer la case à cocher **Paramètres de certificat avancés**. Ici, vous pouvez entrer des détails tels que la période de notification d'expiration du certificat, activer ou désactiver le moniteur d'expiration du certificat.



10. Le cas échéant, vous pouvez sélectionner un **certificat d'autorité de certification SAML IdP** si le certificat SAML IdP entré ci-dessus nécessite l'installation d'un certificat public d'autorité de certification sur Citrix ADC. Assurez-vous de sélectionner « Est un certificat d'autorité de certification » dans la section **Paramètres de certificat avancés** ci-dessus.

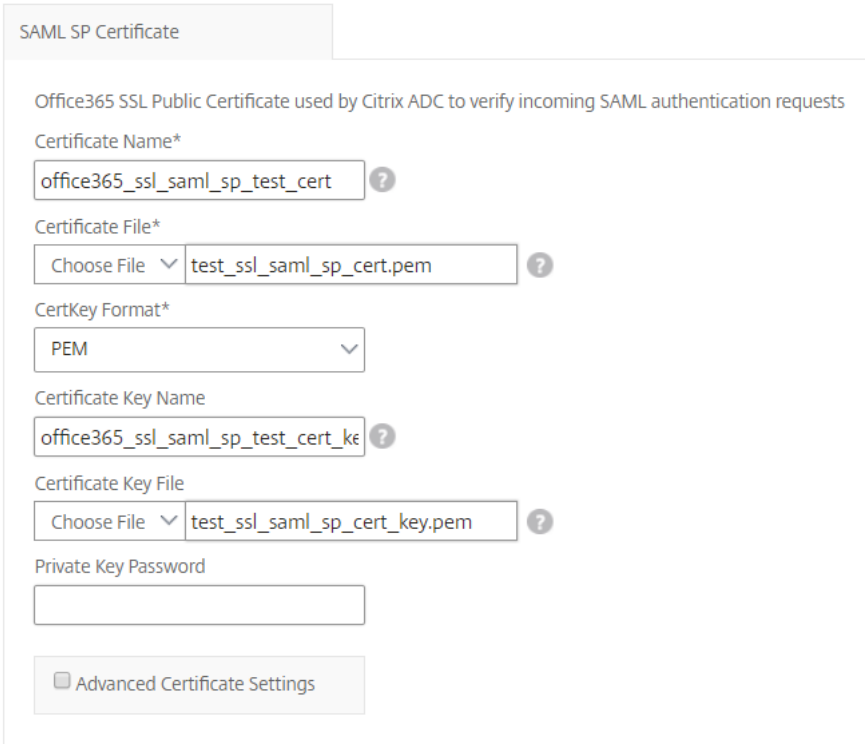
11. Dans la section **Certificat SP SAML**, entrez les détails suivants pour le certificat public SSL Office 365. Ce certificat est utilisé par l'instance de Citrix ADC pour vérifier les demandes d'authentification SAML entrantes.

a) **Nom du certificat**. Tapez le nom du certificat SSL.

b) **Fichier de certificat**. Choisissez le fichier de certificat SSL dans le répertoire de votre système local.

c) **Format CertKey**. Sélectionnez le format du certificat et des fichiers de clé privée dans la zone de liste déroulante. Les formats pris en charge sont les extensions .pem et .der.

Vous pouvez également activer la case à cocher **Paramètres de certificat avancés**. Ici, vous pouvez entrer des détails tels que la période de notification d'expiration du certificat, activer ou désactiver le moniteur d'expiration du certificat.



12. La section **Paramètres d'identification 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 Citrix ADC AAA créé à l'étape 3.

    a) **Nom de l'émetteur SAML**. Dans ce champ, tapez le nom de domaine complet public de votre serveur virtuel d'authentification. Exemple : `https://\<Citrix ADC_VIP_Address\>/saml/login`

    b) **Nom Identifiant Expression**. Tapez l'expression Citrix ADC évaluée pour extraire le SAML NameIdentifier envoyé dans l'assertion SAML. Exemple : `"HTTP.REQ.USER.ATTRIBUTE(2).B64ENCODE"`

    c) **Algorithme de signature** : sélectionnez l'algorithme pour vérifier/signer les demandes/réponses SAML (par défaut est « RSA-SHA256 »).

    d) **Méthode Digest**. Sélectionnez la méthode pour digérer le hachage pour les demandes/réponses SAML (par défaut est « SHA256 »).

    e) **Nom du public**. Saisissez le nom de l'entité ou l'URL qui représente le fournisseur de ser-

vices (Microsoft Office 365).

f) **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 correspondant à cet ID.

g) **URL du service aux consommateurs d'assertion**. Entrez l'URL du fournisseur de services où le fournisseur d'identité Citrix ADC doit envoyer les assertions SAML après l'authentification utilisateur réussie. L'URL du service consommateur d'assertion peut être initiée sur le site du serveur du fournisseur d'identité ou sur le site du fournisseur de services.

h) Il existe d'autres champs facultatifs que vous pouvez saisir dans cette section. Par exemple, vous pouvez définir les options suivantes :

   i. **Nom de l'attribut SAML**. Nom de l'attribut utilisateur envoyé dans l'assertion SAML.

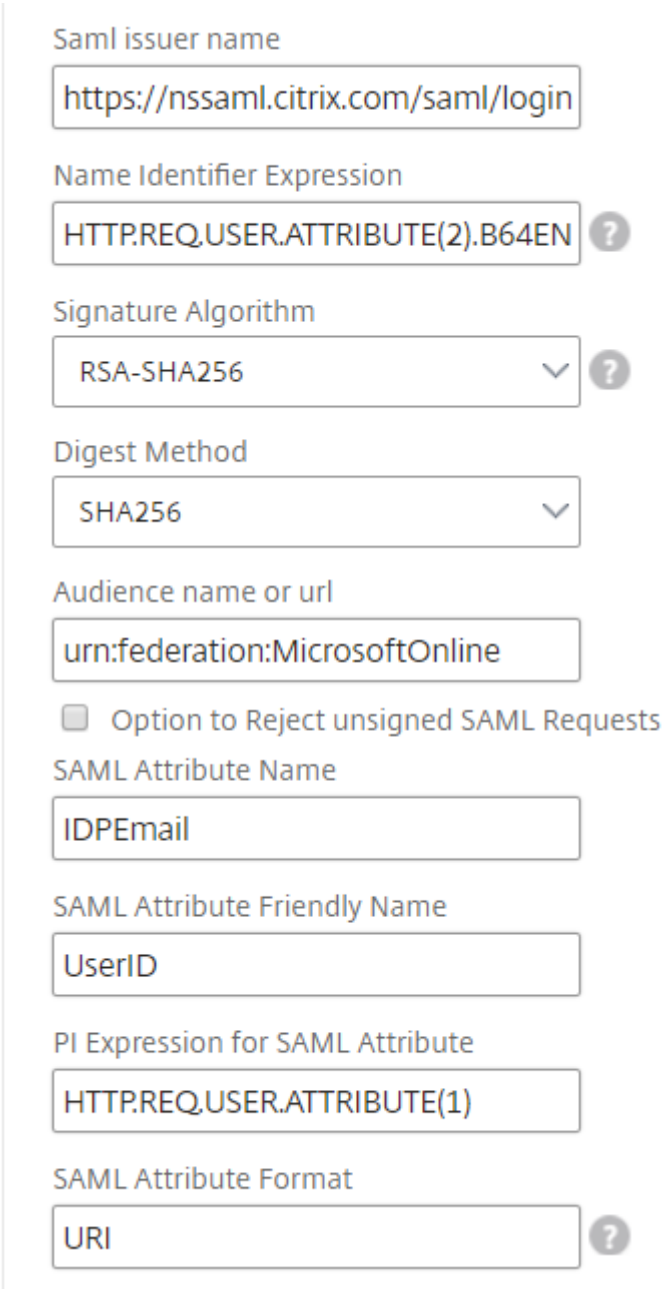
   ii. **Nom convivial de l'attribut SAML**. Nom convivial de l'attribut utilisateur envoyé dans l'assertion SAML.

   iii. **Expression PI pour l'attribut SAML**. Par défaut, l'expression Citrix ADC Policy (PI) suivante est utilisée : HTTP.REQ.USER.ATTRIBUTE (1). Ce champ spécifie le premier attribut utilisateur envoyé à partir du serveur LDAP (courrier) en tant qu'attribut d'authentification SAML.

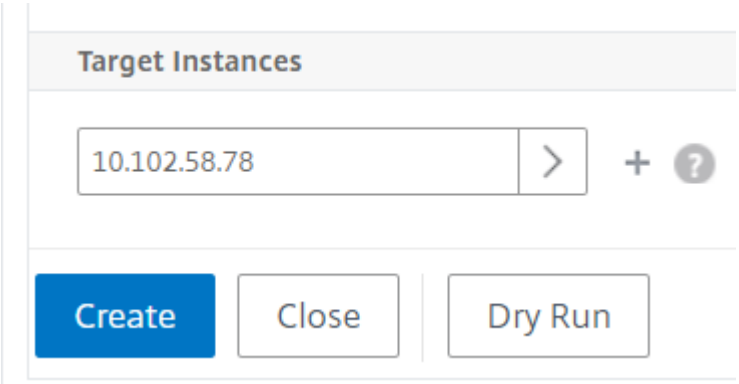
   iv. Sélectionnez le format de l'attribut utilisateur.

   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 prendre en charge les applications Microsoft Office 365.



13. Cliquez sur **Instances cibles** et sélectionnez la ou les instances Citrix ADC sur lesquelles déployer cette configuration Microsoft Office 365 SSO. Cliquez sur **Créer** pour créer la configuration et déployer la configuration sur les instances Citrix ADC sélectionnées.



Conseil

Citrix recommande qu'avant d'exécuter la configuration réelle, vous sélectionnez **Exécuter à sec** pour afficher les objets de configuration créés sur les instances Citrix ADC cibles par le StyleBook.

Microsoft Skype for Business StyleBook

April 29, 2021

L'application Skype for Business 2015 repose sur plusieurs composants externes pour fonctionner. Le réseau Skype for Business se compose de 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 l'infrastructure réseau, et les systèmes PBX téléphoniques. Skype for Business Server 2015 est disponible en deux versions, Standard Edition et Advanced Edition. La principale différence réside dans la prise en charge des fonctionnalités de haute disponibilité qui ne sont incluses que dans Advanced Edition. 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 Advanced Edition permet la création de plusieurs serveurs avec différents rôles.

Les composants principaux de l'application Skype for Business 2015 sont :

- 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, la conférence A/V, le partage d'applications, la messagerie instantanée et la conférence Web. Si vous déployez Skype for Business 2015 Édition Entreprise, la topologie se compose généralement d'au moins deux serveurs frontaux de charge équilibrée 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 à votre

le réseau interne de l'organisation doit 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 Skype for Business Edge Server :

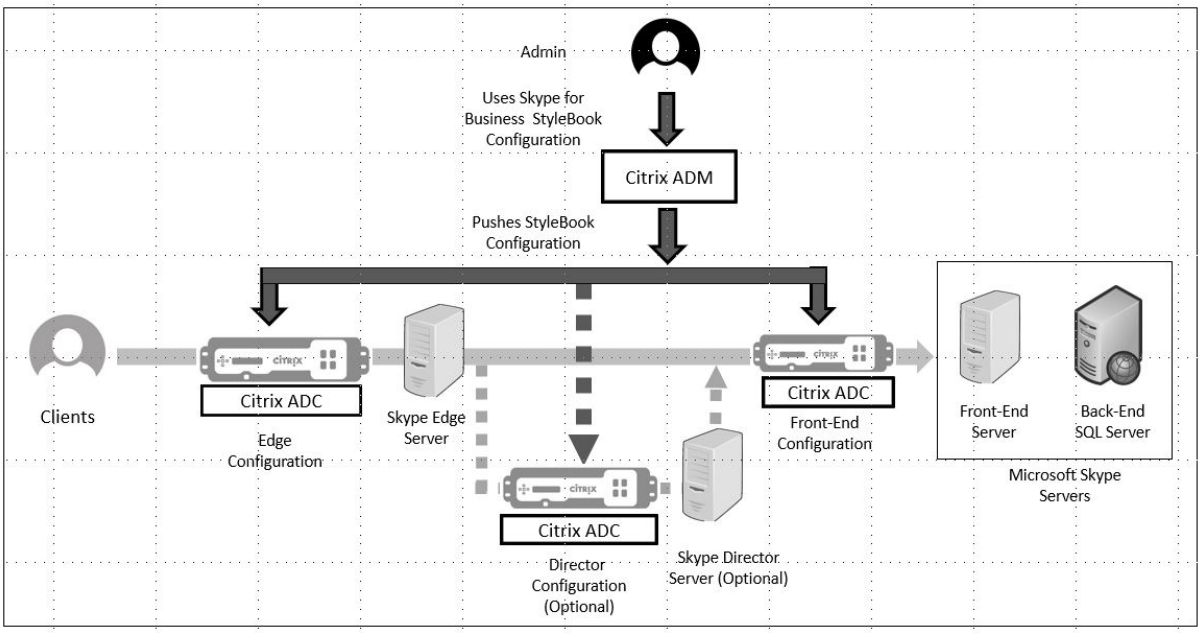
- Access Edge, qui gère le trafic SIP et authentifie les connexions externes, permet la connexion à distance et permet la connexion de fédération
- Web Conferencing, qui gère les paquets de conférence de données et permet aux utilisateurs externes d'accéder à Skype for Business
- A/V Conferencing, qui gère les paquets de conférence A/V 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 directeurs :

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 directeur 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 l'authentification des points de terminaison. De plus, pour les utilisateurs distants, un directeur sert de saut supplémentaire entre le pool Edge et le pool Front-End, ajoutant une couche supplémentaire de protection 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 :

Skype pour les serveurs professionnels	Adresse IP virtuelle	Adresses IP du serveur	Instance de Citrix ADC
Serveurs Edge	VIP externe - 192.20.20.20	192.20.20.21; 192.20.20.22	10.102.29.141
	VIP interne - 10.10.10.20	10.10.10.21; 10.10.10.22	
Serveurs frontaux	10.10.10.10	10.10.10.11; 10.10.10.12	10.102.29.60
Serveur Director	10.10.10.30	10.10.10.31; 10.10.10.32	10.102.29.93

Pour configurer des serveurs frontaux :

1. Dans Citrix Application Delivery Management (ADM), accédez à **Applications** > **Configuration**, puis cliquez sur **Créer un nouveau** . La page **Choisir StyleBook** affiche tous les StyleBooks disponibles pour votre utilisation dans Citrix ADM. Faites défiler 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 adresses IP suivantes de tous les serveurs Edge du réseau.
   a) Adresse VIP externe et adresses IP pour les serveurs Edge qui seront utilisés pour Access Edge, les conférences Web Edge et A/V Edge.
   b) Adresse VIP interne et adresses IP pour les serveurs Edge qui seront connectés au réseau interne.
   c) Deux serveurs Edge externes et deux serveurs Edge internes dans 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. En outre, entrez les adresses IP de tous les serveurs front-end Skype for Business dans le réseau.
4. Dans la section **Director Server**, entrez l'adresse IP virtuelle (VIP) pour les serveurs Director qui doit être créé pour l'application Skype for Business. En outre, entrez les adresses IP de tous les serveurs Skype for Business Director dans le 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 :

Étiquette	Port	Protocole	Description
Port HTTP	80	HTTP	Utilisé pour la communication entre les serveurs frontaux et les FQDN de batterie de serveurs Web lorsque 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.

Étiquette	Port	Protocole	Description
Port interne de découverte automatique	4443	HTTPS	HTTPS (à partir de Reverse Proxy) et HTTPS Front-End inter-pool communications pour la connexion Auto Discover.
Port RPC	135	Appel DCOM et procédure distante (RPC)	Utilisé pour les opérations DCOM telles que le déplacement des utilisateurs, la synchronisation du réplicateur utilisateur 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 mise au point SIP	444	HTTPS, TCP	Utilisé pour la communication HTTPS entre le Focus (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 de groupe de réponses.

Étiquette	Port	Protocole	Description
Port SIP AppSharing	5065	TCP	Utilisé pour les demandes d'écoute SIP entrantes pour le partage d'applications.
Port du standard SIP	5072	TCP	Utilisé pour les demandes SIP entrantes pour le préposé (c'est-à-dire pour la conférence d'accès à distance).
`SIP Conf Announcement Port`	5073	TCP	Utilisé pour les demandes SIP entrantes pour le service d'annonce de conférence de serveur Skype for Business (c'est-à-dire pour la conférence à distance).
Port SIP CallPark	5075	TCP	Utilisé pour les demandes SIP entrantes pour l'application CallPark.
Port d'admission d'appel SIP	448	TCP	Utilisé pour le contrôle d'admission d'appel par le service de stratégie de bande passante du serveur Skype for Business.

Étiquette	Port	Protocole	Description
Port d'admission d'appel SIP TORN	5080	TCP	Utilisé pour le contrôle d'admission d'appel par le service de stratégie de bande passante pour le trafic TURN Edge Audio/Vidéo.
Port de test audio SIP	5076	TCP	Utilisé pour les demandes SIP entrantes pour le service de test audio.
Port externe HTTPS	443	HTTPS	Utilisé pour les ports externes pour la communication SIP/TLS pour l'accès des utilisateurs à distance, l'accès aux conférences Web internes et les communications multimédia STUN/TCP entrantes et sortantes pour l'accès aux médias internes et aux sessions A/V.

Étiquette	Port	Protocole	Description
Port interne HTTPS	443	HTTPS	Utilisé pour les ports internes pour la communication SIP/TLS pour l'accès des utilisateurs à distance, l'accès aux conférences Web internes et les communications multimédia STUN/TCP entrantes et sortantes pour l'accès 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 distant ou la fédération.
Port d'accès à distance interne SIP	5061	TCP	Utilisé pour les ports internes pour la communication SIP/MTLS pour l'accès utilisateur distant ou la fédération.
Port UDP STUN externe SIP	3478	UDP	Utilisé pour les ports externes pour les communications multimédia entrantes et sortantes STUN/UDP.

Étiquette	Port	Protocole	Description
Port UDP STUN interne SIP	3478	UDP	Utilisé pour les ports internes pour les communications multimédia entrantes et sortantes STUN/UDP.
Port IM interne SIP	5062		Utilisé pour les ports internes pour l'authentification SIP/MTLS des communications IM sortantes via le pare-feu interne.
Port HTTP	80	TCP	Utilisé pour la communication initiale entre les directeurs et les FQDN de batterie de serveurs Web.
Port HTTPS	443	HTTPS	Utilisé pour la communication entre les directeurs et les noms de domaine complets de la batterie de serveurs Web.
Port interne de découverte automatique	4443	HTTPS	Utilisé pour les communications HTTPS (à partir de Reverse Proxy) et HTTPS Director inter-pool pour la connexion Auto Discover.

Étiquette	Port	Protocole	Description
Port interne SIP	5061	TCP	Utilisé pour les communications internes entre les serveurs et pour les connexions client.

1. Dans la section **Instances cibles**, sélectionnez les trois instances Citrix ADC sur lesquelles déployer les trois serveurs Skype for Business.

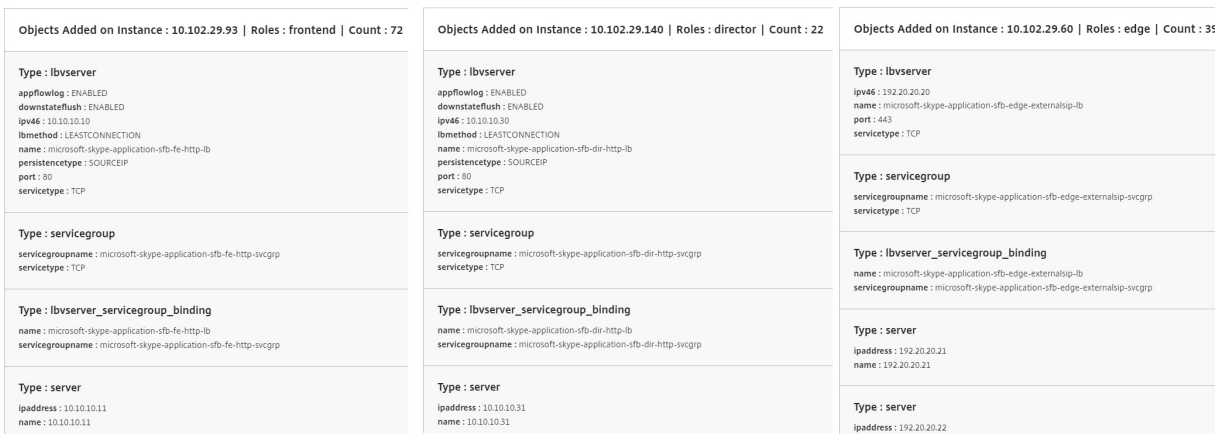
   > **Remarque**
   >
   > Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter des instances Citrix ADC récemment découvertes dans Citrix ADM à la liste des instances disponibles dans cette fenêtre.

2. Cliquez sur **Créer** pour créer la configuration sur les instances Citrix ADC sélectionnées.

   > **Conseil**
   >
   > Citrix vous recommande de sélectionner **Exécuter à sec** 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. Autrement dit, 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 :



Microsoft Exchange StyleBook

April 29, 2021

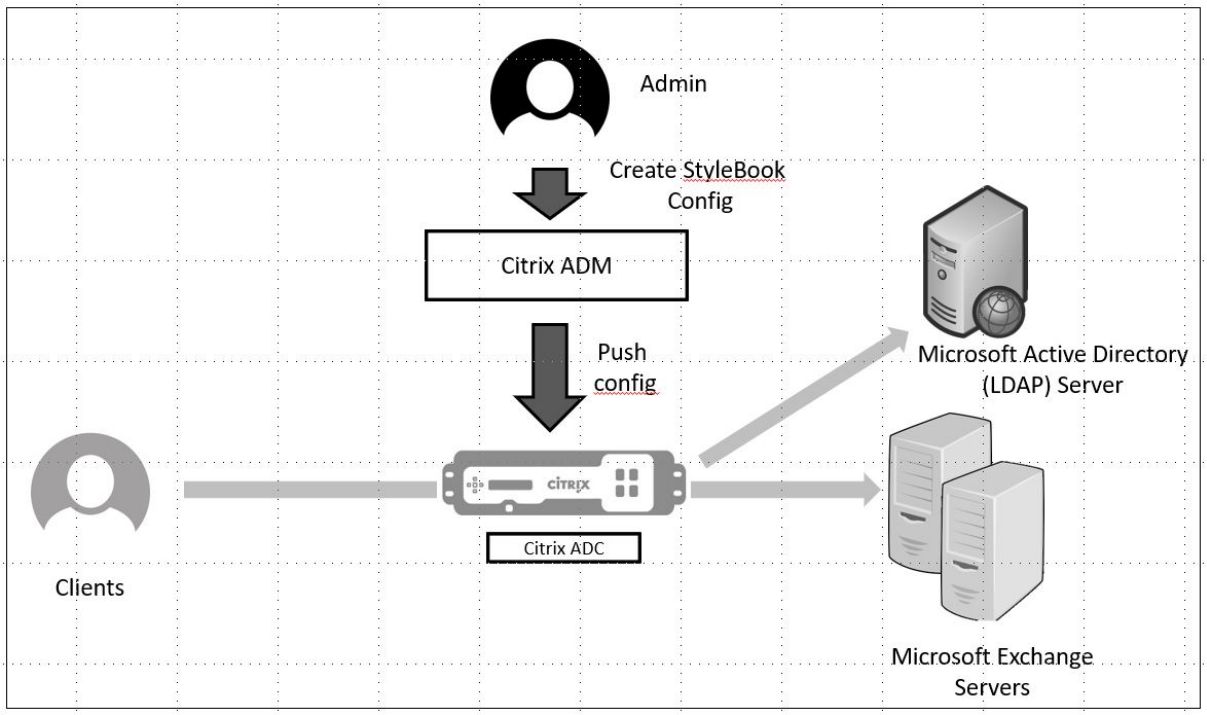
Vous pouvez utiliser Microsoft Exchange 2016 StyleBook pour déployer une configuration Citrix ADC qui optimise et sécurise une application d'entreprise Microsoft Exchange 2016 dans votre réseau. Microsoft Exchange 2016 est une application d'entreprise clé pour fournir des services de messagerie, de gestion des informations personnelles et de messagerie à vos employés et à d'autres parties prenantes.

Fonctionnalités Citrix ADC configurées à l'aide de Microsoft Exchange StyleBook

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 l'accès à une seule adresse IP et la redirection des requêtes vers les serveurs virtuels d'équilibrage de charge corrects
- Rewrite - Redirige les utilisateurs vers des pages sécurisées
- Déchargement SSL : décharge le traitement SSL sur le 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 les certificats, tous les hôtes adressables qui font partie de la configuration réseau doivent avoir des noms de domaine résolus et pas seulement des adresses IP.
- Assurez-vous que les ports SIP sont accessibles dans le serveur Microsoft Exchange 2016.

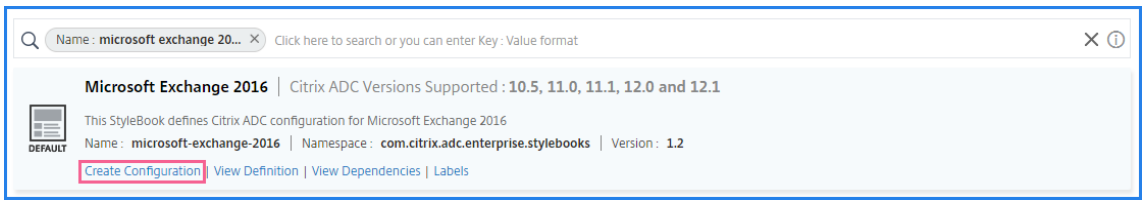
Configuration de Microsoft Exchange StyleBook

Configurez le Microsoft Exchange StyleBook dans votre entreprise pour déployer la configuration de 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 entrer 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 des demandes client 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 sur Citrix ADM. Entrez les noms du certificat et des fichiers clés et téléchargez à partir du stockage local. Vous pouvez également fournir un mot de passe de clé privée pour chiffrer le fichier de 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 de l'expiration du certificat ou des paramètres avancés, 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.

   - **VIP d'authentification Active Directory** : adresse IP virtuelle utilisée pour créer et configurer le serveur virtuel AD (LDAP) sur une appliance Citrix ADC.
   - **IP du serveur Active Directory** - Adresse IP de votre Controller de domaine Active Directory.
   - **Chaîne de base Active Directory - Chaîne** de base LDAP dans Active Directory. Par exemple, CN=Users, DC=CTXNSSFB, DC=COM.
   - **Active Directory LDAP Bind Name (DN)** - LDAP Bind Distinguished Name (DN) est utilisé pour lier cet objet au serveur LDAP (AD). Par exemple « CN=Administrateur, CN=Utilisateurs, dc=acme, dc=com »
   - Mot de**passe du nom unique (DN) de liaison LDAP Active Directory** - Le nom unique de liaison LDAP est le mot de passe de l'authentification AD

- Attribut de**nom d'utilisateur Active Directory - Attribut** AD pour le nom d'utilisateur. L'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'attribut du groupe LDAP configurés sur le serveur LDAP. Par exemple, « MemberOf » pour l'attribut group dans LDAP.
- **Nom de sous-attribut Active Directory** : noms de sous-attribut LDAP configurés sur le serveur LDAP. Par exemple, « cn » pour le sous-attribut dans LDAP.
- **Domaine d'authentification Active Directory** - Nom de domaine AD/LDAP utilisé pour l'authentification. Par exemple, ctxnssfb.com.

6. Dans la section **Instances cibles**, sélectionnez l'instance Citrix ADC sur laquelle déployer cette configuration Exchange.

   > **Remarque**
   >
   > Si vous souhaitez afficher les instances Citrix ADC récemment découvertes, cliquez sur l'icône d'actualisation.

7. Cliquez sur **Créer** pour créer le fichier de configuration et exécuter la configuration sur l'instance Citrix ADC sélectionnée.

   Citrix vous recommande d'abord 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 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 créés et liés aux serveurs virtuels d'équilibrage de charge.

Microsoft SharePoint StyleBook

April 29, 2021

Microsoft SharePoint 2016 est une application d'entreprise clé qui fournit principalement un système de gestion de documents et de stockage, hautement configurable et pris en charge par tous les principaux navigateurs.

Vous pouvez utiliser Microsoft SharePoint 2016 StyleBook pour déployer une configuration de Citrix ADC qui optimise et sécurise l'application d'entreprise Microsoft SharePoint 2016 dans votre réseau.

Conditions préalables

- Microsoft SharePoint 2016

- Citrix Application Delivery Management (ADM), version 12.0 et ultérieure
- Citrix ADC, version 10.5 et ultérieure

Fonctionnalités de Citrix ADC configurées par Microsoft SharePoint 2016 StyleBook

Vous pouvez utiliser le Microsoft SharePoint 2016 StyleBook pour activer et configurer les fonctionnalités Citrix ADC suivantes pour Microsoft SharePoint 2016 :

- Équilibrage de charge
- Commutation de contenu
- Répondeur
- Réécrire
- Compression SSL
- Mise en cache intégrée

Équilibrage de charge

L'équilibrage de charge Citrix ADC distribue uniformément les demandes aux serveurs SharePoint back-end. La surveillance intelligente des serveurs back-end empêche l'envoi de demandes à 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.

Citrix ADM prend désormais en charge le mode SSL de l'application SharePoint en configurant des serveurs virtuels SSL LB. Assurez-vous de sélectionner SSL comme protocole frontal. Notez que le port virtuel est défini sur 443 par défaut.

Commutation de contenu

La fonction 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, documents, images et fichiers audio ou vidéo). Le module de commutation de contenu dirige le trafic entrant vers un serveur virtuel d'équilibrage de charge correspondant optimal qui peut traiter ce type de contenu. Vous pouvez donc appliquer différentes stratégies d'optimisation à différents types de trafic. Par exemple, vous pouvez utiliser des stratégies de compression ou de mise en cache différentes pour la vidéo que pour les documents texte.

Répondeur

La fonctionnalité de répondeur d'une instance de Citrix ADC peut être utilisée pour rediriger en toute transparence les utilisateurs de HTTP vers HTTPS. Le répondeur peut également être configuré pour

fournir des pages d'erreur personnalisées. La stratégie Répondeur détermine les demandes (trafic) sur lesquelles une action doit être effectuée et lie chaque stratégie à un serveur virtuel d'équilibrage de charge. SharePoint StyleBook inclut une configuration qui redirige les utilisateurs des URL HTTP vers 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 selon les cas d'utilisation particuliers. Par exemple, la réécriture peut donner accès au contenu demandé sans exposer de détails inutiles sur le serveur du site Web.

Dans SharePoint StyleBook, la fonctionnalité de réécriture est utilisée pour supprimer les en-têtes inutiles des demandes des utilisateurs.

Compression SSL

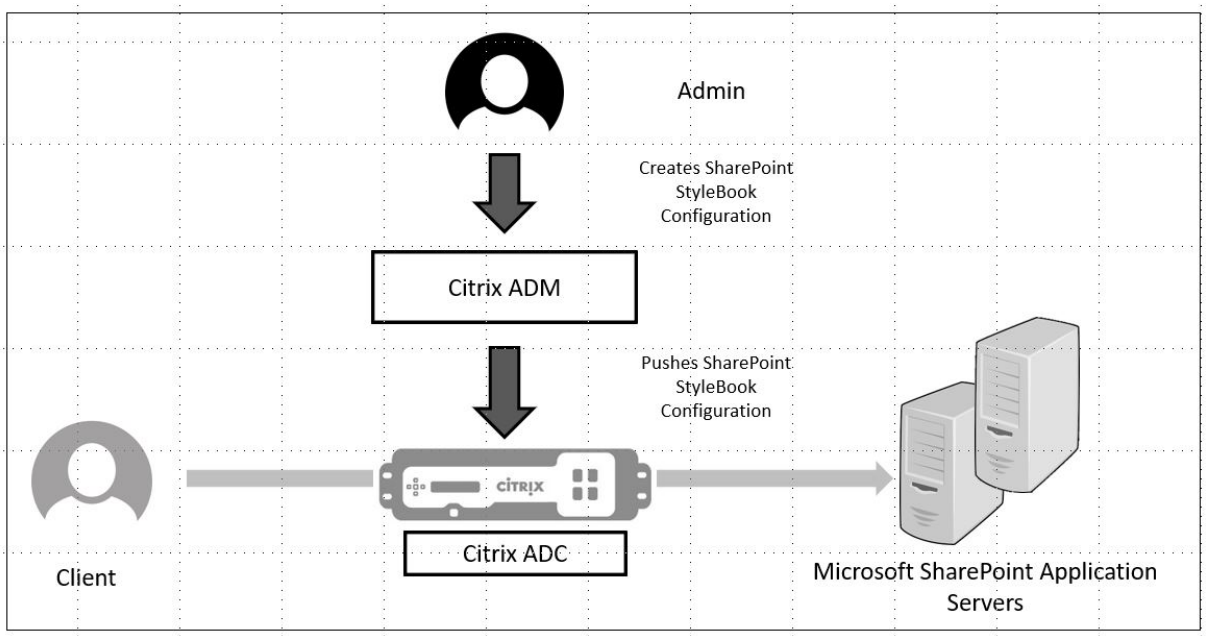
Le moteur de compression Citrix ADC identifie et compresse le contenu compressible. Ce processus améliore le temps de transmission des données et réduit les besoins en bande passante réseau pour les clients, tout en économisant les cycles CPU sur les serveurs de contenu SharePoint. Une instance de Citrix ADC peut compresser à la fois des données statiques et 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 plus efficace. La capacité du navigateur client à décompresser les données dépend du ou des algorithmes qu'il prend en charge : GZIP, DEFLATE, ou les deux.

Une instance de Citrix ADC est configurée pour compresser le texte en HTML, XML, texte brut, feuille de style en cascade (CSS) et documents 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 WAN et de meilleures performances du serveur.

Mise en cache intégrée

Le cache en mémoire Citrix ADC peut stocker des objets SharePoint afin de fournir rapidement du 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 Microsoft SharePoint 2016 StyleBook dans votre réseau d'entreprise.

Pour déployer Microsoft SharePoint 2016 StyleBook :

1. Dans Citrix ADM, accédez à **Applications** > **Administration** > **Configuration**, puis cliquez sur **Créer un nouveau**.

   La page **Choisir StyleBook** affiche tous les StyleBooks disponibles pour votre utilisation dans Citrix ADM.

2. Faites défiler la page vers le bas et sélectionnez **Microsoft SharePoint 2016 StyleBook**.

   > **Remarque**
   >
   > Dans Citrix ADM, accédez à **Applications**> **Configurations**> **StyleBooks**. Faites défiler la page vers le bas pour trouver le **Microsoft SharePoint 2016 StyleBook**. Dans le panneau **StyleBook Microsoft SharePoint 2016**, cliquez sur **Créer une configuration**.

   Le StyleBook s'ouvre sous la forme d'un 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) **IP virtuelle SharePoint**. Adresse IP virtuelle à laquelle l'instance de Citrix ADC reçoit des demandes client pour l'application Microsoft SharePoint.

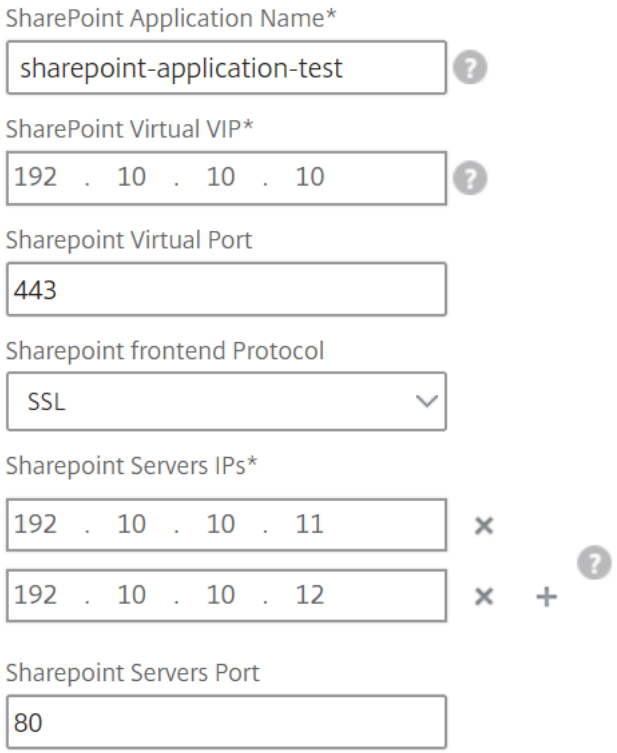
c) **Port virtuel SharePoint**. Port TCP à utiliser par les utilisateurs pour accéder à l'application SharePoint

d) **Protocole frontend SharePoint**. Sélectionnez le protocole frontal SharePoint dans la liste déroulante. Les options disponibles sont HTTP ou SSL.

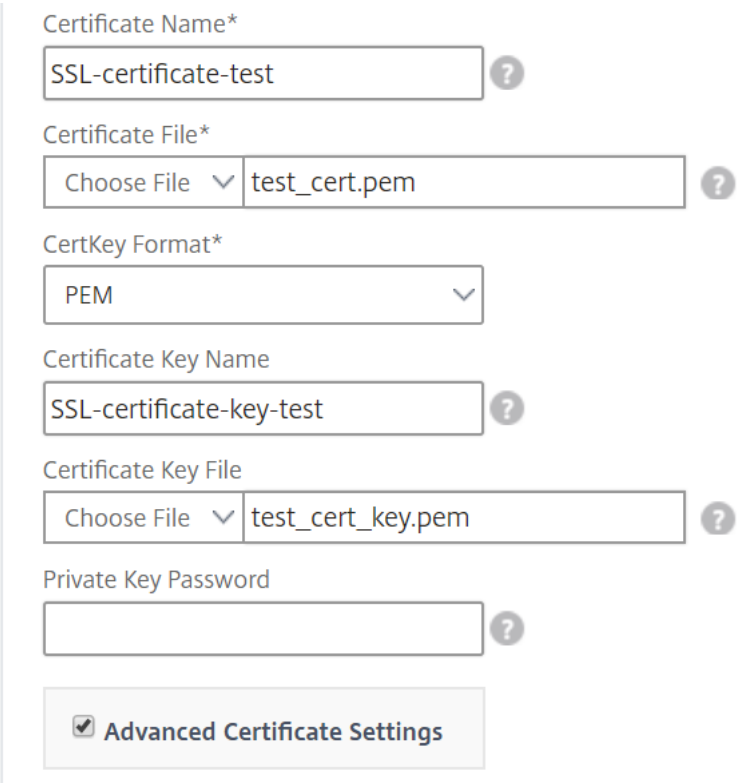
> **Remarque**
>
> Si vous sélectionnez SSL, assurez-vous que le paramètre Configuration de réécriture est activé dans la section Paramètres avancés de SharePoint de ce StyleBook.

e) **IP SharePoint Server**. Adresses IP de tous les serveurs SharePoint du réseau.

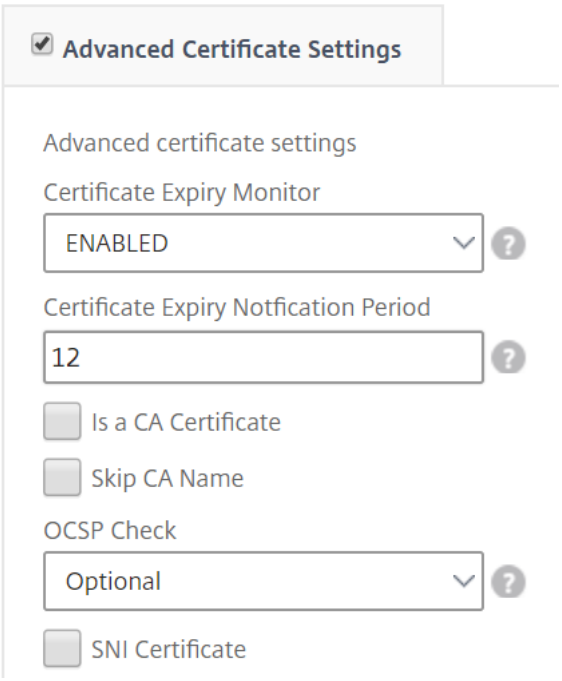
f) **Port des serveurs SharePoint**. Numéro de port TCP utilisé par les serveurs SharePoint. Par défaut, il s'agit de 80. Vous pouvez modifier cette valeur si nécessaire, mais assurez-vous que ce port est accessible sur les serveurs Microsoft SharePoint 2016.



3. Dans la section **Paramètres des certificats SSL**, cliquez sur + pour entrer le nom du certificat SSL, la clé de certificat, et sélectionnez les fichiers respectifs dans votre dossier de stockage local.

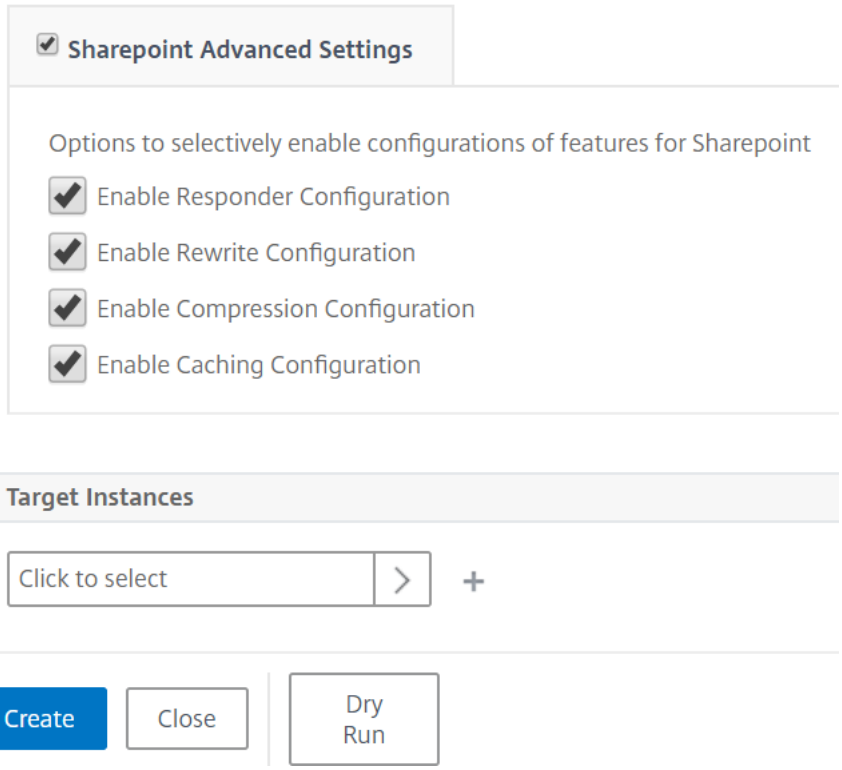


4. Vous pouvez également cliquer sur **Paramètres de certificat avancés** pour activer ou désactiver la surveillance de l'expiration des certificats SSL. Si vous activez la surveillance de l'expiration des certificats, définissez le nombre de jours de sorte que Citrix ADM émet une alarme après ces nombreux jours où le certificat est sur le point d'expirer. Vous avez également la possibilité de vérifier l'OCSP en tant que fonctionnalité facultative ou obligatoire.



5. La section **Paramètres avancés** de SharePoint vous permet d'activer les fonctionnalités de Citrix ADC qui seront configurées sur les instances de Citrix ADC. Alors que les fonctions d'équilibrage de charge et de commutation de contenu sont configurées par défaut sur les instances, 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 **Instances cibles** et sélectionnez l'instance Citrix ADC sur laquelle déployer cette configuration SharePoint. Cliquez sur **Créer** pour créer la configuration et déployer la configuration sur l'instance Citrix ADC sélectionnée.

   > **Remarque**
   >
   > Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter des instances Citrix ADC récemment découvertes dans Citrix ADM à la liste des instances disponibles dans cette fenêtre.



> **Remarque**
>
> Citrix recommande qu'avant d'exécuter la configuration réelle, vous sélectionnez **Exécuter à sec** 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 de Citrix ADC pour SharePoint StyleBook. Accédez à **Applications** > **Administration** > **Configuration**, puis cliquez sur **Afficher les objets créés** . La figure suivante montre certains des objets créés, avec les adresses IP spécifiées dans l'exemple illustré dans « Deploying SharePoint StyleBook Configurations from Citrix ADM. »

Type : lbvserver

appflowlog : DISABLED
backuppersistencetimeout : 20
downstateflush : DISABLED
ipv46 : 0.0.0.0
lbmethod : LEASTCONNECTION
name : sharepoint application test frontpage services lb
persistencebackup : SOURCEIP
persistencetype : COOKIEINSERT
port : 0
servicetype : HTTP
timeout : 20

Type : servicegroup

cip : DISABLED
cka : YES
cmp : NO
downstateflush : DISABLED
healthmonitor : NO
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp
servicetype : HTTP
sp : ON
state : ENABLED
tcpb : NO
useproxyport : NO
usip : NO

Type : lbvserver_servicegroup_binding

name : sharepoint-application-test-frontpage-services-lb
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.10.10.11
port : 80
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.10.10.12
port : 80
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

Type : csaction

name : sharepoint-application-test-cs-frontpage-services-csaction
targetlbvserver : sharepoint-application-test-frontpage-services-lb

Type : cspolicy

action : sharepoint-application-test-cs-frontpage-services-csaction
policyname : sharepoint-application-test-cs-frontpage-services-cspol
rule : HTTP.REQ.HEADER("X-Vermeer-Content-Type").EXISTS

Type : csvserver_cspolicy_binding

name : sharepoint-application-test-cs
policyname : sharepoint-application-test-cs-frontpage-services-cspol
priority : 10

Microsoft ADFS Proxy StyleBook

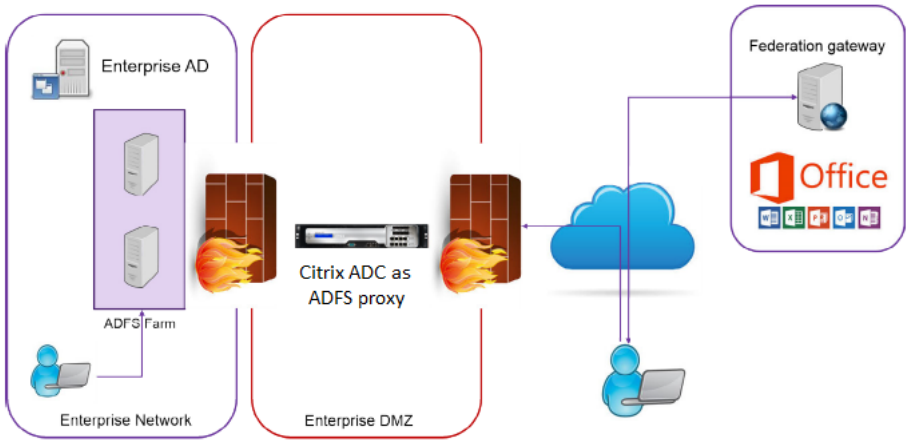
April 29, 2021

Le proxy ADFS Microsoft™ joue un rôle important en accordant un accès à l'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 depuis Internet. Le proxy ADFS est un proxy inverse et réside généralement dans le réseau de périmètre (DMZ) de votre organisation. Le proxy ADFS joue un rôle essentiel dans la connectivité utilisateur distante et l'accès aux applications.

Citrix ADC dispose de la technologie précise permettant de sécuriser la connectivité, l'authentification et la gestion de l'identité fédérée. L'utilisation de Citrix ADC comme proxy ADFS évite le besoin de déployer un composant supplémentaire dans la zone DMZ.

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 illustre le déploiement d'une instance 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 aux besoins d'équilibrage de charge et de proxy ADFS
2. Prend en charge les scénarios d'accès utilisateur interne et externe
3. Prend en charge les méthodes riches pour la pré-authentification
4. Offre une expérience d'authentification unique pour les utilisateurs
5. Prend en charge les protocoles actifs et passifs
    a) Exemples d'applications de protocole actives : Microsoft Outlook, Microsoft Skype for Business

   b) Exemples d'applications de protocole passives : application Web Microsoft Outlook, navigateurs Web
6. Périphérique renforcé pour un déploiement basé sur DMZ
7. Ajoute de la valeur à l'aide de fonctionnalités principales supplémentaires de Citrix ADC
   a) Commutation de contenu
   b) Déchargement SSL
   c) Réécrire
   d) Sécurité (Citrix ADC AAA)

Pour les scénarios basés sur le 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 Gateway 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 la Federation Gateway. La Federation Gateway, à son tour, soumet le jeton à Office 365 pour fournir un accès client.

Pour les clients passifs, ADFS Proxy StyleBook crée un compte utilisateur KCD (Kerberos Constrained Délégation). Le compte KCD est nécessaire pour que l'authentification Kerberos SSO se connecte 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 s'assurer que les serveurs DNS sur le Citrix ADC sont configurés pour ADFS.

La section de configuration ci-dessous décrit comment configurer Citrix ADC pour gérer l'authentification client basée sur le protocole actif et passif.

Détails de la configuration

Le tableau ci-dessous répertorie les versions logicielles minimales requises pour que cette intégration puisse être déployée avec succès.

Produit	Version minimale requise
Citrix ADC	11.0, Licence avancée/Premium

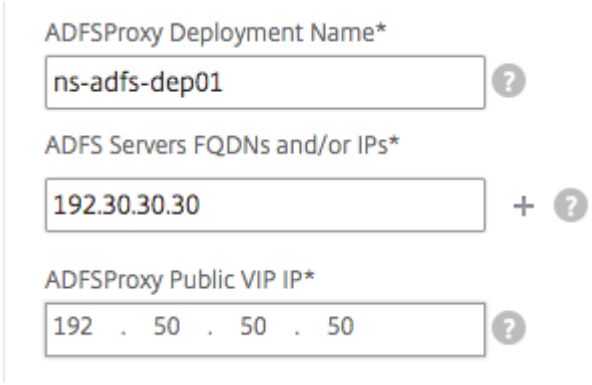
Les instructions suivantes supposent que vous avez déjà créé les entrées DNS externes et internes appropriées.

Déploiement des configurations StyleBook proxy Microsoft ADFS à partir de Citrix ADM

Les instructions suivantes vous aident lors de l'implémentation du Proxy Microsoft ADFS StyleBook dans votre réseau d'entreprise.

Pour déployer Microsoft ADFS Proxy StyleBook

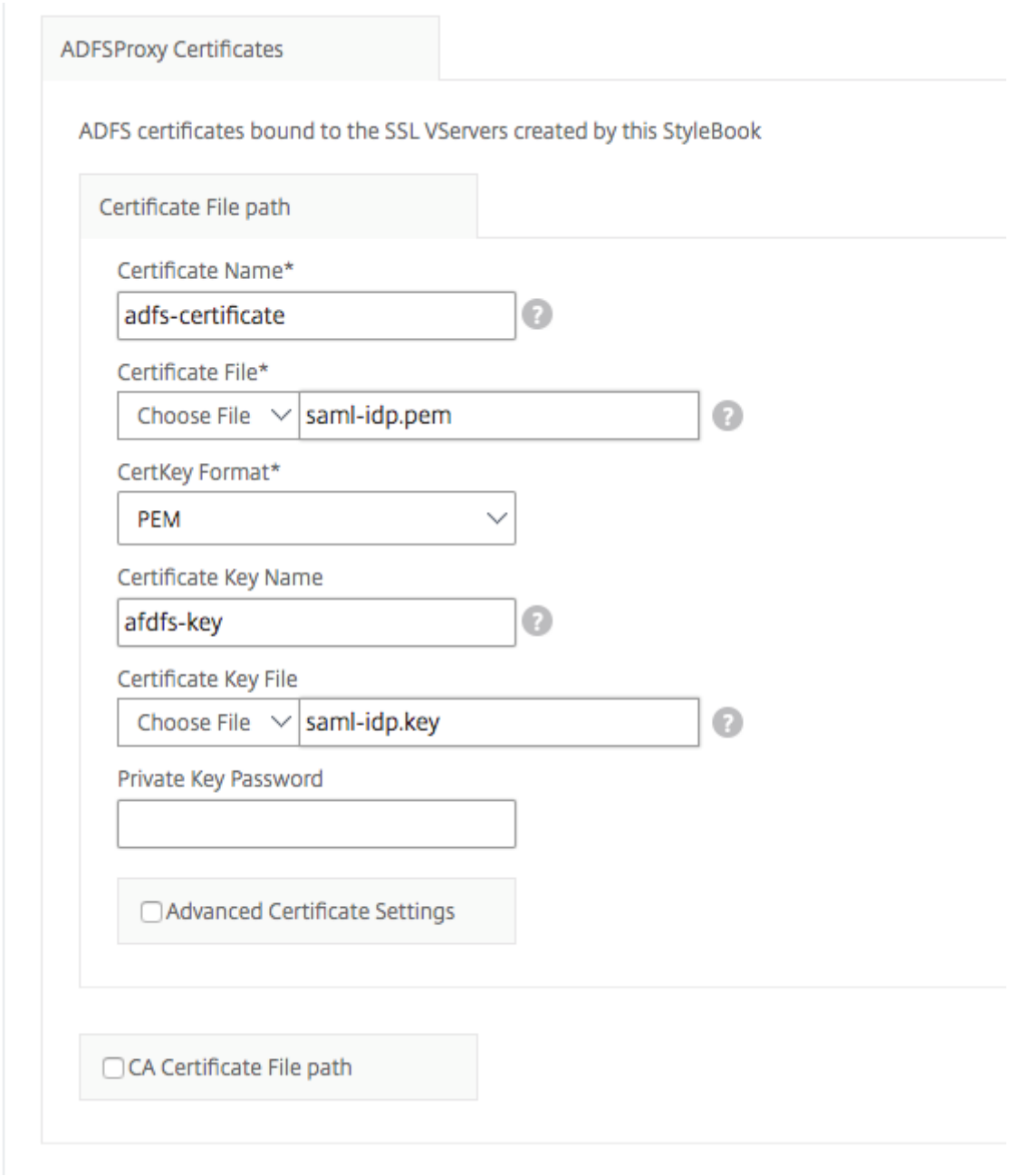
1. Dans Citrix ADM, accédez à **Applications** > **StyleBooks**. La page **StyleBooks** affiche tous les StyleBooks disponibles pour votre utilisation dans Citrix ADM.
2. Faites défiler vers le bas et recherchez le **Proxy Microsoft ADFS StyleBook**. Cliquez sur **Créer une configuration**.
   Le StyleBook s'ouvre sous la forme d'une page d'interface utilisateur sur laquelle vous pouvez taper les valeurs de tous les paramètres définis dans ce StyleBook.
3. Tapez des valeurs pour les paramètres suivants :
   a) **Nom de déploiement du proxy ADFS**. Sélectionnez un nom pour la configuration de proxy ADFS déployée sur votre réseau.
   b) **FQDN ou adresses IP des serveurs ADFS**. Tapez les adresses IP ou FQDN (noms de domaine) de tous les serveurs ADFS du réseau.
   c) **IP VIP publique du proxy ADFS**. Tapez l'adresse IP virtuelle publique sur l'Citrix ADC qui fonctionne en tant que serveur proxy ADFS.



4. Dans la section **Certificats de proxy ADFS**, tapez les détails du certificat SSL et de la clé de certificat.

   Ce certificat SSL est lié à tous les serveurs virtuels créés sur l'instance de Citrix ADC.

   Sélectionnez les fichiers respectifs dans votre dossier de stockage local. Vous pouvez également saisir le mot de passe de clé privée pour charger les clés privées chiffrées au format .pem.



Vous pouvez également activer la case à cocher **Paramètres de certificat avancés**. Ici, vous pouvez taper des détails tels que la période de notification d'expiration du certificat, activer ou désactiver le moniteur d'expiration du certificat.

5. Le cas échéant, vous pouvez cocher la case **Certificat d'autorité de certification SSL** si le certificat SSL 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** .
6. Activer l'authentification pour les clients actifs et passifs. Tapez le nom de domaine DNS util-

isé dans Active Directory pour l'authentification utilisateur. Vous pouvez ensuite configurer l'authentification pour les clients actifs ou passifs, ou les deux.

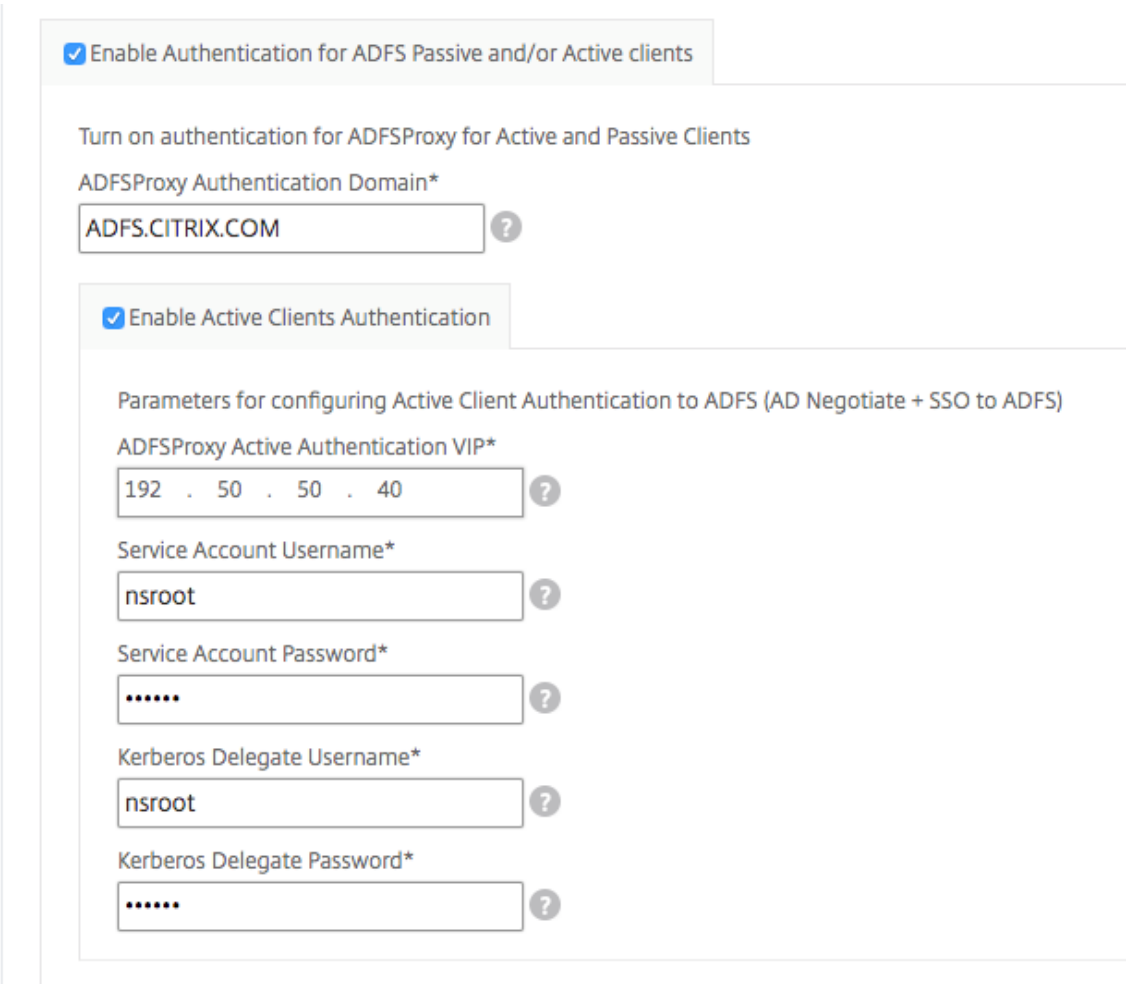
7. Tapez les détails suivants pour activer l'authentification pour les clients actifs :

   > **Remarque**
   >
   > Il est facultatif de configurer la prise en charge des clients actifs.

   a) **ADFS Proxy Active Authentication VIP**. Tapez l'adresse IP virtuelle du serveur d'authentification virtuel sur l'instance de Citrix ADC dans laquelle les clients actifs sont redirigés pour authentification.

   b) Nom d'**utilisateur du compte de service**. Tapez le nom d'utilisateur du compte de service utilisé par Citrix ADC pour authentifier vos utilisateurs dans l'annuaire actif.

   c) Mot de**passe du compte de service**. Saisissez le mot de passe utilisé par Citrix ADC pour authentifier vos utilisateurs dans l'annuaire actif.



8. Configurez l'authentification pour les clients passifs en activant l'option correspondante et en configurant les paramètres LDAP.

> **Remarque**
>
> Il est facultatif de configurer la prise en charge des clients passifs.

Tapez les détails suivants 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) **LDAP (Active Directory) Bind DN**. Ajoutez un compte de domaine (à l'aide d'une adresse e-mail pour faciliter la configuration) qui dispose des 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)**. Tapez le mot de passe du compte de domaine pour l'authentification.

Voici quelques autres champs que vous devez saisir dans les valeurs de cette section :

d) **IP du serveur LDAP (Active Directory)**. Tapez l'adresse IP du serveur Active Directory pour que l'authentification AD fonctionne correctement.

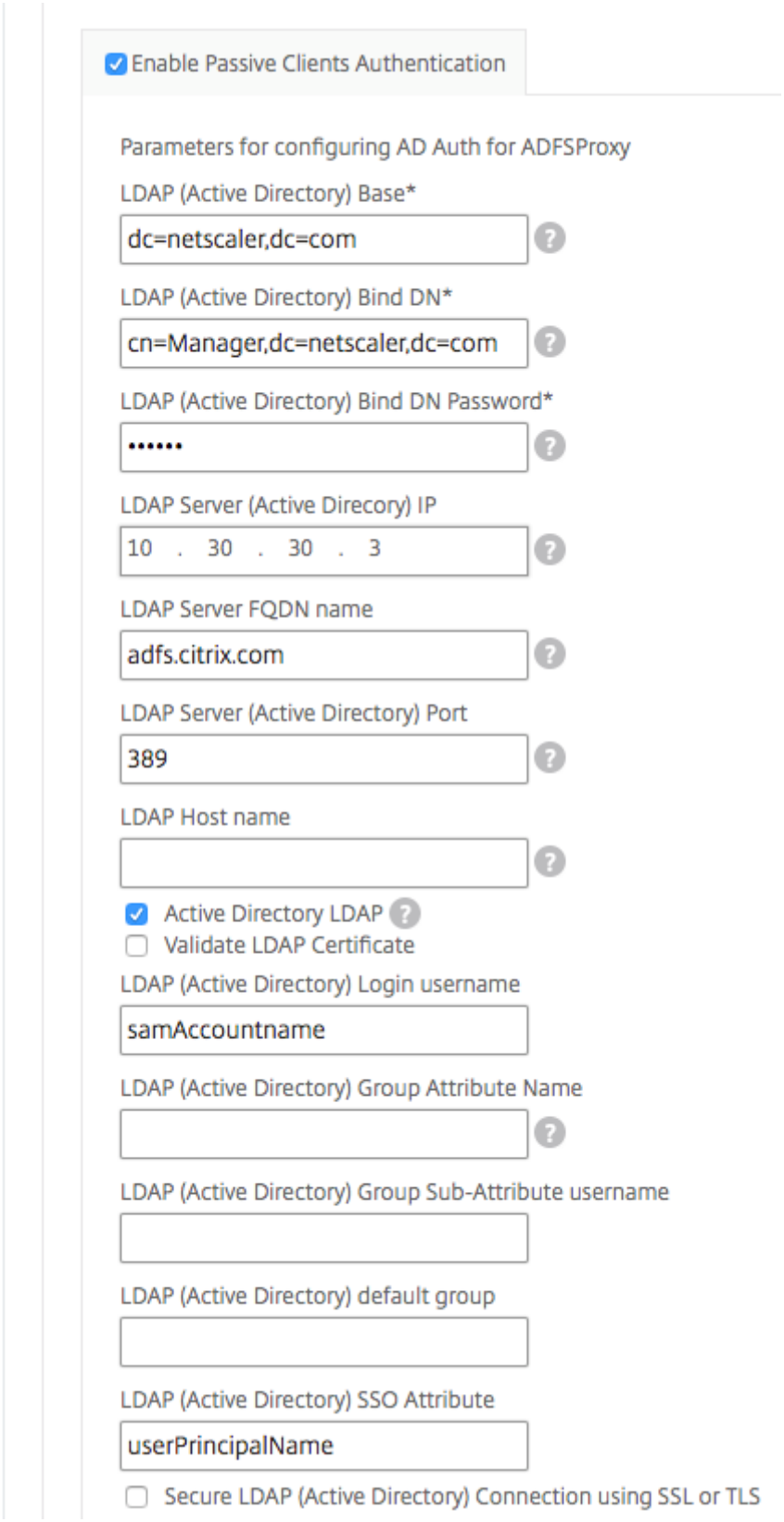
e) **Nom de domaine complet du serveur LDAP**. Tapez le nom de domaine complet du serveur Active Directory. Le nom de domaine complet est facultatif. Indiquez l'adresse IP comme à l'étape 1 ou le nom de domaine complet.

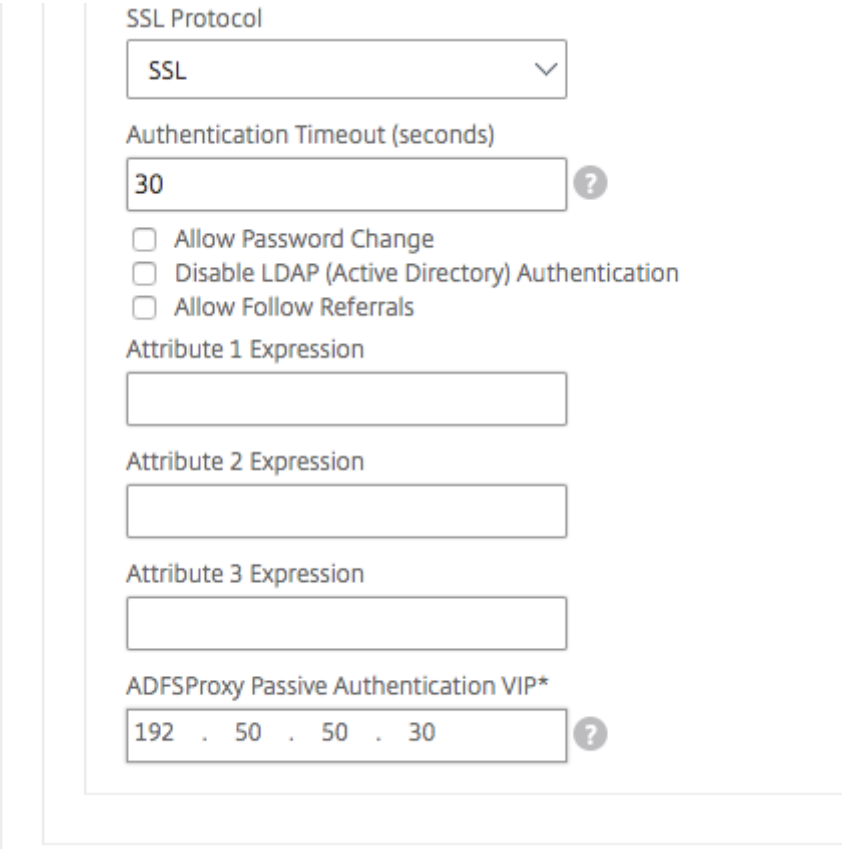
f) **Port Active Directory du serveur LDAP**. Par défaut, les ports TCP et UDP pour le protocole LDAP sont 389, tandis que le port TCP pour Secure LDAP est 636.

g) **Nom d'utilisateur de connexion LDAP (Active Directory)**. Tapez le nom d'utilisateur comme « SamAccountName. «

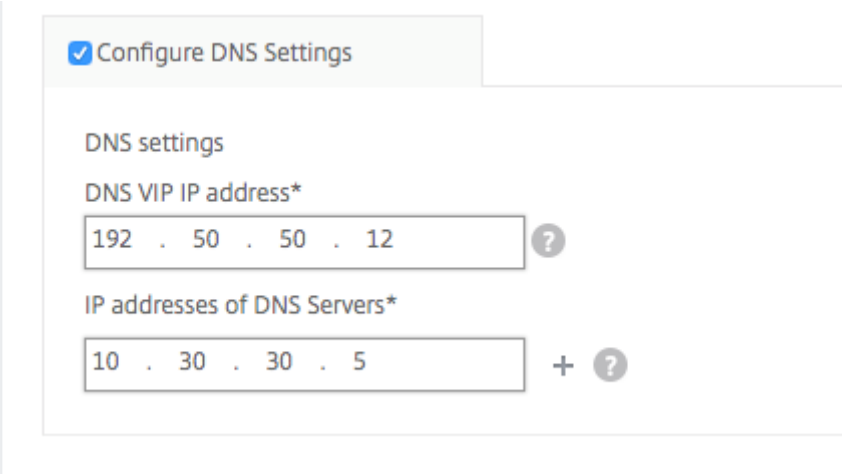
h) **VIP de l'authentification passive par proxy ADFS**. Tapez l'adresse IP du serveur virtuel proxy ADFS pour les clients passifs.

> **Remarque**
>
> Les champs marqués par « * » sont obligatoires.

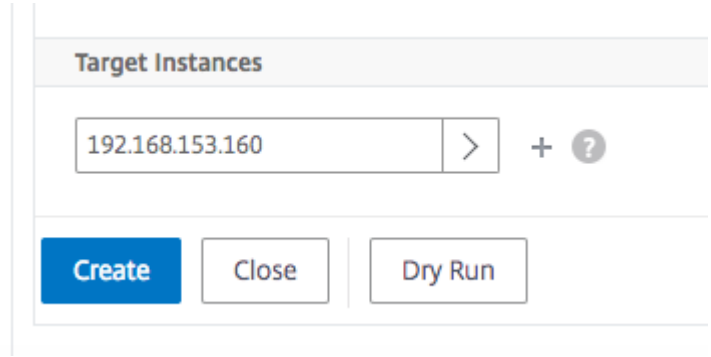




9. Vous pouvez également configurer un VIP DNS pour vos serveurs DNS.



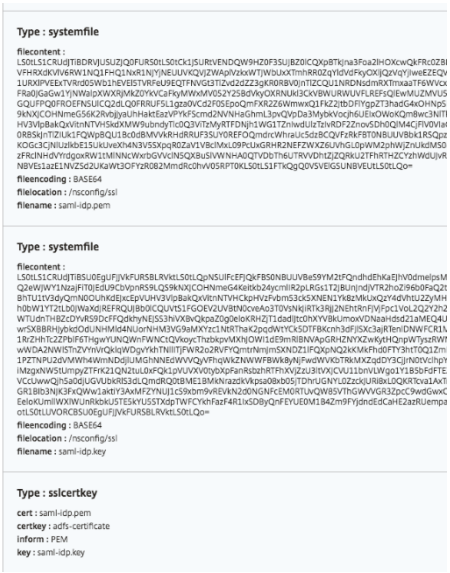
10. Cliquez sur **Instances cibles** et sélectionnez les instances Citrix ADC pour déployer cette configuration de proxy Microsoft ADFS. Cliquez sur **Créer** pour créer la configuration et déployer la configuration sur les instances Citrix ADC sélectionnées.



> **Remarque**
>
> Citrix recommande qu'avant d'exécuter la configuration réelle, vous sélectionnez **Exécuter à sec.** Vous pouvez d'abord afficher les objets de configuration créés sur les instances Citrix ADC cibles par le StyleBook. Vous pouvez ensuite cliquer sur **Créer** pour déployer la configuration sur les instances sélectionnées.

Objets créés

Plusieurs objets de configuration sont créés lorsque la configuration du proxy ADFS est déployée sur l'instance de Citrix ADC. L'image suivante affiche la liste des objets créés.



Objects Added on Instance : 192.168.153.160 | Count : 57

Type : nsfeature

Meta Properties
action : **enable**

feature : cs lb ssl rewrite aaa

Type : lbvserver

ipv46 : 192.50.50.12
name : ns-adfs-dep01-adfs-dns
port : 53
servicetype : DNS

Type : service

ip : 10.30.30.5
name : ns-adfs-dep01-dns-svc-1
port : 53
servicetype : DNS

Type : lbvserver_service_binding

name : ns-adfs-dep01-adfs-dns
servicename : ns-adfs-dep01-dns-svc-1

Type : authenticationnegotiateaction

domain : ADFS.CITRIX.COM
domainuser : nsroot
domainuserpasswd : nsroot
name : ns-adfs-dep01-negotiate-action

Type : authenticationpolicy

action : ns-adfs-dep01-negotiate-action
name : ns-adfs-dep01-negotiate-policy
rule : true

Type : aaakcdaccount

delegateduser : nsroot
kcdaccount : ns-adfs-dep01-adfs-auth401-kcd-
kcdpassword : nsroot
realmstr : ADFS.CITRIX.COM

Type : tmsessionaction

kcdaccount : ns-adfs-dep01-adfs-auth401-kcd-
name : ns-adfs-dep01-adfs-auth401-tmsession-action
persistentcookie : ON
persistentcookievalidity : 3
sso : ON

Type : tmsessionpolicy

action : ns-adfs-dep01-adfs-auth401-tmsession-action
name : ns-adfs-dep01-adfs-auth401-tmsession-policy
rule : ns_true

Type : authenticationvserver

authenticationdomain : ADFS.CITRIX.COM
failedlogintimeout : 1
ipv46 : 192.50.50.40
maxloginattempts : 255
name : ns-adfs-dep01-adfs-auth401-auth-vserver
port : 443
servicetype : SSL

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-adfs-auth401-auth-vserver

Type : authenticationvserver_authenticationpolicy_binding

name : ns-adfs-dep01-adfs-auth401-auth-vserver
policy : ns-adfs-dep01-negotiate-policy
priority : 10

Type : authenticationvserver_tmsessionpolicy_binding

name : ns-adfs-dep01-adfs-auth401-auth-vserver
policy : ns-adfs-dep01-adfs-auth401-tmsession-policy
priority : 10

Type : authenticationldapaction

authentication : ENABLED
authtimeout : 30
followreferrals : OFF
ldapbase : dc=netscaler,dc=com
ldapbinddn : cn=Manager,dc=netscaler,dc=com
ldapbinddnpassword : nsroot
ldaploginname : samAccountname
name : ns-adfs-dep01-ldap-action
passwdchange : DISABLED
sectype : PLAINTEXT
serverip : 10.30.30.3
serverport : 389
ssonameattribute : userPrincipalName
svrtype : AD
validateservercert : NO

Type : authenticationpolicy

action : ns-adfs-dep01-ldap-action
name : ns-adfs-dep01-ldap-policy
rule : true

Type : aaakcdaccount

kcdaccount : ns-adfs-dep01-adfs-ldap-kcd-acc
realmstr : ADFS.CITRIX.COM

Type : tmsessionaction

kcdaccount : ns-adfs-dep01-adfs-ldap-kcd-acc
name : ns-adfs-dep01-adfs-ldap-tmsession-action
persistentcookie : OFF
sso : ON

Type : tmsessionpolicy

action : ns-adfs-dep01-adfs-ldap-tmsession-action
name : ns-adfs-dep01-adfs-ldap-tmsession-policy
rule : ns_true

Type : authenticationvserver

authenticationdomain : ADFS.CITRIX.COM
failedlogintimeout : 1
ipv46 : 192.50.50.30
maxloginattempts : 255
name : ns-adfs-dep01-adfs-ldap-auth-vserver
port : 443
servicetype : SSL

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-adfs-ldap-auth-vserver

Type : authenticationvserver_authenticationpolicy_binding

name : ns-adfs-dep01-adfs-ldap-auth-vserver
policy : ns-adfs-dep01-ldap-policy
priority : 10

Type : authenticationvserver_tmsessionpolicy_binding

name : ns-adfs-dep01-adfs-ldap-auth-vserver
policy : ns-adfs-dep01-adfs-ldap-tmsession-policy
priority : 10

Type : csvserver

ipv46 : 192.50.50.50
name : ns-adfs-dep01-cs
port : 443
servicetype : SSL

Type : lbvserver

ipv46 : 192.50.50.50
name : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb
port : 445
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp

Type : server

ipaddress : 192.30.30.30
name : 192.30.30.30

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol
rule : HTTP.REQ.URL.CONTAINS("/adfs/services/trust") || HTTP.REQ.URL.CONTAINS("/federa

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol
priority : 9800

Type : lbvserver

appflowlog : ENABLED
authentication : ON
authenticationhost : ADFS.CITRIX.COM
authn401 : OFF
authnvsname : ns-adfs-dep01-adfs-ldap-auth-vserver
downstateflush : ENABLED
ipv46 : 192.50.50.50
lbmethod : LEASTCONNECTION
name : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb
port : 446
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-cspol
rule : HTTP.REQ.URL.CONTAINS("/adfs/ls/auth/integrated") || HTTP.REQ.URL.CONTAINS("/adfs/ls/wia")

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-cspol
priority : 9900

Type : lbvserver

appflowlog : ENABLED
authentication : OFF
authn401 : ON
authnvsname : ns-adfs-dep01-adfs-auth401-auth-vserver
downstateflush : ENABLED
ipv46 : 192.50.50.50
lbmethod : LEASTCONNECTION
name : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb
port : 444
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-cspol
rule : true

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-cspol
priority : 10000

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-cs

Type : rewritepolicylabel

labelname : ns-adfs-dep01-request-rewritepolicylabel
transform : HTTP_REQ

Type : rewritepolicylabel

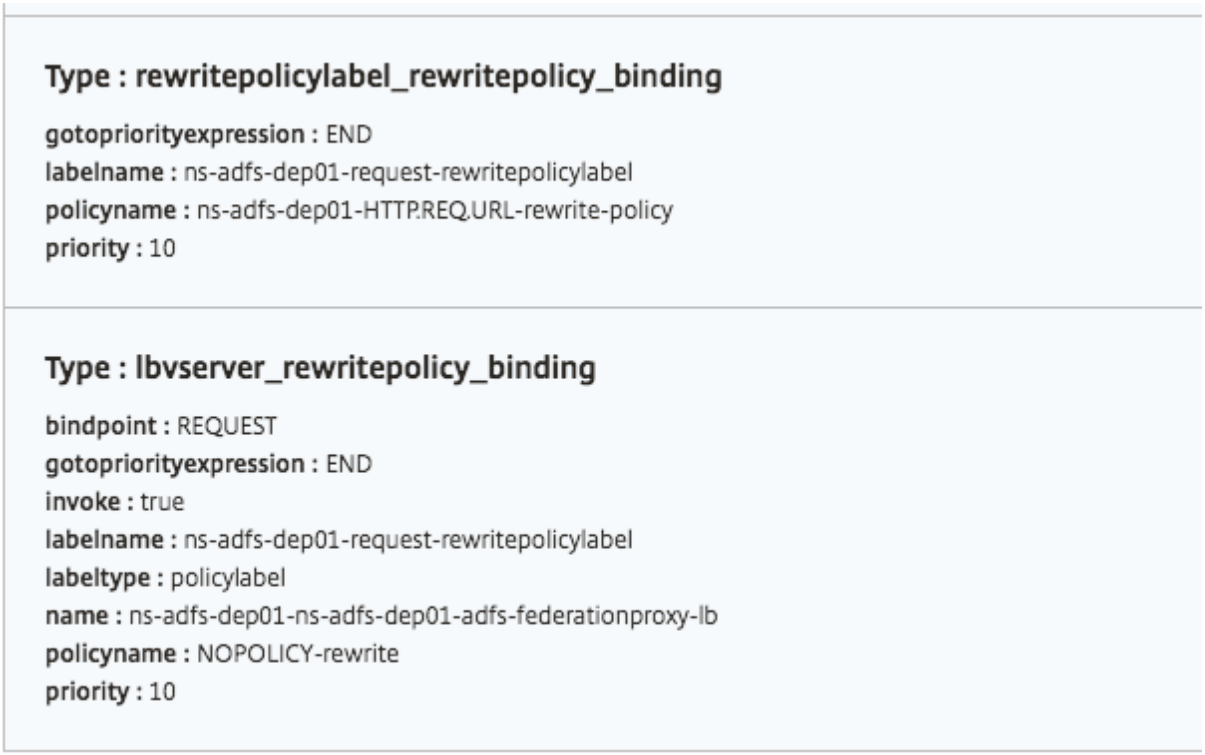
labelname : ns-adfs-dep01-response-rewritepolicylabel
transform : HTTP_RES

Type : rewriteaction

name : ns-adfs-dep01-HTTP.REQ.URL-rewrite-action
stringbuilderexpr : "/adfs/services/trust/proxymex"
target : HTTP.REQ.URL
type : REPLACE

Type : rewritepolicy

action : ns-adfs-dep01-HTTP.REQ.URL-rewrite-action
name : ns-adfs-dep01-HTTP.REQ.URL-rewrite-policy
rule : HTTP.REQ.URL.CONTAINS("/adfs/services/trust") && (!HTTP.REQ.URL.CONTAINS("/trust/proxymex"))



Oracle e-business StyleBook

April 29, 2021

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'augmenter les performances et se compose des applications suivantes.

- progiciel de gestion intégré (PGI)
- Gestion de la relation client (CRM)
- Gestion de la chaîne d'approvisionnement (SCM)

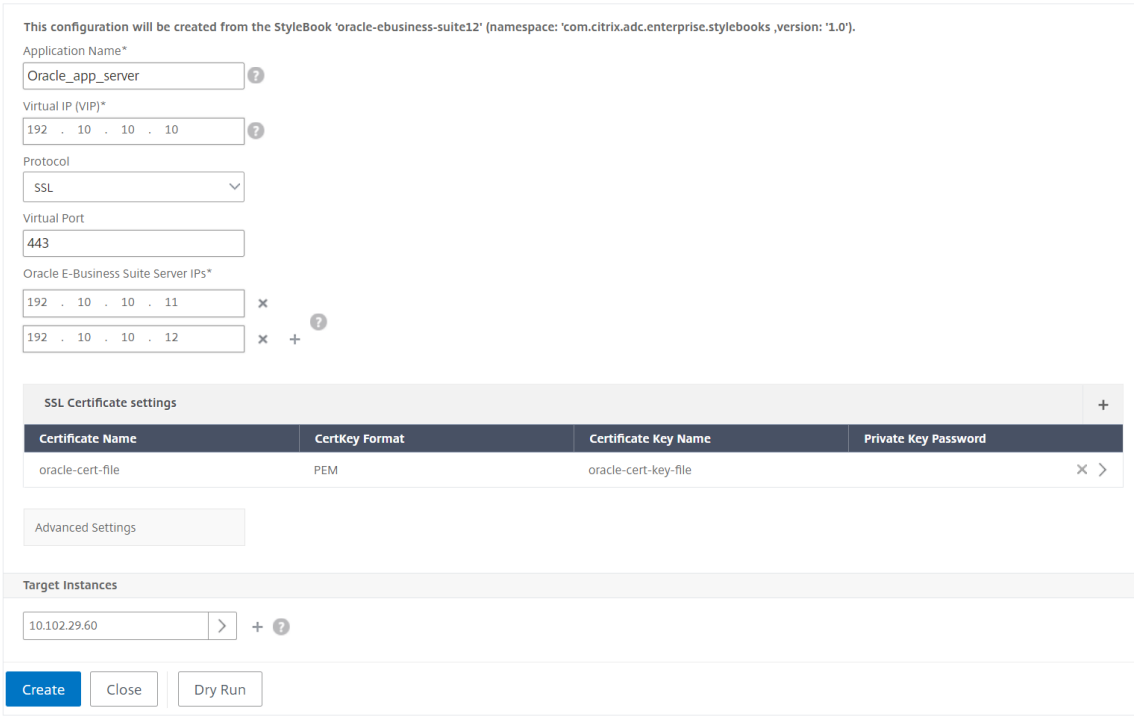
Ces applications informatiques sont développées ou acquises par Oracle. Oracle E-Business Suite 12.2 StyleBook vous permet de déployer la configuration sur les instances Citrix ADC sélectionnées.

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 la communication cryptée 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 la page vers le bas et sélectionnez **Oracle E-Business Suite 12.2**. Vous pouvez également utiliser l'option de recherche pour effectuer une recherche dans StyleBook.
2. Cliquez sur **Créer une configuration** dans le panneau StyleBook.
3. Tapez le nom de l'application d'équilibrage de charge et l'adresse IP virtuelle dans la section Paramètres d'équilibrage de charge.
4. Sélectionnez le protocole requis. Vous avez deux options ici - HTTP et HTTP/SSL. Vous pouvez également taper le numéro de port.
5. Tapez les adresses IP de tous les serveurs d'applications Oracle E-Business Suite du réseau qui doivent être équilibrés de charge. Cliquez sur **+** pour ajouter d'autres adresses IP de serveur.
6. Dans la section **Paramètres des certificats SSL**, sélectionnez les fichiers respectifs de 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 du certificat.

   Sélectionnez l'instance Citrix ADC cible sur laquelle la configuration doit être créée, puis cliquez sur **Créer**.



> **Conseil**
>
> Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter des instances Citrix ADC récemment découvertes dans Citrix ADM à la liste des instances disponibles dans cette fenêtre. L'icône d'actualisation n'est disponible que sur Citrix ADM.

Pare-feu d'application Web StyleBook

April 29, 2021

Citrix Web App Firewall est un pare-feu d'application Web (WAF) qui protège les applications et les sites Web contre les attaques connues et inconnues, y compris toutes les menaces de couche d'application et de jour zéro.

Citrix ADM fournit désormais un StyleBook par défaut qui vous permet de créer plus facilement une configuration de pare-feu d'application sur les instances de Citrix ADC.

Déploiement des configurations de pare-feu d'application

La tâche suivante vous aide à déployer une configuration d'équilibrage de charge avec le pare-feu d'application et la stratégie de réputation IP sur les instances de Citrix ADC dans votre réseau d'entreprise.

Pour créer une configuration LB avec des paramètres de pare-feu d'application :

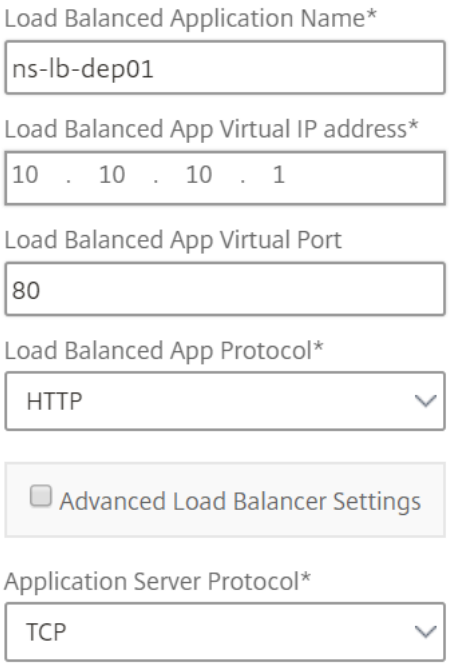
1. Dans Citrix ADM, accédez à **Applications** > **Configurations** > **StyleBooks** . La page StyleBooks affiche tous les StyleBooks disponibles pour votre utilisation dans Citrix ADM. Faites défiler vers le bas et recherchez HTTP/SSL Load Balancing StyleBook avec stratégie de pare-feu d'application et stratégie de réputation IP. Vous pouvez également rechercher le StyleBook en tapant le nom sous la forme `lb-appfw`. Cliquez sur **Créer une configuration**.

   Le StyleBook s'ouvre sous la forme d'une page d'interface utilisateur sur laquelle vous pouvez entrer les valeurs de tous les paramètres définis dans ce StyleBook.

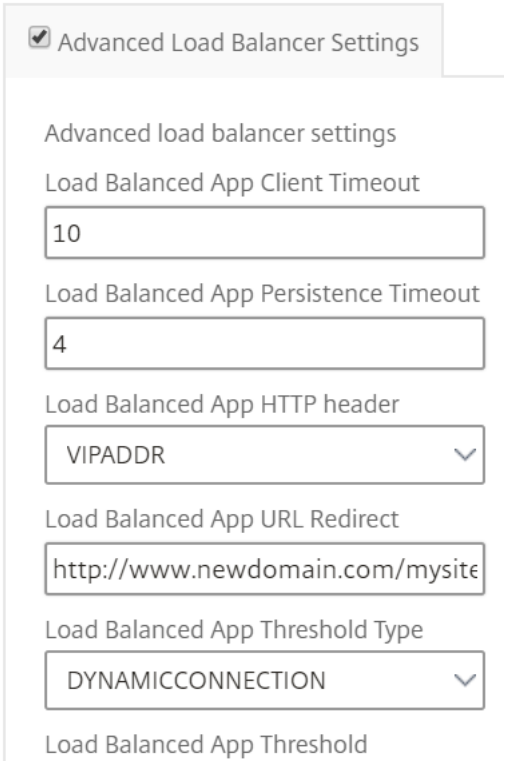
2. Entrez des valeurs pour les paramètres suivants :

   - **Nom de l'application équilibrée de charge**. Nom de la configuration équilibrée de charge avec pare-feu d'application à déployer dans votre réseau.
   - **Adresse IP virtuelle de l'application équilibrée en charge**. Adresse IP virtuelle à laquelle l'instance d'Citrix ADC reçoit les demandes client.
   - **Port virtuel de l'application équilibrée de charge**. Port TCP à utiliser par les utilisateurs pour accéder à l'application équilibrée de charge.

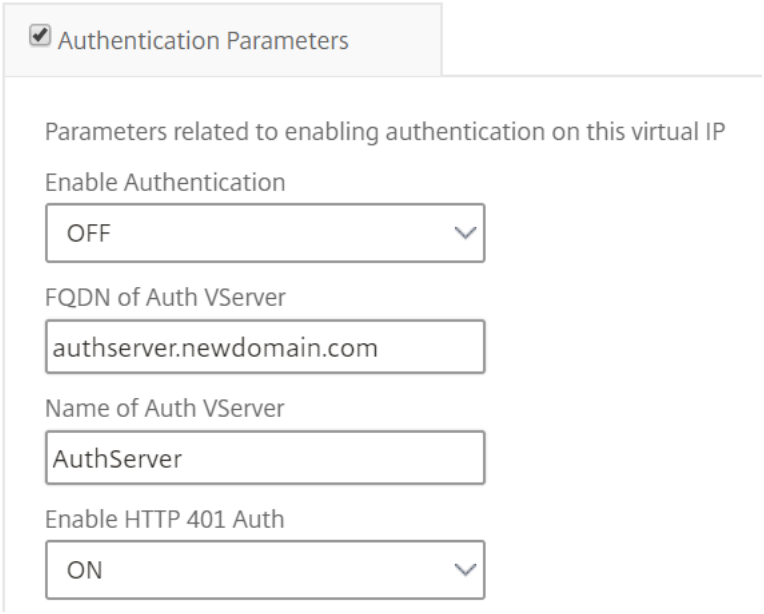
- **Protocole d'application équilibré de charge**. Sélectionnez le protocole frontal dans la liste.
- **Protocole du serveur d'applications**. Sélectionnez le protocole du serveur d'applications.



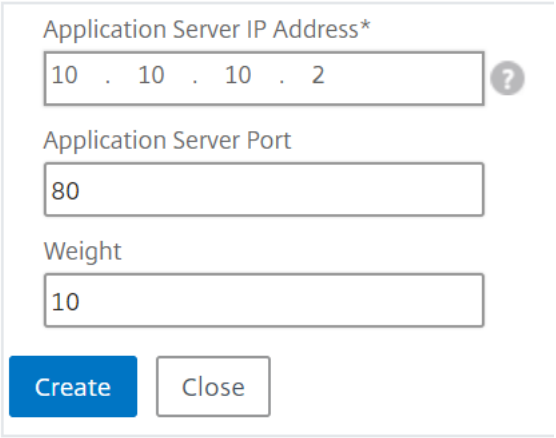
3. En option, vous pouvez activer et configurer les **paramètres avancés d'équilibrage**de charge.



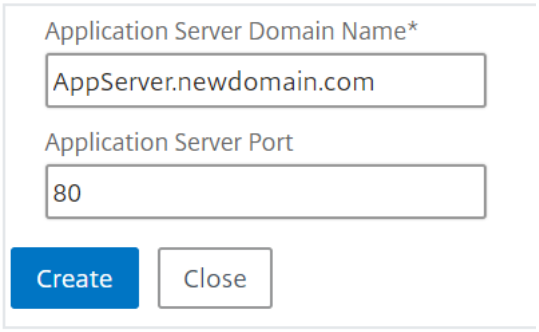
4. Vous pouvez également configurer un serveur d'authentification pour l'authentification du trafic pour le serveur virtuel d'équilibrage de charge.



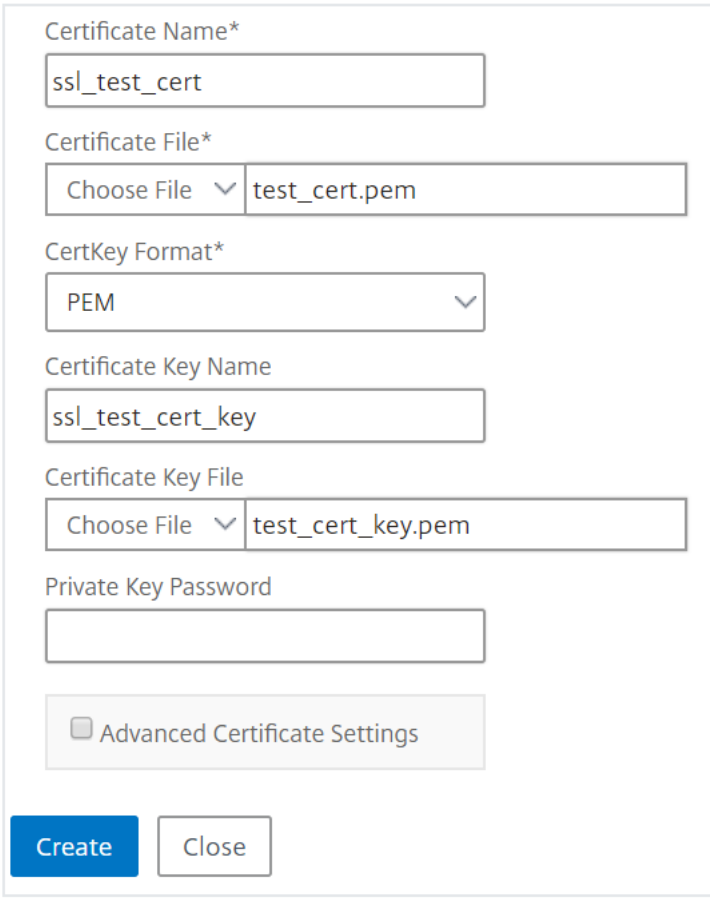
5. Cliquez sur « + » dans la section IP et ports du serveur pour créer des serveurs d'applications et les ports auxquels ils sont accessibles.



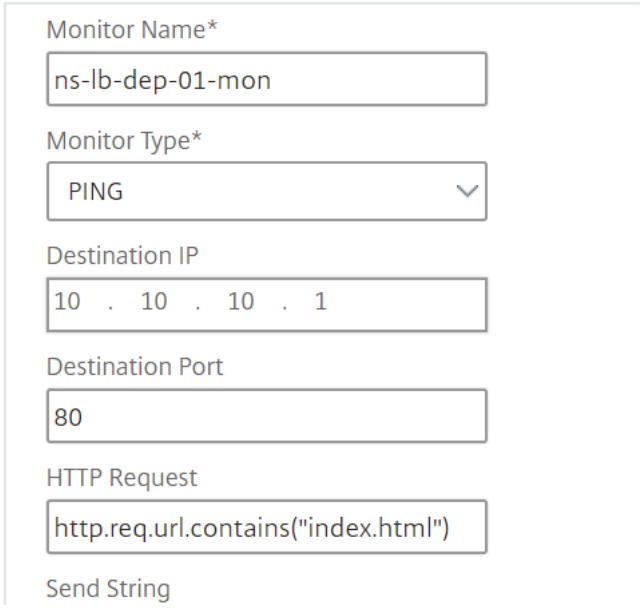
6. Vous pouvez également créer des noms de domaine complet pour les serveurs d'applications.



7. Vous pouvez également spécifier les détails du certificat SSL.

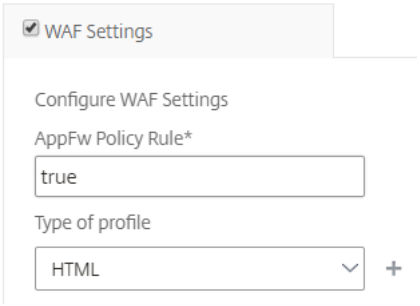


8. Vous pouvez également créer des moniteurs dans l'instance Citrix ADC cible.



9. Pour configurer un pare-feu d'application sur le serveur virtuel, activez les paramètres WAF.

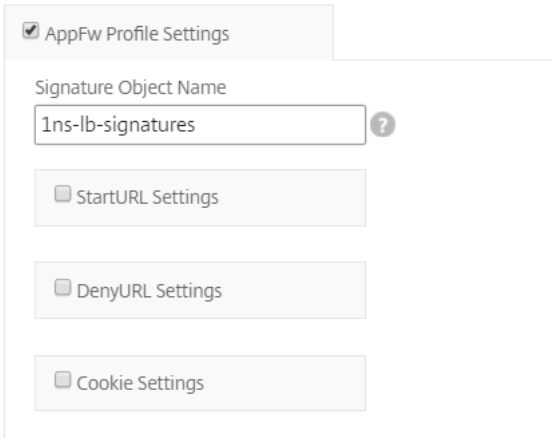
   Assurez-vous que la règle de stratégie de pare-feu d'application est vraie si vous souhaitez appliquer les paramètres du pare-feu de l'application à tout le trafic sur ce VIP. Sinon, spécifiez la règle de stratégie Citrix ADC pour sélectionner un sous-ensemble de demandes auxquelles appliquer les paramètres du pare-feu d'application. Ensuite, sélectionnez le type de profil à appliquer - HTML ou XML.



10. Vous pouvez également configurer des paramètres détaillés de profil de pare-feu d'application en activant la case à cocher Paramètres de profil du pare-feu d'application.
11. Si vous souhaitez configurer les signatures de pare-feu d'application, entrez le nom de l'objet de signature créé sur l'instance de Citrix ADC sur laquelle le serveur virtuel doit être déployé.

    > **Remarque**
    >
    > Vous ne pouvez pas créer un objet de signature à l'aide de ce StyleBook.

12. Ensuite, vous pouvez également configurer d'autres paramètres de profil de pare-feu d'application tels que les paramètres StarTURL, DenyURL et autres.

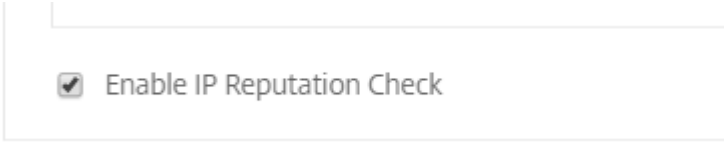


Pour plus d'informations sur le pare-feu d'application et les paramètres de configuration, voir Pare-feu d'application.

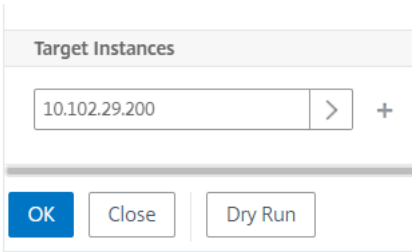
13. Dans la section **Instances cibles**, sélectionnez l'instance Citrix ADC sur laquelle déployer le serveur virtuel d'équilibrage de charge avec le pare-feu d'application.

> **Remarque**
>
> Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter des instances Citrix ADC récemment découvertes dans Citrix ADM à la liste des instances disponibles dans cette fenêtre.

14. Vous pouvez également activer la **vérification de réputation IP** pour identifier l'adresse IP qui envoie des demandes indésirables. Vous pouvez utiliser la liste de réputation IP pour rejeter préventivement les demandes provenant de l'IP avec la mauvaise réputation.



15. Cliquez sur **Créer** pour créer la configuration sur les instances Citrix ADC sélectionnées.

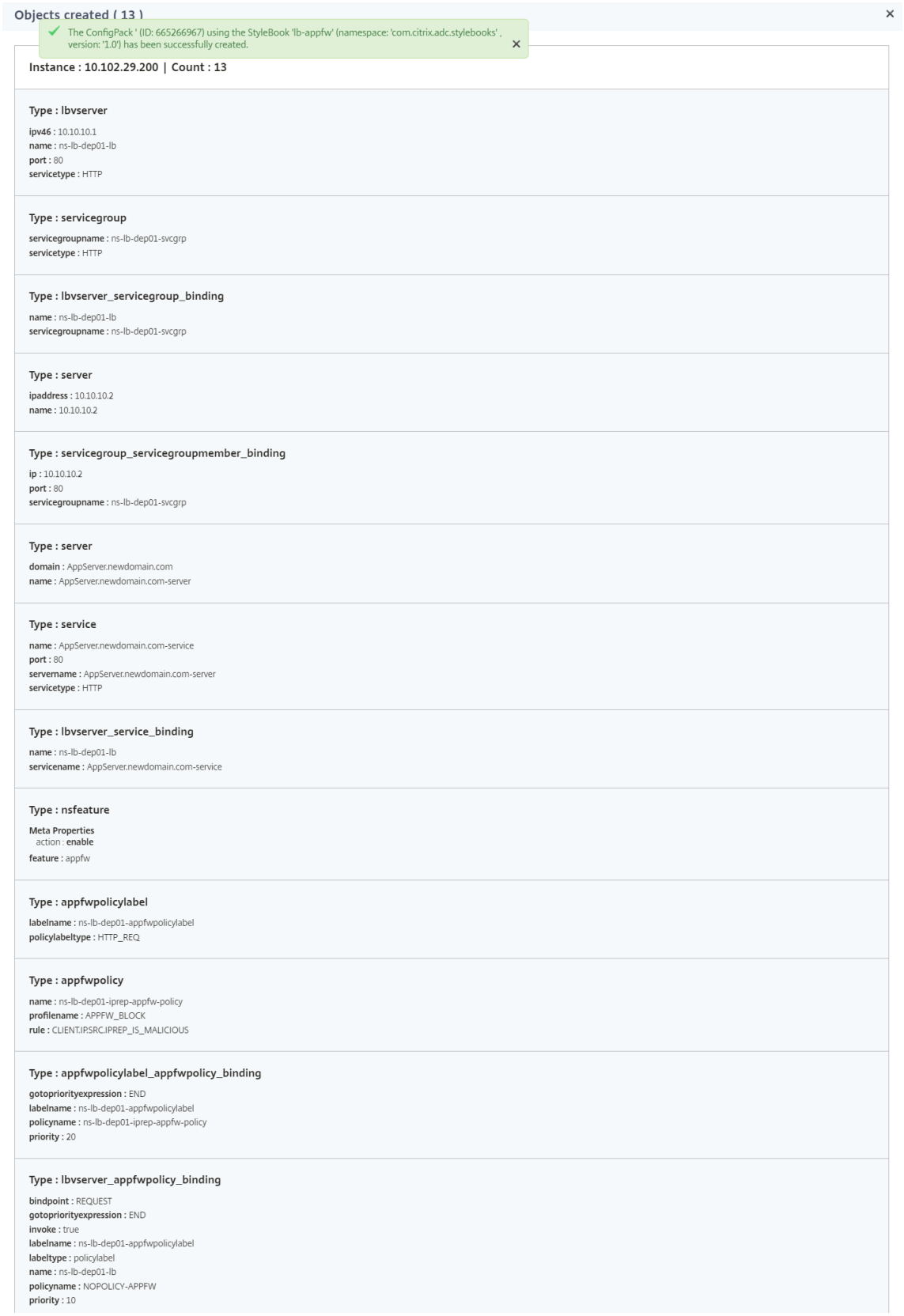


> **Conseil**
>
> Citrix vous recommande de sélectionner Exécuter à sec pour vérifier les objets de configuration qui doivent être créés sur l'instance cible avant d'exécuter la configuration réelle

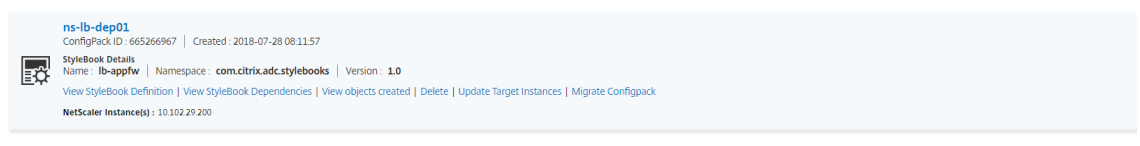
> sur l'instance.

Lorsque la configuration est correctement créée, le StyleBook crée le serveur virtuel d'équilibrage de charge requis, le serveur d'applications, les services, les groupes de services, les étiquettes de pare-feu d'application, les stratégies de pare-feu d'application et les lie au serveur virtuel d'équilibrage de charge.

La figure suivante montre les objets créés sur chaque serveur :



16. Pour afficher le ConfigPack créé sur Citrix ADM, accédez à **Applications** > **Configurations** .



Créer des profils WAF et BOT à l'aide de StyleBook

April 29, 2021

Lorsque vous pouvez sélectionner une stratégie pour une ressource API dans **API Gateway, elle**vous permet de définir les critères de sélection du trafic pour authentifier une demande d'API. En outre, il vous permet de configurer les stratégies de sécurité de l'API sur le trafic de l'API. Pour de plus amples informations, consultez la section Gérer la passerelle API.

Vous pouvez configurer des stratégies WAF et BOT sur une ressource API. Avant de configurer une stratégie, assurez-vous de créer son profil dans Citrix Application Delivery Management (ADM). Utilisez les StyleBooks par défaut suivants pour créer un profil :

- API WAF Détection Stylebook
- API BOT Detection StyleBook

Créer un profil WAF à l'aide du StyleBook

Effectuez les opérations suivantes pour créer un profil WAF :

1. Dans Citrix ADM, accédez à **Applications** > **Configurations** > **StyleBooks**. Recherchez le StyleBook en tapant le nom en tant que `api-waf-profile`. Cliquez sur **Créer une configuration**.

   Le StyleBook s'ouvre en tant que page d'interface utilisateur sur laquelle vous pouvez entrer les valeurs de tous les paramètres définis dans ce StyleBook.

2. Spécifiez les valeurs pour les paramètres suivants :

   - **Nom du profil WAF API** - Nom permettant d'identifier un profil WAF.
   - **Type d'application** : ajoutez des types d'application au profil. Le profil WAF prend en charge les types d'application JSON et XML.

3. Facultatif, activez **Paramètres de sécurité** pour spécifier des vérifications de protection HTTP, JSON ou XML. Vous pouvez également spécifier une URL d'erreur vers le Citrix Web App Firewall. Pour de plus amples informations, consultez la section Création d'un profil Web App Firewall.

4. Sélectionnez l'instance Citrix ADC cible ou le groupe d'instances sur lequel vous souhaitez déployer cette configuration.

5. Cliquez sur **Créer**.

Pour configurer une stratégie WAF, reportez-vous à la section Ajouter des stratégies à un déploiement d'API.

Créer un profil BOT à l'aide du StyleBook

Effectuez les opérations suivantes pour créer un profil BOT :

1. Dans Citrix ADM, accédez à **Applications** > **Configurations** > **StyleBooks**. Recherchez le StyleBook en tapant le nom en tant que `api-bot-profile`. Cliquez sur **Créer une configuration**.

   Le StyleBook s'ouvre en tant que page d'interface utilisateur sur laquelle vous pouvez entrer les valeurs de tous les paramètres définis dans ce StyleBook.

2. Dans **Nom du profil BOT**, spécifiez un nom pour identifier un profil BOT.
3. Facultatif, activez les options suivantes en fonction de vos besoins :
   - **Activer la vérification de la réputation IP** - Cette option identifie l'adresse IP qui envoie des demandes indésirables. Vous pouvez utiliser la liste de réputation IP pour rejeter préventivement les demandes provenant de l'IP avec la mauvaise réputation.
   - **Activer les signatures BOT** - Spécifiez le nom de la signature BOT. Il bloque les requêtes de la signature spécifiée.
   - **Autoriser la liste** - Spécifiez l'adresse IPv4 ou de sous-réseau (CIDR). Cette option permet au profil BOT de contourner les requêtes de l'adresse IPv4 ou de sous-réseau spécifiée.
   - **Refuser List** - Spécifiez l'adresse IPv4 ou de sous-réseau (CIDR). Cette option permet au profil BOT de bloquer les demandes provenant de l'adresse IPv4 ou de sous-réseau spécifiée.
4. Sélectionnez l'instance Citrix ADC cible ou le groupe d'instances sur lequel vous souhaitez déployer cette configuration.
5. Cliquez sur **Créer**.

Pour configurer une stratégie BOT, reportez-vous à la section Ajouter des stratégies à un déploiement d'API.

Créer et utiliser des StyleBooks personnalisés

April 29, 2021

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 renseignements suivants :

Avant de commencer

Avant de commencer à créer StyleBooks, assurez-vous d'avoir connaissance des éléments suivants :

- API NITRO. Pour de plus amples informations, consultez la section Documentation de l'API NITRO.
- YAML

Les fichiers StyleBook utilisent le format YAML. Pour plus d'informations sur le format YAML, reportez-vous à la section Syntaxe YAML.

Voici une liste des instructions YAML dont vous devez tenir compte lors de la création de StyleBooks :

- YAML est sensible à la casse.
- YAML nécessite une indentation appropriée
- Utilisez la touche <spacebar> pour créer une indentation appropriée. N'utilisez pas la clé <tab>. L'utilisation de la clé <tab> crée une erreur de compilation lors de l'importation de votre StyleBook vers MA Service.
- N'utilisez pas de chaînes entre guillemets. Inclure la chaîne entre guillemets uniquement si une chaîne contient des signes de ponctuation (tirets, deux-points, etc.). Si vous souhaitez interpréter un nombre comme une chaîne, incluez le nombre entre guillemets ou utilisez la fonction intégrée str () de StyleBooks.
- Des littéraux comme 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 booléens, et sont équivalents à true et false respectivement. 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 valider 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.

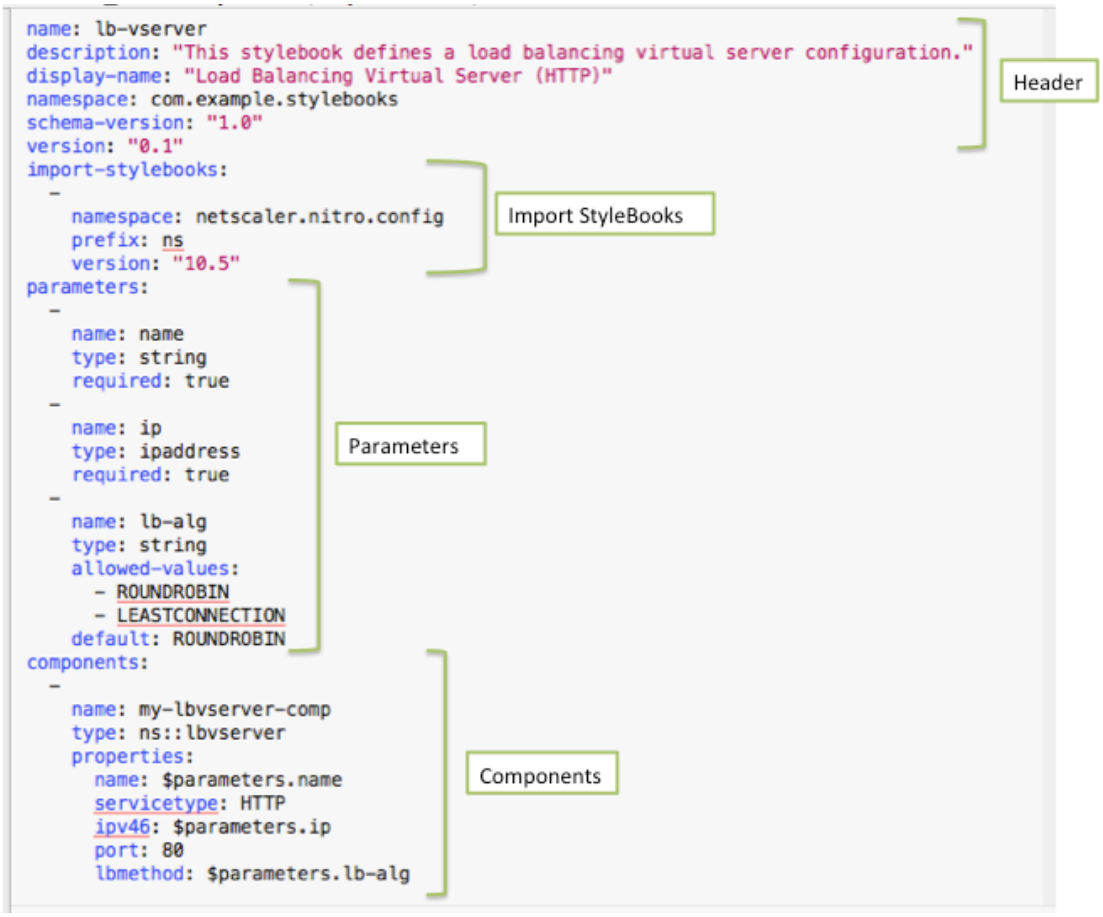
> Lors de la configuration de StyleBooks, vous ne pouvez utiliser que les ressources de configuration NITRO prenant en charge les opérations **Create** and **Delete** (méthodes POST et DELETE HTTP). Pour de plus amples informations, consultez la section Documentation des API NITRO.

Anatomie d'un StyleBook

Pour écrire StyleBooks, vous devez comprendre la grammaire, la syntaxe et la structure de StyleBooks. Un StyleBook typique comporte les sections suivantes :

- **En-tête** : Cette section vous permet de définir l'identité d'un StyleBook et de décrire ce qu'il fait. Il s'agit d'une section obligatoire.
- **Importer StyleBooks** : cette section vous permet de déclarer les autres StyleBook auxquels vous souhaitez faire référence à partir de votre StyleBook actuel. L'importation de la configuration Citrix ADC NITRO StyleBooks ou d'autres StyleBooks est nécessaire 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 prise par votre StyleBook. 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 avoir 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 contenant uniquement une section de composants peut être utilisé lorsque vous souhaitez spécifier les valeurs des attributs dans le StyleBook au lieu de définir des paramètres pour prendre l'entrée de l'utilisateur.
- **Sorties** : alors que la section 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 à d'autres StyleBooks qui importent ce StyleBook. Les utilisateurs et l'importation de StyleBooks peuvent ensuite référencer les propriétés des composants exposés.
- **Opérations** : Un StyleBook peut contenir une section facultative permettant d'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 à l'aide des attributs GUI

StyleBook pour créer un serveur virtuel d'équilibrage de charge

April 29, 2021

Dans cet exemple, vous concevez un StyleBook de base qui crée un serveur virtuel d'équilibrage de charge de type protocole HTTP et écoute sur le port 80. Le nom du serveur virtuel, l'adresse IP et les paramètres de la méthode d'équilibrage de charge acceptent les 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 comprennent la section d'en-tête. Dans cet exemple, la section d'en-tête est écrite comme suit :

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

La section d'en-tête comprend les détails suivants :

- **name** : Un nom pour ce StyleBook.
- **description** : Description définissant ce que fait ce StyleBook. Cette description apparaît sur Citrix Application Delivery Management (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**
>
> Considérez que vous avez mis à jour votre StyleBook et que vous avez un numéro de version mis à jour. Maintenant, si vous faites référence à (c'est-à-dire, si vous importez) ce StyleBook dans d'autres StyleBooks, assurez-vous de mettre à jour le numéro de version dans d'autres StyleBooks aussi, afin qu'ils utilisent la version correcte du StyleBook importé.

Importer StyleBooks

La section après en-tête est appelée "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 reconstruire la même configuration dans votre propre StyleBook.

Dans cet exemple, la section Import-Stylebooks est écrite comme suit :

```
import-stylebooks:
 -
  namespace: netscaler.nitro.config
  prefix: ns
  version: "10.5"
<!--NeedCopy-->
```

Chaque StyleBook doit faire référence à l'espace de noms netscaler.nitro.config s'il utilise directement l'un des objets de configuration NITRO. Cet espace de noms contient tous les types NITRO Citrix ADC, tels que LBVServer.Comme les versions logicielles 10.5 et ultérieures sont prises en charge, vous pouvez utiliser votre StyleBook pour créer et exécuter des configurations sur n'importe quelle instance Citrix ADC exécutant les versions 10.5 et ultérieures.

Le préfixe utilisé dans la section Import-Stylebooks est un raccourci pour faire référence à la combinaison de l'espace de noms et de la version. Dans ce cas, ns se réfère à netscaler.nitro.config de la version 10.5. Dans les sections ultérieures 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 version 10.5 ou ultérieure, Citrix recommande d'importer l'espace de noms NITRO 10.5 dans vos StyleBooks qui utilisent directement les StyleBooks intégrés NITRO (espace de noms : netscaler.nitro.config, version : 10.5).

Il est important qu'un StyleBook qui importe d'autres StyleBooks doit être basé sur une version NITRO qui est identique ou supérieure à celle des StyleBooks qu'il importe. Par exemple, un StyleBook basé sur NITRO version 10.5 ne peut pas dépendre, utiliser ou importer un StyleBook basé sur la version 11.1. 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 des composants NITRO, mais peut importer (dépendre) StyleBooks qui définit 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, il est utilisé pour configurer Citrix ADC qui sont de cette version ou supérieure.

Paramètres

La section paramètres vous permet de déclarer tous les paramètres dont vous avez besoin dans votre StyleBook. En tant que développeur de StyleBook, vous devez décider quelle est l'entrée que vous souhaitez spécifier par les utilisateurs de votre StyleBook. Dans cet exemple, vous avez créé votre StyleBook d'une manière qui exige que ses utilisateurs fournissent le nom du serveur virtuel, son adresse IP et la méthode d'équilibrage de charge.

La section des paramètres se présenterait comme suit :

```
parameters:
 -
  name: name
  label: "Application Name"
  description: "Give a name to the application configuration."
  type: string
  required: true
 -
  name: vip-ipaddress
  label: "Load Balancer IP Address"
  description: "The Application VIP that clients access"
  type: ipaddress
  required: true
 -
  name: lb-alg
  label: LB Algorithm
  description: Load Balancing Algorithm
  type: string
  default: ROUNDROBIN
  allowed-values:
   - ROUNDROBIN
   - LEAST-CONNECTION
<!--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 de **nom** - **nom** pour le nom du serveur virtuel, **ip** pour l'adresse IP du serveur virtuel et **lb-alg** pour la méthode d'équilibrage de charge.

- **fait référence au type de valeur que ces paramètres peuvent prendre.** Par exemple, nom et `lb-alg` peut 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 :
- **string** : Un tableau de caractères. Si aucune longueur n'est spécifiée, la valeur de chaîne peut prendre n'importe quel nombre de caractères. Toutefois, vous pouvez limiter la longueur d'un type de chaîne en utilisant les attributs min-length et max-length.
- **number** : nombre entier. Vous pouvez spécifier le nombre minimum et maximum que ce type peut prendre à l'aide des 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** : valeur de chaîne opaque/secrète. Lorsque Citrix ADM affiche une valeur pour ce paramètre, elle est affichée sous forme d'astérisques (*****).
- **certfile : fichier**de certificat.
- **keyfile : fichier**de clé privée de certificat.
- **file** : un paramètre de ce type nécessite que l'utilisateur télécharge un fichier, par exemple un certificat ou un fichier de clé.
- **objet** : Se compose de plusieurs éléments et chacun de ces éléments est un paramètre. Ce type peut être utilisé pour regrouper plusieurs paramètres liés sous un seul paramètre parent.
- **required** : 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, **name** et **ip** sont des paramètres obligatoires tandis que **lb-alg** est un paramètre facultatif dont la valeur par défaut est « ROUNDROBIN. »

Utilisez l'attribut **par défaut** 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. 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 le nom et l'adresse IP permettent de `ipaddress` saisir la chaîne et le type de valeur, et le `lb-alg` champ est affiché sous la forme d'une liste déroulante avec ROUNDROBIN sélectionné comme valeur par défaut.

> **Remarque**
>
> En plus des types intégrés, un paramètre peut avoir un autre StyleBook comme type. Ceci 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 :

```
components:
 -
  name: lbvserver-comp
  description: This StyleBook component (a Builtin Nitro StyleBook)
     builds a Citrix ADC lbvserver configuration object.
  type: ns::lbvserver
  properties:
   name: $parameters.name
   ipv46: $parameters.vip-ipaddress
   lbmethod: $parameters.lb-alg
   servicetype: HTTP
   port: 80
<!--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 que ce composant fournit. Les composants sont de deux types :

- **Type intégré** : Ce type est fourni par le système et vous n'avez pas besoin de le définir, par exemple, les types d'entité 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 dansCréer un StyleBook composite.

Dans cet exemple, vous avez défini un composant appelé **lbvserver-comp**. Ce composant est de 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 aviez 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 `lbvserver` ressource. Pour en savoir plus sur toutes les ressources Citrix ADC NITRO disponibles et leurs attributs, consultez la section Documentation de l'API REST Citrix ADC NITRO.

Les propriétés de cette section incluent les attributs obligatoires de la `lbvserver` ressource et vous

permettent de spécifier des valeurs pour ces attributs. Dans cet exemple, vous spécifiez des valeurs statiques pour `servicetype` et port tandis que le nom, ipv46 et les `lbmethod` propriétés 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, réunissez-les pour créer votre premier StyleBook. Copiez et collez le contenu de StyleBook dans un éditeur de texte, puis enregistrez le fichier sous **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."
```



```
    type: string
    required: true
  -
    name: vip-ipaddress
    label: "Load Balancer IP Address"
    description: "The Application VIP that clients access"
    type: ipaddress
    required: true
  -
    name: lb-alg
    label: LB Algorithm
    description: Load Balancing Algorithm
    type: string
    default: ROUNDROBIN
    allowed-values:
      - ROUNDROBIN
      - LEAST-CONNECTION

components:
  -
    name: lbvserver-comp
    description: This StyleBook component (a Builtin Nitro StyleBook)
       builds a Citrix ADC lbvserver configuration object.
    type: ns::lbvserver
    properties:
      name: $parameters.name
      ipv46: $parameters.vip-ipaddress
      lbmethod: $parameters.lb-alg
      servicetype: HTTP
      port: 80
<!--NeedCopy-->
```

Pour commencer à utiliser votre StyleBook pour créer des configurations, vous devez l'importer dans Citrix ADM, puis l'utiliser. Pour de plus amples informations, consultez la section Procédure d'utilisation de 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

April 29, 2021

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 nom différent, puis le mettre à jour pour inclure des paramètres et des composants supplémentaires pour une configuration d'équilibrage de charge de base. Enregistrez ce fichier StyleBook en tant que **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 construire 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 l'équilibrage de charge du serveur virtuel StyleBook. Dans la section d'en-tête, changez la valeur du **nom** en basic-lb-config. En outre, mettez à jour la **description** et **le nom d'affichage** pour décrire ce StyleBook de manière appropriée. Vous n'avez pas à modifier les valeurs de l' **espace de noms** et de **la version** . Comme vous avez modifié le nom, la combinaison du nom, de l'espace de noms et de la version crée un identifiant unique pour ce StyleBook dans le système.

```
name: basic-lb-config
namespace: com.example.stylebooks
version: "0.1"
display-name: Load Balancing Configuration
description: This StyleBook defines a simple load balancing
   configuration.
schema-version: "1.0"
<!--NeedCopy-->
```

Importer StyleBooks

La section import-stylebooks reste la même. Il fait référence à l'espace de noms netscaler.nitro.config pour utiliser les objets de configuration NITRO.

```
import-stylebooks:
 -
 namespace: netscaler.nitro.config
 prefix: ns
```



```
 version: "10.5"
<!--NeedCopy-->
```

Paramètres

Vous devez mettre à jour la section des paramètres pour ajouter deux paramètres supplémentaires pour définir la liste des services ou serveurs et le port sur lequel les services écoutent. Les trois premiers paramètres `nameip`, et `lb-alg` restent les mêmes.

```
parameters:
 -
  name: name
  type: string
  label: Application Name
  description: Give a name to the application configuration.
  required: true
 -
  name: ip
  type: ipaddress
  label: Application Virtual IP (VIP)
  description: The Application VIP that clients access
  required: true
 -
  name: lb-alg
  type: string
  label: LoadBalancing Algorithm
  description: Choose the loadbalancing algorithm (method) used for
     loadbalancing client requests between the application servers.
  allowed-values:
     - ROUNDROBIN
     - LEASTCONNECTION
  default: ROUNDROBIN
 -
  name: svc-servers
  type: ipaddress[]
  label: Application Server IPs
  description: The IP addresses of all the servers of this application
  required: true
 -
  name: svc-port
  type: tcp-port
  label: Server Port
  description: The TCP port open on the application servers to receive
     requests.
```



```
    default: 80
<!--NeedCopy-->
```

Dans cet exemple, le paramètre **svc-servers** est ajouté pour accepter une liste d'adresses IP des services qui représentent les serveurs back-end 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 `svc-port` le paramètre, s'il n'est pas spécifié par l'utilisateur.

Composants

Vous devez également mettre à jour la section Composants pour définir des composants supplémentaires de sorte qu'ils utilisent les deux nouveaux paramètres et construisent la configuration complète d'équilibrage de charge.

Pour cet exemple, vous devez écrire la section des composants comme suit :

```
components:
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name + "-lb"
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg

components:
 -
  name: svcg-comp
  type: ns::servicegroup
  properties:
   name: $parameters.name + "-svcgrp"
   servicetype: HTTP

components:
 -
  name: lbvserver-svg-binding-comp
  type: ns::lbvserver_servicegroup_binding
  properties:
   name: $parent.parent.properties.name
   servicegroupname: $parent.properties.name
 -
```



```
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) a maintenant un composant enfant appelé **svcg-comp** . Et, le composant **svcg-comp** a deux composants enfants à l'intérieur. L'imbrication d'un composant dans un autre composant permet au composant imbriqué de créer des objets de configuration en faisant référence 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 à l'aide des valeurs fournies pour les attributs de la ressource `servicegroup`. Dans cet exemple, vous spécifiez une valeur statique pour `servicetype`, 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**.

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 **répét-item**) du groupe de services, et il définit l'attribut **ip** dans chaque Objet de configuration NITRO à l'adresse IP du serveur correspondant.

En règle générale, vous pouvez utiliser les constructions de **répétitionet d'élément**répété dans un composant pour que ce composant génère plusieurs objets de configuration du même type. Vous

pouvez attribuer un nom de variable à la construction d'**élément répété**, par exemple `srv`, pour désigner la valeur actuelle dans l'itération. Ce nom de variable est mentionné 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 la seule façon de construire la configuration. Vous pouvez obtenir le même résultat sans imbrication, comme indiqué ci-dessous :

```
components:
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name + "-lb"
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg
 -
  name: svcg-comp
  type: ns::servicegroup
  properties:
    servicegroupname: $parameters.name + "-svcgrp"
    servicetype: HTTP
 -
  name: lbvserver-svg-binding-comp
  type: ns::lbvserver_servicegroup_binding
  properties:
   name: $components.lbvserver-comp.properties.name
   servicegroupname: $components.svcg-comp.properties.servicegroupname
 -
  name: members-svcg-comp
  type: ns::servicegroup_servicegroupmember_binding
  repeat: $parameters.svc-servers
  repeat-item: srv
  properties:
   ip: $srv
   port: 80
   servicegroupname: $components.svcg-comp.properties.servicegroupname
<!--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'affecte pas l'ordre de création des objets de configuration. Dans cet exemple, les composants **svcg-comp** et **lbvserver-comp**, même s'ils sont déclarés en dernier, doivent être construits avant de construire le deuxième composant **lbvserver-svg-binding-comp**, car il existe des références vers ces composants dans le second composant.

> **Remarque**
>
> Par convention, les noms de StyleBooks, paramètres, substitutions, composants et sorties sont en minuscules. Lorsqu'ils contiennent plusieurs mots, ils sont séparés par un caractère « - ». Par exemple `lb-bindings`, `app-name`, `rewrite-config`, et ainsi de suite. Une autre convention consiste à suffixe les noms de composants avec `-comp` une chaîne.

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 sorties pour exposer les objets `servicegroup` de configuration `lbvserver` et qui seraient créés par ce StyleBook.

```
1  outputs:
2  -
3    name: lbvserver-comp
4    value: $components.lbvserver-comp
5    description: The component that builds the Nitro lbvserver
        configuration object
6  -
7    name: servicegroup-comp
8    value: $components.svcg-comp
9    description: The component that builds the Nitro servicegroup
        configuration object
10 <!--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 en tant que sorties, il permet à tous les StyleBooks qui importent ce StyleBook plus de flexibilité comme vous pouvez le voir lors de la création d'un StyleBook composite.

> **Remarque**
>
> Il est recommandé d'exposer un composant entier du StyleBook dans la section sorties, plutôt qu'une seule propriété d'un composant (par exemple, exposer l'ensemble

> $components.lbvserver-comp plutôt que seulement le nom $components.lbvserver-comp.properties.name). Ajoutez également une description à la sortie expliquant ce que représente la sortie spécifique.

Créez votre StyleBook

Maintenant que vous avez défini toutes les sections requises de ce StyleBook, réunissez-les pour construire votre deuxième StyleBook. Vous avez déjà enregistré ce fichier StyleBook en tant que **basic-lb-config.yaml**. Citrix vous recommande d'utiliser le validateur YAML intégré dans StyleBooks pour valider et importer le contenu YAML.

Le contenu complet du fichier **basic-lb-config.yaml** est reproduit ci-dessous :

```
name: basic-lb-config
namespace: com.example.stylebooks
version: "0.1"
display-name: Load Balancing Configuration
description: This StyleBook defines a simple load balancing
   configuration.
schema-version: "1.0"

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  version: "10.5"
  prefix: ns
parameters:
 -
  name: name
  type: string
  label: Application Name
  description: Give a name to the application configuration.
  required: true
 -
  name: ip
  type: ipaddress
  label: Application Virtual IP (VIP)
  description: The Application VIP that clients access
  required: true
 -
  name: lb-alg
  type: string
  label: LoadBalancing Algorithm
  description: Choose the loadbalancing algorithm (method) used for
     loadbalancing client requests between the application servers.
  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      name: svc-port
43      type: tcp-port
44      label: Server Port
45      description: The TCP port open on the application servers to receive
           requests.
46      default: 80
47
48  components:
49    -
50      name: lbvserver-comp
51      type: ns::lbvserver
52      properties:
53        name: $parameters.name + "-lb"
54        servicetype: HTTP
55        ipv46: $parameters.ip
56        port: 80
57        lbmethod: $parameters.lb-alg
58    -
59      name: svcg-comp
60      type: ns::servicegroup
61      properties:
62        servicegroupname: $parameters.name + "-svcgrp"
63        servicetype: HTTP
64    -
65      name: lbvserver-svg-binding-comp
66      type: ns::lbvserver_servicegroup_binding
67      properties:
68        name: $components.lbvserver-comp.properties.name
69        servicegroupname: $components.svcg-comp.properties.servicegroupname
70    -
71      name: members-svcg-comp
72      type: ns::servicegroup_servicegroupmember_binding
73      repeat: $parameters.svc-servers
74      repeat-item: srv
75      properties:
```



```
76     ip: $srv
77     port: 80
78     servicegroupname: $components.svcg-comp.properties.servicegroupname
79
80 outputs:
81 -
82   name: lbvserver-comp
83   value: $components.lbvserver-comp
84   description: The component that builds the Nitro lbvserver
        configuration object
85 -
86   name: servicegroup-comp
87   value: $components.svcg-comp
88   description: The component that builds the Nitro servicegroup
        configuration object
89 <!--NeedCopy-->
```

Pour commencer à utiliser votre StyleBook pour créer des configurations, vous devez l'importer dans Citrix ADM, puis l'utiliser. Pour de plus amples informations, consultez la section Procédure d'utilisation de 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

April 29, 2021

Une caractéristique importante et puissante de StyleBooks est qu'ils peuvent être utilisés comme blocs de construction pour d'autres StyleBooks. Un StyleBook peut être importé dans un autre StyleBook et peut être désigné comme un **type** utilisé par les composants du second StyleBook similaire à un StyleBook intégré NITRO.

Par exemple, vous pouvez utiliser le **Basic-lb-config** StyleBook que vous avez créé dans la section précédente, pour créer un autre StyleBook appelé **composite-example** . Pour utiliser le « basic-lb-config » StyleBook, vous devez l'importer dans le nouveau StyleBook dans la section Import-Stylebooks.

Créez votre StyleBook

Le nouveau StyleBook se présente comme suit :


```
name: composite-example
namespace: com.example.stylebooks
version: "0.1"
display-name: Load Balancing Virtual Server (HTTP/RoundRobin)
description: This StyleBook defines a RoundRobin load balancing
   configuration with a monitor.
schema-version: "1.0"
import-stylebooks:
  -
   namespace: netscaler.nitro.config
   version: "10.5"
   prefix: ns
  -
   namespace: com.example.stylebooks
   version: "0.1"
   prefix: stlb
parameters:
  -
    name: name
    type: string
    label: Application Name
    description: Give a name to the application configuration.
    required: true
  -
    name: ip
    type: ipaddress
    label: Application Virtual IP (VIP)
    description: The Application VIP that clients access
    required: true
  -
    name: svc-servers
    type: ipaddress[]
    label: Application Server IPs
    description: The IP addresses of all the servers of this
       application
    required: true

  -
    name: response-code
    type: string[]
    label: List of Response Codes
    description: List of Response Codes - Provide a list of response
       codes in integer.

```



```
components:
  -
    name: basic-lb-comp
    type: stlb::basic-lb-config
    description: This component's type is another StyleBook that builds
        the NetScaler lbvserver, servicegroups and services
       configuration objects.
    properties:
     name: $parameters.name
     ip: $parameters.ip
     svc-servers: $parameters.svc-servers
  -
     name: monit-comp
     type: ns::lbmonitor
     description: This component is a basic Nitro type (a Builtin
        StyleBook) that builds the NetScaler monitor configuration
        object.
     properties:
       monitorname: $parameters.name + "-mon"
       type: HTTP
       respcode: $parameters.response-code
       httprequest: "'GET /'"
       lrtm: ENABLED
       secure: "YES"

     components:
        -
          name: monit-svcgrp-bind-comp
          type: ns::servicegroup_lbmonitor_binding
          properties:
            servicegroupname: $components.basic-lb-comp.outputs.
               servicegroup-comp.properties.servicegroupname
            monitor_name: $parent.properties.monitorname
<!--NeedCopy-->
```

Dans la section import-stylebooks, vous importez le styleBook basic-lb-config à l'aide de son espace de noms et de sa version, auxquels il est fait référence avec 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[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 cependant utiliser n'importe quel paramètre du StyleBook (obligatoire et facultatif). Au lieu de re-créer un `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 dispose également d'un sous-composant `monit-svcgrp-bind-comp` pour créer l'objet de configuration de liaison qui lie le moniteur à l' `servicegroup` créé dans le premier composant. Étant donné que le `servicegroup` composant créé dans le « basic-lb-config » StyleBook est exposé comme une sortie, ce StyleBook peut y accéder en utilisant 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 de StyleBook dans un éditeur de texte, puis enregistrez le fichier sous **composite-example.yaml**. Assurez-vous de valider le contenu YAML avant d'importer le fichier dans Citrix ADM. Importez-le ensuite 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

April 29, 2021

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 pour le paramètre à l'aide de l'attribut label et ajouter une info-bulle pour ce paramètre à l'aide de l'attribut description.

```
name: ip
label: Virtual Server IP Address
description: IP address of the virtual server that represents the load
   balanced application.
type: ipaddress
required: true
<!--NeedCopy-->
```

Exemple : Si vous avez un paramètre de type object, vous pouvez définir la mise en page à l'aide de l'attribut **gui**. Dans cet exemple, la mise en page est un objet pliable où les champs sont affichés en deux colonnes.


```
name: svcg-advanced
label: Advanced Application Server Settings
type: object
required: false
gui:
 collapse_pane: true
 columns: 2
<!--NeedCopy-->
```

Exemple. Vous pouvez également afficher une vue récapitulative d'un paramètre d'objet type[] (liste d'objets) sous la forme d'une table avec les paramètres internes représentant les colonnes. Pour inclure ou exclure un paramètre interne de la vue récapitulative, vous pouvez utiliser l' `summary_display` attribut dans la `gui` section comme suit :

```
name: settings
label: Settings
type: object[]
parameters:
  -
    name: name
    label: Name
    description: Name of this setting
    type: string
    gui:
      summary_display: true
<!--NeedCopy-->
```

Exemple : certains StyleBooks sur Citrix ADM sont utilisés uniquement comme blocs de construction pour d'autres StyleBooks. Et, vous pouvez 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 utilisateur graphique Citrix ADM.

```
name: basic-lb-config
namespace: com.example.stylebooks
version: "0.1"
display-name: Load Balancing Configuration
description: This StyleBook defines a simple load balancing
   configuration.
schema-version: "1.0"
<!--NeedCopy-->
```


Importer des StyleBooks personnalisés

April 29, 2021

Après avoir créé votre StyleBook, vous devez l'importer dans Citrix Application Delivery Management (ADM) pour l'utiliser. Citrix ADM vous permet d'importer un seul StyleBook sous forme YAML ou plusieurs fichiers YAML StyleBook sous forme de bundle sous forme de .zip, .tgz ou .gz. Le système Citrix ADM valide vos StyleBooks lors de l'importation. Le StyleBook est maintenant prêt à être utilisé pour créer des configurations.

Citrix ADM dispose également d'un éditeur YAML intégré que vous pouvez utiliser pour composer le contenu de StyleBook YAML. L'éditeur YAML vous permet de valider vos constructions YAML à partir de l'interface graphique Citrix ADM elle-même. Vous n'avez pas besoin d'utiliser un outil distinct pour ces vérifications de validation. Le contenu est validé par rapport aux normes YAML et toute déviation est mise en évidence. Vous pouvez ensuite corriger le contenu et tenter d'importer le StyleBook dans Citrix ADM. L'éditeur YAML intégré offre deux avantages lors de l'écriture de votre propre StyleBook.

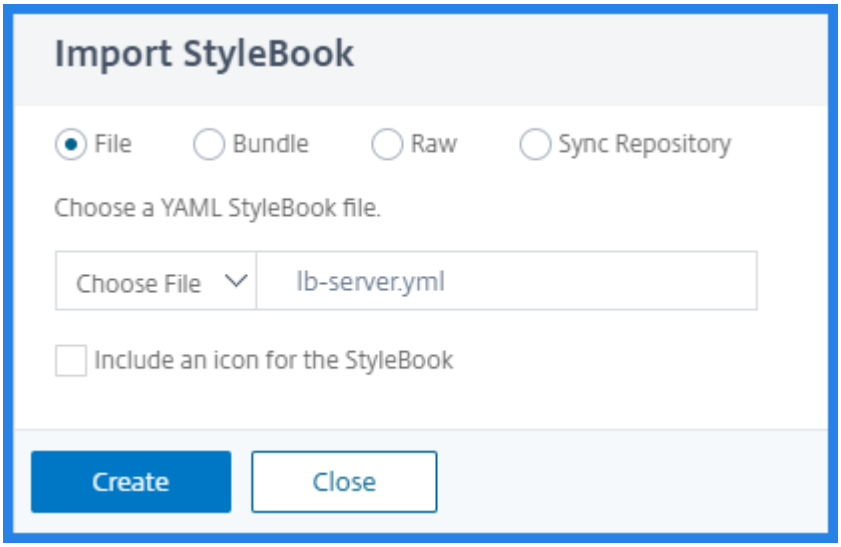
- **Code couleur**. L'éditeur affiche le contenu StyleBook analysé selon les directives YAML, et le codage couleur vous aide à différencier facilement entre les clés et les valeurs définies dans le contenu YAML.
- **Validation YAML**. Le contenu est validé pour toute erreur YAML lorsque vous tapez et toute déviation est immédiatement mise en surbrillance. Cette validation vous permet d'écrire du texte conforme aux directives YAML avant même d'importer le StyleBook dans Citrix ADM.

> **Remarque**
>
> Actuellement, l'éditeur valide le contenu selon les directives de YAML. Il ne valide pas l'exactitude du code et les erreurs typographiques.

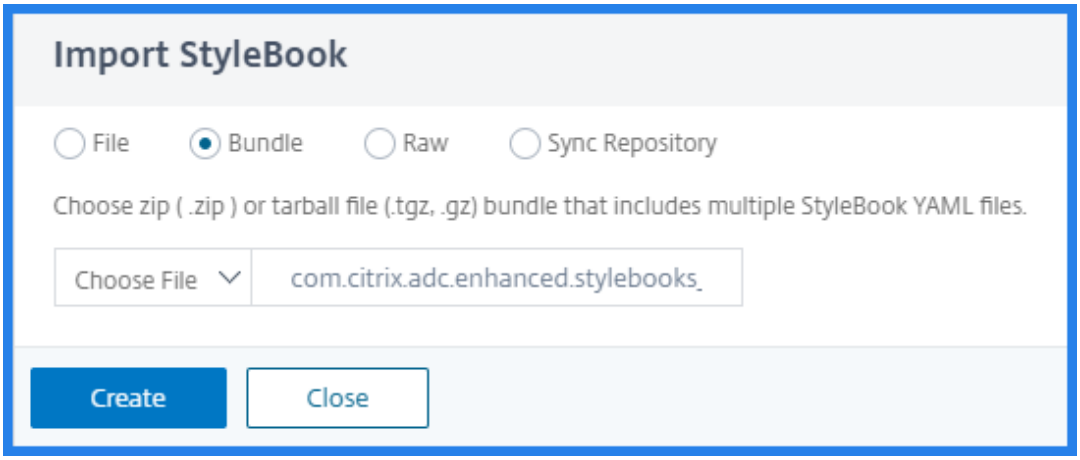
Pour importer votre StyleBook

1. Dans Citrix ADM, accédez à **Applications** > **Configuration** > **StyleBooks**, puis cliquez sur **Importer un nouveau StyleBook** .
2. Cliquez sur l'une des options suivantes pour importer un StyleBook.
   - **Fichier** : sélectionnez le fichier requis ou l'ensemble de fichiers à partir de votre stockage local.

     > **Remarque**
     >
     > Dans cet exemple, importez le `lb-vserver.yml` StyleBook dans lequel vous avez créé StyleBook pour créer un serveur virtuel d'équilibrage de charge.



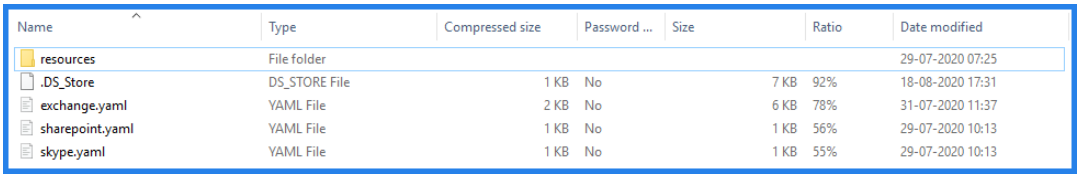
- **Bundle** - Citrix ADM vous permet d'importer plusieurs StyleBooks au format YAML. Vous pouvez importer plusieurs fichiers YAML StyleBook compressés au format zip (.zip) ou tar-ball (.tgz, .gz).



Vous pouvez désormais inclure des icônes à chaque StyleBook de l'offre groupée. Pour ce faire, téléchargez les icônes et le `icon_mapping.json` fichier `resources` dans le dossier. Si le nom du fichier d'icône et le nom de StyleBook correspondent, les icônes sont automatiquement mappées aux StyleBooks. Sinon, mappez StyleBooks et icônes dans le `icon_mapping.json` fichier comme suit :

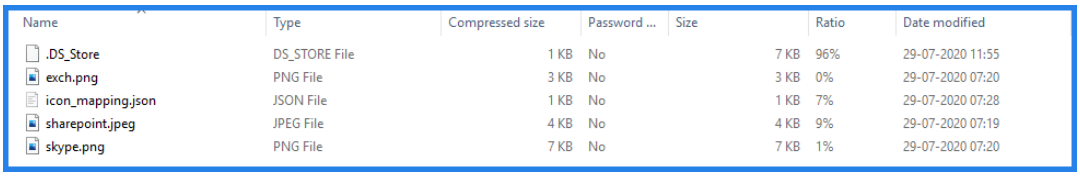
```
<StyleBook file name> : <icon file name>
<!--NeedCopy-->
```

Voici un exemple de pack StyleBook :



Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
resources	File folder					29-07-2020 07:25
.DS_Store	DS_STORE File	1 KB	No	7 KB	92%	18-08-2020 17:31
exchange.yaml	YAML File	2 KB	No	6 KB	78%	31-07-2020 11:37
sharepoint.yaml	YAML File	1 KB	No	1 KB	56%	29-07-2020 10:13
skype.yaml	YAML File	1 KB	No	1 KB	55%	29-07-2020 10:13

Le `resources` dossier contient les icônes requises.



Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
.DS_Store	DS_STORE File	1 KB	No	7 KB	96%	29-07-2020 11:55
exch.png	PNG File	3 KB	No	3 KB	0%	29-07-2020 07:20
icon_mapping.json	JSON File	1 KB	No	1 KB	7%	29-07-2020 07:28
sharepoint.jpeg	JPEG File	4 KB	No	4 KB	9%	29-07-2020 07:19
skype.png	PNG File	7 KB	No	7 KB	1%	29-07-2020 07:20

Dans cet exemple, `sharepoint.yaml` et `skype.yaml` les fichiers sont automatiquement mappés à `sharepoint.jpeg` et `skype.png` respectivement.

Pour `exchange.yaml` mapper à `exch.png`, spécifiez les éléments suivants dans le `icon_mapping.json` fichier :

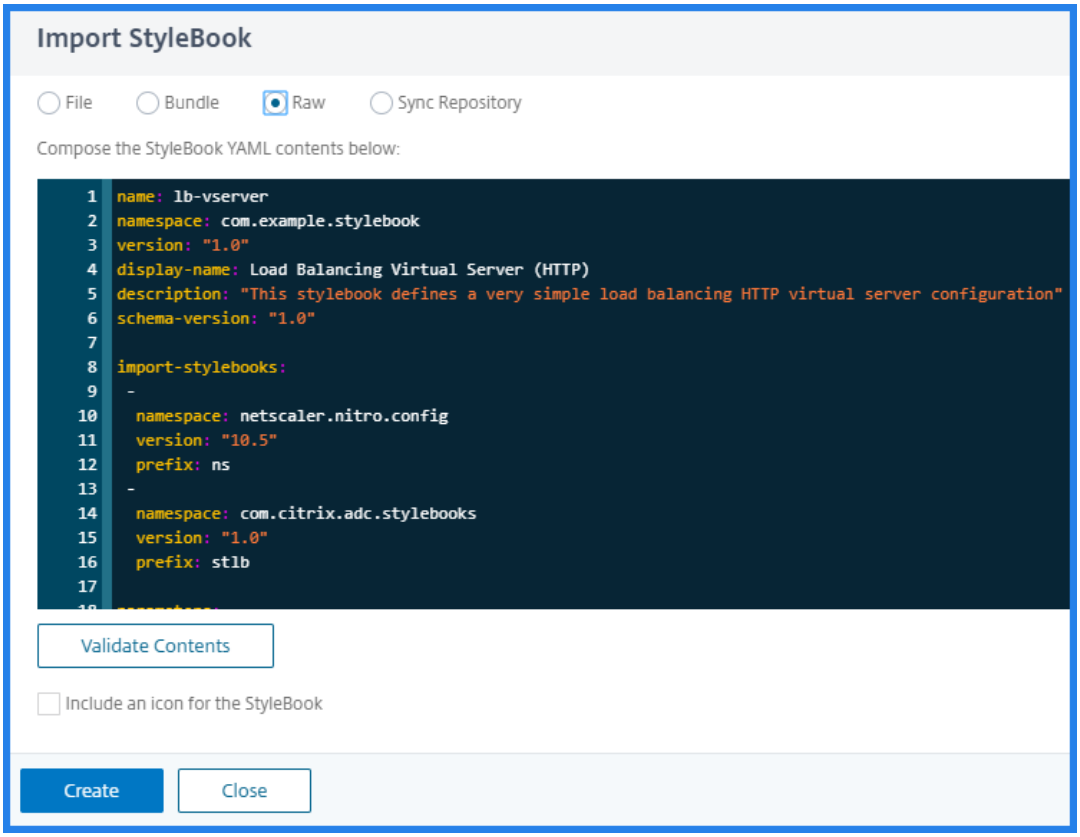
```
{

"exchange.yaml":"exch.png"
 }

<!--NeedCopy-->
```

- **Raw** - Composez le contenu de votre StyleBook dans l'éditeur YAML.

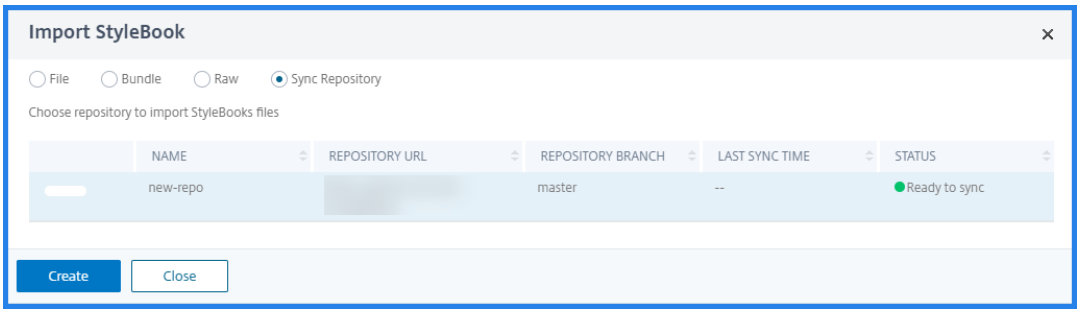
  Vous pouvez valider le contenu du StyleBook pour vérifier les erreurs de grammaire du StyleBook. Pour valider le contenu du StyleBook, cliquez sur **Valider le contenu**.

  > **Remarque**
  >
  > Lors de la composition de StyleBook, assurez-vous de connaître les concepts suivants :
  >
  > - API NITRO
  > - YAML

  Pour plus d'informations sur la façon d'écrire vos propres StyleBooks, reportez-vous à la section Comment créer vos propres styleBooks.



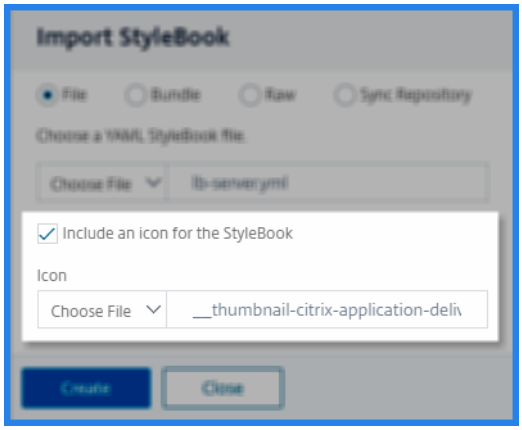
- **Référentiel de synchronisation** - Cette option répertorie les référentiels ajoutés à ADM. Sélectionnez le référentiel à synchroniser avec ADM.



> **Remarque**
>
> Vous pouvez également copier et coller le contenu d'un fichier YAML StyleBook dans l'éditeur YAML.

3. Facultatif, sélectionnez une icône pour un StyleBook.

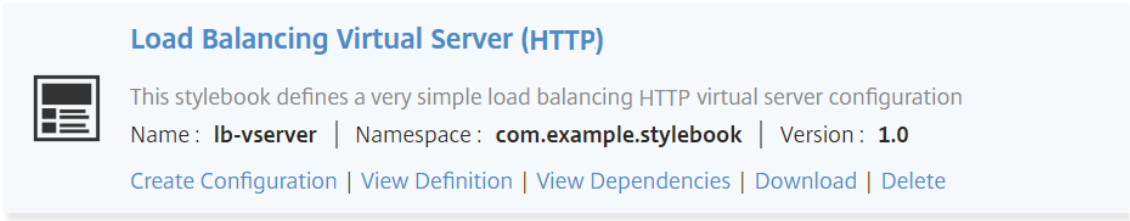
   Dans **Applications > StyleBook**, le StyleBook importé apparaît avec cette icône.



4. Cliquez sur **Créer**.

   Citrix ADM valide désormais votre StyleBook pour toutes les erreurs syntaxiques et sémantiques selon la grammaire StyleBook. Votre StyleBook n'est pas importé dans Citrix ADM s'il y a des erreurs.

   S'il n'y a pas d'erreur, le StyleBook est correctement importé et répertorié sur la page **StyleBooks**. Vous pouvez identifier le StyleBook par le nom complet que vous aviez défini dans la section d'en-tête du StyleBook.

   > **Remarque**
   >
   > Si vous importez un ensemble de fichiers, Citrix ADM décompresse le dossier zippé 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 et la syntaxe de StyleBook des différentes constructions et attributs, reportez-vous à la section Grammaire de StyleBook.

5. Cliquez sur le lien **Créer une configuration** pour créer des configurations à partir de ce StyleBook.

   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.

6. Spécifiez les valeurs requises pour les paramètres.

   Dans l'exemple suivant,

a) Spécifiez les champs**obligatoires du nom de l'**application**et de l'adresse IP de l'**équilibreur de charge.

b) Sélectionnez l'algorithme **** LoadBalancing dans la liste. Par défaut, **ROUNDROBIN** est sélectionné.

! [Exemple de déploiement de configuration] (/en-us/citrix-application-delivery-management-service/media/nmas-stylebooks-yaml-editor-4.png)

7. Sous **Instances cibles**, sélectionnez l'adresse IP de l'instance Citrix ADC sur laquelle vous souhaitez déployer la configuration.

   Vous pouvez également déployer la configuration sur plus d'un Citrix ADC, en spécifiant autant d'instances cibles que nécessaire.

8. Si vous souhaitez tester les objets de configuration Citrix ADC (NITRO) avant de déployer la configuration, cliquez sur **Exécuter à sec**.

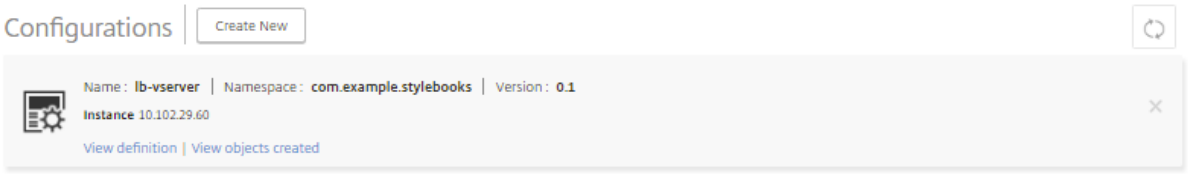
   Si la configuration est valide, les objets de configuration sont créés en fonction des valeurs spécifiées.

   Dans cet exemple, le StyleBook ne crée qu'un seul objet de type `lbvserver`. Ce serveur d'équilibrage de charge était le seul composant défini dans cet exemple de base StyleBook.

   Plus tard, cliquez sur **Créer** pour déployer la configuration sur les instances Citrix ADC sélectionnées.

Une fois la configuration déployée avec succès, un nouveau pack de configuration apparaît dans la page **Configurations**.

> **Remarque**
>
> Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter des instances Citrix ADC récemment découvertes dans Citrix ADM à la liste des instances disponibles dans cette fenêtre.



Rechercher StyleBooks personnalisés

Citrix ADM vous permet désormais de rechercher StyleBooks en fonction de leur type. Autrement dit, vous pouvez maintenant rechercher StyleBooks par défaut ou StyleBooks personnalisés. Cette option est particulièrement utile lorsque vous devez rechercher vos StyleBooks définis par l'utilisateur parmi de nombreux StyleBooks par défaut.

Pour rechercher des StyleBooks personnalisés

1. Dans Citrix ADM, accédez à **Applications** > **Configurations** > **StyleBooks** .
2. Cliquez sur l'icône de recherche en haut à droite.
3. Dans la barre de recherche, sélectionnez **Type**, puis **Personnalisé** dans la sous-liste.
4. Citrix ADM affiche uniquement les StyleBooks définis par l'utilisateur.

Importer un StyleBook pour configurer une application pour le groupe Mise à l'Autoscale

April 29, 2021

Vous pouvez utiliser les livres StyleBooks par défaut dans ADM pour configurer une application sur un groupe de mise à Autoscale ADC. Pour plus d'informations, consultez les liens suivants :

- AWS
- Microsoft Azure

Vous pouvez également créer ou importer vos propres StyleBooks pour créer une application. Les livres StyleBooks du groupe Autoscale sont similaires aux StyleBooks traditionnels. Cependant, les StyleBooks pour configurer des applications sur les groupes et instances de Autoscale ADC ont quelques variations. Cet article vous aide à vous familiariser avec les règles StyleBook pour configurer une application de mise à Autoscale.

Avant de commencer, assurez-vous qu'un groupe de mise à l'Autoscale ADC a été créé dans ADM.

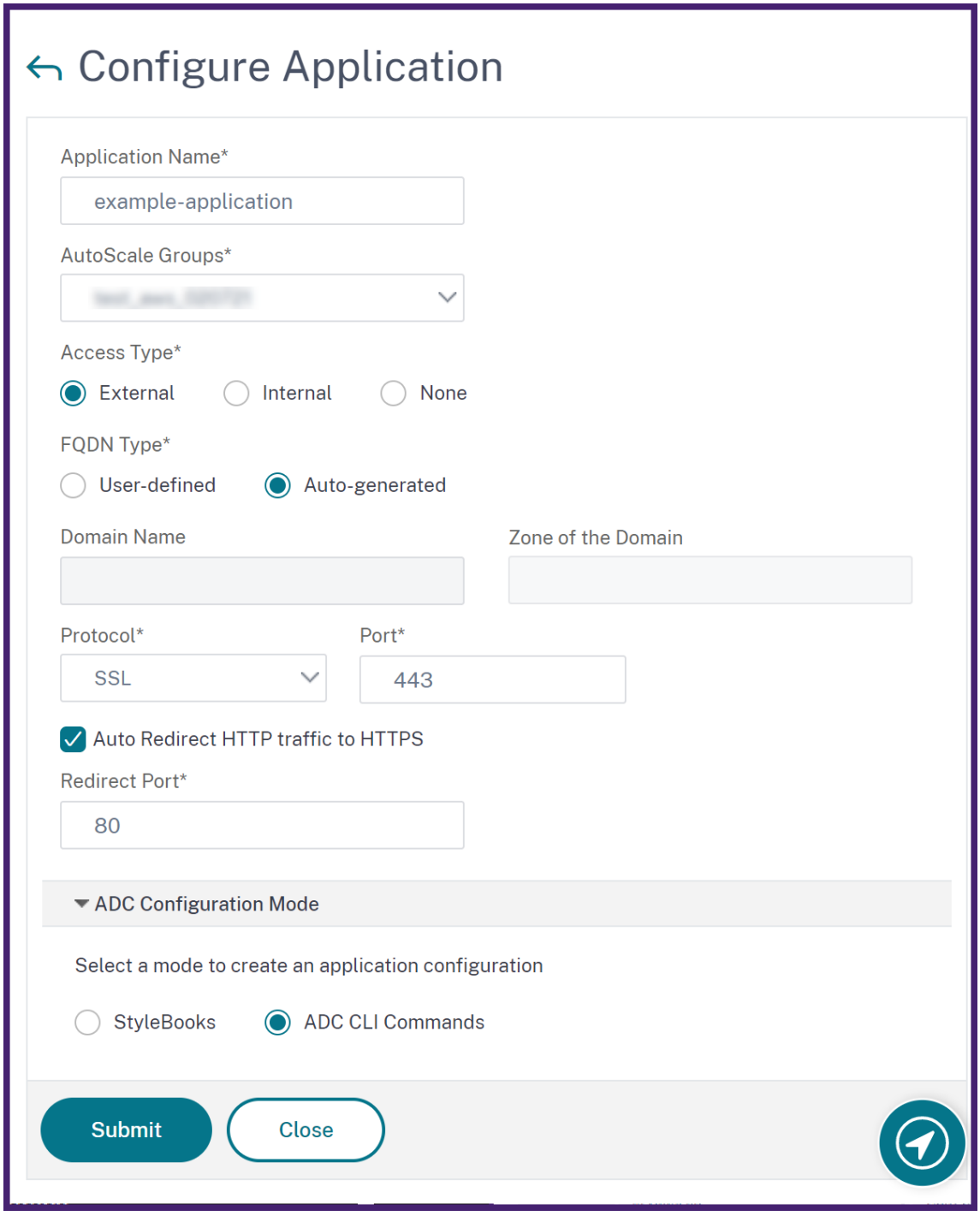
Pour importer un StyleBook personnalisé afin de configurer une application de mise à Autoscale, procédez comme suit :

1. Accédez à **Réseaux > Groupe d'échelle automatique**.
2. Sélectionnez le groupe Autoscale que vous souhaitez configurer.
3. Cliquez sur **Configurer**.
4. Spécifiez les détails suivants :
    - **Nom de l'application** : spécifiez le nom d'une application.
    - **Type d'accès** : vous pouvez utiliser la solution de mise à l'échelle automatique ADM pour des applications externes et internes. Sélectionnez le type d'accès à l'application requis.
    - **Type de nom de domaine complet** - Sélectionnez un mode d'attribution de noms de domaine et de zone.

Si vous souhaitez spécifier manuellement, sélectionnez Définie **par l'utilisateur**. Pour attribuer automatiquement des noms de domaine et de zone, sélectionnez **Généré automatiquement**.

- **Nom de domaine** - Spécifiez le nom de domaine d'une application. Cette option n'est applicable que lorsque vous sélectionnez Type de nom de domaine complet défini par l'utilisateur.
- **Zone du domaine** : sélectionnez le nom de zone d'une application dans la liste. Cette option n'est applicable que lorsque vous sélectionnez Type de nom de domaine complet défini par l'utilisateur.

  Ce nom de domaine et de zone redirige vers les serveurs virtuels dans Azure. Par exemple, si vous hébergez une application dans `app.example.com`, le `app` est le nom de domaine et `example.com` le nom de la zone.
- **Protocole** : sélectionnez le type de protocole dans la liste. L'application configurée reçoit le trafic en fonction du type de protocole sélectionné.
- **Port** : spécifiez la valeur du port. Le port spécifié est utilisé pour établir une communication entre l'application et le groupe Mise à l'Autoscale.



5. Cliquez sur **Choisir StyleBook**.
6. Dans la page **Choisir un livre de style**, cliquez sur **Importer un nouveau livre de style**. Pour plus d'
   informations sur les options d'importation, reportez-vous à la section Importer et utiliser StyleBook.

Le groupe Autoscale StyleBooks a quelques paramètres obligatoires. La liste d'attributs suivante

décrit la variation entre le groupe Mise à l'Autoscale et les livres StyleBooks traditionnels :

- **Type** - Dans la section d'en-tête, incluez l' `type` attribut avec la valeur : `autoscale`.

```
type: autoscale
<!--NeedCopy-->
```

Cet attribut garantit que StyleBook est utilisé pour configurer une application sur le groupe de mise à l'Autoscale ADC uniquement. De plus, il empêche le StyleBook d'apparaître dans la liste **Applications > StyleBooks**.

Voici un exemple d'en-tête du groupe Autoscale StyleBook :

```
name: autoscale-params
namespace: com.citrix.adc.commontypes
version: "1.0"
description: "This StyleBook defines the parameters required for
   Autoscale Deployment"
display-name: "Autoscale Parmeters StyleBook"
private: true
type: autoscale
schema-version: "1.0"
<!--NeedCopy-->
```

- **Nom de l'application** - Ce paramètre décrit le nom et la description de l'application. Spécifiez le champ d'étiquette pour afficher le paramètre dans l' interface graphique ADM. Ce champ est un type de chaîne.

```
-
    name: app_name
    label: "Application Name"
    description: "Name of the Application"
    type: string
    key: true
    gui:
      updatable: false
      required: true
<!--NeedCopy-->
```

- **Adresse IP virtuelle** - Ce paramètre décrit l'adresse IP d'un serveur virtuel. Le groupe Mise à Autoscale met à jour ce paramètre automatiquement.

```
-
    name: ip_address
    label: "IP Address of the LoadBalancer"
    description: "IP Address of the LoadBalancer"
```



```
      type: ipaddress
      gui:
        hidden: true
<!--NeedCopy-->
```

- **IPset** - Lorsque vous déployez une application, un `IPset` est créé sur les clusters dans chaque zone de disponibilité.
  - Dans AWS, les adresses IP du domaine et de l'instance sont enregistrées auprès de DNS/NLB.
  - Dans Azure, le domaine et les adresses IP de l'instance sont enregistrées auprès du gestionnaire de trafic Azure ou ALB.

  Vous pouvez spécifier des adresses IP ou un jeu d'adresses IP dans le groupe Autoscale StyleBook.

```
-
    name: ipset
    label: "IPSet"
    description: "Configuration for network ipset resource"
    type: string
    gui:
      hidden: true
<!--NeedCopy-->
```

Créer un StyleBook pour télécharger des fichiers sur Citrix ADM

April 29, 2021

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 certificat ou de géolocalisation. Vous pouvez également spécifier le répertoire pour charger ces fichiers.

Configuration de StyleBook

Voici un exemple StyleBook qui décrit comment télécharger un fichier de géolocalisation sur l'instance de Citrix ADC. Les fichiers géographiques sont généralement utilisés dans les configurations GSLB pour définir la proximité statique en fonction de l'emplacement géographique :

Créez votre StyleBook - 1

```
name: upload-geolocations
namespace: com.citrix.adc.stylebooks.samples
version: "1.0"
display-name: GeoLocation File Upload
description: This StyleBook is used to upload a geolocation file to
   Citrix ADC
schema-version: "1.0"

import-stylebooks:
-
 namespace: netscaler.nitro.config
 version: "11.1"
 prefix: ns

parameters:
-
 name: locationfile
 label: Location File
 description: The system file path of the geolocation file on Citrix
    ADM
 type: file
 required: true

components:
-
 name: upload-file-comp
 type: ns::systemfile
 properties:
    filename: $parameters.locationfile.filename
    filelocation: "/var/netscaler/inbuilt_db/"
    filecontent: base64.encode($parameters.locationfile.contents)
<!--NeedCopy-->
```

> **Remarque**
>
> Le paramètre utilisé dans cet exemple est d'un fichier de type. Vous pouvez importer ce StyleBook dans Citrix ADM et l'utiliser pour télécharger des fichiers de géolocalisation.

Ce StyleBook nécessite que le fichier soit déjà présent dans Citrix ADM (par exemple, vous l'auriez déjà copié sur Citrix ADM à l'aide d'un utilitaire tel que 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 un autre StyleBook pour charger un fichier de géolocalisation :

Créez votre StyleBook - 2

```
name: upload-geolocations-alt
namespace: com.citrix.adc.stylebooks.samples
version: "1.0"
display-name: GeoLocation File Upload
description: This StyleBook is used to upload a geolocation file to
   Citrix ADC
schema-version: "1.0"

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  version: "11.1"
  prefix: ns

parameters:
 -
  name: filename
  label: Location Filename
  description: The name of the location file on the Citrix ADC
  type: string
  required: true
 -
  name: filecontents
  label: Location File Contents
  description: The contents of the location file
  type: string
  required: true

components:
 -
  name: upload-file-comp
  type: ns::systemfile
  properties:
   filename: $parameters.filename
   filelocation: "/var/Citrix ADC/inbuilt_db/"
   filecontent: base64.encode($parameters.filecontents)
<!--NeedCopy-->
```


Création de configurations pour télécharger des fichiers

La procédure suivante crée une configuration sur une instance Citrix ADC sélectionnée qui téléchargerait un fichier de géolocalisation à l'aide du premier StyleBook décrit ci-dessus.

Pour créer une configuration pour le téléchargement de fichiers :

1. Dans Citrix ADM, accédez à **Applications** > **Configuration**, puis cliquez sur **Créer un nouveau** . La page Choisir StyleBook affiche tous les StyleBooks disponibles dans votre Citrix ADM. Faites défiler la page vers le bas et sélectionnez le StyleBook que vous avez importé.

   Les paramètres StyleBook apparaissent sous la forme d'une page d'interface utilisateur qui vous permet d'entrer 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 Paramètres de base de l'équilibreur de charge.

3. Dans la section **Fichier d'emplacement**, entrez le nom ou l'emplacement du fichier.

   > **Remarque**
   >
   > Assurez-vous que dans Citrix ADM, le fichier se trouve uniquement sous le dossier du locataire actif. Utilisez n'importe quel FTP pour copier le fichier sur 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 recommande de sélectionner **Exécuter à sec** pour vérifier les objets de configuration créés sur l'instance cible avant d'exécuter la configuration réelle sur l'instance.

Lorsque la création du pack de configuration réussit, le fichier est enregistré sur le système de fichiers d'instance Citrix ADC à l'emplacement : /var/netscaler/inbuilt_db/

> **Remarque**
>
> Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter des instances Citrix ADC récemment découvertes dans Citrix ADM à la liste des instances disponibles dans cette fenêtre.

Utilisation de l'API Citrix ADM pour créer un pack de configuration

Vous pouvez également utiliser l'API Citrix ADM pour créer un pack de configuration qui télécharge des fichiers vers l'instance Citrix ADC sélectionnée. Pour plus d'informations sur l'utilisation des API, reportez-vous à la sectionComment utiliser l'API pour créer des configurations pour charger n'importe quel type de fichier.

Créer un StyleBook pour télécharger des fichiers de certificat SSL et de clé de certificat vers Citrix ADM

April 29, 2021

Lorsque vous créez 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 à partir de votre système local à l'aide de l'interface graphique Citrix Application Delivery Management (ADM). Vous pouvez également utiliser les API Citrix ADM pour télécharger des fichiers de certificats et des fichiers clés qui sont déjà gérés par Citrix ADM.

Configuration de StyleBook

Ce document vous aide à créer votre propre StyleBook - **Load Balancing Virtual Server (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 charger 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. Ceux-ci sont spécifiés dans la section « paramètres », comme indiqué ci-dessous :

```
parameters:
 -
  name: name
  type: string
  required: true
 -
  name: ip
  type: ipaddress
  required: true
 -
  name: lb-alg
  type: string
  allowed-values:
    - ROUNDROBIN
    - LEASTCONNECTION
  default: ROUNDROBIN
 -
  name: certificate
```



```
19    label: "SSL Certificate File"
20    description: "The file name of the SSL certificate file"
21    type: certfile
22   -
23    name: key
24    label: "SSL Certificate Key File"
25    description: "The file name of the server certificate's private key
          file"
26    type: keyfile
27  <!--NeedCopy-->
```

Deux composants sont ensuite créés dans la section Composants du StyleBook, comme indiqué ci-dessous. Le `my-lbvserver-comp` composant est de type ns lbvserver, où :

- « ns » est le préfixe qui fait référence à l'espace de noms intégré netscaler.nitro.config et à la version 10.5 que vous aviez spécifiés dans la section import stylebooks.
- `lbvserver` est un StyleBook intégré dans cet espace de noms. Il correspond à la `lbvserver` ressource Citrix ADC NITRO du même nom.

Le deuxième composant `lbvserver-certificate-comp` est de type `stlb::vserver-certs-binds`. Le préfixe `stlb` fait référence à l'espace de noms « com.citrix.adc.stylebooks » et à la version 1.0 qui est spécifié 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 `vserver-certs-binds` StyleBook utilisé par StyleBooks défini par l'utilisateur vous permet de configurer facilement les certificats en téléchargeant les fichiers de certificat et de clé vers l'instance Citrix ADC cible, et en configurant la liaison des fichiers de certificat et de clé aux serveurs virtuels appropriés. Les propriétés de ce composant sont - le nom du serveur virtuel lb et les noms des certificats SSL que vous fournissez lors de la création du pack de configuration.

```
1  components:
2   -
3    name: my-lbvserver-comp
4    type: ns::lbvserver
5    properties:
6     name: $parameters.name
7     servicetype: SSL
8     ipv46: $parameters.ip
9     port: 443
10    lbmethod: $parameters.lb-alg
11  -
12   name: lbvserver-certificate-comp
13   type: stlb::vserver-certs-binds
```



```
  description: Binds lbvserver with server certificate
  properties:
   vserver-name: $components.my-lbvserver-comp.properties.name
   certificates:
    -
     cert-name: $parameters.name + "-lb-cert"
     cert-file: $parameters.certificate
     ssl-inform: PEM
     key-name: $parameters.name + "-key"
     key-file: $parameters.key
<!--NeedCopy-->
```

Lorsque vous utilisez l'API pour créer une configuration à partir d'un tel StyleBook, utilisez uniquement les noms de fichiers (pas le chemin complet du fichier). Ces fichiers devraient être déjà disponibles dans les dossiers de fichiers de certificats et de clés sur Citrix ADM. Le fichier de certificat SSL téléchargé est stocké sur Citrix ADM dans le fichier /var/mps/tenants/… /ns_ssl_certs, et le fichier de clé de certificat SSL est stocké dans /var/mps/tenants/… /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 de 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.

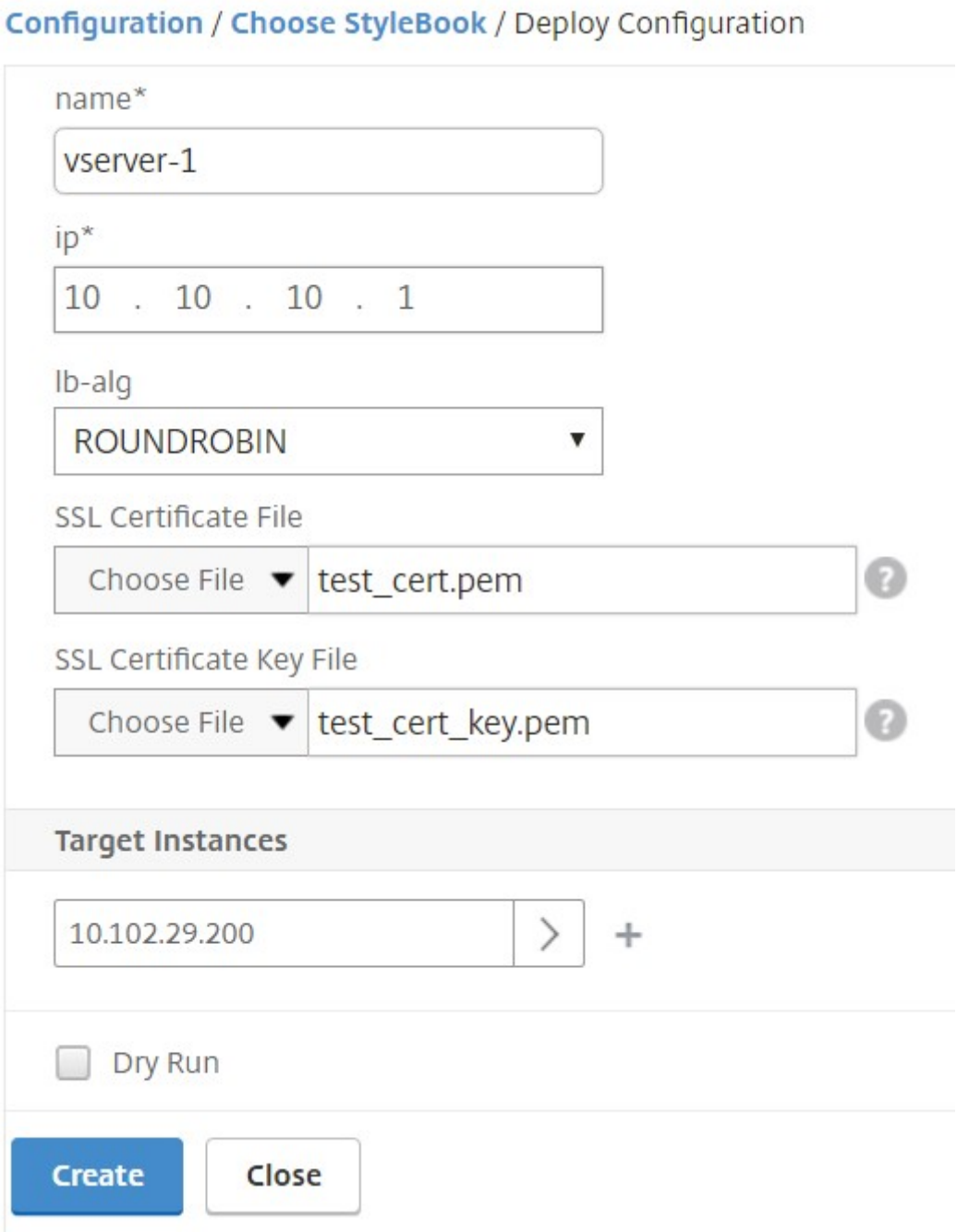
Pour créer une configuration pour le téléchargement de fichiers :

1. Dans Citrix ADM, accédez à **Applications** > **Configuration > StyleBooks** . La page **StyleBooks** affiche tous les StyleBooks disponibles dans votre Citrix ADM.
2. Faites défiler la page vers le bas et sélectionnez **Load Balancing Virtual Server (SSL)** ou tapez **Load Balancing Virtual Server (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 StyleBook apparaissent sous la forme d'une page d'interface utilisateur qui vous permet d'entrer 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 Paramètres de base de l'équilibreur de charge.
5. Dans la section **Paramètres des certificats SSL**, sélectionnez les fichiers respectifs 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**.

> **Remarque**
>
> Vous pouvez également cliquer sur l'icône d'actualisation pour ajouter des instances Citrix ADC récemment découvertes dans Citrix ADM à la liste des instances disponibles dans cette fenêtre.



> **Remarque**
>
> Dans Citrix ADM, les StyleBooks par défaut suivants, qui sont expédiés dans le cadre de Citrix ADM, vous permettent de créer la prise en charge SSL en téléchargeant les certificats et clés SSL.
>
> - StyleBook LoadBalancing HTTP/SSL (lb)
> - Équilibrage de charge HTTP/SSL (avec moniteurs) StyleBook (`lb-mon`)
> - Application commutée de contenu HTTP/SSL avec moniteurs (`cs-lb-mon`)
> - Exemple de style d'application utilisant les fonctionnalités CS, LB et SSL (`sample-cs-app`)
>
> Vous pouvez également créer vos propres StyleBooks qui utilisent les certificats SSL de la même manière que décrite dans le StyleBook ci-dessus

Créez votre StyleBook

Le contenu complet du fichier lb-vserver-ssl.yaml est illustré ci-dessous :

```
name: lb-vserver-ssl
description: "This stylebook defines a load balancing virtual server
   configuration."
display-name: "Load Balancing Virtual Server (SSL)"
namespace: com.example.ssl.stylebooks
schema-version: "1.0"
version: "0.1"

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  prefix: ns
  version: "10.5"
 -
  namespace: com.citrix.adc.stylebooks
  prefix: stlb
  version: "1.0"

parameters:
 -
  name: name
  type: string
  required: true
 -
  name: ip
  type: ipaddress
  required: true
 -
```



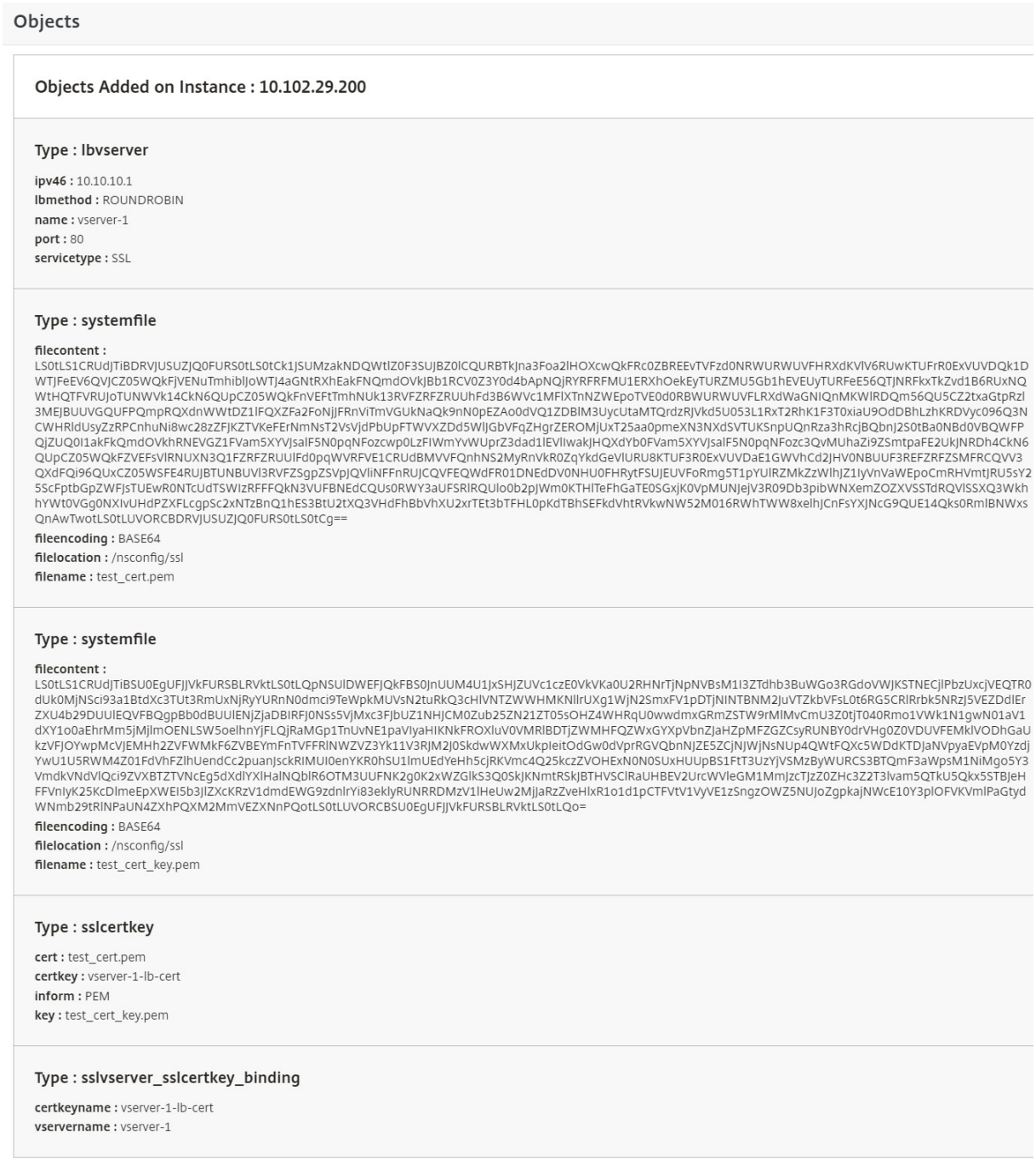
```
28    name: lb-alg
29    type: string
30    allowed-values:
31      - ROUNDROBIN
32      - LEASTCONNECTION
33    default: ROUNDROBIN
34   -
35    name: certificate
36    label: "SSL Certificate File"
37    description: "The file name of the SSL certificate file"
38    type: certfile
39   -
40    name: key
41    label: "SSL Certificate Key File"
42    description: "The file name of the server certificate's private key
          file"
43    type: keyfile
44
45  components:
46   -
47    name: my-lbvserver-comp
48    type: ns::lbvserver
49    properties:
50      name: $parameters.name
51      servicetype: SSL
52      ipv46: $parameters.ip
53      port: 443
54      lbmethod: $parameters.lb-alg
55   -
56    name: lbvserver-certificate-comp
57    type: stlb::vserver-certs-binds
58    description: Binds lbvserver with server certificate
59    properties:
60     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 pack de configuration qui télécharge les fichiers Cert et Key vers l'instance Citrix ADC sélectionnée. Pour plus d'informations sur l'utilisation des API, voir Comment utiliser l'API pour créer des configurations pour télécharger des fichiers de certificats et de clés.

Affichage des objets définis sur l'instance de Citrix ADC

Une fois la configuration StyleBook (pack de configuration) créée sur Citrix ADM, cliquez sur **Afficher les objets créés** pour afficher tous les objets Citrix ADC créés sur l'instance Citrix ADC cible



Activer l’analyse et configurer les alarmes sur un serveur virtuel défini dans un StyleBook

April 29, 2021

Vous pouvez utiliser la construction d’opérations pour configurer les analyses de Citrix Application

Delivery Management (ADM) pour collecter des enregistrements AppFlow sur tout ou partie des transactions de trafic traitées par un composant de serveur virtuel faisant partie d'un StyleBook. Vous pouvez également utiliser cette construction pour configurer des alarmes afin d'obtenir un aperçu du trafic géré par le serveur virtuel.

L'exemple suivant montre une section Opérations d'un StyleBook :

```
operations:
  analytics:
   -
    name: lbvserver-ops
    properties:
      target: $components.basic-lb-comp
      filter: HTTP.REQ.URL.CONTAINS("catalog")
  alarms:
   -
    name: lbvserver-alarm
    properties:
      target: $components.basic-lb-comp
      email-profile: $parameters.emailprofile
      sms-profile: "MyProdSMS"
      rules:
       -
         metric: "total_requests"
         operator: "greaterthan"
         value: 25
         period-unit: $parameters.period
       -
         metric: "total_bytes"
         operator: "lessthan"
         value: 60
         period-unit: "day"
<!--NeedCopy-->
```

Les attributs de la section Analytics sont utilisés pour demander à la fonctionnalité d'analyse Citrix ADM de collecter des enregistrements AppFlow sur un composant serveur virtuel identifié par la propriété cible. Vous pouvez également spécifier une propriété de filtre qui accepte une expression de stratégie Citrix ADM pour filtrer les demandes pour lesquelles des enregistrements AppFlow sont collectés sur le serveur virtuel.

Lorsqu'un pack de configuration est créé à partir de ce StyleBook, la fonctionnalité d'analyse Citrix ADM est configurée pour collecter les enregistrements AppFlow sur les serveurs virtuels qui ont été spécifiés lors de la création d'un pack de configuration.

Les attributs de la section alarmes permettent de définir des seuils pour générer des alarmes et en-

voyer 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 spécifie 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` pour >
- `lessthan` pour <
- `greaterthanequal` pour >=
- `lessthanequal` pour <=

Notez que StyleBooks utilise des noms d'API pour les mesures et non pas les noms affichés sur l'interface graphique d'analyse Citrix ADM.

Pour savoir comment afficher et analyser les données collectées sur des serveurs virtuels créés dans le cadre d'un pack de configuration, consultez la documentation d'analyse Citrix ADM.

Rôles d'instance

April 29, 2021

Dans Citrix Application Delivery Management (ADM), il peut y avoir un scénario dans lequel vous devez configurer plusieurs instances de Citrix ADC pour une seule application, mais également dans lequel chaque instance d'ADC nécessite une configuration différente pour être déployée sur ces instances. Un exemple de ce cas est le Microsoft Skype for Business StyleBook par défaut.

StyleBooks prend actuellement en charge la possibilité de créer un pack de configuration et d'appliquer la même configuration sur plusieurs instances Citrix ADC. Un tel scénario où la configuration est identique sur toutes les instances ADC, peut être appelé configuration symétrique.

Maintenant, avec la fonctionnalité « rôles d'instance » de StyleBooks, vous pouvez créer une configuration asymétrique, c'est-à-dire un pack de configuration qui peut être appliqué sur plusieurs instances ADC, mais avec des configurations différentes sur différentes instances ADC.

Lorsqu'une fonctionnalité StyleBook avec rôles d'instance est utilisée pour créer un pack de configuration, chaque instance ADC d'un pack de configuration peut se voir attribuer un rôle différent. Ce rôle détermine les objets de configuration du pack de configuration que l'instance ADC recevra.

Points à noter :

- L'ensemble des rôles d'instance dans un StyleBook sont définis lors de la création du StyleBook.

- Les rôles sont attribués à une instance ADC spécifique lors de la création ou de la mise à jour du pack de configuration.

Section Rôles de cible

Une nouvelle section dans un StyleBook appelée « target-roles » est introduite, où 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 « Target roles » - A et B.

```
target-roles:

  -
   name: A
   name: B
     min-targets: 2
     max-targets: 5
<!--NeedCopy-->
```

Vous pouvez voir que le rôle B définit également deux sous-propriétés facultatives, min-targets et max-targets.

Bien que ces deux sous-propriétés soient facultatives, min-targets spécifient le nombre minimum obligatoire d'instances ADC à assigner ce rôle lors de la création d'un pack de configuration à partir de ce StyleBook, et max-targets spécifient le nombre maximal d'instances ADC pouvant être affectées à ce rôle lors de la création d'un pack de configuration de ce StyleBook.

Si ces sous-propriétés ne sont pas spécifiées, le nombre d'instances ADC pouvant être configurées pour ce rôle n'est pas limité. Si min-targets = 0, la configuration associée à ce rôle est facultative et si min-targets = 1, cette configuration est obligatoire et au moins une instance ADC doit être configurée pour ce rôle.

Rôle « par défaut »

En plus des rôles explicitement définis, il existe un rôle implicite que tous les StyleBooks ont, et ce rôle est appelé comme rôle par défaut. Ce rôle peut être utilisé comme n'importe quel autre rôle dans un StyleBook. Lors de la création d'un pack de configuration, si une instance ADC n'est pas affectée avec un rôle spécifique, l'instance est implicitement affectée au rôle « par défaut ». L'instance recevra désormais tous les objets de configuration générés par les composants qui ont le rôle « par défaut ».

Composants avec rôles

Après avoir défini les rôles qu'un StyleBook peut prendre en charge (y compris le rôle « par défaut »), les rôles peuvent être utilisés dans la section Composants d'un StyleBook. Si vous souhaitez qu'un composant soit déployé uniquement sur des instances ADC qui jouent un certain rôle, vous pouvez spécifier l'attribut role dans le cadre du composant, comme illustré dans l'exemple suivant d'un composant :

```
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
<!--NeedCopy-->
```

Dans l'exemple ci-dessus, le composant génère un `lbvserver` qui sera déployé sur les instances jouant le rôle A. Notez que l'attribut rôles d'un composant est une liste et un composant peut se voir attribuer plusieurs rôles. Ces rôles auraient été déclarés dans la section « target-roles » du StyleBook.

Remarque : Si un composant dans un StyleBook ne spécifie pas d'attribut de rôle, les objets de configuration générés par le composant sont créés sur toutes les instances Citrix ADC quel que soit leur rôle. Vous pouvez utiliser cette fonctionnalité efficacement pour créer des objets de configuration qui peuvent être appliqués à toutes les instances d'un pack de configuration.

Supposons qu'il existe un StyleBook avec deux rôles définis - A et B, et qui contient quatre composants.

- Le composant C1 a les rôles A et B
- Le composant C2 a le rôle B
- Le composant C3 n'a aucun rôle défini
- Le composant C4 a le rôle « par défaut »

La section composants de ce StyleBook est reproduite ci-dessous :

```
components:
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
      - B
```



```
8       properties:
9         name: lb1
10        servicetype: HTTP
11        ipv46: 1.1.1.1
12        port: 80
13    -
14      name: C2
15      type: ns::lbvserver
16      roles:
17        - B
18      properties:
19        name: lb2
20        servicetype: HTTP
21        ipv46: 12.12.12.12
22        port: 80
23    -
24      name: C3
25      type: ns::lbvserver
26      properties:
27        name: lb3
28        servicetype: HTTP
29        ipv46: 13.13.13.13
30        port: 80
31    -
32      name: C4
33      type: ns::lbvserver
34      roles:
35        - default
36      properties:
37        name: lb4
38        servicetype: HTTP
39        ipv46: 14.14.14.14
40        port: 80
41  <!--NeedCopy-->
```

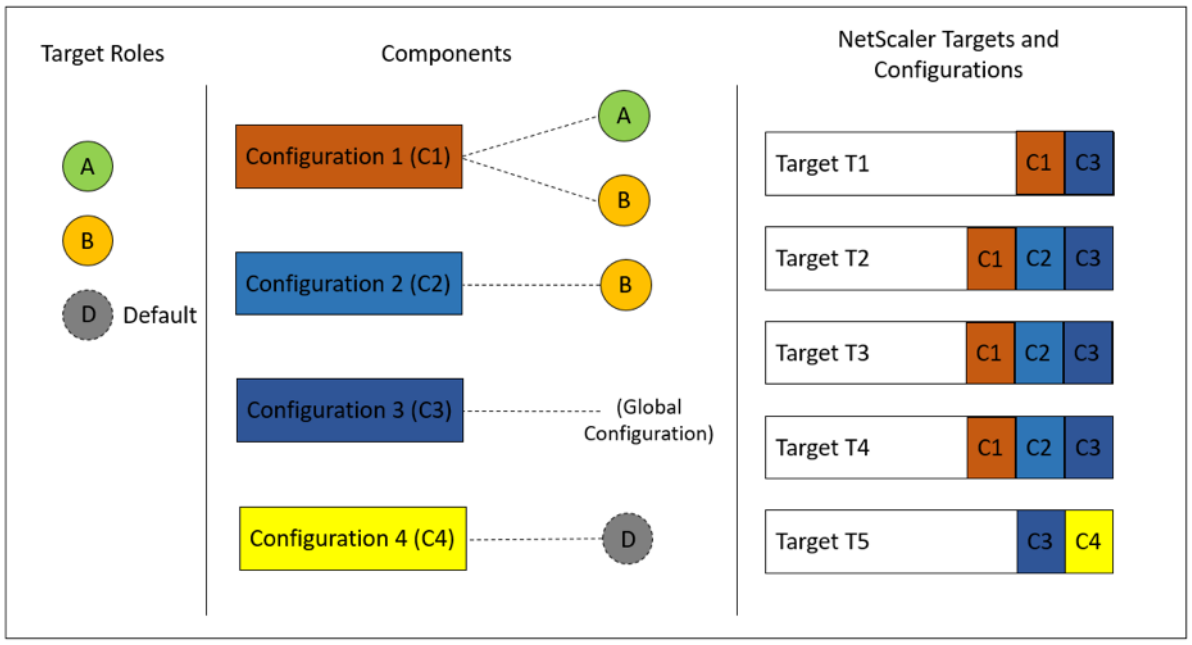
Notez que le composant C3 n'a pas de rôle défini, ce qui signifie que le composant est déployé sur toutes les instances quel que soit leur rôle. D'autre part, le composant C4 a le rôle « default », ce qui signifie qu'il est appliqué à toute instance qui ne lui a pas de rôle explicite.

Maintenant, considérez que vous souhaitez créer un pack de configuration à l'aide de ce StyleBook et le déployer sur cinq instances ADC. À ce stade, vous pouvez affecter les rôles aux instances de la manière suivante :

- Le rôle A est attribué aux instances T1, T2, T3 et T4
- Le rôle B est attribué aux instances T2, T3 et T4

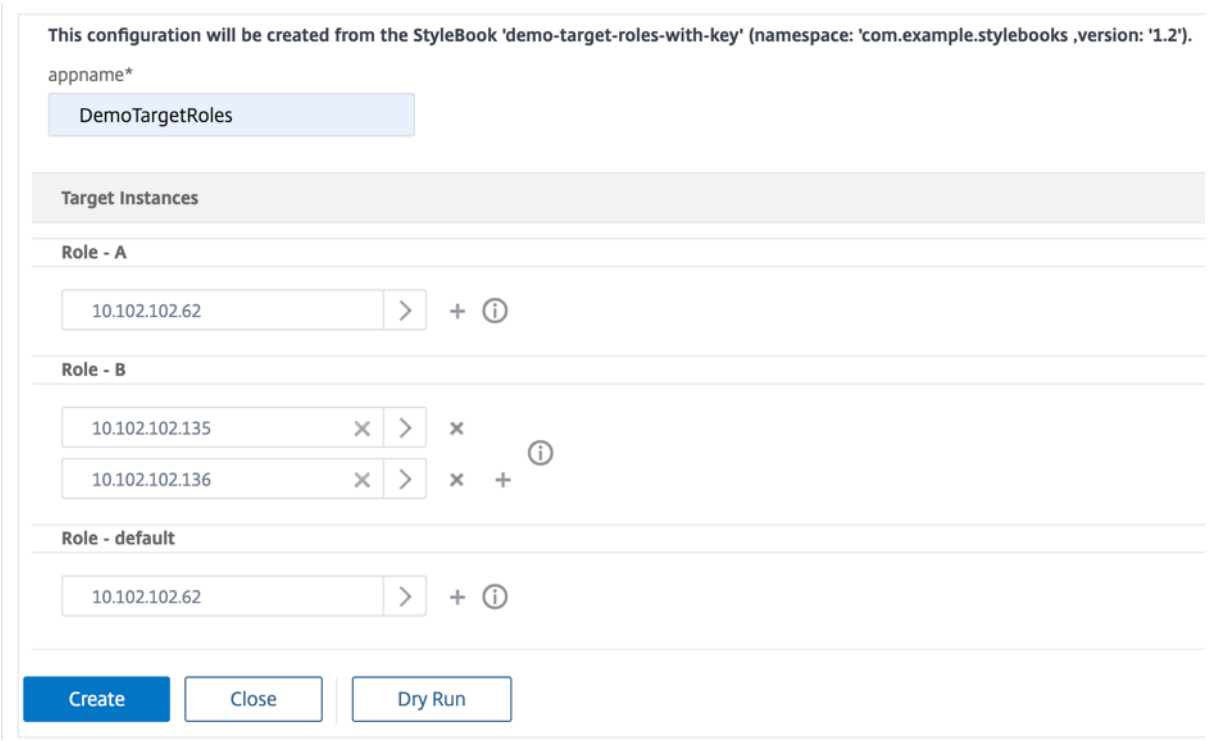
- Instance T5 ne reçoit aucun rôle

L'image suivante résume les attributions de rôle et montre la configuration résultante que chaque instance ADC recevra :



Notez que le composant C3 est déployé sur toutes les instances quel que soit le rôle, car ce composant ne possédait aucun attribut role.

L'image suivante montre l'attribution de rôles lors de la création d'un exemple de pack de configuration :



Vous pouvez également utiliser la fonction « Exécuter à sec » lors de la création d'un pack de configuration pour afficher et vérifier l'attribution correcte des rôles et des objets de configuration qui seront créés sur chaque instance ADC.

Créez votre StyleBook

Le contenu complet du StyleBook « demo-target-roles » est fourni ci-dessous :

```
---
name: demo-target-roles
namespace: com.example.stylebooks
version: "1.2"
schema-version: "1.0"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
parameters:
  -
    name: appname
    type: string
    required: true
    key: true
```

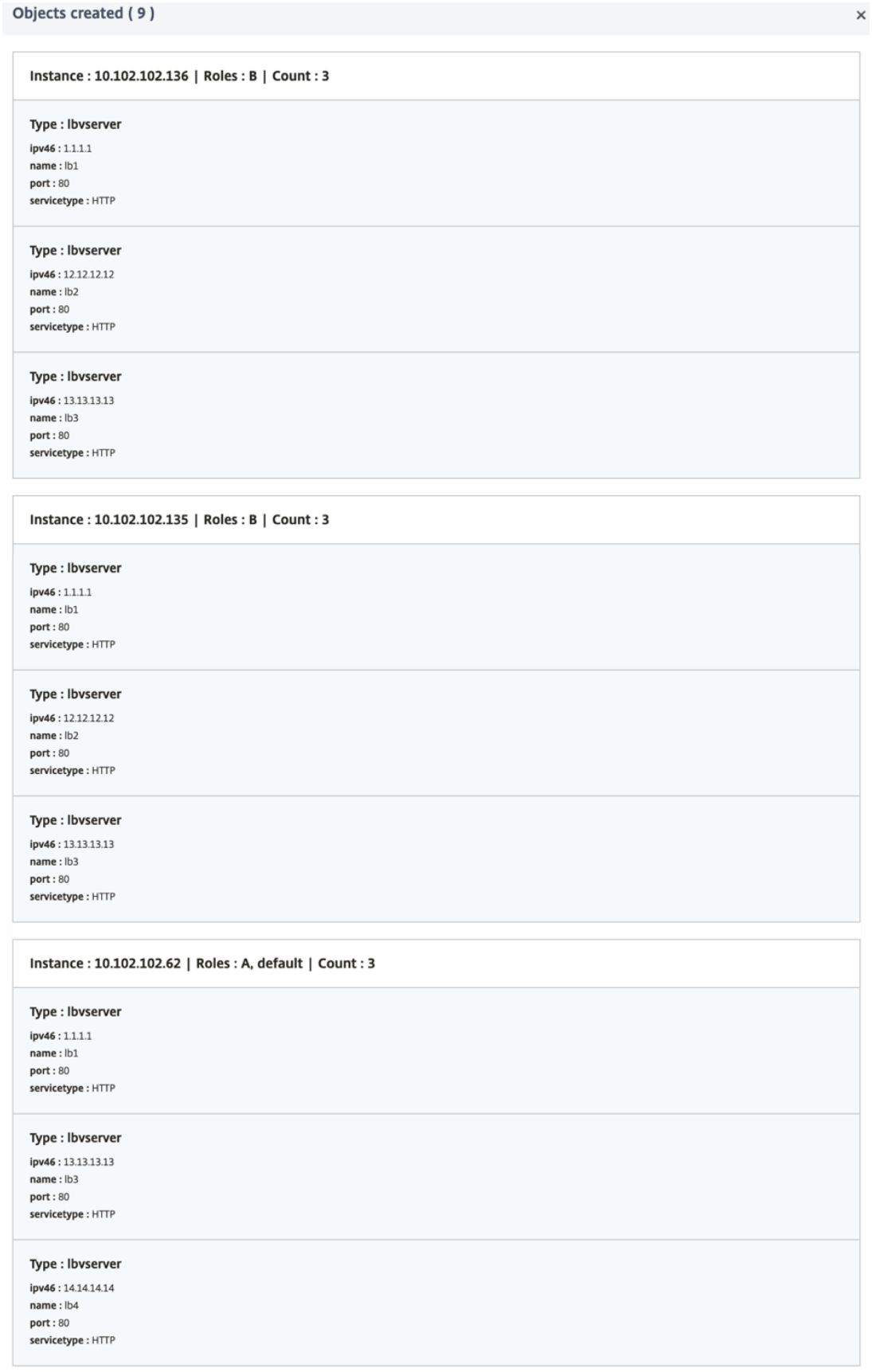


```
target-roles:
  -
    name: A
  -
    name: B
    min-targets: 2
    max-targets: 5
components:
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
      - B
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
  -
    name: C2
    type: ns::lbvserver
    roles:
      - B
    properties:
      name: lb2
      servicetype: HTTP
      ipv46: 12.12.12.12
      port: 80
  -
    name: C3
    type: ns::lbvserver
    properties:
      name: lb3
      servicetype: HTTP
      ipv46: 13.13.13.13
      port: 80
  -
    name: C4
    type: ns::lbvserver
    roles:
      - default
    properties:
      name: lb4
      servicetype: HTTP
```



```
62        ipv46: 14.14.14.14
63        port: 80
64  <!--NeedCopy-->
```

L'image suivante montre les objets créés pour un exemple de pack de configuration :



Utilisation des API

Lorsque vous utilisez l'API REST, vous pouvez spécifier des rôles pour chaque instance ADC lors de la création ou de la mise à jour du pack de configuration comme suit. Dans le bloc « cibles », spécifiez l'UUID de l'instance Citrix ADC spécifique sur laquelle vous souhaitez déployer les composants individuels.

```
"targets": [
            {

             "id": "<ADC-UUID>",
             "roles": ["A"]
             }
 ,
           ]
<!--NeedCopy-->
```

Un exemple complet d'API REST est fourni à titre de référence.

POST /<ADM-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/1.2/demo-target-roles/configpacks

```
{

  "configpack": {

     "parameters": {

     "appname": "app1"
     }
 ,
     "targets": [
        {

          "id": "f53c35c3-a6bc-4619-b4b4-ad7ab6a94ddb",
        "roles": ["A"]
         }
 ,
        {

          "id": "c08caa1c-1011-48aa-b8c7-9aed1cd38ed0",
          "roles": ["A", "B"]
         }
 ,
        {

```



```
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
37             "id": "fa5d97ab-ca29-4adf-b451-06e7a234e3da",
38             "roles": ["default"]
39            }
40
41          ]
42         }
43
44  }
45
46  <!--NeedCopy-->
```

Créer un StyleBook pour effectuer des opérations non CRUD

April 29, 2021

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'équilibreur de charge (`lbvserver`) ou un objet de fonctionnalité Citrix ADC (`nsfeature`) peut prendre en charge l'opération « enable » ou « désactiver ». De même, Citrix ADC `certkeys` prend en charge les opérations « lien » et « dissocier » 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 a `certkey` à a `lbvserver`) n'est pas considérée comme une opération non-CRUD. En effet, les liaisons NITRO sont représentées en tant qu'objets de configuration à part entière. Ces objets sont créés et supprimés comme tout autre objet de configuration Citrix ADC.

Soutenir les opérations non bruts

Une nouvelle construction appelée « méta-propriétés » est ajoutée dans le composant au même niveau que la construction « properties ». Le seul attribut pris en charge dans cette construction est actuellement appelé « action » Cet attribut peut prendre des valeurs telles que « enable » ou « disable » qui sont prises en charge par cet objet de configuration.

```
components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
  meta-properties
   action: enable
  properties:
    name: $parameters.name
    servicetype: HTTP
    ipv46: $parameters.ip
    port: 80
    lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

Dans cet exemple, le `my-lbvserver-comp` composant 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. La `lbvserver` est une ressource NITRO dans cet espace de noms. En tant qu'action implicite, le `lbvserver` est d'abord créé par le StyleBook. Ensuite, l'opération « enable » est effectuée dessus.

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'exécutent pas d'actions non-CRUD.

> **Remarque**
>
> La valeur de l'attribut action ne peut pas être une expression StyleBook évaluée dynamiquement.

Créer et modifier un pack de configuration

April 29, 2021

Dans Citrix Application Delivery Management (ADM), vous pouvez créer un pack de configuration à partir d'un StyleBook. Et, le pack de configuration est lié au StyleBook à partir duquel il est créé. Les mises à jour du pack de configuration sont effectuées via le StyleBook auquel il est lié.

Créer un pack de configuration

Effectuez les opérations suivantes pour créer un pack de configuration à partir d'un StyleBook :

1. Accédez à **Applications > StyleBooks > Configurations**.
2. Cliquez sur **Add**.
3. Dans **Choisir des livres de style**, sélectionnez les StyleBooks requis à partir desquels vous souhaitez créer un pack de configuration.

   Cette page classe StyleBooks dans StyleBooks par défaut et personnalisés. Sélectionnez les onglets respectifs pour trouver les StyleBooks requis.
4. Spécifiez les détails requis, tels que le nom de l'application, l'adresse IP, le port ou le type de protocole.

   Les champs de l'interface graphique diffèrent d'un StyleBook à un autre StyleBook.
5. Dans **Instances cibles**, sélectionnez les instances ou les groupes d'instances dans lesquels vous souhaitez exécuter la configuration.

   > **Remarque**
   >
   > Vous pouvez déployer la configuration sur plusieurs Citrix ADC, en spécifiant autant d'instances cibles que nécessaire.
6. Cliquez sur **Exécuter à sec**.

   La page **Objets** affiche les objets créés, modifiés ou supprimés des instances Citrix ADC.
7. Cliquez sur **Créer**

   Le pack de configuration apparaît dans la page **StyleBook > Configurations**.

Si vous souhaitez modifier les packs de configuration existants, sélectionnez-le et cliquez sur **Modifier**.

Modifier le StyleBook d'un pack de configuration

Parfois, vous devez mettre à jour le StyleBook pour ajouter des fonctionnalités ou résoudre un problème. Si vous avez déjà créé des packs de configuration à l'aide de l'ancien StyleBook, vous pouvez les mettre à jour pour utiliser le nouveau StyleBook mis à jour. Pour utiliser un nouveau StyleBook, modifiez le StyleBook existant du pack de configuration.

Prenons un exemple StyleBook **example-lb** qui déploie une configuration d'équilibrage de charge de base sur une instance ADC. Et, vous créez un pack de configuration CP1 à partir de ce StyleBook.

Lorsque vous souhaitez configurer des moniteurs avec la configuration de base de l'équilibrage de charge, vous avez besoin d'un nouveau StyleBook. Par conséquent, créez **exemple-lb-mon** StyleBook qui inclut la possibilité de configurer des moniteurs ainsi que la configuration de base de l'équilibreur de charge.

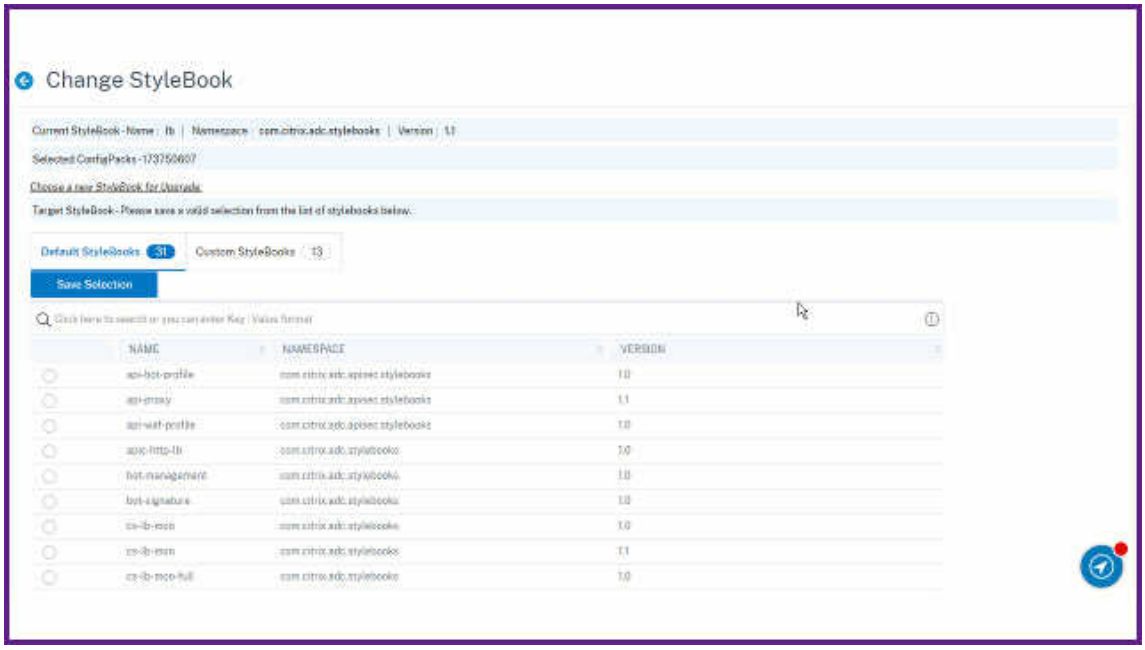
Après avoir créé un StyleBook, mettez à jour le pack de configuration existant CP1 pour ajouter des moniteurs. Pour ce faire, effectuez les opérations suivantes :

1. Accédez à **Applications > StyleBooks > Configurations**.
2. Sélectionnez le pack de configuration pour lequel vous souhaitez modifier le StyleBook.

   Dans cet exemple, sélectionnez CP1 dans la liste.
3. Cliquez sur **Modifier le livre de style**.
4. Sélectionnez le StyleBook requis dans la liste. Cliquez ensuite sur **Enregistrer la sélection**.
5. Cliquez sur **Change**.

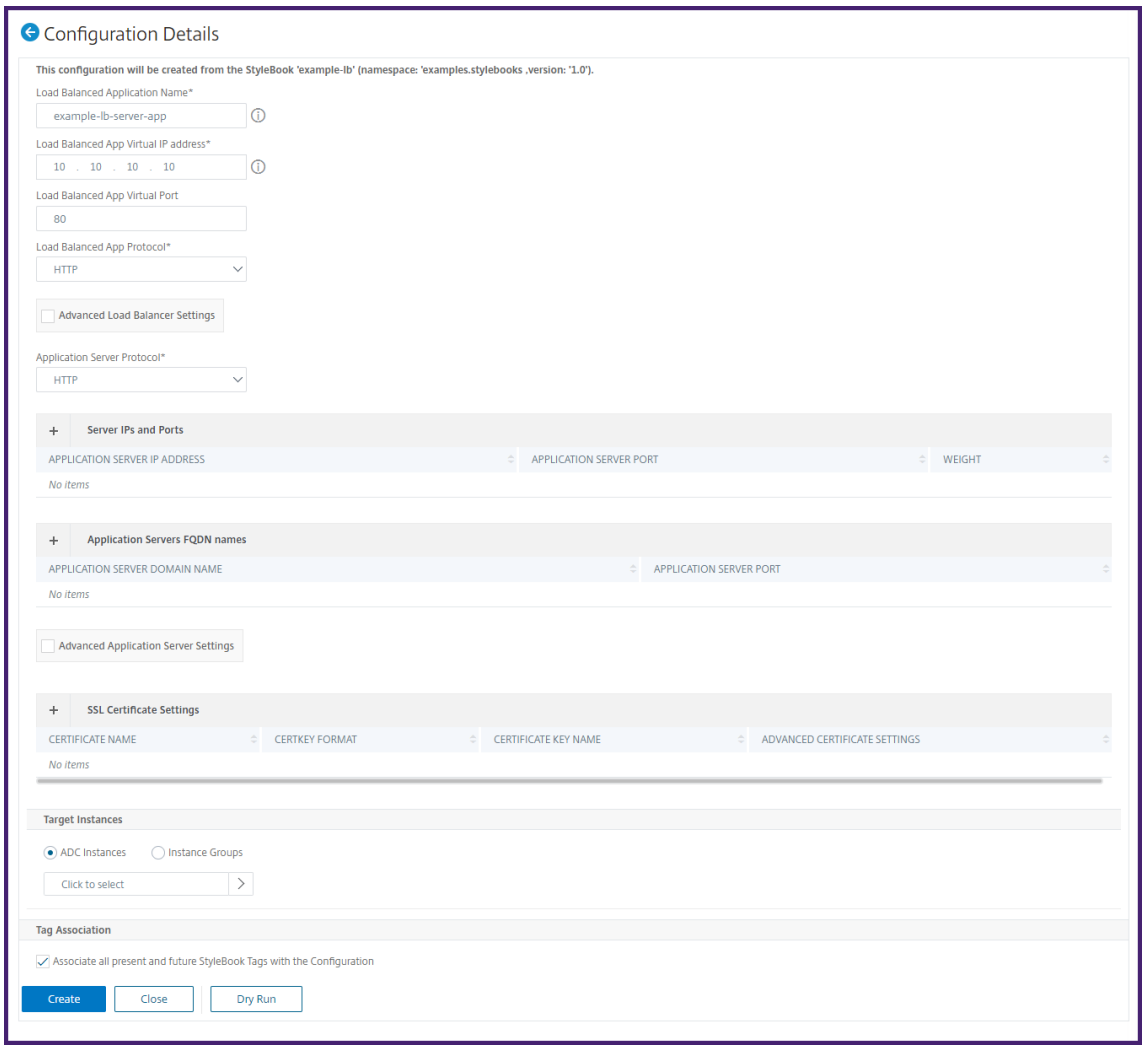
   Dans cet exemple, sélectionnez **exemple-lb-mon** dans la liste.

   Lorsque vous modifiez le StyleBook d'un pack de configuration, les paramètres du nouveau StyleBook peuvent avoir une structure différente de celle du StyleBook existant. Si la structure des paramètres est similaire à la précédente StyleBook, les valeurs des paramètres sont automatiquement conservées dans leurs champs respectifs. Sinon, seuls les paramètres ayant la même structure entre les deux StyleBooks sont transférés. Par exemple, le même nom de paramètre, le même type, le même paramètre parent, et plus encore.

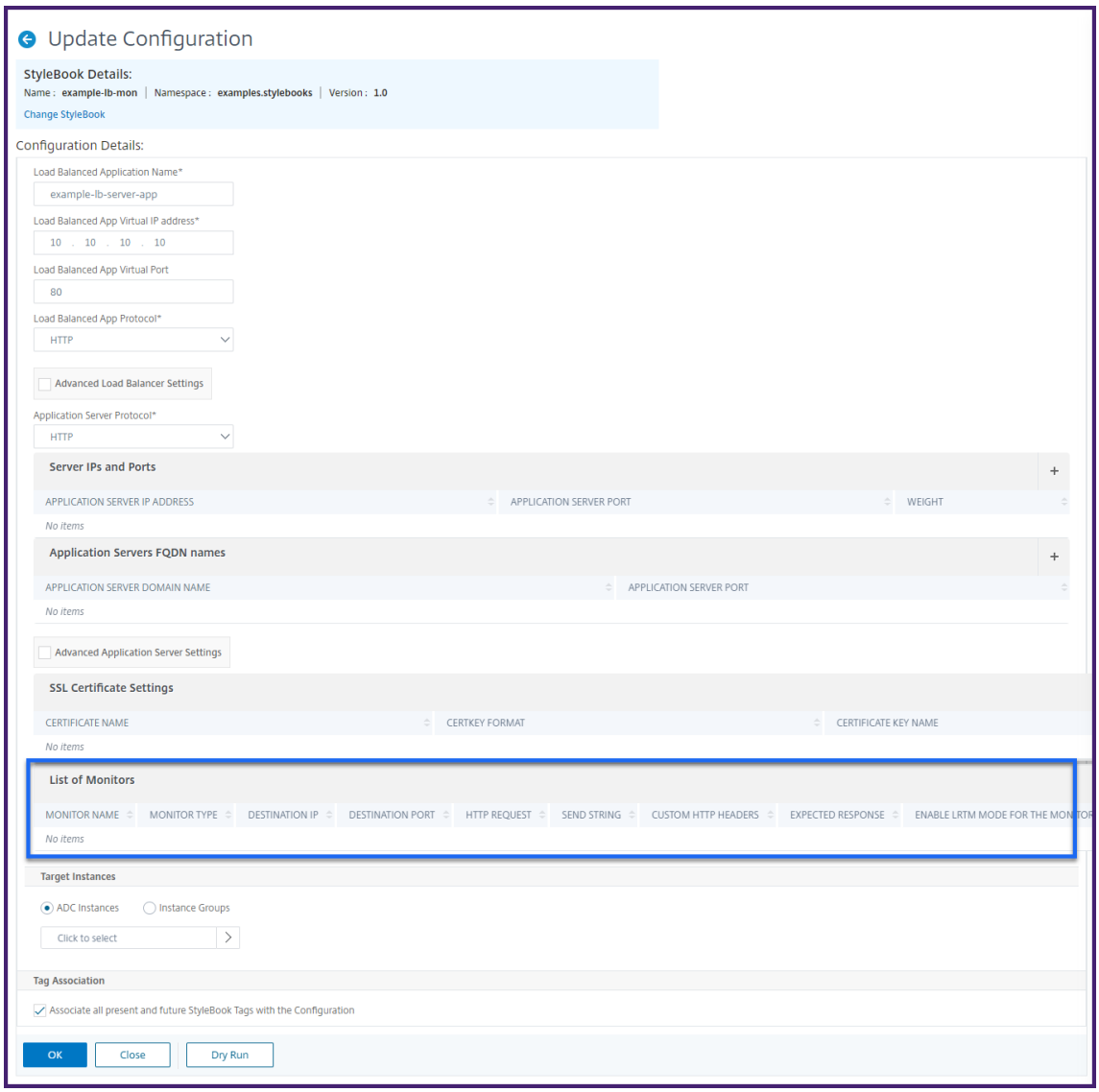


Si de nouveaux paramètres obligatoires sont ajoutés dans le nouveau StyleBook, après avoir modifié le StyleBook, vous devez spécifier manuellement les valeurs de ces paramètres.

Dans cet exemple, les paramètres qui apparaissent sur la page de configuration de l' **example-lb** StyleBook sont les suivants :



Les paramètres qui apparaissent sur la page de configuration du nouveau styleBook **example-lb-mon** sont les suivants :



Dans ce cas, les StyleBooks conservent les anciennes valeurs pour la configuration de base de l'équilibreur de charge car le nouveau StyleBook n'a pas modifié les paramètres existants. Et, il ajoute seulement les nouveaux paramètres. Pour les paramètres du moniteur, spécifiez manuellement les valeurs requises.

6. Dans les **instances cibles**, passez en revue les instances sélectionnées et mettez à jour la liste si nécessaire.
7. Cliquez sur **Exécuter à sec**.

   La page **Objets** affiche les objets créés, modifiés ou supprimés des instances Citrix ADC.
8. Cliquez sur **OK**.

   Dans la page **StyleBook > Configurations**, la colonne **Nom du livre StyleBook** affiche le nouveau nom de StyleBook pour le pack de configuration sélectionné. Dans ce cas, il affiche

exemple-lb-mon.

Modifier le StyleBook qui comporte plusieurs packs de configuration

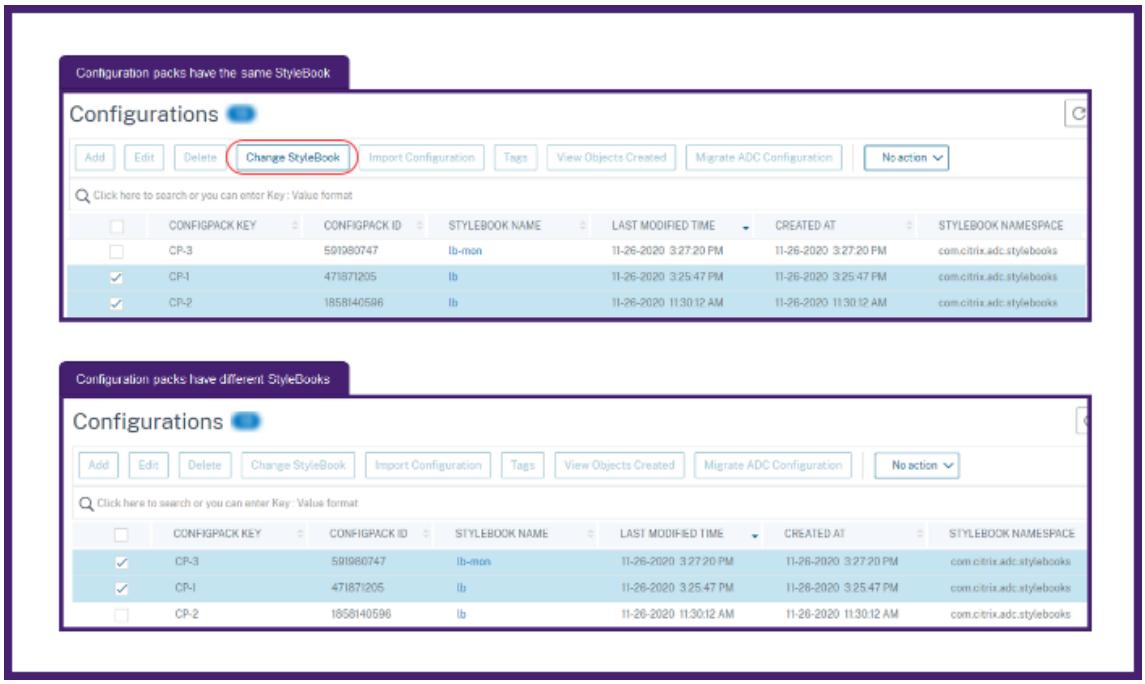
Lorsque vous modifiez un StyleBook existant qui a plusieurs packs de configuration, procédez comme suit :

1. Importez un nouveau StyleBook dans ADM.

   Généralement, le nouveau StyleBook a le même nom et l'espace de noms avec une version supérieure à celle du StyleBook existant. Toutefois, vous pouvez ignorer cette étape si le nom, l'espace de noms ou la version sont différents.

2. Modifiez le StyleBook pour les packs de configuration associés au StyleBook existant.

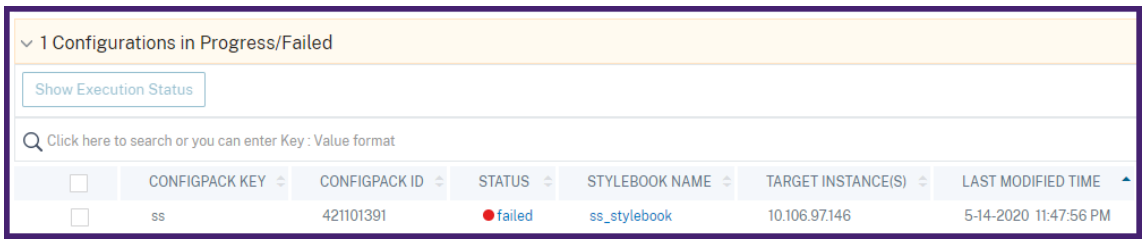
   Vous pouvez sélectionner **Modifier le livre de style** uniquement lorsque les packs de configuration sélectionnés sont associés au même StyleBook.



   Pour les packs de configuration sélectionnés, l'ADM modifie correctement le StyleBook lorsque les conditions suivantes sont remplies :

   - Tous les paramètres de configuration du StyleBook existant doivent être présents dans le StyleBook sélectionné.
   - Les nouveaux paramètres du StyleBook sélectionné sont facultatifs.

   Pour voir la progression des packs de configuration sélectionnés, sélectionnez **Configurations en cours ou en échec** dans la page **Configurations**.



3. Supprimez l'ancien StyleBook d'ADM une fois que tous les packs de configuration sont liés au nouveau StyleBook.

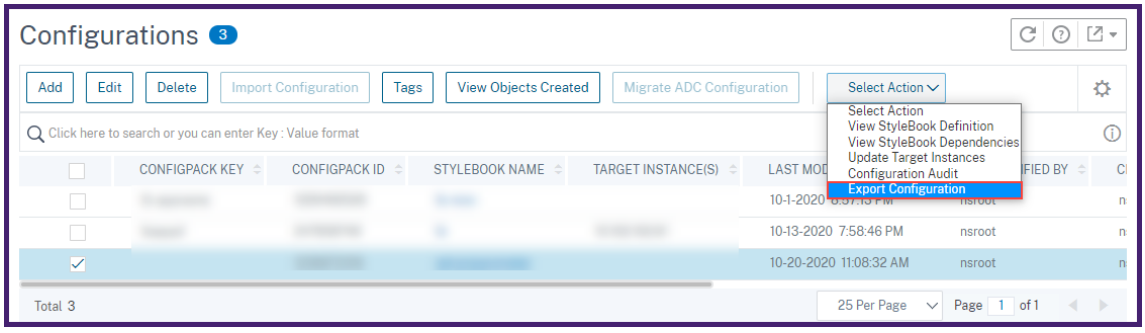
Exporter ou importer des packs de configuration

Vous pouvez exporter ou importer un pack de configuration tel que StyleBooks. Avec cette fonctionnalité, vous pouvez facilement partager la configuration de StyleBook à un autre serveur ADM. Lorsque vous exportez un pack de configuration, un `tgz` ou `zip` bundle se télécharge sur votre ordinateur local. Ce bundle inclut un fichier JSON avec tous les paramètres définis dans un pack de configuration.

Exporter la configuration

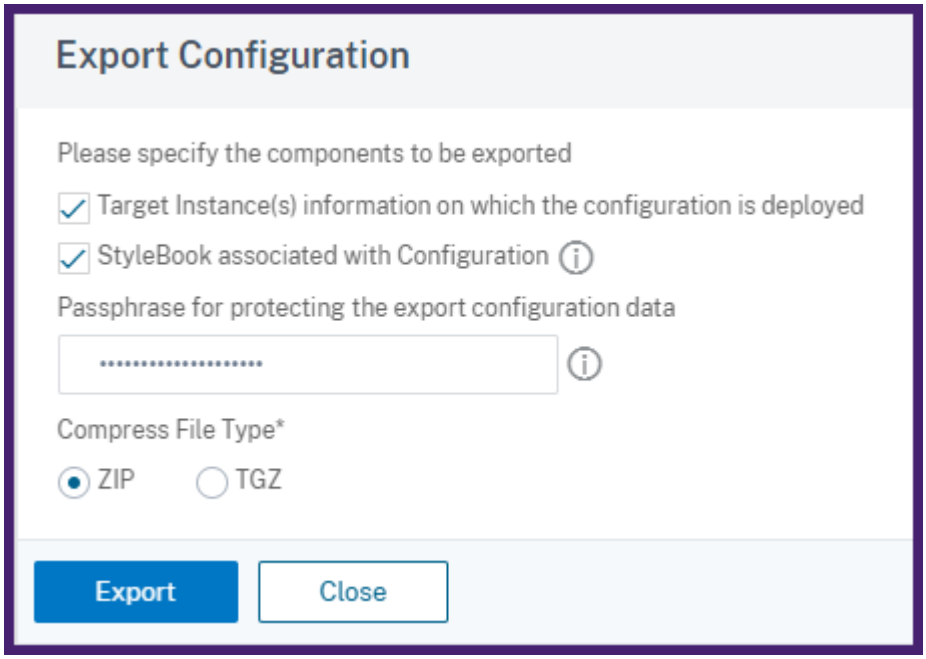
Pour exporter un pack de configuration, procédez comme suit :

1. Accédez à **Applications > StyleBooks > Configurations**.
2. Sélectionnez un pack de configuration que vous souhaitez exporter.
3. Dans **Sélectionner une action**, sélectionnez **Exporter la configuration**.



4. Dans le volet **Configuration d'exportation**, spécifiez les éléments suivants :
   - **Informations sur l'instance cible sur laquelle la configuration est déployée** : sélectionnez cette option pour inclure les informations des instances cibles dans le bundle d'exportation.
   - **StyleBook associé à Configuration** : sélectionnez cette option pour inclure le StyleBook dans l'offre groupée d'exportation.

- **phrase secrète pour protéger les données de configuration d'exportation** : spécifiez une phrase secrète pour chiffrer le bundle d'exportation. Cette phrase secrète sécurise les données sensibles d'un pack de configuration.
- **Compresser le type de fichier** : sélectionnez le type de fichier **ZIP** ou **TGZ** .



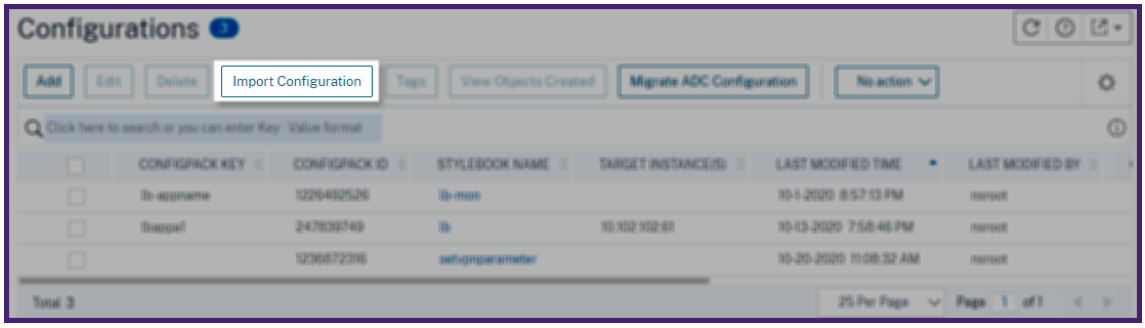
5. Cliquez sur **Exporter**.

   Enregistrez l'offre groupée d'exportation sur votre ordinateur local.

Configuration d'importation

Vous pouvez importer un pack de configuration depuis votre ordinateur local vers un autre serveur ADM. Pour importer un pack de configuration, procédez comme suit :

1. Accédez à **Applications > StyleBooks > Configurations**.
2. Sélectionnez **Importer la configuration**.



3. Choisissez le lot de fichiers d'importation à partir de votre ordinateur.

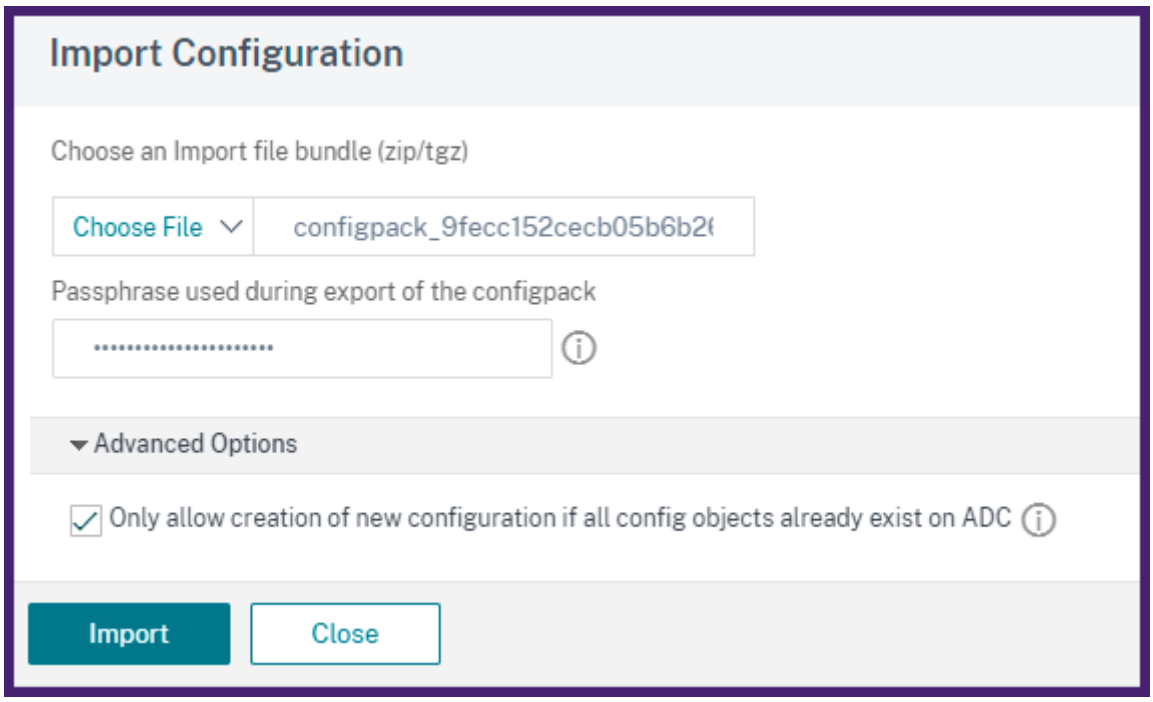
4. Utilisez la phrase secrète que vous avez spécifiée lors de l'exportation.
5. Facultatif, dans Options avancées, sélectionnez **Autoriser uniquement la création d'une nouvelle configuration si tous les objets de configuration existent déjà sur ADC**.

   Cette option ne modifie pas les objets déjà créés sur l'instance ADC.

   Considérez que vous avez ajouté la même instance ADC dans deux serveurs ADM. Et, vous souhaitez migrer un pack de configuration d'un serveur ADM vers un autre serveur. Utilisez cette option pour importer un pack de configuration sans modifier ses objets de configuration sur une instance ADC.

   > **Important**
   >
   > Pour utiliser cette option, vérifiez que le groupe de configuration spécifié dispose des informations sur les instances cibles. Consultez Exporter la configuration.
   >
   > Cette option migre la configuration uniquement si tous les objets sont présents sur l'instance cible.

6. Cliquez sur **Importer**.



Lorsque vous importez un pack de configuration, l'ADM vérifie les éléments suivants :

- **StyleBook associé** : Si le StyleBook associé n'est pas dans l'ADM, il importe le StyleBook avec le pack de configuration.
- **Instances cibles** : recherchez les instances cibles et déploie la configuration sur les instances cibles spécifiées. Si les instances ADC mentionnées sont absentes dans l'ADM, le pack de configuration est importé sans instances cibles.

- **ADM source** : si vous importez un pack de configuration sur le même serveur ADM, le bundle sélectionné met à jour le pack de configuration existant.

Créez vos StyleBooks

Le contenu complet de **example-lb** StyleBook est fourni à titre de référence comme suit :

```
name: example-lb
namespace: examples.stylebooks
version: "1.0"
display-name: Basic Load Balancer App
description: This is an example StyleBook that creates a load balancer
   application
schema-version: "1.0"
import-stylebooks:
  -
    namespace: com.citrix.adc.stylebooks
    prefix: stlb
    version: "1.0"
parameters-default-sources:
  - stlb::lb
components:
  -
    name: lb-comp
    type: stlb::lb
    description: Uses the default lb StyleBook to build the typical lb
       configuration objects
    properties-default-sources:
      - $parameters
<!--NeedCopy-->
```

Le contenu complet de **example-lb-mon** StyleBook est fourni à titre de référence comme suit :

```
name: example-lb-mon
namespace: examples.stylebooks
version: "1.0"
description: This is an example StyleBook that creates a load balancer
   application with monitors
display-name: Basic Load Balancer App with Monitors
schema-version: "1.0"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
```



```
12    -
13      namespace: com.citrix.adc.stylebooks
14      prefix: stlb
15      version: "1.0"
16    -
17      namespace: com.citrix.adc.commontypes
18      prefix: cmtypes
19      version: "1.0"
20  parameters-default-sources:
21    - stlb::lb
22  parameters:
23    -
24      name: monitors
25      label: "List of Monitors"
26      description: "List of Monitors to monitor Application Servers"
27      type: cmtypes::monitor[]
28  substitutions:
29    mon-name(appname, monname): $appname + "-mon-" + $monname
30  components:
31    -
32      name: lb-comp
33      type: stlb::lb
34      description: Uses the default lb StyleBook to build the typical lb
           configuration objects
35      properties-default-sources:
36        - $parameters
37    -
38      name: monitors-comp
39      type: cmtypes::monitor
40      condition: $parameters.monitors
41      repeat: $parameters.monitors
42      repeat-item: mon
43      repeat-index: ndx
44      description: Builds a list of Citrix ADC monitor objects and binds
           them to the servicegroup of this LB config
45      properties-default-sources:
46        - $mon
47      properties:
48          monitorname: $substitutions.mon-name($parameters.lb-appname,
              $mon.monitorname)
49      components:
50        -
51          name: monitor-svcg-binding-comp
52          condition:  $parameters.svc-servers
53          type: ns::servicegroup_lbmonitor_binding
```



```
54          properties:
55            servicegroupname: $components.lb-comp.outputs.servicegroup.
                 properties.servicegroupname
56            monitor_name: $parent.properties.monitorname
57  <!--NeedCopy-->
```

Déploiement de configurations GSLB à l'aide de noms de domaine DNS

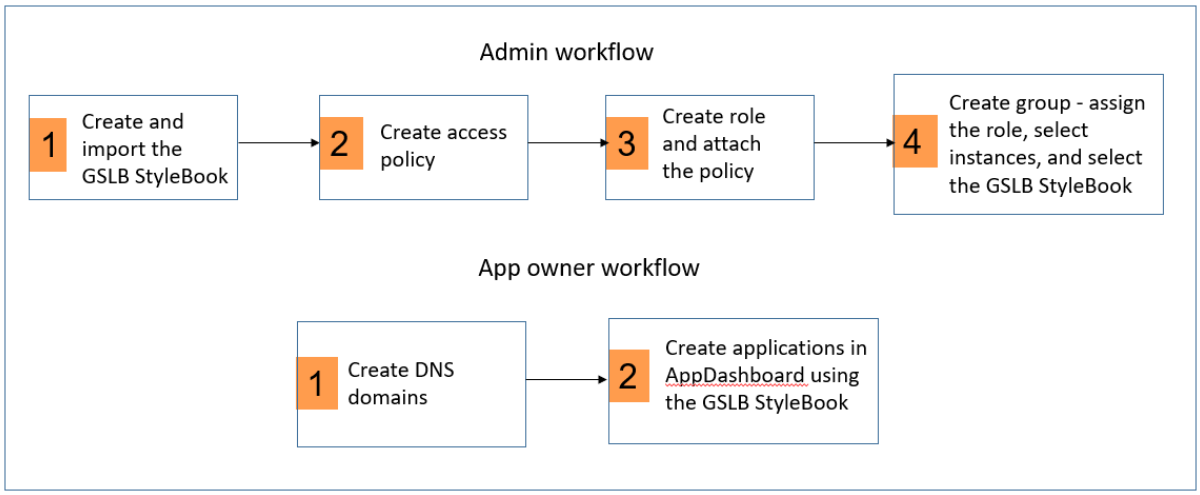
April 29, 2021

Les nouvelles améliorations du RBAC dans Citrix Application Delivery Management (ADM) permettent uniquement aux propriétaires d'applications autorisés de créer et de gérer leurs propres domaines DNS dans Citrix ADM. Vous pouvez désormais autoriser les propriétaires d'applications à créer des configurations GSLB à partir des domaines DNS qu'ils possèdent, à l'aide de StyleBooks spécifiques. Si le nom de domaine DNS sélectionné appartient à l'utilisateur, il peut être utilisé lors de la création de configurations GSLB à l'aide de GSLB StyleBooks dans le tableau de bord de l'application Citrix ADM.

Il existe deux flux de travail dans Citrix ADM pour configurer les configurations GSLB.

1. **Workflow pour les administrateurs**. Configurez l'environnement RBAC dans Citrix ADM. Autrement dit, pour créer et importer des StyleBooks GSLB, vous devez créer des groupes d'utilisateurs, des stratégies et des rôles et affecter des utilisateurs au groupe. En tant qu'administrateur, vous devez effectuer ce workflow.
2. **Workflow pour les propriétaires d'applications**. Les propriétaires d'applications doivent créer des configurations GSLB à l'aide des noms de domaine qu'ils possèdent.

L'organigramme suivant illustre les deux workflows :



Workflow pour les administrateurs

En tant qu'administrateur, votre workflow pour créer un environnement RBAC dans Citrix ADM comprend les étapes suivantes :

Tout d'abord, créez un StyleBook pour déployer des configurations GSLB sur les instances de Citrix ADC. Ce document fournit un exemple de contenu YAML pour vous aider à créer votre propre StyleBook -Créez votre StyleBook.

Pour plus d'informations sur la création de StyleBooks personnalisés, reportez-vous à la sectionCréer et utiliser des StyleBooks personnalisés.

> **Remarque**
>
> Citrix ADM prend en charge une nouvelle construction dans StyleBooks appelée "allowed-dynamic-values." Cette construction peut être utilisée pour permettre à l'utilisateur de lister et de sélectionner les valeurs de domaine DNS présentes dans Citrix ADM pour remplir automatiquement le paramètre « domain-name » dans le StyleBook dans l'interface graphique Citrix ADM.

Un exemple de section de paramètre « domain-name » est fourni à titre de référence.

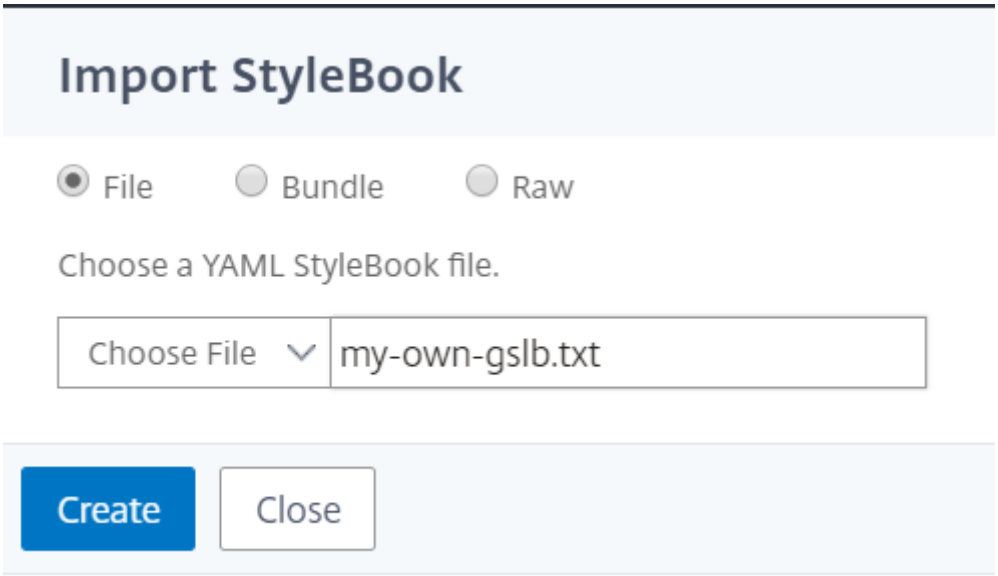
Le paramètre « domain-name » utilisé ici n'est qu'un exemple. Le paramètre peut être différent dans votre StyleBook personnalisé.

```
1  -
2    name: domain-name
3     label: DNS Domain Name
4     description: GSLB DNS Domain Name
5     type: string
6     required: true
7     allowed-dynamic-values:
8        source: local
9        resource-type: dns_domain_entry
10 <!--NeedCopy-->
```

> **Remarque**
>
> Actuellement dans Citrix ADM, la construction « allowed-dynamic-values » n'est utilisée dans aucun des StyleBooks par défaut. Créez un nouveau StyleBook GSLB personnalisé à l'aide du StyleBook GSLB par défaut. Remplacez la partie pour le paramètre de nom de domaine par l'exemple fourni ci-dessus. Vous pouvez utiliser n'importe quel éditeur de texte pour créer de nouveaux StyleBooks.

1. Connectez-vous à Citrix ADM en tant qu'administrateur.
2. Accédez à **Applications** > **Configurations** > **StyleBooks**.

3. Cliquez sur **Importer un nouveau styleBook** et téléchargez le nouveau styleBook GSLB sur Citrix ADM.



   Pour plus d'informations sur l'importation de StyleBooks dans Citrix ADM, reportez-vous à la sectionUtiliser des StyleBooks personnalisés.

4. Accédez à **Système** > **Utilisateurs** > **Stratégies**, puis cliquez sur **Ajouter** pour configurer une stratégie d'accès pour les propriétaires d'applications, comme indiqué ci-dessous.

   Citrix vous recommande de créer une stratégie d'accès pour vous assurer que les propriétaires d'applications n'échappent pas aux règles RBAC définies par vous.

5. Tapez un nom pour la stratégie et une brève description. Dans la section Autorisations, assurez-vous que les autorisations d'affichage suivantes sont vérifiées de manière obligatoire.

   a) Applications > Tableau de bord

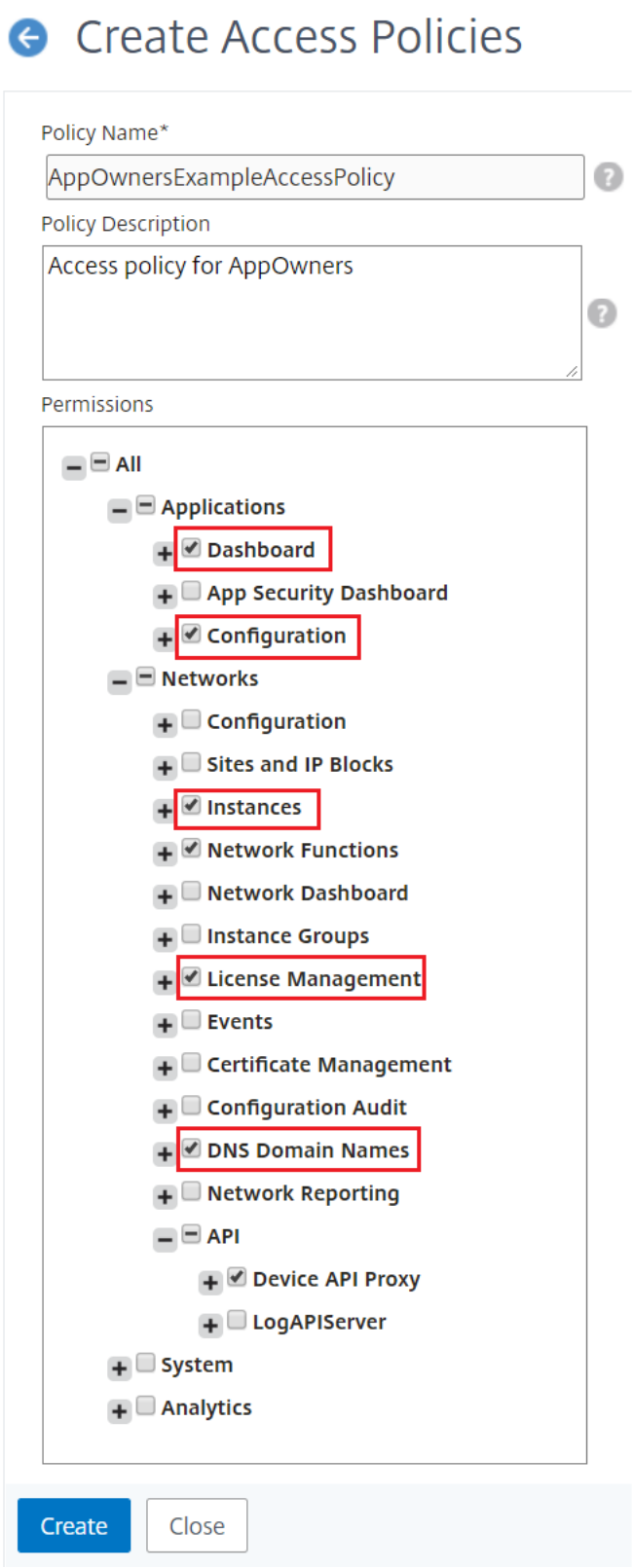
   b) Applications > Configurations

   c) Réseaux > Instances

   d) Réseaux > Gestion des licences

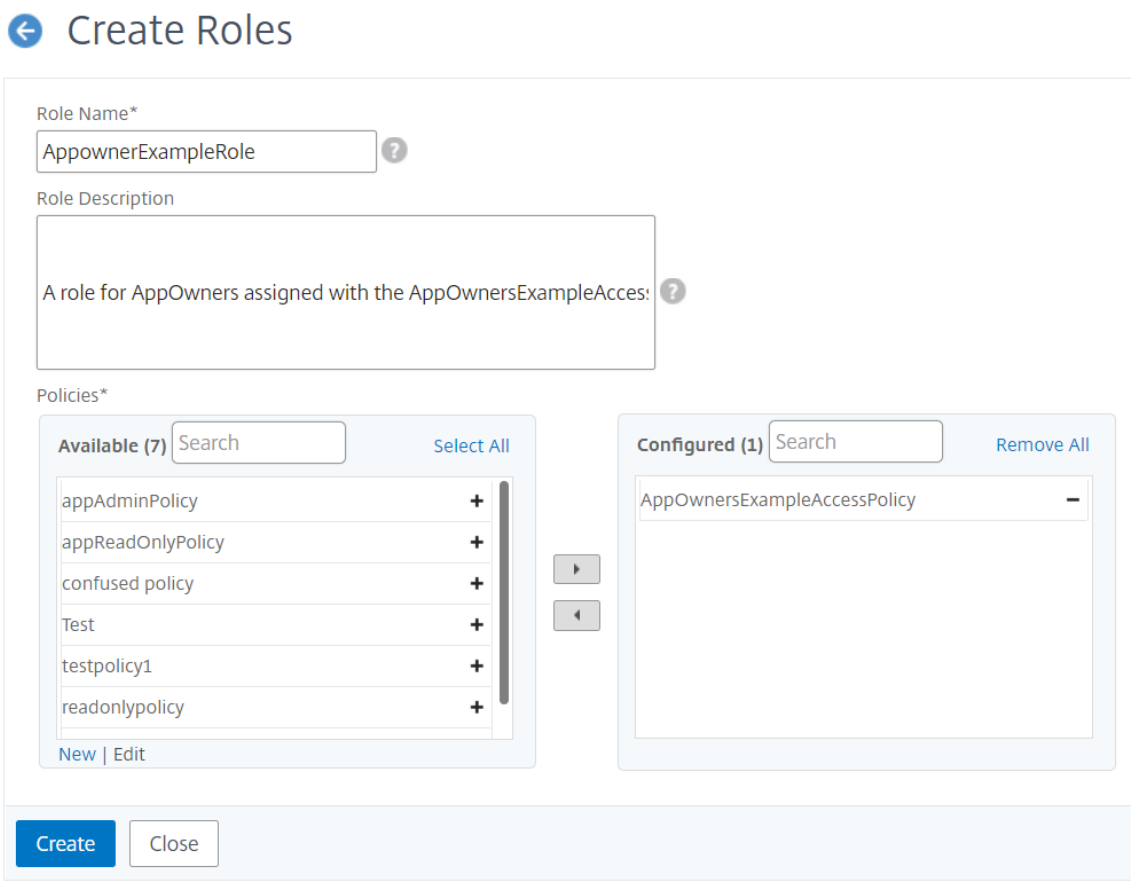
   e) Réseaux > Noms de domaine DNS

   Vous pouvez fournir d'autres autorisations, le cas échéant, puis cliquez sur **Créer**.

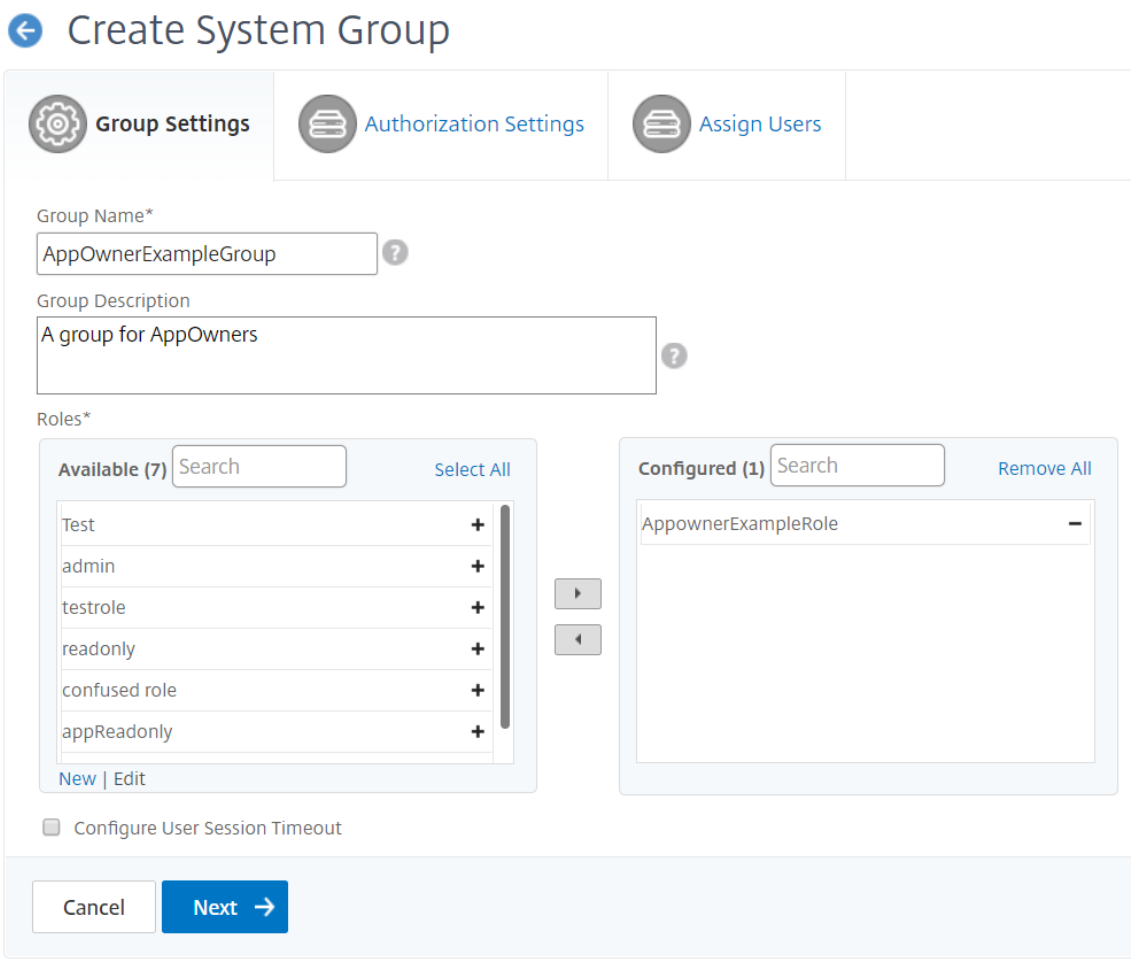


6. Accédez à **Système** > **Utilisateurs** > **Rôles** et créez un rôle et affectez la stratégie créée à l'étape précédente.

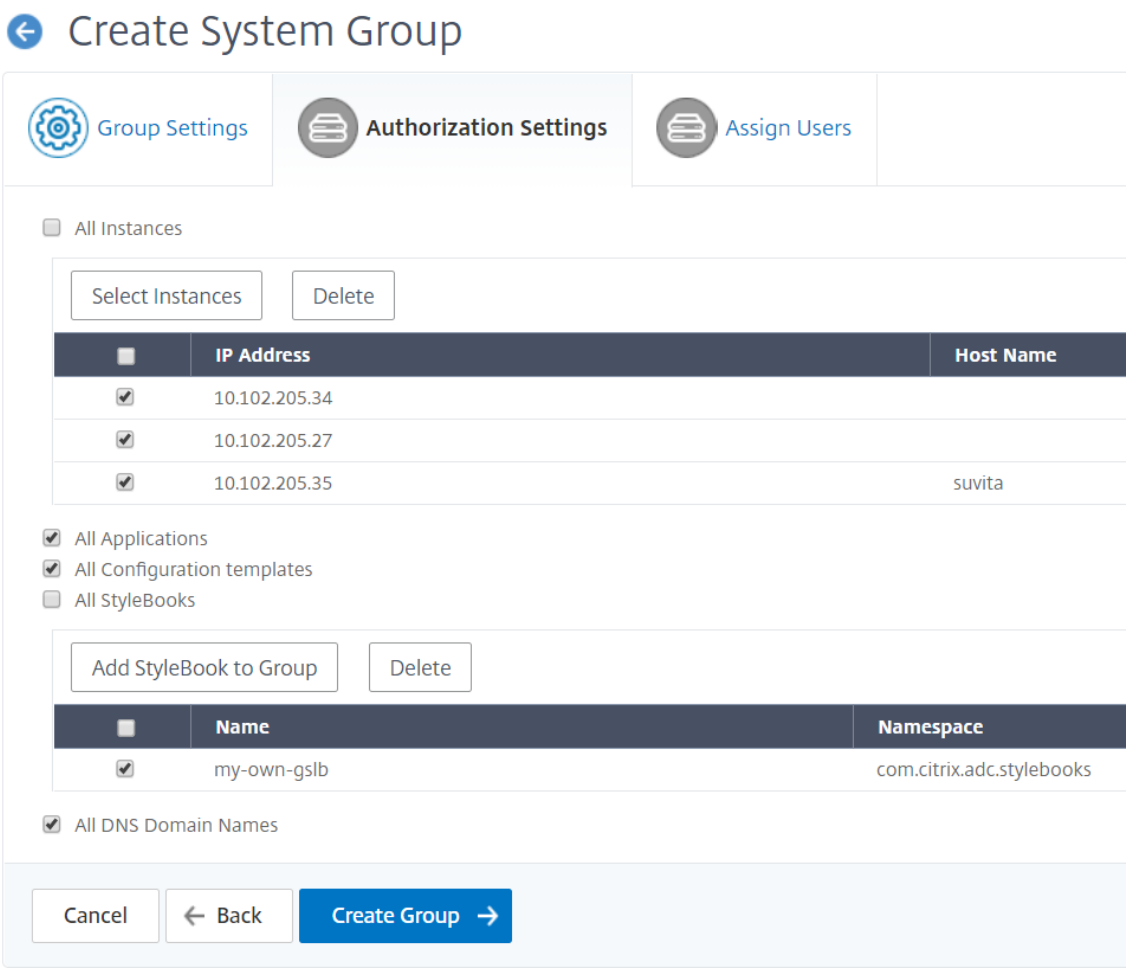
7. Tapez un nom pour le rôle et fournissez une brève description. Dans la section Stratégies, sélectionnez **AppownerExampleAccessPolicy**.



8. Accédez à **Système** > **Utilisateurs** > **Groupes**, créez un groupe et associez le rôle créé à l'étape précédente.
9. Tapez un nom et une description, puis dans la section Rôles, sélectionnez **AppownerExample-Role**.



10. Cliquez sur **Suivant**.
11. Dans l'onglet **Paramètres d'autorisation**, sélectionnez les instances de Citrix ADC auxquelles le propriétaire de l'application a accès et le nouveau StyleBook GSLB.

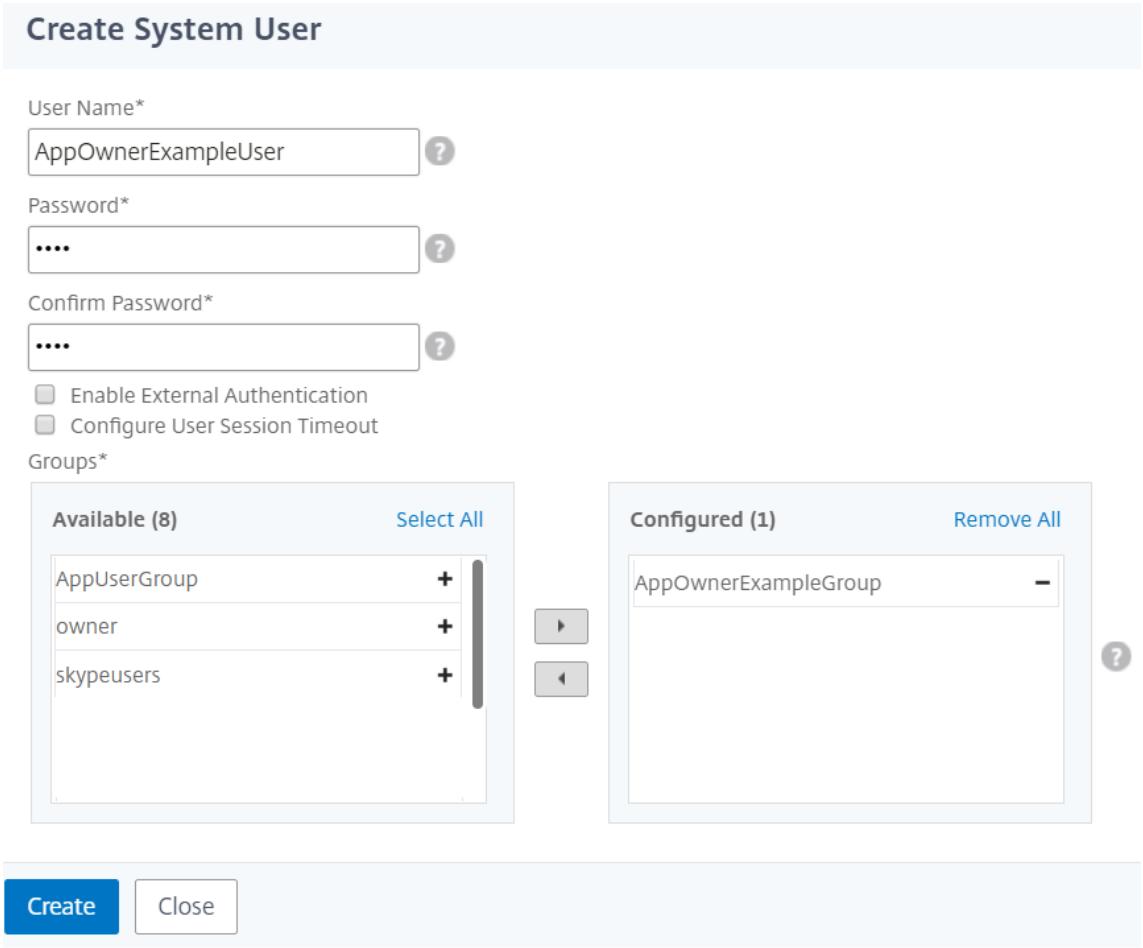


Répétez cette étape pour créer autant de groupes d'utilisateurs que nécessaire dans votre organisation. Cliquez sur **Créer un groupe**.

12. Créez un utilisateur système et affectez l'utilisateur à un groupe d'utilisateurs. Ce document fait référence uniquement aux utilisateurs créés localement. Vous n'avez pas besoin de créer des utilisateurs dans des groupes d'utilisateurs si Citrix ADM est configuré pour utiliser l'authentification externe, par exemple LDAP. Le mappage des utilisateurs vers des groupes est extrait du répertoire d'authentification externe.

    a) Accédez à **Système** > **Utilisateurs** > **Utilisateur** .

    b) Tapez un nom d'utilisateur et un mot de passe pour l'utilisateur système et affectez l'utilisateur au groupe.



> **Remarque**L'
>
> étape 12 est facultative et n'est pas requise si une authentification externe telle que LDAP est utilisée.

API REST Citrix ADM pour le workflow d'administration

API REST pour se connecter à Citrix ADM

```
URL: http: //<MAS_IP>/nitro/v2/config/login
HTTPMETHOD: POST

Body Payload:
{

  "login": {

    "username": "<USER_NAME>",
    "password": "<PASSWORD>",
```



```
    "session_timeout": 1800
   }

 }


The response results in a session cookie header, that can be sent with
   the rest of the API requests below.

Set-Cookie: SESSID=##
   ED31F7C886E248CCDCA8F0E0AD2AA511ACCC5F46C48D6D2BCAA719A9DE62;path=/;
   secure;HttpOnly
<!--NeedCopy-->
```

API REST pour créer une stratégie d'accès

```
URL: https://<MAS_IP>/nitro/v2/config/rba_policy
HTTP METHOD: POST

{

  "rba_policy": {

    "name": " AppOwnerAccessPolicy",
    "description": " ExampleCompany AppOwner Access Policy",
    "tenant_id": "7c12ec97-1472-4096-97e7-a5acb453cc5c",
    "statement": [
      {

        "access_type": true,
        "resource_type": "application",
        "operation_name": "add",
        "dependent_resources": "mail_profile,slack_profile,smtp_server,
           app_category"
       }
 ,
      {

        "access_type": true,
        "resource_type": "application",
        "operation_name": "get",
        "dependent_resources": "download,smtp_server,ns_vserver_license
           ,app_category,app_summary,app_health_dashboard_details,
           haproxy_frontend,haproxy_backend,haproxy_frontend_stats"
```



```
26          }
27    ,
28          {
29
30            "access_type": true,
31            "resource_type": "si_app_unit",
32            "operation_name": "get",
33            "dependent_resources": "download,smtp_server,app_summary,
                 si_app_summary,si_device,security_app_dashboard_details,
                 si_geo_location,si_safety_app_firewall,si_safety_overview,
                 si_safety_security_check,si_safety_system_security,
                 si_safety_signature"
34          }
35    ,
36          {
37
38            "access_type": true,
39            "resource_type": "stylebooks",
40            "operation_name": "get",
41            "dependent_resources": "download,smtp_server,ns_vserver_license
                 "
42          }
43    ,
44          {
45
46            "access_type": true,
47            "resource_type": "stylebooks",
48            "operation_name": "add",
49            "dependent_resources": "mail_profile,slack_profile,smtp_server"
50          }
51    ,
52          {
53
54            "access_type": true,
55            "resource_type": "configpacks",
56            "operation_name": "get",
57            "dependent_resources": "download,smtp_server,stylebooks,
                 ns_vserver_license"
58          }
59    ,
60          {
61
62            "access_type": true,
63            "resource_type": "configpacks",
64            "operation_name": "add",
```



```
65          "dependent_resources": "mail_profile,slack_profile,smtp_server"
66        }
67  ,
68        {
69
70          "access_type": true,
71          "resource_type": "stylebooks_system_settings",
72          "operation_name": "get",
73          "dependent_resources": "download,smtp_server"
74        }
75  ,
76        {
77
78          "access_type": true,
79          "resource_type": "stylebooks_system_settings",
80          "operation_name": "add",
81          "dependent_resources": "mail_profile,slack_profile,smtp_server"
82        }
83  ,
84        {
85
86          "access_type": true,
87          "resource_type": "ns_crvserver",
88          "operation_name": "get",
89          "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                perf_cache_redirection_report,poll_activity_status,
                ns_emon_poll_policy,lb_export_report"
90        }
91  ,
92        {
93
94          "access_type": true,
95          "resource_type": "ns_crvserver",
96          "operation_name": "add",
97          "dependent_resources": "DeviceAPIProxy,mail_profile,
                slack_profile,smtp_server,poll_activity_status,
                ns_emon_poll_policy,lb_export_report"
98        }
99  ,
100       {
101
102         "access_type": true,
103         "resource_type": "haproxy_frontend",
104         "operation_name": "get",
105         "dependent_resources": "download,DeviceAPIProxy,smtp_server,
```



```
                haproxy_backend,haproxy_server"
106          }
107    ,
108          {
109
110            "access_type": true,
111            "resource_type": "haproxy_frontend",
112            "operation_name": "add",
113            "dependent_resources": "DeviceAPIProxy,mail_profile,
                   slack_profile,smtp_server"
114          }
115    ,
116          {
117
118            "access_type": true,
119            "resource_type": "ns_server",
120            "operation_name": "get",
121            "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                   ns_emon_poll_policy,poll_activity_status,ns_server,
                   lb_export_report"
122          }
123    ,
124          {
125
126            "access_type": true,
127            "resource_type": "ns_server",
128            "operation_name": "add",
129            "dependent_resources": "DeviceAPIProxy,mail_profile,
                   slack_profile,smtp_server,ns_emon_poll_policy,
                   poll_activity_status,lb_export_report"
130          }
131    ,
132          {
133
134            "access_type": true,
135            "resource_type": "ns_lbvserver",
136            "operation_name": "get",
137            "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                   perf_lb_vserver_report,ns_emon_poll_policy,
                   poll_activity_status,lb_export_report"
138          }
139    ,
140          {
141
142            "access_type": true,
```



```
143           "resource_type": "ns_lbvserver",
144           "operation_name": "add",
145           "dependent_resources": "DeviceAPIProxy,mail_profile,
                  slack_profile,smtp_server,ns_emon_poll_policy,
                  poll_activity_status,lb_export_report"
146          }
147    ,
148         {
149
150           "access_type": true,
151           "resource_type": "ns_service",
152           "operation_name": "get",
153           "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                  ns_emon_poll_policy,poll_activity_status,
                  ns_visualizer_lb_bindings,lb_export_report"
154          }
155    ,
156         {
157
158           "access_type": true,
159           "resource_type": "ns_service",
160           "operation_name": "add",
161           "dependent_resources": "DeviceAPIProxy,mail_profile,
                  slack_profile,smtp_server,ns_emon_poll_policy,
                  poll_activity_status,ns_visualizer_lb_bindings,
                  lb_export_report"
162          }
163    ,
164         {
165
166           "access_type": true,
167           "resource_type": "ns_servicegroup",
168           "operation_name": "get",
169           "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                  ns_emon_poll_policy,poll_activity_status,
                  ns_servicegroupmember_binding,ns_visualizer_lb_bindings,
                  lb_export_report"
170          }
171    ,
172         {
173
174           "access_type": true,
175           "resource_type": "ns_servicegroup",
176           "operation_name": "add",
177           "dependent_resources": "DeviceAPIProxy,mail_profile,
```



```
                slack_profile,smtp_server,ns_emon_poll_policy,
                poll_activity_status,ns_servicegroupmember_binding,
                ns_visualizer_lb_bindings,lb_export_report"
178          }
179    ,
180          {
181
182            "access_type": true,
183            "resource_type": "ns_authenticationvserver",
184            "operation_name": "get",
185            "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                   perf_authentication_report,poll_activity_status,
                   ns_emon_poll_policy,lb_export_report"
186          }
187    ,
188          {
189
190            "access_type": true,
191            "resource_type": "ns_authenticationvserver",
192            "operation_name": "add",
193            "dependent_resources": "DeviceAPIProxy,mail_profile,
                   slack_profile,smtp_server,poll_activity_status,
                   ns_emon_poll_policy,lb_export_report"
194          }
195    ,
196          {
197
198            "access_type": true,
199            "resource_type": "syslog_messages",
200            "operation_name": "get",
201            "dependent_resources": "download,smtp_server"
202          }
203    ,
204          {
205
206            "access_type": true,
207            "resource_type": "ns_emon_poll_policy",
208            "operation_name": "get",
209            "dependent_resources": "download,poll_activity_status,
                   smtp_server"
210          }
211    ,
212          {
213
214            "access_type": true,
```



```
215           "resource_type": "ns_emon_poll_policy",
216           "operation_name": "add",
217           "dependent_resources": "download,poll_activity_status,
                 mail_profile,slack_profile,smtp_server"
218         }
219   ,
220         {
221
222           "access_type": true,
223           "resource_type": "ns_visualizer_gslb_bindings",
224           "operation_name": "add",
225           "dependent_resources": "DeviceAPIProxy,mail_profile,
                 slack_profile,smtp_server,poll_activity_status,
                 ns_emon_poll_policy,ns_gslbvserver_domain,lb_export_report"
226         }
227   ,
228         {
229
230           "access_type": true,
231           "resource_type": "ns_visualizer_gslb_bindings",
232           "operation_name": "get",
233           "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                 poll_activity_status,ns_emon_poll_policy,
                 ns_gslbvserver_domain,lb_export_report"
234         }
235   ,
236         {
237
238           "access_type": true,
239           "resource_type": "ns_gslbservice",
240           "operation_name": "add",
241           "dependent_resources": "DeviceAPIProxy,mail_profile,
                 slack_profile,smtp_server,poll_activity_status,
                 ns_emon_poll_policy,lb_export_report"
242         }
243   ,
244         {
245
246           "access_type": true,
247           "resource_type": "ns_gslbservice",
248           "operation_name": "get",
249           "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                 poll_activity_status,ns_emon_poll_policy,lb_export_report"
250         }
251   ,
```



```
252         {
253
254           "access_type": true,
255           "resource_type": "ns_gslbvserver",
256           "operation_name": "get",
257           "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                 perf_global_server_load_balancing_report,
                 poll_activity_status,ns_emon_poll_policy,lb_export_report"
258          }
259   ,
260         {
261
262           "access_type": true,
263           "resource_type": "ns_gslbvserver",
264           "operation_name": "add",
265           "dependent_resources": "DeviceAPIProxy,mail_profile,
                 slack_profile,smtp_server,poll_activity_status,
                 ns_emon_poll_policy,lb_export_report"
266         }
267   ,
268         {
269
270           "access_type": true,
271           "resource_type": "ns_vpnvserver",
272           "operation_name": "add",
273           "dependent_resources": "DeviceAPIProxy,mail_profile,
                 slack_profile,smtp_server,poll_activity_status,
                 ns_emon_poll_policy,lb_export_report"
274          }
275   ,
276         {
277
278           "access_type": true,
279           "resource_type": "ns_vpnvserver",
280           "operation_name": "get",
281           "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                 perf_ssl_vpn_report,poll_activity_status,ns_emon_poll_policy
                 ,lb_export_report"
282          }
283   ,
284         {
285
286           "access_type": true,
287           "resource_type": "ns_csvserver",
288           "operation_name": "get",
```



```
289           "dependent_resources": "download,DeviceAPIProxy,smtp_server,
                  perf_content_switching_report,ns_emon_poll_policy,
                  poll_activity_status,ns_visualizer_cs_bindings,
                  lb_export_report"
290         }
291   ,
292         {
293
294           "access_type": true,
295           "resource_type": "ns_csvserver",
296           "operation_name": "add",
297           "dependent_resources": "DeviceAPIProxy,mail_profile,
                  slack_profile,smtp_server,ns_emon_poll_policy,
                  poll_activity_status,ns_visualizer_cs_bindings,
                  lb_export_report"
298         }
299   ,
300         {
301
302           "access_type": true,
303           "resource_type": "dns_domain_entry",
304           "operation_name": "get",
305           "dependent_resources": ""
306         }
307   ,
308         {
309
310           "access_type": true,
311           "resource_type": "dns_domain_entry",
312           "operation_name": "add",
313           "dependent_resources": ""
314         }
315   ,
316         {
317
318           "access_type": true,
319           "resource_type": "devicewise_detail_summary",
320           "operation_name": "get",
321           "dependent_resources": "download,mps_user_heatmap,ns_event,
                  mps_agent,active_event,smtp_server,mps_datacenter,
                  event_severity_report,event_device_report,ns_conf,
                  device_event_summary"
322         }
323   ,
324         {
```



```
325
326           "access_type": true,
327           "resource_type": "devicewise_detail_summary",
328           "operation_name": "add",
329           "dependent_resources": "mail_profile,slack_profile,smtp_server"
330         }
331   ,
332         {
333
334           "access_type": true,
335           "resource_type": "cbwanopt",
336           "operation_name": "get",
337           "dependent_resources": "download,device_backup,traceroute,
                inventory,inventory_status,ping,mps_datacenter,
                cbwanopt_device_profile,sdwanvw_device_profile,
                sdwanvw_snmp_config,sdwanvw_appflowconfig,smtp_server,
                cbwanopt_snmp_config,cbwanopt_appflowconfig,sdwanvw,tag"
338         }
339   ,
340         {
341
342           "access_type": true,
343           "resource_type": "cbwanopt",
344           "operation_name": "add",
345           "dependent_resources": "inventory,managed_device,device_backup,
                upload,cbwanopt_device_profile,mps_datacenter,mail_profile,
                slack_profile,smtp_server,sdwanvw_device_profile,
                sdwanvw_snmp_config,sdwanvw_appflowconfig,
                cbwanopt_snmp_config,cbwanopt_appflowconfig,sdwanvw,tag"
346         }
347   ,
348         {
349
350           "access_type": true,
351           "resource_type": "device_login",
352           "operation_name": "get",
353           "dependent_resources": ""
354         }
355   ,
356         {
357
358           "access_type": true,
359           "resource_type": "ns",
360           "operation_name": "get",
361           "dependent_resources": "download,ns_config_replicate,ns_conf,
```



```
                ns_ns_runningconfig,ns_ns_savedconfig,active_event,
                device_backup,traceroute,inventory,inventory_status,ping,
                ns_device_profile,nssdx_device_profile,sdx_snmp_config,
                sdx_syslog_config,smtp_server,ns_cluster,ns_snmp_config,
                ns_syslog_config,ns_l7_latency_config,ica_l7_latency_update,
                af_vserver_policy,ns_vserver_appflow_config,mps_datacenter,
                ns_appflow_param_config,ns_ns_license,ns_ns_mode,
                ns_network_interface,advanced_analytics_config,tag"
362          }
363    ,
364          {
365
366            "access_type": true,
367            "resource_type": "ns",
368            "operation_name": "add",
369            "dependent_resources": "inventory,ns_l7_latency_config,
                   ica_l7_latency_update,af_vserver_policy,ns_config_replicate,
                   managed_device,device_backup,upload,ns_device_profile,
                   nssdx_device_profile,mps_datacenter,sdx_snmp_config,
                   sdx_syslog_config,mail_profile,slack_profile,smtp_server,
                   ns_cluster,ns_snmp_config,ns_syslog_config,
                   ns_vserver_appflow_config,ns_appflow_param_config,
                   advanced_analytics_config,tag"
370          }
371    ,
372          {
373
374            "access_type": true,
375            "resource_type": "haproxyhost",
376            "operation_name": "get",
377            "dependent_resources": "download,traceroute,inventory,
                   inventory_status,ping,mps_datacenter,smtp_server,
                   haproxy_device_profile,device_backup,tag"
378          }
379    ,
380          {
381
382            "access_type": true,
383            "resource_type": "haproxyhost",
384            "operation_name": "add",
385            "dependent_resources": "inventory,managed_device,mail_profile,
                   slack_profile,smtp_server,mps_datacenter,
                   haproxy_device_profile,haproxy,device_backup,tag"
386          }
387    ,
```



```
388         {
389
390           "access_type": true,
391           "resource_type": "docker_host",
392           "operation_name": "add",
393           "dependent_resources": "inventory,ns_snmp_config,managed_device
                 ,ns,upload,mail_profile,slack_profile,smtp_server,
                 mps_datacenter,ns_device_profile,docker_nscpx_image"
394          }
395    ,
396         {
397
398           "access_type": true,
399           "resource_type": "docker_host",
400           "operation_name": "get",
401           "dependent_resources": "download,ns_snmp_config,ns_conf,
                 ns_ns_runningconfig,ns_ns_savedconfig,smtp_server,
                 mps_datacenter,ns_device_profile,traceroute,inventory,
                 inventory_status,ping,active_event,ns_ns_license,ns_ns_mode,
                 ns_network_interface"
402          }
403    ,
404         {
405
406           "access_type": true,
407           "resource_type": "perf_reports",
408           "operation_name": "add",
409           "dependent_resources": "mail_profile,slack_profile,smtp_server,
                 perf_custom_dashboard"
410          }
411    ,
412         {
413
414           "access_type": true,
415           "resource_type": "perf_reports",
416           "operation_name": "get",
417           "dependent_resources": "download,smtp_server,
                 perf_report_counters,perf_res_util_report,
                 perf_http_req_tcp_conn_report,perf_lb_ssl_traffic_report,
                 perf_ip_bytes_rxtx_report,perf_ip_pkt_rxtx_report,
                 perf_icmp_pkt_rxtx_report,perf_icmp_bytes_rxtx_report,
                 perf_icmpv6_pkt_rxtx_report,perf_icmpv6_bytes_rxtx_report,
                 perf_ipv6_bytes_rxtx_report,perf_ipv6_pkt_rxtx_report,
                 perf_udp_bytes_rxtx_report,perf_udp_packets_rxtx_report,
                 perf_cmp_bytes_rxtx_report,perf_cmp_tcp_bytes_rxtx_report,
```



```
                perf_cmp_tcp_ratiosaving_report,
                perf_cmp_decmp_bytes_rxtx_report,
                perf_cmp_decmp_ratiosaving_report,
                perf_tcp_server_conn_report,
                perf_tcp_surgelen_spareconn_report,perf_http_bytes_rx_report
                ,perf_http_gets_posts_report,
                perf_ssl_transactions_hits_report,
                perf_ssl_client_auth_report,perf_ssl_rsa_dhkey_report,
                perf_ssl_frontend_ciphers_report,
                perf_ssl_backend_ciphers_report,
                perf_wsdevice_cpu_utilization_report,
                perf_wsdevice_send_compression_ratio_report,
                perf_wsdevice_connected_plugins_report,
                perf_wsdevice_data_reduction_report,
                perf_wsdevice_link_utilization_report,
                perf_wsserviceclassstatstable_pass_through_connection_report
                ,perf_wsserviceclassstatstable_service_class_report,
                perf_wsserviceclassstatstable_acceleration_report,
                perf_wslinkstatstable_throughput_report,
                perf_wslinkstatstable_packet_loss_report,
                perf_wsappstatstable_application_report,
                perf_wsqosstatstable_qos_report,
                perf_ssl_cpu_keyexchange_report,perf_ssl_be_rsa_dhkey_report
                ,perf_custom_dashboard,perf_ns_throughput_report,
                perf_network_interface_report"
418          }
419    ,
420          {
421
422            "access_type": true,
423            "resource_type": "perf_threshold",
424            "operation_name": "get",
425            "dependent_resources": "download,perf_reports,
                   perf_report_counters,smtp_server,sms_server,sms_profile"
426          }
427    ,
428          {
429
430            "access_type": true,
431            "resource_type": "perf_threshold",
432            "operation_name": "add",
433            "dependent_resources": "mail_profile,slack_profile,smtp_server,
                   sms_server,sms_profile"
434          }
435    ,
```



```
436         {
437
438           "access_type": true,
439           "resource_type": "perf_poll_config",
440           "operation_name": "add",
441           "dependent_resources": "mail_profile,slack_profile,smtp_server"
442          }
443   ,
444         {
445
446           "access_type": true,
447           "resource_type": "perf_poll_config",
448           "operation_name": "get",
449           "dependent_resources": "smtp_server,download"
450          }
451   ,
452         {
453
454           "access_type": true,
455           "resource_type": "license_server_info",
456           "operation_name": "get",
457           "dependent_resources": "sms_server,license_proxy_server,
                 jazz_license,download,sms_profile,smtp_server,
                 user_managed_tp_vserver,managed_vserver,user_managed_vserver
                 ,haproxy_frontend,haproxy_backend,license_file,
                 device_license_info,license_info,ns_authenticationvserver,
                 ns_gslbvserver,ns_vpnvserver,ns_csvserver,ns_crvserver,
                 ns_lbvserver,autoselection_preference,license_threshold,
                 license_expiry_info"
458          }
459   ,
460         {
461
462           "access_type": true,
463           "resource_type": "license_server_info",
464           "operation_name": "add",
465           "dependent_resources": "sms_server,license_proxy_server,
                 jazz_license,sms_profile,mail_profile,slack_profile,
                 smtp_server,user_managed_tp_vserver,managed_vserver,upload,
                 license_file,license_info,license_threshold,mas_license,
                 user_managed_vserver,autoselection_preference,
                 license_expiry_info"
466          }
467
468      ],
```



```
469     "ui": [
470       {
471
472         "access_type": true,
473         "name": "ApplicationsDashboard",
474         "display_name": "Dashboard"
475        }
476   ,
477       {
478
479         "access_type": true,
480         "name": "SecurityDashboard",
481         "display_name": "App Security Dashboard"
482        }
483   ,
484       {
485
486         "access_type": true,
487         "name": "Stylebooks",
488         "display_name": "StyleBooks"
489        }
490   ,
491       {
492
493         "access_type": true,
494         "name": "Stylebooks",
495         "display_name": "Configpacks"
496        }
497   ,
498       {
499
500         "access_type": true,
501         "name": "StylebooksSettings",
502         "display_name": "Settings"
503        }
504   ,
505       {
506
507         "access_type": true,
508         "name": "CacheRedirection",
509         "display_name": "Cache Redirection"
510        }
511   ,
512       {
513
```



```
          "access_type": true,
          "name": "HAProxy",
          "display_name": "HAProxy"
        }
  ,
      {

          "access_type": true,
          "name": "Servers",
          "display_name": "Servers"
        }
  ,
      {

          "access_type": true,
          "name": "VirtualServers",
          "display_name": "Virtual Servers"
        }
  ,
      {

          "access_type": true,
          "name": "Services",
          "display_name": "Services"
        }
  ,
      {

          "access_type": true,
          "name": "ServiceGroups",
          "display_name": "Service Groups"
        }
  ,
      {

          "access_type": true,
        "name": "Authentication",
          "display_name": "Authentication"
        }
  ,
      {

          "access_type": true,
          "name": "MonitoringAuditing",
          "display_name": "Auditing"
```



```
559         }
560   ,
561         {
562
563           "access_type": true,
564           "name": "MonitoringSettings",
565           "display_name": "Settings"
566         }
567   ,
568         {
569
570           "access_type": true,
571           "name": "GSLBDomains",
572           "display_name": "Domains"
573         }
574   ,
575         {
576
577           "access_type": true,
578           "name": "GSLBServices",
579           "display_name": "Services"
580         }
581   ,
582         {
583
584           "access_type": true,
585           "name": "GSLBVirtualServer",
586           "display_name": "Virtual Server"
587         }
588   ,
589         {
590
591           "access_type": true,
592           "name": "NetScalerGateway",
593           "display_name": "NetScaler Gateway"
594         }
595   ,
596         {
597
598           "access_type": true,
599           "name": "ContentSwitching",
600           "display_name": "Content Switching"
601         }
602   ,
603         {
```



```
604
605           "access_type": true,
606           "name": "DNSDomainNames",
607           "display_name": "DNS Domain Names"
608         }
609   ,
610         {
611
612           "access_type": true,
613           "name": "NetworkDashboard",
614           "display_name": "Instances Dashboard"
615         }
616   ,
617         {
618
619           "access_type": true,
620           "name": "NetScalerSDWANWOInstances",
621           "display_name": "NetScaler SD-WAN"
622         }
623   ,
624         {
625
626           "access_type": true,
627           "name": "InstanceOperations",
628           "display_name": "Instance Operations"
629         }
630   ,
631         {
632
633           "access_type": true,
634           "name": "NetScalerInstances",
635           "display_name": "NetScaler ADC"
636         }
637   ,
638         {
639
640           "access_type": true,
641           "name": "HAProxyInstances",
642           "display_name": "HAProxy"
643         }
644   ,
645         {
646
647           "access_type": true,
648           "name": "NetScalerCPXDockerHost",
```



```
649           "display_name": "Docker Hosts"
650         }
651   ,
652         {
653
654           "access_type": true,
655           "name": "Reports",
656           "display_name": "Reports"
657         }
658   ,
659         {
660
661           "access_type": true,
662           "name": "Thresholds",
663           "display_name": "Thresholds"
664         }
665   ,
666         {
667
668           "access_type": true,
669           "name": "ReportingSettings",
670           "display_name": "Settings"
671         }
672   ,
673         {
674
675           "access_type": true,
676           "name": "Licenses",
677           "display_name": "License Management"
678         }
679
680      ]
681     }
682
683  }
684
685 <!--NeedCopy-->
```

API REST pour créer un rôle d'accès

```
1 URL: https://<MAS_IP>/nitro/v2/config/rba_role
2 HTTPMETHOD: POST
3
4 Payload:
```



```
{

  "rba_role": {

    "name": "AppOwnerRole",
    "description": "ExampleCompany App Owner Role",
    "policies": [
      "AppOwnerAccessPolicy"
    ]
   }

<!--NeedCopy-->
```

API REST pour télécharger un nouveau GSLB StyleBook

```
URL: https://<MAS_IP>/stylebook/nitro/v2/config/stylebooks
HTTPMETHOD: POST

Payload:
{

    "stylebook": {

      "file_name": "my-own-gslb.yaml",
      "source": "bmFtZTogZ3NsYi1kbnMtZG9tYW...aXRvcm5hbWU=",
      "encoding": "base64"
     }

   }

<!--NeedCopy-->
```

> **Remarque**
>
> Le nom du StyleBook peut changer sur votre système.

API REST pour créer des groupes et affecter des instances sélectionnées et StyleBooks

```
URL: https://<MAS_IP>/nitro/v2/config/mpsgroup
HTTPMETHOD: POST

Payload:
{
```



```
6
7    "mpsgroup": {
8
9      "id": "",
10     "name": "AppOwnerGroup1",
11     "description": "ExampleCompany App Owner Group",
12     "roles": [
13       "AppOwnerRole"
14     ],
15     "enable_session_timeout": false,
16     "assign_all_devices": false,
17     "ass ign_all_apps": false,
18     "application_names_with_regex": [
19
20     ],
21     "standalone_instances_id": [
22       "72c178da-47df-4426-9acc-cd6316f92506",
23       "c948061e-6240-4062-931c-f6988ef36e3b"
24     ],
25     "application_list": [
26
27     ],
28     "permission": "none",
29     "application_names": [
30
31     ],
32     "authscope_props": [
33       {
34
35         "propname": "configuration_template_id",
36         "propvalues": [
37           "NONE"
38         ]
39       }
40 ,
41       {
42
43         "propname": "dns_domain_entry_id",
44         "propvalues": [
45           "cf6631e5-2f56-4bb1-b0a5-90fabfc0e3e2",
46           "b268905c-522d-47e3-a2ca-3f8d8a754373"
47         ]
48       }
49 ,
50       {
```



```
51
52          "propname": "stylebook_id",
53          "propvalues": [
54            "gslbbb963abe85936913035e1d4dd14b56f7",
55            "moni72fad4494466d102b19c18ac329fa9f3"
56          ]
57         }
58
59      ],
60      "tenant_id": "6d024111-6636-4571-a250-d47b31aba7a8"
61     }
62
63  }
64
65 <!--NeedCopy-->
```

Remarque

Pour obtenir les ID des noms de domaine DNS et les StyleBooks GSLB à utiliser dans la charge utile API ci-dessus, vous pouvez utiliser les API Citrix ADM standard pour interroger les ID correspondant aux noms d'entité. Par exemple, pour obtenir l'ID d'un domaine DNS appelé « app1.acme.com », vous pouvez utiliser l'API REST Citrix ADM suivante.

```
1  URL: https://<MAS_IP>/nitro/v2/config/dns_domain_entry?filter=name:
       app1.acme.com
2  HTTPMETHOD: GET
3
4  The ID of this domain can be extracted from the following response.
5  {
6
7    "errorcode": 0,
8    "message": "Done",
9    "operation": "get",
10   "resourceType": "dns_domain_entry",
11   "username": "nsroot",
12   "tenant_name": "Owner",
13   "tenant_id": "568d8e12-1d88-42b2-8943-cbaa04826fd1",
14   "resourceName": "",
15   "dns_domain_entry": [
16     {
17
18       "tenant_id": "568d8e12-1d88-42b2-8943-cbaa04826fd1",
19       "name": "app1.acme.com",
20       "id": "3e3d85ea-1c21-49b2-97f4-60fccdbae2e0",
21       "description": "app1 domain name"
```



```
      }

   ]
  }

<!--NeedCopy-->
```

De même, pour obtenir l'ID StyleBook d'un StyleBook dont l'espace de noms est com.citrix.adc.stylebook, version : 1.0, name : `my-own-gslb`, vous pouvez utiliser l'API suivante.

```
URL: https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks?filter=name:
   my-own-gslb,namespace:com.citrix.adc.stylebooks,version:1.0
HTTPMETHOD: GET
<!--NeedCopy-->
```

La réponse contient les détails de StyleBook, y compris son attribut ID.

```
{

  "stylebooks": [
    {

      "author": null,
      "builtin": "false",
      "builtins": "{
 "netscaler.nitro.config": "10.5" }
 ",
      "deprecate": "false",
      "description": " This StyleBook is used to configure one or a
         number of Citrix ADCs in different sites into a GSLB setup. It
          is assumed that the SNIP IP on each Citrix ADC to be used by
         this StyleBook as the Site IP is already configured on the
         appliance.",
      "display_name": "HTTP/SSL LoadBalancing StyleBook",
      "filename": "my-own-gslb.yaml",
      "hide": null,
      "id": "gslb5a748d8b7684846cf6c409ad7dea8ccf",
      "imported_by": "",
      "imported_datetime": "2018-05-25 17:20:32.848902",
      "name": "my-own-gslb",
      "namespace": "com.citrix.adc.stylebooks",
      "pkg_id": "gslb5a748d8b7684846cf6c409ad7dea8ccf",
      "primary_keys": "["name"]",
      "private": "false",
      "recompile": "false",
```



```
        "schema_version": "1.0",
        "source": "LS0tIApuYW1lOiBsYgpuYW1lc…",
        "system": null,
        "tags": "",
        "tenant_id": null,
        "user_sb": "false",
        "version": "1.0"
       }
  ,
     {

        …
       }

   ]
  }

<!--NeedCopy-->
```

> **Remarque**
>
> L'API ci-dessus renvoie une liste de StyleBooks qui correspondent au filtre. Assurez-vous de sélectionner le bon StyleBook dans la réponse pour récupérer l'ID.

API REST pour créer un utilisateur système

> **Remarque**
>
> Cette étape est facultative.

```
URL: https://<MAS_IP>/nitro/v2/config/mpsuser
HTTPMETHOD: POST

Payload:
{

  "mpsuser": {

    "name": "John",
    "password": "welcome",
    "external_authentication": false,
    "enable_session_timeout": false,
    "groups": [
      "AppOwnerGroup1"
    ]
```

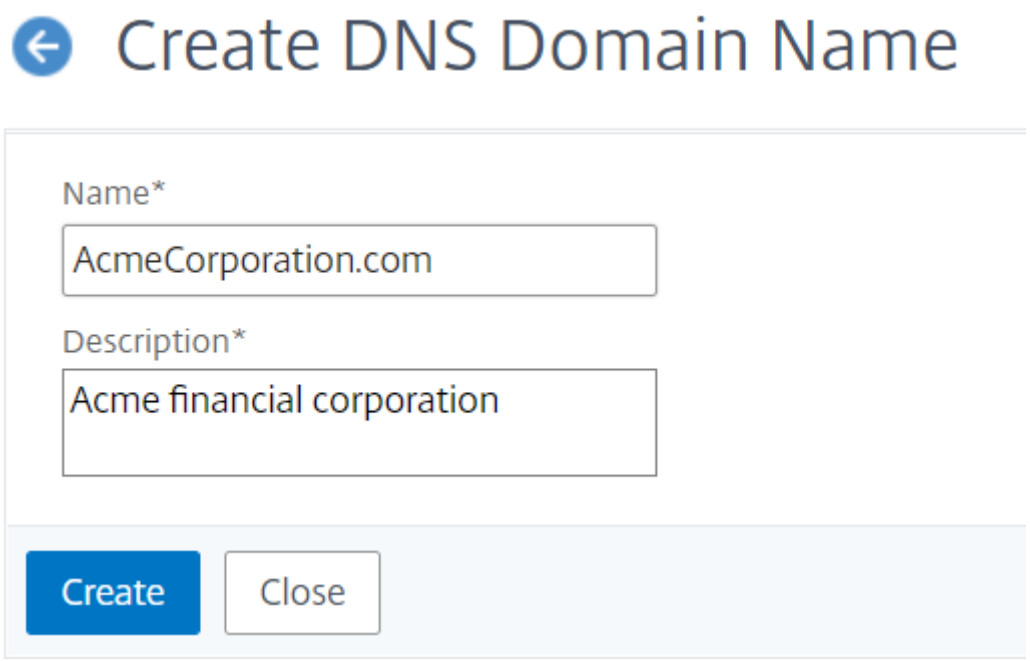


```
16      }
17
18    }
19
20  <!--NeedCopy-->
```

Workflow pour les propriétaires d'applications

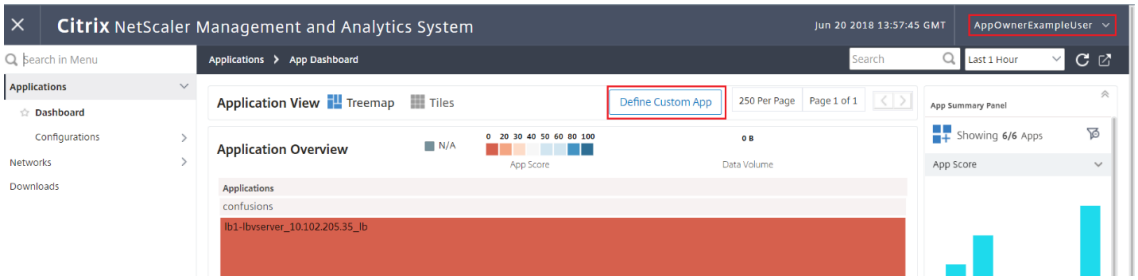
Vos utilisateurs doivent ouvrir une session en tant qu'utilisateurs d'application à l'aide de leurs informations d'identification. Les utilisateurs doivent suivre cette tâche pour créer leurs propres noms de domaine DNS et utiliser le nouveau GSLB StyleBook.

1. Dans Citrix ADM, accédez à **Réseaux** > **Noms de domaine DNS** .
2. Cliquez sur **Ajouter** pour créer un nouveau domaine DNS. Créez les domaines DNS dans Citrix ADM.

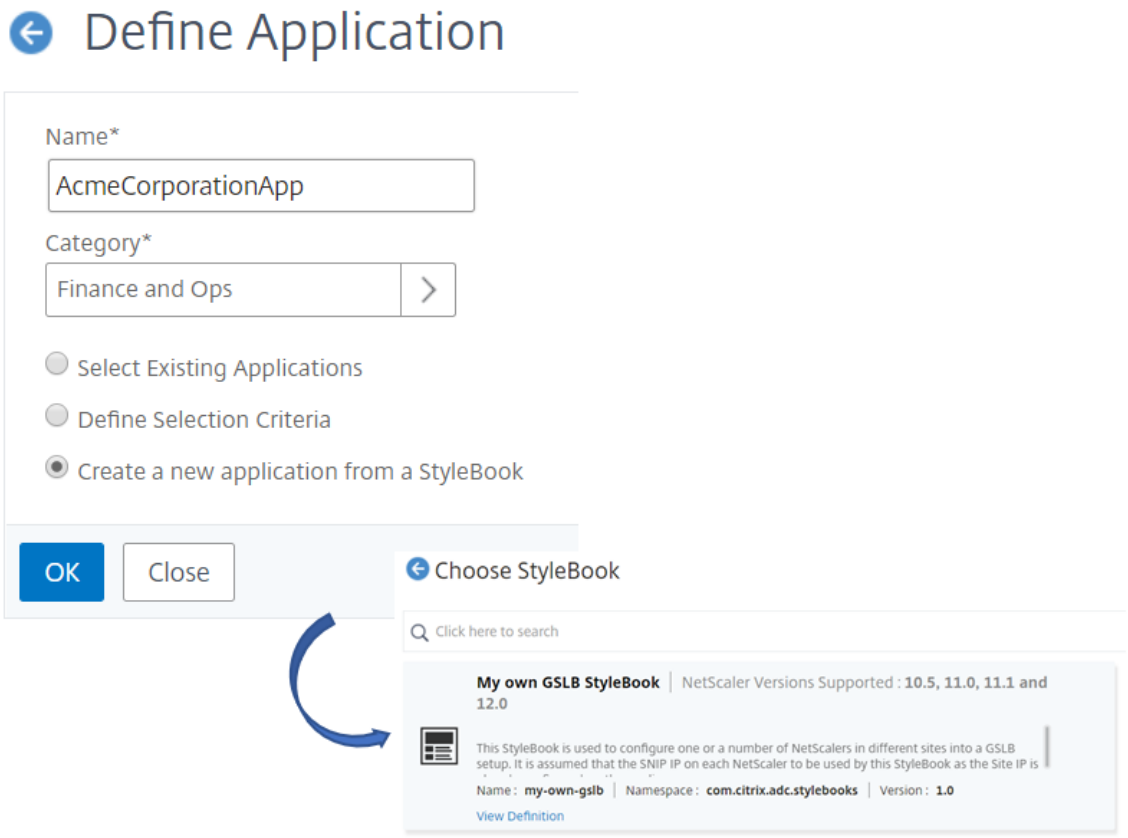


> **Remarque**
>
> En tant qu'administrateur, vous pouvez également créer ces noms de domaine et les affecter aux groupes d'utilisateurs.

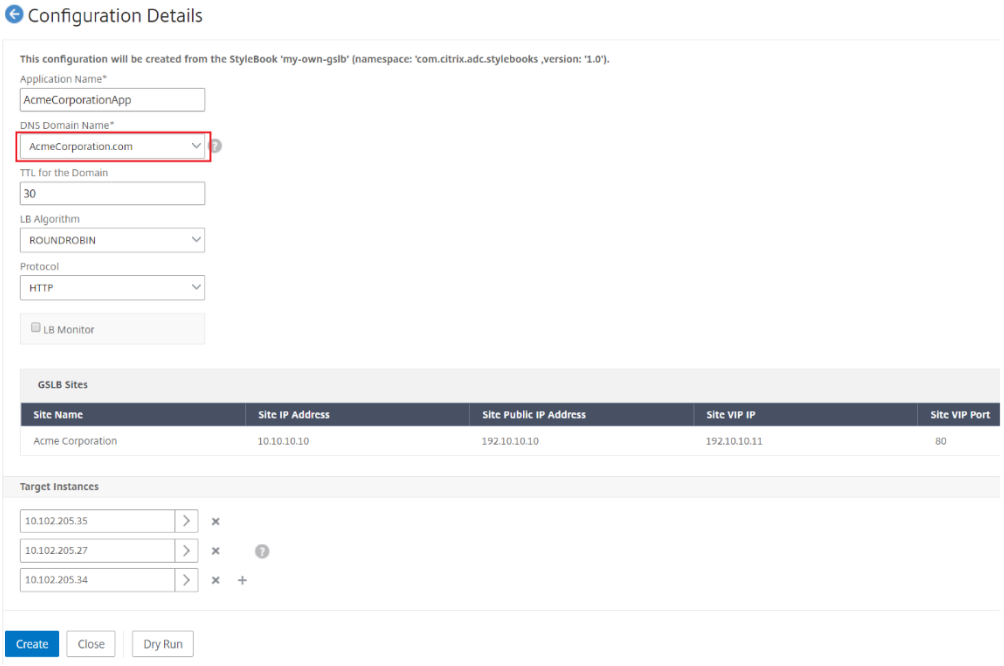
3. Accédez à **Applications** > **Tableau de bord**, puis cliquez sur **Définir une application personnalisée** .



4. Tapez un nom pour l'application et sélectionnez une catégorie. Sélectionnez **Créer une nouvelle application à partir d'un StyleBook** et cliquez sur **OK** . Sélectionnez **Mon propre StyleBook GSLB** pour déployer la configuration sur les instances sélectionnées.



5. Tapez les valeurs requises pour tous les paramètres dans le StyleBook.
   a) Sélectionnez le nom de domaine dans la liste.
   b) Ajoutez les sites GSLB de votre application, selon le cas.
   c) Sélectionnez les instances Citrix ADC cibles dans tous les sites GSLB.
   d) Cliquez sur **Créer** pour créer une configuration GSLB.



> **Remarque**
>
> Le paramètre StyleBook « Nom de domaine DNS » affiche uniquement la liste des domaines DNS appartenant à l'utilisateur dans Citrix ADM.

API REST Citrix ADM pour le workflow des propriétaires d'applications

API REST pour se connecter à Citrix ADM

```
URL: http: //<MAS_IP>/nitro/v2/config/login
HTTPMETHOD: POST

Payload:
{

  "login": {

    "username": "<USER_NAME>",
    "password": "<PASSWORD>",
    "session_timeout": 1800
   }

 }

<!--NeedCopy-->
```


API REST pour créer des noms de domaine DNS

```
URL: https://<MAS_IP>/nitro/v2/config/dns_domain_entry
HTTP METHOD: POST
PAYLOAD: {
 "dns_domain_entry":{
 "name":"app1.acme.com","description":"app1 acme domain"
 }

 }

<!--NeedCopy-->
```

API REST pour créer des applications à l'aide de StyleBook

```
URL: https://<MAS_IP>/nitro/v2/config/application
HTTPMETHOD: POST

Payload:
{

  "params": {

    "action": "app_discovery"
   }
 ,
  "application": {

    "id": "",
    "name": "app1",
    "app_c ategory": "ITOps",
    "stylebook_params": "{
 "name":"my-own-gslb","namespace":"com.citrix.adc.stylebooks","version"
    :"1.0","configpack_payload":{
 "parameters":{
 "name":"app1","domain-name":"app1.acme.com",]"ttl":"30","algorithm":"
    ROUNDROBIN","protocol":"HTTP","sites":[{
 "name":"site1","ipaddress":"6.5.6.77","virtual-ip":"88.6.5.44","
    virtual-port":"80" }
 ] }
 ,"targets":[ {
 "id":"72c178da-47df-4426-9acc-cd6316f92506" }
 , {
 "id":"0e4d0789-bffe-4266-ba1c-09adfc61db4e" }
```



```
, {
"id":"b5af4455-3f06-4f56-b0cb-3d9f868c1f94" }
] }
 }
"
  }

}

<!--NeedCopy-->
```

Dans la charge utile ci-dessus :

- Le « stylebook_params » contient le nom, les espaces de noms et la version du StyleBook à utiliser.
- Le « configpack_payload » contient les paramètres remplis du StyleBook comme indiqué dans le formulaire GUI équivalent ci-dessus. Citrix ADM garantit que seuls les noms de domaine DNS auxquels l'utilisateur a accès peuvent être utilisés comme valeurs pour le paramètre « domain-name ».
- Les « cibles » contiennent la liste des ID NetScaler sur lesquels la configuration GSLB sera déployée (les instances ADC sur les sites GSLB).

Pour obtenir l'ID NetScaler correspondant à l'adresse IP de gestion de NetScaler, vous pouvez utiliser l'API Citrix ADM suivante :

```
URL: https://<MAS_IP>/nitro/v2/config/ns?filter=ip_address:
   192.168.153.162
HTTPMETHOD: GET
<!--NeedCopy-->
```

La charge utile de réponse contient des informations sur ce NetScaler, y compris son ID :

```
{

  "errorcode": 0,
  "message": "Done",
  ⋯.."tenant_id": "ec0eb868-0d6b-4729-bfbd-3005dd2694c1",
  "resourceName": "",
  "ns": [
    {

      "manufacturedate": "9/30/2009",
      "is_grace": "false",
      "hostname": "youcef-ns",
```



```
      "std_bw_config": "0",
      "gateway_deployment": "false",
      "gateway_ipv6": "",
      "ha_master_state": "Primary",
      "instance_available": "0",
      "device_finger_print": "",
      "instance_state": "Down",
      "reason": "Device not reachable",
      "name": "",
      "ent_bw_available": "0",
      "description": "",
      "id": "da9ffff2-c100-45f1-a913-c542718338b2",
      "mgmt_ip_address": "192.168.153.162",
      ….
     }

  ]
 }

<!--NeedCopy-->
```

Créez votre StyleBook

Le contenu complet du fichier « my-own-gslb.yaml » StyleBook est affiché ci-dessous :
Vous pouvez utiliser ce StyleBook personnalisé comme il est ou le personnaliser selon vos besoins pour générer la configuration GSLB requise. Le paramètre important de ce StyleBook appelé « domain-name » doit être présent dans n'importe quel StyleBook pour utiliser la fonctionnalité de noms DNS.

```
name: my-own-gslb
namespace: com.citrix.adc.stylebooks
version: "1.0"
display-name: My own GSLB StyleBook
description: 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.
schema-version: "1.0"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    version: "10.5"
    prefix: ns
  -
    namespace: com.citrix.adc.commontypes
```



```
    version: "1.0"
    prefix: cmtypes
parameters:
  -
    name: name
    label: Application Name
    type: string
    required: true
    key: true

  -
    name: domain-name
    label: DNS Domain Name
    description: GSLB DNS Domain Name
    type: string
    required: true
    allowed-dynamic-values:
      source: local
      resource-type: dns_domain_entry

  -
    name: ttl
    label: TTL for the Domain
    description: Time-To-Live value (number of seconds) for the Domain
    type: number
    default: 30

  -
    name: algorithm
    label: LB Algorithm
    description: Global Load Balancing Algorithm
    type: string
    default: ROUNDROBIN
    allowed-values:
      - ROUNDROBIN
      - STATICPROXIMITY
      - SOURCEIPHASH

  -
    name: protocol
    label: Protocol
    description: The protocol of the GSLB VIP
    type: string
    default: HTTP
    allowed-values:
```



```
59        - HTTP
60        - FTP
61        - TCP
62        - UDP
63        - SSL
64        - SSL_BRIDGE
65        - SSL_TCP
66        - NNTP
67        - ANY
68        - SIP_UDP
69        - SIP_TCP
70        - SIP_SSL
71        - RADIUS
72        - RDP
73        - RTSP
74        - MYSQL
75        - MSSQL
76        - ORACLE
77
78    -
79      name: monitor
80      label: LB Monitor
81      description: Monitor to be bound to the GSLB service
82      type: cmtypes::monitor
83
84    -
85      name: sites
86      label: GSLB Sites
87      description: Provide information about the GSLB Sites
88      type: object[]
89      required: true
90      parameters:
91        -
92          name: name
93          label: Site Name
94          type: string
95          required: true
96        -
97          name: ipaddress
98          label: Site IP Address
99          description: The IP Address of this Site. Use a SNIP IP address
                on the site's appliance.
100         type: ipaddress
101         required: true
102       -
```



```
103         name: public-ipaddress
104         label: Site Public IP Address
105         description: The Public IP Address of this Site. It NATs to the
                Site's IP address
106         type: ipaddress
107       -
108         name: virtual-ip
109         label: Site VIP IP
110         description: The IP Address for the GSLB Service on this site (
               The VIP on this Site)
111         type: ipaddress
112         required: true
113       -
114         name: virtual-port
115         label: Site VIP Port
116         description: The port number for the GSLB Service (VIP) on this
                site
117         type: tcp-port
118         default: 80
119
120 components:
121   -
122     name: enable-gslb-comp
123     type: ns::nsfeature
124     description: Enables the GSLB feature
125     meta-properties:
126       action: enable
127     properties:
128       feature: ["GSLB", "LB"]
129   -
130     name: gslb-monitor-comp
131     type: cmtypes::monitor
132     condition: $parameters.monitor
133     properties:
134       monitorname: $parameters.name + "-" + $parameters.monitor.
              monitorname + "-gslbmon"
135       type: $parameters.monitor.type
136       destip?: $parameters.monitor.destip
137       destport?: $parameters.monitor.destport
138       httprequest?: $parameters.monitor.httprequest
139       send?: $parameters.monitor.send
140       customheaders?: $parameters.monitor.customheaders
141       respcodes?: $parameters.monitor.respcodes
142       recv?: $parameters.monitor.recv
143       lrtm?: $parameters.monitor.lrtm
```



```
144         secure?: $parameters.monitor.secure
145         interval?: $parameters.monitor.interval
146         interval_units?: $parameters.monitor.interval_units
147         resptimeout?: $parameters.monitor.resptimeout
148         retries?: $parameters.monitor.retries
149         downtime?: $parameters.monitor.downtime
150     -
151       name: gslb-vserver-comp
152       type: ns::gslbvserver
153       description: Creates a GSLB VServer config object
154       properties:
155         name: $parameters.name + "-gslbvserver"
156         servicetype: $parameters.protocol
157         lbmethod: $parameters.algorithm
158       components:
159         -
160           name: gslb-domain-comp
161           type: ns::gslbvserver_domain_binding
162           properties:
163             name: $parent.properties.name
164             domainname: $parameters.domain-name
165             ttl: $parameters.ttl
166     -
167       name: gslb-site-comp
168       type: ns::gslbsite
169       description: Creates a GSLB Site config object
170       repeat: $parameters.sites
171       repeat-item: site
172       properties:
173         sitename: $parameters.name + "-" + $site.name + "-gslbsite"
174         siteipaddress: $site.ipaddress
175         publicip?: $site.public-ipaddress
176       components:
177         -
178           name: gslb-service-comp
179           type: ns::gslbservice
180           description: Creates a GSLB Service
181           properties:
182             servicename: $parameters.name + "-" + $site.name + "-
                  gslbservice"
183             ip: $site.virtual-ip
184             servicetype: $parameters.protocol
185             port: $site.virtual-port
186             sitename: $parent.properties.sitename
187           components:
```



```
188             -
189               name: gslb-vserver-service-binding-comp
190               type: ns::gslbvserver_gslbservice_binding
191               description: Creates a Binding between the GSLB vserver and
                      the GSLB Service
192               properties:
193                 name: $components.gslb-vserver-comp.properties.name
194                 servicename: $parent.properties.servicename
195             -
196               name: gslb-service-monitor-binding-comp
197               type: ns::gslbservice_lbmonitor_binding
198               description: Creates a Binding between the GSLB service and
                      the GSLB monitor
199               condition: $parameters.monitor
200               properties:
201                 servicename: $parent.properties.servicename
202                 monitor_name: $components.gslb-monitor-comp.properties.
                      monitorname
203   <!--NeedCopy-->
```

Utiliser l'API pour créer des configurations à partir de StyleBooks

April 29, 2021

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 réussit, 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 `lb-vserver` StyleBook que vous avez créé dans StyleBook pour créer un serveur virtuel d'équilibrage de charge. Utilisez l'API REST pour créer un pack de configuration à partir de ce StyleBook comme suit :

Méthode HTTP : POST

URL : `https://<ADM-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/lb-vserver/configpacks`

En-têtes REQUET :

Content-Type: application/json

Accepter : application/json

CHARGE CORPS DE LA DEMANDE:

```
{

  "configpack":
  {

    "parameters": {

      "name": "lb1",
      "ip": "10.102.117.31"
     }
 ,
    "targets":
    [
      {

        "id": "deecee30-f478-4446-9741-a85041903410"
       }

    ]
   }

 }

<!--NeedCopy-->
```

Dans cette requête HTTP, l'id (par exemple, « deecee30-f478-4446-9741-a85041903410") est l'ID d'instance de l'instance de 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 de 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 exemple, pour récupérer l'ID d'instance ou une instance Citrix ADC dont l'adresse IP est 192.168.153.160, vous pouvez utiliser l'API suivante :

Méthode HTTP : GET

URL : `https://<ADM-IP>/nitro/v1/config/ns?filter=ip_address:192.168.153.160`

EN-TÊTES DE DEMANDE:

Accepter : application/json

La réponse contient l'ID dans la charge utile json :

EN-TÊTES DE RÉPONSE ATTENDUS (en case de succès) :

200 OK

Content-Type: application/json

CORPS DE RÉPONSE ATTENDU (en cas de succès) :

```
{

  "errorcode": 0,
  "message": "Done",
  "operation": "get",
  "resourceType": "ns",
  "username": "nsroot",
  "tenant_name": "Owner",
  "resourceName": "",
  "ns":
  [
    {

    "is_grace": "false",
    "hostname": "",
    "std_bw_config": "0",
    "gateway_deployment": "false",
    "id": "deecee30-f478-4446-9741-a85041903410",
    }

 ]
 }

<!--NeedCopy-->
```

Si la configuration (pack de configuration) est créée avec succès, vous recevez la réponse HTTP suivante :

EN-TÊTES DE RÉPONSE ATTENDUS (en case de succès) :

200 OK

Content-Type: application/json

CORPS DE RÉPONSE ATTENDU (en cas de succès) :

```
{

  "configpack":
```



```
  {

    "config_id": "1460806080"
   }

 }

<!--NeedCopy-->
```

Vous avez créé votre première configuration (pack de configuration) 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 un autre pack de configuration ou de configuration et l'exécuter sur des instances Citrix ADC identiques ou différentes. Dans cet exemple, créez une autre configuration et fournissez un nom et une adresse IP différents pour le serveur virtuel et spécifiez LEASTCONNECTION comme méthode d'équilibrage de charge. Déployez cette configuration sur deux instances Citrix ADC.

La requête HTTP est la suivante :

Méthode HTTP : POST

URL : `https://<ADM-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/lb-vserver/configpacks`

EN-TÊTES DE DEMANDE:

Content-Type: application/json

Accepter : application/json

CHARGE CORPS DE LA DEMANDE:

```
{

  "configpack":
  {

    "parameters":
    {

      "name": "lb2",
      "ip": "10.102.117.32",
      "lb-alg": "LEASTCONNECTION"
```



```
12       }
13   ,
14      "targets"
15      [
16       {
17   "id": "deecee30-f478-4446-9741-a85041903410" }
18   ,
19       {
20   "id": "debecc60-d589-4557-8632-a74032802412" }
21
22      ]
23     }
24
25   }
26
27   <!--NeedCopy-->
```

Dans cette requête HTTP, le serveur virtuel d'équilibrage de charge lb2 avec l'adresse IP 10.102.117.32 est créé sur les deux instances Citrix ADC représentées par les ID « deecee30-f478-4446-9741-a85041903410" et « debecc60-d589-4557-8632-a74032802412".

En cas de création réussie du pack de configuration, la réponse HTTP suivante est reçue :

EN-TÊTES DE RÉPONSE ATTENDUS (en case de succès) :

200 OK

Content-Type: application/json

CORPS DE RÉPONSE ATTENDU (en cas de succès) :

```
1   {
2
3      "configpack":
4     {
5
6        "config_id": "1657696292"
7      }
8
9   }
10
11  <!--NeedCopy-->
```

Ce nouveau pack de configuration a un ID différent 165769629. Vous pouvez mettre à jour ou supprimer cette configuration à l'aide de cet ID.

Exemple 3

Considérez le style « basic-lb-config » que vous avez créé dansStyleBook pour créer une configuration d'équilibrage de charge de base. Utilisez l'API REST pour créer un pack de configuration à partir de ce StyleBook comme suit :

Méthode HTTP : POST

URL : `http://<ADM-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/basic-lb-config/configpacks`

EN-TÊTES DE DEMANDE:

Content-Type: application/json

Accepter : application/json

EN-TÊTES DE RÉPONSE ATTENDUS (en case de succès) :

200 OK

Content-Type: application/json

CORPS DE RÉPONSE ATTENDU (en cas de succès) :

```
{

  "configpack":
  {

    "parameters":
    {

      "name": "myapp",
      "ip": "10.70.122.25",
      "svc-servers": ["192.168.100.11","192.168.100.12"],
       "svc-port": 8080
     }
 ,
    "targets":
    [
     {

      "id": "deecee30-f478-4446-9741-a85041903410"
      }
 ,
     {

      "id": "debecc60-d589-4557-8632-a74032802412"
```



```
25         }
26
27       ]
28     }
29
30   }
31
32 <!--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

Considérons l' **exemple** composite StyleBook que vous avez créé dansCréer un StyleBook composite . Utilisez l'API REST pour créer un pack de configuration à partir de ce StyleBook comme suit :

Méthode HTTP : POST

URL : `http://<ADM-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/composite-example/configpacks`

EN-TÊTES DE DEMANDE:

Content-Type: application/json

Accepter : application/json

CHARGE CORPS DE LA DEMANDE:

```
1  {
2
3    "configpack":
4    {
5
6      "parameters": {
7
8        "name": "myapp",
9        "ip": "2.2.2.2",
10       "svc-servers": ["10.102.29.52","10.102.29.53"]
11      }
12   ,
13     "targets":
14     [
15      {
16
```



```
        "id": "deecee30-f478-4446-9741-a85041903410"
        }
  ,
      {

        "id": "debecc60-d589-4557-8632-a74032802412"
        }

     ]
    }

  }

<!--NeedCopy-->
```

Dans cette requête HTTP, la configuration est créée sur deux instances Citrix ADC représentées par leurs identifiants. 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 « composite-example » StyleBook.

En cas de création réussie du pack de configuration, la réponse HTTP suivante est reçue :

EN-TÊTES DE RÉPONSE ATTENDUS (en case de succès) :

200 OK

Content-Type: application/json

CORPS DE RÉPONSE ATTENDU (en cas de succès) :

```
{

  "configpack": {

    "config_id": "4917276817"
    }

  }

<!--NeedCopy-->
```

Mise à jour d'une configuration

Pour mettre à jour cette configuration, par exemple, en ajoutant un nouveau serveur back-end avec l'adresse IP 10.102.29.54 au serveur virtuel d'équilibrage de charge `myapp`, utilisez l'API pour mettre à

jour un pack de configuration comme suit :

HTTP METHOD: PUT

URL : `http://<ADM-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/composite-example/configpacks/4917276817`

EN-TÊTES DE DEMANDE:

Content-Type: application/json

Accepter : application/json

CHARGE CORPS DE LA DEMANDE:

```
{

  "configpack": {

    "parameters": {

      "name": "myapp",
      "ip": "2.2.2.2",
      "svc-servers": ["10.102.29.52","10.102.29.53","10.102.29.54"]
    }
 ,
  "targets":
    [
      {

       "id": "deecee30-f478-4446-9741-a85041903410"
       }
 ,
      {

       "id": "debecc60-d589-4557-8632-a74032802412"
       }

    ]
    }

 }

<!--NeedCopy-->
```

En cas de mise à jour réussie du pack de configuration, la réponse HTTP suivante est reçue :

EN-TÊTES DE RÉPONSE ATTENDUS (en case de succès) :

200 OK

Content-Type: application/json

CORPS DE RÉPONSE ATTENDU (en cas de succès) :

```
{

   "configpack": {

     "config-id": "4917276817"
   }

 }

<!--NeedCopy-->
```

Suppression d'une configuration

Pour supprimer cette configuration (de toutes les instances Citrix ADC), vous pouvez utiliser l'API pour supprimer un pack de configuration comme suit :

En cas de suppression réussie du pack de configuration, la réponse HTTP suivante est reçue :

Méthode HTTP : DELETE

URL : `http://<ADM-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/composite-example/configpacks/4917276817`

EN-TÊTES DE DEMANDE:

Accepter : application/json

EN-TÊTES DE RÉPONSE ATTENDUS (en case de succès) :

200 OK

Content-Type: application/json

CHARGE DE RÉPONSE ATTENDUE (en cas de succès) :

```
{

   "configpack": {

     "config_id": "4917276817"
   }

 }
```



```
9
10 <!--NeedCopy-->
```

Vous pouvez vous connecter à l'instance Citrix ADC et vérifier que tous les objets de configuration qui font partie de ce pack de configuration ont été supprimés.

Si vous souhaitez supprimer la configuration d'instances Citrix ADC spécifiques au lieu de toutes les instances, utilisez l'opération de pack de configuration de mise à jour décrite ci-dessus et modifiez l'attribut « cibles » dans la charge utile JSON pour supprimer les ID d'instance Citrix ADC spécifiques.

Utiliser l'API pour créer des configurations pour télécharger des fichiers de certificats et de clés

April 29, 2021

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 de navigateur Chrome Postman pour envoyer des requêtes HTTP à Citrix ADM.

Prenons l'exemple StyleBook que vous avez créé pour charger les fichiers de certificat et de clé dans Comment faire pour créer un StyleBook pour charger des fichiers de certificat SSL et de clé de certificat vers Citrix ADM. Utilisez l'API REST pour créer un pack de configuration à partir de ce StyleBook comme suit :

POST

```
https://<MAS_IP_Address>/stylebook/nitro/v1/config/stylebooks/com.citrix.adc.stylebooks/1.0/lb-mon/configpacks?mode=async
```

```
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
```



```
                    "ip": "14.1.1.15",
                    "port": "80" }

        ],
             "certificates": [
                 {

                     "cert-name": "server_cert",
                     "cert-file": "server_cert.pem",
                     "ssl-inform": "PEM",
                     "key-name": "server_key",
                     "key-file": "server_key.pem",
                     "cert-password": "secret",
                     "cert-advanced": {

                         "is-ca-cert": false,
                         "skip-ca-name": false
             }

           }

        ],
             "lb-advanced": {

                 "flush-on-state-down": "ENABLED",
                 "auth-params": {

                     "authentication": "OFF",
                     "authentication-http-401": "OFF"
           }
,
                 "appflow-log": "ENABLED",
                 "algorithm": "LEASTCONNECTION"
         }
,
             "svcg-advanced": {

                 "svc-client-ip": "DISABLED",
                 "svc-use-source-ip": "NO",
                 "svc-use-proxy-port": "NO",
                 "svc-surge-protection": "OFF",
                 "svc-client-keepalive": "NO",
                 "svc-tcp-buffering": "NO",
                 "svc-compression": "NO",
                 "svc-state": "ENABLED",
```



```
                "svc-downstate-flush": "DISABLED",
                "svc-enable-health-monitor": "NO"
        }

      }
  ,
        "targets": [
            {

                "id": "8c158e7a-0087-423f-91b0-0ccf16de552a"
        }

     ]
    }

  }

<!--NeedCopy-->
```

Ce pack de configuration est identifié de manière unique à l'aide de l'ID 8c158e7a-0087-423f-91b0-0ccf16de552a. Vous pouvez utiliser cet ID pour interroger, mettre à jour ou supprimer la configuration. En cas de mise à jour réussie du pack de configuration, les fichiers de certificat et de clé sont téléchargés sur le système de fichiers Citrix ADM.

Utiliser l'API pour créer des configurations pour télécharger n'importe quel type de fichier

April 29, 2021

Vous pouvez également utiliser l'API Citrix Application Delivery Management (ADM) pour créer un pack de configuration qui charge des fichiers vers l'instance Citrix ADC sélectionnée.

Prenons l'exemple StyleBook que vous avez créé pour télécharger des fichiers de n'importe quel type dansComment faire pour créer un StyleBook pour télécharger des fichiers sur Citrix ADM. Dans cet exemple, créez un pack de configuration et spécifiez la valeur du paramètre `locationfile` comme chemin d'accès au fichier d'emplacement sur Citrix ADM.
Utilisez l'API REST pour créer un pack de configuration à partir de ce StyleBook comme suit :

POST

```
https://<mas_ip>/stylebook/nitro/v1/config/stylebooks/com.citrix.adc.
stylebooks.samples/1.0/upload-geolocations/configpacks
```



```
Content-Type: application/json
Accept: application/json
{

   "configpack":
   {

      "parameters": {

         "locationfile": "/var/mps/tenants/root/files/ /
            custom_geolocations.csv"
      }
 ,
      "targets": [
         {

            "id": "5e540839-cd6c-437e-ac53-7d49bc2602b5"
        }

     ]
   }

 }

<!--NeedCopy-->
```

Utiliser l'API pour importer des StyleBooks personnalisés

April 29, 2021

Vous pouvez désormais utiliser les API StyleBook pour importer des StyleBooks personnalisés dans Citrix Application Delivery Management (ADM). Utilisez l'API REST pour créer un pack de configuration à partir de ce StyleBook comme suit dans n'importe quel outil tel que l'outil de ligne de commande cURL ou l'extension 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.

HTTP, méthode : POST

URL : `http://<mas-ip>/stylebook/nitro/v1/config/stylebooks`

En-têtes :


```
Content-Type: application/json
Accept: application/json
<!--NeedCopy-->
```

RequestBody :

```
{

        "stylebook":
   {

      "file_name": "example-lb.yaml",
      "source": "<base64-contents>",
      "encoding": "base64"
    }

 }

<!--NeedCopy-->
```

Où, la valeur de l'attribut « source », est le codage 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, il suffit de changer l'attribut de nom de fichier par le nom de fichier .tgz et la valeur de l'attribut source par l'encodage base64 du contenu de votre fichier .tgz.

Une fois l'API exécutée avec succès dans l'outil, vous obtenez la réponse suivante qui indique que le StyleBook a été importé dans Citrix ADM.

```
200 OK
<!--NeedCopy-->
```

Corps de réponse :

```
{


  "stylebook":
{


```



```
    "name": "example-lb",

    "namespace": "com.example.stylebook",

    "version": "1.0"

   }


 }

<!--NeedCopy-->
```

Utiliser l'API pour télécharger StyleBooks personnalisés

April 29, 2021

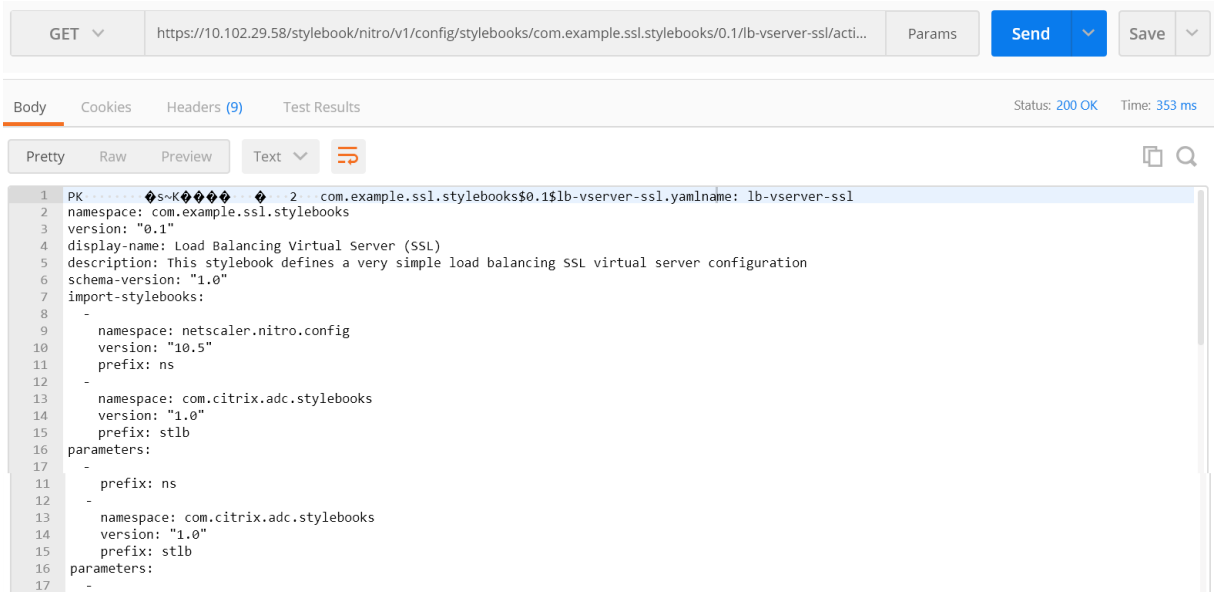
Vous pouvez télécharger un StyleBook personnalisé en fournissant l'API REST StyleBooks suivante :

GET `https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks/<NAMESPACE>/<VERSION>/<NAME>/actions/download`

Vous pouvez exécuter l'API dans n'importe quel outil tel que l'outil de ligne de commande cURL. Vous pouvez également utiliser l'extension du navigateur Chrome Postman après avoir modifié les champs adresse IP, nom, version et espace de noms.

GET `https://10.102.29.58/stylebook/nitro/v1/config/stylebooks/com.example.ssl.stylebooks/0.1/lb-vserver-ssl/actions/download`

Le StyleBook au format .yaml est téléchargé.



Utiliser l'API pour supprimer des StyleBooks personnalisés

April 29, 2021

Vous pouvez supprimer le StyleBook personnalisé en fournissant l'API REST StyleBooks suivante :

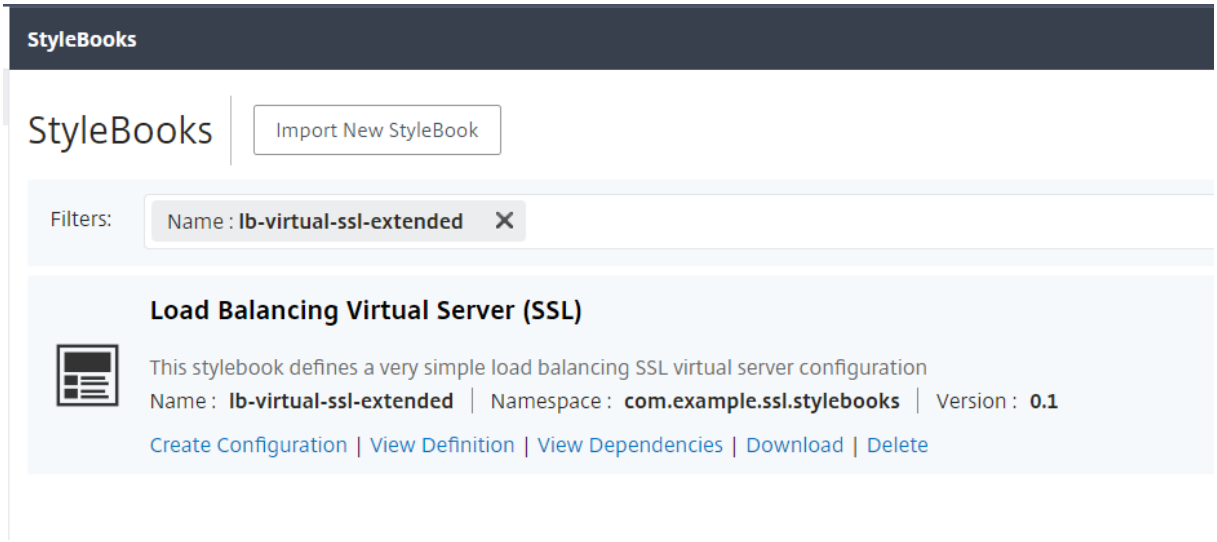
SUPPRIMER `https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks/<NAMESPACE>/<VERSION>/<NAME>?dependencies=true`

Si le paramètre de requête des dépendances dans l'URL n'est pas fourni ou si sa valeur est définie sur false, les dépendances StyleBook ne sont pas supprimées. Et seul le StyleBook est supprimé.

Lorsque vous recevez un code d'état de réponse HTTP 200, cela signifie que le StyleBook personnalisé et ses dépendances sont correctement supprimés de Citrix Application Delivery Management (ADM).

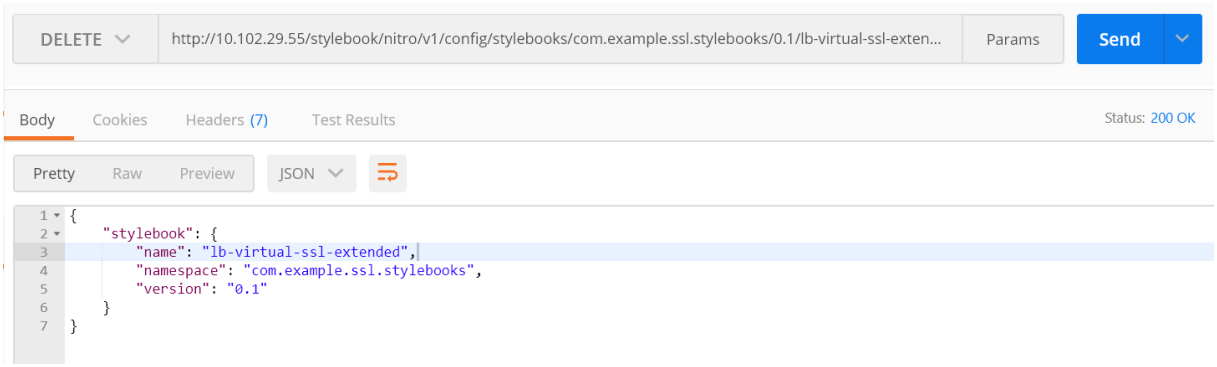
> **Remarque**
>
> Vous ne pouvez pas supprimer un StyleBook personnalisé qui possède d'autres StyleBooks dans le service MA qui en dépendent.

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.

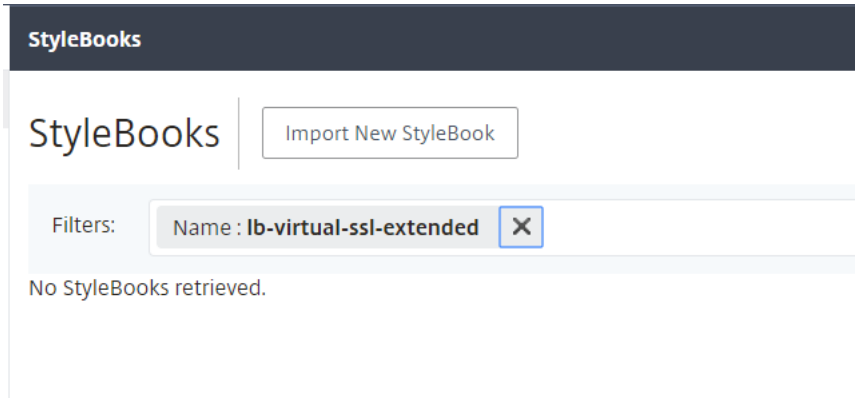


Vous pouvez exécuter l'API dans n'importe quel outil tel que l'outil de ligne de commande cURL. En outre, vous pouvez utiliser l'extension du navigateur Chrome Postman après avoir modifié les champs adresse IP, nom, version et espace de noms.

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

April 29, 2021

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 suivant pour afficher les détails.

—	—
En-tête	Importer StyleBooks
Paramètres	Parameters-default-sources construct
Substitutions	Composants
Propriétés facultatives	Composants d'assistance
Propriétés sources par défaut	Composants imbriqués
Construct de condition	Répéter la construction
Construct à condition répétée	Sorties
Répétitions imbriquées	Référence parente
Référence des paramètres	Référence des substitutions
Référence des composants	Opérations
Référence variable	Alarmes
Analytics	Fonctions intégrées
Expressions	Détection des dépendances
	Interpolations sur place

> **Remarque**
>
> Lors de la définition, `repeat-itemrepeat-index`, ou des arguments de fonctions de substitution, n'utilisez pas les mots réservés suivants pour nommer une variable définie par l'utilisateur : `$<var-name>`
>
> - StyleBook, paramètres, substitutions, composants, propriétés, sorties, parent, auto, opérations, analytique, alarmes
> - repeat-item, repeat-item-0, repeat-item-1, repeat-item-2
> - repeat-index, repeat-index-0, repeat-index-1, repeat-index-2
> - default

- roles, role, targets, target
- context, parent-context, parent_context

Pour plus d'informations et d'exemples sur la conception de vos propres StyleBooks, reportez-vous à la section Comment créer vos propres styleBooks.

En-tête

April 29, 2021

Les six premières lignes d'un StyleBook comprennent la section d'en-tête. Cette section vous permet de définir l'identité d'un StyleBook et de décrire ses activités. Il s'agit d'une section obligatoire.

Le tableau suivant décrit les attributs de la section d'en-tête :

Attribut	Description
nom	Nom permettant d'identifier le StyleBook. Cet attribut est obligatoire.
description	Description définissant ce qu'un StyleBook fait. Cette description apparaît sur l'interface graphique de Citrix Application Delivery Management (ADM). Il s'agit d'un attribut facultatif.
nom-affichage	Un nom descriptif pour le StyleBook. Ce nom apparaît sur l'interface utilisateur graphique Citrix ADM. Il s'agit d'un attribut facultatif.
auteur	L'auteur ou l'organisation qui crée le StyleBook. Il s'agit d'un attribut facultatif.
espace de noms	Un espace de noms fait partie d'un identificateur unique pour un StyleBook afin d'éviter les collisions de noms. Un espace de noms peut être n'importe quelle chaîne, mais une bonne pratique consiste à l'utiliser pour nommer la société, le département ou l'unité qui a créé ou possède un ensemble de StyleBooks. Par exemple, vous pouvez utiliser le format suivant :`<company>.<department>.<unit>.stylebooks`. Il s'agit d'un attribut obligatoire.

Attribut	Description
version	Numéro de version du StyleBook. Vous pouvez modifier le numéro de version lorsque vous mettez à jour un StyleBook. StyleBooks de différentes versions peuvent coexister ensemble. Il s'agit d'un attribut obligatoire.
version de 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 n'est pas affiché sur l'interface graphique de Citrix ADM. Il s'agit d'un paramètre utile pour les StyleBooks qui sont des blocs de construction 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 :

```
    name: lb

    description: "This stylebook defines a sample load balancing
       configuration."

    display-name: "Load Balancing StyleBook (HTTP)"

    author: Mike Smith (ACME Infra team)

    namespace: com.example.stylebooks

    schema-version: "1.0"

    version: "0.1"
<!--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 StyleBooks

April 29, 2021

Il s'agit de la deuxième section de votre StyleBook et vous permet de déclarer 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 reconstruire 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 auquel 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 Citrix ADC NITRO, tels que `lbvserver` service ou 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 de **préfixe** utilisé dans la section import-stylebooks est un raccourci pour faire 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 voulez faire référence à un StyleBook avec cet espace de noms et cette version, vous pouvez simplement utiliser la chaîne de préfixe choisie avec le nom du StyleBook pour l'identifier de manière unique.

Exemple :

```
      import-stylebooks:
       -
         namespace: netscaler.nitro.config
         version: "10.5"
         prefix: ns
      -
         namespace: com.acme.stylebooks
         version: "0.1"
         prefix: stlb
<!--NeedCopy-->
```

Dans cet exemple, le premier préfixe défini est appelé ns et fait référence à l'espace de noms netscaler.nitro.config et à la version 10.5. Le deuxième préfixe défini est appelé `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 certaine version, vous pouvez utiliser la notation **<namespace-shorthand> <type-name>**. Par exemple, **ns lbvserver** fait référence au type `lbvserver` défini dans l'espace de noms netscaler.nitro.config, version 10.5.

De même, si vous voulez faire référence à un StyleBook avec la version « 0.1 » dans l'espace de noms com.acme.stylebooks, vous pouvez utiliser la notation **stlb::<stylebook-name>**.

> **Remarque**
>
> Par convention, le préfixe « ns » est utilisé pour faire référence à l'espace de noms NITRO de Citrix ADC.

Paramètres

April 29, 2021

Cette section vous permet de définir tous les paramètres dont vous avez besoin dans votre StyleBook pour créer une configuration. Il décrit l'entrée que votre StyleBook prend. Bien que cette section soit facultative, la plupart des StyleBook peuvent en avoir besoin. Vous pouvez considérer la section Paramètres pour définir les champs des utilisateurs qui utilisent le StyleBook pour créer une configuration sur une instance Citrix ADC.

Lorsque vous importez votre StyleBook dans Citrix ADM et que vous l'utilisez pour créer une configuration, l'interface graphique utilise cette section du StyleBook pour afficher un formulaire. Ce formulaire prend une entrée pour les valeurs de paramètre définies.

La section suivante décrit les attributs que vous devez spécifier pour chaque paramètre de cette section :

'nom'

Nom du paramètre que vous souhaitez définir. Vous pouvez spécifier un nom alphanumérique.

Le nom doit commencer par un alphabet et peut inclure plus d'alphabets, de nombres, de trait d'union (-) ou de trait de soulignement (_).

Lorsque vous écrivez un StyleBook, vous pouvez utiliser cet attribut « name » pour faire référence au paramètre dans d'autres sections en utilisant la notation $parameters. <name>.

Obligatoire ? Oui

‘étiquette’

Chaîne affichée dans l’interface graphique d’ADM en tant que nom de ce paramètre.

Obligatoire ? Non

‘description’

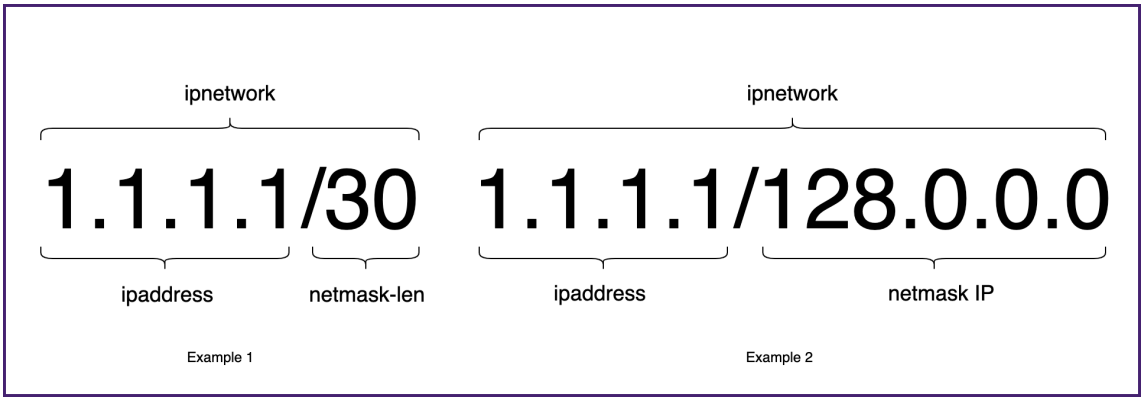
Chaîne d’aide qui décrit à quoi sert le paramètre. L’interface graphique ADM affiche ce texte lorsque l’utilisateur clique sur l’icône d’aide pour ce paramètre.

Obligatoire ? Non

‘type’

Type de valeur que ces paramètres peuvent prendre. Les paramètres peuvent être de l’un des types intégrés
suivants :

- `string` : Un tableau de caractères. Si aucune longueur n’est spécifiée, la valeur de la chaîne peut prendre n’importe quel nombre de caractères. Toutefois, vous pouvez limiter la longueur d’un type de chaîne en utilisant les attributs min-length et max-length.
- `number` : nombre entier. Vous pouvez spécifier le nombre minimum et maximum que ce type peut prendre en utilisant les attributs min-value et max-value.
- **`boolean`** : Peut être vrai ou faux. YAML considère tous les littéraux comme des booléens (par exemple, Oui ou Non).
- `ipaddress` : chaîne représentant une adresse IPv4 ou IPv6 valide.
- `ipnetwork` : Il a deux parties. La première partie est l’adresse IP et la deuxième partie est le masque de réseau.



Le masque de réseau est représenté par une longueur de masque réseau (`netmask-len`) ou une adresse IP de masque de réseau (`netmask_ip`). La longueur du masque de réseau est un

entier compris entre 0 et 32 et 0 à 128 pour une adresse IPv6. Il est utilisé pour déterminer le nombre d'adresses IP dans un réseau.

- `tcp-port` : nombre compris entre 0 et 65535 qui représente un port TCP ou UDP.
- `password` : Représente une valeur de chaîne opaque/secrète. Lorsque l'interface graphique ADM affiche une valeur pour ce paramètre, elle est affichée sous forme d'astérisques (*****).
- `certfile` : Représente un fichier de certificat. Cette valeur vous permet de charger les fichiers directement à partir de votre système local lorsque vous créez une configuration StyleBook à l'aide de l'interface graphique ADM. Le fichier de certificat téléchargé est stocké dans le répertoire `/var/mps/tenants/\<tenant_path>/ns_ssl_certs` d'ADM.

  Le fichier de certificat est ajouté à la liste des certificats gérés par ADM.
- `keyfile` : Représente un fichier de clé de certificat. Cette valeur vous permet de charger le fichier directement à partir de votre système local lorsque vous créez une configuration StyleBook à l'aide de l'interface graphique ADM. Le fichier de certificat téléchargé est stocké dans le répertoire `/var/mps/tenants/\<tenant_path>/ns_ssl_keys` d'ADM.

  Le fichier de clé de certificat est ajouté à la liste des clés de certificat gérées par ADM.
- `file` : Représente un fichier.
- `object` : Ce type est utilisé lorsque vous souhaitez regrouper plusieurs paramètres associés sous un élément parent. Spécifiez le paramètre parent le type comme « objet ». Un paramètre de type « objet » peut avoir une section « paramètres » imbriquée pour décrire les paramètres qu'il contient.
- `another StyleBook` : lorsque vous utilisez ce type de paramètre, ce paramètre s'attend à ce que sa valeur soit sous la forme des paramètres définis dans le StyleBook indiquant son type.

Un paramètre peut également avoir un `type` qui est la liste des types. Pour ce faire, ajoutez `[]` à la fin du type. Par exemple, si l' `type` attribut est `string[]`, ce paramètre prend une liste de chaînes en entrée. Vous pouvez fournir une, deux ou plusieurs chaînes pour ce paramètre lors de la création d'une configuration à partir de ce StyleBook.

Obligatoire ? Oui

'réseau'

Pour `type: ipaddress`, vous pouvez spécifier l' `network` attribut pour allouer automatiquement une adresse IP à partir d'un réseau ADM IPAM.

ADM alloue automatiquement une adresse IP à partir de l'attribut `network` lorsque vous créez une configuration StyleBook.

Exemple :


```
      name: virtual-ip
      label: "Load Balancer IP Address"
      type: ipaddress
      network: "network-1"
      required: true
<!--NeedCopy-->
```

Dans cet exemple, le `virtual-ip` champ alloue automatiquement une adresse IP à partir de `network-1`. L'adresse IP est libérée sur le réseau lorsque la configuration est supprimée.

'allocation dynamique'

L' `dynamic-allocation` attribut est ajouté dans la définition du paramètre de `type:ipaddress`. Utilisez cet attribut pour répertorier dynamiquement les réseaux ADM IPAM. Cet attribut peut prendre **`true`** soit soit **`false`** en entrée. Pour `type: ipaddress`, spécifiez l' `dynamic-allocation: true` attribut pour répertorier dynamiquement les réseaux ADM IPAM qui sont dans ADM. Dans le formulaire de création du pack de configuration, vous pouvez effectuer les opérations suivantes :

1. Sélectionnez le réseau IPAM requis dans la liste.
2. Spécifiez une adresse IP que vous souhaitez allouer à partir du réseau IPAM sélectionné.

   Si aucune adresse IP n'est spécifiée, l'ADM alloue automatiquement une adresse IP à partir du réseau IPAM sélectionné.

Exemple :

```
  -
    name: virtual-ip
    label: "Load Balancer IP Address"
    type: ipaddress
    dynamic-allocation: true
    required: true
<!--NeedCopy-->
```

Dans cet exemple, le `virtual-ip` champ répertorie les réseaux ADM IPAM qui sont dans ADM. Sélectionnez un réseau dans la liste pour allouer automatiquement une adresse IP à partir du réseau. L'adresse IP est libérée sur le réseau lorsque la configuration est supprimée.

'clé'

Spécifiez true ou false pour indiquer si ce paramètre est un paramètre clé pour le StyleBook.

Un StyleBook ne peut avoir qu'un seul paramètre défini comme le paramètre « key ».

Lorsque vous créez des configurations différentes à partir du même StyleBook (sur des instances ADC identiques ou
différentes), chaque configuration a une valeur différente ou unique pour ce paramètre.

La valeur par défaut est false.

Obligatoire ? Non

« requis »

Spécifiez true ou false pour indiquer si un paramètre est obligatoire ou facultatif. S'il est défini sur true, le paramètre est obligatoire et l'utilisateur doit fournir une valeur pour ce paramètre lors de la création de configurations.

L'interface graphique ADM oblige l'utilisateur à fournir une valeur valide pour ce paramètre.

La valeur par défaut est false.

Obligatoire ? Non

« valeurs allouées »

Utilisez cet attribut pour définir une liste de valeurs valides pour un paramètre, lorsque le type est défini sur « string. »

Lors de la création d'une configuration à partir de l'interface graphique ADM, l'utilisateur est invité à sélectionner une valeur de paramètre dans cette liste. Cette liste est statique, l'utilisateur ne peut sélectionner qu'une valeur dans la liste. Si vous souhaitez autoriser l'utilisateur à ajouter des valeurs à la liste, utilisez l'attribut [allow-**new**-values] (#allow -new-values).

> **Remarque**
>
> Si vous souhaitez afficher les valeurs de la liste sous forme d'options radio, définissez l'attribut [layout] (#layout).

Exemple 1 :

```
1 -
2       name: ipaddress
3       type: string
4       allowed-values:
5             -  SOURCEIP
6             -  DEST IP
7             -  NONE
8 <!--NeedCopy-->
```


Exemple 2 :

```
-
      name: TCP Port
      type: tcp-port
      allowed-values:
            - 80
            - 81
            - 8080
<!--NeedCopy-->
```

Exemple 3 :

Liste de `tcp-ports`, où chaque élément de la liste ne peut avoir que des valeurs spécifiées dans `allowed-values`.

```
-
      name: tcpports
      type: tcp-port[]
      allowed-values:
            - 80
            - 81
            - 8080
            - 8081
<!--NeedCopy-->
```

Obligatoire ? Non

'autorise-nouvelles valeurs'

Utilisez cet attribut pour ajouter une liste dynamique pour un paramètre. Lors de la création ou de la mise à jour d'une configuration à partir de l'interface graphique ADM, l'utilisateur peut ajouter des valeurs à la liste.

Spécifiez true si vous souhaitez que l'utilisateur ajoute une valeur à la liste des paramètres. Vous pouvez utiliser les `allowed-values` attributs `allow-new-values` et dans une combinaison. Cette combinaison vous permet de définir une liste de valeurs suggérées pour un paramètre et d'accepter de nouvelles valeurs.

```
-
      name: port
      type: tcp-port
      allowed-values:
            - 80
            - 81
```



```
            - 8080
      allow-new-values: true
<!--NeedCopy-->
```

Dans cet exemple, un utilisateur peut choisir entre 80, 81, 8080 ou entrer une nouvelle valeur pour le paramètre `port` lors de la création ou de la mise à jour d'un pack de configuration.

« par défaut »

Utilisez cet attribut pour affecter une valeur par défaut à un paramètre facultatif. Lorsqu'un utilisateur crée une configuration sans spécifier de valeur, la valeur par défaut est utilisée.

Le paramètre ne prend aucune valeur si les conditions suivantes sont remplies :

- Le paramètre n'a pas de valeur par défaut.
- Un utilisateur ne fournit pas de valeur pour le paramètre.

Exemple 1 :

```
-
      name: timeout
      type: number
      default: 20
<!--NeedCopy-->
```

Exemple 2 :

Pour répertorier les valeurs par défaut du paramètre :

```
-
      name: protocols
      type: string[]
      default:
            - TCP
            - UDP
            - IP
<!--NeedCopy-->
```

Exemple 3 :

```
-
      name: timeout
      type: number
      default: 20
<!--NeedCopy-->
```


Exemple 4 :

```
-
      name: tcpport
      type: tcp-port
      default: 20
<!--NeedCopy-->
```

Obligatoire ? Non

« modèle »

Utilisez cet attribut pour définir un motif (expression régulière) pour les valeurs valides de ce paramètre, lorsque le type du paramètre est « string. »

Exemple :

```
-
      name: appname
      type: string
      pattern: "[a-z]+"
<!--NeedCopy-->
```

Obligatoire ? Non

‘Min-valeur’

Utilisez cet attribut pour définir la valeur minimale pour les paramètres de type `number` ou `tcp-port`.

Exemple :

```
-
      name: audio-port
      type: tcp-port
      min-value: 5000
<!--NeedCopy-->
```

Les `min-value` nombres peuvent être négatifs. Cependant, le `min-value` for `tcp-port` doit être positif.

Obligatoire ? Non

‘max-value’

Utilisez cet attribut pour définir la valeur maximale des paramètres de type `number` ou `tcp-port`.

Assurez-vous que la valeur maximale est supérieure à la valeur minimale, si elle est définie.

Exemple :

```
-
      name: audio-port
      type: tcp-port
      min-value: 5000
      max-value: 15000
<!--NeedCopy-->
```

Obligatoire ? Non

‘min-longueur’

Utilisez cet attribut pour définir la longueur minimale des valeurs acceptées pour un paramètre de type « string. »

Assurez-vous que la longueur minimale des caractères définis comme valeurs est supérieure ou égale à zéro.

Exemple :

```
-
      name: appname
      type: string
      min-length: 3
<!--NeedCopy-->
```

Obligatoire ? Non

‘longueur’

Utilisez cet attribut pour définir la longueur maximale des valeurs acceptées pour un paramètre de type « string. »

Assurez-vous que la longueur maximale des valeurs est supérieure ou égale à la longueur des caractères définis dans `min-length`.

Exemple :

```
-
      name: appname
      type: string
      max-length: 64
<!--NeedCopy-->
```


Obligatoire ? Non

‘min-items’

Utilisez cet attribut pour définir le nombre minimal d’éléments d’un paramètre qui est une liste.

Assurez-vous que le nombre minimum d’articles est supérieur ou égal à zéro.

Exemple :

```
-
      name: server-ips
      type: ipaddress[]
      min-items: 2
<!--NeedCopy-->
```

Obligatoire ? Non

‘max-items’

Utilisez cet attribut pour définir le nombre maximal d’éléments dans un paramètre qui est une liste.

Assurez-vous que le nombre maximal d’éléments est supérieur au nombre minimal d’éléments si défini.

Exemple :

```
-
      name: server-ips
      type: ipaddress[]
      min-items: 2
      max-items: 250
<!--NeedCopy-->
```

Obligatoire ? Non

‘gui’

Utilisez cet attribut pour personnaliser la disposition du paramètre dans l’interface graphique ADM.

Obligatoire ? Non

‘colonnes’

Cet attribut est un sous-attribut de l’ `gui` attribut. Utilisez cet attribut pour définir le nombre de colonnes pour afficher les `type: object[]` paramètres dans l’interface graphique ADM.

Obligatoire ? Non

‘updatable’

Cet attribut est un sous-attribut de l’ `gui` attribut. Utilisez cet attribut pour spécifier si le paramètre peut être mis à jour après la création de la configuration. Définissez cet attribut uniquement sur des types de paramètres simples tels que chaîne, booléenne ou nombre.

Si la valeur est définie sur **`false`**, le champ paramètre est grisé lorsque vous mettez à jour la configuration.

Obligatoire ? Non

‘collapse_pane’

Cet attribut est un sous-attribut de l’ `gui` attribut. Utilisez cet attribut pour spécifier si le volet définissant la disposition de ce paramètre d’objet est réductible.

Si la valeur est définie sur true, l’utilisateur peut développer ou réduire les paramètres enfants sous ce paramètre parent.

Exemple :

```
gui:

 collapse_pane: true

 columns: 2
<!--NeedCopy-->
```

Exemple de section complète des paramètres :

```
parameters:

   -

      name: name

      label: Name

      description: Name of the application
```



```
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
```



```
                label: Server Port

                description: The TCP port of the server

                type: tcp-port

                default: 80

        -

                name: lb-alg

                label: LoadBalancing Algorithm

                type: string

                allowed-values:

                   - ROUNDROBIN

                   - LEASTCONNECTION

                default: ROUNDROBIN

        -

                name: enable-healthcheck

                label: Enable HealthCheck?

                type: boolean

                default: true
<!--NeedCopy-->
```

Voici un exemple qui définit tous les attributs d'une liste et les valeurs expliquées dans les sections précédentes :

```
        -
                name: features-list

                type: string[]

                min-length: 1

```



```
                max-length: 3

                min-items: 1

                max-items: 3

                pattern: "[A-Z]+"

                allowed-values:

                  - SP

                  - LB

                  - CS

                default:

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

‘mise en page ‘

Cet attribut est un sous-attribut de l’ `gui` attribut. Utilisez cet attribut pour afficher les valeurs de liste sous forme de boutons radio. Définissez l’ `layout` attribut sur `radio` dans la section des paramètres d’une définition StyleBook. Elle s’applique au paramètre qui a l’attribut [`allowed-values`] (#allowed -values). Lorsque vous créez un pack de configuration, l’interface graphique ADM affiche les valeurs de la `allowed-values` liste sous forme de boutons radio.

Exemple :

```
-
    gui:
        layout: radio
    allowed-values:
        - One
        - Two
        - Three
<!--NeedCopy-->
```

Les valeurs Un, Deux et Trois apparaissent sous forme de boutons radio dans l’interface graphique ADM.

‘paramètres-dépendants’

Cet attribut est un sous-attribut de l’ `gui` attribut. Il contrôle dynamiquement l’apparence du paramètre ou sa valeur initiale dans l’écran de configuration StyleBook en fonction de la valeur spécifiée dans un autre paramètre.

Spécifiez cet attribut sur un paramètre source qui contrôle le comportement du paramètre sur le formulaire. Vous pouvez inclure plusieurs conditions qui contrôlent d’autres paramètres. Par exemple, un paramètre source `protocol` peut avoir un paramètre dépendant `certificate`, qui n’apparaît que si la valeur du `protocol` paramètre est `SSL`.

Chaque condition peut avoir les attributs suivants :

- **target-paramètre** : spécifiez le paramètre cible auquel cette condition s’applique.
- **valeurs de correspondance** : spécifiez la liste des valeurs du paramètre source qui déclenche l’action.
- **action** : spécifiez l’une des actions suivantes sur le paramètre ciblé :
  - `read-only` : le paramètre est en lecture seule.
  - `show` : le paramètre apparaît dans le formulaire s’il est masqué.
  - `hide` : le paramètre est supprimé du formulaire.
  - `set-value` : la valeur du paramètre est définie sur la valeur spécifiée dans l’attribut value.
- **value** : valeur du paramètre cible si l’action est `set-value`.

Lorsqu’une entrée utilisateur correspond aux valeurs spécifiées sur le paramètre source, l’apparence ou la valeur du paramètre cible change en fonction de l’action spécifiée.

Exemple :

```
1  -
2     name: lb-virtual-port
3     label: "Load Balanced App Virtual Port"
4     description: "TCP port representing the Load Balanced application"
5     type: tcp-port
6     gui:
7       updatable: false
8       dependent-parameters:
9             -
10              matching-values:
11                - 80
12              target-parameter: $parameters.lb-service-type
13              action: set-value
14              allowed-values:
15              - HTTP
```



```
16                - TCP
17                - UDP
18
19      default: 80
20
21  <!--NeedCopy-->
```

Dans cet exemple, le paramètre dépendant est spécifié sous le `lb-virtual-port` paramètre (paramètre source).

Lorsque la valeur du paramètre source est définie sur `80`, le `lb-service-type` paramètre déclenche l' `set-value` action. Par conséquent, un utilisateur est autorisé à sélectionner l'une des options suivantes :

- HTTP
- TCP
- UDP

Parameters-default-sources construct

April 29, 2021

Vous pouvez utiliser cette construction pour réutiliser les définitions de paramètres d'autres StyleBooks.

Considérons 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` où vous définissez tous les paramètres qui lui sont associés, comme illustré dans l'exemple suivant :

```
1       -
2
3       name: vip-params
4
5       namespace: com.acme.commontypes
6
```



```
version: "1.0"

description: This StyleBook defines a typical virtual IP config.

private: true

schema-version: "1.0"

parameters:

  -

      name: lb-appname

      label: Load Balanced Application Name

     description: Name of the Load Balanced application

      type: string

      required: true

  -

      name: lb-virtual-ip

      label: Load Balanced App Virtual IP address

      description: Virtual IP address representing the Load
         Balanced application

      type: ipaddress

      required: true

  -

      name: lb-virtual-port

      label: Load Balanced App Virtual Port

      description: TCP port representing the Load Balanced
         application

      type: tcp-port
```



```
50
51              default: 80
52
53          -
54
55              name: lb-service-type
56
57              label: Load Balanced App Protocol
58
59              description: Protocol used for the Load Balanced application
                    .
60
61              type: string
62
63              default: HTTP
64
65              required: true
66
67              allowed-values:
68
69                   - HTTP
70
71                   - SSL
72
73                   - TCP
74  <!--NeedCopy-->
```

Ensuite, vous pouvez créer d'autres StyleBooks qui utilisent ces paramètres. Voici un exemple d'un tel StyleBook.

```
1       -
2
3       name: acme-biz-app
4
5       namespace: com.acme.stylebooks
6
7       version: "1.0"
8
9       description: This stylebook defines the Citrix ADC configuration
            for Biz App
10
11      schema-version: "1.0"
12
13      import-stylebooks:
14
```



```
15          -
16
17              namespace: com.acme.commontypes
18
19              prefix: cmtypes
20
21              version: "1.0"
22
23          \*\*parameters-default-sources:\*\*
24
25  **              - cmtypes::vip-params**
26
27          parameters:
28
29              -
30
31                name: monitorname
32
33                label: Monitor Name
34
35                description: Name of the monitor
36
37                type: string
38
39                required: true
40
41              -
42
43                name: type
44
45                label: Monitor Type
46
47                description: Type of the monitor
48
49                type: string
50
51                required: true
52
53                allowed-values:
54
55                  - PING
56
57                  - TCP
58
59                  - HTTP
```



```
60
61                - HTTP-ECV
62
63                - TCP-ECV
64
65                - HTTP-INLINE
66  <!--NeedCopy-->
```

Dans le StyleBook, `acme-biz-app`, d'abord, l'espace de noms et la version du `vip-params` StyleBook sont importés à l'aide de la section « import-stylebooks ». Ensuite, la construction **parameters-default-sources** est ajoutée et le nom de StyleBook, c'est-à-dire, `vip-params` est spécifié. Ce paramètre a le même effet que la définition des paramètres du `vip-params` StyleBook 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 d'autres StyleBooks, vous pouvez également définir vos propres paramètres à l'aide de la section Paramètres. La liste complète des paramètres du StyleBook est la combinaison des paramètres inclus dans d'autres StyleBooks et des paramètres définis dans ce StyleBook. Par conséquent, l'expression **$parameters** fait référence à cette combinaison de paramètres.

Si un paramètre est défini à la fois dans un StyleBook importé et dans le StyleBook actif, la définition du StyleBook actuel remplace la définition importée à partir d'un autre StyleBook. Vous pouvez utiliser cette approche efficacement en personnalisant quelques paramètres importés si nécessaire, tout en utilisant le reste des paramètres importés tels qu'ils sont.

La construction parameters-default-sources peut également être utilisée dans les paramètres imbriqués comme indiqué :

```
1  parameters:
2
3      -
4
5        name: vip-details
6
7        label: Virtual IP details
8
9        description: Details of the Virtual IP
10
11       type: object
12
13       required: true
14
15       parameters-default-sources:
```



```
16
17                - cmtypes::vip-params
18 <!--NeedCopy-->
```

Cette approche est similaire à l' `vip-params` ajout direct des paramètres du StyleBook en tant que paramètres enfants du `vip-details` paramètre dans ce StyleBook.

Substitutions

April 29, 2021

La section Substitutions permet de définir des noms abrégés pour les expressions complexes qui peuvent être utilisés dans le reste du StyleBook pour 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 la valeur de substitution uniquement lorsque cette valeur doit être modifiée plutôt que de la mettre à jour à chaque emplacement qu'elle apparaît dans le StyleBook, ce qui peut 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 un raccourci pour 8181. En utilisant une substitution, vous pouvez désigner cela dans le reste du StyleBook comme **$substitutions.http-port** au lieu de 8181.

substitutions :

```
http-port: 8181
```

Cela vous permet de spécifier un nom mnémonique à un numéro de port et de définir ce numéro de port en un seul endroit dans le StyleBook, quel que soit le nombre de fois où il est utilisé. Si vous souhaitez modifier le numéro de port à 8080, vous pouvez le modifier dans la section de substitution, et la modification prendra effet partout où le nom mnémonique `http-port` est utilisé. L'exemple suivant montre comment une substitution est utilisée dans un composant.

```
1 components:
2
3  -
4
5      name: my-lbvserver-comp
```



```
6
7       type: ns::lbvserver
8
9       properties:
10
11            name: $parameters.name + "-lb"
12
13            servicetype: HTTP
14
15            ipv46: $parameters.ip
16
17            port: $substitutions.http-port
18
19            lbmethod: $parameters.lb-alg
20  <!--NeedCopy-->
```

Une substitution peut également être une expression complexe. L'exemple suivant montre comment deux substitutions utilisent des expressions.

```
1  substitutions:
2
3    app-rule: HTTP.REQ.HEADER("X-Test-Application").EXISTS
4
5    app-name: str("acme-") + $parameters.name + str("-app")
6  <!--NeedCopy-->
```

Une expression de substitution peut également utiliser des expressions de substitution existantes comme indiqué dans l'exemple suivant.

```
1  substitutions:
2
3    http-port: 8181
4
5    app-name: str("acme-") + $parameters.name + str($substitutions.http-
       port) + str("-app")
6  <!--NeedCopy-->
```

Une autre caractéristique utile des substitutions est les cartes, où vous pouvez mapper des clés aux valeurs. Voici un exemple de substitution de carte.

```
1  substitutions:
2
3      secure-port:
4
5          true: int("443")
```



```
6
7           false: int("80")
8
9       secure-protocol:
10
11          true: SSL
12
13          false: HTTP
14  <!--NeedCopy-->
```

L'exemple suivant montre comment utiliser les cartes secure-port et secure-protocol.

```
1   components:
2
3    -
4
5        name: my-lbvserver-comp
6
7        type: ns::lbvserver
8
9        properties:
10
11             name: $parameters.name + "-lb"
12
13             servicetype: $substitutions.secure-protocol[$parameters.is-
                   secure]
14
15             ipv46: $parameters.ip
16
17             port: $substitutions.secure-port[$parameters.is-secure]
18
19             lbmethod: $parameters.lb-alg
20  <!--NeedCopy-->
```

Cela implique que si l'utilisateur du StyleBook spécifie la valeur booléenne « true » au paramètre is-secure, ou sélectionne la case à cocher correspondant à ce paramètre dans l'interface graphique Citrix ADM, la `servicetype` propriété de ce composant se voit attribuer la valeur **SSL** et la propriété port est attribué la valeur **443**. Toutefois, si l'utilisateur spécifie « false » pour ce paramètre ou désactivez la case à cocher correspondante dans l'interface graphique Citrix ADM, la valeur **HTTP** est affectée à la `servicetype` propriété 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 peuvent être de type simple, par exemple, string, number `ipaddress`, booléen, et d'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")
```

Il retourne `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 priorité et l’utilise pour calculer une valeur. Dans le reste du StyleBook, cette substitution peut être utilisée comme illustré dans l’exemple suivant :

```
components:

  -

    name: cspolicy-binding-comp

    type: ns::csvserver_cspolicy_binding

    condition: not $parameters.is-default

    properties:

         name: $parameters.csvserver-name

         policyname: $components.cspolicy-comp.properties.policyname

         priority: $substitutions.cspol-priority($parameters.pool.
            priority)
<!--NeedCopy-->
```

La substitution peut également être constituée d’une clé et d’une valeur. La valeur peut être une valeur simple, une expression, une fonction, une carte, une liste ou un dictionnaire.

Voici un exemple de substitution appelée `slist` dont la valeur est une liste :


```
substitutions:

  slist:

    - a

    - b

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

La valeur d'une substitution peut également être un dictionnaire de paires clé-valeur comme indiqué dans l'exemple suivant d'une substitution appelée `sdict` ci-dessous :

```
substitutions:

  sdict:

    a: 1

    b: 2

    c: 3
<!--NeedCopy-->
```

Vous pouvez créer des attributs plus complexes en combinant les listes et les dictionnaires. Par exemple, une substitution appelée `slistofdict` renvoie une liste de paires clé - valeur.

```
  slistofdict:

    -

      a: $parameters.cs1.lb1.port

      b: $parameters.cs1.lb2.port

    -

      a: $parameters.cs2.lb1.port

      b: $parameters.cs2.lb2.port
<!--NeedCopy-->
```

Mais, dans l'exemple suivant, une substitution `sdictoflist` renvoie une paire clé-valeur, où la valeur elle-même est une autre liste.


```
  sdictoflist:

    a:

      - 1

      - 2

    b:

      - 3

      - 4
<!--NeedCopy-->
```

Dans les composants, ces substitutions peuvent être utilisées dans les constructions de condition, de propriétés, de répétition, de condition.

L'exemple suivant d'un composant montre comment une substitution peut être utilisée pour spécifier les propriétés :

```
    properties:

      a: $substitutions.slist

      b: $substitutions.sdict

      c: $substitutions.slistofdict

      d: $substitutions.sdictoflist
<!--NeedCopy-->
```

Un cas d'utilisation pour définir une substitution dont la valeur est une liste ou un dictionnaire est lorsque vous configurez un serveur virtuel de commutation de contenu et plusieurs serveurs virtuels d'équilibrage de charge. Étant donné que 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. En `cs-pools` composant, nous attribuons la valeur de cette substitution à un paramètre lb-pool pour chaque pool.

```
substitutions:

  cs-port[]:

    true: int("80")

    false: int("443")

  lb-properties(name, servicetype, vip, port, servers):

    lb-appname: $name

    lb-service-type: $servicetype

    lb-virtual-ip: $vip

    lb-virtual-port: $port

    svc-servers: $servers

    svc-service-type: $servicetype

    monitors:

      -

        monitorname: $name

        type: PING

        interval: $parameters.monitor-interval

        interval_units: SEC

        retries: 3

components:

  -

    name: cs-pools

```



```
43      type: stlb::cs-lb-mon
44
45      description: | Updates the cs-lb-mon configuration with the
            different pools provided. Each pool with rule result in a dummy
            LB vserver, cs action, cs policy, and csvserver_cspolicy_binding
             configuration.
46
47      condition: $parameters.server-pools
48
49      repeat: $parameters.server-pools
50
51      repeat-item: pool
52
53      repeat-condition: $pool.rule
54
55      repeat-index: ndx
56
57      properties:
58
59        appname: $parameters.appname + "-cs"
60
61        cs-virtual-ip: $parameters.vip
62
63        cs-virtual-port: $substitutions.cs-port($parameters.protocol == "
              HTTP")
64
65        cs-service-type: $parameters.protocol
66
67        pools:
68
69          -
70
71            lb-pool: $substitutions.lb-properties($pool.pool-name, "HTTP"
                  , "0.0.0.0", 0, $pool.servers)
72
73            rule: $pool.rule
74
75            priority: $ndx + 1
76  <!--NeedCopy-->
```

Carte de substitution :

Vous pouvez créer des substitutions qui mappent les clés aux valeurs. Par exemple, considérez 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.


```
substitutions:

     port:

          HTTP: 80

          DNS: 53

          SSL: 443
<!--NeedCopy-->
```

Dans cet exemple, HTTP est mappé à 80, DNS à 53 et SSL à 443. Pour récupérer le port d'un certain protocole qui est 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

April 29, 2021

La construction Components dans un StyleBook est considérée comme la section la plus importante du StyleBook. Dans cette section, vous définissez les objets de configuration à créer. En utilisant 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 paramètres pour adapter la configuration générée par le StyleBook. Il s'agit d'une section facultative, bien que la plupart des StyleBooks aient une section de composants.

Le tableau suivant décrit les principaux attributs d'un composant.

Attribut	Description
nom	Nom du composant. Vous pouvez spécifier un nom alphanumérique. Le nom doit commencer par un alphabet et peut inclure des alphabets, des nombres, un trait d'union (-) ou un trait de soulignement (_).
description	Description du rôle de ce composant dans le StyleBook.
type	Le type détermine les propriétés que ce composant fournit. Les composants ont deux types de types : **Type intégré** : Ce type est fourni par le système et vous n'avez pas à le définir, par exemple, les types d'entité NITRO `lbvserver` ou `servicegroup`. Lorsqu'un composant dispose d'un attribut type intégré, il crée un objet de configuration de ce type sur l'Citrix ADC. Par exemple, si un composant fait référence au type intégré `lbvserver`, ce composant crée un serveur virtuel d'équilibrage de charge sur l'instance Citrix ADC qui est la cible de la configuration. **Type composite** : Ce type fait référence à un StyleBook existant que vous avez créé et importé dans Citrix Application Delivery Management (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, reportez-vous à la section Créer un StyleBook composite.

Attribut	Description
propriétés	Sous-attributs pouvant 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 attributs de l'objet NITRO correspondant. Pour un composant dont le type est un autre StyleBook, c'est-à-dire un type composite, les propriétés correspondent aux paramètres définis dans ce StyleBook.

Exemple :

```
components:

   -

     name: my-lbvserver-comp

     type: ns::lbvserver

     properties:

        name: $parameters.name

        servicetype: HTTP

        ipv46: $parameters.ip

        port: 80

        lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

Dans cet exemple, vous avez défini un composant appelé `my-lbvserver-comp`. Ce composant est de 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 aviez spécifiés 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 `lbvserver` ressource et vous permet de spécifier des valeurs pour ces attributs.

Dans cet exemple, vous spécifiez des valeurs statiques pour `servicetype` et port tandis que le nom, ipv46 et les `lbmethod` propriétés obtiennent leurs valeurs à partir des paramètres d'entrée. Vous faites référence aux noms de paramètres définis dans la section paramètres en utilisant $parameters.<name>, par exemple, $parameters.ip.

Pour en savoir plus sur toutes les ressources Citrix ADC NITRO disponibles et leurs attributs/propriétés, consultez la documentation API Citrix ADC NITRO REST.

> **Remarque**
>
> Vous devez utiliser des minuscules pour les noms d'attributs des types de ressources NITRO (ses propriétés de composant). Sinon, l'importation d'un StyleBook échouera.

Composants d'assistance

April 29, 2021

L'utilisation principale de la section Composants d'un StyleBook consiste à générer des objets de configuration via des types intégrés 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 Helper prennent les entrées d'autres sections comme 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 montre un extrait d'un StyleBook utilisé pour créer un serveur d'équilibrage de charge avec monitor (`lb-mon-comp`) sur une instance Citrix ADC.

```
parameters:

  -

    name: appname

    type: string

  -

    name: ips

    type: ipaddress[]

```



```
15   -
16
17     name: vip
18
19     type: ipaddress
20
21 components:
22
23   -
24
25     name: help-comp
26
27     type: cmtypes::server-ip-port-params
28
29     repeat:
30
31       repeat-list: $parameters.ips
32
33       repeat-item: server-ip
34
35     properties:
36
37       ip: $server-ip
38
39       port: 80
40
41  -
42
43     name: lb-mon-comp
44
45     type: stlb::lb-mon
46
47     properties:
48
49       lb-appname: $parameters.appname
50
51       lb-virtual-ip: $parameters.vip
52
53       lb-virtual-port: 80
54
55       lb-service-type: HTTP
56
57       svc-service-type: HTTP
58
59       svc-servers: $components.help-comp.properties
```



```
60
61 <!--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 `lb-mon-comp` composant, le `svc-servers` paramètre de `lb-mon` StyleBook attend une liste d'objets où chaque élément comporte 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 $parameters.ips en une liste d'objets. Ceci est réalisé en utilisant le composant assistant, help-comp dans l'exemple ci-dessus. Le composant help-comp est de type `server-ip-port-params` StyleBook. Ce StyleBook ne comporte aucun composant. Par conséquent, il ne crée aucun objet de configuration. Help-comp crée une liste de répétition sur $parameters.ips et construit un objet qui se compose de `ip` et port (qui est défini sur un statique 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 des `svc-servers` propriétés. Le résultat de la comp help-comp est affecté à la `svc-servers` propriété de `lb-mon-comp`.

Propriétés facultatives

April 29, 2021

Parfois, une propriété d'un composant prend sa valeur 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 le `lbmethod` (algorithme d'équilibrage de charge) d'un composant dont le type est ns lbvserver. La valeur de la propriété `lbmethod` est extraie d'une valeur de paramètre fournie par l'utilisateur, comme indiqué ci-dessous :

```
1 components
2
3   -
4
5       name: lbvserver_comp
6
```



```
      type: ns::lbvserver

      properties:

        name: $parameters.lb-appname + "-lb"

        servicetype: $parameters.lb-service-type

        ipv46: $parameters.lb-virtual-ip

        port: 80

        lbmethod: $parameters.lb-advanced.algorithm
<!--NeedCopy-->
```

Maintenant, considérez que le paramètre **lb-advanced.algorithm** est un paramètre facultatif. Et, si l'utilisateur ne fournit pas de valeur pour ce paramètre parce qu'il est facultatif, l'expression **$parameters.lb-advanced.algorithm** est évaluée à valeur vide. Par conséquent, une valeur non valide est passée pour la `lbmethod` propriété. Afin d'éviter une telle situation, vous pouvez annoter la propriété comme facultative en suffixant son nom avec « ? « comme suit :

```
components

   -

     name: lbvserver_comp

     type: ns::lbvserver

     properties:

       name: $parameters.lb-appname + "-lb"

       servicetype: $parameters.lb-service-type

       ipv46: $parameters.lb-virtual-ip

       port: 80

       lbmethod?: $parameters.lb-advanced.algorithm
<!--NeedCopy-->
```

L'utilisation de « ? « omet la propriété si l'expression sur le droit n'évalue rien, ce qui équivaudrait, dans ce cas, à un composant défini comme suit :


```
components

  -

    name: lbvserver_comp

    type: ns::lbvserver

    properties:

      name: $parameters.lb-appname + "-lb"

      servicetype: $parameters.lb-service-type

      ipv46: $parameters.lb-virtual-ip

      port: 80
<!--NeedCopy-->
```

Parce que **lbmethod** est facultative, l'omettre fait toujours un composant valide. Notez que `lbmethod` peut prendre sa valeur par défaut si l'on est défini dans son type « ns⊠ lbvserver. «

Properties-default-source construction

April 29, 2021

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 (à partir d'autres StyleBooks) dans un StyleBook, la construction properties-default-sources permet à l'utilisateur de spécifier les propriétés d'un composant en fonction des sources existantes.

Les propriétés d'un composant peuvent être réparties entre différentes sections du StyleBook. Par exemple, les propriétés peuvent provenir de paramètres d'objet, de substitutions qui renvoient un objet, de propriétés d'autres composants ou de sorties d'autres composants. Dans de tels cas, vous devez redéfinir les propriétés qui se produisent dans d'autres sections du StyleBook dans la définition du composant. De toute évidence, 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 `lbvserver` configuration. Ce composant définit les propriétés de la `lbvserver` comme suit.


```
parameters:

  -

    name: lb

    type: ns::lbvserver

components:

  -

    name: lb-comp

    type: ns::lbvserver

    properties:

      name: $parameters.lb.name

      ipv46: $parameters.lb.ipv46

      port: $parameters.lb.port

      servicetype: $parameters.lb.servicetype

      lbmethod: $parameters.lb.lbmethod
<!--NeedCopy-->
```

Dans l'exemple ci-dessus, observez que les valeurs de toutes les propriétés définies dans la section composants sont extraites de l'objet $parameters.lb. Bien qu'elles soient extraites d'une seule source, les propriétés sont à nouveau définies dans le StyleBook. En outre, si un nouveau sous-paramètre à l'objet $parameters.lb qui est pertinent pour la configuration de l' `lbvserver` est ajouté, vous devez mettre à jour le composant lb-comp pour ajouter la nouvelle propriété qui correspond au nouveau sous-paramètre.

Pour éviter de redéfinir les propriétés et récupérer toutes les propriétés pertinentes d'un composant sans les énumérer explicitement dans la section propriétés, la construction properties-default-sources peut être utilisée. L'exemple ci-dessus peut être écrit comme suit.

```
parameters:

  -

```



```
5      name: lb
6
7      type: ns::lbvserver
8
9  components:
10
11    -
12
13     name: lb-comp
14
15     type: ns::lbvserver
16
17     properties-default-sources:
18
19       - $parameters.lb
20 <!--NeedCopy-->
```

Dans l'exemple ci-dessus, l'utilisation de la construction properties-default-sources conduit à une réduction de la taille de la définition du composant, ce qui vous permet de définir de manière concise un composant. De plus, chaque fois que la source des propriétés du composant change, les modifications sont reflétées automatiquement. Par exemple, lorsqu'une nouvelle propriété, disons `persistencetype`, est ajoutée à l'objet $parameters.lb, cette propriété est ajoutée à la configuration de lb-comp par défaut car `persistencetype` est une propriété de `lbvserver`. Ainsi, la construction properties-default-sources fournit une interface dynamique pour définir les composants sans se soucier des changements qui se produisent dans les sources des propriétés du composant.

Calcul des propriétés du composant

Cette section explique comment les propriétés sont récupérées si la construction properties-default-sources est utilisée dans un composant. Tout d'abord, le compilateur StyleBooks identifie la liste des propriétés d'un composant en fonction de son type (dans l'exemple ci-dessus, `lbvserver`.) Ensuite, le compilateur récupère ces propriétés à partir des sources multiples 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 comporte au moins une section propriétés-default-sources ou une section propriétés. Il peut avoir les deux.

Composants imbriqués

April 29, 2021

L'imbrication d'un composant dans un autre composant permet au composant imbriqué de créer ses objets de configuration en faisant référence 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 est un moyen de faciliter la tâche des composants pour construire des objets de configuration dans un contexte existant des composants parents.

Exemple :

```
components:

 -

  name: my-lbvserver-comp

  type: ns::lbvserver

   properties:

      name: $parameters.name + "-lb"

      servicetype: HTTP

      ipv46: $parameters.ip

      port: 80

      lbmethod: $parameters.lb-alg

      components:

        -

         name: my-svcg-comp

         type: ns::servicegroup

         properties:

```



```
31              name: $parameters.name + "-svcgrp"
32
33              servicetype: HTTP
34
35          components:
36
37              -
38
39                name: lbvserver-svg-binding-comp
40
41                type: ns::lbvserver_servicegroup_binding
42
43                properties:
44
45                  name: $parent.parent.properties.name
46
47                  servicegroupname: $parent.properties.name
48
49                    -
50
51                      name: members-svcg-comp
52
53                      type: ns::servicegroup_servicegroupmember_binding
54
55                      repeat:
56
57                        repeat-list: $parameters.svc-servers
58
59                        repeat-item: srv
60
61                      properties:
62
63                        ip: $srv
64
65                        port: str($parameters.svc-port)
66
67                        servicegroupname: $parent.properties.name
68  <!--NeedCopy-->
```

Dans cet exemple, l'imbrication à plusieurs niveaux est utilisée. Le composant `my-lbvserver-comp` a un composant enfant appelé `my-svcg-comp`. Et, le `my-svcg-comp` composant comporte deux composants enfants. Le `my-svcg-comp` composant est utilisé pour créer un objet de configuration de groupe de services sur l'instance Citrix ADC en fournissant des valeurs aux attributs du type de ressource NITRO intégré "`servicegroup`. « Le premier composant enfant du `my-svcg` composant,

`lbvserver-svg-binding-comp`, est utilisé pour lier le groupe de services créé par son composant parent au serveur virtuel d'équilibrage de charge (`lbvserver`) créé par le composant parent du 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 d'un StyleBook pour itérer sur la liste des services spécifiés pour le paramètre `svc-servers`. Pour plus d'informations sur les constructions répétées, reportez-vous à la section Répéter la construction.

Vous pouvez également créer les mêmes objets de configuration sans utiliser l'imbrication de composants. Pour plus d'informations et d'exemples, consultez la page StyleBook pour créer une configuration d'équilibrage de charge de base.

Construct de condition

April 29, 2021

Vous pouvez rendre un composant conditionnel à l'aide d'une construction de condition. La valeur d'une construction conditionnelle est une expression booléenne qui évalue à true ou false. Si la condition est vraie, le composant est utilisé pour construire ses objets de configuration. Si la condition est false, le composant est ignoré et aucun objet de configuration n'est créé par ce biais. L'expression booléenne est souvent basée sur des valeurs de paramètre.

Exemple :

```
components:

      -

        name: servicegroup-comp

        type: ns::servicegroup

        condition: $parameters.svc-server-ips

        properties:

              name: $parameters.name + "-svcgrp"

              servicetype: HTTP
<!--NeedCopy-->
```


Dans cet exemple, si l'utilisateur spécifie une valeur pour le paramètre facultatif `svc-server-ips` , le composant, `servicegroup-comp`, est traité par le moteur StyleBook. Si la condition est false, c'est-à-dire si l'utilisateur ne fournit pas de valeur à ce paramètre, une valeur NULL est affectée à ce paramètre et est évaluée à false, alors le moteur StyleBook ignore la présence de ce composant et aucun n' `servicegroup` 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 construit l'objet de configuration de type NITRO ns : :systemfile si la condition est évaluée à true.

Exemple :

```
1       components
2
3           -
4
5             name: pem_key_files
6
7             type: ns::systemfile
8
9             condition: "$components.der-certificate-files-comp or
                 $components.pem-certificate-files-comp"
10
11            properties:
12
13                    filecontent: $certificate.keyfile.contents
14
15                    fileencoding: "BASE64"
16
17                    filelocation: "/nsconfig/ssl"
18
19                    filename: $certificate.keyfile.filename
20  <!--NeedCopy-->
```

Dans cet exemple, la condition est une expression « ou » complexe, dans laquelle vous souhaitez que cet objet de configuration soit créé par le StyleBook uniquement si deux autres composants du StyleBook ont été traités (non ignorés), créant ainsi une dépendance entre les composants.

Répéter la construction

April 29, 2021

Vous pouvez utiliser la construction **répétée** d'un composant pour créer plusieurs objets de configuration du même type.

Dans l'exemple suivant, le composant **members-svcg-comp** est utilisé pour lier la liste des services au groupe de services créé par le composant parent. Pour créer un objet de configuration qui lie chaque serveur au groupe de services, utilisez la construction de **répétition** pour parcourir la liste des services spécifiés pour le paramètre **svc-servers**. Au cours de l'itération, le composant crée un objet NITRO de type **servicegroup_servicegroupmember_binding** pour chaque service (appelé **srv** dans la construction **répét-item**) dans le groupe de services, et il définit l'attribut **ip** de chaque objet NITRO sur l'adresse IP du service correspondant.

Exemple :

```
components:
  -
      name: my-lbvserver-comp
      type: ns::lbvserver
      properties:
           name: $parameters.name + "-lb"
           servicetype: HTTP
           ipv46: $parameters.ip
           port: 80
           lbmethod: $parameters.lb-alg
           components:
                -
                   name: my-svcg-comp
                   type: ns::servicegroup
                   properties:
                        name: $parameters.name + "-svcgrp"
                        servicetype: HTTP
                   components:
                         -
                         name: lbvserver-svg-binding-comp
                         type: ns::lbvserver\servicegroup\binding
                         properties:
                               name: $parent.parent.properties.name
                               servicegroupname: $parent.properties.
                                   name
                         -
                         name: members-svcg-comp
```



```
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 la **liste de répétition** et **l'élément de répétition** sont des attributs de l'objet de répétition.

- 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 courant dans l'itération.

Si non spécifié, l'élément actuel 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
3           name: members-svcg-comp
4
5           type: ns::servicegroup_servicegroupmember_binding
6
7           repeat:
8
9             repeat-list: $parameters.svc-servers
10
11          properties:
12
13                 ip: $repeat-item
14
15                 port: $parameters.svc-port
16
17                 servicegroupname: $parent.properties.name
18 <!--NeedCopy-->
```

En plus de pouvoir faire référence à l'élément courant en blanc itérant sur une liste, il est également possible de faire référence à l'index courant de l'élément dans la liste en utilisant l' **index répété**. Dans l'exemple suivant, l' **index répété** est utilisé pour calculer un numéro de port basé sur l'index courant :


```
            name: services

            type: ns::service

            repeat:

               repeat-list: $parameters.app-services

               repeat-item: srv

            properties:

                ip: $parameters.app-ip

                port: $parameters.base-port + repeat-index

                servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

Semblable à la construction **repeat-item**, vous pouvez attribuer un nom de variable différent pour faire référence à l'index courant de l'itération. L'exemple précédent est équivalent à l'exemple suivant :

```
    -

            name: services

            type: ns::service

            repeat:

               repeat-list: $parameters.app-services

               repeat-item: srv

               repeat-index: idx

            properties:

                ip: $parameters.app-ip

                port: $parameters.base-port + $idx

                servicegroupname: $parent.properties.name
<!--NeedCopy-->
```


Construct à condition répétée

April 29, 2021

La construction de condition répétée est évaluée dans chaque itération d'une construction de répétition et le résultat détermine s'il faut construire l'objet de configuration dans cette itération ou passer à l'itération suivante. L'exemple suivant montre l'utilisation de la construction repeat-condition :

Exemple :

```
components

   -

      name: der-key-files-comp

      type: ns::systemfile

      repeat:

      repeat-list: $parameters.certificates

      repeat-item: certificate

        repeat-condition: $certificate.ssl-inform == DER

        properties:

         filecontent: base64($certificate.keyfile.contents)

         fileencoding: BASE64

         filelocation: /nsconfig/ssl

         filename: $certificate.keyfile.file
<!--NeedCopy-->
```

Dans cet exemple, le `der-key-files-comp` composant itère sur tous les certificats donnés par l'utilisateur, mais il ne génère que des objets de configuration qui correspondent aux certificats avec encodage 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 construit dans l'itération actuelle et l'itération passe au certificat suivant dans la liste.

Répétitions imbriquées

April 29, 2021

Avec la construction de répétition imbriquée, vous pouvez avoir plus d'une construction de répétition dans chaque composant en fonction de la définition du composant. Considérez une répétition imbriquée de deux niveaux. Pour chaque élément de la liste externe (première liste de répétition), vous pouvez créer une liste de répétition pour tous les éléments de la liste interne (deuxième liste de répétition). Le compilateur StyleBook prend en charge jusqu'à trois répétitions imbriquées. Chaque niveau de répétition a des attributs d'élément répétitif et d'index répétitif qui lui sont associés. Les attributs repeat-item et repeat-index sont facultatifs. En outre, chaque répétition peut également spécifier une condition de répétition.

Exemple :

```
parameters:

  -

      name: vips

      type: ipaddress[]

  -

      name: vip-ports

      type: tcp-port[]

components:

  -

      name: lbvservers-comp

      type: ns::lbvserver

      repeat:

         repeat-list: $parameters.vips

         repeat-item: ip

         repeat:
```



```
30
31                repeat-list: $parameters.vip-ports
32
33                repeat-item: port
34
35        properties:
36
37           name: str("lb-") + str($ip) + '-' + str($port)
38
39           servicetype: HTTP
40
41           ipv46: $ip
42
43           port: $port
44  <!--NeedCopy-->
```

Dans cet exemple, pour chaque élément dans `$parameters.vips`, nous itérons sur tous les éléments de `$parameters.vip-ports`. Ainsi, pour chacun `ipaddress` spécifié dans `$parameters.vips`, nous créons des objets `lbvserver` de configuration 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 de l'adresse IP et du numéro de port.

Si l' `repeat-item` attribut n'est pas fourni, le compilateur génère une valeur par défaut pour lui. Les valeurs par défaut pour l'élément répété sont : `$repeat-item`, `$repeat-item-1`, `$repeat-item-2` respectivement pour chaque niveau de répétition. De même, si l' `repeat-index` attribut n'est pas fourni, le compilateur génère une valeur par défaut pour lui. 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 de répétition et d'index répétitif dans un objet répétition imbriqué.

Exemple :

```
1  components:
2
3  -
4
5       name: lbvservers-comp
6
7       type: ns::lbvserver
8
9       repeat:
10
```



```
          repeat-list: $parameters.vips

          repeat:

             repeat-list: $parameters.vip-ports

      properties:

         name: str("lb-") + str($repeat-item) + '-' + str($repeat-item
            -1)

         servicetype: HTTP

         ipv46: $repeat-item

         port: $repeat-item-1
<!--NeedCopy-->
```

Sorties

April 29, 2021

Dans la section Sorties, vous spécifiez ce qu'un StyleBook expose à ses utilisateurs une fois la création de tous les objets de configuration terminée. La section sorties d'un StyleBook est facultative. Un StyleBook n'a pas besoin de renvoyer des sorties. Cependant, en renvoyant certains composants internes en tant que sorties, il permet à tous les StyleBooks qui l'importent plus de flexibilité que vous pouvez le voir lors de la création d'un StyleBook composite.

Le tableau suivant décrit les attributs utilisés dans la section Sorties.

Attribut	Description	Obligatoire
nom	Nom de la sortie correspondant à l'objet de configuration à exposer.	Oui
description	Chaîne de texte décrivant la sortie.	Non
valeur	Cet attribut spécifie comment extraire la valeur renvoyée par un StyleBook.	Oui

Exemple :

```
outputs:

 -

   name: lbvserver

   description: LBVServer component

   value: $components.my-lbvserver-comp

 -

   name: svc-grp

     description: ServiceGroup name

     value: $components.my-svcg.properties.name
<!--NeedCopy-->
```

Dans cet exemple, vous exposez le composant **lbvserver** et le `servicegroup` **nom** qui serait créé 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 `servicegroup` créé par le composant **my-svcg**.

Référence des paramètres

April 29, 2021

Dans la construction des composants, vous faites référence aux paramètres définis dans la section paramètres à l'aide de la notation `$parameters.<parametername>`. Si `<parametername>` contient des paramètres (lorsque le type est objet), vous devez utiliser la notation, `$parameters.<parametername>.<sub-parametername>`et ainsi de suite.

Exemple :

```
parameters:

  -

    name: name

```



```
    label: Name

    type: string

    required: true

     -

      name: vip

      label: Virtual IP and Port

      type: object

      required: true

      parameters:

        -

          name: ip

          label: Virtual IP

          description: The Virtual IP Address

          type: ipaddress

          required: true

            -

              name: port

              label: The Virtual Port

              description: The TCP port for the Virtual IP

              type: tcp-port

              default: 80

components:

  -
```



```
52
53      name: my-lbvserver-comp
54
55      type: ns::lbvserver
56
57      properties:
58
59         name: $parameters.name
60
61         servicetype: HTTP
62
63         ipv46: $parameters.vip.ip
64
65         port: $parameters.vip.port
66  <!--NeedCopy-->
```

Référence parente

April 29, 2021

Si vous utilisezcomposants 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 construit dans l'itération actuelle par le parent.

Exemple :

```
1  components:
2
3   -
4
5    name: my-lbvserver-comp
6
7    type: ns::lbvserver
8
9    properties:
10
11     name: $parameters.name + "-lb"
12
13     servicetype: HTTP
```



```
14
15      ipv46: $parameters.ip
16
17      port: 80
18
19      lbmethod: $parameters.lb-alg
20
21      components:
22
23        -
24
25          name: my-svcg-comp
26
27          type: ns::servicegroup
28
29          properties:
30
31            name: $parameters.name + "-svcgrp"
32
33            servicetype: HTTP
34
35            components:
36
37             -
38
39               name: lbvserver-svg-binding-comp
40
41               type: ns::lbvserver_servicegroup_binding
42
43               properties:
44
45                  name: $parent.parent.properties.name
46
47                  servicegroupname: $parent.properties.name
48
49                    -
50
51                      name: members-svcg-comp
52
53                      type: ns::servicegroup_servicegroupmember_binding
54
55                      repeat: $parameters.svc-servers
56
57                      repeat-item: srv
58
```



```
                    properties:

                      ip: $srv

                      port: str($parameters.svc-port)

                      servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

Vous pouvez également naviguer vers le haut dans la hiérarchie des composants en accédant aux propriétés des parents des parents jusqu'aux composants de niveau supérieur. Par exemple, le nom de propriété du composant **lbvserver-svg-binding-comp** prend sa valeur du nom de propriété du parent de son parent, le composant **my-lbvserver-comp**, en utilisant la notation **$parent.parent** .

Référence des composants

April 29, 2021

Dans la construction de composants, vous faites référence à un composant de niveau supérieur dans le StyleBook à l'aide de la `$components.<componentname>` notation. S'il y a des composants imbriqués dans un composant de niveau supérieur, la notation utilisée est `$components.<componentname>.components.<component-name>` pour y faire référence, etc.

Exemple :

```
components:

 -

     name: my-lbvserver-comp

     type: ns::lbvserver

     properties:

        name: $parameters.name + "-lb"

        servicetype: HTTP

        ipv46: $parameters.ip

        port: 80

```



```
        lbmethod: $parameters.lb-alg

 -

    name: my-svcg-comp

    type: ns::servicegroup

    properties:

       name: $parameters.name + "-svcgrp"

       servicetype: HTTP

-

    name: members-svcg-comp

    type: ns::servicegroup_servicegroupmember_binding

    repeat: $parameters.svc-servers

    repeat-item: srv

    properties:

       ip: $srv

       port: str($parameters.svc-port)

       servicegroupname: $components.my-svcg-comp.properties.name

-

    name: lbvserver-svg-binding-comp

    type: ns::lbvserver_servicegroup_binding

    properties:

        name: $components.my-lbvserver-comp.properties.name

        servicegroupname: $components.my-svcg-comp.properties.name
<!--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 indiquées par `$components.<componentname>`.

Référence des substitutions

April 29, 2021

Dans la section Composants ou la section Opérations, vous faites référence aux substitutions définies dans la section Substitutions à l'aide de la**`$substitutions.<substitution-name>`**notation. Par exemple, **$substitutions.http-port**.

Si une substitution est une carte, vous pouvez désigner un élément de la carte comme**`$substitutions.<substitutions-name>[<map-key>]`**. Par exemple, **`$substitutions.protocol-map[$parameters.port]`**.

Référence variable

April 29, 2021

Lorsque vous utilisez les constructions de répétition et d'élément répété dans des composants pour créer plusieurs objets de configuration, vous pouvez attribuer un nom de variable à la construction d'élément répété. 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 :

```
components:

  -

    name: server-members-comp

    type: ns::server

    condition: $parameters.svc-server-domain-names

    repeat: $parameters.svc-server-domain-names
```



```
12
13      repeat-item: server-name
14
15      properties:
16
17        name: $server-name + "-server"
18
19        domain: $server-name
20
21      components:
22
23        -
24
25           name: service-members-comp
26
27           type: ns::service
28
29           properties:
30
31             name: $server-name + "-service"
32
33             servername: $parent.properties.name
34
35             servicetype: $parameters.svc-service-type
36
37             port: $parameters.svc-server-port
38  <!--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 référencé dans les propriétés du même composant et dans les composants enfants `$<varname>`.

Opérations

April 29, 2021

La `Operations` est une section facultative dans un StyleBook. Dans cette section, vous pouvez configurer Citrix Application Delivery Management (ADM) Analytics pour collecter les enregistrements AppFlow sur l'ensemble ou une partie des transactions de trafic. Le serveur virtuel créé sur une instance de 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 ADC 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 ADC Gateway Insight ou l'un d'entre eux.

Toute Citrix ADM Insight activée sur les instances Citrix ADC via StyleBooks utilise un protocole IPFIX (AppFlow) pour envoyer les données des instances à Citrix ADC.

En outre, lorsque vous activez Web Insight, les « Mesures côté client » sont activées sur l'équilibrage de charge et les serveurs virtuels de commutation de contenu. Lorsque cette fonctionnalité est activée, ADM capture les mesures de temps de chargement et de rendu des pages HTML par injection HTML. À l'aide de ces mesures, les administrateurs peuvent identifier les problèmes de latence L7.

Exemple 1 :

L'exemple suivant montre comment écrire la section Opérations dans un StyleBook pour activer HDX Insight et Citrix ADC Gateway Insight sur un serveur virtuel VPN :

```
name: simple-vpn-ops

namespace: com.example.stylebooks

schema-version: "1.0"

version: "0.1"

description: Test StyleBook to enable hdxinsight and gatewayinsight on
    a VPN vserver

import-stylebooks:

  -

    namespace: netscaler.nitro.config

    version: "10.5"

```



```
    prefix: ns

components:

  -

    name: vpnvserver-comp

    type: ns::vpnvserver

    properties:

      name: str("vpn-") + str($current-target.ip)

      servicetype: SSL

      ipv46: 1.1.21.37

      port: 443

operations:

    analytics:

      -

        name: comp-ops

        properties:

          target: $components.vpnvserver-comp

          filter: "true"

          insights:

            -

              type: hdxinsight
            -
              type: gatewayinsight

outputs:

  -
```



```
64
65      name: myvpns
66
67      value: $components.vpnvserver-comp
68  <!--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-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: vpnvserver-comp
14         type: ns::vpnvserver
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.vpnvserver-comp
26                 filter: "true"
27                 insights:
28                   -
29                    type: hdxinsight
30                    -
31                    type: gatewayinsight
32 outputs:
33   -
```



```
34      name: myvpns
35      value: $components.vpnvserver-comp
36  <!--NeedCopy-->
```

Analytics

April 29, 2021

La sous-section analytique de la section Opérations a une structure similaire à la section Composants. Chaque élément de la section Analytics est utilisé pour configurer la fonctionnalité Citrix Application Delivery Management (ADM) Analytics pour un ou plusieurs serveurs virtuels créés par le StyleBook.

Un élément de la section Analytics possède les attributs suivants :

Attribut	Description	Obligatoire
nom	Nom de l'élément analytique.	Oui
description	Chaîne de texte décrivant ce qu'est cet élément.	Non
condition	Une expression booléenne. Lorsque cette condition est évaluée à false, l'élément analytique entier est ignoré.	Non
répétition	Itère sur une liste.	Non
condition répétée	Une expression booléenne. Si l'expression est évaluée à false, l'itération actuelle est ignorée.	Non
article répété	Nom de l'élément dans l'itération actuelle.	Non
index répété	Nom de la valeur d'index de l'itération en cours.	Non
propriétés	La liste des propriétés de l'analytique.	Oui

Attribut	Description	Obligatoire
cible	Une des propriétés de la liste. L'expression cible est le nom d'un serveur virtuel, configuré sur l'Citrix ADC, pour lequel les analyses seront collectées.	Oui
filtre	Une des propriétés de la liste. La valeur de cet attribut est une expression de stratégie avancée Citrix ADC qui est utilisée pour filtrer les requêtes sur le serveur virtuel pour lesquelles les analyses seront collectées. Par défaut, les données d'analyse sont collectées sur tout le trafic passant par le serveur virtuel.	Non

Exemple :

```
operations:

  analytics:

    -

    name: lbvserver-ops-comp

    properties:

    target: $components-basic-lb-comp.outputs.lbvserver-name

    filter: HTTP.REQ.URL.CONTAINS("catalog")

    insights:
          -
            type: webinsight
<!--NeedCopy-->
```

Chaque attribut de la section Analytics est utilisé pour demander à la fonctionnalité Citrix ADM Ana-

lytics de configurer les instances Citrix ADC pour collecter les enregistrements AppFlow sur le serveur virtuel identifié par la propriété cible.

Alarmes

April 29, 2021

La sous-section des alarmes de la section Opérations a une structure similaire et les mêmes attributs que dans la sous-section analytique. La seule différence est dans l'attribut properties. Pour obtenir la liste de tous les attributs (autres que l'attribut properties), reportez-vous à la sectionAnalytics.

Les propriétés suivantes sont disponibles dans une sous-section d'alarme :

Attribut	Description	Obligatoire
`target`	Expression qui évalue le nom d'un serveur virtuel, configuré sur Citrix ADC, pour lequel les alarmes sont configurées.	Oui
`email-profile`	Nom d'un profil de messagerie défini dans la fonctionnalité Analytics Citrix Application Delivery Management (ADM) et qui contient une liste d'adresses de messagerie que vous souhaitez notifier lorsque l'alarme est déclenchée.	Non (un `email-profile` ou un `sms-profile` doit être défini)
`sms-profile`	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 `email-profile` ou un `sms-profile` doit être défini)

Attribut	Description	Obligatoire
`rules`	Liste de règles définissant les conditions qui déclencheraient une alarme pour le serveur virtuel défini par la propriété cible.	Oui
`metric`	Un attribut de règle. Nom d'une mesure que vous souhaitez suivre concernant le serveur virtuel Citrix ADC.	Oui
`operator`	Un attribut de règle. Opérateur à utiliser pour comparer la mesure à la valeur. Les opérateurs valides sont `greaterthan` et `lessthan`.	Oui
`value`	Un attribut de règle. Valeur de seuil à laquelle la mesure est comparée à l'aide de l'opérateur. Si la valeur de mesure dépasse ce seuil, les alarmes associées sont déclenchées.	Oui
`period-unit`	Attribut d'une règle. Fréquence à laquelle alerter les utilisateurs si la règle d'alarme est respectée. Cet attribut peut contenir la valeur jour, heure ou hebdomadaire. Cela signifie que si la règle est respectée, une alarme est envoyée une fois par unité de période (par exemple, une fois par jour).	Oui

Le tableau suivant fournit une liste des mesures qui font l'objet d'un suivi 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 session VPN	Nombre total de sessions actives sur ce serveur virtuel VPN démarrées pendant un intervalle de temps spécifié par l'utilisateur.	Compteur d'augmentation monotone, incrémenté à chaque nouveau lancement de 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.	Compteur d'augmentation monotone à chaque lancement d'une nouvelle application
app_launch_duration	Durée du lancement de l'application VPN	Temps moyen 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 demandes	Nombre de demandes client sur ce serveur virtuel depuis le dernier redémarrage de la appliance ou depuis la création du serveur virtuel, selon la date la plus récente.	Compteur d'augmentation monotone, incrémenté sur chaque nouvelle requête à ce serveur virtuel.

Compteurs	Description	Description détaillée	Calcul de Citrix ADM
total_octets	Octets	Nombre total d'octets transférés du serveur virtuel vers Citrix ADM sur l'intervalle de temps spécifié.	Compteur augmentant systématiquement pour tenir compte du nombre total d'octets desservis 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 des deux éventualités.

Exemple d'une section d'alarmes dans un StyleBook :

```
operations:
alarms:
 -
  name:lbvserver_alarm
  properties:
  target: $outputs.lbvserver
  email-profile: $parameters.emailprofile
  sms-profile: "NetScalerSMS"
     rules:
      -
        metric: "total_requests"
        operator: "greaterthan"
        value: 25
        period-unit: weekly
        -
          metric: "total_bytes"
          operator: "lessthan"
          value: 1024
```



```
            period-unit: day

<!--NeedCopy-->
```

Expressions

April 29, 2021

L'une des caractéristiques les plus puissantes d'un StyleBook est l'utilisation d'expressions. Vous pouvez utiliser des expressions StyleBooks dans différents scénarios pour calculer des valeurs dynamiques. L'exemple suivant est une expression permettant de concaténer une valeur de paramètre avec une chaîne littérale.

Exemple :

```
$parameters.appname + "-mon"
```

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

- Addition (+)
- Soustraction (-)
- Multiplication (*)
- Division (/)
- Modulo (%)

Exemples :

- Ajout de deux nombres : $parameters.a + $parameters.b
- Multiplication de deux nombres : $parameters.a * 10
- Trouver le reste après division d'un nombre par un autre :

`15%10` Résultats en `5`

Expressions de chaîne

- Concaténer deux chaînes (+)

Exemple :

Concaténer deux chaînes : str (« app- ») + $parameters.appname

Liste des expressions

Fusionne deux listes (+)

Exemple :

- Concaténer deux listes : $parameters.external-servers + $parameters.internal-servers
- Si `$parameters.ports-1` est [80, 81] et `$parameters.port-2` est [81, 82], le `$parameters.ports-1 + $parameters.ports-2` s'affiche sous forme de liste [80, 81, 81, 82].

Expressions relationnelles

- **==** : Teste si deux opérandes sont égaux et renvoie true s'ils sont égaux, sinon renvoie false.
- **!** = : Teste si deux opérandes sont différents et renvoie true s'ils sont différents, sinon renvoie false.
- ** : Retourne true si le premier opérande est supérieur au second opérande, sinon renvoie false.
- **>=** : Retourne true si le premier opérande est supérieur ou égal au second opérande, else renvoie false.
- **<** : Renvoie true si le premier opérande est inférieur au second opérande, sinon renvoie false.
- **<=** : Retourne true si le premier opérande est inférieur ou égal au second opérande, else renvoie false.

Exemple :

- Utilisation de l'opérateur Equality : `$parameters.name = = "abcd"`
- Utilisation de l'opérateur d'inégalité : `$parameters.name != "default"`
- Exemples pour d'autres opérateurs relationnels

  - `10 > 9`
  - `10 >= 10`
  - `0 < 9`
  - `10 <= 9`
  - `10 == 10`
  - `10 != 1`

Expressions logiques - booléenne

- **et** : L'opérateur logique 'et'. Si les deux opérandes sont vraies, 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 le sens inverse.
- **in** : Teste si le premier argument est une sous-chaîne du second argument
- **in** : Teste si un élément fait partie d'une liste

> **Remarque**
>
> Vous pouvez type-cast expressions où les chaînes sont converties en nombres (en utilisant la fonction intégrée int ()) et les nombres sont convertis en chaînes (en utilisant la fonction intégrée str ()). De même, vous pouvez `tcp-port` convertir en un nombre (en utilisant la fonction intégrée int ()), et une adresse IP peut être convertie en une chaîne (en utilisant la fonction intégrée str ()).
>
> Utilisez un délimiteur avant et après tout opérateur. Vous pouvez utiliser les délimiteurs suivants :
>
> - Devant un opérateur : `space`, `tab`, `comma`, `(`, `)`, `[`, `]`
> - Après un opérateur : `space`, `tab`, `(`, `[`
>
> Par exemple :
>
> - `abc + def`
> - `100 % 10`
> - `10 > 9`
> - `$item in $parameters.some-list`

Expressions de chaîne verbatim

Vous pouvez utiliser des chaînes textuelles lorsque les caractères spéciaux d'une chaîne doivent prendre leur forme littérale. Ces chaînes peuvent contenir des caractères d'échappement, des barres obliques inverses, des guillemets, des parenthèses, des espaces blancs, des crochets, etc. Dans les chaînes textuelles, l'interprétation habituelle des caractères spéciaux est ignorée. Tous les caractères de la chaîne sont conservés dans leur forme littérale.

Dans StyleBooks, vous pouvez inclure des expressions de stratégie Citrix ADC dans leur forme littérale à l'aide de chaînes textuelles. Les expressions de stratégie contiennent généralement des caractères spéciaux. Sans chaînes textuelles, vous devez échapper à des caractères spéciaux en divisant les chaînes en sous-chaînes.

Pour créer une chaîne textuelle, encapsulez une chaîne entre des caractères spéciaux comme suit :

```
~{
 string }
 ~
<!--NeedCopy-->
```


Vous pouvez utiliser des chaînes textuelles dans les expressions StyleBook.

> **Remarque**
>
> N'utilisez pas la séquence de caractères } ~ dans une chaîne d'entrée car cette séquence indique la fin d'une chaîne textuelle.

Exemple :

```
~{
HTTP.REQ.COOKIE.VALUE("jsessionid") ALT HTTP.REQ.URL.BEFORE_STR("=").
    AFTER_STR(";jsessionid=") ALT HTTP.REQ.URL.AFTER_STR(";jsessionid="
    ) }
~
<!--NeedCopy-->
```

Concaténer plusieurs chaînes textuelles

Vous pouvez concaténer des chaînes textuelles avec les chaînes régulières ou des chaînes avec interpolations. Lorsque vous le faites, le StyleBook ignore l'interprétation uniquement pour les chaînes textuelles. Utilisez l'opérateur plus (+) entre les chaînes à concaténer.

Exemple :

```
value: "~{
 "id": " }
 ~ + %{
 $atom.key }
 % + ~{
 ", "value": " }
 ~ + %{
 $atom.value }
 % + ~{
 " }
 ~"
<!--NeedCopy-->
```

Dans cet exemple, `%{ $atom.key } %` et `%{ $atom.value } %` sont interprétés. Et, l'interprétation est ignorée pour le reste.

Expressions cibles

Dans une définition StyleBook, vous pouvez utiliser l' `$current-target` expression pour faire référence à l'instance ADC cible actuelle. Pour référer spécifiquement une adresse IP de l'instance ADC cible, utilisez cette expression comme suit :


```
$current-target.ip
<!--NeedCopy-->
```

Exemple :

```
components:
 -
  name: lb-comp
  type: ns::lbvserver
  properties:
    name: $current-target.ip + "-lbvserver"
<!--NeedCopy-->
```

Dans cet exemple, le nom de l' `lbvserver` utilise l'adresse IP de l'instance ADC cible.

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 d'un StyleBook lui-même plutôt que lors de la création du pack de configuration.

Toutes les références aux paramètres, substitutions, composants, propriétés des composants, sorties des composants, variables définies par l'utilisateur (élément répété, index répété, arguments aux fonctions de substitution) et ainsi de suite sont toutes validées pour leur existence et leur type.

Exemple de vérifications de type :

Dans l'exemple suivant, le type attendu de propriété port de `lbvserver` StyleBook est `tcp-port`. Dans Citrix Application Delivery Management (ADM), les validations de type se produisent au moment de la compilation (au moment de l'importation). Le compilateur trouve cette chaîne et ne `tcp-port` sont pas des types compatibles et, par conséquent, le compilateur StyleBook affiche une erreur et ne parvient pas à importer ou à migrer un StyleBook.

```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: str("80")
      servicetype: HTTP
<!--NeedCopy-->
```


Pour compiler ce StyleBook avec succès, déclarez ce qui suit en tant que nombre dans le compilateur :

```
port: 80
```

Exemple de marquage d'expressions non valides :

Dans les versions antérieures, lorsqu'une expression non valide était affectée à un nom de propriété, le compilateur ne détectait pas les expressions non valides et autorisait l'importation des StyleBooks dans Citrix ADM. Maintenant, si ce StyleBook est importé dans Citrix ADM, le compilateur identifie ces expressions non valides et l'indique. Par conséquent, le StyleBook ne parvient pas à importer vers Citrix ADM.

Dans cet exemple, l'expression affectée à la propriété name dans le `lb-sg-binding-comp` composant est : `$components.lbvserver-comp.properties.lbvservername`. Cependant, il n'y a aucune propriété appelée `lbvservername` dans le composant `lbvserver-comp`. Dans les versions antérieures 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. Cependant, ce type d'erreur est détecté lors de l'importation et le StyleBook n'est pas importé dans Citrix ADM. Corrigez manuellement ces erreurs et importez les StyleBooks.

```
Components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: 80
      servicetype: HTTP
  -
    name: sg-comp
    type: ns::servicegroup
    properties:
      servicegroupname: mysg
      servicetype: HTTP
  -
    name: lb-sg-binding-comp
    type: ns::lbvserver_servicegroup_binding
    condition: $parameters.create-binding
    properties:
      name: $components.lbvserver-comp.properties.lbvservername
      servicegroupname: $components.sg-comp.properties.servicegroupname
<!--NeedCopy-->
```


Listes d'indexation

Les éléments d'une liste sont maintenant accessibles en les indexant directement :

Expression	Description
`$components.test-lbs[0]`	Fait référence au premier élément du `thetest-lbs` composant
`$components.test-lbs[0].properties.p1`	Fait référence à la propriété p1 du premier élément du composant test-lbs
`$components.lbcomps[0].outputs.servicegroups[1].properties.servicegroupname`	Fait référence à `servicegroupname` la propriété du deuxième élément du `servicegroups` composant, qui est une sortie du premier élément du `lbcomps` composant

Interpolations sur place

April 29, 2021

Il est maintenant possible de remplacer des parties d'une chaîne à l'aide d'une expression 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 une valeur de l'expression. Pour inclure des expressions StyleBook dans une chaîne, nous utilisons la notation suivante :

```
"...%{
 ... }
 %..."
<!--NeedCopy-->
```

Où les caractères entre » % {"et « } % » forment une expression StyleBook. Ces expressions sont appelées « interpolations sur place. »

Par exemple, la chaîne `lb-%{ $parameters.appname } %-svc` est une expression de chaîne avec une interpolation sur place d'une expression StyleBook. La valeur de l'expression de chaîne dépend de la valeur de l'expression d'interpolation. Considérez que **$parameters.appname** est affecté avec "app1." Ensuite, l'expression de chaîne est évaluée à **lb-app1-svc**. Cela permet aux valeurs de ne pas être codées en dur dans les expressions de chaîne, mais plutôt 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. Considérez 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 voulez paramétrer l'objet dans l'URL HTTP, vous pouvez ajouter un paramètre de chaîne dans le StyleBook, disons, `$parameters.url-object`. L'expression de stratégie est écrite en fonction de ce paramètre. Pour ce faire, vous utilisez la concaténation de chaînes pour obtenir le résultat. L'expression ressemblerait à :

```
1 str("HTTP.REQ.URL.CONTAINS(\\"" + $parameters.url-object + "\\")")
2 <!--NeedCopy-->
```

Si `$parameter.url-object` est attribué « csv », l'expression ci-dessus est évaluée 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 :

```
1 str("HTTP.REQ.URL.CONTAINS(%{
2  quotewrap($parameters.url-object) }
3  %)")
4 <!--NeedCopy-->
```

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 le même que ce qui précède, 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 une valeur des types suivants dans les interpolations : booléenne `tcp-port`, number `ipaddress`, et string. La valeur générée est automatiquement transformée en chaîne lorsque les interpolations sont remplacées par le résultat.

Les expressions de chaîne peuvent avoir 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}%**” renvoie “lb-81” si $parameters.port a la valeur 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. La valeur des paramètres utilisés dans les exemples est la suivante :

- $parameters.appname: “lb1”
- $parameters.vip: “1.1.1.1”
- $parameters.n1: 1
- $parameters.n2: 3

Interpolations simples

Expression	Résultats
`lb-%{ $parameters.appname } %-def`	`lb-lb1-def`

Conversions automatiques de type

Expression	Résultats
lb-%{1}%	lb-1
lb-%{$parameters.vip}%	lb-1.1.1.1
lb-%{true}%	lb-True

Interpolations séquentielles

Expression	Résultats
%{$parameters.appname}%-%{str($parameters.appname)}%	lb1-lb1
lb-%{1}%-%{2}%	lb-1-2

Interpolations imbriquées

Expression	Résultats
`%{ abc-%{ $parameters.n1 + 1 } % } %`	`abc-2`
`str("%{ abc-%{ $parameters.n1 } % } %-%{ $parameters.n2 } %")`	`bc-1-3`

Interpolations avec `quotewrap`

Expression.	Résultats
`str("%{ quotewrap(abcd)} %")`	`\"abcd\`
`str("%{ quotewrap(https://)} %+HTTP.REQ.HOSTNAME+HTTP.REQ.URL")`	`<https://"+HTTP.REQ.HOST NAME+HTTP.REQ.URL`

Caractères d'échappement dans les interpolations

Si les caractères "%{" ou "}%" font partie de la chaîne, vous devez fournir "\" comme caractère d'échappement afin que le compilateur StyleBook ne les évalue pas en tant que 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	Résultats
—	—	—
Échapper les interpolations	`str("%{ str($parameters.n1)+ \ } \\% } %")`	`1 } %`
	`lb-%{ str($parameters.n1)+ \ } \\% } %`	`lb-1 } %`
	`"%{ str($parameters.n1)+ \\"\\ } \\\%\\"} %"`	`1 } %`

Fonctions intégrées

April 29, 2021

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 `str()` fonction transforme l'argument input en une valeur de chaîne.

Types d'arguments autorisés :

- `string`
- `number`
- `TCP-port`
- **`boolean`**
- `IP address`

Exemples :

- La `"set-"+ str(10)` fonction renvoie `"set-10"`.
- La `str(10)` fonction renvoie `10`.
- La `str(1.1.1.1)` fonction renvoie `1.1.1.1`.
- La `str(T rue)` fonction renvoie `"T rue"`.
- La `str(ADM)` fonction renvoie `"mas"`.

int()

La **`int()`** fonction prend une chaîne, un nombre, une adresse IP ou `tcpport` comme argument et renvoie un entier.

Exemples :

- La **`int("10")`** fonction renvoie `10`.
- La **`int(10)`** fonction renvoie `10`.
- La **`int(ip('0.0.4.1'))`** fonction renvoie `1025`.

bool()

La `bool()` fonction prend n'importe quel type comme argument. Si la valeur de l'argument est **`false`** vide ou absente, cette fonction renvoie **`false`**.

Sinon, il retourne **`true`**.

Exemples :

- La `bool(true)` fonction renvoie **`true`**.
- La `bool(false)` fonction renvoie **`false`**.
- La `bool($parameters.a)` fonction renvoie **`false`** si le `$parameters.a` est **`false`**, vide ou absent.

len()

La `len()` fonction prend une chaîne ou une liste comme argument, et renvoie le nombre de caractères dans une chaîne ou le nombre d'éléments d'une liste.

Exemple 1 :

Si vous définissez une substitution comme suit :

```
items: ["123", "abc", "xyz"]
```

La `len($substitutions.items)` fonction renvoie `3`

Exemple 2 :

La `len("Citrix ADM")` fonction renvoie `10`.

Exemple 3 :

Si `$parameters.vips` a des valeurs `['1.1.1.1', '1.1.1.2', '1.1.1.3']`, la `len($parameters.vips)` fonction renvoie `3`.

min()

La `min()` fonction prend soit une liste, soit une série de nombres ou `tcp-ports` comme arguments, et renvoie le plus petit élément.

Exemples avec une série de numéros/ports tcp :

- La `min(80, 100, 1000)` fonction renvoie `80`.
- La `min(-20, 100, 400)` fonction renvoie `-20`.
- La `min(-80, -20, -10)` fonction renvoie `-80`.
- La `min(0, 100, -400)` fonction renvoie `-400`.

Exemples avec une liste de numéros/tcp-ports :

- `$parameters.ports` Le support est une liste de `tcp-ports` et a des valeurs : `[80, 81, 8080]`.

  La `min($parameters.ports)` fonction renvoie `80`.

max()

La `max()` fonction prend une liste ou une série de nombres ou `tcp-ports` comme arguments, et renvoie le plus grand élément.

Exemples avec une série de numéros/ports tcp :

- La `max(80, 100, 1000)` fonction renvoie `1000`.
- La `max(-20, 100, 400)` fonction renvoie `400`.
- La `max(-80, -20, -10)` fonction renvoie `-10`.
- La `max(0, 100, -400)` fonction renvoie `100`.

Exemples avec une liste de numéros/tcp-ports :

- `$parameters.ports` Le support est la liste de `tcp-ports` et a des valeurs : `[80, 81, 8080]` .

  La `max($parameters.ports)` fonction renvoie `8080`.

bin()

La `bin()` fonction prend un nombre comme argument, et renvoie une chaîne qui représente le nombre au format binaire.

Exemples d'expressions :

La `bin(100)` fonction renvoie `0b1100100`.

oct()

La `oct()` fonction prend un nombre comme argument, et renvoie une chaîne qui représente le nombre au format octal.

Exemples d'expressions :

La `oct(100)` fonction renvoie `0144`.

hex()

La `hex()` fonction prend un nombre comme argument, et renvoie une chaîne minuscule qui représente le nombre au format hexadécimal.

Exemples d'expressions :

La `hex(100)` fonction renvoie `0x64`.

lower()

La `lower()` fonction prend une chaîne comme argument et renvoie la même chaîne en minuscules.

Exemple :

La `lower("ADM")` fonction renvoie `adm`.

upper()

La `upper()` fonction prend une chaîne comme argument et renvoie la même chaîne en majuscules.

Exemple :

La `upper("Citrix ADM")` fonction renvoie `CITRIX ADM`.

sum()

La `sum()` fonction prend une liste de nombres ou `tcpports` comme arguments et renvoie la somme des nombres dans la liste.

Exemple 1 :

Si vous définissez une substitution comme suit :
substitutions :

```
list-of-numbers = [11, 22, 55]
```

La `sum($substitutions.list-of-numbers)` fonction renvoie `88`.

Exemple 2 :

Si `$parameters.ports` c'est `[80, 81, 82]`, la `sum($parameters.ports)` fonction renvoie `243`.

pow()

La `pow()` fonction prend deux nombres comme arguments et renvoie un nombre qui représente le premier argument soulevé à la puissance du second.

Exemple :

La `pow(3,2)` fonction renvoie `9`.

ip()

La `ip()` fonction prend un entier, une chaîne ou une adresse IP comme argument et renvoie l'adresse IP en fonction de la valeur d'entrée.

Exemples :

- Spécifiez une adresse IP dans la `ip` fonction :

  La `ip(3.1.1.1)` fonction renvoie `3.1.1.1`.

- Spécifiez une chaîne dans la `ip` fonction :

  La `ip('2.1.1.1')` fonction renvoie `2.1.1.1`

- Spécifiez un entier dans la `ip` fonction :

  - La `ip(12)` fonction renvoie `0.0.0.12`.
  - Lorsque vous spécifiez un entier en tant que chaîne dans la `ip` fonction, il renvoie une adresse IP équivalente de l'entrée.

    La `ip('1025')` fonction renvoie `0.0.4.1`.

  Cette fonction prend également en charge les opérations d'addition et de soustraction entières et renvoie une adresse IP résultante.

  - Addition : La `ip(1025)+ ip(12)` fonction renvoie `0.0.4.13`.
  - Soustraction : La `ip('1025')- ip(12)` fonction renvoie `0.0.3.245`.
  - Combiner l'addition et la soustraction : Les `ip('1.1.1.1')+ ip('1.1.1.1')- ip(2)` retours `2.2.2.0`.

ip_network ()

La `ip_network` fonction prend l'adresse IP et la longueur du masque réseau comme arguments et renvoie une notation de réseau IP.

Example-1:

La `ip_network(1.1.1.1, 28)` fonction renvoie `1.1.1.1/28`.

Example-2:

Considérez le réseau `1.1.1.1/30`. La `ip_network($parameters.ipaddr, 30)` fonction renvoie `1.1.1.1`.

Example-3:

Considérez le réseau `23.1.12.76/24`. La `ip_network(23.1.12.76, $parameters.netmask-len)` fonction renvoie `24`.

network_ip ()

La `network_ip()` fonction renvoie la première adresse IP du réseau IP spécifié.

Exemple :

La `network_ip(1.1.1.1/28)` fonction renvoie `1.1.1.0`. Dans cet exemple, `1.1.1.0` est la première adresse IP du réseau donné.

sous-réseaux ()

La `subnets()` fonction renvoie la liste des sous-réseaux à partir du réseau IP spécifié et de la longueur du masque de réseau.

Exemple :

La `subnets(1.1.1.1/28, 30)` fonction renvoie la liste des sous-réseaux à partir du réseau IP et de la longueur du masque de réseau donnés. La sortie peut être la suivante :

```
[1.1.1.0/30', '1.1.1.4/30', '1.1.1.8/30', '1.1.1.12/30']
```

netmask_ip ()

La `netmask_ip()` fonction renvoie l'adresse IP du masque de réseau pour le réseau IP spécifié.

Exemple :

La `netmask_ip(1.1.1.1/28)` fonction renvoie `255.255.255.0`. Dans le réseau IP donné, `255.255.255.0` est l'adresse IP du masque de réseau.

broadcast_ip ()

La `broadcast_ip()` fonction renvoie l'adresse IP de diffusion pour le réseau IP spécifié.

Exemple :

La `broadcast_ip(1.1.1.1/28)` fonction renvoie `1.1.1.15`. Dans le réseau donné, `1.1.1.1` est l'adresse IP de diffusion.

cidr ()

La `cidr()` fonction renvoie la notation CIDR pour le réseau IP spécifié.

Exemple :

La `cidr(1.1.1.1/28)` fonction renvoie le `1.1.1.0/28`. Dans le réseau donné, `1.1.1.0/28` est la notation CIDR.

is_cidr ()

La `is_cidr()` fonction accepte un `ipnetwork` comme entrée. Et, il renvoie `True` si la valeur spécifiée correspond à la notation CIDR du réseau IP.

Example-1:

La `is_cidr(1.1.1.0/24)` fonction renvoie `True` car la valeur spécifiée est la notation CIDR du réseau donné.

Example-2:

La `is_cidr(1.1.1.1/28)` fonction renvoie `False` car la notation CIDR du réseau donné est différente de la valeur spécifiée.

is_in_network ()

La `is_in_network()` fonction accepte `ipnetwork` et `ipaddress` valeurs. Et, il renvoie `True` si l'adresse IP spécifiée existe dans le réseau IP spécifié.

Example-1:

La `is_in_network(1.1.1.1/24, 1.1.1.121)` fonction renvoie `True` car l' `1.1.1.121` adresse fait partie du `1.1.1.1/24` réseau.

Example-2:

La `is_in_network(1.1.1.1/28, 2.1.1.1)` fonction renvoie `Fasle` car l' `2.1.1.1` adresse ne fait pas partie du `1.1.1.1/28` réseau.

base64.encode()

La `base64.encode()` fonction prend un argument de chaîne et renvoie la chaîne codée base64.

Exemple :

La `base64.encode("abcd")` fonction renvoie `YWJjZA==`.

base64.decode()

La `base64.decode` fonction prend une chaîne codée base64 comme argument et renvoie la chaîne décodée.

Exemple :

La `base64.decode("YWJjZA==")` fonction renvoie `abcd`.

exists()

La `exists()` fonction prend un argument de n'importe quel type et renvoie un booléen. La valeur renvoyée est `True` si l'entrée a une valeur quelconque. La valeur de retour est `False` Si l'argument input n'a pas de valeur (c'est-à-dire, aucune valeur).

Considérez que le `$parameters.monitor` est un paramètre facultatif. Si vous fournissez une valeur à ce paramètre lors de la création d'un pack de configuration, existez la `($parameters.monitor)` fonction renvoie `True`.

Sinon, il retourne `False`.

filter()

La `filter()` fonction prend deux arguments.

Argument 1 : fonction de substitution qui prend un argument et renvoie une valeur booléenne.

Argument 2 : une liste.

La fonction renvoie un sous-ensemble de la liste d'origine où chaque élément est évalué `True` lorsqu'il est passé à la fonction de substitution dans le premier
argument.

Exemple :

Supposons que nous ayons défini une fonction de substitution comme suit.

Substitutions :

```
x(a): $a != 81
```

Cette fonction renvoie True si la valeur d'entrée n'est pas égale à `81`. Sinon, il retourne `False`.

Supposons,`$parameters.ports` est `[81, 80, 81, 89]`.

Les `filter($substitutions.x, $parameters.ports)` retours `[80, 89]` en supprimant toutes les occurrences `81` de de la liste.

if-then-else()

La fonction **`if`**`-then-`**`else`**`()` prend trois arguments.

Argument 1 : Expression booléenne

Argument 2 : Toute expression

Argument 3 : Toute expression (facultatif)

Si l'expression de l'argument 1 est évaluée à `True`, la fonction renvoie la valeur de l'expression fournie en tant qu'argument 2.

Sinon, si l'argument 3 est fourni, la fonction renvoie la valeur de l'expression dans l'argument 3.

Si l'argument 3 n'est pas fourni, la fonction renvoie `no`.

Exemple 1 :

La `if-then-else($parameters.servicetype == HTTP, 80, 443)` fonction renvoie `80` si `$parameters.servicetype` a une valeur `HTTP`. Sinon, la fonction retourne `443`.

Exemple 2 :

La `if-then-else($parameters.servicetype == HTTP, $parameters.hport, $parameters.sport)` fonction renvoie la valeur de `$parameters.hport` if `$parameters.servicetype` a une valeur `HTTP`.

Sinon, la fonction renvoie la valeur de `$parameters.sport`.

Exemple 3 :

Les `if-then-else($parameters.servicetype == HTTP, 80)` retours `80` si `$parameters.servicetype` a une valeur `HTTP`.

Sinon, la fonction ne renvoie aucune valeur.

join()

La `join()` fonction prend deux arguments :

Argument 1 : liste de nombres `tcp-ports`, de chaînes ou d'adresses IP

Argument 2 : chaîne de délimiteur (facultatif)

Cette fonction rejoint les éléments de la liste fournie en argument un dans une chaîne, où chaque élément est séparé par la chaîne de délimiteur fournie en argument deux. Si l'argument deux n'est pas fourni, les éléments de la liste sont joints sous la forme d'une seule chaîne.

Exemple :

- `$parameters.ports` est `[81, 82, 83]`.
  - Avec l'argument de délimiteur :

    La `join($parameters.ports, '-')` fonction renvoie `81-82-83`.
  - Sans argument de délimiteur :

    La `join($parameters.ports)` fonction renvoie `818283`.

Split ()

La `split()` fonction divise une chaîne d'entrée en plusieurs listes en fonction des séparateurs spécifiés. Si aucun séparateur ou vide (`''`) n'est spécifié, cette fonction considère l'espace comme un séparateur et divise la chaîne en listes.

Exemples :

- La `split('Example_string_split', 's')` fonction renvoie `['Example_','tring_','plit']`.
- La `split('Example string split')` fonction renvoie `['Example','string','split']`.
- La `split('Example string split', '')` fonction renvoie `['Example','string','split']`.
- La `split('Example string')` fonction renvoie `['Example','string']`.

  Cette fonction considère les espaces continus comme un seul espace.

map()

La `map()` fonction 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 `map()` fonction (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

  La `map(str, $parameters.nums)` fonction renvoie `["81", "82", "83"]`

  Le résultat de la fonction map est la liste des chaînes où chaque élément est une chaîne est calculée en appliquant la fonction str sur l'élément correspondant dans la liste d'entrée ($parameters.nums).

- Mapper à l'aide d'une fonction de substitution
  - Substitutions :

    ```
    add-10(port): $port + 10
    ```


- Expression :

  La `map($substitutions.add-10, $parameters.nums)` fonction 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 `quotewrap()` fonction prend une chaîne comme argument et renvoie une chaîne après avoir ajouté un caractère de guillemets doubles avant et après la valeur d'entrée.

Exemple :

La `quotewrap("ADM")` fonction renvoie `"mas"`

replace()

La `replace()` fonction prend trois arguments :

Argument 1 : chaîne

Argument 2 : chaîne ou liste

Argument 3 : chaîne (facultatif)

La fonction remplace toutes les occurrences de l'argument deux par l'argument trois dans l'argument un.

Si l'argument trois n'est pas fourni, toutes les occurrences de l'argument deux sont supprimées de l'argument 1 (en d'autres termes, remplacées par une chaîne vide).

Remplacez une sous-chaîne par une autre sous-chaîne :

- La `replace('abcdef', 'def', 'xyz')` fonction renvoie `abcxyz`.

  Toutes les occurrences de `def` sont remplacées par `xyz`.

- `replace('abcdefabc', 'def')` retourne `abcabc`.

  Comme il n'y a pas de troisième argument, `def` est supprimé de la chaîne résultante.

Spécifiez la liste de caractères que vous souhaitez remplacer dans une chaîne.

```
$parameters.spl_chars = ['@', '##', '!', '%']
```

Cette liste contient les valeurs qui doivent être remplacées dans une chaîne d'entrée.

La `replace('An##example@to%replace!characters', $parameters.spl_chars, '_')` fonction renvoie `An_example_to_replace_characters`.

La chaîne de sortie comporte un trait de soulignement (_) au lieu des caractères spécifiés dans la `$parameters.spl_chars` liste.

trim()

La `trim()` fonction renvoie une chaîne dans laquelle les espaces de début et de fin sont retirés de la chaîne d'entrée.

Exemple :

La `trim('abc ')` fonction renvoie `abc`.

truncate()

La `truncate()` fonction prend deux arguments :

Argument 1 : chaîne

Argument 2 : nombre

La fonction renvoie une chaîne où la chaîne d'entrée dans l'argument un est tronquée à la longueur spécifiée par l'argument deux.

Exemple :

Les `truncate('Citrix ADM', 6)` retours `Citrix`.

distinct ()

La `distinct()` fonction extrait des éléments uniques d'une entrée de liste.

Exemples :
Si `$parameters.input_list` c'est `['ADM', 'ADC', 'VPX', 'ADC', 'ADM', 'CPX']`, la `distinct($parameters.input_list)` fonction renvoie `['ADM', 'ADC', 'VPX', 'CPX']`.

url.encode ()

La `url.encode()` fonction renvoie une chaîne où les caractères sont transformés en utilisant le jeu de caractères ASCII selon RFC 3986.

Exemple :

La `url.encode("a/b/c")` fonction renvoie `a%2Fb%2Fc`.

url.decode ()

La `url.decode()` fonction renvoie une chaîne où l'argument encodé URL est décodé en une chaîne régulière selon RFC 3986.

Exemple :

La `url.decode("a%2Fb%2Fc")` fonction renvoie `a/b/c`.

is-ipv4()

La `is-ipv4()` fonction prend une adresse IP comme argument et renvoie le booléen `True` si l'adresse IP est au format IPv4.

La `is-ipv4(10.10.10.10)` fonction renvoie `True`

is-ipv6()

La `is-ipv6()` fonction prend une adresse IP comme argument et renvoie le booléen `True` si l'adresse IP est au format IPv6.

La `is-ipv6(2001:DB8::)` fonction renvoie `True`

startswith()

La fonction `startswith()` détermine si une chaîne commence par un préfixe donné. Cette fonction nécessite deux arguments de chaîne obligatoires.

```
startswith(str, sub_str)
```

Cette fonction retourne `True` lorsque la chaîne (`str`) commence par la sous-chaîne (`sub_str`).

Exemples :

- La `startswith('Citrix', 'Ci')` fonction renvoie `True`.
- La `startswith('Citrix', 'iC')` fonction renvoie `False`
- La `startswith('Citrix', 'Ab')` fonction renvoie `False`

endswith()

La fonction `endswith()` détermine si une chaîne se termine par un suffixe donné. Cette fonction nécessite deux arguments de chaîne obligatoires.

```
endswith(str, sub_str)
```

Cette fonction retourne `True` lorsque la chaîne (`str`) se termine par la sous-chaîne (`sub_str`).

Exemples :

- La `endswith('Citrix', 'ix')` fonction renvoie `True`.
- La `endswith('Citrix', 'Ix')` fonction renvoie `False`.
- La `endswith('Citrix', 'ab')` fonction renvoie `False`.

contains()

La fonction `contains()` détermine si une chaîne contient une sous-chaîne donnée. Cette fonction nécessite deux arguments de chaîne obligatoires.

```
contains(str, sub_str)
```

Cette fonction renvoie `True` lorsque la sous-chaîne (`sub_str`) est contenue n'importe où dans la chaîne (`str`).

Exemple :

- La `contains('Citrix', 'tri')` fonction renvoie `True`.
- La `contains('Citrix', 'Ci')` fonction renvoie `True`.
- La `contains('Citrix', 'ti')` fonction renvoie `False`

substring()

Utilisez la fonction `substring()` pour extraire une sous-chaîne d'une chaîne.

```
substring(str, start_index, end_index)
```

Cette fonction nécessite les deux arguments obligatoires et un argument entier facultatif.

- `str` (Obligatoire)
- `start_index` (Obligatoire)
- `end_index` (Facultatif)

Cette fonction renvoie la sous-chaîne de la chaîne (`str`) qui se trouve entre les positions d'index spécifiées. Si vous ne spécifiez pas la position d'index de fin, la fonction extrait la sous-chaîne de l'index de début à la fin de la chaîne.

> **Remarque**
>
> Lorsque vous spécifiez `end_index`, la sous-chaîne exclut le caractère à la position `end_index`.

Exemple :

- La `substring('Citrix', 2)` fonction renvoie `trix`
- La `substring('Citrix', 10)` fonction renvoie (")

  Dans cet exemple, la fonction renvoie une chaîne vide car elle a une `start_index` position non valide.

- La `substring('Citrix', 2, 4)` fonction renvoie `tr`

  Dans cet exemple, la fonction extrait les caractères compris entre 2 et 4 positions d'index.

- La `substring('Citrix', -3)` fonction renvoie `rix`

  Si vous souhaitez extraire les caractères qui se trouvent à la fin de la chaîne, spécifiez une valeur négative pour l'argument `start_index`.

  Dans cet exemple, la fonction extrait la sous-chaîne qui inclut les trois derniers caractères de la chaîne.

Détection des dépendances

April 29, 2021

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 par eux-mêmes et ils peuvent ne pas être écrits dans le même ordre qu'ils doivent être exécutés. Le compilateur StyleBook vérifie l'ordre dans lequel les composants sont écrits, puis les exécute dans un ordre logique.

Exemple :

```
components:

  -

    name: lbvserver-comp

    type: ns::lbvserver

    properties:

      name: mylb

      ipv46: 10.102.190.15

      port: 80

      servicetype: HTTP

-
    name: lb-sg-binding-comp

    type: ns::lbvserver_servicegroup_binding
```



```
23
24      condition: $parameters.create-binding
25
26      properties:
27
28        name: $components.lbvserver-comp.properties.name
29
30        servicegroupname: $components.sg-comp.properties.servicegroupname
31
32  -
33      name: sg-comp
34
35      type: ns::servicegroup
36
37      properties:
38
39        servicegroupname: mysg
40
41        servicetype: HTTP
42  <!--NeedCopy-->
```

Dans l'exemple ci-dessus, trois composants sont définis - **lbvserver-comp**, **lb-sg-binding-comp**et **sg-comp**. Lorsque vous exécutez ce StyleBook, le `lbvserver-comp` est d'abord créé. Le `lb-sg-binding-comp` fait référence aux `lbvserver-comp` propriétés, mais il ne peut pas être créé ensuite bien qu'il s'agisse du deuxième composant défini dans le StyleBook. C'est parce que l'a `lb-sg-binding-comp` aussi une dépendance sur `sg-comp` ce qui n'est pas encore créé. Par conséquent, le compilateur réorganise les composants de sorte que les dépendances d'un composant soient résolues lors de la création d'un composant, et exécute cette liste réordonnée de composants. L'ordre d'exécution du StyleBook ci-dessus est : `lbvserver-comp`, `sg-comp`, et `lb-sg-binding-comp`.

Ainsi, l'auteur d'un StyleBook n'a pas besoin de s'inquiéter de l'ordre correct des composants. Les composants peuvent apparaître dans n'importe quel ordre. Le compilateur calcule l'ordre d'exécution correct des composants en fonction de la façon dont les composants se réfèrent. Il convient de noter que cela s'applique également aux sections sur les substitutions et les extrants.

Dépendances cycliques

Comme un composant peut faire référence à un autre composant, il est possible que le cycle des 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 corrige

manuellement la définition de StyleBook pour éliminer ces dépendances cycliques. Le compilateur sera en mesure d'identifier les dépendances cycliques - si elles existent, et de les signaler.

L'exemple suivant montre une dépendance cyclique des composants :

```
components:

  -

    name: lbvserver-comp

    type: ns::lbvserver

    properties:

      name: $components.lb-sg-binding-comp.properties.name

      ipv46: 10.102.190.15

      port: 80

      servicetype: HTTP

  -

    name: lb-sg-binding-comp

    type: ns::lbvserver_servicegroup_binding

    condition: $parameters.create-binding

    properties:

      name: mylb

      servicegroupname: $components.sg-comp.properties.servicegroupname

  -

    name: sg-comp

    type: ns::servicegroup

    properties:

```



```
41        servicegroupname: mysg
42
43        servicetype: $components.lbvserver-comp.properties.servicetype
44  <!--NeedCopy-->
```

Dans l'exemple ci-dessus, il existe trois composants : **lbvserver-comp**, **lb-sg-binding-comp**et **sg-comp**. Le `lbvserver-comp` composant dépend de `lb-sg-binding-comp`, `lb-sg-binding` composants. Et, ces composants dépendent de `sg-comp`. Le `sg-comp` composant dépend de `lbvserver-comp`. Ici, un cycle de dépendances entre ces composants est formé et cela ne peut pas être résolu automatiquement. Par conséquent, ce StyleBook ne peut pas être exécuté. Le compilateur StyleBook détecte cela et empêche l'importation de StyleBook dans Citrix ADM.

Gestion des instances

April 29, 2021

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). Ajoutez des instances à Citrix ADM pour les surveiller. Des instances peuvent être ajoutées lorsque vous configurez Citrix ADM ou version ultérieure. Une fois que vous avez ajouté des instances à Citrix ADM, elles sont interrogées en permanence pour collecter des informations qui peuvent être utilisées ultérieurement pour résoudre des problèmes ou en tant que données de reporting.

Les instances peuvent être regroupées sous la forme d'un groupe statique ou d'un bloc IP privé. Un groupe statique d'instances peut s'avérer utile lorsque vous souhaitez exécuter des tâches spécifiques, telles que des tâches de configuration, etc. Un bloc IP privé regroupe vos instances en fonction de leur emplacement géographique.

Ajouter une instance

Vous pouvez ajouter des instances lors de la configuration du serveur Citrix ADM pour la première fois ou plus tard. Pour ajouter des instances, vous devez spécifier le nom d'hôte ou l'adresse IP de chaque instance Citrix ADC, ou une plage d'adresses IP.

Pour savoir comment ajouter une instance à Citrix ADM, reportez-vous à la sectionAjouter des instances à Citrix ADM.

Lorsque vous ajoutez une instance au serveur Citrix ADM, le serveur s'ajoute implicitement en tant que destination d'interruption pour l'instance et recueille un inventaire de l'instance. Pour en savoir plus, consultez Comment Citrix ADM découvre les instances.

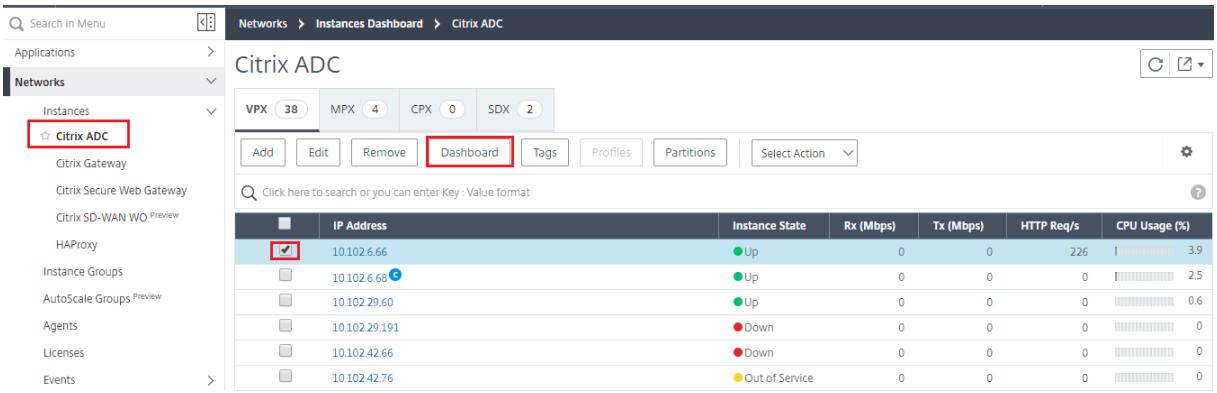
Après avoir ajouté une instance, vous pouvez la supprimer en accédant à **Réseaux**> **Tableau de bord**et en cliquant sur **Toutes les instances**. Dans la page Instances, sélectionnez l'instance à supprimer et cliquez sur **Supprimer**.

Comment utiliser le tableau de bord de l'instance

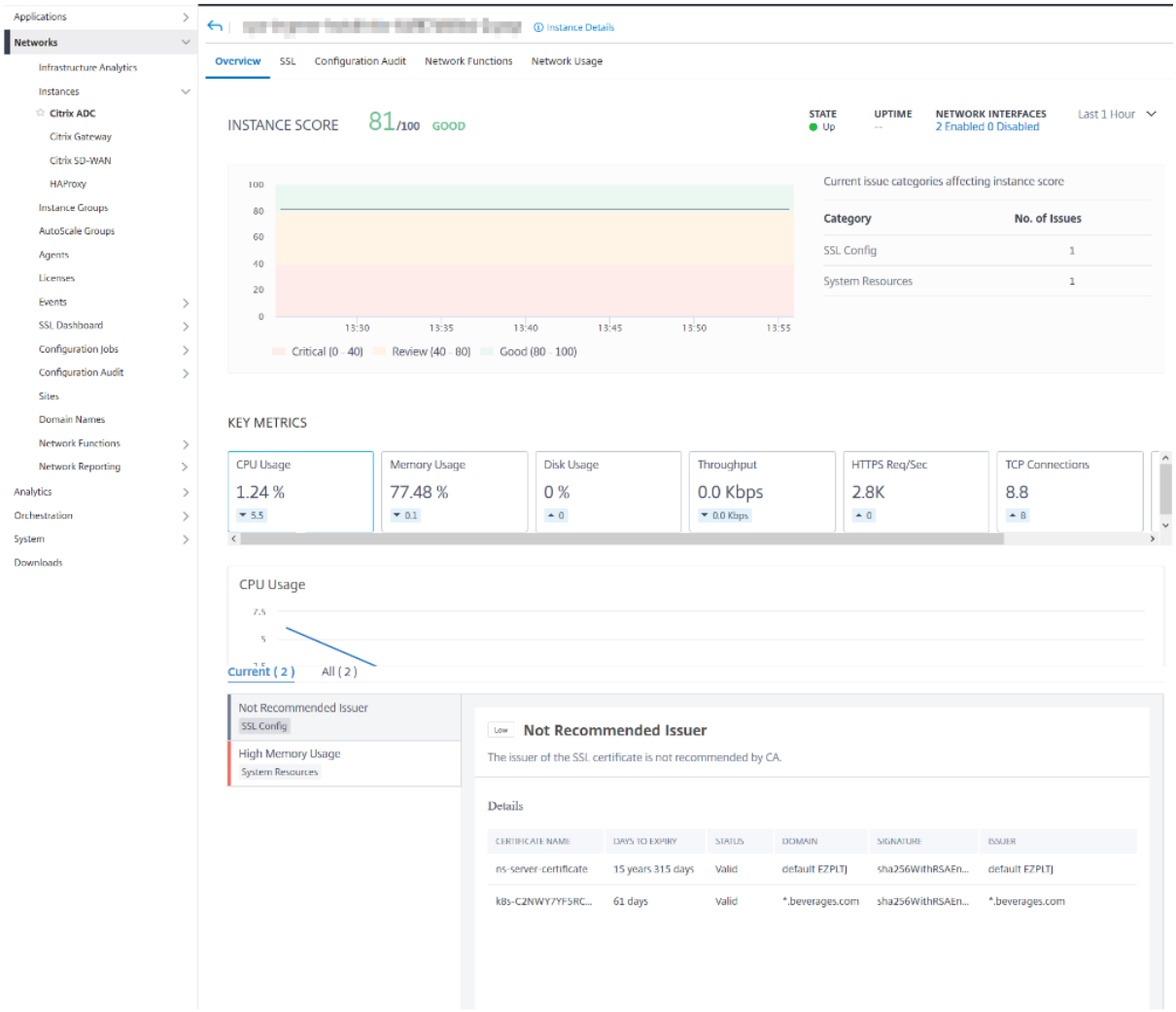
Le tableau de bord par instance de Citrix ADM affiche les données sous forme de tableau et graphique pour l'instance sélectionnée. Les données collectées à partir de votre instance pendant le processus d'interrogation sont affichées sur le tableau de bord.

Par défaut, chaque minute, les instances gérées sont interrogées pour la collecte de données. Des 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 permanence à l'aide d'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** > **Citrix ADC** . Sur la page Citrix ADC, choisissez le type d'instance, 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. Des informations spécifiques à l'instance telles que l'adresse IP, ses versions matérielles et LOM, les détails du profil, le numéro de série, la personne de contact et d'autres sont également affichées ici. En faisant défiler vers le bas, les fonctionnalités sous licence disponibles sur l'instance choisie ainsi que les modes configurés sur celle-ci. Pour de plus amples informations, consultez la section Détails de l'instance.
- Tableau de**bord SSL**. Vous pouvez utiliser l'onglet SSL du tableau de bord par instance pour afficher ou surveiller les détails des certificats SSL, des serveurs virtuels SSL et des protocoles SSL de votre instance 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 Citrix ADC** et les graphiques de **dérive de configuration**

Citrix ADC sur le tableau de bord affichent des détails de haut niveau 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 votre 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 afficher les données de performances réseau pour votre 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 autre rapport de performance.

Comment surveiller les sites distribués à l'échelle mondiale

April 29, 2021

En tant qu'administrateur réseau, vous devrez peut-être surveiller et gérer les instances réseau déployées sur des sites géographiques. Toutefois, il n'est pas facile d'évaluer les besoins du réseau lors de la gestion des instances réseau dans des datacenters répartis géographiquement.

Geomaps dans Citrix Application Delivery Management (Citrix ADM) vous fournit une représentation graphique de vos sites et décompose votre expérience de surveillance réseau par région. Avec les géomaps, vous pouvez visualiser la distribution de votre instance réseau par emplacement et surveiller les problèmes réseau.

Les sections suivantes expliquent comment surveiller les centres de données dans Citrix ADM.

Surveillance des sites distribués à l'échelle mondiale dans Citrix ADM

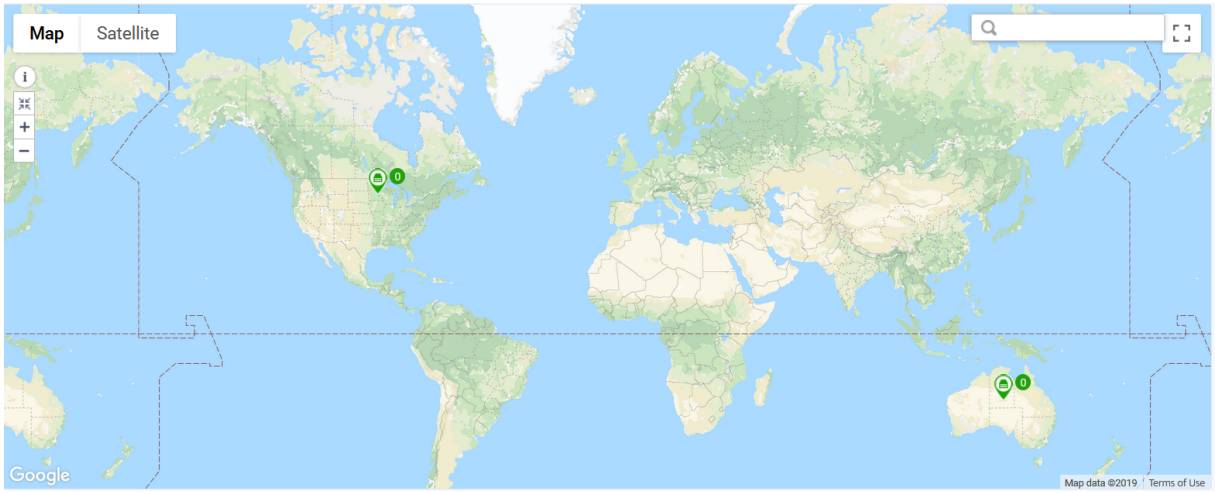
Le site Citrix ADM est un regroupement logique d'instances Citrix Application Delivery Controller (Citrix ADC) dans un emplacement géographique spécifique. Par exemple, alors qu'un site est affecté à Amazon Web Services (AWS) et qu'un autre site peut l'être à Azure™. Encore un autre site est hébergé 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 syslog, AppFlow, SNMP et toutes ces données provenant des instances gérées.

Geomaps dans Citrix ADM vous fournit une représentation graphique de vos sites. Les géomaps décompose également votre expérience de surveillance réseau par géographie. Avec les géomaps, vous

pouvez visualiser la distribution de votre instance réseau par emplacement et surveiller tous les problèmes réseau. Vous pouvez cliquer sur **Réseaux** dans le menu pour afficher le tableau de **bord Instances** pour une représentation visuelle des sites créés sur la carte du monde.

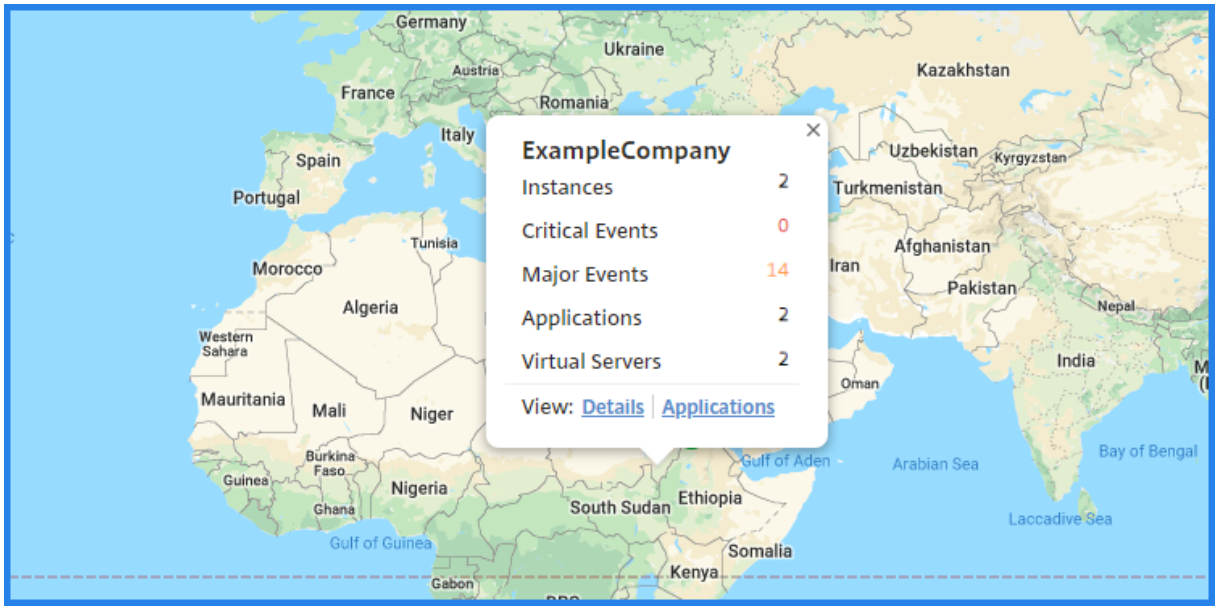
Cas d'utilisation

ExampleCompany, une entreprise de téléphonie mobile de premier plan, comptait sur des fournisseurs de services privés pour héberger leurs ressources et leurs applications. La société avait déjà deux sites - un à Minneapolis aux États-Unis et un autre à Alice Springs en Australie. Dans cette image, vous pouvez voir que deux marqueurs représentent les deux sites existants.



Les marqueurs affichent également le nombre des composants suivants sur le site :

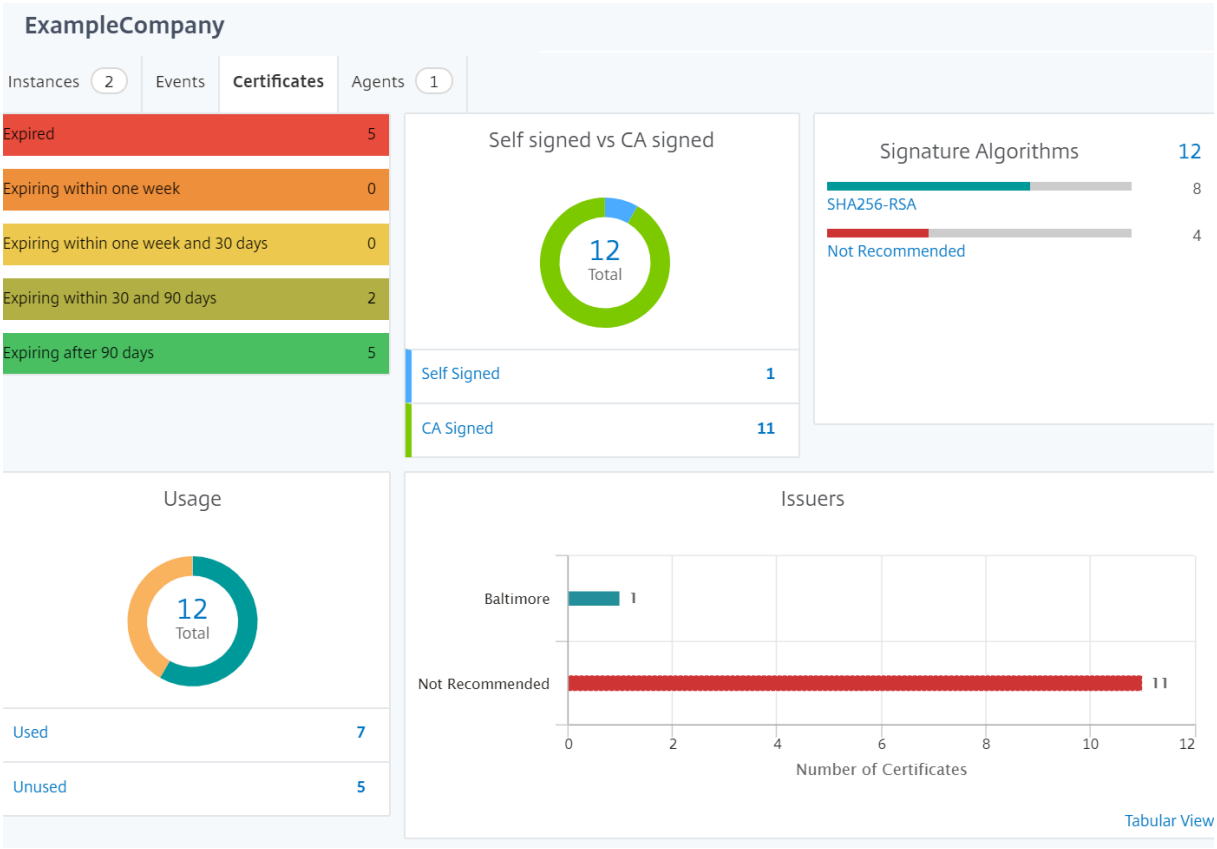
- **Instances** : indique le nombre d'instances disponibles.
- **Applications** : indique le nombre d'applications hébergées.
- **Serveurs virtuels** : indique le nombre de serveurs virtuels disponibles.
- **Événements critiques** : indique le nombre d'événements critiques survenus sur les instances.
- **Événements majeurs** : indique le nombre d'événements majeurs survenus sur les instances.



Cliquez sur **Applications** pour afficher toutes les applications personnalisées créées dans chaque site.

Cliquez sur **Détails** pour afficher la liste des instances Citrix ADC ajoutées dans chaque site. Cliquez sur les onglets pour afficher plus d'informations :

- Onglet**Instances** : Affichez les éléments suivants dans cet onglet :
  - Adresse IP de chaque instance réseau
  - Type de l'instance de Citrix ADC
  - Nombre d'événements critiques
  - Événements significatifs et tous les événements soulevés sur une instance de Citrix ADC.
- Onglet**Événements** : affiche la liste des événements critiques et significatifs soulevés sur les instances.
- **Onglet Certificats** : Affichez les éléments suivants dans cet onglet :
  - Liste des certificats de toutes les instances
  - Statut d'expiration
  - Informations vitales et les 10 principales instances par de nombreux certificats en cours d'utilisation.
- 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, Inde. L'entreprise voulait tester le cloud en déchargeant certaines de ses applications informatiques internes moins critiques vers le bureau de Bangalore. La société a décidé d'utiliser les services de cloud computing AWS.

En tant qu'administrateur, vous devez d'abord créer un site, puis ajouter les instances de Citrix ADC dans Citrix ADM. Vous devez également ajouter l'instance au site, ajouter un agent et lier l'agent au site. Citrix ADM reconnaît ensuite le site auquel appartiennent l'instance de Citrix ADC et l'agent.

Pour plus d'informations sur l'ajout d'instances Citrix ADC, reportez-vous à la sectionAjout 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.

1. Dans Citrix ADM, accédez à **Réseaux** > **Sites**, puis cliquez sur **Ajouter** .
2. Dans la page **Créer un site**, mettez à jour les informations suivantes, puis cliquez sur **Créer** .
    a) **Type de site**. Sélectionnez **Centre de données**.

> **Remarque**
>
> Le site peut fonctionner en tant que centre de données principal ou en tant que branche. Choisissez en conséquence.

a) **Type**. Sélectionnez AWS comme fournisseur de cloud dans la liste.

> **Remarque**
>
> Cochez la case **Utiliser un VPC existant en tant que site**en conséquence.

b) **Nom du site**. Tapez le nom du site.

c) **Rechercher l'emplacement**. Tapez le nom de la ville. Cliquez sur **Obtenir l'emplacement** pour placer le site précisément à l'emplacement.
Les champs Ville, Code postal, Région, Pays, Latitude et Longitude sont remplis automatiquement.

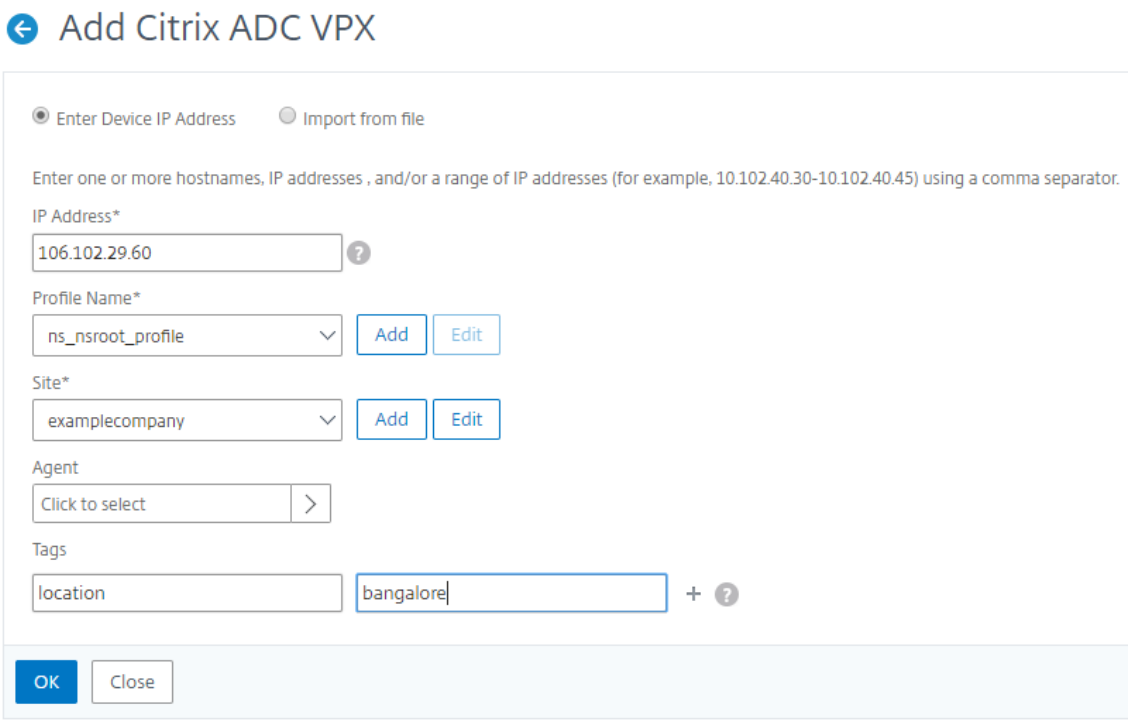
! [Créer des sites] (/en-us/citrix-application-delivery-management-service/media/nmaservice-global-datacenters-4.png)

d) Cliquez sur **Créer** pour créer un site dans Bangalore.

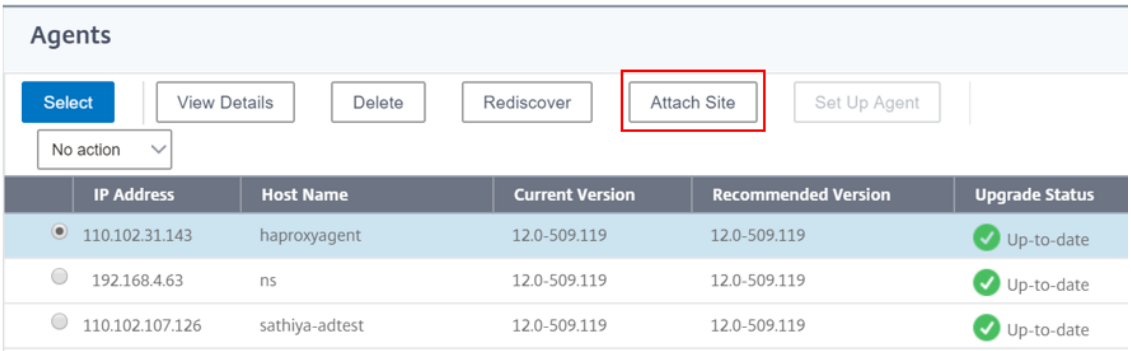
Pour ajouter des instances et sélectionner des sites :

Après avoir créé des sites, vous devez ajouter des instances dans Citrix ADM. Vous pouvez sélectionner le site créé précédemment ou créer un site et associer l'instance.

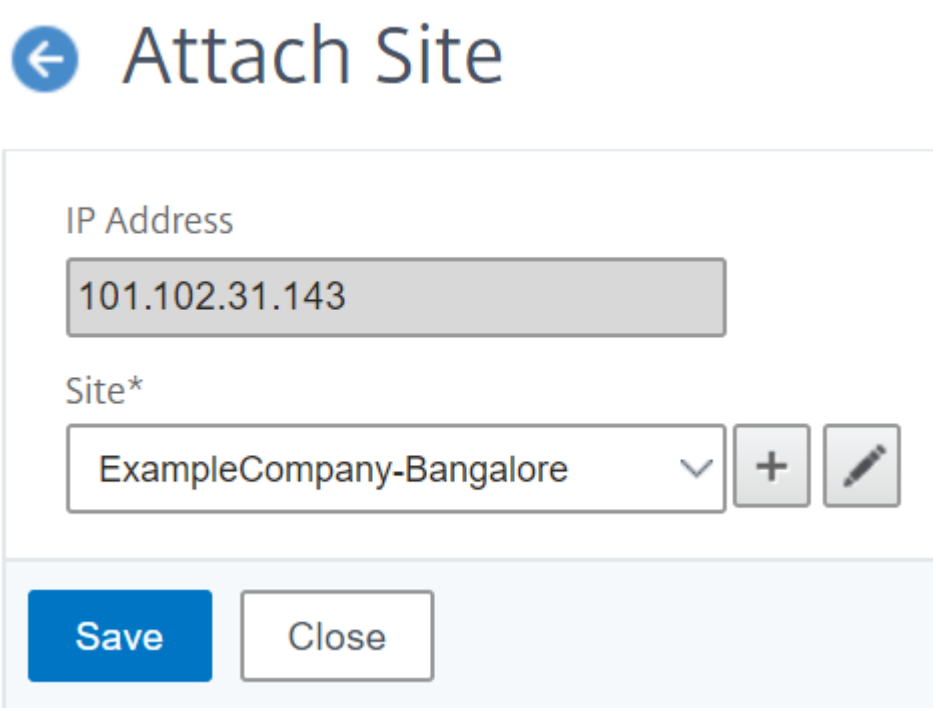
1. Dans Citrix ADM, accédez à **Réseaux** > **Instances** > **Citrix ADC**.
2. Sélectionnez le **VPX**, puis cliquez sur **Ajouter**.
3. Sur la page **Ajouter Citrix ADC VPX**, tapez l'adresse IP et sélectionnez le profil dans la liste.
4. Sélectionnez le site dans la liste. Vous pouvez cliquer sur le bouton **Ajouter** en regard **du champ Site** pour créer un site ou cliquer sur le bouton **Modifier** pour modifier les détails du site par défaut.
5. Cliquez sur la flèche droite et sélectionnez l'agent dans la liste qui s'affiche.



6. Après avoir choisi l'agent, vous devez l'associer au site. Cette étape permet à l'agent d'être lié au site. Sélectionnez l'agent et cliquez sur **Joindre le site**.



a) Sélectionnez le site dans la liste et cliquez sur **Enregistrer**.



7. Le cas échéant, vous pouvez entrer des champs clé et valeur pour les **balises**.
8. 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**.
3. Vous pouvez associer le site et cliquer sur **Enregistrer**.

Citrix ADM commence à surveiller les instances Citrix ADC ajoutées sur le site Bangalore ainsi que les instances des deux autres sites.

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 quotidiennement, hebdomadaire ou mensuel et envoyer le rapport par e-mail ou par un message de marge.

> **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.

Comment créer des balises et assigner à des instances

April 29, 2021

Citrix Application Delivery Management (ADM) vous permet désormais d'associer vos instances Citrix ADC avec des balises. Une balise est un mot-clé ou un terme à un mot que vous pouvez attribuer à une instance. Les balises ajoutent des informations supplémentaires sur l'instance. Les balises peuvent être considérées comme des métadonnées qui aident à décrire une instance. Les balises vous permettent de classer et de rechercher des instances en fonction de ces mots-clés spécifiques. Vous pouvez également affecter plusieurs balises à une seule instance.

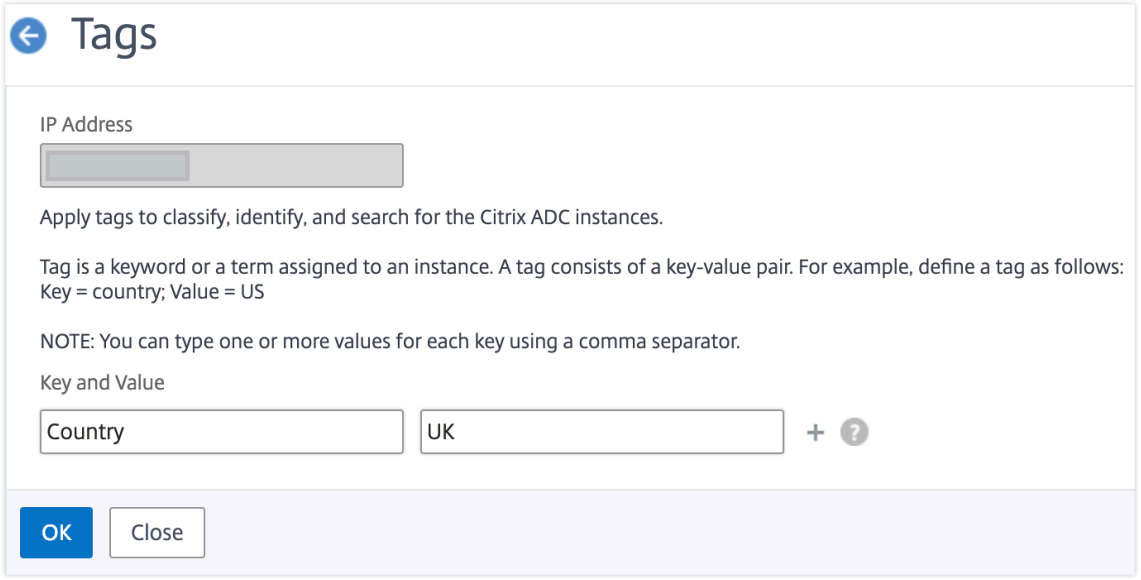
Les cas d'utilisation suivants vous aident à comprendre comment le balisage des instances vous aidera à mieux les surveiller.

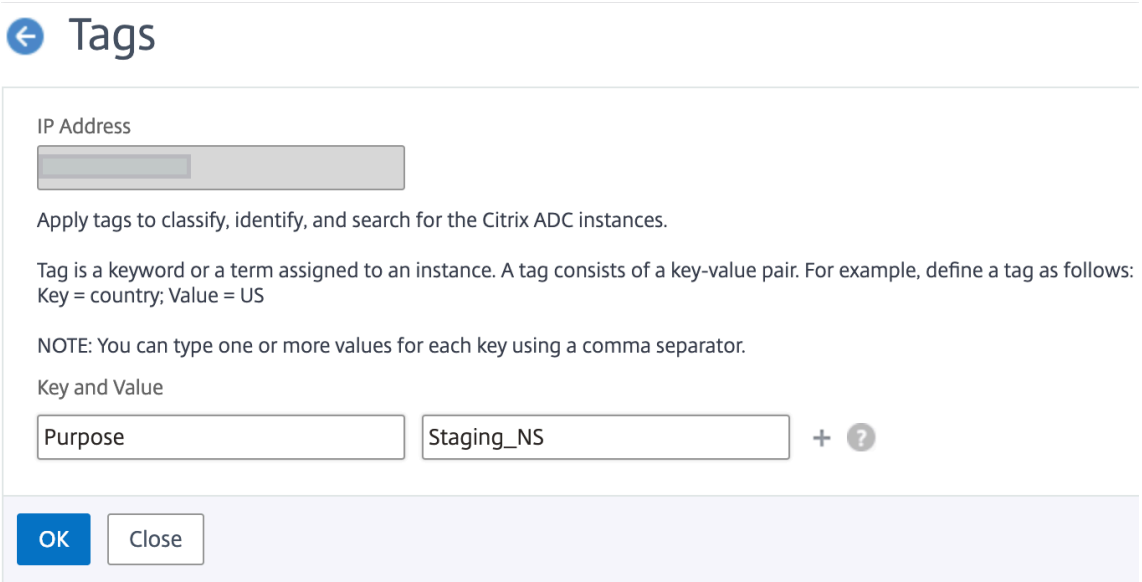
- **Cas d'utilisation 1** : vous pouvez créer une balise pour identifier toutes les instances situées au Royaume-Uni. Ici, vous pouvez créer une balise avec la clé « Pays » et la valeur « UK ». « Cette balise vous permet de rechercher et de surveiller toutes les instances situées au Royaume-Uni.
- **Cas d'utilisation 2** : vous souhaitez rechercher des instances qui se trouvent dans l'environnement intermédiaire. Ici, vous pouvez créer une balise avec la clé « Purpose » et une 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 dans laquelle vous souhaitez connaître la liste des instances Citrix ADC situées dans la zone Swindon au Royaume-Uni et que vous possédez, David T. Vous pouvez créer des balises pour toutes ces exigences et l'affecter à toutes les instances qui satisfont à ces conditions.

Pour affecter des balises à l'instance Citrix ADC VPX :

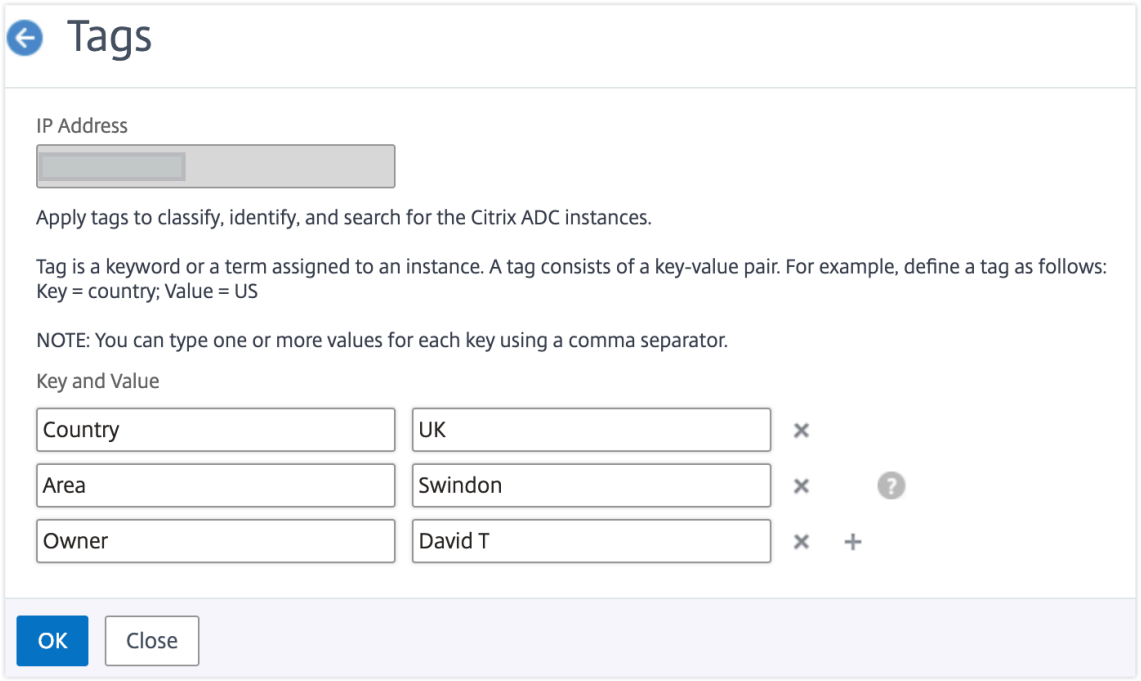
1. Dans Citrix ADM, accédez à **Réseaux** > **Instances** > **Citrix ADC**.
2. Sélectionnez l'onglet **VPX**.
3. Sélectionnez l'instance VPX requise.
4. Cliquez sur **Balises**. La fenêtre **Tags** qui apparaît vous permet de créer vos propres paires clé-valeur en attribuant des valeurs à chaque mot clé que vous créez.

Par exemple, les images suivantes montrent quelques mots-clés créés et leurs valeurs. Vous pouvez ajouter vos propres mots clés et saisir une valeur pour chaque mot clé.



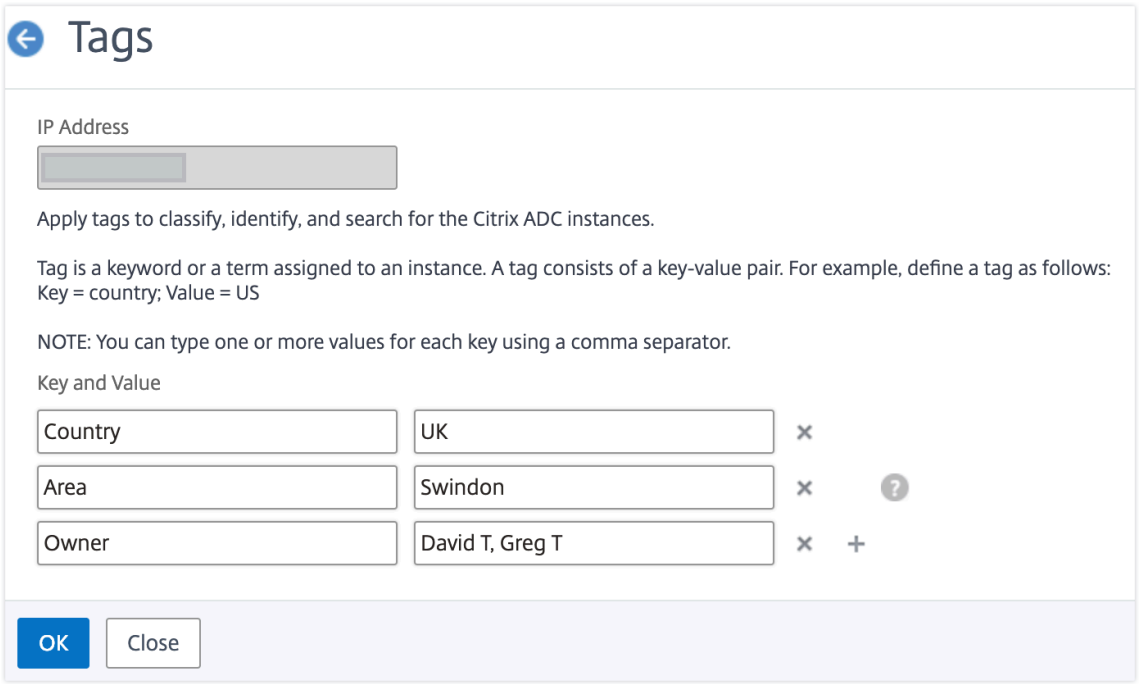


Vous pouvez également ajouter plusieurs balises en cliquant sur « + ». L'ajout de balises multiples et significatives vous permet de rechercher efficacement les instances.



Vous pouvez ajouter plusieurs valeurs à un mot-clé en les séparant par des virgules.

Par exemple, vous attribuez le rôle d'administrateur à un autre collègue, Greg T. Vous pouvez ajouter son nom séparé par une virgule. L'ajout de plusieurs noms vous aide à rechercher par l'un des noms ou par les deux noms. Citrix ADM reconnaît les valeurs séparées par des virgules en deux valeurs différentes.



Pour en savoir plus sur la recherche d'instances basées sur des balises, reportez-vous à la sec-

tion Comment rechercher des instances à l'aide de valeurs de balises et de propriétés.

5. Cliquez sur **OK**.

> **Remarque**
>
> Vous pouvez ultérieurement ajouter de nouvelles balises ou supprimer des balises existantes. Il n'y a aucune restriction sur le nombre de balises que vous créez.

Procédure de recherche d'instances à l'aide de valeurs de balises et de propriétés

April 29, 2021

Dans certains cas, Citrix Application Delivery Management (ADM) gère de nombreuses instances Citrix ADC. En tant qu'administrateur, vous pouvez avoir la possibilité de rechercher dans l'inventaire des instances en fonction de certains paramètres. Citrix ADM offre désormais une fonctionnalité de recherche améliorée pour rechercher un sous-ensemble d'instances de 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 de Citrix ADC pour ajouter une description supplémentaire à propos de l'instance de Citrix ADC. Vous pouvez désormais associer vos instances Citrix ADC avec des balises. Ces balises peuvent être utilisées pour mieux identifier et rechercher les instances de Citrix ADC.
- **Propriétés**. Chaque instance Citrix ADC ajoutée dans Citrix ADM a quelques paramètres ou propriétés par défaut associés à cette instance. Par exemple, chaque instance a son propre nom d'hôte, adresse IP, version, ID hôte, ID de modèle matériel, etc. Vous pouvez rechercher des instances en spécifiant des valeurs pour n'importe laquelle de ces propriétés.

Par exemple, considérez une situation dans laquelle vous souhaitez connaître la liste des instances de Citrix ADC qui se trouvent sur la version 12.0 et qui sont à l'état UP. Ici, la version et l'état de l'instance sont définis par les propriétés par défaut.

En plus de la version 12.0 et de l'état UP des instances, vous pouvez également rechercher les instances que vous possédez. 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, reportez-vous à la section Comment créer des balises et affecter des instances.

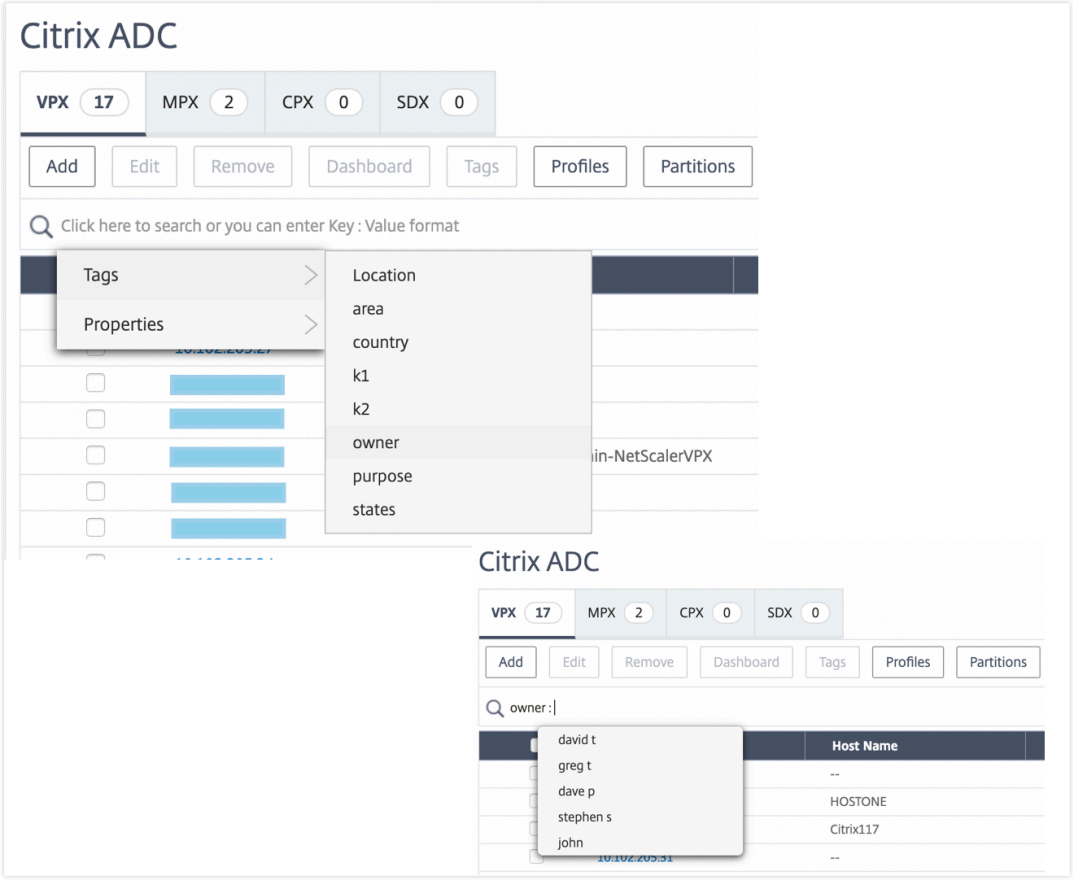
Vous pouvez utiliser une combinaison de balises et de propriétés pour créer vos propres critères de recherche.

Pour rechercher des instances Citrix ADC VPX

1. Dans Citrix ADM, accédez à **Réseaux** > **Instances** > **Citrix ADC**.
2. Sélectionnez l'onglet **VPX**.
3. Cliquez sur le champ de recherche. Vous pouvez créer une expression de recherche en utilisant Balises ou Propriétés ou en combinant les deux.

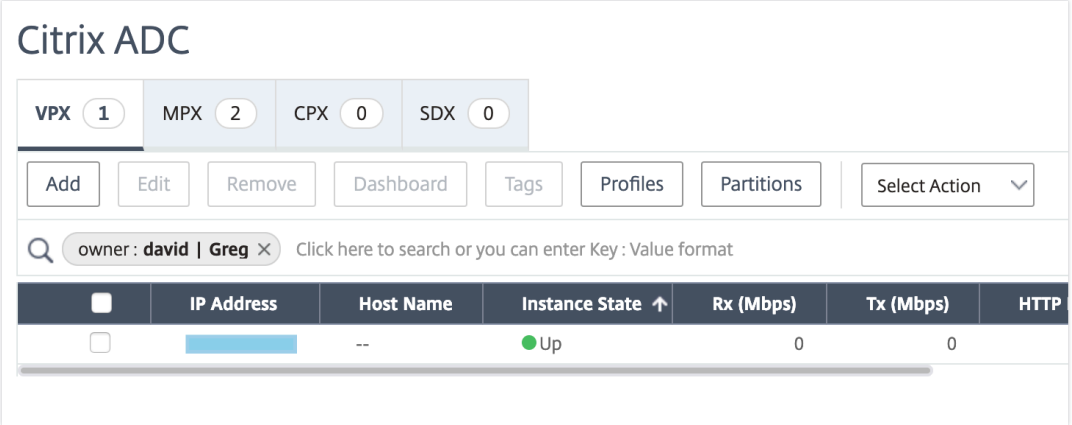
   Les exemples suivants montrent comment utiliser efficacement l'expression de recherche pour rechercher l'instance.

   a) Sélectionnez l'option **Balises** et sélectionnez **Propriétaire** . Sélectionnez « David T ».

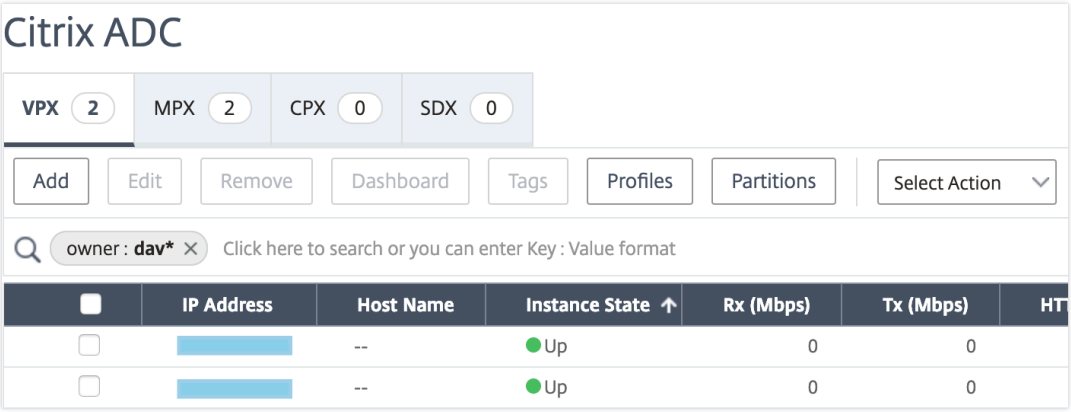


   Citrix ADM prend en charge les expressions régulières et les caractères génériques dans les expressions de recherche.

   a) Vous pouvez utiliser des expressions régulières pour développer davantage 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 « | ».



b) Vous pouvez également utiliser des caractères génériques pour remplacer ou représenter un ou plusieurs caractères. Par exemple, vous pouvez `Dav*` taper pour rechercher toutes les instances appartenant à « David » et « Dave P ».



> **Remarque**
>
> Pour plus d'informations sur les expressions régulières et les caractères génériques et sur leur utilisation, cliquez sur l'icône « Informations » dans la barre de recherche.

Gérer les partitions d'administration des instances de Citrix ADC

April 29, 2021

Vous pouvez configurer des partitions d'administration sur vos instances Citrix Application Delivery Controller (Citrix ADC) afin que différents groupes de votre organisation reçoivent des partitions différentes sur la même instance de Citrix ADC. Vous pouvez affecter un administrateur réseau pour gérer plusieurs partitions sur plusieurs instances de Citrix ADC.

Citrix Application Delivery Management (Citrix ADM) offre un moyen transparent de gérer toutes les partitions détenues par un administrateur à partir d'une console unique. Vous pouvez gérer ces partitions sans perturber d'autres configurations de partitions.

Pour permettre à plusieurs utilisateurs de gérer différentes partitions d'administration, vous devez créer des groupes, puis affecter des utilisateurs et des partitions à ces groupes. Pour plus d'informations sur la création d'un groupe ou d'un utilisateur, consultezCréer un utilisateuretCréer un groupe.

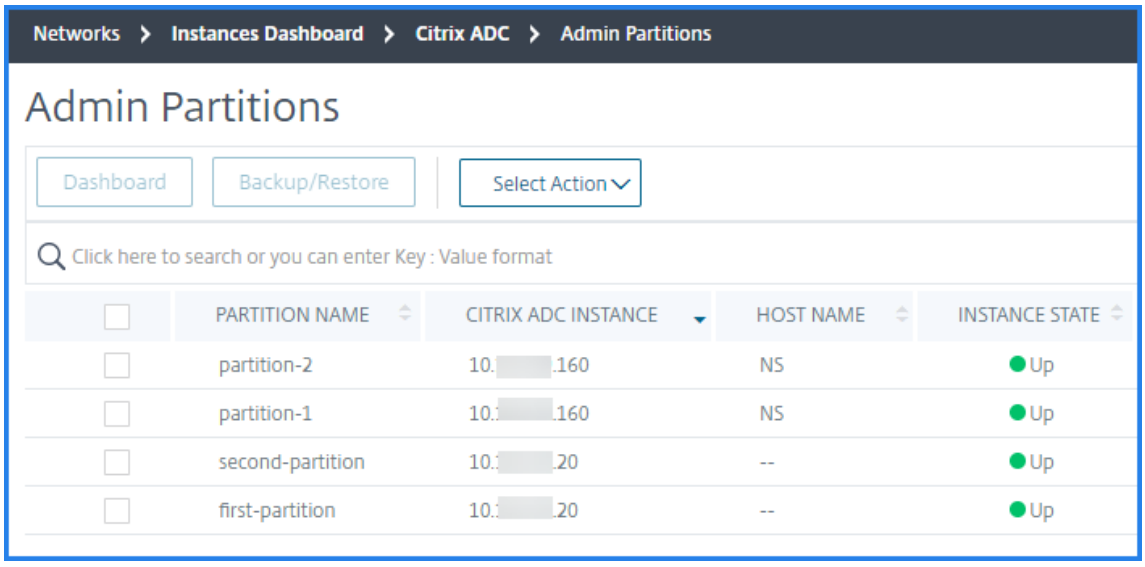
Un utilisateur peut afficher et gérer uniquement les partitions du groupe auquel il appartient. Lorsque vous découvrez une instance de Citrix ADC, les partitions d'administration configurées sur cette instance de Citrix ADC sont automatiquement ajoutées au système. Chaque partition d'administration est considérée comme une instance dans Citrix ADM.

Afficher les partitions d'administration

Considérez que vous avez deux instances Citrix ADC VPX et deux partitions d'administration sont configurées sur chaque instance. Par exemple, l'instance Citrix ADC 10.xx.xx.160 a partition-1 et partition-2 et l'instance 10.xx.xx.20 a la première et la deuxième partition.

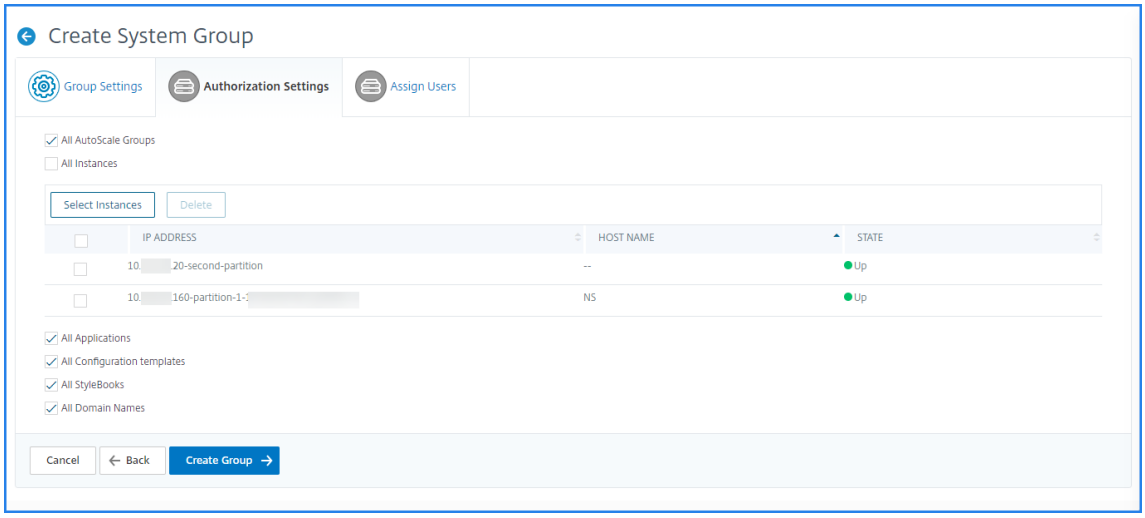
Procédez comme suit pour afficher les partitions d'administration :

1. Accédez à **Réseaux** > **Instances** > **Citrix ADC**.
2. Dans l'onglet **VPX**, cliquez sur **Partitions** .

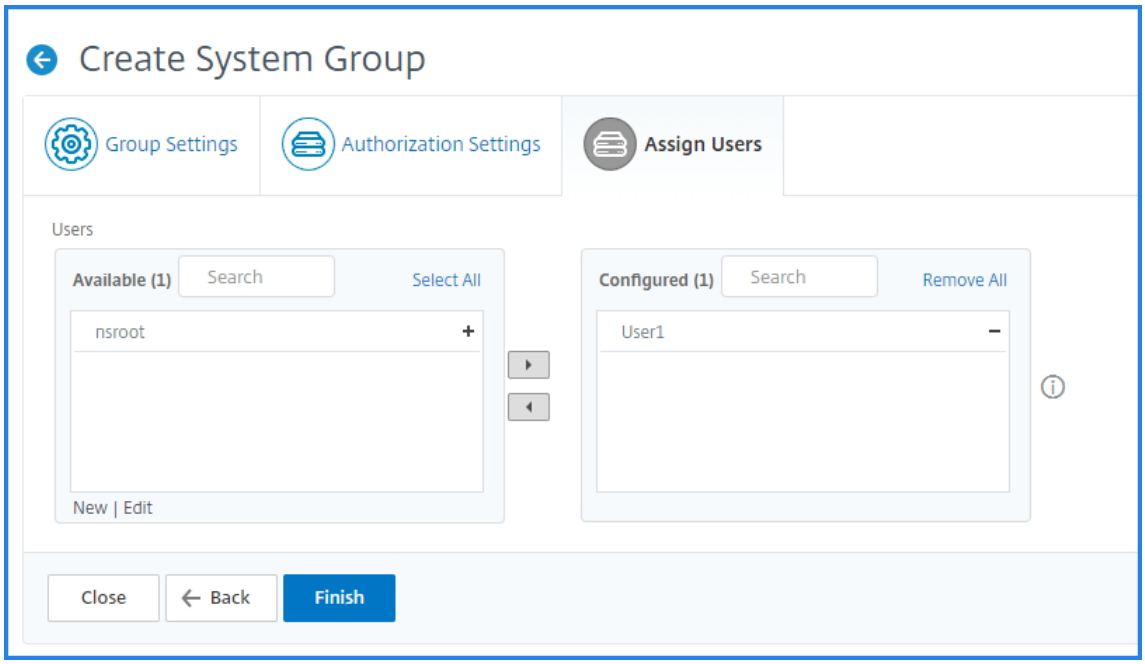


Par exemple, lorsque vous créez un groupe avec les conditions suivantes :

- Dans l'onglet **Paramètres d'autorisation**, les instances « 10.xx.xx.20-seconde partition » et « 10.xx.xx.160-partition-1" sont sélectionnées.



- « User1” est affecté au groupe.



L’utilisateur1 peut afficher et gérer uniquement les partitions ajoutées au groupe. Toutefois, les partitions qui ne sont pas ajoutées au groupe sont limitées à l’utilisateur même si elles appartiennent aux mêmes instances.

Dans cet exemple, 10.xx.xx.20-first partition et 10.xx.xx.160-partition-2 sont restreints. Parce que les instances ne sont pas ajoutées au groupe auquel l’utilisateur est affecté.

Si vous souhaitez qu’un autre utilisateur gère les partitions d’administration 10.xx.xx.20-first partition et 10.xx.xx.160-partition-2, créez un groupe avec les conditions suivantes :

- Dans l’onglet **Paramètres d’autorisation**, sélectionnez les instances 10.xx.xx.20-première partition et 10.xx.xx.160-partition-2.

- Affectez l'utilisateur requis au groupe.

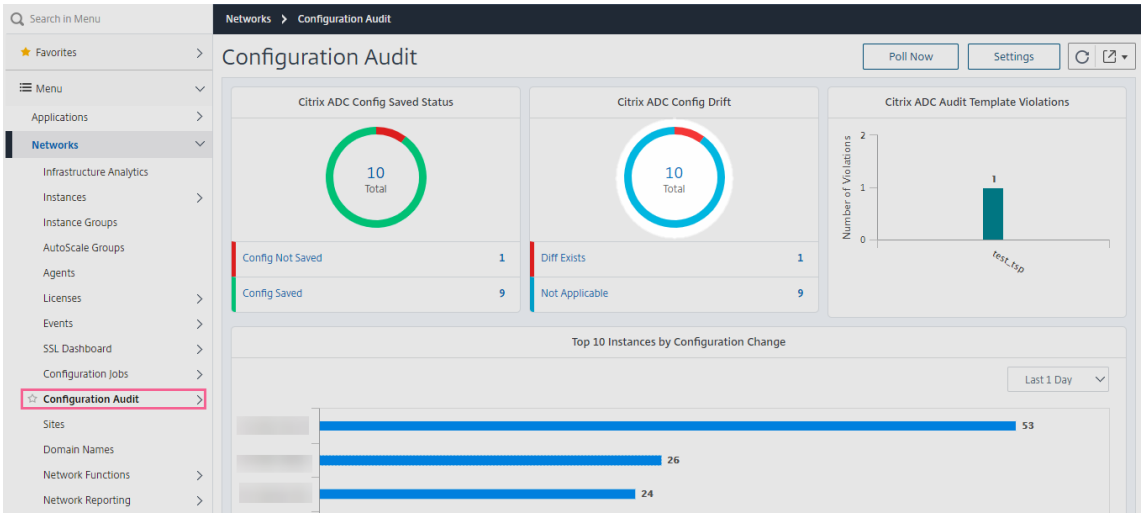
Ce groupe permet à l'utilisateur affecté d'afficher et de gérer les partitions d'administration sélectionnées.

Afficher la différence dans l'historique des révisions

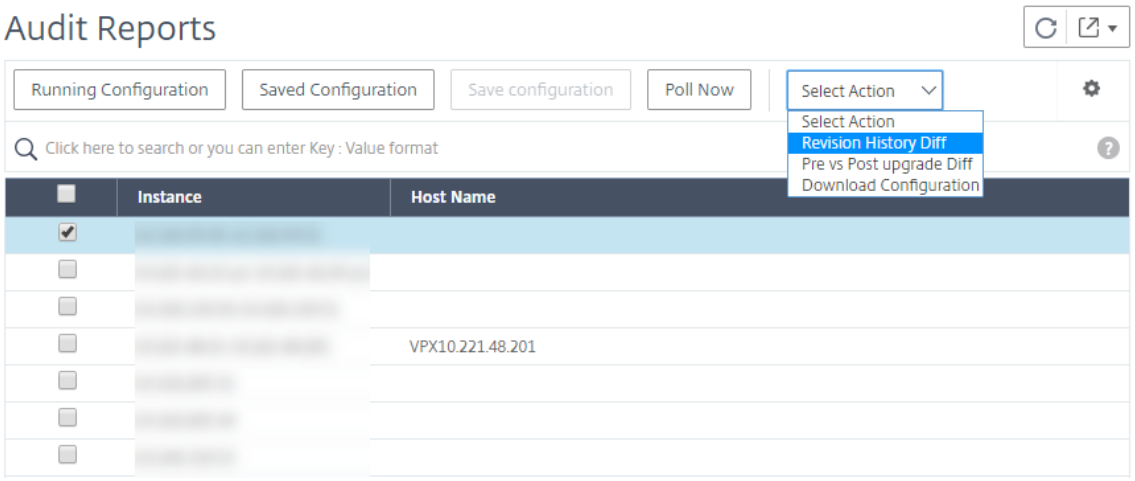
La différence d'historique des révisions pour une partition d'administration vous permet d'afficher la différence entre les cinq derniers fichiers de configuration d'une instance Citrix ADC partitionnée. Vous pouvez comparer les fichiers de configuration les uns avec les autres (exemple : Révision de configuration - 1 avec Révision de configuration -2) ou avec la configuration en cours d'exécution ou enregistrée avec Révision de configuration. Outre 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**. Le tableau de bord Audit de configuration affiche divers rapports. Cliquez sur le numéro affiché au centre du graphique en donut.

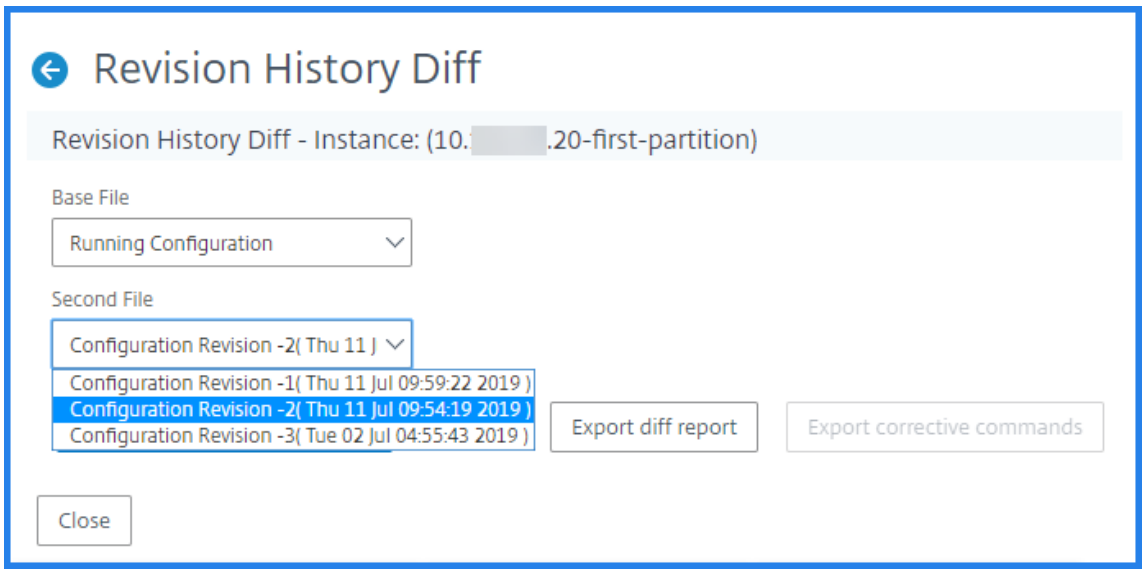


2. Sélectionnez l'instance Citrix ADC partitionnée.
3. Dans la zone Action, cliquez sur **Diff Historique des révisions.**

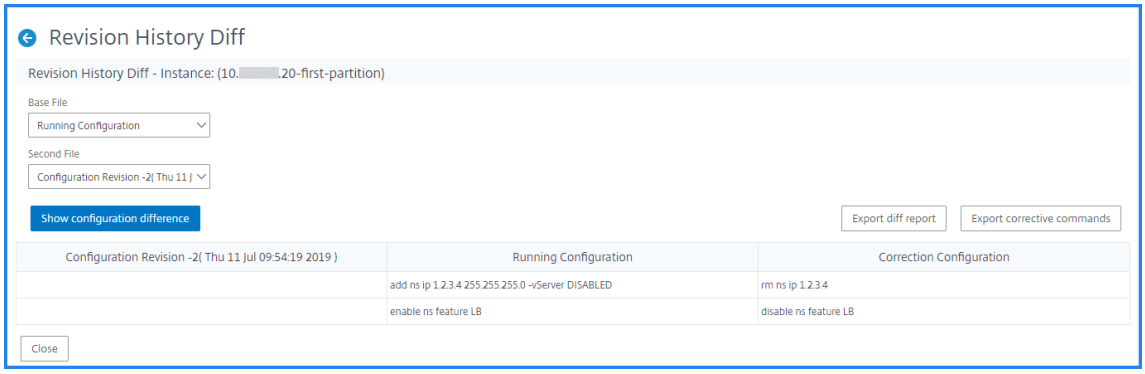


4. Dans la page **Diff de l'historique des révisions**, sélectionnez les fichiers que vous souhaitez comparer. Par exemple, comparez la configuration enregistrée avec Configuration Revision-2, puis cliquez sur **Afficher la différence de configuration**.

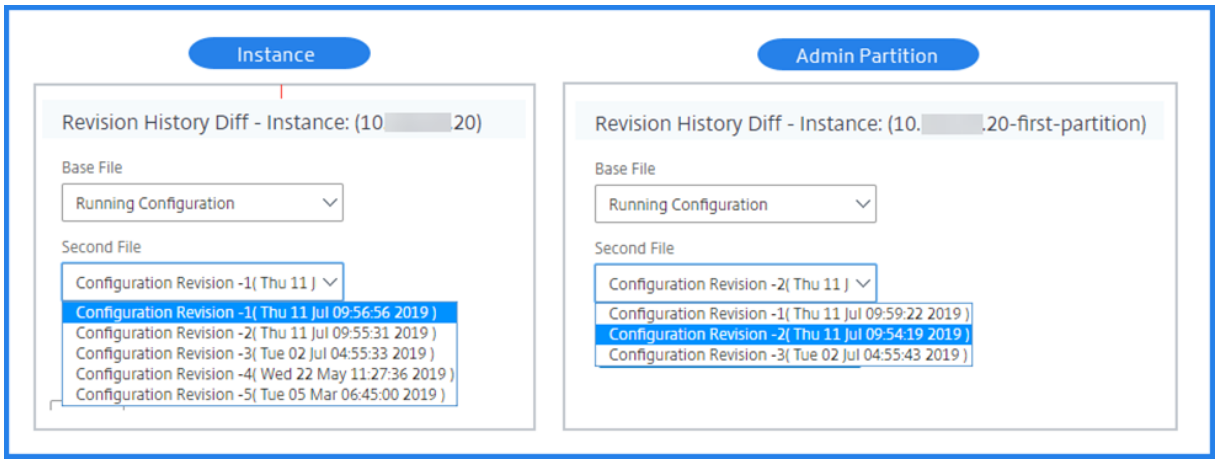
   Vous pouvez ensuite afficher les différences entre les cinq derniers fichiers de configuration pour l'instance Citrix ADC partitionnée sélectionnée. Voici un exemple de partition d'administration qui a trois configurations enregistrées :



   Vous pouvez également afficher les commandes de configuration corrective et exporter ces commandes correctives dans votre dossier local. Ces commandes correctives sont les commandes qui doivent être exécutées sur le fichier de base pour obtenir la configuration à l'état souhaité (fichier de configuration utilisé à des fins de comparaison).



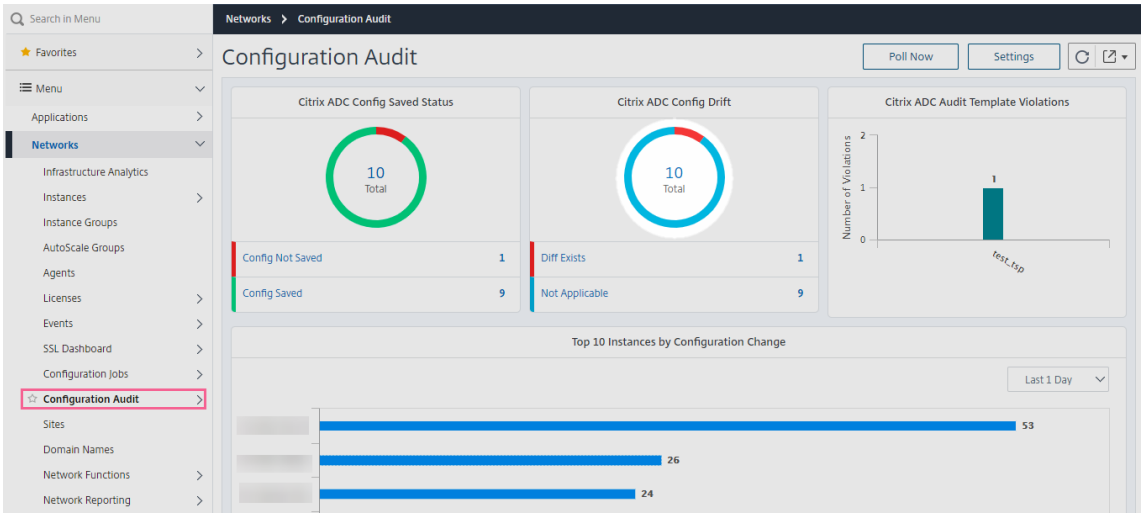
Les configurations enregistrées sur une partition d'administration et l'instance sont différentes. Dans l'exemple suivant, l'instance 10.xx.xx.20 a cinq configurations enregistrées où la partition d'administration de cette instance a trois configurations enregistrées différentes :



Afficher le modèle par rapport à la différence d'exécution

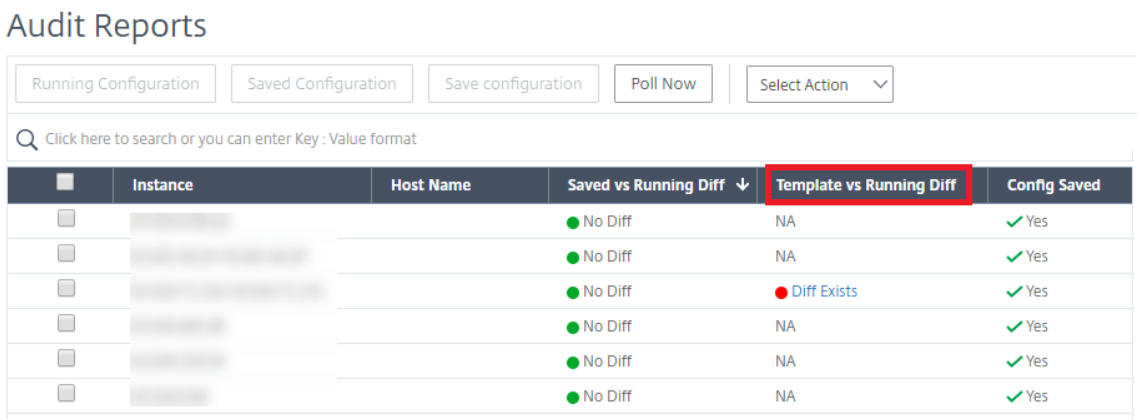
Les modèles d'audit pour la partition vous permettent de créer un modèle de configuration personnalisé et de l'associer à une instance de partition. Toute variation de la configuration en cours d'exécution de l'instance avec le modèle d'audit est affichée dans la colonne « **Modèle vs Running diff** » 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.

1. Accédez à **Réseaux > Audit de configuration**. Le tableau de bord Audit de configuration affiche divers rapports. Cliquez sur le numéro affiché au centre du graphique en donut.



2. Dans la page **Rapports d'audit**, cliquez sur le lien hypertexte **Diff Existe** sous la colonne Modèle vs Exécution de Diff.

   S'il y a une différence entre le modèle d'audit et la configuration en cours d'exécution, la différence est affichée sous forme d'un lien hypertexte. Cliquez sur le lien hypertexte pour afficher les différences le cas échéant. 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 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 quotidiennement, hebdomadaire ou mensuel et envoyer le rapport par e-mail ou par un message de marge.

> **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.

Sauvegarde et restauration des instances de Citrix ADC

April 29, 2021

Vous pouvez sauvegarder l'état actuel d'une instance Citrix Application Delivery Controller (Citrix ADC) et utiliser ultérieurement les fichiers sauvegardés pour restaurer l'instance Citrix ADC 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 de Citrix ADC. Vous pouvez sauvegarder et restaurer manuellement les configurations de Citrix ADC à l'aide de l'interface utilisateur graphique, de l'interface de ligne de commande ou utiliser Citrix Application Delivery Management (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 des 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 ADC SDX
- Citrix ADC VPX
- Citrix ADC MPX
- Citrix ADC BLX

Pour de plus amples informations, consultez Sauvegarde et restauration d'une instance ADC.

> **Remarque**
>
> - Depuis 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 issu 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/tenants/<specify-the-tenant-name>/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 seule instance Citrix ADC ou plusieurs instances et créer une sauvegarde des fichiers de configuration dans ces instances. Si nécessaire, vous pouvez également restaurer les instances Citrix ADC à l'aide de ces fichiers sauvegardés.

Créer une sauvegarde pour une instance Citrix ADC sélectionnée à l'aide de Citrix ADM

Effectuez cette tâche si vous souhaitez sauvegarder une instance Citrix ADC sélectionnée ou plusieurs instances :

1. Dans Citrix ADM, accédez à **Réseaux** > **Instances**. Sous **Instances**, sélectionnez le type d'instances (par exemple, VPX) à afficher à l'écran.
2. Sélectionnez l'instance que vous souhaitez sauvegarder.
    - Pour les instances MPX, VPX et BLX, sélectionnez **Sauvegarde/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. Spécifiez s'il faut chiffrer votre fichier de sauvegarde pour plus de sécurité. Vous pouvez entrer votre mot de passe ou utiliser le mot de passe global que vous avez précédemment spécifié sur la page Paramètres de sauvegarde de l'instance.
5. Cliquez sur **Continue**.

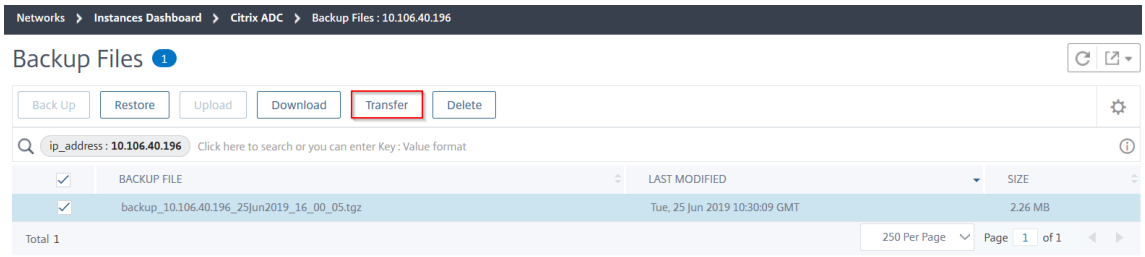
Transfert d'un fichier de sauvegarde vers un système externe

Vous pouvez transférer 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 de sauvegarde sur le serveur Citrix ADM, puis effectuer l'opération de restauration.

Pour transférer un fichier de sauvegarde Citrix ADM :

1. Accédez à **Réseaux** > **Instances** > **Citrix ADC**, puis sélectionnez le type d'instance. Par exemple, VPX.
2. Sélectionnez l'instance et dans la liste **Sélectionner une action**, sélectionnez **Sauvegarde/Restaurer** .

3. Sélectionnez le fichier de sauvegarde, puis cliquez sur **Transférer**.



La page **Transférer le fichier de sauvegarde** s'affiche. Spécifiez les paramètres suivants :

a) **Serveur** - Adresse IP du système sur lequel vous souhaitez transférer le fichier de sauvegarde.

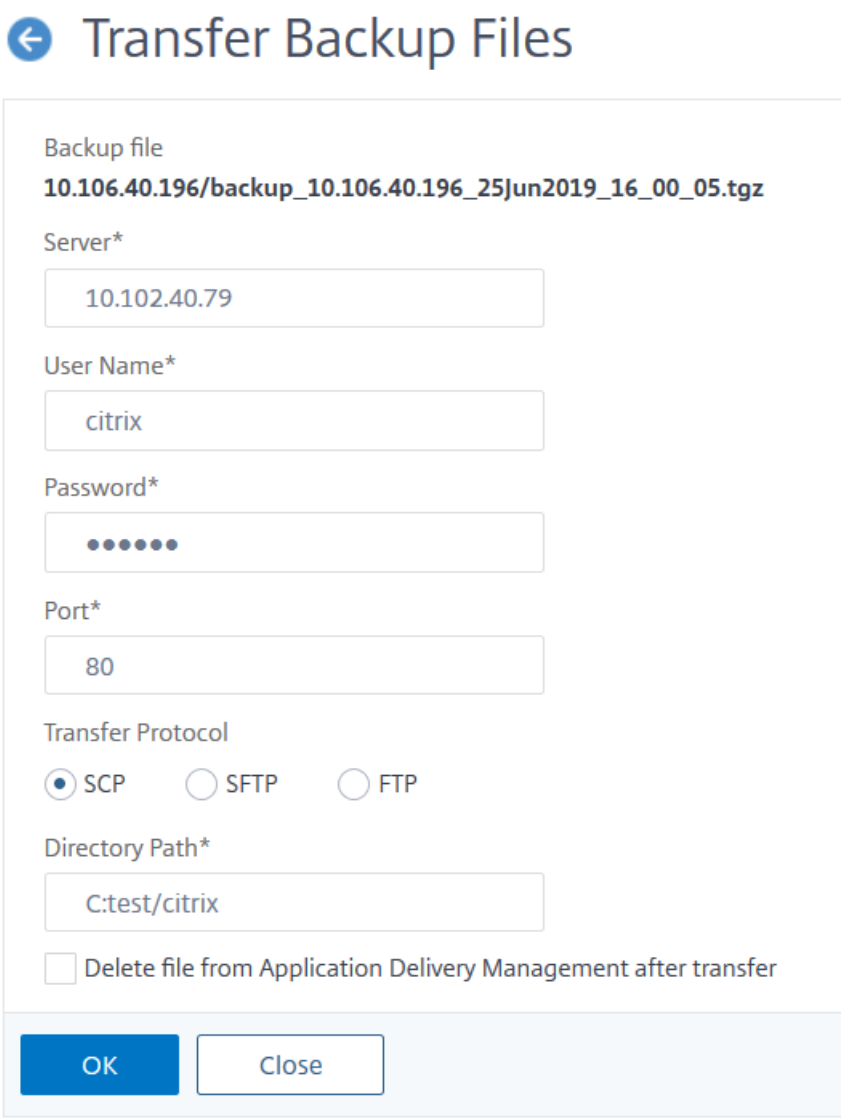
b) **Nom d'utilisateur** et **mot de passe** : informations d'identification de l'utilisateur du nouveau système, dans lequel les fichiers sauvegardés sont copiés.

c) **Port** — Numéro de port du système vers lequel les fichiers sont transférés.

d) **Protocole de transfert** : protocole utilisé pour effectuer le transfert de fichier de sauvegarde. Vous pouvez sélectionner les protocoles SCP, SFTP ou FTP pour transférer le fichier de sauvegarde.

e) **Chemin d'accès au répertoire** : emplacement où le fichier sauvegardé est transféré sur le nouveau système.

f) Cliquez sur **OK**.



Restaurer une instance Citrix ADC à l'aide de Citrix ADM

Remarque :

Si vous avez des instances de Citrix ADC dans une paire HA, vous devez noter ce qui suit :

- Restaurez la même instance à partir de laquelle le fichier de sauvegarde a été créé. Par exemple, considérons un scénario qu'une sauvegarde a été prise à partir de l'instance principale de la paire HA. Pendant le processus de restauration, assurez-vous que vous restaurez 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 devient **STAYSECONDARY**. Une fois le processus de restauration terminé sur l'instance principale, l'instance ADC sec-

> ondaire passe du mode **STAYSECONDARY** au mode **ENABLED** et devient 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 de Citrix ADC à l'aide du fichier de sauvegarde que vous avez créé précédemment :

1. Accédez à **Réseaux** > **Instances**, sélectionnez l'instance à restaurer, puis cliquez sur **Afficher la sauvegarde** .
2. Dans la page **Fichiers de sauvegarde**, sélectionnez le fichier de sauvegarde contenant les paramètres à restaurer, puis cliquez sur **Restaurer** .

Restaurer un dispositif 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 SSL SVM et clés
- Paramètres de taille de l'instance (au format XML)
- Paramètres de sauvegarde d'instance (au format XML)
- Paramètres d'interrogation de certificat SSL (au format XML)
- SVM fichier db
- Fichiers de configuration Citrix ADC des périphériques présents sur SDX
- Images de construction de Citrix ADC
- Images Citrix ADC XVA, ces images sont stockées à l'emplacement suivant : `/var/mps/sdx_images/`
- Image de pack unique SDX (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'appliance pour qu'ils correspondent à ceux du fichier de sauvegarde avant de démarrer le processus de restauration.

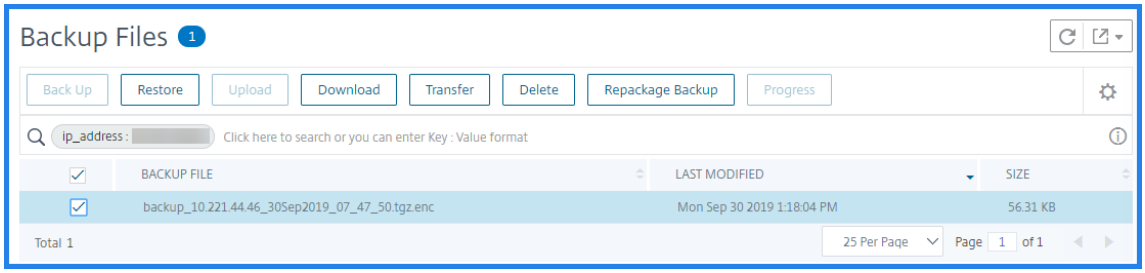
Assurez-vous que la variante de plate-forme SDX Citrix ADC qui a été sauvegardée est la même que celle sur laquelle vous essayez de restaurer. Vous ne pouvez pas restaurer à partir d'une variante de plate-forme différente.

> **Remarque**
>
> Avant de restaurer l'appliance SDX RMA, assurez-vous que la version sauvegardées est identique

> ou supérieure à la version RMA.

Pour restaurer l'appliance SDX à partir du fichier sauvegardé :

1. Dans l'interface utilisateur graphique Citrix ADM, accédez à **Réseaux > Instances > Citrix ADC**.
2. Cliquez sur **Sauvegarde/Restaurer**.
3. Sélectionnez le fichier de sauvegarde de la même instance que vous souhaitez restaurer.
4. Cliquez sur **Reconditionner la sauvegarde**.



   Lorsque l'appliance SDX est sauvegardée, les fichiers et images XVA sont stockés séparément pour économiser la bande passante réseau et l'espace disque. Par conséquent, vous devez reconditionner le fichier sauvegardé avant de restaurer l'appliance SDX.

   Lorsque vous reconditionnez le fichier de sauvegarde, il inclut tous les fichiers sauvegardés ensemble pour restaurer l'appliance SDX. Le fichier de sauvegarde reconditionné assure la restauration réussie de l'appliance SDX.

5. Sélectionnez le fichier de sauvegarde qui est reconditionné et cliquez sur **Restaurer**.

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 quotidiennement, hebdomadaire ou mensuel et envoyer le rapport par e-mail ou par un message de marge.

> **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.

Forcer un basculement vers l'instance secondaire de Citrix ADC

April 29, 2021

Vous pouvez forcer un basculement si, par exemple, vous devez remplacer ou mettre à niveau l'instance principale de Citrix Application Delivery Controller (Citrix ADC). Vous pouvez forcer le basculement à partir de l'instance principale ou secondaire. Lorsque vous forcez un basculement sur incident sur l'instance principale, le principal devient le secondaire et le secondaire devient le principal. Le basculement forcé n'est possible que lorsque l'instance principale peut déterminer que l'instance secondaire est UP.

Un basculement forcé n'est ni propagé ni synchronisé. Pour afficher l'état de synchronisation après un basculement forcé, vous pouvez afficher l'état de l'instance.

Un basculement forcé échoue dans l'une des circonstances suivantes :

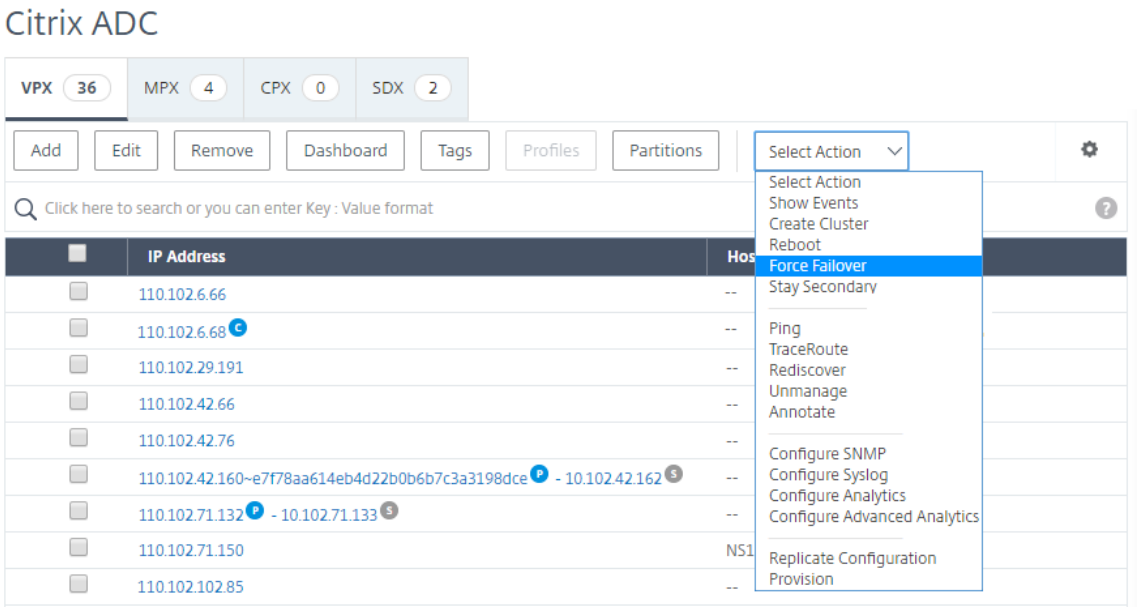
- Vous forcez le basculement sur incident sur un système autonome.
- L'instance secondaire est désactivée ou inactive. Si l'instance secondaire est dans un état inactif, vous devez attendre que son état soit UP pour forcer un basculement sur incident.
- L'instance secondaire est configurée pour rester secondaire.

L'instance de Citrix ADC affiche un message d'avertissement si elle détecte un problème potentiel lorsque vous exécutez la commande force de basculement. Le message inclut les informations qui ont déclenché l'avertissement et demande une confirmation avant de continuer.

Vous pouvez forcer un basculement sur une instance principale ou secondaire.

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

1. Dans Citrix ADM, accédez à **Réseaux** > **Instances**. Accédez à l'onglet **VPX** et sélectionnez une instance.
2. Sélectionnez des instances dans une configuration HA parmi les instances répertoriées sous le type d'instance sélectionné.
3. Dans la zone **Action**, sélectionnez **Forcer le basculement.**
4. Cliquez sur **Oui** pour confirmer l'action de basculement forcé.



Forcer une instance Citrix ADC secondaire à rester secondaire

April 29, 2021

Dans une configuration haute disponibilité (HA), le nœud secondaire peut être forcé de rester secondaire quel que soit l'état du nœud principal.

Par exemple, supposons que le nœud principal doit être mis à niveau et que le processus prend quelques secondes. Pendant la mise à niveau, le nœud principal peut tomber en panne pendant quelques secondes, mais vous ne voulez pas que le nœud secondaire prenne la relève et vous voulez qu'il reste le nœud secondaire même s'il détecte une défaillance dans le nœud principal.

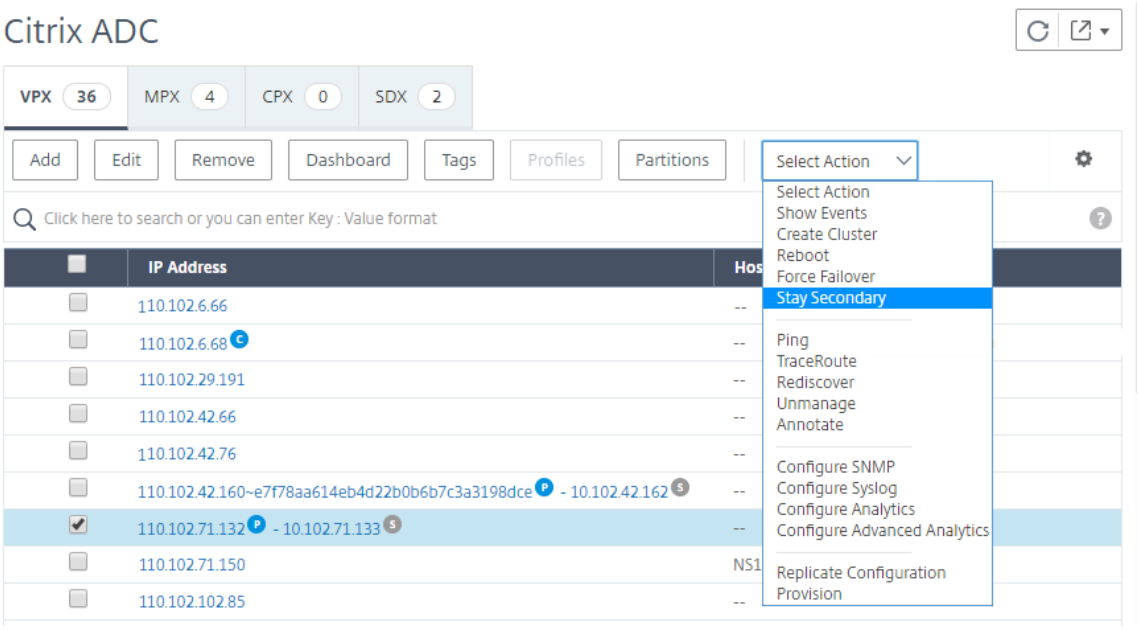
Lorsque vous forcez le nœud secondaire à rester secondaire, il reste secondaire même si le nœud principal tombe en panne. En outre, lorsque vous forcez l'état d'un nœud dans une paire HA à rester secondaire, il ne participe pas aux transitions de machines d'état HA. L'état du nœud est affiché en tant que STAYSECONDARY.

> **Remarque**
>
> Lorsque vous forcez un système à rester secondaire, le processus de forçage n'est ni propagé ni synchronisé. Elle affecte uniquement le nœud sur lequel vous exécutez la commande.

Pour configurer une instance de Citrix ADC secondaire pour qu'elle reste secondaire à l'aide de Citrix ADM :

1. Dans Citrix ADM, accédez à **Réseaux** > **Instances**, puis sélectionnez une instance sous un type d'instance (VPX).

2. Sélectionnez des instances dans une configuration HA parmi les instances répertoriées sous le type d'instance sélectionné.
3. Dans la zone **Action**, sélectionnez **Rester secondaire** .
4. Cliquez sur **Oui** pour confirmer l'exécution de l'action « Rester secondaire ».



Créer des groupes d'instances

April 29, 2021

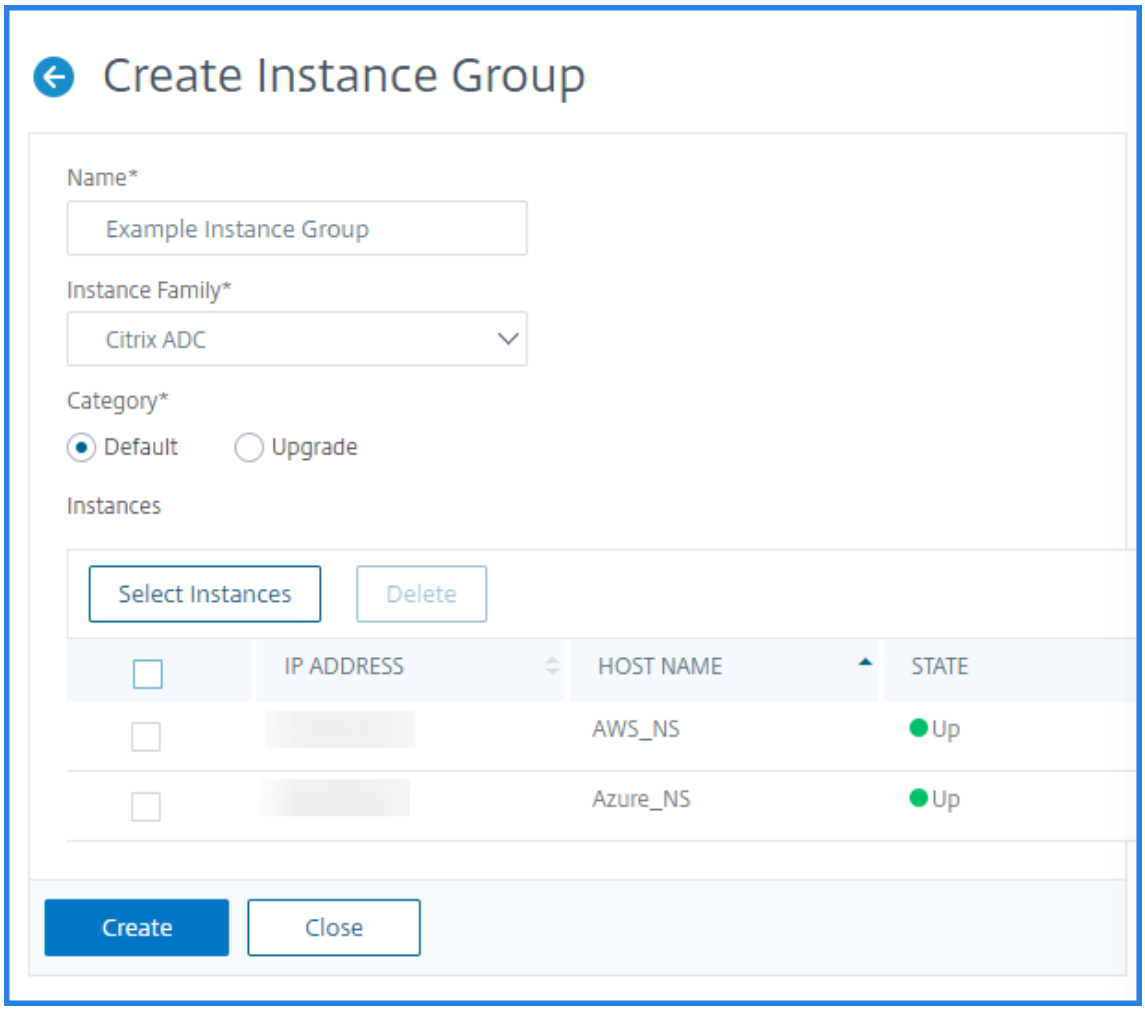
Pour créer un groupe d'instances, vous devez d'abord ajouter toutes vos instances Citrix ADC à Citrix ADM. Après avoir ajouté les instances avec succès, créez des groupes d'instances en fonction de leur famille d'instances. La création d'un groupe d'instances vous permet de mettre à niveau, de sauvegarder ou de restaurer les instances groupées en même temps.

Pour créer un groupe d'instances à l'aide de Citrix ADM

1. Dans Citrix ADM, accédez à **Réseaux** > **Groupes d'instances**, puis cliquez sur **Ajouter** .
2. Spécifiez un nom à votre groupe d'instances et sélectionnez **Citrix ADC** dans la liste **Famille d'instances** .
3. Dans **Catégorie**, sélectionnez l'option **Par défaut**.
4. Cliquez sur **Sélectionner les instances**. Dans la page **Sélectionner des instances**, sélectionnez les instances à regrouper, puis cliquez sur **Sélectionner** .

Le tableau répertorie les instances sélectionnées et leurs détails. Si vous souhaitez supprimer une instance du groupe, sélectionnez-la dans la table et cliquez sur **Supprimer**.

5. Cliquez sur **Créer**.



Provisionner des instances VPX ADC sur SDX à l'aide d'ADM

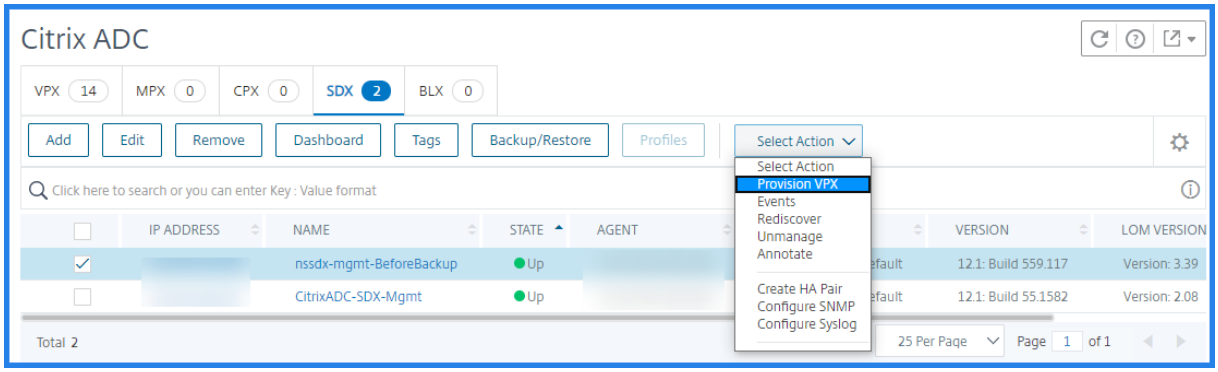
April 29, 2021

Vous pouvez provisionner une ou plusieurs instances VPX ADC sur l'appliance SDX à l'aide de Citrix ADM. Le nombre d'instances que vous pouvez déployer dépend de la licence que vous avez achetée. Si le nombre d'instances ajoutées est égal au nombre spécifié dans la licence, le service ADM ne vous permet pas de provisionner davantage d'instances Citrix ADC.

Avant de commencer, assurez-vous d'ajouter une instance SDX dans ADM où vous souhaitez provisionner des instances VPX.

Pour provisionner une instance VPX, procédez comme suit :

1. Accédez à **Réseaux > Instances > Citrix ADC**.
2. Dans l'onglet **SDX**, sélectionnez une instance SDX dans laquelle vous souhaitez provisionner une instance VPX.
3. Dans **Sélectionner une action**, sélectionnez **Provisionner VPX**.



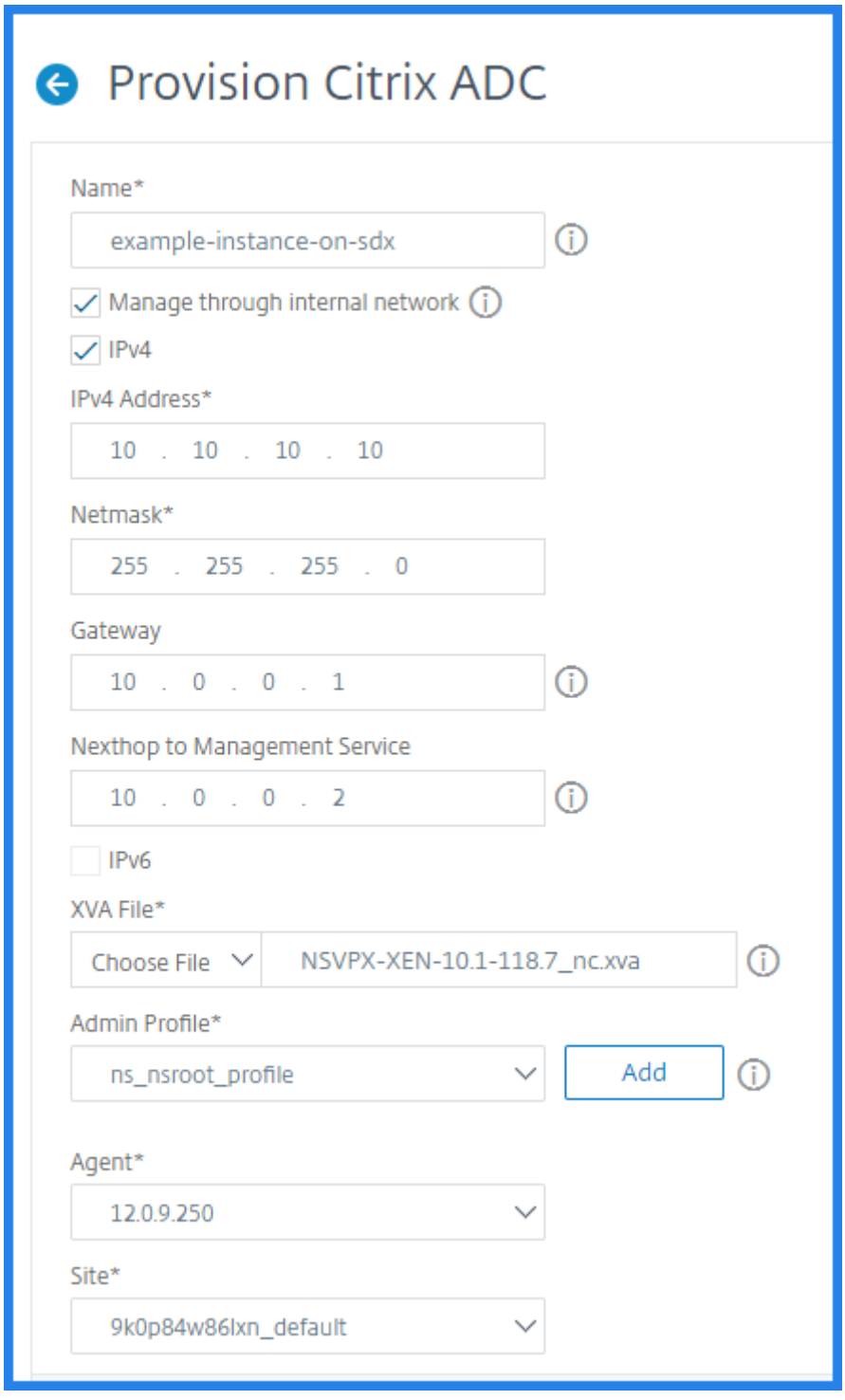
Étape 1 - Ajouter une instance VPX

Le service ADM utilise les informations suivantes pour configurer les instances VPX dans une appliance SDX :

- **Nom** : spécifiez un nom à une instance ADC.
- Établir un réseau de communication entre SDX et VPX. Pour ce faire, sélectionnez les options requises dans la liste :
  - **Gérer via le réseau interne** - Cette option établit un réseau interne pour une communication entre ADM et une instance VPX.
  - **Adresse IP** - Vous pouvez sélectionner une adresse **IPv4** ou **IPv6** ou les deux pour gérer l'instance Citrix VPX. Une instance VPX ne peut avoir qu'une seule adresse IP de gestion (également appelée Citrix ADC IP). Vous ne pouvez pas supprimer l'adresse IP Citrix ADC.

    Pour l'option sélectionnée, attribuez un masque de réseau, une passerelle par défaut et un saut suivant au service ADM pour l'adresse IP.
- **XVA File** - Sélectionnez le fichier XVA à partir duquel vous souhaitez provisionner une instance VPX. Utilisez l'une des options suivantes pour sélectionner le fichier XVA.
  - **Local** - Sélectionnez le fichier XVA de votre ordinateur local.
  - **Appliance** - Sélectionnez le fichier XVA dans un navigateur de fichiers ADM.
- **Profil d'administrateur** - Ce profil permet d'accéder au provisionnement des instances VPX. Avec ce profil, ADM récupère les données de configuration d'une instance. Si vous devez ajouter un profil, cliquez sur **Ajouter**.

- **Agent** - Sélectionnez l'agent auquel vous souhaitez associer les instances
- **Site** - Sélectionnez le site où vous souhaitez ajouter l'instance.



Étape 2 - Allouer des licences

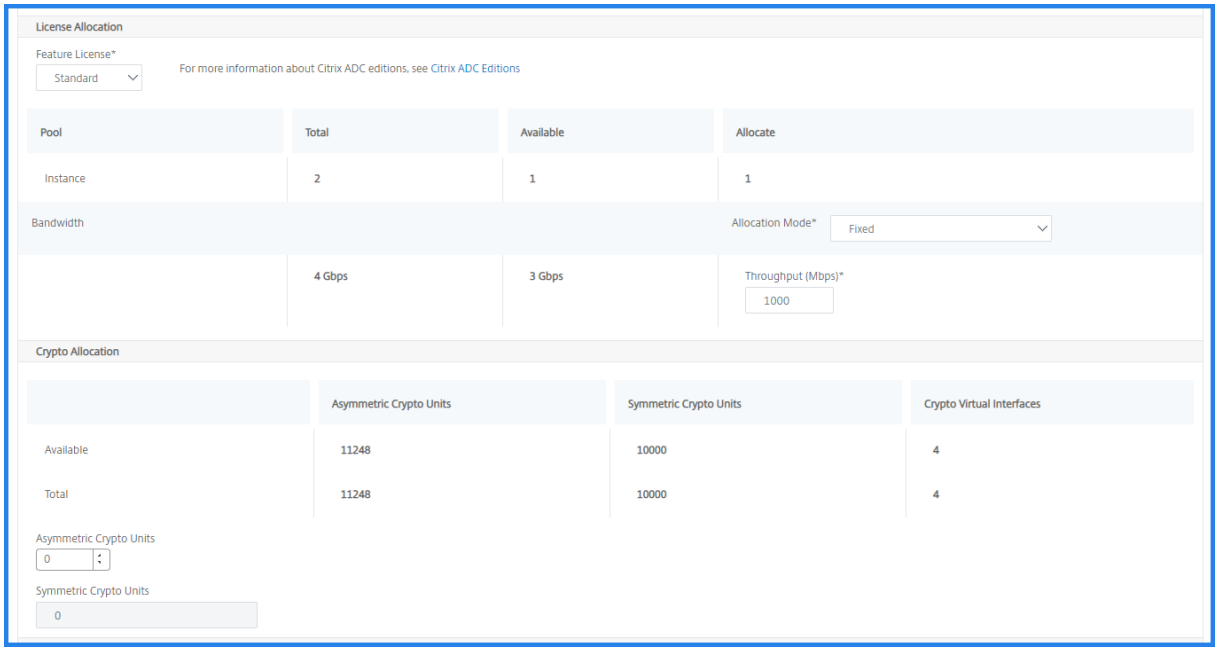
Dans la section **Allocation de licences**, spécifiez la licence VPX. Vous pouvez utiliser des licences Standard, Advanced et Premium.

- **Mode d'allocation** - Vous pouvez choisir les modes **Fixe** ou **Burstable** pour le pool de bande passante.

  Si vous choisissez le mode **Burstable**, vous pouvez utiliser une bande passante supplémentaire lorsque la bande passante fixe est atteinte.

- **Débit** - Affectez le débit total (en Mbps) à une instance.

> **Remarque**
>
> Achetez une licence distincte (SDX 2-Instance Add-On Pack pour Secure Web Gateway) pour les instances Citrix Secure Web Gateway (SWG) sur les appliances SDX. Ce pack d'instances est différent de la licence de plate-forme SDX ou du pack d'instances SDX.
>
> Pour plus d'informations, reportez-vous à la section Déploiement d'une instance Citrix Secure Web Gateway sur une appliance SDX.



À partir de la version SDX 12.0 57.19, l'interface pour gérer la capacité de chiffrement a changé. Pour de plus amples informations, consultez la section Gérer la capacité crypto.

Étape 3 - Allouer les ressources

Dans la section **Allocation de ressources**, allouez des ressources à une instance VPX pour maintenir le trafic.

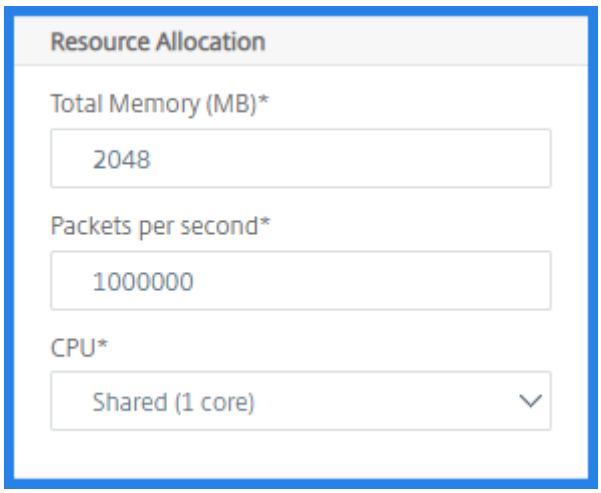
- **Mémoire totale (Mo)** - Affectez la mémoire totale à une instance. La valeur minimale est `2048` Mo.
- **Paquets par seconde** - Spécifiez le nombre de paquets à transmettre par seconde.
- **CPU** - Spécifiez le nombre de cœurs de CPU à une instance. Vous pouvez utiliser des cœurs CPU partagés ou dédiés.

  Lorsque vous sélectionnez un cœur partagé pour une instance, les autres instances peuvent utiliser le noyau partagé au moment de la pénurie de ressources.

  Redémarrez les instances sur lesquelles les cœurs CPU sont réaffectés pour éviter toute dégradation des performances.

  Si vous utilisez la plate-forme SDX 25000xx, vous pouvez affecter un maximum de 16 cœurs à une instance. De plus, si vous utilisez la plate-forme SDX 2500xxx, vous pouvez affecter un maximum de 11 cœurs à une instance.

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



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

Nom de la plateforme	Nombre total de noyaux	Nombre total de cœurs disponibles pour le provisionnement VPX	Nombre maximal de cœurs pouvant être affectés à une seule instance
SDX 8015, SDX 8400 et SDX 8600	4	3	3
SDX 8900	8	7	7

Nom de la plateforme	Nombre total de noyaux	Nombre total de cœurs disponibles pour le provisionnement VPX	Nombre maximal de cœurs pouvant être affectés à une seule instance
SDX 11500, SDX 13500, SDX 14500, SDX 16500, SDX 18500 et SDX 20500	12	10	5
SDX 11515, SDX 11520, SDX 11530, SDX 11540 et SDX 11542	12	10	5
SDX 17500, SDX 19500 et SDX 21500	12	10	5
SDX 17550, SDX 19550, SDX 20550 et SDX 21550	12	10	5
SDX 14020, SDX 14030, SDX 14040, SDX 14060, SDX 14080 et SDX 14100	12	10	5
SDX 22040, SDX 22060, SDX 22080, SDX 22100 et SDX 22120	16	14	7
SDX 24100 et SDX 24150	16	14	7
SDX 14020 40 G, SDX 14030 40 G, SDX 14040 40 G, SDX 14060 40 G, SDX 14080 40G et SDX 14100 40 G	12	10	10

Nom de la plateforme	Nombre total de noyaux	Nombre total de cœurs disponibles pour le provisionnement VPX	Nombre maximal de cœurs pouvant être affectés à une seule instance
SDX 14020 FIPS, SDX 14030 FIPS, SDX 14040 FIPS, SDX 14060 FIPS, SDX 14080 FIPS et SDX 14100. FIPS	12	10	5
SDX 14040 40S, SDX 14060 40S, SDX 14080 40S et SDX 14100 40S	12	10	5
SDX 25100A, 25160A, 25200A	20	18	9
SDX 25100-40G, 25160-40G, 25200-40G	20	18	16 (si la version est 11.1-51.x ou supérieure) ; 9 (si la version est 11.1-50.x ou inférieure ; toutes les versions de 11.0 et 10.5)
SDX 26100, 26160, 26200, 26250	28	26	13
15000-50G	16	14	7

Remarque

Sur la plate-forme SDX 26xxx, un maximum de 26 cœurs de CPU peuvent être affectés à une instance VPX. Si des unités crypto sont affectées à l'instance, le nombre maximal de cœurs dépend du nombre d'unités de crypto et d'interfaces de données.

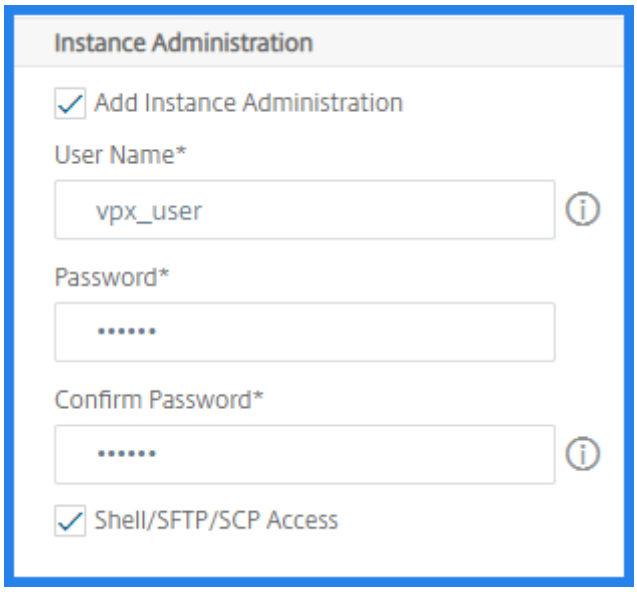
Par exemple, si vous affectez 24000 unités de chiffrement à une instance, vous pouvez affecter 24 cœurs de CPU et deux interfaces de données maximum à l'instance. L'appliance SDX considère les interfaces de données et les unités de chiffrement comme des périphériques PCI. Pour 26000 unités crypto, le provisionnement d'instance VPX échoue en raison de l'absence d'espace pour ajouter des interfaces de données.

Étape 4 - Ajouter l'administration d'instance

Vous pouvez créer un utilisateur administrateur pour l'instance VPX. Pour ce faire, sélectionnez **Ajouter une administration d'instance** dans la section **Administration de l'instance**.

Spécifiez les détails suivants :

- **Nom d'utilisateur** : nom d'utilisateur de l'administrateur de l'instance Citrix ADC. Cet utilisateur dispose d'un accès superutilisateur, mais n'a pas accès aux commandes de mise en réseau pour configurer des VLAN et des interfaces.
- **Mot de passe** : spécifiez le mot de passe du nom d'utilisateur.
- **Accès Shell/Sftp/SCP** : Accès autorisé à l'administrateur de l'instance Citrix ADC. Cette option est sélectionnée par défaut.



Étape 5 - Spécifier les paramètres réseau

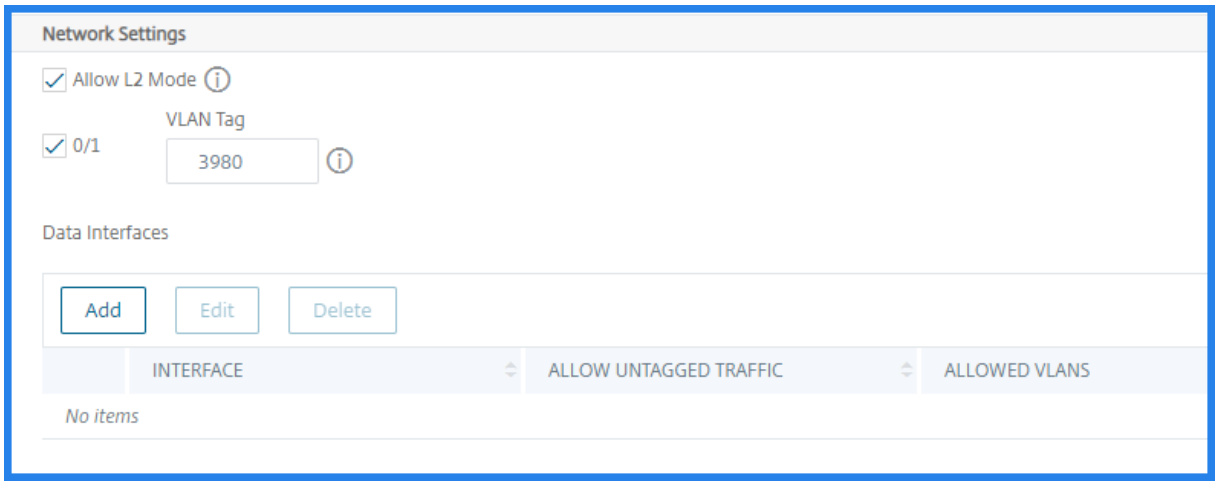
Sélectionnez les paramètres réseau requis pour une instance :

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

  > **Remarque**
  >
  > Si vous désactivez le mode L2 pour une instance, vous devez vous connecter à l'instance et désactiver le mode L2 à partir de cette instance. Sinon, tous les autres modes Citrix ADC peuvent être désactivés après le redémarrage de l'instance.

- **0/1** - Dans la **balise VLAN**, spécifiez un ID VLAN pour l'interface de gestion.
- **0/2** - Dans la **balise VLAN**, spécifiez un ID VLAN pour l'interface de gestion.

Par défaut, les interfaces **0/1** et **0/2** sont sélectionnées.



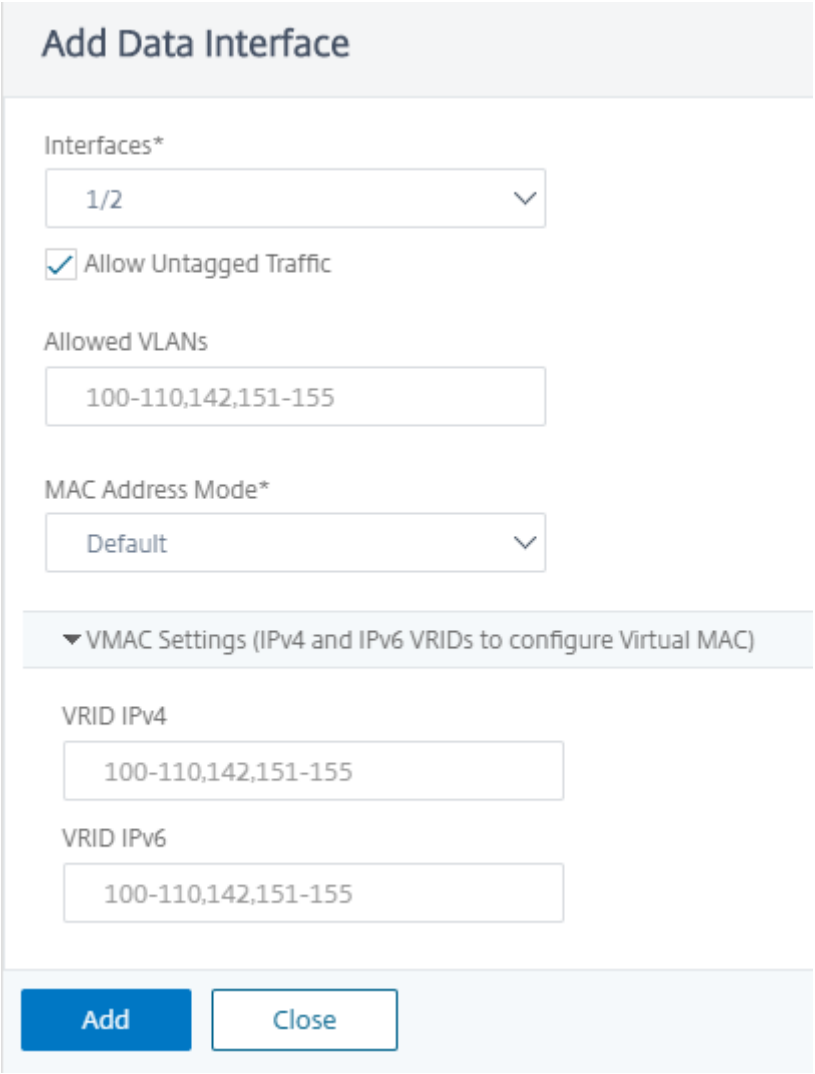
Dans **Interfaces de données**, cliquez sur **Ajouter** pour ajouter des interfaces de données et spécifiez les éléments suivants :

- **Interfaces** - Sélectionnez l'interface dans la liste.

  > **Remarque**
  >
  > Les ID d'interface des interfaces que vous ajoutez à une instance ne correspondent pas nécessairement à la numérotation de l'interface physique sur l'appliance SDX.
  >
  > Par exemple, la première interface que vous associez à instance-1 est l'interface SDX 1/4, elle apparaît sous la forme d'interface 1/1 lorsque vous affichez les paramètres de l'interface dans cette instance. Cette interface indique qu'il s'agit de la première interface que vous avez associée à instance-1.

- **VLAN autorisés :** spécifiez une liste d'ID VLAN pouvant être associés à une instance Citrix ADC.
- **Mode d'adresse MAC** - Affectez une adresse MAC à une instance. Sélectionnez l'une des options suivantes :
  - **Valeur par défaut** - Citrix Workspace attribue une adresse MAC.
  - **Personnalisé** : choisissez ce mode pour spécifier une adresse MAC qui remplace l'adresse MAC générée.
  - **Généré : générez** une adresse MAC à l'aide de l'ensemble d'adresses MAC de base précédemment. Pour plus d'informations sur la définition d'une adresse MAC de base, consultez Affectation d'une adresse MAC à une interface.
- **Paramètres VMAC (VRID IPv4 et IPv6 pour configurer Virtual MAC)**

- **VRID IPV4** - Le VRID IPv4 qui identifie le VMAC. Valeurs possibles : 1—255. Pour de plus amples informations, consultez la section Configuration des VMAC sur une interface.
- VRID IPV6 - Le VRID IPv6 qui identifie le VMAC. Valeurs possibles : 1—255. Pour de plus amples informations, consultez la section Configuration des VMAC sur une interface.



Cliquez sur **Ajouter**.

Étape 6 - Spécifier les paramètres du VLAN de gestion

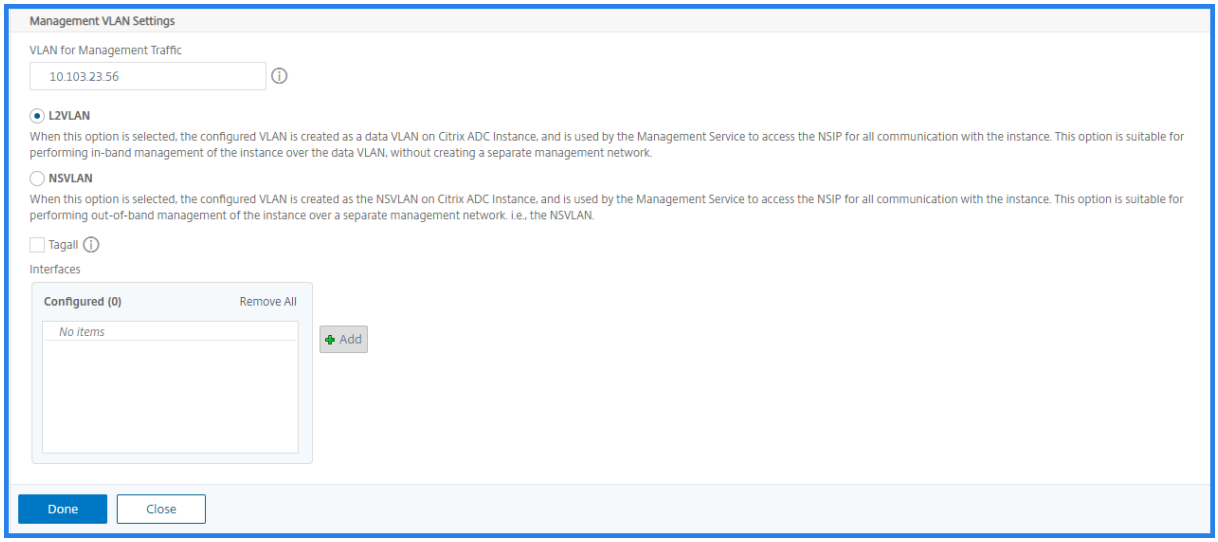
Le service de gestion et l'adresse de gestion (NSIP) de l'instance VPX se trouvent dans le même sous-réseau, et la communication se fait via une interface de gestion.

Si le service de gestion et l'instance se trouvent dans des sous-réseaux différents, spécifiez un ID VLAN pendant que vous provisionnez une instance VPX. Par conséquent, l'instance est accessible sur le réseau lorsqu'elle est active.

Si votre déploiement nécessite que le NSIP est accessible uniquement via l'interface sélectionnée lors du provisionnement de l'instance VPX, sélectionnez **NSVLAN**. Et, le NSIP devient inaccessible via d'autres interfaces.

- Les battements de cœur HA sont envoyés uniquement sur les interfaces qui font partie du NSVLAN.
- Vous pouvez configurer un NSVLAN uniquement à partir de la version XVA VPX `9.3-53.4` et ultérieure.

> **Important**
>
> - Vous ne pouvez pas modifier ce paramètre après avoir configuré l'instance VPX.
> - La `clear config full` commande de l'instance VPX supprime la configuration du VLAN si **NSVLAN** n'est pas sélectionnée.

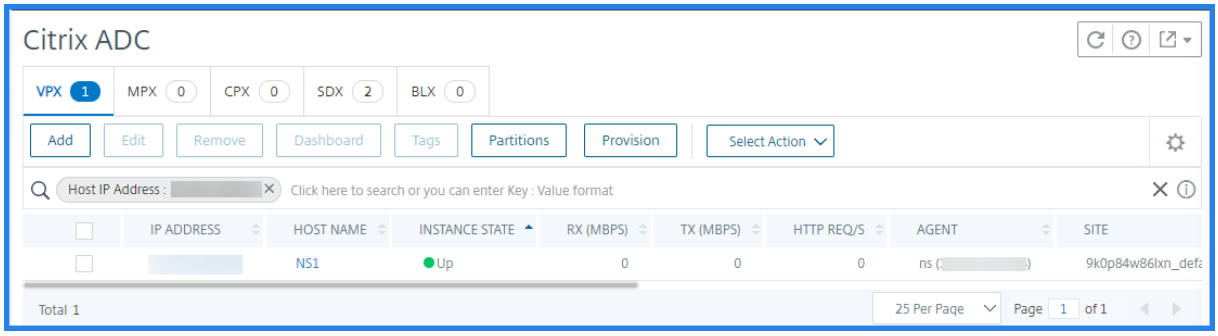


Cliquez sur **Terminé** pour provisionner une instance VPX.

Afficher l'instance VPX provisionnée

Pour afficher l'instance nouvellement provisionnée, procédez comme suit :

1. Accédez à **Réseaux > Instances > Citrix ADC**.
2. Dans l'onglet **VPX**, recherchez une instance à l'aide de la propriété d' **adresse IP de l'hôte** et spécifiez l'adresse IP de l'instance SDX.



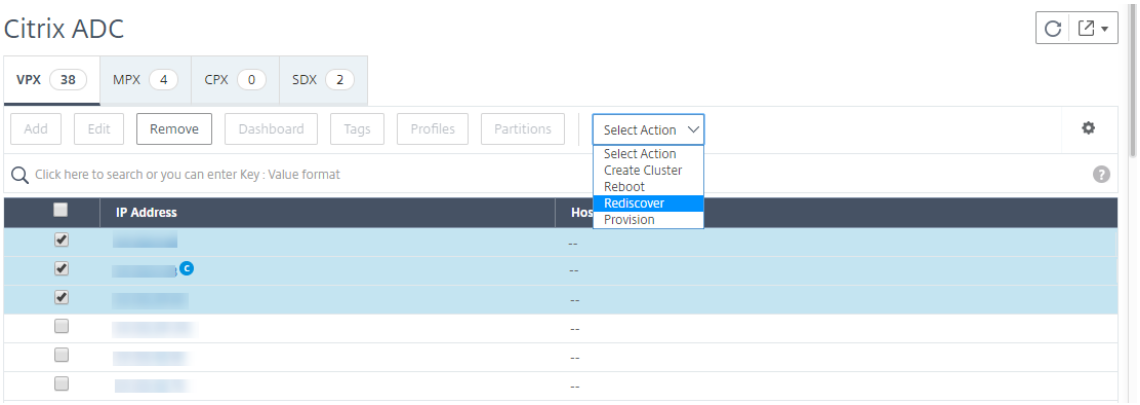
Redécouvrir plusieurs instances Citrix ADC VPX

April 29, 2021

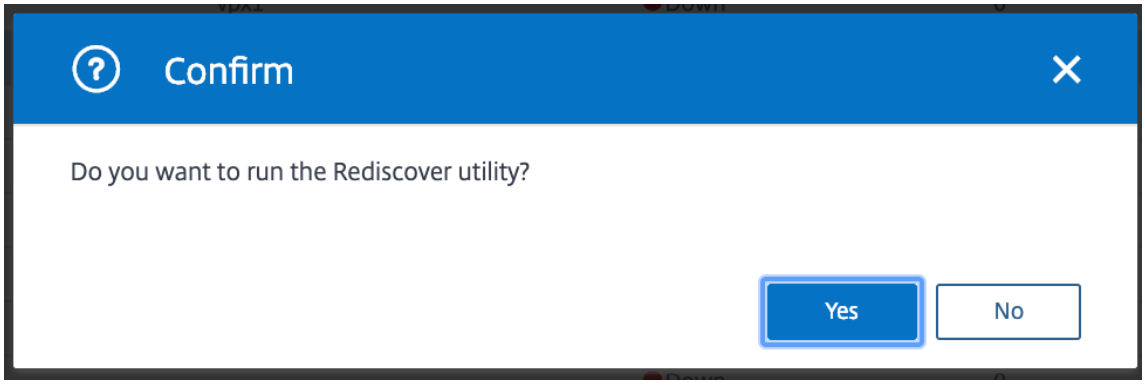
Vous pouvez désormais redécouvrir plusieurs instances VPX Citrix Application Delivery Controller (Citrix ADC) dans votre configuration Citrix Application Delivery Management (Citrix ADM). Auparavant, vous étiez en mesure de redécouvrir uniquement des instances Citrix ADC VPX uniques. Vous pouvez redécouvrir plusieurs instances Citrix ADC VPX lorsque vous souhaitez afficher les derniers états et configurations de ces instances. Le serveur Citrix ADM redécouvre toutes les instances Citrix ADC VPX et vérifie si les instances de Citrix ADC sont accessibles.

Pour redécouvrir plusieurs instances Citrix ADC VPX :

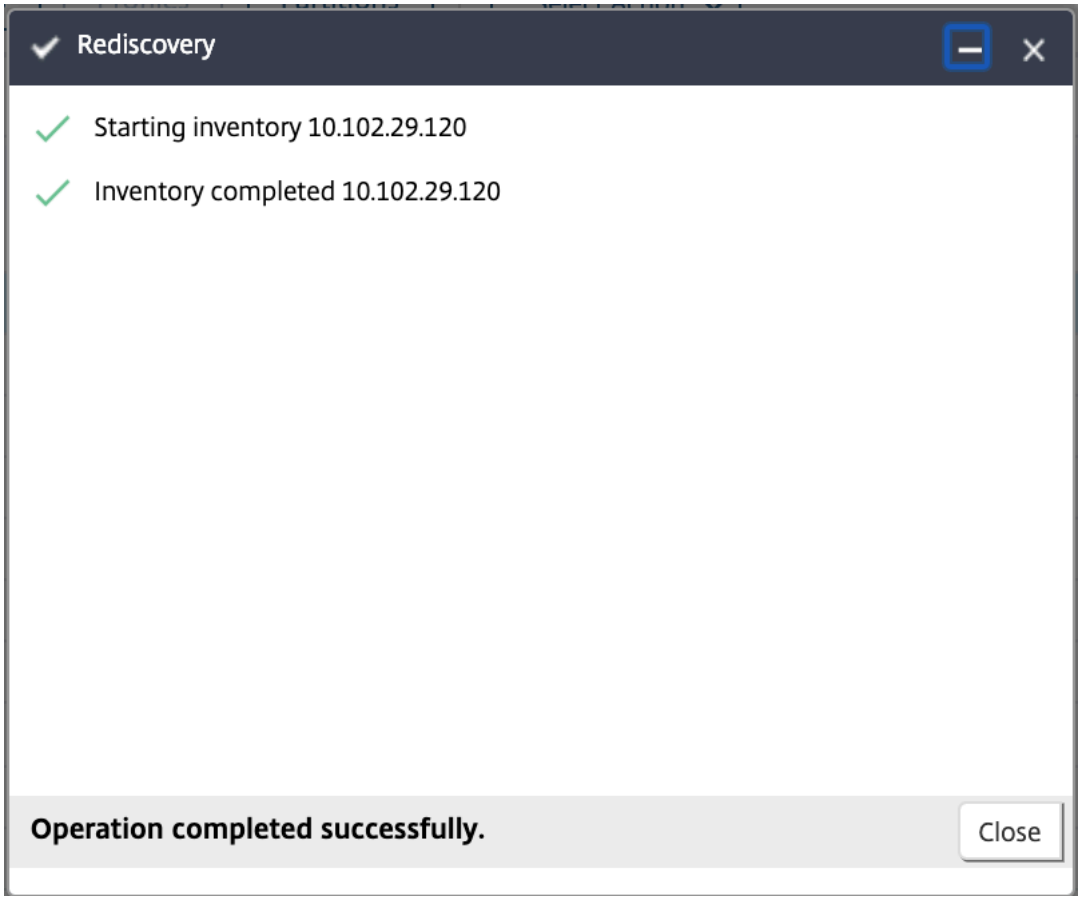
1. Accédez à **Réseaux** > **Instances** > **Citrix ADC** > **VPX**, sélectionnez les instances que vous souhaitez redécouvrir.
2. Dans la zone **Action**, cliquez sur **Redécouvrir** .



3. 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 ADC VPX.



Vue d'ensemble des sondages

April 29, 2021

L'interrogation est un processus dans lequel Citrix Application Delivery Management (ADM) recueille 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 de toutes les instances ADC gérées. Voici les différents types d'interrogation qui se produisent entre ADM et les instances gérées :

- Sondage d'instance
- Inventaire interrogation
- Collecte de données sur les performances
- interrogation de sauvegarde d'instance
- interrogation d'audit de configuration
- interrogation de certificat SSL
- Interrogation d'entité

Citrix ADM utilise des protocoles tels que les appels NITRO, 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 des intervalles d'interrogation pour quelques types d'interrogation et vous permet d'interroger manuellement si nécessaire.

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

Type d'interrogation	Intervalle d'interrogation	Informations sur les sondages	Protocole utilisé	Configuration de l'intervalle d'interrogation
Sondage d'instance	Toutes les 5 minutes (par défaut)	Informations statistiques telles que l'état, les requêtes HTTP par seconde, l'utilisation du processeur, l'utilisation de la mémoire et le débit.	Appel de NITRO.	Non
Inventaire interrogation	Toutes les 60 minutes (par défaut)	Détails de l'inventaire, tels que la version de build, les informations système, les fonctionnalités sous licence et les modes.	Appels NITRO et SSH	Non
Collecte de données sur les performances	Toutes les 5 minutes (par défaut)	Informations sur les rapports réseau	Appel NITRO	Non

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

Type d'interrogation	Intervalle d'interrogation	Informations sur les sondages	Protocole utilisé	Configuration de l'intervalle d'interrogation
				Vous pouvez interroger manuellement les audits de configuration et ajouter immédiatement tous les audits de configuration des instances à Citrix ADM. Pour ce faire, accédez à **Réseaux** > **Audit de configuration** et cliquez sur **Interroger maintenant**. La page **Sondage maintenant** vous permet d'interroger toutes les instances ou certaines instances du réseau.

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

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

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

Remarque

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

Pendant la sauvegarde d'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 d'instances Citrix ADC gérées sont stockées en interne dans

> la base de données.

Différentes méthodes d'interrogation des instances

Voici les différentes méthodes d'interrogation effectuées par Citrix ADM sur les instances gérées :

- Sondage global des instances
- interrogation manuelle des instances
- Sondage manuel des entités

Sondage global 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 60 minutes, vous pouvez définir l'intervalle 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 un écran vide ou le système peut toujours afficher des données antérieures.

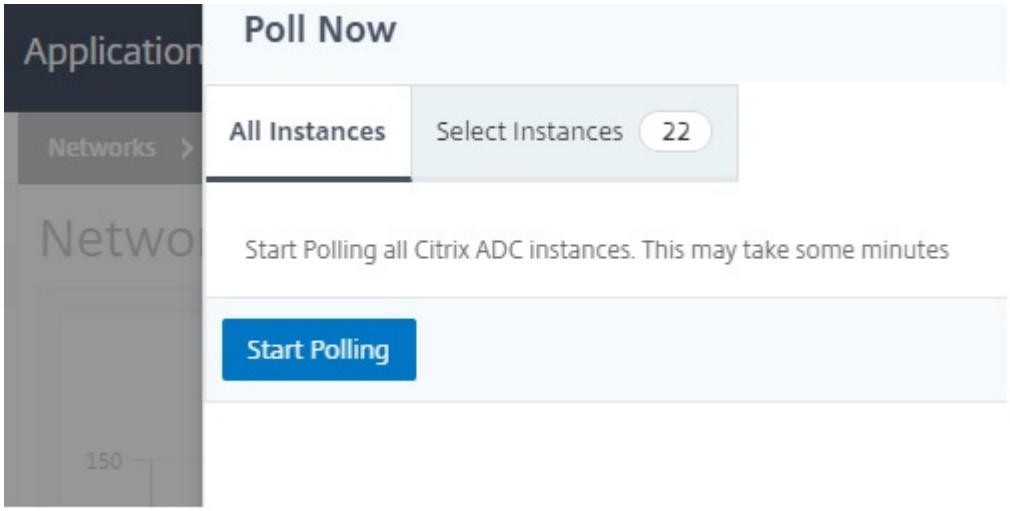
Dans Citrix ADM, il existe une période minimale d'intervalle d'interrogation lorsque l'interrogation automatique ne se produit pas. Si vous ajoutez une nouvelle instance de Citrix ADC ou si une entité est mise à jour, Citrix ADM ne reconnaît pas la nouvelle instance ou les mises à jour apportées à une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

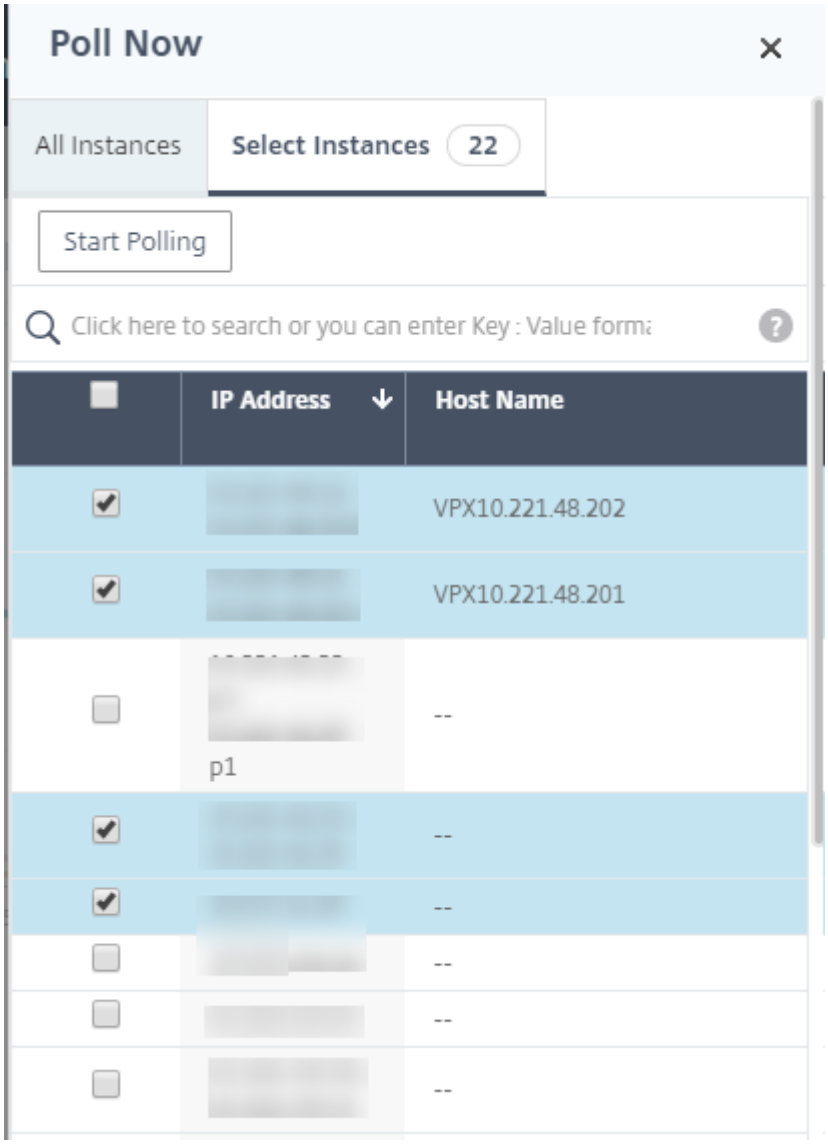
Citrix ADM interroge automatiquement les instances gérées pour collecter des informations à des heures définies par jour. L'interrogation sélectionnée réduit le temps d'actualisation requis par Citrix ADM pour afficher le statut le plus récent des entités liées à ces instances sélectionnées.

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 **Poll Now** vous permet d'interroger toutes les instances de Citrix ADC dans le réseau ou d'interroger les instances sélectionnées.
    a) Onglet**Toutes les instances** : cliquez sur **Démarrer l'interrogation** 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.

Interquation manuelle des entités

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

Prenons un exemple de serveur virtuel en **panne**. L'état de ce serveur virtuel a peut-être changé en **UP**, avant l'interrogation automatique suivante. Pour afficher l'état modifié du serveur virtuel, vous

voudrez peut-être interroger uniquement ce serveur virtuel, afin que le statut correct soit affiché immédiatement sur l'interface graphique.

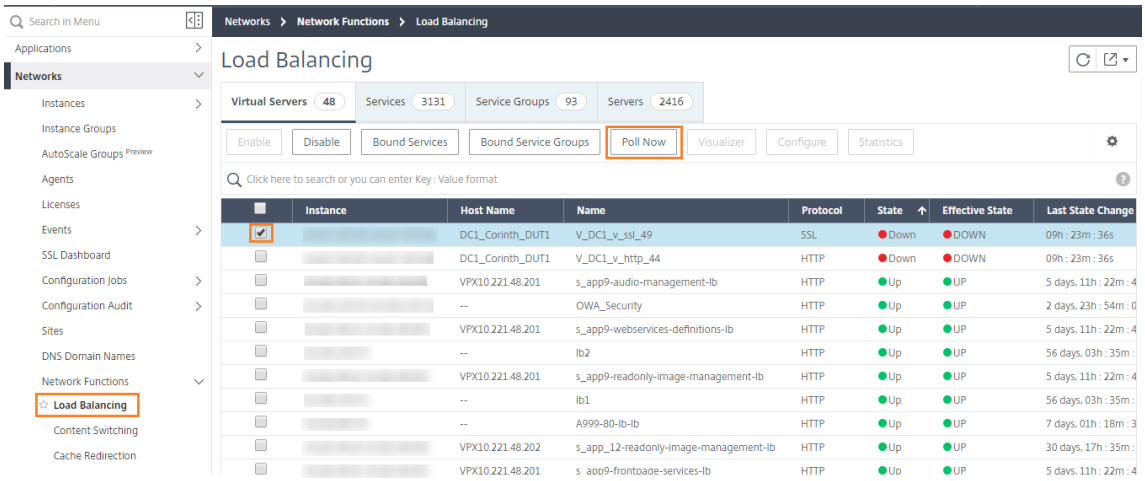
Vous pouvez désormais interroger les entités suivantes pour toute mise à jour de leur état, services, groupes de services, serveurs virtuels d'équilibrage de charge, serveurs virtuels de réduction de cache, serveurs virtuels de commutation de contenu, serveurs virtuels d'authentification, serveurs virtuels 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 manuellement les entités ou vous devez interroger l'instance.

Pour interroger des entités spécifiques dans Citrix ADM :

À titre d'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 **BAS**, puis cliquez sur **Interroger maintenant**. L'état du serveur virtuel passe maintenant à **UP**.



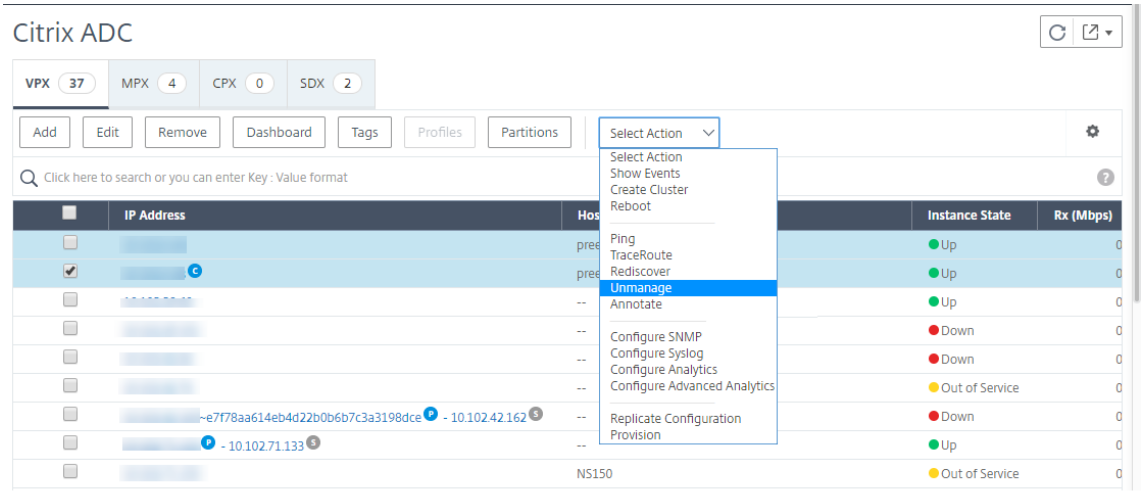
Annuler l'administration d'une instance

April 29, 2021

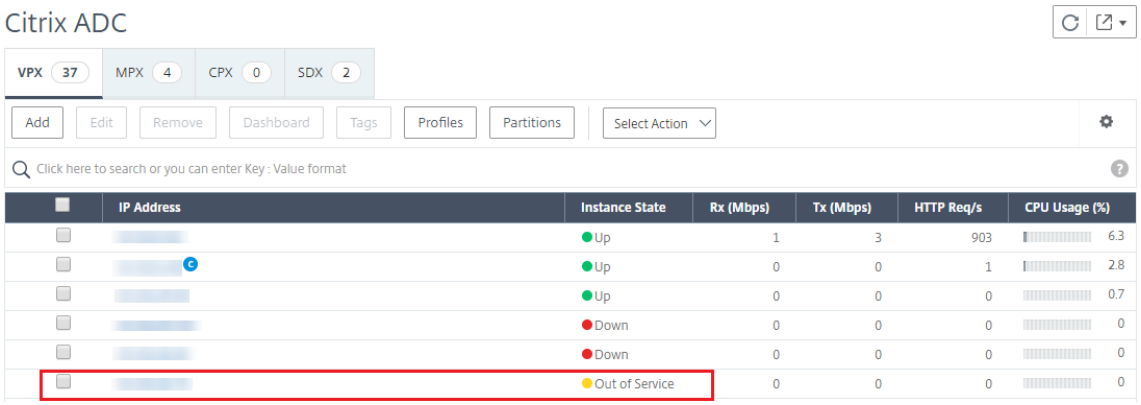
Si vous souhaitez arrêter l'échange d'informations entre Citrix Application Delivery Management (Citrix ADM) et les instances de votre réseau, vous pouvez annuler la gestion des instances.

Pour annuler la gestion d'une instance :

1. Accédez à **Réseaux** > **Instances** > **Citrix ADC**.
2. Sélectionnez l'onglet Instance ADC (par exemple, VPX).
3. Dans la liste des instances, cliquez avec le bouton droit sur une instance, puis sélectionnez **Ne pas gérer**, ou sélectionnez instance et dans la liste **Action**, sélectionnez **Ne pas gérer**.



L'état de l'instance sélectionnée passe à **Out of Service**.



L'instance n'est plus gérée par Citrix ADM et n'échange plus de données avec Citrix ADM.

Tracer l'itinéraire vers une instance

April 29, 2021

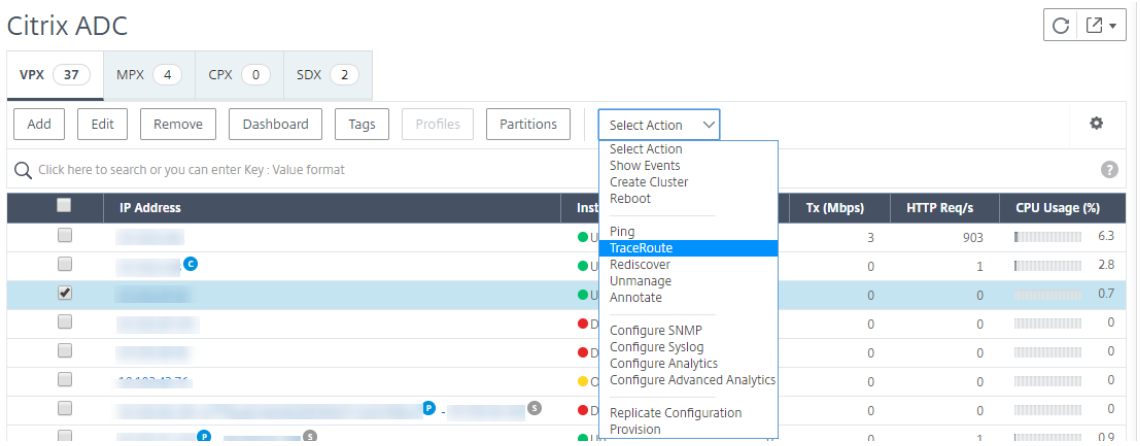
En traçant l'itinéraire d'un paquet depuis Citrix Application Delivery Management (Citrix ADM) vers une instance, vous pouvez trouver des informations telles que le nombre de sauts nécessaires pour

atteindre l'instance. Le 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.

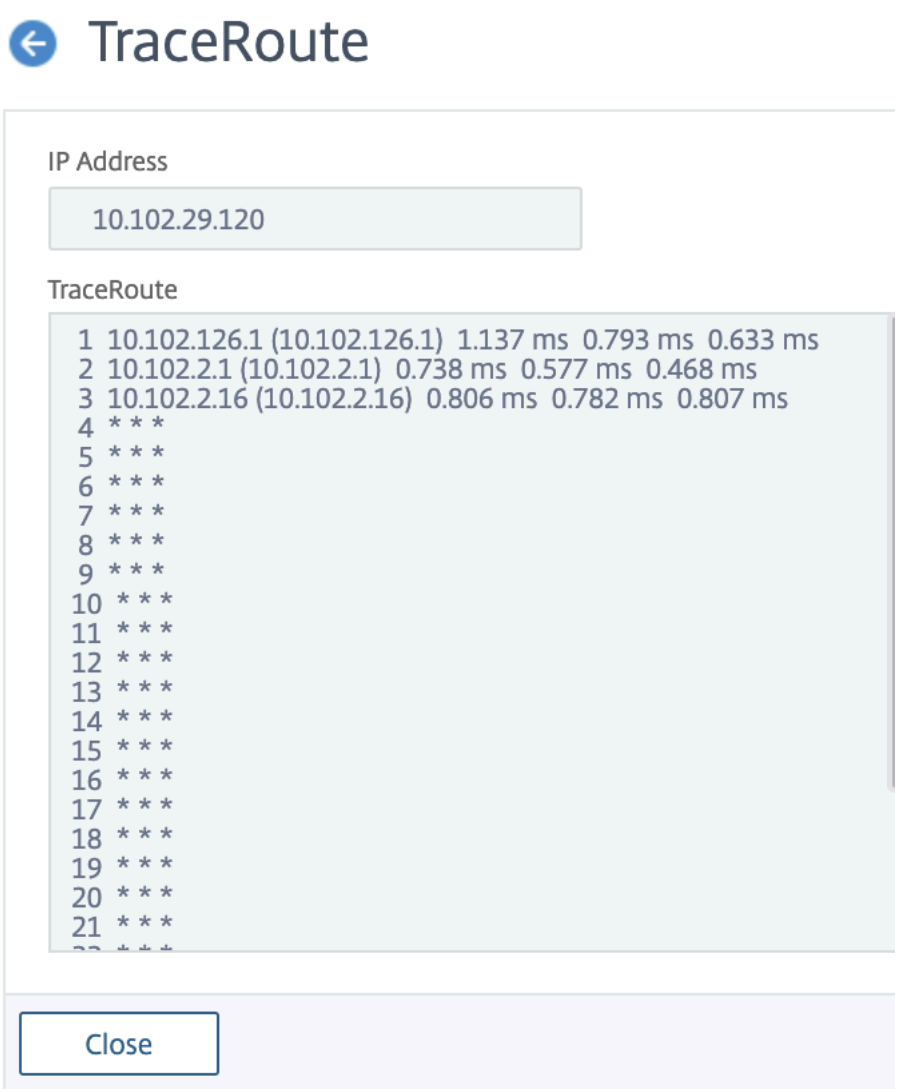
Traceroute enregistre également le temps qu'un paquet prend pour voyager d'un saut à l'autre. S'il y a une interruption dans le transfert des paquets, le traceroute indique où le problème existe.

Pour tracer la route d'une instance :

1. Accédez à **Réseaux** > **Instances** > **Citrix ADC**.
2. Sélectionnez l'onglet Instance ADC (par exemple, VPX).
3. Dans la liste des instances, cliquez avec le bouton droit sur une instance, puis sélectionnez **TraceRoute**, ou sélectionnez l'instance et, dans la liste **Action**, cliquez sur **TraceRoute**.



La boîte de message TraceRoute indique l'itinéraire vers l'instance et le temps, en millisecondes, consommé par chaque saut.



Comment modifier le mot de passe racine Citrix ADC MPX ou VPX

April 29, 2021

Parfois, vous devez modifier le mot de passe racine de l'appliance Citrix ADC pour des raisons de sécurité ou de conformité de la stratégie de rotation des mots de passe.

Ce document décrit les étapes requises pour modifier le mot de passe racine des appliances Citrix ADC MPX et VPX gérées via le cloud Citrix ADM.

Si vous modifiez le mot de passe ADC, vous devez modifier le profil d'administration ADM associé au ADC. Un profil d'administrateur ADM conserve les informations d'identification ADC pour les communications basées sur l'API REST, SSH, SCP ou SNMP avec l'appliance ADC. Grâce aux profils d'administration, Citrix ADM gère les appliances Citrix ADC MPX et VPX.

Modifier le mot de passe à l'aide de la fonctionnalité Travaux de configuration

En utilisant la fonctionnalité Travaux de configuration Citrix ADM, vous pouvez simplifier le processus répétitif de modification de mot de passe et appliquer les modifications aux appliances Citrix ADC, sans accéder aux instances individuelles.

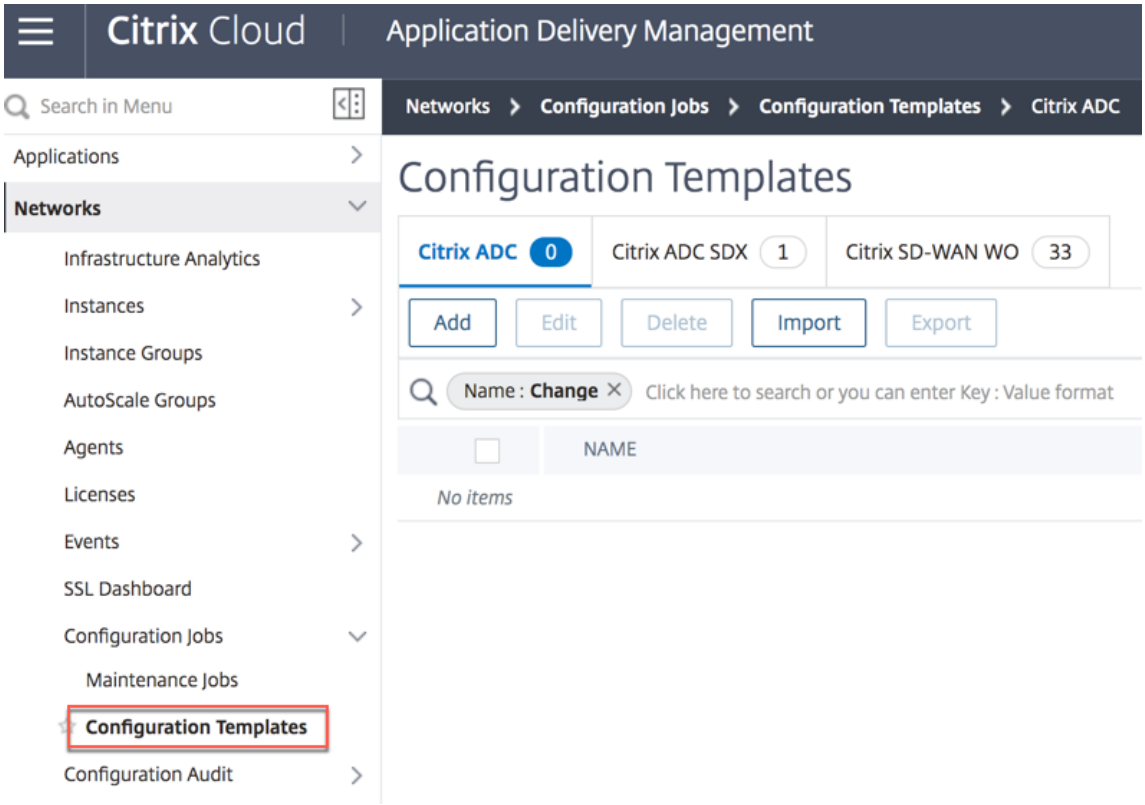
Pour modifier le mot de passe, procédez comme suit :

- Étape 1. Créez un modèle de configuration.
- Étape 2. Créez un travail de configuration.
- Étape 3. Créez un profil admin et modifiez-le.

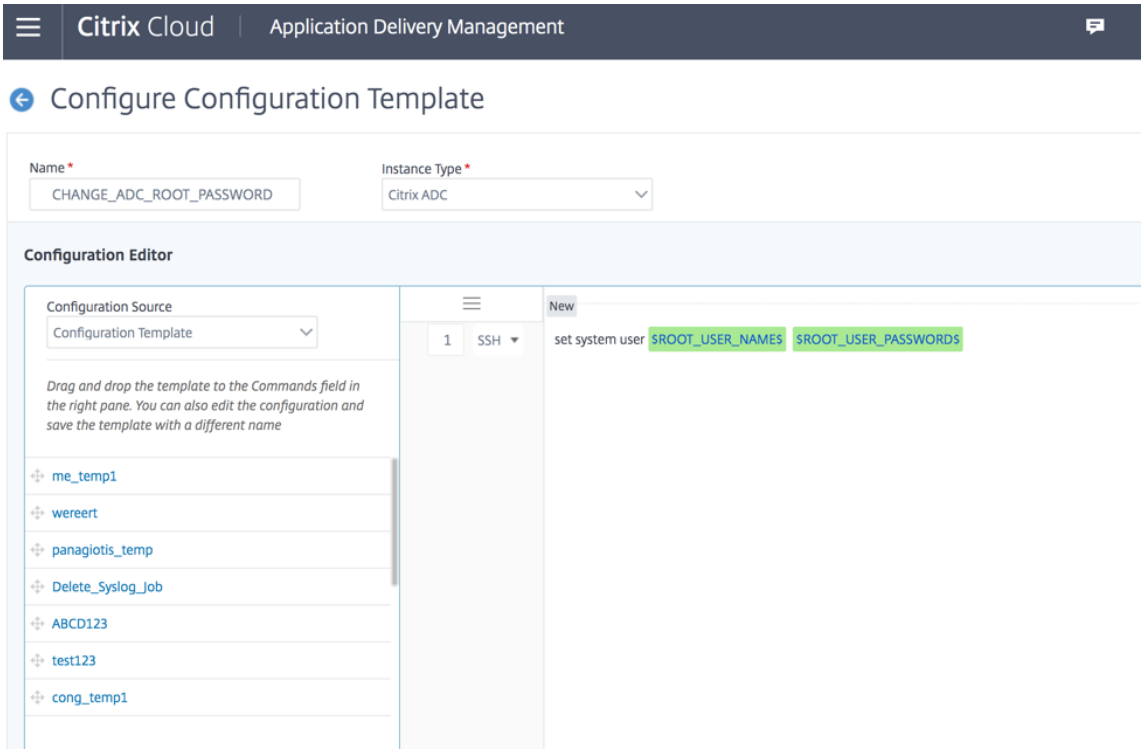
> Remarque : si les appliances ADC sont également gérées par d'autres outils, vous devez également modifier les informations d'identification de ces outils.

Créer un modèle de configuration

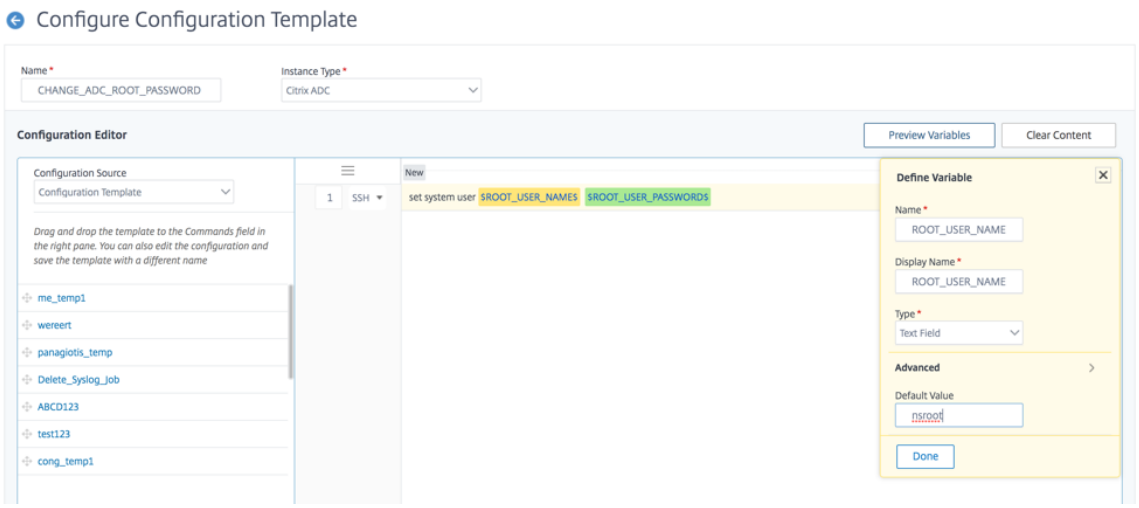
1. Dans l'interface graphique ADM, accédez à **Réseaux > Travaux de configuration > Modèles de configuration**.



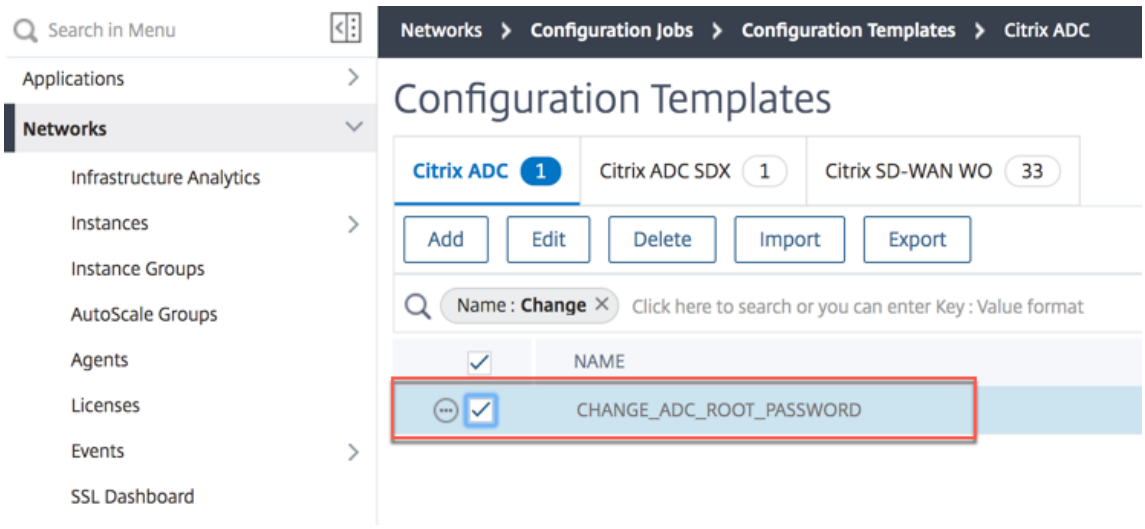
2. Sélectionnez **Ajouter**. Créez un modèle de configuration avec en tapant la commande SSH `set system user $ROOT_USER_NAME$ $ROOT_USER_PASSWORD$`.



3. Sélectionnez la variable $ROOT_USER_NAME$ et sélectionnez **Champ de texte comme Type**.
4. Le cas échéant, indiquez la valeur par défaut du nom d'utilisateur racine. Sélectionnez **Terminé** pour enregistrer les paramètres de la variable.

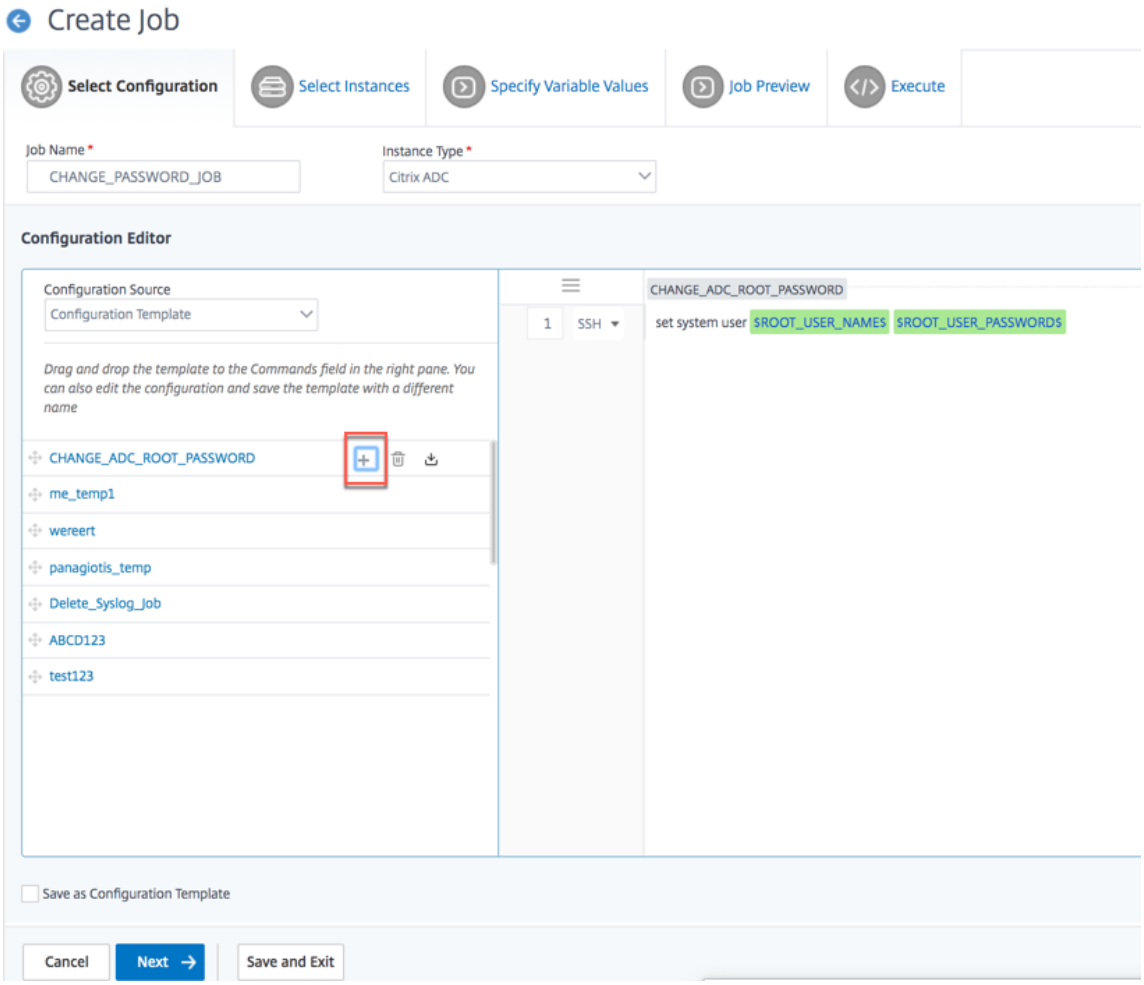


5. Sélectionnez la variable $ROOT_USER_PASSWORD$ et sélectionnez **Champ de mot de passe comme Type**. Sélectionnez **Terminé** pour enregistrer les paramètres de la variable.
6. Sélectionnez **OK** pour enregistrer le modèle de configuration.
7. Le nouveau modèle de configuration apparaît sous **Modèles de configuration**.

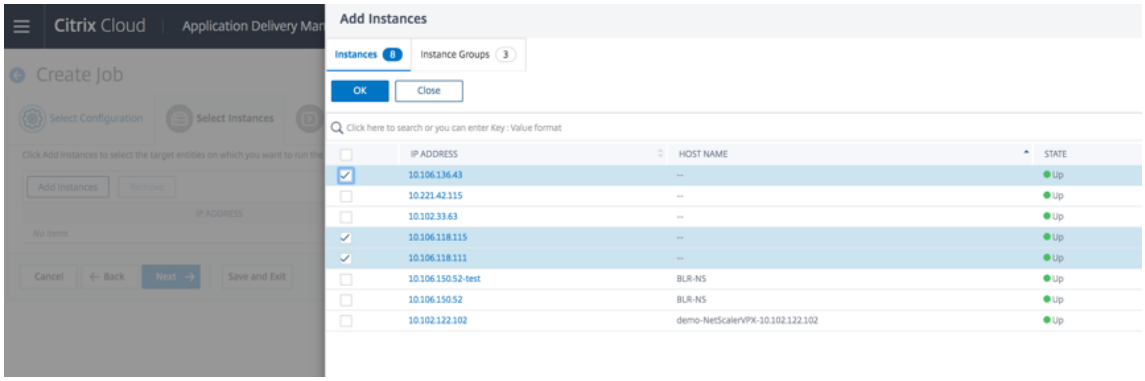


Créer une tâche de configuration

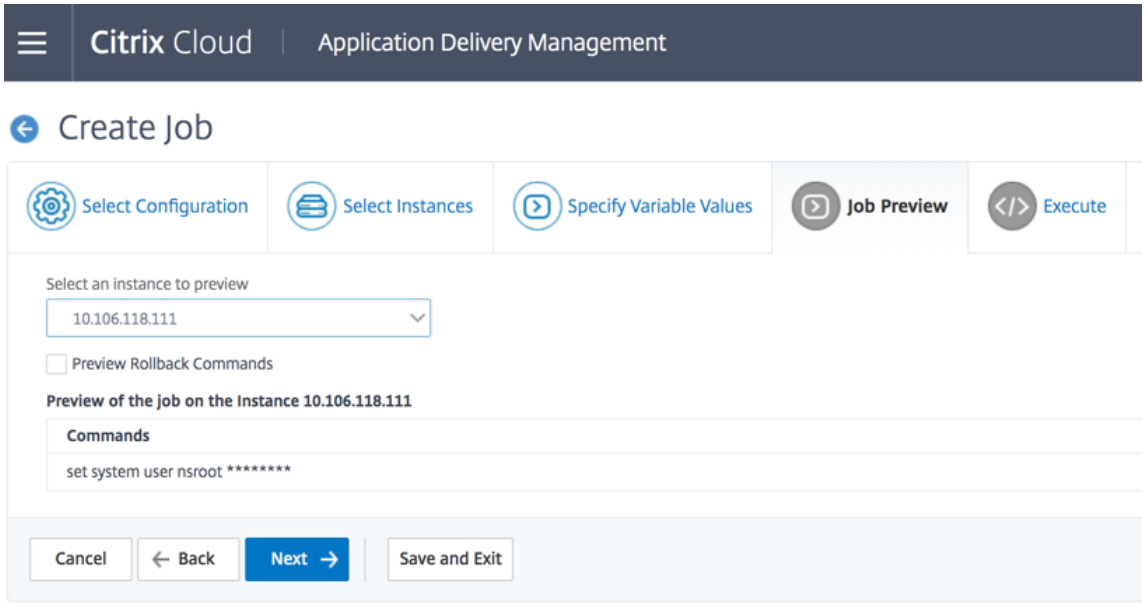
1. À partir de l'interface graphique ADM, accédez à **Réseaux > Travaux de configuration**.
2. Sélectionnez **Créer un travail** et cliquez sur l'icône « + » du nouveau modèle de configuration. Sélectionnez **Next**.



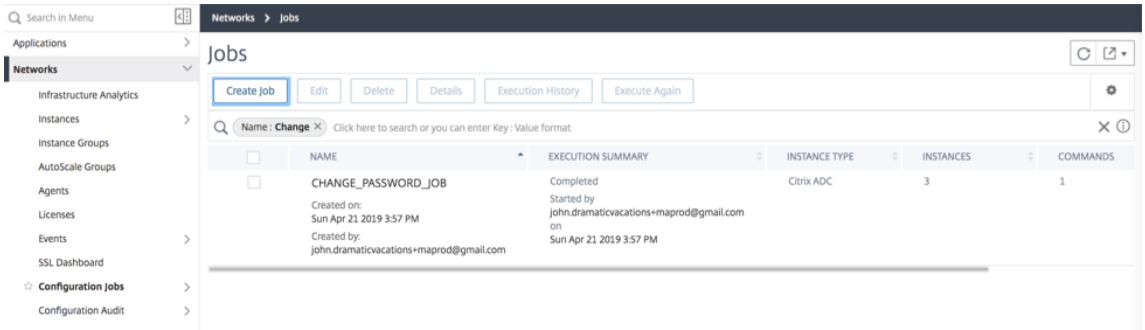
3. Sélectionnez la ou les instances ADC pour lesquelles le mot de passe doit être modifié.



4. Dans le volet **Sélectionner des instances**, sélectionnez les instances, puis cliquez sur **Suivant**.
5. Dans le volet **Spécifier les valeurs de variable**, indiquez des valeurs pour le nom d'utilisateur et le mot de passe, puis cliquez sur **Suivant**.
6. Sous **Aperçu des tâches**, vérifiez les commandes CLI réelles que l'ADM exécutera sur les instances ADC. Si l'aperçu semble correct, cliquez sur **Suivant**.



7. Dans le volet **Exécuter**, vous avez la possibilité d'exécuter le travail immédiatement ou de le programmer ultérieurement. Vous pouvez également choisir d'exécuter le travail en parallèle sur toutes les instances sélectionnées ou de le faire séquentiellement. Sélectionnez Terminer après avoir fourni les détails de l'exécution.
8. La tâche de configuration indique si l'exécution a réussi ou échoué.

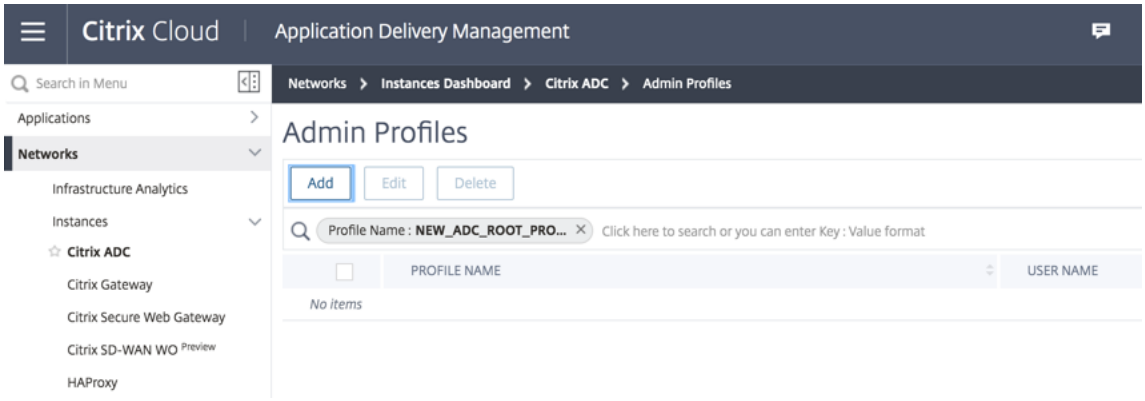


9. Sélectionnez le **travail** et cliquez sur **Détails** . Les détails de l'exécution indiquent l'état au niveau de l'instance individuelle.

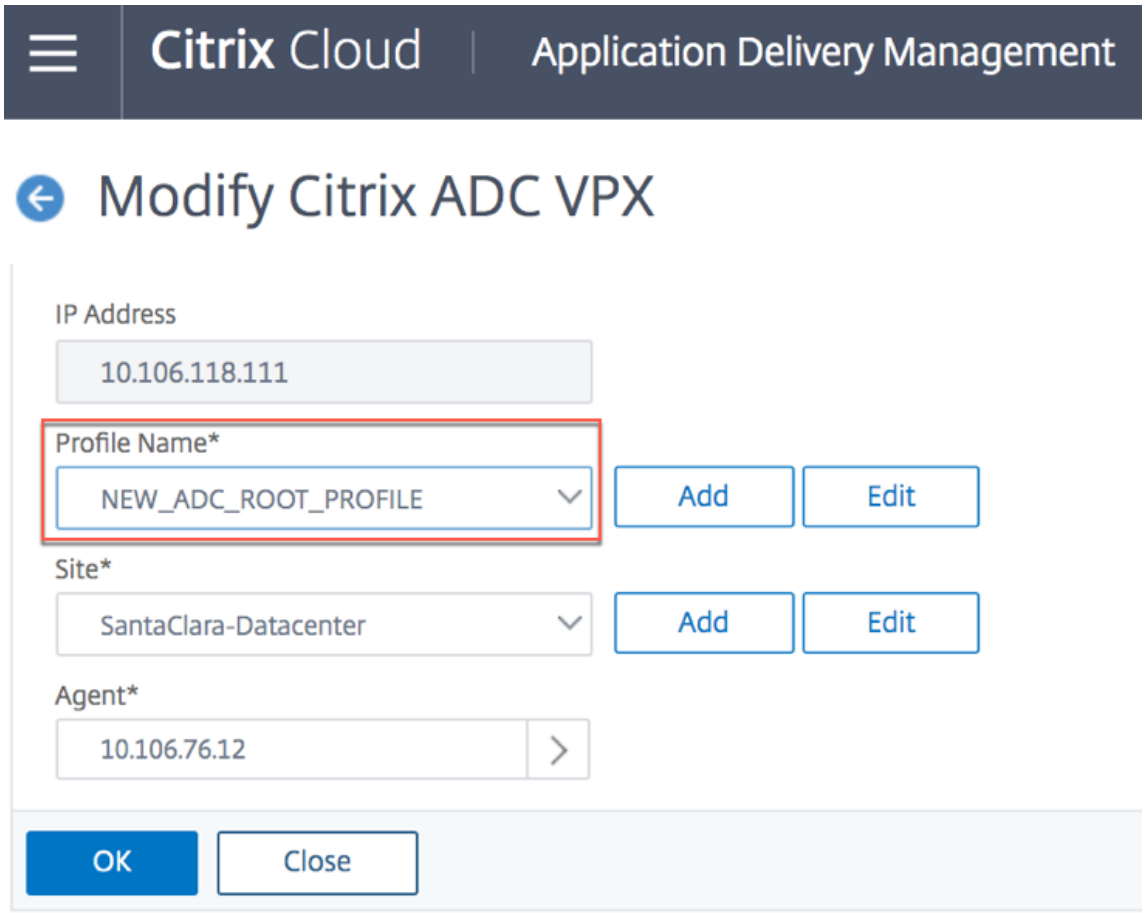
Modifier le profil admin

Après avoir modifié les mots de passe ADC, vous devez ajouter et modifier les profils d'administration des instances. Suivez ces étapes :

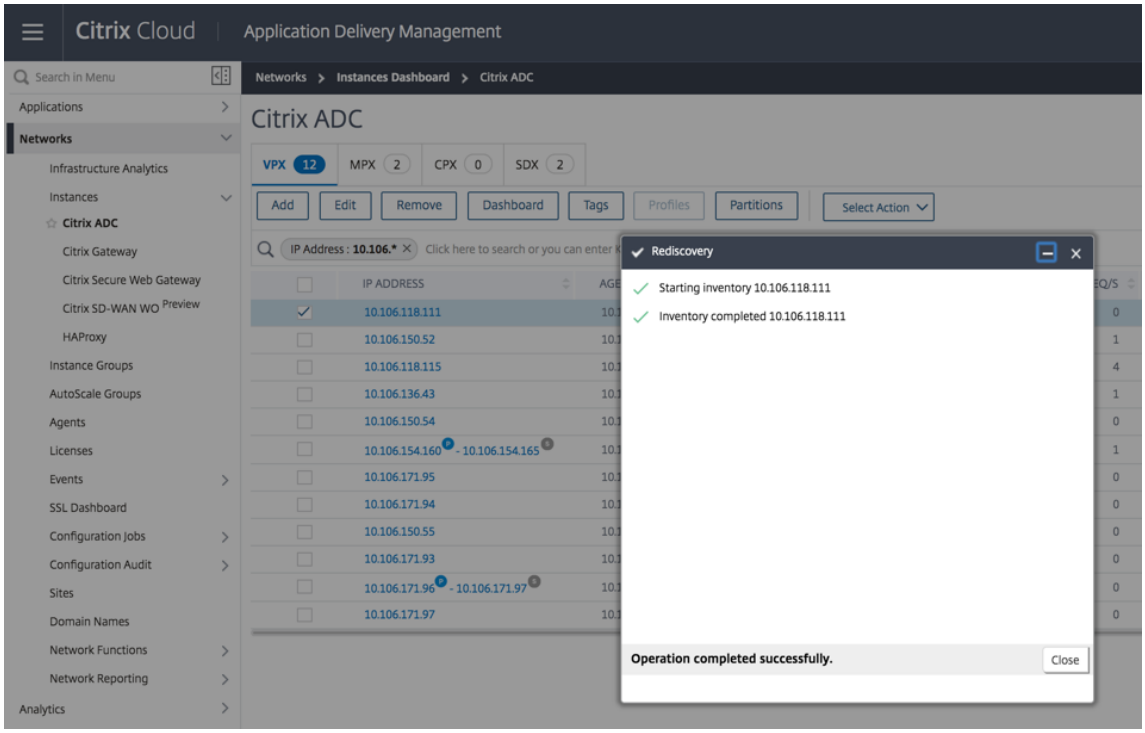
1. Accédez à **Réseaux > Instances > Citrix ADC**.
2. Cliquez sur **Profils** pour afficher tous les profils d'administration.
3. Sélectionnez **Ajouter** pour créer un profil d'administrateur et fournir de nouvelles informations d'identification Citrix ADC.



4. Le profil nouvellement créé apparaît sous **Profils d'administration**.
5. Accédez à **Réseau > Instances > Citrix ADC**. Sélectionnez l'instance Citrix ADC pour laquelle le mot de passe a été modifié, puis sélectionnez **Modifier**.
6. Sélectionnez le nom de profil nouvellement créé et cliquez sur **OK**.



7. Sélectionnez à nouveau l'instance, cliquez avec le bouton droit de la souris, puis sélectionnez **Redécouvrir**.



Vous avez correctement modifié le mot de passe.

Pour plus d'informations sur la modification du mot de passe d'une appliance SDX, reportez-vous à la section Comment modifier un mot de passe racine Citrix ADC SDX.

Comment modifier un mot de passe racine Citrix ADC SDX

April 29, 2021

Parfois, vous devez modifier le mot de passe racine de l'appliance Citrix ADC pour des raisons de sécurité ou de conformité de la stratégie de rotation des mots de passe.

Ce document décrit les étapes requises pour modifier le mot de passe racine d'une appliance Citrix ADC SDX gérée via le cloud Citrix ADM.

Si vous modifiez le mot de passe ADC, vous devez modifier le profil d'administration ADM associé au ADC. Un profil d'administrateur ADM conserve les informations d'identification ADC pour les communications basées sur l'API REST, SSH, SCP ou SNMP avec l'appliance ADC. Grâce aux profils d'administration, Citrix ADM gère les appliances Citrix ADC SDX.

Modifier le mot de passe

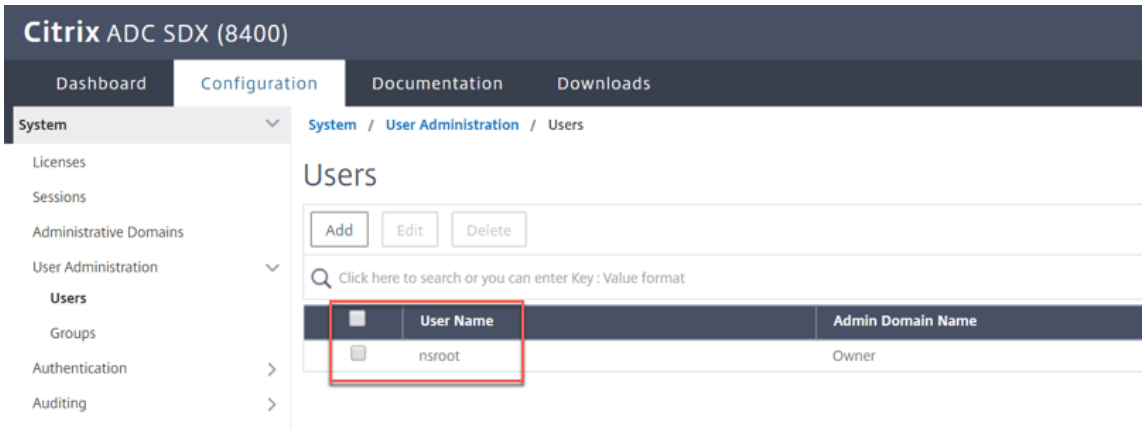
Pour modifier le mot de passe, procédez comme suit :

- Étape 1. Modifiez le mot de passe SDX à partir de l'interface graphique SDX Management Service.
- Étape 2. Modifiez le profil d'administration ADM associé au SDX.

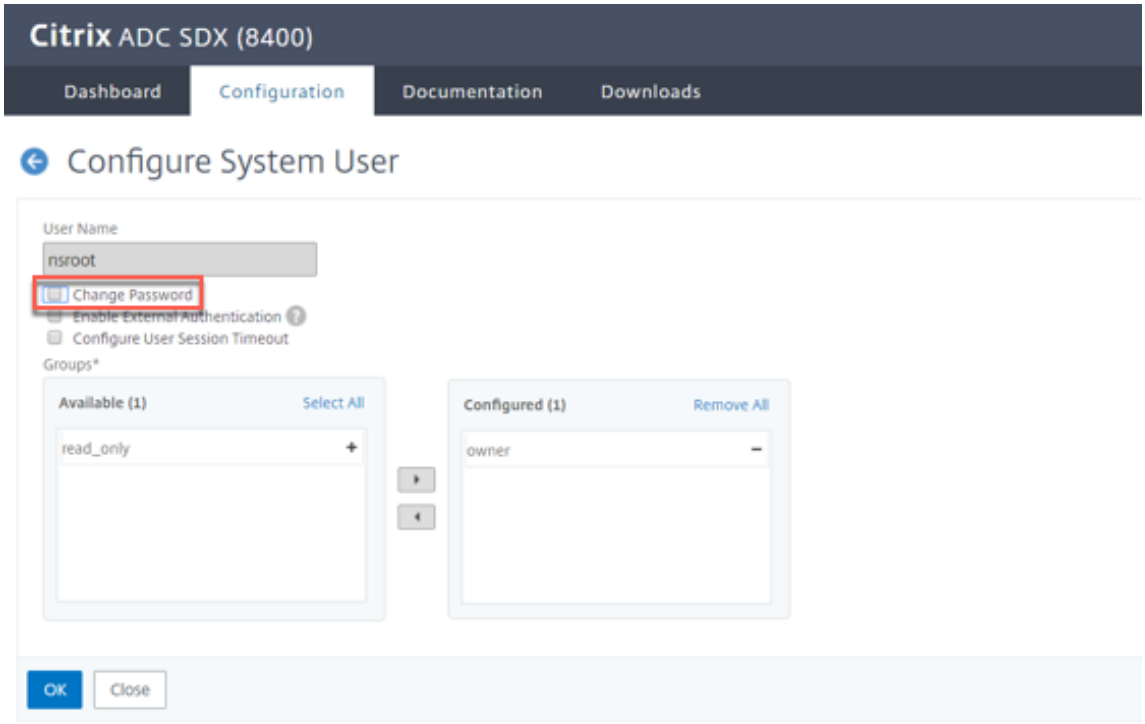
> Remarque : si l'appliance SDX est également gérée par d'autres outils, vous devez également modifier les informations d'identification de ces outils.

Modifier le mot de passe SDX à partir de l'interface graphique SDX Management Service

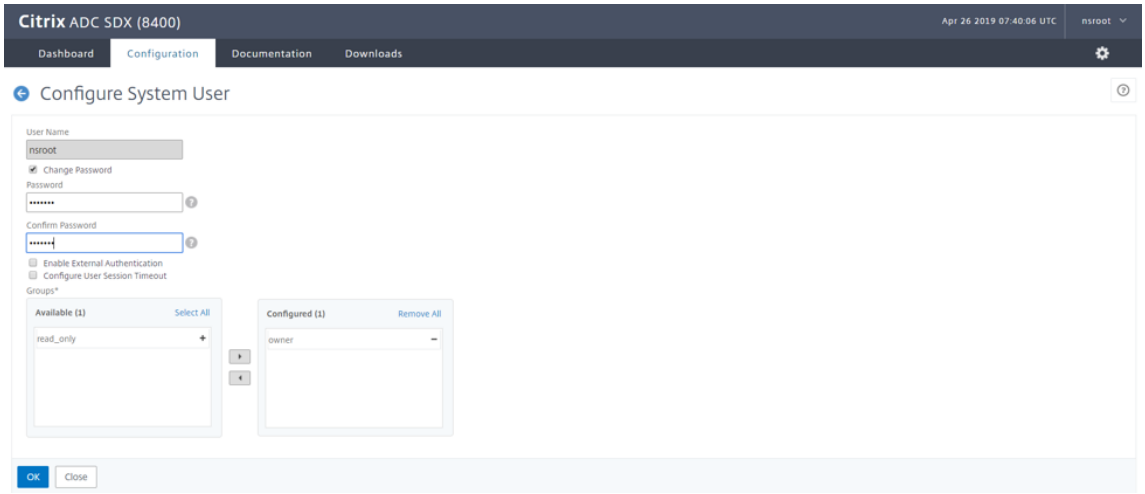
1. Dans SDX Management Service, accédez à **Système > Administration des utilisateurs > Utilisateurs**.
2. Sélectionnez le nom d'utilisateur pour lequel vous souhaitez modifier le mot de passe et cliquez sur **Modifier**.



3. Sélectionnez **Modifier le mot de passe**.



4. Entrez un nouveau mot de passe et cliquez sur **OK**.

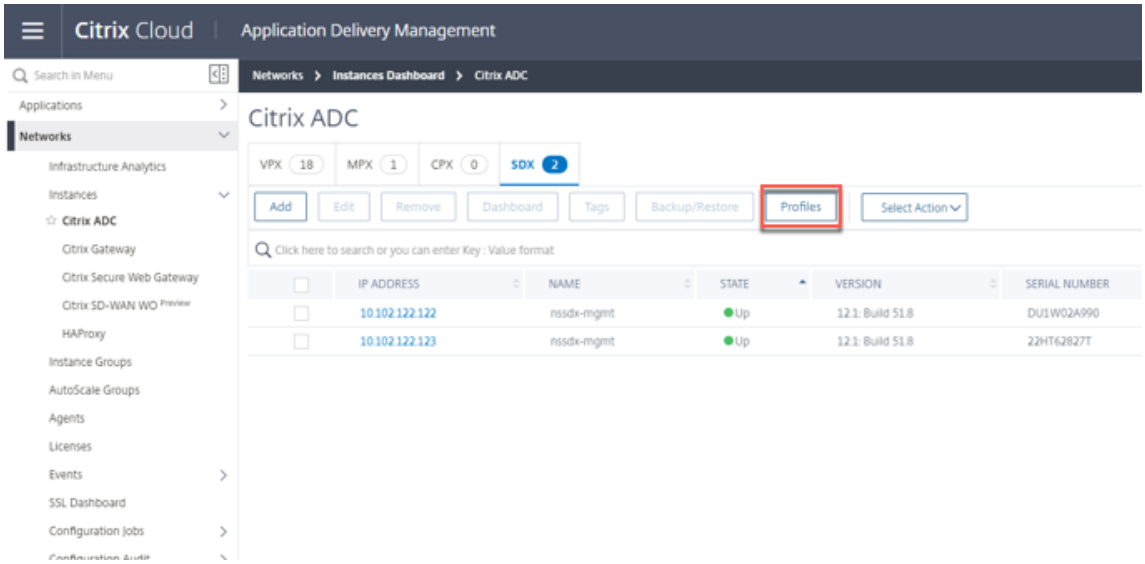


5. Le mot de passe SDX a été modifié

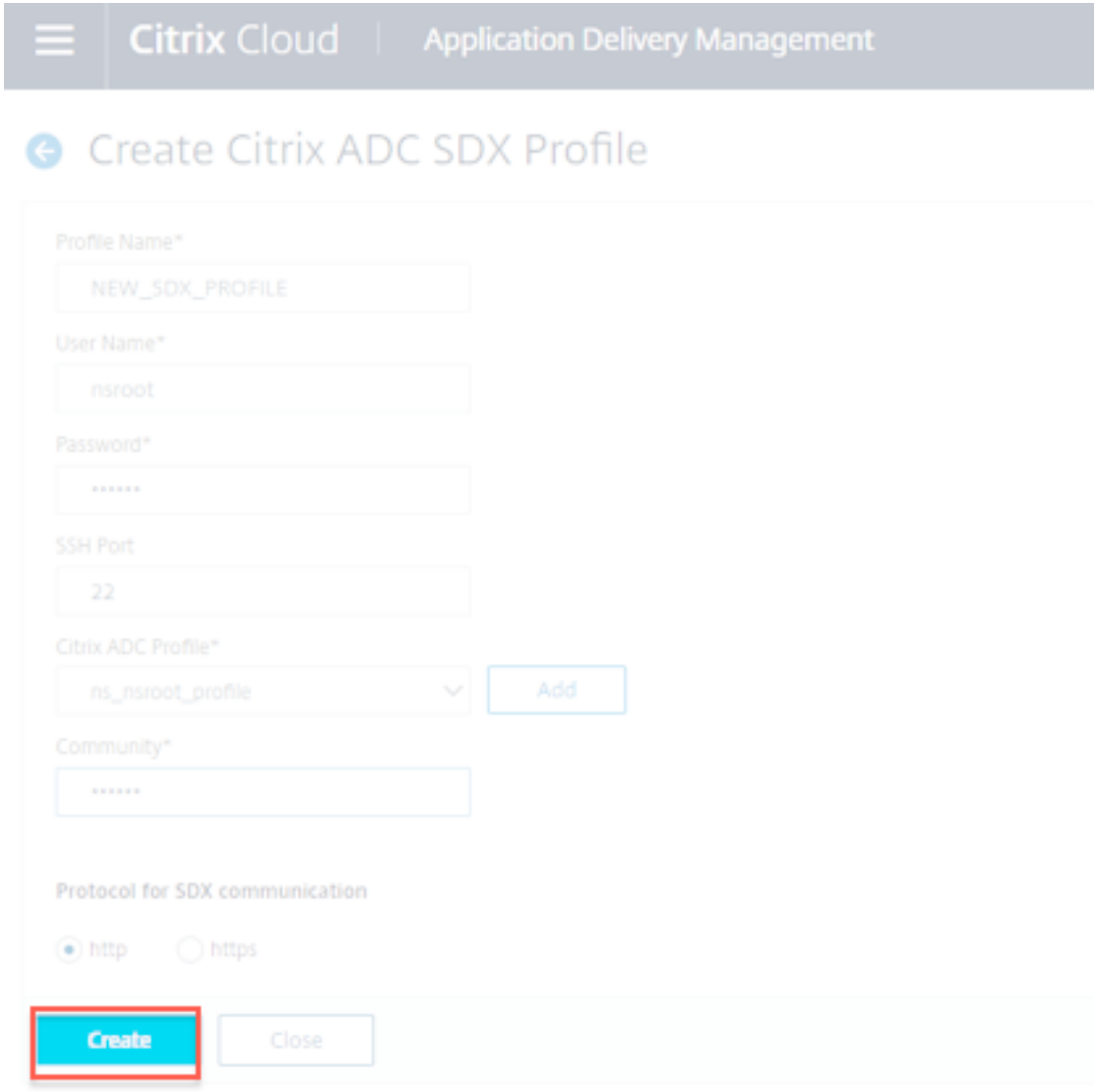
Modifier le profil d'administration ADM

Après avoir modifié les mots de passe SDX, vous devez modifier les profils d'administration des instances. Suivez ces étapes :

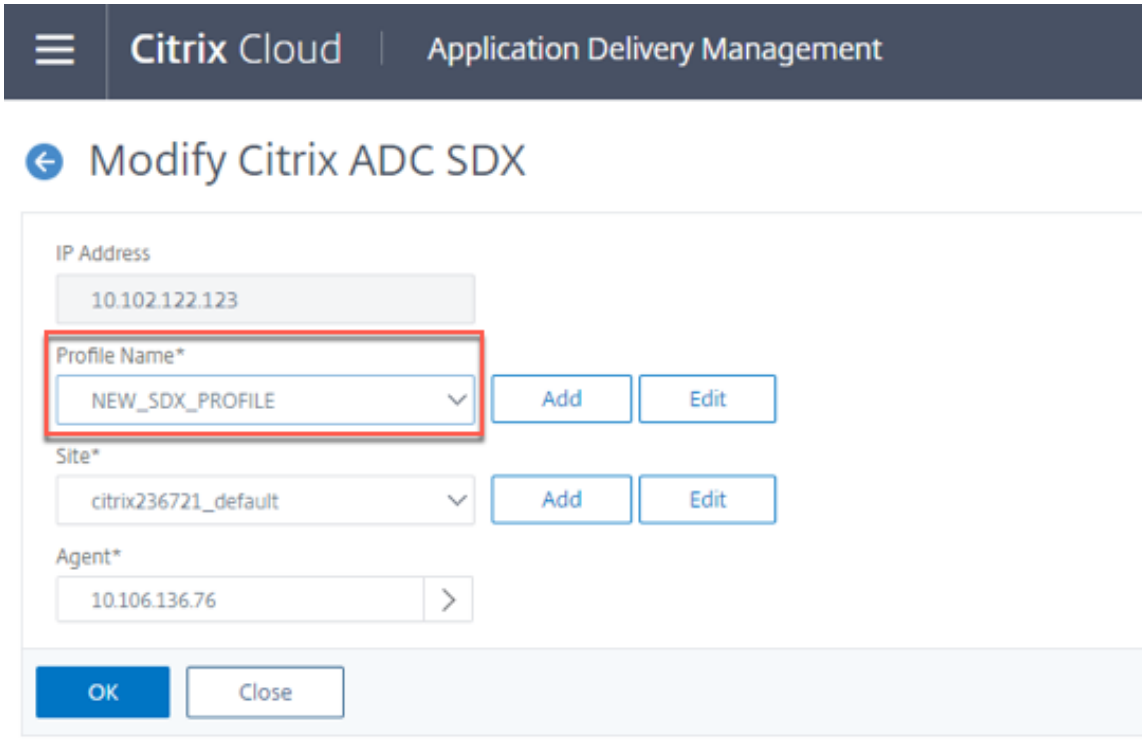
1. Accédez à **Réseaux > Tableau de bord des instances > Citrix ADC > SDX**.
2. Sélectionnez **Profils** pour afficher tous les profils d'administration.



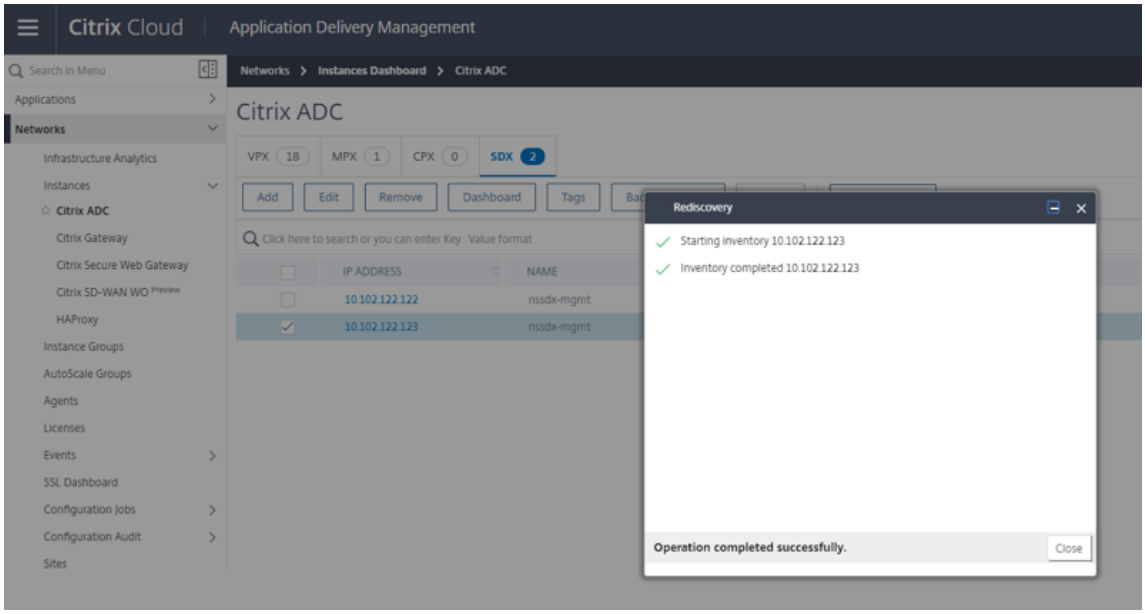
3. Sélectionnez **Ajouter** pour créer un profil d'administrateur.
4. Fournissez de nouvelles informations d'identification Citrix ADC, puis cliquez sur **Créer**.



5. Le profil nouvellement créé apparaît sous **Profils d'administration**.
6. Accédez à **Réseau > Instances > Citrix ADC > SDX**. Sélectionnez l'instance pour laquelle le mot de passe a été modifié, puis sélectionnez **Modifier**.
7. Sélectionnez le nom du profil nouvellement créé et cliquez sur **OK**.



8. Sélectionnez à nouveau l'instance, cliquez avec le bouton droit, cliquez sur **Redécouvrir**.



Vous avez correctement modifié le mot de passe.

Pour plus d'informations sur la modification du mot de passe d'une appliance SDX, reportez-vous à la section Comment modifier un mot de passe racine Citrix ADC MPX ou VPX.

Événements

April 29, 2021

Lorsque l'adresse IP d'une instance Citrix Application Delivery Controller (Citrix ADC) est ajoutée à Citrix Application Delivery Management (Citrix ADM), Citrix ADM envoie un appel NITRO et s'ajoute implicitement comme destination d'interruption pour que l'instance reçoive ses interruptions ou événements.

Les événements représentent des occurrences d'événements ou d'erreurs sur une instance Citrix ADC gérée. Par exemple, en cas de défaillance du système ou de modification de la configuration, un événement est généré et enregistré sur le serveur Citrix ADM. Les événements reçus dans Citrix ADM sont affichés 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, les défaillances du système peuvent être classées comme une gravité d'événement « critique » et peuvent être corrigées immédiatement.

Vous pouvez configurer des règles pour surveiller des événements spécifiques. Les règles facilitent la surveillance des différents 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. Par mesure supplémentaire, vous pouvez personnaliser votre e-mail avec une ligne d'objet spécifique, un message utilisateur et télécharger une pièce jointe.

Utiliser le tableau de bord des événements

April 29, 2021

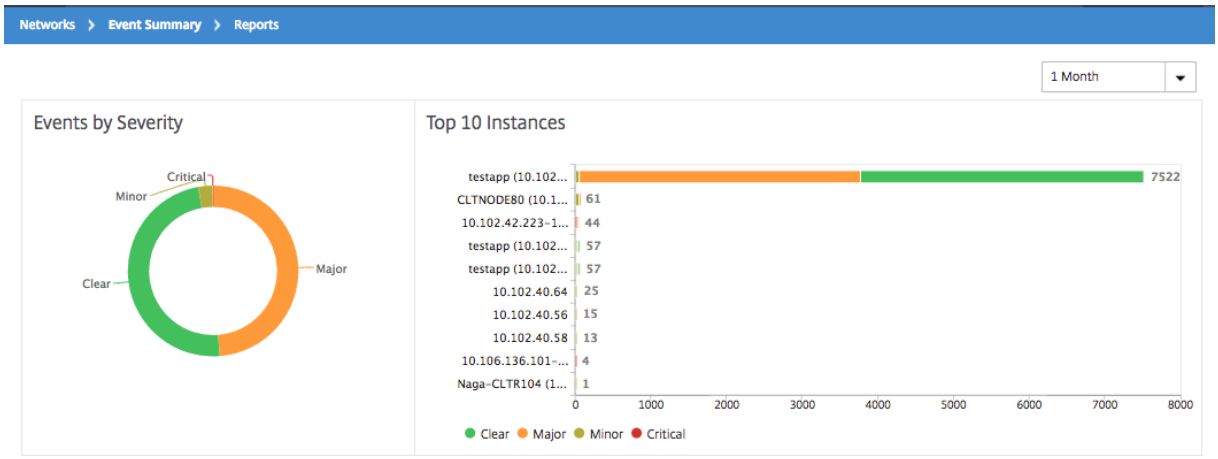
En tant qu'administrateur réseau, vous pouvez afficher des détails tels que les modifications de configuration, les conditions de connexion, les défaillances matérielles, les violations de seuil et les modifications d'état d'entité sur vos instances Citrix Application Delivery Controller (Citrix ADC), 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 (Citrix ADM) pour afficher les rapports générés pour les détails de gravité des événements critiques sur toutes vos instances Citrix ADC.

Pour afficher les détails du tableau de bord des événements :

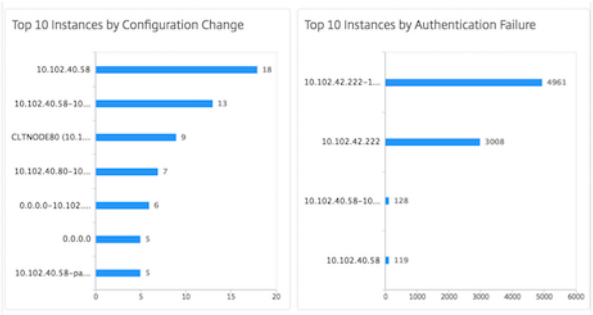
Accédez à **Réseaux** > **Événements** > **Rapports**.

Le graphique 10 principaux périphériques du tableau de bord affiche un rapport des 10 instances les plus importantes selon le nombre d'événements générés sur elles. Vous pouvez cliquer sur une instance sur le graphique pour afficher plus de détails sur la gravité de l'événement.

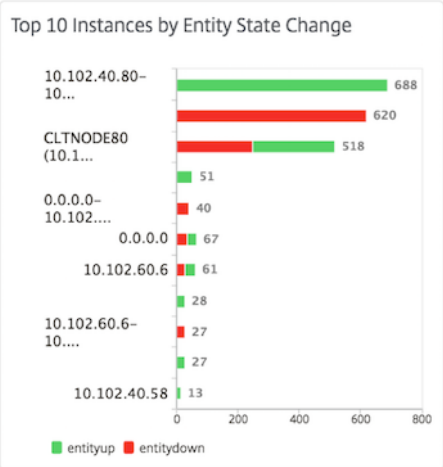


Vous pouvez afficher plus de détails en accédant au type d'instance Citrix ADC (**Réseaux** > **Événements** > **Rapports** > **Citrix ADC/Citrix ADC SDX/ Citrix ADC SD-WAN WO**) pour afficher les éléments suivants :

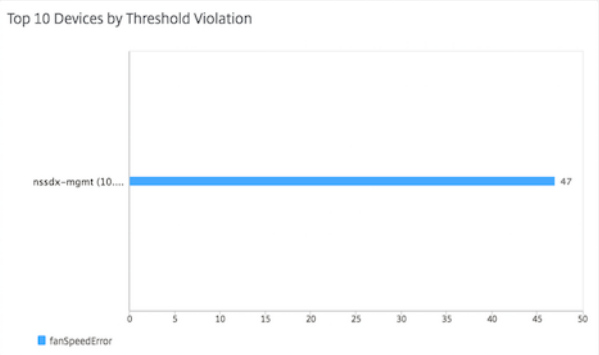
- Les 10 principaux périphériques par défaillance matérielle
- Les 10 principaux périphériques par changement de configuration
- Top 10 des appareils par échec d'authentification



- Top 10 des périphériques par modification de l'état de l'entité



- Top 10 des appareils par violation de seuil



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 quotidiennement, hebdomadaire ou mensuel et envoyer le rapport par e-mail ou par un message de marge.

> **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.

Définir l'âge de l'événement pour les événements

April 29, 2021

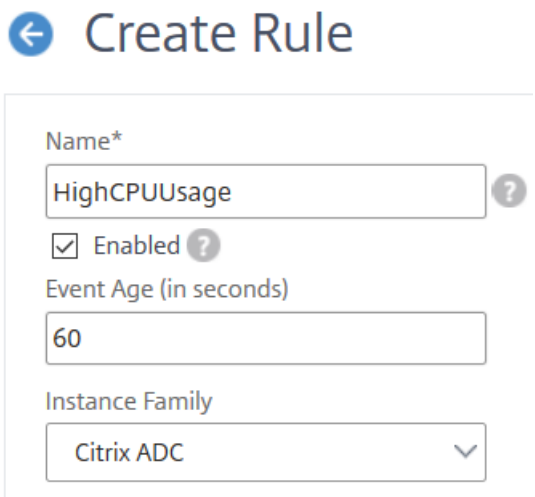
Vous pouvez définir l'option âge de l'événement pour spécifier l'intervalle de temps (en secondes). Citrix ADM surveille les appliances jusqu'à la durée définie et génère un événement uniquement si l'âge de l'événement dépasse la durée définie.

> Remarque :
>
> La valeur minimale pour l'âge de l'événement est de 60 secondes. Si vous conservez le champ **Âge** de l'événement vide, la règle d'événement est appliquée immédiatement après l'événement.

Par exemple, considérez que vous souhaitez gérer diverses appliances ADC et être averti par e-mail lorsque l'un de vos serveurs virtuels tombe en panne pendant 60 secondes ou plus. Vous pouvez créer une règle d'événement avec les filtres nécessaires et définir l'âge d'événement de la règle sur 60 secondes. Ensuite, chaque fois qu'un serveur virtuel reste en panne pendant 60 secondes ou plus, vous recevez une notification par e-mail contenant des détails tels que le nom de l'entité, le changement d'état et l'heure.

Pour définir l'âge des événements dans Citrix ADM :

1. Dans Citrix ADM, accédez à **Réseaux** > **Événements** > **Règles**, puis cliquez sur **Ajouter** .
2. Dans la page **Créer une règle**, définissez les paramètres de la règle.
3. Spécifiez l'âge de l'événement en secondes.



Planifier un filtre d'événement

April 29, 2021

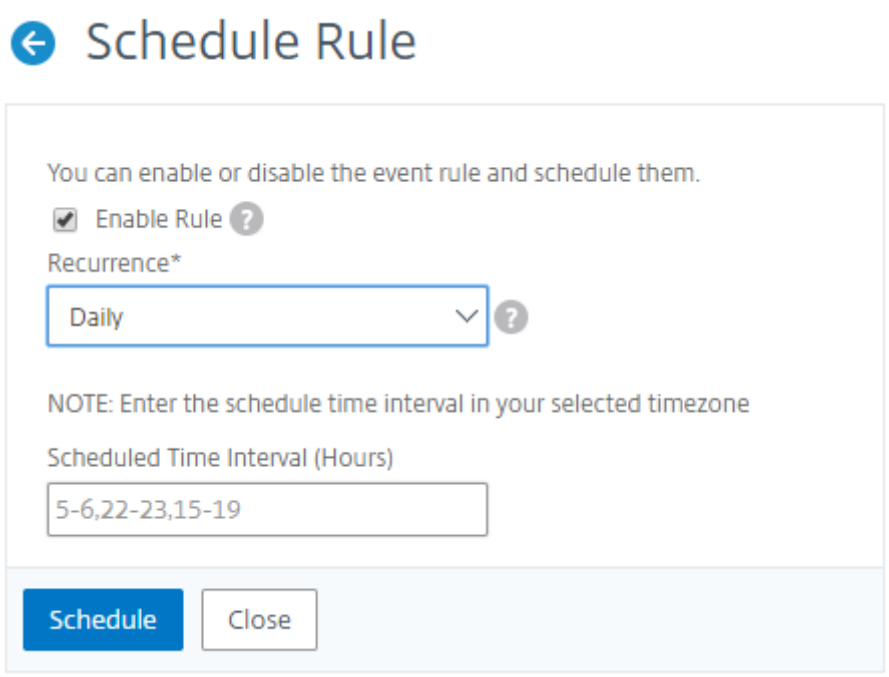
Après avoir créé un filtre pour votre règle, si vous ne souhaitez pas que Citrix Application Delivery Management (Citrix ADM) envoie une notification chaque fois que l'événement généré satisfait aux critères de filtre, vous pouvez programmer le déclenchement du filtre uniquement à des intervalles de 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 de nombreuses notifications par e-mail lorsque Citrix ADM reçoit ces interruptions. Si vous souhaitez que le serveur envoie ces notifications par e-mail uniquement pendant une période spécifique, vous pouvez le faire en planifiant un filtre.

Pour planifier un filtre à l'aide de Citrix ADM :

1. Dans Citrix ADM, accédez à **Réseaux** > **Événements** > **Règles** .
2. Sélectionnez la règle pour laquelle vous souhaitez planifier un filtre, puis cliquez sur **Afficher la planification**.
3. Dans la page **Règle programmée**, cliquez sur **Planifier** et spécifiez les paramètres suivants :
    - **Activer la règle** — Activez cette case à cocher pour activer la règle d'événement planifié.
    - **Récurrence** : intervalle auquel planifier la règle.
    - **Intervalle de temps planifié (heures)** — Heures auxquelles programmer la règle (utilisez le format 24 heures).
4. Cliquez sur **Planifier**.



Définir des notifications par e-mail répétées pour les événements

April 29, 2021

Pour vous assurer que tous les événements critiques sont adressés 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'événement qui répondent aux critères que vous avez sélectionnés. Par exemple, si vous avez créé une règle d'événement pour les instances impliquant 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 courrier électronique répétées concernant ces événements.

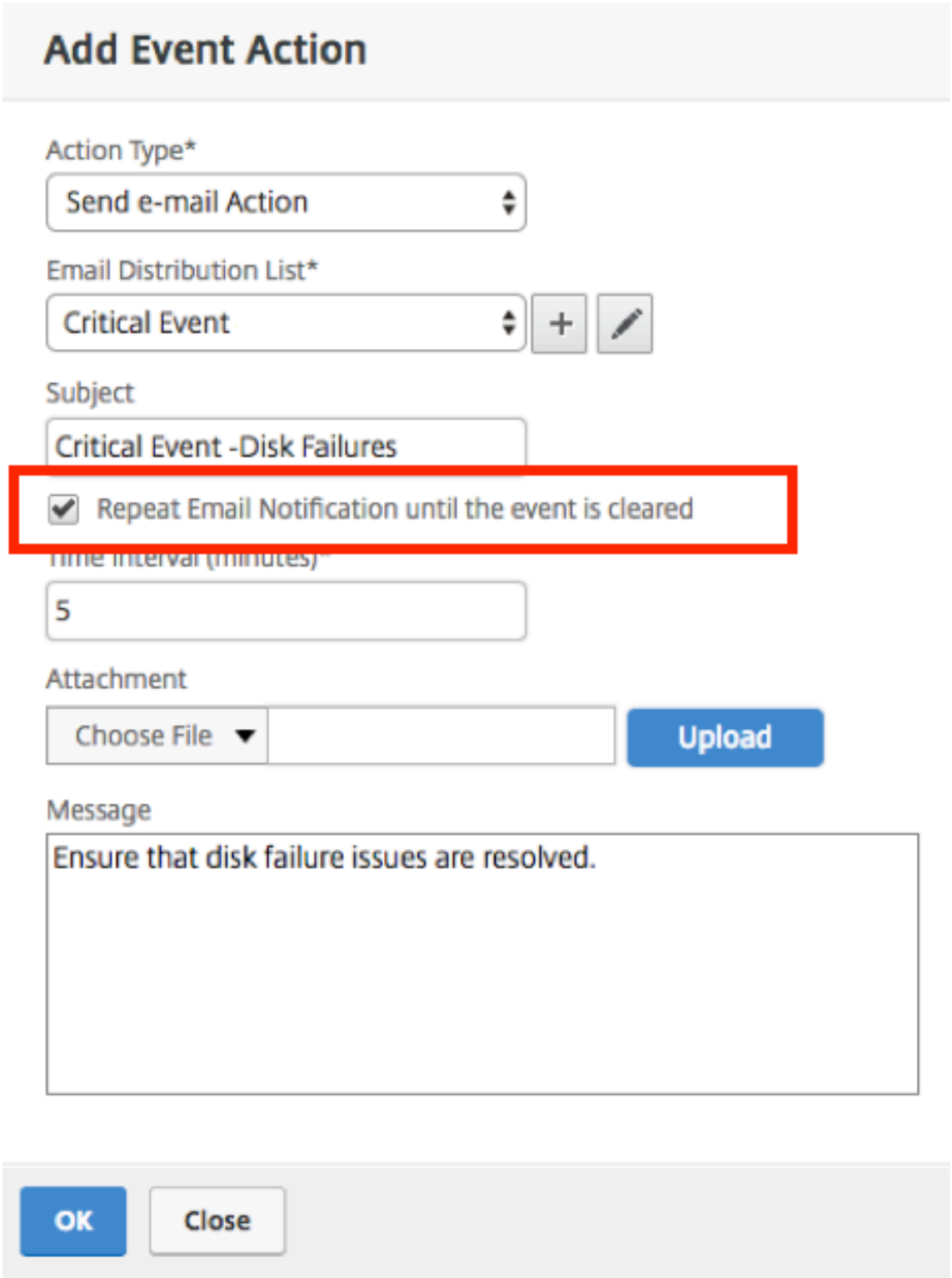
Ces notifications par e-mail sont envoyées à plusieurs reprises, à des intervalles prédéfinis, jusqu'à ce que le destinataire reconnaisse avoir vu la notification ou que la règle d'événement soit effacée.

> **Remarque**
>
> Les événements ne peuvent être effacés automatiquement que s'il existe un jeu d'interruptions « effacer » équivalent et envoyé à partir de votre instance de Citrix ADC.
>
> Pour effacer manuellement un événement, vous pouvez effectuer les opérations suivantes :
>
> - Accédez à **Réseaux > Événements > Résumé**des événements, sélectionnez **Catégorie**, puis 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 suivante, puis cliquez sur **Effacer**.

Pour définir des notifications par e-mail répétées à partir de Citrix ADM :

1. Dans Citrix ADM, accédez à **Réseaux** > **Événements** > **Règles**, puis cliquez sur **Ajouter** pour créer une règle.
2. Dans la page **Créer une règle**, définissez les paramètres de la règle.
3. Sous Actions de **règle d'événement**, cliquez sur **Ajouter une action** . Ensuite, sélectionnez **Envoyer une action de courrier électronique** dans la liste déroulante **Type d'action** et sélectionnez une liste de **distribution de courrier électronique** .
4. Vous pouvez également ajouter une ligne d'objet personnalisée et un message utilisateur, et charger une pièce jointe dans 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**.



Supprimer les événements

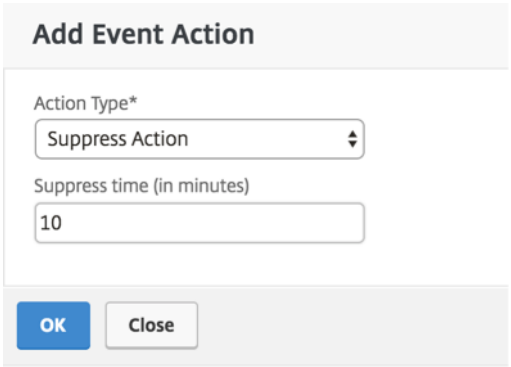
April 29, 2021

Lorsque vous choisissez l' **action d'événement Supprimer** l'action, vous pouvez configurer une période, en minutes, pour laquelle un événement est supprimé ou supprimé. Vous pouvez supprimer l'événement pendant au moins 1 minute.

> Remarque :
>
> Vous pouvez également configurer le temps de suppression comme 0 minutes et cela signifie temps infini. Si vous ne spécifiez aucune durée de temps, Citrix ADM considère l'heure de suppression comme zéro et n'expire jamais.

Pour supprimer des événements à l'aide de Citrix ADM :

1. Dans Citrix ADM, accédez à **Réseaux** > **Événements** > **Règles** .
2. Accédez à la page **Créer une règle** ou **Configurer une règle** . Spécifiez tous les paramètres nécessaires à la création d'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, pendant laquelle un événement doit être supprimé.
5. Cliquez sur **OK**.



Créer des règles d'événement

April 29, 2021

Vous pouvez configurer des règles pour surveiller des événements spécifiques. Les règles facilitent le filtrage des événements générés dans votre infrastructure.

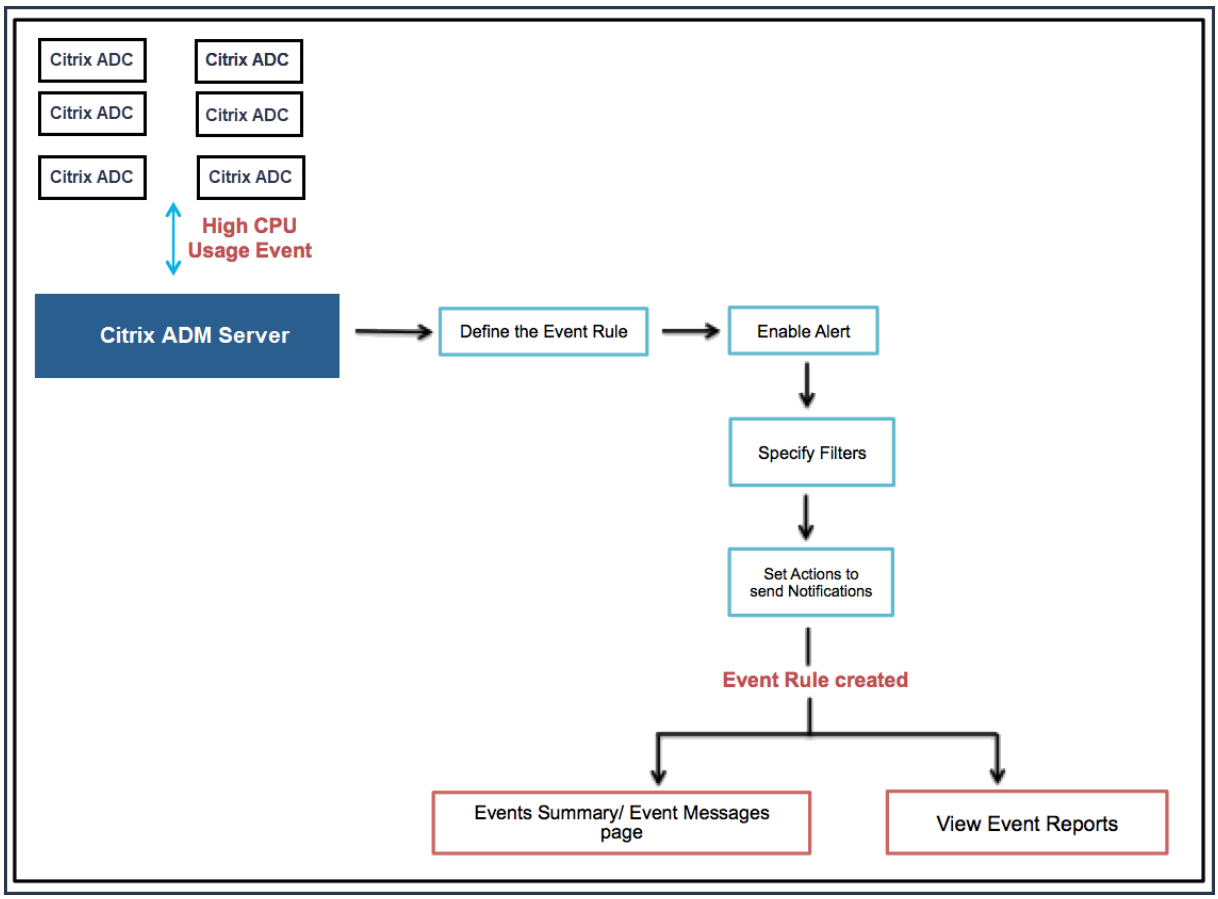
Vous pouvez filtrer un ensemble d'événements en configurant des règles avec des conditions spécifiques et en affectant des actions aux règles. Lorsque les événements générés répondent aux critères de filtre de la règle, l'action associée à la règle est exécutée. Les conditions pour lesquelles vous pouvez créer des filtres sont : gravité, instances Citrix Application Delivery Controller (Citrix ADC), catégorie, objets de défaillance, commandes de configuration et messages.

Vous pouvez affecter les actions suivantes aux événements :

- **Envoyer une action e-mail** : Envoyer un e-mail pour les événements qui correspondent aux critères de filtre.
- **Envoyer une action d'interruption** : envoyer ou transférer des interruptions SNMP vers une destination d'interruption externe
- **Exécuter l'action**de la commande : Exécutez une commande lorsqu'un événement entrant répond à la règle configurée.
- **Exécuter une action de travail** : Exécuter une tâche concerne les événements qui correspondent aux critères de filtre que vous avez spécifiés.
- **Supprimer l'action** : supprime supprimer un événement pour une période spécifique.
- **Envoyer des notifications Slack** : Envoie des notifications sur le canal Slack configuré pour les événements qui correspondent aux critères de filtre.
- **Envoyer des notifications PagerDuty** : Envoyer des notifications d'événements basées sur les configurations PagerDuty pour les événements qui correspondent aux critères de filtre.
- **Envoyer des notifications ServiceNow** : générer automatiquement des incidents ServiceNow pour un événement qui correspond aux critères de filtre.

Pour de plus amples informations, consultez la section Ajouter des actions de règle d'événement.

Vous pouvez également faire renvoyer les notifications à un intervalle spécifié jusqu'à ce qu'un événement soit effacé. Et vous pouvez personnaliser l'e-mail avec une ligne d'objet spécifique, un message utilisateur et une pièce jointe.



Par exemple, en tant qu'administrateur, vous pouvez surveiller les événements « utilisation élevée du processeur » sur les instances ADC qui peuvent entraîner une panne. Vous pouvez effectuer l'une des actions suivantes pour recevoir des notifications :

- Créez une règle pour surveiller les instances. Et, ajoutez une action à la règle pour recevoir des notifications lorsque de tels événements se produisent.
- Planifiez une règle pour surveiller les instances à un intervalle spécifique. Ainsi, vous recevez des notifications lorsque de tels événements se produisent dans cet intervalle.

La configuration d'une règle d'événement implique les tâches suivantes :

1. Définir la règle
2. Choisissez la gravité de l'événement détecté par la règle
3. Spécifiez la catégorie de l'événement
4. Spécifier les instances Citrix ADC auxquelles la règle s'applique
5. Sélectionner les objets d'échec
6. Spécifier les filtres avancés
7. Spécifier les actions à effectuer lorsque la règle détecte un événement

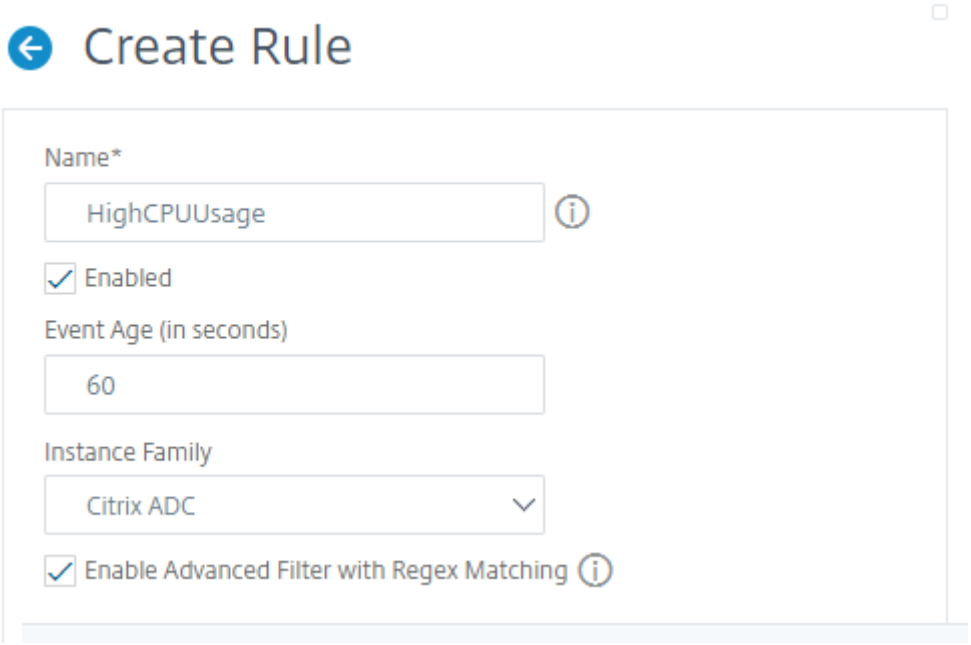
Étape 1 - Définir une règle d'événement

Accédez à **Réseaux** > **Événements** > **Règles**, puis cliquez sur **Ajouter** . Si vous souhaitez activer votre règle, activez la case à cocher **Activer la règle**.

Vous pouvez définir l'option **Age de l'événement** pour spécifier l'intervalle de temps (en secondes) après lequel Citrix ADM actualise une règle d'événement.

> Remarque :
>
> La valeur minimale pour 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 pouvez être averti par e-mail chaque fois que votre instance Citrix ADC a un événement « utilisation élevée du processeur » pendant 60 secondes ou plus. Vous pouvez définir l'âge de l'événement sur 60 secondes, de sorte que chaque fois que votre instance Citrix ADC a un événement « utilisation élevée du processeur » pendant 60 secondes ou plus, vous recevez une notification par e-mail contenant les détails de l'événement.



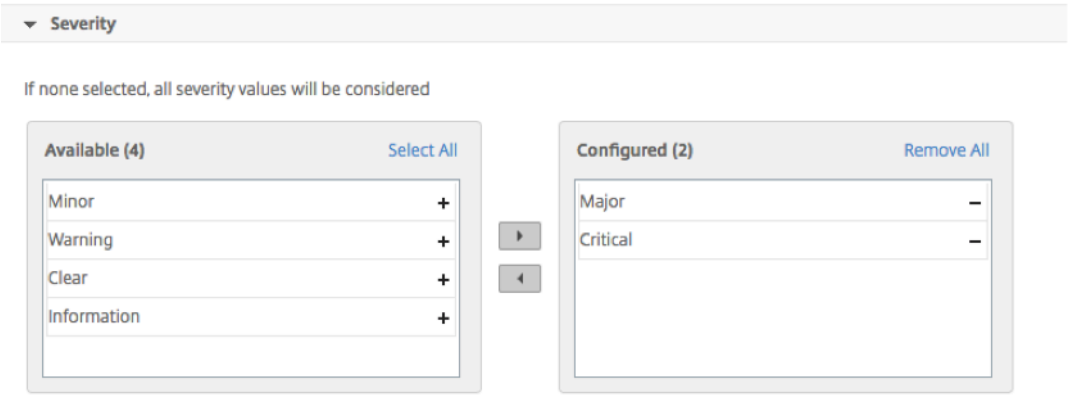
Vous pouvez également filtrer les règles d'événement par **famille d'instances** pour suivre l'instance Citrix ADC à partir de laquelle Citrix ADM reçoit un événement.

Si vous souhaitez inclure une expression régulière autre que la correspondance de motif d'astérisque (*), sélectionnez **Activer le filtre avancé avec la correspondance d'expression régulière**.

Étape 2 - Choisissez la gravité de l'événement

Vous pouvez créer des règles d'événement qui utilisent les paramètres de gravité par défaut. La gravité spécifie la gravité actuelle des événements que vous souhaitez ajouter à la règle d'événement.

Vous pouvez définir les niveaux de gravité suivants : Critique, Majeur, Mineur, Avertissement, Effacer et Informations.

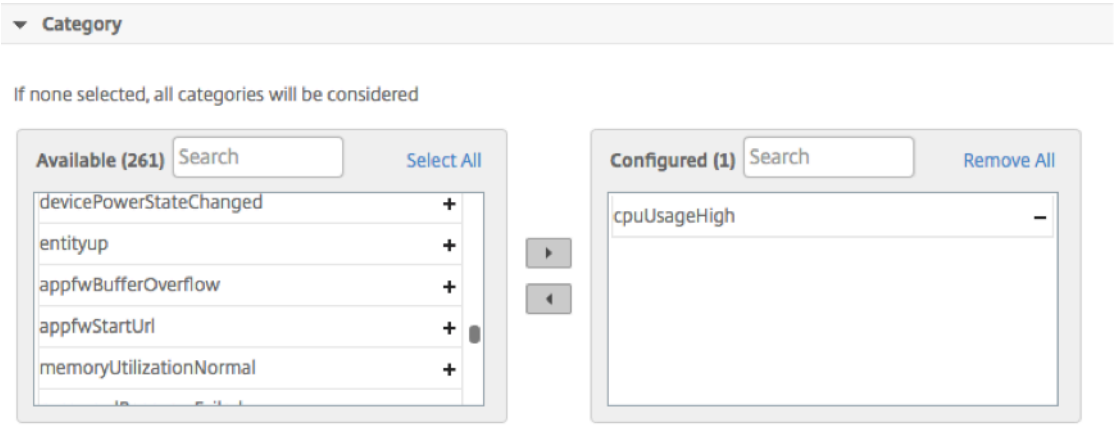


> **Remarque**
>
> Vous pouvez configurer la gravité des événements génériques et spécifiques à Advanced. Pour modifier la gravité des événements pour les instances Citrix ADC gérées sur Citrix ADM, accédez à **Réseaux** > **Événements** > **Paramètres d'événement** . Choisissez la **catégorie** pour laquelle vous souhaitez configurer la gravité de l'événement, puis cliquez sur **Configurer la gravité** . Attribuez un nouveau niveau de gravité et cliquez sur **OK**.

Étape 3 - Spécifiez la catégorie d'événement

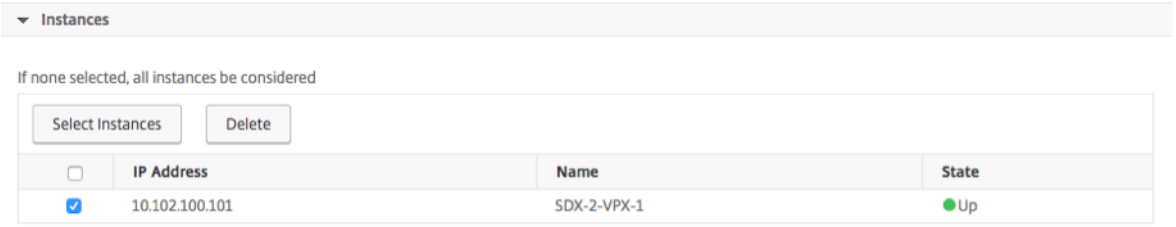
Vous pouvez spécifier la ou les catégories des événements générés par vos instances de Citrix ADC. Toutes les catégories sont créées sur des instances Citrix ADC. Ces catégories sont ensuite mappées avec Citrix ADM qui peut être utilisée pour définir des règles d'événement. Sélectionnez la catégorie à prendre en compte et déplacez-la de la table **Disponible** vers la table **configurée**.

Dans l'exemple ci-dessus, vous devez choisir « CPUUsageHigh » comme catégorie d'événements dans la table affichée.



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 les instances** . Dans la page **Sélectionner des instances**, choisissez vos instances, puis cliquez sur **Sélectionner** .



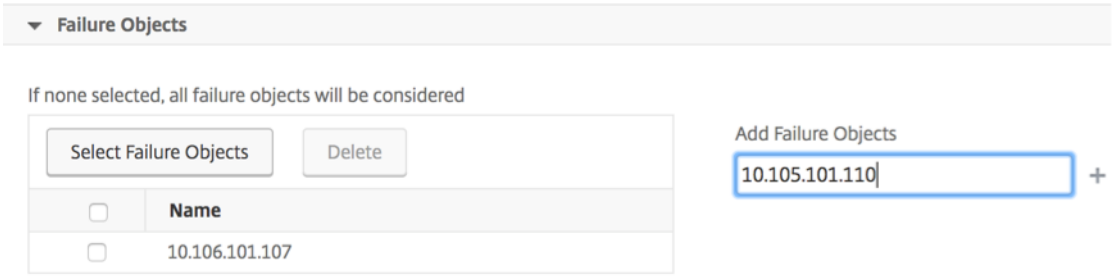
Étape 5 - Sélectionner les objets de défaillance

Vous pouvez sélectionner un objet d'échec dans la liste fournie ou ajouter un objet d'échec pour lequel un événement a été généré. Vous pouvez également spécifier une expression régulière pour ajouter des objets d'échec. En fonction de l'expression régulière spécifiée, les objets d'échec sont automatiquement ajoutés à la liste. Les objets d'échec sont des instances d'entité ou des compteurs pour lesquels un événement a été généré.

> **Important**
>
> Pour répertorier les objets d'échec à l'aide d'une expression régulière, sélectionnez **Activer le filtre avancé avec la correspondance Regex** dans Étape 1.

L'objet d'échec affecte la façon dont un événement est traité et s'assure qu'il reflète exactement le problème tel qu'il a été notifié. Avec ce filtre, vous pouvez suivre rapidement les problèmes sur les objets de défaillance et identifier la cause d'un problème. Par exemple, si un utilisateur a des problèmes de connexion, l'objet d'échec ici est le nom d'utilisateur ou le mot de passe, par exemple `nsroot`.

Cette liste peut contenir des noms de compteur pour tous les événements liés au seuil, des noms d'entité pour tous les événements liés à l'entité, des noms de certificats pour les événements liés au certificat, etc.

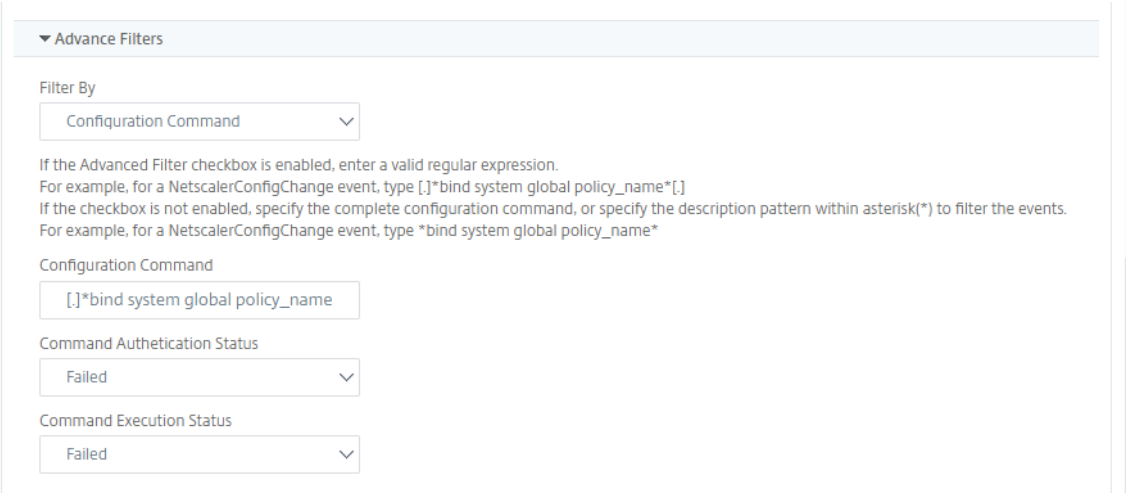


Étape 6 - Spécifier les filtres avancés

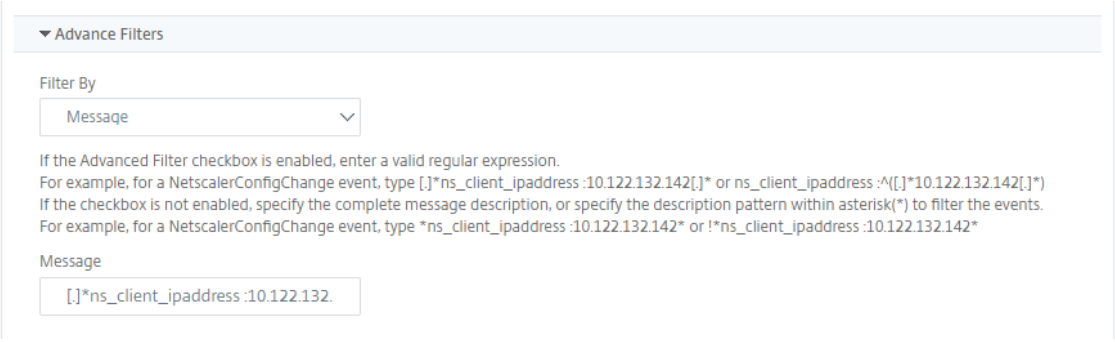
Vous pouvez filtrer davantage une règle d'événement en :

- **Commandes de configuration** : vous pouvez spécifier la commande de configuration complète ou spécifier une expression régulière pour filtrer les événements.

  Vous pouvez également filtrer la règle d'événement en fonction de l'état d'authentification et/de la commande ou de son état d'exécution. Par exemple, pour un `NetscalerConfigChange event`, tapez `[.]*bind system global policy_name[.]*`.



- **Messages** - Vous pouvez spécifier la description complète du message ou spécifier une expression régulière pour filtrer les événements.
  Par exemple, pour un `NetscalerConfigChange` événement, tapez `[.]*ns_client_ipaddress :10.122.132.142[.]* or ns_client_ipaddress :^([.]*10.122.132.142[.]*)`.



> **Important**
>
> Pour filtrer les commandes de configuration et les messages à l'aide d'une expression régulière autre que la correspondance des motifs d'astérisque (*), sélectionnez **Activer le filtre avancé avec correspondance des expressions** régulières dans Étape 1.

Étape 7 - Ajouter des actions de règle d'événement

Vous pouvez ajouter des actions de règle d'événement pour affecter des actions de notification à un événement. Ces notifications sont envoyées ou exécutées lorsqu'un événement répond aux critères de filtre définis ci-dessus. Vous pouvez ajouter les actions d'événement suivantes :

- Envoyer un e-mail Action
- Envoyer une action de recouvrement
- Exécuter l'action de commande
- Exécuter une action de travail
- Supprimer l'action
- Envoyer des notifications Slack
- Envoyer des notifications PagerDuty
- Envoyer des notifications ServiceNow

Pour définir une action de règle d'événement de messagerie électronique

Lorsque vous choisissez **Envoyer une action de messagerie électronique**, un e-mail est déclenché lorsque les événements répondent aux critères de filtre définis. Vous devez soit créer une liste de distribution de courrier électronique en fournissant des détails sur le serveur de messagerie ou le profil de messagerie, soit vous pouvez sélectionner une liste de distribution de messagerie que vous avez précédemment créée.

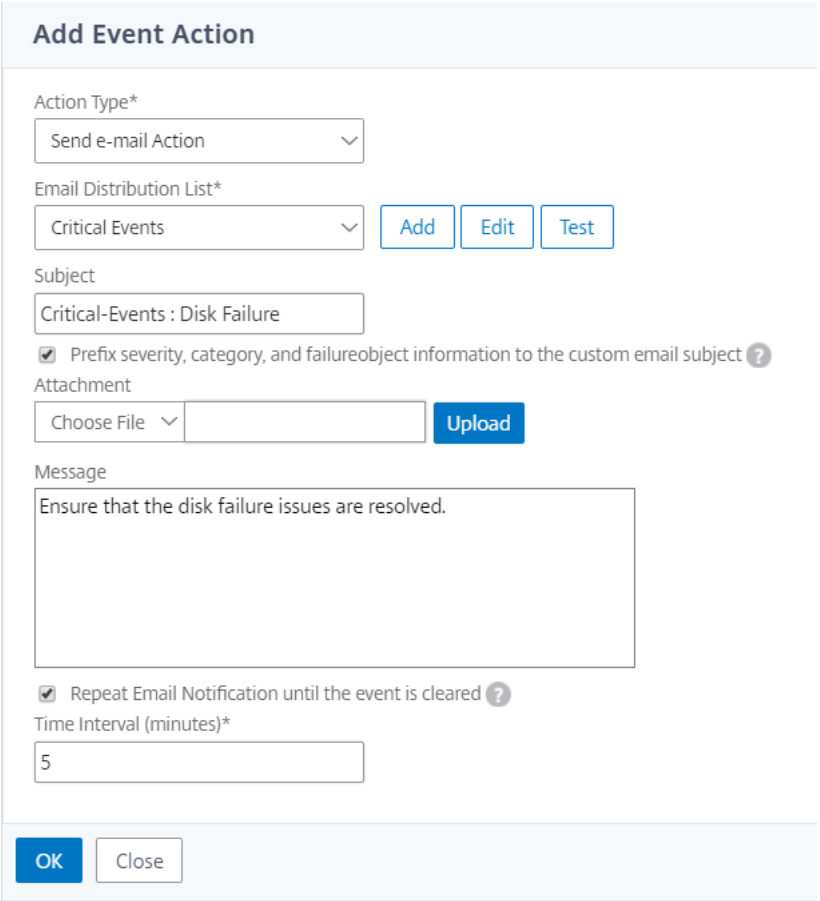
En raison du nombre élevé de serveurs virtuels configurés dans Citrix ADM, vous pouvez recevoir un nombre élevé d'e-mails chaque jour. Les e-mails ont une ligne d'objet par défaut qui fournit des in-

formations sur la gravité de l'événement, la catégorie de l'événement et l'objet d'échec. Mais la ligne d'objet ne contient aucune information sur le nom du serveur virtuel d'où proviennent ces événements. Vous avez maintenant la possibilité d'inclure des informations supplémentaires telles que le nom de l'entité affectée, c'est-à-dire le nom de l'objet d'échec.

Vous pouvez également ajouter une ligne d'objet personnalisée et un message utilisateur, et charger une pièce jointe dans votre e-mail lorsqu'un événement entrant correspond à la règle configurée.

Lors de l'envoi d'e-mails pour les notifications d'événements, vous pouvez envoyer un e-mail de test pour tester les paramètres configurés. Le bouton « Tester » vous permet désormais d'envoyer un e-mail de test après avoir configuré un serveur de messagerie, des listes distribuées associées et d'autres paramètres. Cette fonctionnalité garantit que les paramètres fonctionnent correctement.

Vous pouvez également vous assurer que tous les événements critiques sont résolus et qu'aucune notification par e-mail importante n'est manquée, en activant la case à cocher **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 d'événement qui répondent aux critères que vous avez sélectionnés. Par exemple, si vous avez créé une règle d'événement pour les instances impliquant 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 courrier électronique répétées concernant ces événements.



Pour définir une action de règle d'événement d'interruption

Lorsque vous choisissez le type **d'action d'événement Envoyer une action d'interruption**, les interruptions SNMP sont envoyées ou transférées vers une destination d'interruption externe. En définissant une liste de répartition des interruptions (ou une destination d'interruptions et des détails de profil d'interruptions), les messages d'interruptions sont envoyés à un écouteur d'interruption spécifique lorsque les événements répondent aux critères de filtre définis.

Pour définir l'action Exécuter la commande

Lorsque vous choisissez l' **action d'événement Exécuter une action de commande**, vous pouvez créer une commande ou un script qui peut être exécuté sur Citrix ADM pour les événements correspondant à un critère de filtre particulier.

Vous pouvez également définir les paramètres suivants pour le script **Exécuter une action de commande** :

Paramètre	Description
$source	Ce paramètre correspond à l'adresse IP source de l'événement reçu.
Catégorie $	Ce paramètre correspond au type de pièges défini sous la catégorie du filtre
$entité	Ce paramètre correspond aux instances d'entité ou aux compteurs pour lesquels un événement a été généré. Il peut inclure les noms de compteurs pour tous les événements liés au seuil, les noms d'entités pour tous les événements liés à l'entité et les noms de certificats pour tous les événements liés au certificat.
$sévérité	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 exactement le problème tel qu'il a été notifié. Cela peut être utilisé pour localiser rapidement les problèmes et identifier la raison de l'échec, au lieu de simplement signaler les événements bruts.

> **Remarque**
>
> Pendant l'exécution de la commande, ces paramètres sont remplacés par des valeurs réelles.

Par exemple, considérez que vous souhaitez définir une action de commande d'exécution lorsqu'un statut de serveur virtuel d'équilibrage de charge est **arrêté**. En tant qu'administrateur, vous pouvez envisager de fournir une solution de contournement rapide en ajoutant un autre serveur virtuel. Dans Citrix ADM, vous pouvez :

- Écrivez un fichier de script (.sh).

  Voici un exemple de fichier de script (.sh) :

```
#!/bin/sh
source=$1
failureobj=$2
payload='{
"params":{
"warning":"YES" }
,"lbvserver":{
"name":"'$failureobj'","servicetype":"HTTP","ipv46":"x.x.x.x","
   port":"80","td":"","m":"IP","state":"ENABLED","rhistate":"
   PASSIVE","appflowlog":"ENABLED","
bypassaaaa":"NO","retainconnectionsoncluster":"NO","comment":"" }
 }
'
url="http://$source/nitro/v1/config/lbvserver"
curl --insecure -basic -u nsroot:nsroot -H "Content-type:
   application/json" -X POST -d $payload $url

<!--NeedCopy-->
```

- Enregistrez le fichier .sh dans n'importe quel emplacement persistant sur l'agent Citrix ADM. Par exemple, `/var`.

- Indiquez l'emplacement du fichier .sh dans Citrix ADM à exécuter lorsque les critères de règle sont remplis.

Pour définir l'action **Exécuter la commande** pour créer un nouveau serveur virtuel :

1. Définir la règle
2. Sélectionnez la gravité de l'événement
3. Sélectionnez l' **entité de catégorie d'événement vers le bas**
4. Sélectionnez l'instance sur laquelle le serveur virtuel est configuré
5. Sélectionner ou créer un objet d'échec pour le serveur virtuel
6. Sous **Actions de règle d'événement**, cliquez sur **Ajouter une action**et sélectionnez **Exécuter une action de commande**dans la liste **Type d'action**.
7. Sous **Liste d'exécution des commandes**, cliquez sur **Ajouter**.

   La page Créer une liste de distribution de commandes s'affiche.

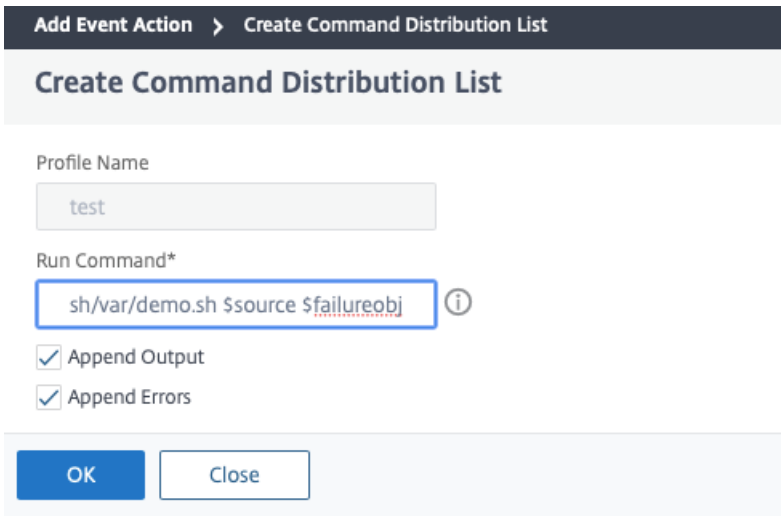
   a) Dans **Nom du profil**, spécifiez un nom de votre choix

   b) Dans **Exécuter la commande**, spécifiez l'emplacement de l'agent Citrix ADM, où le script doit s'exécuter. Par exemple : `/sh/var/demo.sh $source $failureobj`.

   c) Sélectionnez **Ajouter une sortie** et **Ajouter des erreurs**

   > **Remarque**
   >
   > Vous pouvez activer les options **Ajout de sortie** et **Ajout d'erreurs** si vous souhaitez stocker la sortie et les erreurs générées (le cas échéant) lorsque vous exécutez un script de commande dans les fichiers journaux du serveur Citrix ADM. Si vous n'activez pas ces options, Citrix ADM rejette toutes les sorties et erreurs générées lors de l'exécution du script de commande.

   d) Cliquez sur **Créer**.
8. Dans la page **Ajouter une action d'événement**, cliquez sur **OK** .

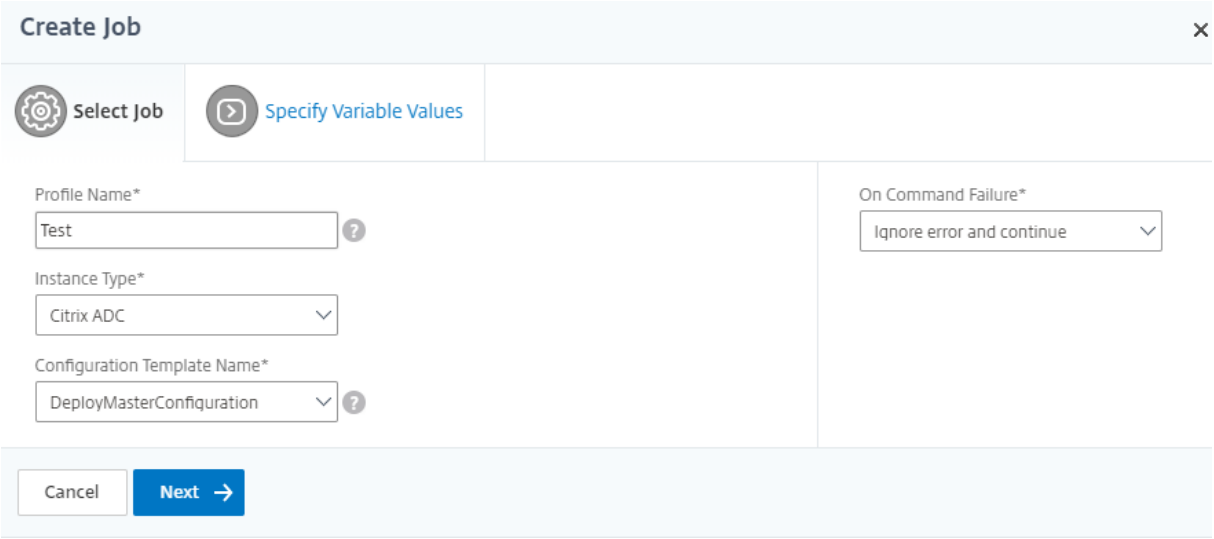


> **Remarque**
>
> Vous pouvez activer les options **Ajout de sortie** et **Ajout d'erreurs** si vous souhaitez stocker la sortie et les erreurs générées (le cas échéant) lorsque vous exécutez un script de commande dans les fichiers journaux du serveur Citrix ADM. Si vous n'activez pas ces options, Citrix ADM rejette toutes les sorties et erreurs générées lors de l'exécution du script de commande.

Pour définir l' action Exécuter le travail

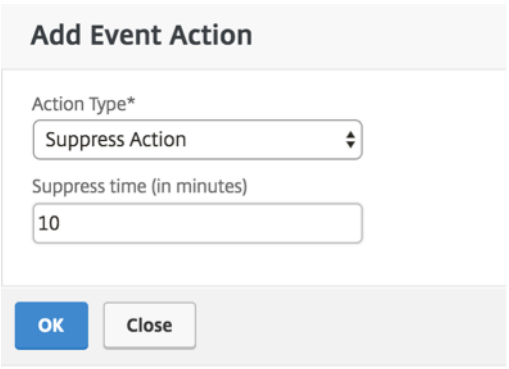
En créant un profil avec des tâches de configuration, un travail est exécuté en tant que travail intégré ou personnalisé pour les instances Citrix ADC, Citrix ADC SDX et Citrix SD-WAN WO, pour les événements et les alarmes correspondant aux critères de filtre que vous avez spécifiés.

1. Sous **Actions de règle d'événement**, cliquez sur **Ajouter une action** et sélectionnez **Exécuter une action de travail** dans la liste **Type d'action** .
2. Créez un profil avec une tâche à exécuter lorsque les événements répondent aux critères de filtre définis.
3. Lors de la création d'une tâche, spécifiez un nom de profil, le type d'instance, le modèle de configuration et l'action que vous souhaitez effectuer si les commandes de la tâche échouent.
4. En fonction du type d'instance sélectionné et du modèle de configuration choisi, spécifiez vos valeurs de variables et cliquez sur **Terminer** pour créer le travail.



Pour définir l'action Supprimer

Lorsque vous choisissez l' **action d'événement Supprimer** l'action, vous pouvez configurer une période, en minutes, pour laquelle un événement est supprimé ou supprimé. Vous pouvez supprimer l'événement pendant au moins 1 minute.



Pour définir des notifications Slack à partir de Citrix ADM

Configurez le canal Slack requis en fournissant le nom du profil et l'URL webhook dans l'interface graphique Citrix ADM. Les notifications d'événement sont ensuite envoyées à ce canal. Vous pouvez configurer plusieurs canaux Slack pour recevoir ces notifications

1. Dans Citrix ADM, accédez à **Réseaux** > **Événements** > **Règles**, puis cliquez sur **Ajouter** pour créer une règle.
2. Dans la page **Créer une règle**, définissez les paramètres de règle tels que gravité et catégorie. Sélectionnez les instances et les objets d'échec que vous souhaitez surveiller.

3. Sous **Actions de règle d'événement**, cliquez sur **Ajouter une action**. Ensuite, sélectionnez **Envoyer des notifications de Slack** dans la liste **Type d'action** et sélectionnez **Liste de profil de marge.**
4. Vous pouvez également ajouter une liste de profils Slack en cliquant sur **Ajouter** en regard du champ **Liste de profils Slack** .
5. Tapez les paramètres suivants pour créer une liste de profils :
    a) **Nom du profil**. Tapez un nom pour la liste de profils à configurer sur Citrix ADM
    b) **Nom du canal**. Tapez le nom du canal Slack auquel les notifications d'événement doivent être envoyées.
    c) **URL Webhook**. Tapez l'URL Webhook du canal que vous avez entré précédemment. Les webhooks entrants sont un moyen simple de publier des messages provenant de sources externes dans Slack. L'URL est liée en interne au nom du canal et toutes les notifications d'événement sont envoyées à cette URL pour être publiées sur ADCal Slack désigné. Un exemple de webhook est le suivant : https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK
6. Cliquez sur **Créer**, puis sur **OK** dans la fenêtre **Ajouter une action d'événement** .

> **Remarque**
>
> Vous pouvez également ajouter les profils Slack en accédant à **Compte**> **Notifications**> **Profils de marge**. Cliquez sur **Ajouter** et créez le profil comme décrit dans la section précédente.

Vous pouvez afficher l'état des profils Slack que vous avez créés.

Votre règle d'événement est maintenant créée avec des filtres appropriés et des actions de règle d'événement bien définies.

Pour définir les notifications PagerDuty à partir de Citrix ADM

Vous pouvez ajouter un profil PagerDuty en tant qu'option dans Citrix ADM pour surveiller les notifications d'incident en fonction de vos configurations PagerDuty. PagerDuty vous permet de configurer les notifications par e-mail, SMS, notification push et appel téléphonique sur un numéro enregistré.

Avant d'ajouter un profil PagerDuty dans Citrix ADM, assurez-vous d'avoir rempli les configurations requises dans PagerDuty. Pour de plus amples informations, consultez la section Documentation PagerDuty.

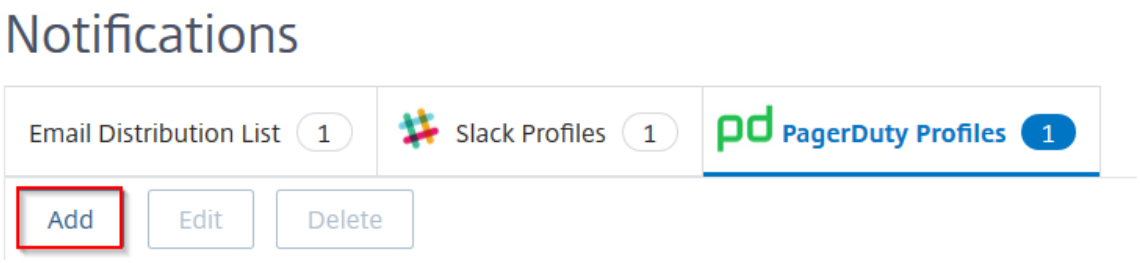
Vous pouvez sélectionner votre profil PagerDuty comme l'une des options pour obtenir des notifications pour les fonctionnalités suivantes :

- **Événements** : liste des événements générés pour les instances Citrix ADC.
- **Licences** : liste des licences actuellement actives, sur le point d'expirer, etc.

- **Certificats SSL** : liste des certificats SSL ajoutés aux instances Citrix ADC.

Pour ajouter un profil PagerDuty dans ADM :

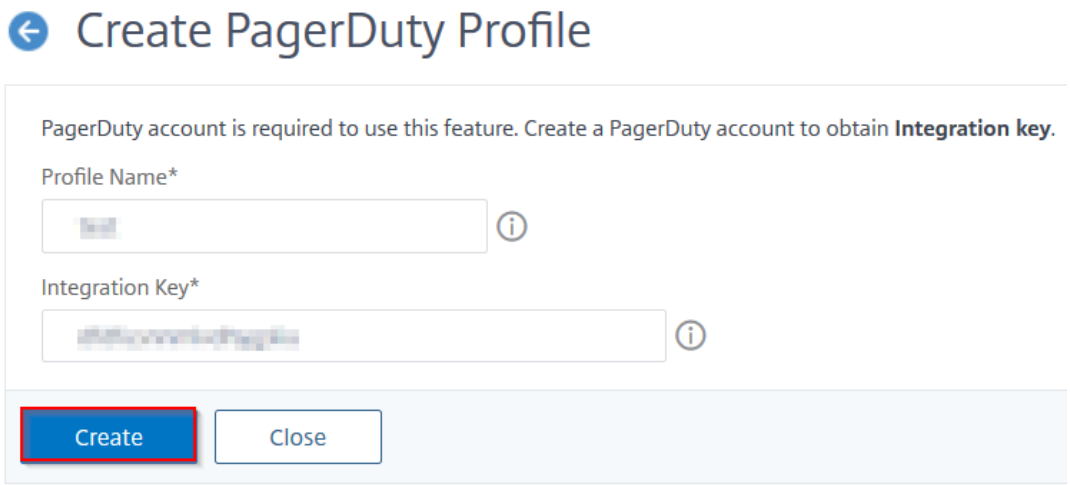
1. Connectez-vous à Citrix ADM à l'aide des informations d'identification de l'administrateur.
2. Accédez à **Compte** > **Notifications** > **Profils PagerDuty** .
3. Cliquez sur **Ajouter** pour créer un profil.



4. Dans la page Créer un profil PagerDuty :
   a) Indiquez le nom de profil de votre choix.
   b) Entrez la **clé d'intégration**.

      Vous pouvez obtenir la clé d'intégration à partir de votre portail PagerDuty.

   c) Cliquez sur **Créer**.



Cas d'utilisation :

Considérez un scénario que vous :

- veulent envoyer des notifications à votre profil PagerDuty.
- ont configuré l'appel téléphonique comme option dans PagerDuty pour recevoir des notifications.
- veulent obtenir des alertes d'appel téléphonique pour les événements Citrix ADC.

Pour configurer :

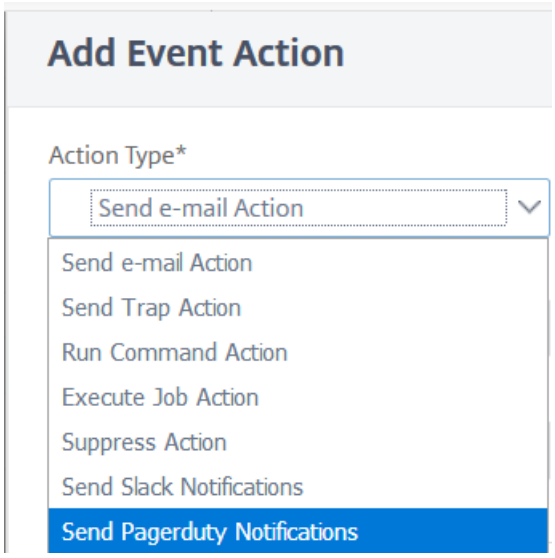
a) Accédez à **Événements** > **Règles**

b) Dans la page **Créer une règle**, configurez tous les autres paramètres pour créer une règle.

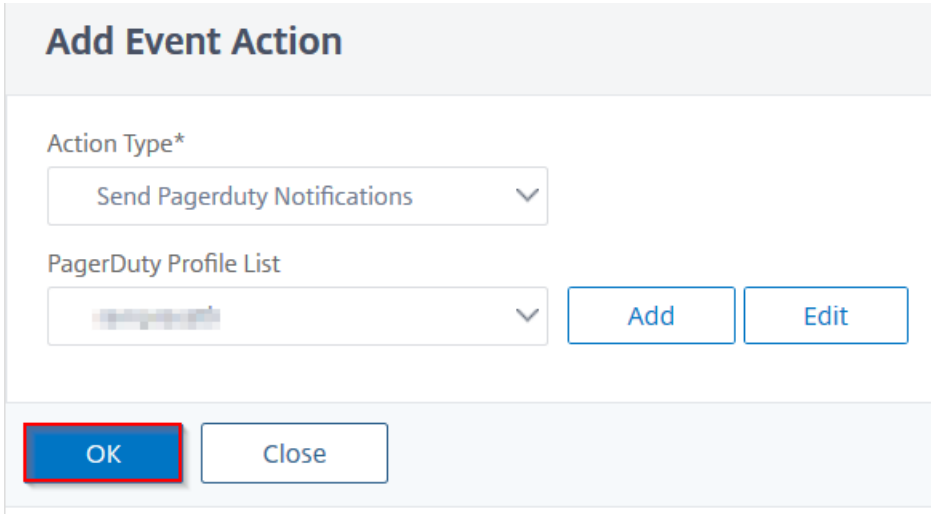
c) Sous **Créer des actions de règle**, cliquez sur **Ajouter une action**.

La page **Ajouter une action d'événement** s'affiche.

i. Sous **Type d'action**, sélectionnez **Envoyer les notifications PagerDuty**.



ii. Sélectionnez votre profil PagerDuty et cliquez sur **OK**.



Une fois la configuration terminée, chaque fois qu'un nouvel événement est généré pour l'instance Citrix ADC, vous recevrez un appel téléphonique. À partir de l'appel téléphonique, vous pouvez décider de :

- Accuser l'événement

- Marquer comme résolu
- Escalade vers un autre membre de l'équipe

Pour générer automatiquement des incidents ServiceNow à partir de Citrix ADM

Vous pouvez générer automatiquement des incidents ServiceNow pour les événements Citrix ADM en sélectionnant le profil ServiceNow dans l'interface graphique graphique Citrix ADM. Vous devez choisir le profil **ServiceNow** dans Citrix ADM pour configurer une règle d'événement.

Avant de configurer une règle d'événement pour générer automatiquement des incidents ServiceNow, intégrez le service Citrix ADM à l'instance ServiceNow. Pour de plus amples informations, consultez la section Configurer la carte ITSM pour ServiceNow.

Pour configurer une règle d'événement, accédez à **Événements** > **Règles** .

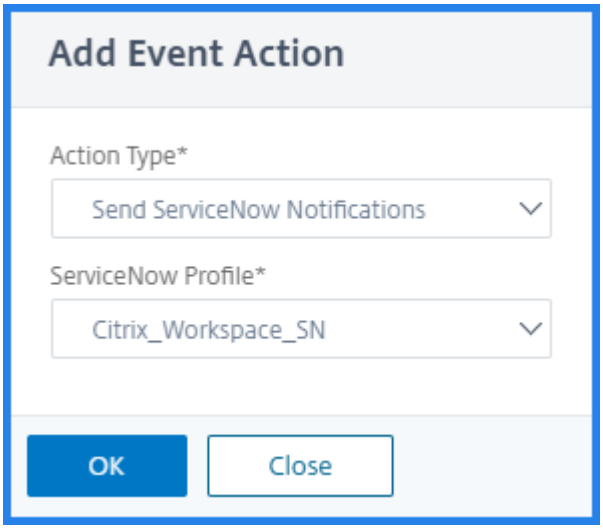
1. Dans la page **Créer une règle**, configurez tous les autres paramètres pour créer une règle.
2. Sous **Créer des actions de règle**, cliquez sur **Ajouter une action**.

   La page **Ajouter une action d'événement** s'affiche.

   a) Dans **Type d'action**, sélectionnez **Envoyer des notifications ServicNow**.

   b) Dans **ServiceNow Profile, sélectionnez le profilCitrix_Workspace_SN**dans la liste.

   c) Cliquez sur **OK**.



Modifier la gravité signalée des événements qui se produisent sur les instances Citrix ADC

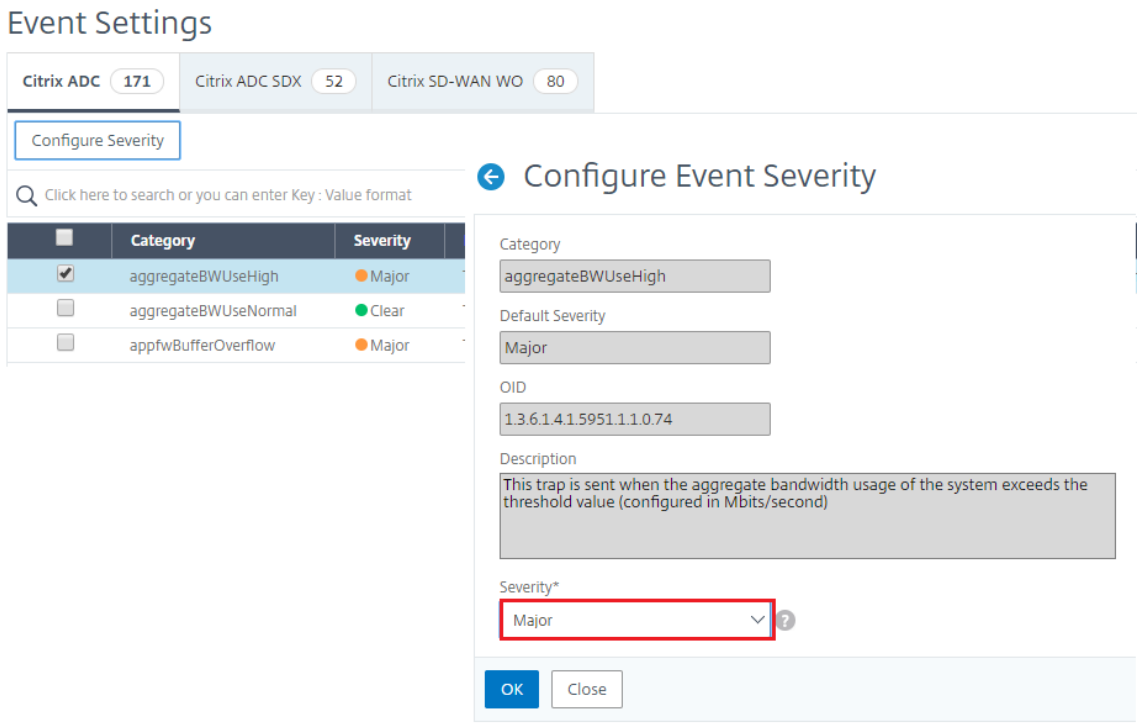
April 29, 2021

Vous pouvez gérer les rapports d'événements générés sur tous vos appareils, de sorte que vous puissiez afficher les détails d'événements relatifs à un événement particulier sur une instance et afficher les rapports en fonction de la gravité de l'événement. Vous pouvez également créer des règles d'événement qui utilisent les paramètres de gravité par défaut et 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, Major, Mineure, Avertissement et Effacer.

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 Citrix 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**.

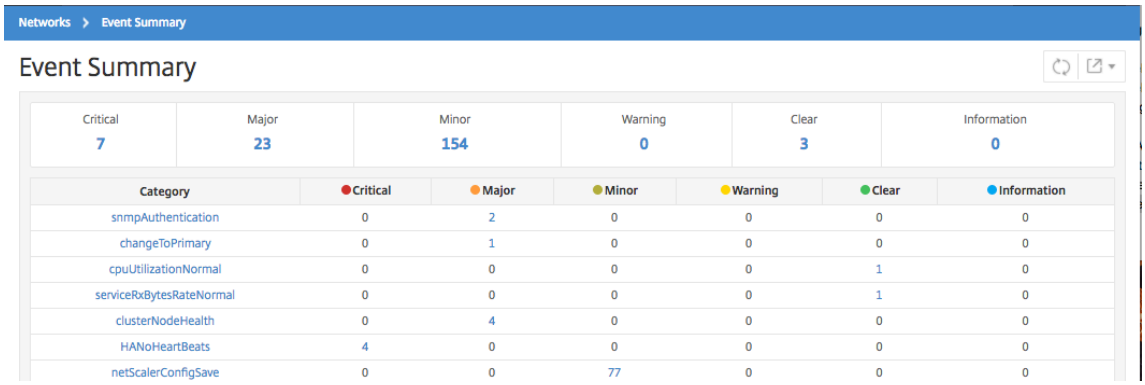


Afficher le résumé des événements

April 29, 2021

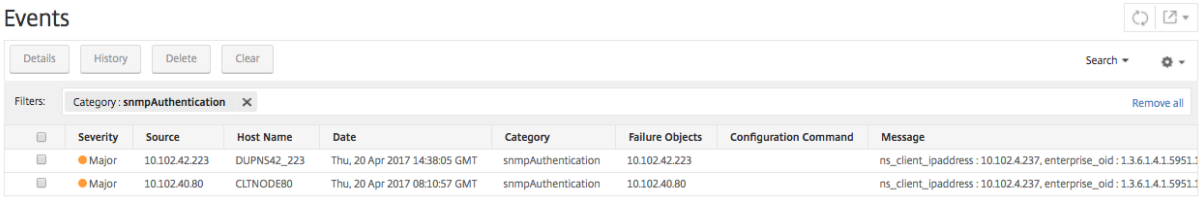
Vous pouvez maintenant afficher une page Récapitulatif des événements pour surveiller les événements et interruptions reçus sur Citrix Application Delivery Management (Citrix ADM). Accédez à **Réseaux** > **Événements** . La page Récapitulatif des événements affiche les informations suivantes sous forme de tableau :

- **Résumé de tous les événements reçus par Citrix ADM**. Les événements sont répertoriés par catégorie et les différentes gravités sont affichées dans différentes colonnes : Critique, Majeur, Mineur, Avertissement, Effacer et Informations. Par exemple, un événement critique se produit lorsqu'une instance Citrix Application Delivery Controller (Citrix ADC) tombe en panne et cesse d'envoyer des informations à Citrix ADM. Pendant l'événement, une notification est envoyée à un administrateur, expliquant la raison de l'arrêt de l'instance, l'heure pour laquelle elle a été arrêtée, etc. L'événement est ensuite enregistré sur la page Récapitulatif des événements, sur laquelle vous pouvez afficher le résumé et accéder aux détails de l'événement.



- **Nombre de pièges reçus pour chaque catégorie**. Nombre de pièges reçus, classés par gravité. Par défaut, chaque interruption envoyée à partir d'instances Citrix ADC à Citrix ADM a une gravité attribuée, mais en tant qu'administrateur réseau, vous pouvez spécifier sa gravité dans l'interface graphique Citrix ADM.

Si vous cliquez sur un type de catégorie ou une interruption, vous accédez à la page **Événements**, sur laquelle des filtres tels que Catégorie et Gravité sont présélectionnés. Cette page affiche plus d'informations sur l'événement, telles que l'adresse IP et le nom d'hôte d'une instance d'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.



Vous pouvez configurer le nombre de jours compris entre 1 et 40, pour lesquels vous souhaitez afficher les événements dans Citrix ADM. Par exemple, si vous sélectionnez 30 jours, Citrix ADM affiche les événements pendant 30 jours et après 30 jours, les événements sont effacés. Pour configurer ce

paramètre d'événement, accédez à **Paramètres > Stratégie de location de données**. Pour de plus amples informations, consultez la section Stratégie de rétention des données.

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 quotidiennement, hebdomadaire ou mensuel et envoyer le rapport par e-mail ou par un message de marge.

> **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.

Afficher les sévérité des événements et les détails des interruptions SNMP

April 29, 2021

Lorsque vous créez un événement et ses paramètres dans Citrix Application Delivery Management (Citrix ADM), vous pouvez afficher l'événement immédiatement sur la page Récapitulatif des événements. De même, vous pouvez afficher et surveiller l'intégrité, la durée de fonctionnement, les modèles et les versions de toutes les instances Citrix Application Delivery Controller (Citrix ADC) ajoutées à votre serveur Citrix ADM en détail sur 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, l'état de santé, le temps d'arrêt, les modèles et la version des instances de Citrix ADC en détail.

Par exemple, les événements ayant un niveau de gravité **critique** peuvent se produire rarement. Toutefois, lorsque ces événements critiques se produisent sur votre réseau, vous pouvez rechercher, dépanner et surveiller où et quand l'événement s'est produit. Si vous sélectionnez tous les niveaux de gravité sauf Critique, le graphique affiche uniquement les occurrences des événements critiques. En outre, en cliquant sur le graphique, vous accédez à la page **Événements basés sur la gravité**, où vous pouvez voir tous les détails concernant le moment où un événement critique s'est produit pendant la durée sélectionnée : la source de l'instance, la date, la catégorie et la notification de message envoyée lorsque l'événement critique s'est produit.

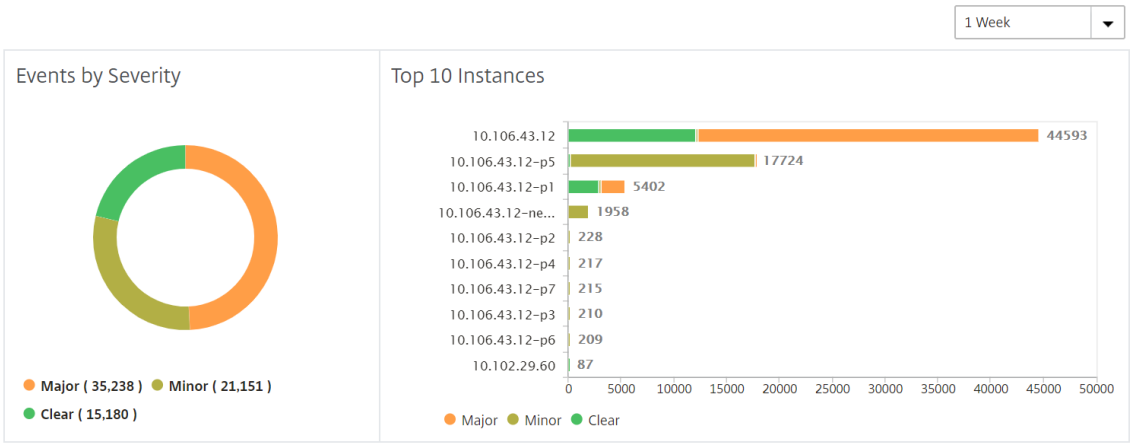
De même, vous pouvez afficher l'intégrité d'une instance Citrix ADC VPX sur le tableau de bord. Vous pouvez masquer le temps pendant lequel l'instance était en cours d'exécution et afficher uniquement les heures où elle était hors service. En cliquant sur le graphique, vous accédez à la page de cette 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 l'instance 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

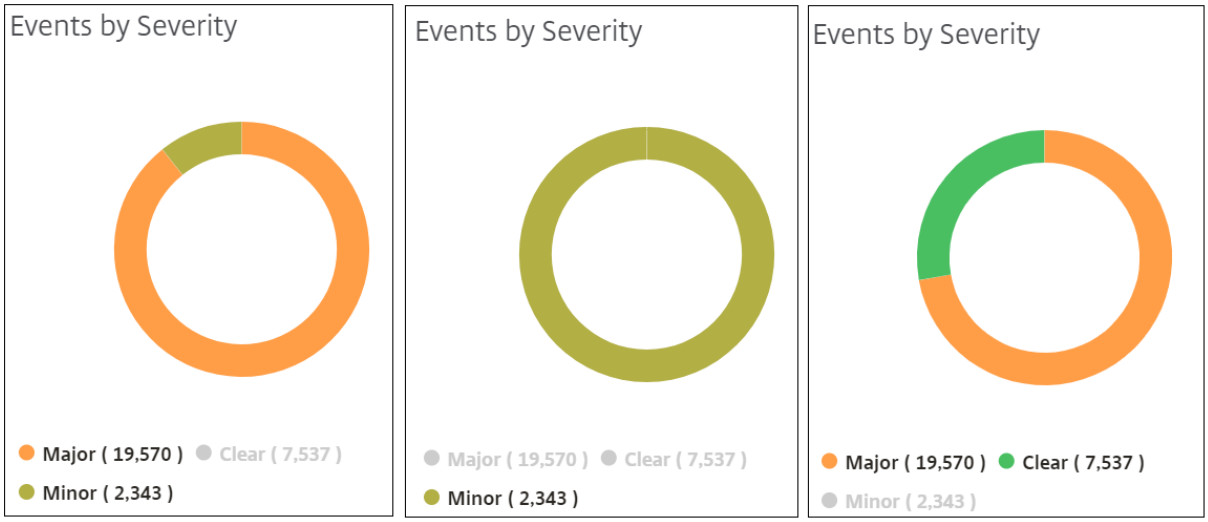
   Accédez à **Réseaux** > **Événements** > **Rapports**.
3. Dans la liste déroulante située dans le coin supérieur droit de la page, sélectionnez la durée pour laquelle vous souhaitez afficher les événements par gravité.



4. Le graphique en beignet **Événements par gravité** affiche une représentation visuelle de tous les événements selon leur gravité. Différents types d'événements sont représentés sous la 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 beignet pour afficher la page d' **événements basés sur la gravité** correspondante, qui affiche les détails suivants pour la gravité sélectionnée pour la durée sélectionnée :

   - Source de l'instance
   - Données de l'événement
   - Catégorie d'événements générés par l'instance d'Citrix ADC
   - Notification de message envoyée

> **Remarque**
>
> Sous le graphique 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 et, 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.

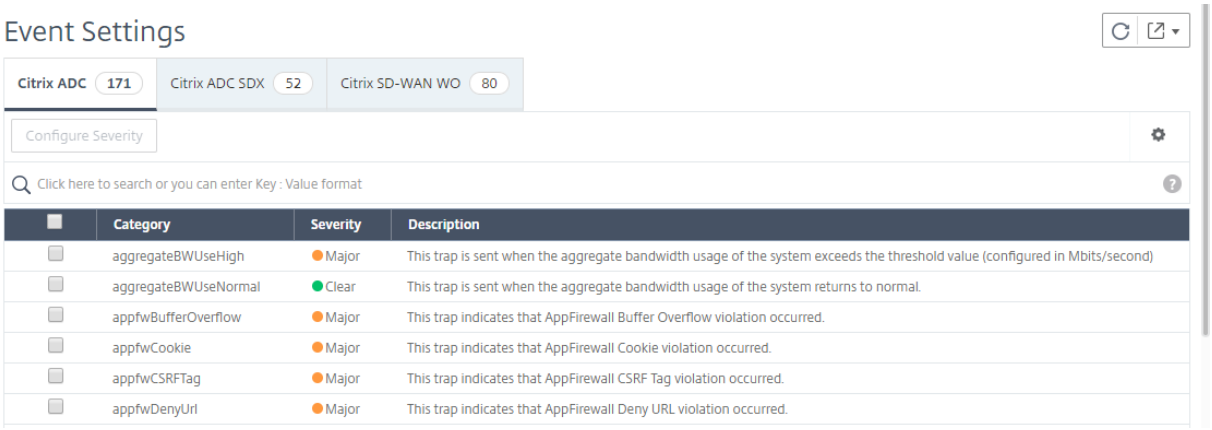


Pour afficher les détails des interruptions SNMP Citrix ADC sur Citrix ADM :

Vous pouvez maintenant afficher les détails de chaque interruption SNMP reçue de ses instances Citrix ADC gérées sur Citrix ADM sur 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, un événement avec la catégorie d'interruption **MonrespTimeOutBelowThresh**, la description de l'interruption s'affiche comme suit : "Cette interruption est envoyée lorsque le délai d'attente de réponse d'une sonde de moniteur revient à la normale, inférieure au seuil défini."



Afficher et exporter les messages syslog

April 29, 2021

Vous pouvez afficher les messages syslog sans vous connecter à Citrix Application Delivery Management (Citrix ADM), en planifiant l'exportation de tous les messages syslog reçus sur le serveur. Vous pouvez exporter les messages syslog générés sur vos instances Citrix Application Delivery Controller (Citrix ADC) au format PDF, CSV, PNG et JPEG. En outre, vous pouvez planifier l'exportation de ces rapports vers des adresses e-mail spécifiées à différents intervalles.

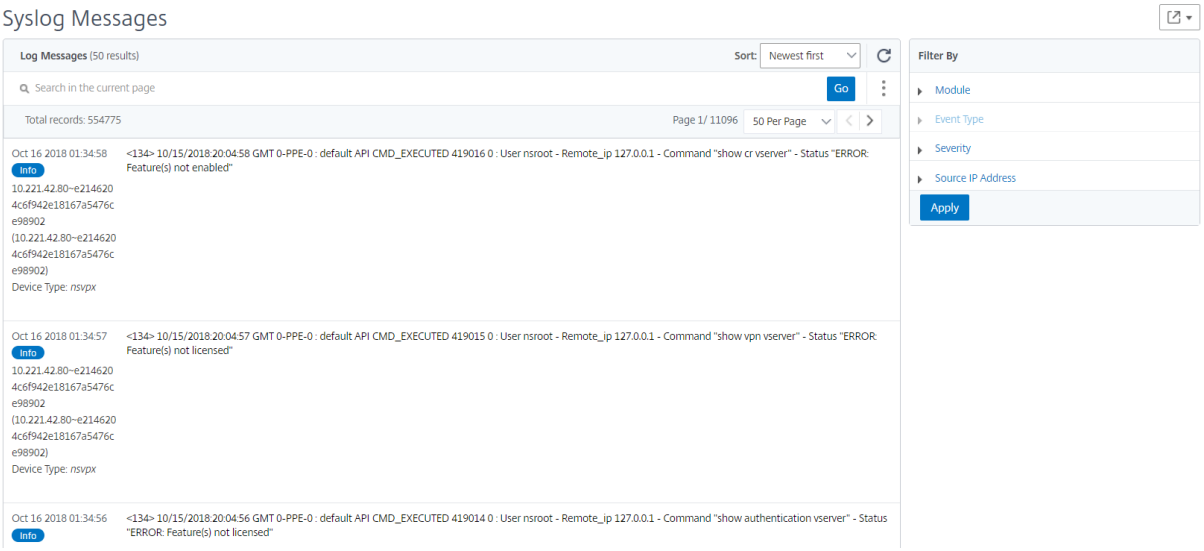
> **Remarque**
>
> Pour plus d'informations sur la configuration d'un serveur syslog et l'affichage des messages syslog sur Citrix ADM, reportez-vous à la sectionComment afficher les informations d'audit de Citrix ADM.

Afficher les messages syslog

Vous pouvez afficher tous vos messages syslog générés sur vos instances Citrix ADC gérées. Pour afficher les messages, vous devez configurer les instances pour rediriger les messages syslog vers le serveur Citrix ADM. Les messages syslog sont stockés dans la base de données de manière centralisée et sont disponibles dans la visionneuse Syslog à des fins d'audit. Vous pouvez combiner ces informations de journalisation et dériver des rapports pour les analyses à partir des données collectées.

Vous pouvez également configurer syslog pour consigner différents types d'événements.

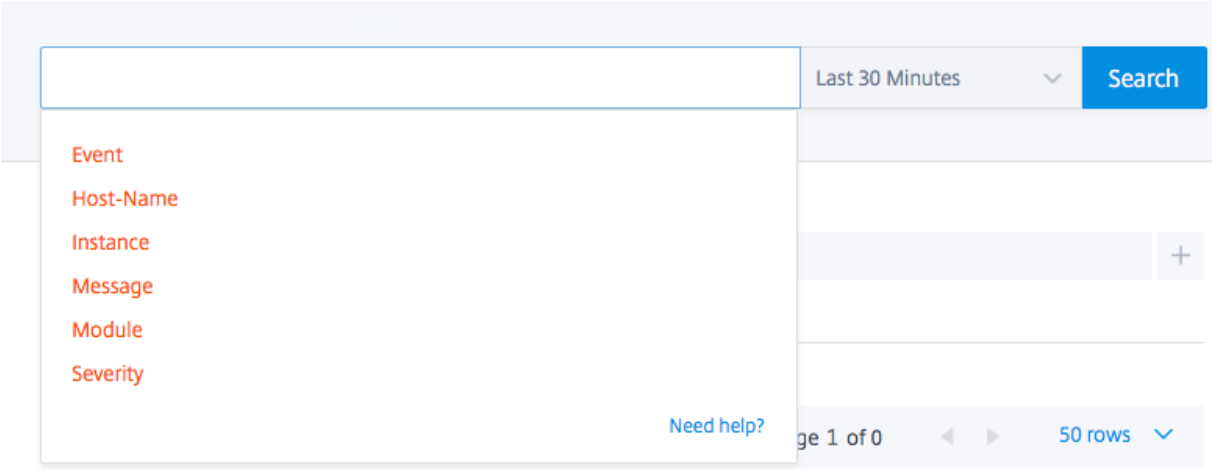
Pour afficher la visionneuse Syslog, accédez à **Réseaux** > **Événements** > **Messages Syslog** . Choisissez les filtres appropriés pour afficher vos messages du journal système.



Rechercher des messages syslog

Vous pouvez utiliser des filtres pour rechercher les messages syslog et les messages du journal d'audit pour affiner vos résultats et trouver exactement ce que vous recherchez et en temps réel.

Pour rechercher des messages syslog pour toutes les instances ADC présentes dans le logiciel ADM, à partir de l'interface graphique d'ADM, accédez à **Réseaux > Événements > Messages Syslog**. Les nouvelles catégories de filtres sont instance, module, événement, gravité et message.



Pour rechercher tous les messages du journal d'audit système ADM présents dans le logiciel ADM, à partir de l'interface graphique ADM, accédez à **Compte > Messages du journal d'audit**. Les nouvelles catégories de filtres sont instance, module, événement, gravité et message.

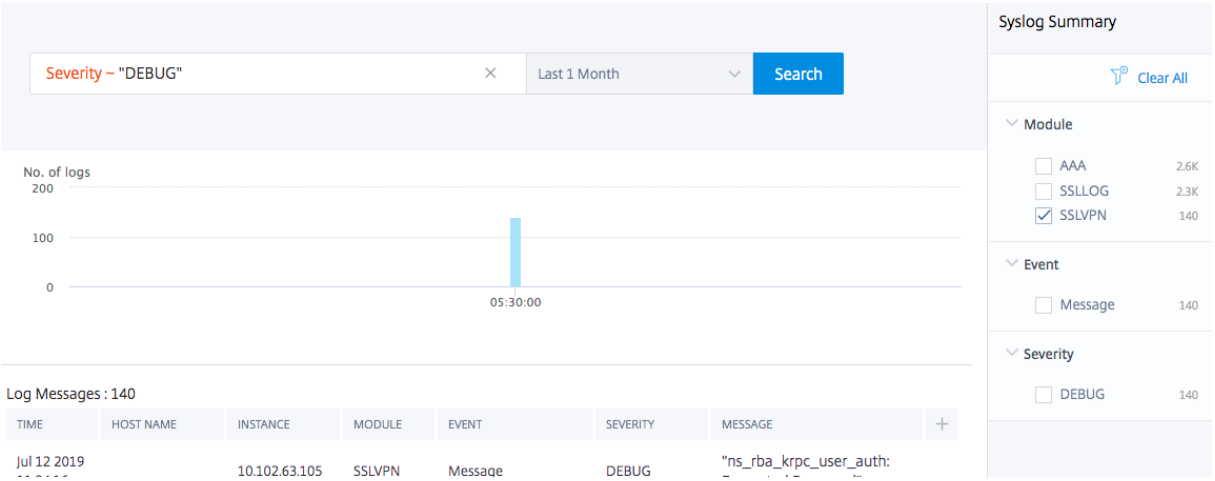
Pour rechercher les messages du journal d'audit pour toutes les applications présentes dans ADM, à partir de l'interface graphique d'ADM, accédez à **Réseaux > Fonctions réseau> Audit**.

Pour rechercher les messages du journal d'audit pour une application spécifique sur l'ADM, à partir de

l'interface graphique ADM, accédez à **Application>Tableau de bord** et sélectionnez le serveur virtuel pour lequel vous souhaitez rechercher les messages du journal d'audit. Cliquez ensuite sur l'onglet **Journal d'audit**.

Après avoir sélectionné une catégorie de filtre, indiquez si elle est égale ou contient le terme de recherche.

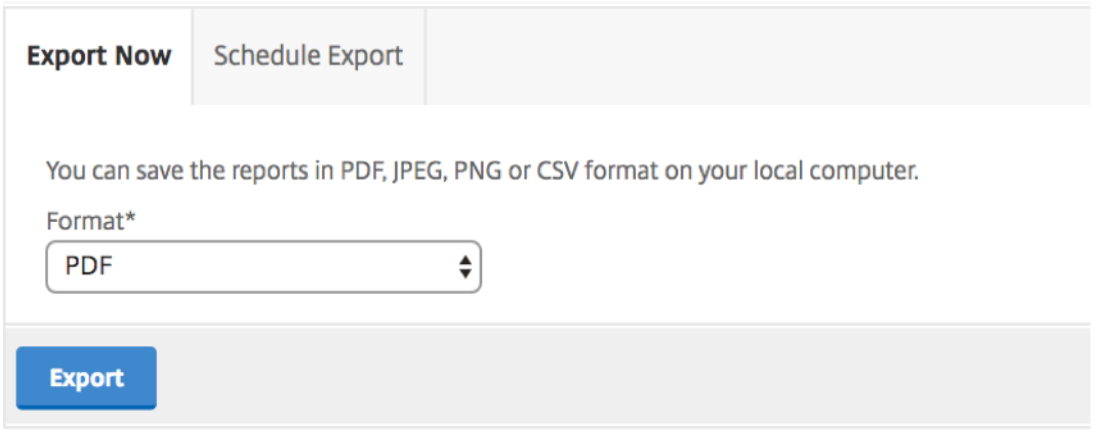
Ensuite, ajoutez le terme de recherche. Pour certaines catégories, une liste préremplie de termes de recherche s'affiche. Par défaut, la durée de recherche est de 1 jour. Vous pouvez modifier la plage d'heure et de dates en cliquant sur la flèche vers le bas. Vous pouvez affiner davantage votre recherche en sélectionnant des options dans le volet Synthèse **Syslog ou Récapitulatifdu journal d'audit** .



Exporter les messages syslog

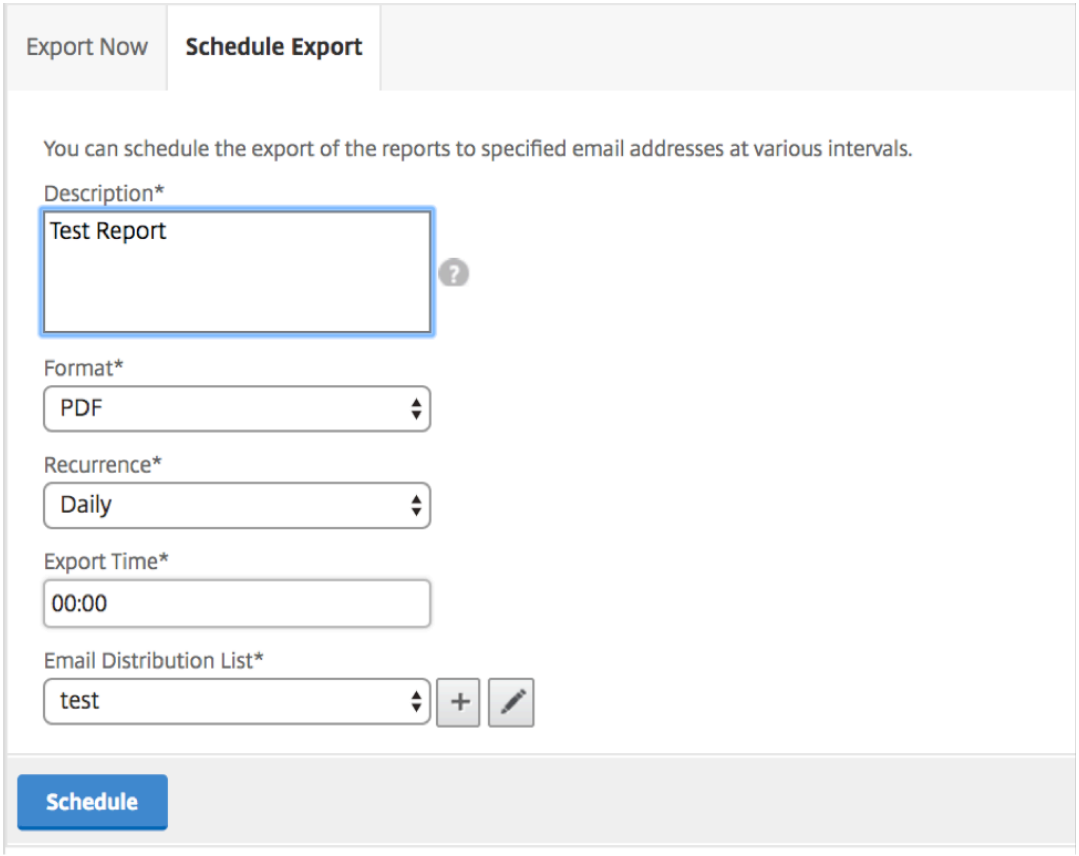
Pour exporter un rapport de messages syslog à l'aide de Citrix ADM :

1. Accédez à **Réseaux** > **Événements** > **Messages Syslog**.
2. Dans le volet droit, cliquez sur le bouton d'exportation situé dans le coin supérieur droit de la page Messages Syslog.
3. Sous **Exporter maintenant**, sélectionnez le format requis, puis cliquez sur **Exporter**.



Pour planifier l'exportation du rapport de messages syslog à l'aide de Citrix ADM :

1. Accédez à **Réseaux** > **Événements** > **Messages Syslog**.
2. Dans 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 le motif de l'exportation du rapport.
    - **Format** : Format dans lequel exporter l'état.
    - **Périodicité** : intervalle auquel exporter l'état.
    - **Heure d'exportation** : Heure à laquelle l'état doit être exporté. Entrez l'heure dans un format 24 heures, pour votre fuseau horaire local.
    - **Liste de distribution par courrier électronique** : Liste des destinataires pour recevoir le rapport par courriel. Choisissez une liste de distribution de courrier électronique dans la liste fournie. Un e-mail est déclenché lorsque le rapport est généré et répond aux critères d'heure planifiée. Si vous souhaitez créer une liste de distribution de messagerie, cliquez sur **+** et fournissez les détails du serveur de messagerie et du profil de messagerie.



Suppression des messages syslog

April 29, 2021

Lorsqu'il est configuré en tant que serveur syslog, Citrix Application Delivery Management (ADM) reçoit tous les messages syslog des instances Citrix Application Delivery Controller (Citrix ADC) configurées. Il se peut que vous ne vouliez pas voir de nombreux messages. Par exemple, vous pourriez ne pas être intéressé par l'affichage de tous les messages au niveau de l'information. Vous pouvez maintenant ignorer certains des messages syslog qui ne vous intéressent pas. Vous pouvez supprimer certains messages syslog entrant dans 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 des messages syslog consignés entrant dans 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

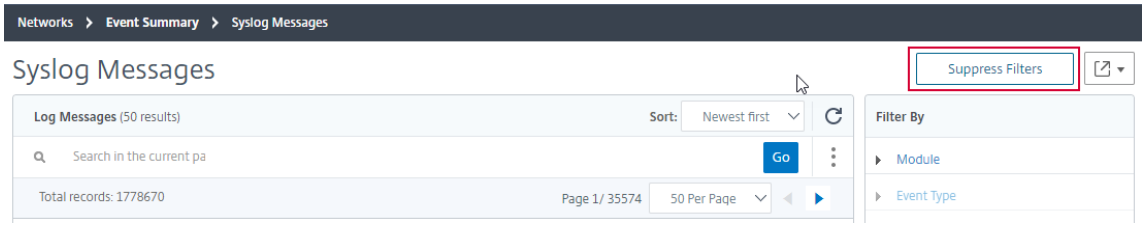
ADM pour rechercher et supprimer des messages. Citrix ADM supprime tous les messages correspondant aux critères. Ces messages supprimés n'apparaissent pas sur l'interface graphique Citrix ADM et ne sont pas non plus stockés dans la base de données client. Par conséquent, une bonne quantité d'espace est enregistrée sur le serveur de stockage.

Certains cas d'utilisation pour supprimer les messages syslog sont les suivants :

- Si vous souhaitez ignorer tous les messages de niveau information, supprimez le niveau 6 (information)
- Si vous souhaitez uniquement enregistrer les conditions d'erreur de 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** .
2. Cliquez sur **Supprimer les filtres**.

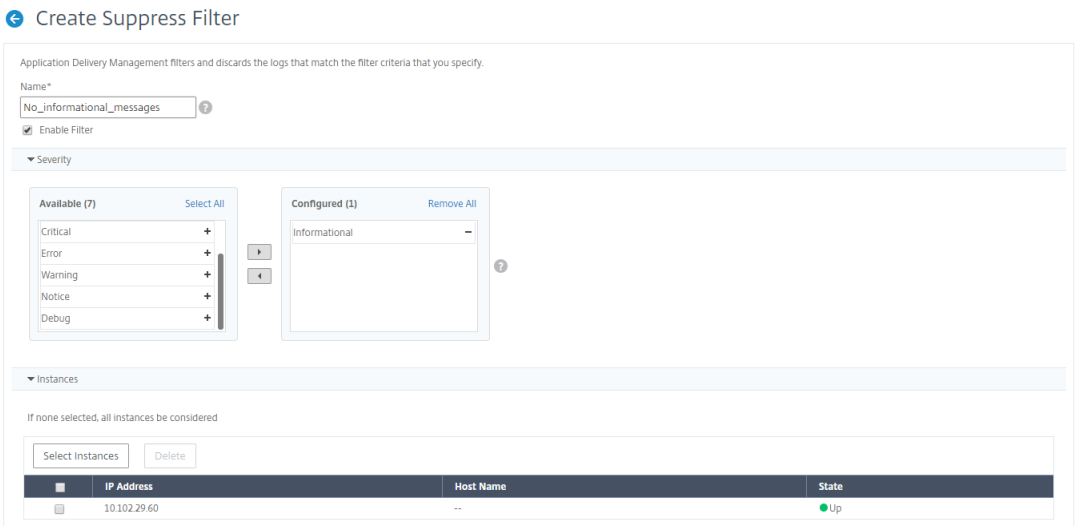


3. Dans la page **Supprimer les filtres**, cliquez sur **Ajouter** .
4. Sur la page **Créer un filtre de suppression**, mettez à jour les informations suivantes :
   a) **Nom** : saisissez un nom pour le filtre.

   > **Remarque**
   >
   > Si différents utilisateurs ont un accès différent à plusieurs instances de Citrix ADC, des filtres différents doivent être créés pour différentes instances, car les utilisateurs ne peuvent voir que les filtres dans lesquels ils ont accès à toutes les instances.

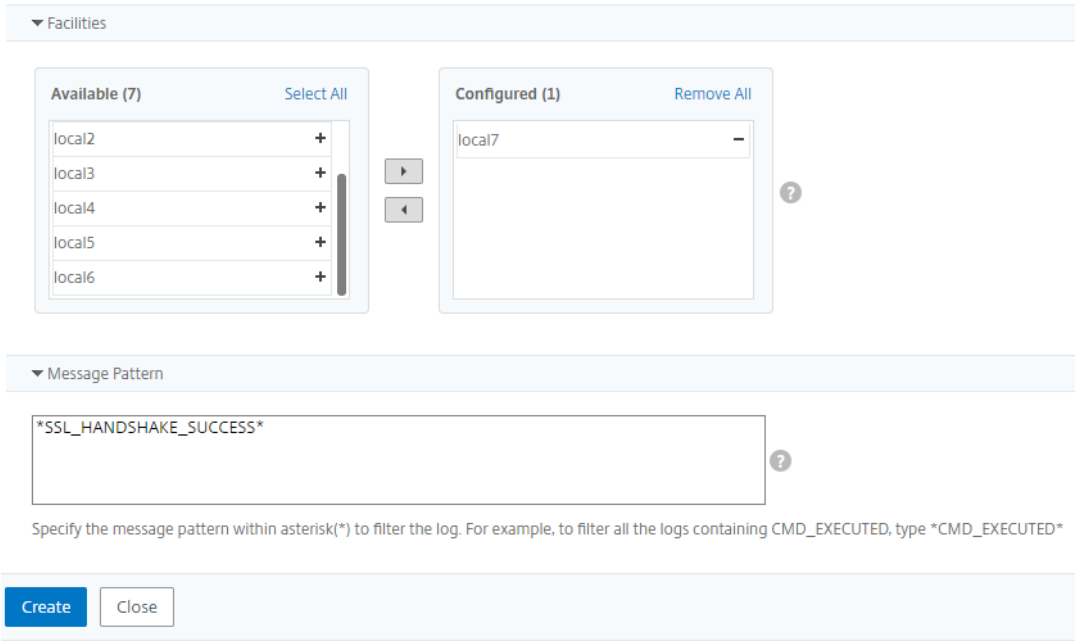
   b) **Gravité** - Sélectionnez et ajoutez les niveaux de journal pour lesquels vous devez supprimer les messages.
   Par exemple, si vous ne souhaitez pas afficher les messages d'information entrants, vous pouvez sélectionner **Informations** pour supprimer ces messages.

   c) **Instances** : sélectionnez les instances Citrix ADC sur lesquelles les messages syslog ont été configurés.



d) **Installations :** sélectionnez la fonction permettant de supprimer les messages en fonction de la source qui les génère.

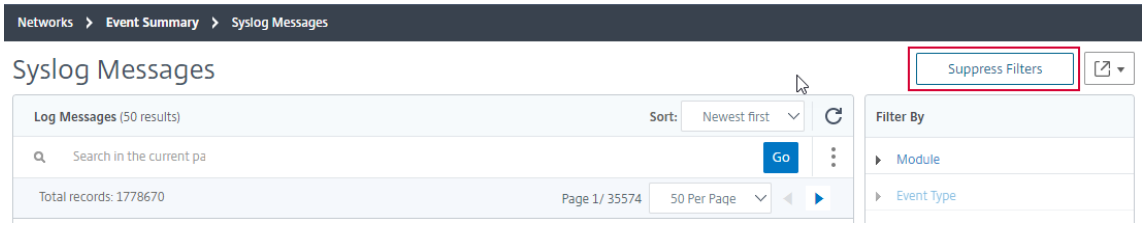
e) **Modèle de message** - Vous pouvez également taper un motif de texte entouré d'astérisques (*) pour supprimer les messages. Les messages sont recherchés pour la chaîne de modèle de texte et les messages qui contiennent ce modèle sont supprimés.



Désactivation du filtre

Pour autoriser l'affichage des messages sur Citrix ADM, vous devez désactiver le filtre.

1. Accédez à **Réseaux** > **Événements** > **Messages Syslog**.
2. Cliquez sur **Supprimer les filtres**.



3. Dans la page **Supprimer les filtres**, sélectionnez le filtre et cliquez sur **Modifier** .
4. Sur la page **Configurer Supprimer le filtre**, **désactivez la case à cocher Activer le filtre** pour désactiver le filtre.

Tableau de bord SSL

April 29, 2021

Citrix Application Delivery Management (Citrix 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 approprié, la force de la clé et les algorithmes corrects, tout en gardant un œil étroit sur les certificats inutilisés ou qui expirent bientôt. 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 a un composant de clé publique visible par tout client qui souhaite initier une transaction sécurisée avec le serveur. La clé privée correspondante, qui réside en toute sécurité sur l'appliance Citrix ADC, est utilisée pour effectuer le chiffrement et le déchiffrement de clé asymétrique (ou clé publique).

Vous pouvez obtenir un certificat SSL et une clé de l'une des manières suivantes :

- 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. Dans le tableau de bord SSL, vous pouvez afficher des graphiques qui vous aident à suivre les émetteurs de certificats, les points forts, 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 un certificat d'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. Une fois que vous avez lié un ou plusieurs certificats à un certificat d'autorité de certification, vous pouvez les dissocier.

> **Remarque**
>
> Vous pouvez également utiliser un serveur Venafi Trust Protection Platform avec ADM pour automatiser la gestion de l'ensemble du cycle de vie des certificats SSL. Pour de plus amples informations, consultez la section Automatisation de la gestion des certificats SSL.

Utiliser le tableau de bord SSL

April 29, 2021

Vous pouvez utiliser le tableau de bord des certificats SSL dans Citrix Application Delivery Management (Citrix ADM) pour afficher des graphiques qui vous aident à suivre les émetteurs de certificats, les points forts clés et les algorithmes de signature. Le tableau de bord des certificats SSL affiche également des graphiques indiquant les éléments suivants :

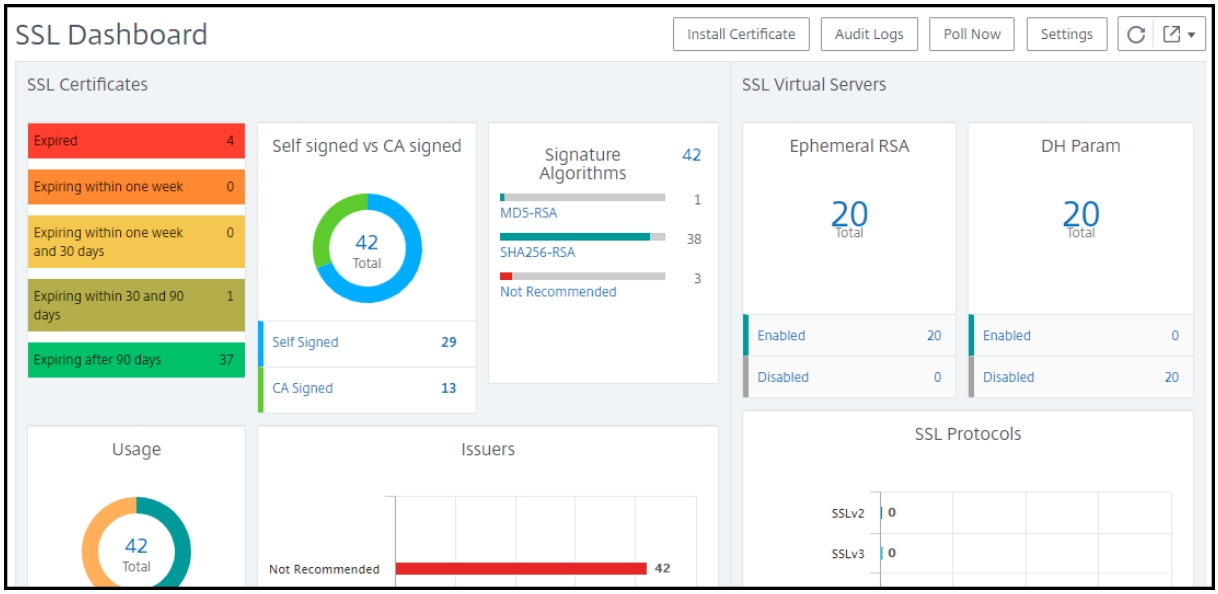
- Nombre de jours après lesquels les certificats expirent
- Nombre de certificats utilisés et inutilisés
- Nombre de certificats autosignés et signés par une autorité de certification
- Nombre d'émetteurs
- Algorithmes de signature
- Protocoles SSL
- 10 instances les plus importantes selon le nombre de certificats utilisés

Surveillance des certificats SSL

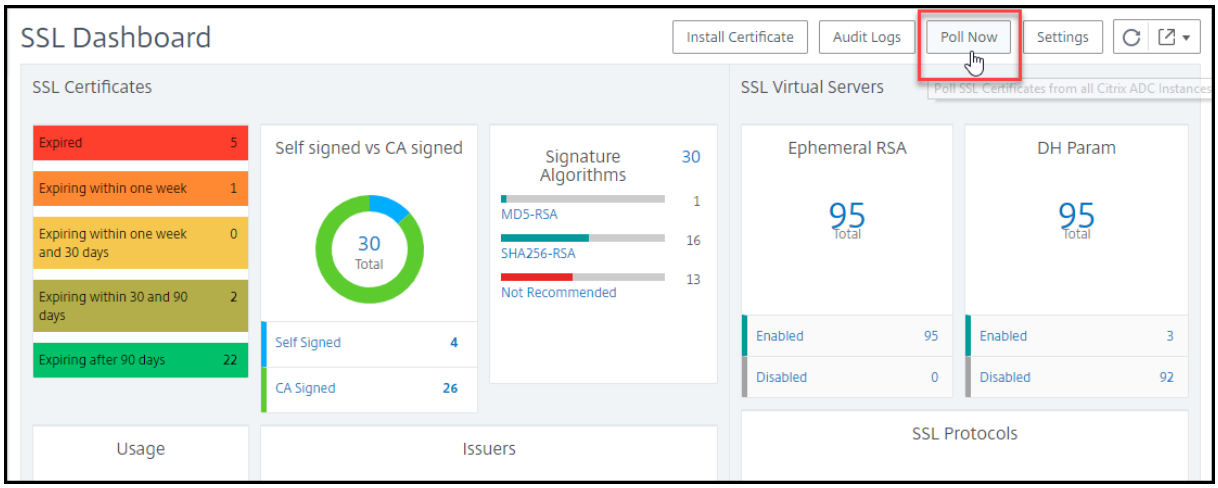
Vous pouvez utiliser le tableau de bord SSL sur Citrix ADM pour surveiller vos certificats si votre entreprise dispose d'une stratégie SSL dans laquelle vous avez défini certaines exigences en matière de certificat SSL, telles que tous les certificats doivent avoir des forces clés minimales de 2048 bits et une autorité de certification approuvée 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 utilisés. Dans la section **Utilisation**, vous pouvez voir le nombre de certificats installés et le nombre de certificats utilisés. Vous pouvez cliquer sur le graphique pour voir le nom du certificat, l'instance sur laquelle il est utilisé, sa validité, son algorithme de signature, etc.

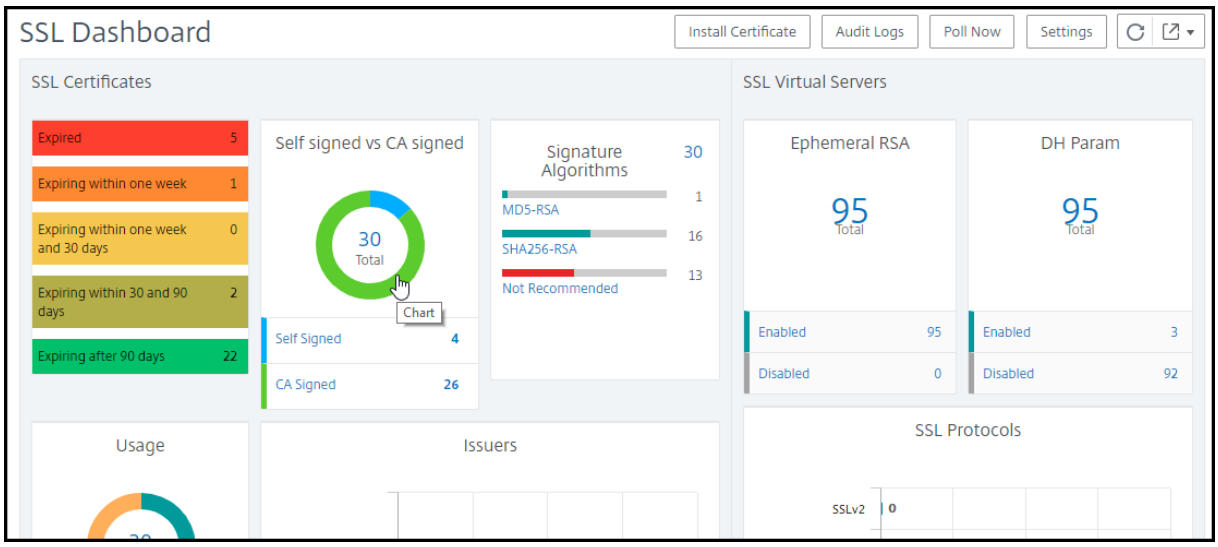
Pour surveiller les certificats SSL dans Citrix ADM, accédez à **Réseaux** > Tableau de **bord SSL** .



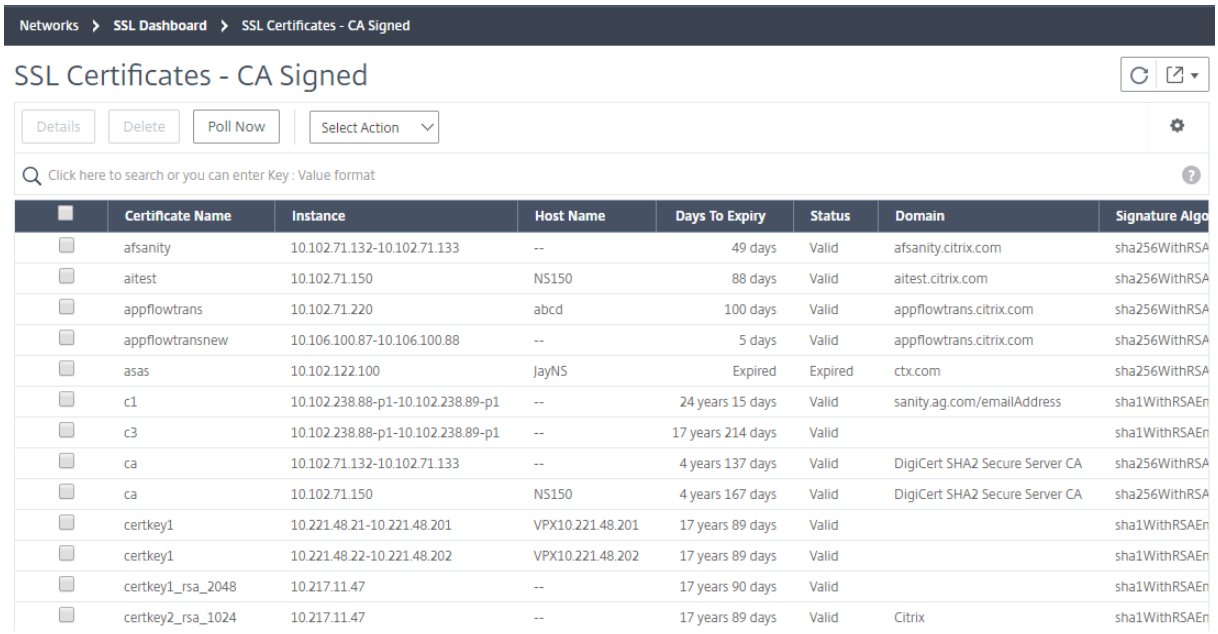
Citrix ADM vous permet d'interroger les certificats SSL et d'ajouter immédiatement tous les certificats SSL des instances à Citrix ADM. Pour ce faire, accédez à **Réseaux** > Tableau de **bord SSL** et cliquez sur **Interroger maintenant**. La page **Sondage maintenant** apparaît, présentant l'option permettant d'interroger toutes les instances de Citrix ADC dans le réseau ou d'interroger les instances sélectionnées.



Vous pouvez utiliser le tableau de bord Citrix ADM SSL pour afficher ou surveiller les détails des certificats SSL, 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 numéro 30 sous « Auto-signé vs. Autorité de certification signée » dans la figure ci-dessus, une nouvelle fenêtre apparaît, montrant les détails des 30 certificats SSL sur les instances de Citrix ADC.

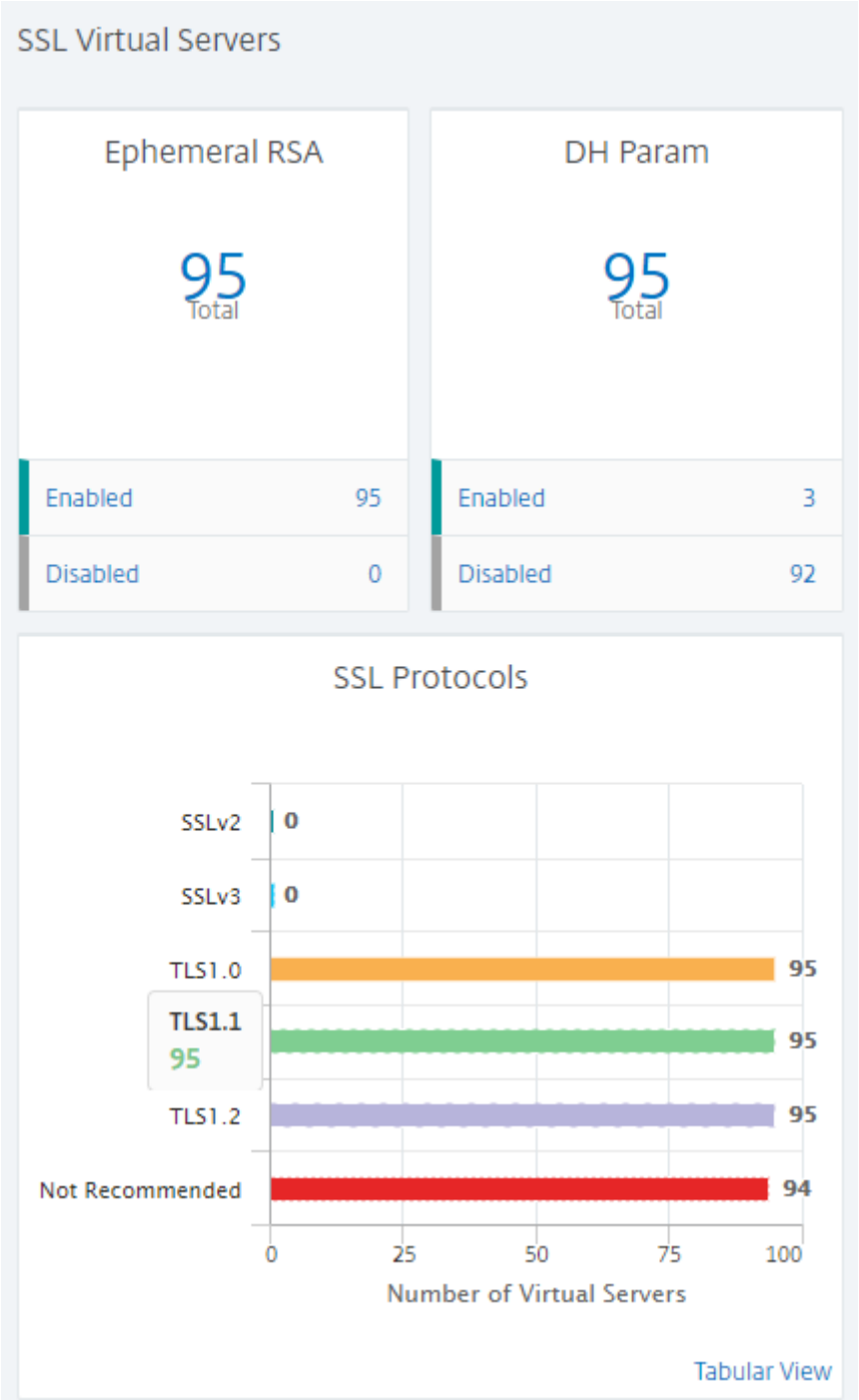


Certificate Name	Instance	Host Name	Days To Expiry	Status	Domain	Signature Algo
afsanity	10.102.71.132-10.102.71.133	--	49 days	Valid	afsanity.citrix.com	sha256WithRSA
aitest	10.102.71.150	NS150	88 days	Valid	aitest.citrix.com	sha256WithRSA
appflowtrans	10.102.71.220	abcd	100 days	Valid	appflowtrans.citrix.com	sha256WithRSA
appflowtransnew	10.106.100.87-10.106.100.88	--	5 days	Valid	appflowtrans.citrix.com	sha256WithRSA
asas	10.102.122.100	JayNS	Expired	Expired	ctx.com	sha256WithRSA
c1	10.102.238.88-p1-10.102.238.89-p1	--	24 years 15 days	Valid	sanity.ag.com/emailAddress	sha1WithRSAEn
c3	10.102.238.88-p1-10.102.238.89-p1	--	17 years 214 days	Valid		sha1WithRSAEn
ca	10.102.71.132-10.102.71.133	--	4 years 137 days	Valid	DigiCert SHA2 Secure Server CA	sha256WithRSA
ca	10.102.71.150	NS150	4 years 167 days	Valid	DigiCert SHA2 Secure Server CA	sha256WithRSA
certkey1	10.221.48.21-10.221.48.201	VPX10.221.48.201	17 years 89 days	Valid		sha1WithRSAEn
certkey1	10.221.48.22-10.221.48.202	VPX10.221.48.202	17 years 89 days	Valid		sha1WithRSAEn
certkey1_rsa_2048	10.217.11.47	--	17 years 90 days	Valid		sha1WithRSAEn
certkey2_rsa_1024	10.217.11.47	--	17 years 89 days	Valid	Citrix	sha1WithRSAEn

Le tableau de bord SSL Citrix ADM affiche également la distribution des protocoles SSL qui s'exécutent sur vos serveurs virtuels. En tant qu'administrateur, vous pouvez spécifier les protocoles que vous souhaitez surveiller via la stratégie SSL. Pour plus d'informations, reportez-vous à la section Configuration des stratégies SSL. Les protocoles pris en charge sont SSLv2, SSLv3, 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 lorsque 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

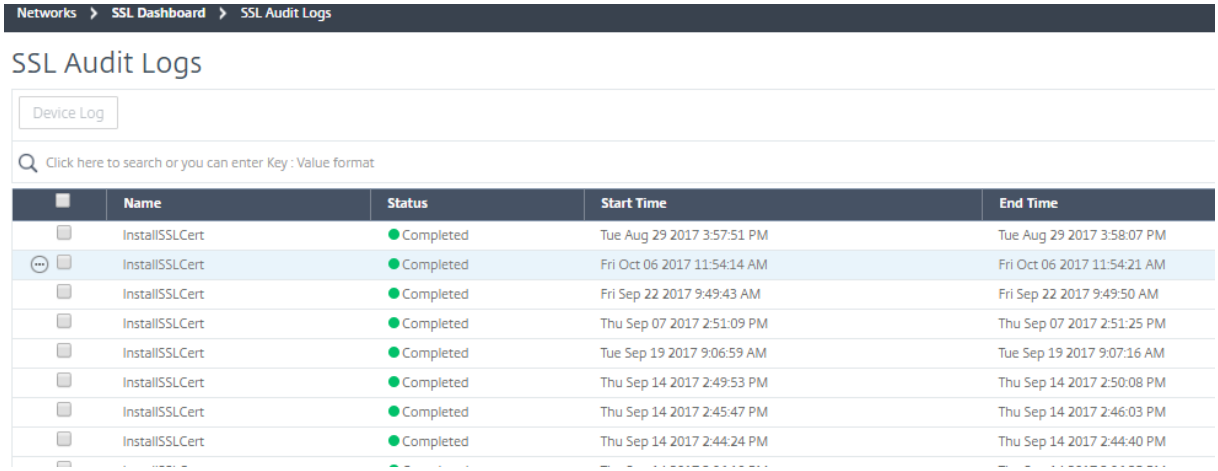
clients d'exportation même si le certificat de serveur ne prend pas en charge les clients d'exportation, comme dans le cas d'un certificat 1024 bits. Cliquez sur le graphique approprié pour afficher la liste des serveurs virtuels sur lesquels les clés DH ou Ephemeral RSA sont activées.



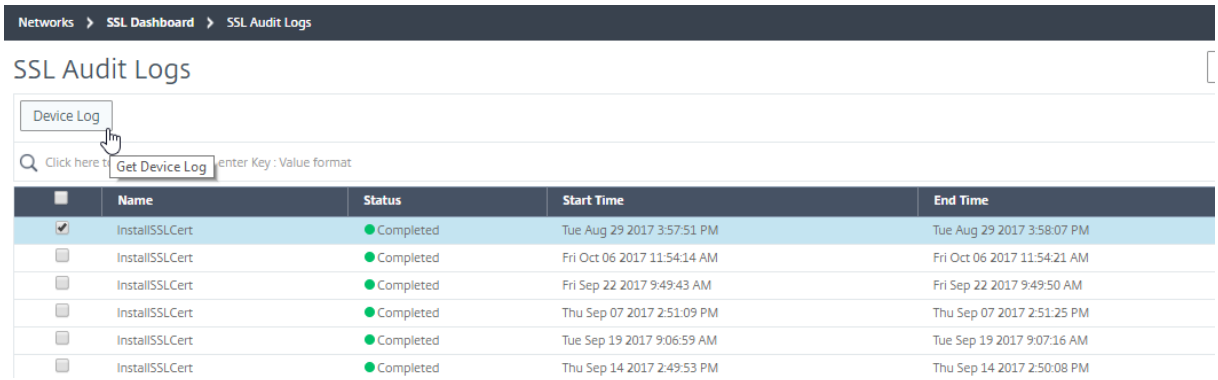
Afficher les journaux d'audit pour les certificats SSL

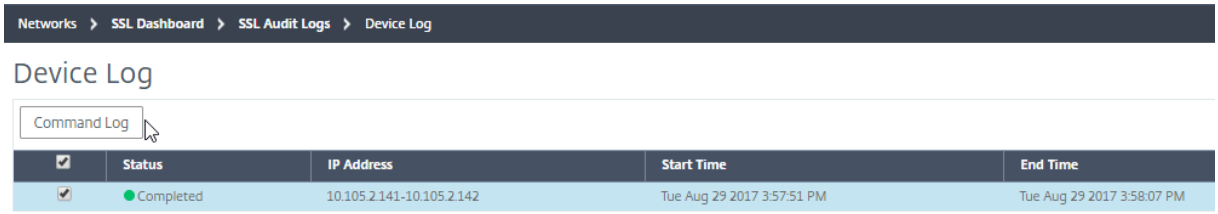
Vous pouvez maintenant afficher les détails du journal des certificats SSL sur Citrix ADM. Les détails du journal affichent les opérations effectuées à l'aide de certificats SSL sur Citrix ADM, telles que : installation de certificats SSL, liaison et dissociation de certificats SSL, mise à jour de certificats SSL et suppression de certificats SSL. Les informations du journal d'audit sont utiles lors de la surveillance des modifications de certificat SSL effectuées sur une application avec plusieurs propriétaires.

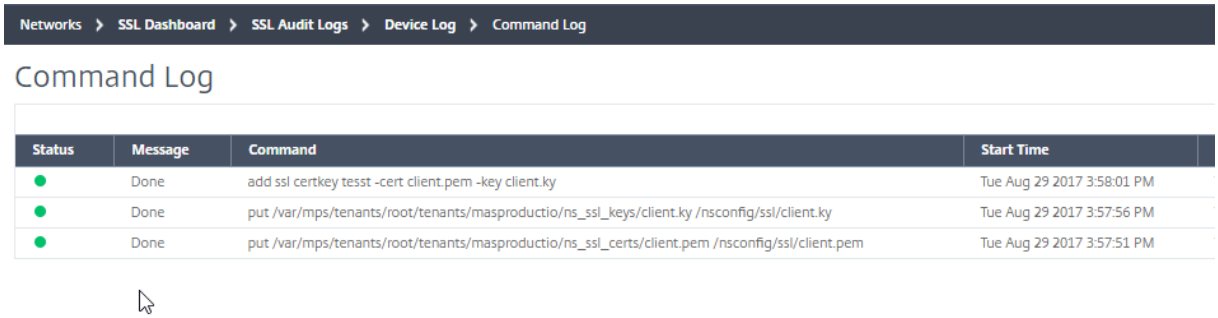
Pour afficher un journal d'audit pour une opération particulière effectuée sur Citrix ADM à l'aide de certificats SSL, accédez à **Réseaux** > Tableau de **bord SSL** et sélectionnez **Journaux d'audit** .



Pour une opération particulière effectuée à l'aide du certificat SSL, vous pouvez afficher son état, son heure de début et son heure de fin. En outre, vous pouvez afficher l'instance sur laquelle l'opération a été effectuée et les commandes s'exécutent sur cette instance.





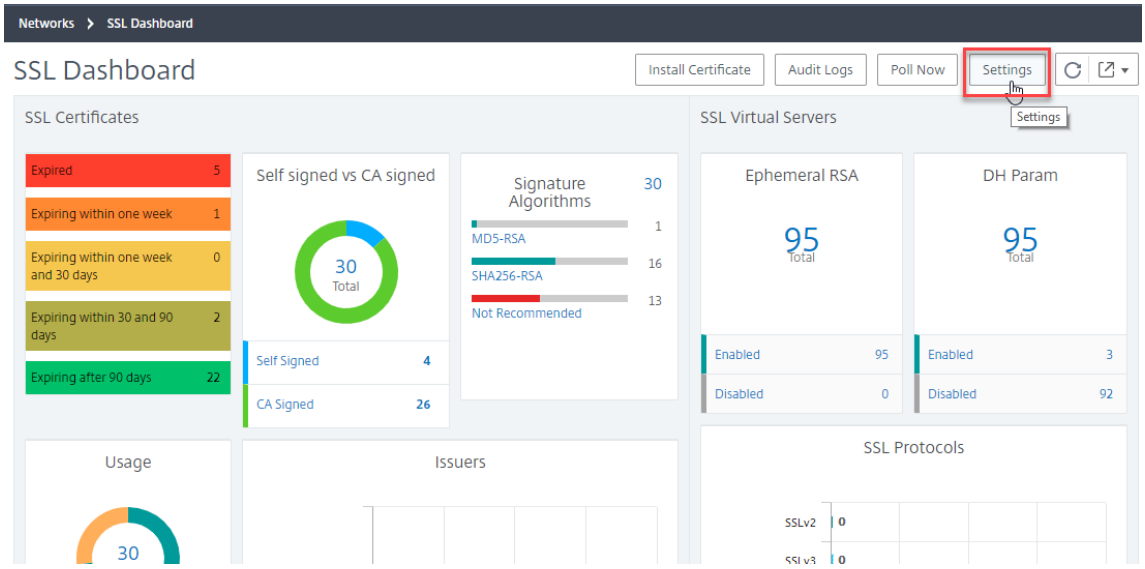


Exclure les certificats Citrix ADC par défaut sur le tableau de bord SSL

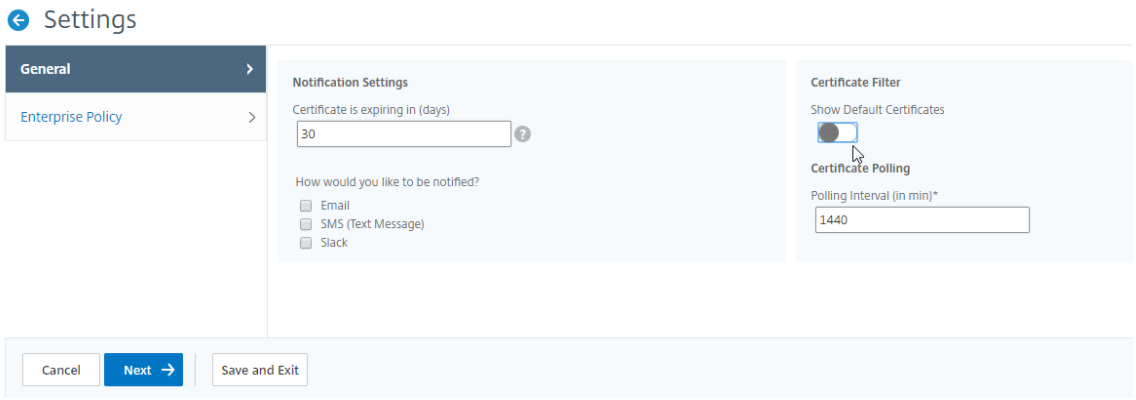
Citrix ADM vous permet d'afficher ou de masquer les certificats par défaut qui apparaissent sur les graphiques SSL Dashboard en fonction de vos préférences. Par défaut, tous les certificats sont affichés sur le tableau de bord SSL, y compris les certificats par défaut.

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 graphique Citrix ADM.
2. Sur la page **Tableau de bord SSL**, cliquez sur **Paramètres**.



3. Dans la page **Paramètres**, sélectionnez **Général** .
4. Dans la section **Filtre de certificat**, désactivez l'option **Afficher les certificats par défaut** et sélectionnez **Enregistrer et quitter** .



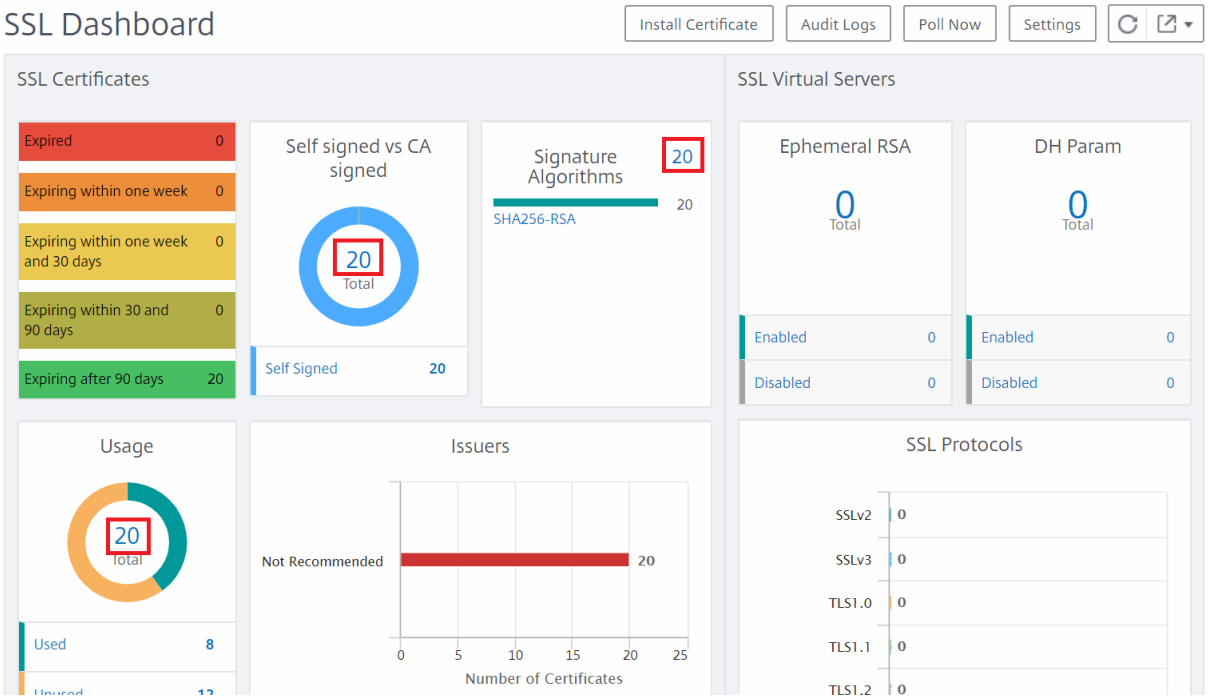
Télécharger les certificats SSL

Les certificats SSL doivent être gérés individuellement par instance. Citrix ADM fournit une visibilité sur tous les certificats déployés sur plusieurs instances.

- Vous pouvez sélectionner les certificats qui expirent et automatiser les renouvellements de certificats.
- Les stratégies peuvent être définies et appliquées en fonction des types de certificats et de pouvoirs de signature autorisés.
- Vous pouvez également télécharger les certificats SSL pour renouvellement et les télécharger ultérieurement.

Pour télécharger les certificats 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 le nombre total de certificats SSL dans l'un des graphiques.



1. Sur la page **Certificats SSL**, cliquez sur le certificat que vous souhaitez télécharger. Par exemple, vous voulez télécharger celui qui expire dans la semaine suivante.
2. **Dans la zone de liste Sélectionner une action**, sélectionnez **Télécharger** .
3. Le certificat est téléchargé sur votre système.

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 quotidiennement, hebdomadaire ou mensuel et envoyer le rapport par e-mail ou par un message de marge.

> **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 notifications pour l'expiration du certificat SSL

April 29, 2021

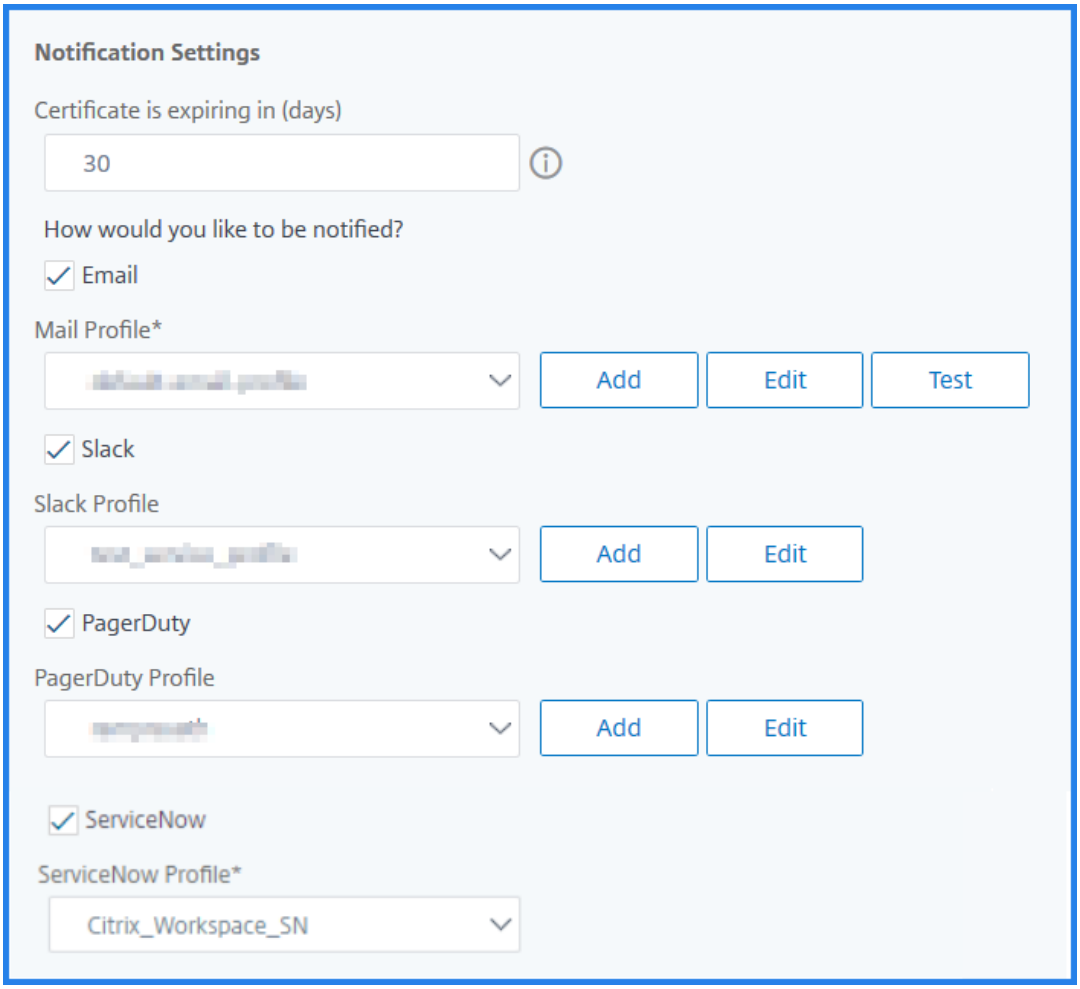
En tant qu'administrateur de sécurité, vous pouvez configurer des notifications lorsque les certificats sont sur le point d'expirer et inclure des informations sur les instances Citrix ADC qui utilisent ces certificats. En activant les notifications, vous pouvez renouveler vos certificats SSL à temps.

Par exemple, vous pouvez définir une notification par e-mail pour qu'une liste de distribution par e-mail soit envoyée 30 jours avant l'expiration de votre certificat.

Pour configurer des notifications à partir de Citrix ADM :

1. Dans Citrix ADM, accédez à **Réseaux** > **Tableau de bord SSL**.
2. Dans la page **Tableau de bord SSL**, cliquez sur **Paramètres** .
3. Dans la page **Paramètres**, cliquez sur **Général** .
4. Dans la section **Paramètres de notification**, indiquez quand 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. 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.
    - **Slack** : spécifiez un profil de marge. Une notification est envoyée lorsque vos certificats sont sur le point d'expirer.
    - **PagerDuty** - Spécifiez un profil PagerDuty. En fonction des paramètres de notification configurés dans votre portail PagerDuty, une notification est envoyée lorsque vos certificats sont sur le point d'expirer.
    - **ServiceNow** - Une notification est envoyée au profil ServiceNow par défaut lorsque vos certificats sont sur le point d'expirer.

      > **Important**
      >
      > Assurez-vous que Citrix Cloud ITSM Adapter est configuré pour ServiceNow et intégré au service Citrix ADM. Pour de plus amples informations, consultez la section Intégrer Citrix ADM Service à l'instance ServiceNow.



6. Cliquez sur **Enregistrer et quitter**.

Mettre à jour un certificat installé

April 29, 2021

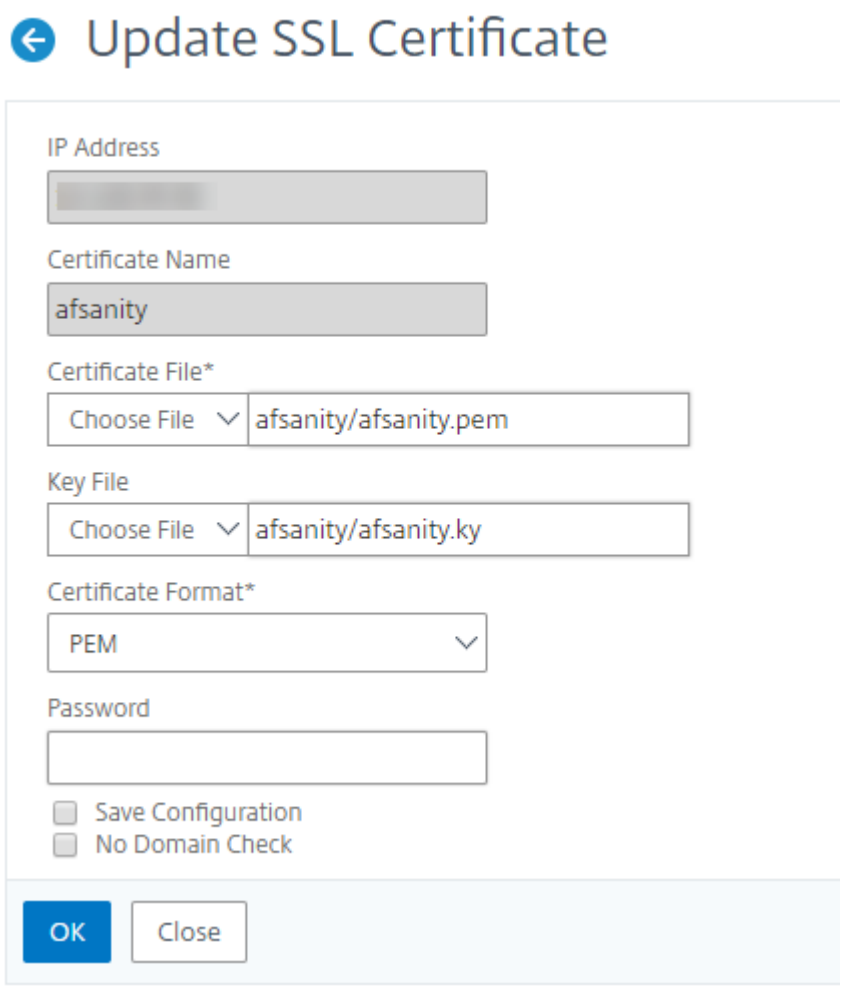
Après avoir reçu un certificat renouvelé de l'autorité de certification, vous pouvez mettre à jour les certificats existants à partir de Citrix Application Delivery Management (Citrix ADM) sans avoir à ouvrir une session sur des instances Citrix ADC individuelles.

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 de Citrix ADC

April 29, 2021

Avant d'installer des certificats SSL sur des instances de Citrix ADC, 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 2 048 bits ou plus et que les clés sont signées avec des algorithmes de signature sécurisés.

Pour installer un certificat SSL à partir d'une autre instance d'Citrix ADC :

Vous pouvez également importer un certificat à partir d'une instance d'Citrix ADC choisie et l'appliquer à d'autres instances d'ADC Citrix ciblées à partir de l'interface graphique d'Citrix ADM.

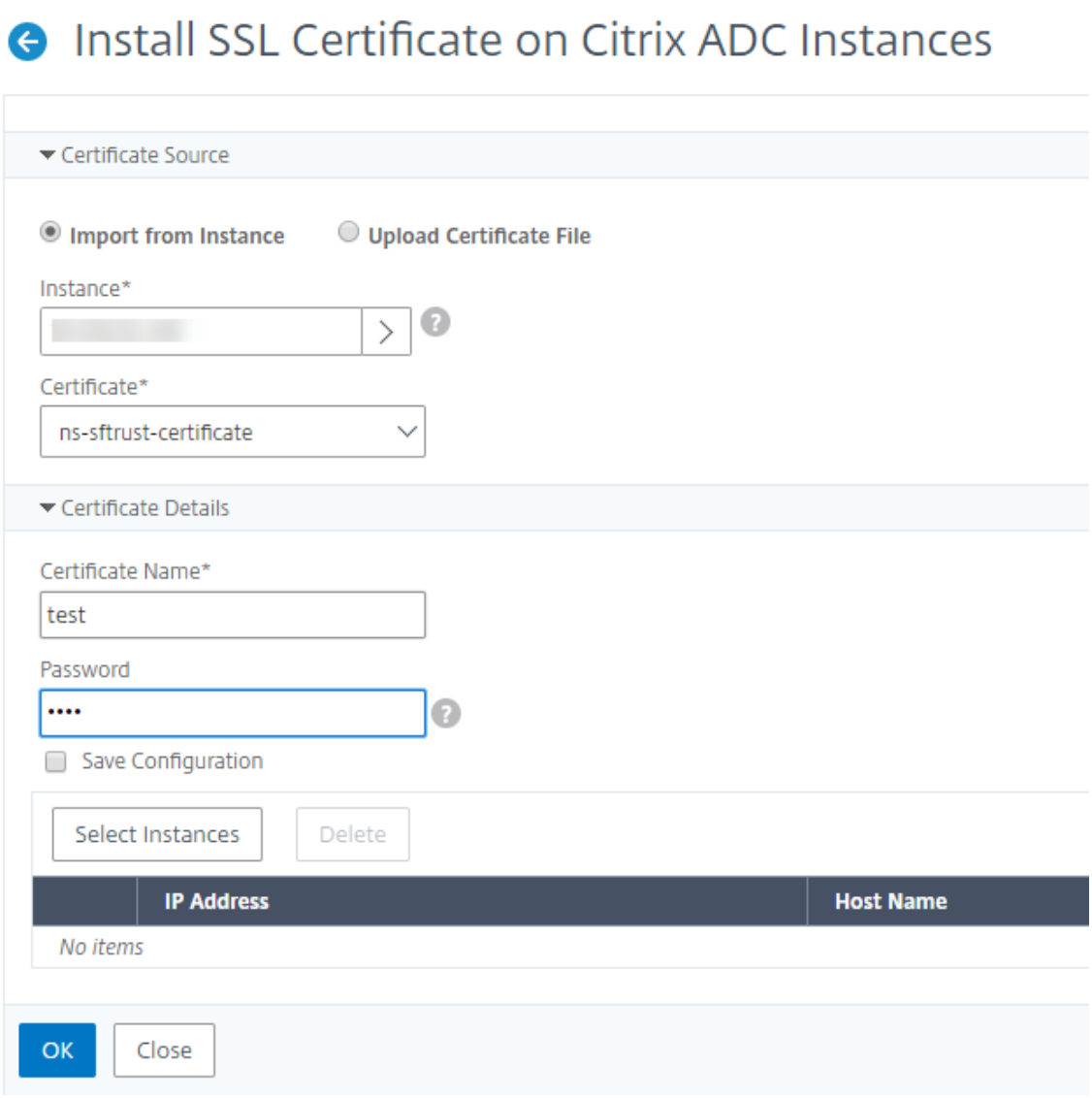
1. Accédez à **Réseaux** > **Tableau de bord SSL**.
2. Dans l'angle supérieur droit du tableau de bord SSL, cliquez sur **Installer le certificat**.
3. Sur la page **Installer un certificat SSL sur les instances Citrix ADC**, spécifiez les paramètres suivants :
   a) Source du certificat

      Sélectionnez l'option **Importer à partir d'une instance**.

      - Choisissez l'**instance** à partir de laquelle vous souhaitez importer le certificat.
      - Choisissez le **certificat** dans la liste de tous les fichiers de certificat SSL de l'instance.

   b) Détails du certificat

      - **Nom du certificat**. Spécifiez un nom pour la clé de certificat.
      - **Mot de passe**. Mot de passe pour crypter la clé privée. Vous pouvez utiliser cette option pour télécharger des clés privées chiffrées.
4. Cliquez sur **Sélectionner les instances** pour sélectionner les instances Citrix ADC sur lesquelles vous souhaitez installer vos certificats.
5. Cliquez sur **OK**.

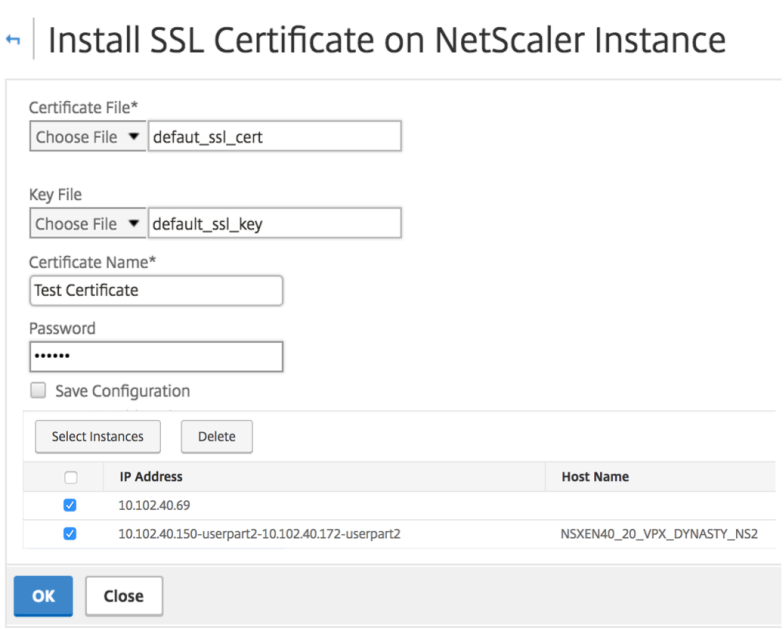


Pour installer un certificat SSL à partir de Citrix ADM :

1. Dans Citrix ADM, accédez à **Réseaux** > **Tableau de bord SSL**.
2. Dans le coin supérieur droit du tableau de bord, cliquez sur **Installer le certificat**.
3. Sur la page **Installer un certificat SSL sur une instance Citrix ADC**, spécifiez les paramètres suivants :
   - **Fichier de certificat** : chargez un fichier de certificat SSL en sélectionnant **Local** (votre machine locale) ou **Appliance** (le fichier de certificat doit être présent sur l'instance virtuelle Citrix ADM).
   - **Fichier clé** : téléchargez le fichier clé.
   - **Nom du certificat** : spécifiez un nom pour 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 ADC sur lesquelles vous souhaitez installer vos certificats.

4. Pour enregistrer la configuration pour une utilisation ultérieure, activez la case à cocher **Enregistrer la configuration** .
5. Cliquez sur **OK**.



Créer une demande de signature de certificat (CSR)

April 29, 2021

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 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 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 une CSR** dans la liste déroulante **Sélectionner une action**.

3. Dans la page **Créer une demande de signature de certificat (CSR)**, spécifiez un nom pour la CSR.
4. Procédez comme suit :
   - **Télécharger une clé** - Sélectionnez l'option **J'ai une clé** . Pour charger votre fichier de clé, sélectionnez **Local** (votre machine locale) ou **Appliance** (le fichier de clé doit être présent sur l'instance virtuelle Citrix ADM).
   - **Créer une clé** - Sélectionnez l'option **Je n'ai pas de clé**, puis spécifiez les paramètres suivants :

Algorithme de chiffrement	Type de clé. Par exemple, RSA.
Nom du fichier clé	Nom du fichier dans lequel la clé RSA est stockée.
Taille de la clé	Taille de la clé en bits.
Valeur de l'exposant public	Choisissez **3** ou **F4** dans la liste déroulante fournie. Cette valeur fait partie de l'algorithme de chiffrement requis pour créer votre clé RSA.
Format de clé	Le PEM par défaut est sélectionné. PEM est le format de clé recommandé pour votre certificat SSL.
Algorithme d'encodage PEM	Dans la liste déroulante, sélectionnez l'algorithme (**DES** ou **DES3**) à utiliser pour chiffrer la clé RSA générée. Si vous sélectionnez cet algorithme, vous devez fournir une phrase secrète PEM.
Passphrase PEM	Si vous avez choisi l'algorithme d'encodage PEM, entrez une phrase secrète.
Confirmer la phrase secrète PEM	Confirmez votre phrase secrète PEM.

5. Cliquez sur **Continue**.
6. Sur la page suivante, fournissez plus de détails.

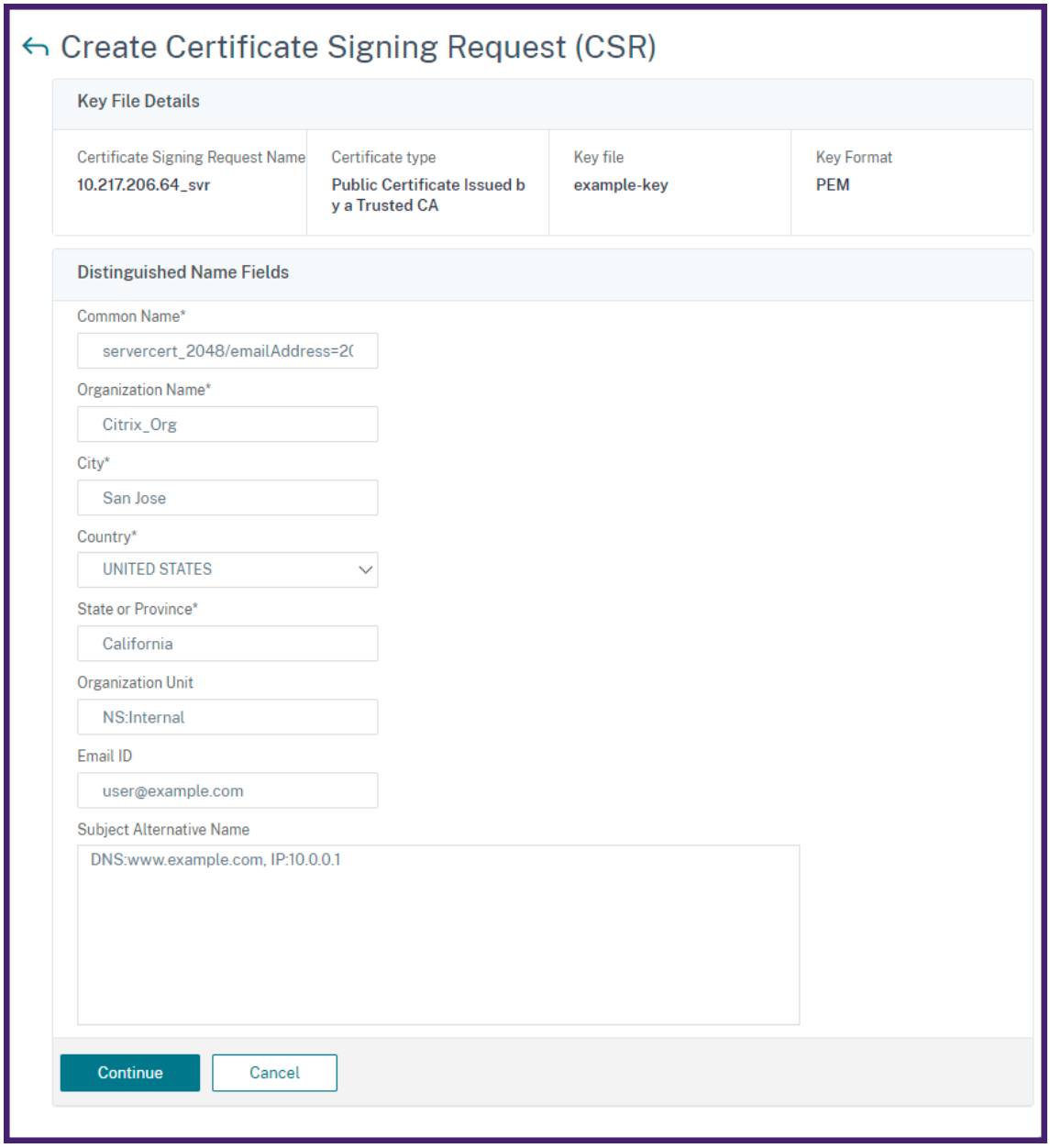
   La plupart des champs ont des valeurs par défaut extraites de l'objet du certificat sélectionné. L'objet contient des détails tels que le nom commun, le nom de l'organisation, l'état et le pays.

   Dans le champ **Nom alternatif de l'objet**, vous pouvez spécifier plusieurs valeurs, telles que des noms de domaine et des adresses IP avec un seul certificat. Les noms alternatifs d'objet

vous aident à sécuriser plusieurs domaines avec un seul certificat.

Spécifiez les noms de domaine et les adresses IP dans le format suivant :

```
DNS:<Domain name>, IP:<IP address>
<!--NeedCopy-->
```



Dans cet exemple, il sécurise `10.0.0.1` et `www.example.com`.

Vérifiez les champs et cliquez sur **Continuer**.

> **Remarque**
>
> La plupart des autorités de certification acceptent les soumissions de certificats par courriel. L'autorité de certification renvoie un certificat valide à l'adresse e-mail à partir de laquelle vous soumettez le CSR.

Liaison et dissociation des certificats SSL

April 29, 2021

Vous créez un ensemble de certificats en liant plusieurs certificats ensemble. 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 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 **Sélectionner une 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 liés, puis sélectionnez **Unlink** dans la liste déroulante **Sélectionner une 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

April 29, 2021

Vous pouvez configurer une stratégie d'entreprise et ajouter toutes les autorités de certification approuvées, les algorithmes de signature sécurisés et sélectionner la force de clé recommandée pour vos clés de certificat dans Citrix Application Delivery Management (Citrix ADM). Si l'un des certificats installés sur votre instance Citrix 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.

En outre, si la force de la clé de certificat ne correspond pas à celle recommandée dans la stratégie d'entreprise, le tableau de bord du certificat SSL affiche les forces de ces clés comme Non recommandé.

Pour configurer une stratégie d'entreprise sur Citrix ADM :

1. Dans Citrix ADM, accédez à **Réseaux** > **Tableau de bord SSL**, puis cliquez sur **Paramètres** .
2. Dans la page **Paramètres**, cliquez sur l'icône **Stratégie d'entreprise** pour ajouter toutes les autorités de certification approuvées, des algorithmes de signature sécurisés, puis sélectionnez la force de clé recommandée pour vos certificats et clés.
    - **Points forts clés recommandés** - Indique la sécurité de l'algorithme et le nombre de bits dans une clé.
    - **Algorithmes de signature recommandés** - Indique les problèmes de jetons signés pour les applications.
    - **Autorité de certification approuvée recommandée** : désigne l'entité approuvée qui émet les certificats numériques. Cliquez sur l'icône **+** pour ajouter d'autres entités.
    - **Protocoles SSL recommandés** - Indique les versions TLS/SSL.
3. Cliquez sur **Terminer** ou **Enregistrer et quitter** pour enregistrer votre stratégie d'entreprise.

Étudier les certificats SSL à partir d'instances de Citrix ADC

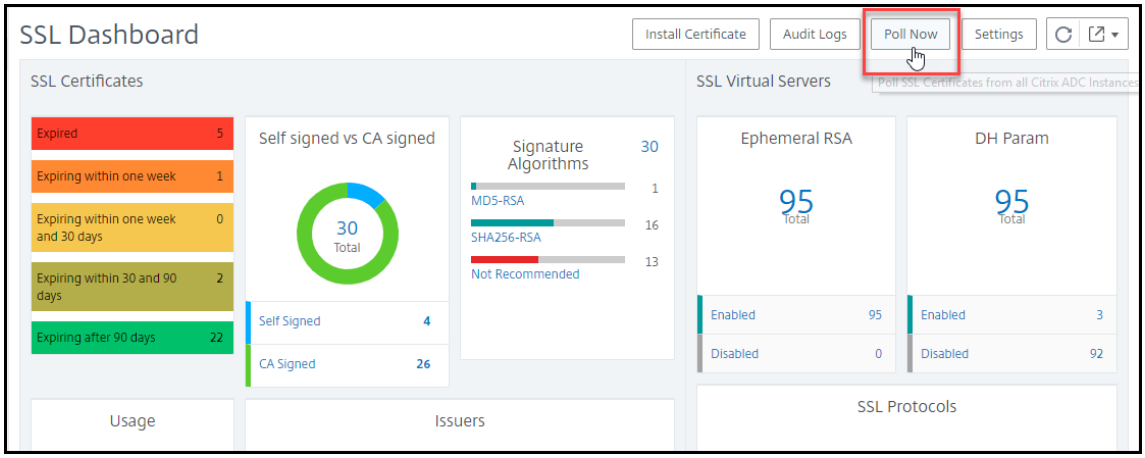
April 29, 2021

Citrix Application Delivery Management (Citrix ADM) interroge automatiquement les certificats SSL une fois toutes les 24 heures à l'aide des appels NITRO et du protocole SCP (Secure Copy). Vous pouvez également interroger manuellement les certificats SSL pour découvrir les certificats SSL nouvellement ajoutés sur les instances Citrix ADC. L'interrogation de toutes les instances de Citrix ADC certificats SSL impose une lourde charge sur le réseau.

Au lieu d'interroger tous les certificats SSL d'instances Citrix ADC, vous pouvez interroger manuellement uniquement les certificats SSL d'une ou plusieurs instances sélectionnées.

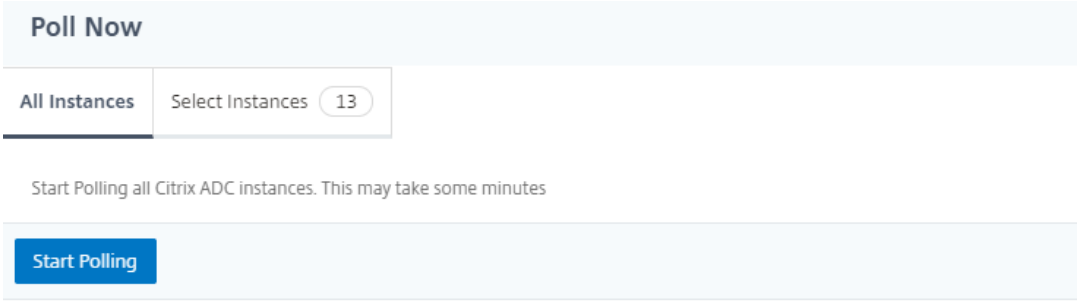
Pour interroger les certificats SSL sur les instances Citrix ADC :

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** .

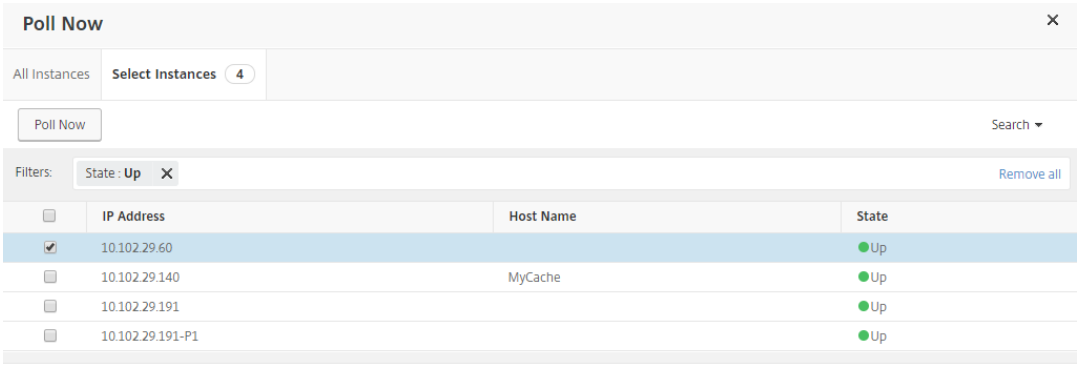


3. La page **Interroger maintenant** apparaît, vous donnant la possibilité d'interroger toutes les instances Citrix ADC dans le réseau ou d'interroger les instances sélectionnées.

   - Pour interroger les certificats SLL de toutes les instances Citrix ADC, sélectionnez l'onglet **Toutes les instances** et cliquez sur **Démarrer l'interrogation**.



   - Pour interroger des instances spécifiques, sélectionnez l'onglet **Sélectionner des instances**, sélectionnez les instances dans la liste, puis cliquez sur **Sondage maintenant**.



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 quotidiennement, hebdomadaire ou mensuel et envoyer le rapport par e-mail ou par un message de marge.

> **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 la gestion des adresses IP (IPAM)

April 29, 2021

ADM IPAM vous permet d'attribuer et de libérer automatiquement des adresses IP dans les configurations gérées par ADM. Vous pouvez attribuer des adresses IP à partir de réseaux ou de plages d'adresses IP définies à l'aide des fournisseurs IP suivants :

- Fournisseur IPAM intégré ADM.
- Solution IPAM Infoblox. Pour de plus amples informations, consultez la section Infoblox DDI.

Actuellement, vous pouvez utiliser ADM IPAM dans :

- **StyleBooks** : allouer automatiquement des adresses IP aux serveurs virtuels lorsque vous créez des configurations.
- **Ingress de Kubernetes** : Affectez automatiquement une adresse IP virtuelle à une configuration d'entrée dans un cluster Kubernetes.

- **Passerelle API** : allouer automatiquement une adresse IP au proxy de l'API.

Vous pouvez également suivre les adresses IP allouées et disponibles dans chaque réseau ou plage d'adresses IP gérée par ADM.

Ajouter un fournisseur d'adresses IP externe

ADM dispose d'un fournisseur IPAM intégré pour gérer les adresses IP et les plages d'adresses IP. Vous pouvez également ajouter un fournisseur d'adresses IP externe à ADM.

> **Important**
>
> Avant de commencer, assurez-vous que les autorisations suivantes sont activées dans le fournisseur d'adresses IP externe :
>
> - Possibilité d'interroger les réseaux présents dans le fournisseur.
> - Enregistrez un nouveau réseau.
> - Désinscrire un réseau existant.
> - Réserver une adresse IP dans le réseau.
> - Libérez une adresse IP du réseau.
> - Récupérer les adresses IP utilisées à partir d'un réseau.
> - Récupérer les adresses IP disponibles à partir d'un réseau.

Procédez comme suit pour ajouter une solution de fournisseur IP externe dans ADM :

1. Accédez à **Réseaux > IPAM**.
2. Dans **Fournisseurs**, cliquez sur **Ajouter**.
3. Spécifiez les détails suivants pour ajouter un fournisseur IP :
   - **Nom** : spécifiez le nom du fournisseur IP à utiliser dans ADM.
   - **Fournisseur** - Sélectionnez un fournisseur IPAM dans la liste.
   - **URL :** spécifiez l'URL de la solution IPAM qui attribue des adresses IP dans un environnement ADM. Veillez à spécifier l'URL dans le format suivant :

     ```
     https://<host name>
     <!--NeedCopy-->
     ```

     Exemple : `https://myinfoblox.example.com`
   - **Nom d'utilisateur** : spécifiez le nom d'utilisateur pour vous connecter à la solution IPAM.
   - **Mot de passe** : spécifiez le mot de passe pour vous connecter à la solution IPAM.
4. Cliquez sur **Add**.

Ajouter un réseau

Ajoutez un réseau pour utiliser IPAM avec les configurations gérées ADM.

1. Accédez à **Réseaux > IPAM**.
2. Dans **Réseaux**, cliquez sur **Ajouter**.
3. Spécifiez les détails suivants :
   - **Nom du réseau** : spécifiez le nom du réseau pour identifier le réseau dans ADM.
   - **Fournisseur** : sélectionnez le fournisseur dans la liste.

     Cette liste affiche les fournisseurs ajoutés dans ADM.
   - **Type de réseau** : sélectionnez **Gamme IP** ou **CIDR** dans la liste en fonction de vos besoins.
   - **Valeur du réseau** : spécifiez la valeur du réseau.

     > **Remarque**
     >
     > ADM IPAM ne prend en charge que les adresses IPv4.

     Pour la **plage IP**, spécifiez la valeur réseau au format suivant :

     ```
     <first-IP-address>-<last-IP-address>
     <!--NeedCopy-->
     ```

     Exemple :

     ```
     10.0.0.20-10.0.0.100
     <!--NeedCopy-->
     ```

     Pour **CIDR**, spécifiez la valeur réseau au format suivant :

     ```
     <IP-address>/<subnet-mask>
     <!--NeedCopy-->
     ```

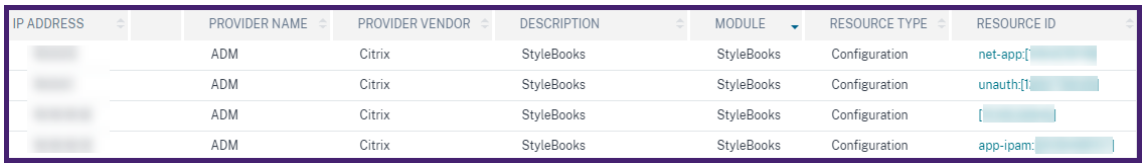
     Exemple :

     ```
     10.70.124.0/24
     <!--NeedCopy-->
     ```
4. Cliquez sur **Créer**.

Afficher les adresses IP allouées

Pour afficher plus de détails sur les adresses IP allouées à partir du réseau IPAM, procédez comme suit :

1. Accédez à **Réseaux > IPAM**.
2. Dans l'onglet **Réseaux**, cliquez sur **Afficher toutes les adresses IP allouées**.



Ce volet affiche l'adresse IP, le nom du fournisseur, le fournisseur et la description. Il affiche également les détails de la ressource qui a réservé cette adresse IP :

- **Module** : Affiche le module ADM qui a réservé l'adresse IP. Par exemple, si StyleBooks a réservé l'adresse IP, cette colonne affiche StyleBooks comme module.
- **Type de ressource** : Affiche le type de ressource dans ce module. Pour le module StyleBooks, seul le type de ressource configurations utilise le réseau IPAM. Ainsi, il affiche Configurations sous cette colonne.
- **ID de ressource** : affiche l'ID de ressource exact avec un lien. Cliquez sur ce lien pour accéder à la ressource qui utilise l'adresse IP. Pour le type de ressource de configuration, il affiche l'ID du pack de configuration en tant qu'ID de ressource.

> **Remarque**
>
> Si vous souhaitez libérer l'adresse IP, sélectionnez l'adresse IP à publier et cliquez sur **Libérer les adresses IP allouées**.

Travaux de configuration

April 29, 2021

Le processus de gestion de la configuration de Citrix Application Delivery Management (ADM) garantit la réplication correcte des modifications de configuration, des mises à niveau du système et d'autres activités de maintenance sur plusieurs instances de Citrix ADC dans le réseau.

Citrix ADM vous permet de créer des tâches de configuration qui vous aident à effectuer toutes ces activités facilement sur plusieurs appareils en une seule tâche. Les tâches de configuration et les modèles simplifient les tâches administratives les plus répétitives en une seule tâche sur Citrix ADM. Une tâche de configuration contient un ensemble de commandes de configuration que vous pouvez exécuter sur un ou plusieurs périphériques gérés.

Les tâches de configuration peuvent soit utiliser des commandes SSH pour effectuer des commandes de configuration, soit utiliser SCP pour copier des fichiers à partir de 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 jouer

Modèle de configuration :

Vous pouvez créer des modèles de configuration tout en créant un travail et en enregistrant un ensemble de commandes de configuration en tant que modèle. Lorsque vous enregistrez ces modèles sur la page Créer des travaux, ils s'affichent automatiquement dans la page Créer un modèle .

> **Remarque**
> L'option **Renommer** est désactivée pour les modèles de configuration par défaut. Toutefois, vous pouvez renommer des modèles de configuration personnalisés.

Vous pouvez utiliser l'un des modèles suivants :

Éditeur de configuration : vous pouvez utiliser l'éditeur de configuration pour taper 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 leurs descriptions dans le tableau ci-dessous. Vous pouvez planifier une tâche à l'aide de l'option de modèle intégrée. Un travail est un ensemble de commandes de configuration que vous pouvez exécuter sur une ou plusieurs instances gérées. Par exemple, vous pouvez utiliser l'option de modèle intégrée pour planifier une tâche de configuration des serveurs syslog. Vous pouvez également choisir d'exécuter le travail immédiatement ou de planifier l'exécution ultérieure.

Instance :

Vous pouvez effectuer une mise à niveau groupée unique de vos instances Citrix ADC SDX exécutant Citrix ADC version 11.0 et ultérieure. Pour effectuer une mise à niveau groupée unique, vous utilisez une tâche intégrée dans Citrix ADM. 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. Cette mise à niveau 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.
- Tout type de formatage n'est pas requis.
- Le fichier peut être enregistré sur votre ordinateur local.

Vous pouvez soit créer et enregistrer un nouveau fichier, soit importer un fichier existant, puis exécuter les commandes.

Enregistrer et jouer :

À l'aide de Create job, vous pouvez entrer vos propres commandes CLI, ou vous pouvez utiliser le bouton Enregistrer et lire pour obtenir les commandes d'une session Citrix ADC. Lorsque vous exécutez le travail, les modifications apportées au fichier ns.conf sur l'instance sélectionnée sont enregistrées et copiées dans Citrix ADM.

Articles connexes

- Comment utiliser la commande SCP (put) dans les travaux de configuration
- Comment utiliser des variables dans les travaux de configuration
- Procédure de création de tâches de configuration à partir de commandes correctives
- Procédure d'utilisation des 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 principale sur Citrix ADM

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 quotidiennement, hebdomadaire ou mensuel et envoyer le rapport par e-mail ou par un message de marge.

> **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.

Créer une tâche de configuration

April 29, 2021

Un travail 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. Vous pouvezrépliquer des configurations sur plusieurs instancessur votre réseau et enregistrement et lecture des tâches de configurationà l'aide de Citrix Application Delivery Management (ADM) et le convertir en commandes CLI.

Vous pouvez utiliser la fonctionnalité Travaux de configuration de Citrix ADM pour créer une tâche de configuration, envoyer des notifications par e-mail et vérifier les journaux d'exécution des tâches créées.

Pour créer une tâche de configuration sur Citrix ADM :

1. Accédez à **Réseaux** > **Travaux de configuration** .
2. Cliquez sur **Créer un travail**.
3. 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.
4. Dans la liste **Source de configuration**, sélectionnez le modèle de tâche de configuration que vous souhaitez créer. Ajoutez les commandes du modèle sélectionné.
    - Vous pouvez entrer les commandes ou importer les commandes existantes à partir des modèles de configuration enregistrés.
    - Vous pouvez également ajouter plusieurs modèles de différents types dans l'éditeur de configuration tout en créant une tâche dans les tâches de configuration.
    - Dans la liste **Source de configuration**, sélectionnez les différents modèles, puis faites glisser les modèles dans l'éditeur de configuration. Les types de modèle peuvent être **Modèle de configuration**, **Modèle intégré**, **Configuration principale**, **Enregistrement et lecture**, **Instance**et **Fichier**.

    > **Remarque**
    >
    > Si vous ajoutez le modèle Déployer la tâche de configuration principale pour la première fois, ajoutez un modèle de type différent, l'ensemble du modèle de tâche devient un type de configuration principale.

    Vous pouvez également réorganiser et réorganiser les commandes dans l'éditeur de configuration. Vous pouvez déplacer la commande d'une ligne à l'autre en faisant glisser la ligne de commande. Vous pouvez également déplacer ou réorganiser la ligne de commande d'une ligne à

n'importe quelle ligne cible en changeant simplement le numéro de ligne de commande dans la zone de texte. Vous pouvez également réorganiser et réorganiser la ligne de commande lors de la modification du travail de configuration.

Vous pouvez définir des variables qui vous permettent d'affecter des valeurs différentes pour ces paramètres ou d'exécuter un travail sur plusieurs instances. Vous pouvez consulter toutes les variables que vous avez définies lors de la création ou de la modification d'un travail de configuration dans une vue consolidée unique. Cliquez sur l'onglet **Aperçu des variables** pour prévisualiser les variables dans une vue consolidée unique que vous avez définie lors de la création ou de la modification d'un travail de configuration.

Vous pouvez personnaliser les commandes d'annulation pour chaque commande de l'éditeur de configuration. Pour spécifier vos commandes personnalisées, activez l'option de restauration personnalisée.

> **Important**
>
> Pour que la restauration personnalisée prenne effet, exécutez l'Assistant **Créer un travail**. Et dans l'onglet **Exécuter**, sélectionnez l'option **Annuler les commandes réussies** dans **la liste En échec de commande** .

5. Dans l'onglet **Sélectionner des instances**, sélectionnez les instances sur lesquelles vous souhaitez exécuter l'audit de configuration.

   a) Dans une paire Citrix ADC haute disponibilité, vous pouvez exécuter un travail de configuration local sur un nœud principal ou secondaire. Sélectionnez le nœud sur lequel vous souhaitez exécuter la tâche.

      - **Exécuter sur les nœuds principaux** - Sélectionnez cette option pour exécuter le travail uniquement sur les nœuds principaux.
      - **Exécuter sur les nœuds secondaires** - Sélectionnez cette option pour exécuter le travail uniquement sur les nœuds secondaires.

      Vous pouvez également choisir le nœud principal et le nœud secondaire pour exécuter le même travail de configuration. Si vous ne sélectionnez ni nœud principal ni secondaire, le travail de configuration s'exécute automatiquement sur le nœud principal.

   b) Cliquez sur **Ajouter des instances** et sélectionnez les instances dans la liste. Cliquez sur **OK**.

   c) Cliquez sur **Suivant**.

6. Dans l'onglet **Spécifier les valeurs de variable**, vous avez deux options :

   a) Téléchargez le fichier d'entrée pour entrer les valeurs des variables que vous avez définies dans vos commandes, puis téléchargez le fichier sur le serveur Citrix ADM.

b) Entrez des valeurs communes pour les variables que vous avez définies pour toutes les instances

c) Cliquez sur **Suivant**.

7. Évaluez et vérifiez les commandes à exécuter sur chaque instance sous l'onglet **Aperçu des tâches** . Cet onglet affiche également les commandes d'annulation si elles sont spécifiées dans l'onglet **Sélectionner la configuration** .

8. Dans l'onglet **Exécuter**, choisissez d'exécuter votre travail maintenant ou de planifier l'exécution ultérieure.

   En outre, sélectionnez l'une des actions suivantes dans la liste **Échec de la commande** que Citrix ADM doit effectuer en cas d'échec de la commande :

   - **Ignorer l'erreur et continuer** : Citrix ADM ignore la commande ayant échoué et exécute les commandes restantes pour l'instance sélectionnée.

     > **Remarque**
     >
     > Cette action ne vous permet pas d'interrompre une tâche de configuration en cours.

   - **Arrêter l'exécution ultérieure** : Citrix ADM arrête les commandes restantes si une commande échoue pendant l'exécution.
   - **Commandes réussie** : Citrix ADM restaure les commandes exécutées avec succès si une commande échoue pendant l'exécution.

     Si la restauration personnalisée est activée, Citrix ADM exécute les commandes d'annulation correspondantes pour les commandes ayant échoué.

9. Cliquez sur **Terminer**.

Pour envoyer un e-mail et une notification Slack pour une tâche :

Un e-mail et une notification Slack sont désormais envoyés chaque fois qu'une tâche est exécutée ou planifiée. La notification comprend des détails tels que le succès ou l'échec du travail ainsi que les détails pertinents.

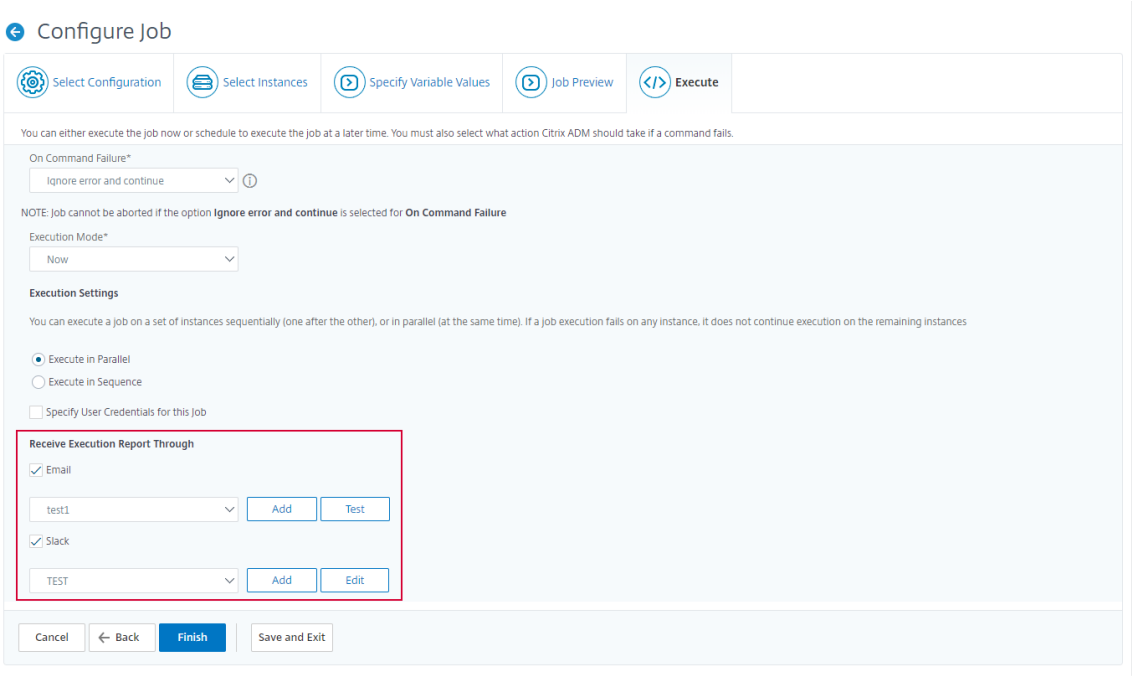
1. Accédez à **Réseaux**>**Travaux de configuration**.
2. Sélectionnez le travail que vous souhaitez activer la notification par e-mail et Slack, puis cliquez sur **Modifier**.
3. Dans l'onglet **Exécuter**, accédez au volet **Recevoir le rapport d'exécution via** :

   - Activez la case à cocher **Email** et choisissez la liste de distribution de courrier électronique à laquelle vous souhaitez envoyer le rapport d'exécution.

     Si vous souhaitez ajouter une liste de distribution de courrier électronique, cliquez sur **Ajouter** et spécifiez les détails du serveur de messagerie.

- **Activez la case à cocher Slack et choisissez ADCal de marge auquel vous souhaitez envoyer le rapport d'exécution.**

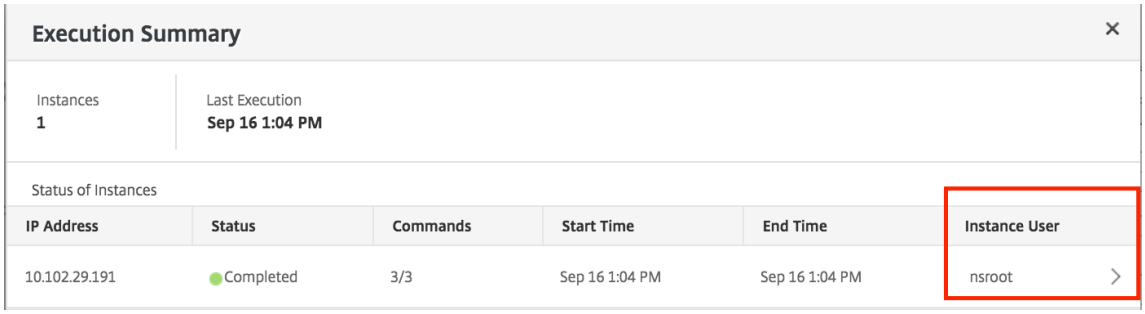
  Si vous souhaitez ajouter un profil Slack, cliquez sur **Ajouter** et spécifiez le **nom du profil**, le **nom du canal** et le **jeton** du canal Slack requis.



4. Cliquez sur **Terminer**.

Pour afficher les détails du résumé de l'exécution :

1. Accédez à **Réseaux** > **Travaux de configuration**.
2. Sélectionnez le travail que vous souhaitez afficher le résumé de l'exécution, puis cliquez sur **Détails**.
3. Cliquez sur **Résumé de l'exécution** pour afficher :
   - Statut de l'instance sur la tâche exécutée
   - Les commandes s'exécutent sur le travail
   - L'heure de début et de fin de la tâche, et
   - Nom de l'utilisateur de l'instance



Utiliser l'enregistrement et la lecture pour créer des tâches de configuration

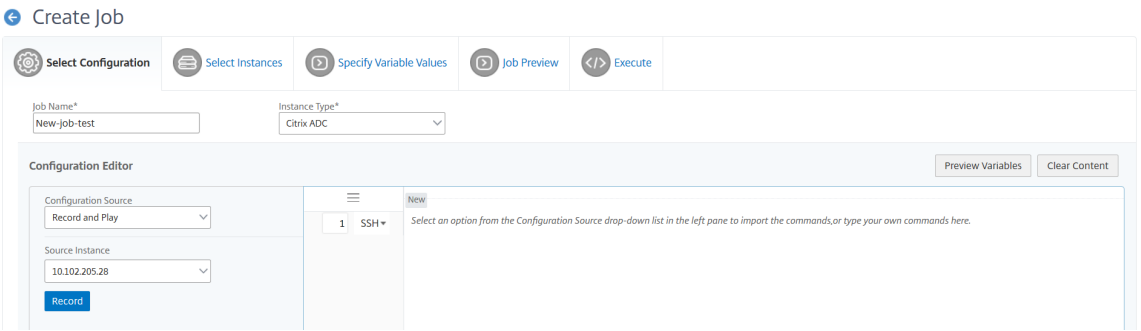
April 29, 2021

Si vous êtes habitué à utiliser l'interface graphique Citrix ADC pour configurer une instance Citrix ADC, il peut arriver que vous ayez du mal à rappeler les commandes CLI exactes pour créer une tâche de configuration et l'exécuter sur plusieurs instances Citrix ADC.

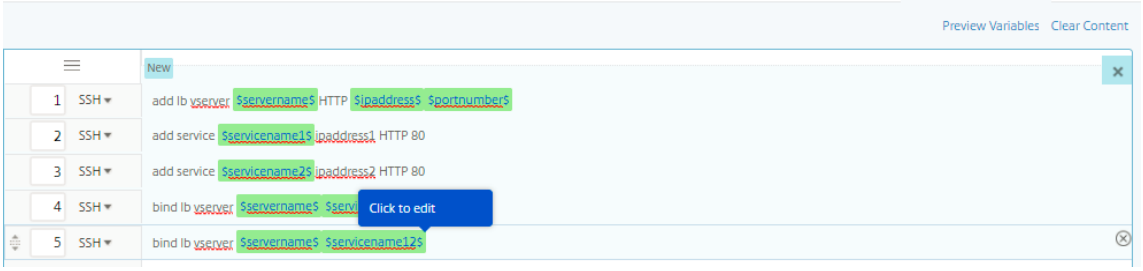
Citrix Application Delivery Management (ADM) vous permet d'enregistrer les tâches de configuration effectuées à l'aide de l'interface graphique d'une instance Citrix ADC et de la convertir en commandes CLI. Vous pouvez ensuite créer une tâche de configuration à partir de ces commandes CLI et exécuter cette tâche sur plusieurs instances.

Pour enregistrer la configuration de l'interface graphique et la convertir en tâche de configuration :

1. Accédez à **Réseaux** > **Travaux de configuration**, puis cliquez sur **Créer un travail** .
2. Spécifiez le nom du travail et le type d'instance.
3. Dans la liste **Source de configuration**, sélectionnez **Enregistrer et lire**, puis sélectionnez l'instance source à partir de laquelle vous souhaitez enregistrer la configuration. Cliquez sur **Enregistrer**.



4. L'**interface graphique Citrix ADC** s'ouvre. Configurez les fonctionnalités et les paramètres que vous souhaitez que la tâche de configuration contienne. Fermez ensuite la fenêtre GUI Citrix ADC et cliquez sur **Arrêter** dans l' **Éditeur de configuration** . Les commandes apparaissent sous la forme d'un lien dans le volet gauche. Faites glisser les commandes vers le volet droit, puis cliquez sur **Suivant**.



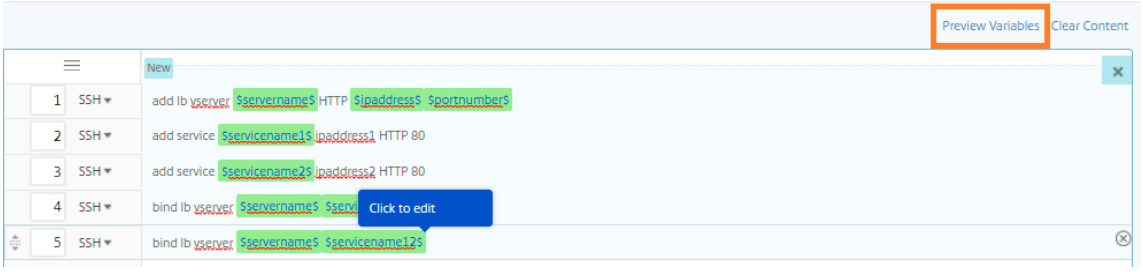
Vous pouvez ensuite réorganiser les commandes dans l'éditeur de configuration selon les besoins. Vous pouvez déplacer la commande d'une ligne à l'autre en faisant glisser la ligne de commande. Vous pouvez également déplacer ou réorganiser la ligne de commande d'une ligne à n'importe quelle ligne cible en changeant simplement le numéro de ligne de commande dans la zone de texte.

5. Vous pouvez consulter toutes les variables que vous avez définies lors de la création ou de la modification d'un travail de configuration dans une vue consolidée unique.

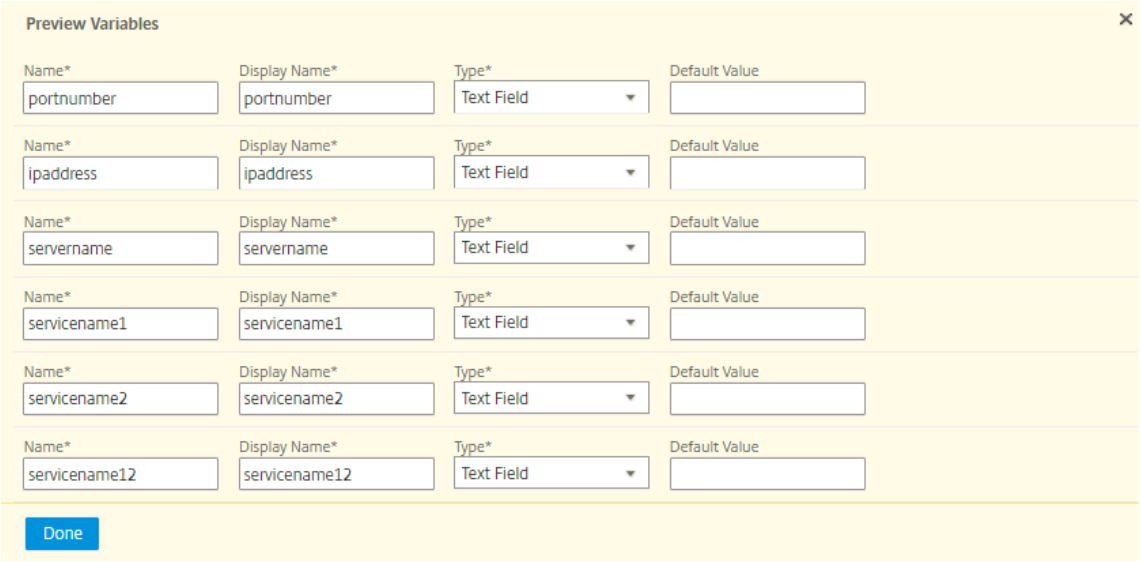
6. Pour afficher toutes les variables dans une seule vue consolidée, procédez de l'une des manières suivantes :

   - Lors de la création d'une tâche de configuration, accédez à **Réseaux > Travaux de configuration**, sélectionnez **Créer un travail**. Sur la page **Créer un travail**, vous pouvez consulter toutes les variables que vous avez ajoutées lors de la création du travail de configuration.
   - Lors de la modification d'un travail de configuration, accédez à **Réseau > Travaux de configuration**, sélectionnez le nom du travail et cliquez sur **Modifier**. Sur la page **Configurer le travail**, vous pouvez passer en revue toutes les variables qui ont été ajoutées lors de la création du travail de configuration.

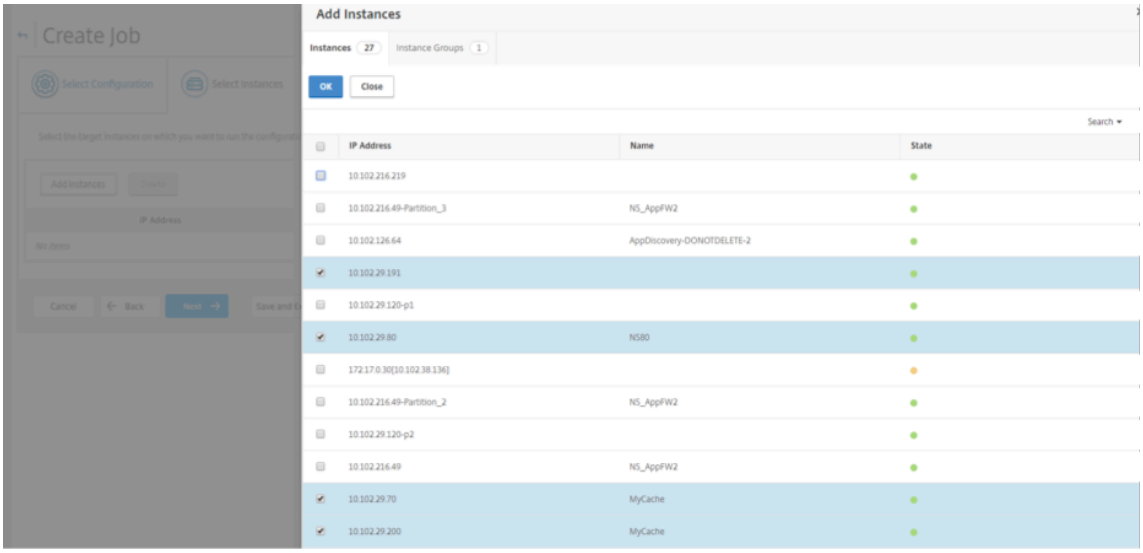
7. Vous pouvez ensuite cliquer sur l'onglet **Aperçu des variables** pour prévisualiser les variables dans une vue consolidée unique que vous avez définie lors de la création ou de la modification d'un travail de configuration.



8. Une nouvelle fenêtre contextuelle apparaît et affiche tous les paramètres des variables telles que Nom, Nom d'affichage, Type et valeur par défaut dans un format tabulaire. Vous pouvez également modifier ces paramètres. Cliquez sur le bouton **Terminé** après avoir modifié l'un des paramètres.



9. Cliquez sur **Ajouter des instances** et sélectionnez les instances sur lesquelles vous souhaitez exécuter le travail de configuration. Cliquez sur **OK**, puis sur **Suivant**.



10. Si vous avez spécifié des variables dans les commandes, sous l'onglet **Spécifier 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 de variables** : cliquez sur **Télécharger le fichier de 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.

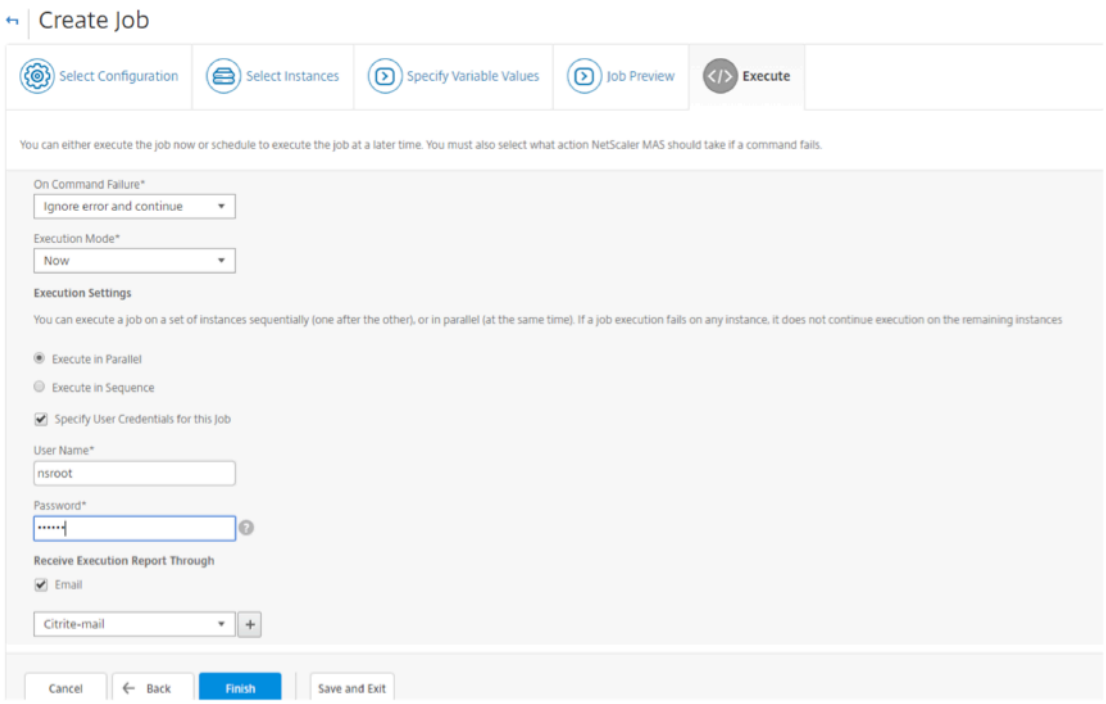
Les fichiers d'entrée contenant les valeurs de variables sont conservés (avec le même nom de fichier) dans les tâches de configuration. Vous pouvez afficher et modifier ces fichiers d'entrée que vous avez utilisés et chargés précédemment lors de la création ou de la modification des tâches de configuration.

Pour afficher les travaux de configuration exécutés lors de la création d'un travail de configuration, accédez à **Réseau** > **Travaux de configuration**, puis cliquez sur **Créer un travail**. Dans la page **Créer une tâche**. Sous l'onglet **Spécifier les valeurs 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 chargez les fichiers (en conservant le même nom de fichier).

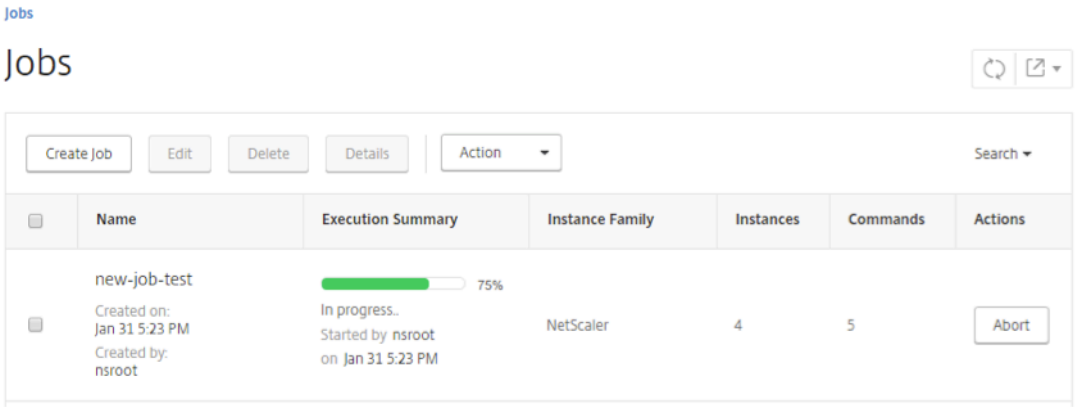
Pour afficher les travaux de configuration déjà exécutés lors de la modification d'un travail de configuration, accédez à **Réseau** > **Travaux de configuration**, sélectionnez le nom du travail et cliquez sur **Modifier**. Dans la page **Configurer la tâche**, sous l'onglet **Spécifier les valeurs de variable**, sélectionnez l'option **Valeurs variables communes pour toutes les instances** pour afficher les fichiers chargés. Pour modifier les fichiers d'entrée, téléchargez le fichier d'entrée, puis modifiez et téléchargez les fichiers (en conservant le même nom de fichier) .10. Sous l'onglet **Aperçu des tâches**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances.

11. Sous l'onglet **Aperçu des tâches**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances.
12. Sous l'onglet**Exécuter**, vous pouvez choisir d'exécuter votre travail maintenant ou de le programmer pour qu'il soit exécuté ultérieurement. Vous pouvez également choisir l'action que Citrix ADM doit prendre en cas d'échec de la commande.

    Vous pouvez également choisir d'autoriser les utilisateurs autorisés à exécuter des travaux sur vos instances gérées, et vous pouvez choisir d'envoyer une notification par e-mail concernant le succès ou l'échec de la tâche, ainsi que d'autres détails.



13. Sur la page **Tâches**, vous pouvez ensuite afficher la progression de l'exécution de votre tâche de configuration sur toutes les instances.



Utiliser les tâches de configuration pour répliquer la configuration d'une instance vers plusieurs instances

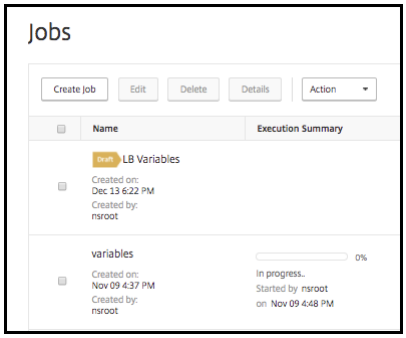
April 29, 2021

Vous avez peut-être configuré l'équilibrage de charge et AppFlow sur une instance de Citrix ADC pour votre déploiement. Cependant, vous voulez maintenant répliquer uniquement la configuration AppFlow vers d'autres instances de Citrix ADC.

Vous pouvez utiliser la fonctionnalité Travaux de configuration de Citrix Application Delivery Management (ADM) pour extraire la configuration AppFlow à partir d'une instance de Citrix ADC et la répliquer sur plusieurs instances.

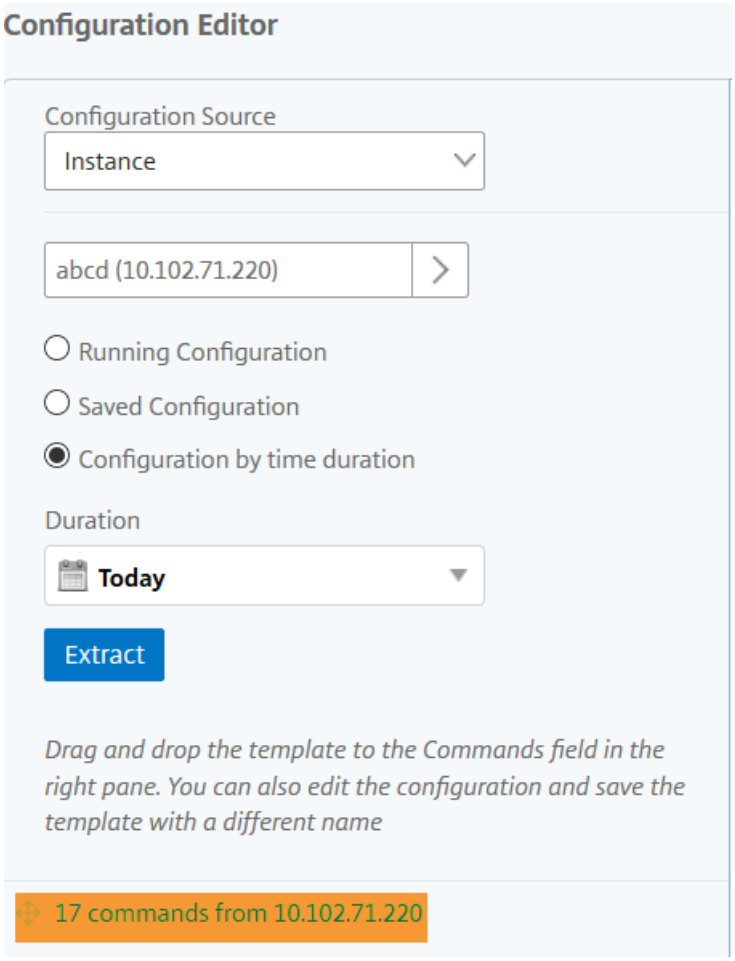
Pour récupérer et répliquer la configuration d'une instance vers d'autres instances Citrix ADC :

1. Accédez à **Réseaux** > **Travaux de configuration**, puis cliquez sur **Créer un travail** .



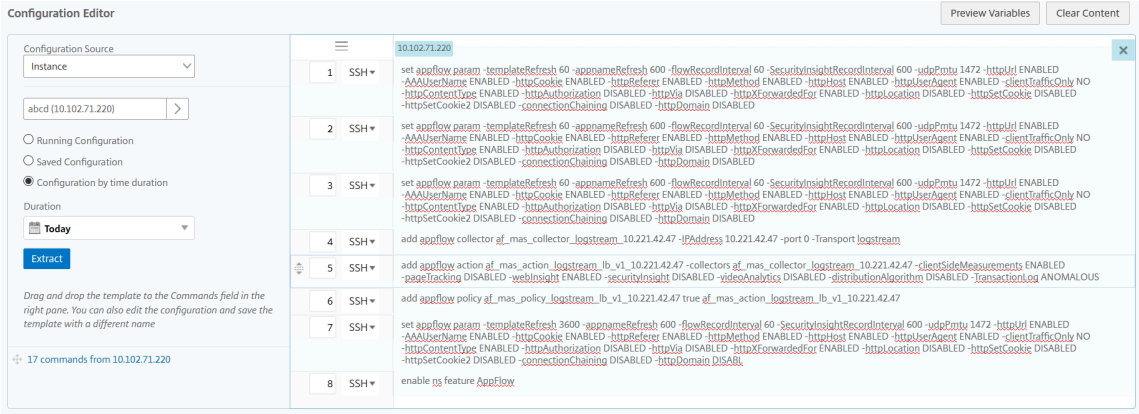
2. Spécifiez le nom de la tâche et le type d'instance.
3. Sélectionnez **Instance** comme **source de configuration** et sélectionnez l'instance source dont vous souhaitez répliquer la configuration. Sélectionnez le type de configuration que vous souhaitez extraire. Si vous sélectionnez « Configuration par durée de temps », définissez la période pendant laquelle vous avez exécuté cette configuration, puis cliquez sur **Extraire**.

   Le nombre de commandes exécutées sur cette instance pendant la durée sélectionnée s'affiche à l'écran comme indiqué dans l'image ci-dessous.



4. Faites glisser les commandes vers le champ **Commandes** dans le volet droit.

Conservez uniquement les commandes liées à FEO et supprimez manuellement les commandes liées à l'équilibrage de charge ou les commandes liées à toute autre configuration, puis cliquez sur **Suivant**.



5. Cliquez sur **Ajouter des instances** et ajoutez les instances sur lesquelles vous souhaitez appliquer la configuration FEO. Cliquez sur **OK**, puis sur **Suivant**.

   Si vous avez spécifié des variables dans les commandes, sous l'onglet Spécifier les valeurs variables, cliquez sur **Télécharger le fichier de clé d'entrée**. Dans le fichier téléchargé, spécifiez les valeurs des variables, puis téléchargez le fichier dans Citrix ADM.

Sous l'onglet **Aperçu des tâches**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances.

Sous l'onglet **Exécuter**, cliquez sur **Terminer** pour exécuter le travail sur les instances Citrix ADC sélectionnées.

Utiliser des variables dans les tâches de configuration

April 29, 2021

Un travail de configuration est un ensemble de commandes de configuration que vous pouvez exécuter sur une ou plusieurs instances gérées. Lorsque vous exécutez la même configuration sur plusieurs instances, vous pouvez utiliser des valeurs différentes pour les paramètres utilisés dans votre configuration. Vous pouvez définir des variables qui vous permettent d'affecter des valeurs différentes pour ces paramètres ou d'exécuter un travail sur plusieurs instances.

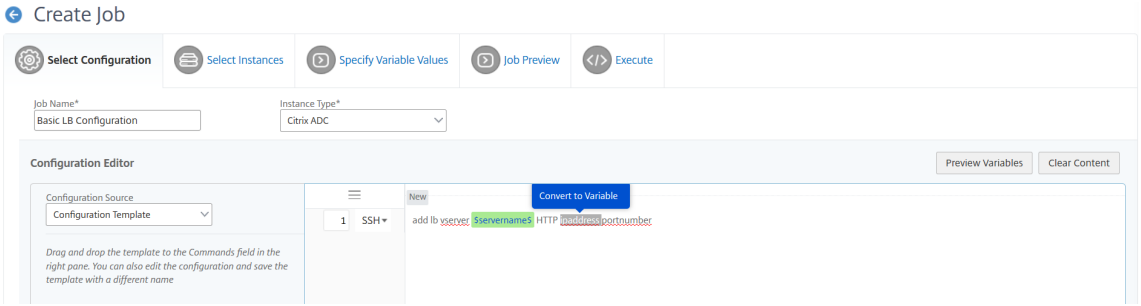
Par exemple, envisagez une configuration d'équilibrage de charge de base dans laquelle vous ajoutez un serveur virtuel d'équilibrage de charge, ajoutez deux services et liez les services au serveur virtuel. Maintenant, vous pouvez souhaiter avoir la même configuration sur deux instances, mais avec des valeurs différentes pour les noms et adresses IP du serveur virtuel et des services. Vous pouvez utiliser la fonctionnalité de tâches de configuration pour y parvenir en utilisant des variables pour définir les noms et adresses IP du serveur virtuel et des services.

Dans cet exemple, les commandes et variables suivantes sont utilisées :

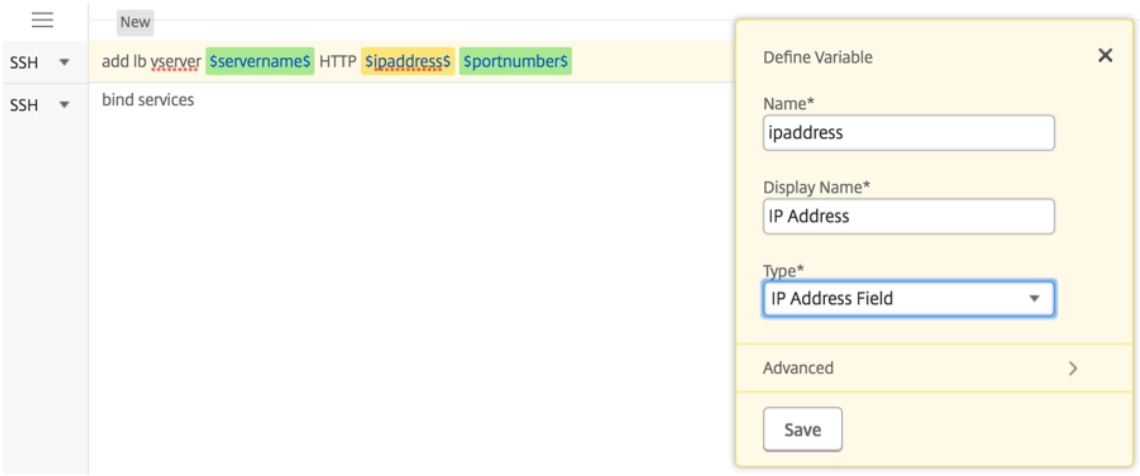

```
add lb vserver \*\*servername\*\* HTTP \*\*ipaddress\*\* \*\*portnumber
    \*\*

add service \*\*servicename1\*\* \*\*ipaddress1\*\* HTTP 80

add service \*\*servicename2\*\* \*\*ipaddress2\*\* HTTP 80

bind lb vserver \*\*servername\*\* \*\*servicename1\*\*

bind lb vserver \*\*servername\*\* \*\*servicename2\*\*
<!--NeedCopy-->
```

Pour créer une tâche de configuration en définissant des variables dans Citrix ADM :

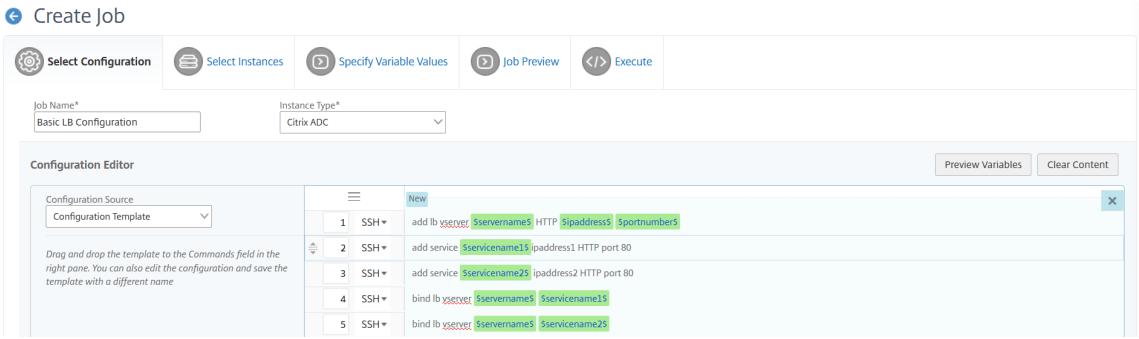
1. Accédez à **Réseaux** > **Travaux de configuration**.
2. Cliquez sur **Créer un travail**.
3. Dans la page **Créer un travail**, sélectionnez les paramètres de travail personnalisés tels que le nom de la tâche, le type d'instance et le type de configuration.
4. Dans l'Éditeur de configuration, tapez 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.



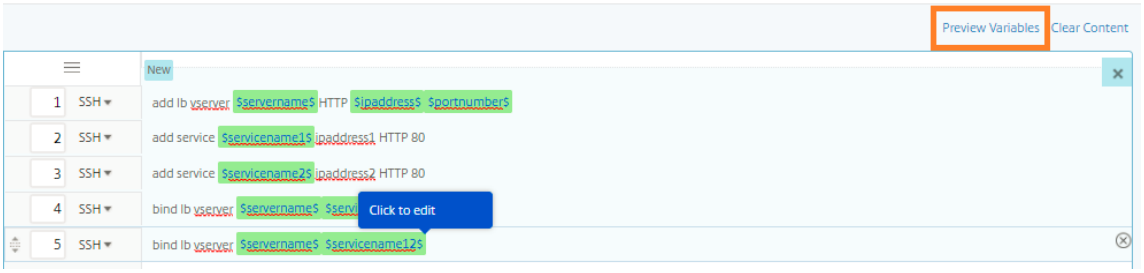
5. Une fois que vous voyez des signes dollar enferment la valeur de la variable, cliquez sur la variable pour spécifier davantage les détails de la variable, tels que le nom, le nom complet et le type. Vous pouvez également cliquer sur l'option **Avancé** si vous souhaitez spécifier une valeur par défaut pour votre variable. Cliquez sur **Enregistrer**, puis sur **Suivant**.



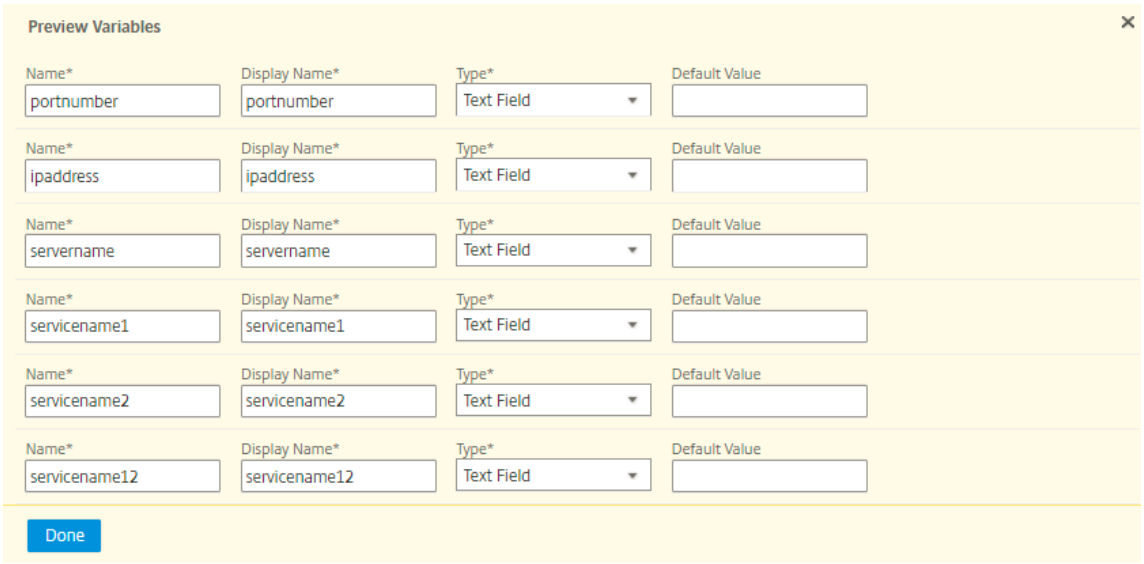
Tapez le reste de vos commandes et définissez toutes les variables.



6. Vous pouvez consulter toutes les variables que vous avez définies lors de la création ou de la modification d'un travail de configuration dans une vue consolidée unique.
7. Pour afficher toutes les variables dans une seule vue consolidée, procédez de l'une des manières suivantes :
   - Lors de la création d'un travail de configuration, accédez à **Réseaux** > **Travaux de configuration**, sélectionnez **Créer un travail**. Sur la page **Créer un travail**, vous pouvez consulter toutes les variables que vous avez ajoutées lors de la création du travail de configuration.
   - Lors de la modification d'un travail de configuration, accédez à **Réseau** > **Travaux de configuration**, sélectionnez le nom du travail et cliquez sur **Modifier**. Sur la page **Configurer le travail**, vous pouvez passer en revue toutes les variables qui ont été ajoutées lors de la création du travail de configuration.
8. Vous pouvez ensuite cliquer sur l'onglet **Aperçu des variables** pour prévisualiser les variables dans une vue consolidée unique que vous avez définie lors de la création ou de la modification d'un travail de configuration.



9. Une nouvelle fenêtre contextuelle apparaît et affiche tous les paramètres des variables telles que Nom, Nom d'affichage, Type et valeur par défaut dans un format tabulaire. Vous pouvez également modifier ces paramètres. Cliquez sur le bouton **Terminé** après avoir modifié l'un des paramètres.



10. Vous pouvez ensuite réorganiser les commandes dans l'éditeur de configuration selon les besoins. Vous pouvez déplacer la commande d'une ligne à l'autre en faisant glisser la ligne de commande. Vous pouvez également déplacer ou réorganiser la ligne de commande d'une ligne à n'importe quelle ligne cible en changeant simplement le numéro de ligne de commande dans la zone de texte.

11. Sélectionnez les instances sur lesquelles vous voulez exécuter le travail de configuration.

12. Dans l'onglet **Spécifier les valeurs de variable**, sélectionnez l'option **Télécharger le fichier d'entrée pour les valeurs de variable**, puis cliquez sur **Télécharger le fichier de 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 générer une erreur.

13. Le fichier de clé d'entrée est téléchargé sur votre système local et vous pouvez le modifier en spécifiant les valeurs de variable pour chaque instance de Citrix ADC sélectionnée précédemment,

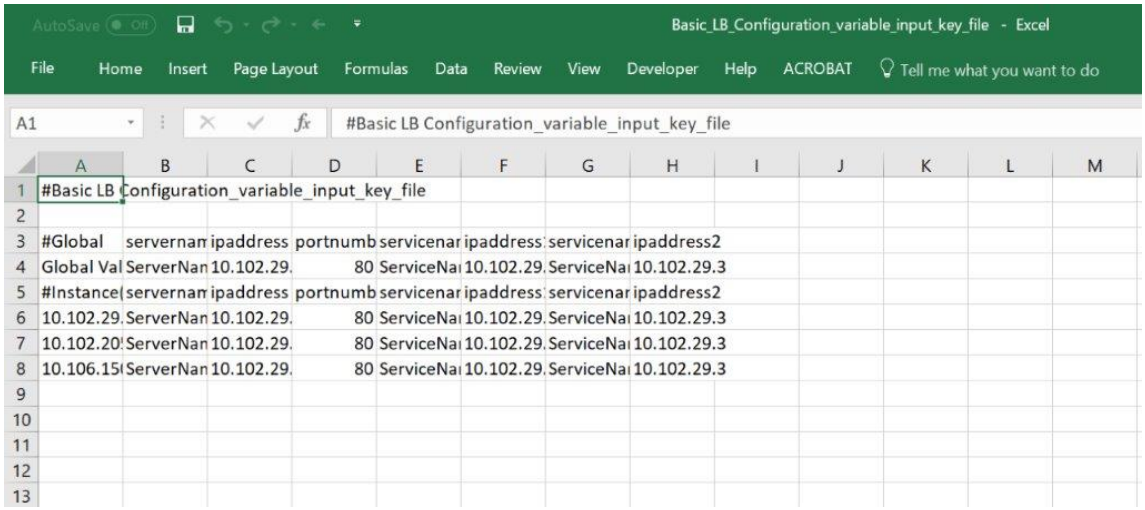
puis en cliquant sur **Télécharger pour charger** le fichier de clé d'entrée dans Citrix Application Delivery Management (ADM). Cliquez sur **Suivant**. Le fichier de clé d'entrée se télécharge sur votre système local et vous pouvez le modifier en spécifiant les valeurs de variable pour chaque instance de Citrix ADC sélectionnée précédemment.

> **Remarque**
>
> Dans le fichier de clé d'entrée, les variables sont définies à trois niveaux :
>
> ```
> 1     -  Niveau mondial
> ```
>
> - Niveau du groupe d'instances
> - Niveau d'instance

Les variables globales sont des valeurs variables qui sont appliquées à toutes les instances. Les valeurs des variables de niveau 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 de niveau 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 de 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 de clé d'entrée dans Citrix ADM. Cliquez sur **Suivant**.



> **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 provoque 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 variable communes à toutes les instances et cliquer sur **Télécharger** pour télécharger le fichier de clé d'entrée dans Citrix ADM.

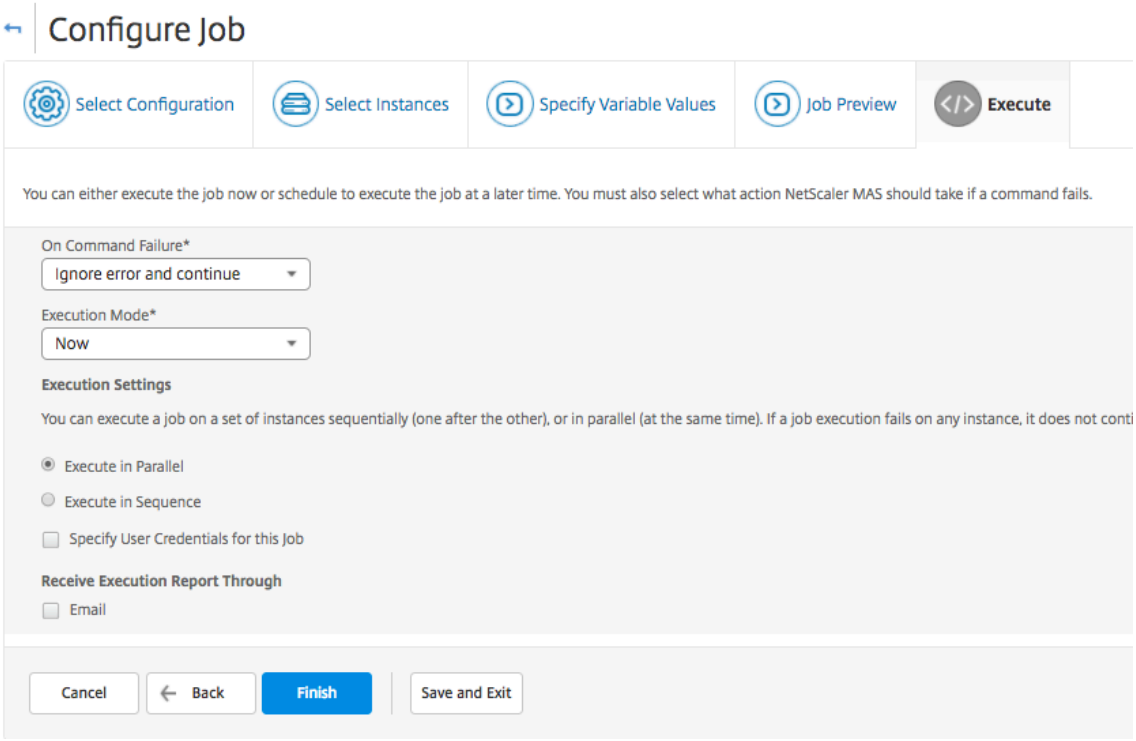
    Les fichiers d'entrée clés contenant les valeurs de variables sont conservés (avec le même nom de fichier) dans les tâches de configuration. Vous pouvez afficher et modifier ces fichiers d'entrée que vous avez utilisés et chargés précédemment lors de la création ou de la modification des tâches de configuration.

    Pour afficher les travaux de configuration exécutés lors de la création d'un travail de configuration, accédez à **Réseau** > **Travaux de configuration**, puis cliquez sur **Créer un travail**. Dans la page **Créer une tâche**. Sous l'onglet **Spécifier les valeurs 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 chargez les fichiers (en conservant le même nom de fichier).

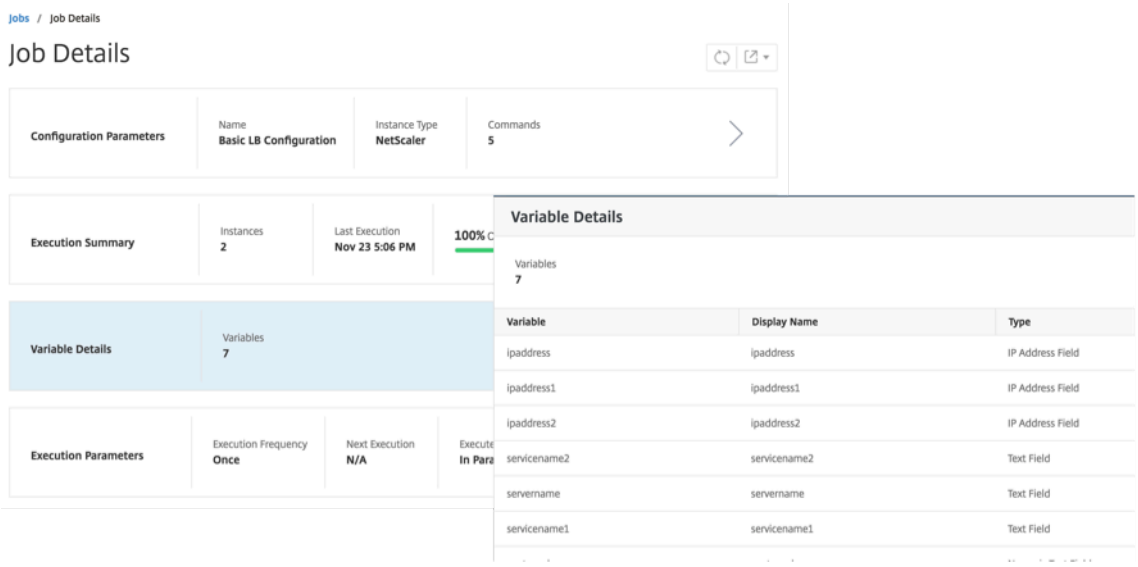
    Pour afficher les travaux de configuration déjà exécutés lors de la modification d'un travail de configuration, accédez à **Réseau** > **Travaux de configuration**, sélectionnez le nom du travail et cliquez sur **Modifier**. Dans la page **Configurer la tâche**, sous l'onglet **Spécifier les valeurs de variable**, sélectionnez l'option **Valeurs variables communes pour toutes les instances** pour afficher les fichiers chargés. Pour modifier les fichiers d'entrée, téléchargez le fichier d'entrée, puis modifiez et téléchargez les fichiers (en conservant le même nom de fichier).

16. Sous l'onglet **Aperçu des tâches**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances.

17. Dans l'onglet **Exécuter**, vous pouvez choisir d'exécuter votre travail maintenant ou de le planifier pour qu'il soit exécuté ultérieurement. Vous pouvez également choisir l'action que Citrix ADM doit prendre si la commande échoue et si vous souhaitez envoyer une notification par e-mail concernant le succès ou l'échec de la tâche ainsi que d'autres détails.



Après avoir configuré vos tâches et les exécuter, vous pouvez afficher les détails de la tâche en accédant à **Réseaux** > Tâces **de configuration** et sélectionnez le travail que vous avez configuré. Cliquez sur **Détails**, puis cliquez sur **Détails des variables** pour afficher la liste des variables ajoutées à votre travail.



> **Remarque**
>
> Les valeurs que vous avez fournies pour les variables à l' **étape 5** sont conservées par Citrix ADM lorsque vous enregistrez le travail et quittez, ou lorsque vous planifiez l'exécution d'un travail à

> un moment ultérieur.

Créer des tâches de configuration à partir de commandes correctives

April 29, 2021

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 standard pour l'audit des modifications de configuration à l'aide de modèles d'audit comprend les étapes suivantes.

1. Créez un modèle d'audit avec un ensemble de commandes Citrix ADC valide/attendues pour l'audit des 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/correctives et utiliser la fonctionnalité « Create Job » pour obtenir les configurations de l'instance à l'état souhaité

Considérons un scénario dans lequel plusieurs administrateurs gèrent cinq instances de Citrix ADC. Tous ces administrateurs effectuent des mises à jour de la configuration d'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, quelles que soient les modifications apportées par d'autres administrateurs. Dans ce cas d'utilisation, le super administrateur crée un modèle de configuration qui devrait être présent sur les instances de 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**.

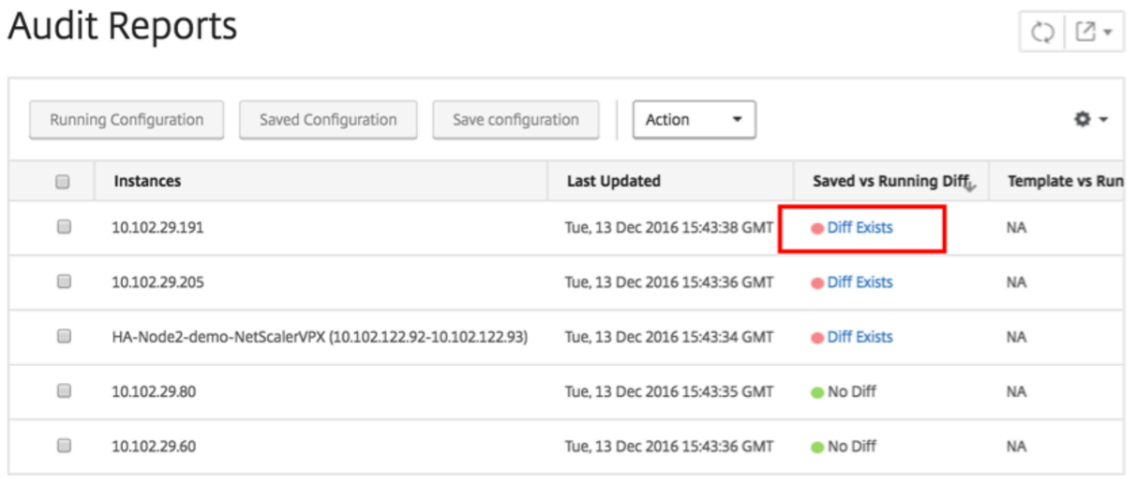
Si vous remarquez qu'il y a un changement dans la configuration de certaines instances, vous pouvez utiliser la fonctionnalité de commandes correctives ADM pour créer un travail de configuration avec les commandes de configuration modifiées et corrigées pour des instances Citrix ADC spécifiques.

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 **Quittes de** différence, vous accédez à la page **Diff de configuration**, où vous pouvez afficher la commande corrective. Vous pouvez également utiliser ces commandes correctives pour créer un travail de configuration et l'exécuter sur les instances Citrix ADC spécifiques pour les ramener à la configuration souhaitée.

Pour créer une tâche de configuration à partir de commandes correctives sur Citrix ADM :

1. Accédez à **Réseaux** > **Audit de configuration**.

2. Sur la page **Audit de configuration**, cliquez à l'intérieur de l'un des deux graphiques en donut pour accéder à la page **Rapports d'audit** .
3. Cliquez sur le lien **Diff Exists** (sous la colonne **Saved vs Running Diff** dans le tableau) pour l'instance pour laquelle vous souhaitez corriger les commandes de configuration. La page **Configuration Diff** apparaît, répertoriant les différences entre la configuration enregistrée, la configuration en cours d'exécution et la configuration de correction pour cette instance.



4. Cliquez sur **Créer un travail** pour accéder à la page **Créer un travail**, sur laquelle les commandes correctives ont été préremplies. Pour obtenir des instructions sur la création d'une tâche de configuration, reportez-vous à la sectionComment faire pour créer une tâche de configuration sur Citrix ADM.

Répliquer la configuration en cours d'exécution et enregistrée d'une instance de Citrix ADC vers une autre

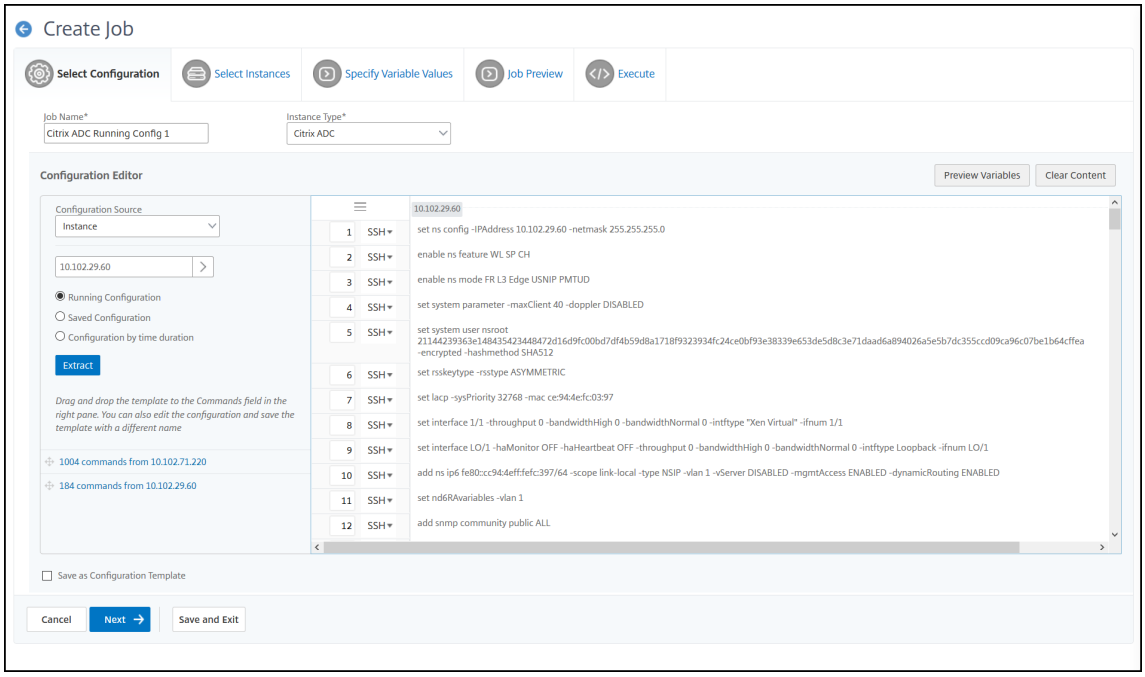
April 29, 2021

Vous pouvez désormais répliquer la configuration d'une instance d'Citrix ADC sur d'autres instances. Lorsque vous configurez un travail dans Citrix Application Delivery Management (ADM), sélectionnez une instance comme source de configuration et choisissez la configuration en cours d'exécution ou enregistrée de l'instance sélectionnée.

Par exemple, lorsque vous sélectionnez **Configuration en cours d'exécution** et que vous cliquez sur **Extraire**, Citrix ADM envoie une demande à l'instance de Citrix ADC sélectionnée pour localiser la configuration en cours d'exécution et l'affiche sous forme de modèle. Vous pouvez faire glisser le modèle dans le champ **Commandes** du volet de droite. Vous pouvez modifier les commandes, les paramètres et les instances.

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

1. Accédez à **Réseaux** > **Travaux de configuration**, puis cliquez sur **Créer un travail**.
2. Spécifiez le nom du travail et le type d'instance. Par exemple, spécifiez *Citrix ADC Running Config1* comme nom de votre tâche et le type d'instance comme *Citrix ADC* .
3. Sélectionnez **Instance** comme **source de configuration**, sélectionnez l'instance source dont vous souhaitez répliquer la configuration sur d'autres instances.
4. Vous voyez les trois options suivantes :
    - Configuration en cours d'exécution
    - Configuration enregistrée
    - Configuration par durée
5. Choisissez **Exécution de la configuration**, puis cliquez sur **Extraire**. Le nombre de commandes de configuration exécutées sur cette instance s'affiche.



6. Faites glisser les commandes dans le champ **Commandes** dans le volet droit.
7. Vous pouvez modifier les commandes dans le champ Commandes. Par exemple, si les commandes extraites doivent configurer une instance Citrix ADC. Cela peut inclure l'ajout de partitions, la configuration de l'équilibrage de charge, la liaison du serveur d'équilibrage de charge aux services, etc. Vous pouvez modifier vos commandes, pour configurer vos nouvelles instances Citrix ADC sans partitions. Ainsi, pour supprimer des 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 téléchargez le fichier dans Citrix ADM.
10. Sous l'onglet **Aperçu des tâches**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances.
11. Dans l'onglet **Exécuter**, vous pouvez choisir d'exécuter votre travail maintenant ou de le planifier pour qu'il soit exécuté ultérieurement. Vous pouvez également choisir l'action que Citrix ADM doit prendre si la commande échoue et si vous souhaitez envoyer une notification par e-mail concernant le succès ou l'échec de la tâche ainsi que d'autres détails.

Réutiliser les travaux de configuration d'exécution

April 29, 2021

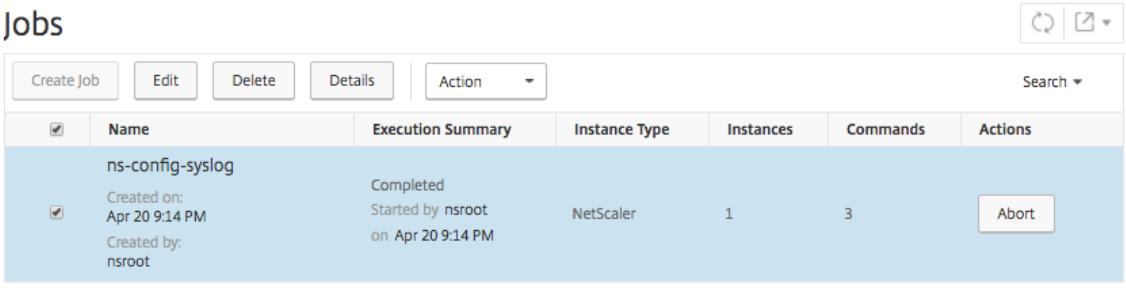
Les tâches de configuration vous permettent de créer un ensemble de commandes de configuration que vous pouvez exécuter sur une ou plusieurs instances gérées. Vous pouvez également exécuter le même ensemble de tâches de configuration enregistrées après avoir modifié les commandes, les paramètres, la source de configuration et les instances de la tâche. Cette fonctionnalité 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.

Citrix Application Delivery Management (ADM) fournit une fonction permettant d'exécuter à nouveau les travaux terminés. Avec cette fonction, les travaux exécutés complètement peuvent être exécutés à nouveau sans modifier le nom de la tâche.

> **Remarque**
>
> Vous pouvez réexécuter uniquement les tâches qui sont exécutées lorsque le mode d'exécution est « Maintenant ».

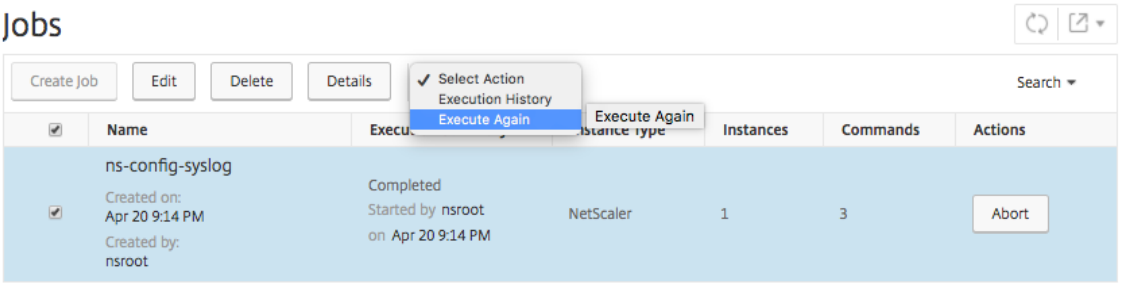
Pour modifier les tâches terminées :

1. À partir de la page d'accueil d'ADM, accédez à **Réseaux** > **Travaux de configuration**.
2. Dans la page **Tâches**, sélectionnez un travail qui affiche le résumé de l'exécution comme terminé, puis cliquez sur **Modifier** . Vous pouvez également modifier une tâche de configuration planifiée.
3. Dans la page **Configurer le travail**, vous pouvez voir que le nom du travail et le type d'instance ne sont pas modifiables. Vous pouvez modifier d'autres champs comme la source de configuration, ajouter des instances, modifier des valeurs de variable et définir des paramètres d'exécution.
4. Cliquez sur **Terminer** pour exécuter à nouveau la tâche de configuration.



> **Remarque**
>
> Vous pouvez également sélectionner la tâche et cliquer à nouveau sur **Exécuter** pour exé-

> cuter la tâche sans modifier la source, l'instance et les commandes. Cette option est utile lorsque vous devez exécuter le même ensemble de commandes sur les mêmes instances. Parfois, le travail peut rencontrer une erreur transitoire du côté serveur, et vous devrez peut-être exécuter à nouveau la tâche.



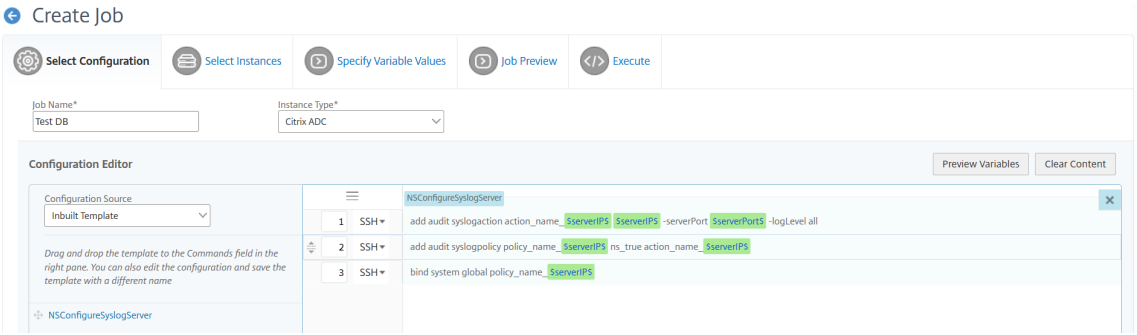
Planifier les tâches créées à l'aide de modèles intégrés

April 29, 2021

Vous pouvez planifier une tâche à l'aide de l'option de modèle intégrée. Un travail est un ensemble de commandes de configuration que vous pouvez exécuter sur une ou plusieurs instances gérées. Par exemple, vous pouvez utiliser l'option de modèle intégrée pour planifier une tâche de configuration des serveurs syslog. Vous pouvez également choisir d'exécuter le travail immédiatement ou de planifier l'exécution ultérieure.

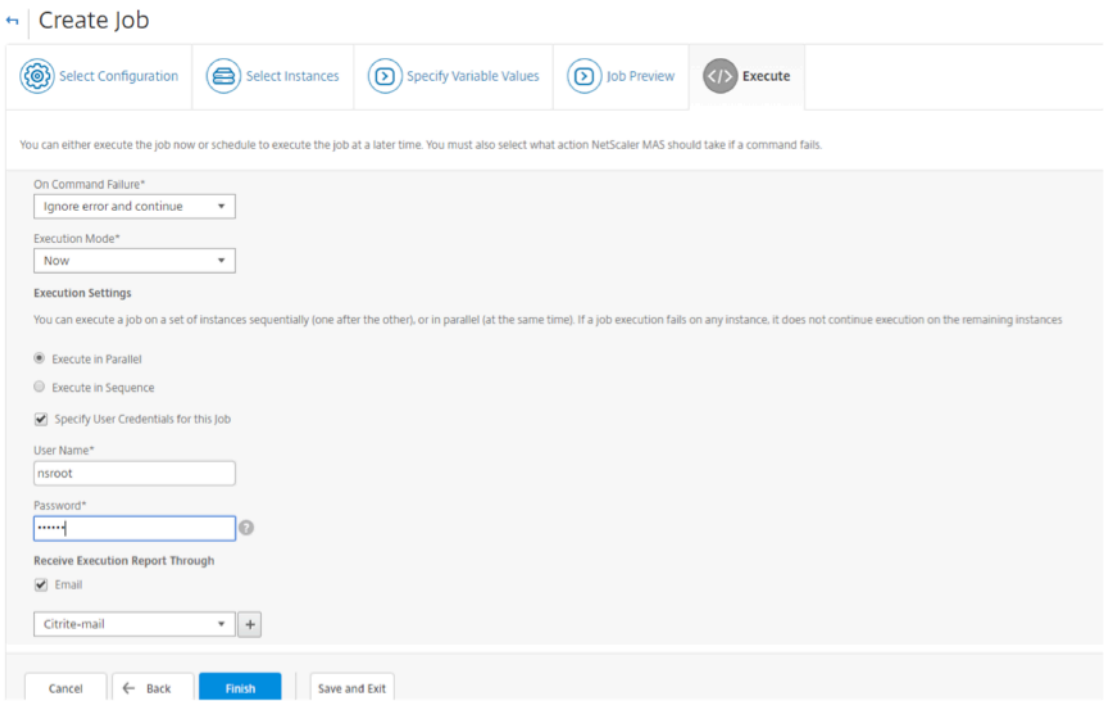
Pour planifier une tâche à l'aide de modèles intégrés dans Citrix ADM :

1. Dans Citrix Application Delivery Management (ADM), accédez à **Réseaux** > **Travaux de configuration**, puis cliquez sur **Créer un travail**.
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 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 entrer 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** : spécifiez l'adresse IP du serveur syslog et le port.
6. Sous l'onglet **Aperçu des tâches**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances.
7. Cliquez sur **Suivant**.
8. Sous l'onglet **Exécuter**, définissez les conditions suivantes :
   - **En cas d'échec de commande** - Si une commande échoue, vous pouvez choisir d'ignorer les erreurs et de continuer à exécuter la tâche ou d'arrêter l'exécution ultérieure de la tâche. Choisissez l'action à exécuter dans la liste déroulante.
   - **Mode d'exécution** - Vous pouvez exécuter le travail maintenant ou planifier son exécution ultérieure. Si vous souhaitez planifier le travail ultérieurement, vous devez spécifier les paramètres de fréquence d'exécution pour ce travail. Choisissez la planification à suivre dans la liste déroulante.
9. Vous pouvez également exécuter un travail sur un ensemble d'instances séquentiellement ou en parallèle en sélectionnant la méthode requise sous **Paramètres d'exécution**. Si l'exécution d'une tâche échoue sur une instance, elle ne se poursuit pas sur les instances restantes.

   Vous pouvez également choisir d'autoriser les utilisateurs autorisés à exécuter des travaux sur vos instances gérées, et vous pouvez choisir d'envoyer une notification par e-mail concernant le succès ou l'échec de la tâche, ainsi que d'autres détails.
10. Cliquez sur **Terminer**.



Utiliser des tâches de maintenance pour mettre à niveau des instances Citrix ADC SDX

April 29, 2021

Vous pouvez effectuer une mise à niveau groupée de vos instances Citrix ADC SDX exécutant Citrix ADC version 11.0 et ultérieure. Pour effectuer une mise à niveau groupée unique, vous utilisez une tâche intégrée dans Citrix Application Delivery Management (ADM). Avec cette tâche intégrée, vous pouvez mettre à niveau Citrix ADC SDX Management Service, l'hyperviseur XenServer et les packs et correctifs supplémentaires pour Citrix Hypervisor.

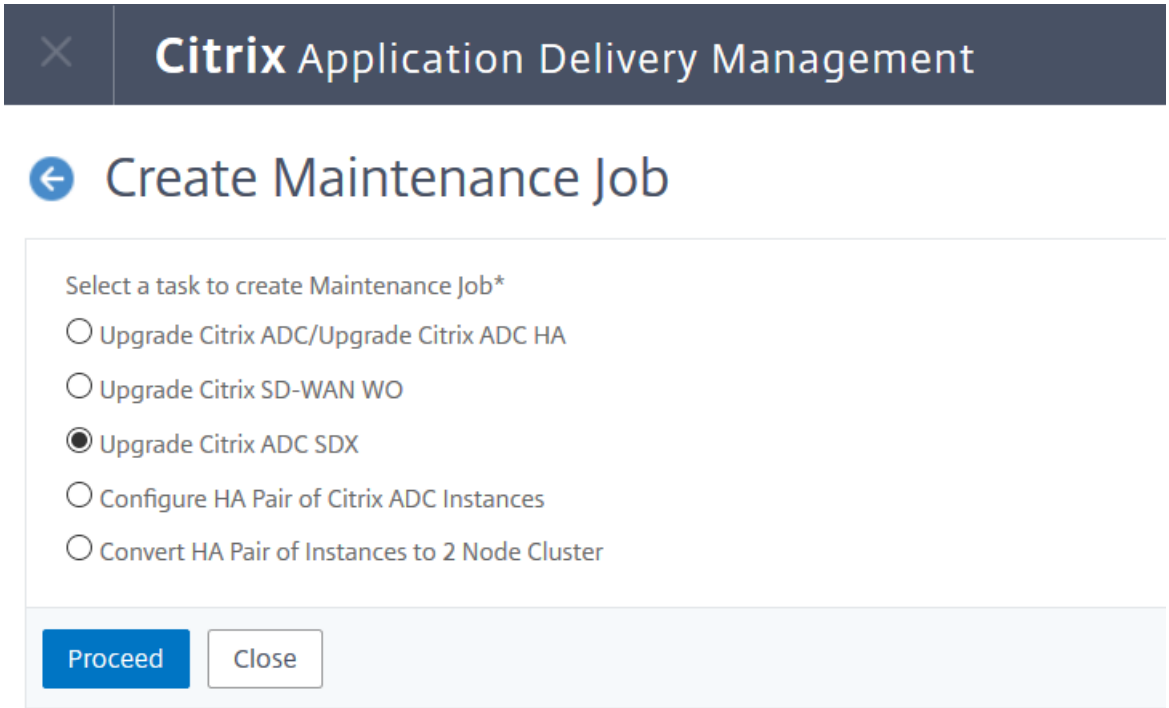
Pour mettre à niveau des instances Citrix ADC SDX à l'aide de Citrix ADM :

1. Dans Citrix ADM, accédez à **Réseaux** > **Travaux de configuration** > **Tobs de maintenance.**
2. Cliquez sur **Créer un travail**. Dans la page Créer un travail, sélectionnez la tâche intégrée de **mise à niveau Citrix ADC SDX** pour mettre à niveau vos instances Citrix ADC SDX. Cliquez sur **Continuer**.
3. Sur la page **Mettre à niveau les appliances Citrix ADC**, dans l'onglet **Sélection d'instance**, spécifiez le **nom de la tâche** et cliquez sur **Ajouter des instances**.
4. Sélectionnez les instances ou groupes d'instances cibles que vous souhaitez mettre à niveau.
5. Après avoir ajouté les instances ou groupes d'instances Citrix ADC, cliquez sur **Suivant** pour démarrer la validation de pré-mise à niveau sur les instances sélectionnées. L'écran signale la

progression de la pré-validation de chacune des instances d'Citrix ADC.

6. Sur la page **Modifier la mise à niveau de Citrix ADC Appliance**, sélectionnez l'onglet **Mise à niveau** . Dans le menu déroulant **Image logicielle**, sélectionnez **Local** (votre machine locale) ou **Appliance** (le fichier de build 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 la forme d'un 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 à la vérification de la mise à niveau de pré-validation, vous pouvez supprimer les instances. Pour supprimer les instances, sélectionnez-les et cliquez sur **Supprimer**.
8. Sous l'onglet **Planifier la tâche**, vous pouvez également définir les détails d'exécution dans lesquels vous pouvez effectuer le processus de mise à niveau maintenant ou le planifier pour une date ultérieure. Vous pouvez également choisir de sauvegarder votre instance Citrix ADC SDX, de recevoir un rapport d'exécution par e-mail ou d'effectuer une mise à niveau en deux étapes pour les nœuds dans HA.

La mise à niveau en deux étapes pour les nœuds dans HA vous donne la possibilité d'effectuer la mise à niveau immédiatement ou de planifier une heure pour les nœuds à mettre à jour les uns après les autres. La synchronisation et la propagation des nœuds sont désactivées jusqu'à ce que les deux nœuds soient correctement mis à niveau.



Création de tâches de configuration pour les instances Citrix SD-WAN WANOP

April 29, 2021

Un travail 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 taper 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 suivant.
- **Fichier** : Vous pouvez télécharger un fichier de configuration à partir de votre machine locale et créer des tâches.

Une fois qu'un travail est créé, vous pouvez choisir d'exécuter le travail immédiatement ou de planifier l'exécution ultérieure. Vous pouvez également définir la fréquence d'exécution

Modèle intégré	Description
EnableCloudBridgeWANOpt	Active le trafic via l'appliance Citrix SD-WAN WANOP.
DisableCloudBridgeWANOpt	Désactive le trafic via l'appliance WANOP Citrix SD-WAN.
RestartCloudBridgeWANOpt	Redémarre l'appliance WANOP Citrix SD-WAN.
RestoreConfig	Restaure la configuration de l'appliance WANOP Citrix SD-WAN.
AddLink	La création ou la définition de liens permettent à l'appliance 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 la liaison et également spécifier qu'il s'agit du trafic côté LAN ou WAN.

Modèle intégré	Description
ConfigureBandwidth	Définit les limites de bande passante et d'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'appliance WANOP SD-WAN avec un ou plusieurs filtres de classes de service et l'active.
SetApplication	Définit la définition du classificateur d'application.
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 soit le cache vidéo, soit 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.
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.

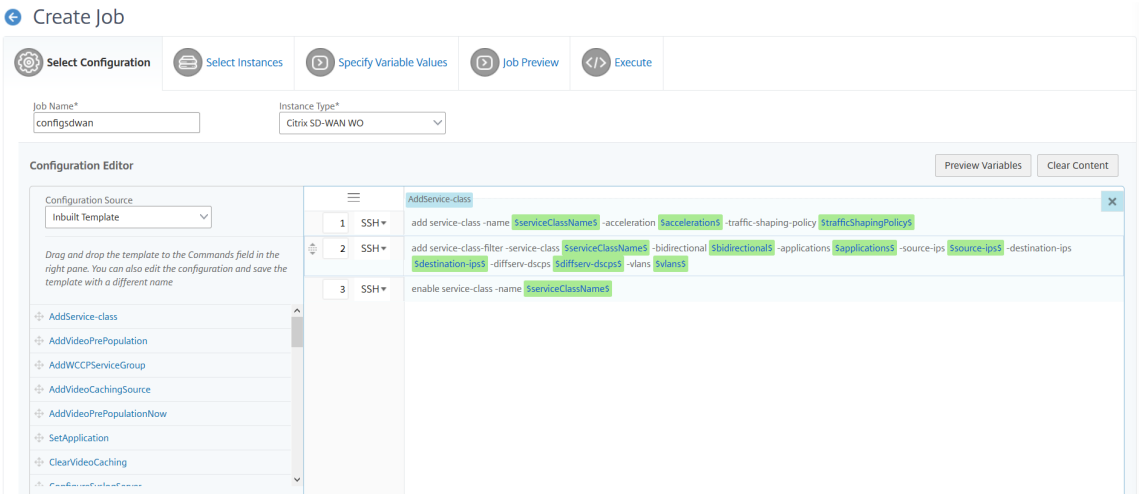
Modèle intégré	Description
ConfigureRemoteLicenseServer	Configure le serveur de licences centralisé. Spécifiez le modèle du serveur de licences, l'adresse IP et le numéro de port.
ConfigureLocalLicenseServer	Définit l'emplacement du serveur de licences comme local.
InstallCACert	Installe les certificats 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 combiné de paires de clés de certificat SSL.
InstallSeperateCertKey	Installe le certificat SSL et la clé en tant que fichiers séparés.
ActiveWCCP	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 mise en forme 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 quand mettre en cache une vidéo.
UpdateVideoPrePopulation	Modifie une entrée de prépeuplement vidéo, qui spécifie quand mettre en cache une vidéo.

Modèle intégré	Description
AddVideoPrePopulationNow	Configure la prépopulation vidéo, ce qui vous permet de télécharger et de mettre en cache une vidéo immédiatement. Vous pouvez contrôler la façon dont vous souhaitez télécharger et mettre en cache des vidéos à partir d'une ou plusieurs URL.
VideoPrePopulationState	Modifie, démarre, met à jour ou supprime la prépopulation vidéo.
ConfigureSyslogServer	Définit l'adresse IP et le numéro de port du serveur syslog.
ConfigureAlert	Configure le niveau d'alerte.

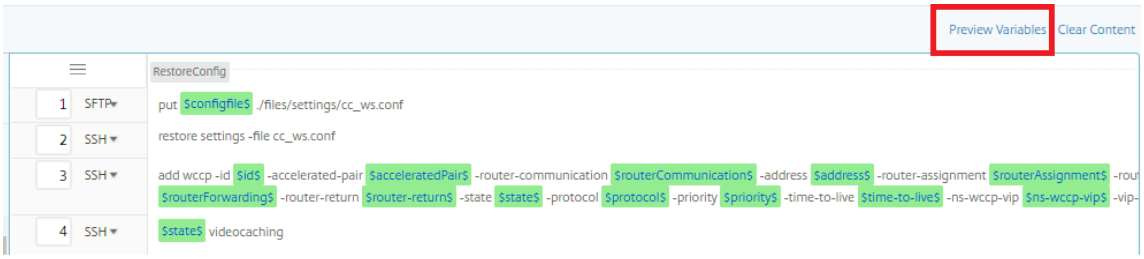
Pour créer une tâche de configuration pour les instances de Citrix SD-WAN WANOP:

1. Dans Citrix ADM, accédez à **Réseaux** > **Travaux de configuration**, puis cliquez sur **Créer un travail** .
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.

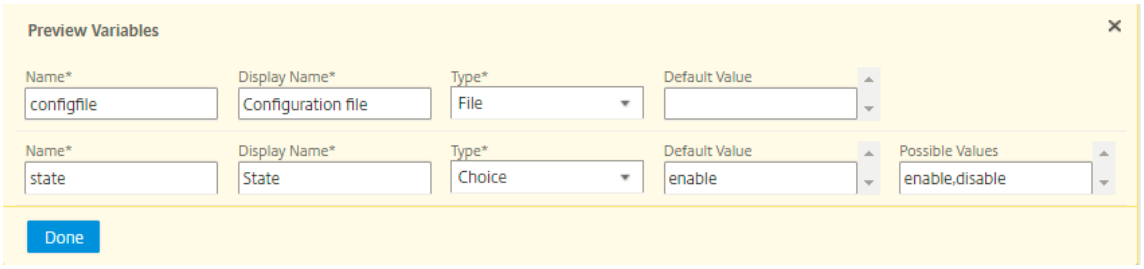
> **Remarque**
>
> Sélectionnez **Enregistrer en tant que modèle de configuration** et spécifiez un nom pour enregistrer la configuration en tant que modèle et la réutiliser.



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'un travail de configuration, accédez à **Réseaux** > **Travaux de configuration**, sélectionnez **Créer un travail**. Sur la page **Créer un travail**, vous pouvez consulter toutes les variables que vous avez ajoutées lors de la création du travail de configuration.
    - Lors de la modification d'un travail de configuration, accédez à **Réseau** > **Travaux de configuration**, sélectionnez le nom du travail et cliquez sur **Modifier**. Sur la page **Configurer le travail**, vous pouvez passer en revue toutes les variables qui ont été ajoutées lors de la création du travail de configuration.
7. Vous pouvez ensuite cliquer sur l'onglet **Aperçu des variables** pour prévisualiser les variables dans une vue consolidée unique que vous avez définie lors de la création ou de la modification d'un travail de configuration.



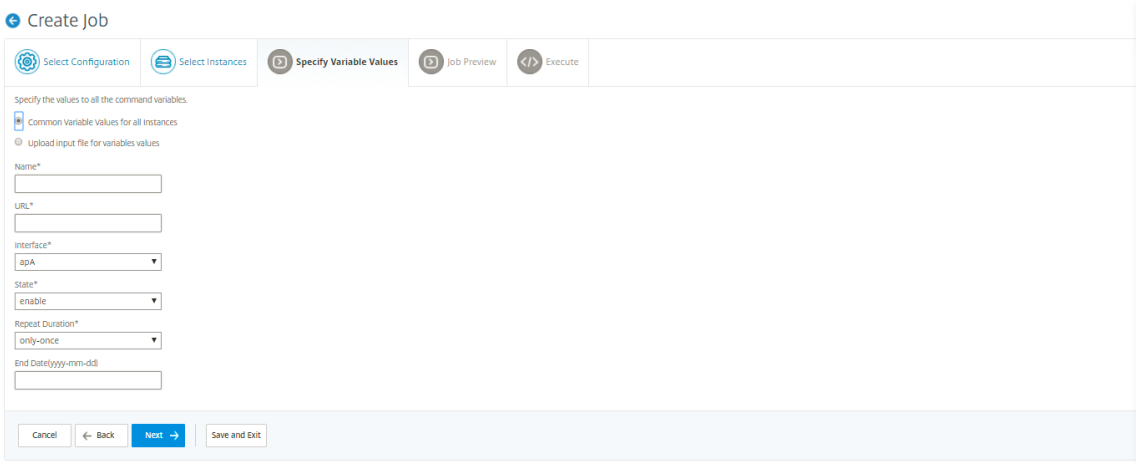
8. Une nouvelle fenêtre contextuelle apparaît et affiche tous les paramètres des variables telles que Nom, Nom d'affichage, Type et valeur par défaut dans un format tabulaire. Vous pouvez également modifier ces paramètres. Cliquez sur le bouton **Terminé** après avoir modifié l'un des paramètres.



9. Cliquez sur **Suivant**, puis 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**.
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 de variables :** cliquez sur **Télécharger**

le fichier de clé d'entrée pour télécharger un fichier d'entrée. Dans le fichier d'entrée, entrez des valeurs pour les variables que vous avez définies dans vos commandes, puis téléchargez le fichier sur le serveur Citrix ADM.

- **Valeurs de variables communes pour toutes les instances** : entrez des valeurs pour les variables. Les variables varient en fonction du modèle sélectionné.



Les fichiers d'entrée contenant les valeurs des variables sont conservés (avec le même nom de fichier) dans les tâches de configuration. Vous pouvez afficher et modifier ces fichiers d'entrée que vous avez utilisés et chargés précédemment lors de la création ou de la modification des tâches de configuration.

Pour afficher les travaux de configuration exécutés lors de la création d'un travail de configuration, accédez à **Réseau** > **Travaux de configuration**, puis cliquez sur **Créer un travail**. Dans la page **Créer une tâche**. Sous l'onglet **Spécifier les valeurs 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 chargez les fichiers (en conservant le même nom de fichier).

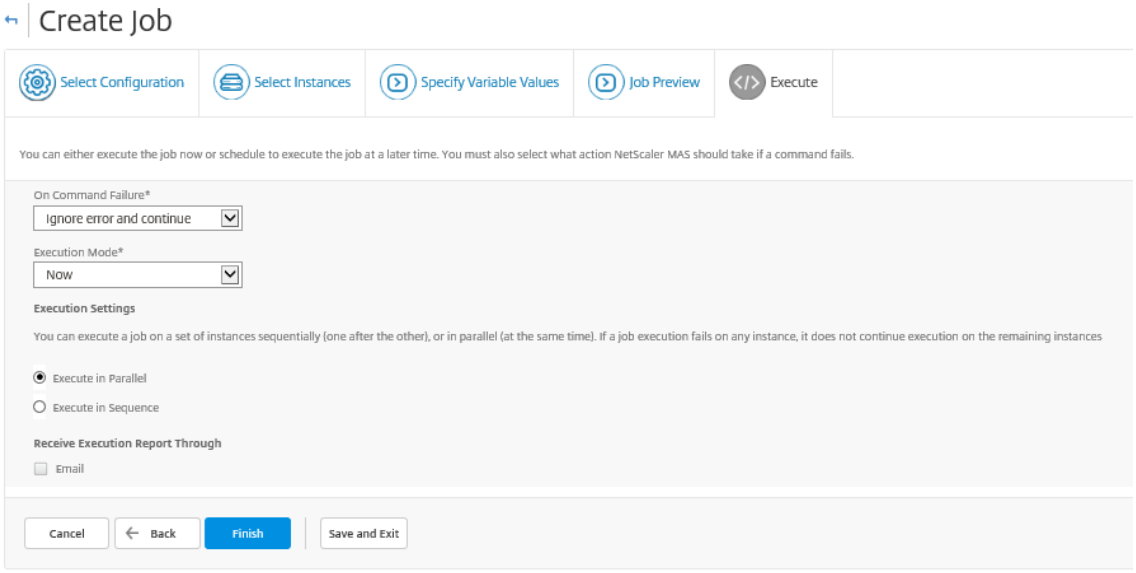
Pour afficher les travaux de configuration déjà exécutés lors de la modification d'un travail de configuration, accédez à **Réseau** > **Travaux de configuration**, sélectionnez le nom du travail et cliquez sur **Modifier**. Dans la page **Configurer la tâche**, sous l'onglet **Spécifier les valeurs de variable**, sélectionnez l'option **Valeurs variables communes pour toutes les instances** pour afficher les fichiers chargés. Pour modifier les fichiers d'entrée, téléchargez le fichier d'entrée, puis modifiez et téléchargez les fichiers (en conservant le même nom de fichier)

11. Cliquez sur **Suivant**, sous l'onglet **Aperçu du travail**, vous pouvez évaluer et vérifier les commandes à exécuter en tant que tâche.
12. Cliquez sur **Suivant**, sous l'onglet **Exécuter**, définissez les conditions suivantes :

    - En cas d'**échec de commande** : Que faire en cas d'échec d'une commande : ignorez les erreurs et continuez le travail, ou arrêtez l'exécution ultérieure du travail. Choisissez une

action dans la liste déroulante.

- **Mode d'exécution** : exécutez le travail immédiatement ou planifiez l'exécution pour une durée ultérieure. Si vous planifiez l'exécution pour une période ultérieure, vous devez spécifier les paramètres de fréquence d'exécution pour la tâche. Choisissez la planification à suivre dans la liste déroulante **Fréquence d'exécution**.



13. Sous **Paramètres d'exécution**, sélectionnez cette option pour exécuter le travail de manière séquentielle (l'un après l'autre) ou en parallèle (en même temps).
14. Pour qu'un rapport d'exécution de travail soit envoyé par e-mail à une liste de destinataires, activez la case à cocher **E-mail** dans la section **Recevoir le rapport d'exécution par le biais**. Dans la liste déroulante qui s'affiche, choisissez une liste de distribution de courrier électronique. Pour créer une liste de distribution de courrier électronique, 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

April 29, 2021

L'utilisation d'un modèle de configuration maître est une option flexible pour la création et le déploiement d'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 une instance de Citrix ADC. Vous pouvez enregistrer la nouvelle configuration en tant que modèle de configuration maître (fichier .conf).

Pour enregistrer votre modèle de configuration maître à partir d'une instance de Citrix 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 d'Citrix ADC, 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 de Citrix ADC, sélectionnez **Configuration enregistrée**. Cliquez sur le lien **Enregistrer le texte dans un fichier** pour enregistrer le fichier 'ns.conf' sur votre machine locale.

Lorsque vous déployez le modèle de configuration maître à l'aide du modèle de configuration 'DeployMasterConfiguration' lors de la création d'une tâche, vous pouvez le personnaliser davantage pour chaque instance Citrix ADC spécifique en ajoutant plus de commandes, en modifiant des commandes existantes et en fournissant différentes valeurs de variables dans le fichier d'entrée .

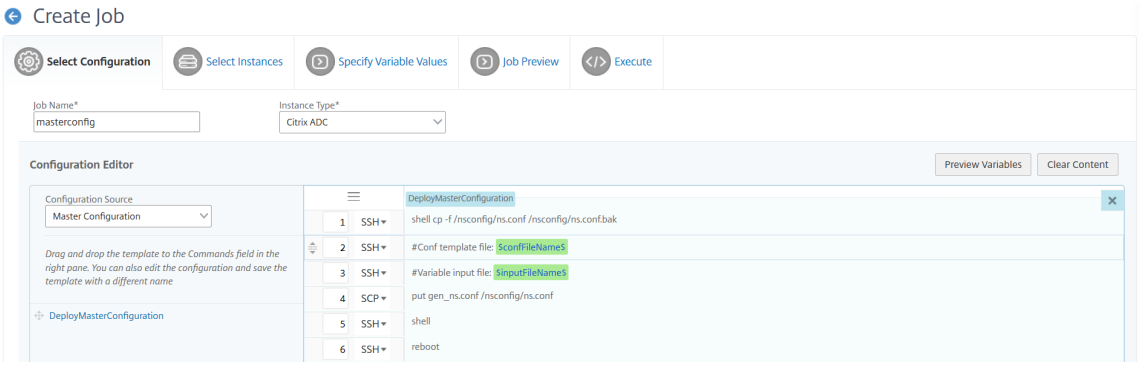
Par exemple, en tant qu'administrateur, vous pouvez télécharger des clés de certificat sur vos instances Citrix ADC en plus du fichier ns.conf et y déployer également la configuration principale.

> **Important**
>
> Vous ne pouvez pas exécuter un travail de configuration à l'aide du modèle DeploymasterConfiguration sur des instances Citrix ADC CPX, des instances Citrix ADC configurées dans un cluster ou sur des instances Citrix ADC partitionnées.

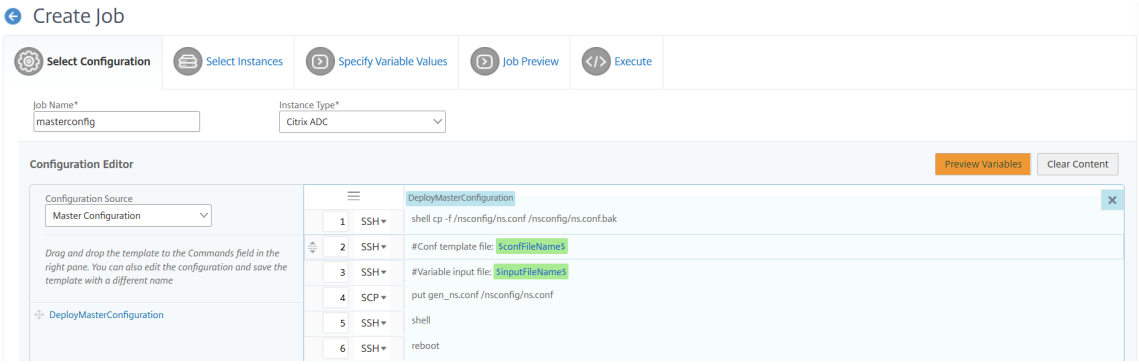
Pour créer une tâche de configuration à l'aide du modèle de configuration Master Config sur Citrix ADM :

1. Dans Citrix Application Delivery Management (ADM), accédez à **Réseaux** > **Travaux de configuration**, puis cliquez sur **Créer un travail**.
2. Dans la page **Créer un travail**, sous l'onglet **Sélectionner une configuration**, spécifiez le **nom du travail** et sélectionnez le **type d'instance** dans la liste déroulante.
3. Sélectionnez **Configuration principale** dans la liste déroulante **Source de configuration** . Faites glisser les commandes du modèle DeployMasterConfiguration vers le volet droit. Vous pouvez également ajouter, modifier ou supprimer des commandes dans le volet droit. Cliquez sur **Suivant**.

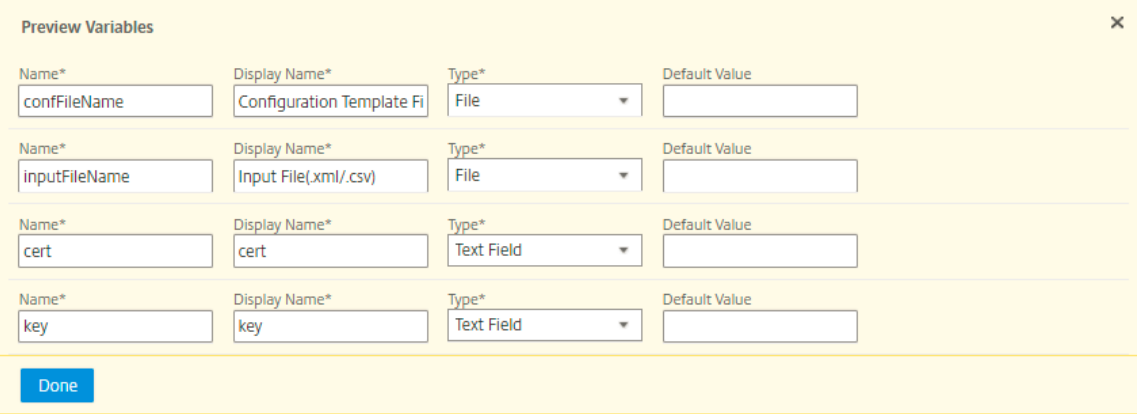
   > **Remarque**
   >
   > Vous pouvez ajouter des commandes de **mise** pour ajouter des fichiers d'entrée à votre modèle. Dans notre exemple, nous devons télécharger des fichiers de certificat et de clé en plus du fichier de modèle de configuration et des fichiers d'entrée de variables.



4. Vous pouvez consulter toutes les variables que vous avez définies lors de la création ou de la modification d'un travail de configuration dans une vue consolidée unique.
5. Pour afficher toutes les variables dans une seule vue consolidée, procédez de l'une des manières suivantes :
   - Lors de la création d'une tâche de configuration, accédez à **Réseaux > Travaux de configuration**, sélectionnez **Créer un travail**. Sur la page **Créer un travail**, vous pouvez consulter toutes les variables que vous avez ajoutées lors de la création du travail de configuration.
   - Lors de la modification d'un travail de configuration, accédez à **Réseau > Travaux de configuration**, sélectionnez le nom du travail et cliquez sur **Modifier**. Sur la page **Configurer le travail**, vous pouvez passer en revue toutes les variables qui ont été ajoutées lors de la création du travail de configuration.
6. Vous pouvez ensuite cliquer sur l'onglet **Aperçu des variables** pour prévisualiser les variables dans une vue consolidée unique que vous avez définie lors de la création ou de la modification d'un travail de configuration.



7. Une nouvelle fenêtre contextuelle s'affiche et affiche tous les paramètres des variables telles que Nom, Nom d'affichage, Type et valeur par défaut sous forme de tableau. Vous pouvez également 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. Sous l'onglet **Spécifier les valeurs de variable**, chargez les éléments suivants :
   - **Fichier de modèle de configuration (.conf)** : téléchargez le fichier .conf extrait d'une instance de Citrix ADC.
   - **Télécharger le fichier d'entrée (.xml/csv)** - Téléchargez le fichier d'entrée avec des valeurs pour les variables que vous avez définies dans vos commandes.

   Un exemple de fichier xml est fourni ici pour votre utilisation. Assurez-vous que les fichiers xml contiennent les détails correspondant aux instances ADC que vous utilisez.

```
<?xml version="1.0" encoding="UTF-8" ?>

<properties>

<!--

Provide inputs for all the parameters defined in the master config
    file.

-  global. This tag contains all the common parameters and value.

-  devicegroup. This tag contains all the instance group specific
   parameters and values.

If the same parameters are defined in global and instance tags,
   the instance specific parameters value will take precedence
   over the instance group. The instance group specific parameters
    value will take precedence over global parameters in the
   execution.

-  name. This attribute represents the name of the instance group.
```



```
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 attibute.
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-->
```

Un exemple de fichier csv est fourni ici pour votre utilisation.

```
1 #job-s_variable_input_key_file ,,,,
2 ,,,,
3 #Global,NSIP,HostName,LBSERVER,SNMPTrapDest
4 Global Values,,,,
```

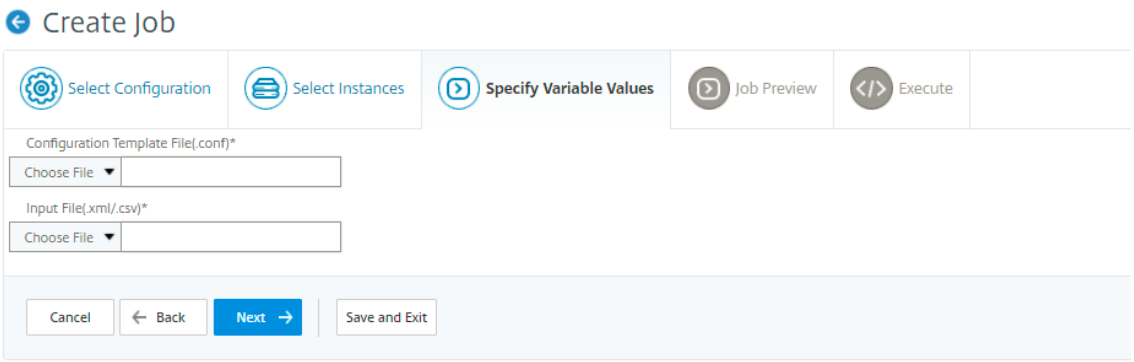


```
#InstanceGroup,NSIP,HostName,LBSERVER,SNMPTrapDest
example_doc,,,,
#Instance(s),NSIP,HostName,LBSERVER,SNMPTrapDest
10.xx.xx.xx,,,,
<!--NeedCopy-->
```

Le même fichier est affiché dans Microsoft Excel :

#job-s_variable_input_key_file				
#Global	NSIP	HostName	*LBSERVER*	SNMPTrapDest
Global Values				
#InstanceGroup	NSIP	HostName	LBSERVER	SNMPTrapDest
example_doc				
#Instance(s)	NSIP	HostName	LBSERVER	SNMPTrapDest

10. Cliquez sur **Suivant**.



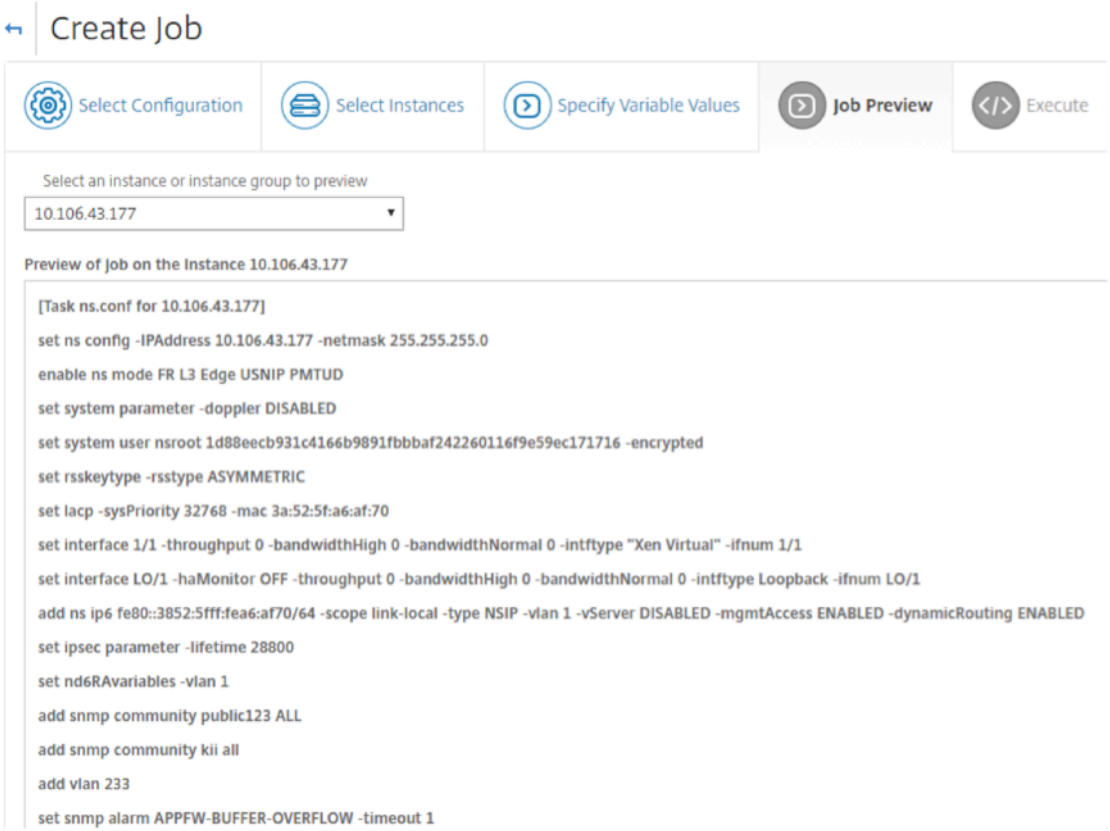
Les fichiers d'entrée contenant les valeurs de variables sont conservés (avec le même nom de fichier) dans les tâches de configuration. Vous pouvez afficher et modifier ces fichiers d'entrée que vous avez utilisés et chargés précédemment lors de la création ou de la modification des tâches de configuration.

Pour afficher les travaux de configuration exécutés lors de la création d'un travail de configuration, accédez à **Réseau** > **Travaux de configuration**, puis cliquez sur **Créer un travail**. Dans la page **Créer une tâche**. Sous l'onglet **Spécifier les valeurs 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 chargez les fichiers (en conservant le même nom de fichier).

Pour afficher les travaux de configuration déjà exécutés lors de la modification d'un travail de configuration, accédez à **Réseau** > **Travaux de configuration**, sélectionnez le nom du travail et cliquez sur **Modifier**. Dans la page **Configurer la tâche**, sous l'onglet **Spécifier les valeurs de**

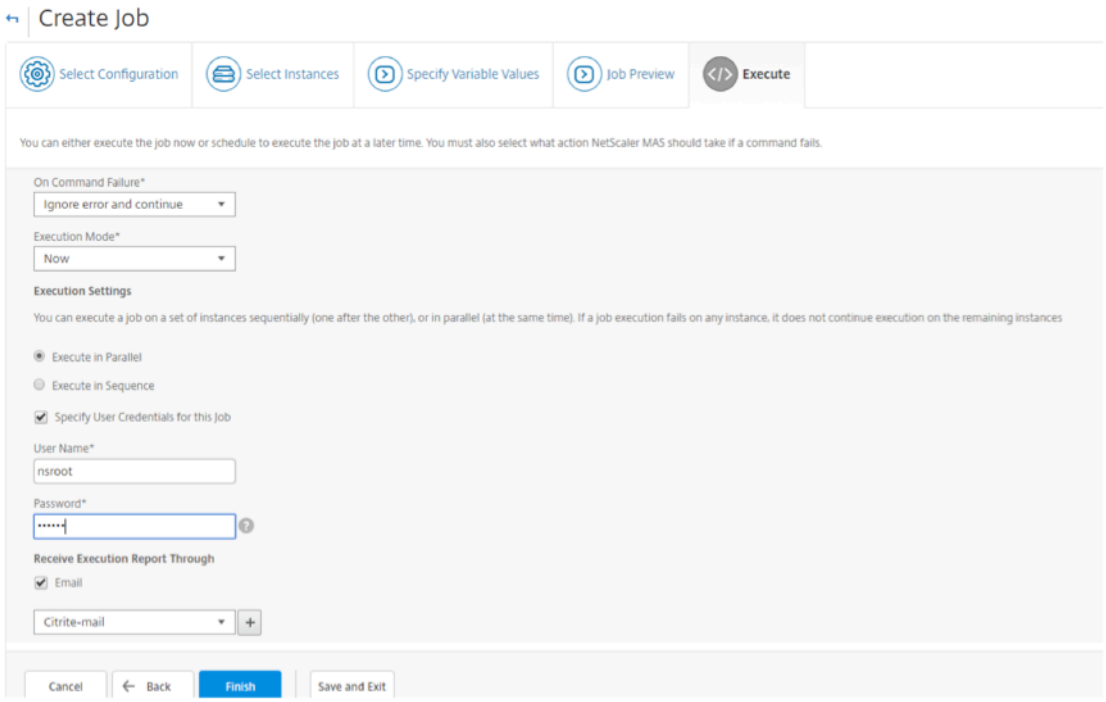
variable, sélectionnez l'option **Valeurs variables communes pour toutes les instances** pour afficher les fichiers chargés. Pour modifier les fichiers d'entrée, téléchargez le fichier d'entrée, puis modifiez et téléchargez les fichiers (en conservant le même nom de fichier).

11. 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** .

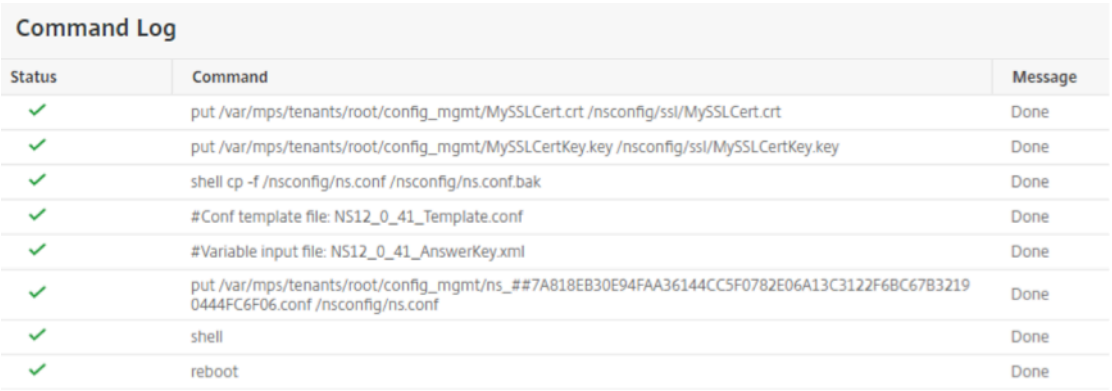


12. Sous l'onglet**Exécuter**, vous pouvez choisir d'exécuter votre travail maintenant ou de le programmer pour qu'il soit exécuté ultérieurement. Vous pouvez également choisir l'action que Citrix ADM doit prendre en cas d'échec de la commande.

    Vous pouvez également choisir d'autoriser les utilisateurs autorisés à exécuter des travaux sur vos instances gérées, et vous pouvez choisir d'envoyer une notification par e-mail concernant le succès ou l'échec de la tâche, ainsi que d'autres détails.



Après avoir exécuté votre travail, vous pouvez voir les détails de la tâche en accédant à **Réseaux** > Tâces de **configuration** et sélectionnez la tâche que vous venez de configurer. Cliquez sur **Détails**, puis sur **Récapitulatif de l'exécution** pour afficher les détails de votre tâche. Cliquez sur l'instance pour afficher les **journaux des commandes** pour voir les commandes exécutées sur la tâche.



Command Log

Status	Command	Message
✓	put /var/mps/tenants/root/config_mgmt/MySSLCert.crt /nsconfig/ssl/MySSLCert.crt	Done
✓	put /var/mps/tenants/root/config_mgmt/MySSLCertKey.key /nsconfig/ssl/MySSLCertKey.key	Done
✓	shell cp -f /nsconfig/ns.conf /nsconfig/ns.conf.bak	Done
✓	#Conf template file: NS12_0_41_Template.conf	Done
✓	#Variable input file: NS12_0_41_AnswerKey.xml	Done
✓	put /var/mps/tenants/root/config_mgmt/ns_##7A818EB30E94FAA36144CC5F0782E06A13C3122F6BC67B32190444FC6F06.conf /nsconfig/ns.conf	Done
✓	shell	Done
✓	reboot	Done

Utiliser les tâches pour mettre à niveau les instances de Citrix ADC

April 29, 2021

Dans Citrix Application Delivery Management (ADM), vous pouvez mettre à niveau une ou plusieurs instances Citrix ADC. Vous devez connaître le cadre de licences et les types de licences avant de mettre à niveau une instance.

Conditions préalables

Avant de mettre à niveau une instance ADC, effectuez la vérification de pré-validation de l'instance que vous souhaitez mettre à niveau.

1. **Rechercher des personnalisations** - Sauvegardez vos personnalisations et supprimez-les des instances. Vous pouvez réappliquer les personnalisations sauvegardées après la mise à niveau de l'instance.
2. **Rechercher des problèmes matériels de disque** - Résolvez les problèmes matériels, le cas échéant.

Paire haute disponibilité ADC

Lorsque vous mettez à niveau une paire ADC haute disponibilité, notez ce qui suit :

- Le nœud secondaire est mis à niveau en premier.
- La synchronisation et la propagation des nœuds sont désactivées jusqu'à ce que les deux nœuds soient correctement mis à niveau.
- Après la mise à niveau des paires haute disponibilité réussie, un message d'erreur s'affiche dans l'historique d'exécution. Ce message s'affiche si vos nœuds de la paire haute disponibilité sont sur différentes versions ou versions. Ce message indique que la synchronisation entre le nœud principal et le nœud secondaire est désactivée.

Vous pouvez mettre à niveau une paire ADC haute disponibilité en deux étapes :

1. Créez un travail de mise à niveau et exécutez immédiatement sur l'un des nœuds ou planifiez plus tard.
2. Planifiez ultérieurement l'exécution du travail de mise à niveau sur le nœud restant. Assurez-vous de planifier ce travail après la mise à niveau du nœud initial.

Clusters CAN

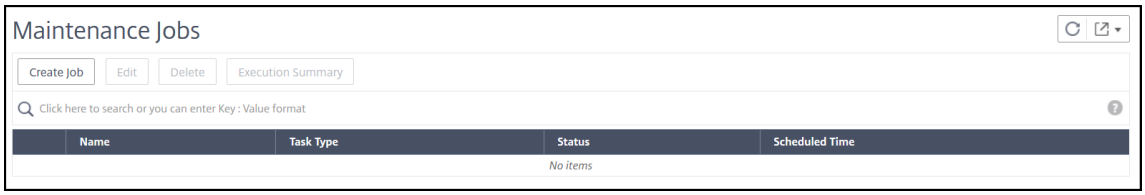
Lorsque vous mettez à niveau un cluster ADC, lors de l'étape de validation préalable à la mise à niveau, l'ADM valide uniquement l'instance spécifiée. Par conséquent, vérifiez et résolvez les problèmes suivants sur les nœuds de cluster :

- Personnalisation
- Utilisation du disque
- problèmes matériels

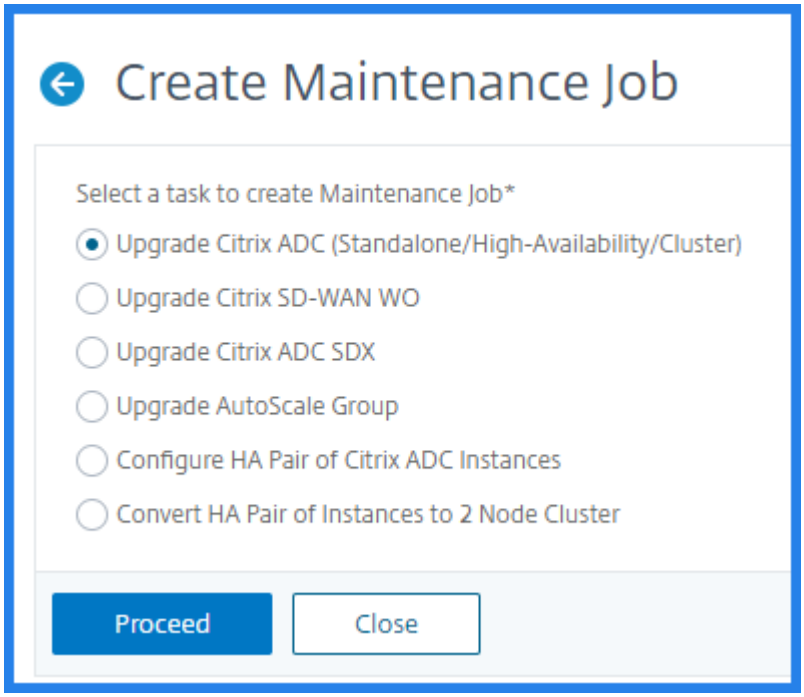
Créer une tâche de mise à niveau ADC

Pour créer une tâche de mise à niveau ADC, procédez comme suit :

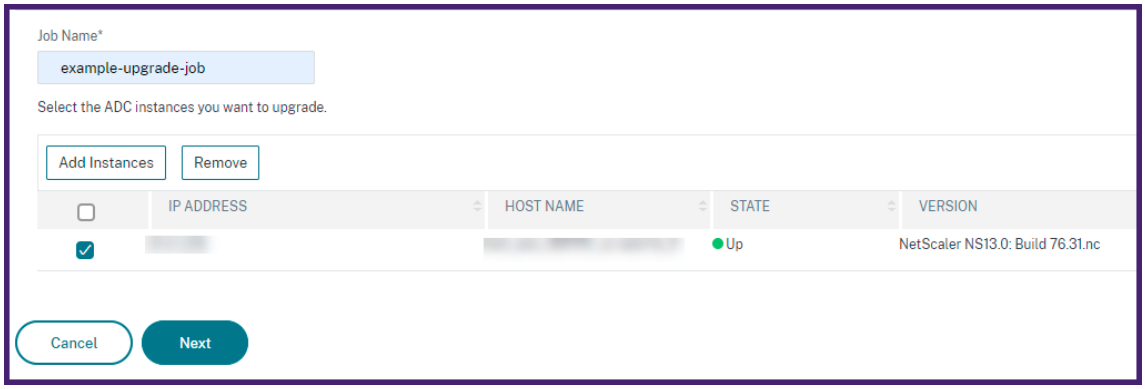
1. Accédez à **Réseaux > Travail de configuration > Tâche de maintenance**.



2. Dans **Créer des tâches de maintenance**, sélectionnez **Mettre à niveau Citrix ADC (Standalone/Haute Disponibilité/Cluster)** et cliquez sur **Continuer**.



3. Dans **Sélectionner une instance**, tapez le nom de votre choix pour **Nom du travail**.
4. Cliquez sur **Ajouter des instances** pour ajouter des instances ADC à mettre à niveau.
   - Pour mettre à niveau une paire ADC haute disponibilité, spécifiez l'adresse IP du nœud principal ou secondaire.
   - Pour mettre à niveau un cluster, spécifiez l'adresse IP du cluster.



5. Cliquez sur **Suivant** pour lancer la validation de pré-mise à niveau sur les instances sélectionnées.

   L'onglet **Validation préalable à la mise à niveau** affiche les instances ayant échoué. Vous pouvez supprimer les instances ayant échoué et cliquer sur **Suivant**.

   > **Important**
   >
   > Si vous spécifiez l'adresse IP du cluster, l'ADM effectue la validation préalable à la mise à niveau uniquement sur l'instance spécifiée et non sur les autres nœuds du cluster.

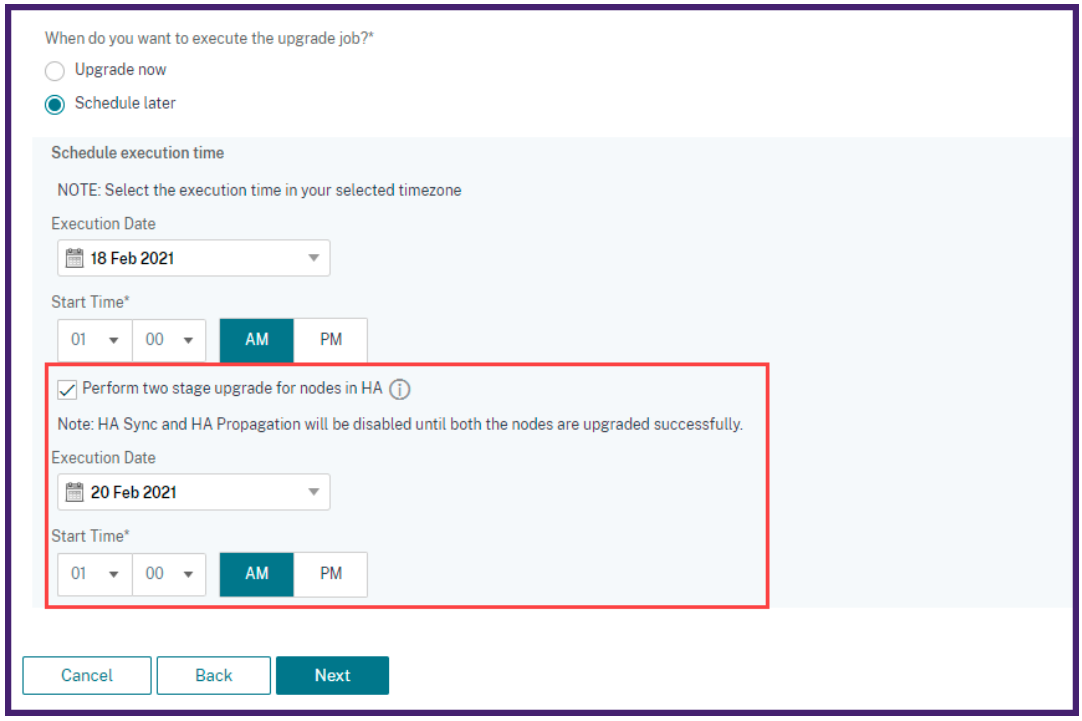
6. Facultatif, dans **Scripts personnalisés**, spécifiez les scripts à exécuter avant et après une mise à niveau d'instance. Pour de plus amples informations, consultez la section Utiliser des scripts personnalisés.

7. Dans **Planifier la tâche**, sélectionnez l'une des options suivantes :

   - **Mise à niveau maintenant** : le travail de mise à niveau s'exécute immédiatement.
   - **Planifier plus tard** : sélectionnez cette option pour exécuter ce travail de mise à niveau ultérieurement. Spécifiez la **date d'exécution** et l'**heure de début** lorsque vous souhaitez mettre à niveau les instances.

     Si vous souhaitez mettre à niveau une paire ADC haute disponibilité en deux étapes, sélectionnez **Effectuer une mise à niveau en deux étapes pour les nœuds en haute disponibilité**.

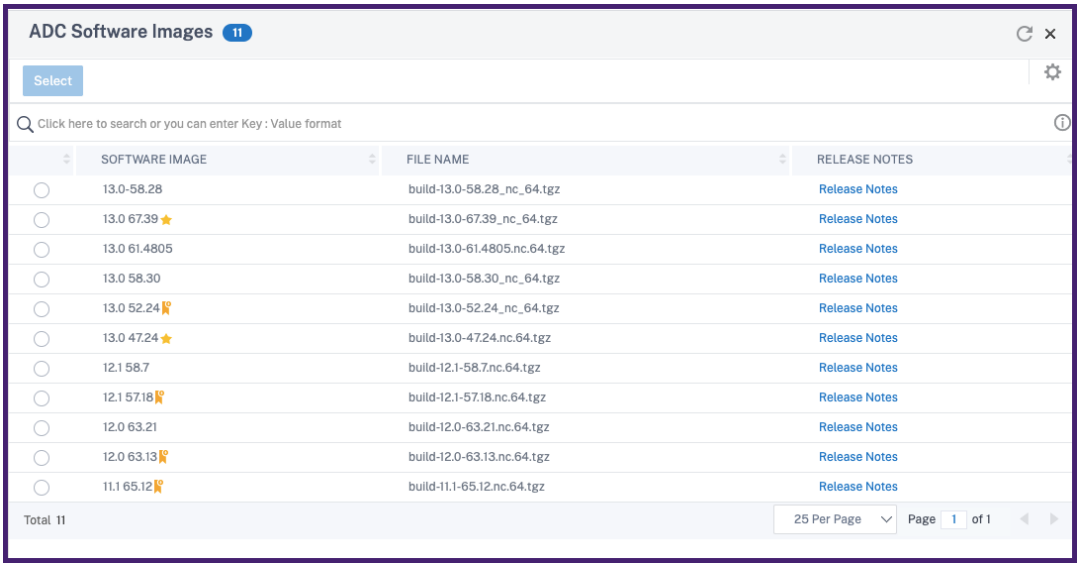
     Spécifiez la **date d'exécution** et l' **heure de début** lorsque vous souhaitez mettre à niveau une autre instance dans la paire haute disponibilité.



Pour de plus amples informations, consultez la section Paire haute disponibilité ADC.

8. Dans **Créer une tâche**, spécifiez les détails suivants :

   - **Sélectionnez l'image du logiciel ADC** : sélectionnez une image ADC dans la liste. Cette option répertorie toutes les images ADC disponibles sur le site Web Citrix Téléchargements.



     Les images du logiciel ADC affichent les versions préférées avec l'icône étoile. Et, les versions les plus téléchargées avec l'icône de signet.

   - **Télécharger l'image du logiciel ADC** : vous pouvez télécharger l'image à partir de votre ordinateur local ou de l'appliance ADC. Lorsque vous sélectionnez le dispositif ADC, l'interface graphique ADM affiche les fichiers d'instance présents dans `/var/mps/mps_images`. Sélectionnez l'image dans l'interface graphique ADM.

   Si vous planifiez le travail de mise à niveau, vous pouvez spécifier quand vous souhaitez télécharger l'image vers une instance :

   - **Télécharger maintenant** : sélectionnez cette option pour télécharger l'image immédiatement. Toutefois, le travail de mise à niveau s'exécute à l'heure planifiée.
   - **Charger au moment de l'exécution** : sélectionnez cette option pour télécharger l'image au moment de l'exécution du travail de mise à niveau.

   Pour plus d'informations sur les autres options de mise à niveau, consultez Options de mise à niveau ADC.

9. Cliquez sur **Créer une tâche**.

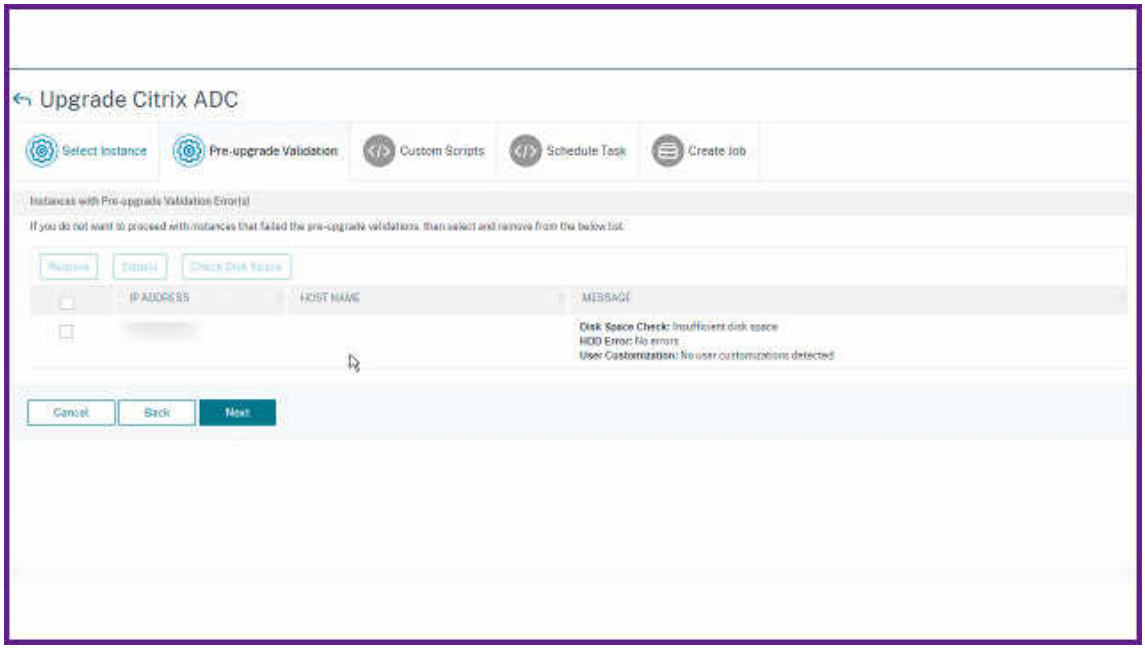
Le travail de mise à niveau apparaît dans **Réseaux > Travail de configuration > Tâche de maintenance**. Lorsque vous modifiez une tâche existante, vous pouvez basculer vers n'importe quel onglet si les champs obligatoires sont déjà remplis. Par exemple, si vous êtes dans l'onglet **Sélectionner une configuration**, vous pouvez basculer vers l'onglet **Aperçu des travaux**.

Nettoyer l'espace disque ADC

Si vous rencontrez un problème d'espace disque insuffisant lors de la mise à niveau d'une instance ADC, nettoyez l'espace disque de l'interface graphique ADM elle-même.

1. Dans l'onglet **Validation préalable à la mise à niveau**, sélectionnez l'instance qui présente le problème d'espace disque.
2. Sélectionnez **Vérifier l'espace disque**.

   Ce volet affiche le disque de l'instance qui dispose d'un espace insuffisant. Il affiche également la quantité de mémoire utilisée et disponible sur le disque.
3. Dans le volet **Vérifier l'espace disque**, sélectionnez l'instance qui nécessite un nettoyage.
4. Cliquez sur **Nettoyage de disque**.



5. Sélectionnez les fichiers que vous souhaitez effacer.
6. Cliquez sur **Supprimer**

Utiliser des scripts personnalisés

Vous pouvez spécifier des scripts personnalisés lorsque vous créer une tâche de mise à niveau ADC. Les scripts personnalisés sont utilisés pour vérifier les modifications avant et après une mise à niveau d'instance ADC. Par exemple :

- Version d'instance avant et après la mise à niveau.
- État des interfaces, des nœuds haute disponibilité, des serveurs virtuels et des services avant et après la mise à niveau.

- Les statistiques des serveurs et services virtuels.
- Les routes dynamiques.

Spécifiez les scripts personnalisés à exécuter dans les étapes suivantes :

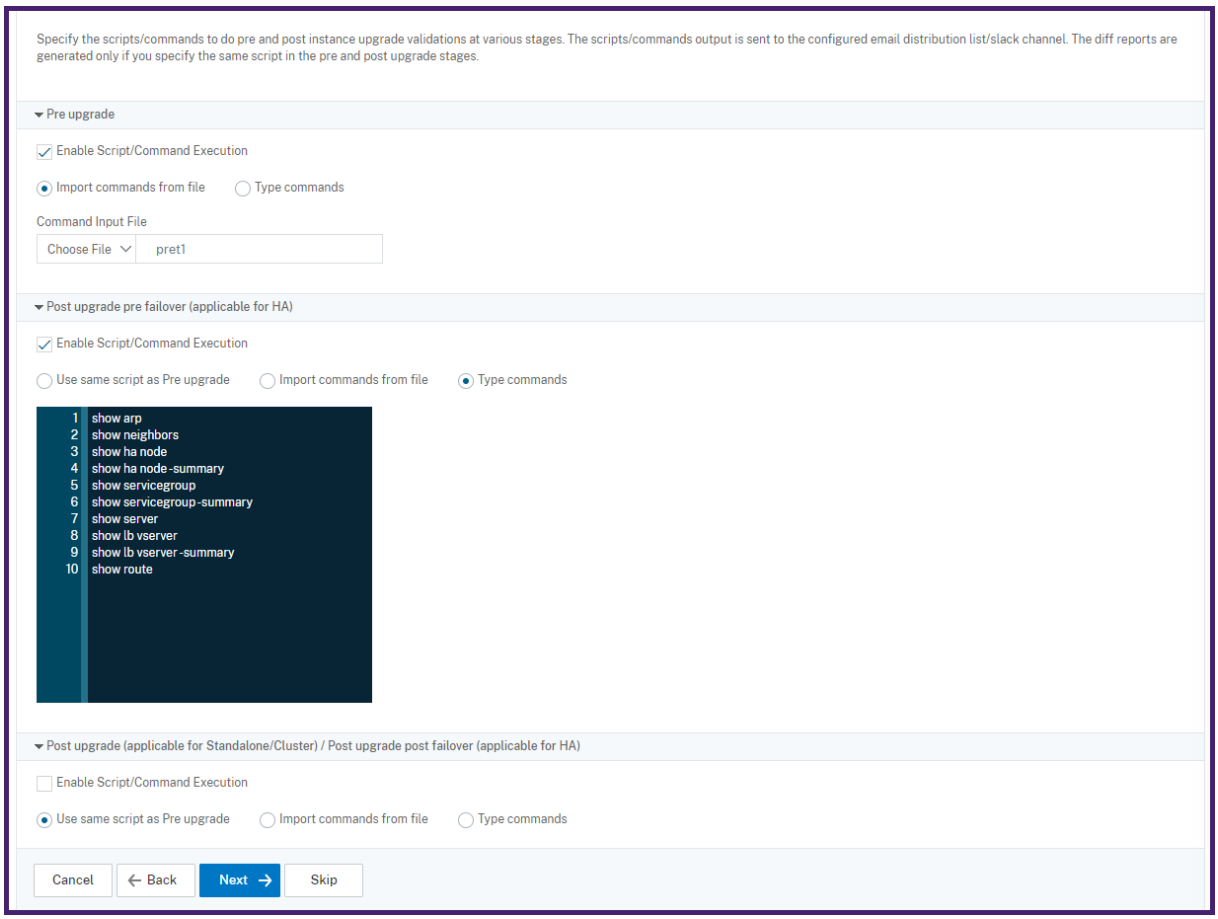
- **Prémise à niveau** : le script spécifié s'exécute avant la mise à niveau d'une instance.
- **Après la mise à niveau avant basculement (applicable pour HA)** : Cette étape s'applique uniquement au déploiement haute disponibilité. Le script spécifié s'exécute après la mise à niveau des nœuds, mais avant leur basculement.
- **Post upgrade (applicable pour autonome)/Post upgrade post basculement (applicable pour HA)** : Le script spécifié s'exécute après la mise à niveau d'une instance dans le déploiement autonome. Dans le déploiement haute disponibilité, le script s'exécute après la mise à niveau des nœuds et leur basculement sur incident.

> **Remarque**
>
> - Assurez-vous d'activer l'exécution du script ou des commandes aux étapes requises. Sinon, les scripts spécifiés ne s'exécutent pas.
> - Le rapport diff n'est généré que si vous spécifiez le même script dans les étapes de pré-mise à niveau et de post-mise à niveau. Par conséquent, veillez à sélectionner **Utiliser le même script que Pré-mise à niveau** dans les étapes de post-mise à niveau. Consultez Télécharger un rapport de diff consolidé d'une tâche de mise à niveau ADC.

Vous pouvez importer un fichier script ou taper des commandes directement dans l'interface graphique ADM.

- **Importer les commandes à partir du fichier** : sélectionnez le fichier d'entrée de commande à partir de votre ordinateur local.
- **Commandes de type** : entrez les commandes directement sur l'interface graphique.

Dans les étapes de post-mise à niveau, vous pouvez utiliser le même script spécifié dans l'étape de pré-mise à niveau.

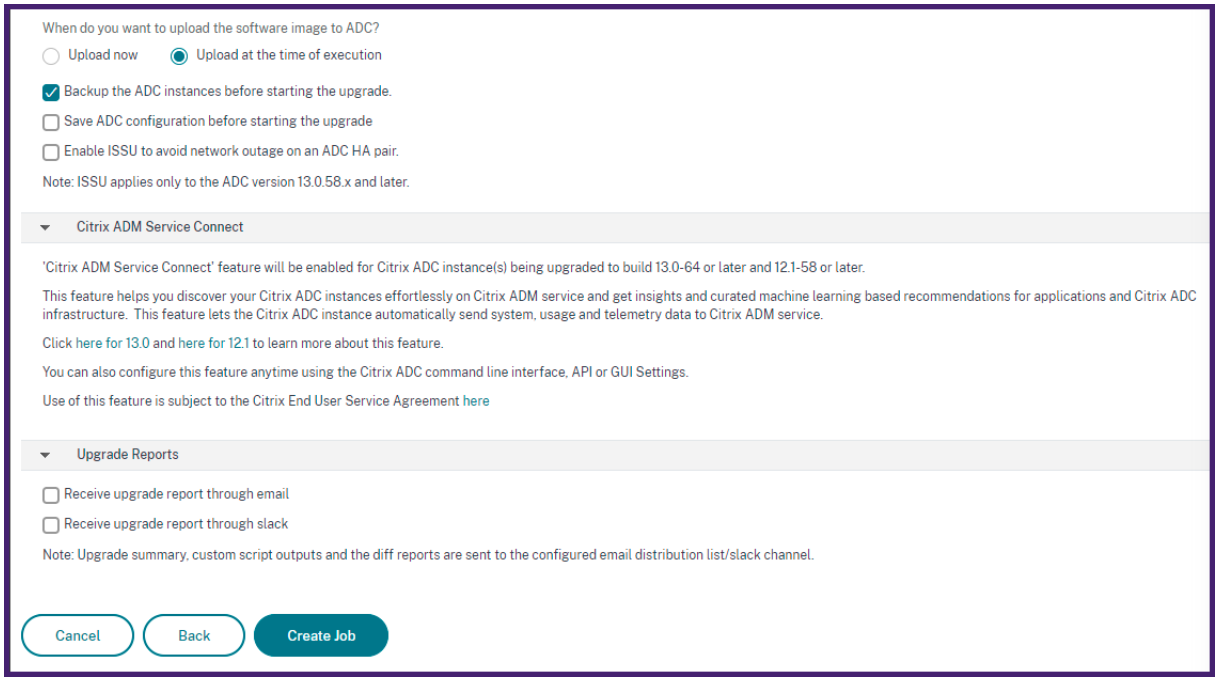


Options de mise à niveau ADC

Pendant que vous créer une tâche de mise à niveau ADC, vous pouvez sélectionner les options suivantes dans l'onglet **Créer une tâche** :

- **Nettoyer l'image logicielle à partir de Citrix ADC lors de la mise à niveau réussie** - Sélectionnez cette option pour effacer l'image téléchargée dans l'instance ADC après la mise à niveau de l'instance.
- **Sauvegardez les instances ADC avant de commencer la mise à niveau.** : crée une sauvegarde des instances ADC sélectionnées.
- **Conserver le statut principal et secondaire des nœuds haute disponibilité après la mise à niveau** : sélectionnez cette option si vous souhaitez que le travail de mise à niveau initie un basculement après la mise à niveau de chaque nœud. De cette façon, le travail de mise à niveau conserve l'état principal et secondaire des nœuds.
- **Enregistrer la configuration ADC avant de commencer la mise à niveau** - Enregistre la configuration ADC en cours d'exécution avant la mise à niveau des instances ADC.

- **Permet à ISSUE d'éviter une panne réseau sur une paire ADC HA** - ISSU garantit la mise à niveau zéro temps d'arrêt sur une paire ADC haute disponibilité. Cette option fournit une fonctionnalité de migration qui respecte les connexions existantes lors de la mise à niveau. Ainsi, vous pouvez mettre à niveau une paire ADC haute disponibilité sans temps d'arrêt. Spécifiez le délai de migration ISSU en minutes.
- **Recevoir le rapport d'exécution par e-mail** - Envoie le rapport d'exécution par e-mail. Pour ajouter une liste de distribution d'e-mails, reportez-vous à la section Créer une liste de distribution d'e-mails.
- **Recevoir le rapport d'exécution via la marge** - Envoie le rapport d'exécution en marge. Pour ajouter un profil Slack, reportez-vous à la section Créer un profil Slack.



Télécharger un rapport de diff consolidé d'une tâche de mise à niveau ADC

Dans Citrix ADM, vous pouvez télécharger un rapport diff d'une tâche de mise à niveau d'ADC. Pour ce faire, la tâche de mise à niveau doit avoir scripts personnalisés. Un rapport diff contient les différences entre les sorties du script pré-mise à niveau et post-mise à niveau. Avec ce rapport, vous pouvez déterminer quelles modifications ont eu lieu sur l'instance ADC après mise à niveau.

> **Remarque**
>
> Le rapport diff n'est généré que si vous spécifiez le même script dans les étapes de pré-mise à niveau et de post-mise à niveau.

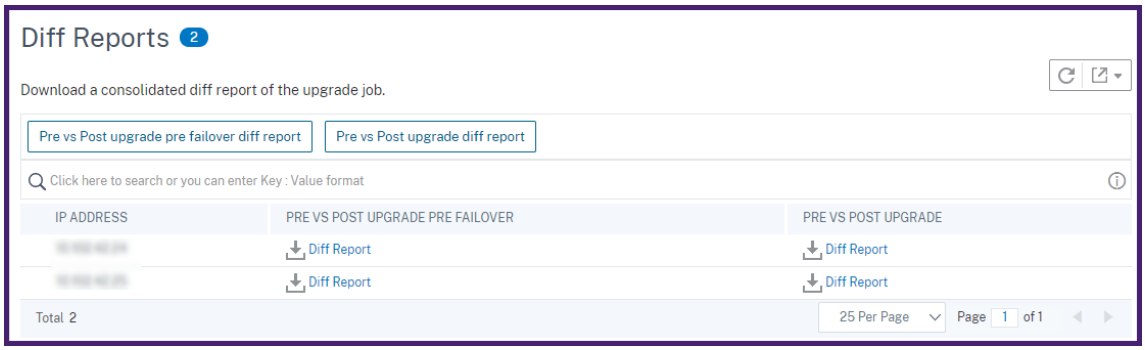
Pour télécharger un rapport diff d'une tâche de mise à niveau, procédez comme suit :

1. Accédez à **Réseaux > Tâches de configuration > Tâches de maintenance**.

2. Sélectionnez le travail de mise à niveau pour lequel vous souhaitez télécharger un rapport de diff.
3. Cliquez sur **Rapports de différé**.
4. Dans **Rapports Diff**, téléchargez un rapport de diff consolidé du travail de mise à niveau sélectionné.

   Dans cette page, vous pouvez télécharger l'un des rapports diff suivants :

   - **Rapport de différentiel pré-basculement avant la mise à niveau et après mise à niveau**
   - **Rapport de diff pré vs post mise à niveau**



Utiliser des modèles de configuration pour créer des modèles d'audit

April 29, 2021

Vous pouvez désormais utiliser des commandes de configuration précédemment enregistrées en tant que modèles de configuration pour créer des modèles d'audit qui peuvent être appliqués à des instances Citrix ADC spécifiques. Lors de la création d'un modèle d'audit, vous pouvez faire glisser des modèles de configuration précédemment enregistrés dans le champ **Commandes** et modifier le modèle en fonction de vos besoins. Vous pouvez ensuite appliquer le modèle d'audit à des instances Citrix ADC spécifiques. Citrix Application Delivery Management (ADM) compare ces instances avec le modèle d'audit et signale toute incompatibilité. Ce processus vous aide à identifier les erreurs et à les corriger en temps opportun.

Vous pouvez créer des modèles de configuration tout en créant un travail et en enregistrant un ensemble de commandes de configuration en tant que modèle. Lorsque vous enregistrez ces modèles sur la page **Créer des travaux**, ils sont automatiquement affichés sur la page **Créer un modèle**.

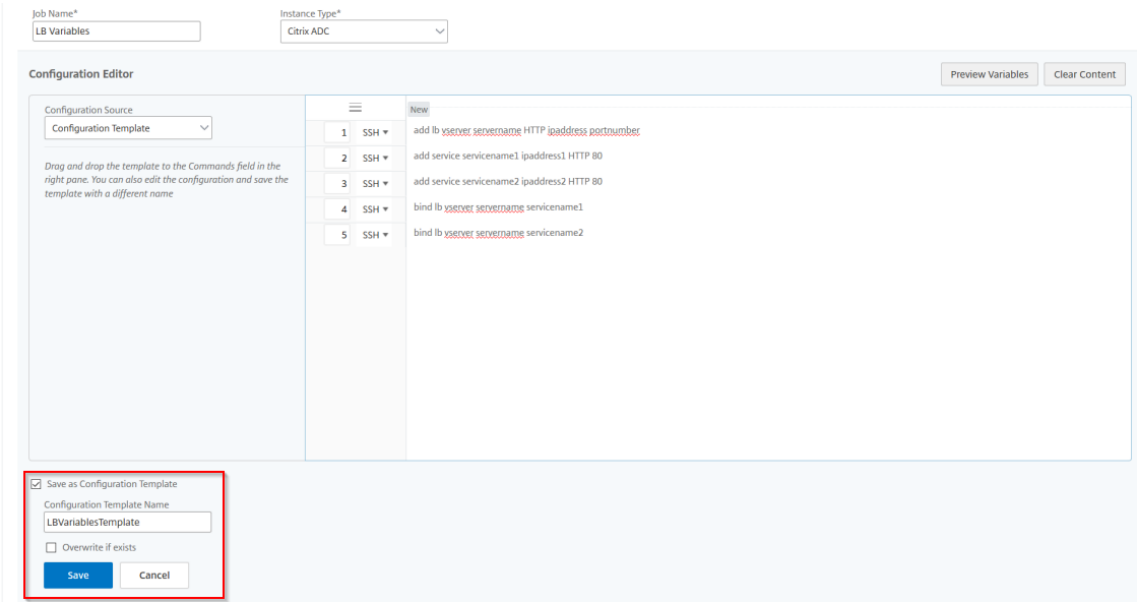
Par exemple, considérez une configuration d'équilibrage de charge de base pour laquelle vous ajoutez un serveur virtuel d'équilibrage de charge, ajoutez deux services et liez les services au serveur virtuel.

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 :

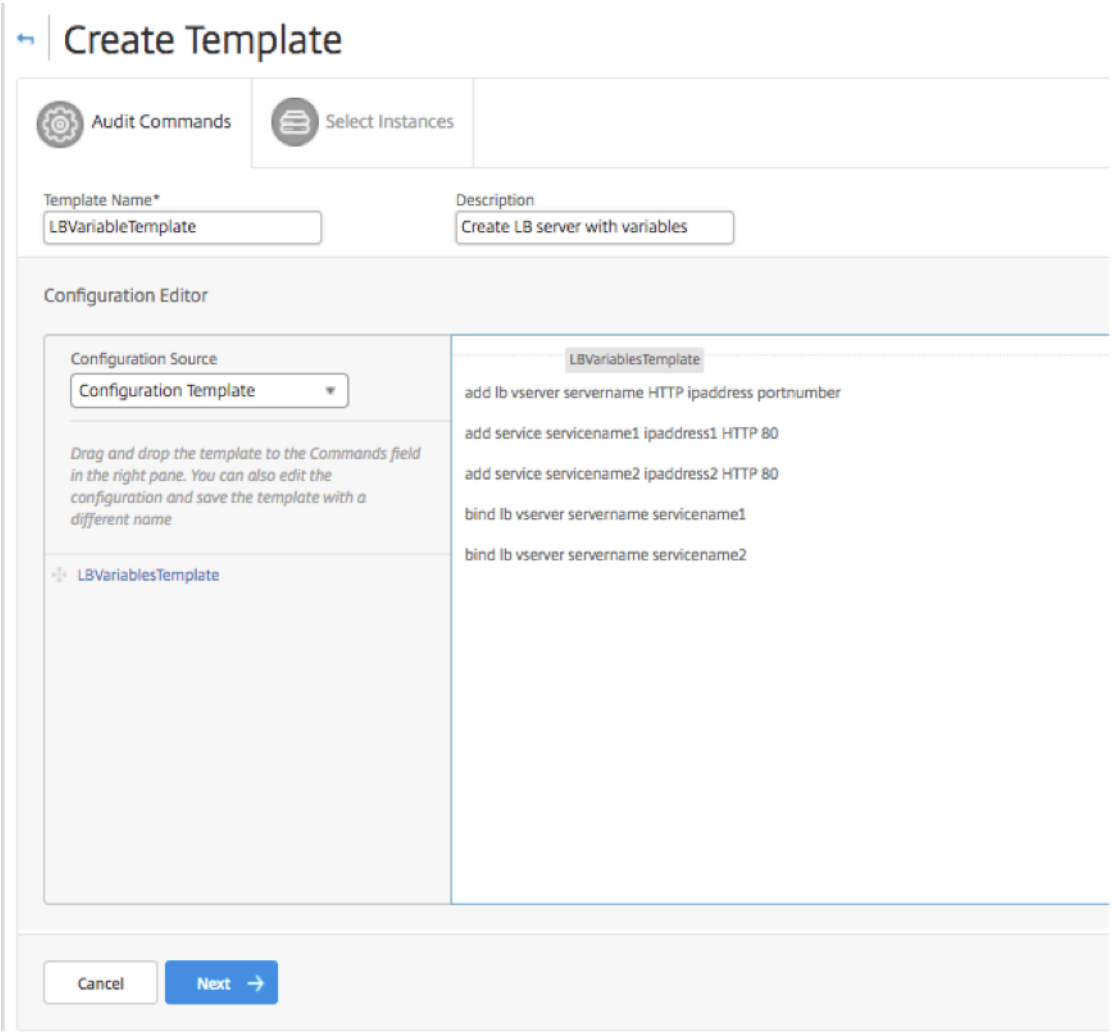
1. Accédez à **Réseaux** > **Travaux de configuration**, puis cliquez sur **Créer un travail**.
2. Sur la page **Créer un travail**, spécifiez le nom du travail et le type d'instance.
3. Choisissez **Modèle de configuration** comme Source de configuration et, dans le champ **Commandes**, entrez des commandes telles que celles de l'exemple précédent.
4. Activez la case à cocher **Enregistrer en tant que modèle de configuration** et indiquez un nom pour votre modèle. Vous pouvez choisir d'écraser d'autres modèles qui existent avec le même nom.
5. Cliquez sur **Enregistrer**.



Pour utiliser un modèle de configuration pour créer un modèle d'audit dans Citrix ADM :

1. Accédez à **Réseaux** > **Audit de configuration** > **Modèles d'audit**, puis cliquez sur **Ajouter**.
2. Dans la page **Créer un modèle**, spécifiez un nom pour le nom du modèle et entrez une description.
3. Dans la liste **Source de configuration**, sélectionnez **Modèle de configuration**, puis faites glisser le modèle dans le champ Commandes dans le volet droit. Vous pouvez également modifier la configuration et enregistrer le modèle sous un autre nom. Cliquez sur **Suivant**.

4. Sous l'onglet **Sélectionner des instances**, cliquez sur **Ajouter des instances** et ajoutez les instances sur lesquelles vous souhaitez exécuter la configuration. Cliquez sur **OK**.
5. Cliquez sur **Terminer**.



Le modèle d'audit apparaît dans la liste Modèles d'audit et est exécuté toutes les 12 heures par rapport aux configurations des instances spécifiées.

Utiliser la commande SCP (put) dans les tâches de configuration

April 29, 2021

Vous pouvez utiliser la fonctionnalité **Jobs de configuration** de Citrix Application Delivery Management (ADM) pour créer des tâches de configuration, envoyer des notifications par e-mail et vérifier les journaux d'exécution des tâches créées. Un travail 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 de périphériques.

Les tâches de configuration dans Citrix ADM utilisent les commandes Secure Shell (SSH) pour configurer des instances, et vous pouvez configurer une tâche de configuration pour utiliser la copie sécurisée (SCP) pour transférer des fichiers en toute sécurité. SCP est basé sur le protocole SSH. L'une des commandes SCP que vous pouvez inclure dans une tâche de configuration est la commande « put ». Vous pouvez utiliser la commande « put » dans les tâches de configuration pour télécharger ou transférer un ou plusieurs fichiers stockés dans un répertoire local de votre système vers Citrix ADM, puis vers un répertoire sur l'instance ou les instances de Citrix ADC.

> **Remarque**
>
> Le fichier est téléchargé sur Citrix ADM et il est ensuite copié (mis) dans les instances Citrix ADC sélectionnées. Le fichier téléchargé est stocké dans Citrix ADM et est supprimé uniquement lorsque le travail est supprimé. Ceci est nécessaire pour les travaux planifiés pour s'exécuter plus tard.

La commande a la syntaxe suivante :

```
put <local_filename> <remote_path/remote_filename>
<!--NeedCopy-->
```

Où,

<local_filename> est le nom du fichier local à télécharger.

<remote_path/ remote_filename> est le chemin d'accès à un répertoire distant et le nom à attribuer au fichier lorsqu'il est copié dans ce répertoire.

Lors de la création du travail de configuration, vous pouvez convertir les paramètres de nom de fichier local et distant en variables. Cela vous permet d'affecter différents fichiers à ces paramètres pour le même ensemble d'instances Citrix ADC chaque fois que vous exécutez le travail. En outre, lorsque vous utilisez un fichier à plusieurs endroits dans une tâche et si vous souhaitez renommer le fichier, vous pouvez redéfinir la variable au lieu de changer le nom du fichier à tous les endroits.

Pour utiliser la commande put pour télécharger des fichiers dans une tâche de configuration :

1. Dans Citrix ADM, accédez à **Réseaux** > **Travaux de configuration**.
2. Sur la page **Travaux**, cliquez sur **Créer un travail** .
3. Dans la page **Créer un travail**, entrez le nom du travail dans le champ Nom du travail et, dans le volet **Éditeur de configuration**, entrez la commande « put ».

   Par exemple, si vous souhaitez créer un travail de configuration qui copie un fichier de certificat SSL enregistré sur votre système local vers plusieurs instances Citrix ADC, vous pouvez ajouter

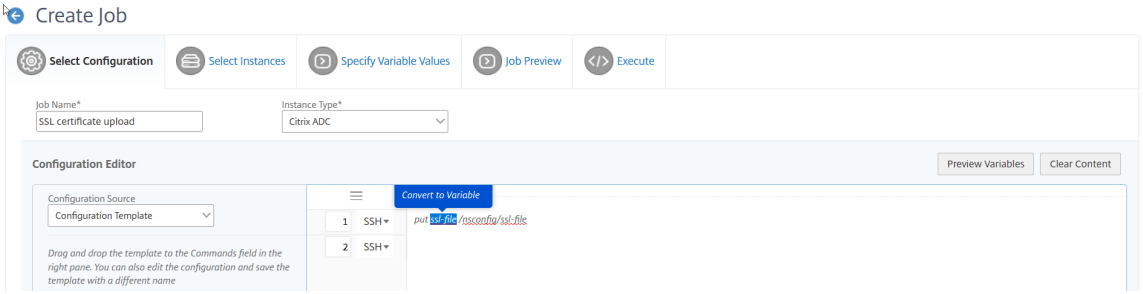
une commande « put » qui utilise une variable au lieu du nom d'un fichier particulier et définir le type de variable comme « fichier ».

```
1 put ssl-file /nsconfig/ssl-file
2 <!--NeedCopy-->
```

Dans cet exemple,

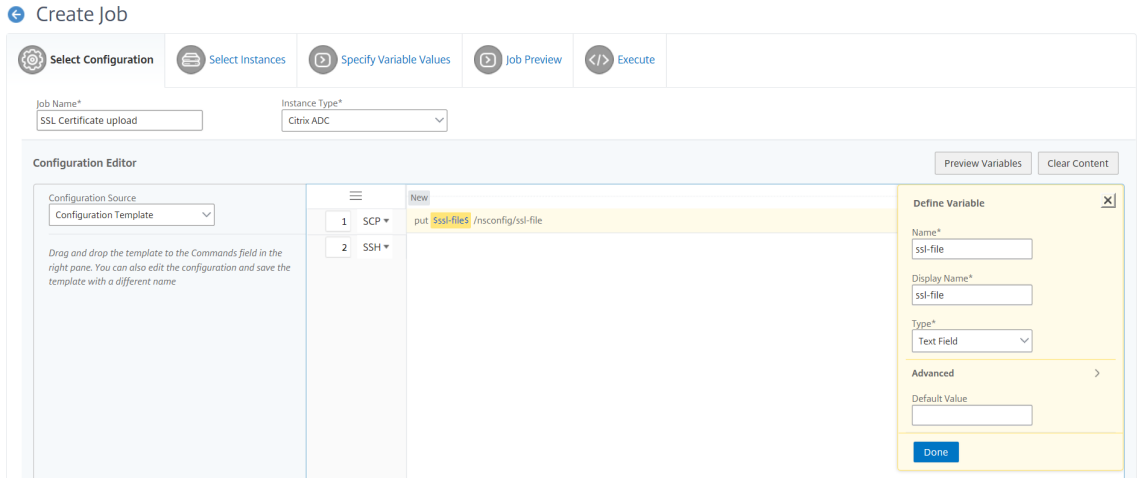
- `ssl-file` : c'est le nom du fichier qui doit être téléchargé dans l'instance Citrix ADC.
- `/nsconfig/ssl-file` - c'est le dossier de destination sur l'instance où le `ssl-file` sera placé après l'exécution de la tâche.

4. Dans la commande que vous avez saisie, sélectionnez le nom de fichier que vous souhaitez convertir en variable, puis cliquez sur **Convertir en variable**, comme illustré dans la figure suivante.



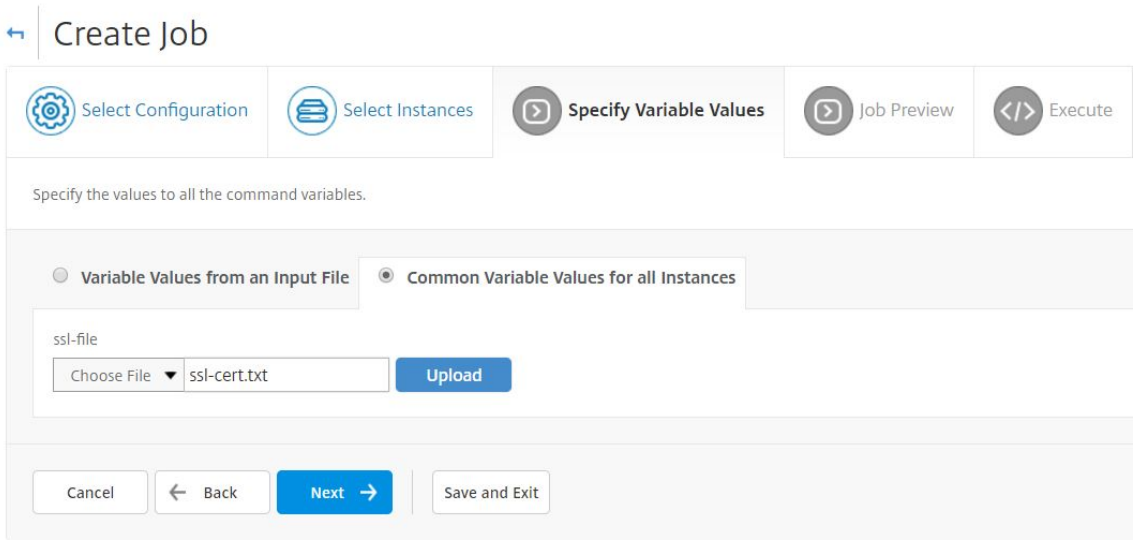
5. Vérifiez que le nom du fichier a été entouré de signes dollar (indiquant qu'il s'agit maintenant d'une variable), puis cliquez sur la variable.
6. Spécifiez les détails de la variable, tels que le nom, le nom complet et le type.
7. Dans la liste déroulante **Type**, sélectionnez **Fichier** . Cliquez 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 Citrix ADC vers lesquelles copier les fichiers.

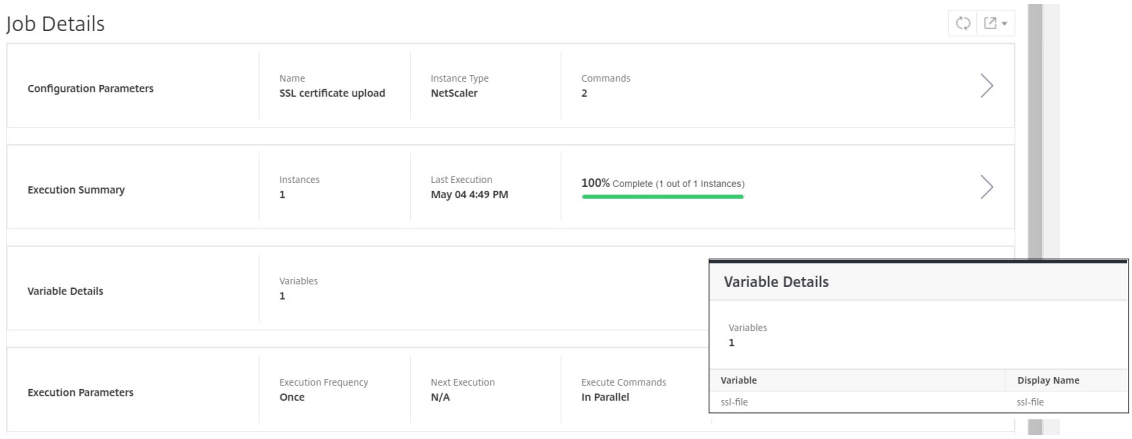
9. Sous l'onglet **Spécifier les valeurs de variable**, sélectionnez la section **Valeurs de variables communes pour toutes les instances**, sélectionnez le fichier dans le stockage local de votre système, cliquez sur Télécharger pour **télécharger** le fichier sur Citrix ADM, puis cliquez sur **Suivant** .



10. Sous l'onglet **Aperçu des tâches**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances.

11. Sous l'onglet **Exécuter**, vous pouvez exécuter le travail maintenant ou planifier son exécution ultérieure. Vous pouvez également choisir l'action que Citrix ADM doit prendre en cas d'échec de la commande. Vous pouvez également créer une notification par e-mail pour recevoir une notification sur le succès ou l'échec de la tâche, ainsi que d'autres détails. Cliquez sur **Terminer**.

12. Vous pouvez afficher les détails de la tâche en accédant à **Réseaux** > Tâces de **configuration**et en sélectionnant la tâche que vous avez configurée. Cliquez sur **Détails**, puis cliquez sur **Détails de la variable**pour répertorier les variables ajoutées à votre tâche.



Replanifier les tâches configurées à l'aide de modèles intégrés

April 29, 2021

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 aviez 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 une tâche configurée 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 le travail.

> **Remarque**
>
> Vous pouvez également sélectionner la tâche et cliquer à nouveau sur **Exécuter** pour exécuter la tâche sans modifier la source, l'instance et les commandes. Ceci est utile lorsque vous devez exécuter le même ensemble de commandes sur les mêmes instances. Parfois, le travail peut rencontrer une erreur transitoire du côté serveur, et vous devrez peut-être exécuter à nouveau la tâche.

Réutiliser les modèles d'audit de configuration dans les tâches de configuration

April 29, 2021

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 lorsque vous exécutez un audit de configuration. Le modèle de configuration créé et enregistré dans le module **Jobs de configuration** 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 **Audit de configuration** est disponible dans les travaux de configuration afin que vous puissiez exécuter le modèle en tant que travail de configuration. Toute modification apportée au modèle est désormais visible dans les modules Jobs de **configuration et Configuration Audi**t.

Auparavant, les modèles de travail de configuration et d'audit de configuration devaient être créés séparément pour la même configuration et enregistrés en tant que fichiers différents. Cela a provoqué

une duplication des efforts dans la création et 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 travaux de configuration et les audits de configuration.

Par exemple, envisagez une configuration d'équilibrage de charge de base pour laquelle vous ajoutez un serveur virtuel d'équilibrage de charge, ajoutez deux services et liez les services au serveur virtuel.

Cet exemple utilise les commandes suivantes :

```
add lb vserver servername HTTP ipaddress portnumber

add service servicename1 ipaddress1 HTTP 80

add service servicename2 ipaddress2 HTTP 80

bind lb vserver servername servicename1

bind lb vserver servername servicename2
<!--NeedCopy-->
```

Création d'un modèle dans les audits de configuration et réutilisation dans les travaux de configuration

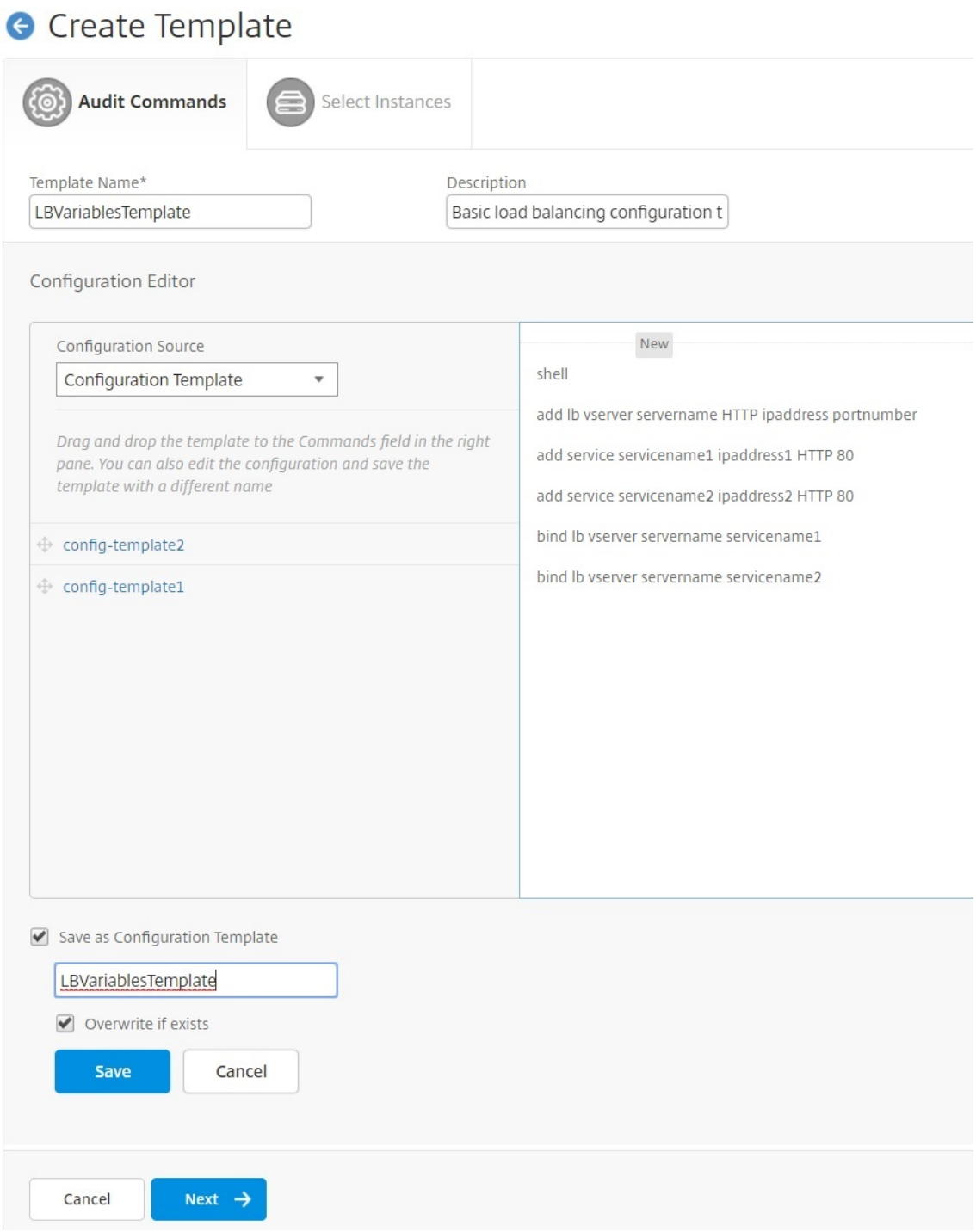
Effectuez la tâche suivante pour créer un modèle sur le module d'audit de configuration et le réutiliser dans le module tâches de configuration.

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 des commandes telles que celles de l'exemple précédent.
4. Activez la case à cocher **Enregistrer en tant que modèle de configuration** et spécifiez un nom pour votre modèle. Par exemple, vous pouvez nommer ce modèle comme « LBVariablesTemplate. « Vous pouvez choisir d'écraser d'autres modèles qui existent avec le même nom.

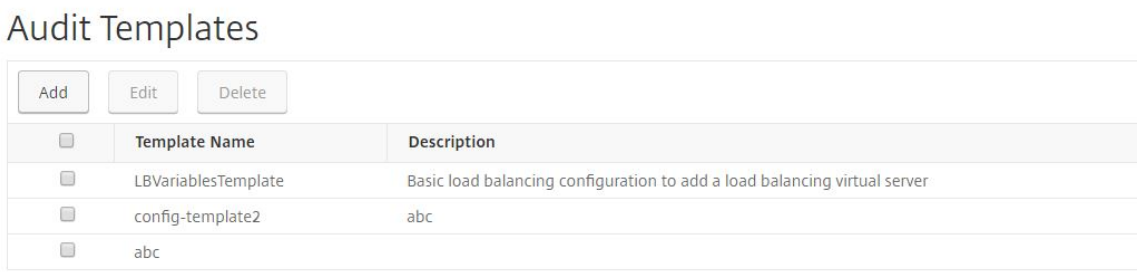
> **Remarque**
>
> Le nom du modèle d'audit peut être identique au nom du modèle de configuration.

5. Cliquez sur **Enregistrer**, puis sur **Suivant** .

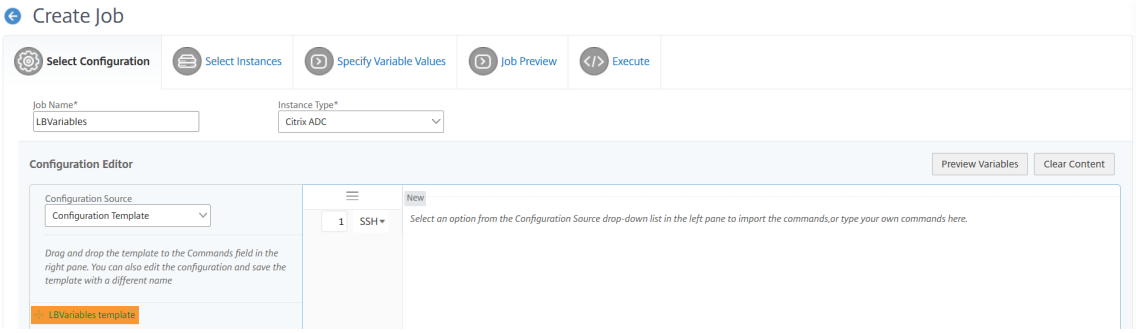


6. Cliquez sur **Suivant**.

7. **Dans l'onglet Sélectionner les instances**, sélectionnez les instances Citrix ADC sur lesquelles vous souhaitez exécuter ces commandes de configuration, puis cliquez sur **Terminer** . Le nouveau modèle est désormais visible dans la liste des modèles d'audit.

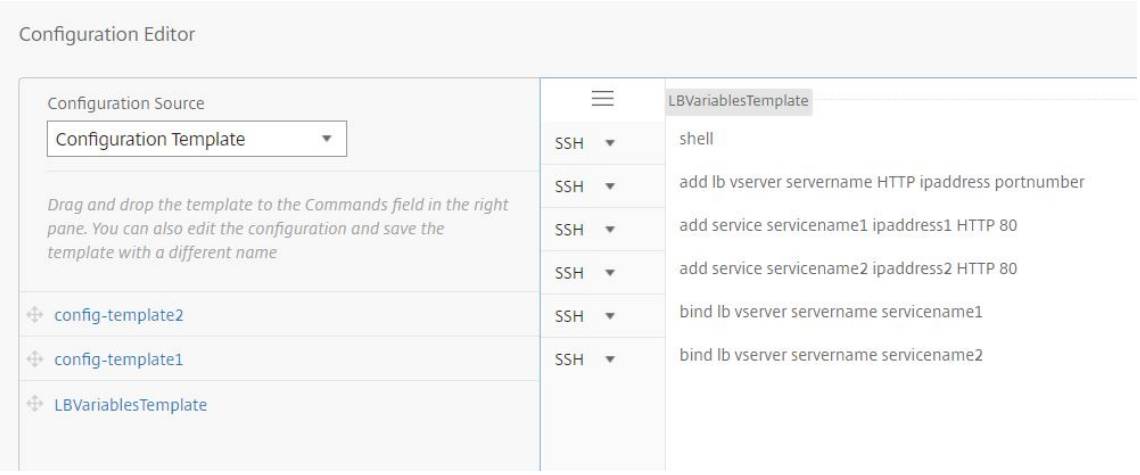


8. Lorsque vous souhaitez exécuter ces commandes de configuration, accédez à **Réseaux** > **Tâches de configuration,** puis cliquez sur **Créer une tâche**. Le modèle d'audit que vous avez créé précédemment est répertorié en tant que modèle de configuration.



Pour réutiliser le modèle d'audit dans les tâches de configuration :

1. Entrez un nom pour la tâche, sélectionnez le type d'instance, puis faites glisser le modèle vers le volet des commandes.

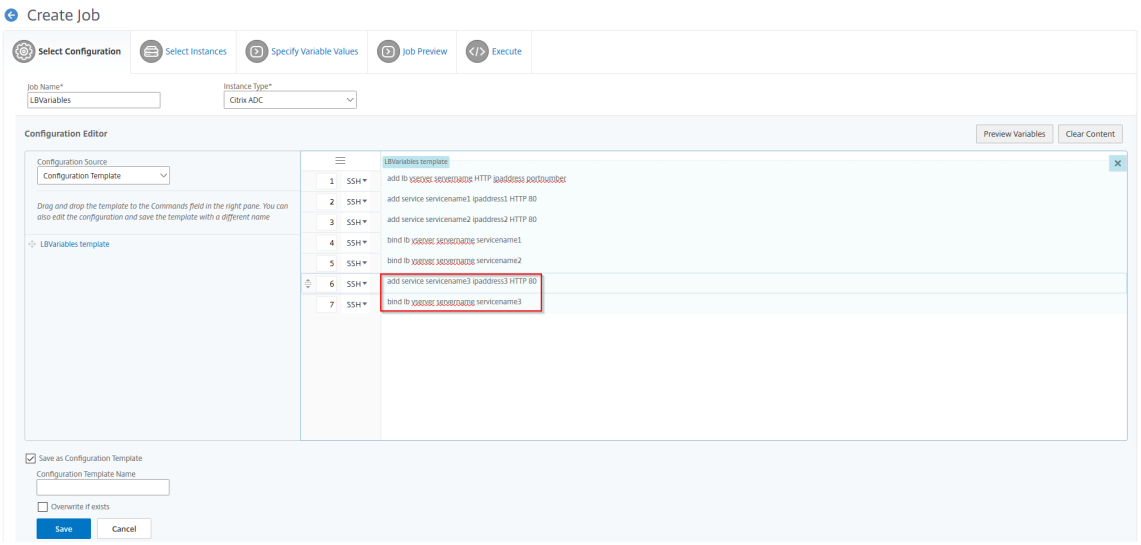


Lors de la création du travail de configuration, vous pouvez convertir les paramètres de nom

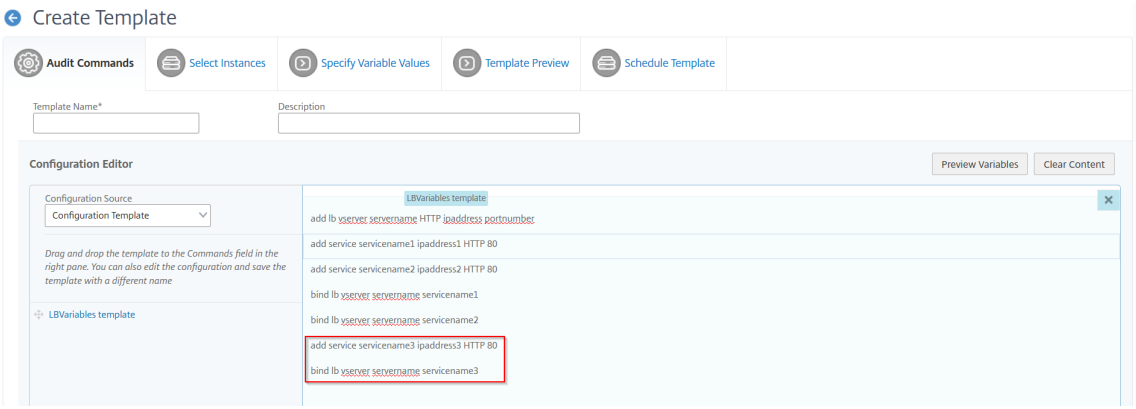
de fichier local et distant en variables. Cela vous permet d'affecter différents fichiers à ces paramètres pour le même ensemble d'instances Citrix ADC chaque fois que vous exécutez le travail.

2. Dans la commande que vous avez saisie, sélectionnez le nom de fichier que vous souhaitez 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 entrer 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 : spécifiez l'adresse IP du serveur syslog et le port.
5. Dans l'onglet **Aperçu des tâches**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances, puis cliquer sur **Suivant** .
6. Dans l'onglet **Exécuter**, cliquez sur **Terminer** pour exécuter le travail de configuration.

   Maintenant, si vous souhaitez ajouter un autre service à ce serveur d'équilibrage de charge et lier le service au serveur, vous pouvez modifier les commandes dans la page de commande et les enregistrer.



7. Accédez à **Modèles d'audit** et cliquez sur **Ajouter**.
8. Faites glisser le modèle « LBVariablesTemplate » vers le volet des commandes. Vous pouvez voir que le modèle a été mis à jour avec les nouvelles commandes.



Le modèle d'audit apparaît dans la liste Modèles d'audit et est exécuté toutes les 12 heures sur les 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

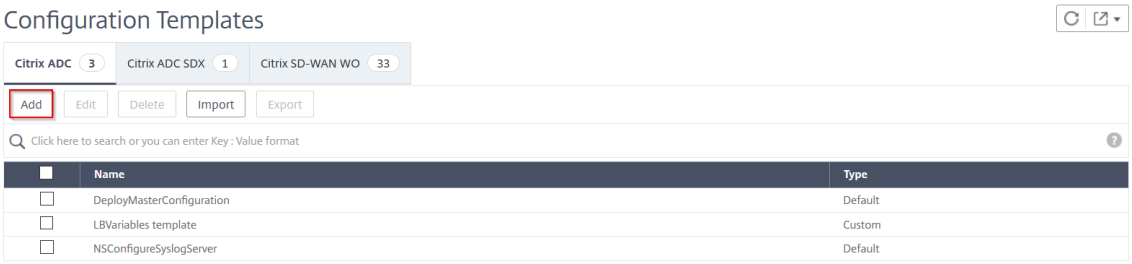
April 29, 2021

Vous pouvez exporter les modèles de configuration à partir de n'importe quelle appliance Citrix Application Delivery Management (ADM) et importer le fichier vers la même appliance Citrix ADM ou vers un autre dispositif Citrix ADM à tout moment. Les données des modèles de configuration (telles que les commandes de configuration, les définitions de variables et les paramètres) ne sont pas perdues.

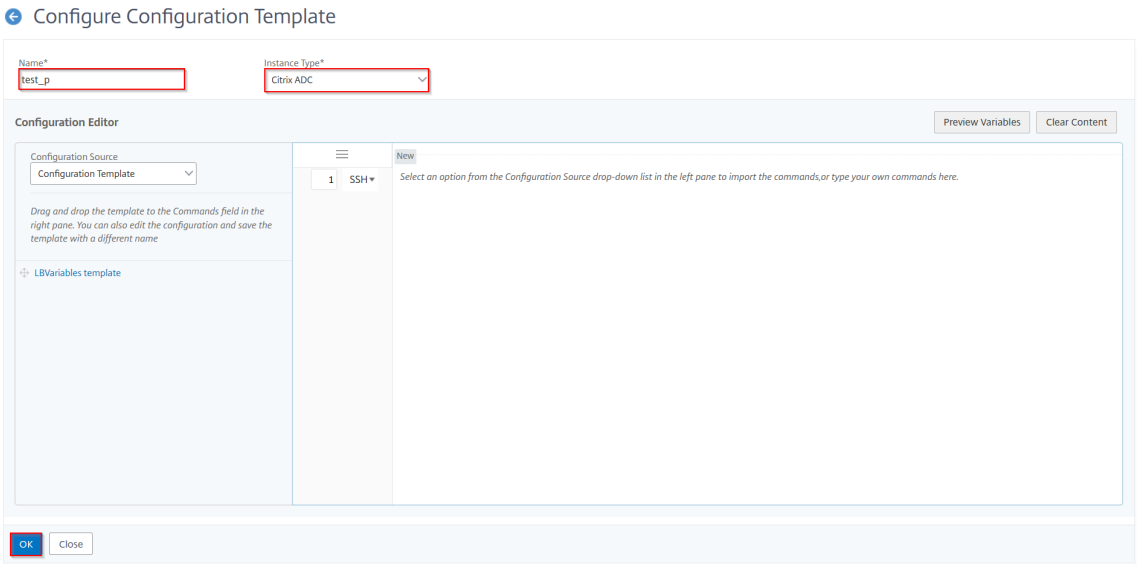
Vous pouvez exporter les modèles de configuration dans un format de fichier **.json** et les enregistrer dans le dossier local. Vous pouvez importer un modèle de configuration.**json** dans les appliances Citrix ADM que vous avez peut-être exporté à partir de la même appliance Citrix ADM ou d'une autre appliance Citrix ADM ou créés manuellement.

Pour exporter les modèles de configuration :

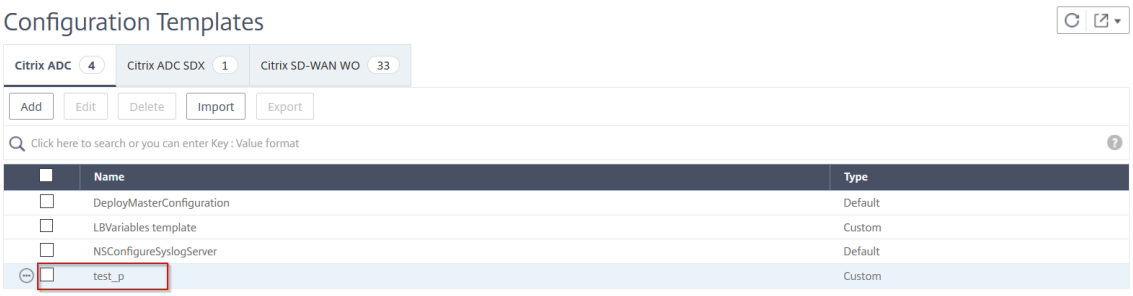
1. Accédez à **Réseaux** > **Travaux de configuration** > **Modèles de configuration** .
2. Cliquez sur **Ajouter** pour créer le modèle de configuration.



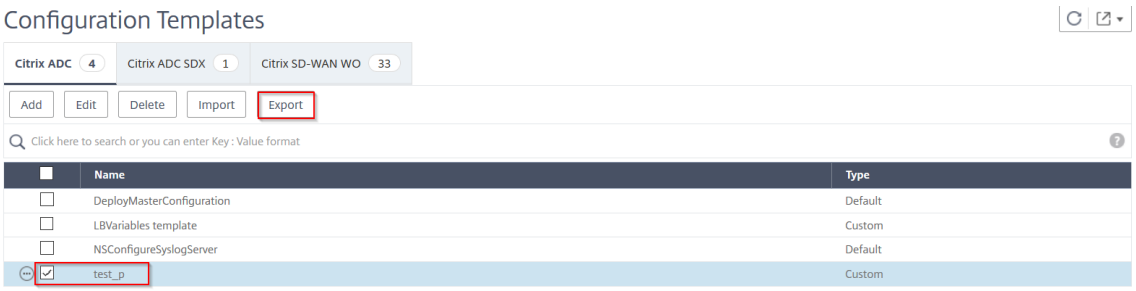
3. Dans la page **Créer un modèle de configuration**, spécifiez le nom du modèle de configuration et choisissez le type d'instance. Sous **Éditeur de**configuration, sélectionnez la source de configuration comme Modèle de configuration dans le menu déroulant. Vous pouvez faire glisser les modèles de configuration existants vers l'éditeur de configuration. Cliquez sur **OK**.



4. Accédez à **Réseaux** > **Travaux** de **configuration > Modèles** de configuration pour afficher les modèles créés dans la liste des modèles de configuration.



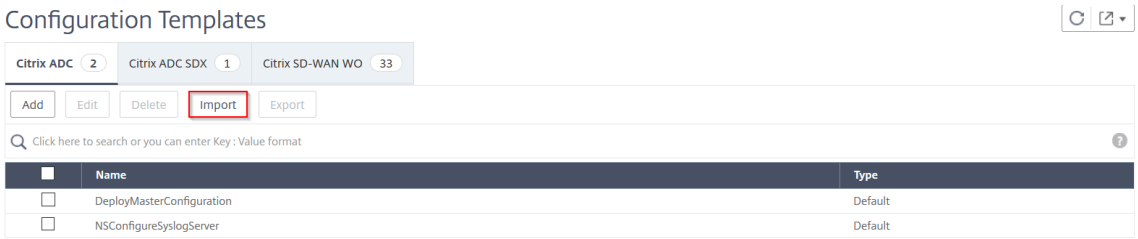
5. Sélectionnez le modèle de configuration nouvellement créé et cliquez sur le bouton **Exporter**.



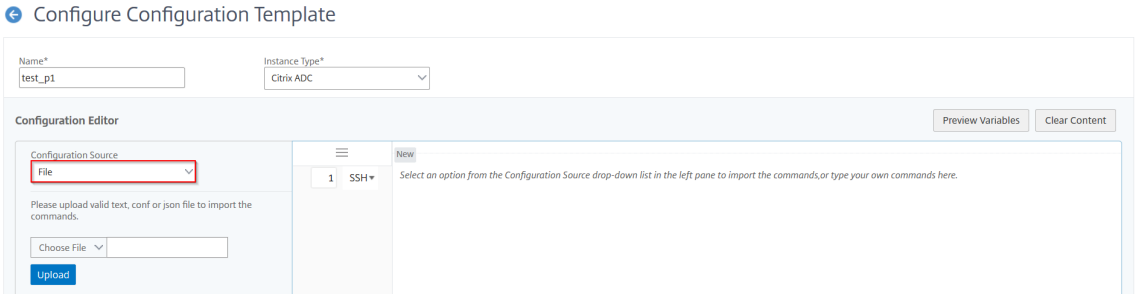
Le modèle de configuration correspondant est téléchargé sur votre système local au format **.json**.

Pour importer les modèles de configuration :

1. Accédez à **Réseaux** > **Travaux de configuration** > **Modèles de configuration**, puis 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**. Sélectionnez **Fichier** dans le menu déroulant de l' **Éditeur de configuration** et **Choisissez Fichier** (.**json**) à partir de votre système local et téléchargez le modèle de configuration. fichiers**json**.



> **Remarque**
>
> Vous ne pouvez importer les modèles de configuration que si le fichier est enregistré dans le. format**json** . Si vous importez des modèles de configuration autres que des fichiers **.json**, à partir de votre système local, une erreur s'affiche et échoue l'importation des fichiers.

Offres d'emploi Maintenance

April 29, 2021

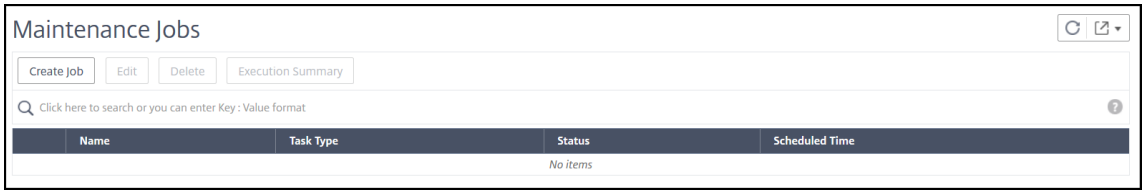
Vous pouvez créer les tâches de maintenance suivantes à l'aide de Citrix Application Delivery Management (ADM). Vous pouvez ensuite planifier les tâches de maintenance à une date et à une heure spécifiques.

- Mise à niveau des instances de Citrix ADC
- Mise à niveau des instances WAN-WO Citrix SD
- Mettre à niveau les instances Citrix ADC SDX

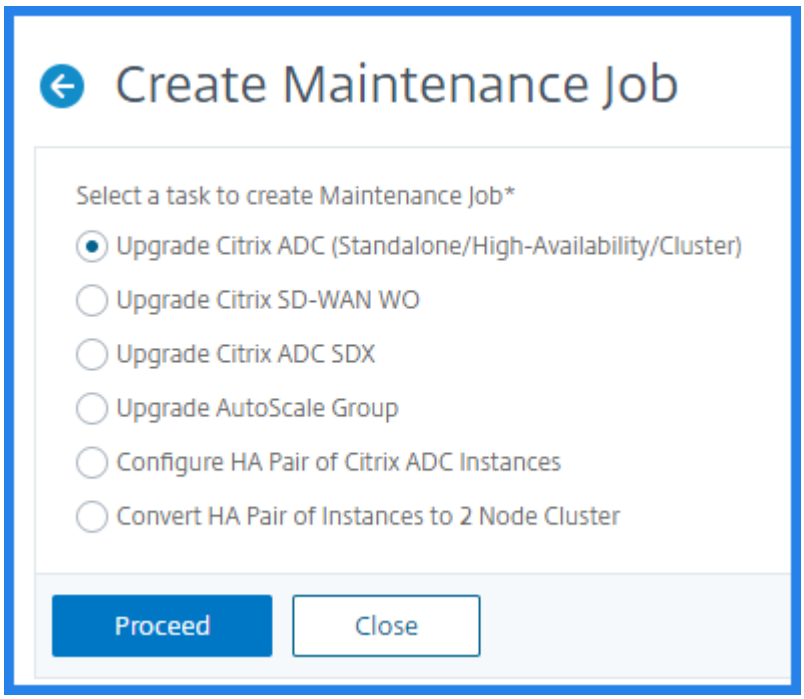
- Mettre à niveau les instances Citrix ADC dans le groupe Autoscale
- Configurer la paire HA d'instances Citrix ADC
- Convertir une paire d'instances HA en cluster

Planifier la mise à niveau des instances Citrix ADC

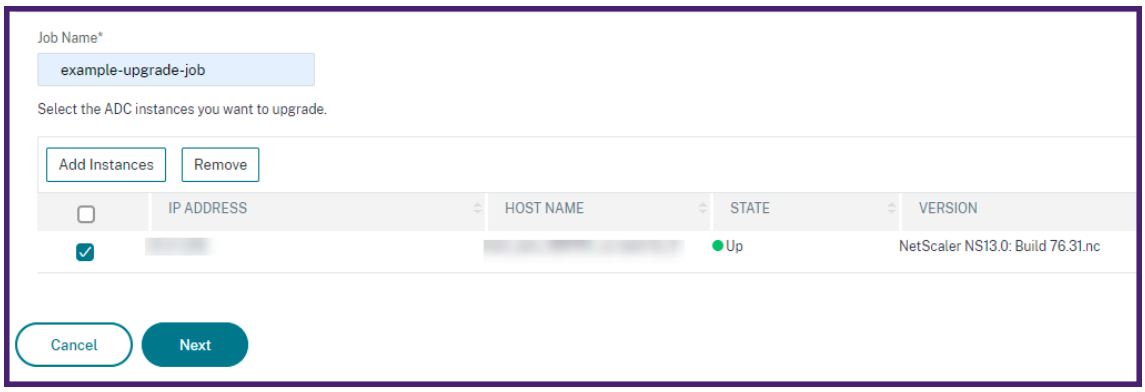
1. Dans Citrix ADM, accédez à **Réseaux** > Tâches **de configuration > Tâches** de **maintenance**. Cliquez sur le bouton **Créer un travail**.



2. Dans **Créer des tâches de maintenance**, sélectionnez **Mettre à niveau Citrix ADC (Standalone/Haute Disponibilité/Cluster)** et cliquez sur **Continuer**.



3. Dans **Sélectionner une instance**, tapez le nom de votre choix pour **Nom du travail**.
4. Cliquez sur **Ajouter des instances** pour ajouter des instances ADC à mettre à niveau.
   - Pour mettre à niveau une paire HA, spécifiez l'adresse IP d'un nœud principal ou secondaire. Toutefois, il est recommandé d'utiliser l'instance principale pour mettre à niveau la paire HA.
   - Pour mettre à niveau un cluster, spécifiez l'adresse IP du cluster.



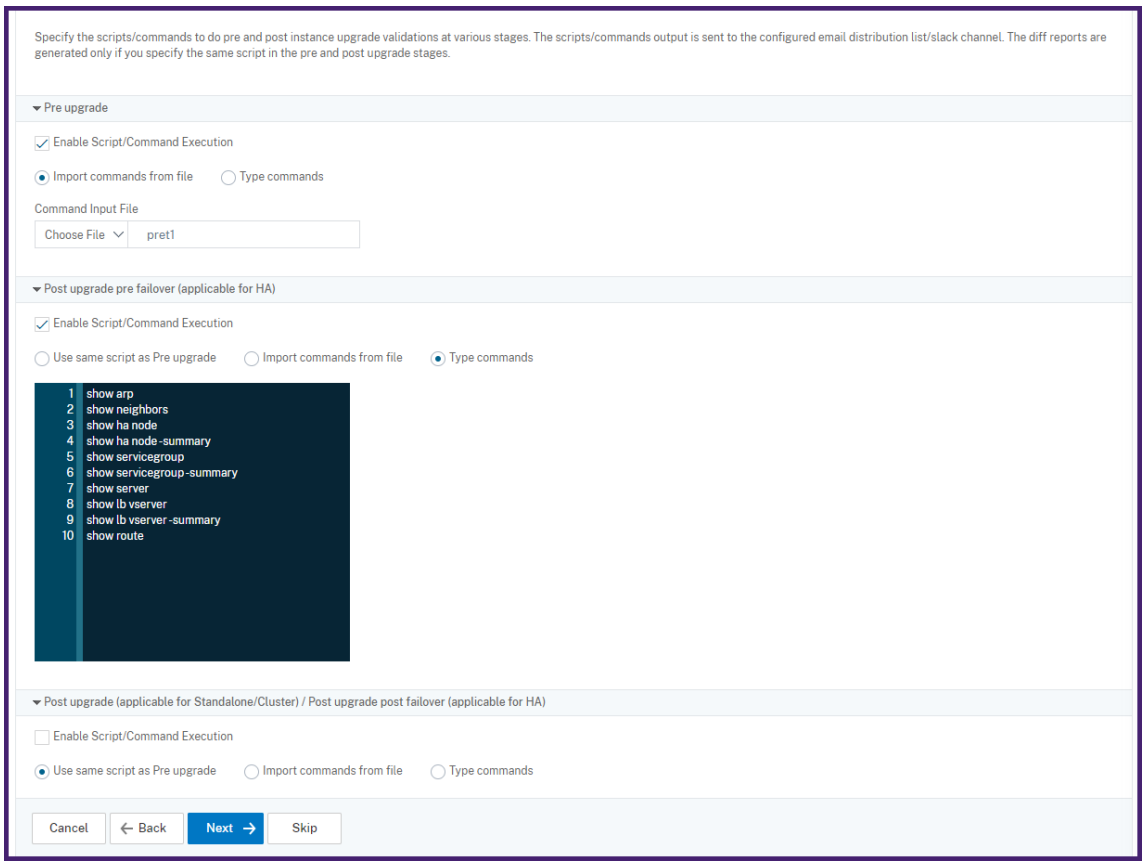
5. Cliquez sur **Suivant** pour lancer la validation de pré-mise à niveau sur les instances sélectionnées.

   L'onglet **Validation préalable à la mise à niveau** affiche les instances ayant échoué. Supprimez les instances ayant échoué et cliquez sur **Suivant**.

   > **Important**
   >
   > Si vous spécifiez l'adresse IP du cluster, l'ADM effectue la validation préalable à la mise à niveau uniquement sur l'instance spécifiée et non sur les autres nœuds du cluster.

6. Facultatif, dans **Scripts personnalisés**, spécifiez les scripts à exécuter avant et après une mise à niveau d'instance. Utilisez l'une des méthodes suivantes pour exécuter les commandes :

   - **Importer des commandes à partir d'un fichier** - Sélectionnez le fichier d'entrée de commandes à partir de votre ordinateur local.
   - **Taper les commandes** - Entrez les commandes directement sur l'interface graphique.



Vous pouvez utiliser des scripts personnalisés pour vérifier les modifications avant et après une mise à niveau d'instance. Par exemple :

- Version d'instance avant et après la mise à niveau.
- État des interfaces, des nœuds haute disponibilité, des serveurs virtuels et des services avant et après la mise à niveau.
- Les statistiques des serveurs et services virtuels.
- Les routes dynamiques.

7. Dans **Planifier la tâche**, sélectionnez l'une des options suivantes :

   - **Mise à niveau maintenant** - Le travail de mise à niveau s'exécute immédiatement.
   - **Planifier plus tard** - Sélectionnez cette option pour exécuter ce travail de mise à niveau ultérieurement. Spécifiez la **date d'exécution** et l'**heure de début** lorsque vous souhaitez mettre à niveau les instances.

     Si vous souhaitez mettre à niveau une paire ADC HA en deux étapes, sélectionnez **Effectuer une mise à niveau à deux étapes pour les nœuds dans HA**.

     Spécifiez la **date d'exécution** et l'**heure de début** lorsque vous souhaitez mettre à niveau une autre instance dans la paire HA.

8. Dans **Créer une tâche**, spécifiez les détails suivants :

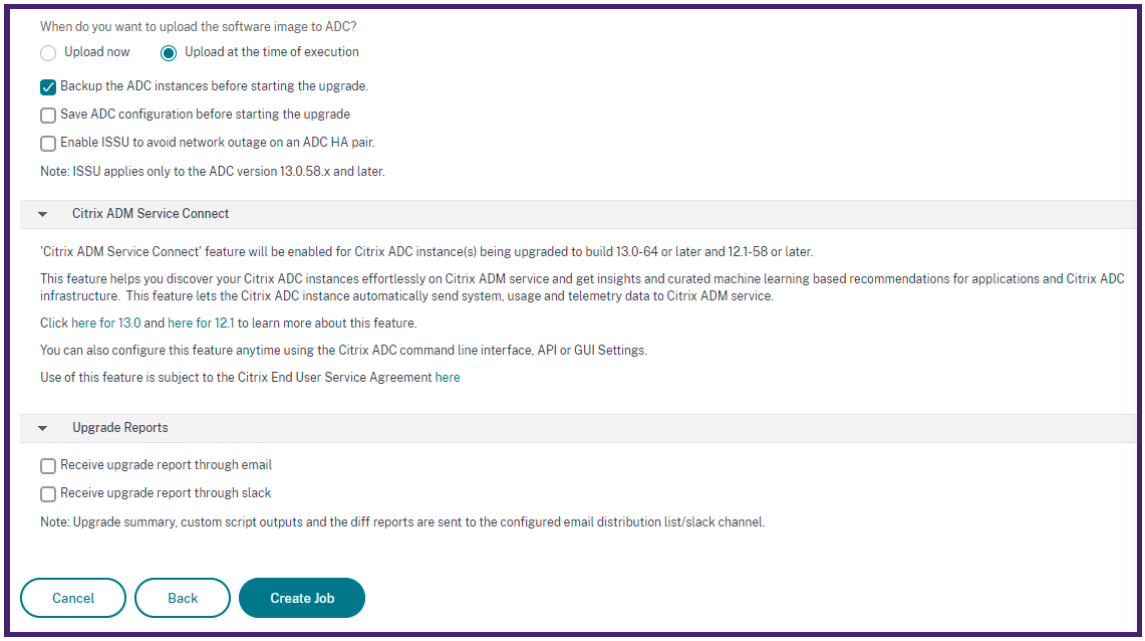
a) Sélectionnez l'une des options suivantes dans la liste **Image logicielle** :

- **Local** : sélectionnez le fichier de mise à niveau d'instance à partir de votre machine locale.
- **Appliance** : sélectionnez le fichier de mise à niveau d'instance dans un navigateur de fichiers ADM. L'interface graphique ADM affiche les fichiers d'instance présents à `/var/mps/mps_images`.

b) Spécifiez quand vous souhaitez télécharger l'image vers une instance :

- **Télécharger maintenant** - Sélectionnez cette option pour télécharger l'image immédiatement. Toutefois, le travail de mise à niveau s'exécute à l'heure planifiée.
- **Télécharger au moment de l'exécution** - Sélectionnez cette option pour télécharger l'image au moment de l'exécution de la tâche de mise à niveau.

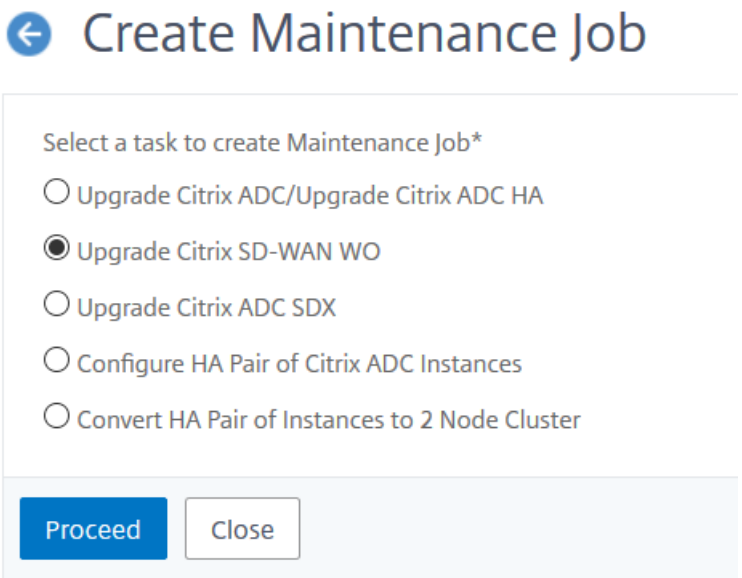
- **Nettoyer l'image logicielle à partir de Citrix ADC lors de la mise à niveau réussie** - Sélectionnez cette option pour effacer l'image téléchargée dans l'instance ADC après la mise à niveau de l'instance.
- **Sauvegardez les instances ADC avant de commencer la mise à niveau.** - Crée une sauvegarde des instances ADC sélectionnées.
- **Permet à ISSUE d'éviter une panne réseau sur une paire ADC HA** - ISSU garantit la mise à niveau zéro temps d'arrêt sur une paire ADC haute disponibilité. Cette option fournit une fonctionnalité de migration qui respecte les connexions existantes lors de la mise à niveau. Ainsi, vous pouvez mettre à niveau une paire ADC HA sans temps d'arrêt. Spécifiez le délai de migration ISSU en minutes.
- **Recevoir le rapport d'exécution par e-mail** - Envoie le rapport d'exécution par e-mail. Pour ajouter une liste de distribution d'e-mails, reportez-vous à la section Créer une liste de distribution d'e-mails.
- **Recevoir le rapport d'exécution via la marge** - Envoie le rapport d'exécution en marge. Pour ajouter un profil Slack, reportez-vous à la section Créer un profil Slack.



9. Cliquez sur **Créer une tâche**.

Planifier la mise à niveau des instances WO Citrix SD-WAN

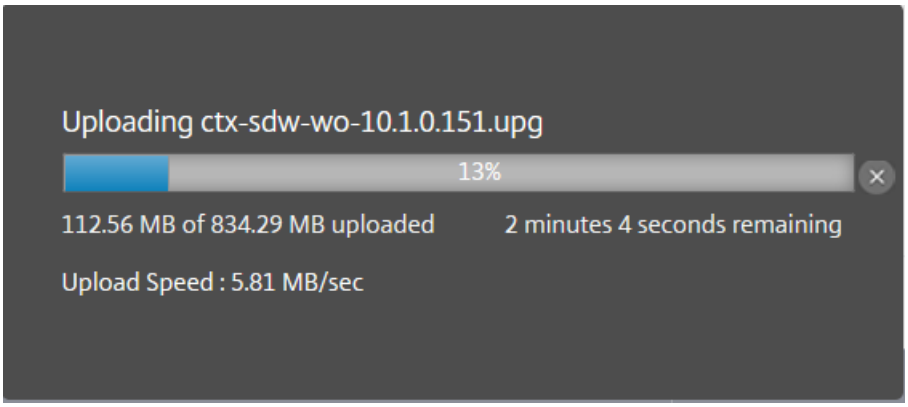
1. Dans Citrix ADM, accédez à **Réseaux** > Tâches **de configuration > Tâches** de **maintenance**. Cliquez sur le bouton **Créer un travail**.
2. Sélectionnez **Mettre à niveau Citrix SD-WAN WO** et cliquez sur **Continuer**.



3. Sur la page **Mettre à niveau Citrix SD-WAN WO**, dans l'onglet **Sélection d'instance** :
   a) Ajoutez un **nom de tâche**.

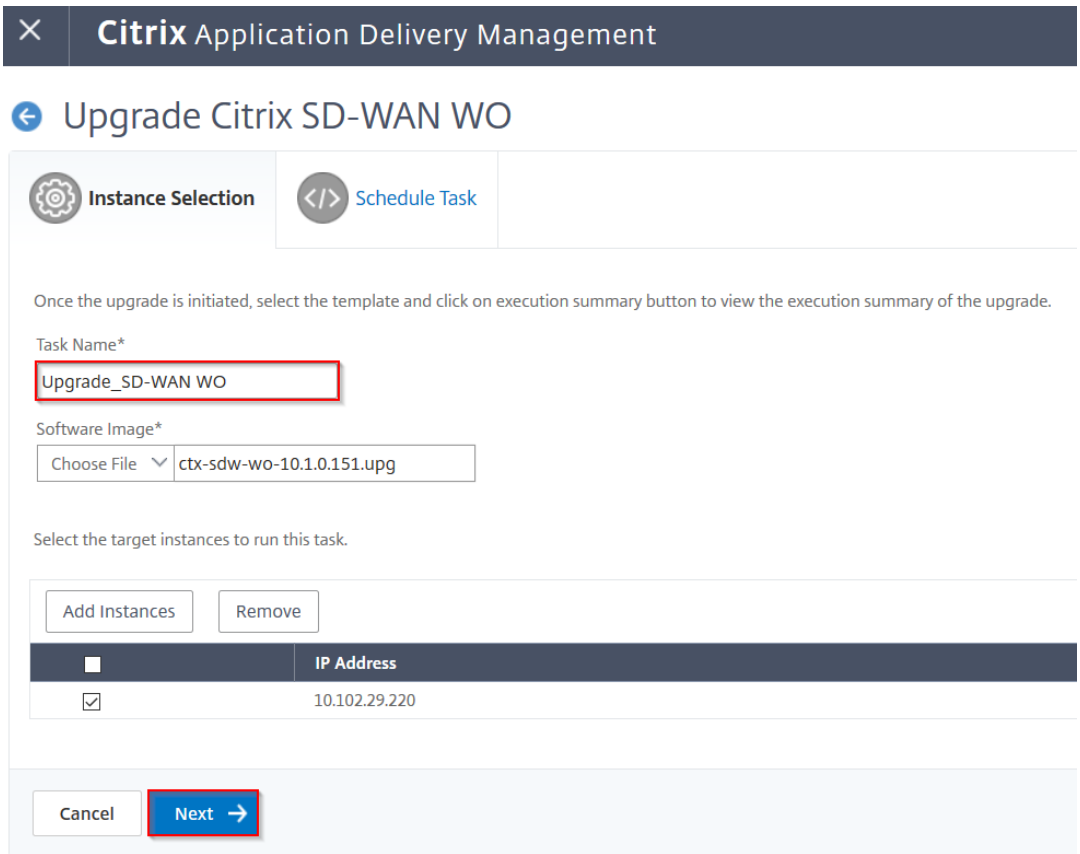
b) Cliquez sur Dans le menu déroulant Image logicielle, sélectionnez Local (votre machine locale) ou Appliance (le fichier de build doit être présent sur l'appliance virtuelle Citrix ADM).

Le processus de chargement commence.



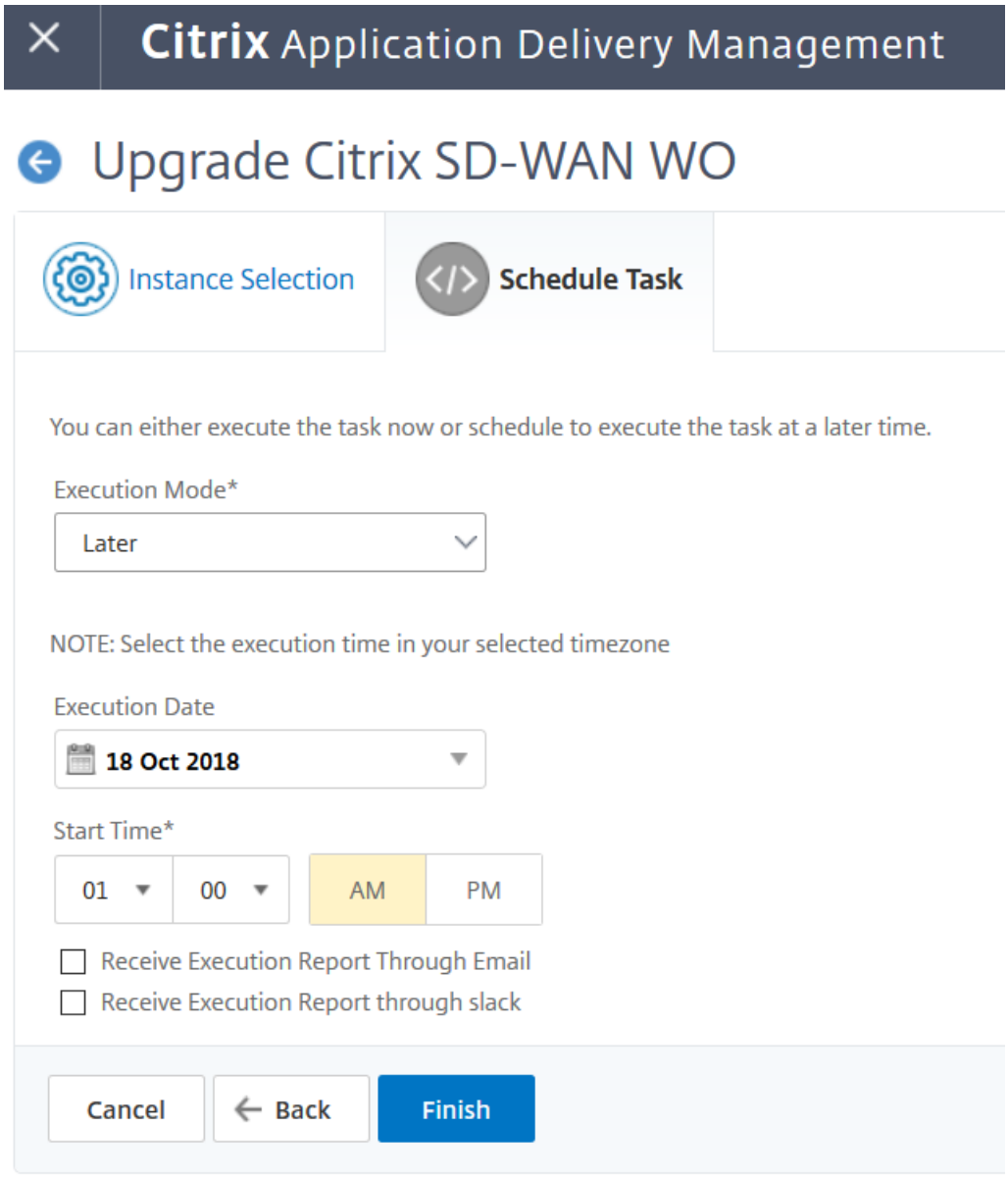
c) Cliquez sur **Ajouter des instances** pour ajouter les instances WO Citrix SD-WAN sur lesquelles vous souhaitez exécuter le processus de mise à niveau.

d) Cliquez sur **Suivant**.



4. Sous l'onglet **Planifier la tâche**, sélectionnez **Maintenant** dans la liste **Mode d'exécution** pour mettre à niveau une instance Citrix SD-WAN WO maintenant, puis cliquez sur **Terminer**.

5. Pour mettre à niveau une instance Citrix ADC SD-WAN WO ultérieurement, sélectionnez **Plus tard** dans la liste **Mode d'exécution**. Vous pouvez ensuite choisir la date d'exécution et l'heure de début pour la mise à niveau de l'instance SD-WAN de Citrix ADC, puis cliquez sur **Terminer**

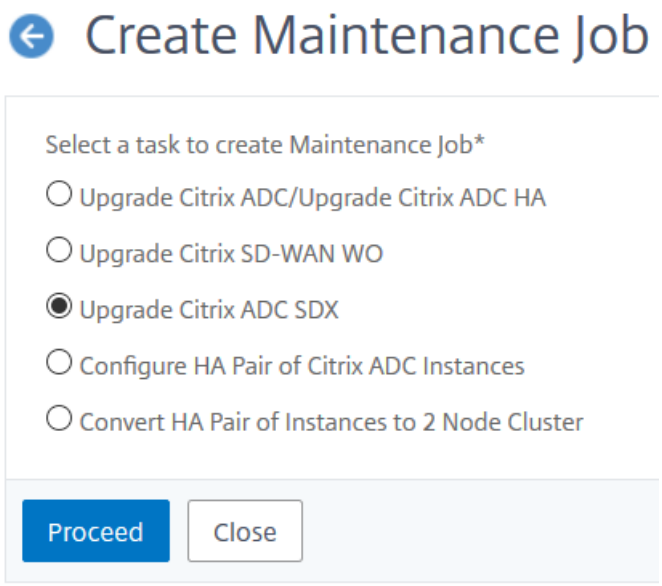


6. Vous pouvez également activer les notifications par e-mail et de marge pour recevoir le rapport d'exécution de la mise à niveau d'une instance Citrix SD-WAN WO. Cliquez sur la la case à cocher **Recevoir le rapport d'exécution par courrier électronique** et la case à cocher **Recevoir le rapport d'exécution via Slack** pour activer les notifications.

   Pour plus d'informations sur la configuration de la liste de distribution de courrier électronique et du canal de slack, reportez-vous à l'**étape 8** de la section Planifier la mise à niveau des instances Citrix ADC

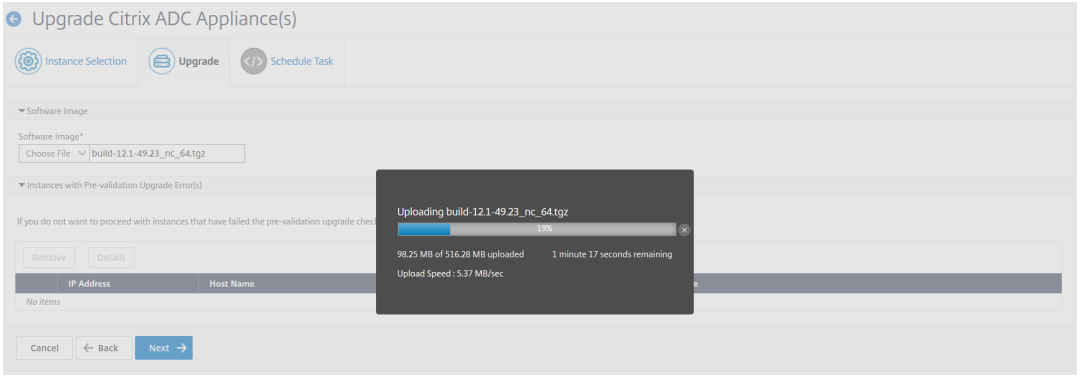
Planifier la mise à niveau des instances Citrix ADC SDX

1. Dans Citrix ADM, accédez à **Réseaux > Travaux de configuration > Travaux de maintenance**. Cliquez sur le bouton **Créer un travail**.
2. Sélectionnez **Mettre à niveau Citrix ADC SDX** et cliquez sur **Continuer**.

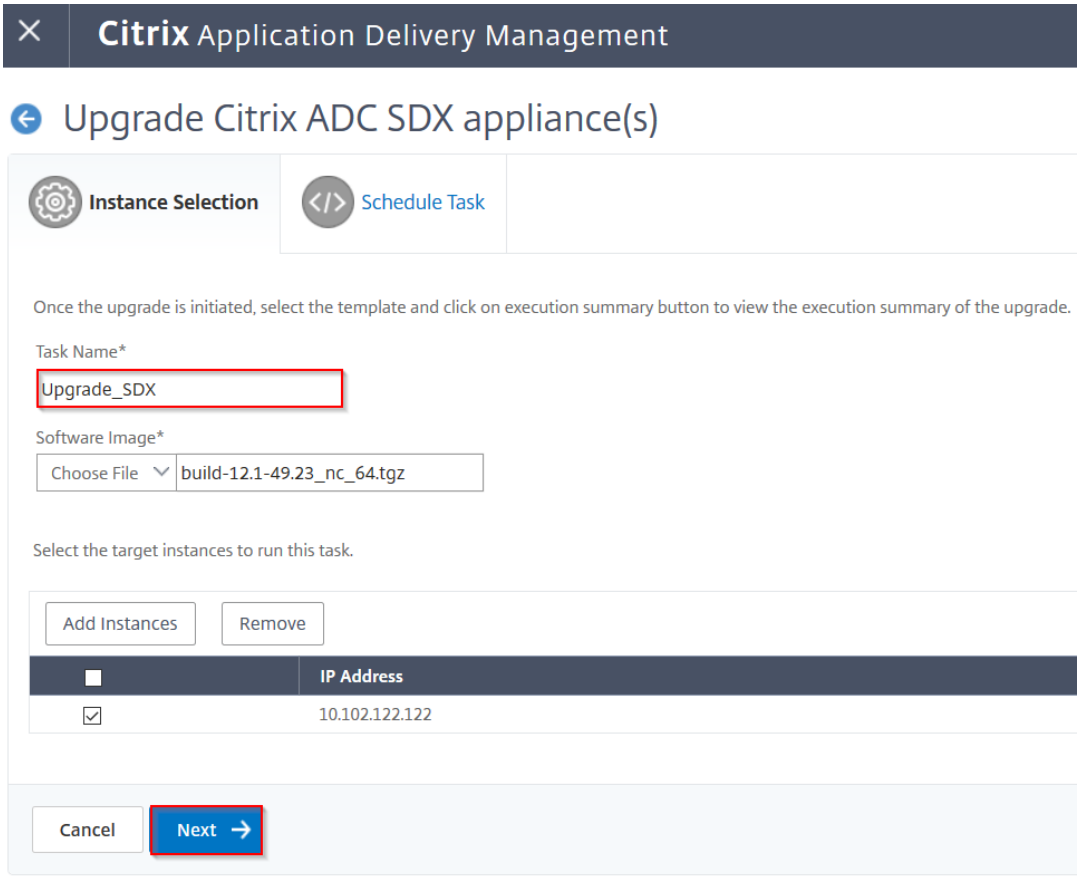


3. Sur la page **Mettre à niveau Citrix ADC SDX**, dans l'onglet **Sélection d'instance** :
   a) Ajoutez un **nom de tâche**.
   b) Dans le menu déroulant Image logicielle, sélectionnez Local (votre machine locale) ou Appliance (le fichier de build doit être présent sur l'appliance virtuelle Citrix ADM).

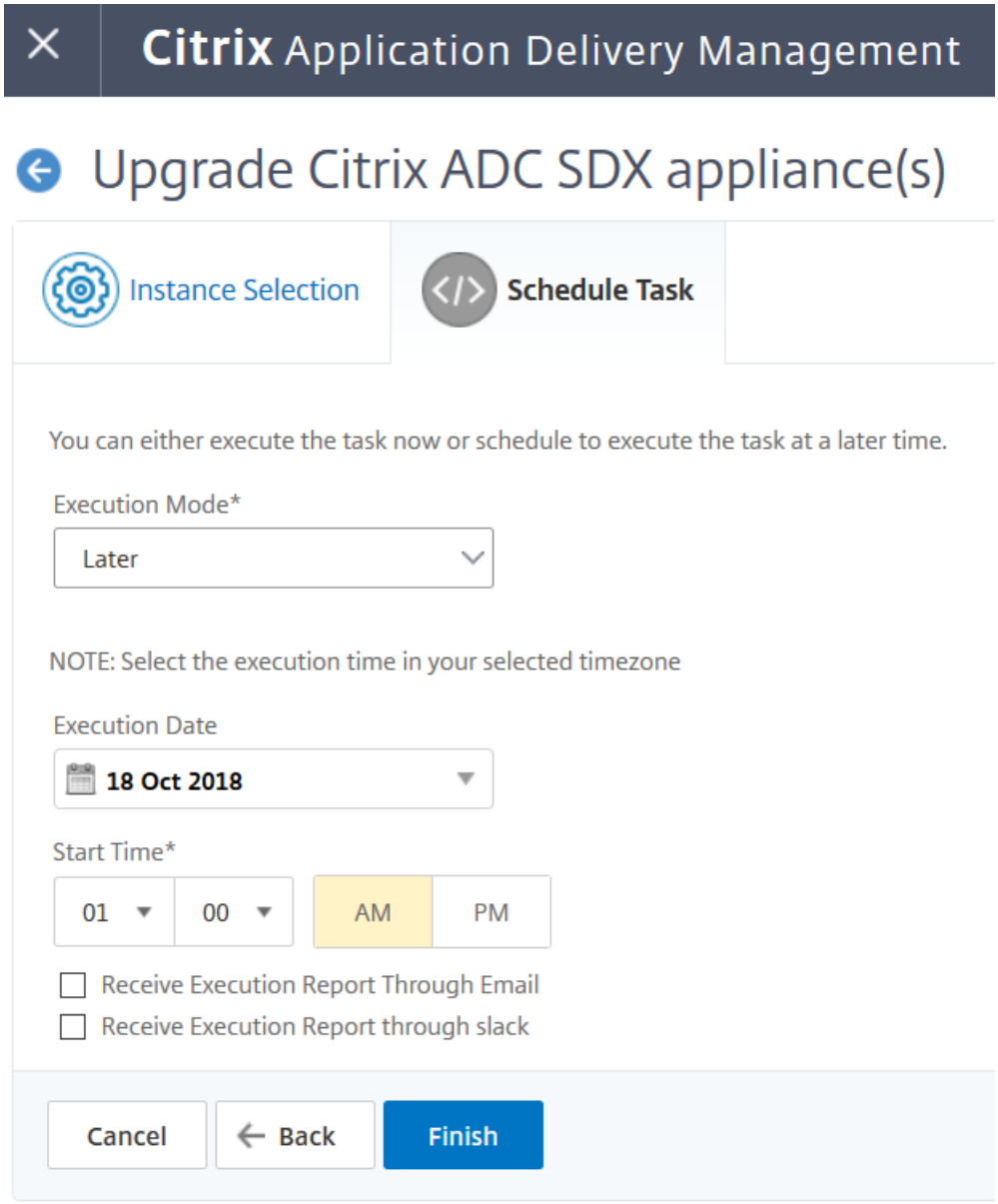
      Le processus de chargement commence.



   c) Ajoutez les instances Citrix ADC SDX sur lesquelles vous souhaitez exécuter le processus de mise à niveau.
   d) Cliquez sur **Suivant**.



4. Sous l'onglet **Planifier la tâche**, sélectionnez **Maintenant** dans la liste **Mode d'exécution** pour mettre à niveau une instance Citrix SD-WAN WO maintenant, puis cliquez sur **Terminer**.
5. Pour mettre à niveau une instance Citrix ADC SDX ultérieurement, sélectionnez **Plus tard** dans la liste **Mode d'exécution**. Vous pouvez ensuite choisir la date d'exécution et l'heure de début pour la mise à niveau de l'instance SD-WAN de Citrix ADC, puis cliquez sur **Terminer**



6. Vous pouvez également activer les notifications par e-mail et de marge pour recevoir le rapport d'exécution de l'instance Citrix ADC SDX mise à niveau. Cliquez sur la la case à cocher **Recevoir le rapport d'exécution par courrier électronique** et la case à cocher **Recevoir le rapport d'exécution via Slack** pour activer les notifications.

   Pour plus d'informations sur la configuration de la liste de distribution de courrier électronique et du canal de slack, reportez-vous à l'**étape 8** de la section Planifier la mise à niveau des instances Citrix ADC

Planifier la mise à niveau du groupe Autoscale

Procédez comme suit pour mettre à niveau toutes les instances des services cloud qui font partie du groupe Autoscale :

1. Dans Citrix ADM, accédez à **Réseaux > Travaux de configuration > Travaux de maintenance**. Cliquez sur le bouton **Créer un travail**.
2. Sélectionnez **Mettre à niveau le groupe Autoscale** et cliquez sur **Continuer**.
3. Dans l'onglet **Paramètres de mise à niveau** :
   a) Sélectionnez le **groupe de mise à niveau automatique** que vous souhaitez mettre à niveau.
   b) Dans **Image**, sélectionnez la version Citrix ADC. Cette image est la version existante des instances Citrix ADC dans le groupe Autoscale.
   c) Dans **Citrix ADC Image**, parcourez le fichier de version Citrix ADC vers lequel vous souhaitez mettre à niveau.

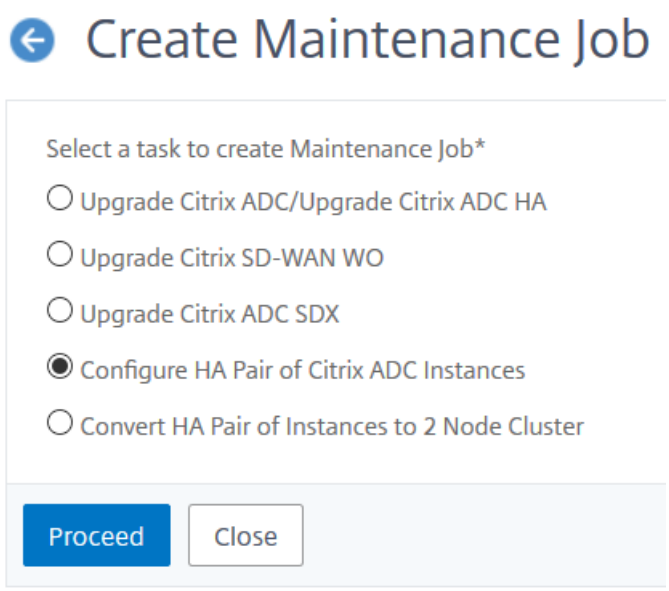
      Si vous cochez **Mise à niveau gracieuse**, la tâche de mise à niveau attend l'expiration de la période de connexion de drain spécifiée.
   d) Cliquez sur **Suivant**.
4. Dans l'onglet **Planifier la tâche** :
   a) Sélectionnez l'une des options suivantes dans la liste Mode d'exécution :
      - **Maintenant :**Pour démarrer les instances de Citrix ADC, mettez à niveau immédiatement.
      - **Plus tard :** Pour démarrer la mise à niveau des instances de Citrix ADC ultérieurement.
   b) Si vous sélectionnez l'option **Plus tard**, sélectionnez la date d'exécution et l'heure de début lorsque vous souhaitez démarrer la tâche de mise à niveau.

   Vous pouvez également activer les notifications par e-mail et les notifications de marge pour recevoir le rapport d'exécution du groupe Mise à niveau Autoscale. Cliquez sur la la case à cocher **Recevoir le rapport d'exécution par courrier électronique** et la case à cocher **Recevoir le rapport d'exécution via Slack** pour activer les notifications.
5. Cliquez sur **Terminer**.

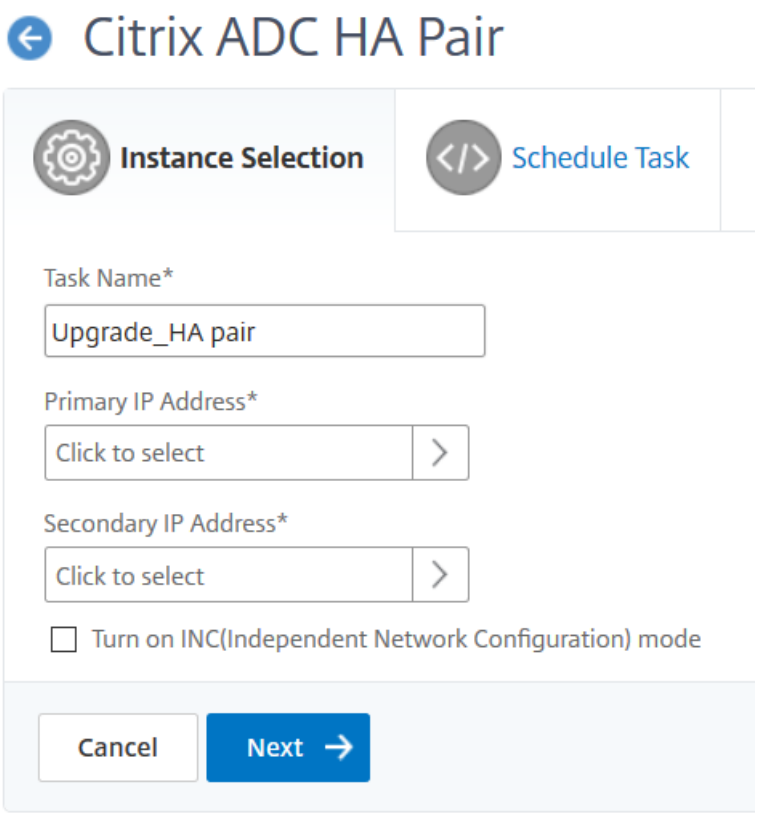
Planification de la configuration de la paire HA d'instances Citrix ADC

1. Dans Citrix ADM, accédez à **Réseaux > Travaux de configuration > Travaux de maintenance**. Cliquez sur le bouton **Créer un travail**.

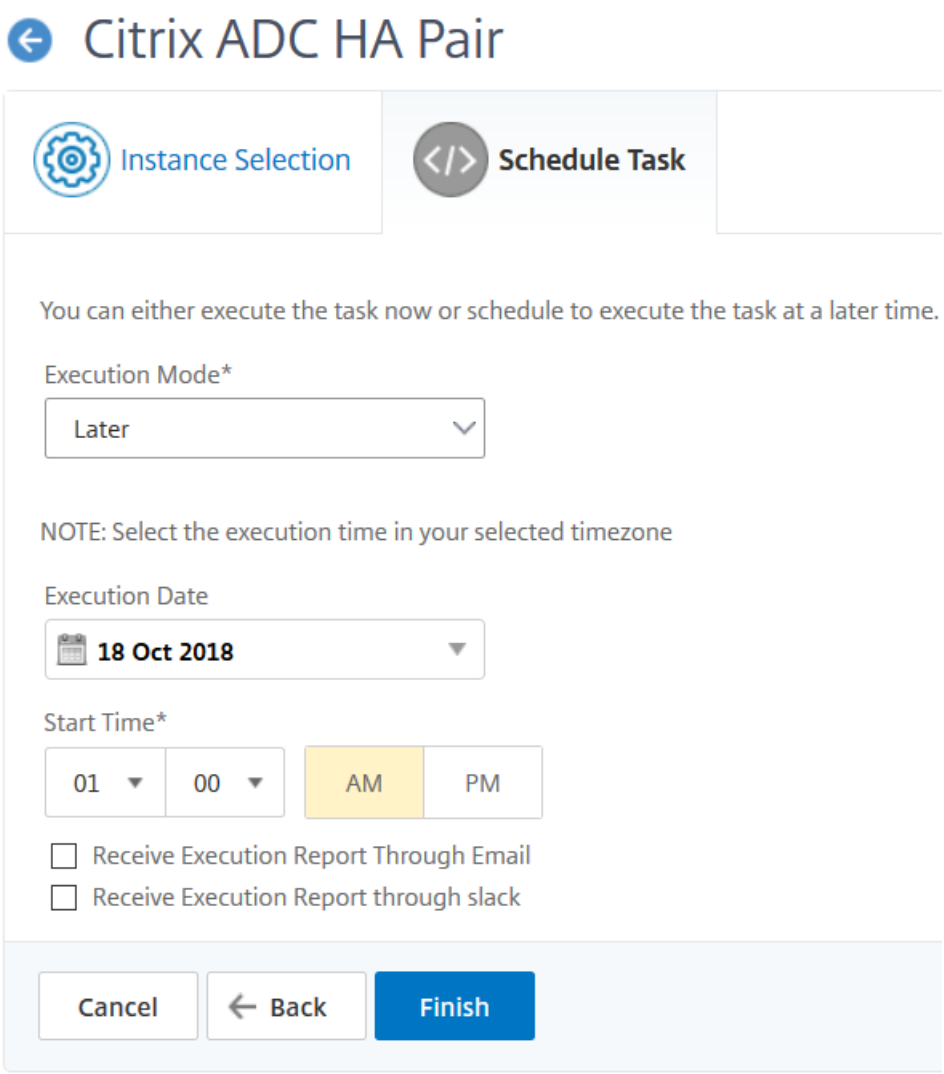
2. Sélectionnez **Configurer la paire HA d'instances Citrix ADC** et cliquez sur **Continuer**.



3. Sur la page **Citrix ADC HA Pair**, dans l'onglet **Sélection d'instance** :
   a) Ajoutez un **nom de tâche**.
   b) Entrez l'adresse IP principale.
   c) Entrez l'adresse IP secondaire.
   d) Cliquez sur **Suivant**.
   e) Cliquez pour **activer le mode INC (Independent Network Configuration)** si vous avez les instances de paires HA dans deux sous-réseaux.



4. Sous l'onglet **Planifier la tâche**, sélectionnez **Maintenant** dans la liste **Mode d'exécution** pour mettre à niveau une instance Citrix SD-WAN WO maintenant, puis cliquez sur **Terminer**.
5. Pour mettre à niveau une paire Citrix ADC HA ultérieurement, sélectionnez **Plus tard** dans la liste **Mode d'exécution**. Vous pouvez ensuite choisir la date d'exécution et l'heure de début pour la mise à niveau de l'instance SD-WAN de Citrix ADC, puis cliquez sur **Terminer**.

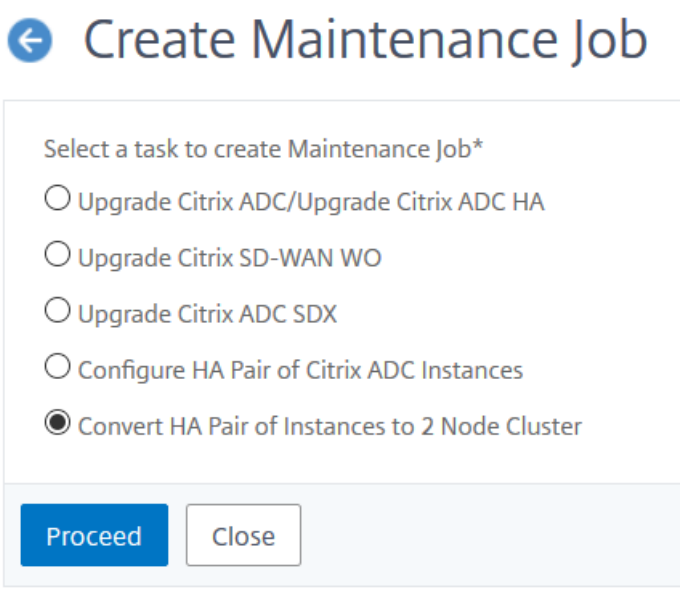


6. Vous pouvez également activer les notifications par e-mail et les notifications de marge pour recevoir le rapport d'exécution de la création de la paire ADC HA. Cliquez sur la la case à cocher **Recevoir le rapport d'exécution par courrier électronique** et la case à cocher **Recevoir le rapport d'exécution via Slack** pour activer les notifications.

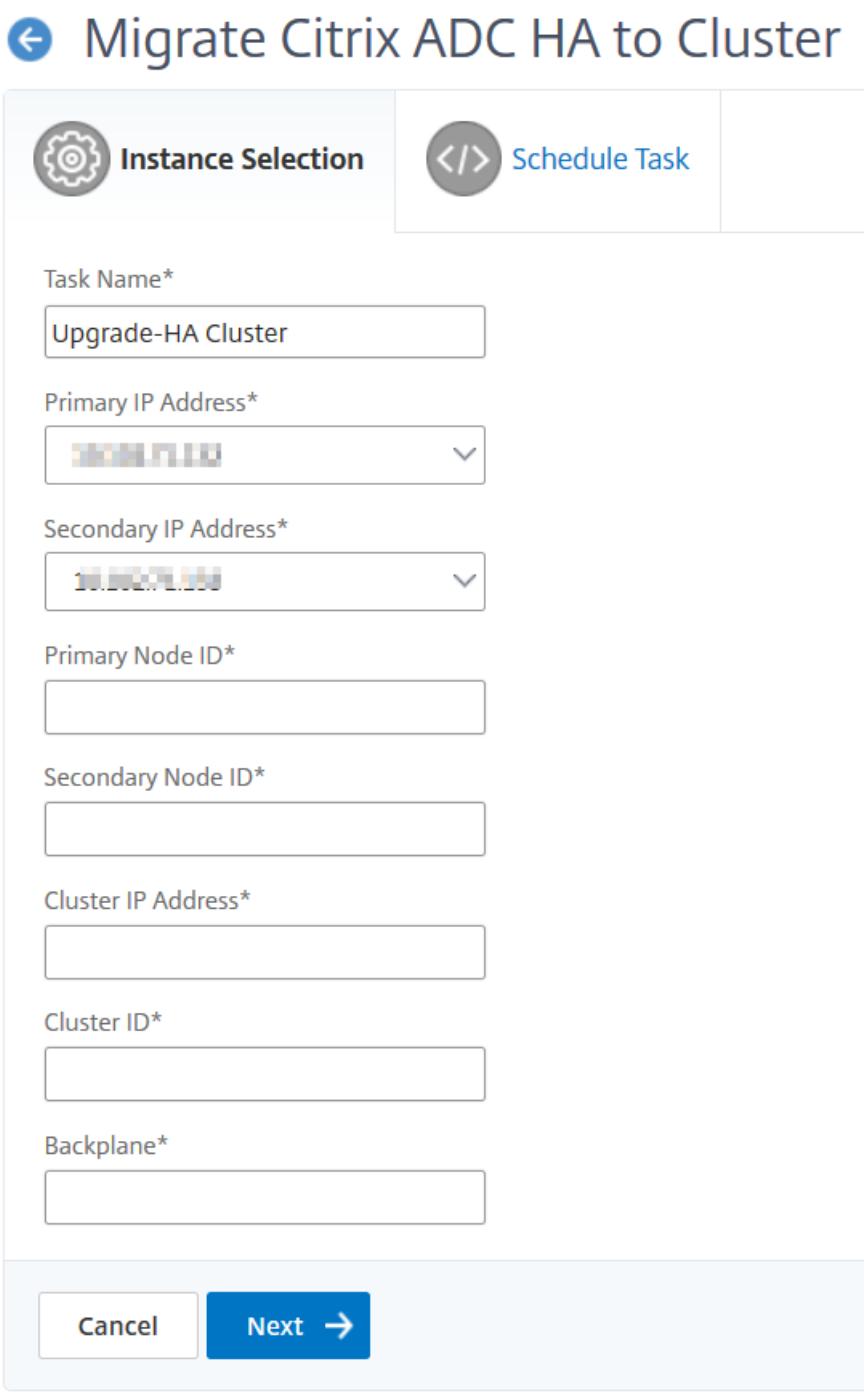
   Pour plus d'informations sur la configuration de la liste de distribution de courrier électronique et du canal de slack, reportez-vous à l'**étape 8** de la section Planifier la mise à niveau des instances Citrix ADC

Planifier la conversion d'une paire d'instances HA en cluster

1. Dans Citrix ADM, accédez à **Réseaux > Travaux de configuration > Travaux de maintenance**. Cliquez sur le bouton **Créer un travail**.
2. Sélectionnez **Convertir la paire d'instances HA en cluster à 2 nœuds** et cliquez sur **Continuer**.



3. Dans la page **Migrer NetScaler HA vers le cluster**, dans l'onglet **Sélection d'instance**, ajoutez un **nom de tâche** . Spécifiez l'adresse IP principale, l'adresse IP secondaire, l'ID du nœud principal, l'ID du nœud secondaire, l'adresse IP du cluster, l'ID du cluster et le fond de panier, puis cliquez sur **Suivant**.



4. Sous l'onglet **Planifier la tâche**, sélectionnez **Maintenant** dans la liste **Mode d'exécution** pour mettre à niveau une instance Citrix SD-WAN WO maintenant, puis cliquez sur **Terminer**.
5. Pour effectuer une mise à niveau ultérieure, sélectionnez **Plus tard** dans la liste **Mode d'exécution**. Vous pouvez ensuite choisir la **date d'exécution** et l' **heure de début** pour la mise à niveau de l'instance Citrix ADC SD-WAN WO, puis cliquer sur **Terminer**.
6. Vous pouvez également activer les notifications par e-mail et de marge pour recevoir le rapport

d'exécution de la mise à niveau d'une instance Citrix ADC SDX. Cliquez sur la la case à cocher **Recevoir le rapport d'exécution par courrier électronique** et la case à cocher **Recevoir le rapport d'exécution via Slack** pour activer les notifications.

Pour plus d'informations sur la configuration de la liste de distribution de courrier électronique et du canal de slack, reportez-vous à l'**étape 8** de la section Planifier la mise à niveau des instances Citrix ADC

Audit de configuration

April 29, 2021

Ce document comprend :

- Création de modèles d'audit
- Affichage des rapports d'audit
- Audit des modifications de configuration entre les instances
- Obtenir des conseils de configuration sur la configuration du réseau
- Comment interroger l'audit de configuration des instances Citrix ADM
- Générer un diff d'audit de configuration pour les interruptions SNMP ConfigChange

Créer des modèles d'audit

April 29, 2021

Vous voulez vous assurer que certaines configurations sont exécutées sur des instances spécifiques pour des performances optimales de votre réseau. Vous souhaitez également surveiller les modifications de configuration sur les instances Citrix 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 (ADM) compare ces instances avec le modèle d'audit et signale en cas d'inadéquation 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

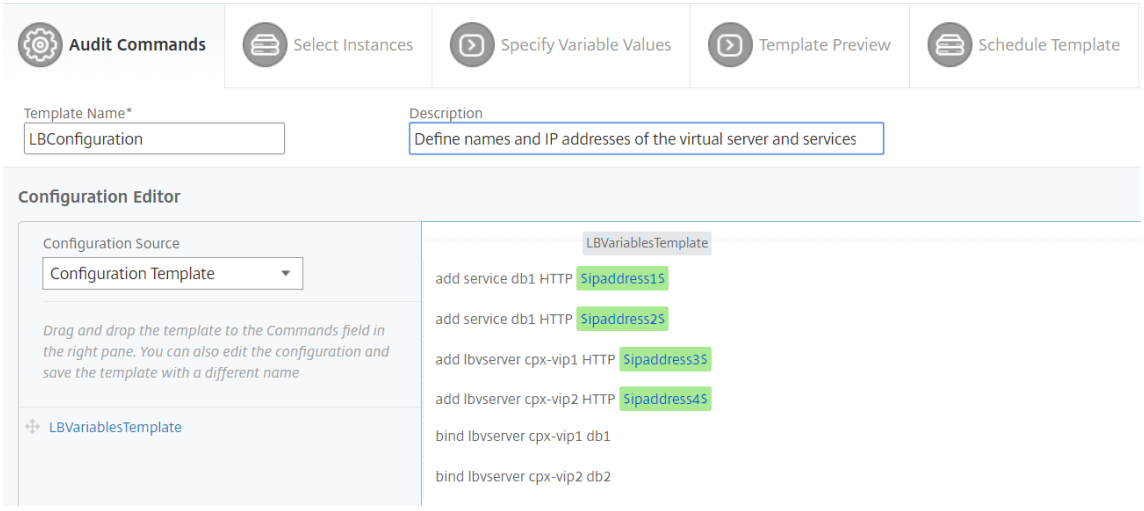
- Planification de l'heure à laquelle le modèle doit être exécuté
- Définition de la fréquence à laquelle Citrix ADM doit exécuter le modèle. Vous pouvez exécuter le modèle tous les jours, un jour spécifique d'une semaine ou à une date spécifique d'un mois.

En outre, vous avez la possibilité d'envoyer le rapport de diff généré par Citrix ADM aux adresses e-mail spécifiées que vous pouvez configurer. Grâce à cette option, votre utilisateur peut recevoir le rapport sous forme de pièce jointe et il n'est pas nécessaire que l'utilisateur se connecte à Citrix ADM pour exporter les rapports manuellement.

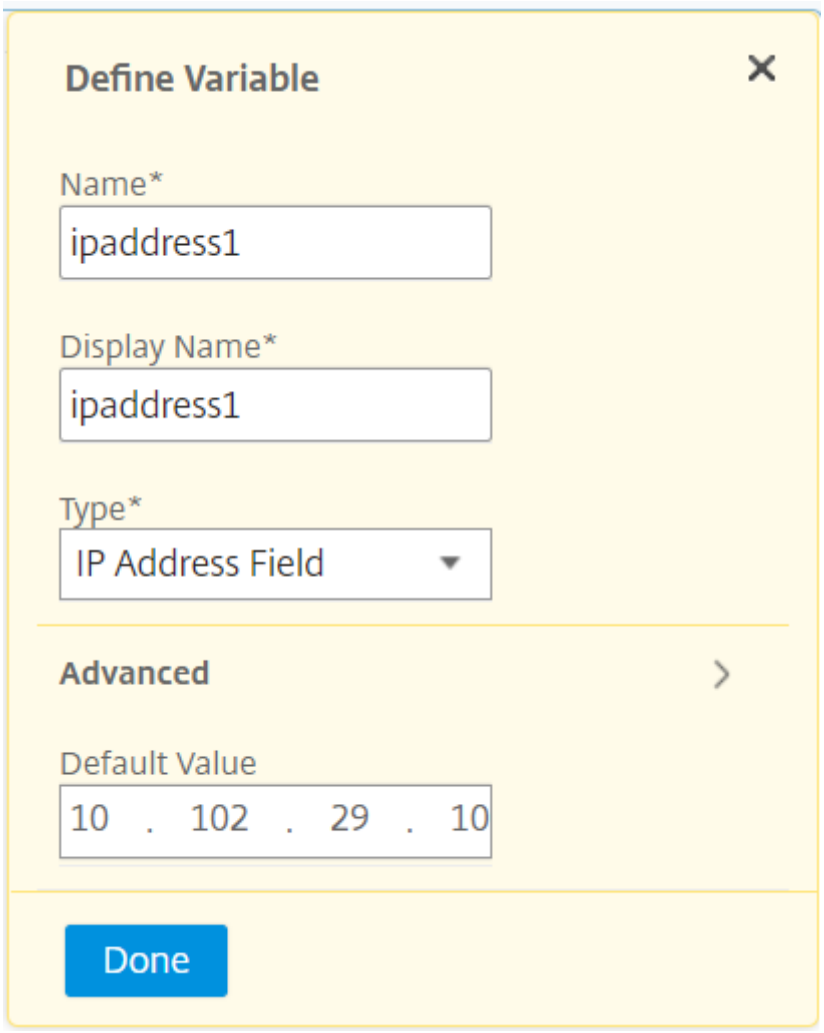
> **Remarque**
> L'option **Renommer** est désactivée pour les modèles de configuration par défaut. Toutefois, vous pouvez renommer des modèles de configuration personnalisés.

Pour créer des modèles d'audit :

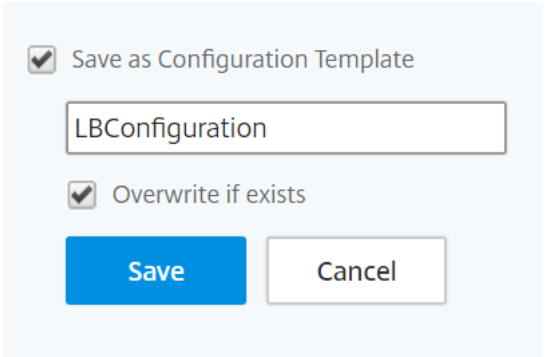
1. Accédez à **Réseaux** > **Audit de configuration** > **Modèles d'audit**, puis cliquez sur **Ajouter**.
2. Dans la page **Créer un modèle** et dans l'onglet **Commandes d'audit**, spécifiez le nom du modèle et sa description.
3. Dans la page **Éditeur de configuration**, tapez vos commandes et enregistrez les commandes en tant que modèle de configuration. Vous pouvez également faire glisser un modèle existant du volet gauche vers l'éditeur.
4. Sélectionnez les valeurs à convertir en variable, puis cliquez sur **Convertir en variable**. Par exemple, sélectionnez l'adresse IP du serveur d'équilibrage de charge « ipaddress1 », puis cliquez sur **Convertir en variable**. La variable est maintenant entourée de « $ » comme indiqué dans l'image ci-dessous.



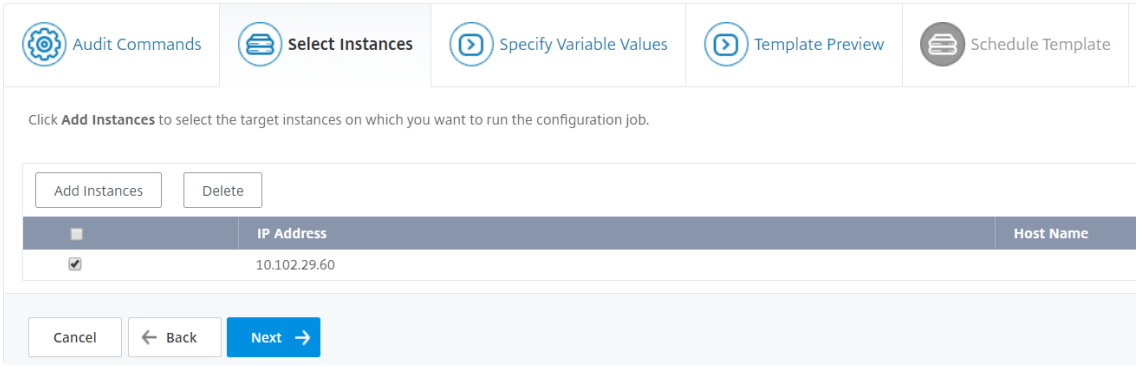
   Dans la fenêtre **Définir une variable**, définissez les propriétés de cette variable - nom, nom d'affichage et type de la variable. Cliquez sur l'option **Avancé** si vous souhaitez spécifier une valeur par défaut pour votre variable.



Vous pouvez également enregistrer les commandes en tant que modèle de configuration.



5. Cliquez sur **Enregistrer**, puis sur **Suivant**.
6. Dans l'onglet **Sélectionner les instances**, sélectionnez les instances sur lesquelles vous souhaitez exécuter l'audit de configuration et cliquez sur **Suivant**.

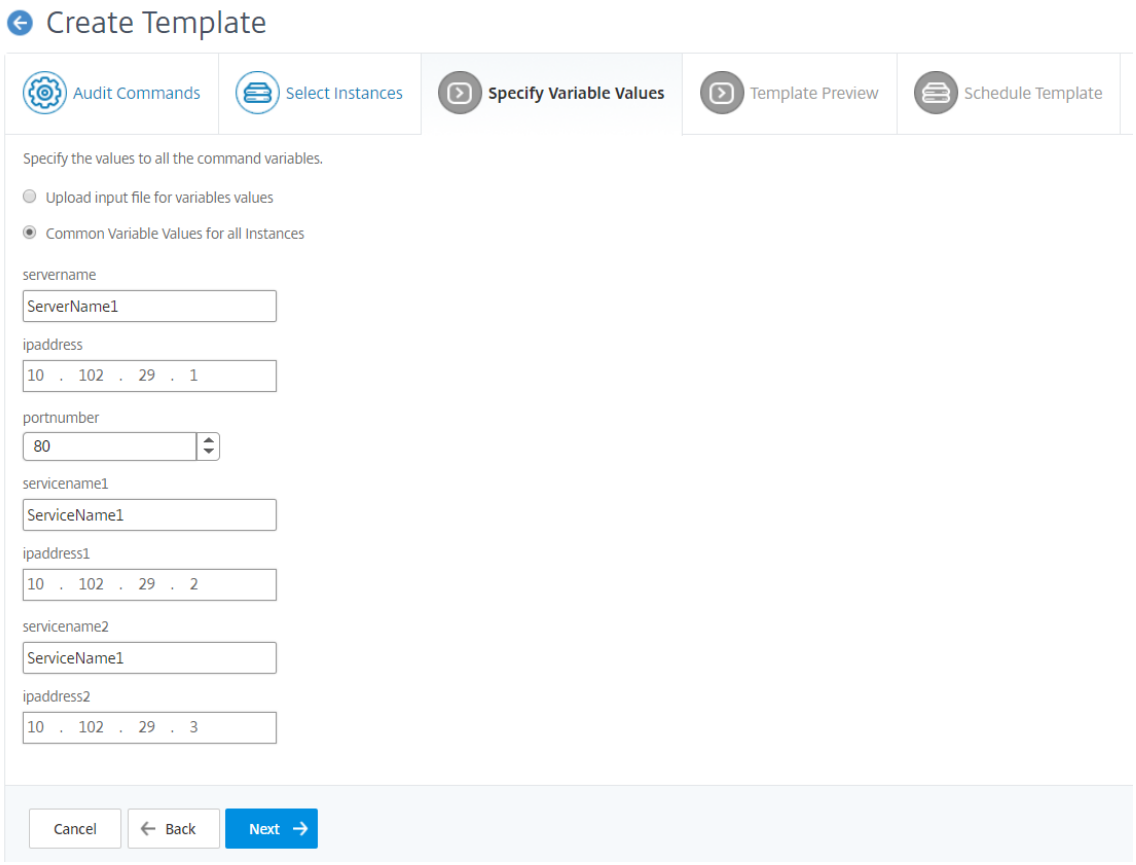


7. Dans l'onglet **Spécifier les valeurs de variable**, vous avez deux options :

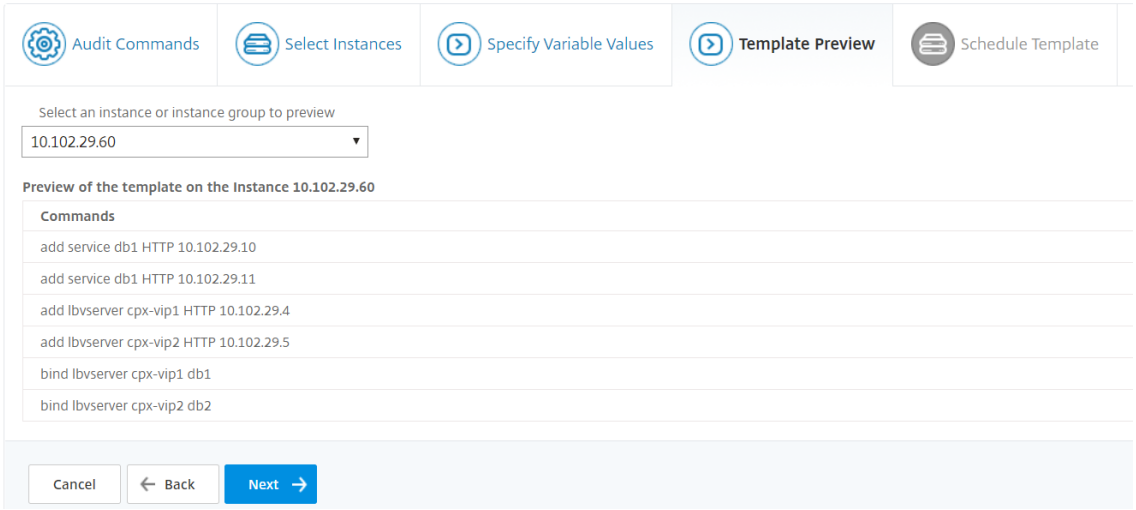
   a) Téléchargez le fichier d'entrée pour entrer les valeurs des variables que vous avez définies dans vos commandes, puis téléchargez le fichier sur le serveur Citrix ADM

   b) Entrez des valeurs communes pour les variables que vous avez définies pour toutes les instances

8. Cliquez sur **Suivant**.



9. Dans l'onglet **Aperçu du modèle**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances. Cliquez sur **Suivant**.



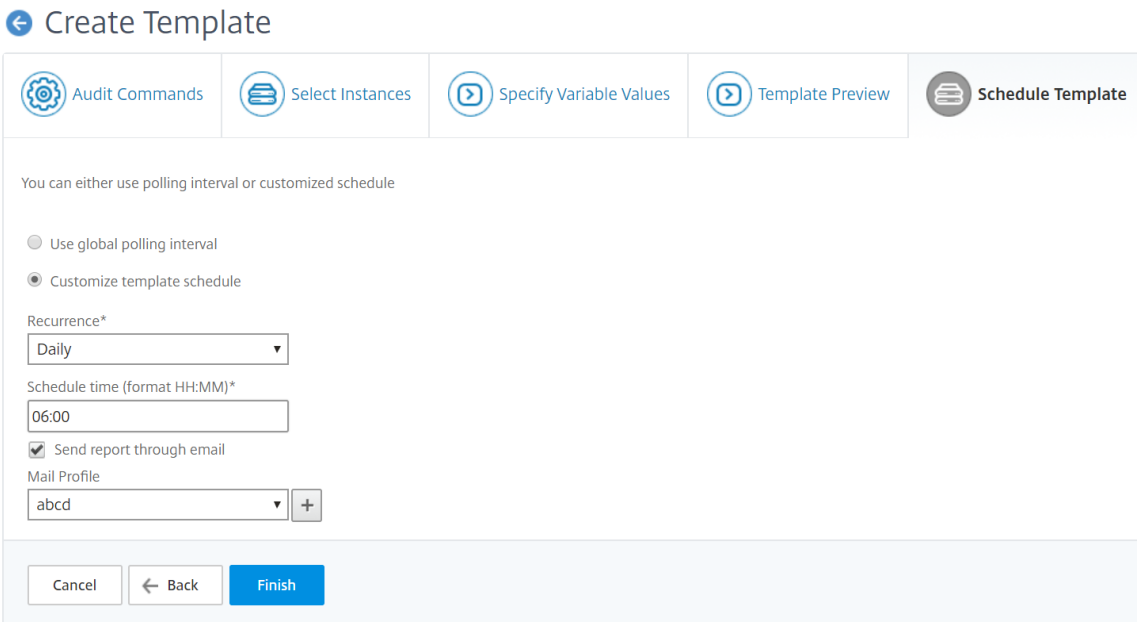
10. Dans l'onglet **Modèle de planification**, vous disposez des options suivantes pour planifier l'exécution du modèle et configurer l'adresse de messagerie pour envoyer le rapport de diff.

    - **Utilisez l'intervalle d'interrogation global**. Sélectionnez cette option pour exécuter le modèle sur les instances à un moment configuré globalement sur Citrix ADM.

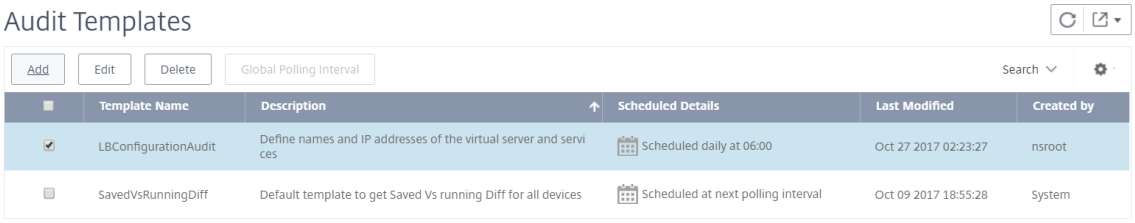
      > **Remarque**
      >
      > Pour configurer l'intervalle d'interrogation global dans Citrix ADM, accédez à **Réseaux** > **Audit de configuration** > **Modèles d'audit,** puis cliquez sur **Intervalle d'interrogation globale**. Dans le champ **Intervalle d'interrogation**, entrez les minutes auxquelles Citrix ADM doit interroger globalement les instances.

    - **Personnaliser la planification du modèle**. Utilisez cette option pour configurer l'heure et la fréquence auxquelles les modèles doivent être exécutés
    - **Envoyer un rapport par courrier électronique**. Utilisez cette option pour configurer le profil de messagerie auquel le rapport diff doit être envoyé en tant que pièce jointe.

11. Cliquez sur **Terminer**.



Le modèle d'audit apparaît dans la liste **Modèles d'audit** et est exécuté à l'heure planifiée par rapport aux configurations dans les instances spécifiées.



Audit de configuration d'interrogation des instances Citrix ADC

April 29, 2021

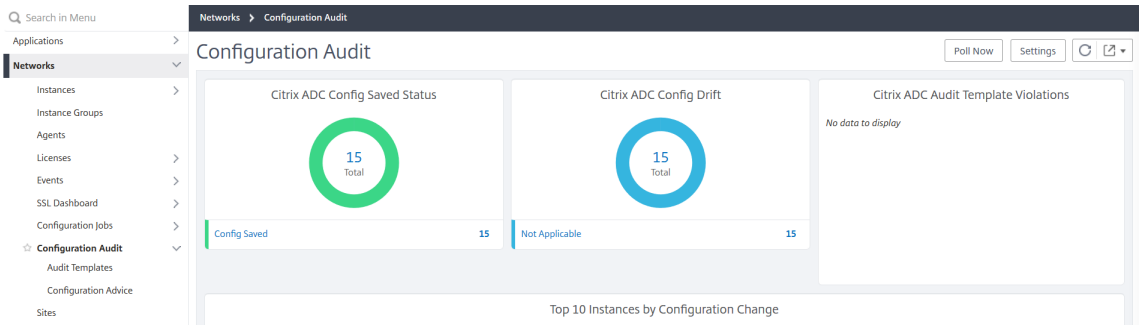
Citrix Application Delivery Management (ADM) interroge automatiquement les audits de configuration toutes les 10 heures pour rechercher les modifications de configuration qui se produisent sur les instances de Citrix ADC. Vous pouvez également interroger manuellement les audits de configuration pour découvrir les modifications récentes, mais l'interrogation de toutes les configurations d'instances Citrix ADC entraîne une lourde charge sur le réseau.

Au lieu d'interroger l'intégralité 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 :

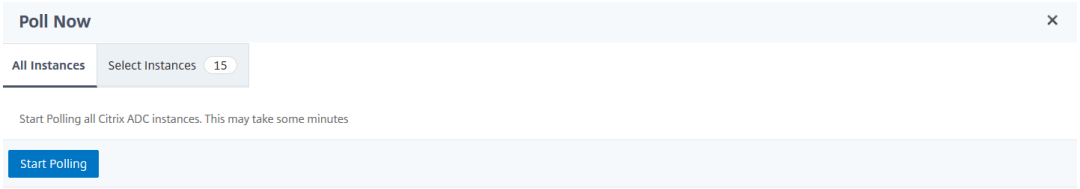
1. Dans Citrix ADM, accédez à **Réseaux** > **Audit de configuration**.

2. Dans la page **Audit de configuration**, dans le coin supérieur droit, cliquez sur **Sondage maintenant** .

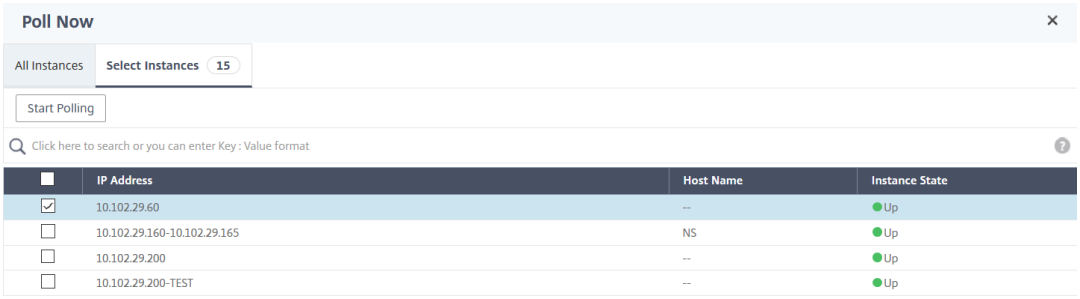


3. La page **Interroger maintenant** apparaît, vous donnant la possibilité d'interroger toutes les instances Citrix ADC dans le réseau ou d'interroger les instances sélectionnées.

   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 **Démarrer l'interrogation** .



Afficher les rapports d'audit

April 29, 2021

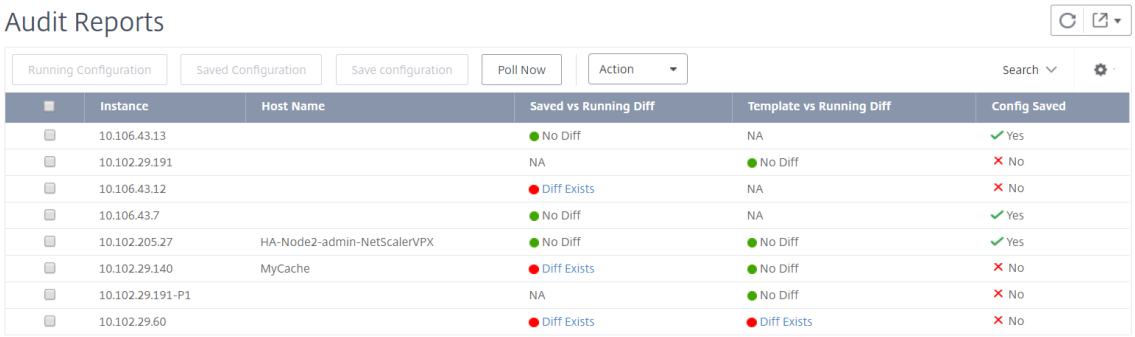
Citrix Application Delivery Management (ADM) vous permet d'afficher et de télécharger le rapport de diff d'audit de configuration dans la section Audit de configuration. La section Audit de configuration vous permet d'exporter le rapport récapitulatif sur toutes les instances et par instance, ainsi que d'exporter un rapport de diff granulaire pour chaque paire instance-modèle.

Les modèles d'audit qui apparaissent dans la liste Modèles d'audit sont exécutés à l'heure planifiée par rapport aux configurations dans les instances spécifiées. Le graphique **Citrix ADC Config Drift** du tableau de bord **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 **Citrix ADC Config Drift**, la page **Rapports d'audit** suivante affiche une liste d'instances qui affiche à la fois "Diff Exists" et "Aucun Diff." Vous pouvez télécharger les rapports de différence affichés par Citrix ADM.

Citrix ADM offre également une option pour planifier l'exportation automatique du rapport de diff en tant que pièce jointe au courrier. Pour plus d'informations sur la planification de l'exportation des rapports, reportez-vous à la sectionCréation de modèles d'audit.

Exporter les rapports d'audit de configuration

1. Dans Citrix ADM, accédez à **Réseaux** > **Audit de configuration**.
2. Dans la page **Audit de configuration**, cliquez dans le graphique **Citrix ADC 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.



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

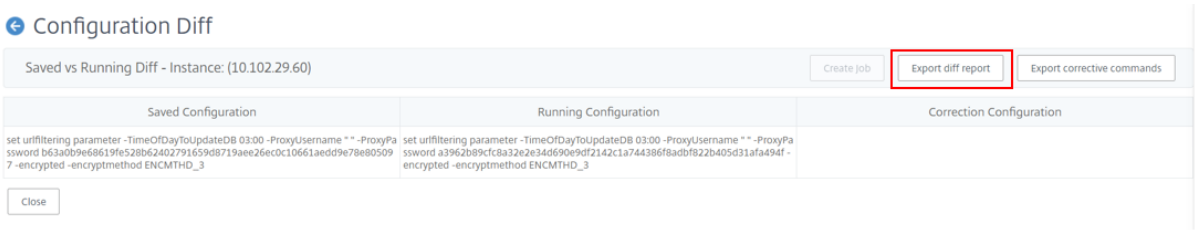
Dans l'image, vous pouvez voir que pour certains cas, un diff est présent uniquement dans **Sauvegardé vs Running Diff** et pour certains cas, un diff est présent uniquement dans **Template vs Running Diff**. Dans certains cas, des différences existent à la fois dans le **Diff enregistré vs en cours d'exécution** et dans le **modèle vs Diff en cours d'exécution** .

Sauvegarde vs exécution Diff :

Vous pouvez afficher un rapport de différence 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

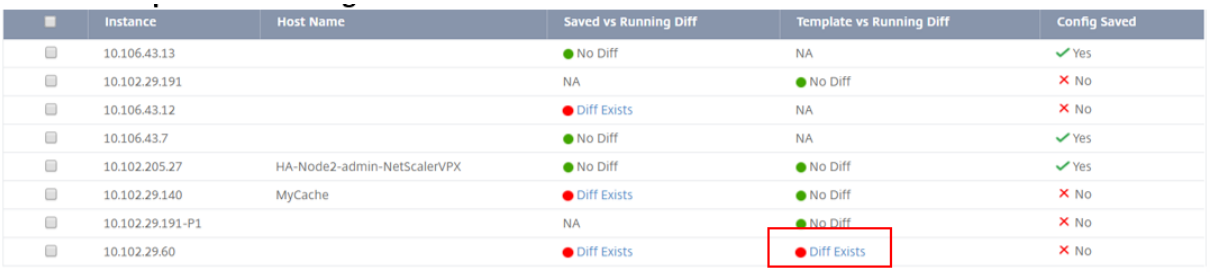
Ici, vous pouvez voir un rapport pour la configuration enregistrée par rapport à l'exécution de diff de configuration pour cette instance.



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 ADC associée à partir de tâches de configuration pour corriger la configuration dans cette instance.

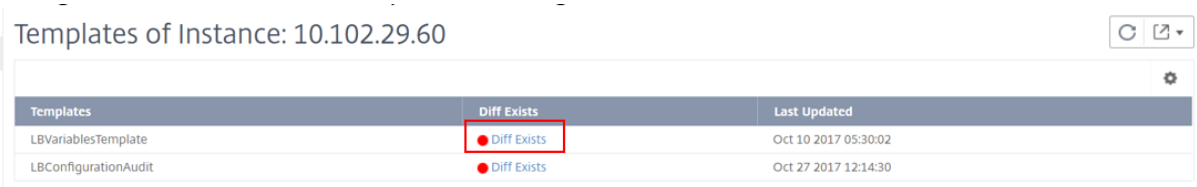
Modèle vs exécution de Diff :

Le **Diff Template vs Running** inclut tous les modèles autres que **Sauvé 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.**



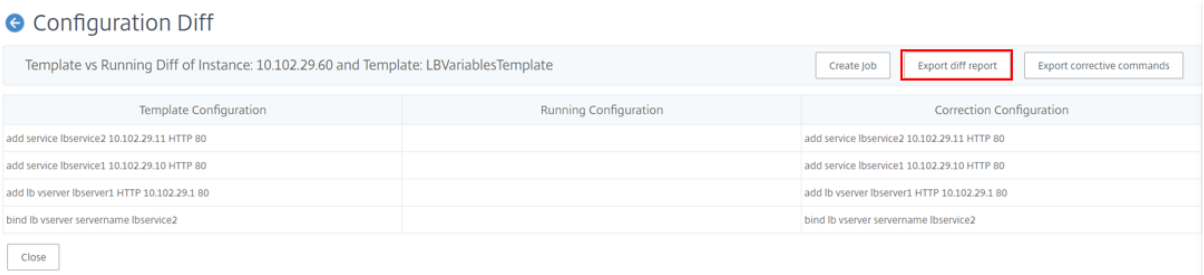
	Instance	Host Name	Saved vs Running Diff	Template vs Running Diff	Config Saved
	10.106.43.13		No Diff	NA	Yes
	10.102.29.191		NA	No Diff	No
	10.106.43.12		Diff Exists	NA	No
	10.106.43.7		No Diff	NA	Yes
	10.102.205.27	HA-Node2-admin-NetScalerVPX	No Diff	No Diff	Yes
	10.102.29.140	MyCache	Diff Exists	No 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 de Citrix ADC a une configuration différente de celle que le modèle recherche.



Templates	Diff Exists	Last Updated
LBVariablesTemplate	Diff Exists	Oct 10 2017 05:30:02
LBConfigurationAudit	Diff Exists	Oct 27 2017 12:14:30

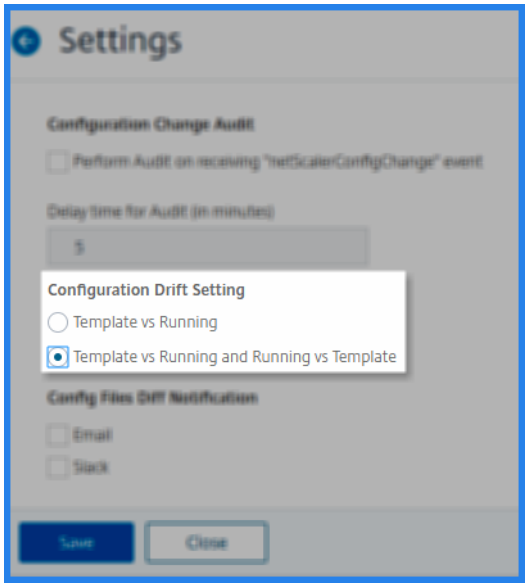
Cliquez à nouveau sur **Diff Existe** . L'image suivante montre la configuration recherchée par le modèle et la configuration en cours d'exécution vide, car aucune commande de ce type n'a été configurée ou n'a été supprimée. Vous pouvez également voir les configurations de correction ou les commandes à exécuter pour corriger la configuration.



Vous pouvez également utiliser le paramètre de dérive Template vs Running et Running vs template, pour comparer la configuration des deux façons :

- Compare la configuration du modèle d'audit avec la configuration en cours d'exécution sur l'instance.
- Compare la configuration en cours d'exécution sur l'instance avec le modèle d'audit.

Par défaut, le paramètre de dérive Template vs Exécution est sélectionné. Pour modifier le paramètre de dérive, dans l'interface graphique d'ADM, sélectionnez **Paramètres** dans la page **Vérification de la configuration**.



Cliquez sur **Exporter le rapport de diff** pour télécharger un fichier .csv du rapport de diff. Vous pouvez également cliquer sur **Exporter les commandes correctives** pour exporter les commandes dans un fichier .txt. Vous pouvez ensuite exécuter les commandes dans l'interface de ligne de commande pour corriger la configuration dans cette instance.

L'image suivante montre un exemple de fichier diff .csv téléchargé sur votre système :

#Template vs Running Diff of Instance: 10.102.29.60 and Template: LBVariablesTemplate		
Template Configuration	Running Configuration	Correction Configuration
add service lbservice2 10.102.29.11 HTTP 80		add service lbservice2 10.102.29.11 HTTP 80
add service lbservice1 10.102.29.10 HTTP 80		add service lbservice1 10.102.29.10 HTTP 80
add lb vserver lbserver1 HTTP 10.102.29.1 80		add lb vserver lbserver1 HTTP 10.102.29.1 80
bind lb vserver servername lbservice2		bind lb vserver servername lbservice2

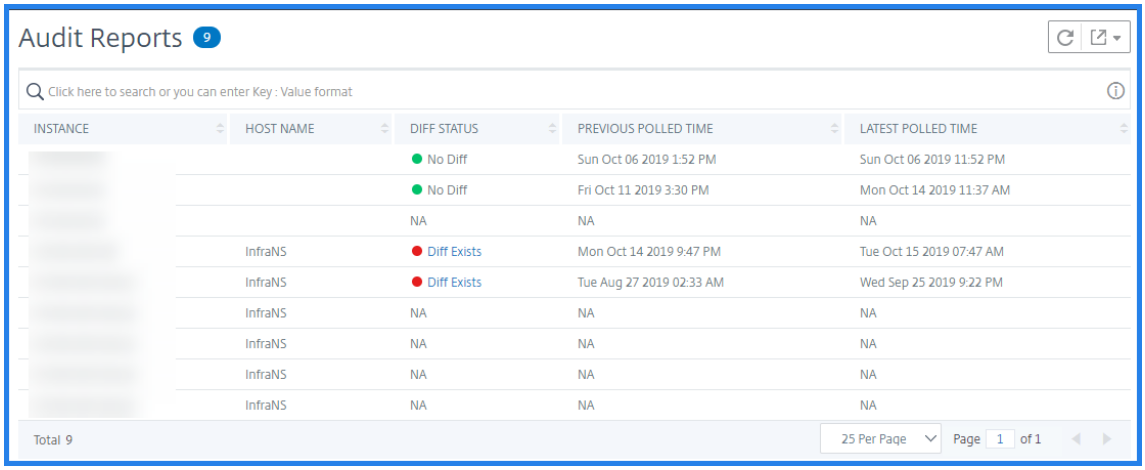
Afficher les rapports d'audit de l'état des fichiers

À l'aide du graphique **Citrix ADC File Status**, vous pouvez vérifier si des fichiers sont ajoutés, modifiés ou supprimés dans le `nsconfig` dossier. Par exemple : si le fichier de licence est mis à jour sur une instance ADC, vous pouvez vérifier la date de la dernière mise à jour de ce fichier et prendre les mesures appropriées.

Pour exporter les rapports d'audit d'état des fichiers pour les instances de Citrix ADC :

1. Dans Citrix ADM, accédez à **Réseaux** > **Audit de configuration**.
2. Dans la page **Audit de configuration**, cliquez dans le graphique **État du fichier Citrix ADC** .

   La page **Rapports d'audit** répertorie les instances ayant le statut Diff.



   L' **état de la** différence est calculé pour l'intervalle entre l'heure d' **interrogation précédente et l'heure** d' **interrogation la plus récente** . L' **état** de la différence peut être l'un des suivants :

   - **Diff existe** - Cet état indique que les fichiers ont changé dans le`nsconfig` dossier d'une instance depuis l' **heure d'interrogation précédente** . Pour afficher ce qui a changé sur le fichier, cliquez sur **Diff Exists**.

     ! [Diff existe dans `nsconfig` le dossier] (/en-us/citrix-application-delivery-management-service/media/config-audit-file-status-diff.png)

   - **No Diff** - Cet état indique que les fichiers du `nsconfig` dossier n'ont pas changé depuis l'heure d'interrogation précédente.

- **NA** - Cet état indique que la surveillance de l'état du fichier n'est pas applicable. Cet état apparaît lorsque Citrix ADM n'interroge pas l'instance. Par exemple, lorsqu'une instance est ajoutée récemment ou que l'état de l'instance est inactif, l'interrogation de l'instance ne se produit pas.

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 tous les jours, toutes les semaines ou tous les mois et envoyer le rapport par e-mail ou par message de marge.

> **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.

Générer un diff d'audit de configuration pour les interruptions SNMP ConfigChange

April 29, 2021

Chaque fois qu'il y a une modification de configuration dans une instance de Citrix ADC dans le réseau, le fichier de configuration est mis à jour. L'instance envoie une interruption SNMP ConfigChange à Citrix Application Delivery Management (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 Diff Exists s'affiche sur la page Rapport d'audit. En cliquant sur le lien Quittes de différence, vous accédez à la page Diff de configuration, où vous pouvez afficher la commande corrective. Vous pouvez utiliser ces commandes correctives pour créer un travail de configuration et l'exécuter sur les instances Citrix ADC spécifiques. Lorsque vous exécutez le travail de configuration, les instances sont ramenées à la configuration souhaitée. Pour plus d'informations sur la création d'un travail de configuration à partir de commandes correctives, reportez-vous à la sectionComment créer des tâches 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 **Audit de configuration** .
3. Cliquez sur l'icône Modifier dans la section **Paramètres d'audit des modifications de configuration** .
4. **Activez la case à cocher Do Configuration Audit 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 recevant à l'avenir les interruptions SNMP NetScaler-ConfigChange.

5. Dans le champ **Délai d'exécution du modèle d'audit (en minutes)**, tapez 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.

Audit des modifications de configuration entre les instances

April 29, 2021

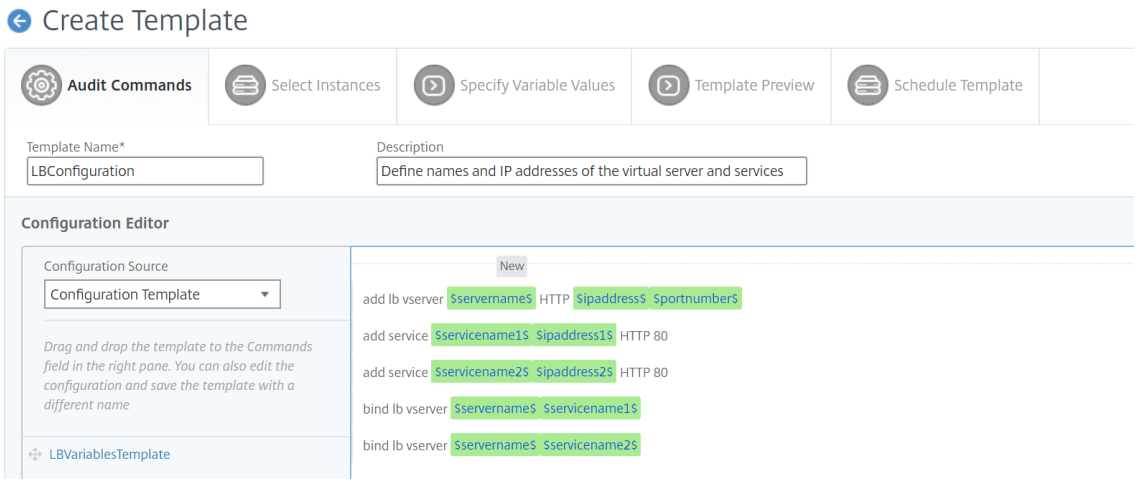
Vous voulez vous assurer que certaines configurations sont exécutées sur des instances spécifiques pour des performances optimales de votre réseau. Vous souhaitez également surveiller les modifications de configuration sur les instances Citrix ADC gérées, résoudre les erreurs de configuration et restaurer 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 (ADM) compare ces instances avec le modèle d'audit et les rapports en cas de non-concordance dans la configuration. Cette comparaison 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 pouvez également envoyer le rapport diff généré par Citrix ADM à des

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.

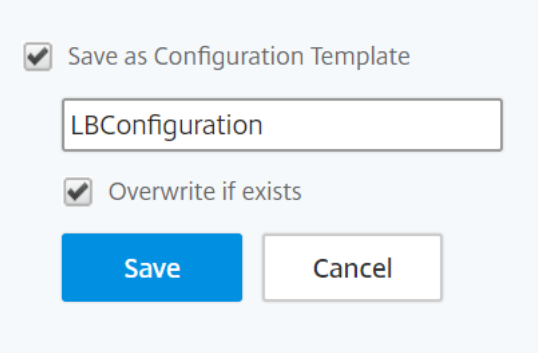
Pour créer des modèles d'audit :

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 à 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 illustré dans l'image suivante.



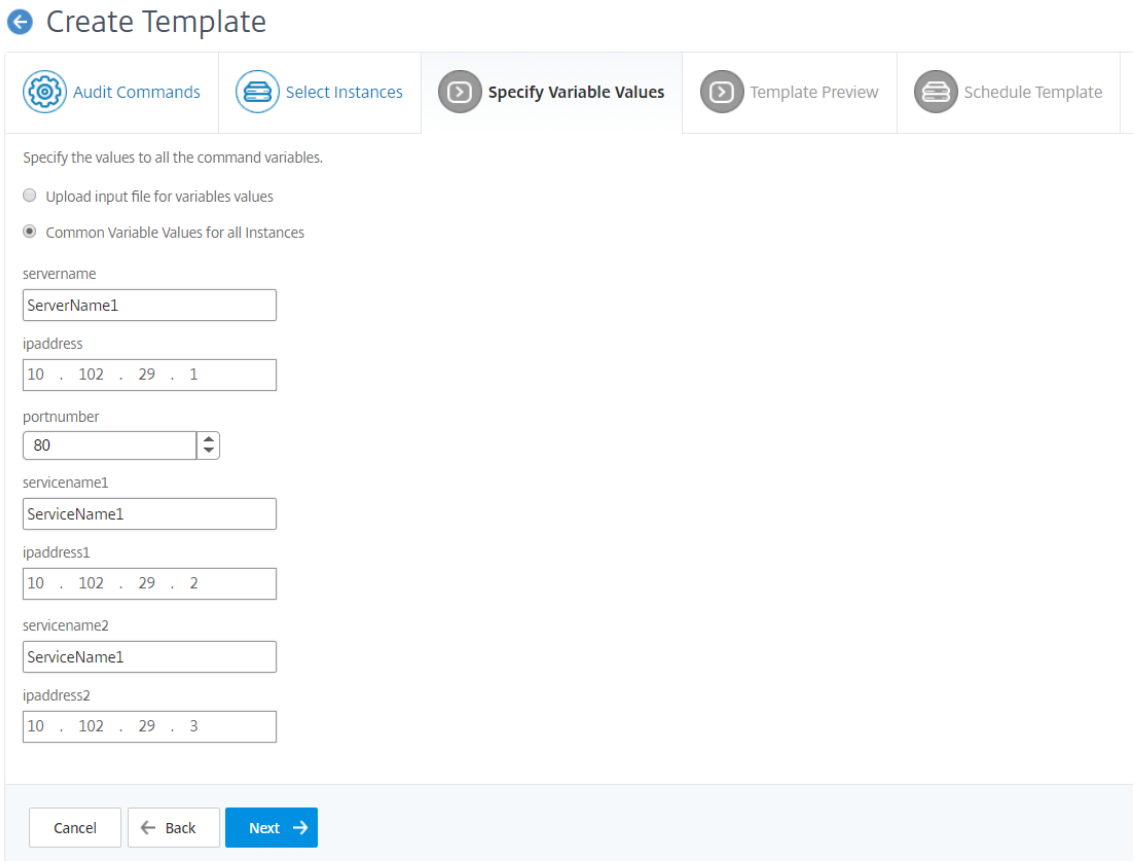
Cliquez sur l'option **Avancé** si vous souhaitez spécifier une valeur par défaut pour votre variable.

Vous pouvez également enregistrer les commandes en tant que modèle de configuration.



5. Cliquez sur **Enregistrer**, puis sur **Suivant**.

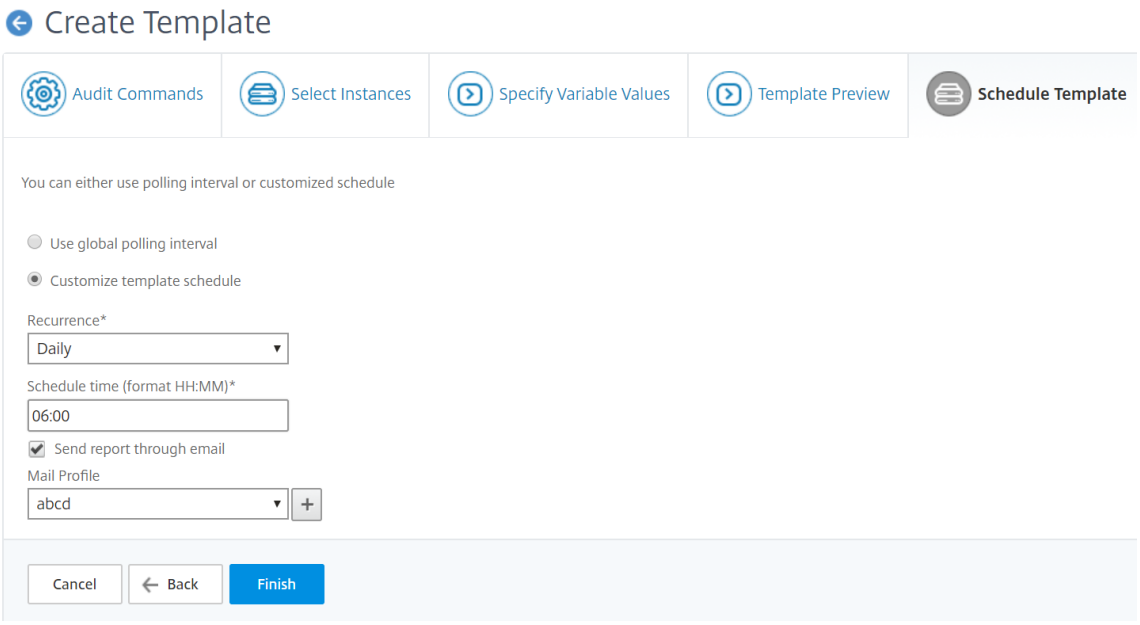
6. Dans l'onglet **Sélectionner les instances**, sélectionnez les instances sur lesquelles vous souhaitez exécuter l'audit de configuration.
7. Dans l'onglet **Spécifier les valeurs de variable**, vous avez deux options :
   a) Téléchargez le fichier d'entrée pour entrer les valeurs des variables que vous avez définies dans vos commandes, puis téléchargez le fichier sur le serveur Citrix ADM
   b) Entrez des valeurs communes pour les variables que vous avez définies pour toutes les instances
8. Cliquez sur **Suivant**.



9. Dans l'onglet **Aperçu du modèle**, vous pouvez évaluer et vérifier les commandes à exécuter sur chaque instance ou groupe d'instances. Cliquez sur **Suivant**.
10. Dans l'onglet **Modèle de planification**, vous avez trois options pour automatiser l'exécution du modèle et 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
    - **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 e-mail**. Utilisez cette option pour configurer le profil de messagerie auquel le rapport diff doit être envoyé en tant que pièce jointe.

11. Cliquez sur **Terminer**.

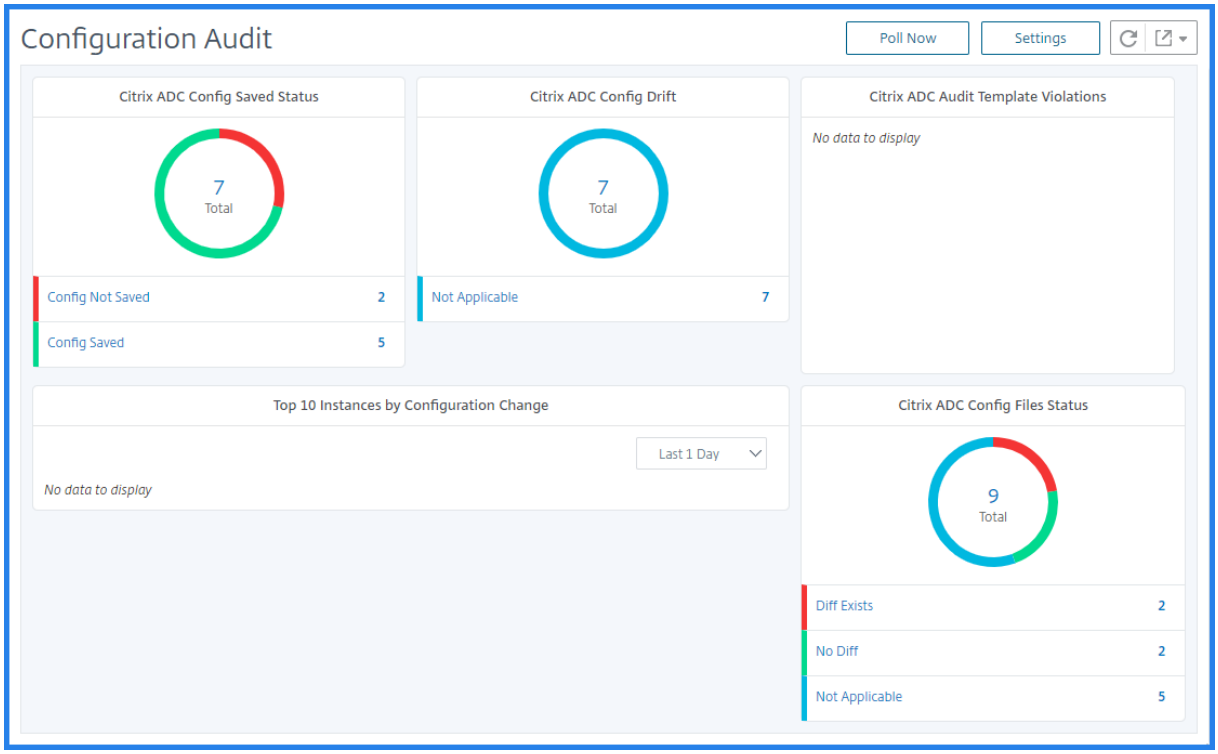


Le modèle d'audit apparaît dans la liste Modèles d'audit et est exécuté à l'heure planifiée sur les configurations des instances spécifiées.

Affichage des détails des modifications de configuration

Vous pouvez également utiliser le tableau de bord Vérification de la configuration pour afficher des détails de haut niveau sur les modifications de configuration telles que :

- Les 10 premières instances par changement de configuration
- Nombre de configurations enregistrées et non enregistrées
- Le fichier ajouté, supprimé ou modifié dans le `nsconfig` dossier

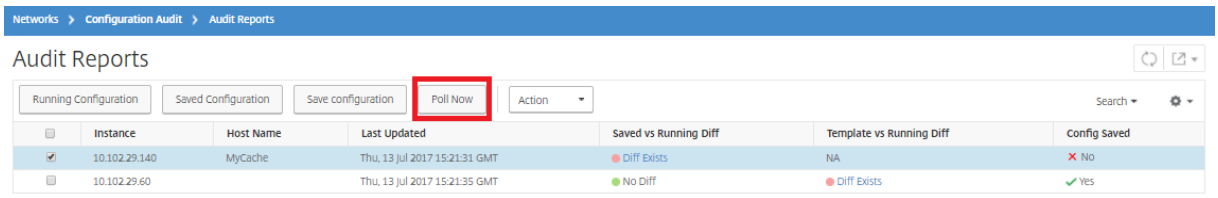


Citrix ADM vous permet également d'interroger manuellement les audits de configuration et ajoute immédiatement tous les audits de configuration des instances à Citrix ADM. Pour ce faire, accédez à **Réseaux** > **Audit de configuration,** cliquez sur **Interroger maintenant,** la page contextuelle **Interroger maintenant** vous offre une option pour interroger toutes les instances de Citrix ADC du réseau ou interroger les instances sélectionnées.

Vous pouvez également forcer un audit sur une instance. Pour ce faire, cliquez sur l'un des graphiques suivants :

- **Statut enregistré de Citrix ADC Config**
- **Drift de configuration Citrix ADC**

Sur la page **Rapports d'audit**, sélectionnez l'instance et, dans la liste **Action**, sélectionnez **Interroger maintenant** .

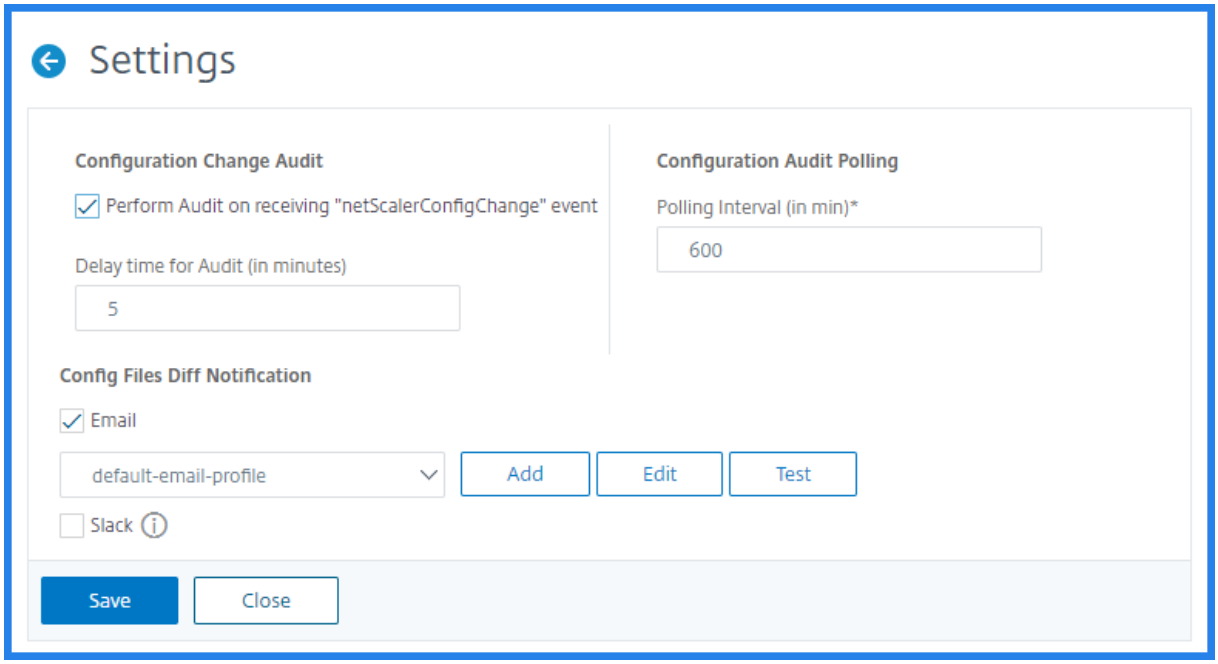


Le graphique **État du fichier de configuration Citrix ADC** vous indique l'état des fichiers Citrix ADC présents dans le `nsconfig` dossier. Citrix ADM enregistre et compare les modifications apportées aux fichiers dans le dossier `nsconfig` et affiche les différences. Consultez Afficher les rapports d'audit d'état des fichiers.

Définir les notifications d'audit de configuration

1. Accédez à **Réseaux** > **Audit de configuration**.
2. Dans la page **Audit de configuration**, cliquez sur **Paramètres** .
3. Sur la page **Paramètres** :
   a) Activez la case à cocher **Effectuer l'audit à la réception de l'événement « NetScaler-ConfigChange**, pour activer les paramètres de notification.
   b) Définissez l'heure de retard pour Audit.
4. Dans Intervalle **d'audit de configuration**, définissez l' **intervalle d'interrogation**.

   Citrix ADM interroge les événements d'audit de configuration pour l'intervalle d'interrogation spécifié.
5. Dans **Config Files Diff Notification**, sélectionnez la plate-forme sur laquelle vous souhaitez recevoir les notifications :
   - **E-mail** : sélectionnez la liste de distribution des e-mails. Cliquez sur Ajouter pour ajouter une liste de distribution par e-mail pour recevoir une notification.
   - **Slack** - Sélectionnez ADCal Slack dans la liste. Cliquez sur Ajouter pour ajouter un canal pour recevoir une notification.



Obtenir des conseils de configuration sur la configuration du réseau

April 29, 2021

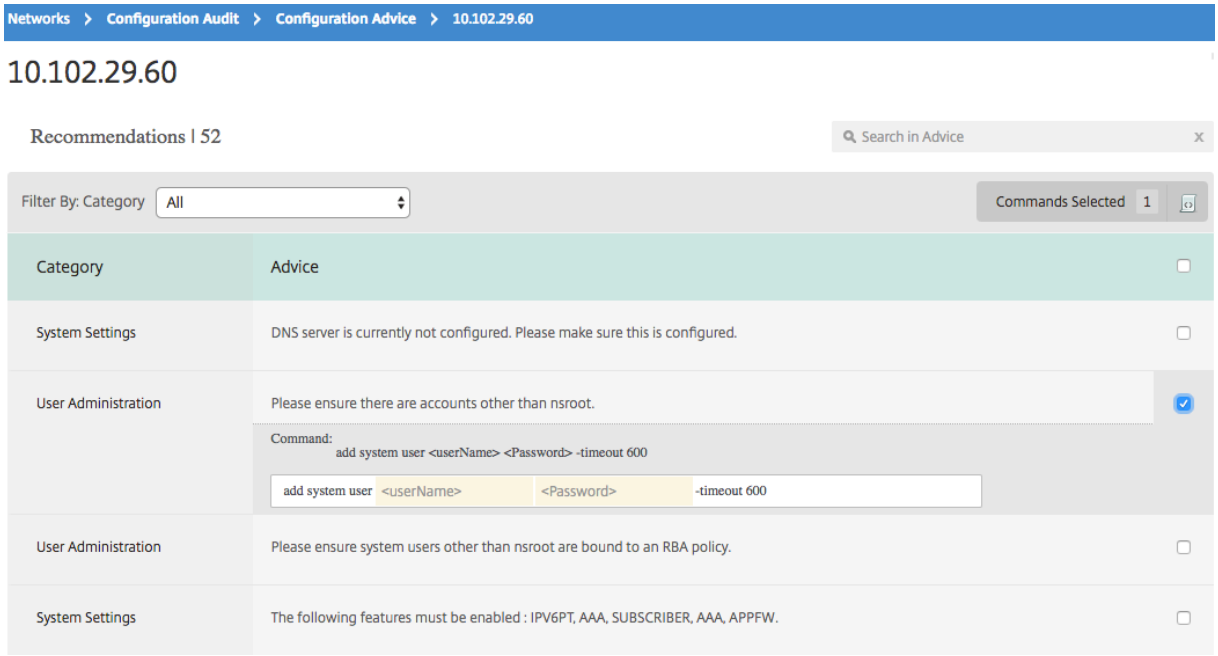
Vous configurez vos instances Citrix ADC avec des configurations optimales afin d'obtenir des performances optimales sur vos applications. Cependant, il est possible que certaines configurations ne soient pas des configurations standard, ce qui affecte les performances de vos applications.

Pour vous aider à optimiser les performances de votre application, Citrix Application Delivery Management (ADM) analyse la configuration de l'instance Citrix ADC et vous fournit des recommandations. Vous pouvez appliquer les configurations recommandées à partir de Citrix ADM.

Pour analyser l'instance de Citrix ADC :

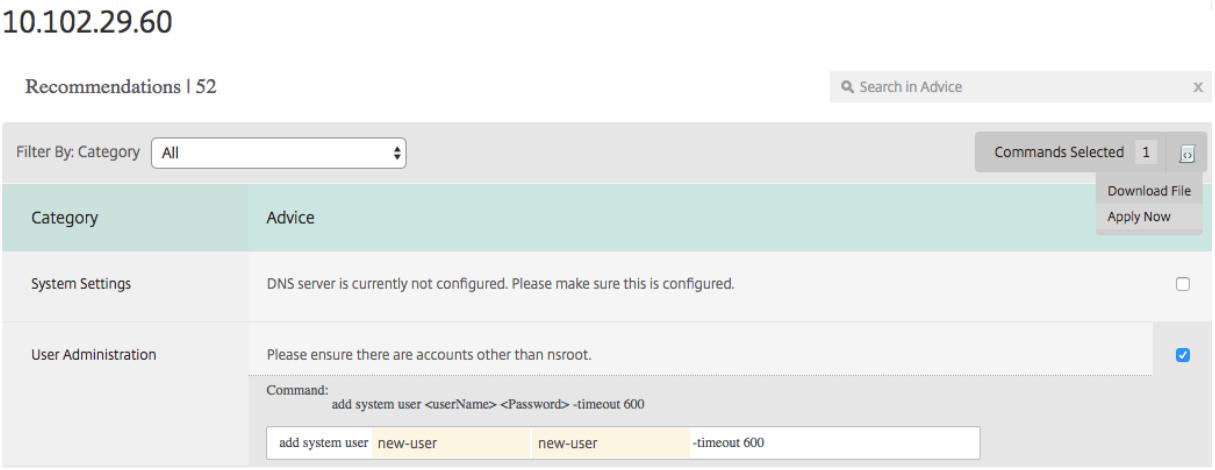
1. Accédez à **Réseaux** > **Audit deconfiguration > Conseil de configuration** .
2. Procédez comme suit :
    - Cliquez sur **Télécharger le fichier de configuration** et chargez le fichier de configuration de votre instance réseau.
    - Cliquez sur **Sélectionner un périphérique**, puis sélectionnez l'instance Citrix ADC que vous souhaitez analyser.

Citrix ADM analyse la configuration de votre instance et fournit une liste de recommandations de configuration, comme indiqué dans l'image suivante. Cochez la case située en regard d'un conseil de configuration pour afficher les commandes correctives.

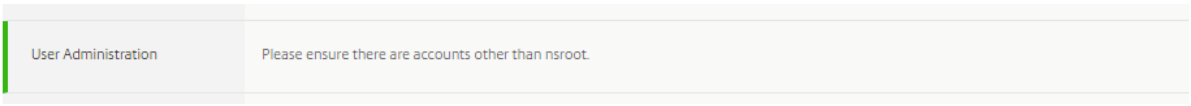


Si vous souhaitez mettre à jour votre configuration, spécifiez les valeurs des variables dans les commandes correctives et cliquez sur **Appliquer maintenant** comme indiqué dans l'image suivante.

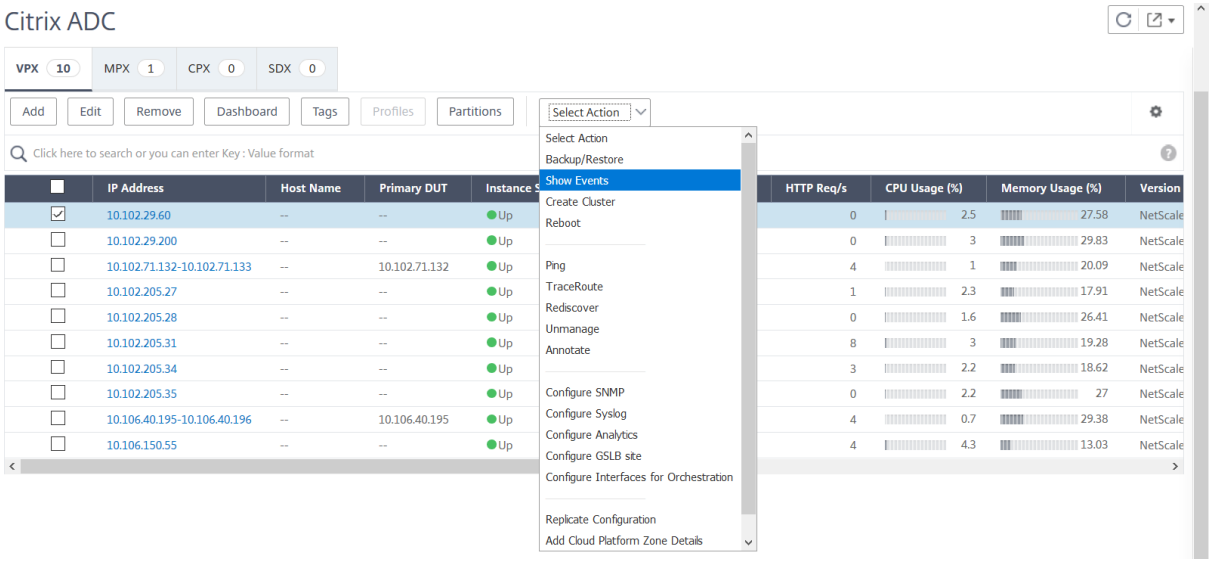
> **Remarque**
>
> Les commandes répertoriées ici ne sont que des recommandations. Un utilisateur disposant d'un accès en lecture et en écriture peut modifier n'importe quelle commande à l'aide de cette fonctionnalité. Assurez-vous d'accorder un accès privilégié limité aux utilisateurs qui, selon vous, ne doivent pas modifier les commandes.



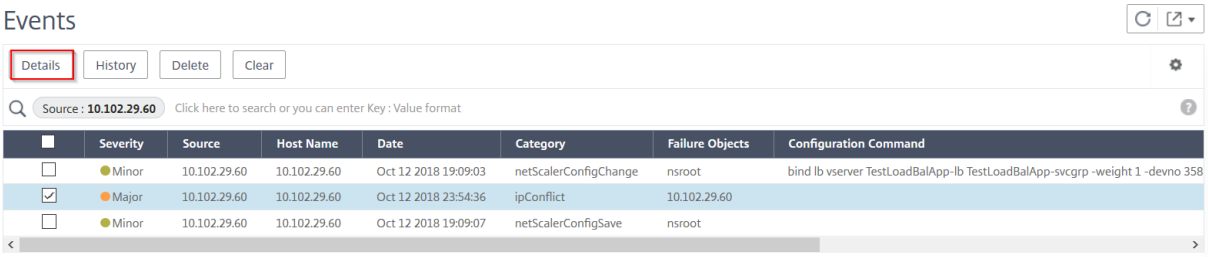
Lorsque la commande est exécutée avec succès sur l'instance réseau, la case à cocher en regard de l'avis disparaît.



Si vous souhaitez afficher les détails des commandes exécutées sur votre instance réseau, accédez à **Réseaux** > **Instances** > **<Instance_Type>**, sélectionnez l'adresse IP de l'instance, puis cliquez sur **Afficher les événements** dans le menu **Sélectionner les actions** liste déroulante.



Sur la page **Événements**, vous pouvez afficher les détails de la modification de configuration.



Fonctions réseau

April 29, 2021

À l'aide de la fonctionnalité Fonctions réseau, vous pouvez surveiller l'état des entités configurées sur vos instances Citrix Application Delivery Controller (Citrix 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 Fonctions réseau fournit les graphiques suivants :

- Les 5 meilleurs serveurs virtuels avec les connexions client les plus élevées
- Les 5 meilleurs serveurs virtuels avec les connexions serveur les plus élevées
- Les 5 principaux serveurs virtuels avec un débit maximal (Mo/s)
- 5 serveurs virtuels les plus bas avec un débit le plus faible (Mo/s)
- Top 5 des instances avec la plupart des serveurs virtuels

- État des serveurs virtuels
- Santé des serveurs virtuels d'équilibrage de charge
- Protocoles
- Méthode d'équilibrage de charge
- Persistance de l'équilibrage de charge
- Top 5 des instances HaProxy avec la plupart des fronts
- Top 5 des instances Hproxy avec la plupart des serveurs

Générer des rapports pour les entités d'équilibrage de charge

April 29, 2021

Citrix Application Delivery Management (Citrix ADM) vous permet d'afficher les rapports des entités d'instance Citrix Application Delivery Controller (Citrix ADC) à tous les niveaux. Il existe deux types de rapports que vous pouvez télécharger dans **Citrix ADM > Fonctions réseau** : les rapports consolidés et les rapports individuels.

Rapports consolidés : vous pouvez télécharger et afficher un rapport consolidé ou récapitulatif 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 d'Citrix ADC, les partitions et les entités d'équilibrage de charge correspondantes (serveurs virtuels, groupes de services et services) présentes dans 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
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	cs_lb1#0.0.0.0:0		cs_svc1#192.168.4.56:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	cs_lb2#0.0.0.0:0		cs_svc2#192.168.4.57:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	v1#192.168.3.100:80		s1#192.168.4.51:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	v1#192.168.3.100:80		s3#192.168.4.53:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	v1#192.168.3.100:80		s5#192.168.4.55:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	v1#192.168.3.100:80		s4#192.168.4.54:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	v1#192.168.3.100:80		s2#192.168.4.52:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	cs_lb3#0.0.0.0:0		cs_svc3#192.168.2.58:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	vs1#192.168.1.100:443		s4#192.168.2.54:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	vs1#192.168.1.100:443		s1#192.168.2.51:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	vs1#192.168.1.100:443		s2#192.168.2.52:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	vs1#192.168.1.100:443		s3#192.168.2.53:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	vs1#192.168.1.100:443		s5#192.168.2.55:80	

Le rapport consolidé est au format CSV. Les entrées de chaque colonne sont décrites comme suit :

- **Adresse IP Citrix ADC** : l'adresse IP de l'instance de Citrix ADC est affichée dans le rapport
- **Citrix ADC HostName : 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 -Adresse:Port_Number

- **Groupes de services** : <name_of_service_group>#server_member1_IP_address:port,server_member2_IP_

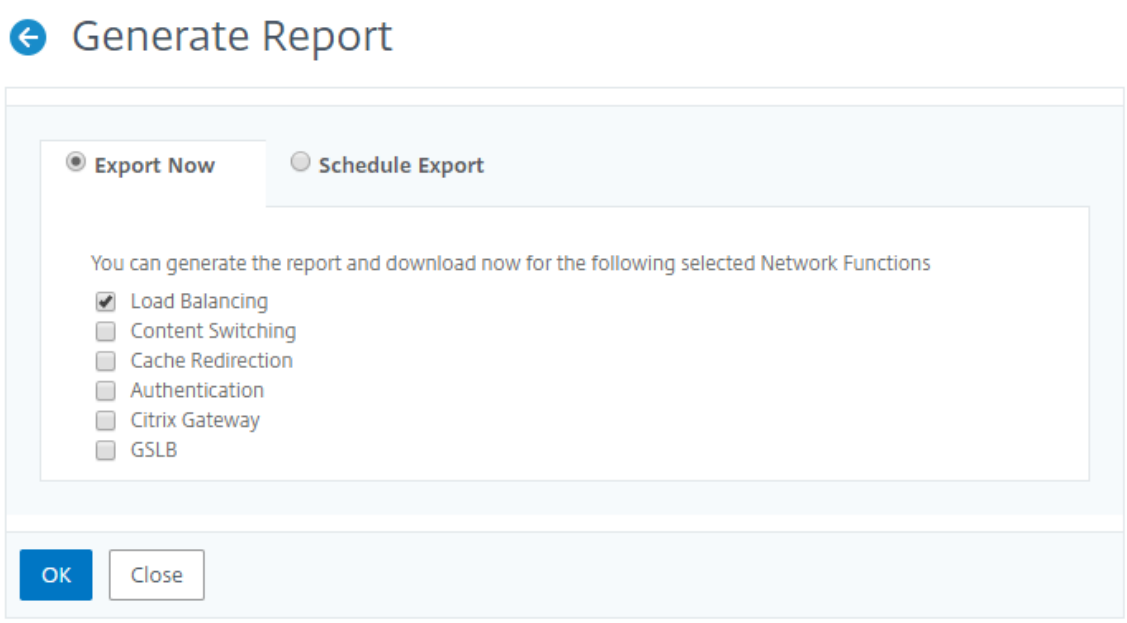
> **Remarque**
>
> - Si aucun nom d'hôte n'est disponible, l'adresse IP correspondante s'affiche.
> - Les colonnes vides indiquent que les entités respectives ne sont pas configurées pour cette instance d'Citrix ADC.

Rapports individuels : vous pouvez également télécharger et afficher des rapports indépendants de toutes les instances et entités. Par exemple, vous pouvez télécharger un rapport uniquement pour 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**.
2. Cliquez sur **Générer un rapport**.



3. Dans la page **Générer un rapport** qui s'ouvre, vous avez deux options pour afficher le rapport :
   a) Sous l'onglet **Exporter maintenant**, sélectionnez **Équilibrage de charge** et cliquez sur **OK** .

      Le rapport consolidé est téléchargé sur votre système.

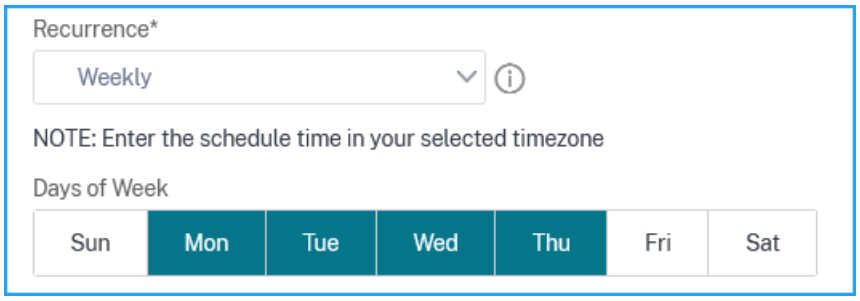
   b) Sélectionnez **Planifier le rapport** pour créer un calendrier de génération et d'exportation de rapports à intervalles réguliers. Spécifiez les paramètres de récurrence de génération

de rapport et créez un profil de messagerie vers lequel le rapport est exporté.

i. Sélectionnez **Activer la planification**.

ii. **Récurrence** : sélectionnez **Quotidien**, **Hebdomadaire**ou **Mensuel** dans la liste.

> **Remarque**
>
> Si vous sélectionnez Périodicité **hebdomadaire**, veillez à sélectionner les jours de semaine pendant lesquels vous souhaitez que le rapport soit planifié.



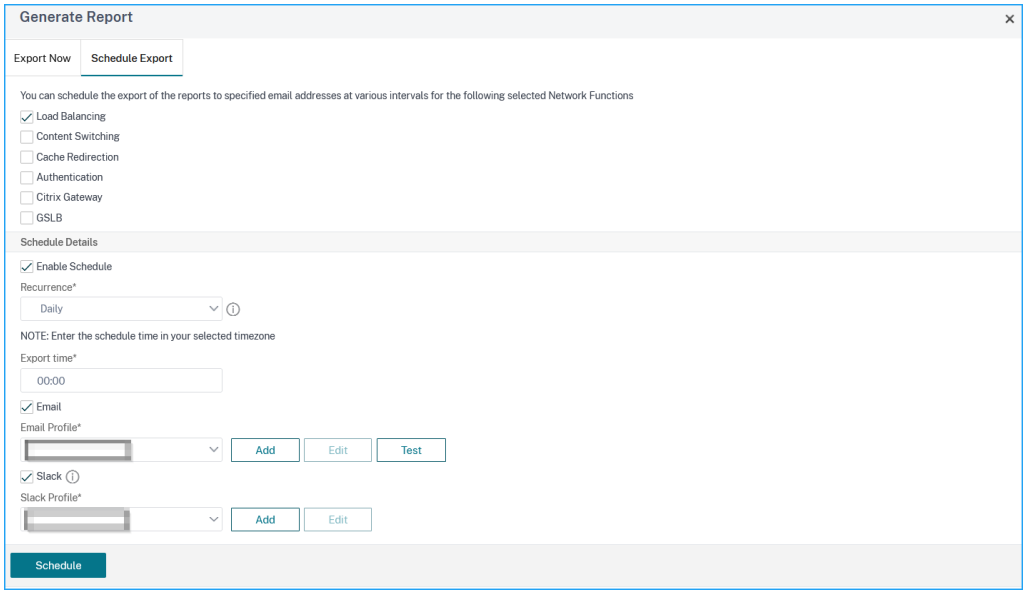
> **Remarque**
>
> Si vous sélectionnez Récurrence **mensuelle**, assurez-vous de saisir les jours du mois, avec les valeurs comprises entre 1 et 31.

iii. **Heure d'exportation** - Saisissez l'heure dans le format Heure : Minute au format 24 heures.

iv. **E-mail** : cochez la case, puis sélectionnez un profil dans la liste, ou cliquez sur **Ajouter** pour créer un profil de messagerie.

v. **Slack** - Activez la case à cocher Slack, puis sélectionnez un profil dans la zone de liste, ou cliquez sur **Ajouter** pour créer un profil de marge.

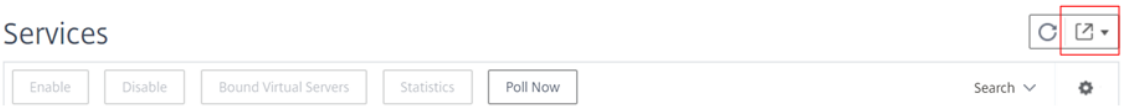
vi. Cliquez sur **Planifier** pour terminer le processus.



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.

> **Remarque**
>
> Vous ne pouvez télécharger les rapports ou les exporter que sous forme de pièces jointes. Vous ne pouvez pas afficher les rapports sur l'interface graphique graphique Citrix ADM.

Exportation ou planification de l'exportation de rapports de fonctions réseau

April 29, 2021

Vous pouvez générer un rapport complet pour certaines fonctions réseau, telles que l'équilibrage de la charge, la commutation de contenu, la redirection de cache, l'équilibrage de la charge de serveur global (GSLB), l'authentification et Citrix Gateway dans Citrix Application Delivery Management (Citrix ADM). Ce rapport vous permet d'avoir une vue de haut niveau du mappage entre les instances, les partitions et les entités liées correspondantes (serveurs virtuels, groupes de services et services) présentes dans le réseau. Vous pouvez exporter ces rapports au format .csv.

Le rapport affiche les données de serveur virtuel suivantes :

- Adresse IP Citrix ADC
- 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 Commutation de contenu et redirection de cache, la colonne Serveur virtuel LB cible répertorie tous les serveurs LB, c'est-à-dire les serveurs par défaut et les serveurs basés sur des stratégies.

- Nom du service
- Nom du groupe de services

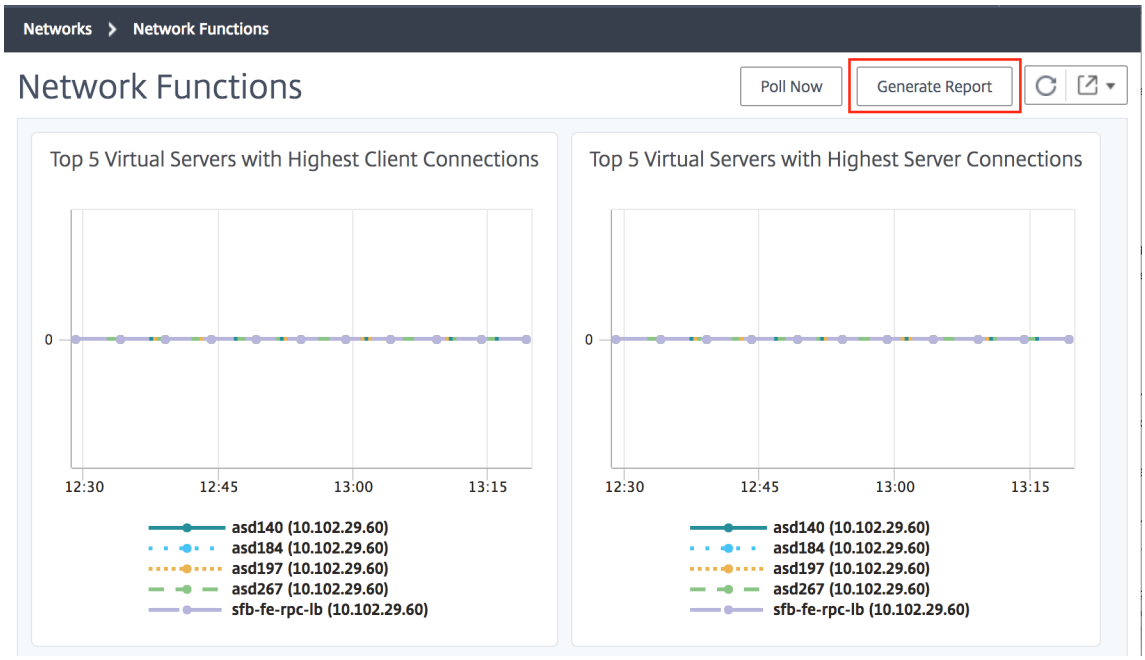
Vous pouvez planifier l'exportation de ces rapports vers des adresses e-mail spécifiées à des intervalles différents.

> **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 Commutation de contenu et redirection de cache, le rapport affiche uniquement les liaisons avec les serveurs LB associés.
> - Les serveurs virtuels SSL ne sont pas répertoriés dans ce rapport car une liste distincte de serveurs virtuels SSL n'est pas conservée sur Citrix ADM.
> - Lorsqu'un nouveau rapport est généré, les anciens rapports sont automatiquement purgés de votre compte.
> - Vous ne pouvez pas générer de rapport de fonctions réseau pour HAProxy.

Pour exporter et planifier des rapports sur les fonctions réseau :

1. Accédez à **Réseaux** > **Fonctions réseau**.

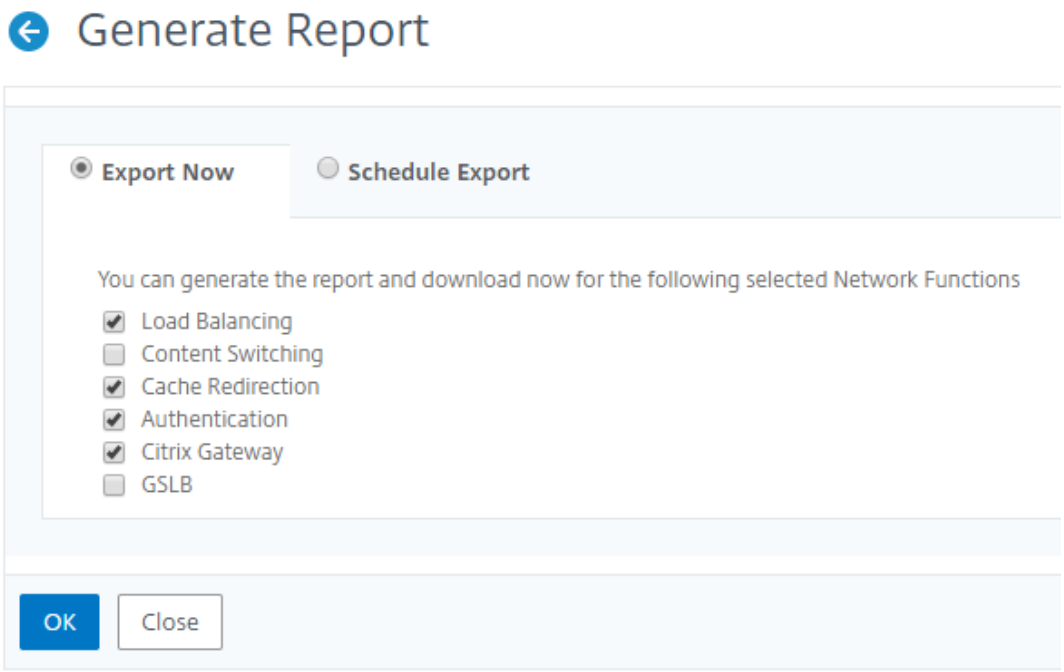
2. Dans la page **Fonctions réseau**, dans le volet droit, cliquez sur **Générer un rapport** dans le coin supérieur droit de la page.



3. Sur la page **Générer un rapport**, vous disposez des 2 options suivantes :

   a) Sélectionnez **l'onglet Exporter maintenant** et cliquez sur **OK** .

   Le rapport est téléchargé sur votre système.



   L'image suivante montre un exemple de rapport de fonctions réseau.

Citrix ADC IP Address	Citrix ADC HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
121.123.020.85	121.123.020.85		Load Balancing				
121.123.020.100	NS		Load Balancing				
121.123.020.101	admin-NetScalerVPX-10.102.122.101		Load Balancing				
121.123.020.111	PartitionsHost-sp-final-NetScalerVPX	121.123.020.111-partition_	Load Balancing				
121.123.020.115	121.123.020.115	121.123.020.115-partition-	Load Balancing				
121.123.020.139	NS1		Load Balancing				
121.123.020.49	NS1		Load Balancing				

b) Sélectionnez **Planifier le rapport** dans l'onglet pour créer une planification pour générer et exporter des rapports à intervalles réguliers. Spécifiez les paramètres de récurrence de génération de rapport et créez un profil de messagerie vers lequel le rapport est exporté.

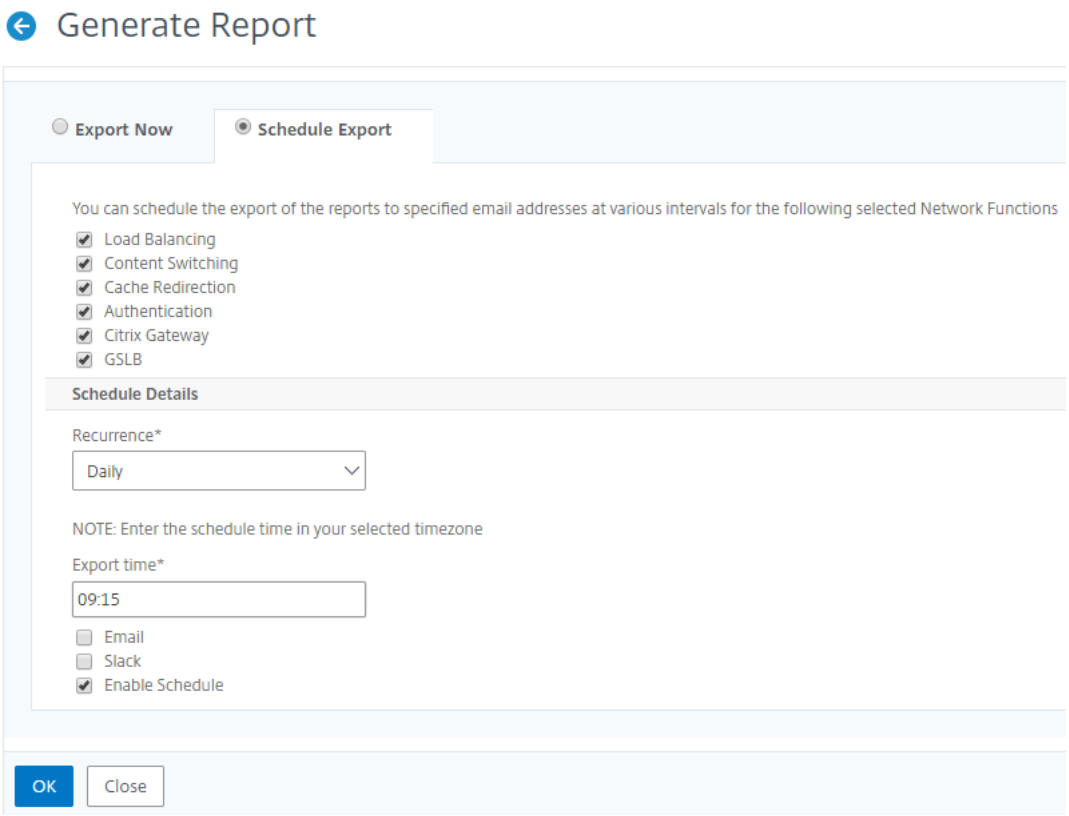
   i. **Récurrence** : sélectionnez **Quotidien**, **Hebdomadaire** ou **Mensuel** dans la zone de liste déroulante.

   ii. **Temps de récurrence** - Entrez l'heure dans le format Heure : Minute au format 24 heures.

   iii. **E-mail** - Activez la case à cocher, puis sélectionnez le profil dans la zone de liste déroulante, ou cliquez sur **Ajouter** pour créer un profil de messagerie.

   iv. **Slack** - Activez la case à cocher, puis sélectionnez le profil dans la zone de liste déroulante, ou cliquez sur **Ajouter** pour créer un profil de messagerie.

Cliquez sur **Activer la planification pour planifier** votre rapport, puis cliquez sur **OK**. En cochant la case **Activer la planification**, vous pouvez générer les rapports sélectionnés.



Rapports réseau

April 29, 2021

Vous pouvez optimiser l'utilisation des ressources en surveillant vos rapports réseau sur Citrix Application Delivery Management (Citrix ADM). Vous pouvez avoir 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 Citrix Application Delivery Controller (Citrix ADC) pour équilibrer la charge, basculer 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.

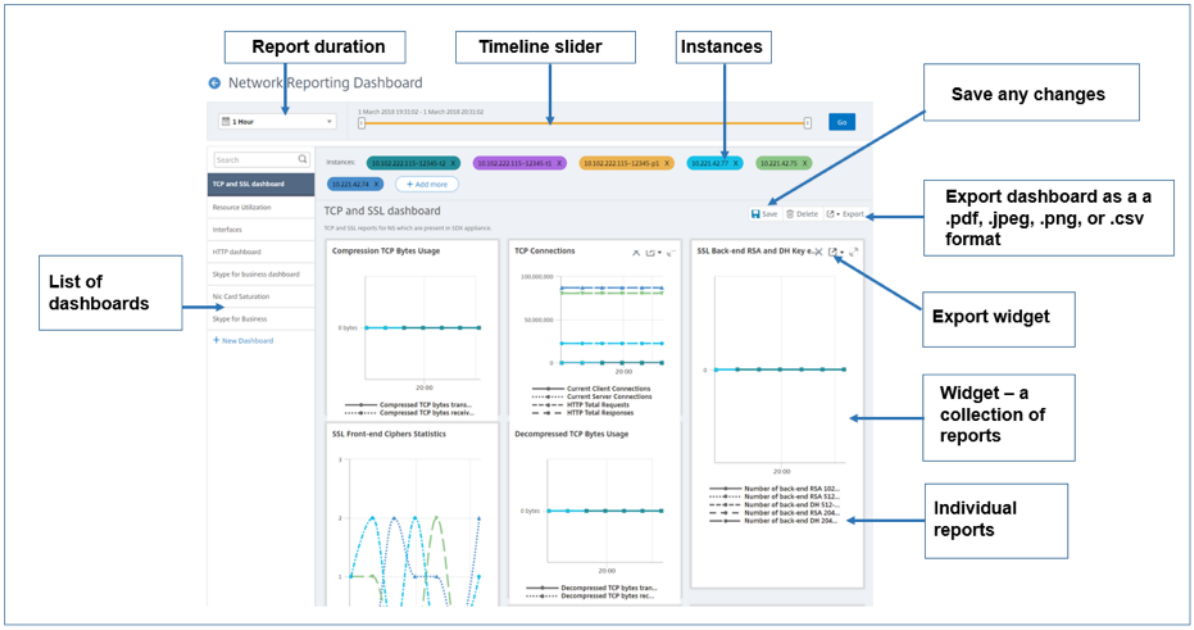
Citrix ADM vous permet de générer des rapports non seulement pour les instances au niveau global, mais aussi pour les entités telles que les serveurs virtuels et les interfaces réseau. La famille d'instances comprend les instances Citrix ADC et SD-WAN. Les serveurs virtuels pour lesquels vous pouvez générer des rapports sont les suivants :

- Serveurs, services et groupes de services d'équilibrage de charge
- Serveurs de commutation de contenu
- Serveurs de redirection de cache
- Équilibrage global de charge de service (GSLB)
- Authentification
- Citrix Gateway

Le tableau de bord de rapports réseau dans ADM est un tableau de bord hautement personnalisable. Vous pouvez créer plusieurs tableaux de bord pour différentes instances, serveurs virtuels et autres entités.

Tableau de bord de rapports réseau

L'image suivante appelle les différentes fonctionnalités du tableau de bord :



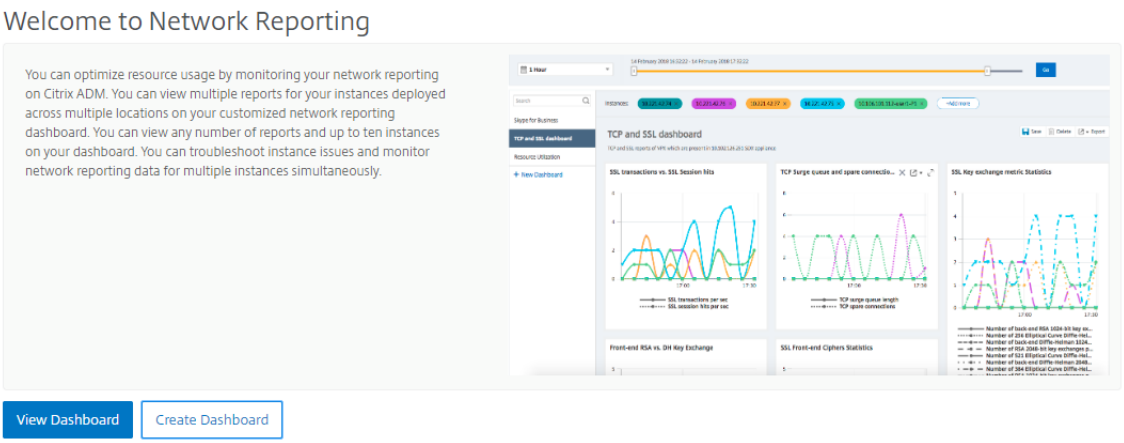
- Le panneau de gauche répertorie tous les tableaux de bord personnalisés créés dans Citrix ADM. Vous pouvez cliquer sur l'un d'eux pour afficher les différents rapports que le tableau de bord est composé. Par exemple, un tableau de bord TCP et SSL contient divers rapports liés aux protocoles TCP et SSL.
- Vous pouvez personnaliser chaque tableau de bord avec plusieurs widgets pour afficher différents rapports. Un widget représente un rapport sur le tableau de bord, c'est-à-dire une collection de rapports plus associés. Par exemple, un rapport d'utilisation des octets TCP de compression contient des rapports pour 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 de curseur de montage pour personnaliser la durée des rapports générés sur Citrix ADM.
- Vous pouvez supprimer un rapport en cliquant sur « X ». Vous pouvez également exporter le rapport au format .pdf, .jpeg, .png ou .csv vers votre système. Vous pouvez également planifier l'heure et la récurrence du moment où générer le rapport. Vous pouvez également configurer une liste de distribution de courrier électronique à laquelle vous souhaitez envoyer les rapports.
- La section Instances en haut du tableau de bord répertorie les adresses IP de toutes les instances pour lesquelles le rapport est généré.
- Vous pouvez supprimer des instances en cliquant sur « X » ou ajouter d'autres instances aux rapports. Toutefois, Citrix ADM vous permet actuellement d'afficher des rapports pour 10 instances.
- Vous pouvez également exporter l'intégralité du tableau de bord au format .pdf, .jpeg, .png ou .csv vers votre système. Toute modification apportée au tableau de bord doit être enregistrée. Cliquez sur Enregistrer pour enregistrer vos modifications.

La section suivante explique en détail les tâches pour créer un tableau de bord, générer des rapports

et exporter des rapports.

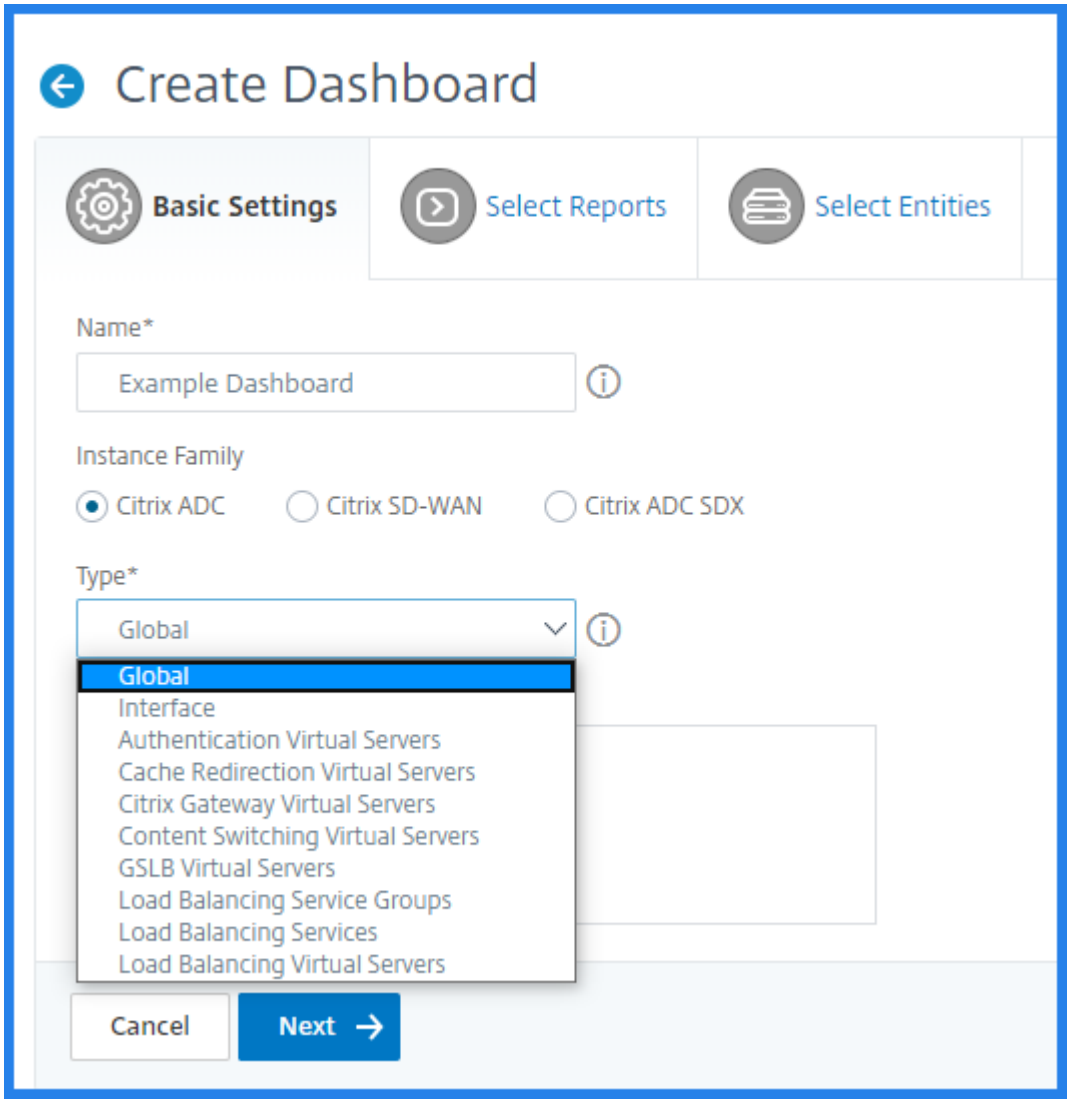
Pour afficher ou créer un tableau de bord :

1. Dans Citrix ADM, accédez à **Réseaux** > **Network Reporting**.

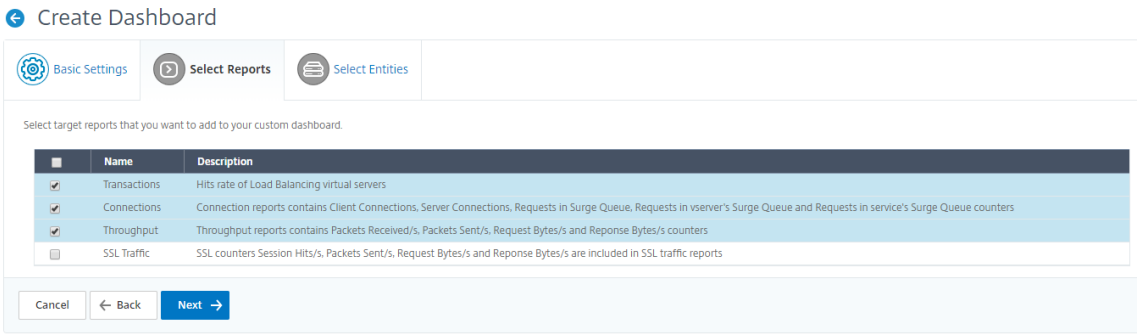


2. Pour afficher les tableaux de bord existants, cliquez sur **Afficher le tableau de bord**. La page **Tableau de bord** Network Reporting s'ouvre et vous permet d'afficher tous vos tableaux de bord et widgets de rapport.
3. Pour créer un tableau de bord, cliquez sur **Créer un tableau de bord**.

   La page **Créer un tableau de bord** s'ouvre.



4. Dans l'onglet **Paramètres de base**, entrez les détails suivants :
   a) **Nom**. Tapez le nom du tableau de bord.
   b) **Famille d'instances**. Sélectionnez le type d'instance - Citrix ADC, Citrix SD-WAN ou Citrix ADC SDX.
   c) **Type**. Sélectionnez le type d'entité pour lequel vous souhaitez générer des rapports. Dans cet exemple, sélectionnez des serveurs virtuels d'équilibrage de charge.
   d) **Description**. Tapez une description significative pour le tableau de bord.
5. Cliquez sur **Suivant**.
6. Dans l'onglet **Sélectionner des rapports**, sélectionnez les rapports requis. Dans cet exemple, vous pouvez sélectionner des transactions, des connexions et du débit. Cliquez sur **Suivant**.



7. Dans l'onglet **Sélectionner les entités**, cliquez sur **Ajouter** .

   Une fenêtre apparaît avec la liste des entités en fonction du type d'entité sélectionné dans l'onglet **Paramètres de base**. Dans cet exemple, la fenêtre **Choisir des serveurs virtuels LB** apparaît.

8. Sélectionnez les entités que vous souhaitez surveiller.

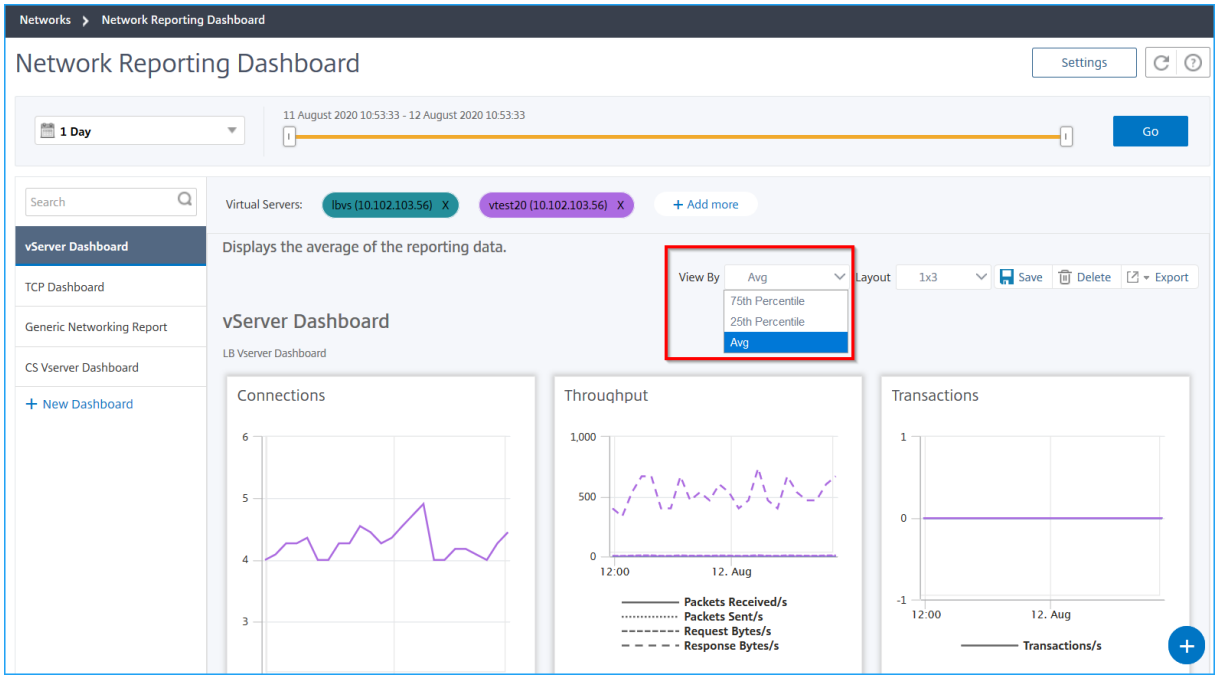
9. Cliquez sur **Créer**.

Le tableau de bord est créé et affiche tous les rapports que vous avez sélectionnés.

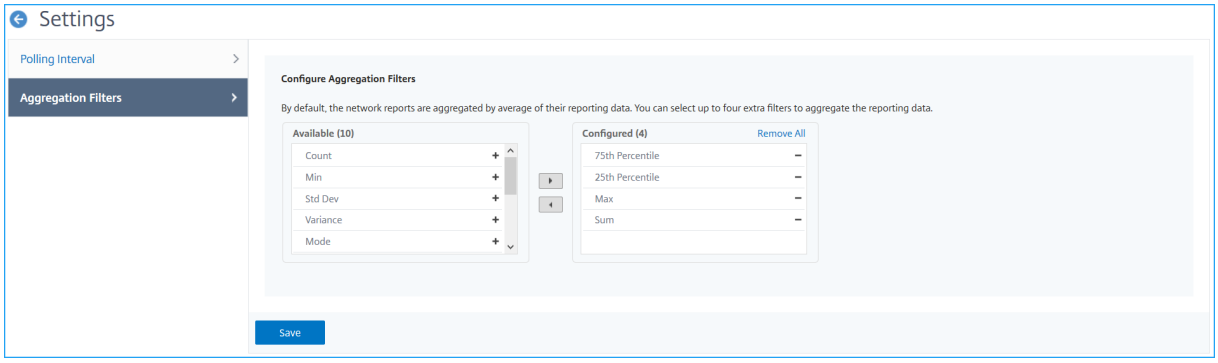
> **Remarque**
>
> Actuellement, les modifications que vous apportez aux légendes ou aux filtres ne peuvent pas être enregistrées.

Afficher les données de reporting réseau en appliquant des agrégations

Vous pouvez appliquer des agrégations aux données de performances réseau et afficher les performances des applications sur le tableau de bord. Vous pouvez également exporter les résultats en fonction de vos besoins. En utilisant ces agrégations appliquées aux données, vous pouvez analyser et vérifier si toutes les ressources sont utilisées de manière optimale. Accédez à **Réseau > Rapports réseau** et sélectionnez la durée d'un jour ou plus tard pour obtenir l'option **Afficher par**.



Dans les données moyennes existantes, vous pouvez appliquer des agrégations en sélectionnant l'option dans la liste **Voir par**. Lorsque vous appliquez l'agrégation, les données sont mises à jour pour chaque mesure du tableau de bord. Cliquez sur **Paramètres**, puis sélectionnez **Filtres d'agrégation**.



Les agrégations que vous pouvez ajouter sont les suivantes :

- Nombre
- Max

- Min
- Somme
- Dev Std
- Variance
- Mode
- Médiane
- 25e centile
- 75e centile
- 95e centile
- 99e centile
- Premier
- Dernier

Vous pouvez ajouter jusqu'à 4 options d'agrégation au tableau de bord. Après avoir ajouté les options d'agrégation, Citrix ADM prend environ 1 heure pour générer des rapports pour les options d'agrégation sélectionnées.

Exportation de rapports réseau

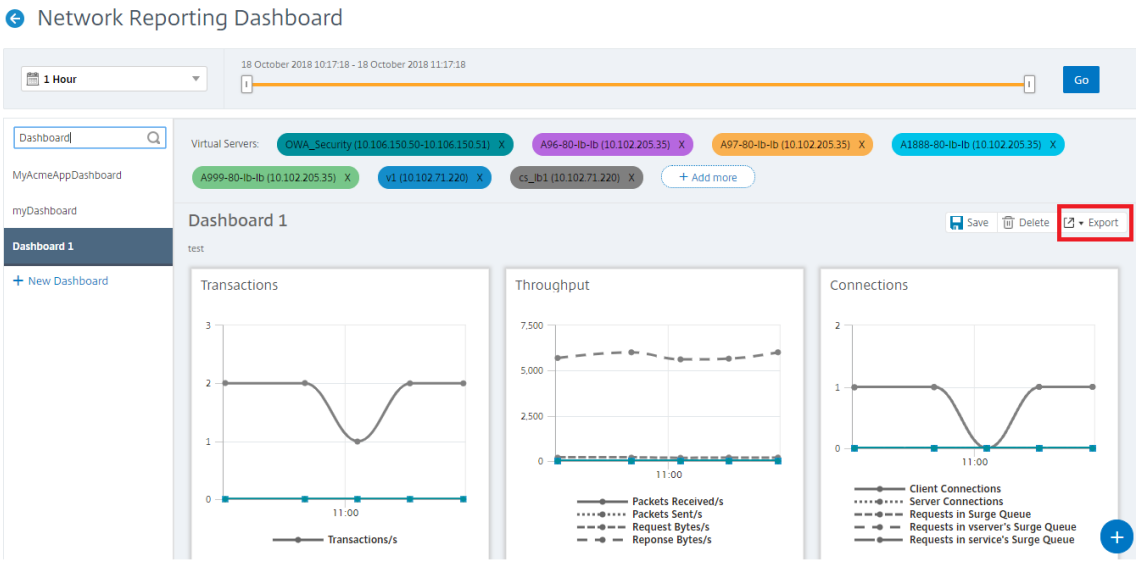
Bien que vous puissiez exporter des rapports de widget dans les formats .pdf, .png, .jpeg ou .csv, vous pouvez exporter l'intégralité des tableaux de bord uniquement dans les formats .pdf, .jpeg ou .png.

> **Remarque**
>
> Vous ne pouvez pas exporter les 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 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 situé dans le coin supérieur droit de la page.

5. Sous l'onglet **Exporter maintenant**, sélectionnez le format requis, puis cliquez sur **Exporter**.



Sur la page **Exporter**, vous pouvez effectuer l'une des opérations suivantes :

6. Sélectionnez l'onglet **Exporter maintenant**. Pour afficher et enregistrer le rapport au format PDF, JPEG, PNG ou CSV.
7. Sélectionnez l'onglet **Planifier l'exportation**. Pour planifier le rapport tous les jours, hebdomadaires ou mensuels et envoyer le rapport par e-mail ou message de marge.

   Vous pouvez planifier une exportation récurrente de la page **Tableau de bord de rapports réseau**. Par exemple, vous pouvez définir une option permettant de générer un rapport de tableau de bord chaque semaine pour l'heure précédente à un moment donné. Le rapport est alors généré chaque semaine et affiche l'état du tableau de bord. Le rapport remplace l'horodatage et l'horodatage, s'il est défini par l'utilisateur.

> **Remarque**
>
> - si vous sélectionnez Périodicité hebdomadaire, veillez à sélectionner les jours de semaine sur 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.

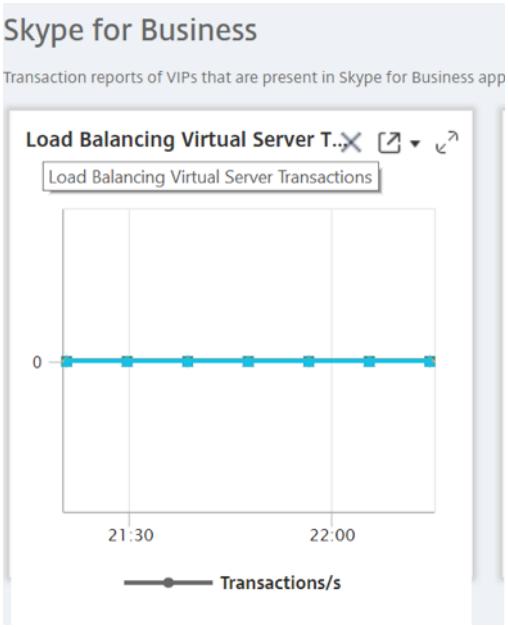
Lors de la planification des rapports réseau, vous pouvez personnaliser l'en-tête du rapport en saisissant une chaîne de texte dans le champ **Objet**. Le rapport créé à l'heure planifiée a cette chaîne comme nom.

Par exemple, pour les rapports réseau provenant d'un serveur virtuel particulier, vous pouvez taper le sujet comme « authentication-reports-10.106.118.120 », où 10.106.118.120 est l'adresse IP du serveur virtuel surveillé.

> **Remarque**
>
> Actuellement, cette option n'est disponible que lorsque vous planifiez l'exportation des rapports. Vous ne pouvez pas ajouter d'en-tête au rapport lorsque vous les exportez instantanément.

Pour exporter des rapports de widget :

1. Accédez à **Réseaux** > **Rapports réseau**.
2. Cliquez sur **Afficher les tableaux de bord** pour afficher tous les tableaux de bord que vous avez créés.
3. Dans le volet gauche, cliquez sur un tableau de bord. Dans cet exemple, cliquez également sur **Skype for Business**.
4. Sélectionnez un widget. Par exemple, sélectionnez **Load Balancing Virtual Server Transactions**.
5. Cliquez sur le bouton d'exportation en haut à droite 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 de 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 Connexions d'un serveur virtuel de commutation de contenu atteint une valeur spécifiée. Vous pouvez définir un seuil

pour un type d'instance spécifique. Vous pouvez également choisir les rapports que vous souhaitez générer pour des mesures de compteur spécifiques à partir de l'instance choisie.

Lorsque la valeur d'un compteur dépasse ou tombe en dessous (comme spécifié par la règle) la valeur de seuil, un événement de la gravité spécifiée est généré pour signifier 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 en fonction de leur 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 dépassement du seuil.

Pour créer un seuil :

1. Dans Citrix ADM, accédez à **Réseaux > Rapports réseau > Seuils**. Sous **Seuils**, cliquez sur **Ajouter**.
2. Dans la page **Créer un seuil**, spécifiez les détails suivants :
   - **Nom**. Nom du seuil.
   - **Type d'instance**. Choisissez Citrix ADC ou Citrix SD-WAN WO.
   - **Nom du rapport**. Nom du rapport de performances qui fournit des informations sur ce seuil.
3. Vous pouvez également définir des règles pour spécifier quand un événement doit être généré ou effacé. Vous pouvez spécifier les détails suivants dans la section **Configurer la règle** :
   - **Métrique**. Sélectionnez la mesure pour laquelle vous souhaitez définir un seuil.
   - **Comparateur**. Sélectionnez un comparateur pour vérifier si la valeur surveillée est supérieure ou égale à ou inférieure à la valeur seuil.
   - **Valeur de seuil**. Tapez la valeur pour laquelle la gravité de l'événement est calculée. Par exemple, vous pouvez générer un événement dont la gravité est 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 en fonction de leur gravité.
   - **Effacer la valeur**. Tapez la valeur qui indique quand la valeur doit être effacée. Par exemple, vous pouvez supprimer le seuil Connexions client actuelles lorsque la valeur surveillée atteint 50 %. Dans ce cas, tapez 50 comme valeur claire.
   - **Gravité de l'événement**. Sélectionnez le niveau de sécurité que vous souhaitez définir pour la valeur de seuil.
4. Choisissez l'adresse IP de la ou des instances pour lesquelles vous souhaitez définir le seuil.
5. Vous pouvez également ajouter un **message d'événement**. Tapez un message que vous

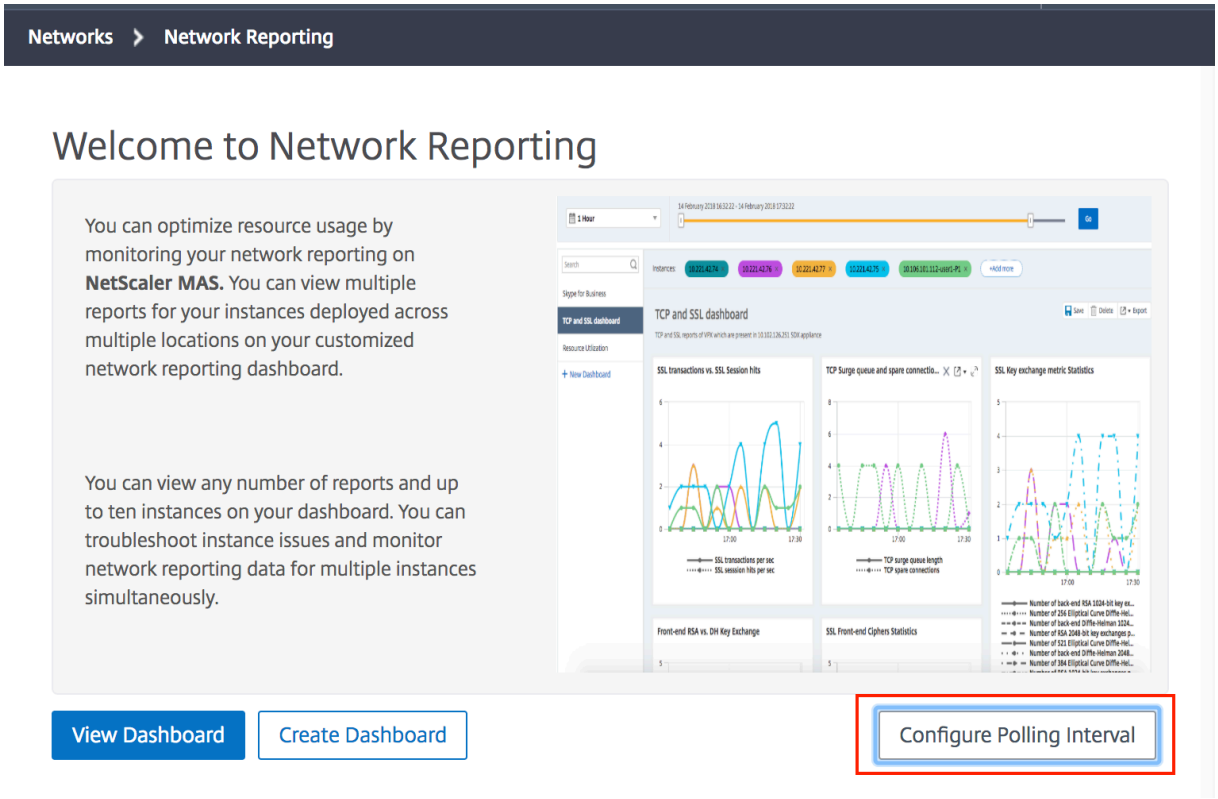
souhaitez afficher lorsque le seuil est atteint. Citrix ADM ajoute la valeur surveillée et la valeur de seuil à ce message.

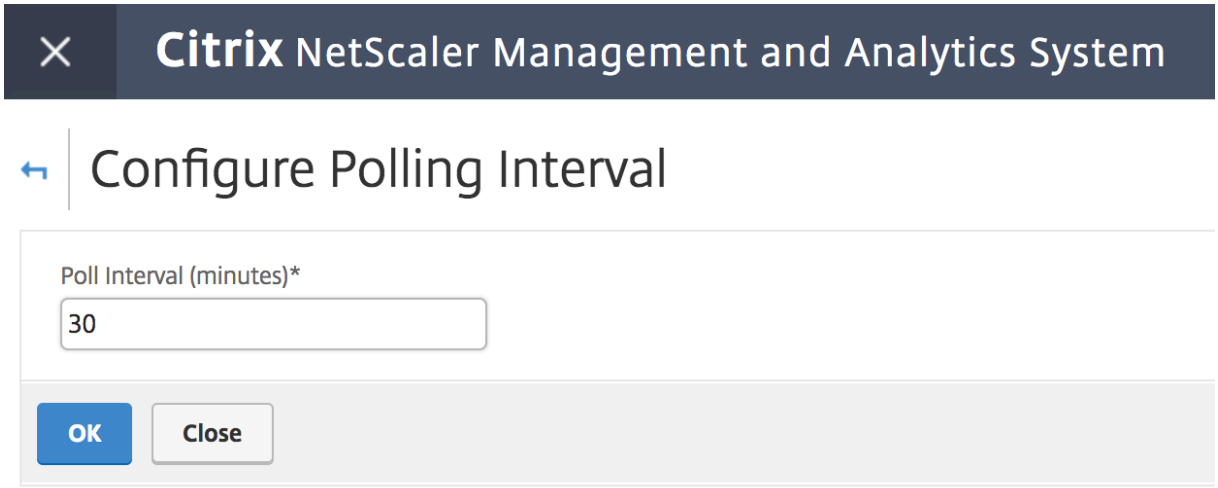
6. Sélectionnez **Activer** pour activer le seuil pour générer des alarmes.
7. Vous pouvez également configurer des **actions** telles que les notifications par e-mail ou Slack.
8. Cliquez sur **Créer**.

Définir l'intervalle d'interrogation des performances pour les rapports réseau

Par défaut, toutes les 5 minutes, les appels NITRO recueillent des données de performances pour les rapports réseau. L'ADM récupère les statistiques d'instance telles que les informations de compteur et les regroupe en fonction de la minute, de l'heure, du jour ou de la semaine. Vous pouvez afficher ces données agrégées dans des rapports prédéfinis.

Pour définir l'intervalle d'interrogation des performances, accédez à **Réseaux** > **Rapports réseau, puis** cliquez sur **Configurer l'intervalle d'interrogation** . Votre intervalle de scrutin ne peut pas être inférieur à 5 minutes ou supérieur à 60 minutes.





Configuration des paramètres de nettoyage des rapports réseau

Vous pouvez configurer l'intervalle de purge des données de rapport réseau dans Citrix ADM. Cet intervalle 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 ou être inférieure à 1 jour.

Orchestration

December 17, 2019

Gérer la configuration de Kubernetes Ingress dans Citrix ADM

April 29, 2021

Kubernetes (K8s) est une plate-forme d'orchestration de conteneurs open source qui automatise le déploiement, la mise à l'échelle et la gestion des applications natives du cloud.

Kubernetes fournit la fonctionnalité Ingress qui permet au trafic client en dehors du cluster d'accéder aux microservices d'une application exécutée à l'intérieur du cluster Kubernetes. Les instances ADC peuvent agir comme entrée pour les applications s'exécutant à l'intérieur d'un cluster Kubernetes.

Les instances ADC peuvent équilibrer la charge et acheminer le trafic Nord-Sud depuis les clients vers n'importe quel microservice à l'intérieur du cluster Kubernetes.

> **Remarque**
>
> - Citrix ADM prend en charge la fonctionnalité Ingress sur les clusters avec Kubernetes version 1.14 et versions ultérieures.
> - Citrix ADM prend en charge les appliances Citrix ADC VPX et MPX en tant que périphériques d'entrée.
> - Dans un environnement Kubernetes, la charge de l'instance Citrix ADC équilibre uniquement le type de service « NodePort ».

Vous pouvez configurer plusieurs instances ADC pour qu'elles agissent en tant que périphériques d'entrée sur le même cluster ou sur différents clusters ou espaces de noms. Après avoir configuré les instances, vous pouvez affecter chaque instance à différentes applications en fonction de la stratégie Ingress.

Vous pouvez créer et déployer une configuration Ingress à l'aide de Kubernetes `kubectl` ou d'API. Vous pouvez également configurer et déployer une entrée à partir de Citrix ADM.

Vous pouvez spécifier les aspects suivants de l'intégration de Kubernetes dans ADM :

- **Cluster** : vous pouvez enregistrer ou annuler l'inscription de clusters Kubernetes pour lesquels ADM peut déployer des configurations d'entrée. Lorsque vous enregistrez un cluster dans Citrix ADM, spécifiez les informations du serveur d'API Kubernetes. Ensuite, sélectionnez un agent ADM qui peut atteindre le cluster Kubernetes et déployer les configurations d'entrée.
- **Stratégies** : les stratégies d'entrée permettent de sélectionner l'instance ADC en fonction du cluster ou de l'espace de noms pour déployer une configuration d'entrée. Spécifiez les informations de cluster, de site et d'instance lorsque vous ajoutez une stratégie.
- **Configuration d'entrée** — Cette configuration est la configuration de Kubernetes Ingress, qui inclut les règles de commutation de contenu et les chemins d'URL correspondants des microservices et de leurs ports. Vous pouvez également spécifier les certificats SSL/TLS (pour décharger le traitement SSL sur l'instance ADC) à l'aide des ressources secrètes Kubernetes.

Citrix ADM mappe automatiquement les configurations d'entrée aux instances ADC à l'aide des stratégies d'entrée.

Pour chaque configuration d'entrée réussie, Citrix ADM génère un StyleBook ConfigPack. Le ConfigPack représente la configuration ADC appliquée à l'instance ADC qui correspond à la configuration d'entrée. Pour afficher le ConfigPack, accédez à **Applications > StyleBooks > Configurations**.

Avant de commencer

Pour utiliser des instances Citrix ADC en tant que périphériques d'entrée sur les clusters Kubernetes, assurez-vous que vous disposez des éléments suivants :

- Cluster Kubernetes en place.
- Agent Citrix ADM installé et configuré pour activer la communication entre ADM et le cluster Kubernetes ou les instances gérées. Vous pouvez utiliser les instances gérées présentes dans votre datacenter ou votre nuage.
- Cluster Kubernetes enregistré dans Citrix ADM.

Configurer l'agent Citrix ADM pour qu'il s'enregistre auprès du cluster Kubernetes

Pour activer la communication entre le cluster Kubernetes et Citrix ADM, vous devez installer et configurer un agent Citrix ADM. Vous pouvez déployer un agent sur les plates-formes suivantes :

- Hyperviseur (ESX, XenServer, KVM, Hyper-V)
- Services de cloud public (tels que Microsoft Azure, AWS)

Suivez laprocédurepour configurer un agent.

> **Remarque**
>
> Vous pouvez également utiliser un agent ADM existant si un agent est déjà déployé.

Configurer Citrix ADM avec un jeton secret pour gérer un cluster Kubernetes

Pour que Citrix ADM puisse recevoir des événements de Kubernetes, vous devez créer un compte de service dans Kubernetes pour Citrix ADM. Et, configurez le compte de service avec les autorisations RBAC nécessaires dans le cluster.

1. Créez un compte de service pour Citrix ADM. Par exemple, le nom du compte de service peut êtrecitrixadm-sa. Pour créer un compte de service, reportez-vous à la sectionUtiliser plusieurs comptes de service.
2. Utilisez le rôle cluster-admin pour lier le compte de service Citrix ADM. Cette liaison accorde un ClusterRole à travers le cluster à un compte de service. Voici un exemple de commande pour lier uncluster-admin rôle au compte de service.

```
kubectl create clusterrolebinding citrixadm-sa-admin --clusterrole
   =cluster-admin --serviceaccount=default:citrixadm-sa
<!--NeedCopy-->
```


Après avoir lié le compte de service Citrix ADM au rôle, `cluster-admin`le compte de service dispose de l'accès à l'échelle du cluster. Pour plus d'informations, consultez [`kubectl` create `clusterrolebinding`] (https://kubernetes.io/docs/reference/access-authn-authz/rbac/#kubectl-create-clusterrolebinding).

3. Obtenez le jeton à partir du compte de service créé.

   Par exemple, exécutez la commande suivante pour afficher le jeton du compte`citrixadm-sa` de service :

   ```
   kubectl describe sa citrixadm-sa
   <!--NeedCopy-->
   ```

4. Exécutez la commande suivante pour obtenir la chaîne secrète du jeton :

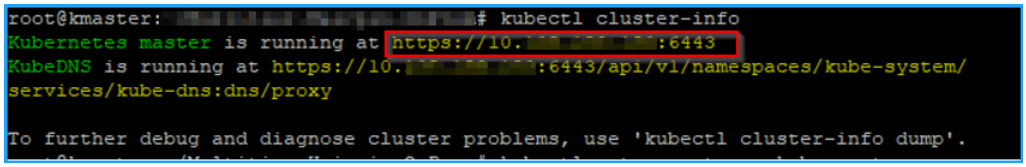
   ```
   kubectl describe secret <token-name>
   <!--NeedCopy-->
   ```

Ajouter le cluster Kubernetes dans Citrix ADM

Après avoir configuré un agent Citrix ADM et configuré des itinéraires statiques, vous devez enregistrer le cluster Kubernetes dans Citrix ADM.

Pour enregistrer le cluster Kubernetes :

1. Connectez-vous à Citrix ADM avec les informations d'identification de l'administrateur.
2. Accédez à **Orchestration** > **Kubernetes** > **Cluster** .
   La page Clusters s'affiche.
3. Cliquez sur **Ajouter**.
4. Dans la page **Ajouter un cluster**, spécifiez les paramètres suivants :
   a) **Nom** - Indiquez le nom de votre choix.
   b) **API Server URL** - Vous pouvez obtenir les détails de l'URL API Server à partir du nœud Master Kubernetes.
      i. Sur le nœud maître Kubernetes, exécutez la commande`kubectl cluster-info`.

      ii. Entrez l'URL qui s'affiche pour **"Kubernetes master est en cours d'exécution à."**

c) **Authentication Token** - Spécifiez la chaîne de jeton d'authentification obtenue pendant que vous configurer Citrix ADM pour gérer un cluster Kubernetes. Le jeton d'authentification est requis pour valider l'accès pour la communication entre le cluster Kubernetes et Citrix ADM. Pour générer un jeton d'authentification :

i. Sur le nœud maître Kubernetes, exécutez les commandes suivantes :

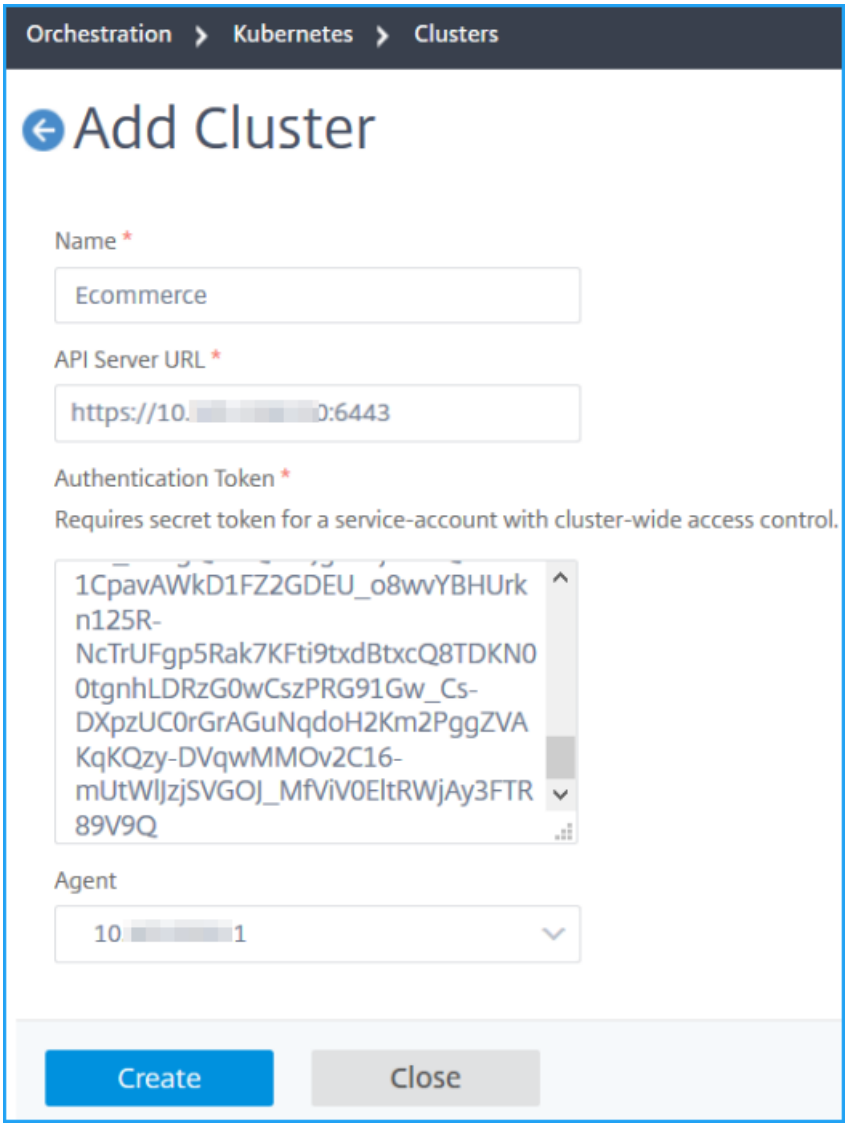
```
kubectl describe secret <token-name>
<!--NeedCopy-->
```

ii. Copiez le jeton généré et collez-le en tant que jeton d'authentification

Pour de plus amples informations, consultez la documentation de Kubernetes.

d) Sélectionnez l'agent dans la liste.

e) Cliquez sur **Créer**.



Définir une stratégie d'entrée

La stratégie d'entrée détermine quel Citrix ADC est utilisé pour déployer une configuration d'entrée, basée sur le cluster d'entrée ou l'espace de noms, ou les deux.

1. Accédez à **Orchestration > Kubernetes > Stratégie**.
2. Cliquez sur **Ajouter** pour créer une stratégie.
    a) Spécifiez le nom de la stratégie.
    b) Définissez **des conditions** pour déployer la configuration Ingress sur un cluster Kubernetes. Ces conditions sont généralement basées sur Ingress Cluster et Namespace.
    c) Dans le cadre du groupe Infrastructure,
        - **Site** - Sélectionnez un site dans la liste.
        - **Instance** - Sélectionnez l'instance ADC dans la liste.

        Les listes **Site** et **Instance** renseignent les options en fonction de la sélection du cluster dans le panneau **Conditions** .

        Ces listes affichent les sites ou instances associés à l'agent Citrix ADM configuré avec le cluster Kubernetes.
    d) Dans **Choisir un réseau**, sélectionnez le réseau à partir duquel ADM attribue automatiquement les adresses IP virtuelles à une configuration d'entrée.

        Cette liste affiche les réseaux créés dans **Réseaux > IPAM**.
    e) Cliquez sur **Créer**.

Déployer la configuration d'entrée

Vous pouvez déployer la configuration Ingress à partir de Kubernetes à l'aide `kubectl`de l'API Kubernetes ou d'autres outils. Vous pouvez également déployer la configuration Ingress directement à partir de Citrix ADM.

1. Accédez à **Orchestration > Kubernetes > Ingresses**.
2. Cliquez sur **Ajouter**.
3. Dans le champ **Créer une entrée**, spécifiez les détails suivants :
    a) Spécifiez le nom de l'entrée.
    b) Dans **Cluster**, sélectionnez le cluster Kubernetes sur lequel vous souhaitez déployer une entrée.
    c) Sélectionnez l' **espace de noms de cluster** dans la liste. Ce champ répertorie les espaces de noms présents dans le cluster Kubernetes spécifié.

d) Facultatif, sélectionnez **Affecter automatiquement l'adresse IP frontend**.

e) Sélectionnez **Ingress Protocol** dans la liste. Si vous sélectionnez **HTTPS**, spécifiez **TLS secret**.

Ce secret intègre la ressource secrète Kubernetes qui intègre le certificat HTTPS et la clé privée.

Une entrée HTTPS nécessite un secret basé sur TLS configuré sur le cluster Kubernetes. Spécifiez les`tls.crt` champs`tls.key` et à inclure respectivement le certificat de serveur et la clé de certificat.

f) Pour le routage de contenu, spécifiez les détails suivants :

- **URL path** : spécifiez le chemin d'accès associé au service et au port Kubernetes.
- **Service Kubernetes** - Spécifiez le service souhaité.
- **Port** : spécifiez le port de service.
- **Méthode LB** : sélectionnez la méthode d'équilibrage de charge préférée pour le service Kubernetes sélectionné.

  La méthode sélectionnée met à jour la spécification d'entrée avec une annotation appropriée. Par exemple, si vous sélectionnez la méthode **ROUNDROBIN**, l'annotation Citrix apparaît comme suit :

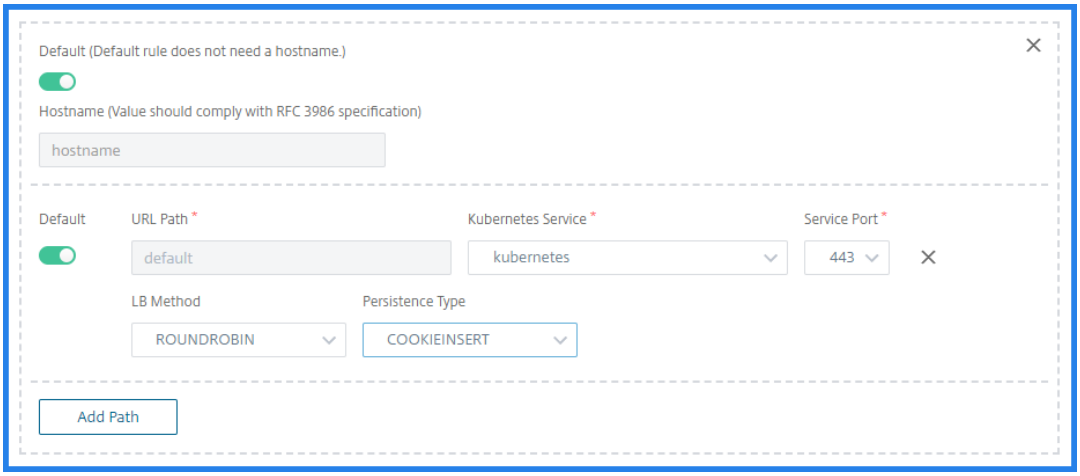
```
1  "lbmethod":"ROUNDROBIN"
2  <!--NeedCopy-->
```

- **Type de persistance** : sélectionnez le type de persistance d'équilibrage de charge préféré pour le service Kubernetes sélectionné.

  Le type de persistance sélectionné met à jour la spécification d'entrée avec une annotation appropriée. Par exemple, si vous sélectionnez **COOKIEINSERT**, l'annotation Citrix apparaît comme suit :

```
1  "persistenceType":"COOKIEINSERT"
2  <!--NeedCopy-->
```

Cliquez sur **Ajouter** pour ajouter d'autres chemins d'URL et ports à la configuration Ingress.



Après le déploiement, la configuration Ingress redirige le trafic client vers un service spécifique en fonction des éléments suivants :

- Le chemin d'accès et le port de l'URL demandés.
- Méthode LB définie et type de persistance.

> **Remarque Les**services
>
> Kubernetes utilisés dans une configuration d'entrée devraient être de type NodePort.

g) Facultatif, spécifiez une **description d'entrée**.

h) cliquez sur **Déployer**.

Si vous souhaitez vérifier la configuration avant de déployer, cliquez sur **Générer les spécifications d'entrée**. La configuration d'entrée spécifiée apparaît au format YAML. Après avoir examiné la configuration, cliquez sur **Déployer**.

> **Remarque**
> Appliquer des licences aux serveurs virtuels créés à l'aide des configurations d'entrée. Pour appliquer une licence, effectuez les opérations suivantes :
>
> 1. Accédez à **Système > Licences et analyses**.
> 2. Sous **Récapitulatif des licences du serveur virtuel**, activez la **sélection automatique des serveurs virtuels**.

Utiliser les journaux d'audit ADM pour gérer et surveiller votre infrastructure

April 29, 2021

Vous pouvez utiliser le service Citrix ADM pour suivre tous les événements sur les événements ADM et syslog générés sur les instances ADC gérées par ADM. Ces messages peuvent vous aider à gérer et surveiller votre infrastructure. Mais les messages de journal ne sont une excellente source d'information que si vous les examinez, et ADM simplifie la façon de consulter les messages de journal.

Vous pouvez utiliser des filtres pour rechercher les messages syslog d'ADM et du journal d'audit. Les filtres aident à affiner vos résultats et à trouver exactement ce que vous recherchez et en temps réel. L'aide intégrée à la recherche vous guide pour filtrer les journaux. Une autre façon d'afficher les messages du journal consiste à les exporter au format PDF, CSV, PNG et JPEG. Vous pouvez planifier l'exportation de ces rapports vers des adresses e-mail spécifiées à différents intervalles.

Vous pouvez consulter les types de messages de journal suivants à partir de l'interface graphique d'ADM :

- Journaux d'audit liés à une instance ADC
- Journaux de vérification liés à ADM
- Journaux d'audit des applications

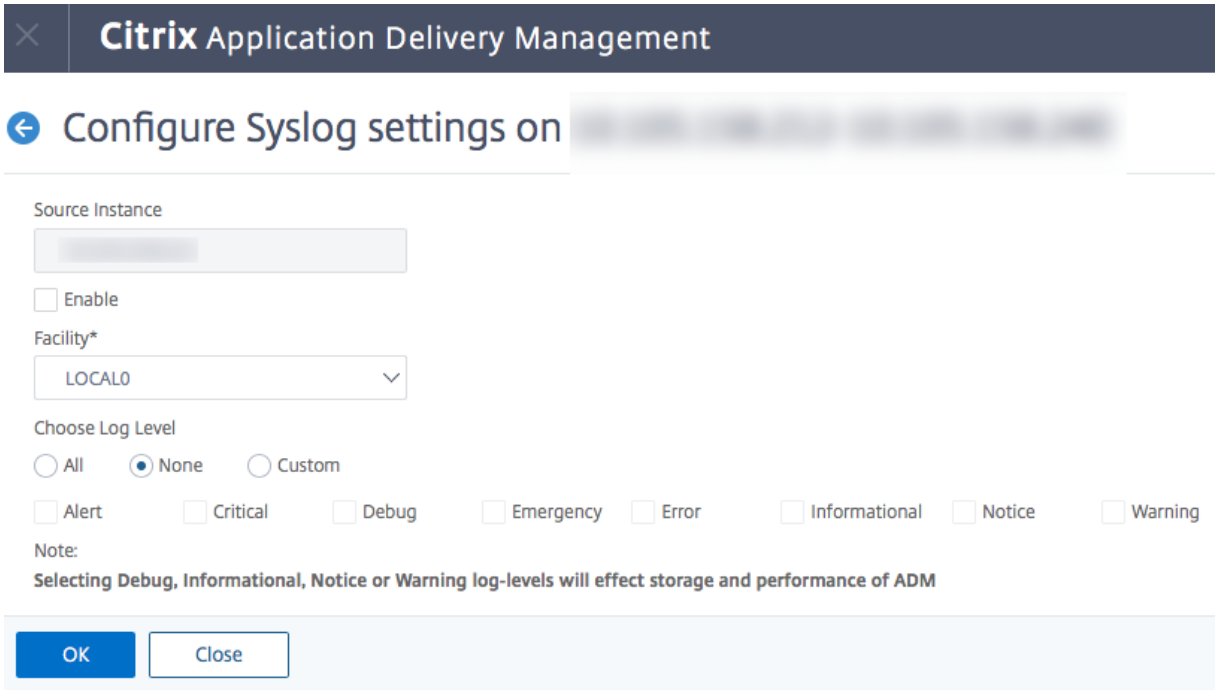
Journaux d'audit liés à une instance ADC

Avant de pouvoir afficher les messages syslog liés à une instance ADC à partir d'ADM, configurez le service Citrix ADM en tant que serveur syslog pour votre instance Citrix ADC. Une fois la configuration terminée, tous les messages syslog sont redirigés de l'instance vers ADM.

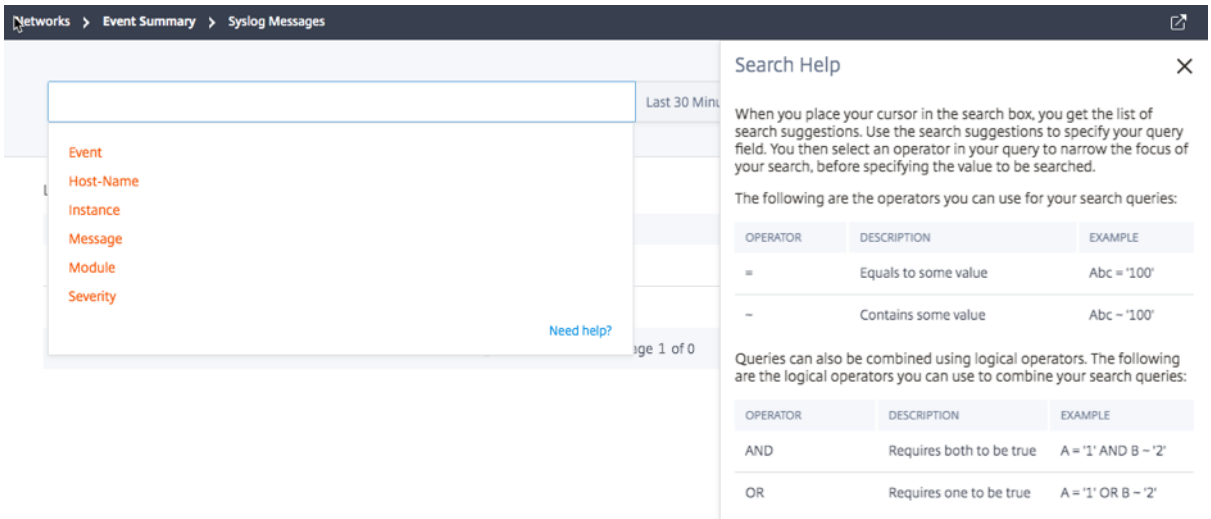
Configurer ADM en tant que serveur syslog

Procédez comme suit pour configurer ADM en tant que serveur syslog :

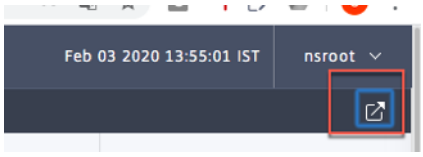
1. À partir de l'interface graphique ADM, accédez à **Réseaux > Instances**.
2. Sélectionnez l'instance Citrix ADC à partir de laquelle vous souhaitez que les messages syslog soient collectés et affichés dans Citrix ADM.
3. Dans la liste **Sélectionner une action**, sélectionnez **Configurer Syslog**.
4. Cliquez sur **Activer**.
5. Dans la liste déroulante **Facility**, sélectionnez une ressource locale ou de niveau utilisateur.
6. Sélectionnez le niveau de journal requis pour les messages syslog.
7. Cliquez sur **OK**.



Ces étapes configurent toutes les commandes syslog dans l'instance de Citrix ADC et Citrix ADM commence à recevoir les messages syslog. Vous pouvez afficher les messages en accédant à **Réseaux > Événements > Messages Syslog**. Cliquez sur **Besoin d'aide ?** pour ouvrir l'aide de recherche intégrée. Pour de plus amples informations, consultez la section Afficher et exporter les messages syslog.



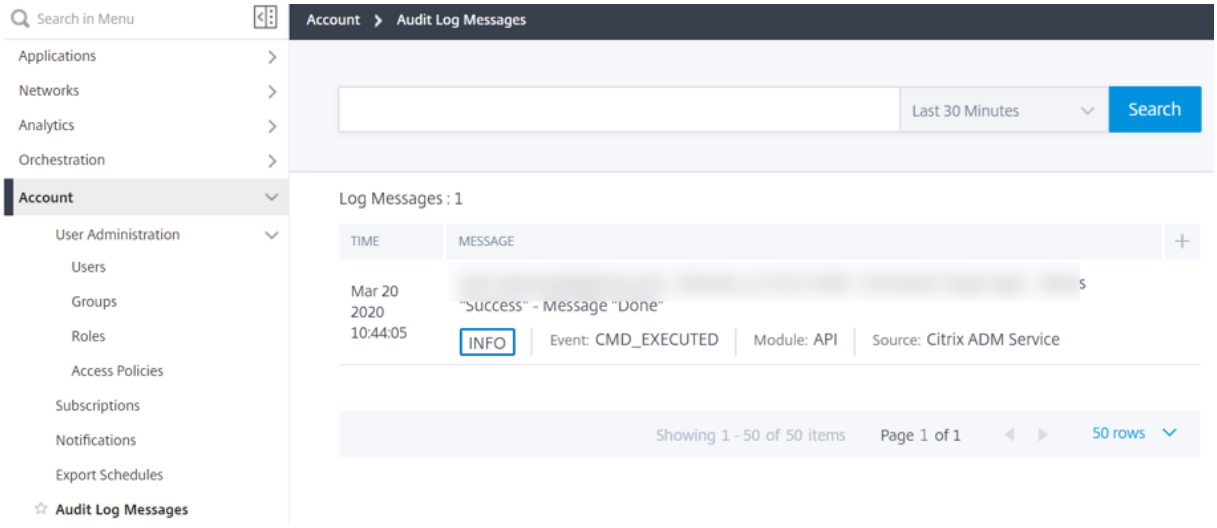
Pour exporter les messages du journal, cliquez sur l'icône en forme de flèche dans le coin supérieur droit.



Ensuite, cliquez sur **Exporter maintenant** ou **Planifier l'exportation**. Pour de plus amples informations, consultez la section Exporter les messages syslog.

Journaux de vérification liés à ADM

Sur la base de règles préconfigurées, ADM génère des messages de journal d'audit pour tous les événements sur, ce qui vous aide à surveiller l'intégrité de votre infrastructure. Pour afficher tous les messages du journal d'audit présents dans ADM, accédez à **Comptes->Messages du journal d'audit**.

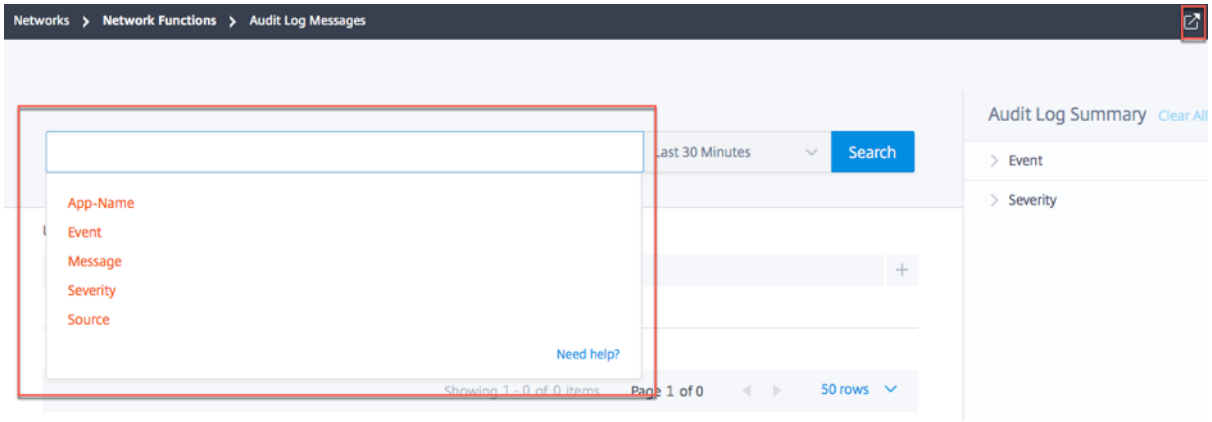


Pour exporter les messages du journal, cliquez sur l'icône en forme de flèche dans le coin supérieur droit.

Journaux d'audit liés aux applications

Vous pouvez afficher les messages du journal d'audit pour toutes les applications ADM ou pour une application spécifique.

- Pour afficher tous les messages du journal d'audit pour toutes les applications présentes dans ADM, accédez à **Réseaux > Fonctions réseau > Audit**.



- Pour afficher les messages du journal d'audit pour une application spécifique dans ADM, accédez à **Application > Tableau de bord > double-cliquez sur le serveur virtuel > Journal d'audit**.

> Remarque
>
> Vous pouvez transférer les messages du journal d'audit ADM à un serveur externe. Pour plus de détails, consultez la section Afficher les informations d'audit.

Analytics

April 29, 2021

L'analyse de Citrix Application and Delivery Management (ADM) fournit un moyen simple et évolutif d'examiner les différentes informations des données des instances Citrix ADC pour décrire, prédire et améliorer les performances de l'application. Vous pouvez utiliser simultanément une ou plusieurs fonctionnalités d'analyse sur Citrix ADM. Le tableau suivant décrit diverses fonctionnalités d'analyse prises en charge par Citrix ADM :

Fonctionnalités analytiques	Description
Web Insight	Web Insight permet 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.
Aperçu HDX	HDX Insight fournit une visibilité de bout en bout pour le trafic ICA passant par Citrix ADC. HDX Insight permet aux administrateurs d'afficher en temps réel les mesures de latence client et réseau, les rapports historiques, les données de performances de bout en bout et de résoudre les problèmes de performances.
Gateway Insight	Gateway Insight fournit une visibilité sur les échecs rencontrés par tous les utilisateurs, quel que soit le mode d'accès, au moment de la connexion à Citrix Gateway.

Fonctionnalités analytiques	Description
Security Insight	Security Insight fournit une solution à volet unique 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 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.

Conditions de licence

April 29, 2021

Les exigences de licence requises pour les instances ADC pour afficher les différents rapports d'analyse sur Citrix Application Delivery Management (ADM) sont décrites dans le tableau suivant :

Fonctionnalités de Citrix ADM Analytics	Exigence de licence ADC
Web Insight	Le rapport Web Insight sur Citrix ADM est pris en charge sur toutes les éditions de licences ADC (Standard/Advanced/Premium).
HDX Insight	Le rapport HDX Insight sur Citrix ADM est pris en charge sur l'une des licences ADC suivantes : Advanced Edition (pour les rapports < 1 heure) ou Premium Edition (pour les rapports illimités). **Remarque :** L'édition de licence standard n'est pas prise en charge.

Fonctionnalités de Citrix ADM Analytics	Exigence de licence ADC
Security Insight	Le rapport Security Insight sur Citrix ADM est pris en charge sur Premium Edition ou Advanced Edition avec une licence App Firewall. **Remarque :** l'édition de licence standard et la licence de pare-feu d'application autonome ne sont pas prises en charge.
SSL Insight	Le rapport SSL Insight sur Citrix ADM est pris en charge sur toutes les éditions de licences ADC (Standard/Advanced/Premium).
Gateway Insight	Le rapport Gateway Insight sur Citrix ADM est pris en charge sur l'une des licences ADC suivantes : Advanced Edition (pour les rapports < 1 heure) ou Premium Edition (pour les rapports illimités). **Remarque :** L'édition de licence standard n'est pas prise en charge.
TCP Insight	Le rapport TCP Insight est pris en charge sur toutes les éditions de licence ADC (Standard/Advanced/Premium).
Video Insight	Le rapport Video Insight sur Citrix ADM est pris en charge sur ADC Premium (ADC-T série 1000, VPX-T) édition.
WAN Insight	Le rapport WAN Insight sur Citrix ADM est pris en charge sur ADC SD-WAN WO Edition (WAN Optimization Edition).

Présentation de Logstream

April 29, 2021

Les instances de Citrix ADC génèrent des enregistrements AppFlow et constituent un point de contrôle central pour tout le trafic d'application dans le datacenter. **IPFIX** et **Logstream** sont les protocoles qui transportent ces enregistrements AppFlow à partir d'instances Citrix ADC vers Citrix ADM. Pour de plus amples informations, consultez la section AppFlow.

- **IPFIX** est une norme ouverte Internet Engineering Task Force (IETF) définie dans la RFC 5101. **IPFIX** utilise le protocole UDP qui n'est pas fiable protocole de transport utilisé pour le flux de

données dans une direction. Comme IPFIX utilise le protocole UDP, le respect de la norme IPFIX entraîne le traitement de plus de ressources dans Citrix ADM.

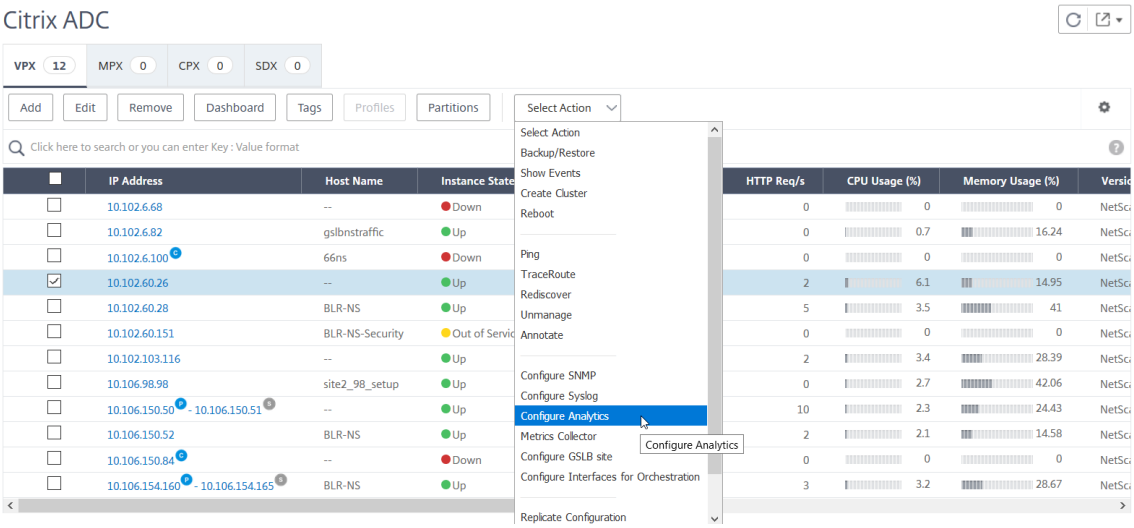
- **Logstream** est un protocole appartenant à Citrix qui est utilisé comme l'un des modes de transport pour transférer efficacement les données du journal d'analyse des instances Citrix ADC vers Citrix ADM. **Logstream** utilise un protocole TCP fiable et nécessite moins de ressources pour le traitement des données.

Pour Citrix ADC entre **11.1 Build 47.14 et 11.1 Build 62.8**, **Logstream** est le mode de transport par défaut pour activer Web Insight (HTTP) et IPFIX est le seul mode de transport permettant d'activer d'autres informations. Pour la version **12.0 à la dernière version** de Citrix ADC, vous pouvez sélectionner **Logstream**ou **IPFIX**comme mode de transport.

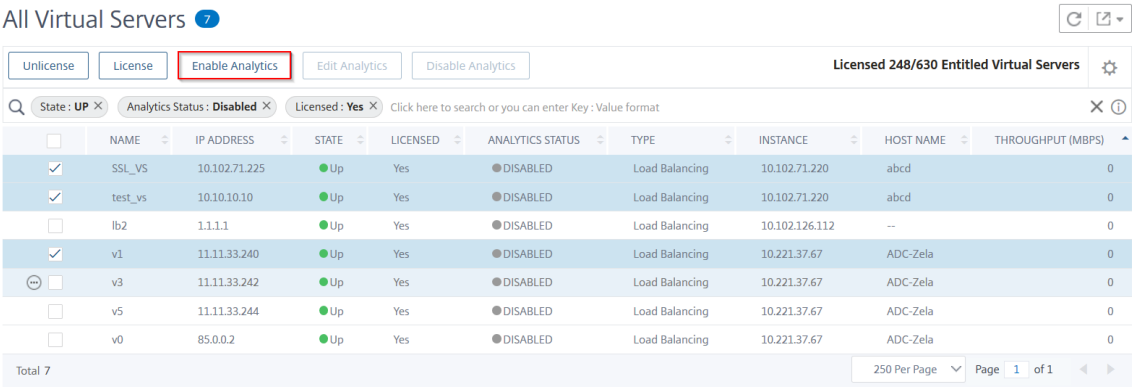
> **Remarque**
>
> La version et la version Citrix ADM doivent être **égales ou supérieures à** votre version Citrix ADC et version. Par exemple, si vous avez installé Citrix ADC 12.1 Build 50.28/50.31, assurez-vous d'avoir installé Citrix ADM 12.1 Build 50.39 ou version ultérieure.

Activer Logstream en mode de transport

1. Accédez à **Réseaux** > **Instances**, puis sélectionnez l'instance ADC que vous souhaitez activer l'analyse.
2. Dans la liste **Sélectionner une action**, sélectionnez **Configurer Analytics**.



3. Sélectionnez les serveurs virtuels, puis cliquez sur **Activer Analytics**.



4. Dans la fenêtre **Activer Analytics** :

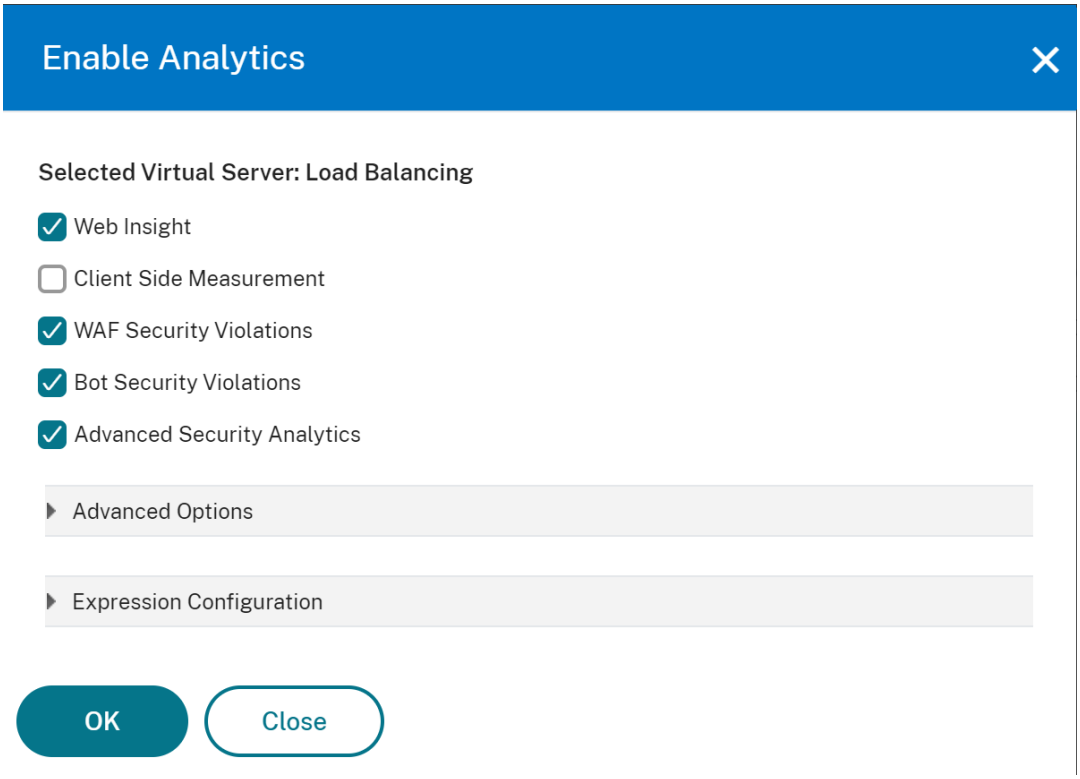
   a) Sélectionnez les types d'informations (Web Insight ou Security Insight)

   b) Sélectionnez **Logstream** comme mode de transport

   > **Remarque**
   >
   > Pour Citrix ADC entre **11.1 Build 47.14 et 11.1 Build 62.8**, **Logstream** est le mode de transport par défaut pour activer Web Insight (HTTP) et IPFIX est le seul mode de transport permettant d'activer d'autres informations. Pour la version **12.0 à la dernière version** de Citrix ADC, vous pouvez sélectionner **Logstream**ou **IPFIX**comme mode de transport.

   c) L'expression est true par défaut

   d) Cliquez sur **OK**.



Remarque

```
- Si vous sélectionnez des serveurs virtuels qui ne sont pas sous licence, Citrix ADM concéde d'abord ces serveurs virtuels, puis active l'analyse

- Pour les partitions d'administration, seul **Web Insight** est pris en charge

- Pour les serveurs virtuels tels que la redirection de cache, l'authentificationet GSLB, vous ne pouvez pas activer l'analyse. Un message d'erreur s'affiche.
```

Le tableau suivant décrit les fonctionnalités de Citrix ADM qui prend en charge **Logstream en** tant que mode de transport :

Fonctionnalité	**IPFIX**	**Logstream**
Web Insight	•	•
Security Insight	•	•
Gateway Insight	•	•

Fonctionnalité	**IPFIX**	**Logstream**
HDX Insight	•	•
SSL Insight	Non pris en charge	•
CR Insight	•	•
Réputation IP	•	•
AppFirewall	•	•
Mesure côté client	•	•
Syslog/Auditlog	•	•

Diagnostics en libre-service pour l'analyse

April 29, 2021

Citrix 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
- Bot Insight
- Analyses de proxy de transfert SSL

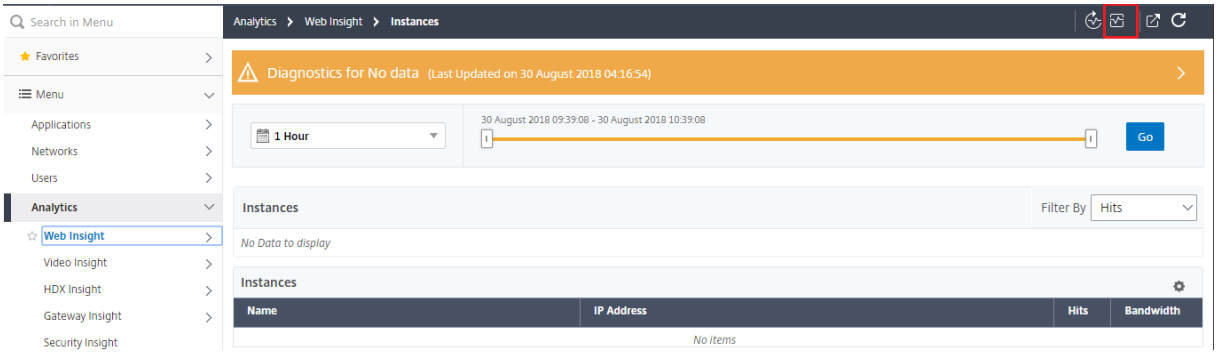
Les diagnostics en libre-service s'exécutent toutes les 12 heures et génèrent un rapport de diagnostic si des problèmes sont détectés pour chacune des fonctionnalités d'analyse spécifiées. Le rapport de diagnostic fournit les sources des problèmes, les types de problèmes et les mesures correctives à prendre pour résoudre les problèmes. 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. Les diagnostics en libre-service identifient les problèmes et génèrent un rapport de diagnostic. Vous pouvez consulter le rapport de diagnostic pour vérifier les problèmes et effectuer les actions correctives.

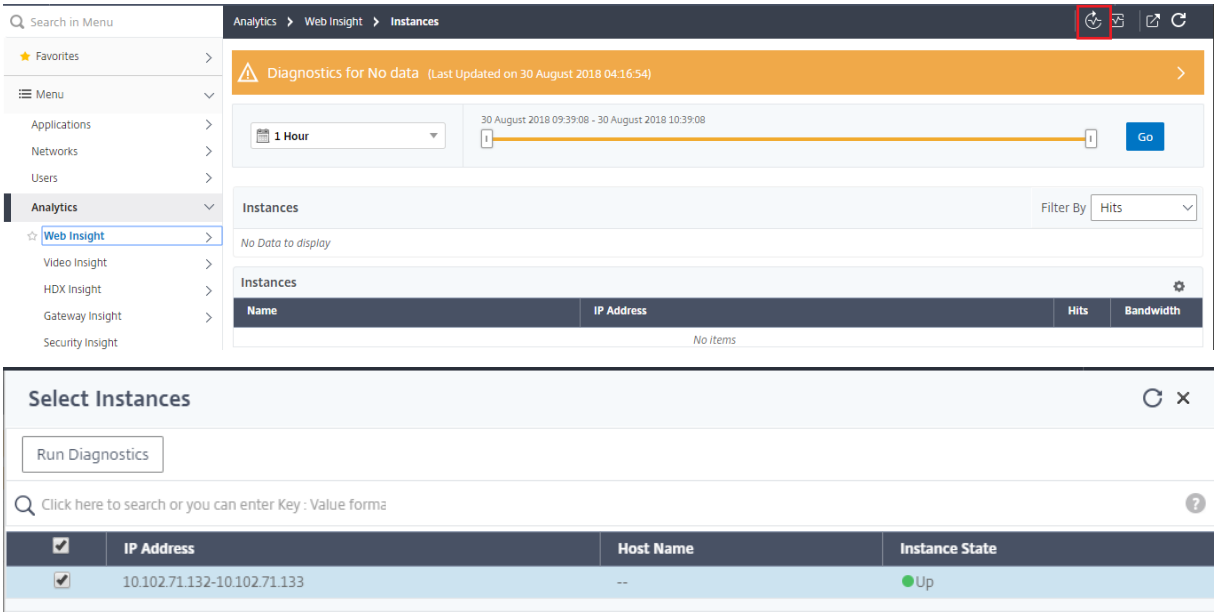
Voir le rapport de diagnostic

Pour afficher les rapports de diagnostic pour les fonctionnalités d'analyse spécifiées, accédez au mode d'analyse correspondant dans le tableau de bord 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**.



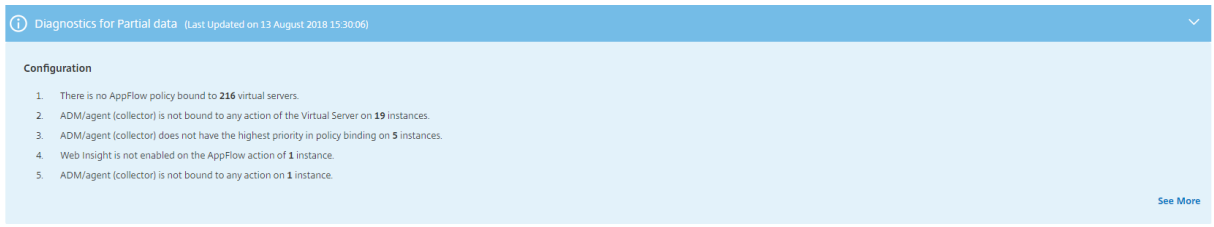
Analyser le rapport de diagnostic

Les diagnostics en libre-service affichent le rapport de diagnostic en arrière-plan orange ou bleu en fonction de la criticité des problèmes.

Le rapport de diagnostic sur fond orange indique une criticité plus élevée que le fond bleu.

Par exemple, cinq serveurs virtuels sont configurés sur votre instance Citrix ADC. Si vous n'avez pas activé les paramètres AppFlow sur des serveurs virtuels, Citrix ADM ne reçoit pas le trafic Web Insight et Security Insight pour analyse. Les diagnostics en libre-service identifient les problèmes de configuration comme critiques. Les rapports de diagnostic s'affichent en arrière-plan orange dans les fonctionnalités Web Insight et Security Insight.

Si vous avez activé AppFlow sur l'un des serveurs virtuels, Citrix ADM reçoit des données à des fins d'analyse. Vous voyez le rapport de diagnostic en arrière-plan bleu car au moins un serveur virtuel envoie du trafic pour analyse.

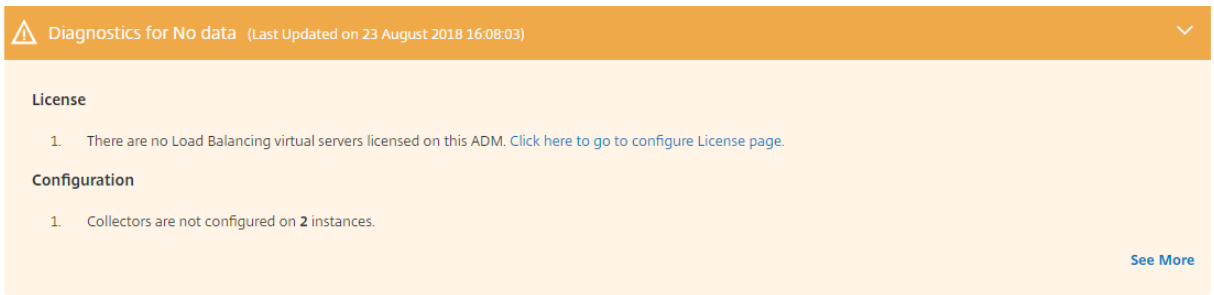


> **IMPORTANT**
>
> Les tests de diagnostic en libre-service ne vérifient pas le flux de trafic. Il vérifie uniquement les problèmes de licence ou de configuration associés aux fonctionnalités d'analyse spécifiées sur les instances gérées. Parfois, vous ne voyez aucune donnée analytique car aucun trafic actif ne circule à travers les serveurs virtuels.

Le rapport Diagnostic comporte une page récapitulative et une page d'informations détaillées.

La page de résumé fournit une vue d'ensemble sur les types de problèmes - licence ou configuration. La page peut contenir des liens hypertexte qui vous dirigent vers les pages de configuration pertinentes.

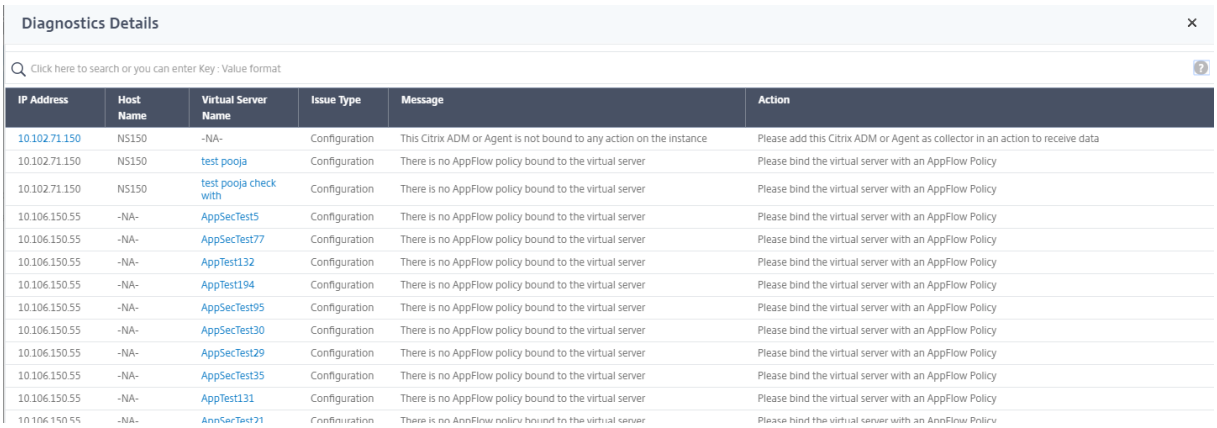
Par exemple, si aucun serveur virtuel d'équilibrage de charge n'est sous licence, la page récapitulative fournit un lien hypertexte qui vous dirige vers la page **Licences système**.



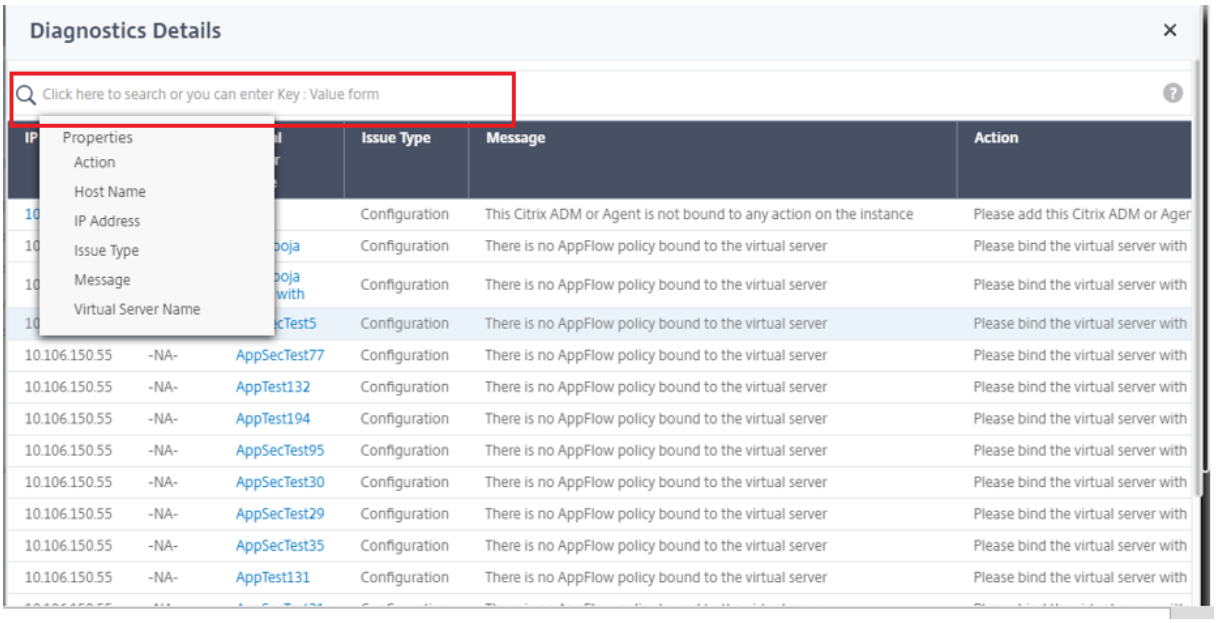
Pour afficher les informations détaillées sur les problèmes, cliquez sur **Voir plus** sur la page récapitu-

lative.

La page d'informations détaillées fournit des informations complètes sur les problèmes et recommande les actions que vous devez effectuer. Vous pouvez cliquer sur le lien hypertexte correspondant à chaque problème pour configurer l'instance gérée ou le serveur virtuel.



Vous pouvez également rechercher les problèmes en fonction de l'action, du nom d'hôte, de l'adresse IP et du type de problème, etc.



Après avoir résolu les problèmes, vous devez exécuter un diagnostic instantané pour générer le dernier rapport de diagnostic.

Web Insight

April 29, 2021

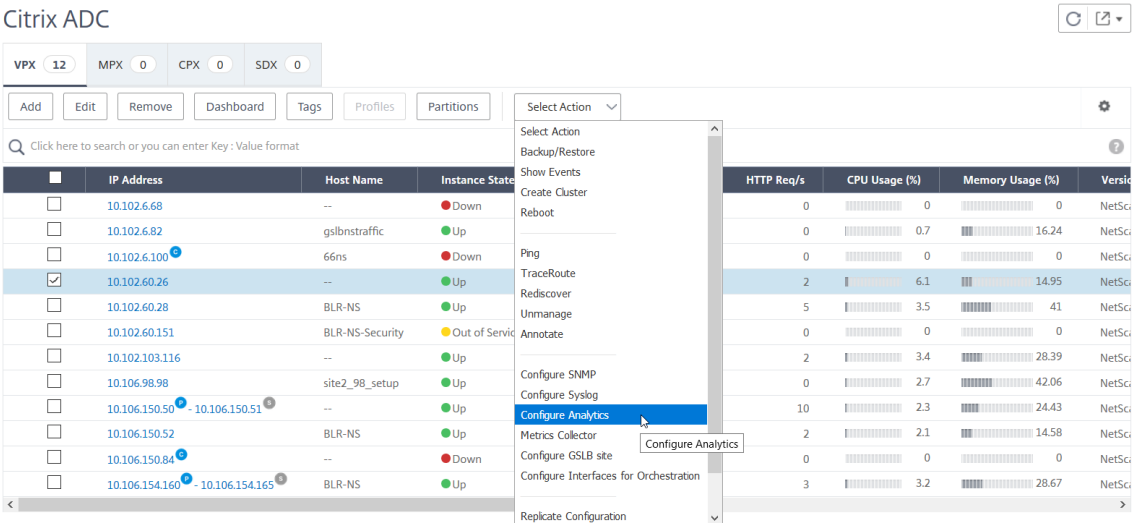
Web Insight permet aux administrateurs de surveiller toutes les applications Web desservies par les instances de Citrix ADC. En tant qu'administrateur, vous pouvez obtenir une surveillance intégrée et en temps réel des applications à partir d'instances de Citrix ADC. Web Insight fournit des informations critiques telles que la latence du réseau client et le temps de réponse du serveur, garantissant ainsi la surveillance et l'amélioration des performances des applications. Les données utilisées pour l'analyse sont capturées à partir de chaque transaction HTTP, HTTPS traitée par l'instance de Citrix ADC. Les données d'analyse vous permettent d'analyser les performances des instances Citrix ADC, de l'application, de l'URL, du client et du serveur dans votre environnement.

Voici quelques-uns des cas d'utilisation que vous pouvez afficher les données à l'aide de Web Insight :

- La liste des clients qui connaissent une latence élevée lors de l'accès à une application telle que SharePoint
- La meilleure application qui a eu le plus de succès en une heure
- La liste des applications et des URL accessibles depuis les clients
- Le système d'exploitation et le navigateur utilisés par un client particulier
- Applications ou serveurs qui envoient le plus de réponses liées aux erreurs
- Problèmes d'accessibilité avec un client particulier
- Problèmes d'accessibilité pour une partie ou l'ensemble des applications d'un client particulier
- Peu de pages d'une application sont lentes à partir d'un client particulier et d'un serveur backend
- L'application est lente lorsqu'elle est accessible à partir d'un client particulier et d'un serveur principal

Vous pouvez activer Web Insight pour un serveur virtuel spécifique sur une instance sélectionnée afin de surveiller le trafic sur votre application Web. La fonctionnalité Web Insight fournit ensuite des statistiques pour le serveur virtuel dans Citrix ADM. Pour activer le Web Insight :

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 Analytics sur les serveurs virtuels** :

   a) Sélectionnez les serveurs virtuels que vous souhaitez activer Web Insight et cliquez sur **Activer Analytics**

   La fenêtre **Activer les analyses** s'affiche.

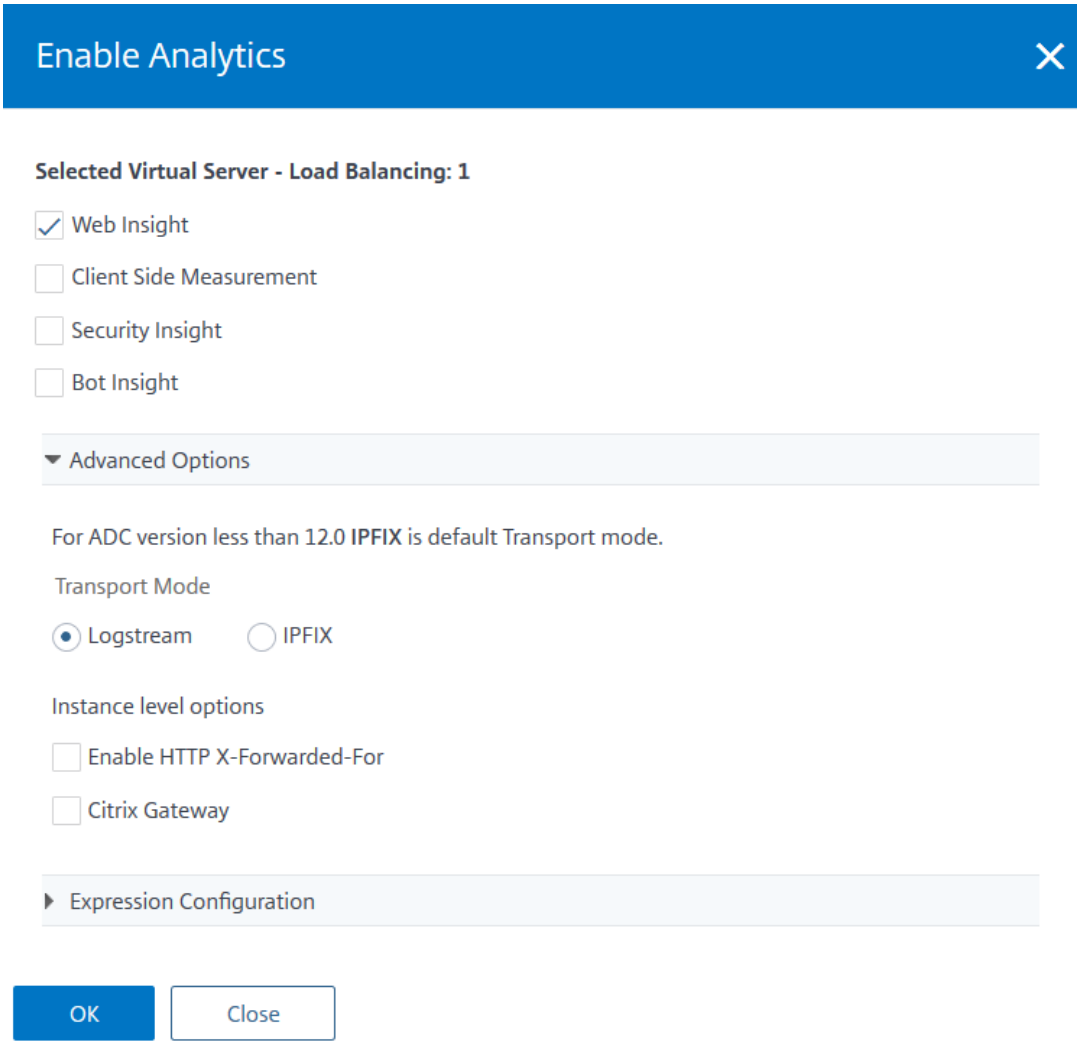
   b) Sélectionner **Web Insight**

   c) Sous **Options avancées**, sélectionnez **Logstream**ou **IPFIX**comme mode de transport

   > **Remarque**
   >
   > Pour Citrix ADC 12.0 ou version antérieure, **IPFIX** est l'option par défaut pour le mode de transport. Pour Citrix ADC 12.0 ou version ultérieure, vous pouvez sélectionner **Logstream** ou **IPFIX** comme mode de transport.
   >
   > Pour plus d'informations sur **IPFIX** et **Logstream**, reportez-vous à la section **Présentation de Logstream**.

   d) L'expression est true par défaut

   e) Cliquez sur **OK**.



Analyser les problèmes liés aux applications Web

L'un des problèmes courants qu'un administrateur doit identifier est les problèmes de latence. En tant qu'administrateur, vous devez déterminer si le problème de latence provient du réseau serveur, du réseau client ou du temps de réponse du serveur. À l'aide de Citrix ADM, vous pouvez identifier ces informations en accédant à **Analytics** > **Web Insight** .

Lorsque vous accédez à **Analytics** > **Web Insight**, il affiche les instances Citrix ADC activées avec Web Insight. Vous pouvez afficher les informations détaillées pour les instances telles que l'adresse IP, le nom d'hôte, le nombre total d'accès et la bande passante.

À l'aide de la liste, vous pouvez sélectionner la durée pour afficher les informations relatives aux instances.

Vous pouvez également utiliser le curseur pour personnaliser la durée du temps et cliquer sur **Aller** pour afficher les résultats.

Lorsque vous cliquez sur le graphique ou l'adresse IP de l'instance, les informations détaillées sur l'instance s'affichent. Vous pouvez afficher des informations sur les éléments suivants :

- **Nombre total de visites**
- **Bande passante**
- **Applications**
- **Domaines**
- **URL**
- **Méthodes de requête HTTP**
- **État de la réponse HTTP**
- **Clients**
- **Serveurs**
- **Systèmes d'exploitation**
- **Agents utilisateurs**

Vous pouvez également sélectionner **des entités Web Insight** pour lesquelles vous souhaitez afficher des rapports sur l'interface graphique.

1. Accédez à **Analytics** > **Web Insight** > **Paramètres** .
2. Cliquez sur **Configurer les journaux des enregistrements de données Analytics**.
3. Sous **Paramètres de rapport Web Insight**, sélectionnez les entités que vous souhaitez afficher des rapports sur l'interface graphique.
4. Cliquez sur **OK**.

Pour effectuer une analyse plus poussée, vous pouvez cliquer sur chaque catégorie d'informations sous Web Insight dans l'interface graphique. Par exemple, si vous souhaitez vérifier les problèmes pour les serveurs configurés :

1. Accédez à **Analytics** > **Web Insight** > **Serveurs**.
2. La page Serveurs s'affiche avec tous les serveurs configurés.
3. Cliquez sur l'adresse IP du graphique. Vous pouvez également cliquer sur l'adresse IP dans le tableau.

   La vue d'aperçu détaillée du serveur sélectionné s'affiche. Dans cette vue, vous pouvez rechercher plusieurs informations telles que :

   - Nombre total de visites reçues par le serveur
   - Bande passante

- Temps de traitement du serveur
- Latence réseau du serveur
- Serveurs virtuels configurés pour le serveur
- Nombre total de clients accédant au serveur
- Nombre total de codes de réponse fournis par le serveur

Cas d'utilisation 1 - Erreur interne du serveur

Considérez un scénario selon lequel vos utilisateurs rencontrent une erreur d'inaccessibilité 500 pour votre application Web. L'erreur 500 (introuvable) est une erreur d'état de réponse HTTP qui indique un problème sur le serveur Web, mais le serveur n'indique pas le problème explicitement. Pour identifier et analyser le problème réel :

1. Accédez à **Analytics** > **Web Insight** > **État des réponses**.

   La page du tableau de bord s'affiche. Le tableau de bord fournit les mesures que vous pouvez utiliser pour analyser le succès et l'échec des transactions HTTP traitées.

2. Cliquez sur **Non trouvé** dans le graphique.

3. Faites défiler vers le bas pour afficher le **graphique Serveurs**et, dans la liste **Filtrer par**, sélectionnez **Latence réseau du serveur**.

   Le graphique indique que chaque serveur d'applications a rencontré un problème lors de la récupération de l'application Web et donc le temps de réponse pour le serveur Web est augmenté. Le problème peut être lié au fait que le serveur Web ne répond à aucune demande d'un serveur.

Cas d'utilisation 2 - L'utilisateur connaît une lenteur dans l'accès à l'application Web

Considérez un scénario selon lequel votre application Web est hébergée par 10 serveurs Web différents. Lorsque plusieurs utilisateurs accèdent à l'application en même temps, un ou plusieurs utilisateurs peuvent rencontrer une lenteur de l'application. En tant qu'administrateur, vous devez analyser les scénarios suivants pour comprendre la cause première du problème :

Scénario 1 - Temps de traitement du serveur :

Lorsque plusieurs demandes atteignent les 10 serveurs Web différents en même temps, le temps de chargement de la requête diffère en fonction des éléments suivants :

- 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' `CSTOLBTarget` application dans l'image est un serveur virtuel de commutation de contenu lié à d'autres serveurs virtuels d'équilibrage de charge
3. Cliquez sur le serveur virtuel de commutation de contenu pour afficher l'autre serveur virtuel d'équilibrage de charge. Vous pouvez également cliquer sur le nom de l'application dans le tableau.

Vous pouvez également cliquer sur les serveurs d'équilibrage de charge liés pour afficher les détails Web Insight de ces applications.

Analyser des informations pour les navigateurs et les systèmes d'exploitation

Vous pouvez utiliser Web Insight pour vous aider à séparer les problèmes de latence L7 et à comprendre l'utilisation des appareils mobiles. En tant qu'administrateur, les informations peuvent vous aider à comprendre les différentes prises de système d'exploitation au sein de votre base d'utilisateurs.

Accédez à **Analytics** > **Web Insight** > **Système d'exploitation** pour voir pourquoi l'accès des utilisateurs est lent et si cela est dû à une incompatibilité entre certains navigateurs. Vous pouvez également voir quels systèmes d'exploitation sont utilisés sur certains clients et quels navigateurs sont accessibles. Vous pouvez comparer le temps de rendu sur les différents navigateurs et effectuer une exploration vers le bas à un navigateur particulier pour identifier les pages d'application qui sont associées au temps de rendu le plus élevé pour ce navigateur.

Par exemple, vous pouvez sélectionner **Google Chrome** et voir les temps de rendu correspondants pour les différentes pages URL d'une application particulière.

Instances Citrix ADC déployées en mode haute disponibilité

Citrix ADM fournit des rapports pour les instances ADC déployées en mode haute disponibilité. Les rapports agrégés pour les instances en mode haute disponibilité sont pris en charge dans toutes les analyses.

Vous pouvez cliquer sur le nom des instances qui sont en haute disponibilité pour afficher plus de détails.

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, les noms de domaine d'observation ID/d'observation sont remplacés par le nom d'hôte CLIP et CLIP. Toutes les données

> précédemment collectées continuent de déclarer l'ID de domaine d'observation/nom de domaine d'observation.

Configuration de la carte géographique Web Insight

La fonctionnalité Geomaps de Citrix ADM affiche l'utilisation des applications Web sur différents emplacements géographiques sur une carte. Les administrateurs peuvent utiliser ces informations pour comprendre les tendances de l'utilisation des applications et pour la planification des capacités.

Geo map fournit des informations sur les mesures suivantes spécifiques à un pays, un état et une ville :

- Nombre total de visites : nombre total d'accès à une application.
- Bande passante : bande passante totale consommée pendant le traitement des demandes du client
- Temps de réponse : Temps moyen nécessaire pour envoyer les 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 **active automatiquement** les géomaps pour les adresses IP privées ou les adresses IP publiques, lorsque vous activez **Web Insight**.

Créer un bloc IP privé

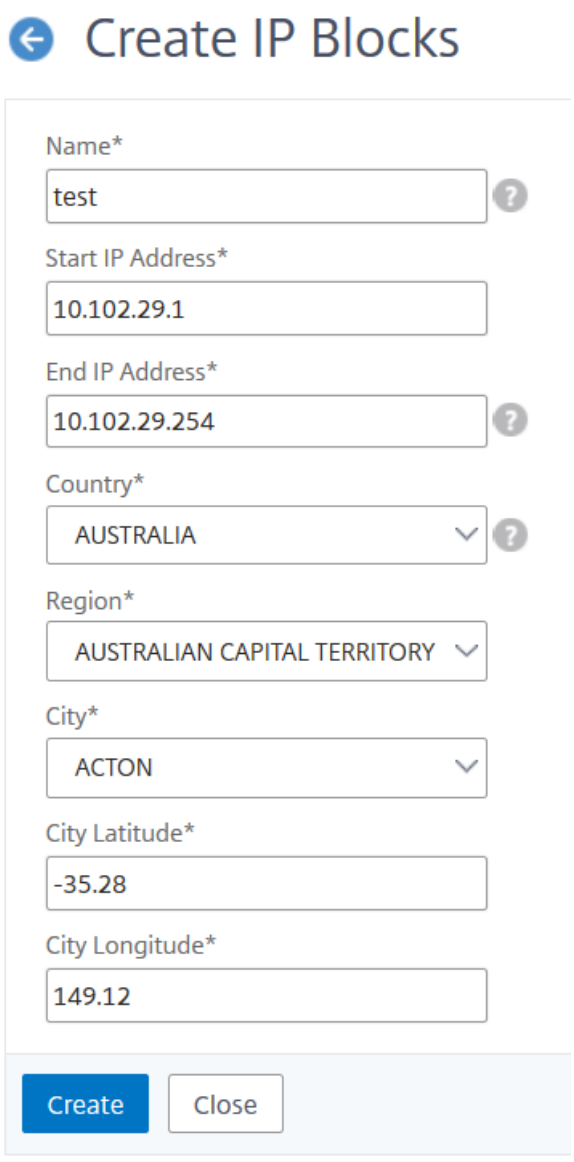
Citrix ADM peut reconnaître l'emplacement du client lorsque l'adresse IP privée du client est ajoutée au serveur Citrix ADM. Par exemple, si l'adresse IP d'un client se situe dans la plage d'un bloc d'adresse IP privé associé à la ville A, Citrix ADM reconnaît que le trafic provient de la ville A pour 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**. Spécifier un nom pour le bloc IP privé
    - **Démarrer l'adresse IP**. Spécifiez la plage d'adresses IP la plus basse pour le bloc IP.
    - **Adresse IP de fin**. Spécifiez la plage d'adresses IP la plus élevée pour le bloc 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 automatiquement remplie, 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 automatiquement remplies.

3. Cliquez sur **Créer** pour terminer.

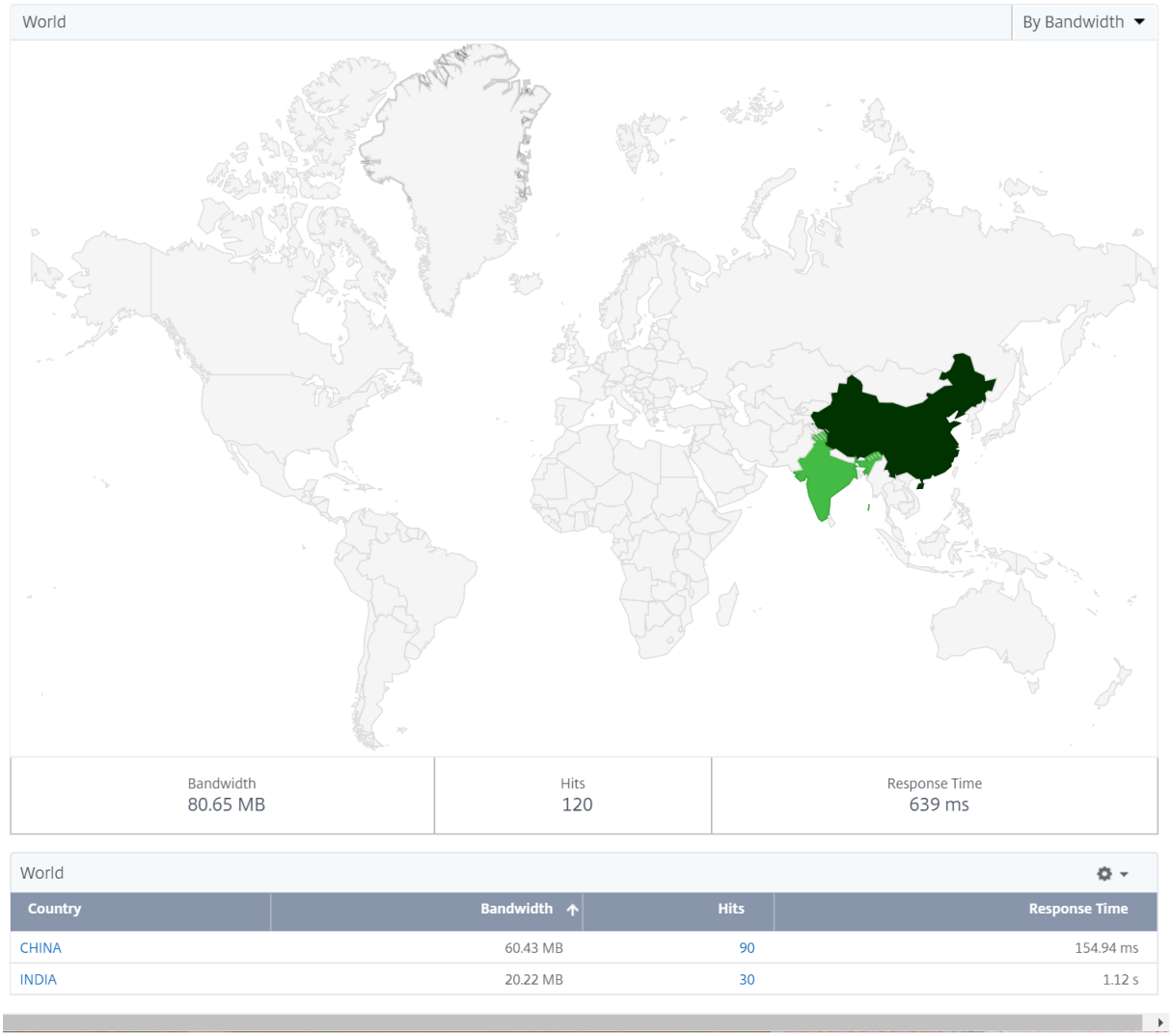


Blocs IP publics

Citrix ADM peut également reconnaître l'emplacement du client si le client utilise une adresse IP publique. Citrix ADM possède son fichier CSV d'emplacement intégré qui correspond à l'emplacement

basé sur la plage d'adresses IP du client. Pour utiliser le bloc IP public, la seule condition est que vous devez activer la collecte de données géographiques **Activer la collecte de données géographiques** à partir de la page Configurer Insight.

> Remarque
>
> Citrix ADM nécessite une connexion Internet pour afficher les géomaps d'un emplacement 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 tous les jours, toutes les semaines ou tous les mois et envoyer le rapport par e-mail ou par message de marge.

> **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 les recevoir notifiés chaque fois que la valeur du seuil ne respecte pas. Dans un déploiement standard, vous pouvez définir des seuils sur :

- Suivi de diverses mesures d'application
- Faciliter la planification
- Recevez une notification chaque fois que la valeur de mesure des applications dépasse le seuil défini

Pour configurer le seuil :

1. Accédez à **Analytics** > **Paramètres** > **Seuils** .
2. Dans 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 automatiquement générée en fonction du type de trafic et de l'entité que vous avez sélectionnés.
   e) **Durée** - Dans la liste, sélectionnez l'intervalle de temps pour lequel vous souhaitez surveiller l'entité. Vous pouvez surveiller les entités pendant une heure, une journée ou une semaine.
   f) Dans la section **Configurer la règle**, créez une règle en choisissant la mesure, un comparateur requis et indiquez une valeur de seuil.
   g) Dans la section **Paramètres des notifications**, sélectionnez **Activer le seuil** et le mode d'alerte pour lequel vous souhaitez recevoir les alertes.

4. Cliquez sur **Créer**.

SSL Insight

April 29, 2021

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 ce qui suit :

- **Déterminez l'impact des modifications de configuration sur l'utilisation du client**. L'administrateur peut comprendre l'impact sur les clients d'effectuer une modification de configuration comme la désactivation de SSLv3 ou la suppression d'un chiffrement comme RC4-MD5. Cela peut être fait en évaluant les données historiques sur les transactions relatives à ce protocole et à ce chiffrement.
- **Quantifiez les performances du client**. L'administrateur peut comprendre l'impact sur le temps de réponse de l'application en fonction des chiffres/protocole SSL utilisés ou des certificats négociés.
- **Sécurité des applications**. Déterminer si l'une des applications a des transactions exécutées sur des protocoles de faible sécurité, des chiffrements ou une force de clé faible.

Lorsque SSL Analytics est activé sur une instance 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.)

SSL Insight fournit les informations critiques suivantes, qui sont affichées par Citrix ADM Analytics :

- Version du protocole SSL négociée
- Chiffrement négocié, et force de chiffrement
- Algorithme de hachage de signature du certificat utilisé
- Type et taille du certificat
- Erreurs SSL frontal et back-end

> **Remarque**
>
> Pour les connexions SSL réussies, la journalisation SSL AppFlow se produit à la fin de chaque transaction.

Conditions préalables

- L'instance Citrix ADC sur laquelle vous avez l'intention de 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 la version d'Citrix ADM doivent être égales ou supérieures à la version et à la version d'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 for Web Insight sur chaque instance ADC.
- Activez le mode ULFD sur chaque instance ADC.
- Activez les paramètres AppFlow requis sur chaque instance ADC.

Permettre la perspicacité

> **Remarque**
>
> Vous pouvez activer la fonctionnalité AppFlow à partir de Citrix ADM ou de chaque instance ADC.

Activer la fonctionnalité AppFlow à partir de Citrix ADM

1. Accédez à **Réseaux** > **Instances**, puis sélectionnez l'instance ADC sur laquelle vous souhaitez activer l'analyse.
2. Dans la liste **Sélectionner une action**, sélectionnez **Configurer Analytics**.
3. Sur la page **Configurer Analytics sur les serveurs virtuels** :
   a) Sélectionnez les serveurs virtuels que vous souhaitez activer Web Insight et cliquez sur **Activer Analytics**

      La fenêtre **Activer les analyses** s'affiche.

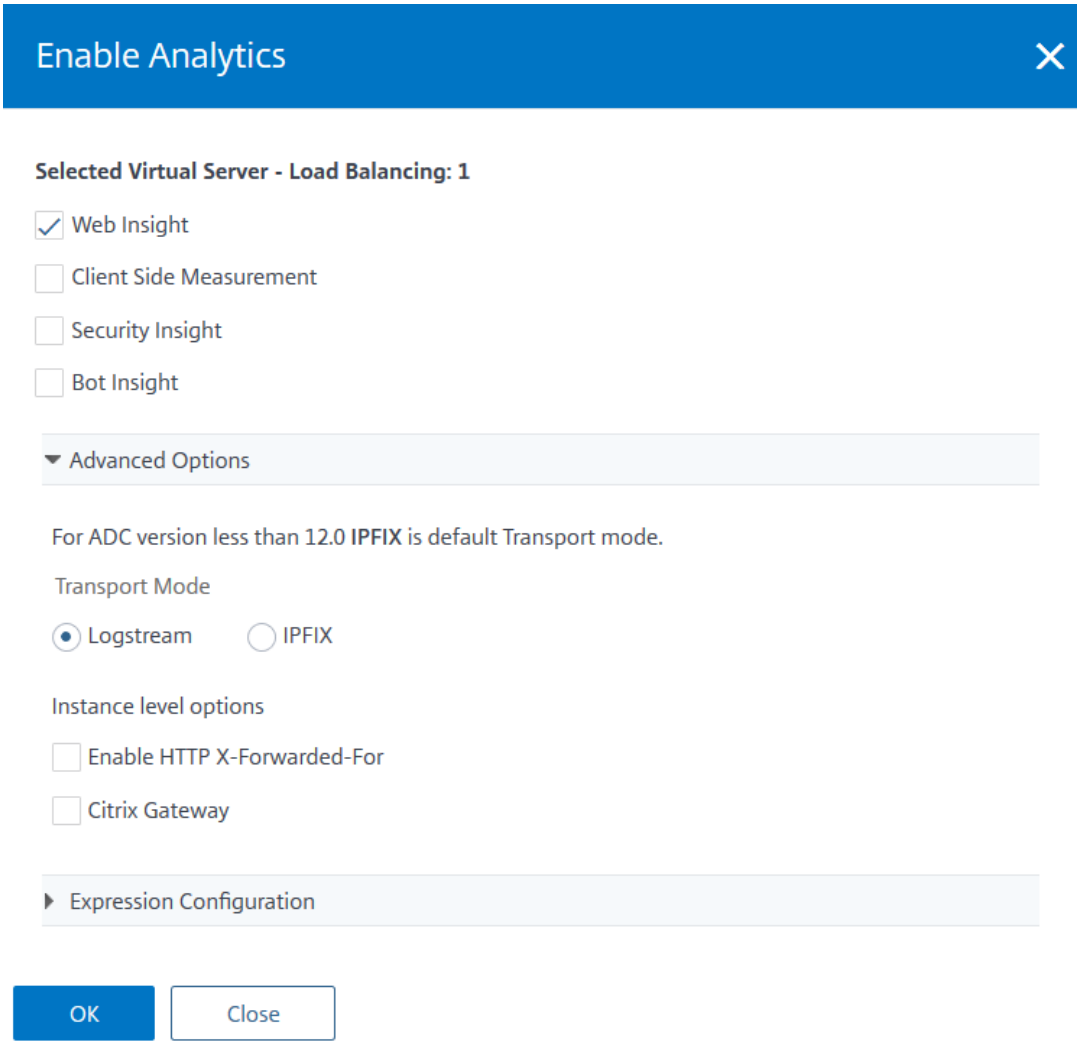
   b) Sélectionner **Web Insight**

c) Sous **Options avancées**, sélectionnez **Logstream**ou **IPFIX**comme mode de transport

> **Remarque**
>
> Pour Citrix ADC 12.0 ou version antérieure, **IPFIX** est l'option par défaut pour le mode de transport. Pour Citrix ADC 12.0 ou version ultérieure, vous pouvez sélectionner **Logstream** ou **IPFIX** comme mode de transport.
>
> Pour plus d'informations sur **IPFIX** et **Logstream**, reportez-vous à la section **Présentation de Logstream**.

d) L'expression est true par défaut

e) Cliquez sur **OK**.



> **Remarque**
>
> Vous ne pouvez pas activer la collecte de données sur un serveur virtuel si l'état opérationnel du serveur virtuel est autre que UP.

Activer la fonctionnalité AppFlow à l'aide de l'interface graphique ADC

Dans l'interface graphique d'une instance ADC, accédez à **Configuration** > **Système** > **Paramètres**, cliquez sur **Configurer les fonctionnalités avancées** et sélectionnez **AppFlow** .

Activation du mode ULFD

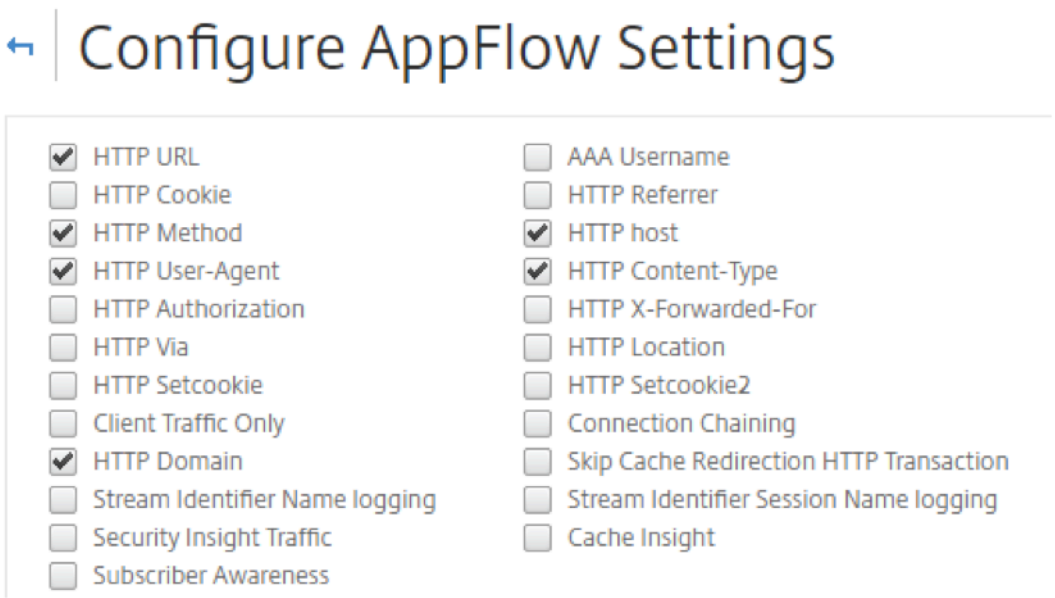
Après avoir activé le mode ULFD sur les instances ADC sur lesquelles les serveurs virtuels sont configurés, le serveur ULFD diffuse les données d'analyse des instances ADC vers Citrix ADM.

Activer les paramètres SSL Insight

Sur chaque instance ADC, vous devez activer certains paramètres HTTP pour afficher les enregistrements SSL Insight dans Citrix ADM.

Activer les paramètres SSL Insight à partir de l'utilitaire de configuration ADC

1. Accédez à **Configuration** > **Système** > **AppFlow**, puis cliquez sur **Modifier AppFlowSettings** .
2. Activez les cases à cocher suivantes : **Domaine HTTP**, **Hôte HTTP, Méthode HTTP, URL HTTP, Agent utilisateur HTTP, Type de contenu HTTP**.
3. Cliquez sur **OK**.



Afficher les métriques SSL Insight

Les mesures SSL Insight dans Citrix ADM fournissent une vue détaillée des performances des transactions SSL desservies par les instances ADC. Vous pouvez afficher les mesures SSL Insight au niveau du client, du serveur ou de l'application, ainsi que les mesures de réussite et d'échec SSL des transactions. À l'aide de ces mesures, vous pouvez analyser et optimiser vos paramètres HTTPS ADC et les paramètres de certificat SSL, et suivre les problèmes de performances.

> **Remarque**
>
> Lorsque vous créez un groupe, vous pouvez attribuer des rôles au groupe, fournir un accès au groupe au niveau de l'application et affecter des utilisateurs au groupe. L'analyse Citrix ADM prend désormais en charge l'autorisation basée sur l'adresse IP virtuelle. Vos utilisateurs peuvent désormais voir des rapports pour tous les Insights uniquement pour les applications (serveurs virtuels) pour lesquelles ils sont autorisés. Pour plus d'informations sur les groupes et l'affectation d'utilisateurs au groupe, reportez-vous à la section Configuration de groupes sur Citrix ADM.

Surveillance des mesures SSL Insight dans Citrix ADM

1. Sous 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 le menu, 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.

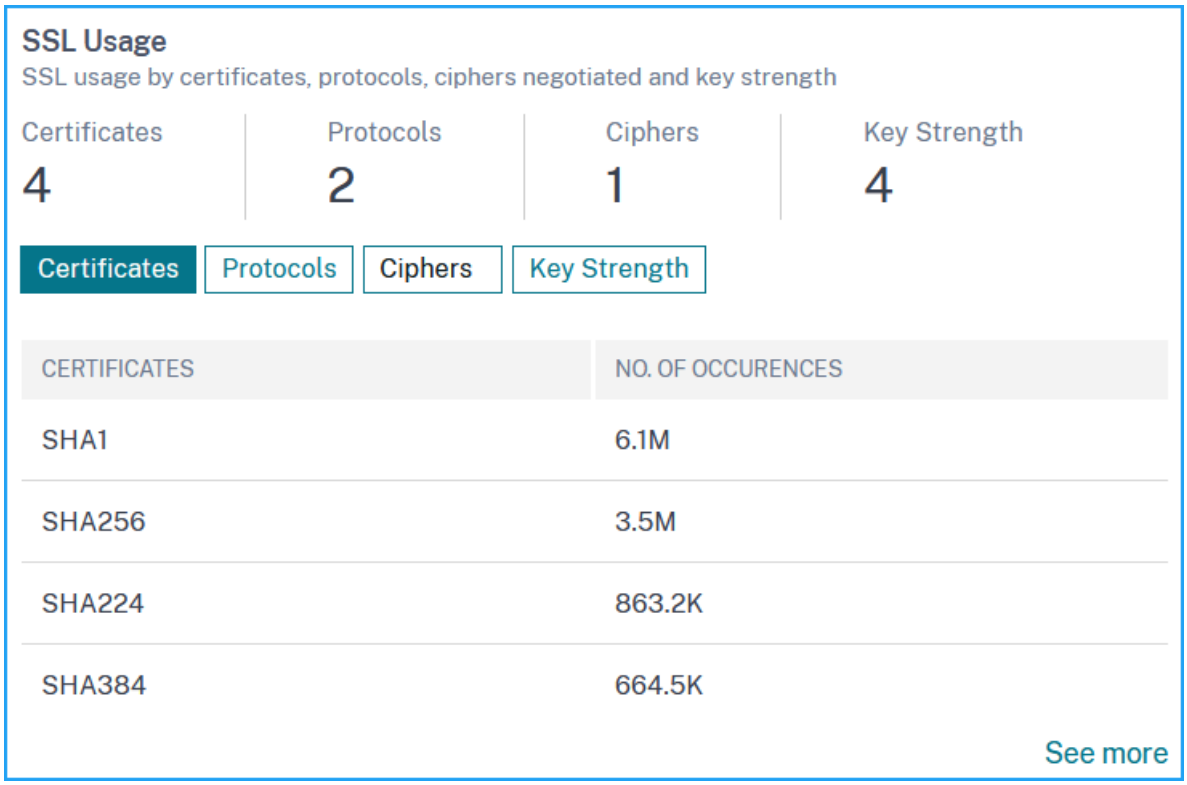
4. Pour afficher les détails d'une application, d'un client ou d'un serveur spécifique, cliquez sur la valeur correspondante dans le graphique à barres.
5. Pour afficher les transactions SSL en échec, dans la section SSL, sélectionnez le bouton radio de la section SSL.

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. Vous devrez peut-être examiner fréquemment les applications afin de pouvoir vous concentrer d'abord sur les applications qui nécessitent le plus d'attention. Le tableau de bord d'aperçu SSL fournit un résumé des différents paramètres SSL utilisés par vos applications sur une période de temps de votre choix et pour un périphérique ADC sélectionné. Elles sont répertoriées comme suit :

- Certificats SSL
- Protocoles SSL
- Cipher SSL négocié
- Force des clés SSL
- Défaillance SSL — Frontal
- Échec SSL — Back end



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 : TSLv1.2, TSLv1.1, TSLv1 et SSLv3.

Vous pouvez également voir que les 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 échecs SSL front-end et back-end sont affichés séparément dans deux graphiques à secteurs. 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.

HDX Insight

April 29, 2021

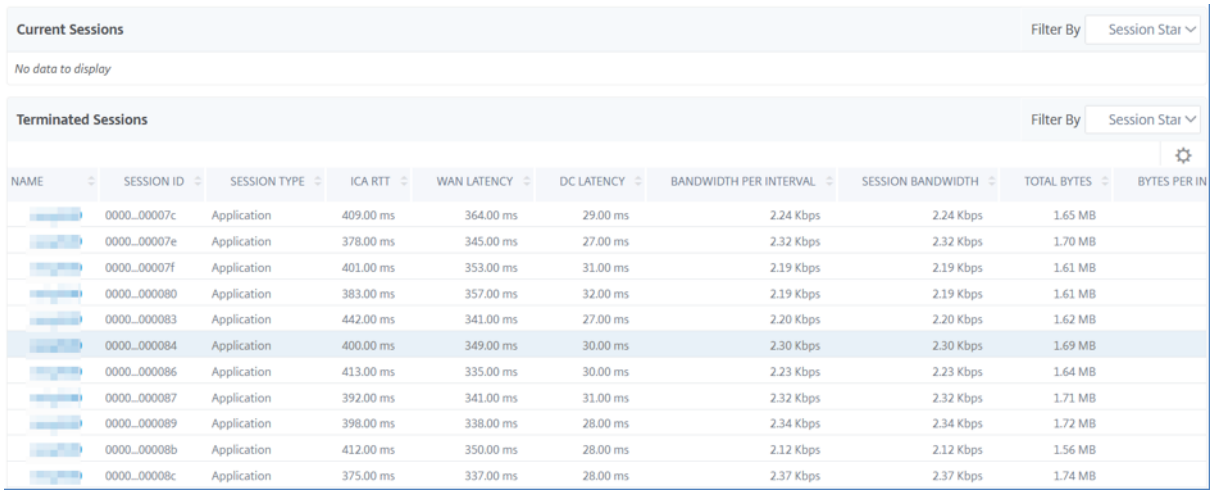
HDX Insight fournit une visibilité de bout en bout pour le trafic HDX vers les Citrix Virtual Apps and Desktops passant par Citrix ADC. Il permet également aux administrateurs d'afficher en temps réel les mesures de latence client et réseau, les rapports historiques, les données de performances de bout 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 ADC Gateway. AppFlow peut être livré par le protocole **IPFIX** ou la méthode **Logstream**.

> **Remarque**
>
> Pour autoriser l'enregistrement des calculs de temps aller-retour ICA, activez les paramètres de stratégie suivants :
>
> - Calcul de l'ICA aller-retour
> - Intervalle de calcul des aller-retour ICA
> - Calcul de l'aller-retour ICA pour les connexions au ralenti

Si vous cliquez sur un utilisateur individuel, vous pouvez voir chaque session HDX, active ou terminée, effectuée par l'utilisateur dans la période sélectionnée. D'autres informations incluent plusieurs statistiques de latence et la bande passante consommée pendant la session. Vous pouvez également obtenir des informations sur la bande passante à partir de canaux virtuels individuels tels que l'audio, le mappage d'imprimante et le mappage de lecteur client.

Vous pouvez également visualiser une vue consolidée de tous les utilisateurs des sessions actives et terminées.



En tant qu'administrateur, cette vue vous permet d'effectuer les opérations suivantes :

- Afficher tous les détails des utilisateurs dans une visualisation à un seul volet
- Éliminer la complexité de la sélection de chaque utilisateur et de voir les sessions actives et terminées

> **Remarque**
>
> Lorsque vous créez un groupe, vous pouvez attribuer des rôles au groupe, fournir un accès au groupe au niveau de l'application et affecter des utilisateurs au groupe. L'analyse Citrix ADM prend désormais en charge l'autorisation basée sur l'adresse IP virtuelle. Vos utilisateurs peuvent désormais voir des rapports pour tous les Insights uniquement pour les applications (serveurs virtuels) pour lesquelles ils sont autorisés. Pour plus d'informations sur les groupes et l'affectation d'utilisateurs au groupe, reportez-vous à la section Configuration de groupes sur Citrix ADM.

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 afficher l'agent utilisateur de tous les utilisateurs connectés en accédant à **HDX Insight > Utilisateurs**.

> **Remarque**
>
> HDX insight prend en charge les partitions d'administration configurées dans les instances ADC exécutées sur la version 12.0 du logiciel.

Les clients légers suivants prennent en charge HDX Insight :

- Clients légers Windows WYSE
- Clients légers basés sur Linux WYSE
- Clients légers basés sur WYSE Thinos
- Clients légers basés sur Ubuntu-10ZiG

Identification de la cause première des problèmes de performance lente

Scénario 1

L'utilisateur rencontre des retards lors de l'accès aux Citrix Virtual Apps and Desktops de travail

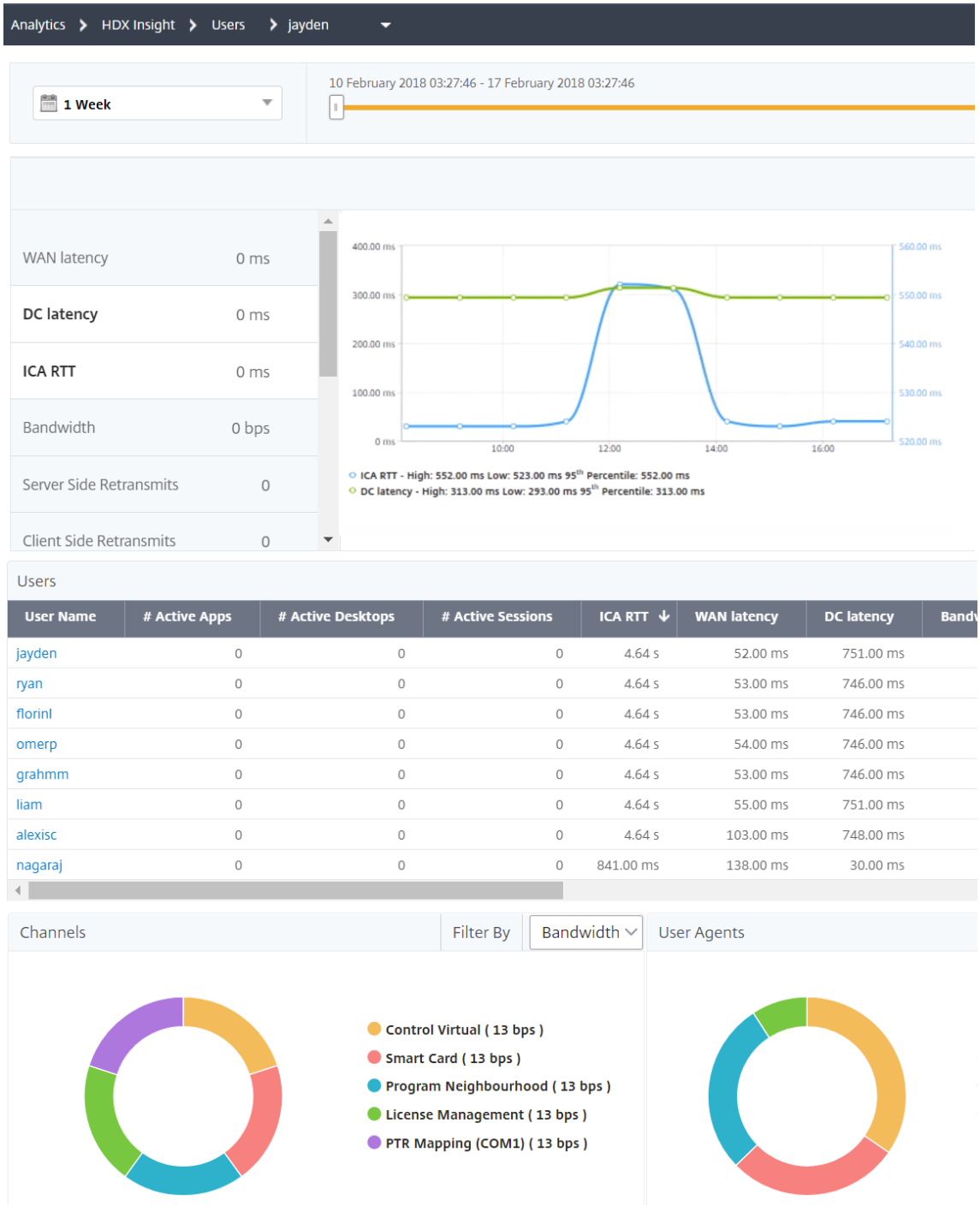
Les retards peuvent être dus à une latence sur le réseau serveur, à des retards de trafic ICA causés par le réseau serveur ou à une latence sur le réseau client.

Pour identifier la cause première du problème, analysez les mesures suivantes :

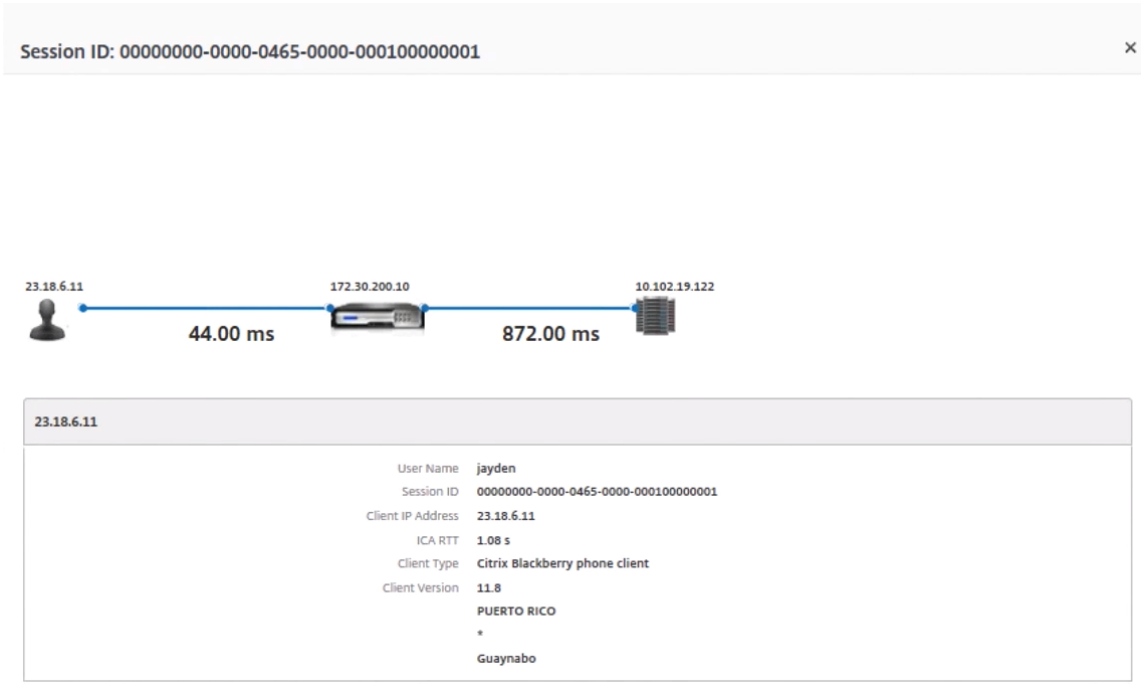
- Latence WAN
- Latence du contrôleur de domaine
- Délai d'hôte

Pour afficher les mesures client :

1. Sous l'onglet **Analytics**, accédez à **HDX Insight** > **Utilisateurs**.
2. Faites défiler vers le bas et sélectionnez le nom d'utilisateur et sélectionnez la période dans la liste. La période peut être d'un jour, d'une semaine, d'un mois, ou vous pouvez même personnaliser la période pour laquelle vous souhaitez voir les données.
3. Le graphique affiche sous forme de graphique les valeurs de latence ICA RTT et DC de l'utilisateur pour la période spécifiée.



4. Dans la table **Sessions d'applications actuelles**, placez la souris sur la valeur **RTT** et notez les valeurs de délai de l'hôte, de latence DC et de latence WAN.
5. Dans le tableau **Sessions d'applications actuelles**, 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 du contrôleur** de domaine est de 751 millisecondes, la **latence du réseau étendu** est de 52 millisecondes et les **retards de l'hôte** est de 6 secondes. Cela indique que l'utilisateur rencontre un retard dû à une latence moyenne causée par le réseau serveur.

Scénario 2

L'utilisateur rencontre un retard lors du lancement d'une application sur Citrix Virtual Apps ou Ordinateurs de bureau

Le retard peut être dû à la latence sur le réseau serveur, aux retards de trafic ICA causés par le réseau serveur, à la latence sur le réseau client ou au temps nécessaire pour lancer une application.

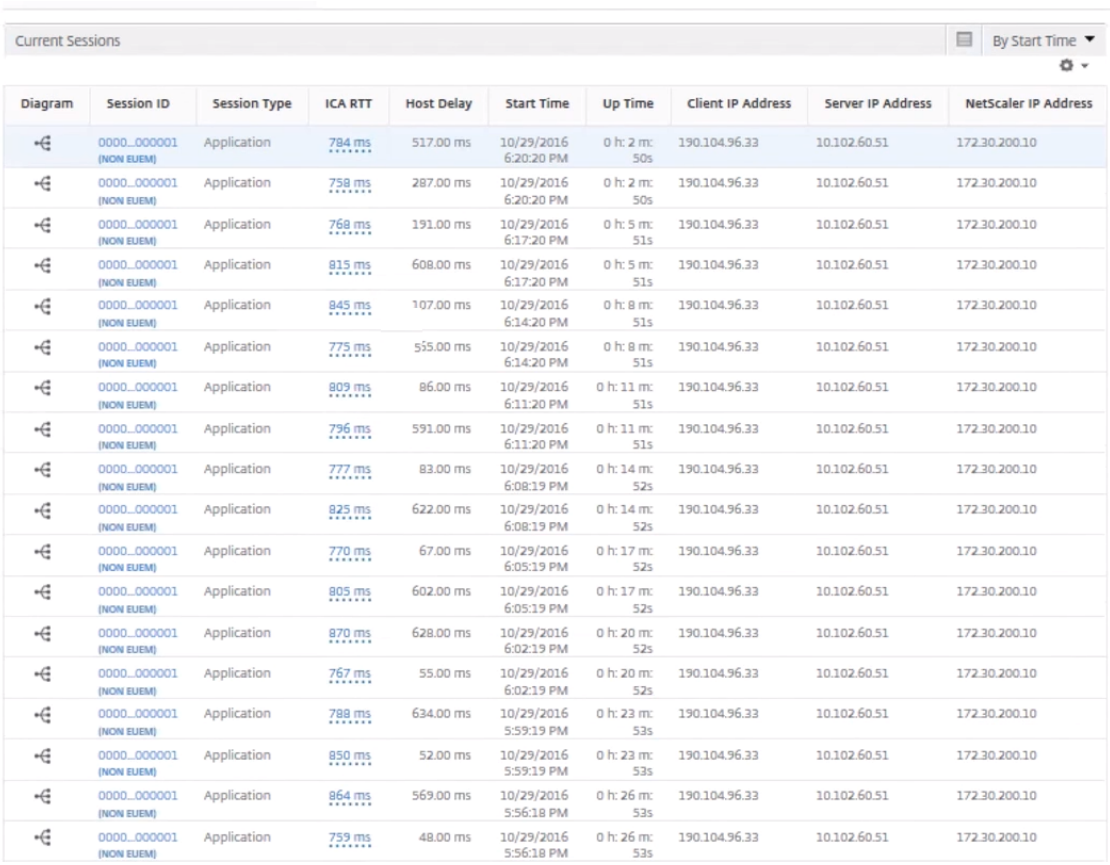
Pour identifier la cause première du problème, analysez les mesures suivantes :

- Latence WAN
- Latence DC
- Délai de l'hôte

Pour afficher les mesures utilisateur :

1. Sous l'onglet **Analytics**, accédez à **HDX Insight** > **Utilisateurs**.
2. Faites défiler la page vers le bas et cliquez sur le nom d'utilisateur.
3. Dans la représentation graphique, notez les valeurs Latence WAN, Latence DC et RTT pour la session particulière.

4. Dans le tableau **Sessions d'applications actuelles**, notez que le délai de l'hôte est élevé.



Current Sessions — By Start Time

Diagram	Session ID	Session Type	ICA RTT	Host Delay	Start Time	Up Time	Client IP Address	Server IP Address	NetScaler IP Address
	0000...000001 (NON EUEM)	Application	784 ms	517.00 ms	10/29/2016 6:20:20 PM	0 h: 2 m: 50s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	758 ms	287.00 ms	10/29/2016 6:20:20 PM	0 h: 2 m: 50s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	768 ms	191.00 ms	10/29/2016 6:17:20 PM	0 h: 5 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	815 ms	608.00 ms	10/29/2016 6:17:20 PM	0 h: 5 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	845 ms	107.00 ms	10/29/2016 6:14:20 PM	0 h: 8 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	775 ms	535.00 ms	10/29/2016 6:14:20 PM	0 h: 8 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	809 ms	86.00 ms	10/29/2016 6:11:20 PM	0 h: 11 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	796 ms	591.00 ms	10/29/2016 6:11:20 PM	0 h: 11 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	777 ms	83.00 ms	10/29/2016 6:08:19 PM	0 h: 14 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	825 ms	622.00 ms	10/29/2016 6:08:19 PM	0 h: 14 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	770 ms	67.00 ms	10/29/2016 6:05:19 PM	0 h: 17 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	805 ms	602.00 ms	10/29/2016 6:05:19 PM	0 h: 17 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	870 ms	628.00 ms	10/29/2016 6:02:19 PM	0 h: 20 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	767 ms	55.00 ms	10/29/2016 6:02:19 PM	0 h: 20 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	788 ms	634.00 ms	10/29/2016 5:59:19 PM	0 h: 23 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	850 ms	52.00 ms	10/29/2016 5:59:19 PM	0 h: 23 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	864 ms	569.00 ms	10/29/2016 5:56:18 PM	0 h: 26 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	759 ms	48.00 ms	10/29/2016 5:56:18 PM	0 h: 26 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10

Résumé :

Dans cet exemple, la **latence DC** est de 1 milliseconde, la **latence WAN** est de 12 millisecondes, mais le **délai d'hôte** est de 517 millisecondes. Le RTT élevé avec des latences DC et WAN faibles indique une erreur d'application sur le serveur hôte.

> **Remarque**
>
> HDX Insight affiche également plus de mesures utilisateur, telles que la gigue WAN et les re-transmet 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.

Carte géographique pour HDX Insight

L'entité cartographique géographique de Citrix ADM affiche l'utilisation des applications Web sur différents emplacements géographiques sur une carte. En tant qu'administrateur, vous pouvez utiliser ces informations pour comprendre les tendances dans l'utilisation des applications et pour la planification des capacités.

Geo map fournit des informations sur les mesures suivantes spécifiques à un pays, un état et une ville :

- Nombre total de visites : nombre total d'accès à une application.
- Bande passante : bande passante totale consommée pendant le traitement des demandes du client
- Temps de réponse : Temps moyen nécessaire pour envoyer des réponses aux demandes des clients.

Geo map fournit 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 **active automatiquement** les géomaps pour les adresses IP privées ou les adresses IP publiques, lorsque vous activez l' **information Web**.

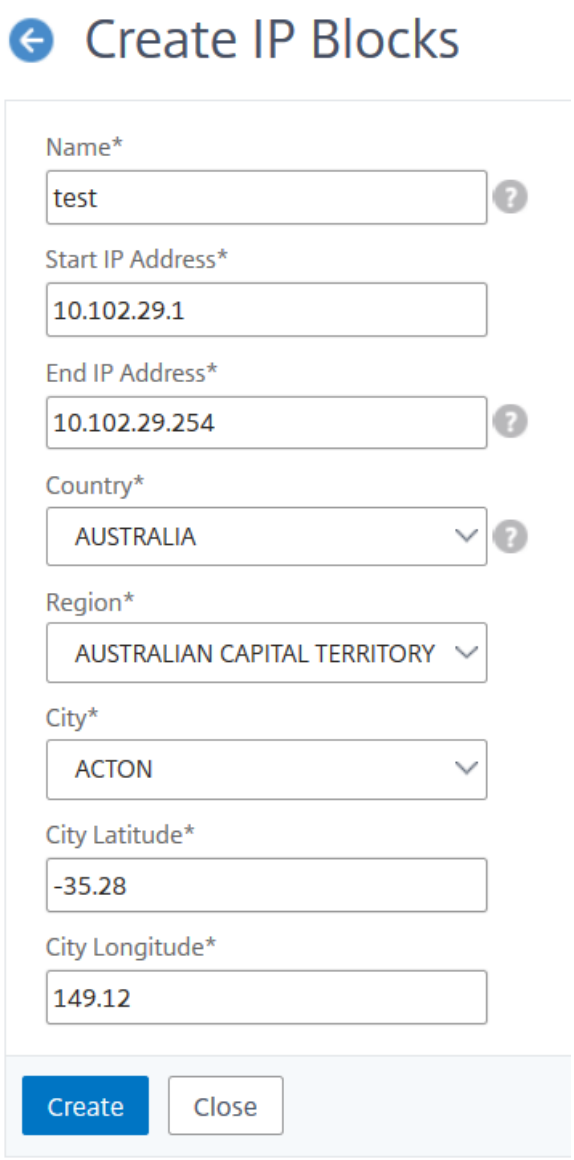
Créer un bloc IP privé

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'adresses 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**. Spécifier un nom pour le bloc IP privé
    - **Démarrer l'adresse IP**. Spécifiez la plage d'adresses IP la plus basse pour le bloc IP.
    - **Adresse IP de fin**. Spécifiez la plage d'adresses IP la plus élevée pour le bloc 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 automatiquement remplie, 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 automatiquement remplies.
3. Cliquez sur **Créer** pour terminer.

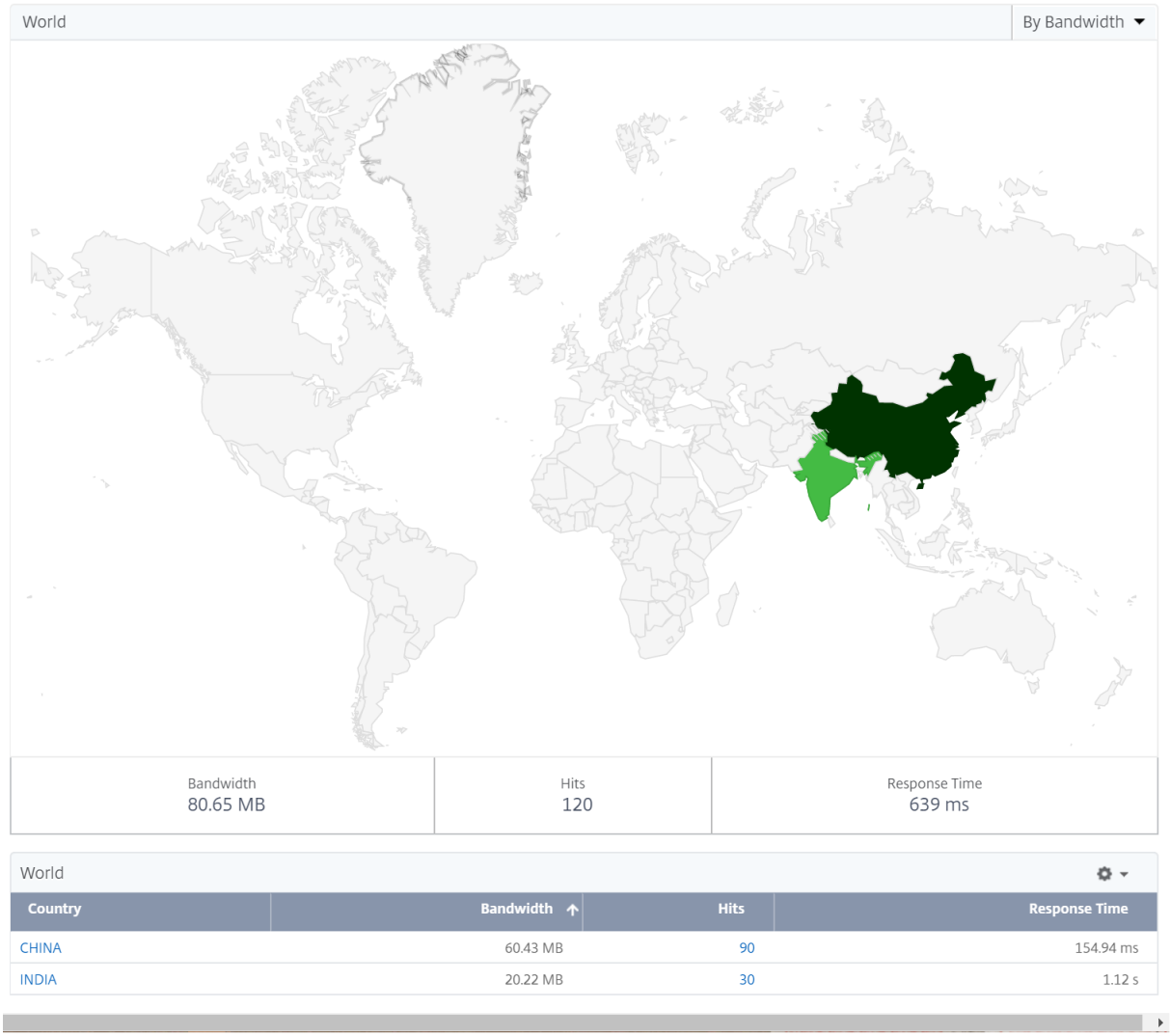


Blocs IP publics

Citrix ADM peut également reconnaître l'emplacement du client si le client utilise une adresse IP publique. Citrix ADM possède son fichier CSV d'emplacement intégré qui correspond à l'emplacement basé sur la plage d'adresses IP du client. Pour utiliser le bloc IP public, la seule condition est que vous devez activer la collecte de données géographiques **Activer la collecte de données géographiques** à partir de la page Configurer Insight.

> Remarque
>
> Citrix ADM nécessite une connexion Internet pour afficher les géomaps d'un emplacement géographique particulier. Une connexion Internet est également nécessaire pour exporter le Ge-

> oMap 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 :

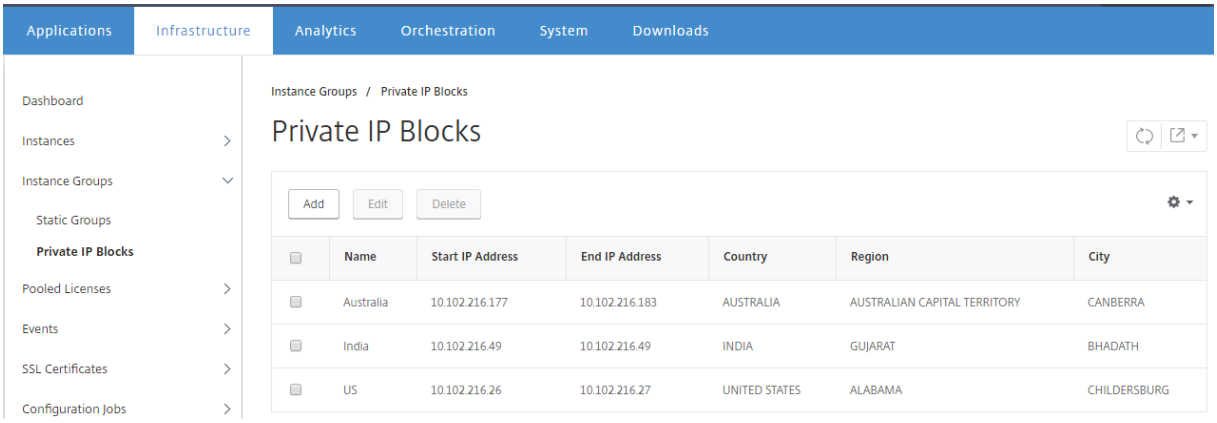
1. Sélectionnez l'onglet **Exporter maintenant**. Pour afficher et enregistrer le rapport au format PDF, JPEG, PNG ou CSV.
2. Sélectionnez l'onglet **Planifier l'exportation**. Pour planifier le rapport tous les jours, toutes les semaines ou tous les mois et envoyer le rapport par e-mail ou par message de marge.

> **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.

Pour configurer une carte géographique pour les centres de données :

Sous l'onglet **Réseaux**, accédez à **Sites** > **Blocs IP privés** pour configurer des géomaps pour un emplacement particulier.



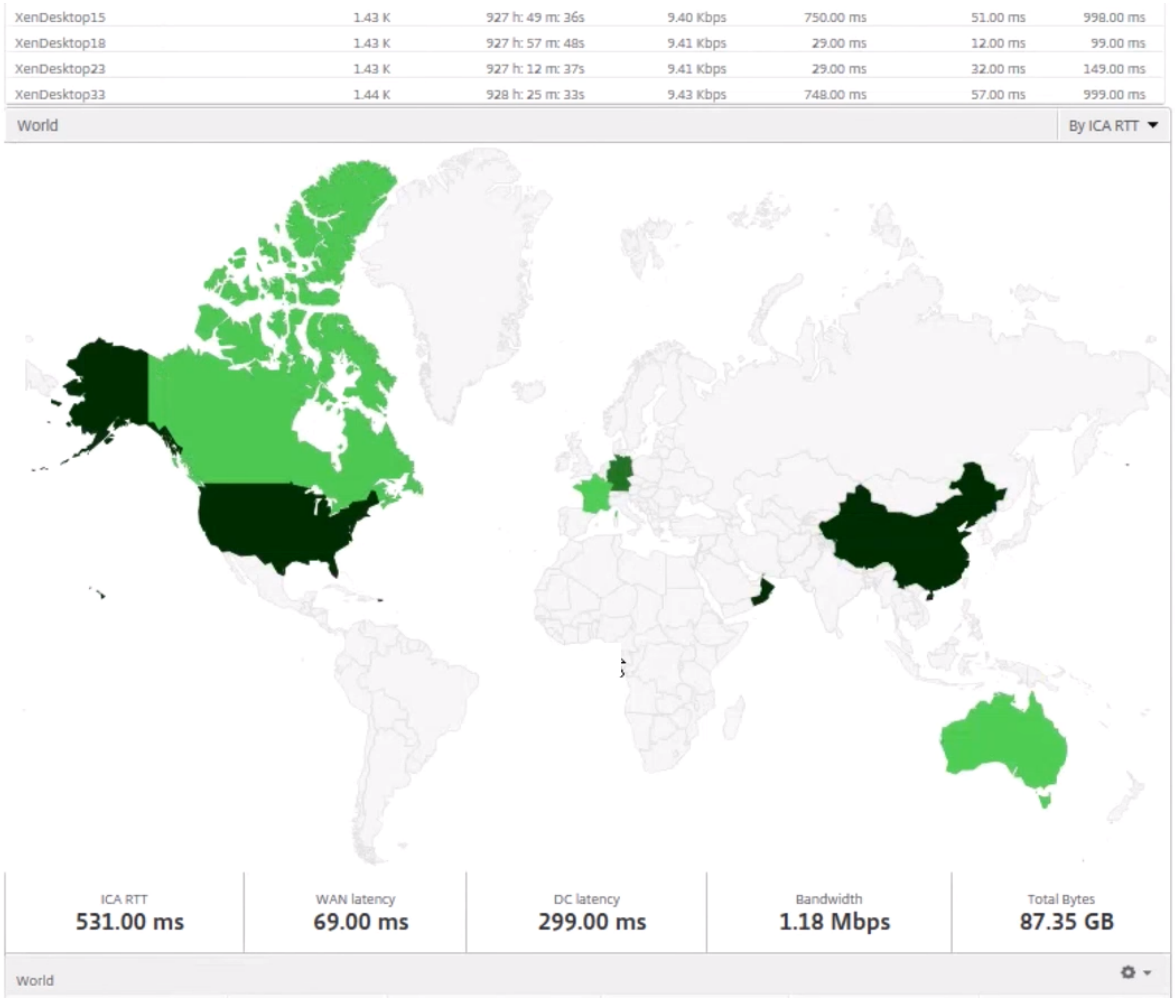
Cas d'utilisation

Considérons un scénario dans lequel l'organisation ABC a 2 succursales, l'une à Santa Clara et l'autre en Inde.

Les utilisateurs de Santa Clara utilisent l'appliance ADC Gateway sur Sclara.x.com pour accéder au trafic VPN. Les utilisateurs indiens utilisent l'appliance ADC Gateway sur India.x.com pour accéder au trafic VPN.

Pendant un intervalle de temps particulier, disons 10h à 17h, les utilisateurs de Santa Clara se connectent à Sclara.x.com pour accéder au trafic VPN. La plupart des utilisateurs accèdent à la même passerelle ADC, provoquant 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 ADC qui analyse le trafic peut utiliser la fonctionnalité de géo map pour afficher le trafic dans le bureau de Santa Clara. La carte montre que le temps de réponse dans le bureau de Santa Clara est élevé, car le bureau de Santa Clara ne dispose qu'd'une seule appliance ADC Gateway permettant aux utilisateurs d'accéder au trafic VPN. L'administrateur peut donc décider d'installer une autre passerelle ADC, de sorte que les utilisateurs disposent de deux appliances ADC Gateway locales via lesquelles accéder au VPN.



Limitations

Si les instances ADC disposent d'une licence avancée, les seuils définis sur Citrix ADM pour HDX Insight ne seront pas déclenchés car les données analytiques sont collectées pendant une heure seulement.

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 tous les jours, toutes les semaines ou tous les mois et envoyer le rapport par e-mail ou par message de marge.

> **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.

Activer la collecte de données HDX Insight

April 29, 2021

HDX Insight permet à l'administrateur de fournir une expérience utilisateur exceptionnelle en fournissant une visibilité de bout en bout sur le trafic ICA qui passe par les appliances Citrix ADC ou Citrix SD-WAN.

HDX Insight offre des fonctionnalités de veille décisionnelle et d'analyse des défaillances convaincantes et puissantes pour le réseau, les postes de travail virtuels, les applications et la structure applicative. HDX Insight peut à la fois trier instantanément les problèmes des utilisateurs, collecter des données sur les connexions de bureau virtuel et générer des enregistrements AppFlow et les présenter sous forme de rapports visuels.

La configuration permettant d'activer la collecte de données dans les instances ADC diffère en fonction de la position de l'appliance dans la topologie de déploiement. Cette rubrique comprend les détails suivants :

- Activation de la collecte de données pour la surveillance des Citrix ADC déployés en mode transparent
- Activation de la collecte de données pour les appliances Citrix ADC Gateway déployées en mode saut unique
- Activation de la collecte de données pour les appliances Citrix ADC Gateway déployées en mode double-saut
- Activation de la collecte de données pour la surveillance des Citrix ADC déployés en mode utilisateur LAN

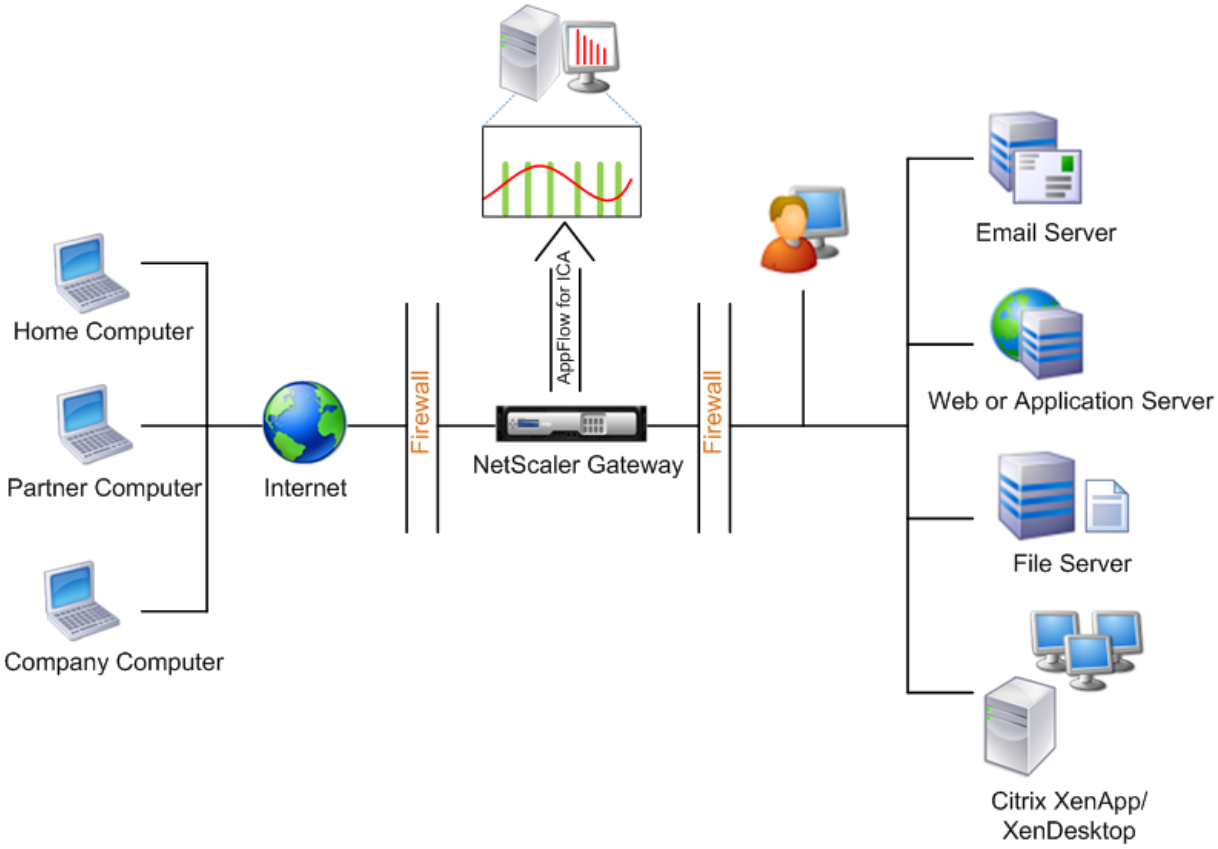
Activer la collecte de données pour les appliances Citrix ADC Gateway déployées en mode saut unique

April 29, 2021

Lorsque Citrix ADC Gateway est déployé en mode à saut unique, la passerelle ADC se trouve à la périphérie du réseau et proxie les connexions ICA à l'infrastructure de livraison des postes de travail. Ce déploiement est le déploiement le plus simple et le plus courant. Ce mode assure la sécurité si un

utilisateur externe tente d'accéder au réseau interne d'une organisation. En mode saut simple, les utilisateurs accèdent aux appliances ADC via un réseau privé virtuel (VPN).

Pour commencer à collecter les rapports, vous devez ajouter l'appliance ADC Gateway à l'inventaire ADM (Citrix Application Delivery Management) et activer AppFlow sur ADM. L'image suivante illustre un Citrix ADM déployé en mode à saut unique



Activer la fonctionnalité AppFlow à partir de Citrix ADM

1. Accédez à **Infrastructure** > **Instances**, puis sélectionnez l'instance ADC que vous souhaitez activer l'analyse.
2. Dans la liste **Action**, sélectionnez **Activer/Désactiver Insight**.
3. Sélectionnez les serveurs virtuels VPN, puis cliquez sur **Activer AppFlow**.
4. Dans le champ **Activer AppFlow**, tapez **true** et sélectionnez **ICA** .
5. Cliquez sur **OK**.

> **Remarque**
>
> Les commandes suivantes commencent à s'exécuter en arrière-plan lorsque vous activez AppFlow en mode 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`

Activer la collecte de données pour surveiller les Citrix ADC déployés en mode transparent

April 29, 2021

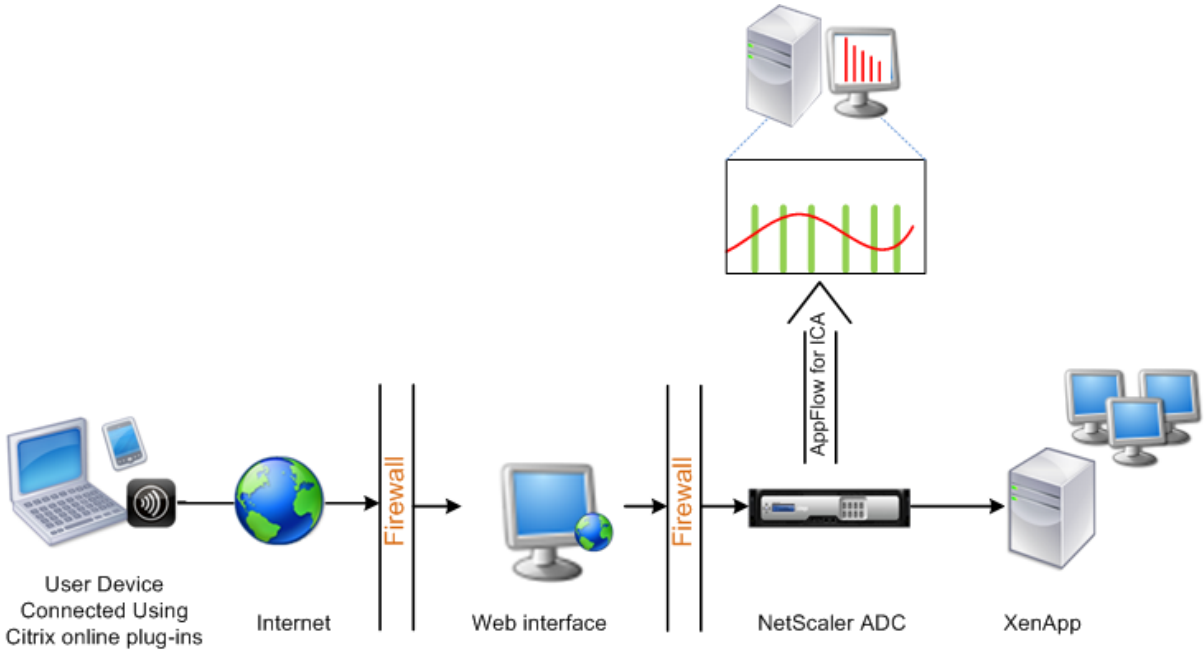
Lorsqu'un Citrix ADC est déployé en mode transparent, les clients peuvent accéder directement aux serveurs, sans serveur virtuel intervenant. Si une appliance Citrix ADC est déployée en mode transparent dans un environnement Citrix Virtual Apps and Desktops, le trafic ICA n'est pas transmis via un VPN.

Après avoir ajouté Citrix ADC à l'inventaire Citrix Application Delivery Management (ADM), vous devez activer AppFlow pour la collecte de données. L'activation de la collecte de données dépend du périphérique et du mode. Dans ce cas, vous devez ajouter Citrix ADM en tant que collecteur AppFlow sur chaque appliance Citrix ADC, et vous devez configurer une stratégie AppFlow pour collecter tout le trafic ICA ou spécifique qui circule via l'appliance.

Remarque

- Vous ne pouvez pas activer la collecte de données sur un Citrix ADC déployé en mode transparent à l'aide de l'utilitaire de configuration Citrix ADM.
- Pour plus d'informations sur les commandes et leur utilisation, reportez-vous à la section Référence de commande.
- Pour plus d'informations sur les expressions de stratégie, reportez-vous à la section Stratégies et expressions.

L'image suivante montre 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 auxquels l'appliance Citrix ADC écoute le trafic.

```
set ns param --icaPorts <port>...
<!--NeedCopy-->
```

Exemple :

```
set ns param -icaPorts 2598 1494
<!--NeedCopy-->
```

> **Remarque**
>
> - Vous pouvez spécifier jusqu'à 10 ports avec cette commande.
> - Le numéro de port par défaut est 2598. Vous pouvez modifier le numéro de port selon vos besoins.

3. Ajoutez NetScaler Insight Center en tant que collecteur AppFlow sur l'appliance Citrix ADC.

```
add appflow collector <name> -IPAddress <ip_addr>
<!--NeedCopy-->
```

Exemple :


```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```

> **Remarque**
>
> Pour afficher les collecteurs AppFlow configurés sur l'appliance Citrix ADC, utilisez la commande **show appflow collector** .

4. Créez une action AppFlow et associez le collecteur à l'action.

```
add appflow action <name> -collectors <string> ...
<!--NeedCopy-->
```

Exemple :

```
add appflow action act -collectors MyInsight
<!--NeedCopy-->
```

5. Créez une stratégie AppFlow pour spécifier la règle de génération du trafic.

```
add appflow policy <policyname> <rule> <action>
<!--NeedCopy-->
```

Exemple :

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. Liez la stratégie AppFlow à un point de liaison global.

```
bind appflow global <policyname> <priority> -type <type>
<!--NeedCopy-->
```

Exemple :

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--NeedCopy-->
```

> **Remarque**
>
> La valeur de **type** doit être ICA_REQ_OVERRIDE ou ICA_REQ_DEFAULT pour s'appliquer au trafic ICA.

7. Définissez la valeur du paramètre FlowRecordInterval pour AppFlow sur 60 secondes.

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```


8. Enregistrez la configuration.

```
save ns config
<!--NeedCopy-->
```

Activer la collecte de données pour les appliances Citrix ADC Gateway déployées en mode double-saut

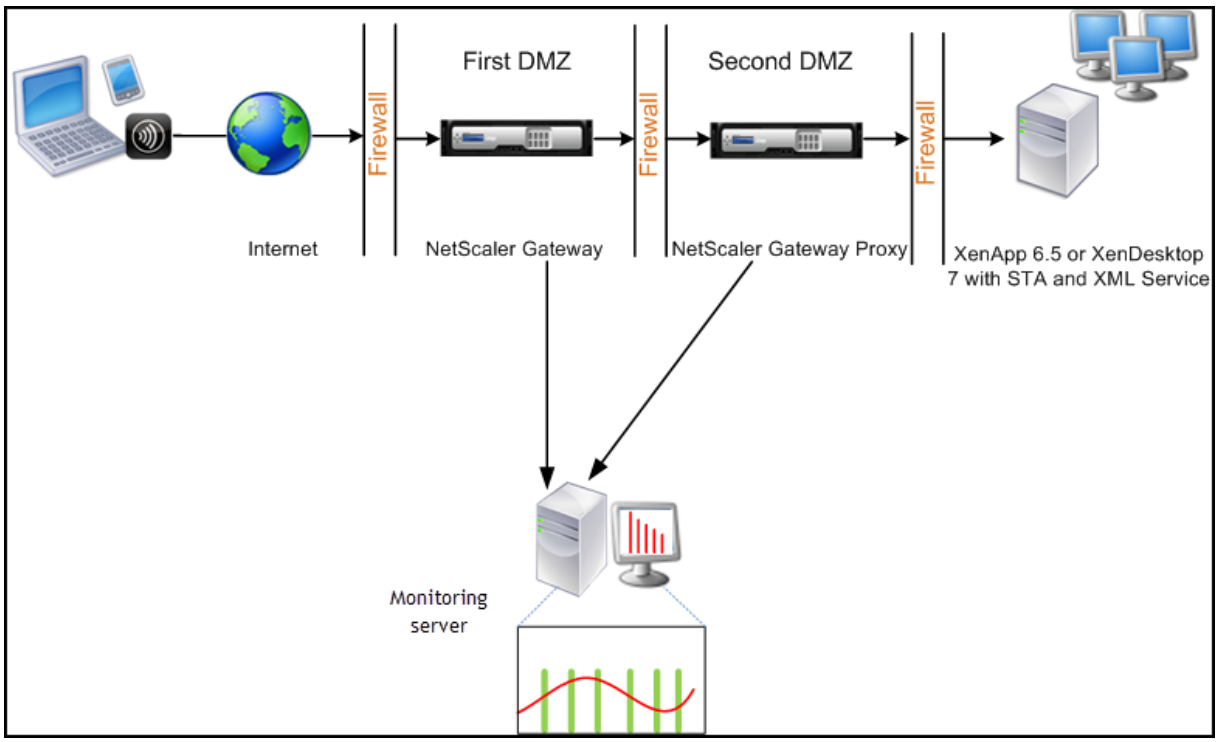
April 29, 2021

Le mode double saut Citrix ADC Gateway fournit une protection supplémentaire au réseau interne d'une organisation car un attaquant devrait pénétrer plusieurs zones de sécurité ou zones démilitarisées (DMZ) pour atteindre les serveurs du réseau sécurisé.

En tant qu'administrateur, à l'aide de Citrix ADM, vous pouvez analyser :

- Nombre de sauts (appliances Citrix ADC Gateway) par lesquels les connexions ICA passent
- Les détails sur la latence sur chaque connexion TCP et comment elle se présente contre la latence ICA totale perçue par le client

L'image suivante indique que Citrix ADM et Citrix ADC Gateway dans la première DMZ sont déployés dans le même sous-réseau.



Citrix ADC Gateway dans la première DMZ gère les connexions utilisateur et exécute les fonctions de sécurité d'un VPN SSL. Cette Citrix ADC Gateway chiffre les connexions utilisateur, détermine la manière dont les utilisateurs sont authentifiés et contrôle l'accès aux serveurs du réseau interne.

Citrix ADC Gateway dans la deuxième zone DMZ sert de périphérique proxy Citrix ADC Gateway. Cette Citrix ADC Gateway permet au trafic ICA de traverser la deuxième zone DMZ pour terminer les connexions utilisateur à la batterie de serveurs.

Citrix ADM peut être déployé soit dans le sous-réseau appartenant à l'appliance Citrix ADC Gateway dans la première DMZ, soit dans le sous-réseau appartenant à l'appliance Citrix ADC Gateway deuxième DMZ.

En mode double saut, Citrix ADM collecte les enregistrements TCP d'une appliance et les enregistrements ICA de l'autre appliance. Après avoir ajouté les appliances Citrix ADC Gateway à l'inventaire Citrix ADM et activé la collecte de données, chaque appliance exporte les rapports en gardant le suivi du nombre de sauts et de l'ID de chaîne de connexion.

Pour que Citrix ADM identifie l'appliance qui exporte des enregistrements, chaque appliance est spécifiée avec un nombre de sauts et chaque connexion est spécifiée avec un ID de chaîne de connexion. Le nombre de sauts représente le nombre d'appliances Citrix ADC Gateway via lequel 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 associer les données des appliances Citrix ADC Gateway et générer les rapports.

Pour surveiller les appliances Citrix ADC Gateway déployées dans ce mode, vous devez d'abord ajouter Citrix ADC Gateway à l'inventaire Citrix ADM, activer AppFlow sur Citrix ADM, puis afficher 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. Pour surmonter cette situation, vous devez activer AppFlow for ICA sur le premier dispositif Citrix ADC Gateway, puis activer AppFlow for TCP sur la deuxième appliance. Ce faisant, l'une des appliances exporte les enregistrements ICA AppFlow et l'autre exporte les enregistrements TCP AppFlow. Cela permet également d'économiser du 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 Citrix ADC que vous souhaitez activer l'analyse.
2. Dans la liste **Action**, sélectionnez **Activer/Désactiver Insight**.

3. Sélectionnez les serveurs virtuels VPN, puis cliquez sur **Activer AppFlow**.
4. Dans le champ **Activer AppFlow**, tapez **true** et sélectionnez **ICA**/**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 affiche Activé.

5. Cliquez sur **OK**.

Configurer les appliances Citrix ADC Gateway pour exporter des données

Après avoir installé les appliances Citrix ADC Gateway, vous devez configurer les paramètres suivants sur les appliances Citrix ADC Gateway pour exporter les rapports vers Citrix ADM :

- Configurez les serveurs virtuels des appliances Citrix ADC Gateway dans la première et la deuxième zone DMZ pour communiquer entre eux.
- Liez le serveur virtuel Citrix ADC Gateway dans la deuxième DMZ au serveur virtuel Citrix ADC Gateway dans la première DMZ.
- Activez le double saut sur Citrix ADC Gateway dans la seconde DMZ.
- Désactivez l'authentification sur le serveur virtuel Citrix ADC Gateway dans la deuxième zone DMZ.
- Activer l'une des appliances Citrix ADC Gateway pour exporter des enregistrements ICA
- Activez l'autre appliance Citrix ADC Gateway pour exporter les enregistrements TCP :
- Activez le chaînage des connexions sur les deux appliances Citrix ADC Gateway.

Configurez Citrix ADC Gateway à l'aide de l'interface de ligne de commande :

1. Configurez le serveur virtuel Citrix ADC Gateway dans la première DMZ pour qu'il communique avec le serveur virtuel Citrix ADC Gateway dans la seconde DMZ.

   add vpn nextHopServer <name> <nextHopIP> <nextHopPort> [**-secure** (ON|OFF)] [**-imgGifToPng**] …

   ```
   add vpn nextHopServer nh1 10.102.2.33 8443 -secure ON
   <!--NeedCopy-->
   ```

2. Liez le serveur virtuel Citrix ADC Gateway dans la deuxième DMZ au serveur virtuel Citrix ADC Gateway dans la première DMZ. Exécutez la commande suivante sur Citrix ADC Gateway dans la première DMZ :

bind vpn vserver <name> **-nextHopServer** <name>

```
bind vpn vserver vs1 -nextHopServer nh1
<!--NeedCopy-->
```

3. Activez le double saut et AppFlow sur Citrix ADC Gateway dans la seconde DMZ.

   set vpn vserver <name> [**- doubleHop** (ENABLED |DISABLED)] [**- AppFlowLog** (ENABLED |DISABLED)]

```
set vpn vserver vpnhop2  - doubleHop ENABLED  - appFlowLog ENABLED
<!--NeedCopy-->
```

4. Désactivez l'authentification sur le serveur virtuel Citrix ADC Gateway dans la deuxième zone DMZ.

   définir vpn vserver<name> [**-authentification** (ON|OFF)]

```
set vpn vserver vs -authentication OFF
<!--NeedCopy-->
```

5. Activez l'une des appliances Citrix ADC Gateway pour exporter les enregistrements TCP.

   lier vpn vpn [<name> -policy **<string> **-priority **] [<positive_integer> -type **<type>]

```
bind vpn vserver vpn1 -policy appflowpol1 -priority 101  - type
   OTHERTCP_REQUEST
<!--NeedCopy-->
```

6. Activez l'autre appliance Citrix ADC Gateway pour exporter les enregistrements ICA :

   lier vpn vpn [<name> -policy **<string> **-priority **] [<positive_integer> -type **<type>]

```
bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
   ICA_REQUEST
<!--NeedCopy-->
```

7. Activer le chaînage des connexions sur les deux appliances Citrix ADC Gateway :

set appFlow param [**-connectionChaining** DISABLED)] (ENABLED

```
set appflow param -connectionChaining ENABLED
<!--NeedCopy-->
```


Configuration de Citrix ADC Gateway à l'aide de l'utilitaire de configuration :

1. Configurez Citrix ADC Gateway dans la première DMZ pour communiquer avec Citrix ADC Gateway dans la deuxième DMZ et liez Citrix ADC Gateway dans la deuxième DMZ à Citrix ADC Gateway dans la première DMZ.
    a) Sous l'onglet **Configuration**, développez **Citrix ADC 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 ADC Gateway.
2. Activez le double saut sur Citrix ADC Gateway dans la seconde DMZ.
    a) Sous l'onglet **Configuration**, développez **Citrix ADC Gateway** et cliquez sur **Serveurs virtuels**.
    b) Dans le volet droit, double-cliquez sur le serveur virtuel et, dans le groupe **Paramètres de base**, cliquez sur l'icône Modifier.
    c) Développez **Plus**, sélectionnez **Double Hop** et cliquez sur **OK** .
3. Désactivez l'authentification sur le serveur virtuel sur Citrix ADC Gateway dans la deuxième zone DMZ.
    a) Sous l'onglet **Configuration**, développez **Citrix ADC Gateway** et cliquez sur **Serveurs virtuels**.
    b) Dans le volet droit, double-cliquez sur le serveur virtuel et, dans le groupe **Paramètres de base**, cliquez sur l'icône Modifier.
    c) Développez **Plus**et **désactivez Activer l'authentification**.
4. Activez l'une des appliances Citrix ADC Gateway pour exporter les enregistrements TCP.
    a) Sous l'onglet **Configuration**, développez **Citrix ADC Gateway** et cliquez sur **Serveurs virtuels**.
    b) Dans le volet droit, double-cliquez sur le serveur virtuel et, dans le groupe Avancé, développez Stratégies.
    c) Cliquez sur l'icône + et dans la liste **Choisir une stratégie**, sélectionnez **AppFlow** et dans la liste **Choisir un type**, sélectionnez **Autre demande TCP**.
    d) Cliquez sur **Continue**.
    e) Ajoutez une liaison de stratégie, puis cliquez sur **Fermer**.
5. Activez l'autre appliance Citrix ADC Gateway pour exporter les enregistrements ICA :

a) Sous l'onglet **Configuration**, développez **Citrix ADC Gateway** et cliquez sur **Serveurs virtuels**.

b) Dans le volet droit, double-cliquez sur le serveur virtuel et, dans le groupe **Avancé**, développez **Stratégies**.

c) Cliquez sur l'icône + et dans la liste **Choisir une stratégie**, sélectionnez **AppFlow** et dans la liste **Choisir un type**, sélectionnez **Autre demande TCP**.

d) Cliquez sur **Continue**.

e) Ajoutez une liaison de stratégie, puis cliquez sur **Fermer**.

6. Activez le chaînage des connexions sur les deux appliances Citrix ADC 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) Sélectionnez **Chaîne de connexion** et cliquez sur **OK** .

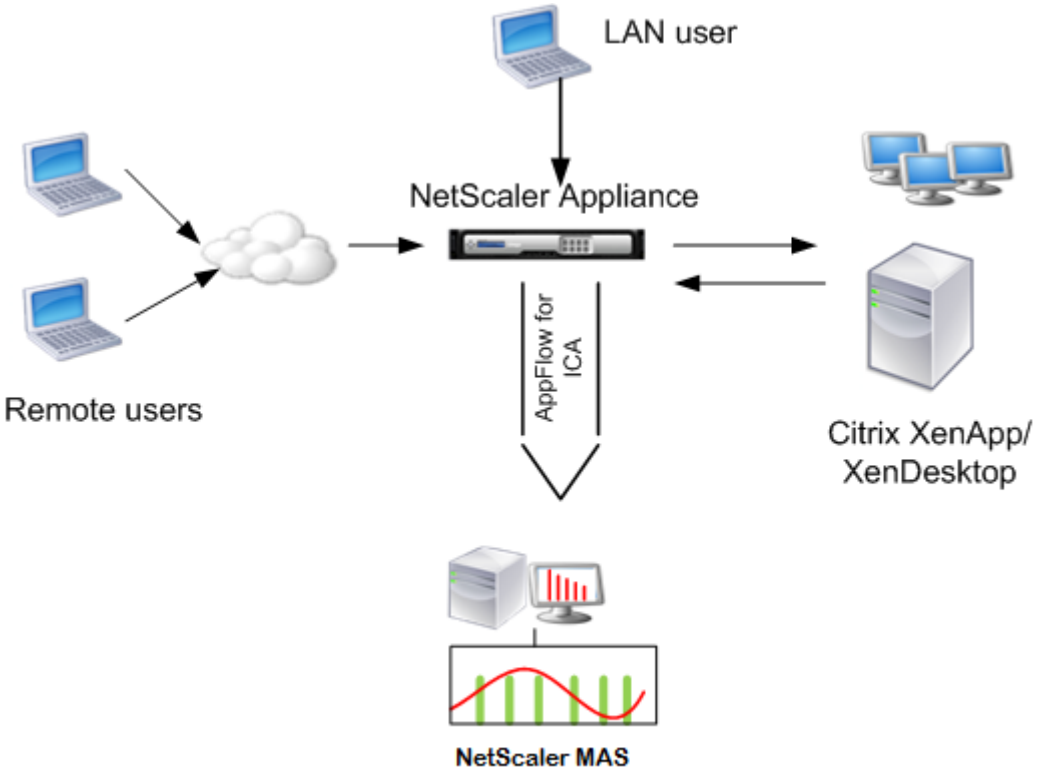
Activer la collecte de données pour surveiller les Citrix ADC déployés en mode utilisateur LAN

April 29, 2021

Les utilisateurs externes qui accèdent aux applications Citrix Virtual App ou Desktop doivent s'authentifier sur Citrix ADC Gateway. Toutefois, les utilisateurs internes peuvent ne pas avoir besoin d'être redirigés vers la passerelle ADC. 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 de réseau local puissent se connecter directement aux applications Citrix Virtual App and Desktop, vous pouvez déployer l'appliance ADC en mode utilisateur LAN en configurant un serveur virtuel de redirection de cache. Le serveur virtuel de redirection de cache agit comme un proxy SOCKS sur l'appliance de passerelle ADC.

L'image suivante illustre Citrix Application Delivery Management (ADM) déployé en **mode utilisateur LAN**.



> **Remarque**
>
> L'appliance Citrix ADC Gateway doit pouvoir atteindre l'agent Citrix ADM.

Pour surveiller les appliances Citrix ADC déployées dans ce mode, ajoutez d'abord l'appliance Citrix ADC à l'inventaire Citrix ADC Insight, activez AppFlow, puis affichez les rapports sur le tableau de bord.

Après avoir ajouté l'appliance Citrix ADC à l'inventaire Citrix ADM, vous devez activer AppFlow pour la collecte de données.

> **Remarque**
>
> - Vous ne pouvez pas activer la collecte de données sur un Citrix ADC déployé en mode utilisateur LAN à l'aide de l'utilitaire de configuration Citrix ADM.
> - Pour plus d'informations sur les commandes et leur utilisation, voir 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 Citrix ADC à l'aide de l'interface de ligne de commande :

À l'invite de commandes, procédez comme suit :

1. Connectez-vous à l'appliance Citrix ADC.

2. Ajoutez un serveur virtuel de redirection de cache proxy aval avec l'adresse IP et le port proxy, et spécifiez le type de service en tant que HDX.

```
add cr vserver <name> <servicetype> [<ipaddress> <port>] [-
   cacheType <cachetype>] [ - cltTimeout <secs>]
<!--NeedCopy-->
```

Exemple :

```
add cr vserver cr1 HDX 10.12.2.2 443  - cacheType FORWARD  -
   cltTimeout 180
<!--NeedCopy-->
```

> **Remarque**
>
> Si vous accédez au réseau LAN à l'aide d'une appliance Citrix ADC Gateway, ajoutez une action pour appliquer une stratégie qui correspond au trafic VPN.

```
add vpn trafficAction** <name> <qual> [-HDX ( ON | OFF )]

add vpn trafficPolicy** <name> <rule> <action>
<!--NeedCopy-->
```

Exemple :

```
add vpn trafficAction act1 tcp -HDX ON

add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
<!--NeedCopy-->
```

3. Ajoutez Citrix ADM en tant que collecteur AppFlow sur l'appliance Citrix ADC.

```
add appflow collector** <name> \*\*-IPAddress\*\* <ip_addr>
<!--NeedCopy-->
```

Exemple :

```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```

4. Créez une action AppFlow et associez le collecteur à l'action.

```
add appflow action** <name> \*\*-collectors\*\* <string> ...
<!--NeedCopy-->
```

Exemple :


```
add appflow action act -collectors MyInsight
<!--NeedCopy-->
```

5. Créez une stratégie AppFlow pour spécifier la règle de génération du trafic.

```
add appflow policy** <policyname> <rule> <action>
<!--NeedCopy-->
```

Exemple :

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. Liez la stratégie AppFlow à un point de liaison global.

```
bind appflow global** <policyname> <priority> \*\*-type\*\* <type>
<!--NeedCopy-->
```

Exemple :

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--NeedCopy-->
```

> **Remarque**
>
> La valeur de type doit être ICA_REQ_OVERRIDE ou ICA_REQ_DEFAULT pour s'appliquer au trafic ICA.

7. Définissez la valeur du paramètre FlowRecordInterval pour AppFlow sur 60 secondes.

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

Exemple :

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

8. Enregistrez la configuration.

```
save ns config
<!--NeedCopy-->
```


Créer des seuils et configurer des alertes pour HDX Insight

April 29, 2021

HDX Insight on Citrix Application Delivery Management (ADM) vous permet de surveiller le trafic HDX passant 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 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 plusieurs 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. Maintenant, cette gestion des seuils est étendue pour configurer un groupe de règles de seuil. Vous pouvez désormais surveiller le groupe au lieu de règles individuelles. Un groupe de règles de seuil comprend une ou plusieurs règles de seuil définies par l'utilisateur pour les mesures choisies à partir d'entités telles que les utilisateurs, les applications et les postes de travail. Chaque règle est surveillée par rapport à une valeur attendue que vous entrez lors de la création de la règle. Dans l'entité utilisateurs, 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 sur le nombre total de lancements de session ainsi que sur le nombre de lancements d'application en tant que groupe de seuils. Une alerte n'est générée que si les deux règles sont enfreintes. Cela vous permet de définir des seuils plus réalistes sur une entité.

Voici quelques exemples :

- Règle de seuil1 : la RTT ICA (métrique) pour les utilisateurs (entité) doit être <= 100 ms
- Règle de seuil2 : la latence WAN (métrique) pour les utilisateurs (entité) doit être <= 100 ms

Un exemple de groupe de seuil peut être : {Règle de seuil 1 + Règle de seuil 2}

Pour créer une règle, vous devez d'abord sélectionner l'entité que vous souhaitez surveiller. Choisissez ensuite une mesure lors de la création d'une règle. Par exemple, vous pouvez sélectionner l'entité applications, puis sélectionner Nombre **total de lancements de session ou Nombre de lancements d'applications**. Vous pouvez créer une règle pour chaque combinaison d'une entité et d'une mesure. Utilisez les comparateurs fournis (>, <, >= et <=) et tapez une valeur seuil pour chaque mesure.

> **Remarque**
>
> Si vous ne souhaitez pas surveiller plusieurs entités dans 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 signifier une violation 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 ou recevoir l'alerte sous la forme d'un e-mail ou des deux, ou sous forme de 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 à Géolocalisations pour la surveillance géographique spécifique de l'entité utilisateur.

Exemples de cas d'utilisation

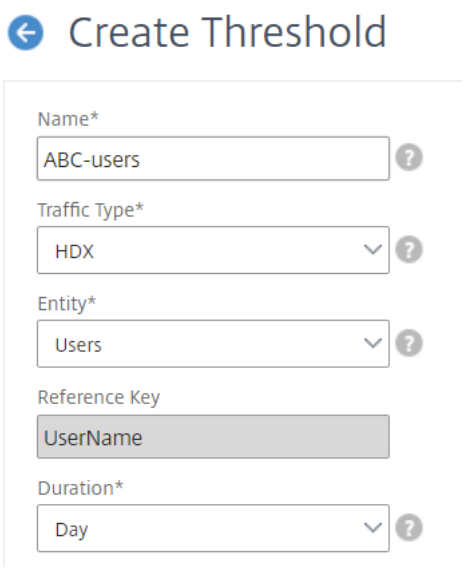
ABC Inc. est une entreprise mondiale et possède des bureaux dans plus de 50 pays. L'entreprise dispose de deux centres de données, l'un à Singapour et l'autre en Californie qui hébergent Citrix Virtual Apps and Desktops. Les employés de l'entreprise accèdent aux Citrix Virtual Apps and Desktops partout dans le monde à l'aide de Citrix ADC Gateway et de la redirection basée sur GSLB. Eric, l'administrateur Citrix Virtual Apps and Desktops pour ABC Inc. souhaite suivre l'expérience utilisateur de tous leurs bureaux afin d'optimiser la distribution des applications et des postes de travail pour un accès en tout lieu et en tout temps. Eric veut également vérifier les paramètres de l'expérience utilisateur tels que 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 alors que le même pour un emplacement distant peut être d'environ 100 ms.

Avec la gestion des groupes de règles de seuil pour HDX Insight, Eric peut définir des groupes de règles de seuil spécifiques à chaque emplacement et être averti par e-mail ou SMS des violations par zone. Eric est également capable de combiner le suivi de plusieurs mesures au sein d'un groupe de règles de seuil et de réduire la cause principale aux problèmes de capacité, le cas échéant. Eric est désormais en mesure de suivre de manière proactive toute déviation sans avoir à se soucier de la complexité de la recherche manuelle de toutes les mesures du portefeuille Citrix Virtual Apps and Desktops.

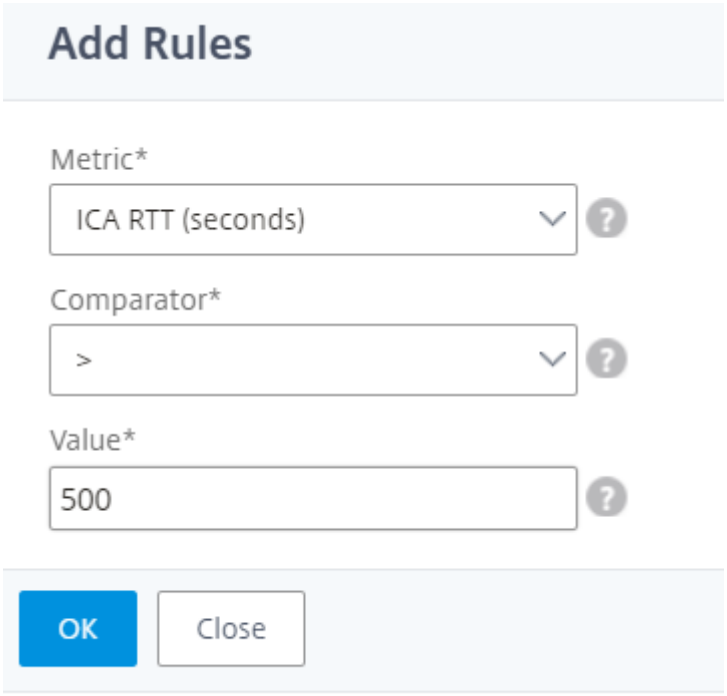
Créer un groupe de règles de seuil et configurer des alertes pour HDX Insight à l'aide de Citrix ADM

1. Dans Citrix ADM, accédez à **Analytics** > **Paramètres** > **Seuils**. Dans la page **Seuils** qui s'ouvre, cliquez sur **Ajouter**.
2. Dans la page **Créer des seuils et des alertes**, spécifiez les détails suivants :
   a) **Nom**. Saisissez un nom pour créer un événement pour lequel Citrix ADM génère une alerte.
   b) **Type de trafic**. Dans la zone de liste déroulante, sélectionnez HDX.
   c) **Entité**. Dans la zone de 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 générée automatiquement en fonction du type de trafic et de l'entité que vous avez sélectionnés.
   e) **Durée**. Dans la zone de liste déroulante, 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.

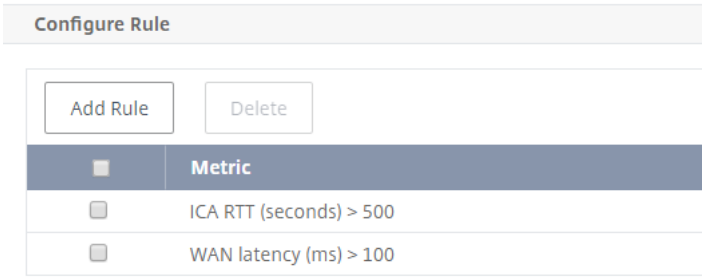


3. **Création d'un groupe de règles de seuil pour toutes les entités :**

   Pour le trafic HDX, vous devez créer une règle en cliquant sur **Ajouter une règle**. Entrez les valeurs dans la fenêtre contextuelle **Ajouter des règles** qui s'ouvre.

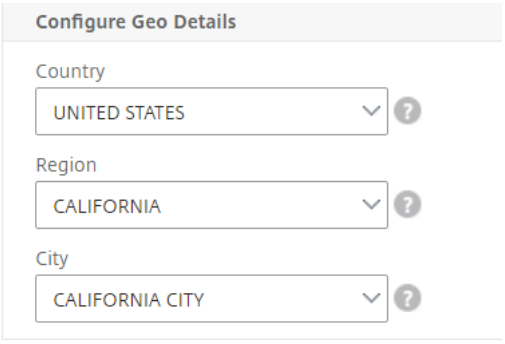


Vous pouvez créer plusieurs règles pour surveiller chaque entité. La création de plusieurs règles dans un seul groupe vous permet de surveiller les entités sous la forme d'un groupe de règles de seuil plutôt que de règles individuelles. Cliquez sur **OK** pour fermer la fenêtre.

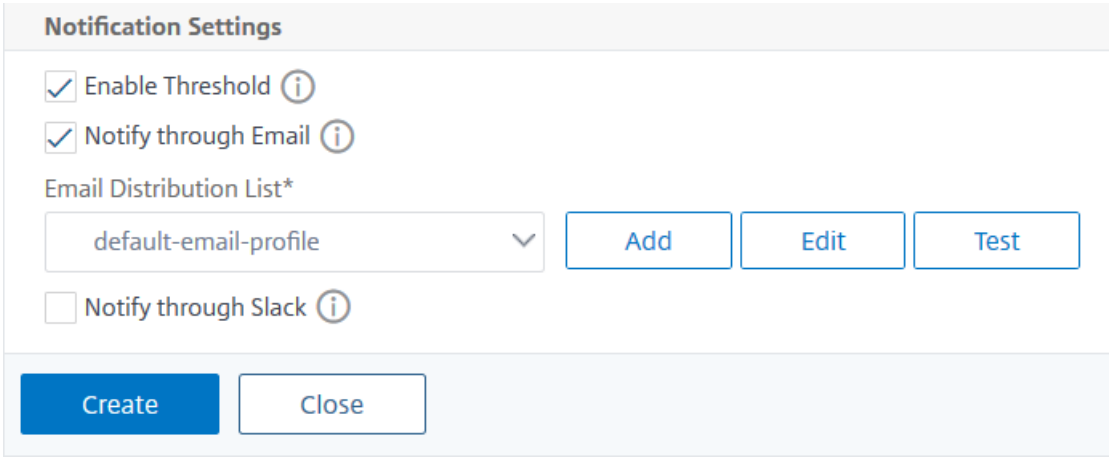


4. **Configuration du balisage de géolocalisation pour l'entité Utilisateurs :**

   Vous pouvez éventuellement créer une alerte basée sur l'emplacement pour l'entité utilisateur dans la section **Configurer les détails géographiques** . L'image suivante montre un exemple de création d'un balisage basé sur la géolocalisation pour surveiller les performances de latence WAN pour les utilisateurs de la côte ouest des États-Unis.



5. Cliquez sur **Activer les seuils** pour permettre à Citrix ADM de commencer à surveiller les entités.
6. Vous pouvez également configurer des actions telles que les notifications par e-mail et Slack.



7. Cliquez sur **Créer** pour créer un groupe de règles de seuil.

Afficher les rapports et les mesures HDX Insight

April 29, 2021

HDX Insight fournit une visibilité complète des rapports et des mesures relatifs au trafic HDX sur vos instances Citrix ADC.

Vous pouvez afficher les mesures HDX pour 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 pour le nombre total d'applications, ainsi que toutes les informations pertinentes connexes, telles que le nombre total de fois où les applications ont été lancées dans l'intervalle de temps spécifié.

- **Instances** : affiche les rapports sur les instances ADC qui agissent comme des passerelles pour le trafic entrant.
- **Postes de travail** : affiche les rapports pour les postes de travail 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 ADC SD-WAN.

Ce document comprend les éléments suivants :

Rapports et mesures d'affichage des applications

April 29, 2021

Les rapports et les mesures de cette vue sont axés sur Citrix Virtual Apps. Accédez à **Analytics** > **HDX Insight** > **Applications**

Vue récapitulative

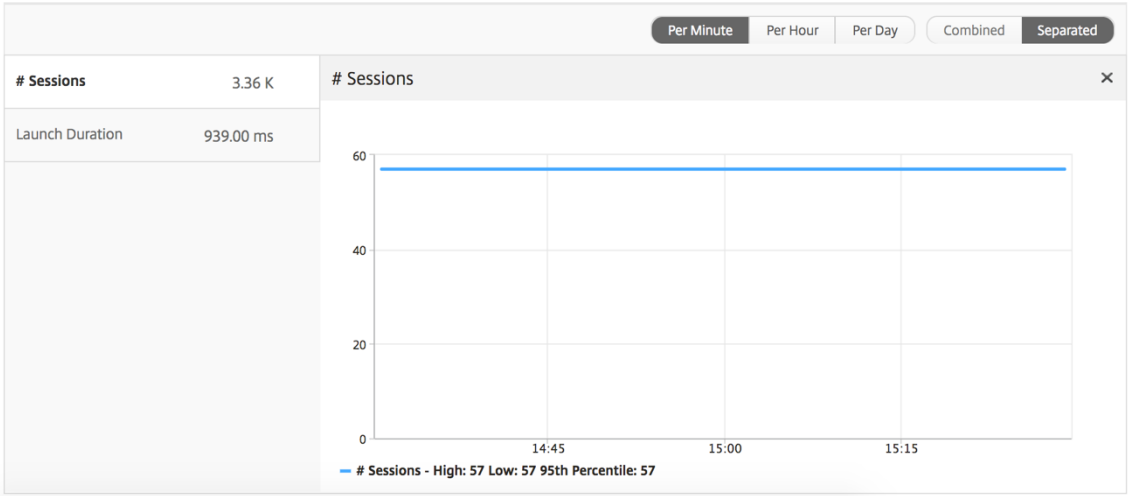
La vue récapitulative affiche les rapports de toutes les applications qui sont connectées au cours de la chronologie sélectionnée.

Toutes les métriques/rapports, sauf mention explicite, auront les valeurs qui leur correspondent pour la période de sélection.

Graphique en courbes

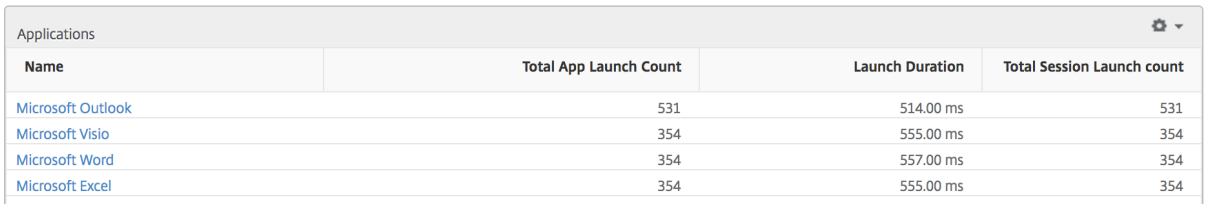
Mesures	Description
Nbre de sessions	Nombre total de sessions au cours d'un intervalle de temps donné.

Mesures	Description
Durée du lancement	Temps moyen requis pour lancer une application.



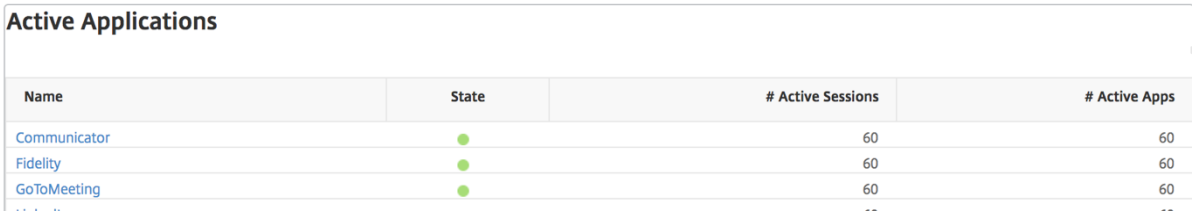
Rapport de synthèse des applications

Mesures	Description
Nom	Nom de Citrix Virtual Apps.
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 d'applications Citrix Virtual Apps lancées au cours de l'intervalle de temps donné.
Durée de lancement	Temps moyen requis pour lancer Citrix Virtual Apps.



Rapport sur les applications actives

Mesures	Description
Nom	Nom de Citrix Virtual Apps.
État	Affiche l'état de l'application : Green-Active, Rouge-Inactif
Nbre de sessions actives	Nombre de sessions utilisateur actives utilisant cette application pendant un intervalle de temps donné.
Nbre d'applications actives	Nombre de sessions actives pour cette application.

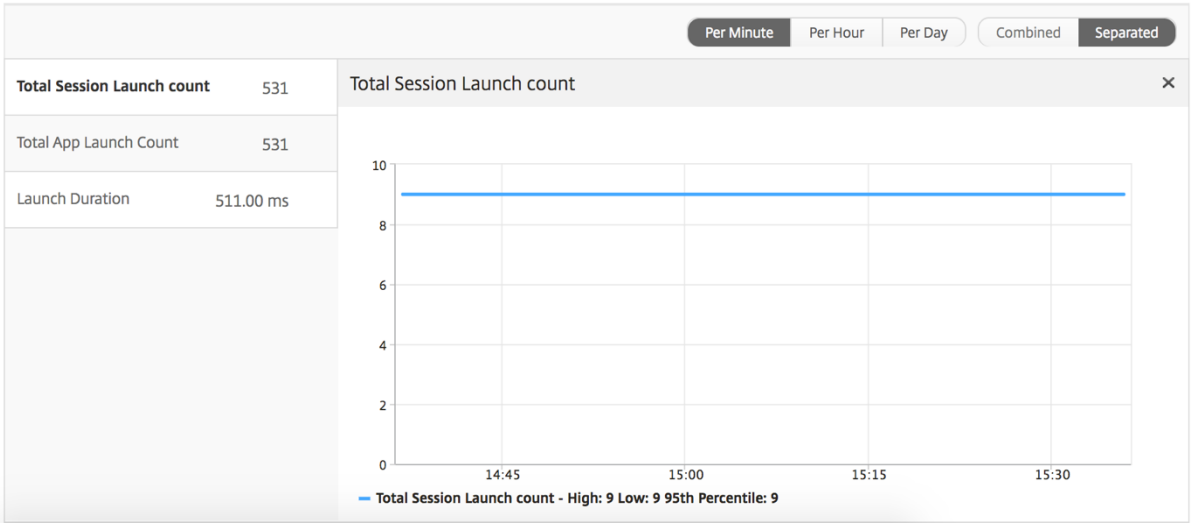


Rapport sur les seuils

L'état des seuils représente le nombre de seuils violés lorsque l'*entité* est sélectionnée comme application dans la période sélectionnée.

Graphique en courbes

Mesures	Description
Nbre 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.



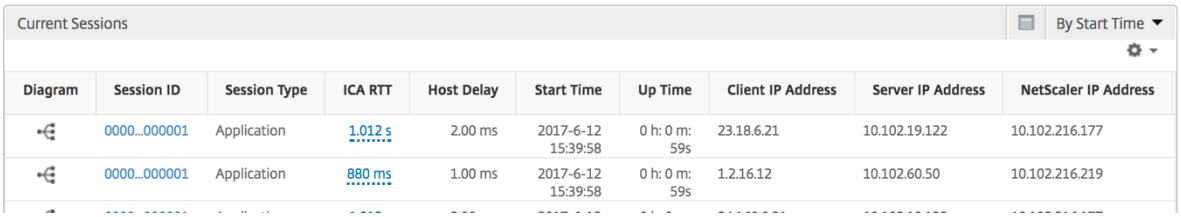
Rapport sur les sessions en cours

Mesures	Description
ID de session	Une identité unique pour une session ICA.
Type de session	Application/Ordinateur de bureau.
État	Vert/Rouge pour les sessions actives/inactives.
Délai d'hôte	Délai moyen du trafic ICA qui passe par les Citrix ADC causés par le réseau de serveurs.
Bande passante par intervalle	Bande passante consommée par la session pendant cet intervalle de temps particulier.
Bande passante de session	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.
Heure de début	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	IP du serveur dorsal/Citrix Virtual Apps.
Adresse IP NetScaler	NetScaler Management IP (NSIP).
Type de client	Type de récepteur : Client Windows Citrix.
Version du client	Version de Receiver.

Mesures	Description
MSI	Booléen (Oui/Non). Indique si la session est une ICA multi-flux.
Reconnexions de session	Nombre de fois que la session a été reconnectée.
Nb d'ACR	Nombre total de fois qu'un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, utilisateur/mode transparent Citrix ADC Gateway.
Pays	Pays à partir duquel la session a été créée.
Région	Région à partir de laquelle la session a été établie.
Ville	Ville à partir de laquelle la session a été établie.
État USB	Actif/Inactif -Vert/Rouge.
Nombre d'instances USB acceptées	Nombre d'instances USB acceptées.
Nombre d'instances USB rejetées	Nombre d'instances USB rejetées.
Nombre d'instances USB arrêtées	Nombre d'instances USB arrêtées.
Nom d'hôte du client	Nom d'hôte du client.
Nombre de basculements haute disponibilité	Nombre de fois où le basculement HA s'est produit.
Motif de l'arrêt	Affiche le motif de la fin d'une session. Par exemple, ICA Session Timeout, Session interrompue par l'utilisateur.
RTT ICA	RTT ICA est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps ou Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de Citrix ADC aux serveurs back-end.

Mesures	Description
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 sur 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 que le client a annoncé une fenêtre TCP zéro.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit pendant la connexion entre Citrix ADC et l'utilisateur final.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois que le serveur a annoncé une fenêtre TCP zéro.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit sur la connexion entre Citrix ADC et le serveur principal.
Nom d'utilisateur	Nom d'utilisateur de l'utilisateur accédant à cette application virtuelle Citrix particulière.
ID de session	Identifiant unique pour la session Citrix Virtual App.
Type de session	Sera « Application ».
État	État de la session : vert pour actif, rouge pour inactif.
Latence maximale de violation	Valeur la plus élevée de la latence L7 lorsqu'une violation d'un seuil défini pour un intervalle de temps défini se produit.
Latence moyenne de violation	Valeur moyenne de latence L7 lorsque le système est dans un état « L7 latence brisé ».

Mesures	Description
Nombre de violations du seuil L7	Nombre de fois qu'une violation du seuil L7 s'est produite.
Latence côté client L7	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 le périphérique Citrix ADC et Citrix Virtual Apps. Cette mesure est utile pour les périphériques non Citrix présents dans le chemin de remise.



Vue par session d'application

La vue par session d'application affiche des rapports pour une session d'application particulière sélectionnée.

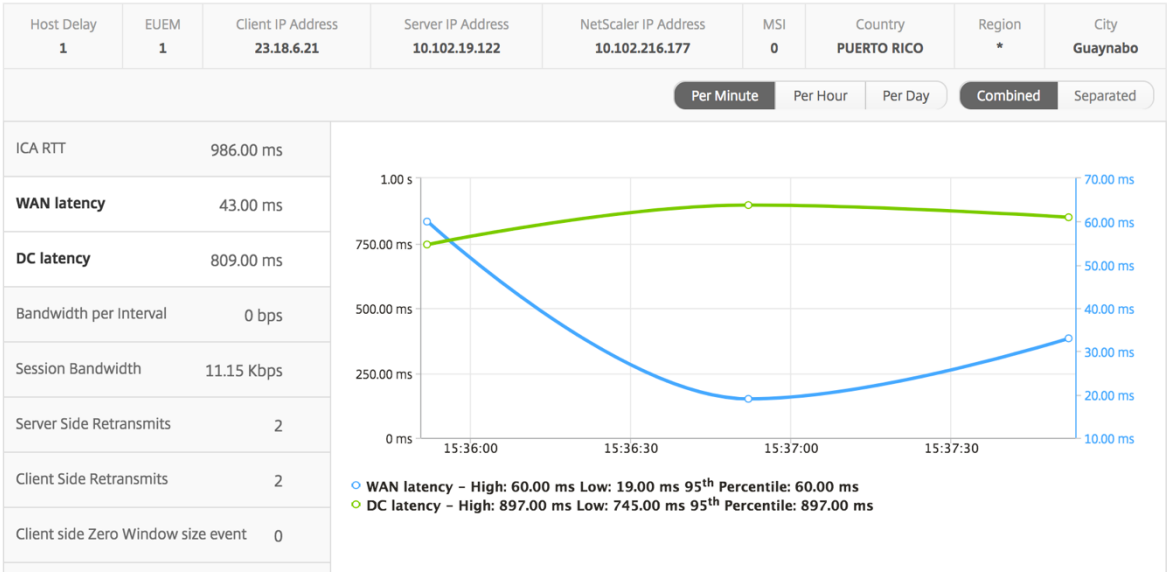
Pour afficher les rapports de session :

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

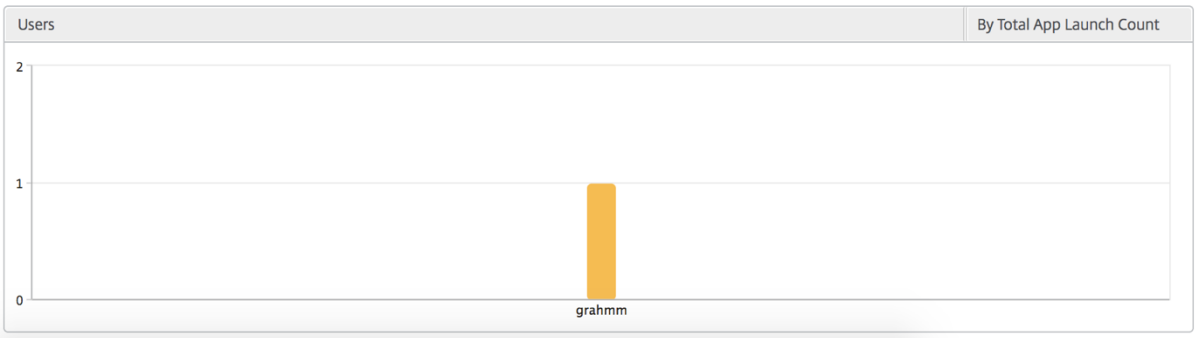
Mesures	Description
Reconnexions de session	Nombre de fois que la session a été reconnectée.
Nb d'ACR	Nombre total de fois qu'un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.

Mesures	Description
RTT ICA	RTT ICA est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps ou Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de Citrix ADC à l'utilisateur final.
Événement de taille de fenêtre nulle côté serveur	Latence causée par le côté serveur du réseau. C'est-à-dire, de Citrix ADC aux serveurs back-end.
Bande passante par intervalle	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 sur 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	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 que le serveur a annoncé une fenêtre TCP zéro.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit pendant la connexion entre Citrix ADC et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit sur la connexion entre Citrix ADC et le serveur 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 **utilisateur** représente les utilisateurs connectés à cette application particulière.



Rapports et mesures d’affichage du Bureau

April 29, 2021

Les rapports et les mesures de cette vue sont centrés sur Citrix Virtual Desktop. Accédez à **Analytics** > **HDX Insight** > **Bureau**

Vue récapitulative

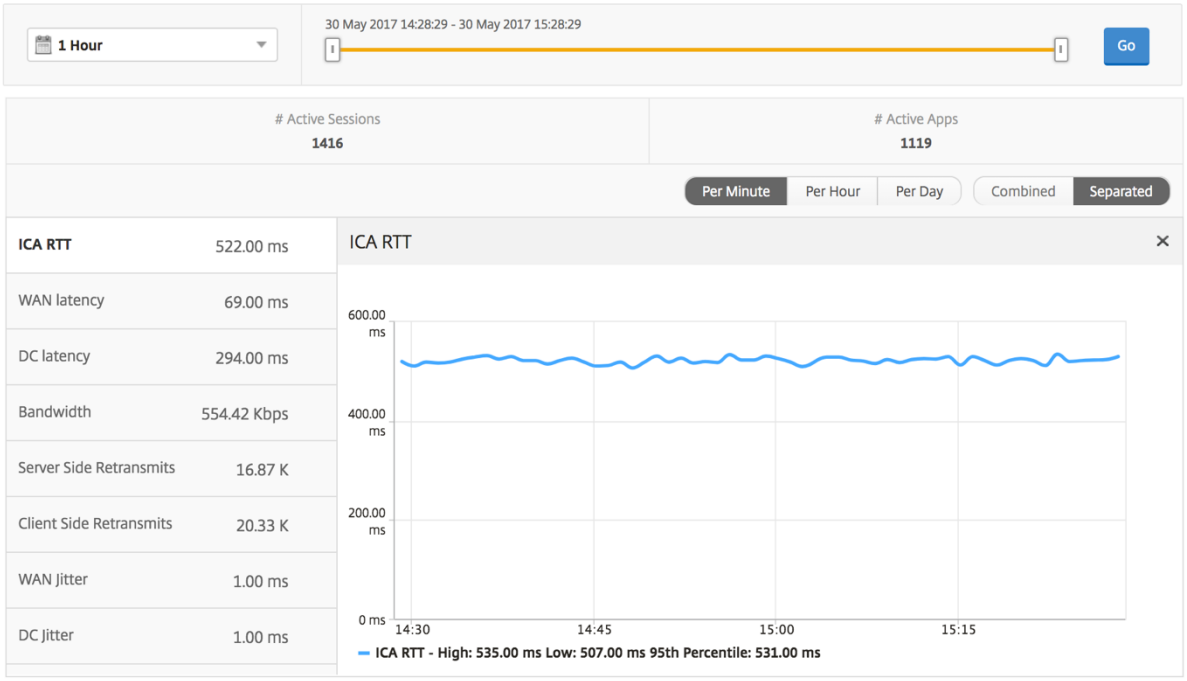
La vue récapitulative affiche les rapports de tous les Citrix Virtual Desktops qui sont connectés au cours de la chronologie sélectionnée.

Tous les compteurs/rapports ci-dessous, sauf mention explicite, auront les valeurs qui leur correspondent pour la période sélectionnée.

Graphique en courbes

Mesures	Description
Nbre 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	RTT ICA est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps ou Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de Citrix ADC aux serveurs back-end.
Bande passante	Nombre total d'octets par seconde 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 sur 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 pendant la connexion entre Citrix ADC et l'utilisateur final.

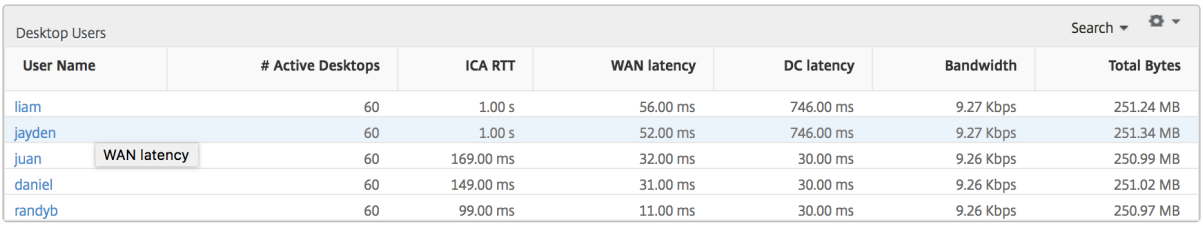
Mesures	Description
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit sur la connexion entre Citrix ADC et le serveur principal.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois que le client a annoncé une fenêtre TCP zéro.
Événement 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

Mesures	Description
Active Sessions	Nombre total de sessions Citrix Virtual Desktops 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.

Mesures	Description
RTT ICA	RTT ICA est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps ou Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de Citrix ADC aux serveurs back-end.
Bande passante	Nombre total d'octets par seconde pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Nb total d'octets	Nombre total d'octets consommés par l'utilisateur pendant la période sélectionnée.



Rapport sur les seuils

Le rapport de seuil représente le nombre de seuils dépassés lorsque l'*entité* est sélectionnée en tant que Bureau au cours de la période sélectionnée.

Par affichage de bureau

La vue par poste de travail fournit des rapports détaillés sur l'expérience utilisateur final pour un Citrix Virtual Desktop sélectionné.

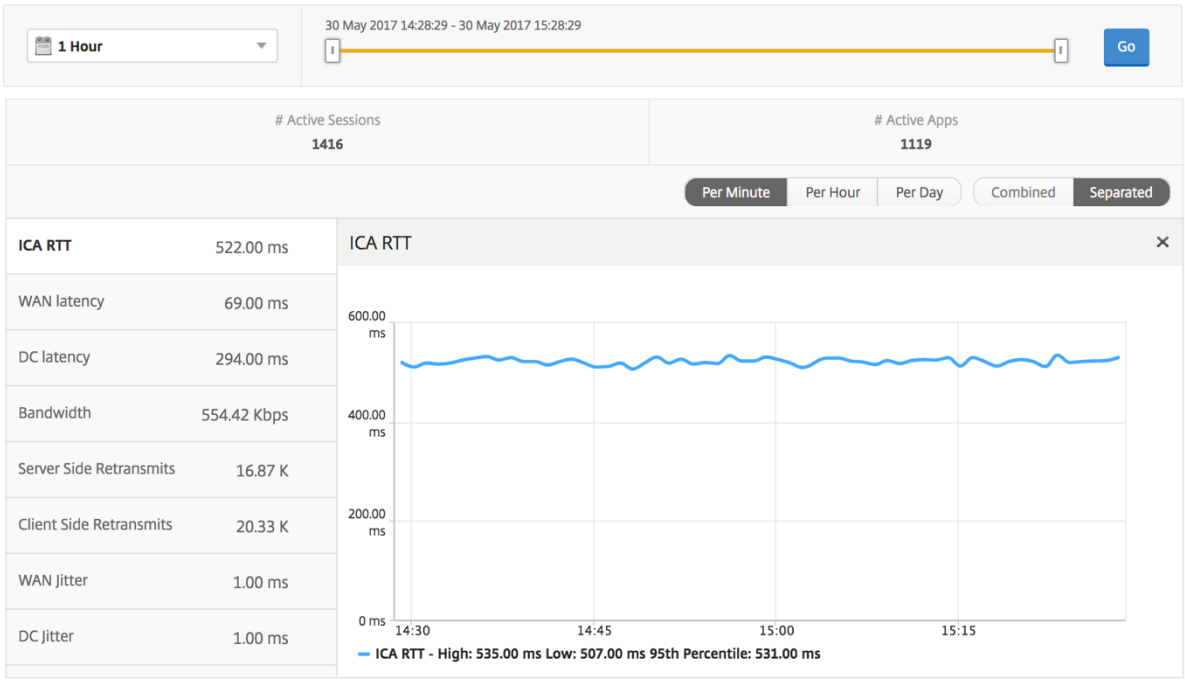
Pour accéder à la vue Bureau particulière :

1. Accédez à **Analytics > HDX Insight > Bureau**.
2. Sélectionnez un **poste de travail** particulier dans le **rapport récapitulatif des postes** de travail.

Graphique en courbes

Mesures	Description
Nbre 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	RTT ICA est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps ou Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de Citrix ADC aux serveurs back-end.
Bande passante	Nombre total d'octets par seconde 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 sur 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 pendant la connexion entre Citrix ADC et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit sur la connexion entre Citrix ADC et le serveur principal.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois que le client a annoncé une fenêtre TCP zéro.

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.

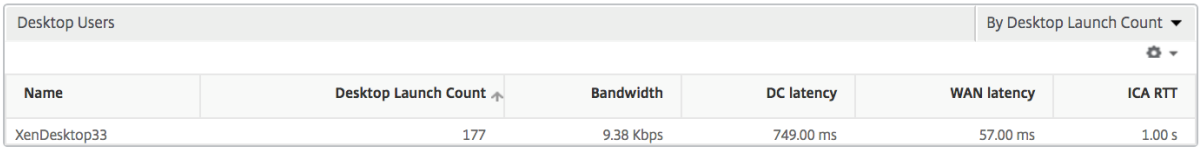


Rapport sur les utilisateurs du bureau

Ce tableau donne un aperçu des sessions Citrix Virtual Desktops pour un utilisateur particulier. Ces mesures peuvent être triées par nombre de lancements de bureau et bande passante.

Mesures	Description
Nom	Nom de Citrix Virtual Desktops.
Nb de lancements de bureaux	Nombre de fois que le bureau a été lancé.
Bande passante	Nombre total d'octets par seconde pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de Citrix ADC aux serveurs back-end.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de Citrix ADC à l'utilisateur final.

Mesures	Description
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps ou Desktops respectivement.



Rapport sur les postes de travail actifs/inactifs

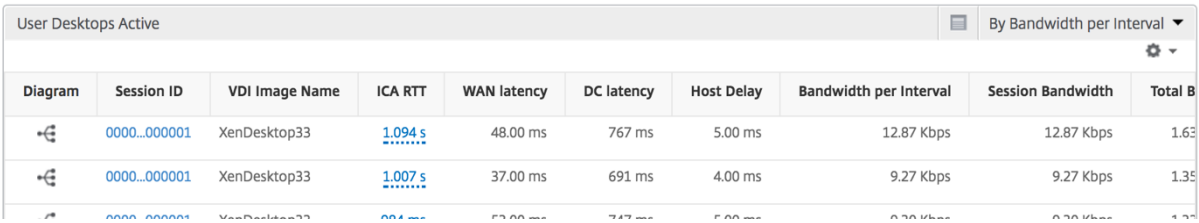
Les mesures suivantes peuvent être triées en fonction de la bande passante par intervalle, des reconnexions de session et du nombre d'ACR.

Mesures	Description
ID de session	Une identité unique pour une session ICA.
Type de session	Application/Ordinateur de bureau.
État	Vert/Rouge pour les sessions actives/inactives.
Délai d'hôte	Délai moyen du trafic ICA qui passe par les Citrix ADC causés par le réseau de serveurs.
Bande passante par intervalle	Bande passante consommée par la session pendant cet intervalle de temps particulier.
Bande passante de session	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.
Heure de début	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	IP du serveur dorsal/Citrix Virtual Apps.
Adresse IP NetScaler	NetScaler Management IP (NSIP).
Type de client	Type de récepteur - Client Windows Citrix

Mesures	Description
Version du client	Version de Receiver.
MSI	Booléen (Oui/Non). Indique si la session est une ICA multi-flux.
Reconnexions de session	Nombre de fois que la session a été reconnectée.
Nb d'ACR	Nombre total de fois qu'un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, utilisateur/mode transparent Citrix ADC Gateway.
Pays	Pays à partir duquel la session a été créée.
Région	Région à partir de laquelle la session a été établie.
Ville	Ville à partir de laquelle la session a été établie.
État USB	Actif/Inactif -Vert/Rouge.
Nombre d'instances USB acceptées	Nombre d'instances USB acceptées.
Nombre d'instances USB rejetées	Nombre d'instances USB rejetées.
Nombre d'instances USB arrêtées	Nombre d'instances USB arrêtées.
Nom d'hôte du client	Nom d'hôte du client.
Nombre de basculements haute disponibilité	Nombre de fois où le basculement HA s'est produit.
Motif de l'arrêt	Affiche le motif de la fin d'une session. Par exemple, ICA Session Timeout, Session interrompue par l'utilisateur.
RTT ICA	RTT ICA est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps ou Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de Citrix ADC à l'utilisateur final.

Mesures	Description
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de Citrix ADC aux serveurs back-end.
Nb total d'octets	Nombre total d'octets consommés par l'utilisateur pendant la période sélectionnée.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis sur 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 que le client a annoncé une fenêtre TCP zéro.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit pendant la connexion entre Citrix ADC et l'utilisateur final.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois que le serveur a annoncé une fenêtre TCP zéro.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit sur la connexion entre Citrix ADC et le serveur principal.
Nom de l'image VDI	Nom du Citrix Virtual Desktops auquel l'utilisateur est connecté

Diagramme



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 de chronologie

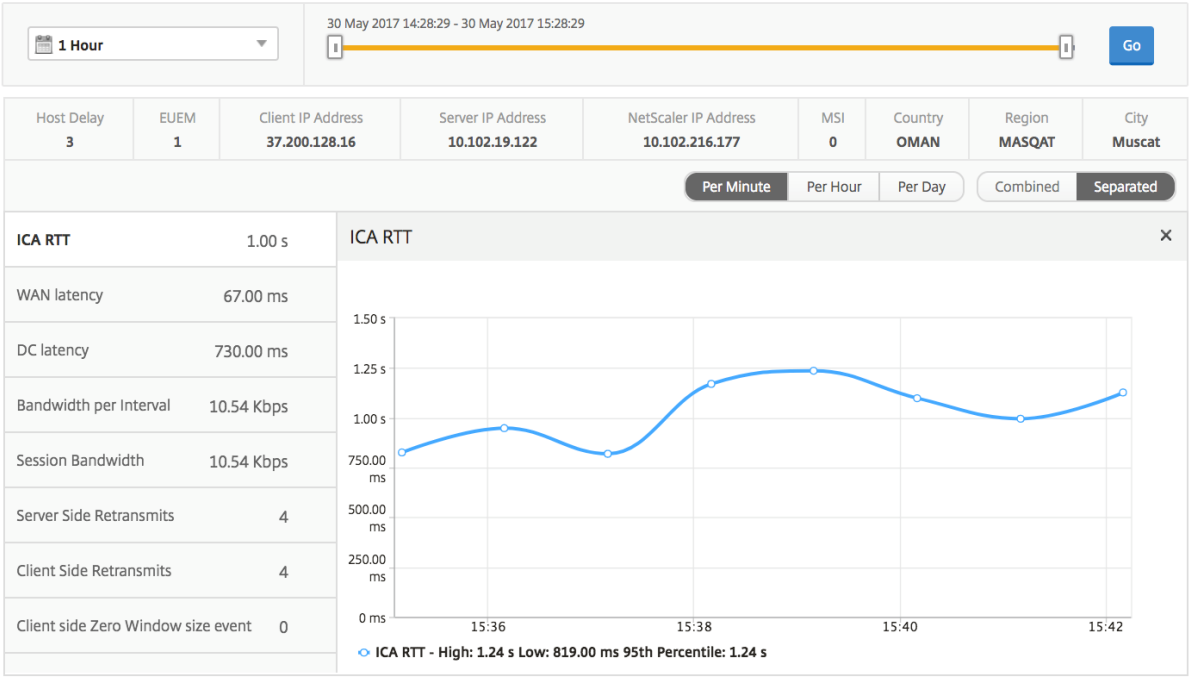
La vue de session par utilisateur fournit des rapports pour la session d'un utilisateur particulier sélectionné.

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. Select 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	RTT ICA est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps ou Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de Citrix ADC aux serveurs back-end.
Bande passante de session	Bande passante consommée par la session quel que soit l'intervalle de temps.

Mesures	Description
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis sur 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 pendant la connexion entre Citrix ADC et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit sur la connexion entre Citrix ADC et le serveur principal.
Bande passante par intervalle	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 que le serveur a annoncé une fenêtre TCP zéro.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.



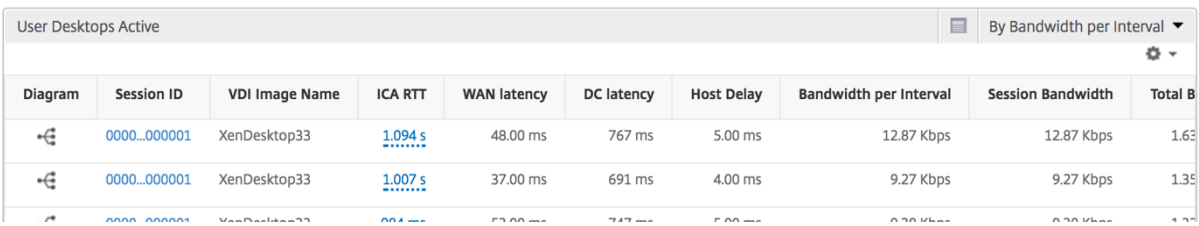
Rapport sur les sessions de bureau associées

Les mesures suivantes peuvent être triées en fonction de la bande passante par intervalle, des reconnexions de session et du nombre d'ACR.

Mesures	Description
ID de session	Une identité unique pour une session ICA.
Type de session	Application/Ordinateur de bureau.
État	Vert/Rouge pour les sessions actives/inactives.
Délai d'hôte	Délai moyen du trafic ICA qui passe par les Citrix ADC causés par le réseau de serveurs.
Bande passante par intervalle	Bande passante consommée par la session pendant cet intervalle de temps particulier.
Bande passante de session	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.
Heure de début	Heure de début de la session.
Temps d'activité	Durée de la session.
Adresse IP cliente	IP de l'utilisateur final.

Mesures	Description
Adresse IP du serveur	IP du serveur dorsal/Citrix Virtual Apps.
Adresse IP NetScaler	NetScaler Management IP (NSIP).
Type de client	Type de récepteur - Client Windows Citrix
Version du client	Version de Receiver.
MSI	Booléen (Oui/Non). Indique si la session est une ICA multi-flux.
Reconnexions de session	Nombre de fois que la session a été reconnectée.
Nb d'ACR	Nombre total de fois qu'un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, utilisateur/mode transparent Citrix ADC Gateway.
Pays	Pays à partir duquel la session a été créée.
Région	Région à partir de laquelle la session a été établie.
Ville	Ville à partir de laquelle la session a été établie.
État USB	Actif/Inactif -Vert/Rouge.
Nombre d'instances USB acceptées	Nombre d'instances USB acceptées.
Nombre d'instances USB rejetées	Nombre d'instances USB rejetées.
Nombre d'instances USB arrêtées	Nombre d'instances USB arrêtées.
Nom d'hôte du client	Nom d'hôte du client.
Nombre de basculements haute disponibilité	Nombre de fois où le basculement HA s'est produit.
Motif de l'arrêt	Affiche le motif de la fin d'une session. Par exemple, ICA Session Timeout, Session interrompue par l'utilisateur.
RTT ICA	RTT ICA est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps ou Desktops respectivement.

Mesures	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, de Citrix ADC aux serveurs back-end.
Nb total d'octets	Nombre total d'octets consommés par l'utilisateur pendant la période sélectionnée.
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis sur 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 que le client a annoncé une fenêtre TCP zéro.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit pendant la connexion entre Citrix ADC et l'utilisateur final.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois que le serveur a annoncé une fenêtre TCP zéro.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit sur la connexion entre Citrix ADC et le serveur principal.
Nom de l'image VDI	Nom du Citrix Virtual Desktops auquel l'utilisateur est connecté

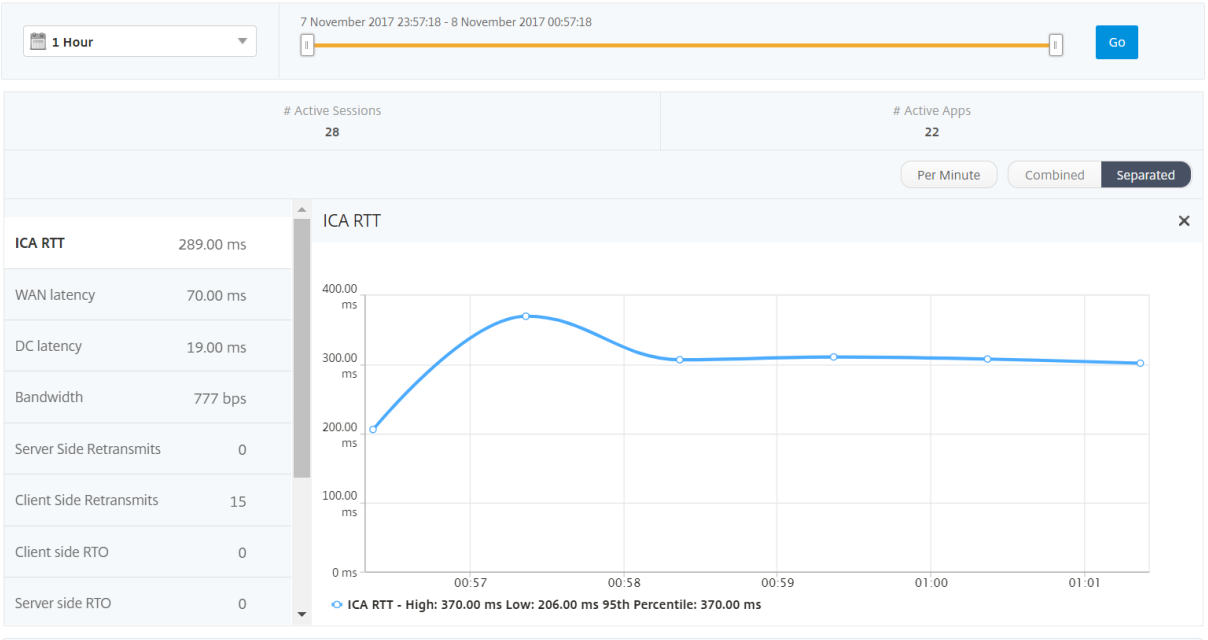


Rapports et mesures d'affichage utilisateur

April 29, 2021

Les rapports et les mesures de cette vue s'affichent par utilisateur Citrix Virtual App ou Desktop.

Accédez à **Analytics** > **HDX Insight** > **Utilisateurs**



Vue récapitulative

La vue récapitulative affiche les rapports de tous les utilisateurs qui se sont connectés au cours de la chronologie sélectionnée. Toutes les métriques/rapports de cette vue affichent les valeurs qui leur correspondent pour la période sélectionnée, sauf indication contraire.

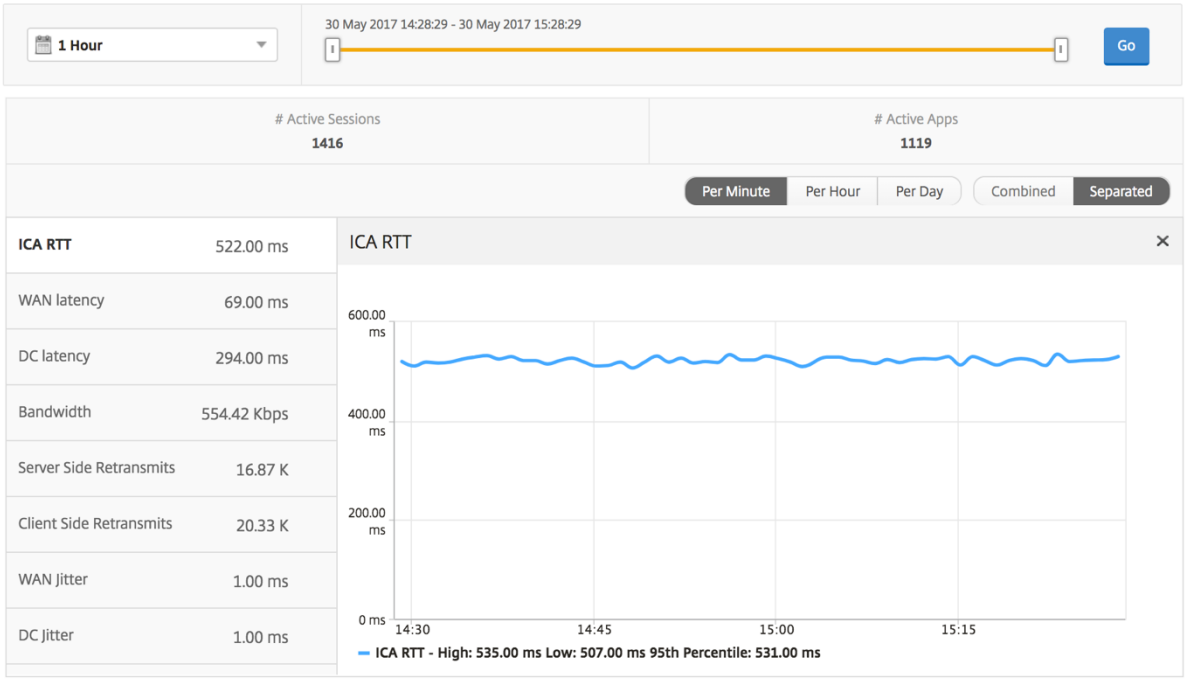
Pour modifier la période sélectionnée :

1. Utilisez la liste des périodes ou le curseur temporel pour définir l'intervalle de temps souhaité.
2. Cliquez sur **OK**.

Graphique en courbes

Mesures	Description
Nbre de sessions actives	Ce nombre indique le nombre de sessions Citrix Virtual Apps and Desktops actives.

Mesures	Description
Nbre d'applications actives	Ce nombre indique le nombre de sessions Citrix Virtual Apps actives.
RTT ICA	RTT ICA est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps ou Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de Citrix ADC aux serveurs back-end.
Bande passante	Nombre total de bits 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 sur 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 pendant la connexion entre Citrix ADC et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit sur la connexion entre Citrix ADC et le serveur principal.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois que le client a annoncé 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
Nbre 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	RTT ICA est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps ou Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de Citrix ADC aux serveurs back-end.
Bande passante	Nombre total de bits par seconde pris pour la communication de bout en bout pendant l'intervalle de temps sélectionné.

Mesures	Description
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis sur 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 pendant la connexion entre Citrix ADC et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit sur la connexion entre Citrix ADC et le serveur principal.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois que le client a annoncé une fenêtre TCP zéro.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois que le serveur a annoncé une fenêtre TCP zéro.
Nb total d'applications lancées	Total des applications lancées par l'utilisateur pendant la période sélectionnée.
Nb total d'octets	Nombre total d'octets consommés par l'utilisateur pendant la période sélectionnée.
Ordinateurs de bureau actifs	Nombre total de Citrix Virtual Desktops actifs au cours d'un intervalle de temps donné.

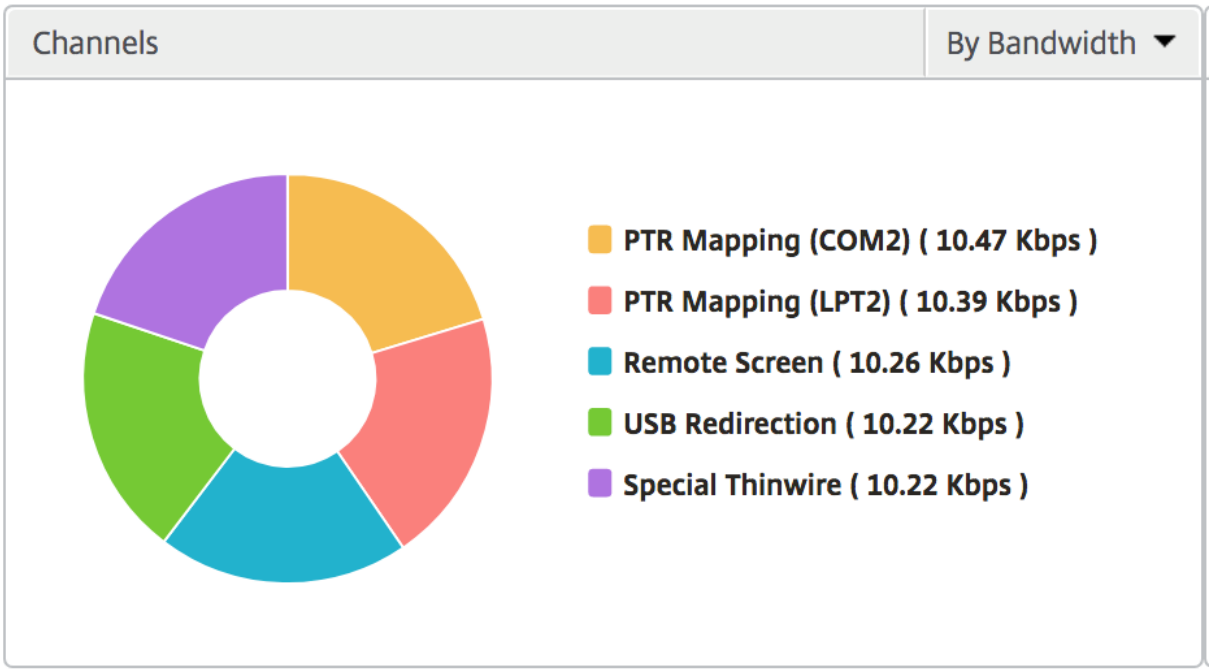
Users

Search

User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT	WAN latency	DC latency	Bandwidth	Server Side Retransmits	Cl
liam	59	59	118	999.00 ms	57.00 ms	751.00 ms	47.25 Kbps	3.74 K	
jayden	59	59	118	999.00 ms	52.00 ms	751.00 ms	47.06 Kbps	3.71 K	
florinl	59	0	59	997.00 ms	52.00 ms	754.00 ms	23.66 Kbps	1.88 K	
ramas	59	0	59	997.00 ms	778.00 ms	1.00 ms	7.03 Kbps	0	
omerp	59	0	59	997.00 ms	57.00 ms	754.00 ms	23.80 Kbps	1.89 K	
grahmm	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.80 Kbps	1.89 K	
ryan	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.69 Kbps	1.88 K	
rajivs	59	0	59	801.00 ms	11.00 ms	1.00 ms	23.97 Kbps	0	
alexisc	117	0	118	622.00 ms	56.00 ms	392.00 ms	47.67 Kbps	1.88 K	
juan	59	59	118	169.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
lennoxl	59	0	59	169.00 ms	31.00 ms	30.00 ms	23.86 Kbps	0	
daniel	59	59	118	149.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
woojunek	58	0	59	149.00 ms	31.00 ms	30.00 ms	23.85 Kbps	0	
parkerf	59	0	59	149.00 ms	31.00 ms	30.00 ms	23.88 Kbps	0	
randyb	59	59	118	99.00 ms	11.00 ms	29.00 ms	47.71 Kbps	0	
bradp	177	0	177	74.00 ms	27.00 ms	1.00 ms	71.75 Kbps	0	

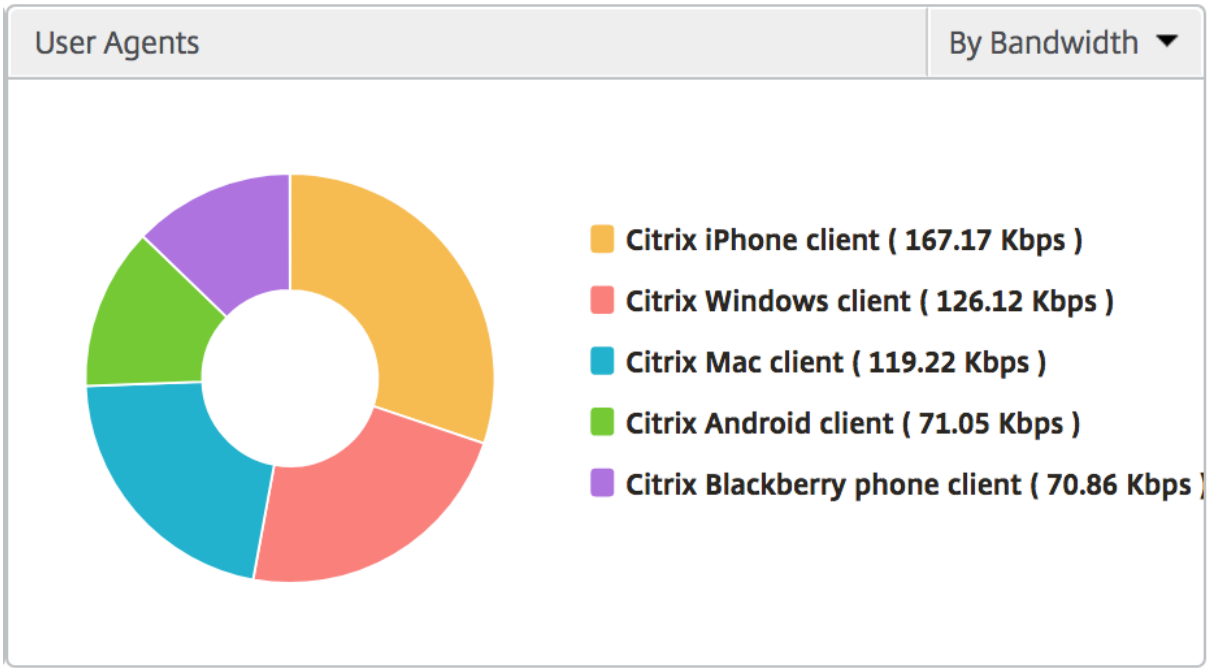
Canaux

Les canaux représentent la bande passante globale ou le nombre total d'octets consommés par chaque canal virtuel ICA sous la forme d'un graphique en beignet. Vous pouvez également trier les mesures par bande passante ou Nombre total d'octets.



Agents utilisateurs

Les agents utilisateurs représentent la bande passante globale et totale des bits 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 dépassés au cours de la période sélectionnée.

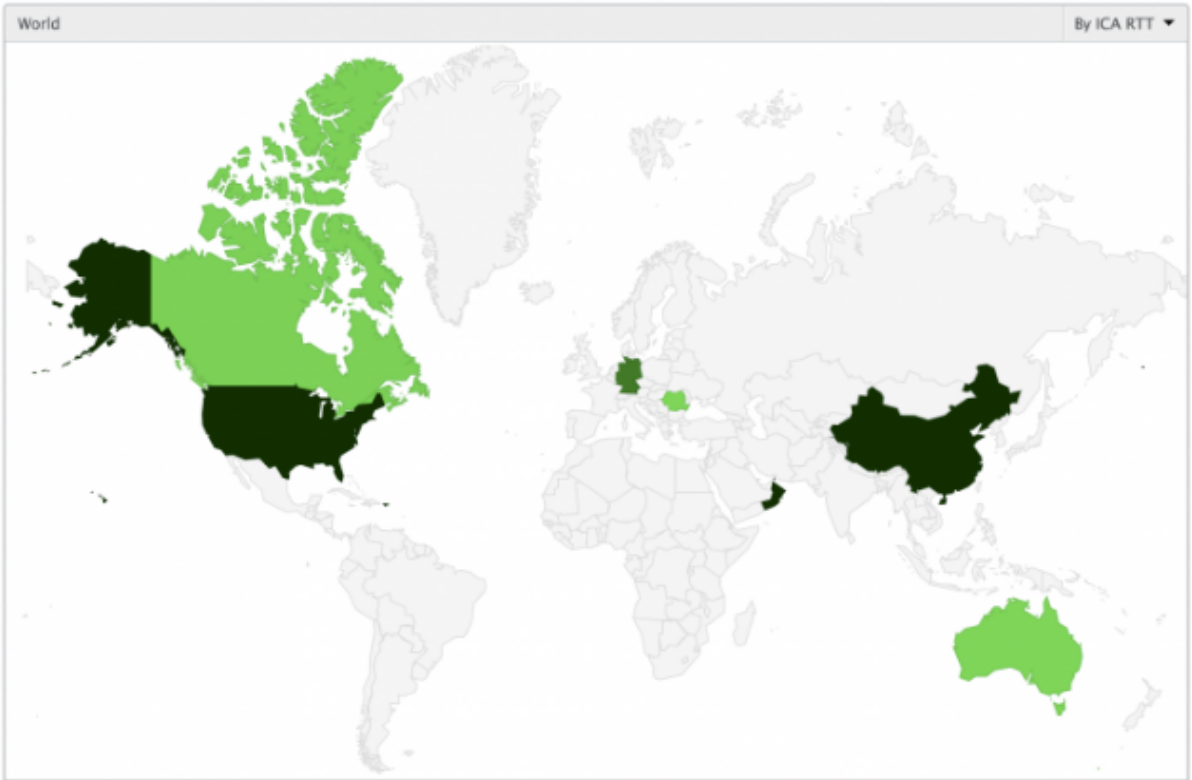
Carte du Monde

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 simplement sur la région. Les administrateurs peuvent approfondir l'exploration vers le bas pour afficher les informations par ville et par État. À partir de Citrix ADM version 12.0 et ultérieure, vous pouvez effectuer une exploration vers le bas vers les utilisateurs connectés à partir d'un emplacement géographique.

Les détails suivants peuvent être consultés sur la carte du monde dans un aperçu HDX, et la densité de chaque mesure est affichée sous la forme d'une carte thermique :

- RTT ICA
- Latence WAN

- Latence du contrôleur de domaine
- Bande passante
- Nb total d'octets



ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
523.00 ms	69.00 ms	293.00 ms	14.83 Mbps	4691.53 GB

World

Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

Par vue utilisateur

La vue par utilisateur fournit des rapports détaillés sur l'expérience utilisateur final pour tout utilisateur sélectionné.

Pour accéder aux mesures spécifiques d'un utilisateur :

1. Accédez à **Analytics** > **HDX Insight** > **Utilisateurs**.
2. Sélectionnez un utilisateur particulier dans le rapport de synthèse Utilisateurs.

Graphique en courbes

Le graphique en courbes affiche le résumé de toutes les mesures de l'utilisateur sélectionné pendant la période sélectionnée.

Rapport Sessions actuelles/terminées

Ce rapport est pertinent pour toutes les sessions utilisateur actuelles/terminées pour l'utilisateur sélectionné. Ces mesures peuvent être triées en fonction de l'heure de début, des reconnexions de session et du nombre ACR.

Mesures	Description
ID de session	Une identité unique pour une session ICA.
Type de session	Application/Ordinateur de bureau.
État	Vert/Rouge pour les sessions actives/inactives.
Délai d'hôte	Délai moyen du trafic ICA qui passe par les Citrix ADC causés par le réseau de serveurs.
Bande passante par intervalle	Bande passante consommée par la session pendant cet intervalle de temps particulier.
Bande passante de session	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.
Heure de début	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 Citrix Virtual App.
Adresse IP NetScaler	NetScaler Management IP (NSIP).
Type de client	Type de récepteur - Client Windows Citrix
Version du client	Version de Receiver.
MSI	Booléen (Oui/Non). Indique si la session est une ICA multi-flux.

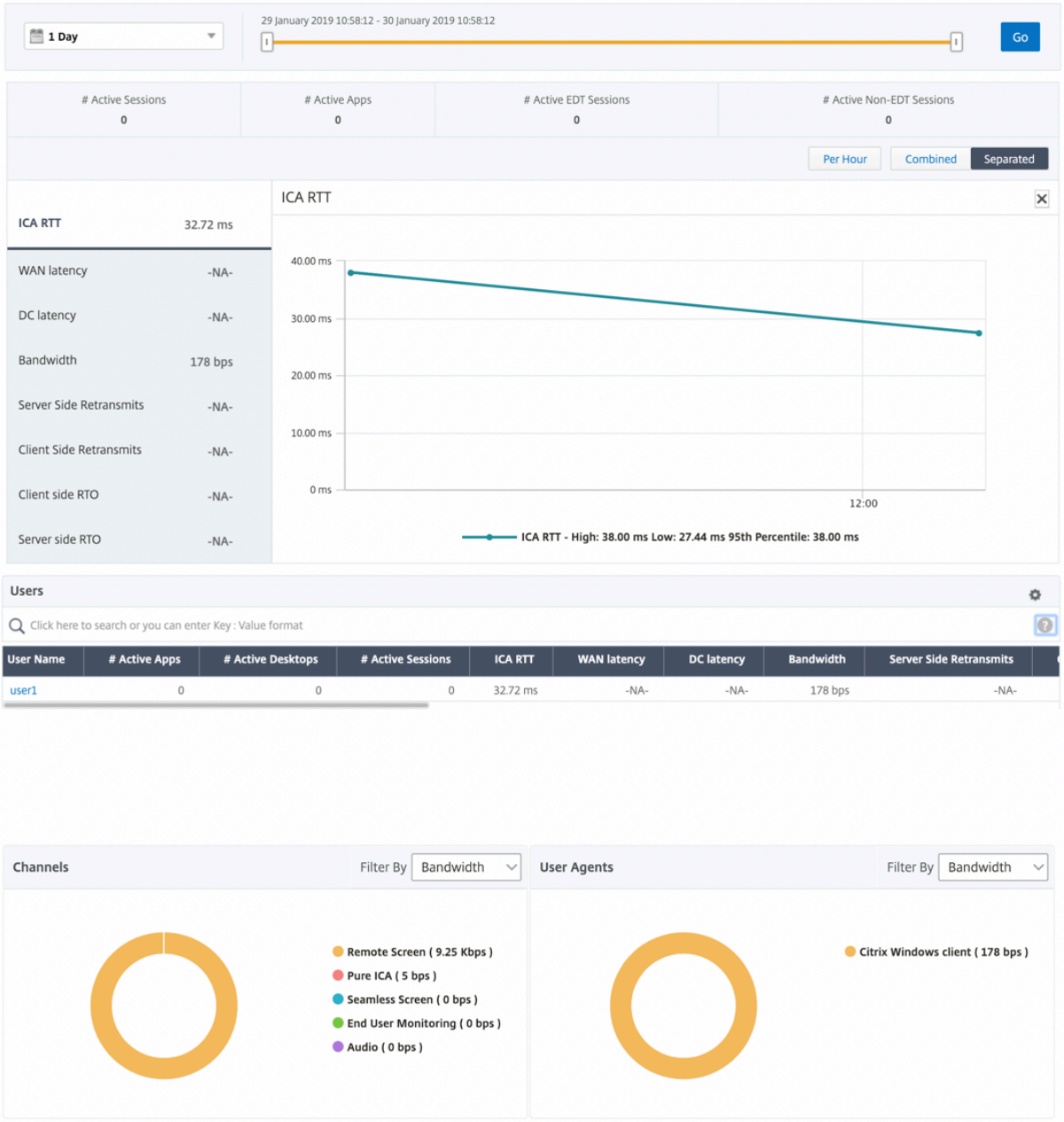
Mesures	Description
Reconnexions de session	Nombre de fois que la session a été reconnectée.
Nb d'ACR	Nombre total de fois qu'un client reconnecte automatiquement les utilisateurs aux sessions déconnectées.
Type d'accès utilisateur	Affiche le mode d'accès de la session ICA. Par exemple, utilisateur/mode transparent Citrix ADC Gateway.
Pays	Pays à partir duquel la session a été créée.
Région	Région à partir de laquelle la session a été établie.
Ville	Ville à partir de laquelle la session a été établie.
État USB	Actif/Inactif -Vert/Rouge.
Nombre d'instances USB acceptées	Nombre d'instances USB acceptées.
Nombre d'instances USB rejetées	Nombre d'instances USB rejetées.
Nombre d'instances USB arrêtées	Nombre d'instances USB arrêtées.
Nom d'hôte du client	Nom d'hôte du client.
Nombre de basculements haute disponibilité	Nombre de fois où le basculement HA s'est produit.
Motif de l'arrêt	Affiche le motif de la fin d'une session. Par exemple, ICA Session Timeout, Session interrompue par l'utilisateur.
RTT ICA	RTT ICA est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps ou Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de Citrix ADC aux serveurs back-end.
Nb total d'octets	Nombre total d'octets consommés par l'utilisateur pendant la période sélectionnée.

Mesures	Description
Retransmissions côté serveur	Nombre de paquets retransmis sur la connexion entre Citrix ADC et le serveur principal.
Retransmissions côté client	Nombre de paquets retransmis sur 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 que le client a annoncé une fenêtre TCP zéro.
RTO rapide côté client	Nombre de fois où le délai de retransmission s'est produit la connexion entre l'Citrix ADC et l'utilisateur final.
Événement de taille de fenêtre nulle côté serveur	Ce compteur indique le nombre de fois que le serveur a annoncé une fenêtre TCP zéro.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit sur la connexion entre Citrix ADC et serveur principal.

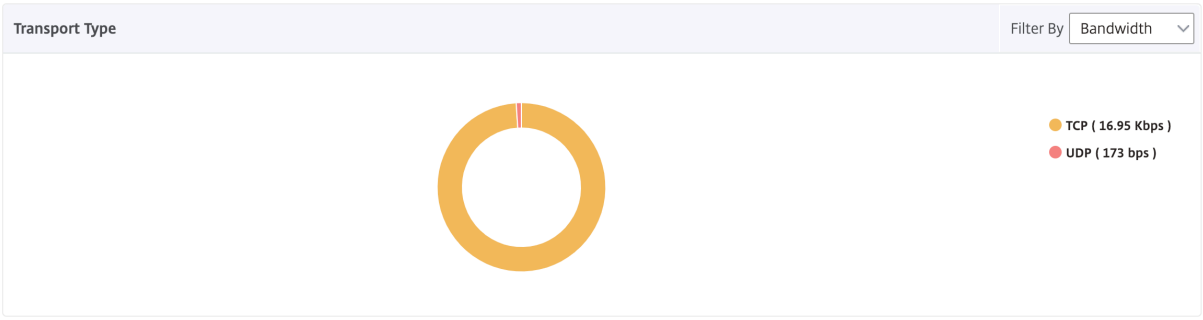
Prise en charge de l'EDT dans HDX Insight

Citrix Application Delivery Management (ADM) prend désormais en charge le transport de données éclairé (EDT) pour l'affichage des analyses pour HDX Insight. Autrement dit, ADM prend désormais en charge les protocoles UDP et TCP. La prise en charge EDT de Citrix Gateway garantit une expérience utilisateur en session haute définition 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 les 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 telles qu'elles sont calculées à partir de la pile TCP actuellement. Par conséquent, ils apparaissent comme « NA ».

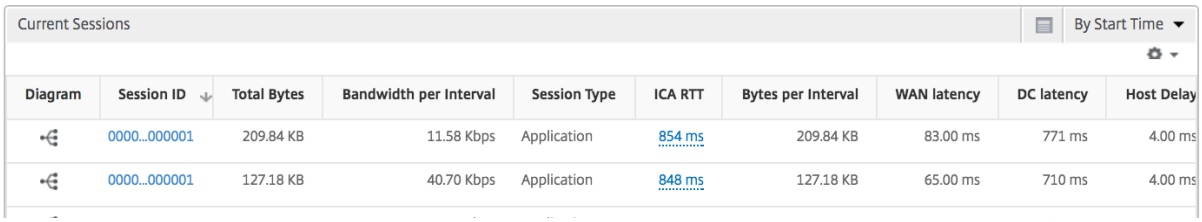


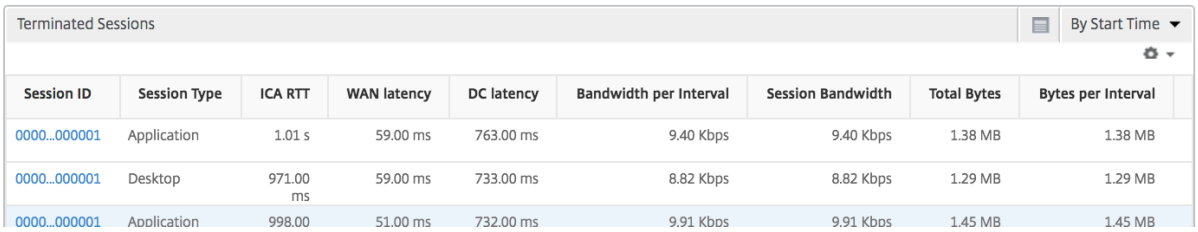
Un nouveau graphique en anneau a été introduit pour vous permettre de voir la bande passante consommée par l'utilisateur ainsi que le nombre total d'octets en fonction du type de protocole utilisé par les utilisateurs.



Mesures HDX Insight disponibles à partir de Citrix ADM 12.0 et versions ultérieures

Latence côté client L7	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 le périphérique Citrix ADC et Citrix Virtual Apps. Cette mesure est utile pour les périphériques non Citrix présents dans le chemin de remise.
Latence maximale de violation	Valeur la plus élevée de la latence L7 lorsqu'une violation d'un seuil défini pour un intervalle de temps défini se produit.
Latence moyenne de violation	Valeur moyenne de latence L7 lorsque le système est dans un état « L7 latence brisé ».
Nombre de violations du seuil L7	Nombre de fois qu'une violation du seuil L7 s'est produite.

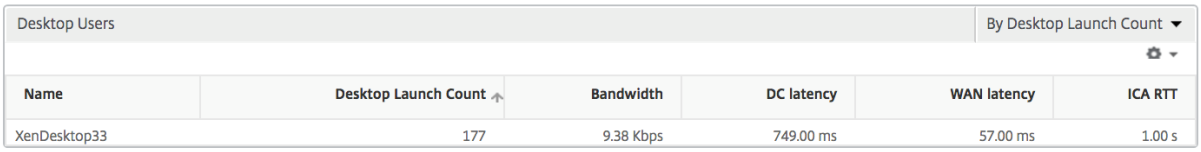




Utilisateurs de bureau

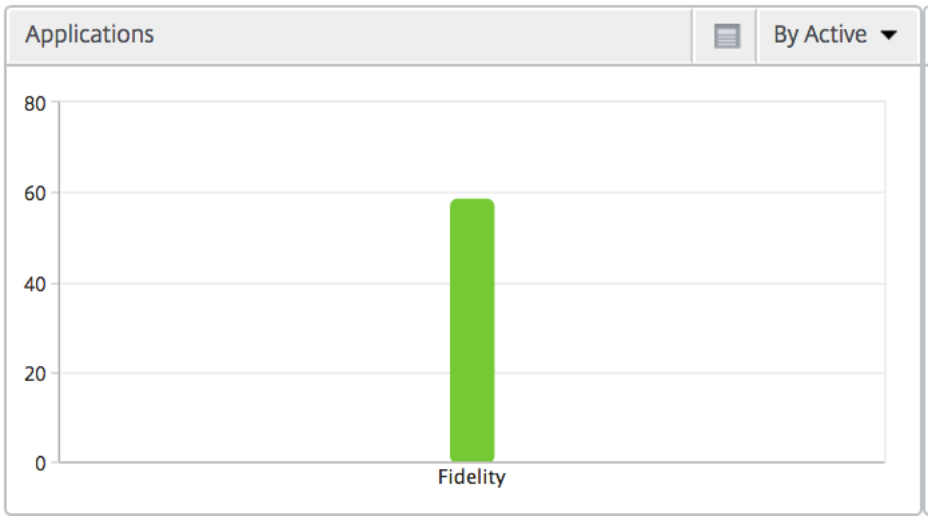
Ce tableau donne un aperçu des sessions Citrix Virtual Desktops pour un utilisateur particulier. Ces mesures peuvent être triées par nombre de lancements de bureau et bande passante.

Mesures	Description
Nom	Nom de Citrix Virtual Desktops.
Nb de lancements de bureaux	Nombre de fois que le bureau a été lancé.
Bande passante	Nombre total de bits par seconde pris pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de Citrix ADC aux serveurs back-end.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de Citrix ADC à l'utilisateur final.
RTT ICA	ICA RTT est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps ou Desktops respectivement.



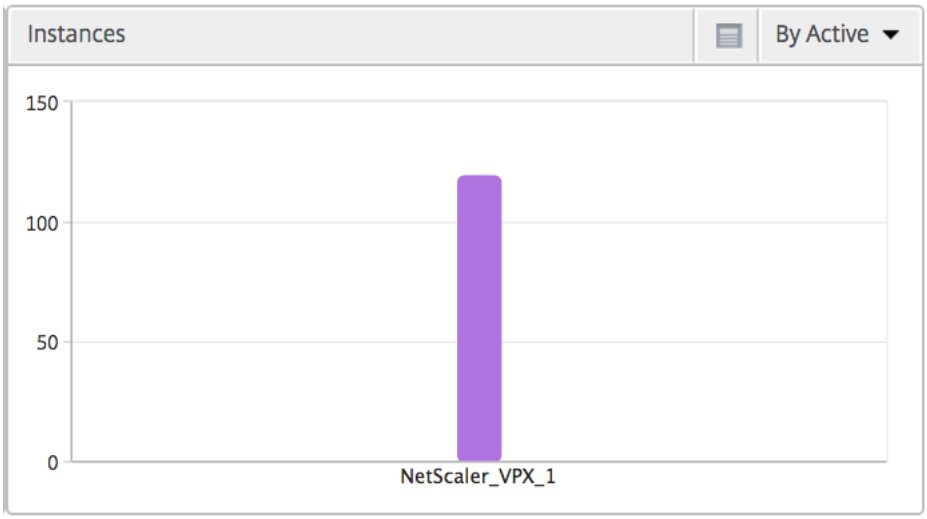
Applications

Graphique à barres représentant les applications triées par Active, nombre total de lancements de session, nombre total de lancements d'applications et durée de lancement.



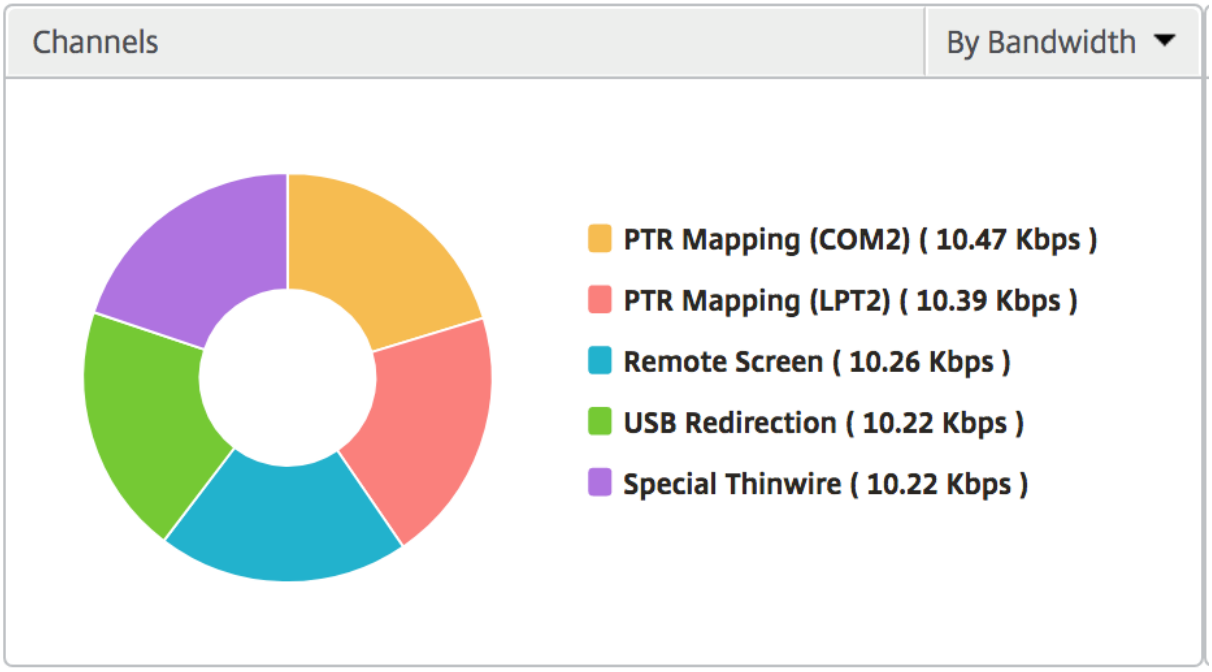
Instances

Graphique à barres représentant les instances ADC triées par applications actives et totales



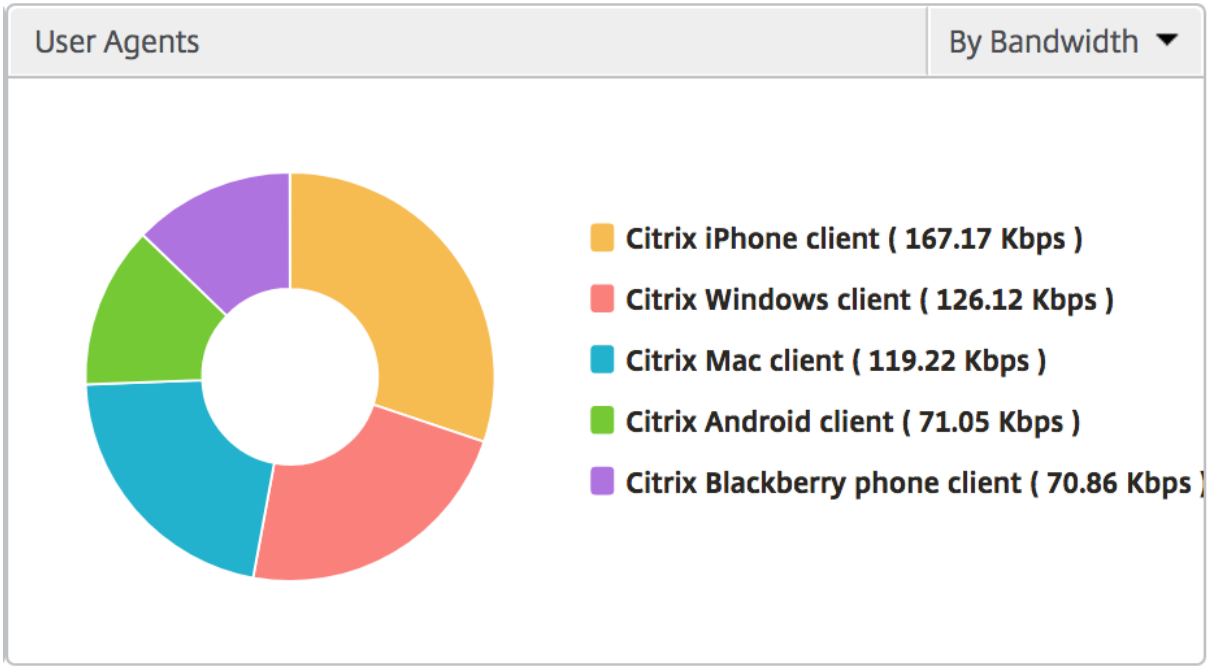
Canaux

Les canaux représentent la bande passante globale ou le nombre total de bits consommés par chaque canal virtuel ICA sous la forme d'un graphique en donut. Vous pouvez également trier les mesures par bande passante ou Total bits.



Agents utilisateurs

Les agents utilisateurs représentent la bande passante globale et totale des bits consommés par chaque point final sous la forme d'un graphique en donut. Vous pouvez également trier les mesures par bande passante ou Total bits.



Vue par session utilisateur

La vue de session par utilisateur fournit des rapports pour la session d'un utilisateur particulier sélectionné.

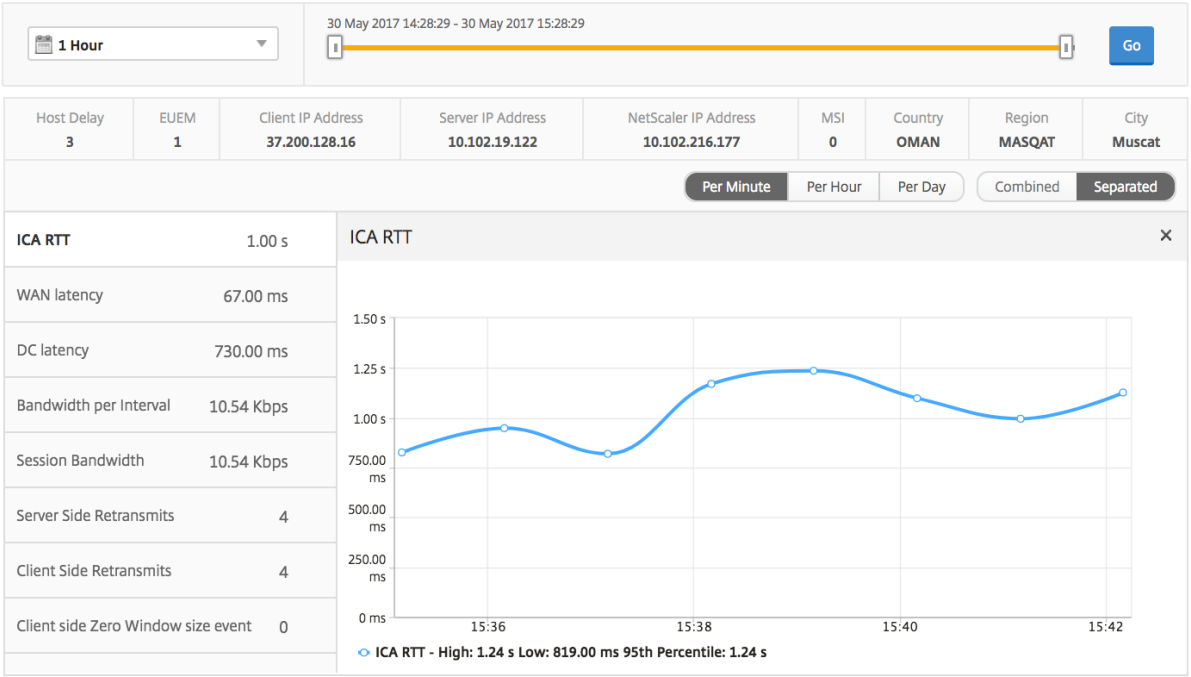
Pour afficher les mesures de la session d'un utilisateur sélectionné :

1. Accédez à **Analytics** > **HDX Insight** > **Utilisateurs**.
2. Select un utilisateur particulier dans la section **Rapport récapitulatif de l'utilisateur**.
3. Select une session dans la colonne **Sessions en cours** ou **Sessions terminées**.

Graphique de chronologie

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	RTT ICA est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps ou Desktops respectivement.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de Citrix ADC à l'utilisateur final.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de Citrix ADC aux serveurs back-end.
Bande passante de session	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.

Mesures	Description
Retransmissions côté client	Nombre de paquets retransmis sur 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 pendant la connexion entre Citrix ADC et l'utilisateur final.
RTO rapide côté serveur	Nombre de fois où le délai de retransmission s'est produit sur la connexion entre Citrix ADC et le serveur principal.
Bande passante par intervalle	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 que le serveur a annoncé une fenêtre TCP zéro.
Événement de taille de fenêtre nulle côté client	Ce compteur indique le nombre de fois où le client a signalé une fenêtre TCP zéro.

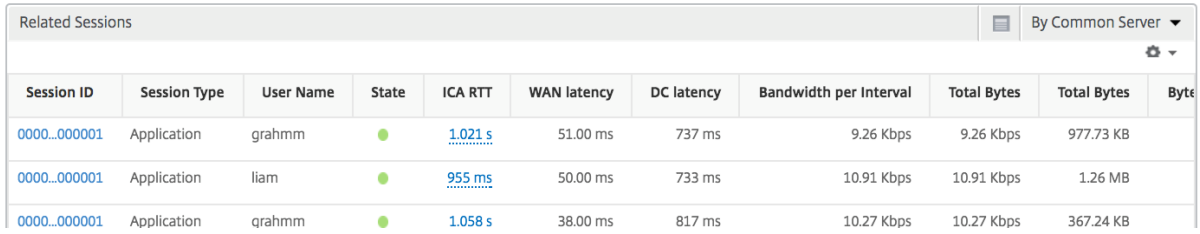


Application active

La section **Applications actives** affiche les applications actives de l'utilisateur sélectionné. Ces applications peuvent également être triées en fonction du nombre de sessions actives et des durées de lancement.

Sessions connexes

La section Sessions associées affiche les sessions associées des sessions de l'utilisateur sélectionné. La relation peut être sélectionnée comme serveurs communs ou Citrix ADC commun.



Rapports et mesures de vue d'instance

April 29, 2021

Les rapports et les mesures de la vue d'instance sont concentrés sur une ou plusieurs 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**.

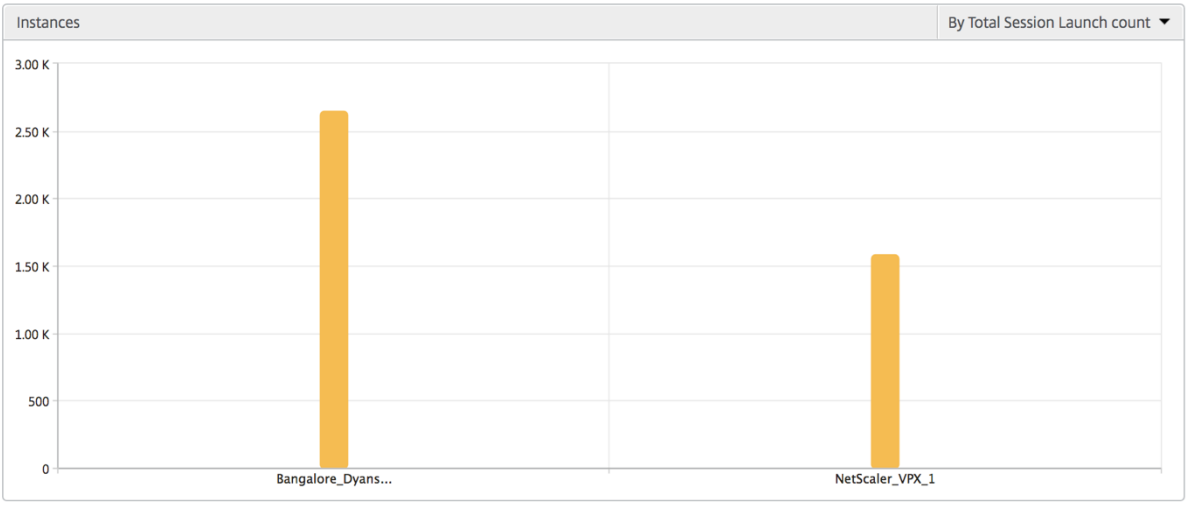
Vue récapitulative de l'instance

Cette vue est appelée vue récapitulative car elle affiche les rapports de toutes les instances ADC ajoutées à Citrix ADM.

Tous ces métriques/rapports, sauf mention explicite, ont les valeurs qui leur correspondent pour la période sélectionnée.

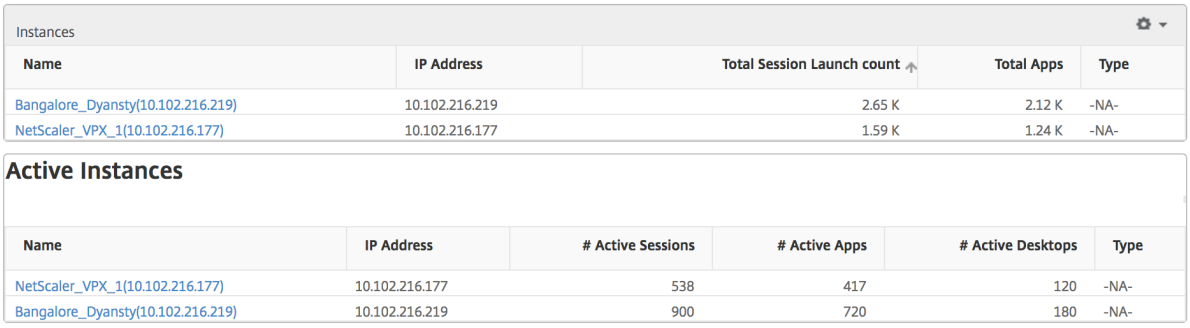
Graphique à barres d'instance

Ce graphique affiche l'instance par rapport au nombre total de lancements de session et Total des applications dans la liste en haut à droite du canevas du graphique.



Rapport de synthèse des instances actives et des instances actives

Mesures	Description
Nom	Nom d'hôte de l'instance 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.
Total des applications	Nombre total d'applications uniques lancées au cours d'un intervalle de temps donné.
Type	S.O.


Instances

Name	IP Address	Total Session Launch count	Total Apps	Type
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	2.65 K	2.12 K	-NA-
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	1.59 K	1.24 K	-NA-

Active Instances

Name	IP Address	# Active Sessions	# Active Apps	# Active Desktops	Type
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	538	417	120	-NA-
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	900	720	180	-NA-

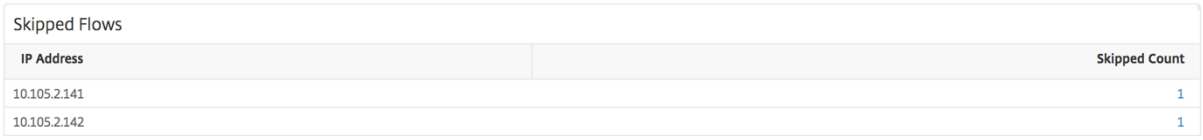
Rapport sur les seuils

L'état des seuils représente le nombre de seuils dépassés lorsque l'*entité* est sélectionnée en tant qu'instance dans la période sélectionnée. Pour de plus amples informations, consultez la section comment créer des seuils et des alertes.

Flux ignorés

Un flux ignoré est un enregistrement qui a ignoré l'analyse de la connexion ICA. Ce flux peut se produire pour plusieurs raisons, telles que l'utilisation de versions de Citrix Virtual Apps and Desktops non prises en charge, la version non prise en charge du type récepteur ou 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 d'autorisation. Par conséquent, ces sessions sont ignorées de la surveillance.

Pour plus de détails sur les problèmes liés à l'analyse ICA, consultez Problème de génération d'enregistrement pour le trafic HDX/ICA dans Citrix ADC liste de vérification


Skipped Flows

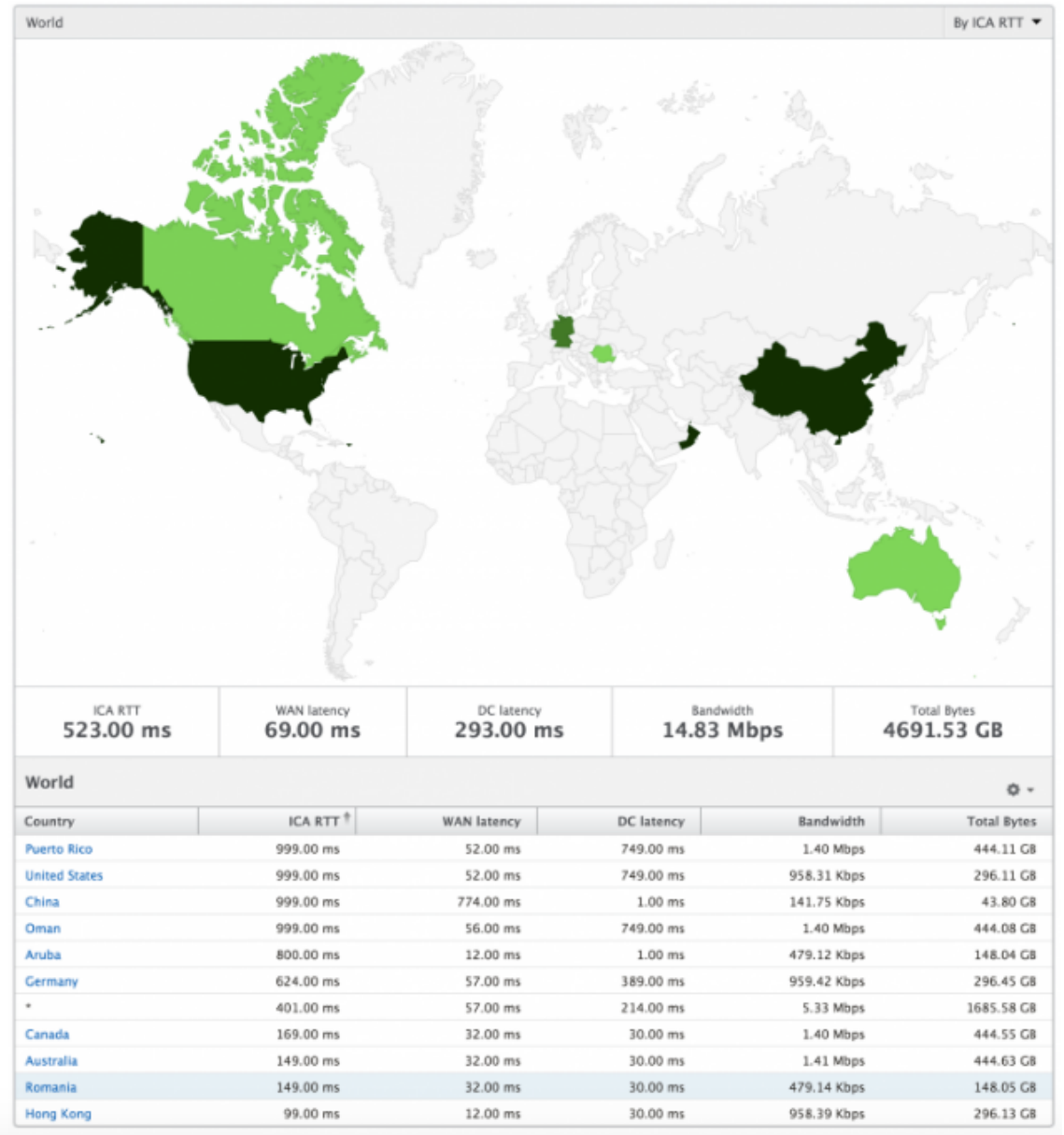
IP Address	Skipped Count
10.105.2.141	1
10.105.2.142	1

Vue du monde

La vue Carte du monde dans HDX Insight permet aux administrateurs de visualiser les détails historiques et actifs des utilisateurs 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 du contrôleur de domaine
- Bande passante
- Nb total d'octets



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

Vue par instance

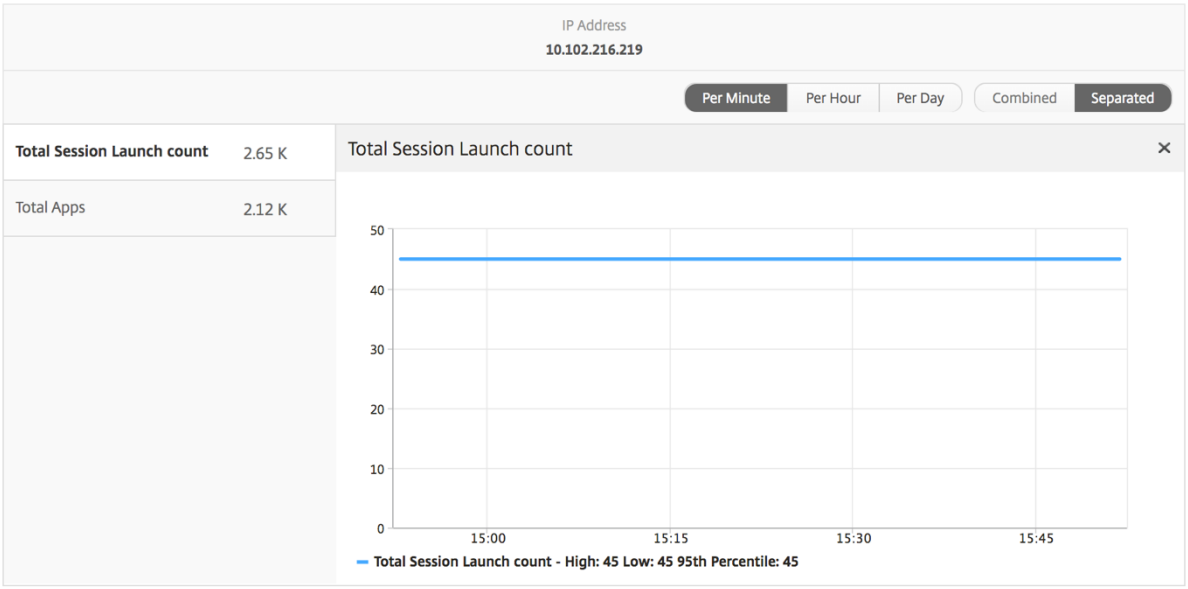
La vue par instance fournit des rapports détaillés sur l'expérience utilisateur final pour une instance ADC sélectionnée particulière.

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**.

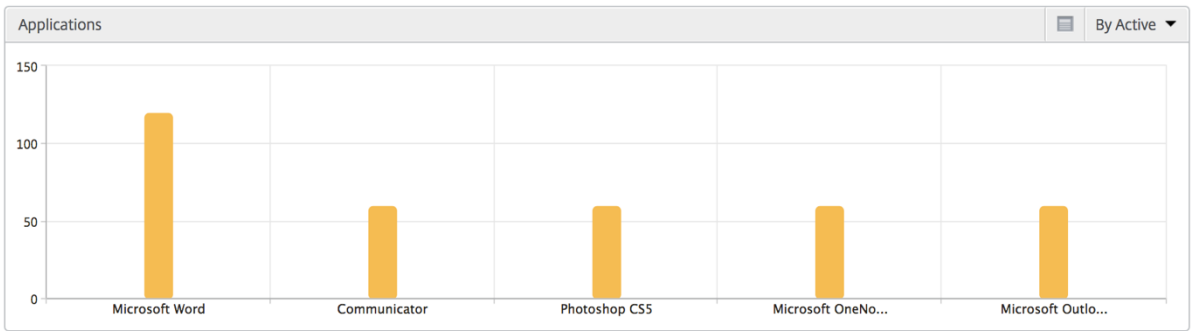
Graphique en courbes

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.
Total des applications	Nombre total d'applications uniques lancées au cours d'un intervalle de temps donné.



Graphique à barres d'applications

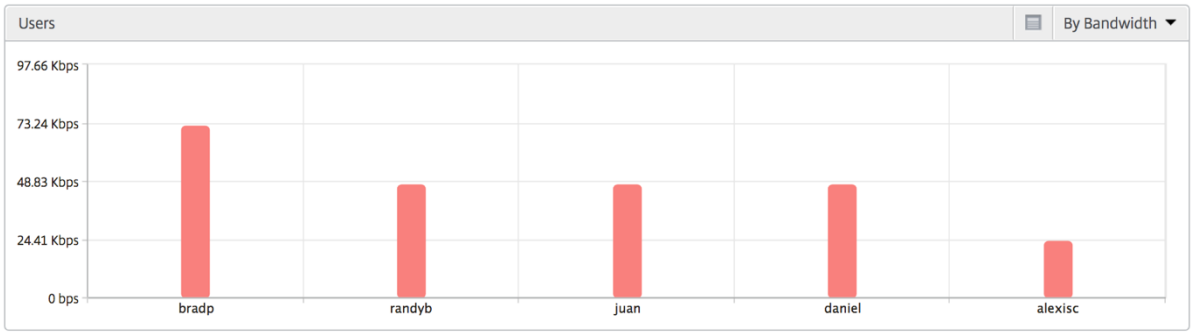
Affiche les 5 principales applications en fonction des applications actives, du nombre total de lancements de session, du nombre total de lancements d'applications ou de la durée de lancement.



Graphique à barres Utilisateurs

Le graphique à barres Utilisateurs affiche les 5 premiers utilisateurs en fonction des critères suivants

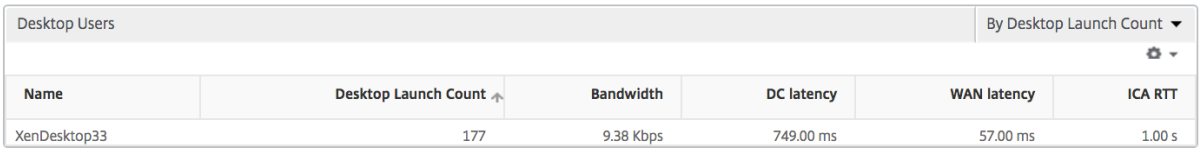
- Bande passante
- Latence WAN
- Latence du contrôleur de domaine
- RTT ICA



Rapport sur les utilisateurs du bureau

Ce tableau donne un aperçu des sessions Citrix Virtual Desktops pour un utilisateur particulier. Ces mesures peuvent être triées par nombre de lancements de bureau et bande passante.

Mesures	Description
Nom	Nom Citrix Virtual Desktop.
Nb de lancements de bureaux	Nombre de fois que le bureau a été lancé.
Bande passante	Nombre total d'octets par seconde pour la communication de bout en bout pendant l'intervalle de temps sélectionné.
Latence DC	Latence causée par le côté serveur du réseau. C'est-à-dire, de Citrix ADC aux serveurs back-end.
Latence WAN	Latence causée par le côté client du réseau. C'est-à-dire, de Citrix ADC à l'utilisateur final.
RTT ICA	RTT ICA est le décalage d'écran que l'utilisateur rencontre lors de l'interaction avec une application ou un bureau hébergé sur Citrix Virtual Apps ou Desktops respectivement.

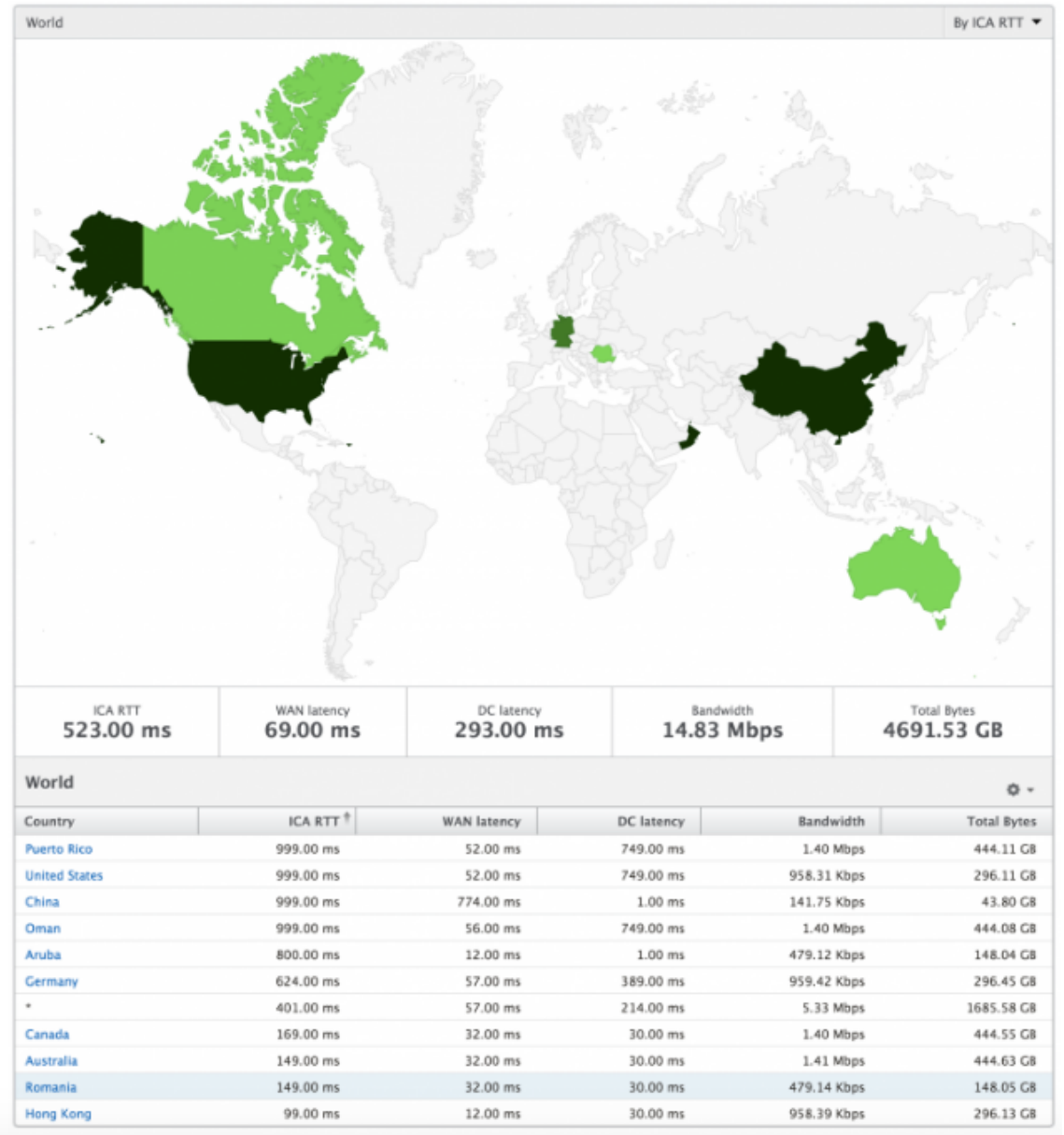


Vue du monde

La vue Carte du monde dans HDX Insight permet aux administrateurs de visualiser les détails historiques et actifs des utilisateurs 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 du contrôleur de domaine
- Bande passante
- Nb total d'octets



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

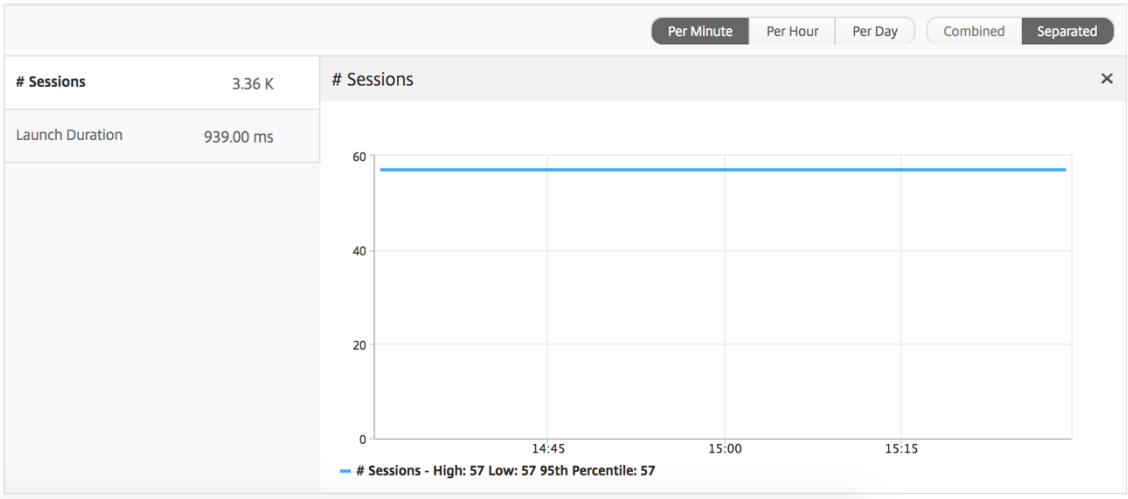
Rapports et mesures d'affichage des licences

April 29, 2021

La vue Licence fournit des détails sur les informations de licence Citrix ADC Gateway. Accédez à **Analytics** > **HDX Insight** > **Licences**.

Graphique en courbes

Mesures	Description
Licences utilisées	Licences CCU Citrix ADC Gateway utilisées au cours de la chronologie sélectionnée. Chaque nombre représente le nombre de sessions utilisateur. Ceci est indépendant des sessions d'application et de bureau lancées par cet utilisateur.
Nombre total de licences	Nombre total de licences CCU Citrix ADC Gateway 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.

Résoudre les problèmes HDX Insight

April 29, 2021

Si la solution HDX Insight ne fonctionne pas comme prévu, le problème peut être lié à l'un des éléments suivants. Reportez-vous aux listes de contrôle des sections respectives pour le dépannage.

- Configuration HDX Insight.
- Connectivité entre Citrix ADC et Citrix ADM.

- Génération d'enregistrements pour le trafic HDX/ICA dans Citrix ADC.
- Population d'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 la section Activation d'AppFlow.
- Vérifiez la configuration HDX Insight dans la configuration en cours d'exécution de Citrix ADC.

  Exécutez la commande `show running | grep -i <appflow_policy>` pour vérifier la configuration HDX Insight. Assurez-vous que le type de liaison est ICA REQUEST. Par exemple ;

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
  ```

  Pour le mode transparent, le type de liaison doit être ICA_REQ_DEFAULT. Par exemple ;

  ```
  bind appflow global afp 100 END -type ICA_REQ_DEFAULT
  ```

- Pour un déploiement de passerelle à guichet unique ou à double saut, assurez-vous que la stratégie AppFlow HDX Insight est liée au serveur virtuel VPN, où le trafic HDX/ICA circule.
- Pour le mode transparent ou le mode utilisateur LAN, assurez-vous que les ports ICA 1494 et 2598 sont définis.
- Vérifiez le paramètre `appflowlog` dans Citrix Gateway ou le serveur virtuel VPN est activé pour le déploiement Access Gateway ou à double saut. Pour plus de détails, consultez la section Activation d'AppFlow pour les serveurs virtuels.
- Cochez « Connection Chaining » est activé dans Citrix ADC double saut. Pour plus de détails, voir Configuration des appliances 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 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 plus de détails, consultez Comment faire pour vérifier l'état de la connectivité entre Citrix ADC et AppFlow Collector.
- Vérifiez les hits de stratégie AppFlow HDX Insight.

  Exécutez la commande `show appflow policy <policy_name>` pour vérifier les succès de stratégie AppFlow.

  Vous pouvez également accéder à **Système > AppFlow > Stratégies** dans l'interface graphique pour vérifier les accès à la stratégie AppFlow.

- Validez tout pare-feu bloquant les ports AppFlow 4739 ou 5557.

Génération d'enregistrement pour le trafic HDX/ICA dans Citrix ADC

Exécutez la commande `tail -f /var/log/ns.log | grep -i "default ICA Message"` pour la validation du journal. En fonction des journaux générés, vous pouvez utiliser ces informations pour le dépannage.

- Journal : **ICA d'analyse ignorée - HDX Insight n'est pas 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 l'application Citrix Workspace vers une version prise en charge. Pour plus de détails, consultez Application Citrix Workspace.

- Journal : **Erreur de Expand Packet - Ignorer tout le traitement hdx pour ce flux**

  Cause : Problème avec la 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 avec l'analyse de la poignée de main ICA

  Solution : Aucun rapport n'est disponible pour cette session ICA particulière tant qu'une nouvelle session n'est pas établie.

- Journal : **EUEM ICA RTT manquant**

  Cause : impossible d'analyser les données du 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 d'utiliser les versions prises en charge de Citrix Workspace App.

- Journal : **En-tête de canal non valide**

  Cause : impossible d'identifier l'en-tête de canal

  Solution : Aucun rapport n'est disponible pour cette session ICA particulière tant qu'une nouvelle session n'est pas établie.

- Journal : **Ignorer le code**

  Si vous voyez l'une des valeurs suivantes pour ignorer le code, les détails Insight sont analysés.

  > Ignorer le code 0 indique que l'enregistrement est exporté à partir de Citrix ADC.

Ignorer le code	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 poignée de main non valide reçue
102	NS_ICA_ERR_REDUC_PARAM_C	Paramètre non valide spécifié pour l'initialisation de l'expandeur V3
103	NS_ICA_ERR_REDUC_INIT	Impossible d'initialiser correctement l'expandeur V3
104	NS_ICA_ERR_REDUC_PARAM_B	Octets insuffisants pour attribuer un codeur à un canal
105	NS_ICA_ERR_INVALID_CHANNEL	Numéro de canal ICA non valide
106	NS_ICA_ERR_INVALID_DECODE	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_DEC	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_EXPAN	Échec de l'extension des données de canal
111	NS_ICA_ERR_REDUC_BYTES_V3_ERR	Erreur de l'expanseur : octets consommés plus que les octets disponibles

Ignorer le code	Message d'erreur	Cause de l'erreur
112	NS_ICA_ERR_REDUC_BYTES_O	Erreur : dépassement de données non compressées
113	NS_ICA_ERR_REDUC_INVALID_CMD	Commande Expander non définie
114	NS_ICA_ERR_CGP_FILL_HOLE	Erreur lors de la gestion des trames CGP fractionnées
115	NS_ICA_ERR_MEM_NSB_ALLOC	Erreur d'allocation NSB — en raison de conditions de mémoire insuffisantes
116	NS_ICA_ERR_MEM_REDUC_CTX	Erreur d'allocation de mémoire pour le contexte de l'expandeur
117	NS_ICA_ERR_ICA_OLD_SERVER	Ancien serveur, blocs de capacités non pris en charge
118	NS_ICA_ERR_PIR_MANY_FRAG	La requête d'initialisation de paquets est fragmentée, impossible à traiter
119	NS_ICA_ERR_INIT_ICA_CAPS	Erreur d'initialisation de capacité ICA
120	NS_ICA_ERR_NO_MSI_SUPPOR	Hôte ne prend pas en charge la fonctionnalité MSI. Indique pour la version XenApp inférieure à 6.5 ou les versions XenDesktop inférieures à 5.0
121	NS_ICA_ERR_CGP_INVALID_CMD	Commande CGP non valide rencontrée
122	NS_ICA_ERR_INSUFFICENT_CH	Octets insuffisants sur le canal
123	NS_ICA_ERR_CHANNEL_DATA	Données incorrectes sur le canal EUEM, CONTROL ou SEAMLESS
124	NS_ICA_ERR_INVALID_PURE_C	Commande non valide reçue lors du traitement de données de canal ICA pures

Ignorer le code	Message d'erreur	Cause de l'erreur
125	NS_ICA_ERR_INVALID_PURE_LEN	Longueur non valide rencontrée lors du traitement de données de canal ICA pures
126	NS_ICA_ERR_INVALID_PURE_LI	Longueur non valide rencontrée lors du traitement des données de canal PURE ICA
127	NS_ICA_ERR_INVALID_CLNT_DATA	Longueur de données non valide reçues du client
128	NS_ICA_ERR_MSI_GUID_SZ	Erreur dans la taille du GUID MSI
129	NS_ICA_ERR_INVALID_CHANNELHEADER	En-tête de canal non valide détecté
130	NS_ICA_ERR_CGP_PARSE_REC(	Échec de la récupération de la session reconnectée
131	NS_ICA_ERR_DISABLE_SR_NON_HS_RECONNECT	Erreur lors de la désactivation de SR
132	NS_ICA_ERR_REDUC_NOT_V3	Version ICA Reducer non prise en charge
133	NS_ICA_ERR_HS_COMPRESSION_DISABLED	Compression désactivée, non honorée 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 incorrecte ou chaîne magique
136	NS_ICA_ERR_PARSE_RAW	Erreur lors de l'analyse du paquet de poignée de main ICA
137	NS_ICA_ERR_INCOMPLETE_PKT	Paquet incomplet reçu en poignée de main
138	NS_ICA_ERR_ICAFRAME_TOO_I	Le cadre ICA est trop grand, dépasse 1 460 octets

Ignorer le code	Message d'erreur	Cause de l'erreur
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 réassembler le cadre ICA correctement
142	NS_ICA_ERR_UNSUPPORTED_F	Analyse ICA ignorée pour ce récepteur (client) car il n'est pas dans la liste d'autorisation
143	NS_ICA_ERR_LOOKUP_RECONNECT_DS	Impossible de détecter l'état d'analyse pour le cookie de reconnexion client
144	NS_ICA_ERR_SYNCUP_RECONN	Longueur de cookie de reconnexion non valide détectée après la reconnexion du client
145	NS_ICA_ERR_INVALID_RECONNECT_CO	Le cookie reconnecte le client a manqué la contrainte nécessaire
146	NS_ICA_ERR_INVALID_CLIENT_	Chaîne de version du récepteur non valide reçue du client
147	NS_ICA_ERR_UNKNOWN_CLIENT_PRODUCT_ID	Produit non valide reçu du client
148	NS_ICA_ERR_V3_HDR_CORRUP	Longueur de canal non valide après l'extension
149	NS_ICA_ERR_SPECIAL_THINWIRE	Erreur de décompression
150	NS_ICA_ERR_SEAMLESS_INSUF	Octets insuffisants rencontrés pour la commande transparente
151	NS_ICA_ERR_EUEM_INSUFFBYTE	Octets insuffisants rencontrés pour la commande EUEM

Ignorer le code	Message d'erreur	Cause de l'erreur
152	NS_ICA_ERR_SEAMLESS_INVAL	Événement non valide pour l'analyse transparente des canaux
153	NS_ICA_ERR_CTRL_INVALID_EVENT	Événement non valide pour l'analyse des canaux CTRL
154	NS_ICA_ERR_EUEM_INVALID_E	Événement non valide pour l'analyse des canaux EUEM
155	NS_ICA_ERR_USB_INVALID_EVENT	Événement non valide pour l'analyse des canaux USB
156	NS_ICA_ERR_PURE_INVALID_E	Événement non valide pour l'analyse des canaux purs
157	NS_ICA_ERR_VCP_INVALID_EVENT	Événement non valide pour l'analyse des canaux virtuels
158	NS_ICA_ERR_ICAP_INVALID_EV	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_INV	État non valide pour une commande crypt dans le chiffrement de base
161	NS_ICA_ERR_BASICCRYPT_INVALIDCRYPTCMD	Commande crypt non valide dans le chiffrement de base
162	NS_ICA_ERR_ADVCRYPT_INVAL	État non valide pour une commande crypt dans le chiffrement RC5
163	NS_ICA_ERR_ADVCRYPT_INVALIDCRYPTCMD	Commande crypt non valide dans le chiffrement RC5
164	NS_ICA_ERR_ADVCRYPT_ENC	Erreur dans le chiffrement ou le déchiffrement RC5
165	NS_ICA_ERR_ADVCRYPT_DEC	Erreur dans le chiffrement ou le déchiffrement RC5
166	NS_ICA_ERR_SERVER_NOT_RE	VDA ne prend pas en charge Reducer Version 3

Ignorer le code	Message d'erreur	Cause de l'erreur
167	NS_ICA_ERR_CLIENT_NOT_REDUCER_V3	Le récepteur ne prend pas en charge le réducteur version 3
168	NS_ICA_ERR_ICAP_INSUFFBYTE	Nombre inattendu d'octets dans ICA handshake
169	NS_ICA_ERR_HIGHER_RECONSEQ	Numéro de séquence de reprise CGP plus élevé à partir des reconnexions de post homologues
170	NS_ICA_ERR_DESCSRINFO_ABS	Impossible de restaurer l'état d'analyse ICA après 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 des données du canal Insight
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_E	Erreur lors de l'analyse des détails de fin de session à partir des données du canal Insight
175	NS_ICA_ERR_NON_NSAP_SN	Analyse ICA ignorée sur le nœud de service en raison de l'absence de prise en charge du canal Insight
176	NS_ICA_ERR_NON_NSAP_CLIEI	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

Ignorer le code	Message d'erreur	Cause de l'erreur
179	NS_ICA_ERR_SN_RECONNECT_TKT_FETCH	Erreur lors de la récupération du service reconnecte le ticket dans le nœud de service
180	NS_ICA_ERR_SN_HIGHER_REC(	Erreur lors de la réception du numéro de séquence de reconnexion supérieur dans le nœud de service
181	NS_ICA_ERR_DISABLE_HDXINSIGHT_NONSAP	Erreur lors de la désactivation de HDX Insight pour les connexions non-NSAP

Exemples de journaux :

```
Jan 9 22:57:02 <local0.notice> 10.106.40.223 01/09/2020:22:57:02 GMT ns-223
 0-PPE-2 : default ICA Message 1234 0 : "Session setup data send: Session
GUID [57af35043e624abab409f5e6af7fd22c], Client IP/Port [10.105.232.40/52314],
 Server IP/Port [10.106.40.215/2598], MSI Client Cookie [Non-MSI], Session
 setup time [01/09/2020:22:56:49 GMT], Client Type [0x0052], Receiver
Version [19.12.0.23], User [user1], Client [10.105.232.40], Server [WIN2K12
-215], Ctx Flags [0x8820220228], 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 [0x8820220008], Track Flags [0x1600010c040], Skip Code [171]"
```

Compteurs d'erreurs

Différents compteurs sont capturés 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	Objectif	Catégorie (Stats/Erreur/Diagnostics)
hdx_tot_ica_conn	Indique le nombre total de connexions ICA Pure détectées par NS.Incrémenté chaque fois qu'une connexion ICA basée sur la signature ICA sur un PCB client est détectée.	Statistiques
hdx_tot_cgp_conn	Indique le nombre total de connexions CGP détectées par NS (Session Reliability ON). Incrémenté chaque fois qu'une connexion CGP basée sur la signature CGP sur un PCB client est détectée.	Statistiques
hdx_dbg_tot_udt_conn	Indique le nombre total de connexions ICA UDP détectées par NS	Statistiques
hdx_dbg_tot_nsap_conn	Indique le nombre total de connexions NSAP prises en charge détectées par NS	Statistiques
hdx_tot_skip_conn	Indique combien de connexions ICA ont été ignorées par l'analyseur en raison d'une signature ICA ou CGP non valide.	Statistiques
hdx_dbg_active_conn	Total des connexions EDT/CGP/ICA actives à cet instant.	Statistiques
hdx_dbg_active_nsap_conn	Total des connexions NSAP EDT/CGP/ICA actives à cet instant.	Statistiques
hdx_dbg_skip_appflow_disabled	Nombre total d'instances où AppFlow a été détaché d'une session en raison de la désactivation d'AppFlow	Statistiques/Diagnostics

Nom du compteur HDX	Objectif	Catégorie (Stats/Erreur/Diagnostics)
hdx_dbg_transparent_user	Nombre total d'accès utilisateur transparent	Statistiques/Diagnostics
hdx_dbg_ag_user	Nombre total d'accès utilisateur Access Gateway	Statistiques/Diagnostics
hdx_dbg_lan_user	Nombre total d'accès au mode utilisateur LAN	Statistiques/Diagnostics
hdx_basic_enc	Indique le nombre de connexions ICA utilisant le chiffrement de base	Statistiques/Diagnostics
hdx_advanced_frc	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_server	Nombre total de connexions CGP/ICA avec Citrix SD-WAN côté serveur	Statistiques/Diagnostics
hdx_dbg_reconnected_session	Nombre total de demandes de reconnexion du client sans erreur Citrix ADC	Statistiques/Diagnostics
hdx_dbg_host_rejected_ns_rec	Nombre total d'hôtes rejetés demandes de reconnexion par client	Statistiques/Diagnostics
hdx_euem_available	Indique le nombre de connexions dont le canal de surveillance de l'expérience utilisateur final est disponible.Le canal de surveillance de l'expérience utilisateur final est requis pour collecter des statistiques telles que ICA RTT.	Statistiques/Diagnostics

Nom du compteur HDX	Objectif	Catégorie (Stats/Erreur/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.	Error
hdx_err_skip_no_msi	Le serveur XA/XD est manquant de capacité MSI. Cela indique une version antérieure du serveur, HDX Insight ignore cette connexion.	Error
hdx_err_skip_old_server	Ancienne version de serveur non prise en charge	Error
hdx_err_clnt_not_whitelist	Le récepteur client n'est pas dans la liste d'autorisation, HDX Insight ignore cette connexion	Error
hdx_sm_ica_cam_channel_disa	Nombre total de NS_ICA_CAM_CHANNEL désactivés via la stratégie SmartAccess	Diagnostics
hdx_sm_ica_usb_channel_disabled	Nombre total de NS_ICA_USB_CHANNEL désactivés via la stratégie SmartAccess	Diagnostics
hdx_sm_ica_clip_channel_disa	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

Nom du compteur HDX	Objectif	Catégorie (Stats/Erreur/Diagnostics)
hdx_sm_ica_cdm_channel_disa	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_di	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_disa	Nombre total de NS_ICA_LPT1_CHANNEL désactivé via la stratégie SmartAccess	Diagnostics
hdx_sm_ica_lpt2_channel_disabled	Nombre total de NS_ICA_LPT2_CHANNEL désactivé via la stratégie SmartAccess	Diagnostics
dx_dbg_sm_ica_msi_disabled	Nombre total de cas où MSI est désactivé via la stratégie SmartAccess	Diagnostics
hdx_sm_ica_file_channel_disabled	Le nombre total de NS_ICA_FILE_CHANNEL est désactivé via la stratégie SmartAccess	Diagnostics
hdx_dbg_usb_accept_device	Nombre total de périphériques USB acceptés	Diagnostics
hdx_dbg_usb_reject_device	Nombre total de périphériques USB rejetés	Diagnostics

Nom du compteur HDX	Objectif	Catégorie (Stats/Erreur/Diagnostics)
hdx_dbg_usb_reset_endpoint	Nombre total de points de terminaison USB réinitialisés	Diagnostics
hdx_dbg_usb_reset_device	Nombre total de périphériques USB réinitialisés	Diagnostics
hdx_dbg_usb_stop_device	Nombre total de périphériques USB arrêtés	Diagnostics
hdx_dbg_usb_stop_device_response	Nombre total de réponses provenant de périphériques USB arrêtés	Diagnostics
hdx_dbg_usb_device_gone	Nombre total de périphériques USB disparus	Diagnostics
hdx_dbg_usb_device_stoppé	Nombre total de périphériques USB arrêtés	Diagnostics

validation nstrace

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.
- Valider le serveur virtuel Citrix Gateway/VPN est sous licence dans Citrix ADM.
- Assurez-vous que le paramètre multi-saut est activé pour le double saut.
- Assurez-vous que Citrix Gateway est désactivée pour le second saut dans le déploiement à double saut.

Avant de contacter le support technique Citrix

Pour une résolution rapide, assurez-vous que vous disposez des informations suivantes avant de contacter le support technique Citrix :

- Détails du déploiement et de la topologie du réseau.
- Versions Citrix ADC et Citrix ADM.
- Versions du serveur Citrix Virtual Apps and Desktops.
- Versions client Receiver.
- Nombre de sessions ICA actives lorsque le problème s'est produit.
- Bundle de support technique capturé en exécutant la commande `show techsupport` à l'invite de commande Citrix ADC.
- Pack de support technique capturé pour Citrix ADM.
- Traces de paquets capturées sur tous les Citrix ADC.
  Pour démarrer une trace de paquets, tapez, `start nstrace -size 0'`
  Pour arrêter une trace de paquets, tapez, `stop nstrace`
- Collectez les entrées de la table ARP du système en exécutant la commande `show arp`.

Problèmes connus

Reportez-vous aux notes de mise à jour de Citrix ADC pour connaître les problèmes connus sur HDX Insight.

Informations sur les mesures pour les seuils

April 29, 2021

Web

Mesures	Entité	Description
Applications	Accès	Nombre total d'accès reçus par un serveur virtuel (application)
	Bande passante (Mo)	Bande passante totale consommée par le serveur virtuel (application)
	Temps de réponse (ms)	Temps de réponse du serveur virtuel

Mesures	Entité	Description
Clients	Demandes	La demande totale reçue par un client
	Temps de rendu (ms)	Temps nécessaire pour rendre la réponse du serveur par le client
	Latence du réseau client	Temps pris pour les demandes du réseau client
Devices	Accès	Nombre total de visites reçues par un appareil. Par exemple : ordinateur portable, téléphone mobile
	Bande passante (Mo)	Bande passante totale consommée par un appareil
Domaines	Accès	Nombre total d'accès reçus par un domaine réseau
	Bande passante (Mo)	Bande passante totale consommée par un domaine réseau
	Temps de réponse (ms)	Temps nécessaire pour répondre aux demandes d'un domaine réseau
OS	Accès	Nombre total d'accès reçus par un système d'exploitation
	Bande passante (Mo)	Bande passante totale consommée par un système d'exploitation
	Temps de rendu (ms)	Temps nécessaire pour rendre la réponse du serveur par un système d'exploitation
Méthodes de requête	Accès	Nombre total de demandes reçues par une méthode de demande. Par exemple : GET, POST

Mesures	Entité	Description
	Bande passante (Mo)	Bande passante totale consommée par une méthode de demande
État de la réponse	Accès	Nombre total de visites reçues avec les codes de réponse
	Bande passante (Mo)	Bande passante totale consommée par le code de réponse
Serveurs	Accès	Nombre total de demandes ou d'accès reçus par un serveur
	Bande passante (Mo)	Bande passante totale consommée par un serveur
	Latence réseau du serveur (ms)	Temps pris pour les demandes du réseau de serveurs
	Temps de traitement du serveur (ms)	Temps pris par un serveur pour répondre aux demandes
URL	Accès	Nombre total de visites reçues par une URL. Par exemple : www.Citrix.com
	Temps de chargement (ms)	Temps requis pour le chargement d'une URL à partir du serveur
	Temps de rendu (ms)	Temps pris par l'URL pour le rendu et l'affichage
Agents utilisateur	Accès	Nombre total de demandes reçues par un agent utilisateur. Par exemple : navigateur Web Chrome
	Bande passante (Mo)	Bande passante totale consommée par l'agent utilisateur

Mesures	Entité	Description
	Temps de rendu (ms)	Temps de rendu de la réponse du serveur par l'agent utilisateur

Sécurité

Mesure	Entité	Description
Applications	Indice des menaces	Système de notation à un chiffre qui indique la criticité des attaques sur l'application. Plus les attaques contre une application sont critiques, plus l'indice de menace pour cette application est élevé. Les valeurs varient de 1 à 7.
	Indice de sécurité	Système de notation à un chiffre qui indique la sécurité avec laquelle vous avez configuré les instances de Citrix ADC pour protéger les applications contre les menaces et vulnérabilités externes. Plus les risques de sécurité pour une application sont faibles, plus l'indice de sécurité est élevé. Les valeurs varient de 1 à 7.

APPANALYTICS

Mesure	Entité	Description
Applications	Score de l'application	App Score définit la performance d'une application et indique si l'application fonctionne bien en termes de réactivité. Les valeurs varient de 0 à 80.

HDX

Pour plus d'informations sur les seuils HDX, voir Créer des seuils et configurer des alertes pour HDX Insight

Gateway Insight

April 29, 2021

Dans un déploiement Citrix Gateway, la visibilité des détails d'accès 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 fournit une visibilité sur les échecs rencontrés par tous les utilisateurs, quel que soit le mode d'accès, au moment de la connexion à Citrix Gateway. Vous pouvez afficher 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 un moment donné. Vous pouvez afficher les échecs d'analyse de point de terminaison (EPA), d'authentification, d'authentification unique (SSO) et de lancement d'application pour un utilisateur. Vous pouvez également afficher les détails des sessions actives et terminées pour 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 d'ouverture de session ou de lancement d'application. Vous pouvez afficher le nombre d'applications lancées, le nombre de sessions totales et actives, le nombre total d'octets et la bande passante consommée par les applications. Vous pouvez afficher les détails des utilisateurs, des sessions, de la bande passante et des erreurs de lancement d'une application.

Vous pouvez 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 de

passerelle ADC. 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 de journal sont stockés dans la base de données Citrix Application Delivery Management (ADM), de sorte que vous pouvez afficher les détails des erreurs pour n'importe quelle période. Vous pouvez également afficher un résumé des échecs d'ouverture de session et déterminer à quelle étape 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 d'ADM doivent être identiques ou postérieures à celles de l'appliance Citrix Gateway.
- Une heure de rapports Gateway Insight peut être consultée pour les instances ADC avec licence Advanced. Une licence Premium est requise pour afficher les rapports Gateway Insight au-delà d'une heure.

Limitations :

- Citrix Gateway ne prend pas en charge Gateway Insight lorsque la méthode d'authentification est configurée en tant qu'authentification basée sur les certificats.
- Les connexions utilisateur réussies, la latence et les détails au niveau de l'application pour les applications ICA virtuelles et les postes de travail ne sont visibles que sur le tableau de bord Users HDX Insight.
- En mode double-saut, la visibilité des pannes de l'appliance ADC Gateway dans la seconde zone DMZ n'est pas disponible.
- Les problèmes d'accès aux postes de travail RDP (Remote Desktop Protocol) ne sont pas signalés.
- Les enregistrements Gateway Insight pour l'authentification SAML 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 voir des divergences dans Gateway Insight.
  - Stockage local
  - LDAP
  - RADIUS
  - TACACS
  - SAML
  - OTP natif

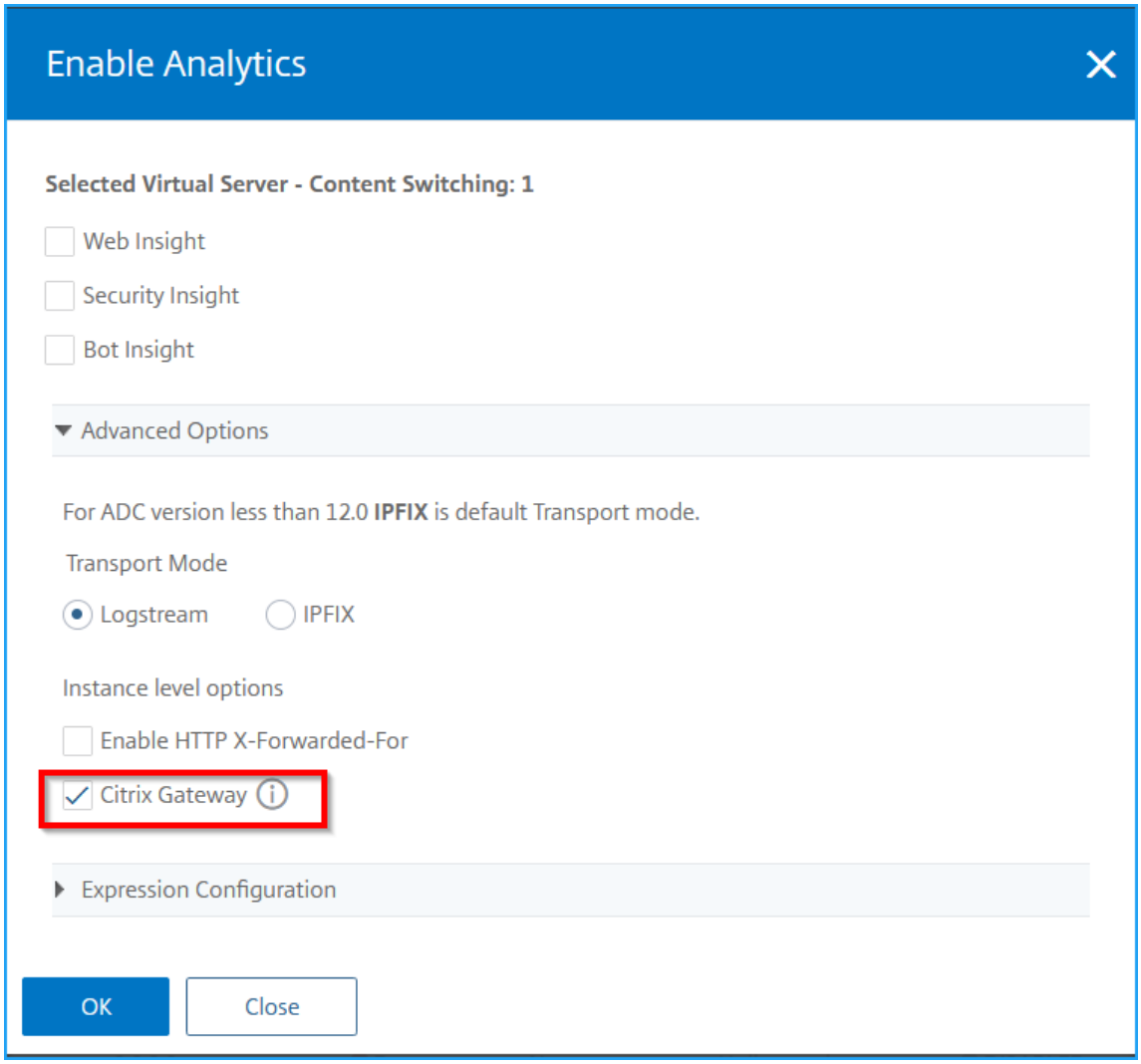
Activer Gateway Insight

Pour activer Gateway Insight pour votre appliance Citrix Gateway, vous devez d'abord ajouter l'appliance ADC Gateway à ADM. Vous devez ensuite activer AppFlow pour le serveur virtuel représentant l'application VPN. Pour plus d'informations sur l'ajout d'un périphérique à ADM, reportez-vous à la section Ajout d'instances.

> **Remarque**
>
> Pour afficher les échecs d'analyse des points de terminaison (EPA) dans Citrix ADM, vous devez activer la journalisation du nom d'utilisateur d'authentification, de l'autorisation et du contrôle d'accès AppFlow sur l'appliance ADC Gateway.

Activer AppFlow pour un serveur virtuel dans ADM

1. Accédez à **Réseaux > Instances > Citrix ADC**, puis sélectionnez l'instance pour laquelle vous souhaitez activer AppFlow.
2. Dans la liste **Sélectionner une action**, sélectionnez **Configurer Analytics**.
3. Sélectionnez le serveur virtuel, puis cliquez sur **Activer Analytics**.
4. Sous **Options avancées**, sélectionnez **Citrix Gateway**.



5. Cliquez sur OK.

Activer la journalisation du nom d'utilisateur AppFlow sur une appliance de passerelle ADC 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 AppFlow**, sélectionnez **Nom d'utilisateur AAA**, puis cliquez sur **OK** .

Afficher les rapports Gateway Insight

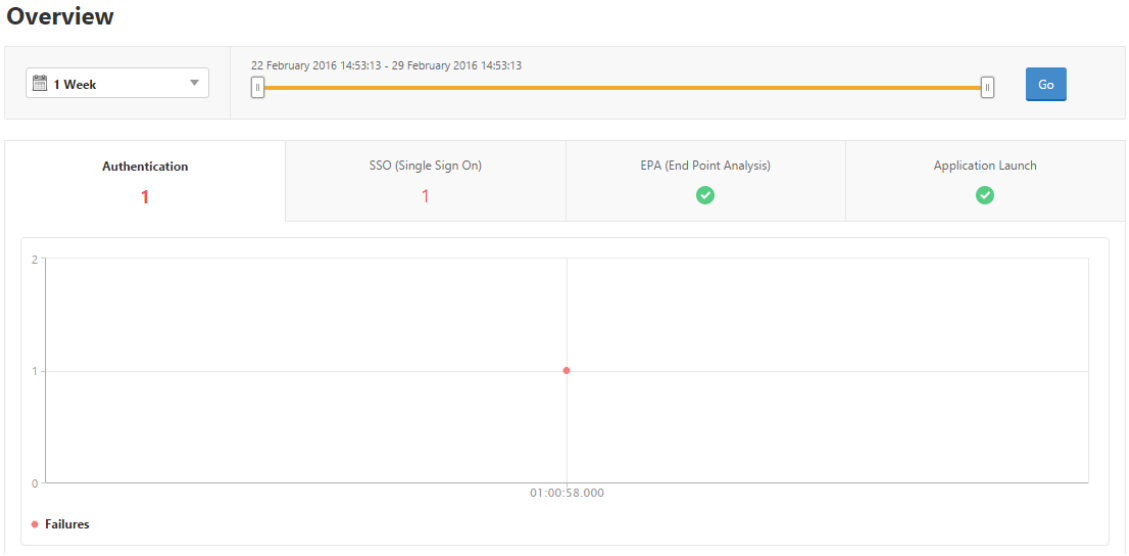
Dans Citrix ADM, vous pouvez afficher des rapports pour tous les utilisateurs, applications et passerelles associés aux appliances ADC Gateway et afficher les détails d'un utilisateur, d'une appli-

cation ou d'une passerelle 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, les types de clients et le nombre d'utilisateurs connectés toutes les heures.

> **Remarque**
>
> Lorsque vous créez un groupe, vous pouvez attribuer des rôles au groupe, fournir un accès au groupe au niveau de l'application et affecter des utilisateurs au groupe. L'analyse Citrix ADM prend désormais en charge l'autorisation basée sur l'adresse IP virtuelle. Vos utilisateurs peuvent désormais voir des rapports pour tous les Insights uniquement pour les applications (serveurs virtuels) pour lesquelles ils sont autorisés. Pour plus d'informations sur les groupes et l'affectation d'utilisateurs au groupe, reportez-vous à la section Configurer des groupes sur Citrix ADM.

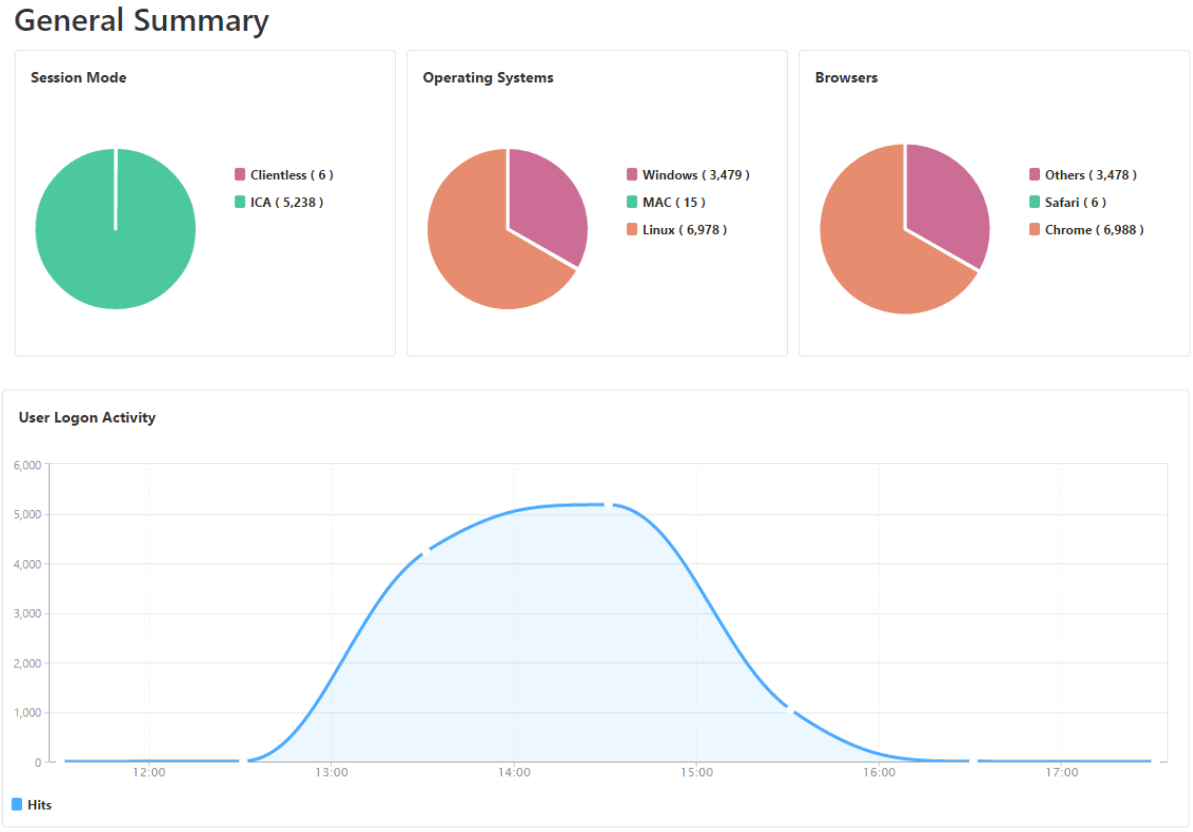
Afficher les échecs EPA, SSO, authentification, autorisation et lancement d'application

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 **OK**.
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.



Afficher le résumé des modes de session, des clients et du nombre d'utilisateurs

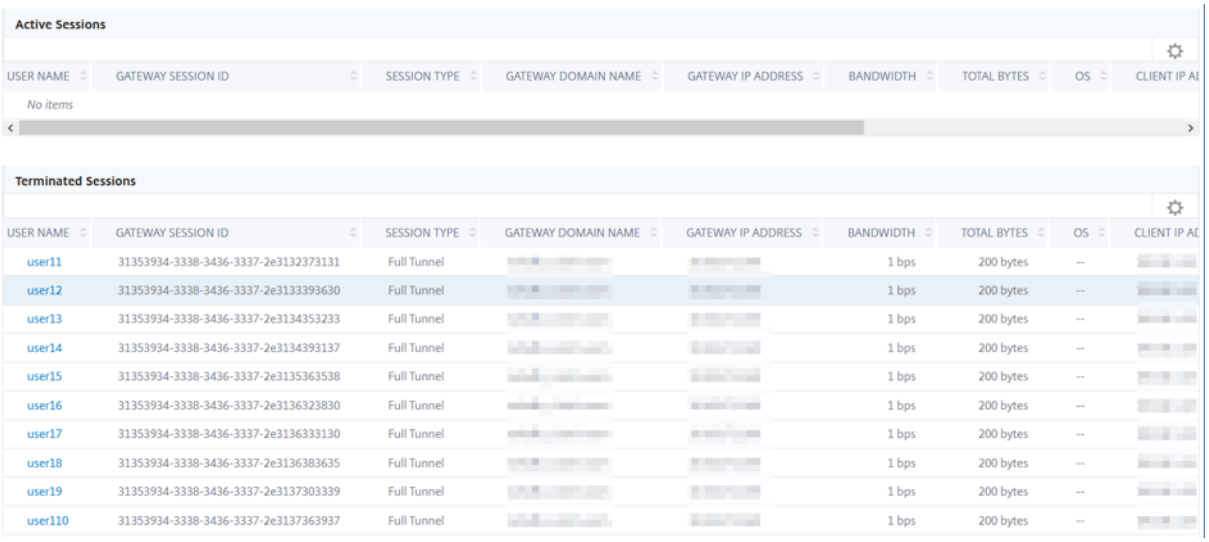
Dans Citrix ADM, accédez à **Analytics > Gateway Insight**, faites défiler vers le bas pour afficher les rapports.



Utilisateurs

Vous pouvez afficher un rapport complet pour les utilisateurs associés aux appliances de passerelle ADC. Vous pouvez afficher l'EPA, l'authentification, l'authentification unique, les échecs de lancement d'application, etc. pour un utilisateur.

Vous pouvez également visualiser une vue consolidée de tous les utilisateurs des sessions actives et terminées.

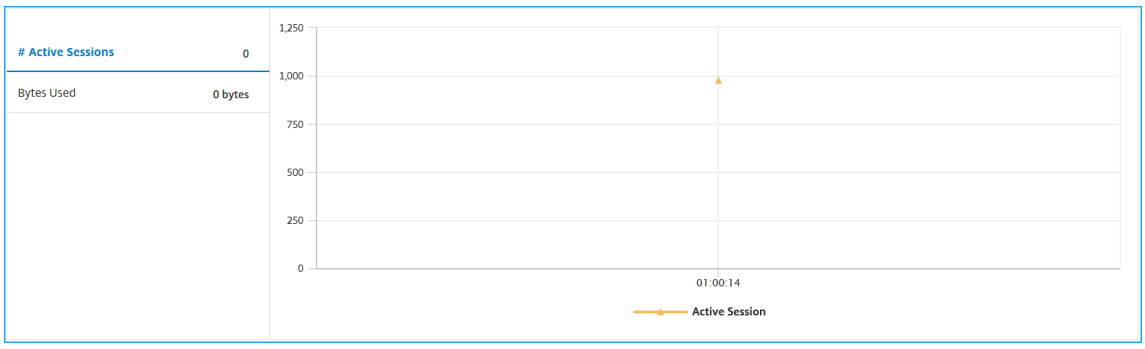


En tant qu'administrateur, cette vue vous permet d'effectuer les opérations suivantes :

- Afficher tous les détails des utilisateurs dans une visualisation à un seul volet
- Éliminer la complexité de la sélection de chaque utilisateur et de voir les sessions actives et terminées

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 **OK**.
3. Vous pouvez afficher le nombre d'utilisateurs actifs, le nombre de sessions actives et d'octets par tous les utilisateurs au cours de la période.

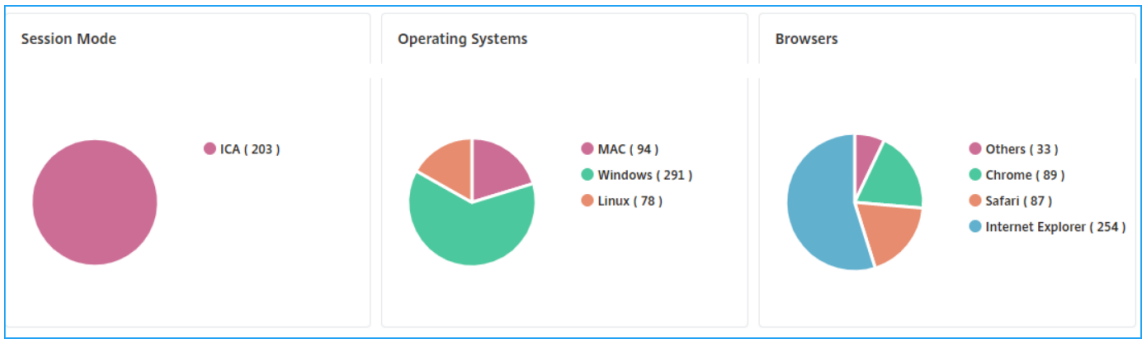


Faites défiler vers le bas pour afficher la liste des utilisateurs disponibles et des utilisateurs actifs.

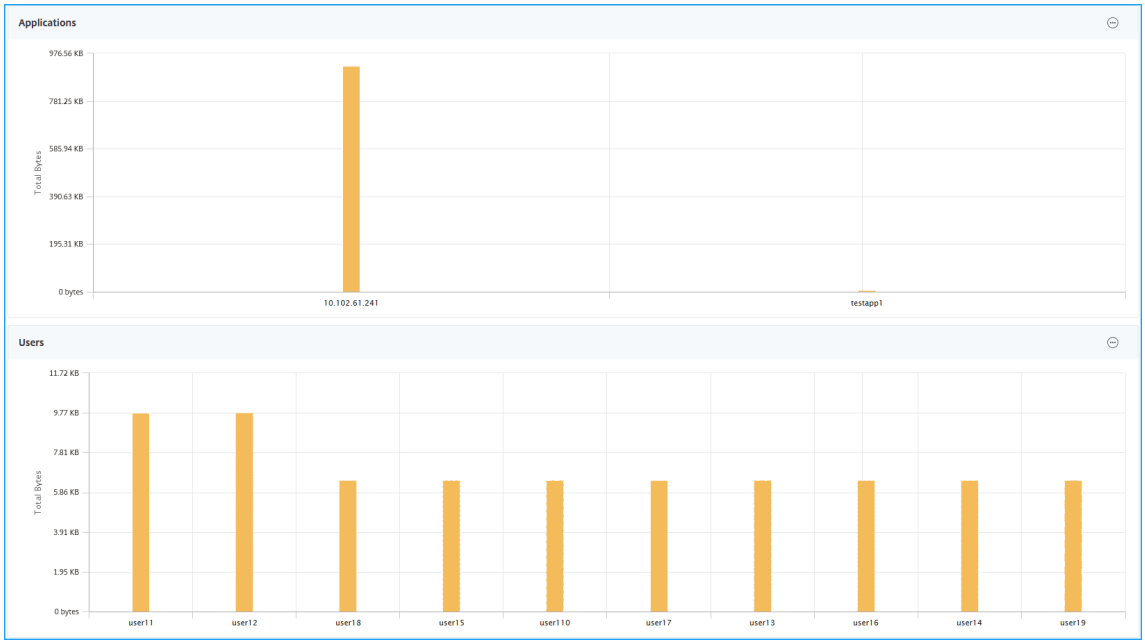
User Name	Total Bytes	# Sessions Used
user1	191.94 KB	11
user10	0	4
user100	2.81 KB	4
user1000	42.66 KB	5
user1001	2.11 KB	4
user1002	4.22 KB	4
user1003	4.22 KB	4

Sous l'onglet **Utilisateurs** ou **Utilisateurs actifs**, cliquez sur un utilisateur pour afficher les détails de l'utilisateur suivants :

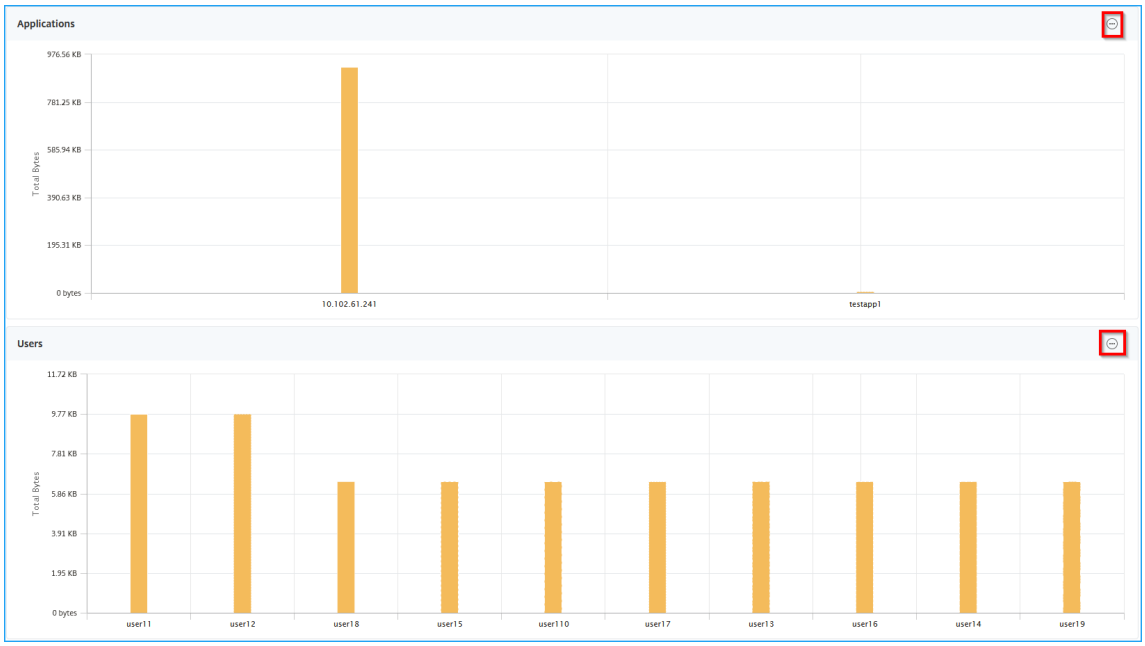
- **Détails de l'utilisateur** - Vous pouvez afficher des informations pour chaque utilisateur associé aux appliances de passerelle ADC. Accédez à **Analytics** > **Gateway Insight** > **Utilisateurs** et cliquez sur un utilisateur pour afficher les informations relatives à l'utilisateur sélectionné, comme le mode session, le système d'exploitation et les navigateurs.



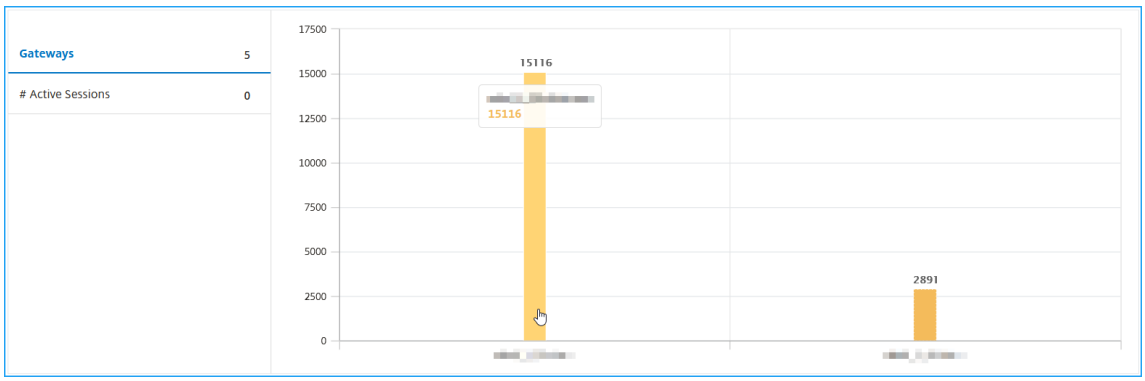
- **Utilisateurs et applications pour la passerelle sélectionnée** - Accédez à **Analytics** > **Gateway Insight** > **Gateway** et cliquez sur un nom de domaine de passerelle pour afficher les 10 principales applications et les 10 principaux utilisateurs associés à la passerelle sélectionnée.



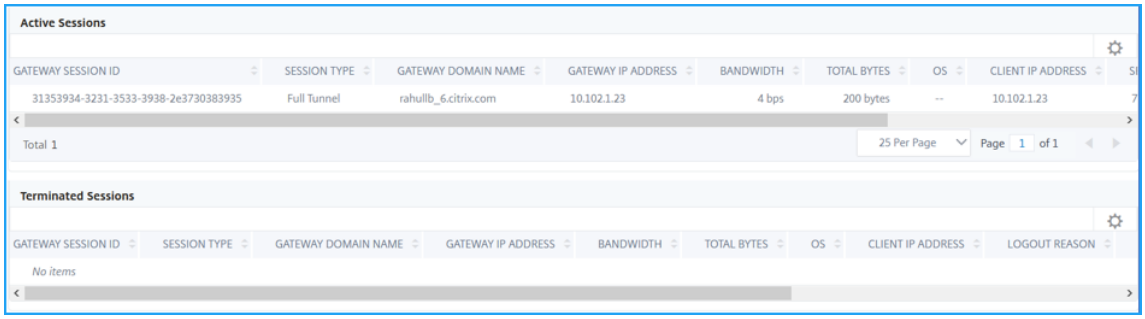
- **Afficher plus d'option pour les applications et les utilisateurs** : pour plus de 10 applications et utilisateurs, vous pouvez cliquer sur l'icône Plus dans Applications et utilisateurs pour afficher tous les détails des utilisateurs et applications associés à la passerelle sélectionnée.



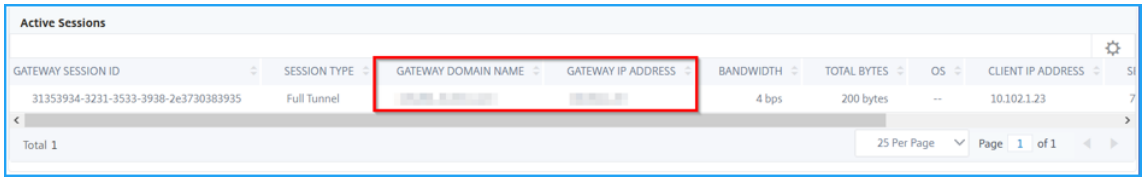
- **Afficher les détails en cliquant sur le graphique à barres** — Lorsque vous cliquez sur un graphique à barres, vous pouvez afficher les détails pertinents. Par exemple, accédez à **Analytics > Gateway Insight > Gateway** et cliquez sur le graphique à barres de passerelle pour afficher les détails de la passerelle.



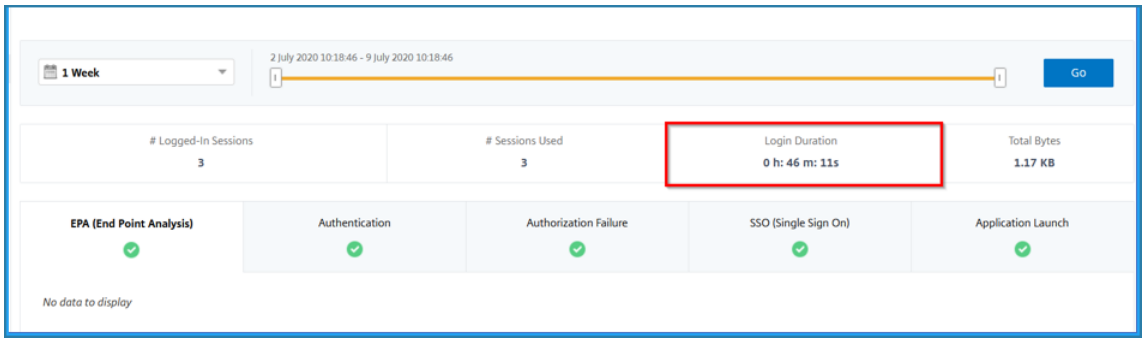
- L'utilisateur **Sessions actives et Sessionsterminées**.



- Le nom de domaine de la passerelle et l'adresse IP de la passerelle dans les **sessions actives**.

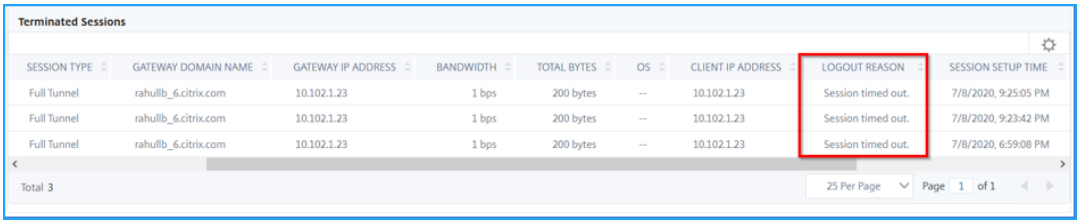


- Durée de connexion de l'utilisateur.



- Raison de la session de déconnexion de l'utilisateur. Les raisons de déconnexion peuvent être :
  - Session expirée
  - Déconnecté en raison d'une erreur interne
  - Déconnecté en raison de la session inactive expiré
  - L'utilisateur s'est déconnecté

– L'administrateur a arrêté la session



Barre de recherche et vue cartographique géographique

Vous pouvez voir :

- Barre de recherche qui vous permet de filtrer les résultats en fonction du nom d'utilisateur. Accédez à **Analytics > Gateway Insight > Utilisateurs** pour afficher la barre de recherche **Utilisateurs** et **Utilisateurs actifs**. Placez le pointeur de la souris sur la barre de recherche, sélectionnez **Nom d'utilisateur**et tapez un nom d'utilisateur pour filtrer les résultats.

- Carte géographique qui affiche les informations sur les utilisateurs en fonction de la position géographique des utilisateurs. En tant qu'administrateur, cette carte géographique vous permet d'afficher le récapitulatif du nombre total d'utilisateurs, du total des applications et du nombre total de sessions pour un emplacement spécifique.

  1. Accédez à **Analytics > Gateway Insight** pour afficher la carte géographique
  2. Cliquez sur un pays. Par exemple, les États-Unis

     La carte géographique affiche les détails tels que la liste des utilisateurs, les sessions actives, les sessions terminées, les applications pour le pays sélectionné.

Applications

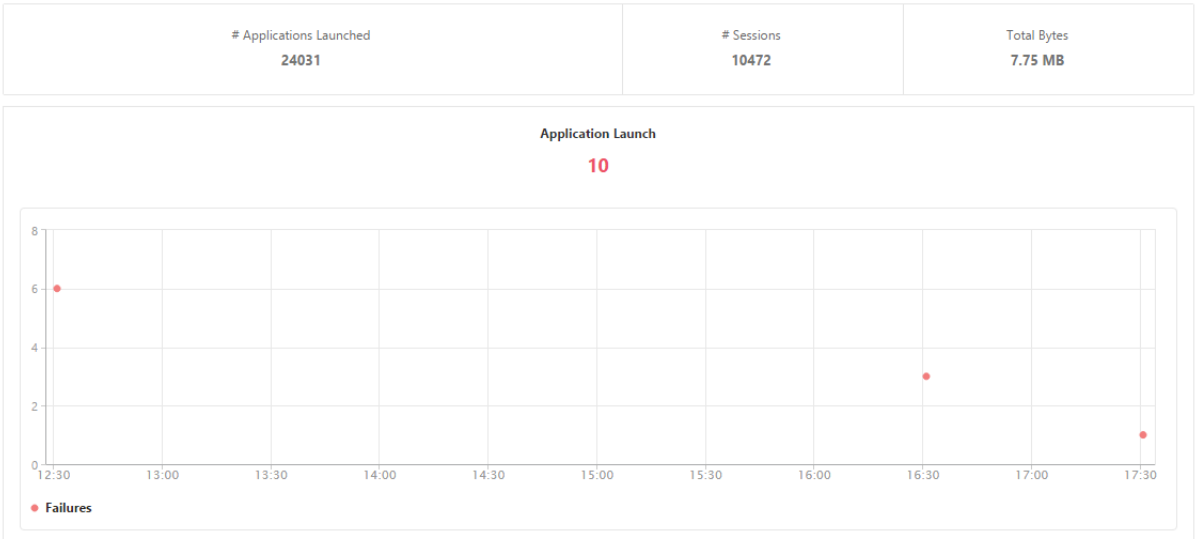
Vous pouvez afficher le nombre d'applications lancées, le nombre de sessions totales et actives, le nombre total d'octets et la bande passante consommée par les applications. Vous pouvez afficher

les détails des utilisateurs, des sessions, de la bande passante et des erreurs de lancement pour une application.

Afficher les détails de l'application

1. Dans Citrix ADM, accédez à **Analytics > Gateway Insight > Applications**.
2. Sélectionnez la période pour laquelle vous souhaitez afficher les détails de l'application. Vous pouvez utiliser le curseur temporel pour personnaliser davantage la période sélectionnée. Cliquez sur **OK**.

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 consommée par les applications.



Faites défiler vers le bas pour afficher le nombre de sessions, la bande passante et le nombre total d'octets consommés par ICA et d'autres applications.

Name	# Sessions	Bandwidth	Total Bytes
10.102.61.249	3972	52 bps	3.79 MB
c.go-mpulse.net	2	0 bps	1.53 KB
cdn.kendostatic.com	1	0 bps	805
code.jquery.com	1	0 bps	1.51 KB
engtools.citrite.net	2	0 bps	160
onebug.citrite.net	2	1 bps	86.21 KB

Sous l'onglet **Autres applications**, vous pouvez cliquer sur une application dans la colonne **Nom** pour afficher les détails de cette application.

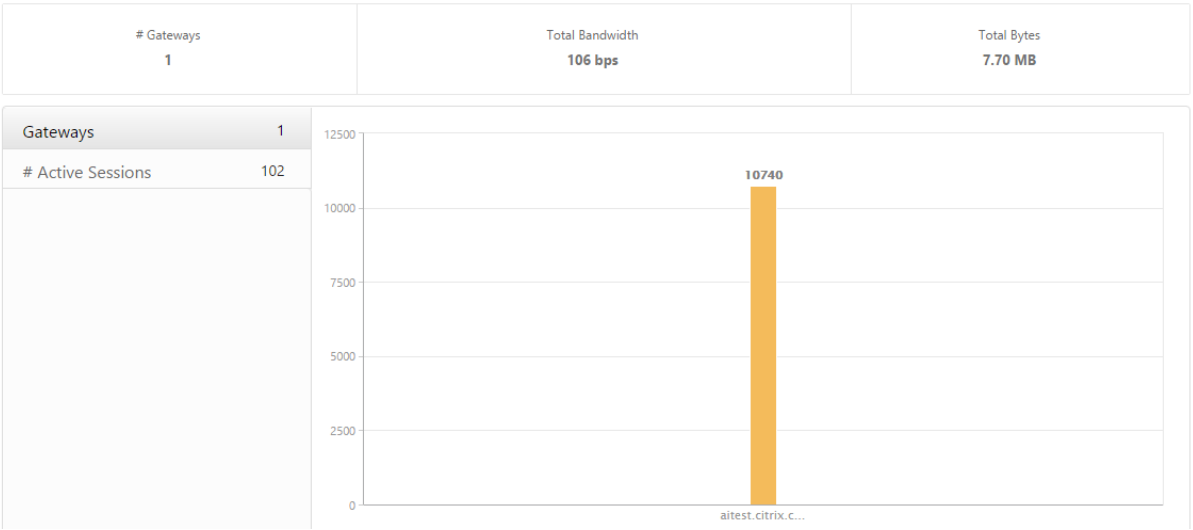
Passerelles

Vous pouvez 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 de passerelle ADC à un moment donné. 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.

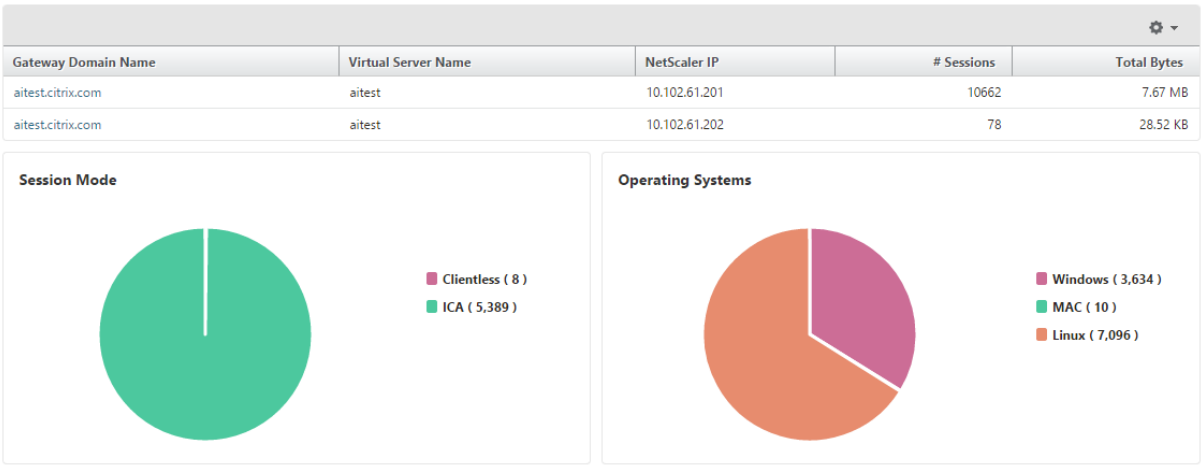
Afficher les détails de la Gateway

1. Dans Citrix ADM, accédez à **Analytics > Gateway Insight > Gateways**.
2. Sélectionnez la période pour laquelle vous souhaitez afficher les détails de la Gateway. Vous pouvez utiliser le curseur temporel pour personnaliser davantage la période sélectionnée. Cliquez sur **OK**.

Vous pouvez désormais 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 de passerelle ADC à un moment donné.



Faites défiler la page 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 ADC, 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.

Vous pouvez également afficher une carte géographique pour les passerelles qui vous permet de filtrer les utilisateurs en fonction d'un emplacement particulier.

1. Accédez à **Analytics > Gateway Insight > Gateways**
2. Sélectionnez un nom de domaine de passerelle pour afficher la carte géographique
3. Cliquez sur un pays. Par exemple, les États-Unis

   La carte géographique affiche les détails tels que la liste des utilisateurs, les sessions actives, les sessions terminées, les applications pour le pays sélectionné.

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 les rapports.
> - Les rapports de carte géographique sont exportés uniquement si l'ADM dispose d'une connectivité Internet.

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 modifier le programme d'exportation :

1. Sous l'onglet Configuration, accédez à **Configuration** > **NetScaler Insight Center** > **Exporter les programmes** .
2. Sélectionnez un rapport dans la liste disponible, puis cliquez sur **Modifier**.
3. Après la modification, cliquez sur **Enregistrer**.

> **Remarque**
>
> Configurez les paramètres du serveur de messagerie avant de planifier le rapport en accédant à **Système**> **Notifications**> **Email**et en cliquant sur **Ajouter**.

Pour ajouter un serveur de messagerie ou une liste de distribution de courrier électronique :

1. Sous l'onglet **Configuration**, accédez à **Système** > **Notifications** > **Email** .
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 obtenir une visibilité sur les détails d'accès, les applications et les passerelles des utilisateurs sur les appliances ADC Gateway.

1. L'utilisateur n'est pas en mesure de se connecter à l'appliance ADC Gateway ou aux serveurs Web internes

Vous êtes un administrateur de passerelle ADC qui surveille les appliances de passerelle ADC via ADM et vous voulez savoir pourquoi un utilisateur ne peut pas se connecter ou à quel stade du processus de connexion l'échec s'est produit.

ADM vous permet d'afficher les détails de l'erreur de connexion utilisateur dans les étapes suivantes du processus de connexion :

- Authentification
- Analyse des points terminaux (EPA)
- Single Sign-On

Dans ADM, vous pouvez rechercher un utilisateur particulier, puis afficher tous les détails de cet utilisateur.

Pour rechercher un utilisateur :

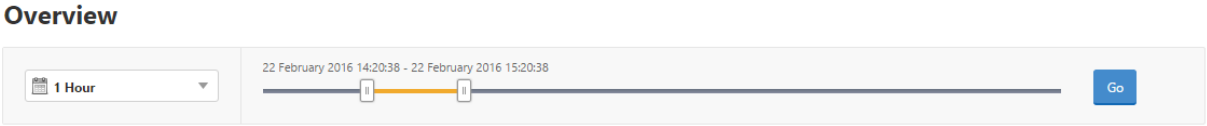
Dans Citrix ADM, accédez à **Analytics > Gateway Insight** et, dans la zone de texte **Rechercher des utilisateurs**, spécifiez l'utilisateur à rechercher.

Échecs d'authentification

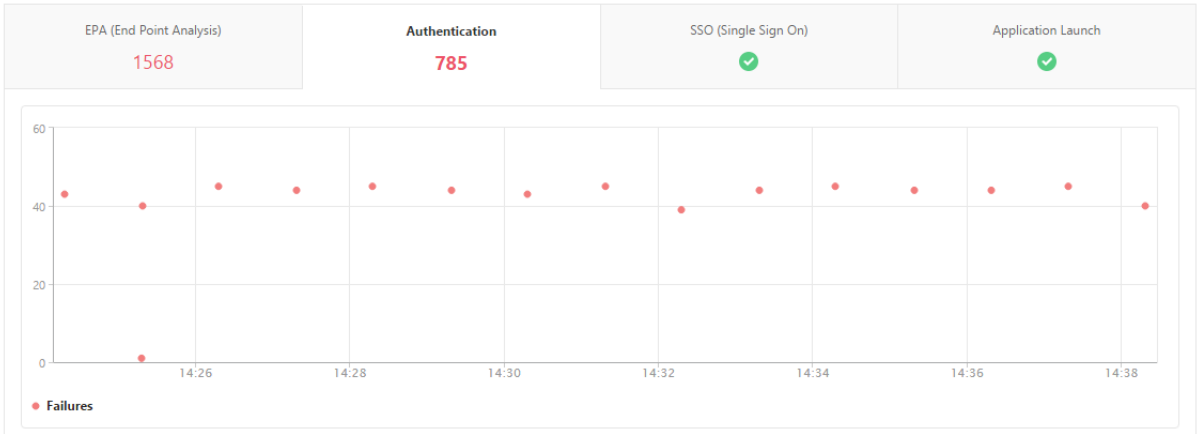
Vous pouvez afficher des erreurs d'authentification telles que des informations d'identification incorrectes ou aucune réponse du serveur d'authentification. Si vous avez configuré l'authentification en deux étapes, vous pouvez voir si les étapes primaire, secondaire ou les deux ont échoué.

Afficher les détails de l'échec d'authentification

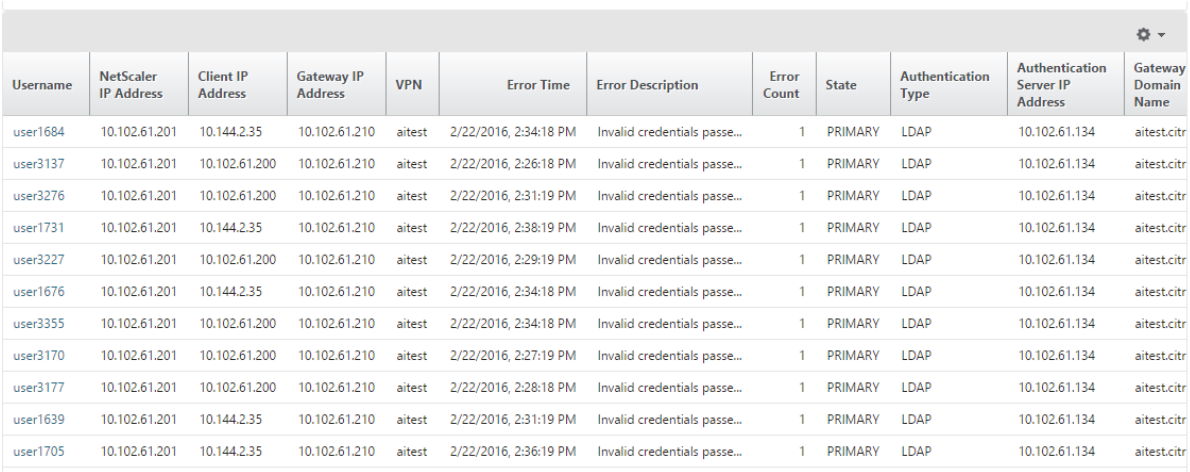
1. Dans Citrix ADM, accédez à **Analytics > Gateway Insight**.
2. Dans la section **Vue d'ensemble**, sélectionnez la période pour laquelle vous souhaitez afficher les erreurs d'authentification. Vous pouvez utiliser le curseur temporel pour personnaliser davantage la période sélectionnée. Cliquez sur **OK**.



1. Cliquez sur l'onglet **Authentification**. Vous pouvez afficher le nombre d'erreurs d'authentification à un moment donné dans le graphique **Échecs** .



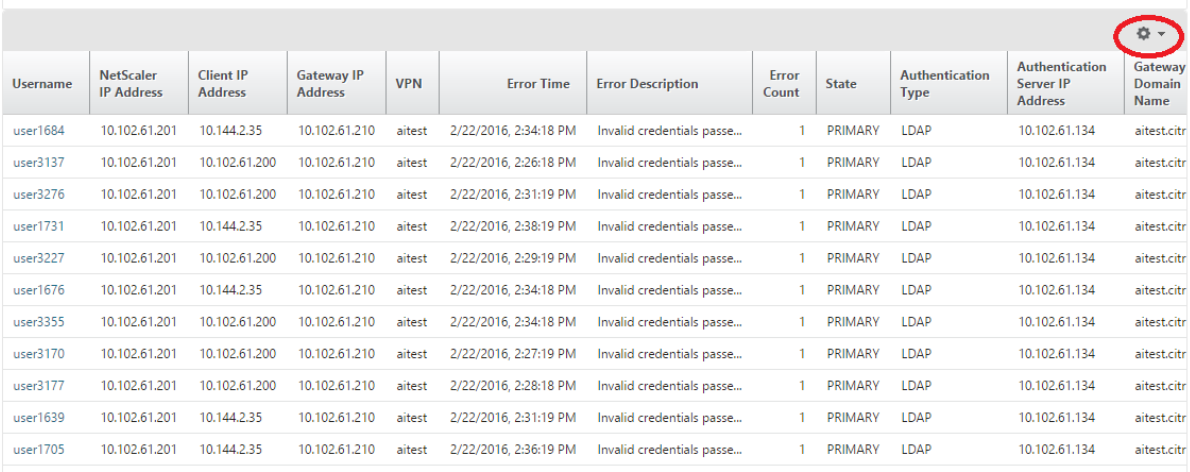
Faites défiler la page vers le bas pour afficher les détails de chaque erreur d'authentification, **tels que Nom d'utilisateur, Adresse IP du client, Heure de l'erreur, Type d'authentification, Adresse IP du serveur**d'authentification, etc., à partir du tableau du même onglet. La colonne **Description 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 de liste comme indiqué dans l'image suivante.



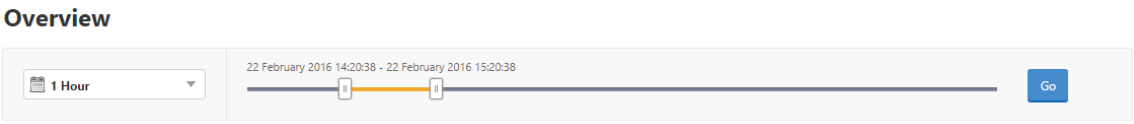
Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	State	Authentication Type	Authentication Server IP Address	Gateway Domain Name
user1684	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	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

Échecs de l'EPA

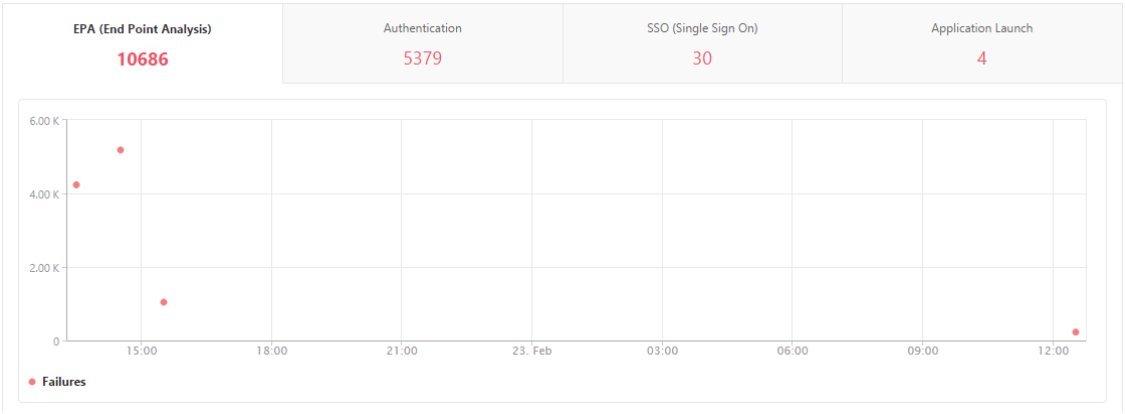
Vous pouvez afficher les échecs EPA au stade de pré-authentification ou post-authentification.

Afficher les détails de l'échec de l'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 **OK**.



3. Cliquez sur l'onglet **EPA (End Point Analysis)**. Vous pouvez afficher le nombre d'erreurs EPA à tout moment dans le graphique **Failures**.



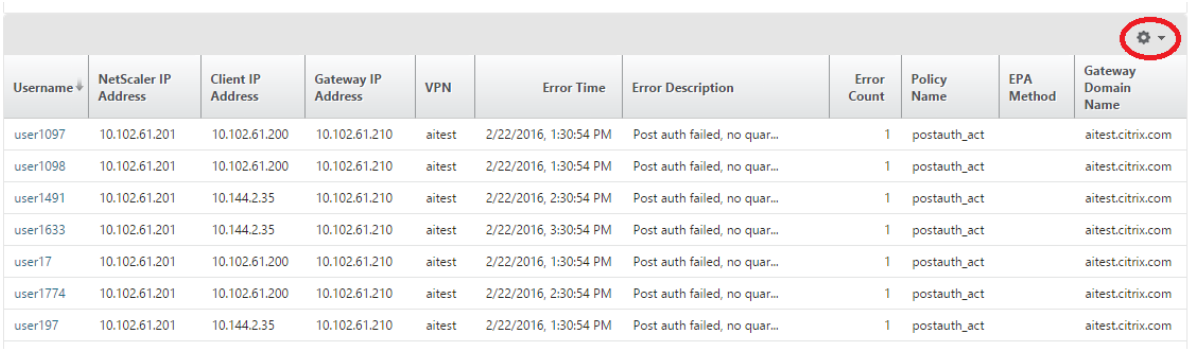
Faites défiler la page vers le bas pour afficher les détails de chaque erreur EPA telles que le **nom d'utilisateur, l'adresse IP ADC, l'adresse IP de la passerelle, le VPN, l'heure de l'erreur, le nom de la stratégie, le nom de domaine de la passerelle** et bien plus encore à partir du tableau du même 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 de

liste comme indiqué dans l'image suivante.



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

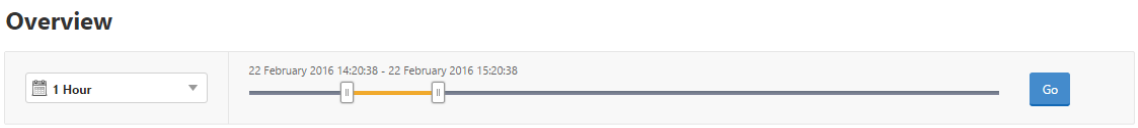
> **Remarque**
>
> ADC Gateway ne signale pas les échecs EPA lorsque l'expression « ClientSecurity » est configurée en tant que règle de stratégie de session VPN.

Échecs SSO

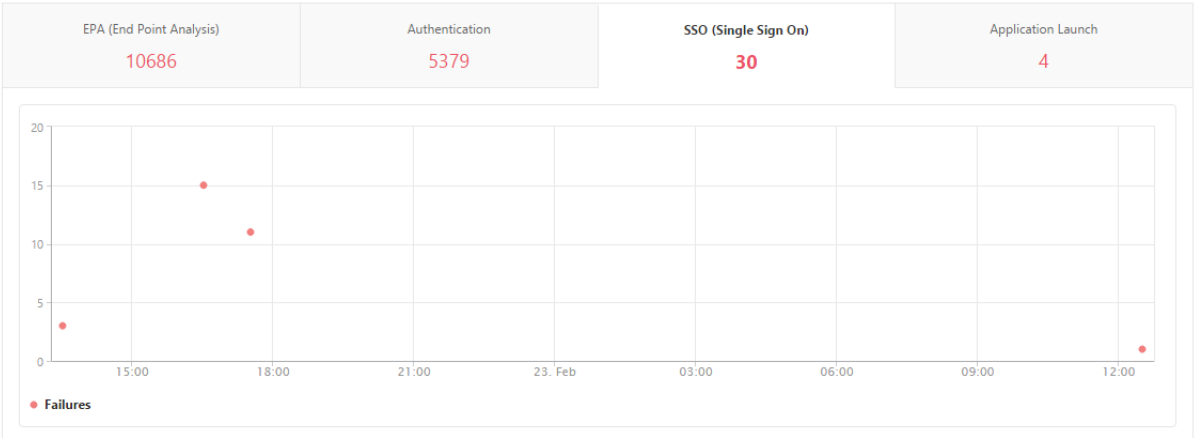
Vous pouvez afficher toutes les échecs SSO à n'importe quel stade pour un utilisateur accédant à des applications via l'appliance ADC Gateway.

Afficher les détails de l'échec de l'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 **OK**.



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 la page vers le bas pour afficher les détails de chaque erreur SSO, tels que le **nom d'utilisateur, l'adresse IP ADC, l'heure de l'erreur, la description de l'erreur, le nom de la ressource,** etc., à partir du 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 de liste comme indiqué dans l'image suivante.

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

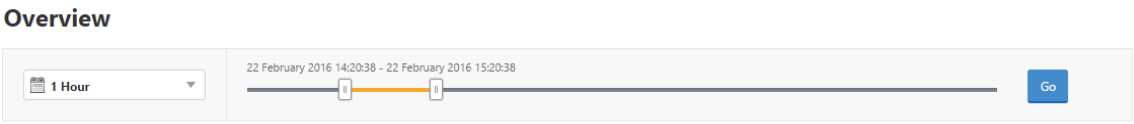
2. Après avoir ouvert une session sur ADC Gateway, un utilisateur ne peut pas lancer d'application virtuelle

En cas d'échec du lancement d'une application, vous pouvez obtenir une visibilité sur les raisons, telles que le serveur STA (Secure Ticket Authority) ou Citrix Virtual App, ou un ticket STA non valide.

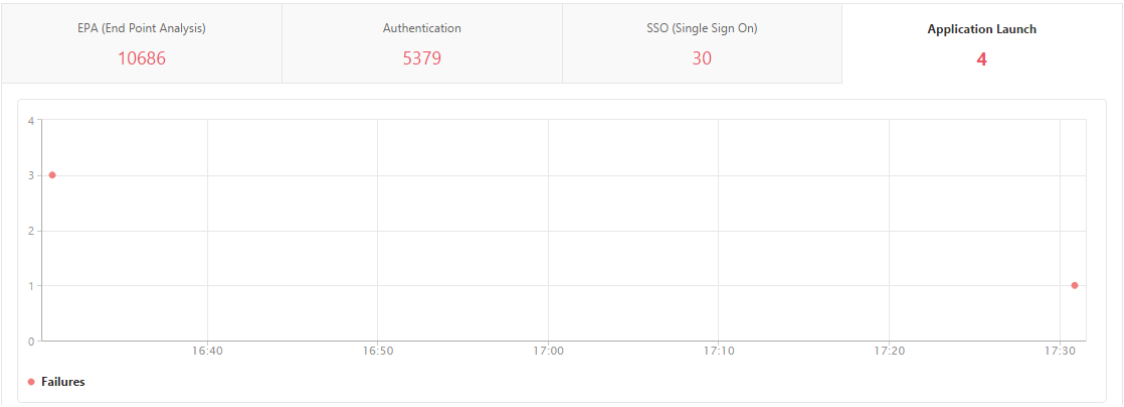
Vous pouvez afficher l'heure à laquelle l'erreur s'est produite, les détails de l'erreur et la ressource pour laquelle la validation STA a échoué.

Afficher les détails de l'échec du 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 **OK**.



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**.

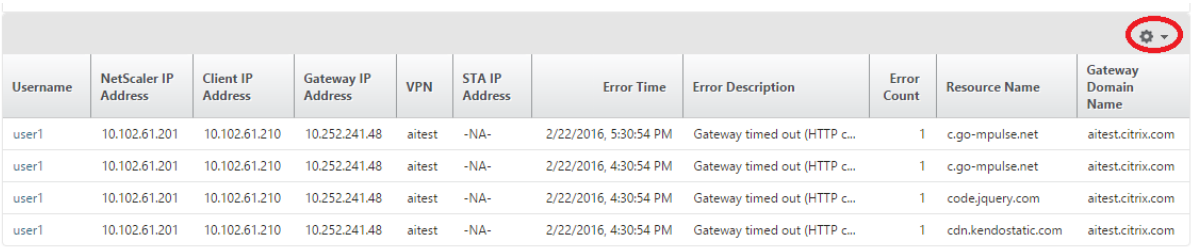


Faites défiler la page vers le bas pour afficher les détails de chaque erreur de lancement d'application, telles que **l'adresse IP ADC, l'heure de l'erreur, la description de l'erreur, le nom de la ressource, le nom de domaine de la passerelle**, etc., à partir du tableau du même onglet. La colonne **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 de liste comme indiqué dans l'image suivante.



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

3. Après le lancement réussi d'une nouvelle application, un utilisateur souhaite afficher le nombre total d'octets et de bande passante consommés par cette application

Après avoir lancé une nouvelle application avec succès, dans Citrix ADM, vous pouvez afficher le nombre total d'octets et de bande passante consommés par cette application.

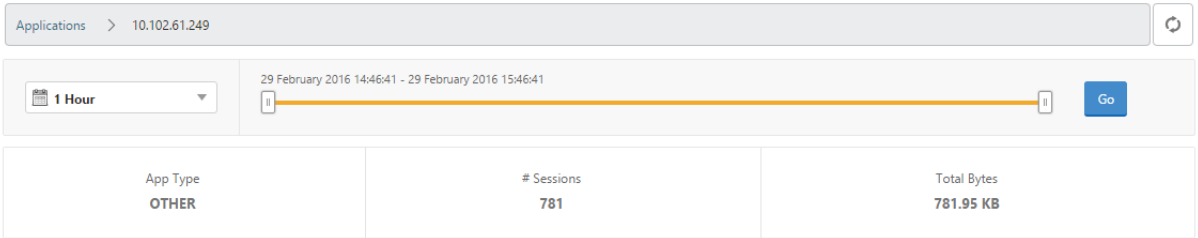
Afficher le nombre total d'octets et de bande passante consommés par une application

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.

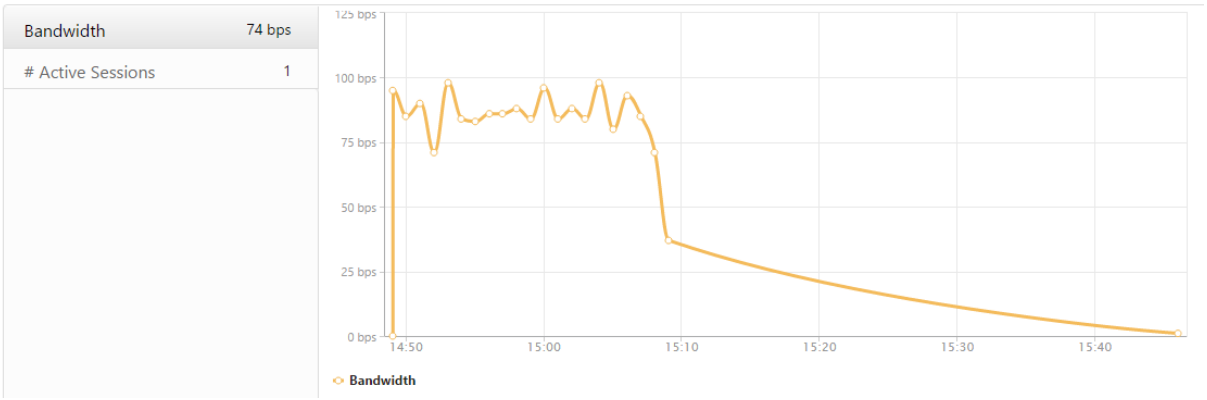
ICA Applications | Other Applications

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.



Vous pouvez également afficher la bande passante consommée par cette application.

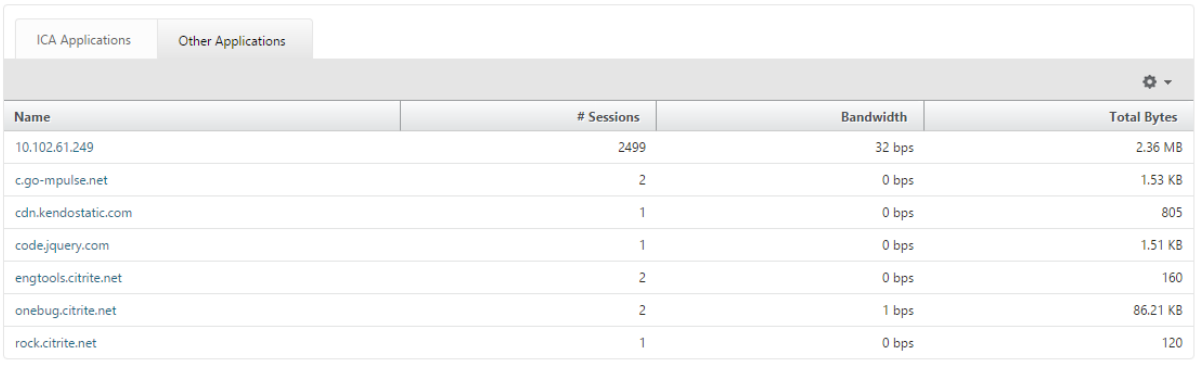


4. Un utilisateur s'est connecté à ADC Gateway avec succès, mais n'est pas en mesure d'accéder à certaines ressources réseau du réseau interne

Avec Gateway Insight, vous pouvez déterminer si l'utilisateur a accès aux ressources réseau ou non. Vous pouvez également afficher le nom de la stratégie à l'origine de l'échec.

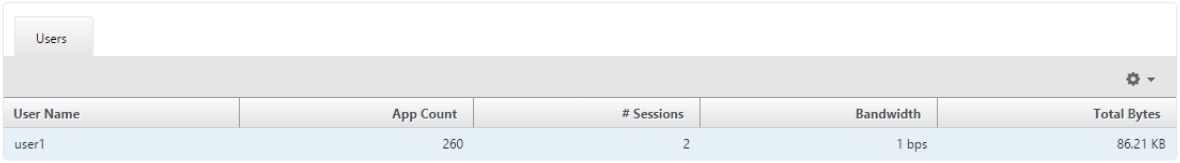
Afficher l'accès utilisateur pour les ressources

1. Dans Citrix ADM, **accédez à Analytics > Gateway Insight > Applications**.
2. Sur l'écran qui apparaît, faites défiler la page vers le bas et **sous l'onglet Autres applications**, sélectionnez l'application à laquelle l'utilisateur n'a pas pu se connecter.



Name	# Sessions	Bandwidth	Total Bytes
10.102.61.249	2499	32 bps	2.36 MB
c.go-mpulse.net	2	0 bps	1.53 KB
cdn.kendostatic.com	1	0 bps	805
code.jquery.com	1	0 bps	1.51 KB
engtools.citrite.net	2	0 bps	160
onebug.citrite.net	2	1 bps	86.21 KB
rock.citrite.net	1	0 bps	120

Sur l'écran qui apparaît, faites défiler vers le bas et dans le tableau **Utilisateurs**, tous les utilisateurs qui ont accès à cette application s'affichent.



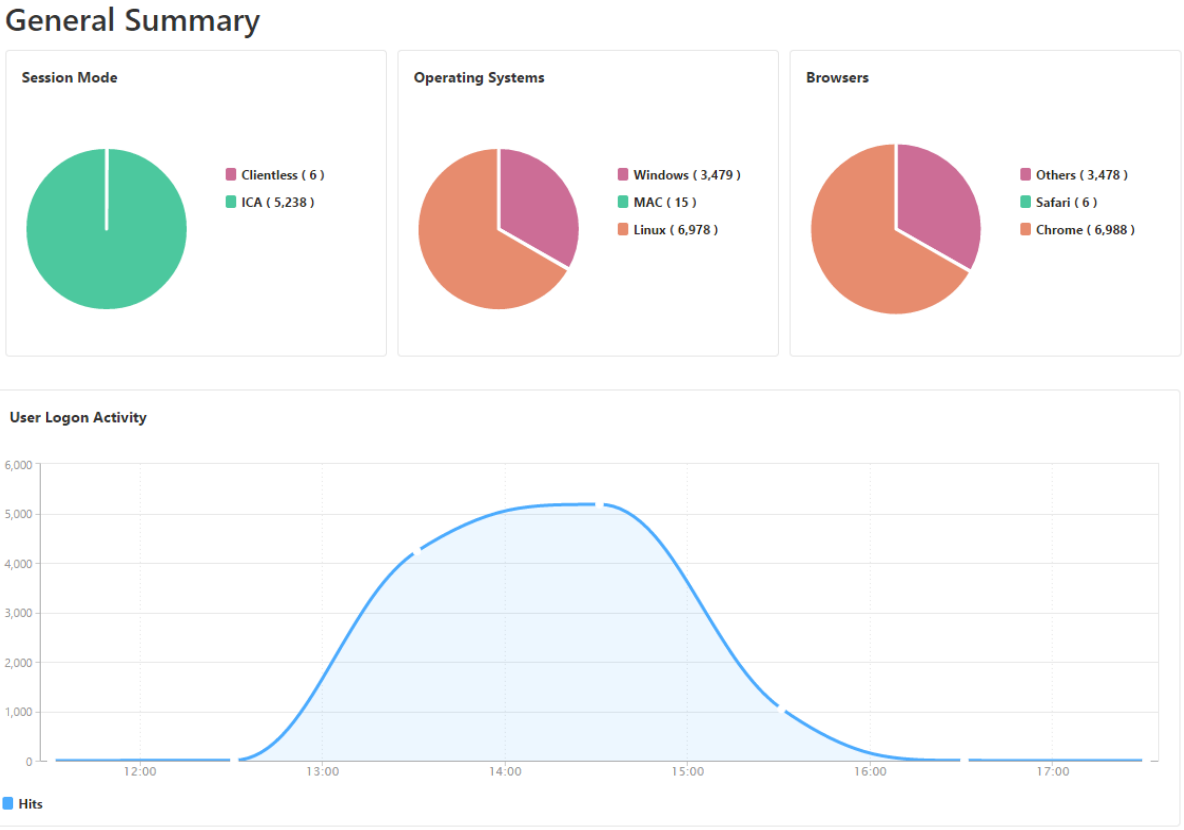
User Name	App Count	# Sessions	Bandwidth	Total Bytes
user1	260	2	1 bps	86.21 KB

5. Différents utilisateurs peuvent utiliser différents déploiements ADC Gateway ou ouvrir une session à ADC 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 ADC 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.

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.



Résoudre les problèmes liés à Gateway Insight

April 29, 2021

Si la solution Gateway Insight ne fonctionne pas comme prévu, le problème peut être lié à l'un des éléments suivants. Reportez-vous aux listes de contrôle des sections respectives pour le dépannage.

- Configuration 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 commande `show running | grep -i <appflow_policy>` pour vérifier la configuration de Gateway Insight. Assurez-vous que le type de liaison est REQUEST. Par exemple ;

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
  ```

- 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, consultez Activation de la collecte de données HDX Insight.
- Vérifiez le paramètre `appflowlog` dans le serveur virtuel Citrix Gateway/VPN. Pour plus de détails, consultez la section 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 plus de détails, consultez Comment faire pour vérifier l'état de la connectivité entre Citrix ADC et AppFlow Collector.
- Vérifiez les accès à la stratégie AppFlow Gateway Insight.

  Exécutez la commande `show appflow policy <policy_name>` pour vérifier les succès de stratégie AppFlow.

  Vous pouvez également accéder à **Système > AppFlow > Stratégies** dans l'interface graphique pour vérifier les accès à la stratégie AppFlow.

- Validez tout pare-feu bloquant les ports AppFlow 4739 ou 5557.

Liste de contrôle de la génération d'enregistrements dans Citrix ADC

- Exécutez la commande `nsconmsg -d stats -g ai_tot` et vérifiez les incréments de statistiques dans Citrix ADC.
- Capturez les journaux `nstrace` et recherchez les paquets CFLOW pour confirmer que Citrix ADC exporte les enregistrements AppFlow.

Validations dans Citrix ADM

- Exécutez la commande `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: vpn_"` pour vérifier les journaux pour confirmer que Citrix ADM reçoit des enregistrements AppFlow.
- Assurez-vous que l'instance Citrix ADC est ajoutée à Citrix ADM.
- Assurez-vous que le serveur virtuel Citrix Gateway/VPN est sous licence dans Citrix ADM.

Statistiques Gateway Insight

Les statistiques Gateway Insight suivantes 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 que vous disposez des informations suivantes avant de contacter le support technique Citrix :

- Détails du déploiement et de la topologie du réseau.
- Versions Citrix ADC et Citrix ADM.
- Offre groupée de support technique pour Citrix ADC et Citrix ADM.

- `nstrace` lors du problème.

Problèmes connus

Reportez-vous aux notes de mise à jour de Citrix ADC pour connaître les problèmes connus sur Gateway Insight.

Afficher les détails des violations de sécurité des applications

April 29, 2021

Les applications Web exposées à Internet sont devenues extrêmement vulnérables aux attaques. Citrix ADM vous permet de visualiser les détails des violations exploitables pour protéger les applications contre les attaques. Accédez à **Analytics** > **Sécurité> Violations** de sécurité pour une solution à volet unique pour :

- Visualisez les applications avec une visibilité totale sur les détails des menaces associés à la fois dans les informations de sécurité et les informations sur les robots
- Accéder aux violations de sécurité des applications en fonction de ses catégories telles que **Network**, **Bot**et **WAF**
- Prendre des mesures correctives pour sécuriser les applications

La page **Violations de sécurité** comporte les options suivantes :

- **Vue d'ensemble des applications** : affiche une vue d'ensemble des applications qui présentent des violations totales, des violations totales de WAF et de bot, des violations par pays, etc. Pour de plus amples informations, consultez la section Présentation de l'application.
- **Toutes les violations** : affiche les détails de la violation de sécurité de l'application. Pour de plus amples informations, consultez la section Toutes les violations.

Configuration

Vous devez activer **Advanced Security Analytics** et sélectionner **Paramètres de transaction Web** sur **tous** pour afficher les violations suivantes dans Citrix ADM :

- Transactions de chargement exceptionnellement élevées (WAF)
- Transactions de téléchargement exceptionnellement élevées (WAF)
- IPs uniques excessifs (WAF)
- Prise en charge de compte (BOT)

- Scanners de site Web (BOT)
- Grattoirs de contenu (BOT)

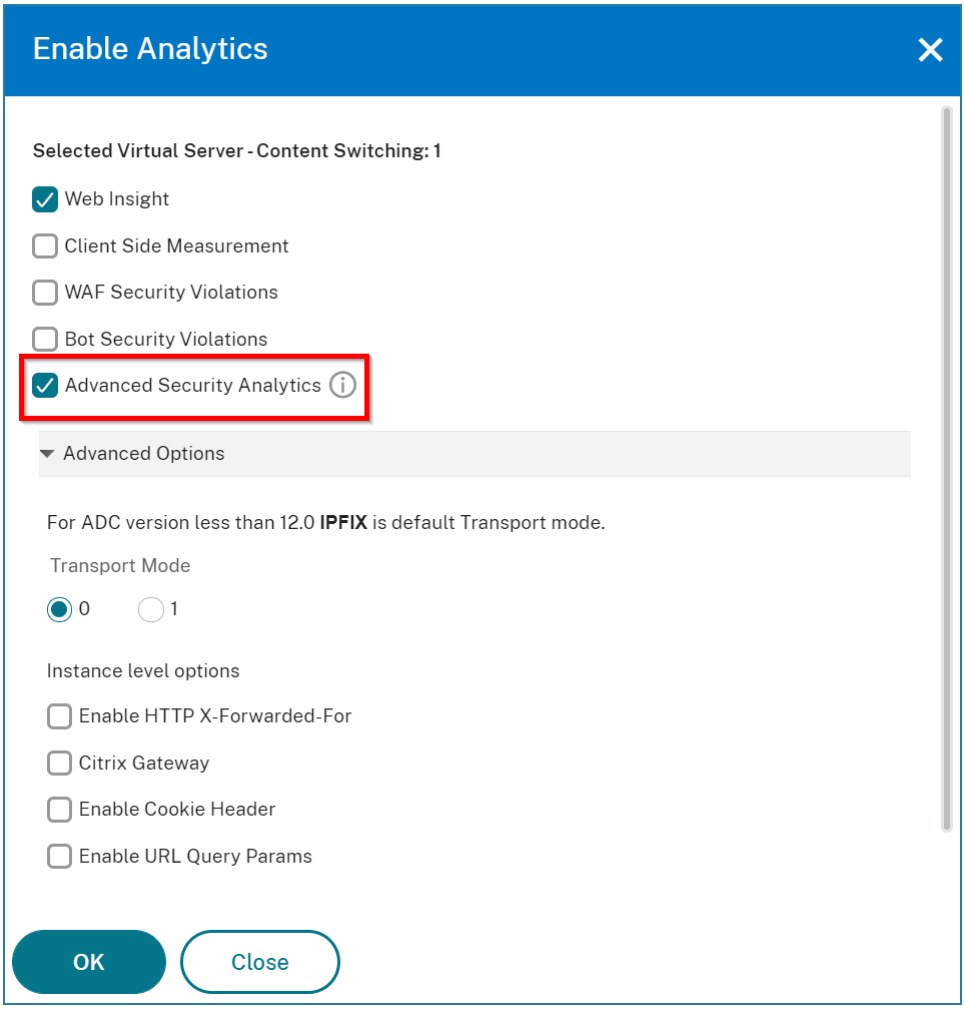
Pour les autres violations, vérifiez si **Metrics Collector** est activé. Par défaut, **Metrics Collector** est activé sur l'instance de Citrix ADC. Pour de plus amples informations, consultez la section Configurer Intelligent App Analytics.

Activer les analyses de sécurité avancées

1. Accédez à **Réseaux** > **Instances** > **Citrix ADC**, puis sélectionnez le type d'instance. Par exemple, MPX.
2. Sélectionnez l'instance Citrix ADC et, dans la liste **Sélectionner une action**, sélectionnez **Configurer Analytics**.
3. Sélectionnez le serveur virtuel et cliquez sur **Activer Analytics**.
4. Dans la fenêtre **Activer Analytics** :
   a) Sélectionnez **Web Insight**. Après avoir sélectionné Web Insight, l'option **Advanced Security Analytics** en lecture seule est activée automatiquement.

      > **Remarque**
      >
      > L'option **Advanced Security Analytics** s'affiche uniquement pour les instances ADC sous licence premium.

   b) Sélectionnez **Logstream** comme mode de transport
   c) L'expression est true par défaut
   d) Cliquez sur **OK**.

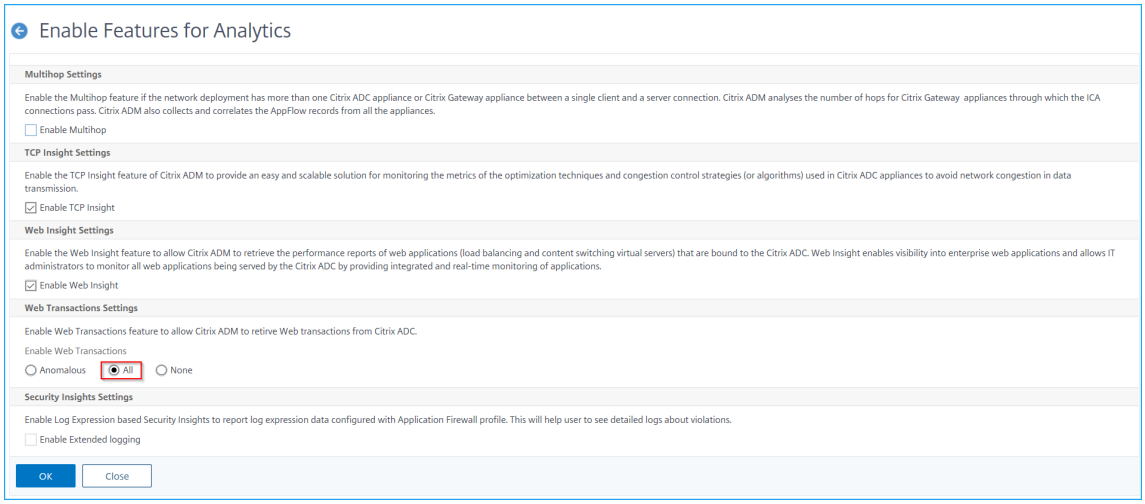


Activer les paramètres de transaction Web

1. Accédez à **Analytics** > **Paramètres** .

   La page **Paramètres** s'affiche.

2. Cliquez sur **Activer les fonctionnalités pour Analytics**.
3. Sous **Paramètres de transaction Web**, sélectionnez **Tout**.



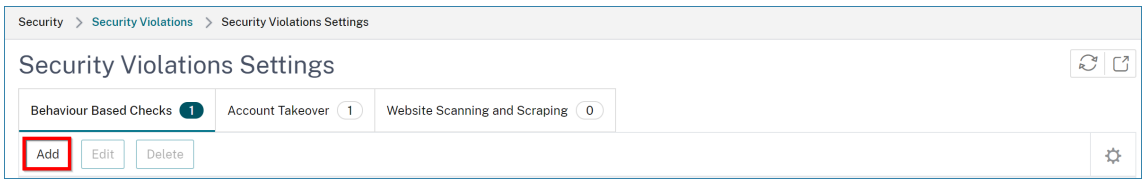
4. Cliquez sur **OK**.

Configurer les profils de vérification du comportement

Citrix ADM vous permet de sélectionner les violations basées sur le comportement. Pour les **connexions client excessives**, l' **analyse de site Web**, les **transactions de téléchargement exceptionnellementélevées et les violations de transactions de téléchargement**exceptionnellement élevées, vous pouvez choisir le niveau de sensibilité comme**Faible**,**Moyen**et**Élevé**. En créant un profil, vous pouvez décider comment Citrix ADM signale le nombre total d'anomalies pour ces violations.

Pour configurer ce paramètre :

1. Accédez à **Analytics > Sécurité > Violations de sécurité**.
2. Cliquez sur l'icône de paramètres disponible en regard de la liste de durée de temps.
3. Sous **Vérifications basées sur le comportement**, cliquez sur **Ajouter**.

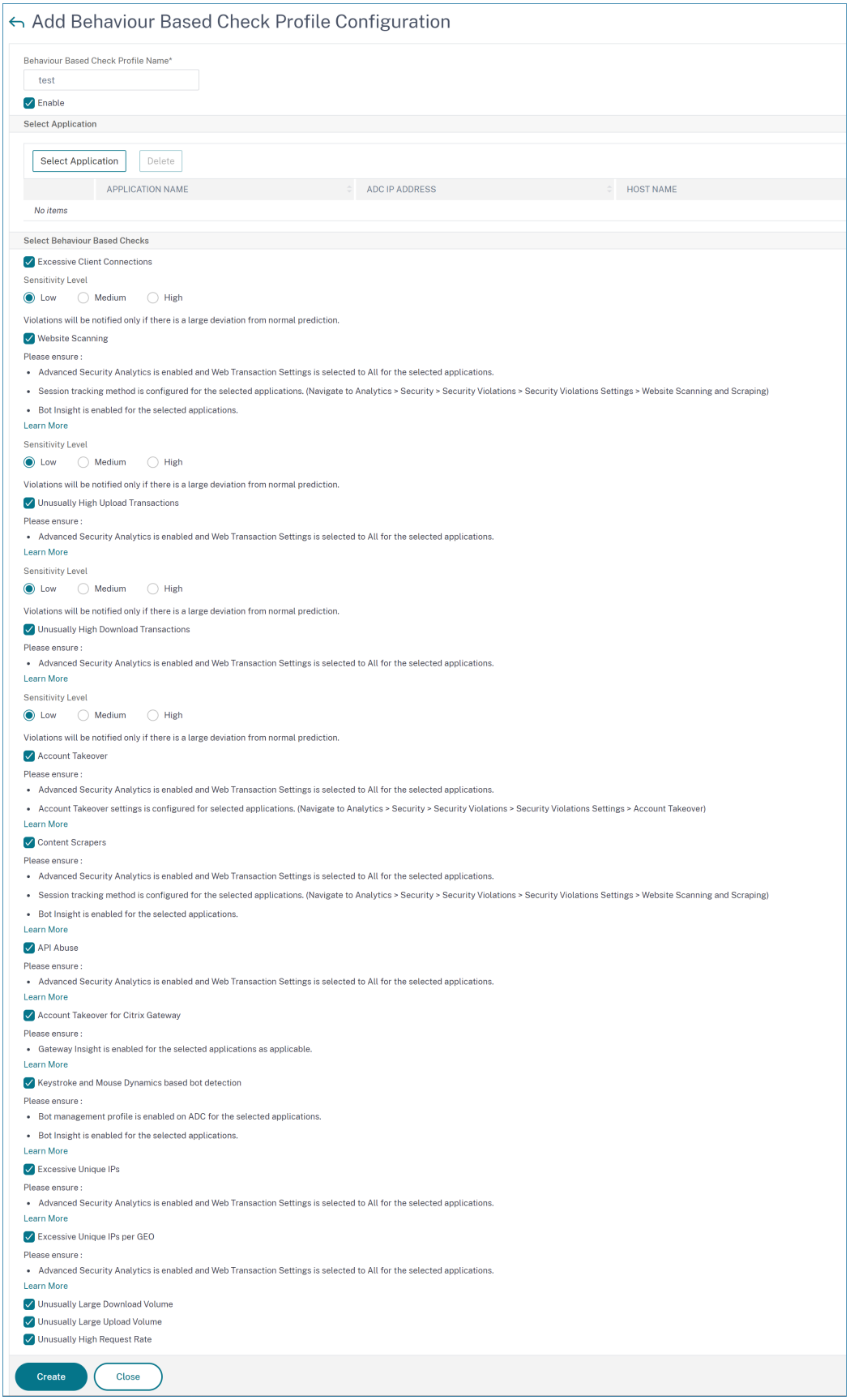


4. Spécifiez les paramètres suivants :
   a) **Nom du profil de vérification basé sur le comportement** — Spécifiez le nom de profil de votre choix.
   b) Sélectionnez l'option **Activer**. Cette option est sélectionnée par défaut.
   c) Sous **Sélectionner une application**, sélectionnez les applications pour lesquelles vous souhaitez appliquer le profil.

d) Sous **Sélectionner les contrôles basés sur le comportement**, sélectionnez **Faible**, **Moyen**ou **Élevé** pour définir le niveau de sensibilité des violations mentionnées.

> **Remarque**
>
> Par défaut, toutes les autres violations basées sur le comportement sont également activées. Si vous désactivez une violation, Citrix ADM détecte les anomalies pour ces violations uniquement en fonction d'une prédiction normale.

e) Cliquez sur **Créer**.



Moteur d'apprentissage WAF

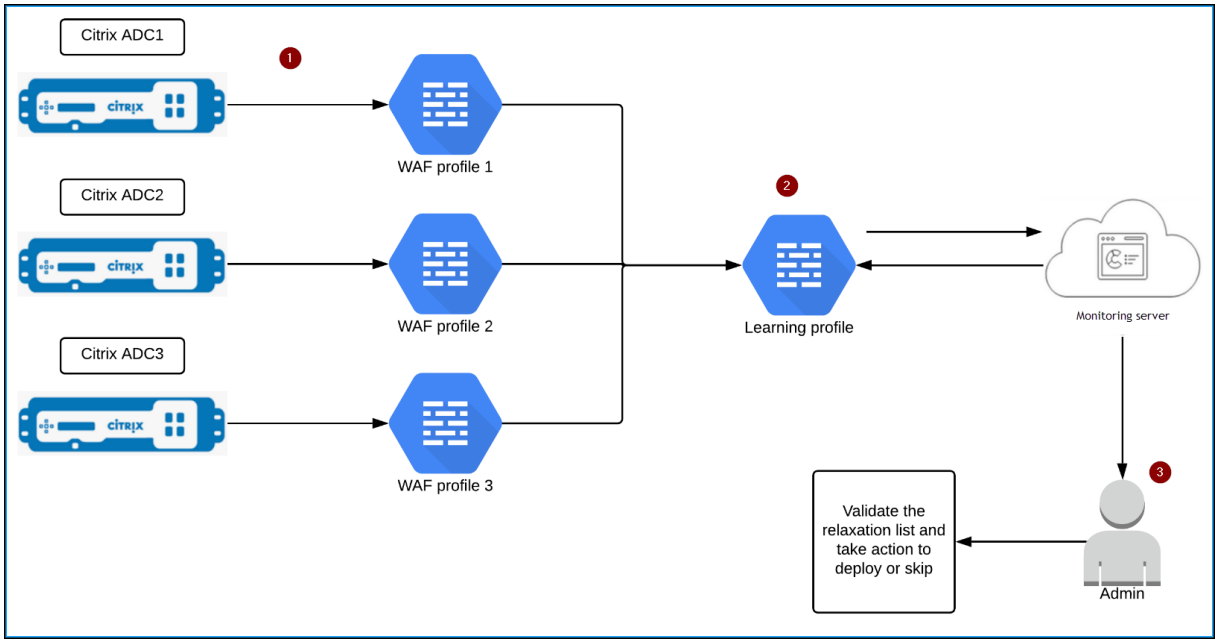
April 29, 2021

Citrix Web App Firewall (WAF) protège vos applications Web contre les attaques malveillantes telles que l'injection SQL et les scripts inter-sites. Pour prévenir les violations de données et assurer la protection de sécurité adéquate, vous devez surveiller votre trafic à la recherche de menaces et de données exploitables en temps réel sur les attaques. Parfois, les attaques signalées peuvent être faussement positives et celles-ci doivent être fournies à titre d'exception.

Le moteur d'apprentissage sur Citrix ADM est un filtre de répétition qui permet à WAF d'apprendre le comportement (les activités normales) de vos applications Web. Sur la base de la surveillance, le moteur génère une liste de règles ou d'exceptions suggérées pour chaque vérification de sécurité appliquée au trafic HTTP.

Il est beaucoup plus facile de déployer des règles de relaxation à l'aide du moteur d'apprentissage que de le déployer manuellement en tant que relaxations nécessaires.

L'image suivante explique les informations de haut niveau sur le fonctionnement de l'apprentissage WAF dans Citrix ADM :



1 — Instances Citrix ADC avec ses profils WAF

2 — Configurez un profil d'apprentissage dans Citrix ADM, ajoutez les profils WAF et sélectionnez de déployer automatiquement ou de déployer manuellement les règles de relaxation

3 — L'administrateur peut valider les règles de relaxation dans Citrix ADM et décider de déployer ou d'ignorer

Mise en route

Pour déployer la fonctionnalité d'apprentissage, vous devez d'abord configurer un profil de Web App Firewall (ensemble de paramètres de sécurité) sur votre appliance Citrix ADC. Pour de plus amples informations, consultez la section Création de profils de Web App Firewall.

Citrix ADM génère une liste d'exceptions (relaxations) pour chaque vérification de sécurité. En tant qu'administrateur, vous pouvez consulter la liste des exceptions dans Citrix ADM et décider de déployer ou d'ignorer.

À l'aide de la fonctionnalité d'apprentissage WAF dans Citrix ADM, vous pouvez :

- Configurer un profil d'apprentissage avec les contrôles de sécurité suivants
  - URL de démarrage
  - Cohérence des
  - Carte de crédit

    > **Remarque**
    >
    > Pour la vérification de sécurité de la carte de crédit, vous devez configurer `doSecureCreditCardLogging` l'instance Citrix ADC et vous assurer que le paramètre est **OFF**.

  - Type de contenu
  - Cohérence des champs de formulaire
  - Formats de champs
  - Balisage de formulaire CSRF
  - Scriptage inter-sites HTML

    > **Remarque**
    >
    > La limitation de l'emplacement d'un script inter-site est uniquement FormField.

  - Injection SQL HTML

    > **Remarque**
    >
    > Pour la vérification de l'injection SQL HTML, vous devez configurer `set -sqlinjectionTransformSpecialChars ON` et `set -sqlinjectiontype sqlspclcharorkeywords`dans l'instance Citrix ADC.

- Vérifiez les règles de relaxation dans Citrix ADM et décidez de prendre les mesures nécessaires (déployer ou ignorer)
- Recevez les notifications par e-mail, slack et ServiceNow

- Utilisez la page **Récapitulatif des actions** pour afficher les détails de relaxation

Pour utiliser l'apprentissage WAF dans Citrix ADM :

1. Configurer le profil d'apprentissage
2. Voir les règles de relaxation
3. Utiliser la page Récapitulatif des actions d'apprentissage WAF

TCP Insight

April 29, 2021

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 « Rapport de vitesse TCP », qui mesure les performances de téléchargement ou de téléchargement 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. Les ventilations par direction du flux (du client à Citrix ADC et Citrix ADC au serveur d'origine), par port TCP et par réseau local virtuel sont fournies pour les mesures ci-dessus.

Conditions préalables

Avant de commencer à configurer la fonctionnalité TCP Insight, assurez-vous que les conditions préalables suivantes sont remplies :

- Les instances de Citrix ADC s'exécutent sur la version logicielle 11.1 build 51.21 ou ultérieure.
- Vous avez installé Citrix ADM en cours d'exécution 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, reportez-vous à la sectionSystème de licences.

Configuration matérielle requise pour Citrix ADM :

Composant	Exigences
RAM	8 Go
CPU virtuel	4
	Remarque Citrix vous recommande d'utiliser 8 processeurs pour de meilleures performances.
Espace de stockage	120 Go
	Remarque Citrix vous recommande d'utiliser 500 Go pour de meilleures performances.

Activation de TCP Insight

Avant de pouvoir afficher les mesures TCP Insight, vous devez activer la fonctionnalité sur Citrix ADM.

Pour activer TCP Insight :

1. Dans un navigateur Web, tapez l'adresse IP de l'appliance virtuelle Citrix ADM (par exemple, `http://192.168.100.1`).
2. Dans **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Accédez à **Analytics** > **Paramètres**, puis cliquez sur **Activer les fonctionnalités pour Analytics** .
4. Sur la page **Activer les fonctionnalités pour Analytics**, sélectionnez **Activer TCP Insight** .
5. Dans la fenêtre de confirmation, cliquez sur **OK**.

Afficher les mesures TCP Insight dans Citrix ADM

Après avoir activé TCP Insight dans Citrix ADM, vous pouvez afficher les informations de couche de transport clés 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 Paramètres du tableau. Vous pouvez également sélectionner la période à laquelle les mesures se rapportent et ajuster la période à l'aide du curseur temporel.

Vous pouvez également afficher des mesures pour des éléments tels que les interfaces, les ports et les débits binaires en sélectionnant dans la liste **TCP Insight** .

Cas d'utilisation

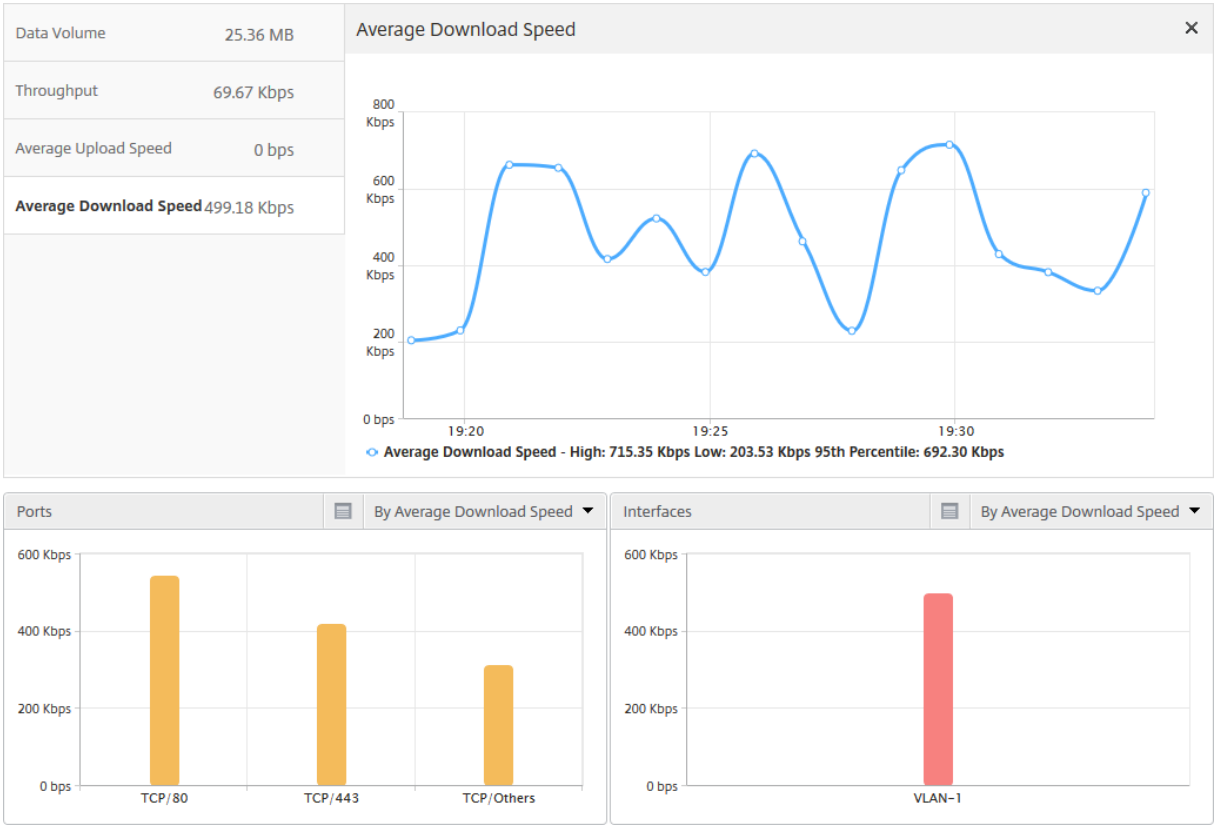
Les cas d'utilisation suivants illustrent certaines des façons d'utiliser TCP Insight sur les appliances Citrix ADC :

- Évaluer les avantages de l'optimisation TCP
- Régler les paramètres TCP
- Mesurer l'impact de l'optimisation TCP sur le volume de trafic

Évaluer les avantages de l'optimisation TCP

Combien l'optimisation Citrix ADC TCP profite réellement à un réseau mobile (radio) ou d'entreprise (internet) ? Vous pouvez afficher la vitesse des transferts de données qui ont lieu sur TCP et comparer les performances non optimisées et optimisées. Ces mesures sont affichées séparément pour les instructions de téléchargement et de téléchargement (toujours côté radio/client), et pour différents ports de destination, HTTP (80) et HTTPS (443).
En examinant les mesures TCP Insight, vous pouvez quantifier l'amélioration de la vitesse obtenue en optimisant les flux TCP.

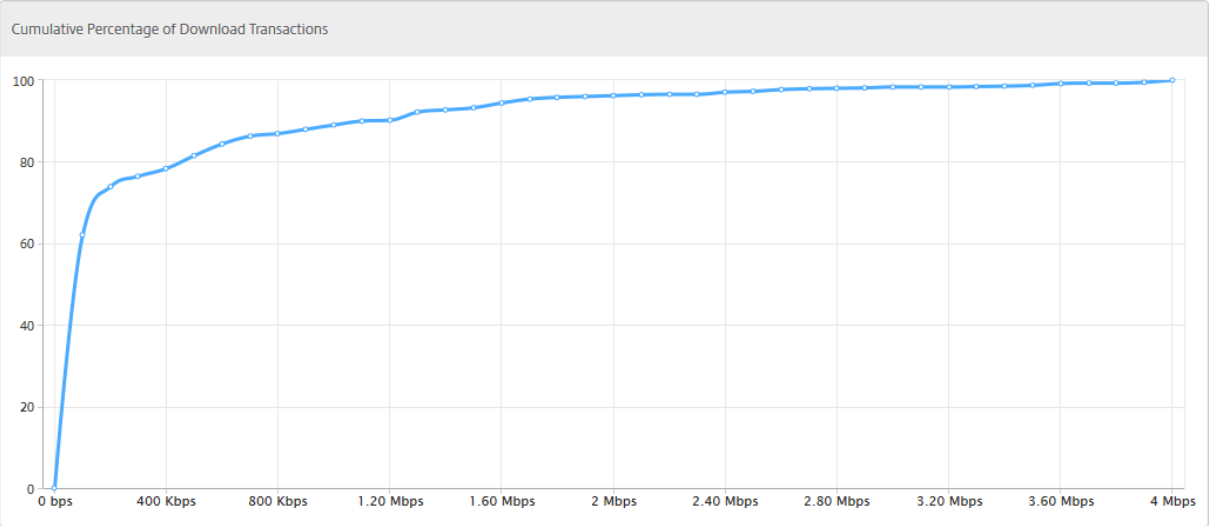
Pour afficher un résumé de ces paramètres, connectez-vous à Citrix ADM et cliquez sur l'onglet **TCP Insight** . Ensuite, cliquez sur **Côtés** et sélectionnez **Internet** ou **Radio** dans le graphique à barres ou dans le tableau situé sous le graphique.



Régler les paramètres TCP

L'utilisation de profils TCP différents peut produire des sorties différentes pour le même trafic. Dans de telles situations, vous pouvez afficher et comparer les mesures de vitesse des périodes au cours desquelles Citrix ADC exécute différents profils d'optimisation TCP. Vous pouvez utiliser les résultats pour régler les paramètres TCP pour une transmission plus rapide et développer un profil TCP qui maximise l'expérience perçue par l'utilisateur dans un réseau client spécifique.

Pour afficher les rapports, connectez-vous à Citrix ADM. Ensuite, sous l'onglet **TCP Insight**, cliquez sur **Bitrates**, puis sélectionnez le débit souhaité dans le graphique à barres ou le tableau situé sous le graphique.

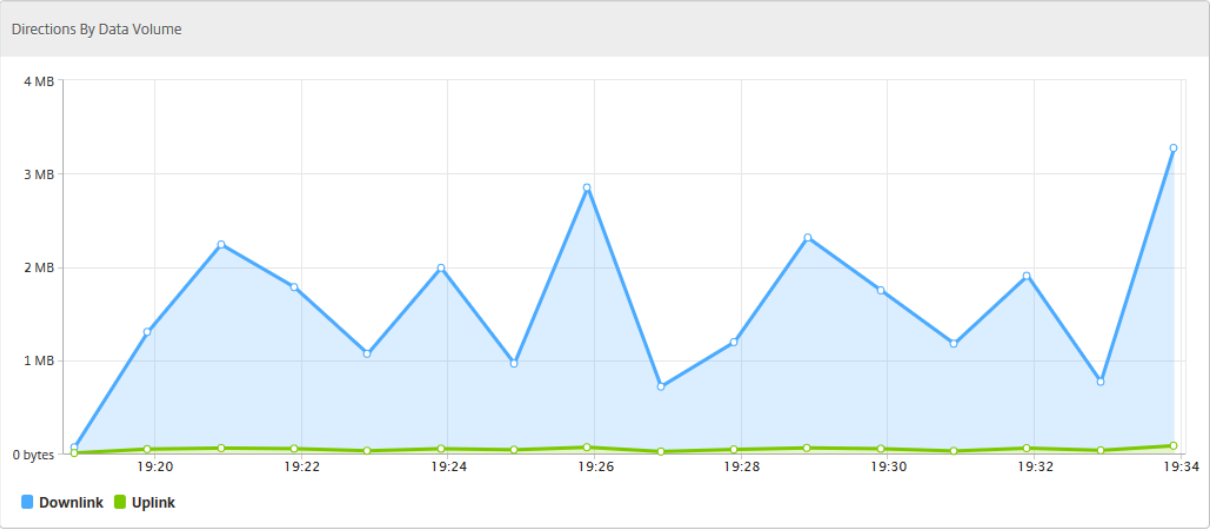


Mesurer l'impact de l'optimisation TCP sur le volume de trafic

Les mesures du volume/débit de données de couche IP traitées par une instance de 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 TCP encourage les abonnés à consommer plus de données.

Pour obtenir un résumé des mesures, connectez-vous à Citrix ADM, puis sous l'onglet **TCP Insight**, cliquez sur **Côtés**, puis sélectionnez **Internet** ou **Radio** dans le graphique à barres ou le tableau situé sous le graphique.

Vous pouvez également sélectionner une autre période dans la liste de temps. Vous pouvez personnaliser la période à l'aide du curseur de période.



WAN Insight

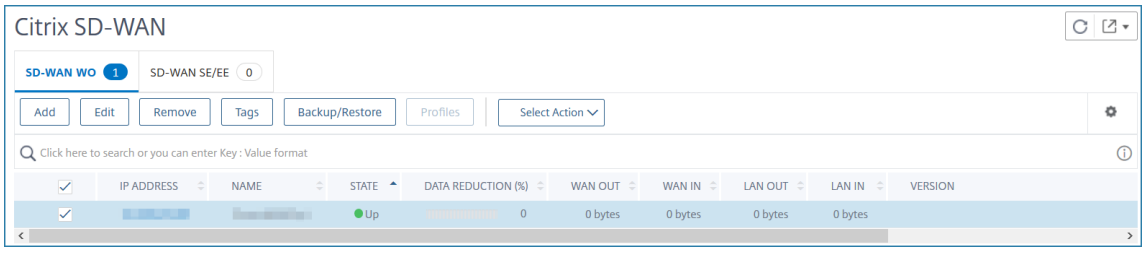
April 29, 2021

Les appliances d'optimisation WAN (WO) Citrix SD-WAN 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 data-center et les sites de succursales. L'analyse WAN Insight permet aux administrateurs de surveiller facilement le trafic WAN accéléré et non accéléré qui circule entre les appliances d'optimisation WAN du centre de données et des succursales. WAN Insight offre une visibilité sur les clients, les applications et les succursales du réseau afin de résoudre efficacement les problèmes réseau. Les rapports actifs et historiques vous permettent de résoudre les problèmes de manière proactive, le cas échéant

L'activation des analyses sur l'appliance d'optimisation WAN 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 datacenter et les appliances d'optimisation WAN de la branche.

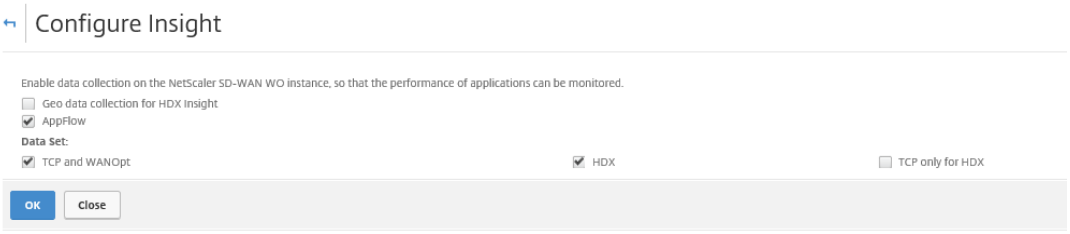
Pour activer les analyses sur l'appliance d'optimisation WAN :

1. Accédez à **Réseaux** > **Instances** > **Citrix SD-WAN**, puis sélectionnez l'instance WO SD-WAN.



2. **Dans la liste Sélectionner une action**, sélectionnez **Activer Insight** .

3. Sélectionnez les paramètres suivants selon les besoins :
    - **Collecte de données géo pour HDX Insight** : partage l'adresse IP du client avec l'API Google Geo.
    - **AppFlow** : Commence la collecte de données à partir d'instances d'optimisation WAN.
    - **TCP et WanOpt** : fournit des rapports TCP et **WanOpt Insight** .
    - **HDX** : fournit des rapports HDX Insight.
    - **TCP uniquement pour HDX** : fournit TCP uniquement pour les rapports HDX Insight.



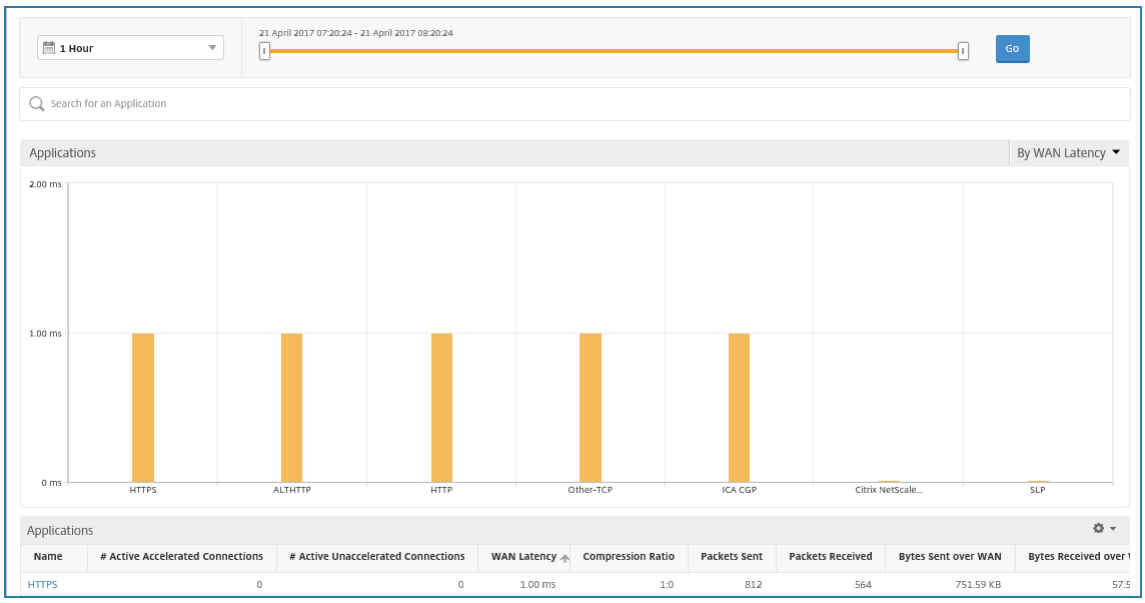
4. Cliquez sur **OK**.

Pour afficher les rapports WAN Insight, accédez à **Analytics** > **WAN Insight**.

> **Remarque**
>
> L'option WAN Insight n'est visible qu'après l'ajout d'une instance WO SD-WAN à Citrix ADM.

Vous pouvez consulter les rapports suivants :

- **Applications** : affiche les statistiques d'utilisation et de performances de toutes les applications pour 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 :

Mesure	Description
Connexions accélérées actives	Nombre de connexions WAN actives qui sont accélérées.
Connexions actives non accélérées	Nombre de connexions WAN actives qui ne sont pas accélérées.
Latence WAN	Retard, en millisecondes, que l'utilisateur rencontre lors de l'interaction avec une application.
Taux de compression	Rapport de compression des données entre la succursale et les appliances du centre de données pour la durée sélectionnée.
Paquets envoyés	Nombre de paquets envoyés par l'appliance d'optimisation WAN sur le réseau pour la durée sélectionnée.
Paquets reçus	Nombre de paquets que l'appliance d'optimisation WAN a reçus du réseau pour la durée sélectionnée.
Octets envoyés sur le WAN	Nombre d'octets que l'appliance d'optimisation du réseau étendu Citrix a envoyés sur le réseau étendu pendant la durée sélectionnée.

Mesure	Description
Octets reçus sur le WAN	Nombre d'octets que l'appliance d'optimisation WAN a reçus du WAN pour la durée sélectionnée.
RTO LAN	Nombre de fois que l'appliance d'optimisation WAN a expiré la retransmission vers le réseau local pour la durée sélectionnée.
RTO WAN	Nombre de fois que l'appliance d'optimisation WAN a expiré la retransmission vers le WAN pendant la durée sélectionnée.
Retransmission de paquets (LAN)	Nombre de paquets que l'appliance d'optimisation WAN a retransmis au réseau LAN pour la durée sélectionnée.
Retransmission de paquets (WAN)	Nombre de paquets que l'appliance d'optimisation WAN a retransmis au réseau WAN pour la durée sélectionnée.

Video Insight

April 29, 2021

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 pour améliorer l'expérience client et l'efficacité opérationnelle, offrant des avantages tels que :

- Gérer le réseau pendant la congestion pendant les heures de pointe.
- Améliorez la cohérence de la lecture vidéo et réduisez le blocage vidéo.
- Activez de nouvelles offres de services vidéo (par exemple, les services vidéo Binge-on).
- Permettez aux clients de sélectionner la meilleure qualité vidéo durable.
- Fournir une expérience utilisateur cohérente à l'abonné.

Tout en optimisant le trafic vidéo, l'appliance Citrix ADC utilise un mécanisme spécial pour accélérer dynamiquement le débit vidéo et une technique d'échantillonnage aléatoire pour estimer les économies réalisées grâce à la technique d'optimisation. Pour plus d'informations sur la fonctionnalité d'optimisation vidéo Citrix ADC, reportez-vous à la sectionOptimisation vidéo. Lorsque vous intégrez l'appliance Citrix ADC à Citrix Application Delivery Management (ADM), il collecte des

informations clés à partir des données vidéo circulant via l'appliance Citrix ADC. Vous pouvez utiliser ces informations pour comparer les performances optimisées et non optimisées du trafic vidéo ABR, déterminer les économies dues à l'optimisation, etc.

> **Remarque**
>
> Les statistiques des sessions non optimisées fournies dans Citrix ADM correspondent aux sessions que vous avez sélectionnées d'échantillonnage aléatoire dans l'appliance Citrix ADC. Pour plus d'informations sur l'échantillonnage aléatoire, reportez-vous à la sectionOptimisation vidéo.

Video Insight dans Citrix ADM fournit des mesures pour les types de trafic vidéo suivants :

- Vidéos de téléchargement progressif sur HTTP
- Vidéos ABR sur HTTP
- Vidéos ABR sur HTTPS
- Vidéos ABR YouTube sur QUIC

Configuration de Video Insight

> **Remarque**
>
> Video Insight est pris en charge sur les instances Citrix ADC avec la 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 de Citrix ADC, activez d'abord la fonctionnalité AppFlow, configurez un collecteur, une action et une stratégie AppFlow, puis 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 un aperçu vidéo sur une instance de Citrix ADC, exécutez les commandes suivantes pour configurer un profil et une stratégie AppFlow et lier globalement la stratégie AppFlow.

add appflow collector <name> **-IPAddress** <ipaddress> **-port** <port_number> **-Transport** logstream

set appflow param -**videoInsight** ENABLED

add appflow action <name> **-collectors** <string> **-videoAnalytics** ENABLED

add appflow policy <name> <rule> <action>

bind appflow global <policyName> <priority> [<gotoPriorityExpression>] [**-type** <type>]

enable ns mode ulfd

enable feature AppFlow

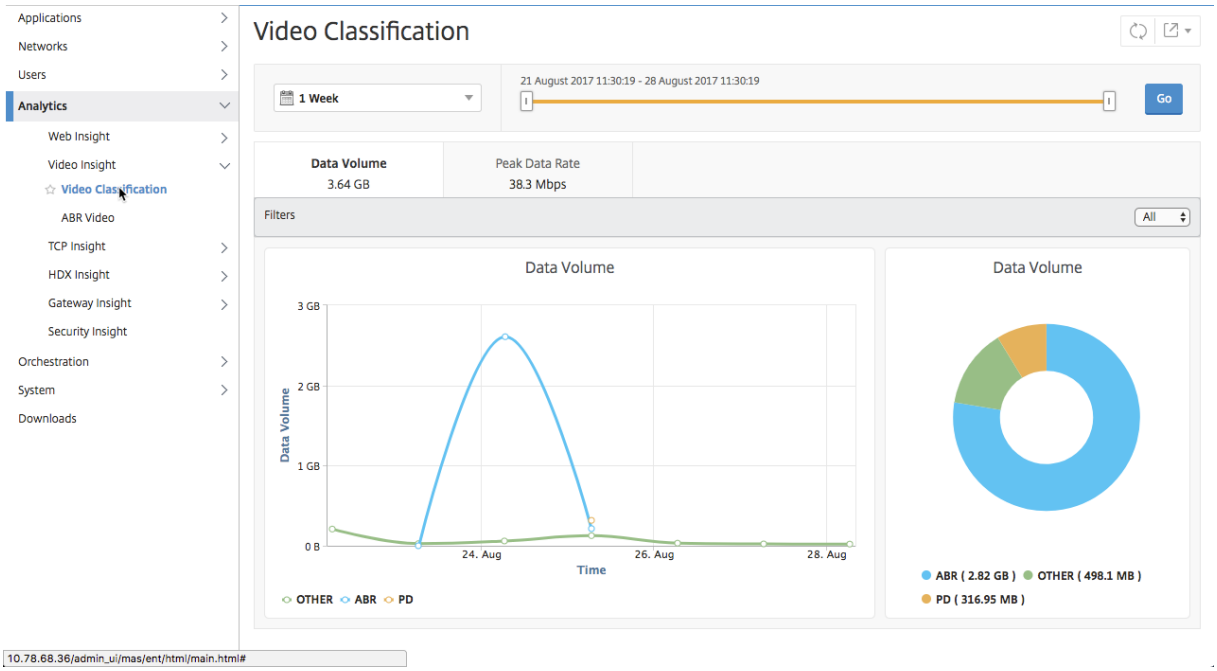
Échantillon

```
add appflow collector col1 -IPAddress 10.106.76.15 -port 5557 -
    Transport logstream
set appflow param -videoInsight ENABLED
add appflow action act1 -collectors col1 -videoAnalytics ENABLED
add appflow policy appol true act1
bind appflow global appol 1
enable ns mode ulfd
enable feature appflow
<!--NeedCopy-->
```

Affichage des 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, accédez à **Analytics > Video Insight**.



> **Remarque**
>
> Les valeurs fournies par la légende **AUTRES** dans les graphiques représentent les données non ABR et non PDD dans le trafic vidéo en fonction du filtre que vous avez sélectionné :
>
> - **All** — Somme des données non-ABR (HTTP, HTTPS et QUIC) et non-DP (HTTP) dans le trafic

vidéo.

- **HTTP** — Somme des données non ABR et non PDD 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.

Voir l'efficacité du réseau

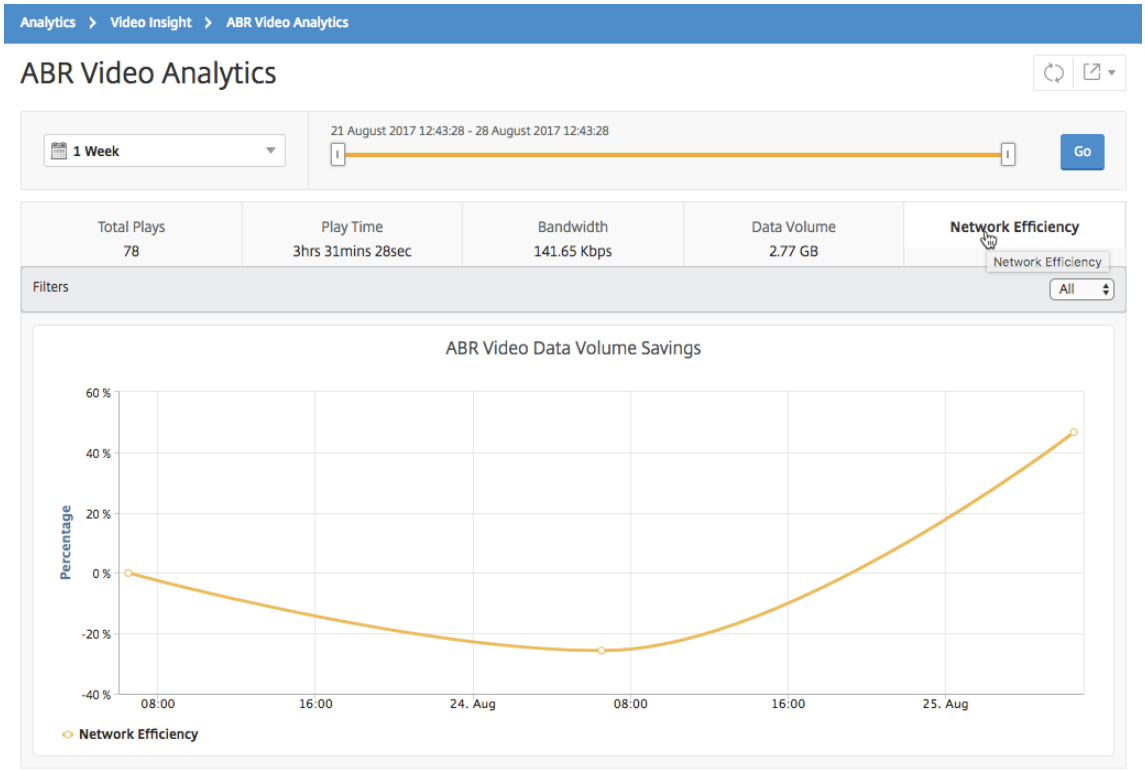
April 29, 2021

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 enregistrée par l'optimisation. Le pourcentage de bande passante enregistrée est calculé à l'aide de la formule suivante :

Pourcentage de bande passante enregistrée = Volume de **données vidéo ABR optimisé moyen/-Moyenne du volume de données vidéo ABR non optimisé** .

Pour voir le pourcentage de bande passante enregistré par l'optimisation :

1. Accédez à **Analytics > Video Insight**, puis cliquez sur **ABR Video**.
2. Dans le volet droit, sélectionnez une période dans la liste. Vous pouvez personnaliser davantage la période à l'aide du curseur temporel.
3. Cliquez sur **Aller** et sélectionnez l'onglet **Efficacité réseau**.



Comparez le volume de données utilisé par les vidéos ABR optimisées et non optimisées

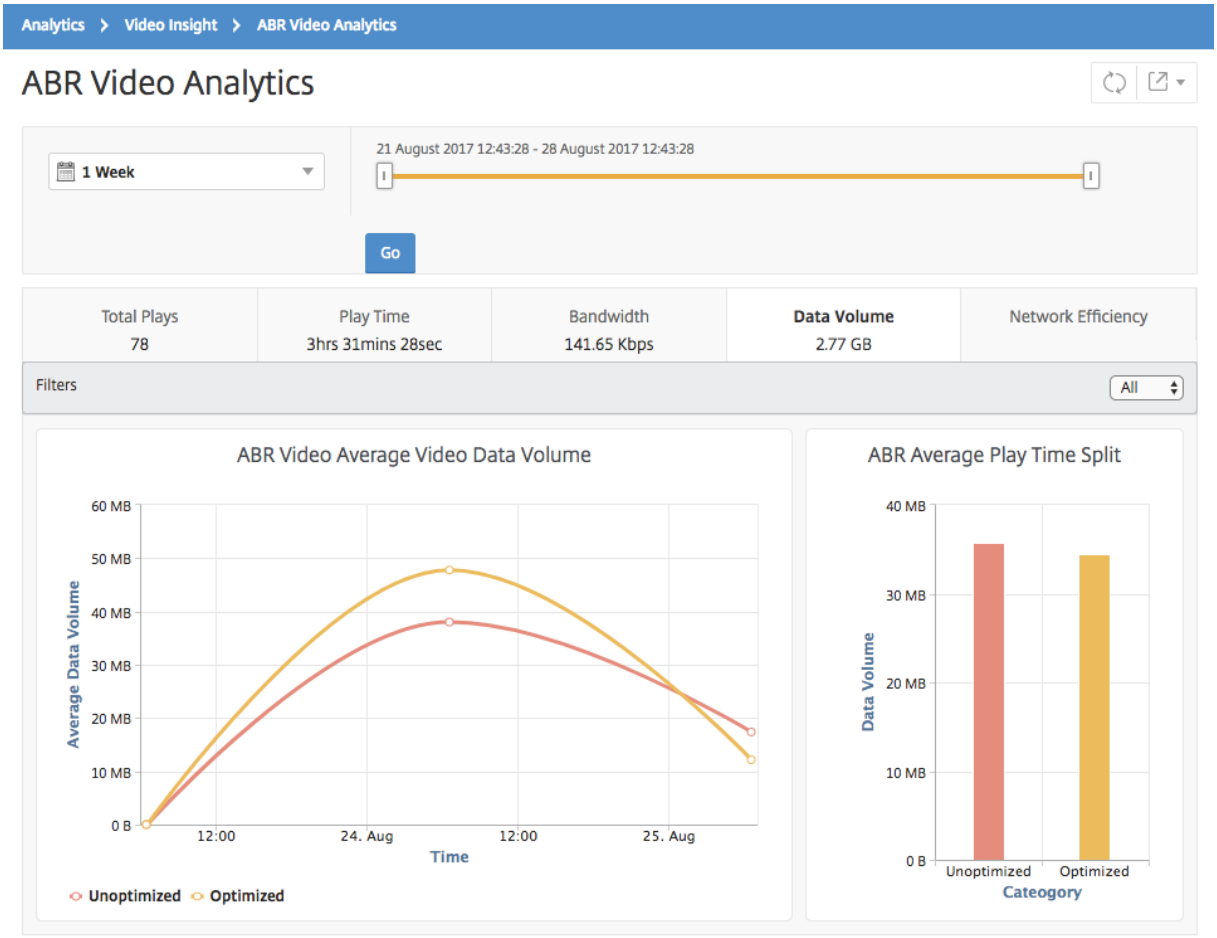
April 29, 2021

Pour une période donnée, Citrix Application Delivery Management (ADM) affiche le volume de données utilisé par les vidéos ABR optimisées et non optimisées, de sorte que vous pouvez comparer les deux volumes.

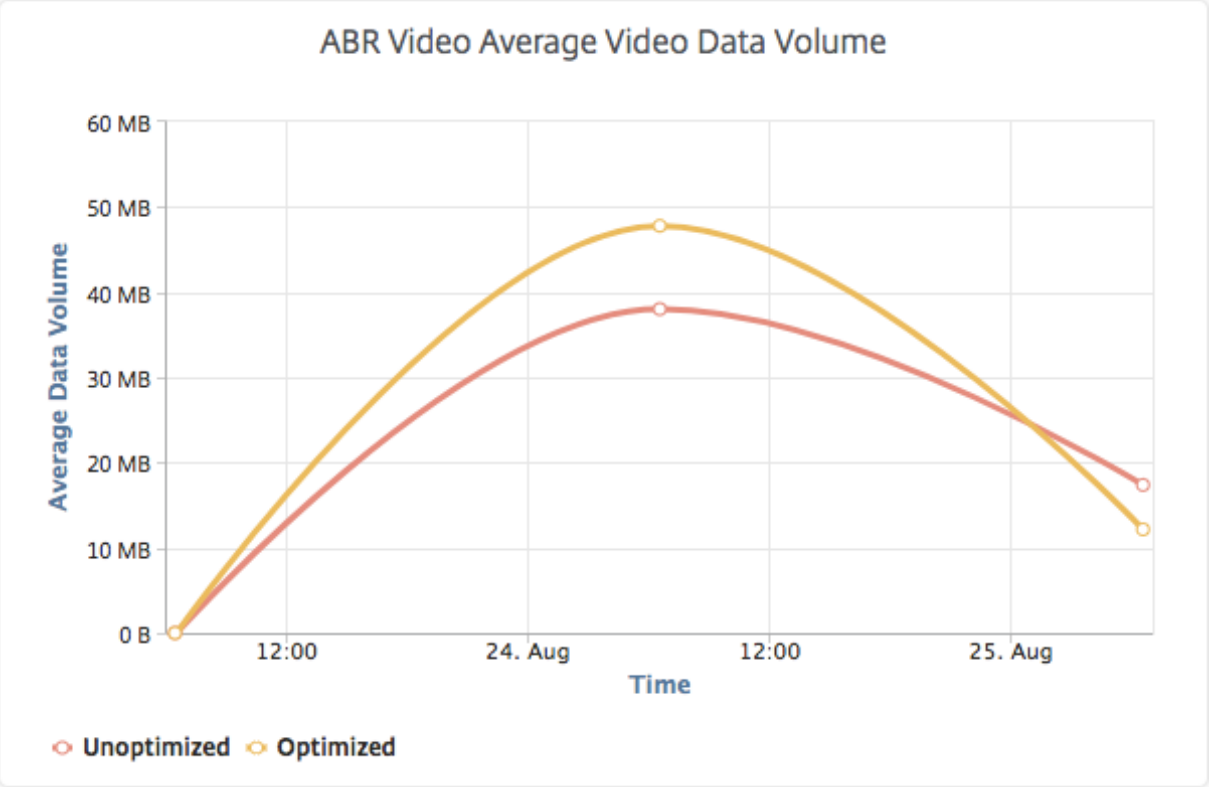
Pour voir le volume de données utilisé par les vidéos ABR :

1. Accédez à **Analytics > Video Insight**, puis cliquez sur **ABR Video**.
2. Dans le volet droit, sélectionnez une période dans la liste. Vous pouvez personnaliser davantage la période à l'aide du curseur temporel.
3. Cliquez sur **Exécuter** et sélectionnez l'onglet **Volume de données** .

Vous pouvez utiliser la liste **Filtres** pour sélectionner les vidéos HTTP, HTTPS ou QUIC ABR.



L'onglet **Volume de données** fournit un graphique linéaire et un graphique circulaire décrivant le volume de données moyen utilisé par les vidéos ABR et le volume de données consommé par les vidéos ABR optimisées et non optimisées de votre réseau pour la période sélectionnée. Vous pouvez placer le pointeur de la souris sur le graphique linéaire pour afficher le volume moyen de données utilisé pendant une période donnée :



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

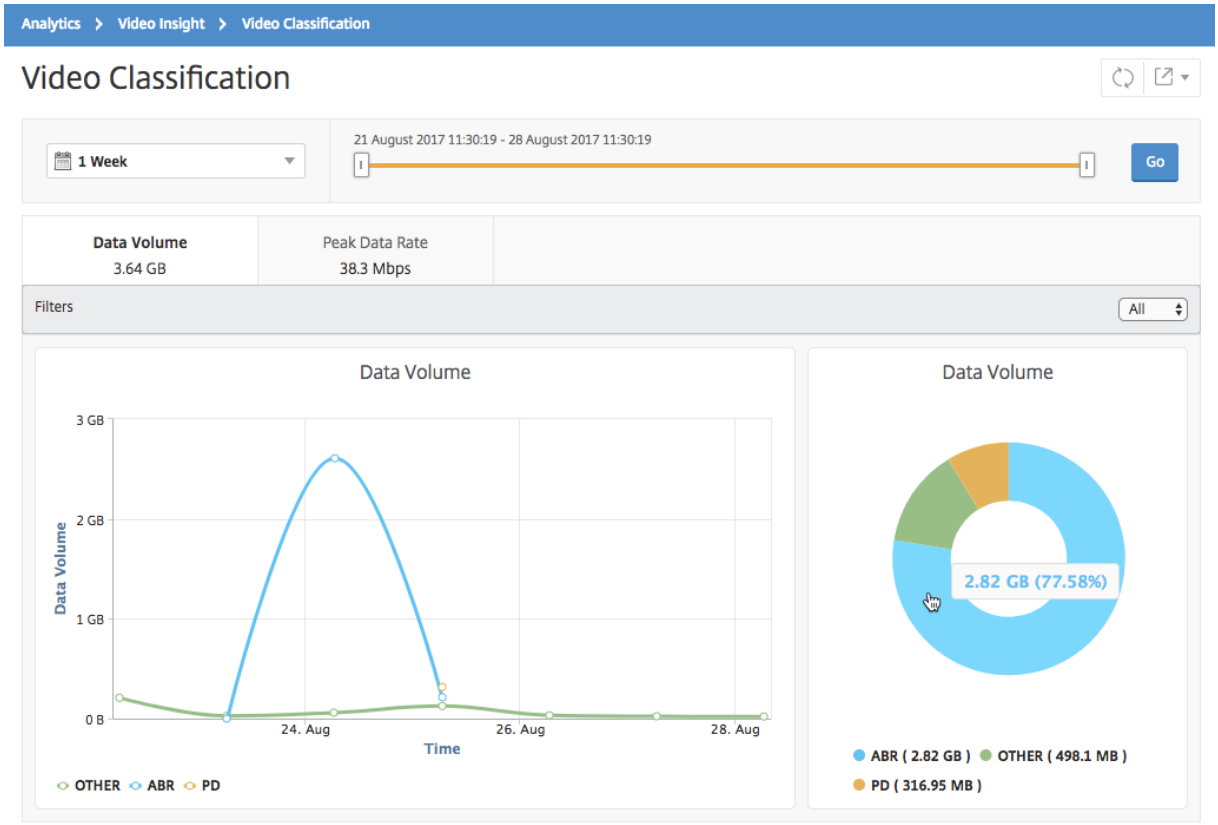
April 29, 2021

L'appliance Citrix ADC détecte le trafic vidéo chiffré ou non chiffré dans votre réseau et le type de diffusion vidéo (DP ou ABR). Citrix Application Delivery Management (ADM) affiche ces mesures et le volume de données consommé par le trafic vidéo pendant une période définie.

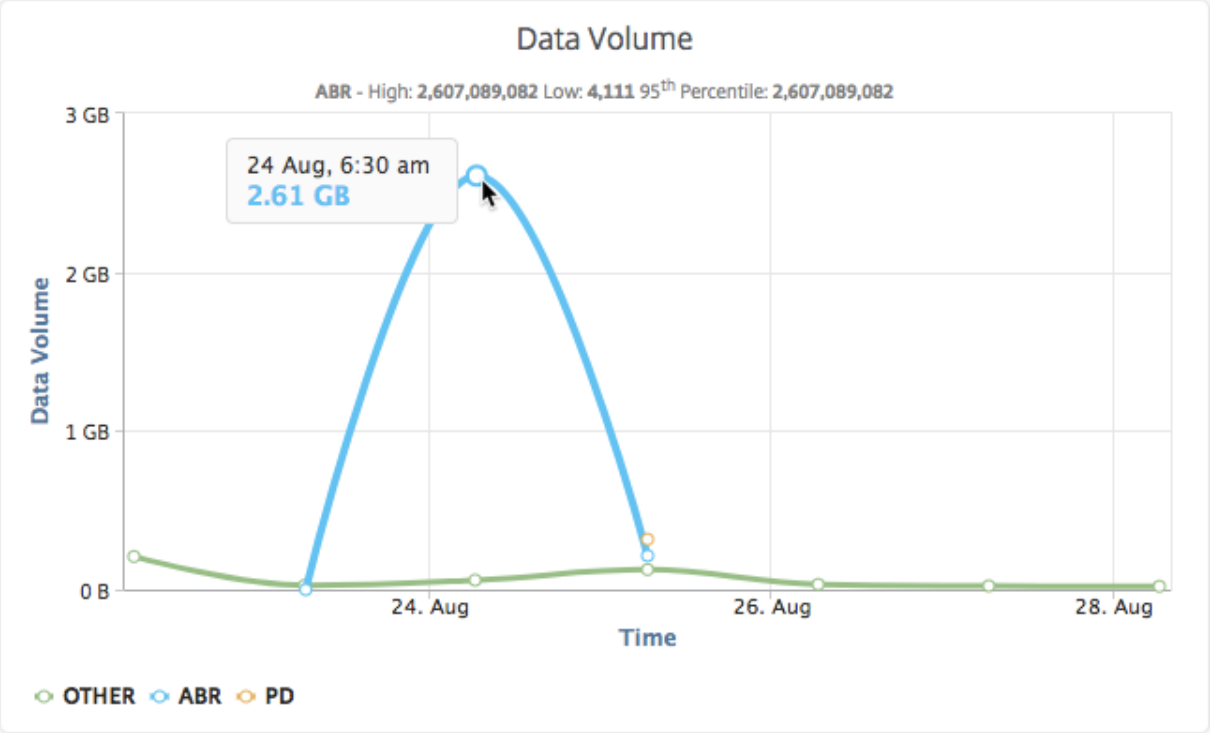
Pour voir les types de vidéos et le volume de données consommé :

1. Accédez à **Analytics > Video Insight**, puis cliquez sur **Video Classification** .
2. Dans le volet droit, sélectionnez une période dans la liste. Vous pouvez personnaliser davantage la période à l'aide du curseur temporel.
3. Cliquez sur **OK**.

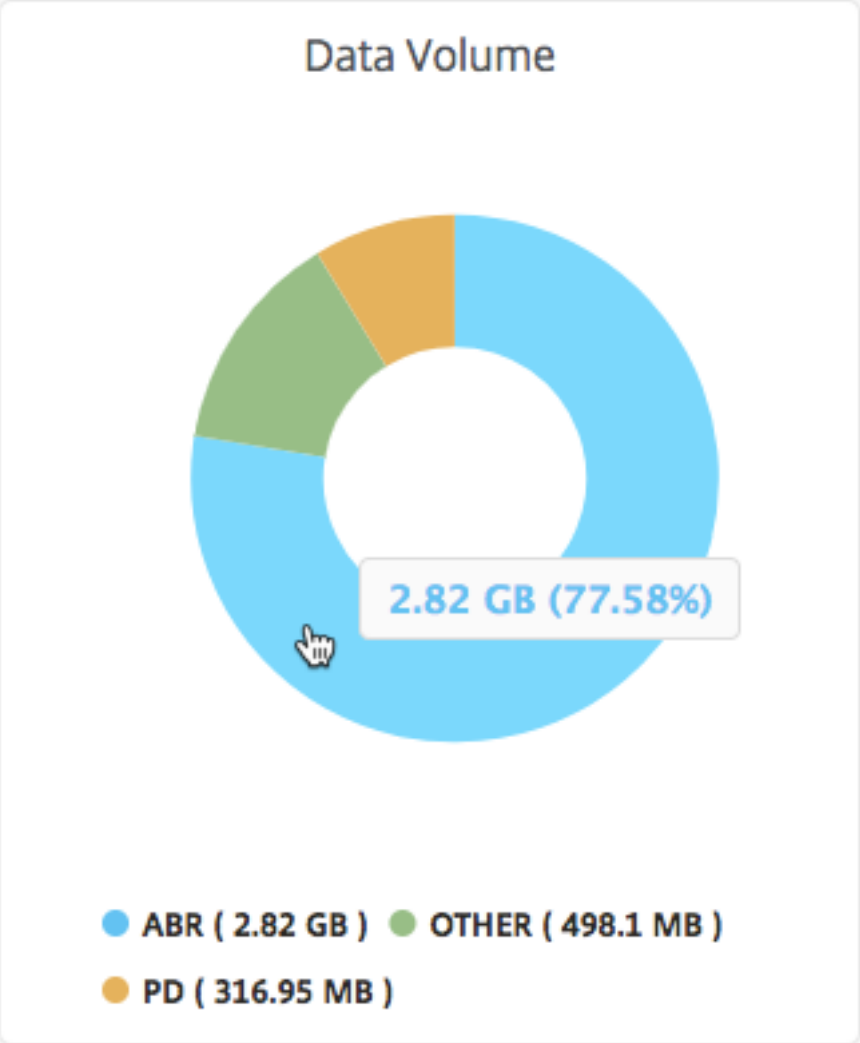
Vous pouvez utiliser la liste **Filtres** pour sélectionner le trafic HTTP, HTTPS ou QUIC.



L'onglet **Volume de données** fournit un graphique linéaire et un graphique circulaire indiquant les types de flux de trafic vidéo à partir de votre réseau et le volume de données consommé par votre réseau. Vous pouvez placer le pointeur de la souris sur le graphique linéaire pour afficher les données consommées pendant une période donnée :



En outre, vous pouvez placer le pointeur de la souris sur le graphique à secteurs pour afficher le pourcentage de volume de données consommé par un type particulier de trafic vidéo.



Comparer les temps de lecture optimisés et non optimisés des vidéos ABR

April 29, 2021

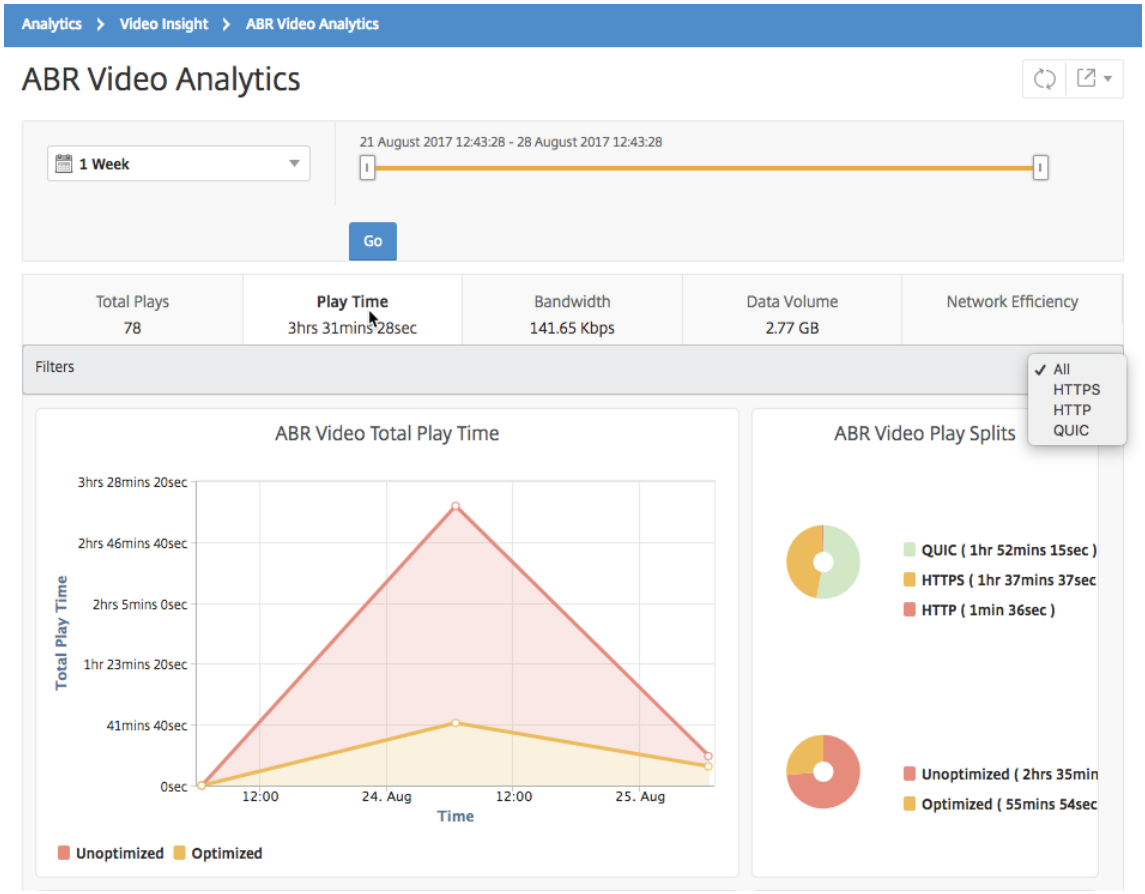
Pour une période donnée, Citrix Application Delivery Management (ADM) fournit la durée de lecture des vidéos ABR et vous permet également de comparer la durée de lecture des vidéos ABR optimisées et non optimisées de votre réseau.

Pour afficher la durée de jeu :

1. Accédez à **Analytics > Video Insight**, puis cliquez sur **ABR Video** .
2. Dans le volet droit, sélectionnez une période dans la liste. Vous pouvez personnaliser davantage la période à l'aide du curseur temporel.

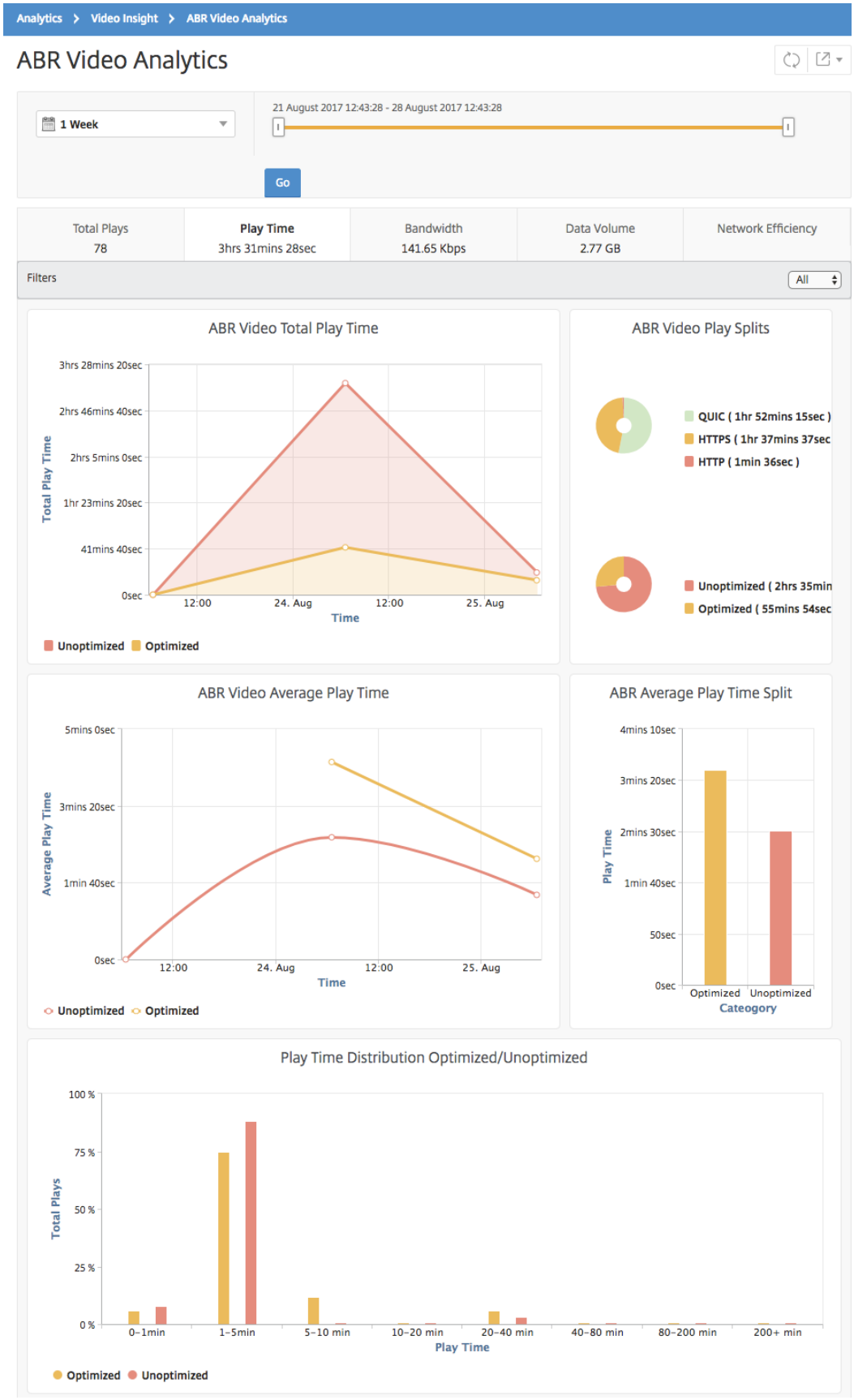
3. Cliquez sur **Aller** et sélectionnez l'onglet **Temps de lecture** .

   Vous pouvez utiliser la liste **Filtres** pour sélectionner les vidéos HTTP, HTTPS ou QUIC ABR.



Pour la période sélectionnée, l'onglet **Temps de lecture** fournit un graphique linéaire et un graphique à secteurs décrivant les éléments suivants :

- Temps total de lecture des vidéos ABR depuis votre réseau
- Temps de lecture total des lectures optimisées et non optimisées des vidéos ABR depuis votre réseau pour la période sélectionnée
- Temps total de lecture des vidéos ABR chiffrées et non chiffrées
- Durée moyenne des vidéos ABR
- Temps moyen de lecture optimisé et non optimisé des vidéos ABR
- Temps de lecture moyen des vidéos ABR chiffrées et non chiffrées
- Distribution du temps de lecture entre les vidéos ABR optimisées et non optimisées



Comparer la consommation de bande passante des vidéos ABR optimisées et non optimisées

April 29, 2021

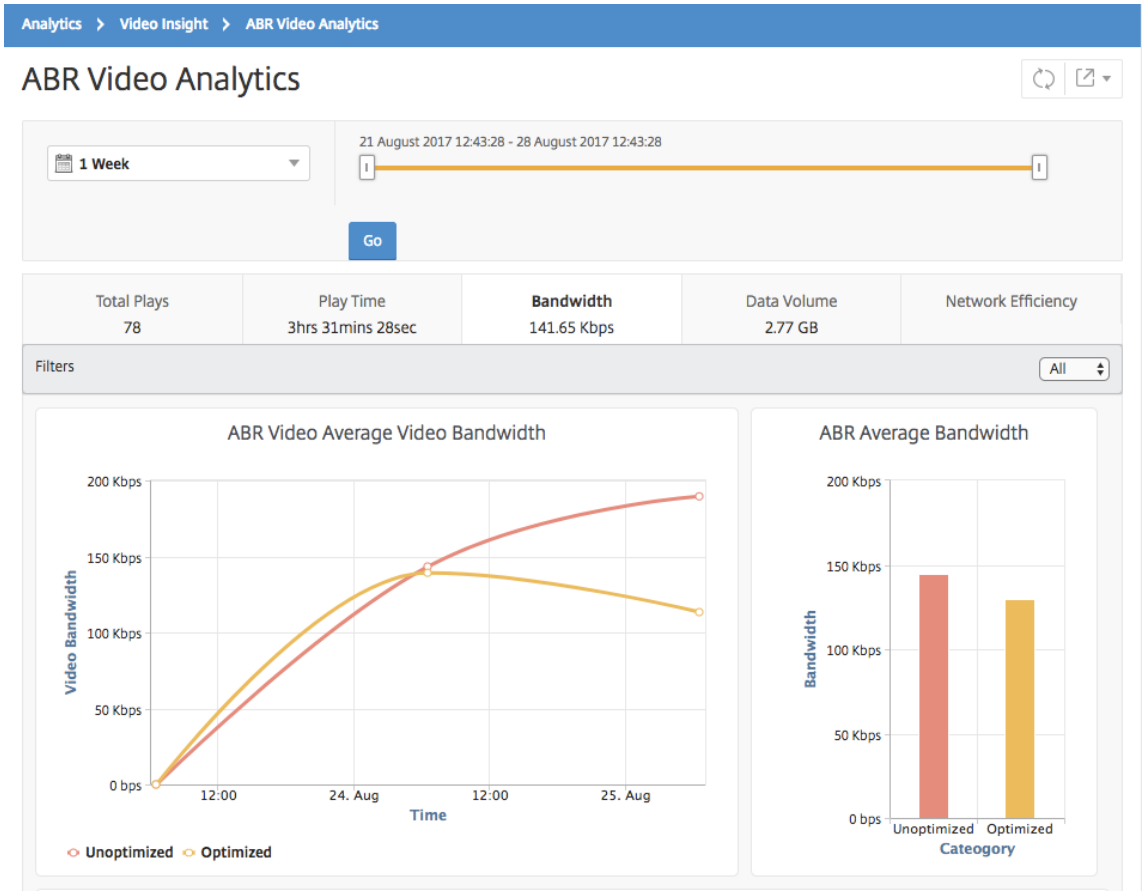
Pour une période donnée, Citrix Application Delivery Management (ADM) fournit la bande passante consommée par les vidéos ABR optimisées et non optimisées et vous permet également de comparer la bande passante consommée par les vidéos ABR optimisées et non optimisées dans votre réseau en fonction des éléments suivants :

- Temps de jeu
- Volume de données

Pour afficher la consommation de bande passante :

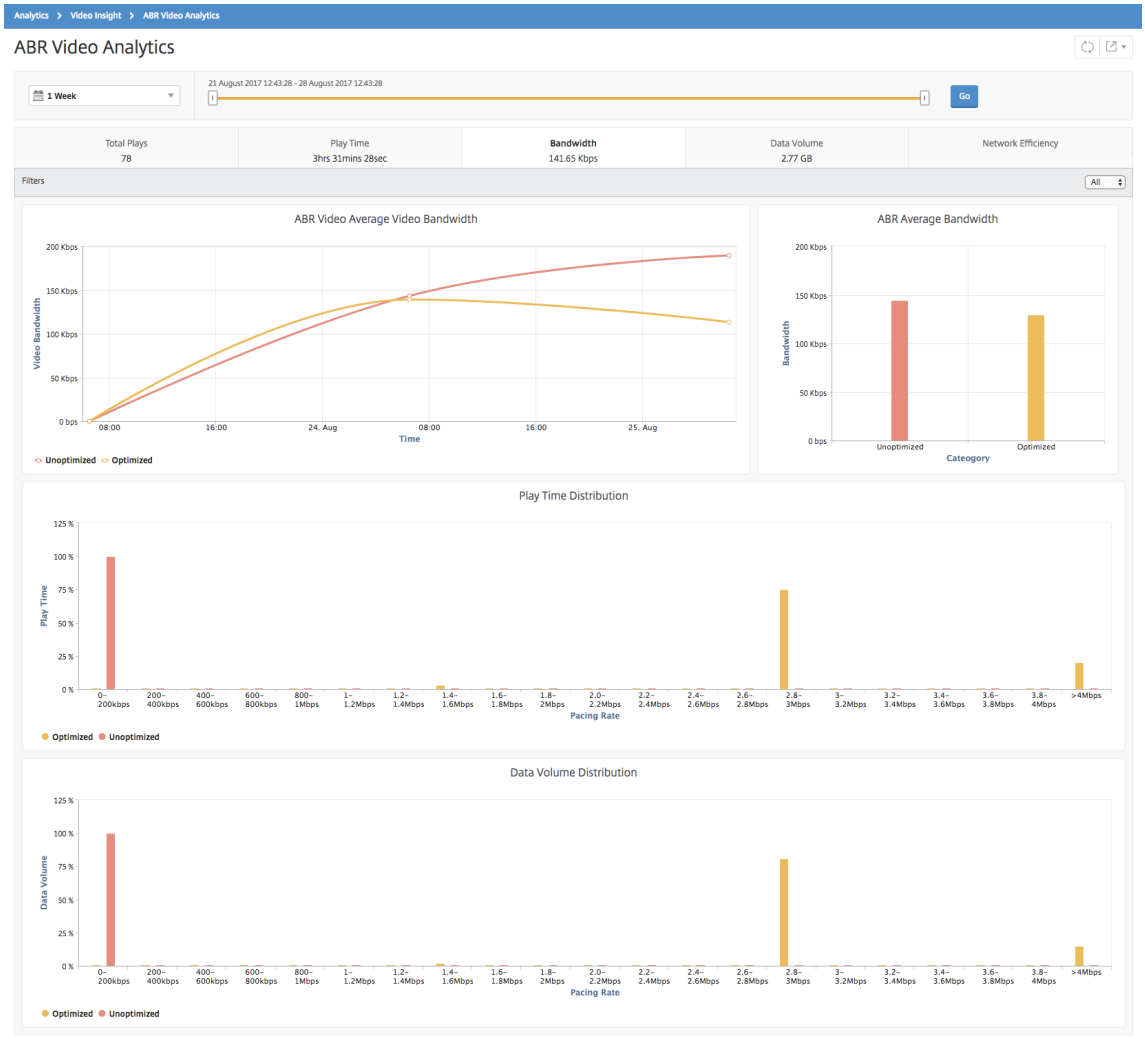
1. Accédez à **Analytics > Video Insight**, puis cliquez sur **ABR Video Analytics** .
2. Dans le volet droit, sélectionnez une période dans la liste. Vous pouvez personnaliser davantage la période à l'aide du curseur temporel.
3. Cliquez sur **Aller** et sélectionnez l'onglet **Bande passante** .

   Vous pouvez utiliser la liste **Filtres** pour sélectionner les vidéos HTTP, HTTPS ou QUIC ABR.



Pour la période sélectionnée, l'onglet **Bande passante** fournit un graphique linéaire et un graphique circulaire 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 visionnages de vidéos ABR

April 29, 2021

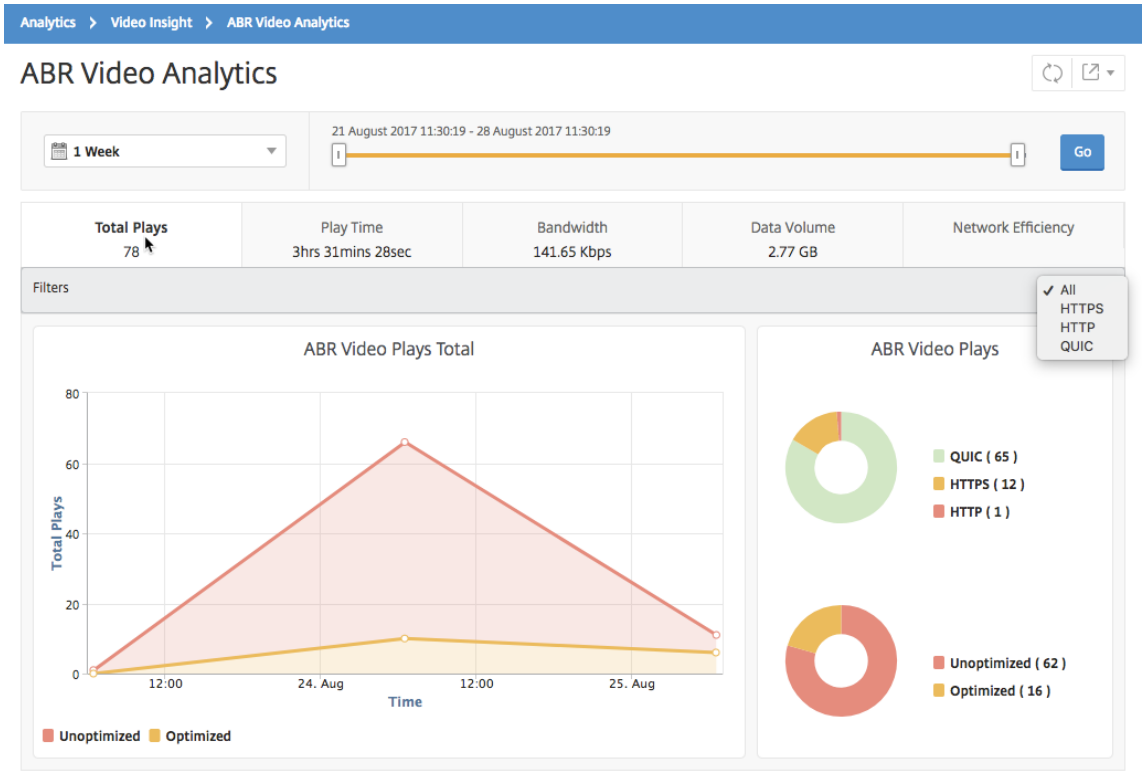
Pour une période donnée, Citrix Application Delivery Management (ADM) affiche le nombre de lectures de vidéos ABR et vous permet de comparer le nombre de lectures optimisées et non optimisées dans votre réseau.

Pour voir le nombre de lectures :

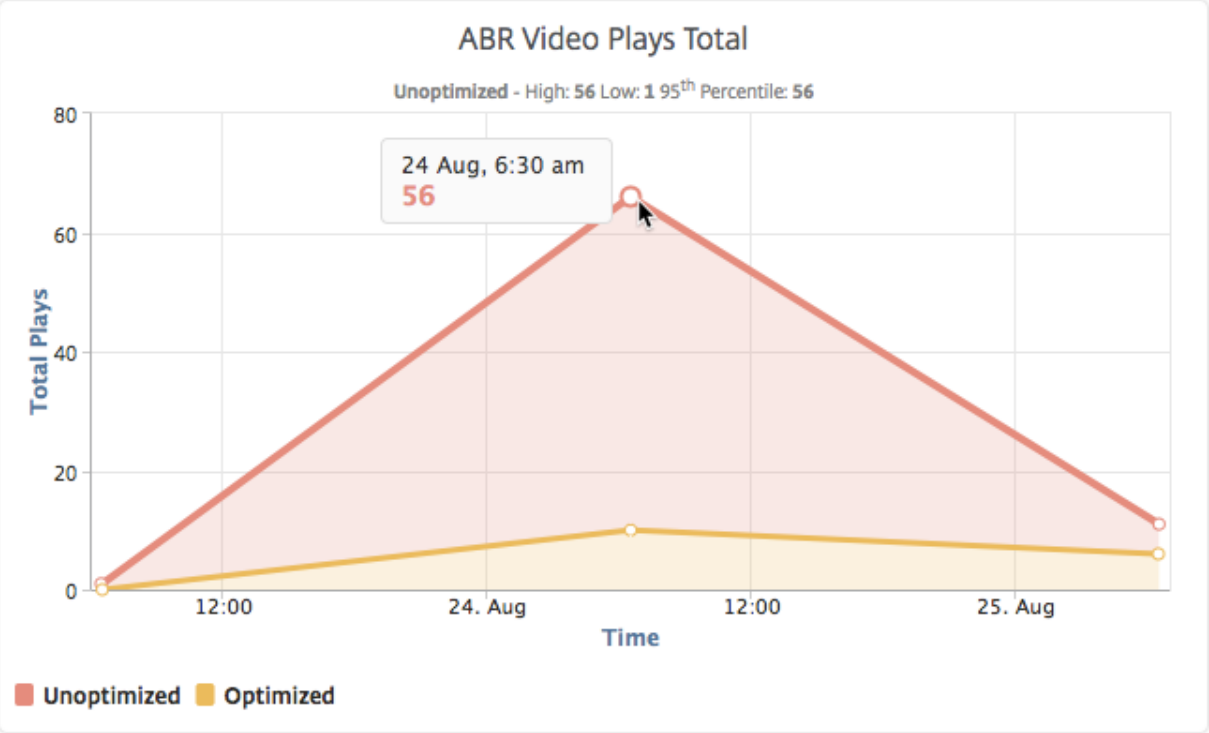
1. Accédez à **Analytics > Video Insight**, puis cliquez sur **ABR Video Analytics**.
2. Dans le volet droit, sélectionnez une période dans la liste. Vous pouvez personnaliser davantage la période à l'aide du curseur temporel.

3. Cliquez sur **Aller** et sélectionnez **# de l'onglet Lecture** .

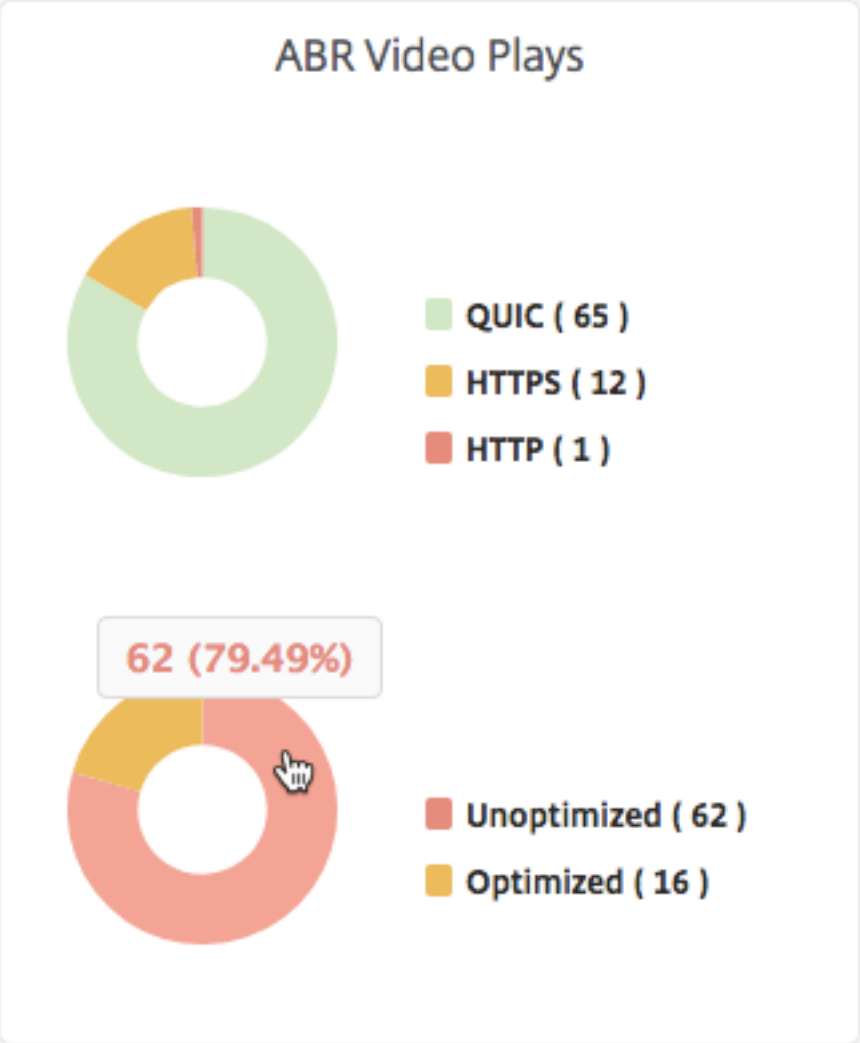
   Vous pouvez utiliser la liste **Filtres** pour sélectionner les vidéos HTTP, HTTPS ou QUIC ABR.



L'onglet **Nombre de lectures** fournit un graphique linéaire et un graphique à secteurs décrivant le nombre de lectures de vidéos ABR de votre réseau et le nombre de lectures optimisées et non optimisées de vidéos ABR de votre réseau pour la période sélectionnée. Vous pouvez placer le pointeur de la souris sur le graphique linéaire pour afficher le nombre de lectures au cours d'une période donnée :



En outre, vous pouvez pointer votre souris sur le graphique à secteurs pour afficher le pourcentage de lectures optimisées et non optimisées et le pourcentage de vidéos ABR chiffrées et non chiffrées pour la période sélectionnée.



Afficher le débit de pointe pour une période spécifique

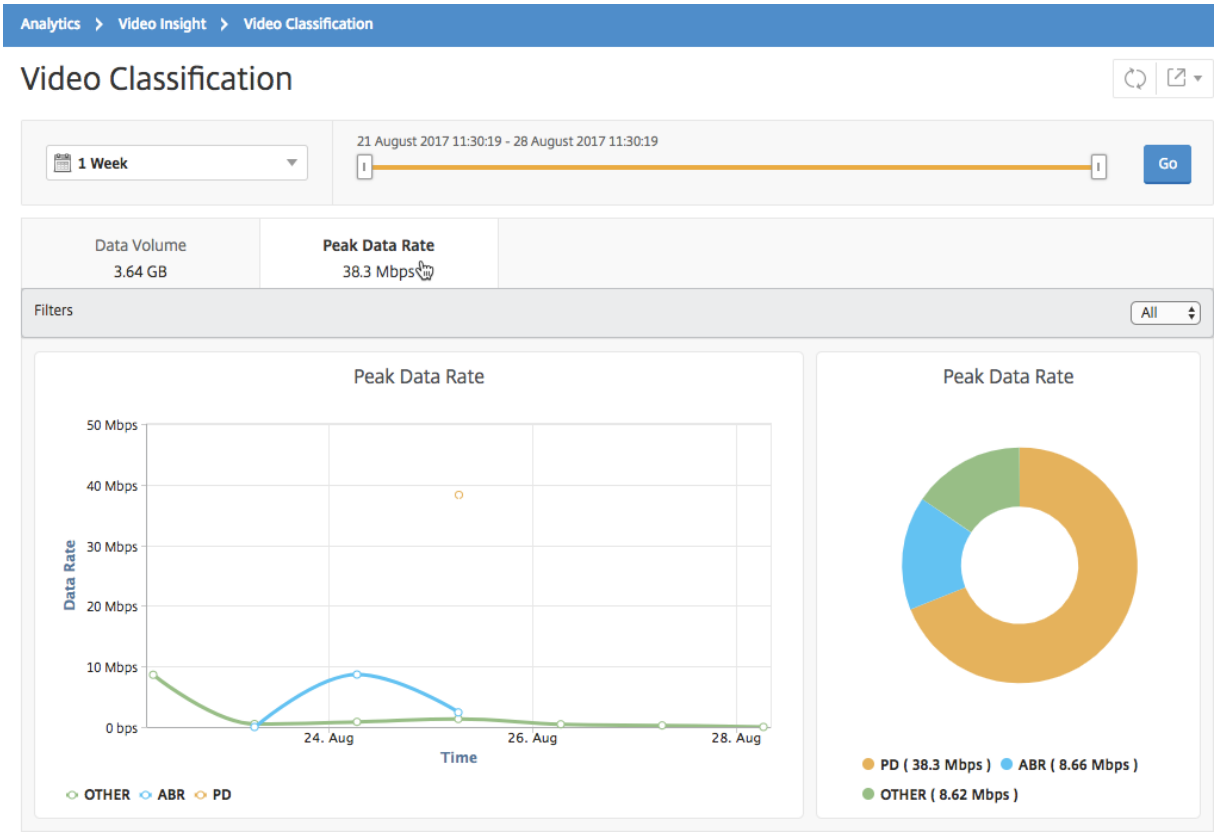
April 29, 2021

Citrix Application Delivery Management (ADM) vous indique le débit maximal ou le débit de données du trafic vidéo dans votre réseau.

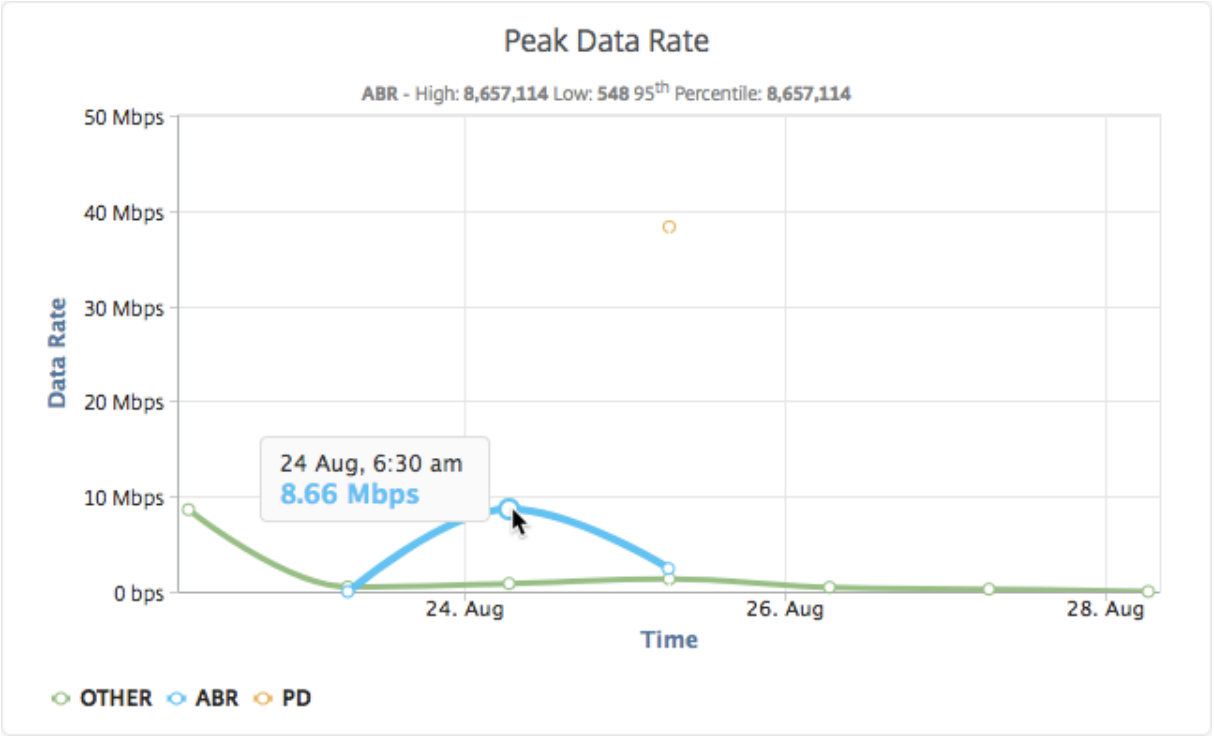
Pour voir le débit maximal de données du trafic vidéo :

1. Accédez à **Analytics > Video Insight**, puis cliquez sur **Video Classification**.
2. Dans le volet droit, sélectionnez une période dans la liste. Vous pouvez personnaliser davantage la période à l'aide du curseur temporel.
3. Cliquez sur **Exécuter** et sélectionnez l'onglet **Taux de données de pointe** .

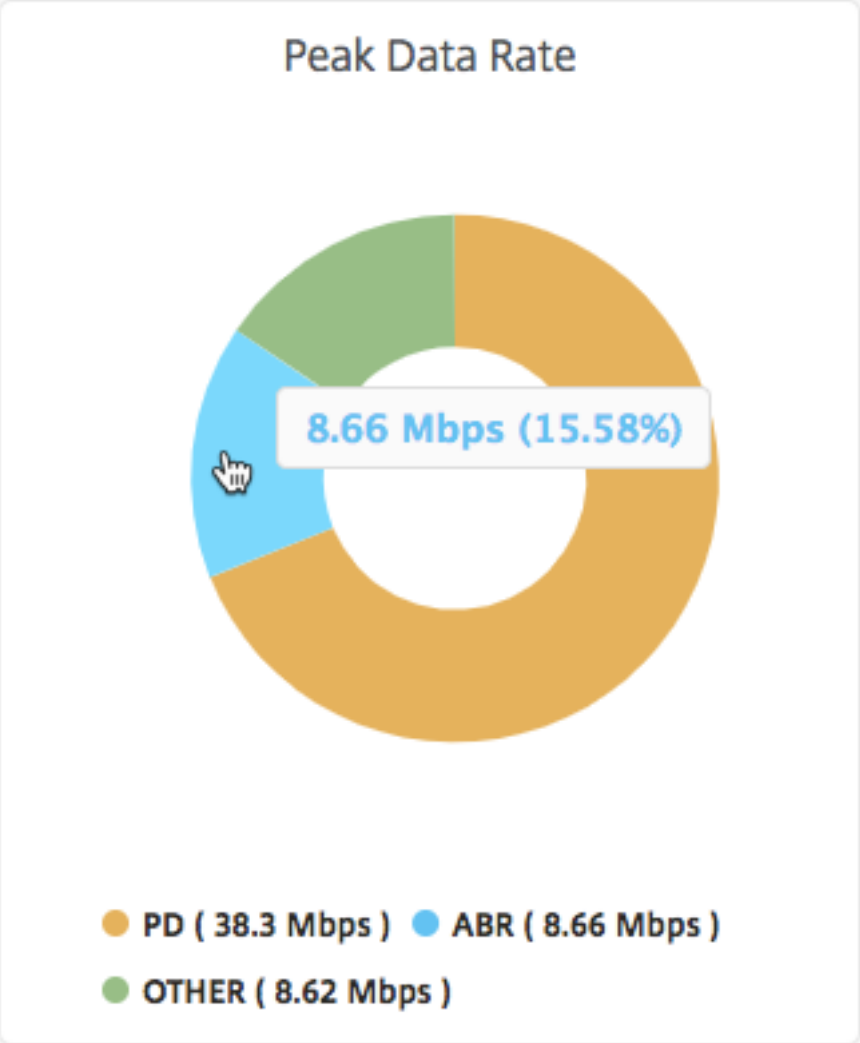
Vous pouvez utiliser la liste **Filtres** pour sélectionner le trafic HTTP, HTTPS ou QUIC.



L'onglet **Taux de crête de données** fournit un graphique linéaire et un graphique circulaire décrivant le débit de données de pointe du type de flux vidéo en continu à partir de votre réseau et le débit de données de pointe du trafic vidéo sur votre réseau pendant la période sélectionnée. Vous pouvez placer le pointeur de la souris sur le graphique linéaire pour afficher le débit de données maximal pendant une période donnée.



En outre, vous pouvez pointer votre souris sur le graphique à secteurs pour afficher le pourcentage du débit de données de pointe consommé par le type de trafic vidéo diffusé pendant la période sélectionnée.



Analyse de proxy de transfert SSL

April 29, 2021

Une appliance Citrix ADC située à la périphérie du réseau d'entreprise agit comme un 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 d'entreprise. Toutes les demandes et réponses sont marquées à l'utilisateur et les activités de l'utilisateur sont enregistrées dans l'appliance. Pour de plus amples informations, consultez la section Proxy de transfert SSL Citrix.

Lorsque vous intégrez Citrix Application Delivery Management (ADM) à une appliance Citrix ADC, l'activité utilisateur consignée et les enregistrements suivants sur l'appliance sont exportés vers

Citrix ADM à l'aide de **Logstream**. Citrix ADM rassemble et présente des informations sur les activités des utilisateurs, telles que les sites Web visités et la bande passante dépensée. Il signale également l'utilisation de la bande passante et les menaces détectées, telles que les logiciels malveillants et les sites de phishing. Vous pouvez utiliser ces mesures clés pour surveiller votre réseau et prendre des mesures correctives avec l'appliance Citrix ADC.

Pour intégrer une appliance Citrix ADC avec Citrix ADM :

1. Sur l'appliance Citrix ADC, lors de la configuration du proxy SSL Forward, activez **Analytics** et fournissez les détails de l'instance Citrix ADM que vous souhaitez utiliser pour l'analyse.
2. Dans Citrix ADM, ajoutez l'appliance Citrix ADC en tant qu'instance à Citrix ADM. Pour plus d'informations, veuillez consulter la section Ajouter des instances à Citrix ADM.

Tableaux de bord

April 29, 2021

Citrix Application Delivery Management (ADM) fournit deux tableaux de bord, le tableau de **bord du trafic sortant** et le **tableau de bord utilisateur** . 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.

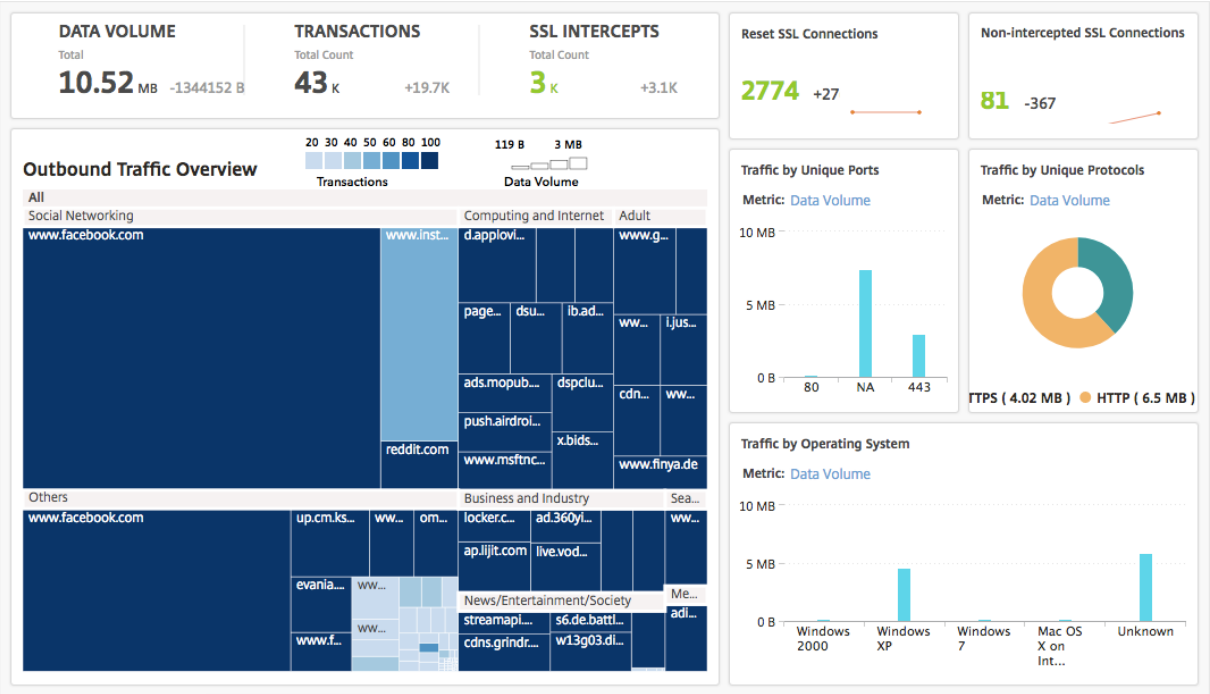
Tableau de bord du trafic sortant

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 holistique 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 :

1. Quantité de bande passante consommée par les URL ou les domaines accessibles depuis votre réseau.
2. Nombre de transactions effectuées lors de l'accès aux URL et aux domaines à partir de votre réseau.
3. Nombre de connexions SSL interceptées par l'appliance Citrix ADC au cours des transactions.
4. Nombre de connexions SSL non interceptées par l'appliance Citrix ADC au cours des transactions.
5. Nombre de connexions SSL réinitialisées par l'appliance Citrix ADC au cours des transactions.

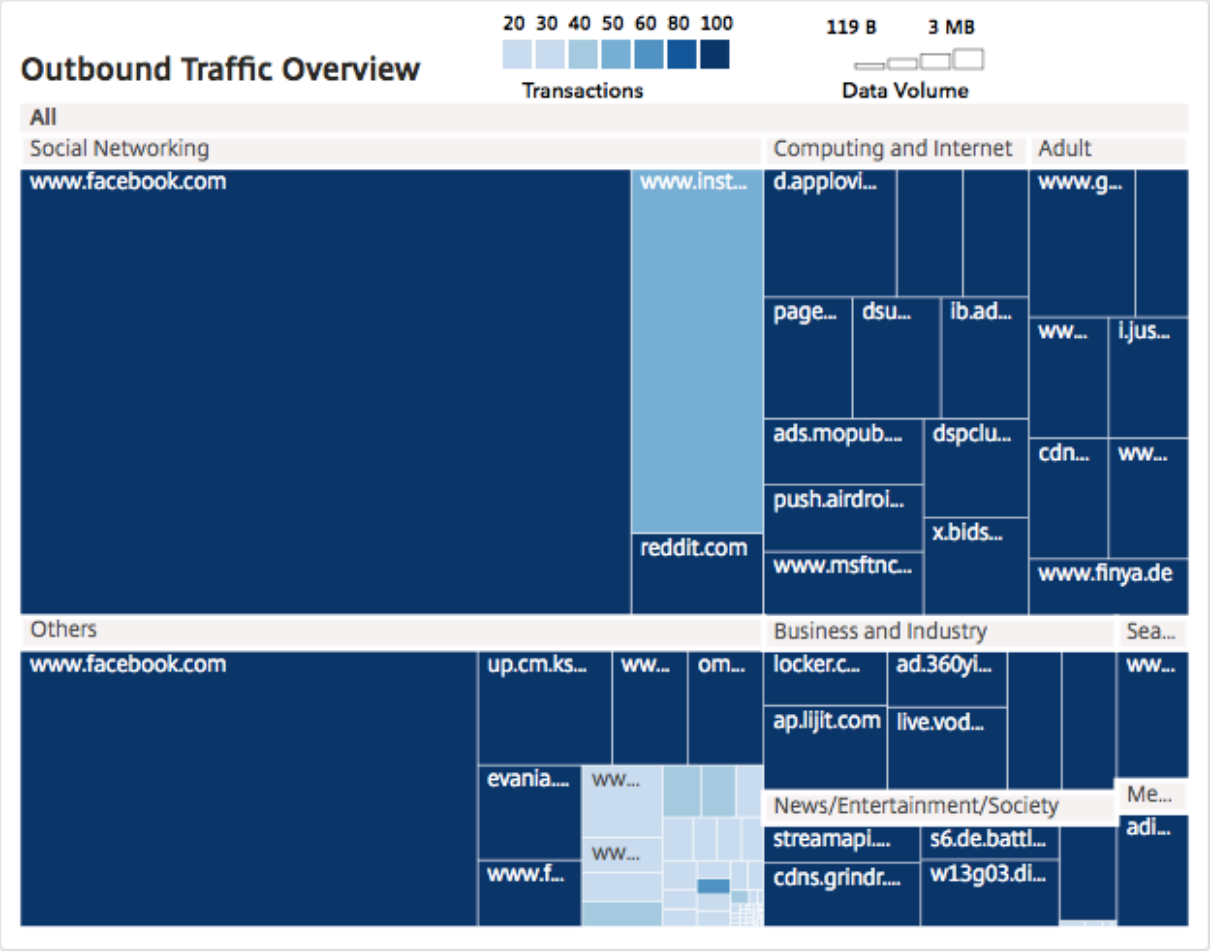
6. Quantité de trafic Web transmis, en fonction du port utilisé pour transmettre le trafic, du protocole utilisé par le trafic Web et des systèmes d'exploitation client utilisés pour transmettre le trafic.

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 du trafic sortant** comprend un volet **Vue d'ensemble 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 **Vue d'ensemble du trafic sortant** affiche les URL ou les domaines accessibles depuis votre réseau en tant que nœuds dans les catégories d'URL. Les nœuds sont dimensionnés en fonction du volume de données consommé en accédant à l'URL ou au domaine. La couleur du nœud indique le nombre de transactions qui se sont produites lors de l'accès à l'URL ou au domaine.



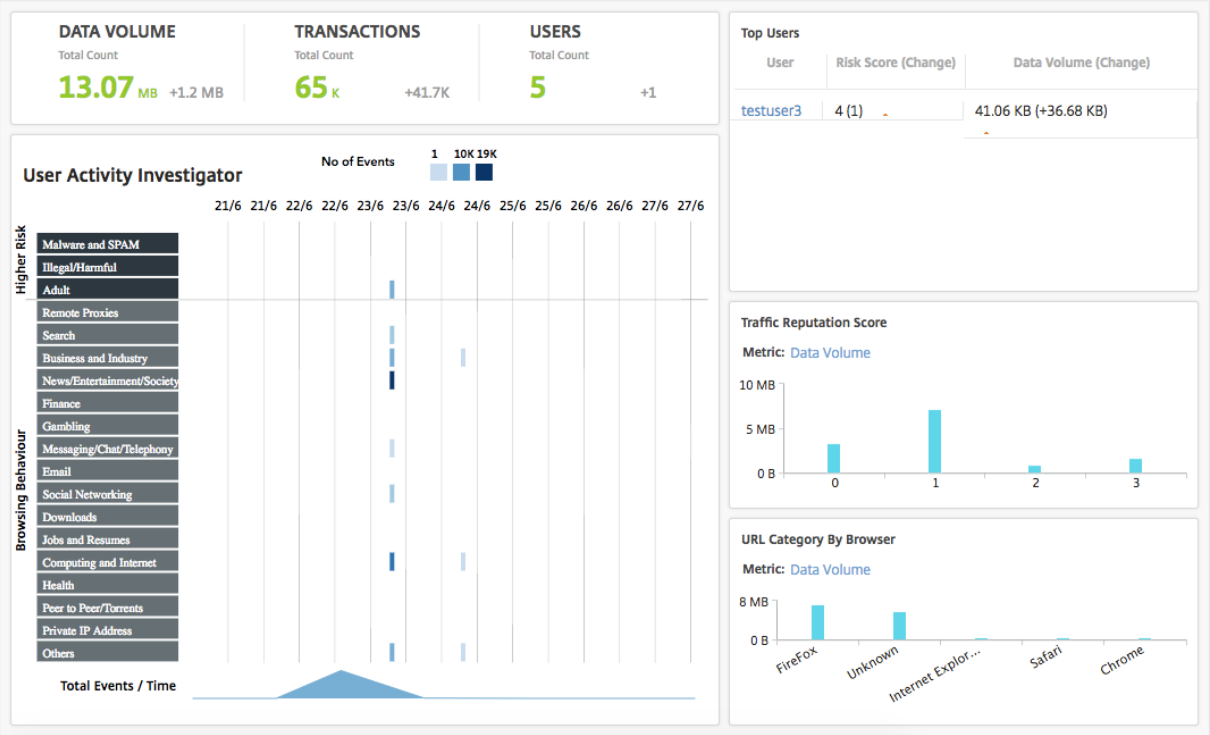
Vous pouvez cliquer sur une catégorie pour filtrer les graphiques afin d'afficher les détails liés à la catégorie pour la période spécifiée.

Tableau de bord utilisateur

Le **tableau de bord utilisateur** affiche un résumé des activités effectuées par les utilisateurs de votre entreprise. Il fournit des mesures clés que vous pouvez utiliser pour déterminer les éléments suivants :

1. Comportement de navigation des utilisateurs de votre entreprise.
2. Catégories d'URL auxquelles les utilisateurs de votre entreprise accèdent.
3. Les cinq principaux utilisateurs, en fonction de leurs scores de risque et de la bande passante qu'ils consomment. Pour plus d'informations sur le score de risque, voir Score de risque.
4. Navigateurs utilisés pour accéder aux URL ou aux domaines.
5. Montant du trafic Web généré par les utilisateurs, en fonction du score de réputation de trafic.

Pour accéder au Tableau de **bord utilisateur**, accédez à **Utilisateurs > Tableau de bord**.

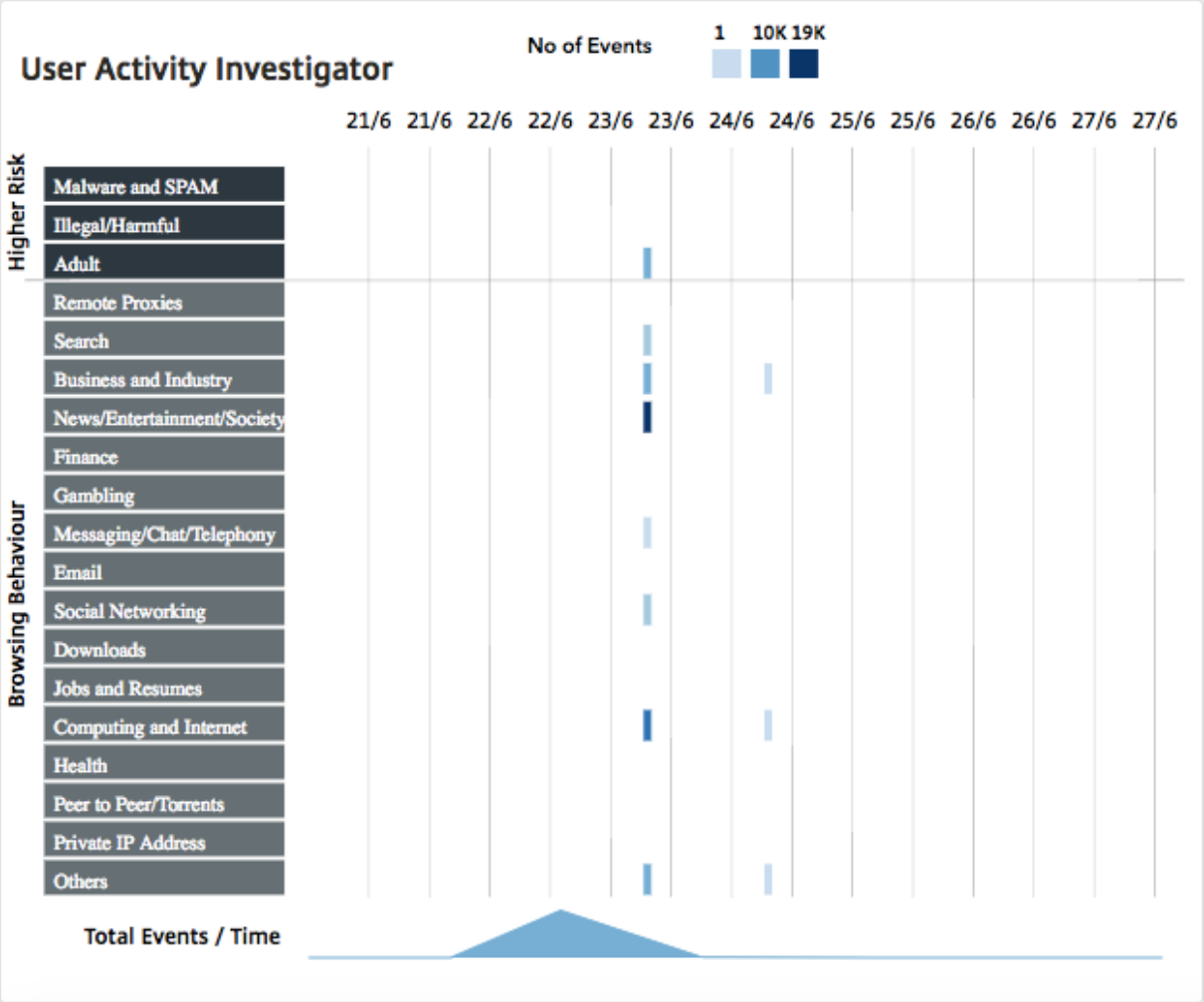


Vous pouvez cliquer sur un utilisateur dans le volet **Utilisateurs les plus importants** pour filtrer les graphiques afin d'afficher les détails de l'activité Web effectuée par l'utilisateur dans la période spécifiée.

Enquêteur d'activité utilisateur

Le **tableau de bord de l'utilisateur comprend un volet de l'enquêteur d'activité utilisateur** qui affiche diverses activités Web effectuées par les utilisateurs. Il affiche les catégories d'URL consultées par les utilisateurs pendant la période sélectionnée, ainsi que les divers événements déclenchés par catégorie d'URL. Vous pouvez cliquer sur les événements pour obtenir les détails du niveau de la transaction.

L' **enquêteur d'activité utilisateur** affiche des informations clés telles que le comportement de navigation de l'utilisateur, l'activité à risque élevé de l'utilisateur et les événements déclenchés, par catégorie d'URL. Les événements sont représentés sous forme de légendes rectangulaires sur le graphique. Chacune des légendes est agrégée à intervalles d'une minute si la durée sélectionnée est d'une heure, et à intervalles d'une heure si la durée sélectionnée est d'un jour.



Ces légendes sont agrégées et sont codées par couleur en fonction du nombre d'événements qui se sont produits. Vous pouvez placer le pointeur de la souris sur une légende pour afficher des détails tels que l'heure et le nombre d'événements agrégés pour la légende sélectionnée. Vous pouvez personnaliser la période du graphique en sélectionnant une heure dans la liste des périodes.

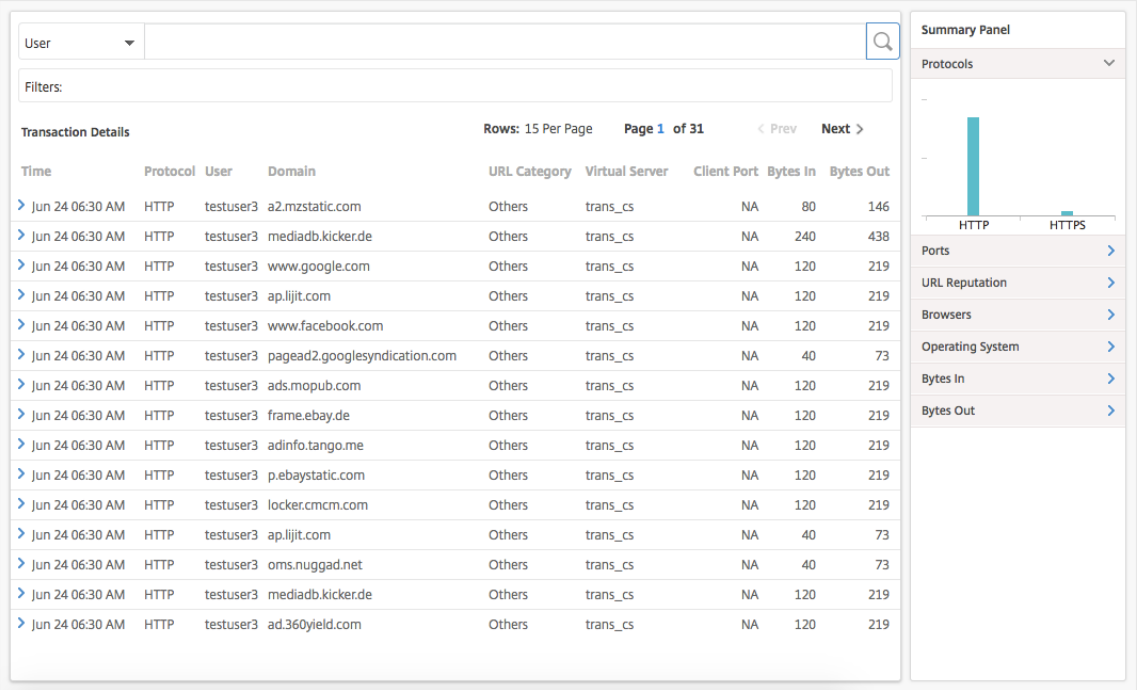
Vous pouvez cliquer sur les événements pour obtenir les détails des transactions.

Transactions utilisateur

La page Transactions utilisateur affiche les détails des transactions utilisateur dans votre réseau. Il fournit des détails au niveau de la transaction, tels que :

1. Heure à laquelle la transaction a eu lieu
2. Protocole utilisé pour la transaction
3. Nom d'utilisateur
4. Domaine accessible par l'utilisateur

5. Catégorie d'URL
6. Serveur proxy utilisé pour intercepter la transaction
7. Détails du port client
8. Octets entrants
9. Octets sortants



Panneau récapitulatif

Le **panneau Récapitulatif** affiche toutes les mesures des transactions visibles dans le volet **Détails des transactions** . Ce panneau vous permet de trier et d'afficher les transactions dans le volet **Détails de la transaction** en sélectionnant ou en désélectionnant les mesures. Le **panneau Récapitulatif** 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

Mesures	Description
Octets entrants	Quantité de données reçues via l'appliance Citrix ADC.
Octets sortants	Quantité de données envoyées via l'appliance Citrix ADC.

Cote de risque

Le score de risque est un système de notation utilisé dans Citrix ADM pour déterminer les risques associés aux utilisateurs de votre entreprise. Citrix ADM attribue un score de risque basé sur le score de réputation d'URL attribué par l'appliance Citrix ADC pour les URL consultées par les utilisateurs de votre réseau. Pour plus d'informations sur le score de réputation d'URL, reportez-vous à la sectionScore 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'a aucune menace perçue ou n'est pas anormale.
2.	L'activité web de l'utilisateur n'a aucune menace perçue ou n'est pas anormale, mais l'utilisateur accède à « Sites inconnus », qui n'ont pas de scores de réputation d'URL.
3	Aucune menace n'est détectée dans l'activité Web de l'utilisateur, mais l'utilisateur 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

April 29, 2021

Surveillance des interceptions SSL

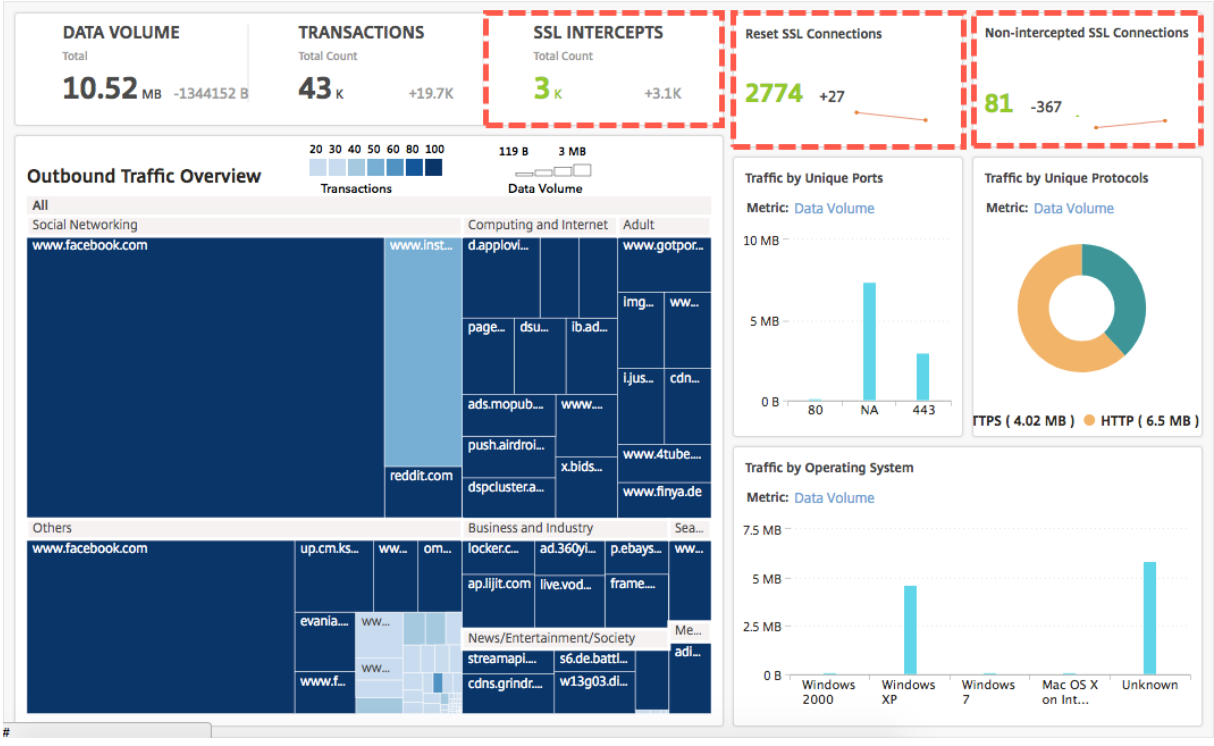
Une appliance Citrix ADC vous permet d'inspecter votre trafic sortant chiffré. Vous pouvez intercepter, contourner ou bloquer toutes les requêtes HTTPS en fonction des stratégies configurées sur l'appliance. Citrix Application Delivery Management (ADM) fournit les détails suivants sur les connexions SSL dans le tableau de **bord du trafic sortant** pour une période sélectionnée :

- Nombre de connexions SSL interceptées, non interceptées et réinitialisées par l'appliance Citrix ADC
- Détails de la transaction des connexions SSL

À l'aide de ces détails, vous pouvez affiner les stratégies de votre appliance Citrix ADC afin d'inspecter efficacement le trafic sortant chiffré. Pour de plus amples informations, consultez la section Proxy de transfert SSL Citrix.

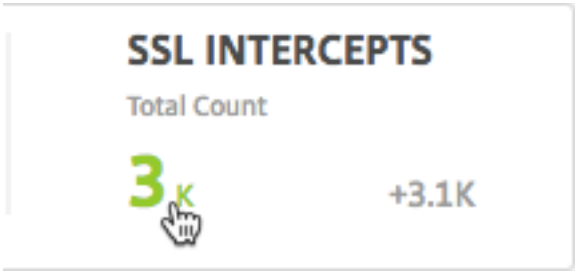
Pour afficher le nombre de connexions SSL interceptées, non interceptées et réinitialisées :

Accédez à **Applications > Tableau de bord du trafic sortant**. Le tableau de bord du trafic hors-bord affiche le nombre de connexions SSL interceptées, non interceptées et réinitialisées.

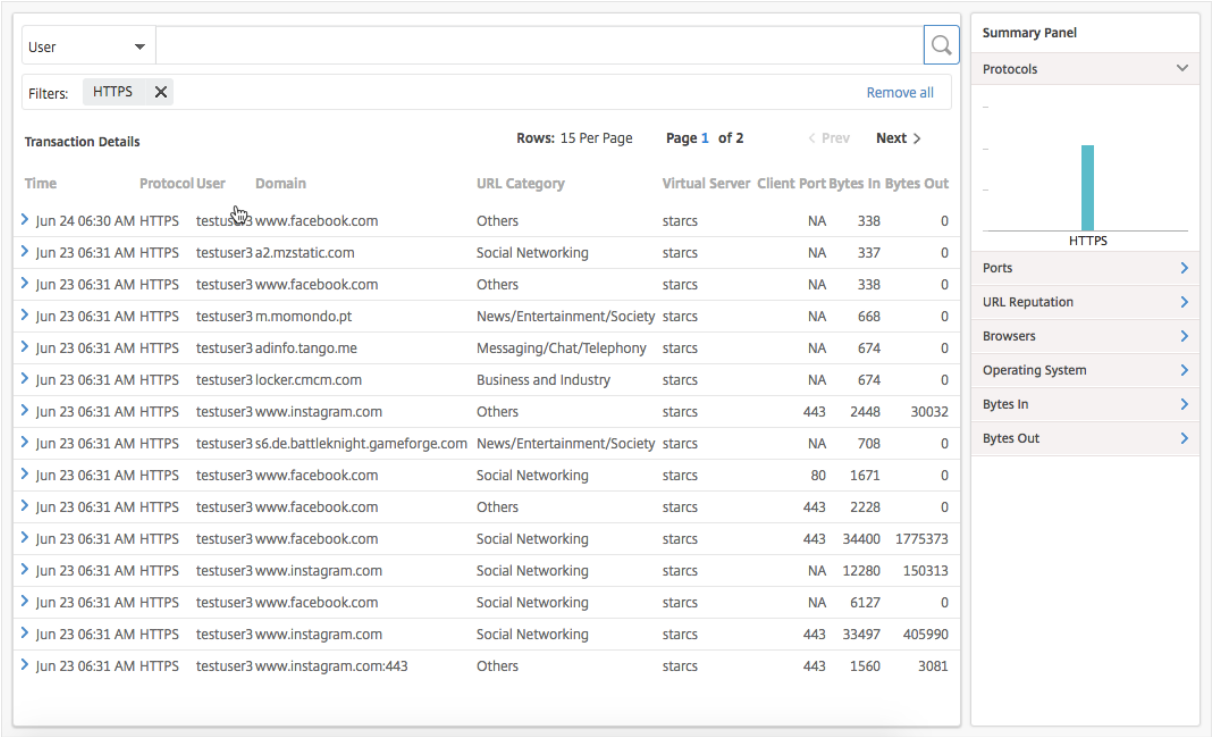


Pour afficher les détails de transaction des connexions SSL interceptées :

1. Accédez à **Applications > Tableau de bord du trafic sortant**.
2. Dans le tableau de **bord du trafic hors-bord**, cliquez sur le nombre total dans la section **INTERCEPTS SSL** .



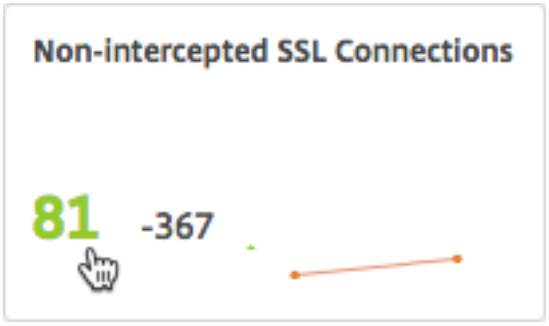
Les détails de transaction des connexions SSL interceptées au cours de la période sélectionnée sont affichés sur la page **Détails de la transaction**.



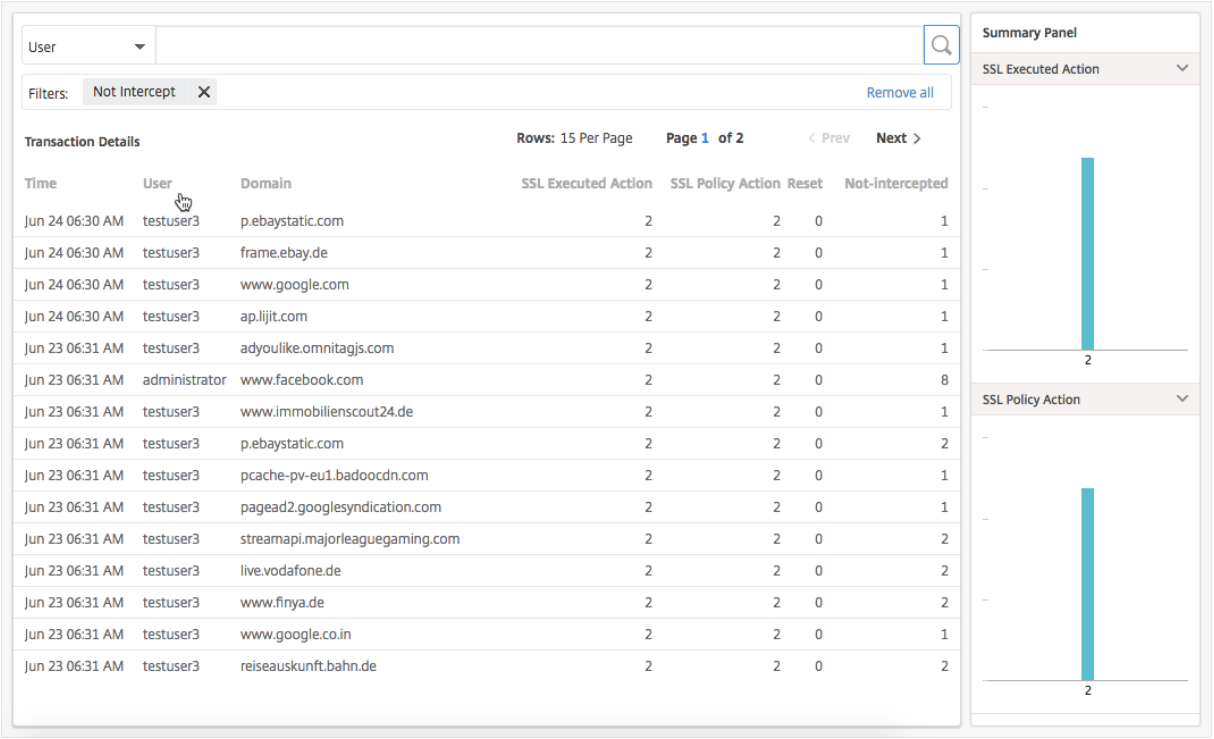
Vous pouvez également filtrer les détails des transactions par utilisateur et par catégorie d'URL.

Pour afficher les détails de transaction des connexions SSL sur lesquelles le trafic n'a pas été intercepté :

1. Accédez à **Applications > Tableau de bord du trafic sortant**.
2. Dans le tableau de **bord du trafic hors-bord**, cliquez sur le nombre total dans la section **Connexions SSL non interceptées** .



Les détails de transaction des connexions SSL sur lesquelles le trafic n'a pas été intercepté pendant la période sélectionnée apparaissent dans la page **Détails de la transaction**.

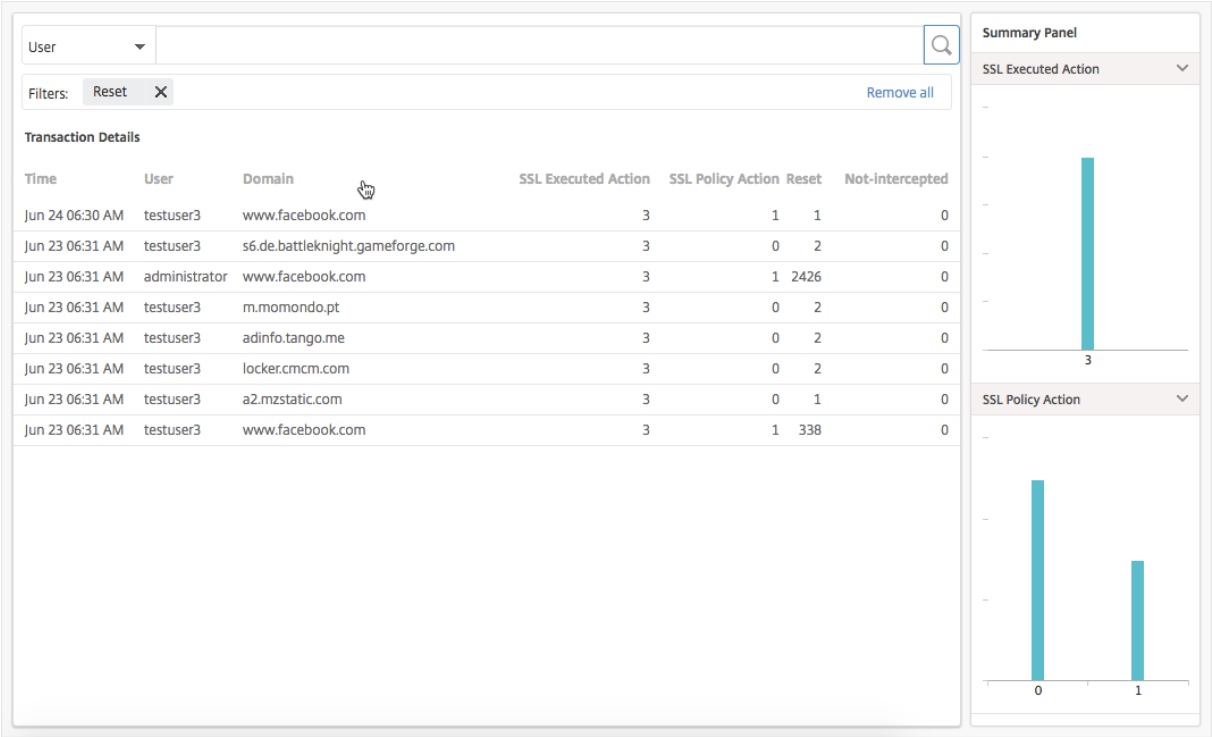


Vous pouvez également filtrer les détails des transactions par utilisateur et par catégorie d'URL.

Pour afficher les détails de transaction des connexions SSL qui sont réinitialisées :

1. Accédez à **Applications > Tableau de bord du trafic sortant**.
2. Dans le tableau de **bord du trafic hors-bord**, cliquez sur le nombre total dans la section **Réinitialiser les connexions SSL** .

Les détails de transaction des connexions SSL sur lesquelles le trafic n'a pas été intercepté pendant la période sélectionnée apparaissent sur la page **Détails de la transaction**.



Vous pouvez également filtrer les détails des transactions en fonction de l'utilisateur et de la catégorie d'URL.

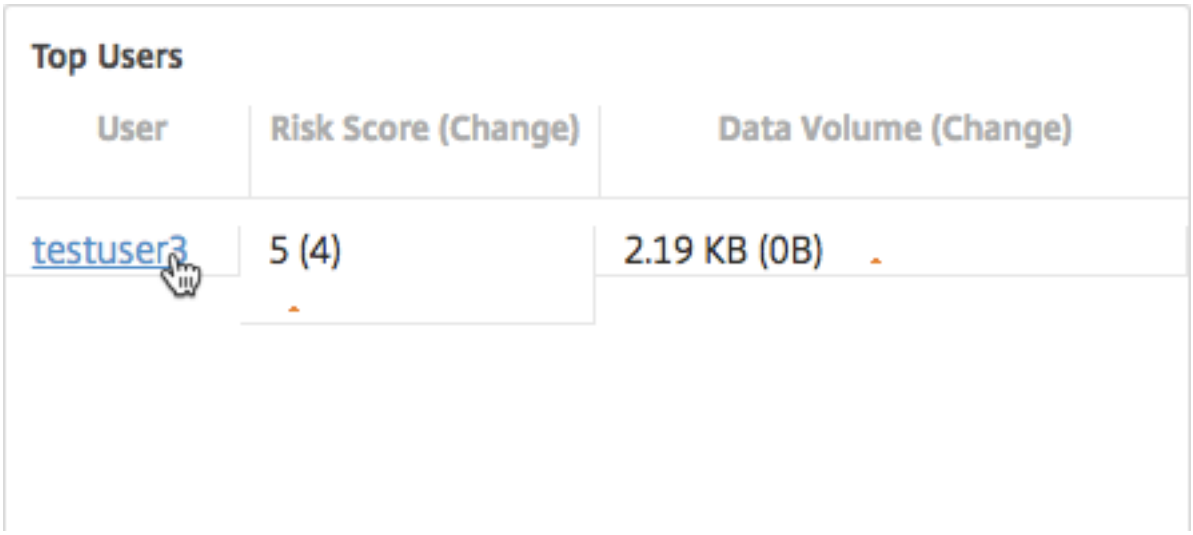
Inspection des points de terminaison

Les stratégies que vous avez configurées sur une appliance Citrix ADC spécifient comment elle enregistre toutes les activités utilisateur effectuées dans votre entreprise. Citrix ADM fournit des mesures clés que vous pouvez utiliser pour déterminer :

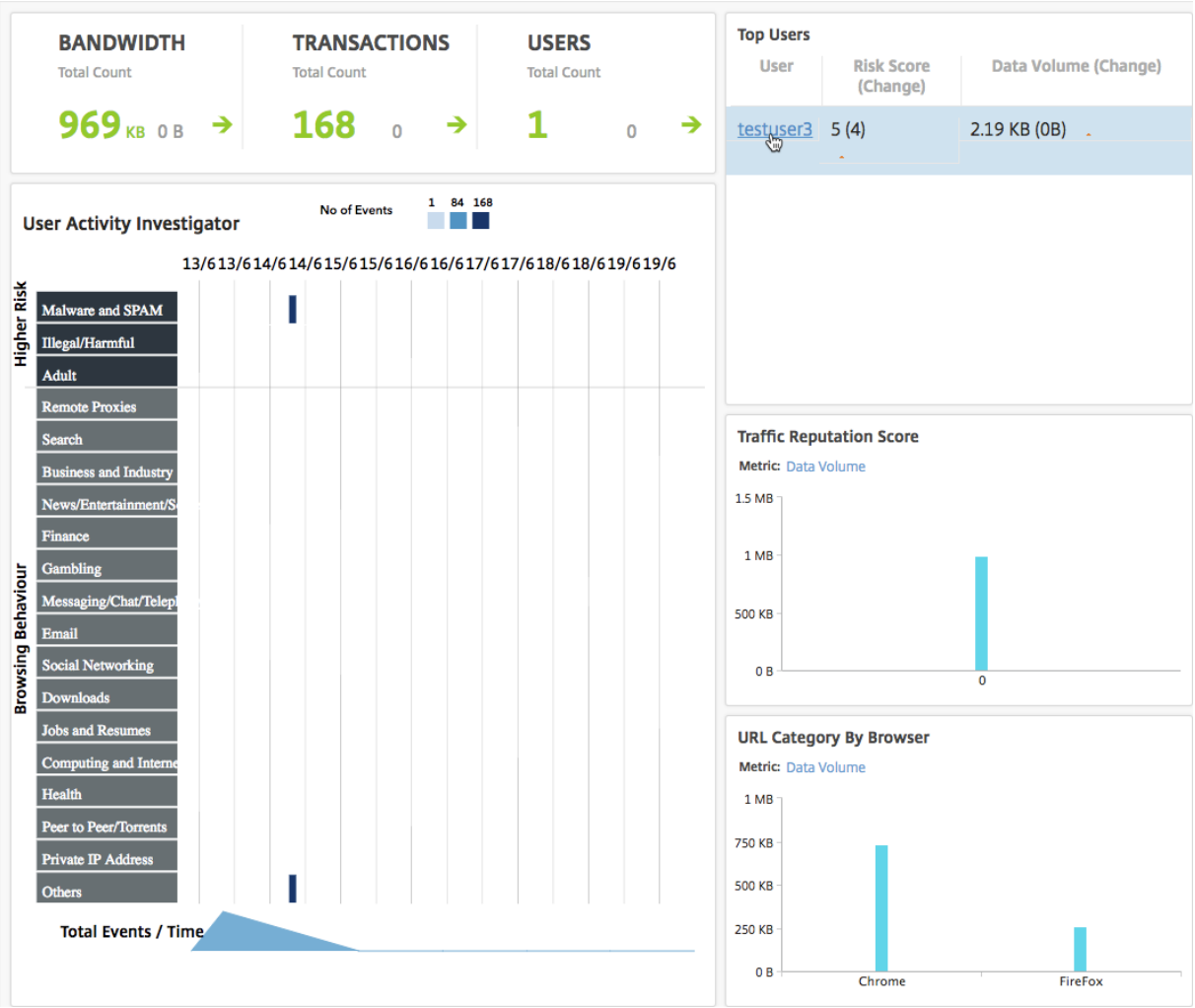
1. Comportement de navigation des utilisateurs de votre entreprise.
2. Catégories d'URL auxquelles les utilisateurs de votre entreprise accèdent.

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, reportez-vous à la sectionCote 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 d'utilisateur testuser3 accède en permanence aux sites liés aux programmes malveillants de votre entreprise, Citrix ADM identifie l'utilisateur en tant qu'utilisateur d'activité à haut risque et lui attribue un score de risque plus élevé. Les informations testuser3 sont affichées dans la section **Utilisateurs les plus importants** du tableau de **bord des utilisateurs**.

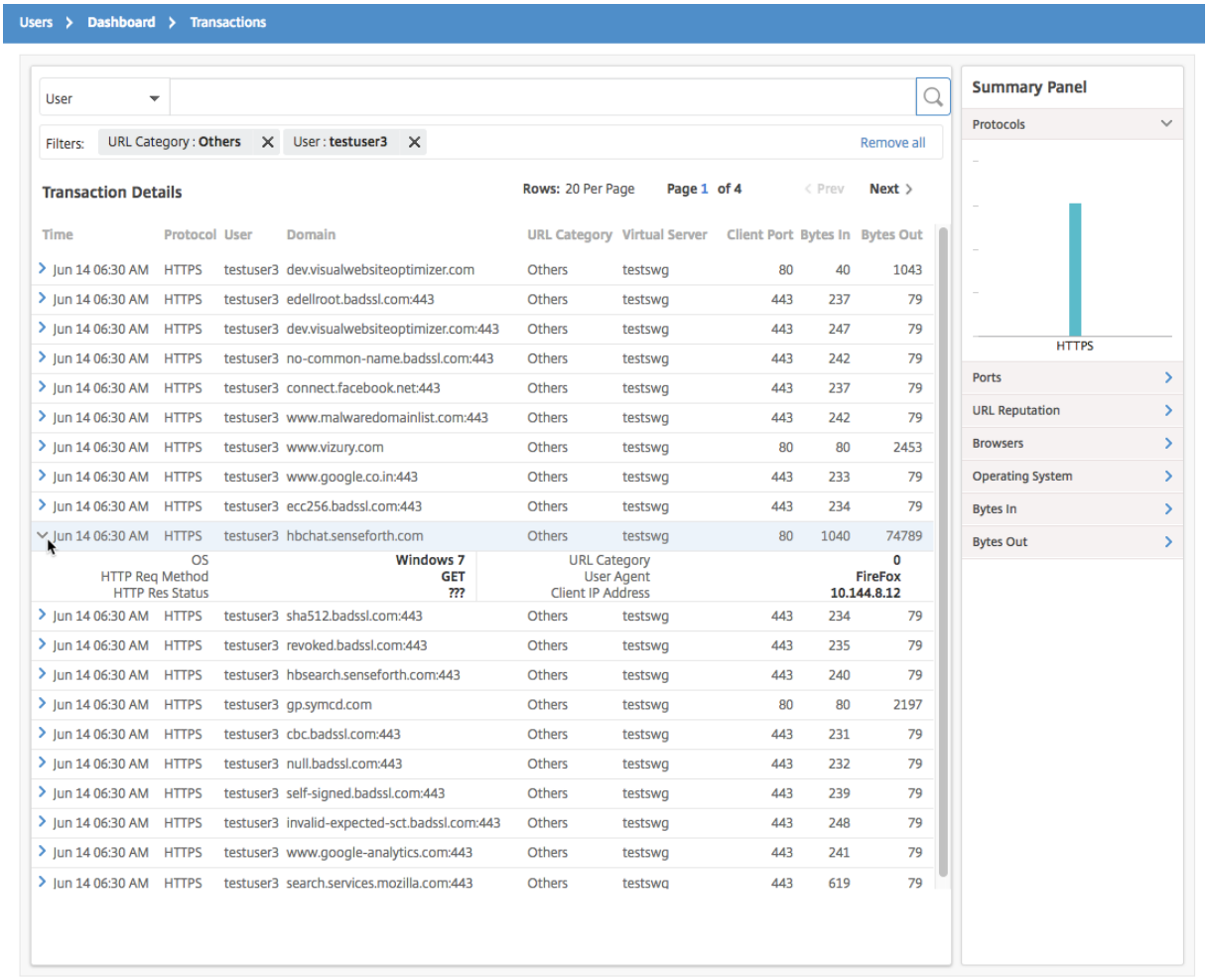


Vous pouvez cliquer sur testuser3 pour filtrer le **tableau de bord utilisateur** afin d'afficher toutes les mesures clés liées à testuser3.



Dans le volet **Enquête sur l'activité de l'utilisateur**, l'activité à haut risque de testuser3 s'affiche sous forme d'événements dans les catégories d'URL respectives.

Vous pouvez survoler les événements pour afficher le nombre d'événements et cliquer sur événements pour analyser les transactions qui se sont produites pendant les événements.

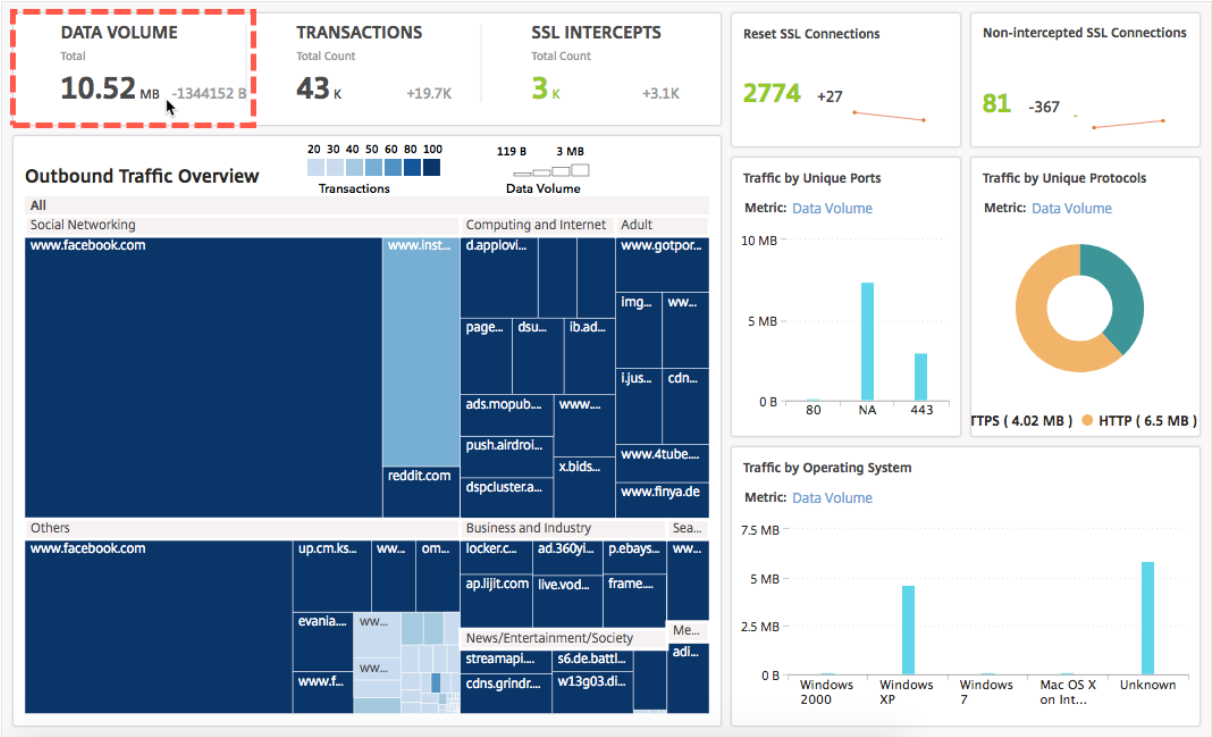


Grâce à ces informations, vous pouvez déterminer si votre système est infecté par des logiciels malveillants, ou bien comprendre le modèle de consommation de bande passante de l'utilisateur et affiner vos stratégies Citrix ADC. Pour de plus amples informations, consultez la section Documentation du proxy de transfert SSL Citrix.

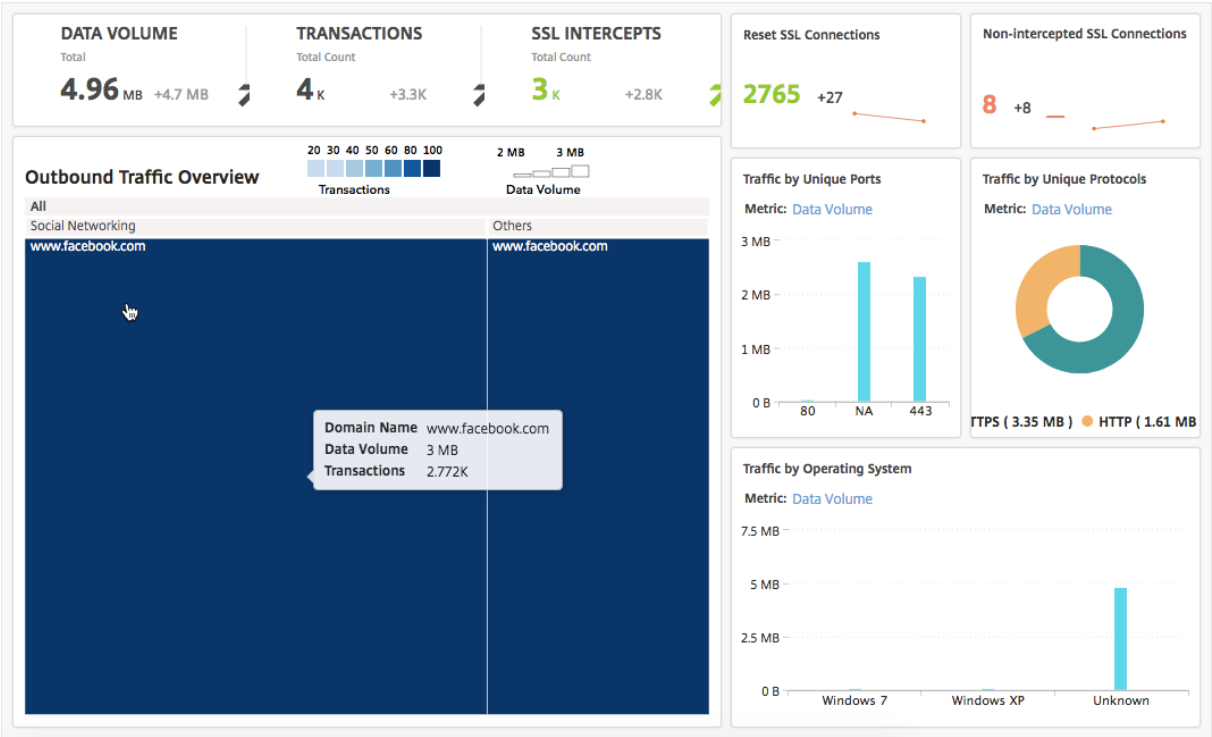
Rapports sur la consommation de bande passante

Le tableau de **bord du trafic sortant** et le tableau de **bord utilisateur** 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 de volume de données par les URL ou les domaines auxquels vous avez accédé à partir de votre réseau. Accédez à **Applications > Tableau de bord du trafic sortant**, où les détails du volume de données sont affichés dans la section **Volume de données** .

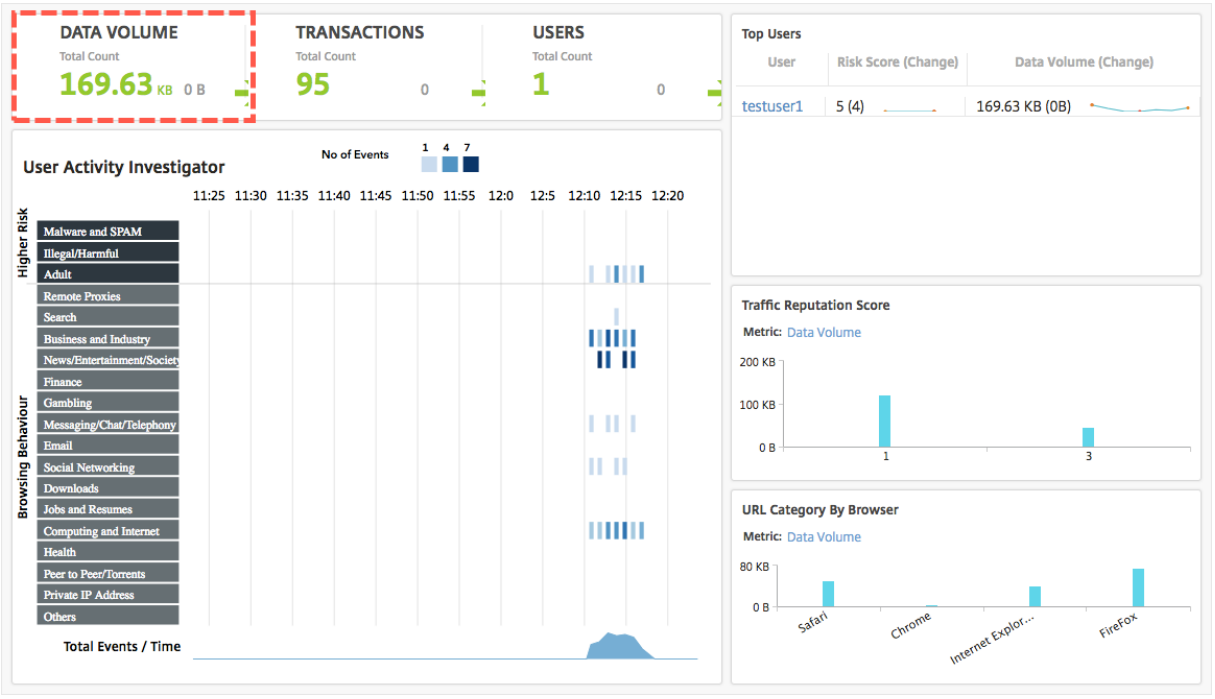


Dans le volet **Vue d'ensemble du trafic sortant**, vous pouvez cliquer sur un domaine ou une URL pour afficher les détails du volume de données consommé par le domaine ou l'URL.

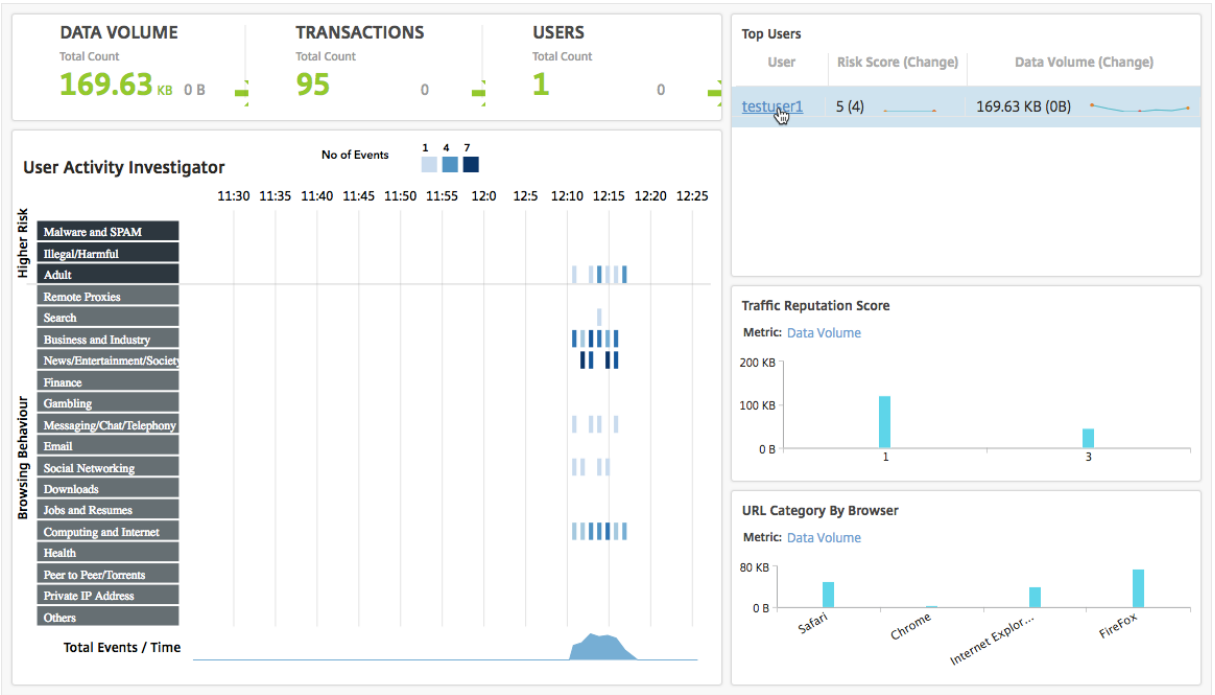


Le **tableau de bord utilisateur** fournit des détails sur la bande passante consommée par les utilisateurs de votre réseau. Accédez à **Utilisateurs > Tableau de bord** pour afficher les détails de la bande

passante consommée par les utilisateurs dans la section **VOLUME DE DONNÉES** du **Tableau de bord utilisateur**.



Vous pouvez afficher les détails de la bande passante consommée par un utilisateur en le sélectionnant dans la section **Utilisateurs les plus importants**. La section **VOLUME DE DONNÉES** et les autres mesures clés du graphique sont filtrées pour l'utilisateur sélectionné.



En utilisant ces détails, vous pouvez comprendre la consommation de bande passante et la raison

de la consommation. Par exemple, si un utilisateur accède aux sites Web de réseaux sociaux et que cela a entraîné une consommation importante de bande passante, l'administrateur peut accéder à l'appliance Citrix ADC et configurer une fonctionnalité de liste d'URL pour contrôler l'accès aux sites Web. Pour de plus amples informations, consultez la section Cas d'utilisation : Filtrage d'URL à l'aide de la rubrique Jeu d'URL personnalisé.

Affichage de la distribution du trafic sortant

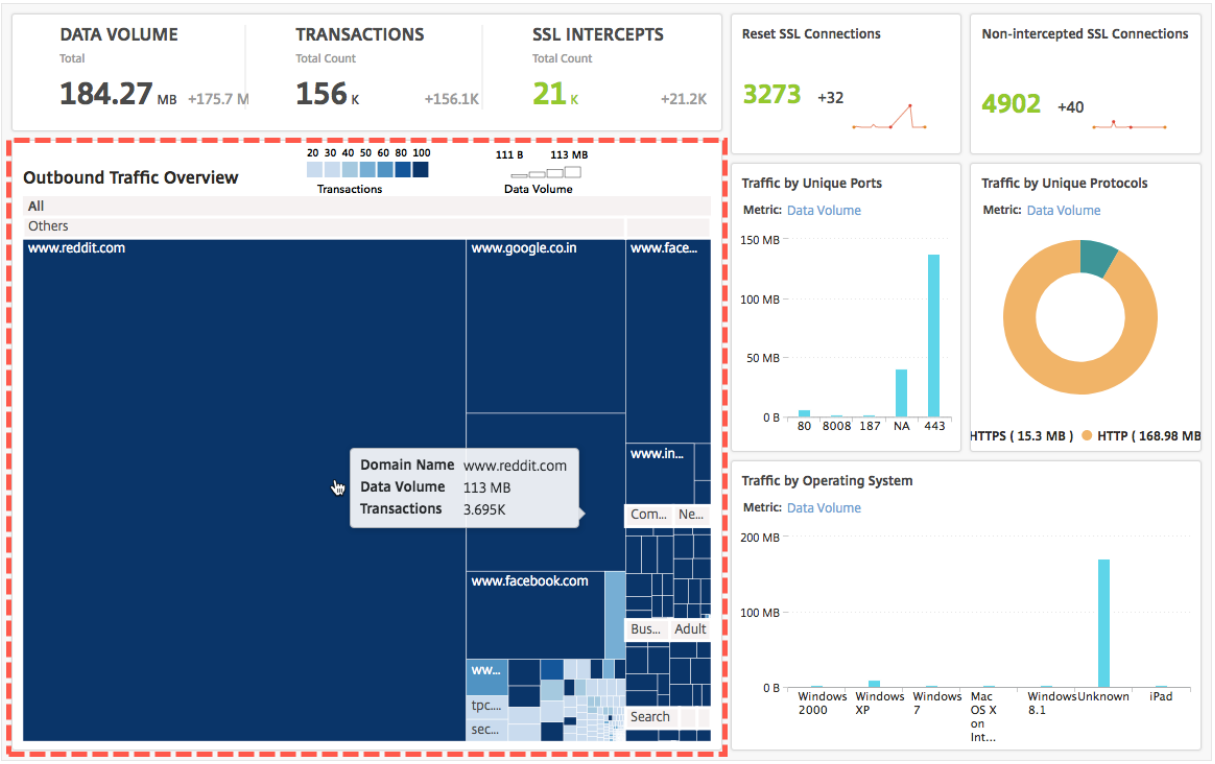
L'appliance Citrix ADC fournit des fonctionnalités de catégorisation et de filtrage d'URL que vous pouvez utiliser pour catégoriser les URL accessibles à partir de votre réseau. Dans Citrix ADM, le tableau de **bord du trafic sortant** inclut un volet **Vue d'ensemble du trafic sortant** . Dans le volet **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 sélectionnée, 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 interceptées, non interceptées et réinitialisées lors de l'accès à l'URL

Grâce à ces informations, vous pouvez comprendre le modèle de trafic sortant et prendre des décisions correctives, telles que le blocage de certaines URL.

Pour afficher 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 **Aperçu du trafic sortant** :



Si vous souhaitez afficher les détails d'une URL particulière, sélectionnez l'URL.

À l'aide de ces informations, vous pouvez comprendre le modèle de trafic sortant et contrôler votre trafic réseau à l'aide d'un filtre d'URL configuré sur votre appliance Citrix ADC. Pour de plus amples informations, consultez la section filtrage d'URL.

Capacité groupée

April 29, 2021

La capacité groupée dans Citrix ADC est un cadre de licence qui comprend une bande passante commune et un pool d'instances hébergé sur Citrix Application Delivery Management (ADM) et desservi par Citrix Application Delivery Management. À partir de ce pool commun, chaque instance ADC de votre datacenter, indépendamment de la plate-forme ou du facteur de forme, vérifie une licence d'instance et seulement autant de bande passante qu'elle en a besoin. Le fichier de licence et, par conséquent, la bande passante ne sont pas liés à l'instance. Lorsque l'instance n'a plus besoin de ces ressources, elle les réintègre dans le pool commun, rendant les ressources disponibles pour les autres instances qui en ont besoin.

> **Remarque**
>
> Dans le service ADM, l'un des agents est le serveur de licences. Dans ADM local, le serveur local

> est le serveur de licences (même si des agents sont déployés).

Ce cadre de licence optimise l'utilisation de la bande passante en veillant à ce que les instances ne soient pas allouées plus de bande passante que leur exigence. La capacité des instances ADC à vérifier les licences et la bande passante dans et hors d'un pool commun vous permet également d'automatiser le Provisioning des instances.

Vous pouvez augmenter ou diminuer la bande passante allouée à une instance au moment de l'exécution sans affecter le trafic. Vous pouvez également transférer les licences du pool d'une instance à une autre.

Configurer la capacité groupée

April 29, 2021

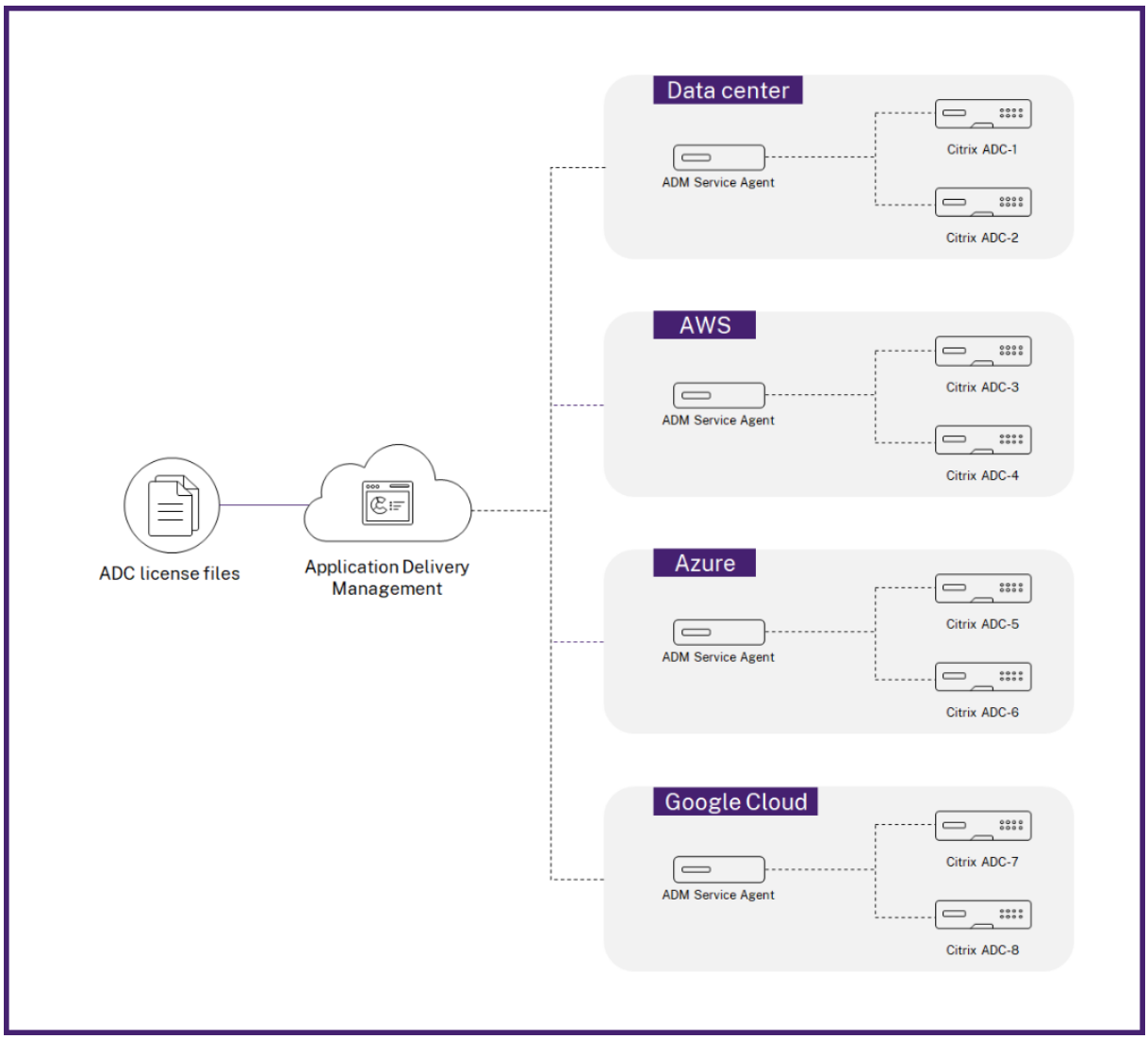
La capacité mise en commun Citrix ADC vous permet de partager des licences de bande passante ou d'instance entre différents facteurs de forme ADC. Pour les instances basées sur un abonnement CPU virtuel, vous pouvez partager la licence CPU virtuelle entre les instances. Utilisez cette capacité groupée 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 assurant l'allocation de bande passante nécessaire à une instance et pas plus que nécessaire. 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.

Pour utiliser la capacité groupée ADC, assurez-vous d'attacher un agent ADM à une instance ADC. Les instances ADC consignent et retirent les licences du service ADM via un agent.

Vous pouvez également utiliser des licences de capacité groupée pour les instances FIPS ADC. Vous pouvez effectuer les tâches suivantes dans le service ADM :

- Téléchargez les fichiers de licences de capacité groupée (pool de bande passante ou pool d'instances) sur le serveur de licences.
- Allouez des licences du pool de licences aux instances ADC à la demande.
- Consultez les licences des instances ADC (MPX-Z /SDX-Z/VPX/CPX/BLX) en fonction de la capacité minimale et maximale de l'instance.



Problèmes de capacité mise en commun des ADC

Les états de capacité groupée indiquent l'exigence de licence sur une instance ADC. Les instances ADC configurées avec une capacité groupée affichent l'un des états suivants :

- **Optimum** : l'instance est en cours d'exécution avec une capacité de licence appropriée.
- **Incompatibilité de capacité** : l'instance est en cours d'exécution avec une capacité inférieure à celle configurée par l'utilisateur.
- **Grace** : Instance est en cours d'exécution sur une licence de grâce.
- **Grace & Mismatch** : L'instance est en cours d'exécution avec grâce mais avec une capacité inférieure à celle configurée par l'utilisateur.
- **Non disponible** : l'instance n'est pas enregistrée auprès d'ADM pour la gestion, ou la communication NITRO entre ADM et les instances ne fonctionne pas.

- **Non alloué** : la licence n'est pas allouée dans l'instance.

Avant de commencer

Assurez-vous de ce qui suit avant de configurer la capacité groupée :

- Installez et enregistrez un agent dans le service ADM. Pour installer et enregistrer un agent, reportez-vous à la section Mise en route.
- Les `7279` ports `27000` et sont disponibles pour extraire les licences d'ADM vers une instance. Voir, Configuration système requise

Étape 1 - Appliquer des licences dans ADM

1. Dans Citrix ADM, accédez à **Réseaux** > **Licences** .
2. Dans la section **Fichiers de licence**, sélectionnez **Ajouter un fichier de licence** et sélectionnez l'une des options suivantes :
   - **Télécharger des fichiers de licence à partir d'un ordinateur local**. Si un fichier de licence est déjà présent sur votre ordinateur local, vous pouvez le télécharger dans ADM.
   - **Utilisez le code d'accès de licence**. Spécifiez le code d'accès à la licence que vous avez achetée auprès de Citrix. Sélectionnez ensuite **Obtenir des licences**. Sélectionnez ensuite **Terminer**.

   > **Remarque**
   >
   > À tout moment, vous pouvez ajouter d'autres licences à ADM à partir des **paramètres de licence**.
3. Cliquez sur **Terminer**.

   Les fichiers de licence sont ajoutés à ADM. L'onglet **Informations sur l'expiration des licences** répertorie les licences présentes dans l'ADM et les jours restants jusqu'à leur expiration.
4. Dans **Fichiers de licence**, sélectionnez un fichier de licence à appliquer et cliquez sur **Appliquer des licences**.

   Cette action permet aux instances ADC d'utiliser la licence sélectionnée comme capacité groupée.

Étape 2 - Enregistrer le service ADM en tant que serveur de licences

Vous pouvez enregistrer le service ADM en tant que serveur de licences auprès d'une instance Citrix ADC à l'aide d'un agent.

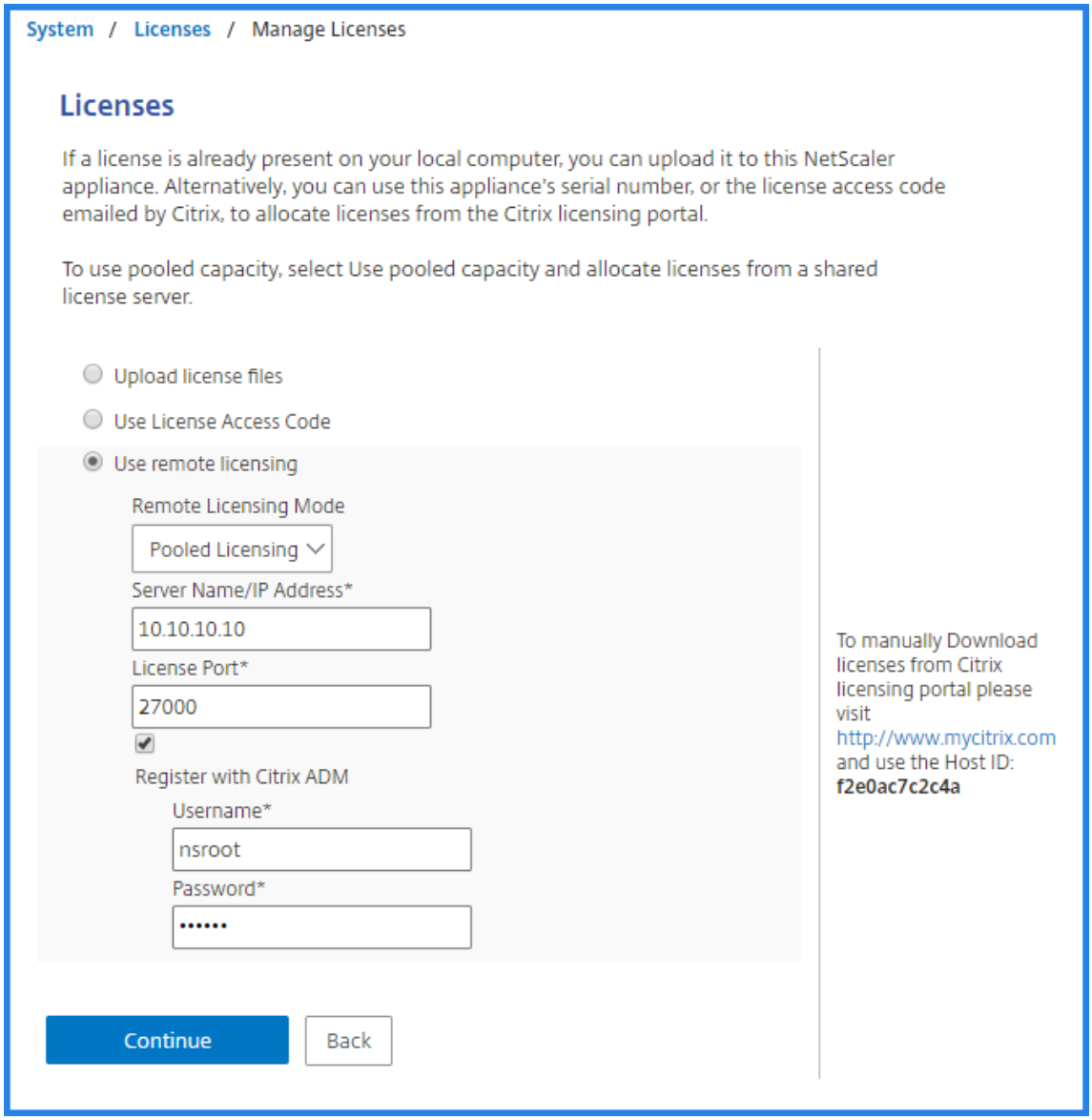
Utilisez l'une des procédures suivantes pour enregistrer le service ADM en tant que serveur de licences :

- Utiliser l'interface graphique
- Utiliser l'interface de ligne de commande

Utiliser l'interface graphique pour enregistrer un agent ADM

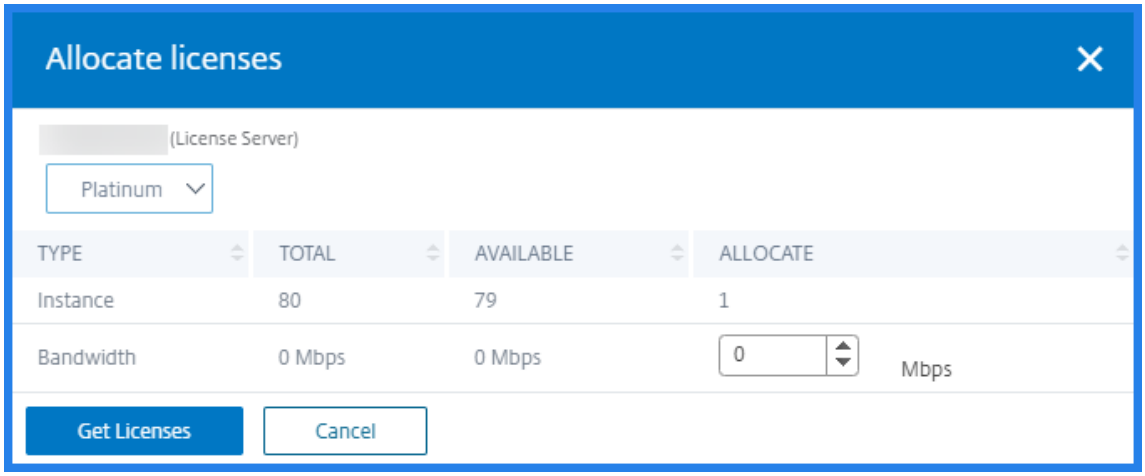
Dans l'interface graphique ADM, enregistrez l'agent ADM associé à une instance ADC.

1. Connectez-vous à l'interface graphique Citrix ADC.
2. Accédez à **Système** > **Licences** > **Gérer les licences** .
3. Cliquez sur **Ajouter une nouvelle licence**.
4. Sélectionnez **Utiliser la licence à distance** et sélectionnez le mode de licence à distance dans la liste.
5. Dans le champ **Nom du serveur/Adresse IP**, spécifiez l'adresse IP de l'agent ADM associé qui est enregistrée auprès du service ADM.
6. Sélectionnez **Enregistrer auprès de Citrix ADM**.
7. Entrez vos informations d'identification ADM pour enregistrer une instance auprès de Citrix ADM, puis cliquez sur **Continuer**.



8. Dans **Allouer les licences**, sélectionnez l'édition de la licence et spécifiez la bande passante requise.

   Pour la première fois, allouez des licences dans Citrix ADC. Vous pouvez modifier ou libérer ultérieurement l'allocation de licence à partir de l'interface graphique Citrix ADM.



9. Cliquez sur **Obtenir les licences**.

> **Important**
>
> Redémarrez l'instance à chaud si vous modifiez l'édition de la licence. Les modifications de configuration ne prennent effet que lorsque vous redémarrez l'instance.

Utiliser l'interface de ligne de commande pour ajouter un agent ADM

Si une instance ADC n'a pas d'interface graphique, utilisez les commandes CLI suivantes pour ajouter un agent ADM associé à une instance :

1. Connectez-vous à la console Citrix ADC.
2. Ajoutez l'adresse IP de l'agent ADM associé qui est enregistrée auprès du service ADM :

```
1 > add ns licenseserver <adm-agent-IP-address> -port <adm-agent-
    license-port-number>
2 <!--NeedCopy-->
```

3. Affichez la bande passante de licence disponible sur le serveur de licences :

```
1 > sh ns licenseserverpool
2 <!--NeedCopy-->
```

4. Allouez la bande passante de licence à partir de l'édition de licence requise :

```
1 > set ns capacity -unit gbps -bandwidth <specify-license-bandwidth
    > edition <specify-license-edition>
2 <!--NeedCopy-->
```

   L'édition de licence peut être **Standard** ou **Advanced** ou **Premium**.

> **Important**
>
> Warm redémarrez l'instance si vous modifiez l'édition de la licence.
>
> `reboot -w`
>
> Les modifications de configuration ne prennent effet que lorsque vous redémarrez l'instance.

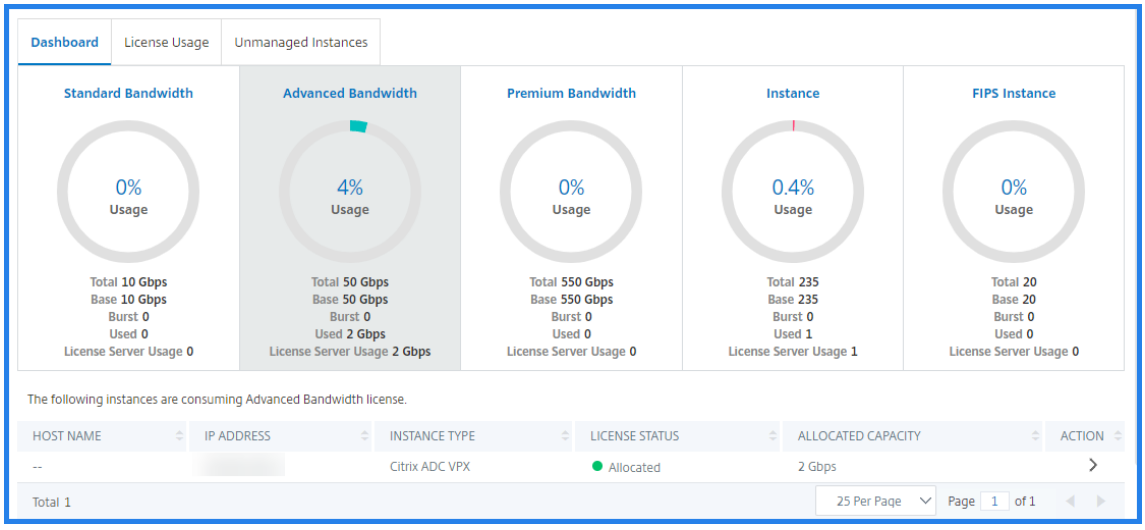
Étape 3 - Allouer des licences groupées aux instances ADC

Pour allouer des licences de capacité groupée à partir de l'interface graphique d'ADM :

1. Connectez-vous à Citrix ADM.
2. Accédez à **Réseaux > Licences > Licences de bande passante > Capacité groupée**.

   La capacité d'instance FIPS n'apparaît que si vous téléchargez des licences d'instance FIPS vers ADM.
3. Cliquez sur le pool de licences que vous souhaitez gérer.

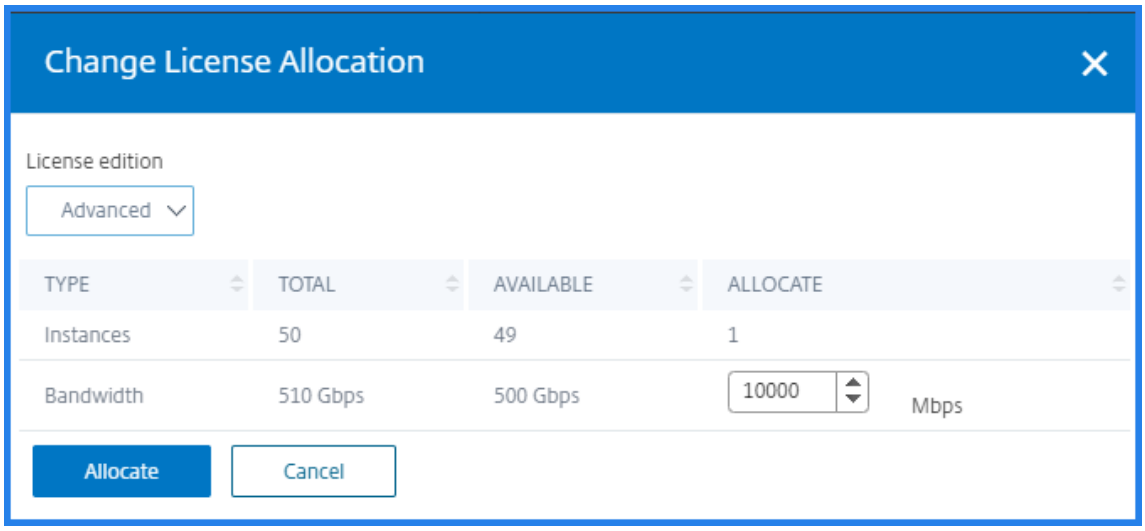
   > **Remarque**
   >
   > Le champ **Capacité allouée** ne reflète pas immédiatement la bande passante modifiée. Le changement de bande passante prend effet après le redémarrage à chaud de l'ADC.
   >
   > Dans **Détails d'allocation**, les champs **Demandé** et **Appliqué** sont mis à jour lorsque vous modifiez l'allocation de bande passante de l'instance.
4. Sélectionnez une instance ADC dans la liste des instances disponibles en cliquant sur le bouton **.



La colonne Statut de la licence affiche les messages d'état d'allocation de licence correspondants.

> **Remarque**
>
> L'onglet **Instances non gérées** affiche les instances qui sont découvertes mais non gérées dans Citrix ADM.
>
> 
>

5. Cliquez sur **Change allocation** ou **Release allocation** pour modifier l'allocation de licence.
6. Une fenêtre contextuelle contenant les licences disponibles dans le serveur de licences s'affiche.
7. Vous pouvez choisir la bande passante ou l'allocation d'instance à l'instance en définissant les options de liste Allouer. Après avoir effectué vos sélections, cliquez sur **Allouer**.
8. Vous pouvez également modifier l'édition de licence allouée à partir des options de liste de la **fenêtre Modifier l'allocation de licence**.



> **Remarque**
>
> Warm redémarre une instance si vous modifiez l'édition de la licence.

Configurer la capacité groupée sur les instances ADC

Vous pouvez configurer des licences de capacité groupée sur les instances ADC suivantes :

- Instances MPX-Z ADC
- Instances VPX ADC
- Paire haute disponibilité ADC

Instances MPX-Z Citrix ADC

MPX-Z est l'appliance ADC MPX à capacité groupée. MPX-Z prend en charge le regroupement de bande passante pour les licences Premium, Advanced ou Standard Edition.

MPX-Z nécessite des licences de plate-forme avant de pouvoir se connecter au serveur de licences. Vous pouvez installer la licence de plate-forme MPX-Z en utilisant l'une des options suivantes :

- Chargement du fichier de licence à partir d'un ordinateur local.
- Utilisation du numéro de série matériel de l'instance.
- Code d'accès à la licence de la section **Système** > **Licences** de l'interface graphique de l'instance.

Si vous supprimez la licence de plate-forme MPX-Z, la fonctionnalité de capacité groupée est désactivée. Les licences d'instance sont libérées 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 procède automatiquement à l'analyse des licences groupées requises pour sa capacité configurée.

Instances Citrix ADC VPX

Une instance VPX ADC à capacité groupée peut extraire des licences d'un pool de bande passante (éditions Premium/Advanced/Standard). Vous pouvez utiliser l'interface graphique ADC pour récupérer les licences du serveur de licences.

Vous pouvez modifier dynamiquement la bande passante d'une instance VPX sans redémarrer. Un redémarrage n'est requis que si vous souhaitez modifier l'édition de la licence.

> **Remarque**
>
> Lorsque vous redémarrez l'instance, les licences de capacité groupée configurées sont automatiquement retirées du serveur ADM.

Paire haute disponibilité Citrix ADC

Avant de commencer, assurez-vous que le serveur ADM est configuré en tant que serveur de licences. Pour de plus amples informations, consultez la section Configurer ADM en tant que serveur de licences.

Lorsque vous allouez la bande passante à une paire ADC HA, Citrix ADM retirera la même bande passante aux instances principales et secondaires. Si vous allouez 10 Mbit/s de bande passante à une paire ADC HA, ADM effectue les opérations suivantes :

1. Vérifie 20 Mbps de bande passante à la paire HA.
2. Allocation 10 Mbit/s à chaque instance de la paire HA.

Pour allouer une licence de pool à une paire ADC HA, reportez-vous à la section Allouer des licences groupées aux instances ADC.

La page **Capacité groupée** affiche séparément les instances et leur capacité allouée. Si vous modifiez ou relâchez la bande passante de l'instance principale, la bande passante de l'instance secondaire se synchronise automatiquement avec l'instance principale. Toutefois, la synchronisation ne se produit pas si vous modifiez ou libérez la bande passante de l'instance secondaire.

Configurer le service ADM uniquement pour la fonctionnalité de licence groupée

April 29, 2021

En tant qu'administrateur, vous pouvez configurer le service ADM uniquement pour la fonctionnalité de licence groupée. Avec cette configuration, le service ADM reçoit uniquement les données de licence des instances ADC.

Parfois, vous pouvez avoir le mandat réglementaire qui exige de restreindre les données des instances ADC de quitter la zone de réglementation. Dans de telles situations, vous pouvez déployer une instance locale d'un serveur ADM sur site dans votre zone réglementaire pour utiliser les fonctionnalités de gestion, de surveillance et d'analyse. Lorsque vous adoptez la même approche pour utiliser la fonctionnalité de licences groupées, vous devez répartir les licences groupées entre différents serveurs de licences ADM. Cette approche ne vous offre pas la flexibilité d'allouer des licences groupées entre vos instances ADC déployées dans le monde entier.

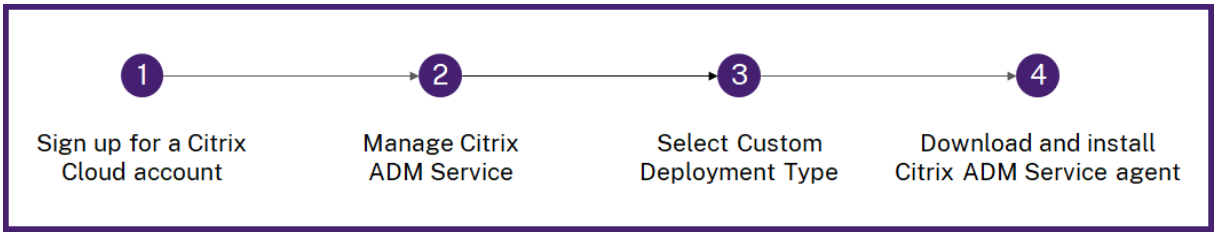
Par conséquent, configurez le service ADM uniquement pour la fonctionnalité de licence groupée. Le service ADM reçoit uniquement les données de licence de toutes les instances ADC. Ainsi, vous pouvez respecter le mandat réglementaire et allouer dynamiquement des licences de capacité groupée entre des instances ADC déployées dans le monde entier.

Ce document explique comment configurer le service ADM uniquement pour la fonctionnalité de licence groupée.

Conditions préalables

Avant de configurer le service ADM uniquement pour la fonctionnalité de licence groupée, effectuez la première intégration et la configuration du service ADM. Assurez-vous d'examiner les spécifications de l'agent dans Configuration système requise.

> **Important**
>
> Lorsque vous embarquez ou configurez le service ADM pour la première fois, assurez-vous que :
>
> - L'option Déploiement personnalisé est sélectionnée.
> - Instances ADC à ajouter une fois que vous avez terminé l'étape 4 procédure de configuration.



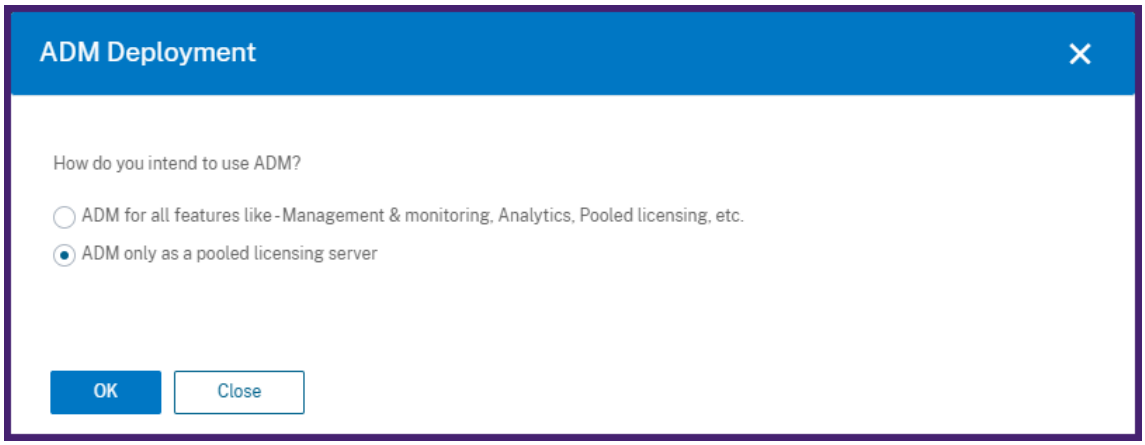
Pour plus d'informations sur l'intégration et la configuration du service ADM, reportez-vous à la section Mise en route.

Après avoir terminé les étapes d'intégration, configurez le service ADM uniquement pour la fonctionnalité de licence groupée.

Comment configurer le service ADM uniquement pour la fonctionnalité de licence groupée

Procédez comme suit pour configurer le service ADM uniquement pour la fonctionnalité de licence :

1. Accédez à **Compte > Administration**.
2. Dans la section **Configurations système**, sélectionnez **Déploiement du système**.
3. Dans le **déploiement ADM**, sélectionnez **ADM uniquement en tant que serveur de licences groupé**.



4. Cliquez sur **OK**.

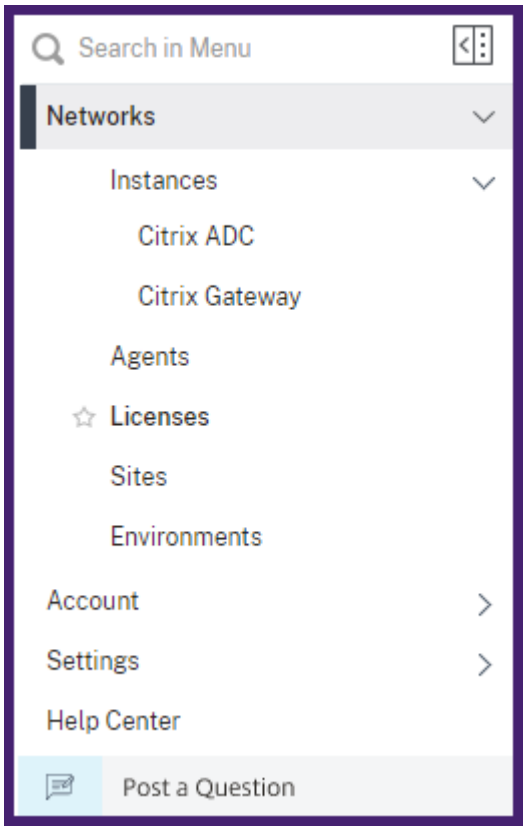
Cette action conserve uniquement la fonctionnalité de licence groupée et désactive les fonctionnalités ADM suivantes :

- Sauvegarde ADM
- Gestion d'événements
- Gestion des certificats SSL
- Rapports sur le réseau
- Fonctions réseau
- Audit de configuration

> **Remarque**
>
> Par défaut, la fonctionnalité d'analyse ADM est désactivée. Assurez-vous de désactiver cette fonctionnalité si vous l'avez activée.

Dans la zone de confirmation, cliquez sur **Oui**.

L'interface graphique ADM affiche désormais uniquement la fonctionnalité de gestion des licences groupées. Et, les entités restantes n'apparaissent pas.



5. Après avoir configuré ADM uniquement pour la fonction de licence, ajoutez des instances ADC dans la page **Réseaux > Instances**.

Remarque

- Vous pouvez également ajouter une instance ADC dans le service ADM et dans d'autres serveurs ADM. Lorsque vous modifiez le mot de passe de telles instances ADC, veillez à mettre à jour le mot de passe sur tous les serveurs ADM où l'instance est découverte. Cette note s'applique lorsque le service ADM est configuré uniquement pour utiliser la fonctionnalité de licence groupée.
- Un utilisateur peut toujours effectuer certaines opérations sur les fonctionnalités désactivées dans l'interface graphique ADM. Par exemple, l'interrogation des événements et la sauvegarde ADC. En tant que super-administrateur, Si vous souhaitez restreindre de telles opérations, désactivez les accès utilisateur pour les autres administrateurs à l'aide d'une stratégie d'accès appropriée. Pour de plus amples informations, consultez la section Configurer les stratégies d'accès sur Citrix ADM.

Appliquer une nouvelle licence à ADM pour une configuration de capacité groupée existante

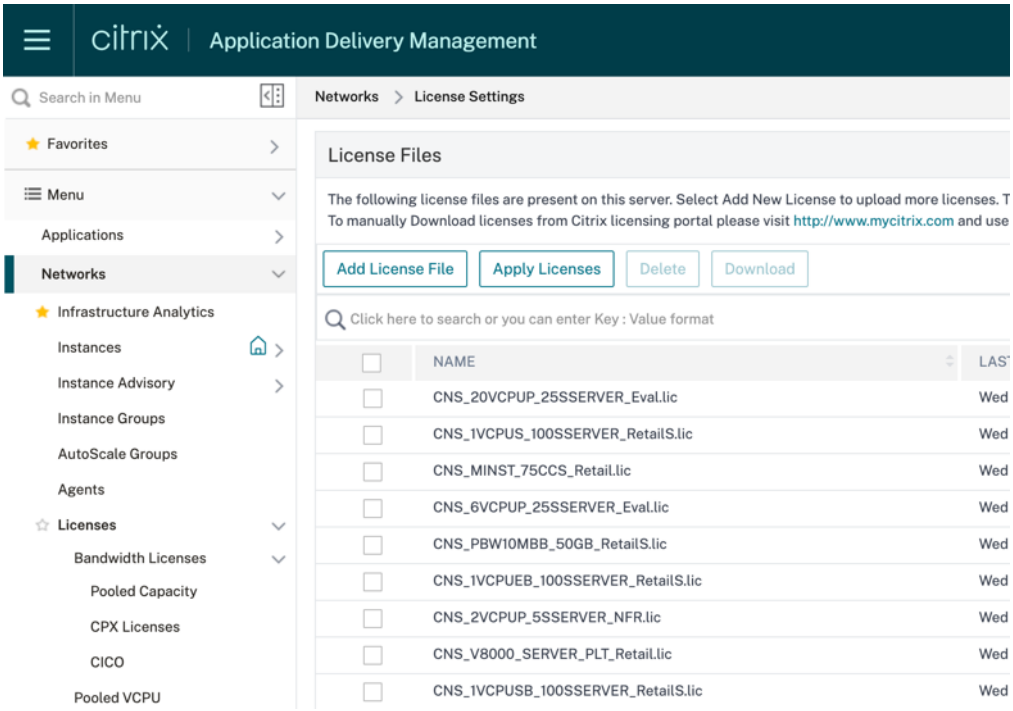
April 29, 2021

Cette rubrique décrit comment appliquer une nouvelle licence sur Citrix ADM pour une configuration de capacité groupée existante. Avant de pouvoir postuler à ADM, vous avez besoin d'un fichier de licence. Si un fichier de licence est déjà présent sur votre ordinateur local, vous pouvez le télécharger sur le serveur de licences ADM. Vous pouvez également utiliser le code d'accès aux licences envoyé par e-mail par Citrix pour allouer des licences à partir du portail de licences Citrix.

Utilisez l'interface graphique **ADM > Réseaux** Licences pour gérer et déployer tous les fichiers de licences de capacité groupée.

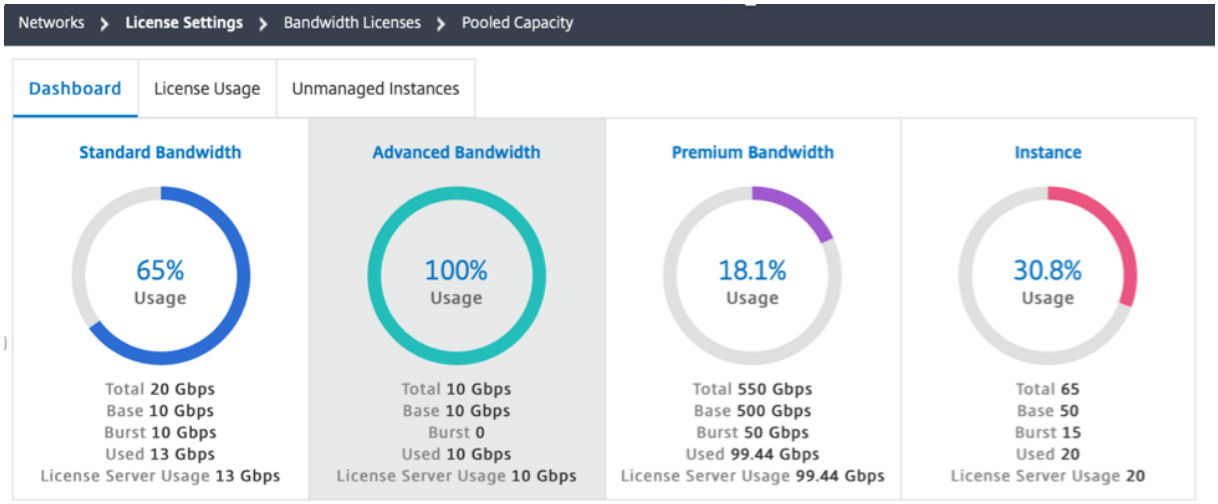
Vérifier l'état des licences et des pools existants

Vous pouvez vérifier les licences disponibles sur ADM en accédant à **Réseaux > Licences**.



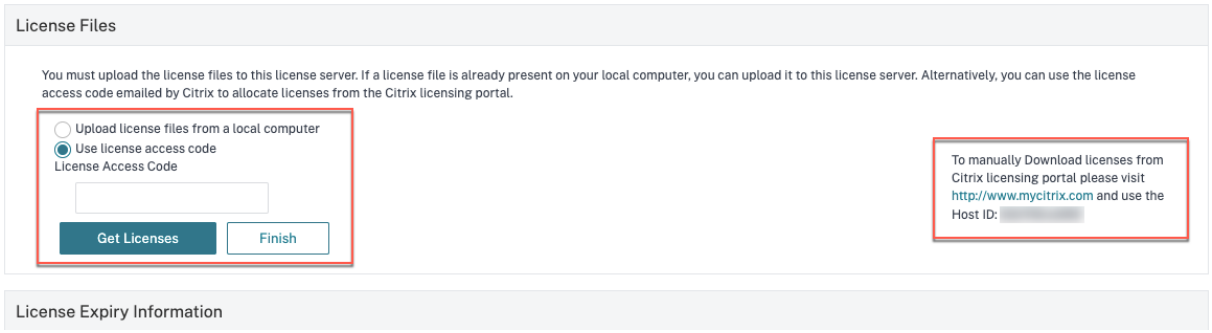
Faites défiler l'écran vers le bas pour afficher les pools de licences disponibles dans le tableau **Informations d'expiration de licence** avec les dates d'expiration.

Pour vérifier les pools disponibles pour différentes éditions, accédez à **Réseaux > Licences > Licences de bande passante > Capacité groupée**



Allouer une nouvelle licence

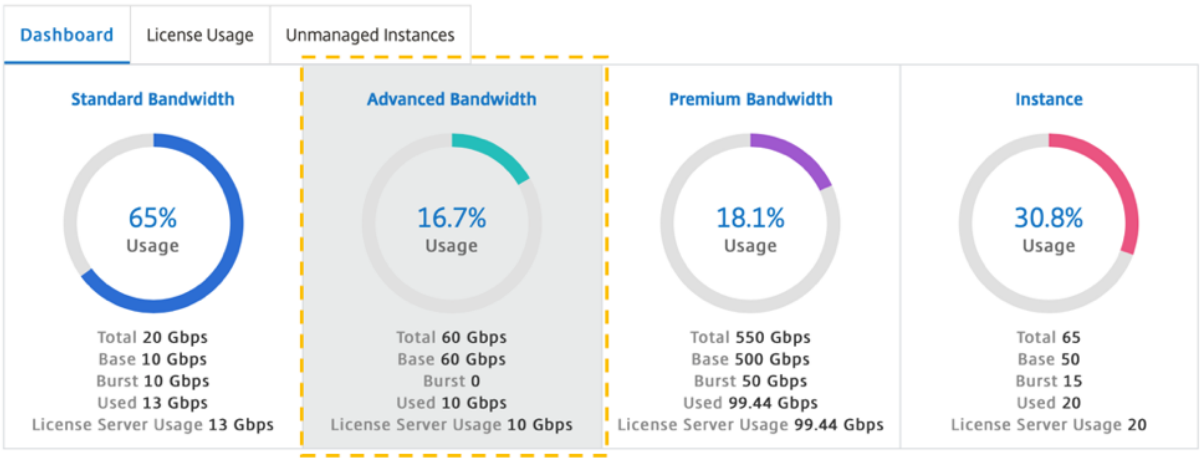
Si vous ne disposez pas d'une licence déjà disponible sur votre ordinateur local, vous pouvez allouer la licence à l'aide du code d'accès fourni par Citrix ou télécharger à partir du portail de licences Citrix à l'aide de l'ID d'hôte indiqué dans l'interface graphique. Pour plus d'informations sur le téléchargement de licences à partir du portail de licences Citrix, consultez l'article de support technique Système de licences Citrix.



Appliquer une nouvelle licence

Procédez comme suit pour appliquer un fichier de licence téléchargé.

1. Accédez à **Réseaux > Licences**, cliquez sur **Ajouter un fichier de licence**.
2. Cliquez sur **Parcourir**, puis téléchargez la nouvelle licence.
3. Cliquez sur **Terminer**. Vous pouvez ajouter d'autres licences à partir de la page Paramètres de licence à tout moment.
4. Une fois la licence ajoutée, le tableau de bord des capacités groupées affiche la nouvelle capacité de disponibilité.



Supprimer une licence

Pour supprimer une licence existante, procédez comme suit.

1. Accédez à **Réseaux -> Licences**.
2. Sélectionnez la licence et cliquez sur **Supprimer** pour supprimer la licence à tout moment.

ADM retire automatiquement la licence demandée pour ADC du nouveau pool disponible.

1. Pour l'ADC sélectionné, pour modifier l'allocation de bande passante, cliquez sur **Allouer** pour modifier le pool sélectionné.

FAQ et autres ressources

April 29, 2021

Cette section répertorie les documentations de référence sur la configuration et l'exploitation des licences groupées. Vous pouvez vous référer à ces documents pour obtenir de l'aide relative aux problèmes de configuration et d'exploitation.

Configuration

1. Où puis-je trouver des informations sur la vue d'ensemble et les fonctionnalités de la capacité groupée ?

   Réponse : Voir Modèle de conception validé de la capacité groupée Citrix ADC.

2. Comment convertir ou migrer perpétuellement vers des licences regroupées et le contraire ?

Réponse : La conversion d'une licence perpétuelle à une licence de capacité groupée est un processus de droits de licence unidirectionnel. Vous ne pouvez pas rétablir la licence de capacité groupée à perpétuel.

3. Comment déployer le serveur ADM ?

   Réponse : Suivez le Mise en route document.

4. Comment ajouter une nouvelle licence à une licence groupée existante et l'allouer ?

   Réponse : Suivez le Appliquer une nouvelle licence à ADM pour une configuration de capacité groupée existante document.

5. Comment allouer/augmenter la capacité et la bande passante sur les instances ?

   Réponse : Suivez le Appliquer une nouvelle licence à ADM pour une configuration de capacité groupée existante document.

Problèmes courants

1. Instances exécutées en mode grâce en raison d'une défaillance de connectivité, de mise à niveau, de séparation du cerveau et d'autres.

   Réponse : Consultez le comportement du serveur de licences ADM documenté à la section Configuration de la capacité groupée Citrix ADC.

2. Les licences ne s'appliquent pas ou ne reflètent pas les instances.

   Réponse : Voir Meilleures pratiques, cas de coin et FAQ.

3. L'allocation de licence est bloquée dans la « synchronisation en cours ».

   Réponse : Voir Meilleures pratiques, cas de coin et FAQ.

4. Erreur due à un ID hôte incorrect sur le fichier de licence.

   Réponse : 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 de plus amples informations, consultez la section Attribuer un nom d'hôte à un serveur Citrix ADM.

5. Problèmes dus à des bogues connus ou corrigés

   Réponse : examiner le Notes de publication, Configuration système requise, et Licences.

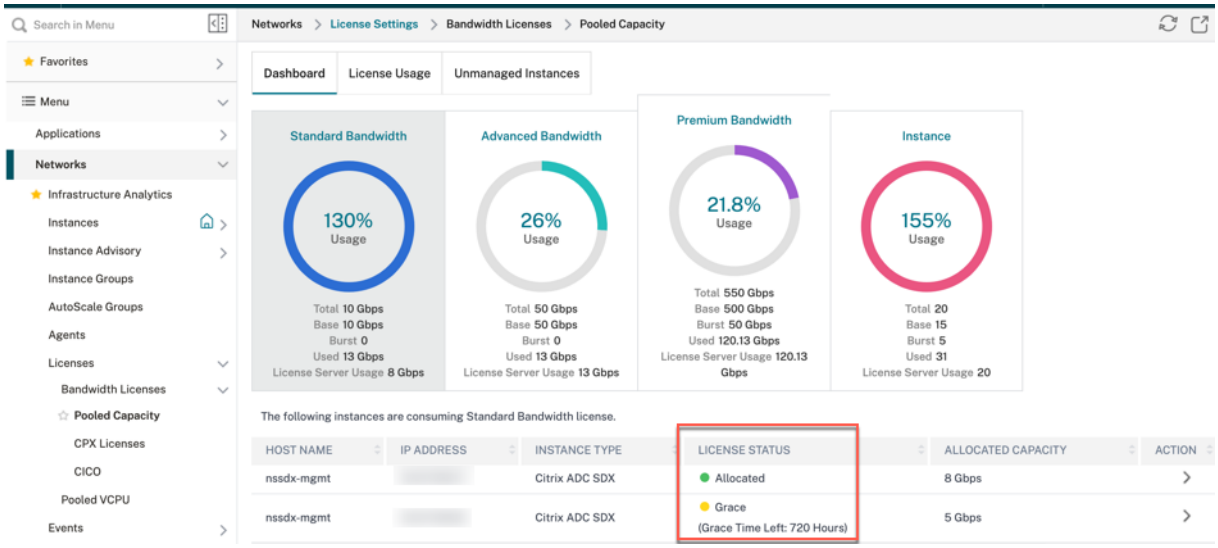
Résoudre les problèmes de licence de capacité groupée

April 29, 2021

Cette section décrit comment analyser et résoudre les problèmes courants de capacité groupée.

Vérifier l'état de la licence

L'ADM agit en tant que serveur de licences pour votre licence de capacité groupée ADC. Vous pouvez utiliser l'interface graphique ADM pour vérifier l'état de la licence. Accédez à **Réseaux > Licences > Capacité groupée > Utilisation des licences**.



Le tableau suivant répertorie les types d'état de licence et leur signification

État	Ce que cela signifie
Attribué	L'état de la licence est bien.
Attribué : non appliqué sur ADC	Citrix ADC peut nécessiter un redémarrage si la licence est retirée ou consignée à partir d'ADC, mais Citrix ADC n'a pas encore redémarré.
Non alloué	La licence n'est pas allouée dans l'instance ADC.
Grace	L'instance Citrix ADC est dans la période de grâce de licence pendant 30 jours
Synchronisation en cours	Citrix ADM récupère les informations de Citrix ADC dans un intervalle de 2 minutes. La synchronisation des licences entre Citrix ADM et Citrix ADC peut prendre jusqu'à 15 minutes. Citrix ADM peut avoir redémarré ou le basculement ADM HAS est déclenché.

État	Ce que cela signifie
Partiellement alloué	Citrix ADC ne peut pas accepter la capacité allouée car elle peut s'exécuter à son allocation maximale. Par exemple, Citrix ADC fonctionne avec une capacité de pool de licences de 10 Gbit/s. Lorsque l'ADC redémarre, les 10 Gbit/s sont consignés sur le serveur de licences ADM. Lorsque Citrix ADC revient en ligne, il essaie de récupérer automatiquement les 10 Gbit/s alloués précédemment. Pendant ce temps, d'autres instances ADC peuvent avoir récupéré cette bande passante. Partiellement alloué apparaît si le pool de licences ne dispose pas d'une capacité suffisante pour allouer 10 Gbit/s ou même une capacité partielle à cet ADC.
Non géré	Citrix ADC n'est pas ajouté à ADM pour plus de facilité de gestion. Cela n'a pas d'impact sur les licences Citrix ADC, mais cela peut avoir un impact sur la surveillance des licences d'ADM.
Non géré	Citrix ADC n'est pas ajouté à ADM pour plus de facilité de gestion. Cela n'a pas d'impact sur les licences Citrix ADC, mais cela peut avoir un impact sur la surveillance des licences d'ADM.
Connexion perdue	Citrix ADC n'est pas accessible à partir d'ADM pour sa facilité de gestion. Par exemple, il existe des problèmes de connectivité réseau, NITRO ne fonctionne pas ou des incohérences de mot de passe Citrix ADC. Si NITRO ne fonctionne pas ou si le mot de passe de Citrix ADC ne correspond pas, cela n'a pas d'impact sur les licences Citrix ADC. Cependant, cela peut avoir un impact sur la surveillance des licences d'ADM.

Vérifier l'état du serveur

Cette section décrit les problèmes courants d'état du serveur ainsi que les raisons et les correctifs possibles.

Problème : ADC affiche le serveur de licences comme inaccessible et l'état de la licence change en grâce.

- La connexion au serveur de licences (ADM ou ADM Service Agent) a été interrompue pendant plus de 15 minutes. Vérifiez si le serveur de licences est disponible et accessible.
- ADC est en mode grâce.

Problème : ADC affiche l'état du serveur de licences comme accessible, mais la tentative de modification de l'allocation par l'utilisateur n'a aucun effet. Cliquez sur **Modifier l'allocation** renvoie 0 0. Cette valeur peut faire apparaître que la capacité configurée a été perdue.

- La connexion au serveur de licences a récemment cessé, mais ADC n'a toujours pas manqué le second rythme cardiaque. Par conséquent, il n'est pas dans Grace (encore). Vérifiez si le serveur de licences est disponible et accessible.

Problème : ADC affiche le nombre de capacités et d'instances, mais le serveur **de licences est atteignable/inaccessible**. Si vous cliquez sur **Modifier l'allocation**, vous renvoie certains nombres mais ne tient pas compte de la capacité configurée.

- La connexion au serveur de licences a été restaurée mais l'ADC doit toujours manquer le second rythme cardiaque ou envoyer la sonde de reconnexion.

Problème : ADC indique Impossible de se connecter au serveur de licences lors de la configuration des licences groupées avec le service ADM

- Vérifiez les règles de pare-feu pour vous assurer que les ports 27000 et 7279 sont ouverts.
- L'agent n'est pas enregistré. Pour de plus amples informations, consultez la section Mise en route.
- Le service ADM n'a pas de fichiers de licence téléchargés. Pour de plus amples informations, consultez Configurer la capacité du pool de Citrix ADC
- ADM a les fichiers de licence incorrects.

Vérifier le rapport d'utilisation de la licence

Sous **Réseaux > Licences > Capacité groupée > Utilisation des licences** dans l'interface graphique ADM, vous pouvez voir le pic mensuel d'utilisation de votre licence. Vous pouvez utiliser ce rapport pour augmenter l'utilisation de votre licence ou planifier l'achat d'une licence supplémentaire.

Voici quelques détails sur la façon dont le rapport est généré et peut être utilisé.

Sondage : les données de licence sont interrogées à partir des instances ADC toutes les 15 minutes.

Maintien des pics par heure : ADM ne conserve qu'une utilisation maximale de licence en une heure, par appareil.

Reporting : vous pouvez générer un rapport GUI pour chaque instance, pour une période spécifique.

Exportation : Vous pouvez exporter des rapports au format CSV ou XLS.

Purger : ADM purge les données le premier jour de chaque mois à 12 h 10. La période de purge est configurable (la période par défaut est de deux mois).

Compteurs et statistiques pour les licences de capacité groupée

Les compteurs, journaux et commandes suivants exposent les mesures de licences groupées Citrix ADC qui indiquent le comportement des instances ADM et ADC en mode de licence groupée.

- **Pièges SNMP** : disponible à partir de la version 13.xx de l'ADC.
- **Compteurs NSCONMSG pour la limitation de débit** : disponible à partir de la version 12.1 57.xx de l'ADC.
- **Compteurs ADM** Actions de commande ADM sont disponibles dans Citrix ADC Cloud Service.

interruptions SNMP

Vous pouvez configurer les alarmes de licence groupées des interruptions SNMP suivantes v.13

- `POOLED-LICENSE-CHECKOUT-FAILURE`
- `POOLED-LICENSE-ONGRACE`
- `Configure POOLED-LICENSE-PARTIAL`

Pour plus d'informations sur ces alarmes, reportez-vous à la section Référence OID SNMP Citrix ADC.

Compteur NSCONMSG

Vérifiez les `NCCONMSG` compteurs suivants et ce qu'ils signifient :

- `allnic_err_rl_cpu_pkt_drops` : les paquets agrégats (toutes les cartes réseau) diminuent après que la limite du processeur a été atteinte
- `allnic_err_rl_pps_pkt_drops` : les paquets agrégés tombent à l'échelle du système après la limite pps
- `allnic_err_rl_rate_pkt_drops` : taux d'agrégation baisse à l'échelle du système
- `allnic_err_rl_pkt_drops` : baisse cumulée de limitation de débit due au débit, pps et CPU
- `rl_tot_ssl_rl_enforced` : nombre de fois où SSL RL a été appliqué (sur les nouvelles connexions SSL)
- `rl_tot_ssl_rl_data_limited` : nombre de fois où la limite de débit SSL a été atteinte
- `rl_tot_ssl_rl_sess_limited` : nombre de fois que la limite SSL TPS a été atteinte

Compteurs ADM

Lorsque vous choisissez l' **action d'événement Exécuter une action de commande**, vous pouvez créer une commande ou un script qui peut être exécuté sur Citrix ADM pour les événements correspondant à un critère de filtre particulier.
Vous pouvez également définir les paramètres suivants pour le script **Exécuter l'action de commande** :

Paramètre	Description
$source	Ce paramètre correspond à l'adresse IP source de l'événement reçu.
Catégorie $	Ce paramètre correspond au type de pièges défini sous la catégorie du filtre.
$entité	Ce paramètre correspond aux instances d'entité ou aux compteurs pour lesquels un événement a été généré. Il peut inclure les noms de compteurs pour tous les événements liés au seuil, les noms d'entités pour tous les événements liés à l'entité et les noms de certificats pour tous les événements liés au certificat.
$sévérité	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 exactement le problème tel qu'il a été notifié. Cela peut être utilisé pour localiser rapidement les problèmes et identifier la raison de l'échec, au lieu de simplement signaler les événements bruts.

> **Remarque**
>
> Pendant l'exécution de la commande, ces paramètres sont remplacés par des valeurs réelles.

Licences d'enregistrement et de sortie Citrix ADC VPX

April 29, 2021

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'un cadre de licences qui fournit un Provisioning de 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.

Installer des licences dans Citrix ADM

Pour installer des fichiers de licence sur Citrix ADM :

1. Accédez à **Réseaux** > **Licences**, puis cliquez sur **Ajouter un fichier de licence** .
2. Dans la section Fichiers de licence, sélectionnez l'une des options suivantes :
   - Télécharger des fichiers de licence à partir d'un ordinateur local - Si un fichier de licence est déjà présent sur votre ordinateur local, vous pouvez le télécharger sur Citrix ADM.

   Pour ajouter des fichiers de licence, cliquez sur Parcourir et sélectionnez le fichier de licence (.lic) à ajouter. Cliquez ensuite sur Terminer.
   - Utiliser le code d'accès aux licences - Citrix envoie par e-mail le code d'accès à la licence pour les licences que vous achetez.

   Pour ajouter des fichiers de licence, entrez le code d'accès à la licence dans la zone de texte, puis cliquez sur Obtenir des licences.

   > **Remarque**
   >
   > Assurez-vous d'être connecté à Internet avant d'utiliser le code d'accès à la licence pour installer les licences.

Vérification

Vous pouvez afficher les licences disponibles et allouées dans Citrix ADM.

Pour afficher les licences

1. Accédez à **Réseaux** > **Licence > Licences** de **bande passante > LicencesVPX** .

   Vous pouvez afficher les licences allouées dans le tableau sous la section Licences disponibles.

Allouer une licence VPX à une instance Citrix ADC VPX à l'aide de l'interface graphique ADC

1. Connectez-vous à l'instance Citrix ADC VPX et accédez à **Système > Licences > Gérer les licences**, cliquez sur **Ajouter une nouvelle licence**, puis sélectionnez **Utiliser les licences à distance**.
2. Entrez les détails du serveur de licences dans le champ **Nom du serveur/Adresse IP**.

   > Remarque
   >
   > Si vous souhaitez gérer les licences VPX de votre instance via Citrix ADM, activez la case à cocher **Enregistrer avec NetScaler MA Service** et entrez les informations d'identification Citrix ADM.

3. Cliquez sur **Continue**.
4. Dans la fenêtre **Allouer des licences**, sélectionnez le type de licence. La fenêtre affiche le total et les CPU virtuels disponibles ainsi que les CPU pouvant être alloués. Cliquez sur **Obtenir les licences**.
5. 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 édition Standard sur votre instance. Vous pouvez libérer cette licence, puis vérifier à partir de Advanced Edition.

6. Vous pouvez modifier ou libérer l'allocation de licence en accédant à **Système** > **Licences** > **Gérer les licences**, puis en sélectionnant **Modifier l'allocation** ou **Libérer l'allocation** .
7. Si vous cliquez sur **Modifier l'allocation**, une fenêtre contextuelle affiche les licences disponibles sur le serveur de licences. Sélectionnez la licence requise, cliquez sur **Obtenir des licences**.

Allouer une licence VPX à une instance Citrix ADC VPX à l'aide de l'interface de ligne de commande ADC

1. Dans un client SSH, entrez l'adresse IP de l'instance Citrix ADC et ouvrez une session à l'aide des informations d'identification de l'administrateur.

2. Pour ajouter un serveur de licences, entrez la commande suivante :

```
add ns licenseserver (<licenseServerIP> | <serverName>) [-port <
   port number >]
<!--NeedCopy-->
```

```
> add ns licenseserver 10.102.29.97 -port 27000
 Done
```

3. Pour afficher les licences disponibles sur le serveur de licences, entrez la commande suivante :

```
sh licenseserverpool
<!--NeedCopy-->
```

```
> sh licenseserverpool
        Instance Total                  : 0
        Instance Available              : 0
        Standard Bandwidth Total        : 0 Mbps
        Standard Bandwidth Availabe     : 0 Mbps
        Enterprise Bandwidth Total      : 0 Mbps
        Enterprise Bandwidth Available  : 0 Mbps
        Platinum Bandwidth Total        : 0 Mbps
        Platinum Bandwidth Available    : 0 Mbps
        VPX25S Total                    : 1
        VPX25S Available                : 1
        VPX200E Total                   : 1
        VPX200E Available               : 1
        VPX1000S Total                  : 1
        VPX1000S Available              : 1
        VPX8000E Total                  : 2
        VPX8000E Available              : 1
 Done
```

4. Pour attribuer une licence à une instance VPX, entrez la commande suivante :

```
set capacity  - platform V[S/E/P][Bandwidth]
<!--NeedCopy-->
```

```
> set capacity -platform VE8000
Warning: The configuration changes will not take effect until the system is rebooted
```


Configurer les vérifications d'expiration pour les licences Citrix ADC VPX de check-in/check-out

Vous pouvez maintenant 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 affiché sur Citrix ADM.

Pour configurer les vérifications d'expiration des licences

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 :
    - Caractéristique : Type de licence qui va expirer.
    - Nombre : nombre de serveurs virtuels ou d'instances affectés.
    - Jours d'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 la capacité de licences groupées à utiliser pour avertir les administrateurs.
4. Sélectionnez le type de notification que vous souhaitez envoyer en cochant la case appropriée. Les types de notification sont les suivants :
    - Profil de messagerie : spécifiez un serveur de messagerie et des détails de profil. Un e-mail est déclenché lorsque vos licences sont sur le point d'expirer.
    - Profil SMS : Spécifiez un serveur SMS (Short Message Service) et les détails du profil. Un message SMS est déclenché lorsque vos licences sont sur le point d'expirer.
    - Profil Slack : spécifiez un canal de marge. Une notification est envoyée lorsque vos licences sont sur le point d'expirer.
5. Indiquez ensuite le nombre de jours avant l'expiration de la licence pendant lesquels vous souhaitez commencer à recevoir la notification.
6. Cliquez sur **Enregistrer**.

Licences de processeur virtuel Citrix ADC

April 29, 2021

Les administrateurs de datacenter comme vous optent pour des technologies plus récentes qui simplifient les fonctions réseau tout en offrant des coûts réduits et une plus grande évolutivité. L'architecture de datacenter plus récente doit inclure les fonctionnalités suivantes dans les moindres :

- Réseau défini par logiciel (SDN)
- Virtualisation des fonctions réseau (NFV)
- Virtualisation réseau (NV)
- Micro-services

Un tel mouvement a également besoin 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 allouées en fonction de la consommation de bande passante par les instances. Un Citrix ADC VPX est limité à utiliser une bande passante spécifique et d'autres mesures de performances basées sur l'édition de licence à laquelle il est lié. Pour augmenter la bande passante disponible, vous devez effectuer une mise à niveau vers une édition de licence offrant plus de bande passante. Dans certains scénarios, la bande passante requise peut être inférieure, mais elle est plus requise pour d'autres performances L7 telles que SSL TPS, 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 Application Delivery Management (ADM) prend désormais en charge l'attribution de licences à l'instance Citrix ADC en fonction des exigences du processeur virtuel.

Dans la fonctionnalité de licence basée sur l'utilisation du processeur virtuel, la licence spécifie le nombre de processeurs auxquels un Citrix ADC VPX particulier a droit. Ainsi, le Citrix ADC VPX peut extraire des licences uniquement pour le nombre de processeurs virtuels s'exécutant sur celui-ci à partir du serveur de licences. Citrix ADC VPX vérifie les licences en fonction du nombre de processeurs en cours d'exécution dans le système. Citrix ADC VPX ne prend pas en compte les processeurs inactifs lors de l'extraction des licences.À l'
instar de la capacité de licence groupée et des 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 CPU virtuelles sont standard, Advanced et Premium. Ces éditions débloquent 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 lorsqu'il y a un changement dans l'édition de la licence. Dans ce cas, vous devez toujours arrêter l'instance avant de lancer une demande pour un nouvel ensemble de licences. Redémarrez le Citrix ADC VPX après avoir retiré les licences.

Pour configurer le serveur de licences dans Citrix ADC VPX à l'aide de l'interface graphique

1. Dans Citrix ADC VPX, accédez à **Système** > **Licences** et cliquez sur **Gérer les licences** .
2. Sur la page **Licence**, cliquez sur **Ajouter une nouvelle licence** .
3. Dans la page **Licences**, sélectionnez l'option **Utiliser les licences à distance** .
4. Sélectionnez **Licences CPU** dans la liste **Mode de licence à distance** .
5. Tapez l'adresse IP du serveur de licences et le numéro de port.
6. Cliquez sur **Continue**.

   > **Remarque**
   >
   > Enregistrez toujours l'instance Citrix ADC VPX auprès de Citrix ADM. Si ce n'est pas déjà fait, activez l'option Enregistrer avec Citrix ADM et tapez les informations d'identification de connexion Citrix ADM.

7. Dans la fenêtre **Allouer des licences**, sélectionnez le type de licence. La fenêtre affiche le total et les CPU virtuels disponibles ainsi que les CPU pouvant être alloués. Cliquez sur **Obtenir les licences**.

   > **Remarque**
   >
   > Pour une paire ADC HA, allouez des licences CPU virtuelles à chaque nœud séparément.

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 la licence Standard Edition sur votre instance. Vous pouvez libérer cette licence, puis extraire à partir de l'édition Advanced.

Paramètres de l'instance

April 29, 2021

Vous pouvez gérer les instances découvertes dans le service Citrix ADM et configurer les paramètres de sauvegarde d'instance.

Gérer la configuration de l'instance

Dans **Instance Management**, vous pouvez modifier les configurations d'instance suivantes :

- **Communication avec les instances** : vous pouvez choisir un canal de communication HTTP ou HTTPS entre le service Citrix ADM et les instances découvertes.
- **Activer le téléchargement de certificats** - Permet de télécharger les certificats SSL à partir d'une instance découverte.
- **Invite les informations d'identification pour la connexion** à l'instance : lorsque vous accédez à l'instance via l'interface graphique Citrix ADM, la page de connexion de l'instance apparaît. Spécifiez vos informations d'identification pour accéder à une instance.

Configurer les paramètres de sauvegarde d'instance

Dans **Paramètres de sauvegarde d'instance**, vous pouvez configurer les paramètres de sauvegarde pour les instances ADC découvertes dans Citrix ADM.

Dans **Configurer les paramètres de sauvegarde d'instance**, sélectionnez **Activer les sauvegardes d'instance**.

- **Paramètres de sécurité de sauvegarde** - Chiffrez le fichier de sauvegarde pour vous assurer que toutes les informations sensibles contenues dans le fichier de sauvegarde sont sécurisées. Sélectionnez le **fichier de protection par mot** de passe pour chiffrer le fichier de sauvegarde.

  > **Remarque**
  >
  > Lorsque vous téléchargez le fichier de sauvegarde chiffré, le fichier ne s'ouvre pas dans l'interface graphique Citrix ADM ou dans un éditeur de texte. Ce fichier peut être récupéré et utilisé uniquement par Citrix ADM. Toutefois, vous pouvez ouvrir un fichier de sauvegarde non chiffré sur votre système.
  >
  > Pour restaurer le fichier de sauvegarde chiffré, spécifiez le mot de passe que vous avez mentionné pour chiffrer le fichier de sauvegarde.

- **Paramètres de planification des sauvegardes**- Vous pouvez planifier une sauvegarde d'instance de deux manières :
  - **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 : spécifiez l'heure au `hours:minutes` format à laquelle Citrix ADM doit effectuer la sauvegarde de l'instance.

- **Paramètres Citrix ADC** - Avec cette option, vous pouvez lancer une sauvegarde en fonction de l'interruption et inclure des fichiers GeoDB avec la sauvegarde. Ce paramètre s'applique aux instances MPX, VPX, CPX et BLX.
  - **Effectuez une sauvegarde d'instance lorsque l'interruption NetScalerConfigSave est reçue** - Par défaut, Citrix ADM ne crée pas de fichier de sauvegarde lorsqu'il reçoit l'interruption « NetScalerConfigSave ». Toutefois, vous pouvez activer l'option de créer un fichier de sauvegarde chaque fois qu'une instance Citrix ADC envoie une `NetScalerConfigSave` interruption à Citrix ADM.

    Une instance Citrix ADC envoie `NetScalerConfigSave` chaque fois que la configuration sur l'instance est enregistrée.

    Spécifiez **Sauvegarde sur le délai d'interruptions** en minutes. Si l'interruption `NetScalerConfigSave` reçue persiste pendant les minutes spécifiées sur Citrix ADM, Citrix ADM sauvegarde l'instance.
  - **Inclure les fichiers GeoDB** - Par défaut, Citrix ADM ne sauvegarde pas les fichiers de géoDatabase. Vous pouvez également activer l'option pour créer une sauvegarde de ces fichiers.
- **Paramètres Citrix SDX** : pour sauvegarder des instances SDX, spécifiez le délai d'**expiration de la sauvegarde** en minutes. Lors d'une sauvegarde d'instance SDX, la connexion entre ADM et SDX est maintenue pendant la période spécifiée.

  Si la taille du fichier de sauvegarde de l'instance SDX est grande, vous pouvez conserver la connexion entre ADM et l'instance SDX pendant une période plus longue afin de terminer la sauvegarde de l'instance SDX.

  > **Important**
  >
  > La sauvegarde échoue si la connexion est épuisée.
- **Transfert externe** - Citrix ADM vous permet de transférer les fichiers de sauvegarde d'instance Citrix ADC vers un emplacement externe :
  1. Spécifiez l'adresse IP de l'emplacement.
  2. Spécifiez le nom d'utilisateur et le mot de passe du serveur externe vers lequel vous souhaitez transférer les fichiers de sauvegarde.
  3. Spécifiez le protocole de transfert et le numéro de port.
  4. Spécifiez le chemin d'accès au répertoire où le fichier doit être stocké.
  5. Si vous souhaitez supprimer le fichier de sauvegarde après avoir transféré le fichier vers un serveur externe, sélectionnez **Supprimer le fichier depuis Application Delivery Management après le transfert**.

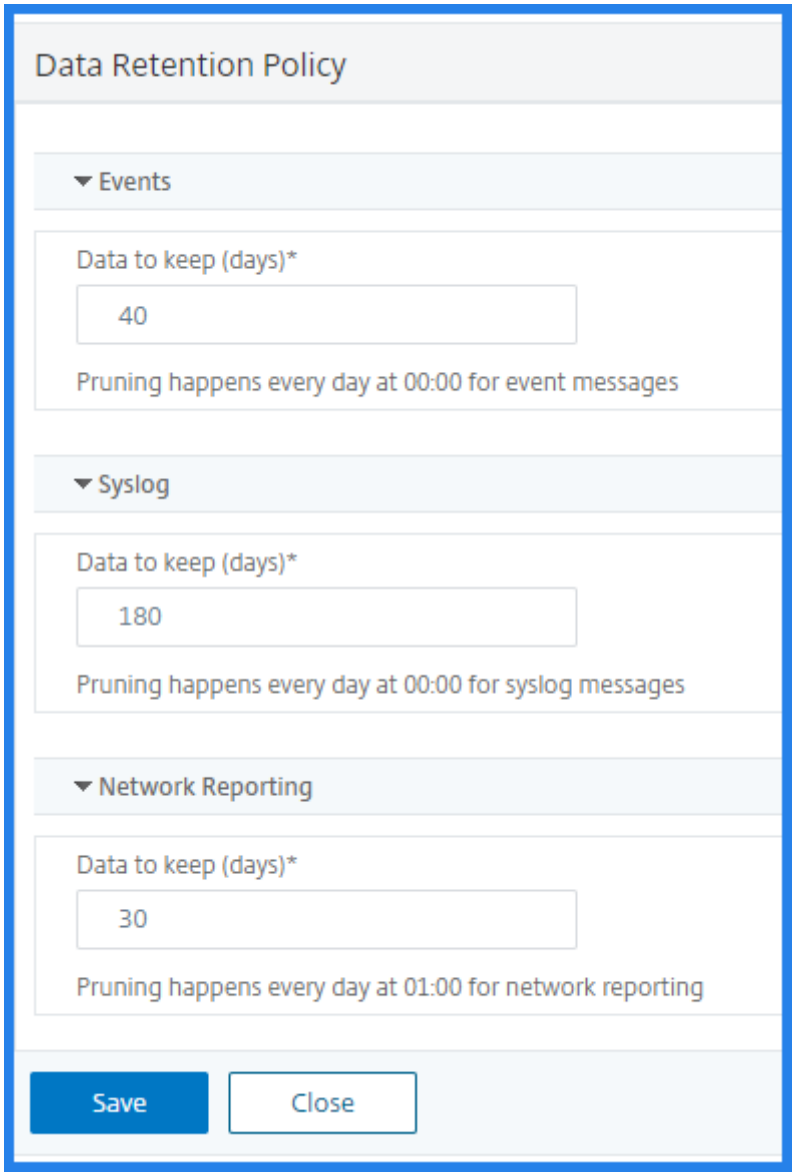
Stratégie de rétention des données

April 29, 2021

Vous pouvez accéder aux événements système, aux messages syslog et aux données de rapport réseau pendant une durée spécifique dans le service ADM.

1. Accédez à **Paramètres > Stratégie de rétention des données** pour configurer la rétention des données.
2. Cliquez sur le bouton Modifier.
3. Spécifiez les jours pour les options suivantes pour conserver les données dans le service ADM :

Options	Description
Événements	Permet de limiter les messages d'événement stockés dans le service ADM jusqu'à 40 jours. Les événements sont supprimés d'ADM après l'expiration de la stratégie de rétention. Les événements effacés sont supprimés après un jour. Pour de plus amples informations, consultez la section Événements.
Syslog	Permet de limiter la quantité de données syslog stockées dans la base de données jusqu'à 180 jours. Pour de plus amples informations, consultez la section Configurer syslog sur les instances.
Rapports réseau	Vous permet de limiter les données de reporting réseau stockées dans Citrix ADM jusqu'à 30 jours. Pour de plus amples informations, consultez la section Rapports réseau.



Important

Vous ne pouvez pas modifier la stratégie de rétention des données avec un compte Express.

Lorsque votre compte est converti en compte Express, le service ADM conserve les données de stockage jusqu'à 500 Mo ou les données d'un jour, selon la moindre des deux éventualités. Pour de plus amples informations, consultez la section Gérer les ressources Citrix ADM à l'aide du compte Express.

Paramètres de l'instance

April 29, 2021

Vous pouvez gérer les instances découvertes dans le service Citrix ADM et configurer les paramètres de sauvegarde d'instance.

Gérer la configuration de l'instance

Dans **Instance Management**, vous pouvez modifier les configurations d'instance suivantes :

- **Communication avec les instances** : vous pouvez choisir un canal de communication HTTP ou HTTPS entre le service Citrix ADM et les instances découvertes.
- **Activer le téléchargement de certificats** - Permet de télécharger les certificats SSL à partir d'une instance découverte.
- **Invite les informations d'identification pour la connexion** à l'instance : lorsque vous accédez à l'instance via l'interface graphique Citrix ADM, la page de connexion de l'instance apparaît. Spécifiez vos informations d'identification pour accéder à une instance.

Configurer les paramètres de sauvegarde d'instance

Dans **Paramètres de sauvegarde d'instance**, vous pouvez configurer les paramètres de sauvegarde pour les instances ADC découvertes dans Citrix ADM.

Dans **Configurer les paramètres de sauvegarde d'instance**, sélectionnez **Activer les sauvegardes d'instance**.

- **Paramètres de sécurité de sauvegarde** - Chiffrez le fichier de sauvegarde pour vous assurer que toutes les informations sensibles contenues dans le fichier de sauvegarde sont sécurisées. Sélectionnez le **fichier de protection par mot** de passe pour chiffrer le fichier de sauvegarde.

  > **Remarque**
  >
  > Lorsque vous téléchargez le fichier de sauvegarde chiffré, le fichier ne s'ouvre pas dans l'interface graphique Citrix ADM ou dans un éditeur de texte. Ce fichier peut être récupéré et utilisé uniquement par Citrix ADM. Toutefois, vous pouvez ouvrir un fichier de sauvegarde non chiffré sur votre système.
  >
  > Pour restaurer le fichier de sauvegarde chiffré, spécifiez le mot de passe que vous avez mentionné pour chiffrer le fichier de sauvegarde.

- **Paramètres de planification des sauvegardes**- Vous pouvez planifier une sauvegarde d'instance de deux manières :
  - **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 : spécifiez l'heure au `hours:minutes` format à laquelle Citrix ADM doit effectuer la sauvegarde de l'instance.

- **Paramètres Citrix ADC** - Avec cette option, vous pouvez lancer une sauvegarde en fonction de l'interruption et inclure des fichiers GeoDB avec la sauvegarde. Ce paramètre s'applique aux instances MPX, VPX, CPX et BLX.
  - **Effectuez une sauvegarde d'instance lorsque l'interruption NetScalerConfigSave est reçue** - Par défaut, Citrix ADM ne crée pas de fichier de sauvegarde lorsqu'il reçoit l'interruption « NetScalerConfigSave ». Toutefois, vous pouvez activer l'option de créer un fichier de sauvegarde chaque fois qu'une instance Citrix ADC envoie une `NetScalerConfigSave` interruption à Citrix ADM.

    Une instance Citrix ADC envoie `NetScalerConfigSave` chaque fois que la configuration sur l'instance est enregistrée.

    Spécifiez **Sauvegarde sur le délai d'interruptions** en minutes. Si l'interruption `NetScalerConfigSave` reçue persiste pendant les minutes spécifiées sur Citrix ADM, Citrix ADM sauvegarde l'instance.
  - **Inclure les fichiers GeoDB** - Par défaut, Citrix ADM ne sauvegarde pas les fichiers de géoDatabase. Vous pouvez également activer l'option pour créer une sauvegarde de ces fichiers.
- **Paramètres Citrix SDX** : pour sauvegarder des instances SDX, spécifiez le délai d'**expiration de la sauvegarde** en minutes. Lors d'une sauvegarde d'instance SDX, la connexion entre ADM et SDX est maintenue pendant la période spécifiée.

  Si la taille du fichier de sauvegarde de l'instance SDX est grande, vous pouvez conserver la connexion entre ADM et l'instance SDX pendant une période plus longue afin de terminer la sauvegarde de l'instance SDX.

  > **Important**
  >
  > La sauvegarde échoue si la connexion est épuisée.
- **Transfert externe** - Citrix ADM vous permet de transférer les fichiers de sauvegarde d'instance Citrix ADC vers un emplacement externe :
  1. Spécifiez l'adresse IP de l'emplacement.
  2. Spécifiez le nom d'utilisateur et le mot de passe du serveur externe vers lequel vous souhaitez transférer les fichiers de sauvegarde.
  3. Spécifiez le protocole de transfert et le numéro de port.
  4. Spécifiez le chemin d'accès au répertoire où le fichier doit être stocké.
  5. Si vous souhaitez supprimer le fichier de sauvegarde après avoir transféré le fichier vers un serveur externe, sélectionnez **Supprimer le fichier depuis Application Delivery Management après le transfert**.

Configurations système

April 29, 2021

Vous pouvez modifier l'intervalle de préservation de l'agent ADM et le fuseau horaire du serveur Citrix ADM.

Définir l'intervalle de garder en vie de l'agent

Le serveur et l'agent Citrix ADM maintiennent la même connexion TCP pour l'intervalle de conservation spécifié. Un agent utilise cette connexion pour envoyer les données des instances gérées au serveur ADM.

1. Accédez à **Paramètres > Paramètres système**.
2. Sélectionnez **Agent et fuseau horaire** sous **Configurations système**.
3. Dans **Agent**, spécifiez l'intervalle de durée entre 30 et 120 secondes.
4. Cliquez sur **Enregistrer**.

Définir le fuseau horaire Citrix ADM

Vous pouvez choisir le fuseau horaire dans lequel vous souhaitez afficher l'heure sur la page Web ADM, les notifications et les rapports.

1. Accédez à **Paramètres > Paramètres système**.
2. Sélectionnez **Agent et fuseau horaire** sous **Configurations système**.
3. Dans **Fuseau horaire**, sélectionnez le fuseau horaire local ou GMT pour afficher l'heure dans ADM.
4. Cliquez sur **Enregistrer**.

Activer ou désactiver les fonctionnalités ADM

April 29, 2021

En tant qu'administrateur, vous pouvez activer ou désactiver les fonctionnalités suivantes dans la page **Paramètres système > Fonctionnalités configurables** :

- **Basculement** de l'agent : le basculement de l'agent peut se produire sur un site qui a deux agents actifs ou plus. Lorsqu'un agent devient inactif (état DOWN) sur le site, le service Citrix

ADM redistribue les instances ADC de l'agent inactif avec d'autres agents actifs. Pour de plus amples informations, consultez la section Configurer les agents Citrix ADM pour un déploiement multisite.

- **Fonction de réseau d'interrogation** d'entité - Une entité est une stratégie, un serveur virtuel, un service ou une action attachée à une instance ADC. Par défaut, Citrix ADM interroge automatiquement les entités de fonction réseau configurées toutes les 60 minutes. Pour de plus amples informations, consultez la section Vue d'ensemble des sondages.
- **Sauvegarde d'instance - Sauvegardez** l'état actuel d'une instance Citrix ADC et utilisez ultérieurement les fichiers sauvegardés pour restaurer l'instance ADC dans le même état. Pour de plus amples informations, consultez la section Sauvegarde et restauration des instances de Citrix ADC.
- **Audit de configuration d'instance** : surveillez les modifications de configuration sur les instances Citrix ADC gérées, résolvez les erreurs de configuration et récupérez les configurations non enregistrées. Pour de plus amples informations, consultez la section Créer des modèles d'audit.
- **Événements d'instance** - Les événements représentent des occurrences d'événements ou d'erreurs sur une instance Citrix ADC gérée. Les événements reçus dans Citrix ADM sont affichés sur la page **Récapitulatif des événements** (**Réseaux > Événements**). Et tous les événements actifs sont affichés dans la page Messages d'événement (**Réseaux > Événements > Messages d'événement**). Pour de plus amples informations, consultez la section Événements.
- **Rapports réseau d'instance** : vous pouvez générer des rapports pour les instances à un niveau global. Aussi, pour les entités telles que les serveurs virtuels et les interfaces réseau. Pour de plus amples informations, consultez la section Rapports réseau.
- **Certificats SSL d'instance** - Citrix ADM fournit une vue centralisée des certificats SSL installés sur toutes les instances Citrix ADC gérées. Pour de plus amples informations, consultez la section Tableau de bord SSL.
- **Instance Syslog** - Vous pouvez surveiller les événements syslog générés sur vos instances Citrix ADC si vous avez configuré votre appareil pour rediriger tous les messages syslog vers Citrix ADM. Pour de plus amples informations, consultez la section Configuration de syslog sur les instances.

Pour activer une fonctionnalité, effectuez les opérations suivantes :

1. Sélectionnez l'entité dans la liste que vous souhaitez activer.
2. Cliquez sur **Activer**.

> **Important**
>
> Si une fonction est désactivée, l'utilisateur ne peut pas effectuer les opérations associées à cette fonctionnalité.

Gestion et surveillance des instances HAProxy

April 29, 2021

Citrix Application Delivery Management (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, il détecte les instances HAProxy sur l'hôte et vous permet de les gérer et de les surveiller. Citrix ADM vous présente les types d'informations suivants sur la configuration HAProxy sur les instances :

- Frontal — Définit comment les demandes doivent être transférées au back-end. Ce sont les entités découvertes dans Citrix ADM qui équilibrent la charge du trafic.
- Back end : ensemble de serveurs qui reçoivent les demandes transférées.
- Serveurs : serveurs parmi lesquels la charge HaProxy équilibre le trafic.

Pour de plus amples informations, consultez la section http://www.haproxy.org/download/1.7/doc/configuration.txt.

Citrix ADM fournit un tableau de bord de l'application HaProxy sur lequel vous pouvez surveiller les fronts en temps réel. Pour plus d'informations, consultez Tableau de bord de l'application HAProxy. En outre, il vous permet d'afficher les détails des fronts, backends et serveurs configurés sur les instances HaProxy.

Pour gérer et surveiller les instances HAProxy sur un hôte HAProxy, vous devez ajouter l'hôte HAProxy à Citrix ADM. Pour de plus amples informations, consultez la section Ajout d'instances HAProxy.

Informations connexes

- Tableau de bord de l'application HAProxy
- Surveiller les instances HaProxy
- Afficher les détails des fronts configurés sur les instances HaProxy
- Afficher les détails des back-end configurés sur les instances HaProxy
- Afficher les détails des serveurs configurés sur les instances HaProxy
- Afficher les instances HaProxy avec le plus grand nombre de serveurs ou de fronts
- Redémarrez une instance HAProxy

Provisionnement d'instances Citrix ADC VPX sur AWS

April 29, 2021

Lorsque vous déplacez vos applications vers le cloud, les composants qui font partie de votre application augmentent, deviennent plus distribués et doivent être gérés dynamiquement.

Avec les instances Citrix ADC VPX sur AWS, vous pouvez étendre en toute transparence votre pile réseau L4-L7 à AWS. Avec Citrix ADC VPX, AWS devient une extension naturelle de votre infrastructure informatique locale. Vous pouvez utiliser Citrix ADC VPX sur AWS pour combiner l'élasticité et la flexibilité du cloud, avec les mêmes fonctionnalités d'optimisation, de sécurité et de contrôle qui prennent en charge les sites Web et les applications les plus exigeants au monde.

Avec Citrix Application Delivery Management (ADM) qui surveille vos instances Citrix ADC, vous obtenez une visibilité sur l'intégrité, les performances et la sécurité de vos applications. Vous pouvez automatiser la configuration, le déploiement et la gestion de votre infrastructure de livraison d'applications dans des environnements multicloud hybrides.

Terminologie AWS

La section suivante fournit une brève description des termes AWS utilisés dans ce document :

Terme	Définition
Image machine Amazon (AMI)	Image de machine, qui fournit les informations nécessaires au lancement d'une instance, qui est un serveur virtuel dans le cloud.
Elastic Compute Cloud (EC2)	Service Web qui fournit une capacité de calcul sécurisée et redimensionnable dans le cloud. Il est conçu pour faciliter l'informatique en nuage à l'échelle du Web pour les développeurs.
Interface réseau élastique (ENI)	Interface réseau virtuelle que vous pouvez attacher à une instance dans un VPC.
Type d'instance	Amazon EC2 propose un large choix de types d'instance optimisés pour s'adapter à différents cas d'utilisation. Les types d'instance comprennent diverses combinaisons de CPU, de mémoire, de stockage et de capacité réseau et vous offrent la flexibilité nécessaire pour choisir la combinaison appropriée de ressources pour vos applications.

Terme	Définition
Rôle de gestion des identités et des accès (IAM)	Identité AWS avec des stratégies d'autorisation qui déterminent ce que l'identité peut et ne peut pas faire dans AWS. Vous pouvez utiliser un rôle IAM pour permettre aux applications exécutées sur une instance EC2 d'accéder en toute sécurité à vos ressources AWS.
Groupes de sécurité	Ensemble nommé de connexions réseau entrantes autorisées pour une instance.
Sous-réseaux	Segment de la plage d'adresses IP d'un VPC auquel les instances EC2 peuvent être attachées. Vous pouvez créer des sous-réseaux pour regrouper des instances en fonction des besoins opérationnels et de sécurité.
Virtual Private Cloud (VPC)	Service Web permettant de Provisioning une section logiquement isolée du cloud AWS dans laquelle vous pouvez lancer des ressources AWS dans un réseau virtuel que vous définissez.

Types d'instance AMI Citrix ADC pris en charge

Pour une bande passante plus élevée, Citrix recommande les types d'instance suivants :

Types d'instance	Bande passante
M4.X Large	Édition Premium 10 Mbps
M4.X Large	Édition Premium 200 Mbps

Conditions préalables

Ce document suppose ce qui suit :

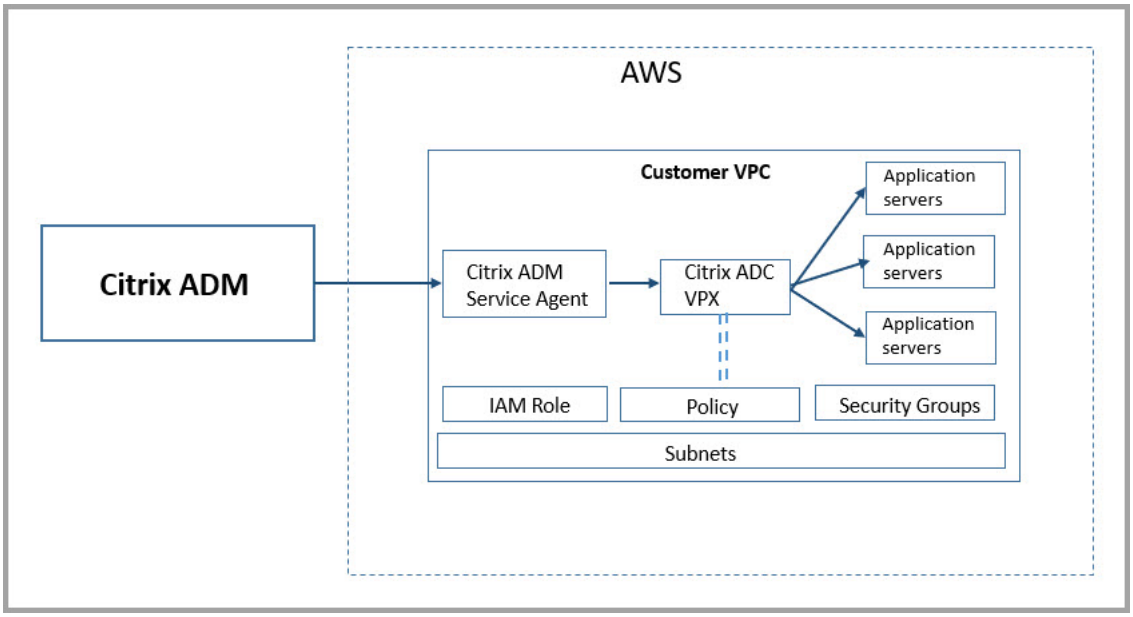
- Vous possédez un compte AWS.
- Vous avez créé le VPC requis et sélectionné les zones de disponibilité.
- Vous avez ajouté l'agent de service Citrix ADM dans AWS.

Pour plus d'informations sur la création d'un compte et d'autres tâches, reportez-vous à la section Documentation AWS.

Pour plus d'informations sur l'installation de l'agent de service Citrix ADM sur AWS, reportez-vous à la sectionInstallation de l'agent de service Citrix ADM sur AWS.

Schéma d'architecture

L'image suivante fournit une vue d'ensemble de la façon dont Citrix ADM se connecte à AWS pour provisionner des instances Citrix ADC VPX dans AWS.



Tâches de configuration

Effectuez les tâches suivantes sur AWS avant de provisionner les instances Citrix ADC VPX dans Citrix ADM :

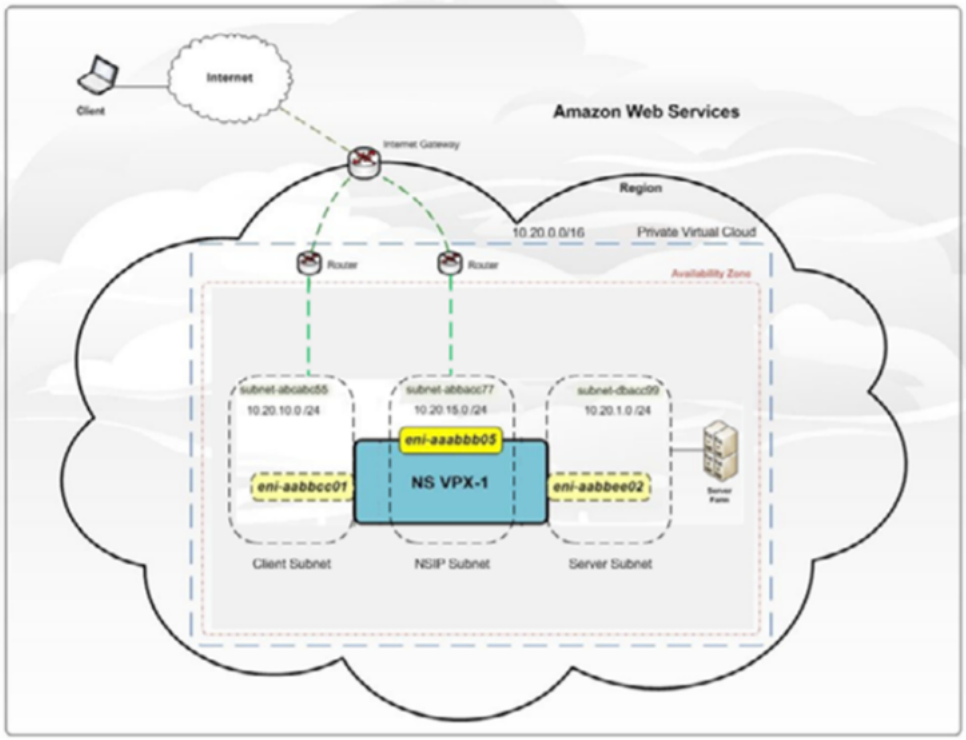
- Créer des sous-réseaux
- Créer des groupes de sécurité
- Créer un rôle IAM et définir une stratégie

Effectuez les tâches suivantes sur Citrix ADM pour provisionner les instances sur AWS :

- Créer un site
- Provisionner l'instance Citrix ADC VPX sur AWS

Pour créer des sous-réseaux

Créez trois sous-réseaux dans votre VPC. Les trois sous-réseaux requis pour provisionner les instances Citrix ADC VPX dans votre VPC sont la gestion, le client et le serveur. Spécifiez un bloc CIDR IPv4 à partir de la plage définie dans votre VPC pour chacun des sous-réseaux. Spécifiez la zone de disponibilité dans laquelle vous souhaitez que le sous-réseau réside. Créez les trois sous-réseaux dans la même zone de disponibilité. L'image suivante illustre les trois sous-réseaux créés dans votre région et leur connectivité au système client.



Pour plus d'informations sur le VPC et les sous-réseaux, reportez-vous à la sectionVPC et sous-réseaux.

Pour créer des groupes de sécurité

Créez un groupe de sécurité pour contrôler le trafic entrant et sortant dans l'instance Citrix ADC VPX. Un groupe de sécurité agit comme un pare-feu virtuel pour votre instance. Créez des groupes de sécurité au niveau de l'instance, et non au niveau du sous-réseau. Il est possible d'attribuer chaque instance d'un sous-réseau de votre VPC à un ensemble différent de groupes de sécurité. Ajoutez des règles pour chaque groupe de sécurité afin de contrôler le trafic entrant qui passe par le sous-réseau client aux instances. Vous pouvez également ajouter un ensemble distinct de règles qui contrôlent le trafic sortant qui passe par le sous-réseau du serveur aux serveurs d'applications. Bien que vous puissiez utiliser le groupe de sécurité par défaut pour vos instances, vous pouvez créer vos groupes. Créez trois groupes de sécurité - un pour chaque sous-réseau. Créez des règles pour le trafic entrant et sortant que vous souhaitez contrôler. Vous pouvez ajouter autant de règles que vous voulez.

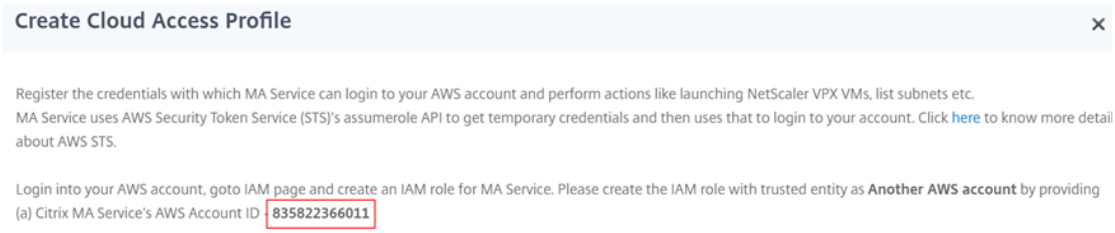
Pour plus d'informations sur les groupes de sécurité, reportez-vous à la sectionGroupes de sécurité pour votre VPC.

Pour créer un rôle IAM et définir une stratégie

Créez un rôle IAM afin que vous puissiez établir une relation d'approbation entre vos utilisateurs et le compte AWS approuvé Citrix et créer une stratégie avec les autorisations Citrix.

1. Dans AWS, cliquez sur **Services**. Dans le volet de navigation de gauche, sélectionnez **IAM > Rôles**, puis cliquez sur **Créer un rôle**.
2. Vous connectez votre compte AWS au compte AWS dans Citrix ADM. Sélectionnez donc **un autre compte AWS** pour permettre à Citrix ADM d'effectuer des actions dans votre compte AWS.

   Saisissez l'ID de compte Citrix ADM AWS à 12 chiffres. L'ID Citrix est 835822366011. Vous pouvez également trouver l'ID Citrix dans Citrix ADM lorsque vous créez le profil d'accès au cloud.



3. Activez l'option **Exiger un ID externe** pour vous connecter à un compte tiers. Vous pouvez augmenter la sécurité de votre rôle en exigeant un identifiant externe facultatif. Tapez un ID qui peut être une combinaison de caractères.
4. Cliquez sur **Autorisations**.
5. Dans la page **Attacher des stratégies d'autorisations**, cliquez sur **Créer une stratégie**.
6. Vous pouvez créer et modifier une stratégie dans l'éditeur visuel ou à l'aide de JSON.

   La liste des autorisations de Citrix est fournie dans la zone suivante :

```
{

"Version": "2012-10-17",
"Statement":
[
    {

          "Effect": "Allow",
         "Action": [
             "ec2:DescribeInstances",
             "ec2:DescribeImageAttribute",
```



```
12              "ec2:DescribeInstanceAttribute",
13              "ec2:DescribeRegions",
14              "ec2:DescribeDhcpOptions",
15              "ec2:DescribeSecurityGroups",
16              "ec2:DescribeHosts",
17              "ec2:DescribeImages",
18              "ec2:DescribeVpcs",
19              "ec2:DescribeSubnets",
20              "ec2:DescribeNetworkInterfaces",
21              "ec2:DescribeAvailabilityZones",
22              "ec2:DescribeNetworkInterfaceAttribute",
23              "ec2:DescribeInstanceStatus",
24              "ec2:DescribeAddresses",
25              "ec2:DescribeKeyPairs",
26              "ec2:DescribeTags",
27              "ec2:DescribeVolumeStatus",
28              "ec2:DescribeVolumes",
29              "ec2:DescribeVolumeAttribute",
30              "ec2:CreateTags",
31              "ec2:DeleteTags",
32              "ec2:CreateKeyPair",
33              "ec2:DeleteKeyPair",
34              "ec2:ResetInstanceAttribute",
35              "ec2:RunScheduledInstances",
36              "ec2:ReportInstanceStatus",
37              "ec2:StartInstances",
38              "ec2:RunInstances",
39              "ec2:StopInstances",
40              "ec2:UnmonitorInstances",
41              "ec2:MonitorInstances",
42              "ec2:RebootInstances",
43              "ec2:TerminateInstances",
44              "ec2:ModifyInstanceAttribute",
45              "ec2:AssignPrivateIpAddresses",
46              "ec2:UnassignPrivateIpAddresses",
47              "ec2:CreateNetworkInterface",
48              "ec2:AttachNetworkInterface",
49              "ec2:DetachNetworkInterface",
50              "ec2:DeleteNetworkInterface",
51              "ec2:ResetNetworkInterfaceAttribute",
52              "ec2:ModifyNetworkInterfaceAttribute",
53              "ec2:AssociateAddress",
54              "ec2:AllocateAddress",
55              "ec2:ReleaseAddress",
56              "ec2:DisassociateAddress",
```



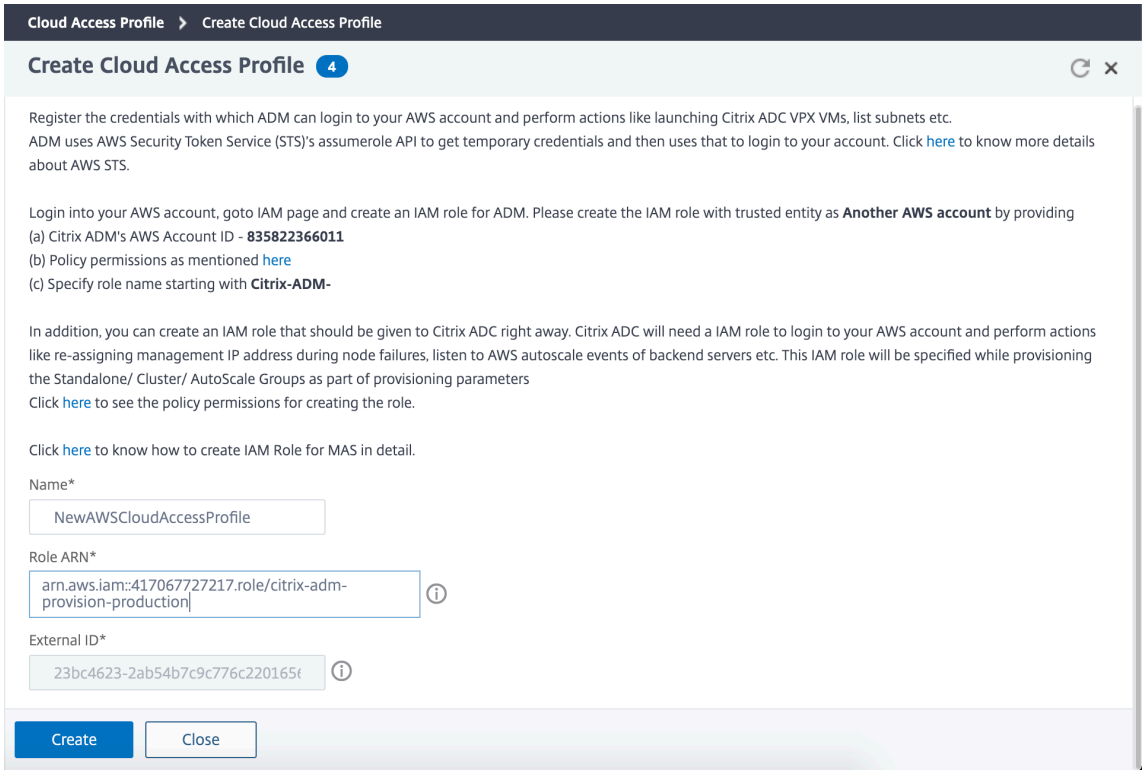
```
57                "ec2:GetConsoleOutput"
58            ],
59                "Resource": "*"
60        }
61
62 ]
63  }
64
65 <!--NeedCopy-->
```

7. Copiez et collez la liste des autorisations dans l'onglet JSON et cliquez sur **Revoir la stratégie**.
8. Dans la page **Vérifier la stratégie**, tapez un nom pour la stratégie, entrez une description, puis cliquez sur **Créer une stratégie** .

Pour créer un site dans Citrix ADM

Créez un site dans Citrix ADM et ajoutez les détails du VPC associé à votre rôle AWS.

1. Dans Citrix ADM, accédez à **Réseaux > Sites**.
2. Cliquez sur **Ajouter**.
3. Sélectionnez le type de service en tant qu'AWS et activez **Utiliser un VPC existant en tant que site**.
4. Sélectionnez le profil d'accès au cloud.
5. Si le profil d'accès au nuage n'existe pas dans le champ, cliquez sur **Ajouter** pour créer un profil.
    a) Dans la page **Créer un profil d'accès au cloud**, tapez le nom du profil avec lequel vous souhaitez accéder à AWS.
    b) Tapez l'ARN associé au rôle que vous avez créé dans AWS.
    c) Tapez l'ID externe que vous avez fourni lors de la création d'un rôle IAM (Identity and Access Management) dans AWS. Reportez-vous à l'étape 4 de Pour créer un rôle IAM et définir une tâche de stratégie. Assurez-vous que le nom de rôle IAM que vous avez spécifié dans AWS commence par « Citrix-ADM- » et qu'il apparaît correctement dans l'ARN des rôles.



Les détails du VPC, tels que la région, l'ID du VPC, le nom et le bloc CIDR, associés à votre rôle IAM dans AWS, sont importés dans Citrix ADM.

6. Tapez un nom pour le site.
7. Cliquez sur **Créer**.

Pour provisionner Citrix ADC VPX sur AWS

Utilisez le site que vous avez créé précédemment pour provisionner les instances Citrix ADC VPX sur AWS. Fournissez les détails de l'agent de service Citrix ADM pour provisionner les instances qui sont liées à cet agent.

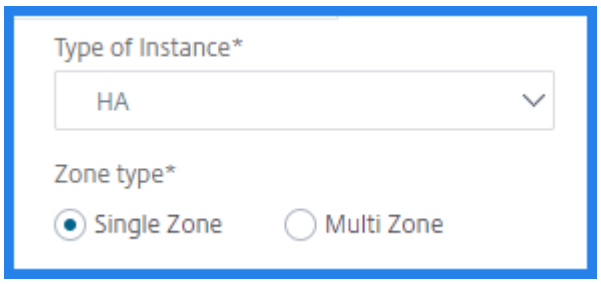
1. Dans Citrix ADM, accédez à **Réseaux** > **Instances** > **Citrix ADC**.
2. Dans l'onglet **VPX**, cliquez sur **Provisionner**.

   Cette option affiche la page **Provisionner Citrix ADC VPX sur le Cloud** .
3. Sélectionnez **Amazon Web Services (AWS)** et cliquez sur **Suivant** .
4. Dans l'onglet **Paramètres de base**,
   a) Sélectionnez le **Type d'instance** dans la liste.
      - **Autonome :** cette option provisionnera une instance autonome Citrix ADC VPX sur AWS.

- **HA :** Cette option provisionnera les instances Citrix ADC VPX haute disponibilité sur AWS.

  Pour provisionner les instances Citrix ADC VPX dans la même zone, sélectionnez l'option **Zone unique** sous **Type de zone**.

  Pour provisionner les instances Citrix ADC VPX sur plusieurs zones, sélectionnez l'option **Multi Zonesous Type de zone**. Dans l'onglet**Paramètres de provisionnement**, assurez-vous de spécifier les détails du réseau pour chaque zone créée sur AWS.



b) Spécifiez le nom d'une instance ADC VPX.

c) Dans **Site**, sélectionnez le site que vous avez créé précédemment.

d) Dans **Agent**, sélectionnez l'agent créé pour gérer l'instance ADC VPX.

e) Dans **Profil d'accès au cloud**, sélectionnez le profil d'accès au nuage créé lors de la création du site.

f) Dans **Profil de périphérique**, sélectionnez le profil pour fournir l'authentification.

Citrix ADM utilise le profil de périphérique lorsqu'il doit ouvrir une session à l'instance Citrix ADC VPX.

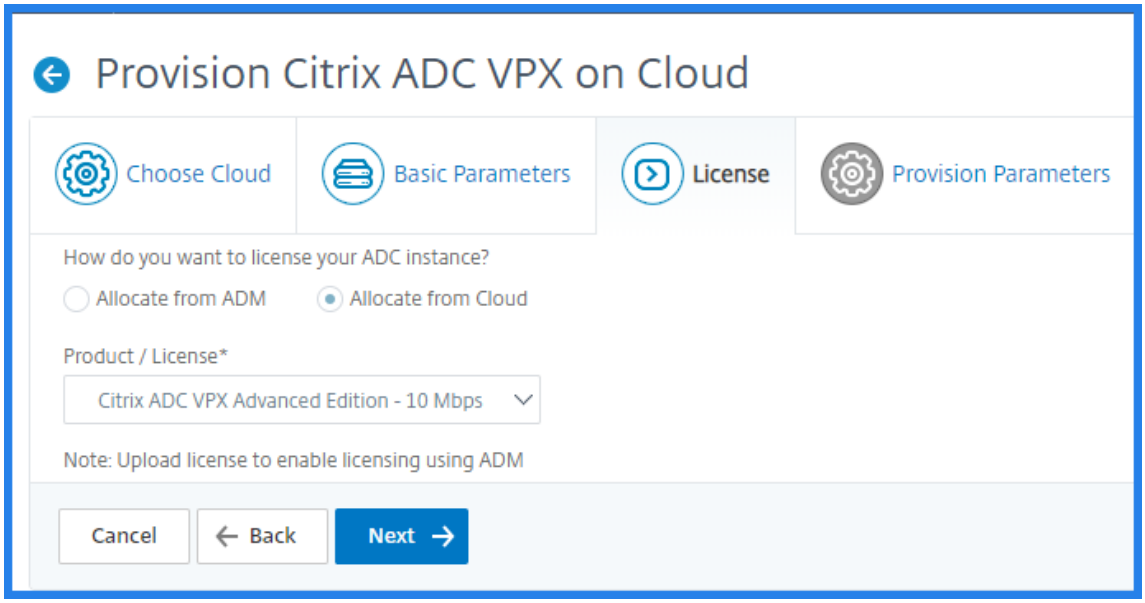
g) Cliquez sur **Suivant**.

5. Dans l'onglet **Licence**, sélectionnez l'un des modes suivants pour appliquer une licence à une instance ADC :

   - **Utilisation de Citrix ADM** : L'instance que vous souhaitez provisionner retirent les licences de Citrix ADM.
   - **Utilisation du cloud AWS** : l'option **Allouer à partir du cloud** utilise les licences de produit Citrix disponibles sur AWS Marketplace. L'instance que vous souhaitez provisionner utilise les licences du site de vente.

     Si vous choisissez d'utiliser des licences d'AWS Marketplace, spécifiez le produit ou la licence dans l'onglet **Paramètres de provisionnement**.

   Pour de plus amples informations, consultez la section Exigences en matière de licence.



6. Dans l'onglet **Licence**, si vous sélectionnez **Allouer à partir d'ADM**, spécifiez les éléments suivants :

   - Type de licence : sélectionnez des licences de bande passante ou de processeur virtuel :

     Licences de bande passante : vous pouvez sélectionner l'une des options suivantes dans la liste **Types de licences de bande passante** :

     - **Capacité groupée :** spécifiez la capacité à allouer à une instance.

       À partir du pool commun, l'instance ADC retirait une licence d'instance et seule la bande passante est spécifiée.

     - **Licences VPX :** lorsqu'une instance Citrix ADC VPX est provisionnée, l'instance extrait la licence de Citrix ADM.

     Licences CPU virtuelles : l'instance Citrix ADC VPX provisionnée retire les licences en fonction du nombre de processeurs exécutés dans l'instance.

     > **Remarque**
     >
     > Lorsque les instances provisionnées sont supprimées ou détruites, les licences appliquées retournent au pool de licences Citrix ADM. Ces licences peuvent être réutilisées pour provisionner de nouvelles instances.

   a) Dans **License Edition**, sélectionnez l'édition de licence. L'ADM utilise l'édition spécifiée pour provisionner des instances.

7. Cliquez sur **Suivant**.

8. Dans l'onglet **Paramètres de provisionnement**,

a) Sélectionnez le **rôle Citrix IAM** créé dans AWS. Un rôle IAM est une identité AWS avec des stratégies d'autorisation qui déterminent ce que l'identité peut ou ne peut pas faire dans AWS.

b) Dans le champ **Produit**, sélectionnez la version du produit Citrix ADC à provisionner.

c) Sélectionnez le type d'instance EC2 dans la liste **Type d'instance** .

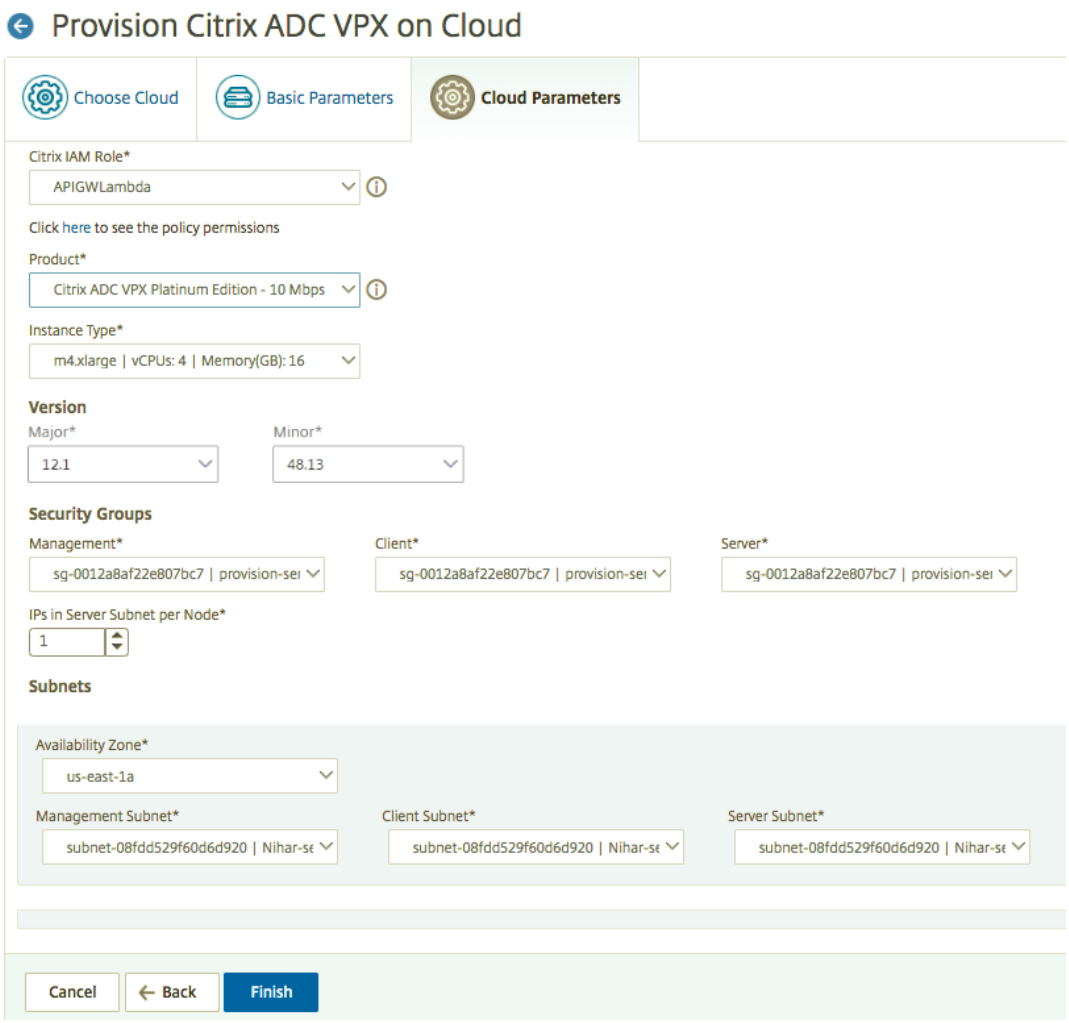
d) Sélectionnez la **version** de Citrix ADC à provisionner. Sélectionnez les versions **Major** et **Minor** de Citrix ADC.

e) Dans **Groupes de sécurité**, sélectionnez les groupes de sécurité Gestion, Client et Serveur que vous avez créés dans votre réseau virtuel.

f) Dans les adresses **IP du sous-réseau du serveur par nœud**, sélectionnez le nombre d'adresses IP dans le sous-réseau du serveur par nœud pour le groupe de sécurité.

g) Dans **Sous-réseaux**, sélectionnez les sous-réseaux Gestion, Client et Serveur pour chaque zone créée dans AWS. Vous pouvez également sélectionner la région dans la liste **Zone de disponibilité** .

h) Cliquez sur **Terminer**.



L'instance Citrix ADC VPX est désormais provisionnée sur AWS.

> **Remarque**
>
> Actuellement, Citrix ADM ne prend pas en charge le déprovisionnement des instances Citrix ADC à partir d'AWS.

Pour afficher le Citrix ADC VPX provisionné dans AWS

1. Depuis la page d'accueil AWS, accédez à **Services** et cliquez sur **EC2**.
2. Dans la page **Ressources**, cliquez sur **Instances en cours d'exécution** .
3. Vous pouvez afficher le Citrix ADC VPX provisionné dans AWS.

Le nom de l'instance Citrix ADC VPX est le même que celui que vous avez fourni lors du provisionnement d'une instance dans Citrix ADM.

Pour afficher le Citrix ADC VPX provisionné dans Citrix ADM

1. Dans Citrix ADM, accédez à **Réseaux** > **Instances** > **Citrix ADC**.
2. Sélectionnez l'onglet **Citrix ADC VPX** .
3. L'instance Citrix ADC VPX provisionnée dans AWS est répertoriée ici.

Mise à l'échelle automatique de Citrix ADC dans AWS à l'aide de Citrix ADM

April 29, 2021

L'hébergement efficace des applications dans un cloud implique une gestion aisée et économique des ressources en fonction de la demande des applications. Par exemple, considérez que vous disposez d'un portail Web de commerce électronique fonctionnant sur AWS. Ce portail offre parfois d'énormes réductions au cours desquelles il y a un pic dans le trafic des applications. Lorsque le trafic des applications augmente au cours de ces offres, les applications doivent être mises à l'échelle dynamique et, par conséquent, les ressources réseau peuvent également être augmentées.

La fonctionnalité de mise à l'échelle automatique Citrix ADM prend en charge le Provisioning et la mise à l'échelle automatique des instances Citrix ADC dans AWS. La fonction de mise à l'échelle automatique Citrix ADM surveille en permanence les paramètres de seuil tels que l'utilisation de la mémoire, l'utilisation du processeur et le débit. Vous pouvez sélectionner l'un de ces paramètres ou plusieurs paramètres pour la surveillance. Ces valeurs de paramètre sont ensuite comparées aux valeurs configurées par l'utilisateur. Si les valeurs des paramètres dépassent les limites, la scale-out ou scale-in est déclenchée en conséquence.

L'architecture de fonctionnalités de mise à l'Autoscale Citrix ADM est conçue de telle sorte que vous puissiez configurer le nombre minimum et maximal d'instances pour chaque groupe de mise à l'Autoscale. La préconfiguration de ces numéros garantit que votre application est toujours opérationnelle.

> **Important**
>
> Autoscaling prend en charge toutes les fonctionnalités de Citrix ADC, à l'exception des fonctionnalités suivantes qui nécessitent une configuration ponctuée sur les nœuds de cluster :
>
> - GSLB
> - Citrix Gateway et ses fonctionnalités
> - Fonctionnalités de télécommunication
>
> Pour plus d'informations sur la configuration ponctuée, reportez-vous à la sectionConfigurations

> striped, striped partielles et spotted.

Avantages de la mise à l'échelle automatique

Haute disponibilité des applications. La mise à l'échelle automatique garantit que votre application dispose toujours du nombre approprié d'instances Citrix ADC VPX pour gérer les demandes de trafic. Cela permet de s'assurer que votre application est en service tout le temps, indépendamment de la demande de trafic.

Décisions de mise à l'échelle intelligente et configuration zéro tactile. La mise à l'échelle automatique surveille en permanence votre application et ajoute ou supprime dynamiquement les instances de Citrix ADC en fonction de la demande. Lorsque la demande augmente, les instances sont automatiquement ajoutées. Lorsque la demande augmente vers le bas, les instances sont automatiquement supprimées.
L' ajout et la suppression d'instances de Citrix ADC se produisent automatiquement, ce qui en fait une configuration manuelle sans contact.

Gestion automatique du DNS. La fonctionnalité de mise à l'Autoscale Citrix ADM offre une gestion DNS automatique. Chaque fois que de nouvelles instances Citrix ADC sont ajoutées, les noms de domaine sont mis à jour automatiquement.

Fin de connexion gracieuse. Lors d'une mise à l'échelle, les instances de Citrix ADC sont supprimées de manière gracieuse, évitant ainsi la perte de connexions client.

Meilleure gestion des coûts. La mise à l'échelle automatique augmente ou diminue dynamiquement les instances de Citrix ADC si nécessaire. Cela vous permet d'optimiser les coûts impliqués. Vous économisez de l'argent en lançant des instances uniquement lorsqu'elles sont nécessaires et en les résiliant lorsqu'elles ne sont pas nécessaires. Ainsi, vous ne payez que pour les ressources que vous utilisez.

Observabilité. L'observabilité est la clé du développement des applications ou du personnel informatique pour surveiller l'état de l'application. Le tableau de bord de mise à l'Autoscale de Citrix ADM vous permet de visualiser les valeurs des paramètres de seuil, les horodatages de déclenchement de mise à l'Autoscale, les événements et les instances participant à la mise à l'échelle automatique.

Prise en charge

Actuellement, la fonctionnalité de Autoscale est prise en charge uniquement pour les instances Citrix ADC déployées dans AWS.

> **Remarque**

> L'utilisation de Citrix ADC version 12.1 build 50.28 image pour créer des groupes de mise à l'Autoscale dans AWS n'est pas prise en charge.

Configuration requise pour le système de licences

Les instances Citrix ADC créées pour le groupe Citrix Autoscale utilisent les licences Citrix ADC Advanced ou Premium ADC. La fonctionnalité de clustering Citrix ADC est incluse dans les licences ADC Advanced ou Premium.

Vous pouvez choisir l'une des méthodes suivantes pour concéder une licence aux Citrix ADC provisionnés par Citrix ADM :

- **Utilisation des licences ADC présentes dans Citrix ADM :** configurez la capacité groupée, les licences VPX ou les licences CPU virtuelles lors de la création du groupe Mise à l'Autoscale. Ainsi, lorsqu'une nouvelle instance est provisionnée pour le groupe Mise à l'Autoscale, le type de licence déjà configuré est automatiquement appliqué à l'instance provisionnée.
  - **Capacité groupée** : alloue la bande passante à chaque instance provisionnée du groupe Mise à l'Autoscale. Assurez-vous que vous disposez de la bande passante nécessaire dans Citrix ADM pour provisionner de nouvelles instances. Pour de plus amples informations, consultez la section Configurer la capacité groupée.

    Chaque instance ADC du groupe Mise à l'Autoscale retirait une licence d'instance et la bande passante spécifiée du pool.
  - **Licences VPX :** Applique les licences VPX aux instances nouvellement provisionnées. Assurez-vous que vous disposez du nombre nécessaire de licences VPX disponibles dans Citrix ADM pour provisionner de nouvelles instances.

    Lorsqu'une instance Citrix ADC VPX est provisionnée, l'instance extraire la licence auprès de Citrix ADM. Pour de plus amples informations, consultez la section Licences d'enregistrement et de sortie Citrix ADC VPX.
  - **Licences de CPU virtuel :** applique des licences de CPU virtuel aux instances nouvellement provisionnées. Cette licence spécifie le nombre de processeurs autorisés à une instance Citrix ADC VPX. Assurez-vous que vous disposez du nombre nécessaire de processeurs virtuels dans Citrix ADM pour provisionner de nouvelles instances.

    Lorsqu'une instance Citrix ADC VPX est provisionnée, l'instance extraire la licence du processeur virtuel à partir de Citrix ADM. Pour de plus amples informations, consultez la section Licences de processeur virtuel Citrix ADC.

  Lorsque les instances provisionnées sont détruites ou déprovisionnées, les licences appliquées sont automatiquement renvoyées à Citrix ADM.

  Pour surveiller les licences consommées, accédez à la page **Réseaux** > **Licences**.

- **Utilisation des licences d'abonnement AWS :** configurez les licences Citrix ADC disponibles sur AWS Marketplace lors de la création du groupe Autoscale. Ainsi, lorsqu'une nouvelle instance est provisionnée pour le groupe Autoscale, la licence est obtenue auprès d'AWS Marketplace.

Terminologie AWS

Le tableau suivant fournit une brève description de certains des termes de mise à l'échelle automatique utilisés dans ce document.

Terminologie	Description
Groupe de mise à l'échelle automatique AWS	AWS Auto Scaling group est un ensemble d'instances EC2 qui partagent des caractéristiques similaires et sont traitées comme un regroupement logique aux fins de la mise à l'échelle et de la gestion des instances.
Image machine Amazon (AMI)	Image de machine, qui fournit les informations nécessaires au lancement d'une instance, qui est un serveur virtuel dans le cloud.
Elastic Compute Cloud (EC2)	Service Web qui fournit une capacité de calcul sécurisée et redimensionnable dans le cloud. Il est conçu pour faciliter l'informatique en nuage à l'échelle du Web pour les développeurs.
Adresses IP élastiques (EIP)	Une adresse IP Elastic est une adresse IPv4 publique statique conçue pour le cloud computing dynamique. Vous pouvez associer une adresse IP Elastic à n'importe quelle instance ou interface réseau pour n'importe quel VPC de votre compte.
Interface réseau élastique (ENI)	Interface réseau virtuelle que vous pouvez attacher à une instance dans un VPC.

Terminologie	Description
Type d’instance	Amazon EC2 propose un large choix de types d’instance optimisés pour s’adapter à différents cas d’utilisation. Les types d’instance comprennent diverses combinaisons de CPU, de mémoire, de stockage et de capacité réseau et vous offrent la flexibilité nécessaire pour choisir la combinaison appropriée de ressources pour vos applications.
Rôle de gestion des identités et des accès (IAM)	Identité AWS avec des stratégies d’autorisation qui déterminent ce que l’identité peut et ne peut pas faire dans AWS. Vous pouvez utiliser un rôle IAM pour permettre aux applications exécutées sur une instance EC2 d’accéder en toute sécurité à vos ressources AWS.
Profil d’instance IAM-IAM-	Identité fournie aux instances Citrix ADC provisionnées dans un cluster dans AWS. Le profil permet aux instances d’accéder aux services AWS lorsqu’il commence à équilibrer la charge des demandes du client.
Écouteur	Un processus d’écoute est un processus qui vérifie les demandes de connexion, à l’aide du protocole et du port que vous configurez. Les règles que vous définissez pour un processus d’écoute déterminent comment l’équilibreur de charge achemine les demandes vers les cibles d’un ou de plusieurs groupes cibles.
NLB	Équilibreur de charge réseau. NLB est un équilibreur de charge L4 disponible dans l’environnement AWS.
Route 53	Route 53 est le service Web DNS (Cloud Domain Name System) hautement disponible et évolutif d’Amazon.
Groupes de sécurité	Ensemble nommé de connexions réseau entrantes autorisées pour une instance.

Terminologie	Description
Sous-réseaux	Segment de la plage d'adresses IP d'un VPC auquel les instances EC2 peuvent être attachées. Vous pouvez créer des sous-réseaux pour regrouper des instances en fonction des besoins opérationnels et de sécurité.
Virtual Private Cloud (VPC)	Service Web permettant de Provisioning une section logiquement isolée du cloud AWS dans laquelle vous pouvez lancer des ressources AWS dans un réseau virtuel que vous définissez.

Terminologie de mise à l'Autoscale Citrix ADC VPX

Le tableau suivant fournit une brève description de certains termes de mise à l'échelle automatique Citrix ADC VPX utilisés dans ce document.

Terminologie	Description
Groupes de mise à l'échelle automatique	Le groupe de mise à l'échelle automatique est un groupe d'instances Citrix ADC qui équilibrent la charge des applications en tant qu'entité unique et déclenchent la mise à l'échelle automatique lorsque les paramètres de seuil dépassent les limites. Les instances Citrix ADC sont évolutives ou évolutives dynamiquement en fonction de la configuration des groupes Mise à l'Autoscale. **Remarque :** le groupe Citrix Autoscale est appelé groupe Autoscale tout au long de ce document, tandis que le groupe AWS Autoscale est explicitement appelé groupe AWS Autoscale.
Clusters Citrix ADC	Un cluster Citrix ADC est un groupe d'instances Citrix ADC VPX et chaque instance est appelée un nœud. Le trafic client est réparti entre les nœuds pour fournir une haute disponibilité, un débit élevé et une évolutivité.

Terminologie	Description
Délai d'expiration de la connexion de vidange	Pendant la mise à l'échelle, une fois qu'une instance est sélectionnée pour le déprovisionnement, Citrix ADM supprime l'instance du traitement des nouvelles connexions vers le groupe Mise à l'Autoscale et attend que le délai d'expiration de connexion de drain spécifié expire avant le déprovisionnement. Cela permet de drainer les connexions existantes à cette instance avant qu'elle ne soit déprovisionnée. Si les connexions sont drainées avant l'expiration du délai d'expiration de la connexion de drain, même Citrix ADM attend que le délai d'expiration de la connexion de drain expire avant de commencer une nouvelle évaluation. **Remarque :** Si les connexions ne sont pas drainées même après l'expiration du délai de connexion de drain, Citrix ADM supprime les instances qui peuvent avoir un impact sur l'application. La valeur par défaut est de 5 minutes et est configurable.
Période de recharge	Après une mise à l'échelle, la période de recharge est le temps pendant lequel l'évaluation des statistiques doit être arrêtée. Cela garantit la croissance organique d'un groupe Autoscale en permettant au trafic actuel de se stabiliser et de faire la moyenne sur l'ensemble actuel d'instances avant que la prochaine décision de mise à l'échelle ne soit prise. La valeur de la période de recharge par défaut est de 10 minutes et est configurable. **Remarque :** La valeur par défaut est déterminée en fonction du temps nécessaire pour que le système se stabilise après une mise à l'échelle (environ 4 minutes), ainsi que de la configuration Citrix ADC et du temps de publication DNS.

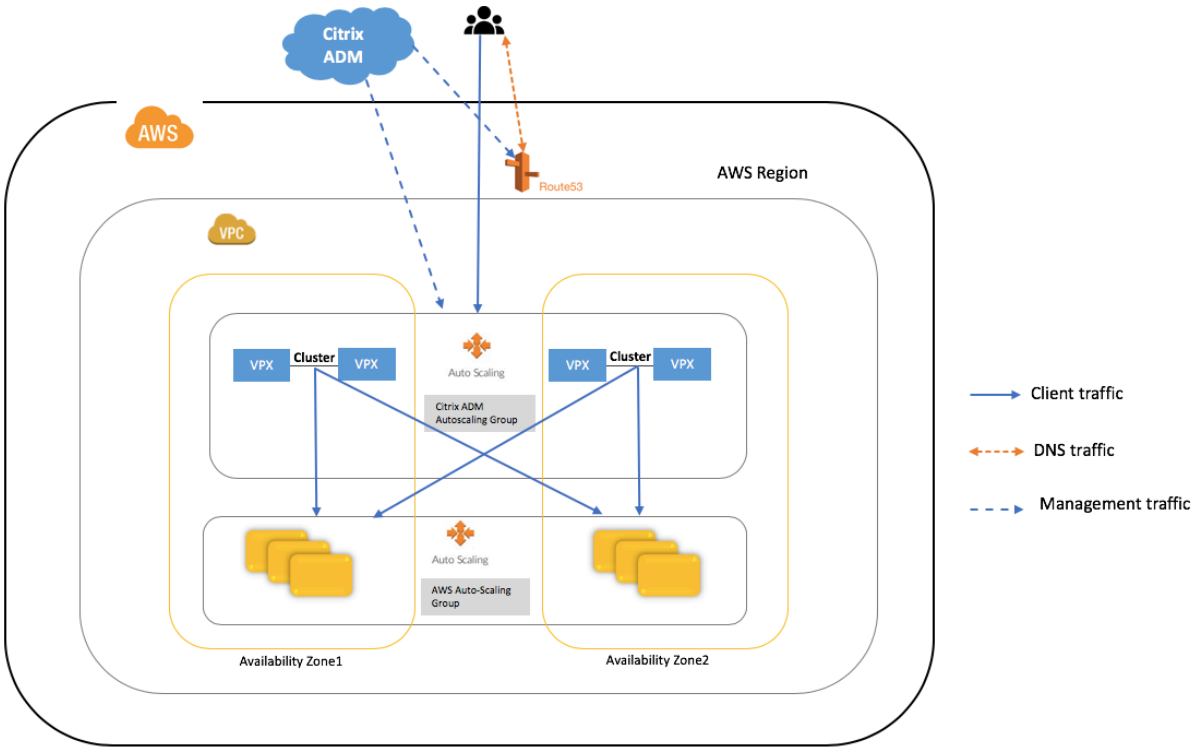
Terminologie	Description
Balises	Chaque groupe de Autoscale se voit attribuer une balise qui est une paire clé et valeur. Vous pouvez appliquer des balises aux ressources qui vous permettent d'organiser et d'identifier facilement les ressources. Les balises sont appliquées à AWS et à Citrix ADM. **Exemple :** Key= nom, Valeur = serveur Web. Il est recommandé d'utiliser un ensemble cohérent de balises pour suivre facilement les groupes de mise à l'Autoscale pouvant appartenir à divers groupes tels que le développement, la production, les tests.
Paramètres de seuil	Paramètres contrôlés pour déclencher la mise à l'échelle ou la mise à l'échelle. Les paramètres sont l'utilisation du CPU, l'utilisation de la mémoire et le débit. Vous pouvez sélectionner un ou plusieurs paramètres pour la surveillance.
Temps de vivre (TTL)	Spécifie l'intervalle de temps pendant lequel l'enregistrement de ressource DNS peut être mis en cache avant que la source des informations ne soit à nouveau consultée. La valeur TTL par défaut est de 30 secondes et est configurable.

Terminologie	Description
Temps de visionnage	Durée pendant laquelle le seuil du paramètre d'échelle doit rester dépassé pour qu'une mise à l'échelle se produise. Si le seuil est dépassé sur tous les échantillons prélevés dans ce délai, une mise à l'échelle se produit. Si les paramètres de seuil restent à une valeur supérieure à la valeur de seuil maximale tout au long de cette durée, une mise à l'échelle est déclenchée. Si les paramètres de seuil fonctionnent à une valeur inférieure à la valeur de seuil minimale, une mise à l'échelle est déclenchée. La valeur par défaut est de 3 minutes et est configurable.

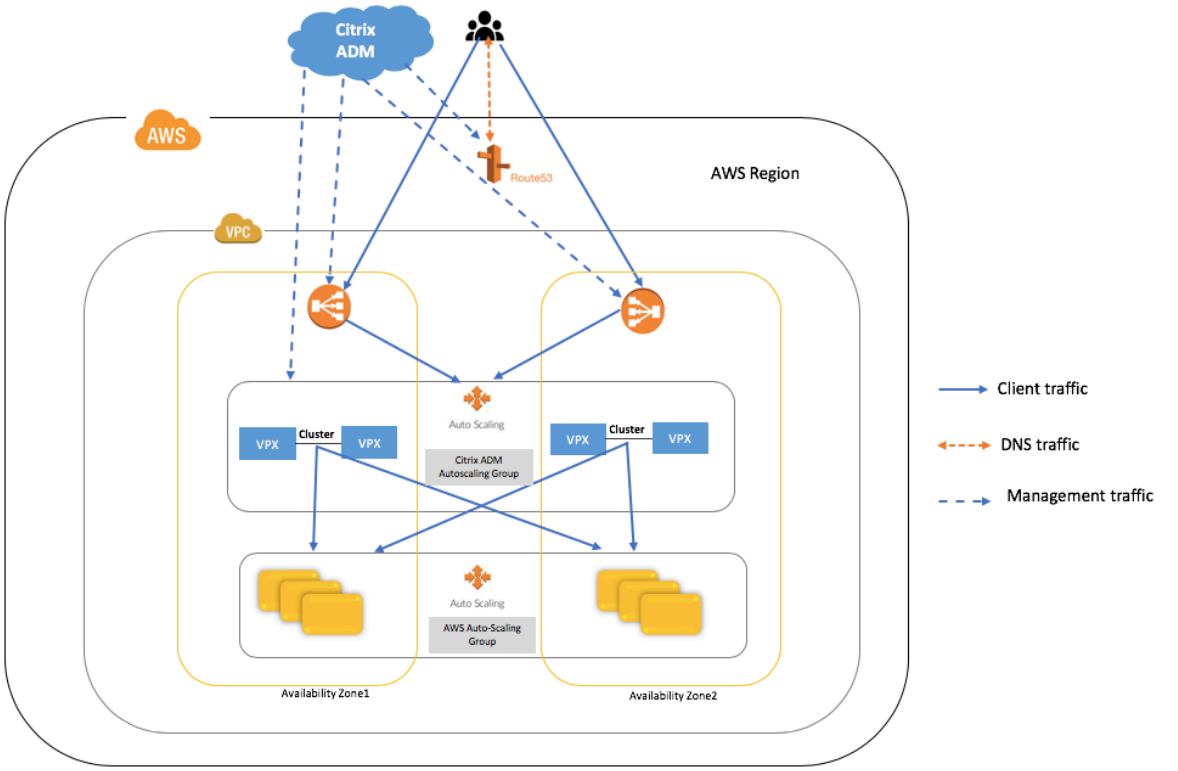
Architecture

April 29, 2021

Le diagramme suivant illustre l'architecture de la fonction de mise à l'échelle automatique avec DNS comme distributeur de trafic.



Le diagramme suivant illustre l'architecture de la fonction de mise à l'échelle automatique avec NLB comme distributeur de trafic.



Citrix Application Delivery Management (ADM)

Citrix Application Delivery Management est une solution Web permettant de gérer tous les déploiements Citrix ADC déployés sur site ou sur le cloud. Vous pouvez utiliser cette solution cloud pour gérer, surveiller et dépanner l'ensemble de l'infrastructure de livraison d'applications globales à partir d'une console unique, unifiée et centralisée basée sur le cloud. Citrix Application Delivery Management (ADM) fournit toutes les fonctionnalités nécessaires pour configurer, déployer et gérer rapidement la livraison d'applications dans les déploiements Citrix ADC, ainsi que des analyses approfondies de l'intégrité, des performances et de la sécurité des applications.

Les groupes de mise à l'Autoscale sont créés dans Citrix ADM et les instances Citrix ADC VPX sont provisionnées à partir de Citrix ADM. L'application est ensuite déployée via StyleBooks dans Citrix ADM.

Distributeurs de trafic (NLB ou DNS/Route53)

NLB ou DNS/route53 est utilisé pour distribuer le trafic sur tous les nœuds d'un groupe de mise à Autoscale. Pour plus d'informations, reportez-vous à la section Modes de distribution du trafic de mise à l'échelle automatique.

Citrix ADM communique avec le distributeur de trafic pour mettre à jour le domaine d'application et les adresses IP des serveurs virtuels d'équilibrage de charge qui frontent l'application.

Groupe Citrix ADM Autoscale

Le groupe de mise à l'échelle automatique est un groupe d'instances Citrix ADC qui équilibrent la charge des applications en tant qu'entité unique et déclenchent la mise à l'échelle automatique en fonction des valeurs de paramètre de seuil configurées.

Clusters de Citrix ADC

Un cluster Citrix ADC est un groupe d'instances Citrix ADC VPX et chaque instance est appelée un nœud. Le trafic client est réparti entre les nœuds pour fournir une haute disponibilité, un débit élevé et une évolutivité.

> **Remarque**
>
> - Les décisions de mise à l'échelle automatique sont prises au niveau du cluster et non au niveau du nœud.
> - Les clusters indépendants sont hébergés dans différentes zones de disponibilité et, par conséquent, la prise en charge de certaines fonctionnalités d'état partagées est limitée.
>
> Les sessions de persistance telles que la persistance de l'IP source et d'autres, à l'exception de la persistance basée sur les cookies, ne peuvent pas être partagées entre les clusters. Cependant,

> toutes les fonctionnalités sans état telles que les méthodes d'équilibrage de charge fonctionnent comme prévu dans les différentes zones de disponibilité.

Groupes de mise à l'échelle automatique AWS

AWS Auto Scaling group est un ensemble d'instances EC2 qui partagent des caractéristiques similaires et sont traitées comme un regroupement logique aux fins de la mise à l'échelle et de la gestion des instances.

Zones de disponibilité AWS

La zone de disponibilité AWS est un emplacement isolé à l'intérieur d'une région. Chaque région est composée de plusieurs zones de disponibilité. Chaque zone de disponibilité appartient à une seule région.

Modes de distribution du trafic

Lorsque vous déplacez votre déploiement d'applications vers le cloud, la mise à l'échelle automatique devient une partie de l'infrastructure. Au fur et à mesure que les applications évolutives ou évolutives à l'aide de la mise à l'échelle automatique, ces modifications doivent être propagées au client. Cette propagation est réalisée à l'aide d'une mise à l'échelle automatique basée sur DNS ou NLB.

Mise à l'échelle automatique basée sur la NLB

En mode de déploiement basé sur NLB, le niveau de distribution vers les nœuds de cluster est l'équilibreur de charge réseau AWS.

Dans la mise à l'échelle automatique basée sur la NLB, une seule adresse IP statique est proposée par zone de disponibilité. Il s'agit de l'adresse IP publique qui est ajoutée à route53 et les adresses IP back-end peuvent être privées. Avec cette adresse IP publique, toute nouvelle instance Citrix ADC provisionnée pendant la mise à l'échelle automatique fonctionne à l'aide d'adresses IP privées et ne nécessite pas d'adresses IP publiques supplémentaires.

Utilisez la mise à l'échelle automatique basée sur NLB pour gérer le trafic TCP. Utilisez la mise à l'échelle automatique basée sur DNS pour gérer le trafic UDP.

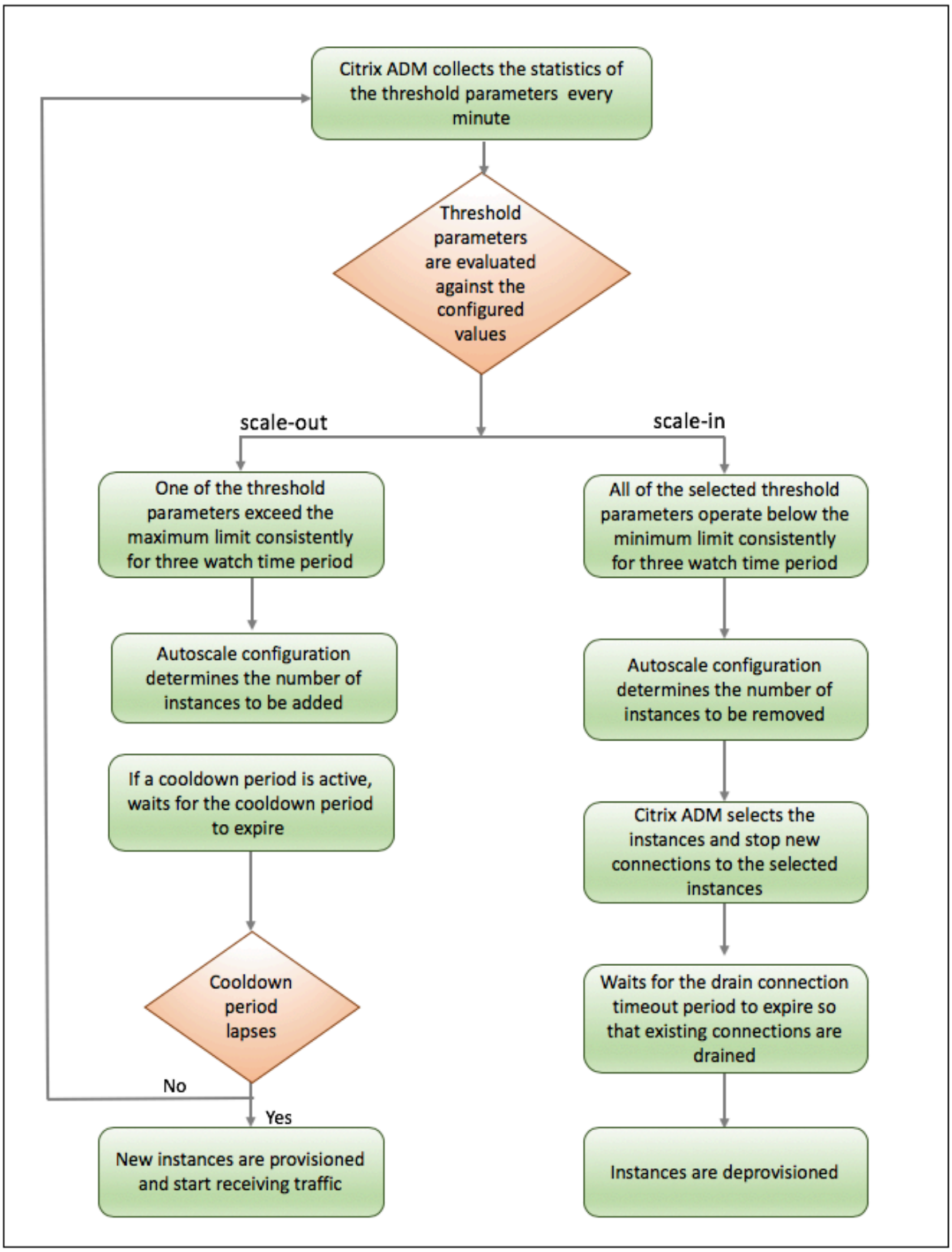
Mise à l'échelle automatique basée sur DNS

Dans la mise à l'échelle automatique basée sur DNS, DNS agit comme la couche de distribution pour les nœuds de cluster Citrix ADC. Les modifications de mise à l'échelle sont propagées au client en mettant à jour le nom de domaine correspondant à l'application. Actuellement, le fournisseur DNS est AWS Route53.

> **Remarque**
>
> Dans la mise à l'échelle automatique basée sur DNS, chaque instance d'Citrix ADC nécessite une adresse IP publique.

Fonctionnement de la mise à l'échelle automatique

L'organigramme suivant illustre le flux de travail de mise à l'échelle automatique.



Citrix ADM collecte des statistiques (utilisation du processeur, utilisation de la mémoire, débit) à partir des clusters provisionnés à l'Autoscale à un intervalle de temps d'une minute.

Les statistiques sont évaluées en fonction des seuils de configuration. Selon que les statistiques dépassent le seuil maximal ou fonctionnent en dessous du seuil minimum, la mise à l'échelle ou la mise à l'échelle est déclenchée respectivement.

- Si une mise à l'échelle est déclenchée :
  - Les nouveaux nœuds sont provisionnés.
  - Les nœuds sont attachés au cluster et la configuration est synchronisée entre le cluster et le nouveau nœud.
  - Les nœuds sont enregistrés auprès de Citrix ADM.
  - Les nouvelles adresses IP de noeud sont mises à jour dans DNS/NLB.

Lorsque l'application est déployée, `IPset` est créée sur des clusters dans chaque zone de disponibilité et le domaine et les adresses IP de l'instance sont enregistrées auprès de DNS/NLB.

- Si une mise à l'échelle est déclenchée :
  - Les adresses IP des nœuds identifiés pour la suppression sont supprimées.
  - Les nœuds sont détachés du cluster, déprovisionnés, puis radiés de Citrix ADM.

Lorsque l'application est supprimée, le domaine et les adresses IP d'instance sont radiés de DNS/NLB et `IPset` sont supprimés.

Exemple

Considérez que vous avez créé un groupe de mise à l'Autoscale nommé asg_arn dans une zone de disponibilité unique avec la configuration suivante.

- Paramètre de seuil — Utilisation de la mémoire
- Limite minimale : 40
- Limite maximale : 85
- Temps de visionnage — 3 minutes
- Période de recharge — 10 minutes
- Délai d'expiration de la connexion de vidange — 10 minutes
- Délai d'expiration TTL — 60 secondes

Une fois le groupe Autoscale créé, les statistiques sont collectées à partir du groupe Mise à Autoscale. La stratégie Mise à l'Autoscale évalue également si un événement de mise à l'Autoscale est en cours et si une mise à l'échelle automatique est en cours, attend la fin de cet événement avant de collecter les statistiques.

ASG ID	Availability zone	Cluster IP address	CPU usage	Throughput	Memory usage	Timestamp
asg_arn	eu-west-2	192.0.2.250	55	65	92	T1
asg_arn	eu-west-2	192.0.2.250	60	50	90	T2
asg_arn	eu-west-2	192.0.2.250	59	45	80	T3
asg_arn	eu-west-2	192.0.2.250	49	75	90	T4
asg_arn	eu-west-2	192.0.2.250	63	70	93	T5
asg_arn	eu-west-2	192.0.2.250	65	80	92	T6
asg_arn	eu-west-2	192.0.2.250	65	85	75	T7
asg_arn	eu-west-2	192.0.2.250	35	70	70	.....
asg_arn	eu-west-2	192.0.2.250	55	70	70	T16
asg_arn	eu-west-2	192.0.2.250	58	55	45	T17
asg_arn	eu-west-2	192.0.2.250	59	65	30	T18
asg_arn	eu-west-2	192.0.2.250	75	45	30	T19
asg_arn	eu-west-2	192.0.2.250	46	64	25	T20
asg_arn	eu-west-2	192.0.2.250	64	65	50	T31
asg_arn	eu-west-2	192.0.2.250	64	65	60	T32
asg_arn	eu-west-2	192.0.2.250	64	65	60	T33

Scale-out event is triggered. Nodes are provisioned.

Evaluation of statistics is skipped for this availability zone from T7 –T16 as the cooldown period is in effect.

Scale-in event is triggered. Drain connection timeout in effect.

Séquence des événements :

- T1 et T2 : l'utilisation de la mémoire dépasse la limite maximale de seuil.
- T3 - L'utilisation de la mémoire est inférieure aux limites de seuil maximum.
- T6, T5, T4 : L'utilisation de la mémoire a dépassé la limite maximale consécutivement pour trois durées de temps de surveillance.
  - Une mise à l'échelle est déclenchée.
  - Le provisionnement des nœuds se produit.
  - La période de recharge est en vigueur.
- T7 — T16 : L'évaluation de l'échelle automatique est ignorée pour cette zone de disponibilité de T7 à T16 lorsque la période de refroidissement est en vigueur.
- T18, T19, T20 - L'utilisation de la mémoire a dépassé la limite minimale consécutive pour trois durées de temps de montre.
  - La mise à l'échelle est déclenchée.
  - Le délai d'expiration de la connexion de vidange est en vigueur.
  - Les adresses IP sont retirées du DNS/NLB.
- T21 — T30 : L'évaluation automatique de la mise à l'échelle est ignorée pour cette zone de disponibilité de T21 à T30 lorsque le délai d'expiration de la connexion de drain est en vigueur.

- T31
  - Pour la mise à l'échelle automatique basée sur DNS, TTL est en vigueur.
  - Pour la mise à l'échelle automatique basée sur la NLB, le désapprovisionnement des instances se produit.
- T32
  - Pour la mise à l'échelle automatique basée sur la NLB, l'évaluation des statistiques commence.
  - Pour la mise à l'échelle automatique basée sur DNS, le désapprovisionnement des instances se produit.
- T33 : Pour la mise à l'échelle automatique basée sur DNS, l'évaluation des statistiques commence.

Configuration Autoscale

April 29, 2021

Pour démarrer la mise à l'échelle automatique des instances Citrix ADC VPX dans AWS, vous devez effectuer les étapes suivantes :

1. Complétez toutes les conditions préalables sur AWS
2. Complétez toutes les conditions préalables sur Citrix ADM
3. Créer des groupes de mise à l'échelle automatique
   a) Initialiser la configuration de mise à l'échelle automatique
   b) Configurer les paramètres de mise à l'échelle automatique
   c) Vérifier les licences
   d) Configurer les paramètres du cloud
4. Déployer l'application

Prérequis pour AWS

Assurez-vous que vous avez rempli toutes les conditions préalables sur AWS pour utiliser la fonctionnalité Mise à l'Autoscale. Ce document suppose ce qui suit :

1. Vous possédez déjà un compte AWS.
2. Vous avez créé un utilisateur IAM (Identity and Access Management) disposant de toutes les autorisations administratives.

Les sections suivantes vous aident à effectuer toutes les tâches nécessaires dans AWS avant de créer des groupes Autoscale dans Citrix ADM. Les tâches que vous devez effectuer sont les suivantes :

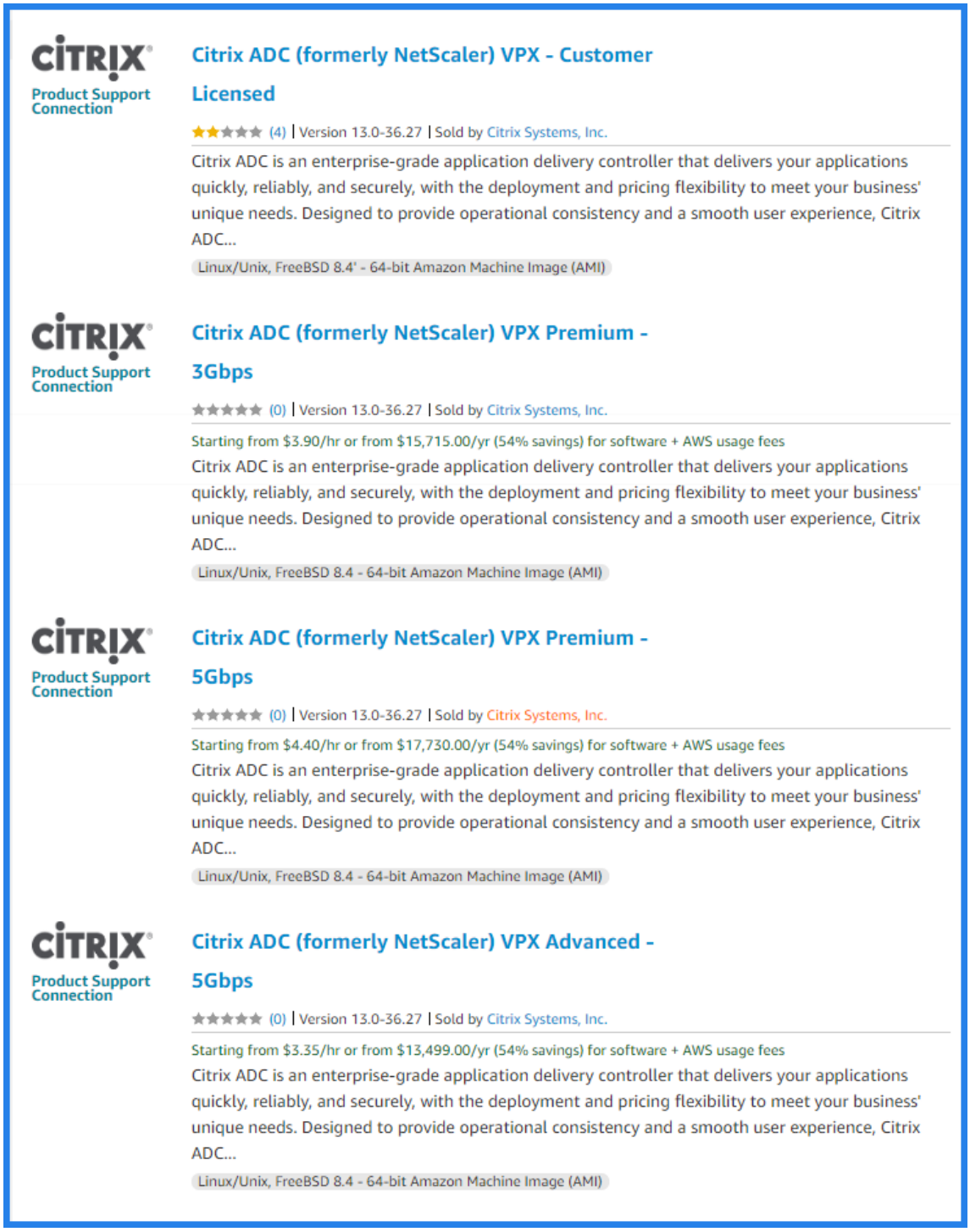
1. Abonnez-vous à l'instance Citrix ADC VPX requise sur AWS.
2. Créez le Virtual Private Cloud (VPC) requis ou sélectionnez un VPC existant.
3. Définissez les sous-réseaux et les groupes de sécurité correspondants.
4. Créez deux rôles IAM, l'un pour Citrix ADM et l'autre pour l'instance Citrix ADC VPX.

> **Conseil**
>
> Vous pouvez utiliserModèles AWS CloudFormationpour automatiser l'étape des prérequis AWS pour la mise à l'échelle automatique Citrix ADC.

Pour plus d'informations sur la création de VPC, de sous-réseau et de groupes de sécurité, reportez-vous à la section Documentation AWS.

S'abonner à la licence Citrix ADC VPX dans AWS

1. Accédez au Marketplace AWS.
2. Connectez-vous avec vos informations d'identification.
3. Recherchez Citrix ADC VPX Client Licence, Premium ou Advanced Edition.



4. Abonnez-vous aux licences Citrix ADC VPX sous licence client, Édition Premium ou Citrix ADC VPX Advanced Edition.

> **Remarque**
>
> Si vous souhaitez que les instances ADC du groupe Mise à l'Autoscale retirent les licences de

> l'ADM, vérifiez ce qui suit :
>
> - Les licences ADC requises sont disponibles dans le SMA.
> - Le produit **sous licence client Citrix ADC VPX** est abonné.

Créer des sous-réseaux

Créez trois sous-réseaux dans votre VPC : un pour les connexions de gestion, client et serveur. Spécifiez un bloc CIDR IPv4 à partir de la plage définie dans votre VPC pour chacun des sous-réseaux. Spécifiez la zone de disponibilité dans laquelle vous souhaitez que le sous-réseau réside. Créez les trois sous-réseaux dans chacune des zones de disponibilité où les serveurs sont présents.

- **Gestion**. Sous-réseau existant dans votre Virtual Private Cloud (VPC) dédié à la gestion. Citrix ADC doit contacter les services AWS et nécessite un accès Internet. Configurez une Gateway NAT et ajoutez une entrée de table de routage pour autoriser l'accès Internet à partir de ce sous-réseau.

  > **Remarque**
  >
  > Assurez-vous d'ouvrir `27000` et `7279` les ports dans Citrix ADM. Ces ports sont utilisés pour extraire les licences Citrix ADC de Citrix ADM. Pour de plus amples informations, consultez la section Ports.

- **Client**. Sous-réseau existant dans votre Virtual Private Cloud (VPC) dédié au trafic côté client. Généralement, Citrix ADC reçoit le trafic client pour l'application via un sous-réseau public à partir d'Internet. Associez le sous-réseau client à une table de routage comportant un itinéraire vers une Gateway Internet. Ce sous-réseau permet à Citrix ADC de recevoir du trafic d'application à partir d'Internet.

- **Serveur**. Sous-réseau existant dans votre Virtual Private Cloud (VPC) dédié au trafic côté serveur. ADC envoie du trafic aux serveurs d'applications back-end via ce sous-réseau. Tous vos serveurs d'applications qui reçoivent le trafic d'application doivent être présents dans ce sous-réseau. Si les serveurs sont en dehors de ce sous-réseau, le trafic de l'application est reçu via la passerelle du sous-réseau.

Créer des groupes de sécurité

Créez un groupe de sécurité pour contrôler le trafic entrant et sortant dans l'instance Citrix ADC VPX. Créez des règles pour le trafic entrant et sortant que vous souhaitez contrôler dans les groupes Citrix Autoscale. Vous pouvez ajouter autant de règles que vous voulez.

- **Gestion**. Groupe de sécurité existant dans votre compte dédié à la gestion de Citrix ADC VPX. Les règles entrantes sont autorisées sur les ports TCP et UDP suivants.
  - TCP : 80, 22, 443, 3008—3011, 4001, 27000, 7279

  - UDP : 67, 123, 161, 500, 3003, 4500, 7000

  Assurez-vous que le groupe de sécurité permet à l'agent Citrix ADM d'accéder au VPX.

- **Client**. Groupe de sécurité existant dans votre compte dédié à la communication côté client des instances Citrix ADC VPX. En règle générale, les règles entrantes sont autorisées sur les ports TCP 80 et 443. Et, le port 60000 est nécessaire pour surveiller l'intégrité des instances ADC.
- **Serveur**. Groupe de sécurité existant dans votre compte dédié à la communication côté serveur de Citrix ADC VPX. Généralement, il bloque toutes les règles entrantes et permet aux règles sortantes d'atteindre l'ensemble du VPC.

Créer des rôles IAM

Créez des entités IAM qui accordent l'autorisation aux instances ADM et ADC d'effectuer des opérations sur votre compte AWS. Le SMA crée ou supprime les éléments suivants de votre compte AWS :

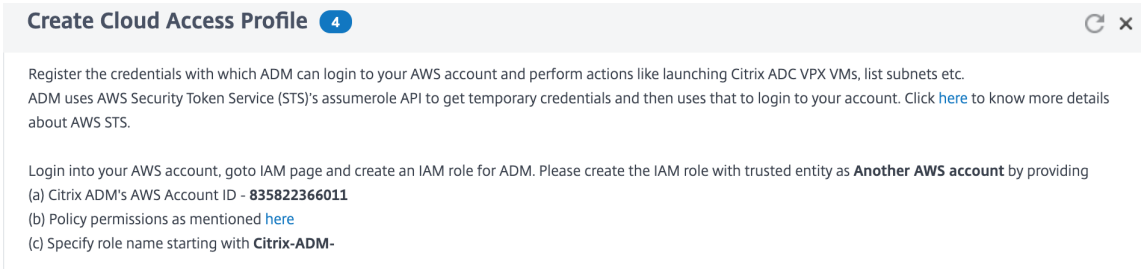
- Instances Citrix ADC EC2
- Équilibreurs de charge dans le cloud
- Route53

> **Remarque**
>
> Assurez-vous que les noms de rôle commencent par « Citrix-adm- » et que le nom du profil d'instance commence par « Citrix-ADC-. »

Pour créer des entités IAM pour ADM

Créez un rôle IAM afin de pouvoir établir une relation d'approbation entre votre compte AWS et le compte AWS de Citrix à l'aide d'une stratégie IAM qui permet à ADM d'effectuer des opérations sur votre compte AWS.

1. Dans **AWS**, cliquez sur **Services**. Dans le volet de navigation de gauche, sélectionnez **IAM > Rôles**, puis cliquez sur **Créer un rôle**.
2. Vous connectez votre compte AWS au compte AWS dans Citrix ADM. Sélectionnez donc **un autre compte AWS** pour permettre à Citrix ADM d'effectuer des actions dans votre compte AWS.
3. Saisissez l'ID de compte Citrix ADM AWS à 12 chiffres. L'ID Citrix est 835822366011. Vous pouvez laisser l'ID externe vide maintenant. Plus tard, vous devez modifier le rôle IAM. Spécifiez l'ID externe fourni par ADM lors de la création du profil d'accès au cloud dans ADM.



4. Cliquez sur **Autorisations**.
5. Dans la page **Attacher des stratégies d'autorisation**, cliquez sur **Créer une stratégie** .
6. Vous pouvez créer et modifier une stratégie dans l'éditeur visuel ou à l'aide de JSON.

   La liste des autorisations de Citrix pour Citrix ADM est fournie dans la zone suivante :

```
{

"Version": "2012-10-17",
"Statement": [
    {

        "Action": [
            "tag:GetResources",
            "tag:TagResources",
            "tag:UntagResources",
            "tag:getTagKeys",
            "tag:getTagValues",
            "ec2:DescribeInstances",
            "ec2:UnmonitorInstances",
            "ec2:MonitorInstances",
            "ec2:CreateKeyPair",
            "ec2:ResetInstanceAttribute",
            "ec2:ReportInstanceStatus",
            "ec2:DescribeVolumeStatus",
            "ec2:StartInstances",
            "ec2:DescribeVolumes",
            "ec2:UnassignPrivateIpAddresses",
            "ec2:DescribeKeyPairs",
            "ec2:CreateTags",
            "ec2:ResetNetworkInterfaceAttribute",
            "ec2:ModifyNetworkInterfaceAttribute",
            "ec2:DeleteNetworkInterface",
            "ec2:RunInstances",
            "ec2:StopInstances",
            "ec2:AssignPrivateIpAddresses",
            "ec2:DescribeVolumeAttribute",
```



```
            "ec2:DescribeInstanceCreditSpecifications",
            "ec2:CreateNetworkInterface",
            "ec2:DescribeImageAttribute",
            "ec2:AssociateAddress",
            "ec2:DescribeSubnets",
            "ec2:DeleteKeyPair",
            "ec2:DisassociateAddress",
            "ec2:DescribeAddresses",
            "ec2:DeleteTags",
            "ec2:RunScheduledInstances",
            "ec2:DescribeInstanceAttribute",
            "ec2:DescribeRegions",
            "ec2:DescribeDhcpOptions",
            "ec2:GetConsoleOutput",
            "ec2:DescribeNetworkInterfaces",
            "ec2:DescribeAvailabilityZones",
            "ec2:DescribeNetworkInterfaceAttribute",
            "ec2:ModifyInstanceAttribute",
            "ec2:DescribeInstanceStatus",
            "ec2:ReleaseAddress",
            "ec2:RebootInstances",
            "ec2:TerminateInstances",
            "ec2:DetachNetworkInterface",
            "ec2:DescribeIamInstanceProfileAssociations",
            "ec2:DescribeTags",
            "ec2:AllocateAddress",
            "ec2:DescribeSecurityGroups",
            "ec2:DescribeHosts",
            "ec2:DescribeImages",
            "ec2:DescribeVpcs",
            "ec2:AttachNetworkInterface",
            "ec2:AssociateIamInstanceProfile",
            "ec2:DescribeAccountAttributes",
            "ec2:DescribeInternetGateways"
        ],
        "Resource": "\*",
        "Effect": "Allow",
        "Sid": "VisualEditor0"
     }
,
    {

        "Action": [
            "iam:GetRole",
            "iam:PassRole",
```



```
77              "iam:CreateServiceLinkedRole"
78          ],
79          "Resource": "\*",
80          "Effect": "Allow",
81          "Sid": "VisualEditor1"
82       }
83  ,
84      {
85
86          "Action": [
87              "route53:CreateHostedZone",
88              "route53:CreateHealthCheck",
89              "route53:GetHostedZone",
90              "route53:ChangeResourceRecordSets",
91              "route53:ChangeTagsForResource",
92              "route53:DeleteHostedZone",
93              "route53:DeleteHealthCheck",
94              "route53:ListHostedZonesByName",
95              "route53:GetHealthCheckCount"
96              "route53:ListResourceRecordSets",
97              "route53.AssociateVPCWithHostedZone",
98          ],
99          "Resource": "\*",
100         "Effect": "Allow",
101         "Sid": "VisualEditor2"
102      }
103 ,
104     {
105
106         "Action": [
107             "iam:ListInstanceProfiles",
108             "iam:ListAttachedRolePolicies",
109             "iam:SimulatePrincipalPolicy",
110             "iam:SimulatePrincipalPolicy"
111         ],
112         "Resource": "\*",
113         "Effect": "Allow",
114         "Sid": "VisualEditor3"
115      }
116 ,
117     {
118
119         "Action": [
120             "ec2:ReleaseAddress",
121             "elasticloadbalancing:DeleteLoadBalancer",
```



```
122                 "ec2:DescribeAddresses",
123                 "elasticloadbalancing:CreateListener",
124                 "elasticloadbalancing:CreateLoadBalancer",
125                 "elasticloadbalancing:RegisterTargets",
126                 "elasticloadbalancing:CreateTargetGroup",
127                 "elasticloadbalancing:DeregisterTargets",
128                 "ec2:DescribeSubnets",
129                 "elasticloadbalancing:DeleteTargetGroup",
130                 "elasticloadbalancing:ModifyTargetGroupAttributes",
131                 "elasticloadbalancing:DescribeLoadBalancers",
132                 "ec2:AllocateAddress"
133             ],
134             "Resource": "*",
135             "Effect": "Allow",
136             "Sid": "VisualEditor4"
137         }
138
139     ]
140   }
141
142
143 <!--NeedCopy-->
```

7. Copiez et collez la liste des autorisations dans l'onglet JSON et cliquez sur **Revoir la stratégie**.
8. Dans la page **Vérifier la stratégie**, tapez un nom pour la stratégie, entrez une description, puis cliquez sur **Créer une stratégie**.

   > **Remarque**
   >
   > Assurez-vous que le nom commence par « Citrix-ADM-. »

9. Dans la page **Créer un rôle**, entrez le nom du rôle.

   > **Remarque**
   >
   > Assurez-vous que le nom du rôle commence par « Citrix-ADM-. »

Pour créer des entités IAM pour les CAN créés par ADM

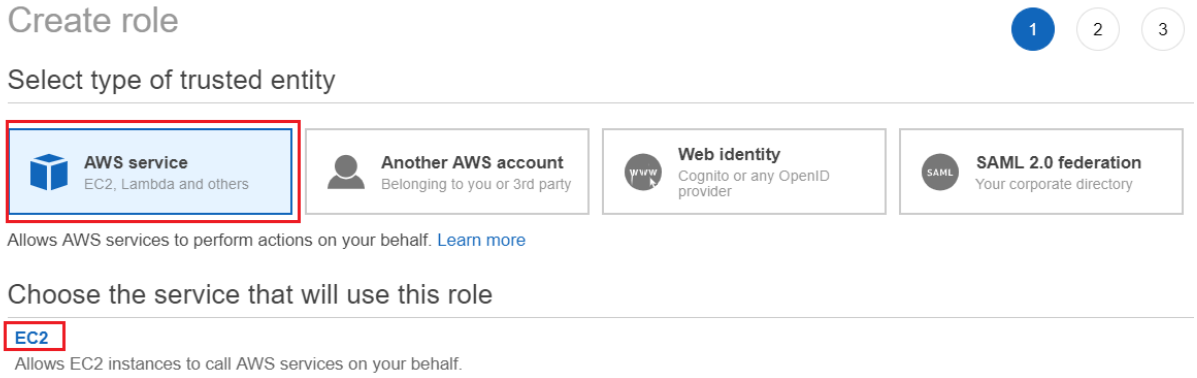
Créez un rôle IAM avec une stratégie IAM qui permet à un ADC d'effectuer des opérations sur votre compte AWS. Ce rôle est associé aux instances ADC qui seront créées par ADM, ce qui permet aux ADC d'accéder à votre compte.

1. Dans **AWS**, cliquez sur **Services**. Dans le volet de navigation de gauche, sélectionnez **IAM > Rôles**, puis cliquez sur **Créer un rôle**.

De même, créez un profil pour les instances de Citrix ADC en fournissant un nom différent commençant par « Citrix-ADC- ».

Assurez-vous de sélectionner le **service AWS > EC2**,

1. Dans la page **Attacher des stratégies d'autorisation**, cliquez sur **Créer une stratégie**.
2. Vous pouvez créer et modifier une stratégie dans l'éditeur visuel ou à l'aide de JSON.



La liste des autorisations des instances ADC Citrix pour Citrix est fournie dans la zone suivante :

```
{

  "Version": "2012-10-17",
  "Statement": [
    {

      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "iam:SimulatePrincipalPolicy",
        "autoscaling:\*",
        "sns:\*",
        "sqs:\*",
        "cloudwatch:\*",
        "ec2:AssignPrivateIpAddresses",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DetachNetworkInterface",
        "ec2:AttachNetworkInterface",
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource": "*"
```



```
25        }
26
27     ]
28    }
29
30  <!--NeedCopy-->
```

Enregistrer le domaine DNS

Assurez-vous d'avoir enregistré le domaine DNS pour héberger vos applications.

Évaluez le nombre d'adresses IP élastiques (EIP) requises dans votre réseau.

Le nombre d'EIP requis varie selon que vous déployez une mise à l'échelle automatique basée sur DNS ou une mise à l'échelle automatique basée sur NLB. Pour augmenter le nombre d'EIP, créez un dossier avec AWS.

- Pour la mise à l'échelle automatique basée sur le DNS, le nombre d'EIP requis par zone de disponibilité est égal au nombre d'applications multiplié par le nombre maximal d'instances VPX que vous souhaitez configurer dans les groupes Autoscale.
- Pour la mise à l'échelle automatique basée sur la NLB, le nombre d'EIP requis est égal au nombre d'applications multiplié par le nombre de zones de disponibilité dans lesquelles les applications sont déployées.

Évaluer les exigences en matière de limite d'instance

Lors de l'évaluation des limites d'instance, assurez-vous de tenir compte également de l'espace requis pour les instances Citrix ADC.

Conditions préalables pour Citrix ADM

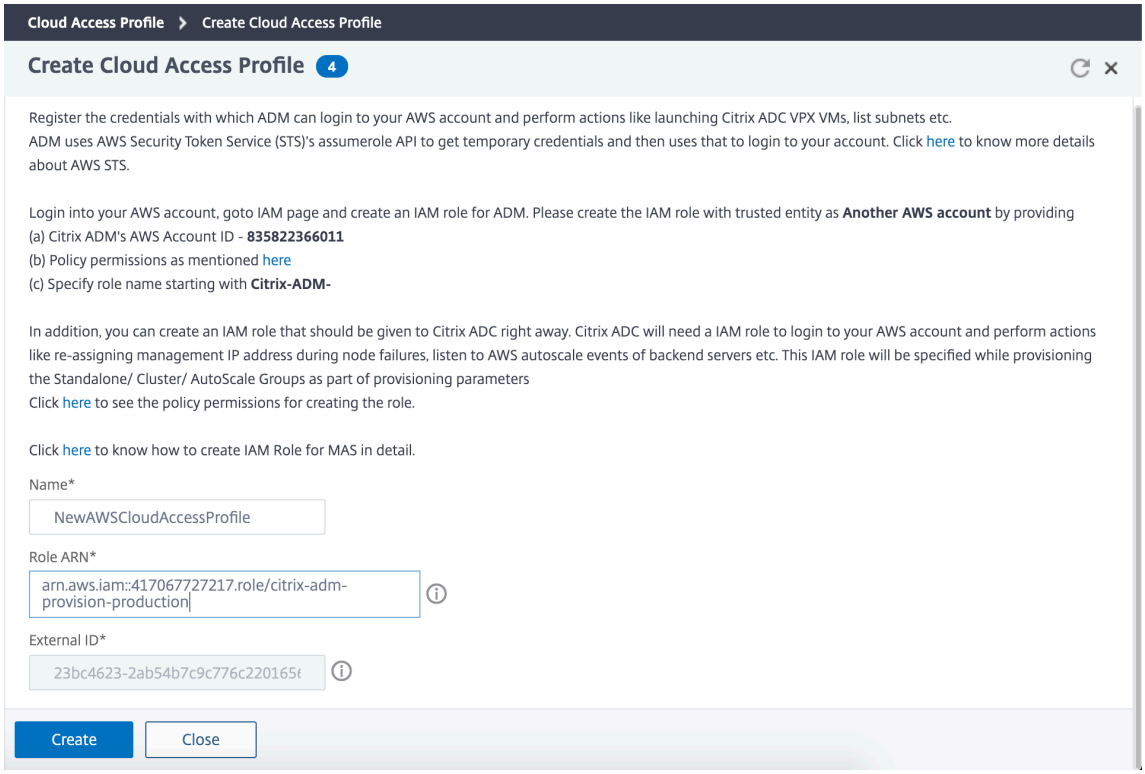
Vérifiez que vous avez rempli toutes les conditions préalables sur Citrix ADM pour utiliser la fonctionnalité de mise à l'échelle automatique.

Créer un site

Créez un site dans Citrix ADM et ajoutez les détails du VPC associé à votre rôle AWS.

1. Dans Citrix ADM, accédez à **Réseaux > Sites**.
2. Cliquez sur **Ajouter**.
3. Sélectionnez le type de service en tant qu'AWS et activez **Utiliser un VPC existant en tant que site**.

4. Sélectionnez le profil d'accès au cloud.
5. Si le profil d'accès au nuage n'existe pas dans le champ, cliquez sur **Ajouter** pour créer un profil.
    a) Dans la page **Créer un profil d'accès au cloud**, tapez le nom du profil avec lequel vous souhaitez accéder à AWS.
    b) Tapez l'ARN associé au rôle que vous avez créé dans AWS.
    c) Copiez l' **ID externe** généré automatiquement pour mettre à jour le rôle IAM.
6. Cliquez sur **Créer**.
7. Cliquez à nouveau sur **Créer** pour créer le site.
8. Mettez à jour le rôle IAM dans AWS à l'aide de l' **ID externe**généré automatiquement :



    a) Connectez-vous à votre compte AWS et accédez au rôle que vous souhaitez mettre à jour.
    b) Dans l'onglet **Relations d'approbation**, cliquez sur **Modifier la relation d'approbation** et ajoutez la condition suivante dans le`Statement` bloc :

```
"Condition": {

  "StringEquals": {

    "sts:ExternalId": "<External-ID>"
   }

```



```
 }

<!--NeedCopy-->
```

L'activation de l'ID externe pour un rôle IAM dans AWS vous permet de vous connecter à un compte tiers. L'ID externe augmente la sécurité de votre rôle.

Les détails du VPC, tels que la région, l'ID du VPC, le nom et le bloc CIDR, associés à votre rôle IAM dans AWS sont importés dans Citrix ADM.

Provisionner l'agent Citrix ADM sur AWS

L'agent de service Citrix ADM fonctionne comme intermédiaire entre Citrix ADM et les instances découvertes dans le centre de données ou sur le cloud.

1. Accédez à **Réseaux > Agents**.
2. Cliquez sur **Provisionner**.
3. Sélectionnez **AWS** et cliquez sur **Suivant** .
4. Dans l'onglet **Paramètres du nuage**, spécifiez les éléments suivants :
   - **Nom** : spécifiez le nom de l'agent Citrix ADM.
   - **Site** : sélectionnez le site que vous avez créé pour provisionner un agent et des instances VPX ADC.
   - **Profil d'accès au nuage** : sélectionnez le profil d'accès au nuage dans la liste.
   - **Zone de disponibilité** : sélectionnez les zones dans lesquelles vous souhaitez créer les groupes de mise à l'Autoscale. Selon le profil d'accès au nuage que vous avez sélectionné, les zones de disponibilité spécifiques à ce profil sont remplies.
   - **Groupe de** sécurité : les groupes de sécurité contrôlent le trafic entrant et sortant dans l'agent Citrix ADC. Vous créez des règles pour le trafic entrant et sortant que vous souhaitez contrôler.
   - **Sous-réseau** : sélectionnez le sous-réseau de gestion dans lequel vous souhaitez provisionner un agent.
   - **Tags** - Tapez la paire clé-valeur pour les balises du groupe Autoscale. Une balise est constituée d'une paire clé-valeur sensible à la casse. Ces balises vous permettent d'organiser et d'identifier facilement les groupes de mise à l'échelle automatique. Les balises sont appliquées à AWS et à Citrix ADM.
5. Cliquez sur **Terminer**.

Vous pouvez également installer l'agent Citrix ADM à partir du site AWS Marketplace. Pour de plus amples informations, consultez la section Installation de l'agent Citrix ADM sur AWS.

Créer des groupes de mise à l'échelle automatique

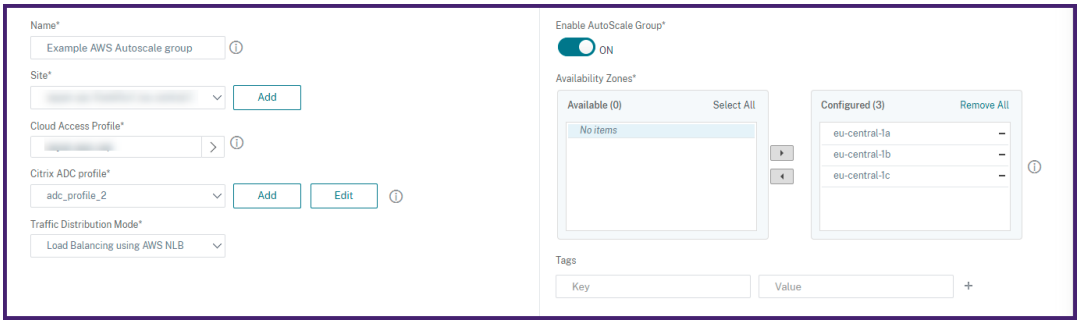
Initialiser la configuration de mise à l'échelle automatique

1. Dans Citrix ADM, accédez à **Réseaux > Groupes de mise à l'échelle automatique**.
2. Cliquez sur **Ajouter** pour créer des groupes de mise à l'échelle automatique. La page **Créer un groupe de mise à l'échelle automatique** s'affiche.
3. Entrez les détails suivants.
   - **Nom**. Saisissez un nom pour le groupe Mise à l'échelle automatique.
   - **Site**. Sélectionnez le site que vous avez créé pour provisionner les instances Citrix ADC VPX sur AWS.
   - **Agent**. Sélectionnez l'agent Citrix ADM qui gère les instances provisionnées.
   - **Profil d'accès au cloud**. Sélectionnez le profil d'accès au cloud.

   -**Note**. Si le profil d'accès au nuage n'existe pas dans le champ, cliquez sur **Ajouter** pour créer un profil.

   - Tapez l'ARN associé au rôle que vous avez créé dans AWS.
   - Tapez l'ID externe que vous avez fourni lors de la création d'un rôle IAM (Identity and Access Management) dans AWS. Selon le profil d'accès au nuage que vous sélectionnez, les zones de disponibilité sont remplies.

   - **Profil du périphérique**. Sélectionnez le profil de périphérique dans la liste. Le profil de périphérique est utilisé par Citrix ADM chaque fois qu'il doit se connecter à l'instance.
   - **Mode de distribution du trafic**. L'option **Équilibrage de la charge à l'aide d'un équilibrage** de charge est sélectionnée comme mode de distribution du trafic par défaut. Si les applications utilisent le trafic UDP, sélectionnez **DNS utilisant AWS route53**.



Remarque

Une fois la configuration de l'échelle automatique configurée, il est impossible d'ajouter de nouvelles zones de disponibilité ou de supprimer des zones de disponibilité existantes.

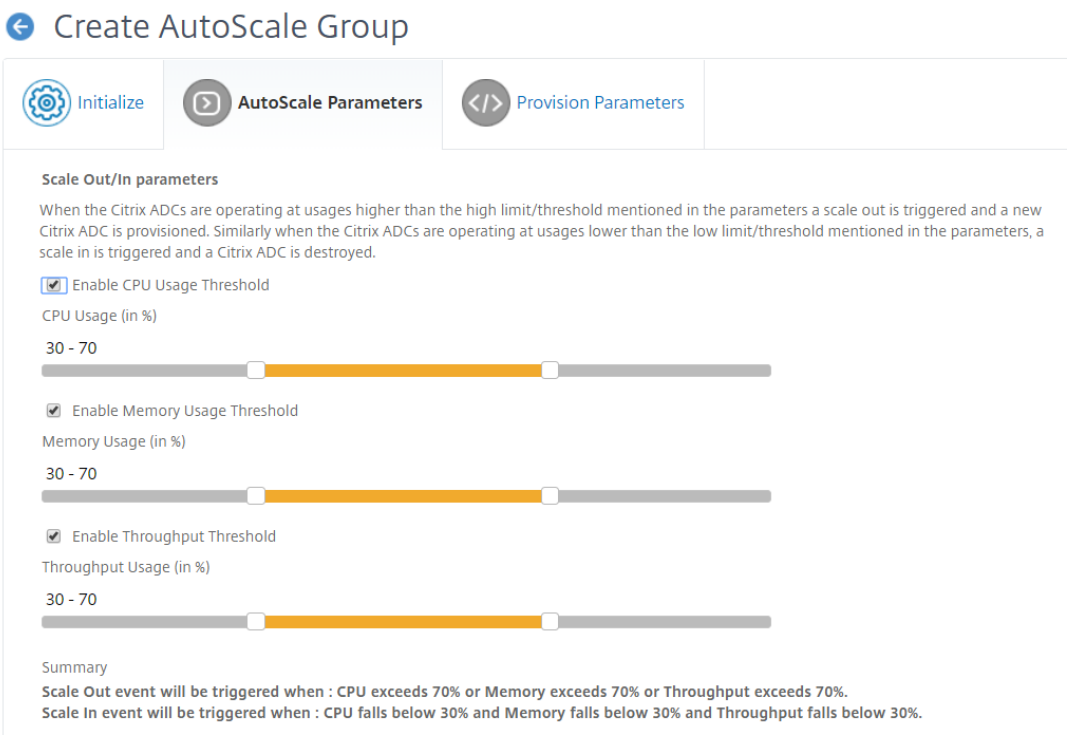
- **Activez le groupe AutoScale**. Activez ou désactivez l'état des groupes ASG. Cette option est activée par défaut. Si cette option est désactivée, la mise à l'échelle automatique n'est pas déclenchée.
- **Zones de disponibilité**. Sélectionnez les zones dans lesquelles vous souhaitez créer les groupes de mise à l'échelle automatique. Selon le profil d'accès au nuage que vous avez sélectionné, les zones de disponibilité spécifiques à ce profil sont remplies.
- **Étiquettes**. Tapez la paire clé-valeur pour les balises de groupe Échelle automatique. Une balise est constituée d'une paire clé-valeur sensible à la casse. Ces balises vous permettent d'organiser et d'identifier facilement les groupes de mise à l'échelle automatique. Les balises sont appliquées à AWS et à Citrix ADM.

4. Cliquez sur **Suivant**.

Configuration des paramètres de mise à l'échelle automatique

1. Dans l'onglet **Paramètres de mise à l'échelle automatique**, entrez les détails suivants.
2. Sélectionnez un ou plusieurs des paramètres de seuil suivants dont les valeurs doivent être surveillées pour déclencher une mise à l'échelle ou une mise à l'échelle.
   - **Activer le seuil d'utilisation du processeur** : surveillez les mesures en fonction de l'utilisation du processeur.
   - **Activer le seuil d'utilisation de la mémoire** : surveillez les mesures en fonction de l'utilisation de la mémoire.
   - **Activer le seuil de débit** : surveillez les mesures en fonction du débit.

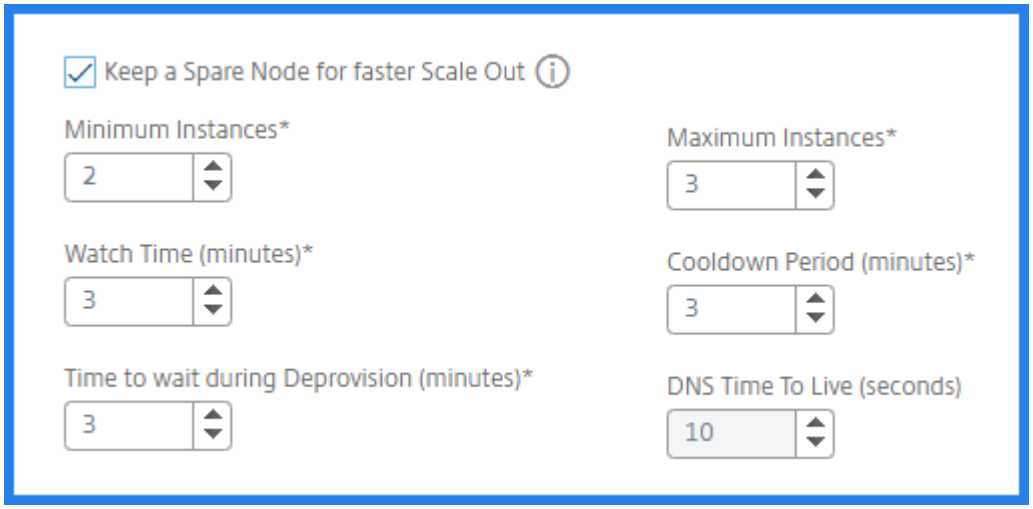
     > **Remarque**
     >
     > – La limite de seuil minimale par défaut est de 30 et la limite de seuil maximale est de 70. Toutefois, vous modifiez les limites.
     > – La limite minimale de seuil doit être égale ou inférieure à la moitié de la limite maximale de seuil.
     > – Plusieurs paramètres de seuil peuvent être sélectionnés pour la surveillance. Dans de tels cas, une mise à l'échelle est déclenchée si au moins un des paramètres de seuil est au-dessus du seuil maximal. Cependant, une mise à l'échelle n'est déclenchée que si tous les paramètres de seuil fonctionnent en dessous de leurs seuils normaux.



- **Conservez un nœud de rechange pour une mise à l'échelle plus rapide :** cette option permet d'obtenir une évolutivité plus rapide. ADM met en service un nœud de secours avant que l'action de mise à l'échelle ne se produise et l'arrête. Lorsque l'action de scale-out se produit pour le groupe Mise à l'Autoscale, l'ADM démarre le nœud de rechange déjà provisionné. En conséquence, il réduit le temps nécessaire pour la mise à l'échelle.
- **Instances minimales**. Sélectionnez le nombre minimal d'instances devant être provisionnées pour ce groupe de mise à l'échelle automatique.
- Par défaut, le nombre minimal d'instances est égal au nombre de zones sélectionnées. Vous pouvez incrémenter les instances minimales par des multiples du nombre de zones.
- Par exemple, si le nombre de zones de disponibilité est 4, le minimum d'instances est 4 par défaut. Vous pouvez augmenter les instances minimales de 8, 12, 16.
- **Nombre maximal d'instances**. Sélectionnez le nombre maximal d'instances devant être provisionnées pour ce groupe de mise à l'échelle automatique.
- Le nombre maximal d'instances doit être supérieur ou égal à la valeur minimale des instances. Le nombre maximal d'instances pouvant être configurées est égal au nombre de zones de disponibilité multiplié par 32.
- Nombre maximal d'instances = nombre de zones de disponibilité * 32
- **Délai de connexion de vidange (minutes)**. Sélectionnez le délai d'expiration de la connexion de drain. Pendant la mise à l'échelle, une fois qu'une instance est sélectionnée pour le déprovisionnement, Citrix ADM supprime l'instance du traitement des nouvelles

connexions au groupe Mise à l'Autoscale et attend l'expiration du délai spécifié avant le déprovisionnement. Cette option permet de drainer les connexions existantes à cette instance avant qu'elle ne soit déprovisionnée.

- **Période de recharge (minutes)**. Sélectionnez la période de recharge. Pendant la mise à l'échelle, la période de recharge correspond à la période pendant laquelle l'évaluation des statistiques doit être arrêtée après une mise à l'échelle. Cette mise à l'échelle permet une croissance organique des instances d'un groupe Autoscale en permettant au trafic actuel de se stabiliser et de se stabiliser sur l'ensemble actuel d'instances avant que la prochaine décision de mise à l'échelle ne soit prise.
- **Durée de vie du DNS (secondes)**. Sélectionnez la durée (en secondes) pendant laquelle un paquet est défini pour exister à l'intérieur d'un réseau avant d'être ignoré par un routeur. Ce paramètre n'est applicable que lorsque le mode de distribution du trafic est DNS utilisant AWS route53.
- **Temps de visionnage (minutes)**. Sélectionnez la durée de la surveillance. Durée pendant laquelle le seuil du paramètre d'échelle doit rester dépassé pour qu'une mise à l'échelle se produise. Si le seuil est dépassé sur tous les échantillons prélevés dans ce délai, une mise à l'échelle se produit.



3. Cliquez sur **Suivant**.

Configurer les licences pour le Provisioning des instances Citrix ADC

Sélectionnez l'un des modes suivants pour concéder des licences aux instances Citrix ADC qui font partie du groupe de mise à l'Autoscale :

- **Utilisation de Citrix ADM** : Lors du Provisioning d'instances Citrix ADC, le groupe Autoscale extrait les licences de Citrix ADM.

- **Utilisation du cloud AWS** : l'option **Allouer à partir du cloud** utilise les licences de produit Citrix disponibles sur AWS Marketplace. Lors du Provisioning des instances Citrix ADC, le groupe Autoscale utilise les licences du marché.

  Si vous choisissez d'utiliser des licences d'AWS Marketplace, spécifiez le produit ou la licence dans l'onglet **Paramètres de provisionnement**.

Pour de plus amples informations, consultez la section Exigences en matière de licences.

Utiliser les licences de Citrix ADM

1. Dans l'onglet **Licence**, sélectionnez **Allouer à partir d'ADM**.
2. Dans **Type de licence**, sélectionnez l'une des options suivantes dans la liste :
   - **Licences de bande passante :** vous pouvez sélectionner l'une des options suivantes dans la liste **Types de licences de bande passante** :
     - **Capacité groupée :** spécifiez la capacité à allouer pour chaque nouvelle instance du groupe Mise à l'échelle automatique.

       À partir du pool commun, chaque instance ADC du groupe Autoscale retire une licence d'instance et seule la bande passante est spécifiée.
     - **Licences VPX :** Lorsqu'une instance Citrix ADC VPX est provisionnée, l'instance extraire la licence auprès de Citrix ADM.
   - **Licences de processeur virtuel :** l'instance Citrix ADC VPX provisionnée récupère les licences en fonction du nombre de processeurs actifs exécutés dans le groupe Autoscale.

   > **Remarque**
   >
   > Lorsque les instances provisionnées sont supprimées ou détruites, les licences appliquées retournent au pool de licences Citrix ADM. Ces licences peuvent être réutilisées pour provisionner de nouvelles instances lors de la prochaine mise à l'Autoscale.
3. Dans **License Edition**, sélectionnez l'édition de licence. Le groupe Mise à l'échelle automatique utilise l'édition spécifiée pour provisionner des instances.
4. Cliquez sur **Suivant**.

Configurer les paramètres du cloud

1. Dans l'onglet **Paramètres du nuage**, entrez les détails suivants.
   - **Rôle IAM** : sélectionnez le rôle IAM que vous avez créé dans AWS. Un rôle IAM est une identité AWS avec des stratégies d'autorisation qui déterminent ce que l'identité peut ou ne peut pas faire dans AWS.

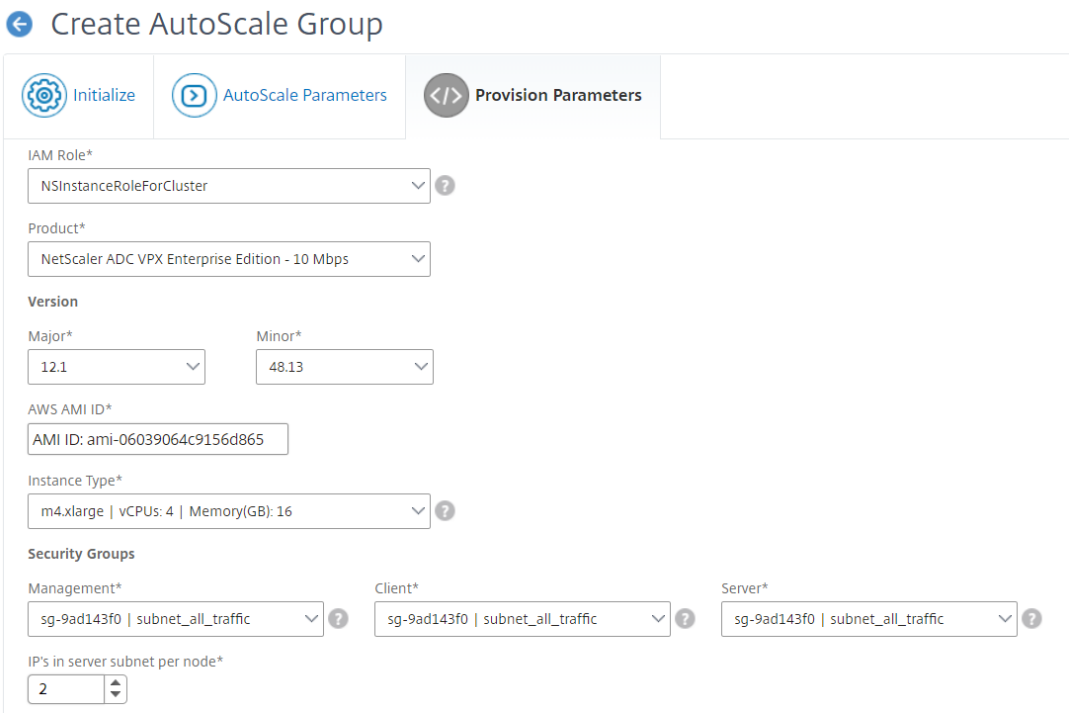
- **Produit** : sélectionnez la version du produit Citrix ADC à provisionner.
- **Version** : sélectionnez la version et le numéro de version du produit Citrix ADC. Les versions de version et les numéros de build sont remplis automatiquement en fonction du produit que vous avez sélectionné.
- **ID AMI AWS** : entrez l'ID AMI spécifique à la région que vous avez sélectionnée.
- **Type d'instance** : sélectionnez le type d'instance EC2.

  > **Remarque**
  >
  > Le type d'instance recommandé pour le produit sélectionné est renseigné automatiquement, par défaut.

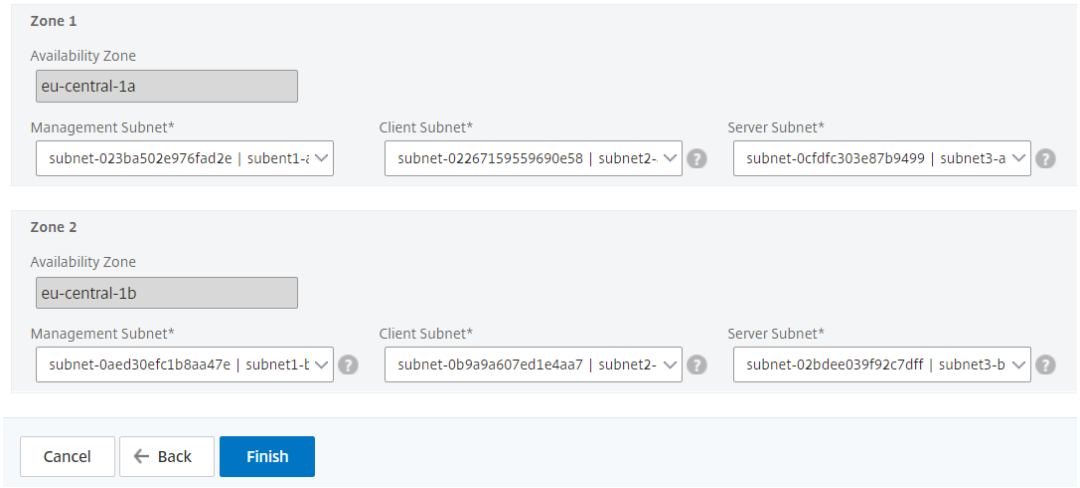
- **Groupes de**sécurité : les groupes de sécurité contrôlent le trafic entrant et sortant dans l'instance Citrix ADC VPX. Vous créez des règles pour le trafic entrant et sortant que vous souhaitez contrôler. Sélectionnez les valeurs appropriées pour les sous-réseaux suivants :
- **Gestion**. Groupe de sécurité existant dans votre compte dédié à la gestion des instances Citrix ADC VPX. Les règles entrantes sont autorisées sur les ports TCP et UDP suivants.

  TCP : 80, 22, 443, 3008-3011, 4001
  UDP : 67, 123, 161, 500, 3003, 4500, 7000

  Assurez-vous que le groupe de sécurité permet à l'agent Citrix ADM d'accéder au VPX.
- **Client**. Groupe de sécurité existant dans votre compte dédié à la communication côté client des instances Citrix ADC VPX. En règle générale, les règles entrantes sont autorisées sur les ports TCP 80, 22 et 443.
- **Serveur**. Groupe de sécurité existant dans votre compte dédié à la communication côté serveur de Citrix ADC VPX.
- **IP dans le sous-réseau serveur par nœud** : sélectionnez le nombre d'adresses IP dans le sous-réseau serveur par nœud pour le groupe de sécurité.

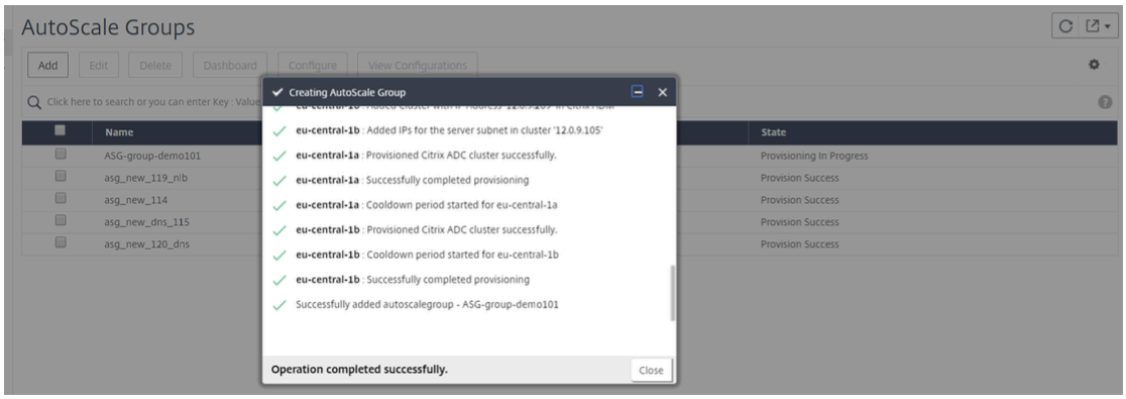


- **Zone** : Le nombre de zones remplies est égal au nombre de zones de disponibilité que vous avez sélectionnées. Pour chaque zone, sélectionnez les valeurs appropriées pour les sous-réseaux suivants :
- **Gestion**. Sous-réseau existant dans votre Virtual Private Cloud (VPC) dédié à la gestion. Citrix ADC doit contacter les services AWS et nécessite un accès Internet. Configurez une Gateway NAT et ajoutez une entrée de table de routage pour autoriser l'accès Internet à partir de ce sous-réseau.
- **Client**. Sous-réseau existant dans votre Virtual Private Cloud (VPC) dédié au côté client. En règle générale, Citrix ADC reçoit le trafic client pour l'application via un sous-réseau public à partir d'Internet. Associez le sous-réseau client à une table de routage comportant un itinéraire vers une Gateway Internet. Ce sous-réseau permet à Citrix ADC de recevoir le trafic d'application à partir d'Internet.
- **Serveur**. Les serveurs d'applications sont provisionnés dans un sous-réseau de serveur. Tous vos serveurs d'applications se trouvent dans ce sous-réseau et reçoivent le trafic d'application de Citrix ADC via ce sous-réseau.



2. Cliquez sur **Terminer**.

   Une fenêtre de progression avec le statut de création du groupe Autoscale apparaît. La création et le provisionnement de groupes de mise à l'Autoscale peuvent prendre plusieurs minutes.



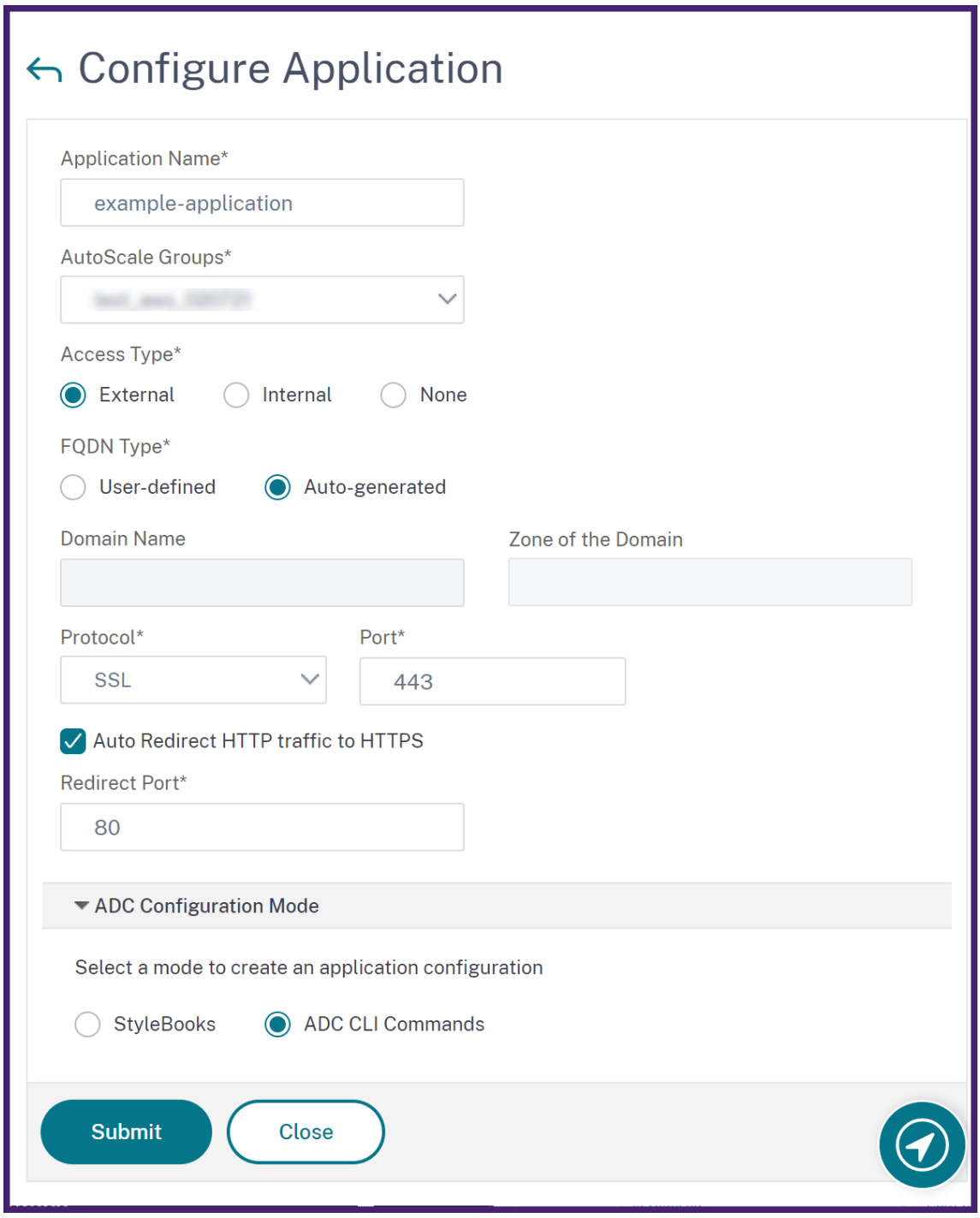
Configurer une application pour le groupe Autoscale

1. Dans Citrix ADM, accédez à **Réseaux** > **Groupes de mise à Autoscale**.
2. Sélectionnez le groupe de mise à l'échelle automatique que vous avez créé et cliquez sur **Configurer**.
3. Dans **Configurer l'application**, spécifiez les détails suivants :
   - **Nom de l'application** : spécifiez le nom d'une application.
   - **Type d'accès** : vous pouvez utiliser la solution de mise à l'échelle automatique ADM pour des applications externes et internes. Sélectionnez le type d'accès à l'application requis.
   - **Type de nom de domaine complet** - Sélectionnez un mode d'attribution de noms de domaine et de zone.

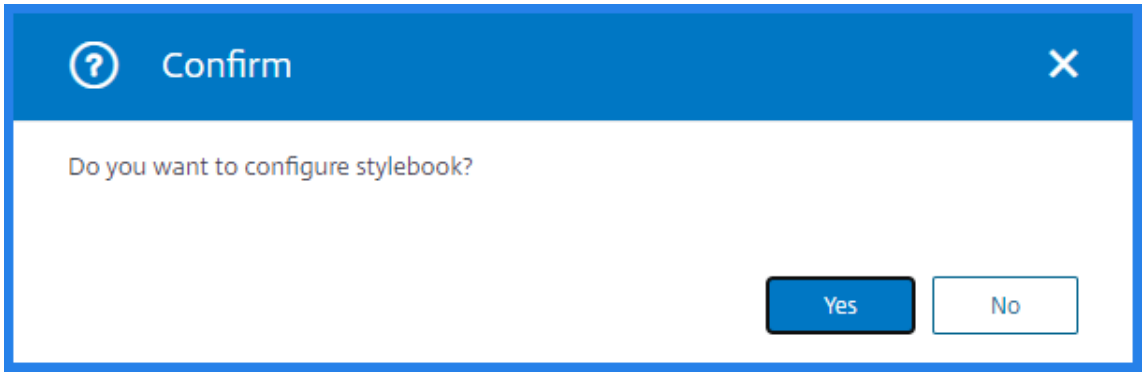
Si vous souhaitez spécifier manuellement, sélectionnez Définie **par l'utilisateur**. Pour attribuer automatiquement des noms de domaine et de zone, sélectionnez **Généré automatiquement**.

- **Nom de domaine** - Spécifiez le nom de domaine d'une application. Cette option s'applique uniquement lorsque vous sélectionnez Type de nom de domaine complet défini par l'utilisateur.
- **Zone du domaine** : sélectionnez le nom de zone d'une application dans la liste. Cette option s'applique uniquement lorsque vous sélectionnez Type de nom de domaine complet défini par l'utilisateur.

  Ce nom de domaine et de zone redirige vers les serveurs virtuels dans AWS. Par exemple, si vous hébergez une application dans `app.example.com`, le `app` est le nom de domaine et `example.com` le nom de la zone.
- **Protocole** : sélectionnez le type de protocole dans la liste. L'application configurée reçoit le trafic en fonction du type de protocole sélectionné.
- **Port** : spécifiez la valeur du port. Le port spécifié est utilisé pour établir une communication entre l'application et le groupe Mise à l'Autoscale.



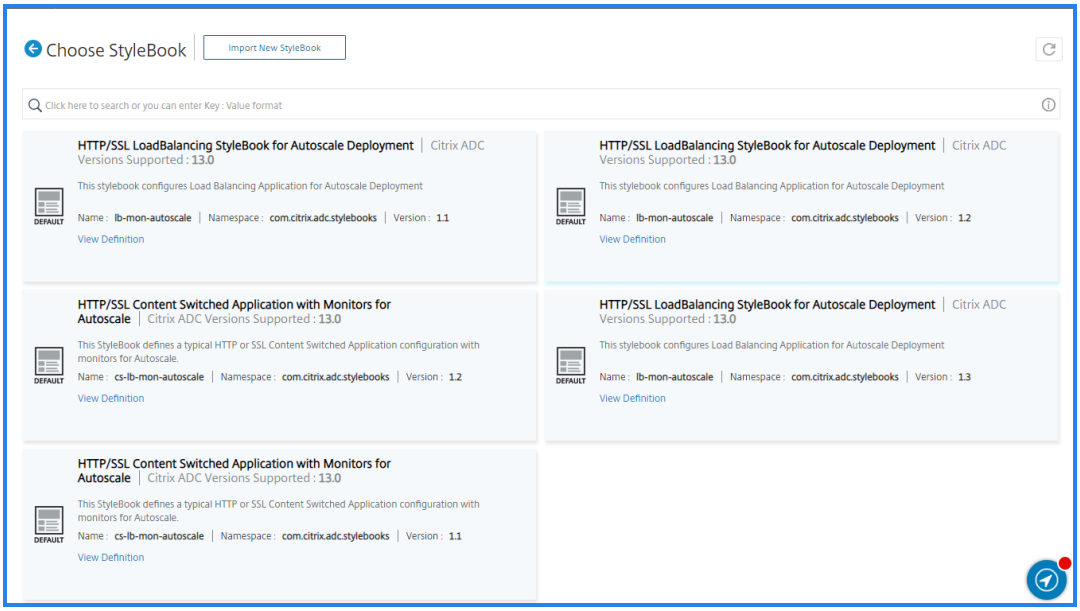
Si vous souhaitez configurer une application à l'aide de StyleBooks, sélectionnez **Oui** dans la fenêtre de confirmation.



> **Remarque**
>
> Modifiez le type d'accès d'une application si vous souhaitez modifier les détails suivants à l'avenir :
>
> - Type de nom de domaine complet
> - Nom de domaine
> - Zone du domaine

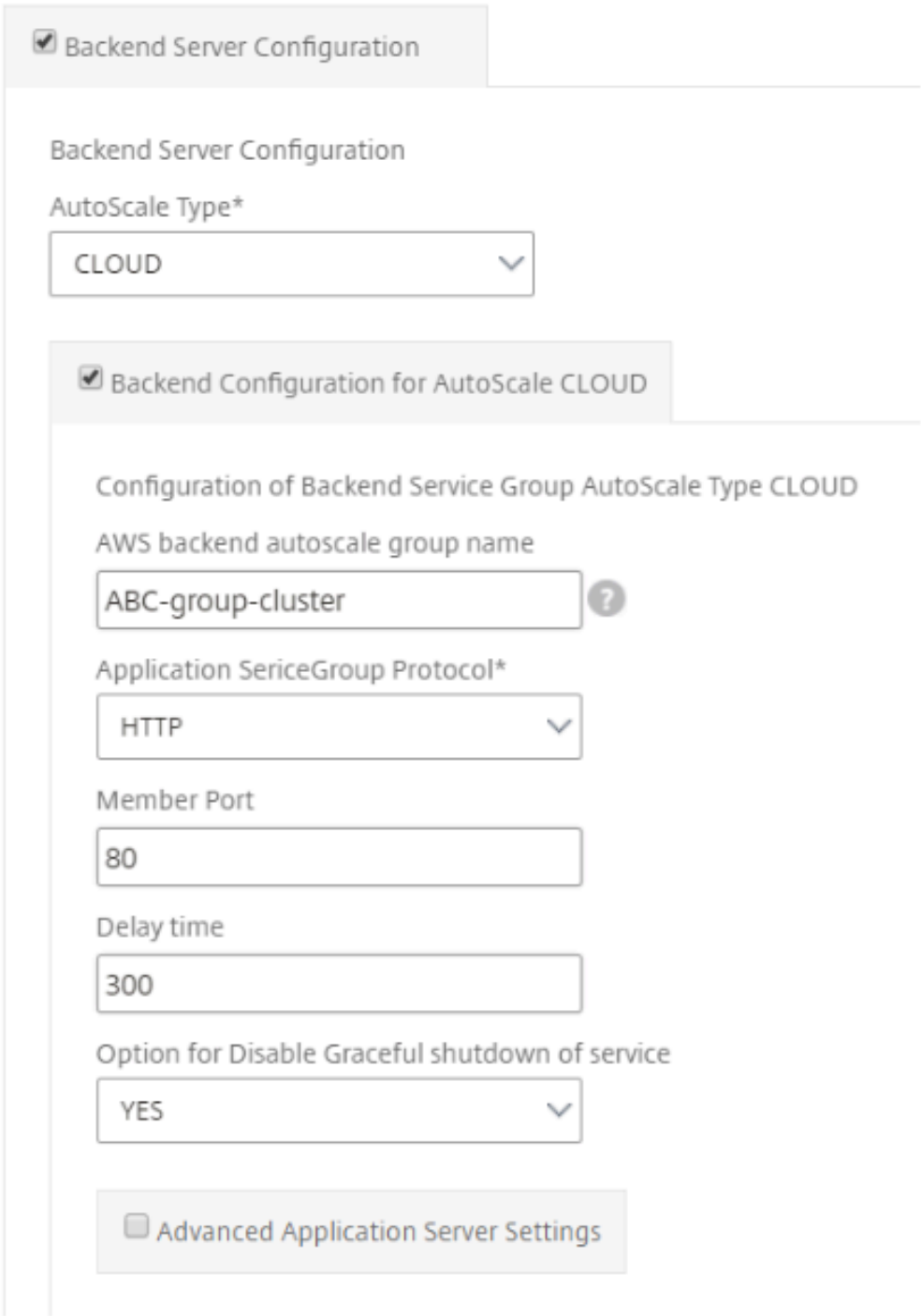
4. La page **Choisir un StyleBook** affiche tous les StyleBooks disponibles pour déployer des configurations dans les clusters de mise à l'échelle automatique.

   - Sélectionnez le StyleBook approprié. Par exemple, vous pouvez utiliser le **HTTP/SSL Loadbalancing StyleBook**. Vous pouvez également importer de nouveaux StyleBooks.



   - Cliquez sur le StyleBook pour créer la configuration requise.
     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.
   - Entrez des valeurs pour tous les paramètres.

- Si vous créez des serveurs back-end dans AWS, sélectionnez Configuration du serveur principal. Sélectionnez ensuite **AWS EC2 Autoscaling** > **Cloud** et entrez les valeurs de tous les paramètres.



- Il peut y avoir quelques configurations facultatives requises en fonction du StyleBook que vous avez choisi. Par exemple, vous devrez peut-être créer des moniteurs, fournir des paramètres de certificat SSL, etc.

- Cliquez sur **Créer** pour déployer la configuration sur le cluster Citrix ADC.

- Le nom de domaine complet de l'application ou du serveur virtuel ne peut pas être modifié après sa configuration et son déploiement.

  Le nom de domaine complet de l'application est résolu à l'adresse IP à l'aide du DNS. Comme cet enregistrement DNS peut être mis en cache sur différents serveurs de noms, la modification du nom de domaine complet peut entraîner le blocage du trafic.

- Le partage de session SSL fonctionne comme prévu dans une zone de disponibilité mais entre les zones de disponibilité nécessite une réauthentification.

  Les sessions SSL sont synchronisées au sein du cluster. Comme le groupe de mise à l'échelle automatique couvrant les zones de disponibilité dispose de clusters distincts dans chaque zone, les sessions SSL ne peuvent pas être synchronisées entre les zones.

- Les limites partagées telles que le client max et le débordement sont définies statiquement en fonction du nombre de zones de disponibilité. Définissez cette limite après l'avoir calculée manuellement. `Limit = \<Limit required\>/\<number of zones\>`.

  Les limites partagées sont distribuées automatiquement entre les nœuds d'un cluster. Comme le groupe de mise à l'échelle automatique couvrant les zones de disponibilité dispose de clusters distincts dans chaque zone, ces limites doivent être calculées manuellement.

Mettre à niveau les clusters Citrix ADC

Mettez à niveau manuellement les nœuds de cluster. Vous mettez d'abord à niveau l'image des nœuds existants, puis mettez à jour l'AMI à partir de Citrix ADM.

> **Important**
>
> Assurez-vous de ce qui suit lors d'une mise à niveau :
>
> - Aucune scale-in ou scale-out n'est déclenchée.
> - Aucune modification de configuration ne doit être effectuée sur le cluster du groupe Mise à l'échelle automatique.
> - Vous conservez une sauvegarde du fichier `ns.conf` de la version précédente. En cas d'échec d'une mise à niveau, vous pouvez revenir à la version précédente.

Procédez comme suit pour mettre à niveau les nœuds de cluster Citrix ADC.

1. Désactivez le groupe Autoscale sur le portail MAS ASG.
2. Sélectionnez l'un des clusters dans les groupes Mise à l'échelle automatique pour la mise à niveau.
3. Suivez les étapes décrites dans la rubrique Mise à niveau ou rétrogradation du cluster Citrix ADC.

> **Remarque**
>
> - Mettez à niveau un nœud dans le cluster.
> - Surveillez le trafic de l'application pour détecter toute défaillance.
> - Si vous rencontrez des problèmes ou des échecs, rétrogradez le nœud qui a été précédemment mis à niveau. Sinon, continuez avec la mise à niveau de tous les nœuds.

4. Continuez à mettre à niveau les nœuds de tous les clusters du groupe Autoscale.

> **Remarque**
>
> Si la mise à niveau d'un cluster échoue, rétrogradez tous les clusters du groupe Mise à l'échelle automatique vers la version précédente. Suivez les étapes décrites dans la rubriqueMise à niveau ou rétrogradation du cluster Citrix ADC.

5. Après la mise à niveau réussie de tous les clusters, mettez à jour l'AMI sur MAS ASG Portal. L'AMI doit être de la même version que l'image utilisée pour la mise à niveau.
6. Modifiez le groupe de mise à l'échelle automatique et tapez l'AMI correspondant à la version mise à niveau.
7. Activez le groupe Mise à l'échelle automatique sur le portail ADM.

Modifier la configuration des groupes de mise à l'échelle automatique

- Vous pouvez modifier une configuration de groupe de mise à l'échelle automatique ou supprimer un groupe de mise à l'échelle automatique. Vous ne pouvez modifier que les paramètres de groupe d'échelle automatique suivants.
  - Mode de distribution du trafic
  - Limites maximales et minimales des paramètres de seuil
  - Valeurs d'instance minimales et maximales
  - Valeur de la période de drainage des connexions
  - Valeur de la période de recharge
  - Durée de vie : si le mode de distribution du trafic est DNS
  - Valeur de durée de la surveillance
- Vous pouvez également supprimer les groupes de mise à l'échelle automatique après leur création.

  Lorsque vous supprimez un groupe de mise à l'échelle automatique, tous les domaines et adresses IP sont désenregistrés de DNS/NLB et les nœuds de cluster sont déprovisionnés.

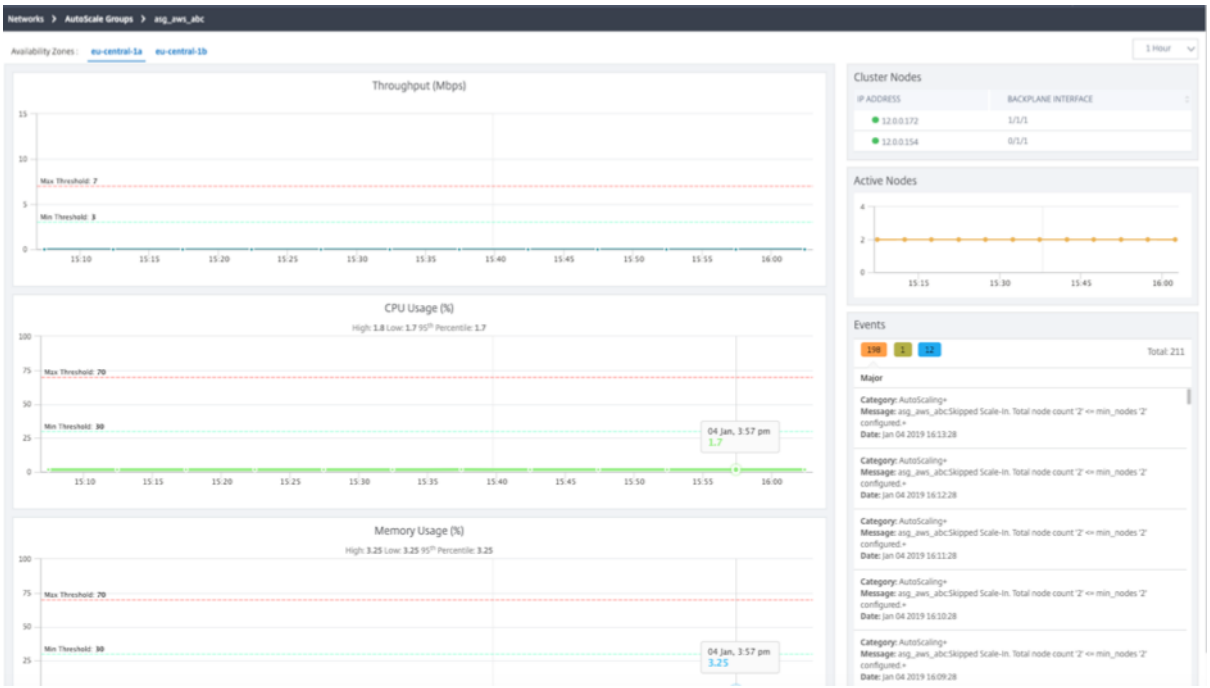
Tableau de bord

April 29, 2021

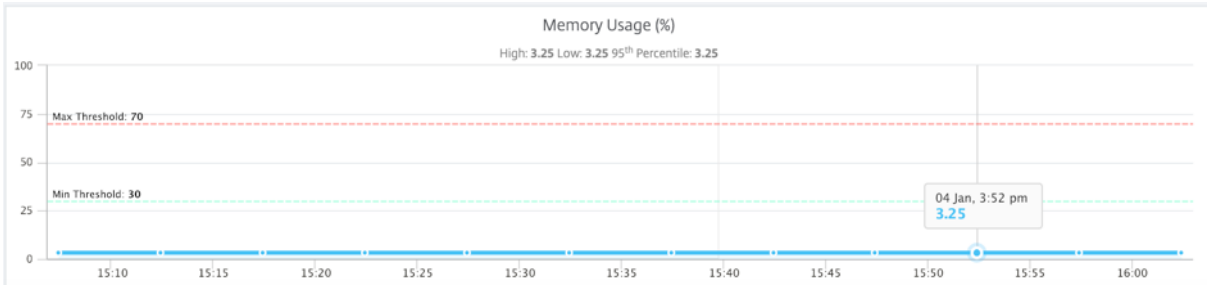
1. Dans Citrix ADM, accédez à **Réseaux > Groupes de mise à l'échelle automatique**.
2. Sélectionnez le groupe Autoscale et cliquez sur **Tableau de bord**.

Vous pouvez afficher le graphique des paramètres de surveillance sélectionnés. Le panneau de droite affiche les événements qui déclenchent la mise à l'échelle automatique. Le panneau de gauche affiche les nœuds actifs dans le cluster par zone, le graphique des nœuds actifs et les événements.

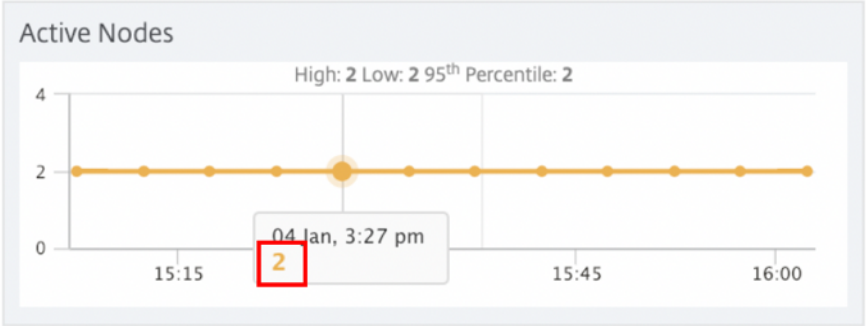
La figure suivante affiche un exemple de tableau de bord.



La figure suivante affiche les événements d'utilisation de la mémoire dans le tableau de bord Autoscale.



La figure suivante affiche le graphique des nœuds actifs. Le nombre sous l'horodatage indique le nombre de nœuds actifs. Vous pouvez afficher à tout moment le nombre de nœuds actifs qui font partie de la zone de disponibilité.



Provisionnement d'instances Citrix ADC VPX sur Microsoft Azure

April 29, 2021

Les applications ou services hébergés sur Azure nécessitent une gestion sécurisée du trafic et une optimisation efficace des ressources réseau ainsi que des avantages du cloud. Les instances Citrix ADC VPX provisionnées sur Microsoft Azure offrent une gestion sécurisée du trafic, une consommation optimisée des ressources et une réduction des coûts de propriété des applications Web.

Citrix ADM vous permet d'automatiser le déploiement, la configuration et la gestion des instances ADC VPX sur Azure. Le provisionnement d'instances Citrix ADC VPX à l'aide d'ADM combine l'élasticité et la flexibilité du cloud avec les fonctionnalités de contrôle de Citrix ADC.

Images de machines virtuelles Citrix ADC Azure prises en charge pour le Provisioning

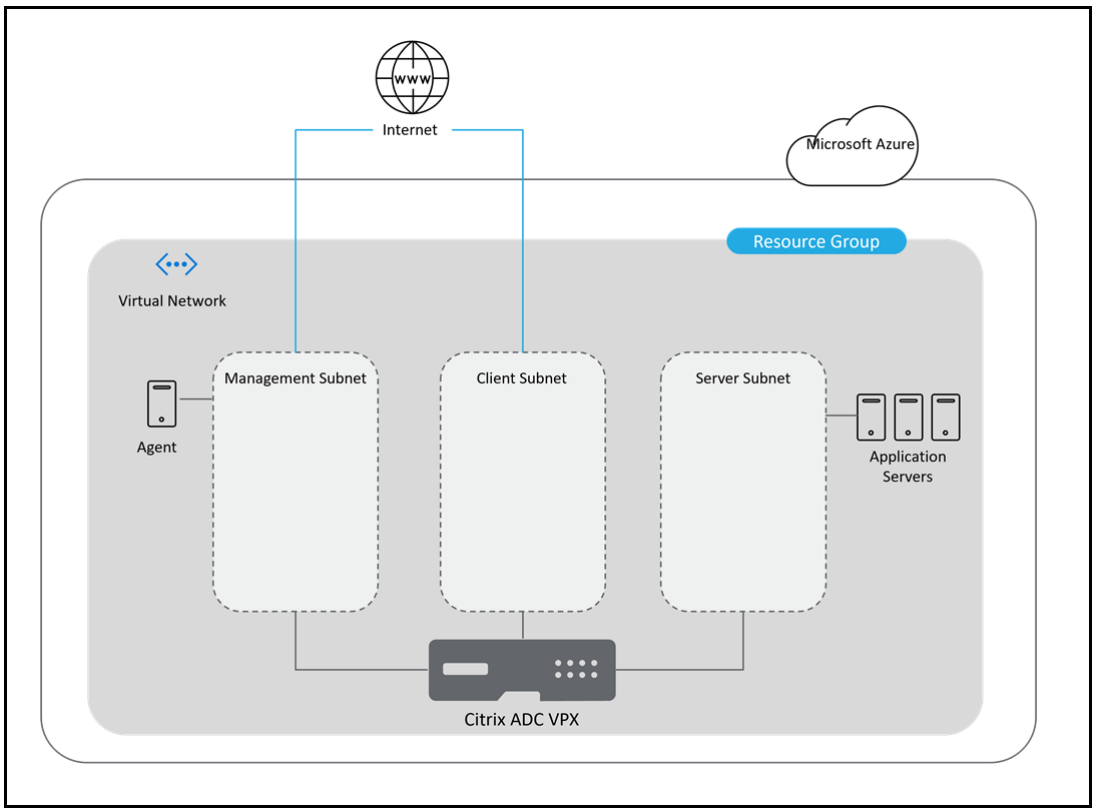
Utilisez l'image de la machine virtuelle Azure qui prend en charge au moins trois cartes réseau. Le provisionnement de l'instance Citrix ADC VPX est pris en charge uniquement sur les éditions Premium et Advanced. Pour plus d'informations sur les types d'image de machine virtuelle Azure, reportez-vous à la section Types et tailles de machines virtuelles dans la documentation Microsoft.

Voici les tailles de machines virtuelles recommandées pour le Provisioning :

- Standard_DS3_v2
- Standard_B2ms
- Standard_DS4_v2

Architecture de déploiement Citrix ADM

L'image suivante fournit une vue d'ensemble de la façon dont Citrix ADM se connecte à Azure pour provisionner des instances Citrix ADC VPX dans Microsoft Azure.



Vous devez disposer de trois sous-réseaux pour provisionner et gérer l'instance Citrix ADC VPX dans Microsoft Azure. Un groupe de sécurité doit être créé pour chaque sous-réseau. Les règles spécifiées dans Citrix Gateway régissent la communication entre les sous-réseaux.

L'agent de service Citrix ADM vous aide à provisionner et à gérer l'instance Citrix ADC VPX.

Conditions préalables

Cette section décrit les conditions préalables que vous devez remplir dans Microsoft Azure et Citrix ADM avant de provisionner des instances Citrix ADC VPX.

Ce document suppose ce qui suit :

- Vous possédez un compte Microsoft Azure qui prend en charge le modèle de déploiement Azure Resource Manager.
- Vous avez un groupe de ressources dans Microsoft Azure.

Pour plus d'informations sur la création d'un compte et d'autres tâches, reportez-vous à la sectionDocumentation Microsoft Azure.

Configurer les composants Microsoft Azure

Effectuez les tâches suivantes dans Azure avant de provisionner les instances Citrix ADC VPX dans Citrix ADM.

1. Créer un réseau virtuel.
2. Créer des groupes de sécurité.
3. Créer des sous-réseaux.
4. S'abonner à la licence Citrix ADC VPX dans Microsoft Azure.
5. Créer et enregistrer une demande.
6. Configurer un agent de service Citrix ADM.

Créer un réseau virtuel

1. Connectez-vous à votre portail Microsoft Azure.
2. Sélectionnez **Créer une ressource**.
3. Sélectionnez **Mise en réseau** et cliquez sur **Réseau virtuel** .
4. Spécifiez les paramètres requis.
    - Dans le **groupe de ressources**, vous devez spécifier le groupe de ressources dans lequel vous souhaitez déployer le produit Citrix ADC VPX.
    - Dans **Emplacement**, vous devez spécifier les emplacements qui prennent en charge les zones de disponibilité telles que :
        - USA Centre
        - Est US2
        - France Centre
        - Europe Nord
        - Asie du Sud-Est
        - Europe de l'Ouest
        - Ouest US2

    > **Remarque**
    >
    > Les serveurs d'applications présents dans ce groupe de ressources.

5. Cliquez sur **Créer**.

Pour plus d'informations, consultez Réseau virtuel Azure dansDocumentation Microsoft.

Créer des groupes de sécurité

Créez trois groupes de sécurité dans votre réseau virtuel (VNet), chacun pour les connexions de gestion, de client et de serveur. Créez un groupe de sécurité pour contrôler le trafic entrant et sortant dans l'instance Citrix ADC VPX. Vous pouvez ajouter autant de règles que vous voulez.

- **Gestion :** groupe de sécurité de votre compte dédié à la gestion de Citrix ADC VPX. Citrix ADC doit contacter les services Azure et nécessite un accès Internet. Les règles entrantes sont autorisées sur les ports TCP et UDP suivants.
  - TCP : 80, 22, 443, 3008-3011, 4001
  - UDP : 67, 123, 161, 500, 3003, 4500, 7000

  > **Remarque**
  >
  > Assurez-vous que le groupe de sécurité permet à l'agent Citrix ADM d'accéder au VPX.

- **Client :** groupe de sécurité de votre compte dédié à la communication côté client des instances Citrix ADC VPX. En règle générale, les règles entrantes sont autorisées sur les ports TCP 80, 22 et 443.
- **Serveur :** groupe de sécurité dans votre compte dédié à la communication côté serveur de Citrix ADC VPX.

Pour plus d'informations sur la création d'un groupe de sécurité dans Microsoft Azure, reportez-vous à la section Créer, modifier ou supprimer un groupe de sécurité réseau.

Créer des sous-réseaux

Créez trois sous-réseaux dans votre réseau virtuel (VNet) - un pour chacun des connexions de gestion, client et serveur. Spécifiez une plage d'adresses définie dans votre réseau virtuel pour chacun des sous-réseaux. Spécifiez la zone de disponibilité dans laquelle vous souhaitez que le sous-réseau réside.

- **Gestion :** sous-réseau de votre réseau virtuel (VNet) dédié à la gestion. Citrix ADC doit contacter les services Azure et nécessite un accès Internet.
- **Client :** sous-réseau de votre réseau virtuel (VNet) dédié au côté client. En règle générale, Citrix ADC reçoit le trafic client pour l'application via un sous-réseau public à partir d'Internet.
- **Serveur :** sous-réseau dans lequel les serveurs d'applications sont provisionnés. Tous vos serveurs d'applications sont présents dans ce sous-réseau et reçoivent le trafic d'application de l'Citrix ADC via ce sous-réseau.

> **Remarque**

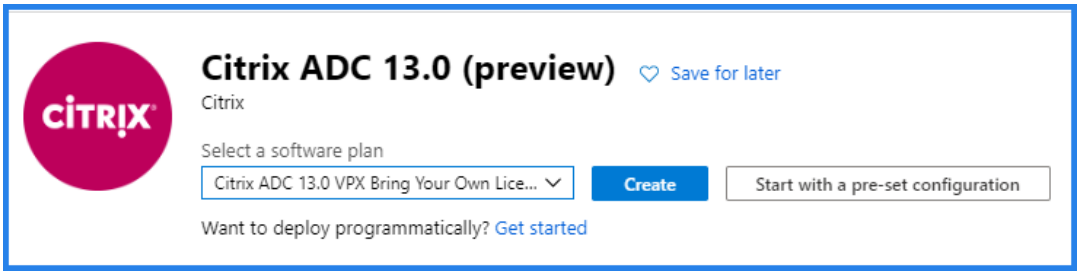
> Spécifiez un groupe de sécurité approprié pour le sous-réseau lors de la création d'un sous-réseau.

Pour plus d'informations sur la création d'un sous-réseau dans Microsoft Azure, reportez-vous à la section Ajouter, modifier ou supprimer un sous-réseau de réseau virtuel.

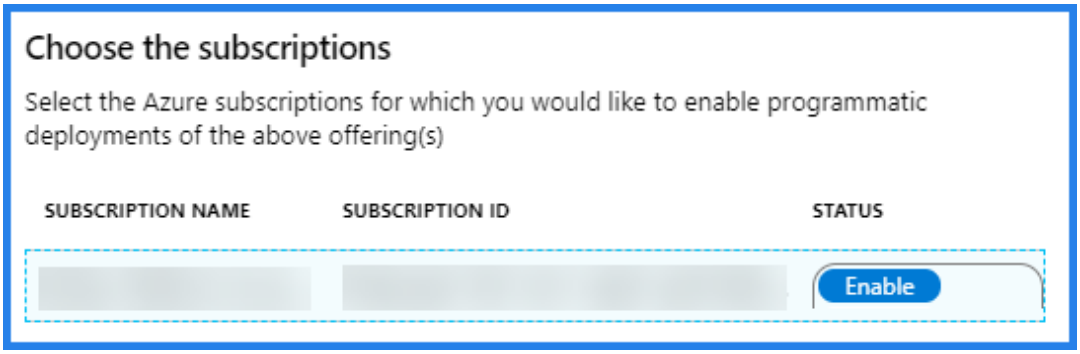
Abonnez-vous à la licence Citrix ADC VPX dans Microsoft Azure

1. Connectez-vous à votre portail Microsoft Azure.
2. Sélectionnez **Créer une ressource**.
3. Dans la barre **Rechercher le site de vente**, recherchez`Citrix ADC` et sélectionnez la version de produit requise.
4. Dans la liste **Sélectionner un plan logiciel**, sélectionnez l'un des types de licence suivants :
   - Apportez votre propre licence
   - Avancé
   - Premium

   > **Remarque**
   >
   > - Si vous choisissez l'option **Apporter votre propre licence**, l'instance que vous souhaitez provisionner retirera les licences de Citrix ADM lors du provisionnement des instances Citrix ADC.
   > - Dans Citrix ADM, **Advanced** et **Premium** sont les types de licence équivalents pour **Enterprise** et **Platinum** respectivement.
5. Assurez-vous que le déploiement programmatique est activé pour le produit Citrix ADC sélectionné.
   a) À côté **Vous voulez déployer par programme ?**, cliquez sur **Démarrer**.



   b) Dans **Choisir les abonnements**, sélectionnez **Activer**pour déployer l'édition Citrix ADC VPX sélectionnée par programme.



> **Important**
>
> L'activation du déploiement programmatique est nécessaire pour provisionner les instances Citrix ADC VPX dans Azure.

c) Cliquez sur **Enregistrer**.

d) Fermez **Configurer le déploiement programmatique**.

6. Cliquez sur **Créer**.

Créer et enregistrer une application

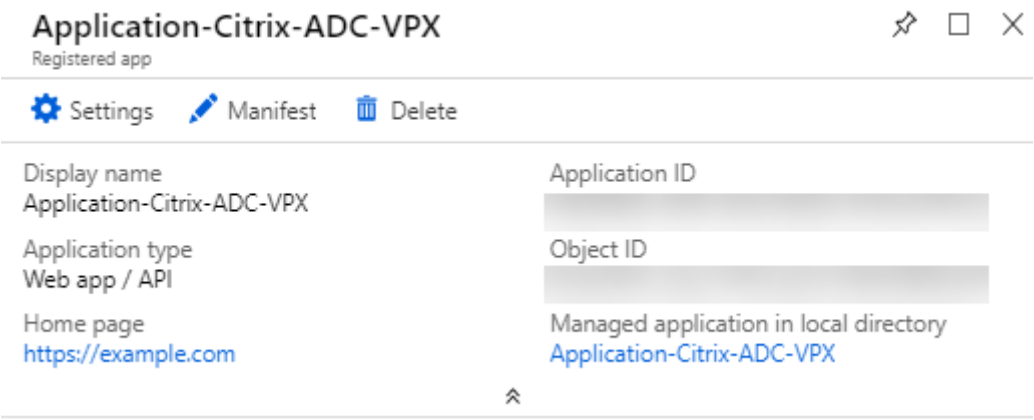
Citrix ADM utilise cette application pour provisionner les instances Citrix ADC VPX dans Azure.

Pour créer et enregistrer une application dans Azure :

1. Dans le portail Azure, sélectionnez **Azure Active Directory**.
   Cette option affiche le répertoire de votre organisation.
2. Sélectionnez **Enregistrements d'applications** :
   a) Dans **Nom**, spécifiez le nom de l'application.
   b) Sélectionnez le **type d'application** dans la liste.
   c) Dans l'URL de **connexion**, spécifiez l'URL de l'application pour accéder à l'application.
3. Cliquez sur **Créer**.

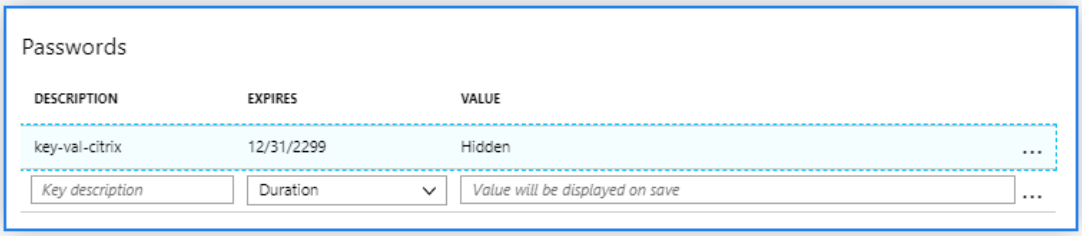
Pour plus d'informations sur les enregistrements d'applications, reportez-vous à la section Documentation Microsoft.

Azure affecte un ID d'application à l'application. Voici un exemple d'application enregistrée dans Microsoft Azure :



Copiez les ID suivants et fournissez ces ID lorsque vous configurez un profil Cloud Access dans Citrix ADM :

- **ID de l'application :** pour savoir comment récupérer l'ID de l'application ou du client.
- **ID de répertoire :** pour savoir comment récupérer le répertoire ou le locataire ou l'ID d'objet.
- **Clé :** pour les étapes à suivre pour récupérer la valeur de clé ou l'ID de secret client.



- **ID d'abonnement :** Copiez l'ID d'abonnement depuis votre compte de stockage.

Pour de plus amples informations, consultez la section Documentation Microsoft.

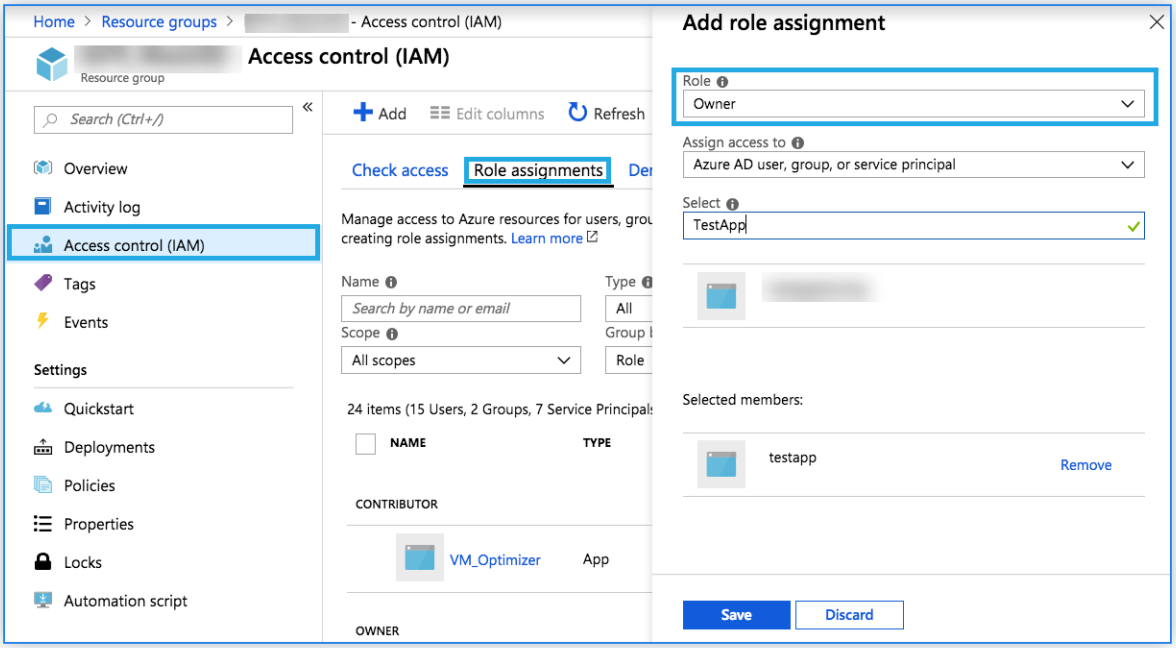
Attribuer l'autorisation de rôle à une application

Citrix ADM utilise le principe de l'application en tant que service pour provisionner les instances de Citrix ADC dans Microsoft Azure. Cette autorisation s'applique uniquement au groupe de ressources sélectionné.

Pour attribuer une autorisation de rôle à votre application enregistrée, vous devez être le propriétaire de l'abonnement Microsoft Azure.

1. Dans le portail Azure, sélectionnez **Groupes de ressources**.
2. Sélectionnez le groupe de ressources auquel vous souhaitez attribuer l'autorisation de rôle.
3. Sélectionnez **Contrôle d'accès (IAM)**.
4. Dans **Affectations de rôles**, cliquez sur **Ajouter**.

5. Sélectionnez **Propriétaire** dans la liste **Rôle** .
6. Sélectionnez l'application enregistrée pour le Provisioning des instances Citrix ADC. Consultez Créer et enregistrer une application.
7. Cliquez sur **Enregistrer**.



Configurer un agent de service Citrix ADM

Installez un agent de service Citrix ADM dans le sous-réseau de gestion. Cet agent fonctionne comme intermédiaire entre Citrix Application Delivery Management (Citrix ADM) et les instances gérées dans Microsoft Azure. Pour plus d'informations sur l'installation de l'agent de service Citrix ADM sur Microsoft Azure, reportez-vous à la section Installation de l'agent Citrix ADM sur le cloud Microsoft Azure.

Configurer les composants Citrix ADM

Effectuez les tâches suivantes dans Azure avant de provisionner les instances Citrix ADC VPX dans Citrix ADM :

1. Créer un site.
2. Attacher le site à un agent de service Citrix.

Créer un site dans Citrix ADM

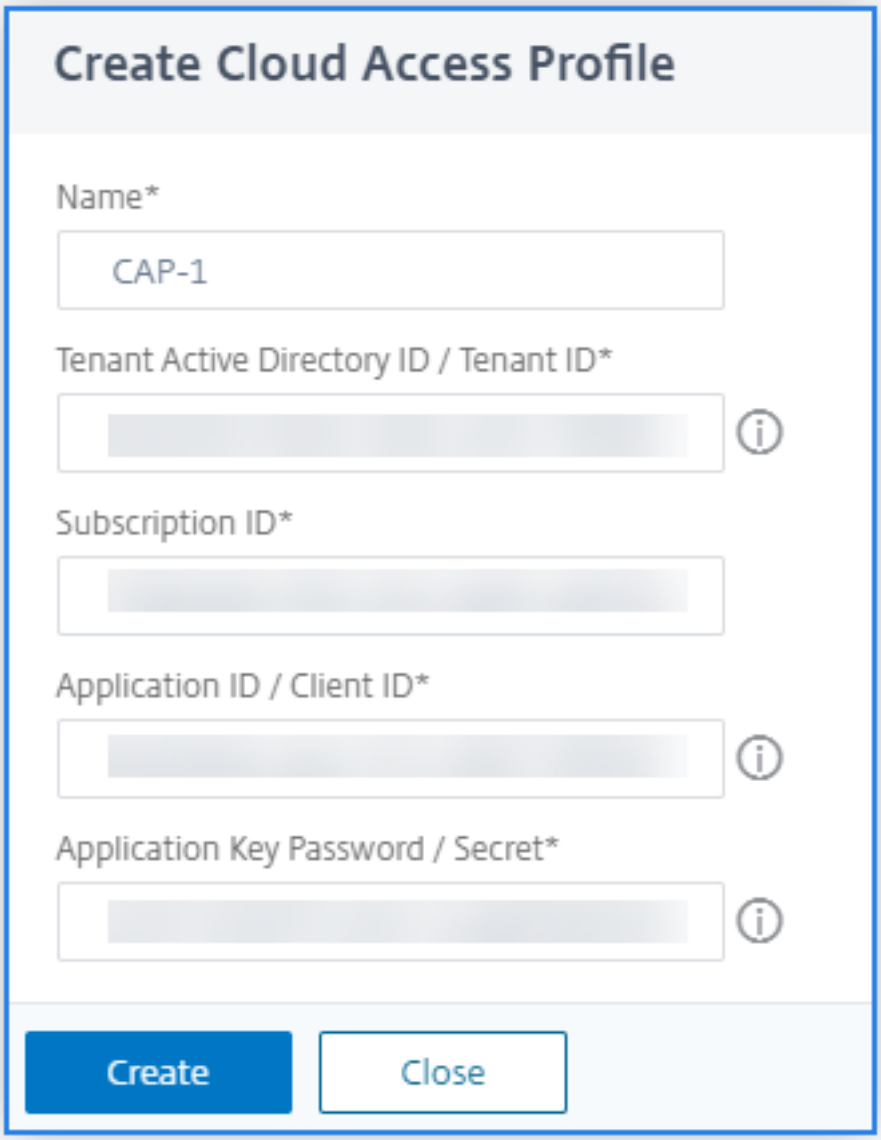
Créez un site dans Citrix ADM et ajoutez les détails de réseau virtuel associés à votre groupe de ressources Microsoft Azure.

1. Dans Citrix ADM, accédez à **Réseaux** > **Sites** .
2. Cliquez sur **Ajouter**.
3. Dans le volet **Sélectionner le Cloud**,
    a) Sélectionnez **Centre de données** comme **type de site**.
    b) Choisissez **Azure** dans la liste **Type**.
    c) Cochez la case **Récupérer le réseau virtuel virtuel à partir d'Azure**.

    Cette option vous aide à récupérer les informations de réseau virtuel existantes à partir de votre compte Microsoft Azure.

    d) Cliquez sur **Suivant**.
4. Dans le panneau **Choisir une région**,
    a) Dans **Cloud Access Profile**, sélectionnez le profil créé pour votre compte Microsoft Azure. S'il n'y a pas de profils, créez un profil.
    b) Pour créer un profil d'accès au cloud, cliquez sur **Ajouter**.
    c) Dans **Nom**, spécifiez un nom pour identifier votre compte Azure dans Citrix ADM.
    d) Dans **ID Active Directory de locataire/ID de locataire**, spécifiez l'ID Active Directory du locataire ou du compte dans Microsoft Azure.
    e) Spécifiez l' **ID d'abonnement**.
    f) Spécifiez l' **ID d'application ID/client**.
    g) Spécifiez le mot de **Secret/mot de passe de la clé d'application**.
    h) Cliquez sur **Créer**.

    Pour plus d'informations, veuillez consulter Créer et enregistrer une application et Map-page du profil d'accès Cloud à l'application Azure.



i) Dans **vNet**, sélectionnez le réseau virtuel contenant les instances Citrix ADC VPX que vous souhaitez gérer.

j) Spécifiez un **nom de site**.

k) Cliquez sur **Terminer**.

Mappage du profil d'accès au cloud à l'application Azure

Terme Citrix ADM	Terme Microsoft Azure
ID Active Directory du locataire/ID du locataire	ID de répertoire
ID d'abonnement	ID d'abonnement
Identifiant de l'application et du client	ID de l'application
Mot de passe de la clé d'application/Secret	Clés ou certificats ou secrets client

Attacher le site à un agent de service Citrix ADM

1. Dans Citrix ADM, accédez à **Réseaux** > **Agents** .
2. Sélectionnez l'agent pour lequel vous souhaitez attacher un site.
3. Cliquez sur **Joindre le site**.
4. Sélectionnez le site dans la liste que vous souhaitez joindre.
5. Cliquez sur **Enregistrer**.

Tâches de configuration

Utilisez le site que vous avez associé à votre groupe de ressources Microsoft Azure pour provisionner les instances Citrix ADC VPX. Fournissez les détails de l'agent de service Citrix ADM pour provisionner les instances qui sont liées à cet agent.

1. Dans Citrix ADM, accédez à **Réseaux** > **Instances** > **Citrix ADC**.
2. Dans l'onglet **VPX**, cliquez sur **Provisionner**.

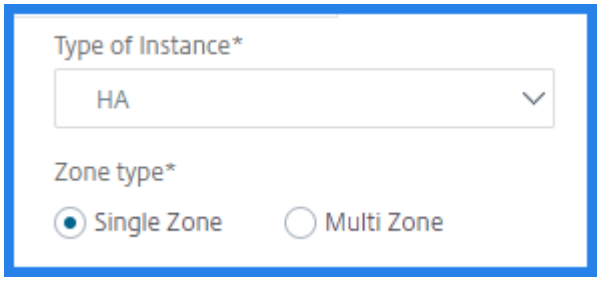
   Cette option affiche la page **Provisionner Citrix ADC VPX sur le Cloud** .
3. Sélectionnez **Microsoft Azure** et cliquez sur **Suivant**. Spécifiez les paramètres requis pour provisionner une instance.

Configurer les paramètres de base

1. Dans l'onglet **Paramètres de base**, spécifiez les éléments suivants :
   - **Type d'instance** : sélectionnez l'une des options suivantes dans la liste.
     - **Autonome** - Cette option fournit une instance Citrix ADC VPX autonome sur Microsoft Azure.
     - **HA :** Cette option provisionnera les instances Citrix ADC VPX haute disponibilité sur Microsoft Azure.

Pour provisionner les instances Citrix ADC VPX dans la même zone, sélectionnez l'option **Zone unique** sous **Type de zone**.

Pour provisionner les instances Citrix ADC VPX sur plusieurs zones, sélectionnez l'option **Multi Zonesous Type de zone**. Dans l'onglet**Paramètres du nuage**, assurez-vous de spécifier les détails réseau pour chaque zone créée sur Microsoft Azure.

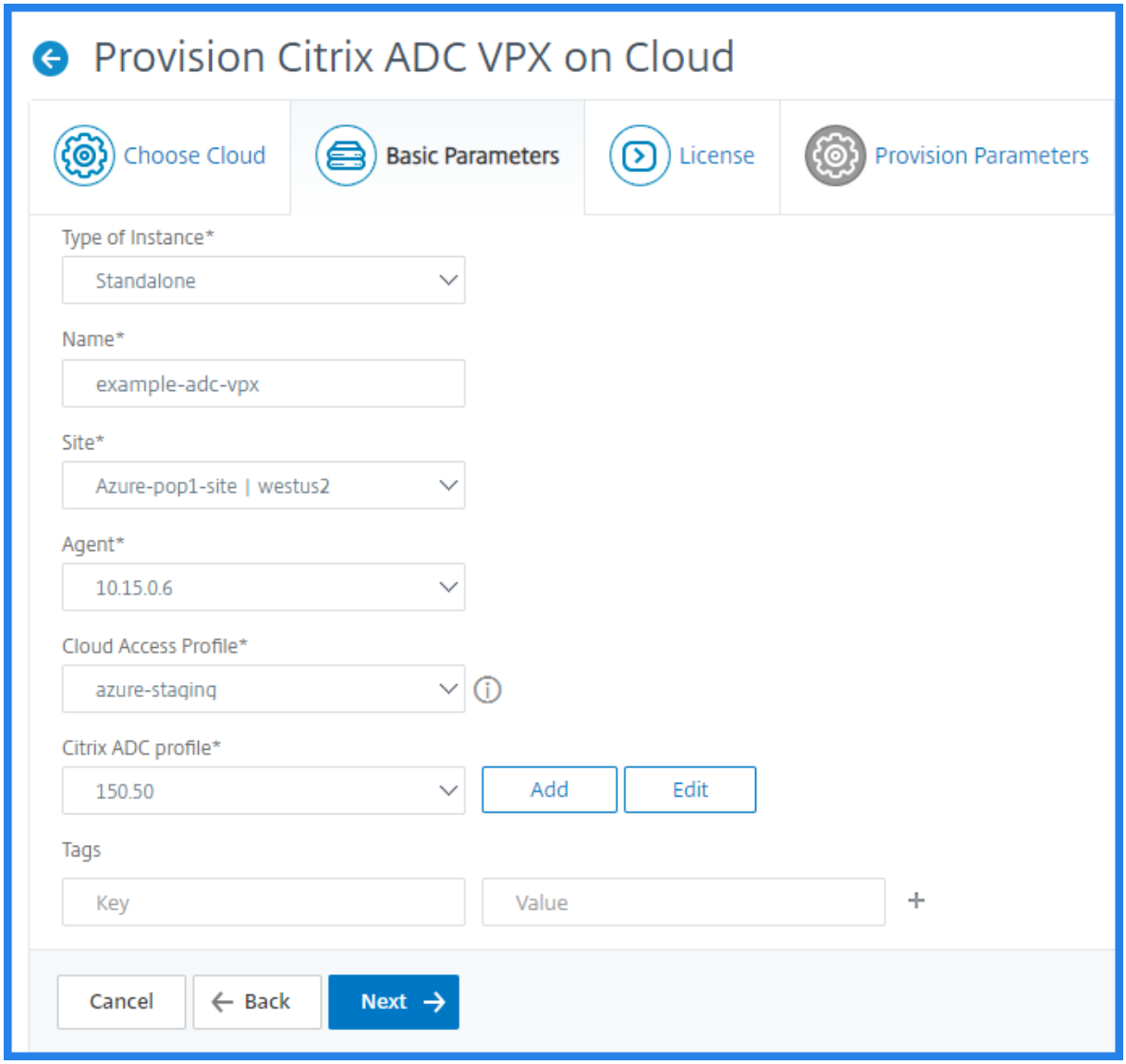


- **Nom** : spécifiez le nom d'une instance ADC VPX.
- **Site** : sélectionnez le site que vous avez créé précédemment.
- **Agent** : sélectionnez l'agent créé pour gérer l'instance Citrix ADC VPX.
- **Profil d'accès au cloud** - Sélectionnez le profil d'accès au cloud créé lors de la création du site.
- **Profil Citrix ADC** - Sélectionnez le profil à fournir l'authentification.

  Citrix ADM utilise le profil de périphérique lorsqu'il doit se connecter à l'instance Citrix ADC VPX.

  > **Remarque**
  >
  > Assurez-vous que le profil de périphérique sélectionné est conforme à Règles de mot de passe Microsoft Azure.

2. Cliquez sur **Suivant**.



Configurer les licences

Sélectionnez l'un des modes suivants pour appliquer une licence à une instance ADC :

- **Utilisation de Citrix ADM** : L'instance que vous souhaitez provisionner retirent les licences de Citrix ADM.
- **Utilisation de Microsoft Azure** : l'option **Allouer à partir du Cloud** utilise les licences de produit Citrix disponibles sur la Place de marché Azure. L'instance que vous souhaitez provisionner utilise les licences du site de vente.

  Si vous choisissez d'utiliser des licences de la Place de Azure Marketplace, spécifiez le produit ou la licence dans l'onglet **Paramètres de provisionnement**.

Pour de plus amples informations, consultez la section Exigences en matière de licences.

Utiliser les licences de Citrix ADM

Pour utiliser cette option, assurez-vous que vous êtes abonné au produit Citrix ADC avec le plan de logiciel **BYOL (avec apport de sa propre licence)** dans Azure. Consultez Abonnez-vous à la licence Citrix ADC VPX dans Microsoft Azure.

1. Dans l'onglet **Licence**, sélectionnez **Allouer à partir d'ADM**.
2. Dans **Type de licence**, sélectionnez l'une des options suivantes dans la liste :
   - **Licences de bande passante :** vous pouvez sélectionner l'une des options suivantes dans la liste **Types de licences de bande passante** :
     - **Capacité groupée :** spécifiez la capacité à allouer à une instance.

       À partir du pool commun, l'instance ADC retirait une licence d'instance et seule la bande passante est spécifiée.
     - **Licences VPX :** lorsqu'une instance Citrix ADC VPX est provisionnée, l'instance extrait la licence de Citrix ADM.
   - **Licences CPU virtuelles :** l'instance Citrix ADC VPX provisionnée retire les licences en fonction du nombre de processeurs exécutés dans l'instance.

   > **Remarque**
   >
   > Lorsque les instances provisionnées sont supprimées ou détruites, les licences appliquées retournent au pool de licences Citrix ADM. Ces licences peuvent être réutilisées pour provisionner de nouvelles instances.
3. Dans **License Edition**, sélectionnez l'édition de licence. L'ADM utilise l'édition spécifiée pour provisionner des instances.
4. Cliquez sur **Suivant**.

Configurer les paramètres de provisionnement

1. Dans l'onglet **Paramètres de provisionnement**, spécifiez les éléments suivants :
   - **Groupe de ressources** : sélectionnez le **groupe de ressources** dans lequel vous souhaitez provisionner l'instance Citrix ADC VPX.
   - **Product/License** - Sélectionnez l' option requise dans la liste.

   a) Sélectionnez la **taille de la machine virtuelle** prise en charge dans la liste.

   > **Remarque**
   >
   > Pour plus d'informations sur les produits pris en charge et les tailles de machines virtuelles, reportez-vous à la sectionImages de machines virtuelles Citrix ADC Azure

> prises en charge.

b) Sélectionnez le profil d'accès au cloud pour ADC.

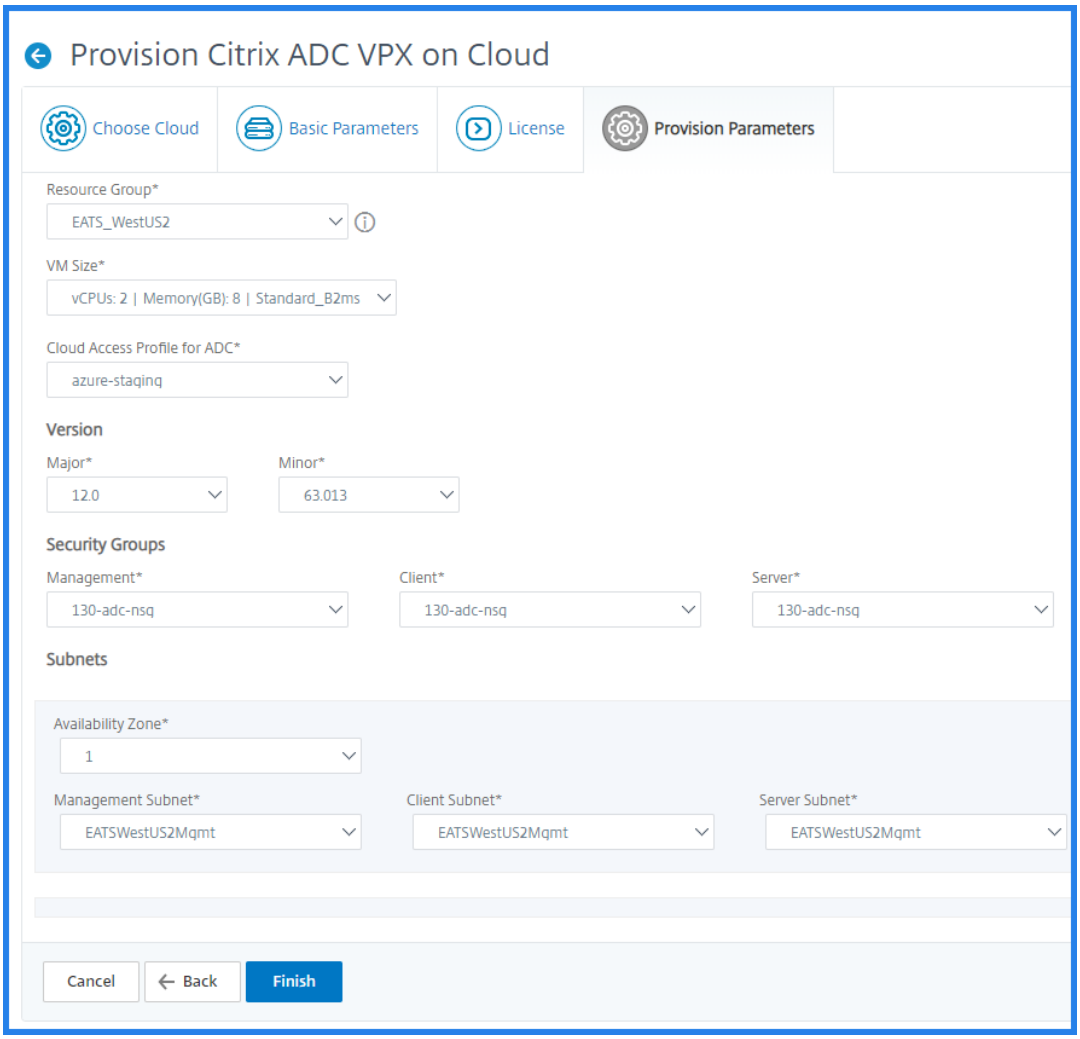
c) Sélectionnez la **version** de Citrix ADC à provisionner. Sélectionnez les versions **Major** et **Minor** de Citrix ADC.

d) Dans **Groupes de sécurité**, sélectionnez les groupes de sécurité Gestion, Client et Serveur que vous avez créés dans votre réseau virtuel.

e) Dans **Sous-réseaux**, spécifiez le nombre requis de zones de disponibilité dans Azure.

f) Dans **Sous-réseaux**, sélectionnez les sous-réseaux Gestion, Client et Serveur que vous avez créés dans votre réseau virtuel.

g) Cliquez sur **Terminer**.



L'instance Citrix ADC VPX est désormais provisionnée sur Microsoft Azure.

Afficher les instances Citrix ADC VPX provisionnées

Pour afficher dans Citrix ADM :

1. Dans Citrix ADM, accédez à **Réseaux** > **Instances** > **Citrix ADC**.
2. Sélectionnez l'onglet **Citrix ADC VPX** .

   L'instance Citrix ADC VPX provisionnée dans Microsoft Azure est répertoriée ici.

Pour afficher dans Microsoft Azure :

1. Connectez-vous à votre portail Azure.
2. Accédez au groupe de ressources créé pour provisionner l'instance Citrix ADC VPX.

   Cette page affiche l'instance Citrix ADC VPX provisionnée.

> **Remarque**
>
> Le nom de l'instance Citrix ADC VPX est identique à celui que vous avez fourni lors du provisionnement d'une instance dans Citrix ADM.

Mise à l'échelle automatique de Citrix ADC VPX dans Microsoft Azure à l'aide de Citrix ADM

April 29, 2021

Autoscaling est une méthode de cloud computing qui ajoute ou supprime automatiquement des ressources en fonction de l'utilisation réelle. La mise à l'échelle automatique est utile lorsque votre site ou votre application a besoin d'une allocation de ressources à la demande pour satisfaire le nombre fluctuant de demandes client ou de tâches de traitement.

La demande d'applications ou de services Web peut varier considérablement. Il est important de maintenir le nombre correct d'instances Citrix ADC pour les différents besoins de trafic. Vous pouvez augmenter ou diminuer les ressources réseau sur Microsoft Azure en fonction de la demande. Ainsi, il offre une optimisation des coûts sans compromettre les performances.

La mise à l'échelle automatique de Citrix Application Delivery Management (ADM) conserve le nombre exact d'instances Citrix ADC pour fluctuer la consommation des ressources. Citrix ADM détermine le flux de trafic en fonction de la consommation fluctuante des ressources, il décide d'évoluer ou d'évoluer dynamiquement dans les instances Citrix ADC. Ainsi, il vous offre la flexibilité nécessaire pour maintenir le nombre correct d'instances Citrix ADC.

Citrix ADM surveille l'utilisation des ressources des instances de Citrix ADC et correspond à la valeur de seuil configurée. Il déclenche l'action de mise à l'échelle si l'une des ressources configurées dépasse la valeur de seuil spécifiée.

Citrix ADM déclenche l'action de mise à l'échelle uniquement lorsque l'utilisation de toutes les ressources configurées est inférieure à la valeur de seuil normale.

> **Important**
>
> Autoscaling prend en charge toutes les fonctionnalités de Citrix ADC, à l'exception des fonctionnalités suivantes qui nécessitent une configuration ponctuée sur les nœuds de cluster :
>
> - GSLB
> - Citrix Gateway et ses fonctionnalités
> - Fonctionnalités de télécommunication
>
> Pour plus d'informations sur la configuration ponctuée, reportez-vous à la sectionConfigurations striped, striped partielles et spotted.

Avantages

Haute disponibilité des applications : La mise à l'échelle automatique garantit que votre application dispose toujours du nombre approprié d'instances Citrix ADC VPX pour gérer les demandes de trafic. Il garantit que votre application est opérationnelle tout le temps, quelles que soient les exigences en matière de trafic.

Décisions de mise à l'échelle intelligente et configuration sans contact : Autoscaling surveille en permanence votre application et ajoute ou supprime dynamiquement les instances de Citrix ADC en fonction de la demande. Les instances sont automatiquement ajoutées lorsque la demande est augmentée pendant une certaine période. Les instances sont automatiquement supprimées lorsque la demande est diminuée pendant une certaine période. L'ajout et la suppression d'instances de Citrix ADC se produisent automatiquement, ce qui en fait une configuration manuelle sans contact.

Gestion automatique du DNS : la fonctionnalité de mise à l'Autoscale Citrix ADM offre une gestion DNS automatique. Chaque fois que de nouvelles instances de Citrix ADC sont ajoutées, les noms de domaine sont mis à jour automatiquement.

Fin de connexion gracieuse : lors d'une mise à l'échelle, les instances de Citrix ADC sont supprimées de manière gracieuse, évitant ainsi la perte de connexions client.

Meilleure gestion des coûts : la mise à l'échelle automatique augmente ou diminue dynamiquement les instances de Citrix ADC selon les besoins. Cette méthode vous permet d'optimiser les coûts impliqués. Le lancement d'instances uniquement lorsqu'elles sont nécessaires et leur arrêt lorsqu'elles ne sont pas nécessaires réduit les coûts opérationnels. Ainsi, vous ne payez que pour les ressources que vous utilisez.

Observabilité : L'observabilité est essentielle pour les développeurs d'applications ou le personnel informatique pour surveiller l'état de l'application. Le tableau de bord de mise à l'Autoscale de Citrix ADM vous permet de visualiser les valeurs des paramètres de seuil, les horodatages de déclenchement de mise à l'Autoscale, les événements et les instances participant à la mise à l'échelle automatique.

Configuration requise pour le système de licences

Les instances Citrix ADC créées pour le groupe Citrix Autoscale utilisent les licences Citrix ADC Advanced ou Premium ADC. La fonctionnalité de mise en cluster Citrix ADC est incluse dans les licences ADC Advanced ou Premium.

> **Remarque**
>
> Les clusters ADC ne sont pris en charge que dans la mise à l'échelle automatique ADM avec les licences ADC Premium ou Advanced.

Vous pouvez choisir l'une des méthodes suivantes pour concéder une licence aux Citrix ADC provisionnés par Citrix ADM :

- **Utilisation des licences ADC présentes dans Citrix ADM :** configurez la capacité groupée, les licences VPX ou les licences CPU virtuelles lors de la création du groupe Mise à l'Autoscale. Ainsi, lorsqu'une nouvelle instance est provisionnée pour le groupe Mise à l'Autoscale, le type de licence déjà configuré est automatiquement appliqué à l'instance provisionnée.
  - **Capacité groupée** : alloue la bande passante à chaque instance provisionnée du groupe Mise à l'Autoscale. Assurez-vous que vous disposez de la bande passante nécessaire dans Citrix ADM pour provisionner de nouvelles instances. Pour de plus amples informations, consultez la section Configurer la capacité groupée.

    Chaque instance ADC du groupe Mise à l'Autoscale retirait une licence d'instance et la bande passante spécifiée du pool.
  - **Licences VPX :** Applique les licences VPX aux instances nouvellement provisionnées. Assurez-vous que vous disposez du nombre nécessaire de licences VPX disponibles dans Citrix ADM pour provisionner de nouvelles instances.

    Lorsqu'une instance Citrix ADC VPX est provisionnée, l'instance extraire la licence auprès de Citrix ADM. Pour de plus amples informations, consultez la section Licences d'enregistrement et de sortie Citrix ADC VPX.
  - **Licences de CPU virtuel :** applique des licences de CPU virtuel aux instances nouvellement provisionnées. Cette licence spécifie le nombre de processeurs autorisés à une instance Citrix ADC VPX. Assurez-vous que vous disposez du nombre nécessaire de processeurs virtuels dans Citrix ADM pour provisionner de nouvelles instances.

    Lorsqu'une instance Citrix ADC VPX est provisionnée, l'instance extraire la licence du processeur virtuel à partir de Citrix ADM. Pour de plus amples informations, consultez la section Licences de processeur virtuel Citrix ADC.

  Lorsque les instances provisionnées sont détruites ou déprovisionnées, les licences appliquées sont automatiquement renvoyées à Citrix ADM.

  Pour surveiller les licences consommées, accédez à la page **Réseaux** > **Licences** .

- **Utilisation des licences d'abonnement Microsoft Azure : configurez les** licences Citrix ADC disponibles dans Azure Marketplace lors de la création du groupe Mise à l'Autoscale. Ainsi, lorsqu'une nouvelle instance est provisionnée pour le groupe Mise à l'Autoscale, la licence est obtenue auprès de la Place de Azure Marketplace.

Images de machines virtuelles Citrix ADC Azure prises en charge pour la mise à l'échelle automatique

Utilisez l'image de machine virtuelle Azure qui prend en charge au moins trois cartes réseau. La mise à l'échelle automatique de l'instance Citrix ADC VPX est prise en charge uniquement sur les éditions Premium et Advanced. Pour plus d'informations sur les types d'image de machine virtuelle Azure, reportez-vous à la section Types et tailles de machines virtuelles dans la documentation Microsoft.

Voici les tailles de machine virtuelle recommandées pour la mise à l'échelle automatique :

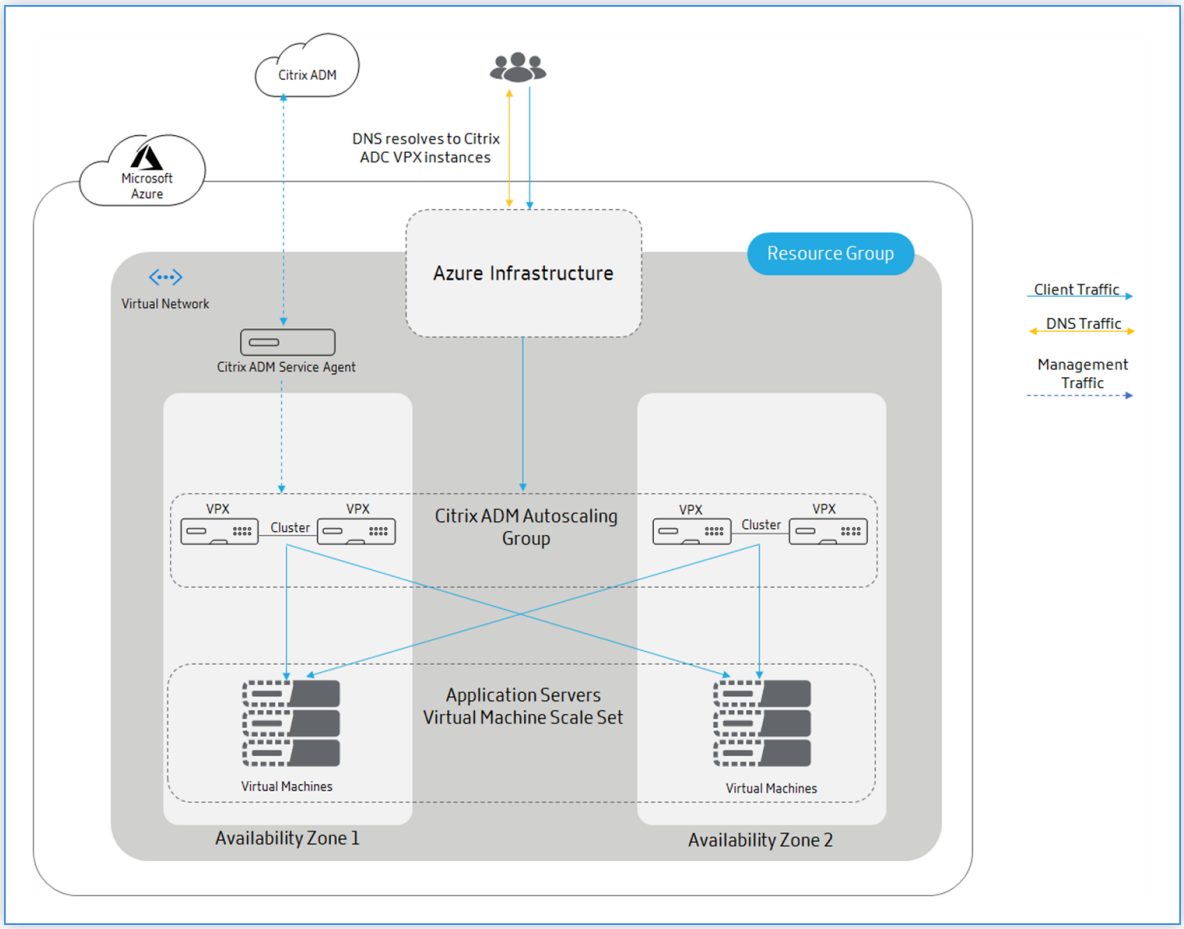
- Standard_DS3_v2
- Standard_B2ms
- Standard_DS4_v2

Architecture

Citrix ADM gère la distribution du trafic client à l'aide du DNS Azure ou de l'équilibreur de charge Azure (ALB).

Distribution du trafic à l'aide du DNS Azure

Le diagramme suivant illustre comment la mise à l'échelle automatique basée sur DNS se produit à l'aide du gestionnaire de trafic Azure en tant que distributeur de trafic :



Dans la mise à l'échelle automatique basée sur DNS, DNS agit comme une couche de distribution. Le gestionnaire de trafic Azure est l'équilibreur de charge basé sur DNS dans Microsoft Azure. Traffic Manager dirige le trafic client vers l'instance appropriée de Citrix ADC disponible dans le groupe de mise à l'échelle automatique Citrix ADM.

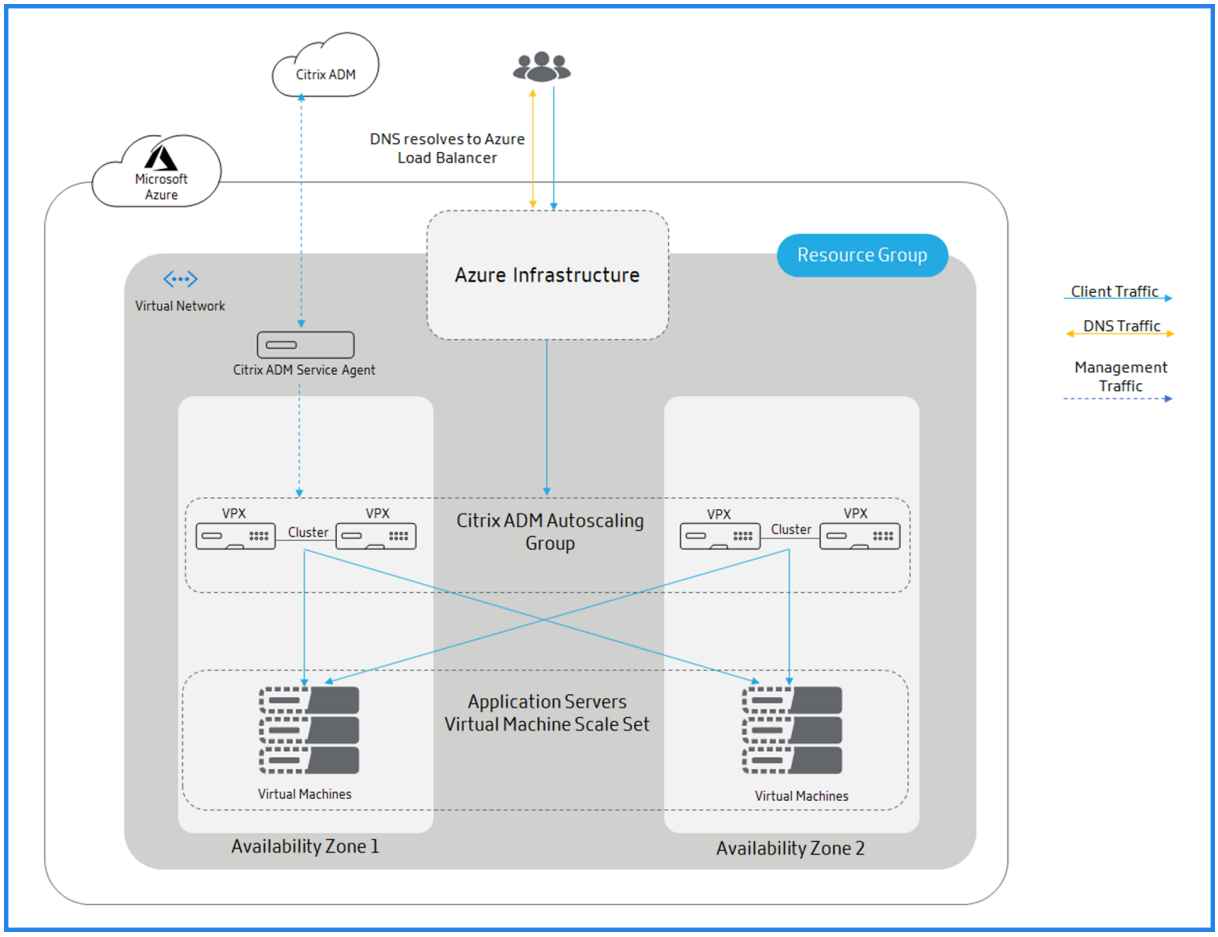
Azure Traffic Manager résout le nom de domaine complet à l'adresse VIP de l'instance de Citrix ADC.

> **Remarque**
>
> Dans la mise à l'échelle automatique basée sur DNS, chaque instance Citrix ADC du groupe Citrix ADM Autoscale nécessite une adresse IP publique.

Citrix ADM déclenche l'action scale-out ou scale-in au niveau du cluster. Lorsqu'une mise à l'échelle est déclenchée, les machines virtuelles enregistrées sont provisionnées et ajoutées au cluster. De même, lorsqu'une mise à l'échelle est déclenchée, les nœuds sont supprimés et déprovisionnés des clusters Citrix ADC VPX.

Distribution du trafic à l'aide de l'équilibreur de charge Azure

Le diagramme suivant illustre la façon dont la mise à l'échelle automatique se produit à l'aide de l'Azure Load Balancer en tant que distributeur de trafic :



Azure Load Balancer est le niveau de distribution vers les nœuds de cluster. ALB gère le trafic client et le distribue aux clusters Citrix ADC VPX. ALB envoie le trafic client aux nœuds de cluster Citrix ADC VPX qui sont disponibles dans le groupe de mise à l'échelle automatique Citrix ADM entre les zones de disponibilité.

> **Remarque**L'adresse IP
>
> publique est allouée à l'équilibreur de charge Azure. Les instances Citrix ADC VPX ne nécessitent pas d'adresse IP publique.

Citrix ADM déclenche l'action scale-out ou scale-in au niveau du cluster. Lorsqu'une mise à l'échelle est déclenchée, les machines virtuelles enregistrées sont provisionnées et ajoutées au cluster. De même, lorsqu'une mise à l'échelle est déclenchée, les nœuds sont supprimés et déprovisionnés des clusters Citrix ADC VPX.

Groupe Citrix ADM Autoscale

Le groupe Autoscale est un groupe d'instances de Citrix ADC qui équilibrent la charge des applications en tant qu'entité unique et déclenche la mise à l'échelle automatique en fonction des valeurs de paramètre de seuil configurées.

Groupe de ressources

Le groupe de ressources contient les ressources liées à la mise à l'échelle automatique Citrix ADC. Ce groupe de ressources vous aide à gérer les ressources requises pour la mise à l'échelle automatique. Pour de plus amples informations, consultez la section Gérer les groupes de ressources.

Jeu d'échelle de machine virtuelle back-end Azure

L'échelle de machine virtuelle Azure est un ensemble d'instances de machine virtuelle identiques. Le nombre d'instances de machine virtuelle peut augmenter ou diminuer en fonction du trafic client. Cet ensemble offre une haute disponibilité à vos applications. Pour de plus amples informations, consultez la section Jeux d'échelles de machine virtuelle.

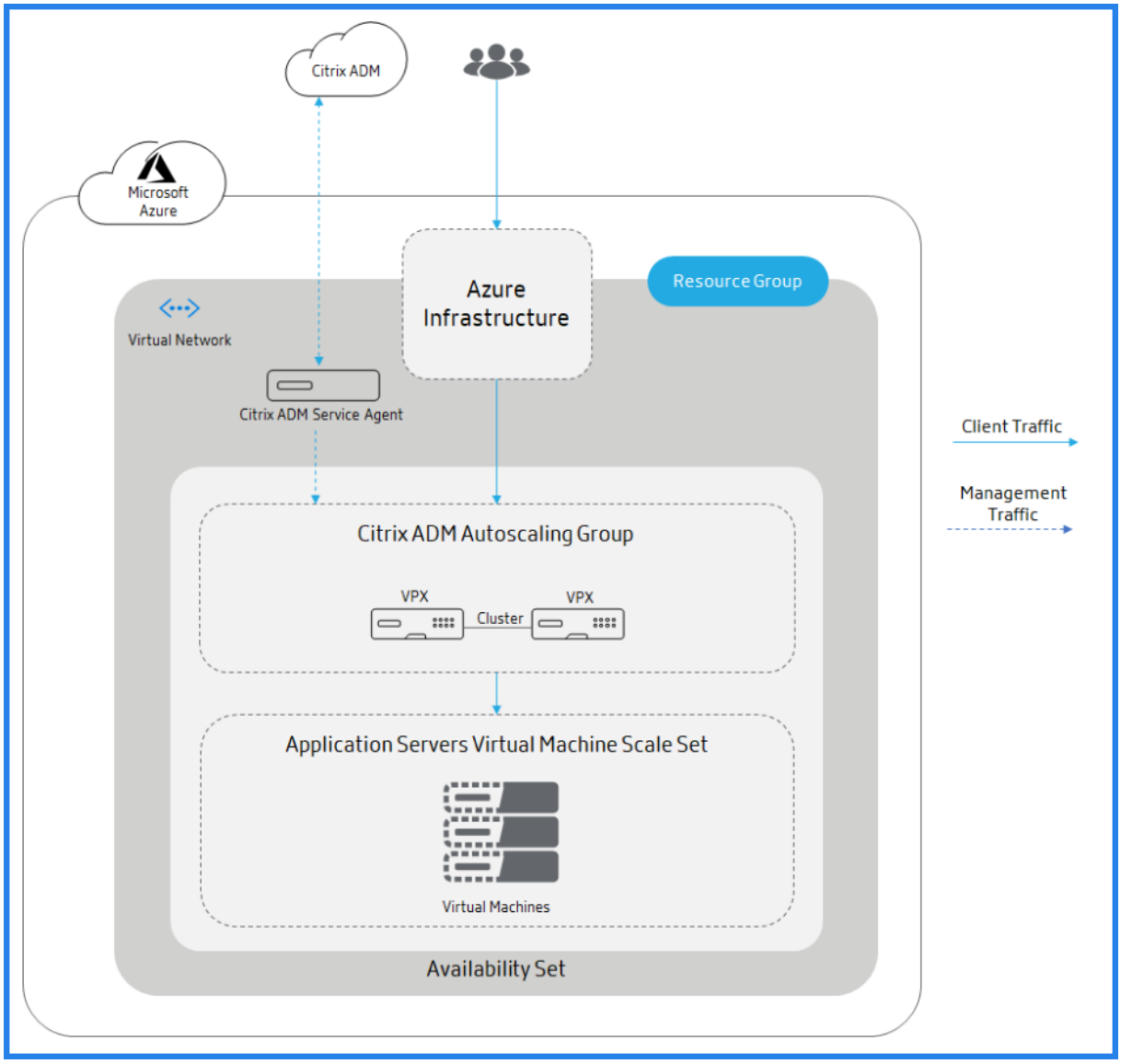
Zones de disponibilité

Les zones de disponibilité sont des emplacements isolés dans une région Azure. Chaque région est composée de plusieurs zones de disponibilité. Chaque zone de disponibilité appartient à une seule région. Chaque zone de disponibilité dispose d'un cluster Citrix ADC VPX. Pour de plus amples informations, consultez la section Zones de disponibilité dans Azure.

Ensembles de disponibilité

Un jeu de disponibilité est un regroupement logique d'un cluster Citrix ADC VPX et de serveurs d'applications. Les jeux de disponibilité sont utiles pour déployer des instances ADC sur plusieurs nœuds matériels isolés dans un cluster. Avec un jeu de disponibilité, vous pouvez garantir une mise à l'échelle automatique d'ADM fiable en cas de panne matérielle ou logicielle dans Azure. Pour de plus amples informations, consultez la section Ensembles de disponibilité.

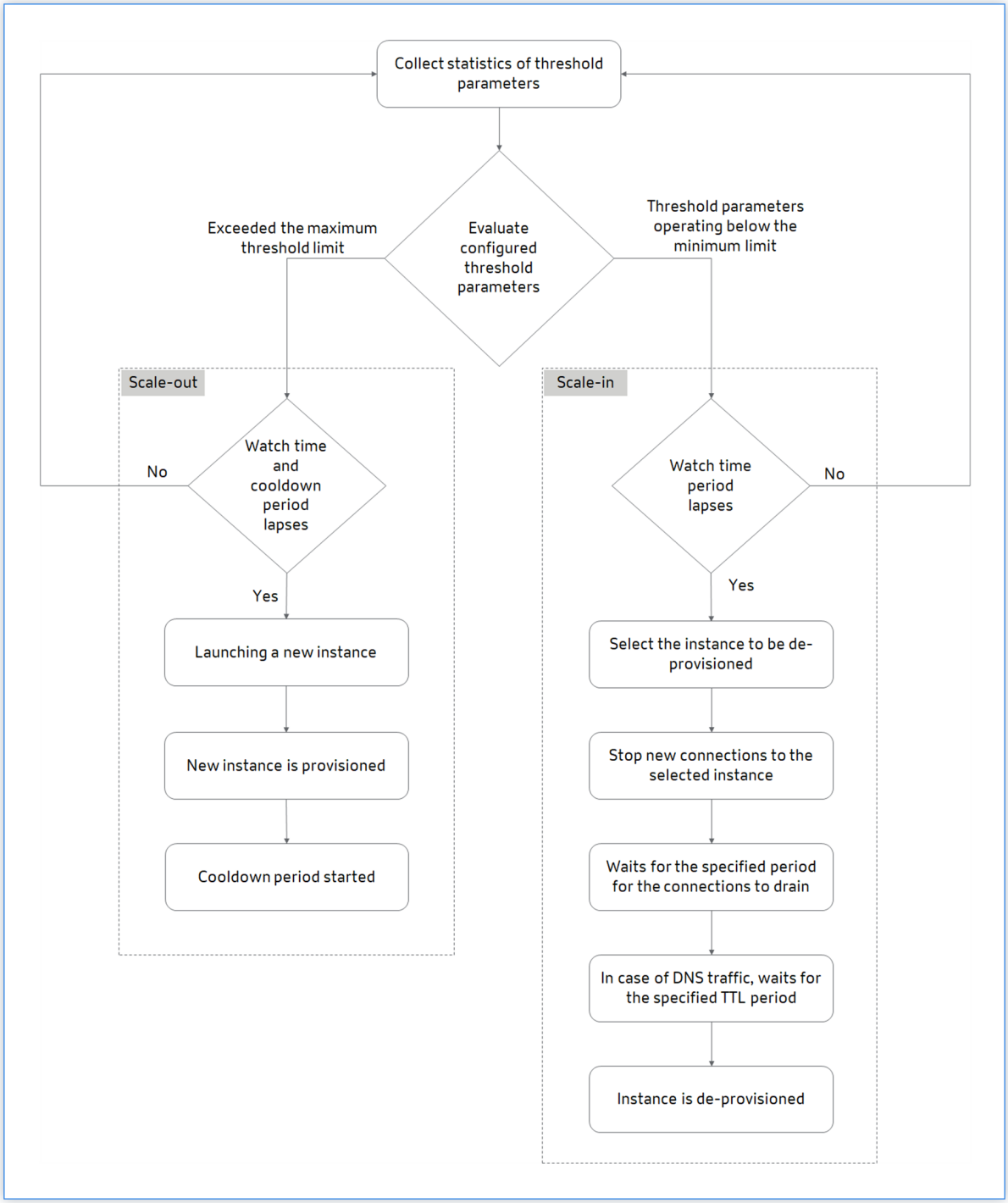
Le diagramme suivant illustre la mise à l'échelle automatique dans un jeu de disponibilité :



L'infrastructure Azure (ALB ou Azure Traffic Manager) envoie le trafic client à un groupe de mise à l'échelle automatique Citrix ADM dans le jeu de disponibilité. Citrix ADM déclenche l'action scale-out ou scale-in au niveau du cluster.

Fonctionnement de la mise à l'échelle automatique

L'organigramme suivant illustre le flux de travail de mise à l'échelle automatique :



Citrix ADM collecte les statistiques (CPU, mémoire et débit) à partir des clusters provisionnés à l'Autoscale pour chaque minute.

Les statistiques sont évaluées par rapport aux seuils de configuration. Selon les statistiques, la mise à l'échelle ou la mise à l'échelle est déclenchée. La mise à l'échelle est déclenchée lorsque les statistiques dépassent le seuil maximal. La mise à l'échelle est déclenchée lorsque les statistiques fonction-

nent en dessous du seuil minimum.

Si une mise à l'échelle est déclenchée :

1. Le nouveau nœud est provisionné.
2. Le nœud est attaché au cluster et la configuration est synchronisée entre le cluster et le nouveau nœud.
3. Le nœud est enregistré auprès de Citrix ADM.
4. Les nouvelles adresses IP de nœud sont mises à jour dans le gestionnaire de trafic Azure.

Si une mise à l'échelle est déclenchée :

1. Le nœud est identifié à supprimer.
2. Arrêter les nouvelles connexions au nœud sélectionné.
3. Attend la période spécifiée pour que les connexions s'écoulent. Dans le trafic DNS, il attend également la période TTL (Time To Live) spécifiée.
4. Le nœud est détaché du cluster, radié de Citrix ADM, puis déprovisionné de Microsoft Azure.

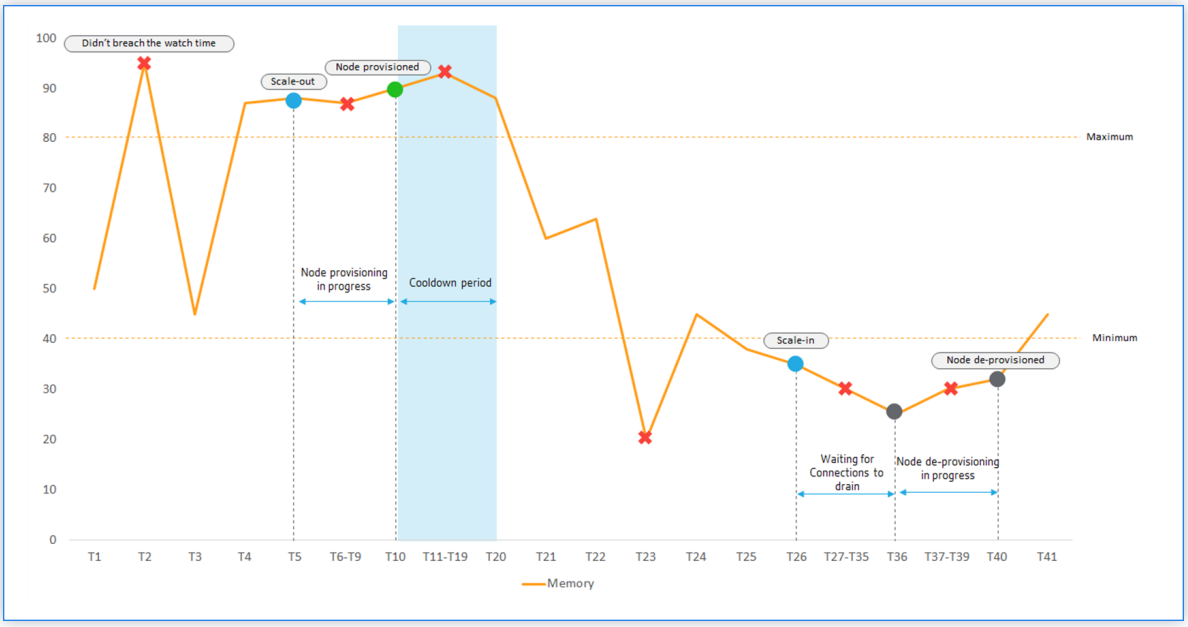
> **Remarque**
>
> Lorsque l'application est déployée, un jeu d'adresses IP est créé sur les clusters de chaque zone de disponibilité. Ensuite, les adresses IP du domaine et de l'instance sont enregistrées auprès du gestionnaire de trafic Azure ou ALB. Lorsque l'application est supprimée, les adresses IP du domaine et de l'instance sont désenregistrées du gestionnaire de trafic Azure ou ALB. Ensuite, le jeu d'adresses IP est supprimé.

Exemple de scénario de mise à l'échelle automatique

Considérez que vous avez créé un groupe de mise à l'Autoscale nommé asg_arn dans une zone de disponibilité unique avec la configuration suivante.

- Paramètres de seuil sélectionnés : utilisation de la mémoire.
- Limite de seuil définie sur la mémoire :
  - Limite minimale : 40
  - Limite maximale : 85
- Temps de visionnage — 2 minutes.
- Période de recharge — 10 minutes.
- Temps d'attente pendant la désapprovisionnement — 10 minutes.
- Durée de vie du DNS — 10 secondes.

Une fois le groupe Autoscale créé, les statistiques sont collectées à partir du groupe Mise à Autoscale. La stratégie Autoscale évalue également si un événement de Autoscale est en cours. Si la mise à l'échelle automatique est en cours, attendez que cet événement se termine avant de collecter les statistiques.



La séquence des événements

1. L'utilisation de la mémoire dépasse la limite de seuil à **T2**. Toutefois, la mise à l'échelle n'est pas déclenchée car elle n'a pas violé la durée de la montre spécifiée.
2. La mise à l'échelle est déclenchée à **T5** après une atteinte d'un seuil maximal pendant 2 minutes (temps de surveillance) en continu.
3. Aucune action n'a été entreprise pour la violation entre **T5-T10** car le Provisioning du nœud est en cours.
4. Le nœud est provisionné à **T10** et ajouté au cluster. La période de recharge a commencé.
5. Aucune mesure n'a été prise pour la rupture entre le **T10-T20** en raison de la période de recharge. Cette période garantit la croissance organique des instances d'un groupe Autoscale. Avant de déclencher la prochaine décision de mise à l'échelle, il attend que le trafic actuel se stabilise et se stabilise sur l'ensemble d'instances en cours.
6. L'utilisation de la mémoire tombe en dessous de la limite minimale de **T23**. Toutefois, la mise à l'échelle n'est pas déclenchée parce qu'elle n'a pas violé la durée de la montre spécifiée.
7. La mise à l'échelle est déclenchée à **T26** après que le seuil minimal est dépassé pendant 2 minutes (temps de surveillance) en continu. Un nœud du cluster est identifié pour le désapprovisionnement.

8. Aucune mesure n'a été prise pour la rupture entre le **T26-T36** car Citrix ADM attend de vider les connexions existantes. Pour la mise à l'échelle automatique basée sur DNS, TTL est en vigueur.

   > **Remarque**
   >
   > Pour la mise à l'échelle automatique basée sur DNS, Citrix ADM attend la période de durée de vie (TTL) spécifiée. Ensuite, il attend que les connexions existantes s'écoulent avant de lancer le désapprovisionnement des nœuds.

9. Aucune mesure n'a été prise pour la violation entre le **T37-T39** car le désapprovisionnement du nœud est en cours.
10. Le nœud est supprimé et déprovisionné à **T40** du cluster.

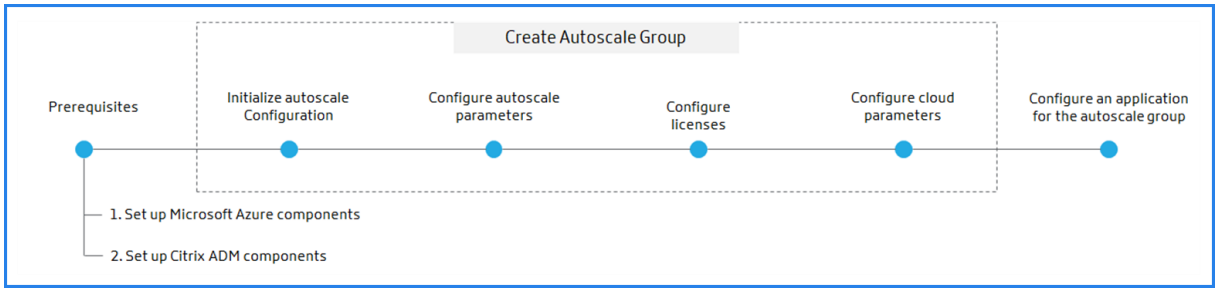
Toutes les connexions au nœud sélectionné ont été drainées avant de lancer le désapprovisionnement du nœud. Par conséquent, la période de recharge est ignorée après la suppression de la mise en service du nœud.

Configuration

April 29, 2021

Citrix ADM gère tous les clusters Citrix ADC VPX dans Microsoft Azure. Citrix ADM accède aux ressources Azure à l'aide du profil d'accès au Cloud.

Le diagramme de flux suivant explique les étapes de création et de configuration d'un groupe de mise Autoscale :



Conditions préalables

Cette section décrit les conditions préalables que vous devez remplir dans Microsoft Azure et Citrix ADM avant de configurer la mise à l'échelle automatique des instances Citrix ADC VPX.

Ce document suppose ce qui suit :

- Vous possédez un compte Microsoft Azure qui prend en charge le modèle de déploiement Azure Resource Manager.

- Vous avez un groupe de ressources dans Microsoft Azure.

Pour plus d'informations sur la création d'un compte et d'autres tâches, reportez-vous à la sectionDocumentation Microsoft Azure.

Configurer les composants Microsoft Azure

Effectuez les tâches suivantes dans Azure avant de mettre à l'échelle automatique des instances Citrix ADC VPX dans Citrix ADM.

1. Créer un réseau virtuel.
2. Créer des groupes de sécurité.
3. Créer des sous-réseaux.
4. Abonnez-vous à la licence Citrix ADC VPX dans Microsoft Azure.
5. Créer et enregistrer une demande.

Créer un réseau virtuel

1. Connectez-vous à votre portail Microsoft Azure.
2. Sélectionnez **Créer une ressource**.
3. Sélectionnez **Mise en réseau** et cliquez sur **Réseau virtuel** .
4. Spécifiez les paramètres requis.
    - Dans le **groupe de ressources**, vous devez spécifier le groupe de ressources dans lequel vous souhaitez déployer un produit Citrix ADC VPX.
    - Dans **Emplacement**, vous devez spécifier les emplacements qui prennent en charge les zones de disponibilité telles que :
        - USA Centre
        - Est US2
        - France Centre
        - Europe Nord
        - Asie du Sud-Est
        - Europe de l'Ouest
        - Ouest US2

> **Remarque**
>
> Les serveurs d'applications sont présents dans ce groupe de ressources.

5. Cliquez sur **Créer**.

Pour plus d'informations, consultez Réseau virtuel Azure dansDocumentation Microsoft.

Créer des groupes de sécurité

Créez trois groupes de sécurité dans votre réseau virtuel (VNet), chacun pour les connexions de gestion, de client et de serveur. Créez un groupe de sécurité pour contrôler le trafic entrant et sortant dans l'instance Citrix ADC VPX. Créez des règles pour le trafic entrant que vous souhaitez contrôler dans les groupes Citrix Autoscale. Vous pouvez ajouter autant de règles que vous voulez.

- **Gestion :** groupe de sécurité de votre compte dédié à la gestion de Citrix ADC VPX. Citrix ADC doit contacter les services Azure et nécessite un accès Internet. Les règles entrantes sont autorisées sur les ports TCP et UDP suivants.
  - TCP : 80, 22, 443, 3008—3011, 4001, 27000, 7279
  - UDP : 67, 123, 161, 500, 3003, 4500, 7000

  > **Remarque**
  >
  > Assurez-vous de ce qui suit :
  >
  > Le groupe de sécurité a autorisé l'agent Citrix ADM à accéder au VPX.
  >
  > Les ports 27000 et 7279 sont ouverts dans Citrix ADM. Ces ports sont utilisés pour extraire les licences Citrix ADC de Citrix ADM. Pour de plus amples informations, consultez la section Ports.

- **Client :** groupe de sécurité de votre compte dédié à une communication côté client des instances Citrix ADC VPX. En règle générale, les règles entrantes sont autorisées sur les ports TCP 80 et 443. Et, le port 60000 est nécessaire pour surveiller l'intégrité des instances ADC.
- **Serveur :** groupe de sécurité de votre compte dédié à une communication côté serveur de Citrix ADC VPX.

Pour plus d'informations sur la création d'un groupe de sécurité dans Microsoft Azure, reportez-vous à la section Créer, modifier ou supprimer un groupe de sécurité réseau.

Créer des sous-réseaux

Créez trois sous-réseaux dans votre réseau virtuel (VNet) - un pour chacun des connexions de gestion, client et serveur. Spécifiez une plage d'adresses définie dans votre réseau virtuel pour chacun des sous-réseaux. Spécifiez la zone de disponibilité dans laquelle vous souhaitez que le sous-réseau réside.

- **Gestion :** sous-réseau de votre réseau virtuel (VNet) dédié à la gestion. Citrix ADC doit contacter les services Azure et nécessite un accès Internet.
- **Client :** sous-réseau de votre réseau virtuel (VNet) dédié au côté client. En règle générale, Citrix ADC reçoit le trafic client pour l'application via un sous-réseau public à partir d'Internet.
- **Serveur :** sous-réseau dans lequel les serveurs d'applications sont provisionnés. Tous vos serveurs d'applications sont présents dans ce sous-réseau et reçoivent le trafic d'application de l'Citrix ADC via ce sous-réseau.

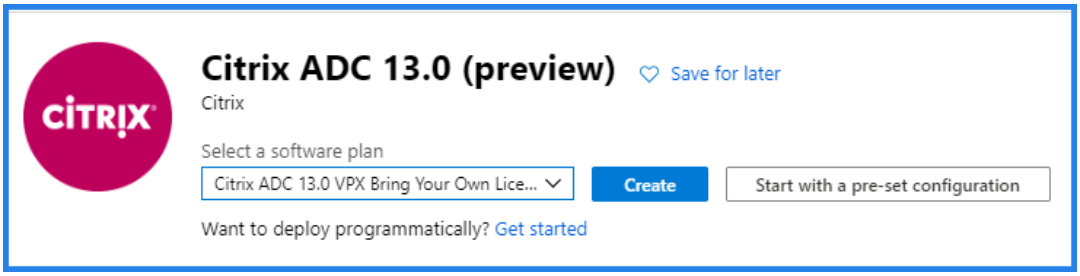
> **Remarque**
>
> Spécifiez un groupe de sécurité approprié pour le sous-réseau lors de la création d'un sous-réseau.

Pour plus d'informations sur la création d'un sous-réseau dans Microsoft Azure, reportez-vous à la section Ajouter, modifier ou supprimer un sous-réseau de réseau virtuel.

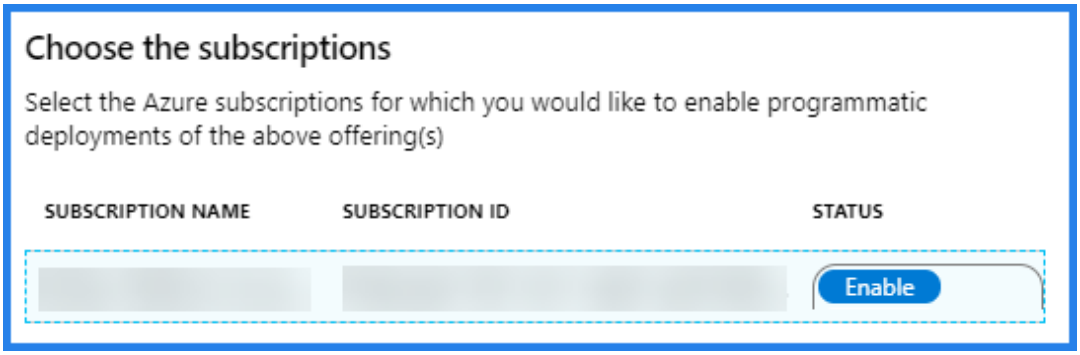
Abonnez-vous à la licence Citrix ADC VPX dans Microsoft Azure

1. Connectez-vous à votre portail Microsoft Azure.
2. Sélectionnez **Créer une ressource**.
3. Dans la barre **Rechercher le site de vente**, recherchez`Citrix ADC` et sélectionnez la version de produit requise.
4. Dans la liste **Sélectionner un plan logiciel**, sélectionnez l'un des types de licence suivants :
   - Apportez votre propre licence
   - Avancé
   - Premium

   > **Remarque**
   >
   > - Si vous choisissez l'option **Apporter votre propre licence**, le groupe Autoscale extrait les licences de Citrix ADM lors du Provisioning des instances Citrix ADC.
   > - Dans Citrix ADM, les licences **Advanced** et **Premium** sont les types de licences équivalents pour **Enterprise** et **Platinum** respectivement.
5. Assurez-vous que le déploiement programmatique est activé pour le produit Citrix ADC sélectionné.
   a) À côté **Vous voulez déployer par programme ?**, cliquez sur **Démarrer**.



b) Dans **Choisir les abonnements**, sélectionnez **Activer**pour déployer l'édition Citrix ADC VPX sélectionnée par programme.



> **Important**
>
> L'activation du déploiement par programmation est requise pour mettre à l'échelle automatique les instances Citrix ADC VPX dans Azure.

c) Cliquez sur **Enregistrer**.

d) Fermez **Configurer le déploiement programmatique**.

6. Cliquez sur **Créer**.

Créer et enregistrer une demande

Citrix ADM utilise cette application pour mettre à l'échelle automatique les instances Citrix ADC VPX dans Azure.

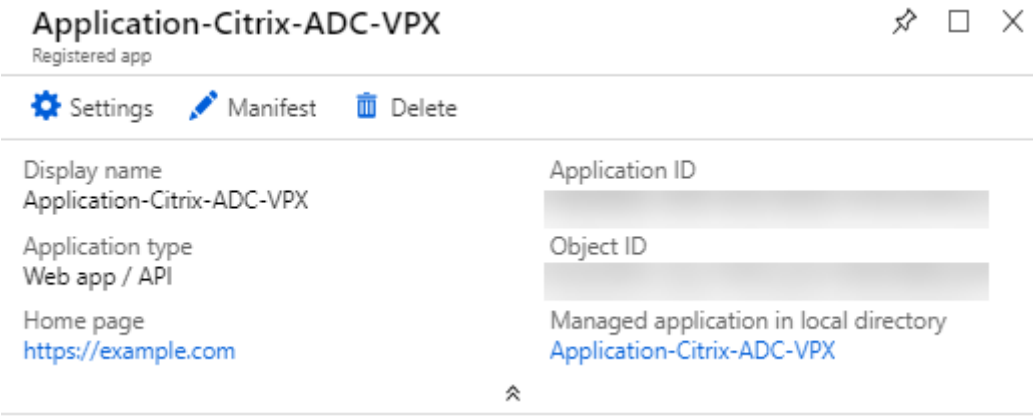
Pour créer et enregistrer une application dans Azure :

1. Dans le portail Azure, sélectionnez **Azure Active Directory**.
   Cette option affiche le répertoire de votre organisation.
2. Sélectionnez **Enregistrements d'applications** :
   a) Dans **Nom**, spécifiez le nom de l'application.
   b) Sélectionnez le **type d'application** dans la liste.
   c) Dans l'URL de **connexion**, spécifiez l'URL de l'application pour accéder à l'application.

3. Cliquez sur **Créer**.

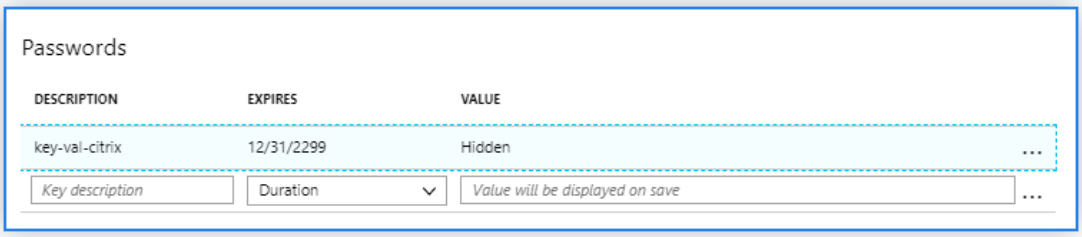
Pour plus d'informations sur les enregistrements d'applications, reportez-vous à la section Documentation Microsoft.

Azure affecte un ID d'application à l'application. Voici un exemple d'application enregistrée dans Microsoft Azure :



Copiez les ID suivants et fournissez ces ID lorsque vous configurez le profil Cloud Access dans Citrix ADM. Pour connaître les étapes à suivre pour récupérer les ID suivants, reportez-vous à la section Documentation Microsoft :

- ID de l'application
- ID de répertoire
- Key



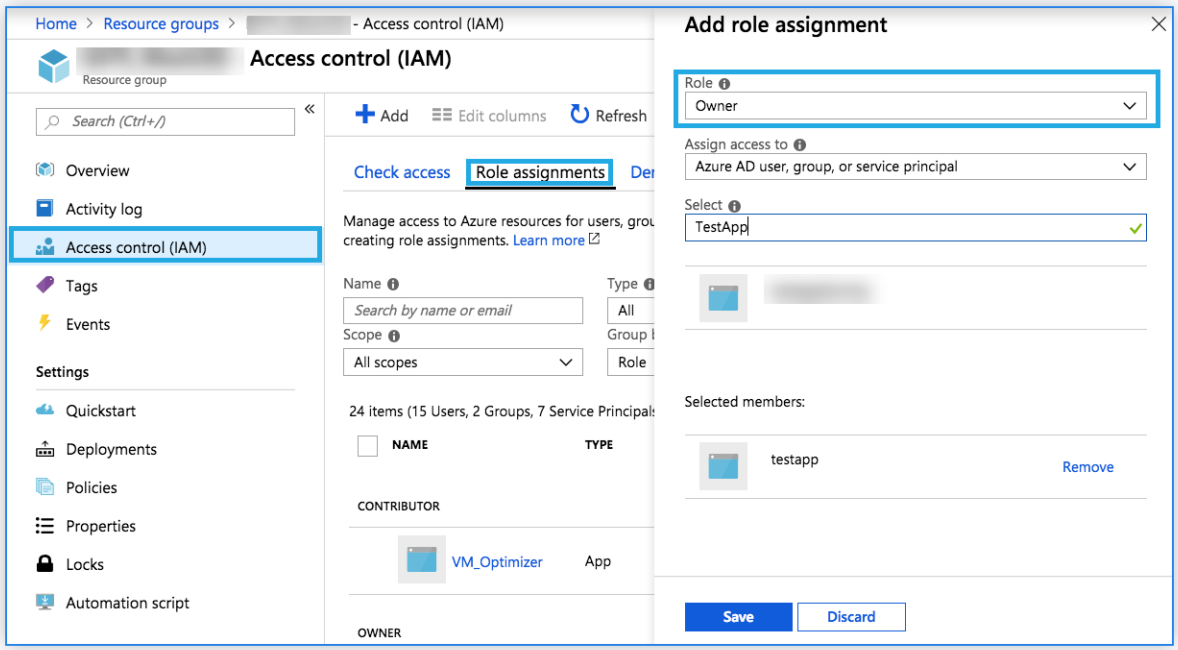
- ID d'abonnement : Copiez l'ID d'abonnement depuis votre compte de stockage.

Attribuer l'autorisation de rôle à une application

Citrix ADM utilise le principe de l'application en tant que service pour mettre à Autoscale des instances Citrix ADC dans Microsoft Azure. Cette autorisation s'applique uniquement au groupe de ressources sélectionné.

Pour attribuer une autorisation de rôle à votre application enregistrée, vous devez être le propriétaire de l'abonnement Microsoft Azure.

1. Dans le portail Azure, sélectionnez **Groupes de ressources**.
2. Sélectionnez le groupe de ressources auquel vous souhaitez attribuer une autorisation de rôle.
3. Sélectionnez **Contrôle d'accès (IAM)**.
4. Dans **Affectations de rôles**, cliquez sur **Ajouter**.
5. Sélectionnez **Propriétaire** dans la liste **Rôle** .
6. Sélectionnez l'application enregistrée pour la mise à l'échelle automatique des instances Citrix ADC.
7. Cliquez sur **Enregistrer**.



Configurer les composants Citrix ADM

Effectuez les tâches suivantes dans Azure avant de mettre à l'échelle automatique des instances Citrix ADC VPX dans Citrix ADM :

1. Provisionner un agent sur Azure
2. Créer un site
3. Attacher le site à un agent de service Citrix ADM

Provisionner l'agent Citrix ADM sur Azure

L'agent de service Citrix ADM fonctionne comme intermédiaire entre Citrix ADM et les instances découvertes dans le centre de données ou sur le cloud.

1. Accédez à **Réseaux > Agents**.
2. Cliquez sur **Provisionner**.
3. Sélectionnez **Microsoft Azure** et cliquez sur **Suivant**.
4. Dans l'onglet **Paramètres de provisionnement**, spécifiez les éléments suivants :
    - **Nom** : spécifiez le nom de l'agent Citrix ADM.
    - **Site** : sélectionnez le site que vous avez créé pour provisionner un agent et des instances VPX ADC.
    - **Profil d'accès au nuage** : sélectionnez le profil d'accès au nuage dans la liste.
    - **Zone de disponibilité** : sélectionnez les zones dans lesquelles vous souhaitez créer les groupes de mise à l'Autoscale. Selon le profil d'accès au nuage que vous avez sélectionné, les zones de disponibilité spécifiques à ce profil sont remplies.
    - **Groupe de** sécurité : les groupes de sécurité contrôlent le trafic entrant et sortant dans l'agent Citrix ADC. Vous créez des règles pour le trafic entrant et sortant que vous souhaitez contrôler.
    - **Sous-réseau** : sélectionnez le sous-réseau de gestion dans lequel vous souhaitez provisionner un agent.
    - **Tags** - Tapez la paire clé-valeur pour les balises du groupe Autoscale. Une balise est constituée d'une paire clé-valeur sensible à la casse. Ces balises vous permettent d'organiser et d'identifier facilement les groupes de mise à l'échelle automatique. Les balises sont appliquées à Azure et Citrix ADM.
5. Cliquez sur **Terminer**.

Vous pouvez également installer l'agent Citrix ADM à partir de la Place de Azure Marketplace. Pour de plus amples informations, consultez la section Installation d'un agent Citrix ADM sur Microsoft Azure.

Créer un site

Créez un site dans Citrix ADM et ajoutez les détails de réseau virtuel associés à votre groupe de ressources Microsoft Azure.

1. Dans Citrix ADM, accédez à **Réseaux** > **Sites** .
2. Cliquez sur **Ajouter**.
3. Dans le volet **Sélectionner le Cloud**,
    a) Sélectionnez **Centre de données** comme **type de site**.
    b) Choisissez **Azure** dans la liste **Type**.

c) Cochez la case **Récupérer le réseau virtuel virtuel à partir d'Azure**.

Cette option vous aide à récupérer les informations de réseau virtuel existantes à partir de votre compte Microsoft Azure.

d) Cliquez sur **Suivant**.

4. Dans le panneau **Choisir une région**,

a) Dans **Cloud Access Profile**, sélectionnez le profil créé pour votre compte Microsoft Azure. S'il n'y a pas de profils, créez un profil.

b) Pour créer un profil d'accès au cloud, cliquez sur **Ajouter**.

c) Dans **Nom**, spécifiez un nom pour identifier votre compte Azure dans Citrix ADM.

d) Dans **ID Active Directory de locataire/ID de locataire**, spécifiez l'ID Active Directory du locataire ou du compte dans Microsoft Azure.

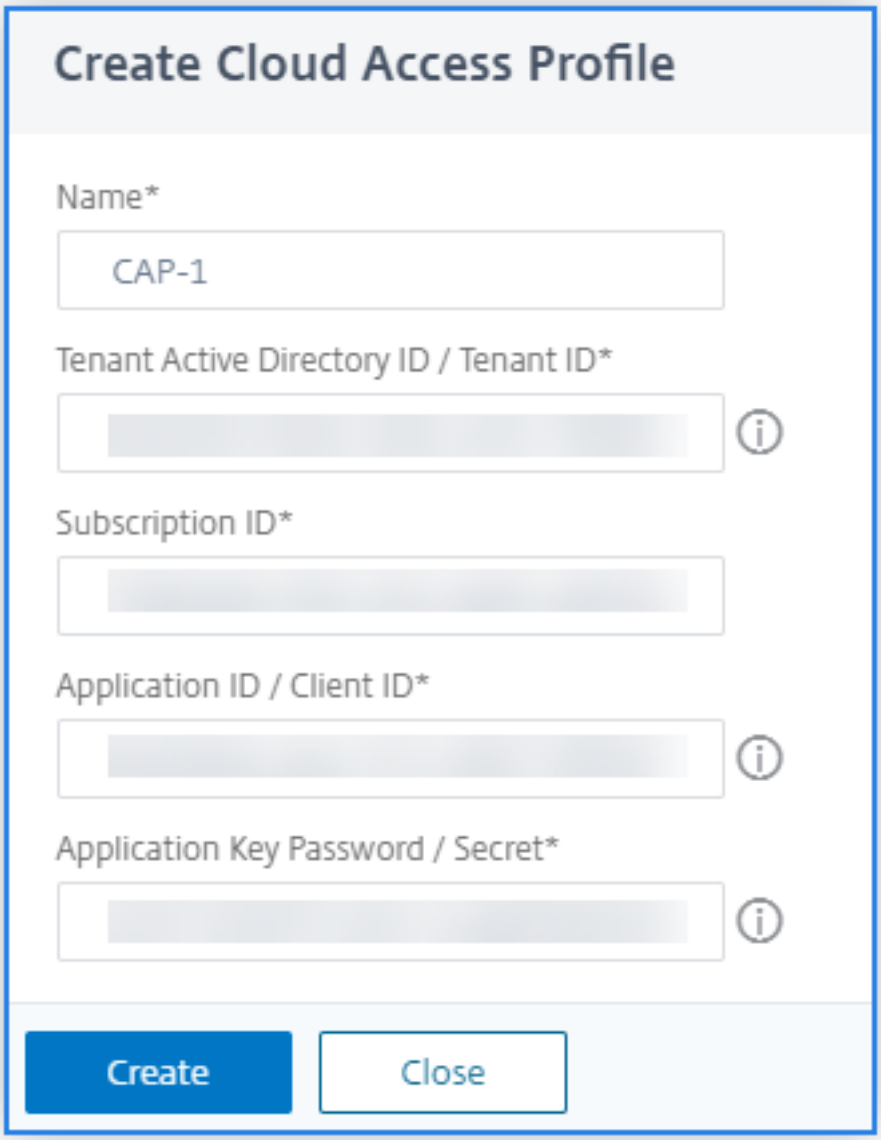
e) Spécifiez l' **ID d'abonnement**.

f) Spécifiez l' **ID d'application ID/client**.

g) Spécifiez le mot de **Secret/mot de passe de la clé d'application**.

h) Cliquez sur **Créer**.

Pour plus d'informations, veuillez consulter Créer et enregistrer une demande et Mappage du profil d'accès au cloud à l'application Azure.



i) Dans **VNet**, sélectionnez le réseau virtuel contenant les instances Citrix ADC VPX que vous souhaitez gérer.

j) Spécifiez un **nom de site**.

k) Cliquez sur **Terminer**.

Mapping du profile d'accès au Cloud à l'application Azure

Terme Citrix ADM	Terme Microsoft Azure
ID Active Directory du locataire/ID du locataire	ID de répertoire
ID d'abonnement	ID d'abonnement
Identifiant de l'application et du client	ID de l'application
Mot de passe de la clé d'application/Secret	Clés ou certificats ou secrets client

Attacher le site à un agent de service Citrix ADM

1. Dans Citrix ADM, accédez à **Réseaux** > **Agents** .
2. Sélectionnez l'agent pour lequel vous souhaitez attacher un site.
3. Cliquez sur **Joindre le site**.
4. Sélectionnez le site dans la liste que vous souhaitez joindre.
5. Cliquez sur **Enregistrer**.

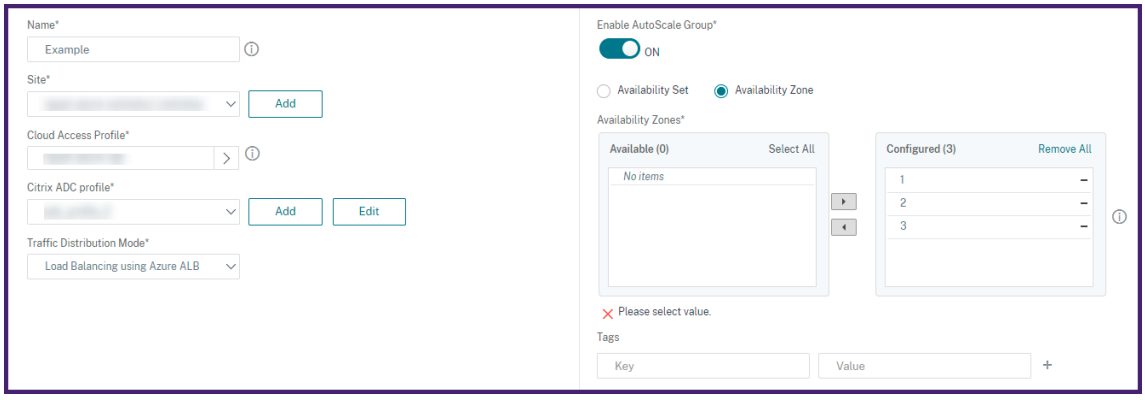
Étape 1 : Initialiser la configuration de mise à l'échelle automatique dans Citrix ADM

1. Dans Citrix ADM, accédez à **Réseaux** > **Groupes d'échelle automatique** .
2. Cliquez sur **Ajouter** pour créer des groupes de mise à l'échelle automatique.

   La page **Créer un groupe de mise à l'échelle automatique** s'affiche.
3. Sélectionnez **Microsoft Azure** et cliquez sur **Suivant**.
4. Dans **Paramètres de base**, entrez les détails suivants :
   - **Nom :** saisissez un nom pour le groupe Mise à l'échelle automatique.
   - **Site :** sélectionnez le site que vous avez créé pour mettre à l'échelle automatique les instances Citrix ADC VPX sur Microsoft Azure. Si vous n'avez pas créé de site, cliquez sur **Ajouter** pour créer un site.
   - **Agent :** sélectionnez l'agent Citrix ADM qui gère les instances provisionnées.
   - **Profil d'accès au cloud :** sélectionnez le profil d'accès au cloud. Vous pouvez également ajouter ou modifier un profil Cloud Access.
   - **Profil de périphérique :** sélectionnez le profil de périphérique dans la liste. Citrix ADM utilise le profil de périphérique lorsqu'il doit ouvrir une session à l'instance Citrix ADC VPX.

> **Remarque**
>
> Assurez-vous que le profil de périphérique sélectionné est conforme à Règles de mot de passe Microsoft Azure.

- **Mode de distribution du trafic :** l'option **Équilibrage de la charge à l'aide d'Azure LB** est sélectionnée comme mode de distribution du trafic par défaut. Vous pouvez également choisir le **DNS à l'aide du mode DNS Azure** pour la distribution du trafic.
- **Activer le groupe AutoScale :** Activez ou désactivez l'état des groupes ASG. Cette option est activée par défaut. Si cette option est désactivée, la mise à l'échelle automatique n'est pas déclenchée.
- **Jeu de disponibilité ou Zone de disponibilité :** sélectionnez le jeu de disponibilité ou les zones de disponibilité dans lesquelles vous souhaitez créer les groupes de mise à l'échelle automatique. Selon le profil d'accès au cloud que vous avez sélectionné, les zones de disponibilité apparaissent dans la liste.
- **Tags :** saisissez la paire clé-valeur pour les balises de groupe de mise à l'échelle automatique. Une balise est constituée d'une paire clé-valeur sensible à la casse. Ces balises vous permettent d'organiser et d'identifier facilement les groupes de mise à l'échelle automatique. Les balises sont appliquées à Microsoft Azure et Citrix ADM.



5. Cliquez sur **Suivant**.

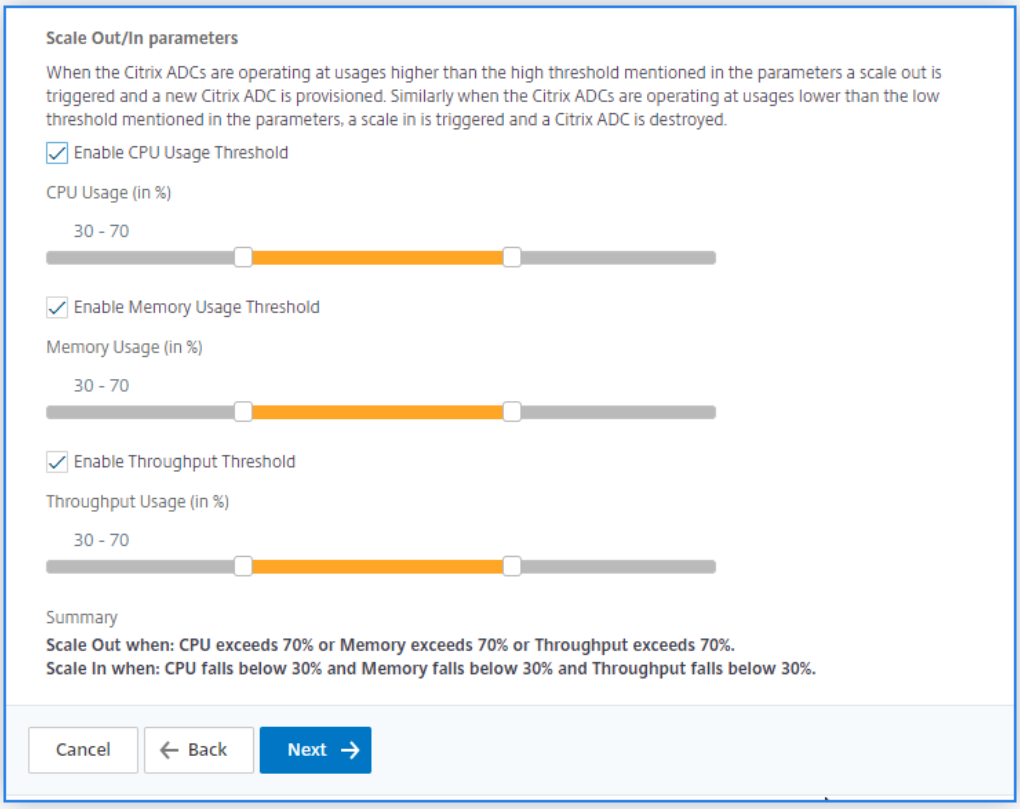
Étape 2 : Configurer les paramètres de mise à l'échelle automatique

1. Dans l'onglet **Paramètres de mise à l'échelle automatique**, entrez les détails suivants.
2. Sélectionnez un ou plusieurs des paramètres de seuil suivants dont les valeurs doivent être surveillées pour déclencher une mise à l'échelle ou une mise à l'échelle.
   - **Activer le seuil d'utilisation de l'UC :** surveillez les mesures en fonction de l'utilisation de l'UC.

- **Activer le seuil d'utilisation de la mémoire :** surveillez les mesures en fonction de l'utilisation de la mémoire.
- **Activer le seuil de débit :** surveillez les mesures en fonction du débit.

  Remarque

  - La limite de seuil minimale par défaut est de 30 et la limite de seuil maximale est de 70. Toutefois, vous modifiez les limites.
  - La limite minimale de seuil doit être égale ou inférieure à la moitié de la limite maximale de seuil.
  - Vous pouvez sélectionner plusieurs paramètres de seuil pour la surveillance. La mise à l'échelle est déclenchée si au moins un des paramètres de seuil est au-dessus du seuil maximal. Cependant, une mise à l'échelle n'est déclenchée que si tous les paramètres de seuil fonctionnent en dessous de leurs seuils normaux.



- **Conservez un nœud de rechange pour une mise à l'échelle plus rapide :** cette option permet d'obtenir une évolutivité plus rapide. ADM met en service un nœud de secours avant que l'action de mise à l'échelle ne se produise et l'arrête. Lorsque l'action de scale-out se produit pour le groupe Mise à l'Autoscale, l'ADM démarre le nœud de rechange déjà provisionné. En conséquence, il réduit le temps nécessaire pour la mise à l'échelle.

- **Instances minimales :** sélectionnez le nombre minimal d'instances qui doivent être provisionnées pour ce groupe de mise Autoscale.

  Le nombre minimal d'instances par défaut est égal au nombre de zones sélectionnées. Vous ne pouvez incrémenter les instances minimales que dans les multiples du nombre de zones spécifié.

  Par exemple, si le nombre de zones de disponibilité est 4, les instances minimales sont 4 par défaut. Vous pouvez augmenter les instances minimales de 8, 12, 16.

- **Maximum d'instances :** sélectionnez le nombre maximal d'instances qui doivent être provisionnées pour ce groupe de mise Autoscale.

  Le nombre maximal d'instances doit être supérieur ou égal à la valeur des instances minimales. Le nombre maximal d'instances ne peut pas dépasser le nombre de zones de disponibilité multiplié par 32.

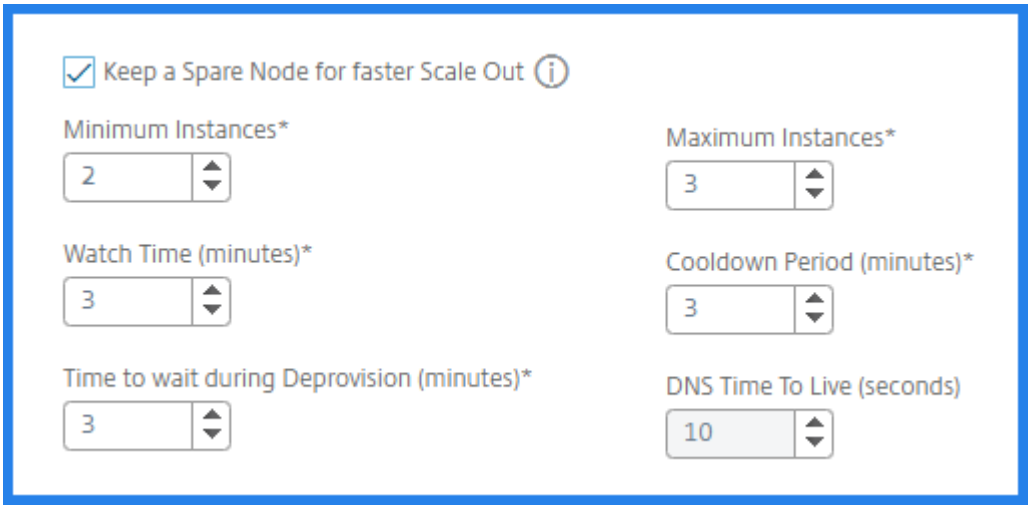
  Nombre maximal d'instances = nombre de zones de disponibilité * 32

- **Temps de surveillance (minutes) :** sélectionnez la durée de surveillance. Durée pendant laquelle le seuil du paramètre d'échelle doit rester dépassé pour que la mise à l'échelle se produise. Si le seuil est dépassé sur tous les échantillons prélevés dans ce délai, une mise à l'échelle se produit.

- **Période de recharge (minutes) :** sélectionnez la période de recharge. Pendant la mise à l'échelle, la période de recharge correspond à la période pendant laquelle l'évaluation des statistiques doit être arrêtée après une mise à l'échelle. Cette période garantit la croissance organique des instances d'un groupe Autoscale. Avant de déclencher la prochaine décision de mise à l'échelle, il attend que le trafic actuel se stabilise et se stabilise sur l'ensemble d'instances en cours.

- **Temps d'attente pendant la déprovisionnement (minutes) :** sélectionnez le délai d'expiration de la connexion de vidange. Au cours de l'action de mise à l'échelle, une instance est identifiée à désapprovisionner. Citrix ADM limite l'instance identifiée de traiter les nouvelles connexions jusqu'à ce que le délai spécifié expire avant le retrait du provisionnement. Au cours de cette période, il permet de vider les connexions existantes à cette instance avant qu'elle ne soit déprovisionnée.

- **Durée de vie DNS (secondes) :** sélectionnez l'heure (en secondes). Pendant cette période, un paquet est défini pour exister à l'intérieur d'un réseau avant que le routeur ne le rejette. Ce paramètre est applicable uniquement lorsque le mode de distribution du trafic est DNS à l'aide du gestionnaire de trafic Microsoft Azure.



3. Cliquez sur **Suivant**.

Étape 3 : Configuration des licences pour le Provisioning des instances Citrix ADC

Sélectionnez l'un des modes suivants pour concéder des licences aux instances Citrix ADC qui font partie du groupe de mise à l'Autoscale :

- **Utilisation de Citrix ADM** : Lors du Provisioning d'instances Citrix ADC, le groupe Autoscale extrait les licences de Citrix ADM.
- **Utilisation de Microsoft Azure** : l'option **Allouer à partir du Cloud** utilise les licences de produit Citrix disponibles sur la Place de marché Azure. Lors du Provisioning des instances Citrix ADC, le groupe Autoscale utilise les licences du marché.

  Si vous choisissez d'utiliser des licences de la Place de Azure Marketplace, spécifiez le produit ou la licence dans l'onglet **Paramètres de provisionnement**.

Pour de plus amples informations, consultez la section Exigences en matière de licences.

Utiliser les licences de Citrix ADM

Pour utiliser cette option, assurez-vous que vous êtes abonné au produit Citrix ADC avec le plan de logiciel **BYOL (avec apport de sa propre licence)** dans Azure. Consultez Abonnez-vous à la licence Citrix ADC VPX dans Microsoft Azure.

1. Dans l'onglet **Licence**, sélectionnez **Allouer à partir d'ADM**.
2. Dans **Type de licence**, sélectionnez l'une des options suivantes dans la liste :
   - **Licences de bande passante :** vous pouvez sélectionner l'une des options suivantes dans la liste **Types de licences de bande passante** :

- **Capacité groupée :** spécifiez la capacité à allouer pour chaque nouvelle instance du groupe Mise à l'échelle automatique.

  À partir du pool commun, chaque instance ADC du groupe Autoscale retire une licence d'instance et seule la bande passante est spécifiée.

- **Licences VPX :** Lorsqu'une instance Citrix ADC VPX est provisionnée, l'instance extraire la licence auprès de Citrix ADM.

- **Licences de processeur virtuel :** l'instance Citrix ADC VPX provisionnée récupère les licences en fonction du nombre de processeurs exécutant dans le groupe Autoscale.

> **Remarque**
>
> Lorsque les instances provisionnées sont supprimées ou détruites, les licences appliquées retournent au pool de licences Citrix ADM. Ces licences peuvent être réutilisées pour provisionner de nouvelles instances lors de la prochaine mise à l'Autoscale.

3. Dans **License Edition**, sélectionnez l'édition de licence. Le groupe Mise à l'échelle automatique utilise l'édition spécifiée pour provisionner des instances.
4. Cliquez sur **Suivant**.

Étape 4 : Configurer les paramètres du nuage

1. Dans l'onglet **Paramètres de provisionnement**, entrez les détails suivants :

   - **Groupe de ressources :** sélectionnez le groupe de ressources dans lequel les instances Citrix ADC sont déployées.
   - **Produit/Licence :** sélectionnez la version du produit Citrix ADC que vous souhaitez provisionner. Assurez-vous que l'accès par programmation est activé pour le type sélectionné. Pour de plus amples informations, consultez la section Abonnez-vous à la licence Citrix ADC VPX dans Microsoft Azure.
   - **Taille de la machine virtuelle Azure :** sélectionnez la taille de la machine virtuelle requise dans la liste.

     > **Remarque**
     >
     > Assurez-vous que la taille de la machine virtuelle Azure sélectionnée possède au moins trois cartes réseau. Pour de plus amples informations, consultez la section Images virtuelles Azure prises en charge pour la mise à l'échelle automatique.

   - **Cloud Access Profile for ADC :** Citrix ADM se connecte à votre compte Azure à l'aide de ce profil pour provisionner ou désapprovisionner les instances ADC. Il configure également Azure LB ou Azure DNS.

- **Image :** sélectionnez l'image de version Citrix ADC requise. Cliquez sur **Ajouter un nouveau** pour ajouter une image Citrix ADC.
- **Groupes de sécurité :** les groupes de sécurité contrôlent le trafic entrant et sortant dans une instance Citrix ADC VPX. Sélectionnez un groupe de sécurité pour le trafic Gestion, Client et Serveur. Pour plus d'informations sur les groupes de sécurité de gestion, de client et de serveur, reportez-vous à la sectionGroupes de sécurité.
- **Sous-réseaux :** vous devez disposer de trois sous-réseaux distincts tels que le sous-réseau Gestion, client et serveur pour les sous-réseaux Citrix ADC à mise à l'échelle automatique. Les sous-réseaux contiennent les entités requises pour la mise à l'échelle automatique. Sélectionnez Pour plus d'informations, reportez-vous à la sectionSous-réseaux.

2. cliquez sur **Terminer**.

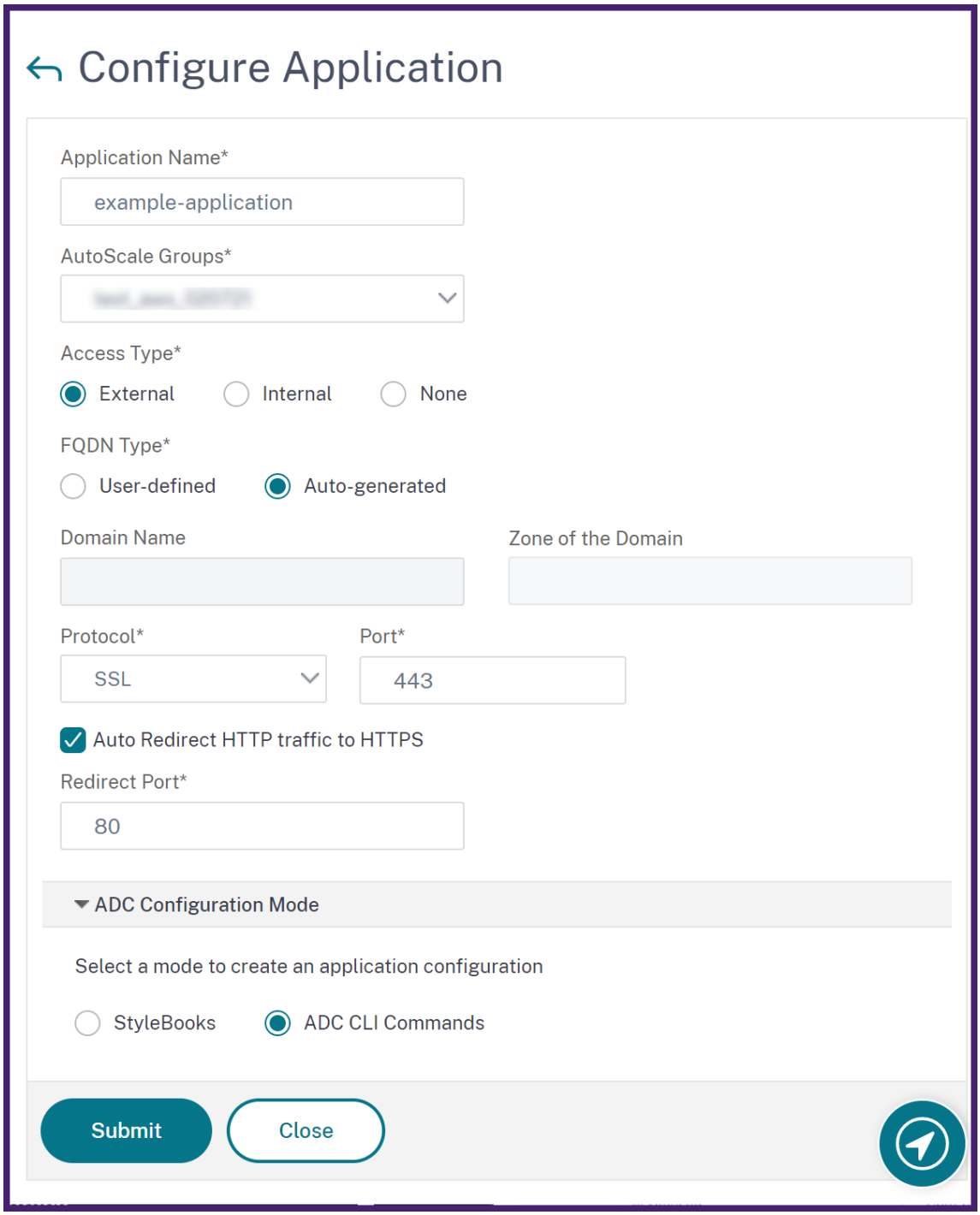
Étape 5 : Configurer une application pour le groupe Mise à l'échelle automatique

1. Dans Citrix ADM, accédez à **Réseaux** > **Groupes de mise à Autoscale**.
2. Sélectionnez le groupe de mise à l'échelle automatique que vous avez créé et cliquez sur **Configurer**.
3. Dans **Configurer l'application**, spécifiez les détails suivants :
   - **Nom de l'application** : spécifiez le nom d'une application.
   - **Type d'accès** : vous pouvez utiliser la solution de mise à l'échelle automatique ADM pour des applications externes et internes. Sélectionnez le type d'accès à l'application requis.
   - **Type de nom de domaine complet** - Sélectionnez un mode d'attribution de noms de domaine et de zone.

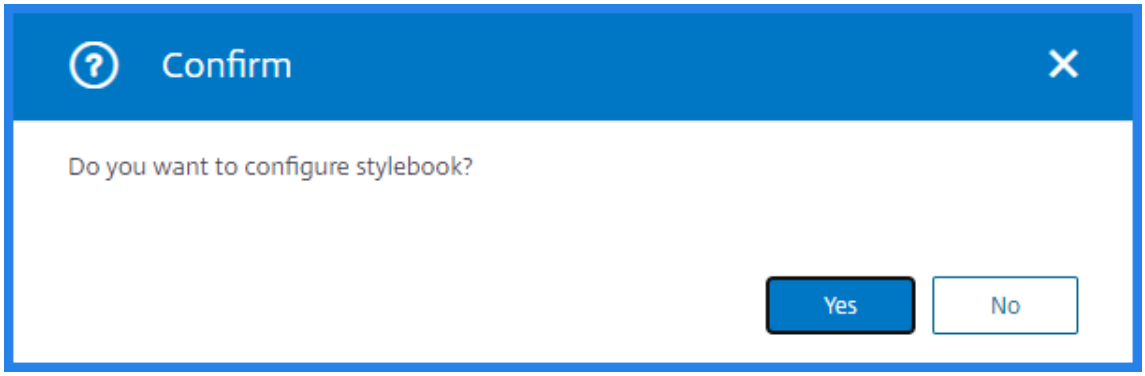
     Si vous souhaitez spécifier manuellement, sélectionnez Définie **par l'utilisateur**. Pour attribuer automatiquement des noms de domaine et de zone, sélectionnez **Généré automatiquement**.
   - **Nom de domaine** - Spécifiez le nom de domaine d'une application. Cette option n'est applicable que lorsque vous sélectionnez Type de nom de domaine complet défini par l'utilisateur.
   - **Zone du domaine** : sélectionnez le nom de zone d'une application dans la liste. Cette option n'est applicable que lorsque vous sélectionnez Type de nom de domaine complet défini par l'utilisateur.

     Ce nom de domaine et de zone redirige vers les serveurs virtuels dans Azure. Par exemple, si vous hébergez une application dans `app.example.com`, le `app` est le nom de domaine et `example.com` le nom de la zone.

- **Protocole** : sélectionnez le type de protocole dans la liste. L'application configurée reçoit le trafic en fonction du type de protocole sélectionné.
- **Port** : spécifiez la valeur du port. Le port spécifié est utilisé pour établir une communication entre l'application et le groupe Mise à l'Autoscale.

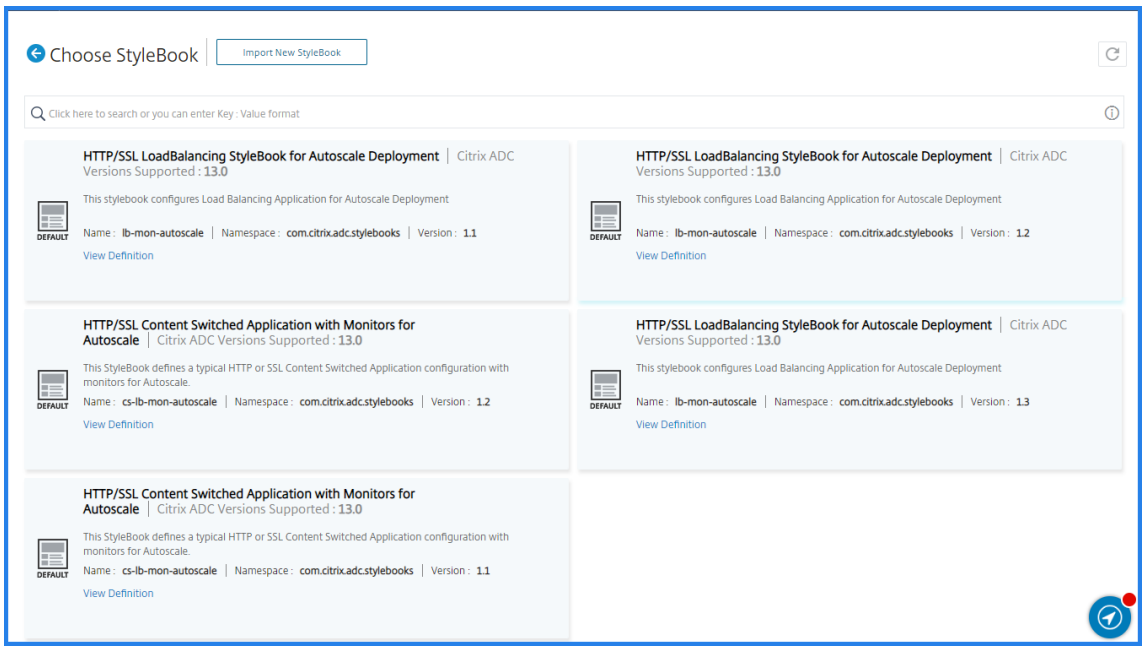


Si vous souhaitez configurer une application à l'aide de StyleBooks, sélectionnez **Oui** dans la fenêtre de confirmation.



> **Remarque**
>
> Modifiez le type d'accès d'une application si vous souhaitez modifier les détails suivants à l'avenir :
>
> - Type de nom de domaine complet
> - Nom de domaine
> - Zone du domaine

4. Choisissez le StyleBook requis que vous souhaitez déployer des configurations pour le groupe de mise à l'échelle automatique sélectionné.



Si vous souhaitez importer des StyleBooks, cliquez sur **Importer un nouveau StyleBook**.

5. Spécifiez les valeurs de tous les paramètres.

   Les paramètres de configuration sont prédéfinis dans le StyleBook sélectionné.

6. Cochez la case **Type de groupe de serveurs d'applications CLOUD** pour spécifier les serveurs d'applications disponibles dans le jeu d'échelle de machine virtuelle.

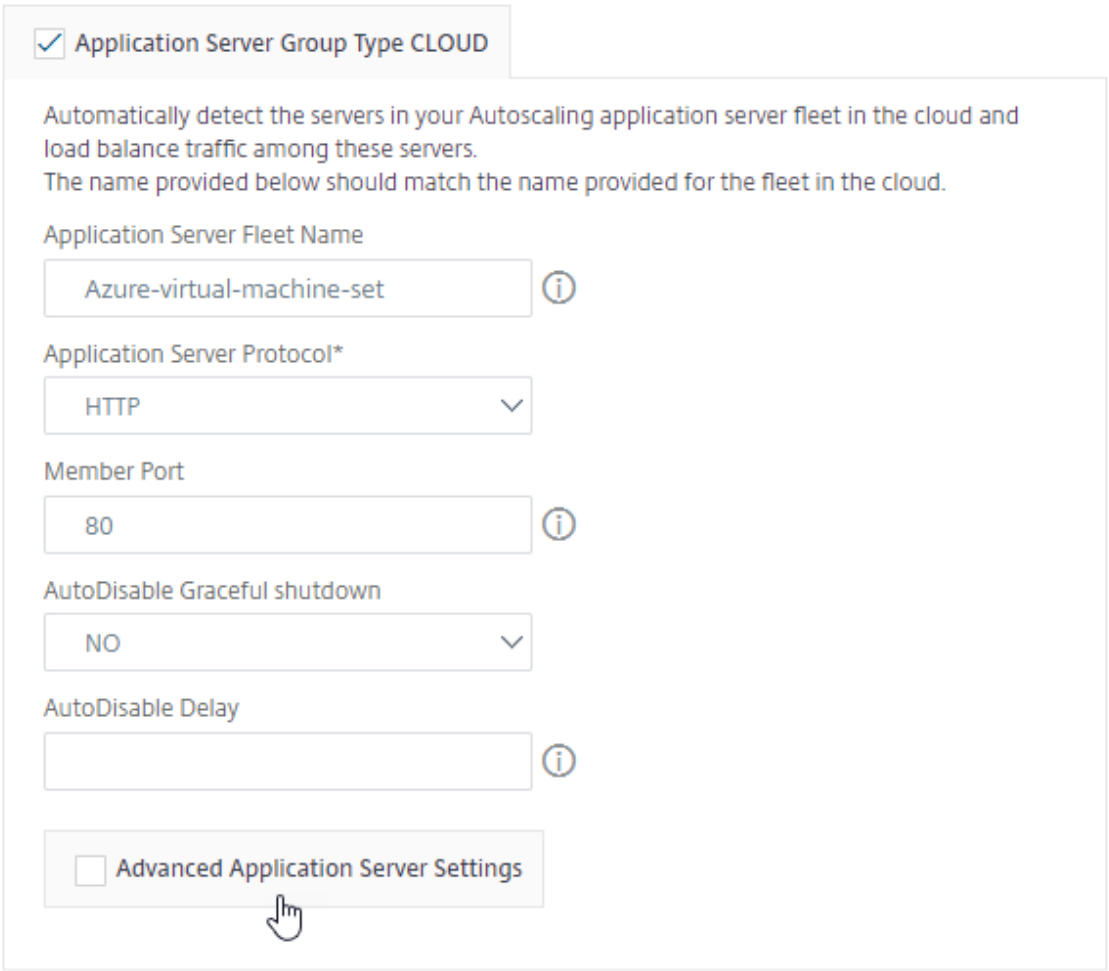
a) Dans **Application Server Fleet Name**, spécifiez le **nom du paramètre Mise Autoscale** de votre jeu d'échelle de machine virtuelle.

b) Sélectionnez **Application Server Protocol** dans la liste.

c) Dans **Port membre**, spécifiez la valeur de port du serveur d'applications.

> **Remarque**
>
> Assurez-vous que la **désactivation automatique Graceful Shutdown** est définie sur **Non** et le champ **Retard de désactivation automatique** est vide.

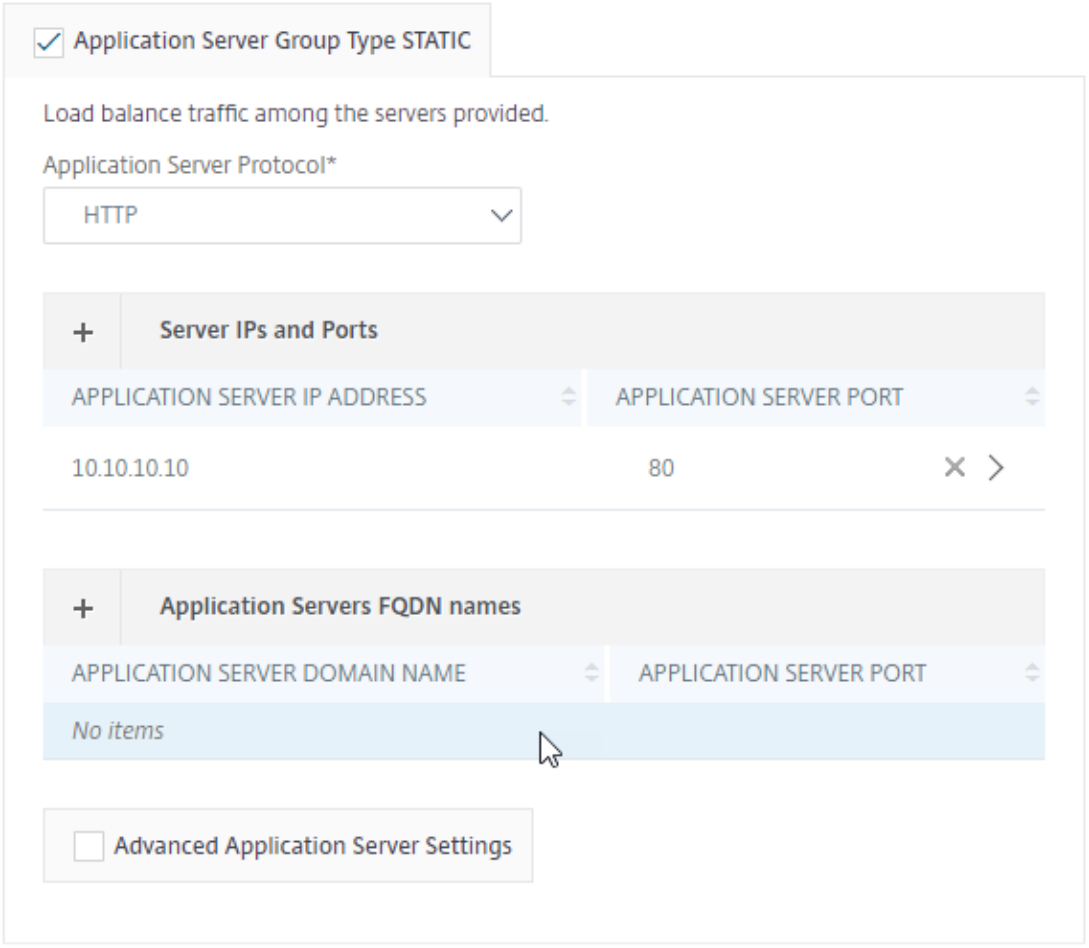
d) Si vous souhaitez spécifier les paramètres avancés de vos serveurs d'applications, cochez la case **Paramètres avancés du serveur d'applications**. Ensuite, spécifiez les valeurs requises répertoriées sous **Paramètres avancés du serveur d'applications**.



7. Si vous avez des serveurs d'applications autonomes dans le réseau virtuel, cochez la case **Type de groupe de serveurs d'applications STATIC** :

a) Sélectionnez **Application Server Protocol** dans la liste.

b) Dans les **adresses IP et ports du serveur**, cliquez sur **+**pour ajouter une adresse IP du serveur d'applications, un port et un poids, puis cliquez sur **Créer**.



8. Cliquez sur **Créer**.

Modifier la configuration des groupes de mise à l'échelle automatique

Vous pouvez modifier une configuration de groupe de mise à l'échelle automatique ou supprimer un groupe de mise à l'échelle automatique. Vous ne pouvez modifier que les paramètres de groupe d'échelle automatique suivants :

- Limites maximales et minimales des paramètres de seuil
- Valeurs d'instance minimales et maximales
- Valeur de la période de drainage des connexions
- Valeur de la période de recharge
- Valeur de durée de la surveillance

Vous pouvez également supprimer les groupes de mise à l'échelle automatique après leur création.

Lorsqu'un groupe de mise à l'échelle automatique est supprimé, tous les domaines et adresses IP sont désenregistrés du DNS et les nœuds de cluster sont déprovisionnés.

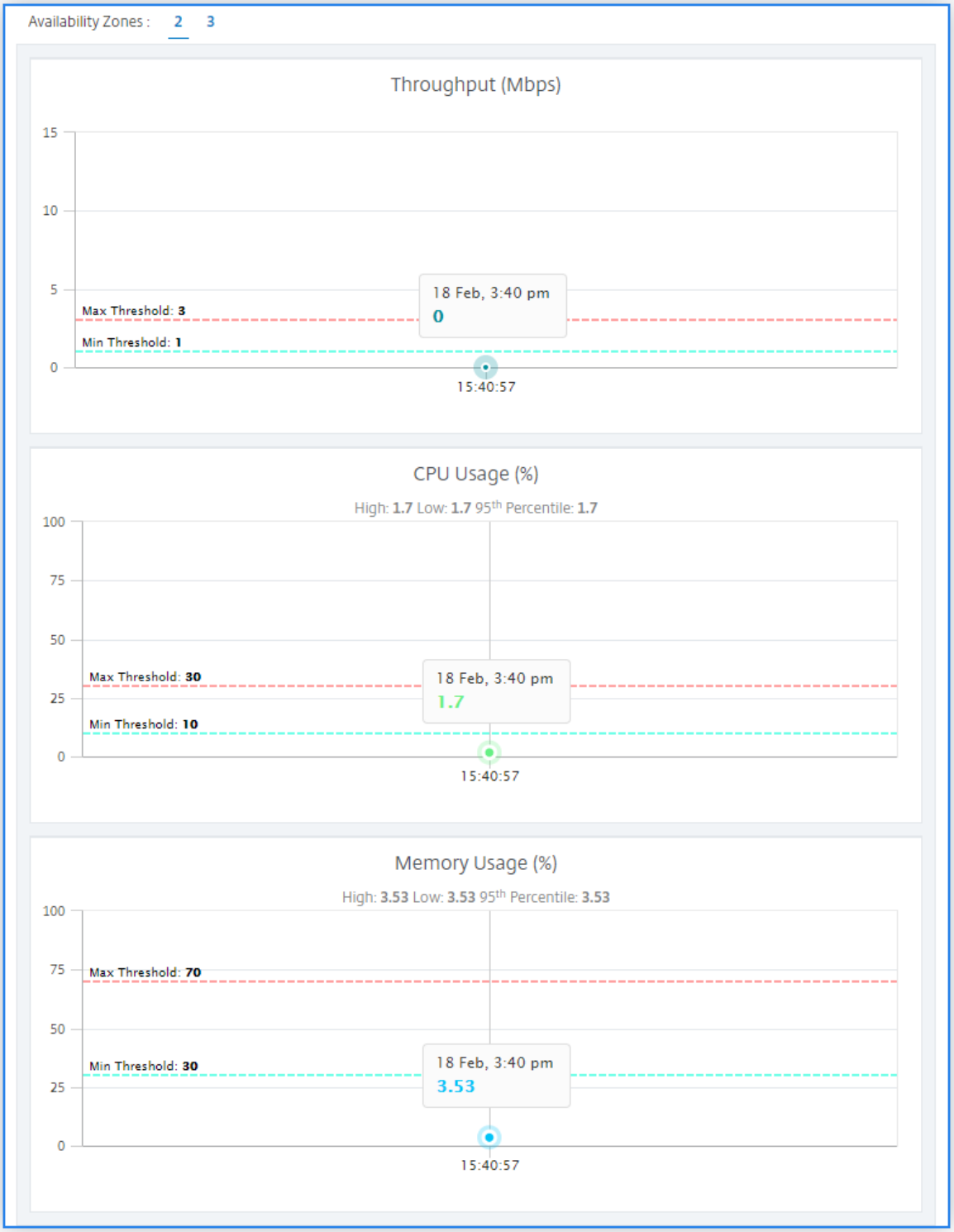
Tableau de bord

April 29, 2021

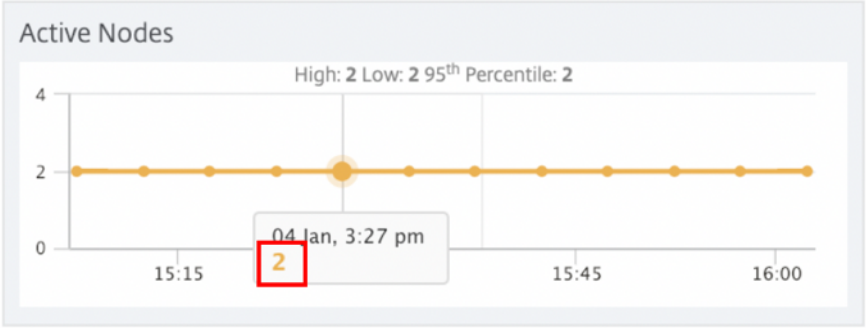
1. Dans Citrix ADM, accédez à **Réseaux > Groupes de mise à l'échelle automatique**.
2. Sélectionnez le groupe de mise à l'échelle automatique et cliquez sur **Tableau de bord**.

Vous pouvez afficher le graphique des paramètres de surveillance sélectionnés. Le panneau de droite affiche les événements qui déclenchent la mise à l'échelle automatique. Le panneau de gauche affiche les nœuds actifs dans le cluster par zone, le graphique des nœuds actifs et les événements.

La figure suivante affiche un exemple de tableau de bord.

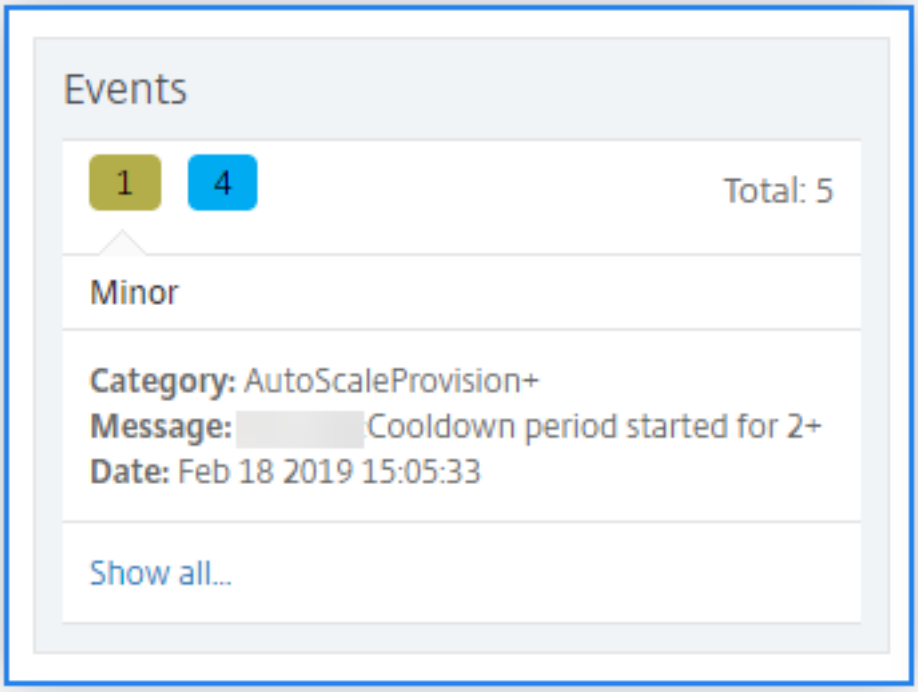


La figure suivante affiche le graphique des nœuds actifs. Le nombre sous l'horodatage indique le nombre de nœuds actifs. Vous pouvez afficher le nombre de nœuds actifs qui font partie de la zone de disponibilité à tout moment.

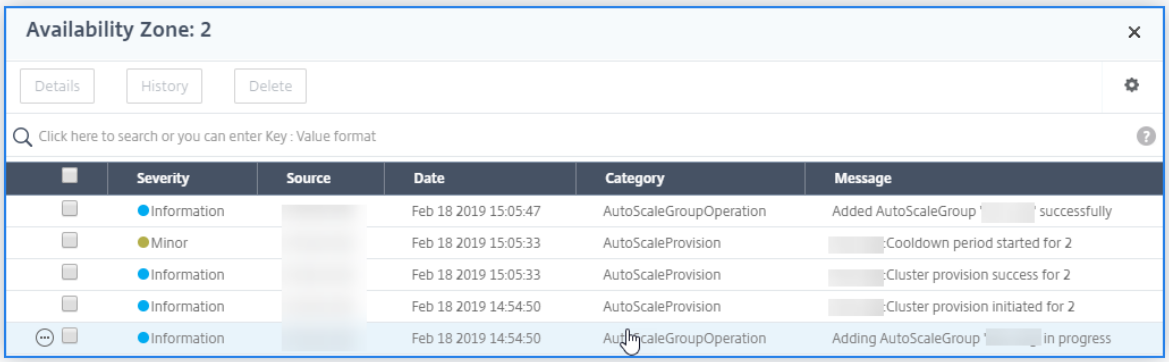


Événements

Dans **Tableau de bord**, l'onglet **Événements**affiche le nombre total d'événements pour le groupe de mise à l'échelle automatique sélectionné. Il affiche également un bref message du dernier événement.



Pour afficher les détails des événements, cliquez sur **Afficher tout**.



Terminologies Azure

April 29, 2021

Voici la liste des terminologies Azure requises dans Citrix ADM :

Terme	Définition
Équilibreur de charge Azure	L'équilibreur de charge Azure est une ressource qui distribue le trafic entrant entre les instances Citrix ADC VPX dans un réseau. Le trafic est distribué entre les machines virtuelles définies dans un jeu d'équilibrage de charge. Un équilibreur de charge peut être externe ou connecté à Internet, ou il peut être interne.
Gestionnaire de trafic	Le gestionnaire de trafic Azure est l'équilibreur de charge basé sur DNS dans Microsoft Azure. Il envoie le trafic entrant à l'instance Citrix ADC VPX souhaitée dans un réseau.
Azure Resource Manager (ARM)	ARM est le nouveau cadre de gestion pour les services dans Azure. Azure Load Balancer est géré à l'aide d'API et d'outils ARM.
Pool d'adresses back-end	Ces adresses IP sont associées à la carte réseau de la machine virtuelle à laquelle la charge est distribuée.
BLOB	Binary Large Object — Tout objet binaire tel qu'un fichier ou une image qui peut être stocké dans le stockage Azure.

Terme	Définition
Configuration IP front-end	Un équilibreur de charge Azure peut inclure une ou plusieurs adresses IP front-end, également appelées adresses IP virtuelles (VIP). Ces adresses IP servent d'entrée pour le trafic.
IP publique au niveau de l'instance (ILPIP)	Un ILPIP est une adresse IP publique que vous pouvez attribuer directement à votre machine virtuelle ou instance de rôle au lieu du service cloud. Cette IP ne remplace pas le VIP (IP virtuelle) attribué à votre service cloud. Il s'agit plutôt d'une adresse IP supplémentaire que vous pouvez utiliser pour vous connecter directement à votre machine virtuelle ou instance de rôle.
Règles NAT entrantes	Ces règles mappent un port public sur l'équilibreur de charge à un port pour la machine virtuelle spécifique dans le pool d'adresses back-end.
Config IP	Il s'agit d'une paire d'adresses IP (IP publique et IP privée) associée à une carte réseau individuelle. Dans une configuration IP, l'adresse IP publique peut être NULL. Chaque carte réseau peut être associée à plusieurs IP Config jusqu'à 255.
Règles d'équilibrage de charge	Propriété de règle qui mappe une combinaison IP et port frontaux donnée à un ensemble d'adresses IP et de combinaisons de ports back-end. Avec une définition unique d'une ressource d'équilibrage de charge, vous pouvez définir plusieurs règles d'équilibrage de charge. Chaque règle reflète une combinaison d'une adresse IP et d'un port frontaux et d'une adresse IP et d'un port back-end associés à des machines virtuelles.

Terme	Définition
Groupe de sécurité réseau (NSG)	NSG contient une liste de règles de liste de contrôle d'accès (ACL) qui autorisent ou refusent le trafic réseau à vos instances de machine virtuelle dans un réseau virtuel. Les NSG peuvent être associés à des sous-réseaux ou à des instances de machine virtuelle individuelles au sein de ce sous-réseau.
Adresse IP privée	Cette adresse est une adresse IP utilisée pour la communication au sein d'un réseau virtuel Azure et de votre réseau local lorsqu'une Gateway VPN est utilisée pour étendre votre réseau à Azure. Les adresses IP privées permettent aux ressources Azure de communiquer avec d'autres ressources. La communication dans un réseau virtuel ou un réseau local se fait via une Gateway VPN ou un circuit ExpressRoute. Cette communication ne nécessite pas d'adresse IP accessible par Internet. Dans le modèle de déploiement Azure Resource Manager, une adresse IP privée est associée aux machines virtuelles, à l'équilibreur de charge interne (ILB) et aux passerelles d'application d'Azure.
Sondes	Sondes d'intégrité utilisées pour vérifier la disponibilité des instances de machines virtuelles dans le pool d'adresses back-end.
Adresses IP publiques (PIP)	PIP est utilisé pour la communication avec Internet. Il inclut les services publics Azure associés aux machines virtuelles, à l'équilibrage de charge interne (ILB), aux passerelles VPN et aux passerelles d'application d'Azure

Terme	Définition
Région	Zone géographique qui ne dépasse pas les frontières nationales, elle contient un ou plusieurs centres de données. Les tarifs, les services régionaux et les types d'offres sont exposés au niveau régional. Une région est généralement jumelée à une autre région, qui s'étend sur une grande distance d'une paire régionale. Les paires régionales sont également utilisées comme mécanisme pour la reprise après sinistre et les scénarios de haute disponibilité. Également connu sous le nom d'emplacement.
Groupe de ressources	Un conteneur dans le Gestionnaire de ressources contient les ressources associées pour une application. Le groupe de ressources peut inclure toutes les ressources d'une application, ou uniquement les ressources qui sont groupées logiquement.
Compte de stockage	Un compte de stockage Azure vous donne accès aux services blob, file d'attente, table et fichiers Azure dans Azure Storage. Votre compte de stockage fournit l'espace de noms unique pour vos objets de données de stockage Azure.
Machine virtuelle	L'implémentation logicielle d'un ordinateur physique qui exécute un système d'exploitation. Plusieurs machines virtuelles peuvent s'exécuter simultanément sur le même matériel. Dans Azure, les machines virtuelles sont disponibles en différentes tailles.

Terme	Définition
Réseau virtuel	Un réseau virtuel Azure est une représentation de votre propre réseau dans le cloud. Il est logiquement isolé et dédié à votre abonnement dans le cloud Azure. Vous pouvez contrôler les blocs d'adresses IP, les paramètres DNS, les stratégies de sécurité et les tables de routage au sein de ce réseau.

Provisionnement des instances Citrix ADC VPX sur Google Cloud

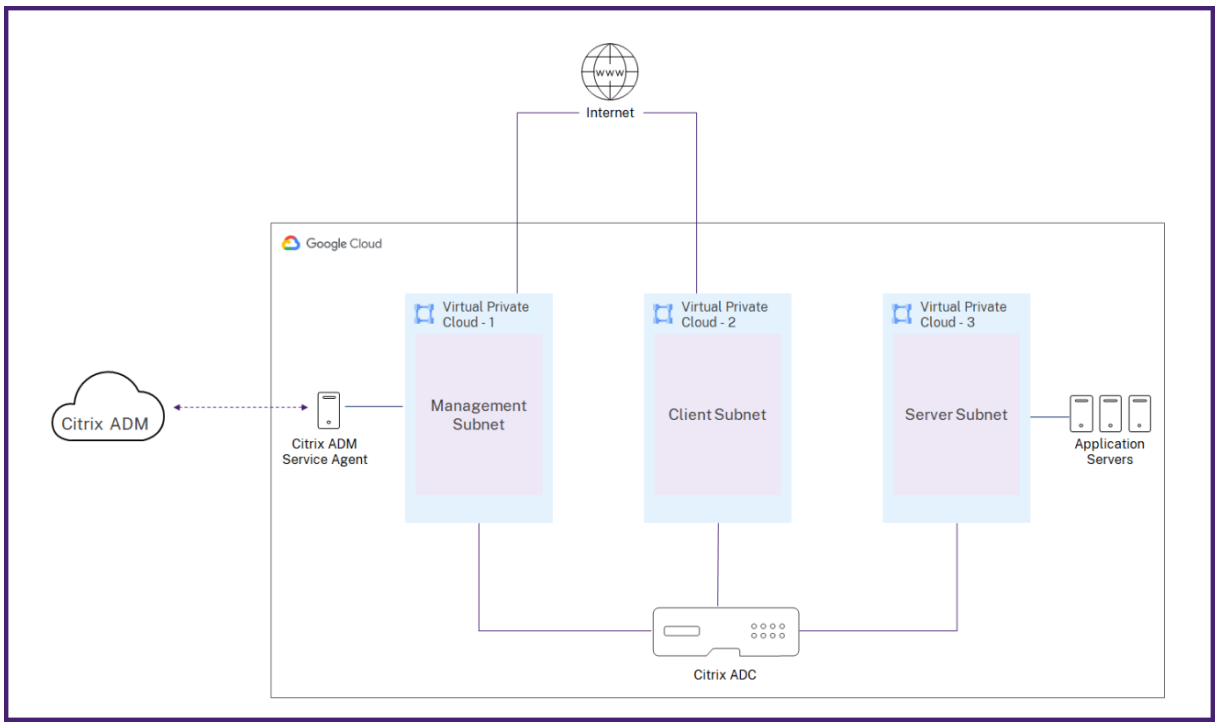
April 29, 2021

Les applications ou services hébergés sur Google Cloud nécessitent une gestion sécurisée du trafic, une optimisation efficace des ressources réseau ainsi que des avantages du cloud. Les instances Citrix ADC VPX provisionnées sur Google Cloud offrent une gestion sécurisée du trafic, une consommation optimisée des ressources et une réduction des coûts de propriété des applications Web.

Citrix ADM vous permet d'automatiser le déploiement, la configuration et la gestion des instances ADC VPX sur Google Cloud. Le provisionnement d'instances Citrix ADC VPX à l'aide d'ADM combine l'élasticité et la flexibilité du cloud avec les fonctionnalités de contrôle de Citrix ADC.

Architecture de déploiement Citrix ADM

L'image suivante fournit une vue d'ensemble de la façon dont Citrix ADM se connecte à Google Cloud pour provisionner des instances Citrix ADC VPX dans Google Cloud.



Vous avez besoin de trois réseaux Virtual Private Cloud (VPC) pour provisionner et gérer l'instance Citrix ADC VPX dans Google Cloud. Un réseau VPC contient un sous-réseau et un pare-feu. Le pare-feu a des règles qui régissent le trafic entrant et sortant vers un sous-réseau.

L'agent de service Citrix ADM vous aide à provisionner et à gérer l'instance Citrix ADC VPX.

Conditions préalables

Cette section décrit les conditions préalables que vous devez remplir dans Google Cloud et Citrix ADM avant de provisionner les instances Citrix ADC VPX.

Ce document suppose que vous possédez un compte Google Cloud. Pour plus d'informations sur la création d'un compte, reportez-vous à la section Documentation Google Cloud.

Configurer les composants Google Cloud

Avant de provisionner des instances Citrix ADC VPX dans Citrix ADM, effectuez les tâches suivantes dans Google Cloud :

1. Activer les API
2. Créer un compte de service
3. Créer un réseau VPC
4. Créer un pare-feu
5. Abonnez-vous à la licence Citrix ADC VPX dans Google Cloud

Activer les API

Citrix ADM requiert un accès programmatique pour déployer et provisionner les ressources requises dans Google Cloud. Activez donc les API suivantes sur votre projet Google Cloud :

- API Compute Engine
- API Cloud DNS

Pour plus d'informations sur l'activation des API dans Google Cloud, reportez-vous à la section Activation des API.

Créer un compte de service

Le SMA utilise un compte de service pour accéder à vos ressources Google Cloud. Pour créer un compte de service, procédez comme suit :

1. Connectez-vous à votre compte Google Cloud.
2. Accédez à **IAM & Admin > Comptes de service**.
3. Cliquez sur **+CRÉER UN COMPTE DE SERVICE**.

   Créez deux comptes de service, un compte de service est utilisé pour ADM. Et, un autre est utilisé pour les instances ADC. Procédez comme suit pour créer un compte de service.

   a) Spécifiez le nom, l'ID et la description, puis cliquez sur Créer.

   b) Attribuez les rôles prédéfinis suivants :

   - Rôles IAM requis pour le SMA

     ```
     roles/iam.serviceAccountUser
     roles/compute.instanceAdmin.v1
     roles/compute.networkAdmin
     roles/dns.admin
     <!--NeedCopy-->
     ```

   - Rôles IAM requis pour les instances ADC créées par ADM :

     ```
     roles/compute.instanceAdmin.v1
     roles/compute.networkAdmin
     <!--NeedCopy-->
     ```

   Ces rôles permettent à votre compte de service d'accéder aux ressources Google Cloud.

   c) Cliquez sur **Terminé**.

Créer un réseau VPC

Créez trois sous-réseaux dans votre réseau VPC - un pour les connexions de gestion, de client et de serveur. Sélectionnez l'option personnalisée pour créer un sous-réseau. Spécifiez une plage d'adresses pour chacun des sous-réseaux. Spécifiez la région dans laquelle vous souhaitez que le sous-réseau réside.

- **Gestion** : Un sous-réseau dans votre réseau VPC de gestion dédié à la gestion. Citrix ADC doit contacter les services Google Cloud et nécessite un accès Internet.
- **Client** : sous-réseau de votre réseau VPC client dédié au côté client. Généralement, Citrix ADC reçoit le trafic client pour l'application via un sous-réseau public à partir d'Internet.
- **Serveur** : sous-réseau où les serveurs d'applications sont provisionnés. Tous vos serveurs d'applications sont présents dans ce sous-réseau et reçoivent le trafic d'application de l'Citrix ADC via ce sous-réseau. Pour plus d'informations sur la création d'un sous-réseau dans Google Cloud, reportez-vous à la section Vue d'ensemble du réseau VPC.

Créer un pare-feu

Le pare-feu possède des règles qui contrôlent le trafic entrant et sortant dans l'instance Citrix ADC VPX. Vous pouvez ajouter autant de règles que vous voulez. Pour mettre à Autoscale des instances Citrix ADC, vous devez créer trois pare-feu :

- **Gestion** : Un pare-feu est dédié à la gestion de Citrix ADC VPX. Citrix ADC doit contacter les services Google Cloud et nécessite un accès Internet. Les règles entrantes sont autorisées sur les ports TCP et UDP suivants.
  - TCP : 80, 22, 443, 3008—3011, 4001, 27000, 7279
  - UDP : 67, 123, 161, 500, 3003, 4500, 7000

  > **Remarque**
  >
  > Assurez-vous que le pare-feu permet à l'agent Citrix ADM d'accéder au VPX.

- **Client** : Un pare-feu est dédié à la communication côté client des instances Citrix ADC VPX. Généralement, les règles entrantes sont autorisées sur les ports TCP 80, 22 et 443.
- **Serveur** : Un pare-feu est dédié à la communication côté serveur de Citrix ADC VPX. Pour plus d'informations sur la création d'un pare-feu dans Google Cloud, reportez-vous à la section Présentation des règles de pare-feu VPC.

Abonnez-vous à la licence Citrix ADC VPX dans Google Cloud

1. Connectez-vous à votre portail Google Cloud.
2. Dans **Marketplace**, recherchez Citrix ADC et sélectionnez la version du produit requise.

3. Sélectionnez l'un des types de licence suivants :
    - Licence client
    - Entreprise
    - Platine

    > **Remarque**
    >
    > Si vous sélectionnez l'option **Licence client**, le groupe Mise à l'Autoscale retirait les licences de Citrix ADM lors du provisionnement des instances Citrix ADC.

Configurer les composants Citrix ADM

Avant de provisionner des instances Citrix ADC VPX dans Citrix ADM, effectuez les tâches suivantes dans Citrix ADM :

1. Créer un site.
2. Provisionner l'agent Citrix ADM sur Google Cloud.
3. Joindre le site à un agent de service Citrix ADM.

Créer un site

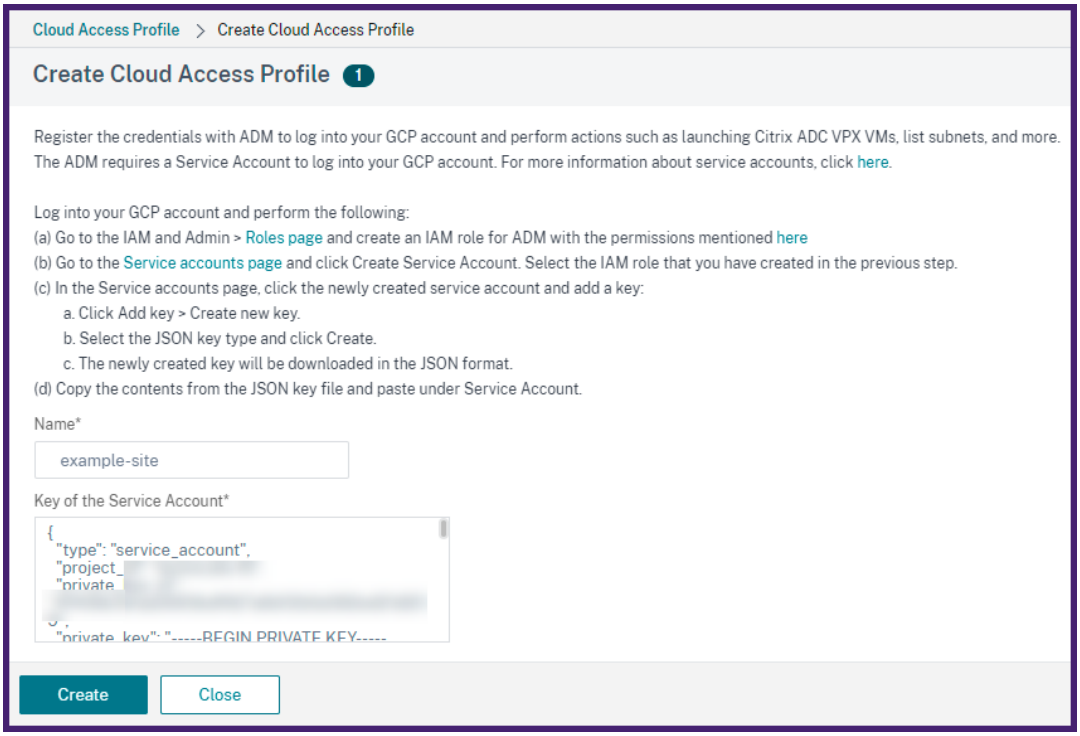
Créez un site dans Citrix ADM et ajoutez les détails VNet associés à votre Google Cloud.

1. Dans Citrix ADM, accédez à **Réseaux > Sites**.
2. Cliquez sur **Ajouter**.
3. Dans le volet **Sélectionner le Cloud**,
    a) Sélectionnez **Data Center** comme type de site.
    b) Choisissez **Google Cloud** dans la liste Type.
    c) Cochez la case **Récupérer les régions à partir de Google Cloud**.

    Cette option vous permet de récupérer les informations sur les régions existantes à partir de votre compte Google Cloud.

    d) Cliquez sur **Suivant**.
4. Dans le panneau **Choisir une région**,
    a) Dans **Profil Cloud Access**, sélectionnez le profil créé pour votre compte Google Cloud. S'il n'y a pas de profils, créez un profil.
    b) Pour créer un profil d'accès au cloud, cliquez sur **Ajouter**.
    c) Dans **Nom**, spécifiez un nom pour identifier votre compte Google Cloud dans Citrix ADM.

d) Dans **Clé du compte de service**, spécifiez le compte de service JSON créé dans Google Cloud.



e) Cliquez sur **Créer**.

Pour de plus amples informations, consultez la section Créer un compte de service.

f) Dans **Régions**, sélectionnez la région qui contient le réseau VPC contenant les instances Citrix ADC VPX que vous souhaitez gérer.

g) Spécifiez un **nom de site**.

h) Cliquez sur **Terminer**.

Provisionner l'agent Citrix ADM sur Google Cloud

L'agent de service Citrix ADM fonctionne comme intermédiaire entre Citrix ADM et les instances découvertes dans le centre de données ou sur le cloud.

1. Accédez à **Réseaux > Agents**.
2. Cliquez sur **Provisionner**.
3. Sélectionnez **Google Cloud** et cliquez sur **Suivant**.
4. Dans l'onglet **Paramètres de provisionnement**, spécifiez les éléments suivants :
   - **Nom** : spécifiez le nom de l'agent Citrix ADM.

- **Site** : sélectionnez le site que vous avez créé pour provisionner un agent et des instances VPX ADC.
- **Profil d'accès au nuage** : sélectionnez le profil d'accès au nuage dans la liste.
- **Zone** : sélectionnez les zones dans lesquelles vous souhaitez créer les groupes de mise à l'Autoscale. Selon le profil d'accès au cloud que vous avez sélectionné, les zones de ce profil sont remplies.
- **Réseau**- Sélectionnez le réseau VPC sur lequel vous souhaitez créer des groupes de mise à Autoscale.
- **Sous-réseau** : sélectionnez le sous-réseau de gestion pour provisionner un agent.
- **Tags** - Tapez la paire clé-valeur pour les balises du groupe Autoscale. Une balise est constituée d'une paire clé-valeur sensible à la casse. Ces balises vous permettent d'organiser et d'identifier facilement les groupes de mise à l'échelle automatique. Les balises sont appliquées à Google Cloud et à Citrix ADM.

5. Cliquez sur **Terminer**.

Vous pouvez également installer l'agent Citrix ADM à partir de Google Cloud Marketplace. Pour de plus amples informations, consultez la section Installation d'un agent Citrix ADM sur Google Cloud.

Joindre le site à un agent de service Citrix ADM

1. Dans Citrix ADM, accédez à **Réseaux > Agents**.
2. Sélectionnez l'agent pour lequel vous souhaitez attacher un site.
3. Cliquez sur **Joindre le site**.
4. Sélectionnez le site dans la liste que vous souhaitez joindre.
5. Cliquez sur **Enregistrer**.

Tâches de configuration

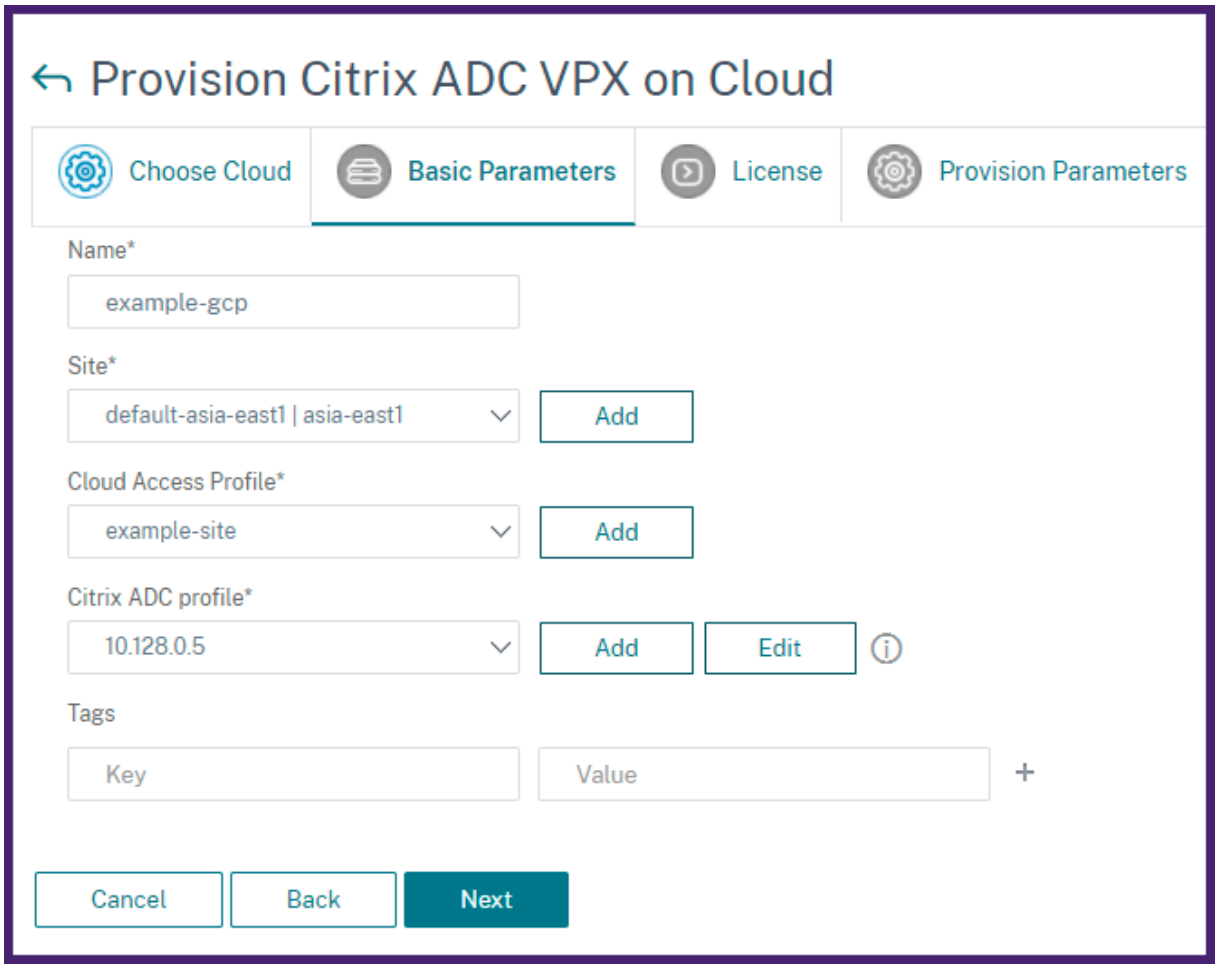
Pour provisionner une instance ADC VPX autonome sur Google Cloud, procédez comme suit :

1. Dans Citrix ADM, accédez à **Réseaux > Instances > Citrix ADC**.
2. Cliquez sur **Provisionner**.
3. Sélectionnez **Google Cloud** et cliquez sur **Suivant**. Spécifiez les paramètres requis pour provisionner une instance.
4. Spécifiez le paramètres de baselicences, et paramètres de provisionnement.

Configurer les paramètres de base

1. Dans l'onglet **Paramètres de base**, spécifiez les éléments suivants :
   - **Nom** : spécifiez le nom d'une instance ADC VPX.
   - **Site** : sélectionnez le site que vous avez créé précédemment.
   - **Agent** : sélectionnez l'agent créé pour gérer l'instance Citrix ADC VPX.
   - **Profil d'accès au cloud** - Sélectionnez le profil d'accès au cloud créé lors de la création du site.
   - **Profil Citrix ADC** - Sélectionnez le profil à fournir l'authentification.

     Citrix ADM utilise le profil de périphérique lorsqu'il doit se connecter à l'instance Citrix ADC VPX.
2. Cliquez sur **Suivant**.



Configurer les licences

Sélectionnez l'un des modes suivants pour appliquer une licence à une instance ADC :

- **Utilisation de Citrix ADM** : L'instance que vous souhaitez provisionner retirent les licences de Citrix ADM.
- **Utilisation de Google Cloud** : l'option **Allouer à partir du Cloud** utilise les licences de produit Citrix disponibles sur Google Cloud Marketplace. L'instance que vous souhaitez provisionner utilise les licences du site de vente.

  Si vous choisissez d'utiliser des licences de Google Cloud Marketplace, spécifiez le produit ou la licence dans l'onglet **Paramètres de provisionnement**.

Pour de plus amples informations, consultez la section Exigences en matière de licences.

Utiliser les licences de Citrix ADM

Pour utiliser cette option, assurez-vous que vous êtes abonné au produit Citrix ADC avec le plan logiciel **Apportez votre propre licence** dans Google Cloud. Consultez Abonnez-vous à la licence Citrix ADC VPX dans Google Cloud.

1. Dans l'onglet **Licence**, sélectionnez **Allouer à partir d'ADM**.
2. Dans **Type de licence**, sélectionnez l'une des options suivantes dans la liste :
   - **Licences de bande passante :** vous pouvez sélectionner l'une des options suivantes dans la liste **Types de licences de bande passante** :
     - **Capacité groupée :** spécifiez la capacité à allouer à une instance.

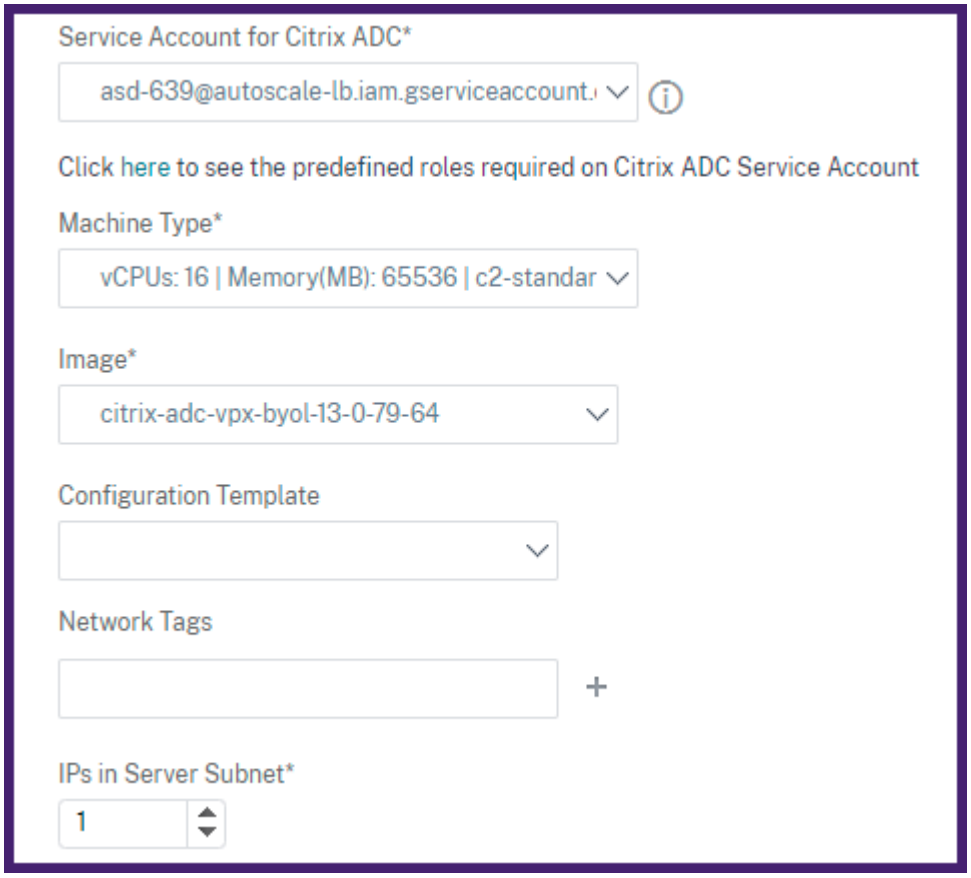
       À partir du pool commun, l'instance ADC retirait une licence d'instance et seule la bande passante est spécifiée.
     - **Licences VPX :** lorsqu'une instance Citrix ADC VPX est provisionnée, l'instance extrait la licence de Citrix ADM.
   - **Licences CPU virtuelles :** l'instance Citrix ADC VPX provisionnée retire les licences en fonction du nombre de processeurs exécutés dans l'instance.

   > **Remarque**
   >
   > Lorsque les instances provisionnées sont supprimées ou détruites, les licences appliquées retournent au pool de licences Citrix ADM. Ces licences peuvent être réutilisées pour provisionner de nouvelles instances.
3. Dans **License Edition**, sélectionnez l'édition de licence. L'ADM utilise l'édition spécifiée pour provisionner des instances.
4. Cliquez sur **Suivant**.

Configurer les paramètres de provisionnement

1. Dans l'onglet **Paramètres de provisionnement**, spécifiez les éléments suivants :

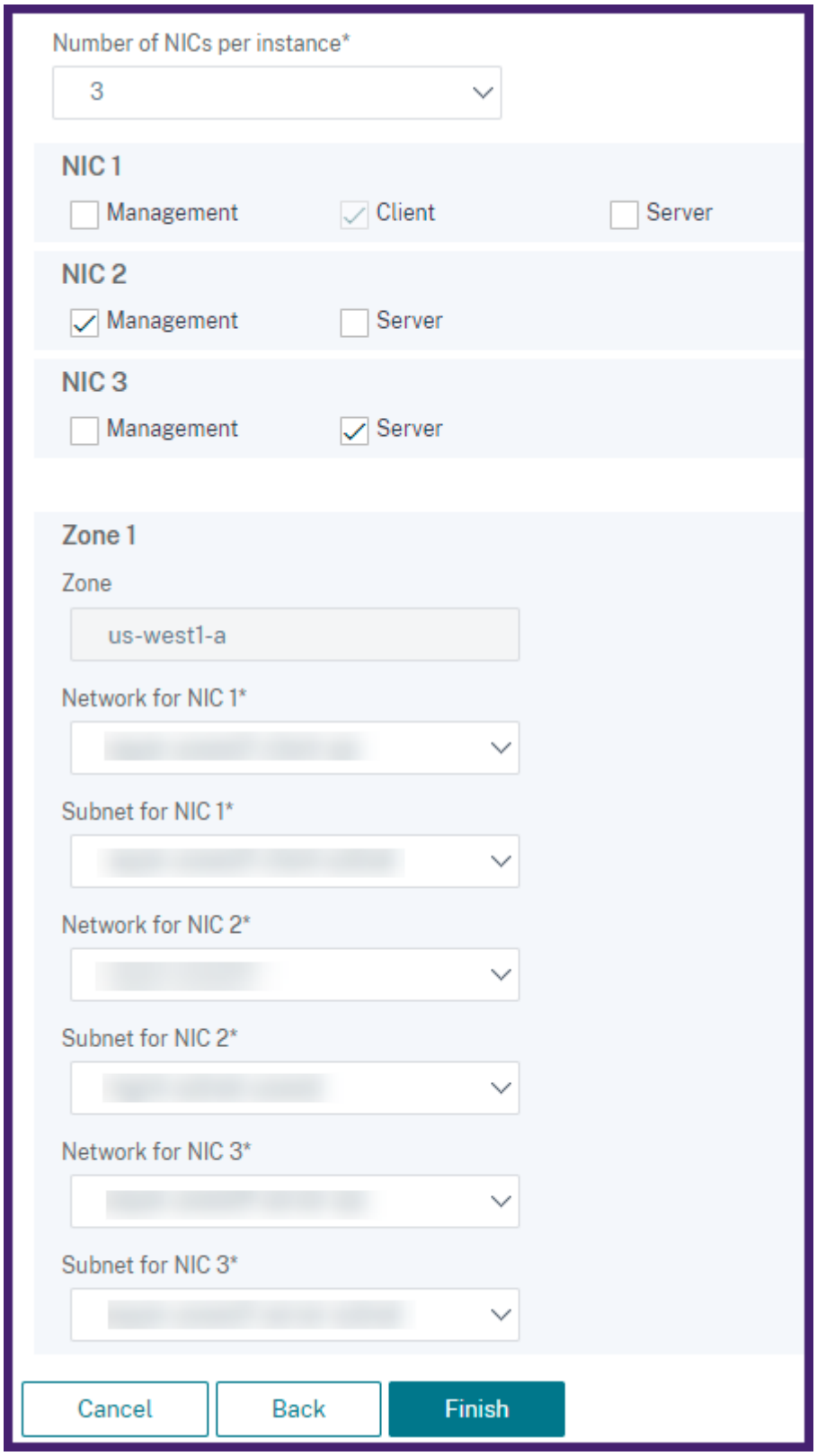
   - **Compte de service ADC** : sélectionnez le compte de service que vous avez créé dans Google Cloud. Le SMA utilise un compte de service pour accéder à vos ressources Google Cloud.
   - **Produit/License** : sélectionnez la version du produit Citrix ADC que vous souhaitez mettre en service. Pour plus d'informations, voir S'abonner à la licence Citrix ADC VPX dans Google Cloud.
   - **Types de machine** : sélectionnez le type de machine requis dans la liste.
   - **Image** : sélectionnez l'image de version Citrix ADC requise. Cliquez sur Ajouter un nouveau pour ajouter une image Citrix ADC.
   - **Modèle de configuration** : sélectionnez le modèle de configuration que vous souhaitez utiliser pour déployer sur les instances ADC.
   - **IP dans le sous-réseau serveur par instance** — Spécifiez le nombre d'adresses SNIP que chaque instance peut avoir dans le sous-réseau serveur.



   Dans cet onglet, vous pouvez également spécifier et configurer les cartes réseau requises.

Chaque carte réseau contient un pare-feu et un sous-réseau dédiés.

Pour plus d'informations, veuillez consulter Créer un réseau VPC et Créer un pare-feu.



2. Cliquez sur **Terminer**.

Afficher les instances Citrix ADC VPX provisionnées

Pour afficher dans Citrix ADM :

1. Dans Citrix ADM, accédez à **Réseaux** > **Instances** > **Citrix ADC**.
2. Sélectionnez l'onglet **Citrix ADC VPX**.

   L'instance Citrix ADC VPX provisionnée dans Google Cloud est répertoriée ici.

Pour afficher dans Google Cloud :

1. Connectez-vous à votre portail Google Cloud.
2. Accédez à l'onglet **Ressources** qui affiche l'instance Citrix ADC VPX provisionnée.

> **Remarque**
>
> Le nom de l'instance Citrix ADC VPX est identique à celui que vous avez fourni lors du provisionnement d'une instance dans Citrix ADM.

Mise à l'échelle automatique de Citrix ADC VPX dans Google Cloud à l'aide de Citrix ADM

April 29, 2021

La mise à l'échelle automatique est une méthode de cloud computing qui ajoute ou supprime automatiquement des ressources en fonction de l'utilisation réelle. La mise à l'échelle automatique est utile lorsque votre site ou votre application a besoin d'une allocation de ressources à la demande pour satisfaire le nombre fluctuant de demandes client ou de tâches de traitement.

La demande d'applications ou de services Web peut varier considérablement. Il est important de maintenir le nombre correct d'instances Citrix ADC pour les différents besoins de trafic. Vous pouvez augmenter ou diminuer les ressources réseau sur Google Cloud en fonction de la demande. Ainsi, il offre une optimisation des coûts sans compromettre les performances.
La mise à l'échelle automatique de Citrix Application Delivery Management (ADM) conserve le nombre exact d'instances Citrix ADC pour fluctuer la consommation des ressources. Citrix ADM détermine le flux de trafic en fonction de la consommation fluctuante des ressources, il décide d'évoluer ou d'évoluer dynamiquement dans les instances Citrix ADC. Ainsi, il vous offre la flexibilité nécessaire pour maintenir le nombre correct d'instances Citrix ADC.

Citrix ADM surveille l'utilisation des ressources des instances de Citrix ADC et correspond à la valeur de seuil configurée. Il déclenche l'action de mise à l'échelle si l'une des ressources configurées dépasse la valeur de seuil spécifiée.

Citrix ADM déclenche l'action de mise à l'échelle uniquement lorsque l'utilisation de toutes les ressources configurées est inférieure à la valeur de seuil normale.

> **Important**
>
> Autoscaling prend en charge toutes les fonctionnalités de Citrix ADC, à l'exception des fonctionnalités suivantes qui nécessitent une configuration ponctuée sur les nœuds de cluster :
>
> - GSLB
> - Citrix Gateway et ses fonctionnalités
> - Fonctionnalités de télécommunication
>
> Pour plus d'informations sur la configuration ponctuée, reportez-vous à la sectionConfigurations striped, striped partielles et spotted.

Avantages

Haute disponibilité des applications : La mise à l'échelle automatique garantit que votre application dispose toujours du nombre approprié d'instances Citrix ADC VPX pour gérer les demandes de trafic. Il garantit que votre application est opérationnelle tout le temps, quelles que soient les exigences en matière de trafic.

Décisions de mise à l'échelle intelligente et configuration sans contact : Autoscaling surveille en permanence votre application et ajoute ou supprime dynamiquement les instances de Citrix ADC en fonction de la demande. Les instances sont automatiquement ajoutées lorsque la demande est augmentée pendant une certaine période. Les instances sont automatiquement supprimées lorsque la demande est diminuée pendant une certaine période. L'ajout et la suppression d'instances de Citrix ADC se produisent automatiquement, ce qui en fait une configuration manuelle sans contact.

Gestion automatique du DNS : la fonctionnalité de mise à l'Autoscale Citrix ADM offre une gestion DNS automatique. Chaque fois que de nouvelles instances de Citrix ADC sont ajoutées, les noms de domaine sont mis à jour automatiquement.

Fin de connexion gracieuse : lors d'une mise à l'échelle, les instances de Citrix ADC sont supprimées de manière gracieuse, évitant ainsi la perte de connexions client.

Meilleure gestion des coûts : la mise à l'échelle automatique augmente ou diminue dynamiquement les instances de Citrix ADC selon les besoins. Cette méthode vous permet d'optimiser les coûts impliqués. Le lancement d'instances uniquement lorsqu'elles sont nécessaires et leur arrêt lorsqu'elles ne sont pas nécessaires réduit les coûts opérationnels. Ainsi, vous ne payez que pour les ressources que vous utilisez.

Observabilité : L'observabilité est essentielle pour les développeurs d'applications ou le personnel informatique pour surveiller l'état de l'application. Le tableau de bord de mise à l'Autoscale de Citrix ADM vous permet de visualiser les valeurs des paramètres de seuil, les horodatages de déclenchement de mise à l'Autoscale, les événements et les instances participant à la mise à l'échelle automatique.

Configuration requise pour le système de licences

Les instances Citrix ADC créées pour le groupe Citrix Autoscale utilisent les licences Citrix ADC Advanced ou Premium ADC. La fonctionnalité de clustering Citrix ADC est incluse dans les licences ADC Advanced ou Premium.

Vous pouvez choisir l'une des méthodes suivantes pour concéder une licence aux Citrix ADC provisionnés par Citrix ADM :

- **Utilisation des licences ADC présentes dans Citrix ADM** : configurez la capacité groupée, les licences VPX ou les licences CPU virtuelles lors de la création du groupe Mise à l'Autoscale. Ainsi, lorsqu'une nouvelle instance est provisionnée pour le groupe Mise à l'Autoscale, le type de licence déjà configuré est automatiquement appliqué à l'instance provisionnée.
  - **Capacité groupée** : alloue la bande passante à chaque instance provisionnée du groupe Mise à l'Autoscale. Assurez-vous que vous disposez de la bande passante nécessaire dans Citrix ADM pour provisionner de nouvelles instances. Pour de plus amples informations, consultez la section Configurer la capacité groupée.

    Chaque instance ADC du groupe Mise à l'Autoscale retirait une licence d'instance et la bande passante spécifiée du pool.
  - **Licences VPX** : applique les licences VPX aux instances nouvellement provisionnées. Assurez-vous que vous disposez du nombre nécessaire de licences VPX disponibles dans Citrix ADM pour provisionner de nouvelles instances.

    Lorsqu'une instance Citrix ADC VPX est provisionnée, l'instance extrait la licence du Citrix ADM. Pour plus d'informations, consultez Licences Citrix ADC VPX d'enregistrement et d'extraction.
  - Licences de processeur virtuel : applique des licences de processeur virtuel aux instances nouvellement provisionnées. Cette licence spécifie le nombre de processeurs autorisés à une instance Citrix ADC VPX. Assurez-vous que vous disposez du nombre nécessaire de processeurs virtuels dans Citrix ADM pour provisionner de nouvelles instances.

  Lorsqu'une instance Citrix ADC VPX est provisionnée, l'instance extrait la licence CPU virtuelle de Citrix ADM. Pour plus d'informations, consultez Licences Citrix ADC Virtual CPU.

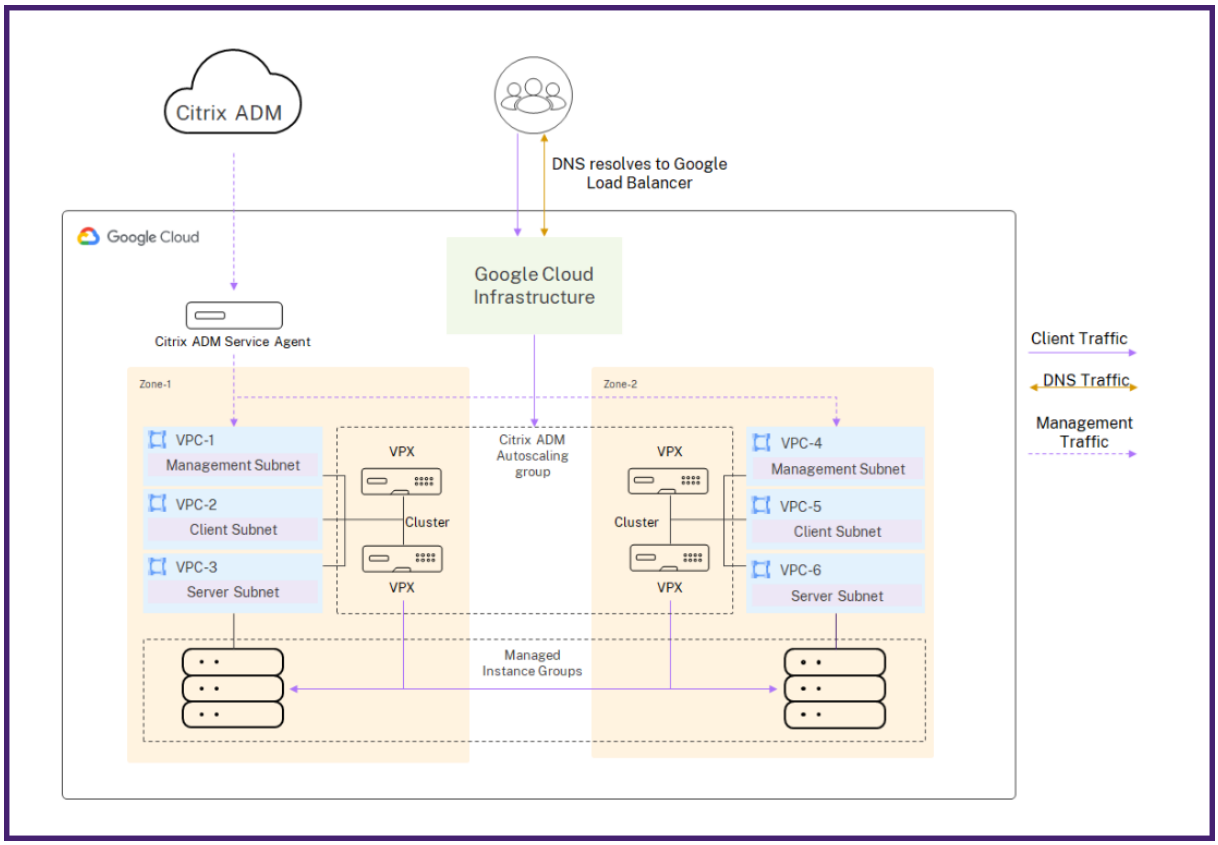
  Lorsque les instances provisionnées sont détruites ou déprovisionnées, les licences appliquées sont automatiquement renvoyées à Citrix ADM.

Pour surveiller les licences consommées, accédez à la page **Réseaux > Licences**.

- **Utilisation des licences d'abonnement Google Cloud : configurez les**licences Citrix ADC disponibles dans Google Marketplace lors de la création du groupe Mise à l'Autoscale. Ainsi, lorsqu'une nouvelle instance est provisionnée pour le groupe Autoscale, la licence est obtenue auprès de Google Marketplace.

Architecture

Citrix ADM gère la distribution du trafic client à l'aide de l'équilibrage de charge réseau Google. Le diagramme suivant illustre la manière dont la mise à l'échelle automatique se produit à l'aide de l'équilibreur de charge réseau Google en tant que distributeur de trafic :



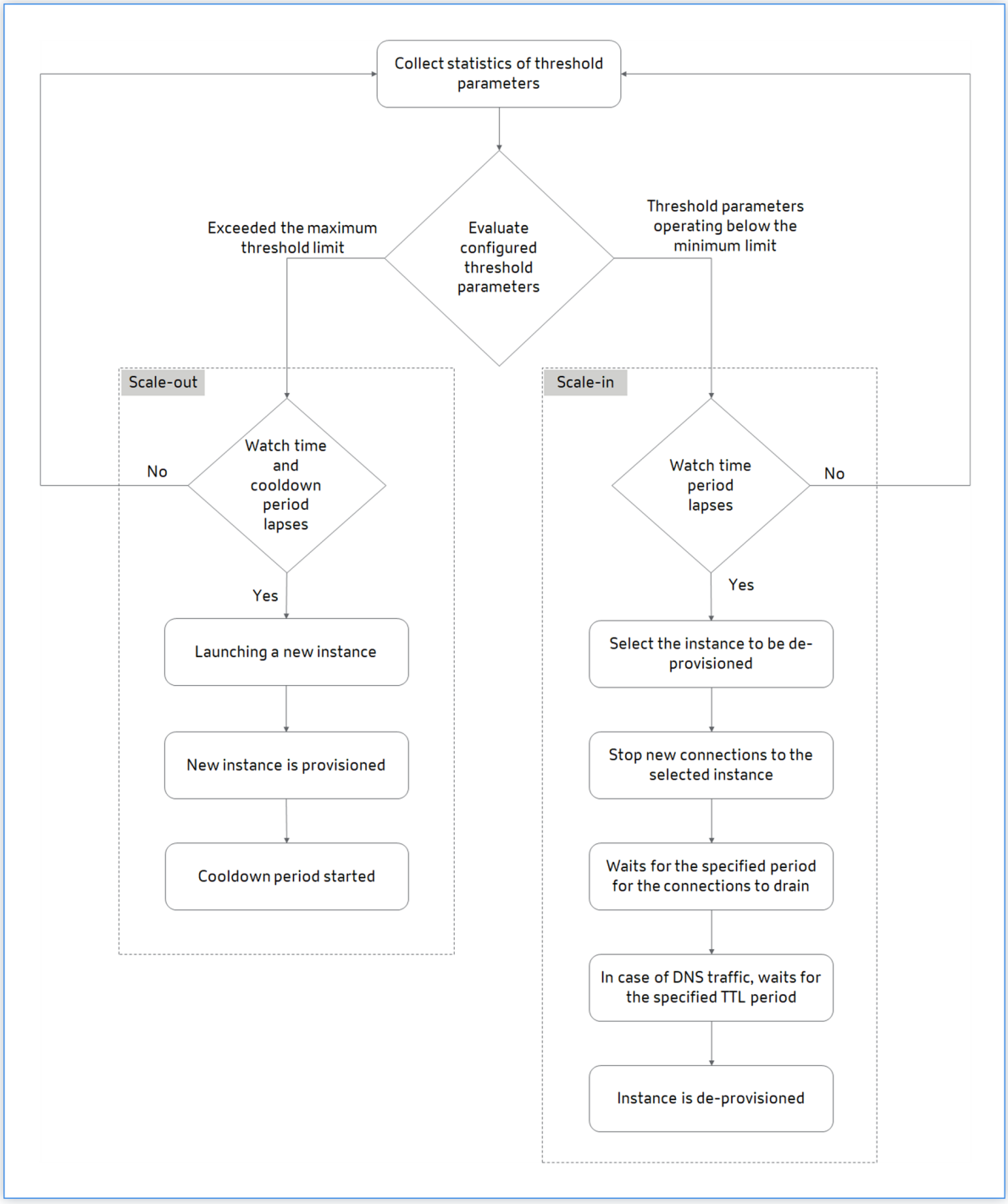
L'équilibreur de charge réseau Google est le niveau de distribution vers les nœuds du cluster. L'équilibreur de charge réseau gère le trafic client et le distribue aux clusters Citrix ADC VPX. L'équilibreur de charge réseau envoie le trafic client aux nœuds de cluster Citrix ADC VPX qui sont disponibles dans le groupe de mise à l'échelle automatique Citrix ADM sur plusieurs zones.

Citrix ADM déclenche l'action de montée en puissance parallèle ou de mise à l'échelle au niveau du cluster. Lorsqu'une mise à l'échelle est déclenchée, les machines virtuelles enregistrées sont provisionnées et ajoutées au cluster. De même, lorsqu'une mise à l'échelle est déclenchée, les nœuds sont supprimés et déprovisionnés des clusters Citrix ADC VPX.

Le groupe Citrix ADM Autoscale est un groupe d'instances Citrix ADC qui équilibrent la charge des applications en tant qu'entité unique et déclenchent la mise à l'échelle automatique en fonction des valeurs de paramètre de seuil configurées.

Fonctionnement de la mise à l'échelle automatique

L'organigramme suivant illustre le flux de travail de mise à l'échelle automatique :



Citrix ADM collecte les statistiques (CPU, mémoire et débit) à partir des clusters provisionnés à l'Autoscale pour chaque minute.

Les statistiques sont évaluées par rapport aux seuils de configuration. Selon les statistiques, la mise à l'échelle ou la mise à l'échelle est déclenchée. La mise à l'échelle est déclenchée lorsque les statistiques dépassent le seuil maximal. La mise à l'échelle est déclenchée lorsque les statistiques fonction-

nent en dessous du seuil minimum.

Si une mise à l'échelle est déclenchée :

1. Le nouveau nœud est provisionné.
2. Le nœud est attaché au cluster et la configuration est synchronisée entre le cluster et le nouveau nœud.
3. Le nœud est enregistré auprès de Citrix ADM.
4. Les nouvelles adresses IP des nœuds sont mises à jour dans l'équilibreur de charge réseau Google.

Si une mise à l'échelle est déclenchée :

1. Le nœud est identifié à supprimer.
2. Arrêtez les nouvelles connexions au nœud sélectionné.
3. Le nœud est détaché du cluster, désenregistré de Citrix ADM, puis déprovisionné de Google Cloud.

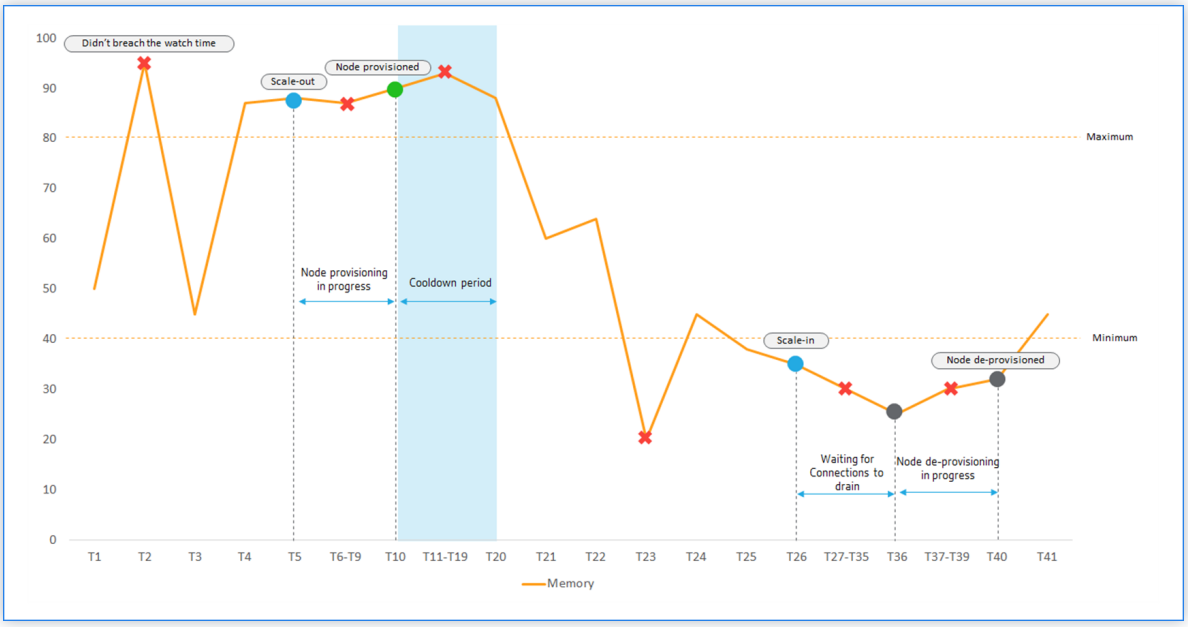
> **Remarque**
>
> Lorsque l'application est déployée, un jeu d'adresses IP est créé sur des clusters dans chaque zone de disponibilité. Ensuite, les adresses IP du domaine et de l'instance sont enregistrées auprès de l'équilibreur de charge réseau Google. Lorsque l'application est supprimée, les adresses IP du domaine et de l'instance sont désenregistrées de l'équilibreur de charge réseau Google. Ensuite, l'ensemble d'adresses IP est supprimé.

Exemple de scénario de mise à l'échelle automatique

Considérez que vous avez créé un groupe de mise à l'Autoscale nommé asg_arn dans une zone de disponibilité unique avec la configuration suivante.

- Paramètres de seuil sélectionnés : utilisation de la mémoire.
- Limite de seuil définie sur la mémoire :
  - Limite minimale : 40
  - Limite maximale : 85
- Temps de visionnage — 2 minutes.
- Période de recharge — 10 minutes.
- Temps d'attente pendant la désapprovisionnement — 10 minutes.
- Durée de vie du DNS — 10 secondes.

Une fois le groupe Autoscale créé, les statistiques sont collectées à partir du groupe Mise à Autoscale. La stratégie Autoscale évalue également si un événement de Autoscale est en cours. Si la mise à l'échelle automatique est en cours, attendez que cet événement se termine avant de collecter les statistiques.



La séquence des événements

1. L'utilisation de la mémoire dépasse la limite de seuil à **T2**. Toutefois, la mise à l'échelle n'est pas déclenchée car elle n'a pas violé la durée de la montre spécifiée.
2. La mise à l'échelle est déclenchée à **T5** après une atteinte d'un seuil maximal pendant 2 minutes (temps de surveillance) en continu.
3. Aucune action n'a été entreprise pour la violation entre **T5-T10** car le Provisioning du nœud est en cours.
4. Le nœud est provisionné à **T10** et ajouté au cluster. La période de recharge a commencé.
5. Aucune mesure n'a été prise pour la rupture entre le **T10-T20** en raison de la période de recharge. Cette période garantit la croissance organique des instances d'un groupe Autoscale. Avant de déclencher la prochaine décision de mise à l'échelle, il attend que le trafic actuel se stabilise et se stabilise sur l'ensemble d'instances en cours.
6. L'utilisation de la mémoire tombe en dessous de la limite minimale de **T23**. Toutefois, la mise à l'échelle n'est pas déclenchée parce qu'elle n'a pas violé la durée de la montre spécifiée.
7. La mise à l'échelle est déclenchée à **T26** après que le seuil minimal est dépassé pendant 2 minutes (temps de surveillance) en continu. Un nœud du cluster est identifié pour le désapprovisionnement.

8. Aucune mesure n'a été prise pour la rupture entre le **T26-T36** car Citrix ADM attend de vider les connexions existantes. Pour la mise à l'échelle automatique basée sur DNS, TTL est en vigueur.

   > **Remarque**
   >
   > Pour la mise à l'échelle automatique basée sur DNS, Citrix ADM attend la période de durée de vie (TTL) spécifiée. Ensuite, il attend que les connexions existantes s'écoulent avant de lancer le désapprovisionnement des nœuds.

9. Aucune mesure n'a été prise pour la violation entre le **T37-T39** car le désapprovisionnement du nœud est en cours.
10. Le nœud est supprimé et déprovisionné à **T40** du cluster.

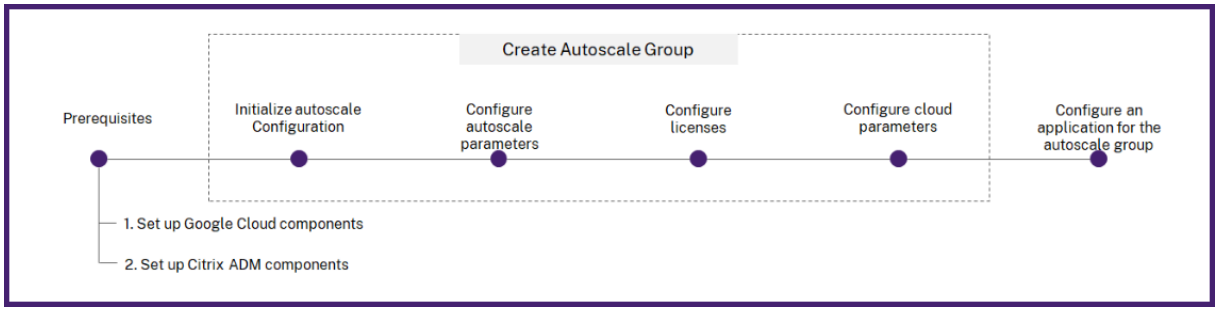
Toutes les connexions au nœud sélectionné ont été drainées avant de lancer le désapprovisionnement du nœud. Par conséquent, la période de recharge est ignorée après la suppression de la mise en service du nœud.

Configuration

April 29, 2021

Citrix ADM gère tous les clusters Citrix ADC VPX dans Google Cloud. Citrix ADM accède aux ressources Google Cloud à l'aide du profil d'accès au Cloud.

Le diagramme de flux suivant explique les étapes de création et de configuration d'un groupe de mise Autoscale :



Conditions préalables

Cette section décrit les conditions préalables que vous devez remplir dans Google Cloud et Citrix ADM avant de mettre à l'Autoscale des instances Citrix ADC VPX.

Ce document suppose que vous possédez un compte Google Cloud. Pour plus d'informations sur la création d'un compte, reportez-vous à la section Documentation Google Cloud.

Configurer les composants Google Cloud

Avant de provisionner des instances Citrix ADC VPX dans Citrix ADM, effectuez les tâches suivantes dans Google Cloud :

1. Activer les API
2. Créer un compte de service
3. Créer un réseau VPC
4. Créer un pare-feu

Activer les API

Citrix ADM requiert un accès programmatique pour déployer et provisionner les ressources requises dans Google Cloud. Activez donc les API suivantes sur votre projet Google Cloud :

- API Compute Engine
- API Cloud DNS

Pour plus d'informations sur l'activation des API dans Google Cloud, reportez-vous à la section Activation des API.

Créer un compte de service

Le SMA utilise un compte de service pour accéder à vos ressources Google Cloud. Pour créer un compte de service, procédez comme suit :

1. Connectez-vous à votre compte Google Cloud.
2. Accédez à **IAM & Admin > Comptes de service**.
3. Cliquez sur **+CRÉER UN COMPTE DE SERVICE**.

   Créez deux comptes de service, un compte de service est utilisé pour ADM. Et, un autre est utilisé pour les instances ADC. Procédez comme suit pour créer un compte de service.

   a) Spécifiez le nom, l'ID et la description, puis cliquez sur Créer.

   b) Attribuez les rôles prédéfinis suivants :

   - Rôles IAM requis pour le SMA

     ```
     roles/iam.serviceAccountUser
     roles/compute.instanceAdmin.v1
     roles/compute.networkAdmin
     roles/dns.admin
     <!--NeedCopy-->
     ```

   - Rôles IAM requis pour les instances ADC créées par ADM :


```
roles/compute.instanceAdmin.v1
roles/compute.networkAdmin
<!--NeedCopy-->
```

Ces rôles permettent à votre compte de service d'accéder aux ressources Google Cloud.

c) Cliquez sur **Terminé**.

Après avoir créé un compte de service, ajoutez-y une clé.

1. Sélectionnez le compte de service auquel vous souhaitez ajouter une clé.
2. Sélectionnez **Ajouter une clé > Créer une nouvelle clé**.
3. Sélectionnez le type de clé JSON et cliquez sur **Créer**.

Créer un réseau VPC

Créez trois sous-réseaux dans votre réseau VPC - un pour les connexions de gestion, de client et de serveur. Sélectionnez l'option personnalisée pour créer un sous-réseau. Spécifiez une plage d'adresses pour chacun des sous-réseaux. Spécifiez la région dans laquelle vous souhaitez que le sous-réseau réside.

- **Gestion** : Un sous-réseau dans votre réseau VPC de gestion dédié à la gestion. Citrix ADC doit contacter les services Google Cloud et nécessite un accès Internet.
- **Client** : sous-réseau de votre réseau VPC client dédié au côté client. Généralement, Citrix ADC reçoit le trafic client pour l'application via un sous-réseau public à partir d'Internet.
- **Serveur** : sous-réseau où les serveurs d'applications sont provisionnés. Tous vos serveurs d'applications sont présents dans ce sous-réseau et reçoivent le trafic d'application de l'Citrix ADC via ce sous-réseau. Pour plus d'informations sur la création d'un sous-réseau dans Google Cloud, reportez-vous à la section Vue d'ensemble du réseau VPC.

Créer un pare-feu

Le pare-feu possède des règles qui contrôlent le trafic entrant et sortant dans l'instance Citrix ADC VPX. Vous pouvez ajouter autant de règles que vous voulez. Pour mettre à Autoscale des instances Citrix ADC, vous devez créer trois pare-feu :

- **Gestion** : Un pare-feu est dédié à la gestion de Citrix ADC VPX. Citrix ADC doit contacter les services Google Cloud et nécessite un accès Internet. Les règles entrantes sont autorisées sur les ports TCP et UDP suivants.
  - TCP : 80, 22, 443, 3008—3011, 4001, 27000, 7279
  - UDP : 67, 123, 161, 500, 3003, 4500, 7000

Configurez Cloud NAT pour autoriser l'accès à Internet à partir de ce sous-réseau. Pour de plus amples informations, consultez la section Utilisation de Cloud NAT.

> **Remarque**
>
> Assurez-vous que le pare-feu permet à l'agent Citrix ADM d'accéder au VPX.

- **Client** : Un pare-feu est dédié à la communication côté client des instances Citrix ADC VPX. En règle générale, les règles entrantes sont autorisées sur les ports TCP 80 et 443. Et, le port 60000 est nécessaire pour surveiller l'intégrité des instances ADC.
- **Serveur** : Un pare-feu est dédié à la communication côté serveur de Citrix ADC VPX. Pour plus d'informations sur la création d'un pare-feu dans Google Cloud, reportez-vous à la section Présentation des règles de pare-feu VPC.

Configurer les composants Citrix ADM

Avant de provisionner des instances Citrix ADC VPX dans Citrix ADM, effectuez les tâches suivantes dans Citrix ADM :

1. Créer un site.
2. Provisionner l'agent Citrix ADM sur Google Cloud.
3. Joindre le site à un agent de service Citrix ADM.

Créer un site

Créez un site dans Citrix ADM et ajoutez les détails VPC client associés à votre Google Cloud.

1. Dans Citrix ADM, accédez à **Réseaux > Sites**.
2. Cliquez sur **Ajouter**.
3. Dans le volet **Sélectionner le Cloud**,
   a) Sélectionnez **Data Center** comme type de site.
   b) Choisissez **Google Cloud** dans la liste Type.
   c) Cochez la case **Récupérer les régions à partir de Google Cloud**.

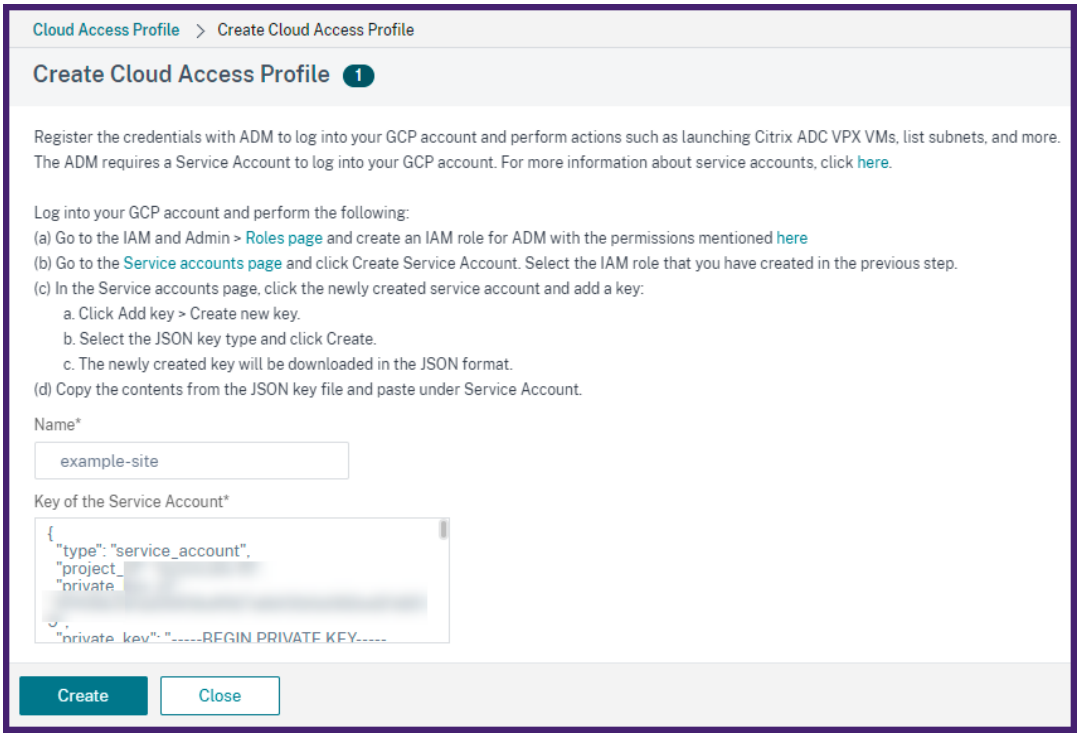
      Cette option vous permet de récupérer les informations sur les régions existantes à partir de votre compte Google Cloud.

   d) Cliquez sur **Suivant**.
4. Dans le panneau **Choisir une région**,
   a) Dans **Profil Cloud Access**, sélectionnez le profil créé pour votre compte Google Cloud. S'il n'y a pas de profils, créez un profil.

b) Pour créer un profil d'accès au cloud, cliquez sur **Ajouter**.

c) Dans **Nom**, spécifiez un nom pour identifier votre compte Google Cloud dans Citrix ADM.

d) Dans **Clé du compte de service**, spécifiez le compte de service JSON créé dans Google Cloud.



e) Cliquez sur **Créer**.

Pour de plus amples informations, consultez la section Créer un compte de service.

f) Dans **Régions**, sélectionnez la région qui contient le réseau VPC contenant les instances Citrix ADC VPX que vous souhaitez gérer.

g) Spécifiez un **nom de site**.

h) Cliquez sur **Terminer**.

Provisionner l'agent Citrix ADM sur Google Cloud

L'agent de service Citrix ADM fonctionne comme intermédiaire entre Citrix ADM et les instances découvertes dans le centre de données ou sur le cloud.

1. Accédez à **Réseaux > Agents**.
2. Cliquez sur **Provisionner**.
3. Sélectionnez **Google Cloud** et cliquez sur **Suivant**.
4. Dans l'onglet **Paramètres de provisionnement**, spécifiez les éléments suivants :

- **Nom** : spécifiez le nom de l'agent Citrix ADM.
- **Site** : sélectionnez le site que vous avez créé pour provisionner un agent et des instances VPX ADC.
- **Profil d'accès au nuage** : sélectionnez le profil d'accès au nuage dans la liste.
- **Zone** : sélectionnez les zones dans lesquelles vous souhaitez créer les groupes de mise à l'Autoscale. Selon le profil d'accès au cloud que vous avez sélectionné, les zones de ce profil sont remplies.
- **Réseau**- Sélectionnez le réseau VPC sur lequel vous souhaitez créer des groupes de mise à Autoscale.
- **Sous-réseau** : sélectionnez le sous-réseau de gestion pour provisionner un agent.
- **Labels** - Tapez la paire clé-valeur pour les étiquettes de groupe Autoscale. Une balise se compose d'une paire clé-valeur sensible à la casse. Ces étiquettes vous permettent d'organiser et d'identifier facilement les groupes de Autoscale. Les étiquettes sont appliquées à Google Cloud et à Citrix ADM.

5. Cliquez sur **Terminer**.

Vous pouvez également installer l'agent Citrix ADM à partir de Google Cloud. Pour de plus amples informations, consultez la section Installation d'un agent Citrix ADM sur Google Cloud.

Joindre le site à un agent de service Citrix ADM

1. Dans Citrix ADM, accédez à **Réseaux > Agents**.
2. Sélectionnez l'agent pour lequel vous souhaitez attacher un site.
3. Cliquez sur **Joindre le site**.
4. Sélectionnez le site dans la liste que vous souhaitez joindre.
5. Cliquez sur **Enregistrer**.

Étape 1 - Initialiser la configuration de Autoscale dans Citrix ADM

1. Dans Citrix ADM, accédez à **Réseaux > Groupes de mise à l'échelle automatique**.
2. Cliquez sur **Ajouter** pour créer des groupes de mise à l'échelle automatique.

   La page **Créer un groupe de mise à l'échelle automatique** s'affiche.
3. Sélectionnez **Google Cloud** et cliquez sur Suivant.
4. Dans **Paramètres de base**, entrez les détails suivants :
   - **Nom** : saisissez un nom pour le groupe Autoscale.

- **Site** : sélectionnez le site que vous avez créé pour mettre à l'Autoscale les instances Citrix ADC VPX sur Google Cloud. Si vous n'avez pas créé de site, cliquez sur Ajouter pour créer un site.
- **Agent** : sélectionnez l'agent Citrix ADM qui gère les instances provisionnées.
- **Profil d'accès au cloud** : sélectionnez le profil d'accès au cloud. Vous pouvez également ajouter ou modifier un profil Cloud Access.
- **Profil Citrix ADC** : sélectionnez le profil de périphérique dans la liste. Citrix ADM utilise le profil de périphérique lorsqu'il doit se connecter à l'instance Citrix ADC VPX.
- **Mode de distribution du trafic** : Google Cloud ne prend en charge qu'une seule distribution de trafic, l'équilibrage de charge à l'aide de l'équilibrage de charge réseau Google.
- **Activer le groupe de mise à l'échelle automatique** : activez ou désactivez l'état des groupes ASG. Cette option est activée par défaut. Si cette option est désactivée, la mise à l'échelle automatique n'est pas déclenchée.
- **Zone** : sélectionnez les régions dans lesquelles vous souhaitez créer les groupes de mise à l'Autoscale. Selon le profil d'accès au cloud que vous avez sélectionné, les régions apparaissent dans la liste.
- **Étiquettes** : saisissez la paire clé-valeur pour les étiquettes de groupe Autoscale. Une balise se compose d'une paire clé-valeur sensible à la casse. Ces étiquettes vous permettent d'organiser et d'identifier facilement les groupes de Autoscale. Les étiquettes sont appliquées à Google Cloud et à Citrix ADM.

5. Cliquez sur **Suivant**.

Étape 2 : Configurer les paramètres de mise à l'échelle automatique

Dans l'onglet **Paramètres de mise à l'échelle automatique**, entrez les détails suivants :

1. Sélectionnez un ou plusieurs des paramètres de seuil suivants dont les valeurs doivent être surveillées pour déclencher une scale-out ou une scale-in.
   - **Activer le seuil d'utilisation du processeur** : surveillez les mesures en fonction de l'utilisation du processeur.
   - **Activer le seuil d'utilisation de la mémoire** : surveillez les mesures en fonction de l'utilisation de la mémoire.
   - **Activer le seuil de débit** : surveillez les mesures en fonction du débit.

     > **Remarque**
     >
     > – La limite de seuil minimale par défaut est de 30 et la limite de seuil maximale est

> de 70. Toutefois, vous modifiez les limites.
>
> – La limite minimale de seuil doit être égale ou inférieure à la moitié de la limite maximale de seuil.
>
> – Vous pouvez sélectionner plusieurs paramètres de seuil pour la surveillance. La mise à l'échelle est déclenchée si au moins un des paramètres de seuil est au-dessus du seuil maximal. Toutefois, une mise à l'échelle n'est déclenchée que si tous les paramètres de seuil fonctionnent en dessous de leurs seuils normaux.

- **Instances minimales** : sélectionnez le nombre minimal d'instances qui doivent être provisionnées pour ce groupe de mise Autoscale.

  Le nombre minimal d'instances par défaut est égal au nombre de zones sélectionnées. Vous ne pouvez incrémenter les instances minimales que dans les multiples du nombre de zones spécifié.

  Par exemple, si le nombre de zones est 4, les instances minimales sont 4 par défaut. Vous pouvez augmenter les instances minimales de 8, 12, 16.

- **Maximum d'instances** : sélectionnez le nombre maximal d'instances qui doivent être provisionnées pour ce groupe de mise Autoscale.

  Le nombre maximal d'instances doit être supérieur ou égal à la valeur des instances minimales. Le nombre maximal d'instances ne peut pas dépasser le nombre de zones multiplié par 32.

  Nombre maximal d'instances = nombre de zones * 32

- **Temps de vision-minute (minutes)** : sélectionnez la durée de vision-temps. Durée pendant laquelle le seuil du paramètre d'échelle doit rester dépassé pour que la mise à l'échelle se produise. Si le seuil est dépassé sur tous les échantillons prélevés dans ce délai, une mise à l'échelle se produit.

- **Période de recharge (minutes)** : Sélectionnez la période de recharge. Pendant la mise à l'échelle, la période de recharge correspond à la période pendant laquelle l'évaluation des statistiques doit être arrêtée après une mise à l'échelle. Cette période garantit la croissance organique des instances d'un groupe Autoscale. Avant de déclencher la prochaine décision de mise à l'échelle, il attend que le trafic actuel se stabilise et se stabilise sur l'ensemble d'instances en cours.

- **Délai d'attente pendant la déprovisionnement (minutes)** : sélectionnez la période de délai d'attente de connexion de vidange. Au cours de l'action de mise à l'échelle, une instance est identifiée à désapprovisionner. Citrix ADM limite l'instance identifiée de traiter les nouvelles connexions jusqu'à ce que le délai spécifié expire avant le retrait du provisionnement. Au cours de cette période, il permet de vider les connexions existantes à cette instance avant qu'elle ne soit déprovisionnée.

2. Cliquez sur **Suivant**.

Étape 3 - Configurer les licences

Citrix ADM propose aux instances ADC la version et la licence souhaitées. Les images ADC peuvent être sous licence client (BYOL) ou sous licence de Google Cloud.

Sélectionnez l'un des modes suivants pour appliquer une licence à une instance ADC :

- **Allouer à partir de Citrix ADM** : L'instance que vous souhaitez provisionner retirera les licences de Citrix ADM.
- **Allouer à partir de Google Cloud** : l'option **Allouer à partir du Cloud** utilise les licences de produit Citrix disponibles dans Google Cloud. L'instance que vous souhaitez provisionner utilise les licences de Google Cloud.

  Si vous choisissez d'utiliser des licences de Google Cloud, spécifiez le produit ou la licence dans l'onglet **Paramètres de provisionnement**.

Pour de plus amples informations, consultez la section Exigences en matière de licence.

Allouer des licences à partir de Citrix ADM

1. Dans l'onglet **Licence**, sélectionnez **Allouer à partir d'ADM**.
2. Dans **Type de licence**, sélectionnez l'une des options suivantes dans la liste :
   - **Licences de bande passante :** vous pouvez sélectionner l'une des options suivantes dans la liste **Types de licences de bande passante** :
     - **Capacité groupée :** spécifiez la capacité à allouer à une instance.

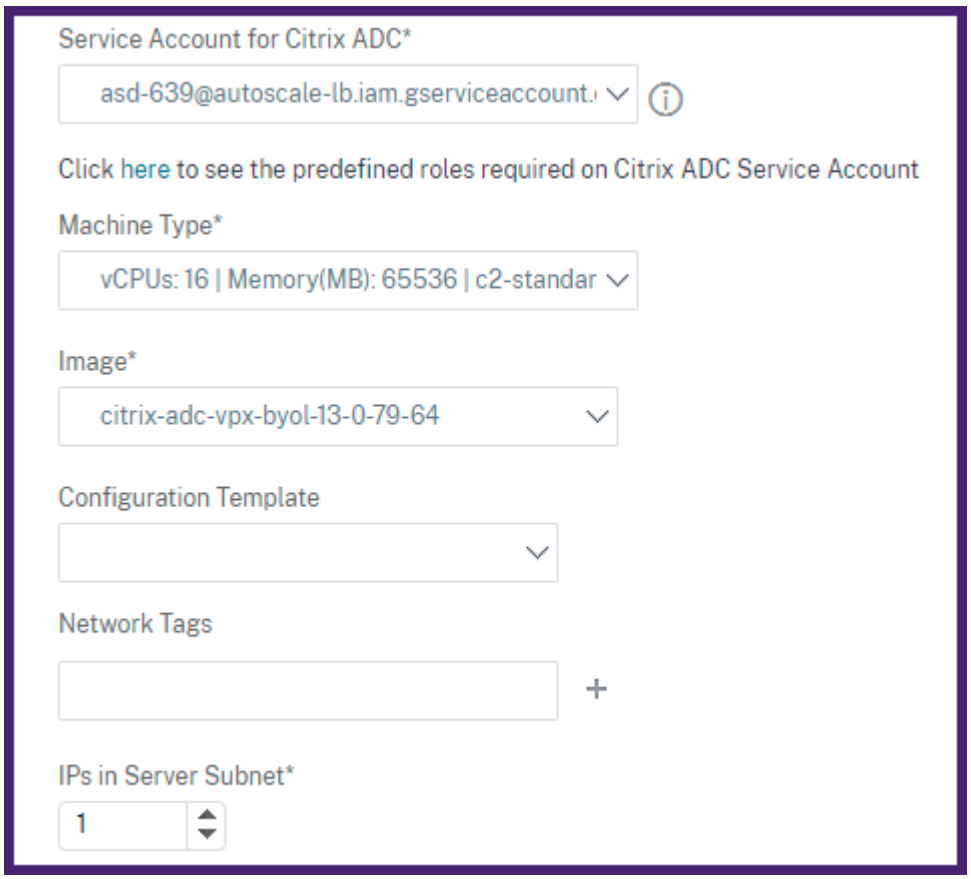
       À partir du pool commun, l'instance ADC retirait une licence d'instance et seule la bande passante est spécifiée.
     - **Licences VPX :** lorsqu'une instance Citrix ADC VPX est provisionnée, l'instance extrait la licence de Citrix ADM.
   - **Licences CPU virtuelles :** l'instance Citrix ADC VPX provisionnée retire les licences en fonction du nombre de processeurs exécutés dans l'instance.

   > **Remarque**
   >
   > Lorsque les instances provisionnées sont supprimées ou détruites, les licences appliquées retournent au pool de licences Citrix ADM. Ces licences peuvent être réutilisées pour provisionner de nouvelles instances.
3. Dans **License Edition**, sélectionnez l'édition de licence. L'ADM utilise l'édition spécifiée pour provisionner des instances.

4. Cliquez sur **Suivant**.

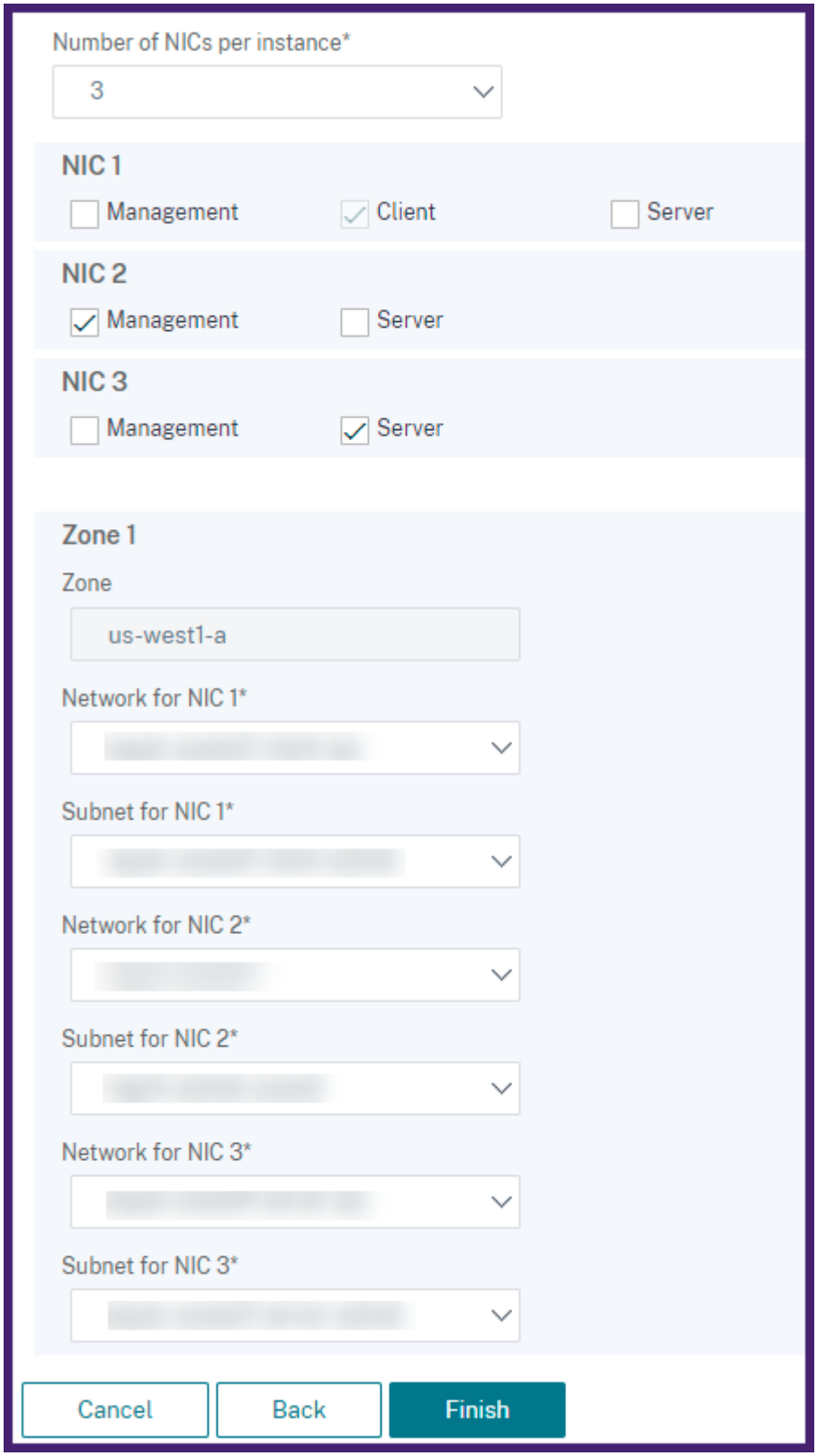
Étape 4 : Configurer les paramètres de provisionnement

1. Dans l'onglet **Paramètres de provisionnement**, spécifiez les éléments suivants :
    - **Compte de service ADC** : sélectionnez le compte de service que vous avez créé dans Google Cloud. Le SMA utilise un compte de service pour accéder à vos ressources Google Cloud.
    - **Produit/License** : sélectionnez la version du produit Citrix ADC que vous souhaitez mettre en service. Pour plus d'informations, voir S'abonner à la licence Citrix ADC VPX dans Google Cloud.
    - **Types de machine** : sélectionnez le type de machine requis dans la liste.
    - **Image** : sélectionnez l'image de version Citrix ADC requise. Cliquez sur Ajouter un nouveau pour ajouter une image Citrix ADC.
    - **Modèle de configuration** : sélectionnez le modèle de configuration que vous souhaitez utiliser pour déployer sur les instances ADC.
    - **IP dans le sous-réseau serveur par instance** — Spécifiez le nombre d'adresses SNIP que chaque instance peut avoir dans le sous-réseau serveur.



Dans cet onglet, vous pouvez également spécifier et configurer les cartes réseau requises. Chaque carte réseau contient un pare-feu et un sous-réseau dédiés.

Pour plus d'informations, veuillez consulter Créer un réseau VPC et Créer un pare-feu.



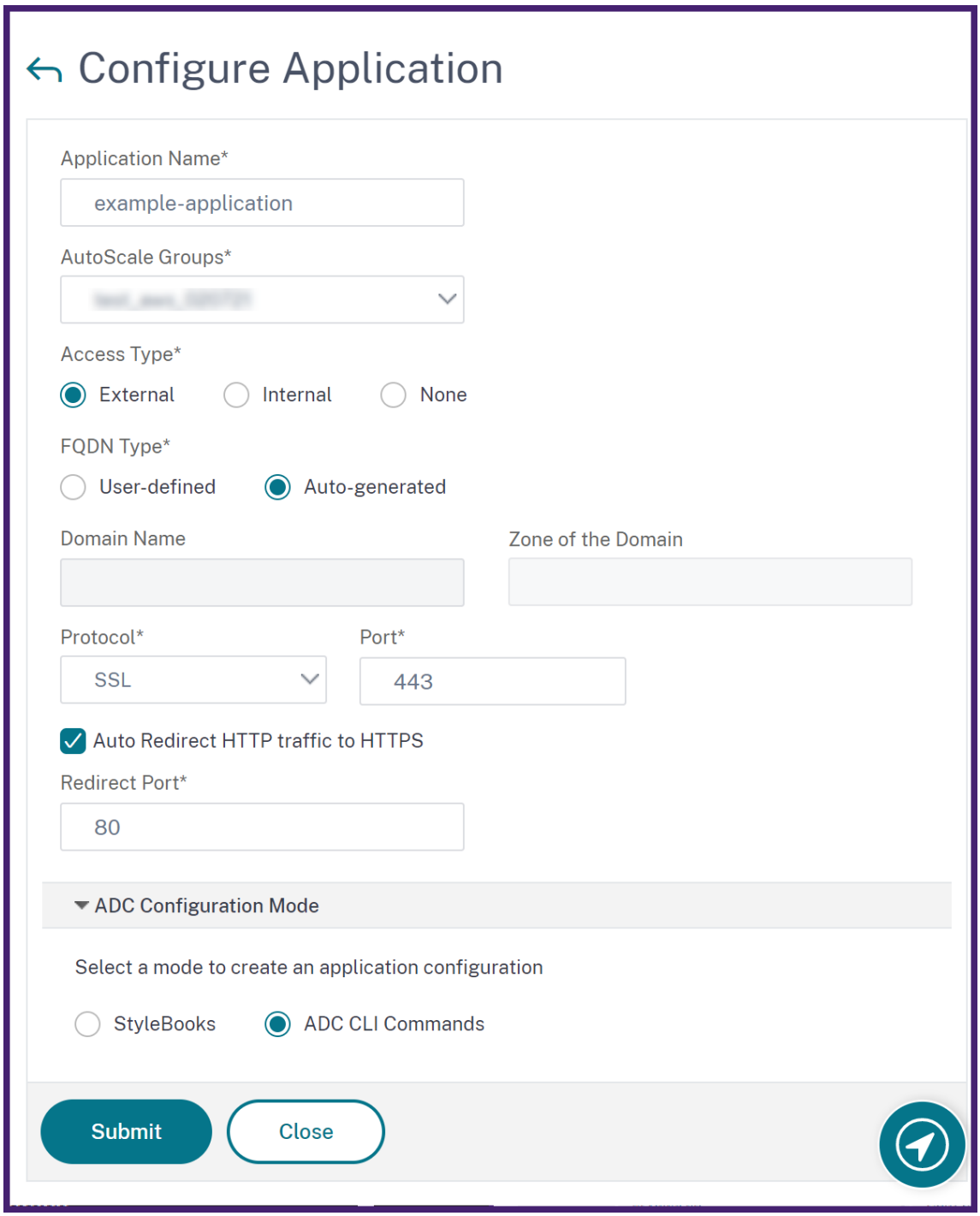
2. Cliquez sur **Terminer**.

Étape 5 : Configurer une application pour le groupe Mise à l'échelle automatique

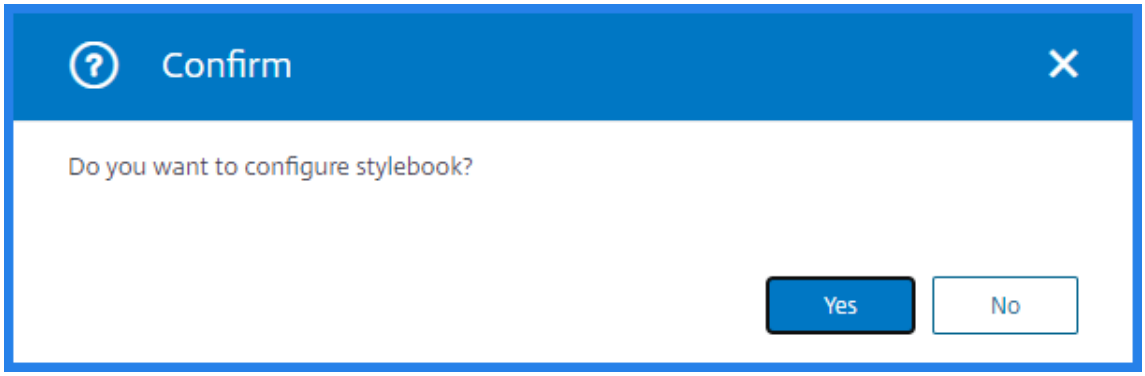
1. Dans Citrix ADM, accédez à **Réseaux** > **Groupes de mise à Autoscale**.
2. Sélectionnez le groupe de mise à l'échelle automatique que vous avez créé et cliquez sur **Configurer**.
3. Dans **Configurer l'application**, spécifiez les détails suivants :
    - **Nom de l'application** : spécifiez le nom d'une application.
    - **Type d'accès** : vous pouvez utiliser la solution de mise à l'échelle automatique ADM pour des applications externes et internes. Sélectionnez le type d'accès à l'application requis.
    - **Type de nom de domaine complet** - Sélectionnez un mode d'attribution de noms de domaine et de zone.

      Si vous souhaitez spécifier manuellement, sélectionnez Définie **par l'utilisateur**. Pour attribuer automatiquement des noms de domaine et de zone, sélectionnez **Généré automatiquement**.
    - **Nom de domaine** - Spécifiez le nom de domaine d'une application. Cette option n'est applicable que lorsque vous sélectionnez Type de nom de domaine complet défini par l'utilisateur.
    - **Zone du domaine** : sélectionnez le nom de zone d'une application dans la liste. Cette option n'est applicable que lorsque vous sélectionnez Type de nom de domaine complet défini par l'utilisateur.

      Ce nom de domaine et de zone redirige vers les serveurs virtuels dans Google Cloud. Par exemple, si vous hébergez une application dans `app.example.com`, le `app` est le nom de domaine et `example.com` le nom de la zone.
    - **Protocole** : sélectionnez le type de protocole dans la liste. L'application configurée reçoit le trafic en fonction du type de protocole sélectionné.
    - **Port** : spécifiez la valeur du port. Le port spécifié est utilisé pour établir une communication entre l'application et le groupe Mise à l'Autoscale.

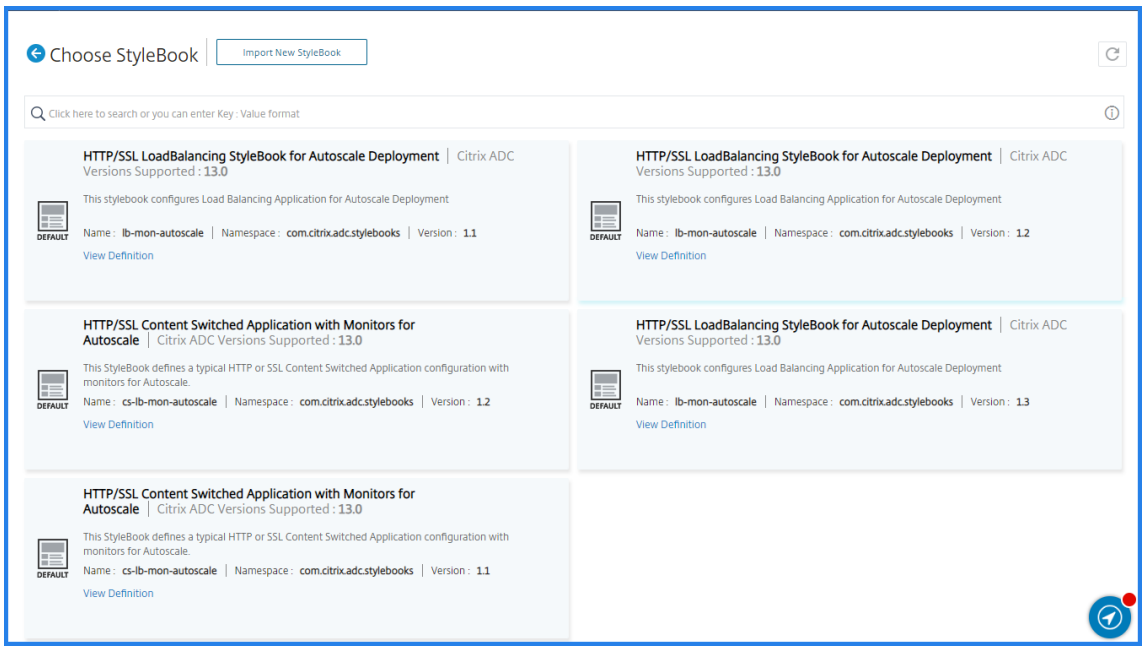


Si vous souhaitez configurer une application à l'aide de StyleBooks, sélectionnez **Oui** dans la fenêtre de confirmation.



> **Remarque**
>
> Modifiez le type d'accès d'une application si vous souhaitez modifier les détails suivants à l'avenir :
>
> - Type de nom de domaine complet
> - Nom de domaine
> - Zone du domaine

4. Choisissez le StyleBook requis que vous souhaitez déployer des configurations pour le groupe de mise à l'échelle automatique sélectionné.



Si vous souhaitez importer des StyleBooks, cliquez sur **Importer un nouveau StyleBook**.

5. Spécifiez les valeurs de tous les paramètres.

   Les paramètres de configuration sont prédéfinis dans le StyleBook sélectionné.

6. Cochez la case **Type de groupe de serveurs d'applications CLOUD** pour spécifier les serveurs d'applications disponibles dans le jeu d'échelle de machine virtuelle.

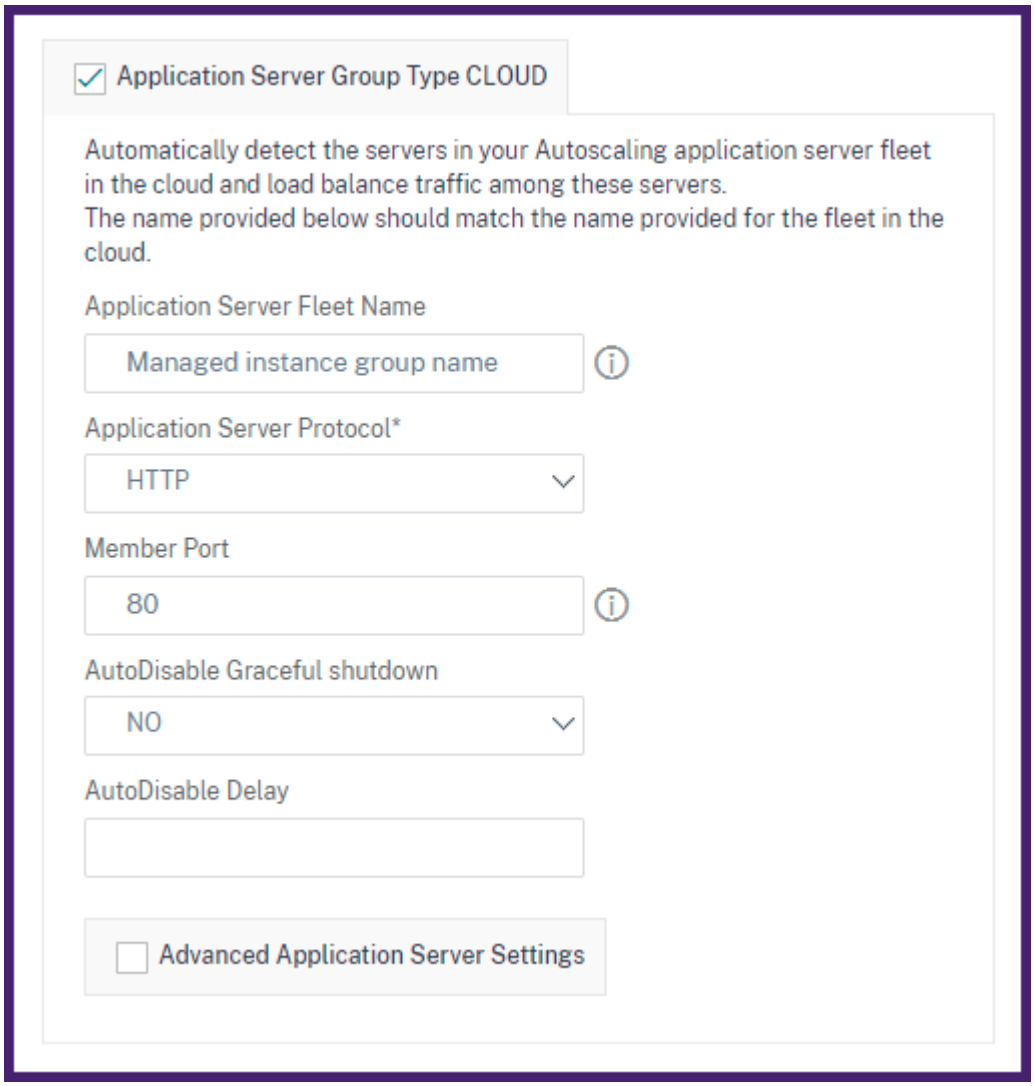
a) Dans **Application Server Fleet Name**, spécifiez le **nom du paramètre Mise Autoscale** de votre jeu d'échelle de machine virtuelle.

b) Sélectionnez **Application Server Protocol** dans la liste.

c) Dans **Port membre**, spécifiez la valeur de port du serveur d'applications.

> **Remarque**
>
> Assurez-vous que la **désactivation automatique Graceful Shutdown** est définie sur **Non** et le champ **Retard de désactivation automatique** est vide.

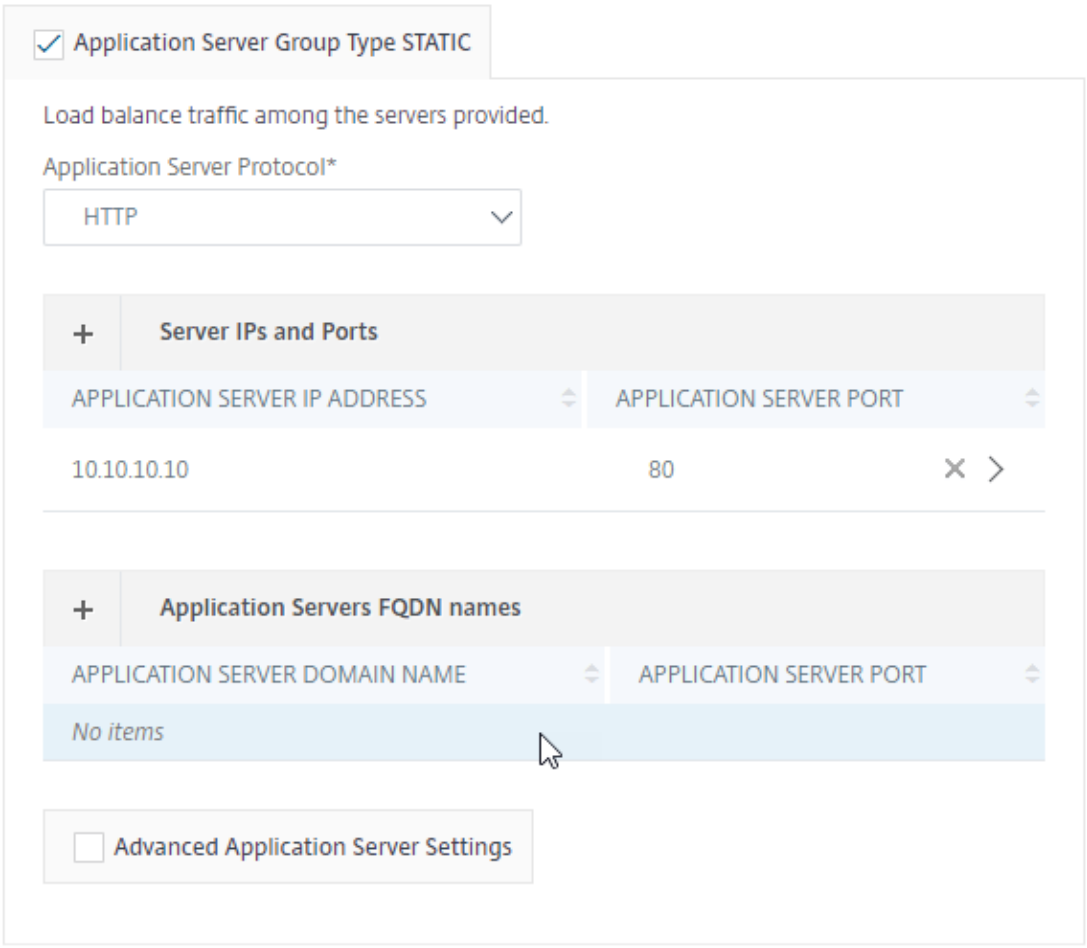
d) Si vous souhaitez spécifier les paramètres avancés de vos serveurs d'applications, cochez la case **Paramètres avancés du serveur d'applications**. Ensuite, spécifiez les valeurs requises répertoriées sous **Paramètres avancés du serveur d'applications**.



7. Si vous avez des serveurs d'applications autonomes dans le réseau virtuel, cochez la case **Type de groupe de serveurs d'applications STATIC** :

a) Sélectionnez **Application Server Protocol** dans la liste.

b) Dans les **adresses IP et ports du serveur**, cliquez sur **+**pour ajouter une adresse IP du serveur d'applications, un port et un poids, puis cliquez sur **Créer**.



8. Cliquez sur **Créer**.

Modifier la configuration des groupes de mise à l'échelle automatique

Vous pouvez modifier une configuration de groupe de mise à l'échelle automatique ou supprimer un groupe de mise à l'échelle automatique. Vous ne pouvez modifier que les paramètres de groupe d'échelle automatique suivants :

- Limites maximales et minimales des paramètres de seuil
- Valeurs d'instance minimales et maximales
- Valeur de la période de drainage des connexions
- Valeur de la période de recharge

- Valeur de durée de la surveillance

Vous pouvez également supprimer les groupes de mise à l'échelle automatique après leur création.

Lorsqu'un groupe de mise à l'échelle automatique est supprimé, tous les domaines et adresses IP sont désenregistrés du DNS et les nœuds de cluster sont déprovisionnés.

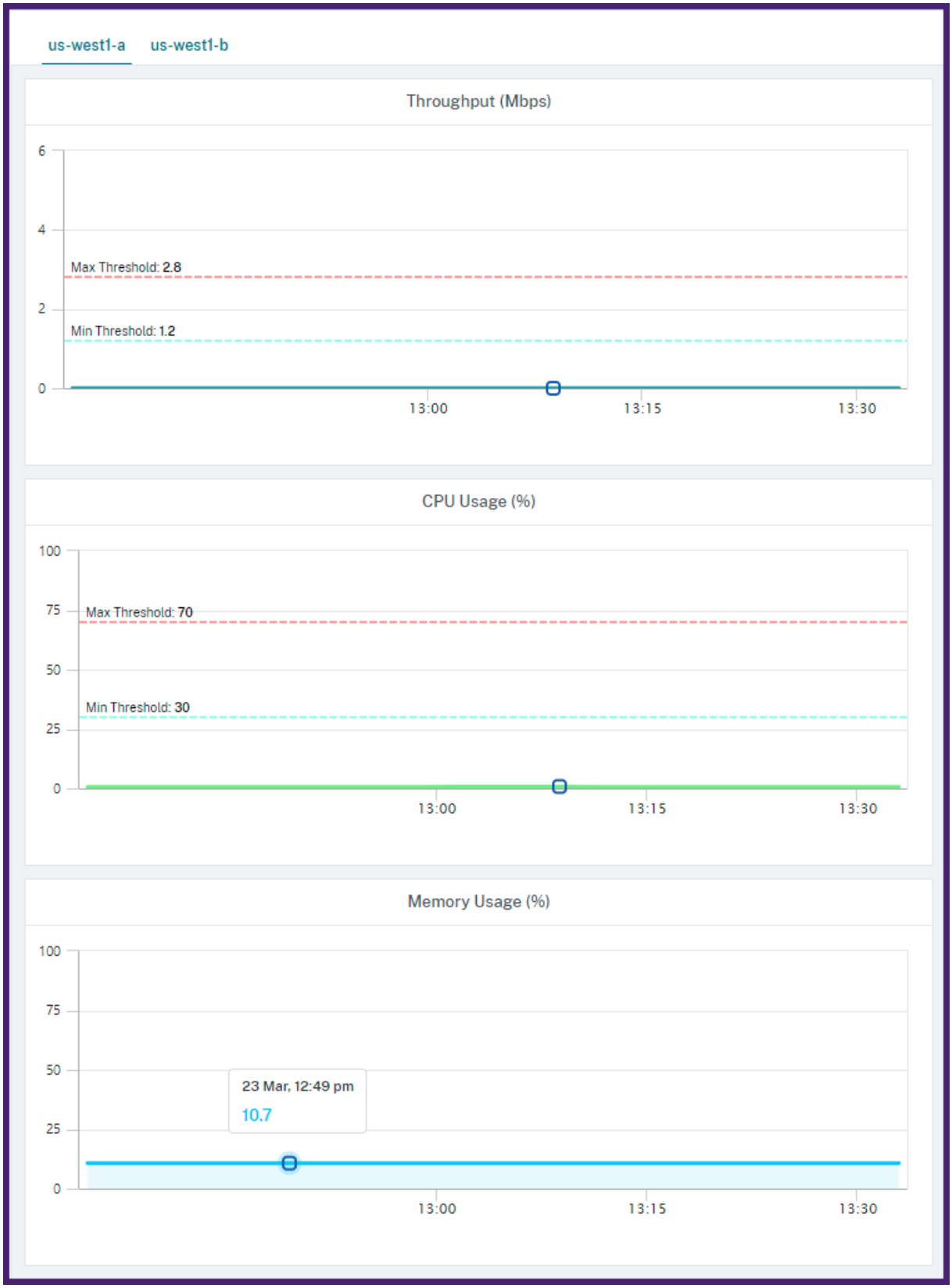
Tableau de bord

April 29, 2021

Vous pouvez afficher le graphique des paramètres de surveillance sélectionnés. Le panneau de droite affiche les événements qui déclenchent la mise à l'échelle automatique. Le panneau de gauche affiche les nœuds actifs dans le cluster par zone, le graphique des nœuds actifs et les événements.

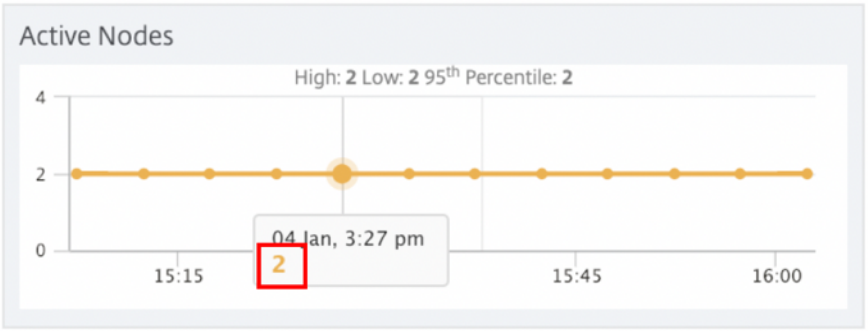
1. Dans Citrix ADM, accédez à **Réseaux > Groupes de mise à l'échelle automatique**.
2. Sélectionnez le groupe Autoscale et cliquez sur **Tableau de bord**.

La figure suivante présente un exemple de tableau de bord :



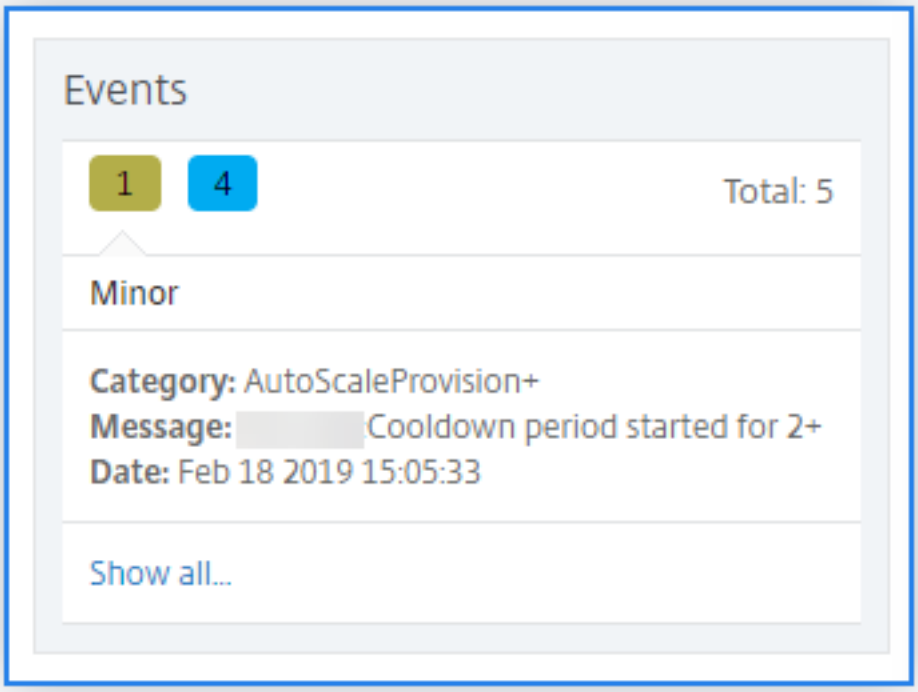
La figure suivante affiche le graphique des nœuds actifs. Le nombre en dessous de l'horodatage in-

dique le nombre de nœuds actifs. Vous pouvez afficher le nombre de nœuds actifs faisant partie de la zone à tout moment.

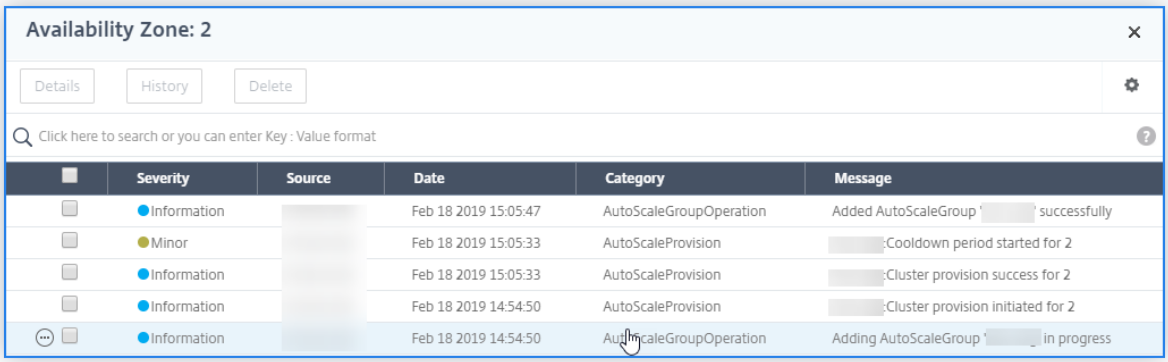


Événements

Dans **Tableau de bord**, l'onglet **Événements** affiche le nombre total d'événements pour le groupe de mise à l'Autoscale sélectionné. Il affiche également un bref message du dernier événement.



Pour afficher les détails des événements, cliquez sur **Afficher tout**.



Équilibrage global de charge Citrix ADC pour les déploiements hybrides et multi-cloud

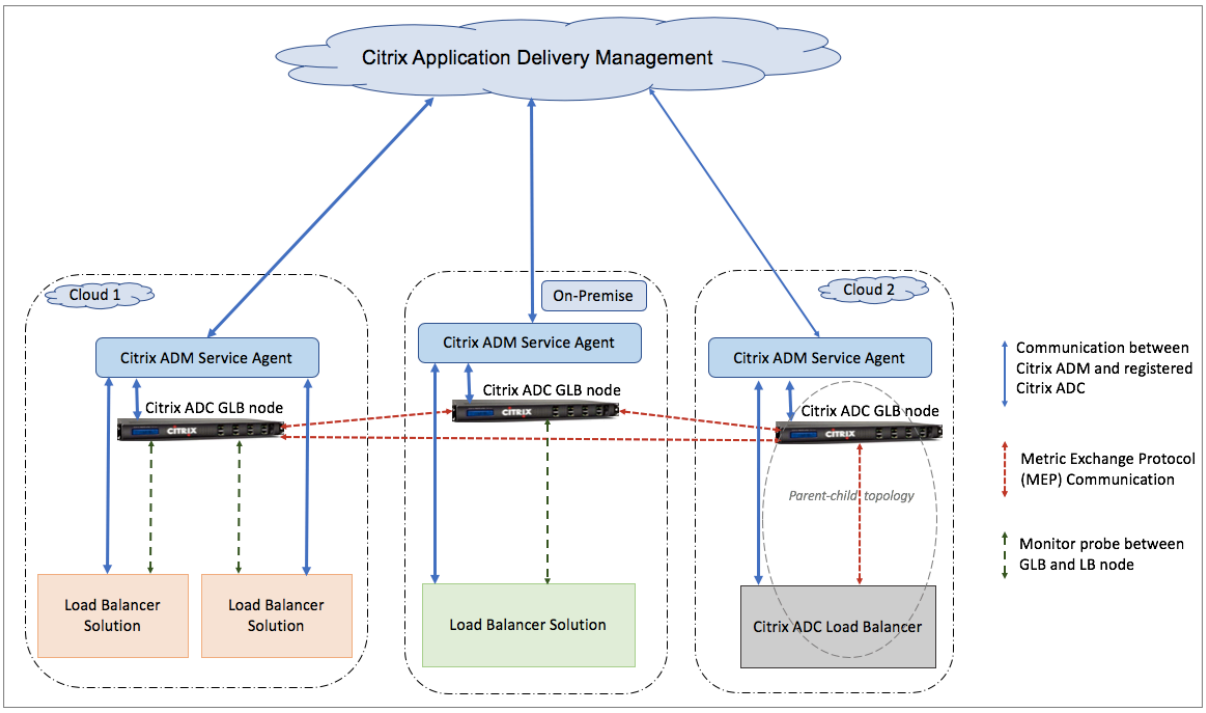
April 29, 2021

La solution d'équilibrage de charge globale (GLB) multi-cloud et hybride de Citrix ADC vous permet de distribuer le trafic d'applications entre plusieurs centres de données dans des clouds hybrides, plusieurs clouds et des déploiements locaux. La solution GLB hybride et multi-cloud de Citrix ADC vous aide à gérer votre configuration d'équilibrage de charge dans un cloud hybride ou multi-cloud sans modifier la configuration existante. En outre, si vous disposez d'une configuration locale, vous pouvez tester certains de vos services dans le cloud à l'aide de la solution GLB hybride et multi-cloud Citrix ADC avant de migrer complètement vers le cloud. Par exemple, vous ne pouvez acheminer qu'un petit pourcentage de votre trafic vers le cloud et gérer la majeure partie du trafic sur site. La solution GLB hybride et multi-cloud Citrix ADC vous permet également de gérer et de surveiller les instances Citrix ADC à travers des emplacements géographiques à partir d'une console unifiée unique.

Une architecture hybride et multi-cloud peut également améliorer les performances globales de l'entreprise en évitant le « verrouillage du fournisseur » et en utilisant différentes infrastructures pour répondre aux besoins de vos partenaires et clients. Grâce à plusieurs architectures cloud, vous pouvez mieux gérer vos coûts d'infrastructure, car vous ne devez désormais payer que pour ce que vous utilisez. Également adapter vos applications à mesure que vous utilisez désormais l'infrastructure à la demande. Il permet également de passer rapidement d'un cloud à un autre pour profiter des meilleures offres de chaque fournisseur.

Architecture de la solution GLB hybride et multi-cloud Citrix ADC

Le diagramme suivant illustre l'architecture de la fonctionnalité GLB hybride et multi-cloud Citrix ADC.



Les nœuds GLB d'Citrix ADC gèrent la résolution de noms DNS. N'importe lequel de ces nœuds GLB peut recevoir des demandes DNS à partir de n'importe quel emplacement client. Le nœud GLB qui reçoit la demande DNS renvoie l'adresse IP du serveur virtuel d'équilibrage de charge sélectionnée par la méthode d'équilibrage de charge configurée. Les mesures (mesures de site, de réseau et de persistance) sont échangées entre les nœuds GLB à l'aide du protocole d'échange de mesures (MEP), qui est un protocole Citrix propriétaire. Pour plus d'informations sur le protocole MEP, reportez-vous à la section Configuration du protocole Metrics Exchange Protocol.

Le moniteur configuré dans le nœud GLB surveille l'état d'intégrité du serveur virtuel d'équilibrage de charge dans le même centre de données. Dans une topologie parent-enfant, les mesures entre les nœuds GLB et Citrix ADC sont échangées à l'aide de MEP. Toutefois, la configuration des sondes de moniteur entre un nœud GLB et Citrix ADC LB est facultative dans une topologie parent-enfant.

L'agent de service Citrix Application Delivery Management (ADM) active la communication entre Citrix ADM et les instances gérées dans votre datacenter. Pour plus d'informations sur les agents de service Citrix ADM et sur leur installation, reportez-vous à la sectionMise en route.

> **Remarque**
>
> Le présent document formule les hypothèses suivantes :

- Si vous disposez d'une configuration d'équilibrage de charge existante, elle est en cours d'exécution.
- Une adresse SNIP ou une adresse IP de site GLB est configurée sur chacun des nœuds GLB Citrix ADC. Cette adresse IP est utilisée comme adresse IP source du centre de données lors de l'échange de mesures avec d'autres centres de données.

- Un service ADNS ou ADNS-TCP est configuré sur chacune des instances GLB d'Citrix ADC pour recevoir le trafic DNS.
- Les groupes de pare-feu et de sécurité requis sont configurés dans les fournisseurs de services cloud.

> **Configuration des groupes de sécurité**
>
> Vous devez configurer la configuration de pare-feu/groupes de sécurité requise dans les fournisseurs de services cloud. Pour plus d'informations sur les fonctionnalités de sécurité AWS, consultez la Documentation AWS. Pour plus d'informations sur les groupes de sécurité réseau Microsoft Azure, consultez la Documentation Microsoft Azure.
>
> En outre, sur le nœud GLB, vous devez ouvrir le port 53 pour l'adresse IP du serveur ADNS Service/DNS et le port 3009 pour l'adresse IP du site GSLB pour l'échange de trafic MEP. Sur le nœud d'équilibrage de charge, vous devez ouvrir les ports appropriés pour recevoir le trafic de l'application. Par exemple, vous devez ouvrir le port 80 pour recevoir du trafic HTTP et le port 443 pour recevoir du trafic HTTPS. Ouvrez le port 443 pour la communication NITRO entre l'agent de service Citrix ADM et Citrix ADM.
>
> Pour la méthode GLB de temps aller-retour dynamique, vous devez ouvrir le port 53 pour autoriser les sondes UDP et TCP en fonction du type de sonde LDNS configuré. Les sondes UDP ou TCP sont lancées à l'aide de l'un des SNIP et ce paramètre doit donc être fait pour les groupes de sécurité liés au sous-réseau côté serveur.

Fonctionnalités de la solution GLB hybride et multi-cloud Citrix ADC

Certaines des fonctionnalités de la solution GLB hybride et multi-cloud Citrix ADC sont décrites dans cette section :

Compatibilité avec d'autres solutions d'équilibrage de charge

La solution GLB hybride et multi-cloud de Citrix ADC prend en charge diverses solutions d'équilibrage de charge, telles que l'équilibreur de charge Citrix ADC, Nginx, HAProxy et d'autres équilibreurs de charge tiers.

> **Remarque**Les solutions d'équilibrage de
>
> charge autres que Citrix ADC ne sont prises en charge que si des méthodes GLB basées sur la proximité et non métrique sont utilisées et si la topologie parent-enfant n'est pas configurée.

Méthodes GLB

La solution GLB hybride et multi-cloud Citrix ADC prend en charge les méthodes GLB suivantes.

- Méthodes GLB basées sur des métriques. Les méthodes GLB basées sur les mesures collectent les mesures à partir des autres nœuds Citrix ADC via le protocole d'échange de mesures.
  - Connexion minimale : la demande du client est acheminée vers l'équilibreur de charge qui a le moins de connexions actives.
  - Bande passante minimale : la demande du client est acheminée vers l'équilibreur de charge qui dessert actuellement le moins de trafic.
  - Moins de paquets : la demande du client est acheminée vers l'équilibreur de charge qui a reçu le moins de paquets au cours des 14 dernières secondes.
- Méthodes GLB non métriques
  - Round Robin : La demande du client est acheminée vers l'adresse IP de l'équilibreur de charge qui se trouve en haut de la liste des équilibreurs de charge. Cet équilibreur de charge se déplace ensuite au bas de la liste.
  - Hash IP source : Cette méthode utilise la valeur hachée de l'adresse IP du client pour sélectionner un équilibreur de charge.
- Méthodes GLB basées sur la proximité
  - Proximité statique : La demande du client est acheminée vers l'équilibreur de charge le plus proche de l'adresse IP du client.
  - Temps aller-retour (RTT) : Cette méthode utilise la valeur RTT (le délai dans la connexion entre le serveur DNS local du client et le centre de données) pour sélectionner l'adresse IP de l'équilibreur de charge le plus performant.

Pour plus d'informations sur les méthodes d'équilibrage de charge, reportez-vous à la section Algorithmes d'équilibrage de charge.

Topologies GLB

La solution GLB hybride et multi-cloud Citrix ADC prend en charge la topologie actif-passif et la topologie parent-enfant.

- Topologie active-passive : assure la reprise après sinistre et assure la disponibilité continue des applications en protégeant contre les points de défaillance. Si le centre de données principal tombe en panne, le centre de données passif devient opérationnel. Pour plus d'informations sur la topologie active-passive GSLB, reportez-vous à la section Configuration de GSLB pour la reprise après sinistre.
- Topologie parent-enfant : peut être utilisée si vous utilisez les méthodes GLB basées sur des mesures pour configurer les nœuds GLB et LB et si les nœuds LB sont déployés sur une autre instance Citrix ADC. Dans une topologie parent-enfant, le nœud LB (site enfant) doit être une appliance Citrix ADC car l'échange de mesures entre le site parent et le site enfant se fait via le protocole MEP (Metrics Exchange Protocol).

Pour plus d'informations sur la topologie parent-enfant, reportez-vous à la section Déploiement de topologie parent-enfant à l'aide du protocole MEP.

Prise en charge de IPv6

La solution GLB hybride et multi-cloud Citrix ADC prend également en charge IPv6.

Surveillance

La solution GLB hybride et multi-cloud de Citrix ADC prend en charge les moniteurs intégrés avec une option permettant d'activer la connexion sécurisée. Toutefois, si les configurations LB et GLB sont sur la même instance d'Citrix ADC ou si la topologie parent-enfant est utilisée, la configuration des moniteurs est facultative.

Persistance

La solution GLB hybride et multi-cloud Citrix ADC prend en charge les éléments suivants :

- Sessions de persistance basées sur IP source, de sorte que plusieurs demandes provenant du même client sont dirigées vers le même service si elles arrivent dans la fenêtre de délai d'expiration configurée. Si la valeur du délai d'expiration expire avant que le client envoie une autre demande, la session est ignorée et l'algorithme d'équilibrage de charge configuré est utilisé pour sélectionner un nouveau serveur pour la prochaine demande du client.
- Persistance de débordement afin que le serveur virtuel de sauvegarde continue à traiter les demandes qu'il reçoit, même après que la charge sur le principal tombe en dessous du seuil. Pour de plus amples informations, consultez la section Configuration du débordement.
- Persistance du site afin que le nœud GLB sélectionne un centre de données pour traiter une demande client et transfère l'adresse IP du centre de données sélectionné pour toutes les demandes DNS suivantes. Si la persistance configurée s'applique à un site qui est DOWN, le nœud GLB utilise une méthode GLB pour sélectionner un nouveau site et le nouveau site devient permanent pour les demandes ultérieures du client.

Configuration à l'aide de Citrix ADM StyleBooks

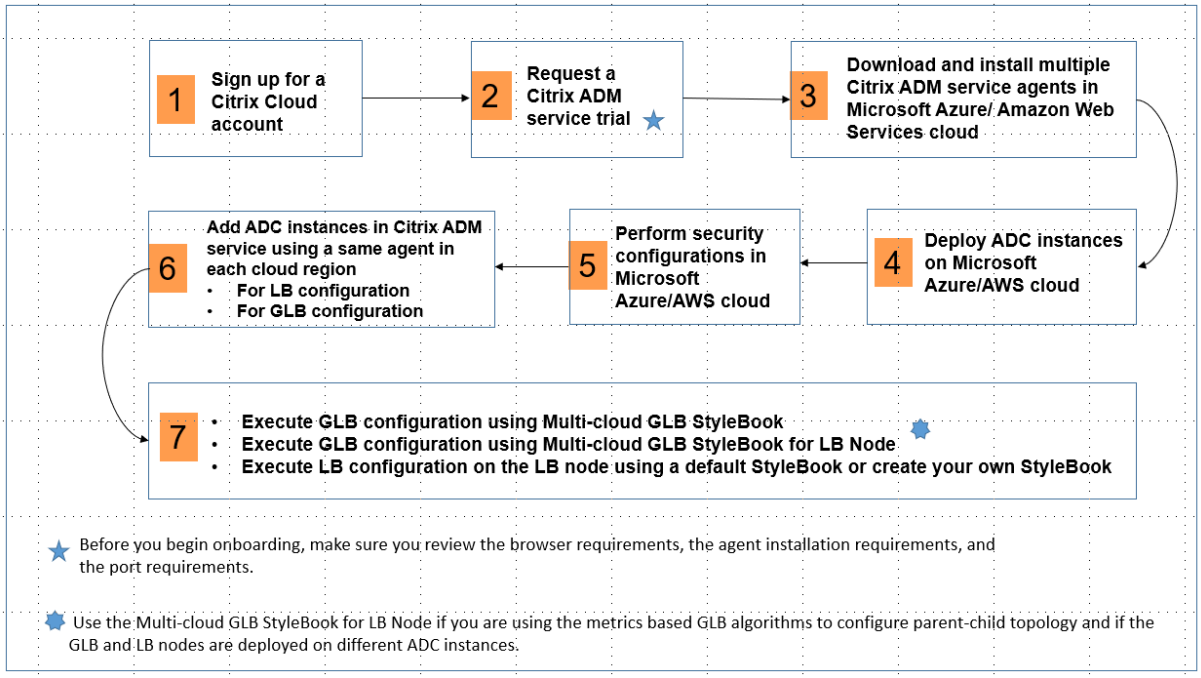
Vous pouvez utiliser le Multi-Cloud GLB StyleBook par défaut sur Citrix ADM pour configurer les instances de Citrix ADC avec une configuration GLB hybride et multi-cloud.

Vous pouvez utiliser le StyleBook GLB Multi-cloud par défaut pour LB Node StyleBook pour configurer les nœuds d'équilibrage de charge Citrix ADC qui sont les sites enfants dans une topologie parent-enfant qui gère le trafic d'application. Utilisez ce StyleBook uniquement si vous souhaitez configurer des nœuds LB dans le cas d'une topologie parent-enfant. Toutefois, chaque nœud LB doit être configuré séparément à l'aide de ce StyleBook.

Flux de travail de la configuration de la solution GLB hybride et multi-cloud Citrix ADC

Vous pouvez utiliser le Multi-Cloud GLB StyleBook fourni sur Citrix ADM pour configurer les instances de Citrix ADC avec une configuration GLB hybride et multi-cloud.

Le diagramme suivant illustre le flux de travail de configuration de la solution GLB hybride et multi-cloud Citrix ADC. Les étapes du diagramme de workflow sont expliquées plus en détail après le diagramme.



Effectuez les tâches suivantes en tant qu'administrateur de cloud :

1. Inscrivez-vous pour un compte Citrix Cloud.

   Pour commencer à utiliser Citrix ADM, créez un compte d'entreprise Citrix Cloud ou rejoignez un compte existant créé par un membre de votre entreprise.

2. Après avoir connecté à Citrix Cloud, cliquez sur **Gérer** dans la vignette **Citrix Application Delivery Management** pour configurer le service ADM pour la première fois.

3. Téléchargez et installez plusieurs agents de service Citrix ADM.

   Vous devez installer et configurer l'agent de service Citrix ADM dans votre environnement réseau pour activer la communication entre Citrix ADM et les instances gérées dans votre datacenter ou cloud. Installez un agent dans chaque région afin de pouvoir configurer les configurations LB et GLB sur les instances gérées. Les configurations LB et GLB peuvent partager un seul agent. Pour plus d'informations sur les trois tâches ci-dessus, reportez-vous à la section Mise en route.

4. Déployez des équilibreurs de charge sur Microsoft Azure/AWS cloud/centres de données locaux.

Selon le type d'équilibreurs de charge que vous déployez sur le cloud et sur site, provisionnez-les en conséquence. Par exemple, vous pouvez provisionner des instances Citrix ADC VPX dans un portail Microsoft Azure Resource Manager (ARM), dans un cloud privé virtuel Amazon Web Services (AWS) et dans des centres de données locaux. Configurez les instances Citrix ADC pour qu'elles fonctionnent en tant que nœuds LB ou GLB en mode autonome, en créant les machines virtuelles et en configurant d'autres ressources. Pour plus d'informations sur le déploiement d'instances Citrix ADC VPX, consultez les documents suivants :

- Lancement de Citrix ADC VPX pour AWS AMI.
- Configuration de Citrix ADC VPX en mode autonome dans Azure Resource Manager.

5. Effectuer des configurations de sécurité.

   Configurez des groupes de sécurité réseau et des ACL réseau dans ARM ou AWS pour contrôler le trafic entrant et sortant pour vos instances et sous-réseaux.

6. Ajoutez des instances de Citrix ADC dans Citrix ADM.

   Les instances de Citrix ADC sont des appliances réseau ou des appliances virtuelles que vous souhaitez découvrir, gérer et surveiller à partir de Citrix ADM. Pour gérer et surveiller ces instances, vous devez ajouter les instances au service et enregistrer les instances LB (si vous utilisez Citrix ADC pour LB) et GLB. Pour plus d'informations sur l'ajout d'instances Citrix ADC dans Citrix ADM, reportez-vous à la sectionMise en route.

7. Implémentez les configurations GLB et LB à l'aide de Citrix ADM StyleBooks par défaut.

   - Utilisez **Multi-cloud GLB StyleBook** pour exécuter la configuration GLB sur les instances GLB Citrix ADC sélectionnées.
   - Mettre en œuvre la configuration d'équilibrage de charge. (Vous pouvez ignorer cette étape si vous disposez déjà de configurations LB sur les instances gérées.)

   Vous pouvez configurer les équilibreurs de charge sur les instances Citrix ADC de l'une des deux manières suivantes :

   - Configurez manuellement les instances pour l'équilibrage de charge des applications. Pour plus d'informations sur la configuration manuelle des instances, reportez-vous à la section Configuration de l'équilibrage de charge de base.
   - Utilisez StyleBooks. Vous pouvez utiliser l'un des Citrix ADM StyleBooks (HTTP/SSL Load-Balancing StyleBook ou HTTP/SSL LoadBalancing (avec Moniteurs) StyleBook) pour créer la configuration de l'équilibrage de charge sur l'instance Citrix ADC sélectionnée. Vous pouvez également créer vos propres StyleBooks. Pour plus d'informations sur StyleBooks, reportez-vous à la section StyleBooks.

8. Utilisez **Multi-cloud GLB StyleBook for LB Node** pour configurer la topologie parent-enfant GLB dans l'un des cas suivants :

- Si vous utilisez les algorithmes GLB basés sur des mesures (moindres paquets, moindres connexions, moindres bandes passantes) pour configurer les nœuds GLB et LB et si les nœuds LB sont déployés sur une autre instance Citrix ADC.
- Si la persistance du site est requise.

Utilisation de StyleBooks pour configurer GLB

April 29, 2021

Vous pouvez utiliser le Multi-Cloud GLB StyleBook pour configurer les configurations GLB sur les instances Citrix ADC qui sont provisionnées dans vos centres de données. Assurez-vous que vous avez configuré l'adresse IP du site sur l'instance GLB d'Citrix ADC dans chaque centre de données.

Vous pouvez également utiliser ce StyleBook pour créer un site parent qui accepte les sites enfants que vous pouvez ajouter ultérieurement dans les nœuds GLB. Pour configurer la configuration GLB multi-cloud sur des instances de Citrix ADC.

1. Accédez à **Applications** > **Configuration**, puis cliquez sur **Créer un nouveau** .
2. La page **Choisir StyleBook** affiche tous les StyleBooks disponibles pour votre utilisation dans Citrix Application Delivery Management (ADM). Faites défiler la page vers le bas et sélectionnez **Multi-cloud GLB StyleBook**.

   Le Multi-Cloud GLB StyleBook est utilisé pour configurer GLB pour une application déployée dans plusieurs clouds et sites locaux. Le StyleBook apparaît sous la forme d'une page d'interface utilisateur sur laquelle vous pouvez entrer les valeurs de tous les paramètres définis dans ce StyleBook.

   > **Remarque**
   >
   > Les termes centre de données et sites sont utilisés de manière interchangeable dans ce document.

3. Définissez les paramètres suivants :

   - **Nom de l'application**. Entrez le nom de l'application déployée sur les sites GLB.
   - **Algorithme GLB**. Choisissez l'algorithme global d'équilibrage de charge (méthode) pour sélectionner le site qui sert un client. Les options disponibles dans la zone de liste déroulante sont LEASTCONNECTION, LEASTBANDWIDTH, LEASTPACKETS, ROUNDROBIN, STATICPROXIMITY, SOURCEIPHASH et RTT.
   - **Fichier de base de données géo**. Si vous avez sélectionné STATICPROXIMITY comme algorithme GLB, entrez le chemin complet et le nom du fichier de base de données contenant les données de proximité statique. Assurez-vous que le fichier de base de données est

présent sur toutes les instances GLB Citrix ADC à l'emplacement spécifié. Vous pouvez également conserver le fichier par défaut.

- **Protocole**. Sélectionnez le protocole d'application de l'application déployée dans la zone de liste déroulante.
- **Paramètres de persistance**. La persistance configurée sur un serveur virtuel conserve les états des connexions sur les serveurs représentés par ce serveur virtuel (par exemple, les connexions utilisées dans le commerce électronique). La persistance remplace les méthodes d'équilibrage de charge une fois le serveur virtuel sélectionné. Si la configuration de persistance est appliquée à un service DOWN, l'instance utilise les méthodes d'équilibrage de charge pour sélectionner un nouveau service et le nouveau service devient permanent pour les demandes ultérieures du client.
- **Type de persistance**. Sélectionnez le type de persistance à utiliser pour cette application. Par exemple, si vous sélectionnez la persistance comme SOURCEIP, après la sélection initiale du site hébergeant l'application, toutes les demandes ultérieures du même client sont envoyées à ce site pour accéder aux services de l'application.
- **Délai d'expiration de la persistance**. Si vous avez sélectionné SOURCEIP comme type de persistance, entrez le nombre de minutes avant l'expiration de la session de persistance après la dernière demande client. La plage est de 2 à 1440 minutes. Les minutes sont résolues en secondes.

4. **Paramètres de débordement**. Configurez la fonction de débordement pour transférer les connexions de débordement vers un serveur virtuel secondaire ou de sauvegarde lorsque, par exemple, la limite de connexion ou la limite de bande passante du serveur virtuel principal a atteint la valeur de seuil.

    - **Méthode de débordement**. Dans la zone de liste déroulante, sélectionnez la méthode de débordement. Par exemple, la méthode de débordement CONNECTION surveille le nombre de connexions actives sur le serveur principal. Si le seuil de débordement est atteint pour cette méthode, les nouvelles connexions sont détournées vers le premier serveur virtuel disponible dans la chaîne de sauvegarde. La méthode de spillover HEALTH vous permet de spillover si le seuil tombe en dessous d'un seuil configuré. Par exemple, moins de 70%.

        > **Remarque**
        >
        > Sauf pour la méthode de débordement HEALTH, d'autres méthodes sont applicables uniquement lorsque Citrix ADC est utilisé comme instance d'équilibrage de charge.

    - **Seuil de débordement.** Entrez une valeur de seuil pour la méthode de débordement que vous avez sélectionnée.
    - **Persistance de débordement.** Activez la persistance des débordements si vous souhaitez que le serveur virtuel de sauvegarde continue à traiter les demandes qu'il reçoit, même après que la charge sur le principal tombe en dessous du seuil.

- **Délai de persistance de débordement**. Configurez la période pendant laquelle la persistance Spillover est en vigueur. La valeur minimale est 2 minutes et la valeur maximale est 1440 minutes. Les minutes sont résolues en secondes.

5. **Persistance/ID de persistance Spillover**. Si vous avez sélectionné SOURCEIP comme type de persistance ou si la persistance Spillover est activée, entrez un numéro unique pour identifier le même domaine sur toutes les appliances GLB. La gamme est de 1 à 65535.

   - **Vérification de l'état des points d'extrémité de service GLB (Facultatif)**
   - **Type de vérification de l'état**. Dans la zone de liste déroulante, sélectionnez le type de sonde utilisée pour vérifier l'état de l'adresse VIP de l'équilibreur de charge qui représente l'application sur un site.
   - **Mode sécurisé**. (Facultatif) Sélectionnez **Oui** pour activer ce paramètre si des vérifications d'intégrité basées sur SSL sont requises.
   - **Demande HTTP**. (Facultatif) Si vous avez sélectionné HTTP comme type de vérification de santé, entrez la requête HTTP complète utilisée pour sonder l'adresse VIP.
   - **Liste des codes de réponse d'état HTTP**. (Facultatif) Si vous avez sélectionné HTTP comme type de vérification de l'état, entrez la liste des codes d'état HTTP attendus dans les réponses aux demandes HTTP lorsque le VIP est sain.

6. **Noms de domaine GLB**. Cette section vous permet de configurer la liste des noms de domaine DNS associés à cette application. Cliquez sur l'icône plus (**+**) pour créer un nom de domaine DNS pour l'application.

7. **Sites GLB**. Cette section vous permet de configurer la liste des sites sur lesquels cette application est déployée.

   Le site GLB est l'entité de niveau supérieur pour les communications GLB. Les informations spécifiées lors de la configuration du site sont utilisées pour lier des sites locaux à des sites distants et partager des données de surveillance à l'aide du protocole MEP (Citrix Metrics Exchange Protocol). L'adresse IP appartient à l'instance GLB Citrix ADC et utilise le port TCP 3009. La section Sites GLB du StyleBook vous permet de spécifier autant de sites GLB que nécessaire.

   Cliquez sur l'icône plus (**+**) pour ajouter des sites.

   - **Nom du site**. Entrez le nom du site.
   - **Adresse IP du site**. Entrez l'adresse IP utilisée par le site comme adresse IP source lors de l'échange de mesures avec d'autres sites. Cette adresse IP est supposée être déjà configurée sur l'instance GLB de chaque site.
   - **Adresse IP publique du site**. (Facultatif) Entrez l'adresse IP publique du site qui est utilisée pour échanger des mesures, si l'adresse IP de ce site est traduite.

8. **Sites enfants**. Cliquez sur l'icône plus (+) pour configurer les sites enfants requis.

   - **Nom du site enfant**. Entrez le nom du site.

- **Adresse IP du site enfant**. Entrez l'adresse IP du site enfant. Ici, utilisez l'adresse IP privée ou SNIP du nœud Citrix ADC configuré en tant que site enfant.
- **Adresse IP publique du site**. (Facultatif) Entrez l'adresse IP publique du site qui est utilisée pour échanger des mesures, si l'adresse IP de ce site est traduite.

9. **Persistance du site des services**. Sélectionnez le type de persistance utilisé dans la zone de liste déroulante à utiliser pour les services GLB sur le site.

   - Sélectionnez ConnectionProxy pour permettre au site de créer une connexion au site GLB qui a inséré le cookie du site, proxy la demande du client au site d'origine, recevoir une réponse du site GLB d'origine, relayer la réponse au client et fermer la connexion.
   - Sélectionnez `HTTPRedirect` cette option pour autoriser le site à rediriger la demande vers le site qui a initialement inséré le cookie. Pour plus d'informations sur la persistance, reportez-vous à la section Configuration des connexions persistantes.

10. **Active GLB Services** : cette section vous permet de configurer la liste des services actifs sur les sites sur lesquels l'application est déployée.

    IP du service. Entrez l'adresse IP du service GLB sur ce site.

    - **Adresse IP publique du service**. Si l'adresse IP virtuelle est privée et possède une adresse IP publique qui lui est attribuée, spécifiez l'adresse IP publique.
    - **Port de service**. Entrez le port du service GLB sur ce site.
    - **Pondération du service**. Entrez la pondération affectée au service GLB.

      > **Remarque**
      >
      > Vous pouvez affecter des pondérations relatives aux services, en fonction du pourcentage de trafic qui doit être envoyé au cloud et du pourcentage de trafic qui doit être géré sur site. Par exemple, si vous avez attribué une pondération de 3 au service GLB basé sur le nuage et de 7 au service GLB local, 30 % du trafic est dirigé vers le cloud et 70 % sont gérés sur site.

    - **Nom du site**. Entrez le nom du site sur lequel se trouve le service GLB.
    - **Préfixe du site**. Entrez un préfixe pour le site sur lequel le service GLB est configuré. Ceci est applicable lorsque la persistance du site est activée et que la méthode est `httpredirect`. La valeur du préfixe de site doit être unique sur tous les services GLB d'une application.
    - **Nombre maximal de connexions client**. Entrez le nombre maximal de connexions clientes configurées dans le service GLB si vous avez sélectionné DYNAMICCONNECTION comme méthode de débordement dans les paramètres de **persistance de débordement**. Si vous ne fournissez pas de valeur, le système attribue par défaut un nombre aux connexions client maximales qui peuvent être configurées.

11. **Services GLB passifs** : cette section vous permet de configurer la liste des services passifs sur les sites où l'application est déployée avec une topologie active-passive. Fournissez des informations pour tous les services GLB de sauvegarde semblables à celles que vous avez fournies pour les services GLB actifs.
12. Cliquez sur **Instances cibles** et sélectionnez les instances Citrix ADC configurées en tant qu'instances GLB sur chaque site sur lequel déployer la configuration GLB.
13. Cliquez sur **Créer** pour créer la configuration GLB sur les instances Citrix ADC sélectionnées. Vous pouvez également cliquer sur **Essai** pour vérifier les objets qui seraient créés dans les instances cibles. La configuration StyleBook (pack de configuration) que vous avez créée apparaît dans la liste des configurations de la page Configurations. Vous pouvez examiner, mettre à jour ou supprimer cette configuration (pack de configuration) à l'aide de l' interface graphique Citrix ADM.

Utilisation de StyleBooks pour configurer GLB sur les nœuds Citrix ADC LB

April 29, 2021

Vous pouvez utiliser le **Multi-Cloud GLB StyleBook for LB Node** si vous utilisez les algorithmes GLB basés sur des mesures (Least Packets, Last Connections, Last Bandwidth) pour configurer les nœuds GLB et LB et si les nœuds LB sont déployés sur une autre instance Citrix ADC.

Vous pouvez également utiliser ce StyleBook pour configurer des sites enfants supplémentaires pour un site parent existant. Ce StyleBook configure un site enfant à la fois. Ainsi, créez autant de configurations (packs de configuration) à partir de ce StyleBook qu'il y a des sites enfants. Le StyleBook applique la configuration GLB sur les sites enfants. Vous pouvez configurer un maximum de 1024 sites enfants.

> **Remarque**
>
> PermetStyleBook GLB multi-cloudde configurer les sites parents.

Ce StyleBook formule les hypothèses suivantes :

- Une adresse SNIP ou une adresse IP de site GLB est configurée.
- Les groupes de pare-feu et de sécurité requis sont configurés dans les fournisseurs de services cloud.

Configuration d'un site enfant dans une topologie parent-enfant à l'aide de Multi-Cloud GLB StyleBook for LB Node

1. Accédez à **Applications** > **Configuration**, puis cliquez sur **Créer un nouveau** .
2. La page **Choisir StyleBook** affiche tous les StyleBooks disponibles pour votre utilisation dans Citrix Application Delivery Management (ADM). Faites défiler la page vers le bas et sélectionnez **Multi-cloud GLB StyleBook for LB Node.**

   Le StyleBook apparaît sous la forme d'une page d'interface utilisateur sur laquelle vous pouvez entrer les valeurs de tous les paramètres définis dans ce StyleBook.

   > **Remarque**
   >
   > Les termes centre de données et sites sont utilisés de manière interchangeable dans ce document.

3. Définissez les paramètres suivants :

   - **Nom de l'application**. Entrez le nom de l'application GLB déployée sur les sites GLB pour lesquels vous souhaitez créer des sites enfants.
   - **Protocole**. Sélectionnez le protocole d'application de l'application déployée dans la zone de liste déroulante.
   - **Vérification de l'état de LB (facultatif)**
     - **Type de vérification de l'état**. Dans la zone de liste déroulante, sélectionnez le type de sonde utilisée pour vérifier l'état de l'adresse VIP de l'équilibreur de charge qui représente l'application sur un site.
     - **Mode sécurisé**. (Facultatif) Sélectionnez **Oui** pour activer ce paramètre si des vérifications d'intégrité basées sur SSL sont requises.
     - **Demande HTTP**. (Facultatif) Si vous avez sélectionné HTTP comme type de vérification de santé, entrez la requête HTTP complète utilisée pour sonder l'adresse VIP.
     - **Liste des codes de réponse d'état HTTP**. (Facultatif) Si vous avez sélectionné HTTP comme type de vérification de l'état, entrez la liste des codes d'état HTTP attendus dans les réponses aux demandes HTTP lorsque le VIP est sain.

4. Configuration du site parent.

   Fournissez les détails du site parent (nœud GLB) sous lequel vous souhaitez créer le site enfant (nœud LB).

   - **Nom du site**. Entrez le nom du site parent.
   - **Adresse IP du site**. Entrez l'adresse IP utilisée par le site parent comme adresse IP sourceIP lors de l'échange de mesures avec d'autres sites. Cette adresse IP est supposée être déjà configurée sur le nœud GLB de chaque site.
   - **Adresse IP publique du site**. (Facultatif) Entrez l'adresse IP publique du site parent qui est utilisée pour échanger des mesures, si l'adresse IP de ce site est Nat'ed.

5. Configuration du site enfant.

   Fournissez les détails du site enfant.

   - **Nom du site**. Entrez le nom du site.
   - **Adresse IP du site**. Entrez l'adresse IP du site enfant. Ici, utilisez l'adresse IP privée ou SNIP du nœud Citrix ADC configuré en tant que site enfant.
   - **Adresse IP publique du site**. (Facultatif) Entrez l'adresse IP publique du site enfant utilisé pour échanger des mesures, si l'adresse IP de ce site est Nat'ed.

6. Configuration des services GLB actifs (facultatif)

   Configurez les services GLB actifs uniquement si l'adresse IP du serveur virtuel LB n'est pas une adresse IP publique. Cette section vous permet de configurer la liste des services GLB locaux sur les sites où l'application est déployée.

   - **IP du service**. Entrez l'adresse IP du serveur virtuel d'équilibrage de charge sur ce site.
   - **Adresse IP publique du service**. Si l'adresse IP virtuelle est privée et possède une adresse IP publique qui lui est attribuée, spécifiez l'adresse IP publique.
   - **Port de service**. Entrez le port du service GLB sur ce site.
   - **Nom du site**. Entrez le nom du site sur lequel se trouve le service GLB.

7. Cliquez sur **Instances cibles** et sélectionnez les instances Citrix ADC configurées en tant qu'instances GLB sur chaque site sur lequel déployer la configuration GLB.

8. Cliquez sur **Créer** pour créer la configuration LB sur l'instance Citrix ADC sélectionnée (nœud LB). Vous pouvez également cliquer sur **Essai** pour vérifier les objets qui seraient créés dans les instances cibles. La configuration de StyleBook que vous avez créée apparaît dans la liste des configurations de la page Configurations. Vous pouvez examiner, mettre à jour ou supprimer cette configuration à l'aide de l'interface graphique Citrix ADM.

Analyse d'infrastructure

April 29, 2021

L'un des principaux objectifs des administrateurs réseau est de surveiller les instances de Citrix ADC. Les instances ADC offrent des informations intéressantes sur l'utilisation et les performances des applications et des postes de travail auxquels elles accèdent. Les administrateurs doivent surveiller l'instance ADC et analyser les flux d'application traités par chaque instance ADC. Les administrateurs doivent également être en mesure de résoudre les problèmes probables de configuration, d'installation, de connectivité, de certificats et autres impacts sur l'utilisation ou les performances de l'application. Par exemple, un changement soudain dans le modèle de trafic d'application peut être dû à un changement de configuration SSL comme la désactivation d'un protocole SSL. Les

administrateurs doivent être en mesure d'identifier rapidement la corrélation entre ces points de données pour s'assurer que :

- La disponibilité des applications est dans un état optimal
- Il n'y a aucun problème de consommation de ressources, de matériel, de capacité ou de modification de configuration
- Il n'y a pas d'inventaire inutilisé
- Il n'y a pas de certificats expirés

La fonctionnalité Analyse de l'infrastructure simplifie le processus d'analyse des données en corrélation de plusieurs sources de données et en quantifiant à un score mesurable qui définit l'intégrité d'une instance. Grâce à cette fonctionnalité, les administrateurs disposent d'un point de contact unique pour comprendre le problème, l'origine du problème et les correctifs probables qu'ils peuvent effectuer.

Analyse de l'infrastructure dans Citrix ADM

La fonctionnalité Analyse de l'infrastructure rassemble toutes les données collectées à partir des instances de Citrix ADC et les quantifie en un **score d'instance** qui définit l'intégrité des instances. Le score d'instance est résumé sur une vue tabulaire ou sous forme de visualisation de pack de cercle. La fonctionnalité Analyse de l'infrastructure vous aide à visualiser les facteurs qui ont entraîné ou pourraient entraîner un problème sur les instances. Cette visualisation vous aide également à déterminer les actions à effectuer pour empêcher le problème et sa récurrence.

Score d'instance

Le score d'instance indique l'état de santé d'une instance ADC. Un score de 100 signifie une instance parfaitement saine sans aucun problème. Le score d'instance capture différents niveaux de problèmes potentiels sur l'instance. Il s'agit d'une mesure quantifiable de la santé par exemple et de multiples « indicateurs de santé » contribuent au score.

Les**indicateurs de santé** sont les éléments constitutifs du score d'instance, où le score est calculé périodiquement pour une « période de surveillance » prédéfinie, en fonction de tous les indicateurs détectés dans cette fenêtre de temps. Actuellement, l'analyse de l'infrastructure calcule le score d'instance une fois par heure en fonction des données recueillies à partir des instances.
Un indicateur peut être défini comme n'importe quelle activité (un événement ou un problème) qui appartient à l'une des catégories suivantes sur les instances.

- Indicateurs de ressources système
- Indicateurs d'événements critiques
- Indicateurs de configuration SSL

- Indicateurs d'écart de configuration

Indicateurs de santé expliqués

- Indicateurs des ressources du système

  Voici les problèmes critiques de ressources système qui peuvent se produire sur les instances de Citrix ADC et surveillés par Citrix ADM.

  - Utilisation**élevée du processeur**. L'utilisation du processeur a franchi la valeur de seuil supérieure dans l'instance de Citrix ADC.
  - Utilisation**élevée de la mémoire**. L'utilisation de la mémoire a franchi la valeur de seuil supérieure dans l'instance de Citrix ADC.
  - Utilisation**élevée du disque**. L'utilisation du disque a franchi la valeur de seuil supérieure dans l'instance de Citrix ADC.
  - **Erreurs de disque**. Il y a des erreurs sur le disque dur 0 ou le disque dur 1 sur l'Hypervisor où l'instance ADC est installée.
  - **Panne de courant**. Le bloc d'alimentation a échoué ou s'est déconnecté de l'instance ADC.
  - **Échec de la carte SSL**. La carte SSL installée sur l'instance a échoué.
  - **Erreurs flash**. Des erreurs Compact Flash sont visibles sur l'instance de Citrix ADC.
  - **rejette la carte réseau**. Les paquets ignorés par la carte NIC ont franchi la valeur de seuil supérieure dans l'instance de Citrix ADC.

Pour plus d'informations sur ces erreurs de ressources système, voirTableau de bord de l'instance.

- Indicateurs d'événements critiques

  Les événements critiques suivants sont identifiés par les événements sous la fonction de gestion des événements d'ADM qui sont configurés avec gravité critique.

  - **Échec de synchronisation HA**. La synchronisation de la configuration entre les instances ADC en haute disponibilité a échoué sur le serveur secondaire.
  - **HA pas de battements cardiaques**. Le serveur principal dans une paire d'instances ADC en haute disponibilité ne reçoit pas de battements cardiaques du serveur secondaire.
  - **HA mauvais état secondaire**. Le serveur secondaire d'une paire d'instances ADC en haute disponibilité est en état Baisse, Inconnu ou Rester secondaire.
  - **La version HA est inexacte**. La version des images logicielles ADC installées sur une paire d'instances ADC en haute disponibilité ne correspond pas.
  - **Échec de la synchronisation du cluster**. La synchronisation de la configuration entre les instances ADC en mode cluster a échoué.

- **La version du cluster est inexacte**. La version des images logicielles ADC installées sur les instances ADC en mode cluster ne correspond pas.
- **Échec de propagation du cluster**. La propagation des configurations vers toutes les instances d'un cluster a échoué.

> **Remarque**
>
> Vous pouvez disposer de votre liste d'événements SNMP critiques en modifiant les niveaux de gravité des événements. Pour plus d'informations sur la modification des niveaux de gravité, voirModifiez la gravité signalée des événements qui se produisent sur les instances Citrix ADC.

Pour plus d'informations sur les événements dans Citrix ADM, consultezÉvénements.

- Indicateurs de configuration SSL
  - **Force de clé non recommandée**. La force clé des certificats SSL n'est pas conforme aux normes Citrix
  - **Émetteur non recommandé**. L'émetteur du certificat SSL n'est pas recommandé par Citrix.
  - Les**certificats SSL ont expiré**. Le certificat SSL installé dans l'instance ADC a expiré.
  - **Expiration des certificats SSL due**. Le certificat SSL installé dans l'instance ADC est sur le point d'expirer dans la semaine suivante.
  - **Algorithmes non recommandés**. Les algorithmes de signature des certificats SSL installés dans l'instance ADC ne sont pas conformes aux normes Citrix.

Pour plus d'informations sur les certificats SSL, voirTableau debord SSL.

- Indicateurs d'écart de configuration
  - **Modèle de dérive de configuration**. Il y a une dérive (modifications non enregistrées) dans la configuration à partir des modèles d'audit que vous avez créés avec des configurations spécifiques que vous souhaitez auditer sur certaines instances.
  - La**dérive de configuration par défaut**. Il y a une dérive (modifications non enregistrées) dans la configuration à partir des fichiers de configuration par défaut.

Pour plus d'informations sur les écarts de configuration et sur la façon d'exécuter des rapports d'audit pour vérifier les écarts de configuration, voirAfficher les rapports d'audit.

Voir les problèmes de capacité ADC

Lorsqu'une instance ADC a consommé la plus grande partie de sa capacité disponible, la suppression de paquets peut se produire lors du traitement du trafic client. Ce problème provoque de faibles

performances dans une instance ADC. En comprenant ces problèmes de capacité ADC, vous pouvez allouer des licences supplémentaires de manière proactive afin de stabiliser les performances de ADC.

Pour afficher les problèmes de capacité de l'ADC,

1. Accédez à **Réseaux > Analyse de l'infrastructure**.
2. Développez l'instance pour laquelle vous souhaitez afficher les problèmes de capacité.

L'ADM interroge ces événements toutes les cinq minutes à partir de l'instance ADC et affiche les baisses de paquets ou les incréments de compteur de limite de vitesse s'il existe. Les problèmes sont classés selon les paramètres de capacité suivants :

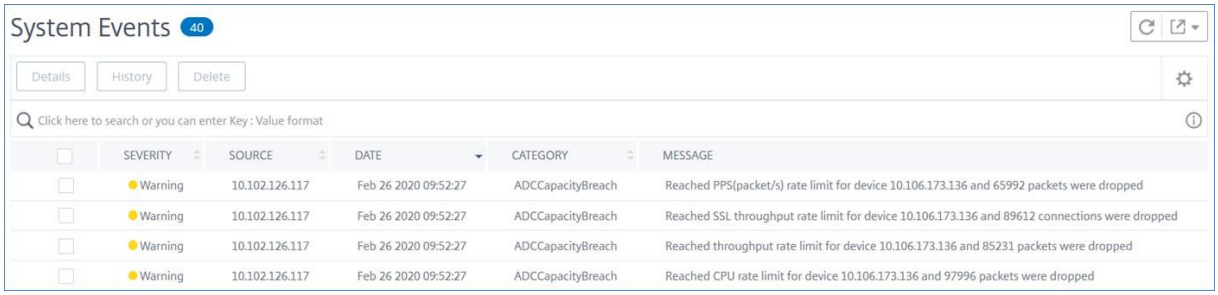
- **Limite de débit atteinte** : nombre de paquets abandonnés dans l'instance après que la limite de débit est atteinte.
- **Limite de CPU PE atteinte** : nombre de paquets abandonnés sur toutes les cartes réseau après que la limite de CPU PE est atteinte.
- **Limite PPS atteinte** : nombre de paquets abandonnés dans l'instance après que la limite PPS est atteinte.
- **Limite de débit SSL** : nombre de fois que la limite de débit SSL est atteinte.
- **Limite de taux TPS SSL** : Nombre de fois que la limite TPS SSL a été atteinte.

L'ADM calcule le score d'instance sur le seuil de capacité défini.

- Seuil bas — 1 incrément de dépassement de paquets ou de compteur de limite de taux
- Seuil élevé : 10000 paquets baisse ou incrément du compteur de limite de taux

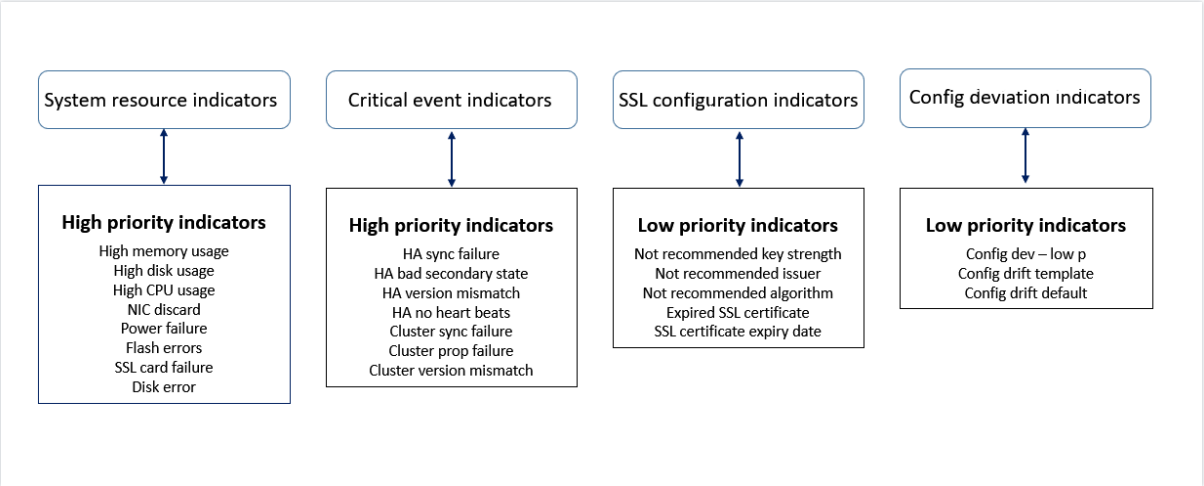
Par conséquent, lorsqu'une instance ADC franchit le seuil de capacité, le score d'instance est affecté.

Lorsque les paquets diminuent ou que le compteur de limite de vitesse s'incrémente, un événement est généré sous la catégorie `ADCCapacityBreach`. Pour afficher ces événements, accédez à **Comptes > Événements système**.



Valeur des indicateurs de santé

Les indicateurs sont classés en indicateurs de priorité élevée et en indicateurs de faible priorité sur la base de leurs valeurs, comme suit :



Les indicateurs de santé d'un même groupe d'indicateurs ont des pondérations différentes qui leur sont attribuées. Un indicateur peut contribuer plus à réduire le score d'instance qu'un autre indicateur. Par exemple, une utilisation élevée de la mémoire réduit le score d'instance plus qu'une utilisation élevée du disque, une utilisation élevée du processeur et un rejet de carte réseau. Si une instance a un plus grand nombre d'indicateurs détectés dessus, le moindre est le score d'instance.

La valeur d'un indicateur est calculée sur la base des règles suivantes. L'indicateur est dit être détecté de l'une des trois façons suivantes :

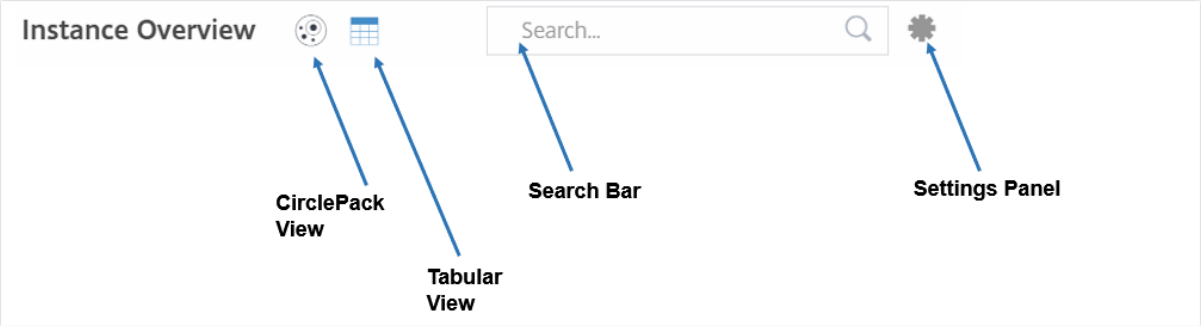
1. **Basé sur une activité**. Par exemple, un indicateur de ressource système est déclenché chaque fois qu'il y a une panne de courant sur l'instance, et cet indicateur réduit la valeur du score d'instance. Lorsque l'indicateur est effacé, la pénalité est effacée et le score de l'instance augmente.
2. **Basé sur la violation de la valeur seuil**. Par exemple, un indicateur de ressource système est déclenché lorsque la carte NIC rejette les paquets et que le seuil est dépassé.
3. **Basé sur la violation des valeurs de seuil faible et élevé**. Ici, un indicateur peut être déclenché de deux façons :
    - Lorsque la valeur de l'indicateur se situe entre les seuils bas et les seuils élevés, auquel cas une pénalité partielle est imposée sur le score de l'instance.
    - Lorsque la valeur dépasse le seuil élevé, auquel cas une pénalité complète est imposée sur le score de l'instance.
    - Aucune pénalité n'est imposée sur le score d'instance si la valeur tombe en dessous d'un seuil bas.

Par exemple, l'utilisation de l'UC est un indicateur de ressource système déclenché lorsque la valeur d'utilisation franchit le seuil bas et également lorsque la valeur franchit le seuil élevé.

Tableau de bord de l'analyse de l'infrastructure

Accédez à **Réseaux** > **Analyse de l'infrastructure** .

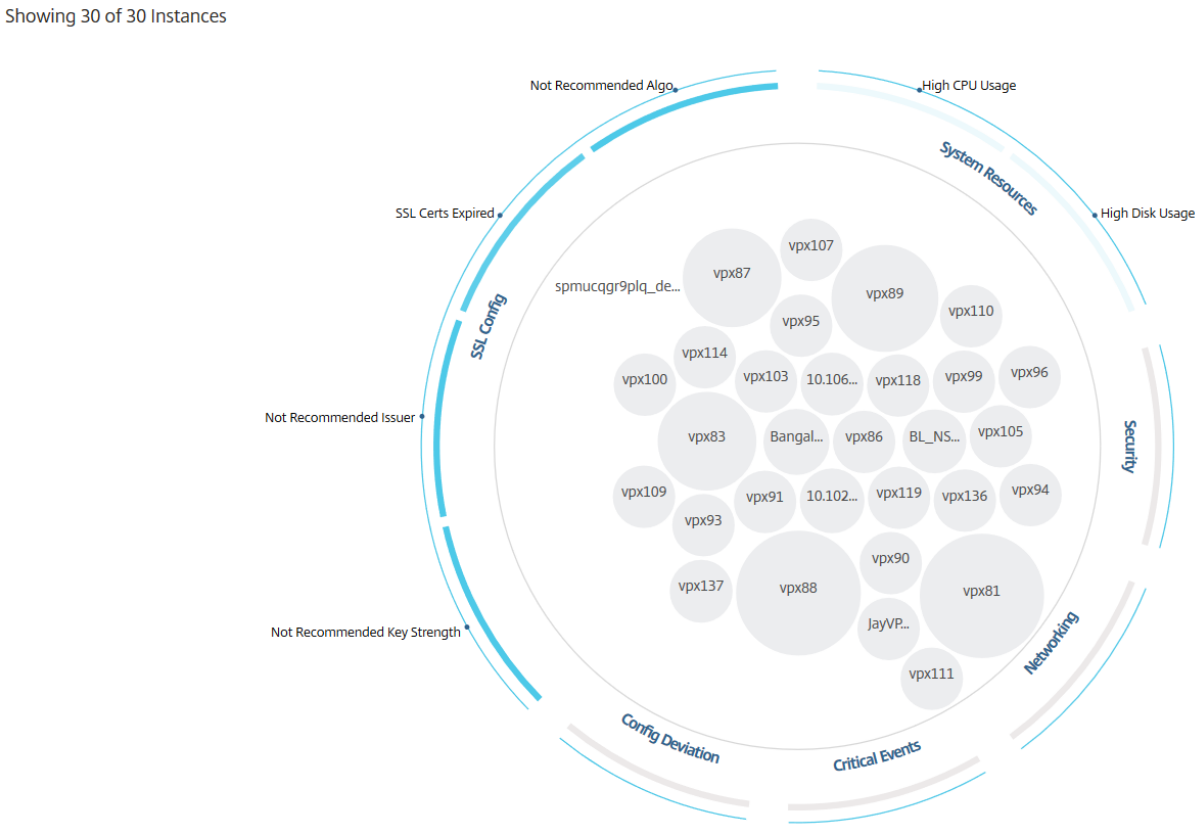
L'analyse de l'infrastructure peut être affichée au format **Circle Pack** ou **Tabulaire** . Vous pouvez basculer entre les deux formats.



- Dans la vue Tabulaire, vous pouvez rechercher une instance en tapant le nom d'hôte ou l'adresse IP dans la barre de recherche.
- Par défaut, la page Analyse de l'infrastructure affiche le panneau Récapitulatif sur le côté droit de la page.
- Cliquez sur l'icône **Paramètres** pour afficher le panneau **Paramètres** .
- Dans les deux formats de vue, le panneau Récapitulatif affiche les détails de toutes les instances de votre réseau.

Vue du pack de cercle

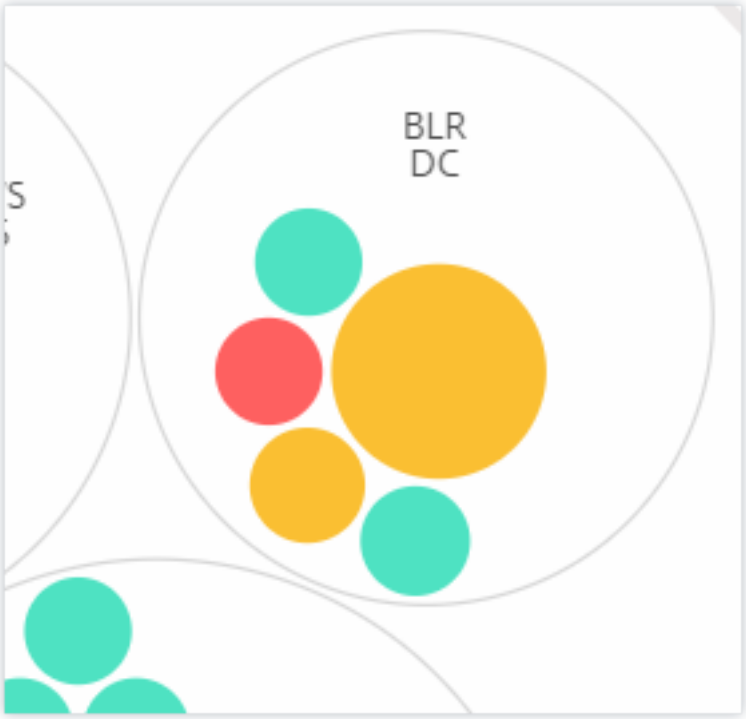
Les diagrammes d'emballage des cercles montrent les groupes d'instances sous forme de cercles étroitement organisés. Ils affichent souvent des hiérarchies où les groupes d'instances plus petits sont soit colorés de la même manière que les autres dans la même catégorie, soit imbriqués dans des groupes plus grands. Les packs Circle représentent des ensembles de données hiérarchiques et montrent différents niveaux de la hiérarchie et comment ils interagissent les uns avec les autres.



Cercles d'instance

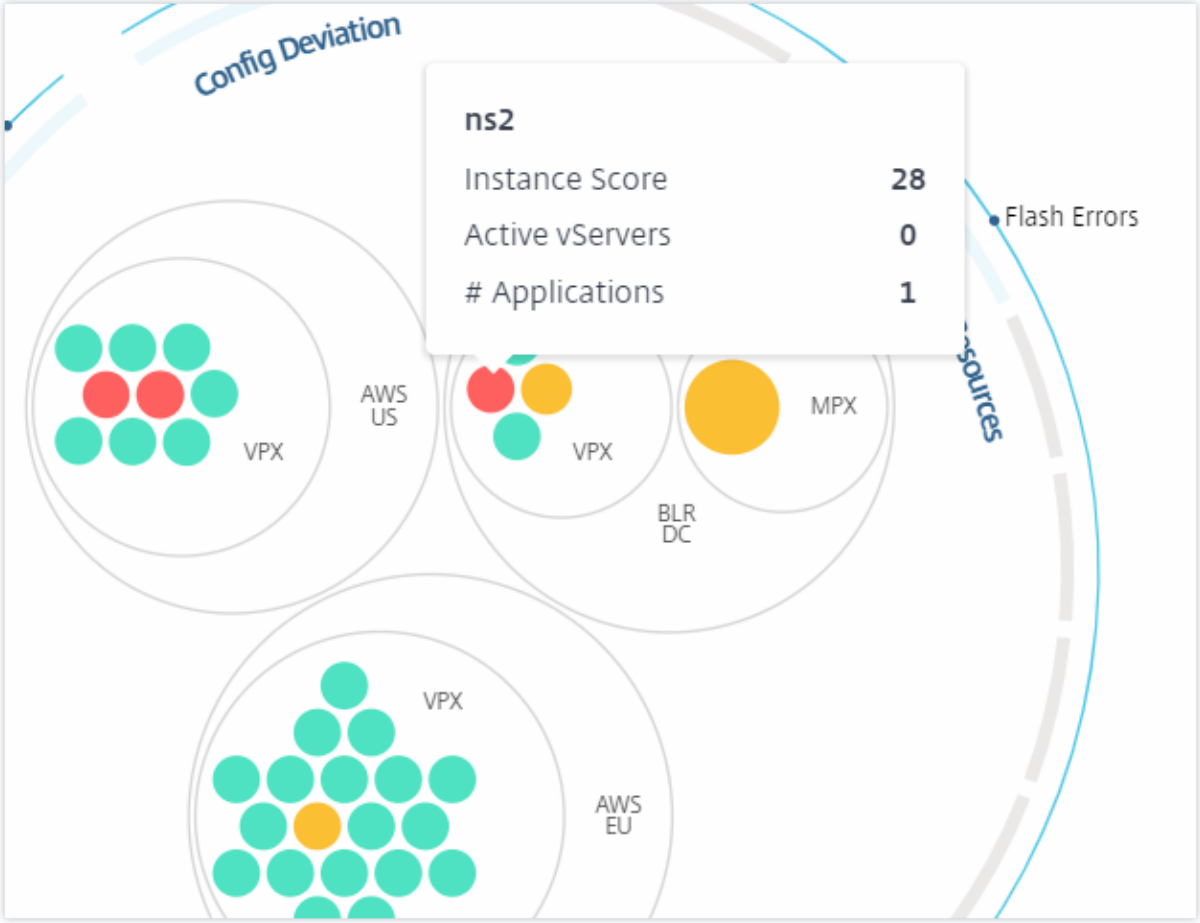
Couleur. Chaque instance est représentée dans Circle Pack sous la forme d'un cercle coloré. La couleur du cercle indique l'état de santé de cette instance.

- **Vert** - le score d'instance est compris entre 100 et 80. L'instance est saine.
- **Jaune** - le score d'instance est compris entre 80 et 50 ; certains problèmes ont été remarqués et ont besoin d'être examinés.
- **Rouge** - le score d'instance est inférieur à 50. L'instance est à un stade critique car plusieurs problèmes sont remarqués sur cette instance.



Taille : La taille de ces cercles colorés indique le nombre de serveurs virtuels configurés sur cette instance. Un cercle plus grand indique qu'il y a un plus grand nombre de serveurs virtuels.

Vous pouvez placer le pointeur de la souris sur chacun des cercles d'instance (cercles colorés) pour afficher un résumé. L'info-bulle de survol affiche le nom d'hôte de l'instance, le nombre de serveurs virtuels actifs et le nombre d'applications configurées sur cette instance.

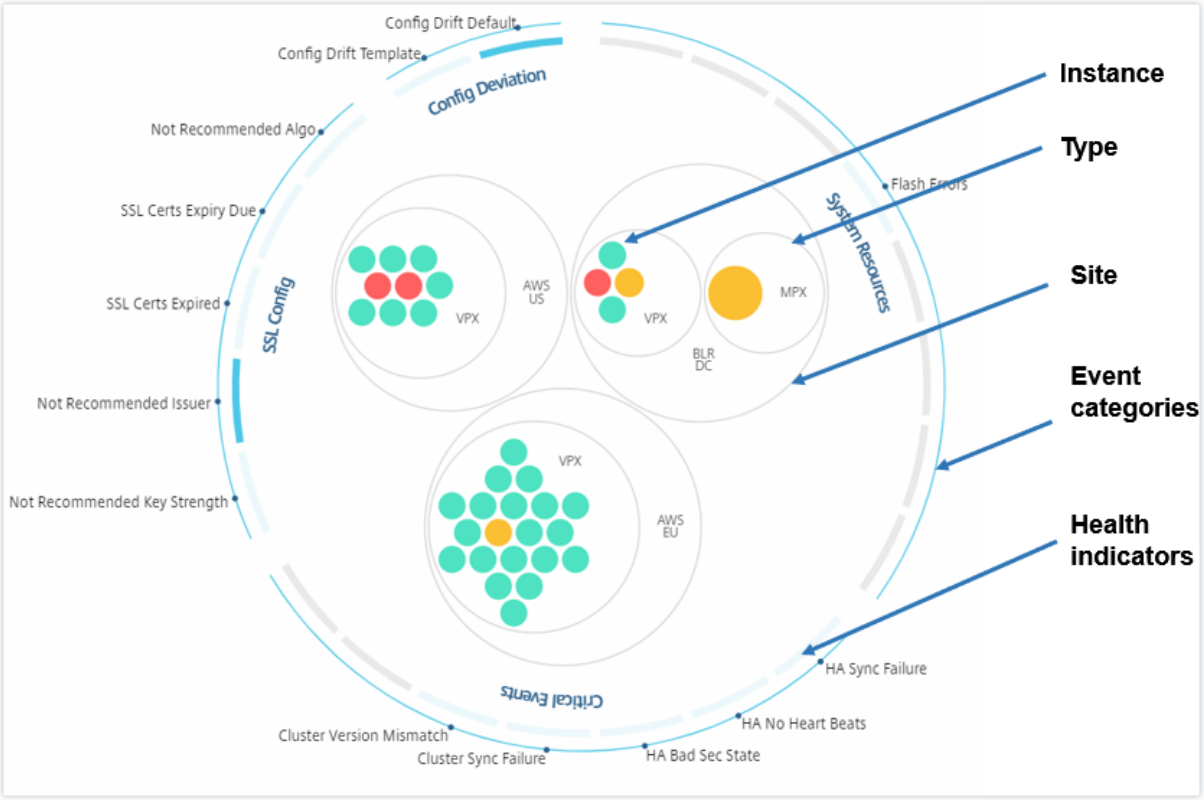


Cercles d'instance groupés

Le pack de cercles au départ comprend des cercles d'instance regroupés, imbriqués ou emballés à l'intérieur d'un autre cercle selon les critères suivants :

- le site où ils sont déployés
- le type d'instances déployées - VPX, MPX, SDX et CPX
- le modèle virtuel ou physique de l'instance ADC
- la version de l'image ADC installée sur les instances

L'image suivante montre un Circle Pack dans lequel les instances sont d'abord regroupées par le site ou le centre de données où elles sont déployées, puis regroupées en fonction de leur type, VPX et MPX.

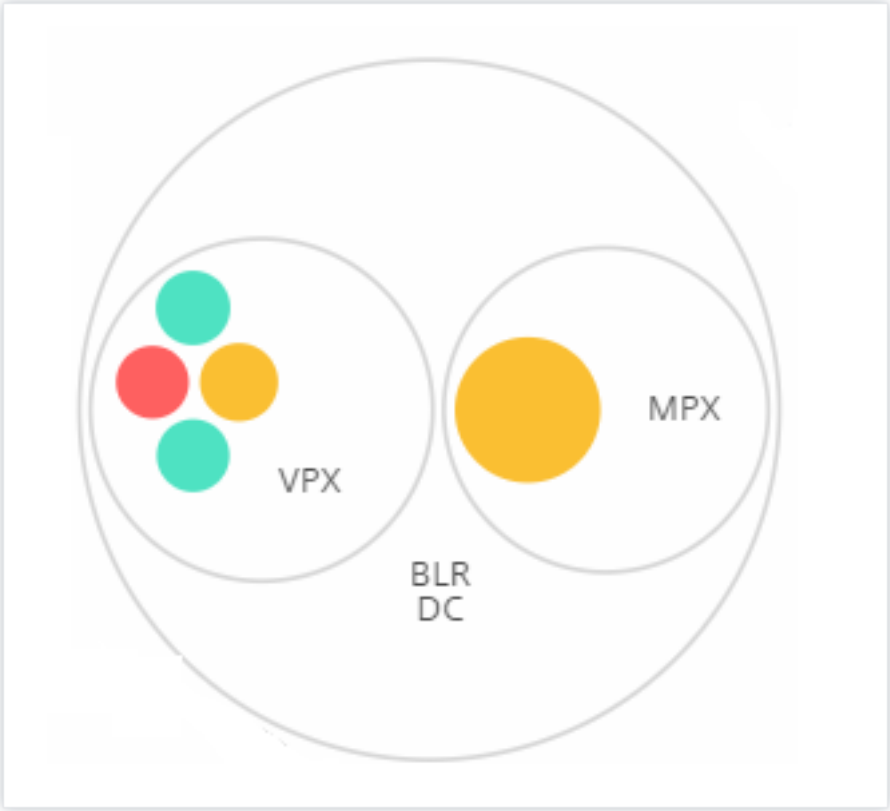


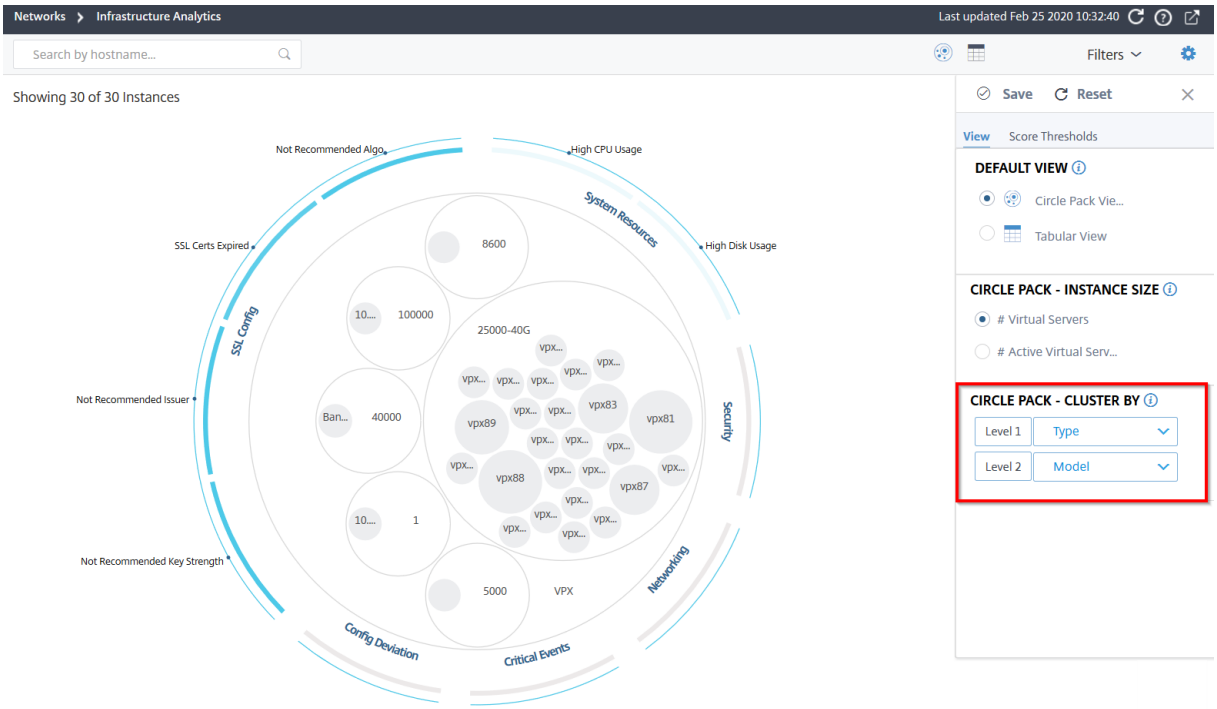
Tous ces cercles imbriqués sont délimités par deux cercles les plus extérieurs. Les deux cercles externes représentent les quatre catégories d'événements surveillés par Citrix ADM (ressources système, événements critiques, configuration SSL et écart de configuration) et les indicateurs de santé contributifs.

Cercles d'instance en cluster

Citrix ADM surveille de nombreuses instances. Pour faciliter la surveillance et la maintenance de ces instances, Infrastructure Analytics vous permet de les regrouper à deux niveaux. Autrement dit, les regroupements d'instances peuvent être imbriqués dans un autre groupe.

Par exemple, le centre de données BLR comporte deux types d'instances ADC - VPX et MPX, déployées dans celui-ci. Vous pouvez d'abord regrouper les instances ADC par leur type, puis regrouper toutes les instances par le site sur lequel elles sont regroupées. Vous pouvez désormais facilement identifier le nombre de types d'instances déployées dans les sites que vous gérez.

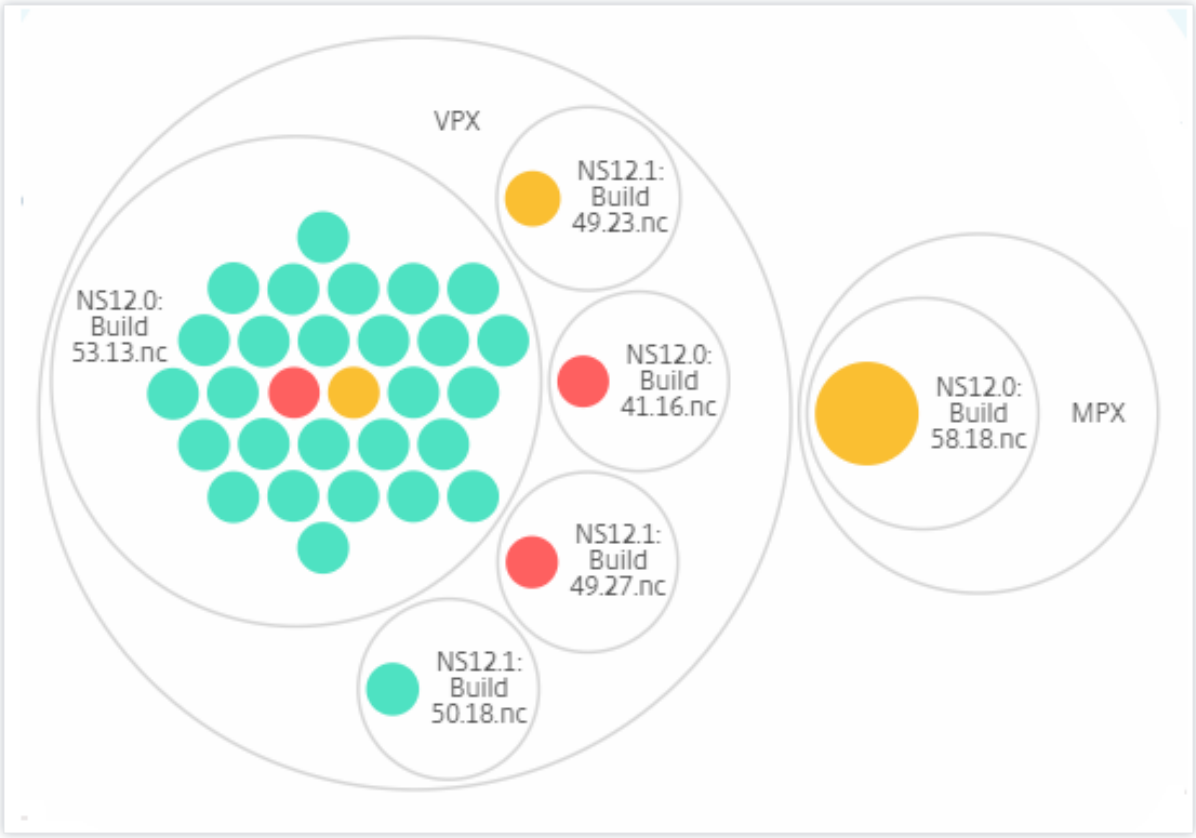




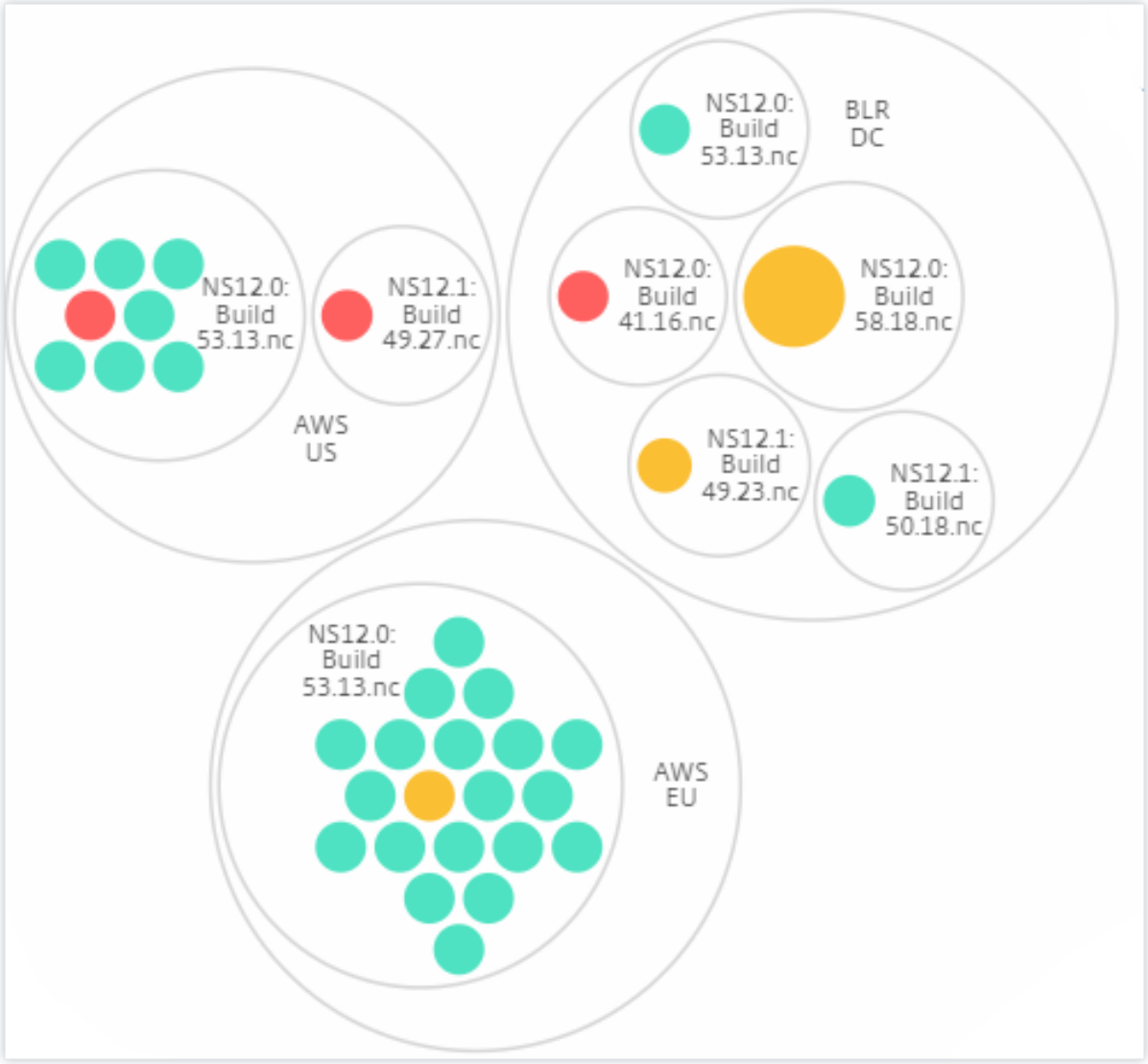
Voici quelques autres exemples de regroupement à deux niveaux :

Site et modèle :

Type et version :

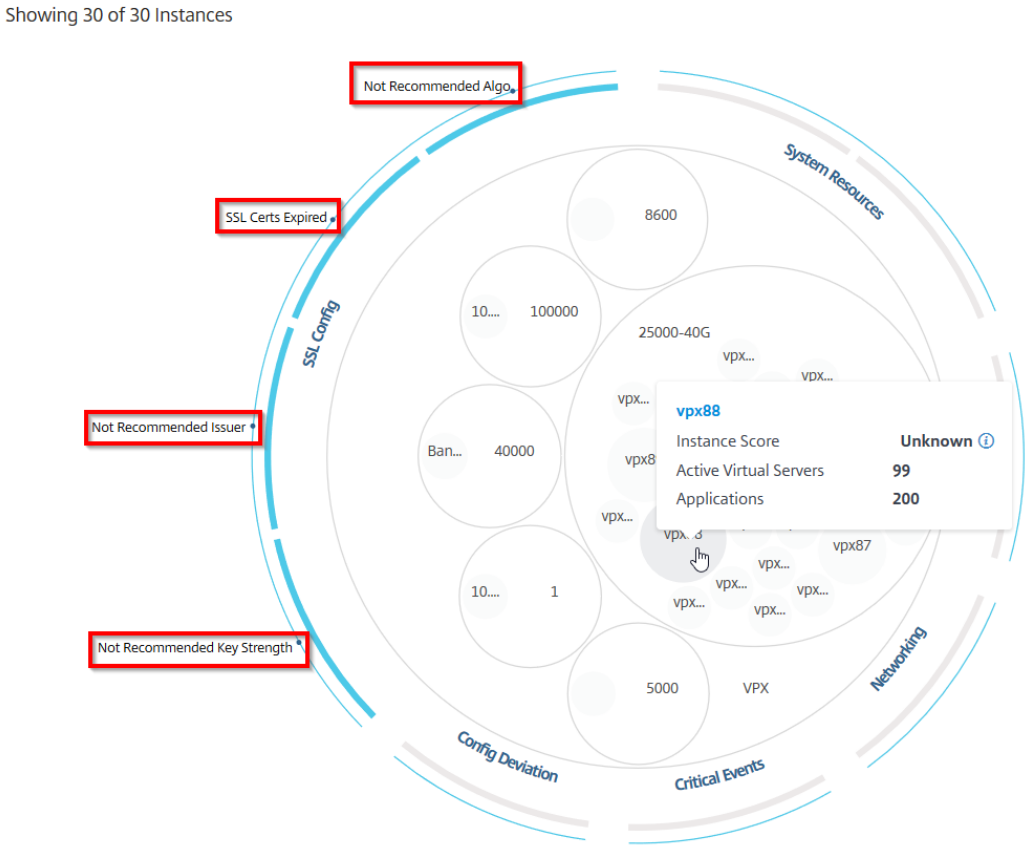


Site et version :



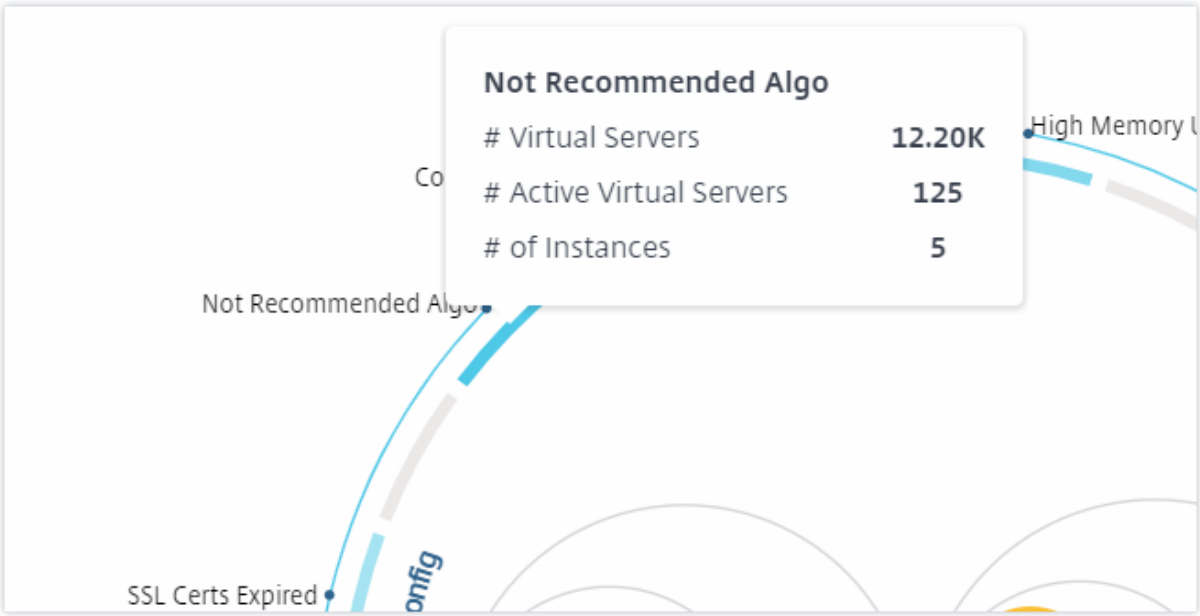
Comment utiliser Circle Pack

Cliquez sur chacun des cercles colorés pour mettre en surbrillance cette instance.



Selon les événements qui se sont produits dans ce cas, seuls ces indicateurs de santé sont mis en évidence dans les cercles extérieurs. Par exemple, les deux images suivantes du pack Circle affichent différents ensembles d'indicateurs de risque, bien que les deux instances soient dans un état critique.

Vous pouvez également cliquer sur les indicateurs de santé pour obtenir plus de détails sur le nombre d'instances qui ont signalé cet indicateur de risque. Par exemple, cliquez sur `Not recommended Algo` pour afficher le rapport récapitulatif de cet indicateur de risque.



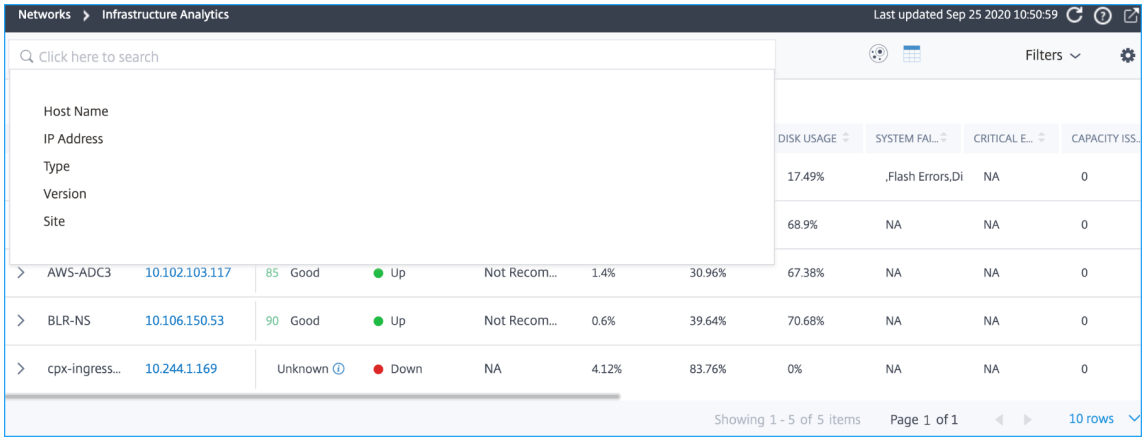
Vue tabulaire

La vue tabulaire affiche les instances et les détails de ces instances dans un format tabulaire. Pour de plus amples informations, consultez Détails de l'instance

Barre de recherche

Placez le curseur de la souris sur la barre de recherche et sélectionnez les attributs de recherche suivants pour filtrer les résultats :

- Nom d'hôte
- Adresse IP
- Type
- Version
- Site



Les résultats de la recherche fonctionnent à la fois pour la vue circulaire et la vue table.

Comment utiliser le panneau Récapitulatif

Le **panel de synthèse** vous aide efficacement et se concentre rapidement sur les cas nécessitant un examen ou un état critique. Le panneau est divisé en trois onglets : aperçu, informations sur l'instance et profil de trafic. Les modifications apportées dans ce panneau modifient l'affichage dans les formats Circle Pack et Tabulaire. Les sections suivantes décrivent ces onglets plus en détail. Les exemples des sections suivantes vous aident à utiliser efficacement les différents critères de sélection pour analyser les problèmes signalés par les instances.

Vue d'ensemble :

L'onglet **Vue d'ensemble** vous permet de surveiller les instances en fonction des erreurs matérielles, de l'utilisation, des certificats expirés et des indicateurs similaires qui peuvent se produire dans les instances. Les indicateurs que vous pouvez surveiller ici sont les suivants :

- Utilisation UC
- Utilisation de mémoire
- Utilisation du disque
- Pannes système
- Événements critiques
- Expiration des certificats SSL

Pour plus d'informations sur ces indicateurs, consultez *Indicateurs d'intégrité dans les instances de Citrix ADC*.

Les exemples suivants illustrent comment vous pouvez interagir avec le panneau **Vue d'ensemble** pour isoler les instances qui signalent des erreurs.

Exemple 1 : Afficher les instances qui sont dans un état de révision :

Activez la case à cocher Vérifier pour afficher uniquement les instances qui ne signalent pas d'erreurs critiques, mais qui nécessitent toujours une attention particulière.

Les histogrammes du panneau **Présentation** représentent un nombre agrégé d'instances basé sur une utilisation élevée de l'UC, une utilisation élevée de la mémoire et des événements d'utilisation élevée du disque. Les histogrammes sont classés à 10 %, 20 %, 30 %, 40 %, 50 %, 60 %, 70 %, 80 %, 90 % et 100 %. Placez le pointeur de la souris sur l'un des graphiques à barres. La légende en bas du graphique affiche la plage d'utilisation et le nombre d'instances dans cette plage. Vous pouvez également cliquer sur le graphique à barres pour afficher toutes les instances de cette plage.

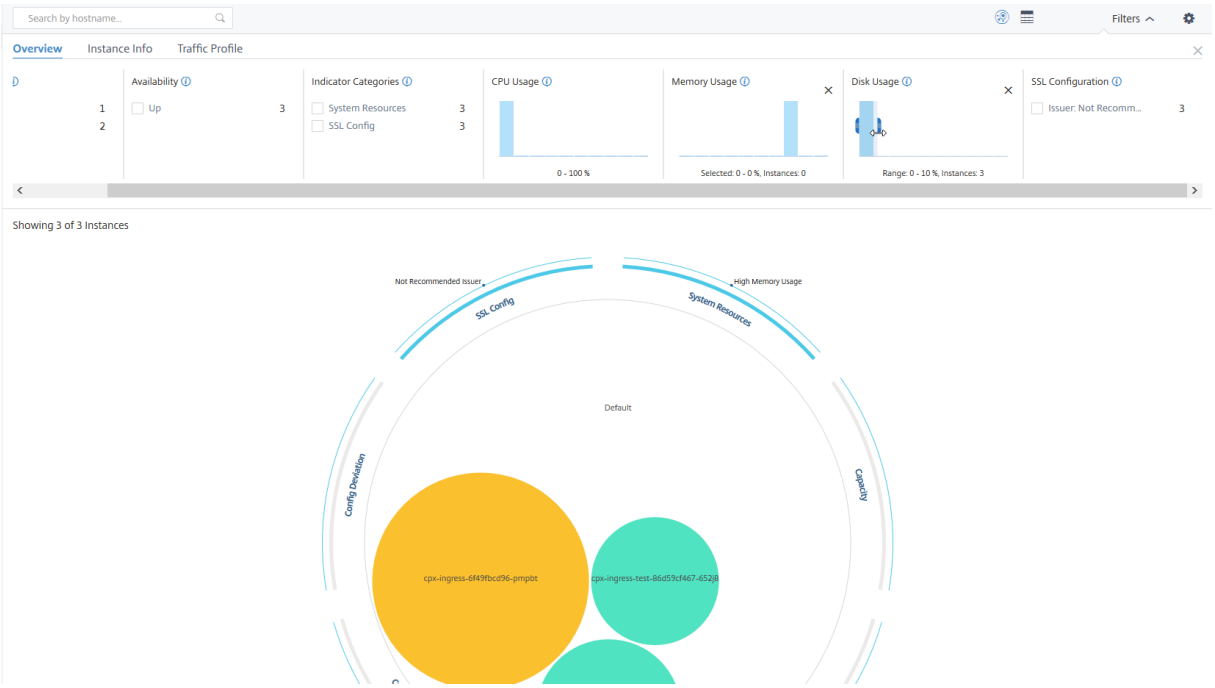
Exemple 2 : Afficher les instances qui consomment entre 10 % et 20 % de la mémoire allouée :

Dans la section Utilisation de la mémoire, cliquez sur le graphique à barres. La légende montre que la plage sélectionnée est de 10 à 20 % et que 29 instances fonctionnent dans cette plage.

Vous pouvez également sélectionner plusieurs plages dans ces histogrammes.

Exemple 3 : Afficher les instances qui consomment de l'espace disque dans plusieurs plages :

Pour afficher les instances qui ont consommé de la mémoire entre 0 % et 10 % d'espace disque, faites glisser le pointeur de la souris sur les deux plages, comme indiqué dans l'image suivante.



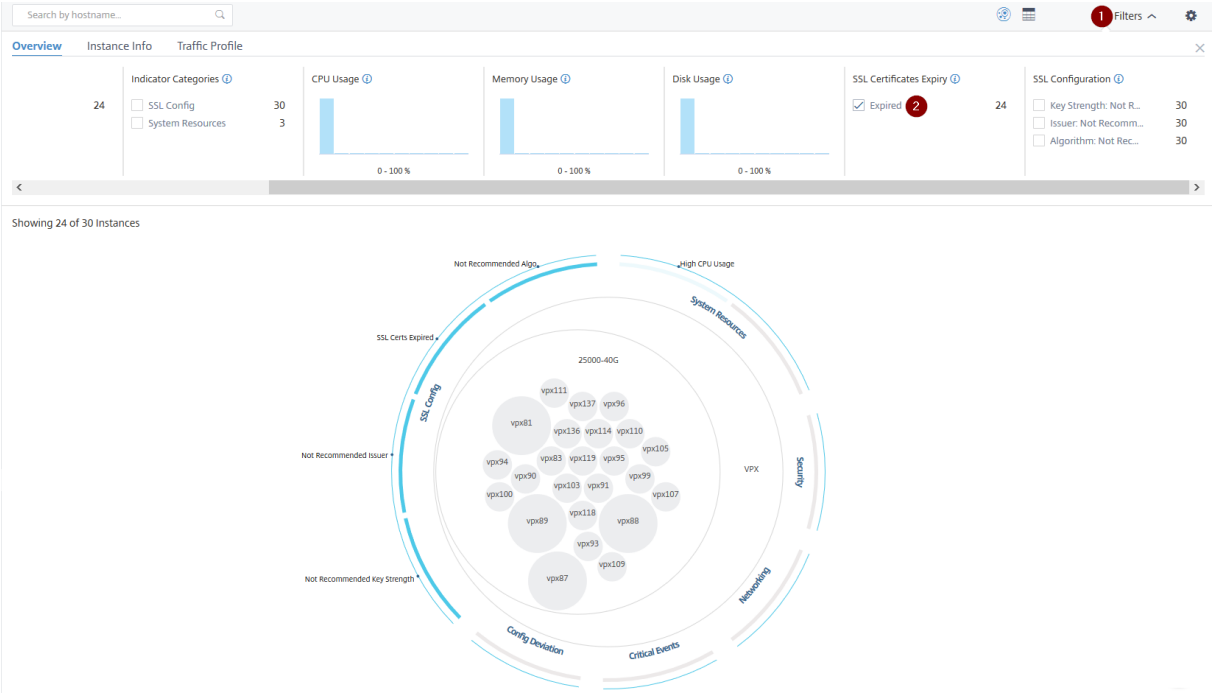
> **Remarque**
>
> Cliquez sur « X » pour supprimer la sélection. Vous pouvez également cliquer sur **Réinitialiser** pour supprimer plusieurs sélections.

Les graphiques à barres horizontales du panneau **Présentation** indiquent le nombre d'instances signalant des erreurs système, des événements critiques et l'état d'expiration des certificats SSL. Activez

la case à cocher pour afficher ces instances.

Exemple 4 : Afficher les instances pour les certificats SSL expirés :

Dans la section **Expiration des certificats SSL**, activez la case à cocher **Expiré** pour afficher les trois instances.



1 - Cliquez sur la liste **Filtre**.

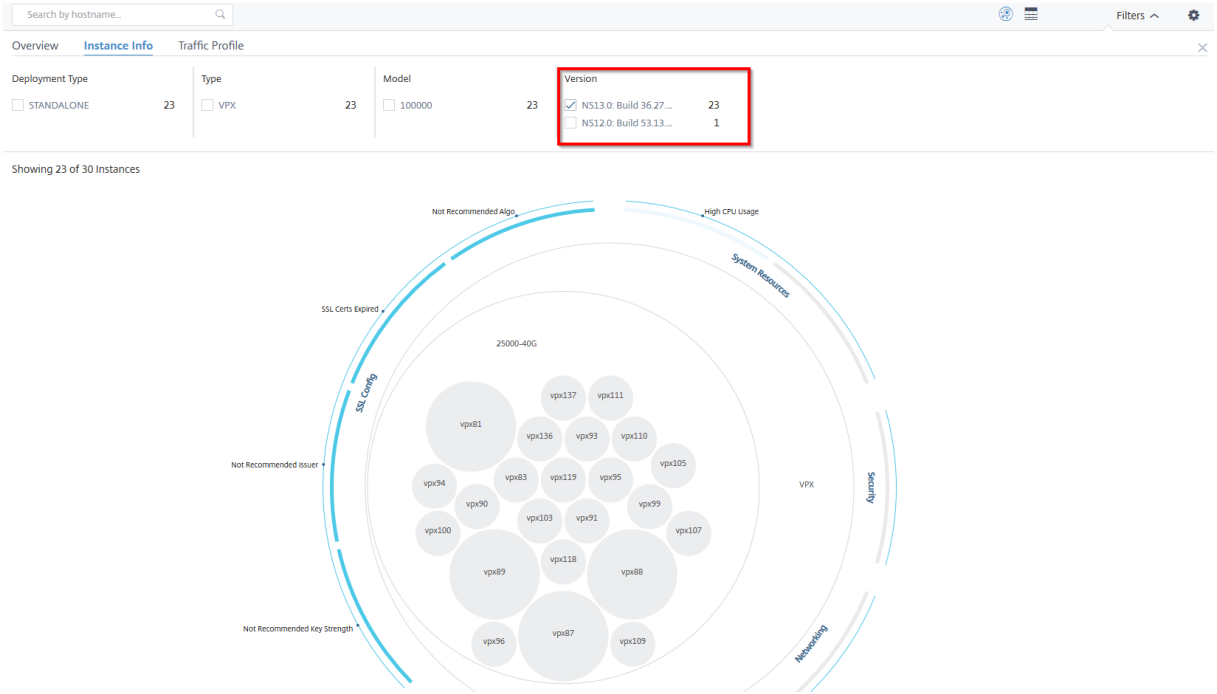
2 - Dans la section **Expiration des certificats SSL**, activez la case à cocher **Expiré** pour afficher les instances.

Infos sur l'instance

Le panneau **Informations sur l'instance** vous permet d'afficher les instances en fonction du type de déploiement, du type d'instance, du modèle et de la version du logiciel. Vous pouvez sélectionner plusieurs cases à cocher pour affiner votre sélection.

Exemple 5 : Afficher les instances VPX ADC avec un numéro de build spécifique :

Sélectionnez la version à afficher.

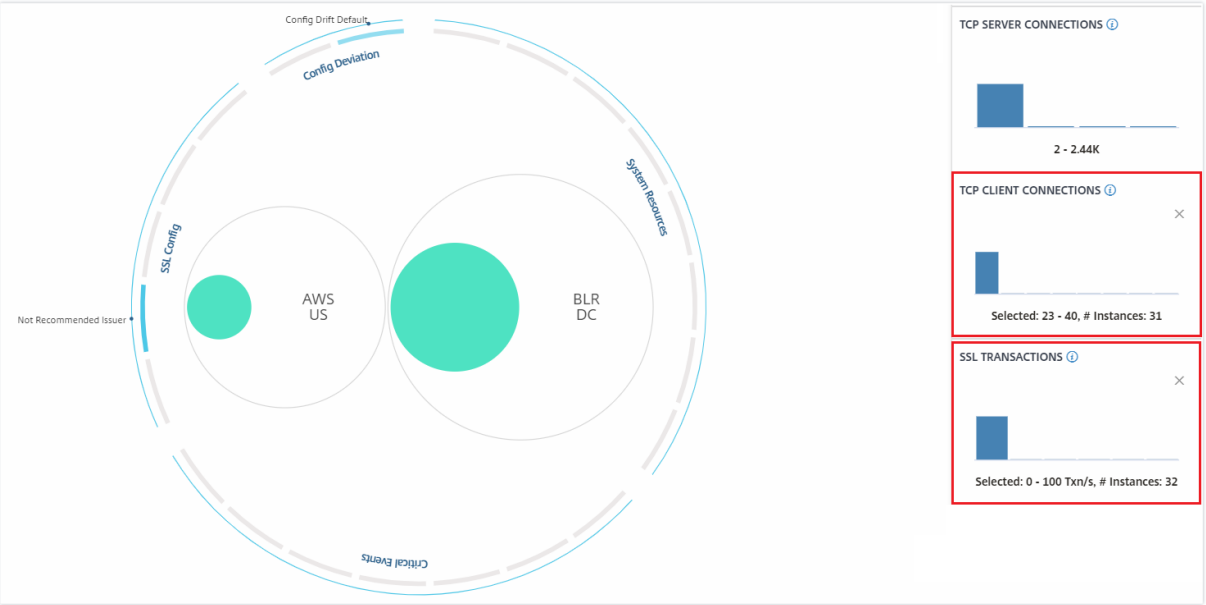


Profil du trafic

Les Histogrammes du panneau **Profil de trafic** représentent un nombre agrégé d'instances en fonction du débit sous licence des instances, du nombre de demandes, de connexions et de transactions traitées par les instances. Sélectionnez le graphique à barres pour afficher les instances dans cette plage.

Exemple 6 : Afficher les instances prenant en charge les connexions TCP :

L'image suivante montre le nombre d'instances prenant en charge les connexions TCP entre 23 et 40, ainsi que le traitement jusqu'à 100 transactions SSL par seconde.

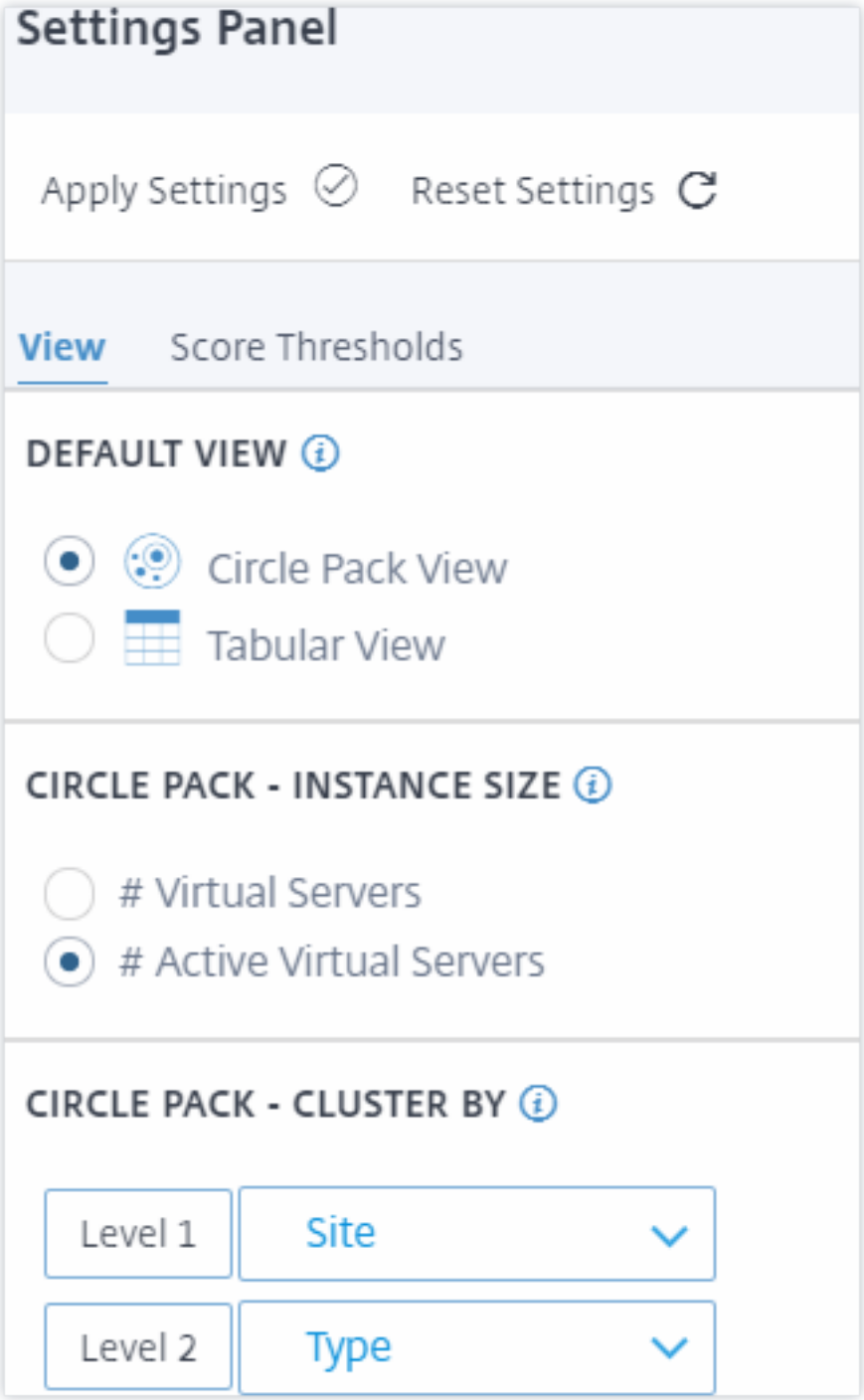


Comment utiliser le panneau des paramètres

Le panneau **Paramètres** vous permet de définir l'affichage par défaut de l'Analyse de l'infrastructure. Il vous permet également de définir les valeurs de seuil bas et élevé pour une utilisation élevée du processeur, une utilisation élevée du disque et une utilisation élevée de la mémoire. Le panneau des paramètres est divisé en deux onglets : Afficher et Score Seuils.

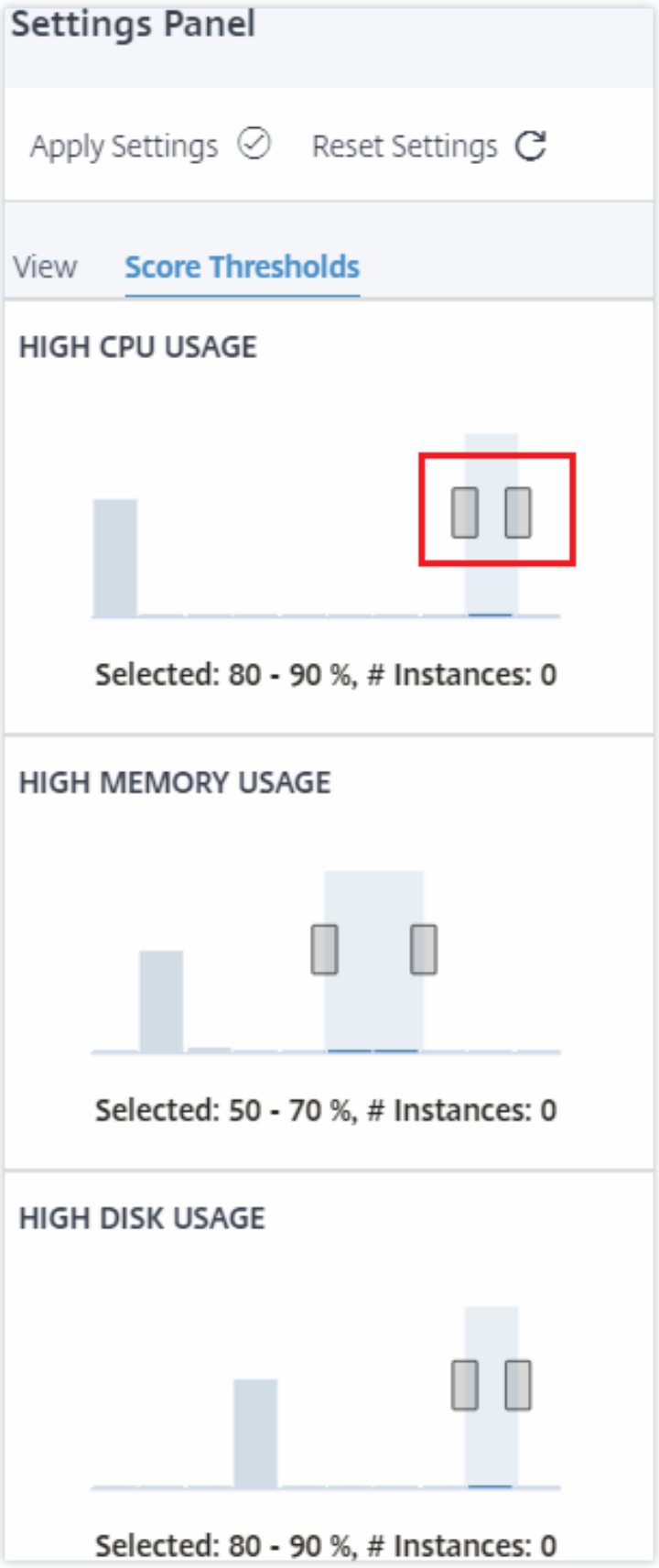
View

- **Vue par défaut**. Sélectionnez **Circle Pack** ou Tabulaire comme affichage par défaut sur la page d'analyse. Le format que vous sélectionnez correspond à ce que vous voyez lorsque vous accédez à la page dans Citrix ADM.
- **Circle Pack - Taille de l'instance**. Autorisez la taille du cercle d'instance sur le nombre de serveurs virtuels ou le nombre de serveurs virtuels actifs.
- **Circle Pack - Cluster By**. Décidez de l'agrégation à deux niveaux des cercles d'instance. Pour plus d'informations sur la mise en cluster d'instances, reportez-vous à la sectionCercles d'instance en cluster.



Seuils de score

Vous pouvez modifier les valeurs de seuil bas et élevé pour une utilisation élevée du processeur, de la mémoire et du disque en fonction des besoins de trafic dans votre organisation. Faites glisser les poignées de chaque histogramme de sélection pour définir les valeurs.



> **Remarque**
>
> Cliquez sur **Appliquer les paramètres**pour appliquer ces modifications ou cliquez sur **Réinitialiser**pour supprimer toutes les modifications.

Comment visualiser les données sur le tableau de bord

Grâce à Infrastructure Analytics, les administrateurs réseau peuvent désormais identifier les instances nécessitant le plus d'attention en quelques secondes. Pour comprendre cela plus en détail, considérons le cas de Chris, un administrateur réseau de ExampleCompany.

Chris gère de nombreuses instances de Citrix ADC dans son organisation. Quelques-unes des instances traitent un trafic élevé, et il doit les surveiller de près. Il remarque que quelques instances à fort trafic ne traitent plus la totalité du trafic qui les traverse. Pour analyser cette réduction, plus tôt, il a dû lire plusieurs rapports de données provenant de diverses sources. Chris a dû passer plus de temps à essayer de corréler les données manuellement et à déterminer quelles instances ne sont pas dans un état optimal et nécessitent une attention particulière. Il utilise la fonctionnalité Analyse de l'infrastructure pour voir visuellement l'état de toutes les instances.

Les deux exemples suivants illustrent comment Infrastructure Analytics aide Chris dans ses activités de maintenance :

Exemple 1 - Pour surveiller le trafic SSL :

Chris remarque sur le Circle Pack qu'une instance a un score d'instance faible et que cette instance est dans l'état « Critique ». Il clique sur l'instance pour voir quel est le problème. Le résumé de l'instance indique qu'il y a une défaillance de carte SSL sur cette instance et que cette instance ne peut donc pas traiter le trafic SSL (le trafic SSL a été réduit). Chris extrait cette information et envoie un rapport à l'équipe pour qu'elle examine immédiatement le problème.

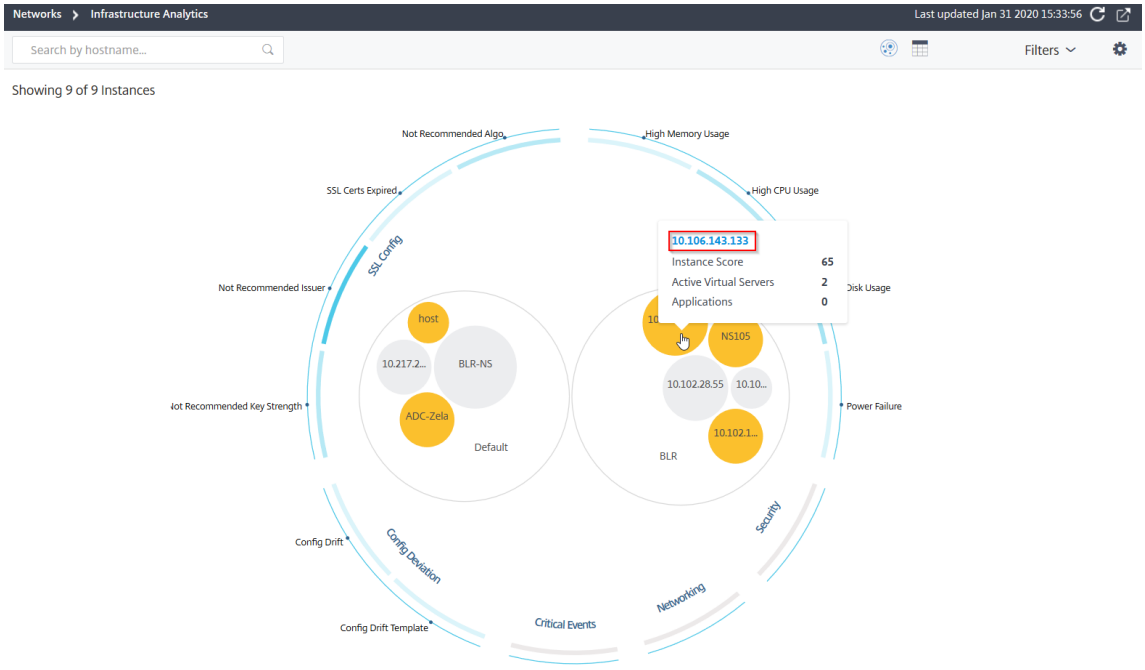
Exemple 2 - Pour surveiller les modifications de configuration :

Chris remarque également qu'une autre instance est dans l'état « Review » et qu'il y a eu un écart de configuration récemment. Lorsqu'il clique sur l'indicateur de risque de déviation de configuration, il remarque que des modifications de configuration liées à RC4 Cipher, SSL v3, TLS 1.0 et TLS 1.1 ont été apportées, ce qui peut être dû à des problèmes de sécurité. Il remarque également que le profil de trafic de transaction SSL pour cette instance est tombé en panne. Il exporte ce rapport et l'envoie à l'administrateur pour en savoir plus.

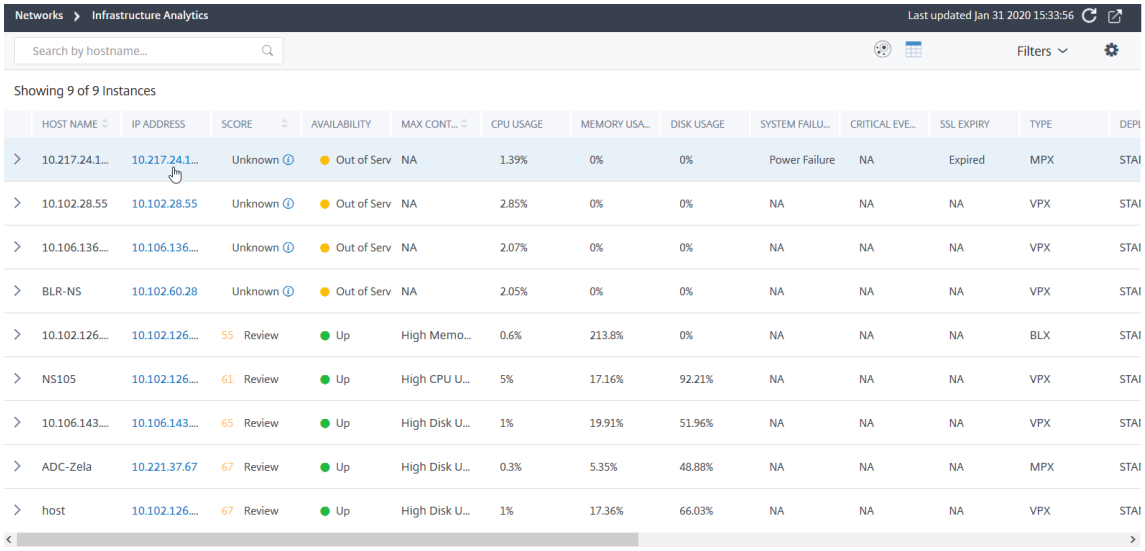
Afficher les détails de l'instance dans Infrastructure Analytics

April 29, 2021

1. Accédez à **Réseaux** > **Analyse de l'infrastructure**
2. Cliquez sur la vue du pack de cercle et sélectionnez l'adresse IP.



Vous pouvez également cliquer sur une adresse IP dans la vue tableau.

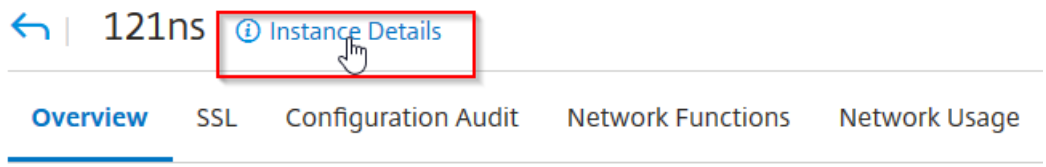


- **Nom d'hôte** — Indique le nom d'hôte attribué à l'instance ADC
- **Adresse IP** — Indique l'adresse IP de l'instance ADC
- **Score** — Indique le score de l'instance ADC et le statut (Critical, Good et Fair)
- **Disponibilité** : indique l'état actuel de l'instance ADC, par exemple, ****Désout**ou Absence de service**.

- **Contribution maximale** : indique la catégorie de problème pour laquelle l'instance ADC a le nombre maximal d'erreurs.
- **Utilisation du processeur** — Indique le pourcentage CPU% actuel utilisé par l'instance
- **Utilisation de la mémoire** — Indique la mémoire actuelle utilisée par l'instance
- **Utilisation du disque** — Indique le pourcentage de disque actuel utilisé par l'instance
- **Défaillance du système** : indique le nombre total d'erreurs pour le système d'instance
- **Evénements critiques** : indique la catégorie d'événement dans laquelle l'instance Citrix ADC a le maximum d'événements
- **Expiration SSL** — Indique l'état actuel du certificat SSL installé sur l'instance ADC
- **Type** : indique le type d'instance ADC tel que VPX, SDX, MPX ou CPX
- **Déploiement** : indique si l'instance ADC est déployée en tant qu'instance autonome ou paire HA
- **Modèle** — Indique le numéro de modèle de l'instance ADC
- **Version** — Indique la version de l'instance ADC et le numéro de build
- **Débit** : indique le débit réseau actuel de l'instance ADC
- **Request/sec HTTPS** — Indique les demandes HTTPS en cours reçues par l'instance ADC
- **Connexion TCP** — Indique les connexions TCP actuelles établies
- **Transaction SSL** — Indique les transactions SSL actuelles traitées par l'instance ADC
- **Site** : indique le nom du site sur lequel l'instance ADC est déployée.

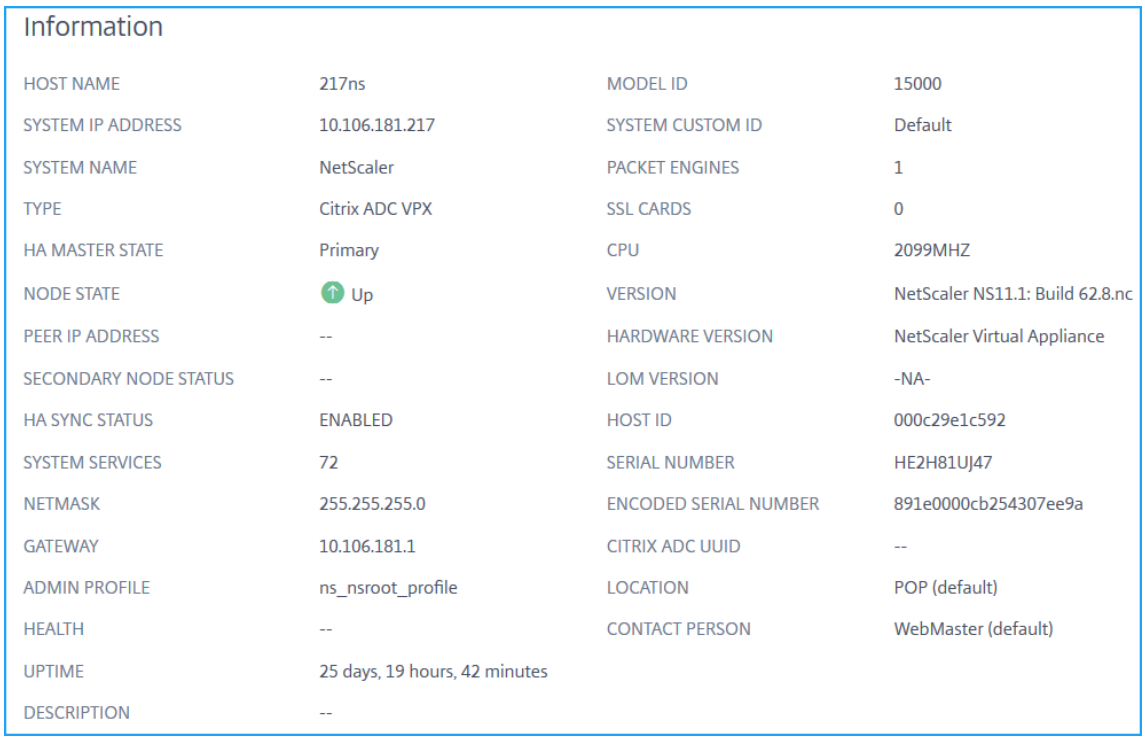
> **Remarque**
>
> Pour toutes les 5 minutes, les valeurs actuelles pour l'utilisation du processeur, l'utilisation de la mémoire, l'utilisation du disque, le débit, etc. sont mises à jour.

Cliquez sur **Détails de l'instance** pour afficher les détails.

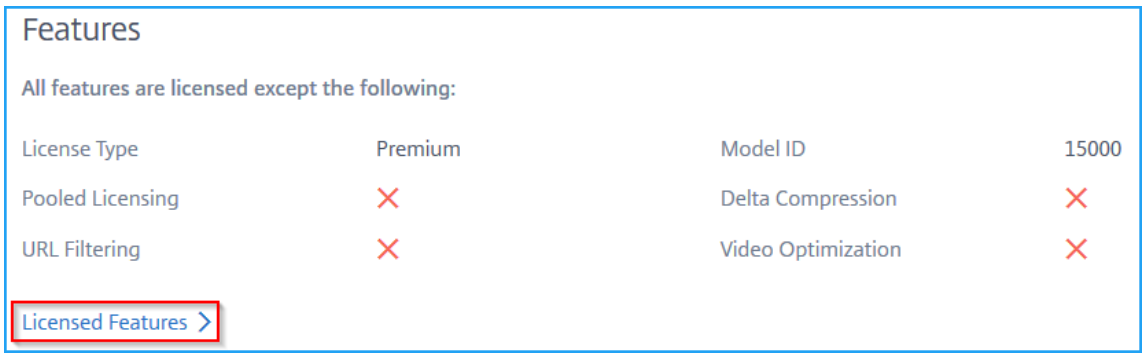


Les détails suivants s'affichent :

- **Informations** : détails d'instance tels que le type d'instance, le type de déploiement, la version, le modèle, etc.



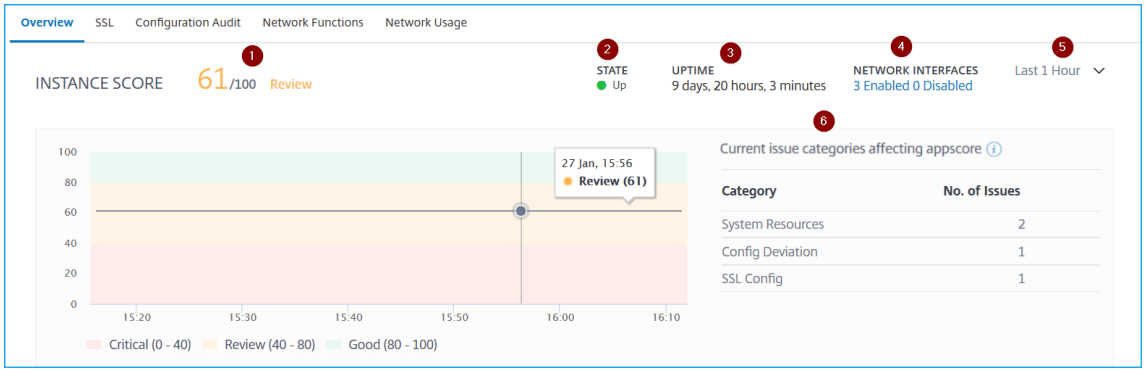
- **Fonctionnalités** : par défaut, les fonctionnalités qui ne sont pas sous licence sont affichées. Cliquez sur **Fonctionnalités sous licence** pour afficher les fonctionnalités sous licence.



- **Modes** : par défaut, tous les modes désactivés sur l'instance sont affichés. Cliquez sur **Afficher les modes activés** pour afficher les modes activés sur l'instance.

Le tableau de bord de l'instance présente une vue d'ensemble de l'instance dans laquelle vous pouvez voir les détails suivants :

- **Score d'instance**

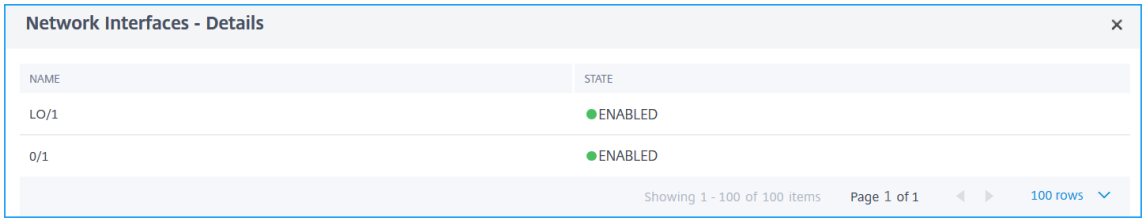


1 — Indique le score d'instance Citrix ADC actuel pour la durée sélectionnée. Le score final est calculé comme **100 moins les pénalités totales**. Le graphique affiche les plages de score pour la durée sélectionnée.

2 — Indique l'état actuel de l'instance Citrix ADC, par exemple En **haut**, **en bas**et **hors service**.

3 — Indique la durée pendant laquelle l'instance de Citrix ADC est en cours d'exécution.

4 — Indique le nombre total d'interfaces réseau activées et désactivées pour l'instance. Cliquez pour afficher les détails tels que le nom de l'interface réseau et l'état (activé ou désactivé).



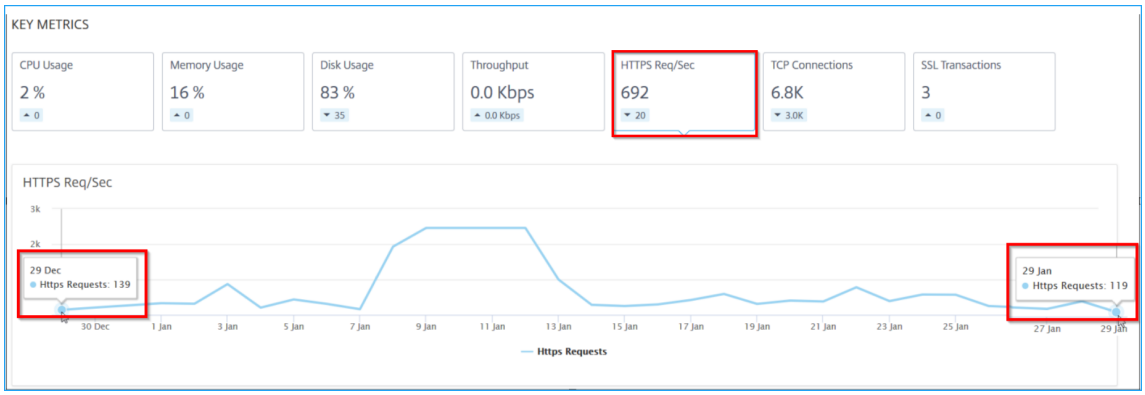
5 — Sélectionnez la durée dans la liste pour afficher les détails de l'instance.

6 — Affiche le nombre total de problèmes et la catégorie de problèmes de l'instance ADC.

- **Principales mesures**

  Cliquez sur chaque onglet pour afficher les détails. Dans chaque mesure, vous pouvez afficher la valeur moyenne et la valeur de différence pour l'heure sélectionnée.

  L'image suivante est un exemple pour HTTPS Req/Sec et la durée sélectionnée est de 1 heure. La valeur **692** est la moyenne HTTPS Req/sec pour la durée d'un mois et la valeur **20** est la valeur de différence. Dans le graphique, la première valeur est **139** et la dernière valeur est **119**. La valeur de la différence est **139 — 119 = 20**.



  Vous pouvez afficher les mesures d'instance suivantes dans un format graphique pour la durée sélectionnée :

  - **Utilisation de l'UC — % de CPU** moyen de l'instance pour la durée sélectionnée (s'affiche à la fois pour l'UC du paquet et pour l'UC de gestion).
  - **Utilisation de la mémoire** : % d'utilisation moyenne de la mémoire de l'instance pour la durée sélectionnée.
  - **Utilisation du disque** : en% d'espace disque moyen de l'instance pour la durée sélectionnée.
  - **Débit : débit** réseau moyen traité par l'instance pour la durée sélectionnée.
  - **Request/sec HTTPS** — Nombre moyen de demandes HTTPS reçues par l'instance pour la durée sélectionnée.

- Connexions**TCP : connexions** TCP moyennes établies par le client et le serveur pour la durée sélectionnée.
- **Transactions SSL — Transactions** SSL moyennes traitées par l'instance pour la durée sélectionnée.

- **Problèmes**

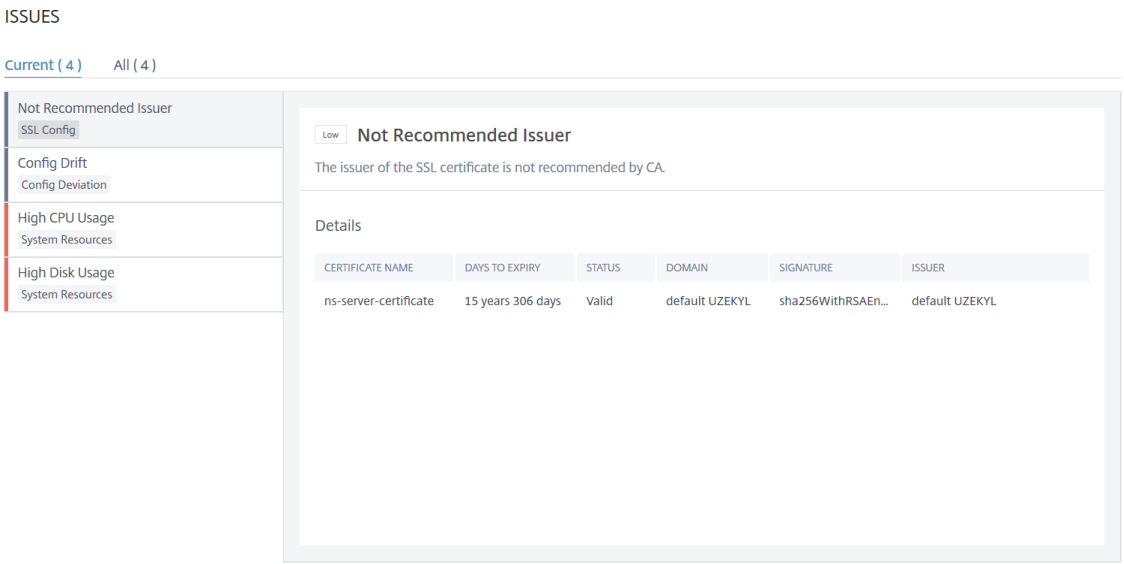
  Vous pouvez afficher les problèmes suivants qui se produisent dans l'instance de Citrix ADC :

Catégorie de problème	Description	Problèmes
Ressources système	Affiche tous les problèmes liés à la ressource système Citrix ADC tels que le processeur, la mémoire, l'utilisation du disque, etc.	- Utilisation élevée du processeur
		- Utilisation élevée de la mémoire
		- Utilisation élevée du disque
		- Échec de la carte SSL
		- Panne de courant
		- Erreur de disque
		- Erreur Flash
		- Rejets de carte réseau
Configuration SSL	Affiche tous les problèmes liés à la configuration SSL sur l'instance de Citrix ADC.	- Certs SSL expirés
		- Émetteur non recommandé
		- Non recommandé Algo
		- Résistance de la clé non recommandée
Déviation de configuration	Affiche tous les problèmes liés aux tâches de configuration appliquées dans l'instance Citrix ADC.	- Config Drift
		- Running vs Template

Catégorie de problème	Description	Problèmes
Événements critiques	Affiche tous les événements critiques liés aux instances Citrix ADC configurées dans la paire HA et dans Cluster.	- Échec de propriété du cluster
		- Échec de la synchronisation du cluster
		- Les versions de cluster sont incompatibles
		- HA Bad Sec état
		- HA Pas de battements de chaleur
		- Échec de synchronisation HA
		- Incompatibilité de la version HA
Problèmes de capacité	Affiche les problèmes de capacité ADC. L'ADM interroge ces événements toutes les cinq minutes à partir de l'instance ADC et affiche les baisses de paquets ou les incréments de compteur de limite de vitesse s'il existe. Les problèmes sont classés en fonction des paramètres de capacité suivants.	- Limite de débit atteinte
		- Limite du processeur PE atteinte
		- Limite PPS atteinte
		- Limite de débit SSL
		- Limite de débit SSL TPS

Catégorie de problème	Description	Problèmes
Mise en réseau	Affiche les problèmes opérationnels qui se produisent dans les instances.	Pour de plus amples informations, consultez la section Analyse de l'infrastructure améliorée avec de nouveaux indicateurs.

Cliquez sur chaque onglet pour analyser et résoudre le problème. Par exemple, considérez qu'une instance présente les erreurs suivantes pour la durée sélectionnée :



- L'onglet **Courant** affiche les problèmes qui affectent actuellement le score d'instance.
- L'onglet **Tout** affiche tous les problèmes infra détectés pour la durée sélectionnée.

Afficher les problèmes de capacité dans une instance ADC

April 29, 2021

Lorsqu'une instance ADC a consommé la plus grande partie de sa capacité disponible, la suppression de paquets peut se produire lors du traitement du trafic client. Ce problème provoque de faibles performances dans une instance ADC. En comprenant ces problèmes de capacité ADC, vous pouvez allouer de manière proactive des licences supplémentaires afin de stabiliser les performances de ADC.

Dans la **vue Circle Pack**, vous pouvez afficher les problèmes de capacité d'instance ADC s'il existe.

Pour afficher les problèmes de capacité de l'ADC,

1. Accédez à **Réseaux > Analyse de l'infrastructure**.
2. Sélectionnez la vue du pack de cercles.

L'illustration suivante suggère que les problèmes de capacité existent dans l'instance sélectionnée :

Les problèmes sont classés selon les paramètres de capacité suivants :

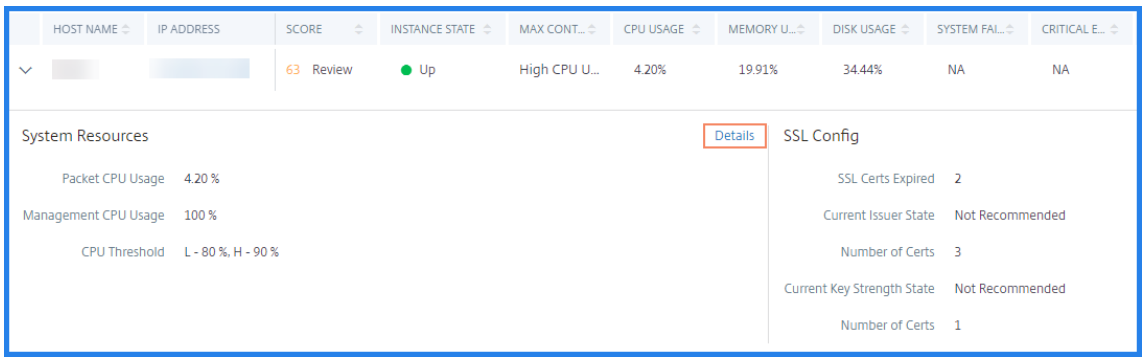
- **Limite de débit atteinte** : nombre de paquets abandonnés dans l'instance après que la limite de débit est atteinte.
- **Limite de CPU PE atteinte** : nombre de paquets abandonnés sur toutes les cartes réseau après que la limite de CPU PE est atteinte.
- **Limite PPS atteinte** : nombre de paquets abandonnés dans l'instance après que la limite PPS est atteinte.
- **Limite de débit SSL** : nombre de fois que la limite de débit SSL est atteinte.
- **Limite de taux TPS SSL** : Nombre de fois que la limite TPS SSL a été atteinte.

Afficher les actions recommandées pour résoudre les problèmes de capacité

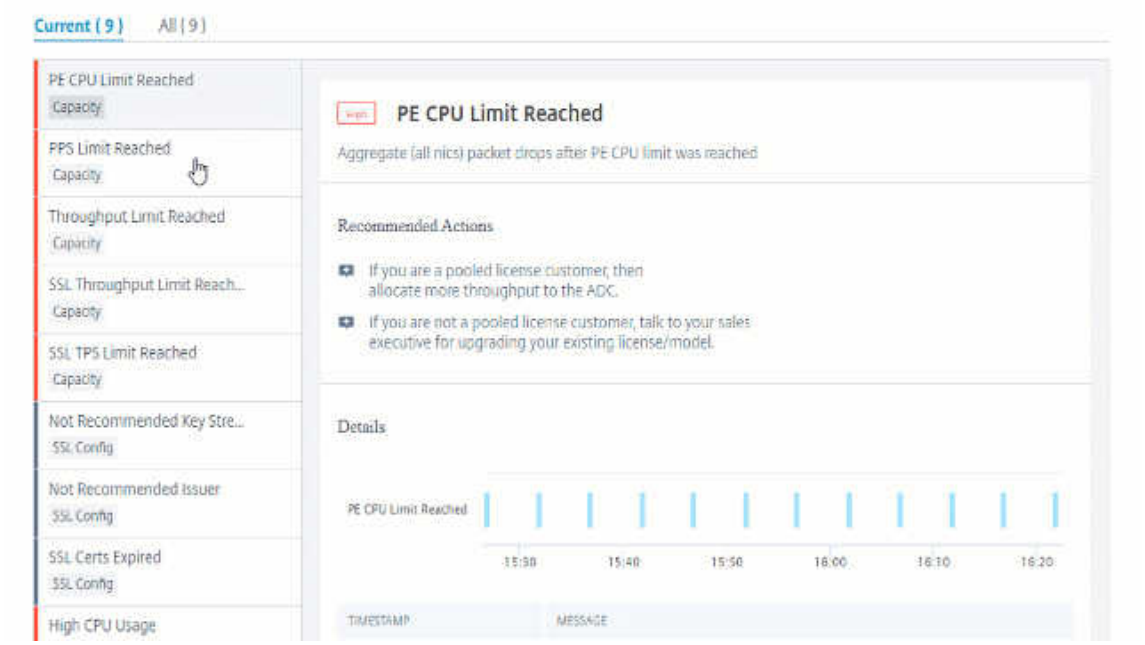
ADM recommande des mesures qui peuvent résoudre les problèmes de capacité. Pour afficher les actions recommandées, effectuez les opérations suivantes :

1. Dans **Réseaux > Analyse de l'infrastructure**, sélectionnez la vue tabulaire.

2. Sélectionnez l'instance qui présente des problèmes de capacité et cliquez sur **Détails**.



3. Dans la page de l'instance, faites défiler jusqu'à la section **Problèmes**.
4. Sélectionnez chaque problème et affichez les actions recommandées pour résoudre les problèmes de capacité.



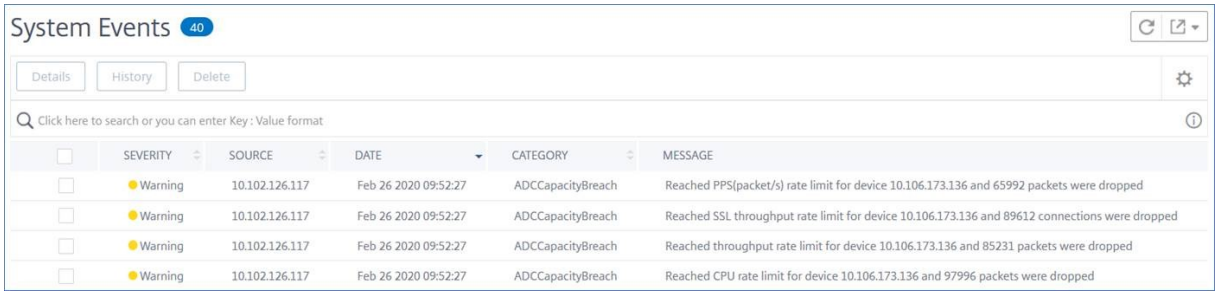
L'ADM interroge ces événements toutes les cinq minutes à partir de l'instance ADC et affiche les baisses de paquets ou les incréments de compteur de limite de vitesse s'il existe.

L'ADM calcule le score d'instance sur le seuil de capacité défini.

- **Seuil bas** — 1 incrément de dépassement de paquets ou de compteur de limite de taux
- **Seuil élevé** : 10000 paquets baisse ou incrément du compteur de limite de taux

Par conséquent, lorsqu'une instance ADC dépasse le seuil de capacité, le score d'instance est affecté.

Lorsque les paquets diminuent ou que le compteur de limite de vitesse s'incrémente, un événement est généré sous la catégorie `ADCCapacityBreach`. Pour afficher ces événements, accédez à **Comptes > Événements système**.



Analyse de l'infrastructure améliorée avec de nouveaux indicateurs

April 29, 2021

À l'aide de Citrix ADM **Infrastructure Analytics**, vous pouvez :

- Afficher un nouvel ensemble de problèmes opérationnels qui se produisent dans les instances de Citrix ADC.
- Affichez les messages d'erreur et vérifiez les recommandations pour résoudre les problèmes.

En tant qu'administrateur, vous pouvez rapidement identifier l'analyse de la cause première des problèmes.

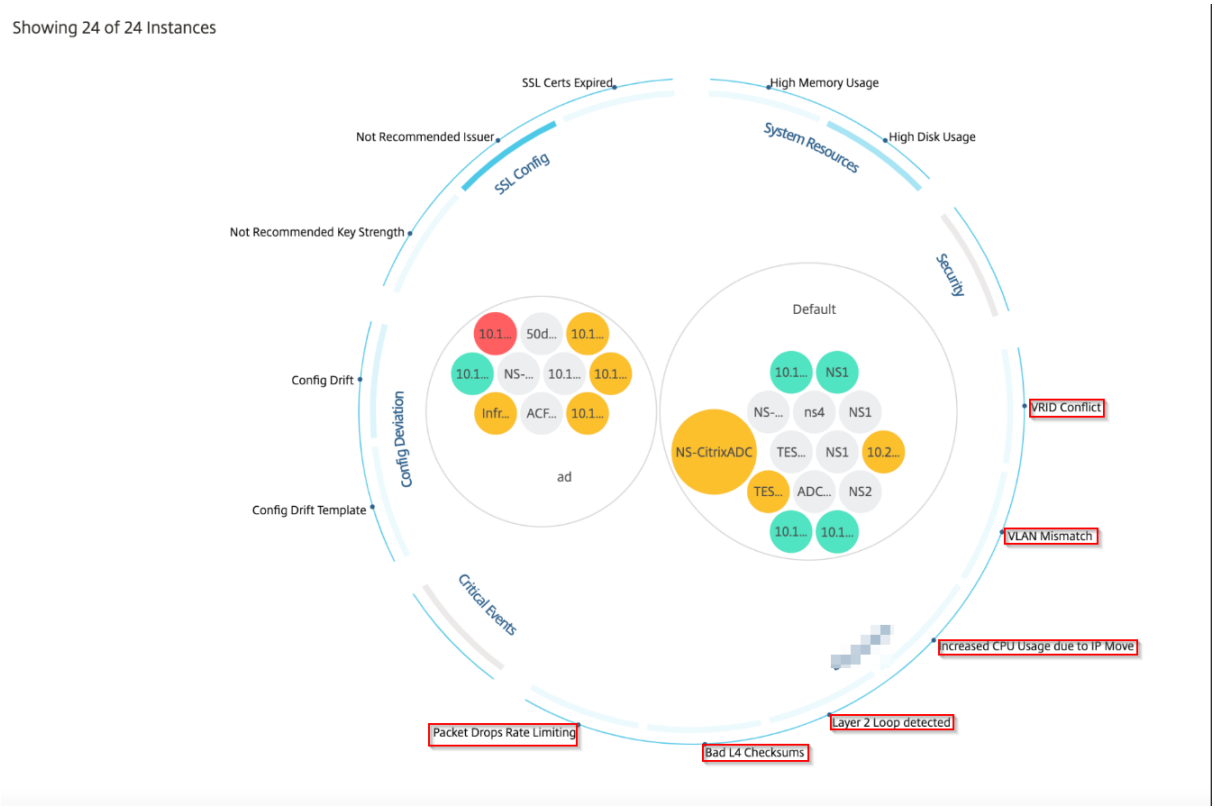
> **Remarque**
>
> Les indicateurs de règle ne sont pas pris en charge pour :
>
> - Instances Citrix ADC configurées en mode cluster.
> - Instances Citrix ADC configurées avec des partitions d'administration.

Dans Citrix ADM, accédez à **Réseaux** > **Analyse de l'infrastructure** pour afficher les indicateurs suivants :

Nom de l'indicateur dans Infrastructure Analytics	Description
Échec de l'allocation de port	Détecte lorsque Citrix ADC utilise SNIP pour communiquer avec une nouvelle connexion serveur et que le total des ports disponibles sur ce SNIP sont épuisés. L'action recommandée consiste à ajouter un autre SNIP dans le même sous-réseau.
Construction de session	Détecte quand la mémoire Citrix ADC est maintenue par des sessions SSL.

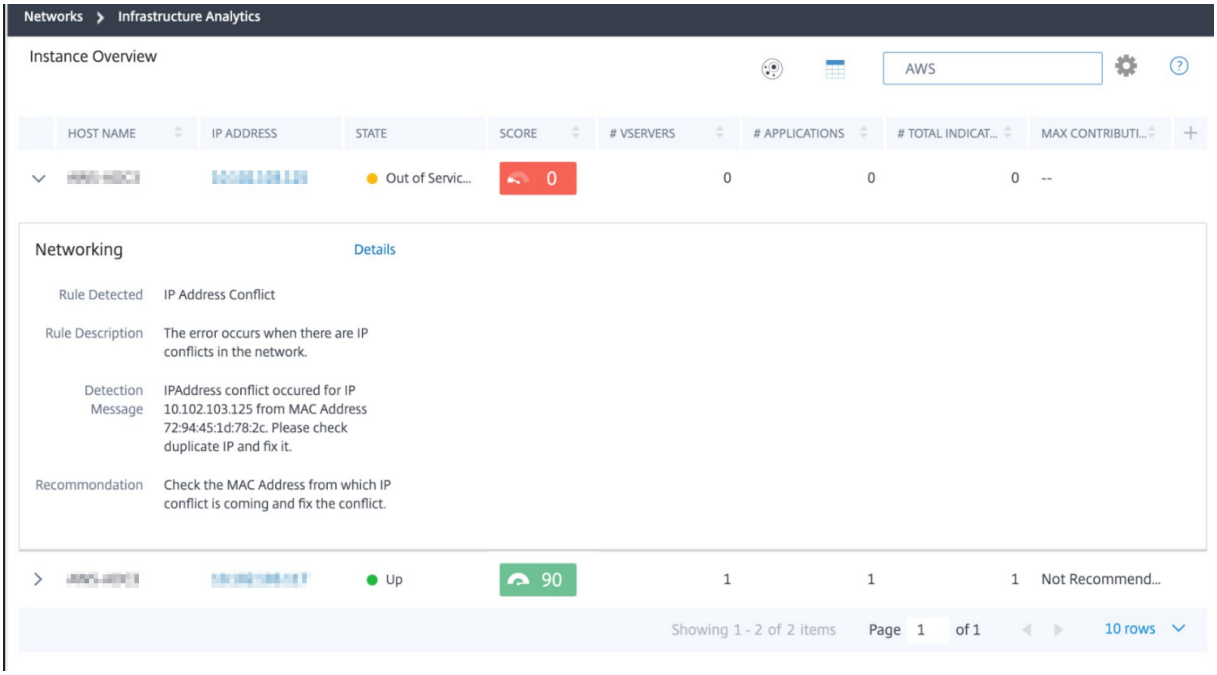
Nom de l'indicateur dans Infrastructure Analytics	Description
Aucune configuration d'itinéraire par défaut	Détecte quand le trafic est abandonné en raison de la non-disponibilité des routes.
Conflit de propriété intellectuelle	Détecte si une même adresse IP est configurée ou appliquée sur deux ou plusieurs instances d'un réseau.
Conflit VRID	Détecte les problèmes d'accès intermittent pour le VRID spécifié.
Inadéquation du VLAN	Détecte si des erreurs se produisent pendant la configuration du VLAN lié aux sous-réseaux IP.
Attaque de petite fenêtre TCP	Détecte lorsqu'il y a une éventuelle attaque de petite fenêtre en cours. Cette alerte est juste à titre informatif, car ADC atténue déjà cette attaque.
Seuil de contrôle du taux	Détecte lorsque les paquets sont supprimés en fonction du seuil de contrôle de débit configuré.
Limite de persistance	Détecte lorsque des hits maximums sont imposés à la mémoire Citrix ADC.
Incompatibilité du nom de site GSLB	Détecte lorsque des échecs de synchronisation de la configuration GSLB se produisent en raison d'une incompatibilité de nom de site.
En-tête IP mal formé	Détecte l'échec des contrôles de santé sur les paquets IPv4.
Mauvaises sommes de contrôle L4	Détecte l'échec de la validation de somme de contrôle pour les paquets TCP.
Augmentation de l'utilisation du processeur en raison du déplacement d'IP	Détecte si un grand nombre de Mac doivent être mis à jour.
Direction excessive des paquets	Détecte les niveaux élevés de direction des paquets logiciels en raison de l'utilisation du type de clé rss asymétrique.
Boucle de couche 2	Détecte la présence de boucles de couche 2 dans le réseau.

Nom de l'indicateur dans Infrastructure Analytics	Description
Tagged VLAN mismatch	Détecte lorsque des paquets VLAN balisés sont reçus sur une interface non balisée.



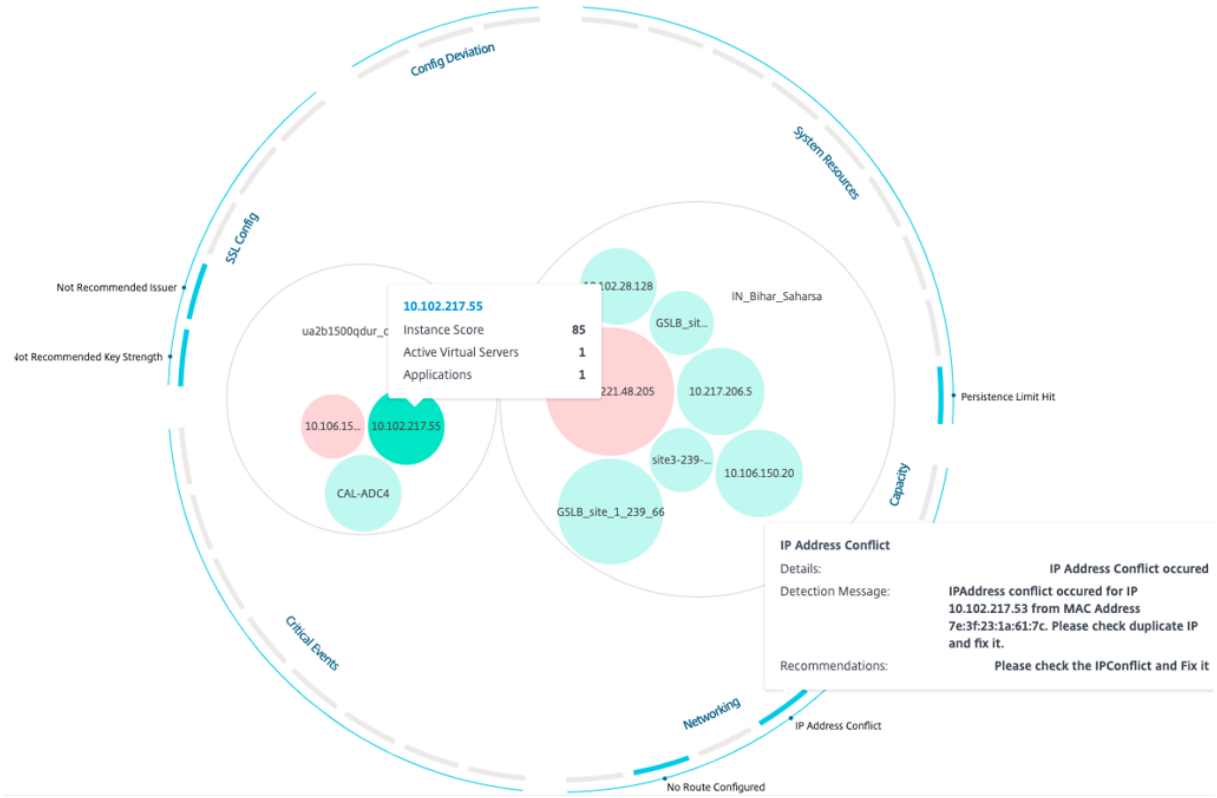
Vue tabulaire

Vous pouvez également afficher les anomalies à l'aide de l'option Vue tabulaire dans **Infrastructure Analytics**. Accédez à **Réseaux** > **Analyse de l'infrastructure**, puis cliquez sur pour afficher toutes les instances gérées. Cliquez › pour développer pour plus de détails.



Afficher les détails d'une anomalie

Par exemple, si vous souhaitez afficher les détails du **conflit d'adresses IP** dans le réseau, cliquez sur l'anomalie affichée pour le conflit d'adresses IP.



- **Détails** - Indique quelle anomalie est détectée
- **Message de détection** - Indique l'adresse MAC pour laquelle l'adresse IP a le conflit
- **Recommandations** - Indique la procédure de dépannage pour résoudre ce conflit d'adresse IP

Articles pratiques

April 29, 2021

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

Cliquez sur un nom de fonctionnalité dans le tableau suivant pour afficher la liste des articles de procédure pour cette fonctionnalité.

SUJETS		
Gestion des instances	Gestion de la configuration	Gestion des certificats
StyleBooks	Gestion des événements	

Gestion des instances

Comment surveiller les sites distribués à l'échelle mondiale

Comment gérer les partitions d'administration des instances de Citrix ADC

Comment ajouter des instances à Citrix ADM

Comment créer des groupes d'instances sur Citrix ADM

Procédure d'interrogation des instances et entités Citrix ADC dans Citrix ADM

Comment configurer des sites pour les géomaps dans Citrix ADM

Comment faire pour forcer un basculement vers l'instance secondaire de Citrix ADC

Comment faire pour forcer une instance Citrix ADC secondaire à rester secondaire

Comment modifier un mot de passe racine Citrix ADC MPX ou VPX

Comment modifier un mot de passe racine Citrix ADC SDX

Gestion de la configuration

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

Comment 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 faire pour replanifier les tâches configurées à l'aide de modèles intégrés dans Citrix ADM

Réutiliser les travaux de configuration d'exécution

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

Comment créer une tâche de configuration sur Citrix ADM

Comment utiliser des variables dans les 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 de Citrix ADC vers une autre sur Citrix ADM

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

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

Comment utiliser le modèle de configuration maître sur Citrix ADM

Gestion des certificats

Comment faire pour configurer une stratégie d'entreprise sur Citrix ADM

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

Comment mettre à jour un certificat installé à partir de 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 des notifications pour l'expiration du certificat SSL à partir de Citrix ADM

Comment utiliser le tableau de bord SSL sur Citrix ADM

StyleBooks

Comment utiliser StyleBooks par défaut dans Citrix ADM

Comment créer vos propres StyleBooks

Comment utiliser StyleBooks définis par l'utilisateur dans Citrix ADM

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

Comment activer l'analyse et configurer les alarmes sur un serveur virtuel défini dans un StyleBook

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

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

Comment utiliser Microsoft Exchange StyleBook dans les entreprises commerciales

Comment utiliser Microsoft SharePoint StyleBook dans les entreprises commerciales

Comment faire pour utiliser Microsoft ADFS Proxy StyleBook

Comment utiliser Oracle E-Business StyleBook

Comment faire pour utiliser SSO Office 365 StyleBook

Comment utiliser SSO Google Apps StyleBook

Gestion des événements

Comment définir l'âge des événements pour les événements sur Citrix ADM

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

Comment définir des notifications par e-mail répétées pour les événements à partir 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 Citrix ADC

Comment afficher le résumé des événements dans Citrix ADM

Comment afficher les gravités d'événements et les biais des interruptions SNMP sur Citrix ADM

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

Comment supprimer les messages Syslog dans Citrix ADM

Questions fréquentes

April 29, 2021

Combien d'agents dois-je installer ?

Le nombre d'agents dépend du nombre d'instances gérées dans un datacenter et du débit total. Citrix recommande d'installer au moins un agent pour chaque centre de données.

Comment puis-je installer plusieurs agents ?

Vous ne pouvez installer qu'un seul agent lorsque vous vous connectez au service pour la première fois. Pour ajouter plusieurs agents, terminez d'abord la configuration initiale, puis accédez à **Paramètres** > **Configurer les agents** .

Puis-je passer d'un agent intégré à un agent externe ?

Oui, tu peux. Pour de plus amples informations, consultez la section Transition d'un agent intégré à un agent externe.

Comment obtenir un nouveau code d'activation si je le perds ?

Si vous effectuez l'intégration pour la première fois, accédez à l'interface graphique du service, accédez à l'écran **Configurer l'agent**, puis cliquez sur **Générer le code d'activation** .

En essayant d'installer un second agent, pour générer un nouveau code d'activation, accédez à **Réseaux > Agents > Générer un code d'activation.**

Comment ouvrir une session sur la machine virtuelle de l'agent ? Quelles sont les informations d'identification par défaut ?

Si votre agent est installé sur un hyperviseur ou un cloud Microsoft Azure, les informations d'identification d'ouverture de session par défaut pour l'agent de service ADM sont `nsrecover`/`nsroot`, ce qui ouvre l'invite shell de l'agent.

Si votre agent est installé sur AWS, les informations d'identification par défaut pour se connecter à l'agent de service Citrix ADM sont`nsrecover`/`instance id`.

Quelles sont les ressources nécessaires pour installer un agent sur un hyperviseur local ?

32 Go de RAM, 8 CPU virtuels, 500 Go de stockage, 1 interface réseau virtuel, débit de 1 Gbit/s

Puis-je installer deux agents dans une configuration HA ?

Non, vous ne pouvez pas.

Dois-je affecter un disque supplémentaire à l'agent pendant le provisionnement ?

Non, vous n'avez pas besoin d'ajouter un disque supplémentaire. L'agent est utilisé uniquement comme intermédiaire entre Citrix ADM et les instances de votre datacenter d'entreprise ou sur le cloud. Il ne stocke pas les données d'inventaire ou d'analyse qui nécessiteraient un disque supplémentaire.

Puis-je réutiliser mon code d'activation avec plusieurs agents ?

Non, vous ne pouvez pas.

Comment réexécuter les paramètres réseau si j'ai entré une valeur incorrecte ?

Accédez à la console de l'agent sur votre hyperviseur, connectez-vous à l'invite shell à l'aide des informations d'identification nsrecover/nsroot, puis exécutez la commande `networkconfig`.

Que dois-je faire si l'inscription de mon agent échoue ?

- Assurez-vous que votre agent a accès à Internet (configurez DNS).
- Assurez-vous d'avoir copié correctement le code d'activation.
- Assurez-vous que vous avez saisi l'URL du service correctement.
- Assurez-vous que les ports requis sont ouverts.

L'enregistrement est réussi, mais comment puis-je savoir si l'agent fonctionne correctement ?

Une fois l'agent enregistré, accédez à Citrix ADM et accédez à l'écran **Configurer l'agent** . Vous pouvez voir l'agent découvert à l'écran. Si l'agent fonctionne correctement, une icône verte apparaît. Si elle n'est pas en cours d'exécution, l'icône rouge apparaît.

Comment puis-je connecter des agents à Citrix ADM à l'aide d'un serveur proxy ?

Vous pouvez connecter des agents au service Citrix ADM à l'aide d'un serveur proxy. Les agents transmettent toutes leurs données au serveur proxy, qui les envoie ensuite à Citrix ADM via Internet.

Pour transférer des données à l'aide du serveur proxy, tapez les détails du serveur proxy sur l'agent à l'aide du script suivant : proxy_input.py, puis suivez les instructions fournies par le script pour entrer plus d'informations. L'agent récupère ces informations lorsqu'il se connecte à Citrix ADM à l'aide du serveur proxy.

Vous pouvez authentifier votre serveur proxy en fournissant vos informations de nom d'utilisateur et de mot de passe. Lorsque l'agent envoie les données, le serveur proxy authentifie les informations d'identification de l'utilisateur avant de les transférer à Citrix ADM.

> **Remarque Le**serveur
>
> proxy prend uniquement en charge l'authentification de base.

Je ne vois pas mes rapports Analytics

Activez Insight sur vos serveurs virtuels pour afficher les rapports Analytics. Pour plus de détails, consultez la section Activation de l'analyse.

Quelles versions des instances de Citrix ADC sont prises en charge dans Citrix ADM ?

Pour les fonctionnalités de gestion et de surveillance, les instances Citrix ADC exécutant 10.5 et versions ultérieures sont prises en charge. Certaines fonctionnalités ne sont prises en charge que sur certaines versions de Citrix ADC. Pour plus de détails, consultez Configuration système requise.

Comment exporter des rapports de tableau de bord dans Citrix ADM ?

Pour exporter le rapport d'un tableau de bord dans Citrix ADM, 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.
   Le rapport est téléchargé sur votre système.
2. Sélectionnez **Planifier l'état** pour configurer des programmes de génération et d'exportation de rapports à intervalles réguliers. Spécifiez les paramètres de récurrence de génération de rapport et créez un profil de messagerie vers lequel le rapport est exporté.
   a) **Récurrence** : sélectionnez **Quotidien**, **Hebdomadaire** ou **Mensuel** dans la zone de liste déroulante.

   > **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 Récurrence **mensuelle**, assurez-vous de saisir tous les jours où vous souhaitez que le rapport soit planifié, séparés par des virgules.

   b) **Temps de récurrence** - Entrez l'heure `Hour` **:** `Minute` au format 24 heures.
   c) **E-mail** - Activez la case à cocher, puis sélectionnez le profil dans la zone de liste déroulante, ou cliquez sur **Ajouter** pour créer un profil de messagerie.
   d) **Slack** - Activez la case à cocher, puis sélectionnez le profil dans la zone de liste déroulante, ou cliquez sur **Ajouter** 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.

Qu’est-ce que l’activation des mesures côté client ?

Lorsque les mesures côté client sont activées, ADM capture les mesures de temps de chargement et de rendu des pages HTML par injection HTML. À l’aide de ces mesures, les administrateurs peuvent identifier les problèmes de latence L7.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States